EC-Council



hide01.ir

Certified Cloud Security Engineer v1

Lab Manual

EC-COUNCIL OFFICIAL CURRICULUM

Certified Cloud Security Engineer

Version 1

hide01.ir

Lab Manual

EC-Council

Copyright © 2021 by EC-Council. All rights reserved. Except as permitted under the Copyright Act of 1976, no part of this publication may be reproduced or distributed in any form or by any means, or stored in a database or retrieval system, without the prior written permission of the publisher, with the exception that the program listings may be entered, stored, and executed in a computer system, but may not be reproduced for publication without the prior written permission of the publisher, except in the case of brief quotations embodied in critical reviews and certain other noncommercial uses permitted by copyright law. For permission requests, write to EC-Council, addressed "Attention: EC-Council," at the address below:

EC-Council New Mexico
101C Sun Ave NE
Albuquerque, NM 87109

Information contained in this publication has been obtained by EC-Council from sources believed to be reliable. EC-Council takes reasonable measures to ensure that the content is current and accurate; however, because of the possibility of human or mechanical error, we do not guarantee the accuracy, adequacy, or completeness of any information and are not responsible for any errors or omissions nor for the accuracy of the results obtained from use of such information.

The courseware is a result of extensive research and contributions from subject-matter experts from all over the world. Due credits for all such contributions and references are given in the courseware in the research endnotes. We are committed to protecting intellectual property rights. If you are a copyright owner (an exclusive licensee or their agent) and you believe that any part of the courseware constitutes an infringement of copyright, or a breach of an agreed license or contract, you may notify us at **legal@eccouncil.org**. In the event of a justified complaint, EC-Council will remove the material in question and make necessary rectifications.

The courseware may contain references to other information resources and security solutions, but such references should not be considered as an endorsement of or recommendation by EC-Council.

Readers are encouraged to report errors, omissions, and inaccuracies to EC-Council at **legal@eccouncil.org**. If you have any issues, please contact us at **support@eccouncil.org**.

NOTICE TO THE READER

EC-Council does not warrant or guarantee any of the products, methodologies, or frameworks described herein nor does it perform any independent analysis in connection with any of the product information contained herein. EC-Council does not assume, and expressly disclaims, any obligation to obtain and include information other than that provided to it by the manufacturer. The reader is expressly warned to consider and adopt all safety precautions that might be indicated by the activities described herein and to avoid all potential hazards. By following the instruction contained herein, the reader willingly assumes all risks in connection with such instructions. EC-Council makes no representations or warranties of any kind, including but not limited to the warranties of fitness for particular purpose or merchantability, nor are any such representations implied with respect to the material set forth herein, and EC-Council takes no responsibility with respect to such material. EC-Council shall not be liable for any special, consequential, or exemplary damages resulting, in whole or in part, from the reader's use of or reliance upon this material.

Notice: Third-Party Connected Apps and Paid Services

Introduction

The guiding principle of EC-Council Education Content and Labs is simple, we want to provide a safe environment to learn, practice, and assess Cyber Security Skills that directly translate to Job-ready skills. We believe in providing our students, educator partners, and professionals with real software and live experiences that behave like those in the "real world" because they are the actual tools and services used in the field, not simulations.

Third-Party and Internet Connected Resources

To provide the most realistic learning experience, EC-Council may employ connections to live networks and services through its labs and lab platforms. While many software and service providers provide education use licenses, trials, or are Open Source, some require a live account with setup requirements and agreements you must review and consent to in order to participate in and/or complete the exercises in our Labs.

Subscription Fees and/or License Fees

EC-Council will never ask you for payment details or sensitive information during our course of learning, however, some of our Live Labs connect to third-party services such as Amazon AWS, Google Cloud Platform, Microsoft Azure, etc. While many of these service providers allow you to sign up for free-tier usage, Education Accounts, or provide promotional credits for trials, many do ask for your credit card during sign-up and may bill for the use of their services, during and even after you have completed your course of study with EC-Council. Be aware, signing up for third-party services may incur expenses related to the use of their services. Our labs can be completed without any additional charges unless explicitly marked, but you are ultimately responsible for any services you may intentionally or unintentionally sign up for when connected to those platforms.

hitec01_it

CCSE, AWS, Azure, and GCP

CCSE provides labs that utilize three major cloud platforms, AWS, Azure, and GCP. In order to provide a thorough hands-on experience, you must create accounts with each cloud platform. While account creation typically requires a credit card, you do have options to bypass this; ask your school or training center if they are an education partner with these cloud players and complete your sign up with an education account, or you can apply directly for a student account with each platform. If you choose to set up a live account with a credit card, be sure to check with each platform how to identify what services are being created that may incur charges. We do provide guides in our programs to check that all services created have been removed, and we do notify you if a lab activity may incur charges if done incorrectly or not terminated, but be aware, you are connecting to live third party services that charge for the use of their platforms if you exceed free tier usage guidelines.

Alternatives

If you are unable to secure an Education/Student account and are not comfortable creating a live account in these platforms, EC-Council provides comprehensive Lab Guides that include complete instruction sets with screenshots (images) of each step. EC-Council also provides video-based walk-through of each lab for you to follow along without actually creating an account. Though you won't be creating an account or performing the live configurations with this method, you will still receive adequate exposure to the platforms, configuration steps, techniques, and knowledge elements required for you to prepare for certification or grasp the knowledge conveyed in the program.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Table of Contents

Module Number	Module Name	Page No.
01	Introduction to Cloud Security	---
02	Platform and Infrastructure Security in Cloud	1
03	Application Security in Cloud	243
04	Data Security in Cloud	363
05	Security Operations in Cloud	637
06	Penetration Testing in Cloud	773
07	Incident Response in Cloud	831
08	Forensic Investigation in Cloud	955
09	Business Continuity and Disaster Recovery in Cloud	1057
10	Governance, Risk Management, and Compliance in Cloud	1273
11	Standards, Policies, and Legal Issues in Cloud	1323

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

CCSE Lab Manual

Platform and Infrastructure Security in Cloud

hide01.ir

Module 02

Module 02 – Platform and Infrastructure Security in Cloud

Caution: Completing the steps in this exercise will require you to sign up for third party services that may incur fees. Be sure to follow proper guidelines for removing billable services from your account before you leave your lab. Deviating from our specific instructions may result in unwanted fees for services from third-party service providers. Be sure to check with your school, instructor, or employer if education accounts are available. If you sign-up and provide your credit card, you will be responsible for any fees related to services you activate. We strongly advise you not to deviate from our explicit instructions while connected to the platforms unless you are fully aware of what the services are and what the respective third-party charges for their use.

vidoo1.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 1

Implementing AWS Identity and Access Management

Amazon Web Services (AWS) provide phased security services through Identity and Access Management (IAM). A network defender can easily manage and control access to AWS services and resources for AWS users using IAM.

ICON KEY

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

Lab Scenario

AWS IAM enables network defenders to control access to AWS services and resources securely. It allows the creation of access rules and permissions for specific users and applications. It controls who is authenticated (signed in) and authorized (has permissions) to access resources. This helps network defenders assign role-based access controls for accessing critical information within the enterprise.

Lab Objectives

This lab will demonstrate how to create an IAM group and user, attach a policy to the user, and enable multi-factor authentication (MFA) for adding a two-factor authentication for individual users to ensure additional security for the AWS user accounts.

In this lab, you will learn to do the following:

- Create an IAM group in AWS
- Create an IAM user in AWS
- Assign a permission policy to a user
- Create a custom IAM policy in AWS
- Enable MFA

Lab Environment

To perform this lab, you need the following:

- **Admin Machine** VM
- **Administrative** privileges
- Registered AWS account

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Duration

Time: 15 minutes

Overview of IAM

IAM enables role-based access control for accessing critical information within the enterprise. It comprises business processes, policies, and technologies that allow the monitoring of electronic or digital identities. IAM provides tools and technologies to regulate user access (creating, managing, and removing access) to systems or networks based on the roles of individual users within the enterprise. Organizations generally prefer all-in-one authentication, which can be extended to identity federation. Identity federation includes IAM with single sign-on (SSO) and a centralized Active directory (AD) account for a secure management. MFA is enabled for the root user account and its associated user accounts in the cloud. MFA is used to control access to cloud service APIs. However, the best option is to choose either a virtual MFA or a hardware device.

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., AWS), the application interface may be updated with time. Hence, in case you happen to work on an updated version of AWS, 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.

hidden_i

Note: Before starting this lab, you should create an AWS Free Tier account using the following link: aws.amazon.com/free, in case you have already not created for the previous lab. Once the registration is complete, perform the following tasks:

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

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1

Creating IAM Group in AWS

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

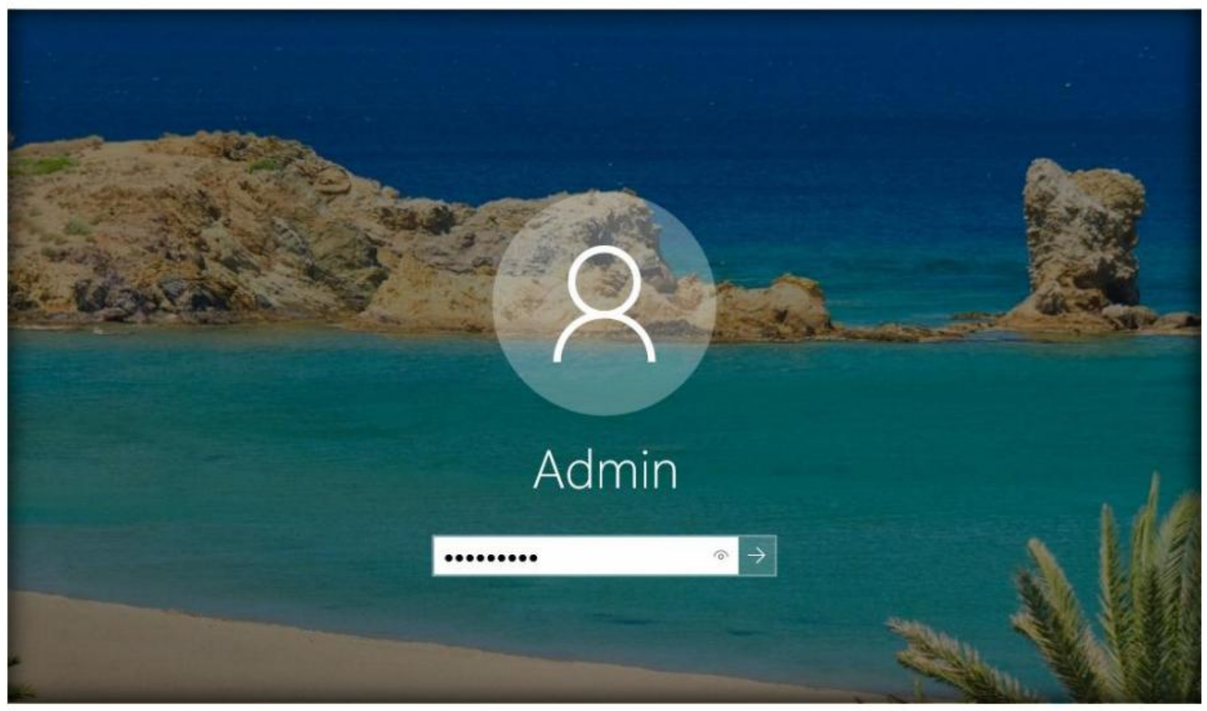


FIGURE 2.1.1: Launch Admin Machine and Log in

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

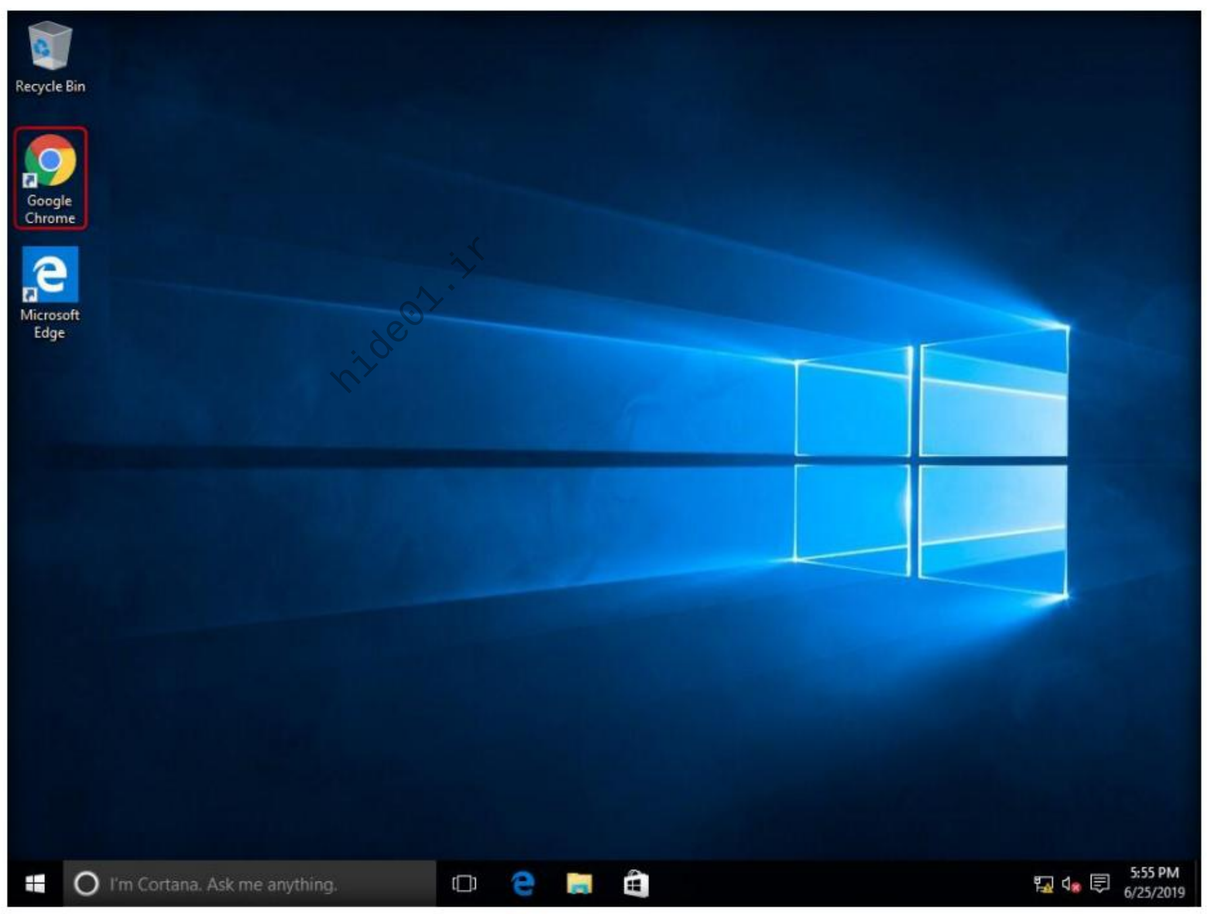


FIGURE 2.1.2: Navigating to the Chrome Browser from Taskbar

3. In the address bar of the **Google Chrome** browser, type **https://aws.amazon.com/** and press **Enter**.

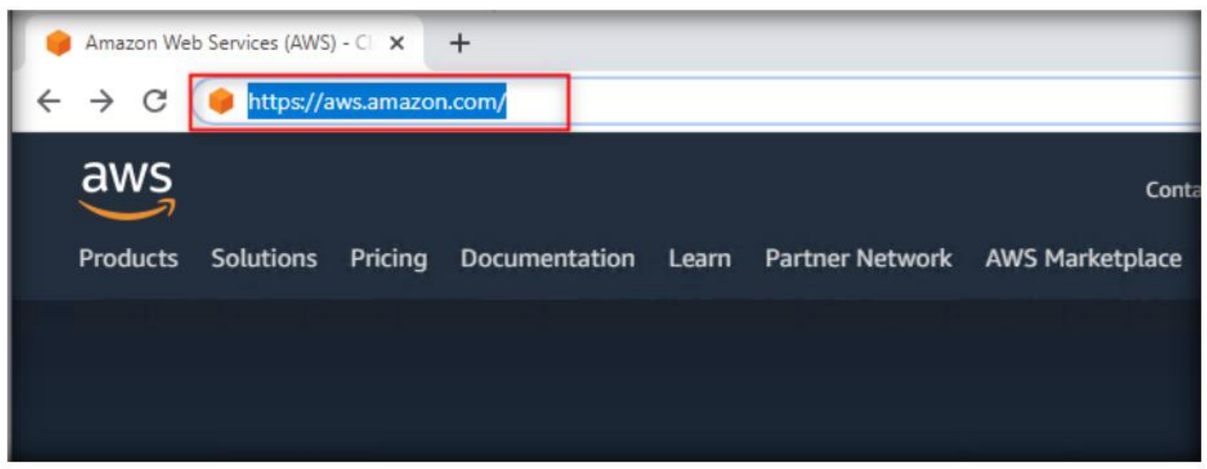


FIGURE 2.1.3: Access AWS in Browser

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

4. The **AWS Web Services -**
5. **Cloud Computing Services** page appears. Click on **AWS Management Console** from the **My Account** dropdown, as shown in the screenshot below.

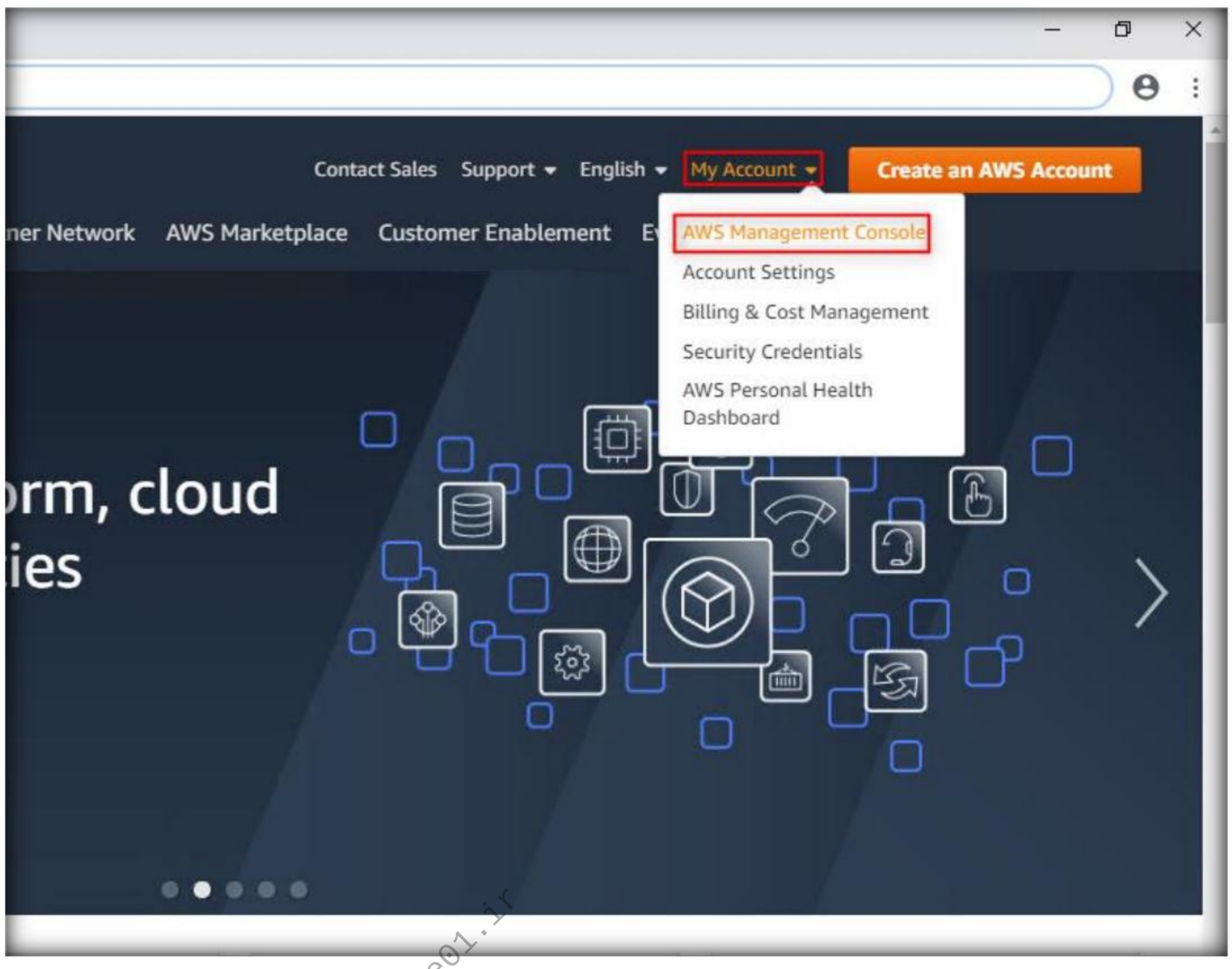


FIGURE 2.1.4: Navigate to AWS Management Console

6. The **AWS Sign-in** page appears. Choose **Root user** and type the AWS administrator account ID (Root user email address), as shown in the screenshot below, and click on **Next**.

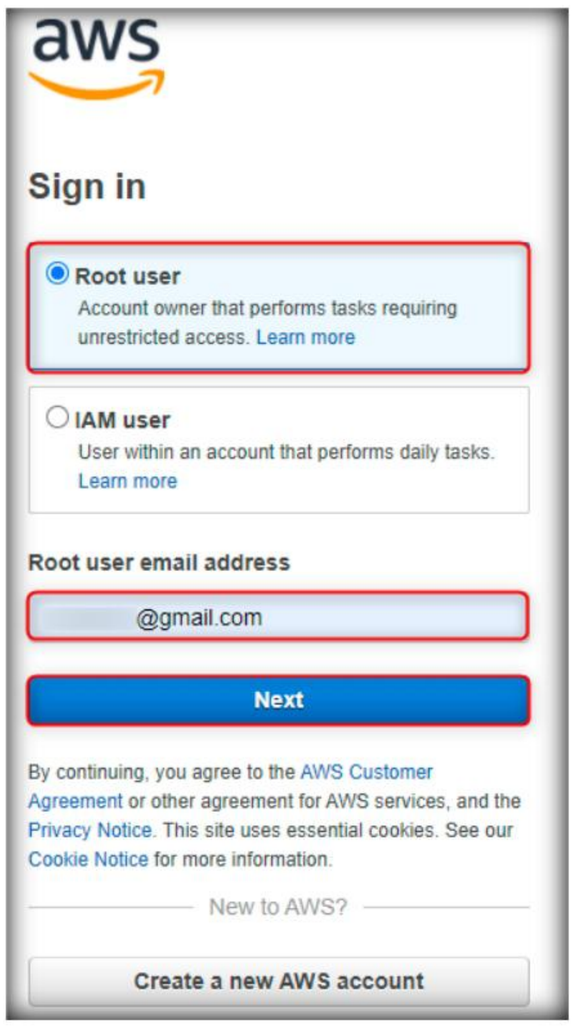


FIGURE 2.1.5: Login Credentials

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

7. The security check page appears. Type the characters shown in the image and click **Submit**.

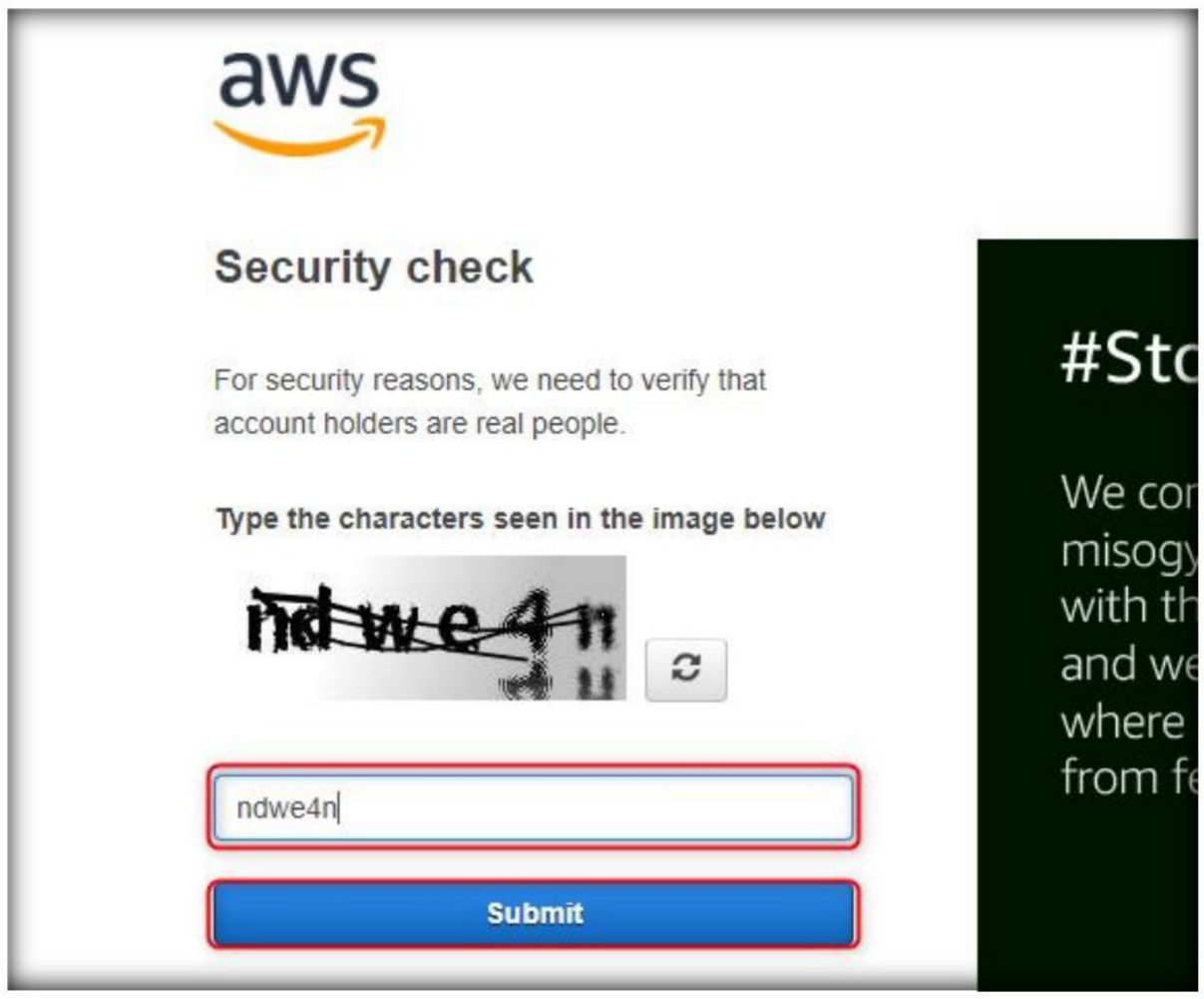


FIGURE 2.1.6: Sign-in -Security check

8. Type the password in the **Password** field and click on **Sign in,** as shown in the screenshot below.

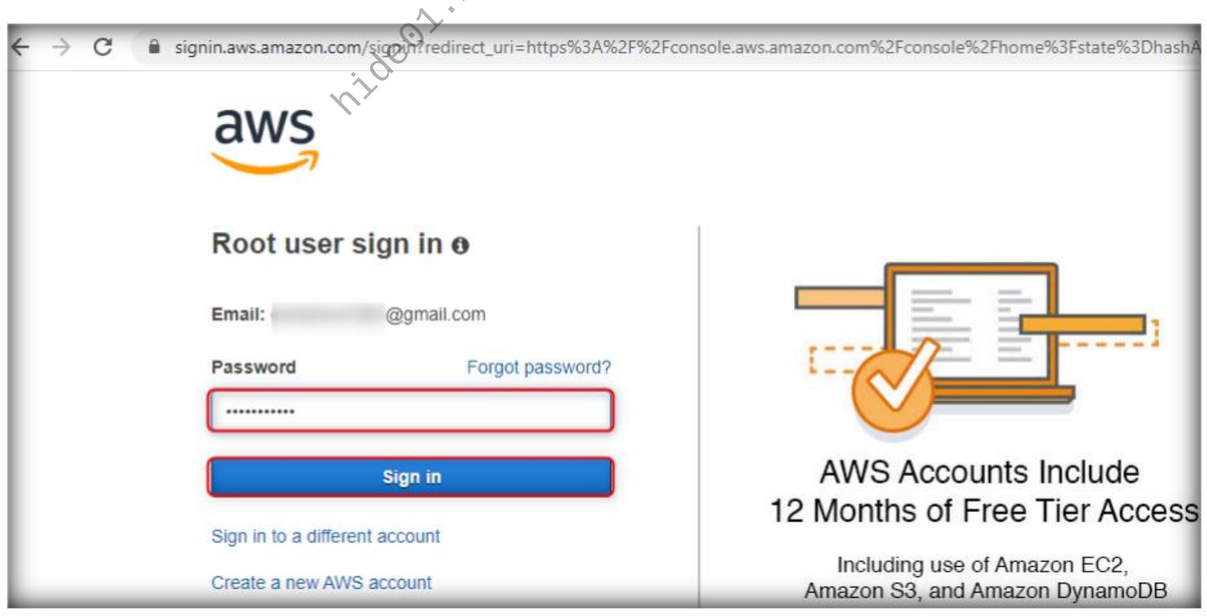


FIGURE 2.1.7: Sign-in to AWS

9. Select **Services** from the menu bar and click on **IAM** under the **Security, Identity, & Compliance** section, as shown in the screenshot below.

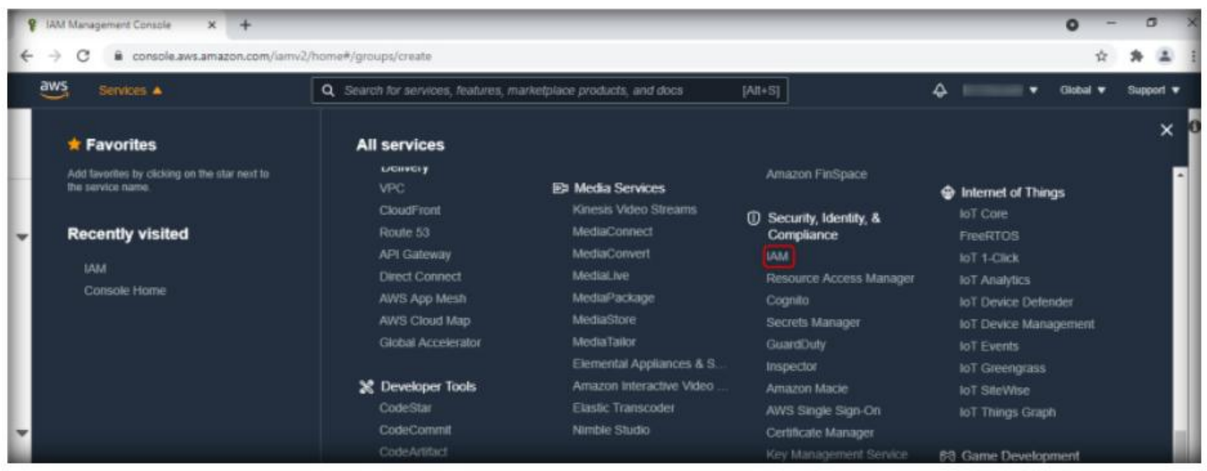


FIGURE 2.1.8: Navigate to IAM Section

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

10. On the **IAM dashboard** page, click on **User groups** in the left pane under **Access management**, as shown in the screenshot below.

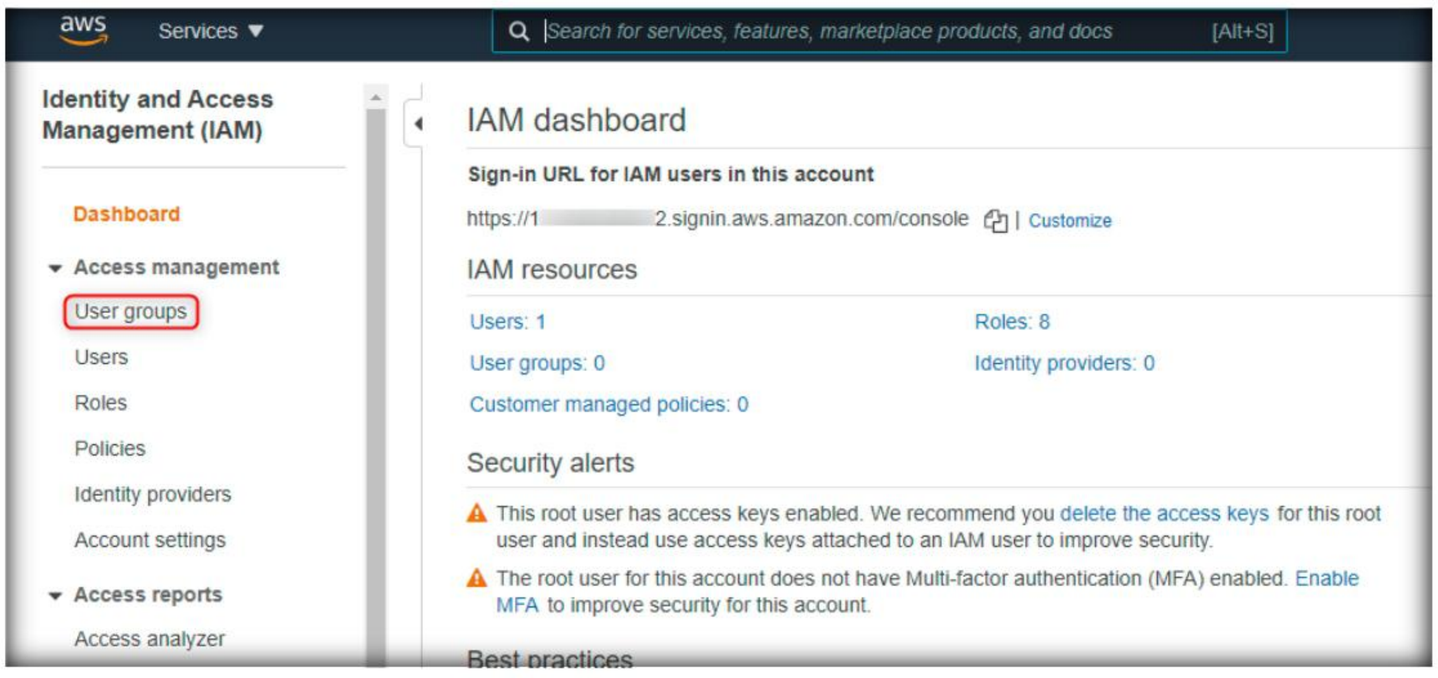


FIGURE 2.1.9: IAM Dashboard

11. Click on **Create group**.

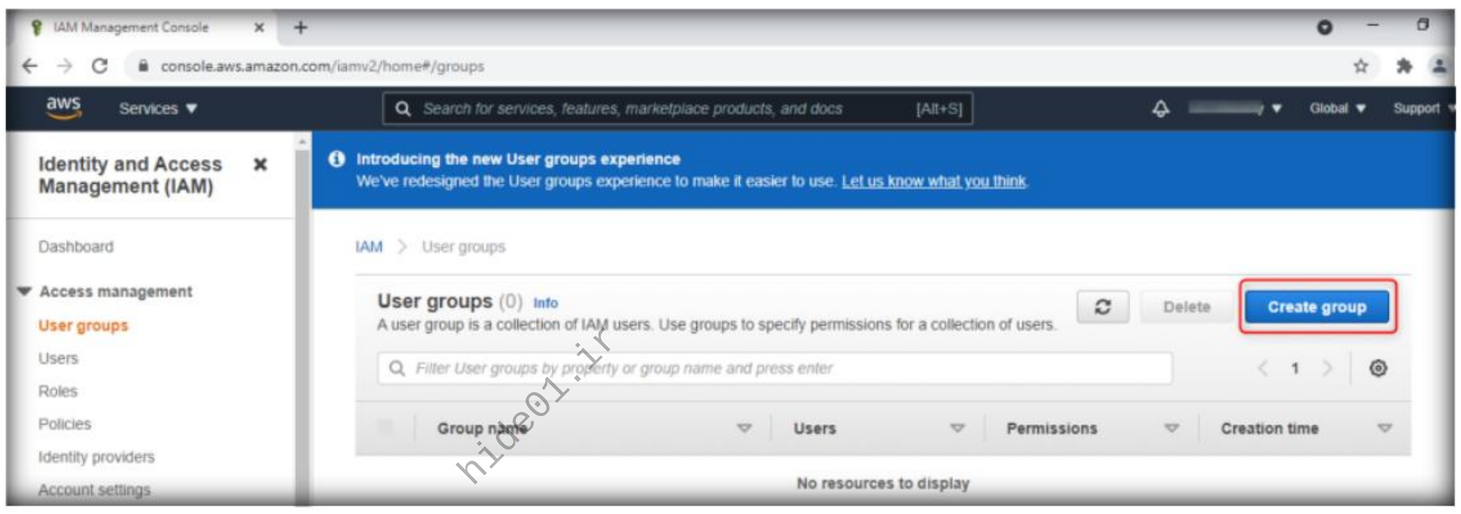


FIGURE 2.1.10: Create New Group

12. On the **Create user group** page, type the user group name in the **User group name** field (**Training_Group**). You can add any existing user to the group under **Add users to the group**. As no user has been created yet, you can leave this field blank.

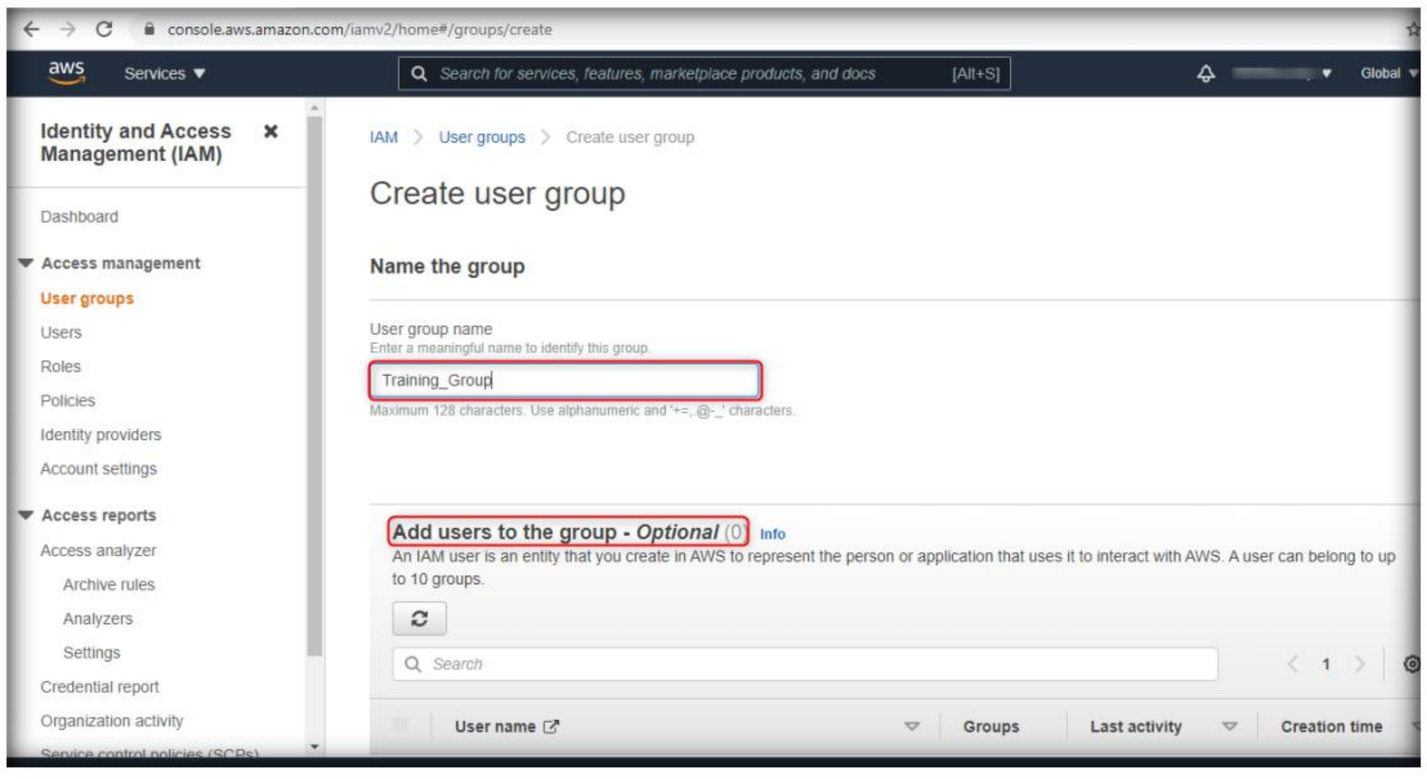


FIGURE 2.1.11: Setting Group Name

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

13. In the **Attach permissions policies** section, search for **Iamuserchangepassword**, as shown in the screenshot below. After the match record is filtered, select **IAMUserChangePassword**.

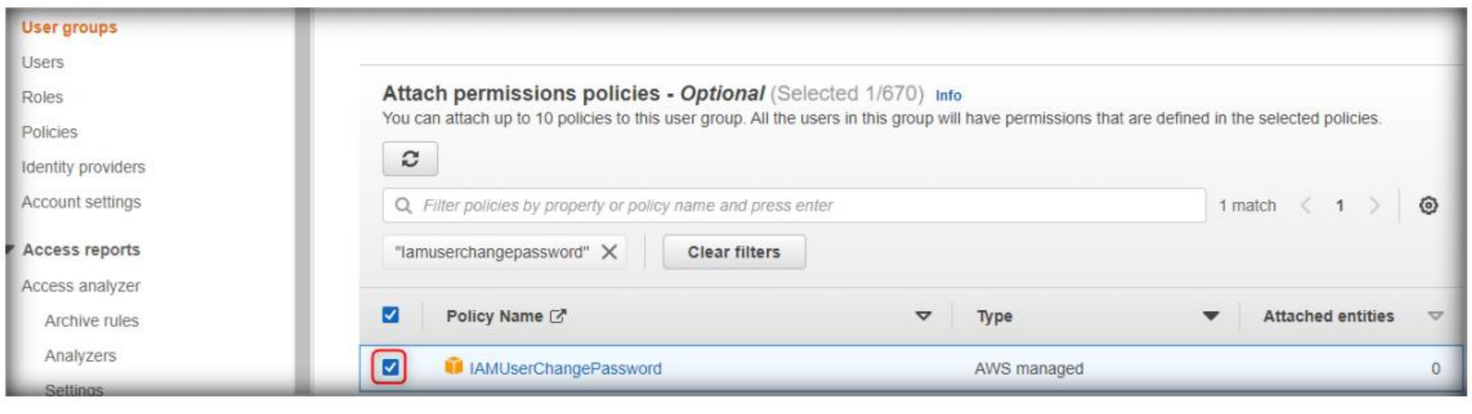


FIGURE 2.1.12: Attach Policy

14. Next, search for **databaseadministrator**. After the match record is filtered, select the **DatabaseAdministrator** policy and click on **Create group**.

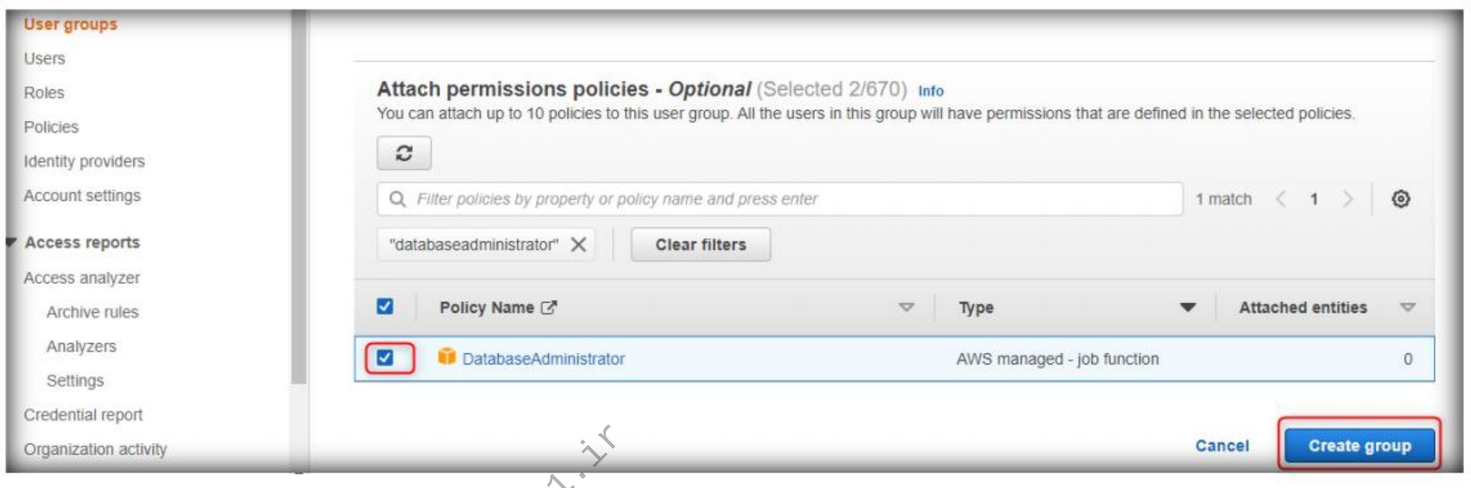


FIGURE 2.1.13: Selecting Policy and Creating Group

15. **Training_Group** will be created under **Group name,** as shown in the screenshot below.

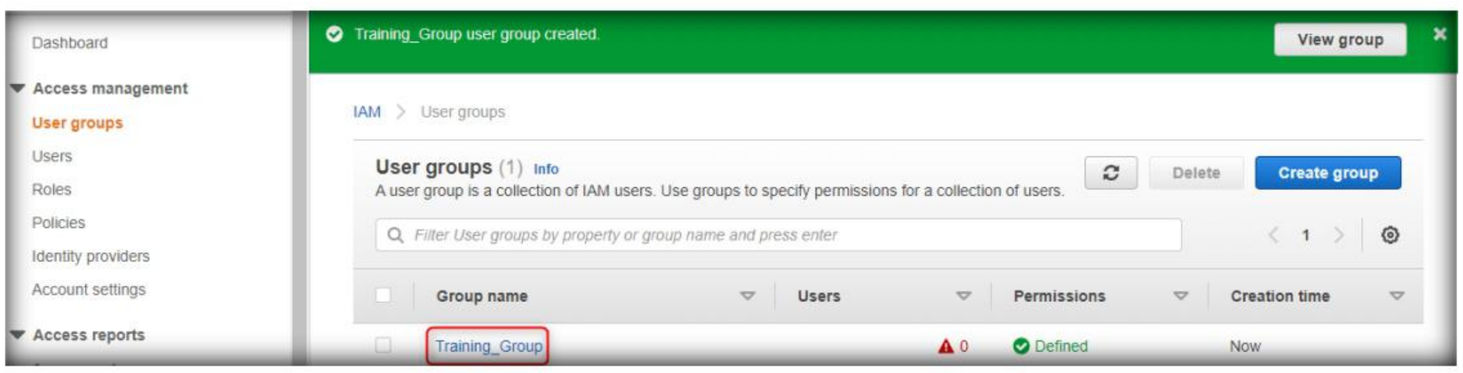


FIGURE 2.1.14: New Group Created

TASK 2

Creating IAM User in AWS

16. Select **Users** from the **Identity and Access Management (IAM)** section and click on **Add user**, as shown in the screenshot below, to create a new user.

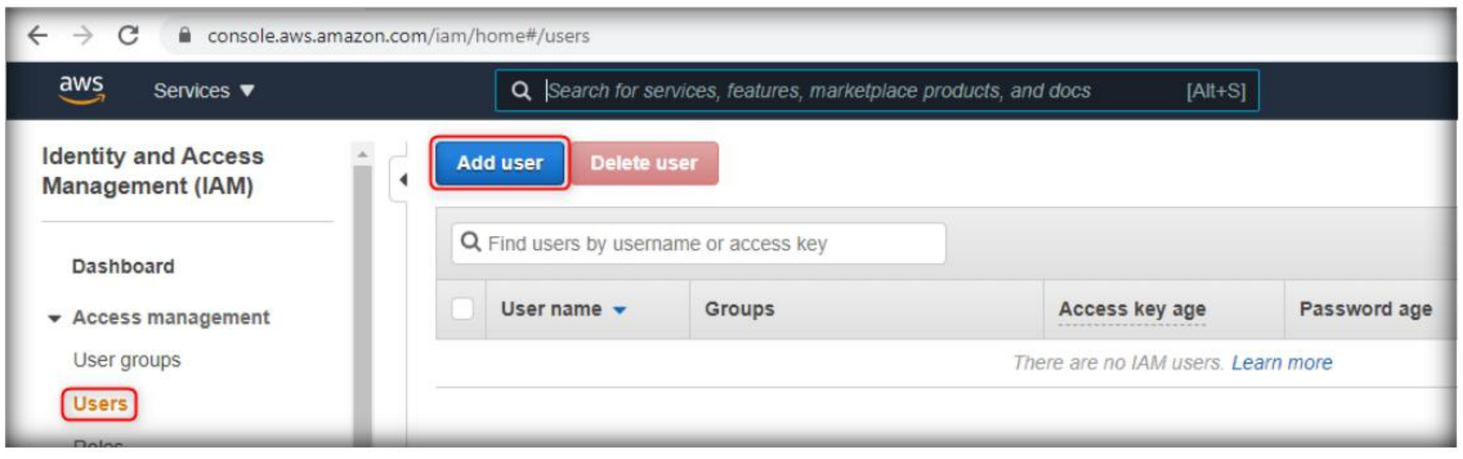


FIGURE 2.1.15: Adding New User

Certified Cloud Security Engineer Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

17. The **Add user** page appears. In the **User name** field, provide any name (e.g., **Alice**). Select **AWS Management Console access and Programmatic access** under **Access type** in the **Select AWS access type** section. Choose the **Custom password** radio button and type the password (**user@123**) in the password field, as shown in the screenshot below. **Require password reset** is optional; however, check this setting. Then, click on **Next: Permissions**.

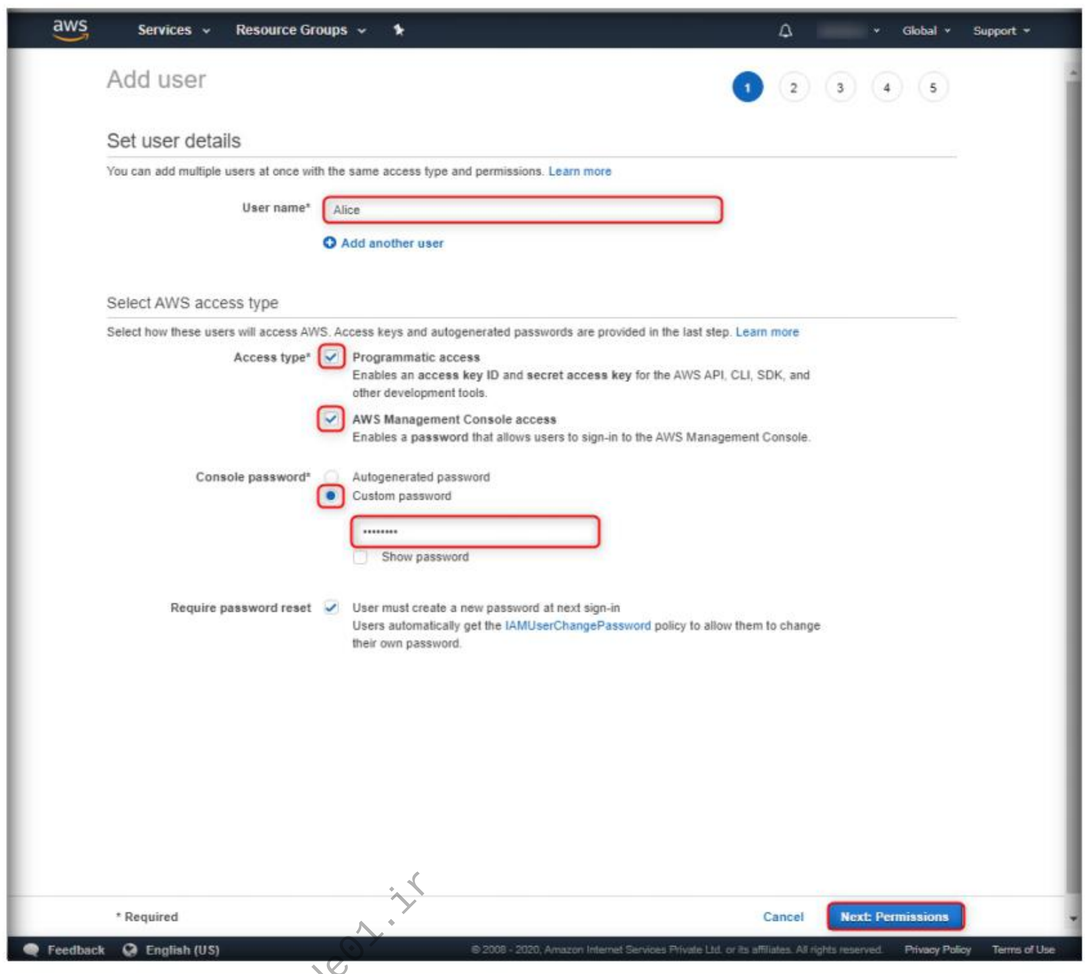


FIGURE 2.1.16: New User Details

18. In the **Set permissions** section, **Add user to group** is selected by default. Check the newly created group (**Training_Group)**, as shown in the screenshot below. You have now added the user to the group. Click on **Next: Tags**.

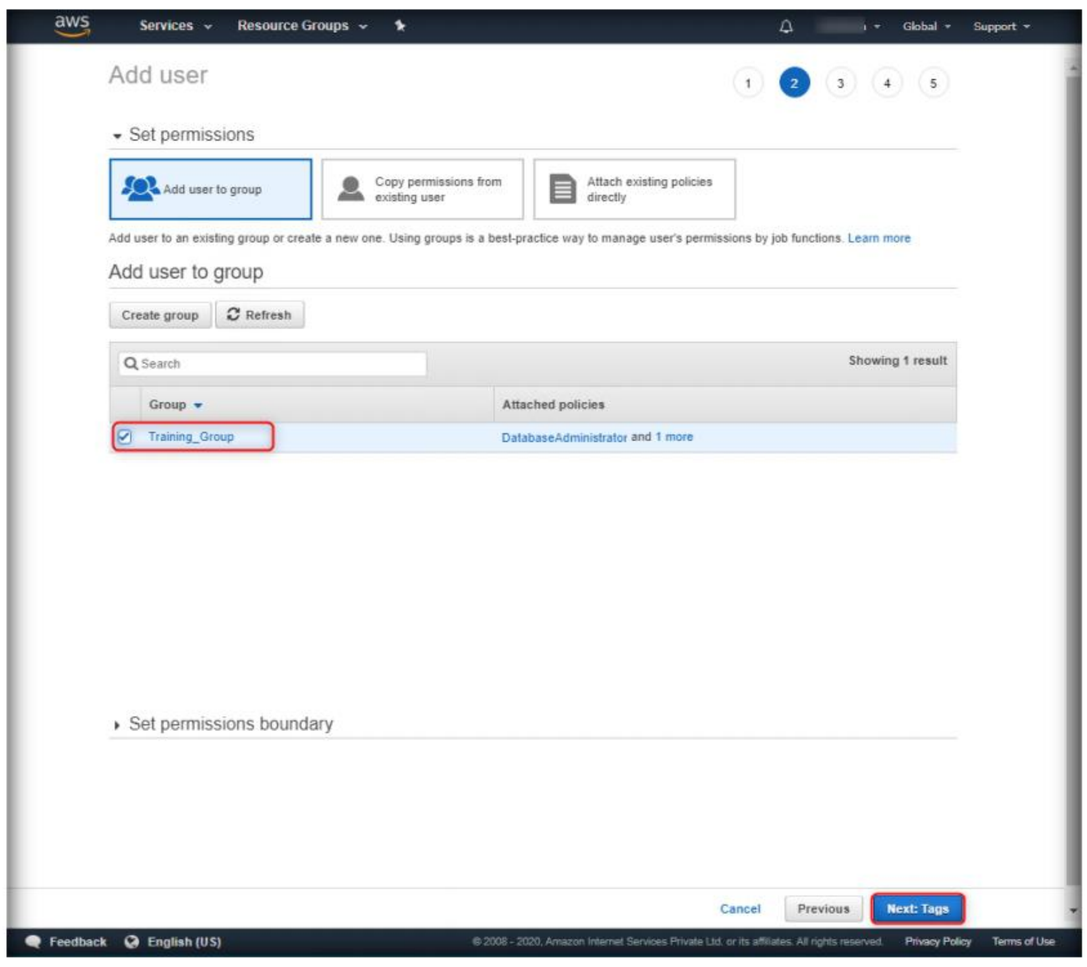


FIGURE 2.1.17: Adding User to Group

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

19. Tags are optional; however, tagging will help us later in searching for tag keys. Type **Department** in the field under **Key** and **Training** under **Value (optional)**. Then, click on **Next: Review** to start reviewing IAM user creation.

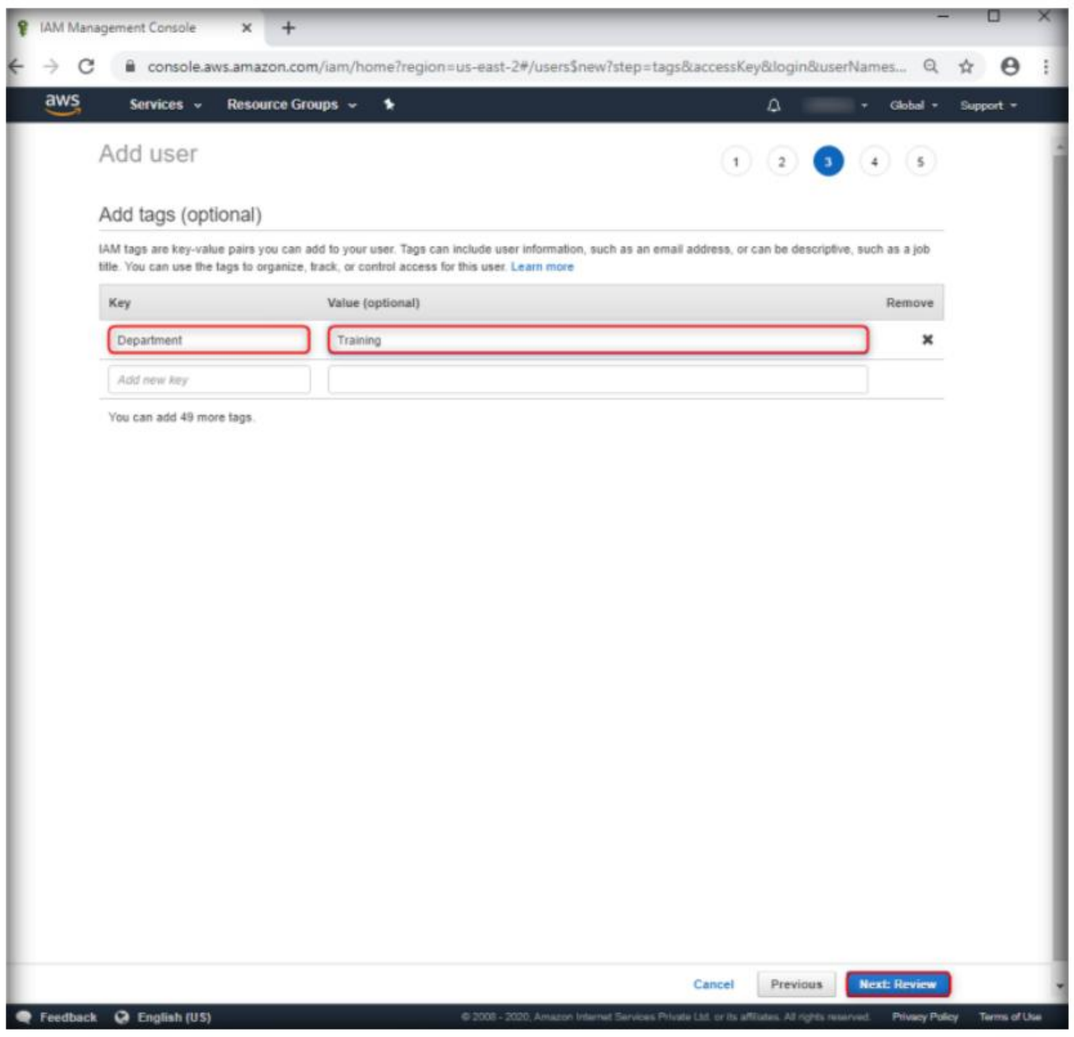


FIGURE 2.1.18: Adding Tag for User

hide01.ir

20. On the **Review** page, you can review the settings and IAM user properties before creating the user. Once you have verified the settings, click on **Create user**.

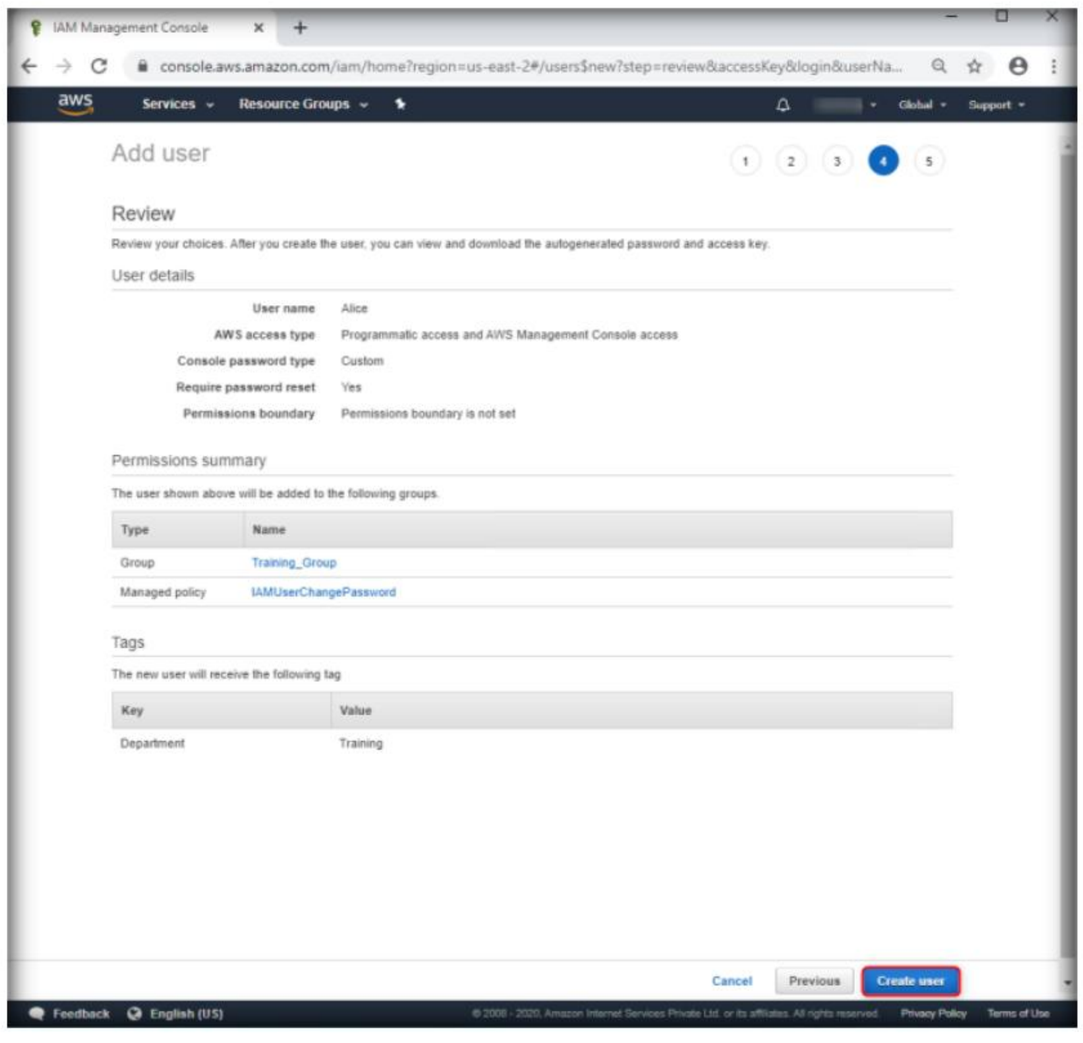


FIGURE 2.1.19: Review New User Details

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

21. After you click on **Create user**, a **Success** message is displayed, as shown in the screenshot below. You have an option to **Send email** to get the login instructions for the newly created IAM user. Click on **Close** (lower right corner of the page) to return to the IAM page. It will redirect you to the **Users** page.

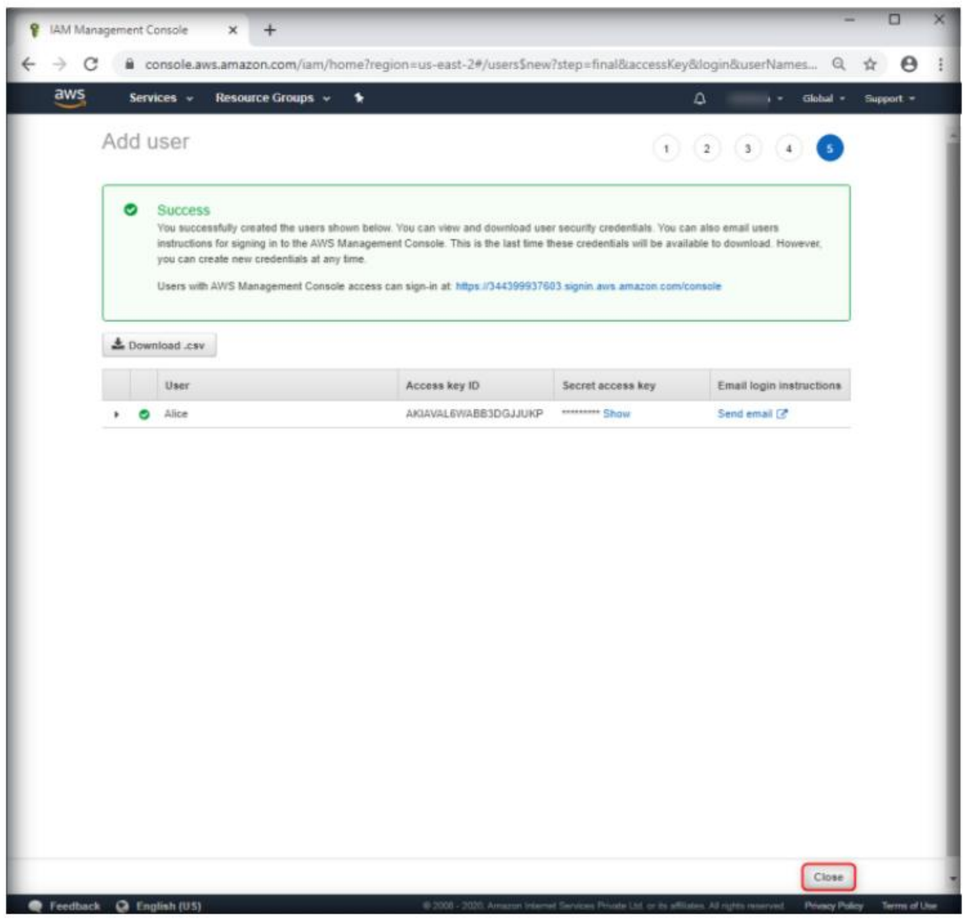


FIGURE 2.1.20: New User Added Successfully

TASK 3

Attaching a Policy to the User

22. Next, attach a policy to the user. Select the user for whom you want to add a policy. Select **Alice** in this case, as shown in the screenshot below.

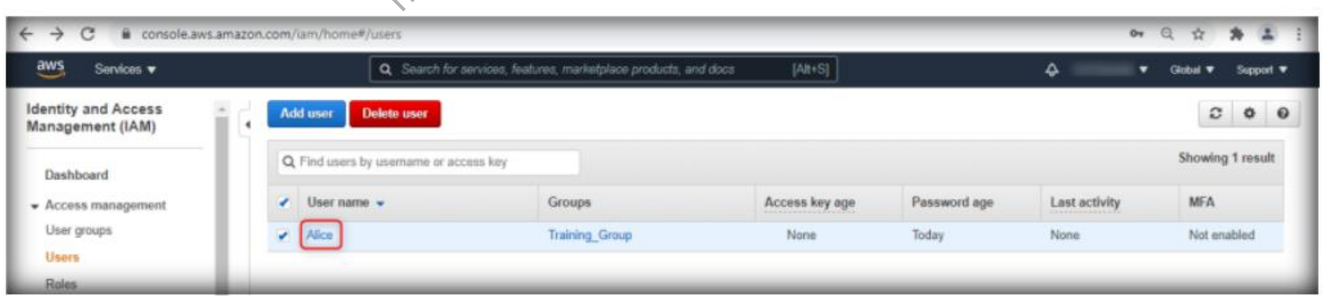


FIGURE 2.1.21: Adding Policy to User

23. The **Summary** page appears (for **Alice**) now. Click on **Add permissions**.

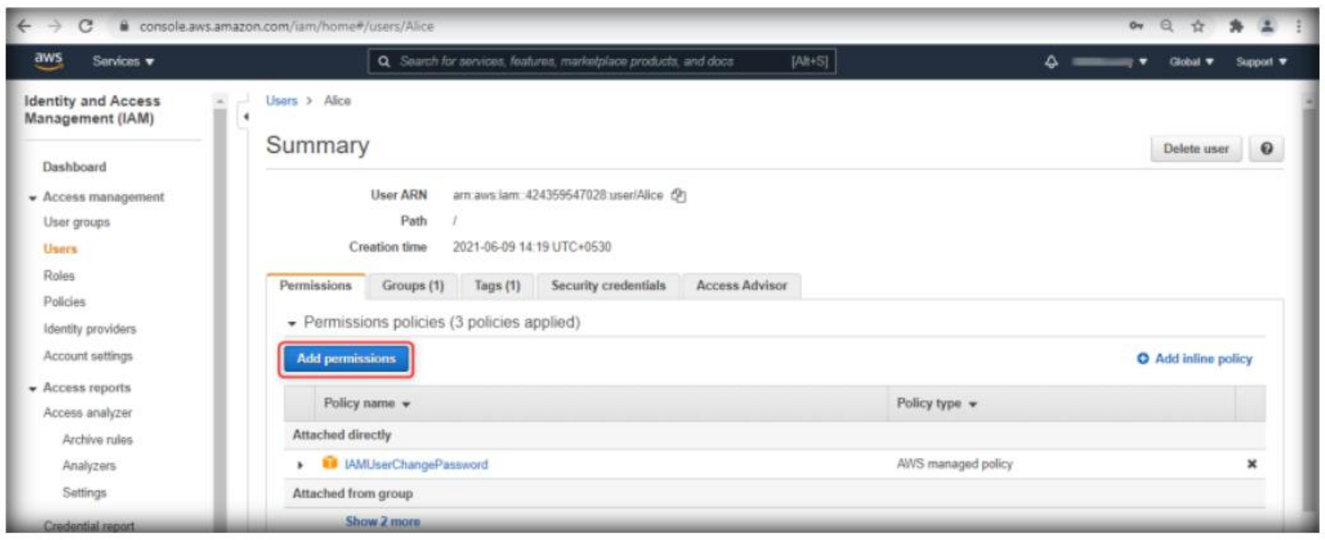


FIGURE 2.1.22: Adding Permissions

24. In the **Grant permissions** page, click on **Attach existing policies directly**.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

25. In the **Filter policies** field, search for **amazons3readonlyaccess**. This will display all pre-configured policies for S3. Select **AmazonS3ReadOnlyAccess** and click on **Next: Review**.

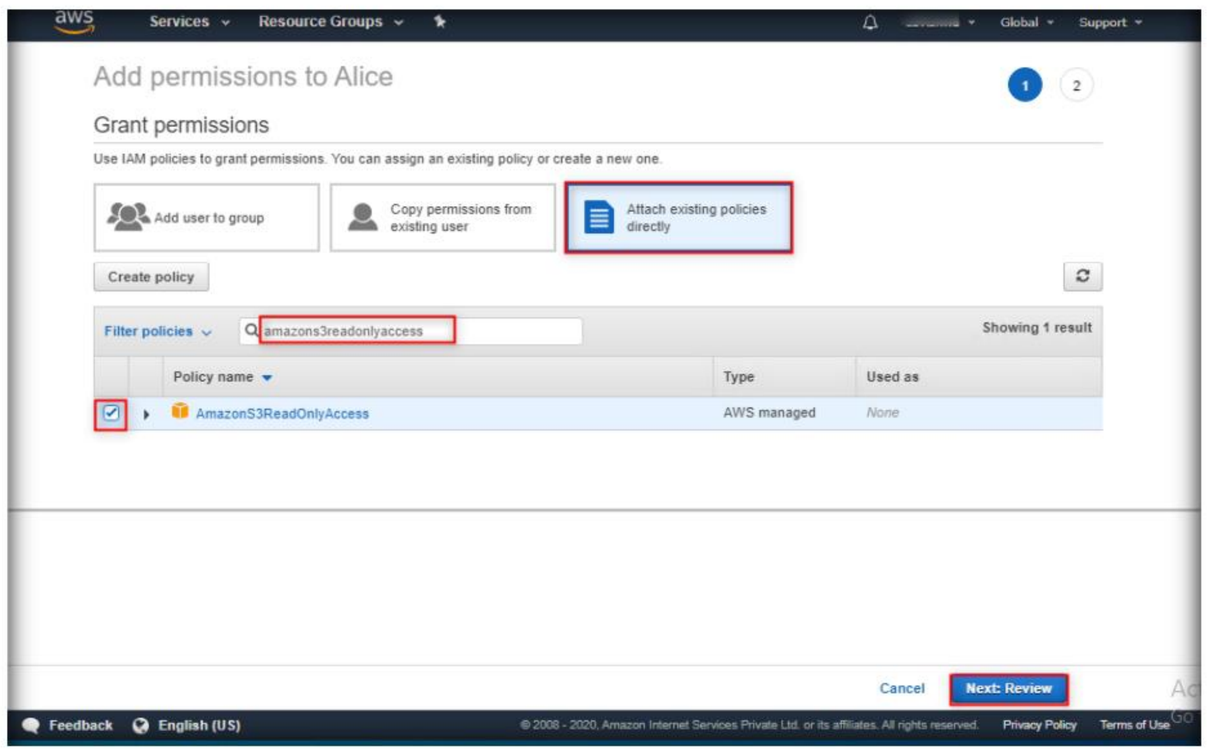


FIGURE 2.1.23: Attaching Existing Policy

26. In the **Permissions summary** page, review the policies assigned to the IAM user. After you have reviewed the policies, click on **Add permissions**.

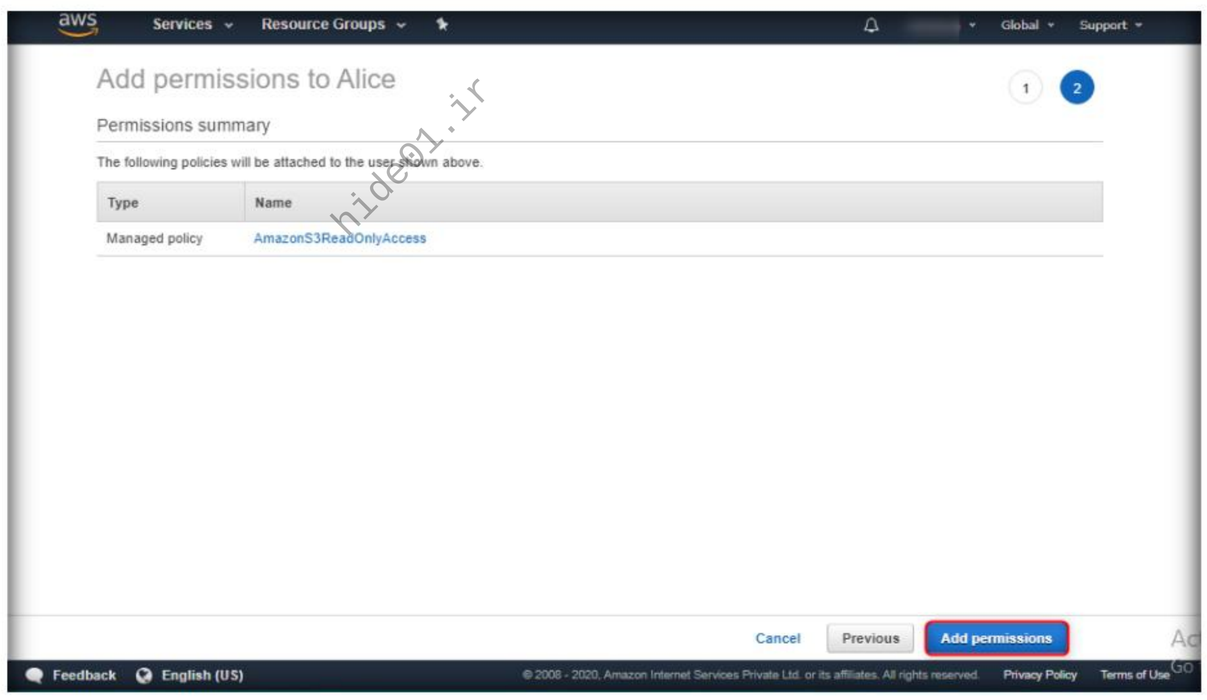


FIGURE 2.1.24: Adding Permissions

27. The assigned policy will be displayed when you view the IAM user (**Alice**). The policy is displayed under **Attached directly.**

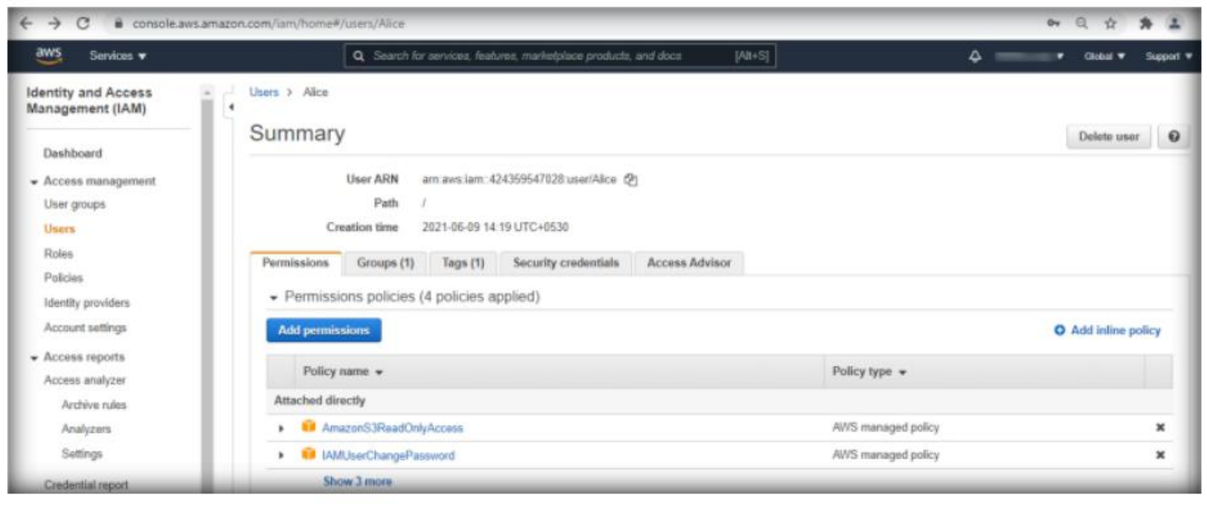


FIGURE 2.1.25: Summary of User Permissions

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 4

Creating a Custom IAM Policy in AWS

28. Next, create a custom IAM policy. Click on **Policies** under **Access management** of the **Identity and Access Management (IAM)** console, and then click on **Create policy**.

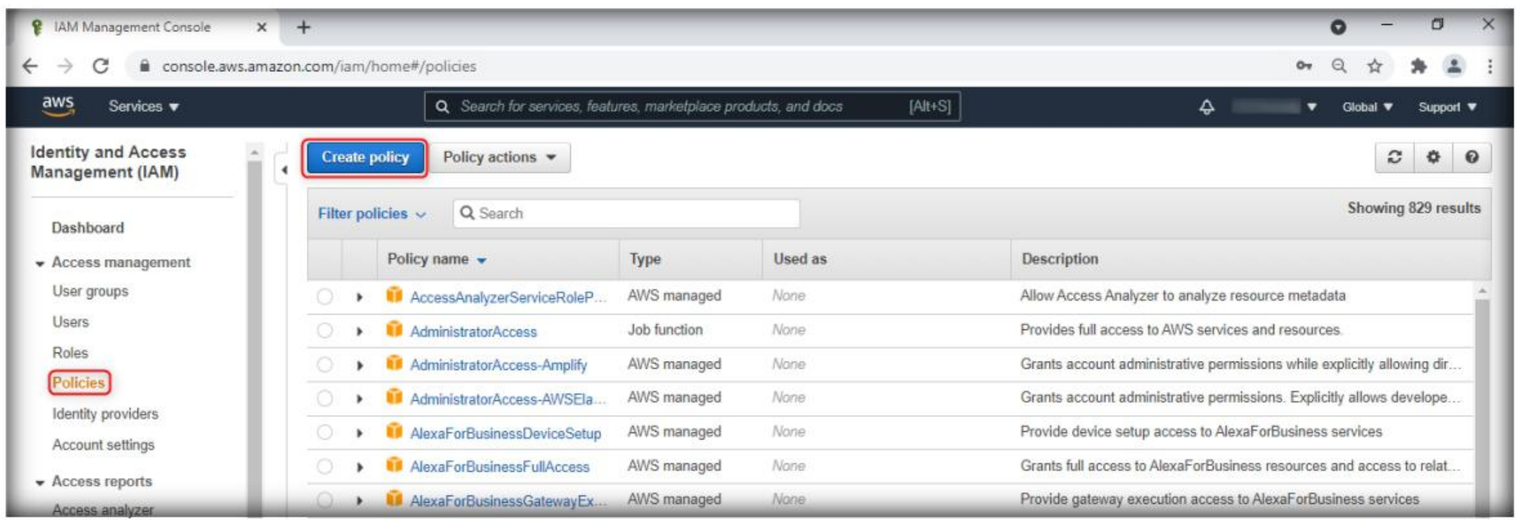


FIGURE 2.1.26: Creating New Policy

29. Specify the service you wish to use and edit the permissions. In this example, choose **CloudFront** for the **Service** field.

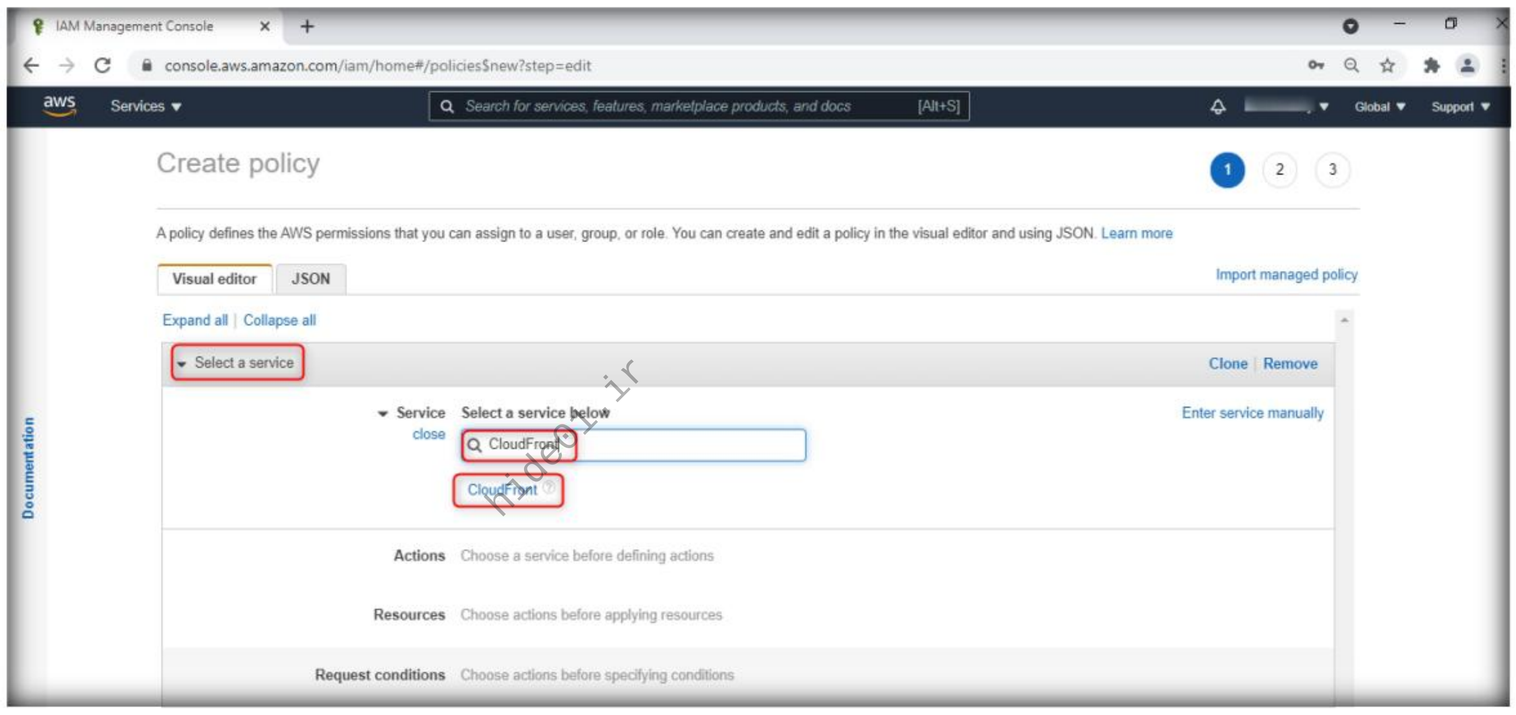


FIGURE 2.1.27: Policy for Existing Service

30. Expand the **Actions** menu to select the **Access level** for **CloudFront** service. In this example, enable only **Read** access for **CloudFront**, as shown in the screenshot below.

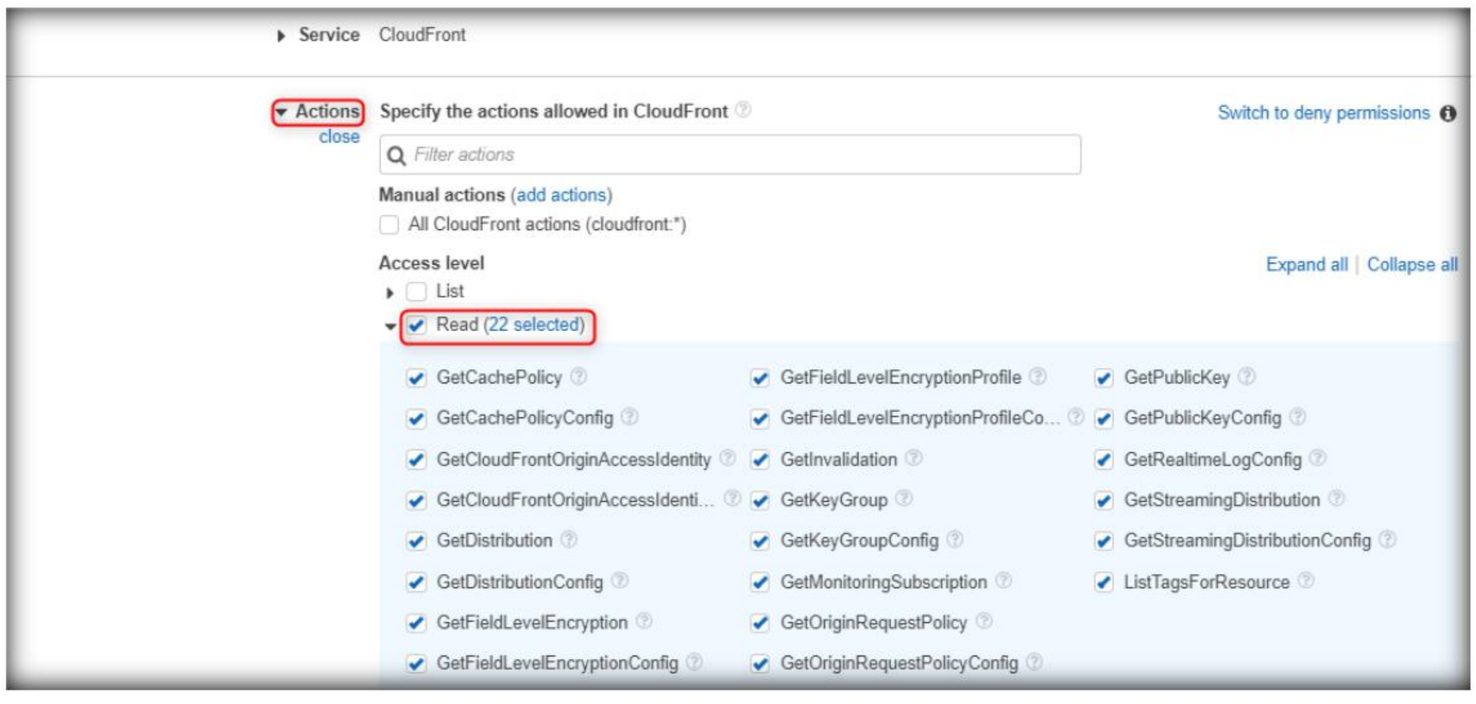


FIGURE 2.1.28: Setting Access Level in Policy

Certified Cloud Security Engineer Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

31. Scroll down and expand the **Resources** section. Then, select **All resources**.

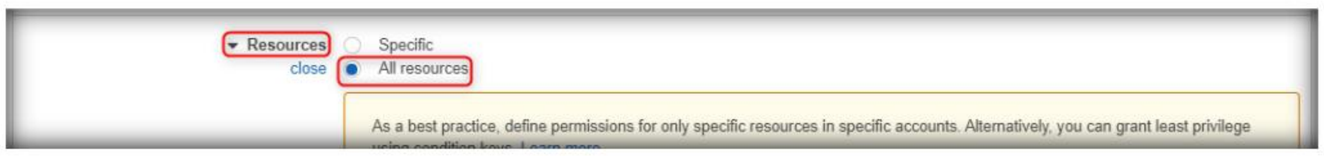


FIGURE 2.1.29: Selecting All Resources

32. Expand **Request conditions**, check **MFA required**, and click on **Next: Tags**.

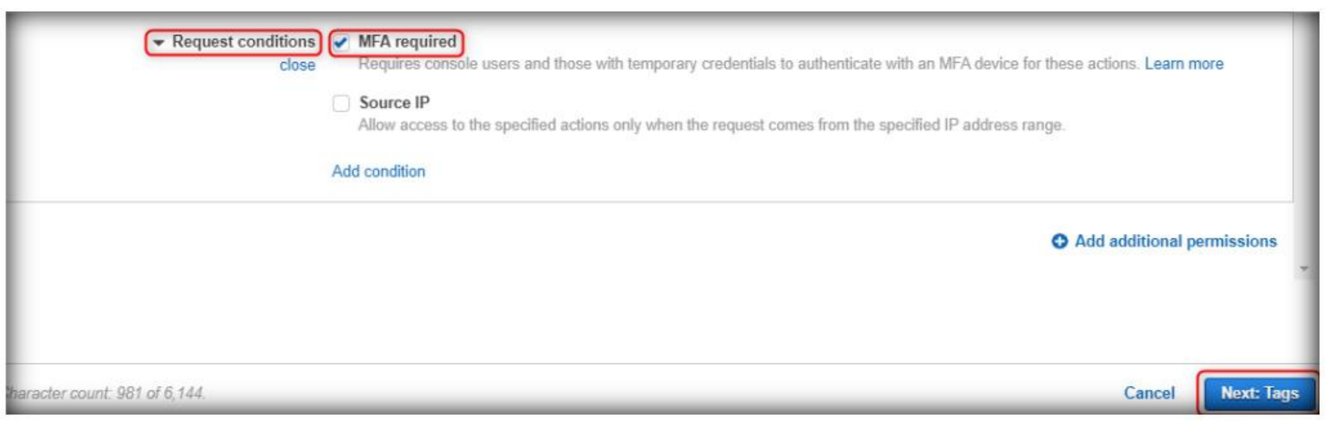


FIGURE 2.1.30: Selecting MFA Required Option

33. On the **Add tags (Optional)** page, add tags to the resource by clicking **Add tag**. Then, click on **Next: Review**. This step is optional.



FIGURE 2.1.31: Adding Tags

34. In the **Review policy** section, provide a name for the policy in the **Name** field, add a description in the **Description** field, and click on **Create Policy**, as shown in the screenshot below.

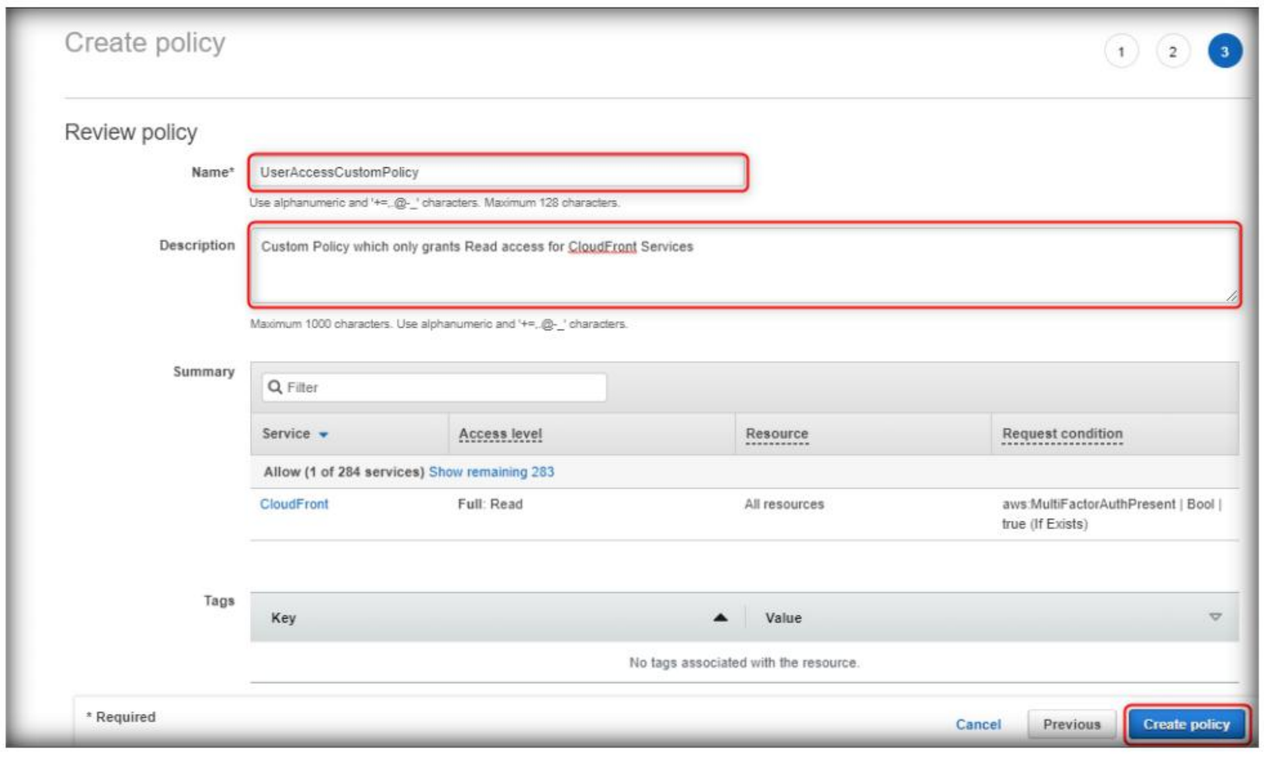


FIGURE 2.1.32: Completing Create Policy

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

35. You have successfully created a new policy, as shown in the screenshot below.

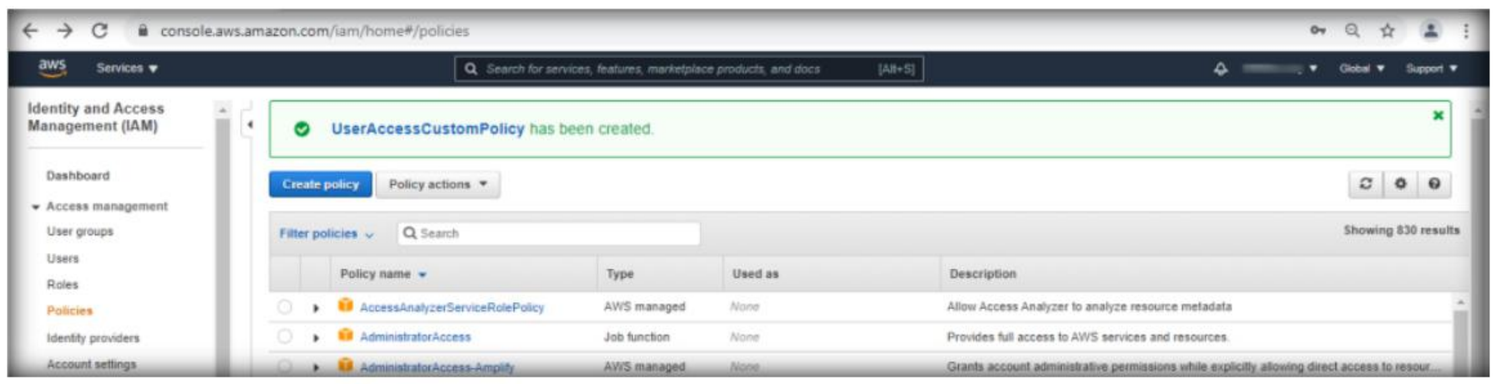


FIGURE 2.1.33: Policy Created Successfully

TASK 5

Accessing AWS Using IAM User

36. Click on **Dashboard** under the **Identity and Access Management (IAM)** section.

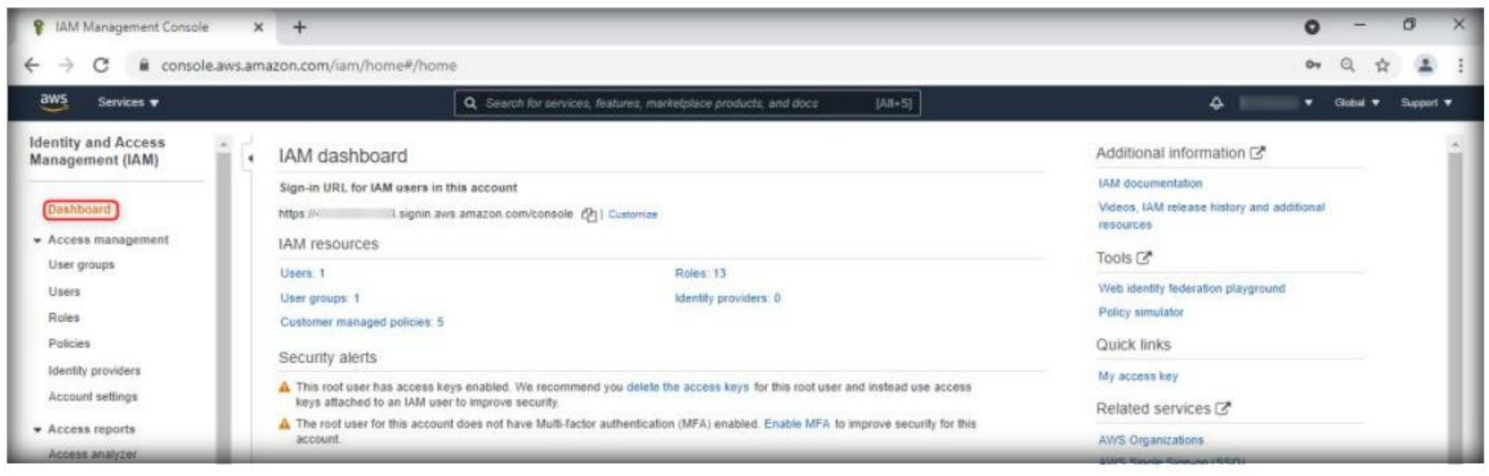


FIGURE 2.1.34: IAM Dashboard

37. You will see a **IAM users sign-in link**. Copy the link, as shown in the screenshot below.

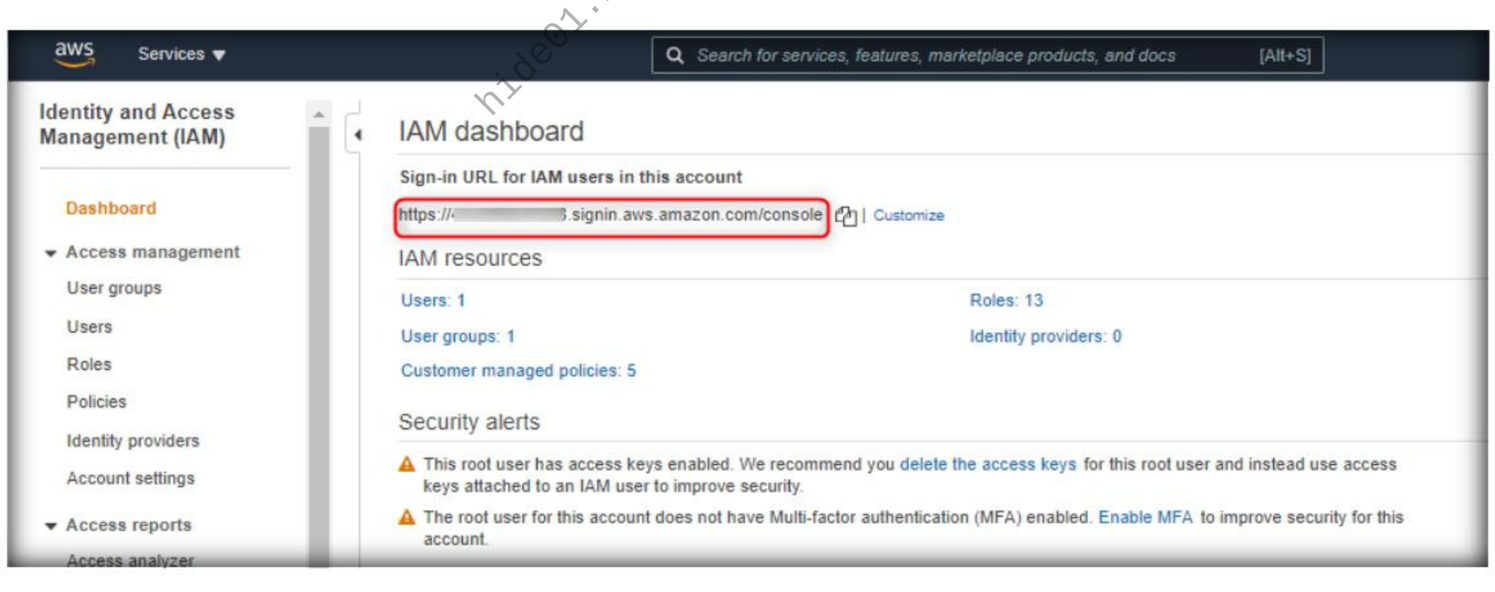


FIGURE 2.1.35: Coping IAM Users Sign-in Link

38. Open the **Google Chrome** browser in incognito mode, paste the copied URL, and hit **Enter**.

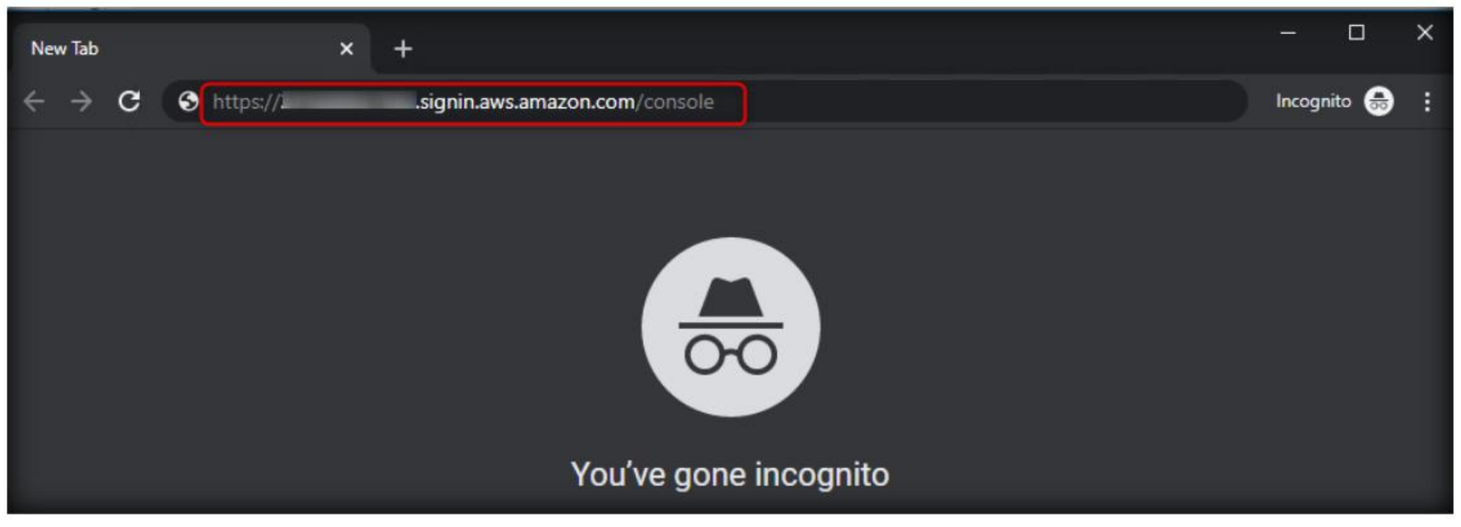


FIGURE 2.1.36: Accessing IAM Users Sign-in Link

Certified Cloud Security Engineer Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

39. A new sign-in page appears. Type the **IAM user name** and **Password** created in the previous step (**IAM username**: **Alice** and **Password**: **user@123**).

    Note: If a new page appears to change the password, type the **Old password**. Next, type a **New password** followed by **Retype new password**. Click **Confirm password change**.

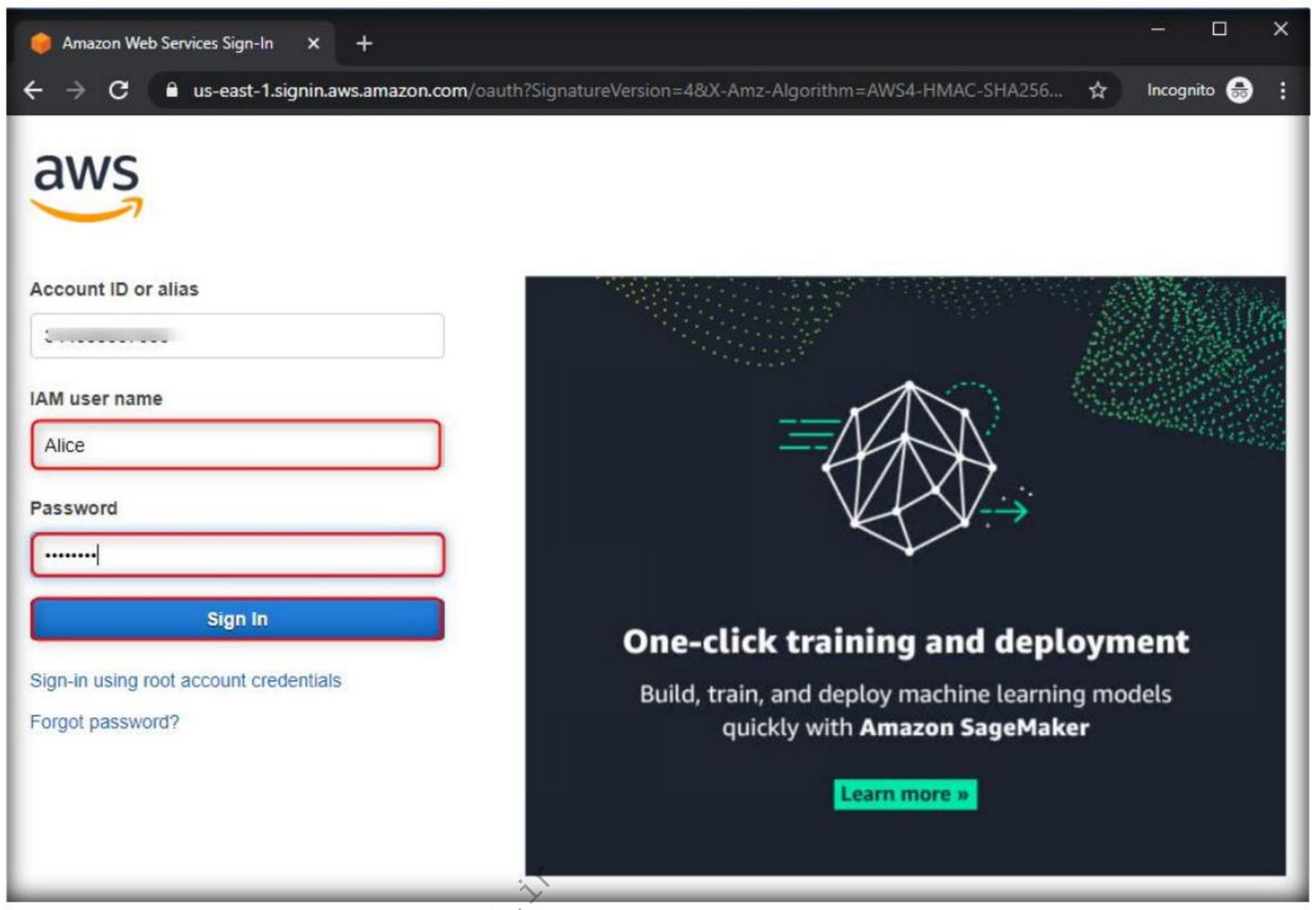


FIGURE 2.1.37: Sign-in of IAM User

40. **Alice** is now logged in as an IAM user and granted read permission only. Therefore, she has a limited access to the resources.

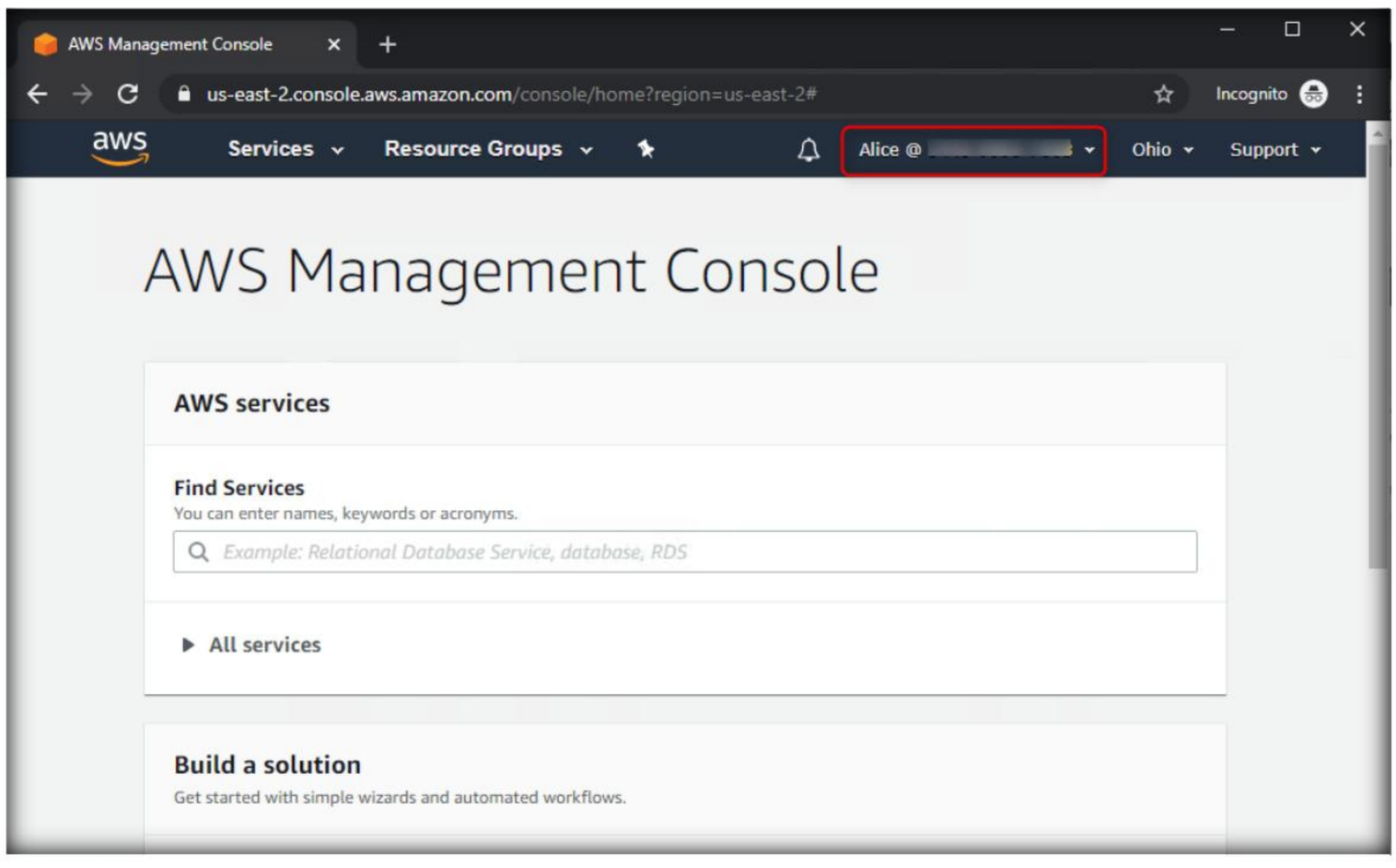


FIGURE 2.1.38: Signing in as IAM User

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

41. Click on Alice ID on the top to open a dropdown menu. You can see the IAM user has been added.

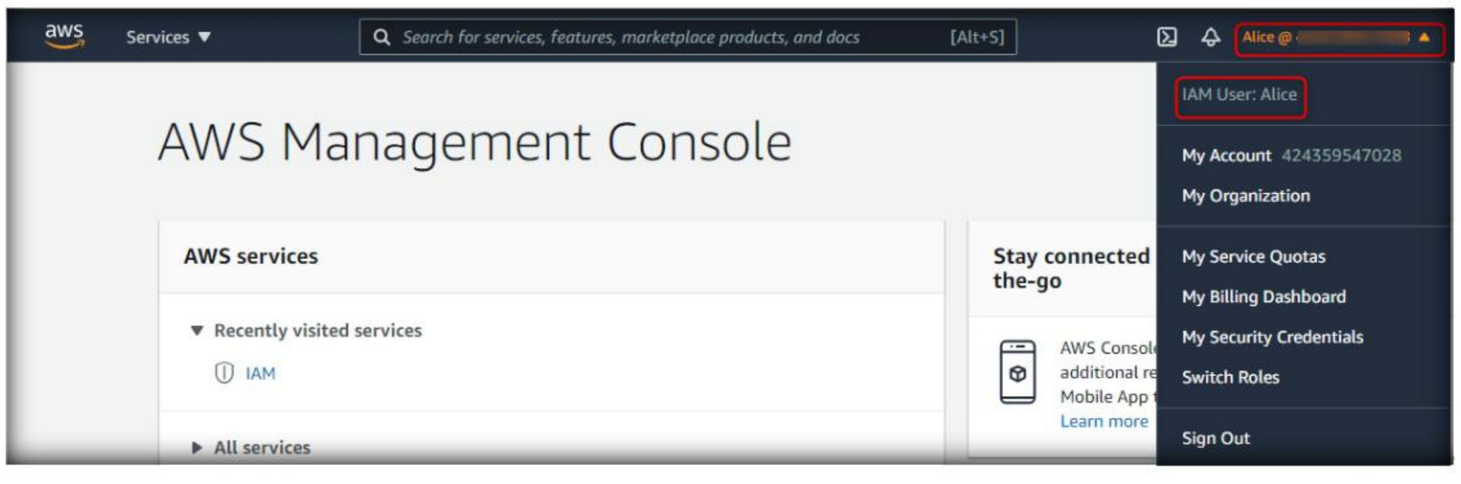


FIGURE 2.1.39: IAM User

42. Next, we will try to access the IAM service. Type **IAM** in the **AWS services** field, as shown in the screenshot below, and then select **IAM**.

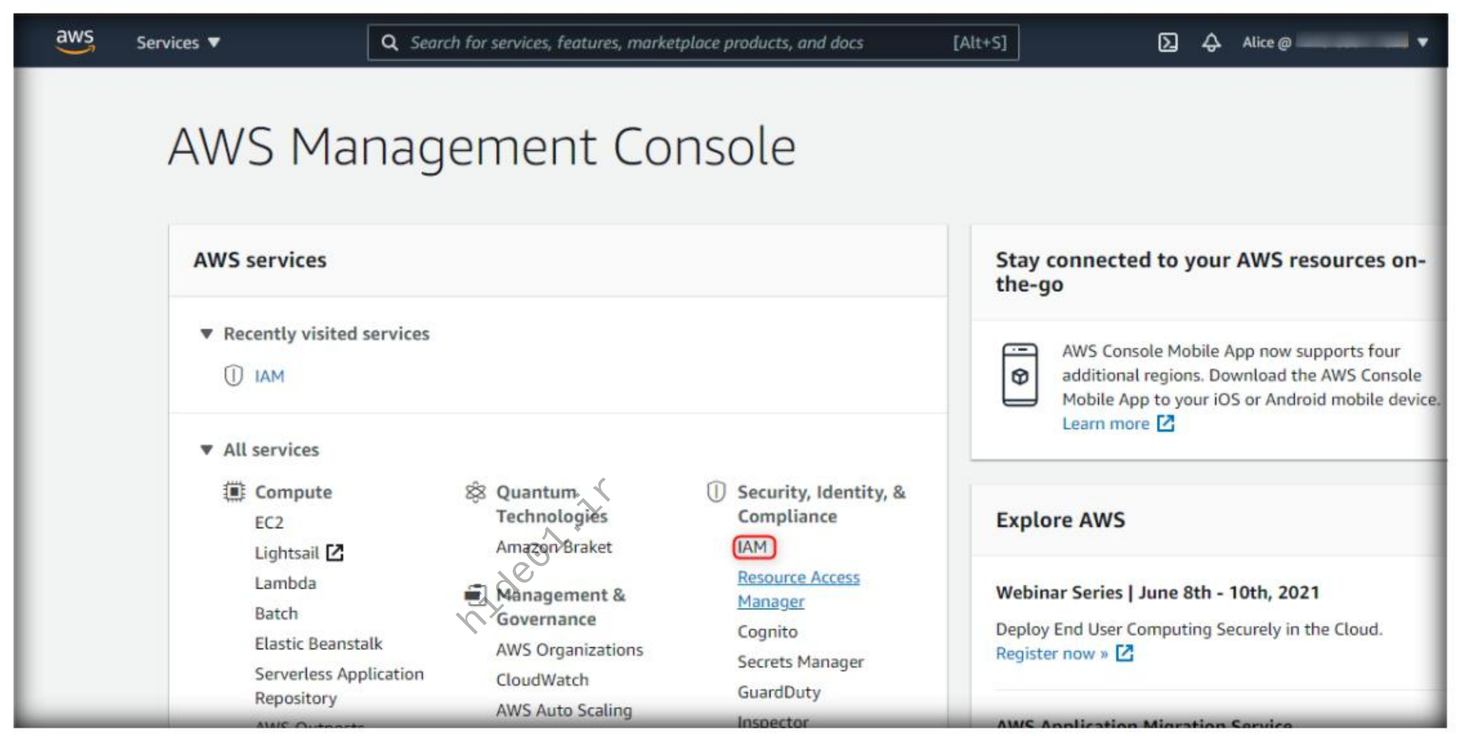


FIGURE 2.1.40: Selecting AWS Service

43. Errors will appear, as shown in the screenshot below. The IAM user **Alice** does not have the permission to access IAM services.

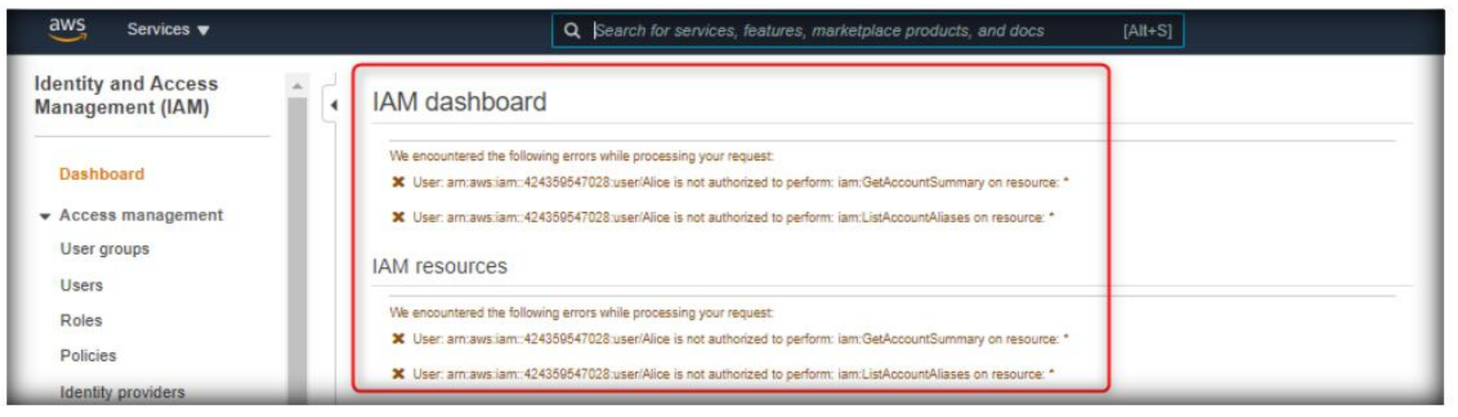


FIGURE 2.1.41: View AWS Permission for IAM User

44. By following the above steps, a network defender can create IAM groups, users, and custom policies in AWS.

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

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

45. To delete the User group and the user created above, first, delete the policy. To delete the policy, navigate to the IAM console and click on **Policies**. Select the checkbox next to the policy (UserAccessCustomPolicy) and click on the **Actions** dropdown. Click on **Delete**. Confirm that you want to delete the policy, and then choose **Delete**.

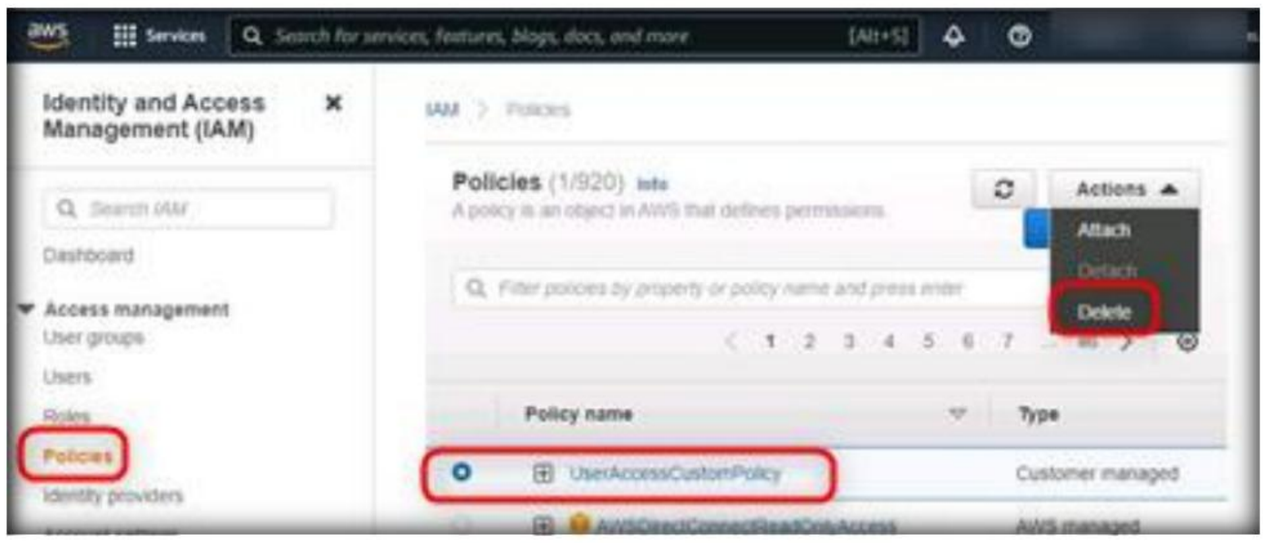


FIGURE 2.1.42: Deleting Policy attached to the User

46. To delete the user, navigate to the IAM console, select **Users** tab and select the checkbox next to the user (**Alice**). Click on **Delete** button. Enter the name of the user to confirm that you want to delete the user and click on **Delete**.

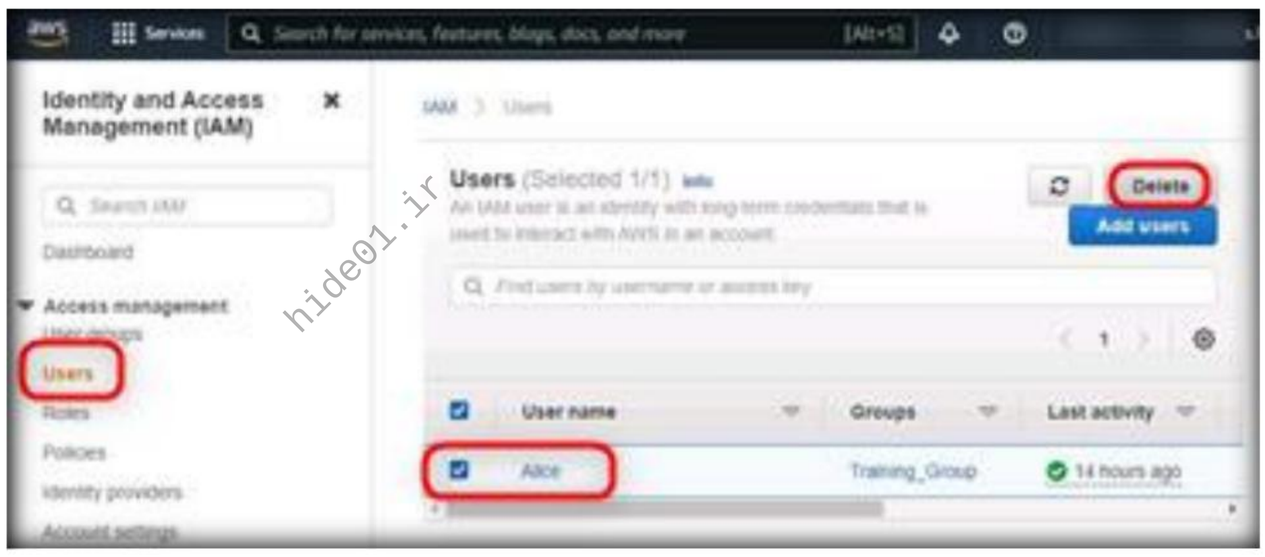


FIGURE 2.1.43: Deleting User

47. To delete the User group, navigate to the IAM console, select **User groups** tab and select the checkbox next to the created user group (**Training_group**). Click on **Delete** button. Enter the name of the user group to confirm that you want to delete the user group and click on Delete.

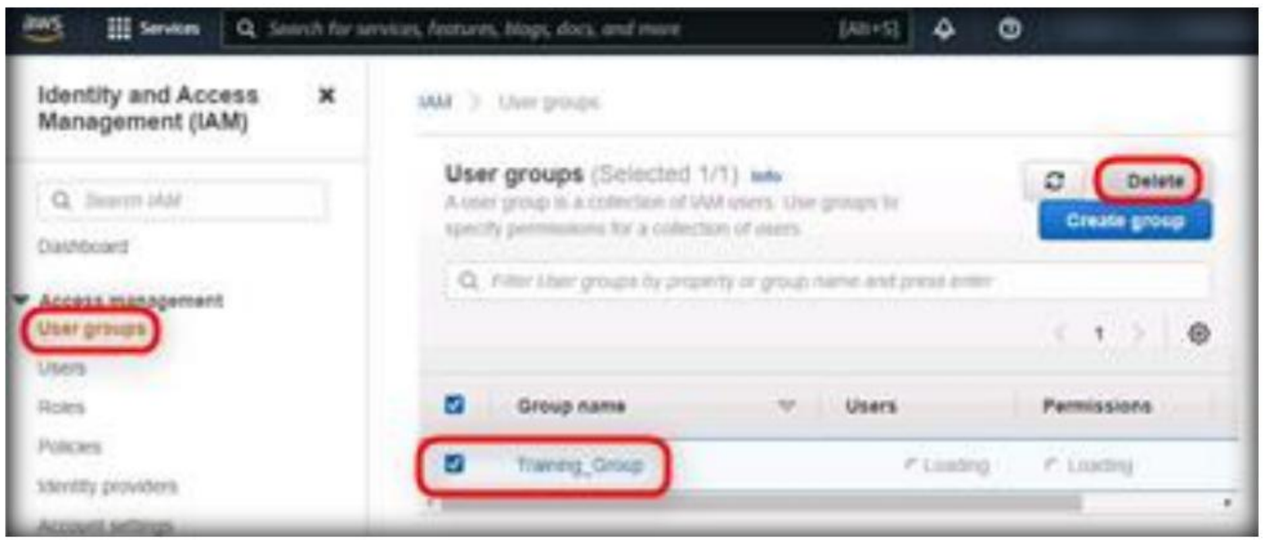


FIGURE 2.1.44: Deleting User group

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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.

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 2

Implementing AWS Key Management Services

Key management involves generating, using, protecting, storing, backing up, and deleting encryption keys.

Lab Scenario

Cloud security engineers follow different data security methods to protect the data on the cloud. Generally, data is encrypted to protect its confidentiality and integrity. Securing the encryption keys from any unauthorized access is a major concern for cloud security engineers. AWS key management service (KMS) enables the secure storage and rotation of encryption keys with strict access control. It is important for a cloud security engineer to understand AWS KMS, learn how to create and manage cryptographic keys, and implement them in AWS services and applications.

Lab Objectives

This lab will demonstrate the implementation of AWS KMS.

In this lab, you will learn to do the following:

- Create KMS master key
- Encrypt AWS S3 using AWS KMS master key
- Encrypt EBS volume using AWS KMS master key
- Encrypt Amazon Redshift Using KMS master key

ICON KEY

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

Lab Environment

To perform this lab, you need the following:

- **Admin Machine** VM
- **Administrative** privileges to run the tools
- **Registered AWS account**

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Duration

Time: 20 minutes

Overview of Key Management

Key management involves generating, using, protecting, storing, backing up, and deleting encryption keys. Cloud key management is linked with identity and access management (IAM) and Cloud Audit Logs for controlling and monitoring access to individual keys and their use.

Lab Tasks

Note: Web applications in a cloud environment may undergo frequent updates. As we will work in a cloud environment for this lab (i.e., AWS), the application interface may be updated with time. Hence, in case you happen to work on an updated version of AWS, 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 an AWS Free Tier account using the following link: aws.amazon.com/free, in case you have already not created for the previous lab. Once the registration is complete, perform the following tasks:

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

TASK 1

Creating IAM User in AWS

1. Log in to the **Admin Machine** VM with the user **Admin** and password **admin@123**.

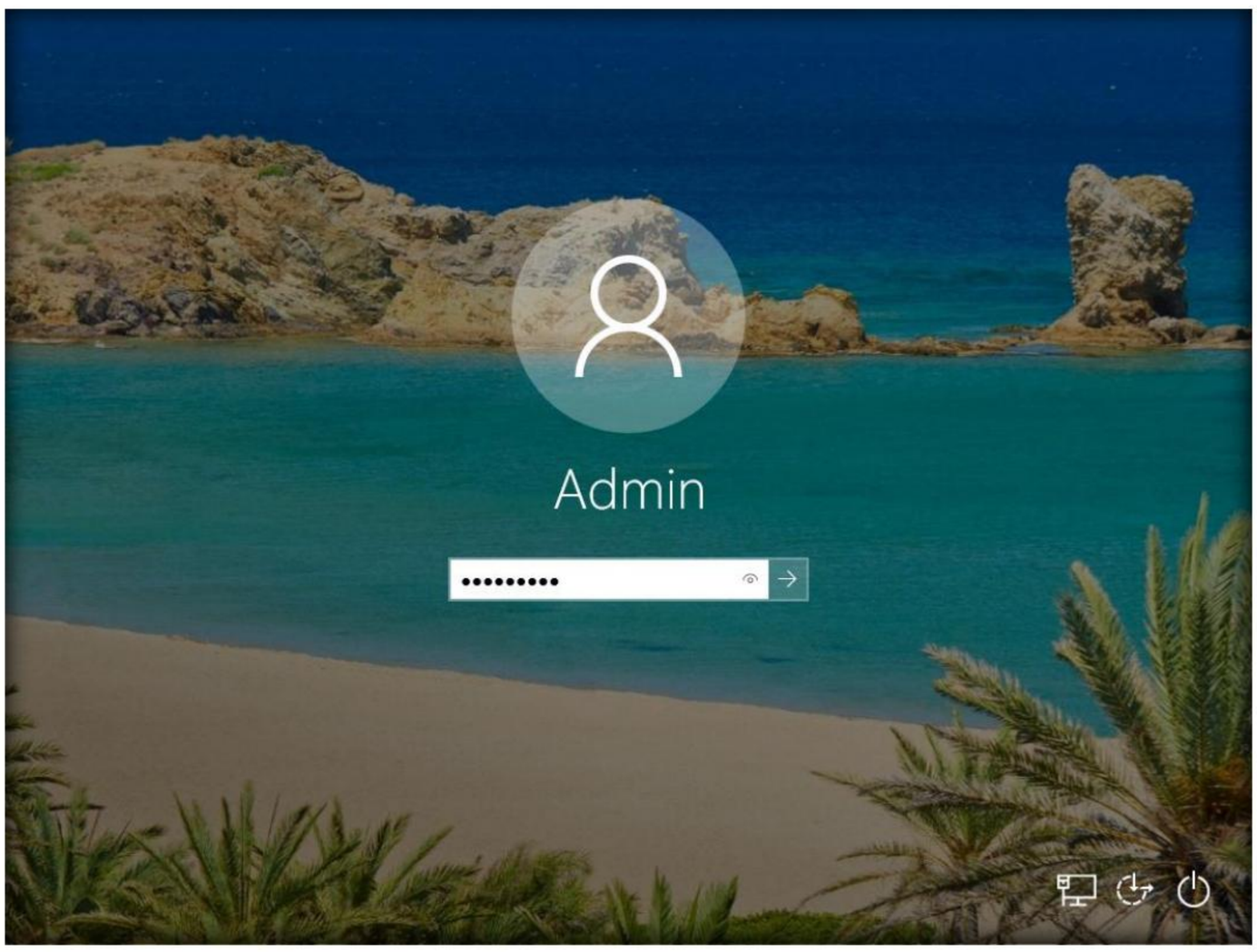


FIGURE 2.2.1: User Login

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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



FIGURE 2.2.2: Navigating to the Chrome Browser from Taskbar

4. In the address bar of the **Google Chrome** browser, type **https://aws.amazon.com/** and press **Enter.**

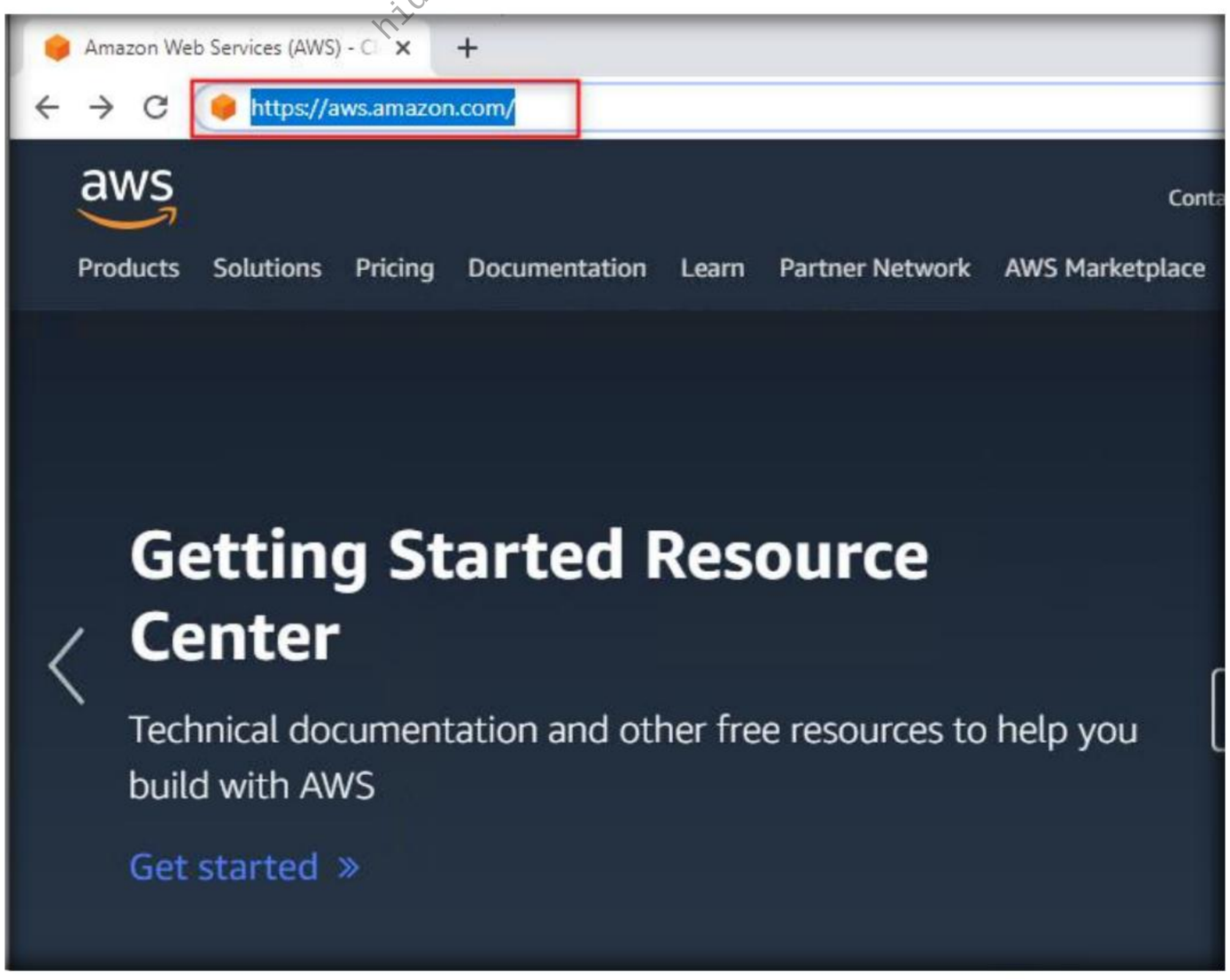


FIGURE 2.2.3: Access AWS in Browser

Note: If you are already logged in, skip the login steps.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

5. The **AWS Web Services - Cloud Computing Services** page appears. Click on the **AWS Management Console** from the **My Account** dropdown, as shown in the screenshot below.

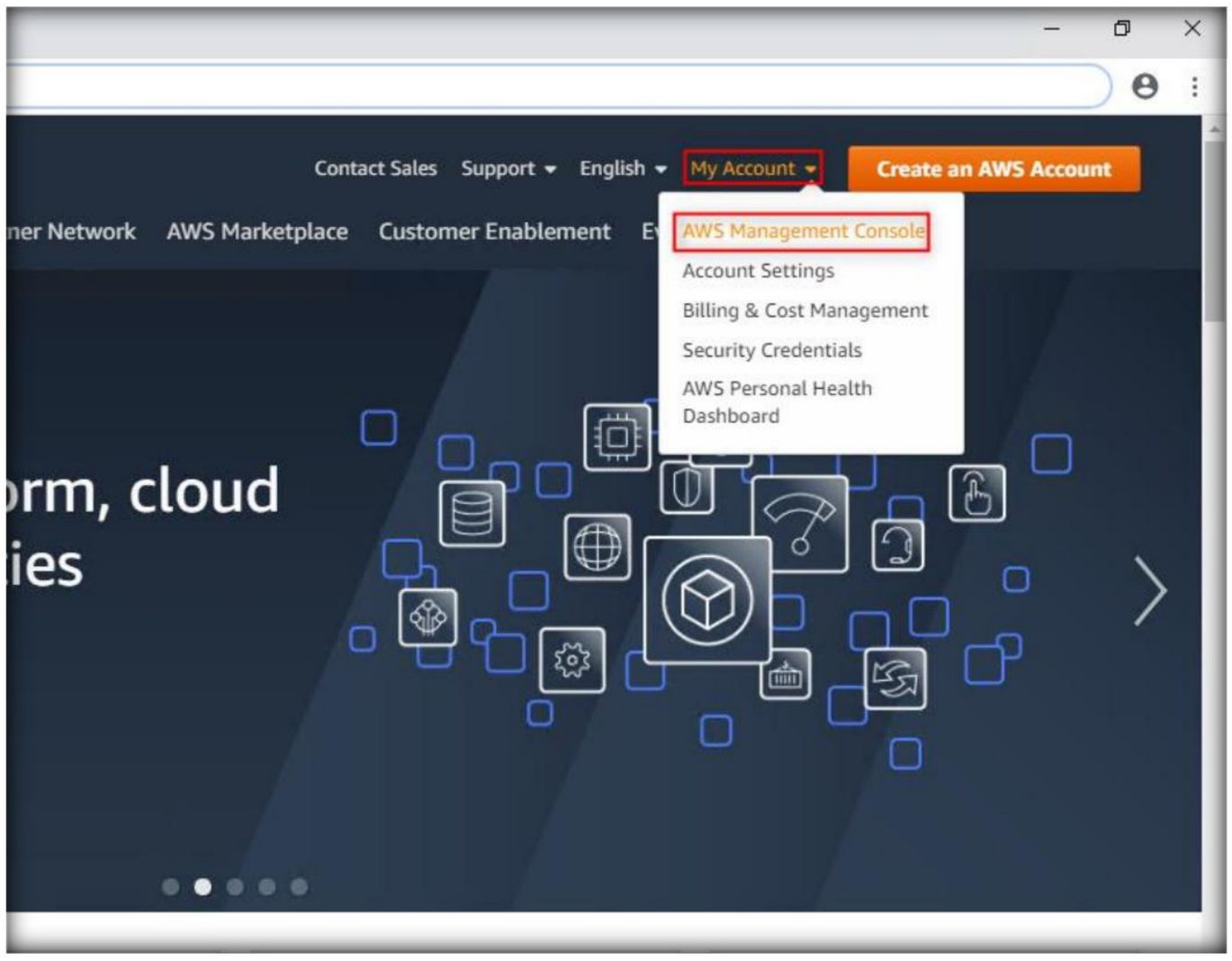


FIGURE 2.2.4: Navigate to AWS Management Console

6. The **AWS Sign-in** page appears. Choose **Root user** and type the AWS administrator account ID (**Root user** email address), as shown in the screenshot below, and then click on **Next**.

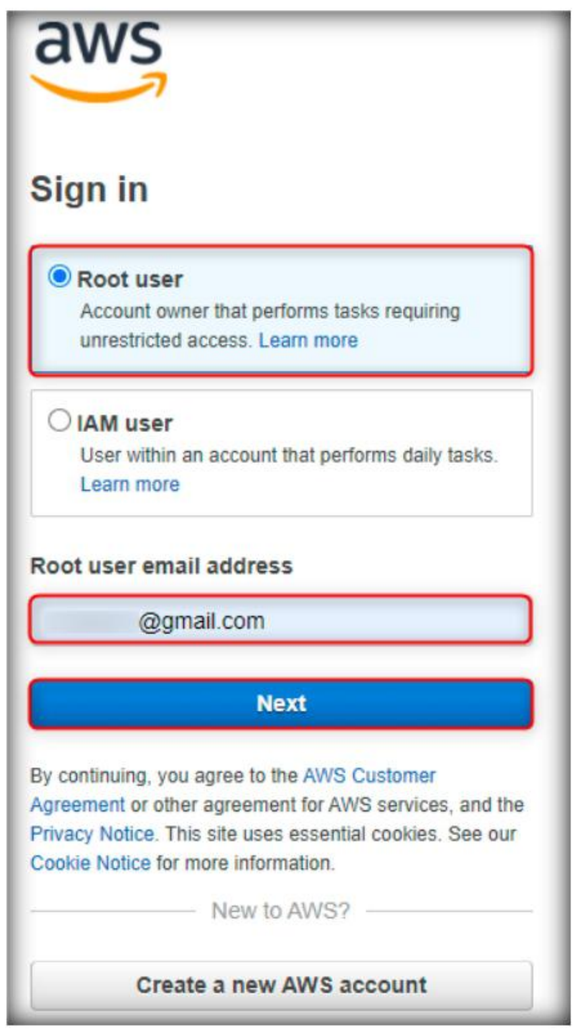


FIGURE 2.2.5: Login Credentials

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

7. The security check page appears. Type the characters shown in the image and click **Submit**.

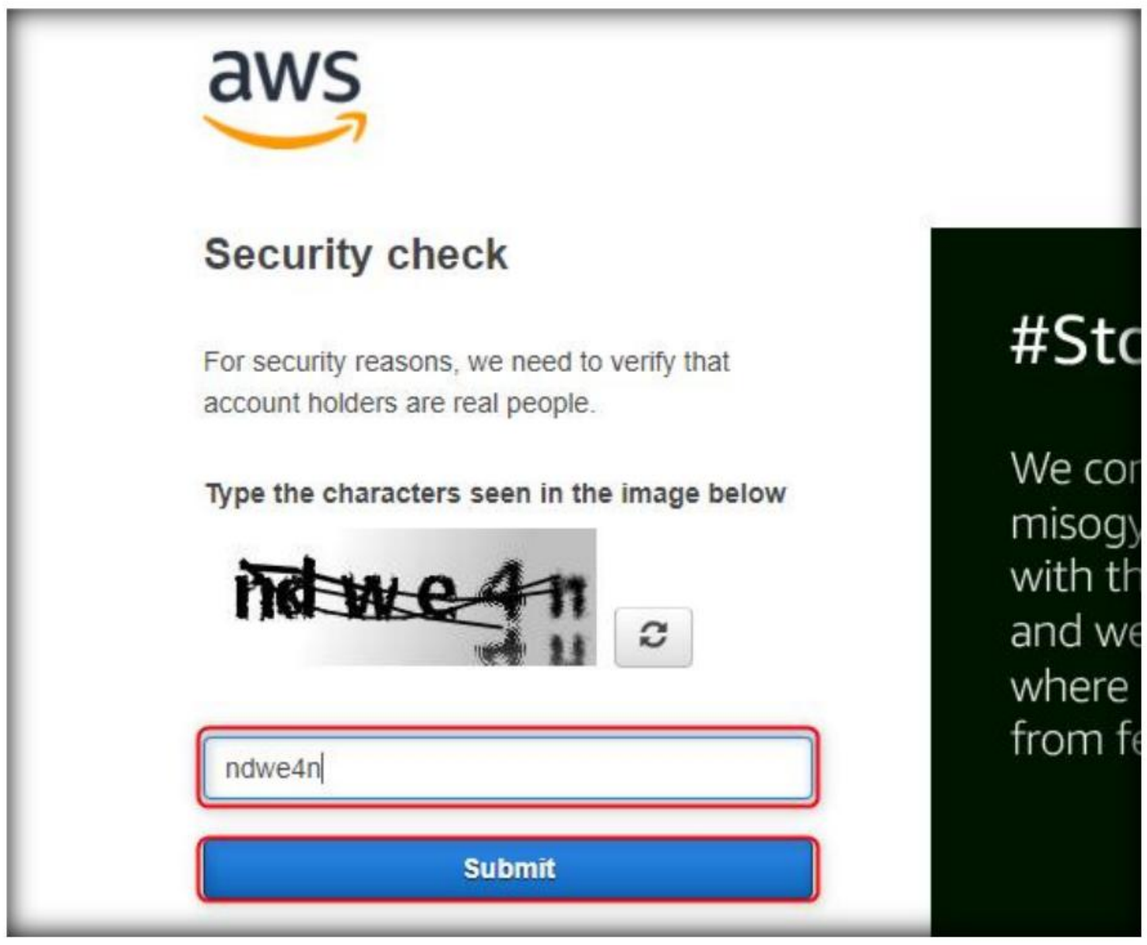


FIGURE 2.2.6: Typing Characters

8. In the **Password** field, type the password and click on **Sign in**, as shown in the screenshot below.

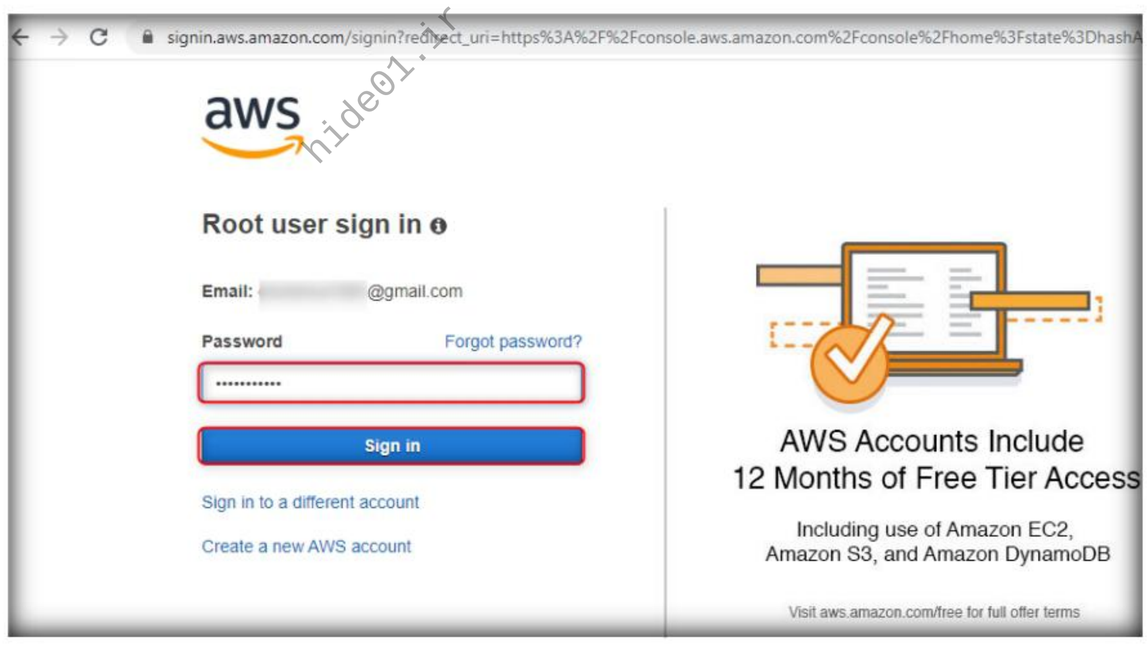


FIGURE 2.2.7: Sign into AWS

9. Select **Users** from the **Identity and Access Management (IAM)** section and click on **Add user**, as shown in the screenshot below, to create a new user.

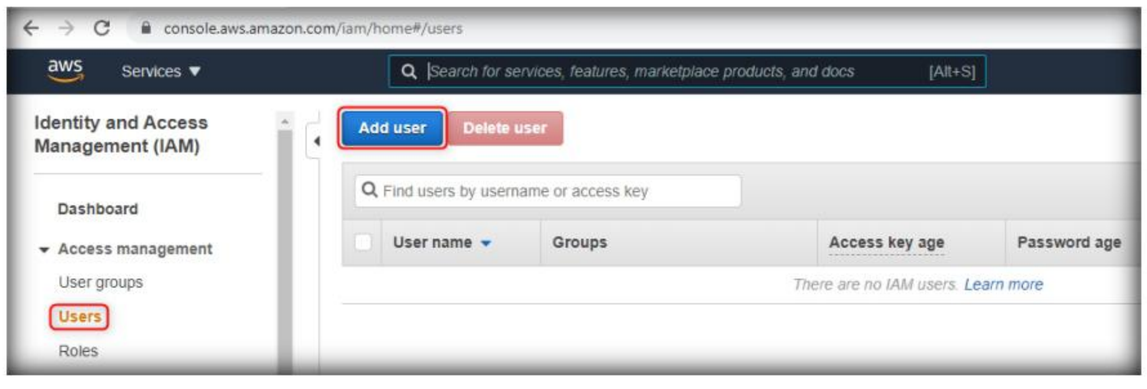


FIGURE 2.2.8: Adding New User

Certified Cloud Security Engineer Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

10. The **Add user** page appears. In the **User name** field, provide any name (e.g., **Alice**). Select **AWS Management Console access and Programmatic access** under **Access type** in the **Select AWS access type** section. Choose the **Custom password** radio button and type the password (**user@123**) in the password field, as shown in the screenshot below. **Require password reset** is optional; however, check this setting. Then, click on **Next: Permissions**.

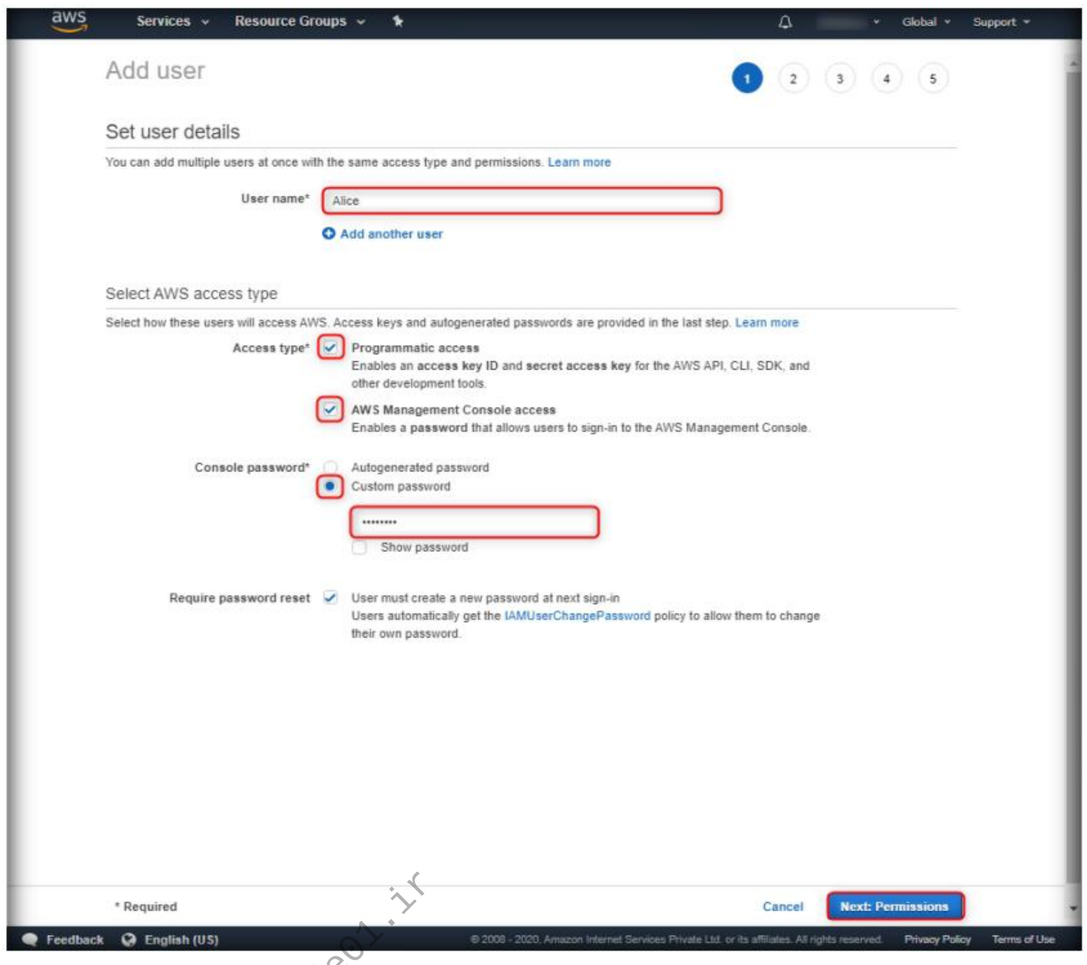


FIGURE 2.2.9: New User Details

11. In the **Set permissions** section, **Add user to group** is selected by default. Check the newly created group (**Training_Group)**, as shown in the screenshot below. You have now added the user to the group. Click on **Next: Tags**.

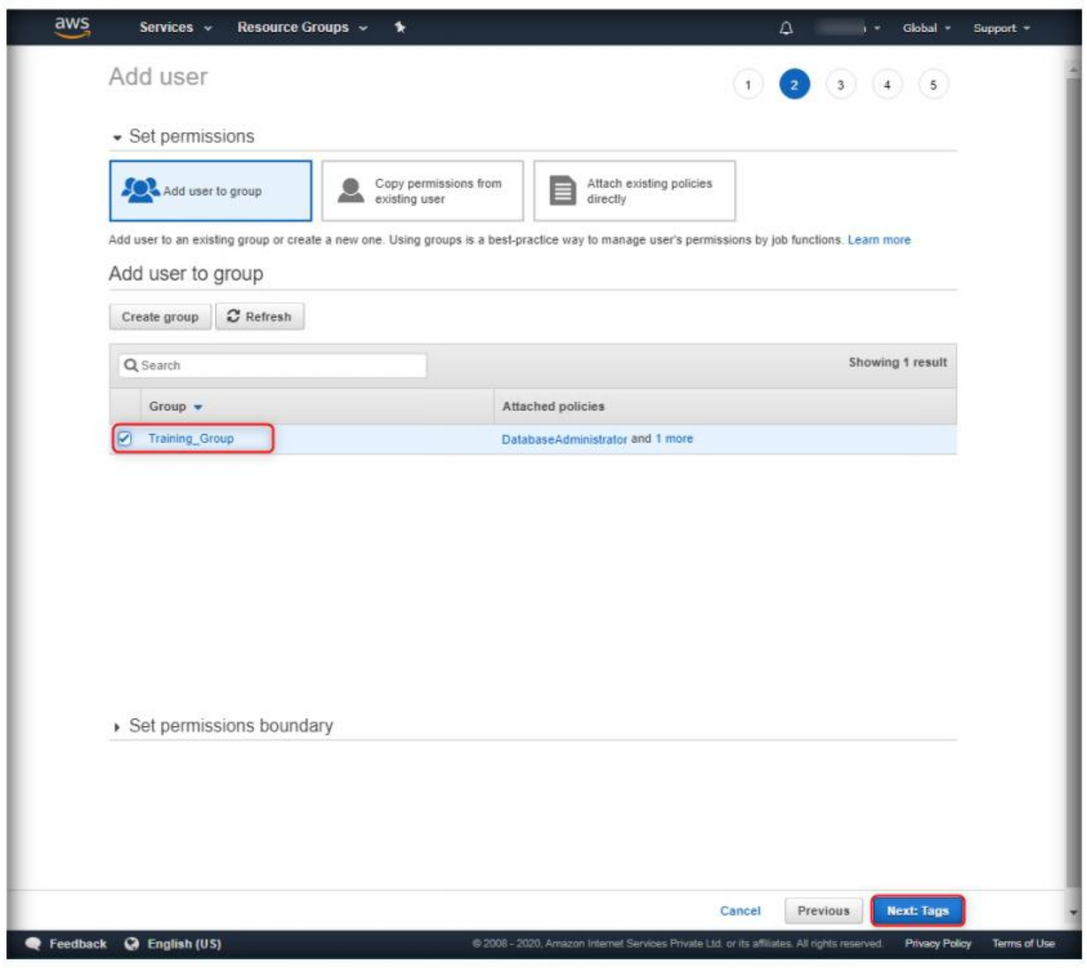


FIGURE 2.2.10: Adding User to Group

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

12. Tags are optional; however, tagging will help us later in searching for tag keys. Type **Department** in the field under **Key** and **Training** under **Value (optional)**. Then, click on **Next: Review** to start reviewing IAM user creation.

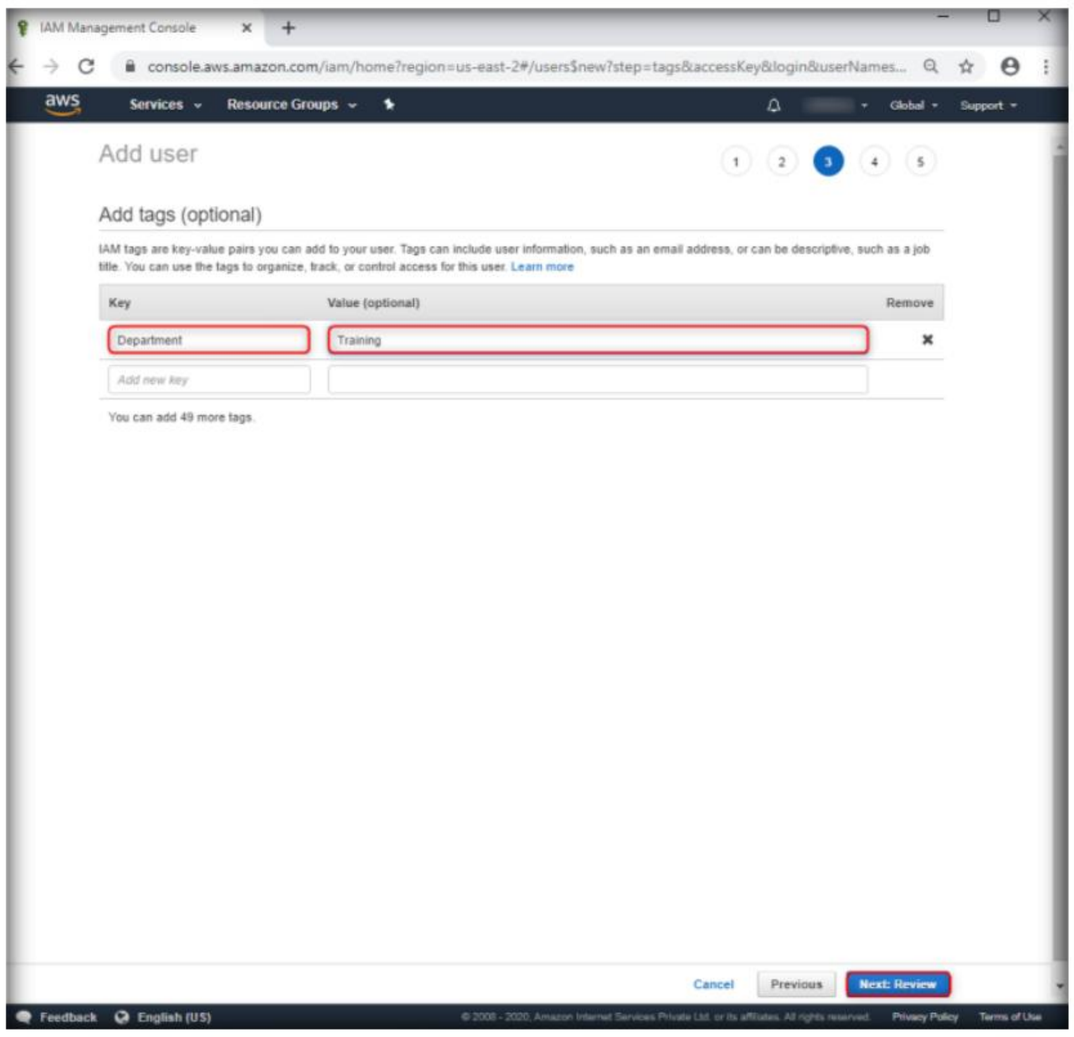


FIGURE 2.2.11: Adding Tag for User

13. On the **Review** page, you can review the settings and IAM user properties before creating the user. Once you have verified the settings, click on **Create user**.

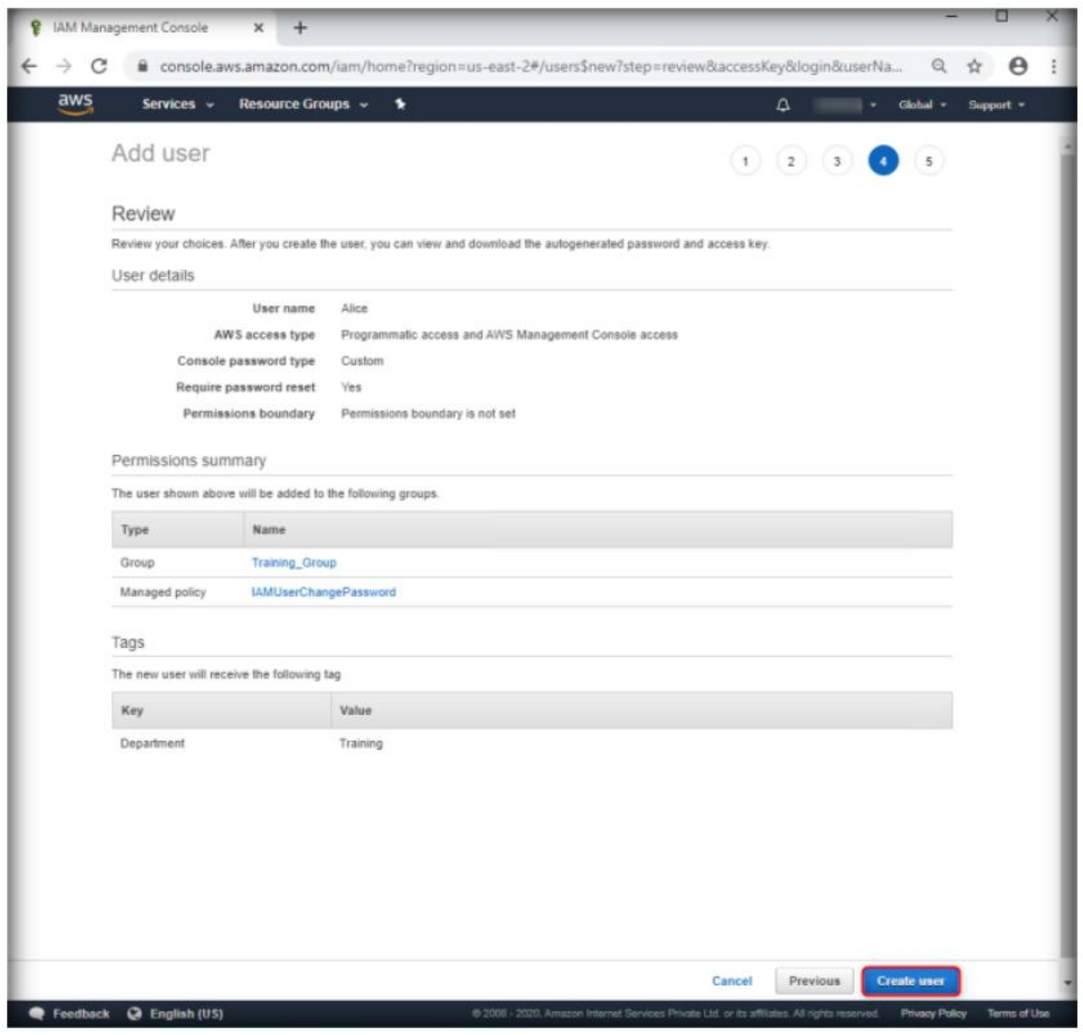


FIGURE 2.2.12: Review New User Details

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

14. After you click on **Create user**, a **Success** message is displayed, as shown in the screenshot below. You have an option to **Send email** to get the login instructions for the newly created IAM user. Click on **Close** (lower right corner of the page) to return to the IAM page. It will redirect you to the **Users** page.

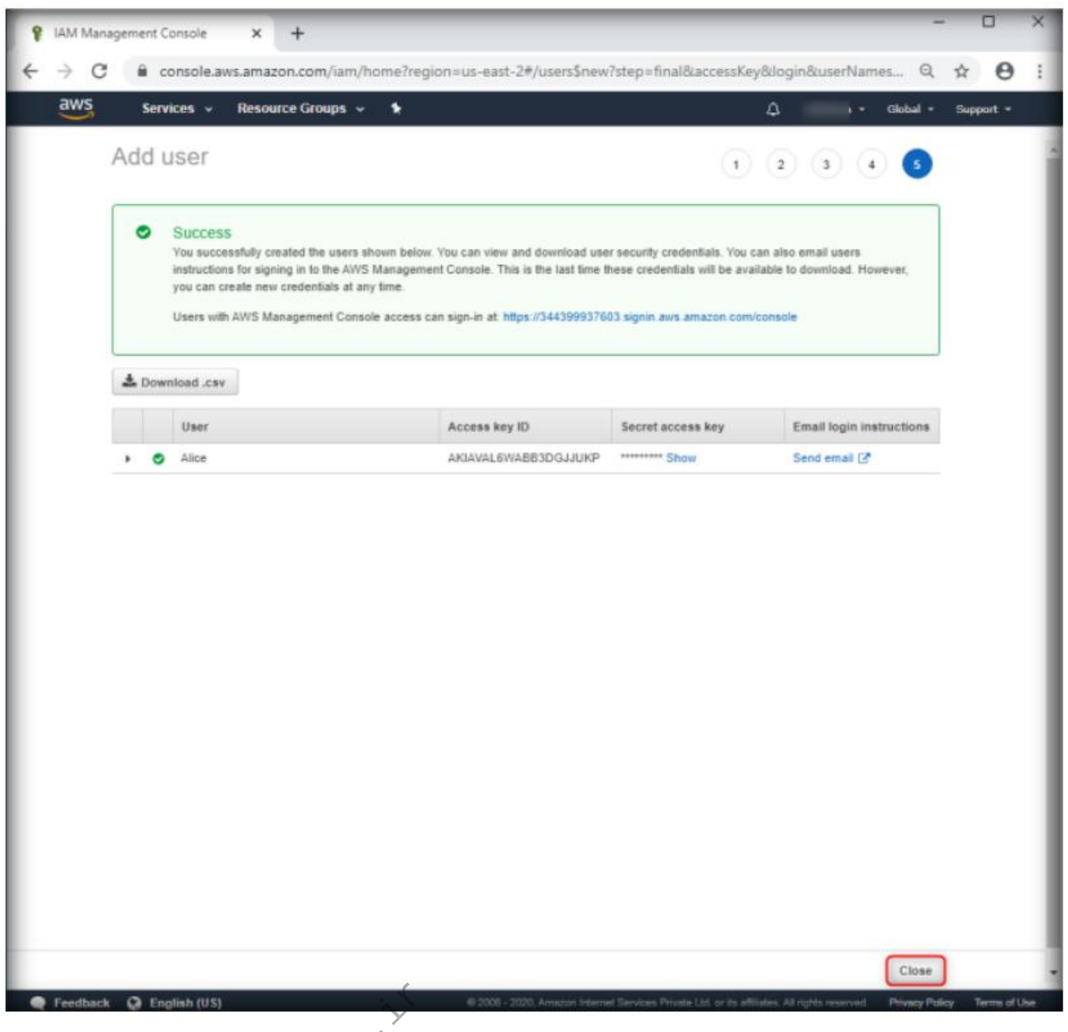


FIGURE 2.2.13: New User Added Successfully

TASK 2

Creating KMS Master Key

15. Click on **Services**. In the **Search** field, type **KMS** and then select **Key Management Service** from the search result, as shown in the screenshot below.

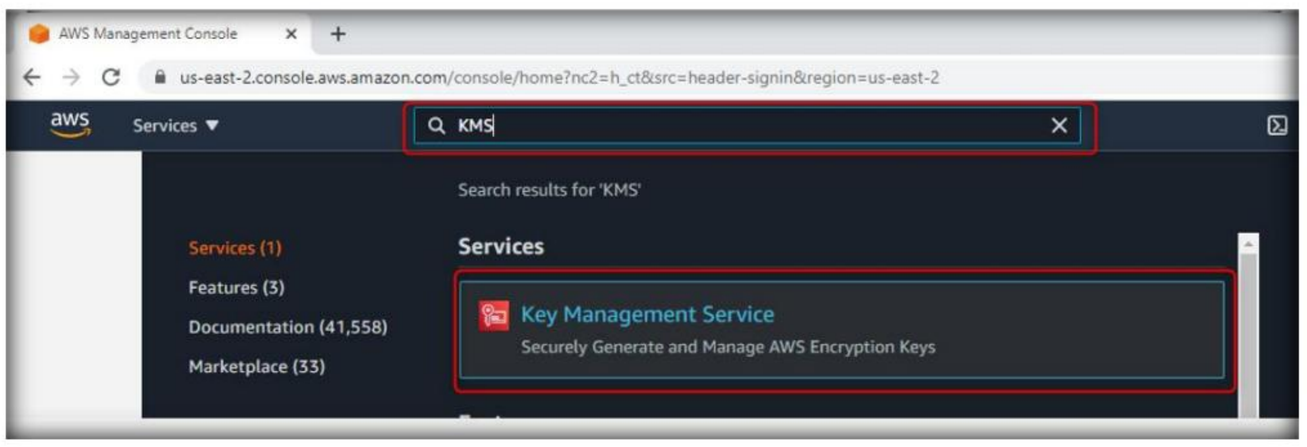


FIGURE 2.2.14: AWS Management Console

16. The **KMS Console** page appears. Click on **Customer managed keys** in the left pane, as shown in the screenshot below.



FIGURE 2.2.15: AWS Key Management Service

Certified Cloud Security Engineer Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

17. The **Customer managed keys** section appears. Click on **Create key**.

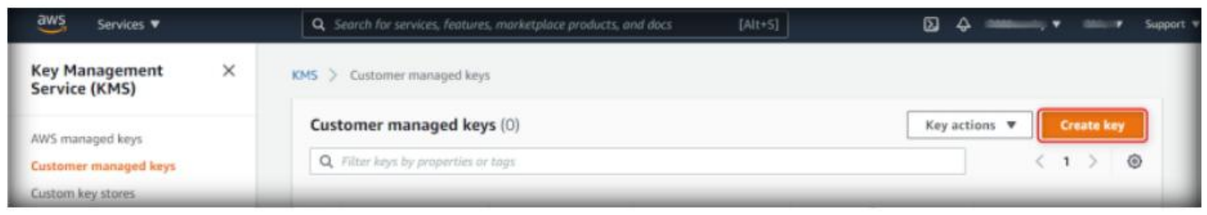


FIGURE 2.2.16: Customer Managed Key

18. Click on the radio button for **Symmetric,** as shown in the screenshot below. Then, click on **Next** to continue.

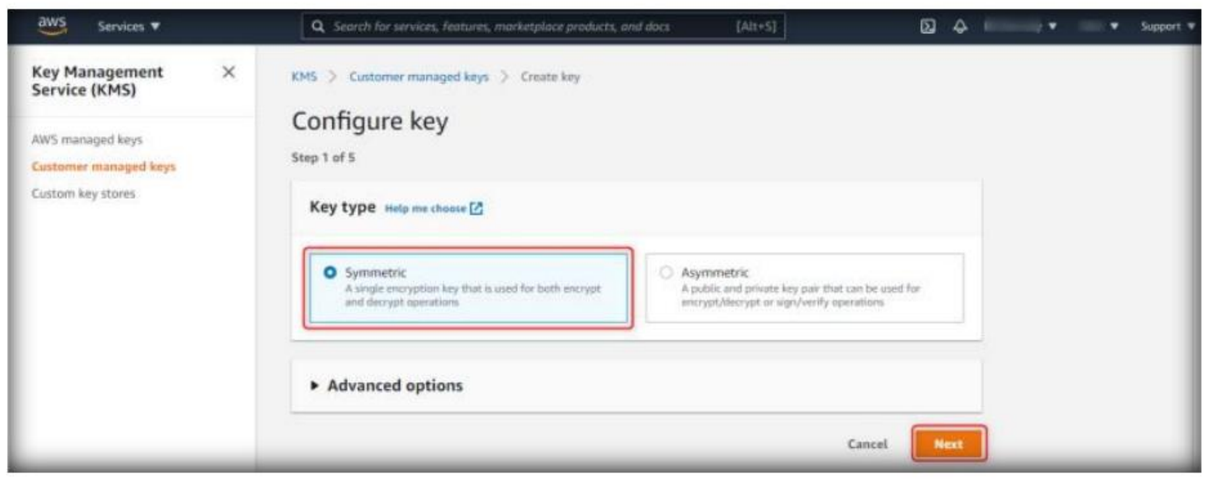


FIGURE 2.2.17: Configure Key

19. Enter an **Alias** of your choice as the name of your master key. Here, we have entered **CCSE_user_MasterKey** in the **Alias** field. The **Description** is optional; however, entering a brief description of what the key does is recommended. Here, we have entered the following **Description: The key is used to protect the files for the Training Group**. Under the **Tags** section, you can add tags to help identify the master key using **Tag key** and **Tag value**, as shown in the screenshot below. Here, we have used **CCSEUserKey** as the **Tag key** and **training** as the **Tag Value.** Click on **Next**.

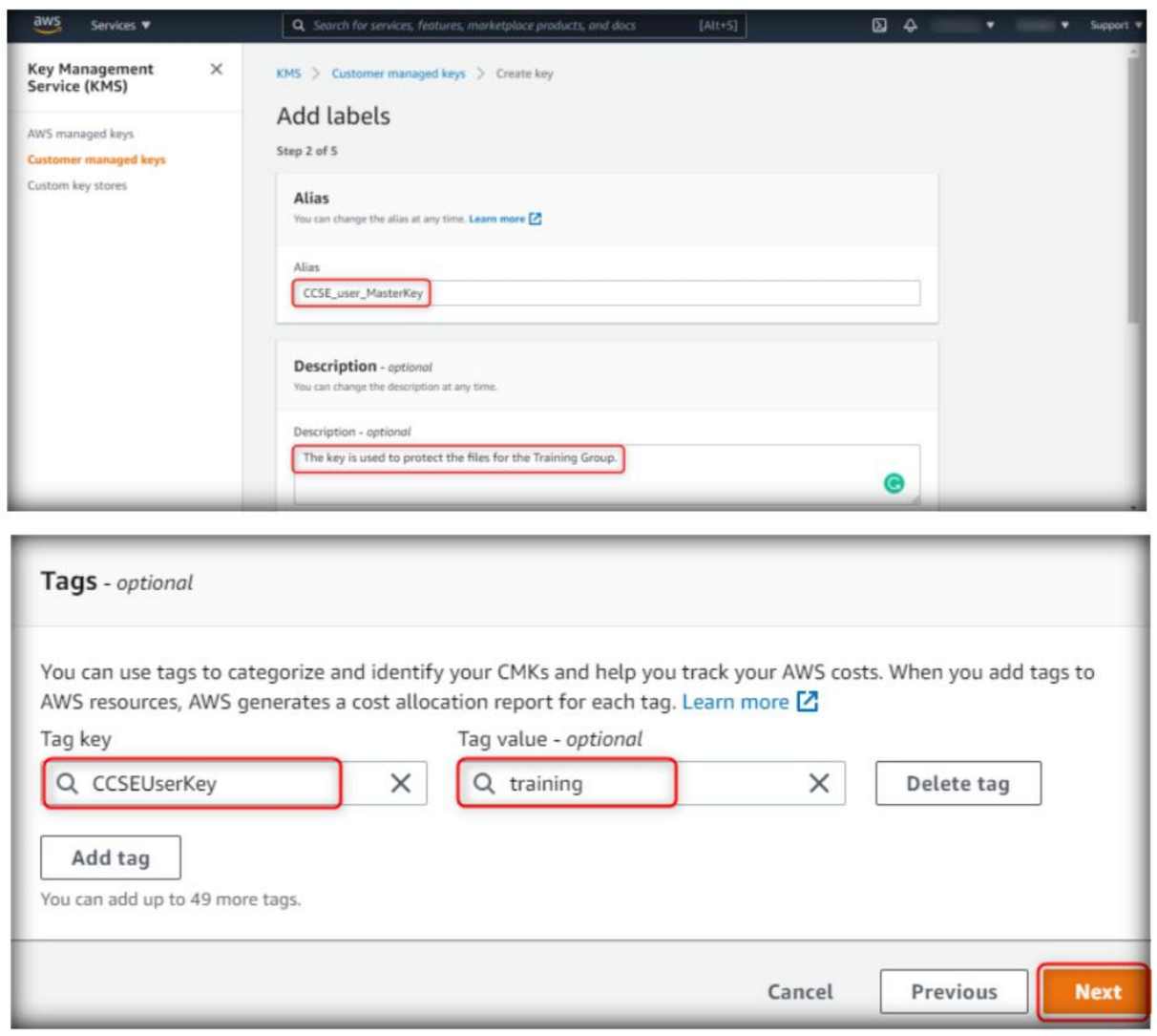


FIGURE 2.2.18: Adding Labels

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

20. To allow users to perform encryption and decryption, you have to assign key permissions to them on the **Define key administrative permissions** page. Permit the user you have created in the previous lab to use the master key by selecting the checkbox near the user. Here, we have selected the user **Alice** we had created in the previous lab. Click on **Next** to continue.

    Note: If a user is not found in this step, create a new user by following **Steps 15–20** in the previous lab.

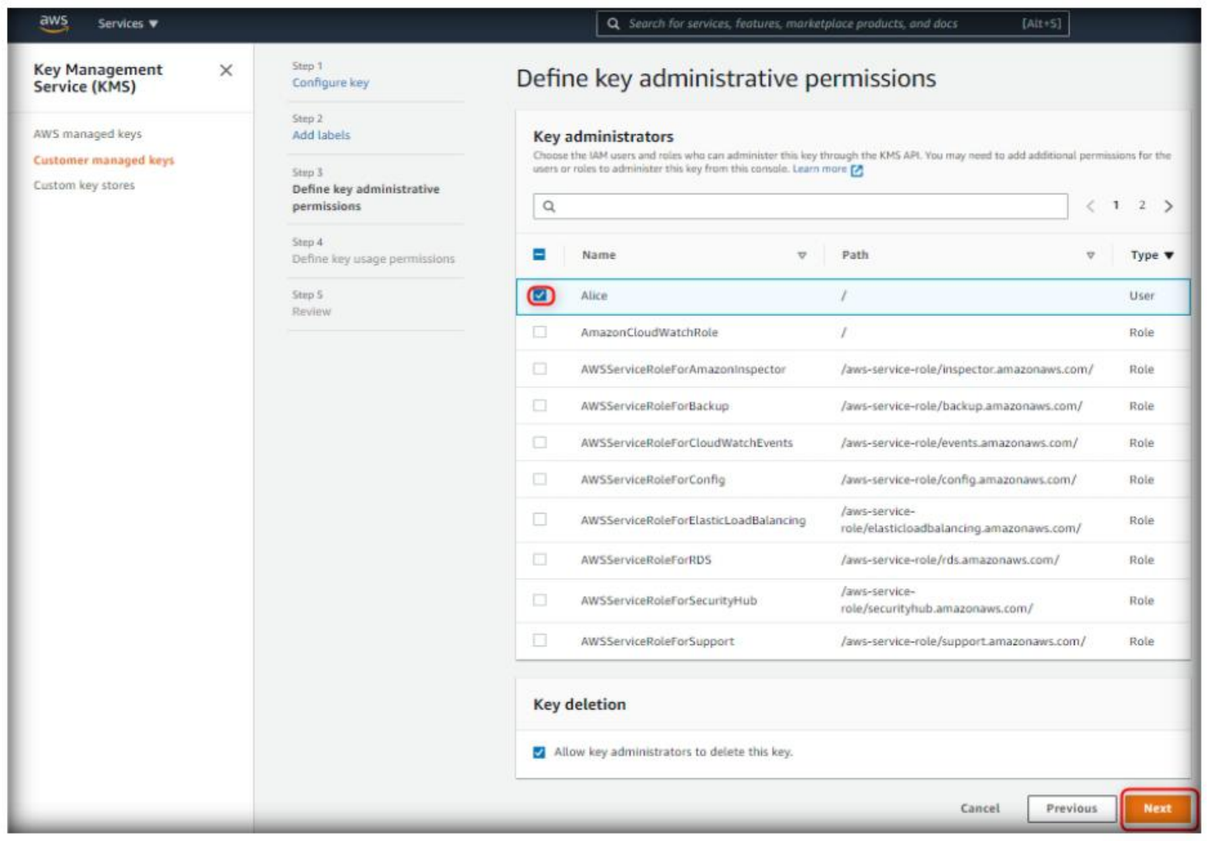


FIGURE 2.2.19: Granting Key Administrative permission

21. On **Define key usage permissions** page, you have the option to add another AWS user account. Here, since you have already added the user, click on **Next** to continue.

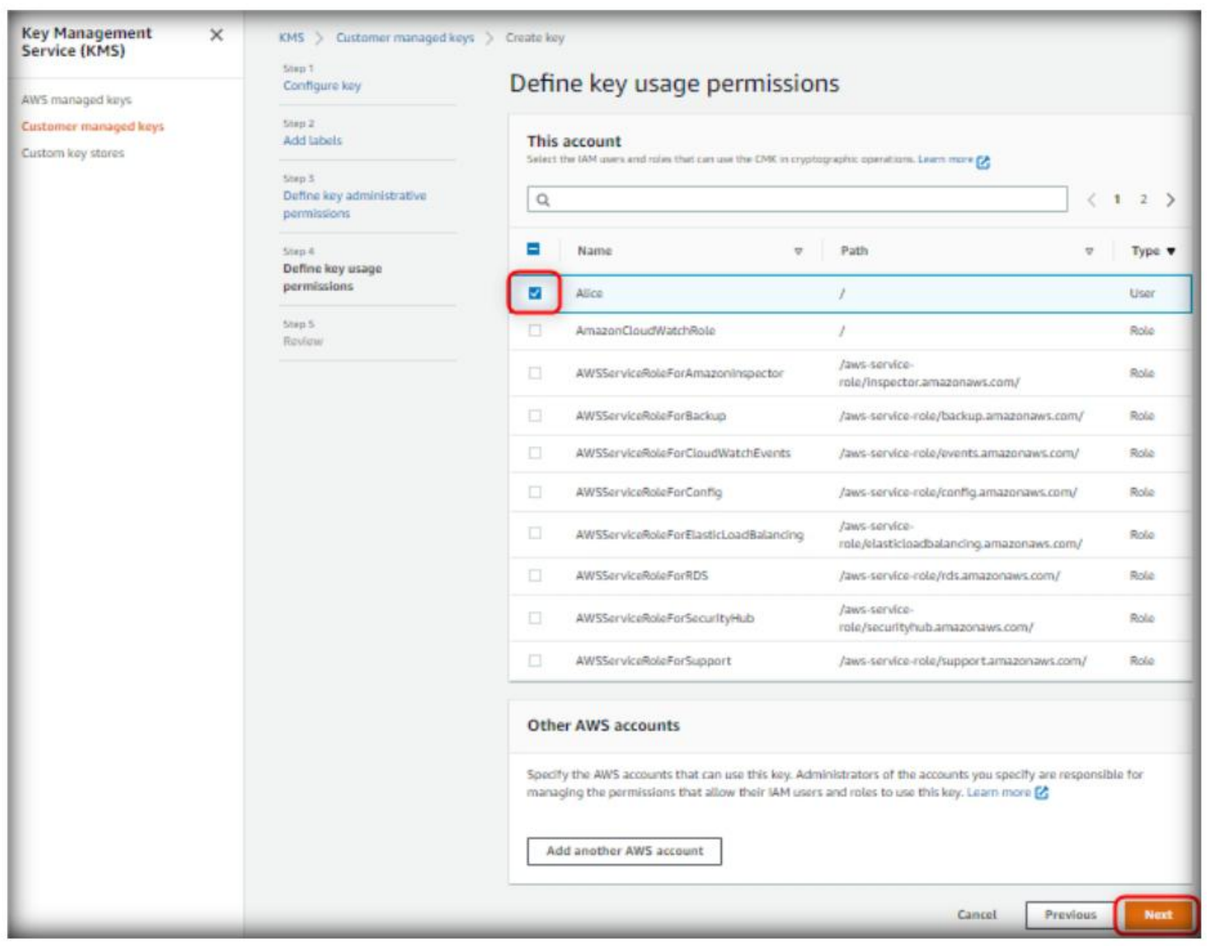


FIGURE 2.2.20: Add User

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

22. On the **Review** page, review the key policy, which is in JSON format, as shown in the screenshot below. Click on **Finish** to create the master key.

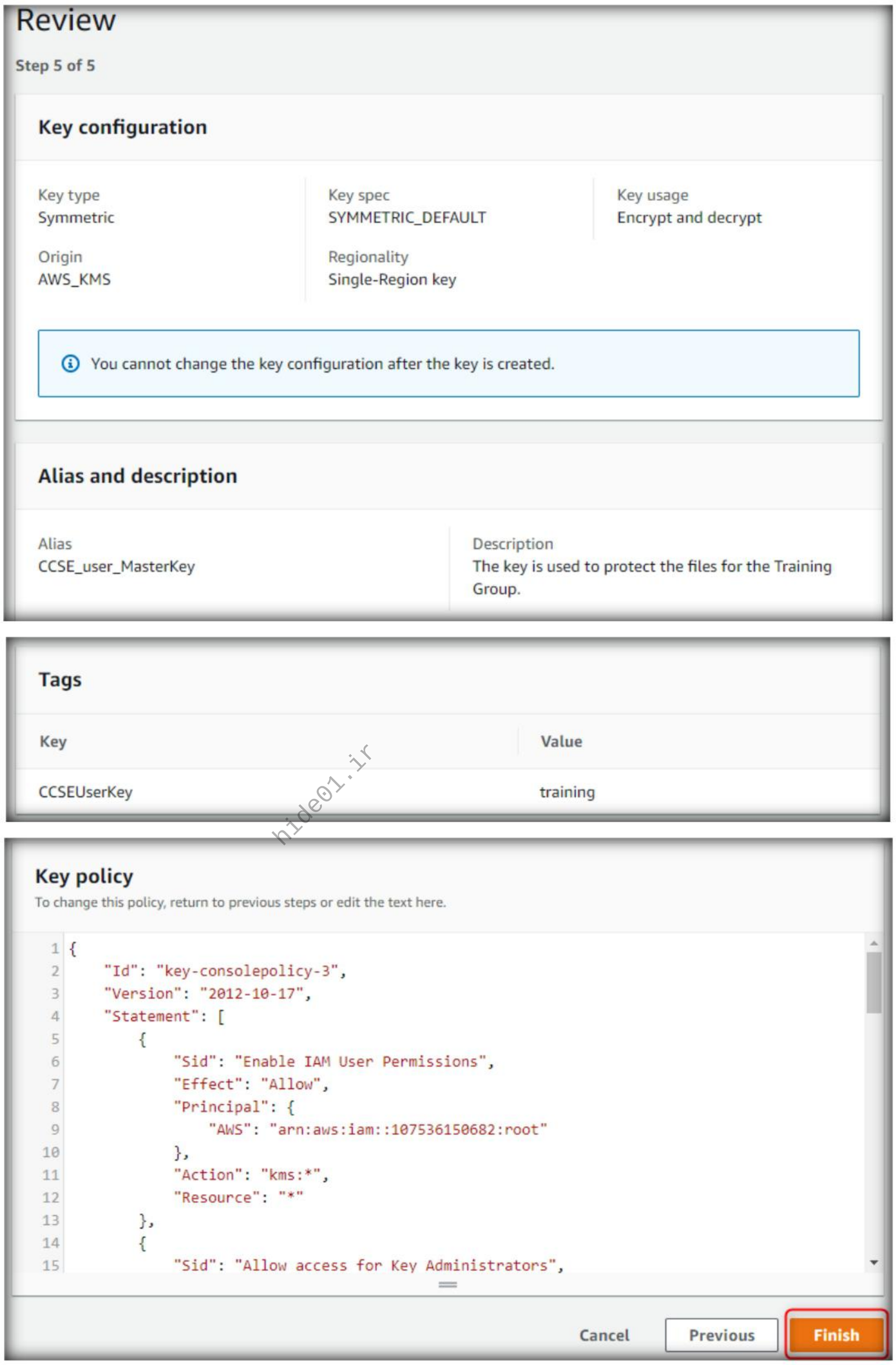


FIGURE 2.2.21: Key Policy

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

23. The key has been created successfully, and it now appears in the **Customer managed keys** section.

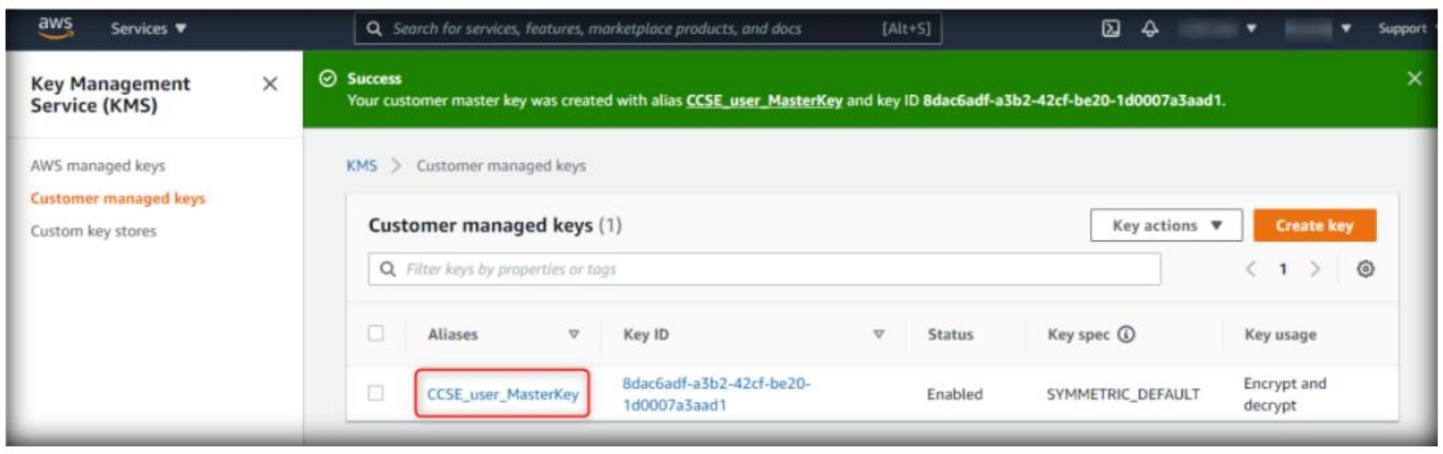


FIGURE 2.2.22: Key Added Successfully

24. After creating the key, go to **Customer managed keys** to view the master key properties.

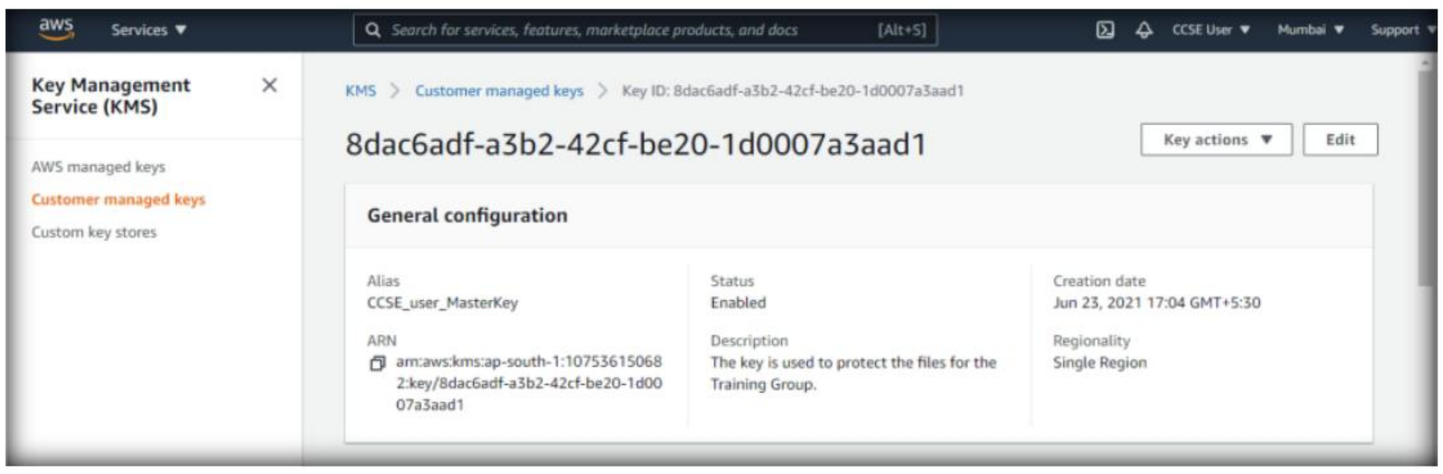


FIGURE 2.2.23: View Key Properties

25. Now, click on **Services** from the menu bar in the **AWS Management Console** and type **S3** in the search field to create a new bucket. Click on **S3 Scalable Storage in the Cloud** from the search results, as shown in the screenshot below.

TASK 2

Implementation of AWS KMS Master Key to Encrypt AWS S3

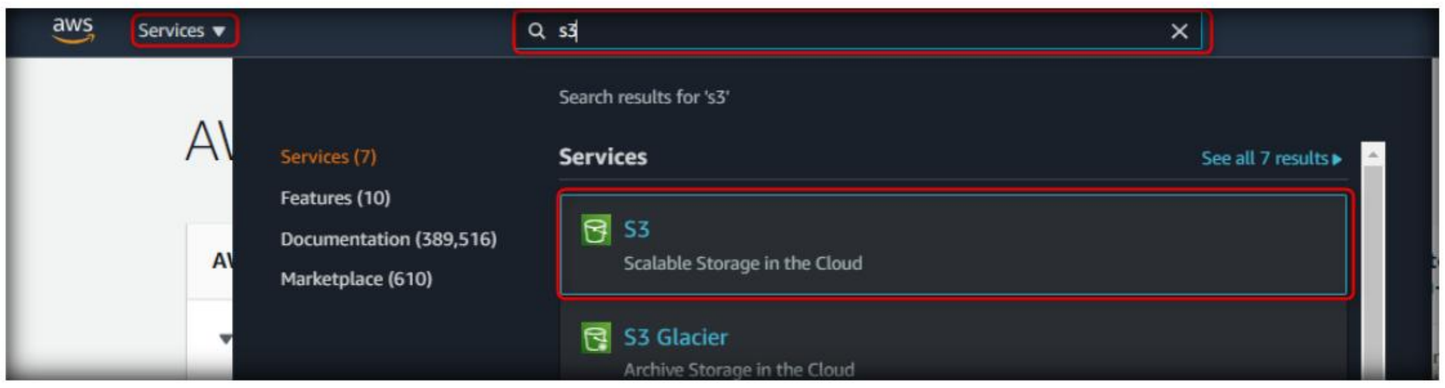


FIGURE 2.2.24: S3 Service

26. The **S3 buckets** page appears. Click on **Create bucket**.

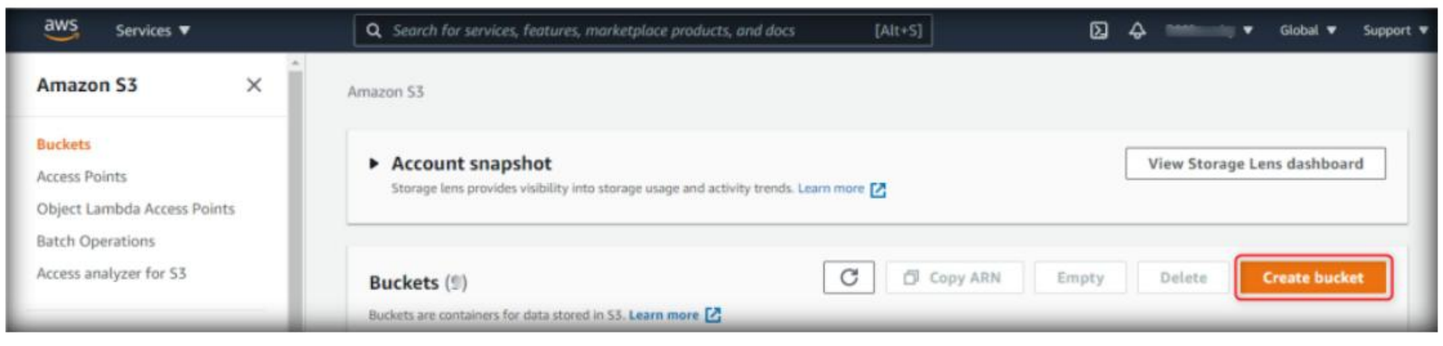


FIGURE 2.2.25: S3 Buckets

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

27. The **Create bucket** popup appears. Under **General configuration**, type the name of the bucket in the **Bucket name** field (here, the bucket name is **training-group001**), and select a region of your choice in the **AWS Region** field (here, we have selected **US East (Ohio) us-east-2**).

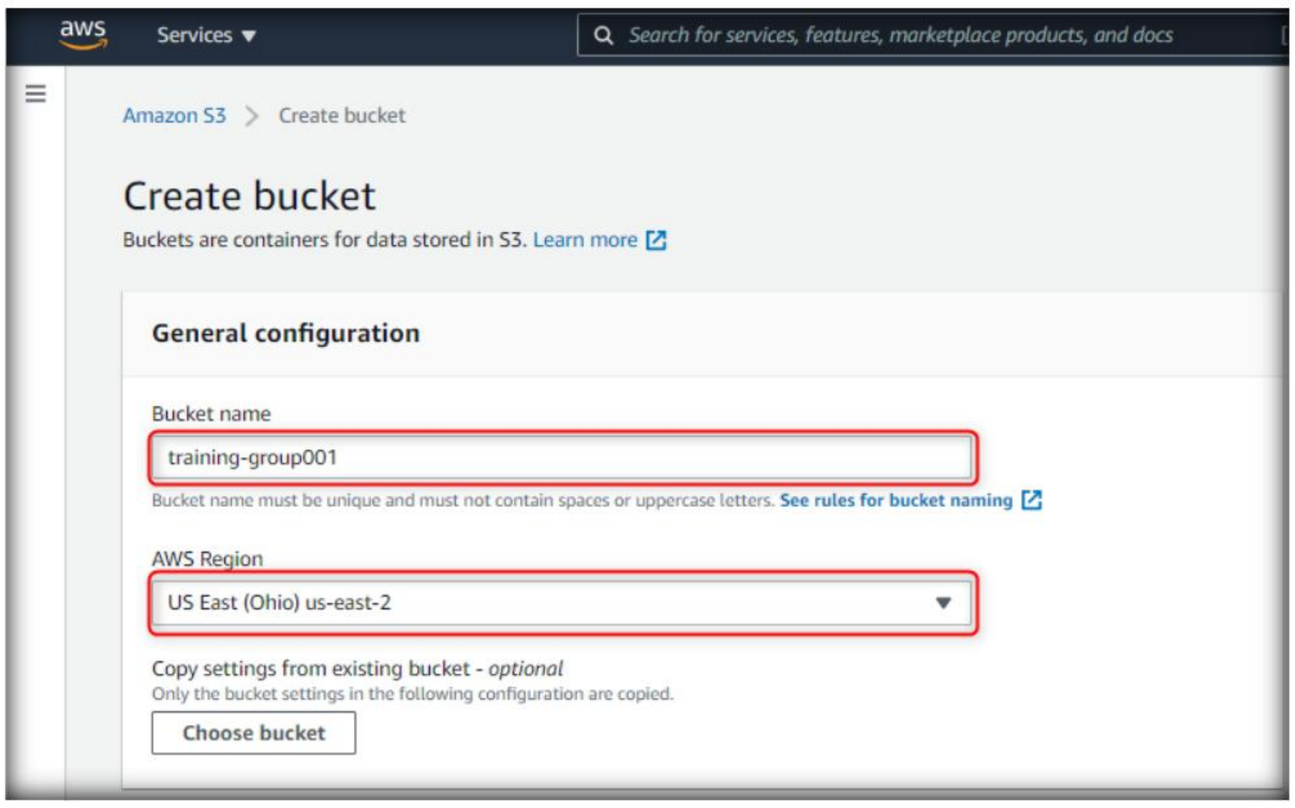


FIGURE 2.2.26: General Configuration of the Bucket

28. Scroll down to **Block Public Access settings for this bucket**. Retain the default settings, as shown in the screenshot below. Similarly, retain the default settings for **Bucket versioning**.

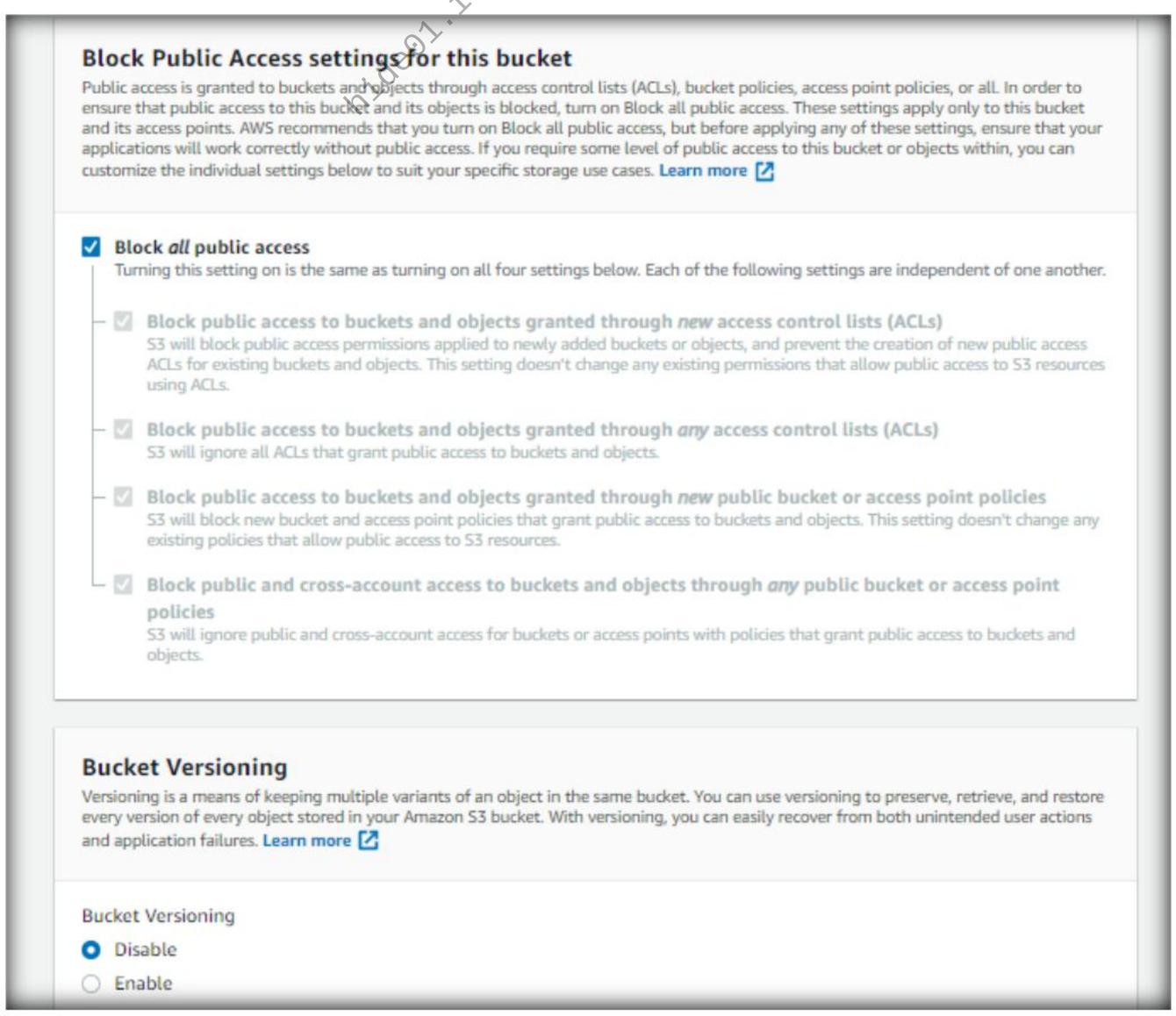


FIGURE 2.2.27: Public Access and Versioning Settings for the Bucket

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

29. Retain the default **Tags** and **Default encryption** settings. Then, click on **Create bucket**.

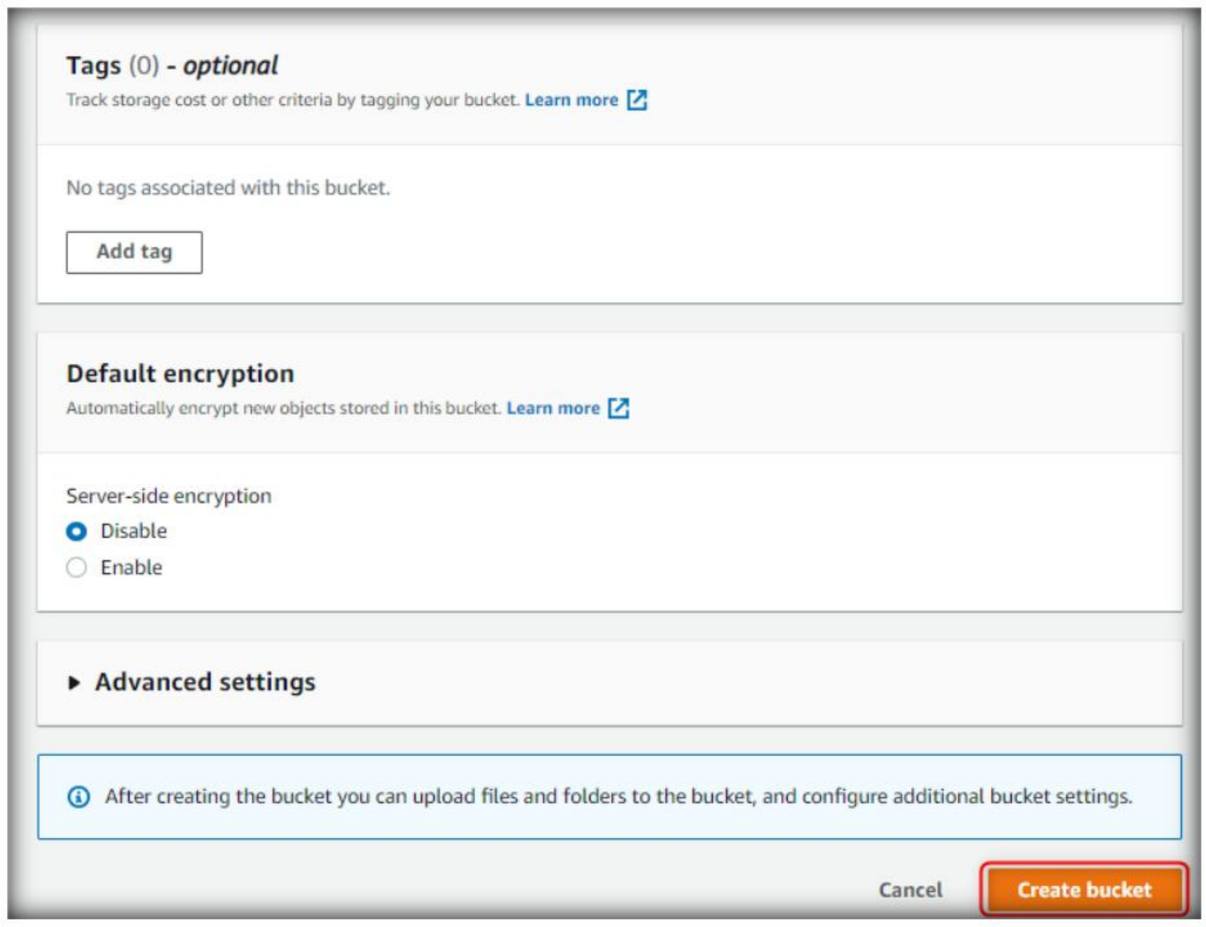


FIGURE 2.2.28: Bucket Encryption and Tags settings

30. A new bucket is created, as shown in the screenshot below. Click on this bucket to configure the encryption settings (here, the bucket is **training-group001**).

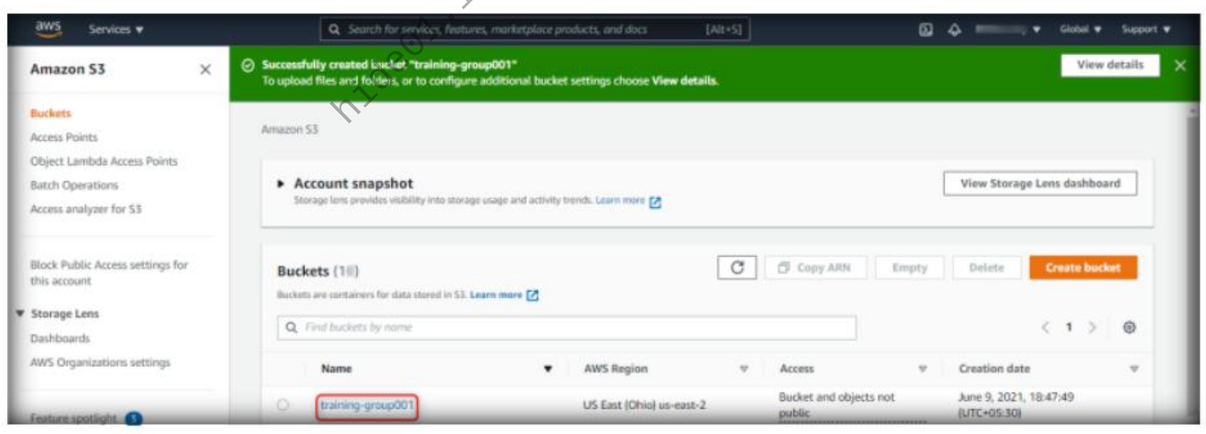


FIGURE 2.2.29: Bucket Selection

31. The **training-group001** bucket page appears. Click on the **Properties** tab and then on **Edit** under the **Bucket Versioning** section.

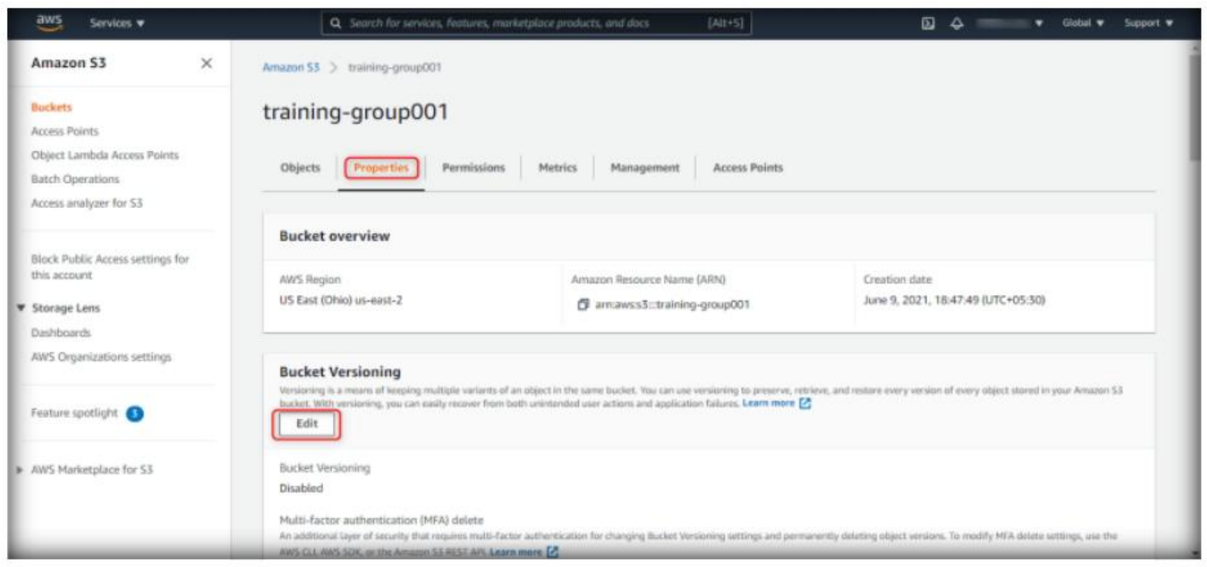


FIGURE 2.2.30: Properties

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

32. Select the **Enable** radio button to enable **Bucket Versioning** and then select **Save changes**.

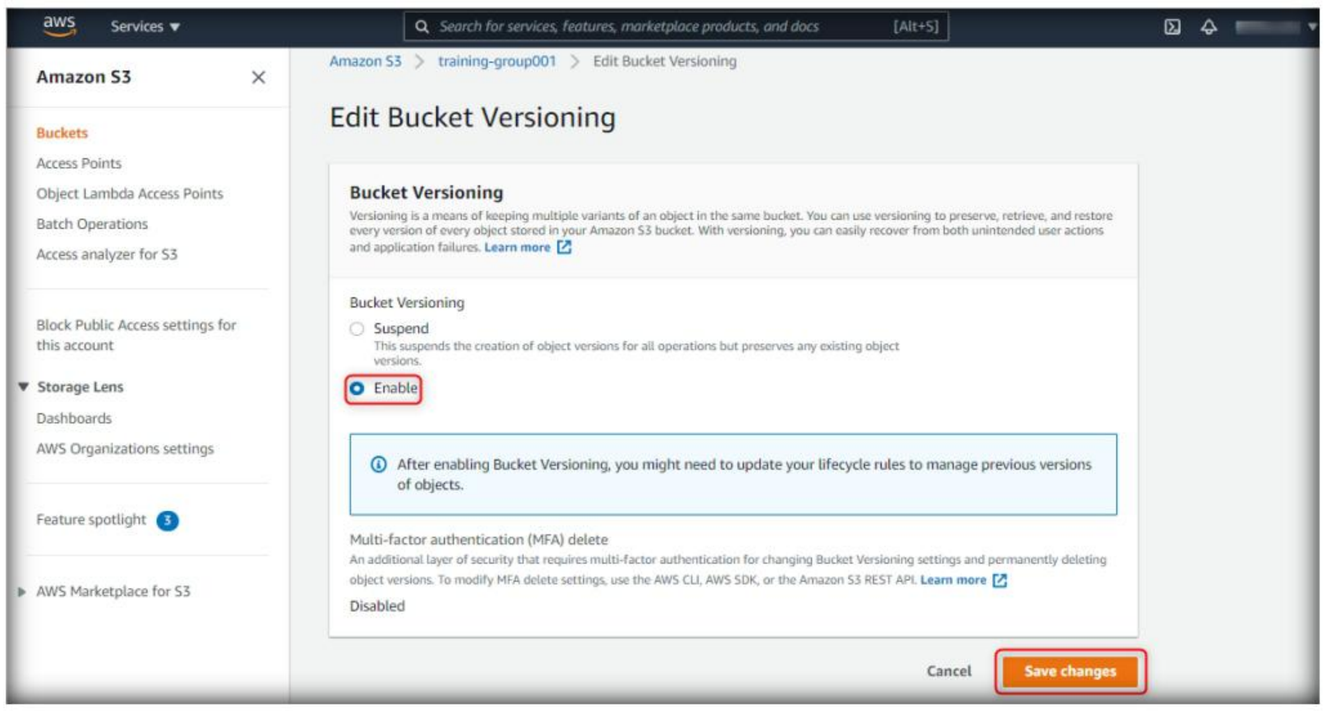


FIGURE 2.2.31: Enable Versioning

33. Scroll down and click on **Edit** in the **Default Encryption** section to enable encryption.



FIGURE 2.2.32: Default Encryption

34. On the **Edit default encryption** page, select the radio button for **Enable**

    - For **Server-side encryption**, choose **AWS Key Management Service key (SSE-KMS)** under **Encryption key type** to create an encryption secured by AWS KMS.
    - Select **AWS managed key (aws/s3)** under **AWS KMS key**.

    Retain the default setting (**Enable**) for **Bucket Key** and click on **Save changes**.

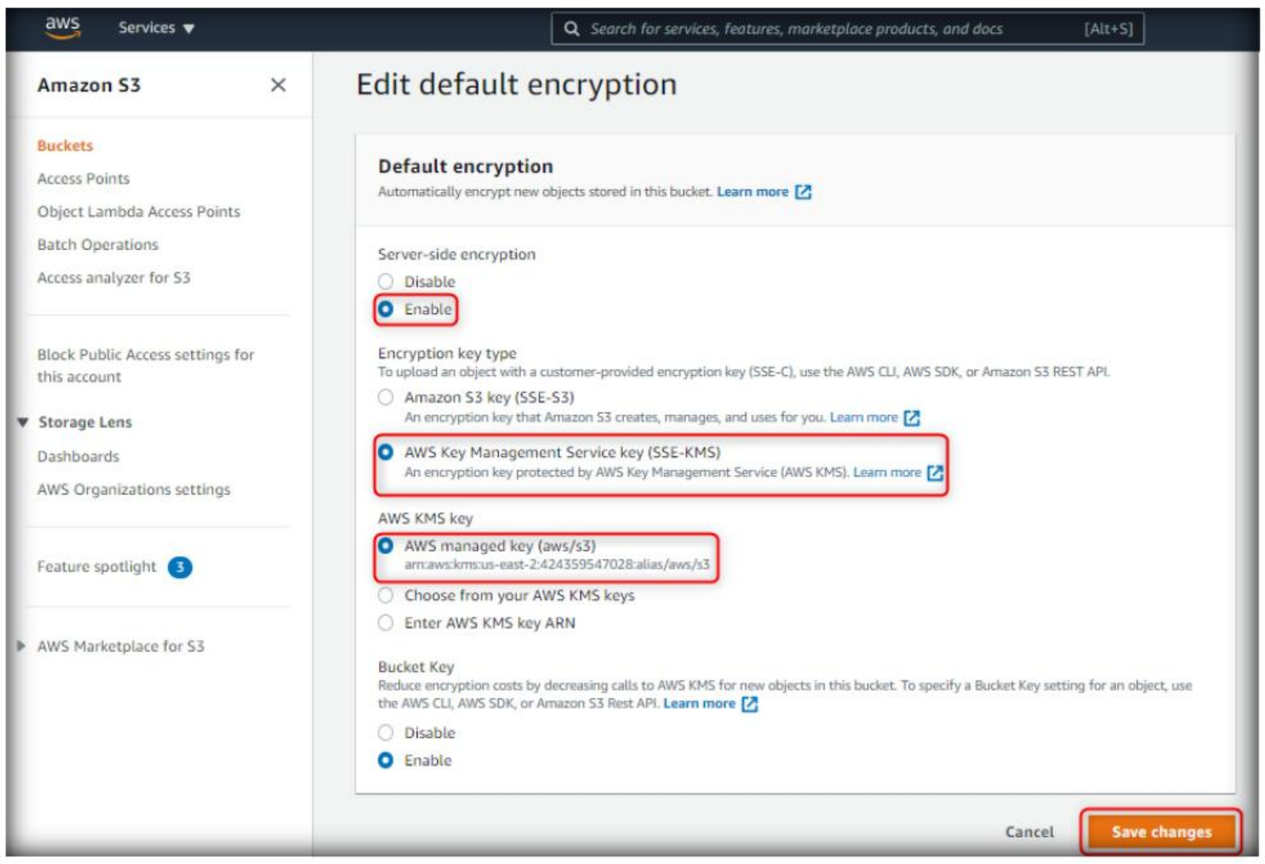


FIGURE 2.2.33: Default Encryption Settings

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

35. Scroll down and click on **Edit** under **Server access logging**.

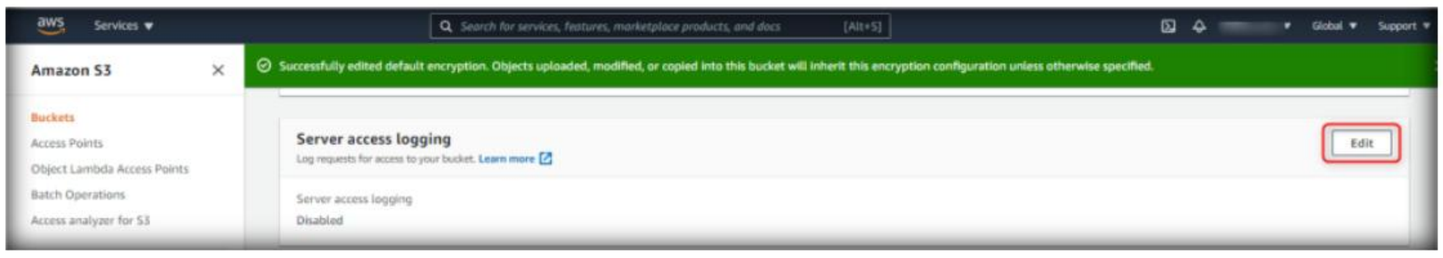


FIGURE 2.2.34: Server access logging

36. Enable **Server access logging** by selecting **Enable**, entering **s3://training-group001** in **Target bucket**, and clicking on **Save changes**.

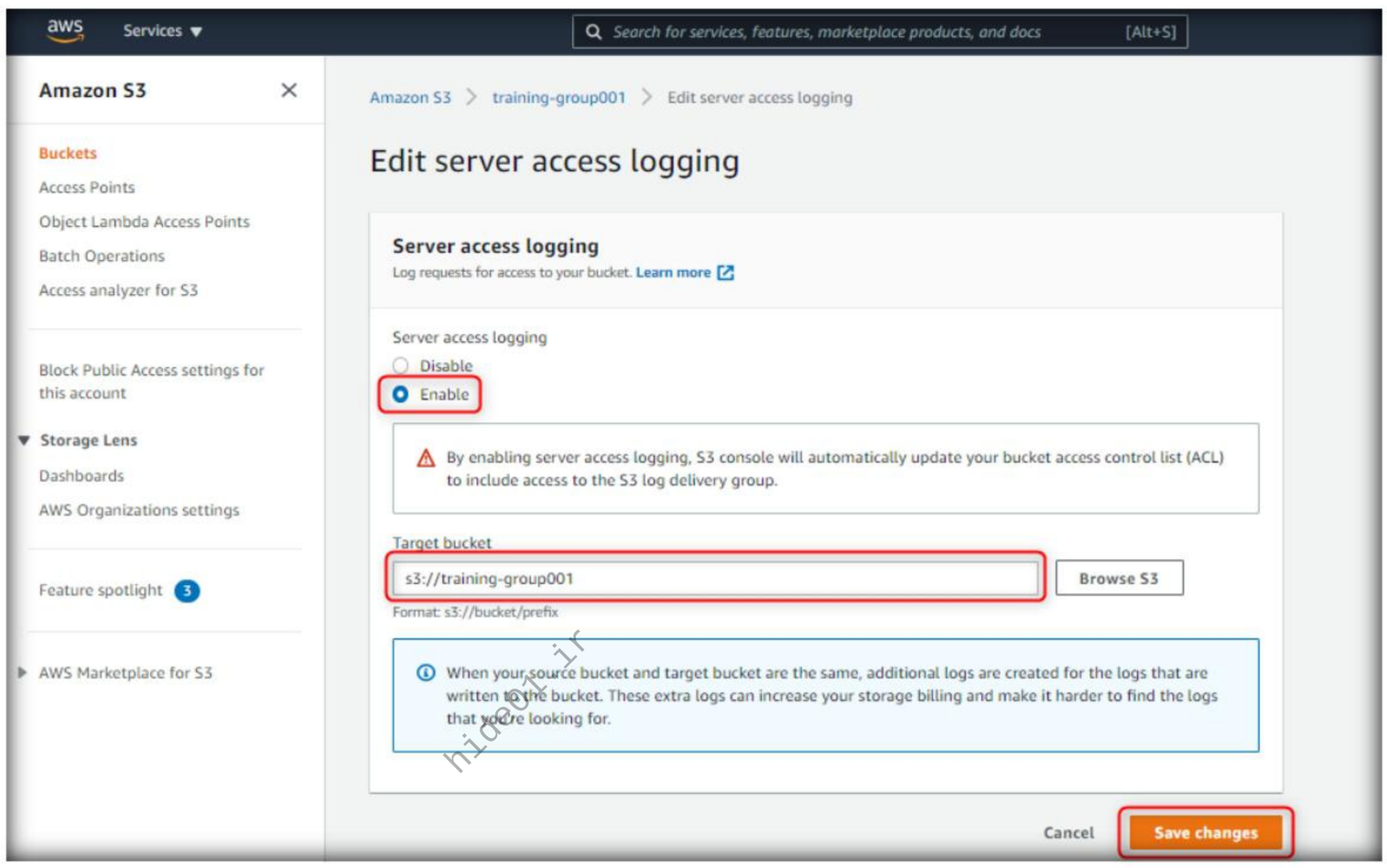


FIGURE 2.2.35: Enabling server access logging

37. You have configured the **training-group001** bucket to encrypt data. The user can now add data into this bucket.

38. The user can also use a customer managed key to encrypt the data in the **training-group001** bucket.

39. Go to **Key Management Services (KMS)** and select **Customer managed keys**. Under the **Customer managed keys** pane, click on the **CCSE_user_MasterKey** alias.

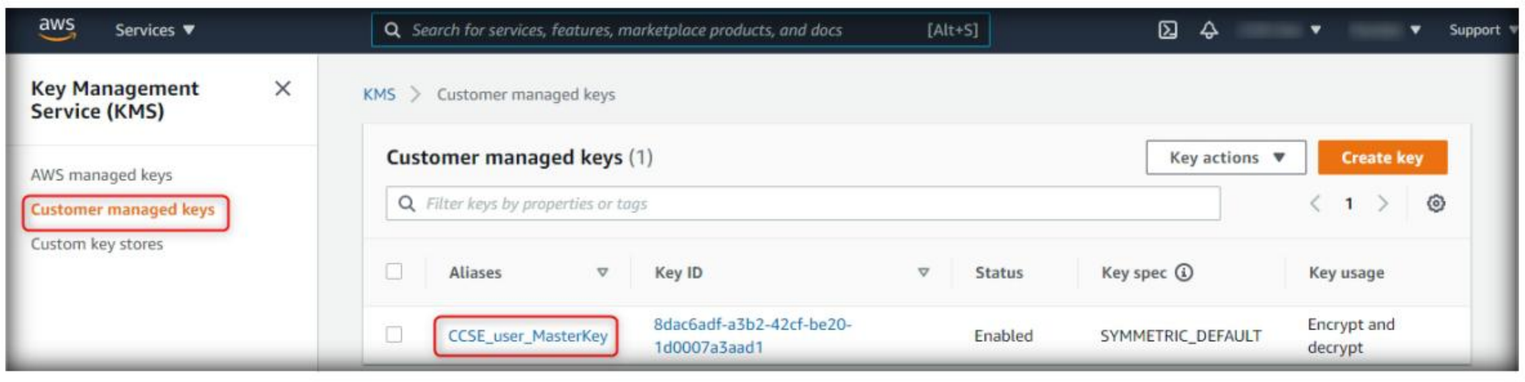


FIGURE 2.2.30: Customer Managed Keys

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

40. Under the **CCSE_user_MasterKey** general configuration, copy the Amazon resource name (ARN) key which uniquely identifies the AWS resources key under the ARN field, as shown in the screenshot below, and paste it to notepad.

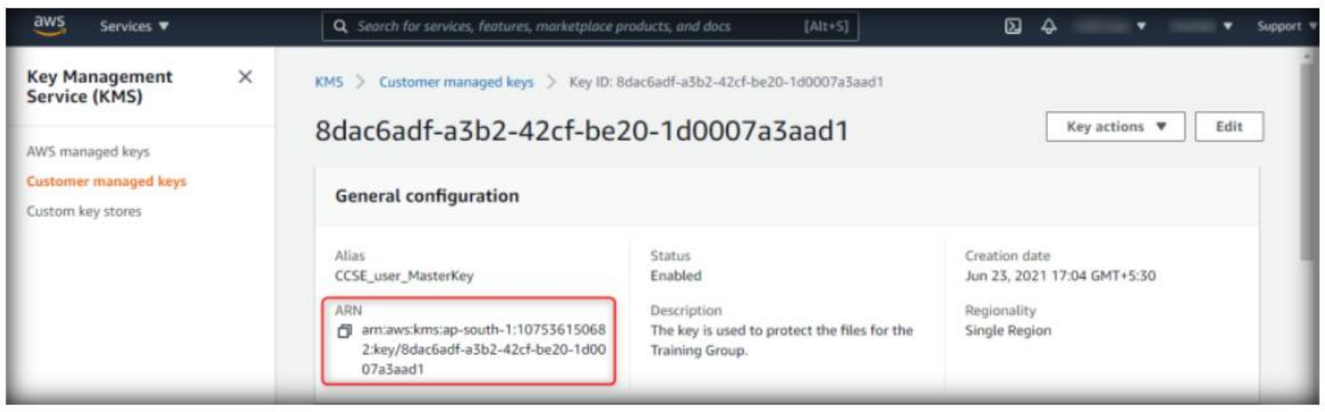


FIGURE 2.2.31: Copy ARN Key

41. Switch to the browser. Navigate to **S3 Management Console** to search for and select **training-group001** under **Bucket name**.

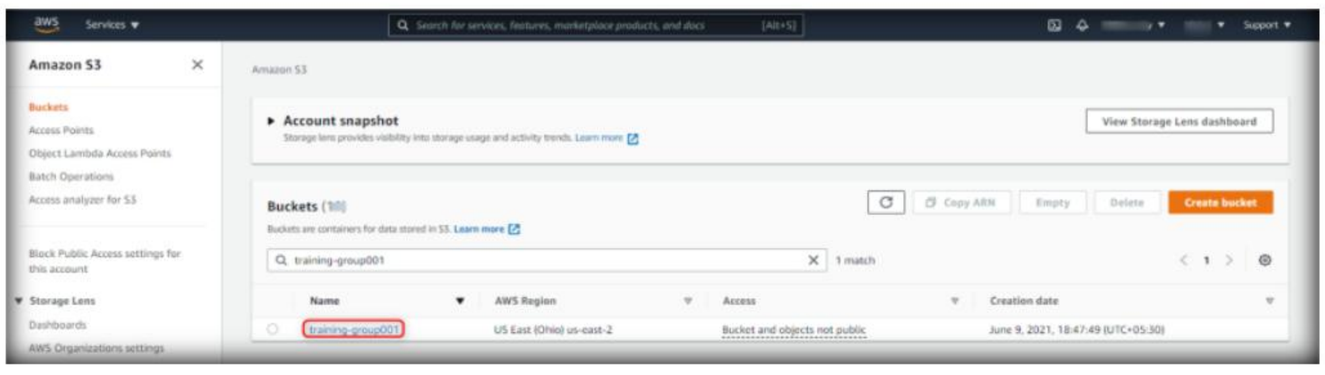


FIGURE 2.2.32: Selecting Bucket

42. The **training-group001** pane opens. Select the **Properties** tab, as shown in the screenshot below.

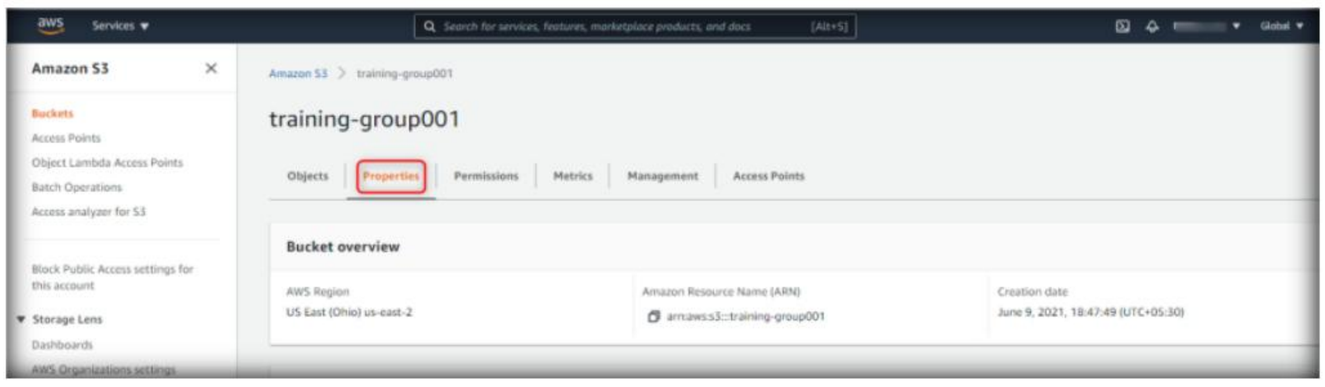


FIGURE 2.2.33: Select Properties

43. Scroll down and click on **Edit** under **Default encryption** to change default encryption.

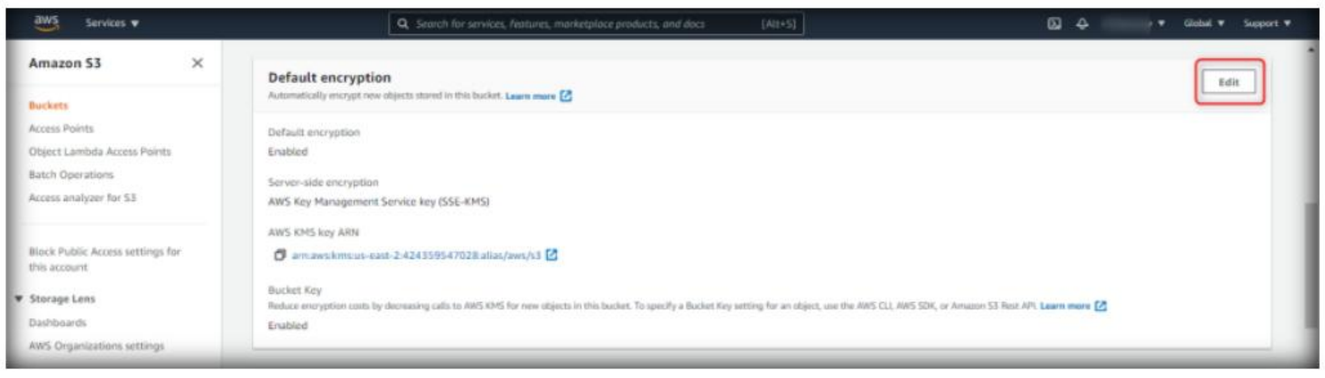


FIGURE 2.2.34: Default Encryption

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

44. On the **Edit default encryption** page, choose **Enter AWS KMS key ARN** under **AWS KMS key**.

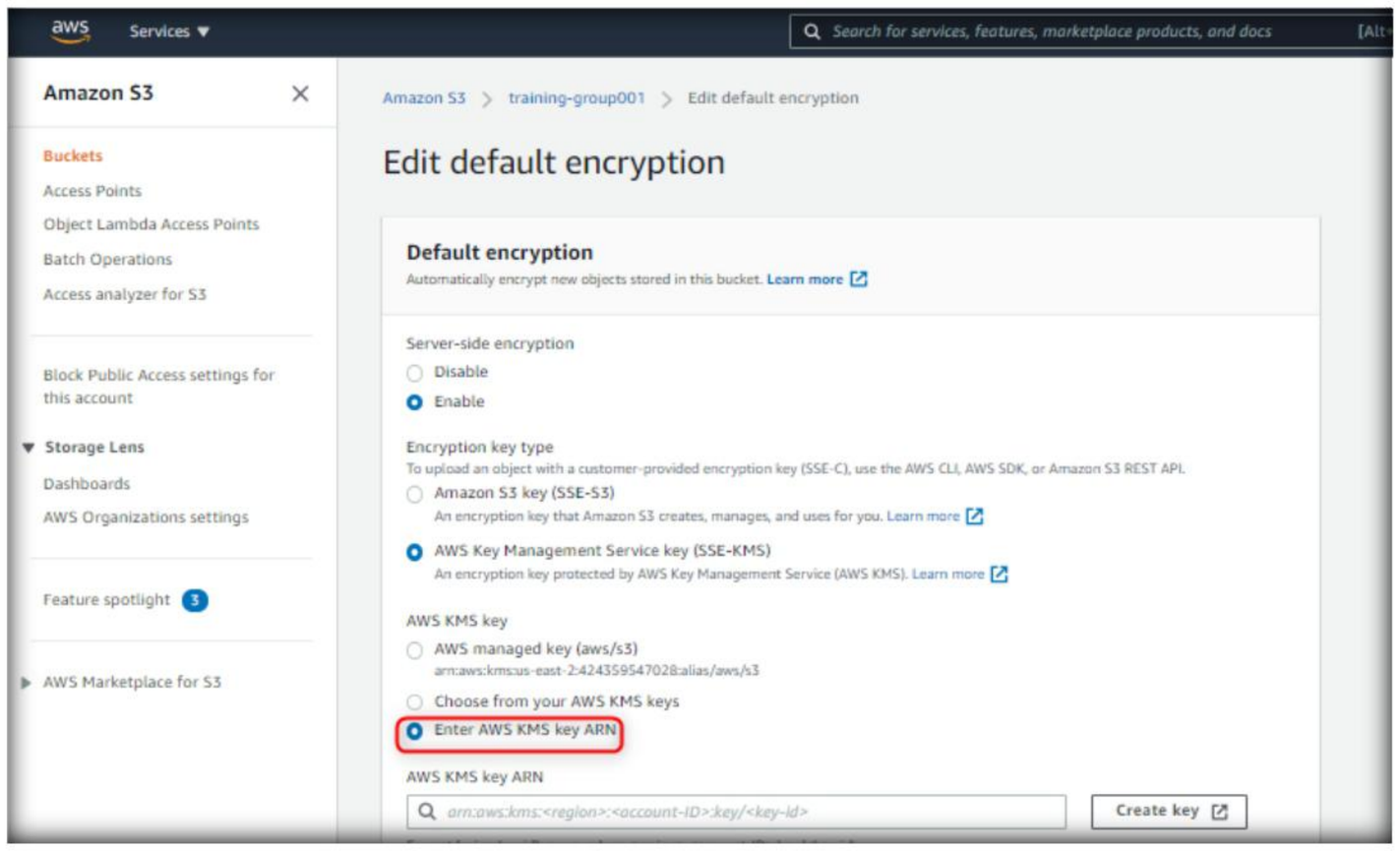


FIGURE 2.2.35: Select Enter AWS KMS key ARN

45. Replace the existing **Custom KMS ARN** value with the ARN value copied to notepad in **Step 34** and click on **Save changes**.

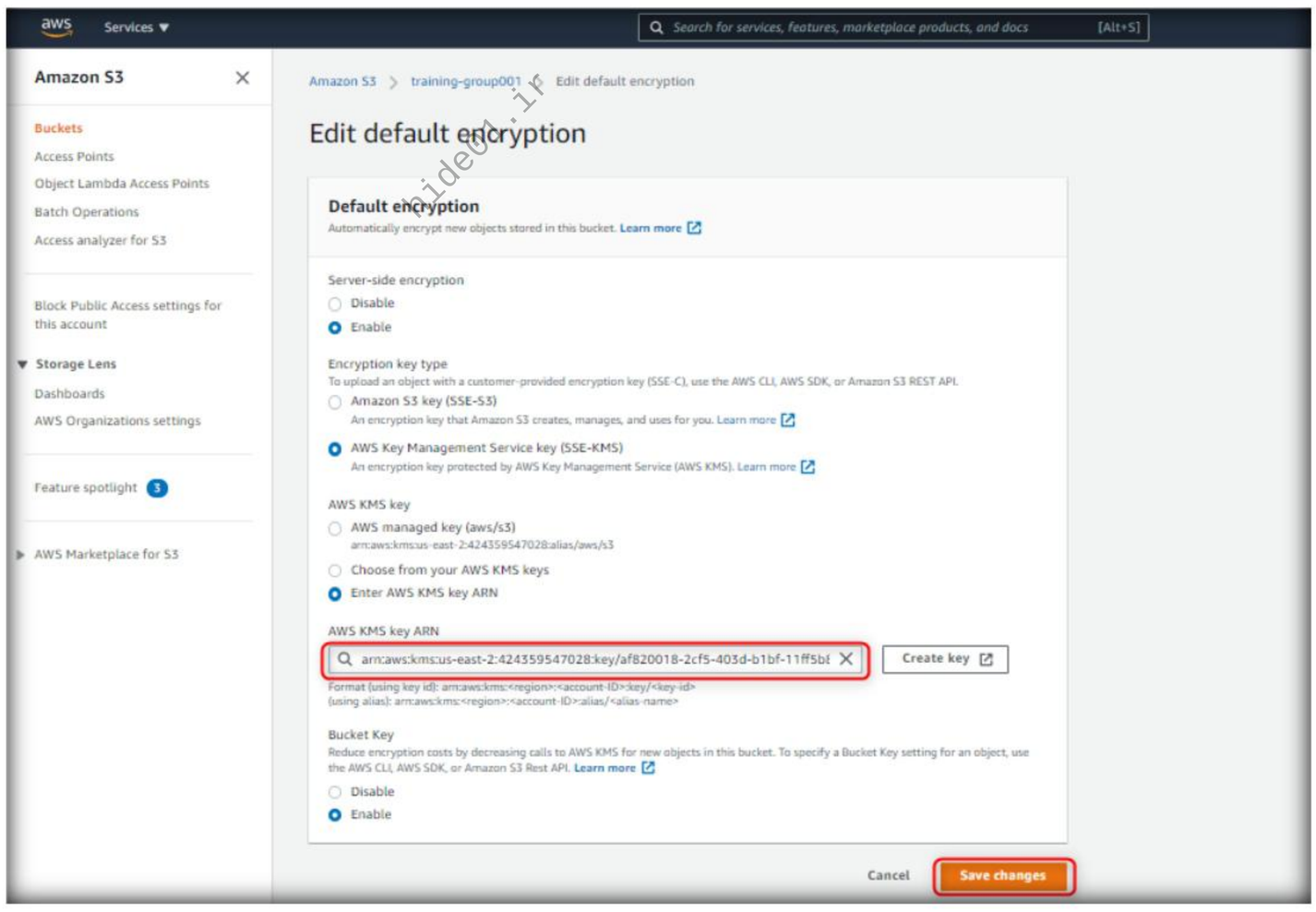


FIGURE 2.2.36: Enter ARN Key

TASK 3

Implement KMS Mater Key for Encrypting EBS Volume

46. This way, a user can encrypt and protect storage data with the help of customer managed keys.
47. Amazon **EBS** supports KMS. Its encryption provides data-at-rest security by encrypting data volumes, boot volumes, and snapshots using Amazon-managed keys or keys created and managed using AWS KMS.

Certified Cloud Security Engineer Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

48. To encrypt EBS volumes with KMS master key, click on **Services** from the menu bar and search for **EC2**. From the search results, click on **EC2 Virtual Servers in the cloud**, as shown in the screenshot below.

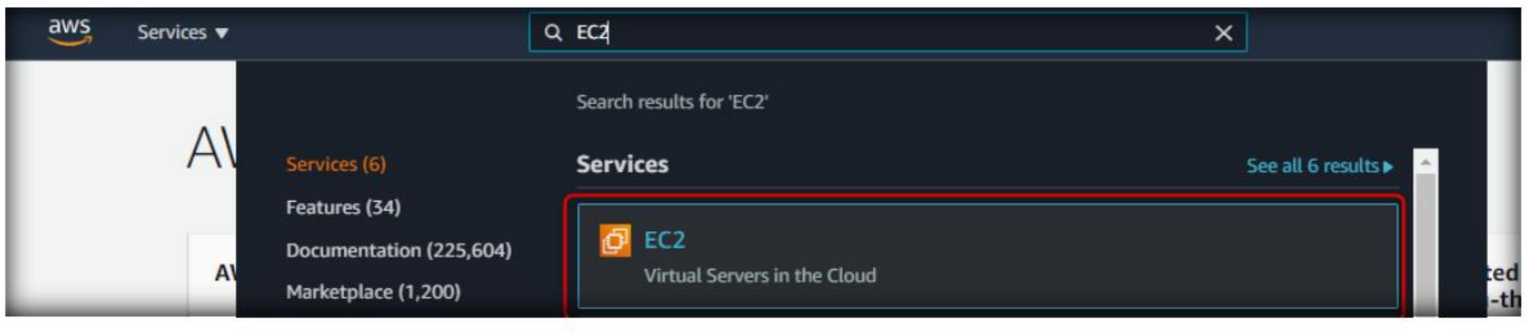


FIGURE 2.2.37: EC2 Services

49. Once the **EC2 Dashboard** page opens, click on **Volumes** in the left pane under **ELASTIC BLOCK STORE**.

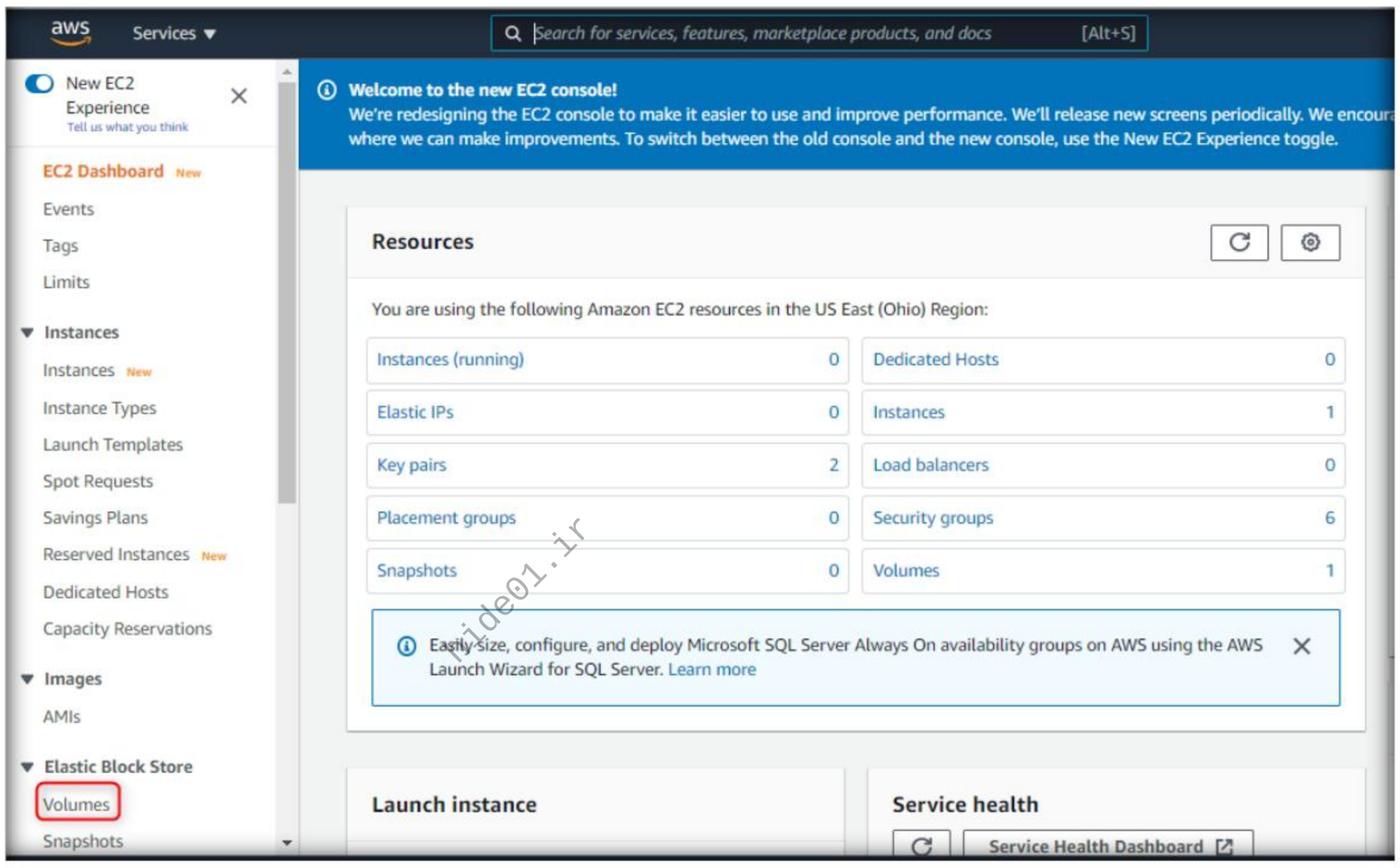


FIGURE 2.2.38: Volumes

50. To create a new volume, click on **Create Volume**.

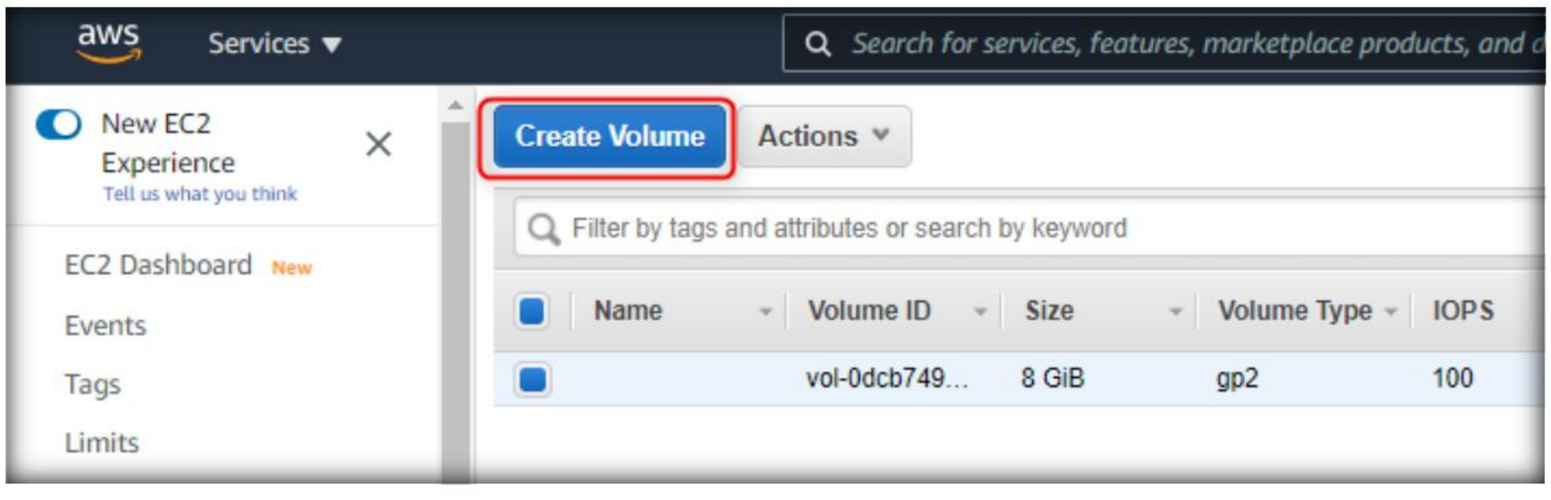


FIGURE 2.2.39: Creating New Volume

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

51. In the **Create Volume** page, select the **Volume Type** as **General Purpose SSD (gp2)**. Specify the size of the volume as **5** in the **Size (GiB)** field. Select the checkbox for **Encrypt this volume** for **Encryption**.

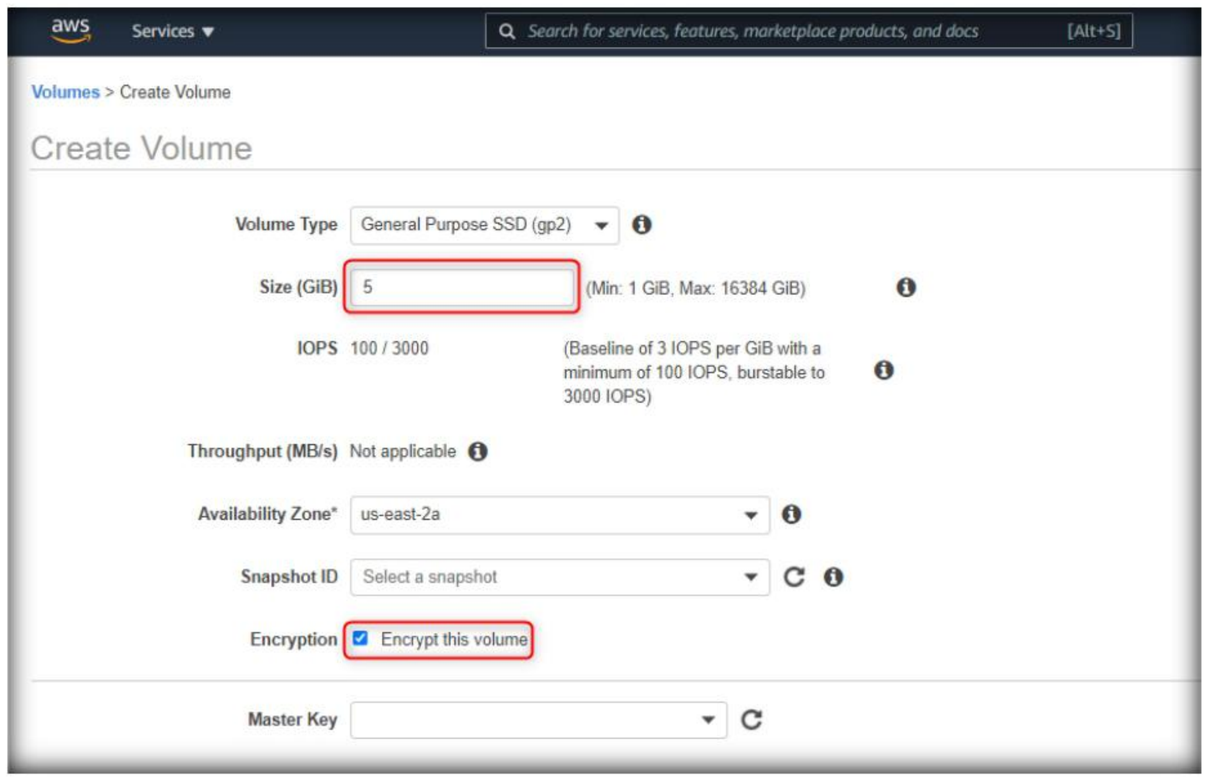


FIGURE 2.2.40: Volume Settings

52. In the **Master Key** field, select the **customer managed key** that was created: **CCSE_user_MasterKey**.

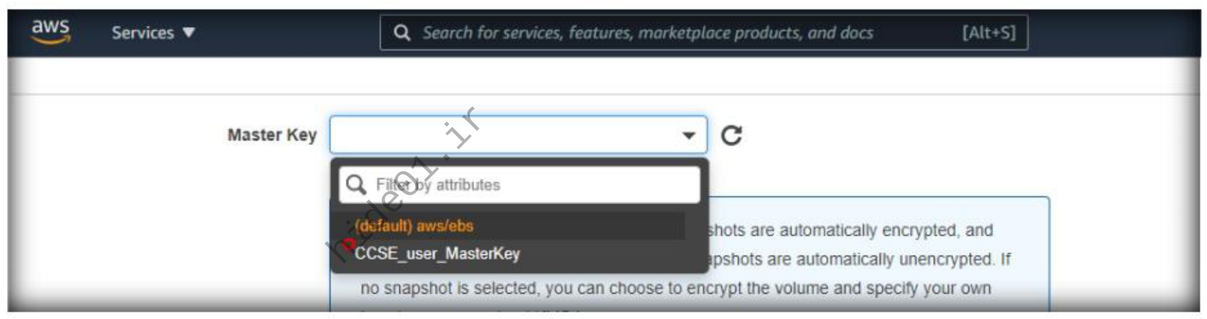


FIGURE 2.2.41: Master Key Selection

53. After entering the required details, scroll down and click on **Create Volume**, as shown in the screenshot below.

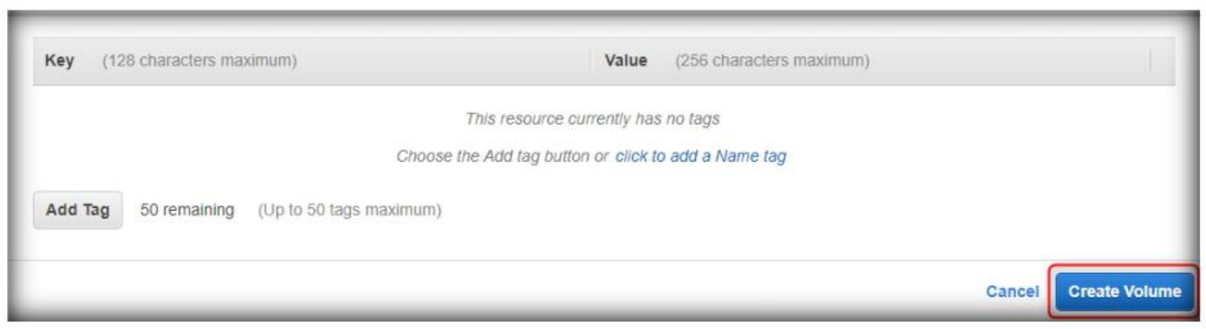


FIGURE 2.2.42: Create Volume

54. A **Volume created successfully** dialog will appear once the disk is created. Click on **Close**.

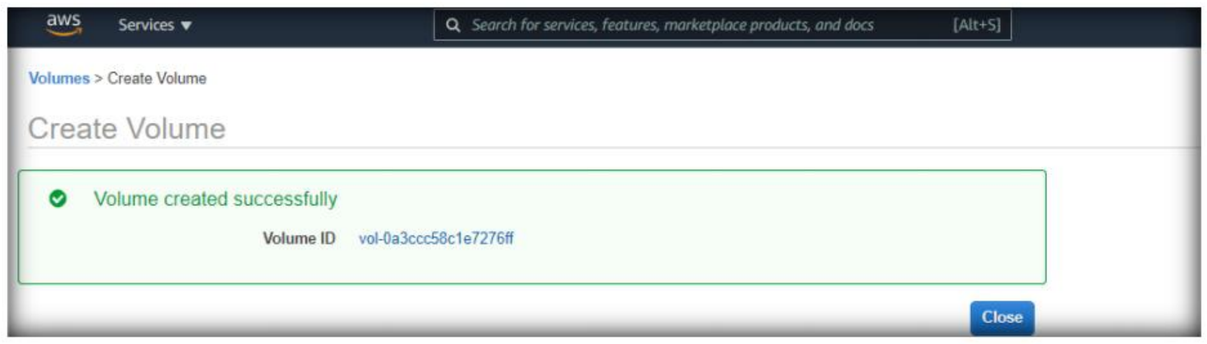


FIGURE 2.2.43: Volume Created Successfully

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 4

Encrypt Amazon Redshift Using KMS Master Key

55. This is how the KMS master key is used to encrypt an EBS volume.
56. Now, encrypt Amazon Redshift using KMS master key as you encrypted the EBS volume.
57. On the **AWS Web Console**, go to **Services**, search for **redshift**, and select **Amazon Redshift**.

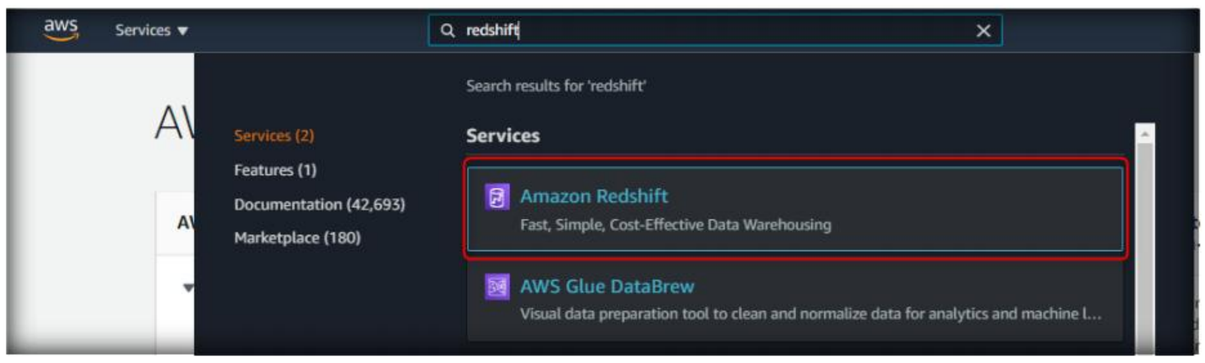


FIGURE 2.2.44: Selecting Redshift Service

58. Close the welcome popup that appears. Click on **Create cluster** in the **Redshift** dashboard, as shown in the screenshot below.



FIGURE 2.2.45: Selecting Create cluster

59. The **Cluster configuration** page appears. Retain the settings. To view the detailed configuration of the cluster, scroll down the page.

    Note: Please note that if you select the Production option, your account will be charged as per the AWS pricing model, so make sure that you delete the Redshift cluster service after performing the lab

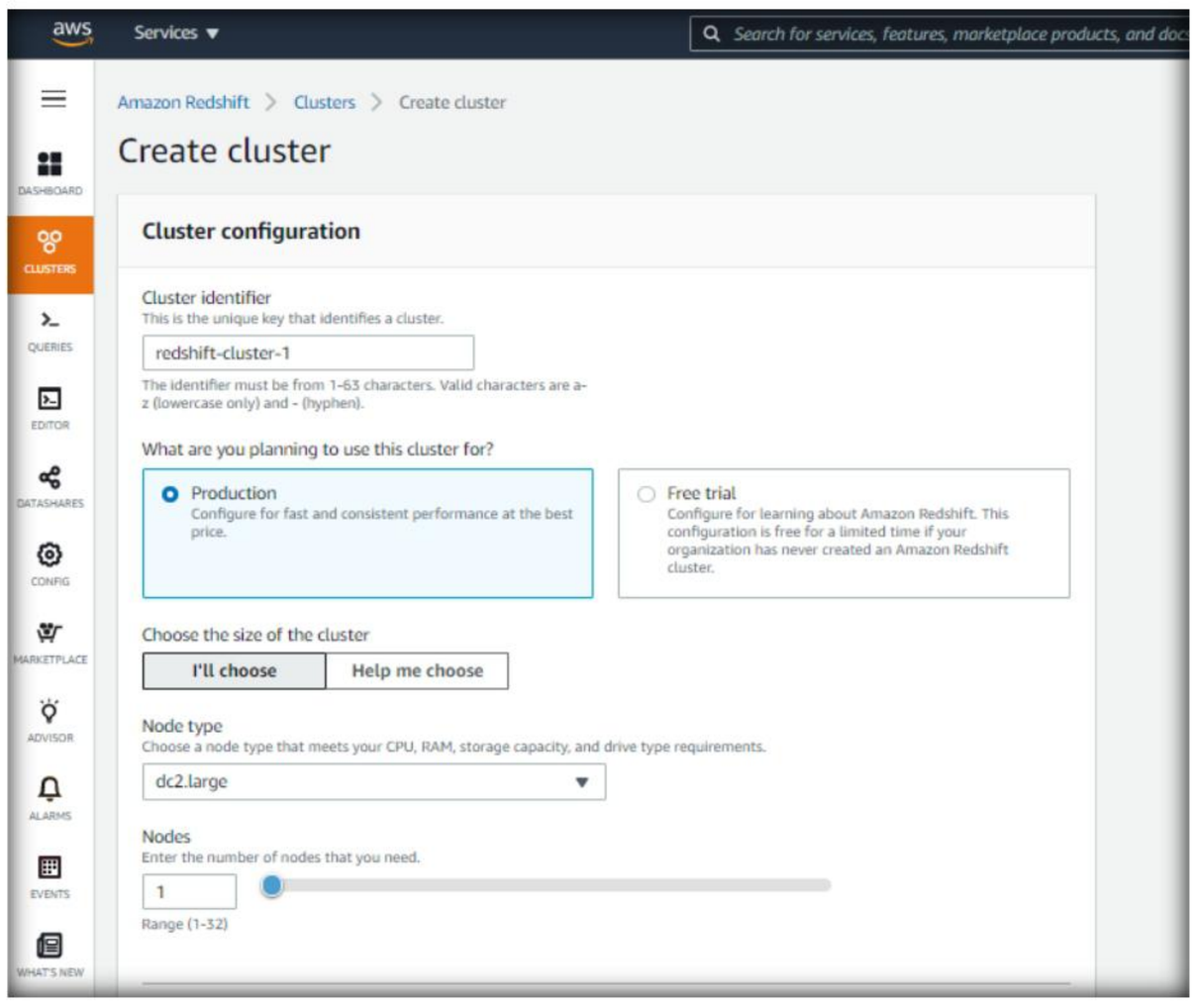


FIGURE 2.2.46: Creating Cluster

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

60. Retain all default settings. Type **Dbuser123** in the **Master user password** field and click on **Create cluster**.

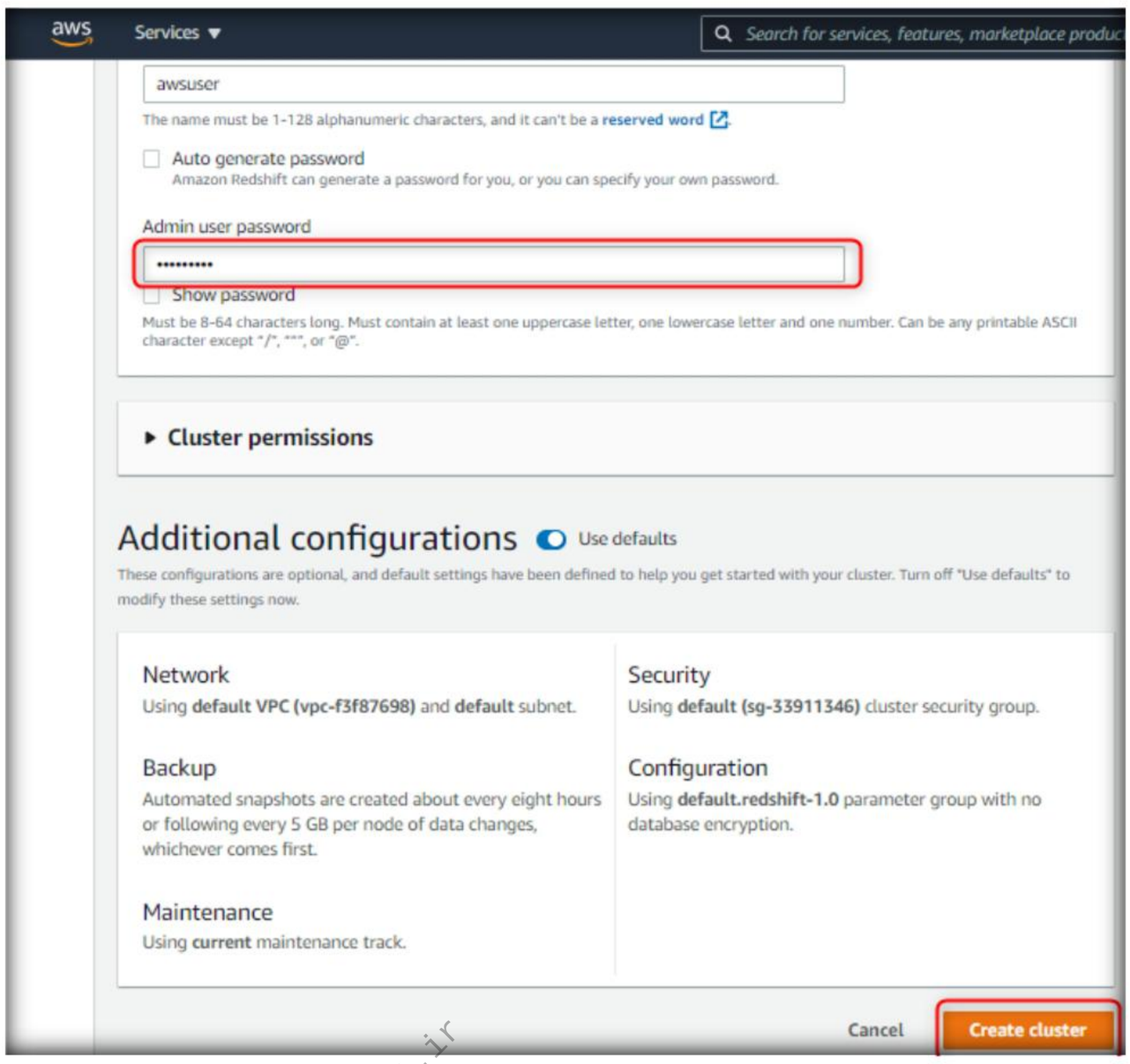


FIGURE 2.2.47: Master User Password

61. The **redshift-cluster-1 is being created** message appears. Wait until the cluster is fully created.

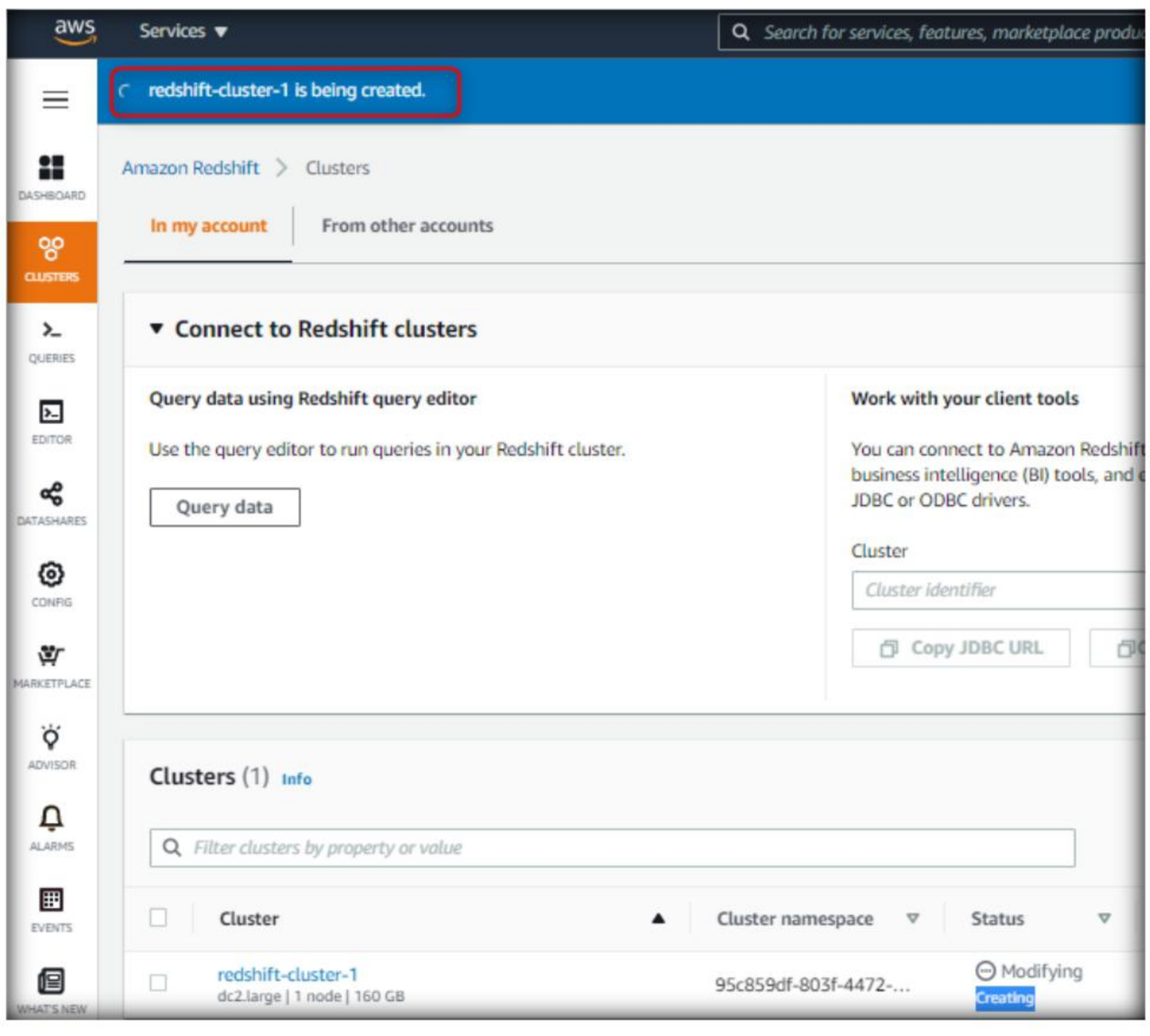


FIGURE 2.2.48: Creating Cluster

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

62. Once the cluster is fully created, you can see the cluster status as **Available,** as shown in the screenshot below. Now, click on the cluster (**redshift-cluster-1**) to configure AWS KMS.

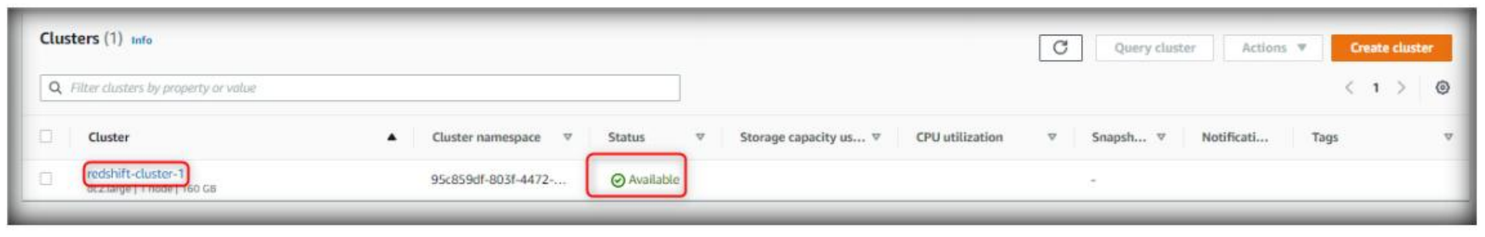


FIGURE 2.2.49: Cluster Status

63. The newly created cluster **redshift-cluster-1** page appears. Select **Properties** and click on **Edit** on the top right side of the **Database configuration** section. Then, click on **Edit encryption**.

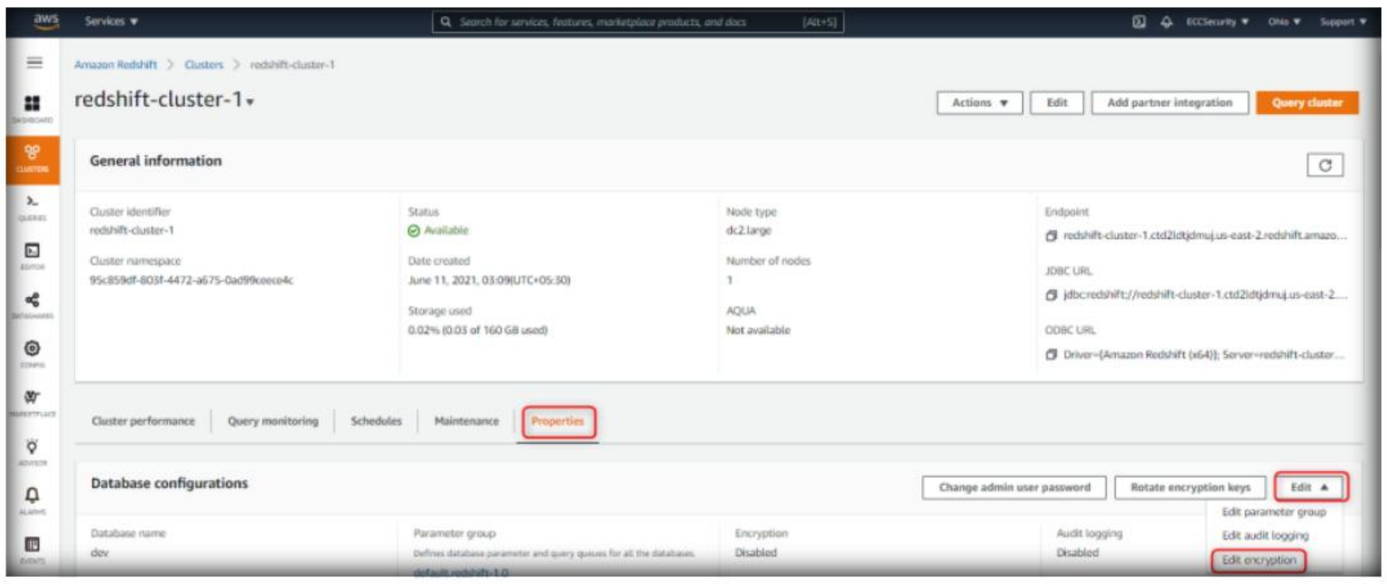


FIGURE 2.2.50: Editing the Cluster

64. The **Edit encryption** page appears. Choose **Use AWS Key Management Service (AWS KMS)** under **Encryption** to encrypt **redshift-cluster-1** with AWS KMS. Under **KMS key ID**, select **CND_user_Masterkey** and click on **Save changes**.

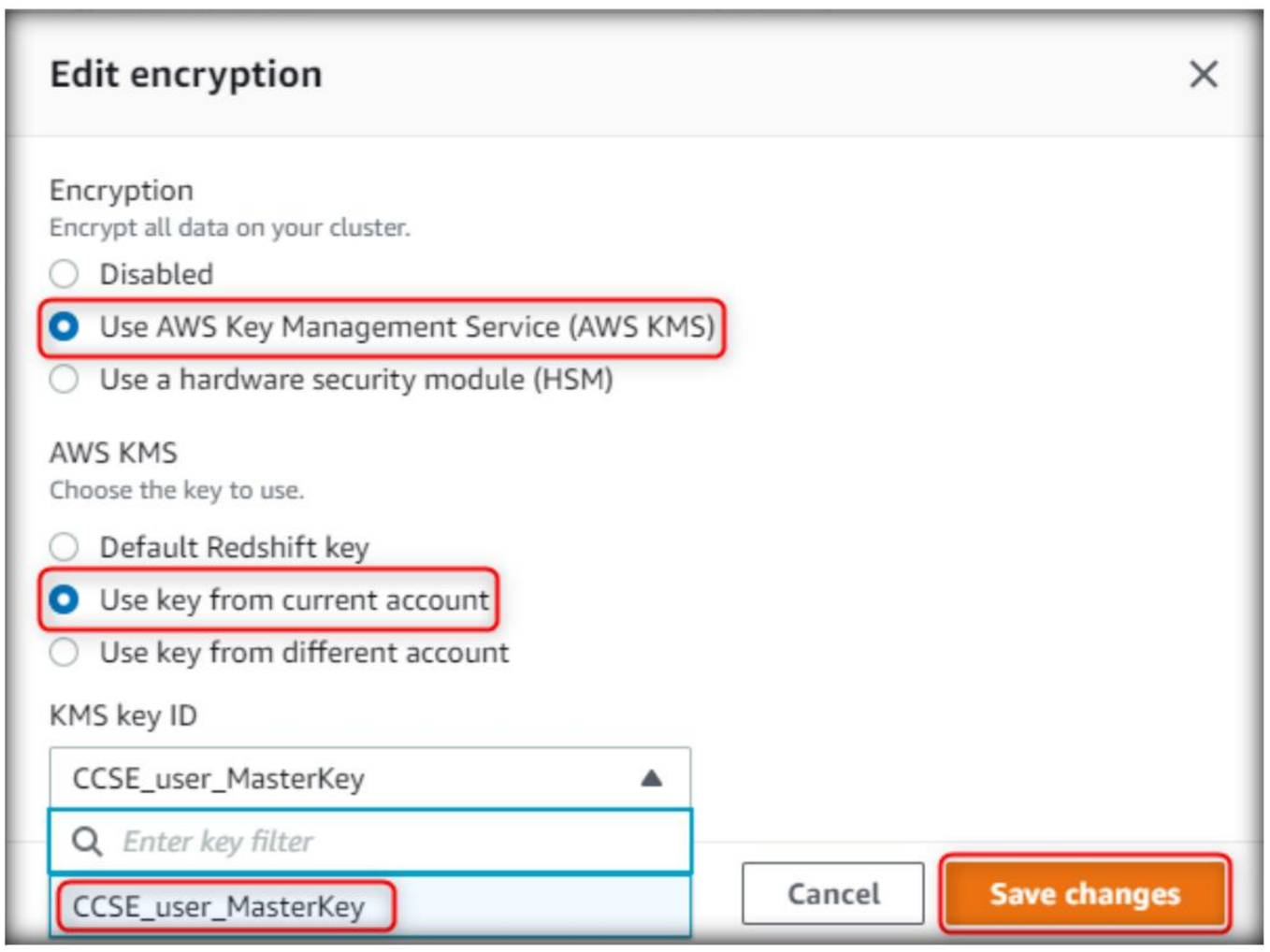


FIGURE 2.2.51: Modifying Cluster

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

65. You will see a message that the cluster is being modified, as shown in the screenshot below.

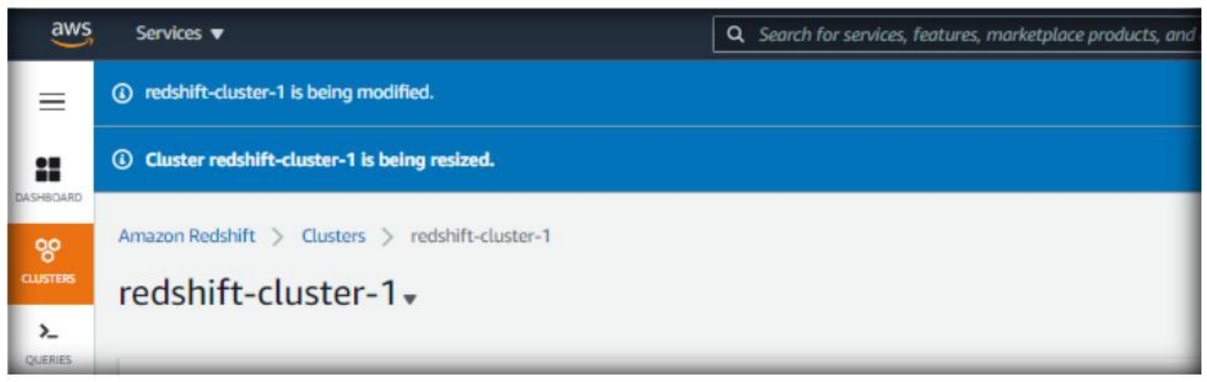


FIGURE 2.2.52: Cluster Modified

TASK 5

Adding New Users to Access the Master Key

66. Next, add new users to access the master key. On the **AWS Web Console**, click on **Services** and search for **kms**. Select **Key Management Service**, as shown in the screenshot below, to get redirected to the **KMS** page.

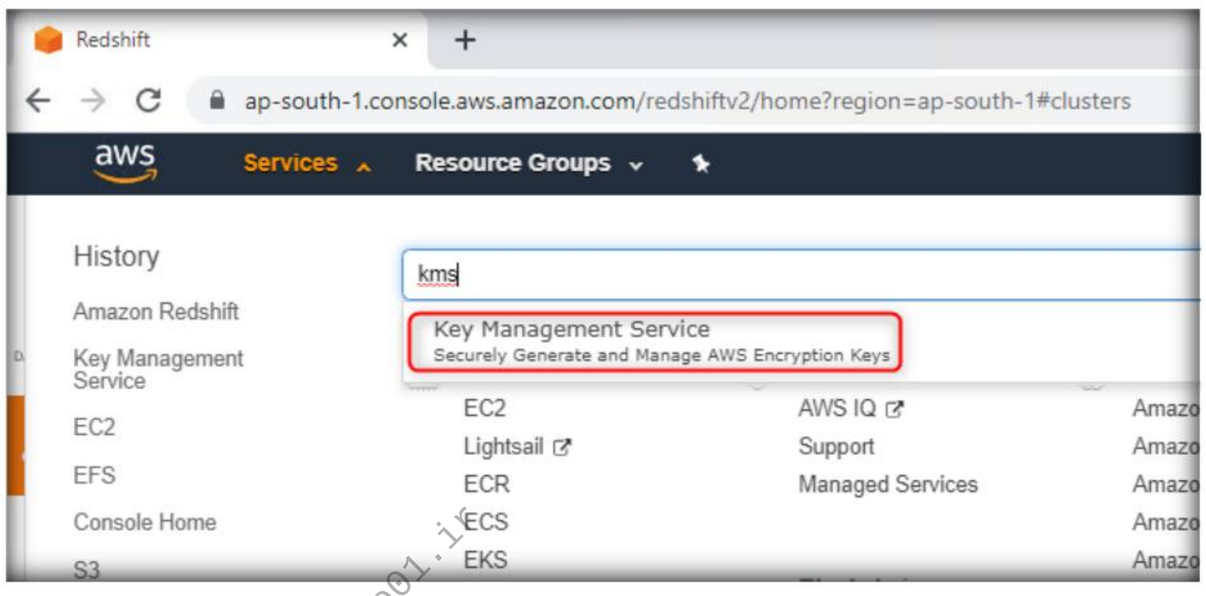


FIGURE 2.2.53: Key Management Service

67. Once the **KMS Console** page appears, click on **Customer managed keys** (here **CCSE_user_MasterKey)**.

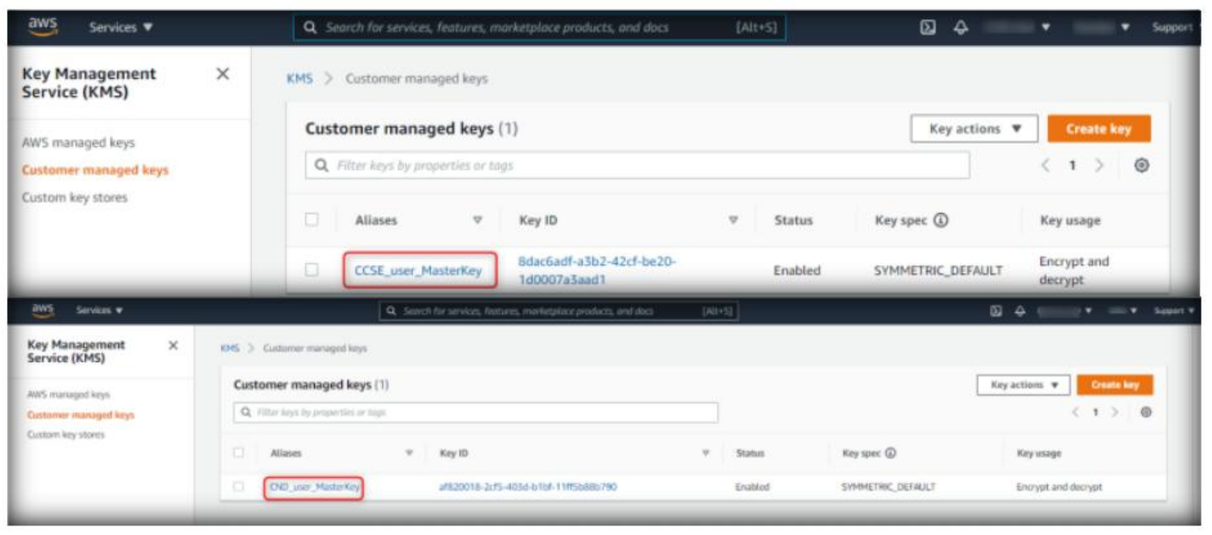


FIGURE 2.2.54: Selecting Customer Managed Keys

68. Scroll down to the **Key users** section. Click on **Add**.

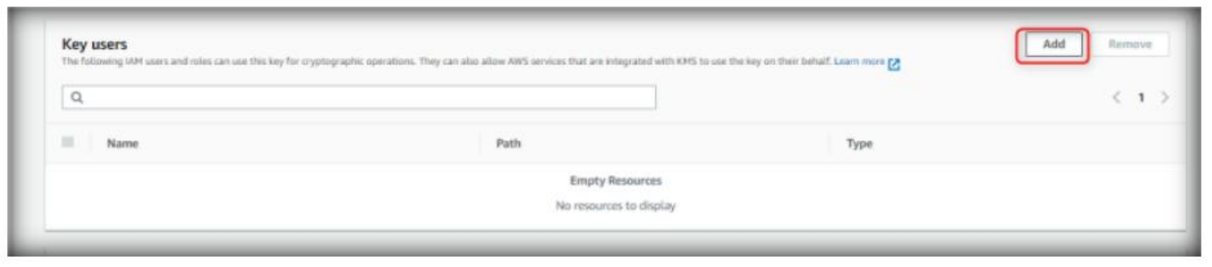


FIGURE 2.2.55: Key Users

69. Use the **Search** box on the **Add key users** window to filter the IAM users. Type the name of user created in the previous lab or in this lab while

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

configuring keys (we have used **Alice)**, as shown in the screenshot below. Add the IAM user (**Alice**) so that they can access the master key. Click on **Add**.

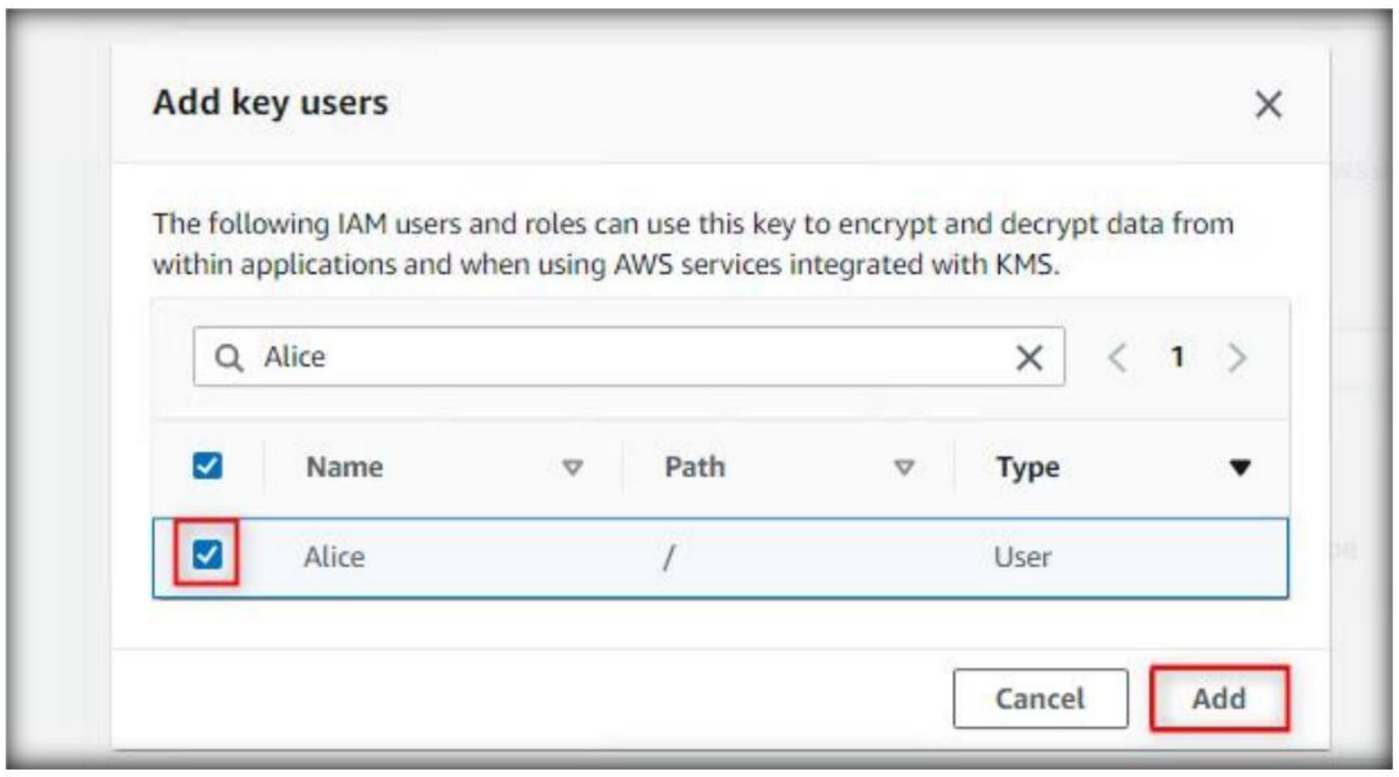
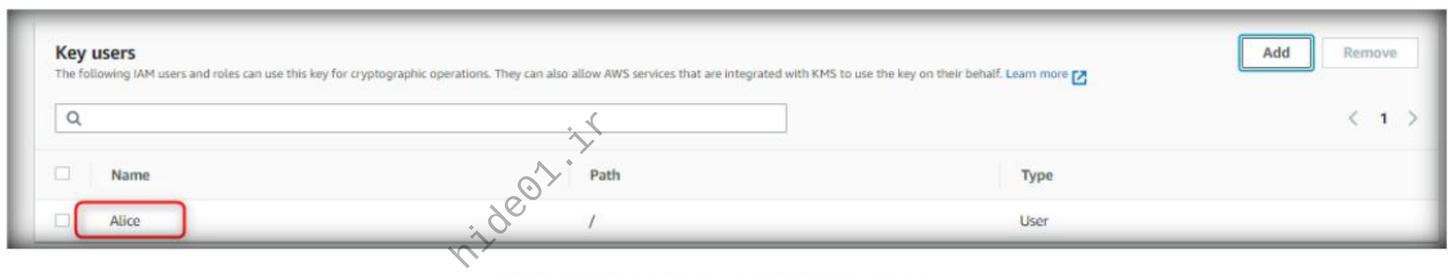


FIGURE 2.2.56: User Selection

70. After you have added the user, it will appear as added in the **Key users** section.



hide01.ir

FIGURE 2.2.57: Added Key User

By following the above steps, a cloud security engineer can implement AWS KMS.

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

71. Now, to delete the Amazon Redshift cluster, navigate to the Amazon Redshift console and select **Snapshots** under **Amazon Redshift provisioned cluster** pane. Select the checkbox for the cluster created in this lab (here, **redshift-cluster-1-final-snapshot**) and click on the **Delete** button. In the pop-up window, click on **Delete**.

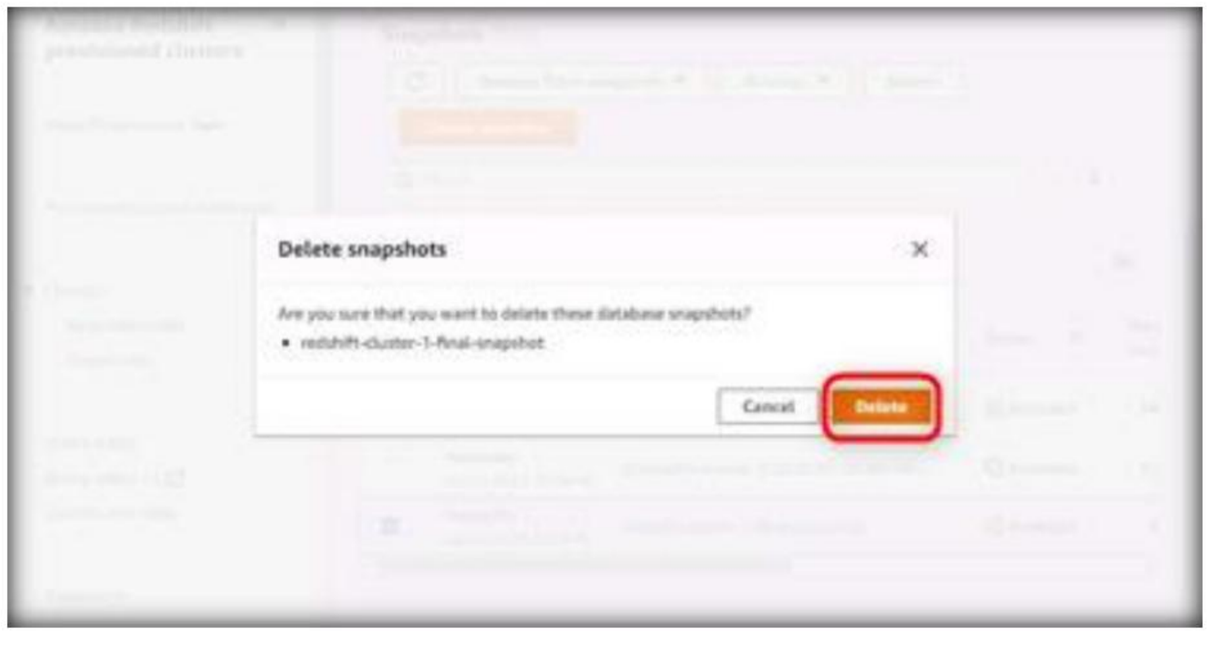


FIGURE 2.2.58: Deleting Amazon Redshift cluster

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

72. Navigate to the Clusters window and select the checkbox for the cluster created in this lab. Click on the **Actions** dropdown and select **Delete**. In the pop-up window, enter delete and click on the **Delete cluster** button.

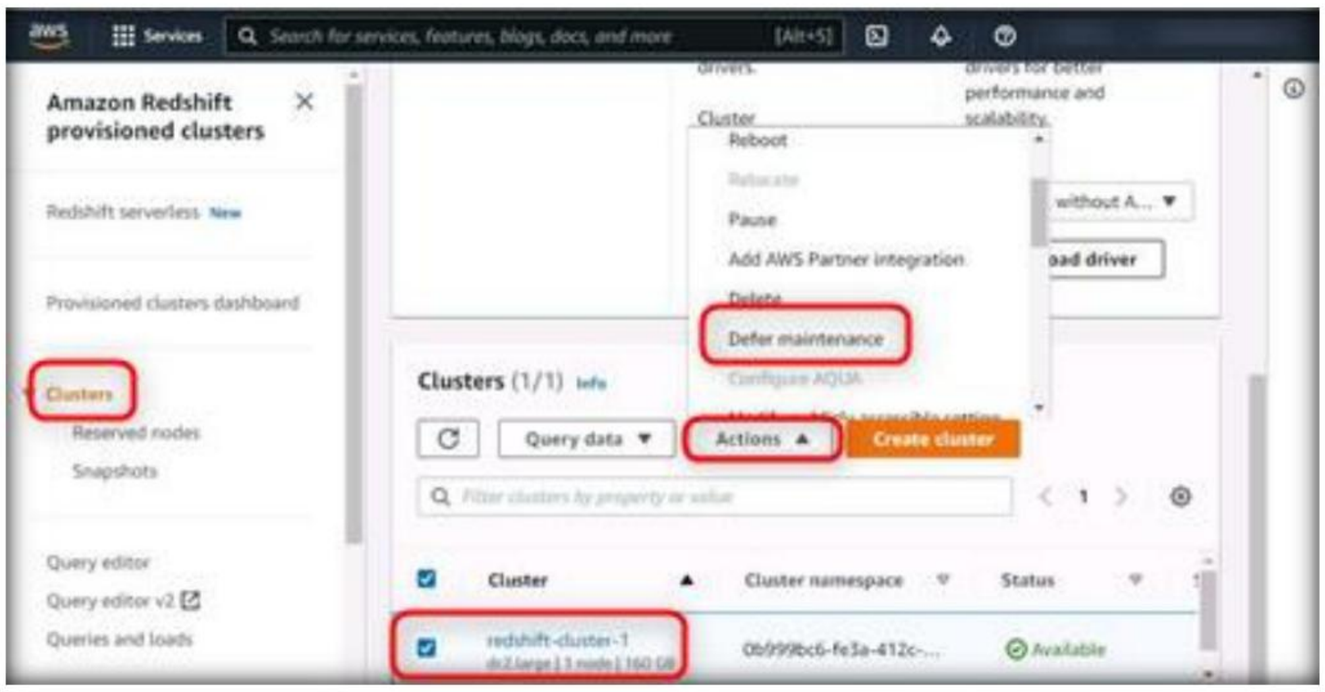


FIGURE 2.2.59: Deleting Amazon Redshift cluster

73. Navigate to the EC2 window and select Volumes. Select the checkbox for the volume created in this lab and click on the **Actions** dropdown. Click on **Delete volume**. In the pop-up window, click on **Delete**.

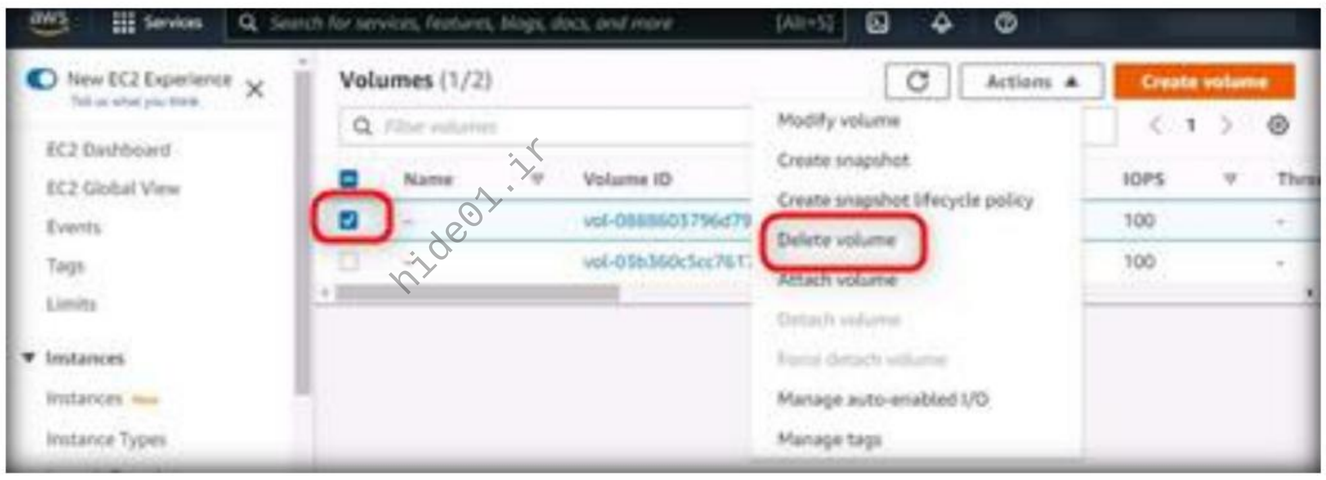


FIGURE 2.2.60: Deleting Volume

74. Navigate to the S3 window and select the checkbox of the bucket created in this lab. Click on the **Delete** button. In the pop-up window, enter the bucket's name and click on the **Delete bucket** button.

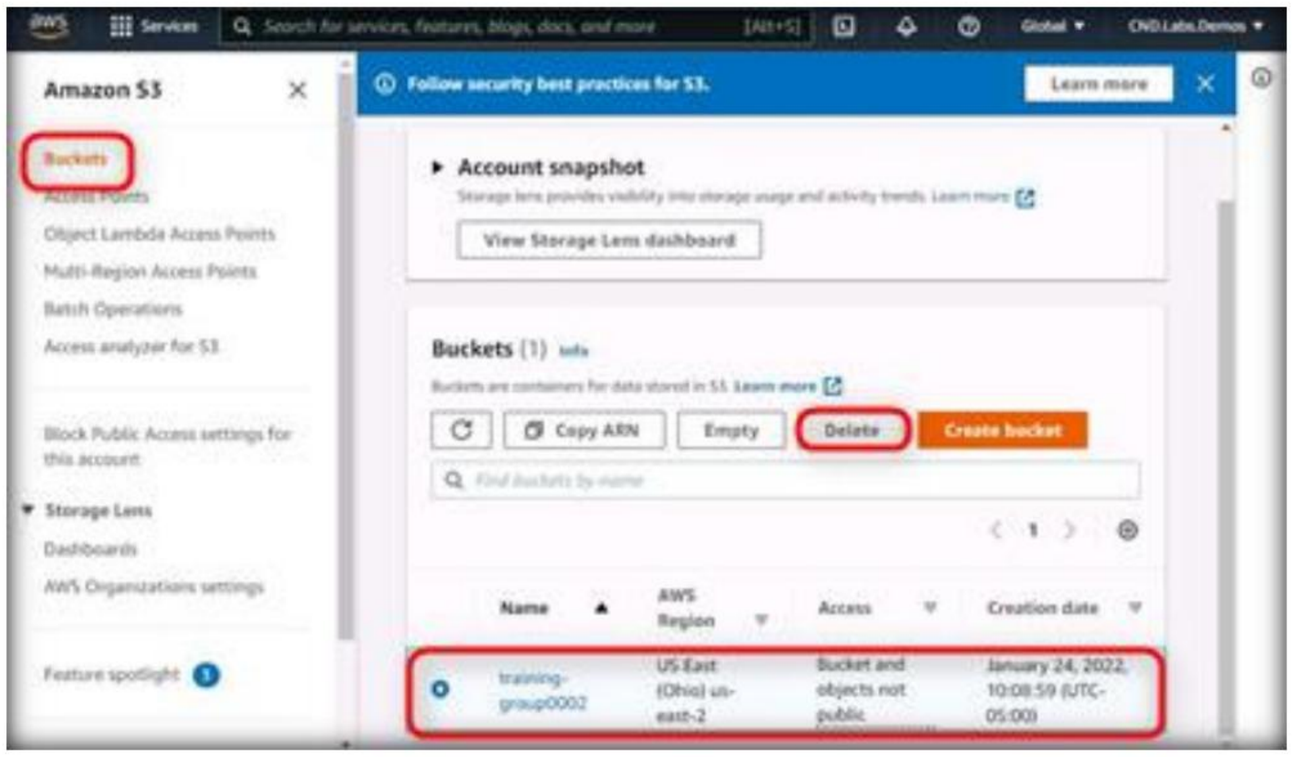


FIGURE 2.2.61: Deleting S3 Bucket

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

75. Navigate to the **Customer managed keys** under the KMS console and select the checkbox of the key created in this lab. Click on the **Key actions** dropdown and click on **Disable** option. In the pop-up window, click on the checkbox to confirm disabling and click on **Disable key**.

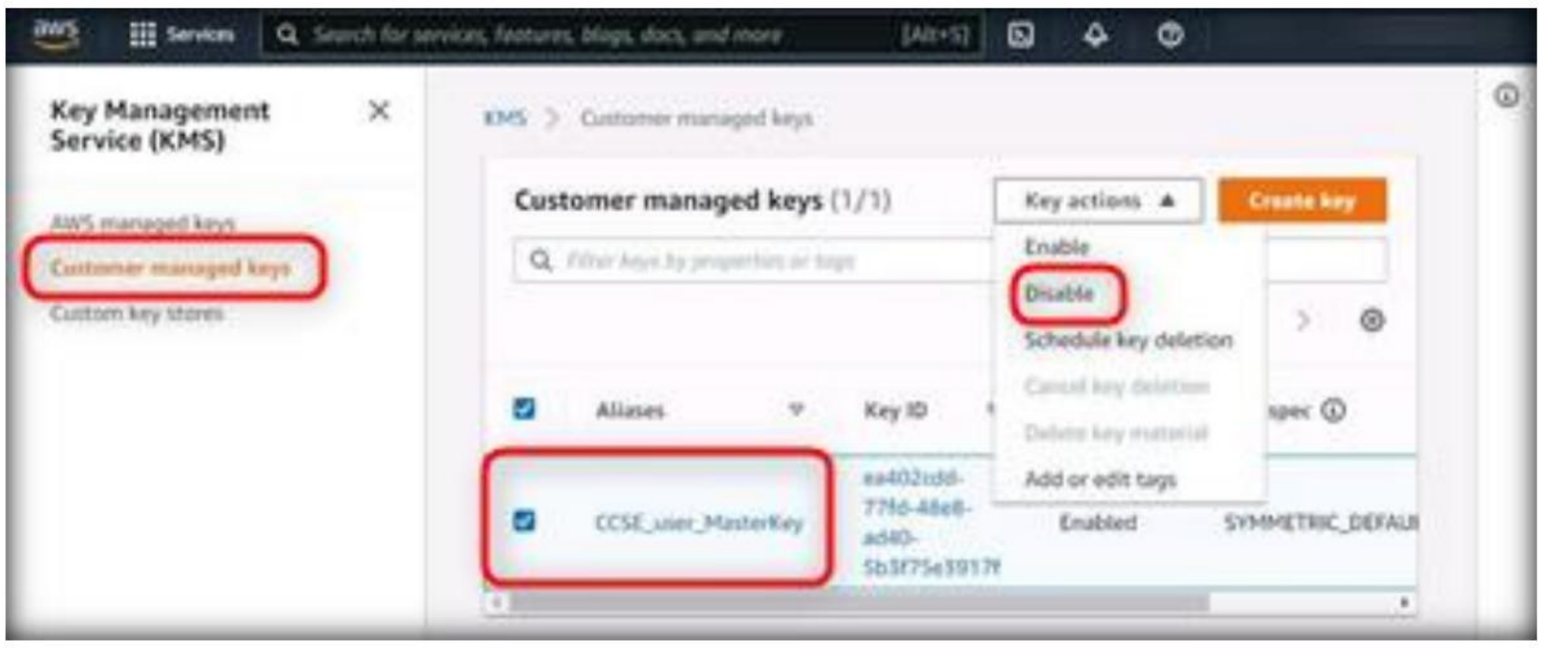


FIGURE 2.2.62: Disabling Customer managed Key

76. Navigate to the **Users** tab and select the checkbox for the user created in this lab (here, **Alice**). Click on the **Delete** button. In the pop-up window, enter the user's name and click on **Delete**.

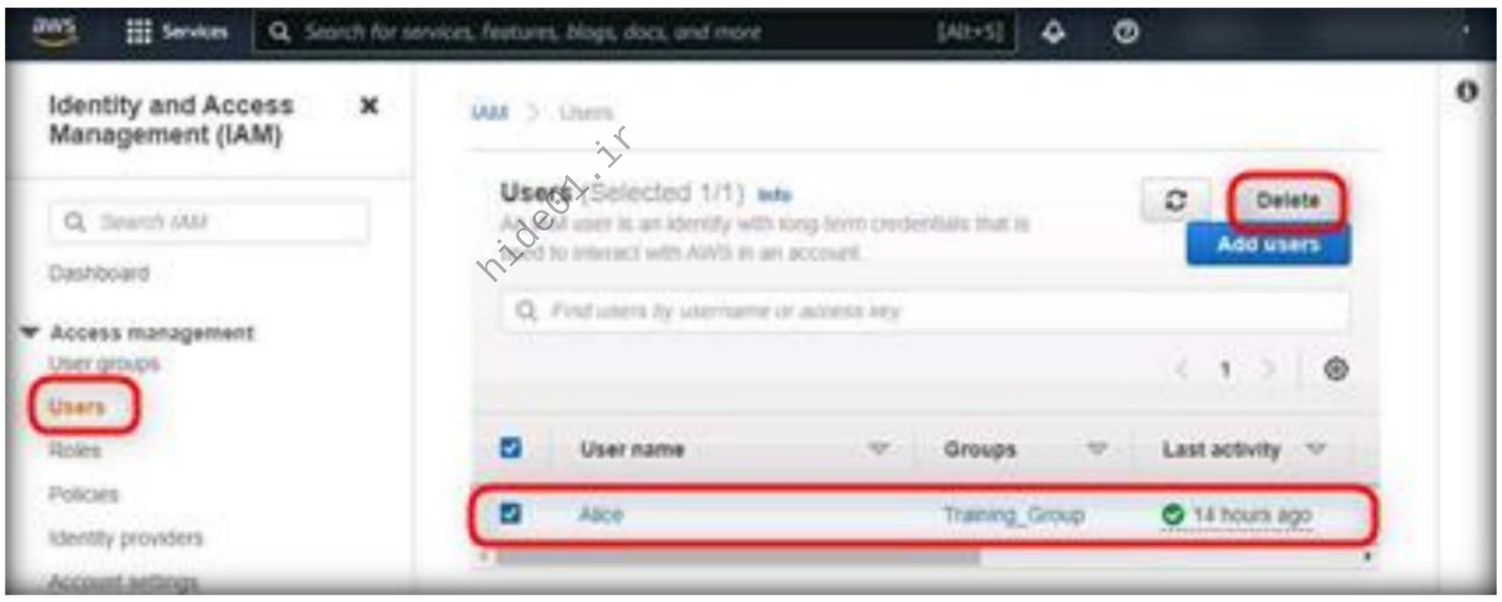


FIGURE 2.2.63: Deleting User

77. Navigate to the **User groups** tab and select the checkbox for the user group created in this lab (here, **Training_Group**). Click on the **Delete** button. In the pop-up window, enter the user group's name and click on **Delete**.



FIGURE 2.2.64: Deleting User Group

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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.

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab

3

Creating Secure EC2 Instances in AWS Virtual Private Cloud (VPC)

Amazon Virtual Private Cloud (VPC) enables cloud security engineers to create an isolated portion of the AWS cloud and launch Amazon EC2 instances that have private addresses in the range based on organizational requirements.

ICON KEY

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

Lab Scenario

With Amazon VPS, cloud security engineers can create an isolated portion of the AWS cloud and launch Amazon EC2 instances that have private addresses in the range based on organizational requirements. This lab demonstrates the creation of a VPC with public and private subnets; the instances in a private subnet cannot be addressed from the internet.

Lab Objectives

This lab will demonstrate the creation of a VPC in AWS, private and public subnets, and EC2 instances in both subnets.

In this lab, you will learn the following:

- Creating a VPC in AWS
- Creating an internet gateway and attaching it to the VPC
- Creating private and public subnets in the VPC
- Creating Route Tables, Security Groups, and Network ACLs
- Creating EC2 instances for both subnets
- Testing access to both EC2 instances

Lab Environment

To perform this lab, you need the following:

- Admin Machine VM
- Administrative privileges
- Registered AWS account

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Duration

Time: 20 minutes

Overview of AWS VPC

Amazon VPC enables cloud security engineers to create an isolated portion of the AWS cloud and launch Amazon EC2 instances that have private addresses in the range based on organizational requirements. Cloud security engineers can define subnets within their VPC by grouping similar types of instances based on the range of IP addresses and set up routing and security to control the traffic flow in and out of the subnets and instances. For a VPC with public and private subnets, the instances in the private subnet cannot be accessed from the internet. The security features in Amazon VPC include security groups, routing tables, external gateways, and network ACLs. Each of these security features is complementary to providing a secure isolated network, which can be extended by selectively enabling private connectivity to another network or direct access to the internet.

Each Amazon VPC is a discrete and isolated network within the cloud. The network traffic within an Amazon VPC is isolated from all other Amazon VPCs. Customers can select an IP address range for their Amazon VPCs during creating it. Customers can create and attach a virtual private gateway, internet gateway, or both to establish external connectivity.

Lab Tasks

ide01.ir

Note: Web applications using cloud environments may undergo frequent updates. For this lab, because we are working on a cloud-based environment, (i.e., AWS), the application interface may be updated with time. Hence, when working on an updated version of AWS, 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 AWS Free Tier account using the following link: https://aws.amazon.com/free/, in case you have already not created it for the previous lab. Once the registration is complete, perform the following task:

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

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1

Creating a VPC in AWS

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

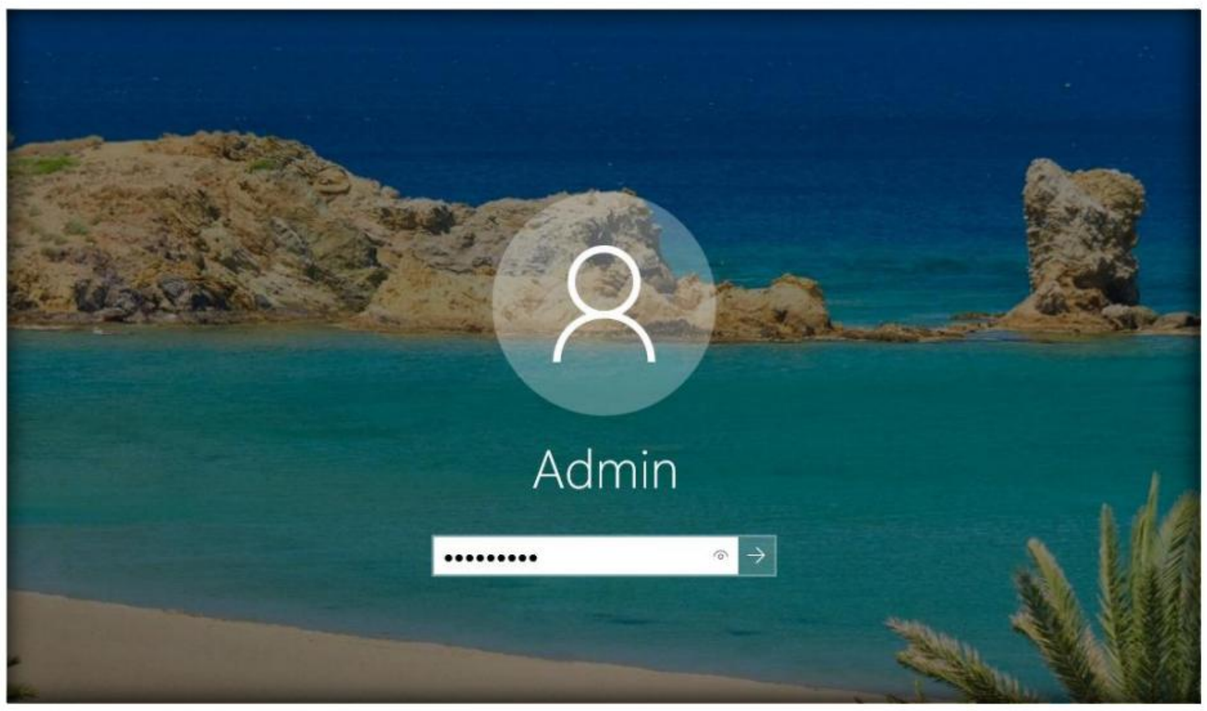


FIGURE 2.3.1: Launch Admin Machine and Log in

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

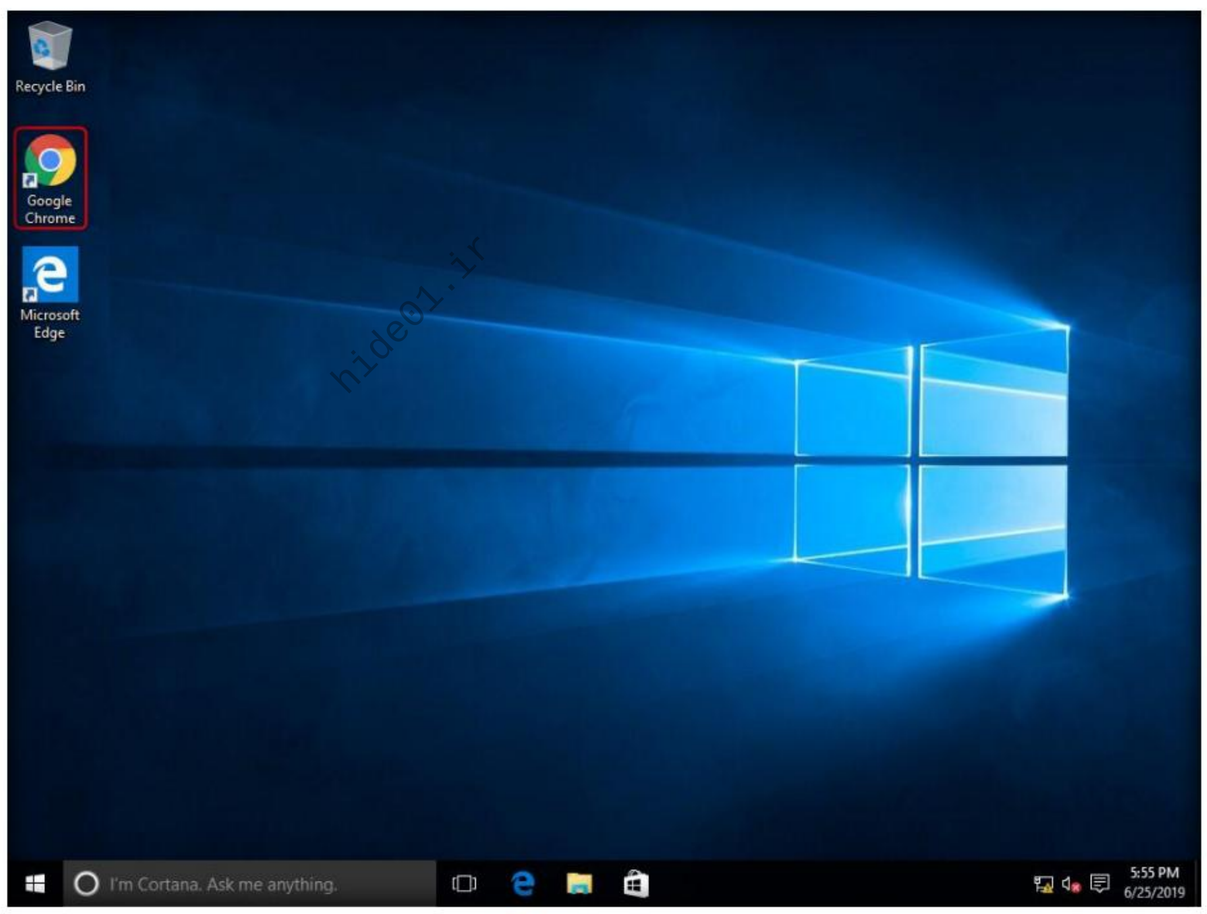


FIGURE 2.3.2: Navigating to the Chrome Browser from Taskbar

3. The **Google Chrome** browser opens. Go to the address bar, type **https://aws.amazon.com/**, and press **Enter**.

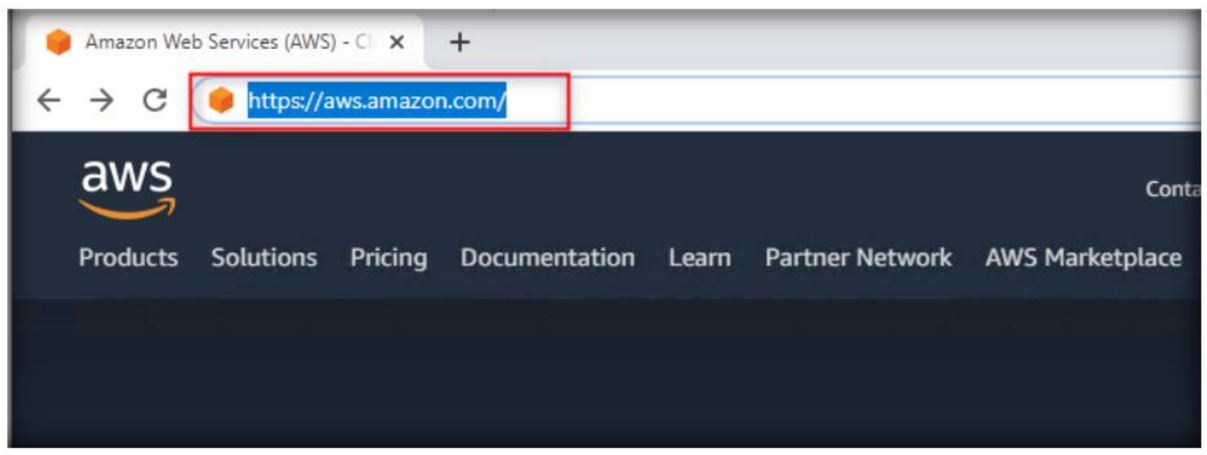


FIGURE 2.3.3: Access AWS in Browser

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

4. The **AWS Web Services - Cloud Computing Services** page appears. Click on **AWS Management Console** from the **My Account** drop-down menu, as shown in the screenshot below.

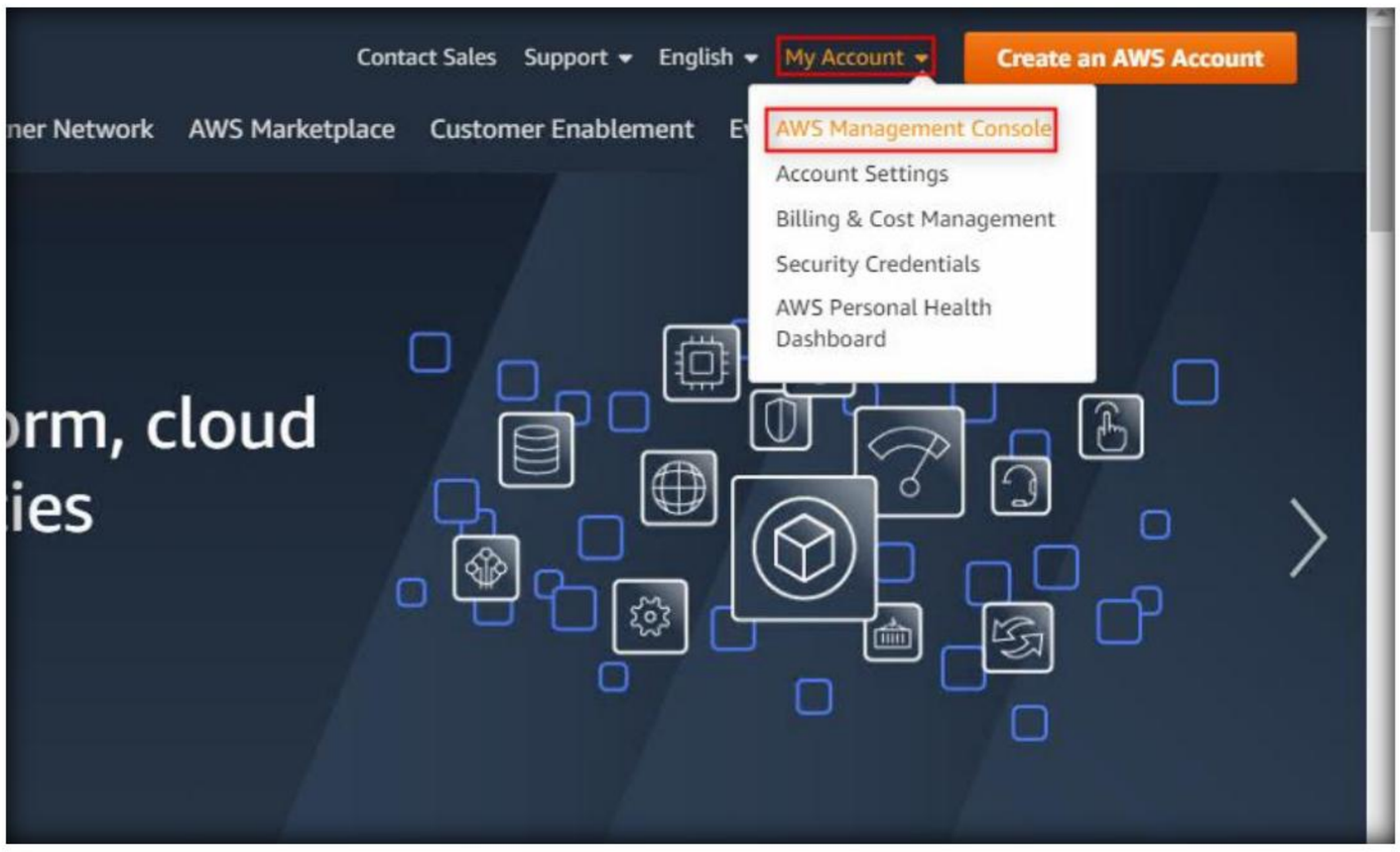


FIGURE 2.3.4: Navigate to AWS Management Console

5. The **AWS Sign-in** page appears. Select **Root user** and type the AWS administrator account ID (root user email address), as shown in the screenshot below, and click on **Next**.

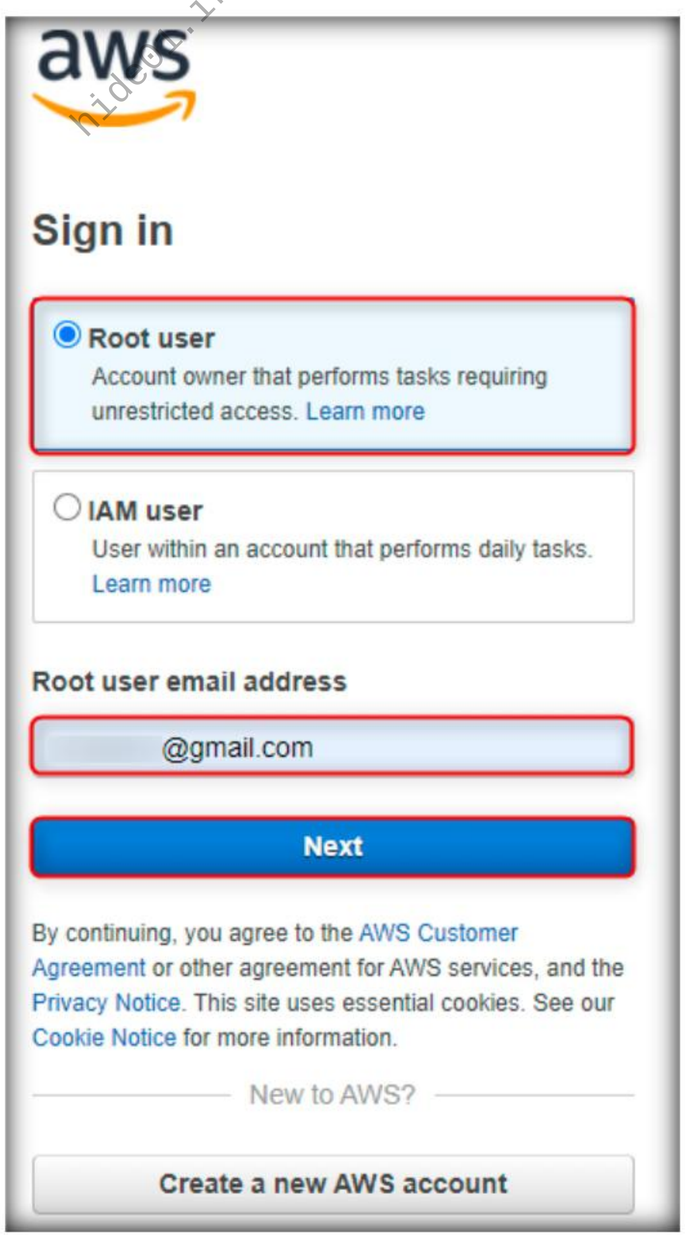


FIGURE 2.3.5: Login Credentials

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

6. Then, the security check page appears; type the characters shown in image and click on **Submit.**



FIGURE 2.3.6: Entering Security Characters

7. In the **Password** field, type the password, and click on **Sign-in,** as shown in the screenshot below.

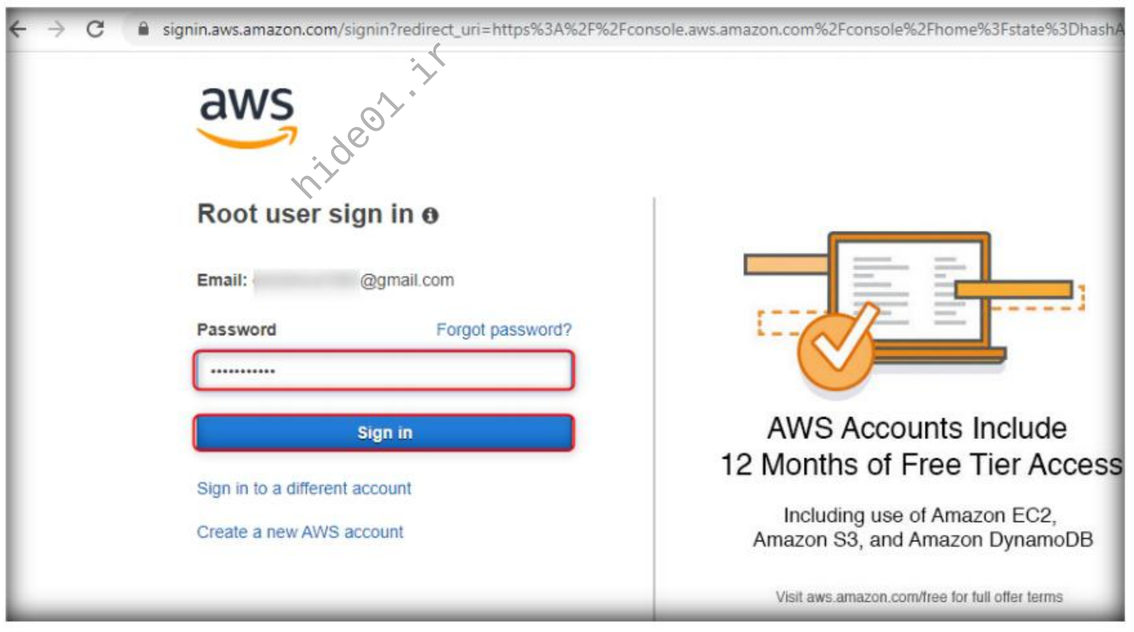


FIGURE 2.3.7: Sign-in to AWS

8. Now, to create the virtual private cloud (VPC), click on **Services** at the top of the AWS console. Search for **VPC** in the search box and click on **VPC (Isolated Cloud Resources)** from the dropdown search results.

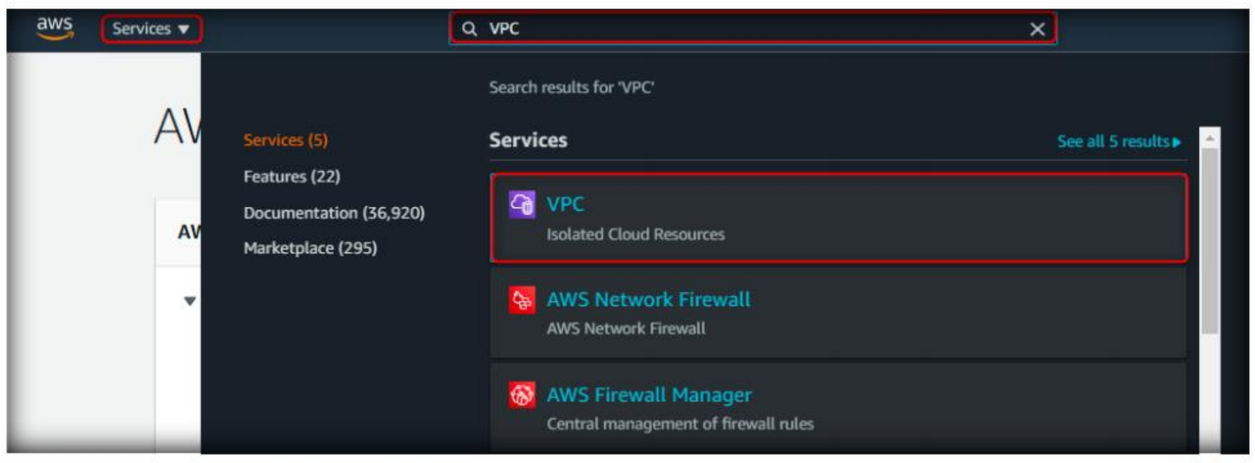


FIGURE 2.3.8: Navigate to VPC

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

9. In the **VPC Dashboard** window, click on **Your VPCs** in the left pane under **VIRTUAL PRIVATE CLOUD**.

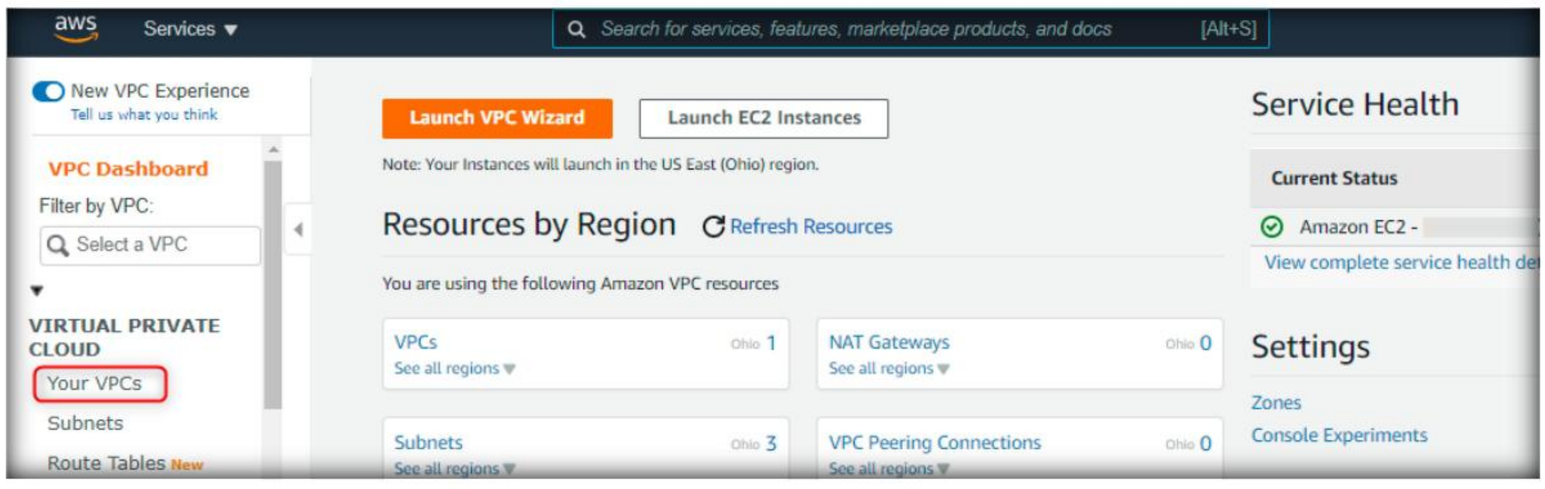


FIGURE 2.3.9: Navigate to Your VPCs

10. Now, the **Your VPCs** window appears. Click on **Create VPC** to create a VPC.

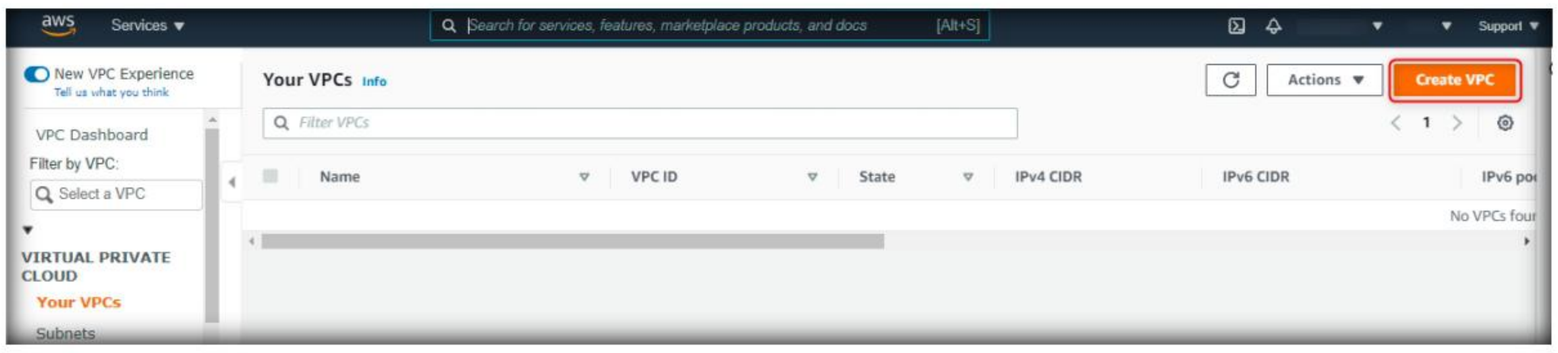


FIGURE 2.3.10: Create VPC

11. Next, in the **Create VPC** window, enter a **Name tag** (e.g., **ecc-demo-vpc**). For **IPv4 CIDR block**, enter the VPC IP address in the form of CIDR block; enter it as **10.0.0.0/16**.

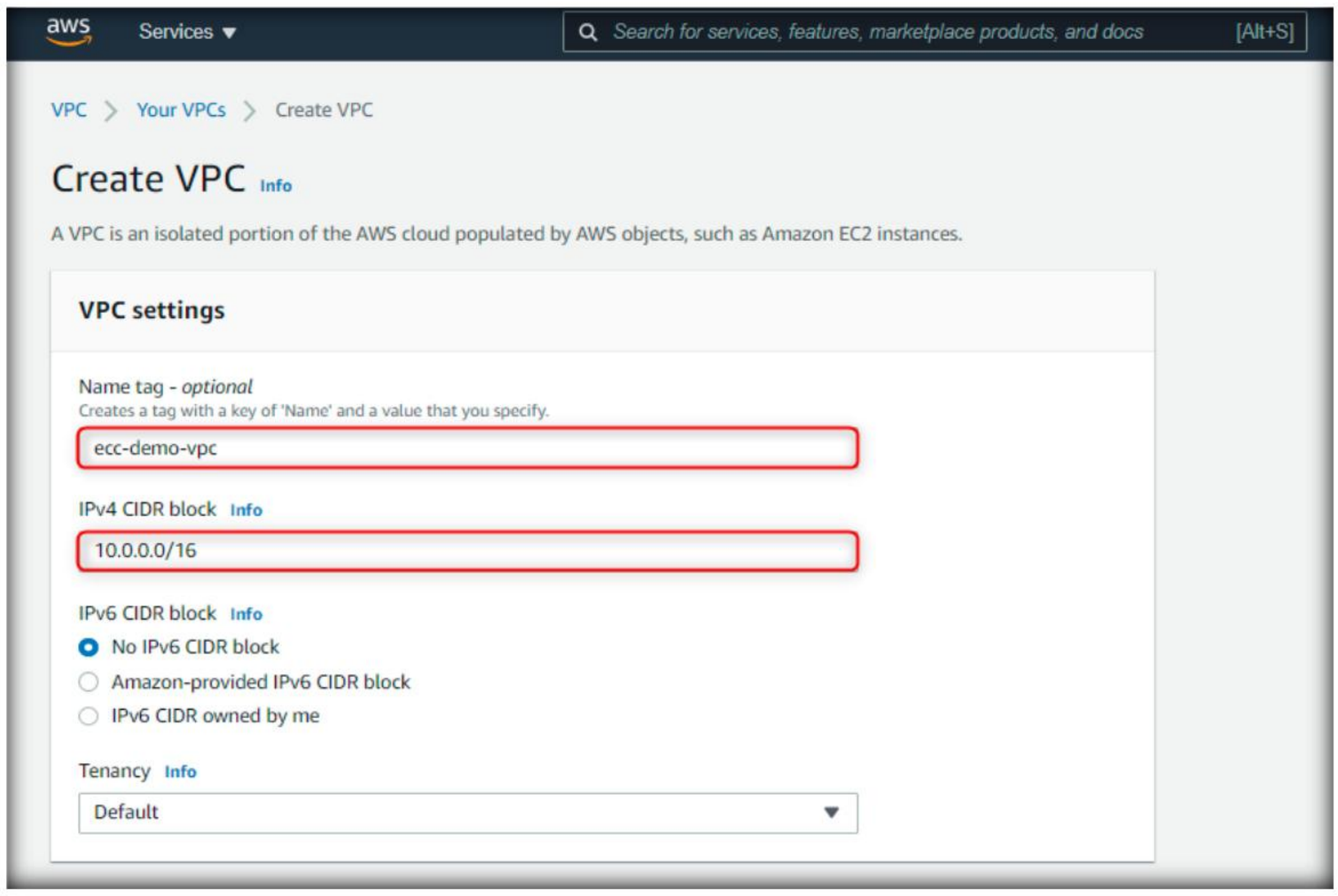


FIGURE 2.3.11: Configuring VPC

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

12. Do not change any other settings. Scroll down to the bottom and click on **Create VPC**.

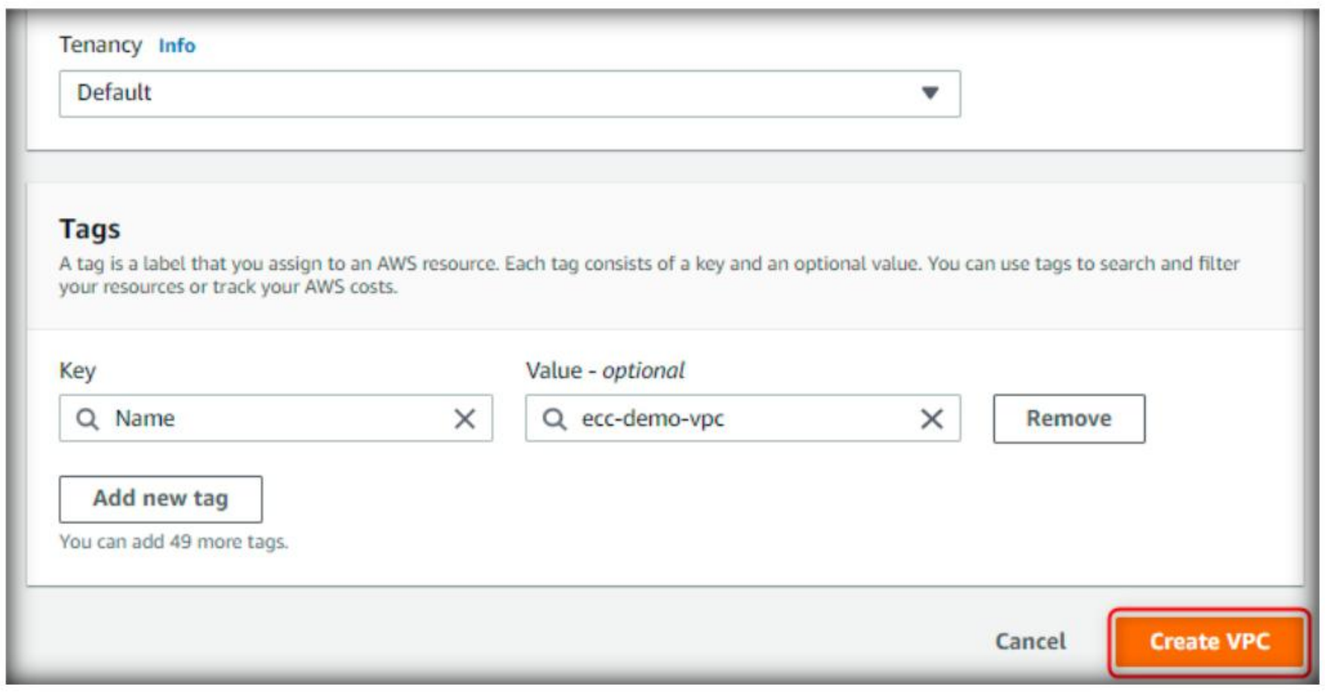
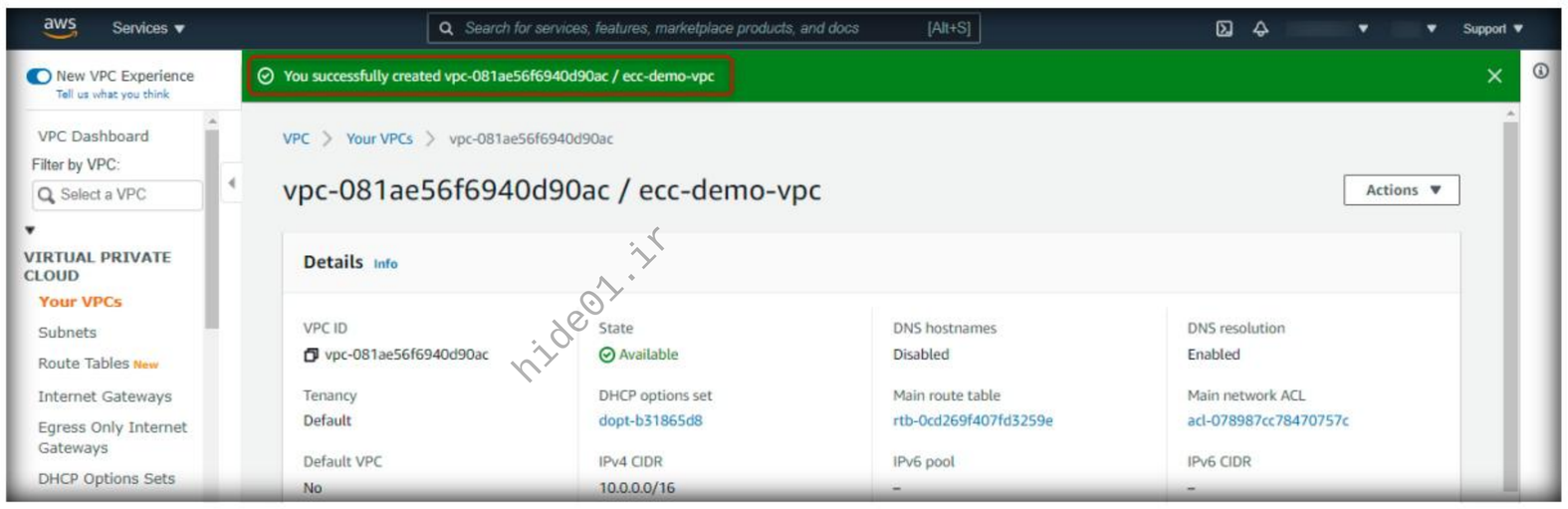


FIGURE 2.3.12: Creating VPC

13. Thus, the VPC is successfully created.

    Note: Note the **VPC ID** for future use in this lab.



hide01.ir

FIGURE 2.3.13: VPC Created Successfully

TASK 2

Creating an internet gateway and attaching it to the VPC

14. Now, you need to create an internet gateway to connect the instances in the VPC to the internet. Therefore, click on **Internet Gateways** on the left pane under **VIRTUAL PRIVATE CLOUD**.

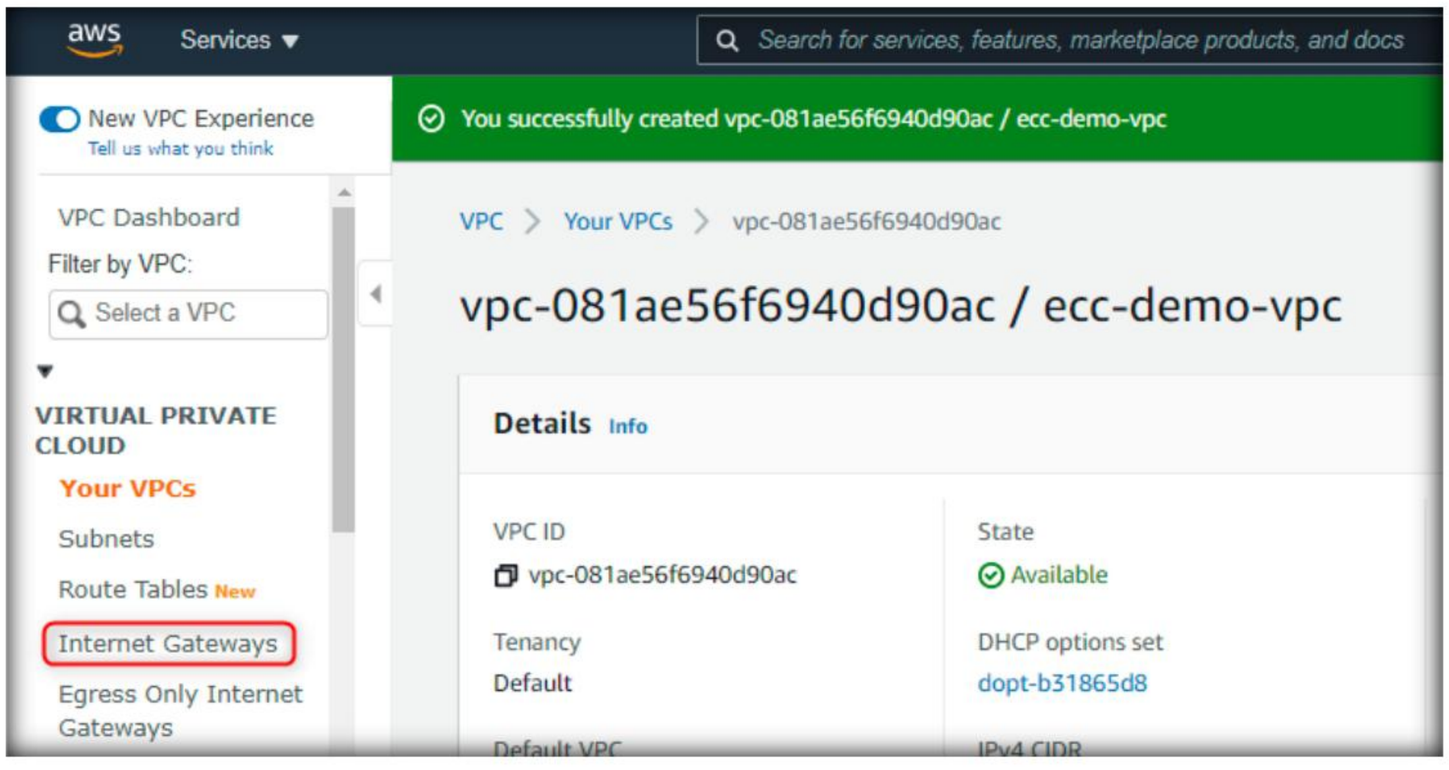


FIGURE 2.3.14: Navigating to Internet Gateways

Certified Cloud Security Engineer Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

15. Click on **Create internet gateway**.

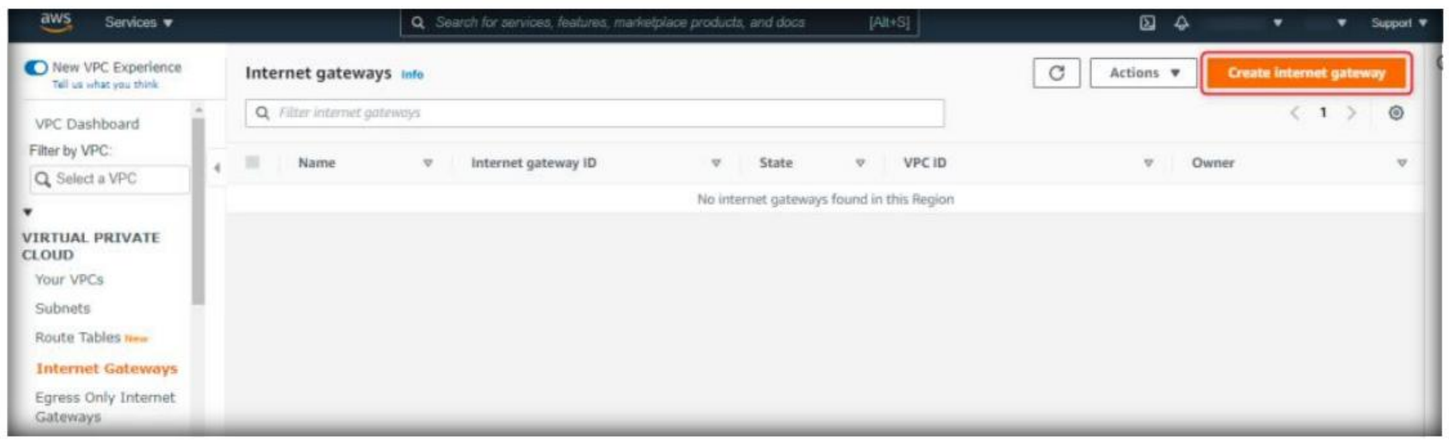
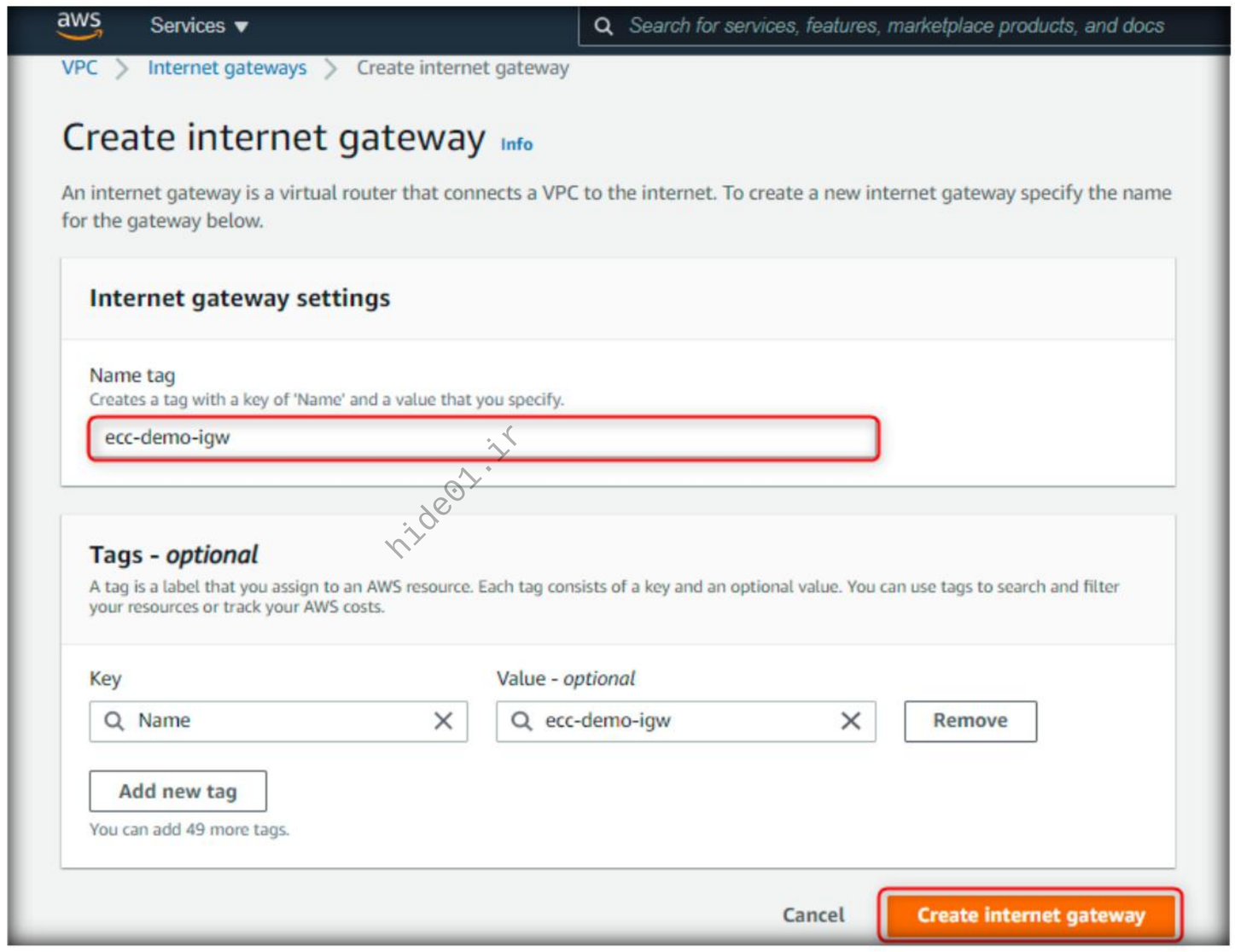


FIGURE 2.3.15: Creating Internet Gateway

16. In the **Create internet gateway** window, enter a **Name tag** (**ecc-demo-igw**) for the internet gateway. For **Tags,** do not configure any other option because it is optional. Click on **Create internet gateway.**



hide01.ir

FIGURE 2.3.16: Creating Internet Gateway

17. The internet gateway is successfully created. Now, to allow the VPC to connect to the internet, attach the internet gateway to the VPC. Click on **Attach to a VPC** in the message displayed on the top.

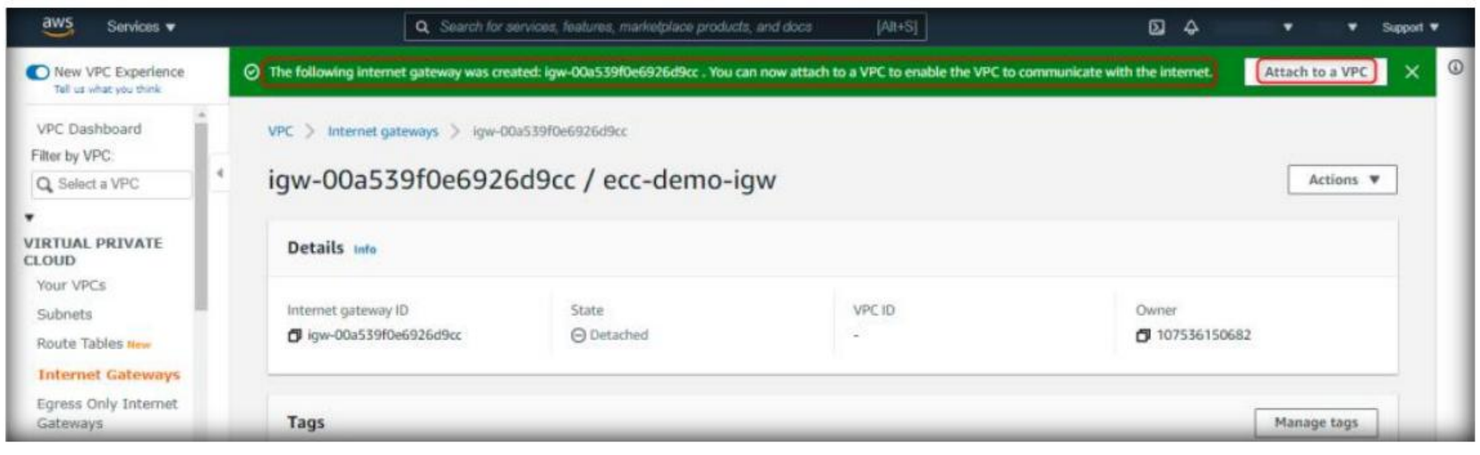


FIGURE 2.3.17: Attaching to a VPC

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

18. In the **Attach to VPC** window, select the created VPC under **Available VPCs**. Click on **Attach internet gateway.**

    Note: You will notice multiple VPCs under **Available VPCs** if other VPCs have been created, including the default VPC. Ensure that you select the VPC created by you for the purpose of this lab.

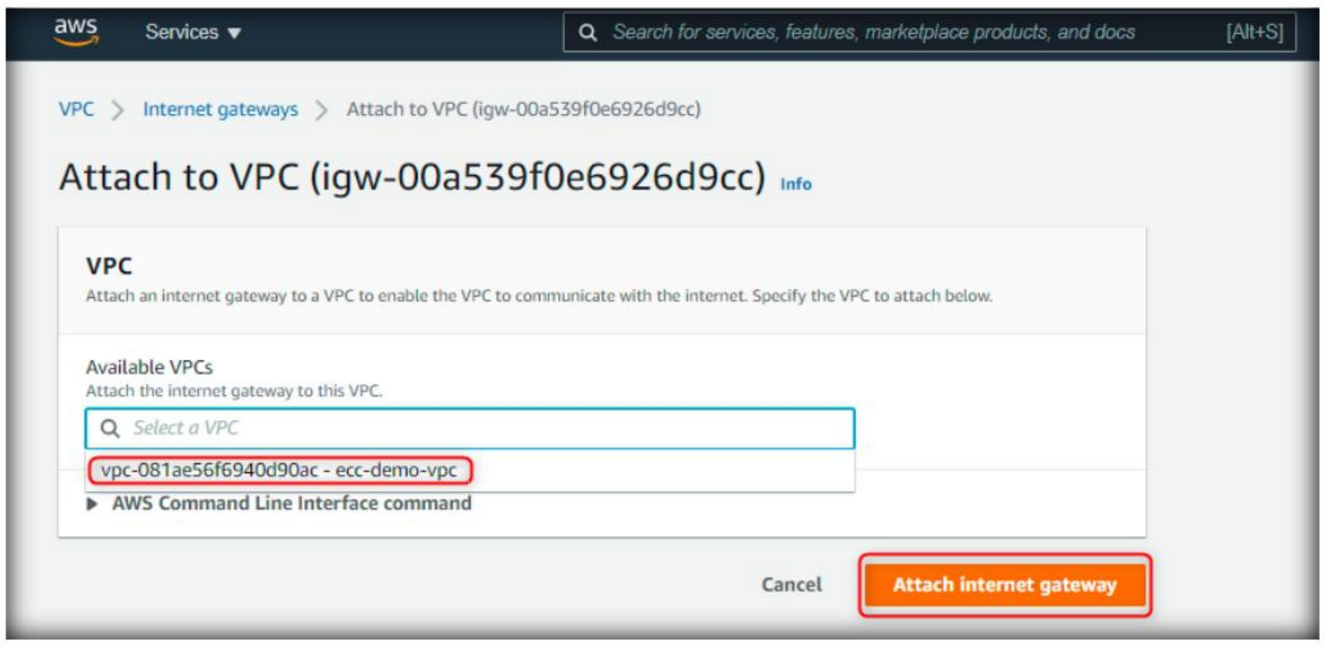
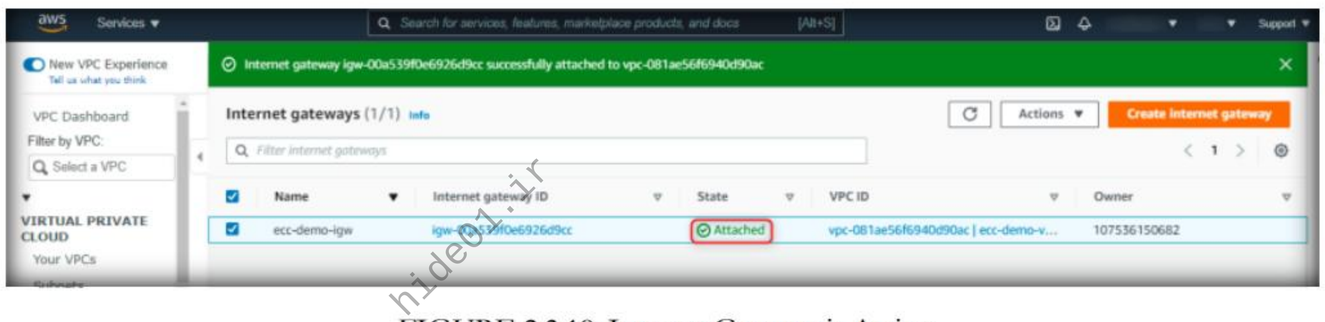


FIGURE 2.3.18: Attaching to a VPC

19. Now, the state of the internet gateway is displayed as attached.



hide01.ir

FIGURE 2.3.19: Internet Gateway is Active

TASK 3

Creating private and public subnets in the VPC

20. Next, you need to create a public and private subnet in the VPC. Public subnets are created for connectivity to the internet. Private subnets are isolated from the internet.

21. To create the subnets, click on **Subnets** below **VIRTUAL PRIVATE CLOUD** in the left pane of VPC.

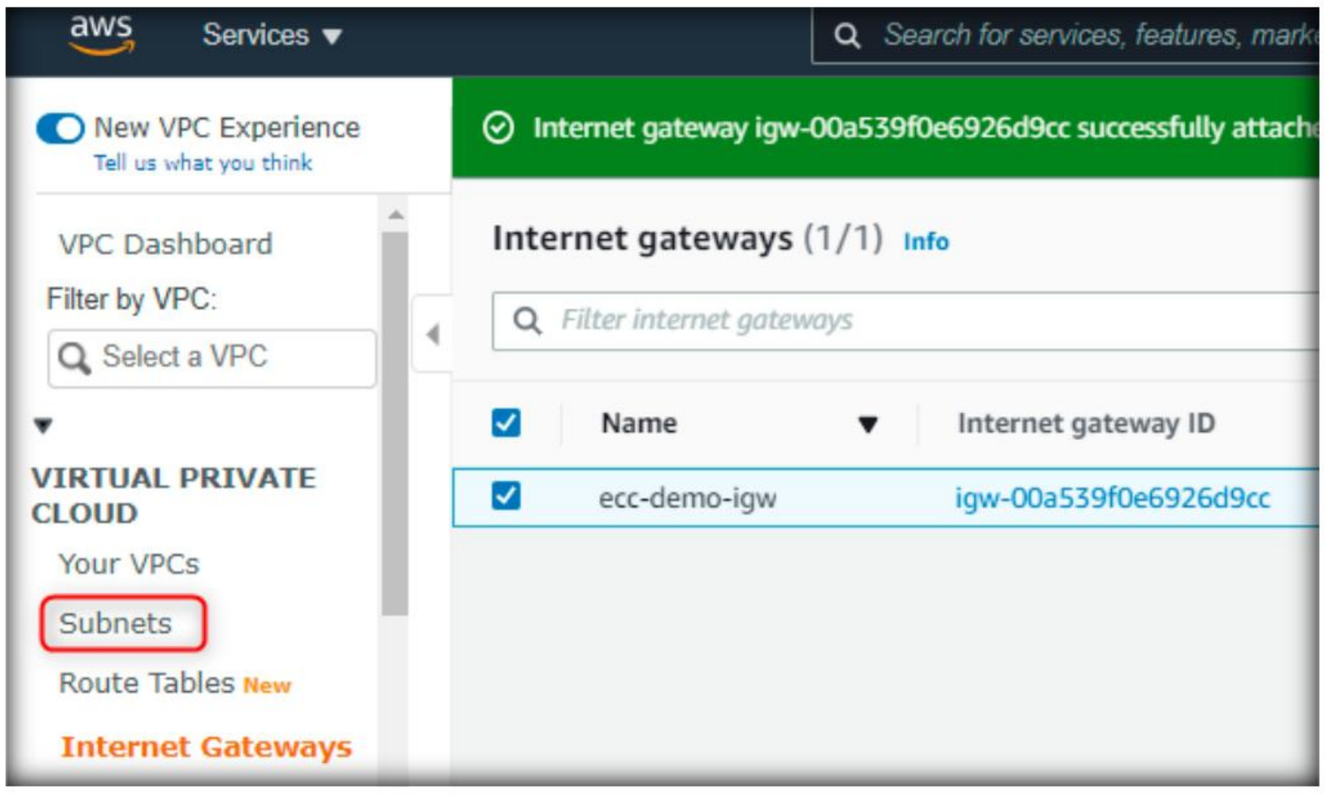


FIGURE 2.3.20: Navigating to Subnets

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

22. First, create a private subnet. Click on **Create Subnet** in the **Subnets** window.

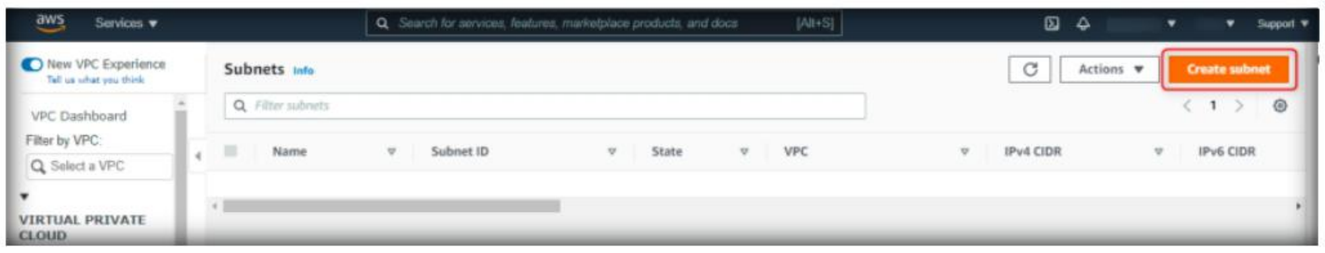


FIGURE 2.3.21: Creating Subnets

23. In the **Create subnet** window, under **VPC ID**, click on the dropdown for **Select a VPC**. Select the VPC (**ecc-demo-vpc**) created by you for this lab.

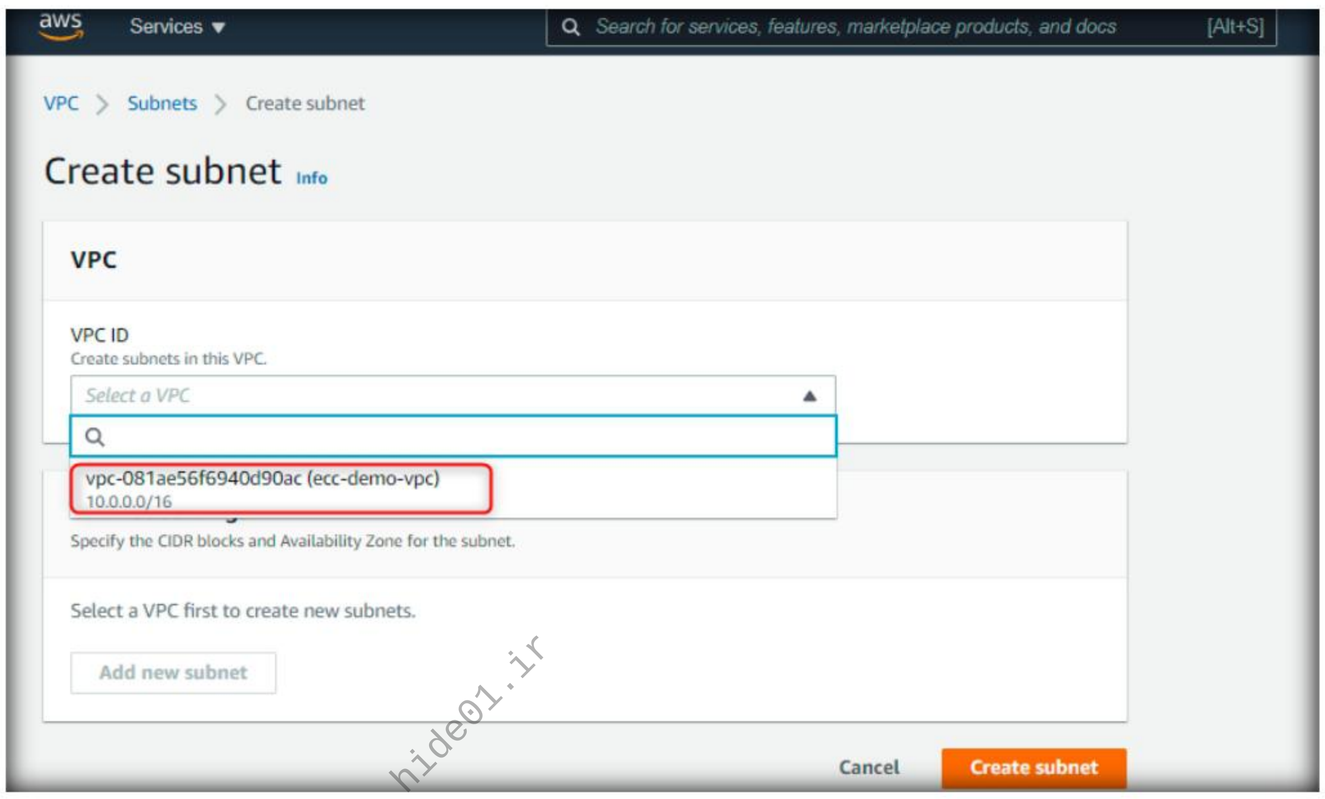


FIGURE 2.3.22: Selecting VPC

24. Scroll down to the bottom. Enter a **Subnet name** for the private subnet (ecc-private-subnet). For **IPv4 CIDR block,** enter the IP range (e.g., **10.0.1.0/24**) for the subnet.

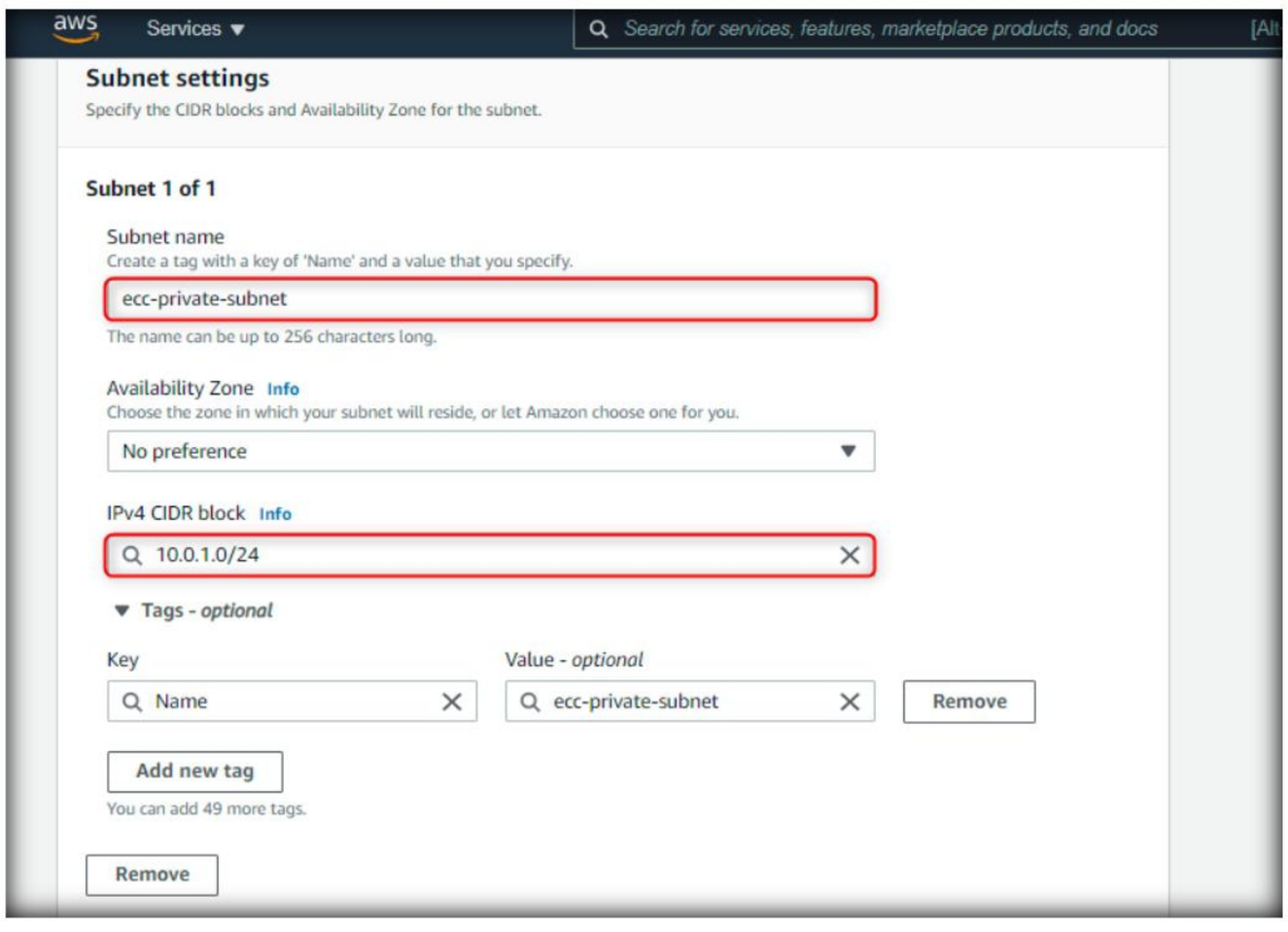


FIGURE 2.3.23: Configuring Subnet

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

25. Scroll down without changing other settings and click on **Create subnet**.

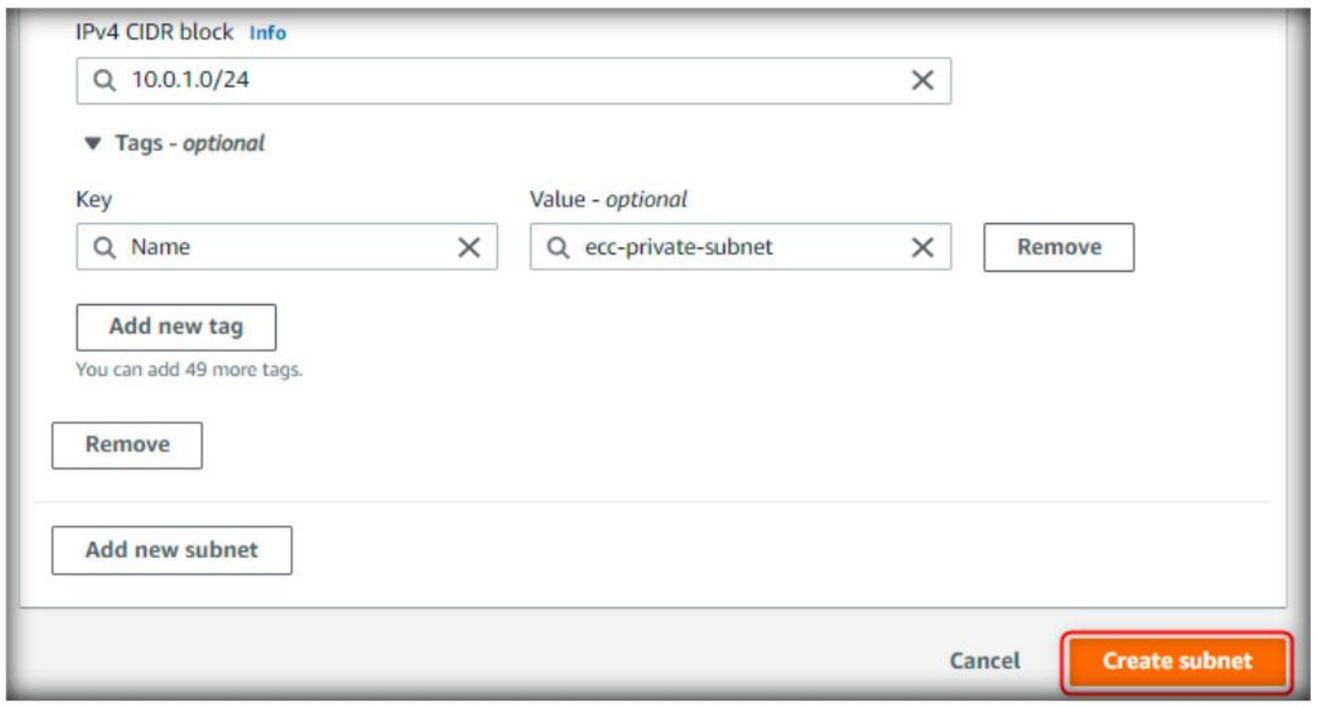


FIGURE 2.3.24: Creating Subnet

26. Thus, a private subnet is created. Now, to create a public subnet, click on **Create subnet.**

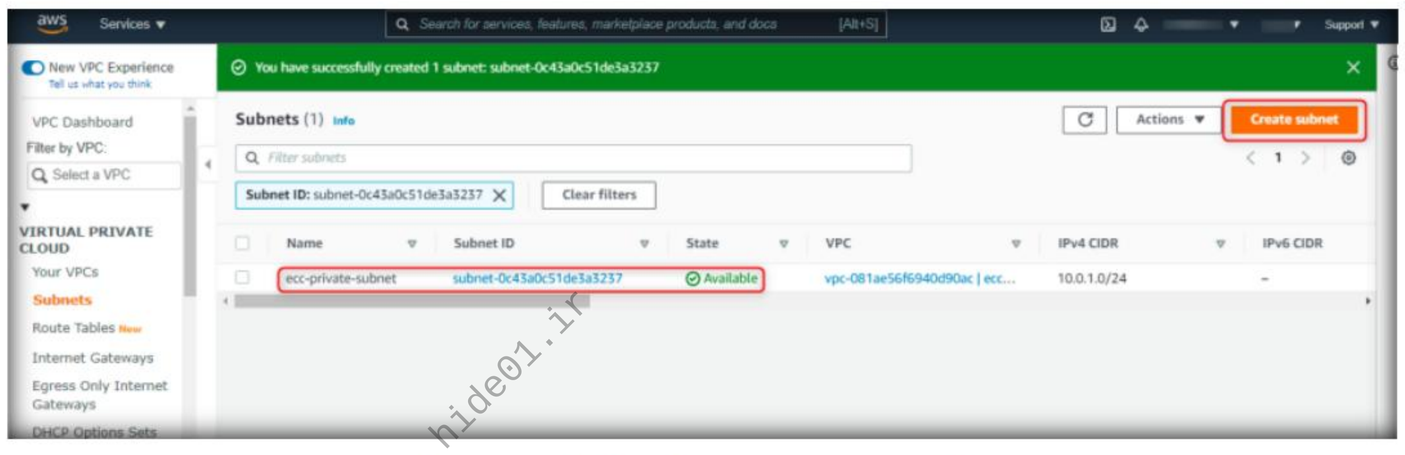


FIGURE 2.3.25: Subnet Created Successfully

27. In the **Create subnet** window under **VPC ID**, click on the dropdown for **Select a VPC**. Select the VPC (**ecc-demo-vpc**) created by you.

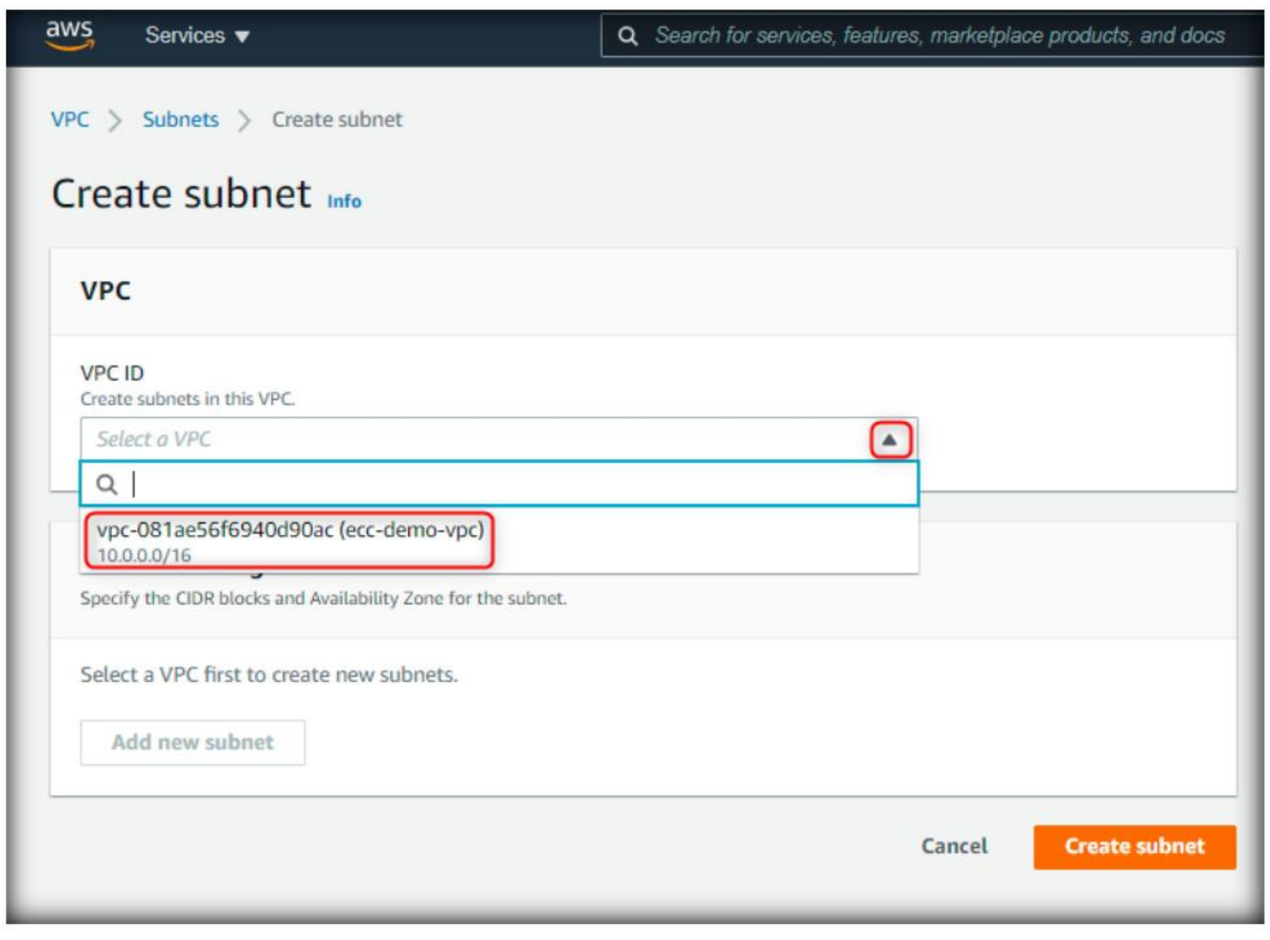


FIGURE 2.3.26: Selecting VPC for Next Subnet

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

28. Scroll down and enter a name (**ecc-public-subnet**) under **Subnet name**. For **IPv4 CIDR block**, enter an IP address range (**10.0.2.0/24**) for the subnet.

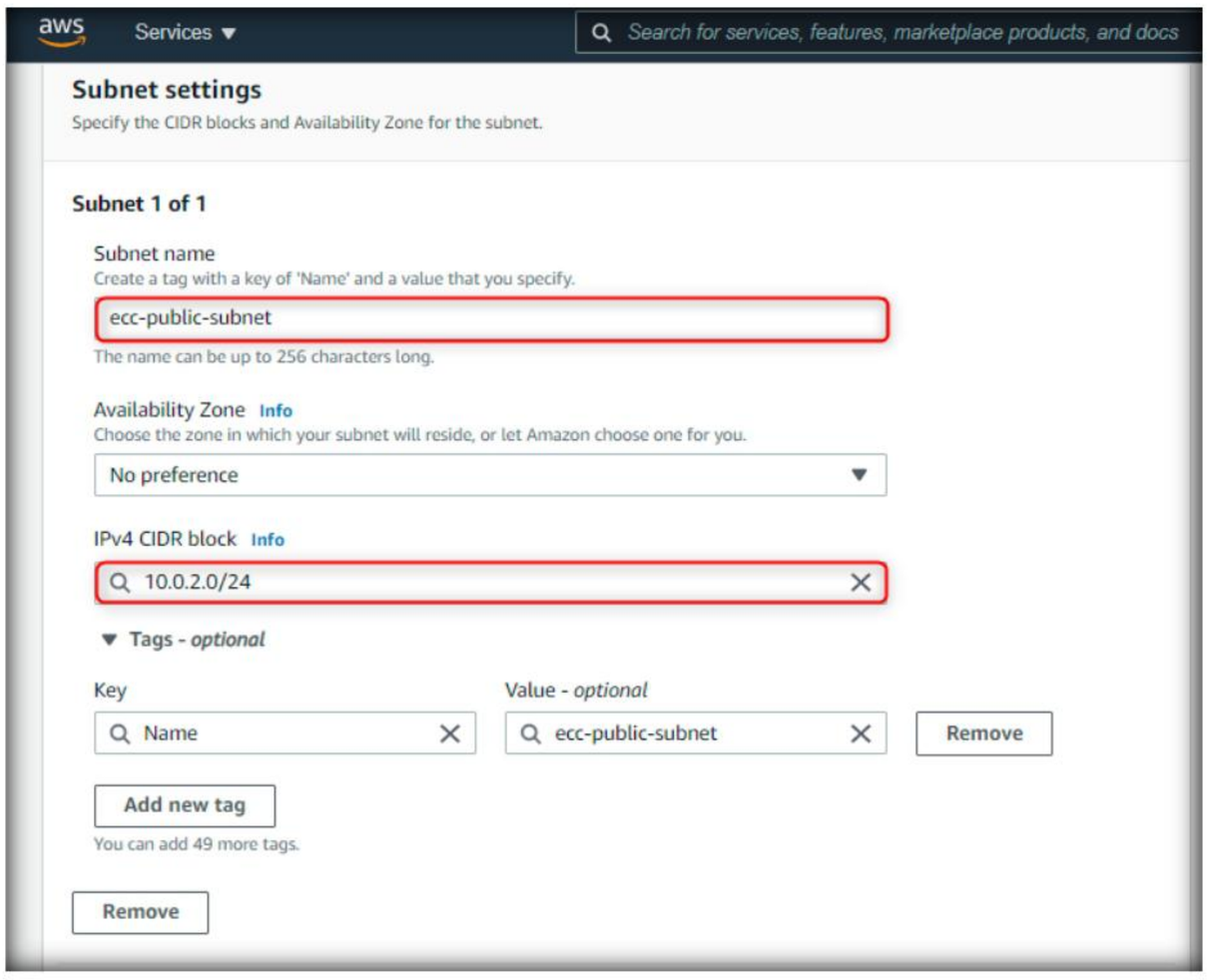
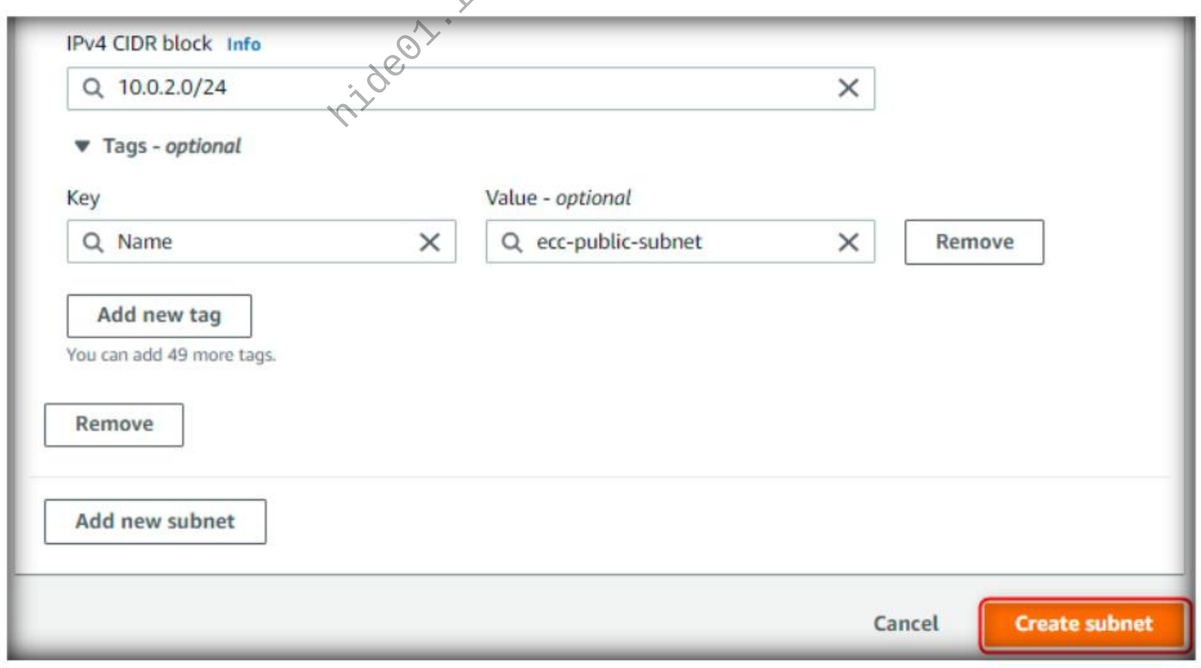


FIGURE 2.3.27: Configuring the Subnet

29. Scroll down, do not change other settings, and click on **Create subnet**.



hide01.ir

FIGURE 2.3.28: Creating the Subnet

30. Thus, two subnets for private and public access are successfully created.

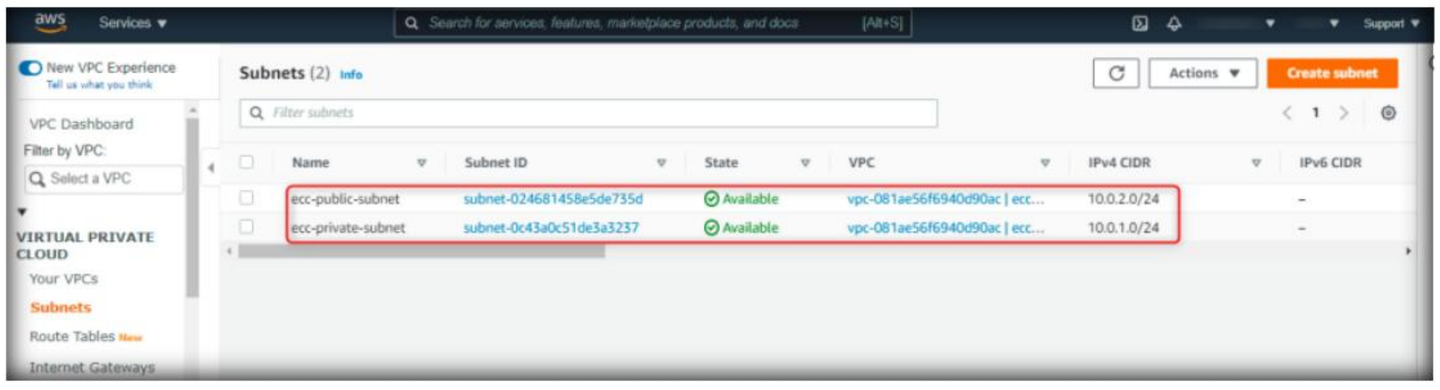


FIGURE 2.3.29: Subnets Created Successfully

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 4

Creating Route tables, Security Groups, and Network ACLs

31. Next, you need to create route tables to route the network traffic for subnets based on private and public routing.
32. To create route tables, click on **Route Tables** in the left pane under **VIRTUAL PRIVATE CLOUD**.

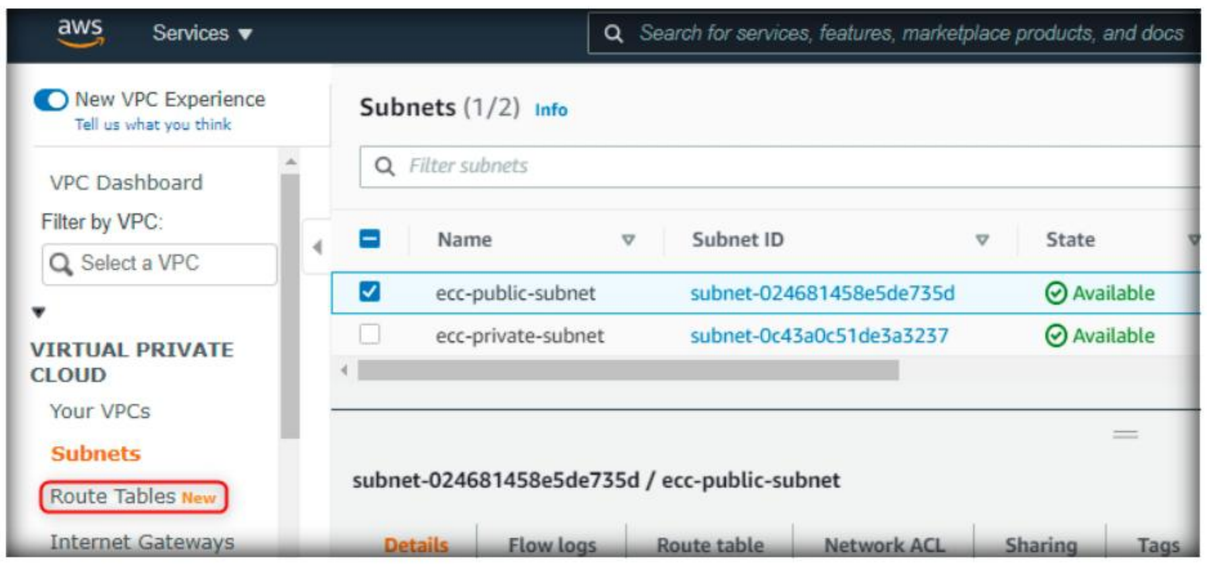


FIGURE 2.3.30: Navigating to Route Table

33. It can be observed that by default, a route table is created and attached to the VPC.

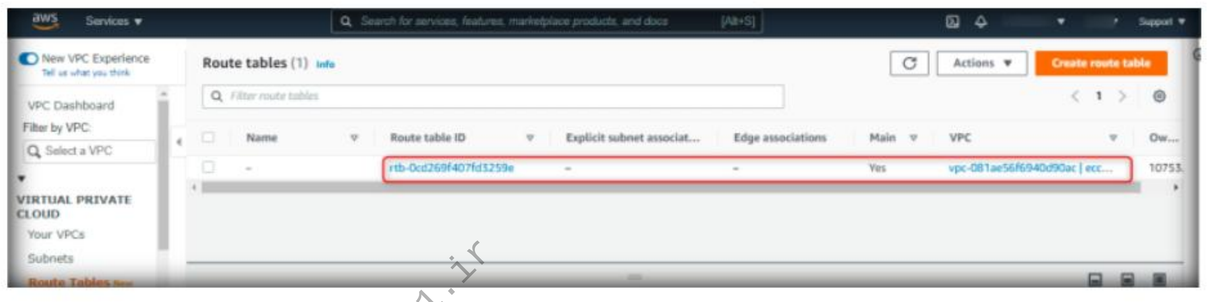


FIGURE 2.3.31: Default Route Table

34. You can edit the tag name of the default route table and add the internet gateway and private subnet to it. For that, click on the edit icon under the **Name** of the default route table. Enter a name (**eccprivate-RT**) for the route table for the private subnet. Click on **Save**.

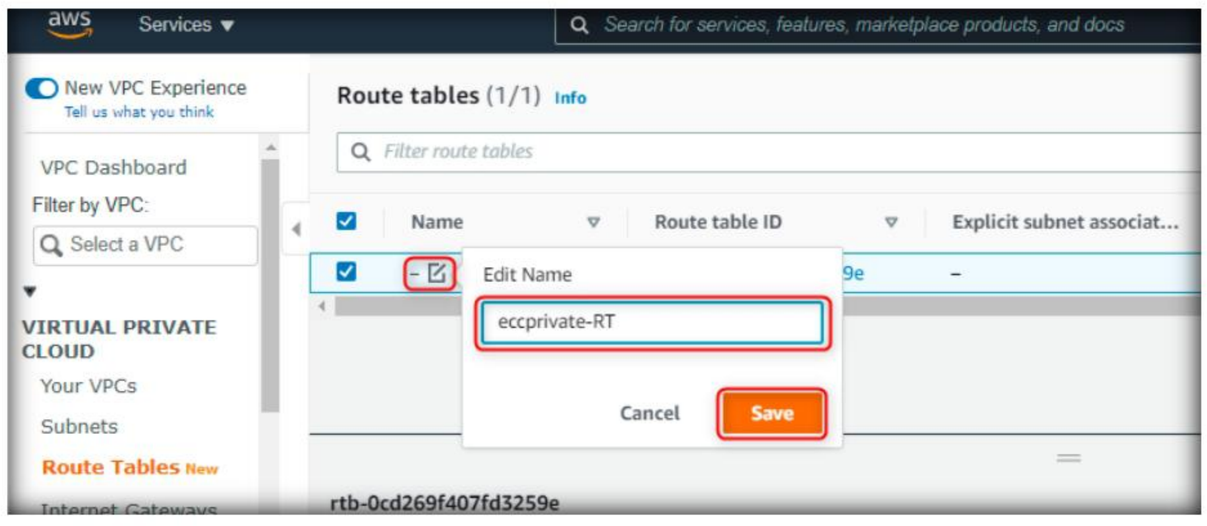


FIGURE 2.3.32: Editing the Route Table Name

35. To create a route table for the public subnet, click on **Create route table**.

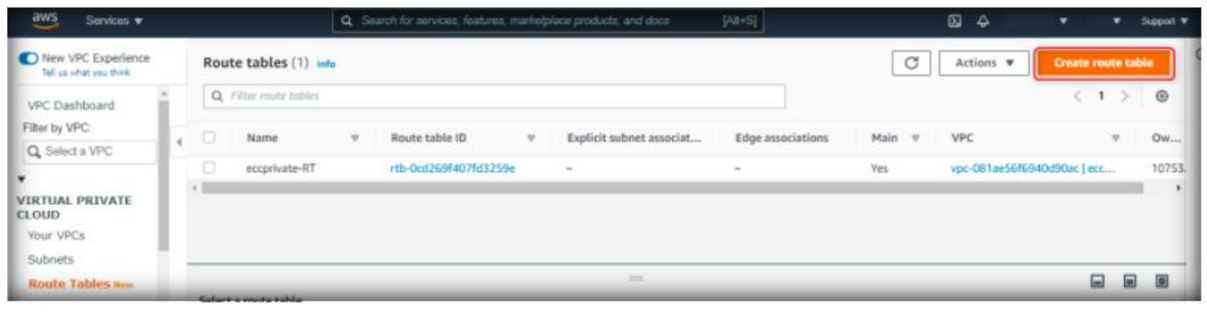


FIGURE 2.3.33: Creating Next Route Table

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

36. In the **Create route table** window, enter a **Name** (**eccpublic-RT**). Under **VPC**, select the VPC (**ecc-demo-vpc**) created by you from the dropdown. Click on **Create route table.**

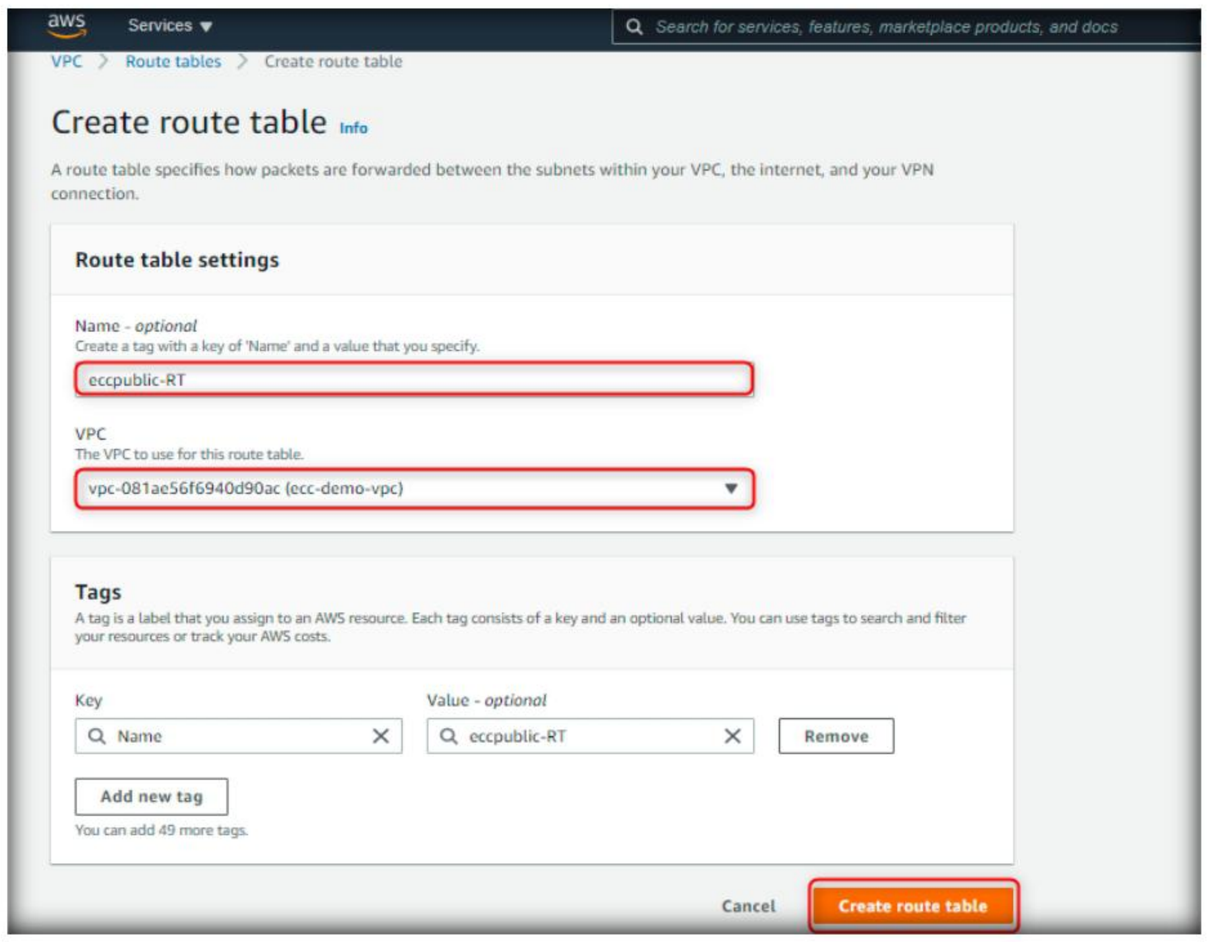


FIGURE 2.3.34: Configuring Route Table

37. Thus, the route table for the public subnet is created successfully. Click on **Route tables** to go back to the route tables window.

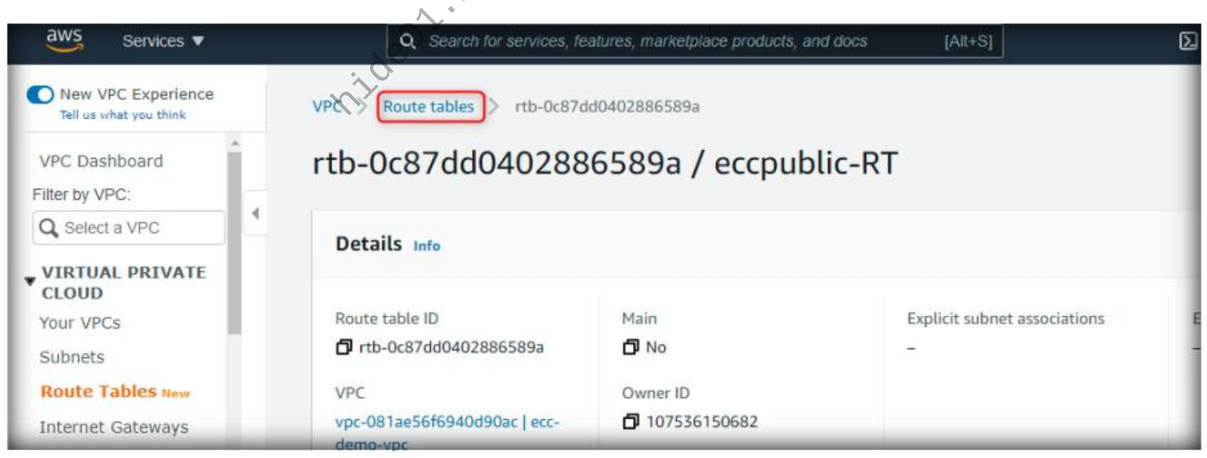


FIGURE 2.3.35: Navigating back to Route Table Window

38. Now, to configure the public route table (**eccpublic-RT**) as public, add the public subnet and internet gateway. Accordingly, select the checkbox for the public route table (**eccpublic-RT**) and click on the **Routes** tab at the bottom.

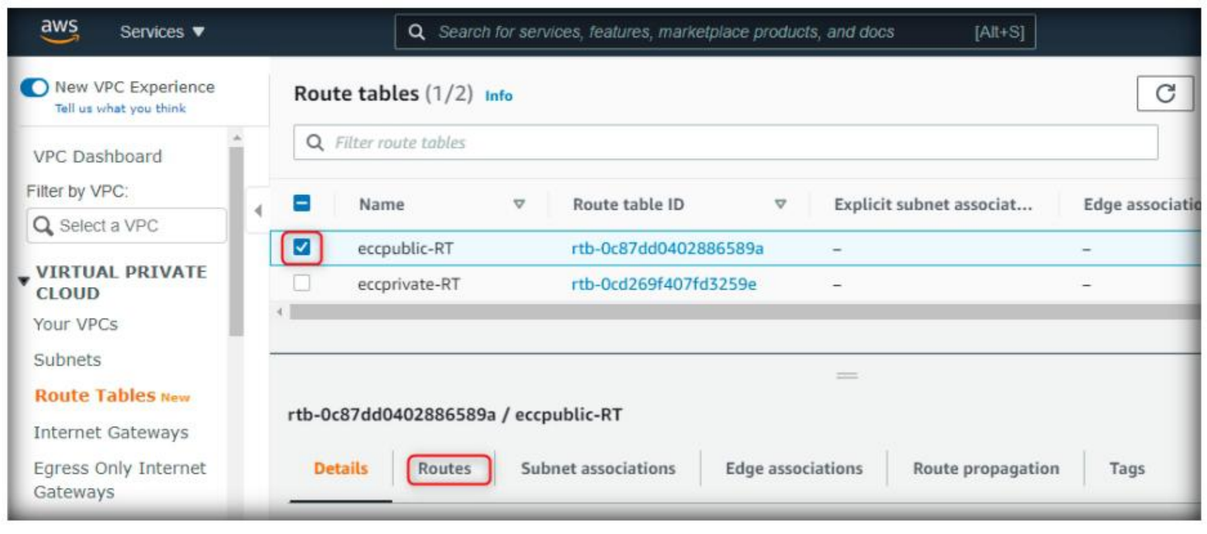


FIGURE 2.3.36: Adding Routes for the Public Subnet

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

39. Click on **Edit routes**.

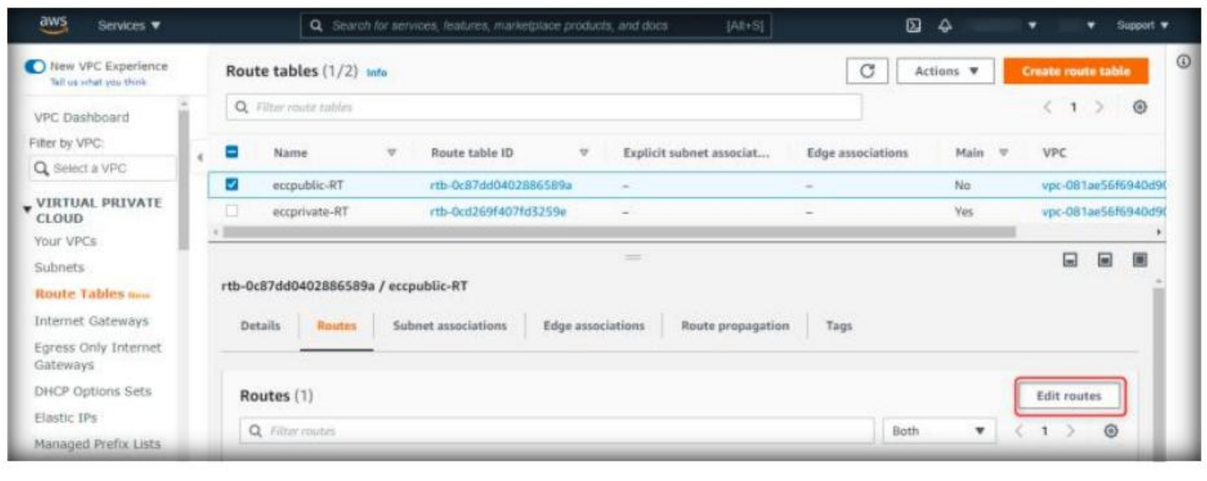


FIGURE 2.3.37: Editing routes

40. Click on **Add route.**

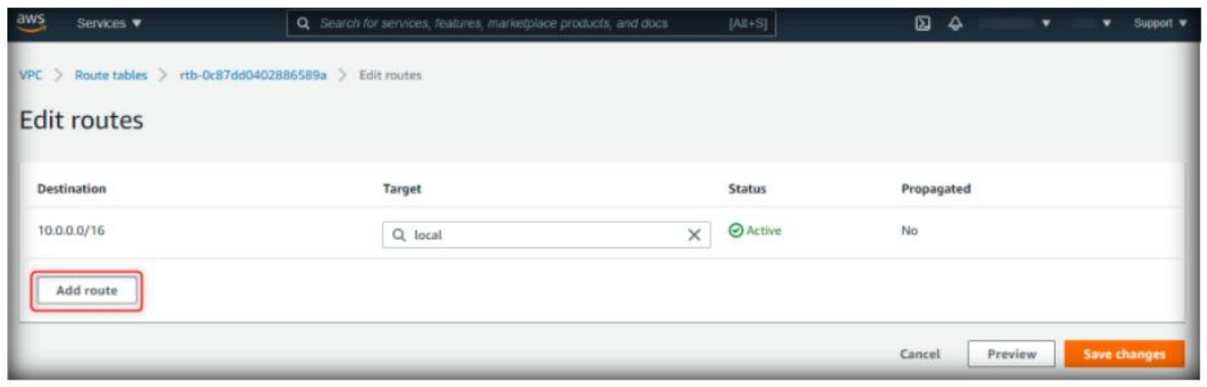


FIGURE 2.3.38: Adding Routes

41. Next, in the **Edit routes** window, for **Destination,** to allow traffic from any IP, enter the IP **0.0.0.0/0**. For **Target**, select **Internet Gateway** from the dropdown.

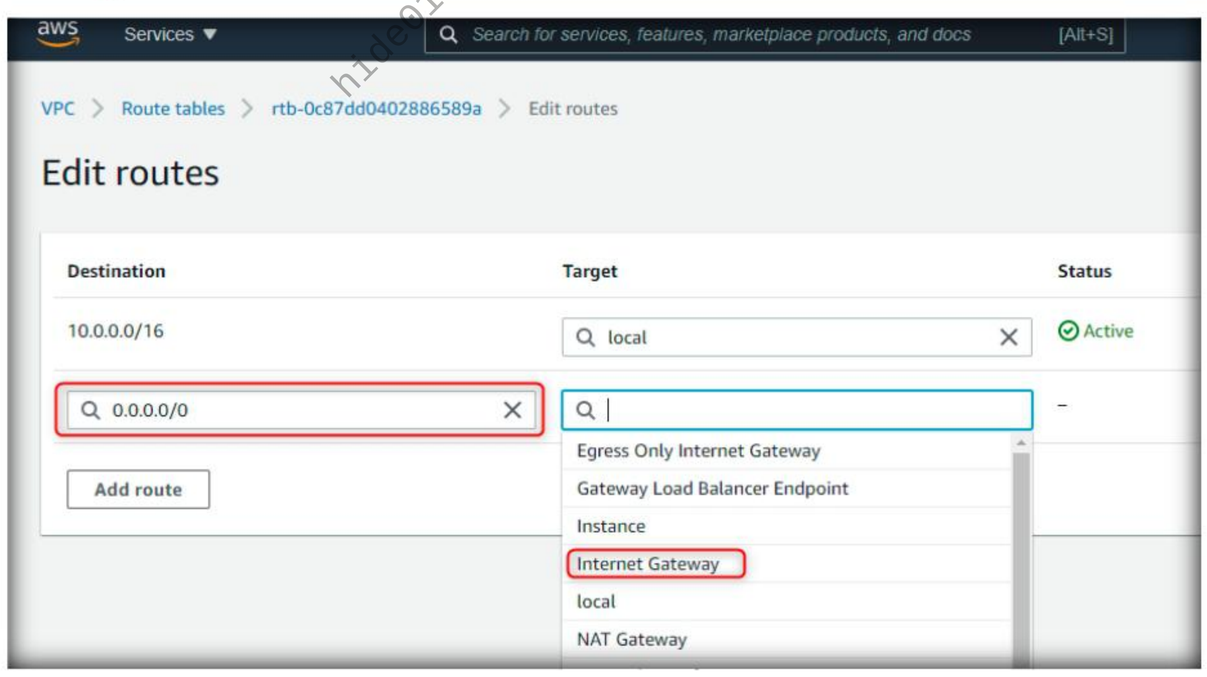


FIGURE 2.3.39: Adding Internet Gateway

42. Select the internet gateway (**ecc-demo-igw**) created by you from the next dropdown starting with **igw-***.** Click on **Save changes.**

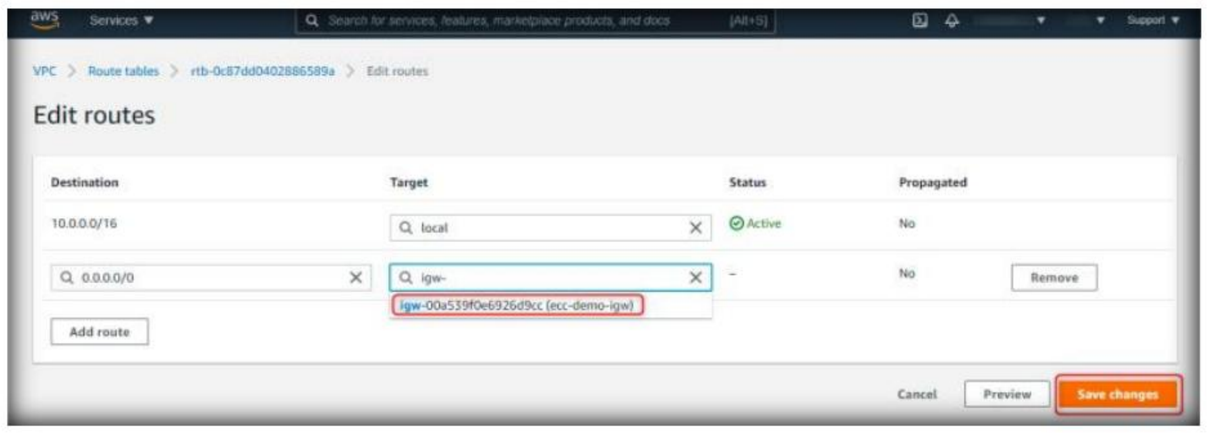


FIGURE 2.3.40: Selecting Internet Gateway

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

43. Thus, the routes for the public subnet are updated successfully. Click on **Route tables** to go back to the route table window.

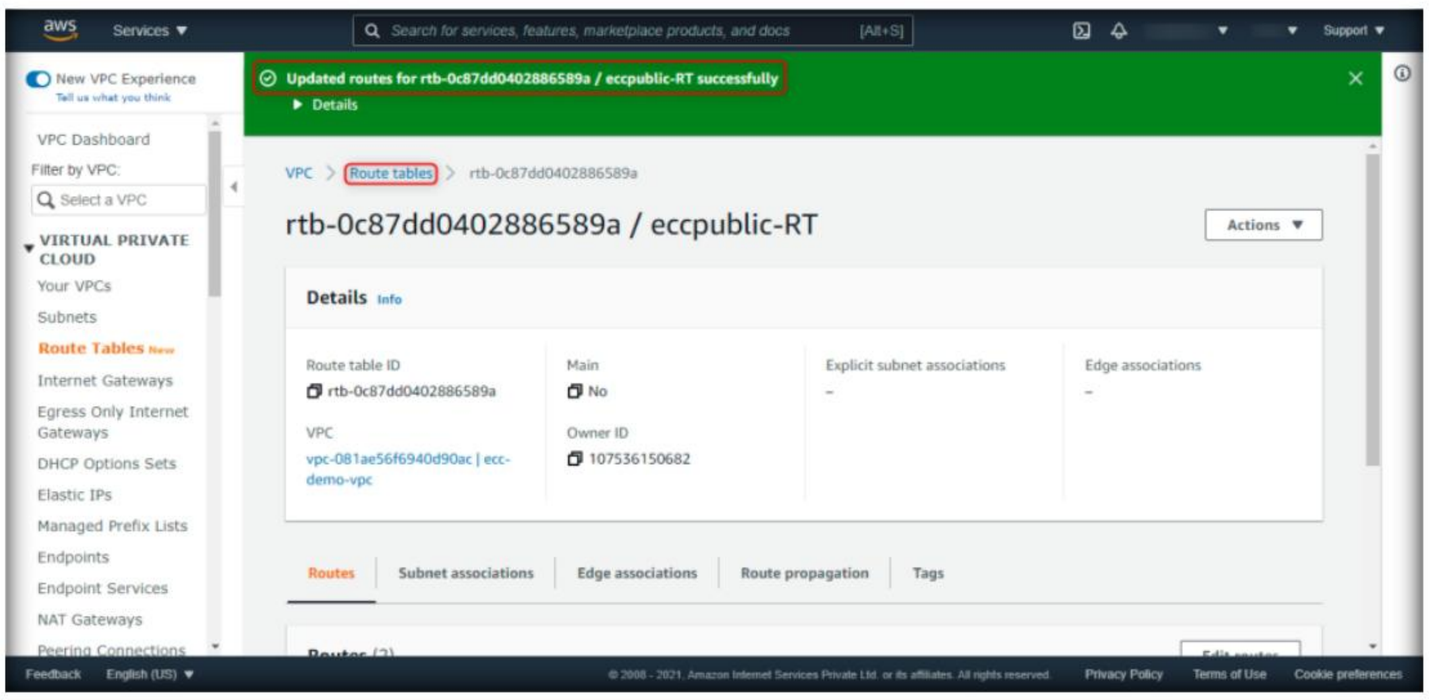


FIGURE 2.3.41: Routes Updated

44. Now, to add the subnet for the public route table, click on **Subnet associations,** followed by **Edit subnet associations**.

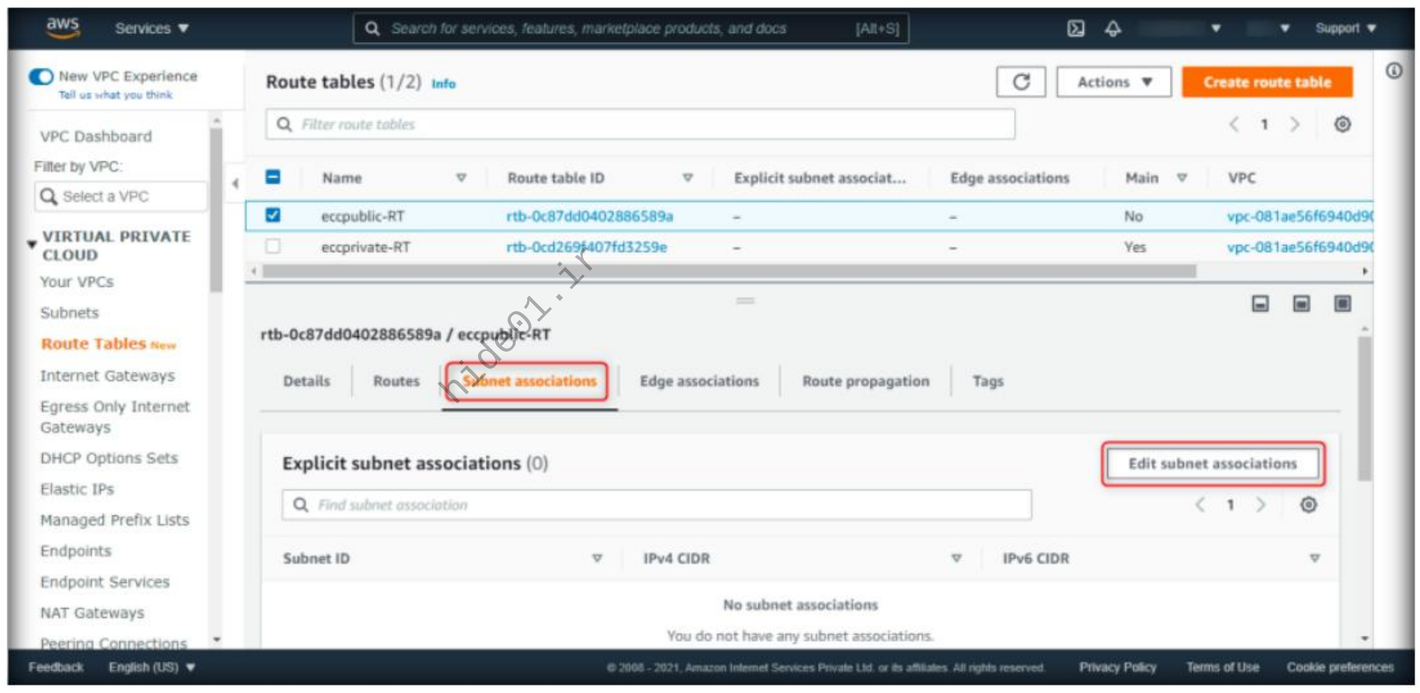


FIGURE 2.3.42: Adding Subnet

45. Select the checkbox for the public subnet (**ecc-public-subnet**). Click on **Save associations.**

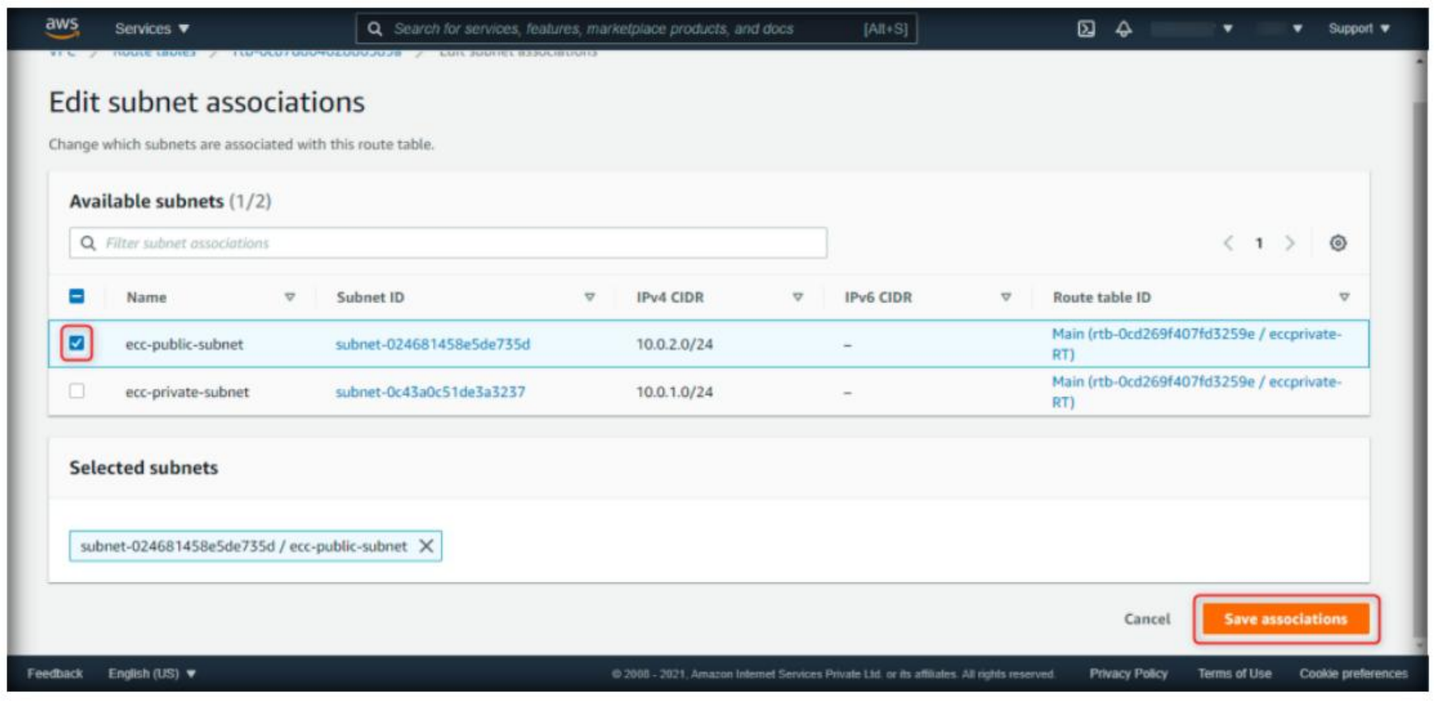


FIGURE 2.3.43: Adding Subnet

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

46. Thus, the subnet for the public route table is added successfully.

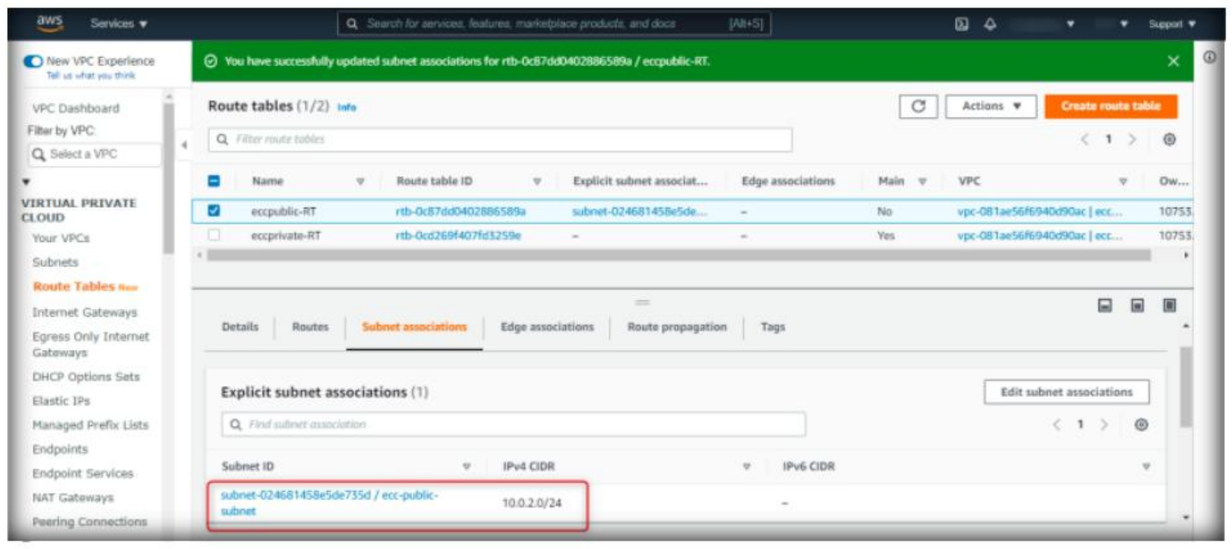


FIGURE 2.3.44: Subnet Added

47. Now, to add the subnet for the private route table, select the checkbox for the private route table (**eccprivate-RT**). Click on **Subnet associations**.

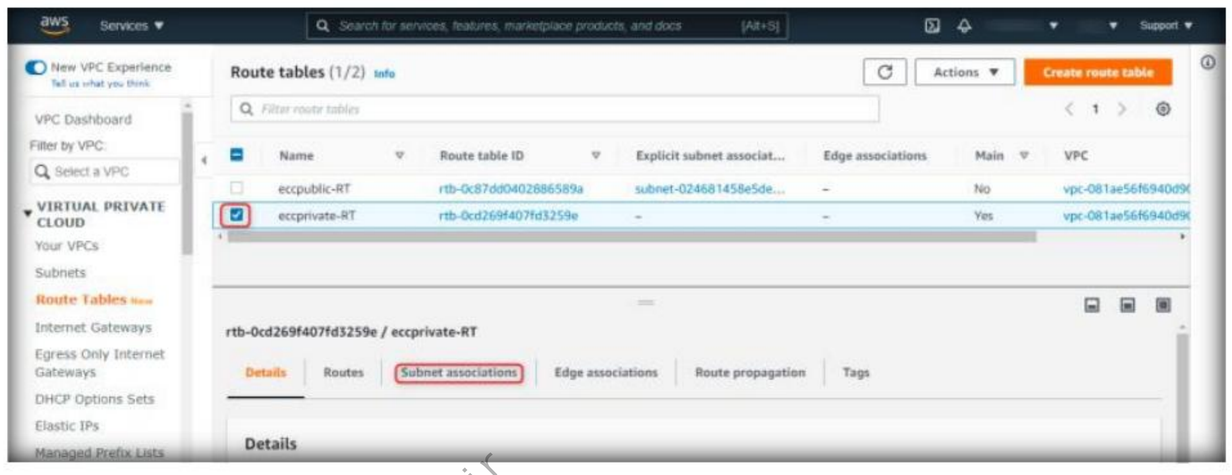


FIGURE 2.3.45: Adding Subnet

48. Click on **Edit subnet associations**.

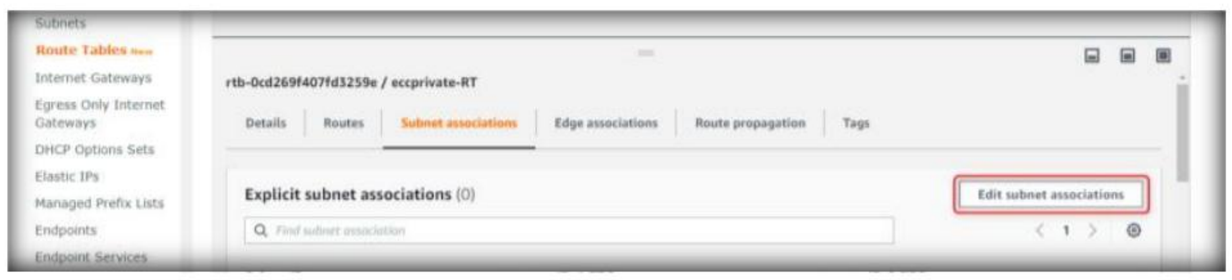


FIGURE 2.3.46: Editing Subnet Associations

49. Select the checkbox for the private subnet (**ecc-private-subnet**) and click on **Save associations**.

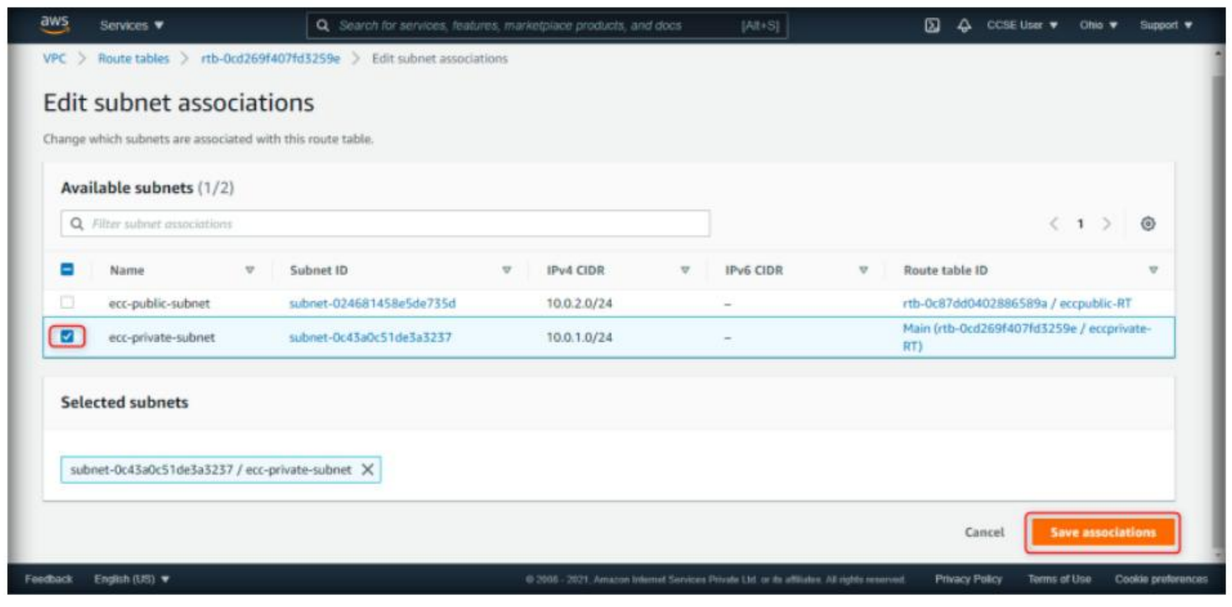


FIGURE 2.3.47: Selecting Private Subnet

Hideo_ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

50. Thus, the subnet for the private route table is added successfully.

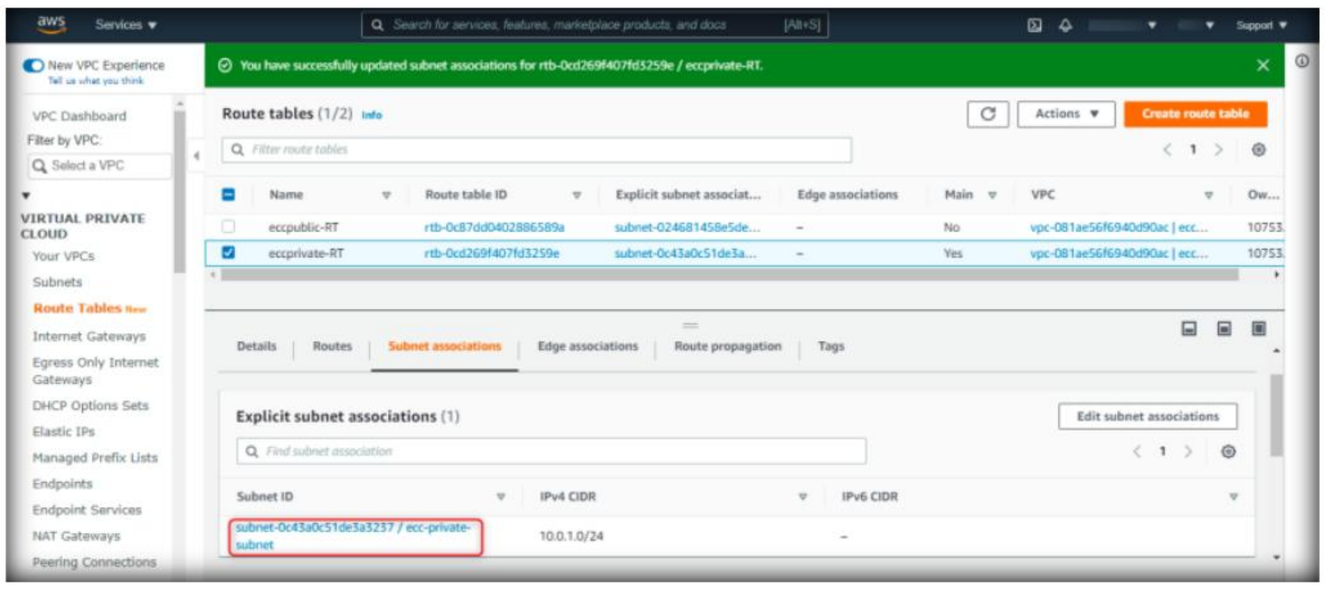


FIGURE 2.3.48: Subnet Added

51. Now, to restrict traffic from the internet to the VPC, configure the security groups. Accordingly, click on **Security Groups** in the left pane.

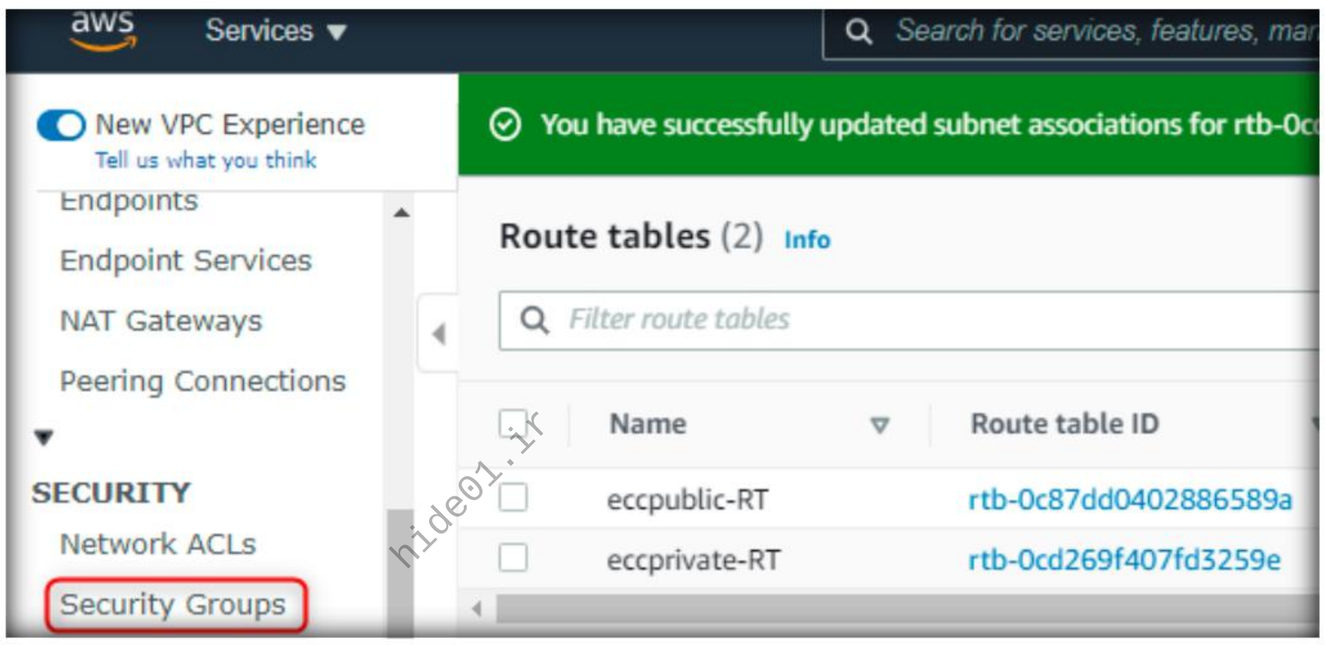


FIGURE 2.3.49: Navigating to Security Groups

52. You will notice that a default security group is created for the VPC.

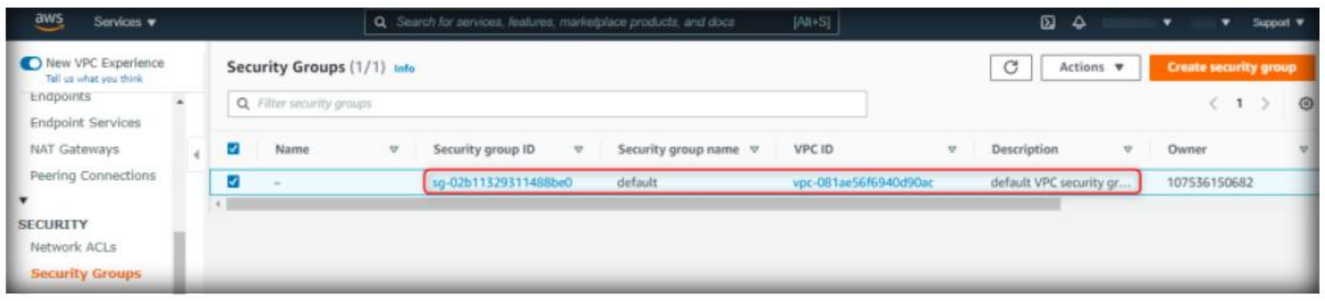


FIGURE 2.3.50: Default Security Group

53. Click on the edit icon under **Name** for the default security group and enter a name (**ecc-demo-sg**). Click on **Save.**

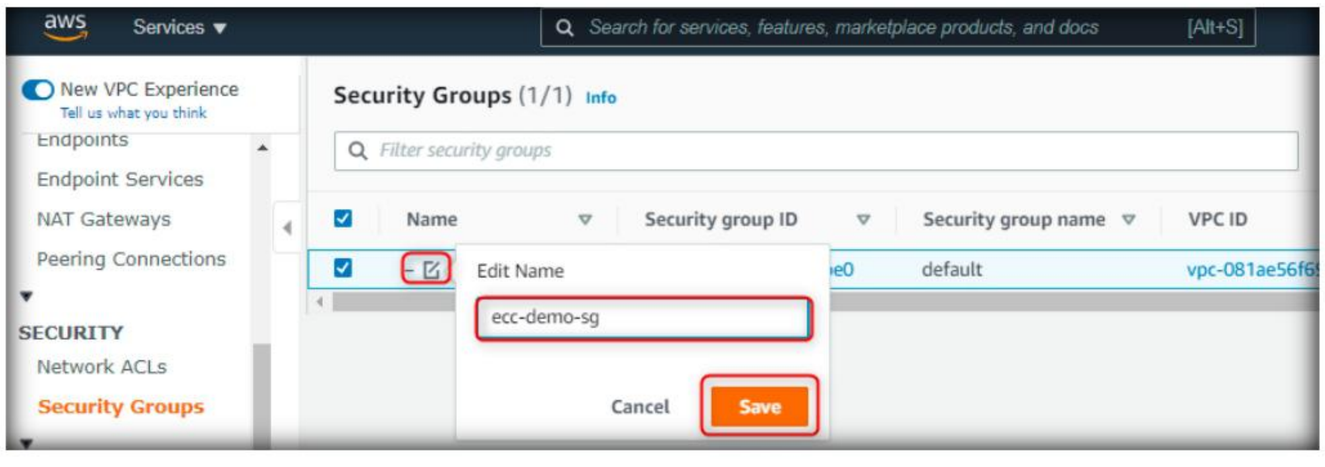


FIGURE 2.3.51: Editing Security Group Name

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

54. Now, select the checkbox for the security group. Click on **Inbound rules** to configure the incoming traffic.

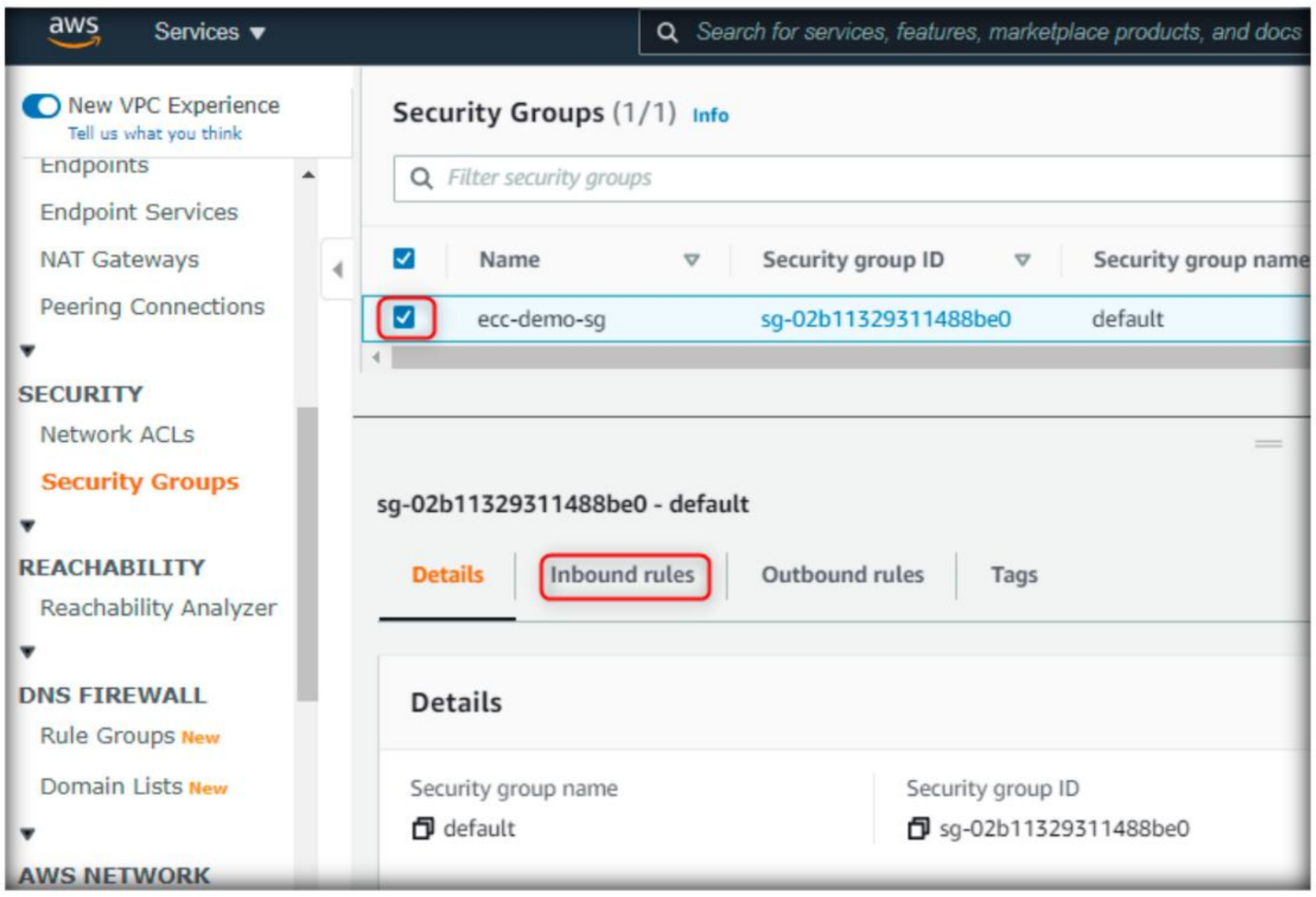


FIGURE 2.3.52: Editing Inbound Rules

55. Click on **Edit inbound rules.**

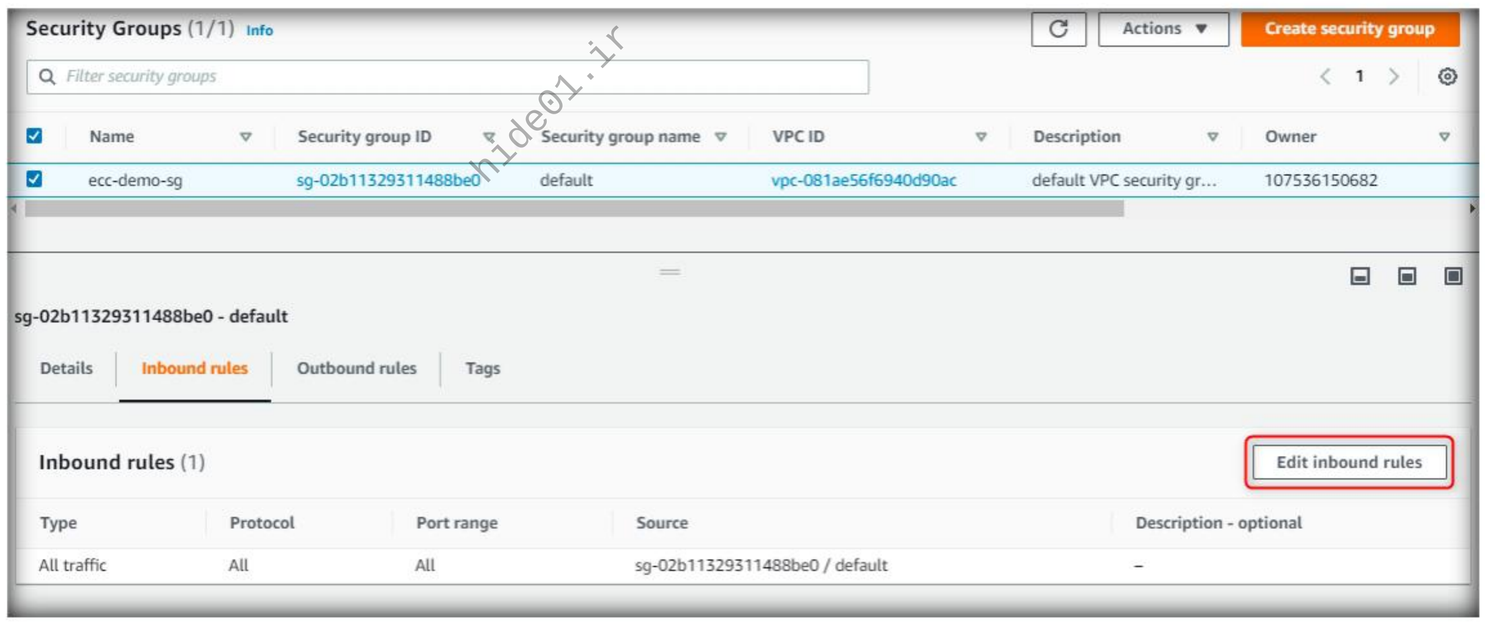


FIGURE 2.3.53: Editing Inbound Rules

56. Click on **Add rule.**

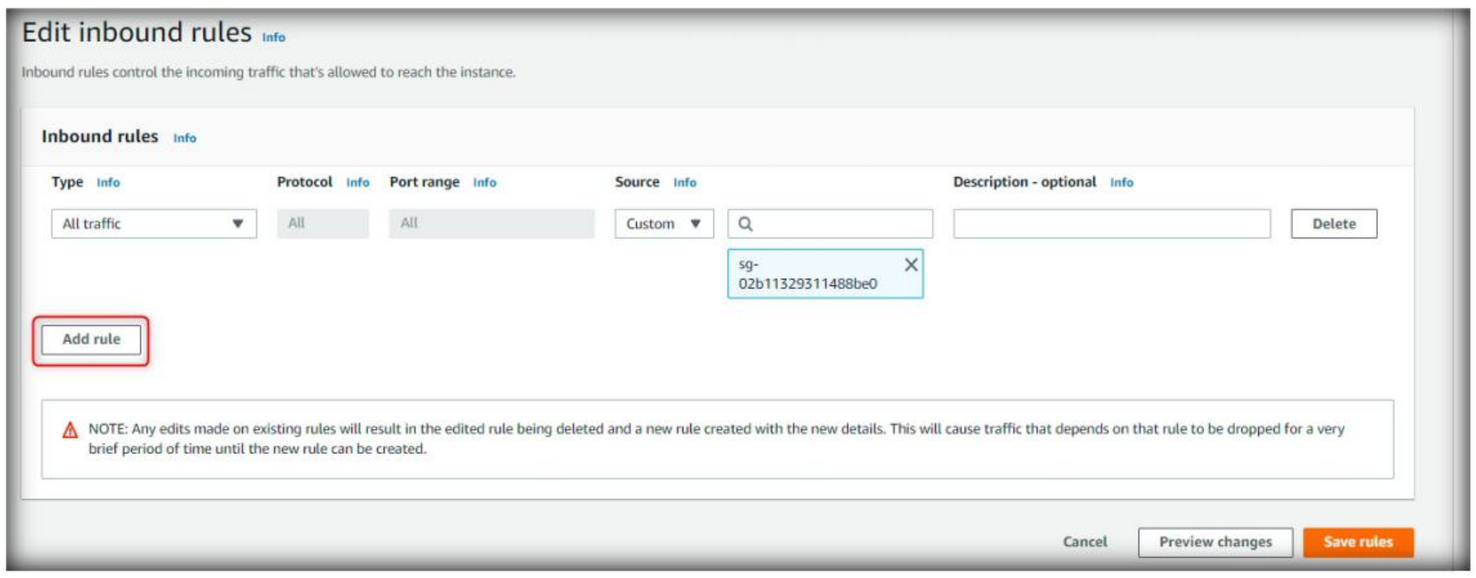


FIGURE 2.3.54: Adding Rule

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

57. For **Type**, select **All traffic.** For **Source**, select **My IP** to restrict traffic to only from your IP. Copy the IP address that appears next to **My IP**, which is the IP address of the local machine. Click on **Save rules.**

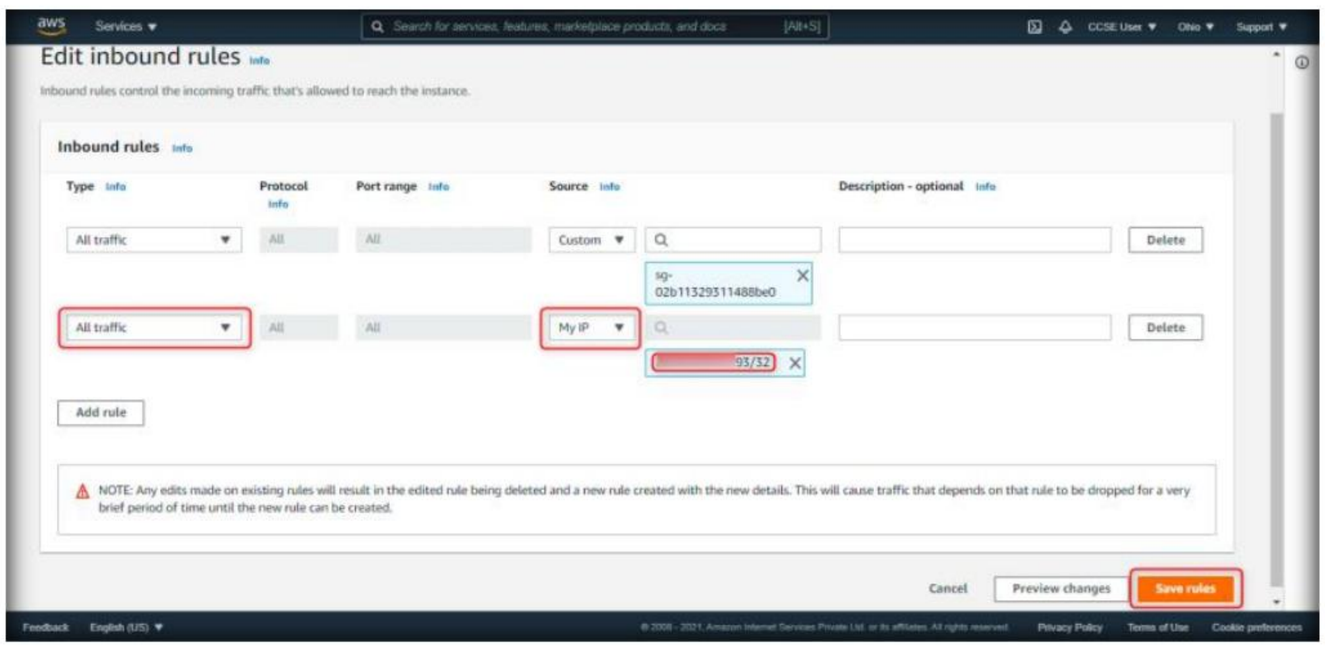


FIGURE 2.3.55: Adding Rule

58. Now, the inbound rules have been updated for the security group. Next, click on **Network ACLs** in the left pane to configure the access control for the subnets.

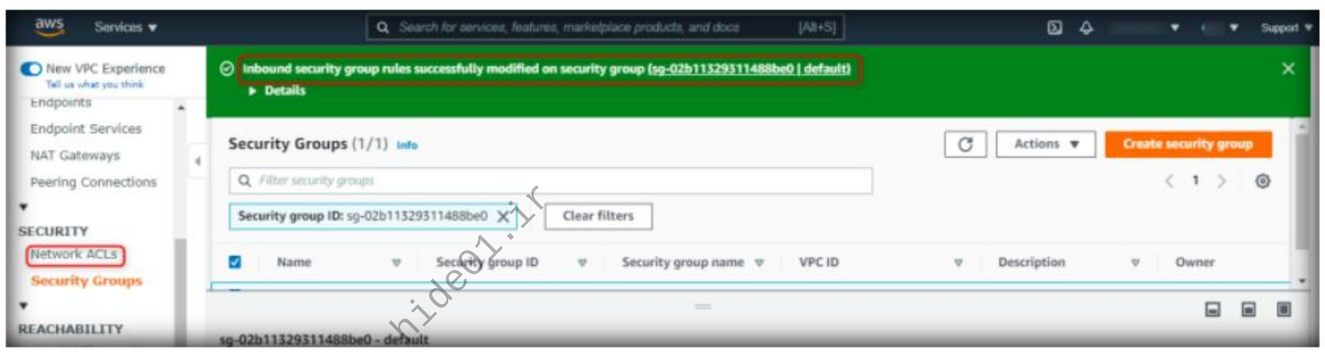


FIGURE 2.3.56: Navigating to Network ACL

59. You can see a default Network ACL. Identify the Network ACL of your VPC based on the VPC ID.

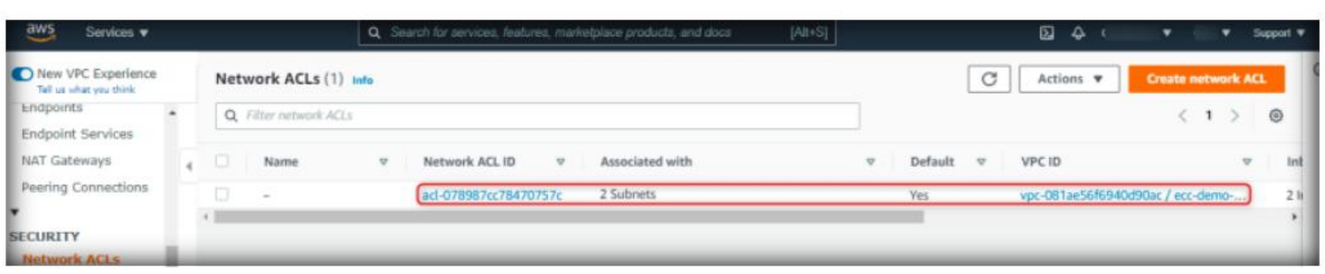


FIGURE 2.3.57: Default Network ACL

60. Click on the edit icon under **Name** for the default network ACL. Enter a name (**ecc-demo-ACL**) under **Edit name**. Click on **Save.**

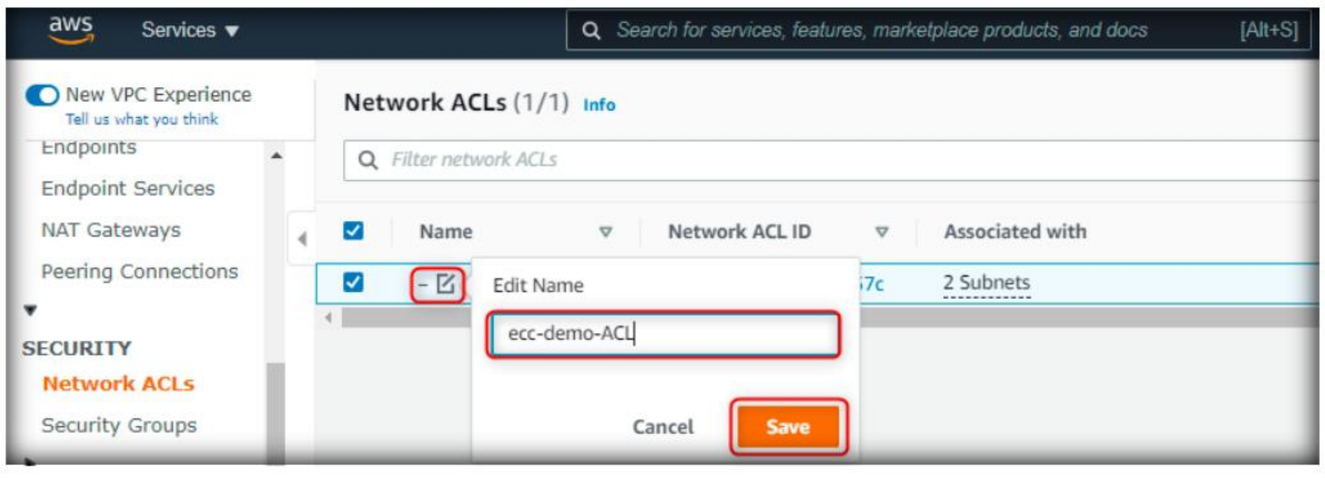


FIGURE 2.3.58: Editing Network ACL Name

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

61. Now, select the checkbox for the network ACL (**ecc-demo-ACL**). Click on **Inbound rules**.

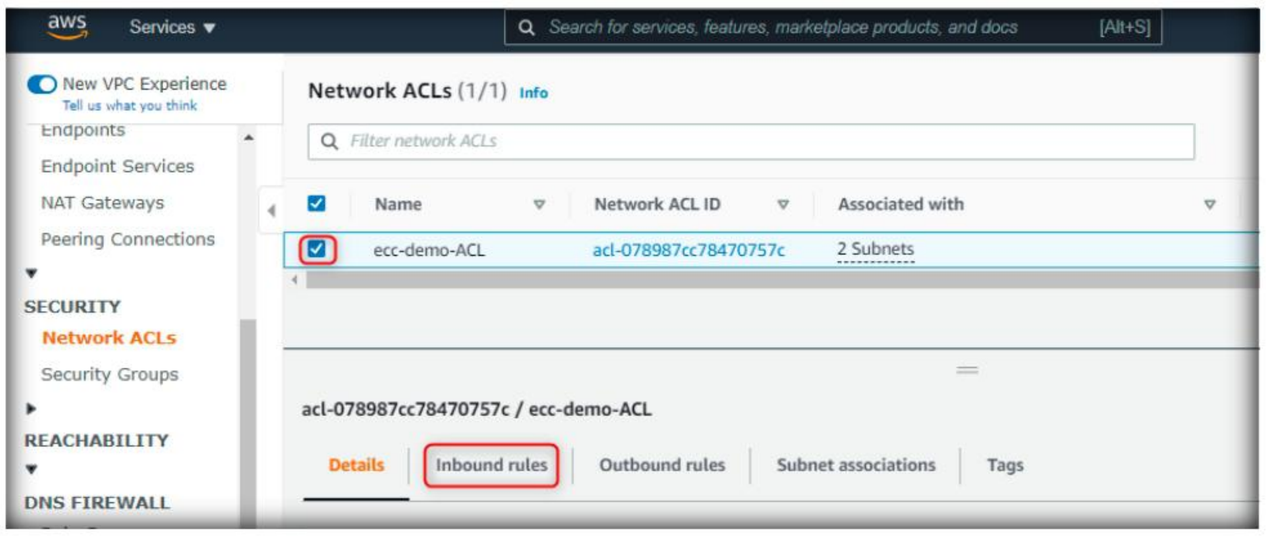


FIGURE 2.3.59: Selecting Inbound Rules

62. Here, you can see that all traffic is allowed. To restrict traffic to only from your IP, click on **Edit inbound rules**.

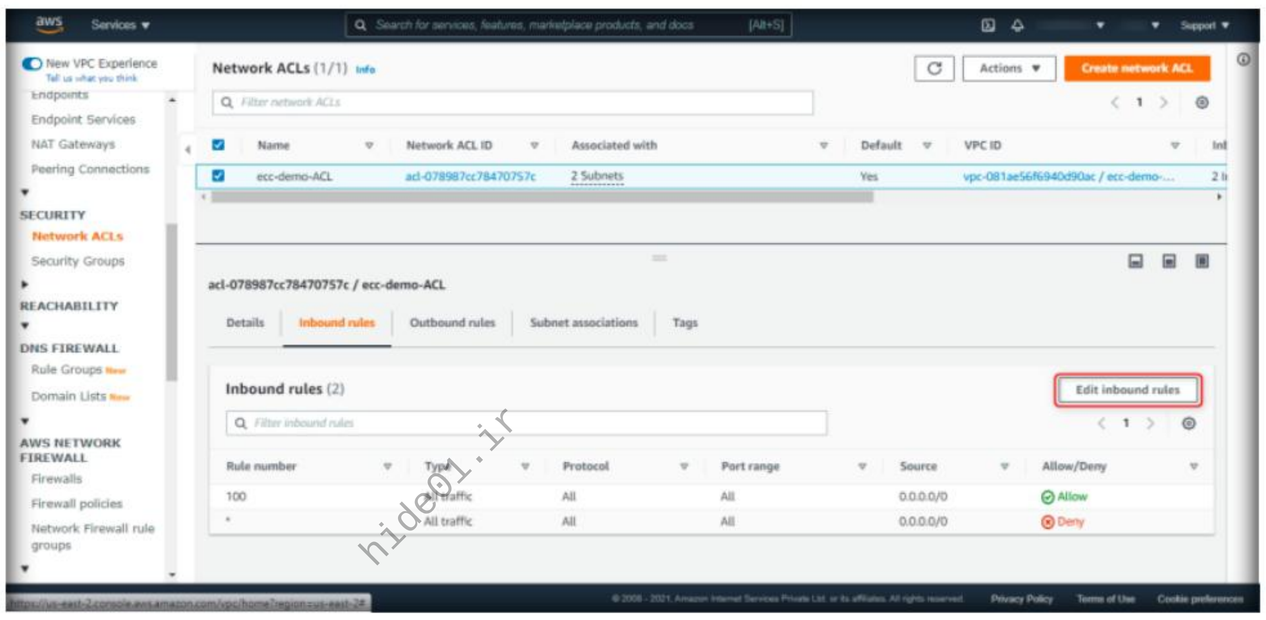


FIGURE 2.3.60: Editing Inbound Rules

63. For **Source,** change it from 0.0.0.0/0 to your IP copied while configuring the security group. Click on **Save changes.**

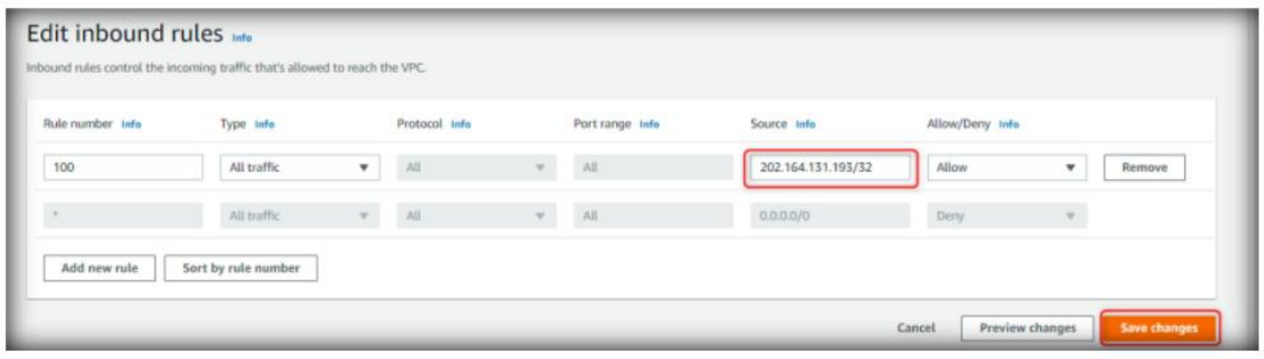


FIGURE 2.3.61: Editing Inbound Rules

64. Thus, the inbound rules for the ACL are successfully updated.

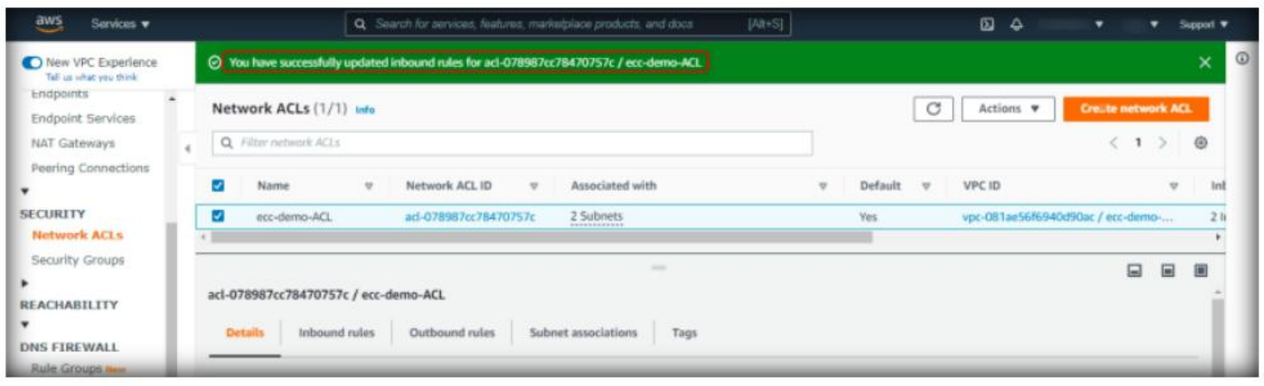


FIGURE 2.3.62: Inbound Rules Updated

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 5

Creating EC2 instances for both subnets

65. Next, create an EC2 instance in the public and private subnets. Click on **Services** at the top and select **EC2** under **Compute.**

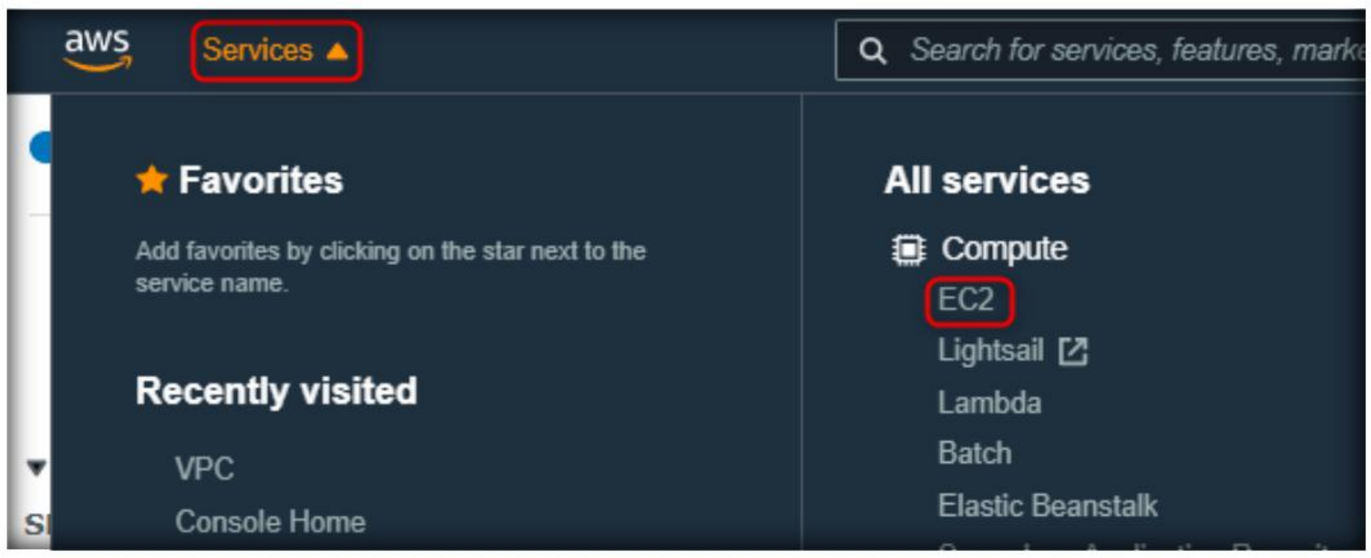


FIGURE 2.3.63: Navigating to EC2

66. In the **EC2 Dashboard** window, click on **Instances** in the left pane.

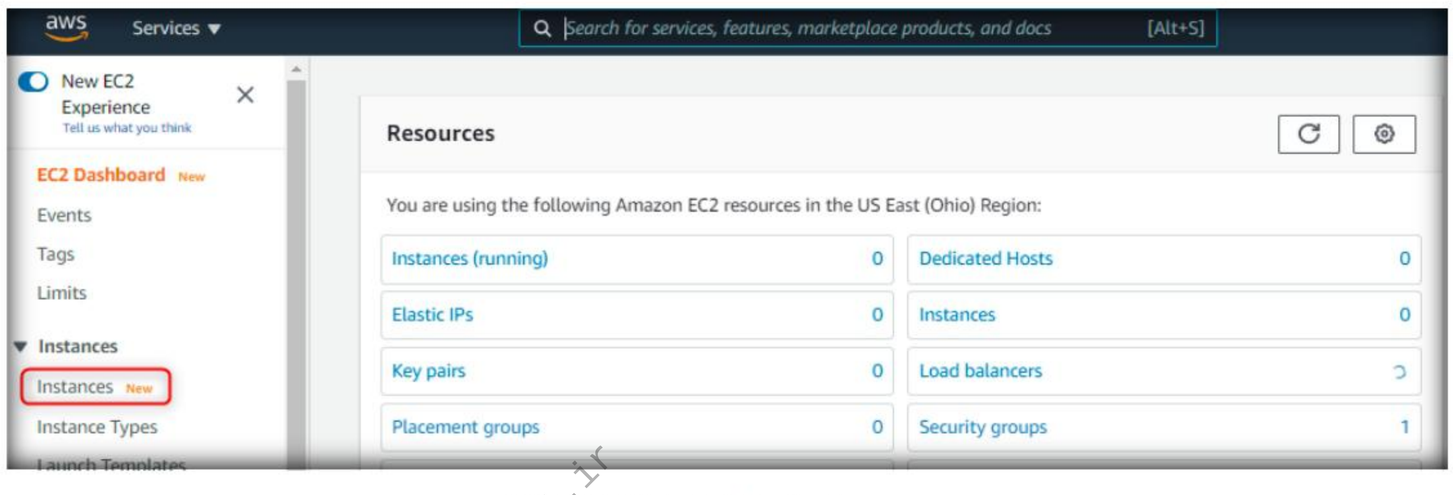


FIGURE 2.3.64: Selecting Instances

67. Click on **Launch instances**.

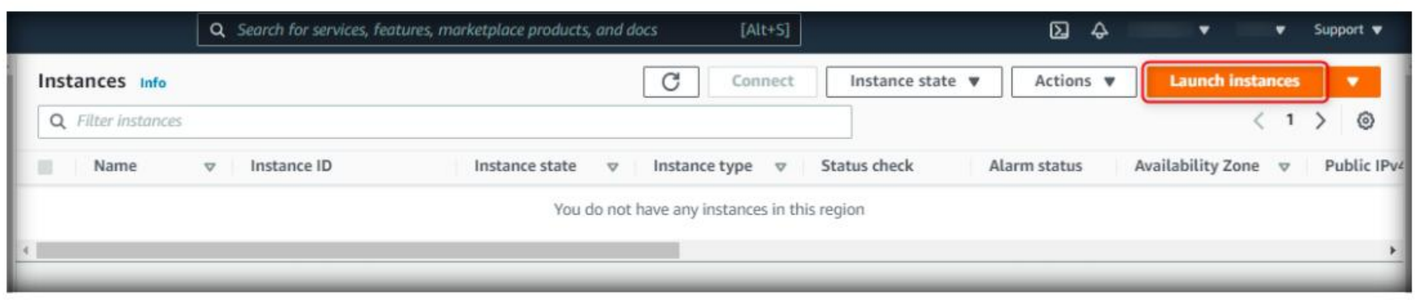


FIGURE 2.3.65: Launching Instances

68. In the window for **Choose an Amazon Machine Image (AMI),** click on **Select** for **Amazon Linux 2 AMI (HVM), SSD Volume Type.**

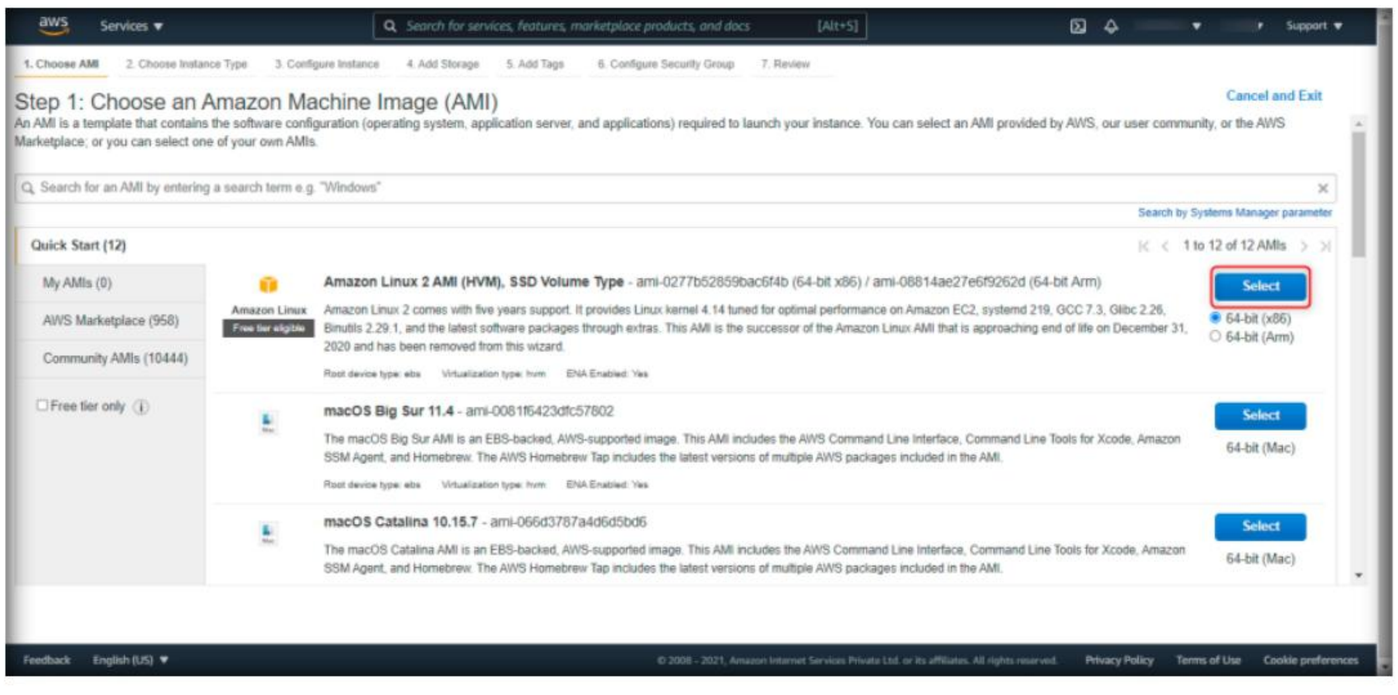


FIGURE 2.3.66: Selecting AMI

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

69. In the next window for **Choose an Instance Type**, select the checkbox for **t2.micro**, which is eligible for free tier. Click on **Next: Configure Instance Details**.

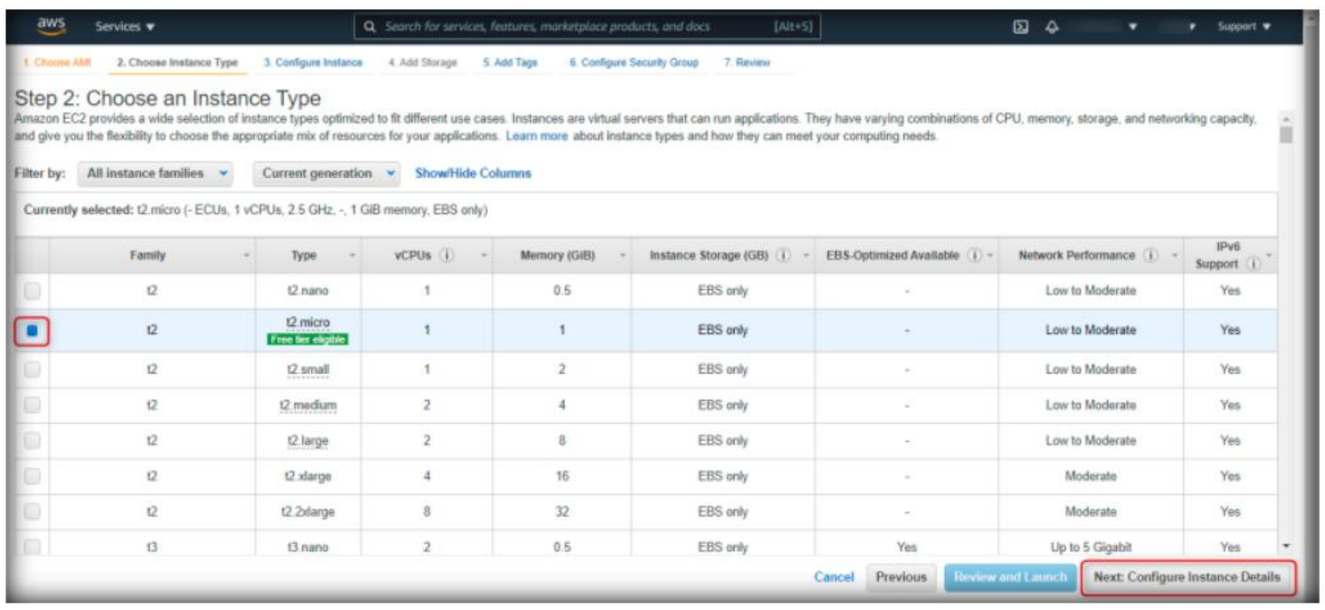


FIGURE 2.3.67: Selecting Instance Type

70. Then, the **Configure Instance Details** window appears. For **Network,** select the VPC network (**ecc-demo-vpc**) created by you for this lab. For **Subnet,** select the public subnet (**ecc-public-subnet**) to configure the first EC2 instance. For **Auto-assign Public IP**, select **Enable** from the dropdown. Click on **Next: Add Storage**.

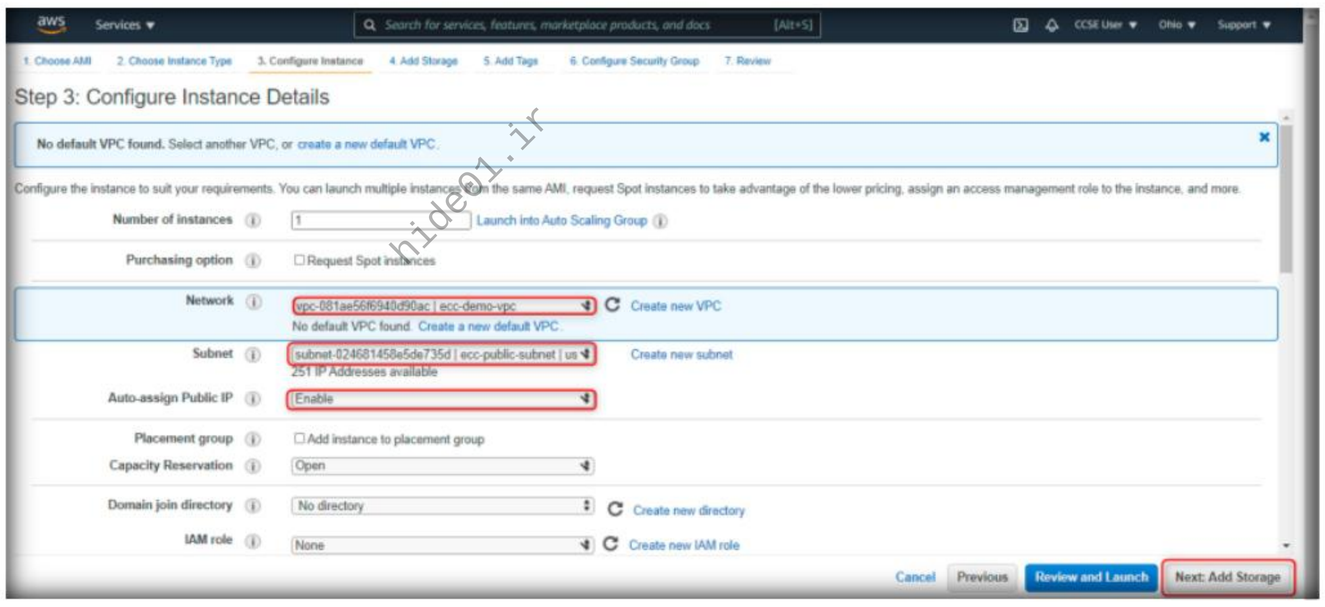


FIGURE 2.3.68: Configuring Instance Details

71. In the **Add Storage** window, do not change the default settings. Click on **Next: Add Tags.**

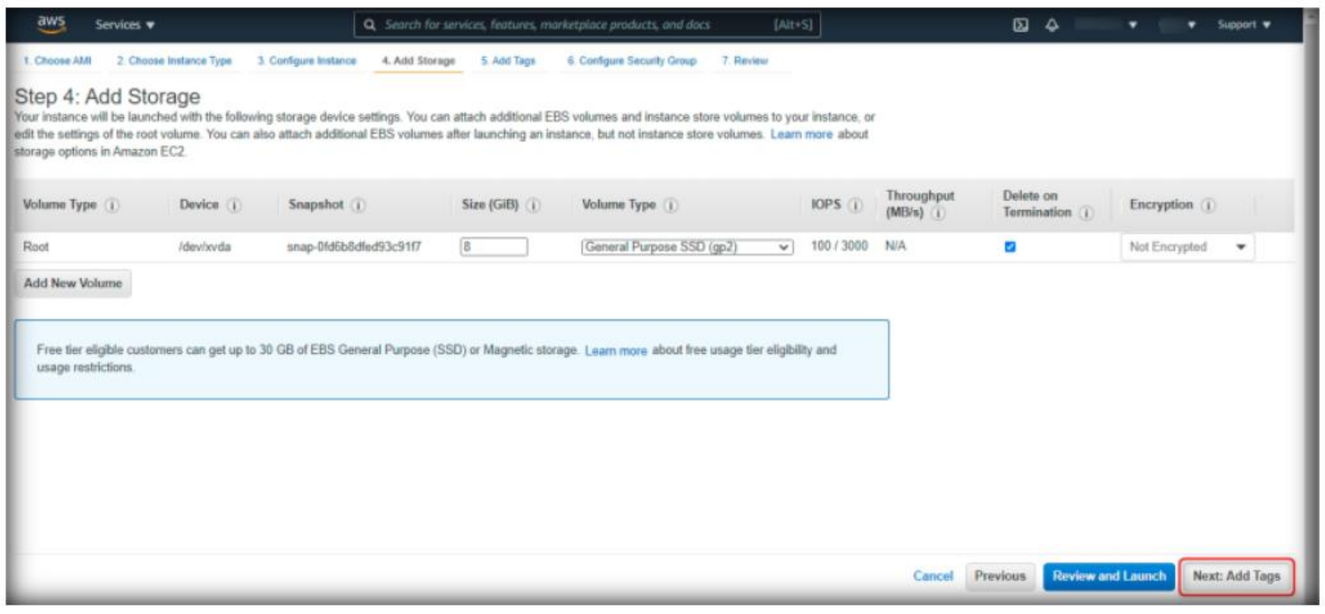


FIGURE 2.3.69: Continue with Configuration

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

72. In the **Add Tags** window, click on **Next: Configure Security Group**.

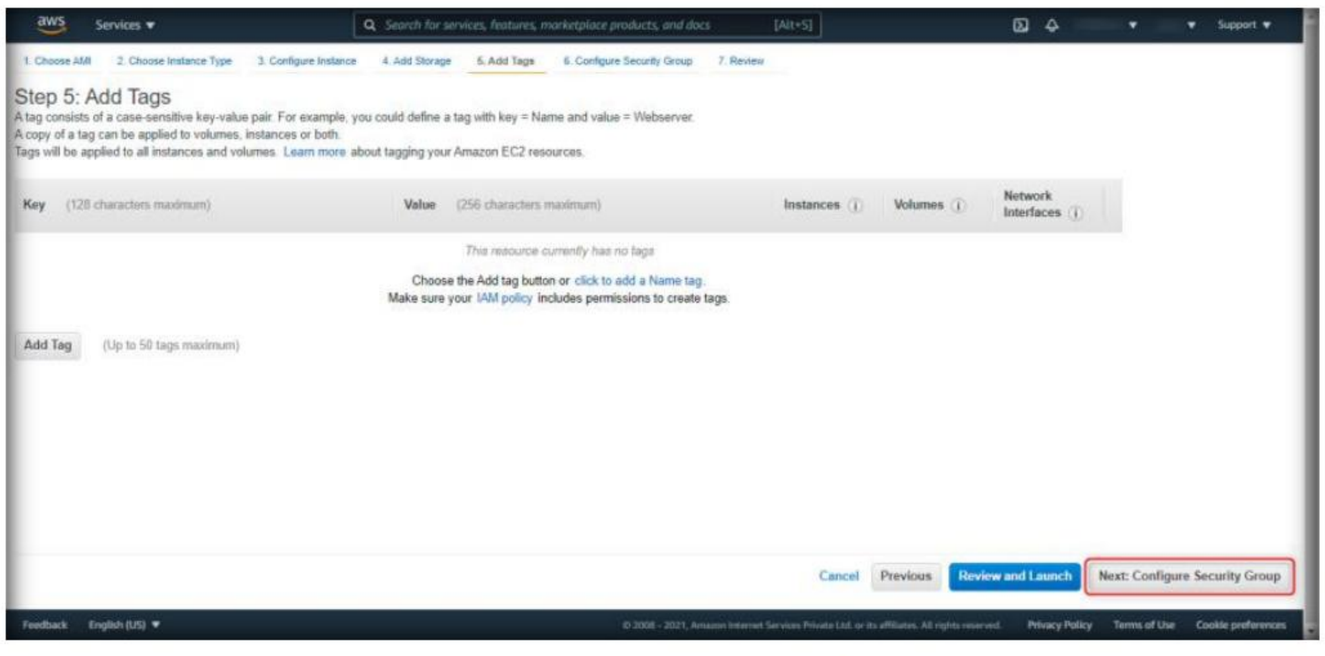


FIGURE 2.3.70: Continue with Configuration

73. Then, the **Configure Security Group** window appears. For **Assign a security group**, select the radio button for **Select an existing security group**. Select the checkbox for the security group configured by you for the VPC. Click on **Review and Launch**.

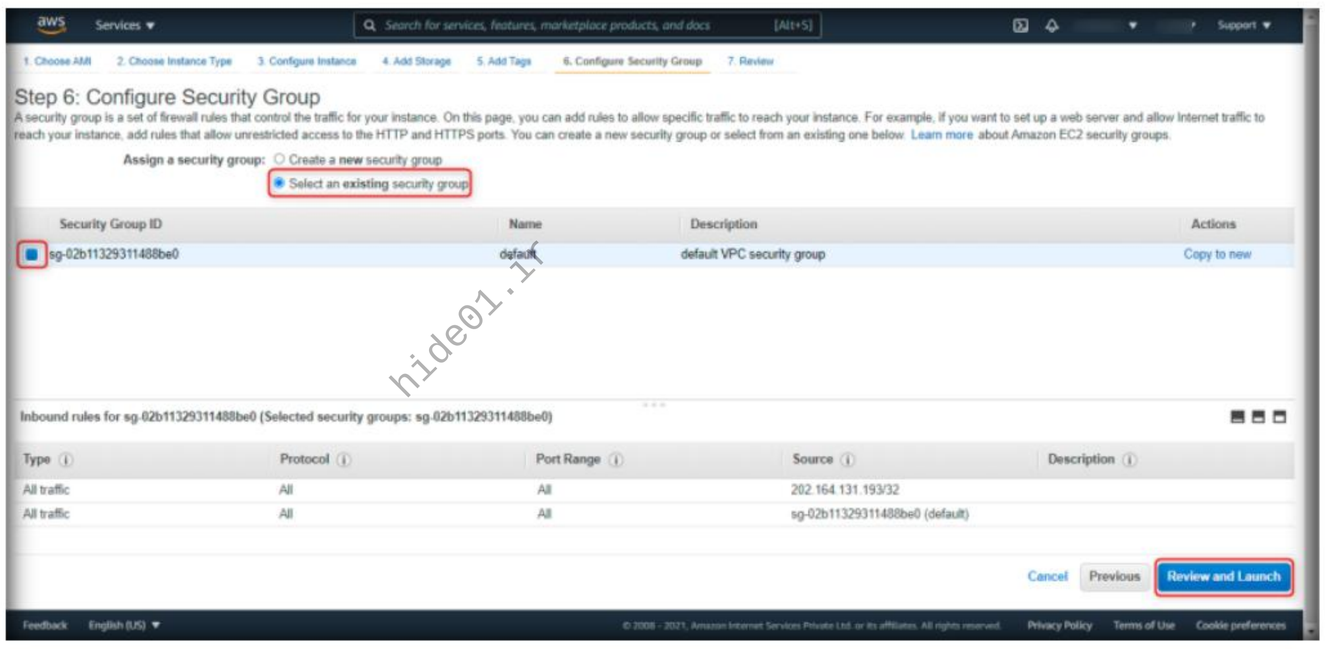


FIGURE 2.3.71: Adding Security Group

74. In the **Review Instance Launch** page, click on **Launch**.

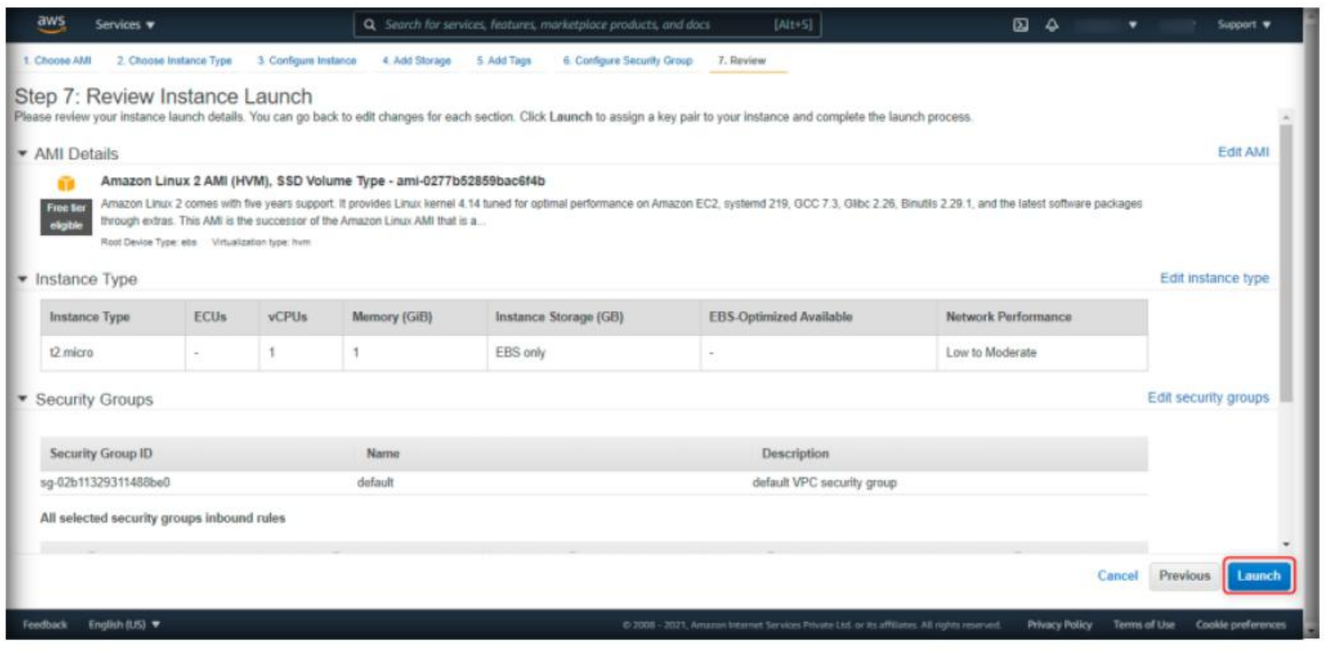


FIGURE 2.3.72: Launching Instance

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

75. A popup appears for **Select an existing key pair or create a new key pair**. Select **Create a new key pair** from the dropdown and enter a name (**eccdemo-key**) under **Key pair name**. Click on **Download key pair**. Thus, the key pair is downloaded to your local machine with a **.pem** extension (**eccdemo-key.pem**).

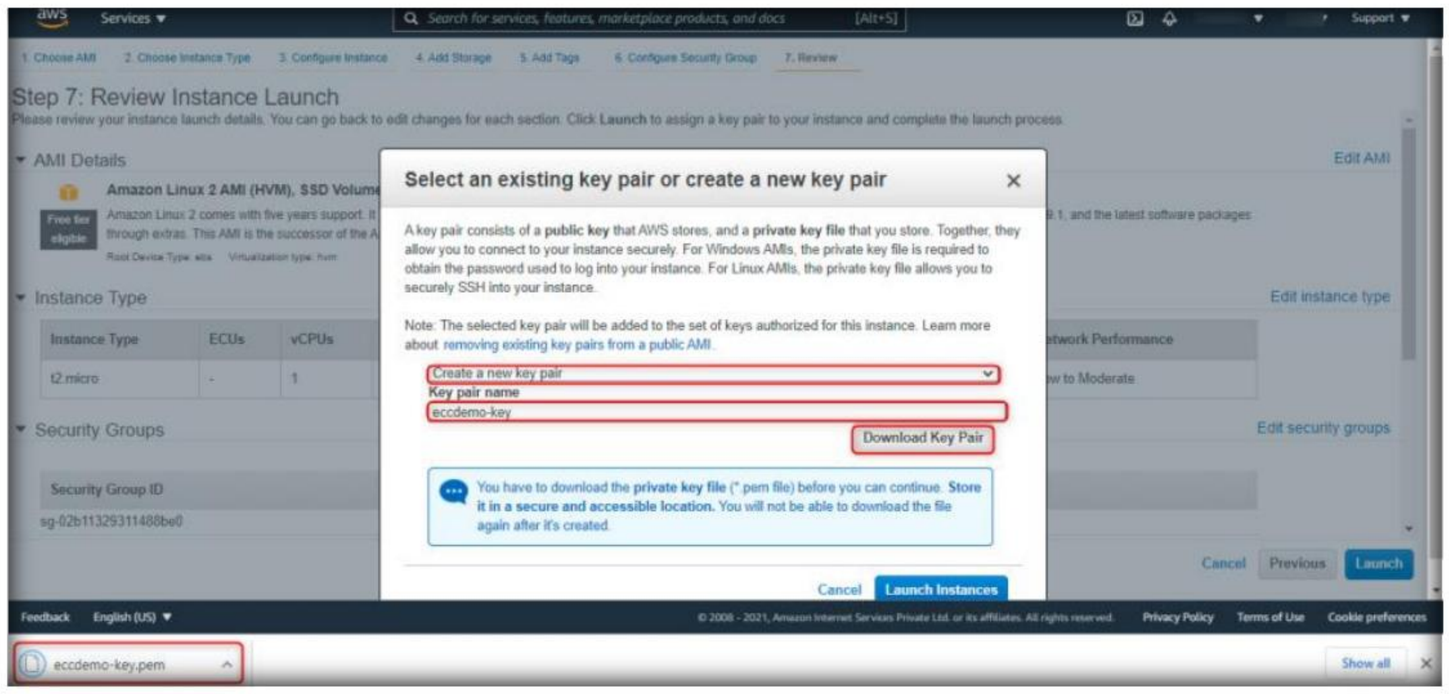


FIGURE 2.3.73: Downloading Key Pair

76. Click on **Launch Instances**.

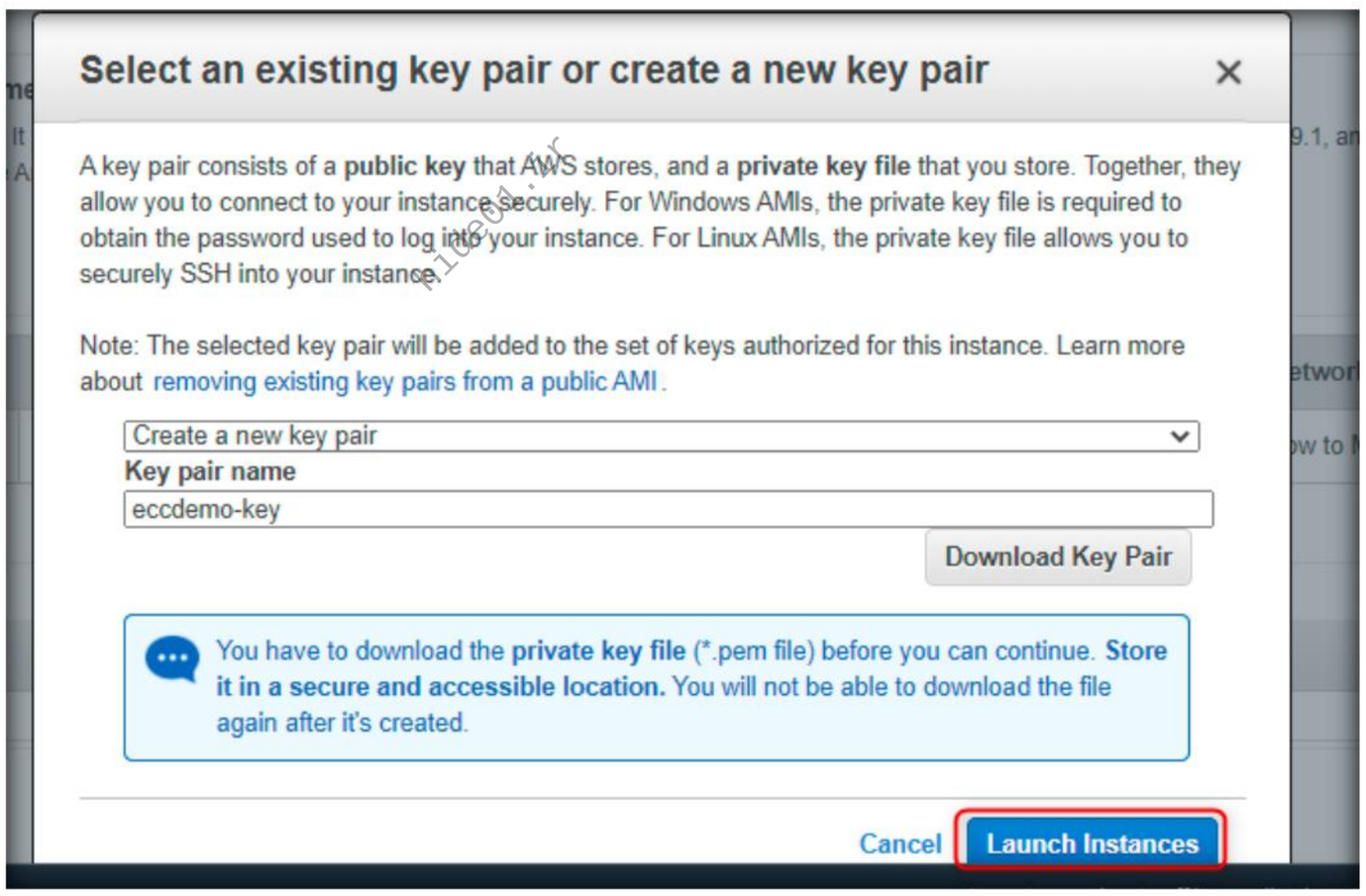


FIGURE 2.3.74: Launching Instance

77. Now, the **Launch Status** window will display "**Your Instances are now Launching**."

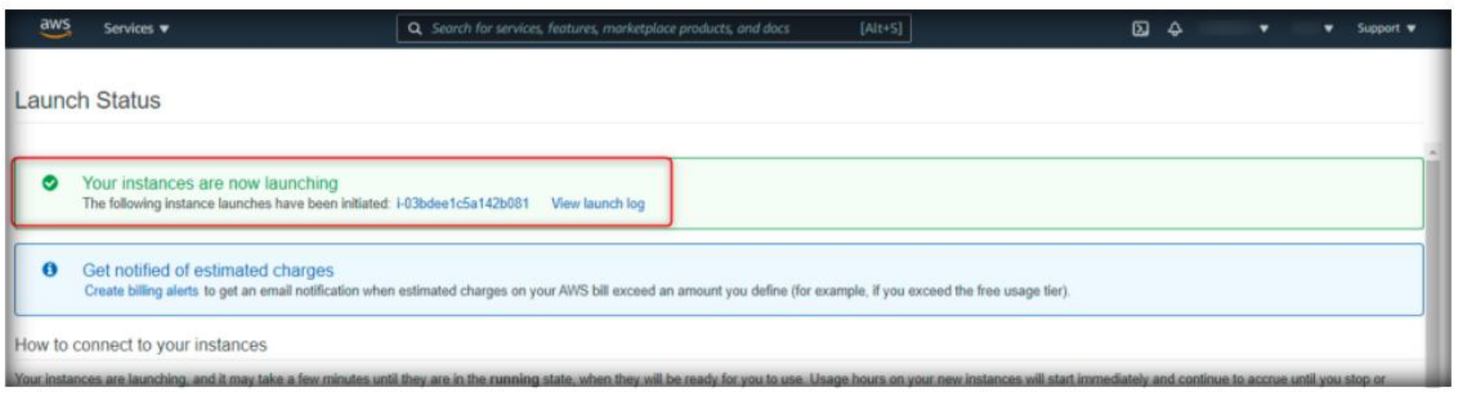


FIGURE 2.3.75: Instance Launching

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

78. Scroll down to the bottom and click on **View Instances**.

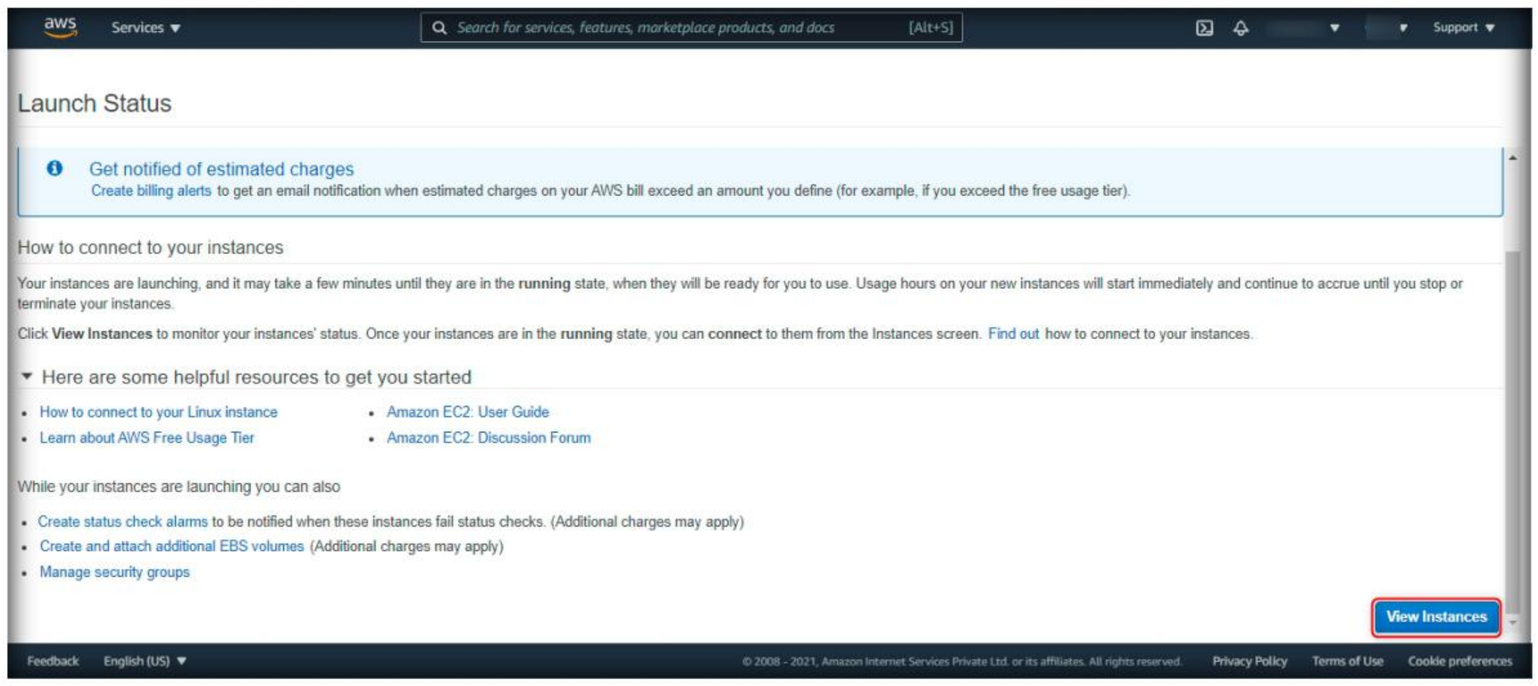


FIGURE 2.3.76: Viewing the Instance

79. The **Instance state** is shown as **Running**.

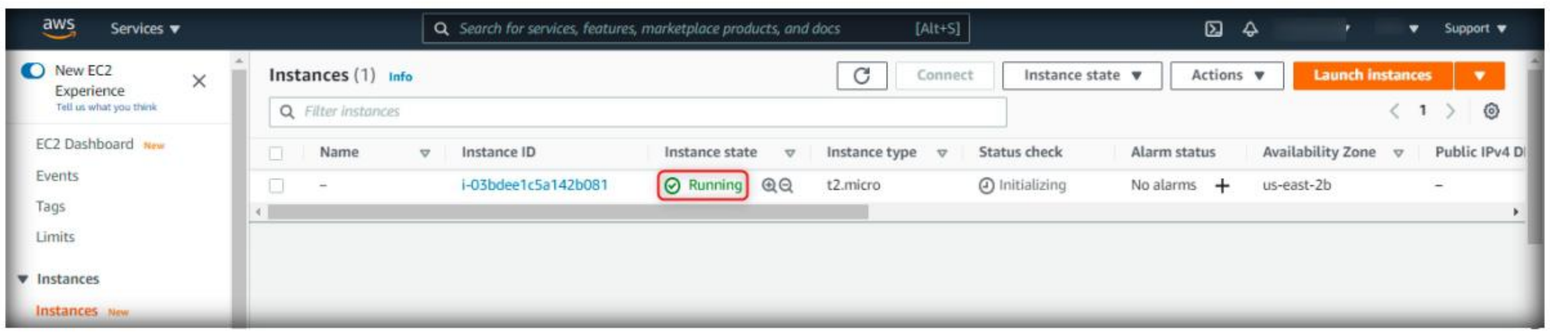


FIGURE 2.3.77: Instance is Running

80. Now, edit the name for the EC2 instance. Click on the **edit** icon under **Name** for the instance you have created. Enter a name (**eccpublic-ec2**) for the public EC2 instance under **Edit Name**. Click on **Save**.

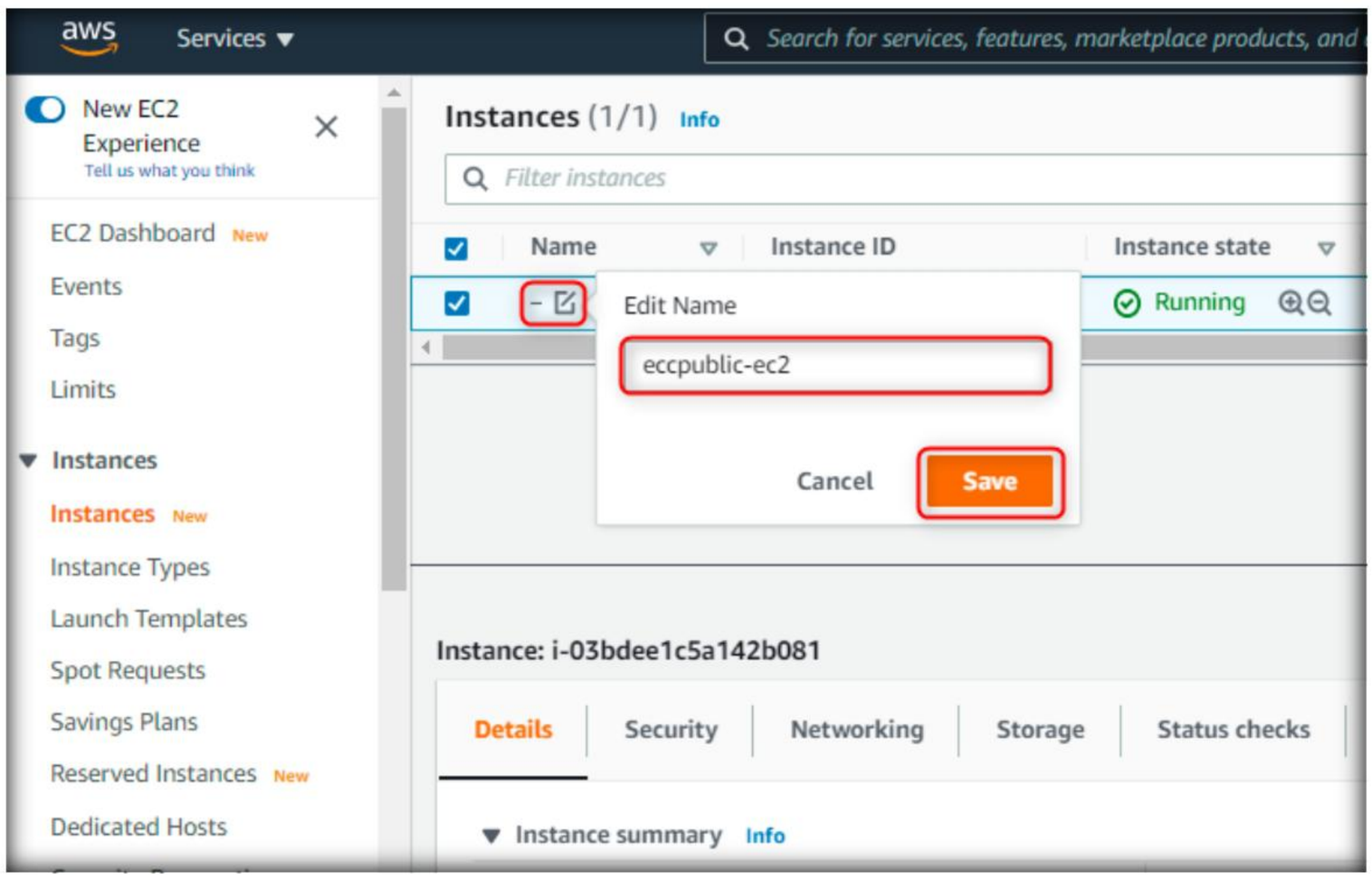


FIGURE 2.3.78: Editing Instance Name

Certified Cloud Security Engineer Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

81. Select the checkbox for the instance. Under the **Details** tab in the bottom, you can see the **Public IPv4 address** and **Private IPv4 addresses** of the instance. Copy the **Public IPv4 address** to Notepad.

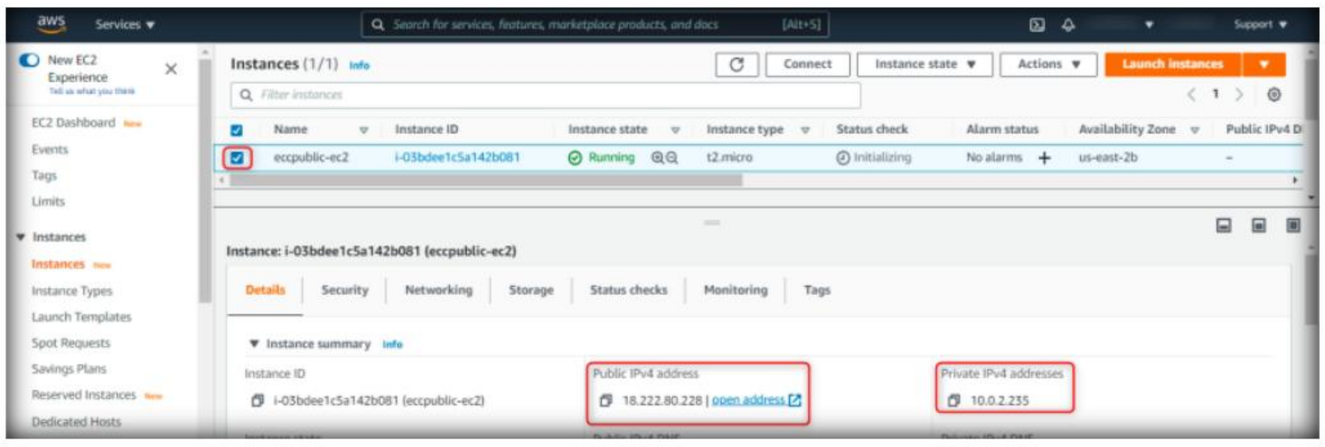


FIGURE 2.3.79: Viewing IPs of Instance

82. Now, create a new EC2 instance for the private subnet. For that, click on **Launch instances**.

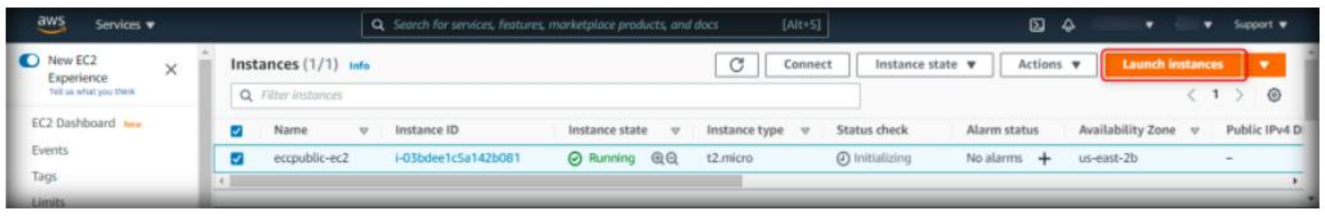


FIGURE 2.3.80: Launching Instance

83. Under **Choose an Amazon Machine Image (AMI),** click on **Select** for **Amazon Linux 2 AMI (HVM), SSD Volume Type**.

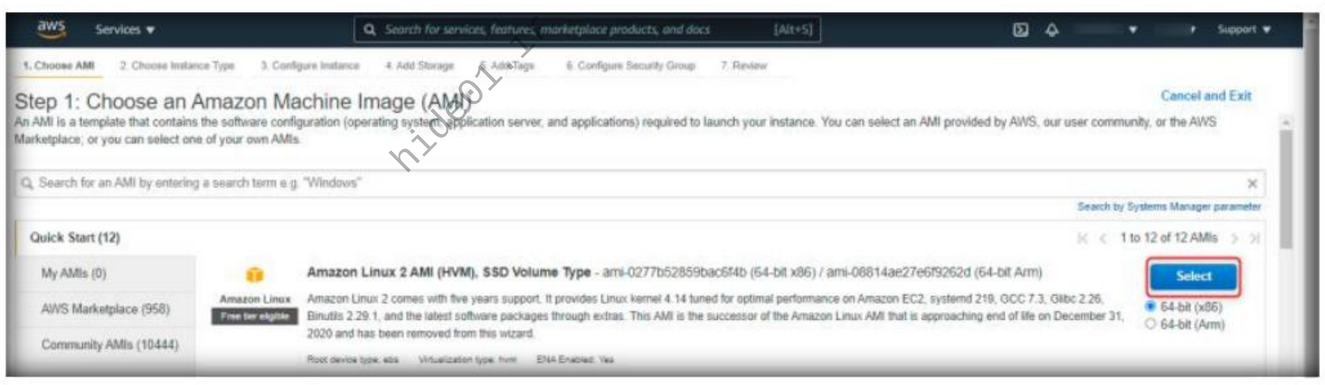


FIGURE 2.3.81: Selecting AMI

84. In the next window for **Choose an Instance Type**, select the checkbox for **t2.micro,** which is eligible for free tier. Click on **Next: Configure Instance Details**.

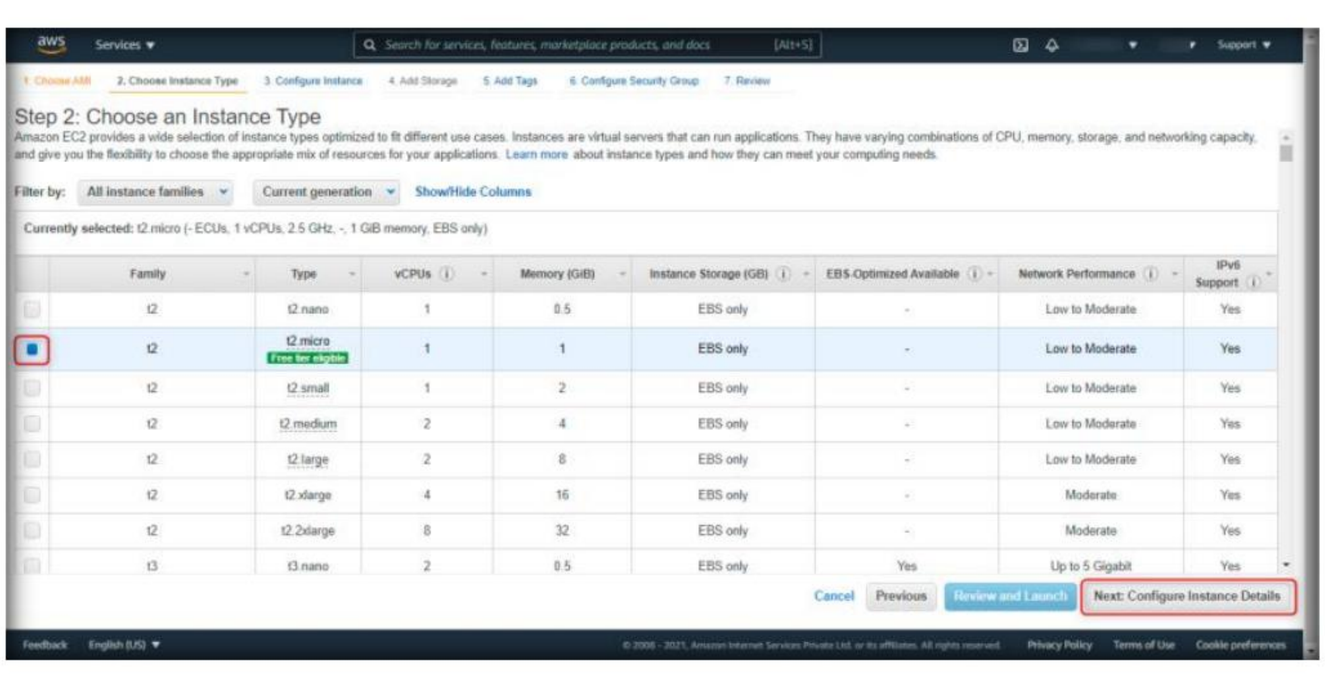


FIGURE 2.3.82: Selecting Instance Type

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

85. Then, the **Configure Instance Details** window appears. For **Network,** select the VPC network (**ecc-demo-vpc**) created by you for this lab. For **Subnet,** select the private subnet (**ecc-private-subnet**) to configure the second EC2 instance. For **Auto-assign Public IP**, select **Enable** from the dropdown. Click on **Next: Add Storage**.

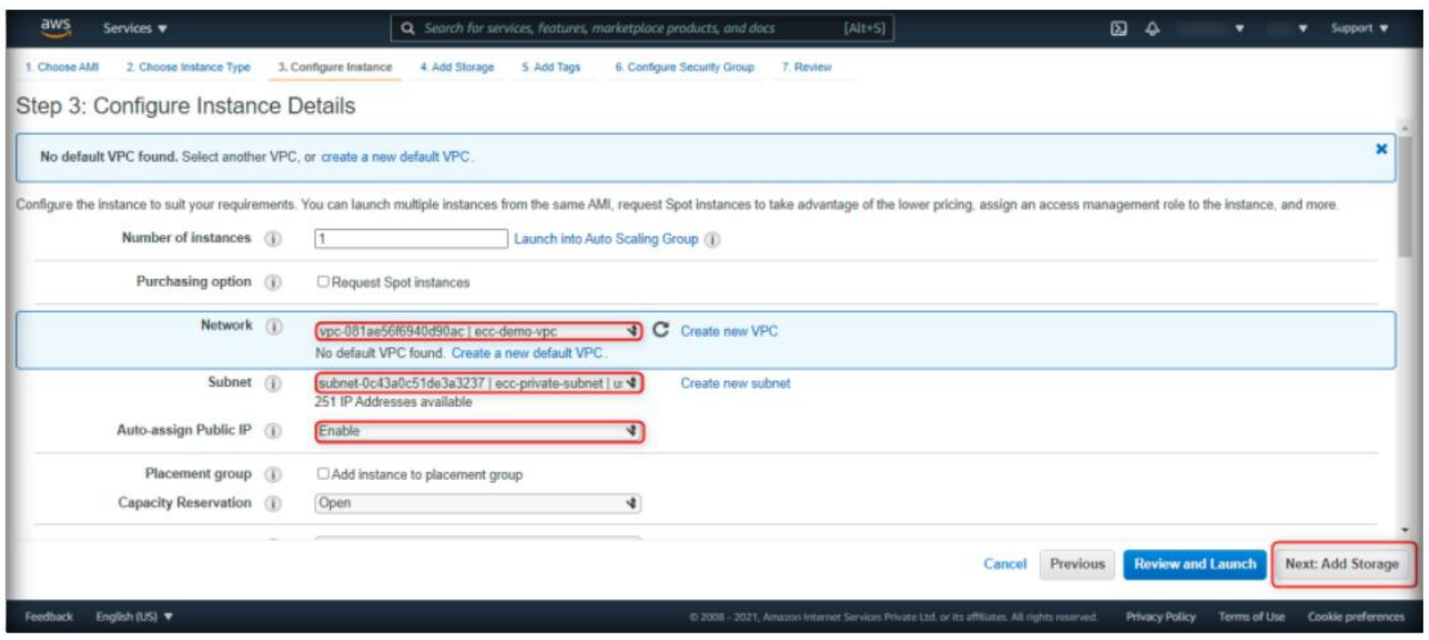


FIGURE 2.3.83: Configuring Instance Details

86. In the **Add Storage** window, do not change the default settings and click on **Next: Add Tags**.

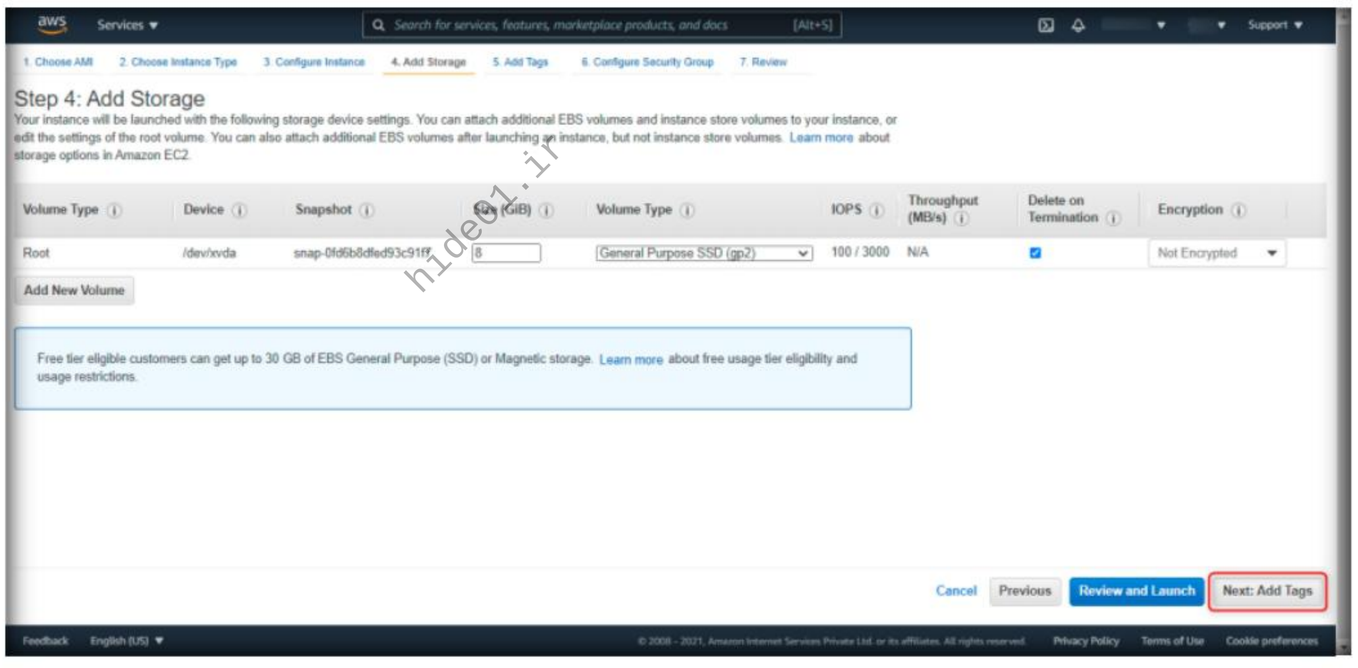


FIGURE 2.3.84: Continue with Configuration

87. In the **Add Tags** window, click on **Next: Configure Security Group**.

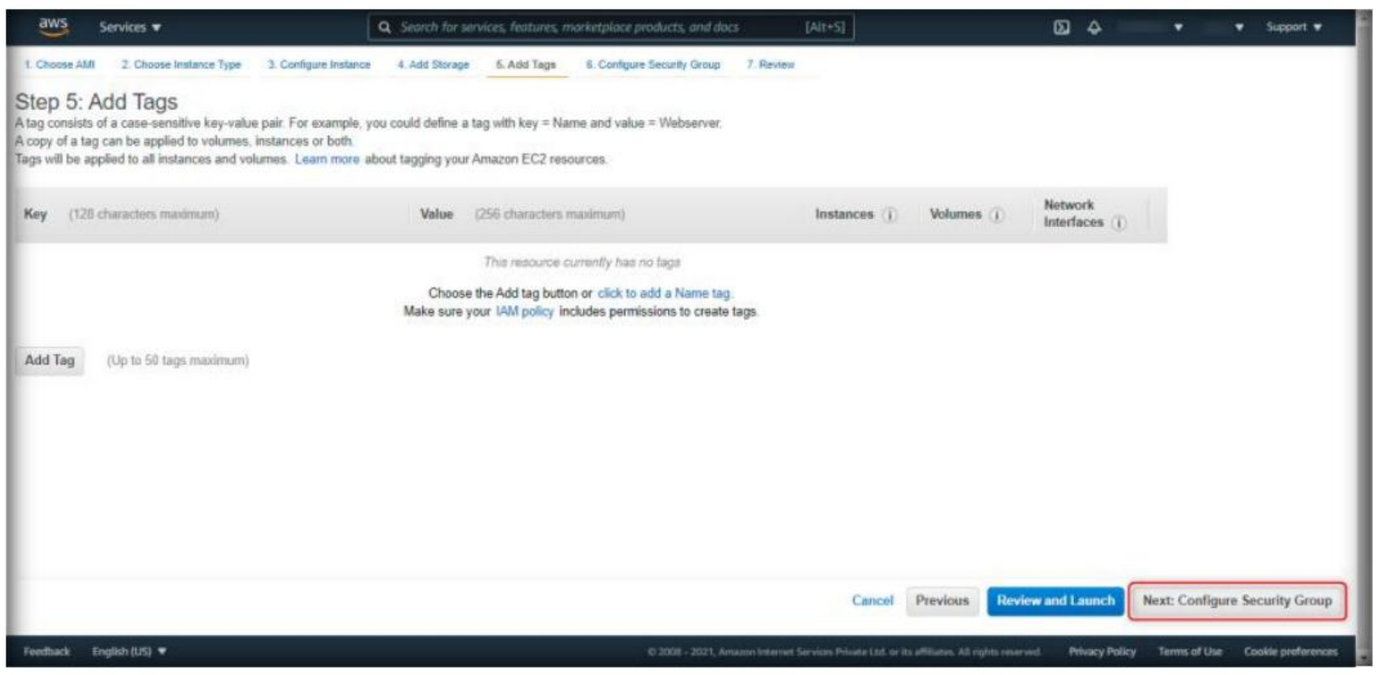


FIGURE 2.3.85: Continue with Configuration

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

88. Then, the **Configure Security Group** window appears. For **Assign a security group**, select the radio button for **Select an existing security group**. Select the checkbox for the security group configured by you for the VPC. Click on **Review and Launch**.

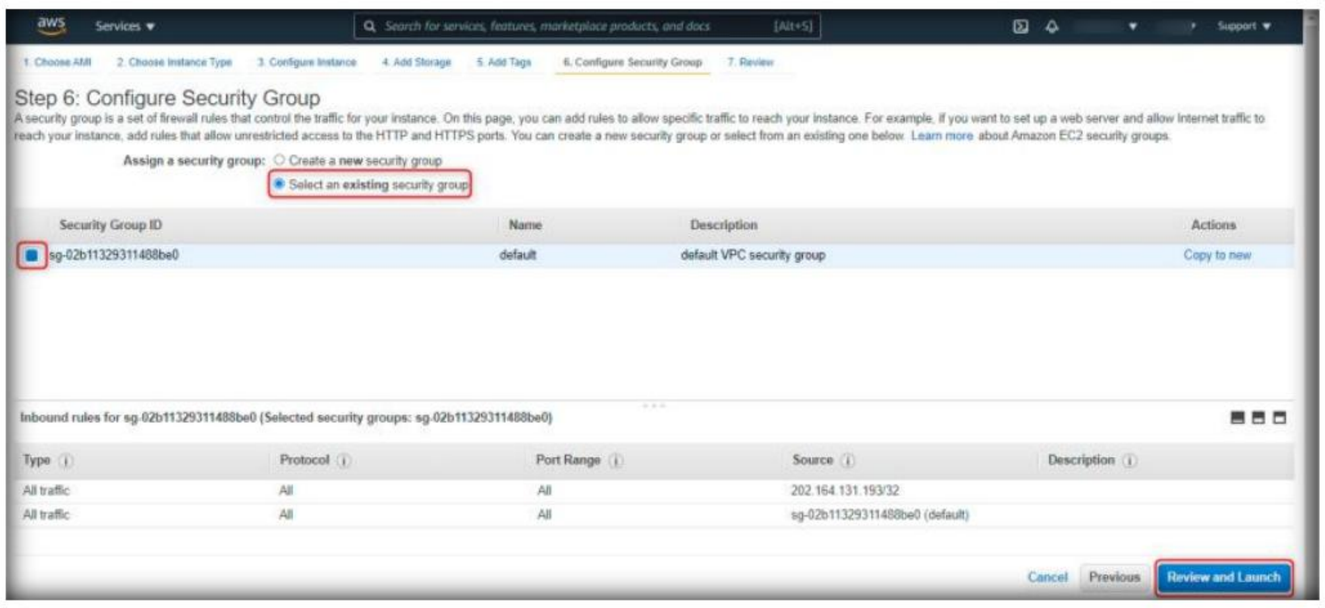
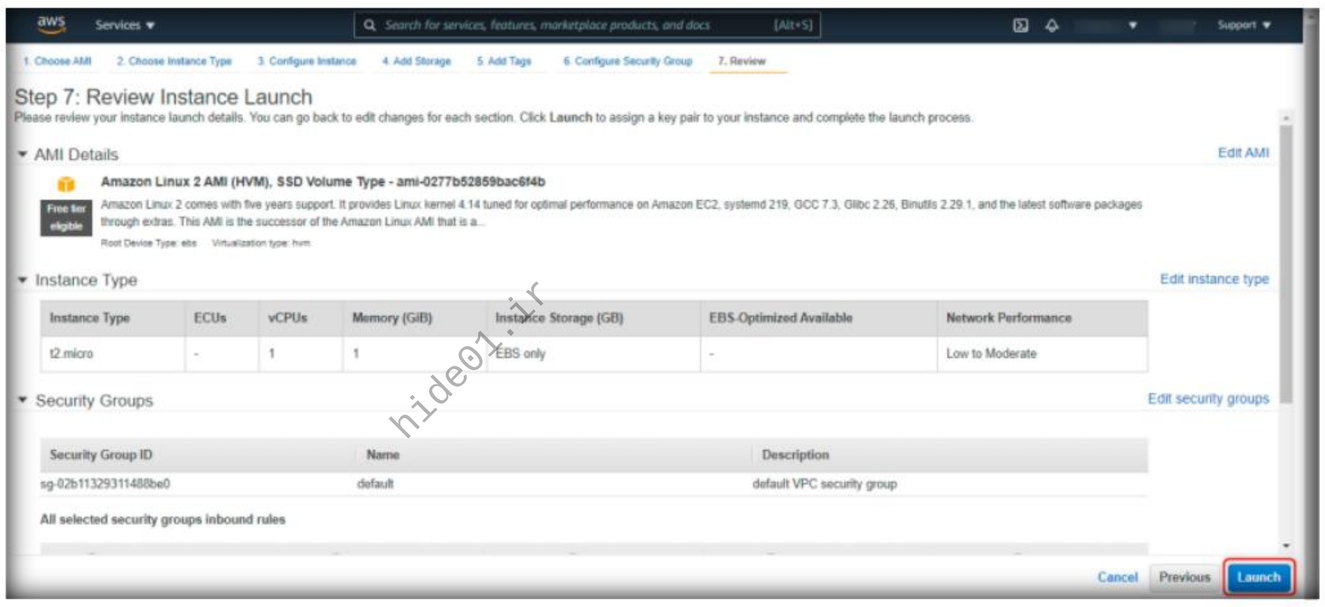


FIGURE 2.3.86: Selecting Security Group

89. In the **Review Instance Launch** page, click on **Launch**.



hide01.ir

FIGURE 2.3.87: Launching Instance

90. A popup appears for **Select an existing key pair or create a new key pair**. Select **Choose an existing key pair** from the dropdown. Under **Select a key pair**, select the name (**eccdemo-key**) entered by you while configuring the previous public EC2 instance. Select the checkbox for **acknowledgement** and click on **Launch Instances**.

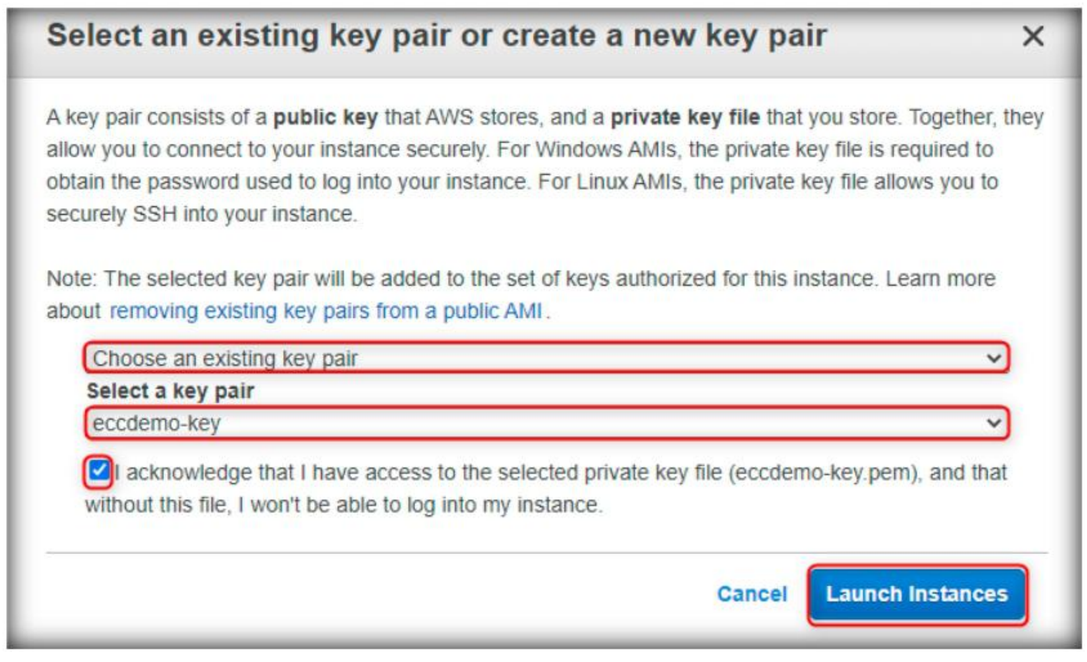


FIGURE 2.3.88: Selecting Key and Launching Instance

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

91. In the next window, scroll down to the bottom and select **View Instances.**

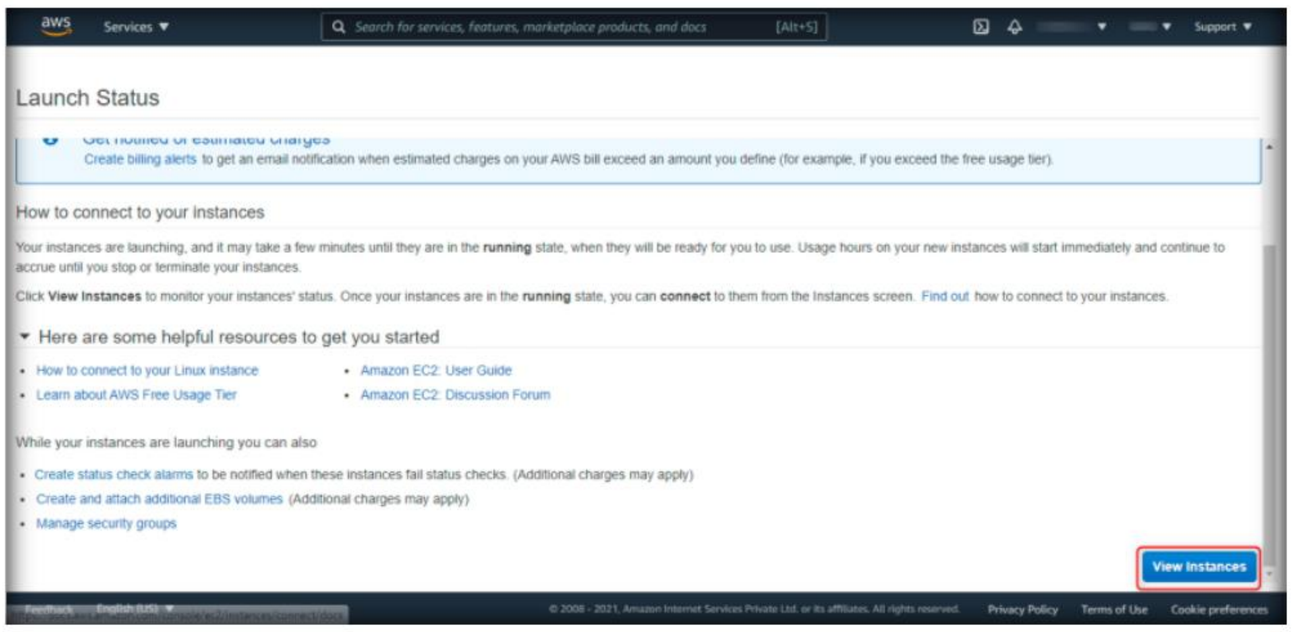


FIGURE 2.3.89: Viewing the Instance

92. Now, edit the name for the EC2 instance. Click on the **edit** icon under **Name** for the instance created by you. Enter a name (**eccprivate-ec2**) for the public EC2 instance under **Edit Name**. Click on **Save**.

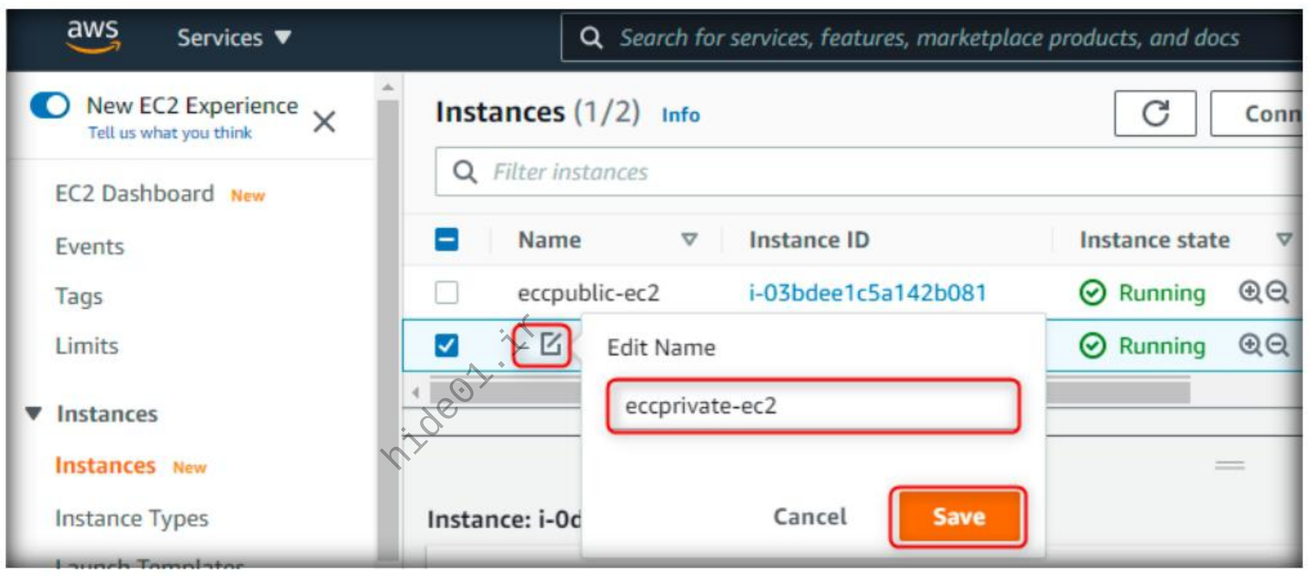


FIGURE 2.3.90: Editing Instance Name

TASK 6

Testing access to both Instances

93. Select the checkbox for the private EC2 instance created by you. Under the **Details** tab, the **Public IPv4 address** and **Private IPv4 addresses** of the instance are displayed.

94. Now, test the access to both instances. First, copy the public IP of the public subnet (**eccpublic-ec2**). Select the checkbox for the public subnet (**eccpublic-ec2**) and copy the **Public IPv4 address** under the **Details** tab.

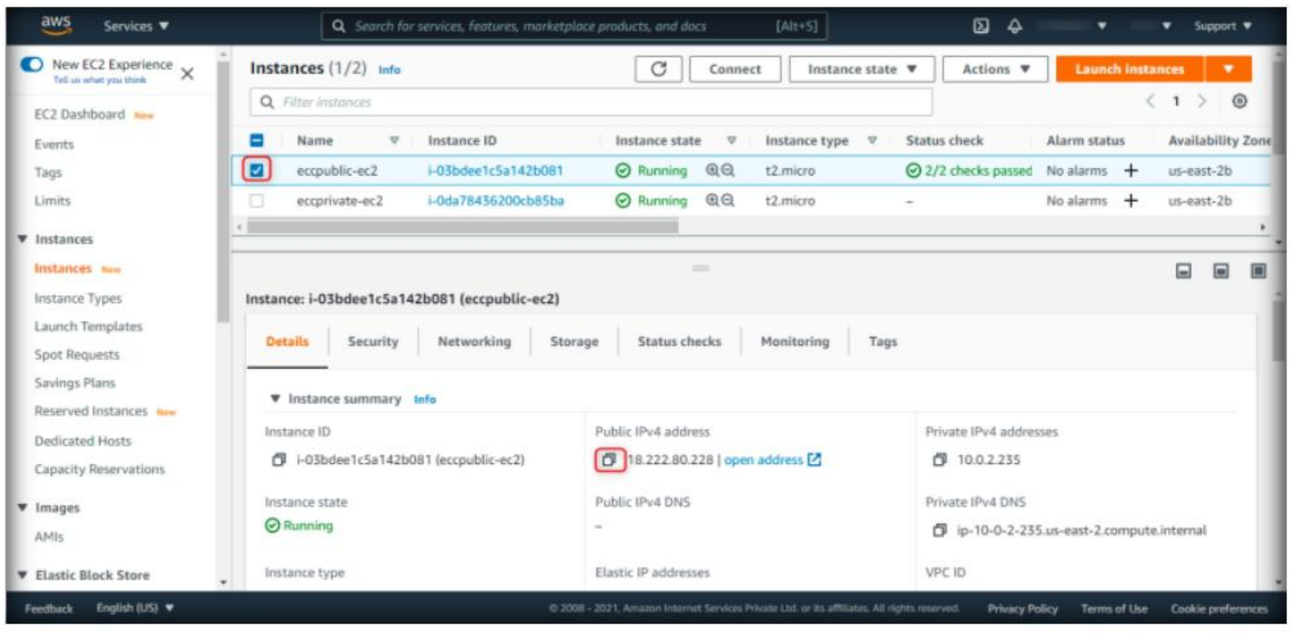


FIGURE 2.3.91: Copying Public IPv4 Address

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

95. Now, type **cmd** in the Windows search box and press **Enter** to open the command prompt.

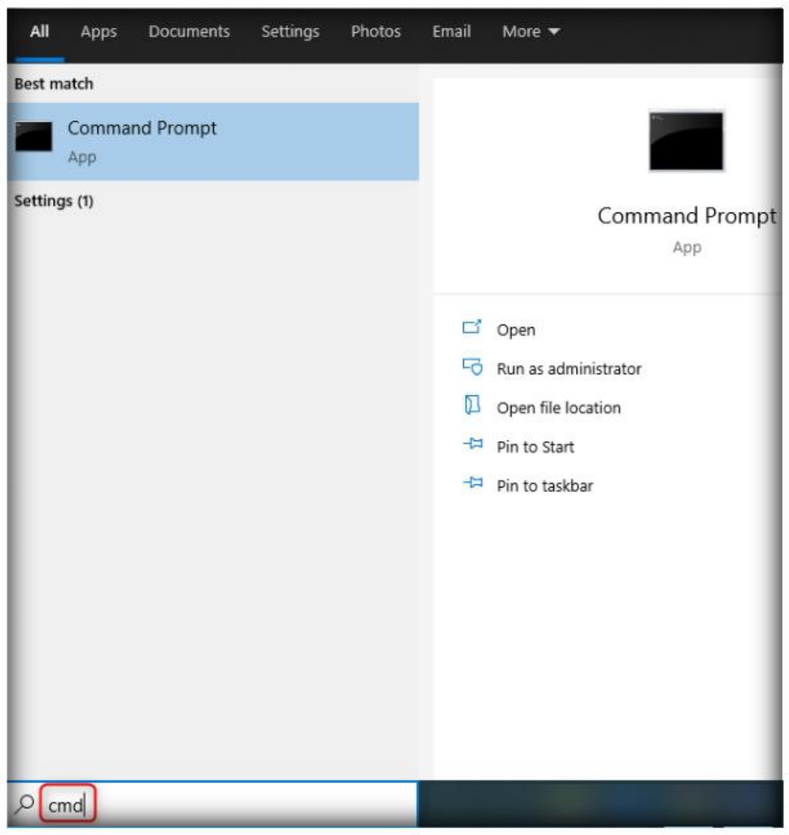


FIGURE 2.3.92: Opening CMD

96. Type the following command and press **Enter** to test access to the public EC2 instance. You will receive a reply, which indicates that there is public access to the instance (**eccpublic-ec2**) in the VPC.

`ping <IP address of the public instance>` **(**Replace <IP address of the public instance> with the IP address of your public EC2 instance.

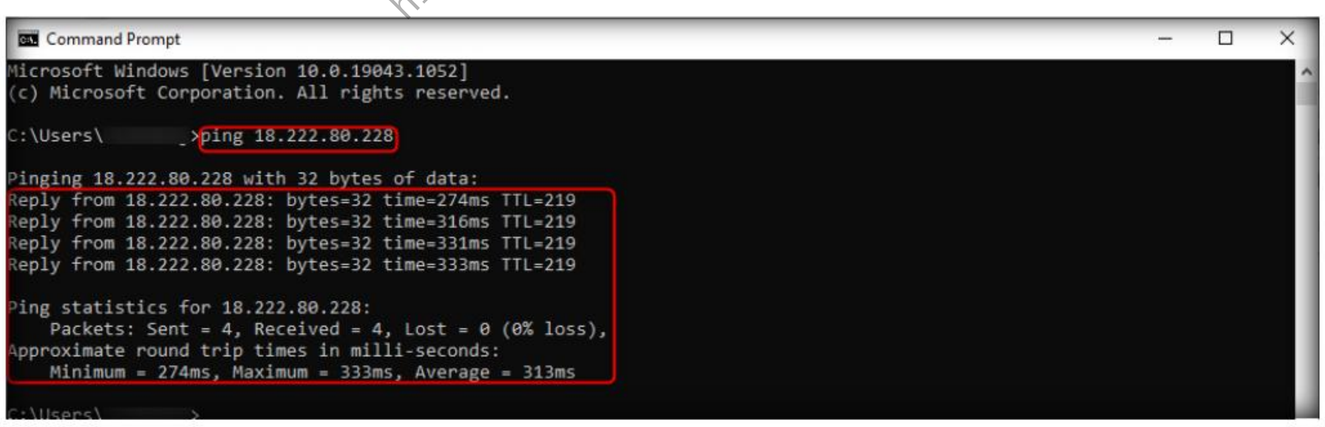


FIGURE 2.3.93: Testing Access to Public Instance

97. Now, go back to the AWS console and select the checkbox for the EC2 instance (**eccprivate-ec2**) in the private subnet. Copy the **Public IPv4 address**.

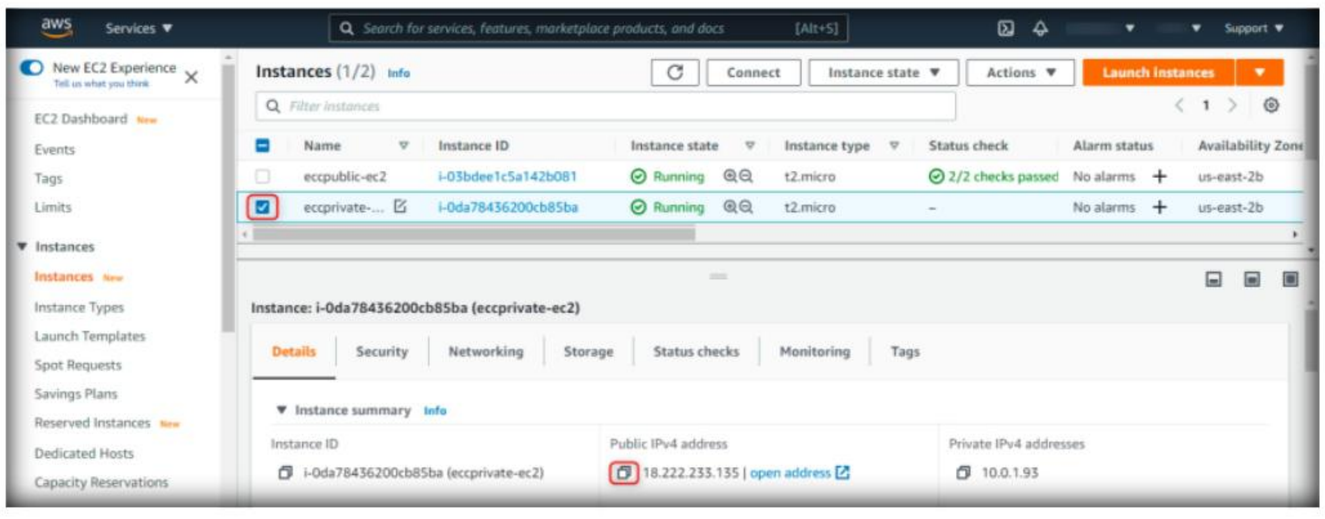


FIGURE 2.3.94: Copying IPv4 Public Address

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

98. Go back to Command Prompt. Type the following command and press **Enter** to test access to the EC2 instance in the private subnet. You will not receive a reply because the instance is in the private subnet.

    `ping <IP address of the private instance>` (Replace <IP address of the private instance> with the IP address of your private EC2 instance.

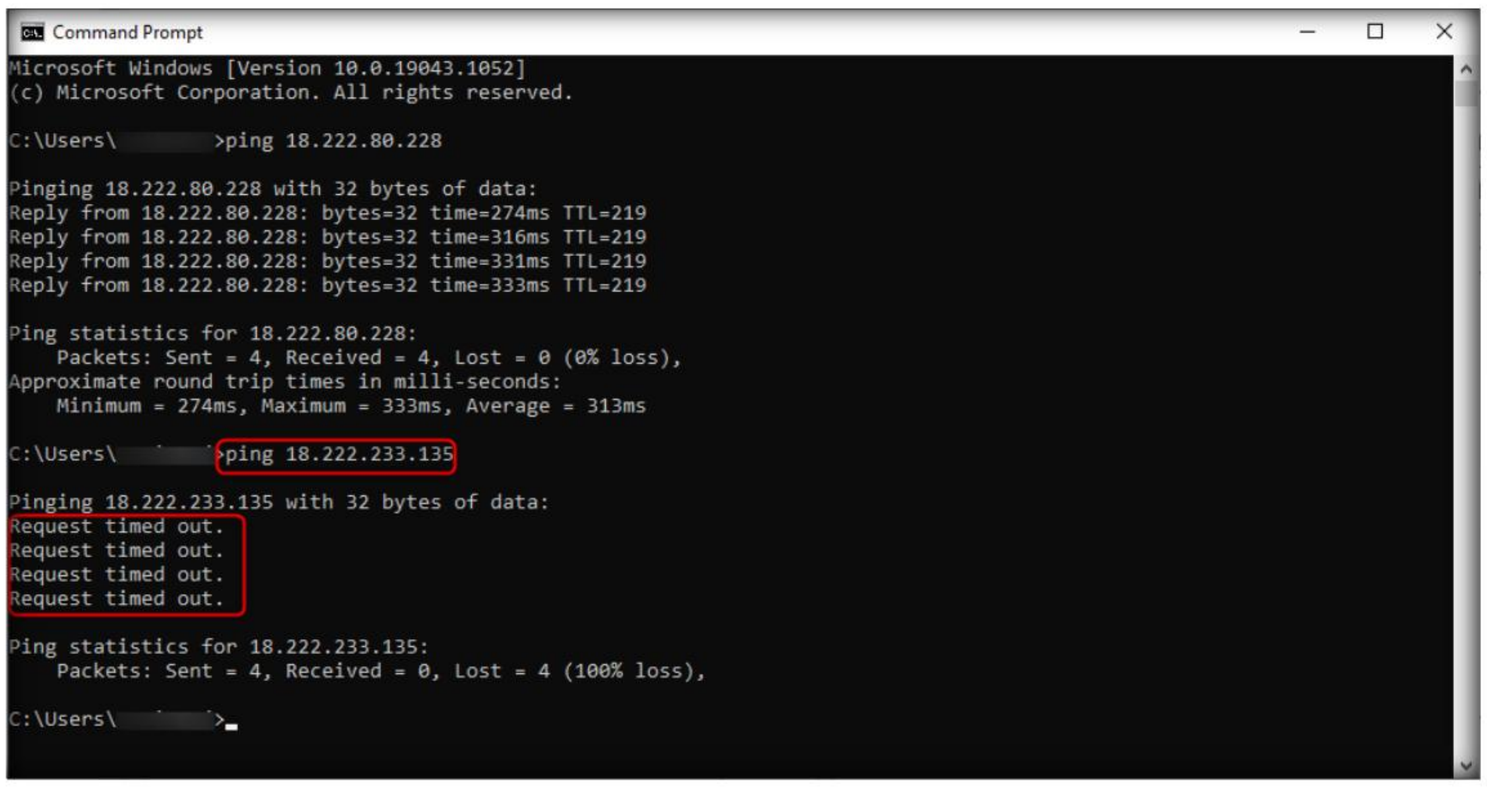


FIGURE 2.3.95: Testing Access to EC2 Private Instance

99. Thus, cloud security engineers can create instances in a VPC by creating a public subnet for instances that are exposed to the internet and private subnet for instances that are isolated from the internet.

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

100. To delete the instances created in this lab, navigate to the **Instances** under EC2 and select the checkbox of the instances created in this lab (here, **eccpublic-ec2** and **eccprivate-ec2**). Select on the **Actions** dropdown and click on **Terminate instance**. In the pop-up window, click on the **Terminate** button.

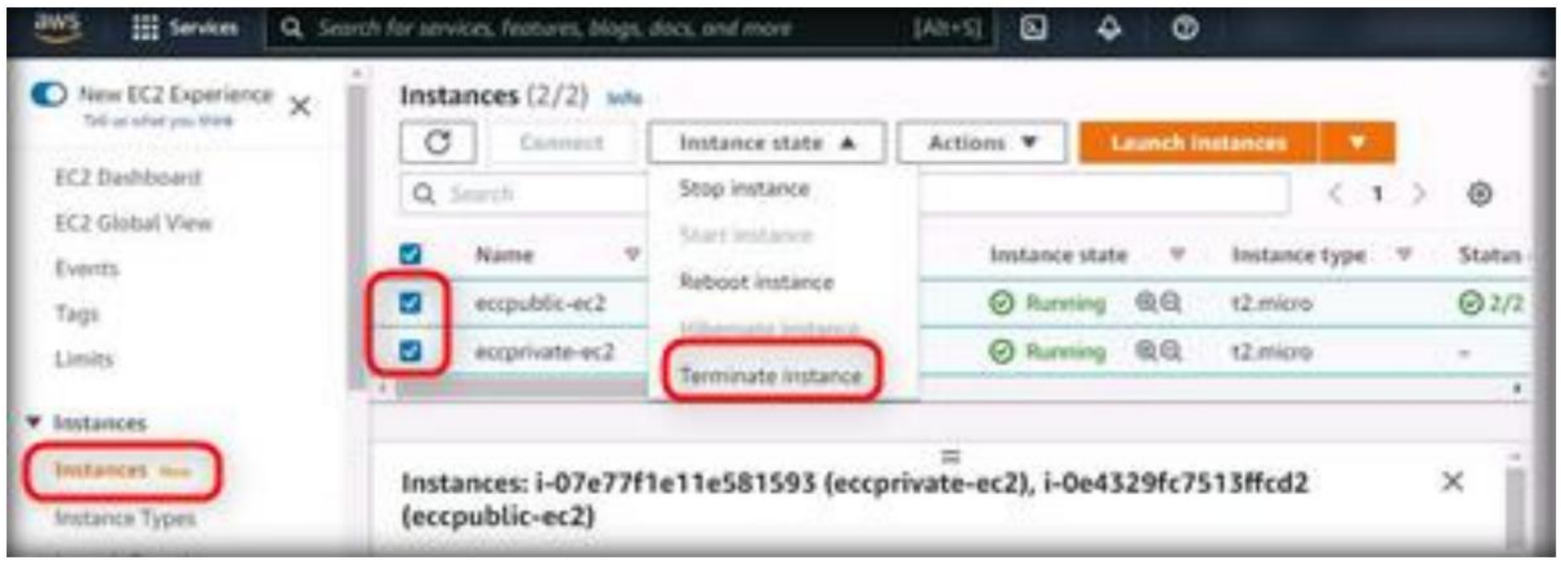


FIGURE 2.3.96: Deleting EC2 Instance

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

101. Navigate to the **Your VPCs** under VPC console and select the checkbox of the instance created in this lab (here, **ecc-demo-vpc**). Select the **Actions** dropdown and click on **Delete VPC**. In the pop-up window, enter delete and click on the **Delete** button. It will delete the Subnets, Route tables, Internet gateways, Network ACLs, and Security groups associated with the VPC.

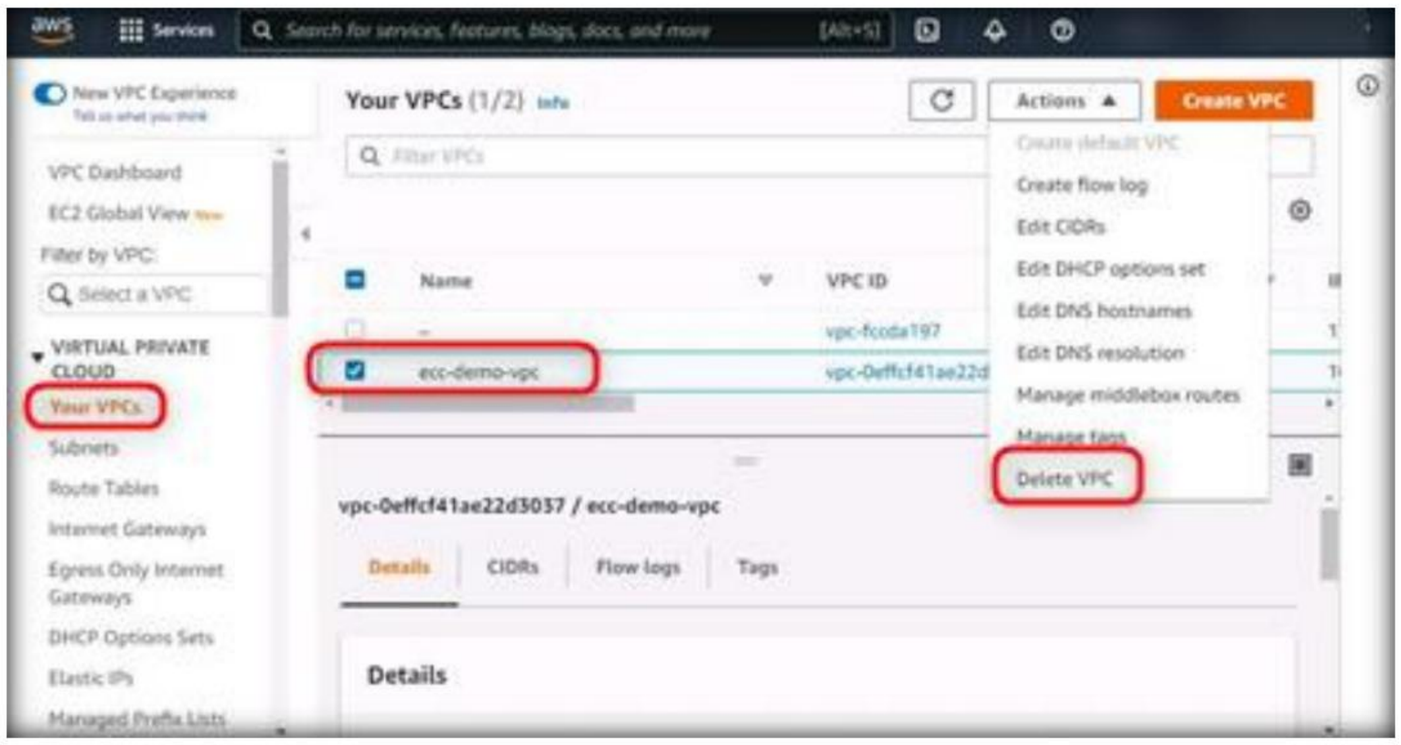


FIGURE 2.3.97: Deleting VPC

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.

hide01.ir

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

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 4

Implementing Role-Based Access Control in Microsoft Azure

RBAC is used to implement the principle of least privilege for a fine-grained granular access control over Azure resources.

ICON KEY

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

Lab Scenario

To implement the principle of least privilege and enforce a fine-grained granular control on Azure resources, you need to assign a role to the new user. Role assignment helps in controlling access to the resources and prevents any accidental or intentional damage to them.

hide01.ir

Lab Objectives

The objective of this lab is to acquaint you with the creation of a new user in Azure Active Directory (AD), and the subsequent assignment of a role to them.

In this lab, you will:

- Create a new user in Azure AD
- Assigning a RBAC role to the user at a subscription level

Lab Environment

To perform this lab, you need the following:

- Admin Machine VM
- Registered Microsoft Azure account

Lab Duration

Time: 10 minutes

Overview of RBAC

Azure role-based access control (RBAC) allows you to manage who can access Azure resources, what they can do with the resources, which areas they are allowed access to,

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

etc. Use built-in roles to segregate duties within the team and grant only the required access to users for their job. If the built-in roles do not meet the requirement of an organization, you can create custom roles for Azure resources. RBAC is used to implement the principle of least privilege for a fine-grained granular access control over your Azure resources.

There are three elements of role assignment: security principal, role definition, and scope.

Security principal: It is an object such as a user, group, or managed identity that needs access to Azure resources. A role can be assigned to any of these security principals.

Role definition: This is used to define a set of actions that you can or cannot perform. Some common RBAC roles are as follows:

- **Owner**: The owner can access all resources in Azure and delegate access to other users.
- **Contributor**: A contributor can access all resources in Azure but cannot delegate control to other users.
- **Reader**: A reader can only view the resources in the Azure environment.
- **User access administrator**: A user access administrator will provide permissions to manage access to Azure resources.

hide01.ir

You can assign a high-level role, such as an owner, or a specific role, such as a virtual machine reader.

Scope: This denotes a set of resources to which access is granted. By defining the scope, you can limit the actions of an assigned role. A scope in Azure can be specified at four levels: management group, subscription, resource group, and resource.

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 an Azure Free Account using the following link: https://azure.microsoft.com/free. 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.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1

Creating New User in Azure AD

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

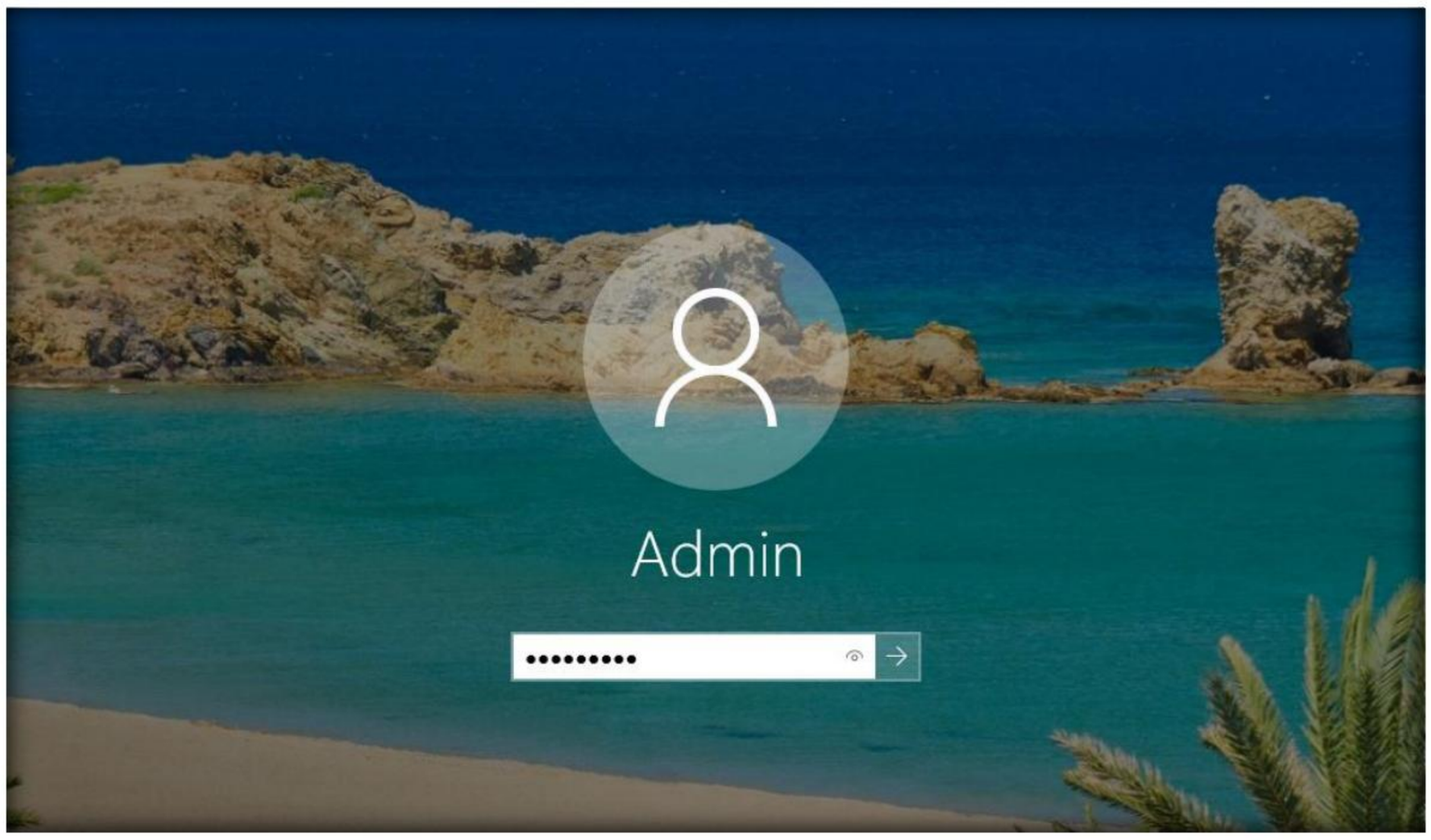


FIGURE 2.4.1: Launch Admin Machine and Log in

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



FIGURE 2.4.2: Navigating to the Chrome Browser from Taskbar

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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

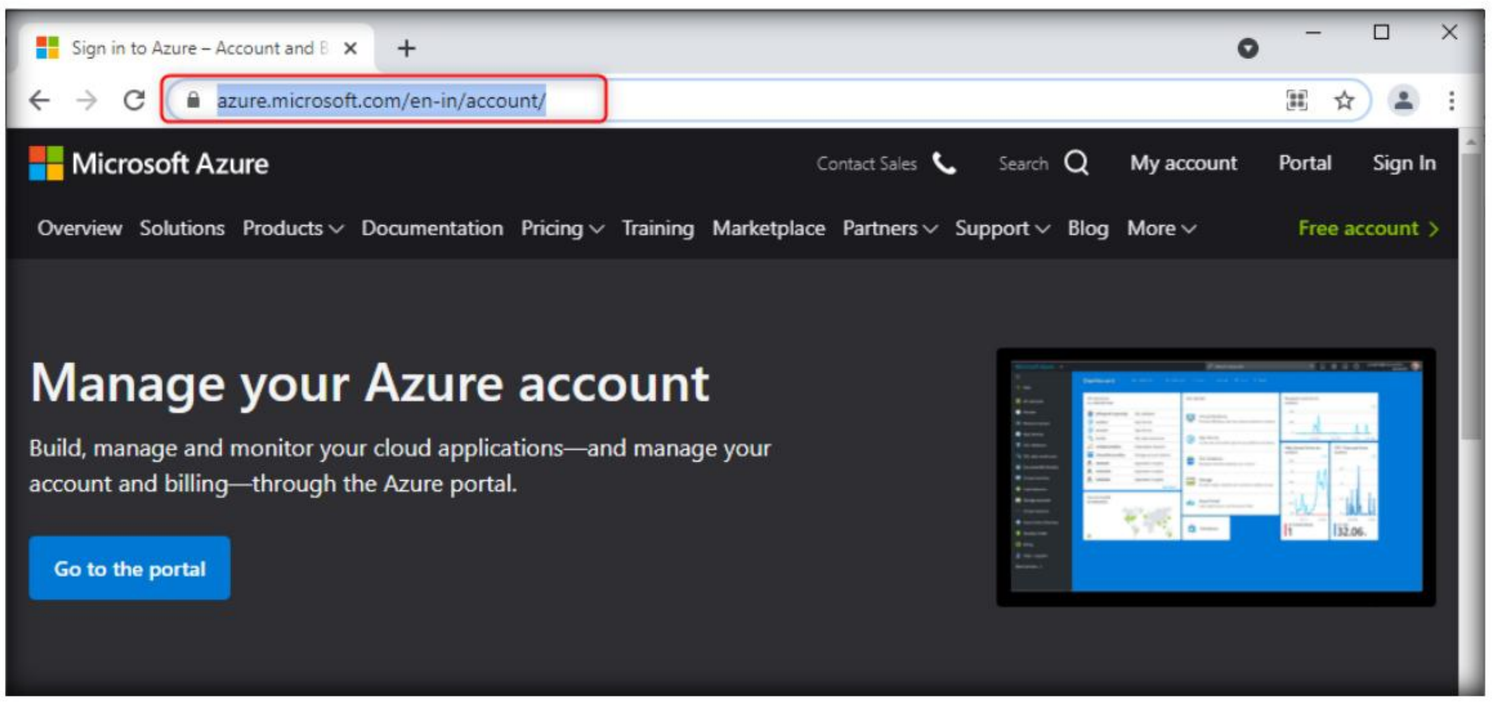


FIGURE 2.4.3: Enter the URL of Microsoft Azure

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

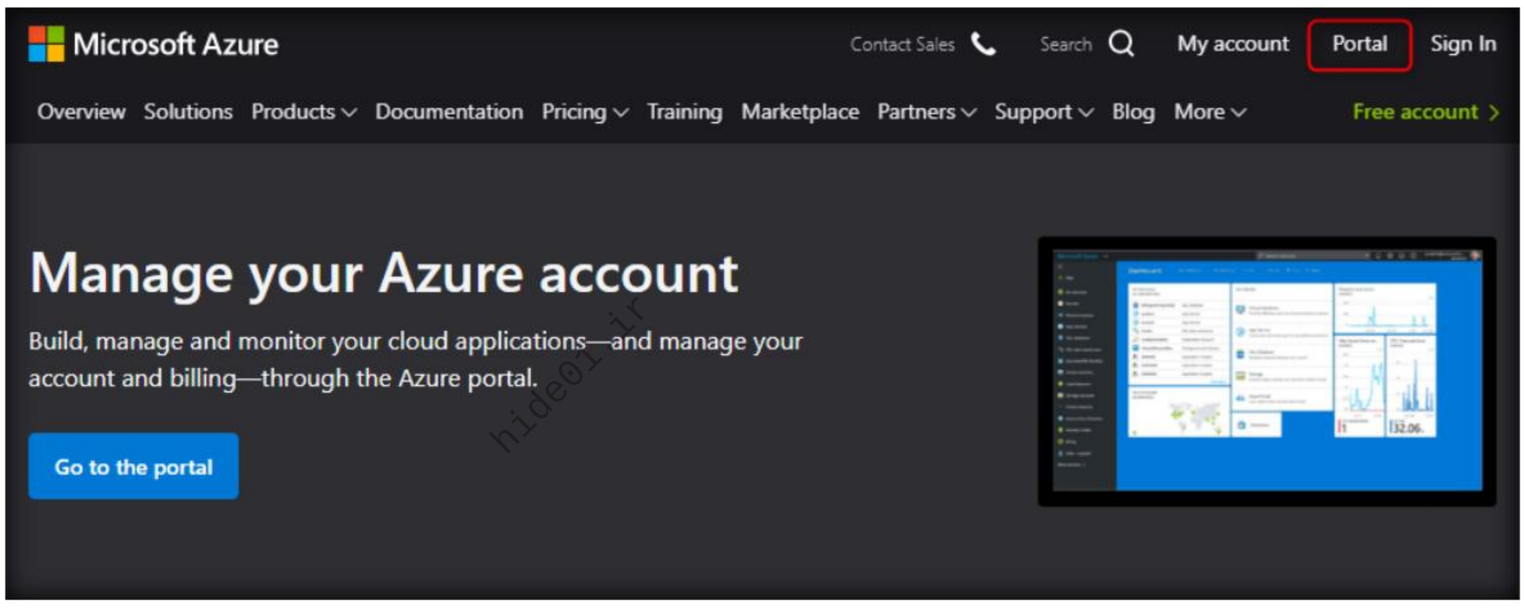


FIGURE 2.4.4: Sign into the Azure Portal

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

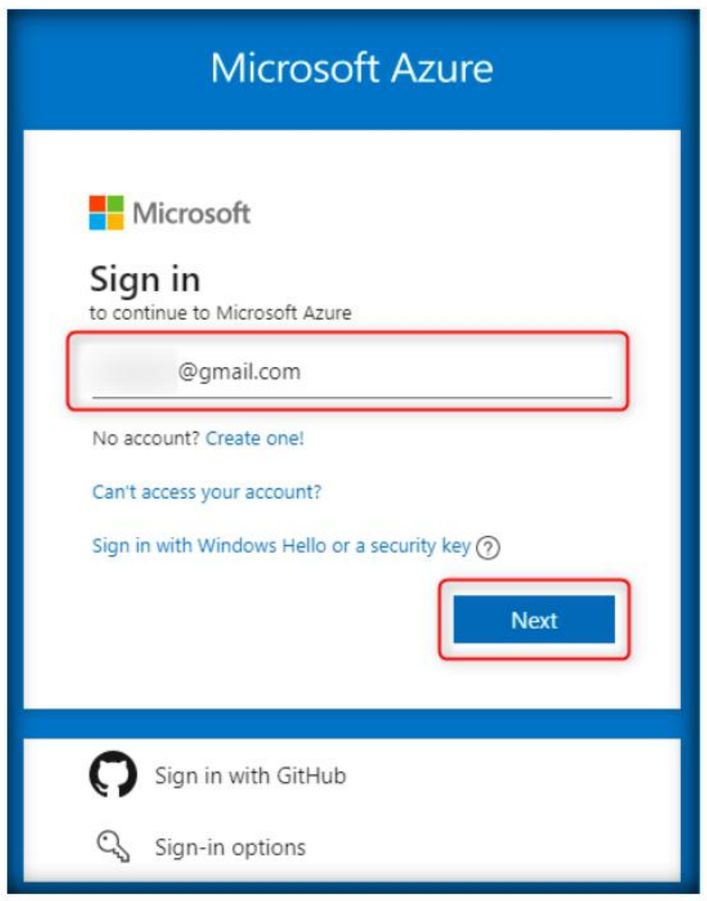


FIGURE 2.4.5: Enter Account ID to continue

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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

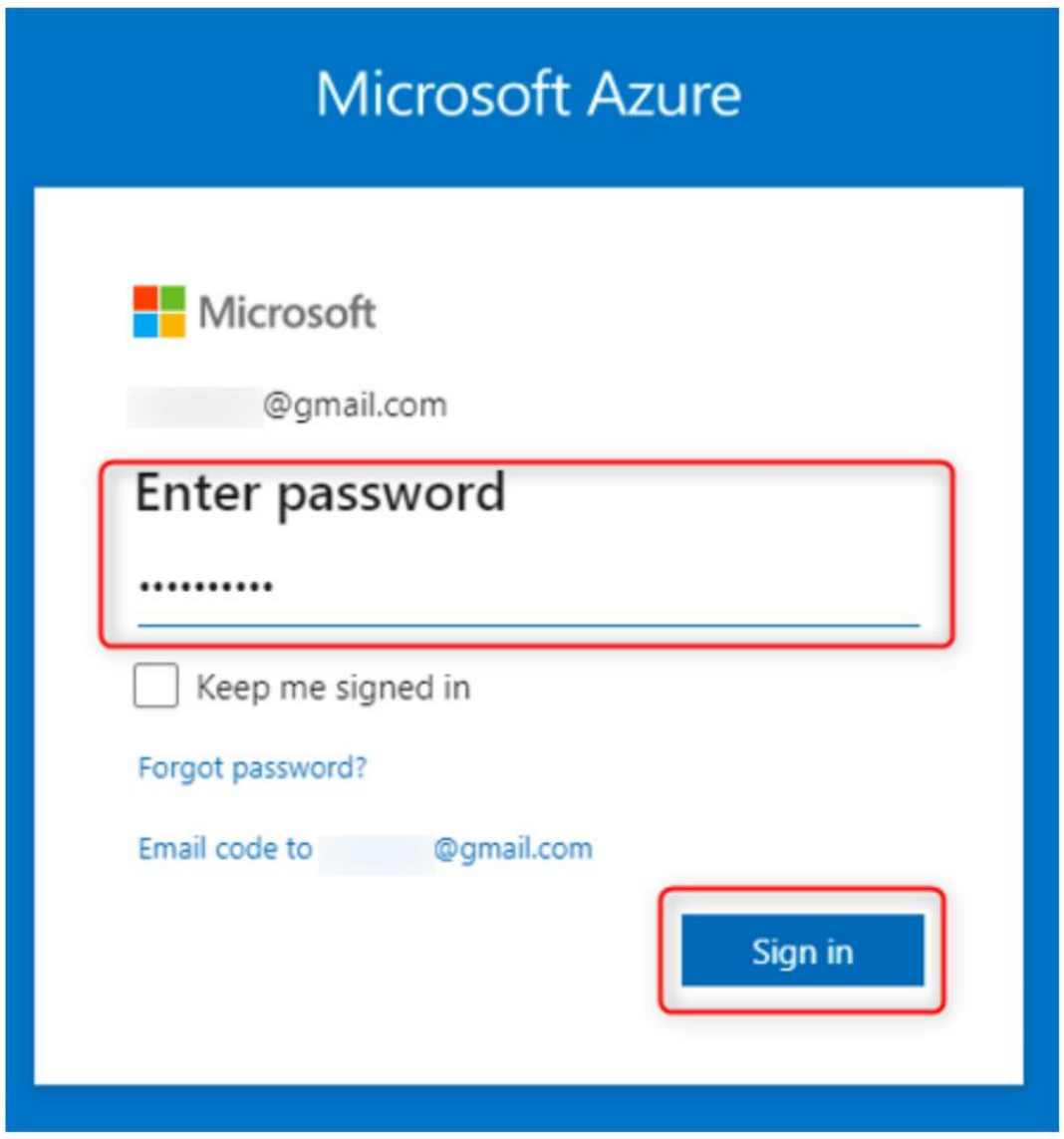


FIGURE 2.4.6: Enter the Log In Password

7. You will be successfully logged into the **Microsoft Azure portal.**

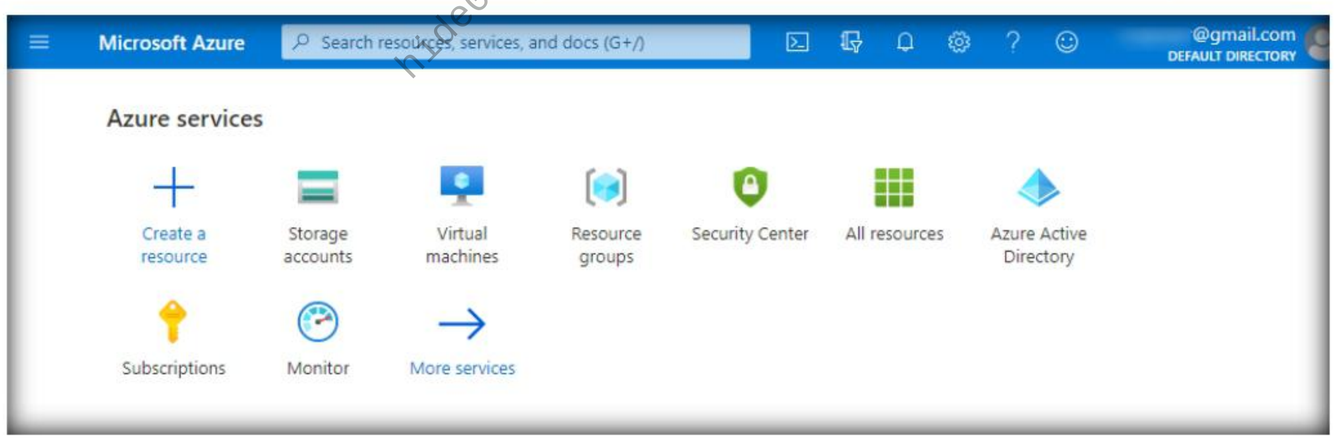


FIGURE 2.4.7: Microsoft Azure Portal

8. Click on the left pane. Then, navigate to and click on **Azure Active Directory**.

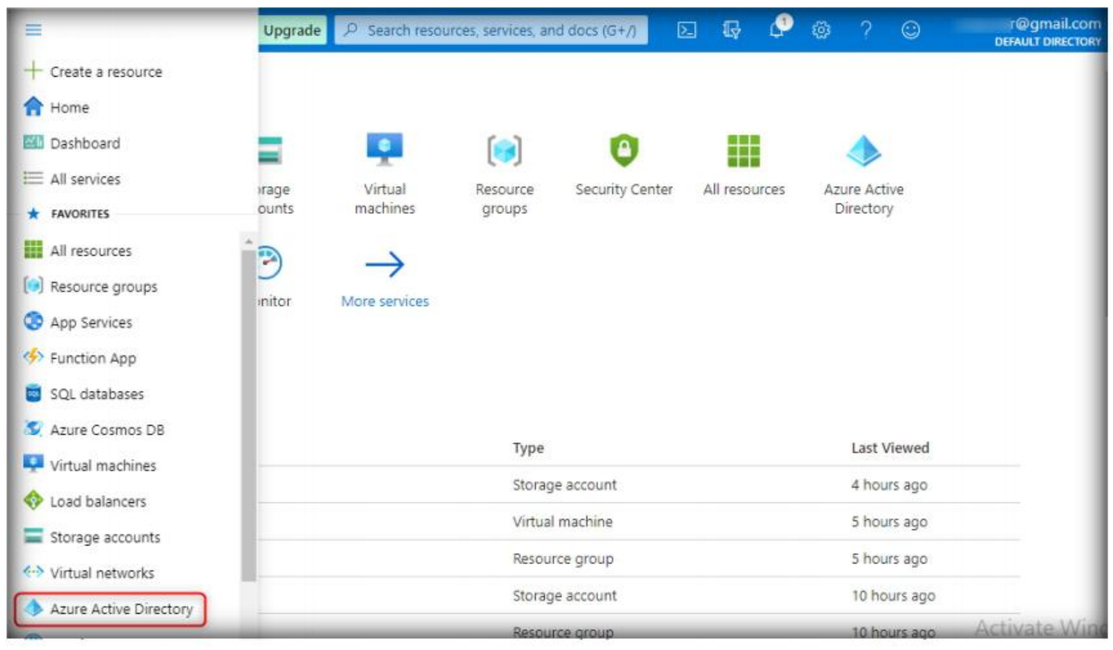


FIGURE 2.4.8: Selecting Azure Active Directory

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

9. On the left pane of the **Default Directory** page, click on **Users** under **Manage**.

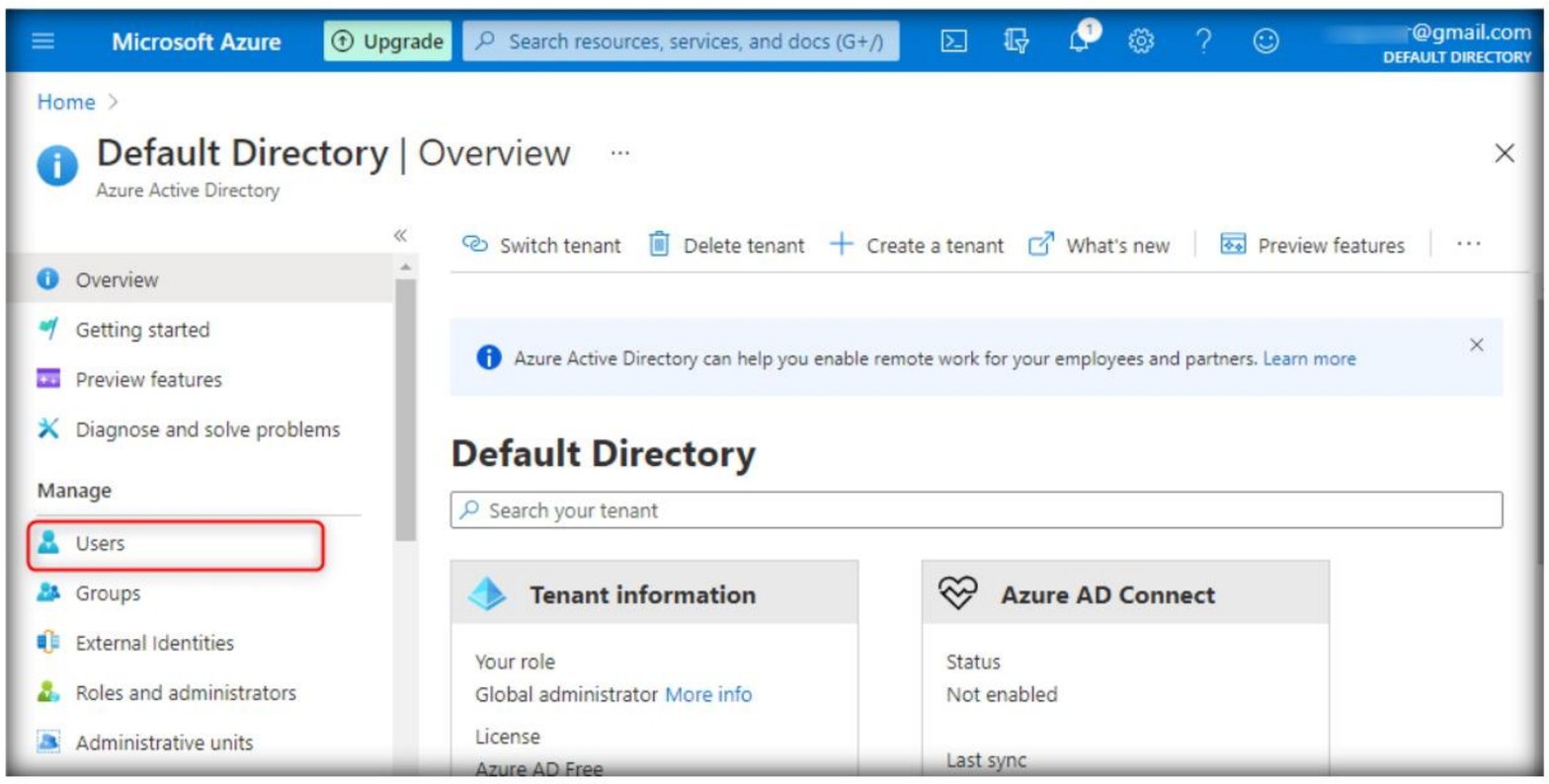


FIGURE 2.4.9: Selecting Users in Azure AD

10. Click on **+ New User**.

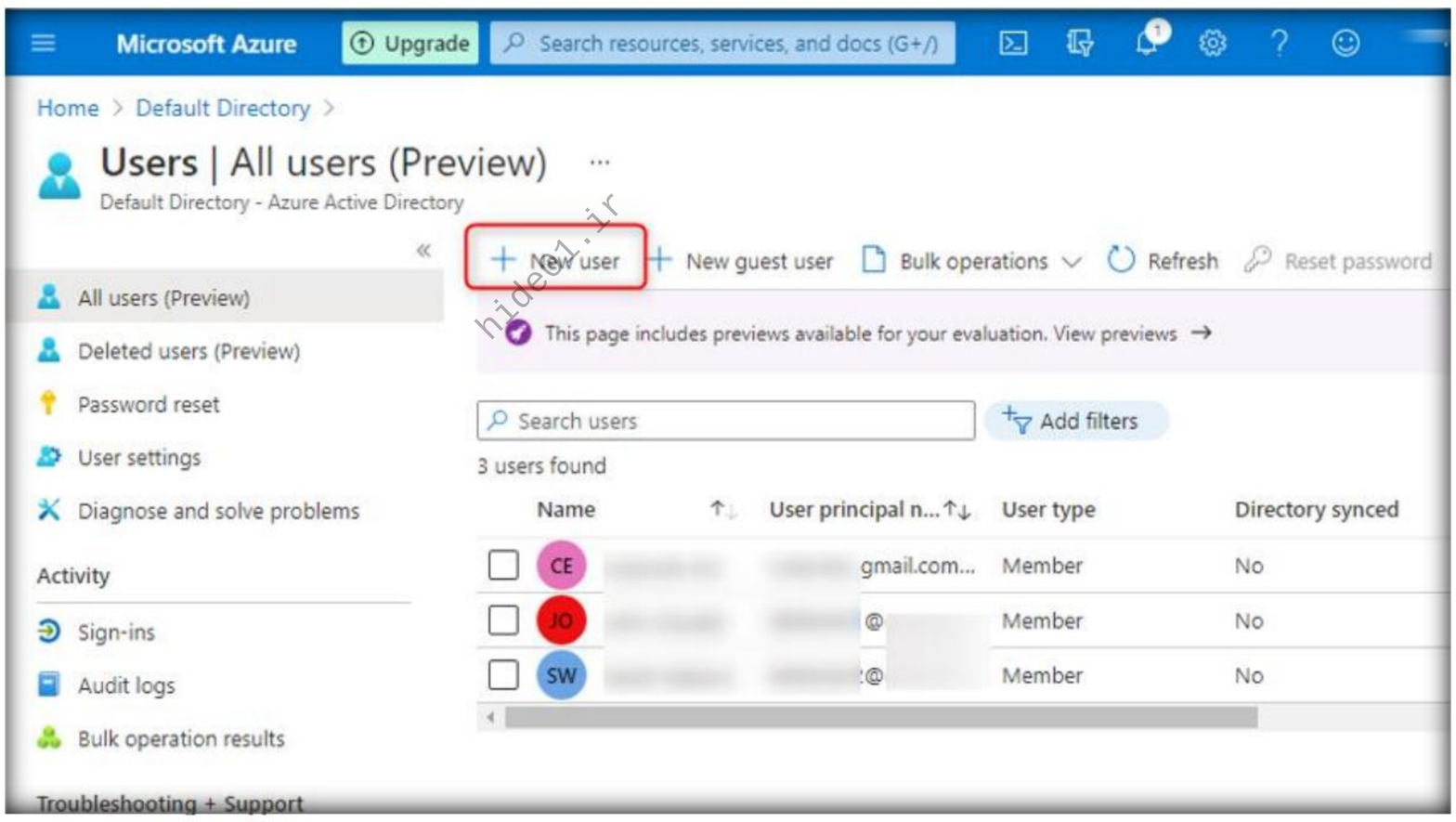


FIGURE 2.4.10: Creating New user

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

11. Check the **Create user** radio button.

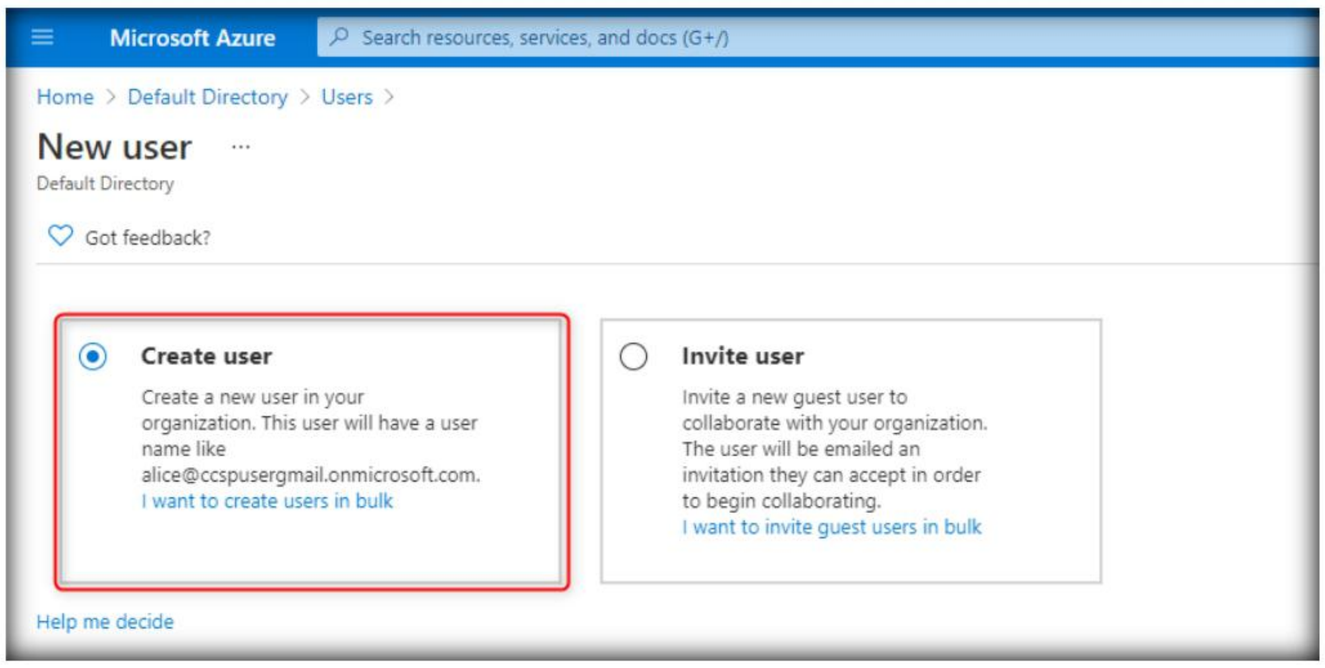


FIGURE 2.4.11: Selecting the Create user radio button

12. Under **Identity**, enter the user details.

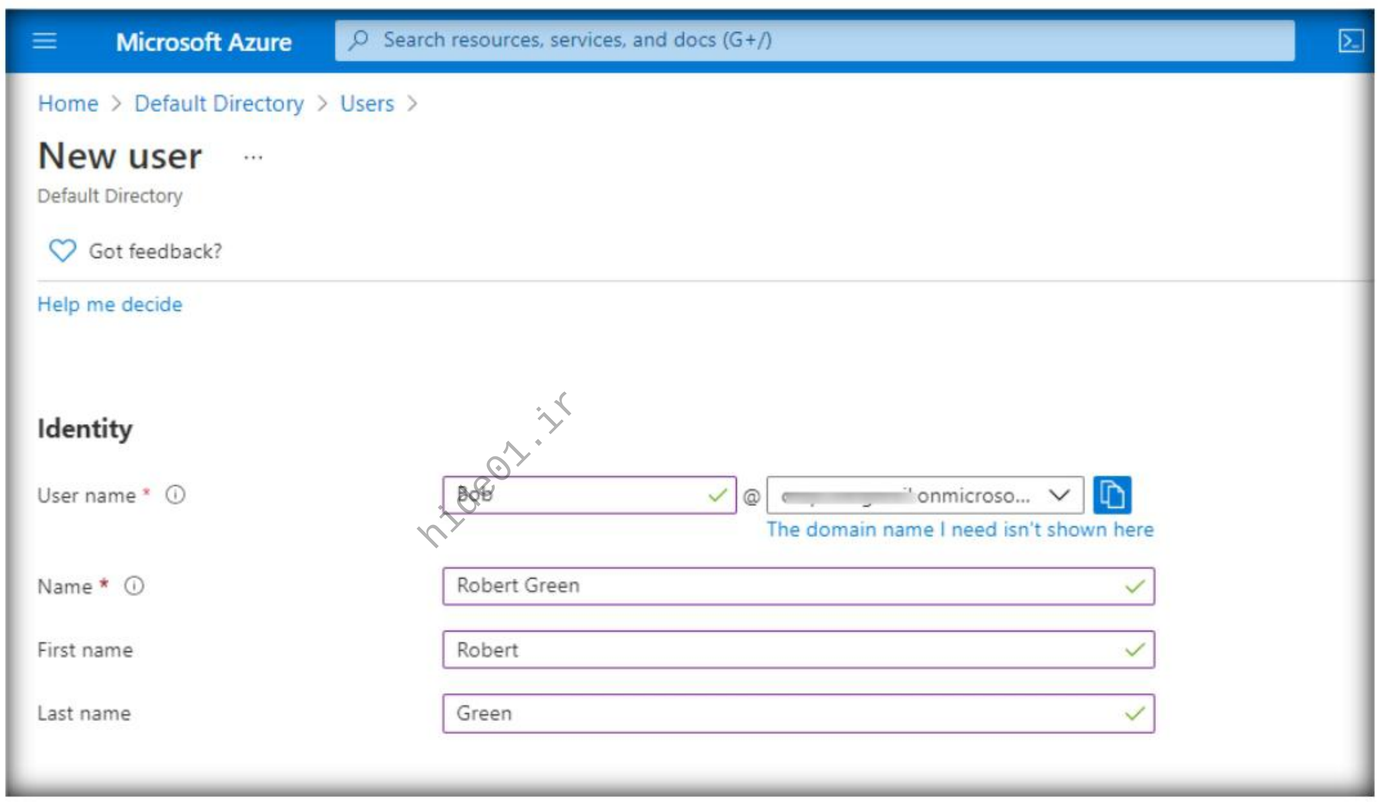


FIGURE 2.4.12: Entering User Details

13. Under the **Password** section, check the **Let me create the password** radio button and enter a password in **Initial password**.

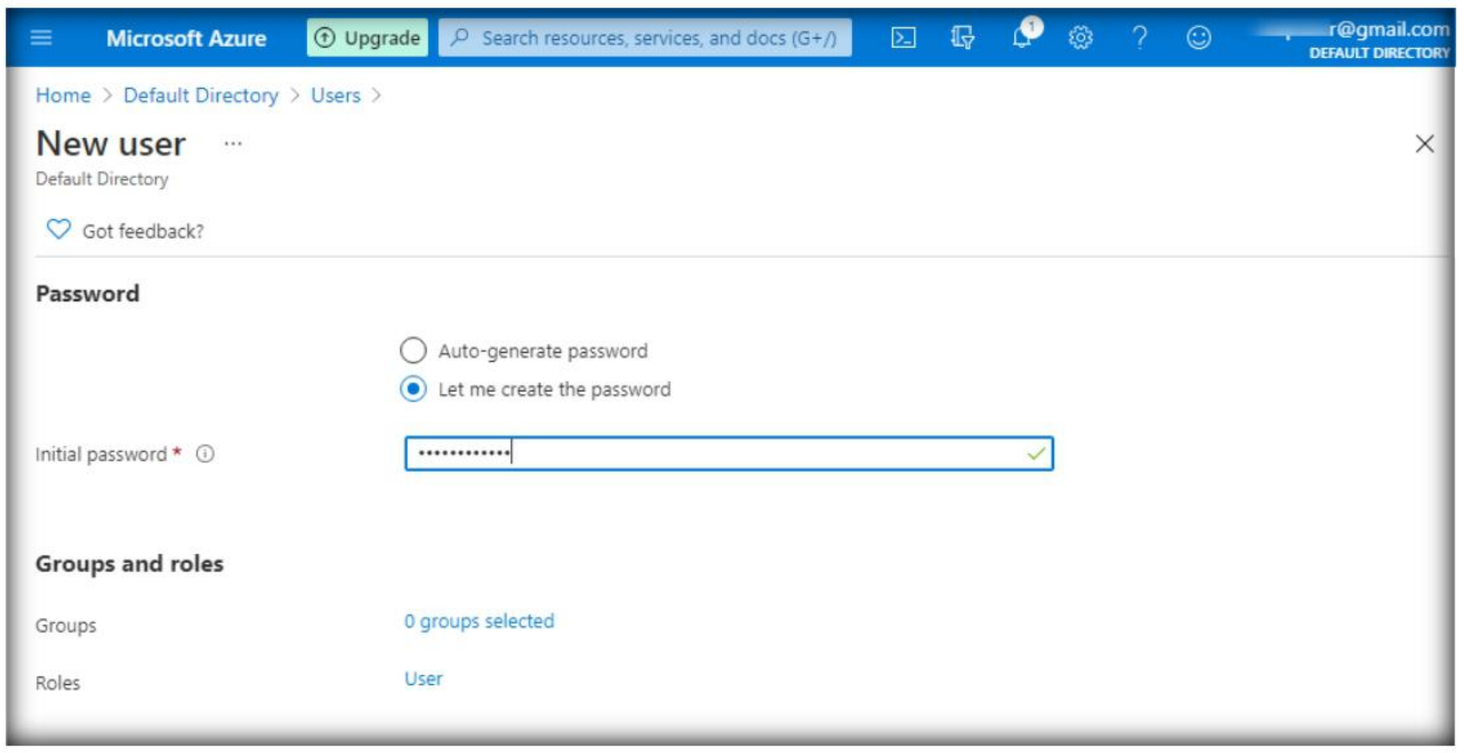


FIGURE 2.4.13: Creating a Password

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

14. Leave **Settings** section in its default state. In the **Job info** section, enter the **Job title**, **Department**, and **Company name**. Then, click on the **Create** button.

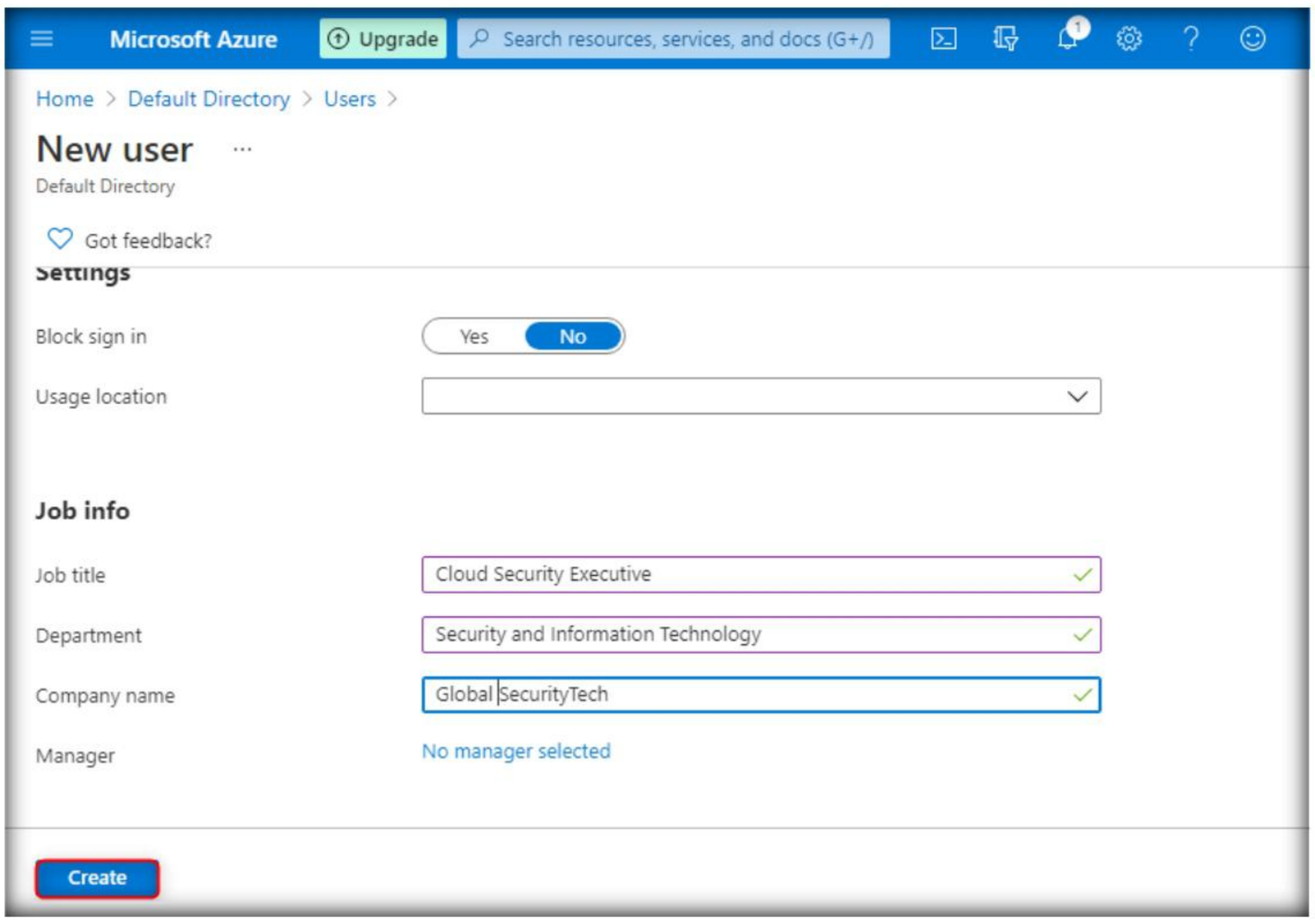


FIGURE 2.4.14: Entering Job Information of the User

15. The new user is successfully created in the Azure AD.

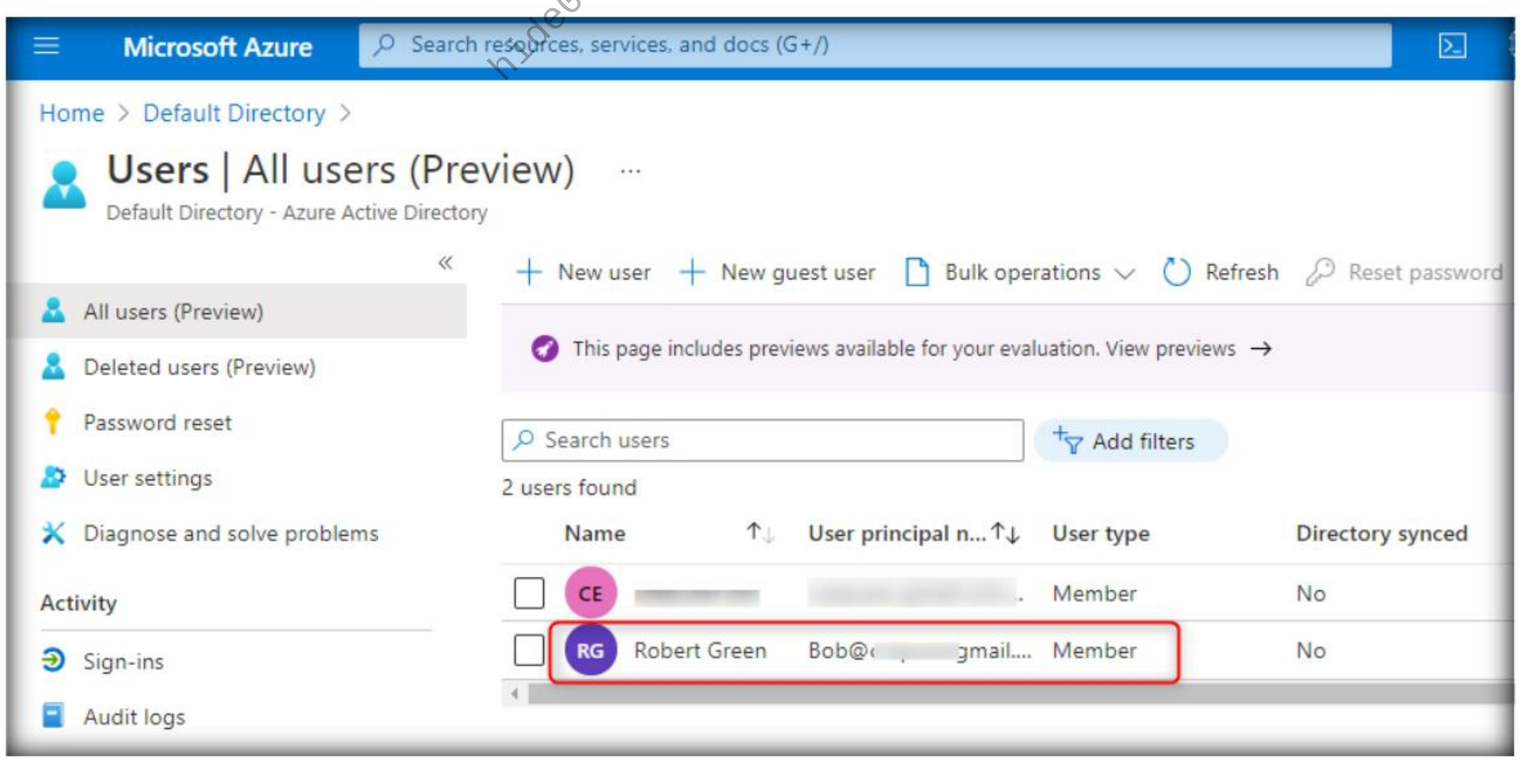


FIGURE 2.4.15: Successfully Creation of a New User

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 2

Assigning RBAC Role to the User

16. Go back to Azure portal, click on the **Free Trial** Subscription or type **Free Trial** in the Azure **Search** box, and then click on **Free Trial** under **Recent resources**.

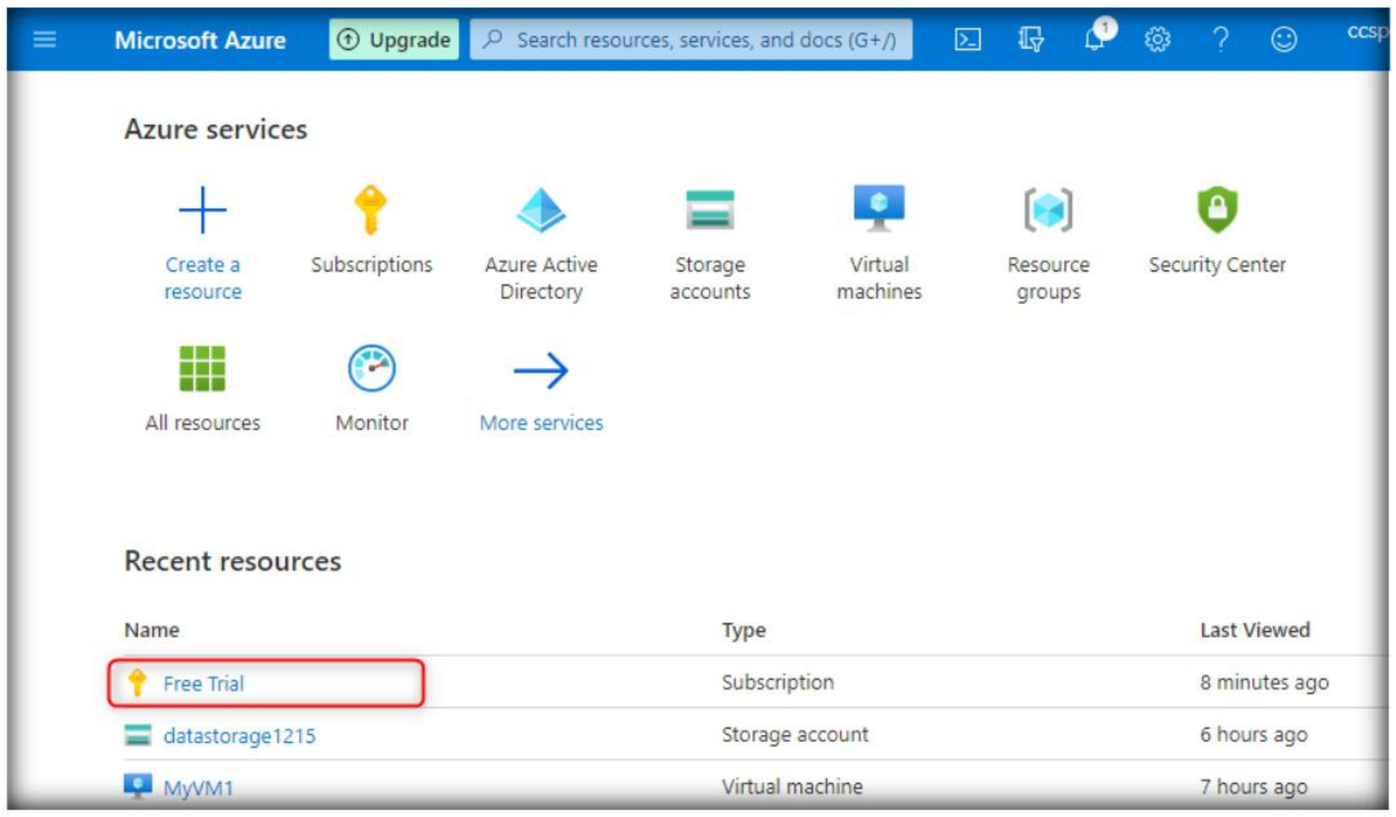


FIGURE 2.4.16: Azure Dashboard

17. In the **Free Trial** window, navigate to and click on **Access control (IAM)** on the left pane.

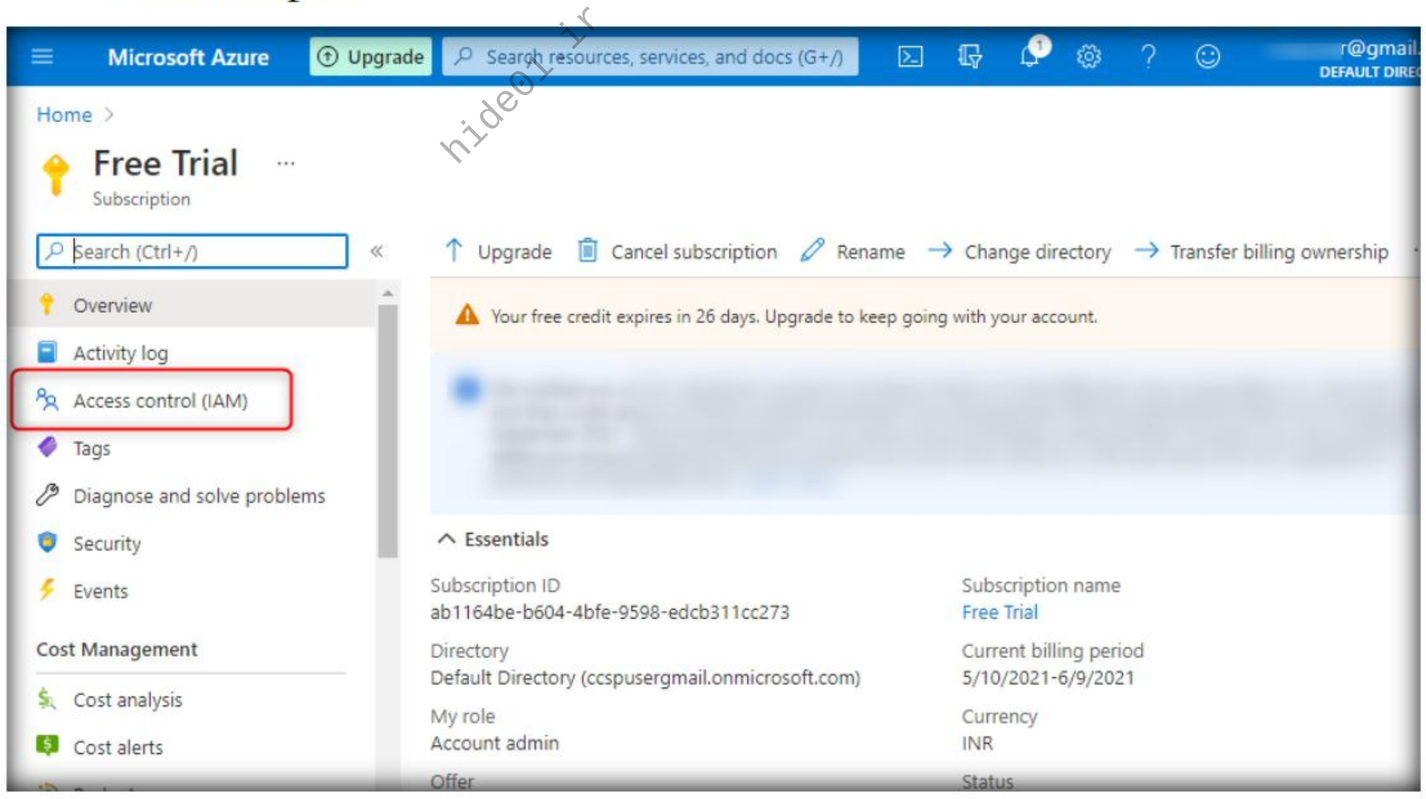


FIGURE 2.4.17: Selecting IAM in Free Trial Window

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

18. Then, click on the **Role assignments** tab. You will observe that no roles have been assigned.

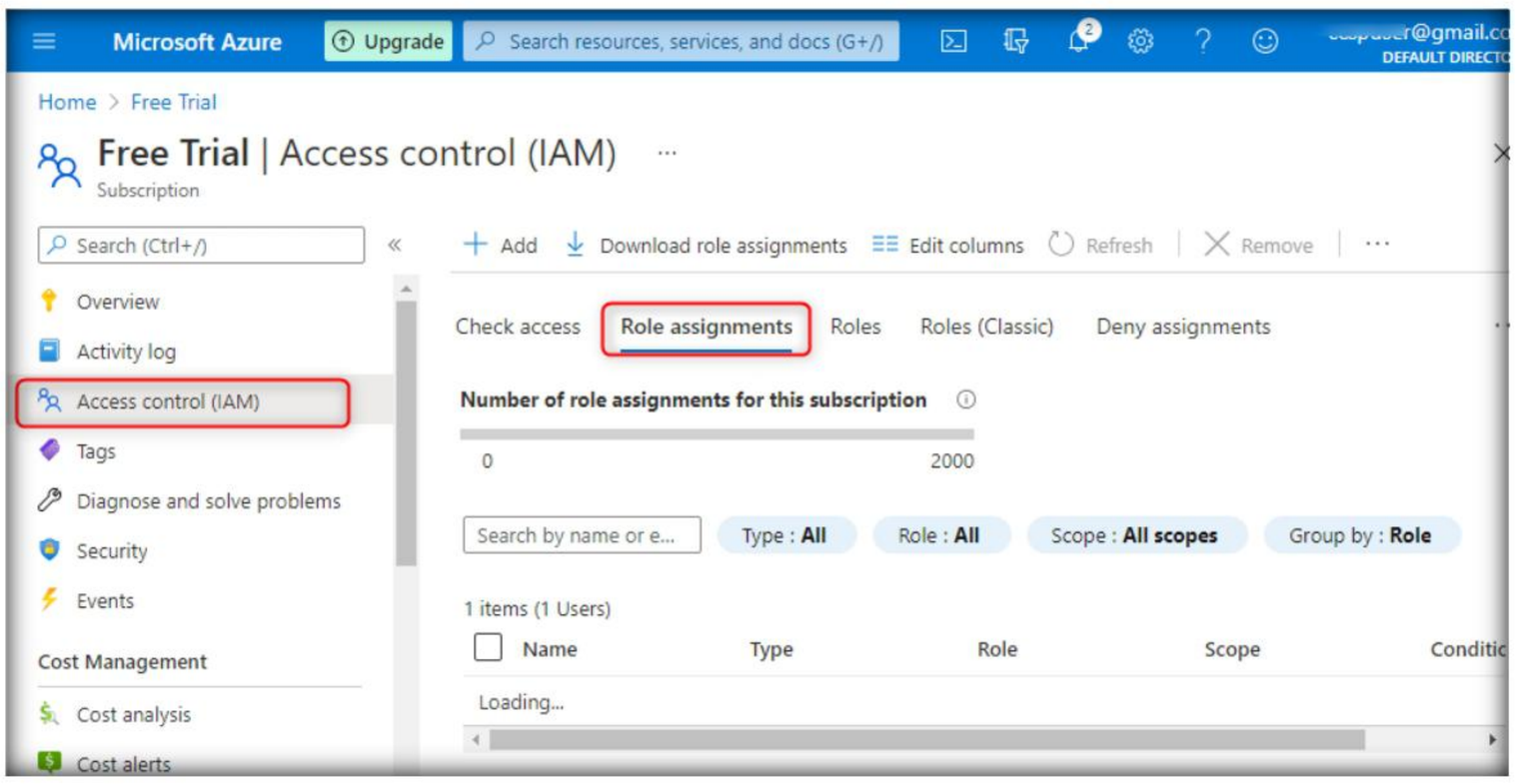


FIGURE 2.4.18: Checking Role assignments

19. Click on **Add**, and then click on **Add role assignment** from the dropdown.

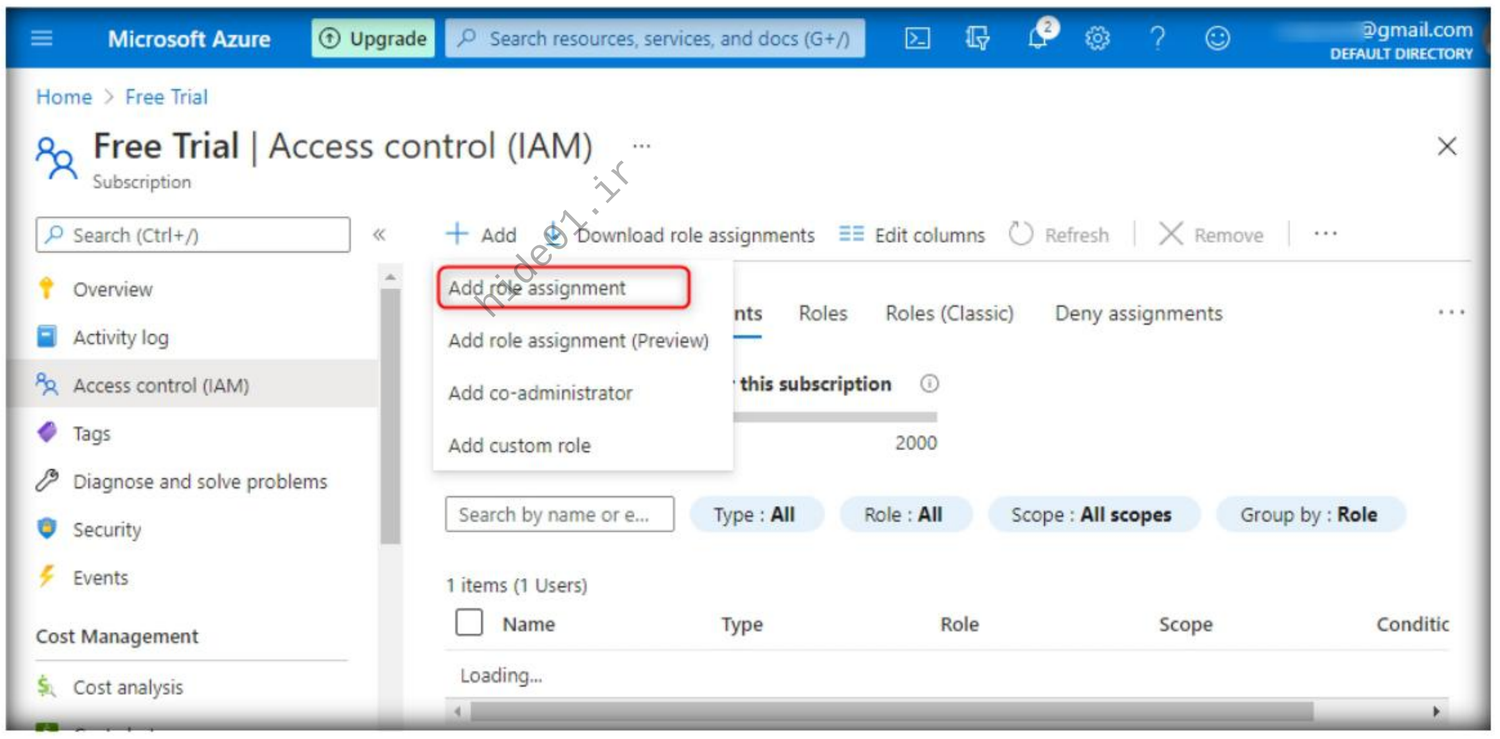


FIGURE 2.4.19: Selecting Add Role Assignment

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

20. In the right side of the **Add role assignment** pane, select the **Role** as **Owner.** In the **Assign access to** field, select **User, group, or service principal**. In the **Select** field, you can select the user to whom you would like to assign the role.

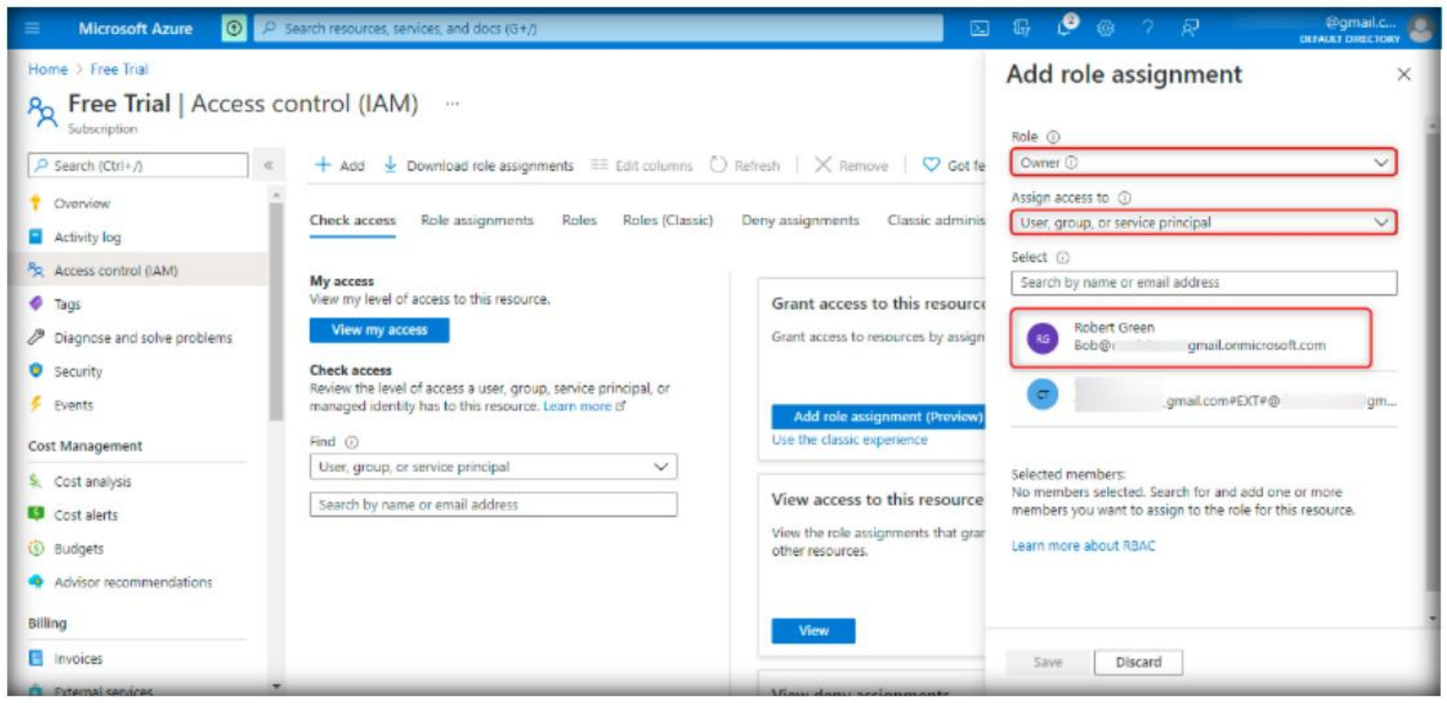


FIGURE 2.4.20: Entering Details Related to Role, Assign Access to, and Selecting the User

21. Click the **Save** button.

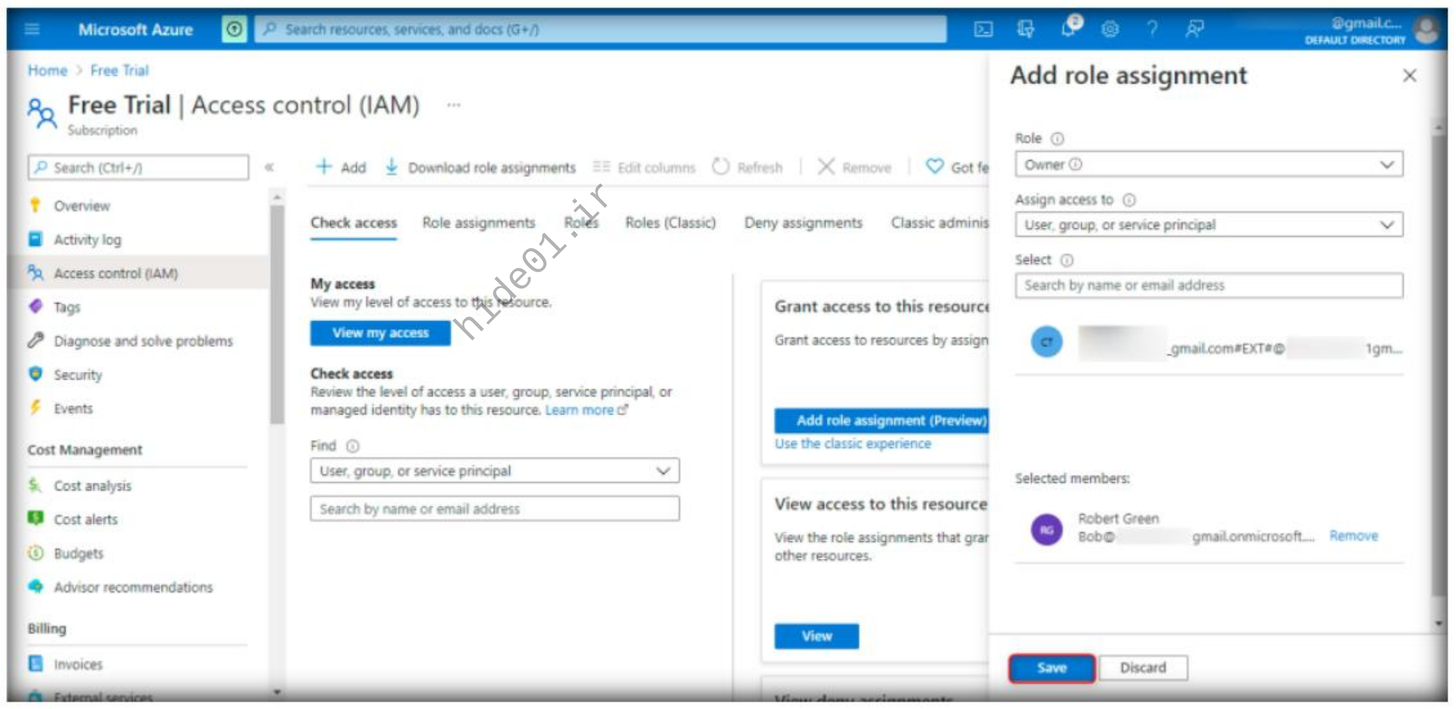


FIGURE 2.4.21: Saving added role assignment

22. Click on the **Role assignments** pane. RBAC Role (Owner) is successfully assigned to the user.

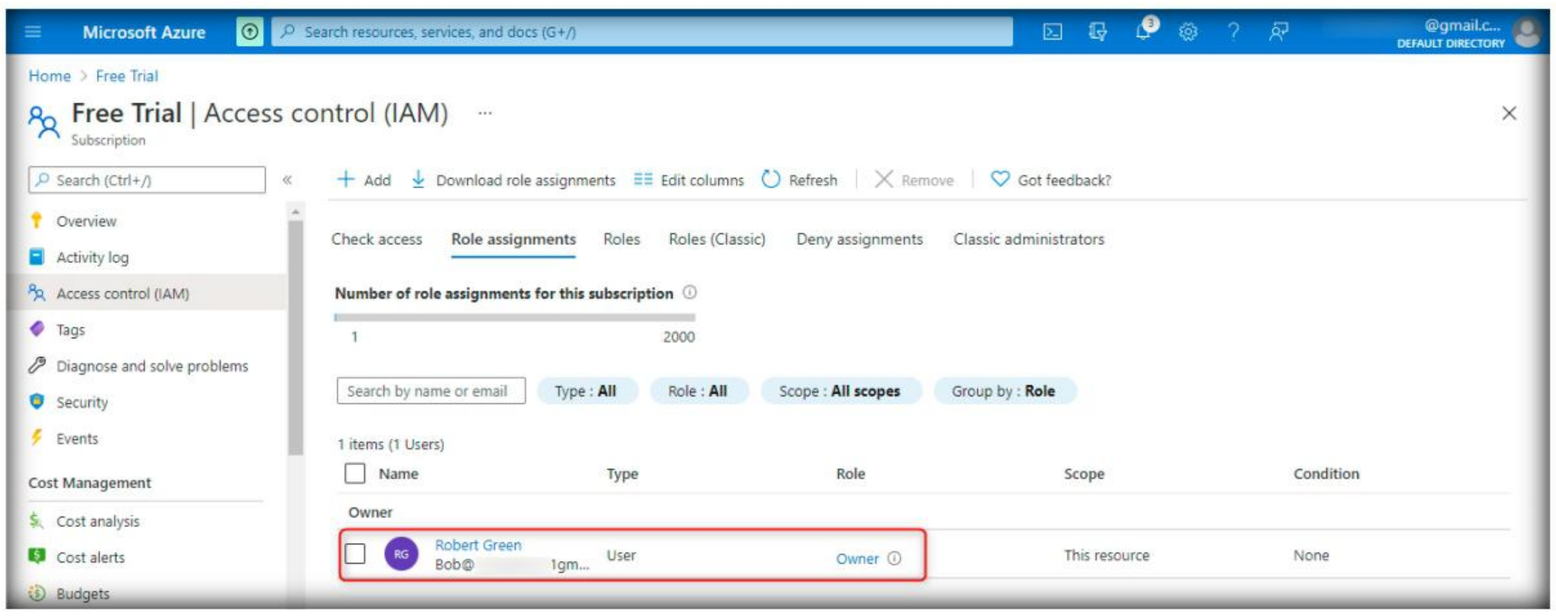


FIGURE 2.4.22: RBAC Role is Successfully Assigned to the New User'

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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

23. To delete the user (Bob) created in this lab, in the Azure portal, navigate and click on Azure Active Directory. Click on **Users** under **Manage** on the left pane. Click on the user's name (Robert Green)) to view the user profile. Click on **Delete** at the top.

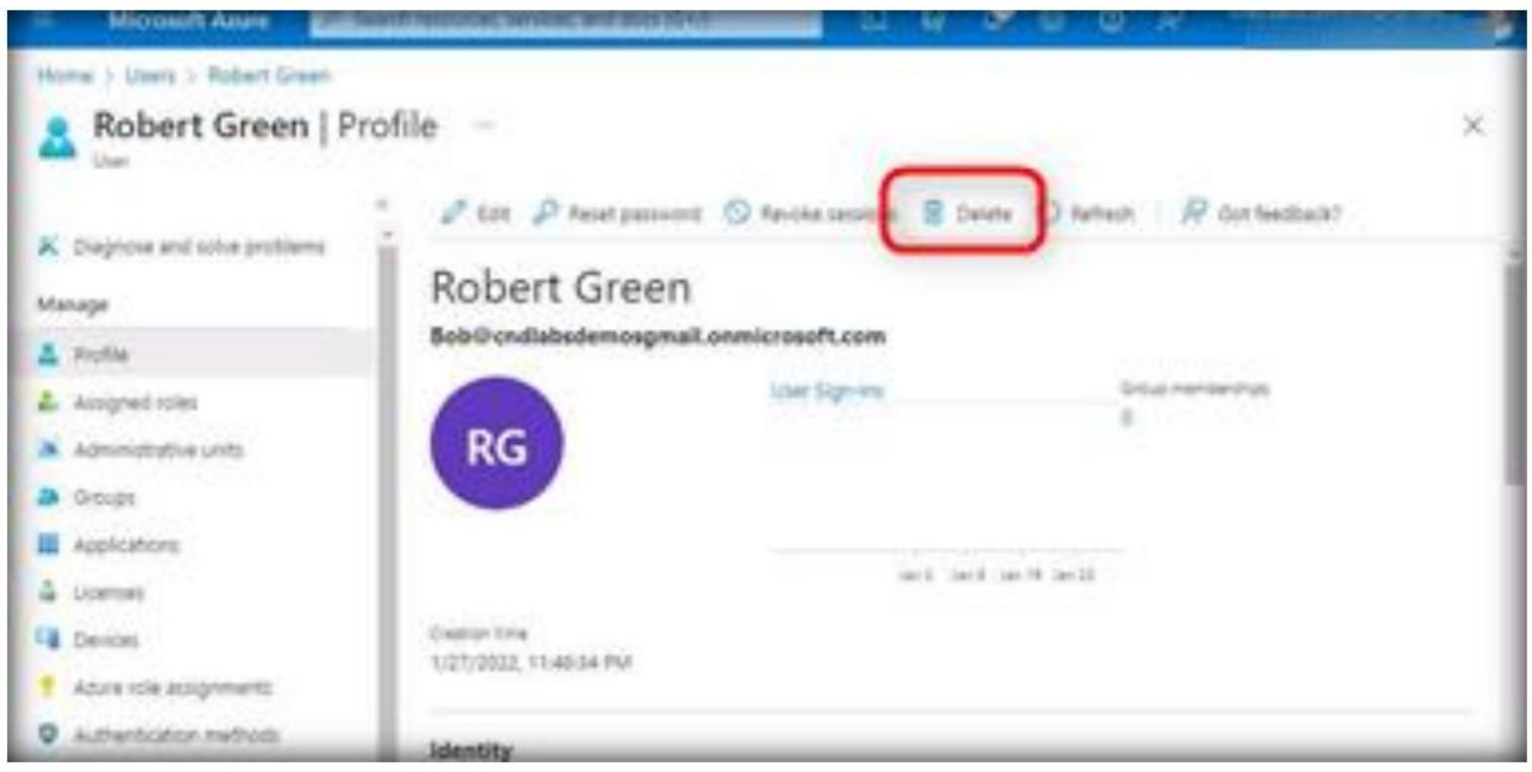


FIGURE 2.4.23: Deleting User

Lab Analysis

hiu01.ir

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.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 5

Deploying a Secure Windows Server VM in Azure with Antimalware Extension Enabled

Azure Antimalware is a free real-time antimalware provision to safeguard the Azure ecosystem against malware.

ICON KEY

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

Lab Scenario

Azure antimalware helps identify and remove viruses, spyware, and malicious software and send alerts whenever an unwanted or known malicious software tries to install or run in the Azure environment. To protect the virtual machine against viruses, spyware, and malicious software, the cloud security engineer should add the antimalware extension when deploying the virtual machines. In this lab, you will learn how to deploy a secure Microsoft Windows Server VM with Antimalware Extension enabled.

Lab Objectives

From this lab, you will learn how to deploy a Windows Server virtual machine from the Azure portal, how to add the Antimalware Extension while deploying the virtual machine, and how to check the version of the Antimalware extension.

In this lab, you will:

- Deploy a windows server VM with Antimalware extension enabled
- Verify the deployment

Lab Environment

To perform this lab, you need the following:

- Admin Machine VM
- Registered Microsoft Azure account.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Duration

Time: 10 minutes

Overview of Antimalware Extension

The threat landscape in the cloud environment has been increasing at a rapid pace, and this has been building tremendous pressure on cloud consumers to implement effective protection to meet the security and compliance requirements.

Microsoft Azure provides a free real-time antimalware provision to safeguard the Azure ecosystem against malware. Azure Antimalware helps in identifying and removing viruses, spyware, and malicious software. It will send alerts whenever an unwanted or known malicious software tries to install or run in the Azure environment. Microsoft Azure Antimalware runs in the background without human intervention. Add Microsoft Azure antimalware extension while deploying the VM to protect the VM against malware. The target VM should be connected to the internet to receive signature and regular engine updates.

The Cloud Security Engineer can enable the Antimalware in Azure environment for VMs and Cloud Services by using the following options:

- Adding Antimalware for VMs – From Azure portal, under Security Extension
- Enabling Antimalware for VMs - In Server Explorer, utilizing the visual studio VM configuration
- Enabling Antimalware for VMs and Cloud Services - Utilizing the antimalware classic deployment model
- Enabling Antimalware for VMs and Cloud Services - Utilizing PowerShell cmdlets

h1e01.ir

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., AWS), the application interface may be updated with time. Hence, in case you happen to work on an updated version of AWS, 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 an Azure Free Account using the following link: https://azure.microsoft.com/free, in case you have already not created it for the previous lab. 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.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1

Deploying Windows Server VM with antimalware extension

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

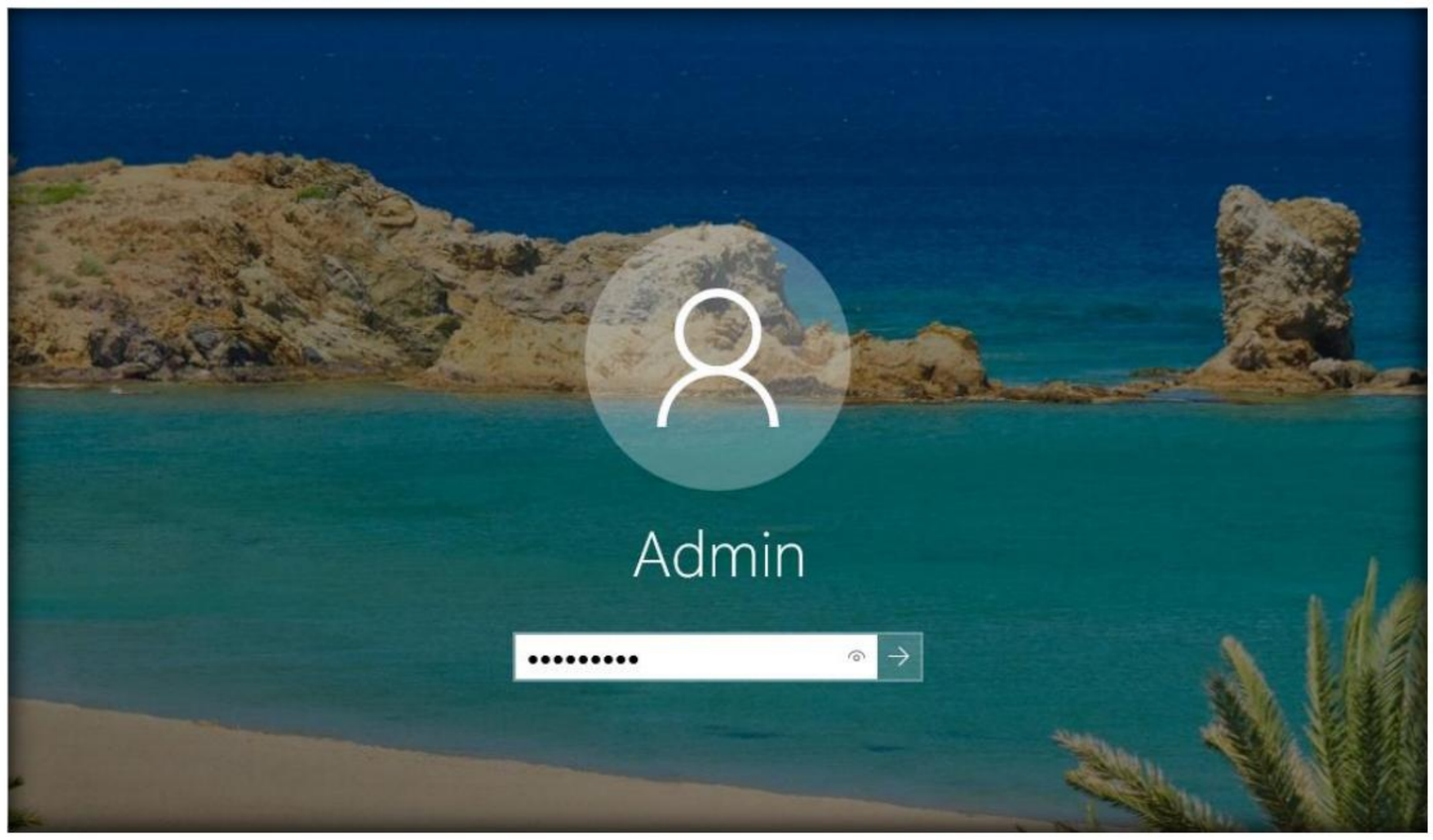


FIGURE 2.5.1: Launch Admin Machine and Log in

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

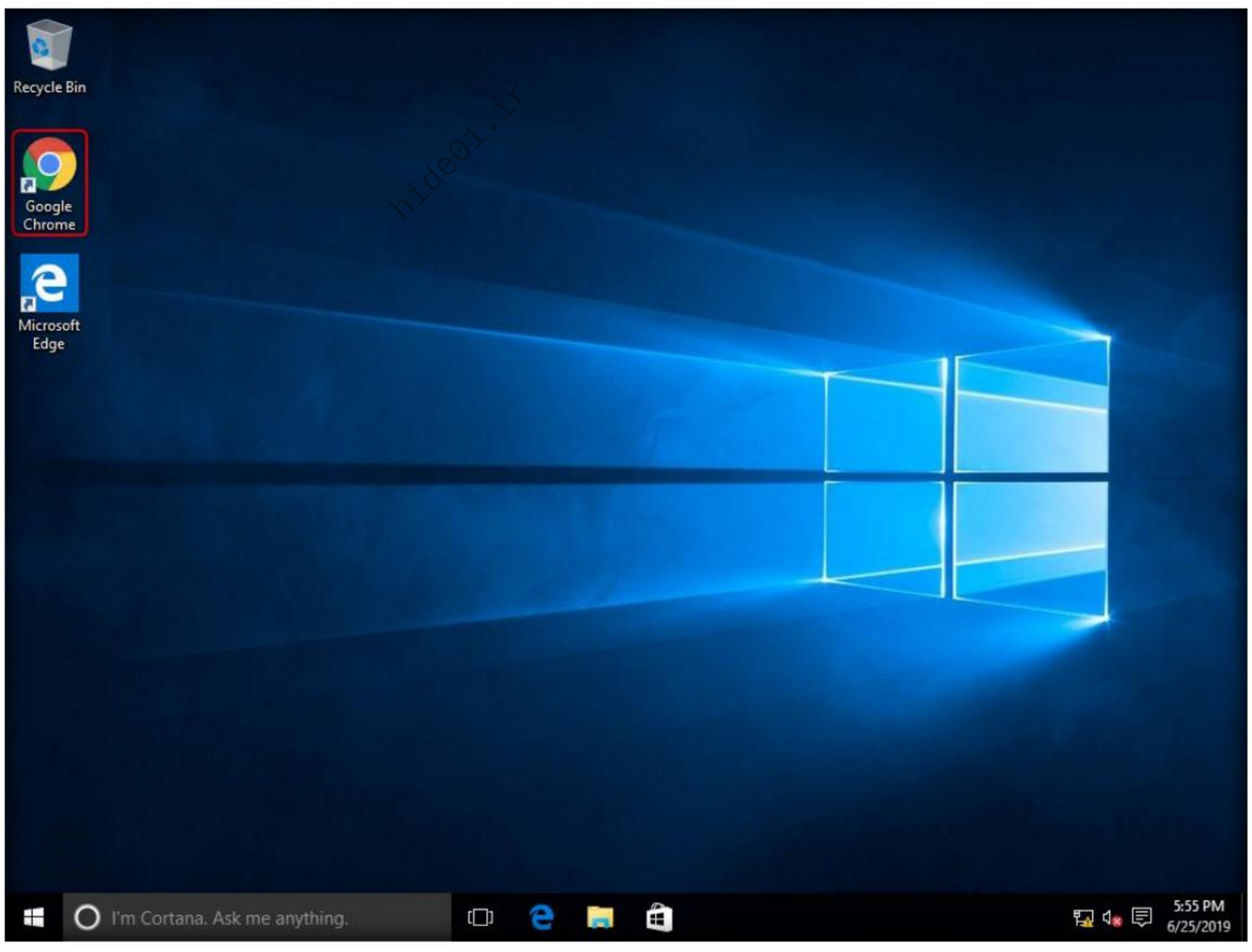


FIGURE 2.5.2: Navigating to the Chrome Browser from Taskbar

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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

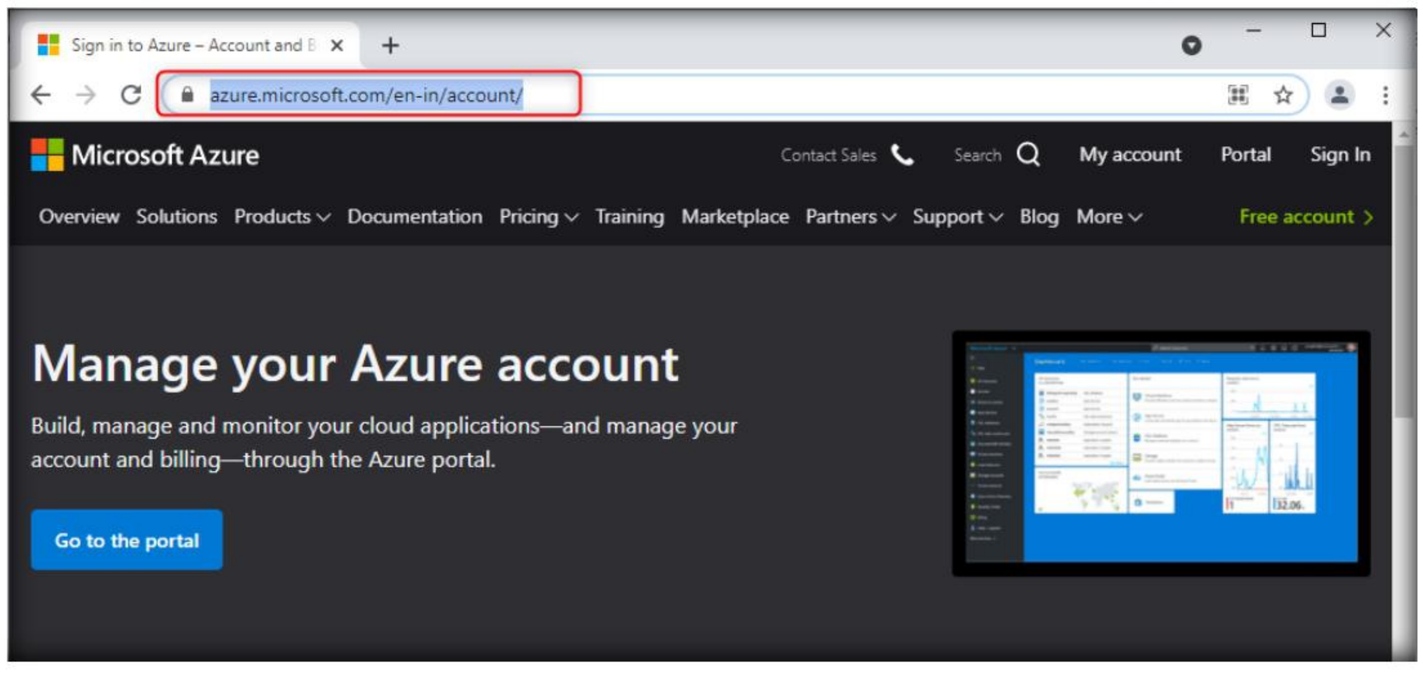


FIGURE 2.5.3: Entering the URL of Microsoft Azure

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

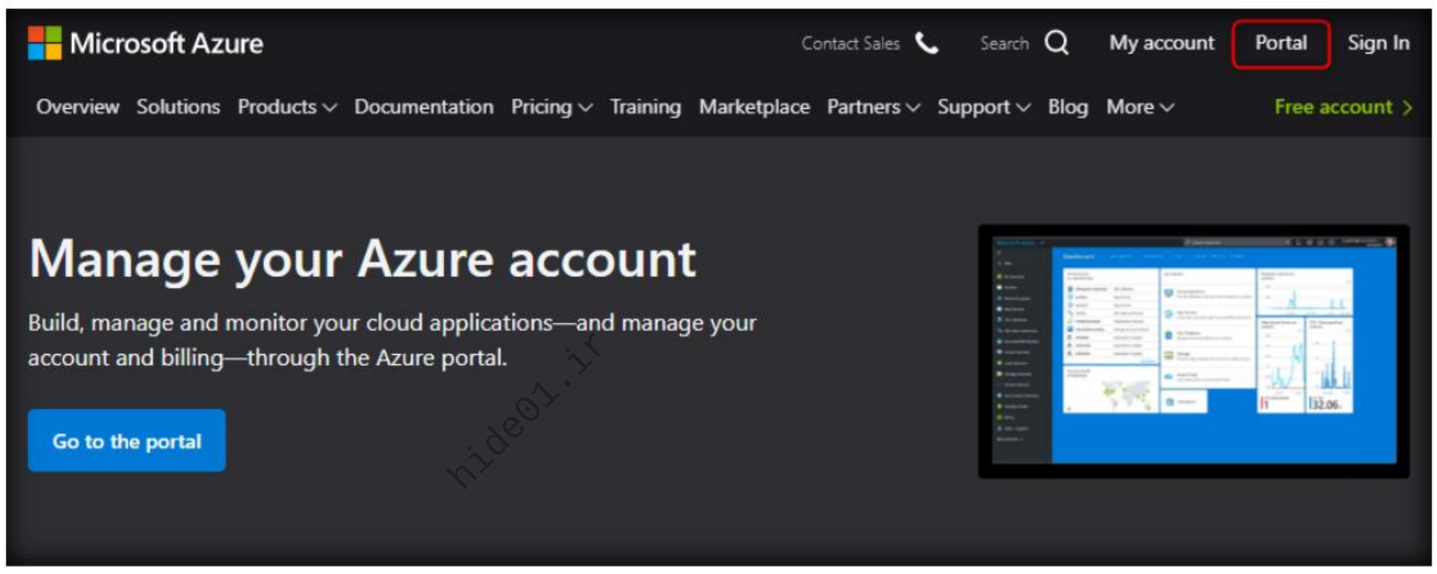


FIGURE 2.5.4: Sign into Azure Portal

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

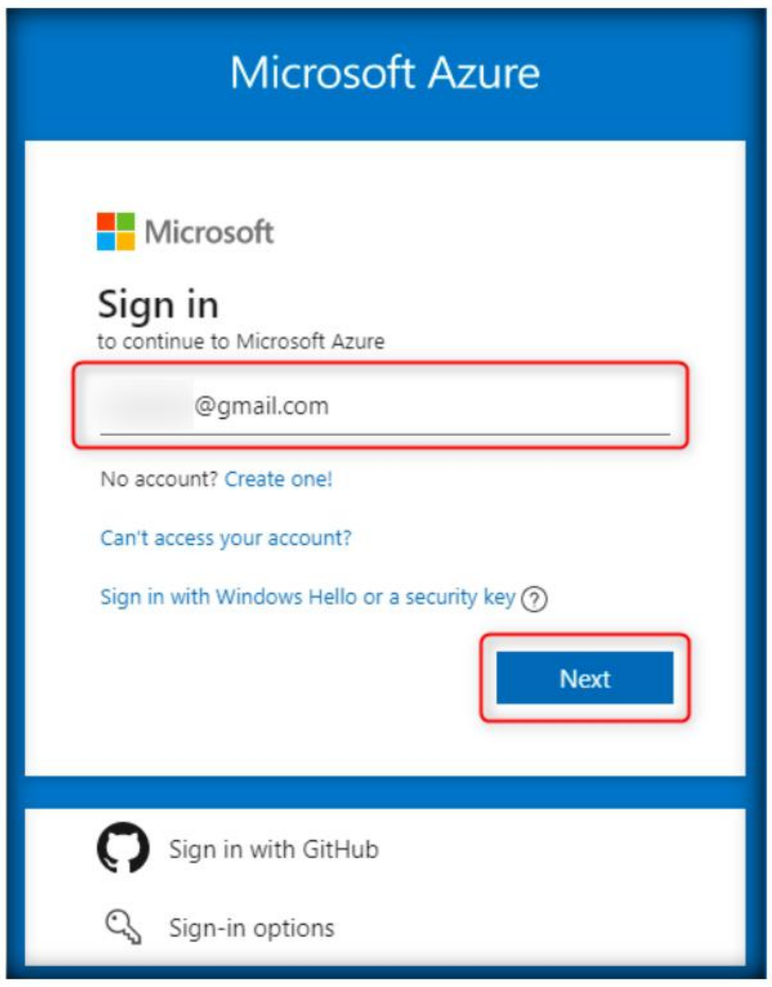


FIGURE 2.5.5: Entering Account ID to continue

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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

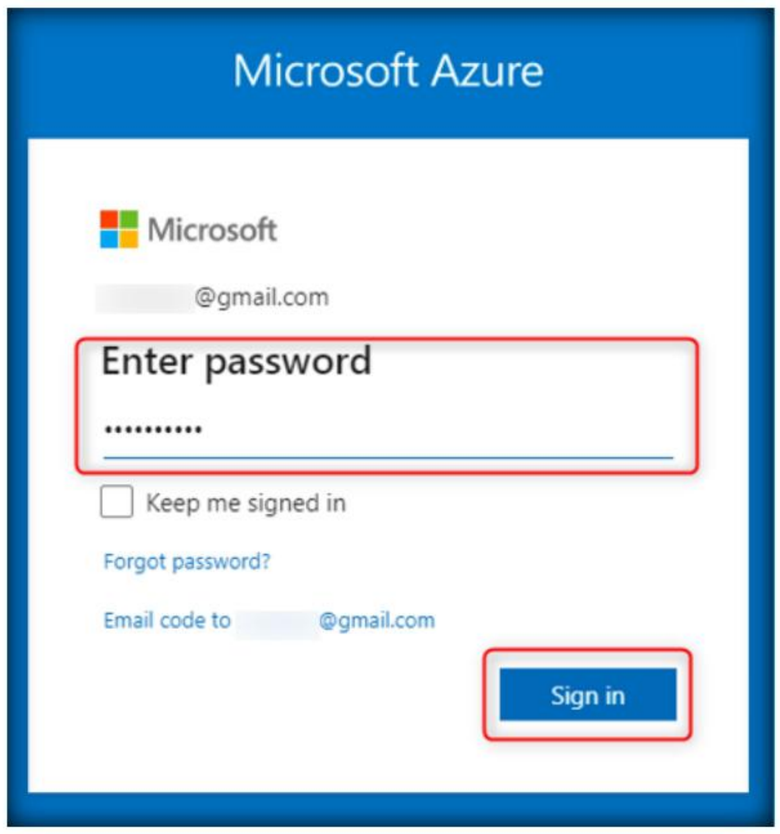


FIGURE 2.5.6: Sign into Azure Account

7. You will be successfully logged in to the **Microsoft Azure portal**. Click on **Virtual machines** under **Azure services**.

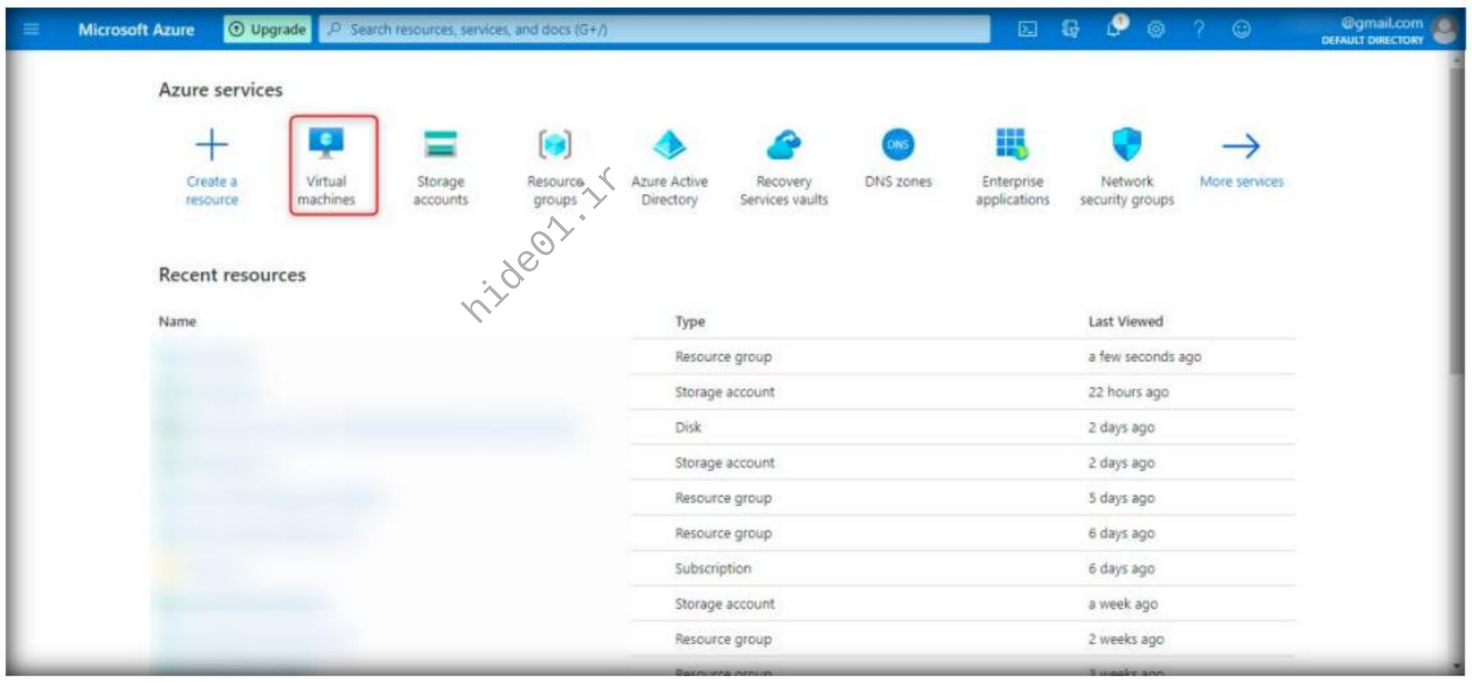


FIGURE 2.5.7: Selecting Virtual machine in Azure portal

8. Click on **Add** drop-down and then click on **Virtual machine.**

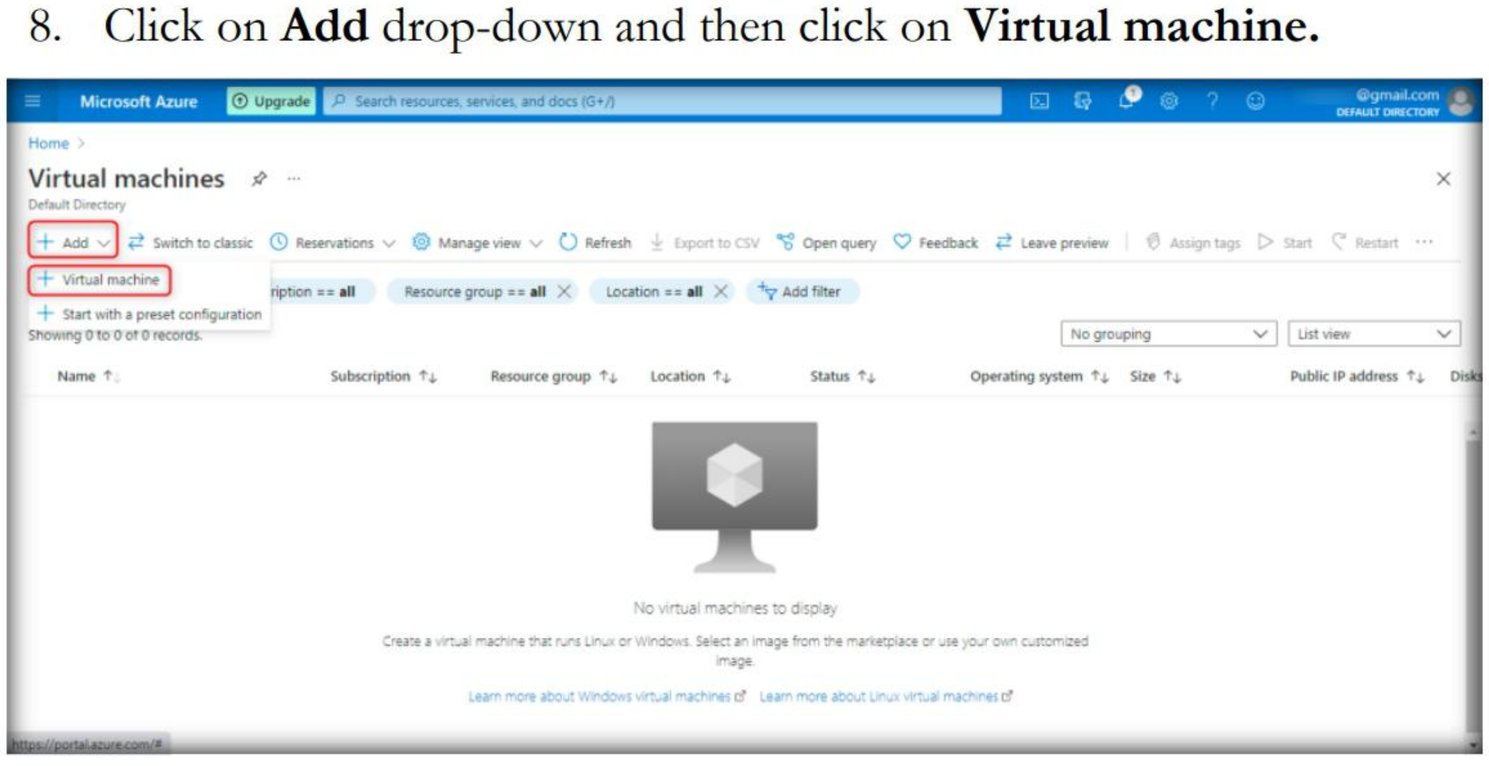


FIGURE 2.5.8: Creating a New Virtual Machine

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

9. **Create a virtual machine** window will open under the **Basics** tab; for **Resource group,** click on **Create new.** Enter the **Name** as **demotest-rg** and click **OK**.

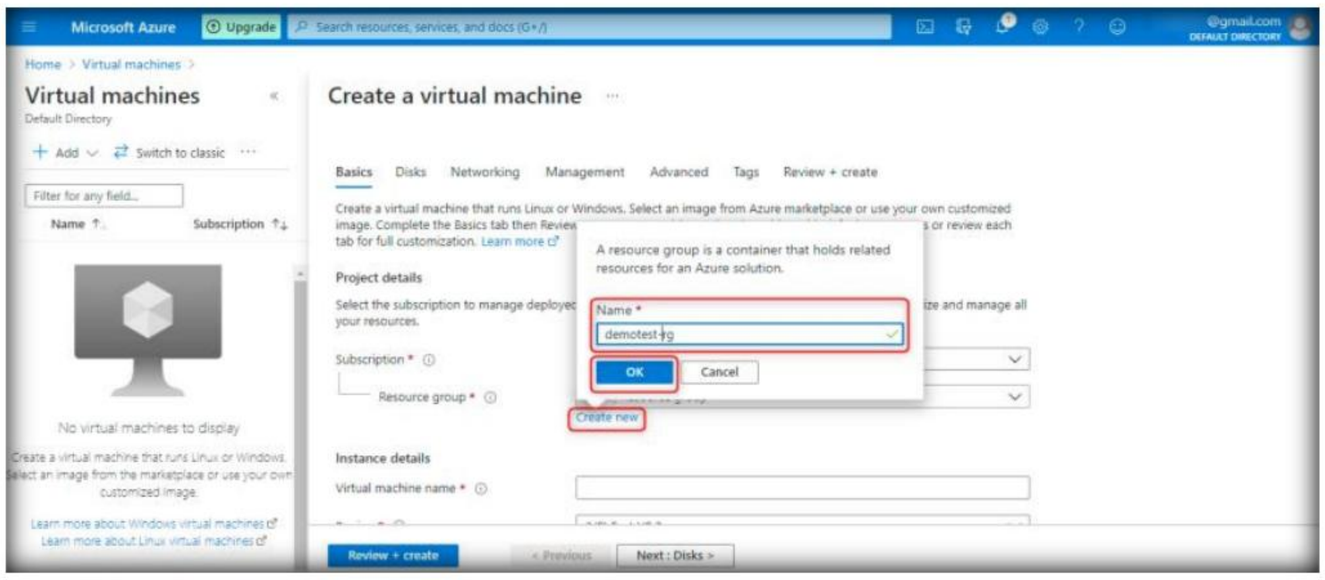


FIGURE 2.5.9: Creating Resource Group

10. Under **Instance details**, for **Virtual machine name,** enter the name as **MyVM-1**. Retain **Region**, **Availability Options**, **Size** in the default state. In the **Image** field, ensure to select **Windows server 2016 Datacenter – Gen1** image.

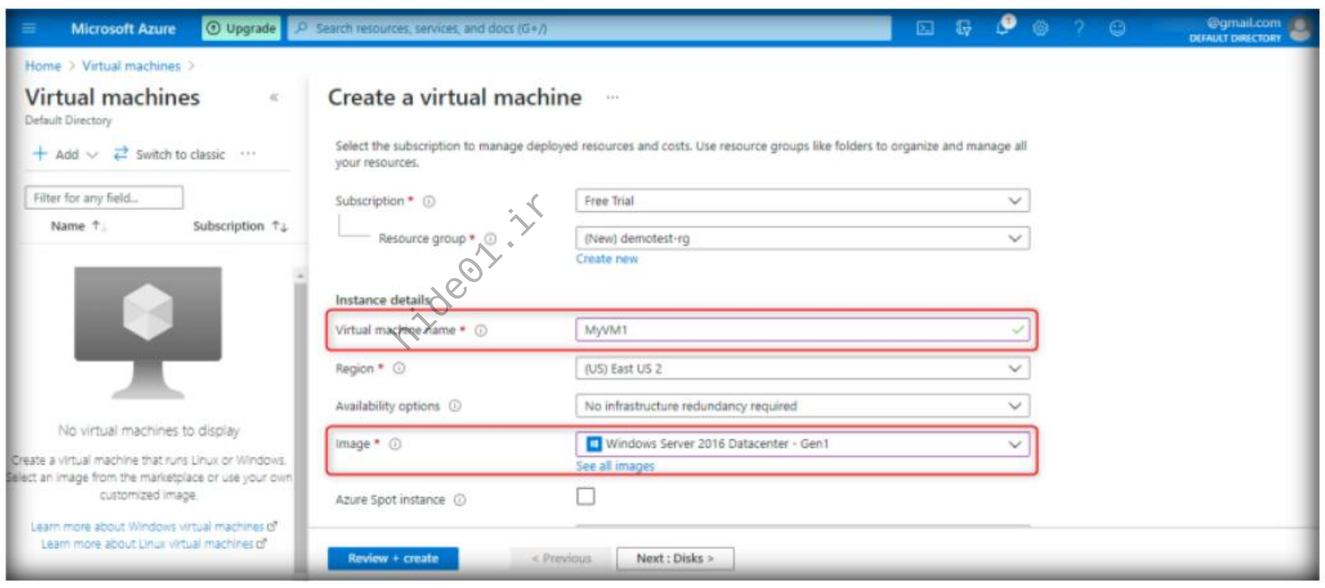


FIGURE 2.5.10: Entering Name and Selecting the Image of VM

11. Under **Administrator** account, enter the **Username** as **ccseuser** and a **Password** of your choice, followed by **Confirm password.**

Note: Copy and paste the **password** and **username** to notepad before you continue.

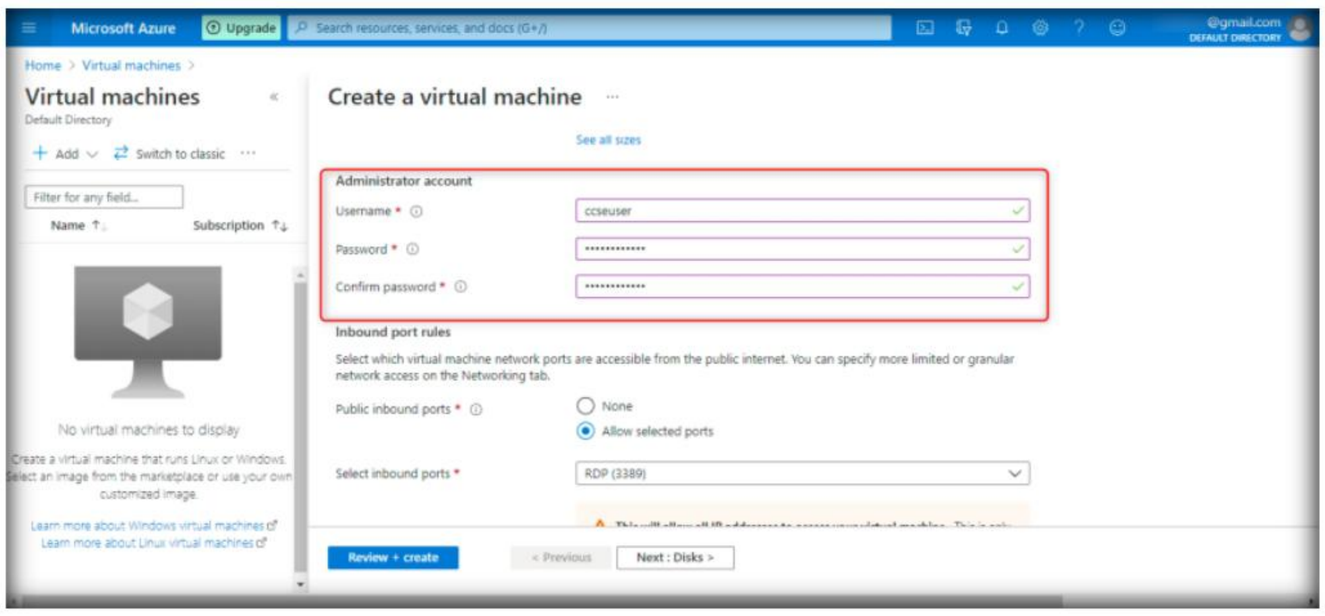


FIGURE 2.5.11: Entering Username and Password

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

12. Retain **Inbound port rules** and **Licensing** in a default state, click on the **Next: Disks >** button.

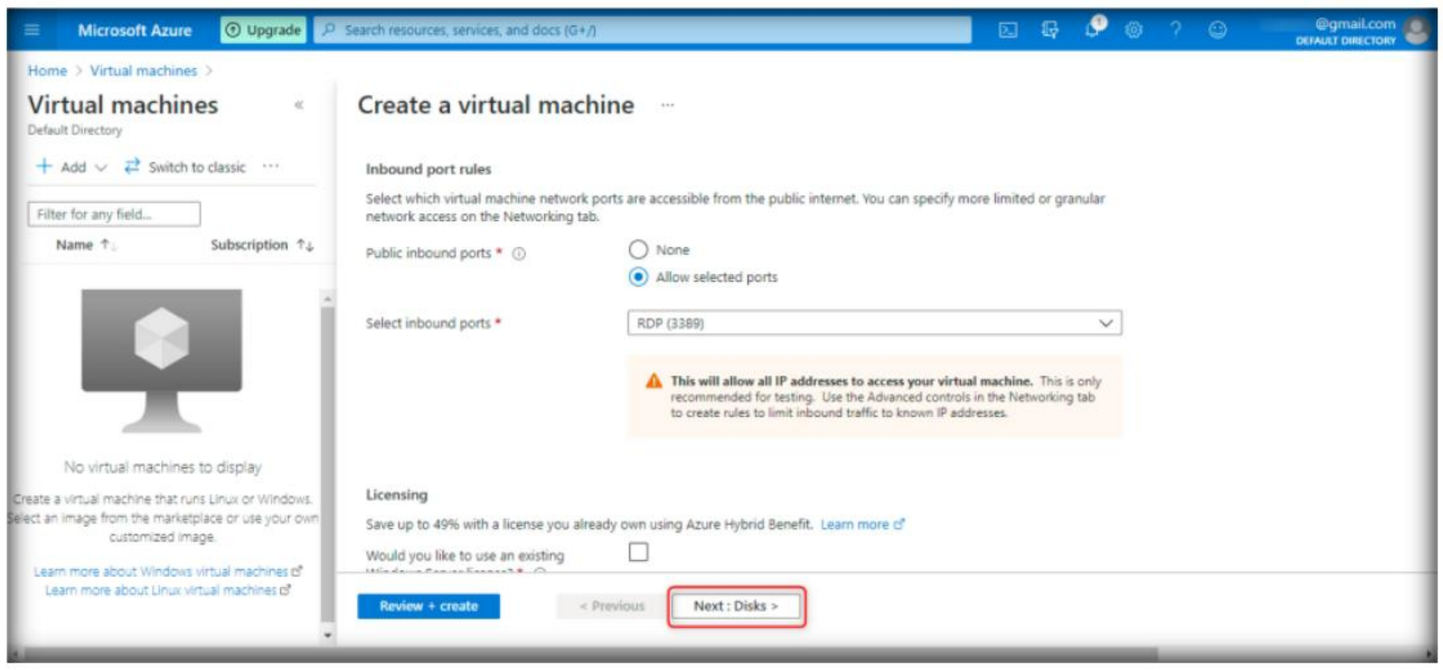


FIGURE 2.5.12: Moving to Disks tab

13. Under the **Disks** tab, retain all the fields in default state, and click on the **Next: Networking >** button.

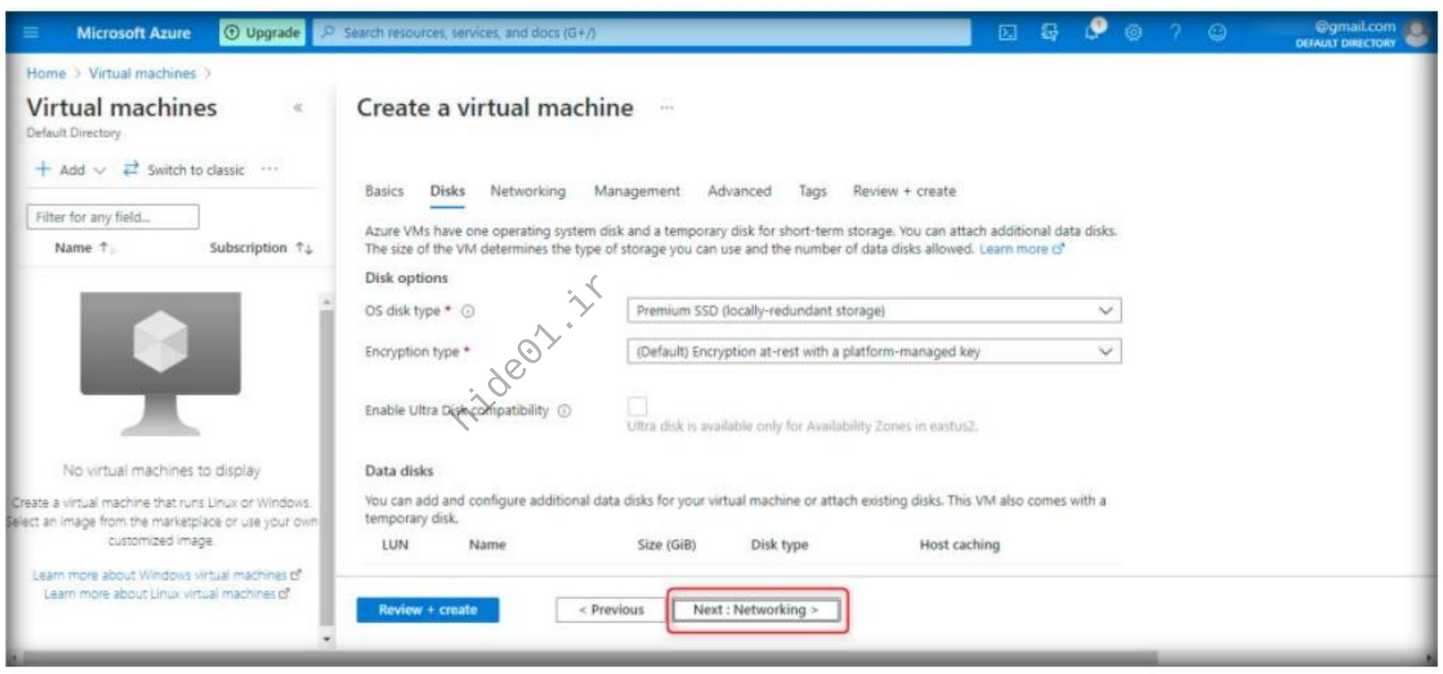


FIGURE 2.5.13: Leaving all Fields in Default State and moving to Networking tab

14. Under the **Networking** tab, retain all the fields in default state, and click on the **Next: Management >** button.

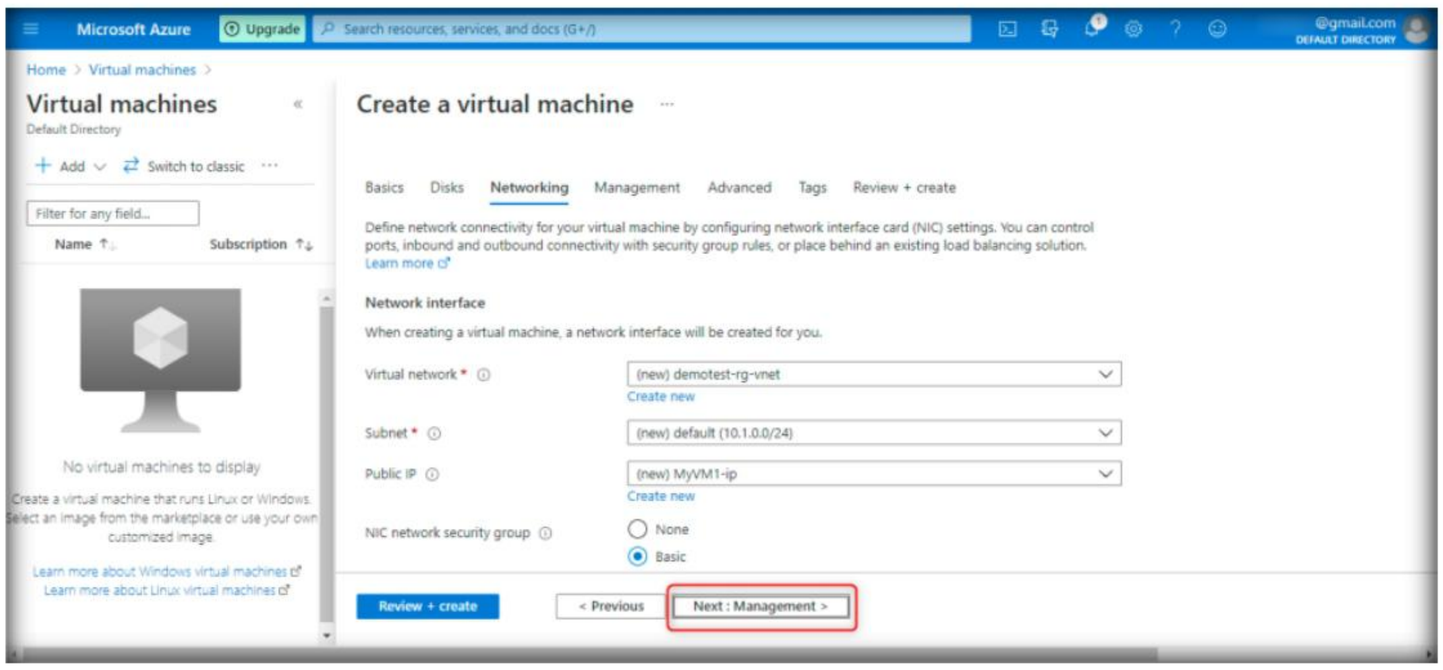


FIGURE 2.5.14: Leaving all Fields in Default State and moving to Management tab

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

15. Under the **Management** tab, retain all the fields in default state, click on the **Next: Advanced>** button.

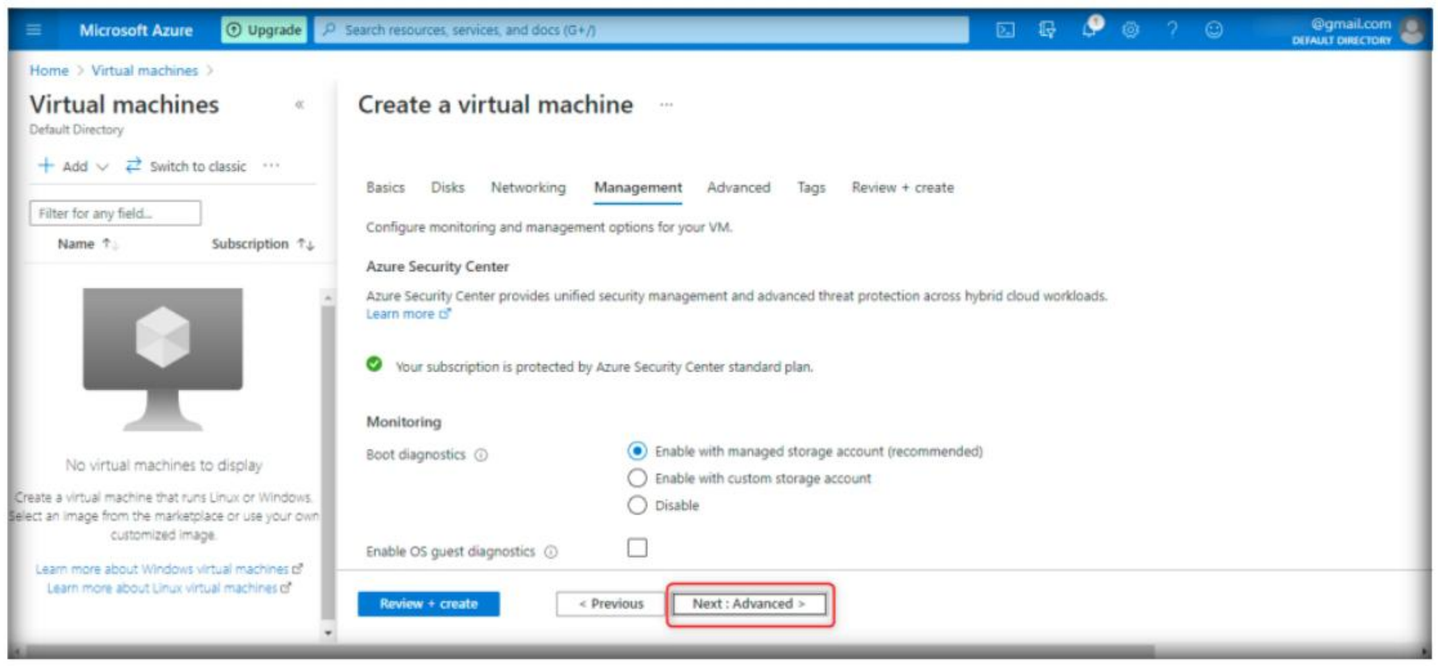


FIGURE 2.5.15: Leaving all Fields in Default State and moving to Advanced tab

16. Under the **Advanced** tab, for **Extensions**, click on **Select an extension to install.**

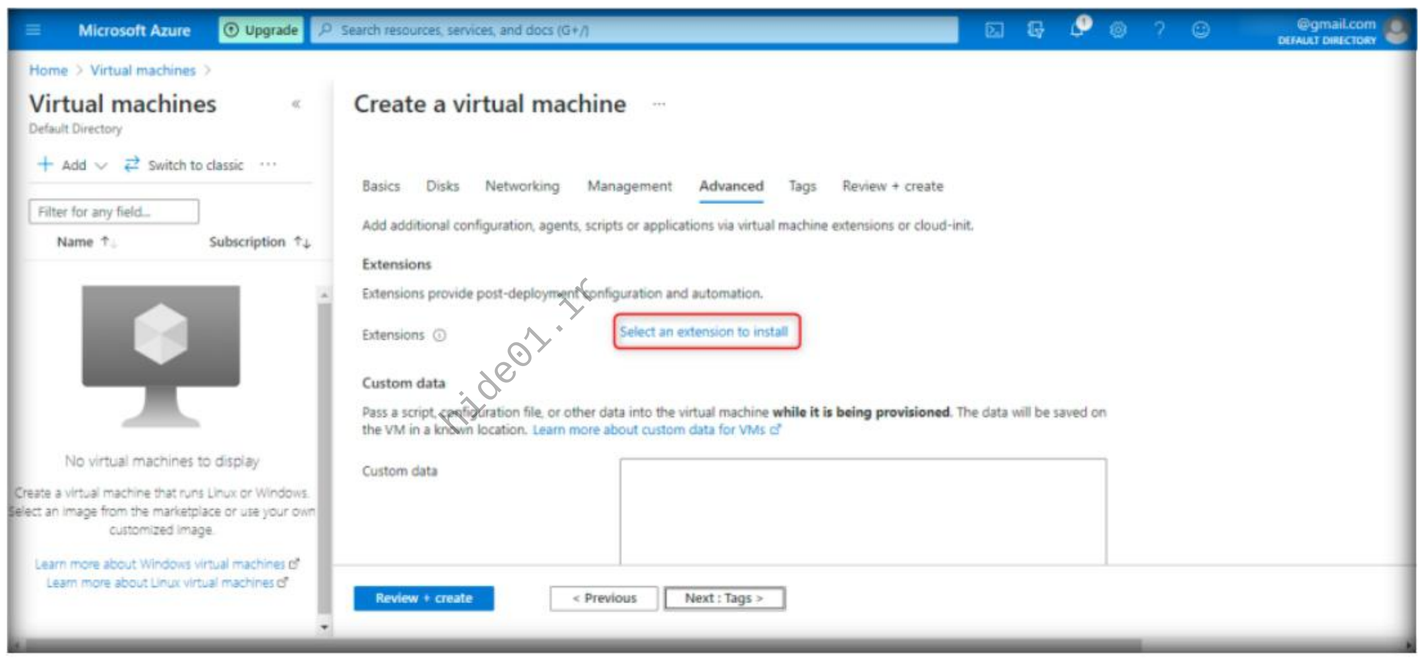


FIGURE 2.5.16: Selecting Antimalware Extension for Installation

17. **The New Resource** window will open, scroll down, and click on **Microsoft Antimalware**.

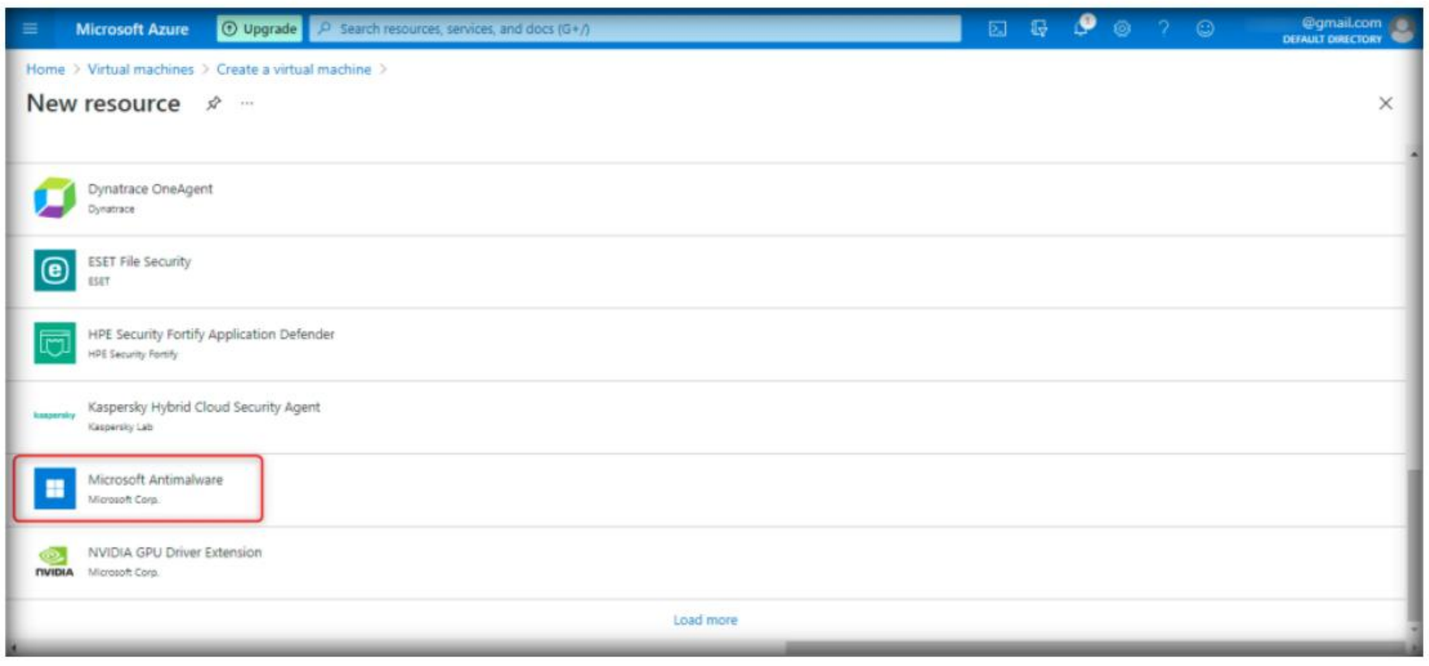


FIGURE 2.5.17: Selecting Microsoft Antimalware

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

18. Then, click on **Create** button.

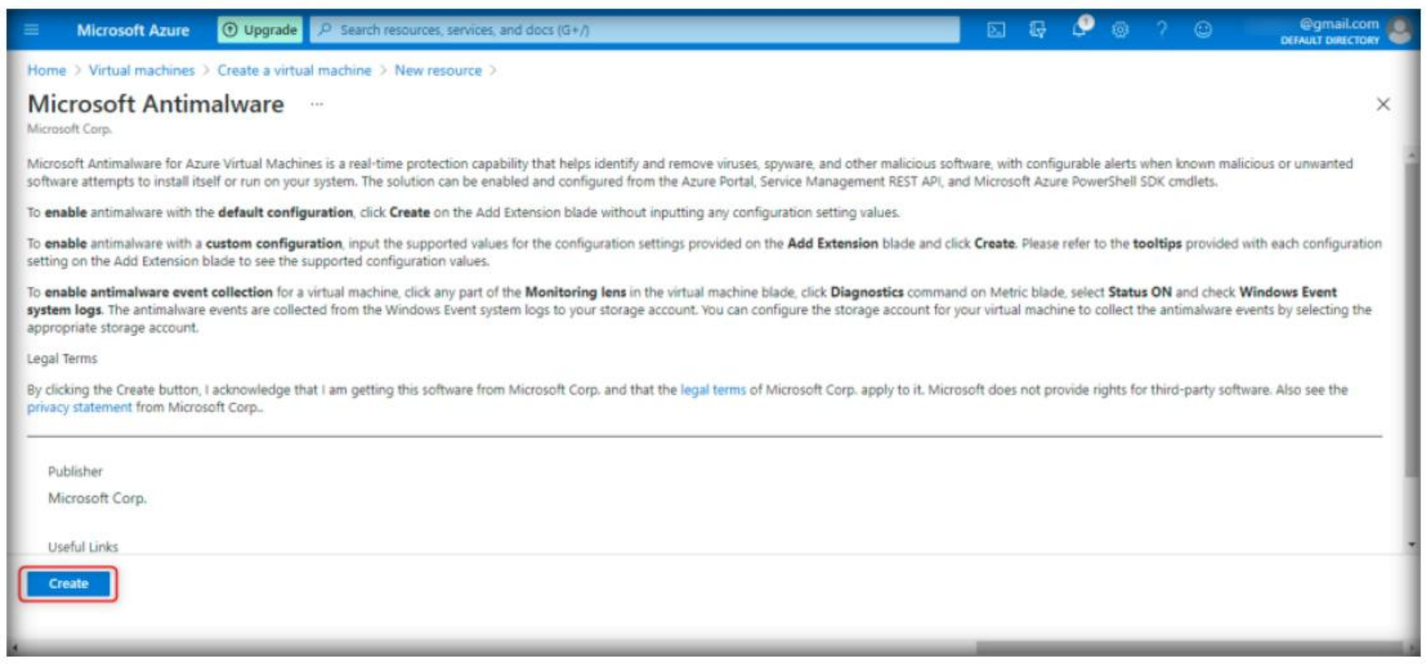


FIGURE 2.5.18: Installing Microsoft Antimalware

19. Install extension window will open, under **Excluded file extensions** enter **.log** and under **Excluded process** enter **SQLServr.exe.** Retain the rest of the fields in the default state and click on **OK.**

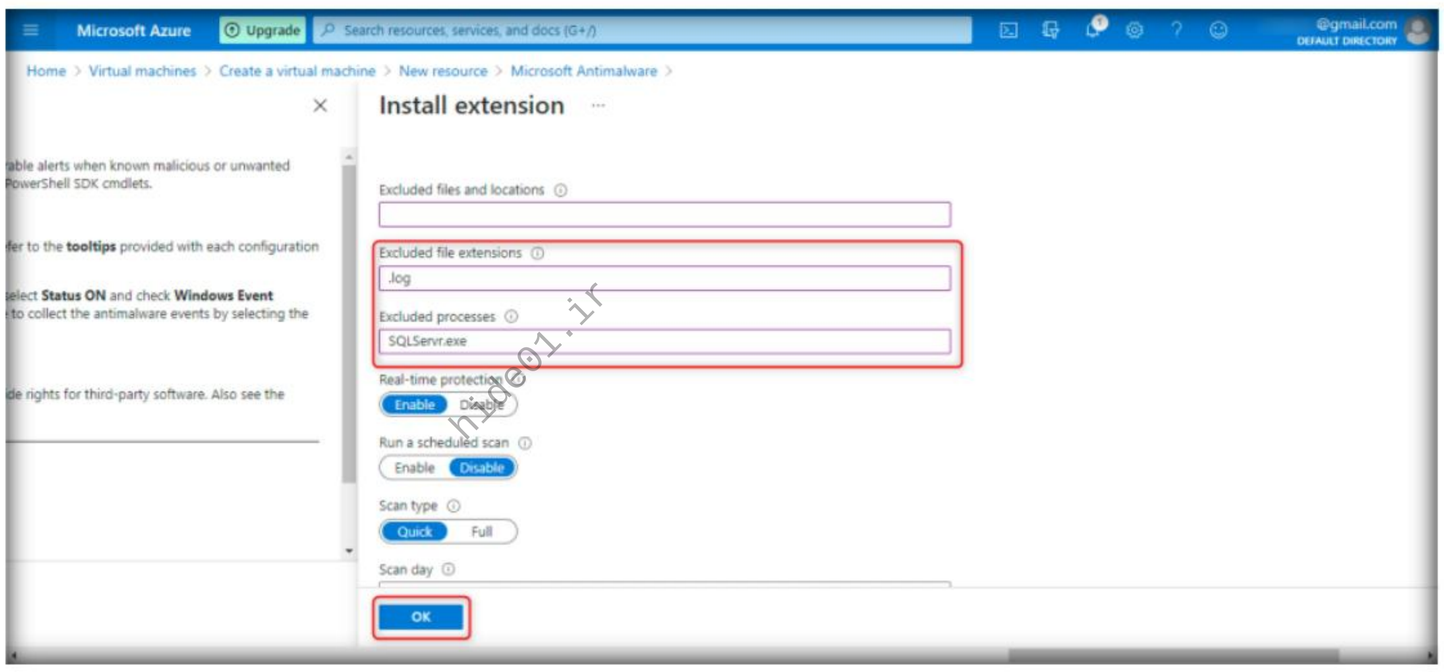


FIGURE 2.5.19: Entering Details in Install Extension Window

20. Leave the rest of the fields in the default state, click on the **Next: Tags >** button.

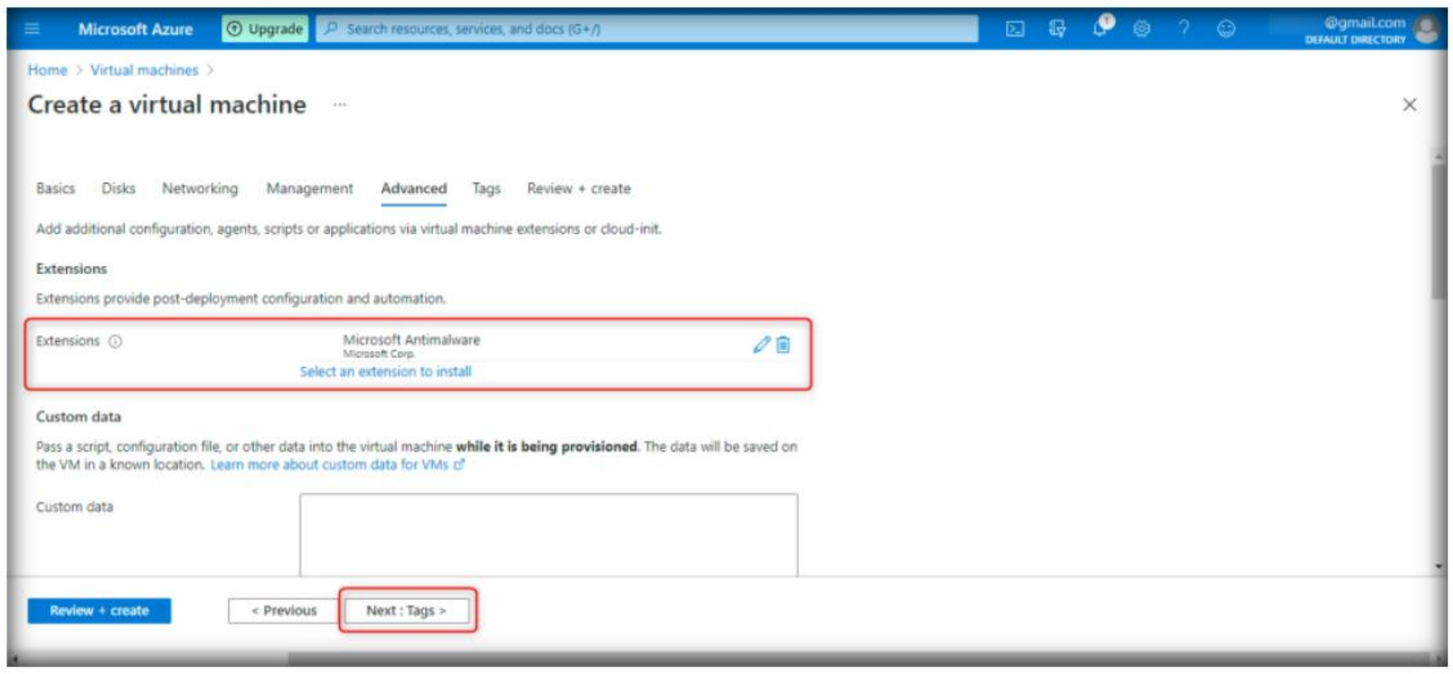


FIGURE 2.5.20: Moving to Tags tab

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

21. Under **Tags**, leave the fields in a default state, click on **Next: Review + create.**

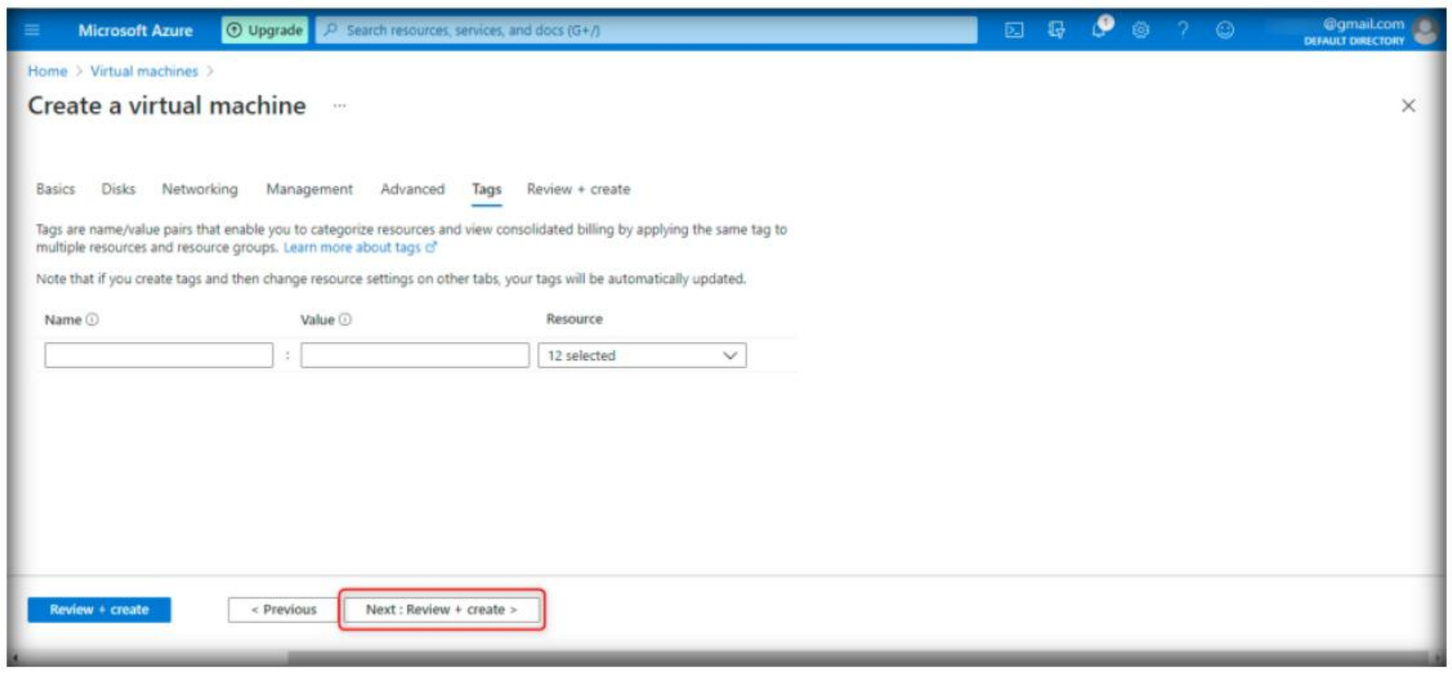


FIGURE 2.5.21: Reviewing and Creating a VM

22. After it has passed validation, click on **Create** button

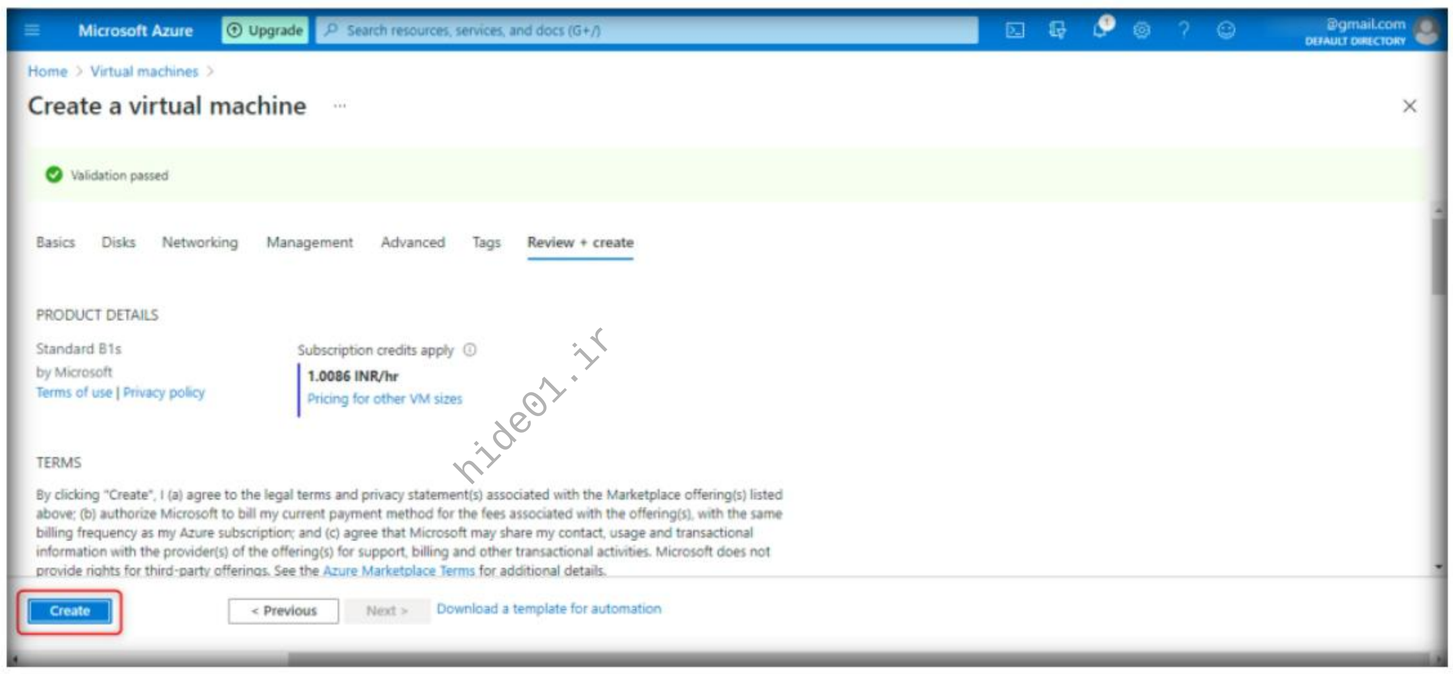


FIGURE 2.5.22: VM Passing the Validation

23. Wait for the deployment to get completed successfully. After the deployment gets completed, click on **Go to resource.**

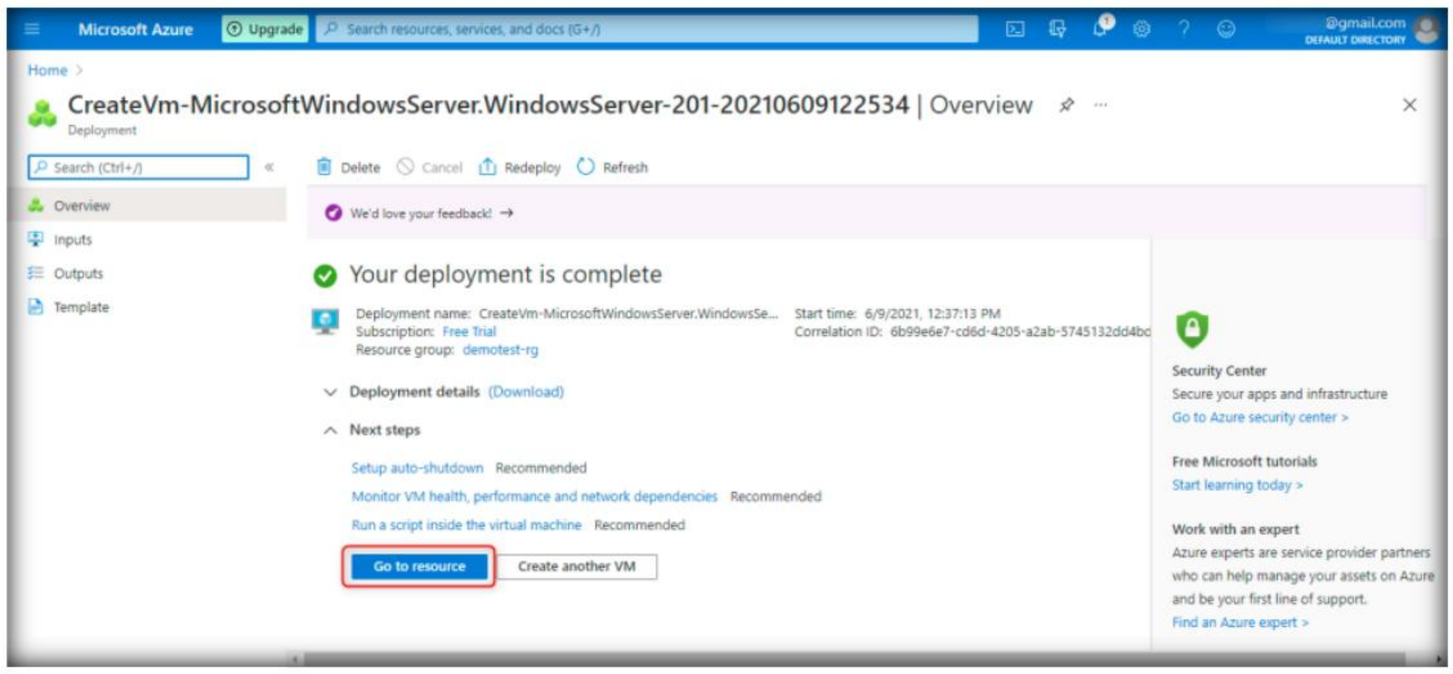


FIGURE 2.5.23: Successfully Completed VM Deployment

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

24. **MyVM1** virtual machine details will appear, note down, or copy the **Public IP address**.

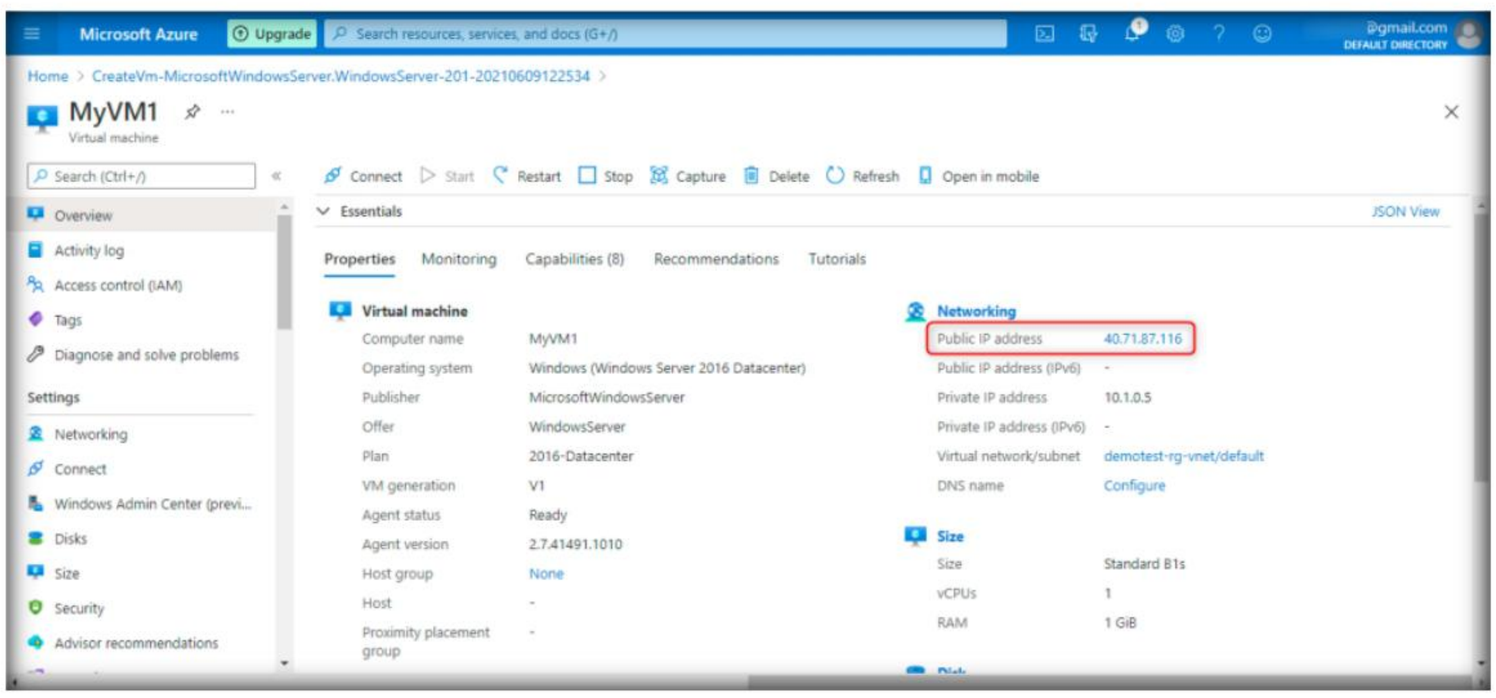


FIGURE 2.5.24: Copying the Public IP address of the VM

TASK 2

Verifying the Windows Server Deployment

25. Type **Remote Desktop Connection** in the windows search field and click on **Remote Desktop Connection** App.

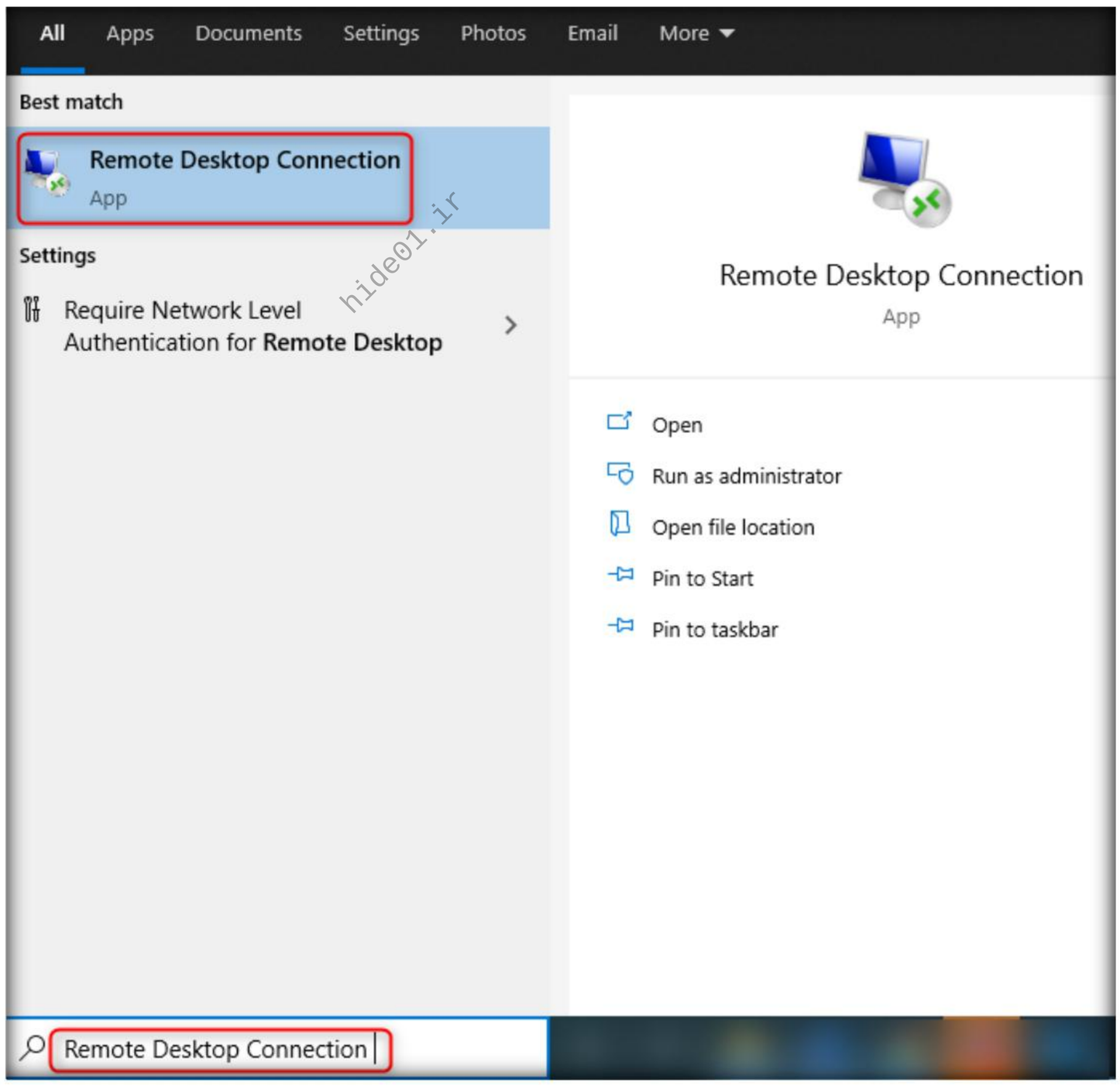


FIGURE 2.5.25: Opening Remote Desktop Connection

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

26. Enter the VM public IP address which you noted earlier in the **Computer** field of **Remote Desktop Connection** and click on **Connect** button.

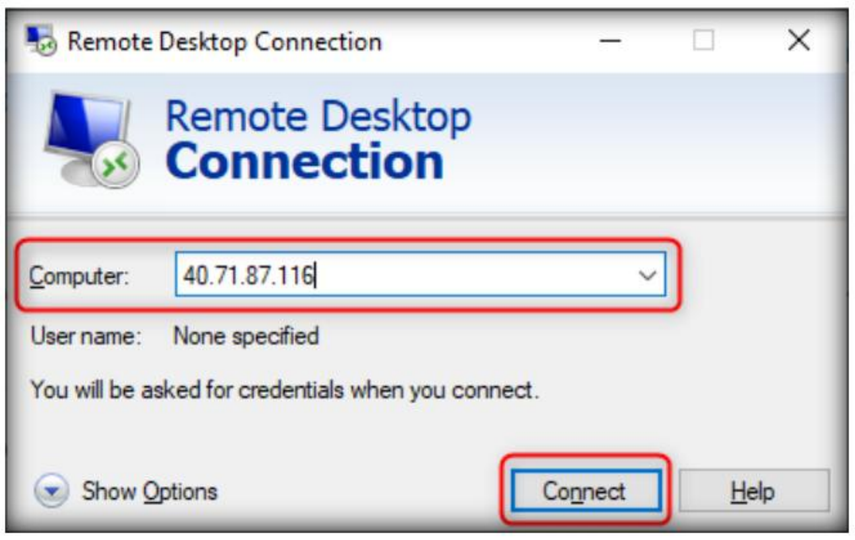
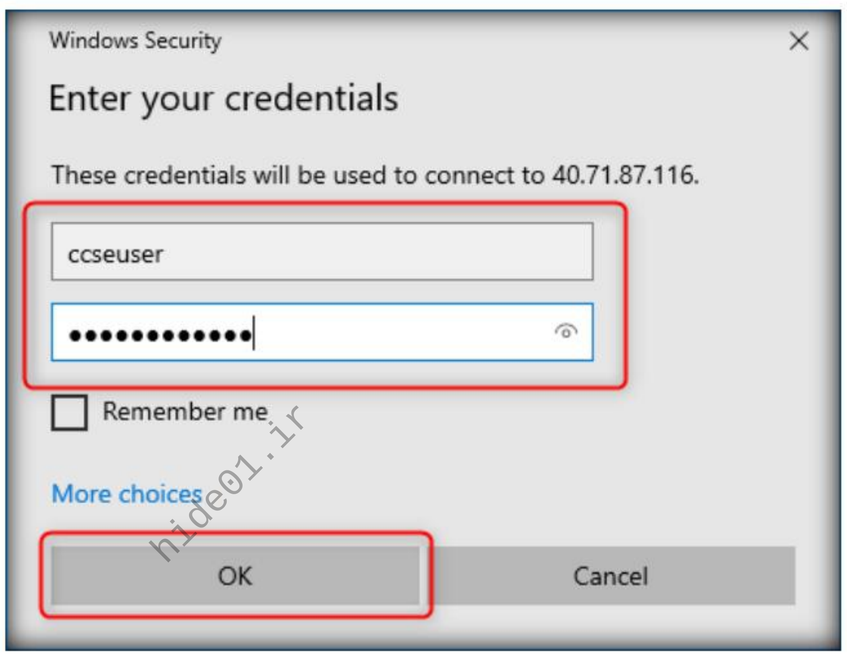


FIGURE 2.5.26: Connecting Remote Desktop Connection

27. Enter the VM **Username** and **Password** that you copied to notepad while deploying the windows server VM. Click on the **OK** button.



hide01.ir

FIGURE 2.5.27: Entering the Credentials to Connect the VM

28. A new window of the certificate will open. Click the **Yes** button.

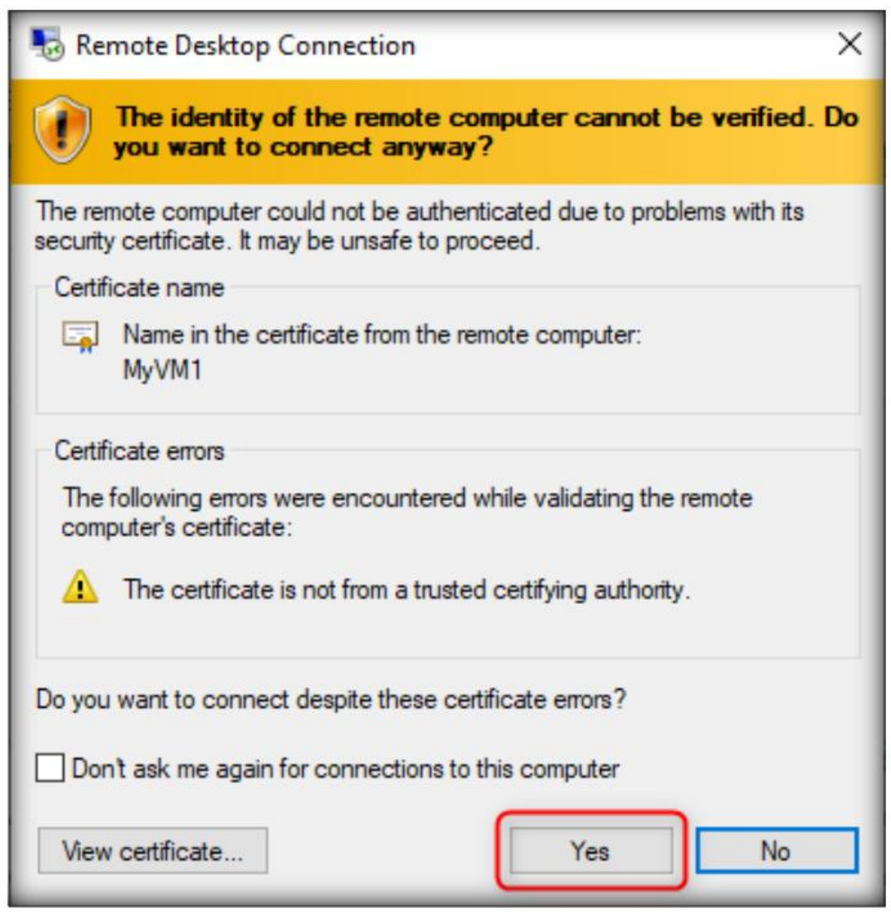


FIGURE 2.5.28: Establishing Connection with the VM

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

29. The windows server remote machine starts. In the windows server remote machine, you will see that the **Networks** window will appear on the right side, click on **Yes** and minimize Server Manager Dashboard.

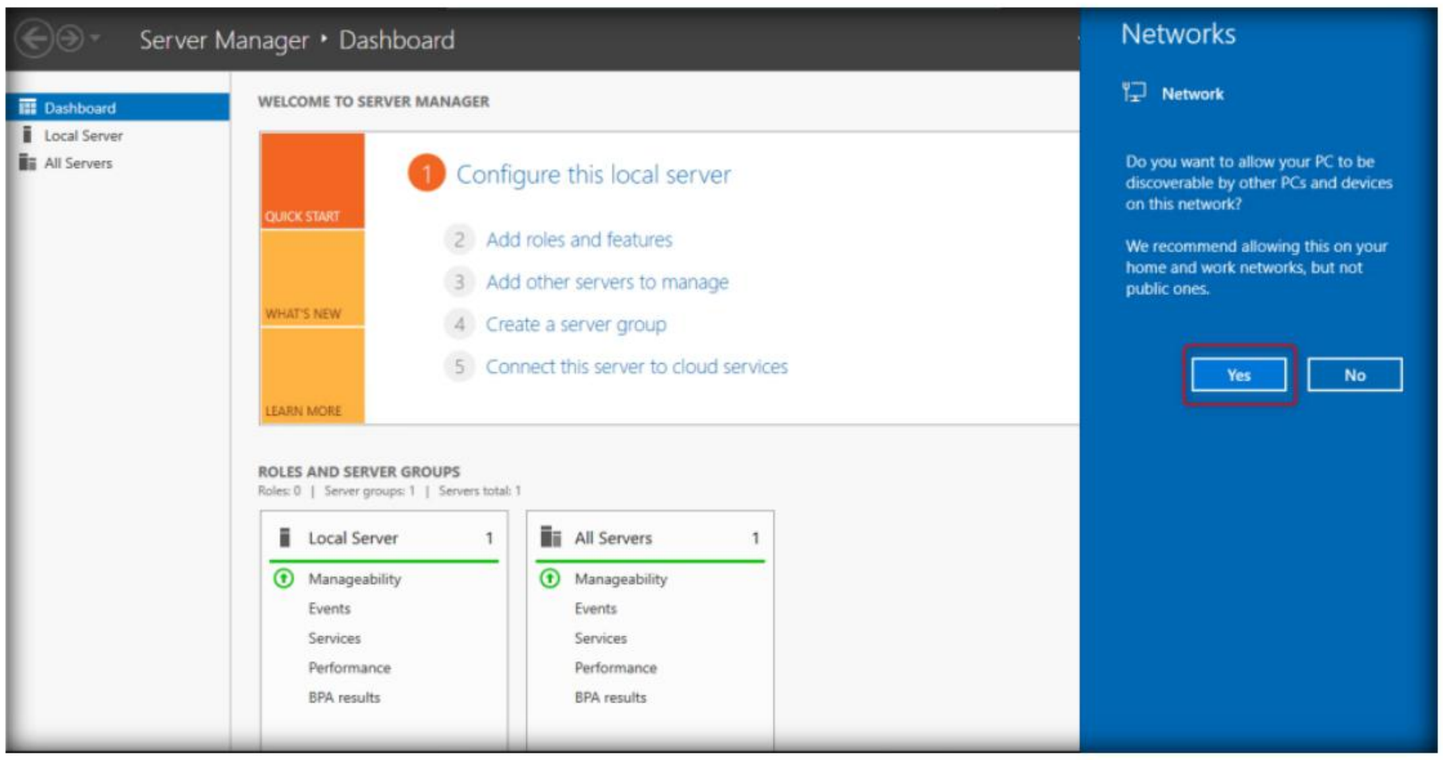


FIGURE 2.5.29: Establishing Network Connection

30. In the remote machine windows search box, type **settings** and click on **Settings.**

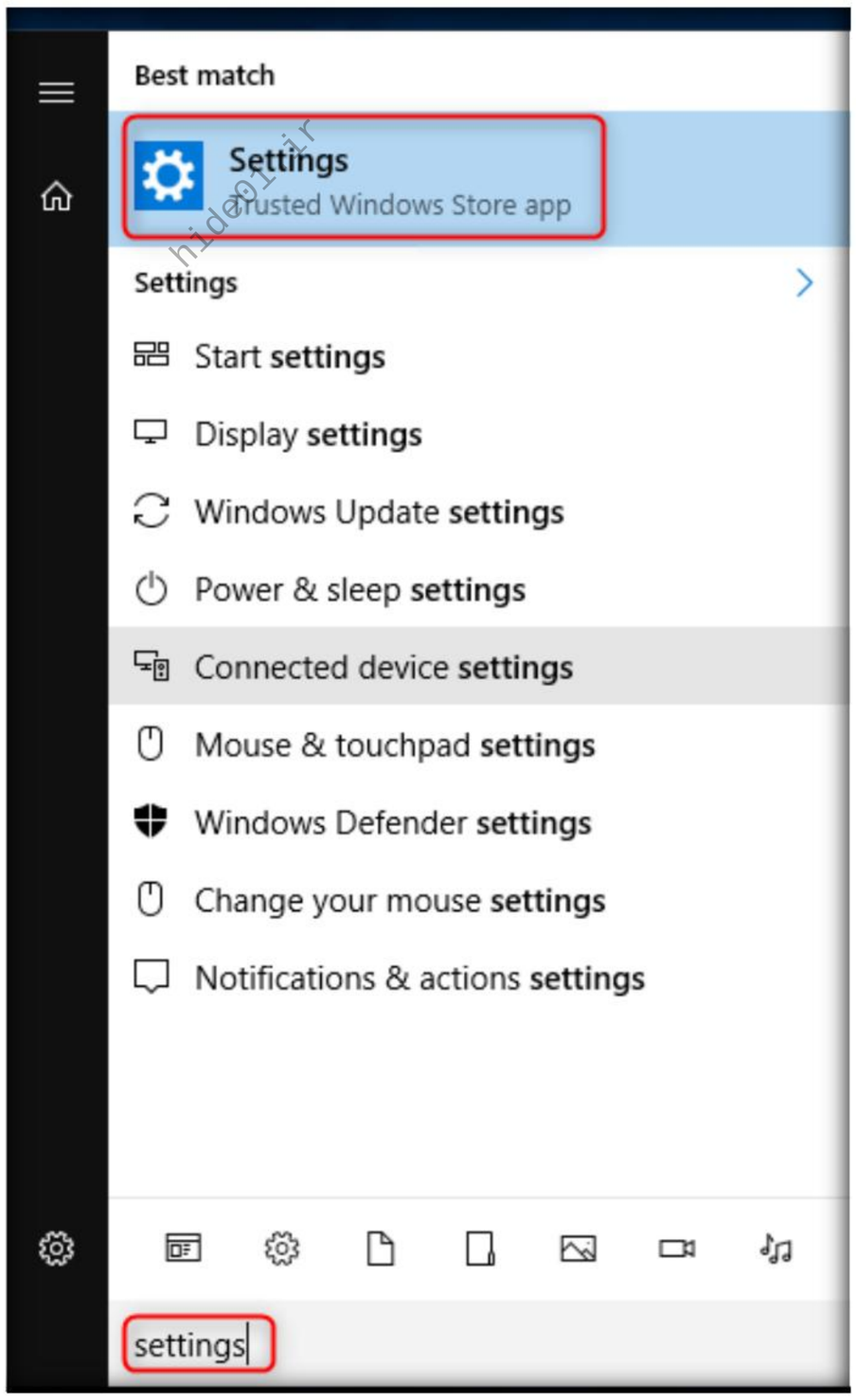


FIGURE 2.5.30: Opening Windows Settings

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

31. Under **Windows Settings**, click on **Update & security**.

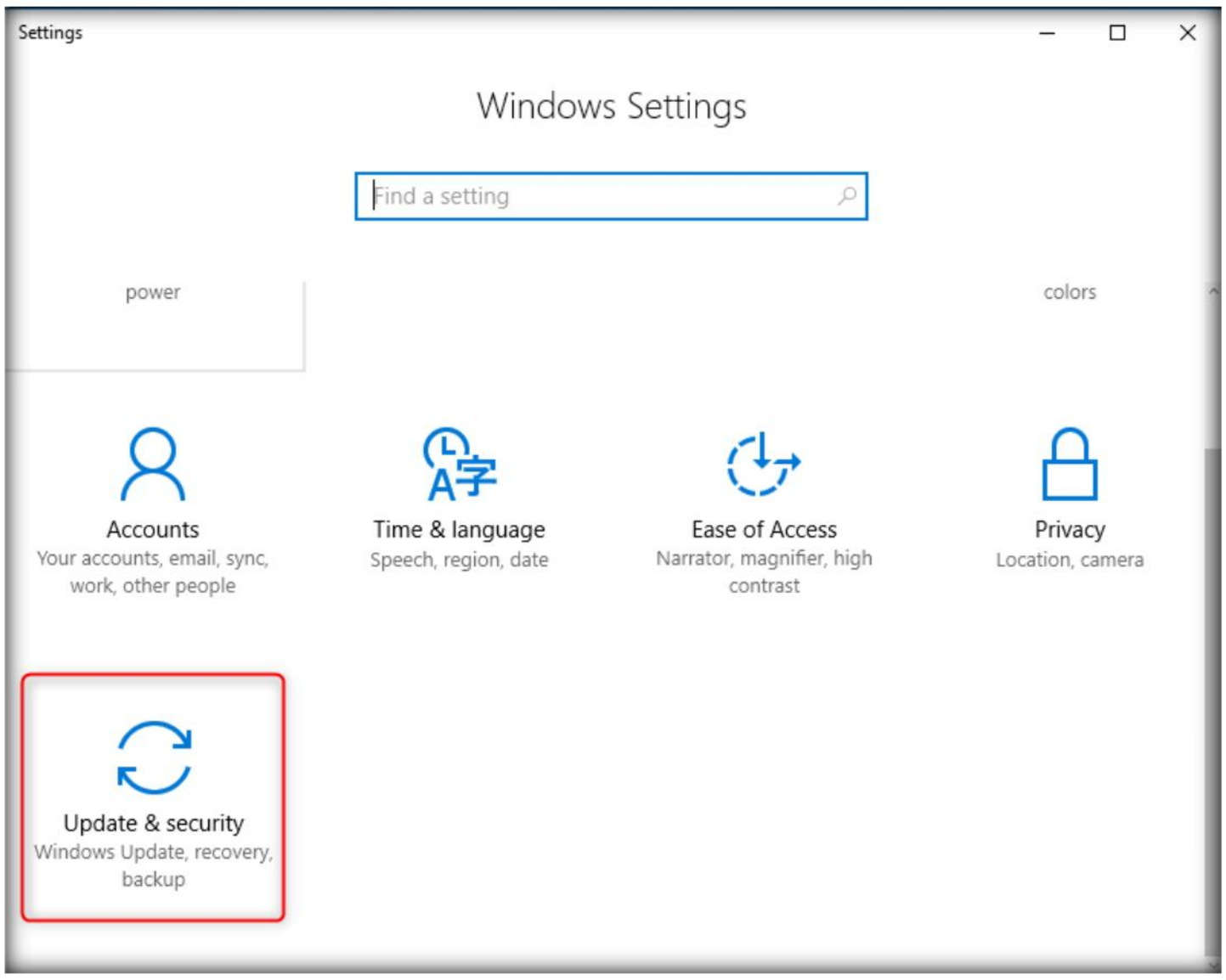


FIGURE 2.5.31: Selecting Windows Update & Security

32. Then, click on **Windows Defender.**

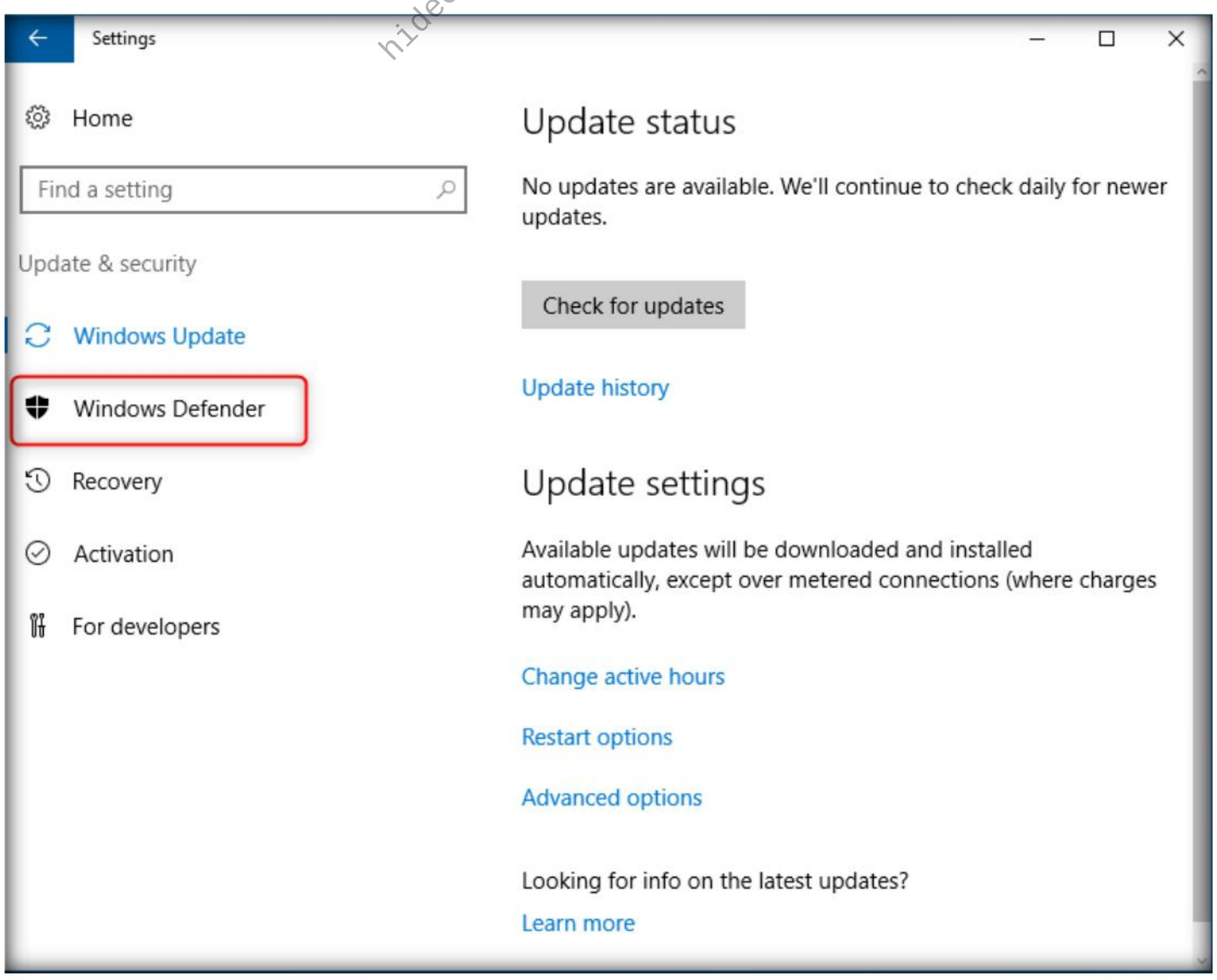


FIGURE 2.5.32: Selecting Windows Defender

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

33. Scroll down and check the **Version info.**

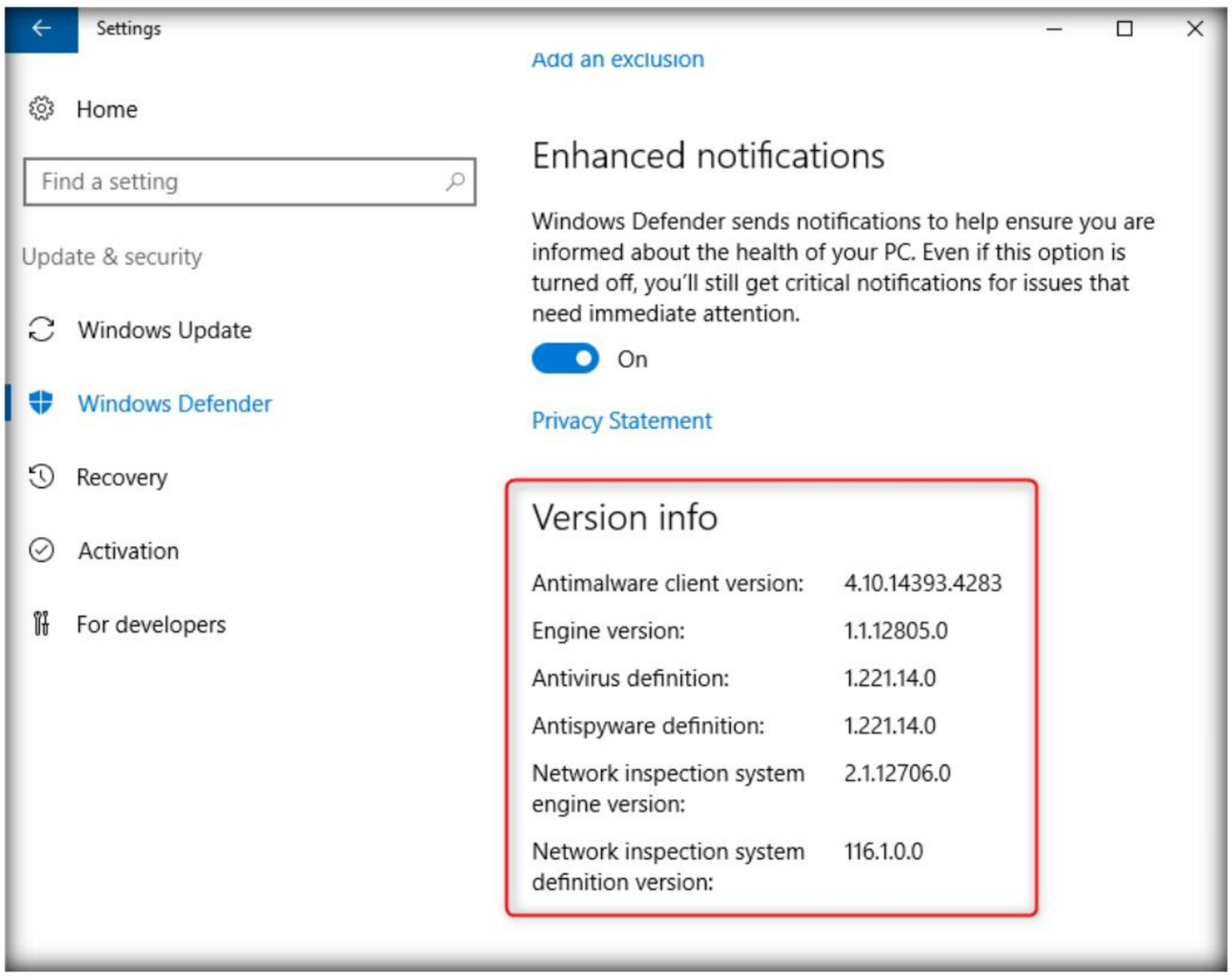


FIGURE 2.5.33: Checking Antimalware Version Information

34. You will see that the Antimalware version information has been enabled in the windows server VM.
35. Thus, a cloud security engineer can deploy a VM with an antimalware extension to protect the resources from malware attacks.

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

36. From the Azure portal navigate to **Virtual Machines**, select the Virtual machine you created (MyVM-1). In the MyVM-1 details page. Click **Delete** to delete the Virtual Machine.

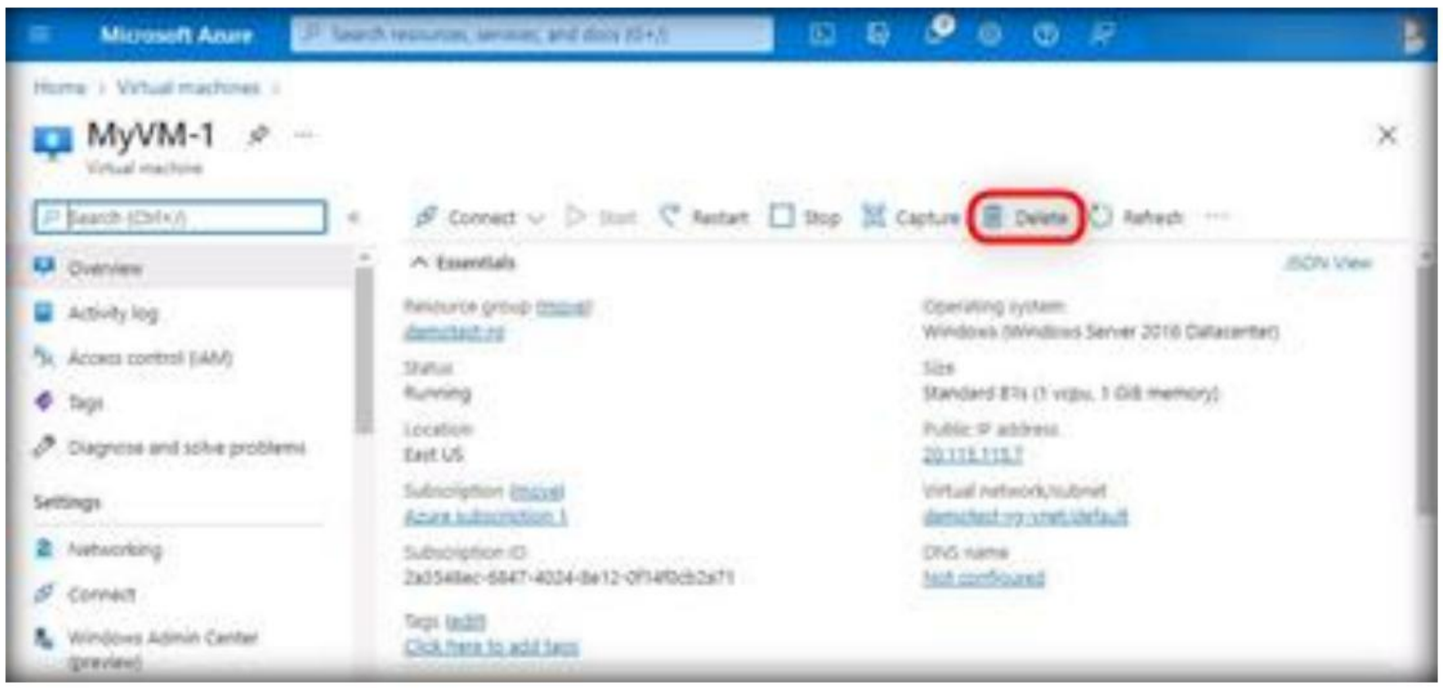


FIGURE 2.5.34: Deleting Virtual Machine

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

37. Select the associated resources to be deleted and select the checkbox **I have read and understood that this virtual machine as well as as any selected associated resources listed above will be deleted** and click **Delete**.

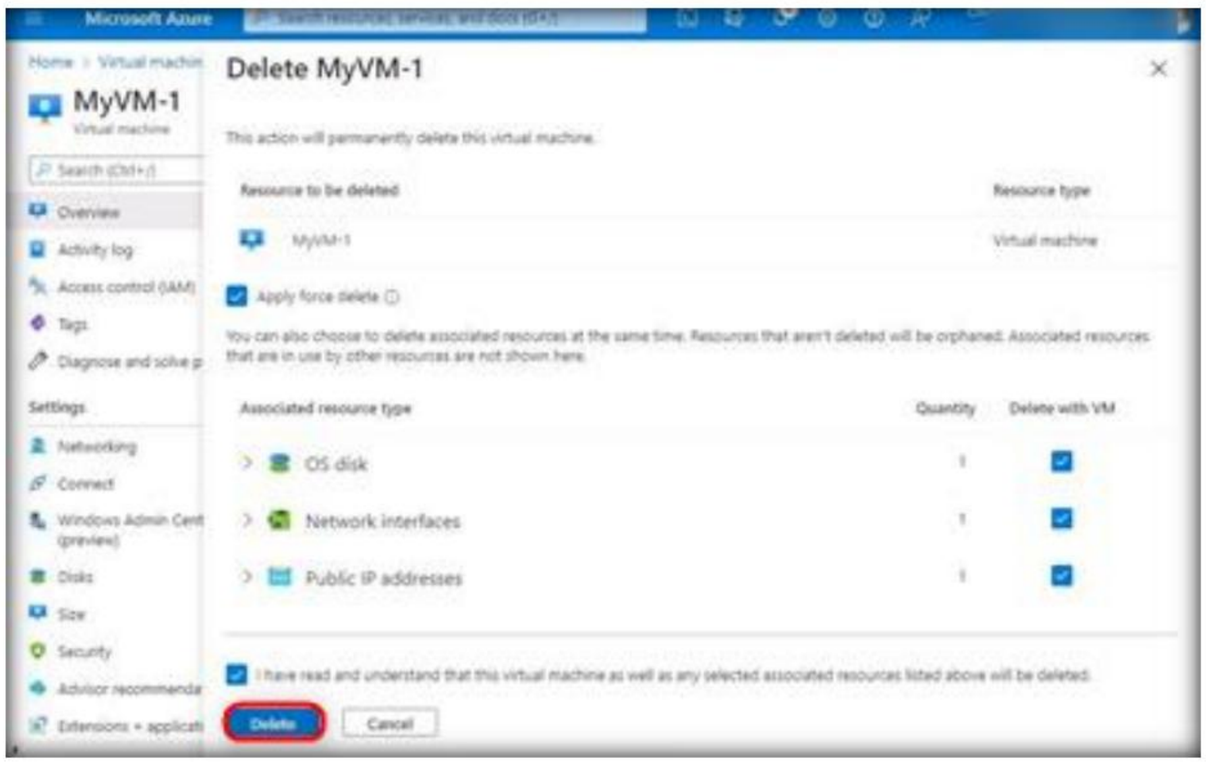


FIGURE 2.5.35: Deleting VM and its associated Resources

38. From the Azure portal, navigate to **Resource groups** and click on the resource group (**demotest-rg**) to open the **Overview** page. Click on **Delete resource group** at the top.



hide01.ir

FIGURE 2.5.36: 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.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 6

Block Management Ports with Azure Security Center to Prevent Brute Force Login Attacks on Virtual Machines in Azure

Azure Security Center's Just-in-Time (JIT) access feature is used to prevent access to the management ports of virtual machines (VMs) when they are not in use.

ICON KEY

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

Lab Scenario

Threat actors search for Azure VMs with open management ports such as RDP/SSH and attempt to access the VMs with brute force login attempts. If the management ports are closed permanently, it may prevent legitimate users from accessing the VMs. Azure Security Center's Just-in-Time (JIT) access feature is used to lock down the inbound connections to VMs, provide access to VMs when required, and reduce exposure to brute force login attacks. This lab demonstrates how to enable JIT Access for a Windows Server VM to restrict RDP access.

Lab Objectives

This lab will demonstrate how to create a resource group, enable Azure Security Center, create a Windows Server VM, and configure JIT access for the VM to prevent remote connections.

In this lab, you will learn the following:

- Creating a resource group in Azure
- Enabling Azure Security Center
- Creating a Windows Server VM
- Testing RDP connection to the VM
- Configuring JIT access for the VM
- Testing RDP connection to the VM after JIT access is enabled

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Granting Temporary RDP Access to the VM

Lab Environment

To perform this lab, you need the following:

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

Lab Duration

Time: 20 minutes

Overview of Azure Security Center Just-in-Time Access

Threat actors search for Azure VMs with open management ports (such as RDP/SSH) and attempt to attack the VMs with brute force login attempts. If a VM is compromised, it can be used as an entry point to attack other Azure resources within the organizational environment. If there are fewer open ports (especially management ports), the attack surface can be reduced. Because legitimate users need to access these VMs, it is not practical to close the management ports permanently. In this case, Azure Security Center's Just-in-Time (JIT) uses network security group (NSG) rules to lock down the inbound traffic to VMs, provide easy access to VMs when required, and reduce exposure to attacks. Cloud security engineers can enable JIT access for VMs and specify the management ports to be kept open or closed, the duration for which the ports should be open, and the IP addresses from which the management ports of these VMs can be accessed.

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 lab. 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.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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**".

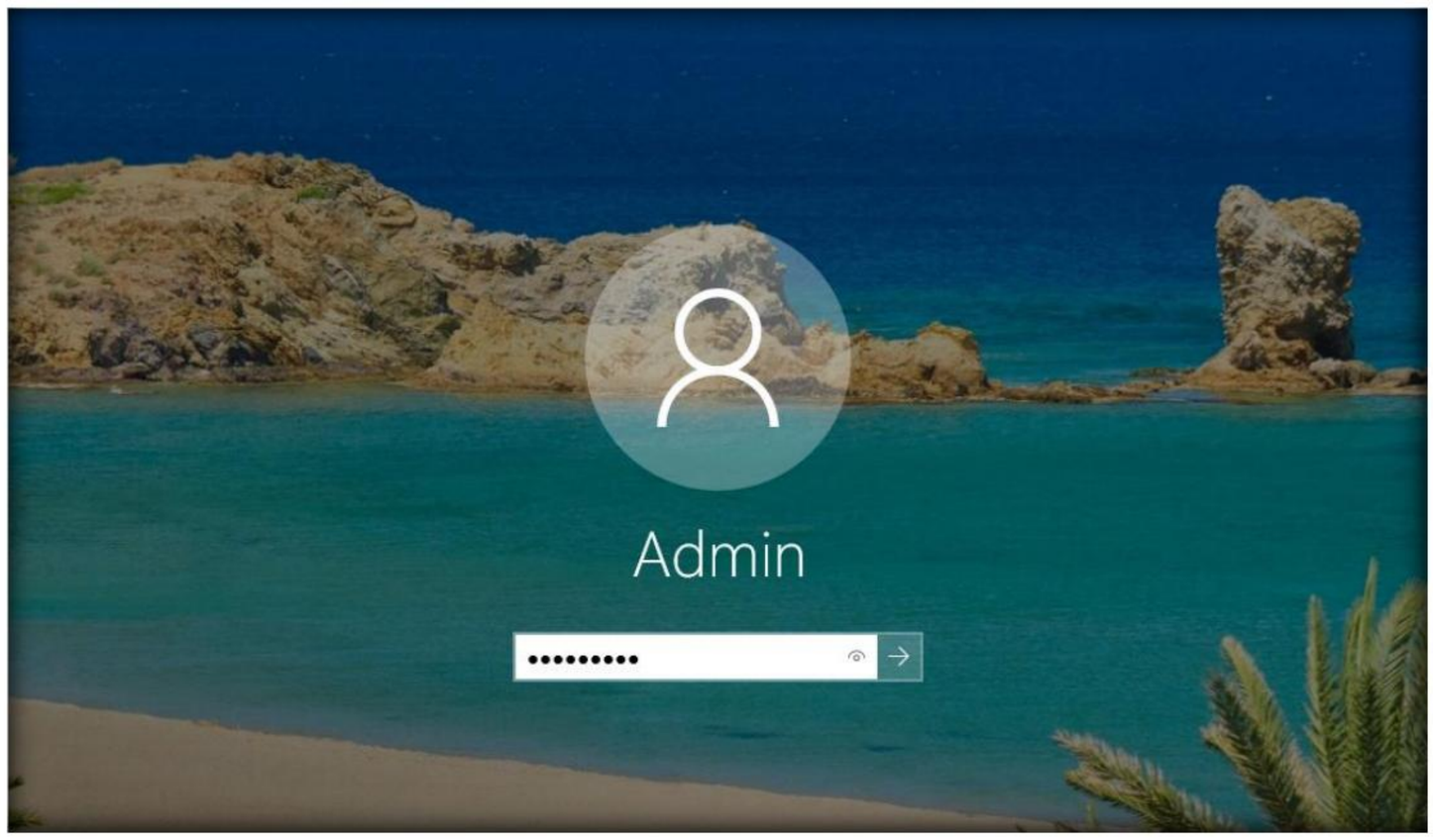


FIGURE 2.6.1: Launch Admin Machine and Log in

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

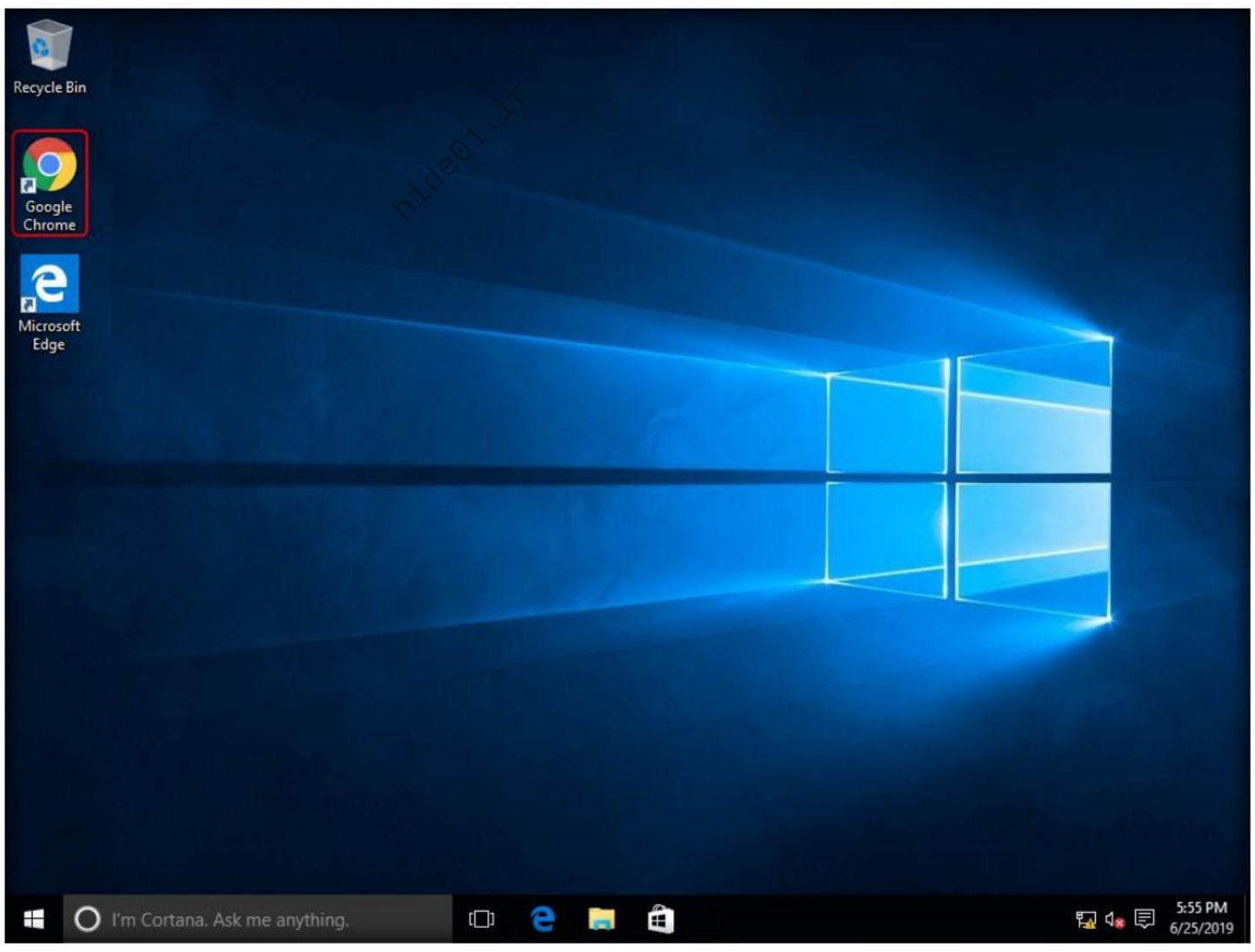


FIGURE 2.6.2: Navigating to the Chrome Browser from Taskbar

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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

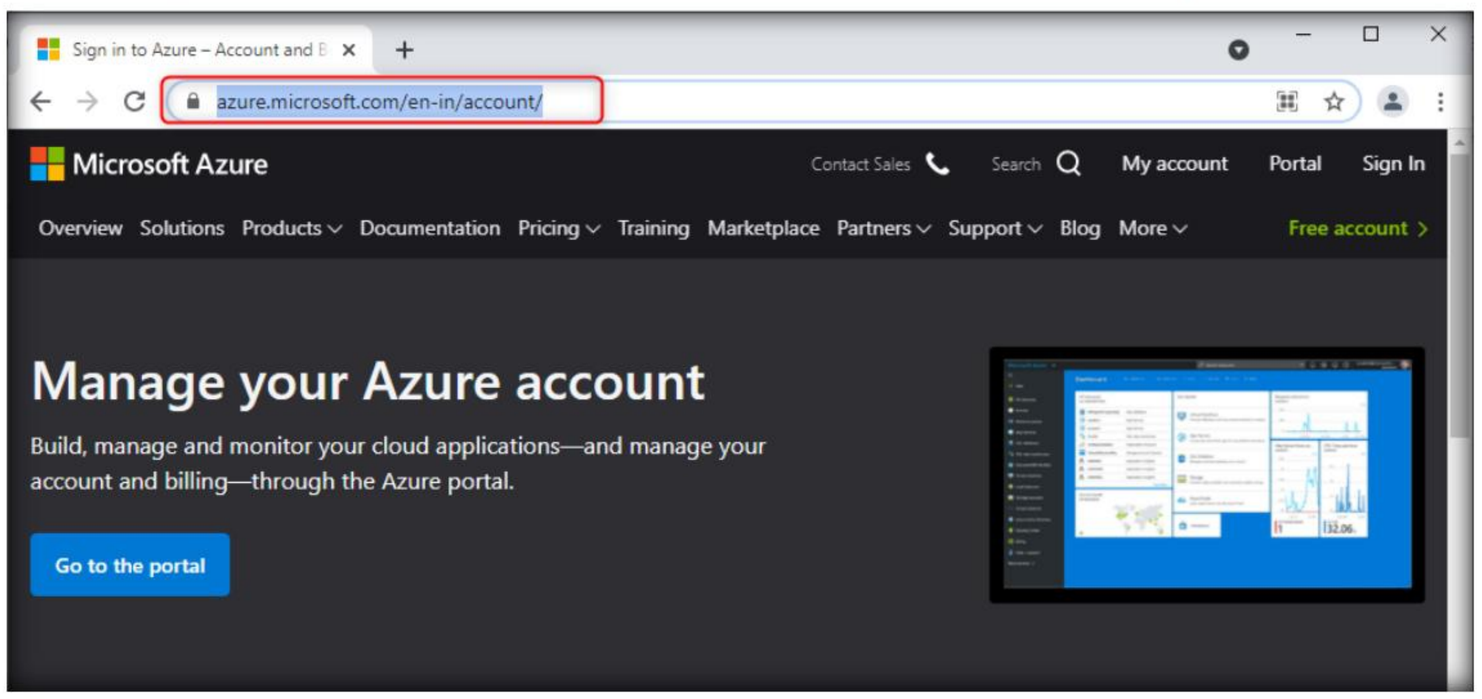


FIGURE 2.6.3: Entering the URL of Microsoft Azure

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

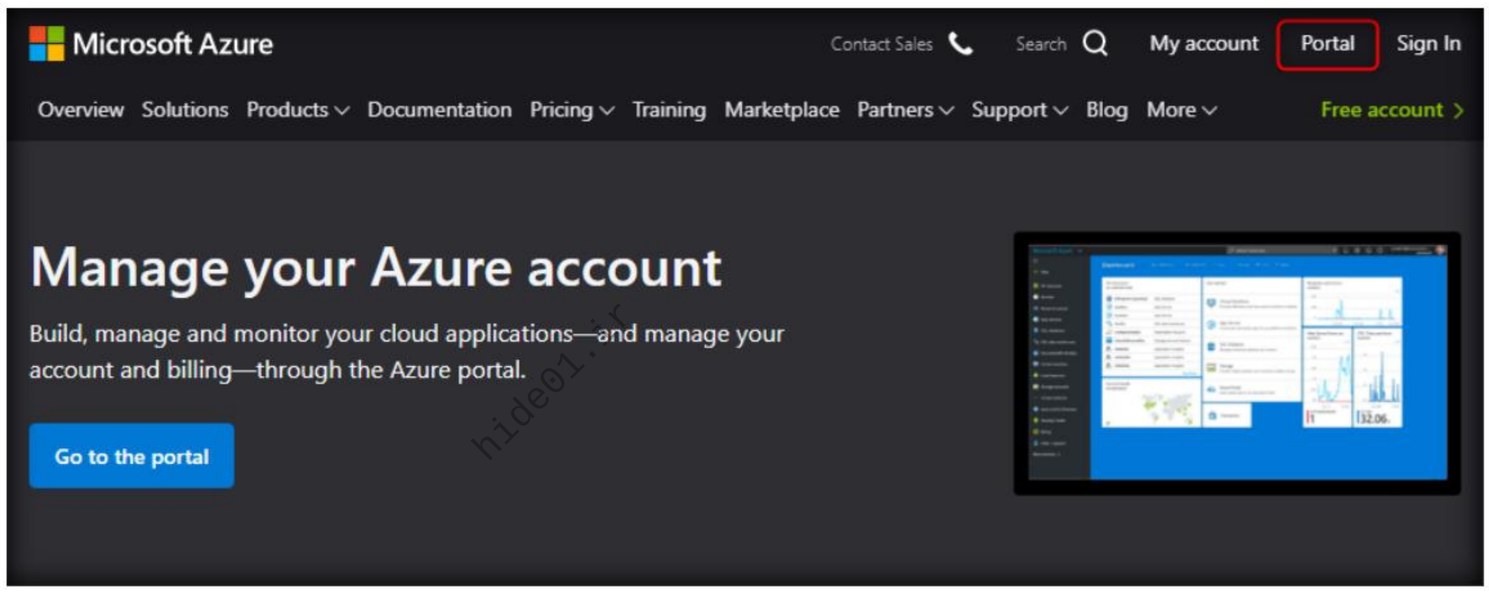


FIGURE 2.6.4: Sign in to Azure Portal

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

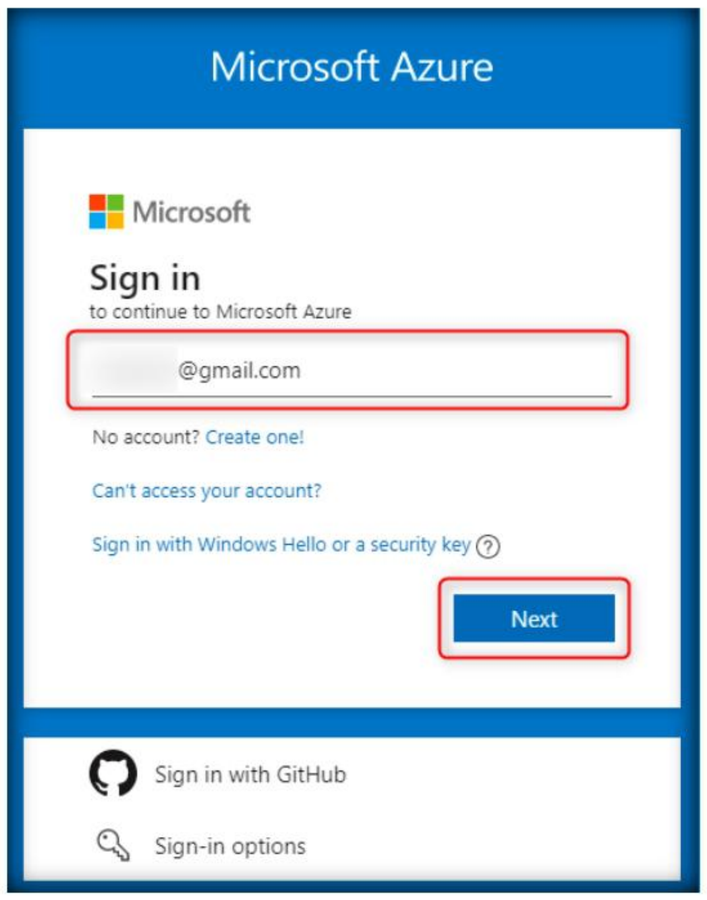


FIGURE 2.6.5: Entering Account ID to Continue

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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

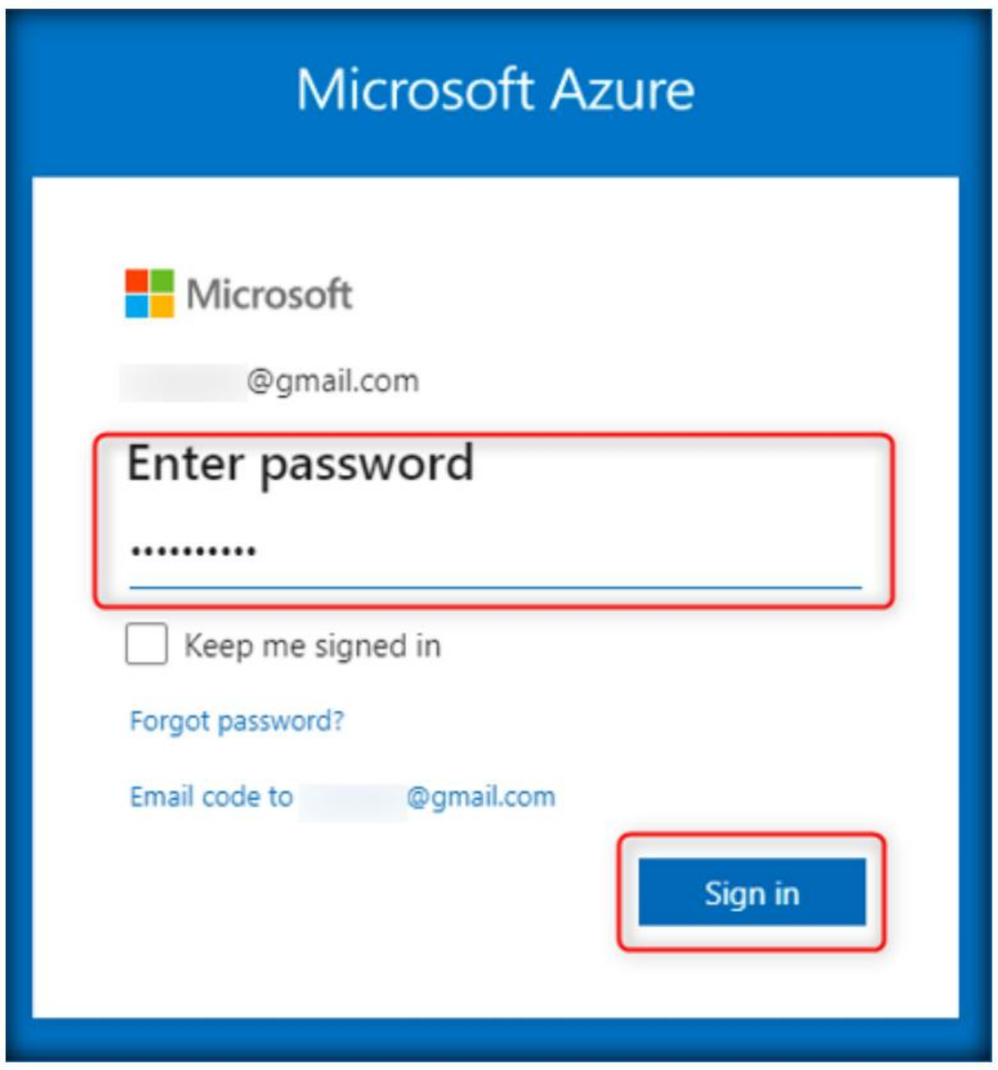


FIGURE 2.6.6: Sign in to Azure Account

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

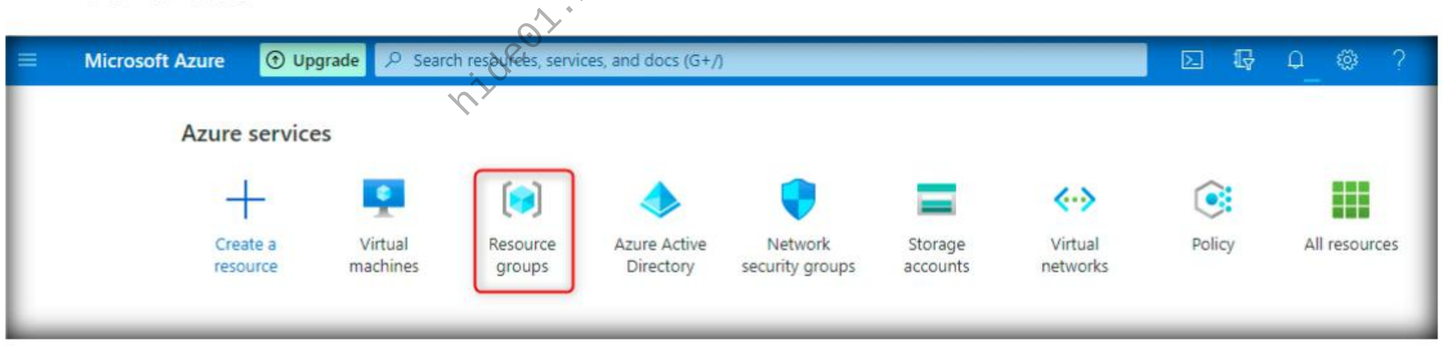


FIGURE 2.6.7: Navigating to Resource Groups

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

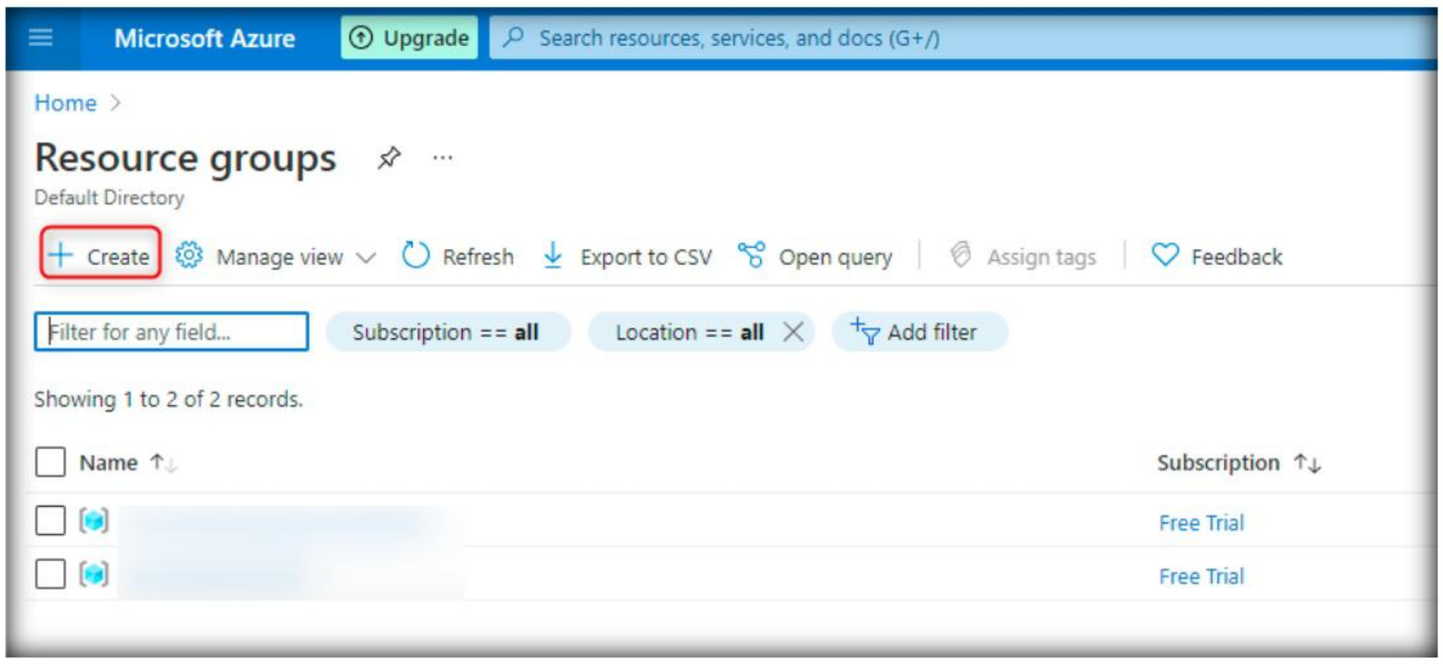


FIGURE 2.6.8: Creating Resource Group

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

9. In the **Create a resource group** window, select **Free Trial** for **Subscription** from the dropdown. Enter a name for **Resource group**. Here, we have given the name "**jitvm-RG**." For **Region**, select an appropriate region. Here, we have selected **East US**. Click on **Next: Tags >**.

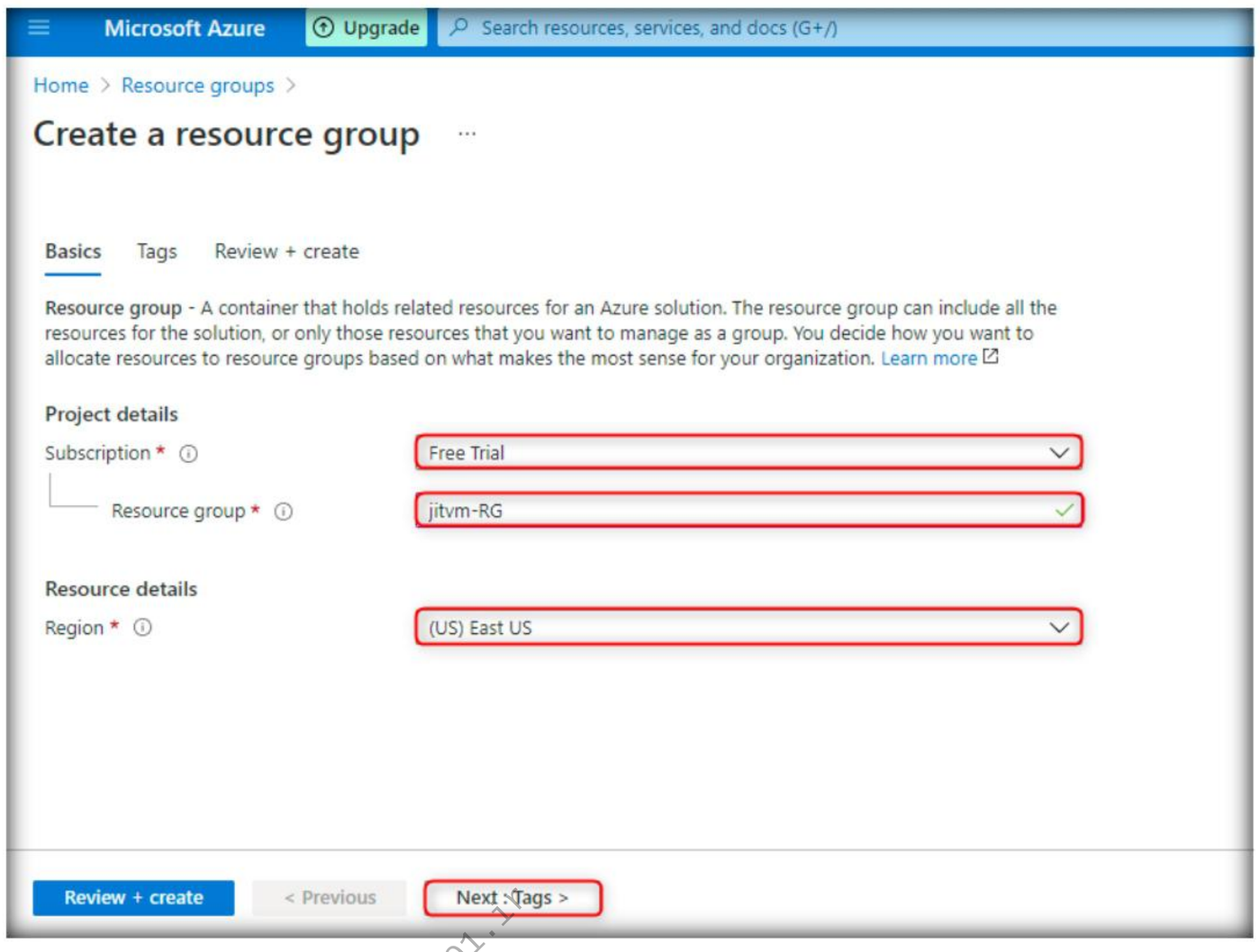


FIGURE 2.6.9: Configuring Resource Group

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

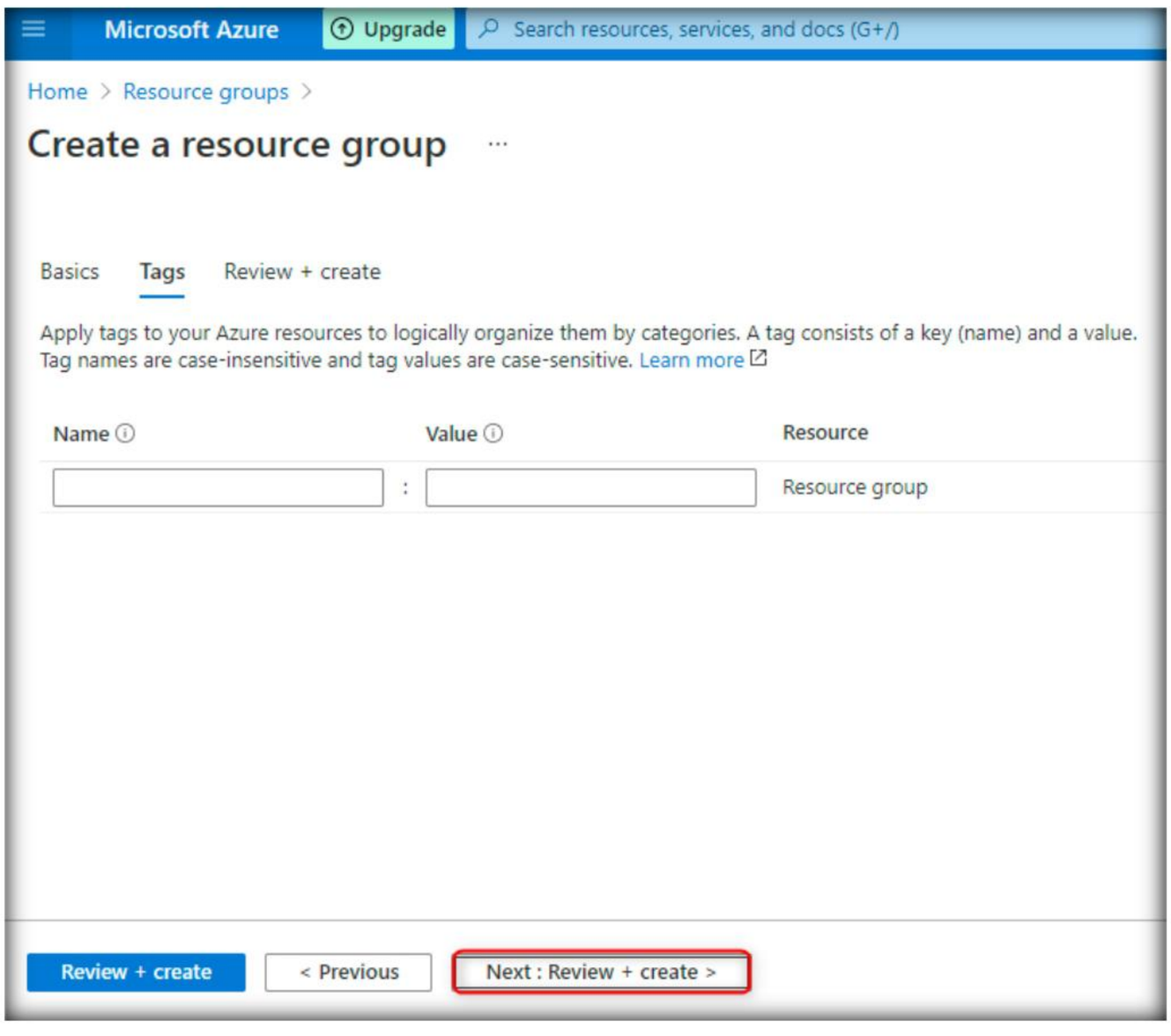


FIGURE 2.6.10: Configuring Resource Group

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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

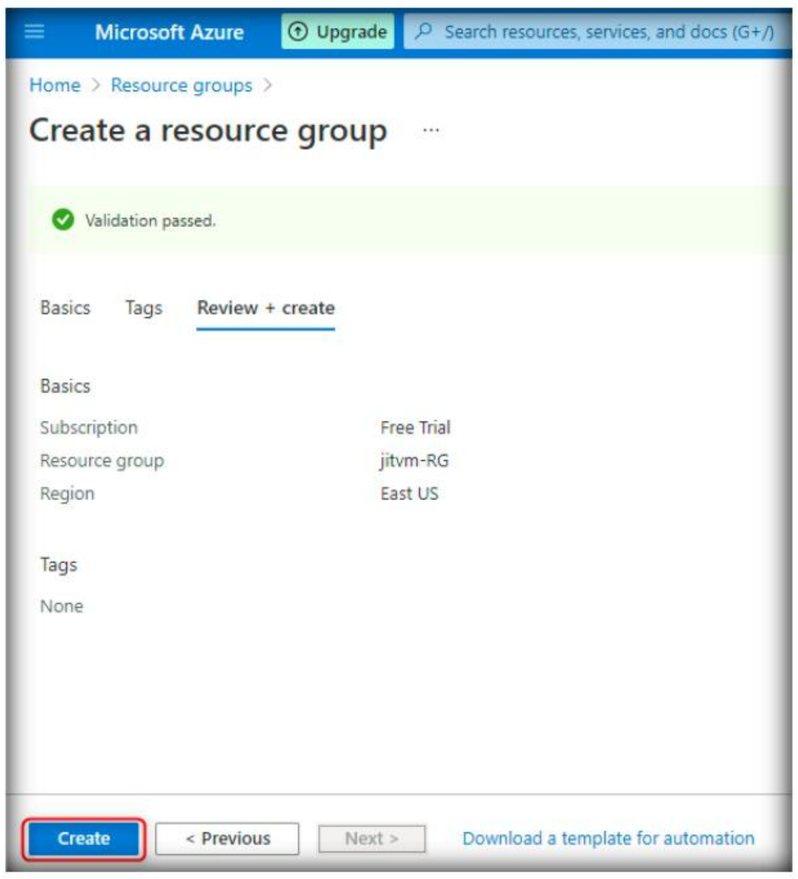


FIGURE 2.6.11: Creating Resource Group

12. Thus, the resource group is successfully created.

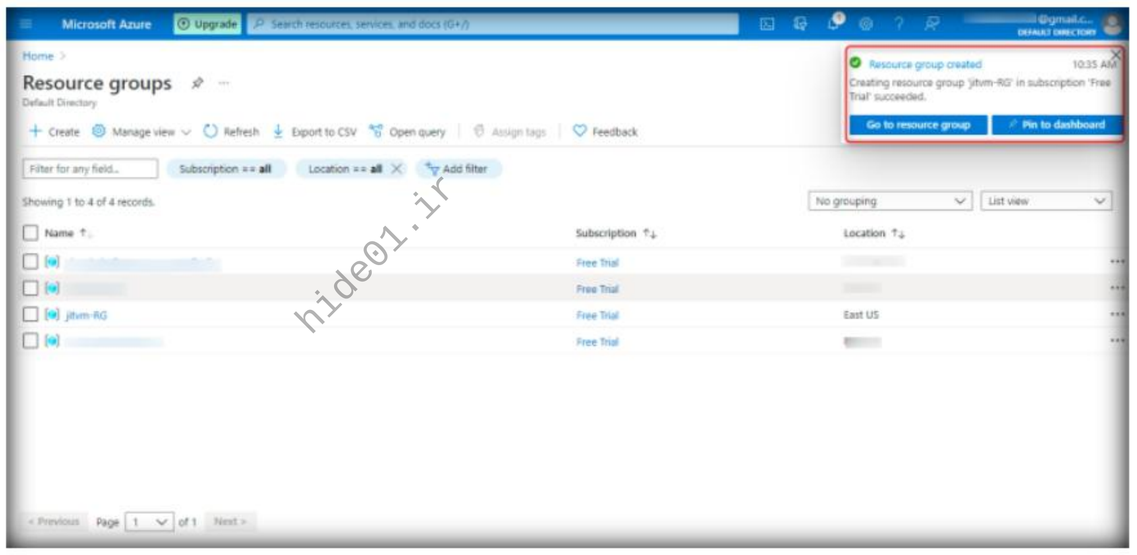


FIGURE 2.6.12: Resource Group Created Successfully

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

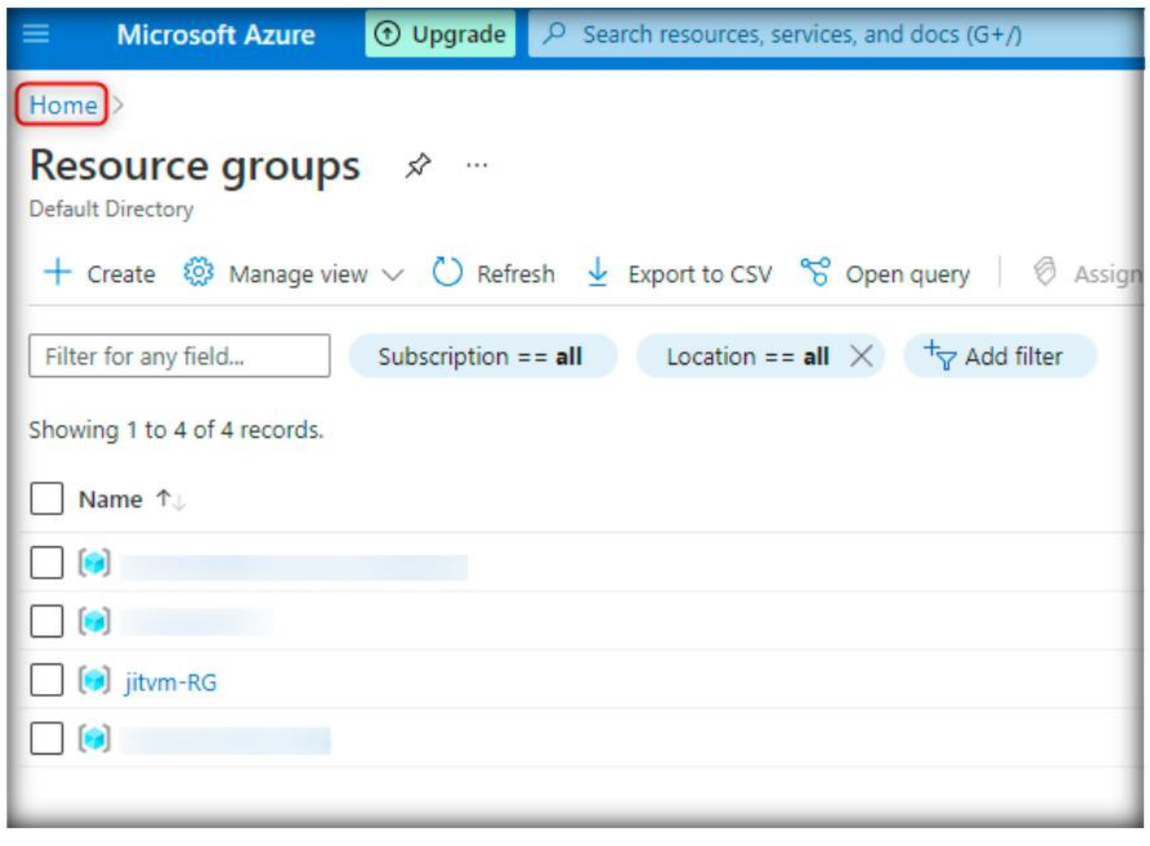


FIGURE 2.6.13: Navigating back to Home Page

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 2

Enabling Azure Security Center

14. Now, enable Azure Security Center if you are using Security Center for the first time. Search for **Security Center** at the top of the Azure portal. Select **Security Center** from the dropdown.

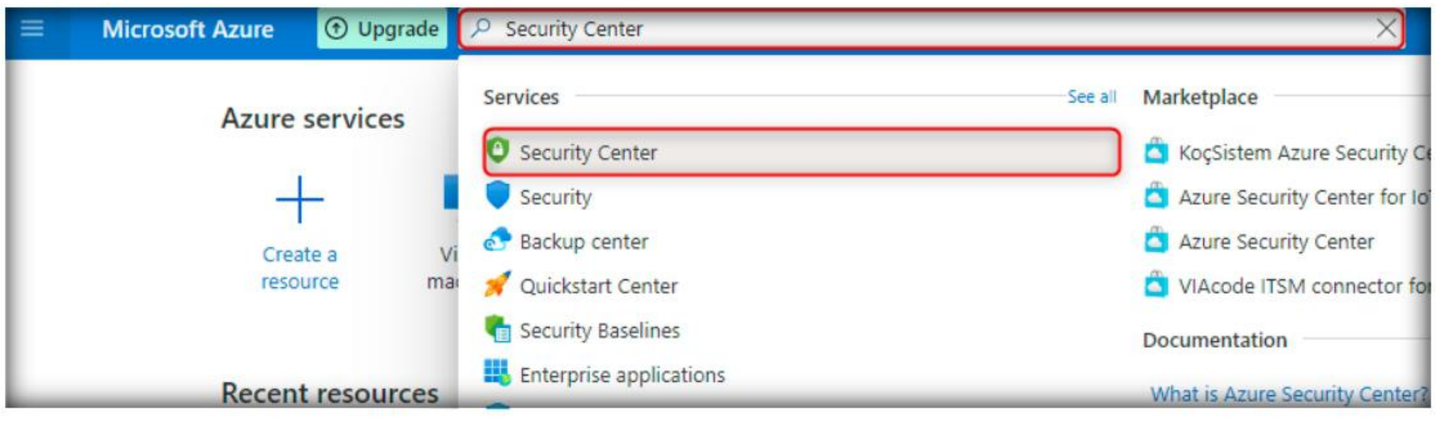


FIGURE 2.6.14: Navigating to Security Center

15. In the **Security Center** window, select **Azure Defender** in the left pane under **Cloud Security**.

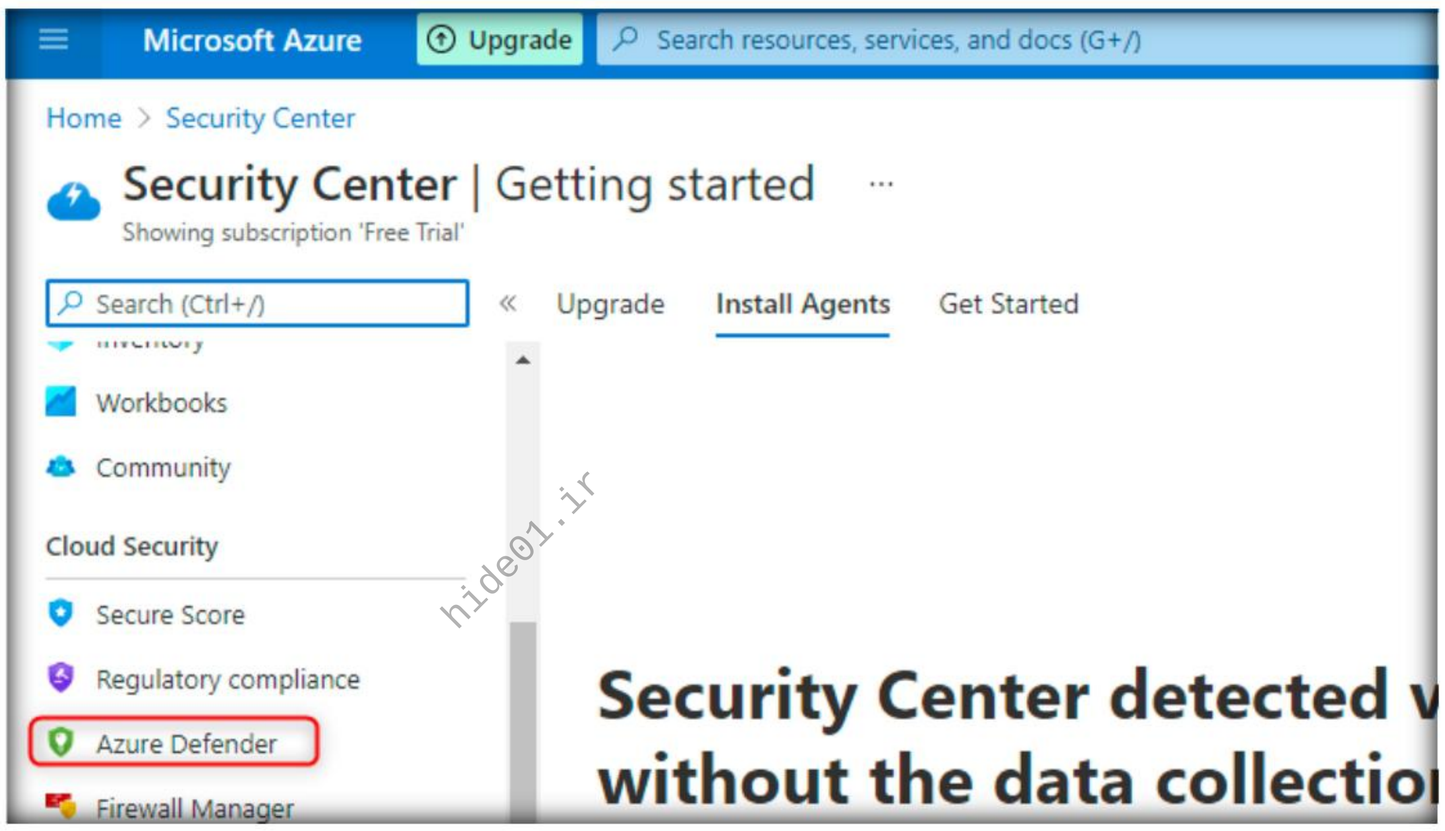


FIGURE 2.6.15: Navigating to Azure Defender

16. In the **Security Center** window, select **Azure Defender** in the left pane under **Cloud Security** and then click on **Enable Azure Defender.**

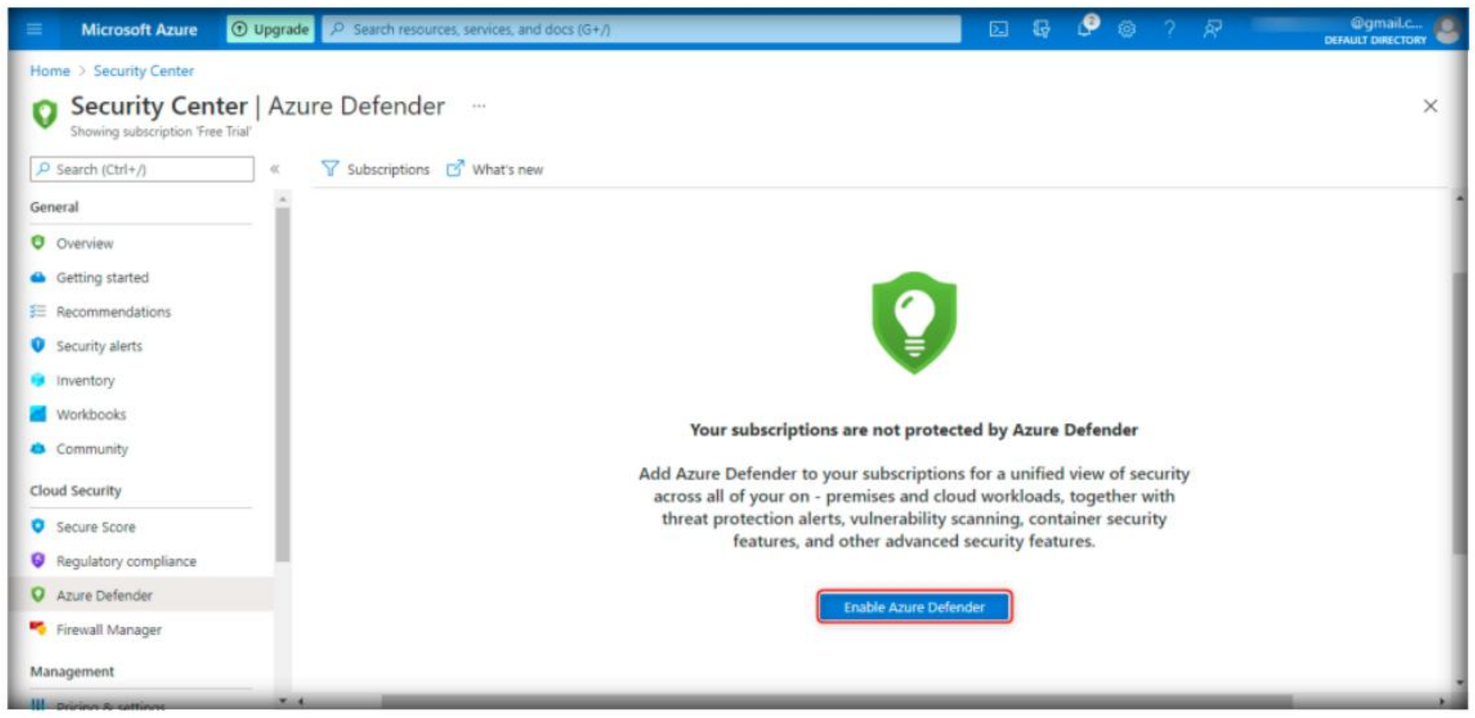


FIGURE 2.6.16: Enabling Azure Defender

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

17. Then, the **Getting started** window opens. Select **Free Trial** under **Enable Azure Defender**.

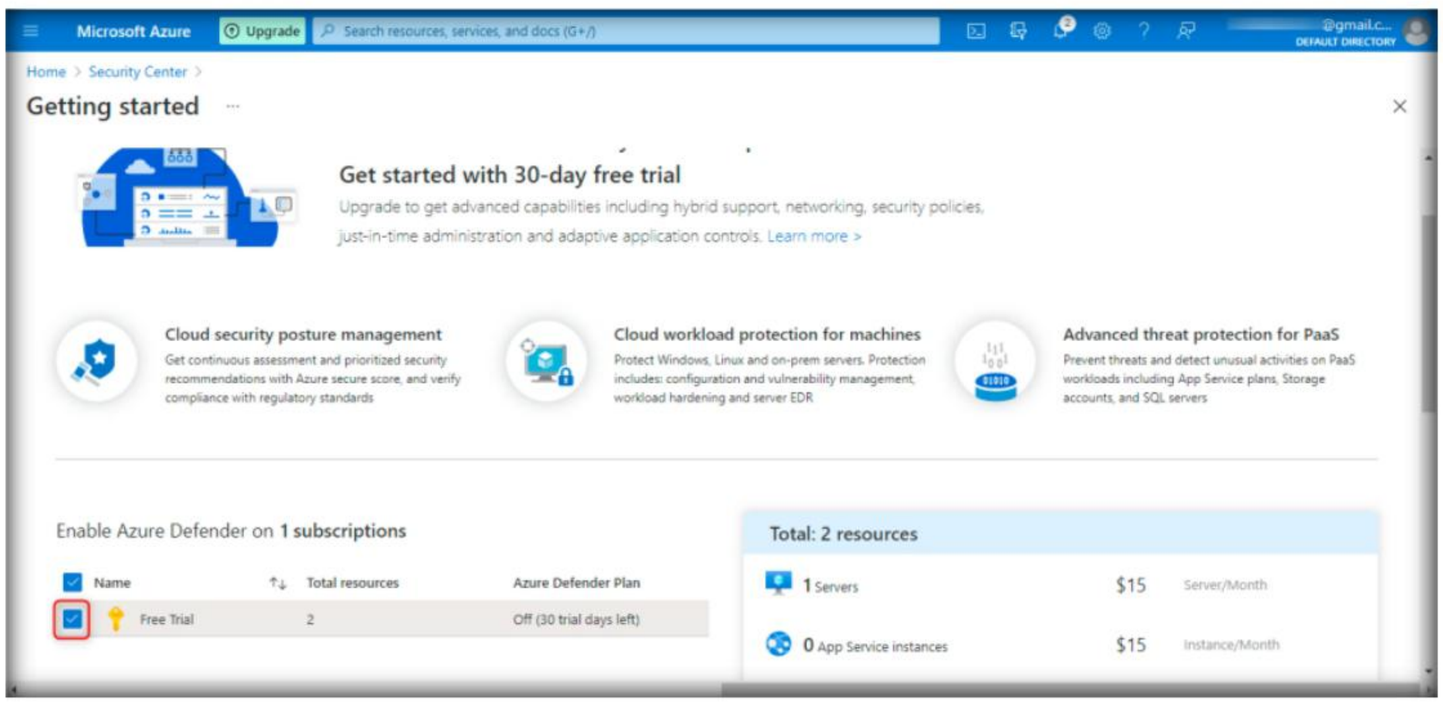


FIGURE 2.6.17: Enabling Azure Defender

18. Scroll down to the bottom and click on **Upgrade**.

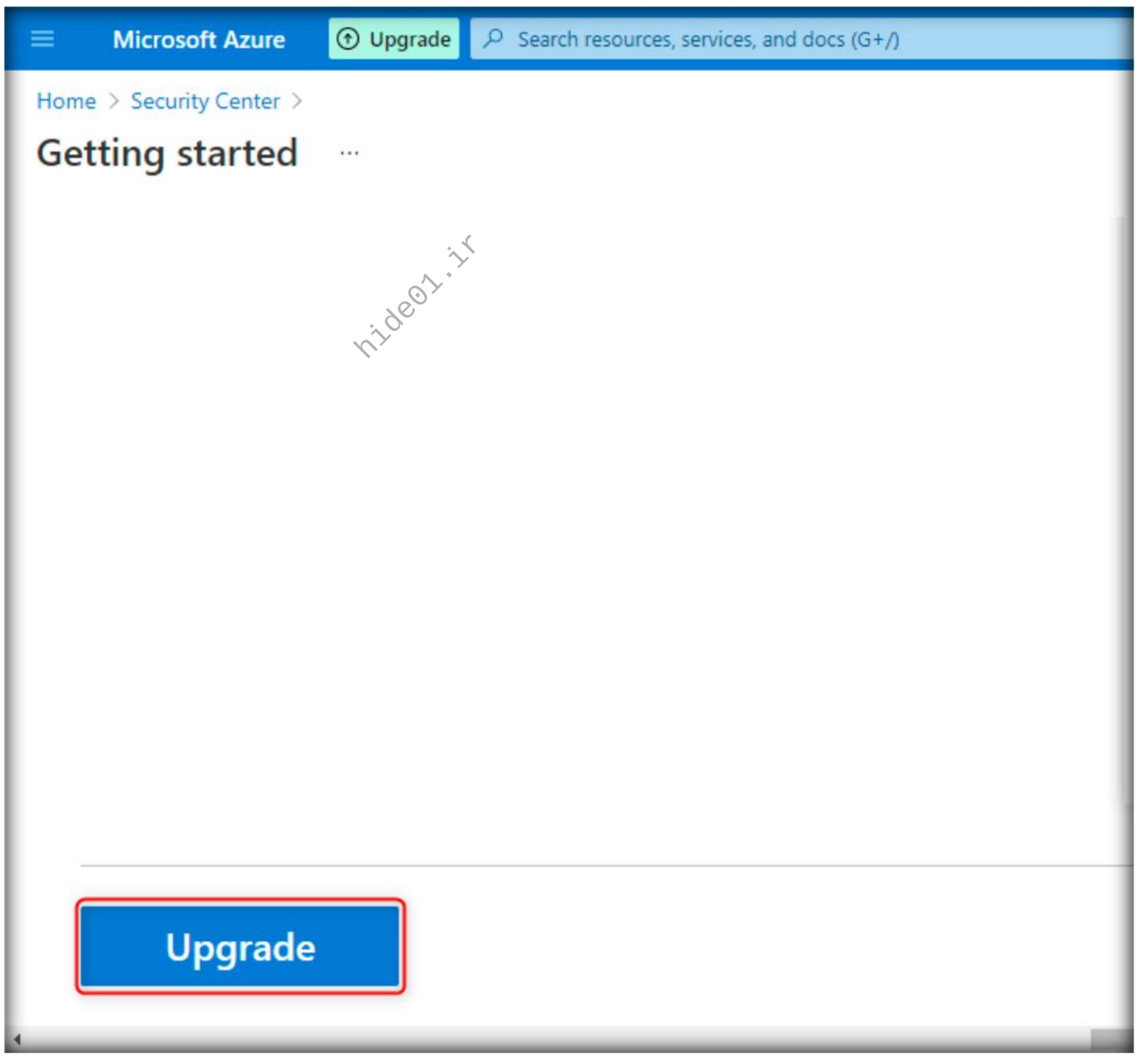


FIGURE 2.6.18: Upgrading to Enable Security Center

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

19. Click on **Install agents** to install the Log Analytics Agent.

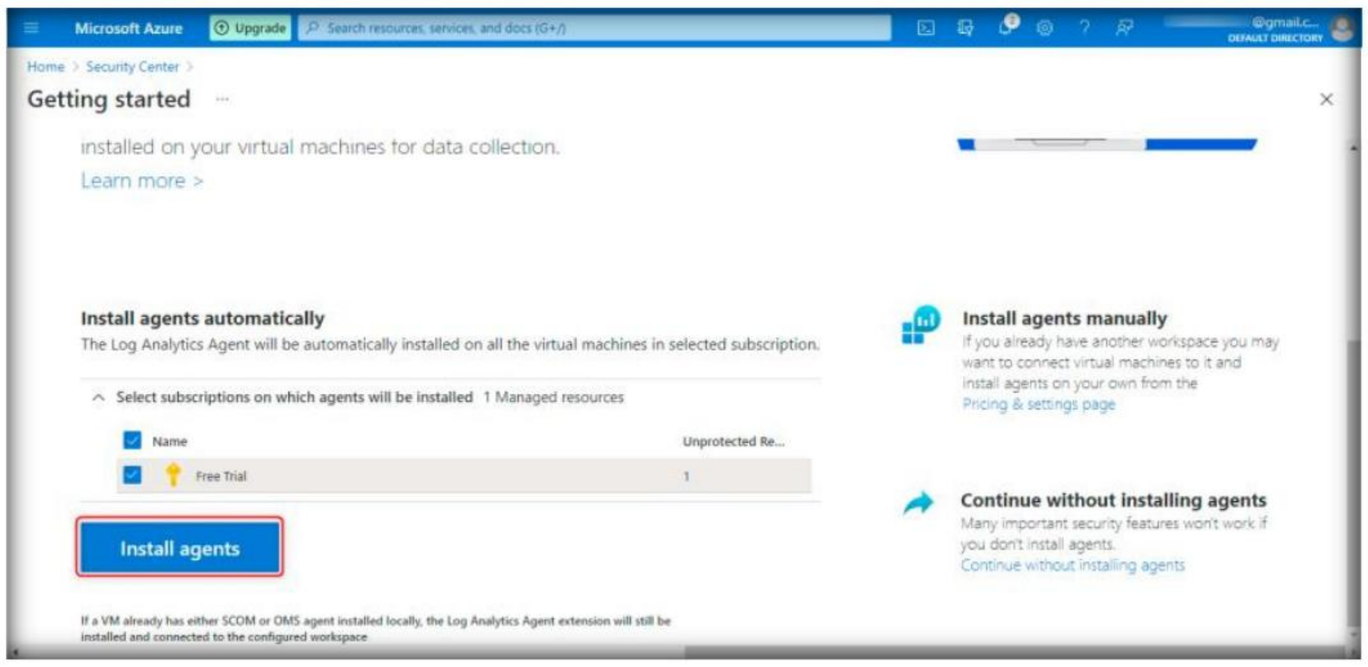


FIGURE 2.6.19: Installing Agents

20. Thus, Azure Defender is enabled and the window shown in the screenshot below is displayed.

    Note: If you are unable to view the window as shown in the screenshot, reload the page.

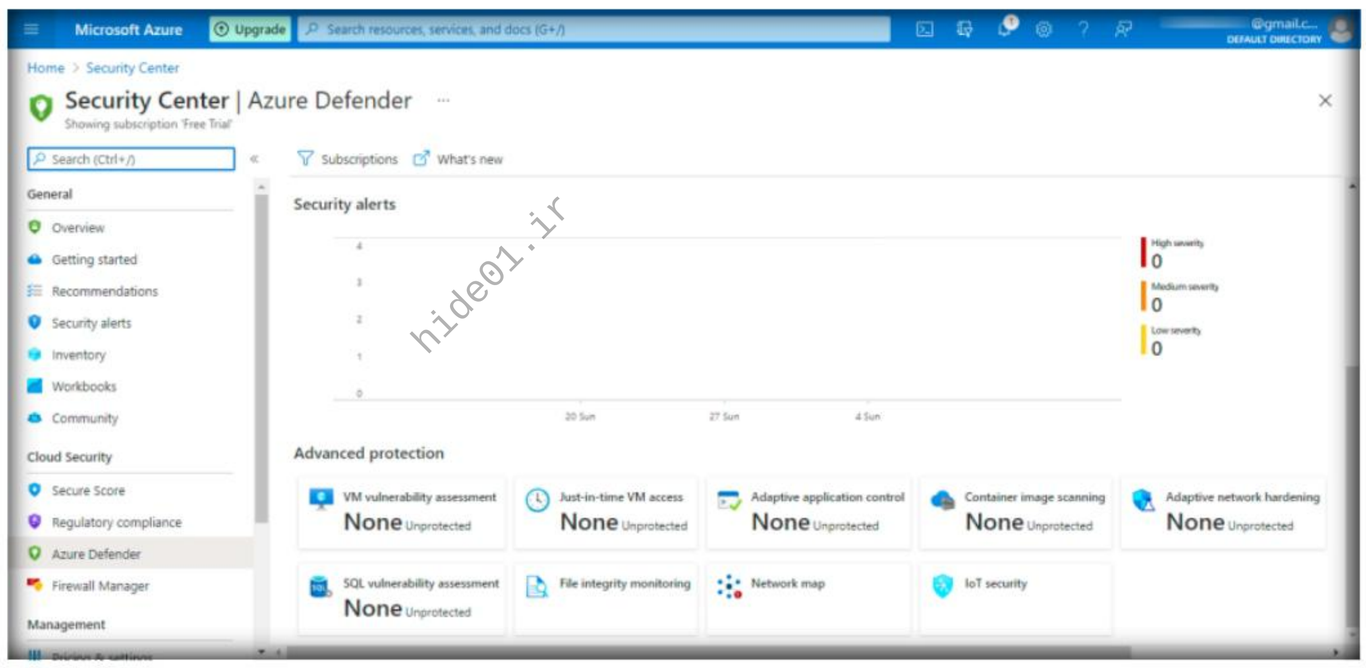


FIGURE 2.6.20: Azure Defender is Enabled

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

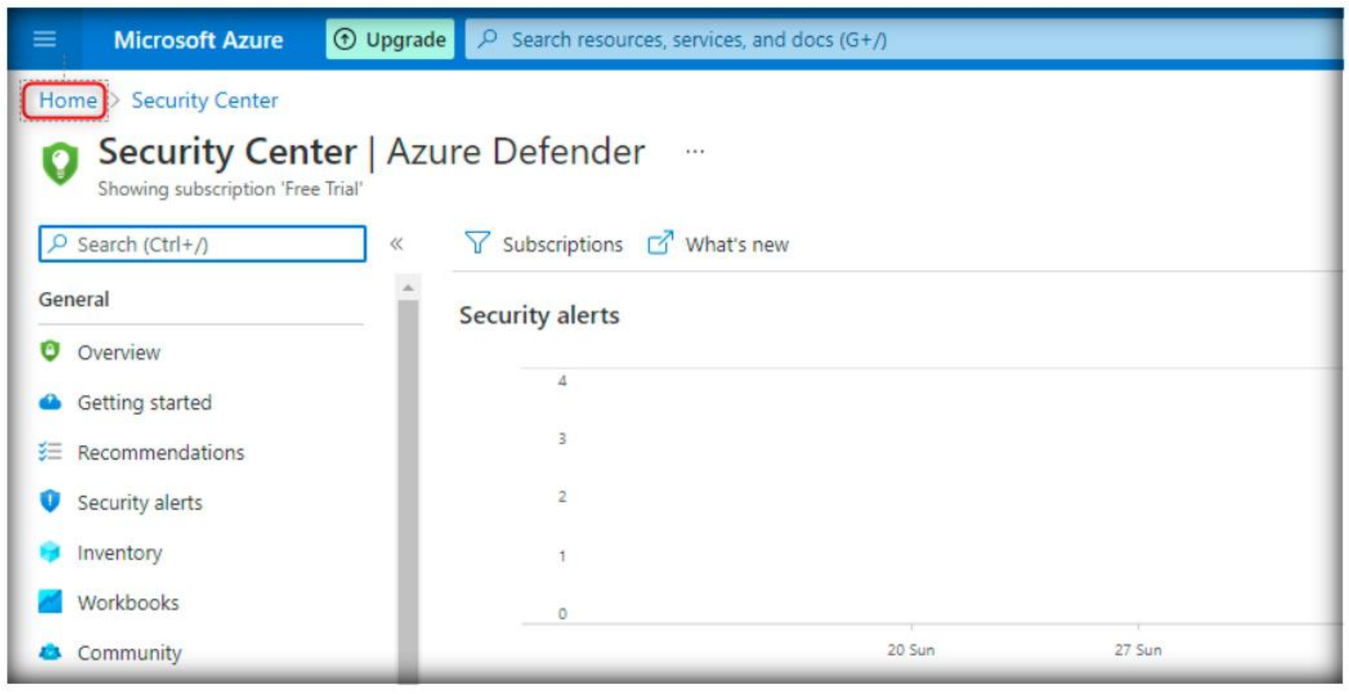


FIGURE 2.6.21: Navigating back to Home Page

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 3

Creating a Windows Server VM

22. Next, create a Windows Server VM. Click on **Virtual machines** under **Azure services** in the home page of the Azure portal.



FIGURE 2.6.22: Navigating to Virtual Machines

23. The **Virtual machines** window appears. Click on **+Create** and select **+ Virtual machine** to create the VM.

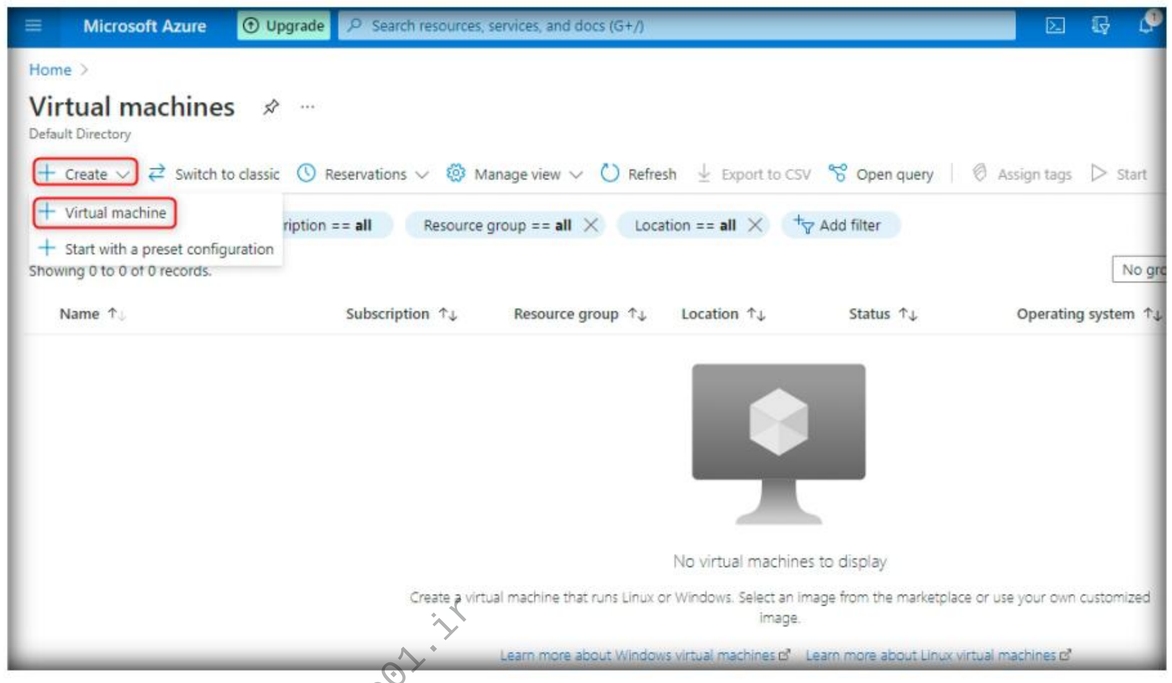


FIGURE 2.6.23: Creating VM

24. In the **Create a virtual machine** window, select **Free Trial** under the **Subscription** dropdown. Select the **Resource Group** (**jitvmRG**) created by you in the previous task. Under **Instance details**, enter a name under **Virtual machine name**. Here, we have used the name **jit-VM**. For **Region**, select an appropriate region in which your VM is to be deployed. Here, we have selected **East US**.

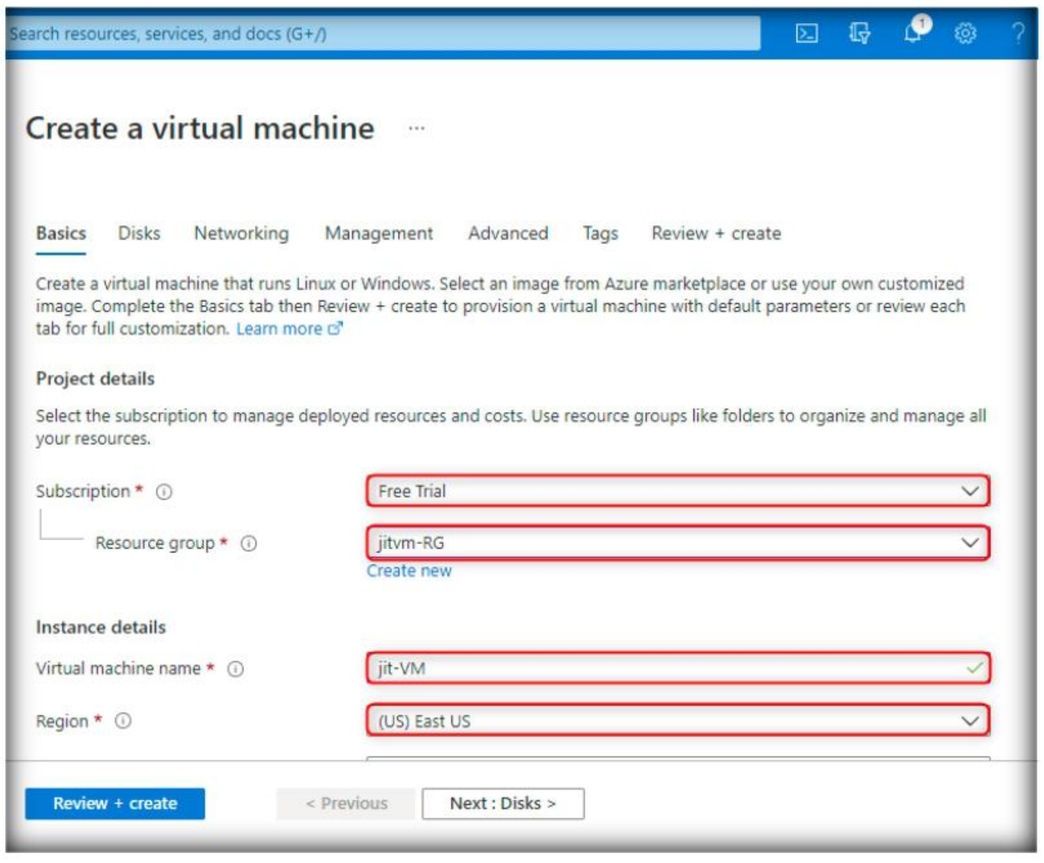
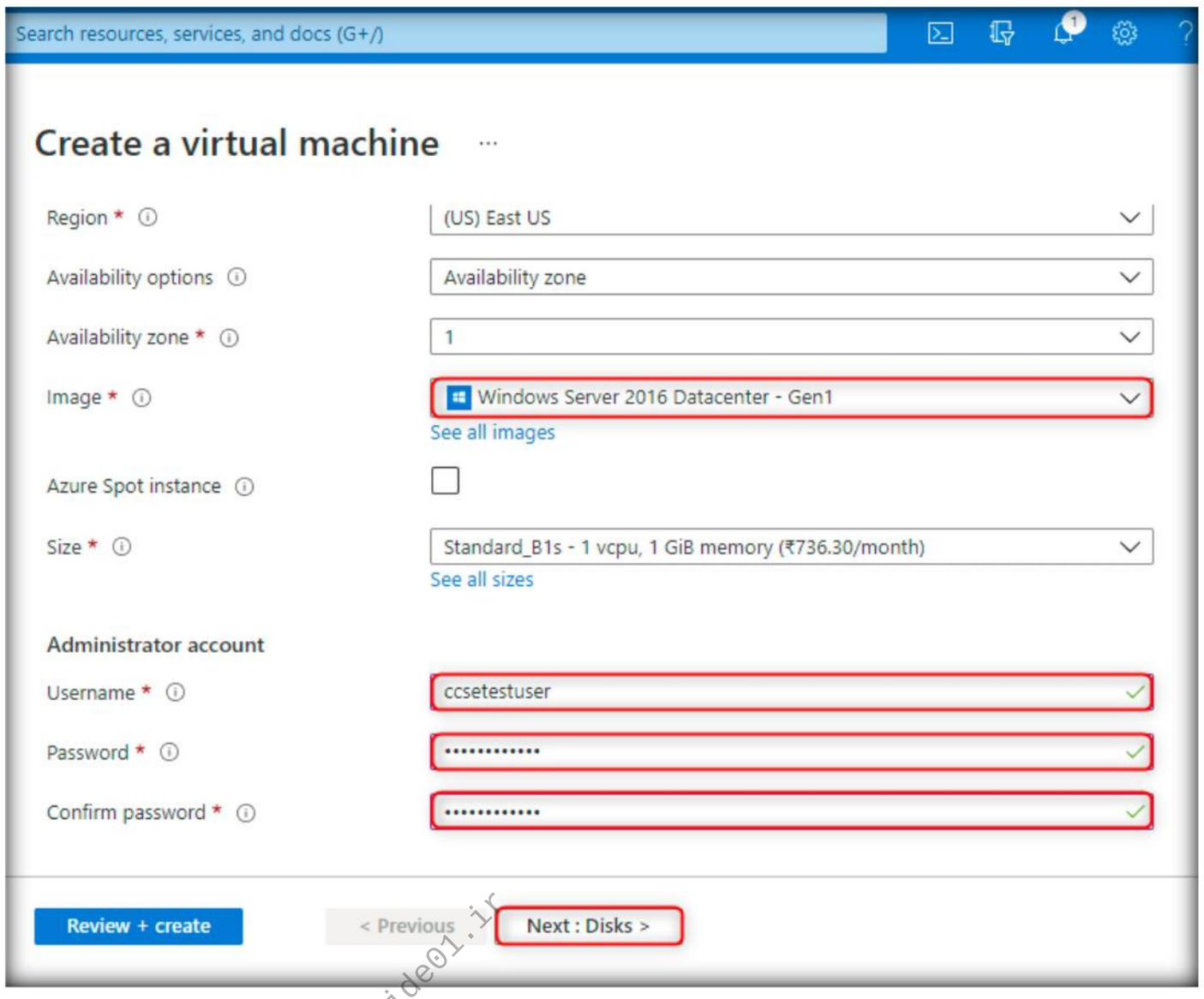


FIGURE 2.6.24: Configuring VM

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

25. Scroll down to the bottom. For **Image**, select **Windows Server 2016 Datacenter -Gen1**. Under **Administrator account**, enter a **Username**; here, we have used **ccsetestuser**. Enter a **Password,** followed by **Confirm password**. Click on **Next : Disks >**.



hide01.ir

FIGURE 2.6.25: Configuring VM

26. In the **Disks** tab, do not change the default settings. Click on **Next : Networking >**.

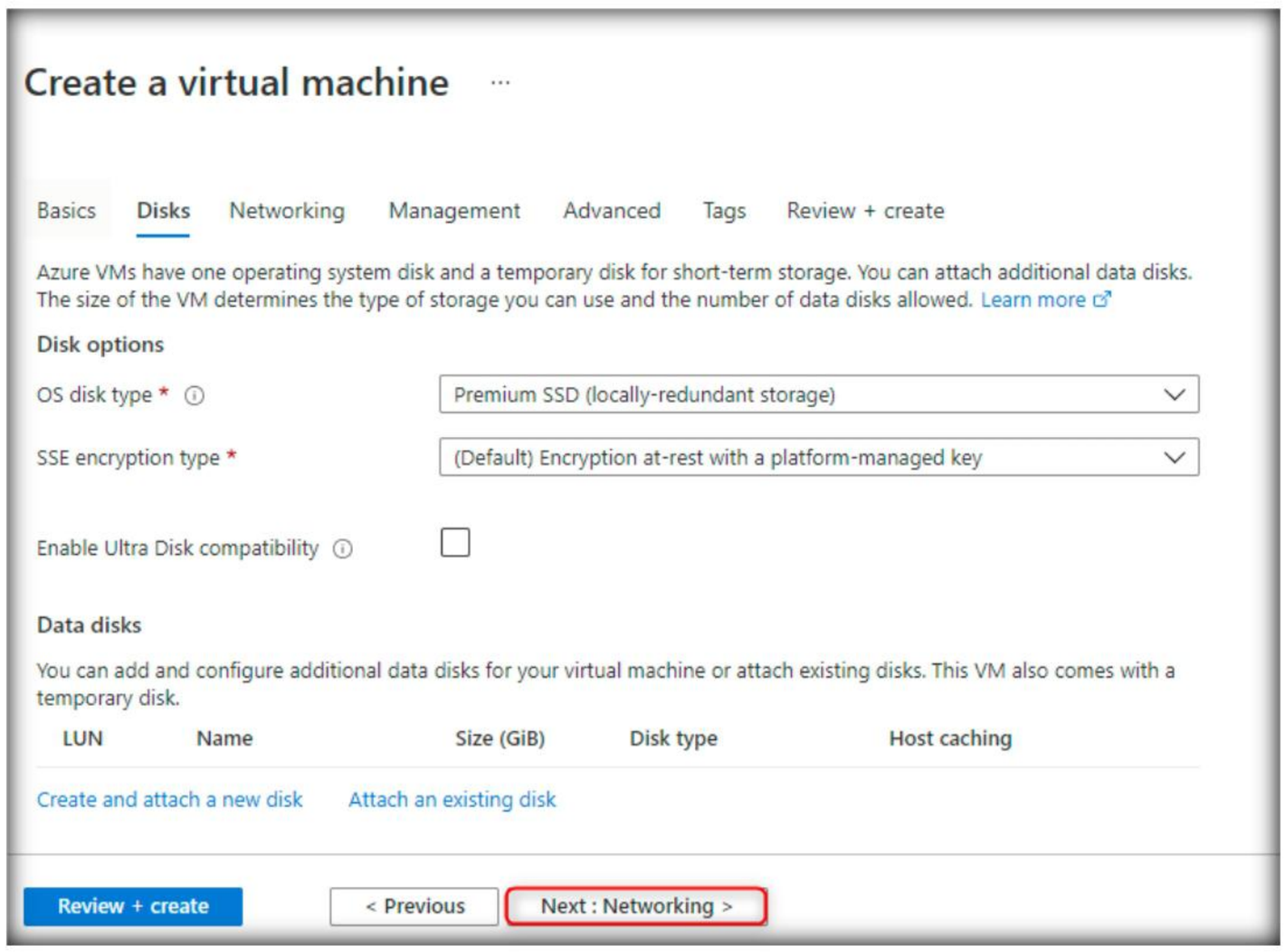


FIGURE 2.6.26: Proceeding with Creating the VM

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

27. For **Networking**, do not change the default settings. Click on **Next : Management >**.

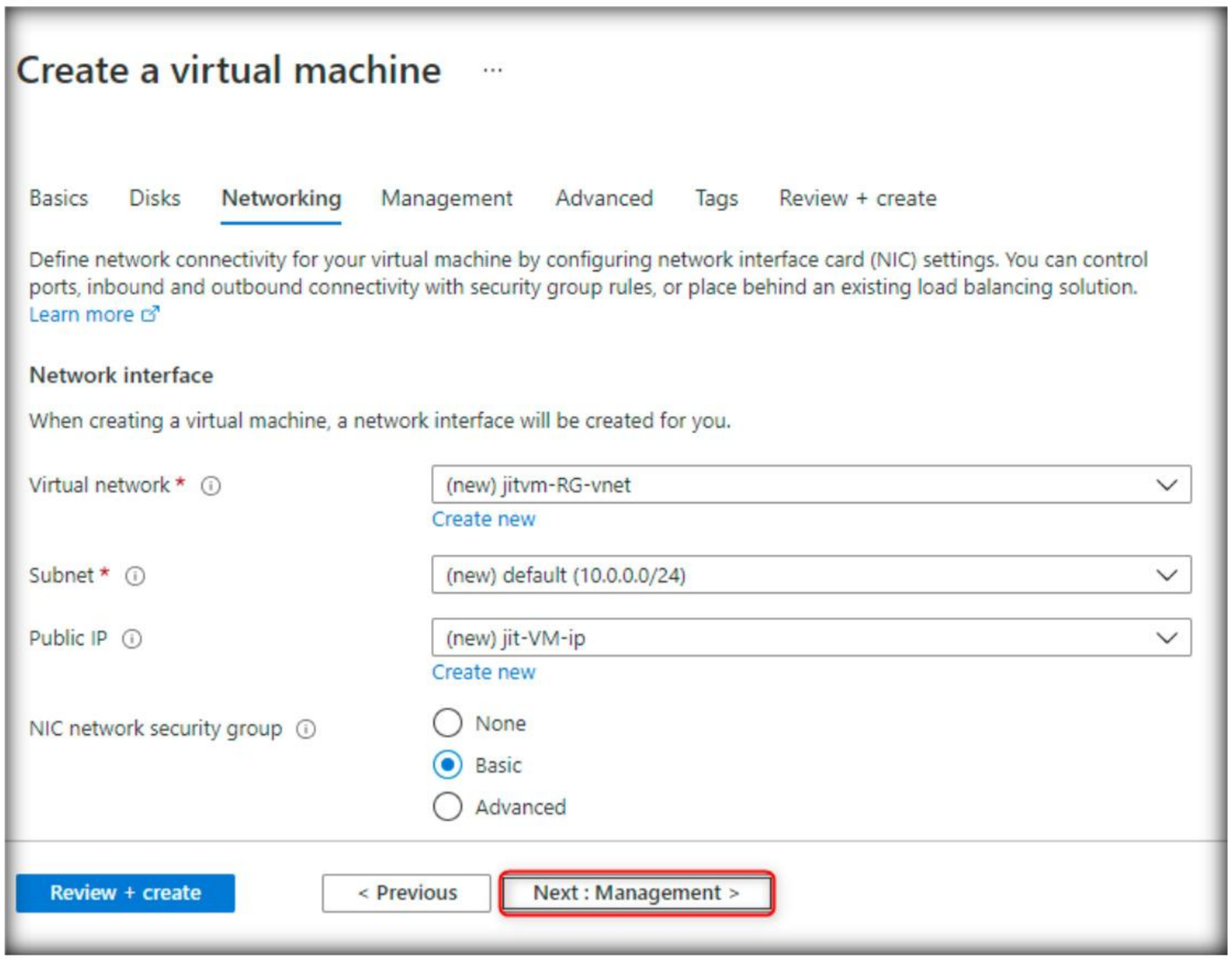


FIGURE 2.6.27: Proceeding with Creating the VM

28. For **Management**, do not change the default settings. Click on **Next : Advanced >**.

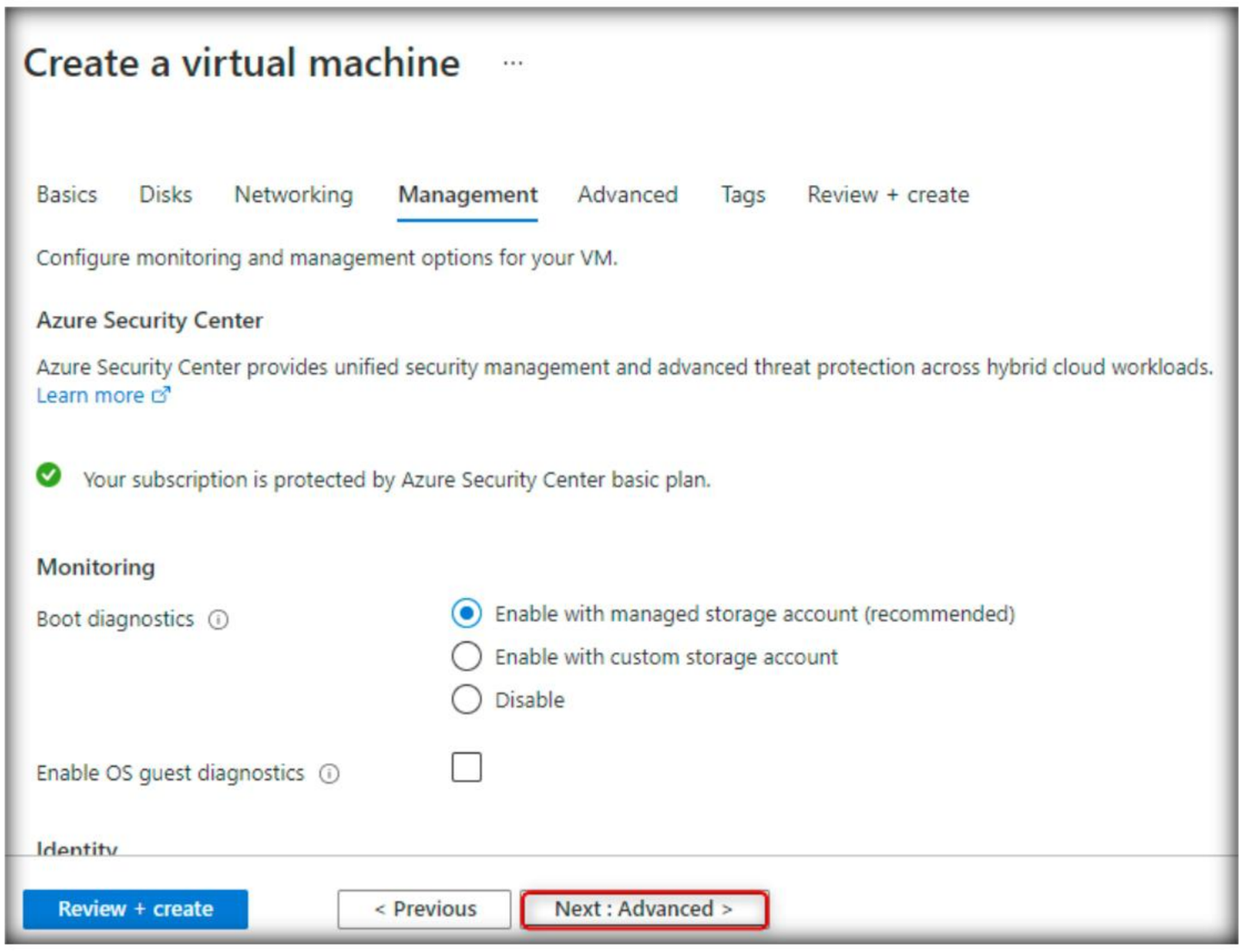


FIGURE 2.6.28: Proceeding with Creating the VM

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

29. Click on **Next : Tags>** in the **Advanced** tab.

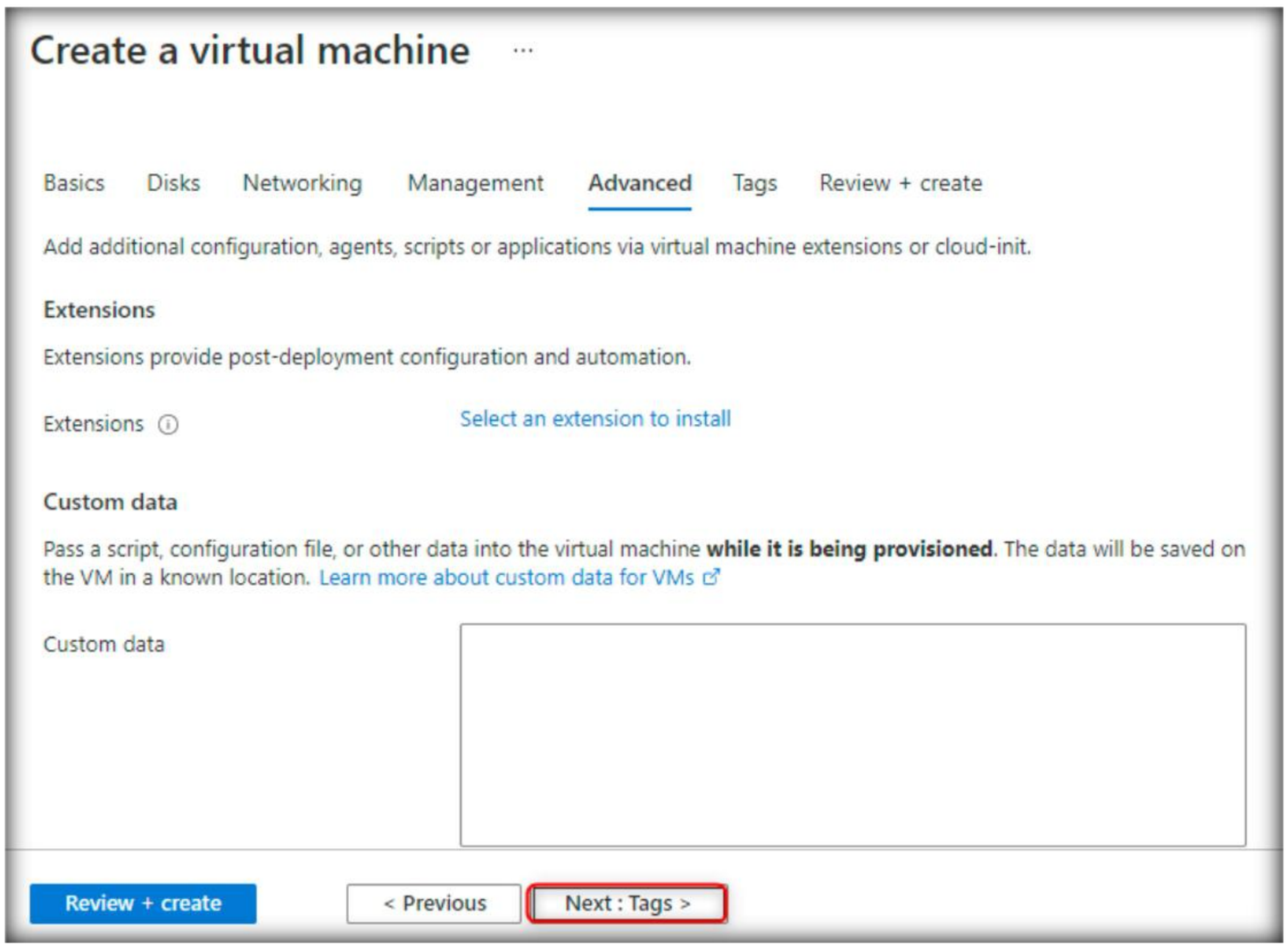


FIGURE 2.6.29: Proceeding with Creating the VM

30. In the **Tags** tab, click on **Next : Review + create >.**

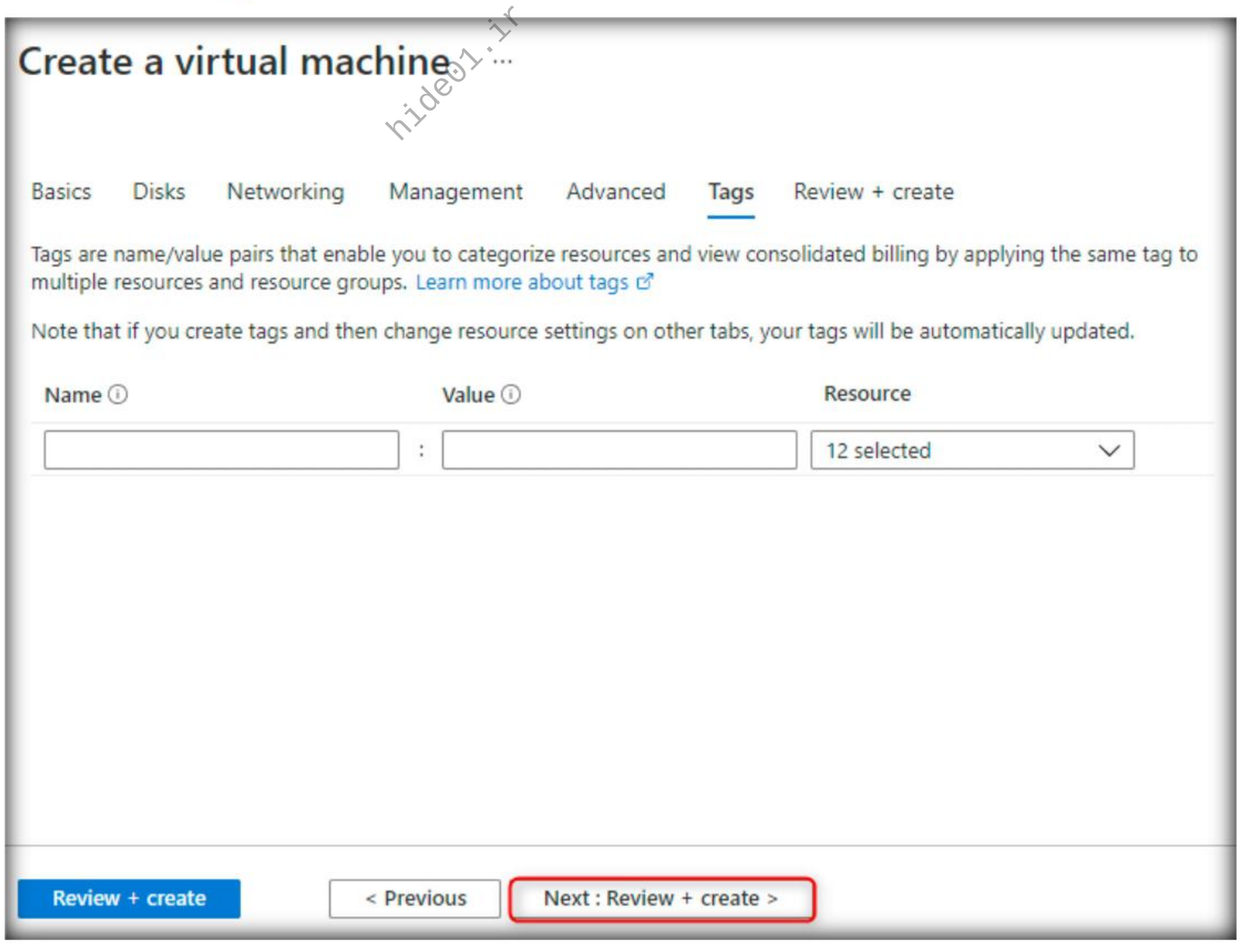


FIGURE 2.6.30: Reviewing and Creating the VM

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

31. Click on **Create** to create the VM.

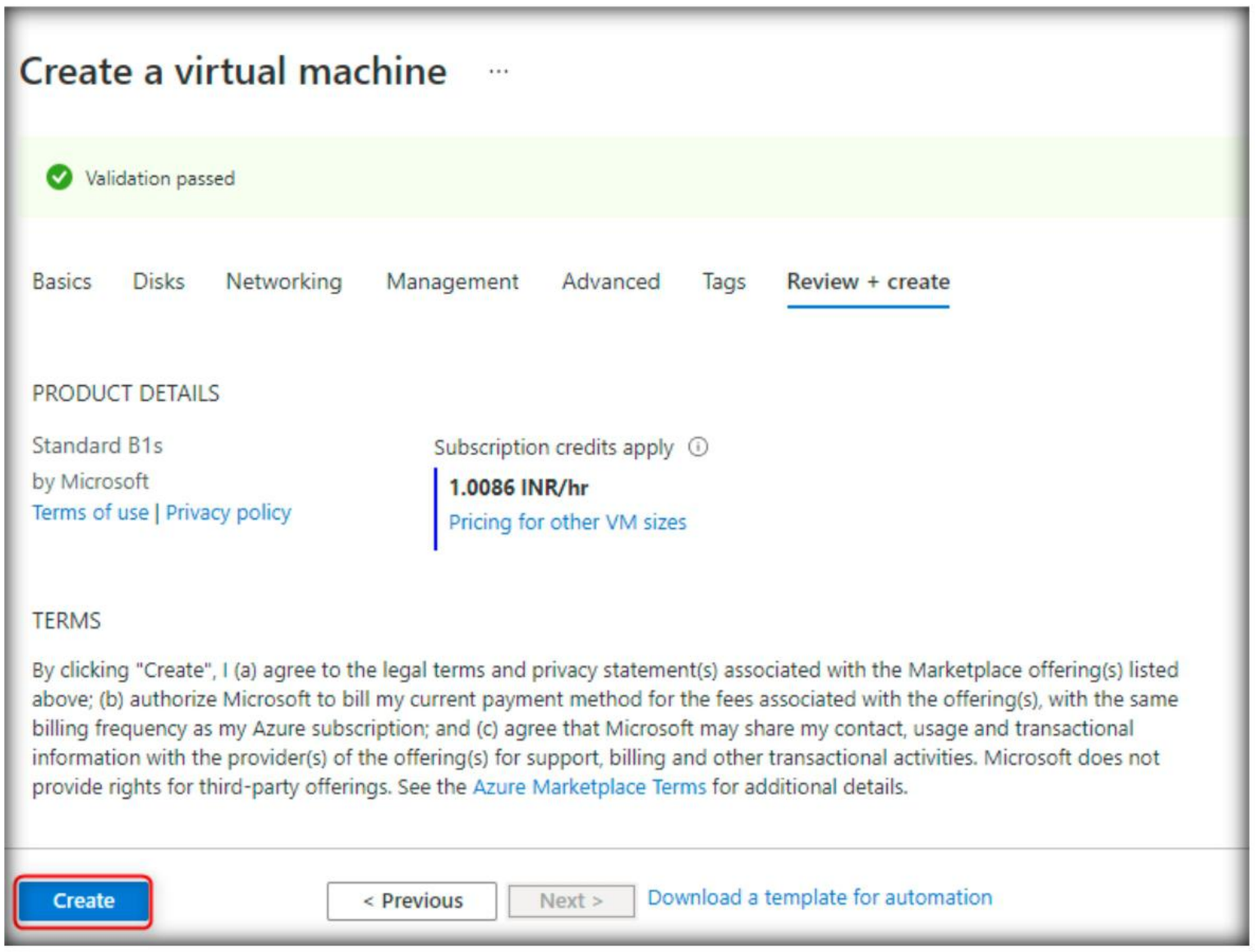


FIGURE 2.6.31: Creating VM

32. Thus, the VM is successfully created.

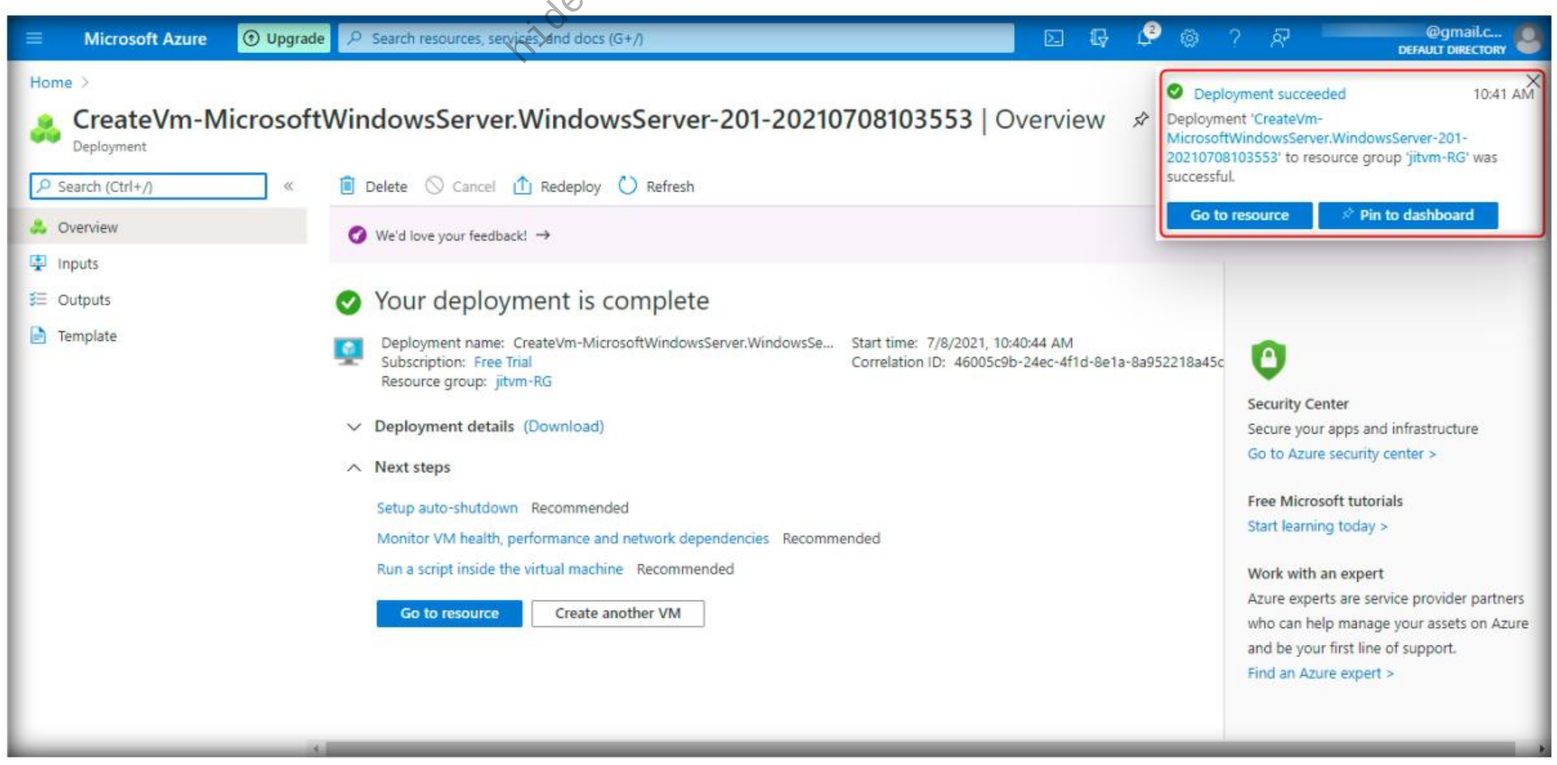


FIGURE 2.6.32: VM Created Successfully

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 4

Testing RDP connection to the VM

33. Now, test whether an RDP connection can be established to the Windows Server VM. Click on **Go to resource** to get the public IP address of the VM.

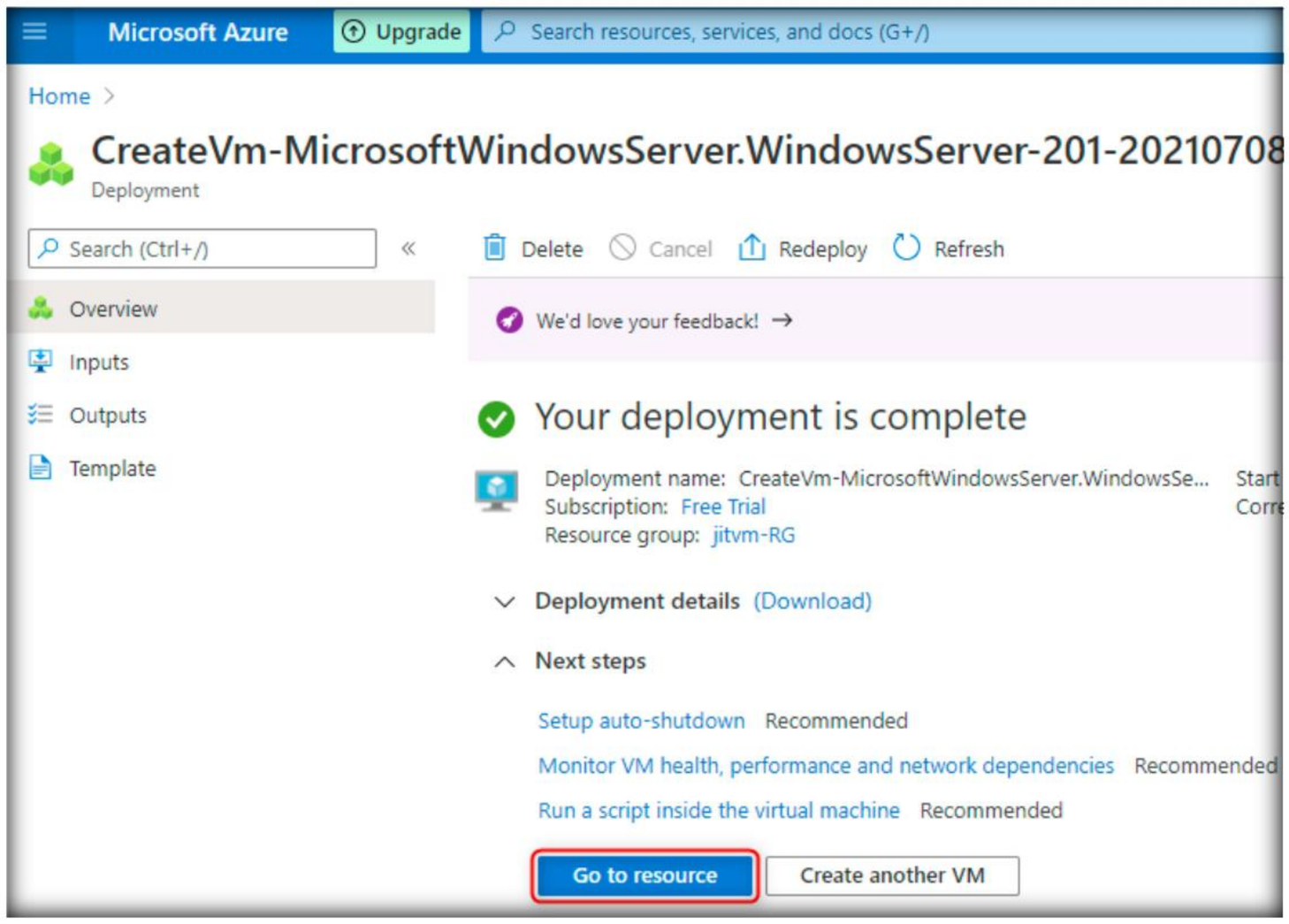


FIGURE 2.6.33: Navigating to the VM

34. Note the **Public IP address** of the VM.

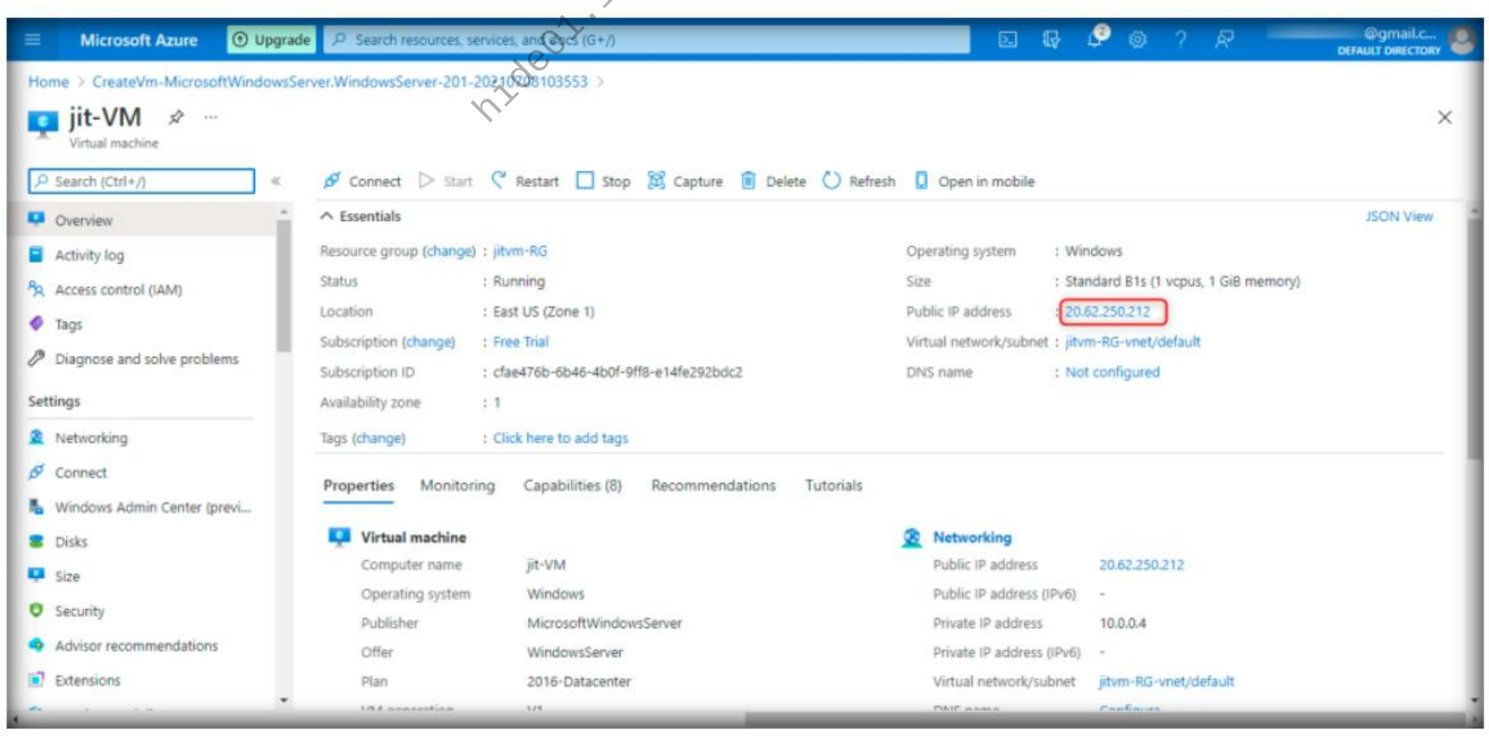


FIGURE 2.6.34: Copying the Public IP address

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

35. Now, search for **Remote Desktop Connection** in Windows search box and press **Enter**.

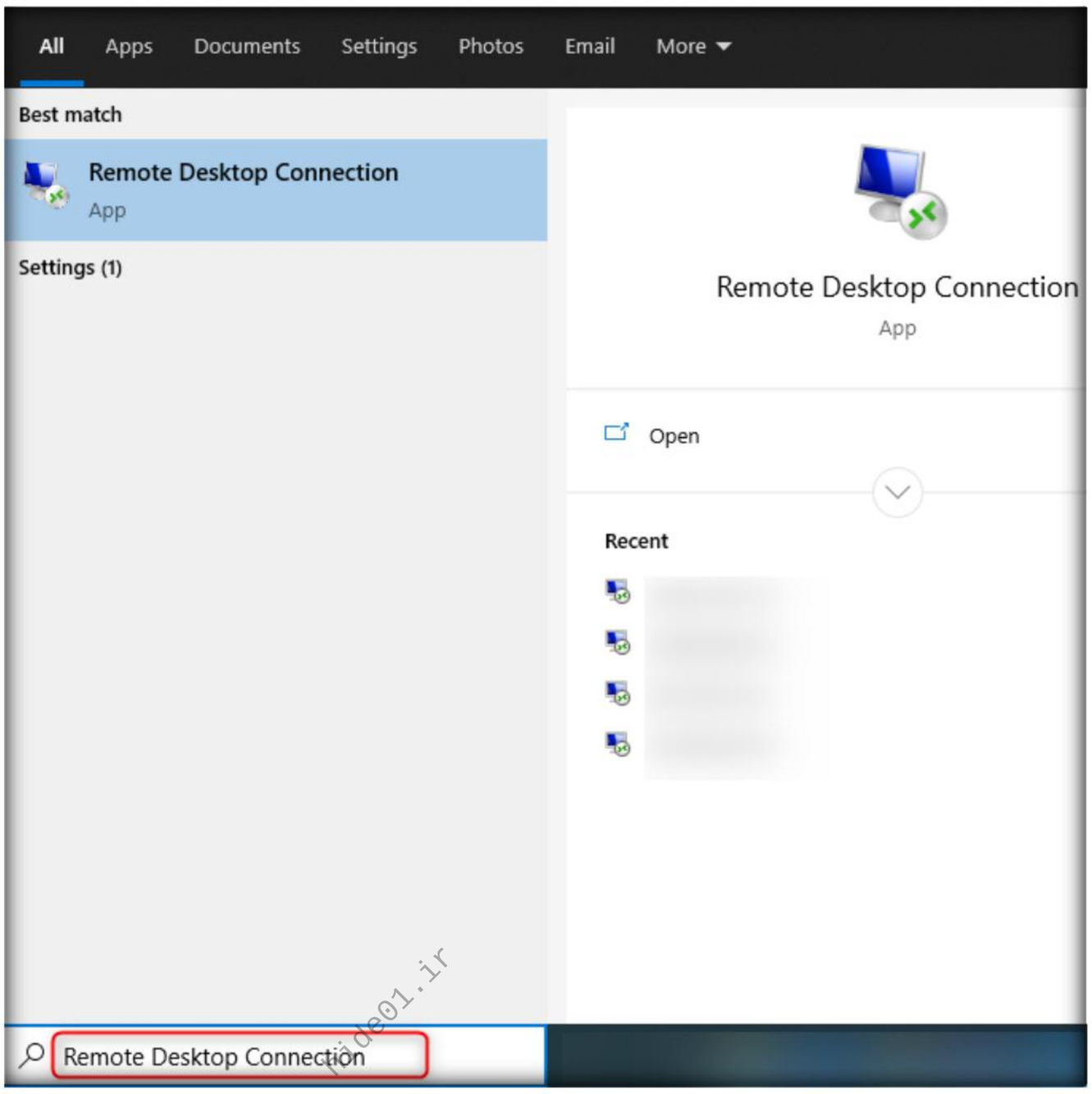


FIGURE 2.6.35: Navigating to Remote Desktop Connection

36. In the **Remote Desktop Connection** window, enter the Public IP address of the Windows VM in the **Computer** field. Click on **Connect**. .

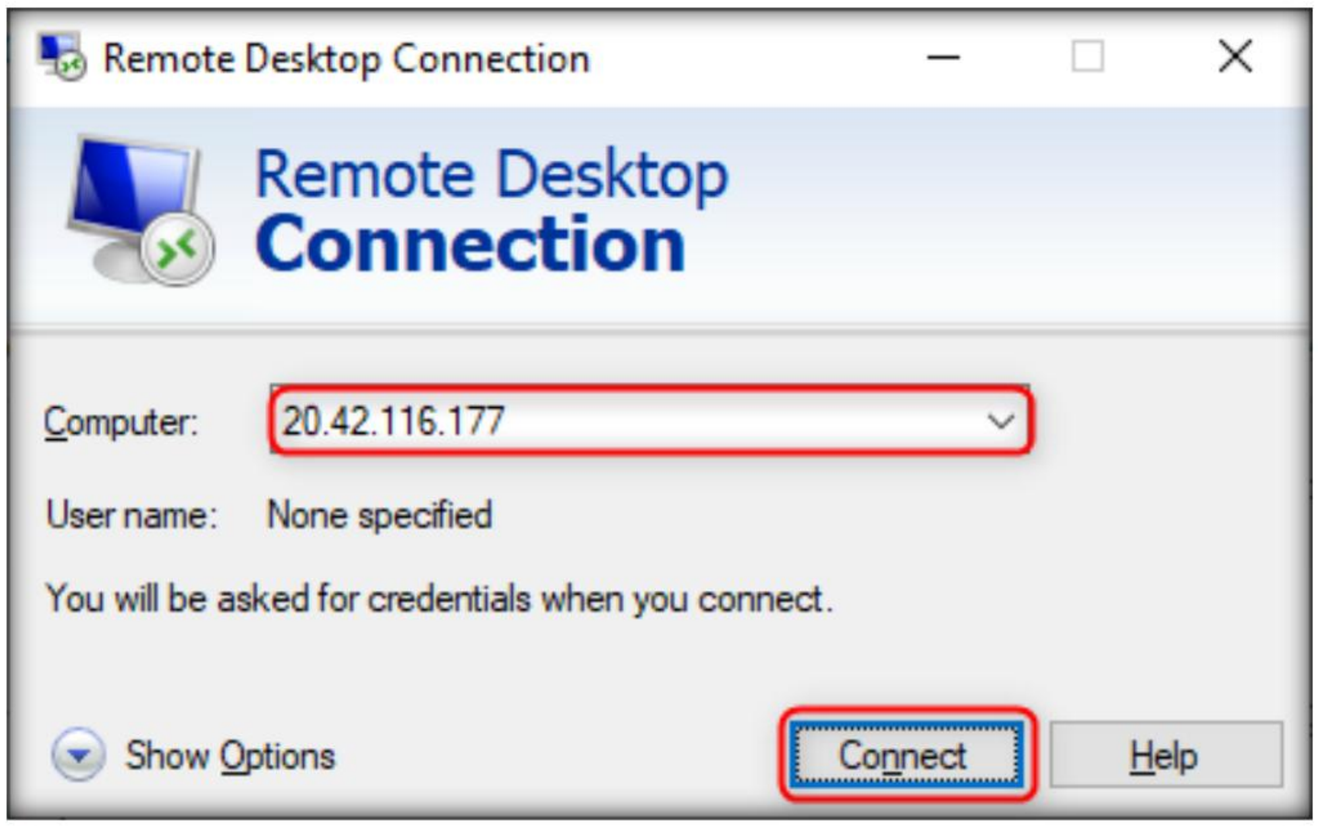


FIGURE 2.6.36: Connecting To VM

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

37. Next, the **Enter your credentials** window appears. Enter the username and password created by you while configuring the VM. Click on **OK**.

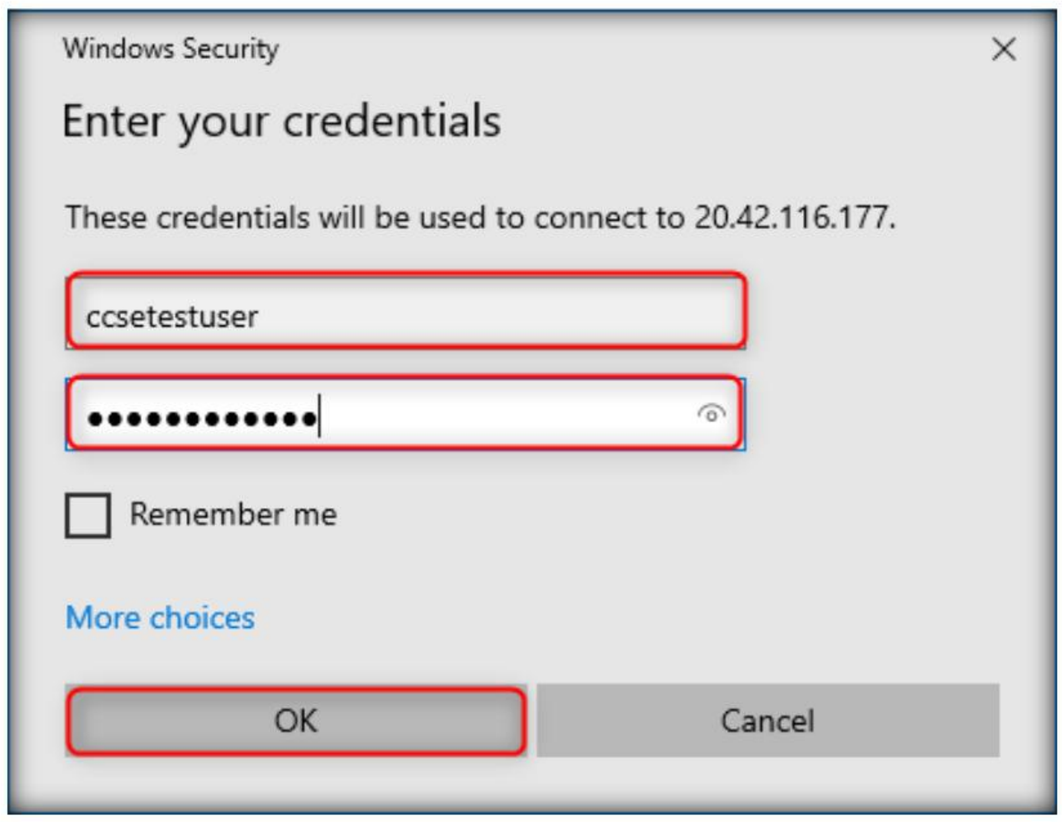


FIGURE 2.6.37: Entering Credentials

38. In the **Certificate errors** warning window, click on **Yes** to proceed.

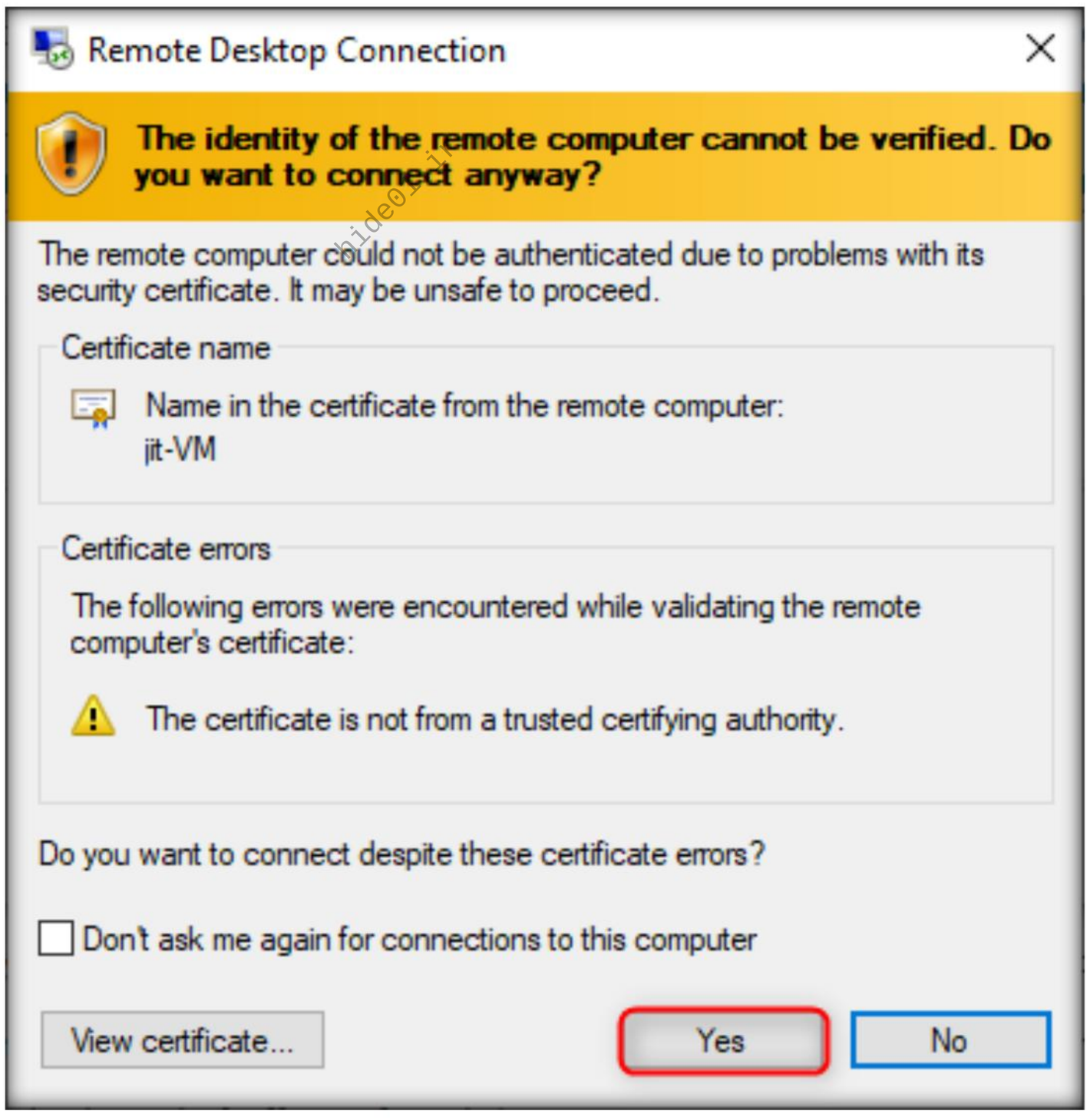


FIGURE 2.6.38: Proceeding with connection

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

39. Thus, remote desktop connection to the VM is successfully established. Close the remote desktop window.

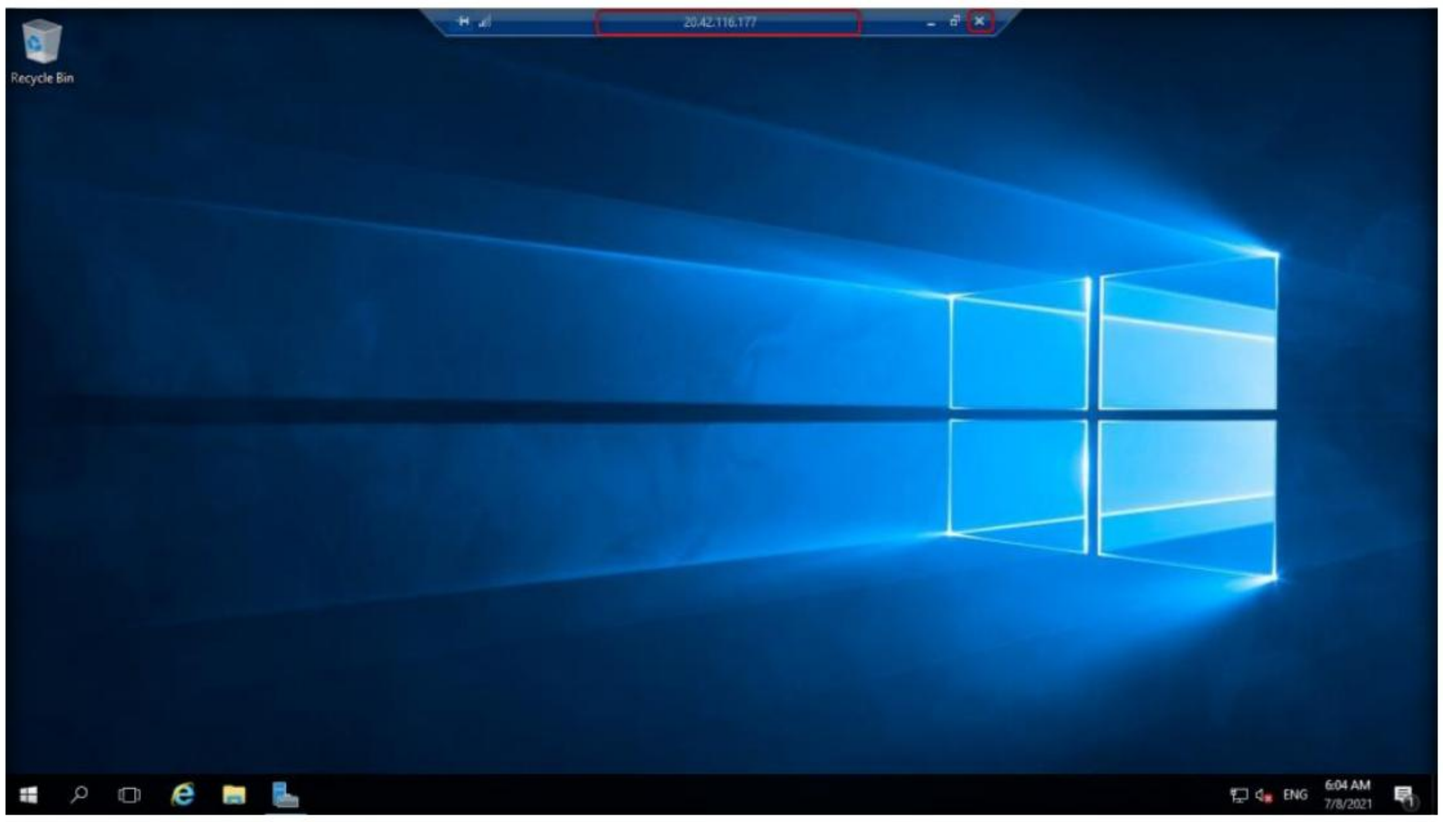


FIGURE 2.6.39: Remote Connection Established

40. Click **OK** to disconnect the session.

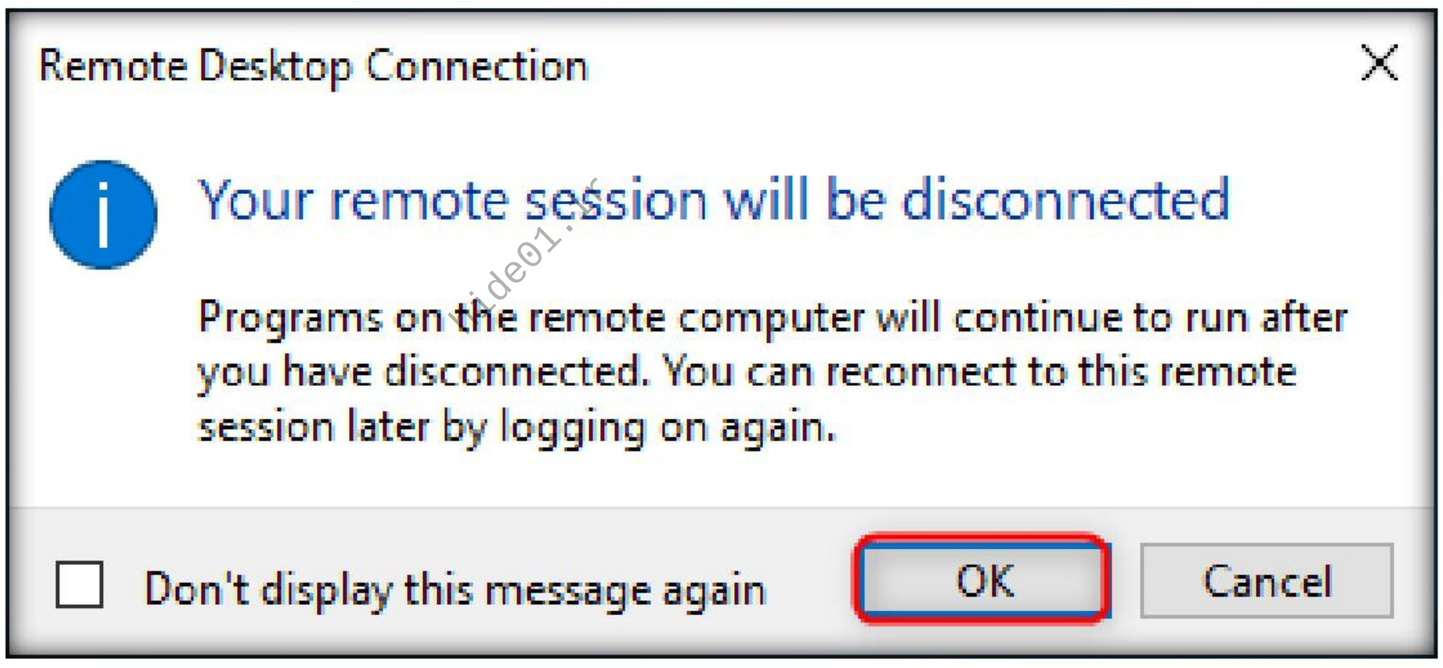


FIGURE 2.6.40: Confirm Disconnection

TASK 5

Configuring Just-in-Time access for the VM

41. Now, configure Just-in-Time (JIT) access for the Windows Server VM to restrict access to the management ports. Go back to the Azure portal. Type **Security Center** in the search box at the top of the Azure portal. Select **Security Center** from the dropdown.

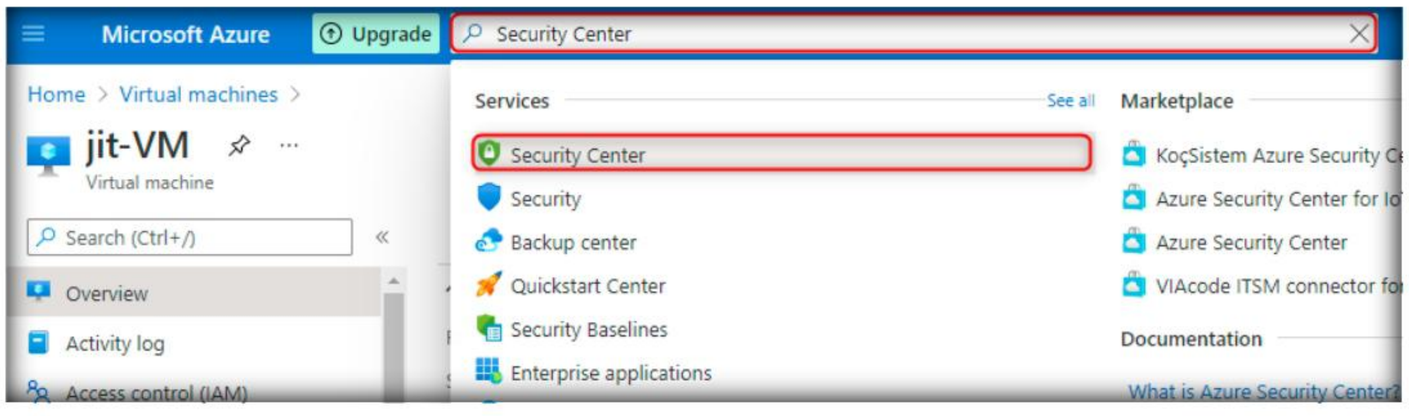


FIGURE 2.6.41: Navigate to Security Center

Certified Cloud Security Engineer Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

42. Now, the **Security Center** window opens. Select **Azure Defender** in the left pane under **Cloud Security**.

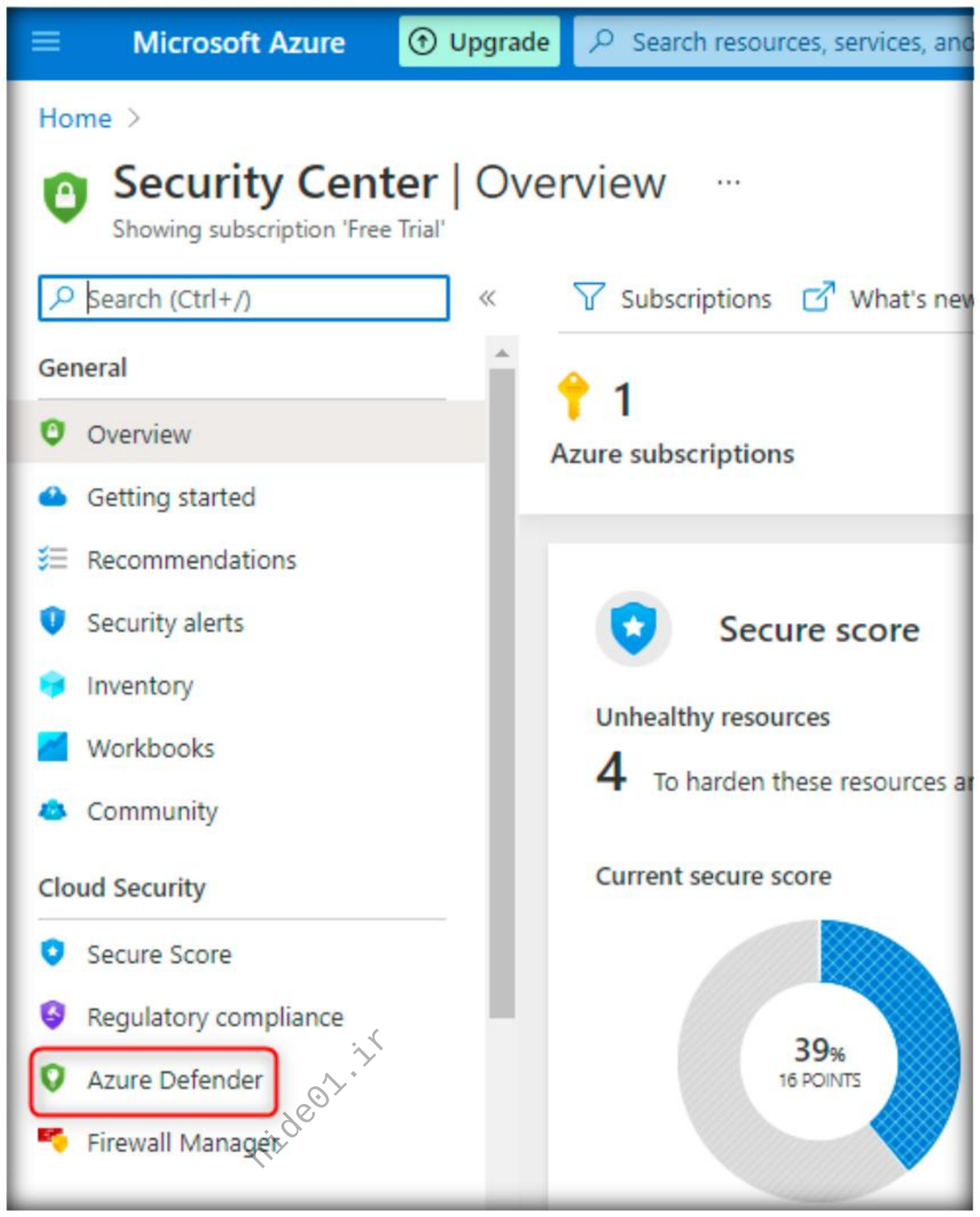


FIGURE 2.6.42: Navigating to Azure Defender

43. In the **Azure Defender** window, click on **Just-in-time VM access** to enable JIT access for the Windows Server VM.

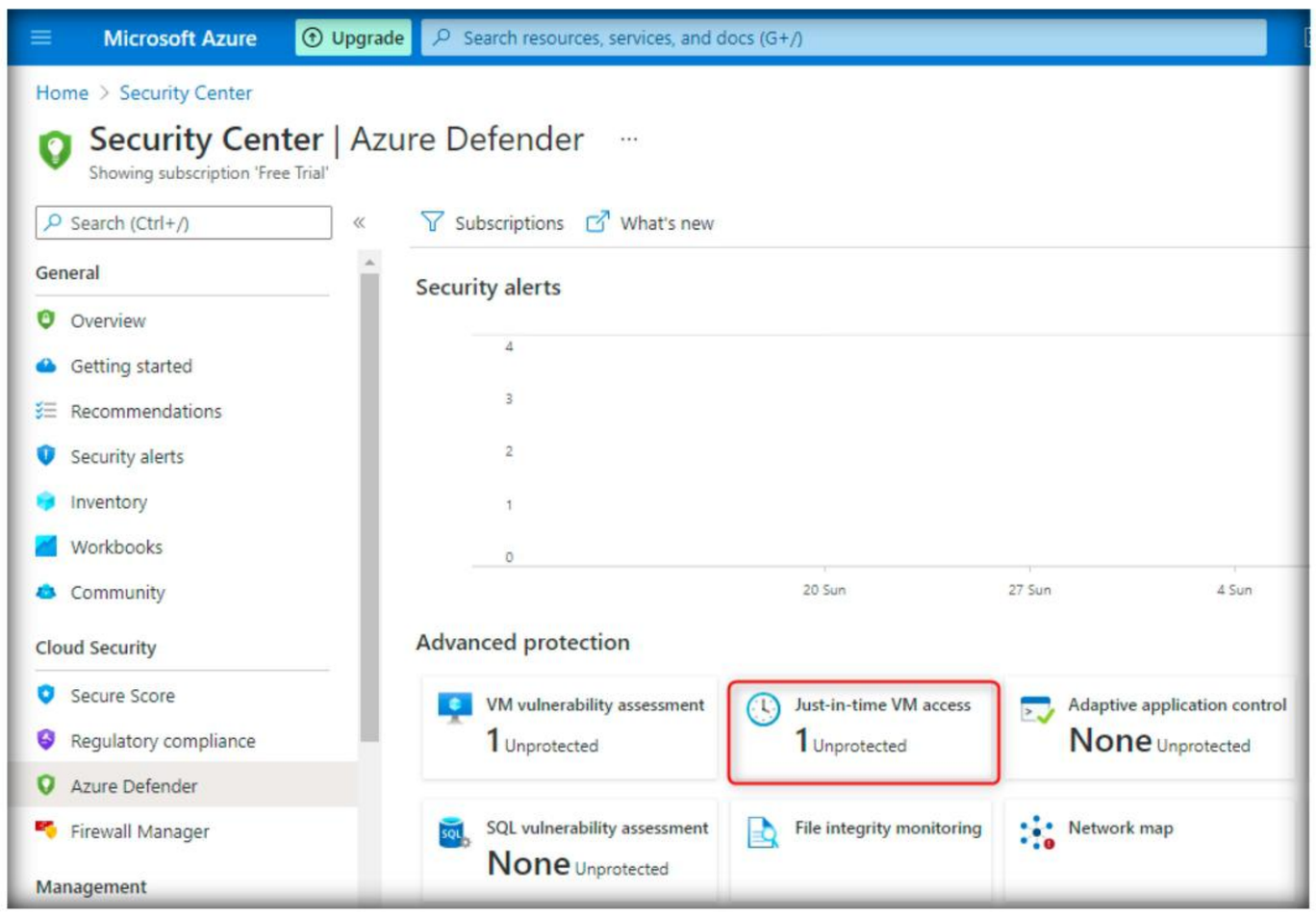


FIGURE 2.6.43: Configuring JIT VM Access

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

44. Click on the **Not-configured** tab.

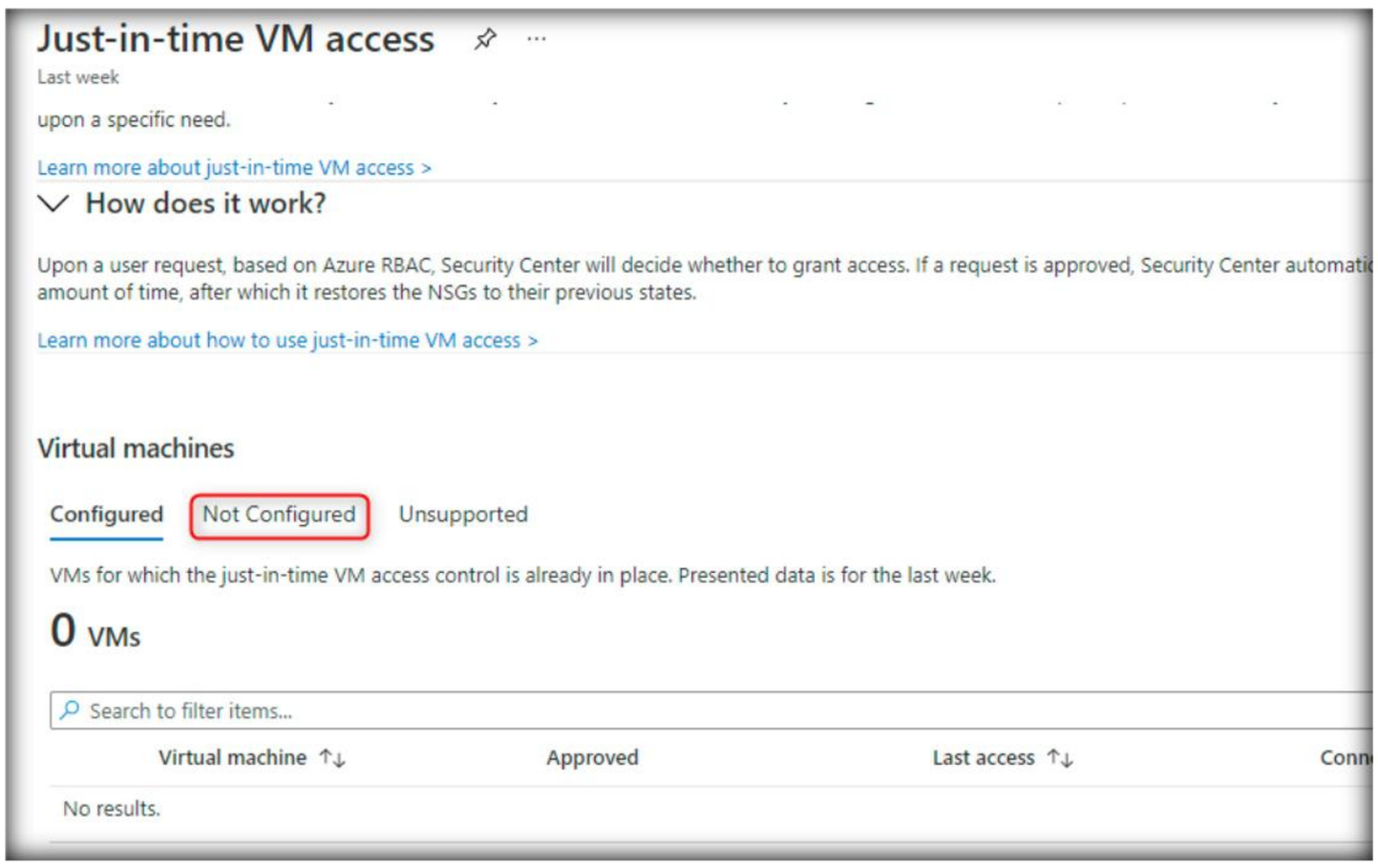


FIGURE 2.6.44: Configuring JIT Access

45. Select the checkbox for the Windows Server VM (**jit-VM**) and click on **Enable JIT on 1 VM**.



FIGURE 2.6.45: Enabling JIT

46. The subsequent window displays the ports for which JIT access is applicable. Click on **Save** to save the configuration.

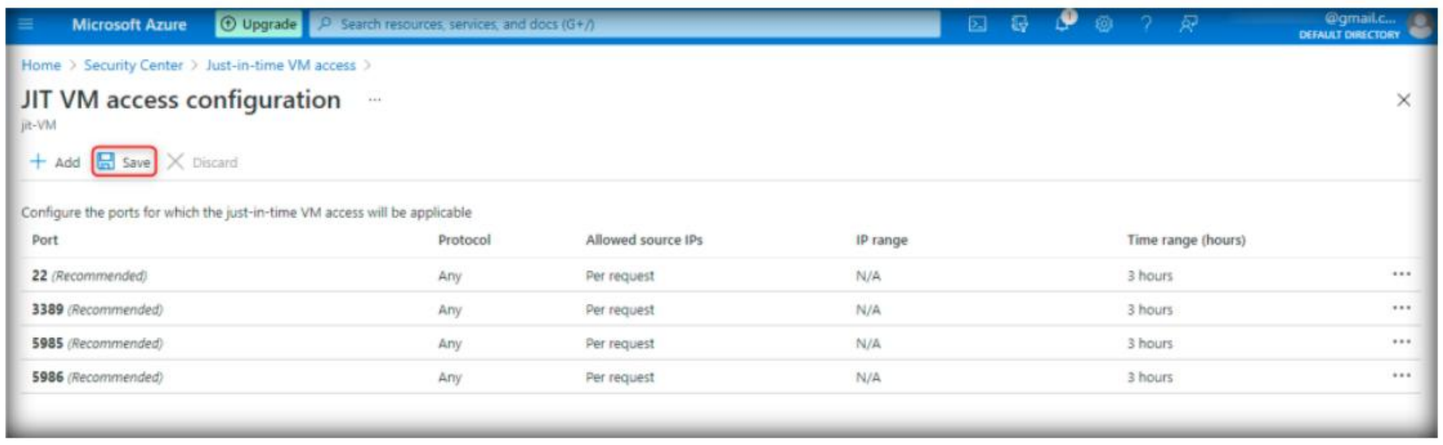


FIGURE 2.6.46: Saving the Configuration

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 6

Testing RDP connection to the VM after JIT access is enabled

47. Now, test the RDP connection to the Windows Server VM after JIT is enabled. Search for **Remote Desktop Connection** in the Windows search bar and press **Enter.**

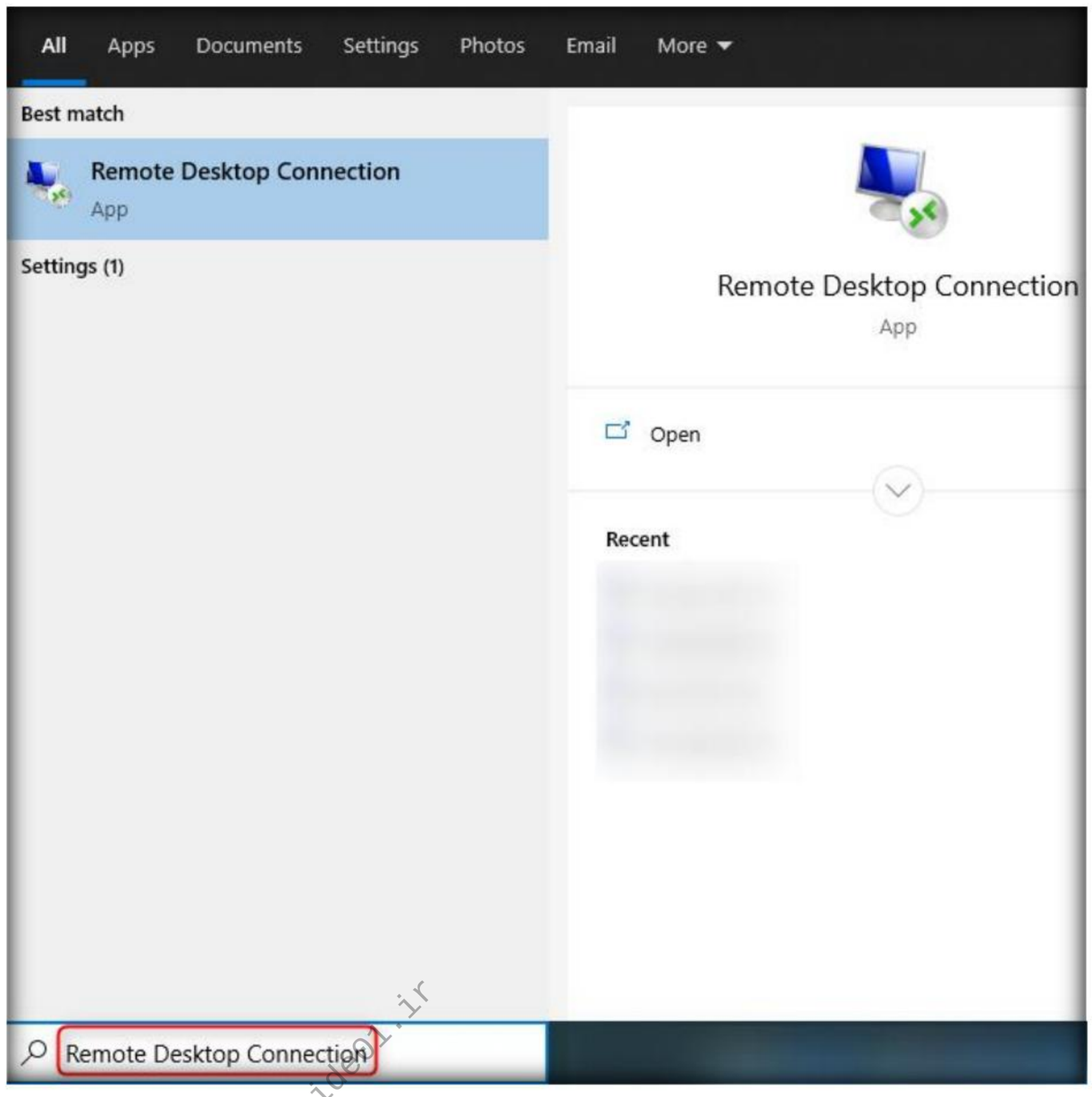


FIGURE 2.6.47: Navigating to RDP

48. Enter the **Public IP address** of the VM in the **Computer** field. Click on **Connect.**

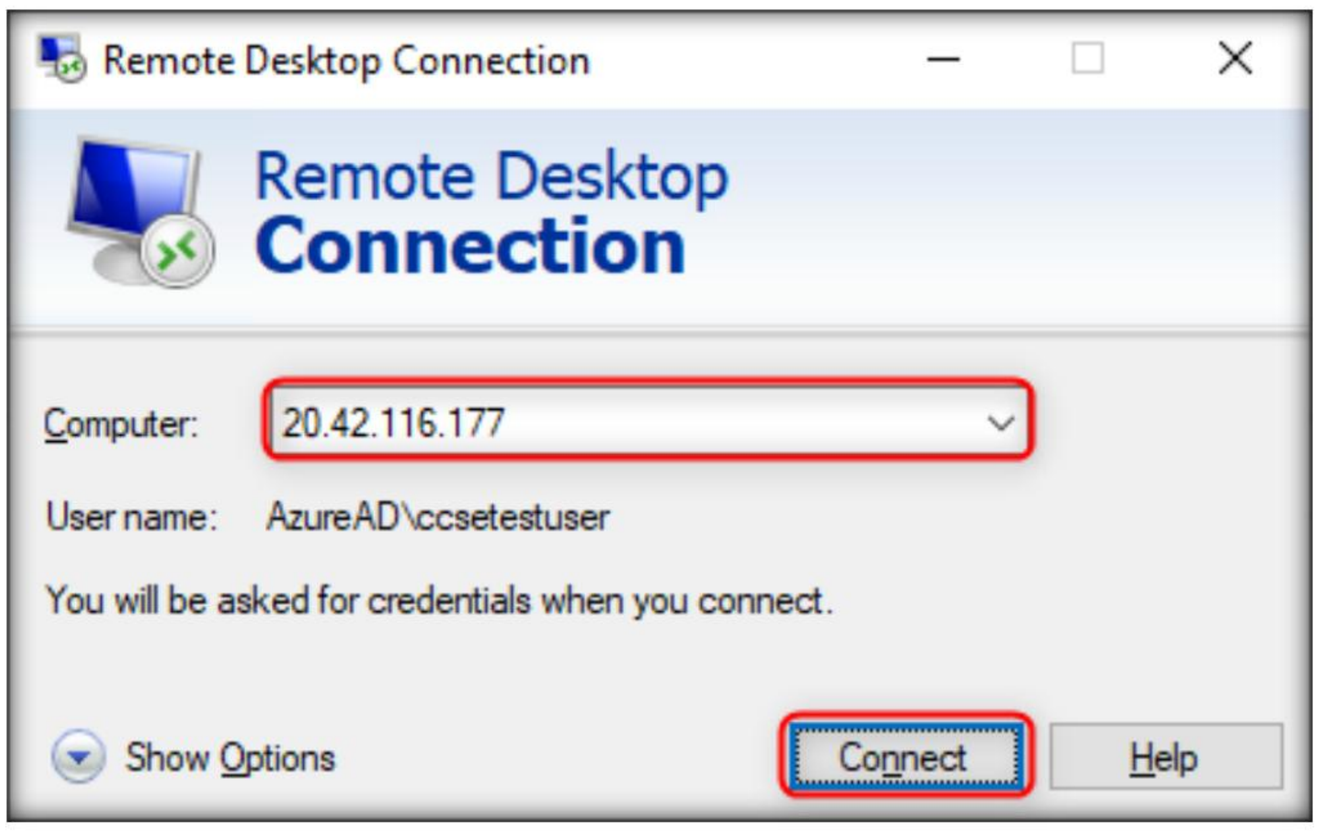


FIGURE 2.6.48: Connecting to VM

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

49. A pop-up window appears next that says that connection cannot be made to the remote computer. Thus, RDP access to the Windows Server VM is blocked by JIT access.

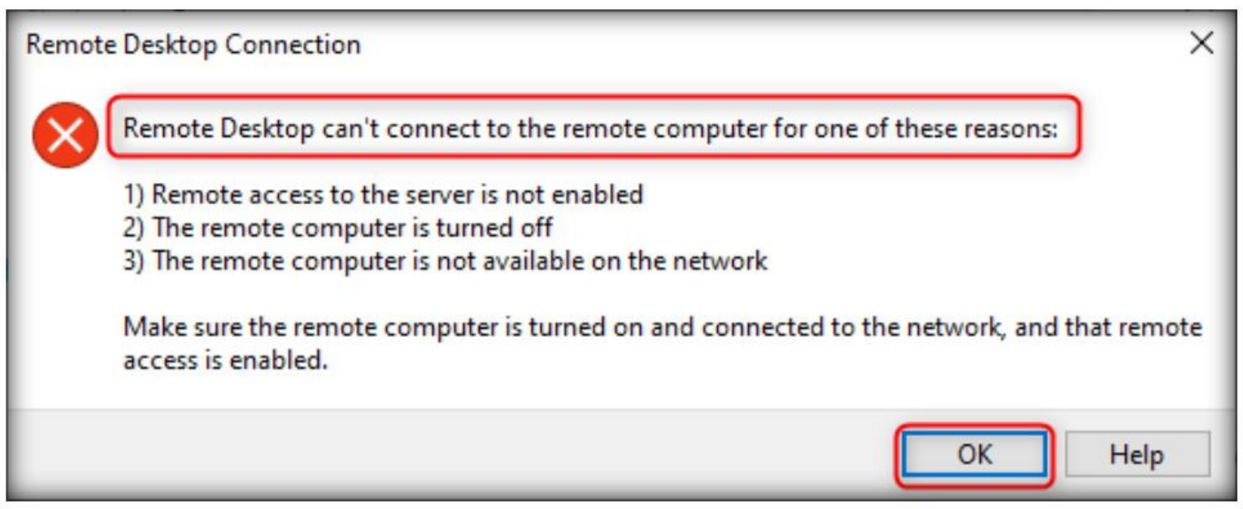


FIGURE 2.6.49: Connection Denied

TASK 7

Granting temporary RDP access to the VM

50. Now, if a user in the organization or a cloud security engineer wants to access the Windows Server VM remotely, you can enable access for a minimum amount of time. Go back to the Azure portal. Click on **Configured** in the **Just-intime VM access** window. Select the checkbox for the Windows Server VM **(jit-VM)**. Click on **Request access**.



FIGURE 2.6.50: Requesting Access

51. Then, the **Request access** window opens. Ensure that the toggle for port number **3389** is **On**. For **Time range (hours),** enter a time range (in hours) for which access should be granted to the VM. Here, we have entered **2 hours**. Type a justification for enabling access in the following field titled **Enter request justification**; here, we have entered **Maintenance**. Click on **Open ports**.

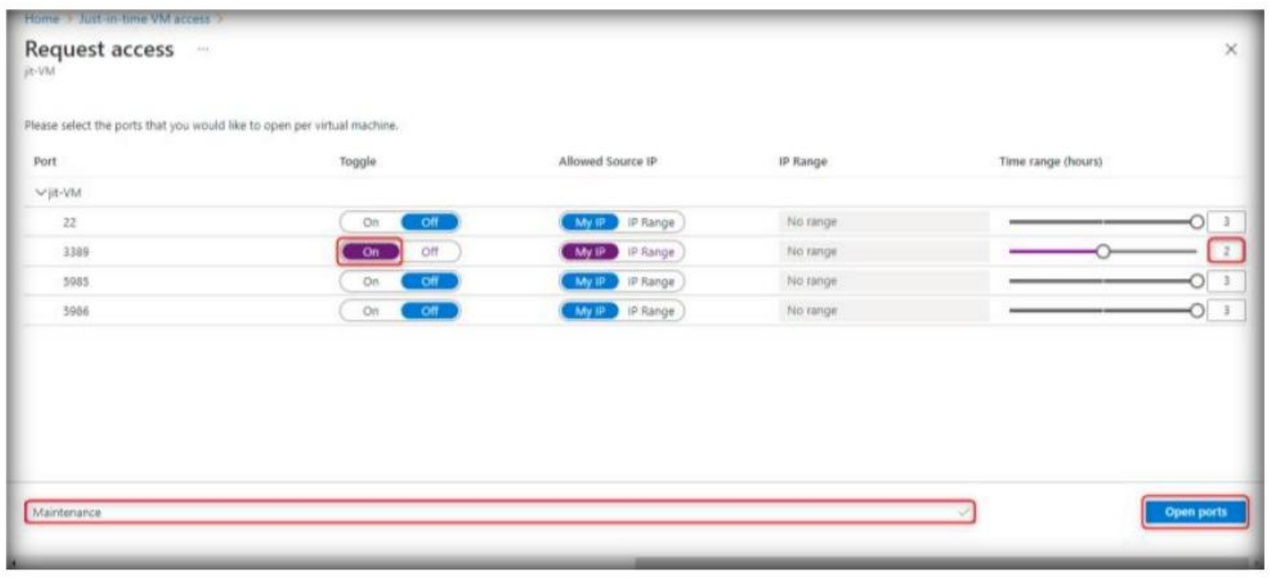


FIGURE 2.6.51: Configuring Access Settings

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

52. Thus, RDP connection (**3389**) to the VM is activated.

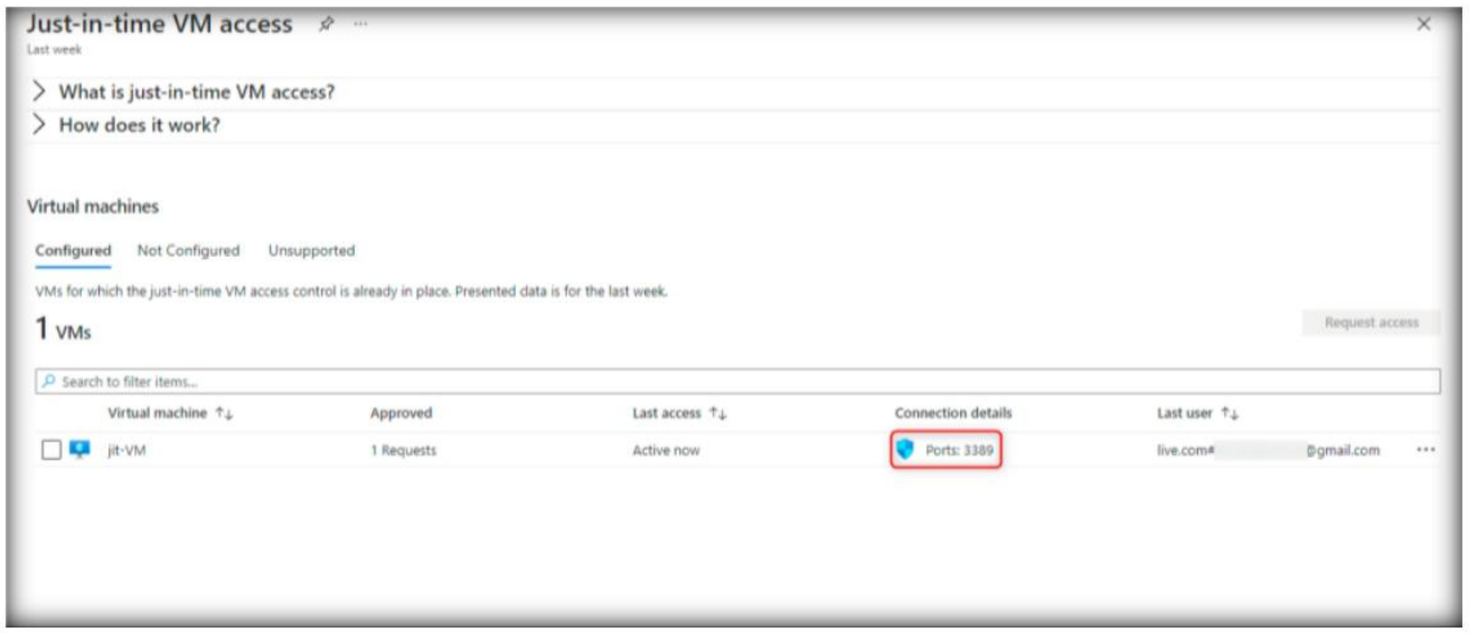


FIGURE 2.6.52: RDP Connection Enabled

53. Now, access the VM via Remote Desktop Connection. Search for **Remote Desktop Connection** in Windows search box. Press **Enter**.

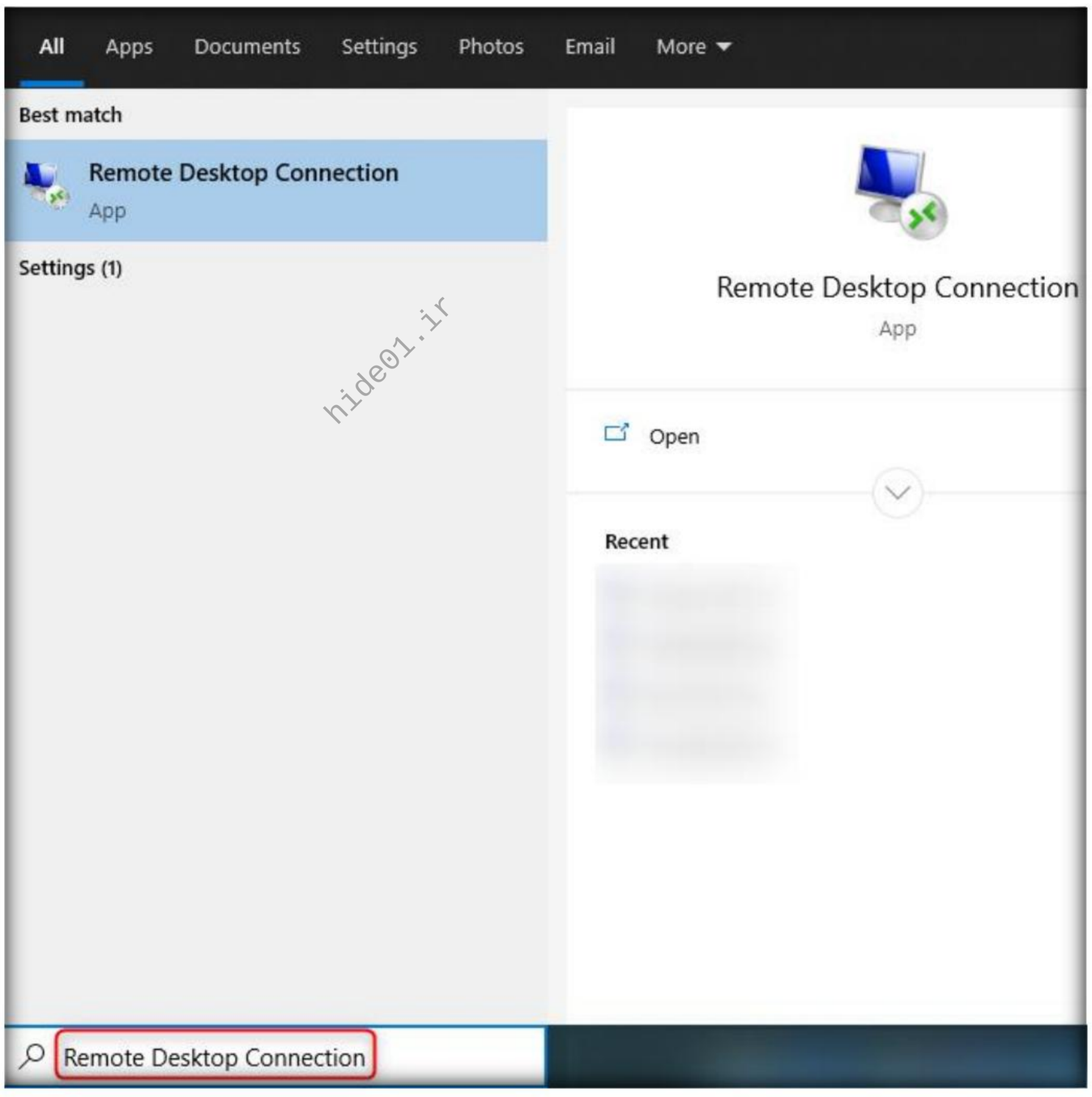


FIGURE 2.6.53: Navigating to Remote Desktop Connection

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

54. Enter the **Public IP address** of the VM in the **Computer** field. Click on **Connect.**

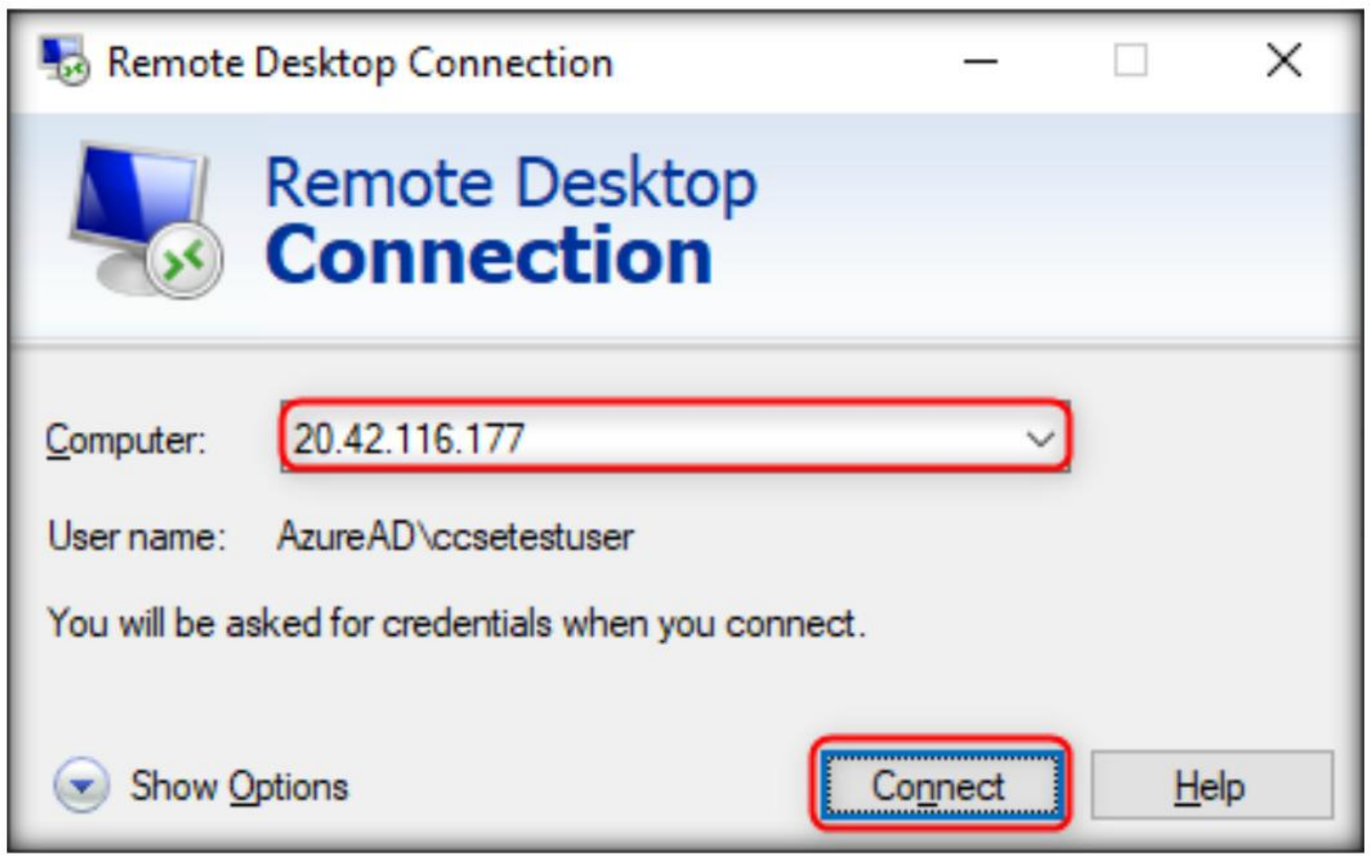


FIGURE 2.6.54: Connecting to VM

55. Now, the **Enter your credentials** window appears. Enter the username and password for the Windows Server VM (**jit-VM**) and click on **OK**.

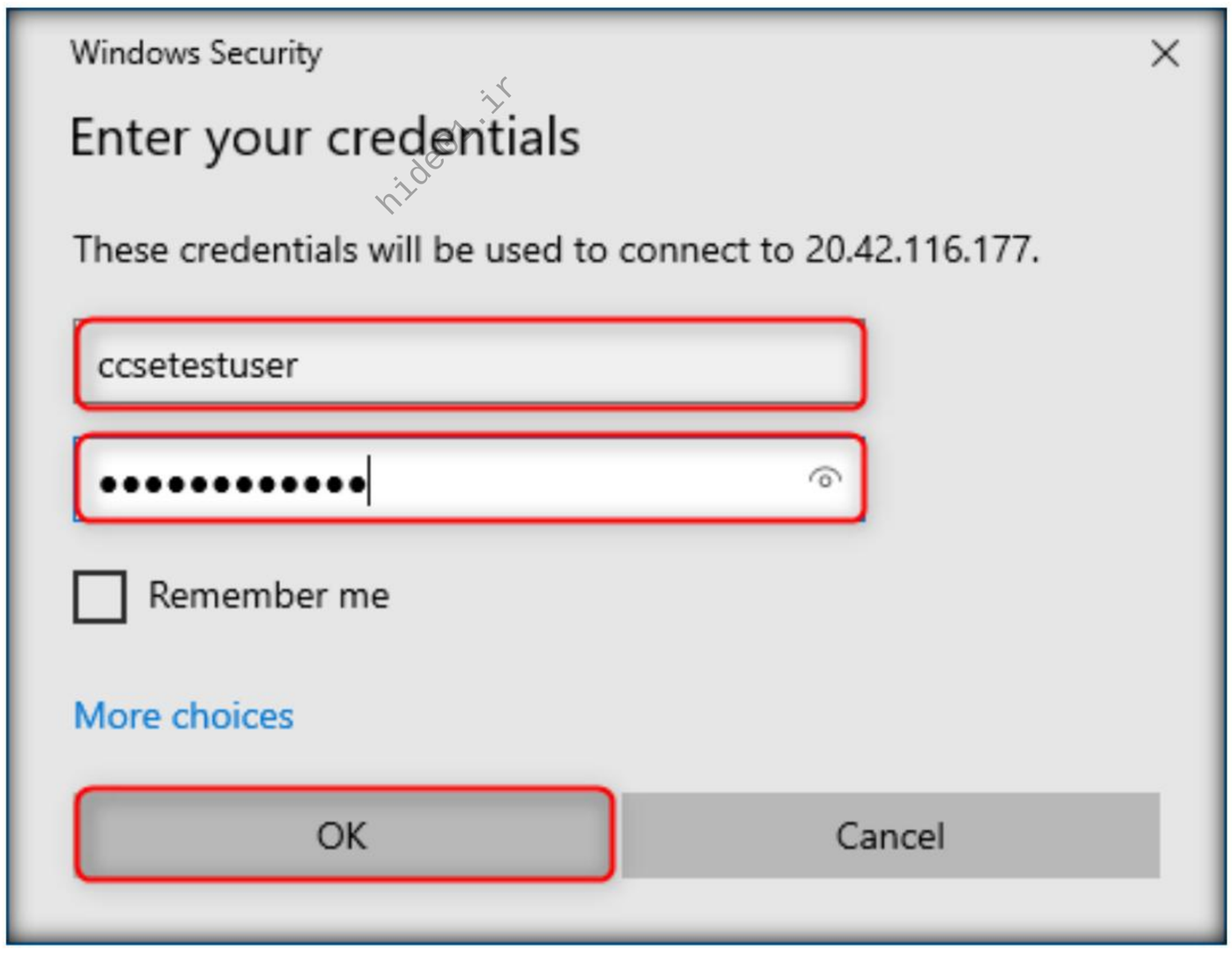


FIGURE 2.6.55: Entering Credentials

Certified Cloud Security Engineer Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

56. Next, the **Remote Desktop Connection** certificate window appears indicating certificate errors; click on **Yes**.

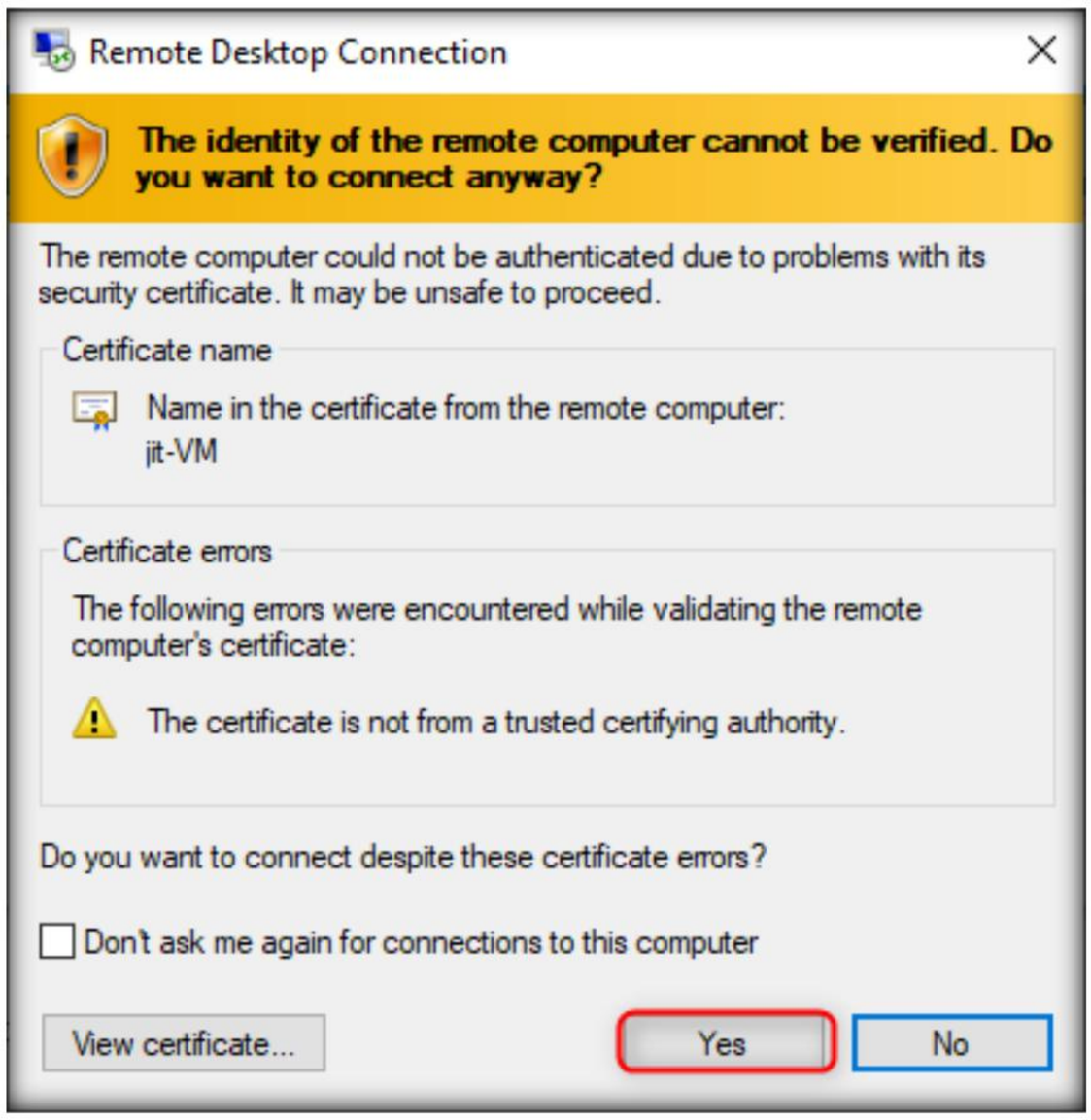


FIGURE 2.6.56: Certificate Error window

57. Thus, the Windows Server VM is connected successfully via remote desktop connection.



FIGURE 2.6.57: Remote Connection Established

58. Thus, with Azure Security Center's JIT access, a cloud security engineer can restrict access to management ports such as RDP and secure the VMs in Azure from brute force login attempts.

h1de01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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

59. Navigate to **Resource groups** from the Azure portal. Click on the resource group (**jitvm-RG**) to open the resource group **Overview** page. Click on **Delete resource group**. Type the name of the resource group (**jitvm-RG**) in the confirmation window that appears and click on **Delete**. The virtual machine (**jit-VM**) gets deleted automatically once you delete the resource group associated with the VM.

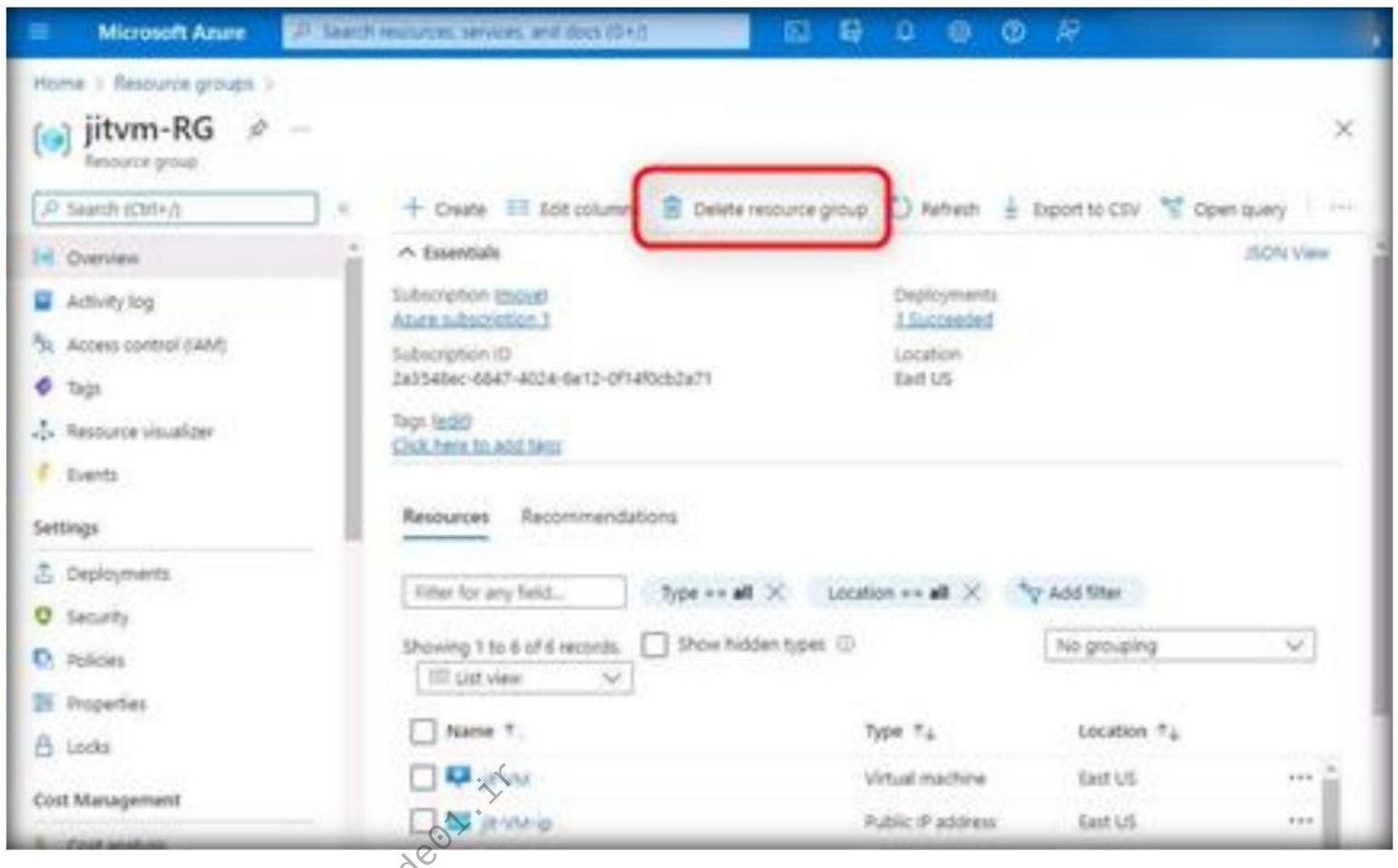


FIGURE 2.6.58: Deleting Resource Group

hideo.ir

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.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab

7

Implementing Role Based Access Control with GCP IAM

GCP IAM roles allow an administrator to grant a granular access to specific Google Cloud resources and prevent any unwanted access to other resources. A cloud professional can control access to Google Cloud resources through IAM.

ICON KEY

Valuable information

Test your knowledge

Web exercise

Workbook review

Lab Scenario

GCP IAM provides a granular access to a user with the principle of least privilege (PoLP) security to essential Google Cloud resources. Users must not be individually assigned access privileges. The admin should assign permissions to roles rather than users in GCP. IAM roles are a set of permissions that allow users under them to perform specified actions on certain cloud resources. GCP IAM not only offers various predefined roles for handling a large number of common use cases but also provides the admin with a customization option for handling roles that require customized access privileges. This lab demonstrates the implementation of predefined roles along with creating and implementing custom roles for users with GCP IAM.

Lab Objectives

This lab will demonstrate how to implement custom roles and create and grant custom roles for users with GCP IAM.

In this lab, you will learn to do the following:

- Grant predefined roles with GCP IAM
- Create and grant custom roles for users with GCP IAM
- Revoke access with IAM

Lab Environment

To perform this lab, you need the following:

- **Admin Machine** VM
- **Administrative** privileges

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Registered GCP account

Lab Duration

Time: 10 minutes

Overview of GCP IAM Roles

IAM roles are a set of permissions that allow users under them to perform certain actions on certain cloud resources. They allow the administrator to grant a granular access to specific Google Cloud resources and prevent unwanted access to other resources.

- **Predefined IAM roles**: They provide a fine-grained access control and are specifically meant to support common control patterns and use cases.
- **Custom IAM roles**: These are user-defined roles and allow the collection of supported permissions to meet an organization's requirements. They provide a granular access to cloud resources based on a user-specified list of permissions. Because Google does not maintain custom roles, such roles are not updated automatically by Google Cloud. It is possible to create custom roles at the organization and project levels, but not at the folder level. When predefined roles do not meet the needs of the organization, custom roles are created and used to meet the security requirements.

Lab Tasks

ide01.ir

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., GCP), the application interface may be updated with time. Hence, in case you happen to work on an updated version of GCP, 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 GCP Free Trial account using the following link: https://cloud.google.com/free. Once the registration is complete, perform the following tasks:

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

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1

Granting Predefined Roles with GCP IAM

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

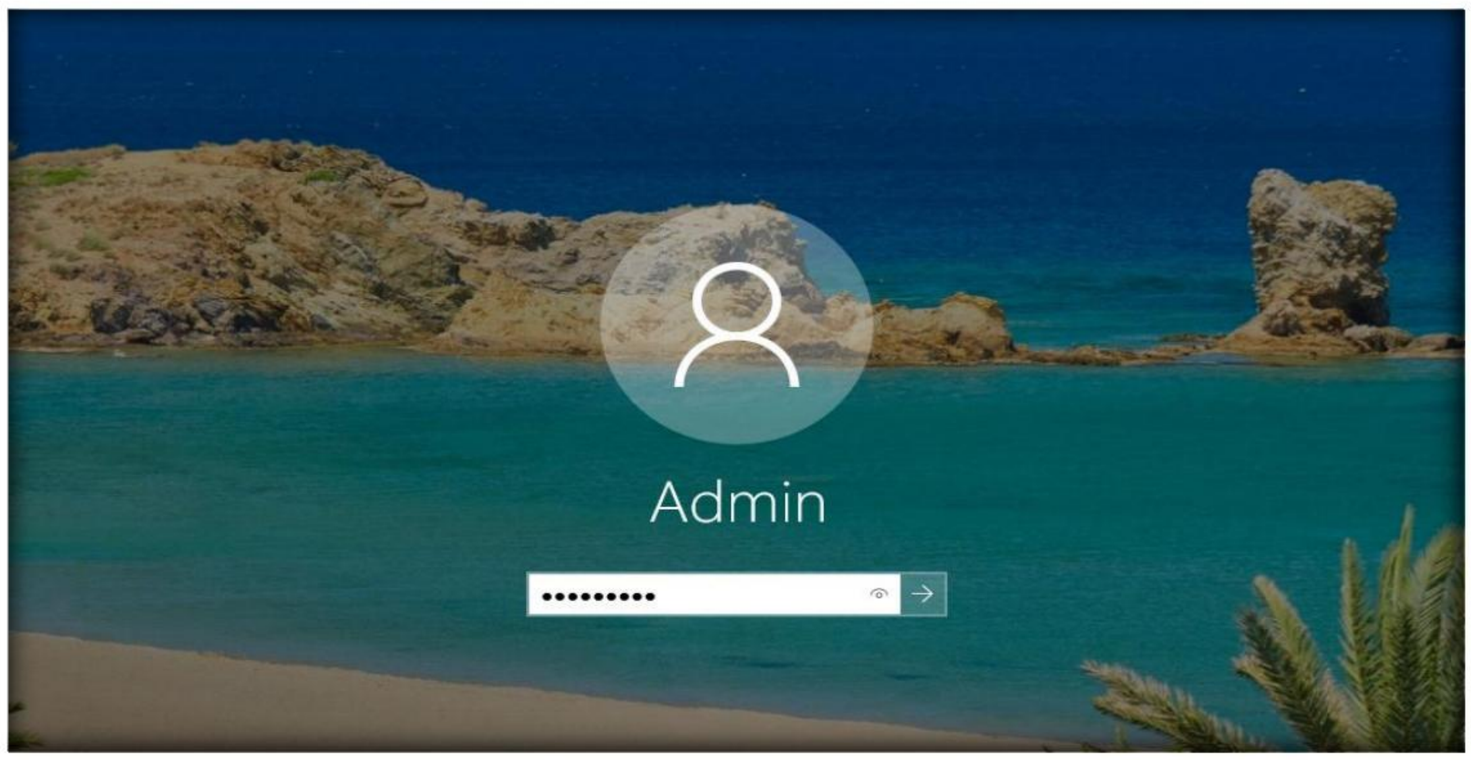


FIGURE 2.7.1: Launch Admin Machine and Log in

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



FIGURE 2.7.2: Navigating to the Chrome Browser from Taskbar

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

3. In the address bar of the Google Chrome browser, type **https://console.cloud.google.com/** and press **Enter**.

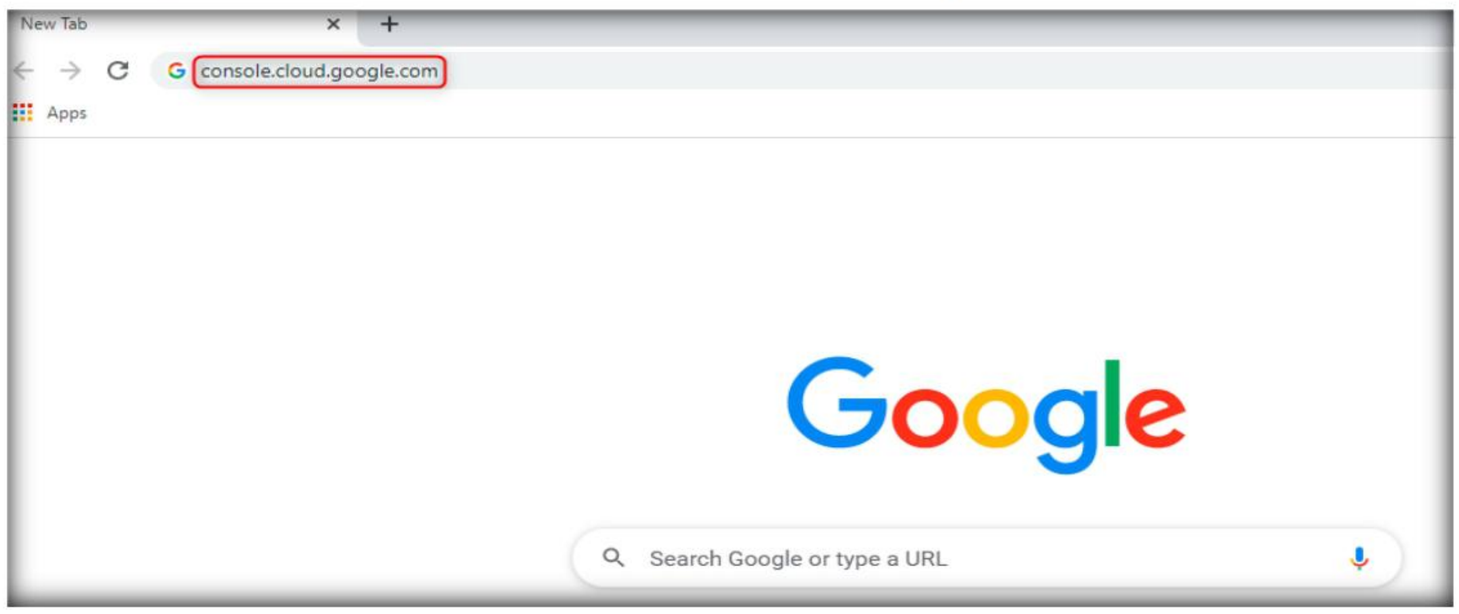


FIGURE 2.7.3: Navigating to the Google Cloud Console

4. Enter the **Email address** to sign into **Google Cloud Platform**.
5. Click **Next**.

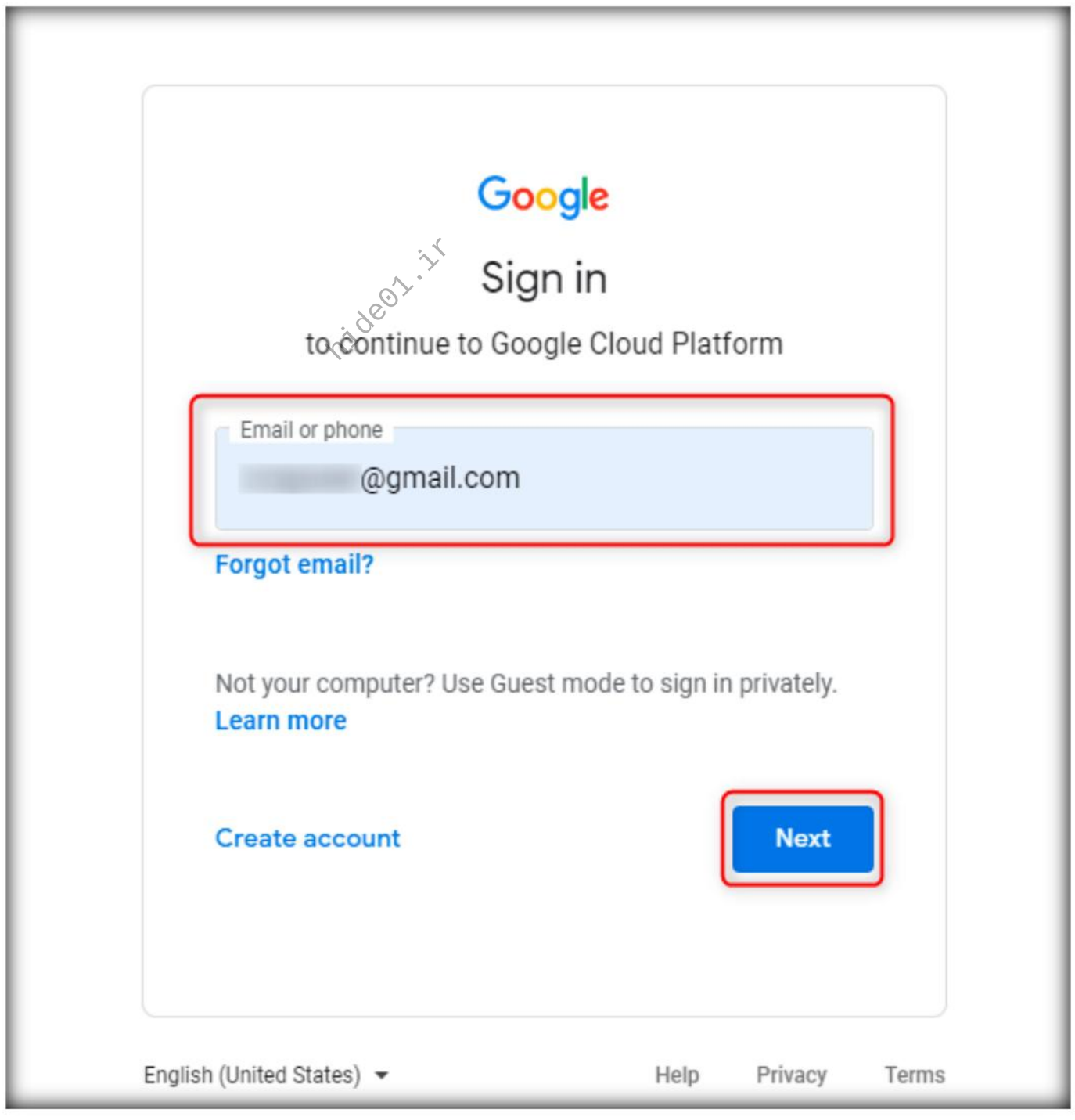


FIGURE 2.7.4: Entering the Account credentials

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

6. Enter the **password** and click on **Next**.

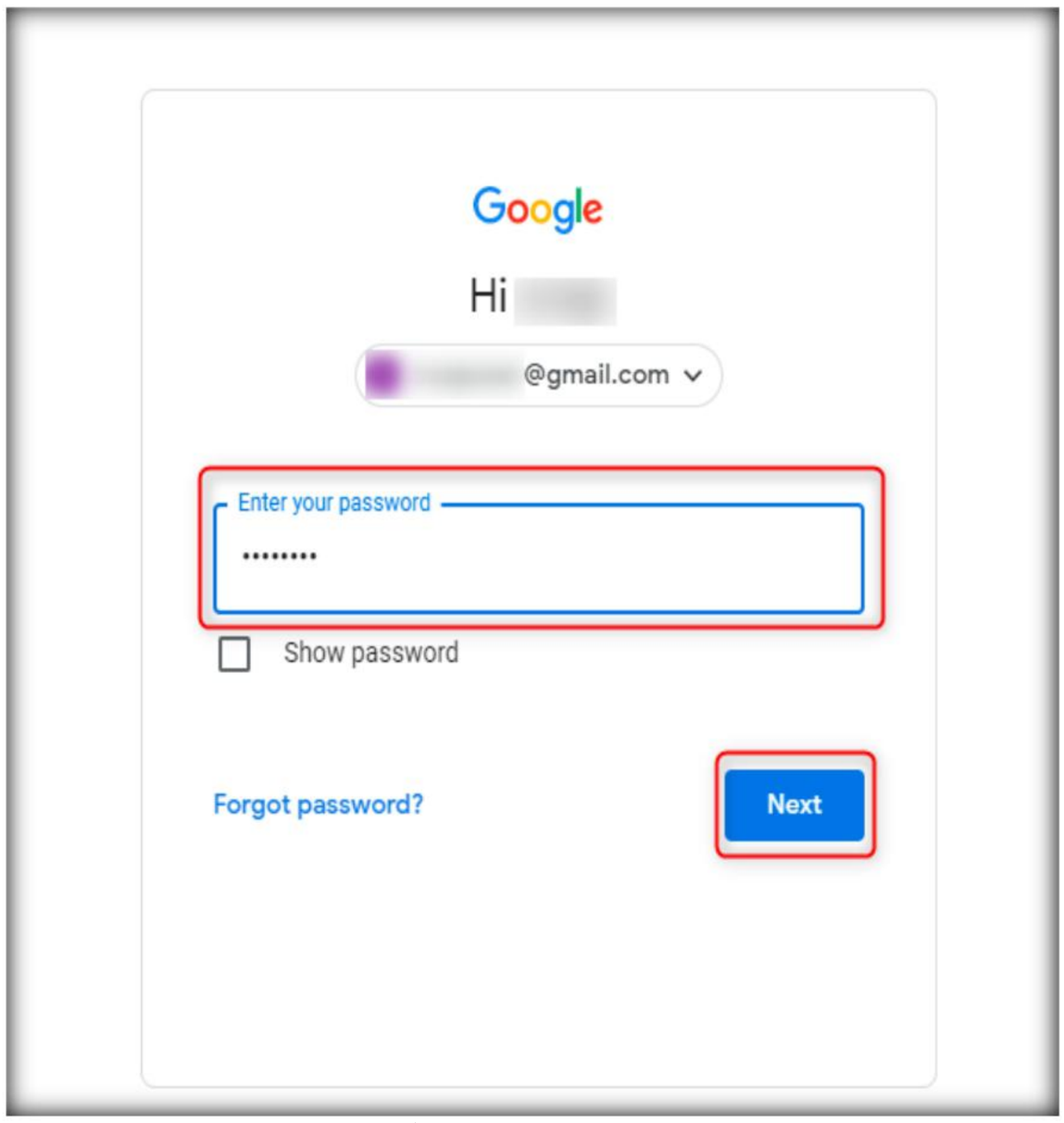


FIGURE 2.7.5: Signing into GCP Console

7. On top left corner, you will see a dropdown. It has a project selected by default (**My First Project**). Click on it to explore more options.

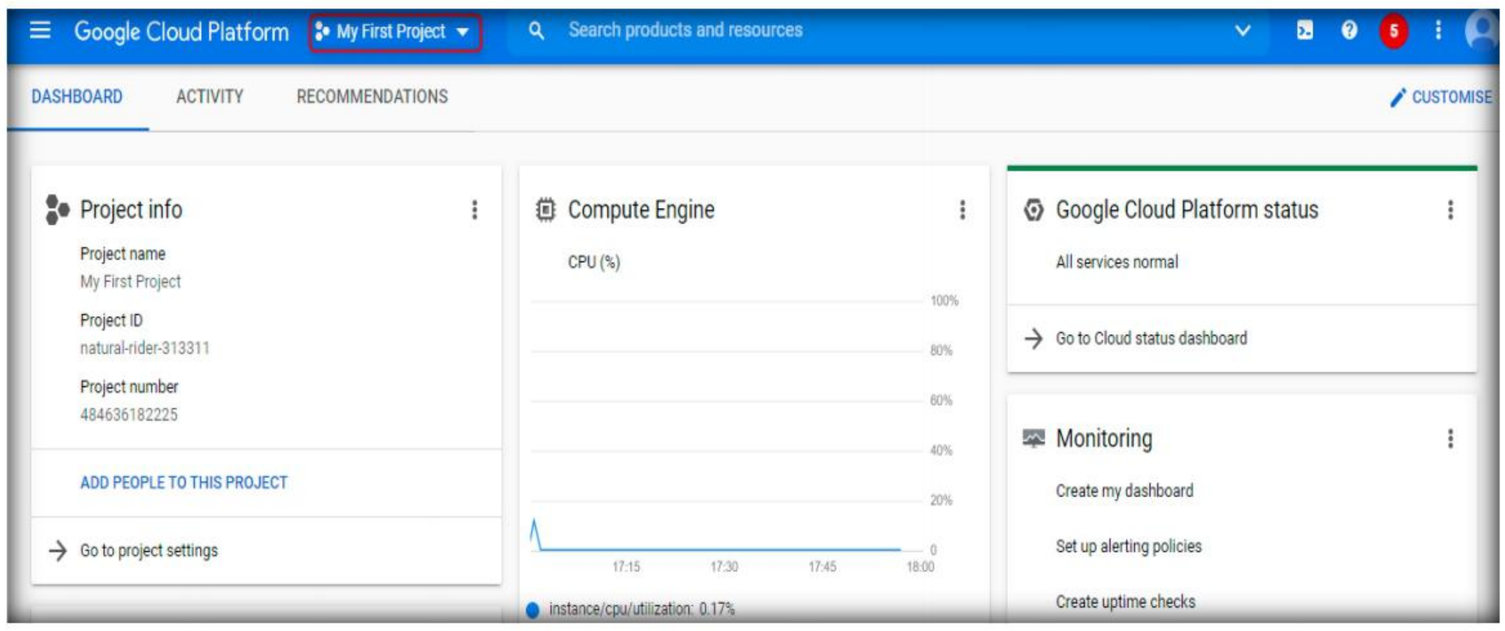


FIGURE 2.7.6: Creating a New Project

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

8. The next web page that appears lets you select an existing project by searching in the **Search projects and folders** field. Alternatively, you can click on **NEW PROJECT** to add a new one. When you add a new project, you will need to set up the billing option, which is a simple, two-step process. Choose the project titled **My First Project**.

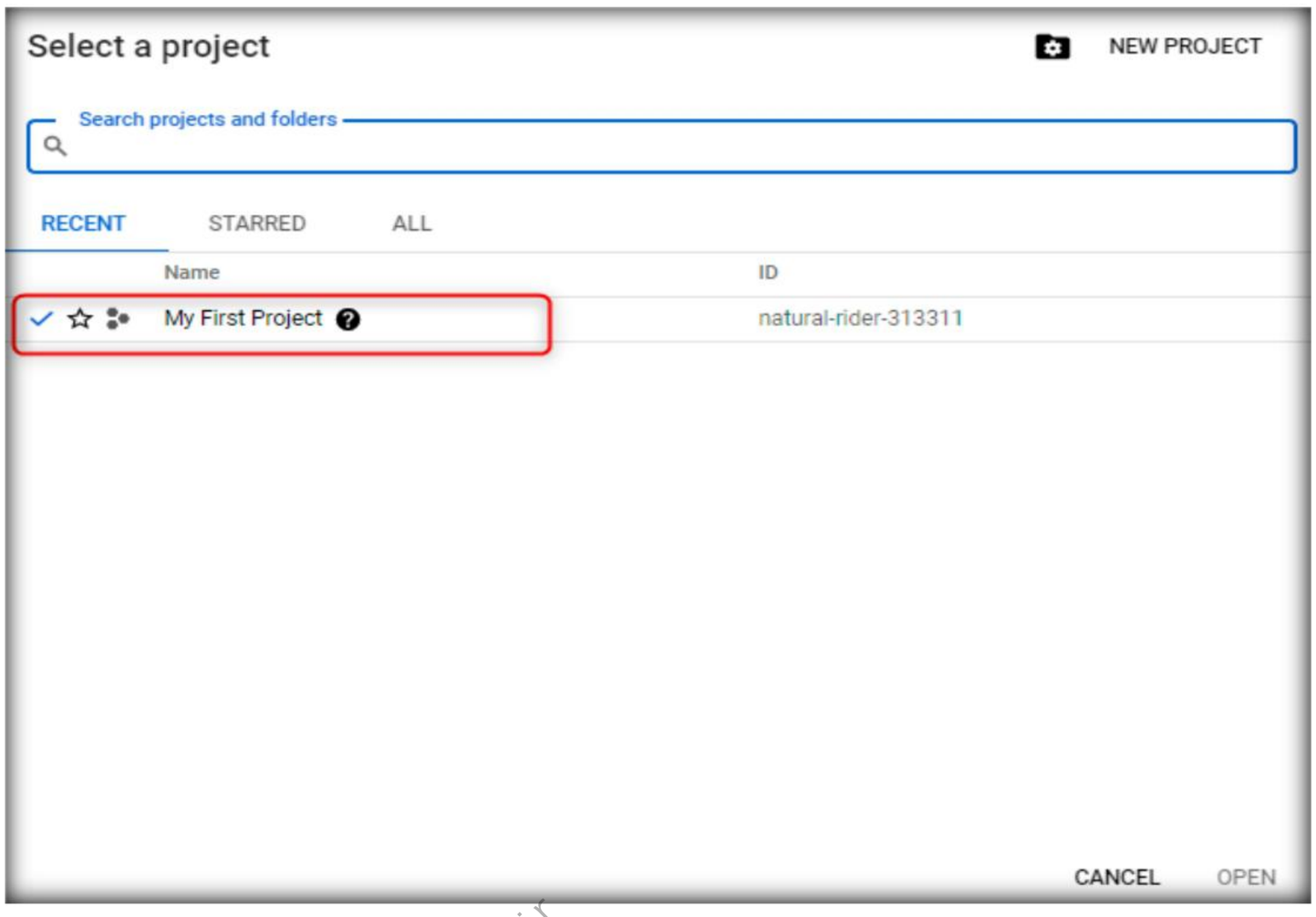


FIGURE 2.7.7: Selecting a New Project

hideo1.ir

9. Navigate to **IAM & Admin** and select **IAM** in the console.

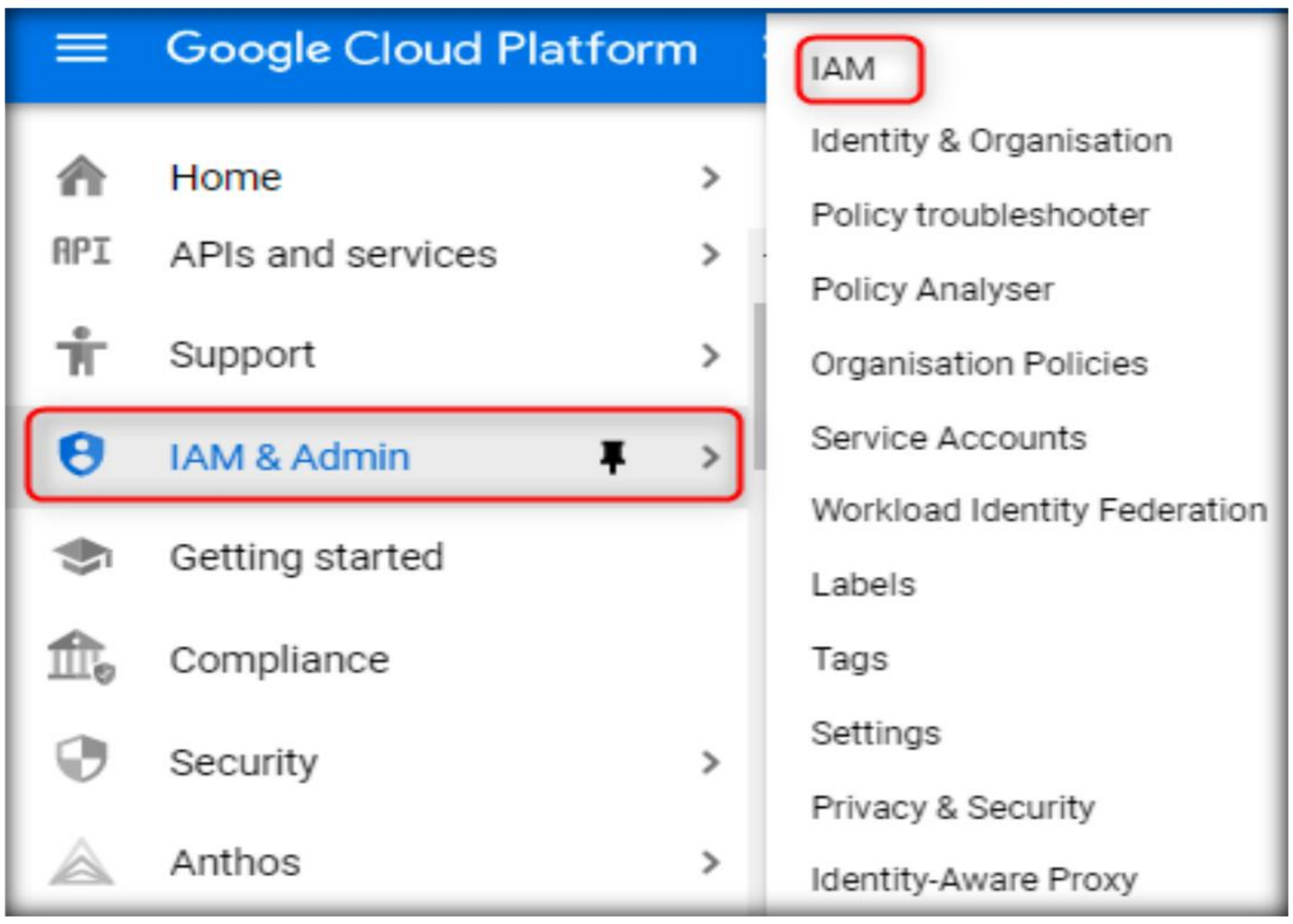


FIGURE 2.7.8: Selecting IAM from console

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

10. In the IAM dashboard window, click on **ADD** at the top to start implementing predefined roles for users.

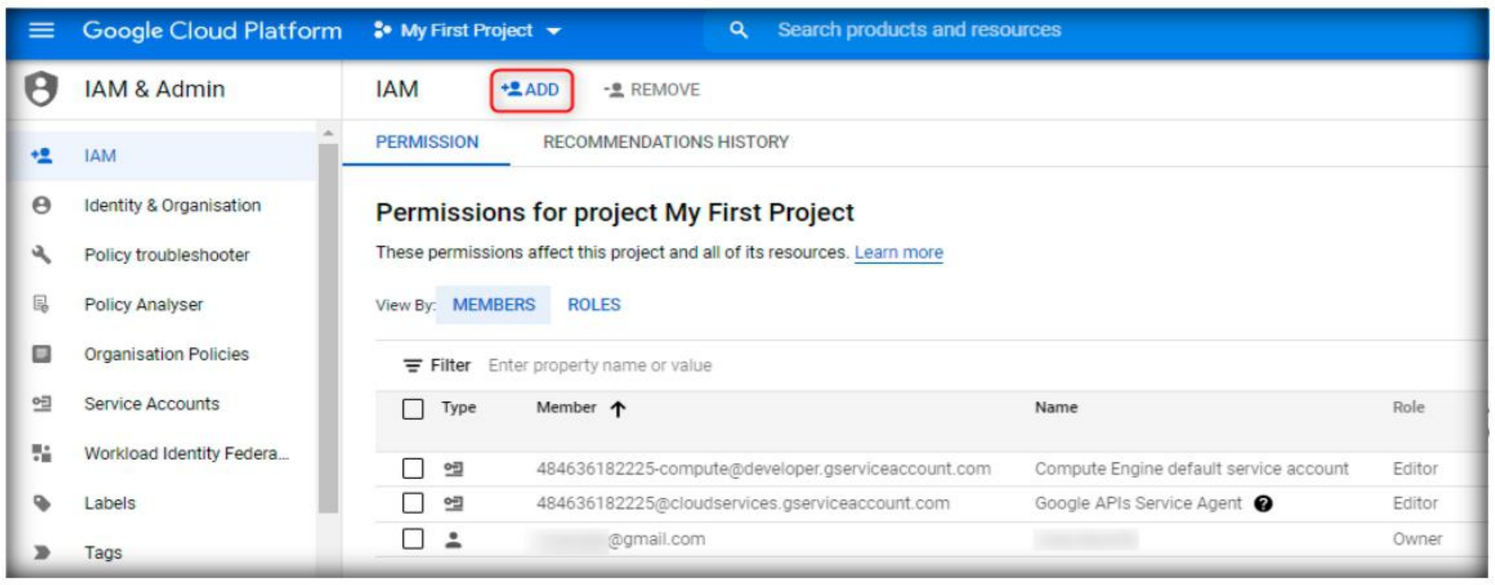


FIGURE 2.7.9: Adding predefined roles

11. In the **Add Members, roles to My First Project project** window, add the user account under **New members**.

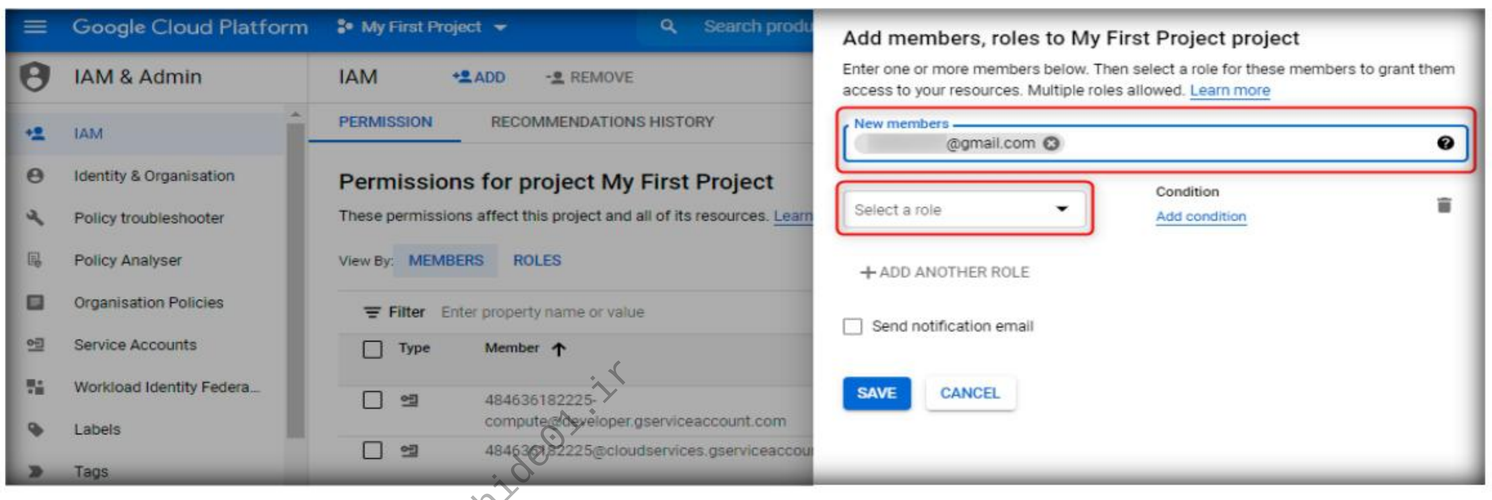


FIGURE 2.7.10: Adding Members and Selecting Another Role

12. Click on **Select a role** and scroll down to the bottom to locate an appropriate service and its corresponding role. Select **Project** as the service and **Editor** as the role.

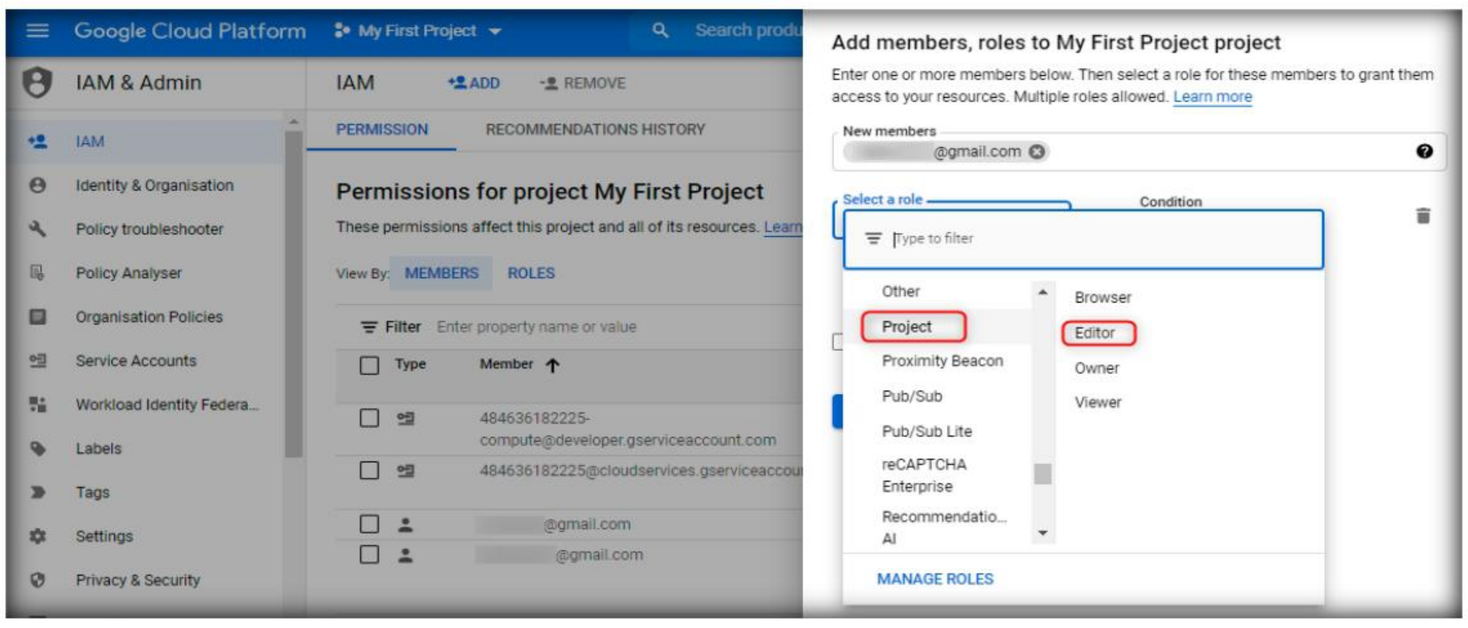


FIGURE 2.7.11: Selecting Role for the Project

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

13. Now, click on **ADD ANOTHER ROLE**.

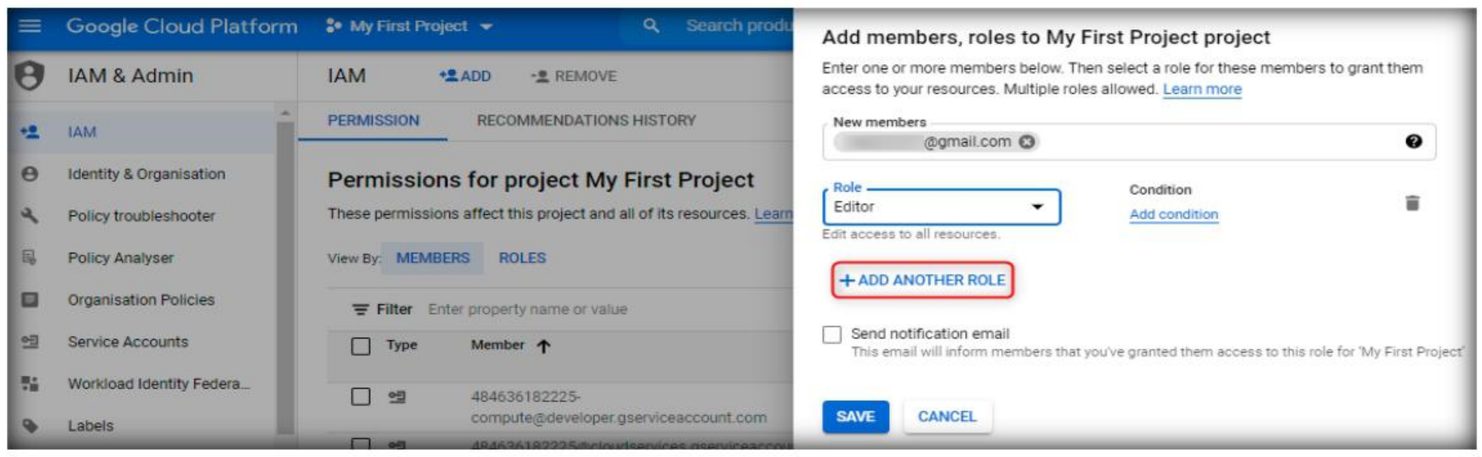


FIGURE 2.7.12: Adding a new role

14. Click on **Select a role** again and scroll down to the bottom. Select **Cloud Storage** as the service and **Storage Object Viewer** as the role.

    Note: In GCP IAM, child resources inherit the policies of parent resources. In other words, in this case, when the user is granted the **Editor** role for a project, a child resource for the same user is granted the **Storage Object viewer** access. Hence, the user has an editor access for the child resource.

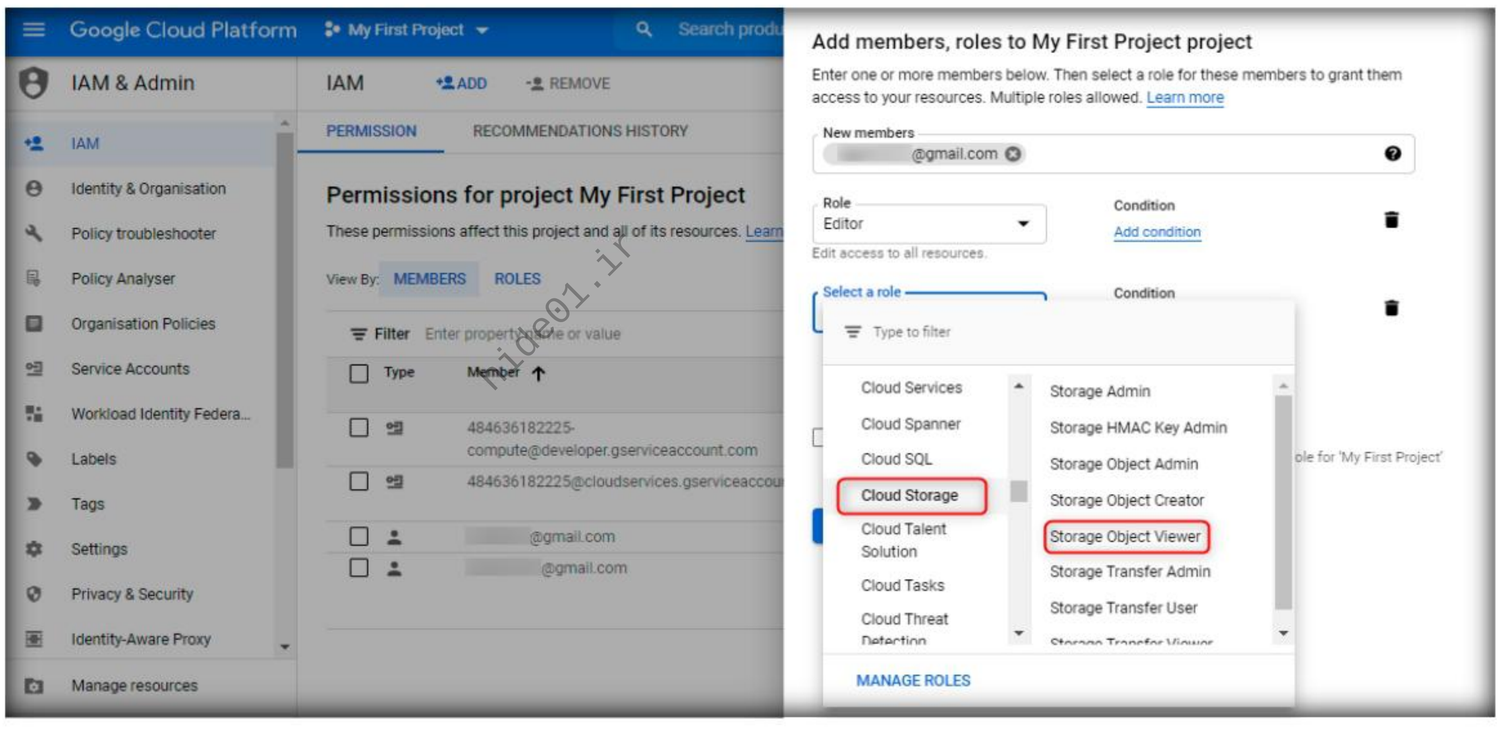


FIGURE 2.7.13: Adding Roles

15. Click on **SAVE**.

    Note: The roles granted here are for this lab only. In a production environment, the IAM administrator can grant access based on the requirements.

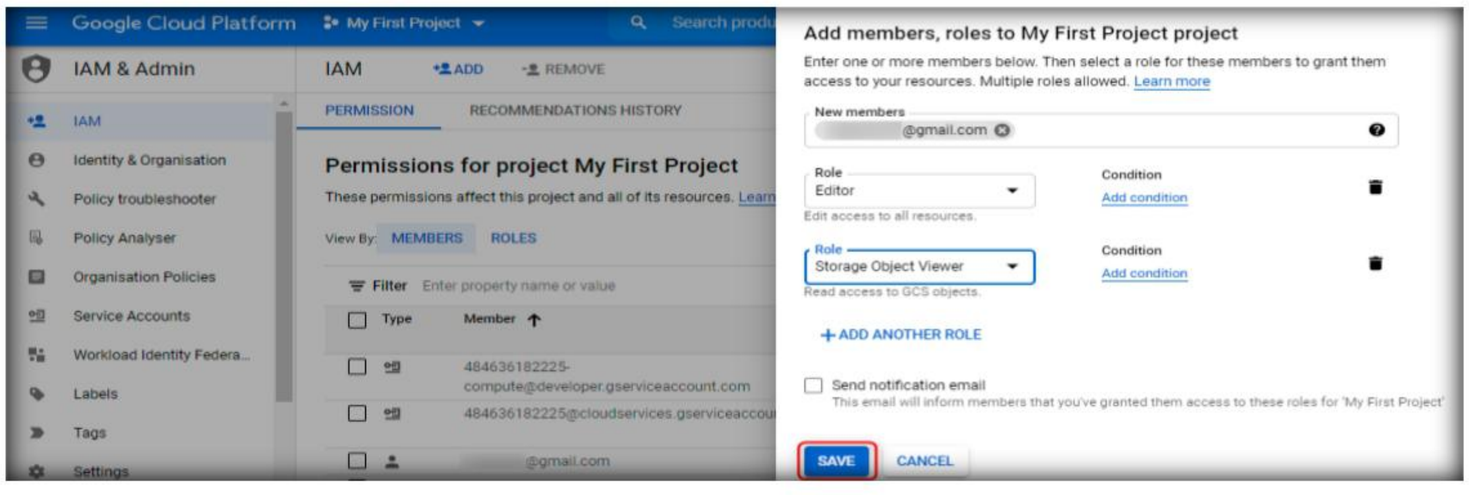


FIGURE 2.7.14: Saving the Roles

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

16. The granted predefined roles for the new user can be viewed from the IAM dashboard.

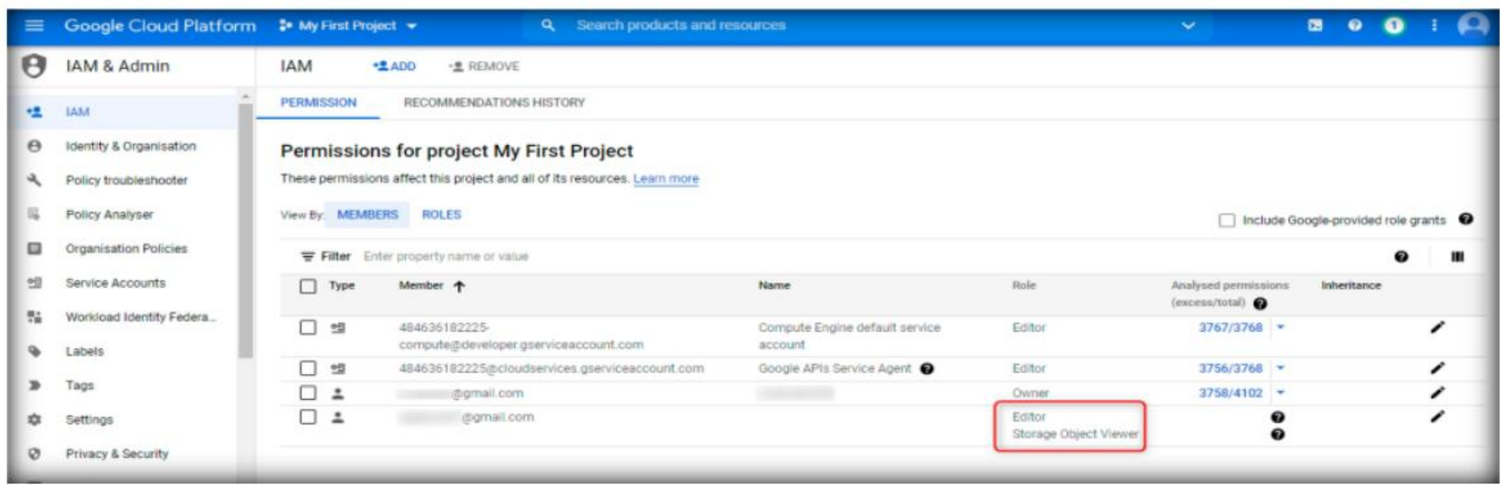


FIGURE 2.7.15: Viewing the Roles

TASK 2

Creating Custom Roles in GCP IAM

17. Navigate to **IAM & Admin** and select **Roles** in the console.

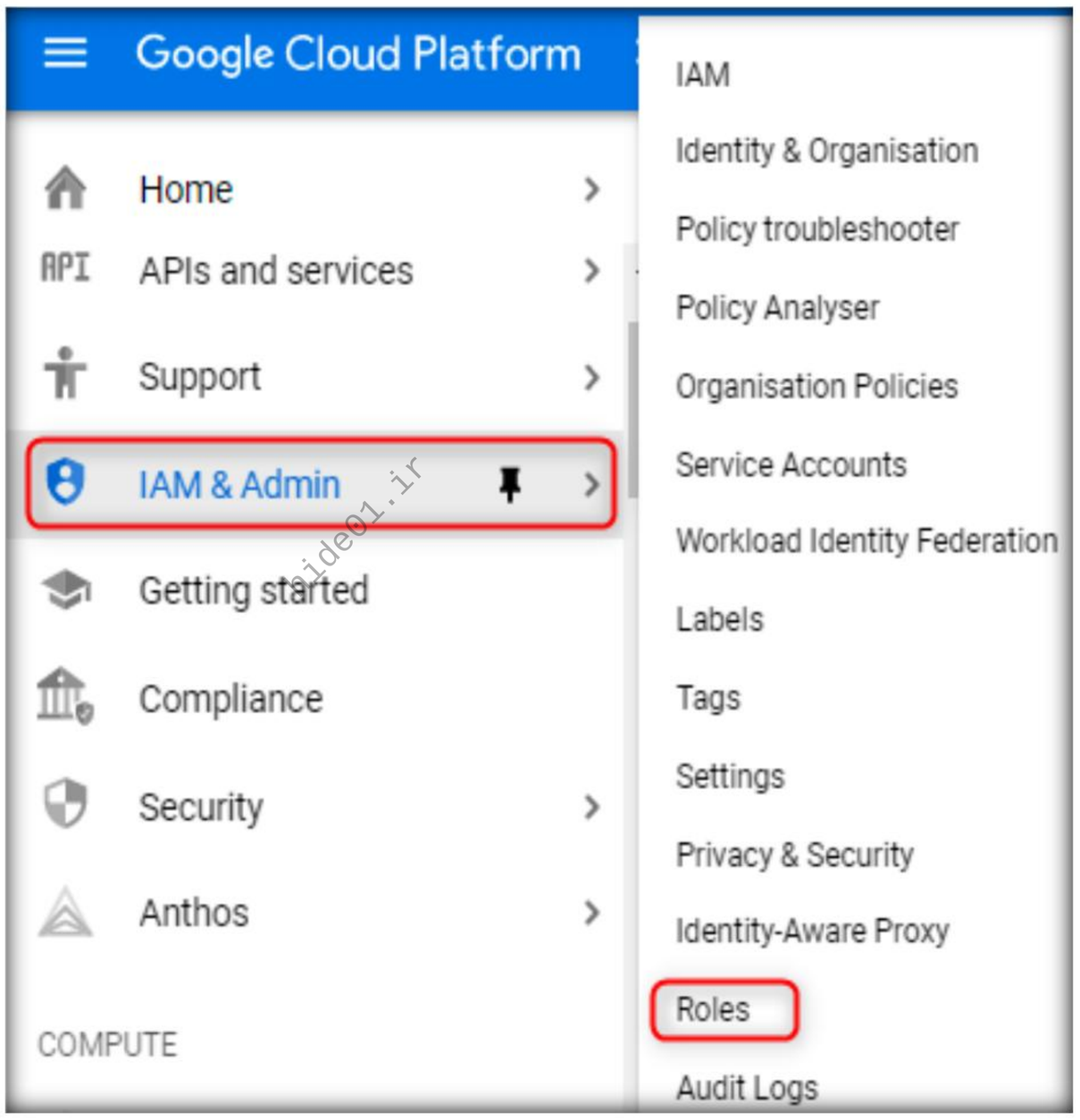


FIGURE 2.7.16: Navigating to Roles in IAM & Admin

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

18. Click on **Filter** and filter by **Name** to select the appropriate role.

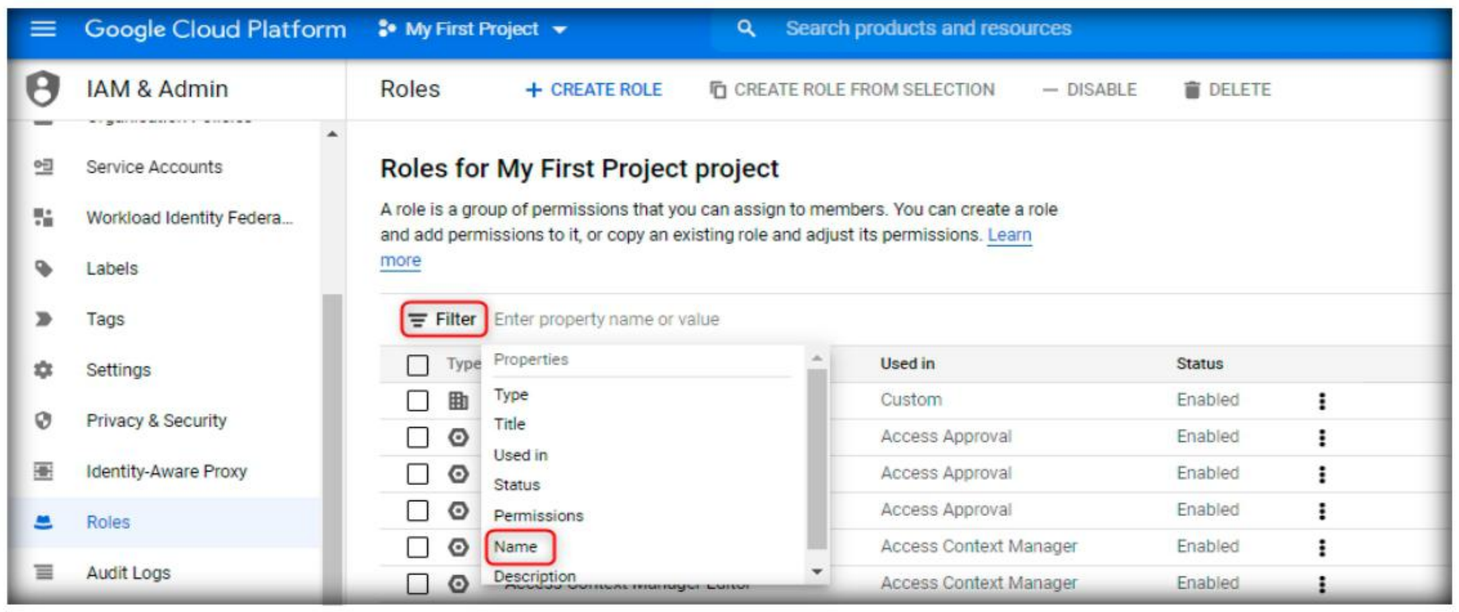


FIGURE 2.7.17: Filtering the Roles

19. You can search for the type of role. Choose **roles/appengine.appAdmin (App Engine Admin)** role.

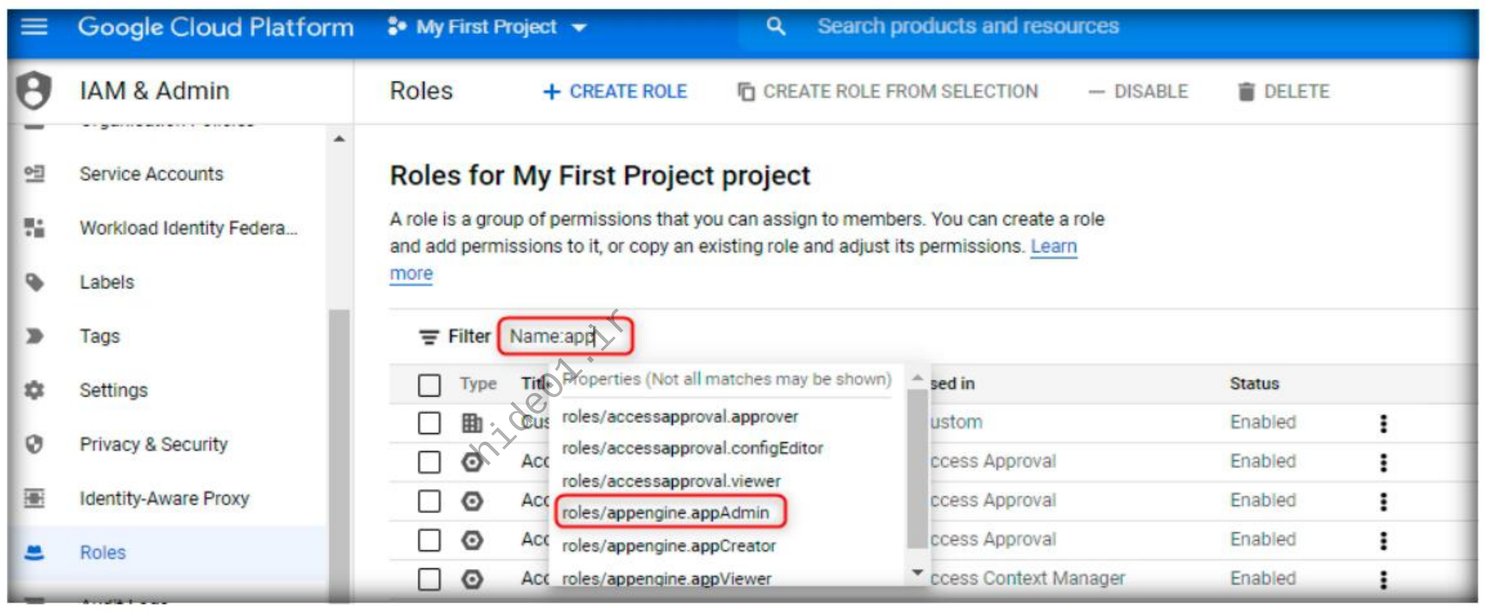


FIGURE 2.7.18: Creating Roles

20. After selecting the role, click on the **three dots** to the right side of the selected role and select **Create role from this role**.

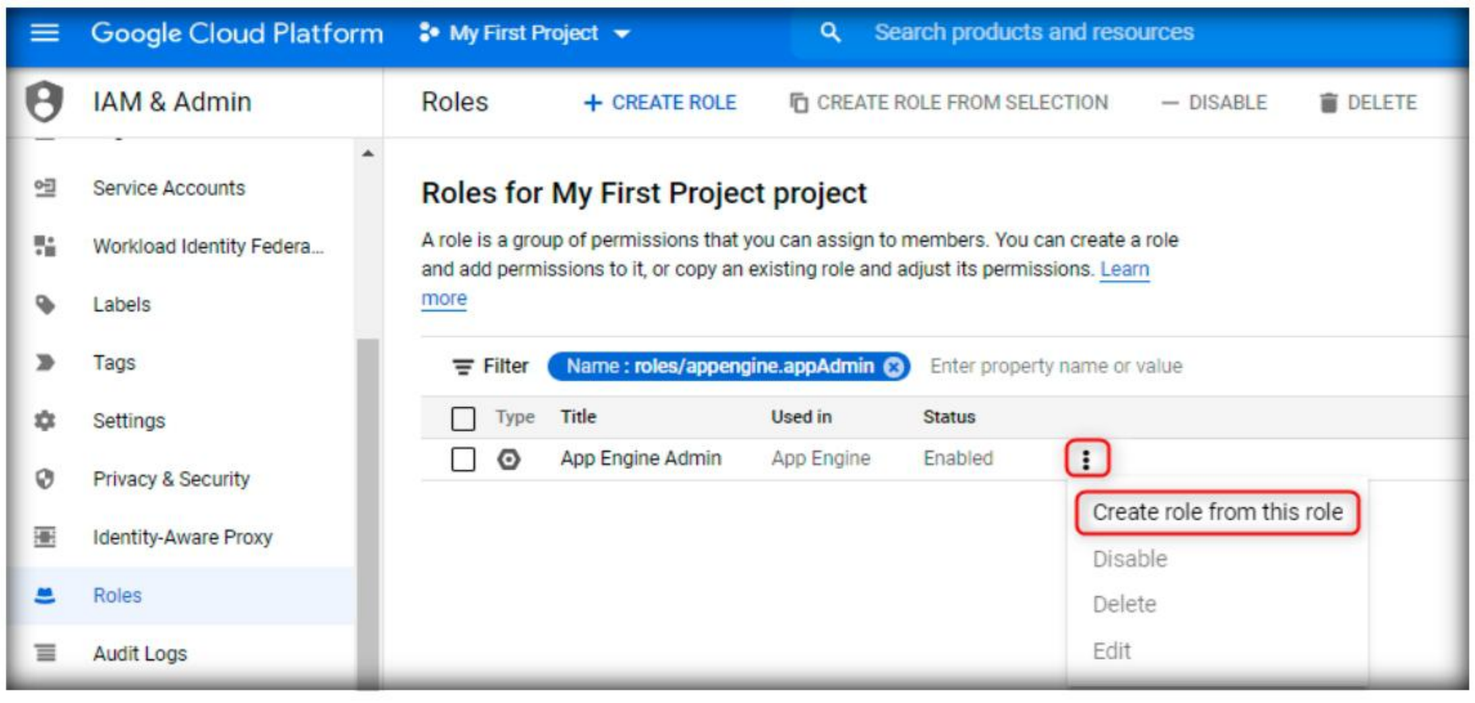


FIGURE 2.7.19: Adding Roles for the Selected Role

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

21. Type the **Title** as **Custom Roles for App Engine Admin** and the **ID** as **CustomAppEngineAdmin** for the role. Next, click on **ADD PERMISSIONS**.

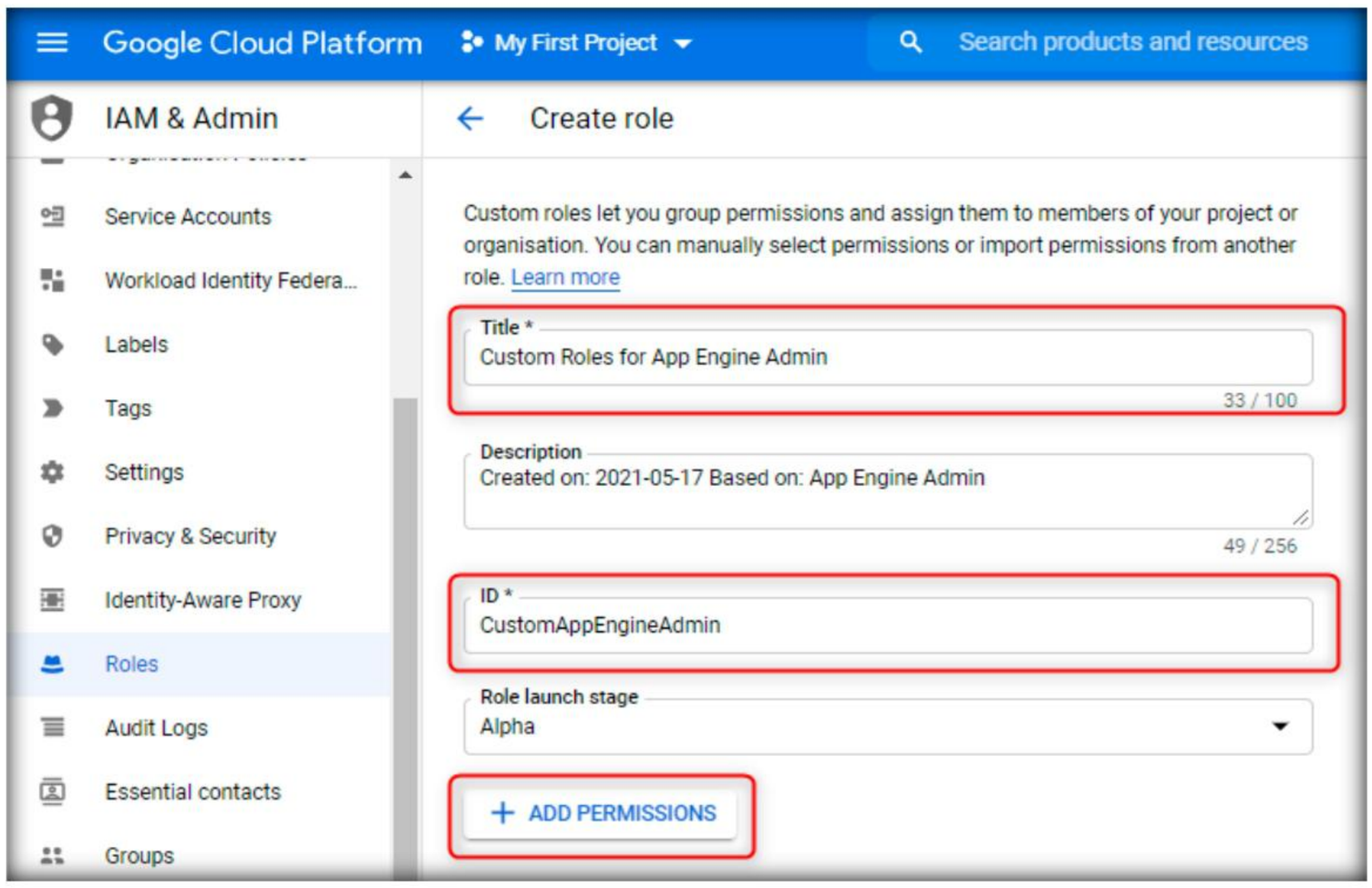


FIGURE 2.7.20: Giving the Role Title and ID

22. Now, select the **accessapproval.requests.dismiss**, **accessapproval.requests.delete**, and **accessapproval.requests.update** permissions, and click **ADD**.

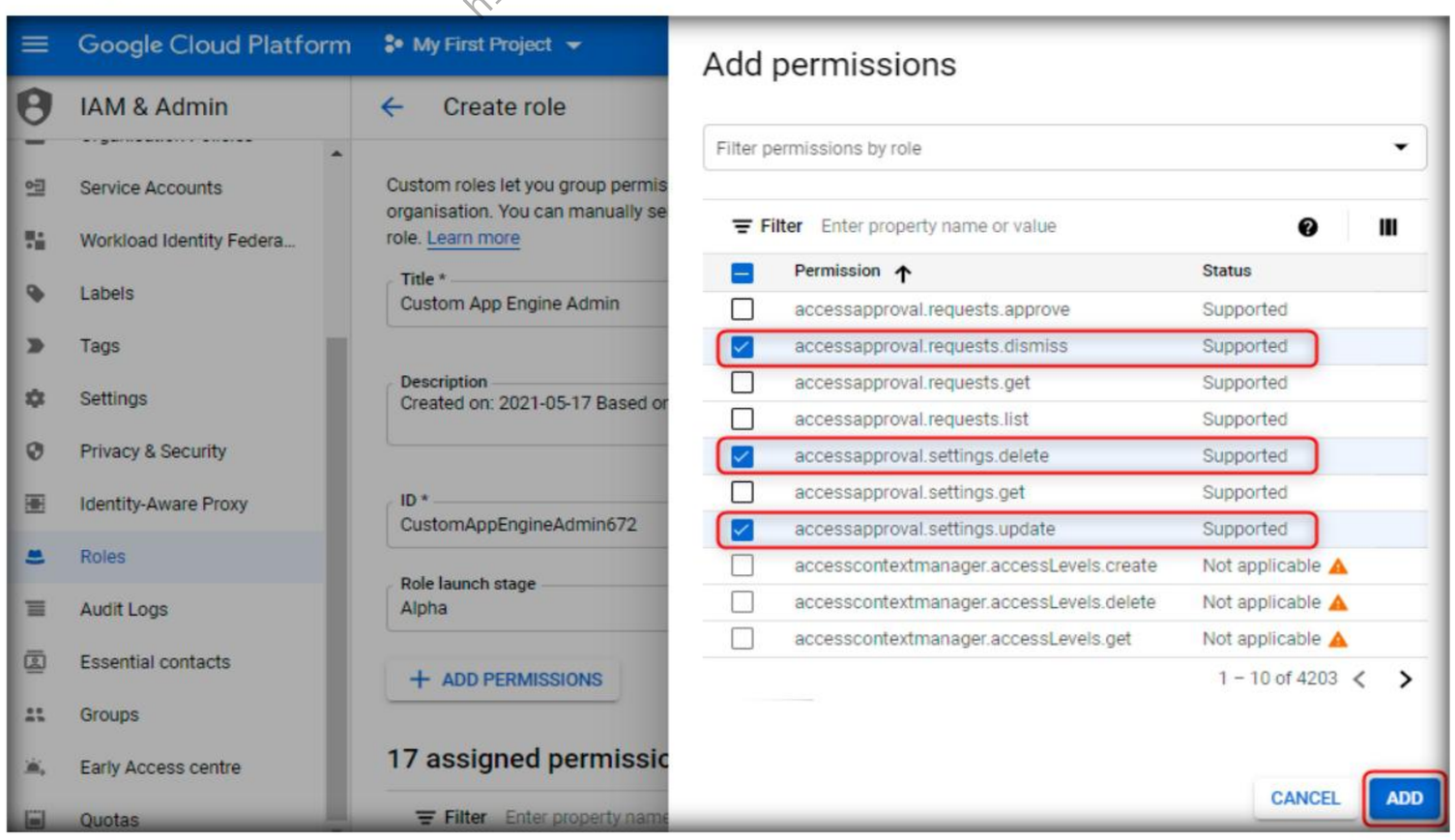


FIGURE 2.7.21: Adding More Permissions

Certified Cloud Security Engineer Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

23. Scroll down to the bottom to view the added permissions. Click on **CREATE**.

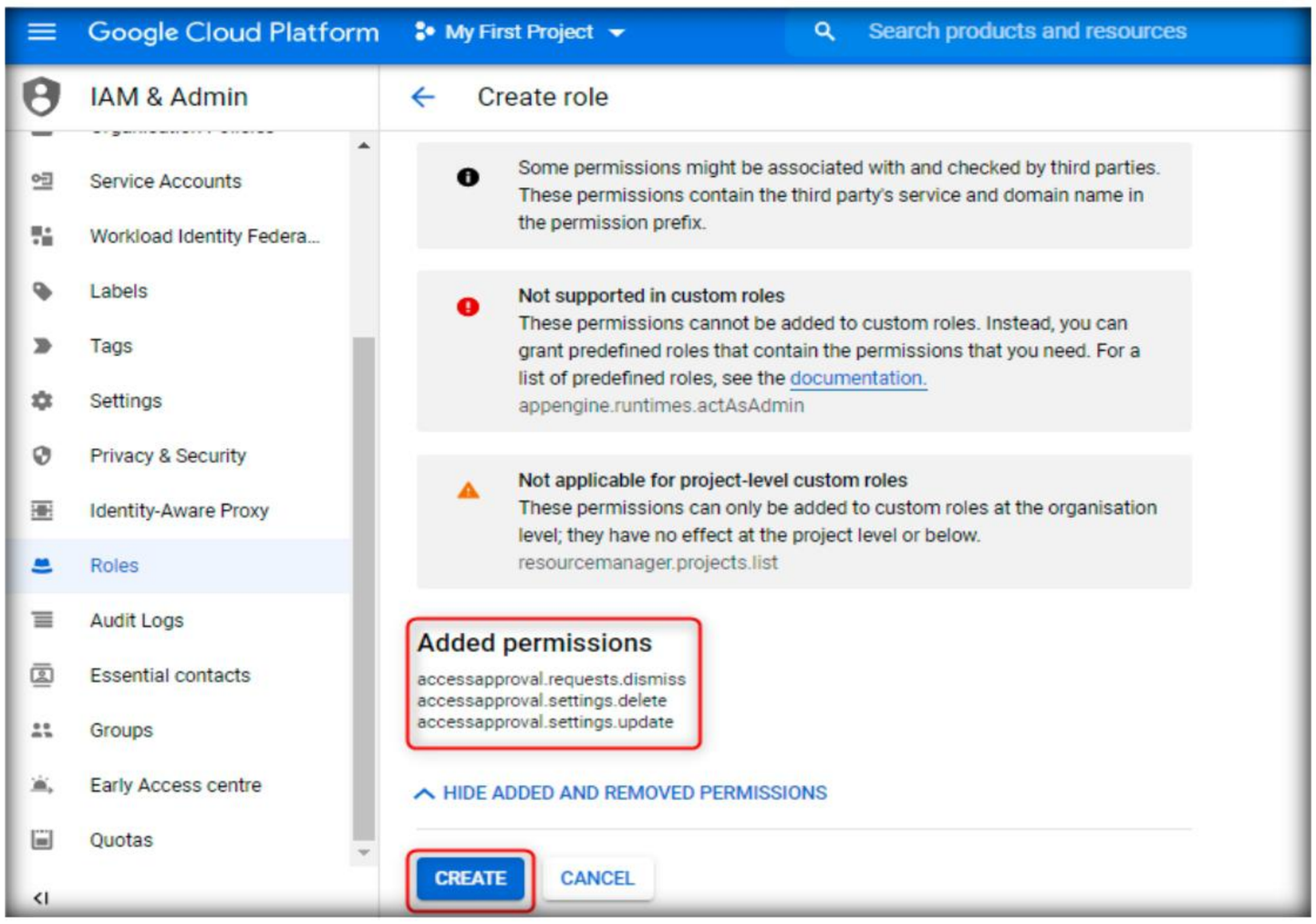


FIGURE 2.7.22: Viewing and Creating the new permissions

24. Now, navigate back to **IAM & Admin** and select **IAM** in the console.

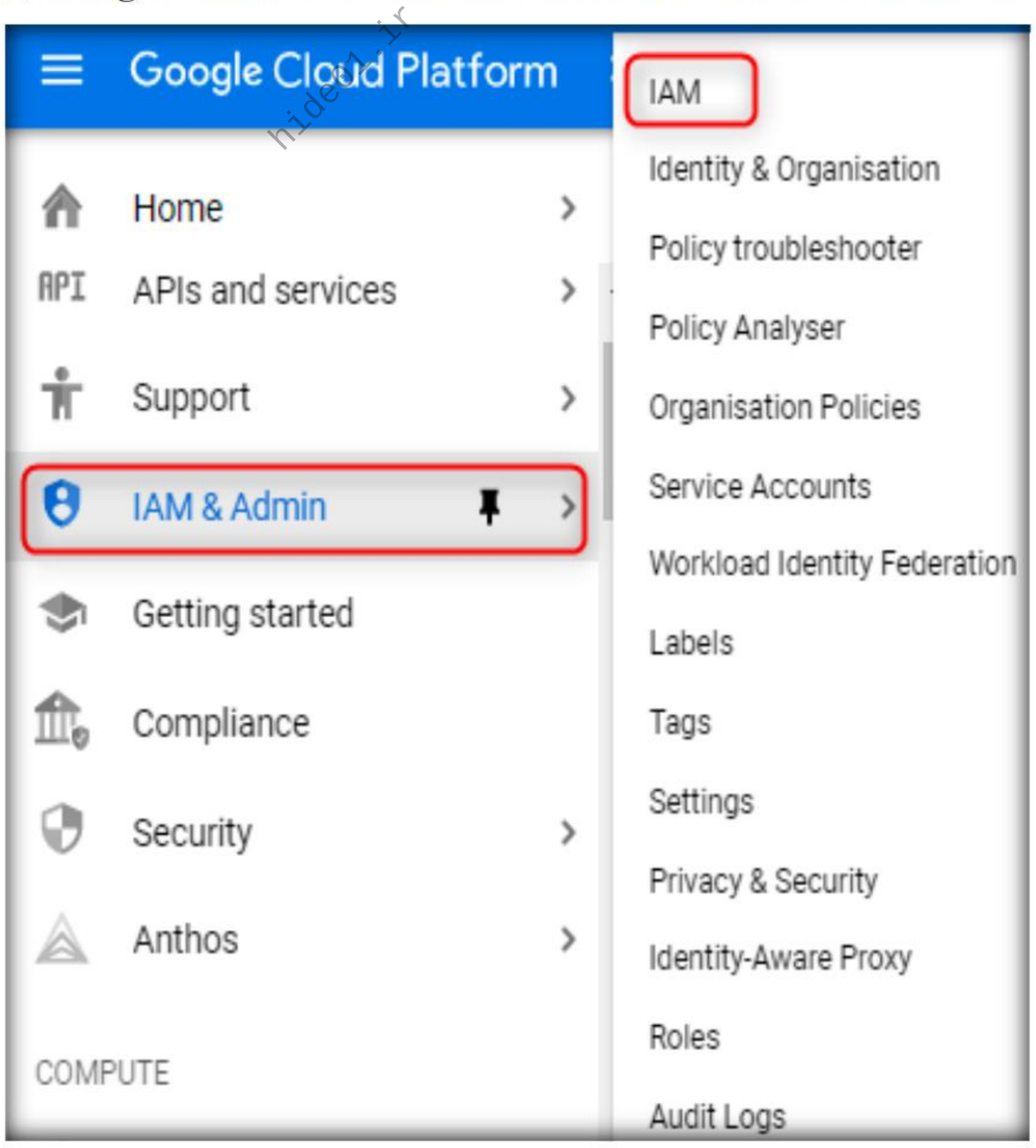


FIGURE 2.7.23: Navigating to IAM in console

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

25. Click on the **edit** icon to the right side of the member's user ID.

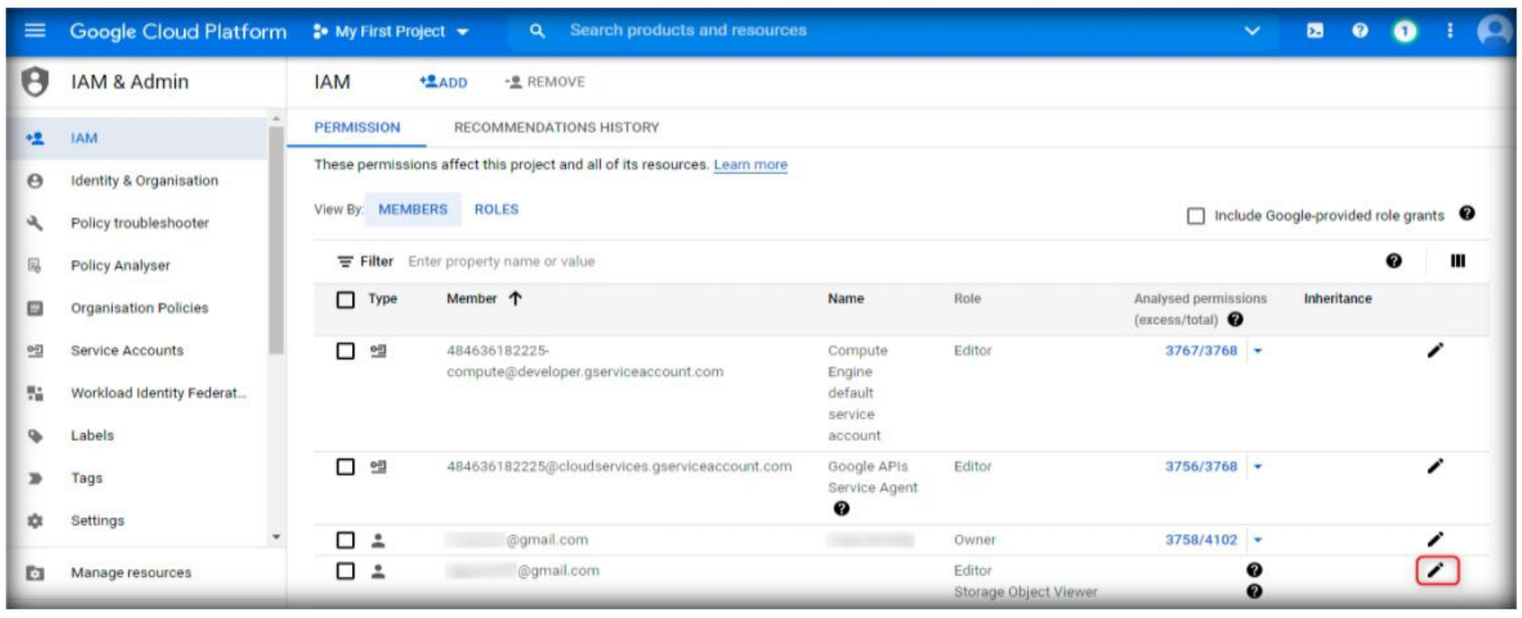


FIGURE 2.7.24: Editing the user role

26. In the **Edit permissions** window, click on **ADD ANOTHER ROLE** to add the custom role you just created.

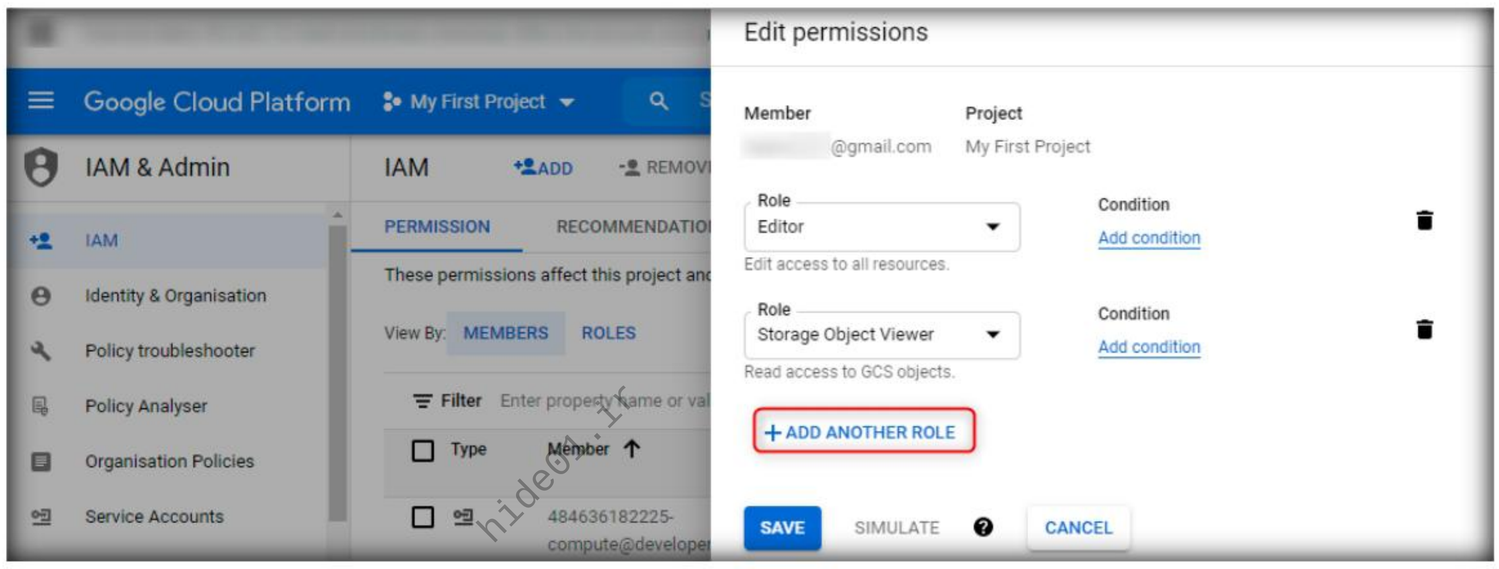


FIGURE 2.7.25: Adding Permission

27. Now, click on **Select a role**. Scroll down to locate **Custom** and then select the name of the custom role: **Custom Roles for App Engine Admin.**

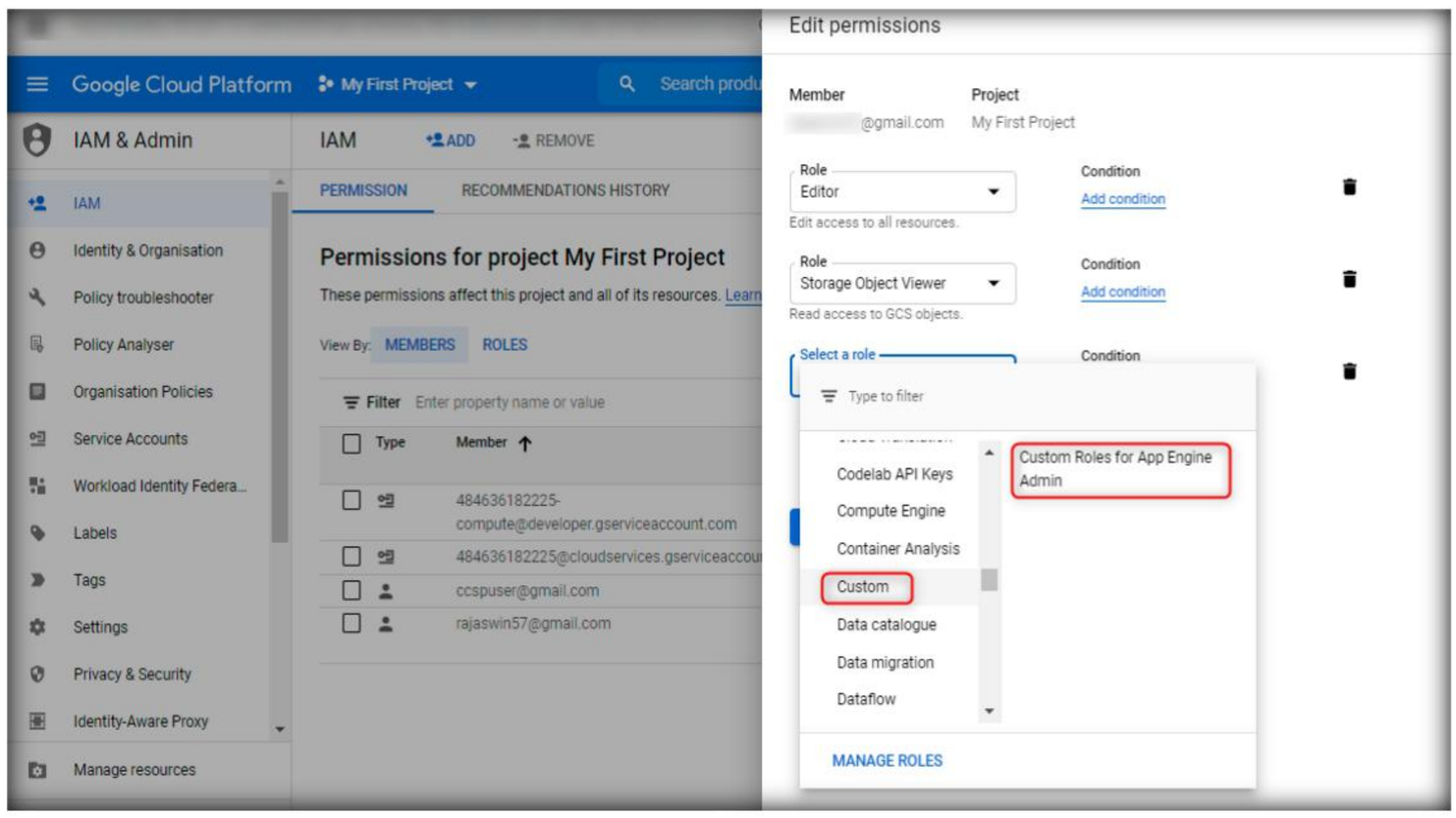


FIGURE 2.7.26: Selecting the Custom Role

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

28. Next, click **SAVE**.

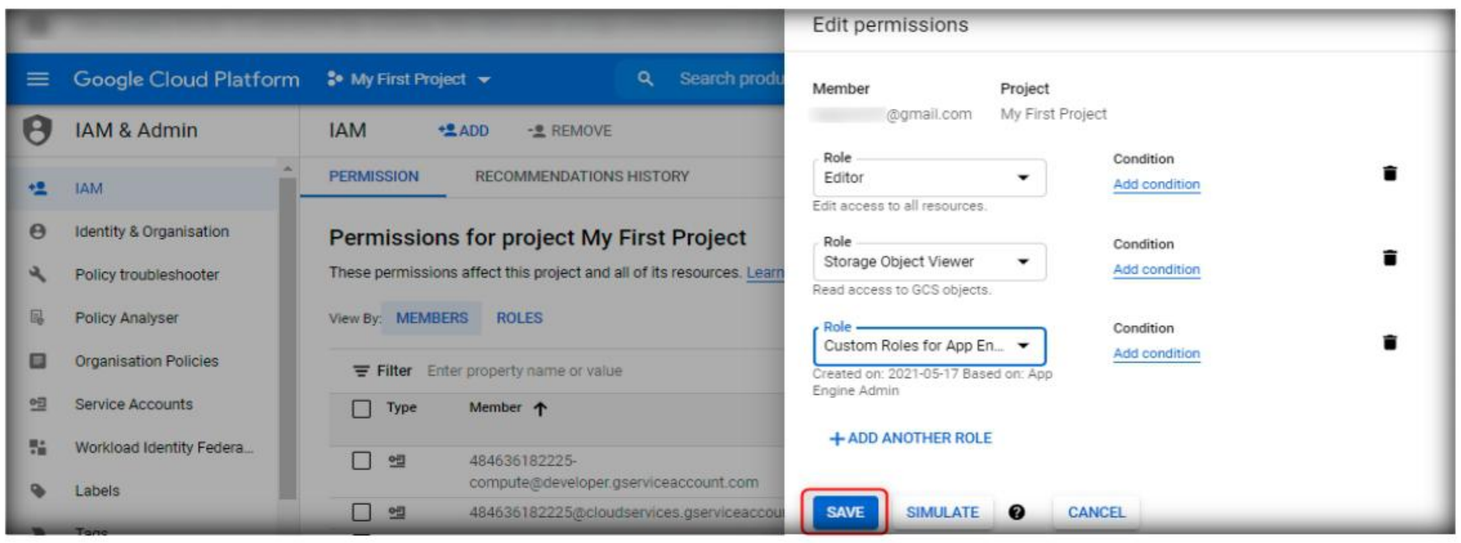


FIGURE 2.7.27: Saving the New Permission

29. The IAM dashboard displays the corresponding granted **Role** of the user.

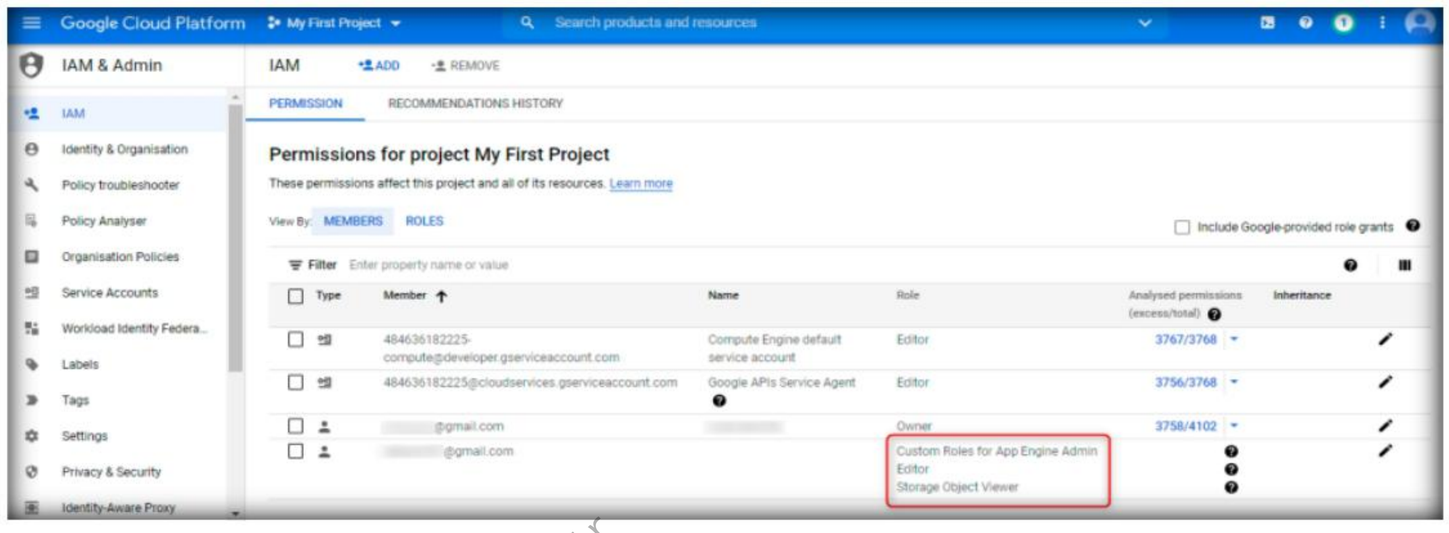


FIGURE 2.7.28: Assigned Roles for the User

TASK 3

Revoking the Granted Access to Users

30. Next, we will revoke a certain set of roles for the users. To do his, go to the IAM dashboard and click on the **Edit** icon to the right side of the user ID.

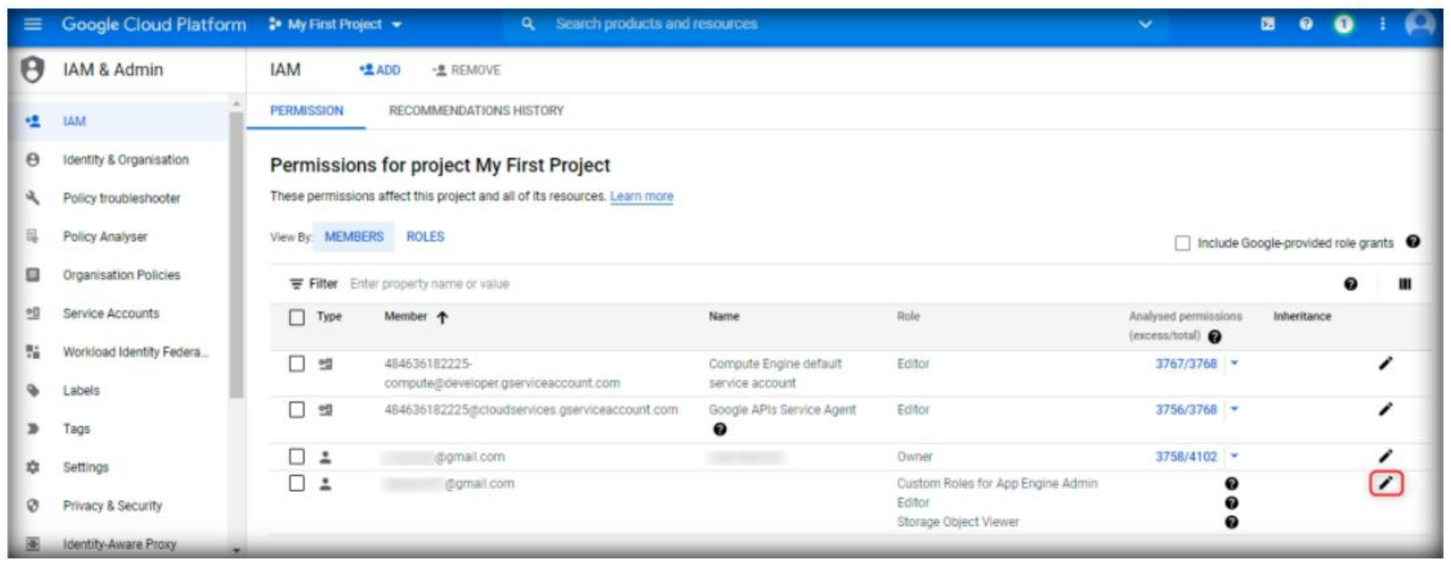


FIGURE 2.7.29: Editing the Roles

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

31. In the **Edit permissions** window, click on the **Delete icon** to the right side of the particular role to be revoked. Click **SAVE**.

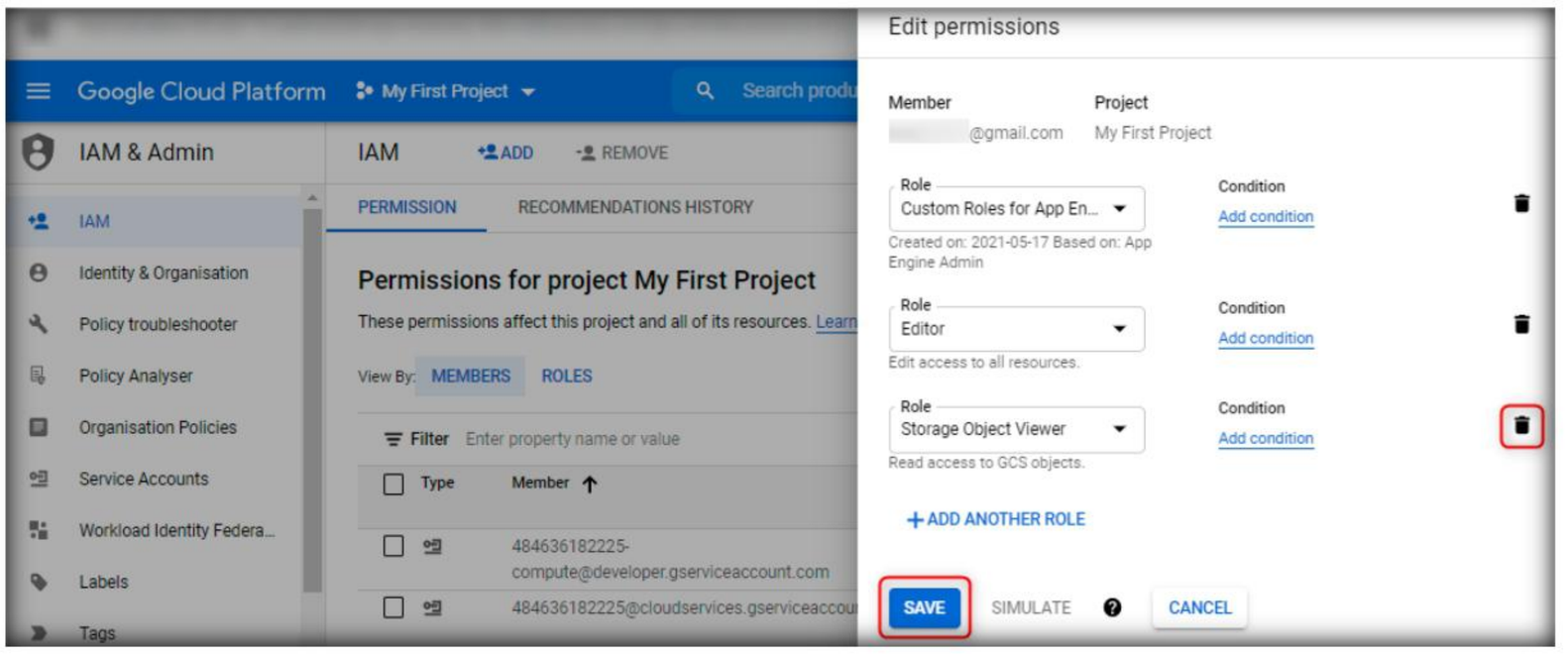


FIGURE 2.7.30: Deleting Roles

32. The roles corresponding to the user will be revoked.

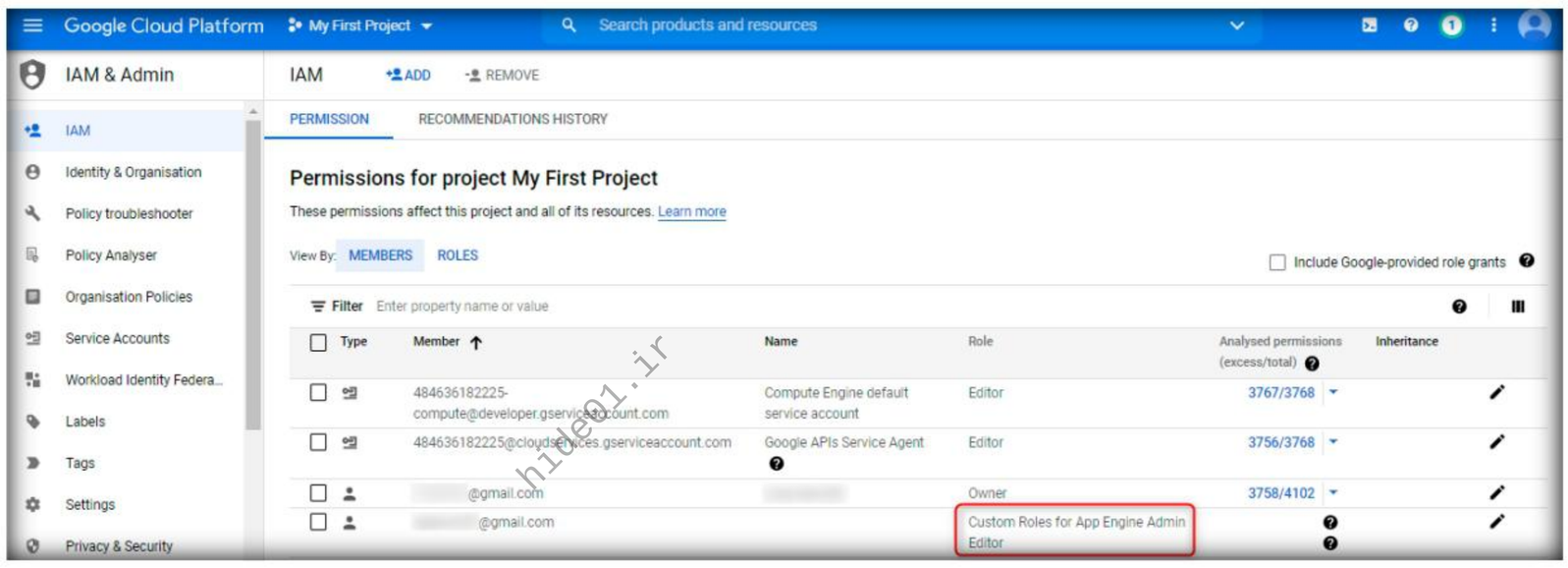


FIGURE 2.7.31: Role is Revoked

33. This way, a cloud security professional can use **GCP IAM** to grant access to users based on certain roles by following the principle of least privilege.

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

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

34. Now, to delete the user you have created, select the checkbox for the user in the IAM window and click on **REMOVE** at the top, as shown in the screenshot below.

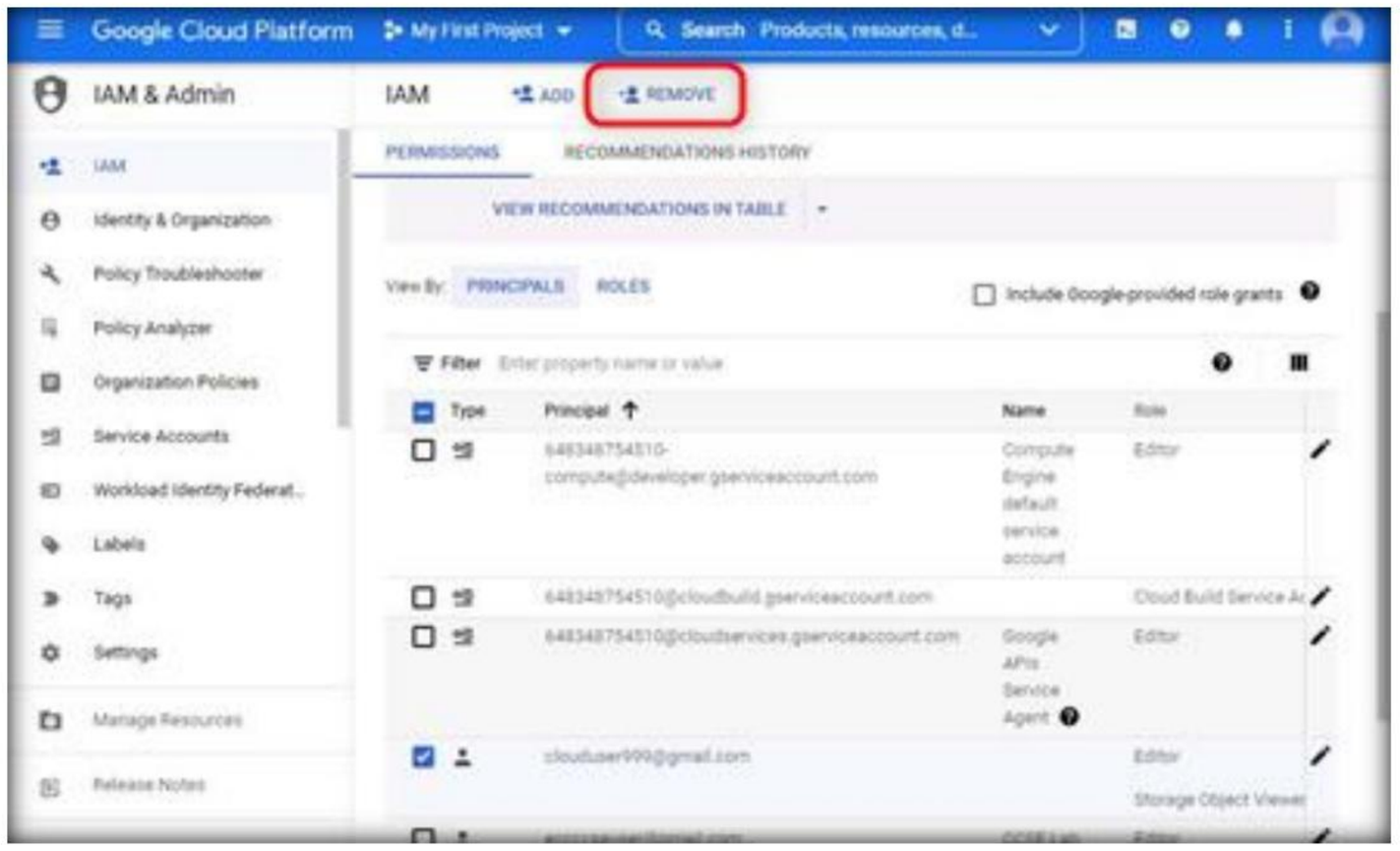


FIGURE 2.7.32: Deleting User

35. To delete the custom role you have created for the user, navigate to **Roles** in the left pane of the **IAM & Admin** window. Click on the ellipsis next to the custom role you have created and click on **Delete**.

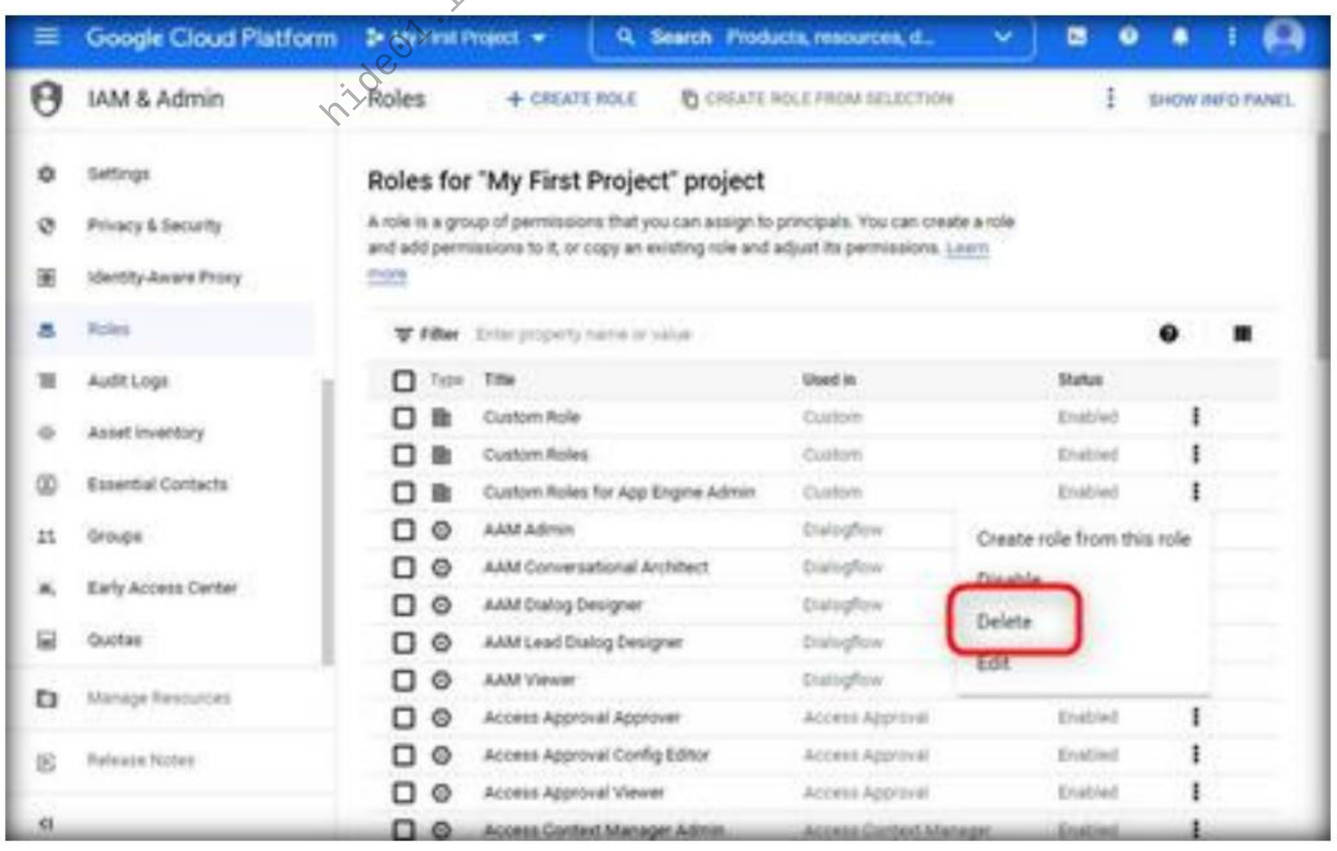


FIGURE 2.7.33: Deleting Role

Note: The custom role will be marked as deleted and deleted permanently after 7 to 14 days.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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.

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 8

Securing GCP Instances using Firewall Rules

Firewall rules are applied in a VPC network in Google Cloud Platform (GCP). The enabled firewall rules are strictly enforced, thereby securing instances within the VPC network, irrespective of their configuration and OS.

Lab Scenario

A cloud professional needs to apply the best security practices while performing cloud operations by implementing firewall rules. In this lab, you will understand how to set up a firewall rule to block ping requests from reaching a VM instance in GCP.

Lab Objectives

This lab will demonstrate the implementation of firewall rules in GCP.

In this lab, you will learn to do the following:

- Create a VM instance
- Configure firewall rules
- Add a firewall rule to the VM instance and verify it

ICON KEY

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

Lab Environment

To perform this lab, you need the following:

- **Admin Machine** VM
- **Administrative** privileges
- Registered GCP account

Lab Duration

Time: 15 minutes

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Overview of VPC Firewall Rules

Firewall rules are applied in the VPC network of GCP. VPC firewall rules are applied to a specific project or network. The enabled firewall rules are strictly enforced, thereby securing instances within the VPC network, irrespective of their configuration and OS. A VPC firewall serves as a distributed firewall and the rules are defined at a network level, where connections are denied or allowed on a per-instance basis. Firewall rules allow or deny traffic to and from the resources attached to the VPC, including Compute Engine VM instances and Google Kubernetes Engine (GKE) clusters. Network tags associate firewall rules and routes with specific VM instances. A cloud admin can apply firewall rules to tagged instances. In GCP, each firewall rule should have a target that specifies the instances to which it applies. By default, a firewall rule targets all instances in the network, but can be customized by the admin using target network tags. These tags specify the VMs in GCP to which they apply.

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., GCP), the application interface may be updated with time. Hence, in case you happen to work on an updated version of GCP, 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.

h4de01.ir

Note: Before starting this lab, you should create a GCP Free Trial account using the following link: https://cloud.google.com/free, in case you have already not created it for the previous lab. Once the registration is complete, perform the following tasks:

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

Note: If you are already logged in to the GCP console, skip the login steps.

TASK 1

Creating a New Project in Google Cloud Console

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

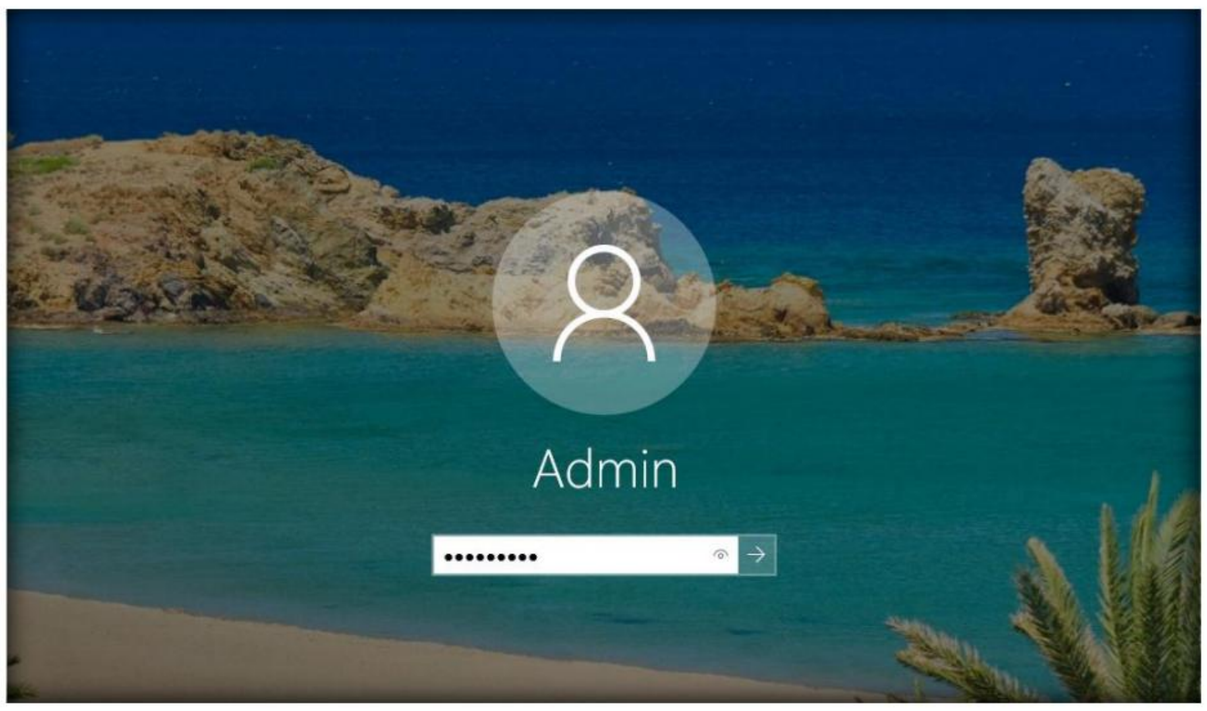


FIGURE 2.8.1: Launch Admin Machine and Log in

Certified Cloud Security Engineer Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

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



FIGURE 2.8.2: Navigating to the Chrome Browser from Taskbar

3. Go to the address bar, type **https://console.cloud.google.com/**, and press **Enter.**
4. In the **Sign in** page, enter the **Email or phone** and click **Next** to login into Google Cloud Console.

hide01.ir

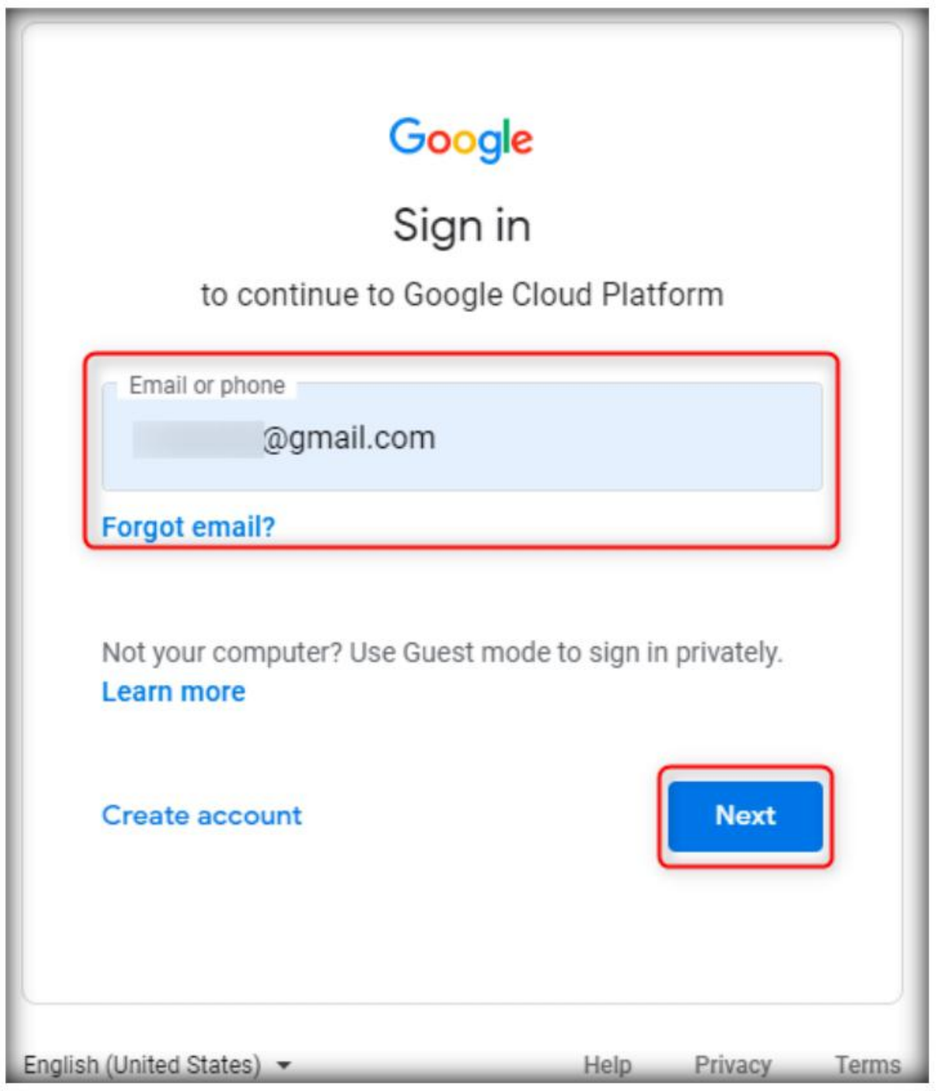


FIGURE 2.8.3: Access GCP in Browser

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

5. Enter the **password** and click on **Next**.

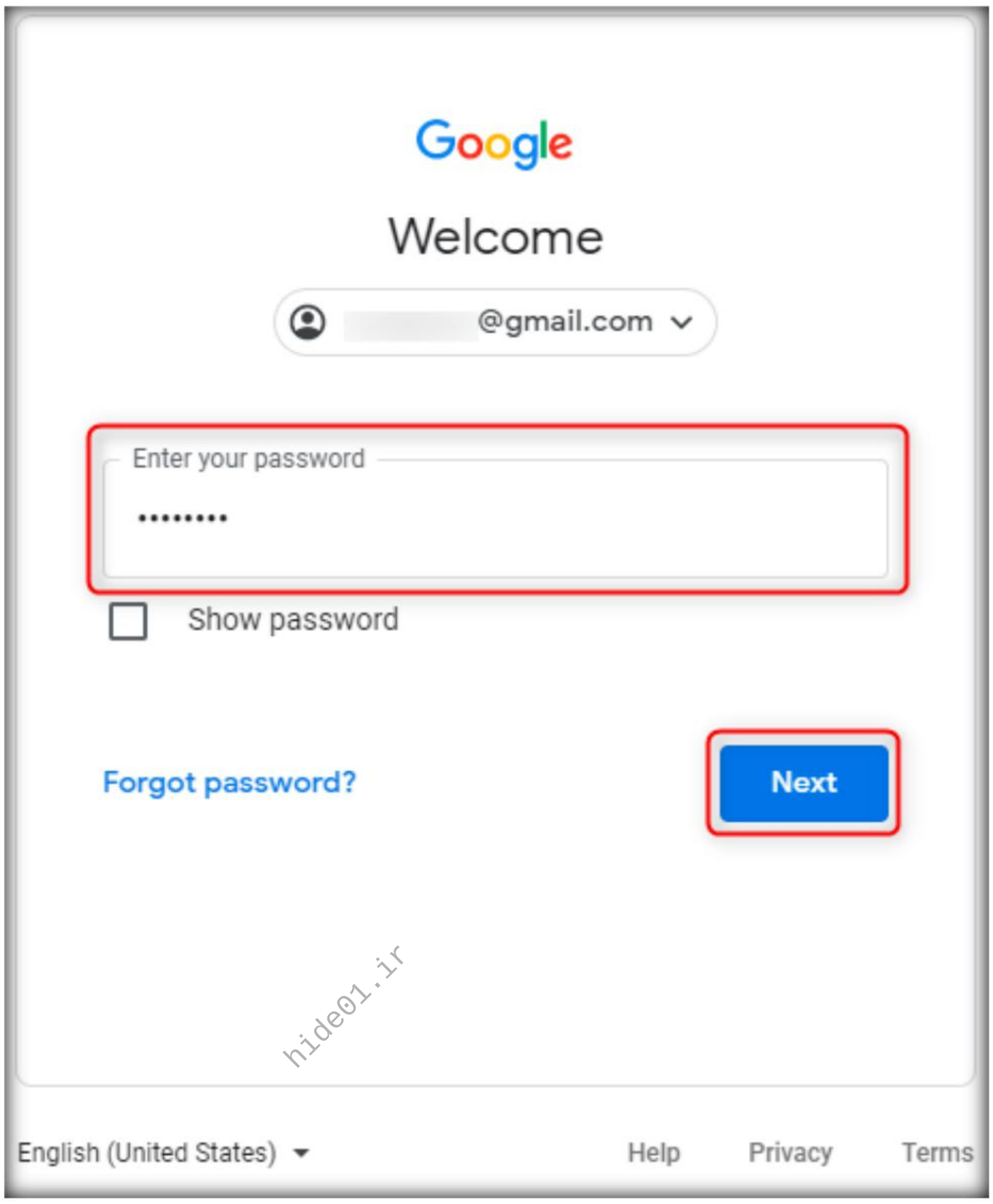


FIGURE 2.8.4: Signing in into GCP console

6. On top left corner, you will see a dropdown. If **My First Project** is the default selected project, then skip **Steps 7–16** and go to **step 17**.

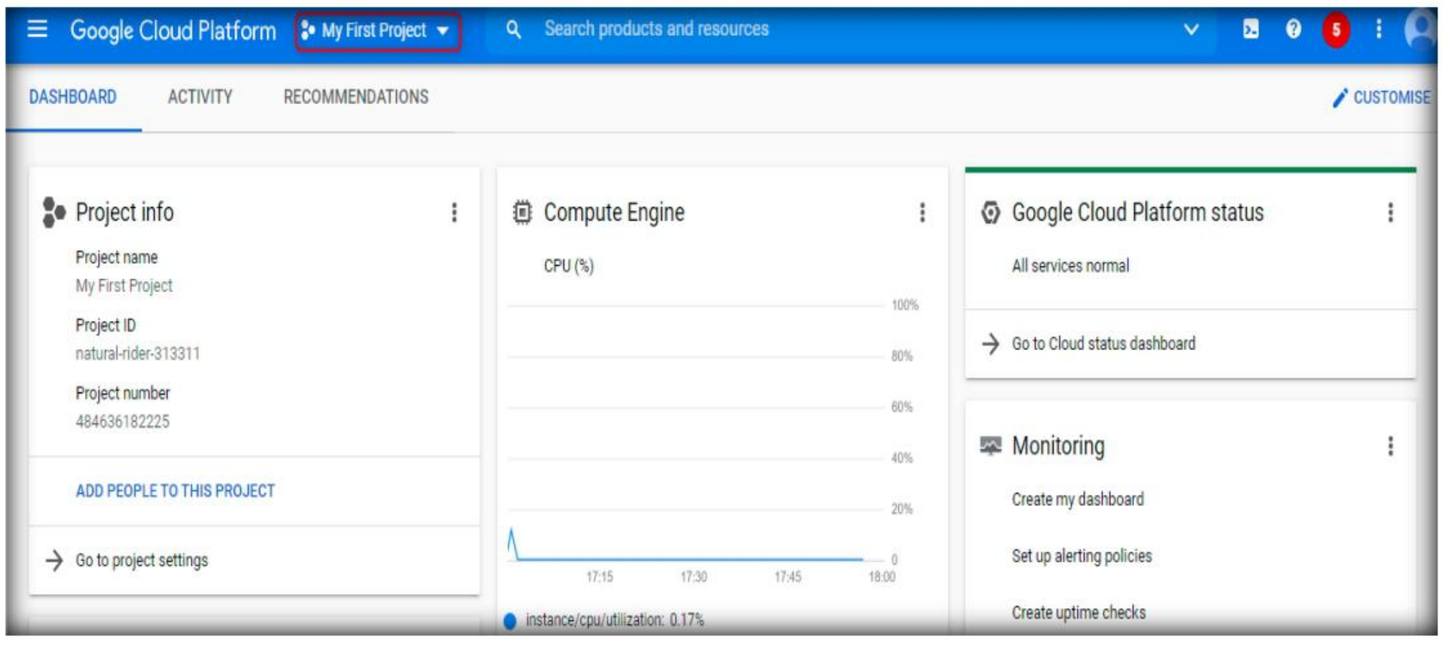


FIGURE 2.8.5: Create New Project

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

7. On top left corner, in the dropdown, if you see **Select a Project** with an empty dashboard, then click on **CREATE PROJECT** to create a new project.

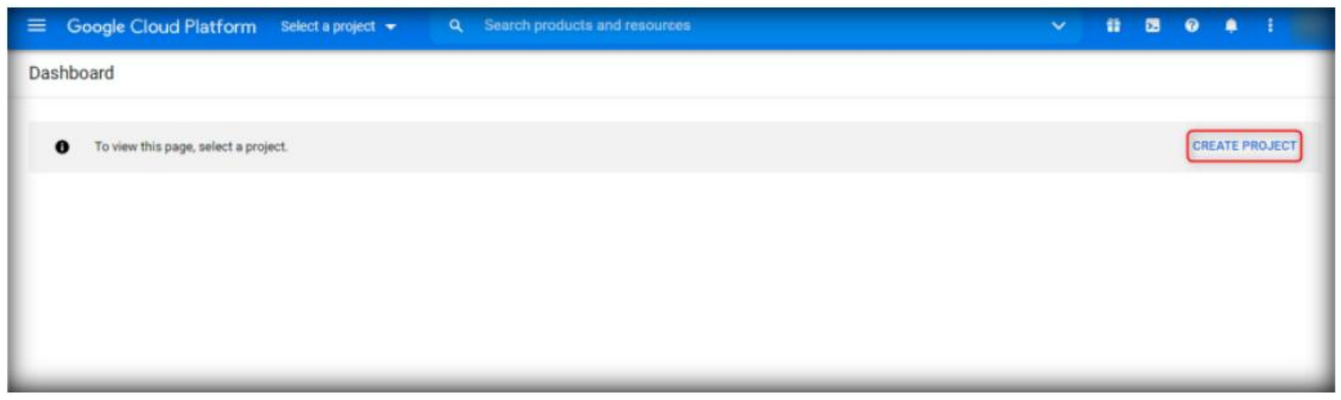


FIGURE 2.8.6: Creating Project

8. In the **New Project** window that opens, type the **Project name** as **My First Project**. Then, click on **CREATE**.

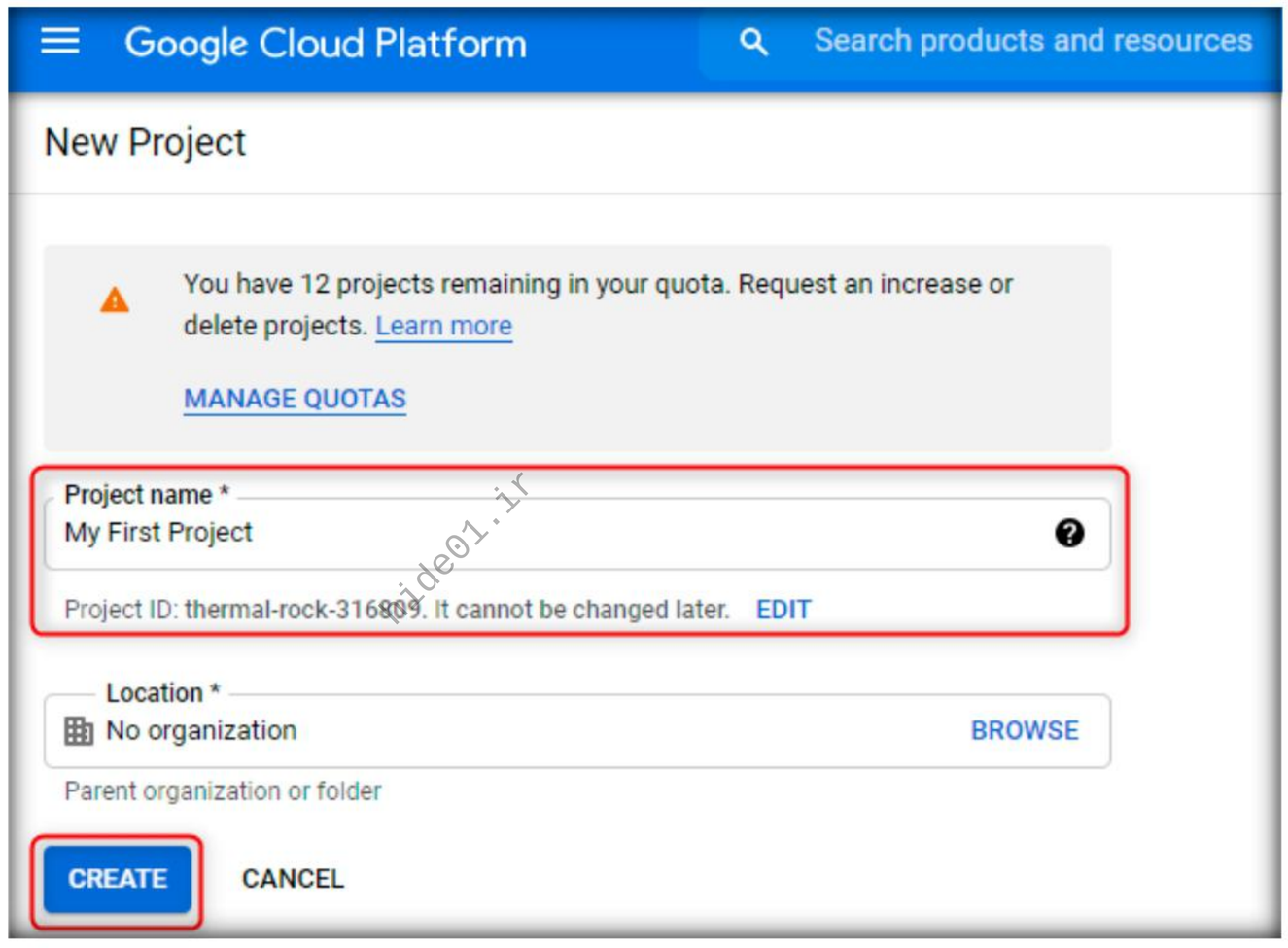


FIGURE 2.8.7: Configuring New Project

9. Your project will be successfully created. You can see that at the top of the window, **My New Project** will be selected as the current project by default.

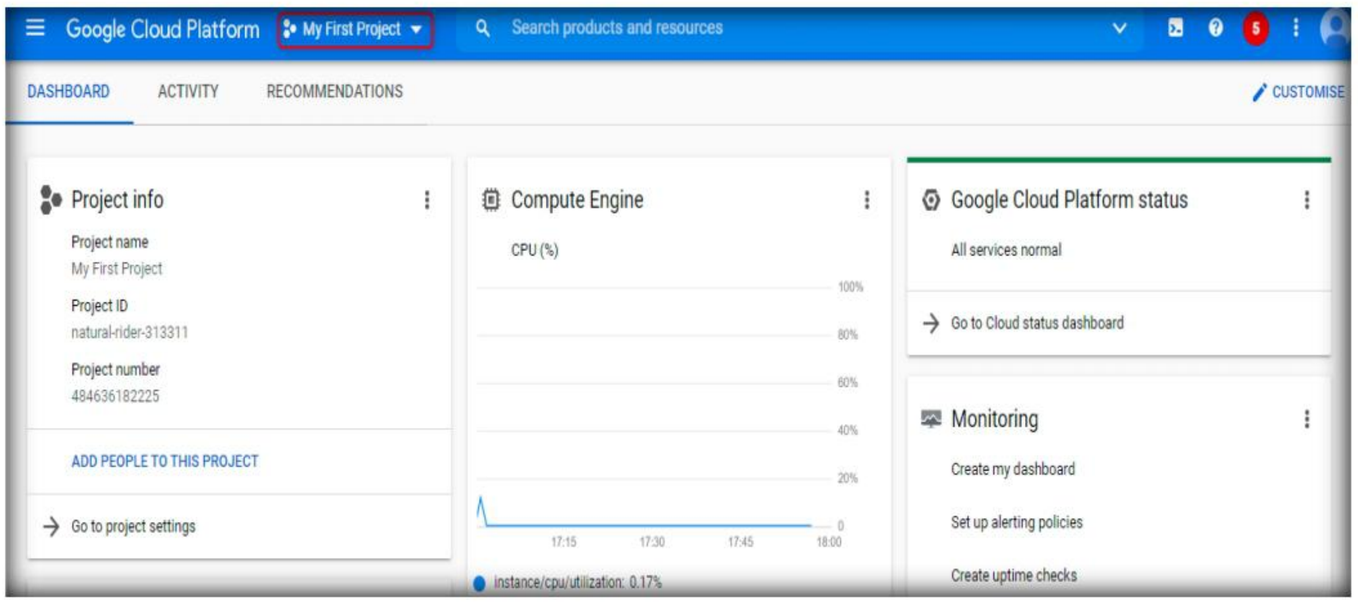


FIGURE 2.8.8: My First Project Selected as Default

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

10. On top left corner, if the dropdown displays a different project by default and not **My First Project**, then click on the dropdown.

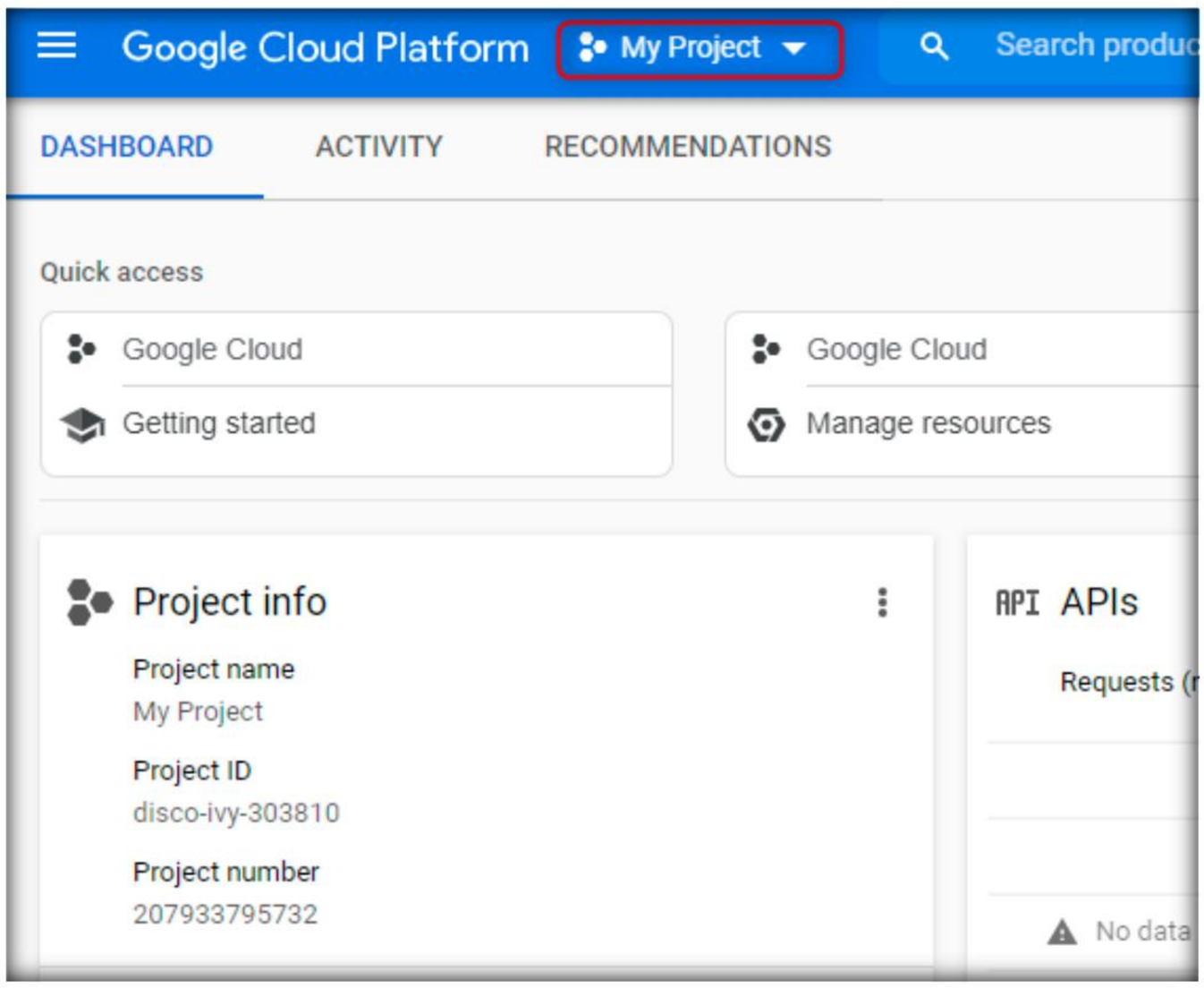


FIGURE 2.8.9: Selecting Project Dropdown

11. A **Select a project** window opens, which displays all existing projects. It also provides a **Search projects and folders** option to search for an existing project. Select **My First Project** from the displayed list of existing projects.

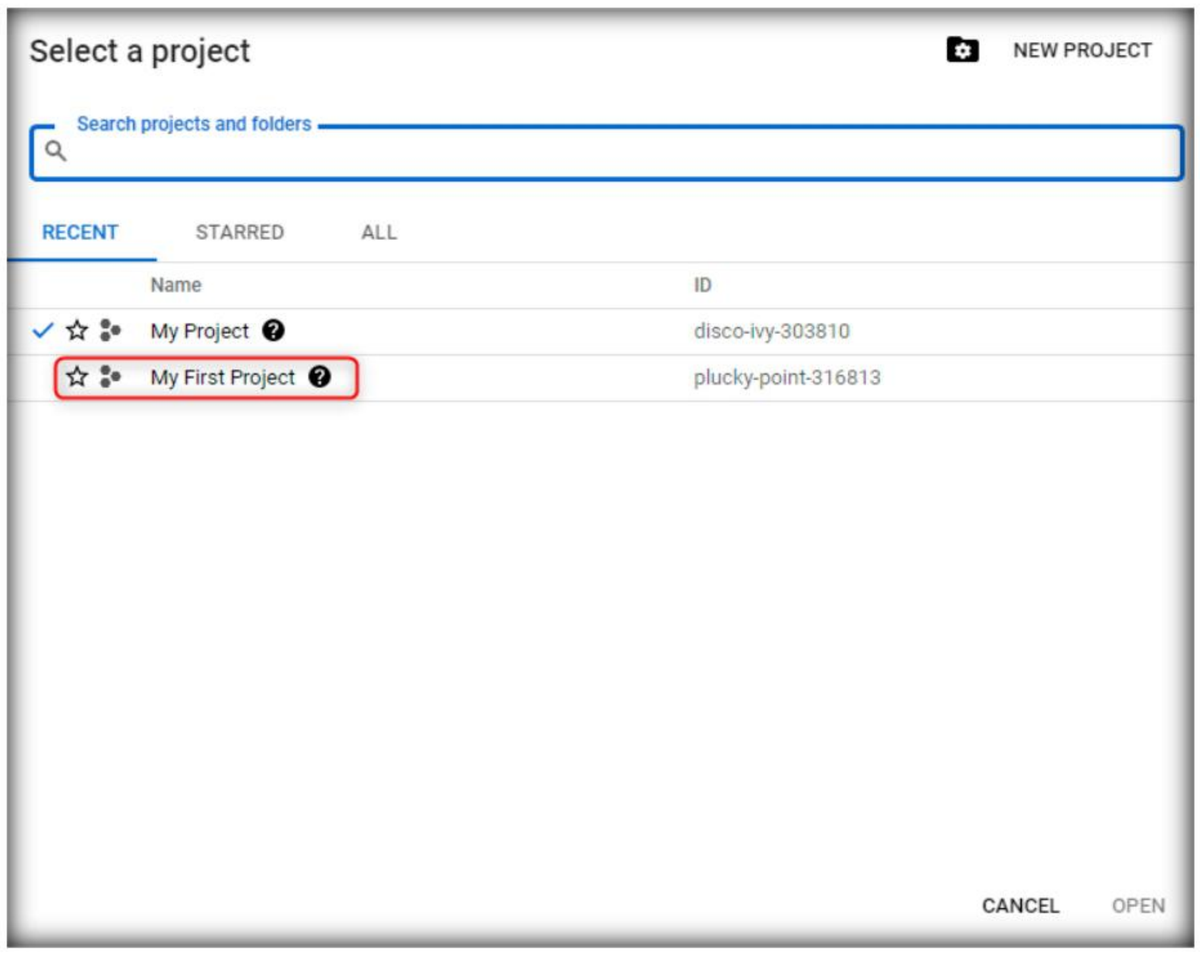


FIGURE 2.8.10: Selecting My First Project

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

12. Now, if **My First Project** is not in the list, click on the **NEW PROJECT** option to create **My First Project**.

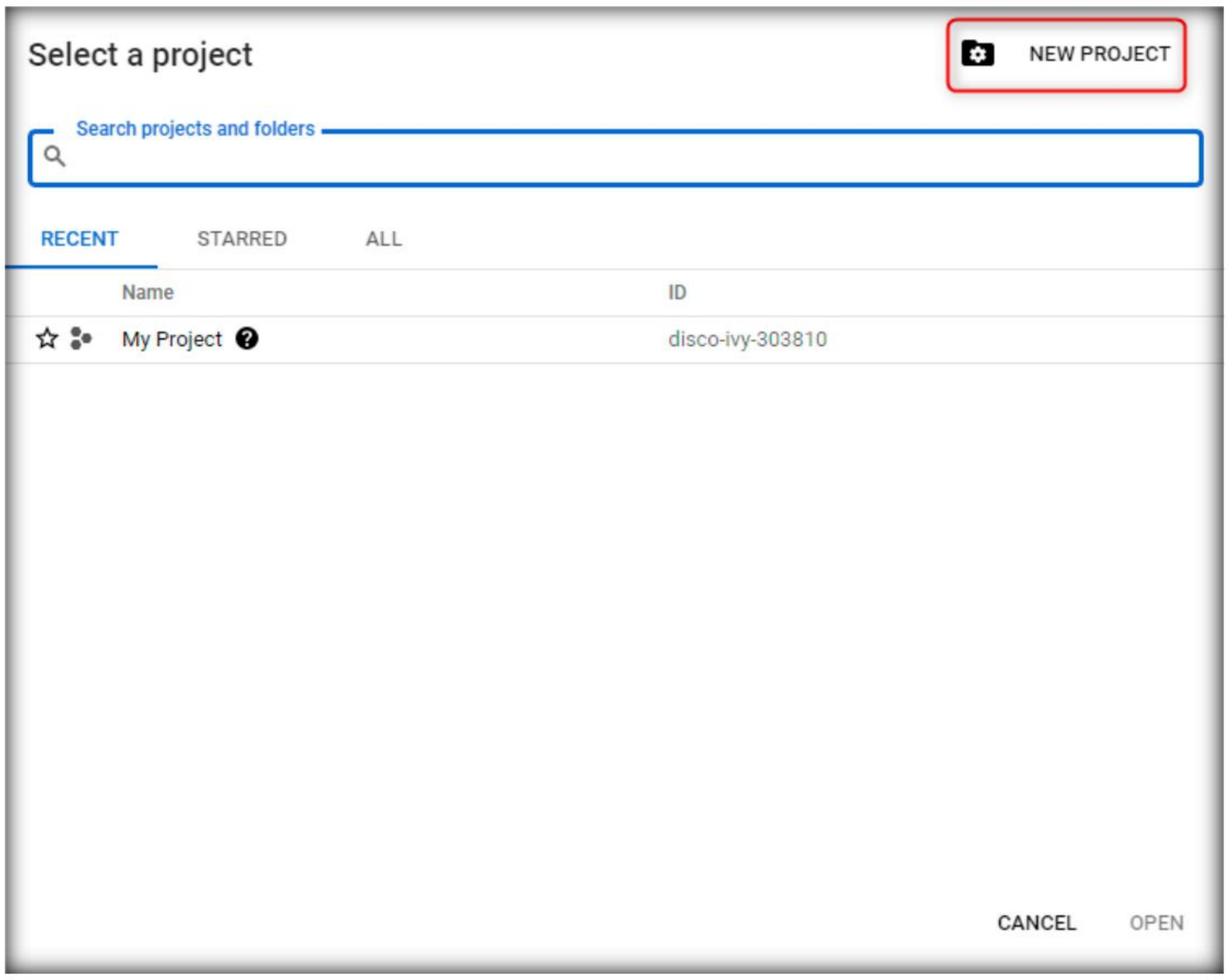


FIGURE 2.8.11: Creating New Project

13. The **New project** window opens. Type the **Name** of the project as **My First Project** and click on **CREATE**, as shown in the screenshot below.

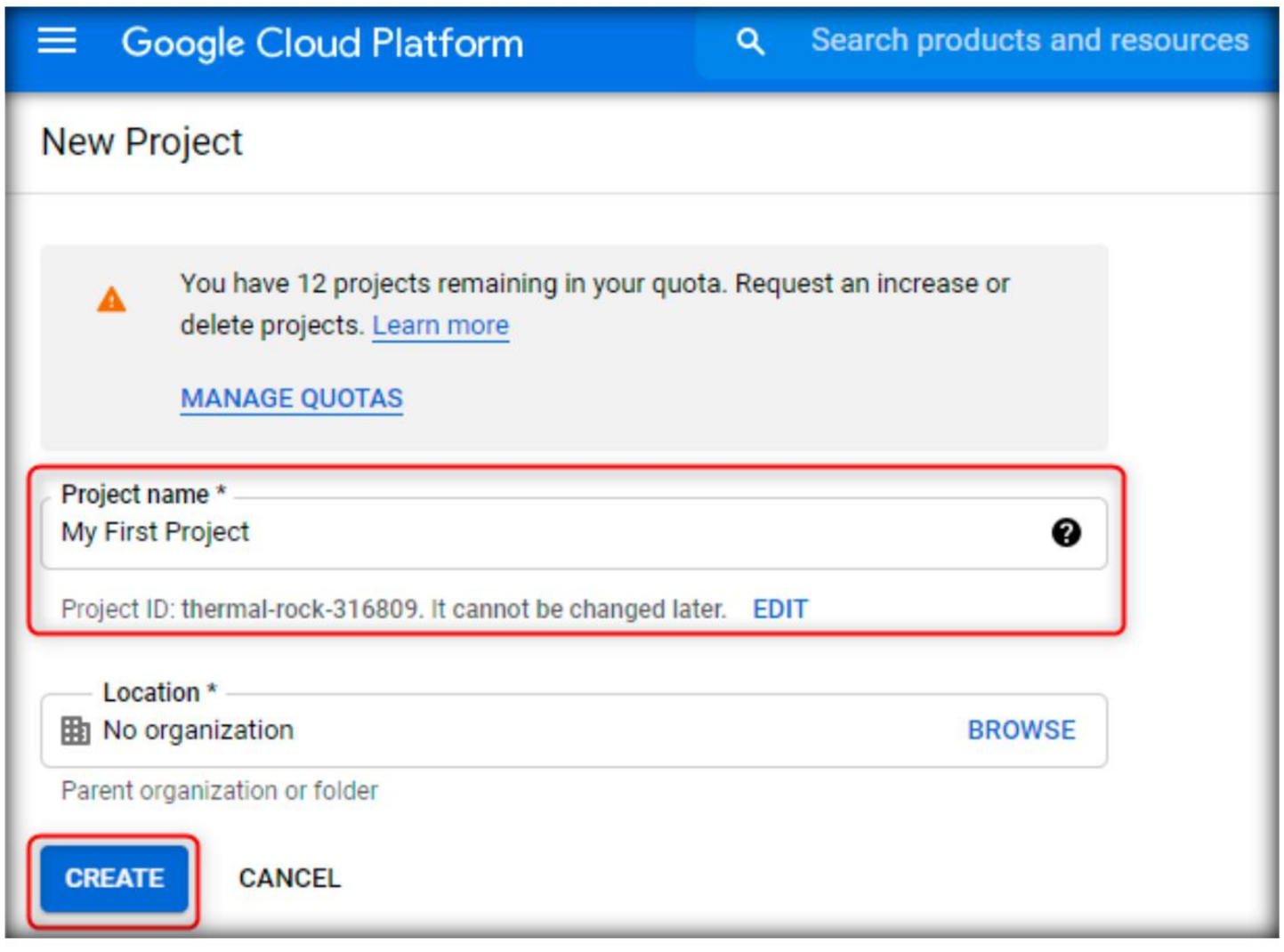


FIGURE 2.8.12: Creating My First Project

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

14. A new **My First Project** will be created. To select **My First Project** as the default project, click on the project dropdown at the top left corner.

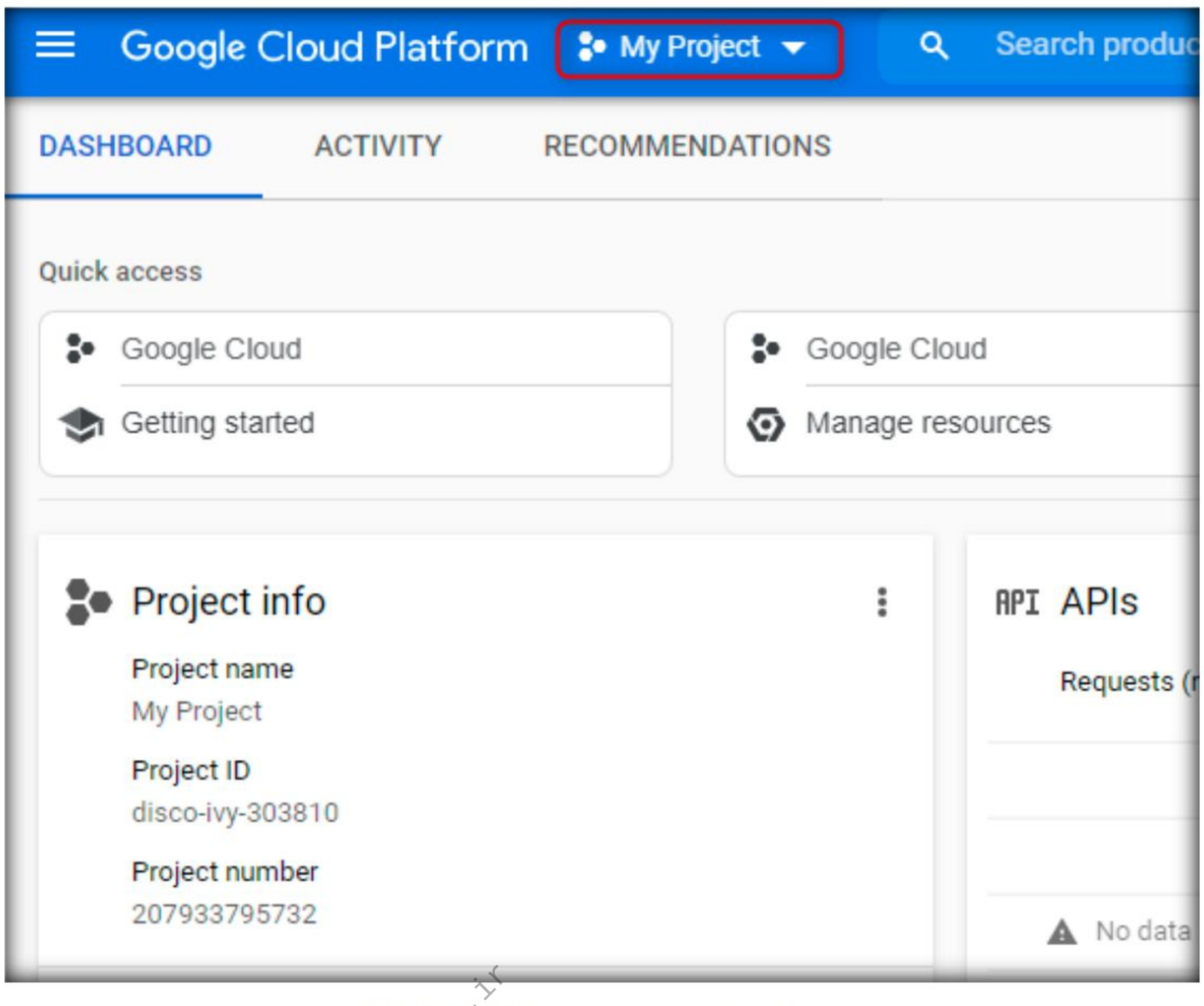


FIGURE 2.8.13: Selecting Project Dropdown

15. Select **My First Project** from the list of projects.

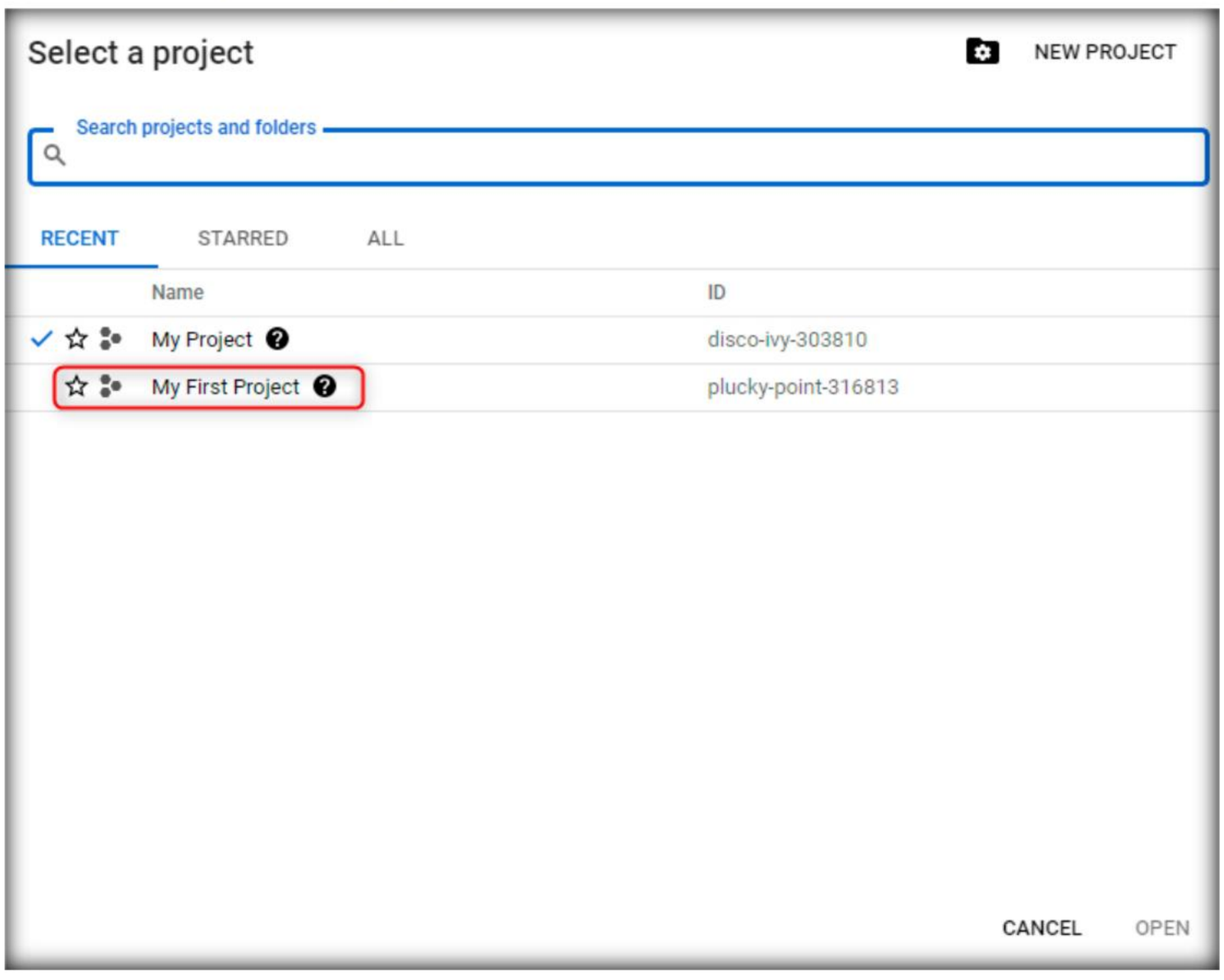


FIGURE 2.8.14: Selecting My First Project

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

16. **My First Project** will get selected as the default project.

TASK 2

Creating an Instance in GCP

17. Now, navigate to **Compute Engine** and select **VM Instances** in the console.

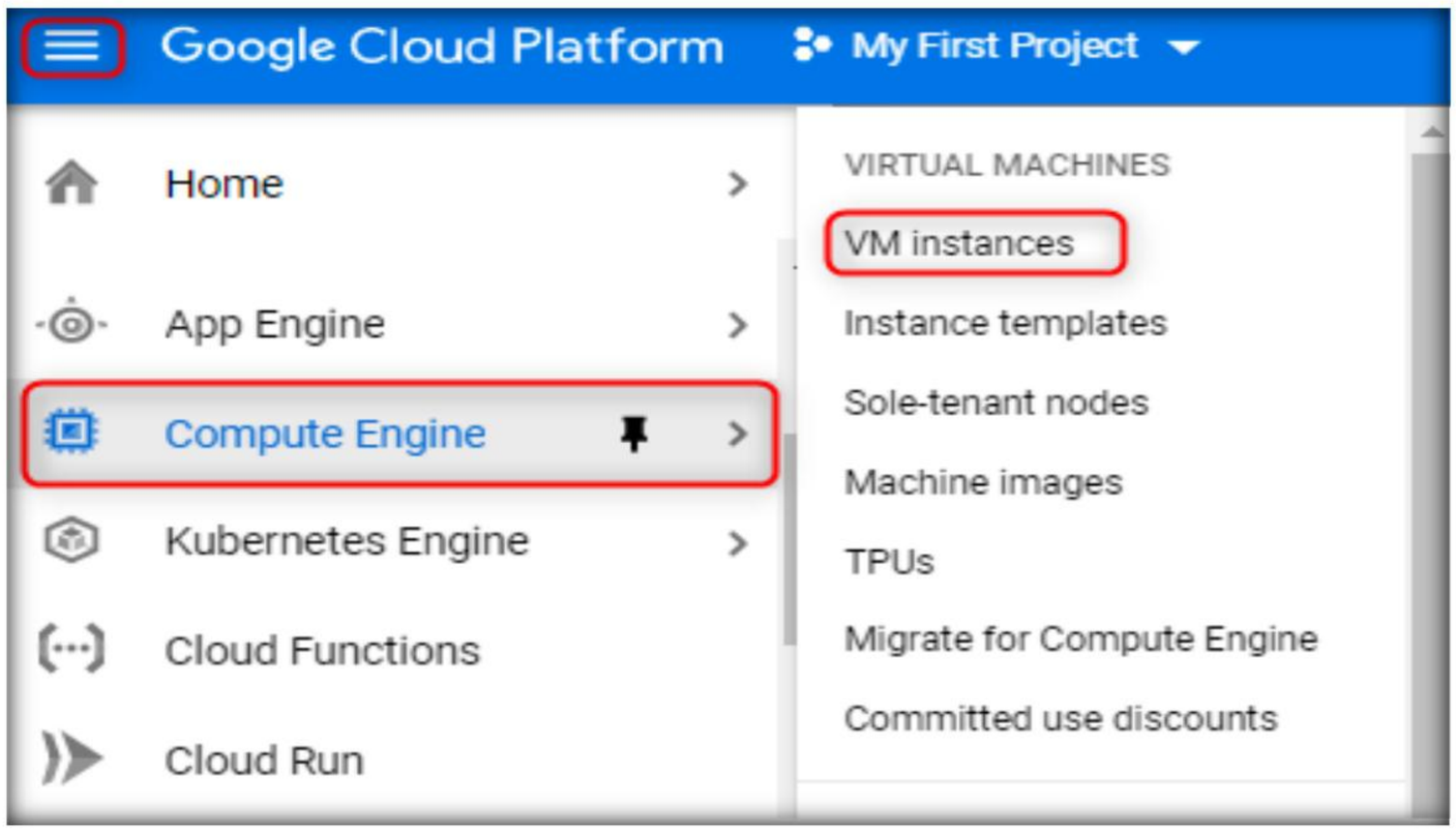


FIGURE 2.8.15: Navigating to Compute Engine and selecting VM Instances

18. Next, click on **Create Instance** to create a new instance.

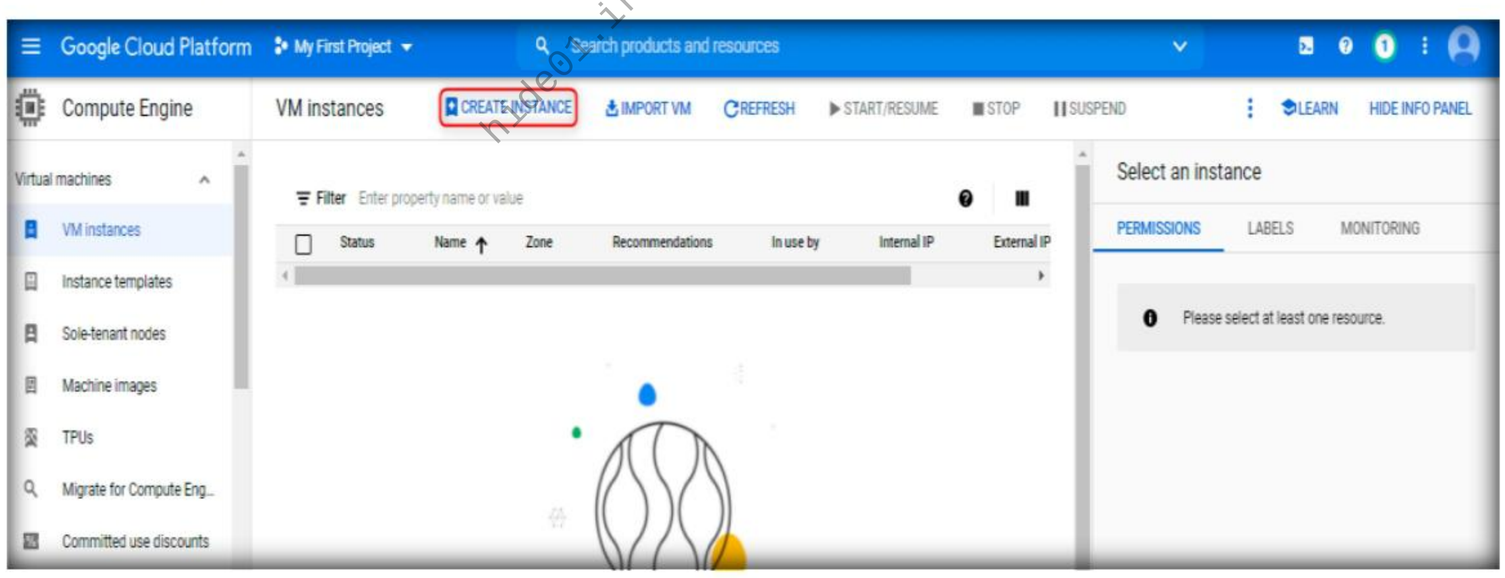


FIGURE 2.8.16: Creating Instance

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

19. In the **Create an instance** window, give an appropriate **Name**, **Region**, and **Zone** to the instance. In this lab, we have used the following details:

    Name: usinstance-1

    Region: us-east1

    Zone: us-east1-b

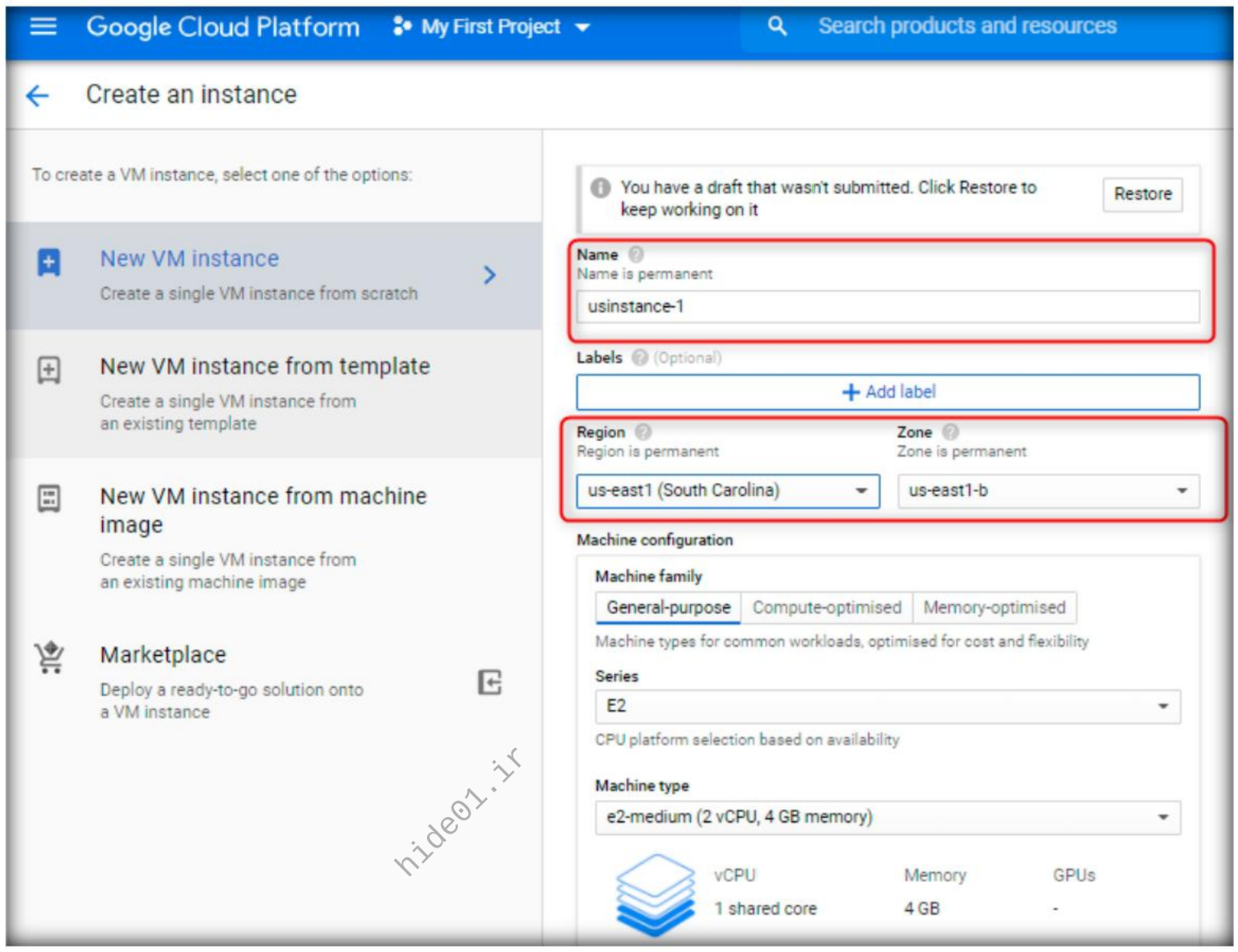


FIGURE 2.8.17: Entering the Name and Selecting the Zone and Region

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

20. Ensure the **Boot Disk** is **Debian GNU/Linux 10 (buster)**. Retain the other settings and click on **Create**.

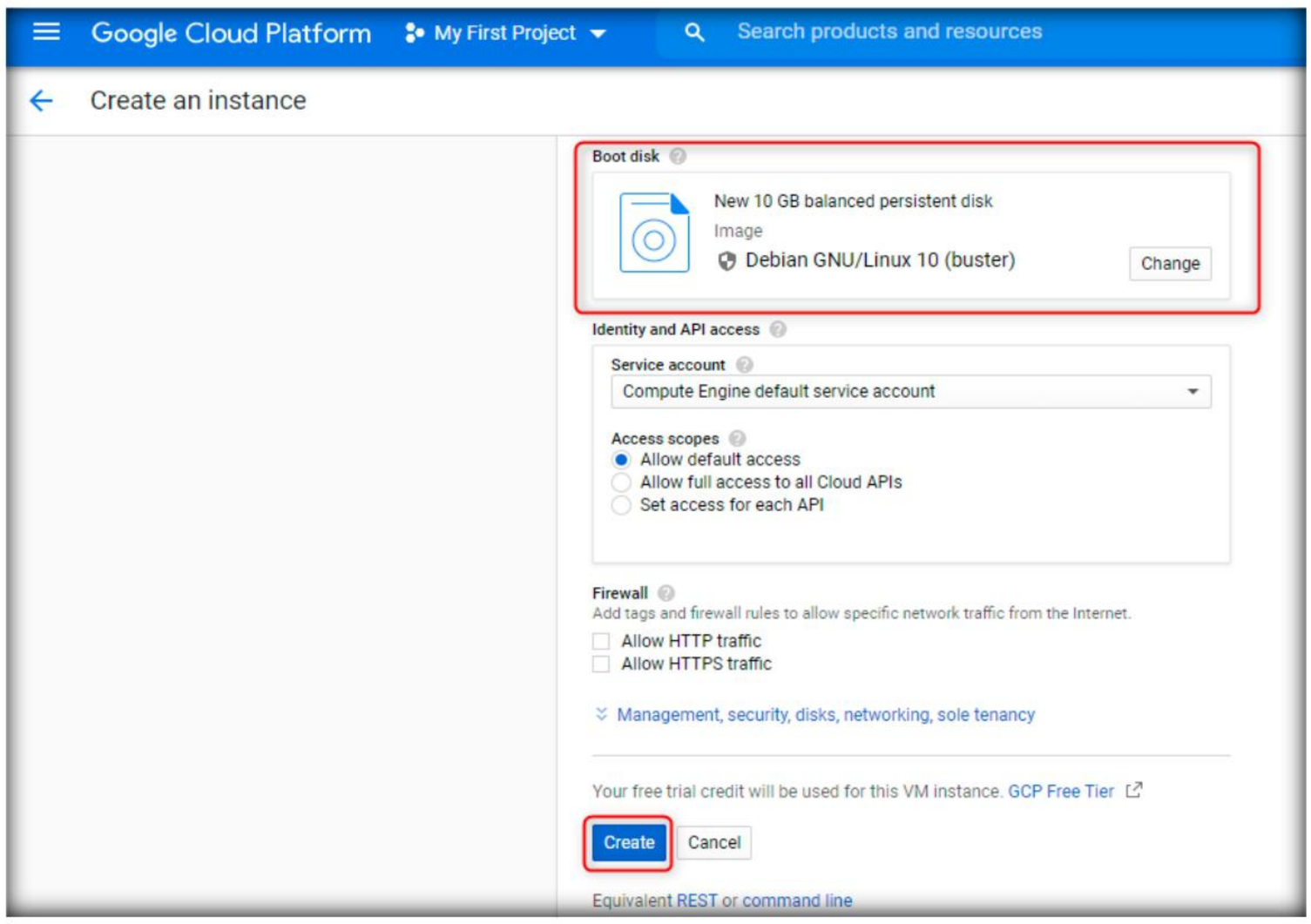


FIGURE 2.8.18: Creating Instance

21. The tick mark under **Status** confirms that your instance is created.

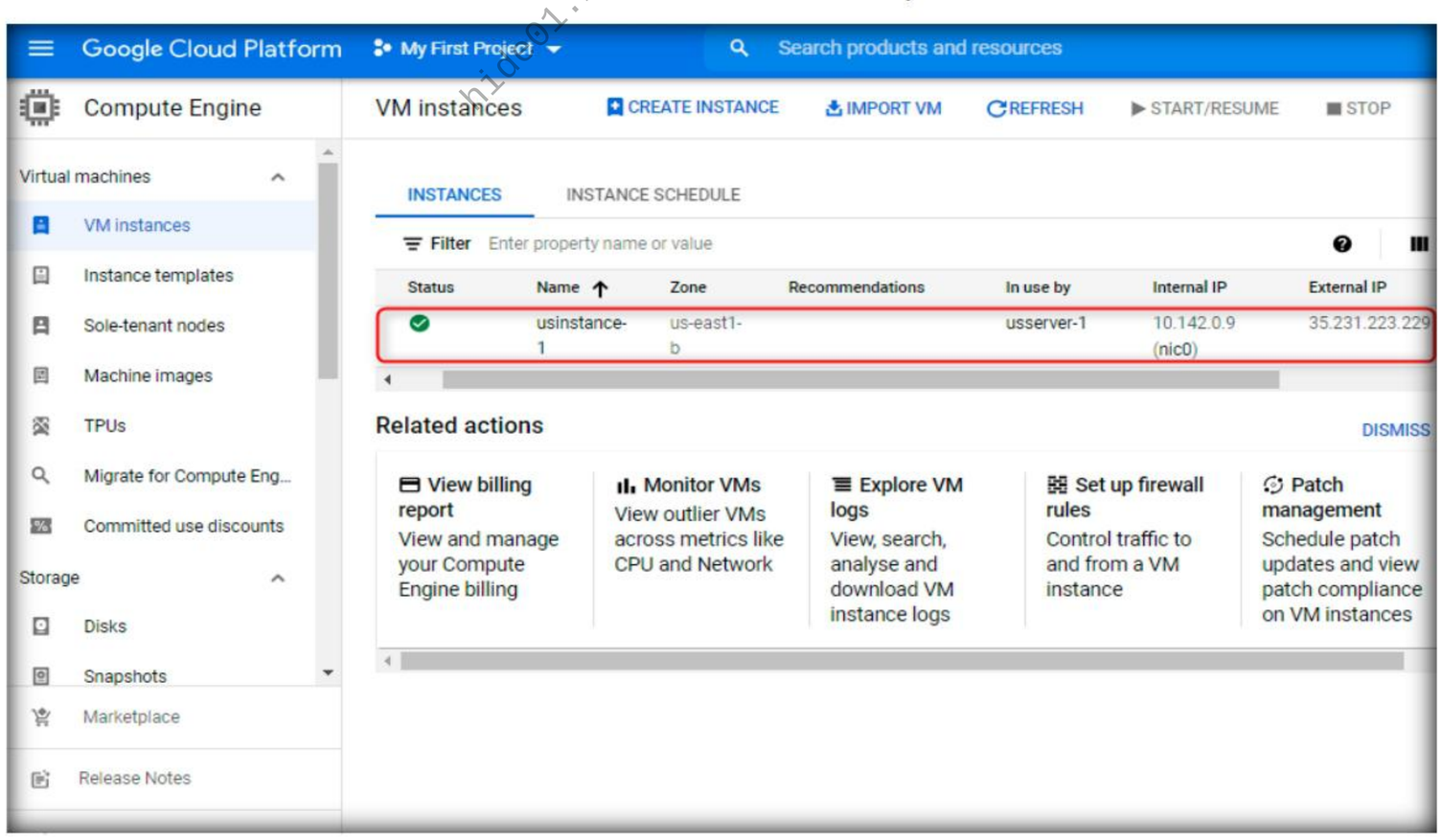


FIGURE 2.8.19: Status of the Instance as created

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 3

Creating Firewall Rules in GCP

22. Navigate to **VPC network** and select **Firewall** in the console.

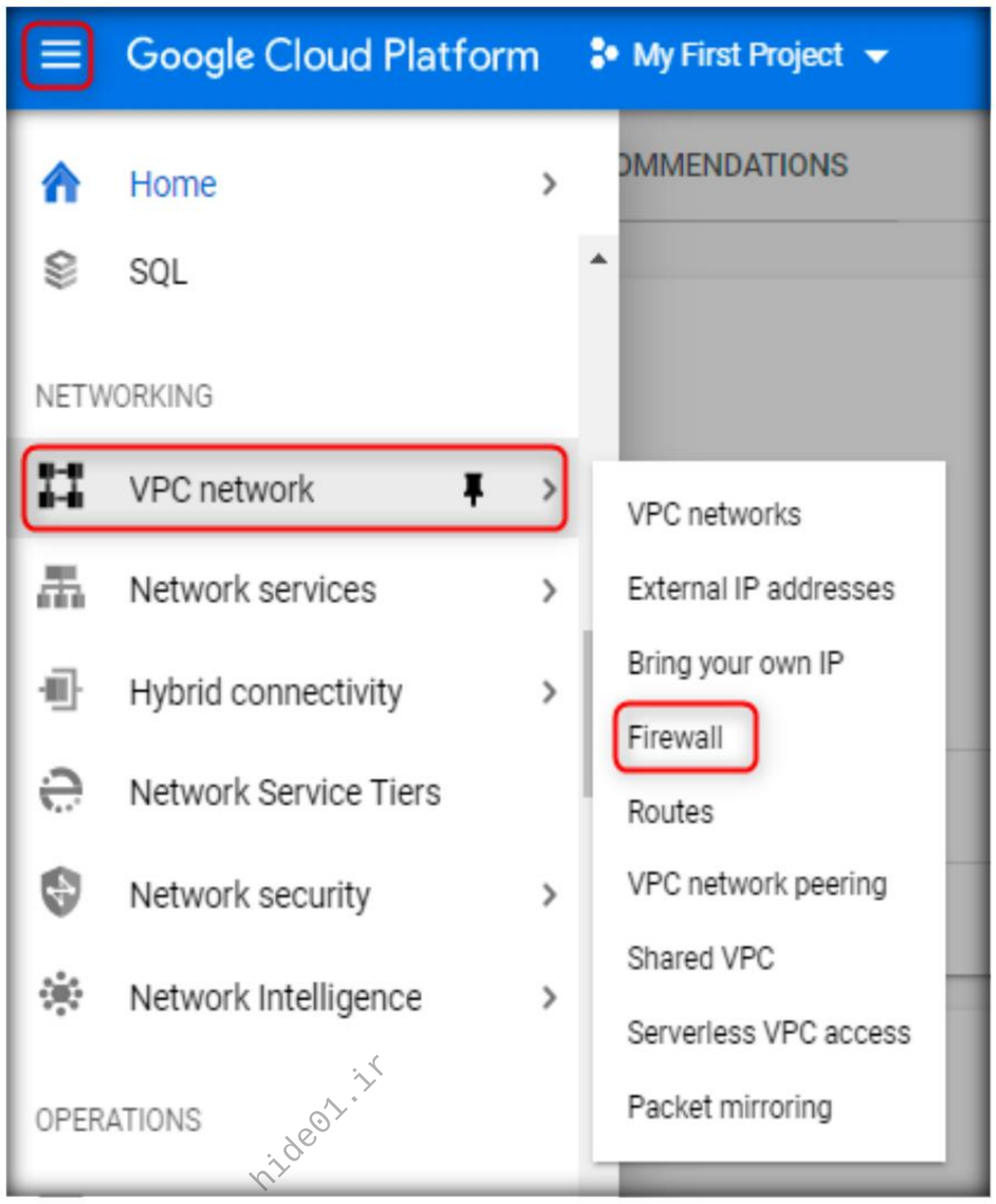


FIGURE 2.8.20: Navigating to VPC Firewall in console

23. Next, in the **Firewall** dashboard that appears, click on **CREATE FIREWALL RULE** at the top.

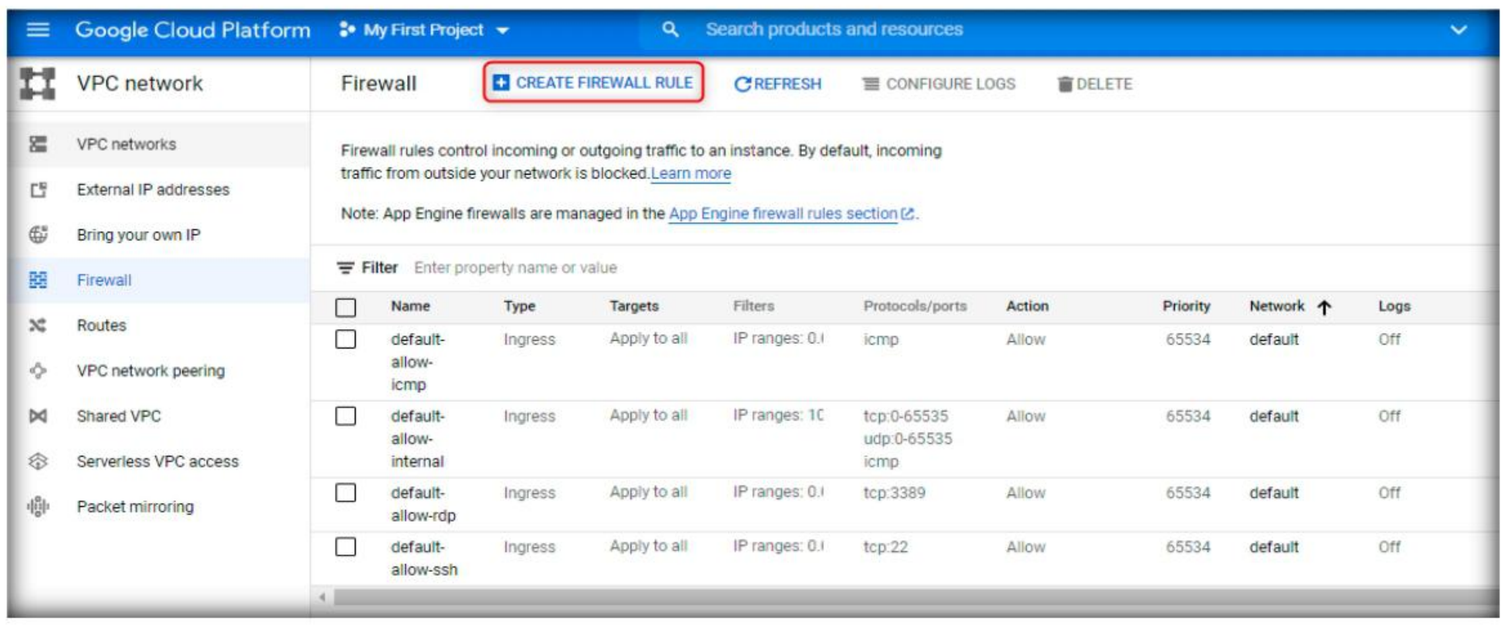


FIGURE 2.8.21: Creating the New Firewall Rule

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

24. Type an appropriate **Name** for the firewall rule here. We are creating a firewall rule named **block-ping-rule** as it will block ping requests to the VM instance.

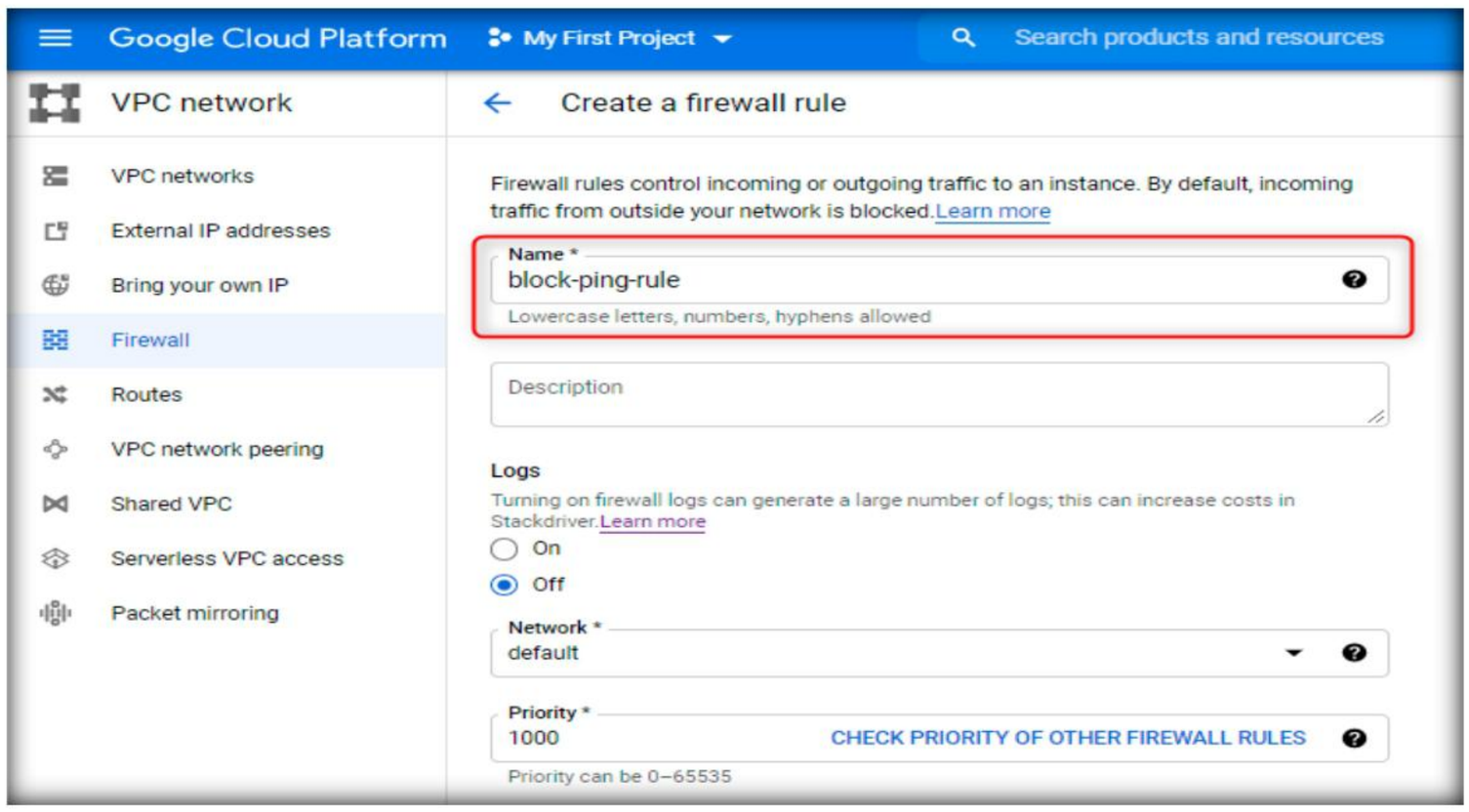


FIGURE 2.8.22: Naming the Firewall Rule

25. Retain the default settings for **Logs**, **Network,** and **Priority**.
26. Now, scroll down to the bottom and add the following details:

    Direction of Traffic: **Ingress** (as it is a firewall rule to block ping requests)

    Action on match: **Deny** (To deny ping requests)

    Targets: Specified target tags

    Target tags: **block-ping**

    Source IP ranges: **0.0.0.0/0** (to block all IPv4 traffic)

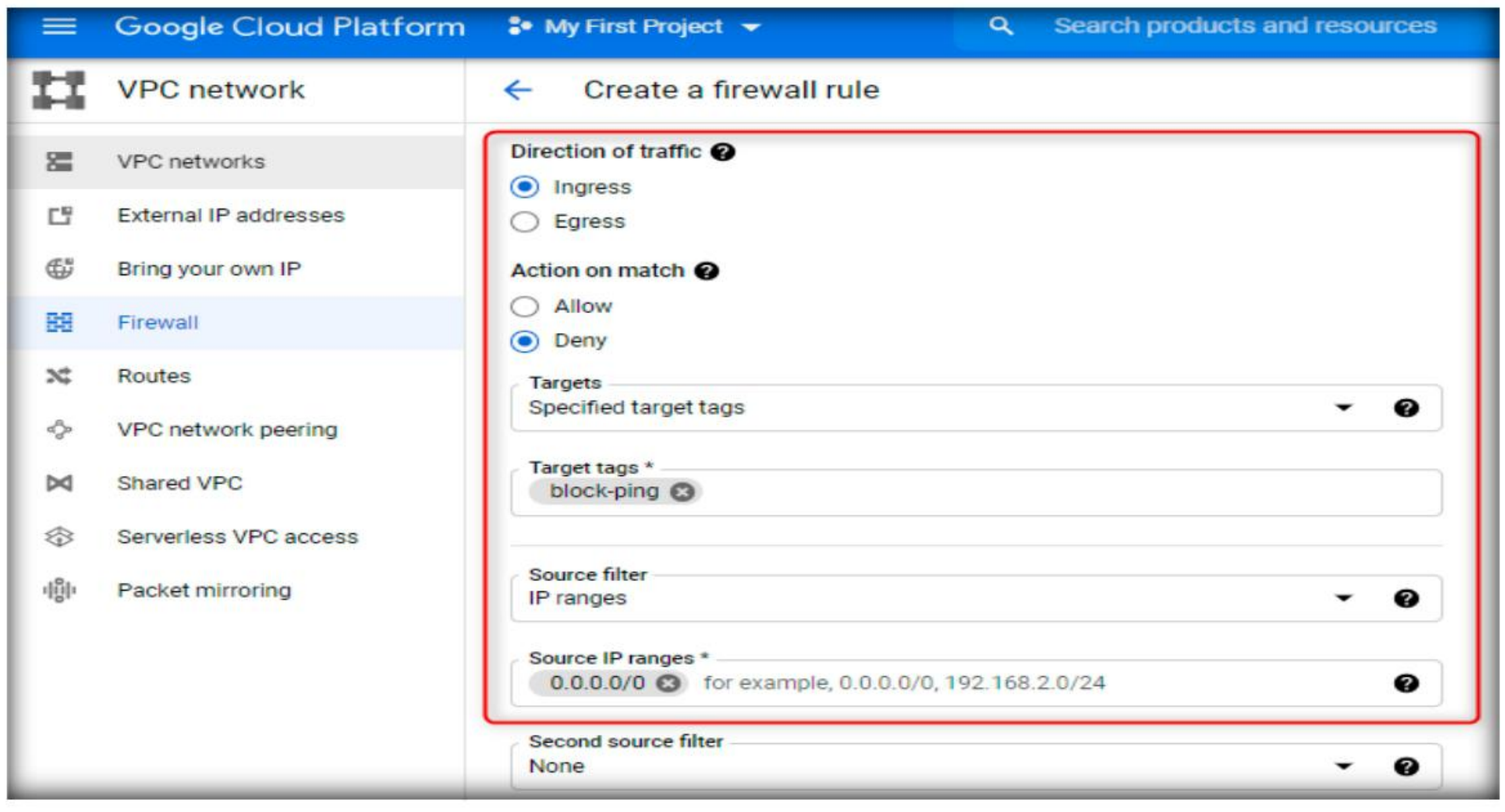


FIGURE 2.8.23: Specifying the firewall rules

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

27. Under **Protocols and ports**, select **Specified protocols and ports**. Then, select **Other protocols** and add **icmp**. Then, click on **CREATE**.

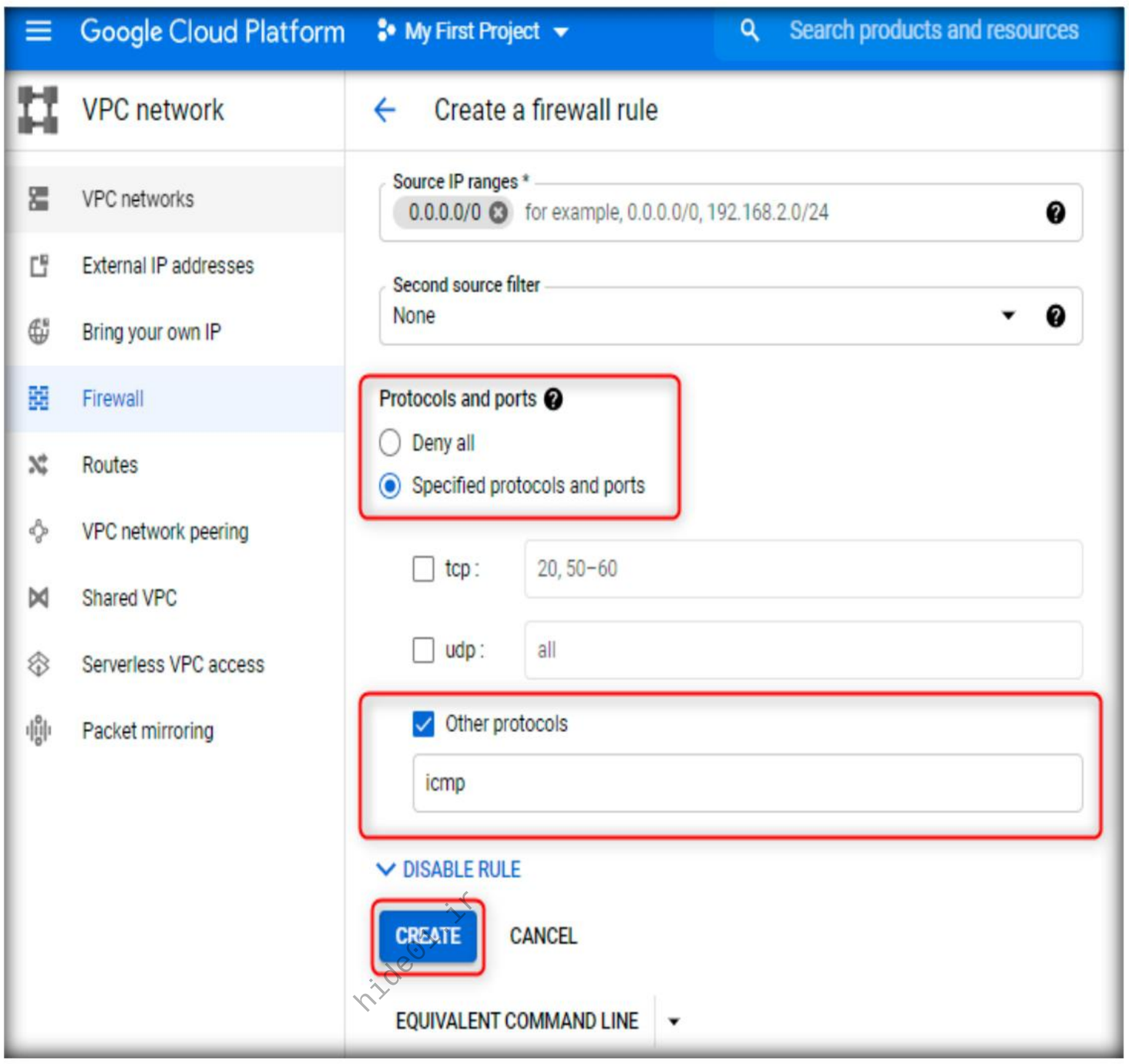


FIGURE 2.8.24: Specifying the Protocols and Creating the Firewall Rule

28. The firewall rule is successfully created.

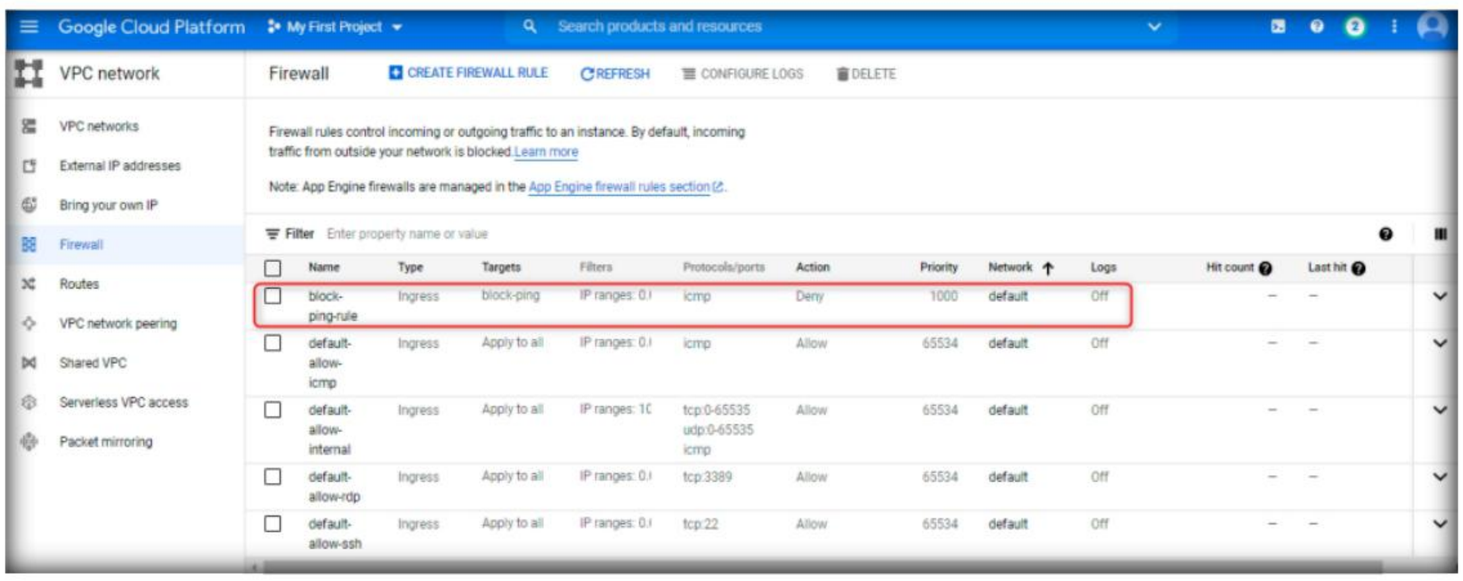


FIGURE 2.8.25: Created the Firewall Rule

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 4

Assigning the Firewall Rule to the VM Instance

29. Next, assign the newly created firewall rule to the VM instance that was created in Task 1 by navigating to **Compute Engine** and selecting **VM instances** from the console.

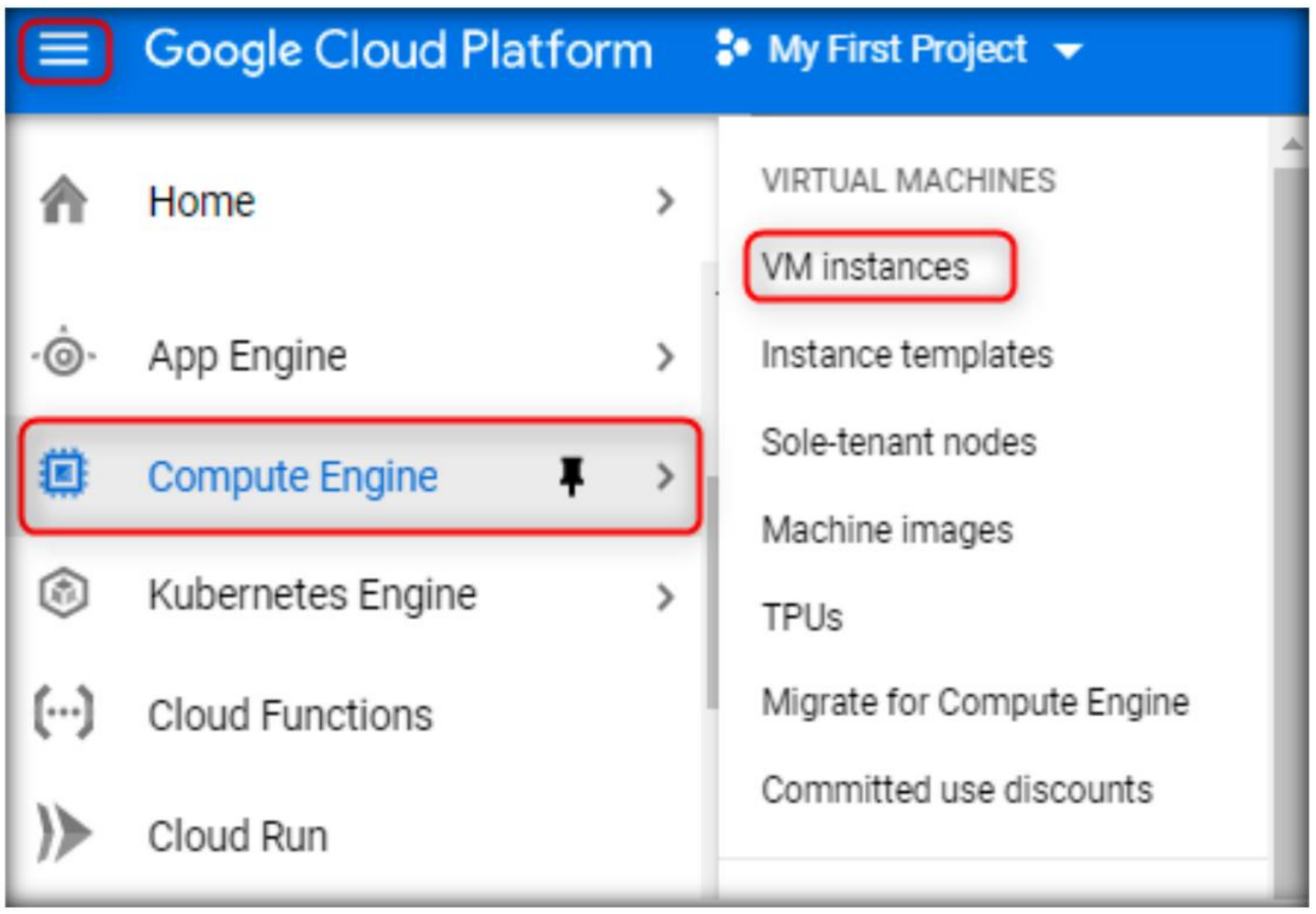


FIGURE 2.8.26: Navigating to Compute Engine and Selecting VM Instances

30. Click on the instance you created.

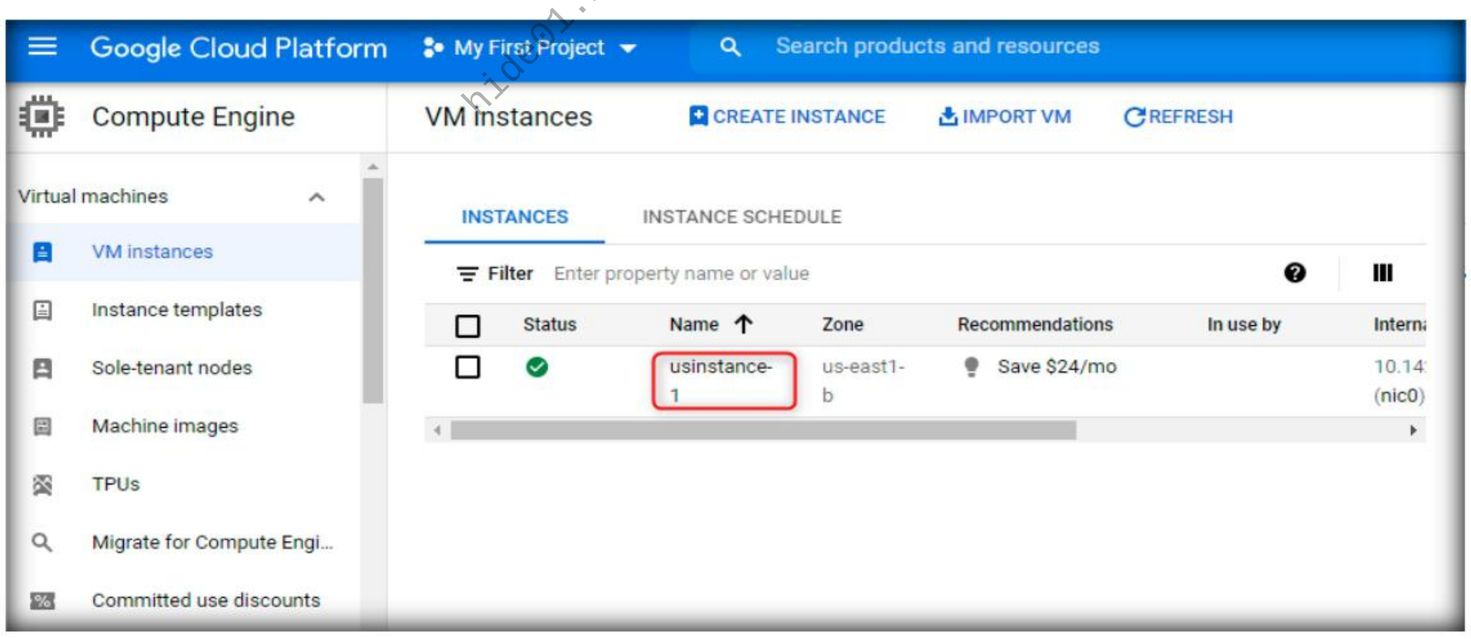


FIGURE 2.8.27: Copying Bucket ARN

31. Scroll down and note the **External IP** of the instance.

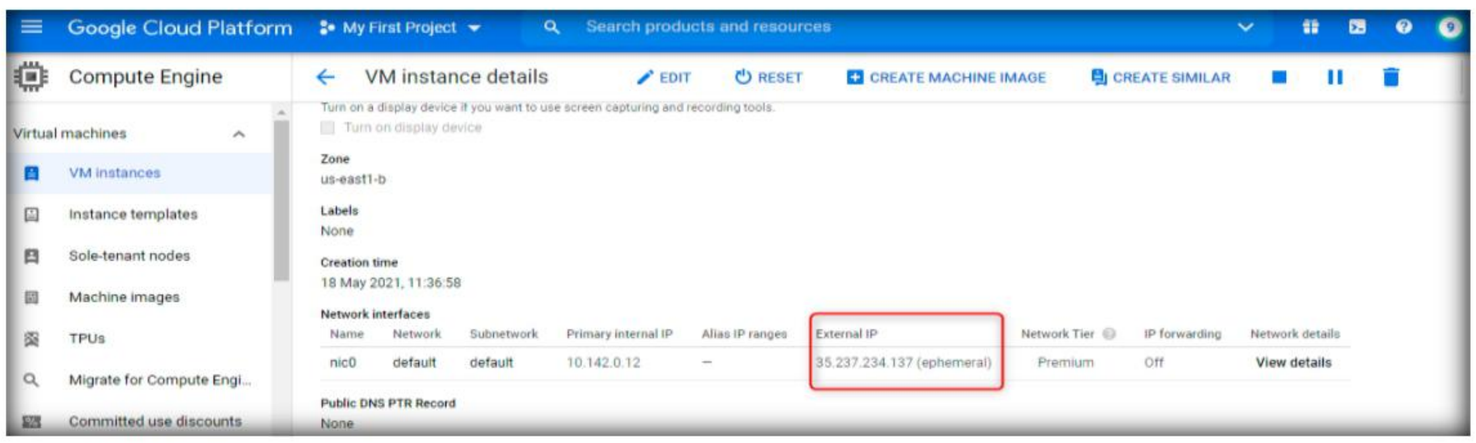


FIGURE 2.8.28: External IP of the Instance

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

32. Now, in the Admin Machine VM, search for **cmd** at the bottom and click on **Open** at the right side.

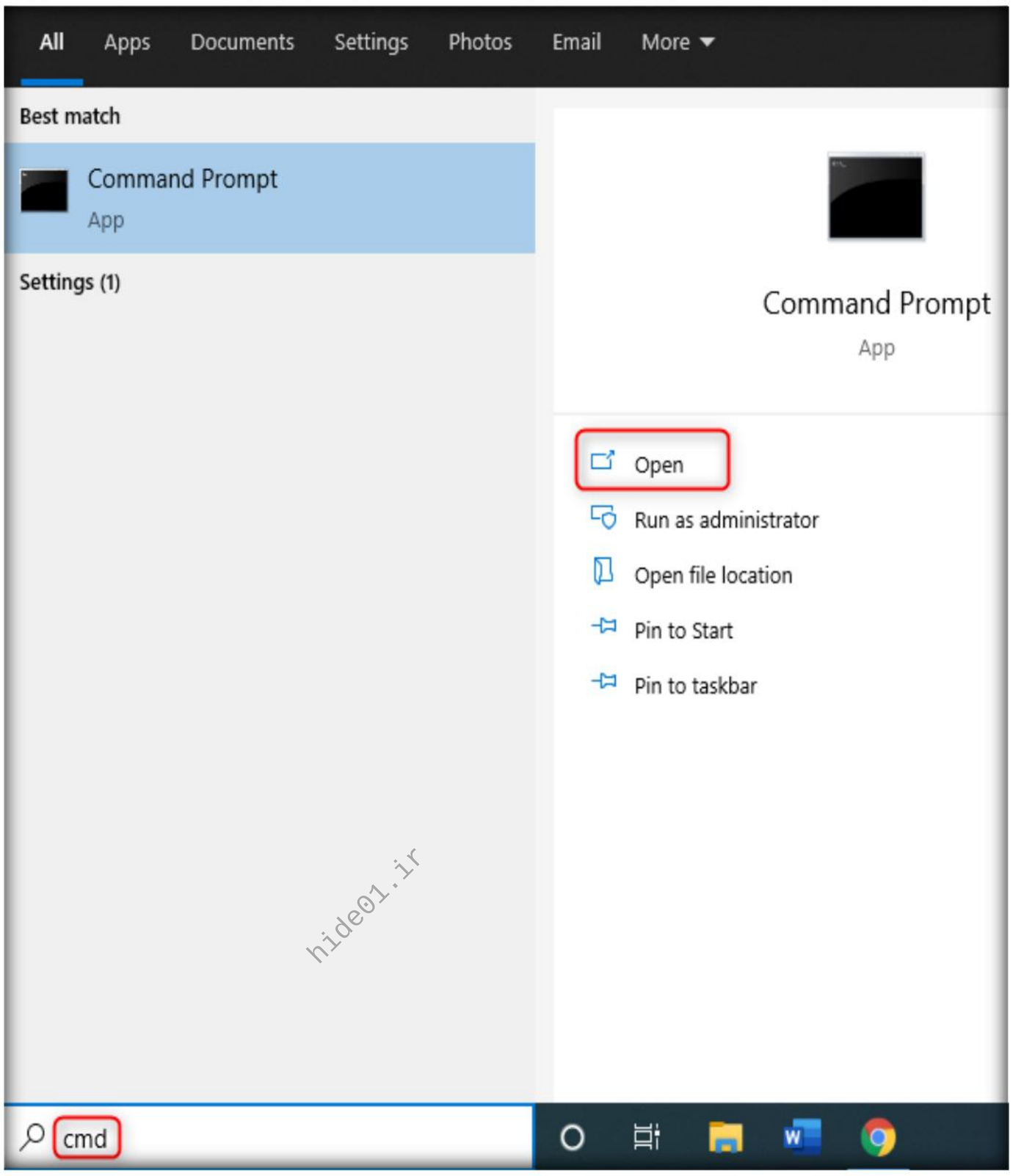


FIGURE 2.8.29: Navigating to Command Prompt

33. In the **Command Prompt** window, type **ping <external IP address>** (replace <external IP address> with the external IP of your VM instance, as in the previous step). For this lab, ping 35.237.234.137 and press **Enter** on the keyboard.

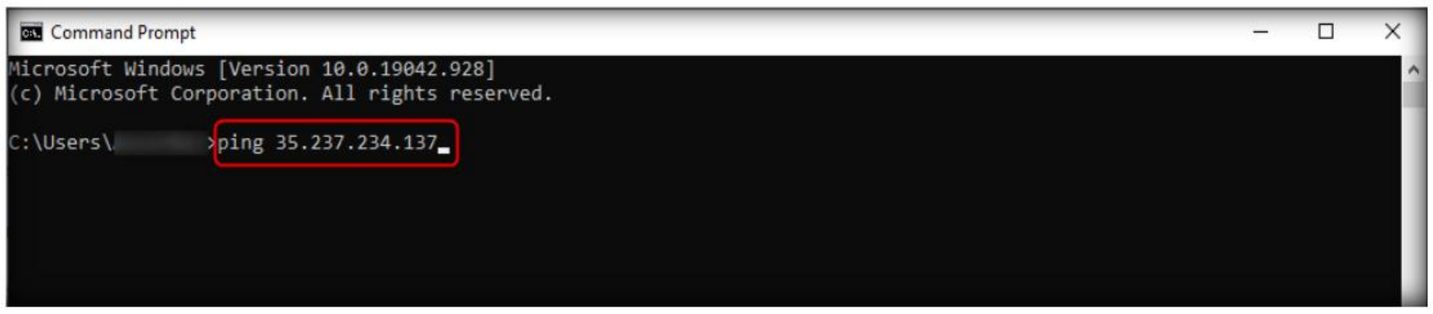


FIGURE 2.8.30: Command Prompt window

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

34. The ping to the VM instance is successful, as shown in the following screenshot.

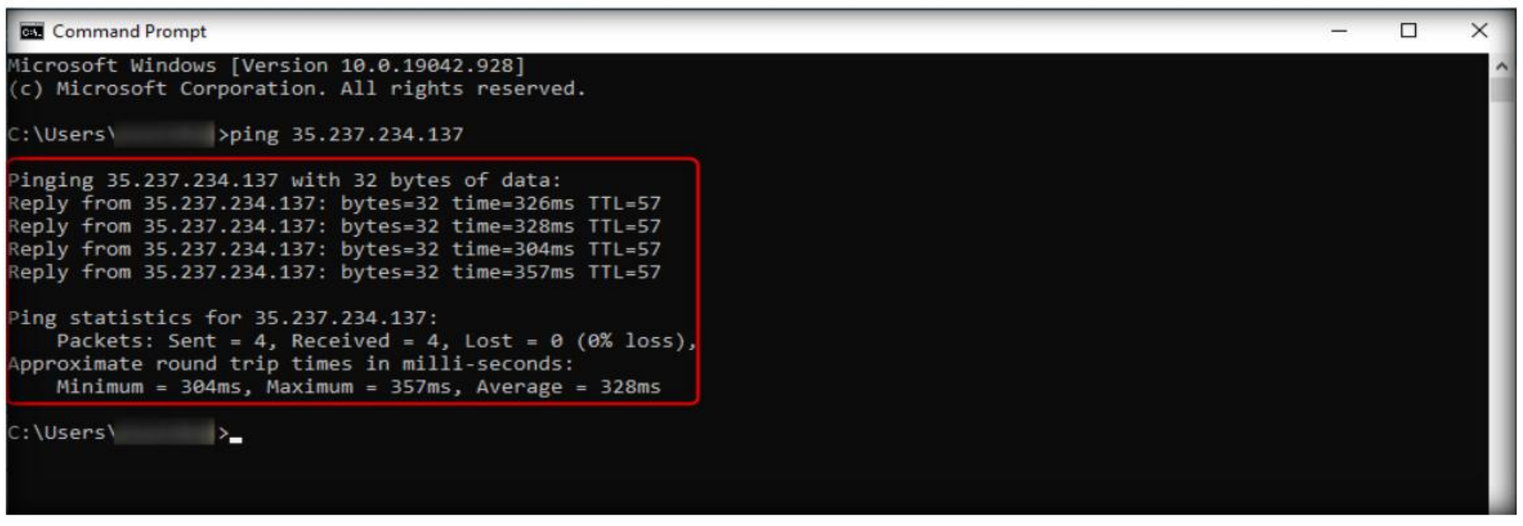


FIGURE 2.8.31: Successful ping

35. Next, go back to the GCP **VM Instances** console and click on **usinstance-1**.

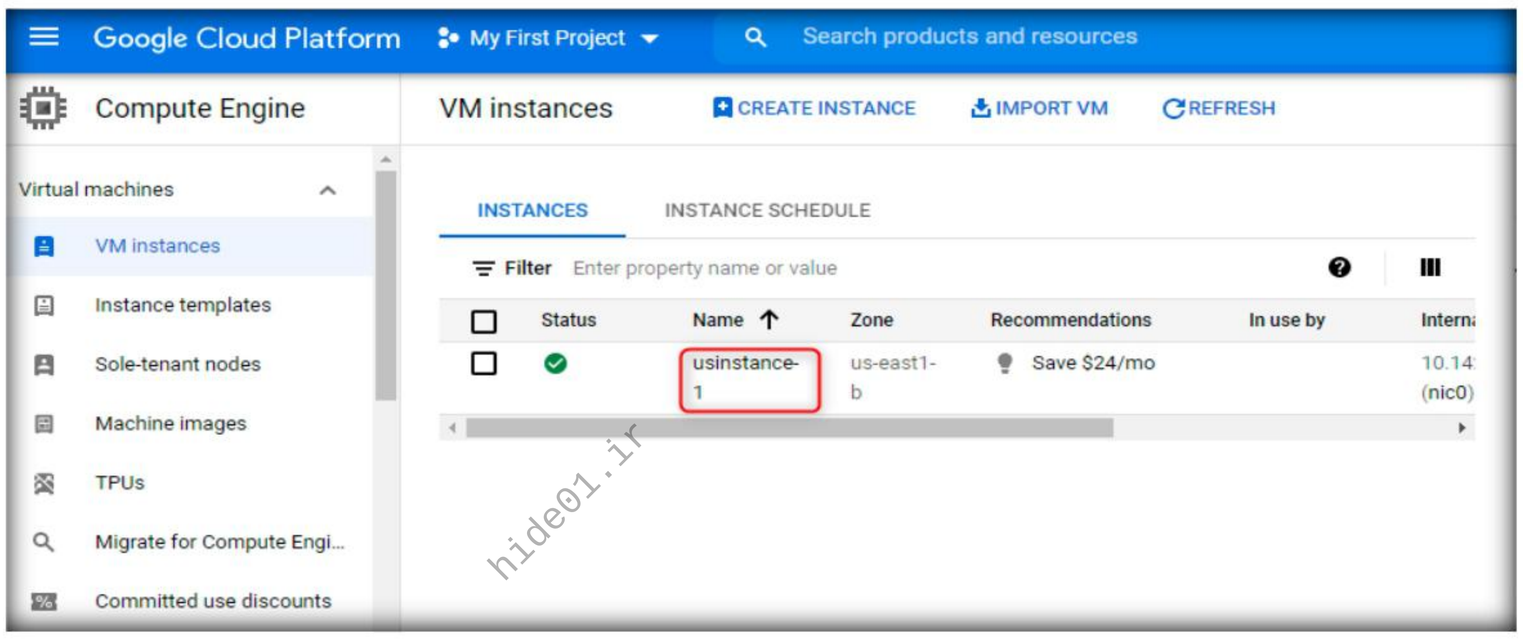


FIGURE 2.8.32: VM Instance window

36. Click on **EDIT** at the top.

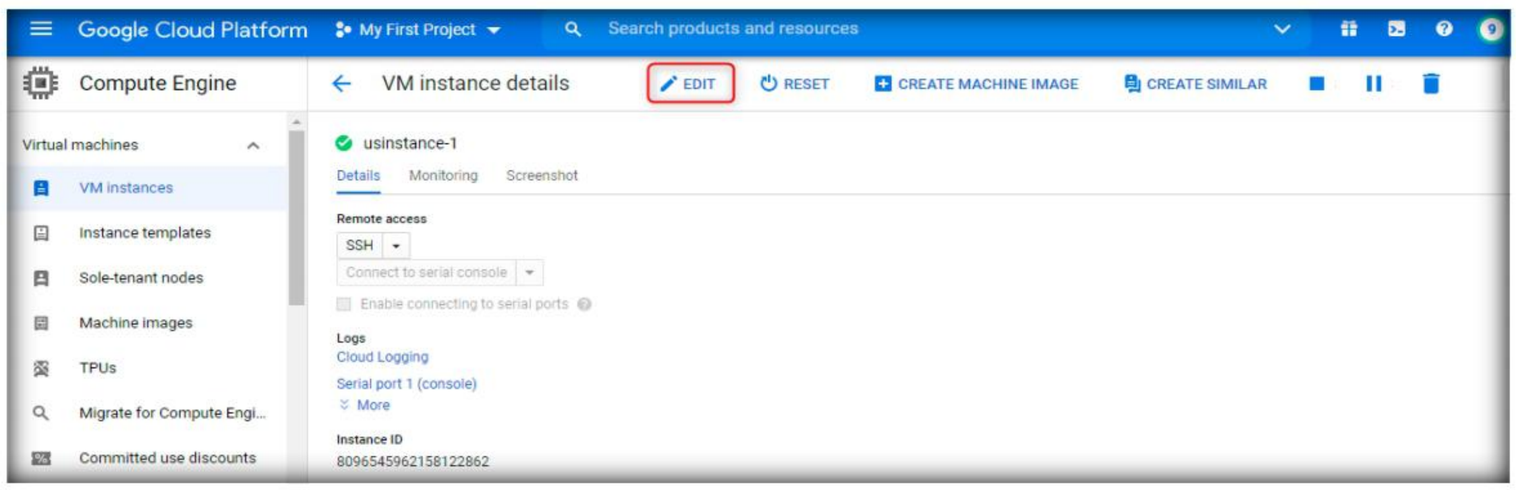


FIGURE 2.8.33: Editing the VM Instance

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

37. In the **EDIT** window, scroll down to the bottom. Under **Network tags,** add the **block-ping** network tag.

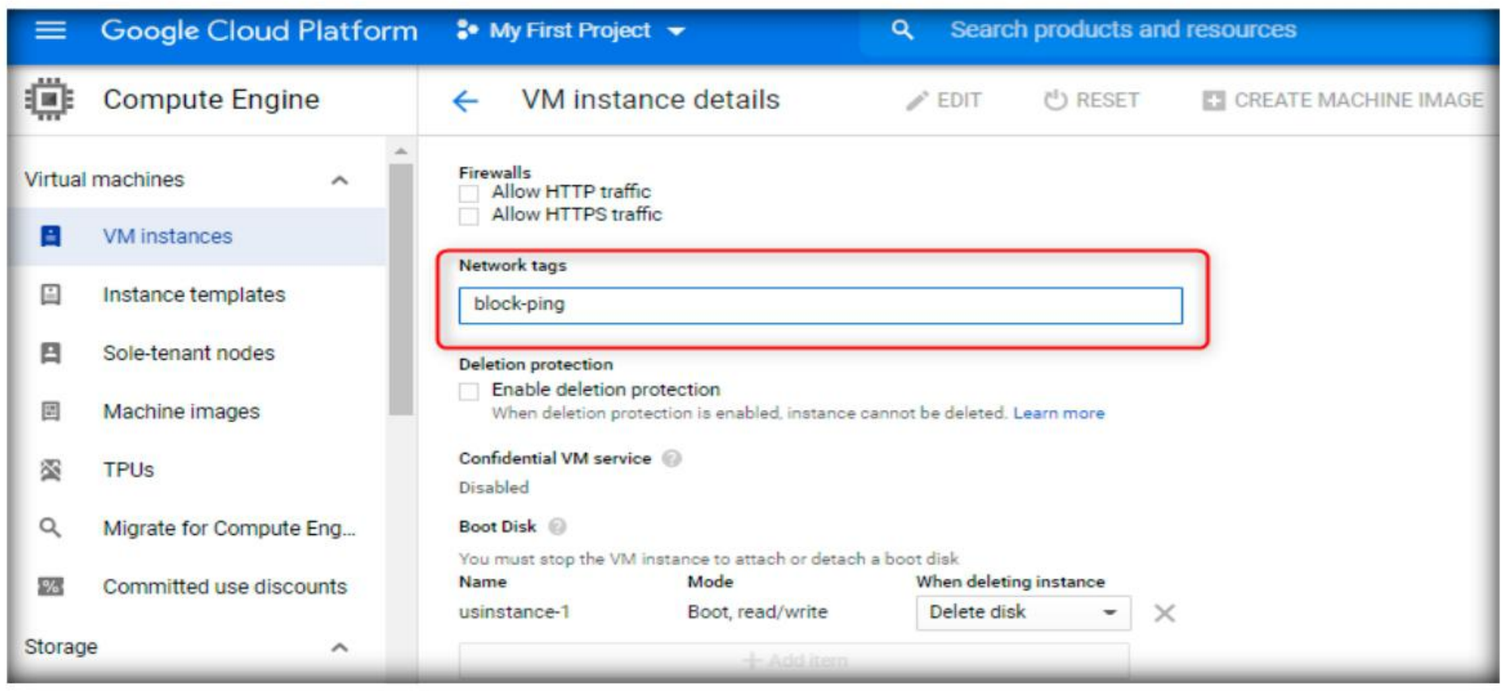


FIGURE 2.8.34: Adding Network Tags

38. Scroll down to the bottom and click on **Save**.

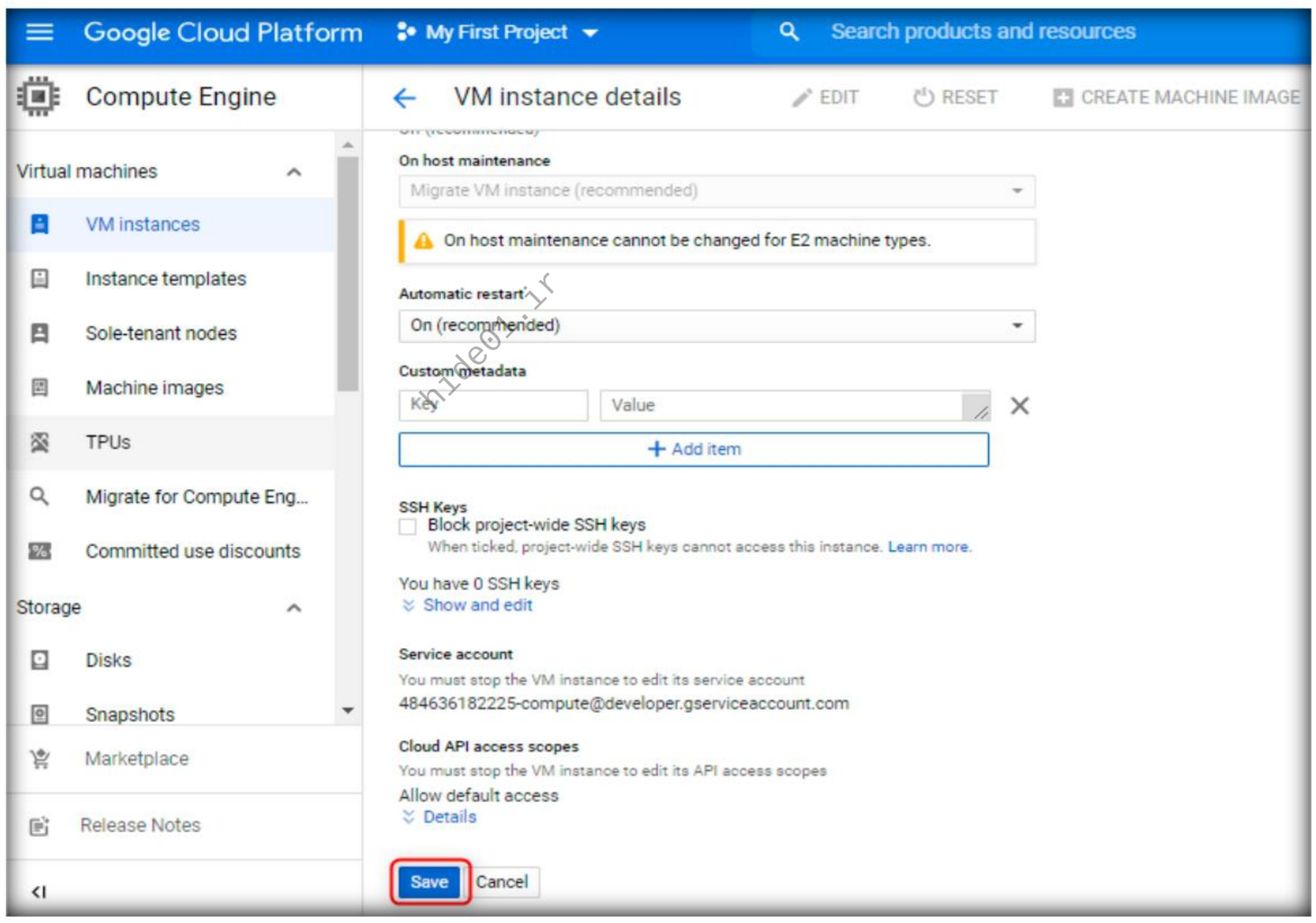


FIGURE 2.8.35: Saving the Changes

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

39. Now, go back to **Command Prompt** and run a continuous ping with the command, **ping <external IP address> -t** (Replace <external IP address with the external IP of your VM instance). For this lab, **ping 35.237.234.137 -t**, and then press **Enter** on the keyboard.

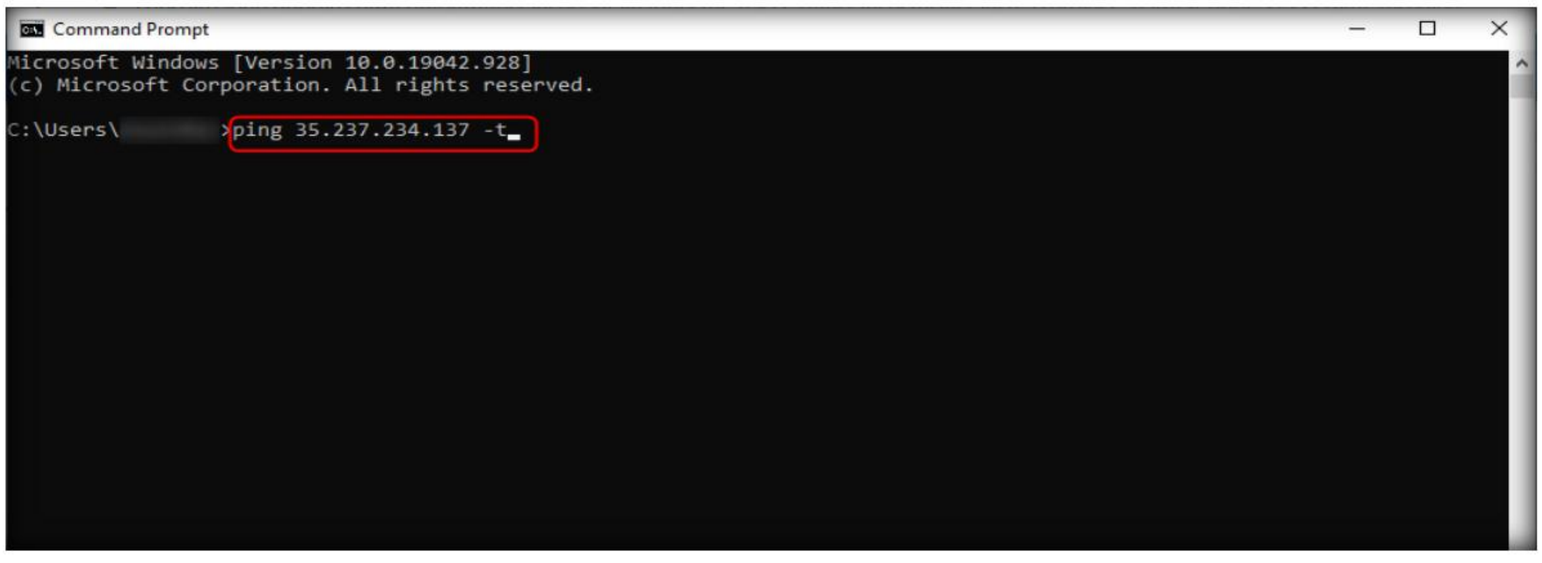


FIGURE 2.8.36: Run continuous ping request

40. The **ping** request to the VM Instance is blocked by the firewall rule.

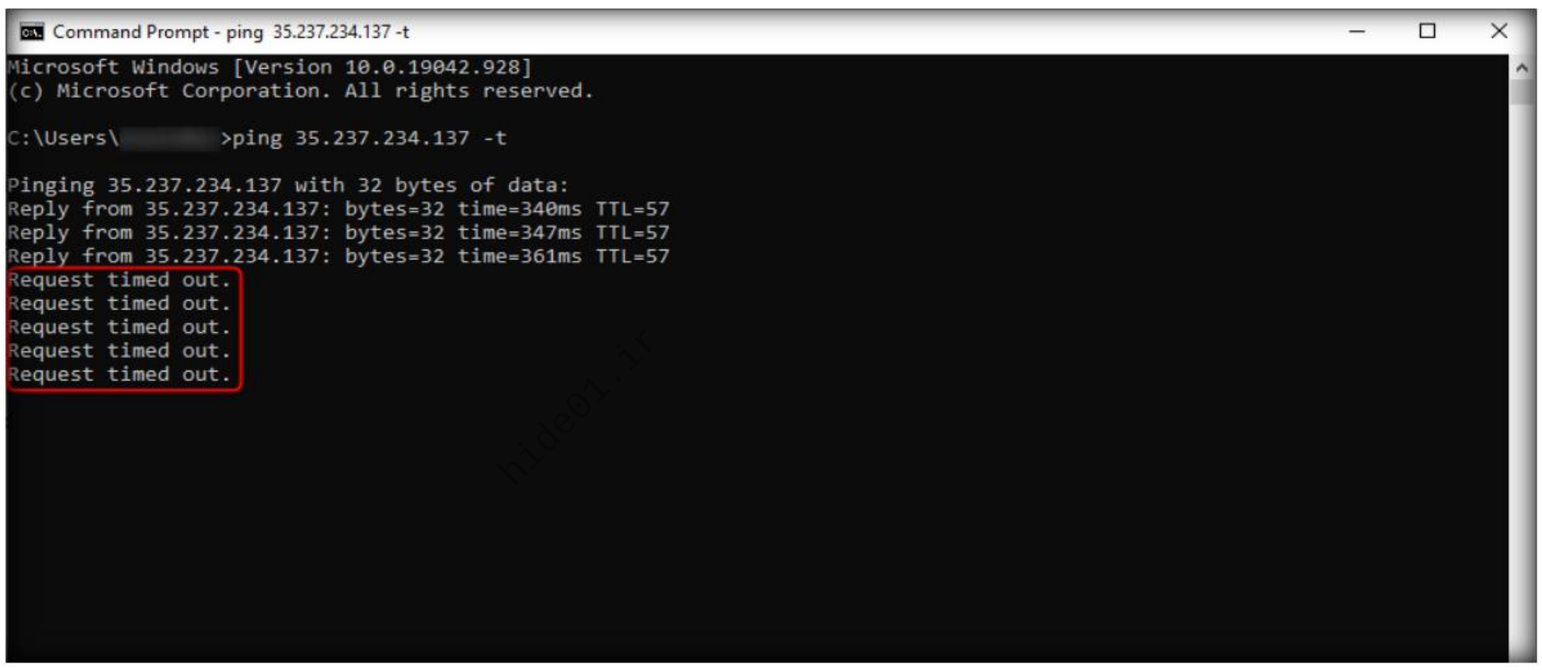


FIGURE 2.8.37: Ping Request is blocked

41. As explained above, a cloud security engineer can secure VM instances from attacks using VPC firewall rules.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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

42. Now, to delete the instance that you have created, navigate to Compute Engine **VM instances** window. Scroll horizontally in the **Instances** tab. Click on the ellipsis, for instance (**usintance-1**) that you have created and click on **Delete**. In the pop-up window, click on **Delete**.

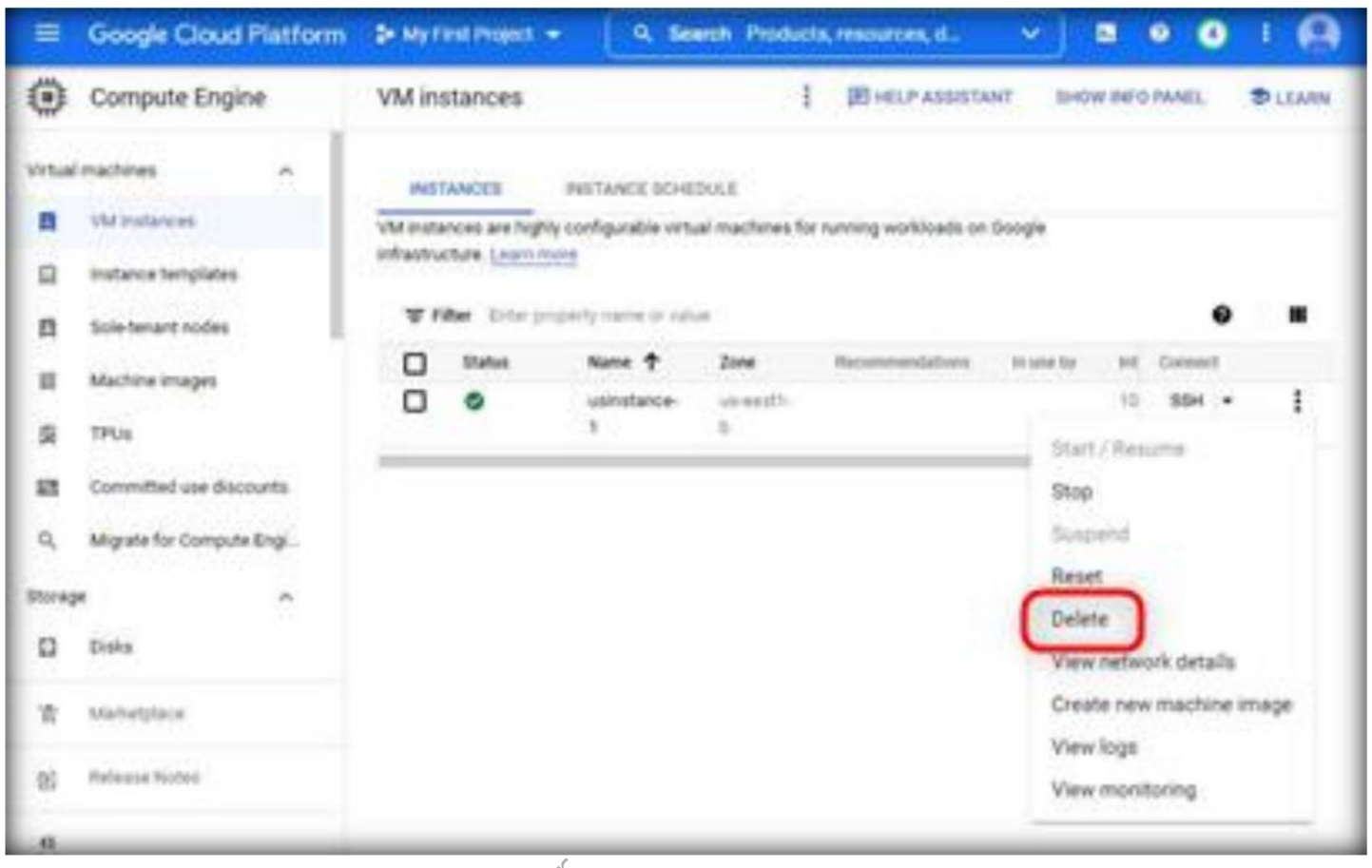


FIGURE 2.8.38: Deleting VM Instance

43. Next, delete the firewall rule you created for this lab. Navigate to the **Firewall** window in the **VPC network**. Select the checkbox for the firewall rule (**block-ping-rule**) that you have created and click on **Delete** at the top. In the pop-up window, click on **Delete**.

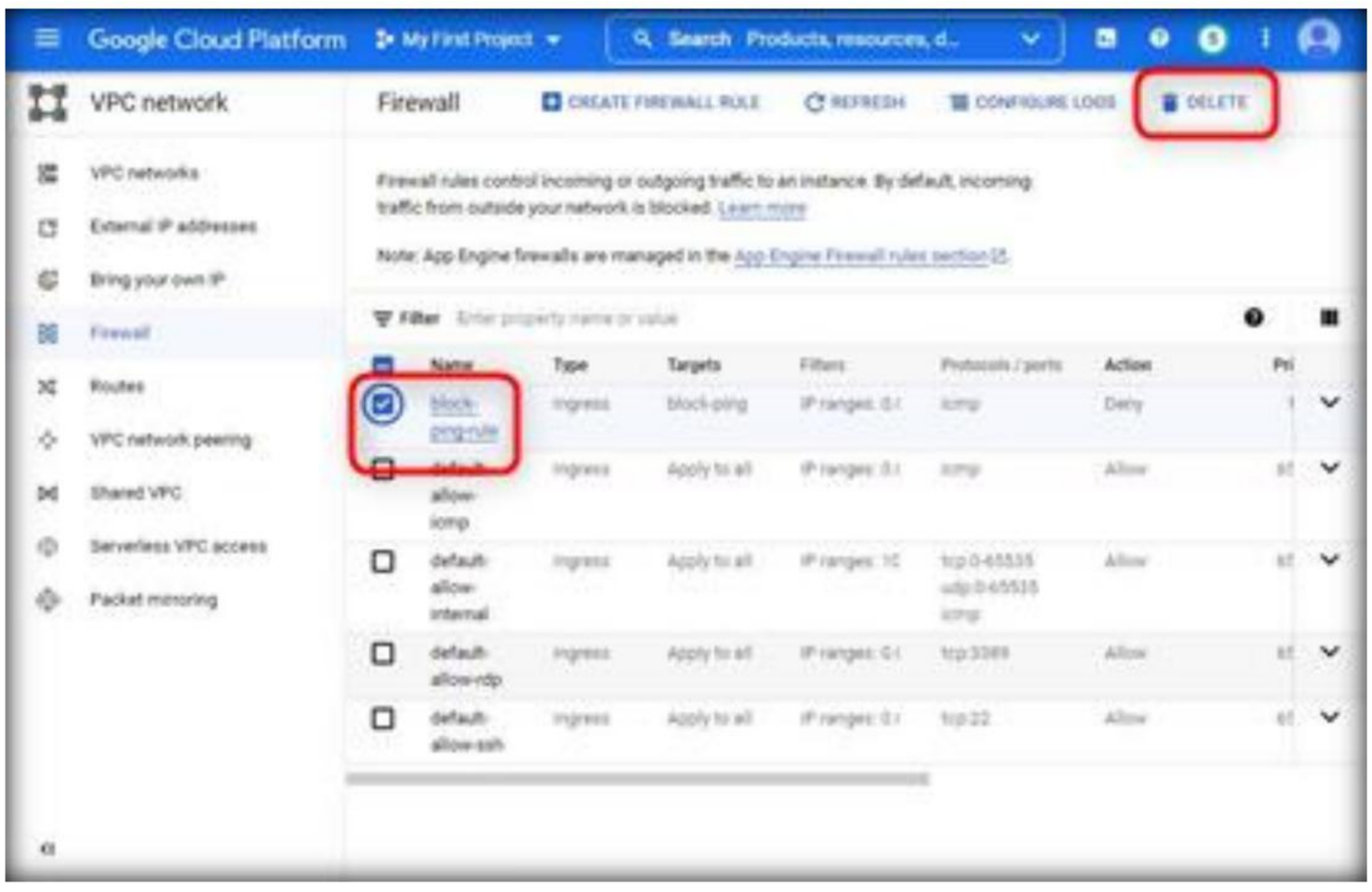


FIGURE 2.8.37: Deleting Firewall Rule

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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.

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 9

Implementing Secure Deployments in GKE with Binary Authorization

Binary Authorization in GCP is a security control that ensures secure deployment of container images in Google Kubernetes Engine (GKE).

ICON KEY

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

Lab Scenario

Binary Authorization in GCP is a security control that helps enforce the secure deployment of container images in Google Kubernetes Engine (GKE). Binary Authorization ensures this security control by signing the container images by trusted authorities during the development process and enforcing signature validation during the deployment. Thus, Binary Authorization ensures that only trusted and secure container images are deployed into the Google Kubernetes Engine (GKE).

Lab Objectives

This lab will demonstrate how to enable Binary Authorization in GKE, defining a policy for binary authorization, creating an attestor and integrating it with the policy, how to sign the container image by an attestor and how to run the signed image

In this lab, you will learn to do the following:

- Creating a Kubernetes cluster and adding containers
- Adding policies to the cluster
- Configuration of an attestor
- Signing the container image by attestor
- Running the signed container image

Lab Environment

To perform this lab, you need the following:

- **Admin Machine** VM
- **Administrative** privileges

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Registered GCP account.

Lab Duration

Time: 20 minutes

Overview of Binary Authorization

Google Kubernetes Engine (GKE) provides better management for applications deployed in the cloud. To ensure that only secure deployments are done with GKE, a cloud security engineer can implement Binary Authorization. Binary Authorization enforces the security of container images by the implementation of policies in the GKE cluster. In binary authorization, the trusted parties called attestors approve the container image. Attestors are implemented on Cloud Container Analysis API, which permits the integration of metadata with container images. Binary Authorization makes use of Container Analysis to integrate signatures with container images. With Binary Authorization, policies can be written to sign the image by an attestor before deployment. With Binary Authorization, only attestors can authorize deployments, where the identity of the attestors are verified with public keys and the attestations are signed with the corresponding private keys. The deployment would be successful only if the attestors verified the container image, else the deployment gets blocked.

Lab Tasks

hid001.ir

Note: Web applications using cloud environments may undergo **frequent updates**. For this lab, since we are working on a cloud-based environment (i.e., GCP), the application interface may be **updated** with time. Hence, in case you happen to work on an updated version of GCP, 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 GCP Free Trial account using the following link: https://cloud.google.com/free, in case you have already not created it for the previous lab. Once the registration is complete, perform the following tasks:

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

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1

Creating a Kubernetes cluster and adding containers

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

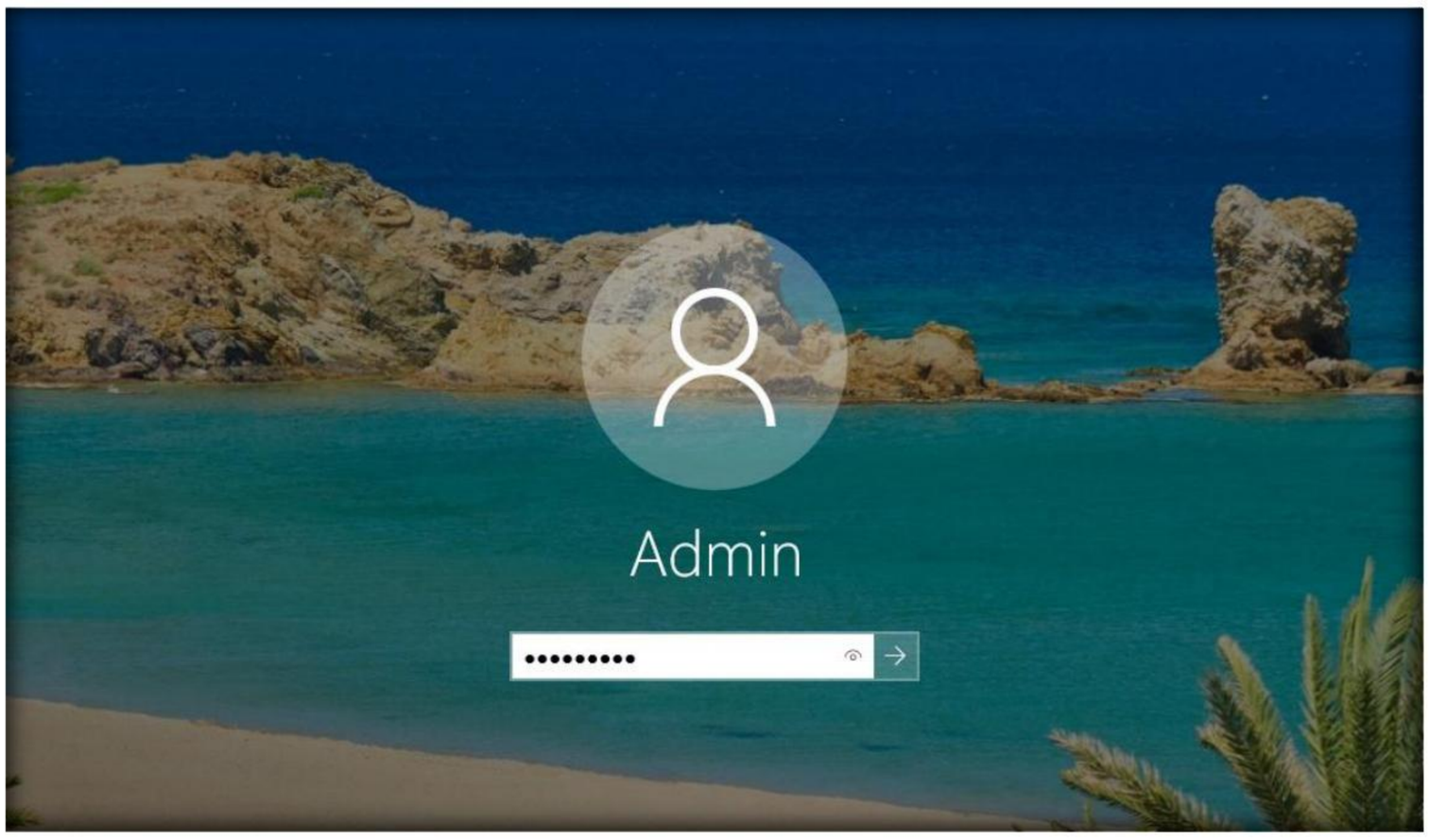


FIGURE 2.9.1: Launch Admin Machine and Log in

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

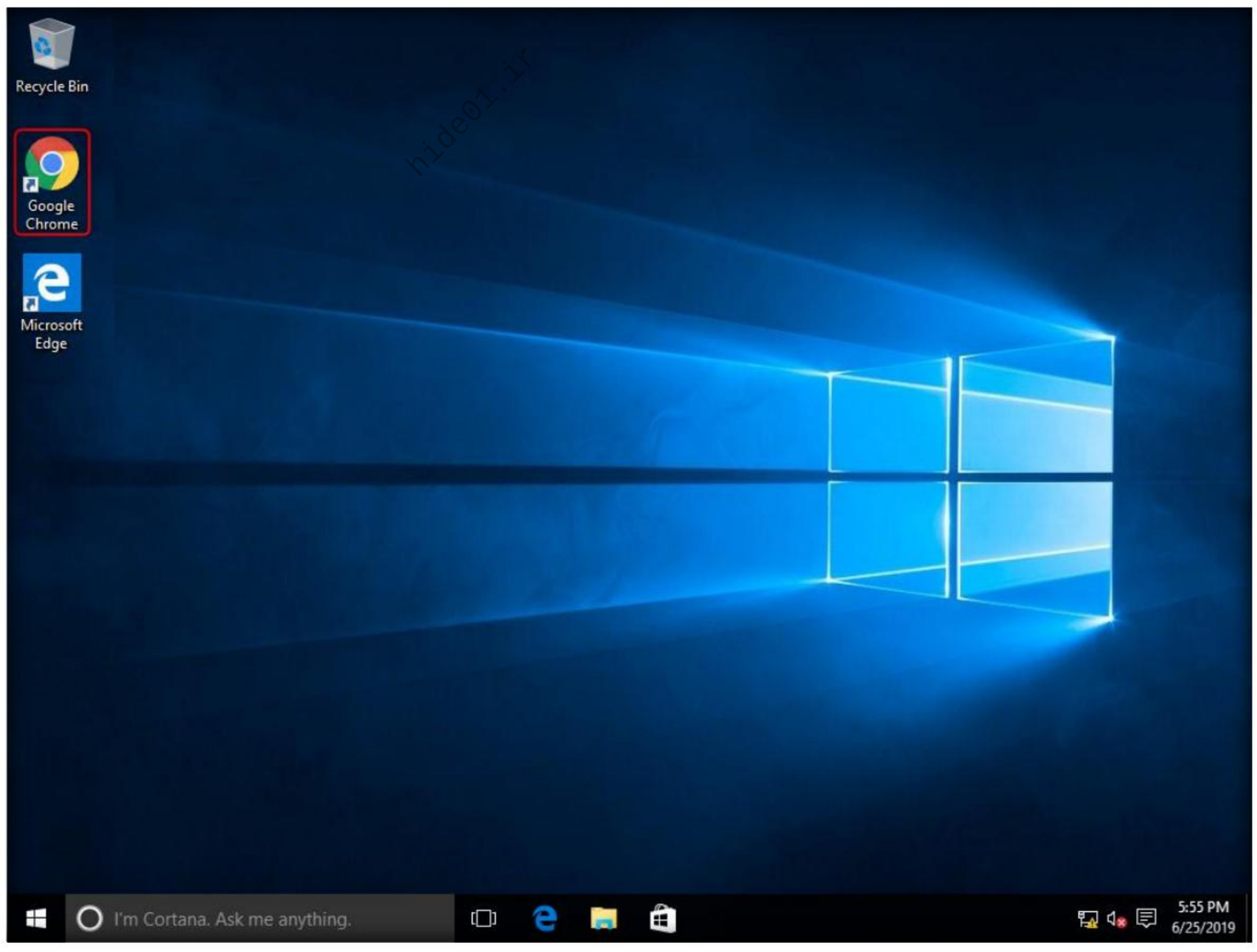


FIGURE 2.9.2: Navigating to the Chrome Browser from Taskbar

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

3. The **Google Chrome** browser opens. Go to the address bar, type **https://console.cloud.google.com/**, and press **Enter**.

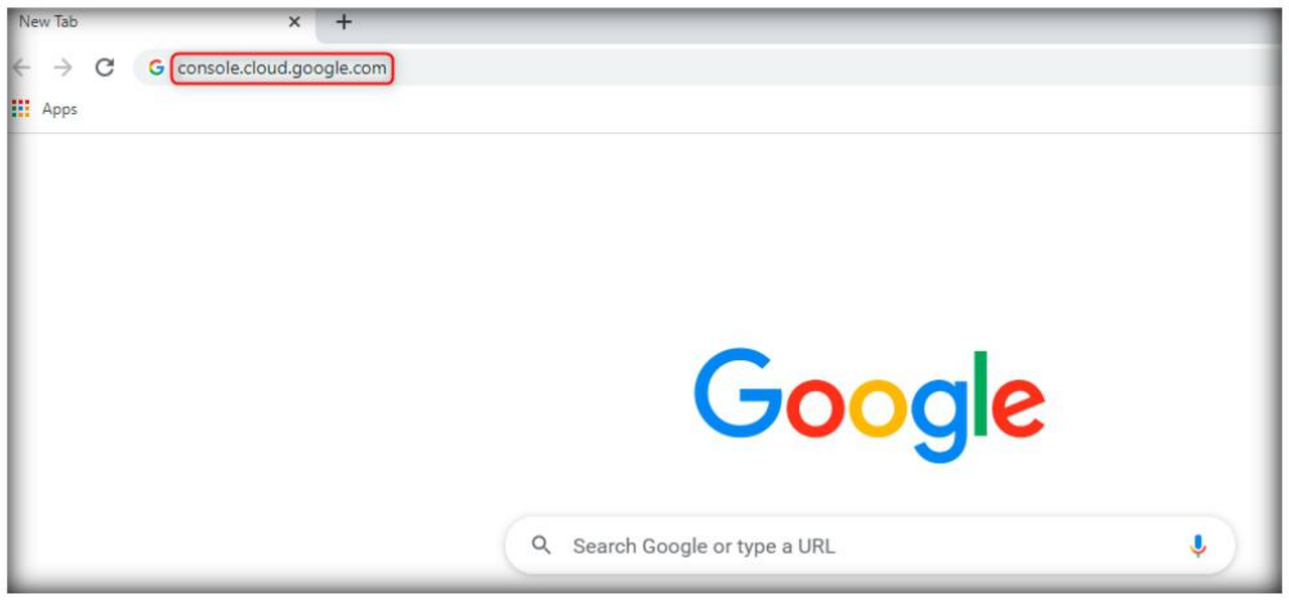


FIGURE 2.9.3: Access GCP in Browser

4. Enter the **Email address** to sign in to Google Cloud Platform and click on **Next.**

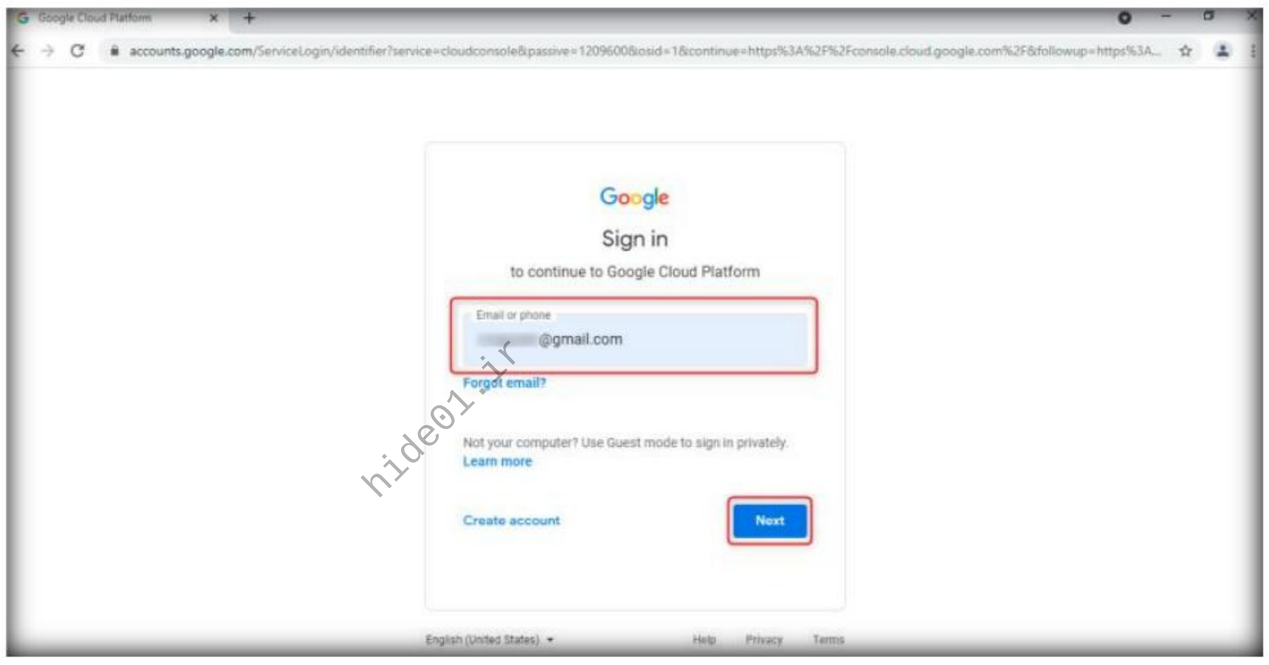


FIGURE 2.9.4: Entering the Email Address

5. Enter the password and click on **Next.**

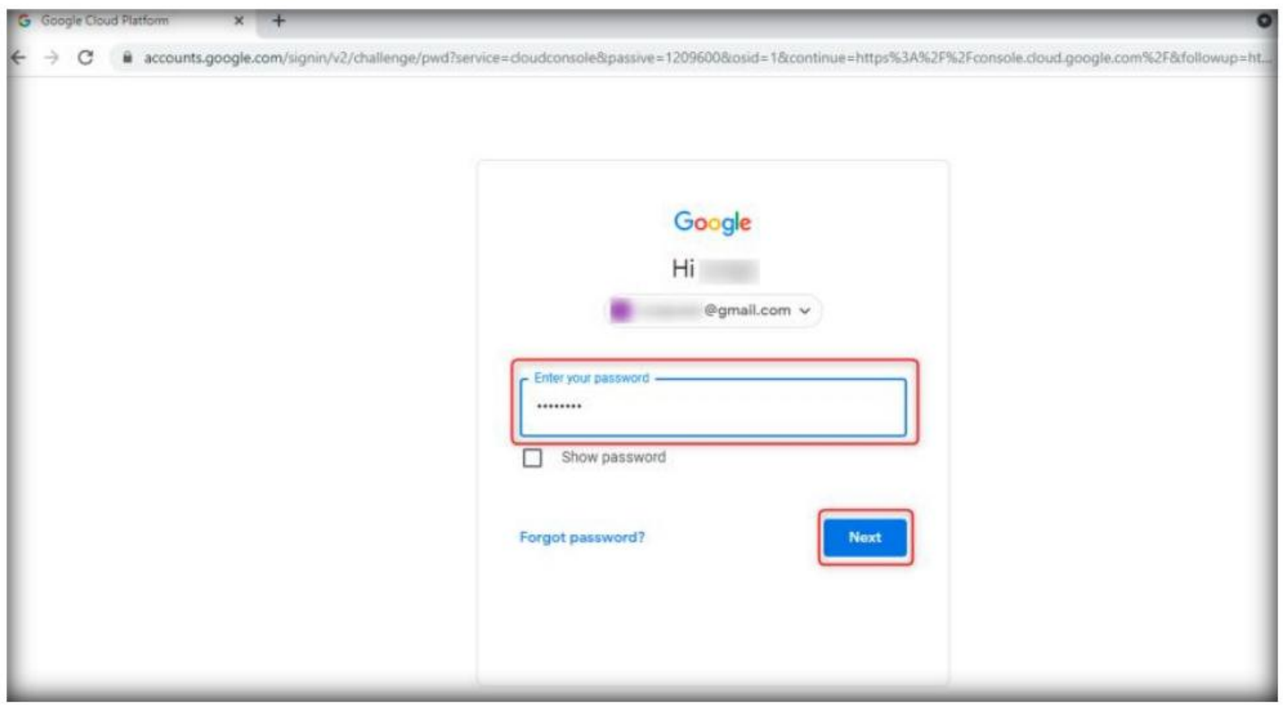


FIGURE 2.9.5: Signing in to the console

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

6. On the top left corner, you will have a drop-down option. It has a by default project selected. Click on it to explore more options.

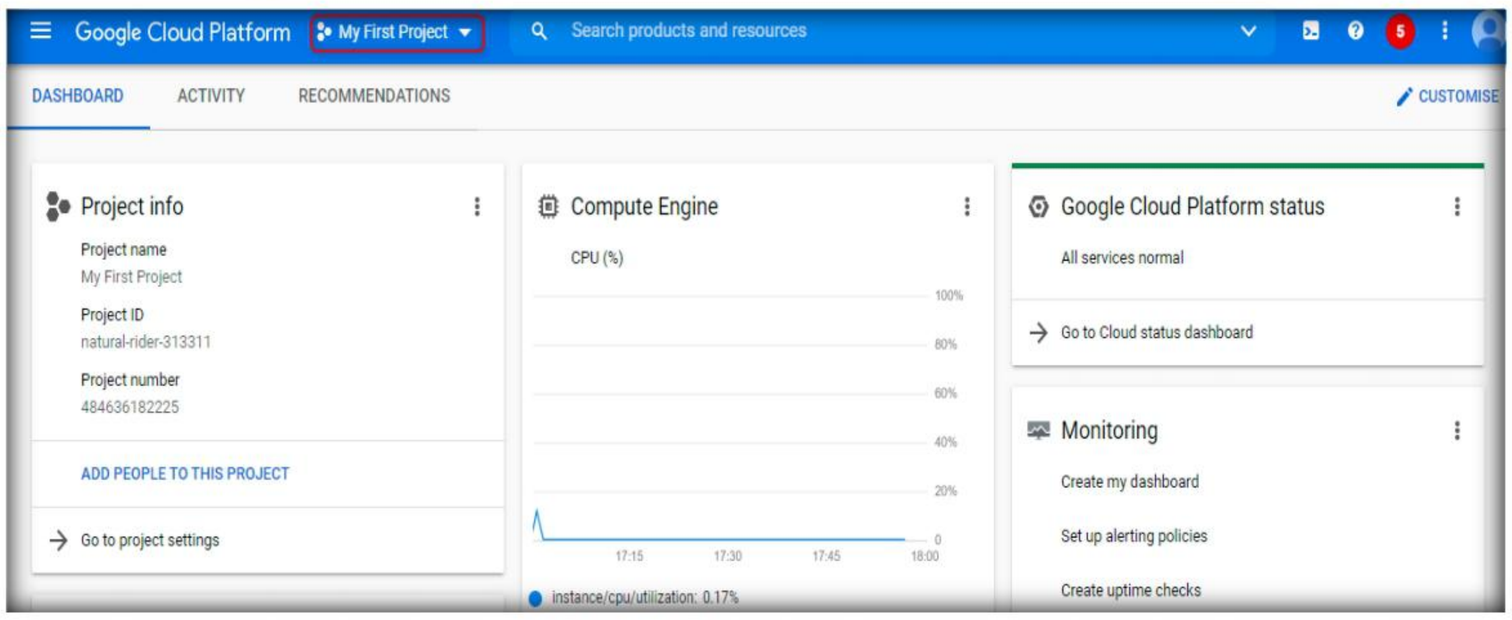


FIGURE 2.9.6: Selecting Project

7. The Web page that appears next lets you select an existing project that you can search by searching in the search tab or can click on **NEW PROJECT** to add a new one. When you add a new project, first-timers will require to set a billing option, which is a simple two-step process. Here, you can continue by selecting the project titled **My First Project**.

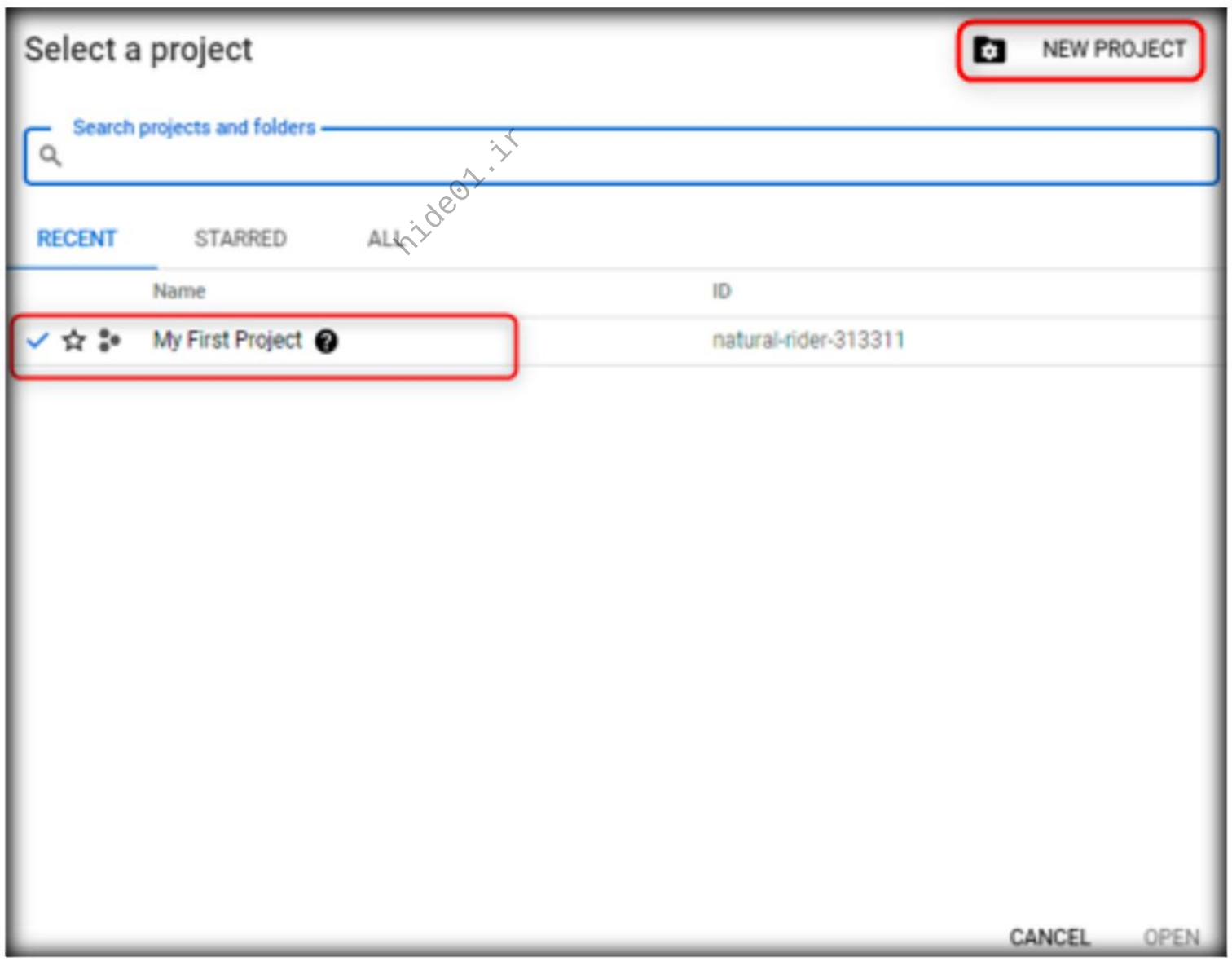


FIGURE 2.9.7: Selecting or Creating a new project

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

8. Now, click on the cloud shell icon on the top right corner of the console.

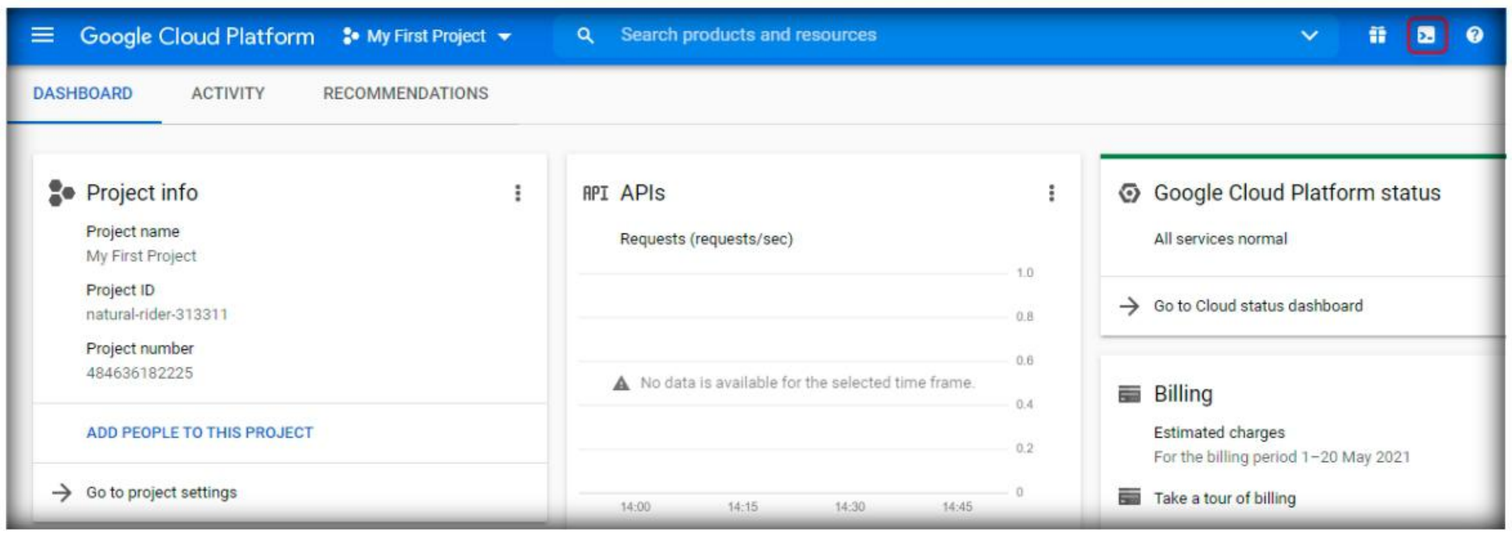


FIGURE 2.9.8: Opening Cloud Shell

9. Now, click on the icon in the top left corner of the cloud shell to open it in a new window.

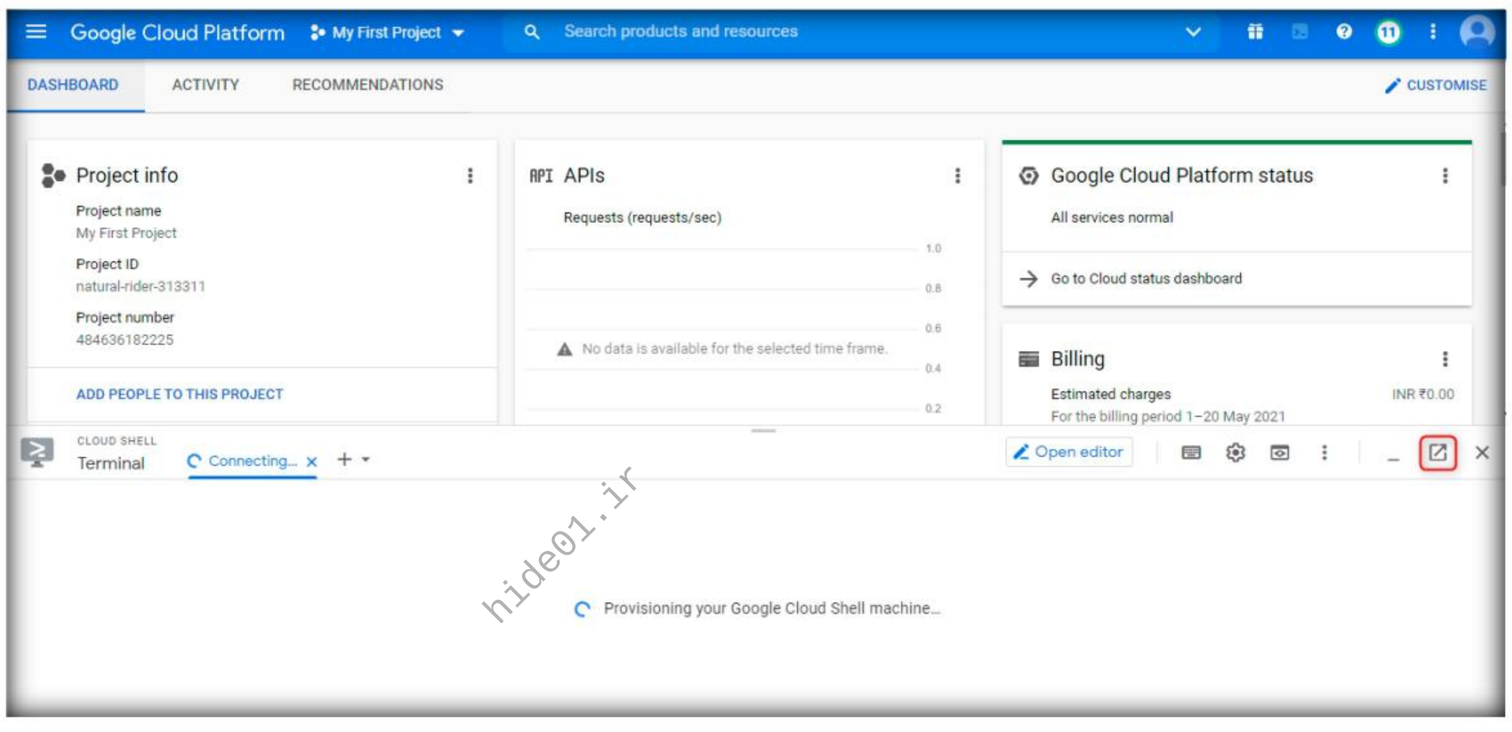


FIGURE 2.9.9: Expanding Cloud Shell Window

10. Now, in the cloud shell window type, the command and press **Enter** to list the projects.

```
gcloud  projects list
```

Note: If a window popup for Authorise Cloud Shell, click on **Authorise.**

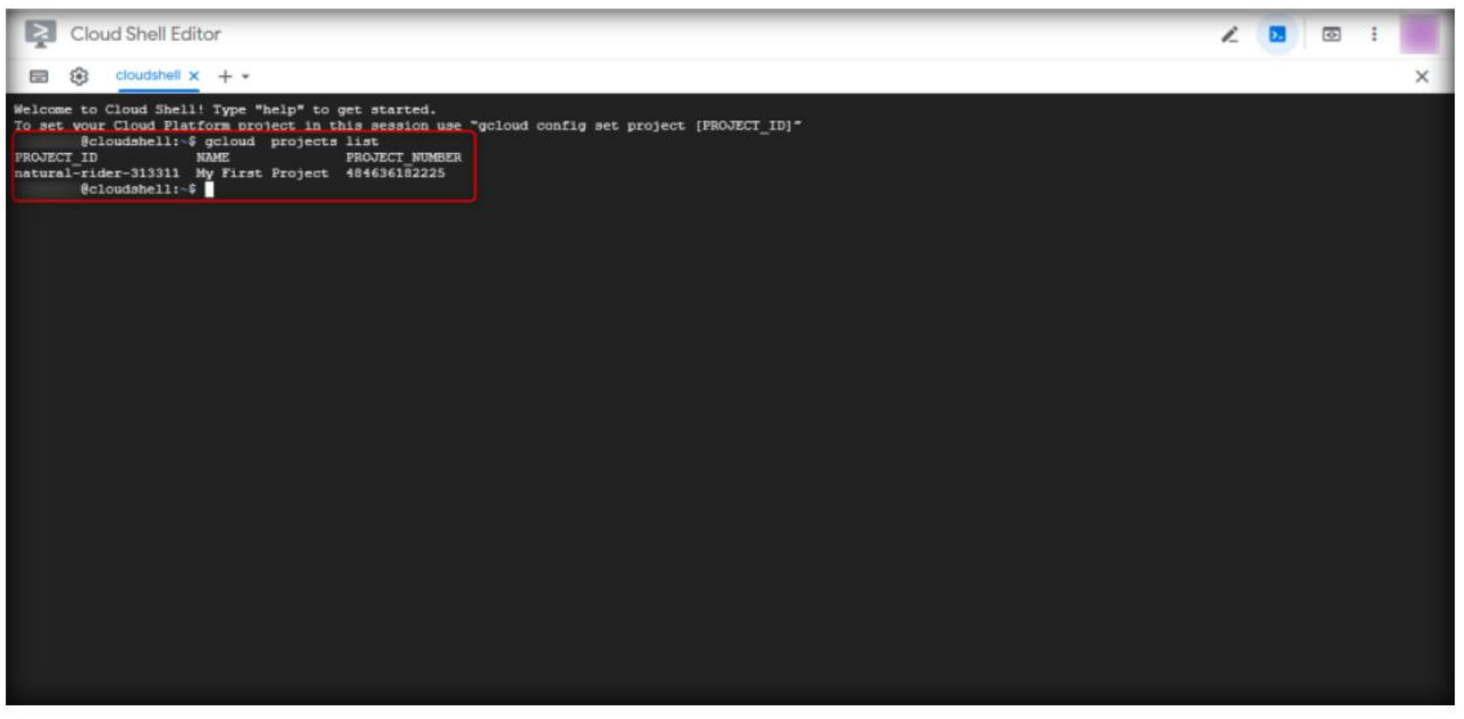


FIGURE 2.9.10: Listing Projects

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

11. Now to set the GCP project in the current session, use the following command and press **Enter**.

    `gcloud config set project [project_ID]` (replace [project-ID] with your project ID of the project you want to deploy the application), E.g., here, we used natural-rider-313311 in the command.

    ```
    gcloud config set project natural-rider-313311
    ```

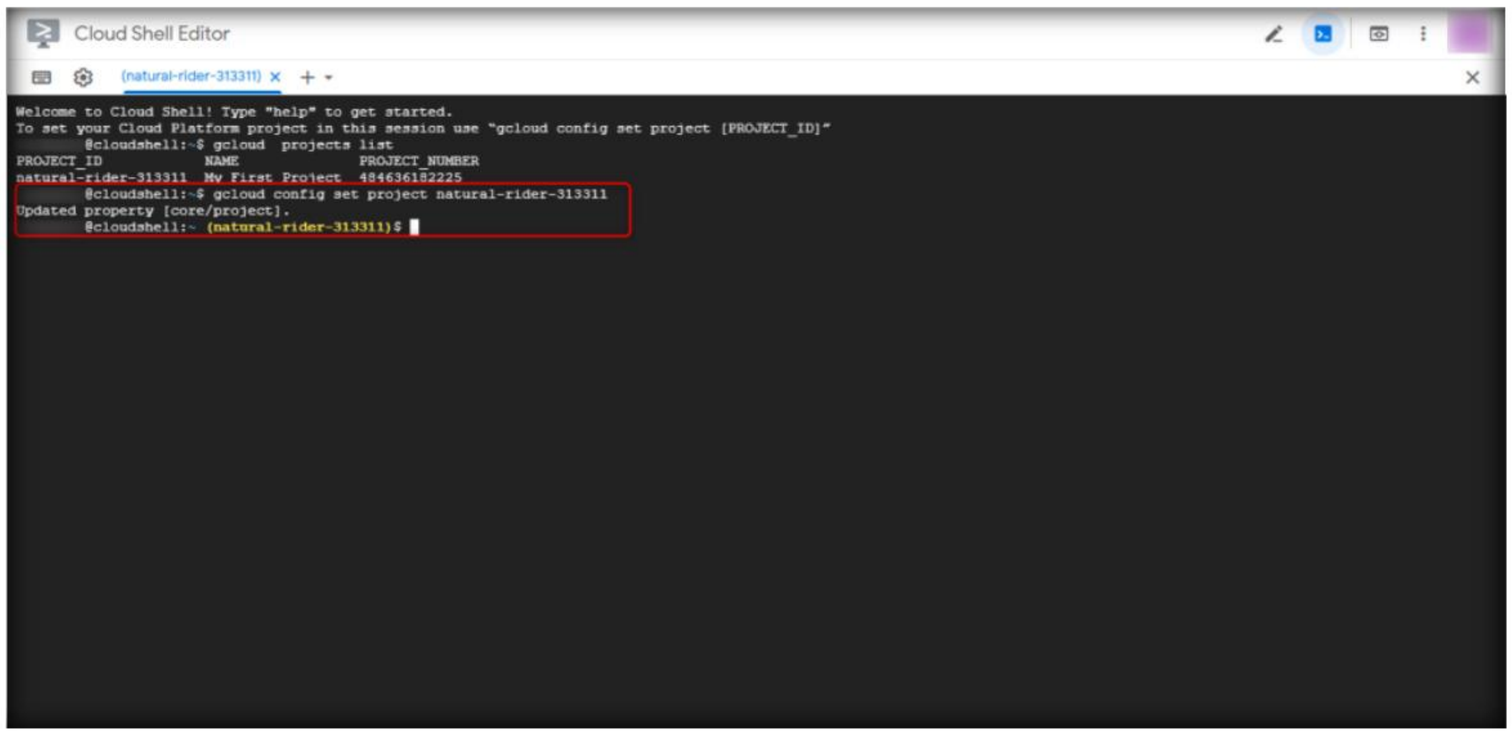


FIGURE 2.9.11: Setting GCP Project

12. Next, we need to setup the project. Consider you as a deployer here. First, you need to run the following command to set the variable PROJECT_ID.

    ```
    export PROJECT_ID=$(gcloud config get-value project)
    ```

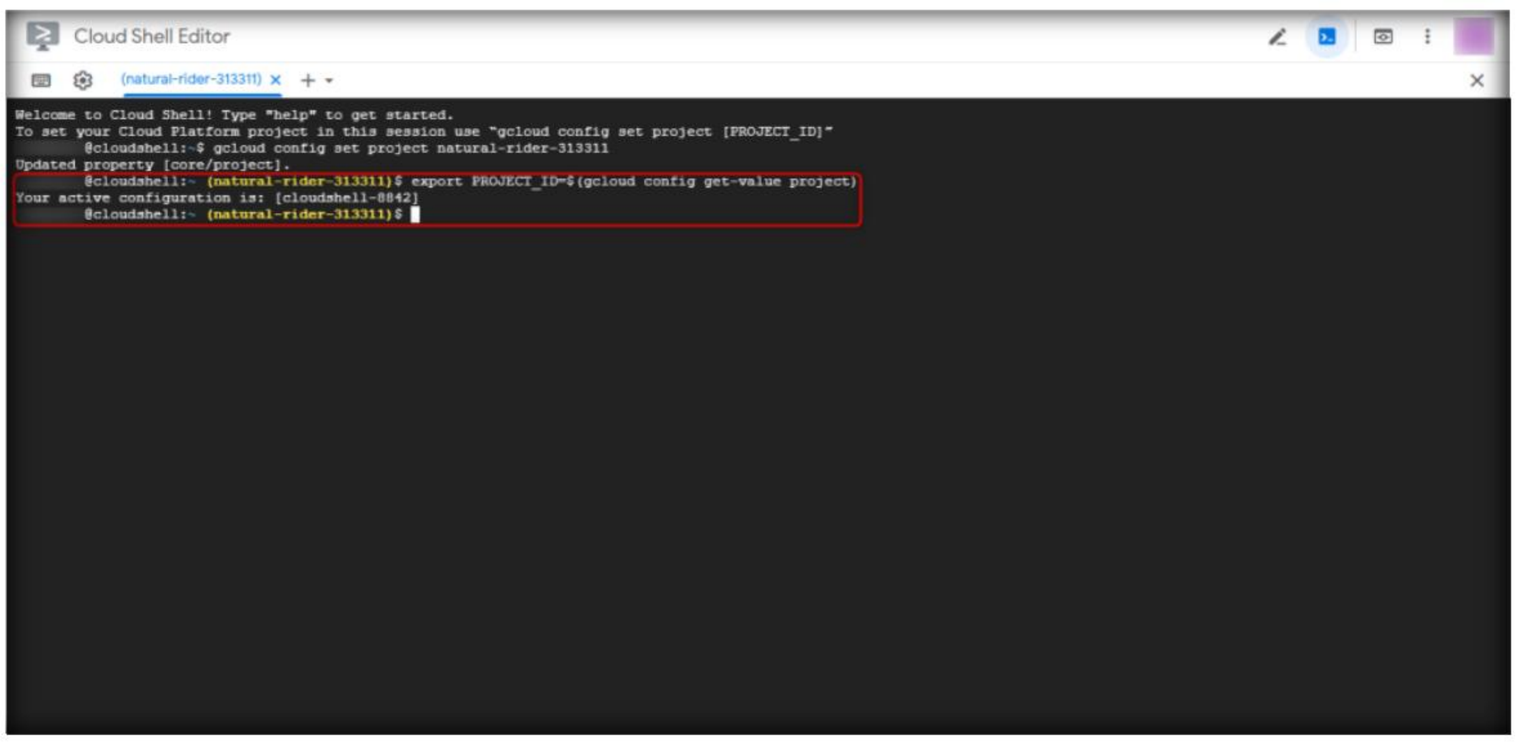


FIGURE 2.9.12: Setting Variable

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

13. Now, you need to enable the **APIs** in the project. Run the following command to enable it.

```
gcloud services enable \
    container.googleapis.com \
    containeranalysis.googleapis.com
```

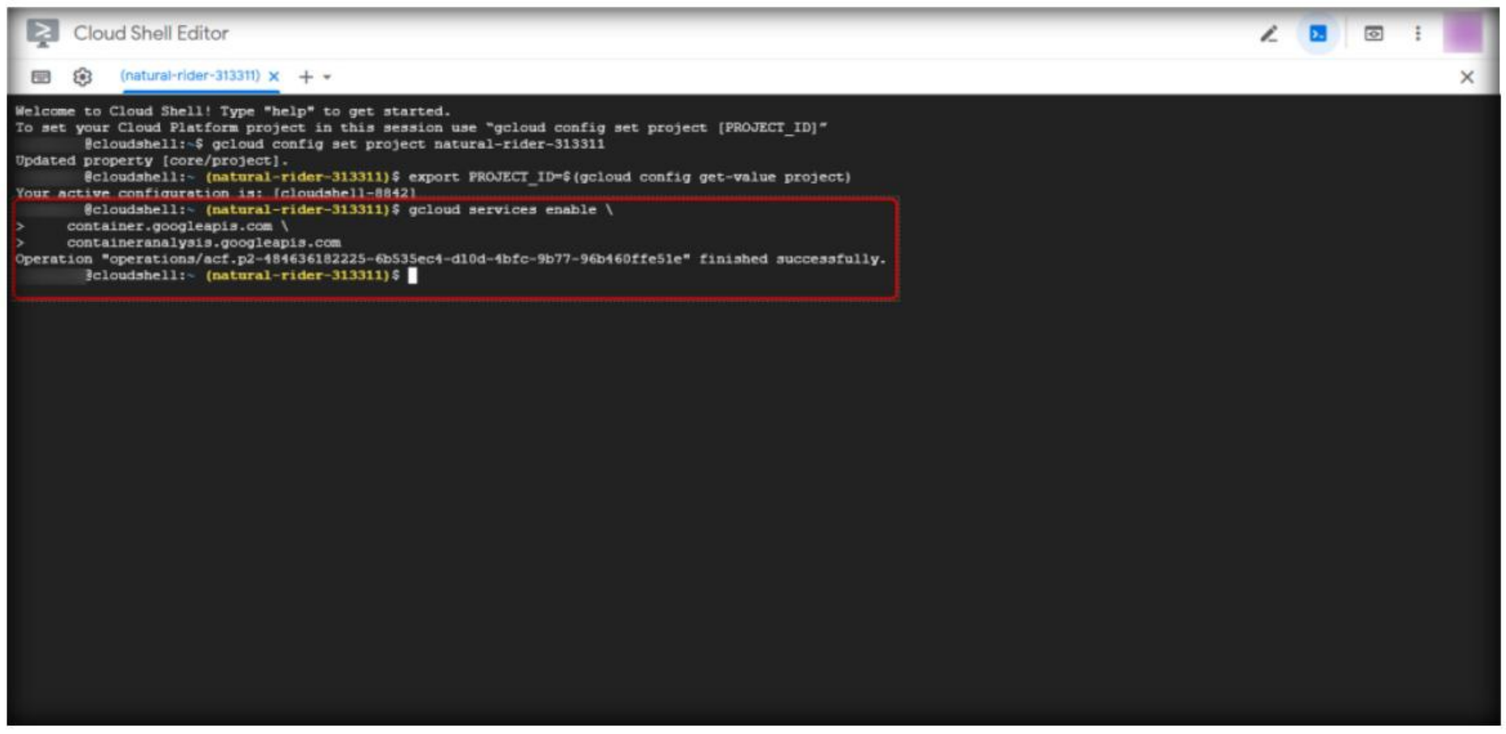


FIGURE 2.9.13: Enabling APIs

14. Now, you need to enable Binary Authorization. For that, go back to the GCP console and navigate to **Security** and select **Binary authorization**.

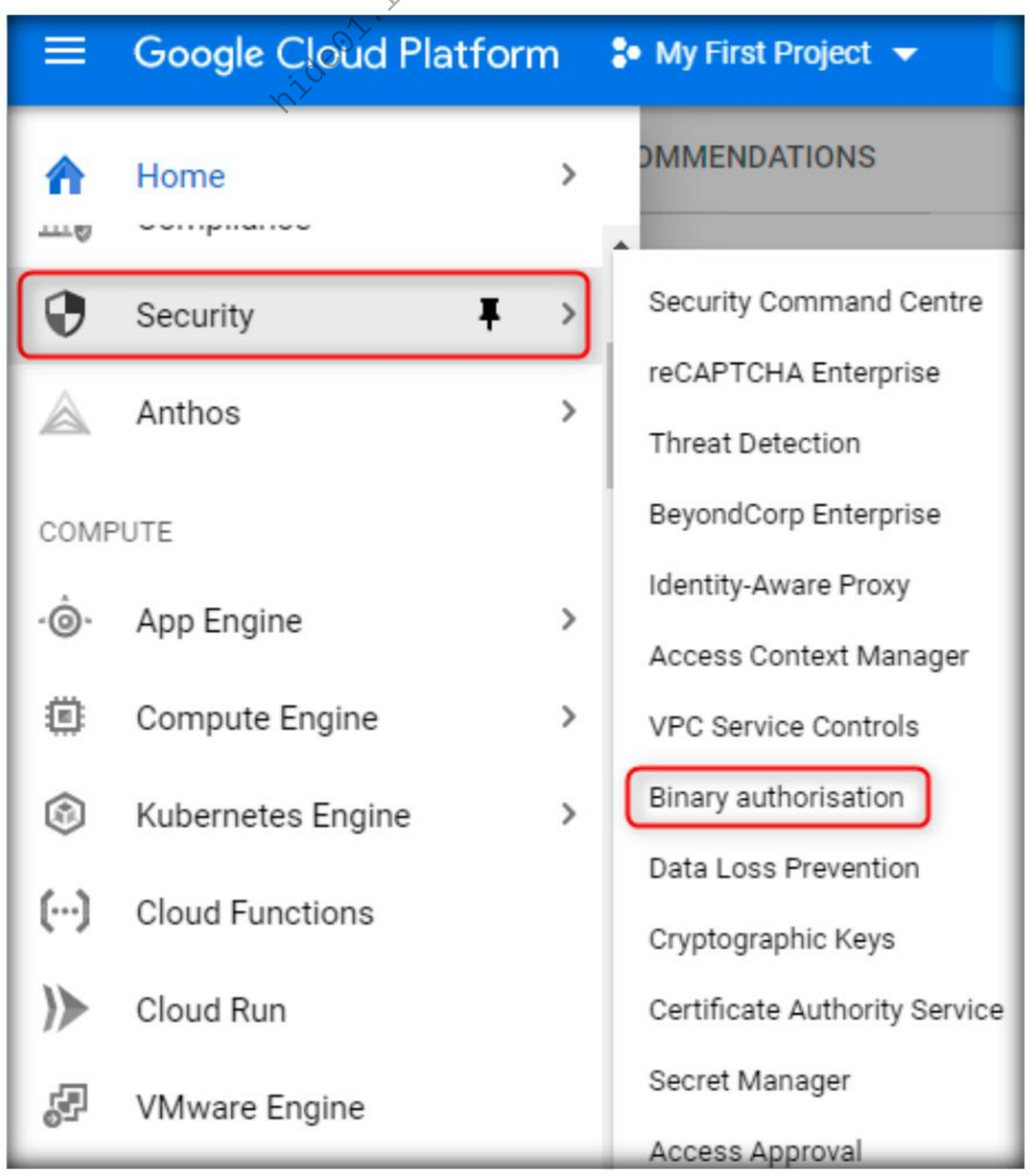


FIGURE 2.9.14: Navigating to Binary authorization

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

15. Click on **ENABLE** to enable the **Binary Authorization API.**

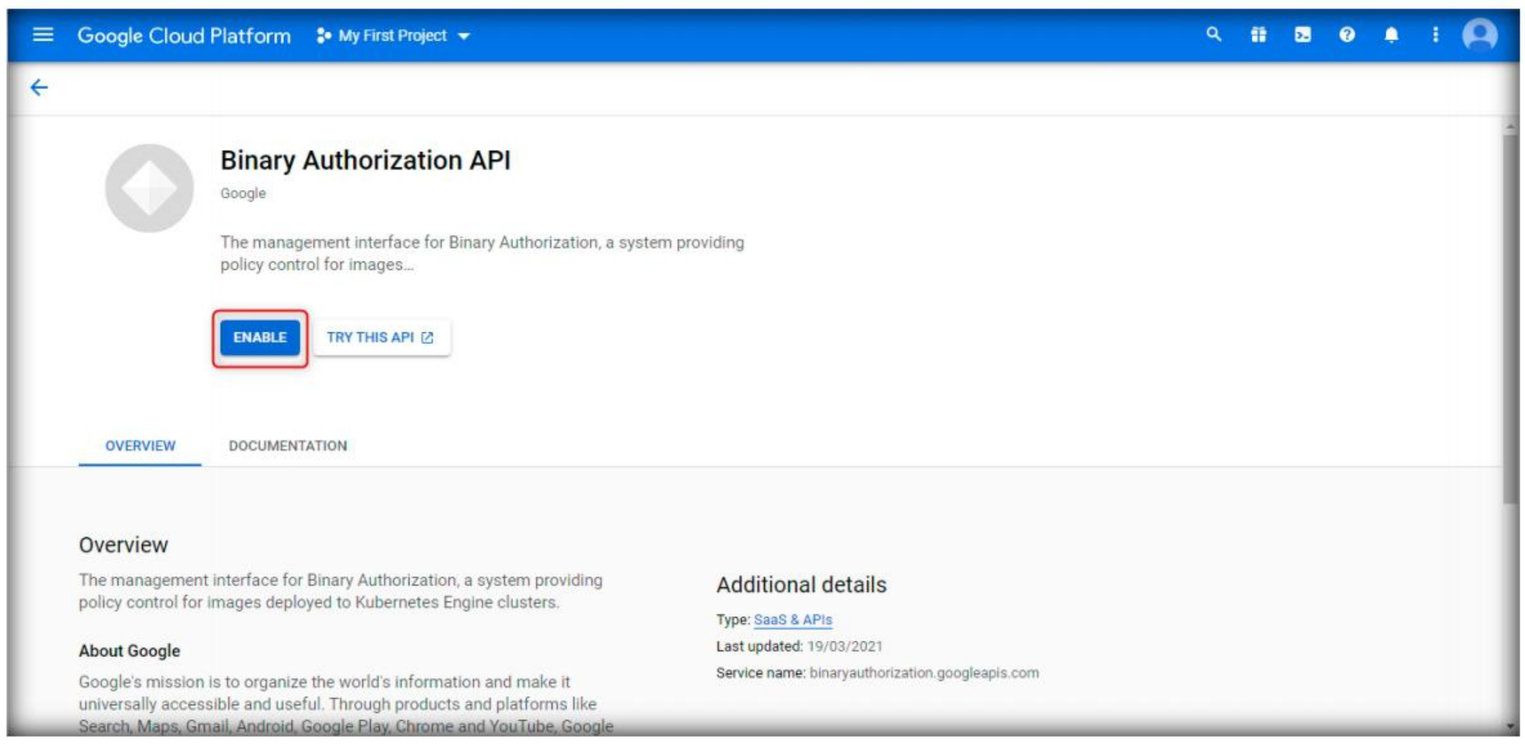


FIGURE 2.9.15: Enabling Binary authorization

16. Go back to the cloud shell window. Now, you need to configure a Kubernetes cluster for the project. To create a cluster with Binary Authorization enabled, run the following command. The name of the cluster is **ecc-binauthz-lab** in the **us-central1-a** zone.

    Note: Type the following command and press **Enter** line by line as shown in the screenshot below.

```
gcloud beta container clusters create \
    --enable-binauthz \
    --zone us-central1-a \
    ecc-binauthz-lab
```

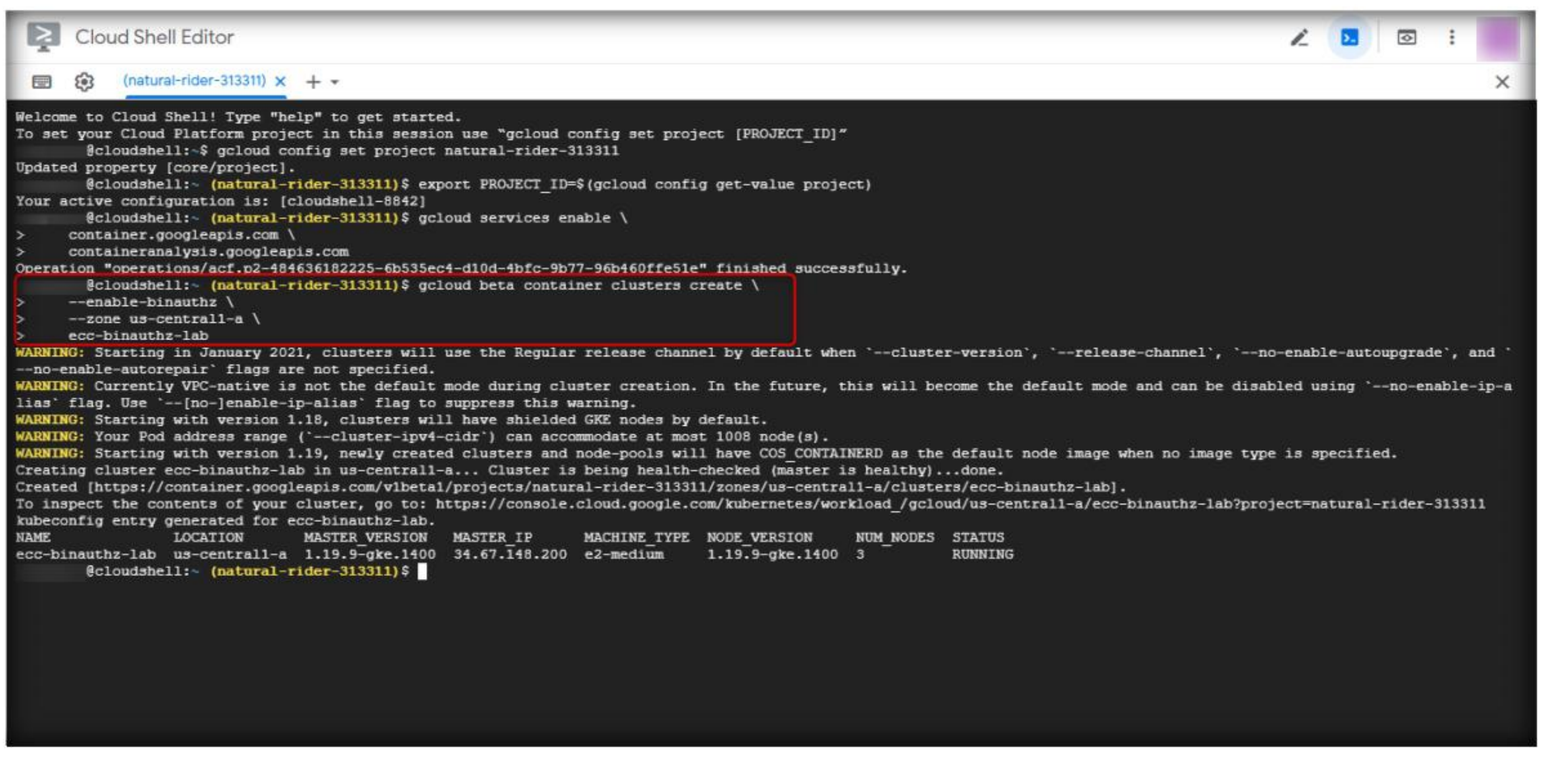


FIGURE 2.9.16: Configuring Cluster

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

17. Now, you need to add the cluster to the local environment. Run the following command to do so.

    Note: Type the following command and press **Enter** line by line as shown in the screenshot below.

```
gcloud container clusters get-credentials \
    --zone us-central1-a \
    ecc-binauthz-lab
```

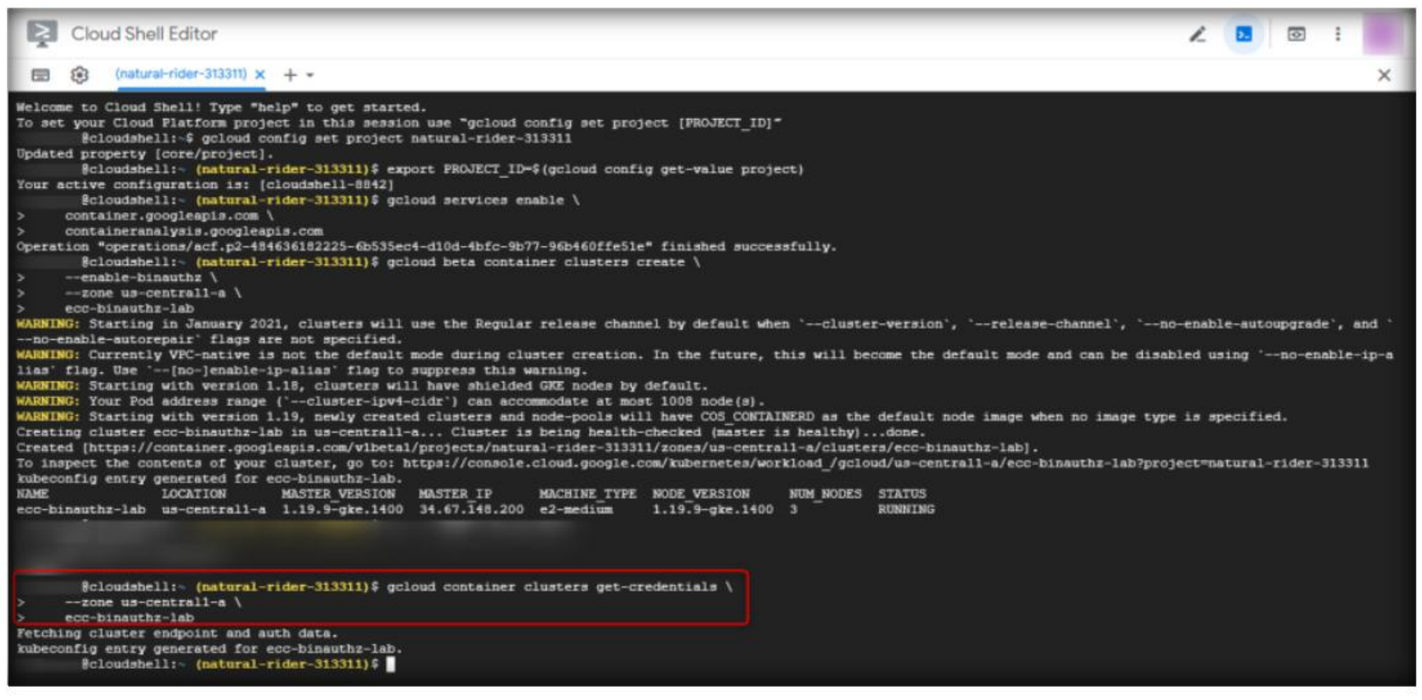


FIGURE 2.9.17: Adding Cluster to the local environment

18. Next, you need to create a container. First, you should create a Docker file. Run the following command to create a docker file.

    Note: Type the following command and press **Enter** line by line as shown in the screenshot below.

```
cat << EOF > Dockerfile
    FROM alpine
    CMD tail -f /dev/null
EOF
```

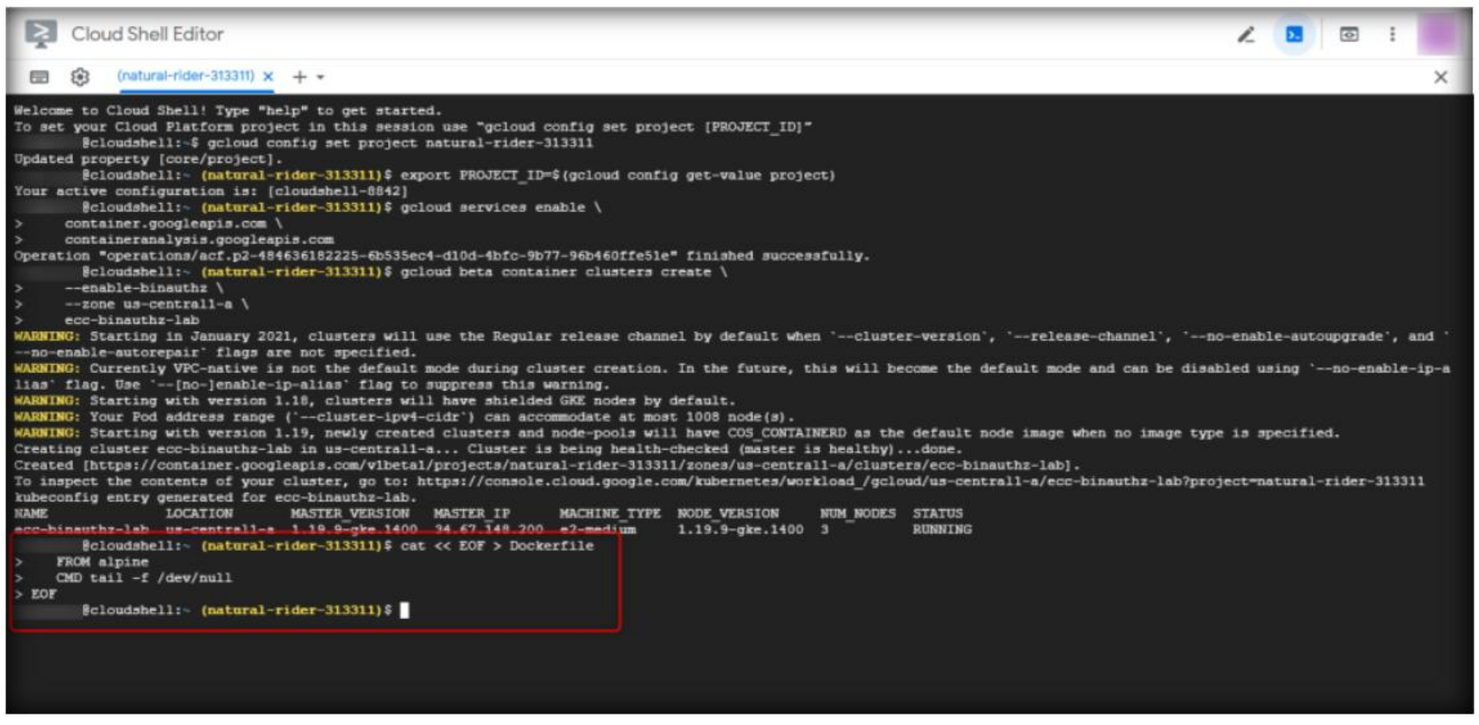


FIGURE 2.9.18: Creating Docker File

Certified Cloud Security Engineer Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

19. Next, run the commands step by step to build the container

```
export
CONTAINER_PATH=us.gcr.io/$PROJECT_ID/hello-
eccuser

docker build -t $CONTAINER_PATH ./
```

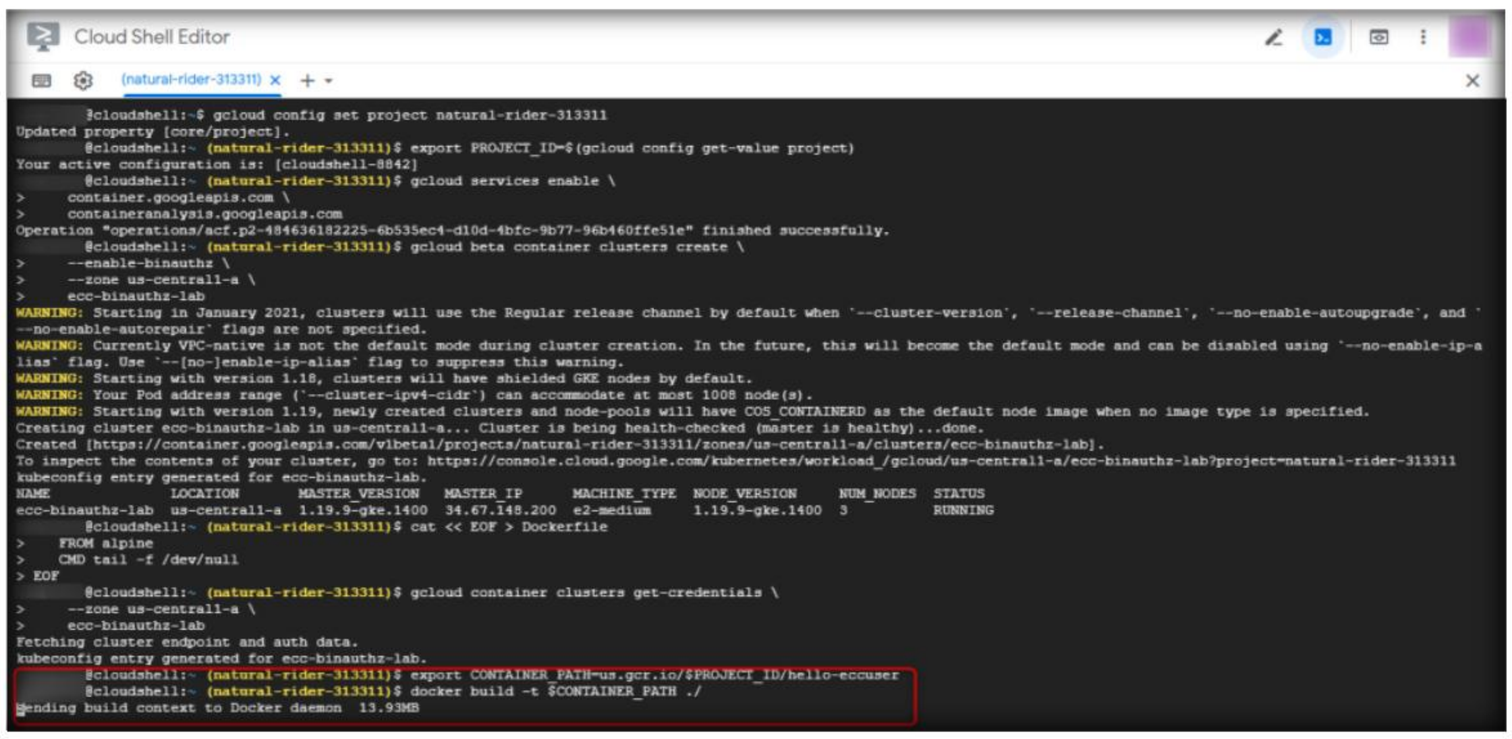


FIGURE 2.9.19: Building Container

20. Now, run the following command step by step to push the container to Google Container Registry (GCR).

```
gcloud auth configure-docker --quiet

docker push $CONTAINER_PATH
```

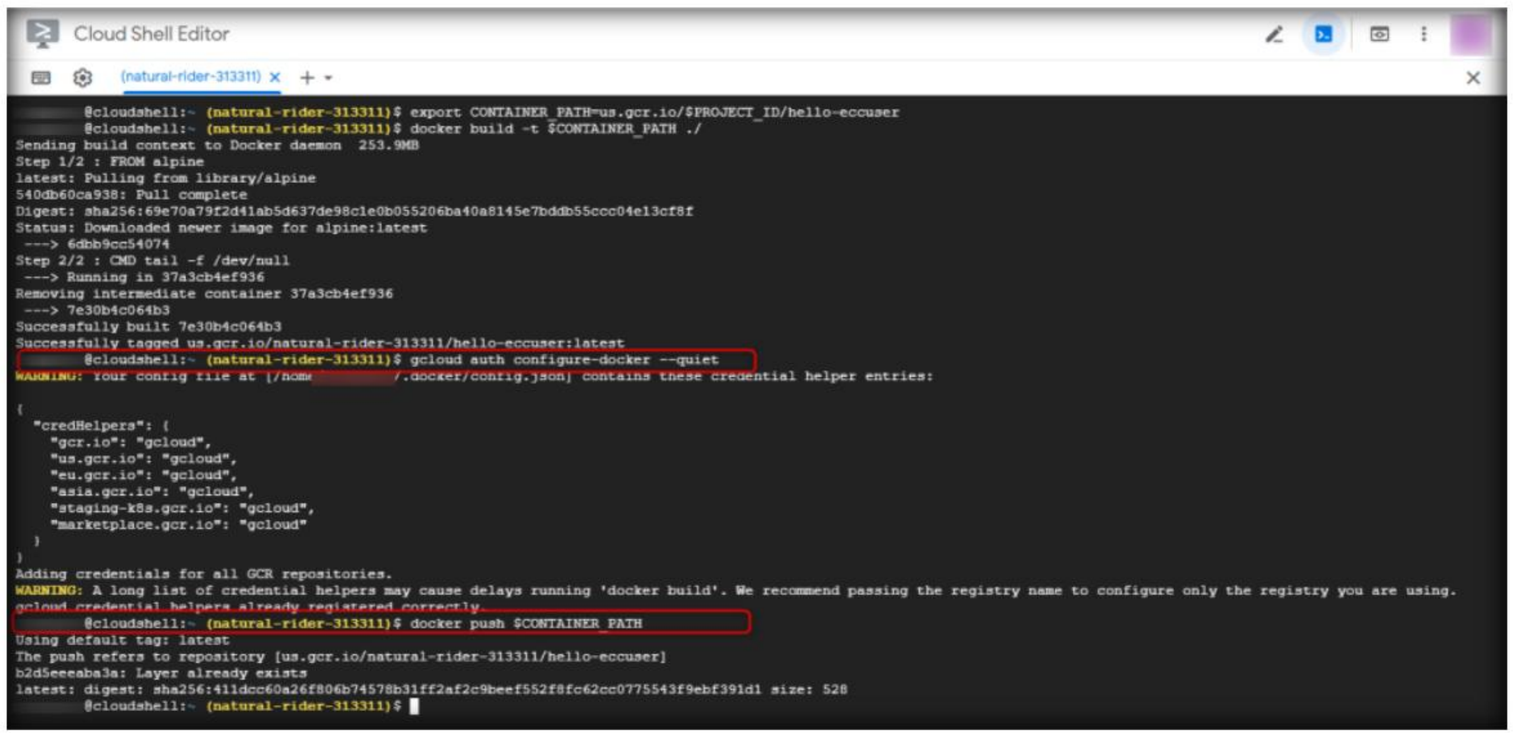


FIGURE 2.9.20: Pushing container to GCR

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

21. To verify if the container is created, go back to the console, navigate to **Container Registry,** and select **Images.**

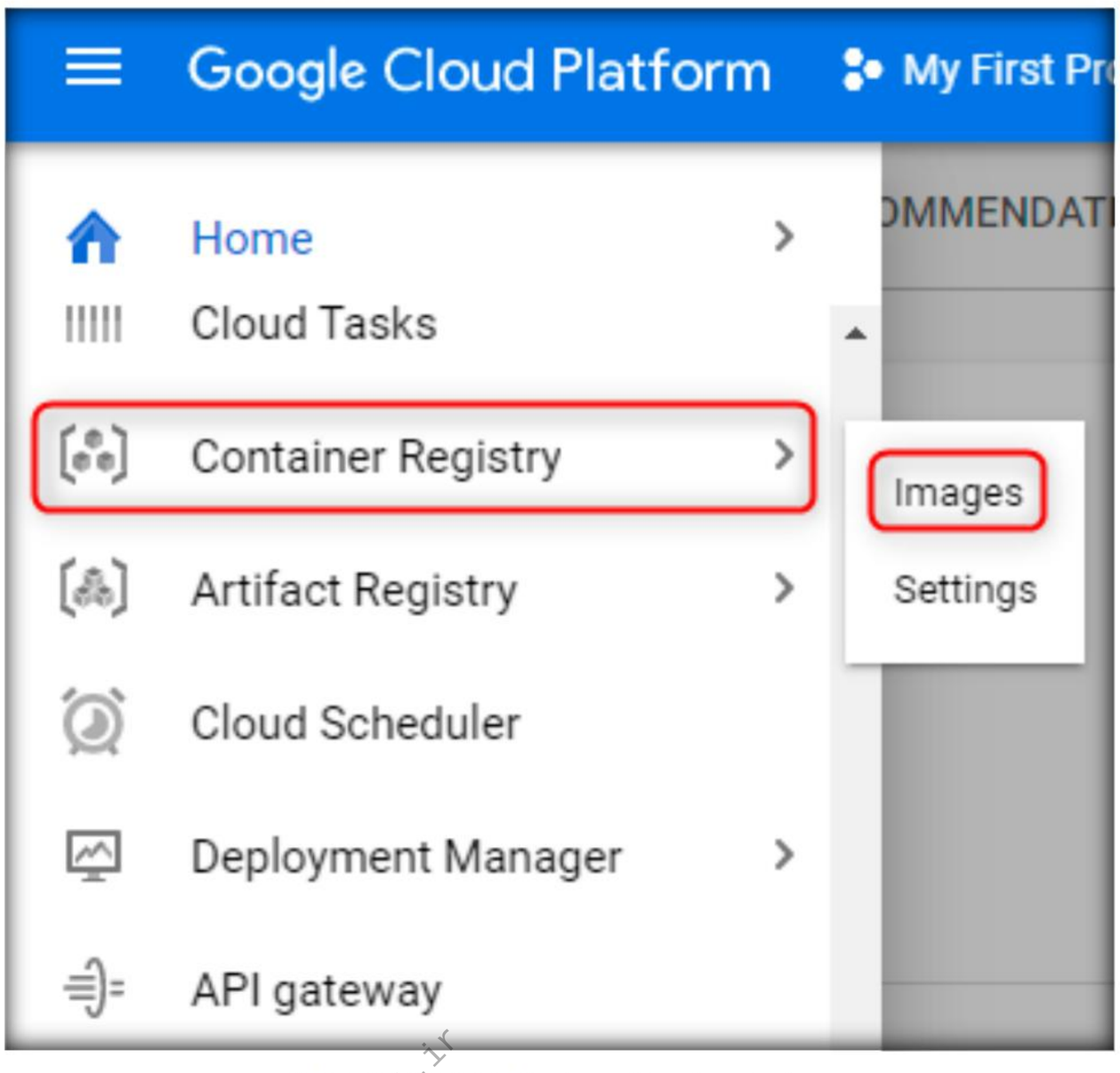


FIGURE 2.9.21: Navigating to Container Registry

22. You can see that the container **hello-eccuser** is successfully created.

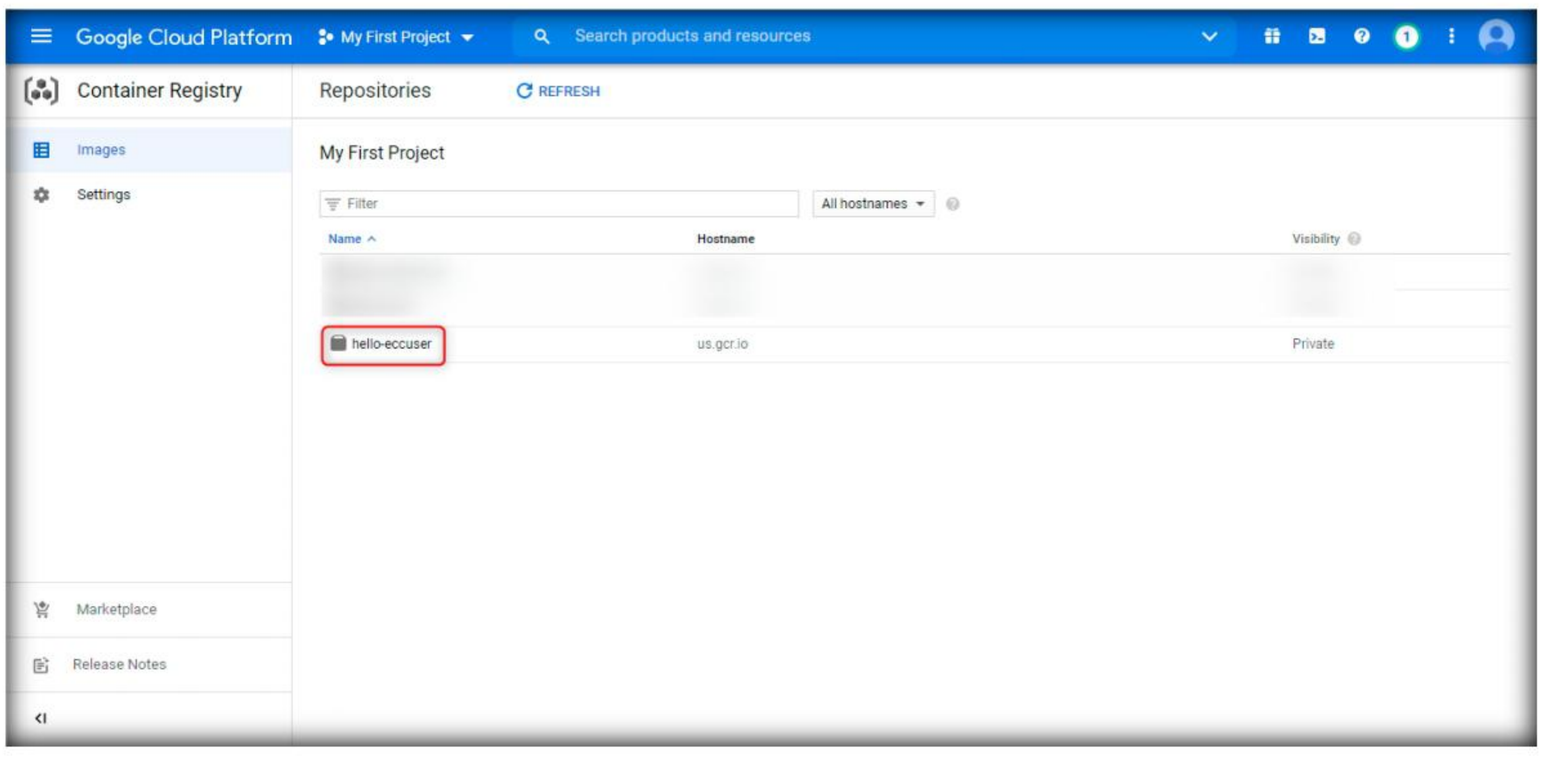


FIGURE 2.9.22: Container Created Successfully

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

23. Next, type the following command and press **Enter** to run the container in the Kubernetes cluster.

```
kubectl create deployment hello-eccuser --
image=$CONTAINER_PATH
```

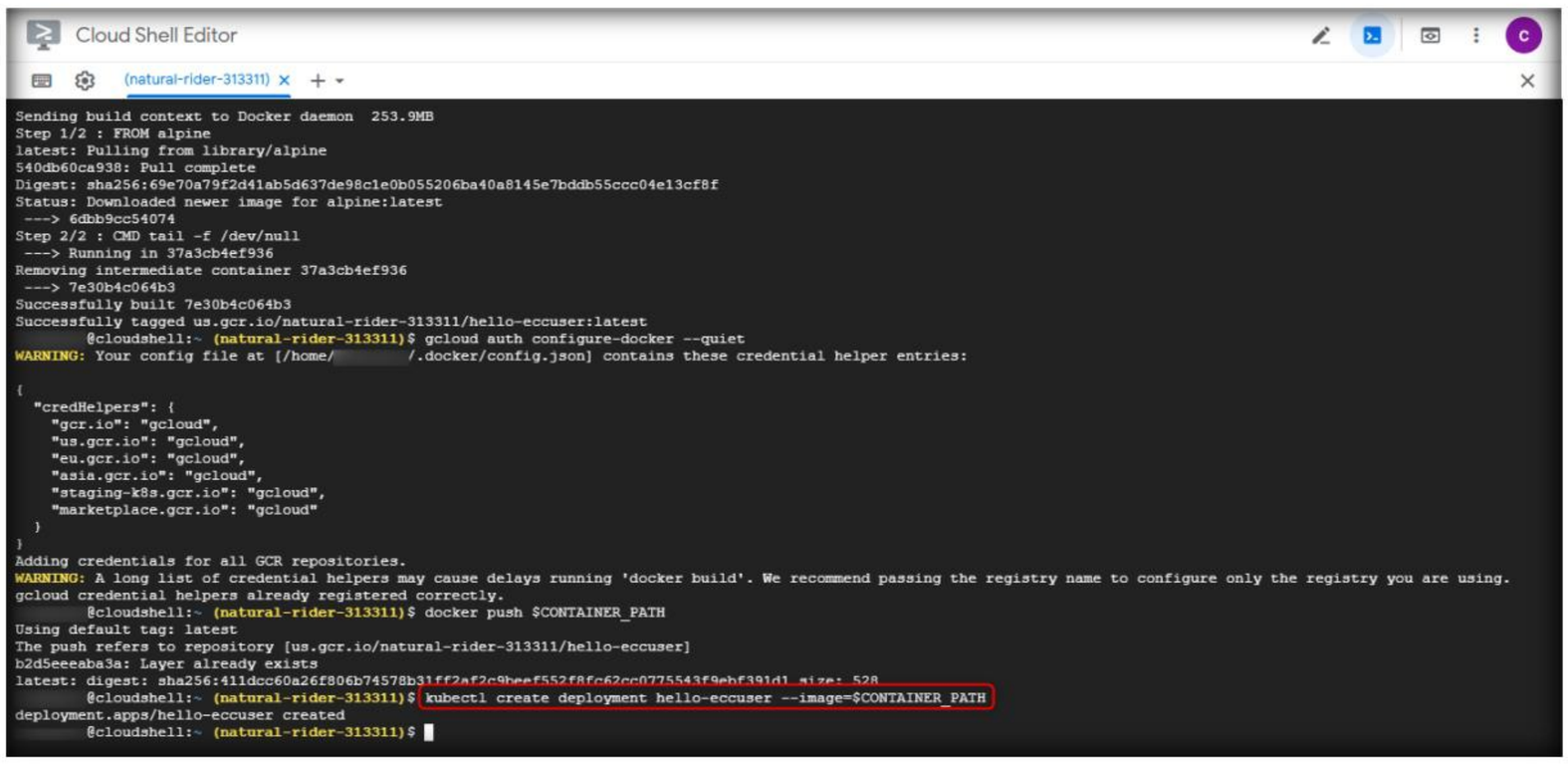


FIGURE 2.9.23: Running the Container

24. Now, to ensure that the container is running, run the following command to list the running pods. You will get the **STATUS** as **Running.**

```
kubectl get pods
```

hide01.ir

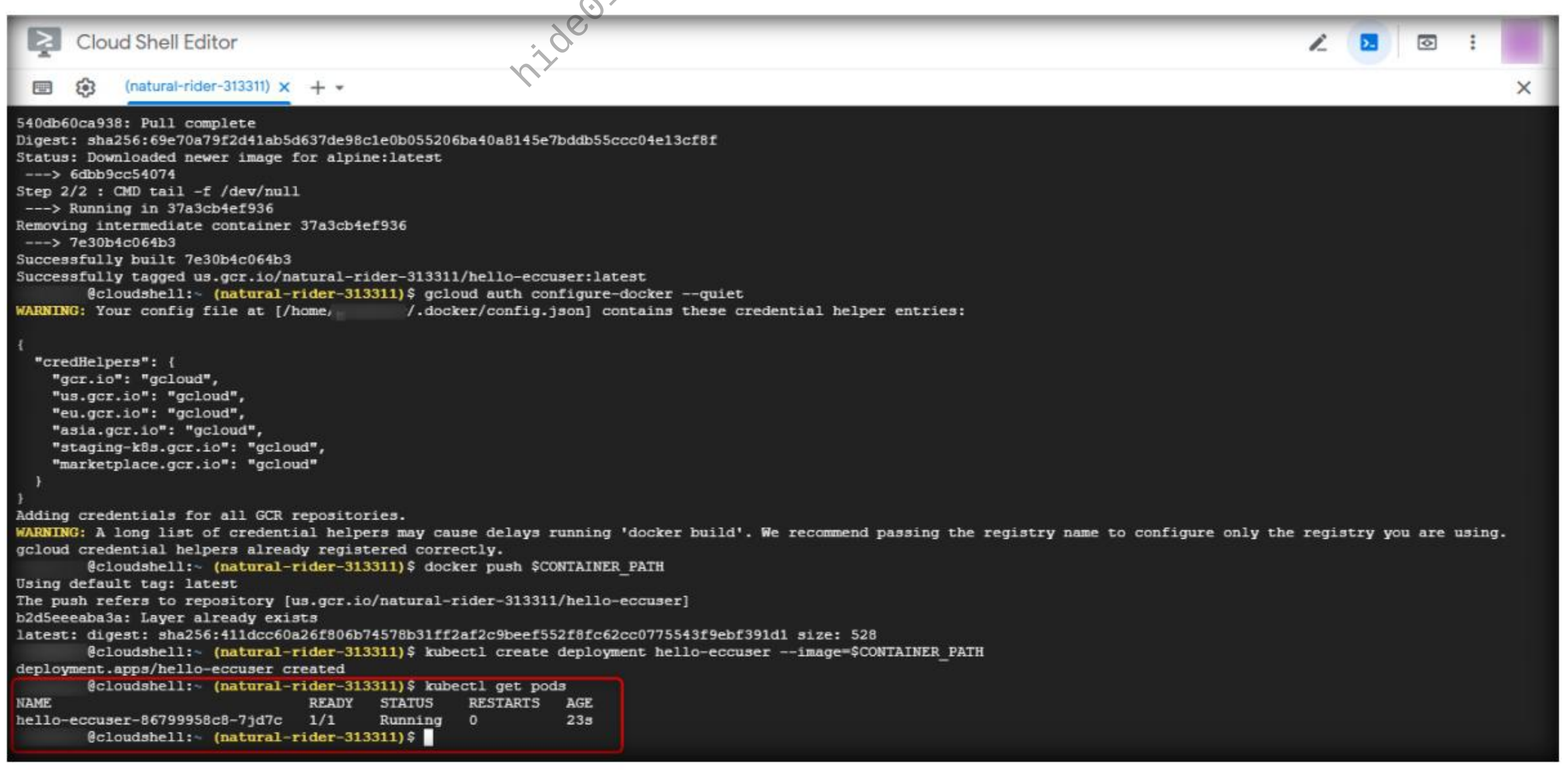


FIGURE 2.9.24: Container is Running

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 2

Adding Policies to Cluster

25. Next, you need to create a policy for the **Kubernetes cluster**. You can create a policy by running the following command.

    Note: Type the following command and press **Enter** line by line as shown in the screenshot below.

```
cat > ./policy.yaml << EOM
    globalPolicyEvaluationMode: ENABLE
    defaultAdmissionRule:
      evaluationMode: ALWAYS_DENY
      enforcementMode:
ENFORCED_BLOCK_AND_AUDIT_LOG
EOM
```

Note: The `globalPolicyEvaluationMode` is to allow all Google Kubernetes Engine containers to run by default. The `defaultAdmissionRule` includes an evaluation mode to reject all other pods. The `enforcementMode` is to declare all the pods that do not follow this rule has to be blocked from running in the Kubernetes cluster.

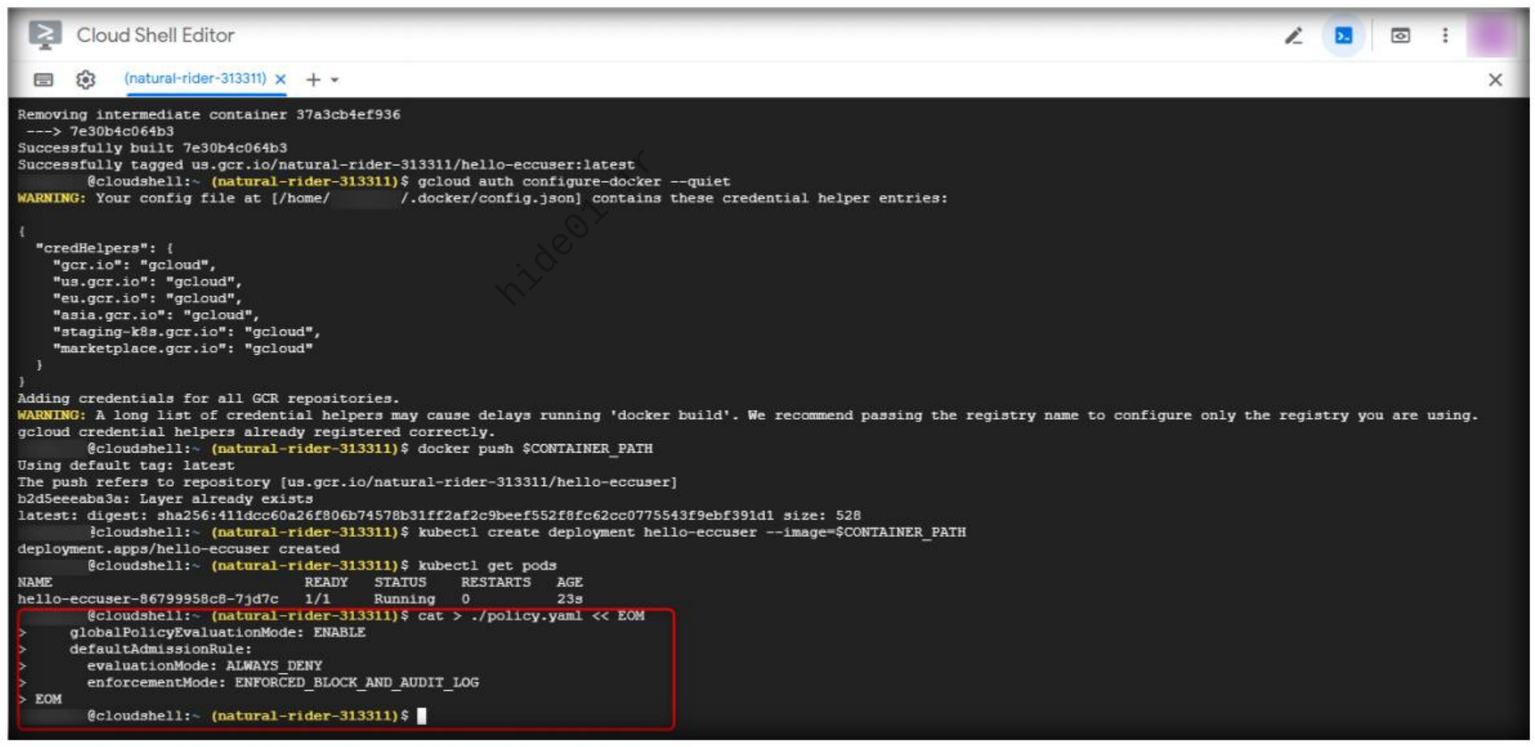


FIGURE 2.9.25: Adding Policy

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

26. Next, type the following command and press **Enter** to apply the above policy to the project.

```
gcloud container binauthz policy import policy.yaml
```

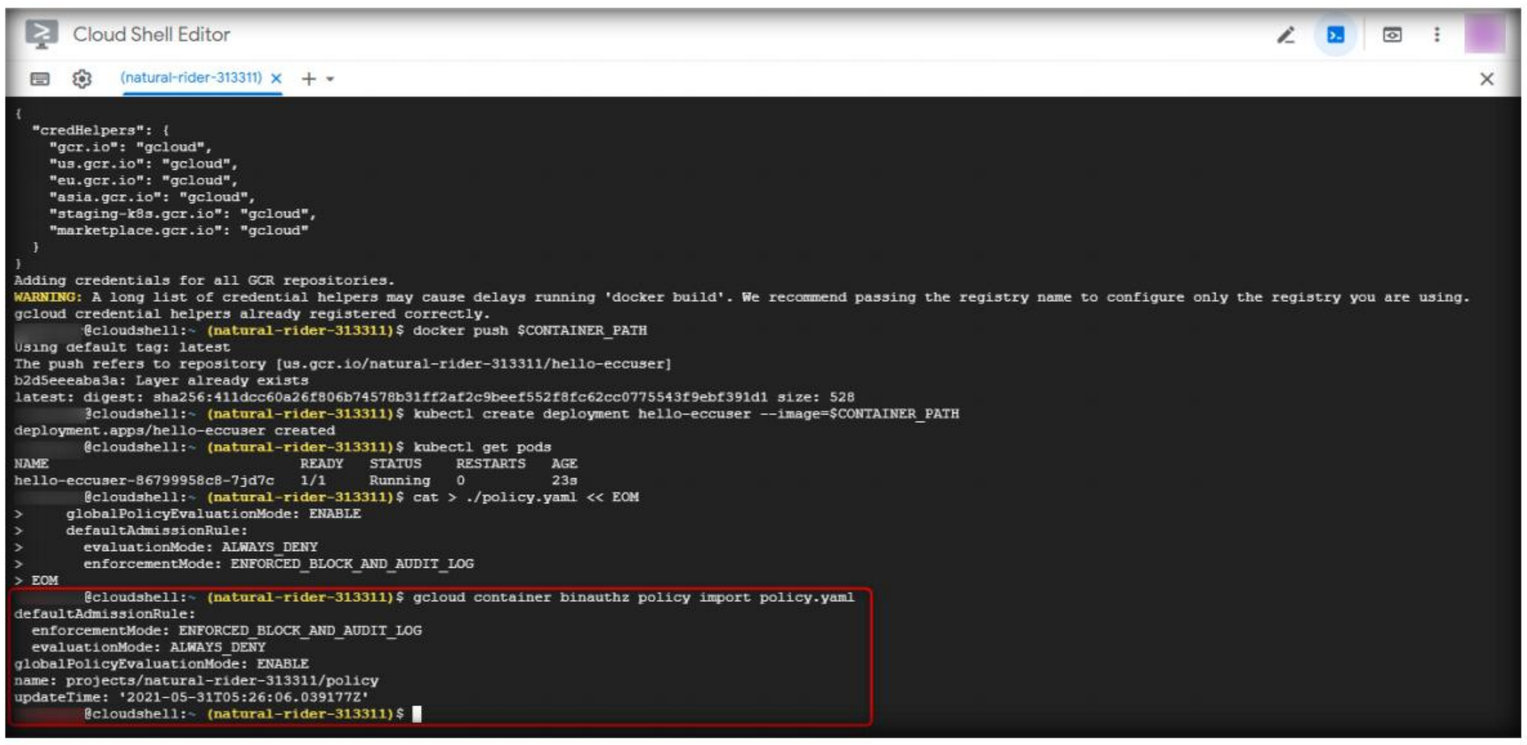


FIGURE 2.9.26: Applying Policy

27. Now, you can test your policy. The policy can be verified to ensure that no custom images are deployed on the cluster. For that, first, delete the pod by running the below two commands step by step.

```
kubectl delete deployment --all

kubectl delete event --all
```

h1de01.ir

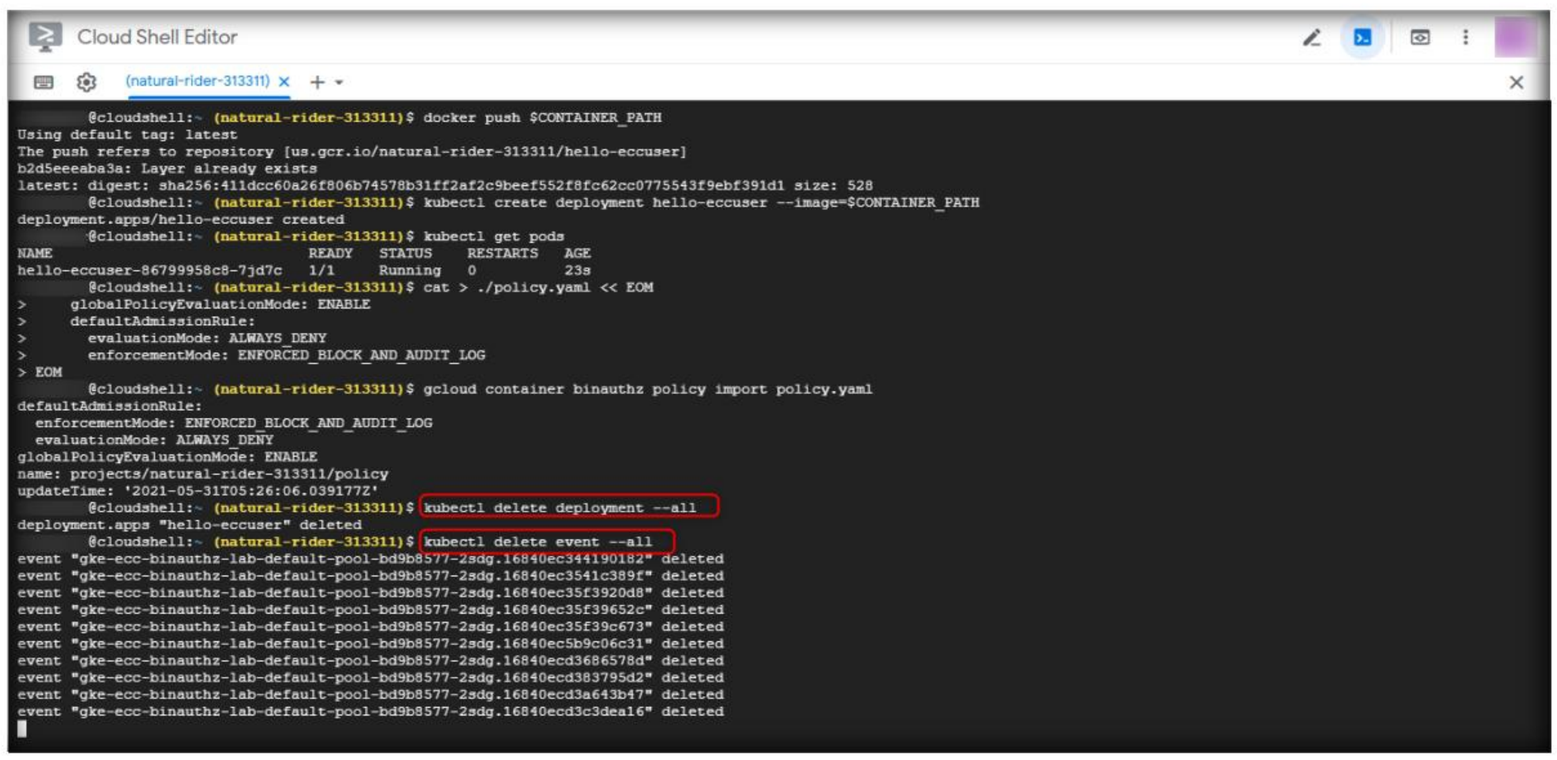


FIGURE 2.9.27: Deleting Pods

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

28. Now run the container on the cluster again by running the following command.

```
kubectl create deployment hello-eccuser --
image=$CONTAINER_PATH
```

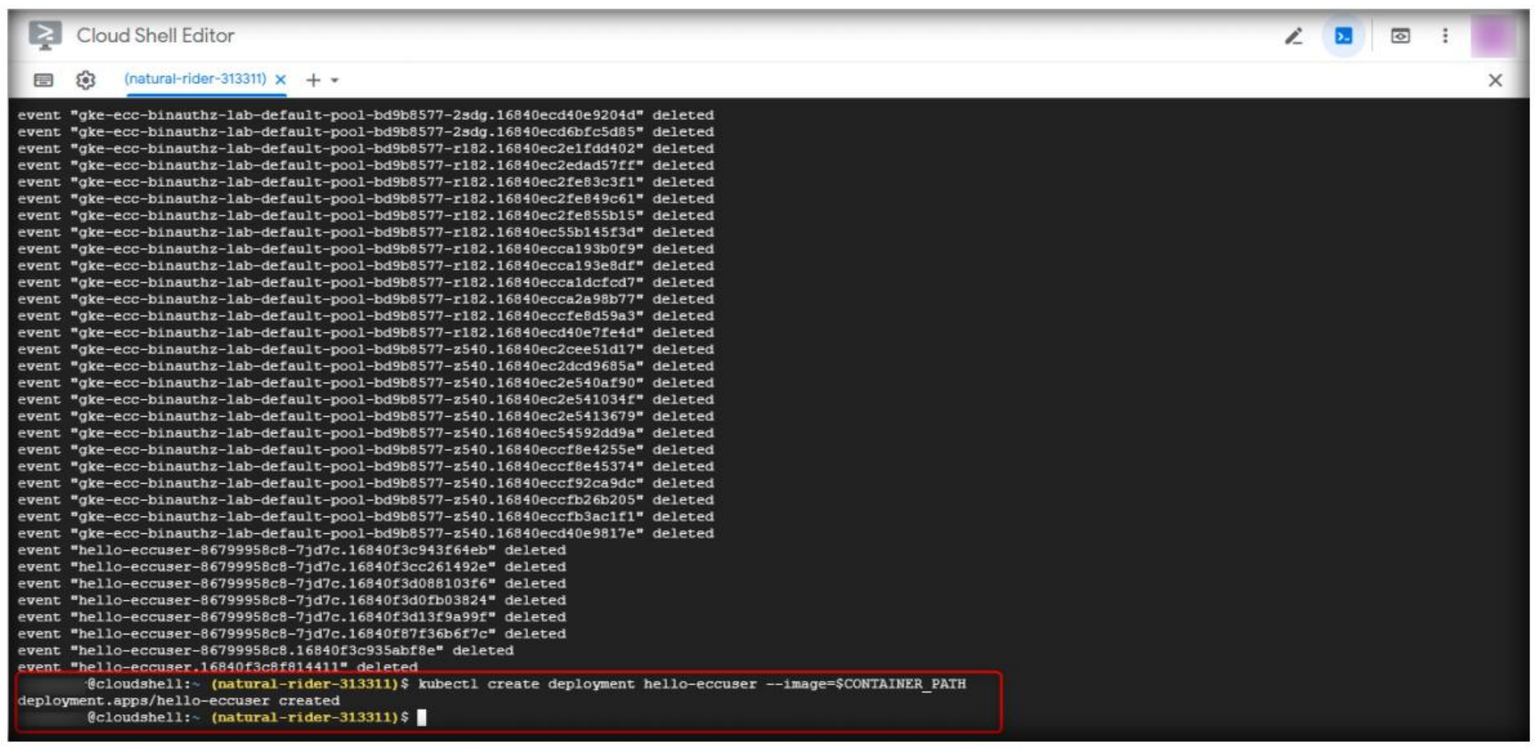


FIGURE 2.9.28: Created the container again

29. Now, type the following command and press **Enter** to verify if there are running pods.

```
kubectl get pods
```

Note: `kubectl` verified the pod with the configured policy and did not accept it since it does not follow the policy

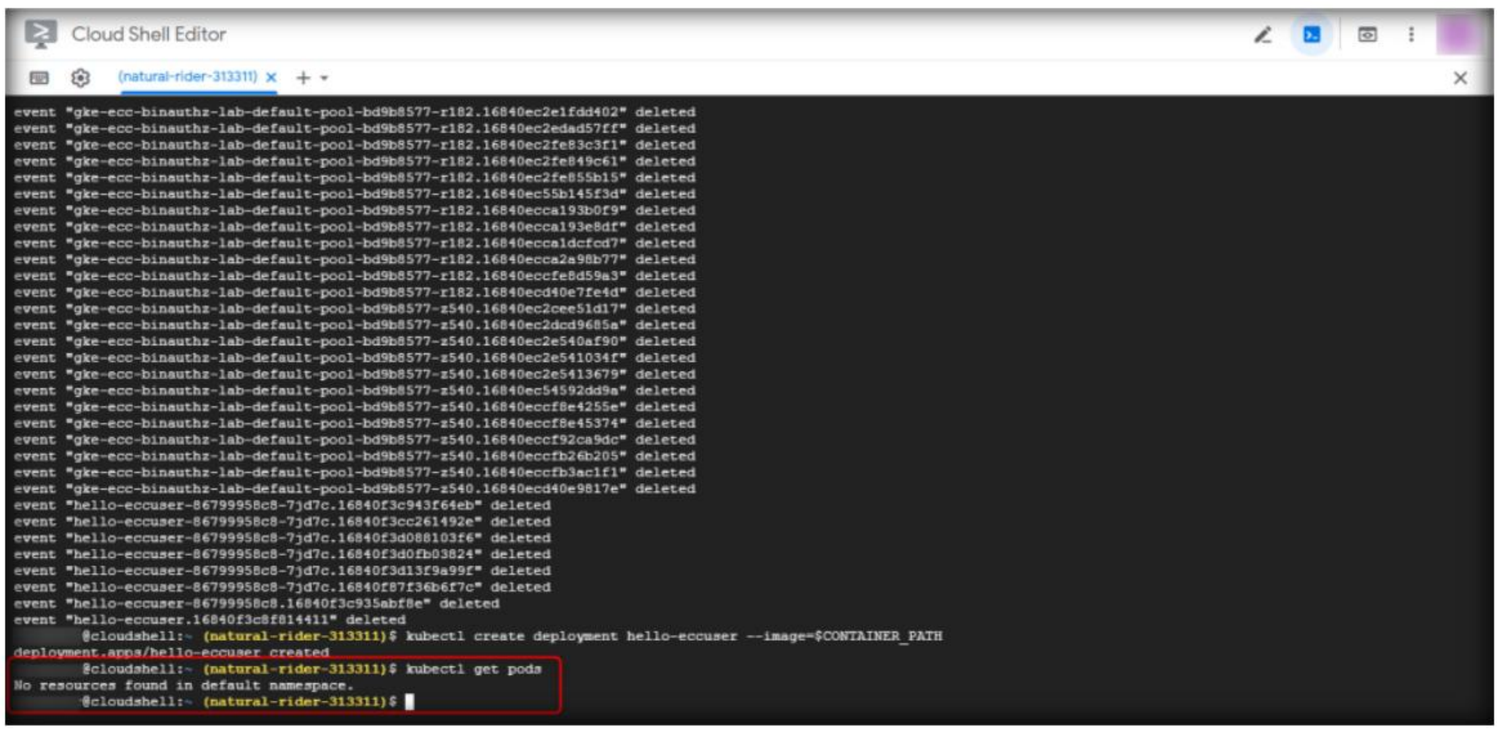


FIGURE 2.9.29: Checking pods

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 3

Configuration of Attestor

30. Now, since the policy is created, the cluster blocks the images that are not trusted. Here, you will create an attestor, the trusted party, to allow the deployment of images. First, you need to create a **Container Analysis Note.**

    Note: In Container Analysis API, **Note** is metadata that represents a single attestor

31. First, you need to create a **JSON file** that contains the **Note**. Run the following command to create a JSON file with Note.

    Note: Type the following command and press **Enter** line by line as shown in the screenshot below.

```
cat > ./create_note_request.json << EOM
{
  "attestation": {
    "hint": {
      "human_readable_name": "This note
represents an attestation authority"
    }
  }
}
EOM
```

hide01.ir

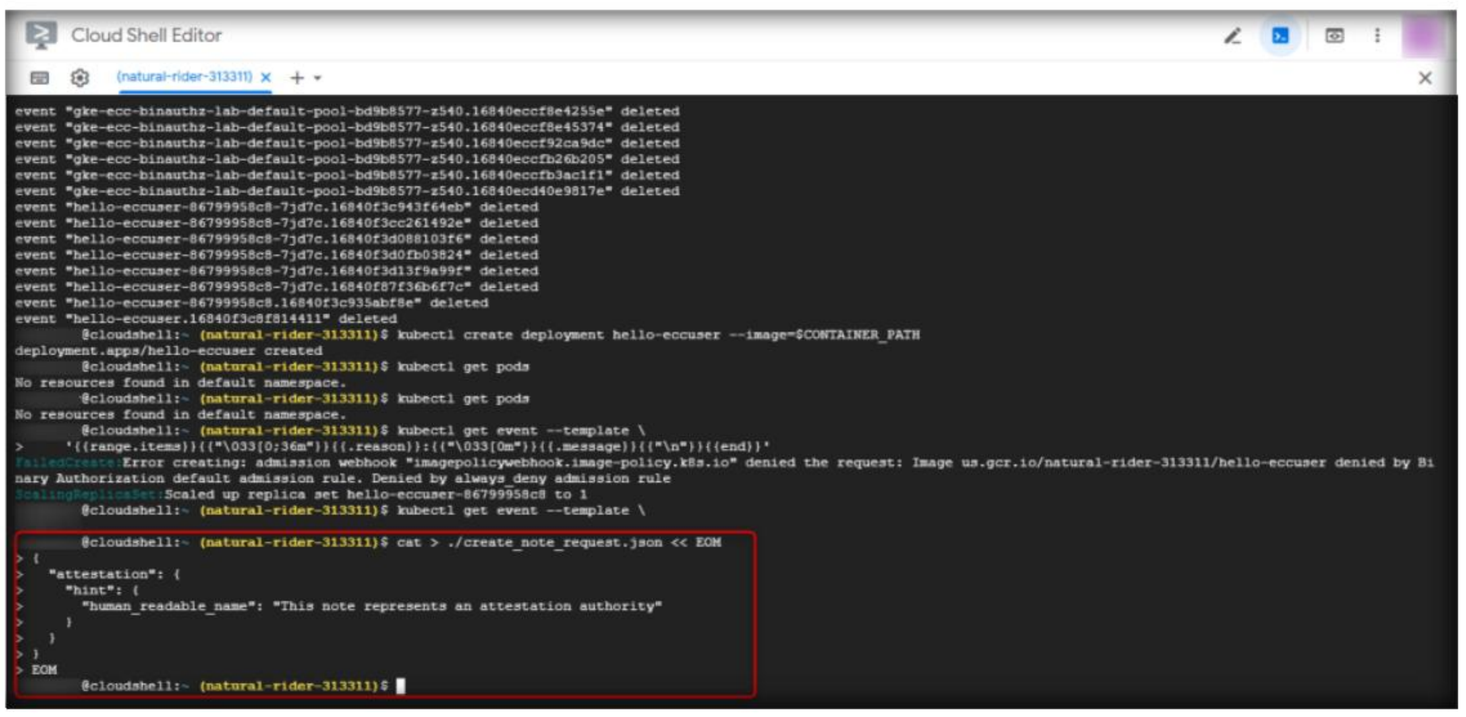


FIGURE 2.9.30: Adding User to Group

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

32. Next, you need to submit the **Note** to your project by running the following two commands step by step.

    Note: Type the following command and press **Enter** line by line as shown in the screenshot below.

```
export NOTE_ID=my-attestor-note

curl -vvv -X POST \

    -H "Content-Type: application/json"  \

    -H "Authorization: Bearer $(gcloud auth
print-access-token)"  \

    --data-binary @./create_note_request.json
\

    "https://containeranalysis.googleapis.com/v1/pr
ojects/${PROJECT_ID}/notes/?noteId=${NOTE_ID}"
```

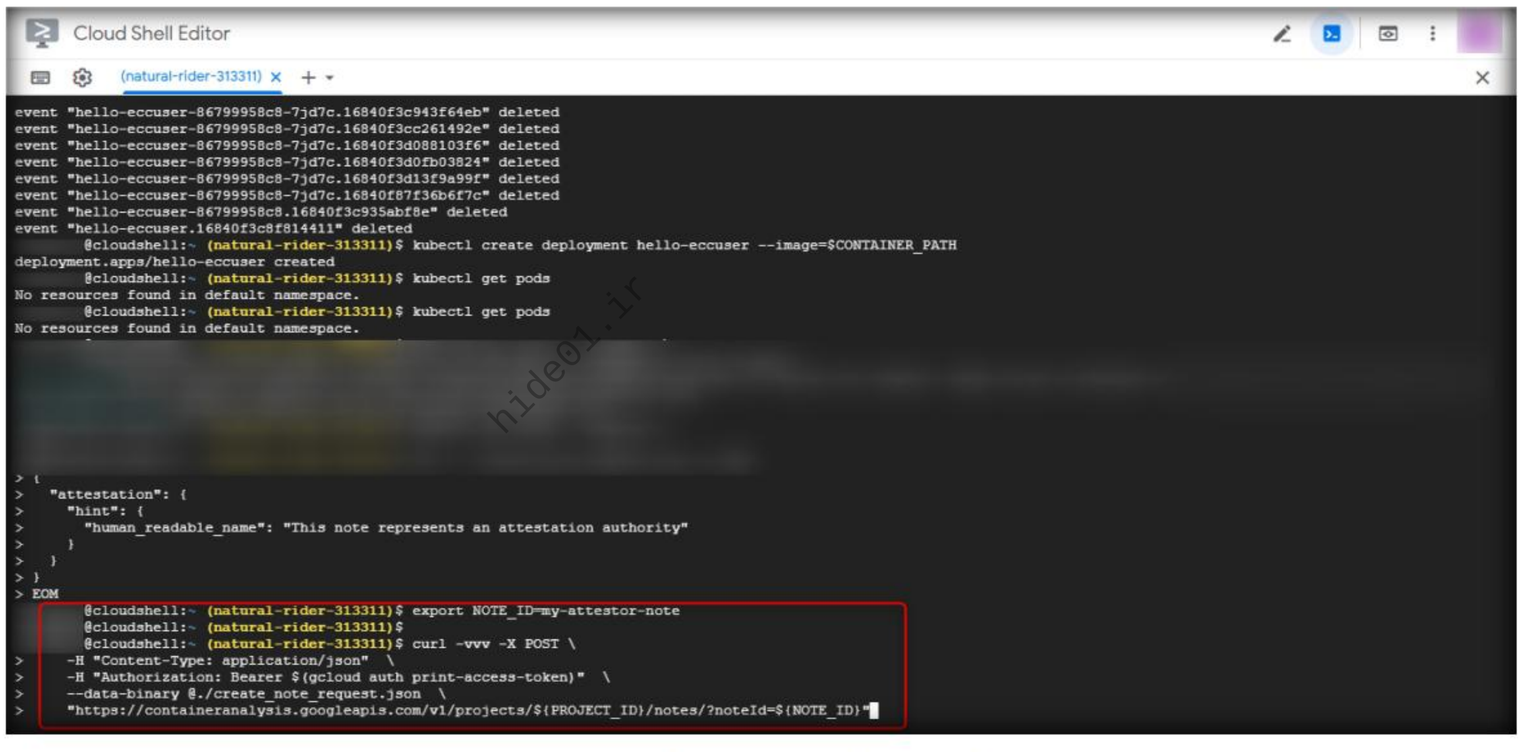


FIGURE 2.9.31: Submitting Note to Project

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

33. Wait for the process to get complete, and you will get output as below,

```
"name": projects/[PROJECT_ID]/notes/my-
attestor-note,

"kind": "ATTESTATION"
```

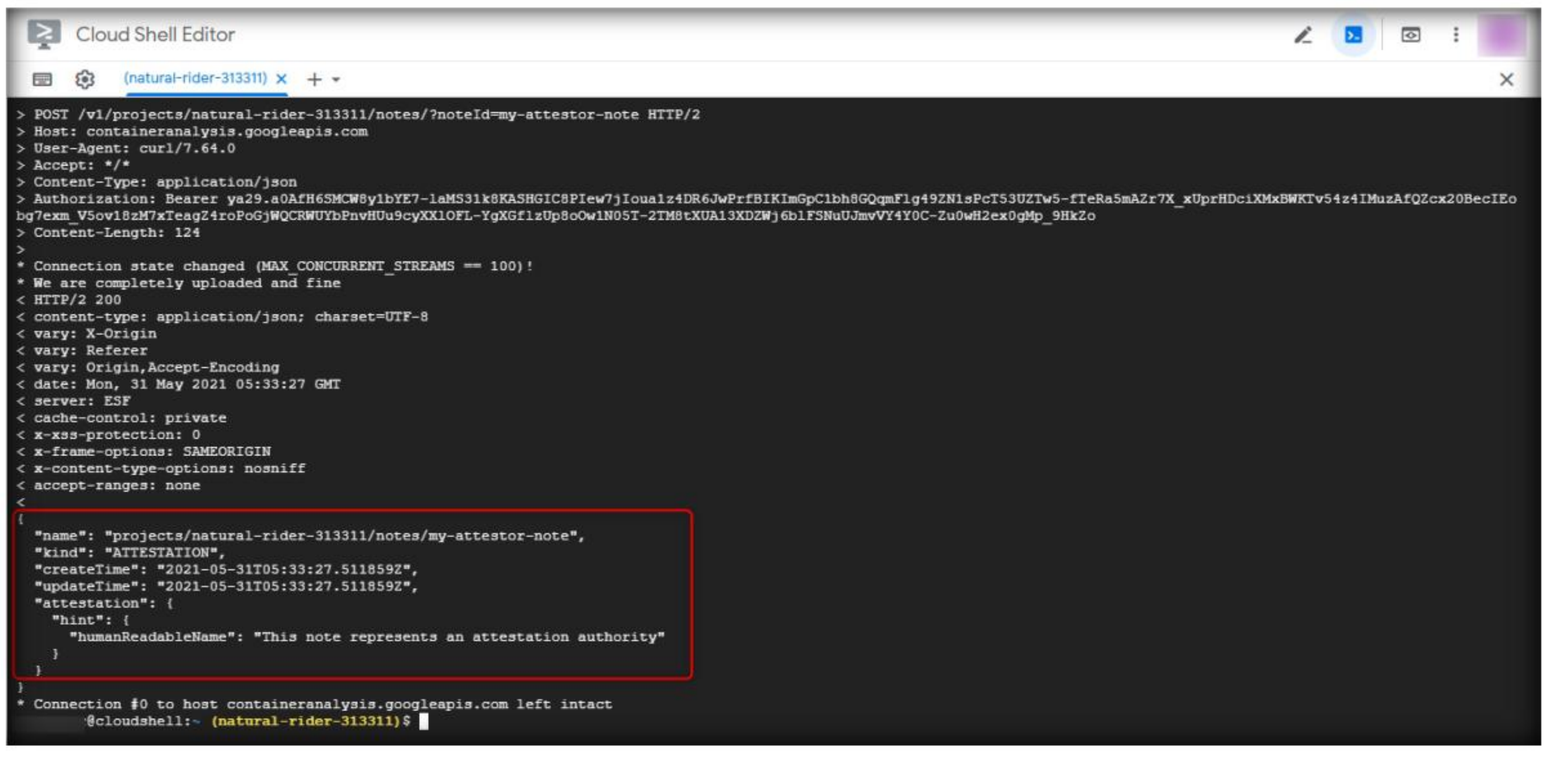


FIGURE 2.9.32: Output of Submitting Note to the Project

34. Now, you need to register the **Container Analysis API Note** with **Binary Authorization** to use the attestor. Run the below two commands step by step.

Note: Type the following command and press **Enter** line by line as shown in the screenshot below.

```
export ATTESTOR_ID=my-binauthz-attestor

gcloud container binauthz attestors create
$ATTESTOR_ID \

--attestation-authority-note=$NOTE_ID \

--attestation-authority-note-
project=${PROJECT_ID}
```

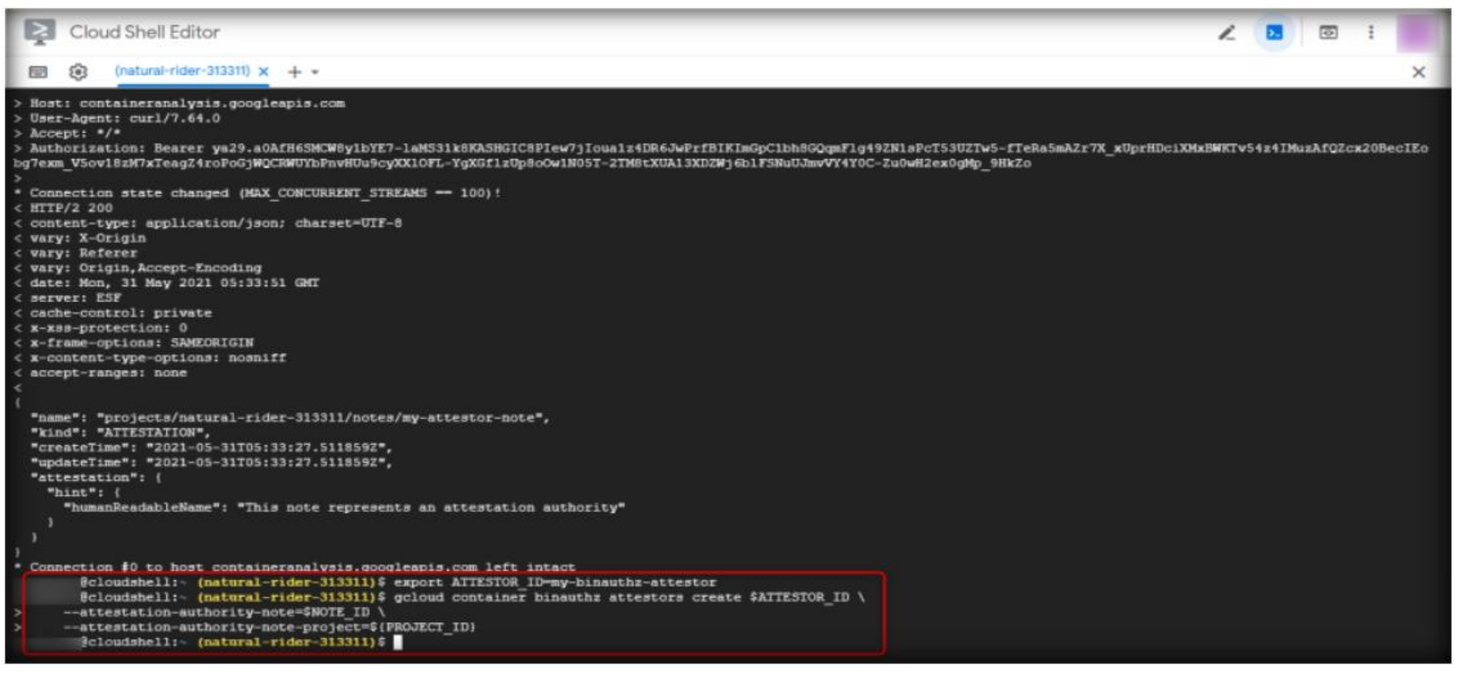


FIGURE 2.9.33: Registering Note with Binary Authorization

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

35. Next, type the following command and press **Enter** to get the list of registered attestors.

```
gcloud container binauthz attestors list
```

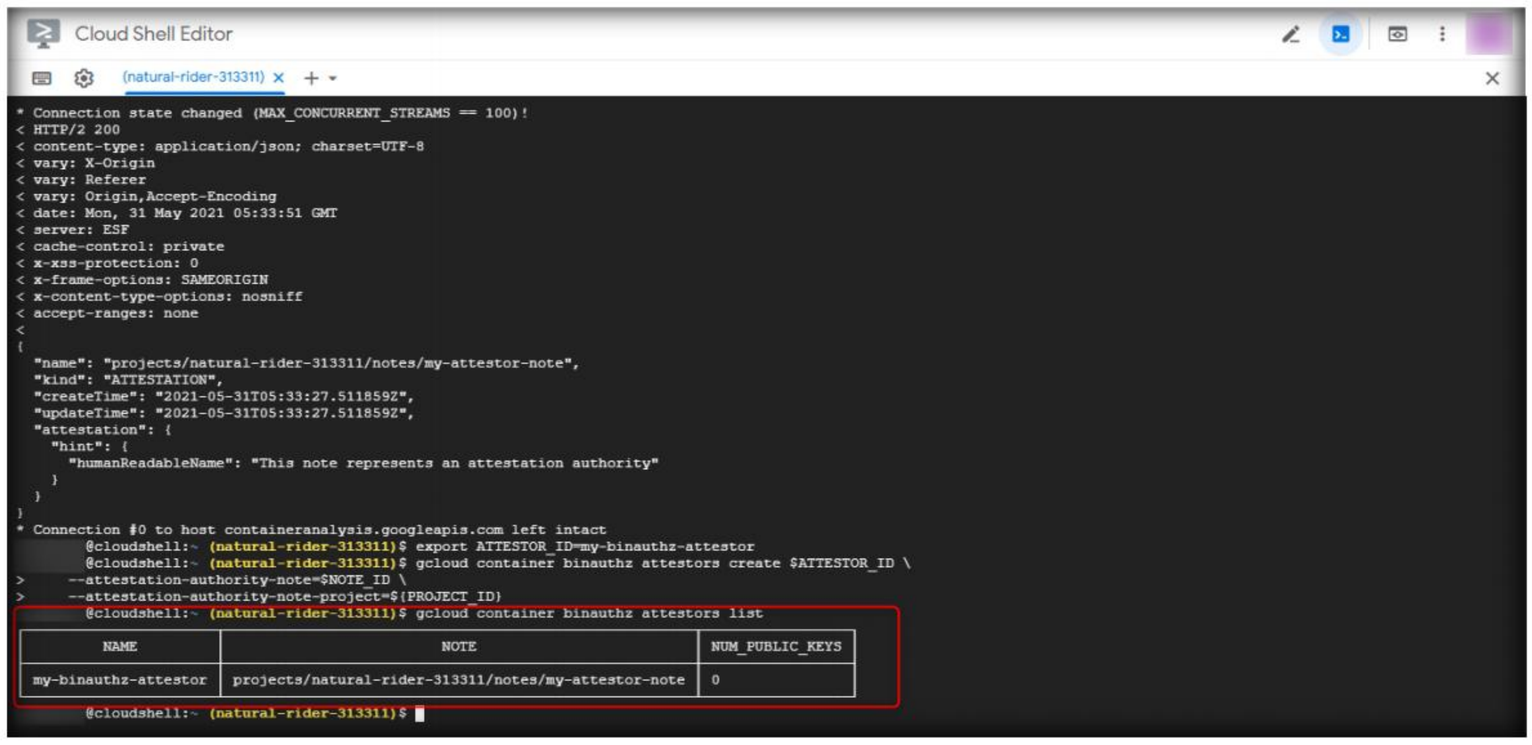


FIGURE 2.9.34: Attestors List

36. Next, you need to create a cryptographic key to sign the container images. First, add the environment variables by running the following commands step by step.

```
export KEY_LOCATION=global
export KEYRING=binauthz-keys
export KEY_NAME=lab-key
export KEY_VERSION=1
```

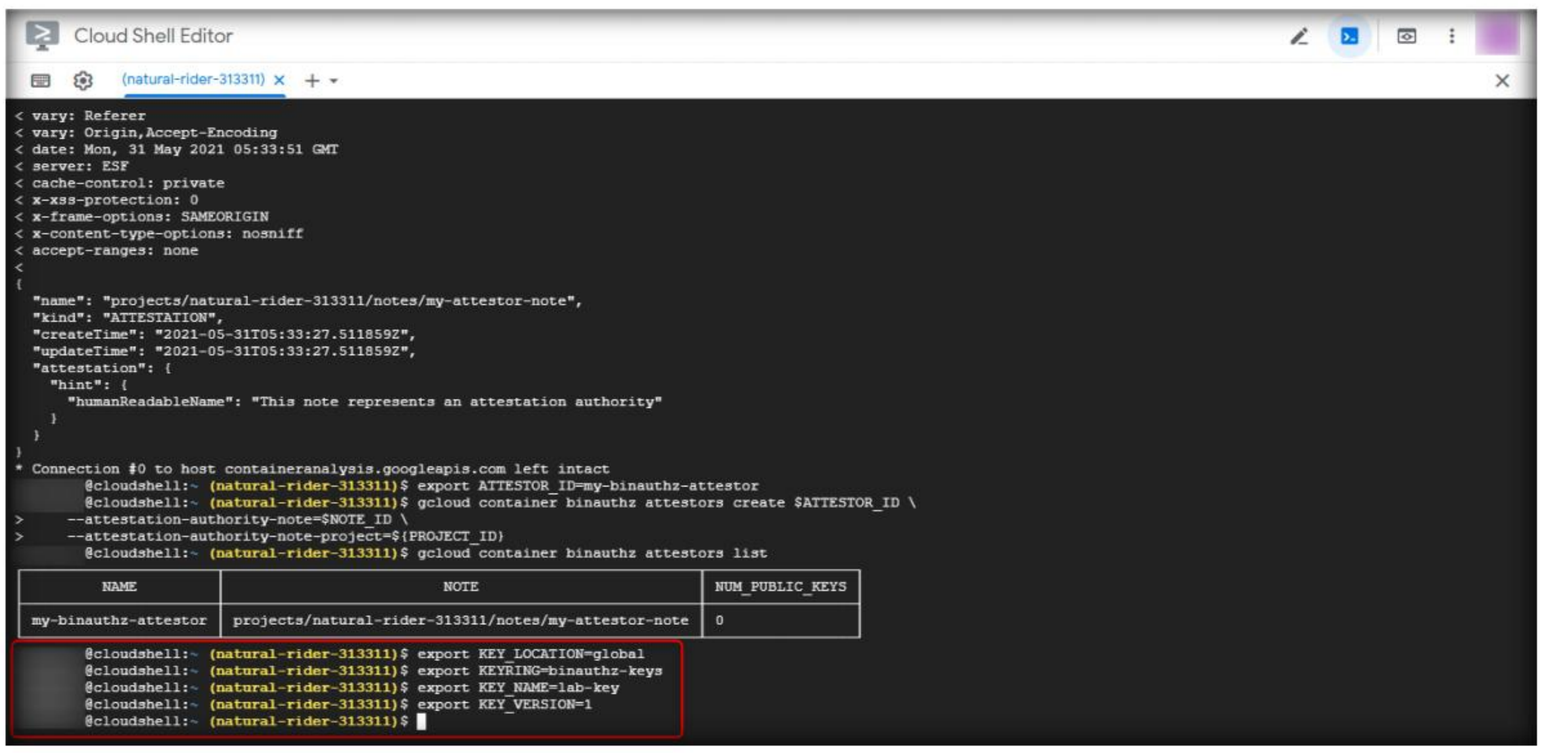


FIGURE 2.9.35: Adding Environment Variables

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

37. Next, type the following command and press **Enter** to create a keyring.

```
gcloud kms keyrings create "${KEYRING}" --
location="${KEY_LOCATION}"
```

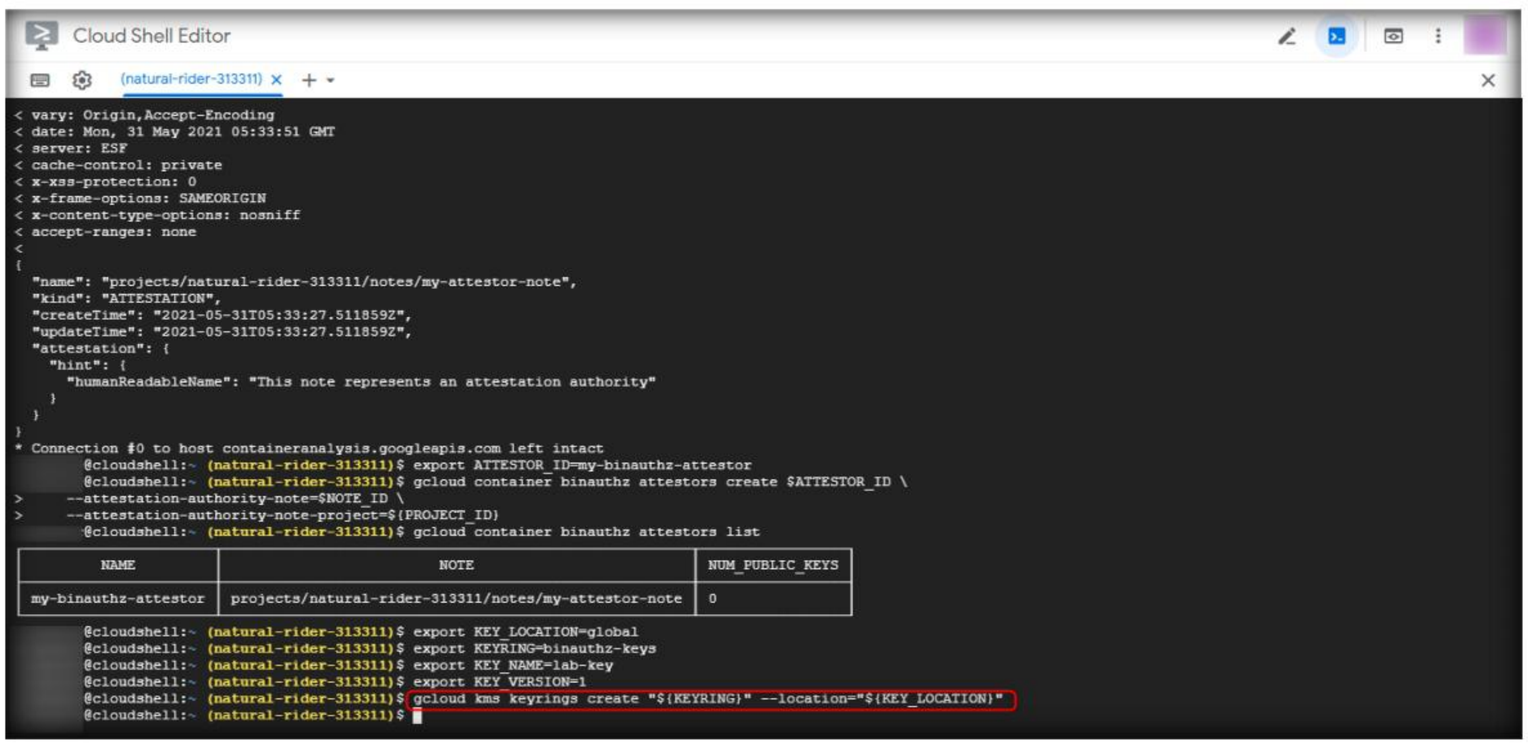


FIGURE 2.9.36: Creating Key Ring

38. After you created the key ring, you have to create the asymmetric key pair for the attestor. Run the following command to create the asymmetric key pair.

Note: Type the following command and press **Enter** line by line as shown in the screenshot below.

```
gcloud kms keys create "${KEY_NAME}" \
    --keyring="${KEYRING}" --
location="${KEY_LOCATION}" \
    --purpose asymmetric-signing  --default-
algorithm="ec-sign-p256-sha256"
```

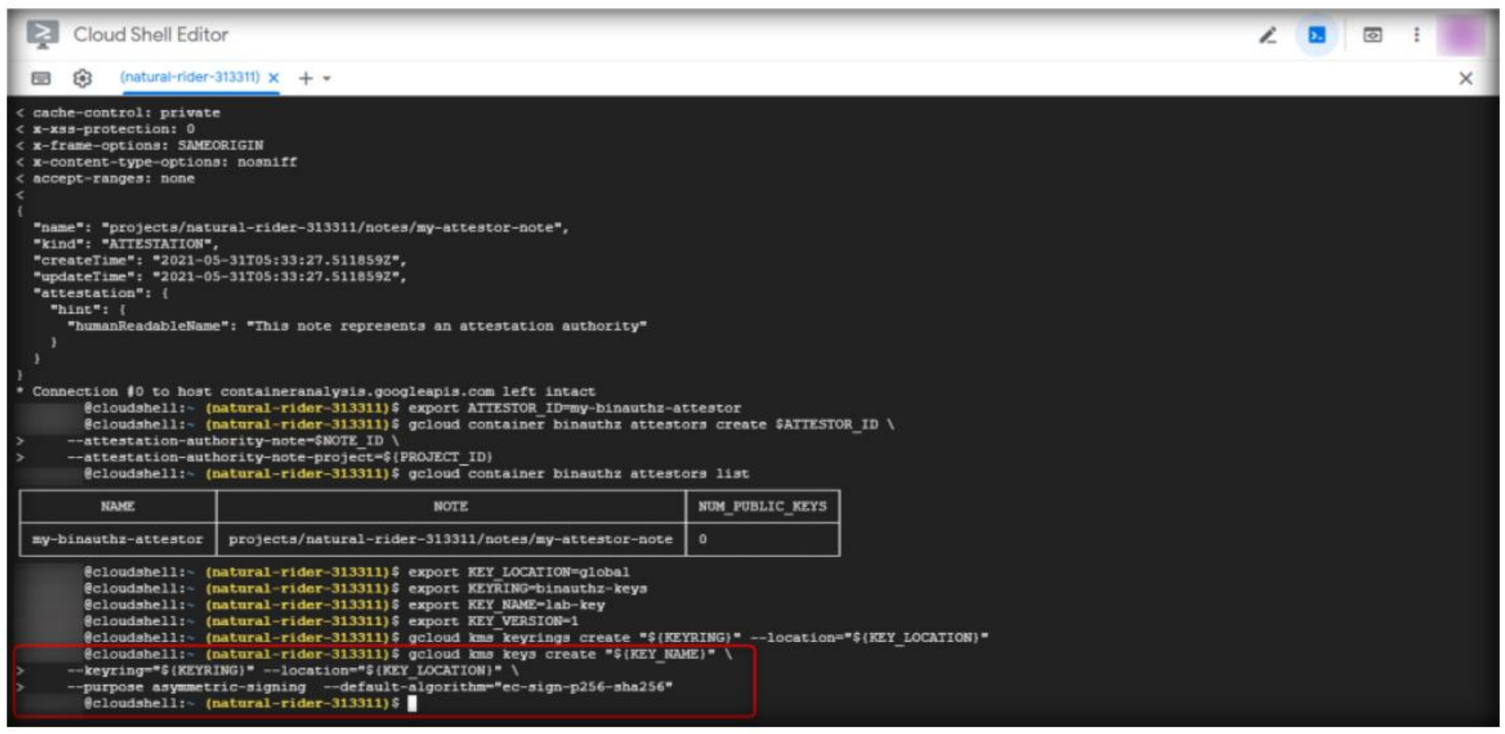


FIGURE 2.9.37: Creating Asymmetric Key

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

39. Next, you need to connect the key with authority. Run the following command to do so.

    Note: Type the following command and press **Enter** line by line as shown in the screenshot below.

```
gcloud beta container binauthz attestors
public-keys add  \
    --attestor="${ATTESTOR_ID}"  \
    --keyversion-project="${PROJECT_ID}"  \
    --keyversion-location="${KEY_LOCATION}" \
    --keyversion-keyring="${KEYRING}" \
    --keyversion-key="${KEY_NAME}" \
    --keyversion="${KEY_VERSION}"
```

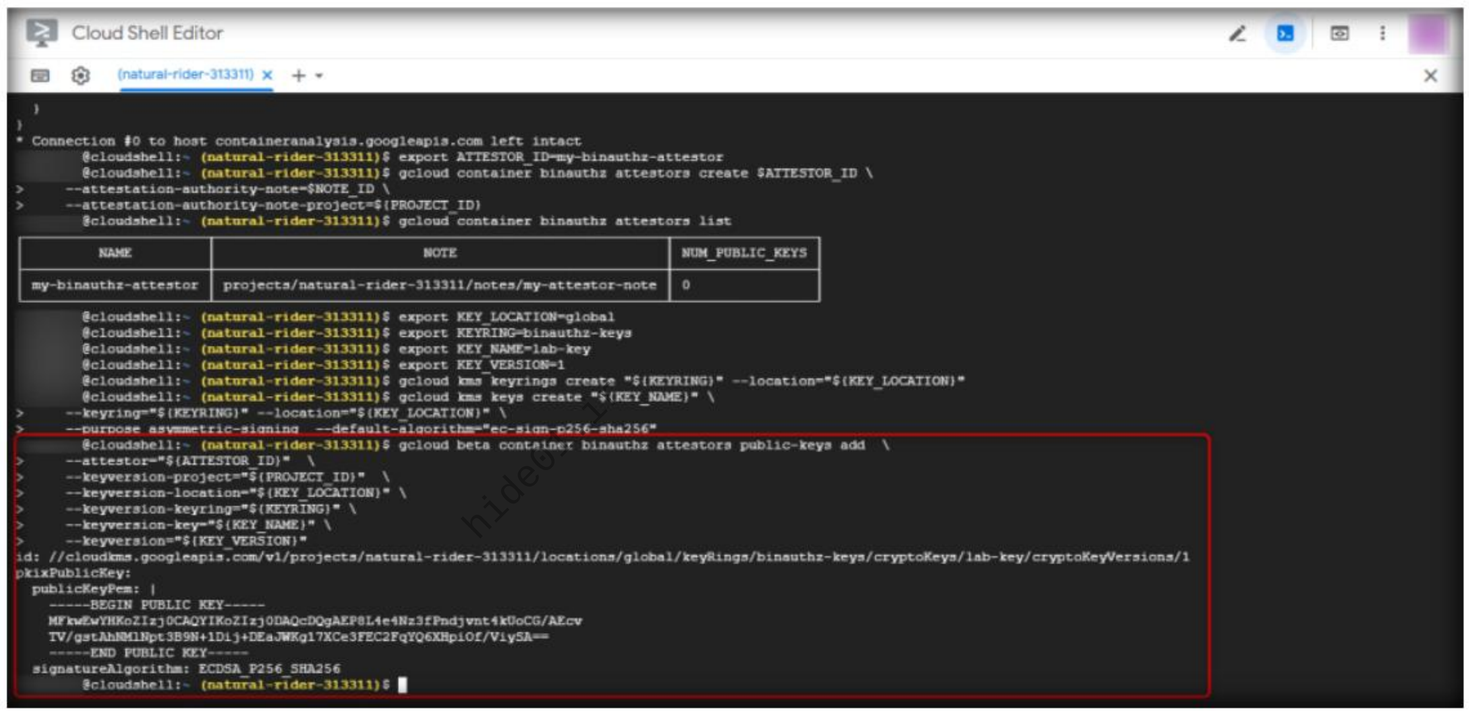


FIGURE 2.9.38: Connecting the key with authority

40. Now, you need to verify whether the key is registered. Run the following command to list the authorities. You will see one key registered under NUM_PUBLIC_KEYS.

```
gcloud beta container binauthz attestors list
```

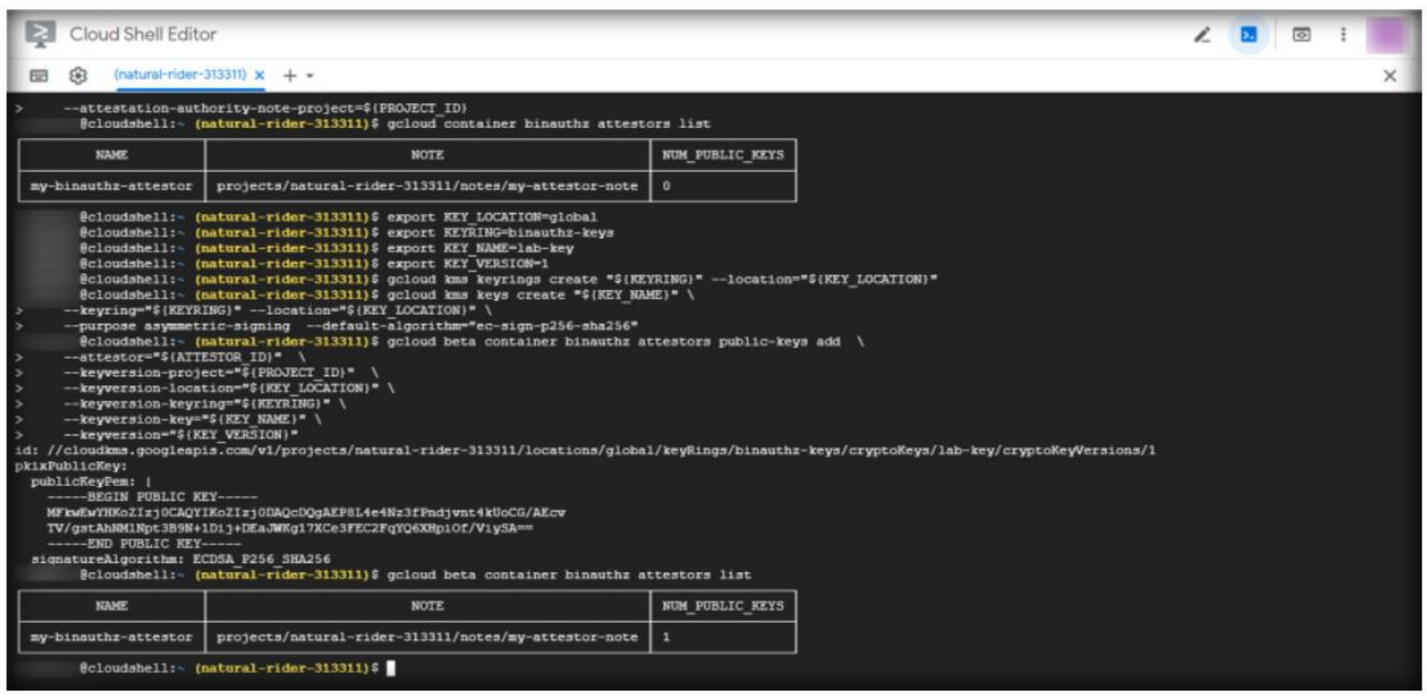


FIGURE 2.9.39: Key is Registered

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 4

Signing the Container Image

41. Now, the attestor is configured. With this attestor, you need to attest the container image **hello-eccuser,** to define that it is safe to deploy. Run the following command to find the digest for the container image.

    Note: Type the following command and press Enter line by line as shown in the screenshot below.

```
export DIGEST=$(gcloud container images describe
${CONTAINER_PATH}:latest \
    --format='get(image_summary.digest)')
```

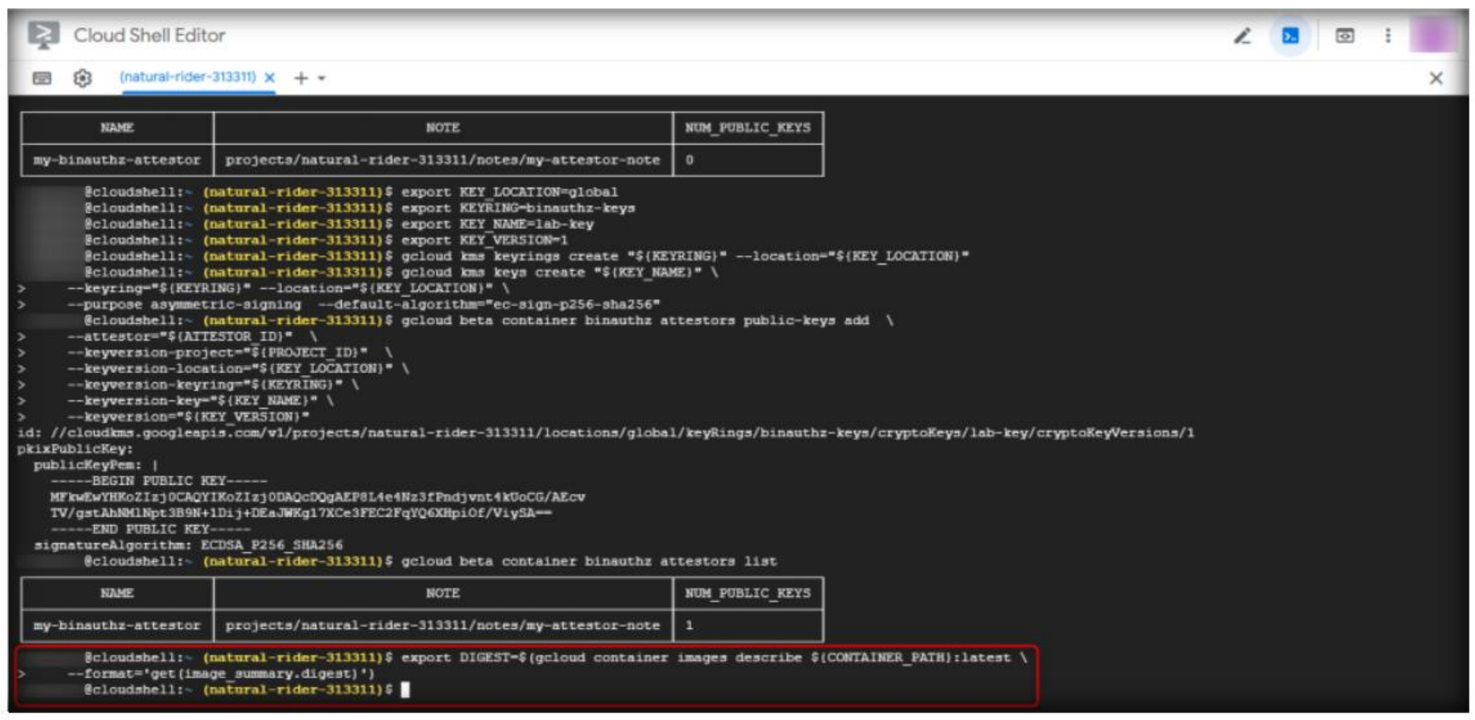


FIGURE 2.9.40: Finding Digest for Container Image

42. Now, you can perform the attestation by running the following command.

    Note: Type the following command and press **Enter** line by line as shown in the screenshot below.

```
gcloud beta container binauthz attestations
sign-and-create  \
    --artifact-
url="${CONTAINER_PATH}@${DIGEST}" \
    --attestor="${ATTESTOR_ID}" \
    --attestor-project="${PROJECT_ID}" \
    --keyversion-project="${PROJECT_ID}" \
    --keyversion-location="${KEY_LOCATION}" \
    --keyversion-keyring="${KEYRING}" \
    --keyversion-key="${KEY_NAME}" \
    --keyversion="${KEY_VERSION}"
```


Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

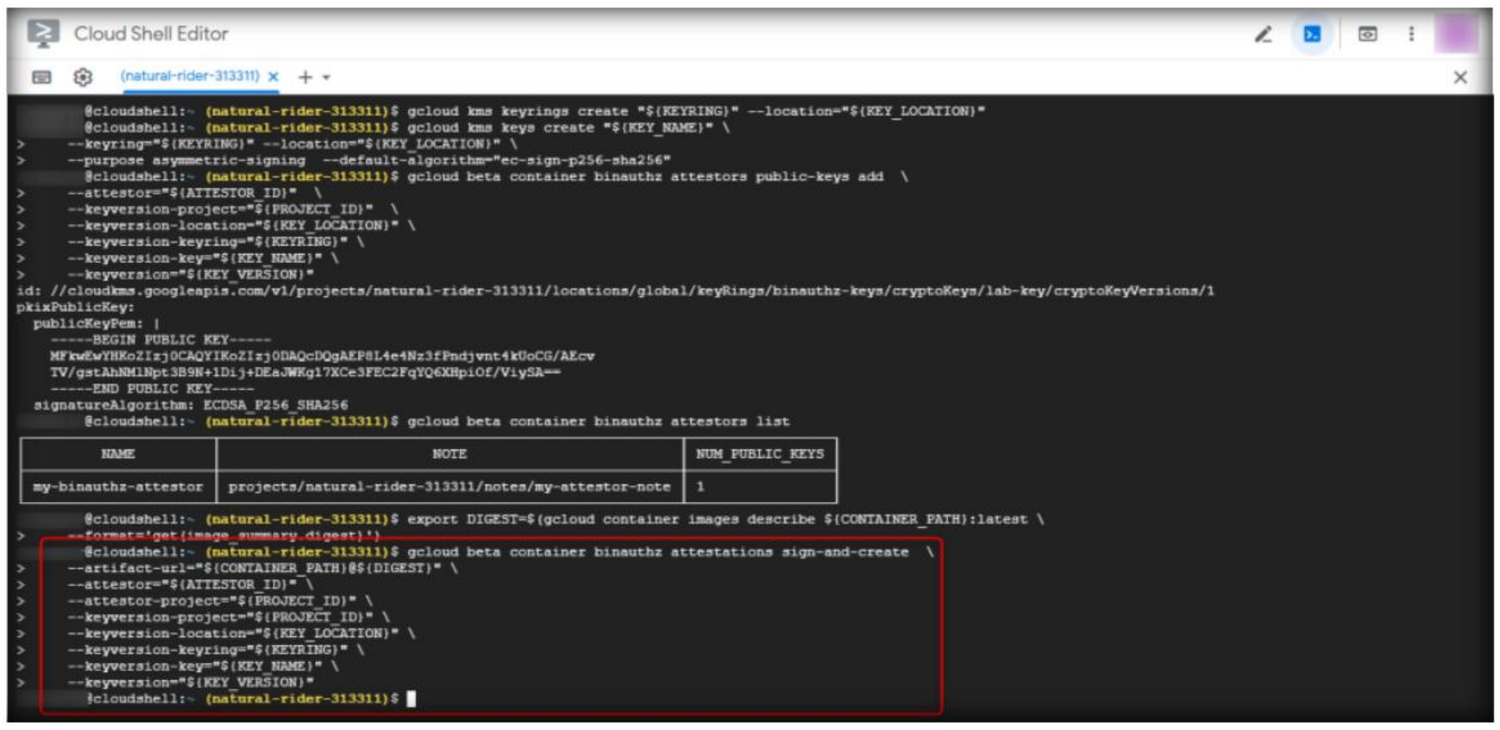


FIGURE 2.9.41: Performing Attestation

43. Now, run the following command to list the attestations to verify that the attestation is implemented successfully.

Note: Type the following command and press **Enter** line by line as shown in the screenshot below.

```
gcloud container binauthz attestations list \
   --attestor=$ATTESTOR_ID          --attestor-
project=${PROJECT_ID}
```

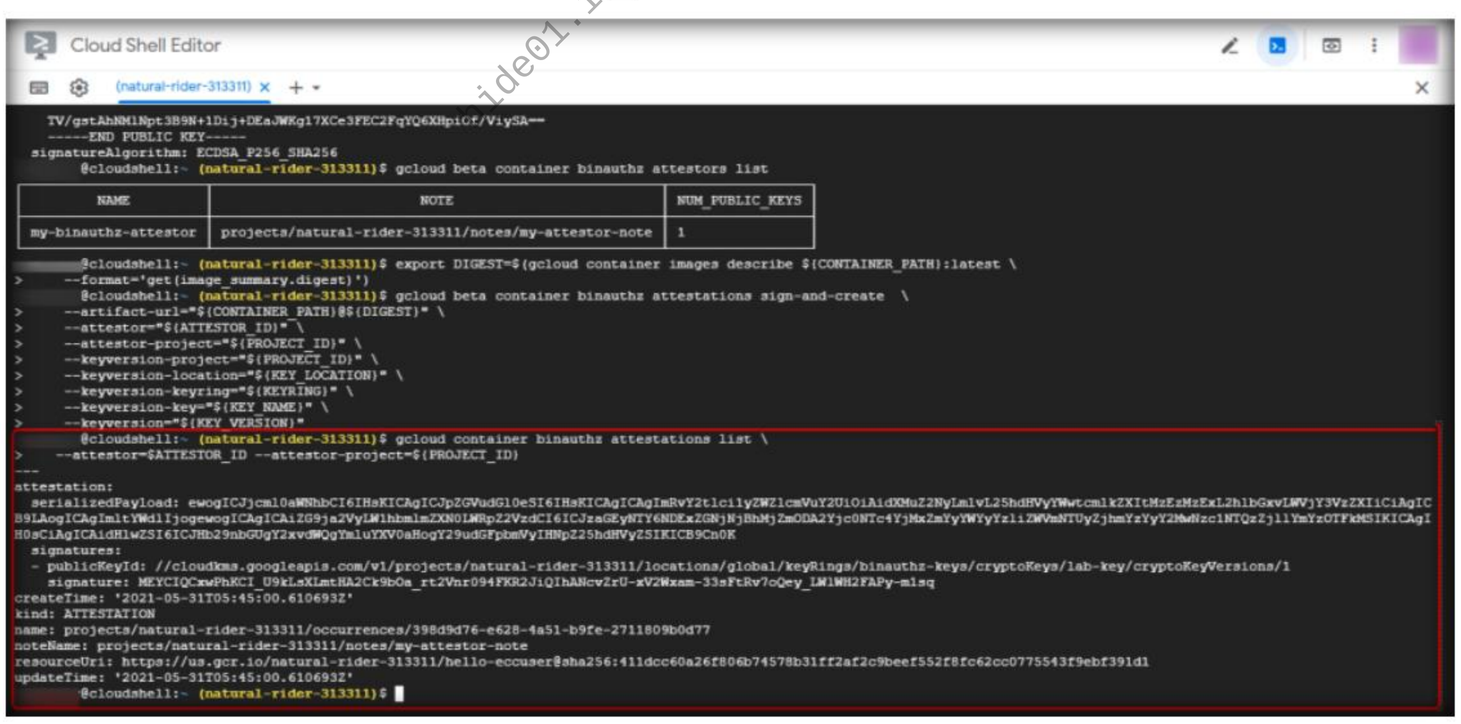


FIGURE 2.9.42: Verification of Attestation

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 5

Running Signed Container Image

44. Now, you need to run the verified container image in the cluster. First, you change the policy to permit only the running of all container images signed by the attestor. Run the following command to permit only signed images and block other images.

    Note: Type the following command and press Enter line by line as shown in the screenshot below.

```
cat << EOF > updated_policy.yaml
    globalPolicyEvaluationMode: ENABLE
    defaultAdmissionRule:
      evaluationMode: REQUIRE_ATTESTATION
      enforcementMode:
ENFORCED_BLOCK_AND_AUDIT_LOG
      requireAttestationsBy:
      -
projects/${PROJECT_ID}/attestors/${ATTESTOR_ID}
EOF
```

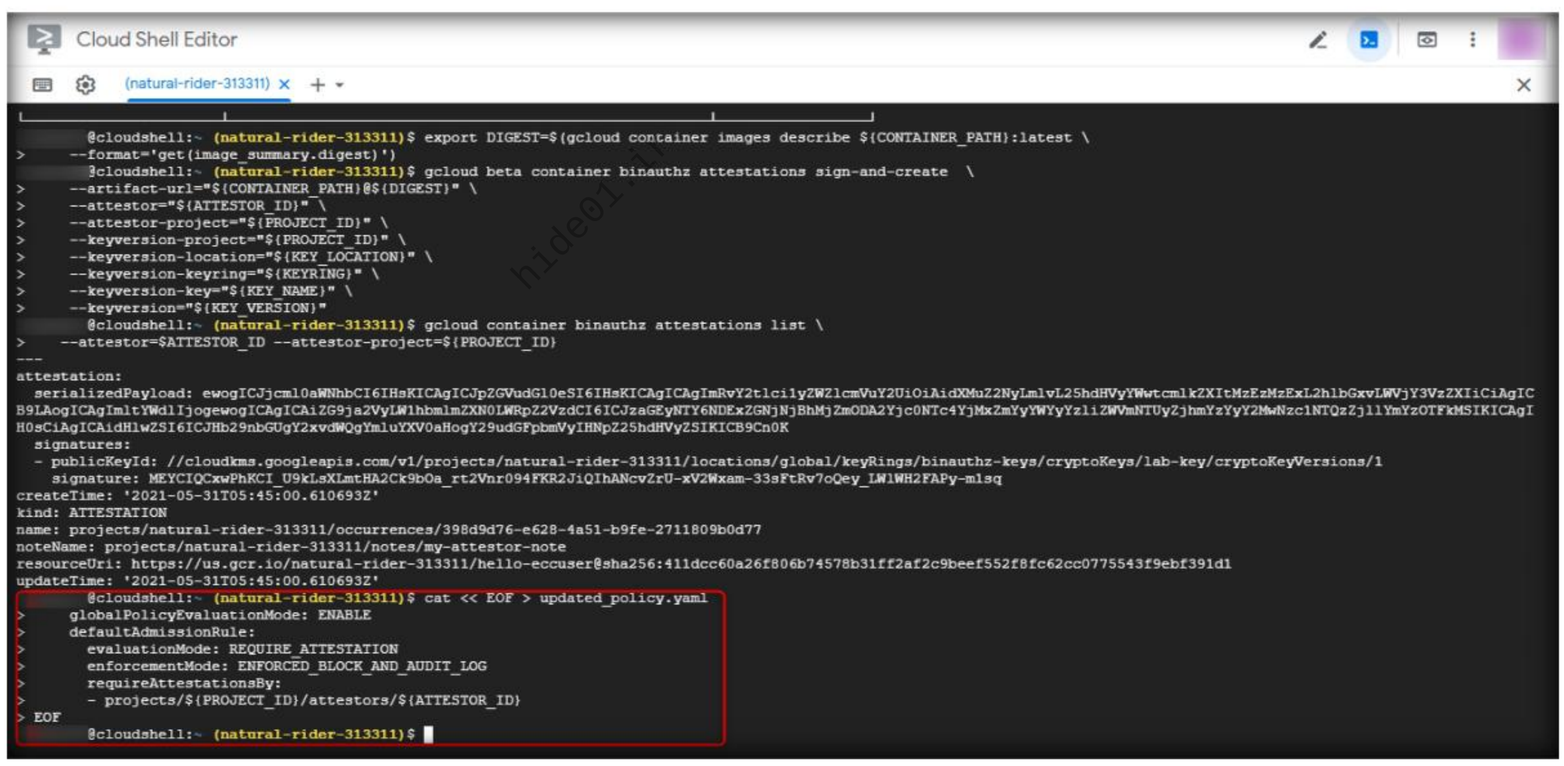


FIGURE 2.9.43: Creating New Policy

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

45. Next, run the below command to add the policy to Binary Authorization.

```
gcloud container binauthz policy import updated_policy.yaml
```

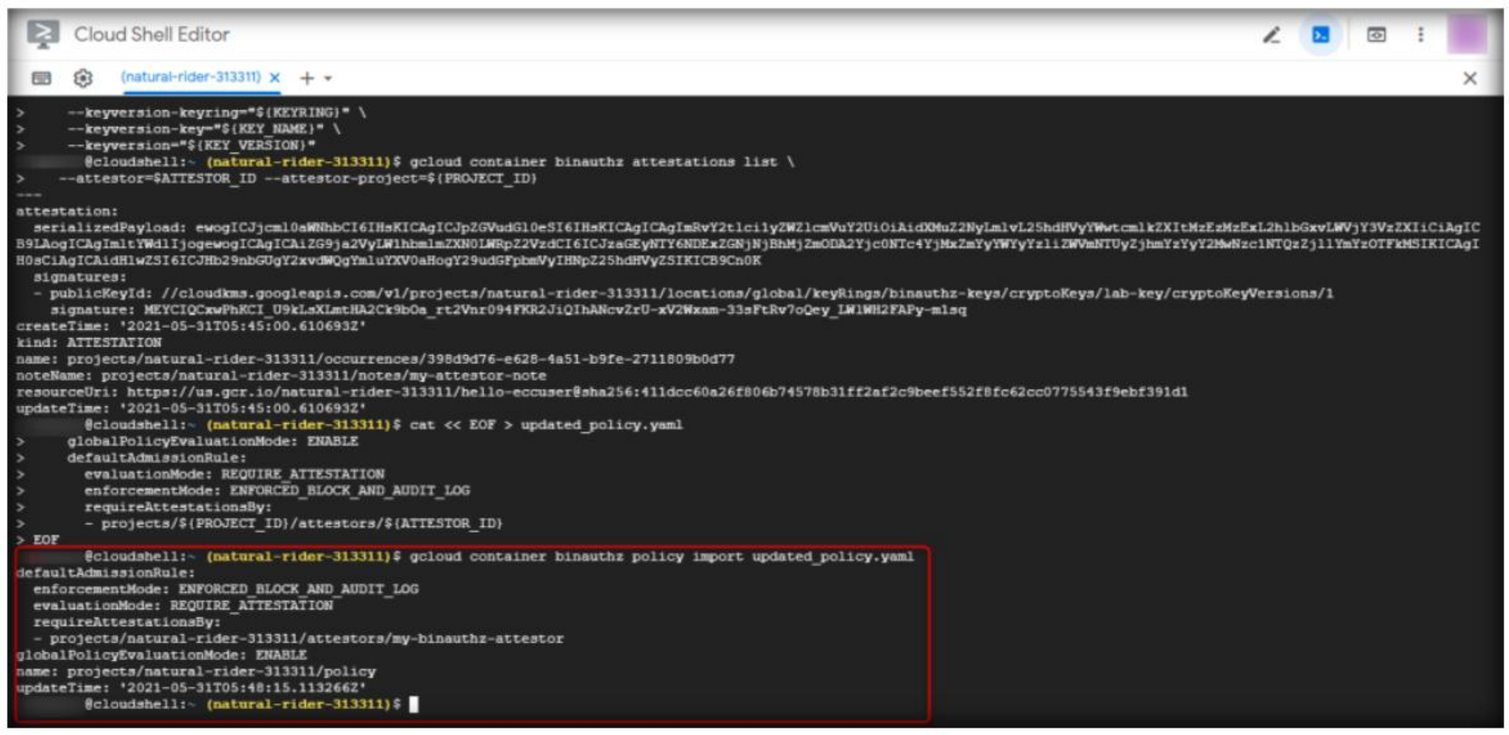


FIGURE 2.9.44: Adding Policy to Binary Authorization

46. Now, you can run the verified container image by running the command below.

```
kubectl create deployment hello-eccuser-signed --image="${CONTAINER_PATH}@${DIGEST}"
```

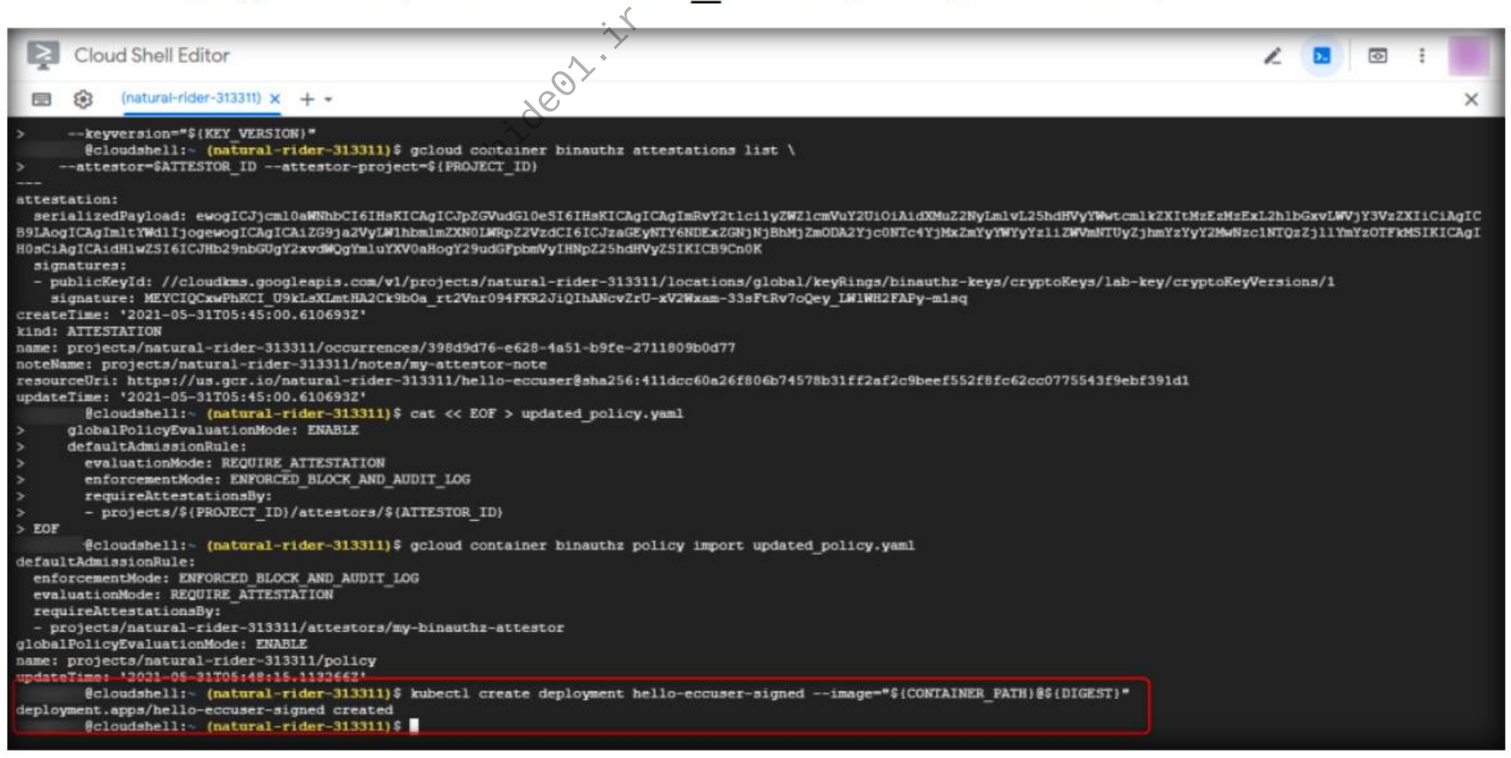


FIGURE 2.9.45: Running the Container Image

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

47. Now, ensure that the pod has matched the policy and is running by typing the following command and pressing **Enter.**

```
kubectl get pods
```

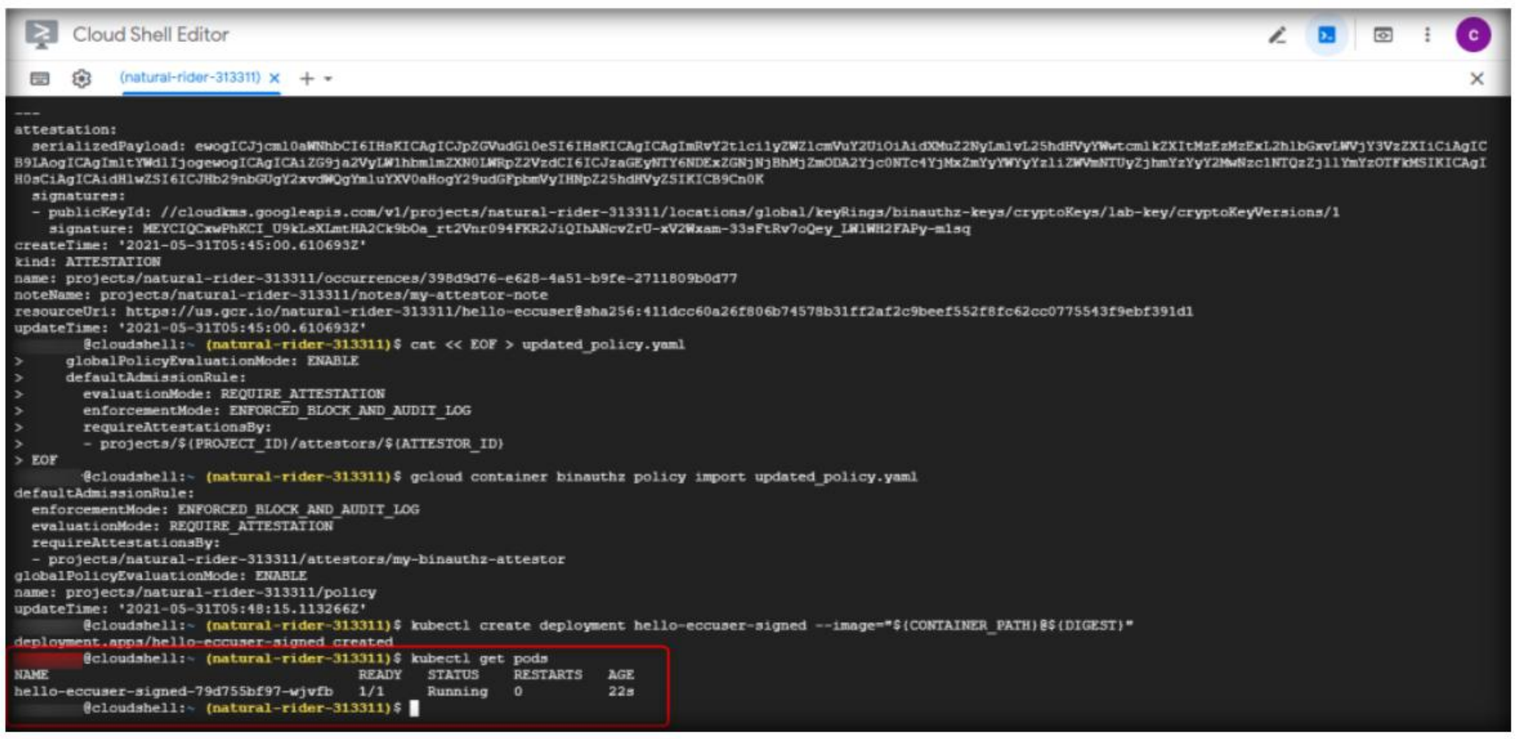


FIGURE 2.9.46: Verifying the status of the pod

48. You will get the **STATUS** of the pod as **Running**.

49. Now, go back to the GCP console and navigate to **Kubernetes Engine,** and select **Workloads** in the console.

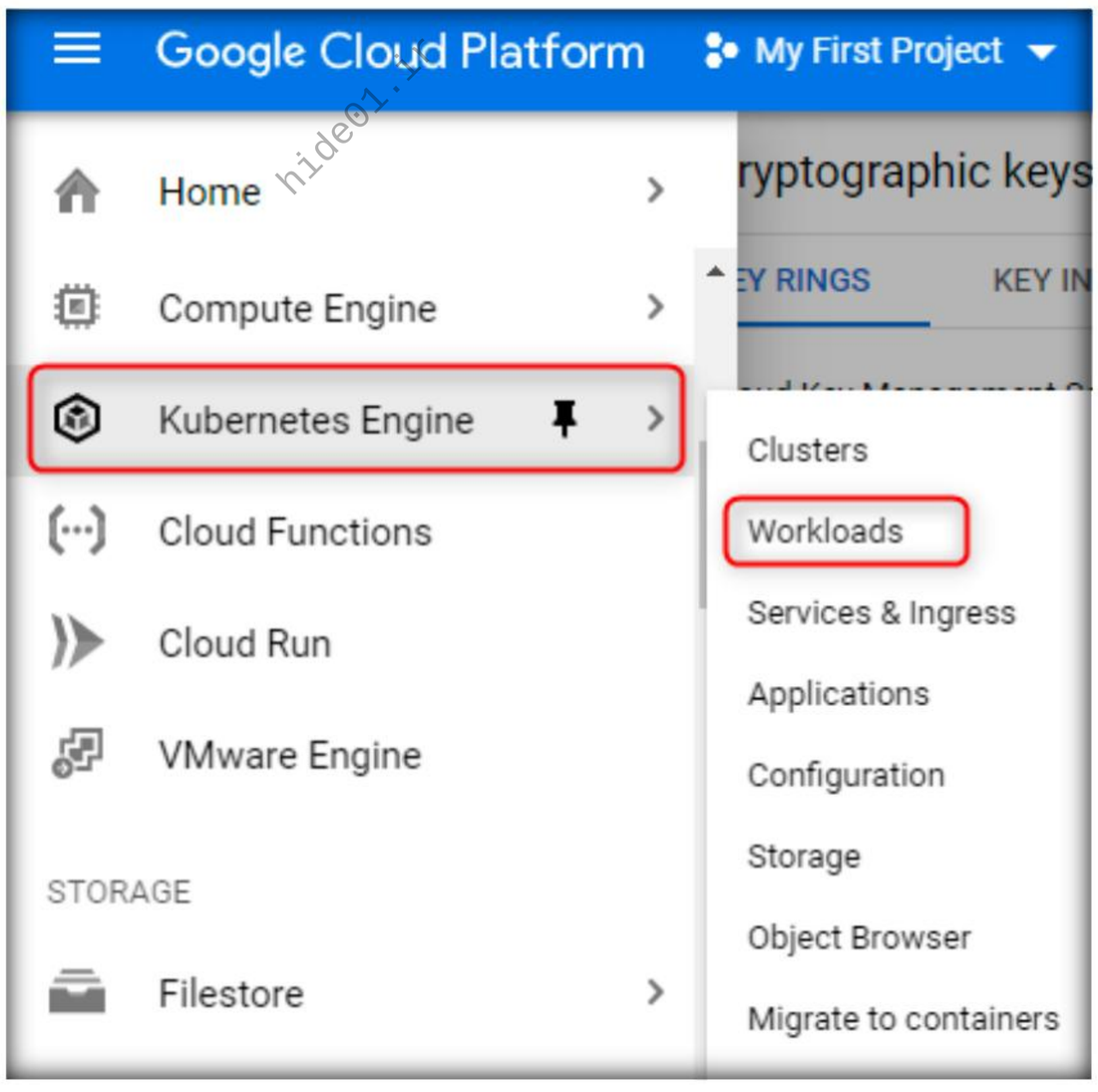


FIGURE 2.9.47: Navigating to Kubernetes Engine Workloads

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

50. In the **Workloads** window, you will get the status as **hello-eccuser-signed** with **Status** marked as **OK** with a green tick mark.

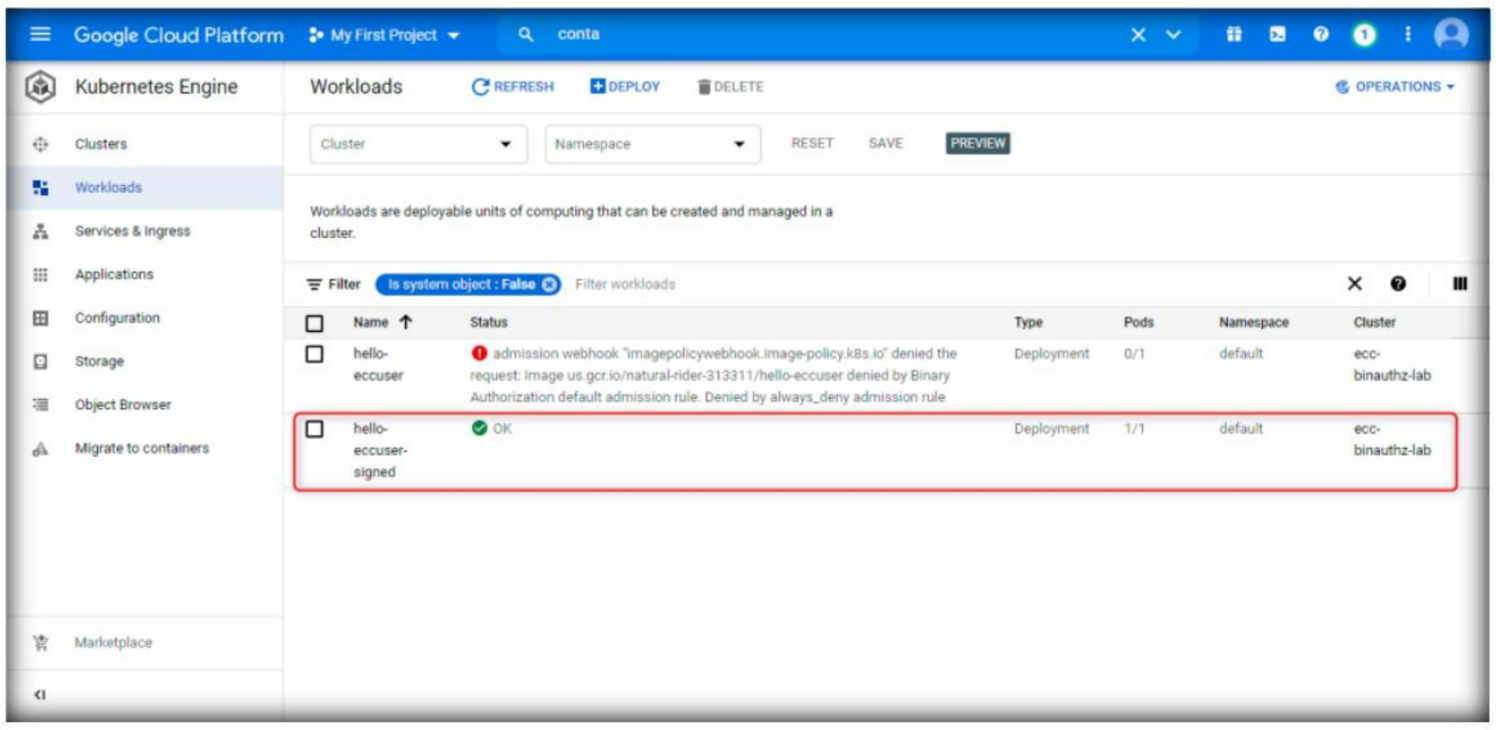


FIGURE 2.9.48: Verifying Kubernetes Engine workloads

51. Thus, with Binary Authorization, a cloud security engineer can perform secure deployment of container images in Google Kubernetes Engine (GKE).

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

34. Now, to delete the Binary Authorization Attestor that you have created for this lab, navigate to the **Binary Authorization** section in **Security**. Click on the ellipsis next to the attestor (here, **my-binauthz-attestor**) and click on **Delete**. In the pop-up window, select the checkbox and click on **Delete**.

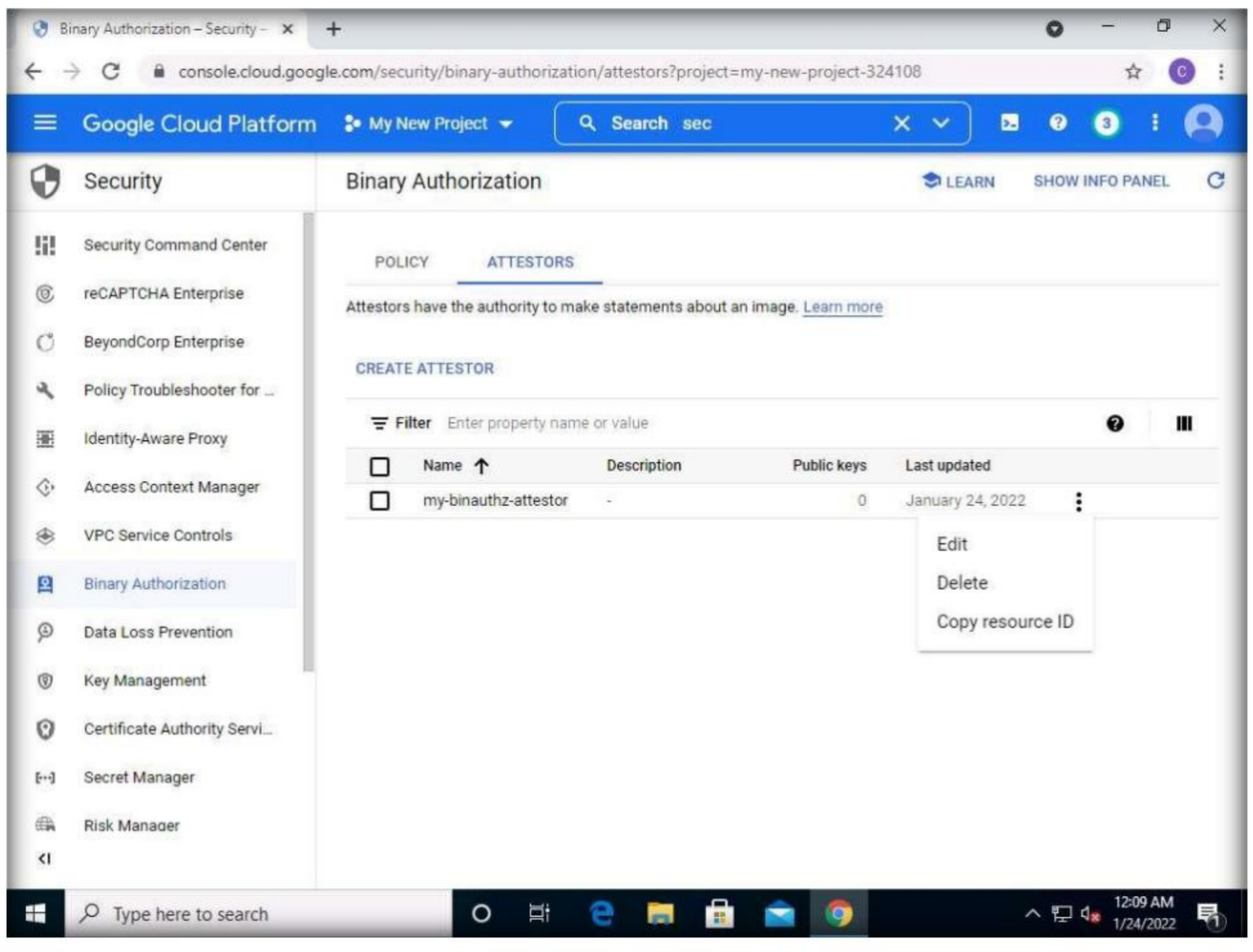


FIGURE 2.9.49: Deleting Binary Authorization

36. To delete the Kubernetes cluster, navigate to **Clusters** in **Kubernetes Engine** and scroll horizontally in the **Overview** tab. Click on the ellipsis at

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

the end of the cluster(**ecc-binauthz-lab**) you have created for this lab. Click **Delete**. In the pop-up window, click on **Delete**

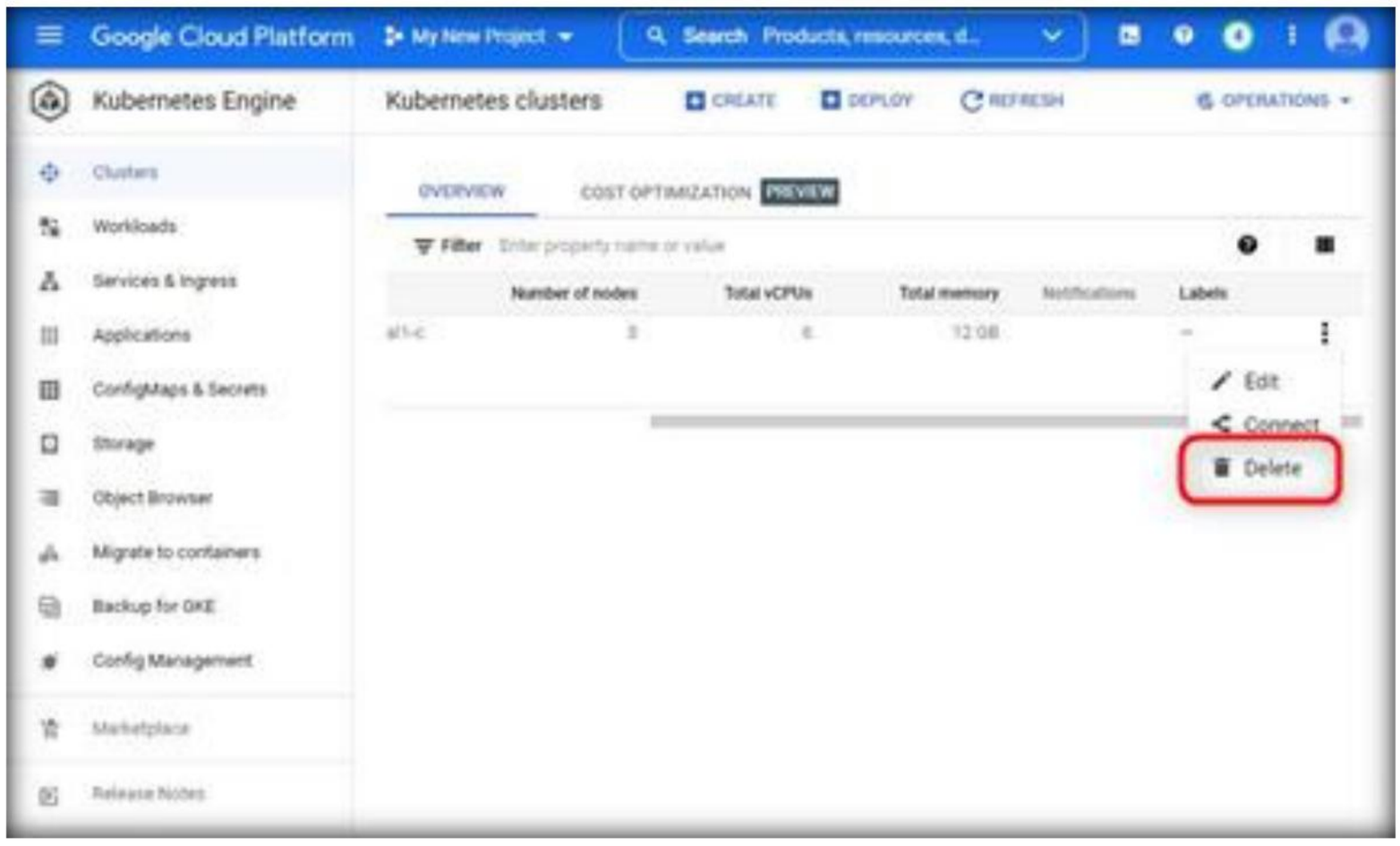


FIGURE 2.9.50: Deleting Kubernetes Cluster

37. Next, destroy the key(**lab-key**), navigate to **Security** and select **Key Management**. Open the key ring(**binauthz-keys**). Click on the ellipsis at the end of the key(**lab-key**) and click on **Destroy all key version material**. If a pop-up appears, enter the name of the key and click on **Schedule destruction**.

Note: The key will get destroyed after 24 hours. You cannot delete the key rings that you have created.

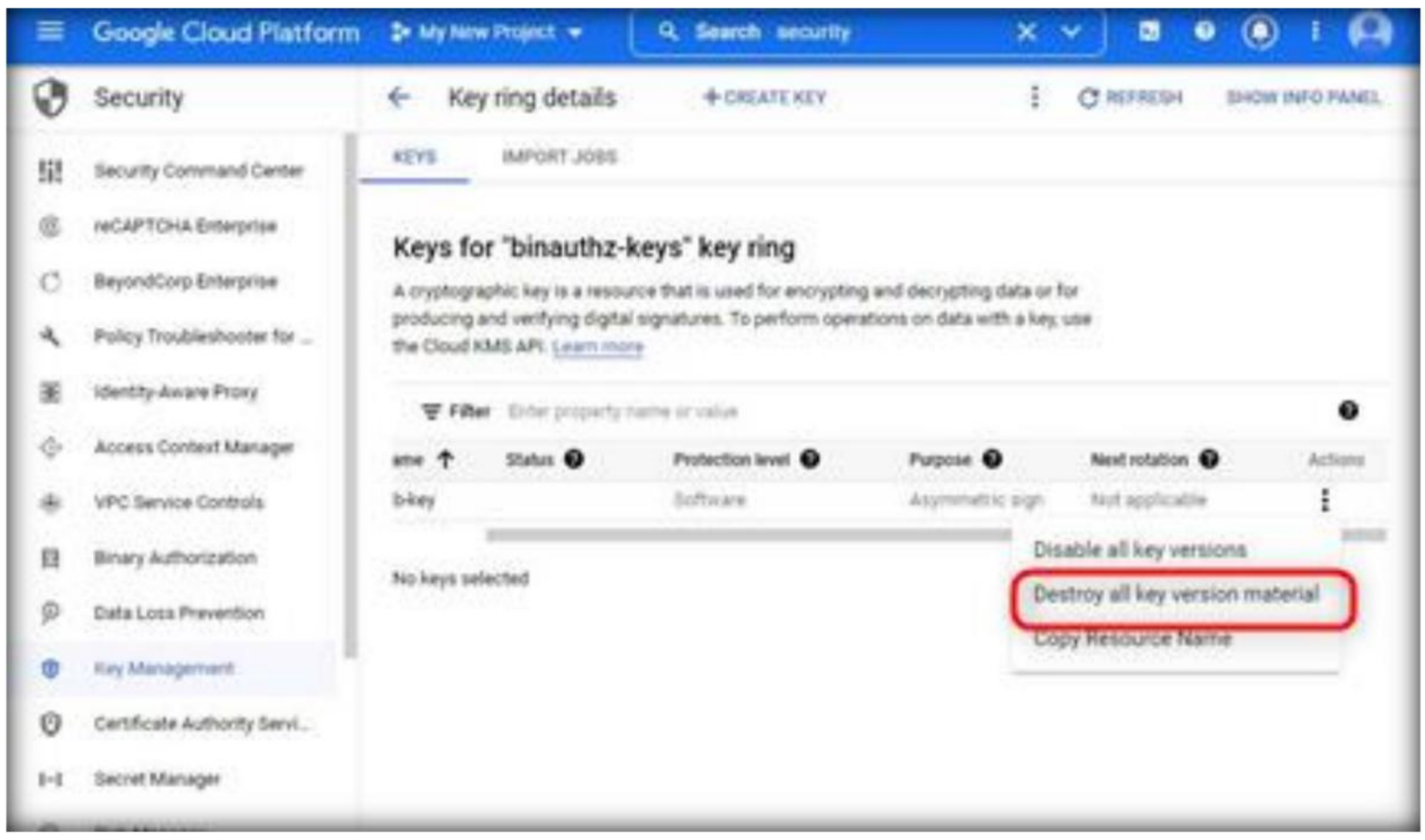


FIGURE 2.9.51: Deleting Key

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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.

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab

10

Implementing a Private Secure Connection Between Instances with VPC Network Peering

A virtual private cloud (VPC) network is an isolated, virtual form of a physical network that provides a secure private connectivity between instances and their internal IP addresses globally.

Lab Scenario

In the cloud, a communication between two VM instances in the same project or in different projects over the Internet can lead to security vulnerabilities. VPC networks are global resources and their corresponding routes and firewall rules allow their resources to communicate with each other with the internal IPv4 addresses. Moreover, connectivity between two VPC networks, which is also known as Google Cloud VPC network peering, allows workloads in different VPC networks to communicate with their internal IP addresses. This lab demonstrates the implementation of a secure private connectivity between the VPC networks of two instances in different projects.

ICON KEY

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

Lab Objectives

This lab will demonstrate how to implement a secure private connection between VPC networks of two instances in different projects.

In this lab, you will learn to do the following:

- Create a new project in GCP
- Create a VPC network for both the projects
- Create instances and configure VPC networks for both projects
- Implement network peering between the VPC networks

Lab Environment

To perform this lab, you need the following:

Certified Cloud Security Engineer Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Admin Machine** VM
- **Administrative** privileges to run the tools

Lab Duration

Time: 20 minutes

Overview of VPC Network Peering

A VPC network is a virtual version of a physical data center network that is isolated. These are global networks that offer a secure communication between instances using internal IP addresses. In a VPC network, traffic to and from the instances can be controlled by network firewall rules. VPC network peering allows a secure connection between VPC networks of different projects or organizations. With VPC network peering, workloads in different VPC networks can communicate internally, thereby eliminating the security risks associated with exposing the services to the Internet. Moreover, VPC network peering offers a lower latency because it uses internal IP addresses for connectivity.

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., GCP), the application interface may be updated with time. Hence, in case you happen to work on an updated version of GCP, 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 GCP Free Trial account using the following link: https://cloud.google.com/free, in case you have already not created it for the previous lab. Once the registration is complete, perform the following tasks:

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

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1

Creating a New Project in GCP

1. Log in to the **Admin Machine** VM with the user name **Admin** and password **admin@123**.

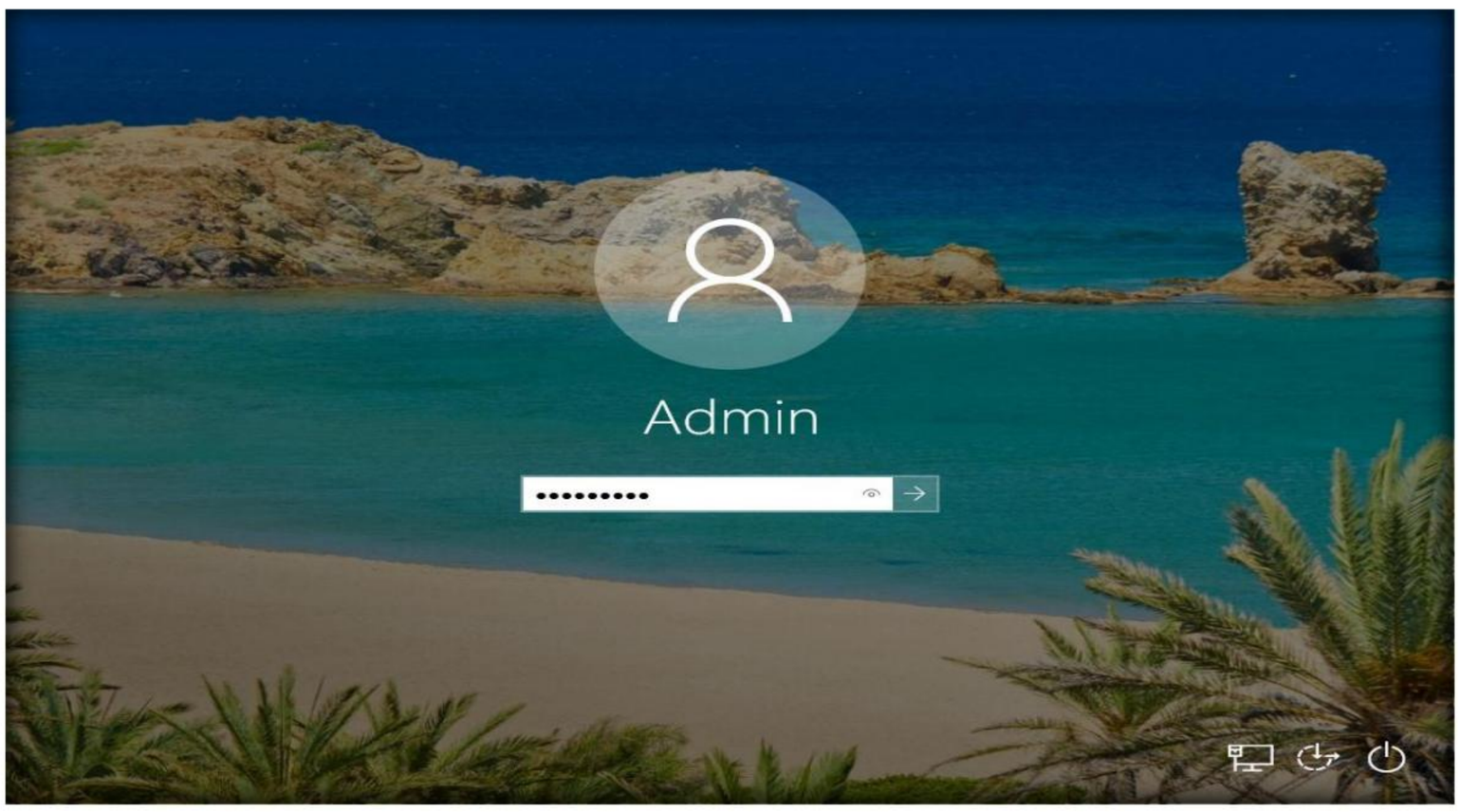


FIGURE 2.10.1: User Login

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

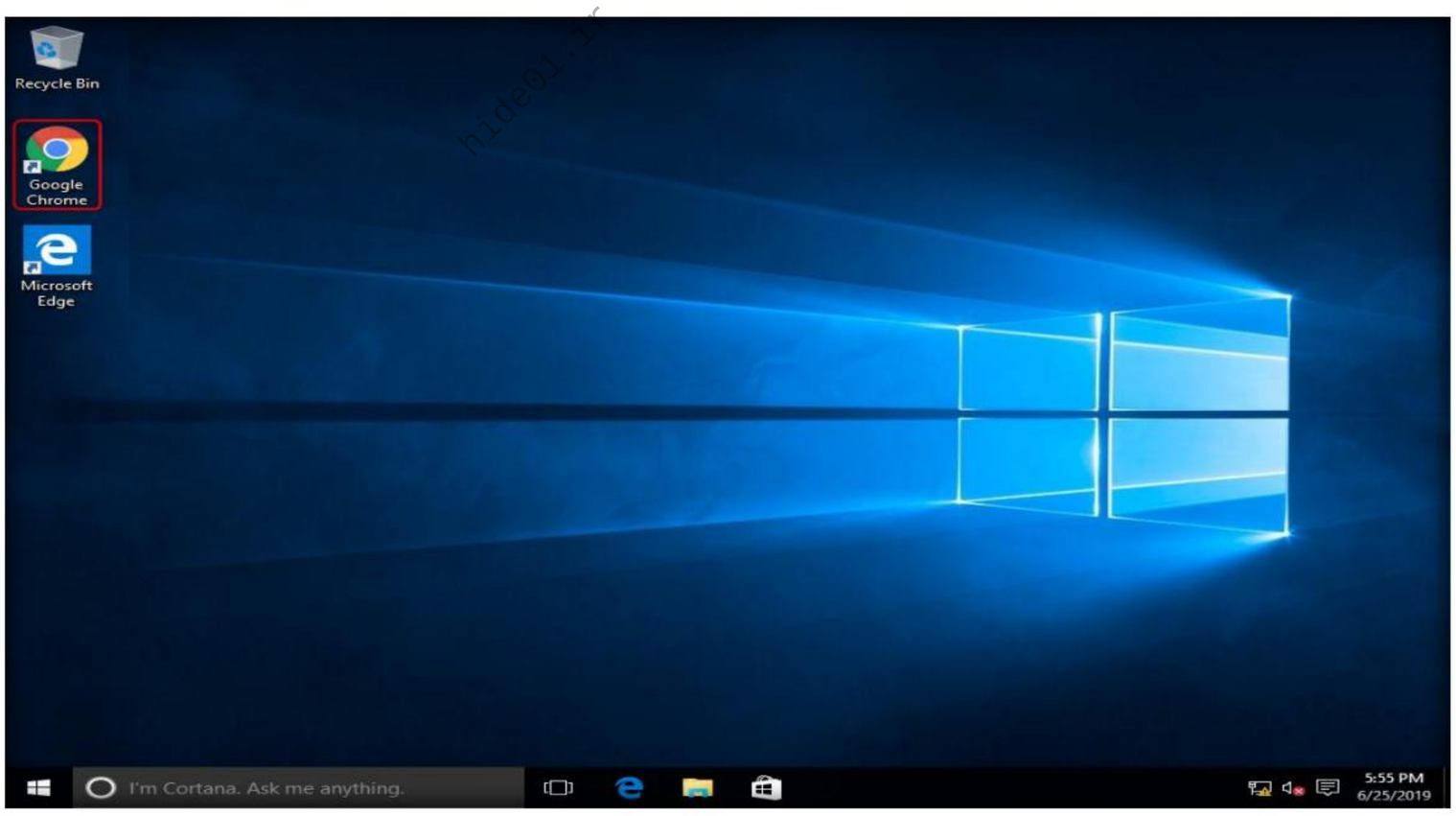


FIGURE 2.10.2: Navigating to the Chrome Browser from Taskbar

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

3. In the address bar of the **Google Chrome** browser, type **https://console.cloud.google.com** and press **Enter.**

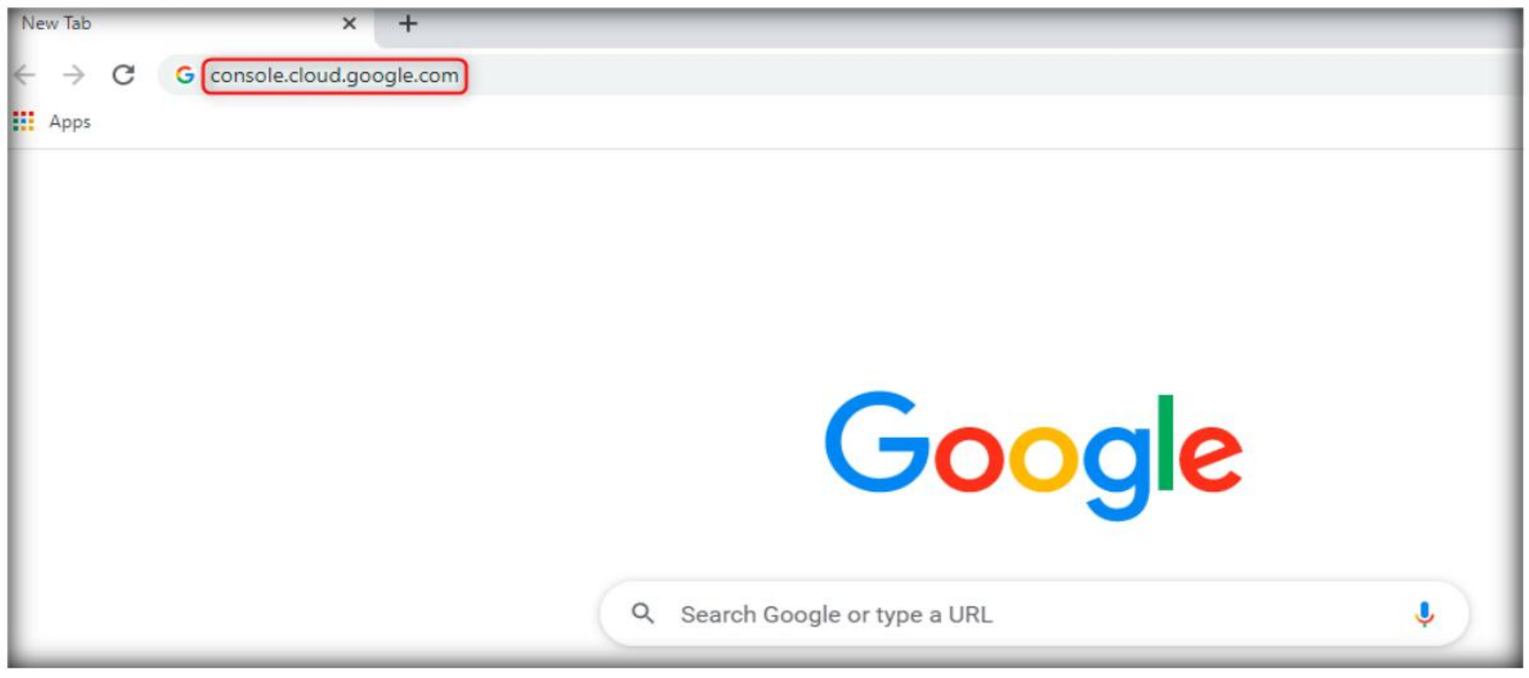


FIGURE 2.10.3: Accessing GCP Console in Google Chrome

Note: If you are already logged in, skip the login steps.

4. Enter the **Email address** to sign into Google Cloud Platform.
5. Click **Next**.

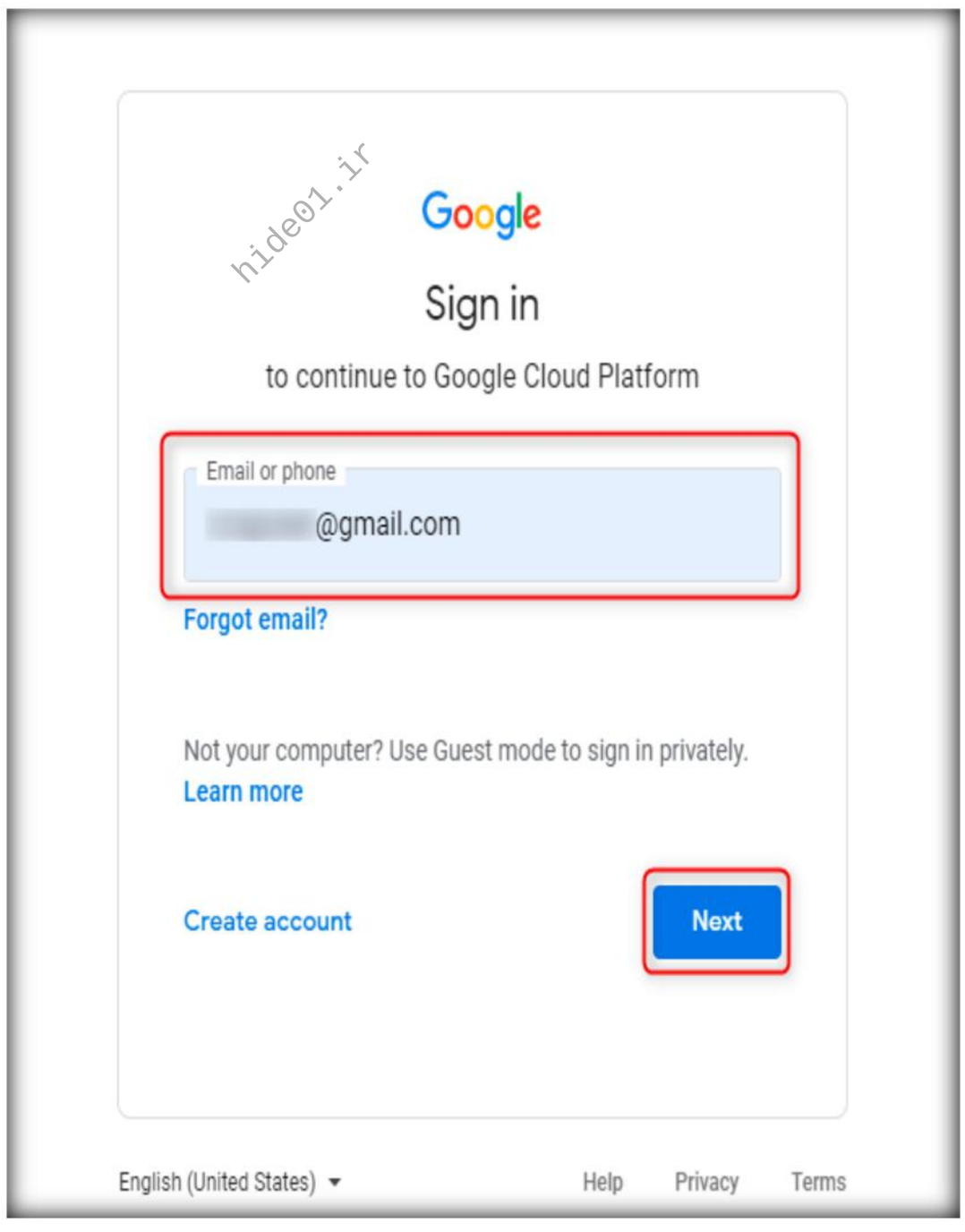


FIGURE 2.10.4: Entering the email address

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

6. Enter the **password** and click on **Next**.



FIGURE 2.10.5: Sign-in to GCP

7. Now, create a new project because you need to implement VPC network peering between two instances in different projects. To do this, click on the existing project title at the top of the console.

   Note: to demonstrate VPC network peering, we need two projects. Here, we are using a project that was created in the previous labs. The second project will be created here. If you are logging into GCP console for the first time, you can follow the following steps to create your first project.

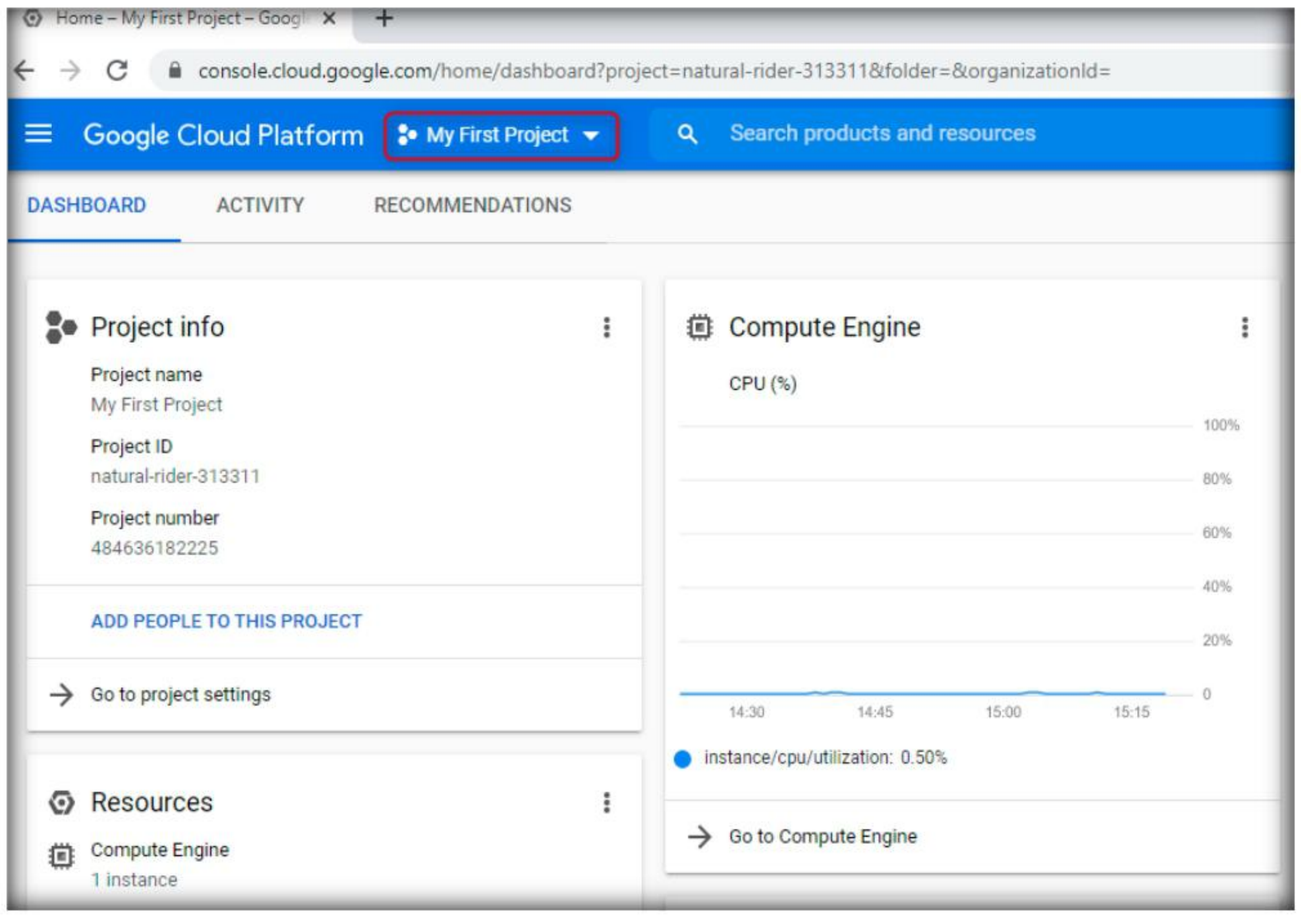


FIGURE 2.10.6: Selecting the Project Title

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

8. In the **Select a project** window, click on **NEW PROJECT**.

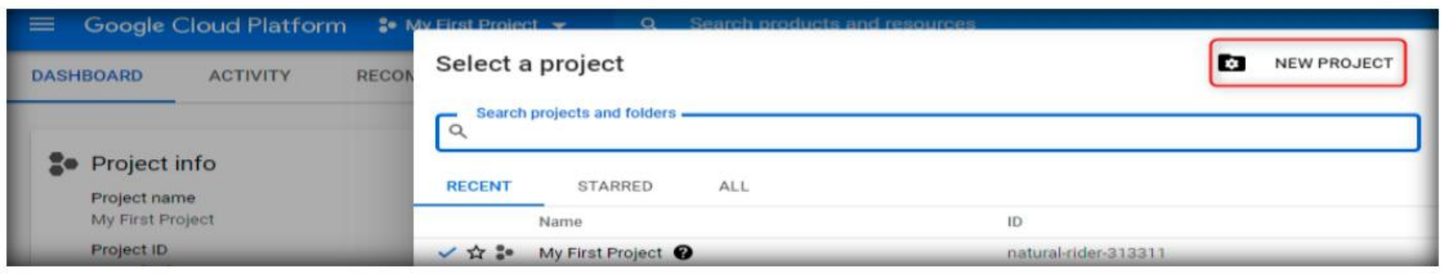


FIGURE 2.10.7: Selecting New Project

9. In the **New project** window, type a **Project name**, or keep the default name and click on **CREATE.**

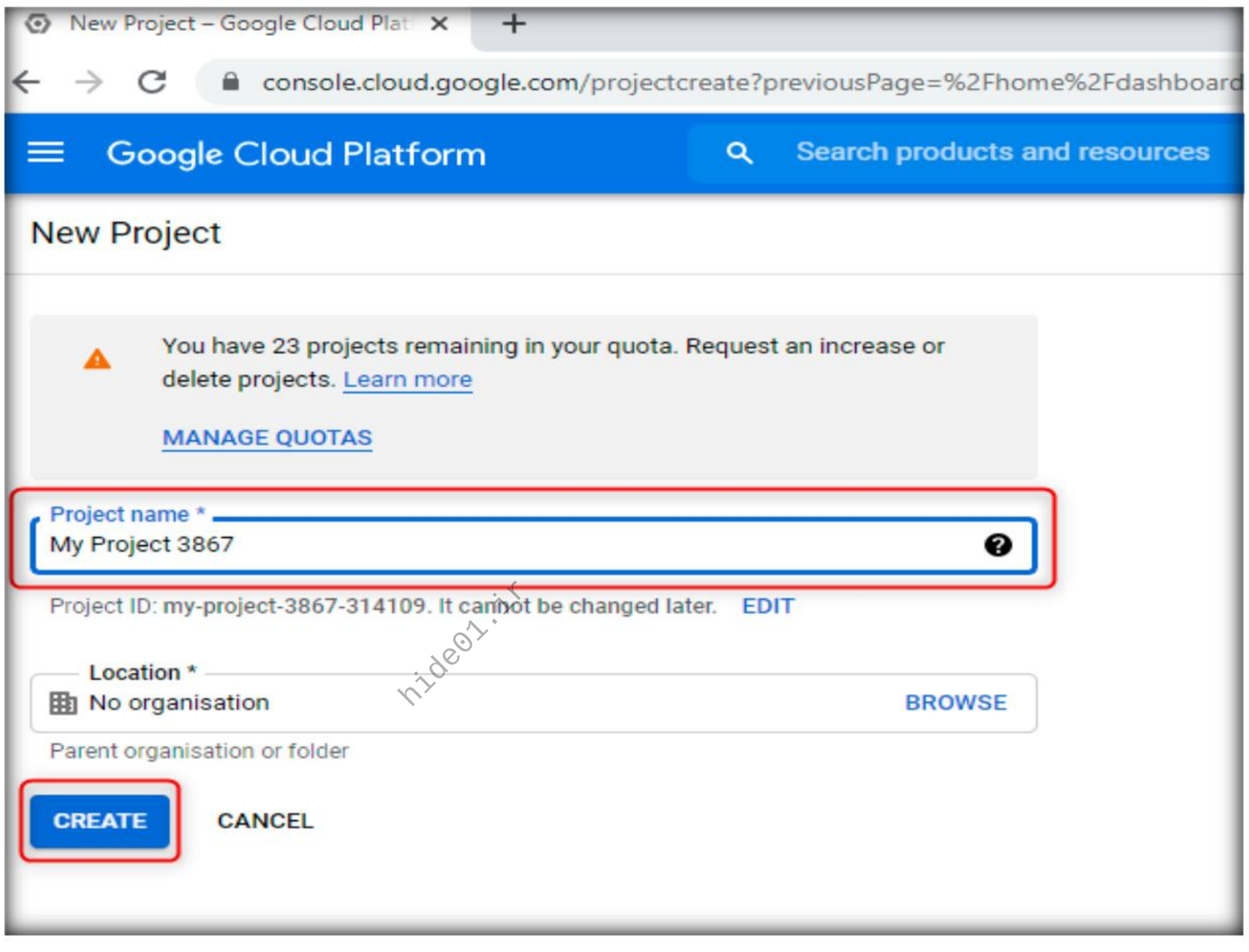


FIGURE 2.10.8: Creating the Project

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

10. Next, click on the project name at the top again to verify whether the new project was created.

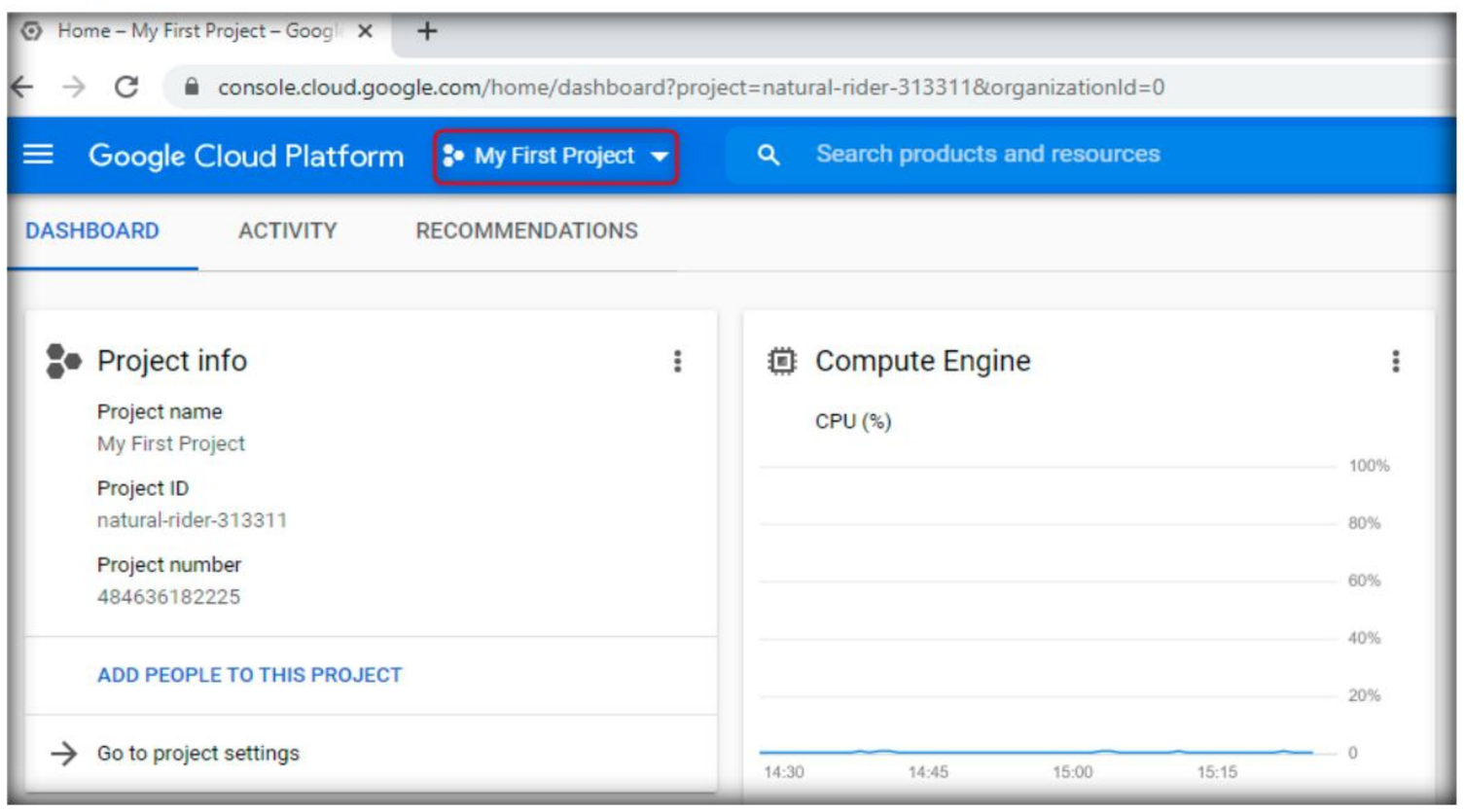


FIGURE 2.10.9: Selecting the Project name

11. Verify whether the new project is successfully created. Note the project **IDs** of both projects for future reference.

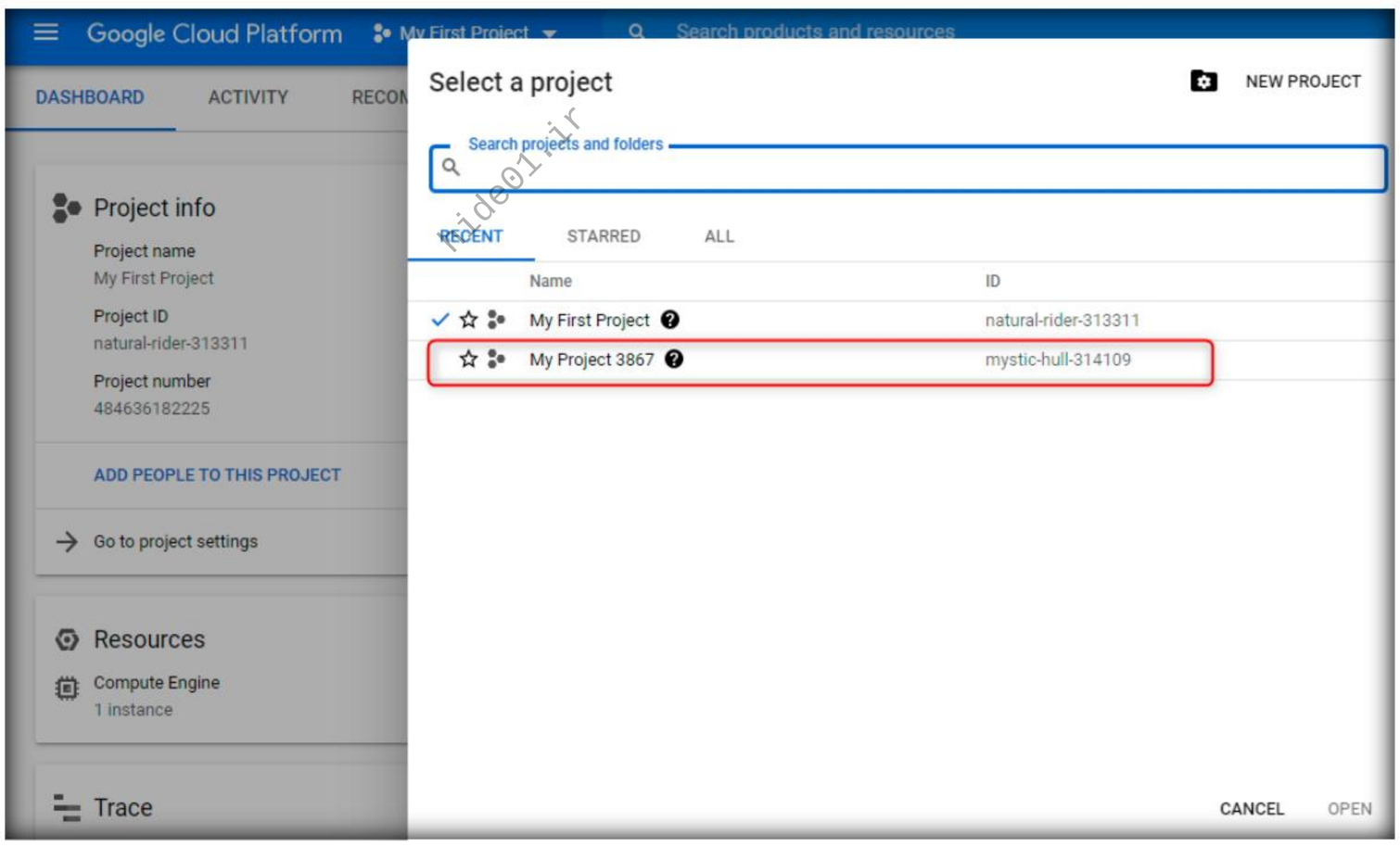


FIGURE 2.10.10: Verifying Whether the New Project is Created

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 2

Creating VPC Network in both Projects

12. Now, you need to create **VPC Networks**.

    13. First, create a VPC network in the first project. Make sure that you are in the first project.

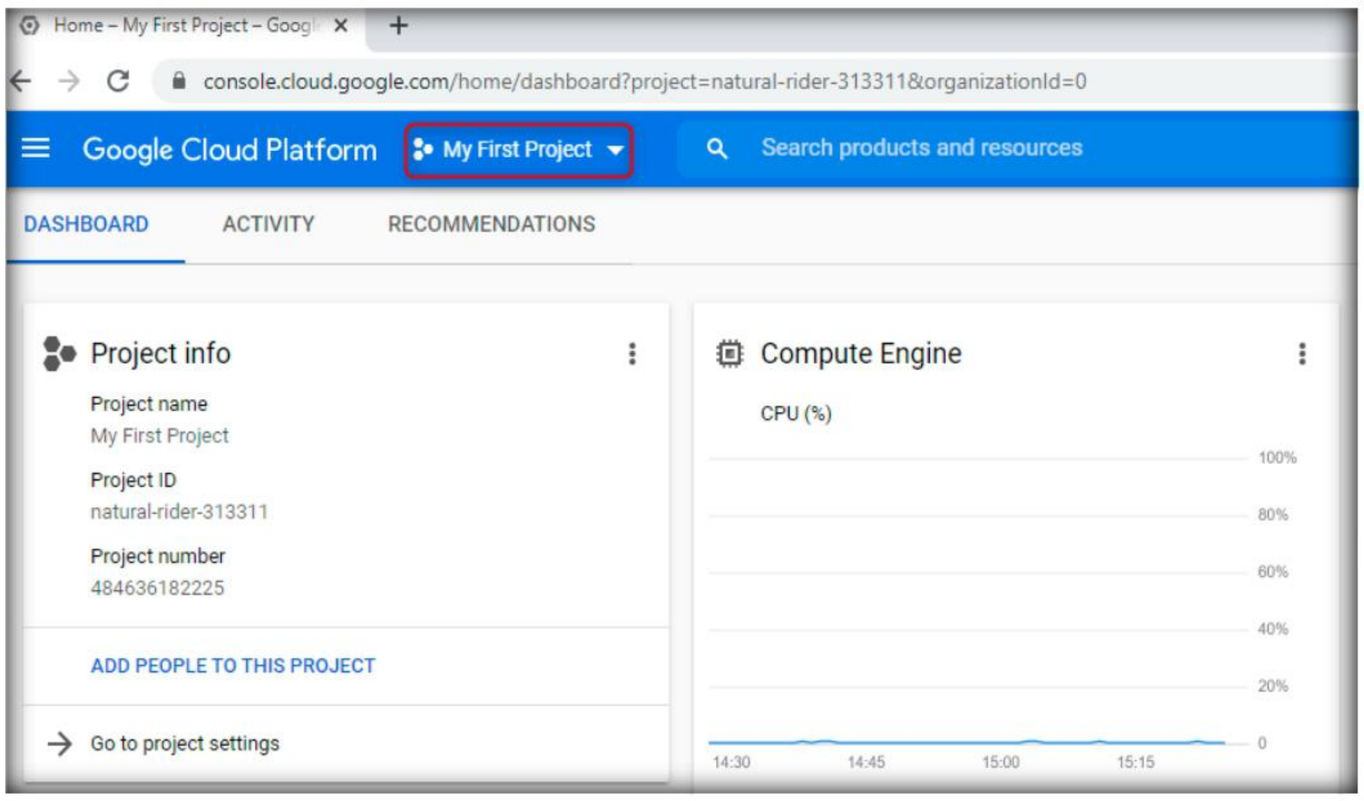


FIGURE 2.10.11: In the First Project

    14. Now, to create your VPC network, navigate to **VPC network** and select **VPC networks** in the console.

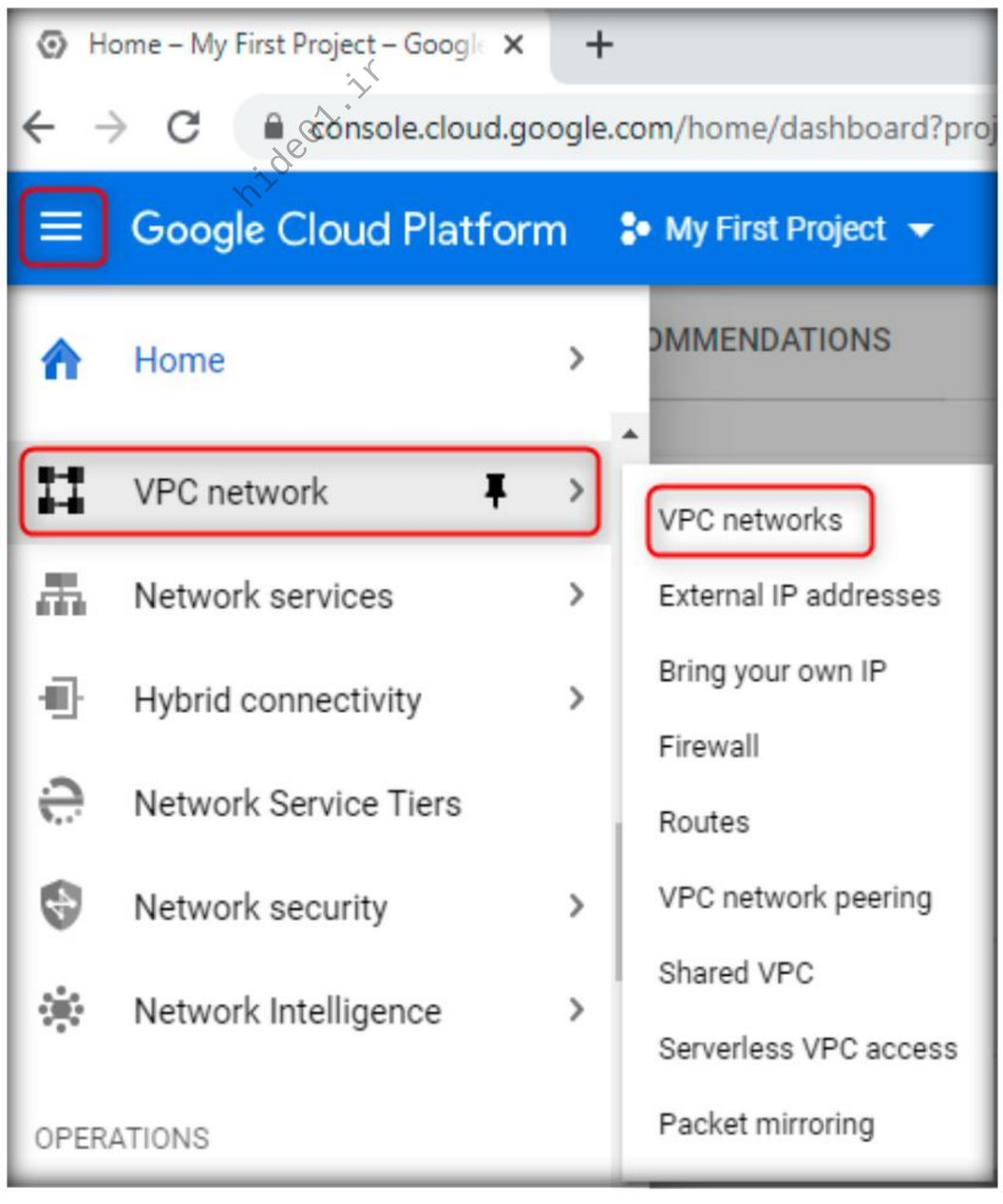


FIGURE 2.10.12: Navigating to VPC networks from the console

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

15. In the **VPC networks** window, click on **CREATE VPC NETWORK** at the top.

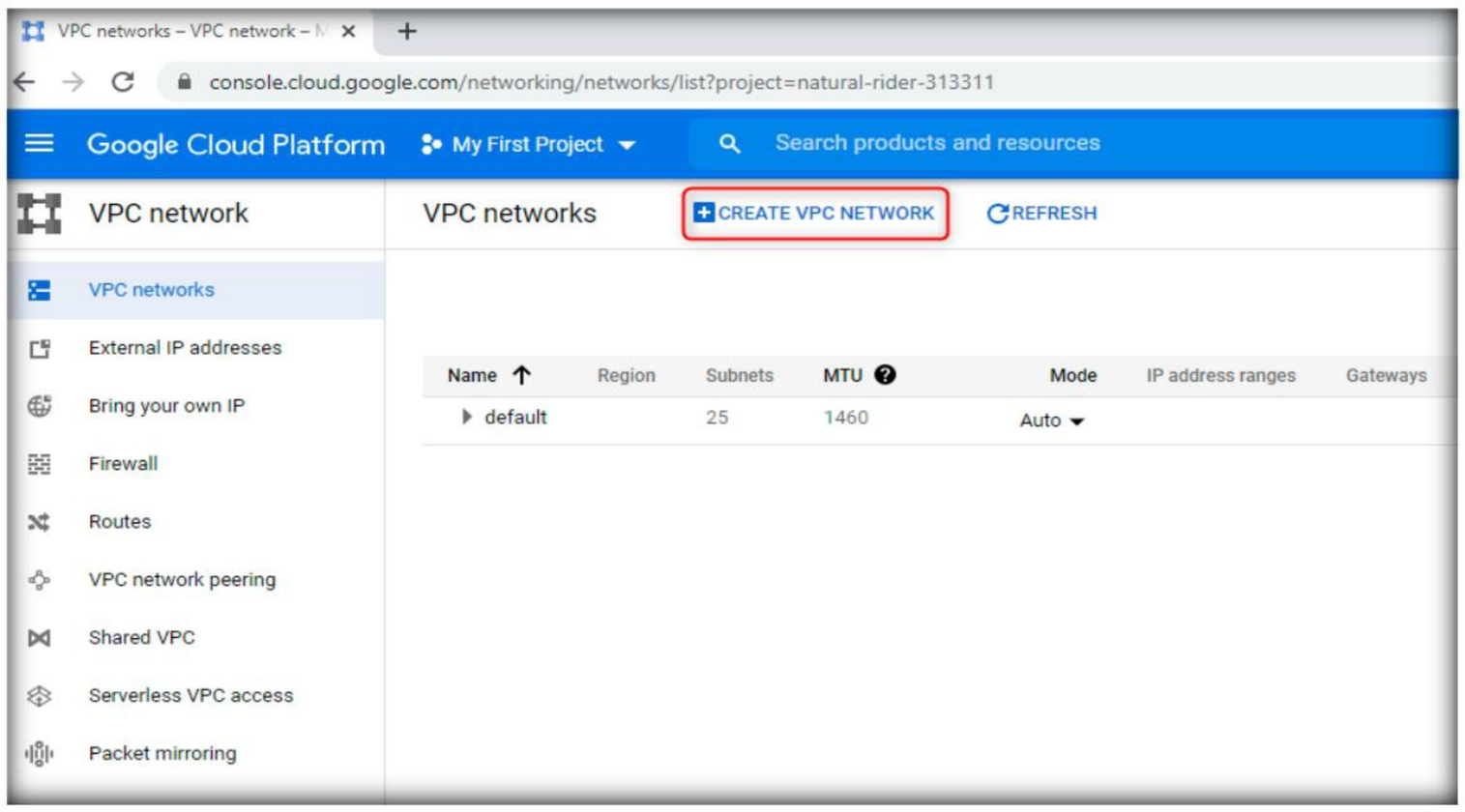


FIGURE 2.10.13: Creating a New VPC Network

16. Type an appropriate **Name** for the first VPC network. In this lab, our VPC network is named **eccvpcnw-1**. For **Subnet creation mode,** select **Custom**.

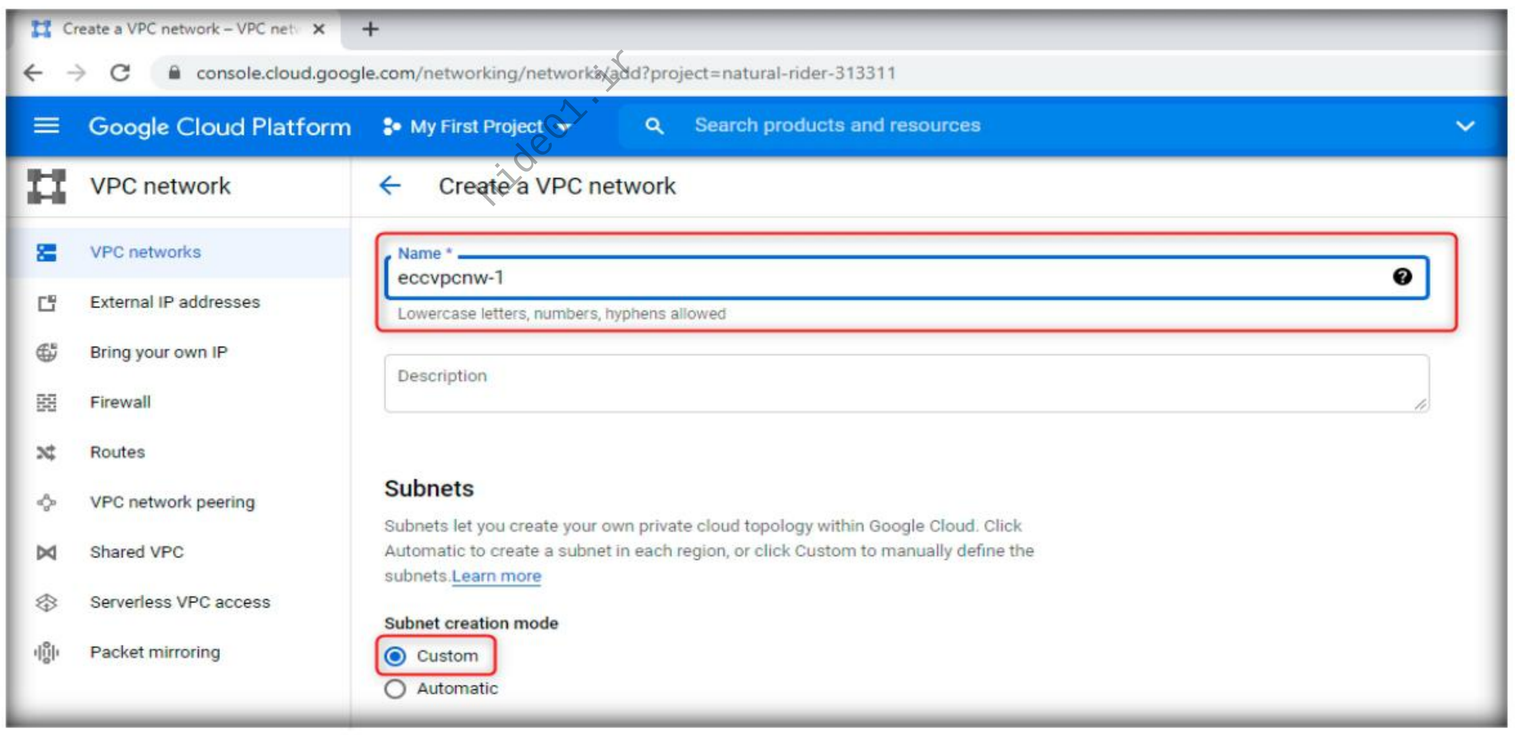


FIGURE 2.10.14: Naming the VPC network and Selecting the Subnet creation mode

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

17. Scroll down to the bottom and provide an appropriate name, region, and IP range for the subnet. In this lab, we have created the subnet with the following details:

    Name: **eccsubnet-1**

    Region: **us-central1**

    IP address range: **10.0.1.0/24**

    Retain the other default settings and click **Done**.

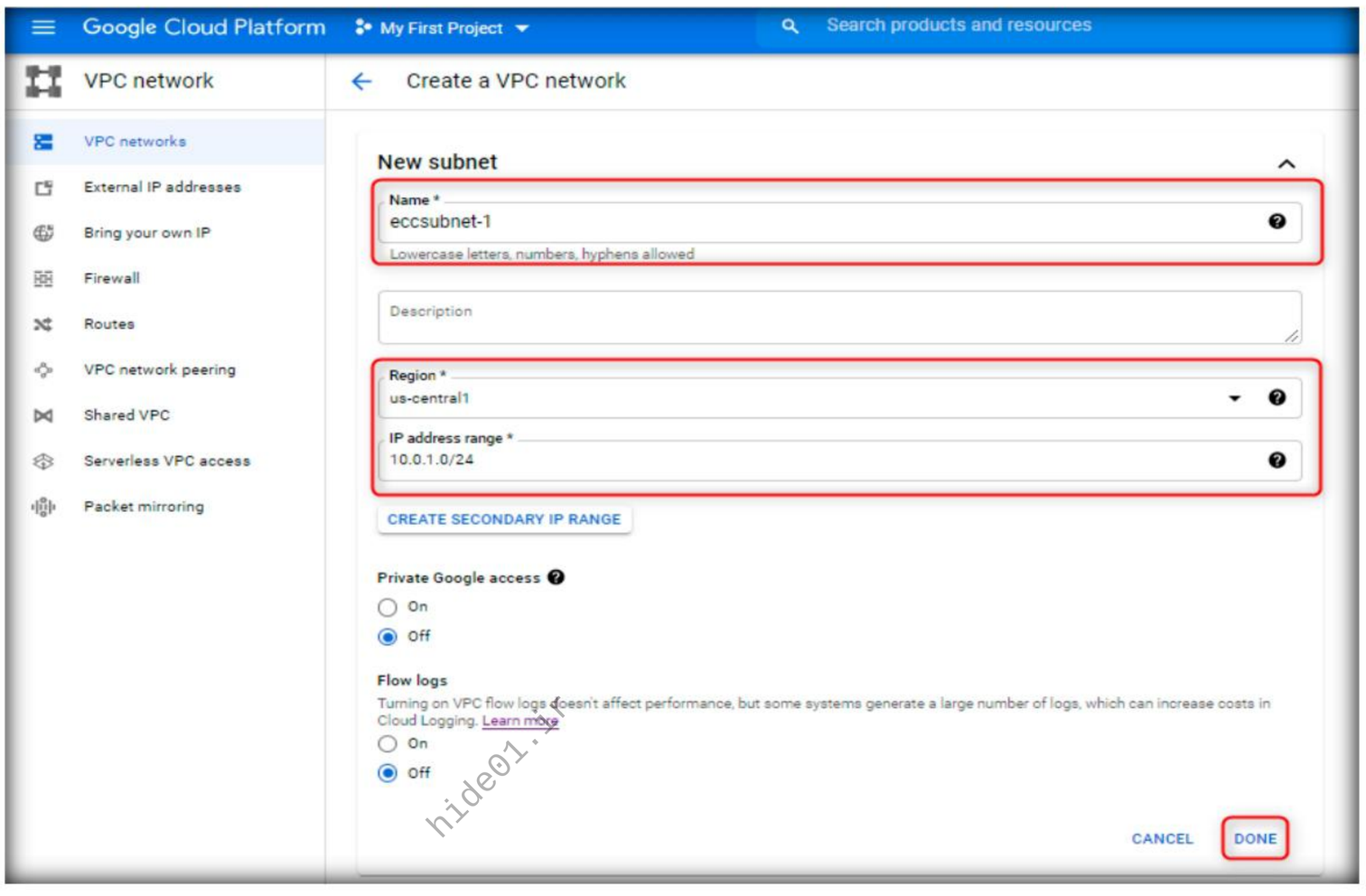


FIGURE 2.10.15: Creating Subnet

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

18. Retain the other default settings and click on **CREATE**.

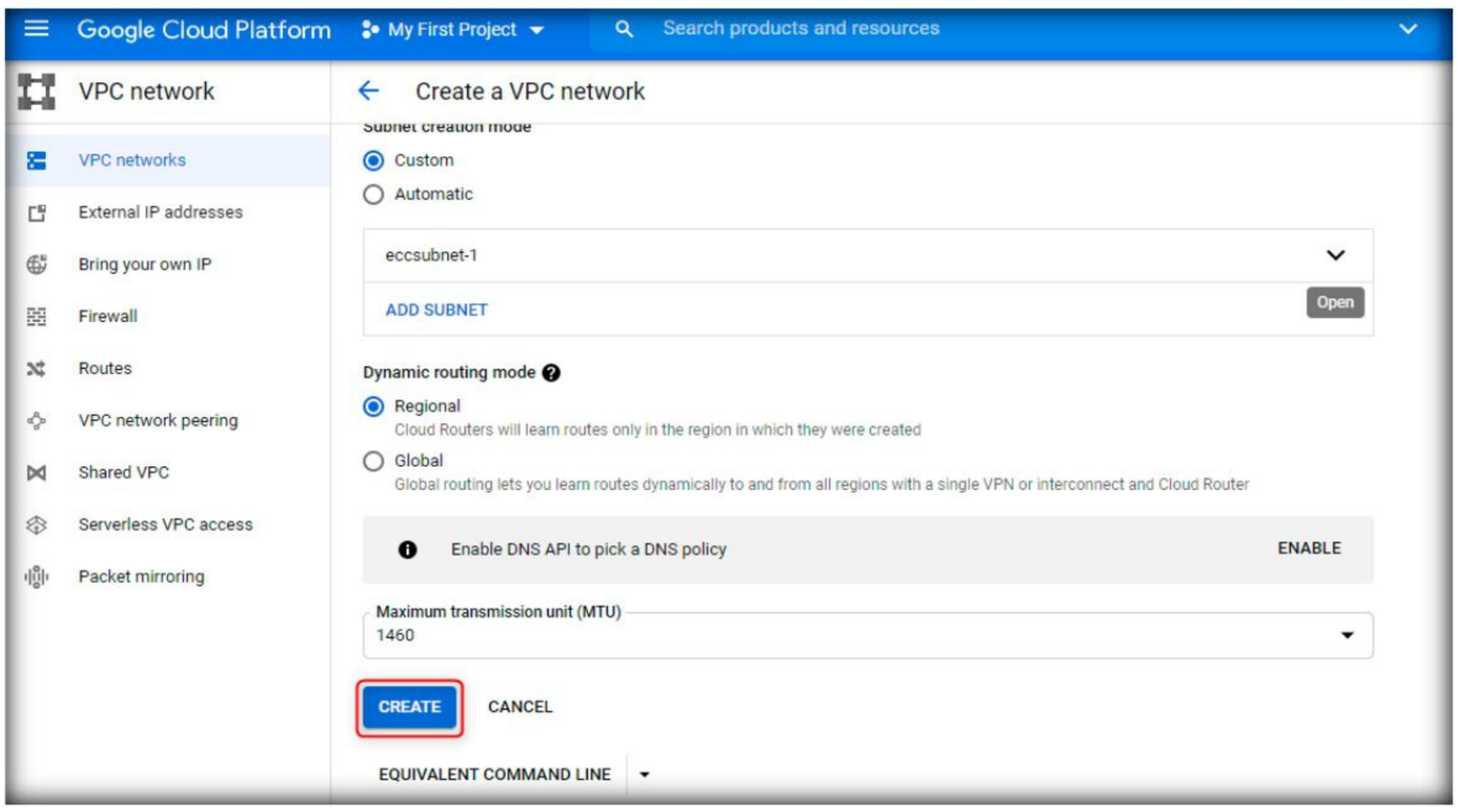
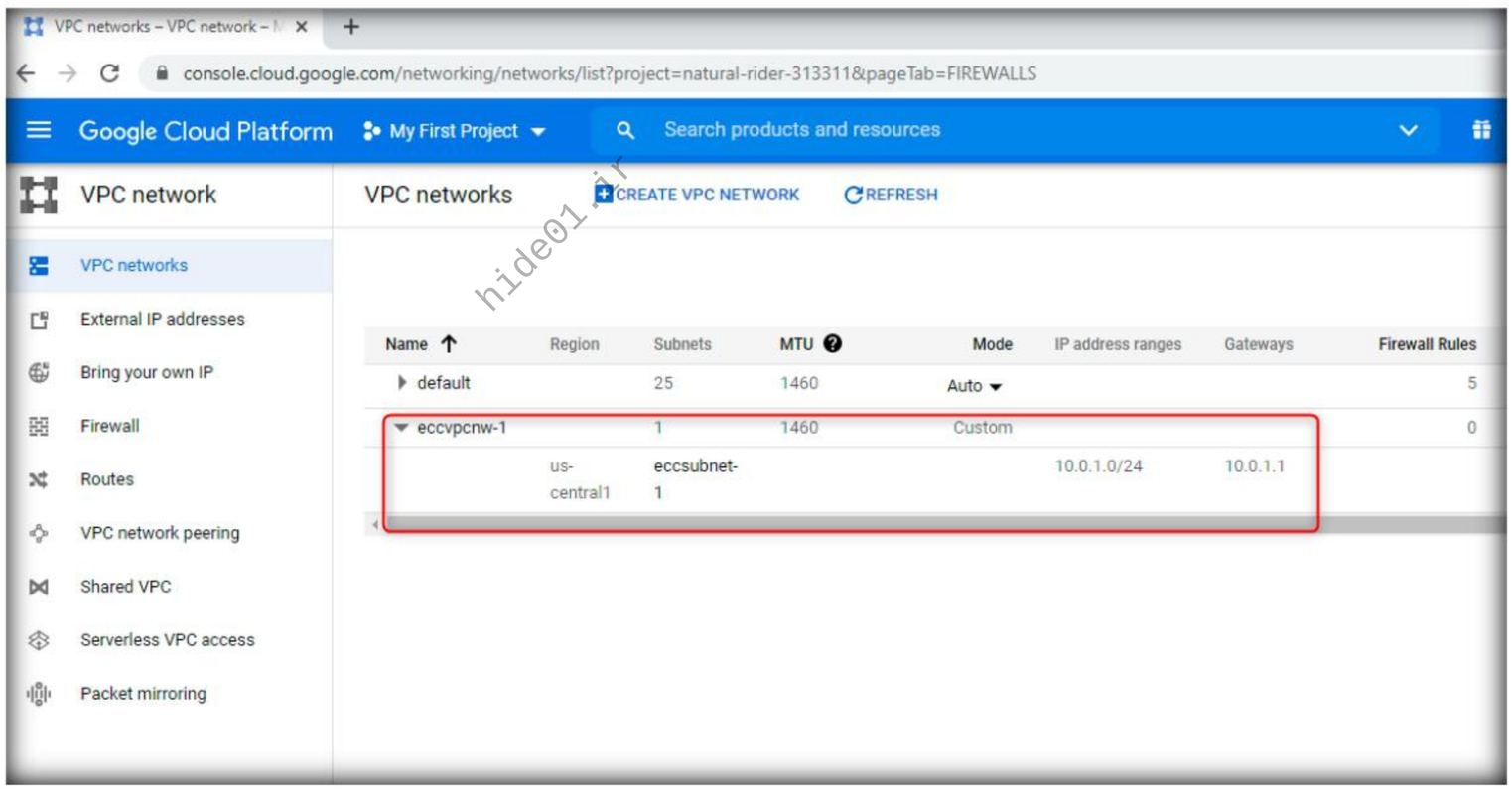


FIGURE 2.10.16: Creating VPC Network

19. In the **VPC networks** window, verify whether the VPC network is successfully created.



hide01.ir

FIGURE 2.10.17: Verifying whether the VPC network is created

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

20. Now, create a firewall rule for the VPC instance to allow SSH connections by selecting the name of the VPC network that was just created.

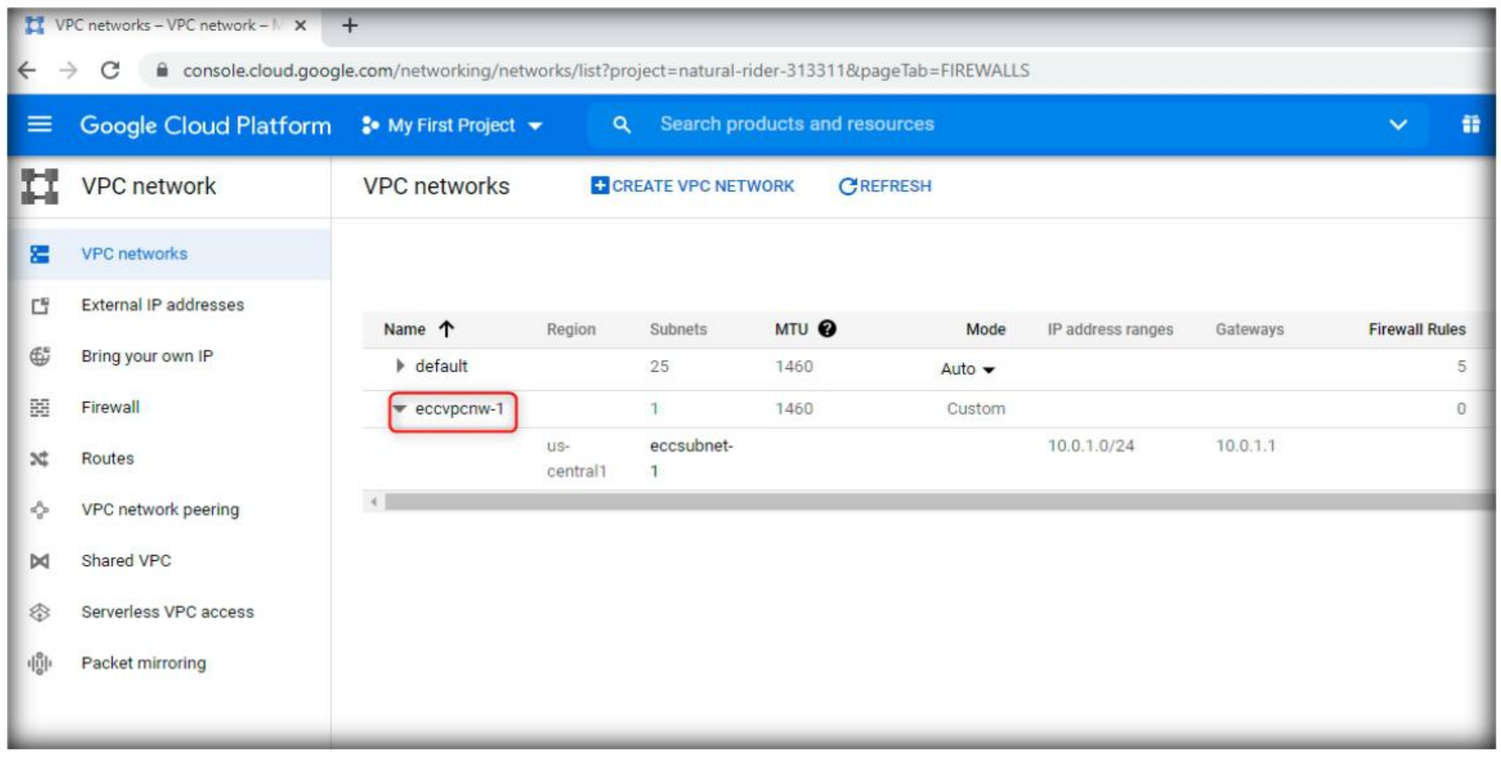


FIGURE 2.10.18: Selecting the VPC Network

21. In the **VPC network details** window, click on **Edit** at the top.

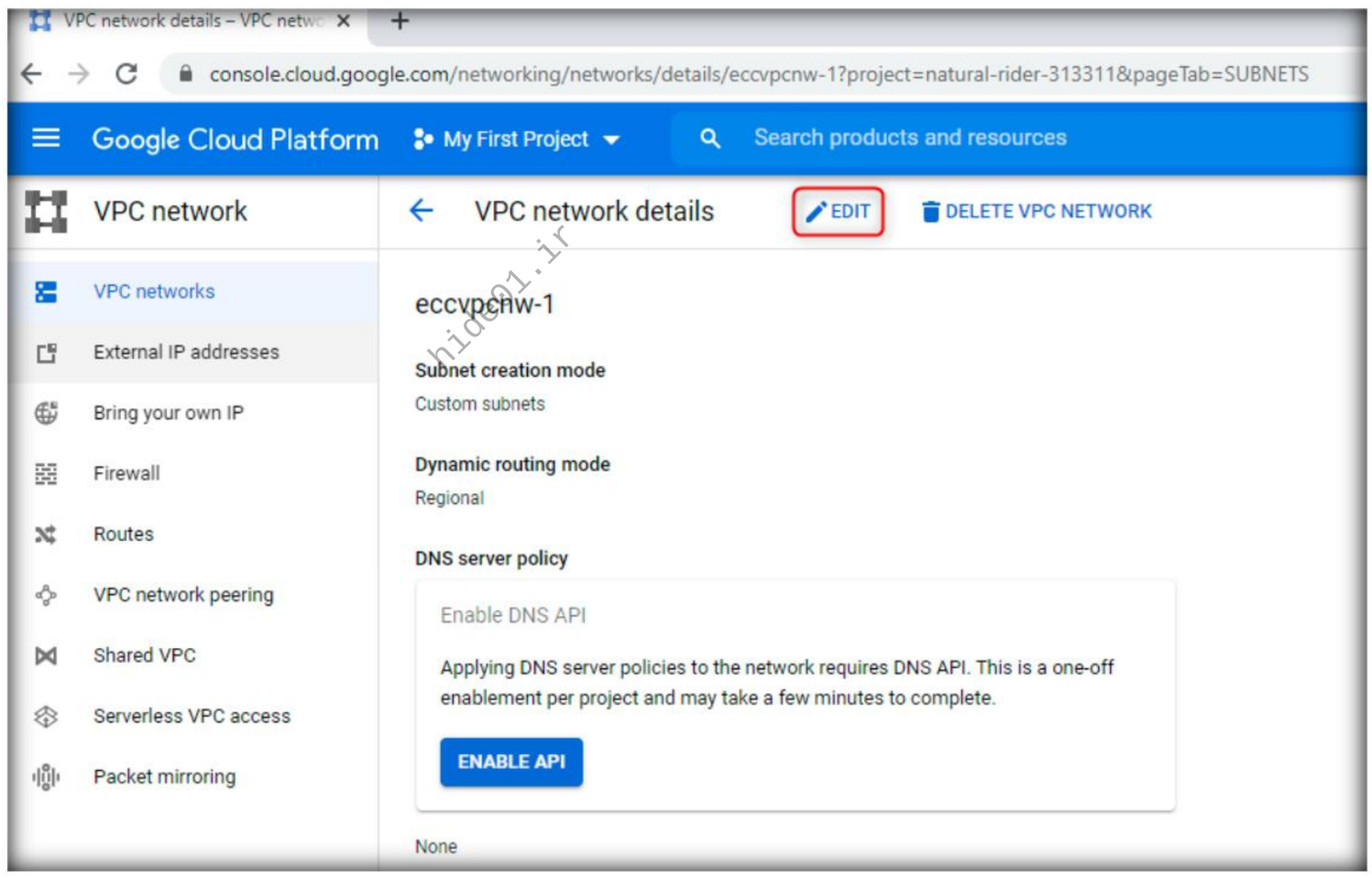


FIGURE 2.10.19: Editing the network details

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

22. Scroll down to the bottom and click on **FIREWALL RULES**.

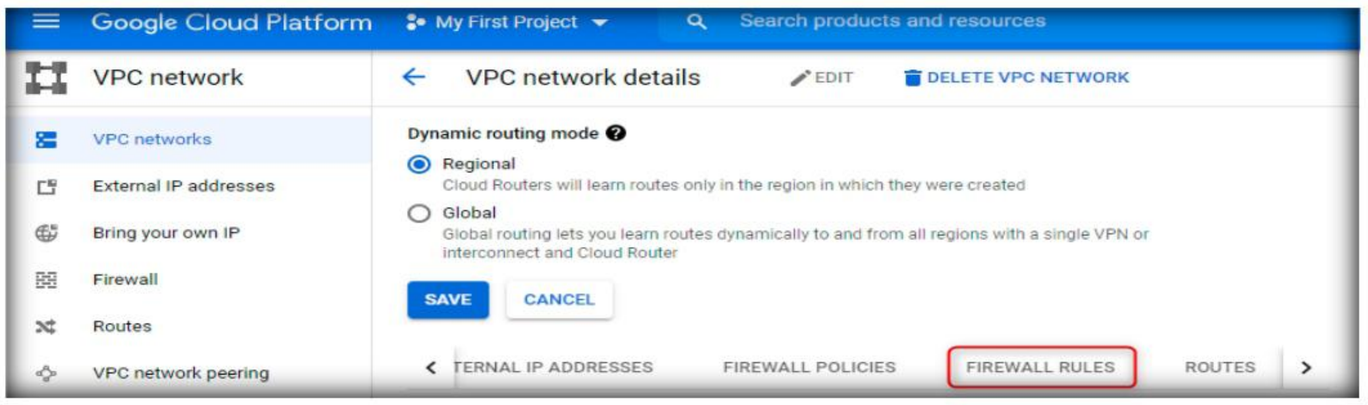


FIGURE 2.10.20: Selecting Firewall Rules

23. Click on **ADD FIREWALL RULE**.

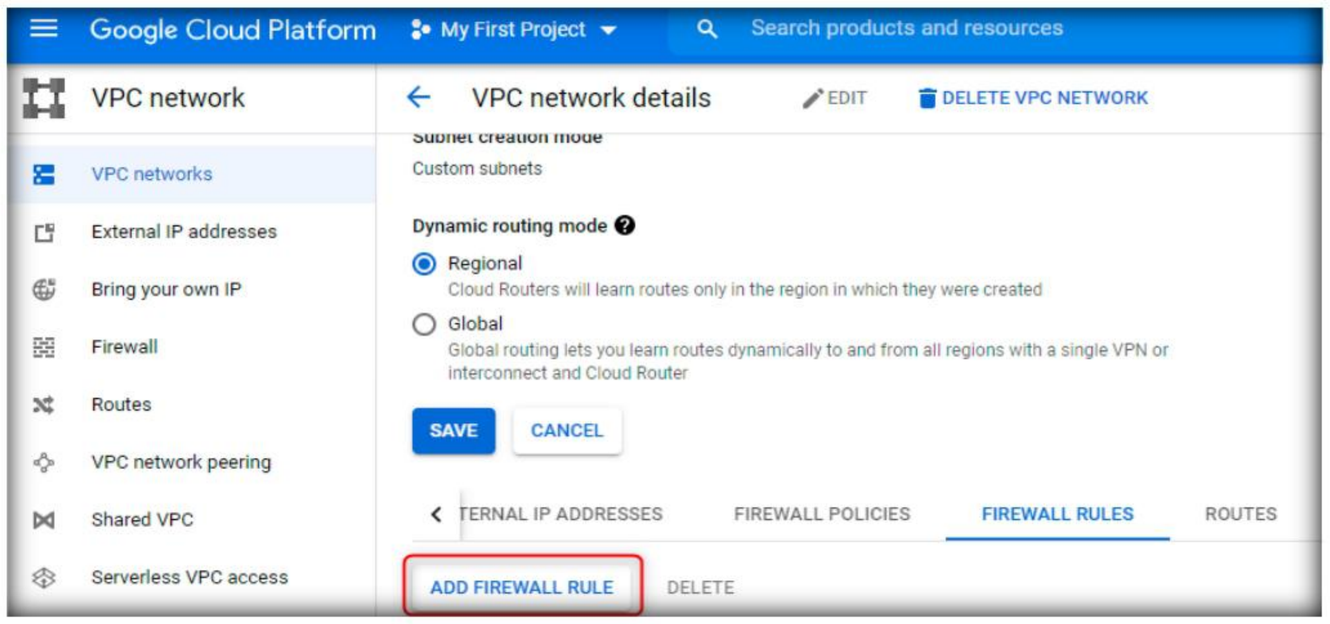


FIGURE 2.10.21: Adding Firewall Rules

24. Type an appropriate **Name** for the firewall rule. Here, we have named the firewall rule as **eccfwssh-1**.

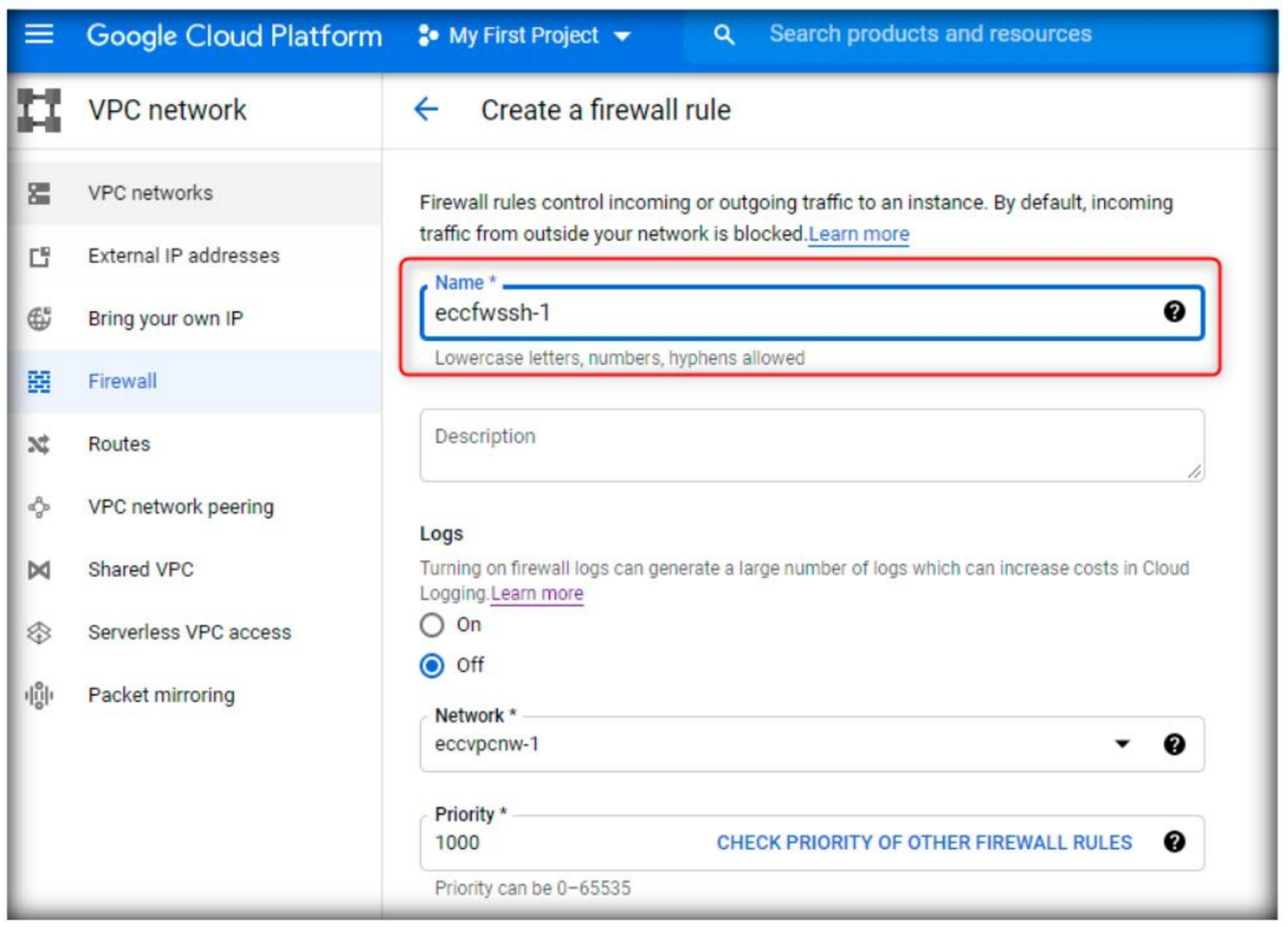


FIGURE 2.10.22: Naming the Firewall Rule

25. Scroll down to the bottom and select **Ingress** for **Direction of traffic** and **Allow** for **Action on match**. For **Targets**, select **All instances in the network**, and specify **Source IP ranges** as **0.0.0.0/0**.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

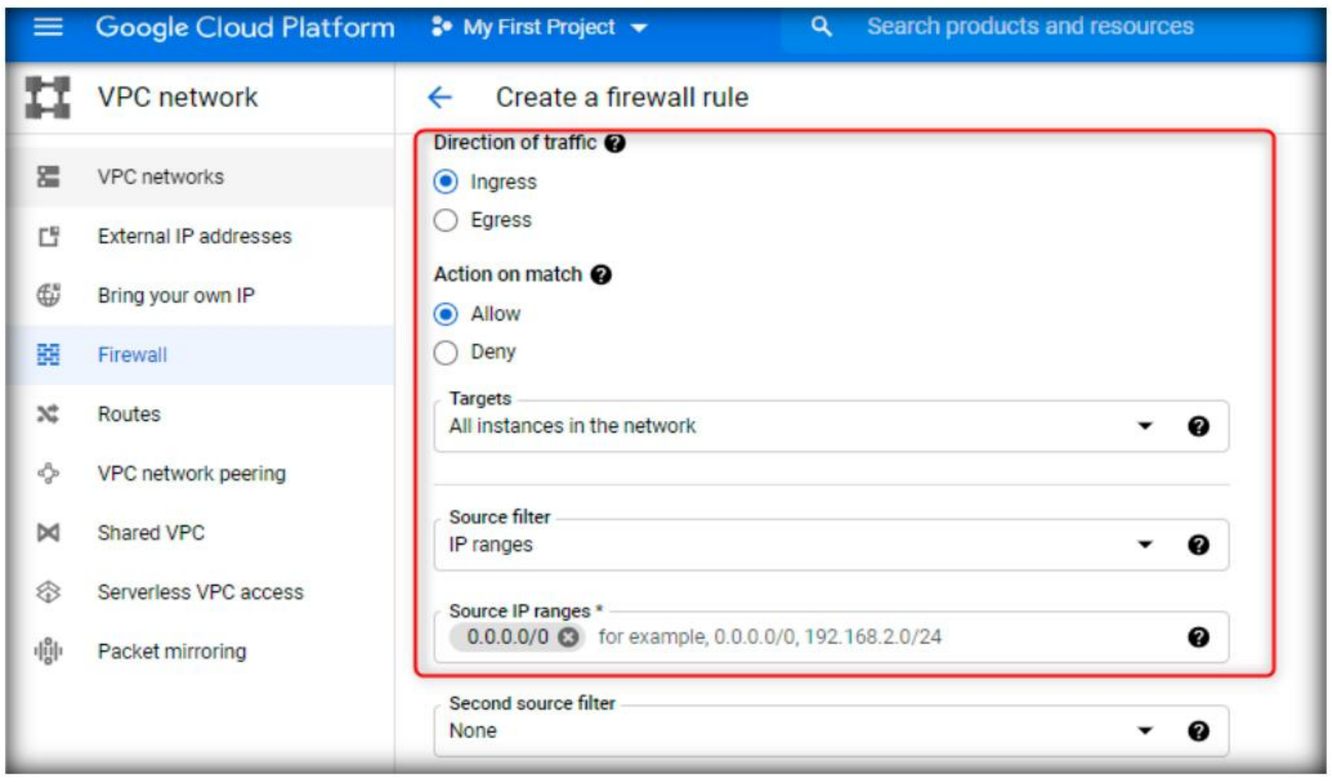


FIGURE 2.10.23: Giving Other Details

26. For **Protocols and ports**, select **Specified Protocols and Ports**. Select **tcp** and enter the port **22** to allow SSH connections. Select **Other Protocols** and enter **icmp.** Finally, click on **CREATE**.

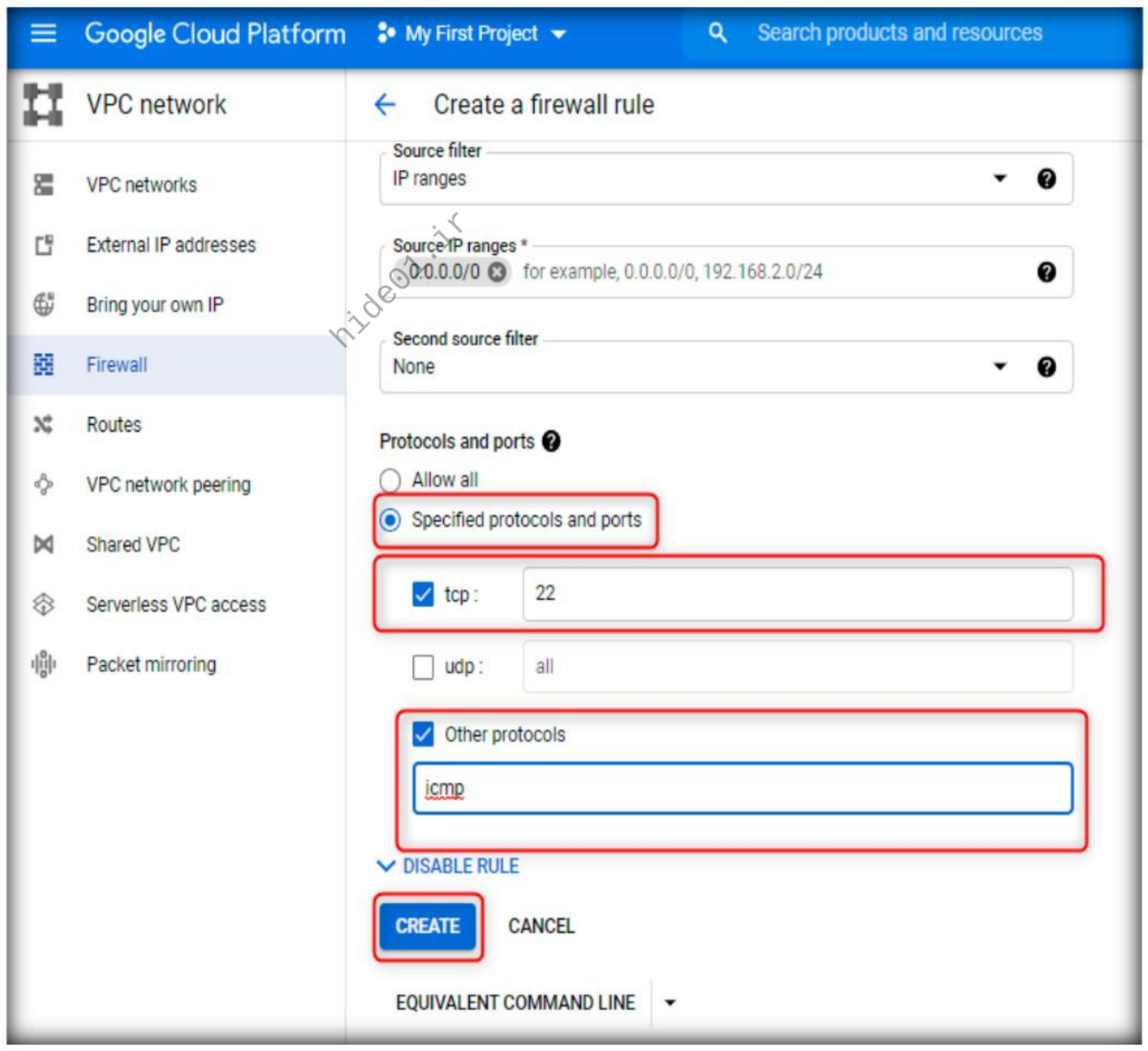


FIGURE 2.10.24: Creating the Firewall Rule

27. Now, you can see that the firewall rule has been assigned to the VPC network.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

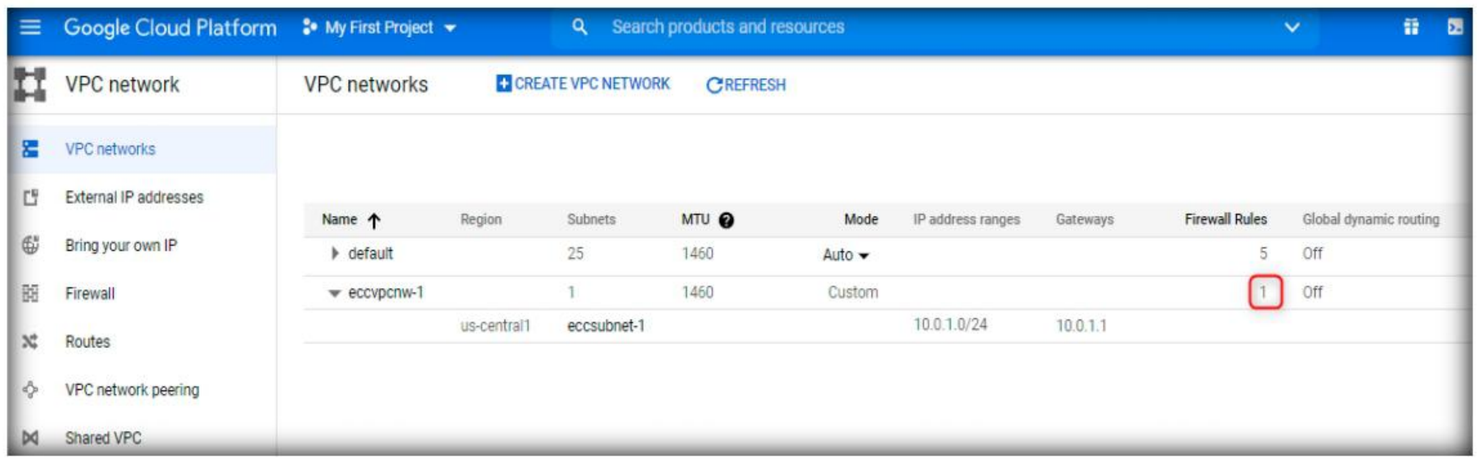


FIGURE 2.10.25: Created Firewall Rule

28. Similarly, create a VPC network for the second project by repeating the same steps as in the first project. Switch the project by selecting the **Project name** on the top of the console.

    Note: For configuring the second project, a new Google Chrome tab to the right is recommended.

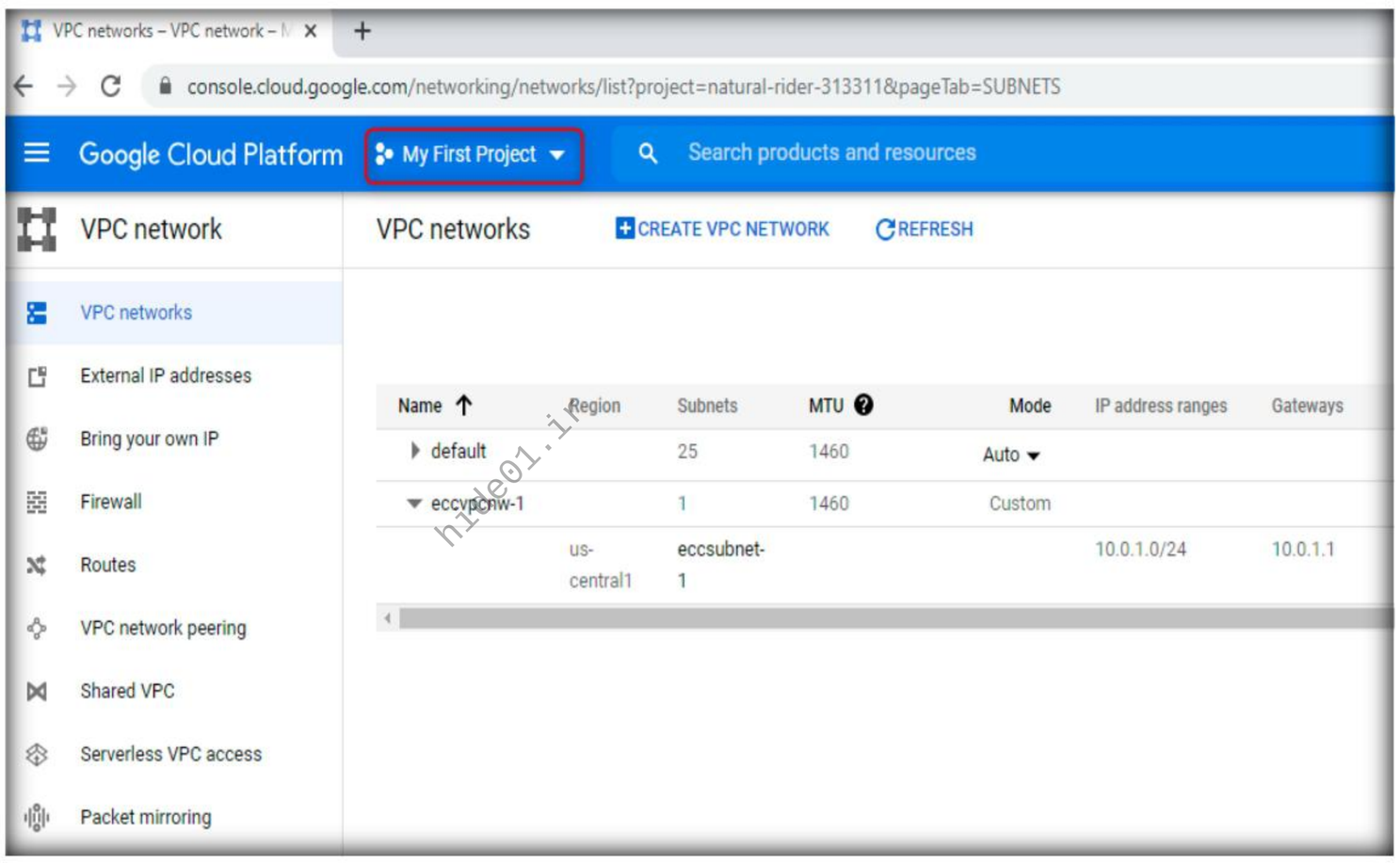


FIGURE 2.10.26: Switching Projects

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

29. Select the second project from the window that opens.

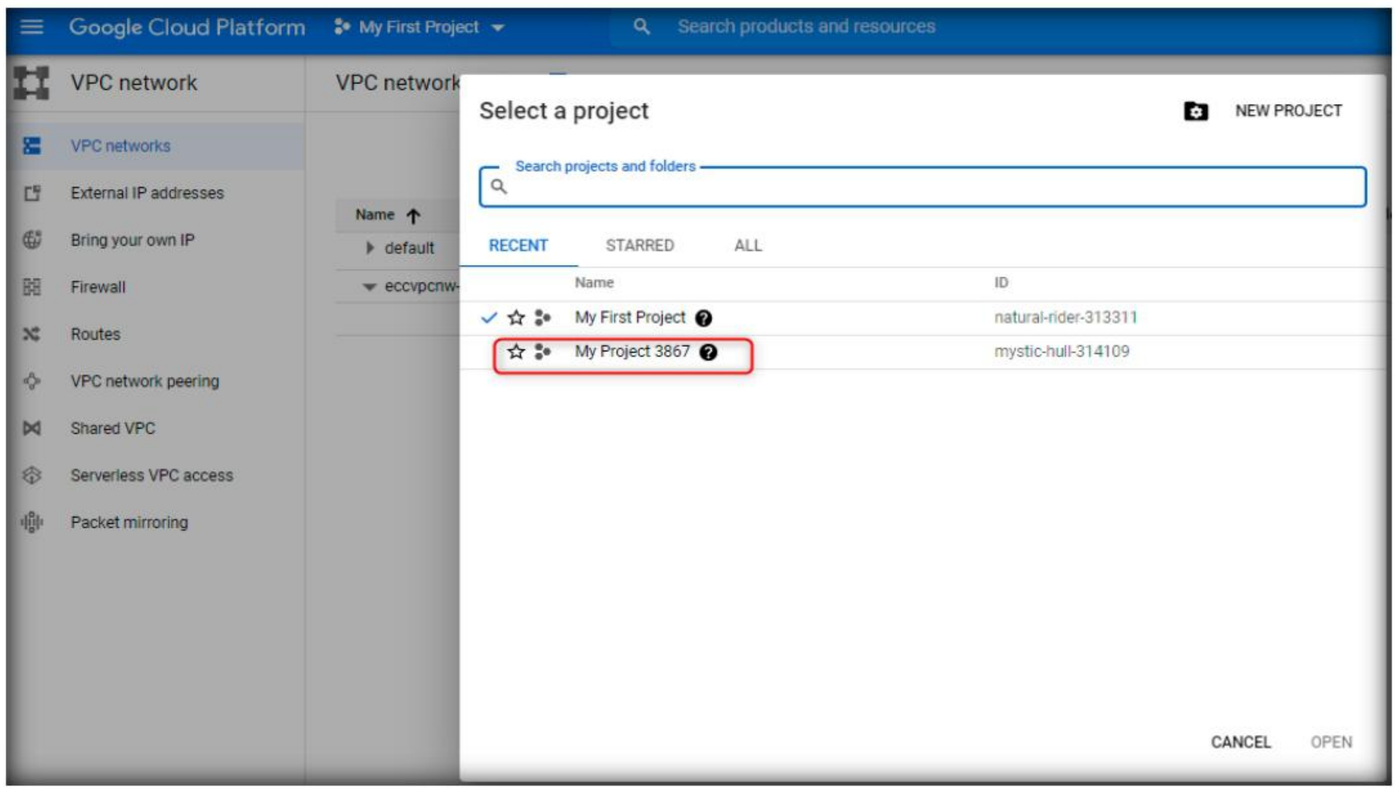


FIGURE 2.10.27: Selecting the Second Project

30. Now, configure the second project's VPC network by navigating to **VPC network** and selecting **VPC networks** in the console.

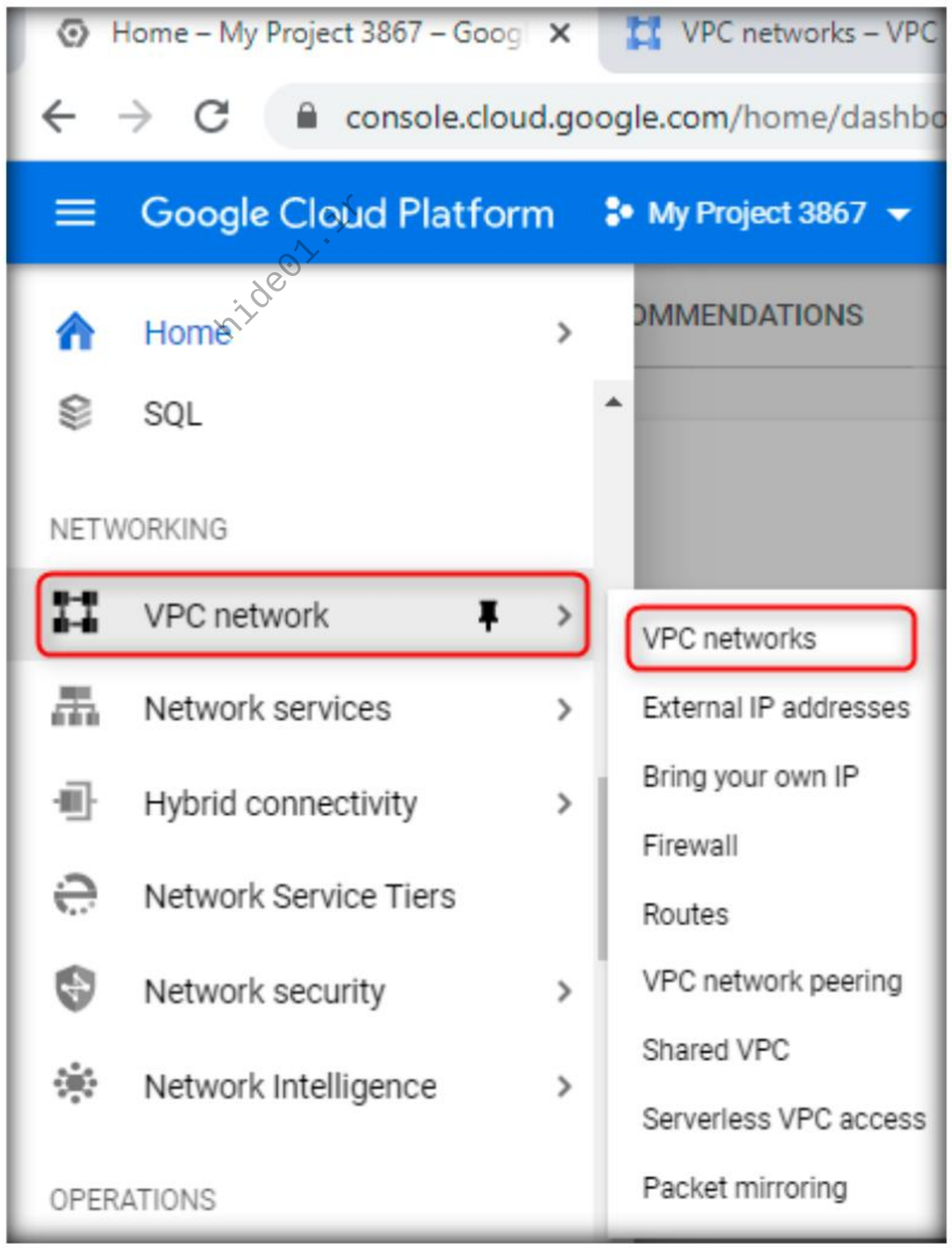


FIGURE 2.10.28: Navigating to VPC networks

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

31. In the **VPC networks** window, click on **CREATE VPC NETWORK**.

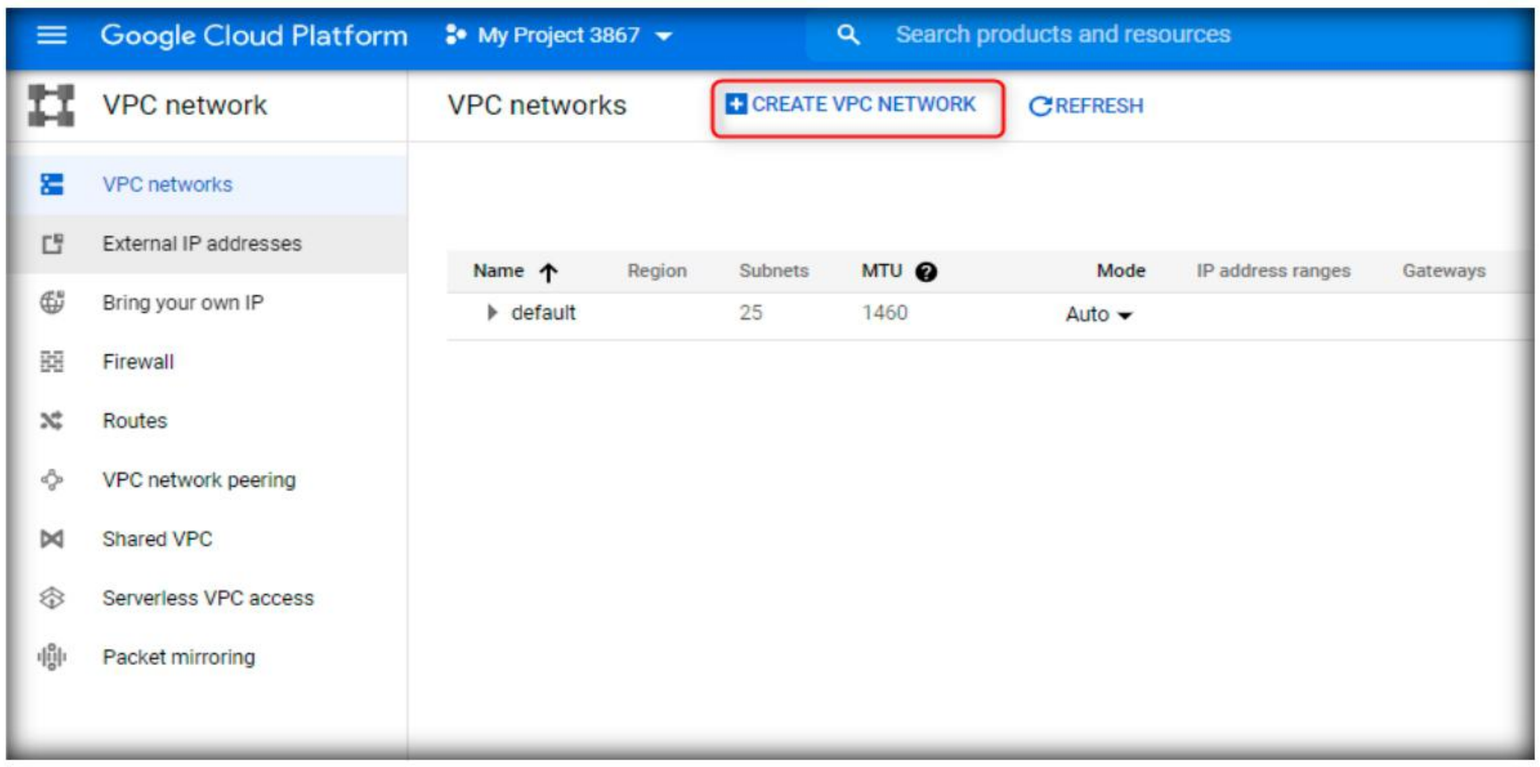


FIGURE 2.10.29: Creating VPC Network

32. Provide an appropriate **Name** for the VPC network. In this lab, we have named the VPC network as **eccvpcnw-2**. For **Subnet creation mode**, select **Custom**.

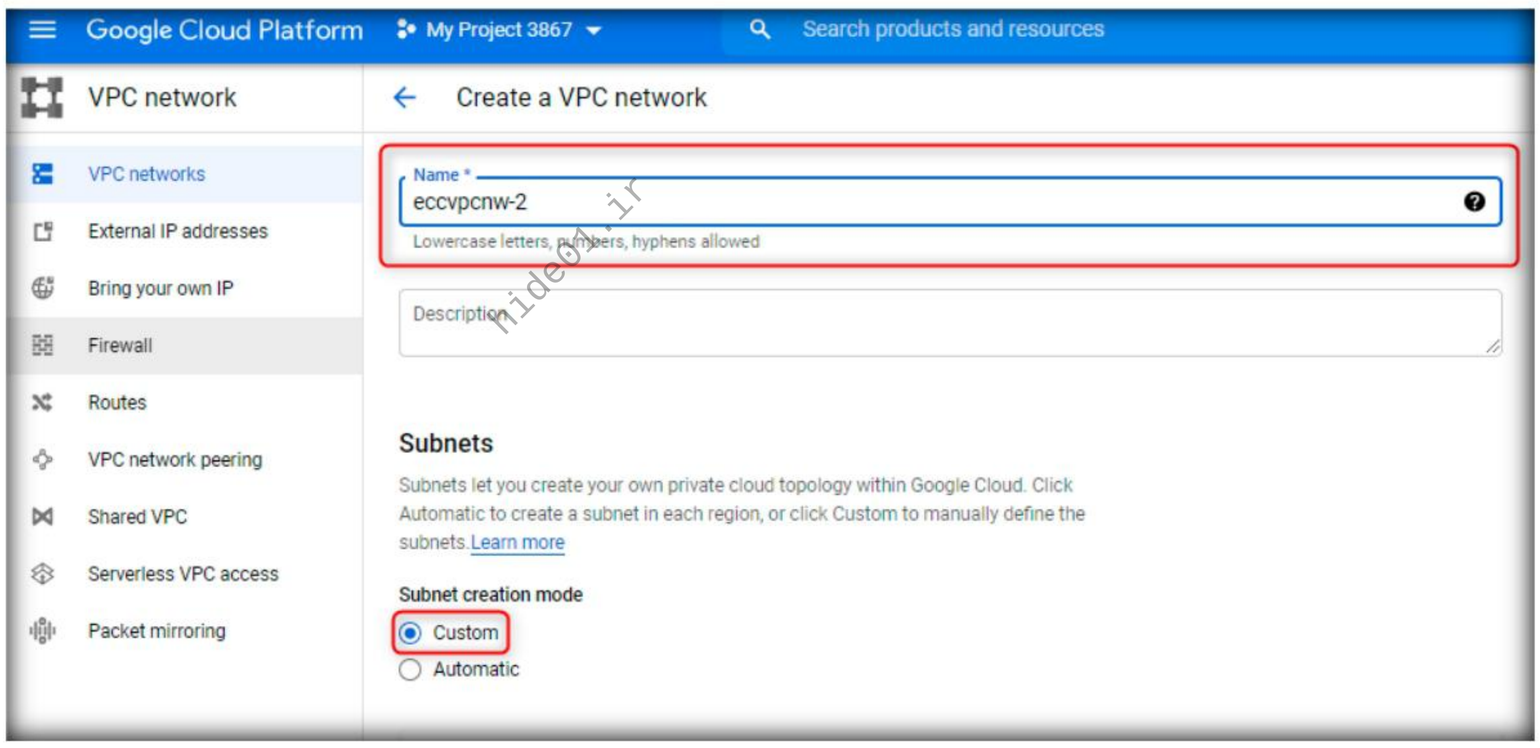


FIGURE 2.10.30: Giving a Name and selecting subnet creation mode

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

33. Now, scroll down to the bottom and provide an appropriate **Name**, **Region**, **and IP address range** for the subnet. In this lab, we have created the subnet with the following details:

    Name: **eccsubnet-2**

    Region: **us-central1**

    IP address range: **10.0.2.0/24**

    Retain the other default settings and click **DONE**.

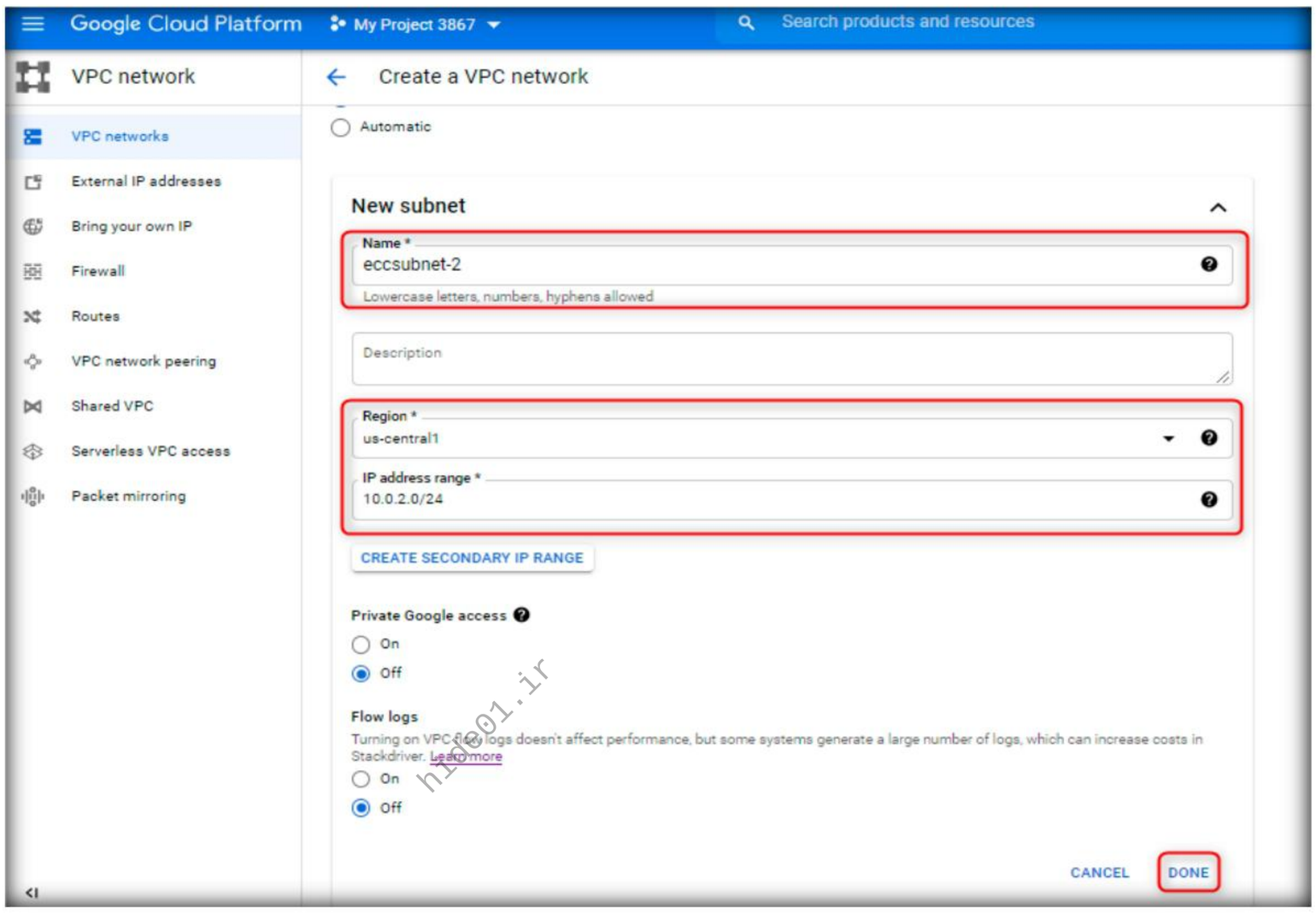


FIGURE 2.10.31: Creating Subnet for VPC networks

34. Retain the other default settings and click on **CREATE**.

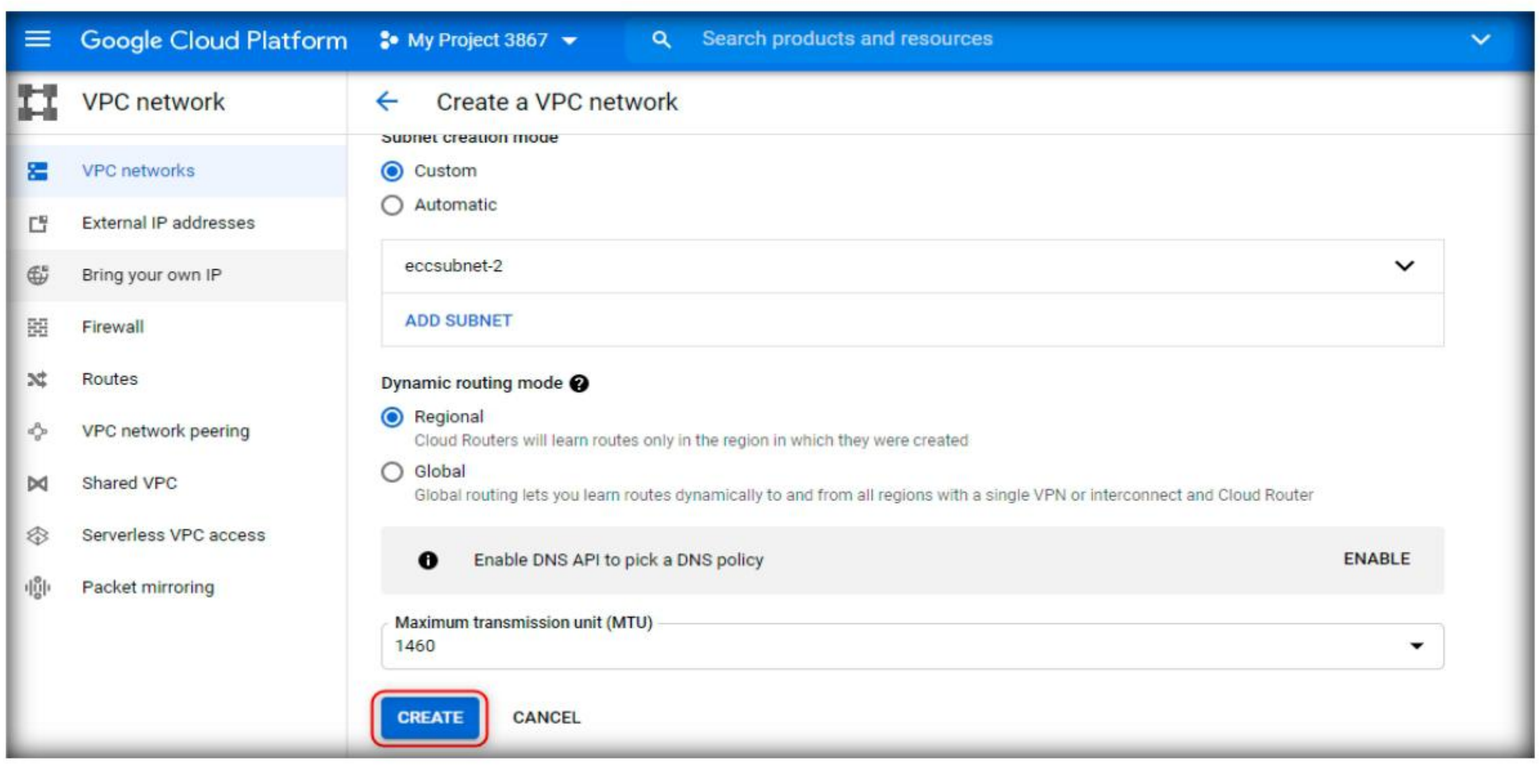


FIGURE 2.10.32: Creating a VPC Network

35. You have now created a new VPC network for your second project.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

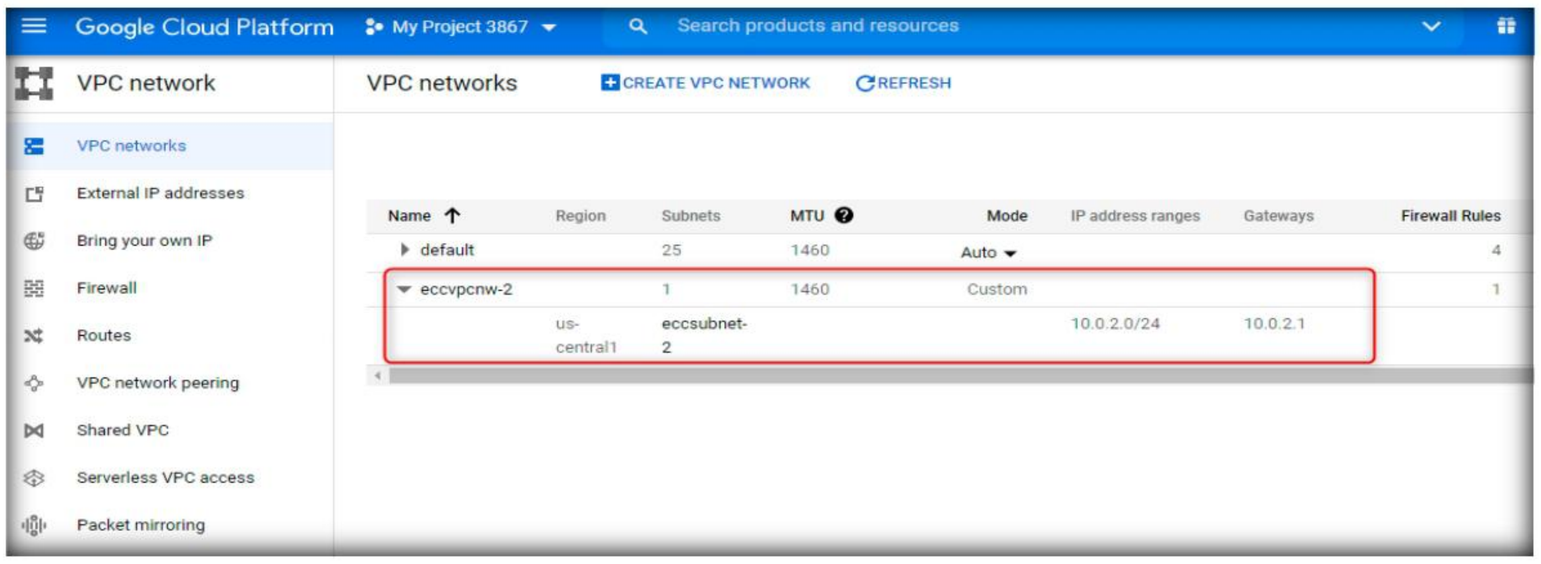


FIGURE 2.10.33: Created the new VPC Network

36. Now, configure a firewall rule for allowing **SSH** connections, as in the first VPC network, by repeating **Steps 20–26**.

    Note: Give a different name to the firewall rule.

37. You have now created the second VPC network and configured its firewall rule.

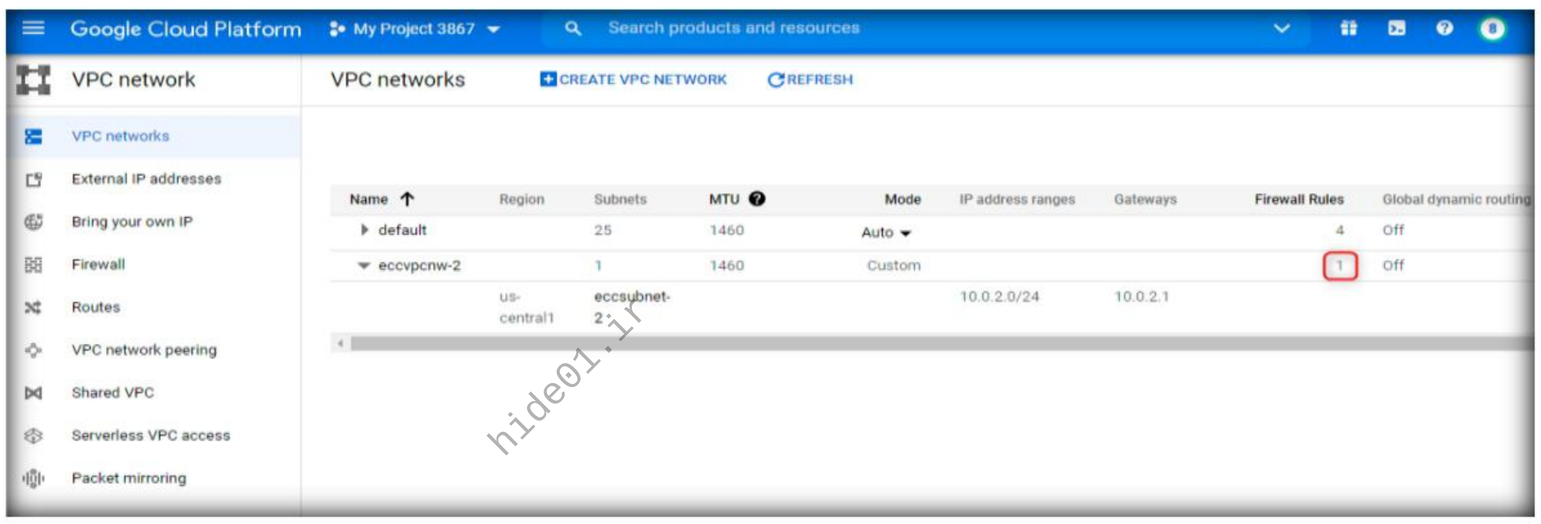


FIGURE 2.10.34: Created the new firewall rule for the VPC Network

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 3

Creating New Instances and Configuring VPC Networks in both projects

38. Next, create instances in both the projects and configure the VPC networks for them.
39. Switch to the first project.

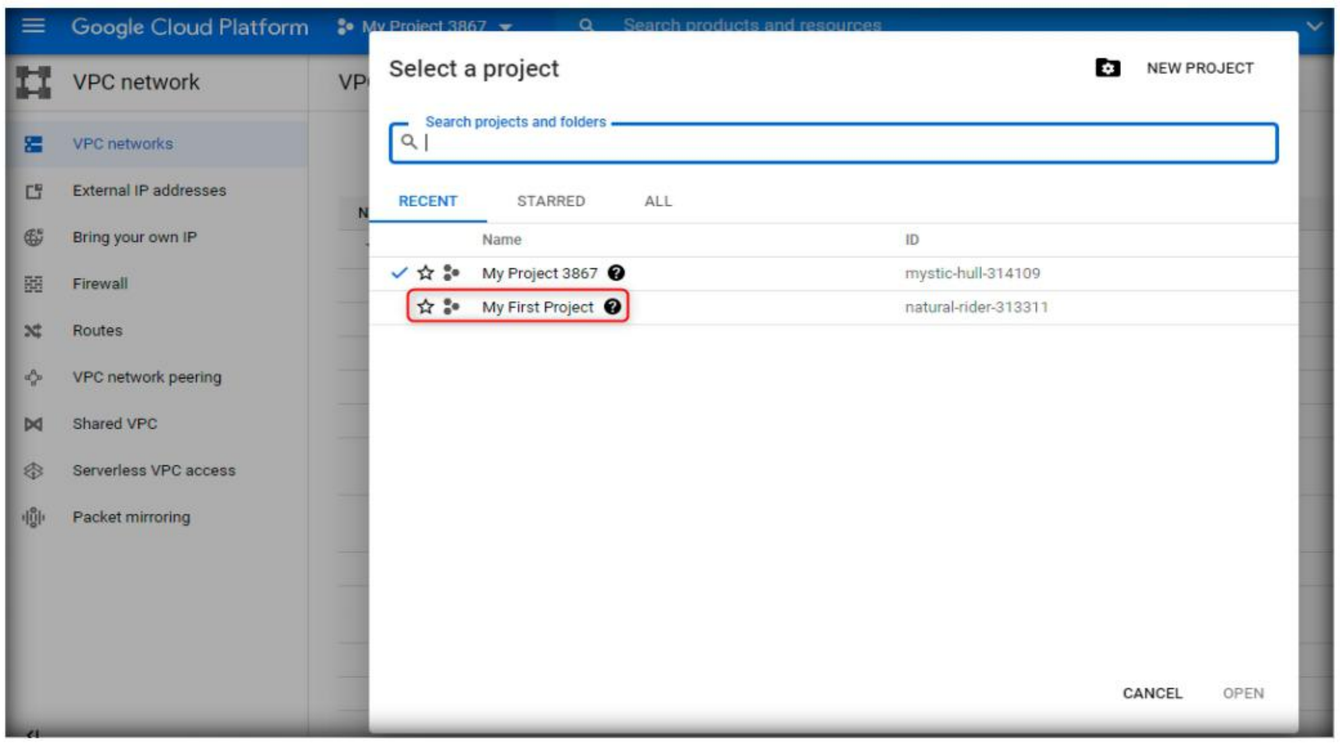


FIGURE 2.10.35: Switching to the first project

40. Navigate to **Compute Engine** and select **VM Instances** in the console.

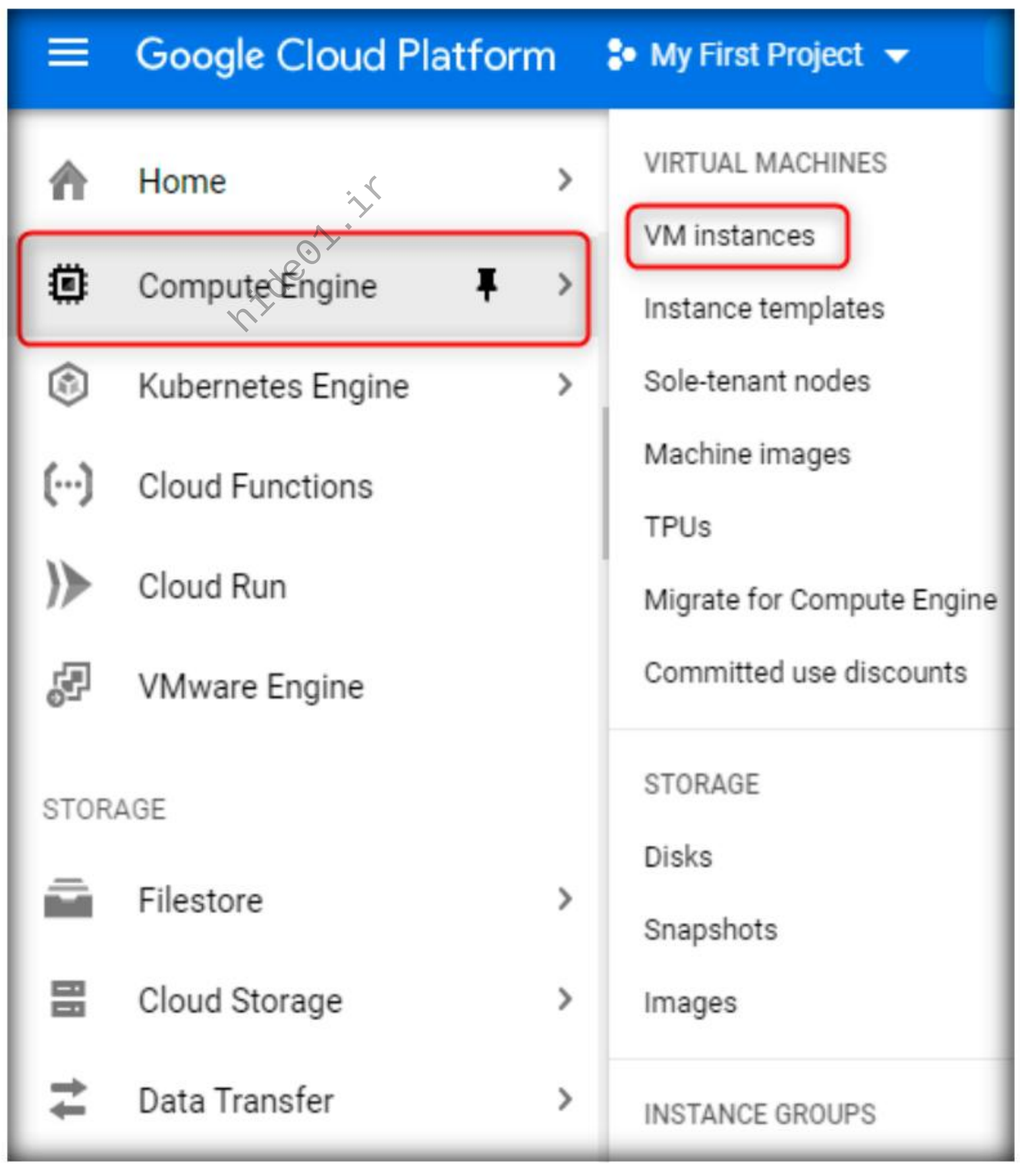


FIGURE 2.10.36: Navigating to VM Instances

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

41. Click on **CREATE INSTANCE** at the top.

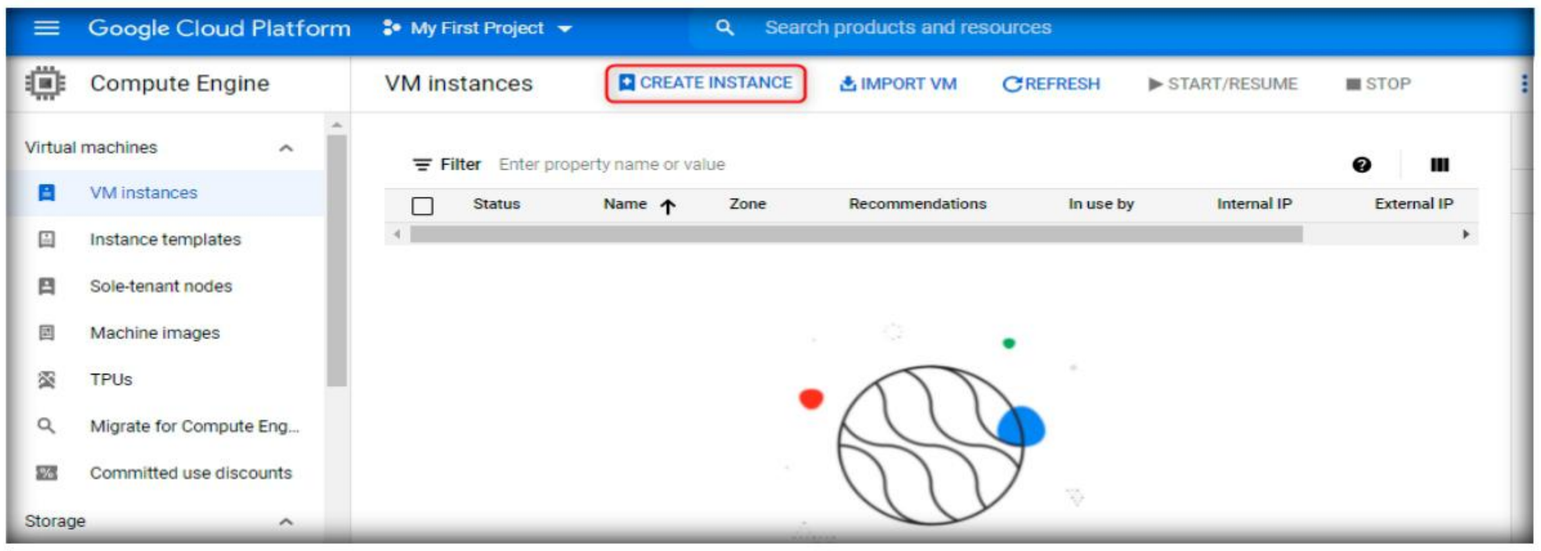


FIGURE 2.10.37: Creating New Instance

42. Provide the appropriate details for the new instance. In this lab, we are creating an instance with the following details:

Name: usinstance-1

Region: us-central1

Zone: us-central1-a

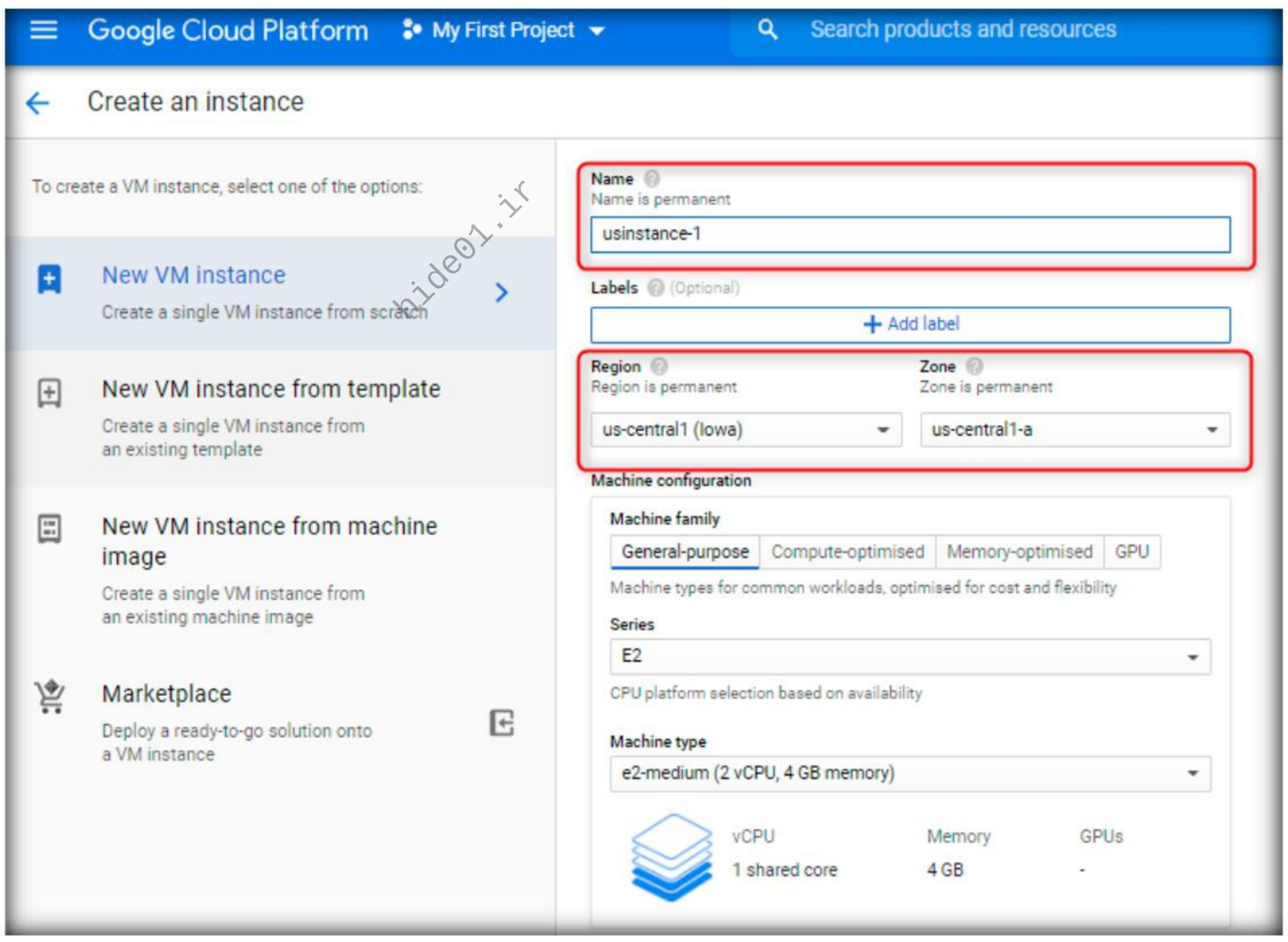


FIGURE 2.10.38: Entering the Name and selecting Region and Zone

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

43. Scroll down to the bottom and click on **Management, security, disks, networking sole tenancy**.

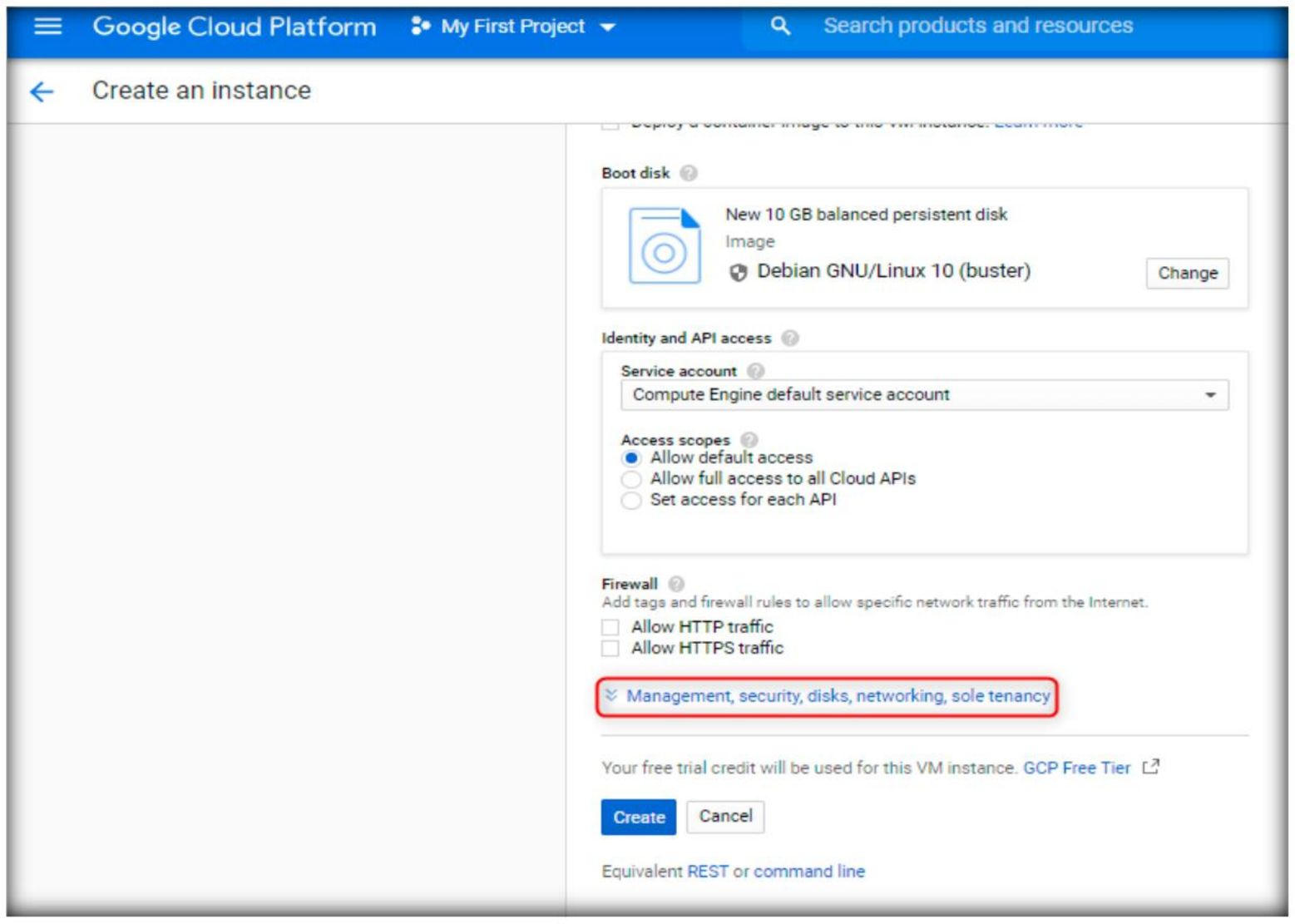


FIGURE 2.10.39: Configuring networking

44. Click on **Networking**.

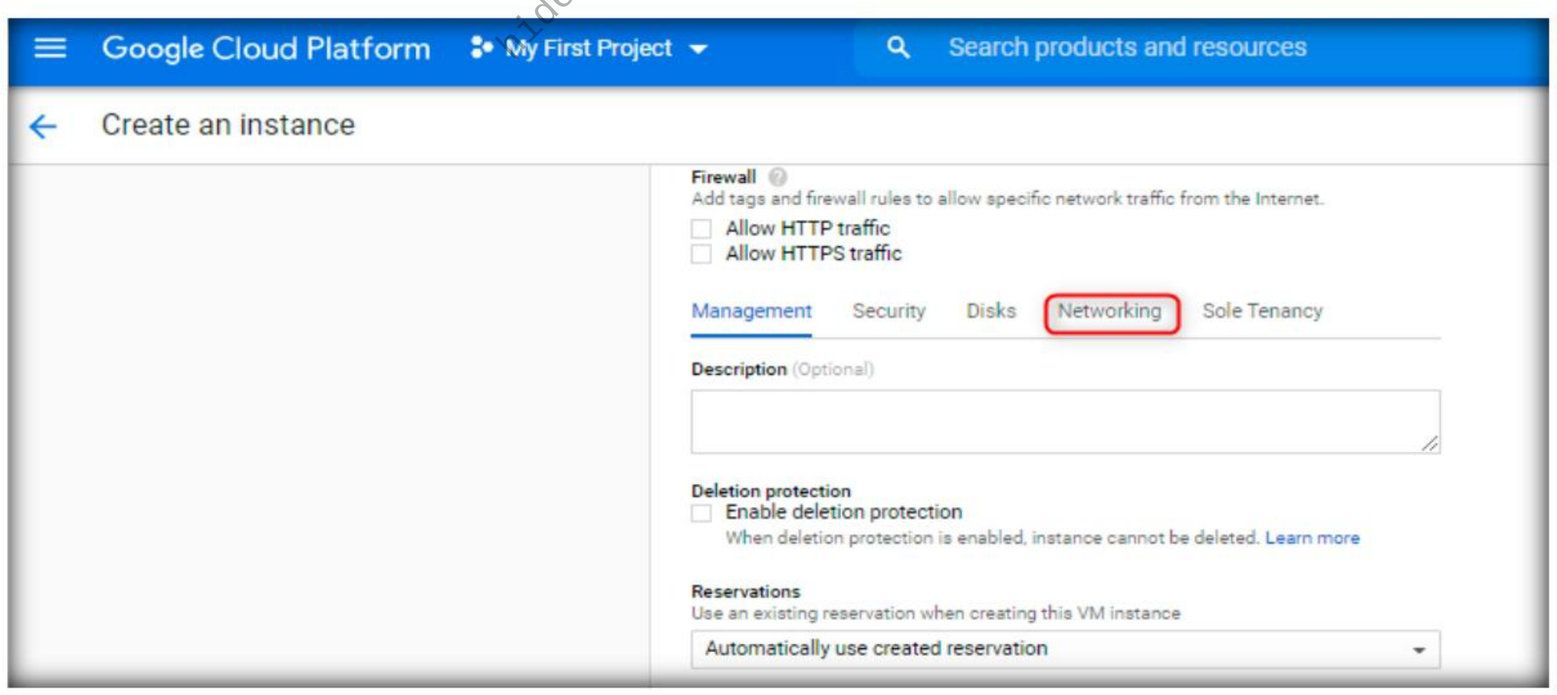


FIGURE 2.10.40: Selecting Networking

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

45. In **Networking**, click on the **edit** icon at the right side of the **default** network interface below **Network interfaces**.

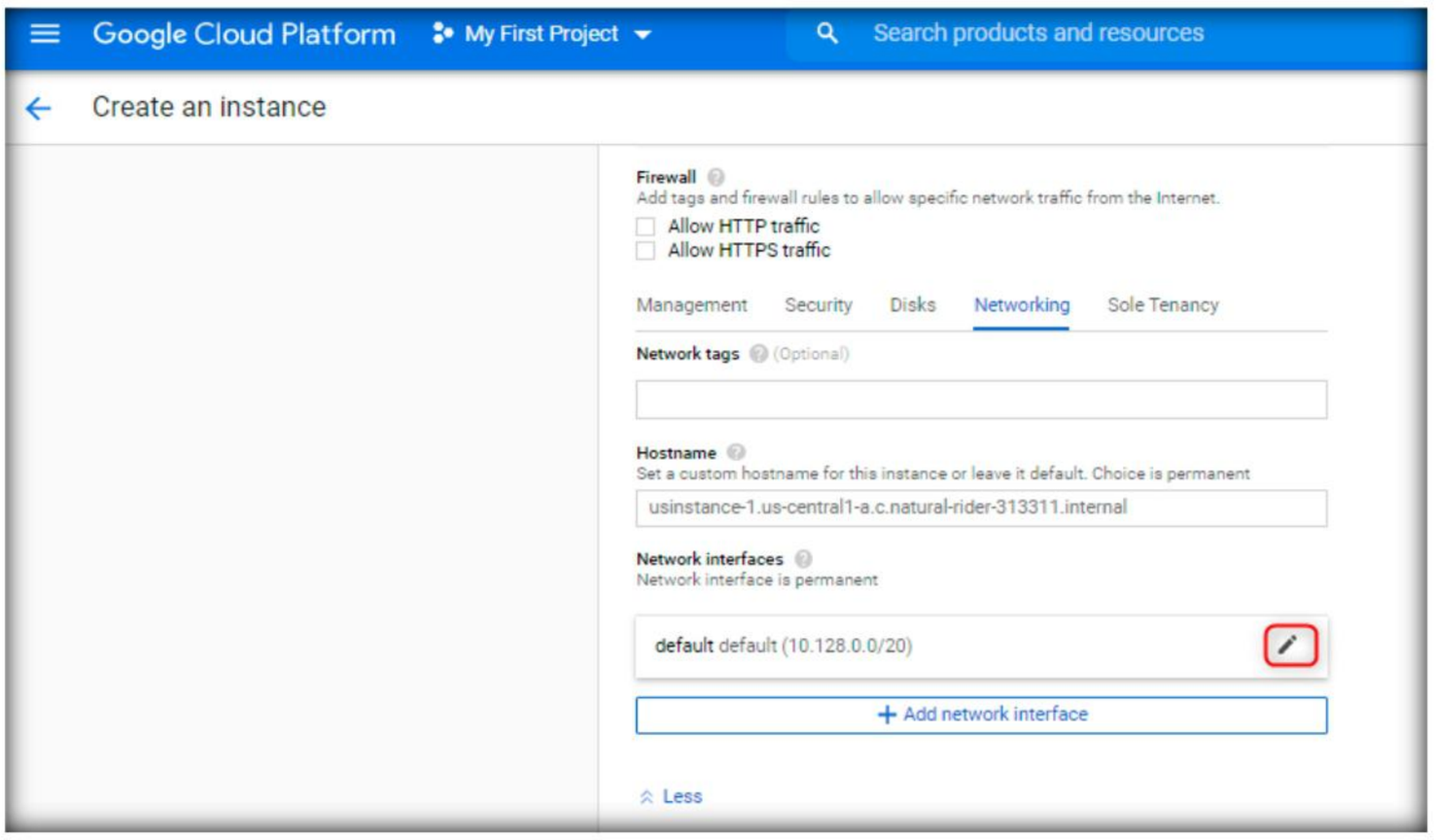


FIGURE 2.10.41: Editing Network Interface

46. Select the VPC network (**eccvpcnw-1**) that was created in the previous task from the dropdown.

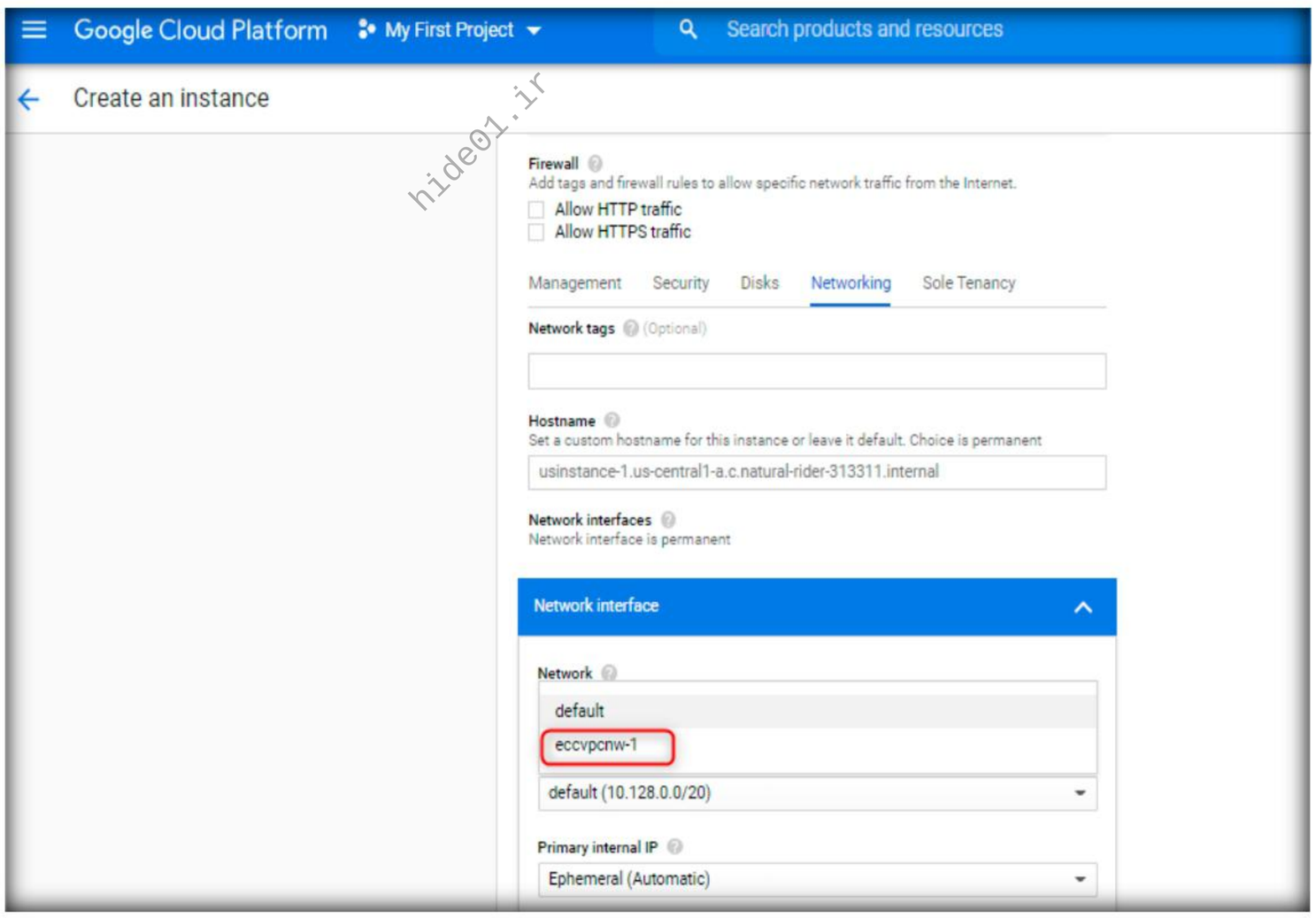


FIGURE 2.10.42: Selecting VPC network

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

47. Retain the other default settings and click on **Done**.

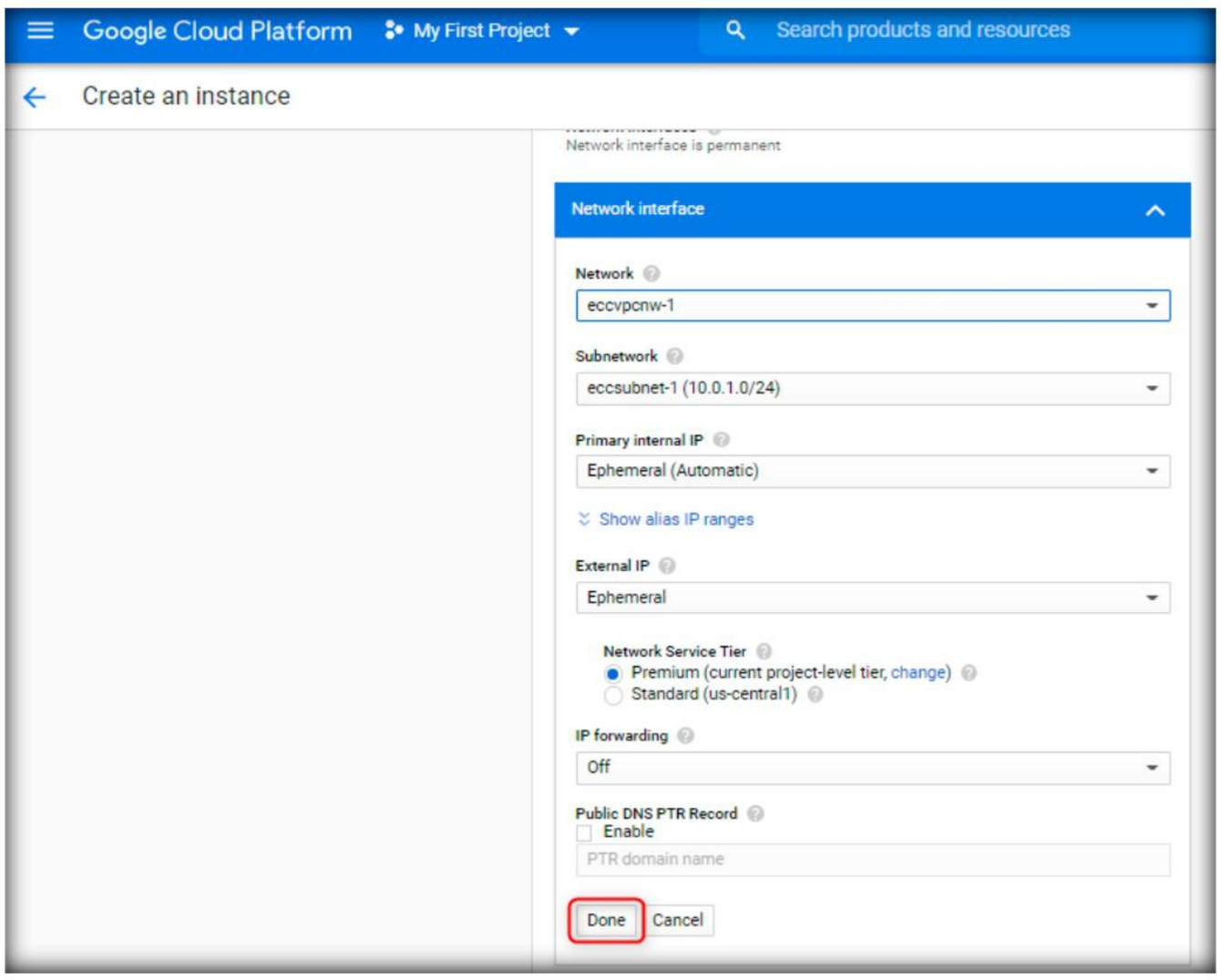


FIGURE 2.10.43: Finish configuring the VPC network

48. Click on **Create** to finish creating the new instance with the configured VPC network.

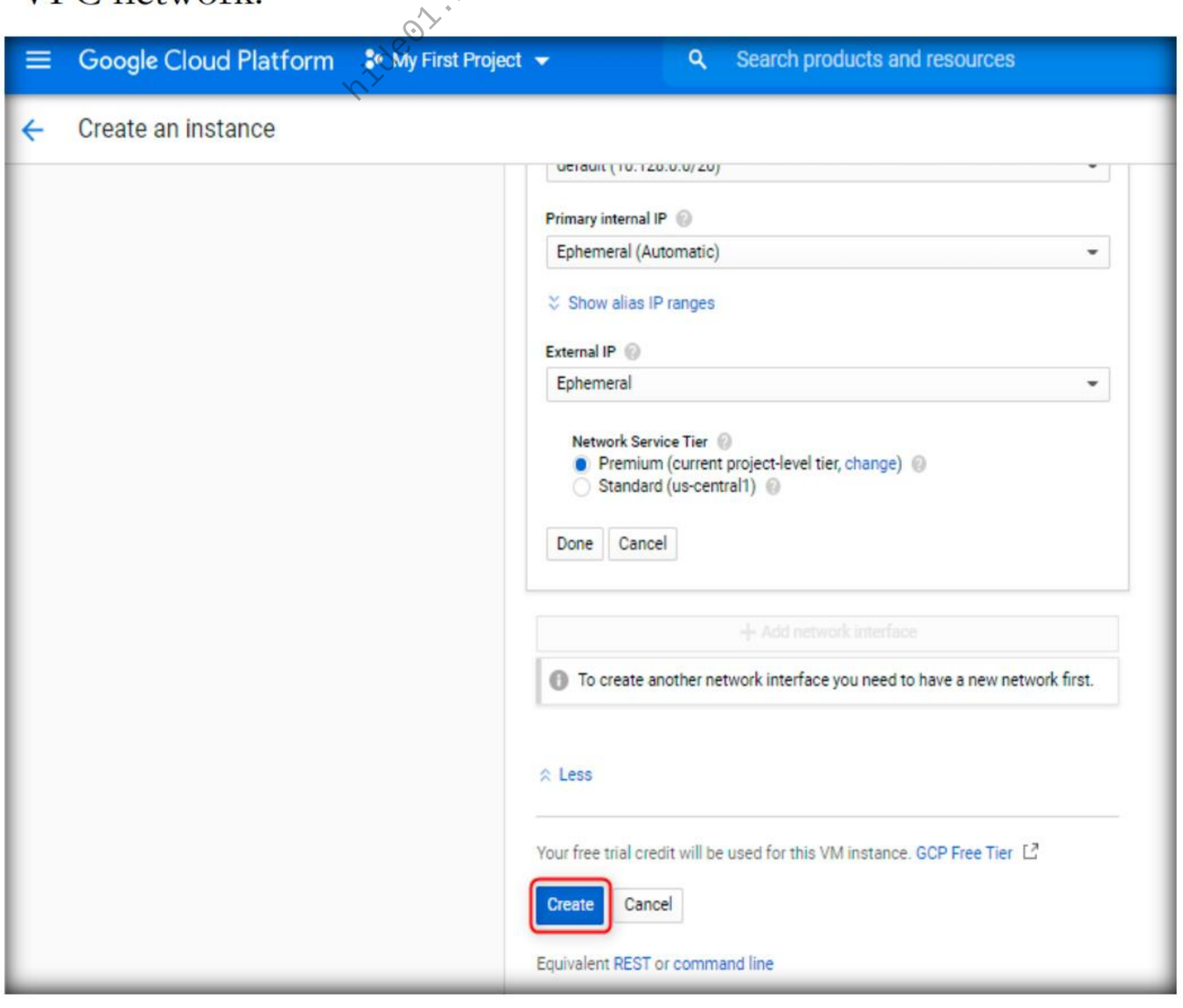


FIGURE 2.10.44: Finish Creating the Instance

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

49. Note the **Internal IP** of the instance for future reference.

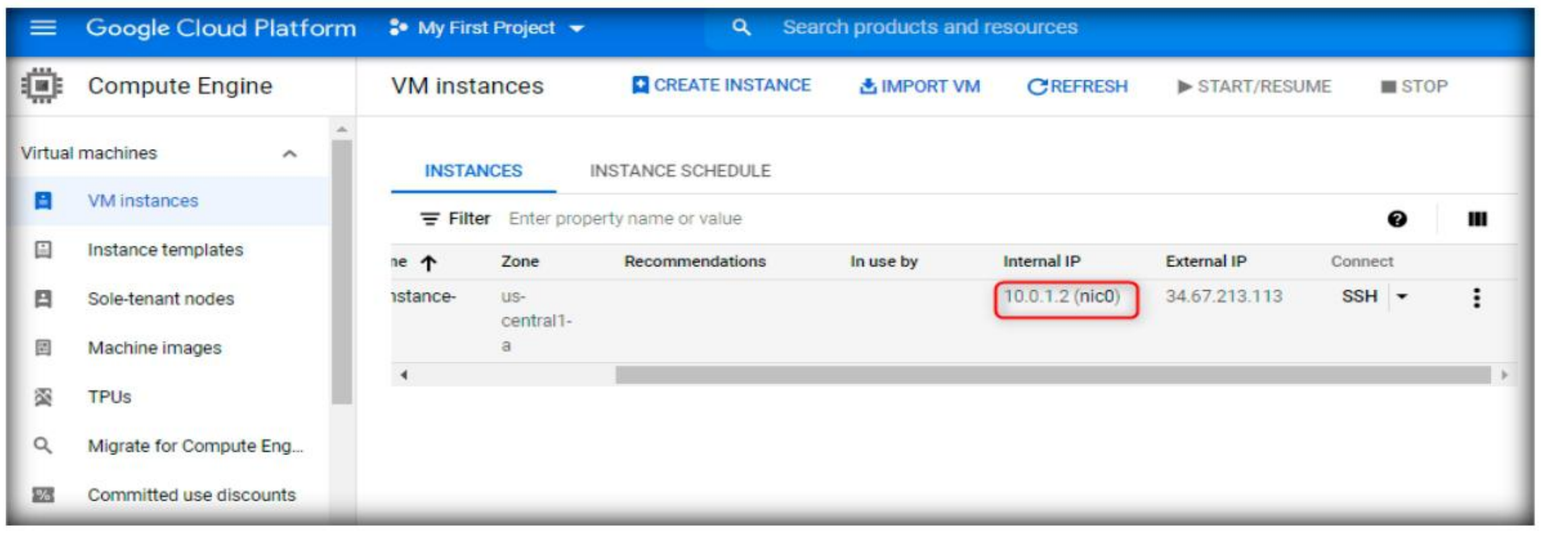


FIGURE 2.10.45: Internal IP

50. Now, switch to the second project.

51. Navigate to **Compute Engine** and select **VM Instances**.

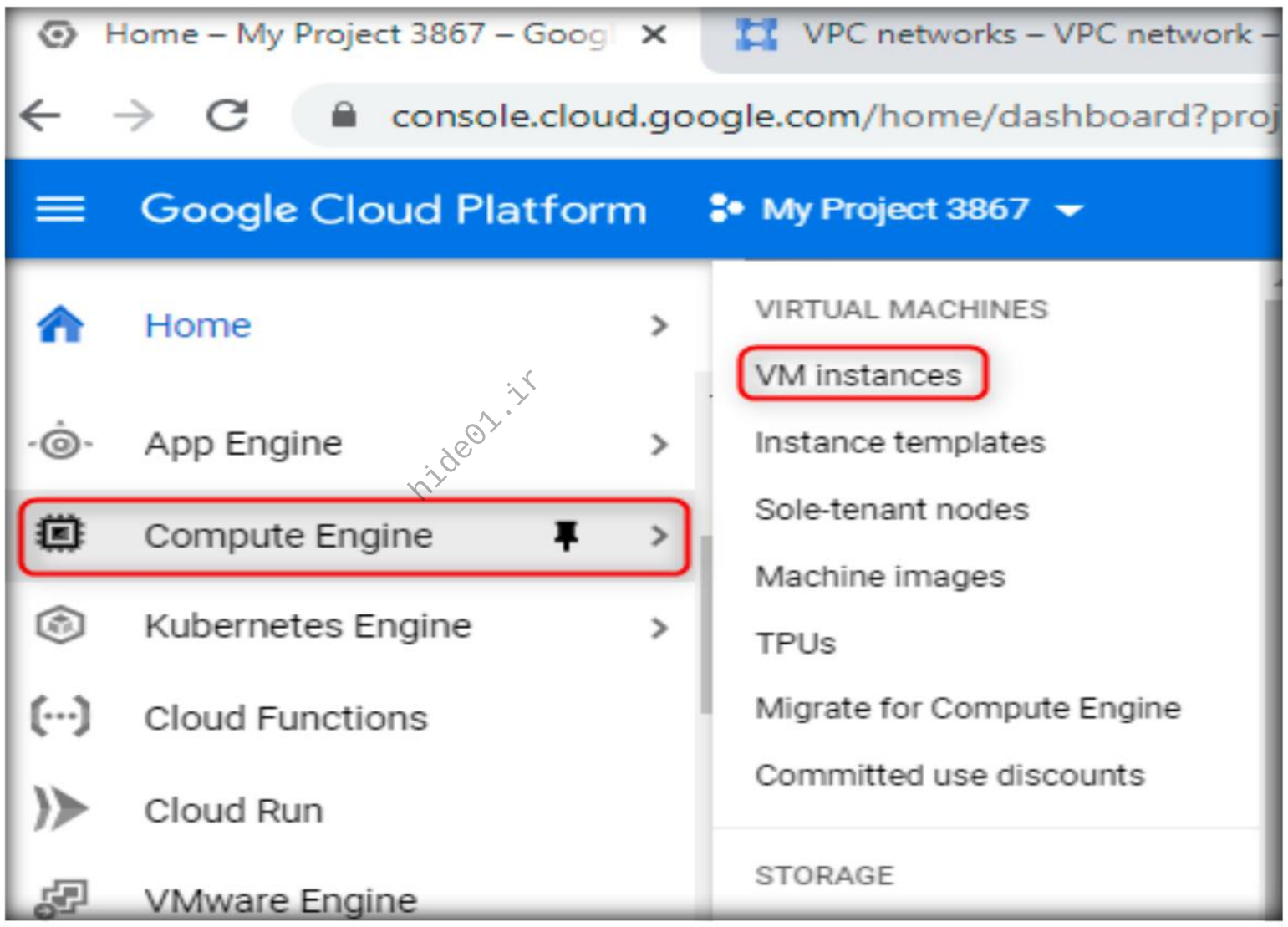


FIGURE 2.10.46: Navigating to VM Instances

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

52. Since you are creating Compute Engine instances for the first time in the second project, you will see a window to enable the **Compute Engine API**. Click on **ENABLE** and wait for it to be enabled.

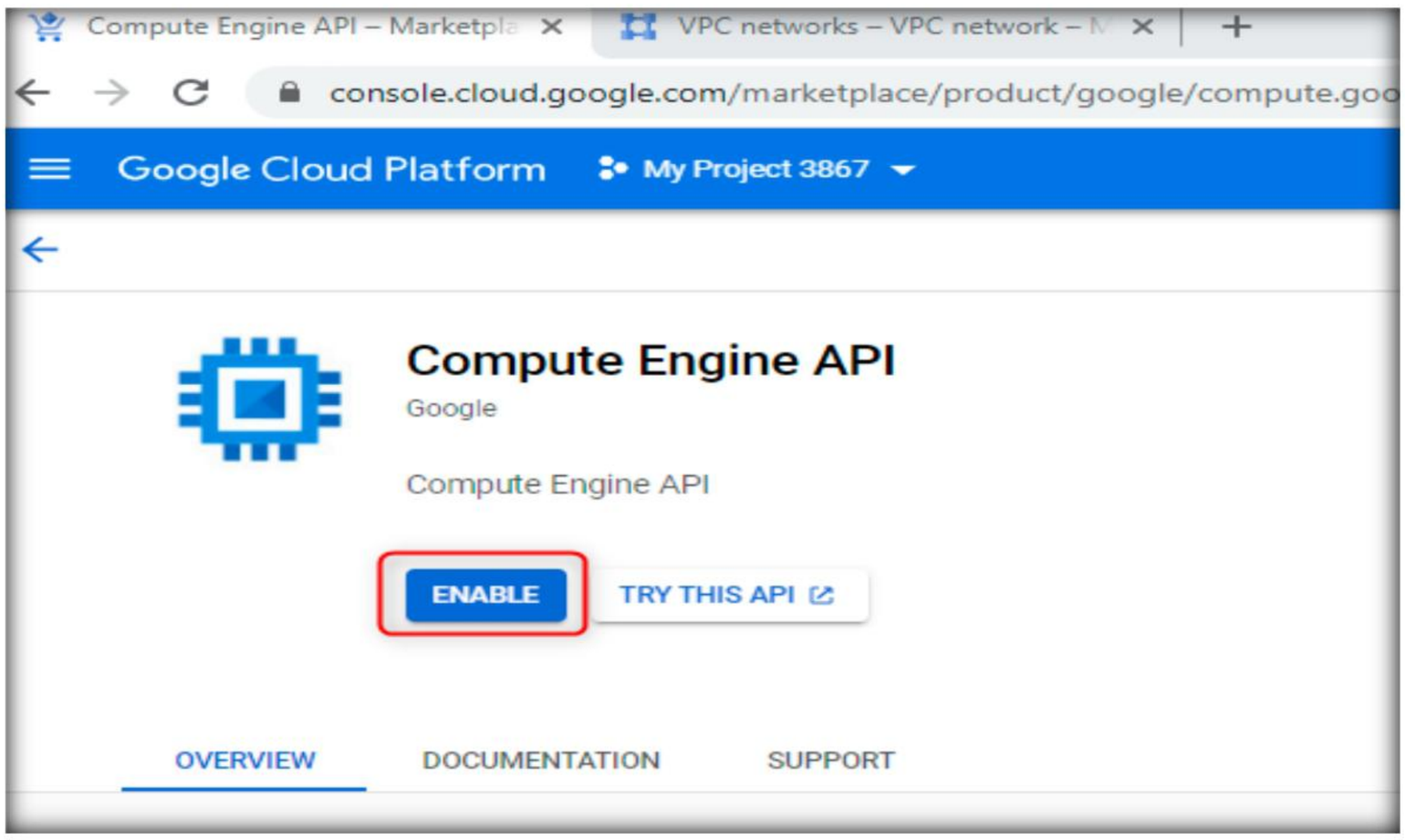


FIGURE 2.10.47: Enabling Compute Engine API

53. Once it is enabled, repeat the steps for the first project, that is, **Steps 40–48**, to create the instance and configure the VPC network for the second project.

    Note: Use a different name for the second project instance.

54. You have now created an instance for the second project and configured the VPC network created in the previous task. In addition, note the internal IP of the VM instance.

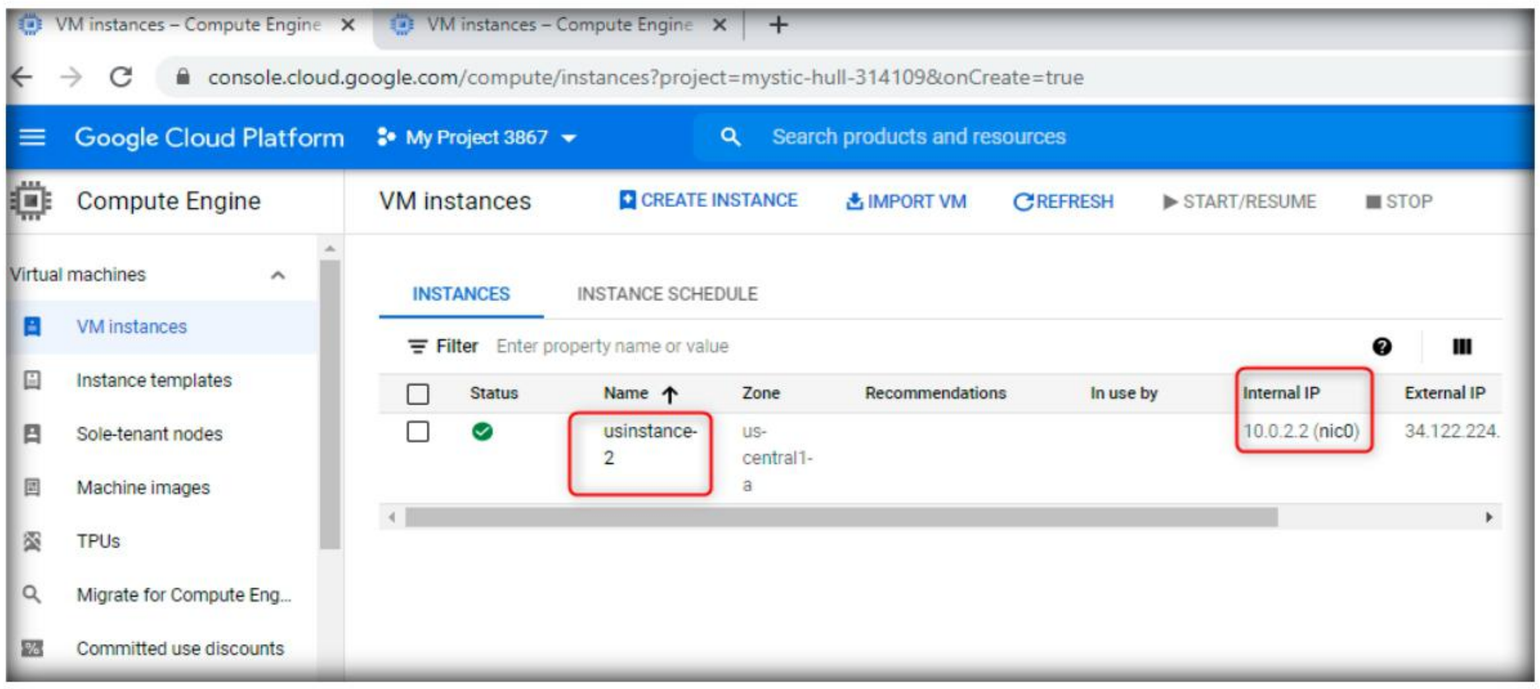


FIGURE 2.10.48: Configured VPC networks and created the instance

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 4

Implementing VPC Network Peering between the Instances

55. Now, switch to the first project. Navigate to **Compute Engine** and select **VM Instances**.

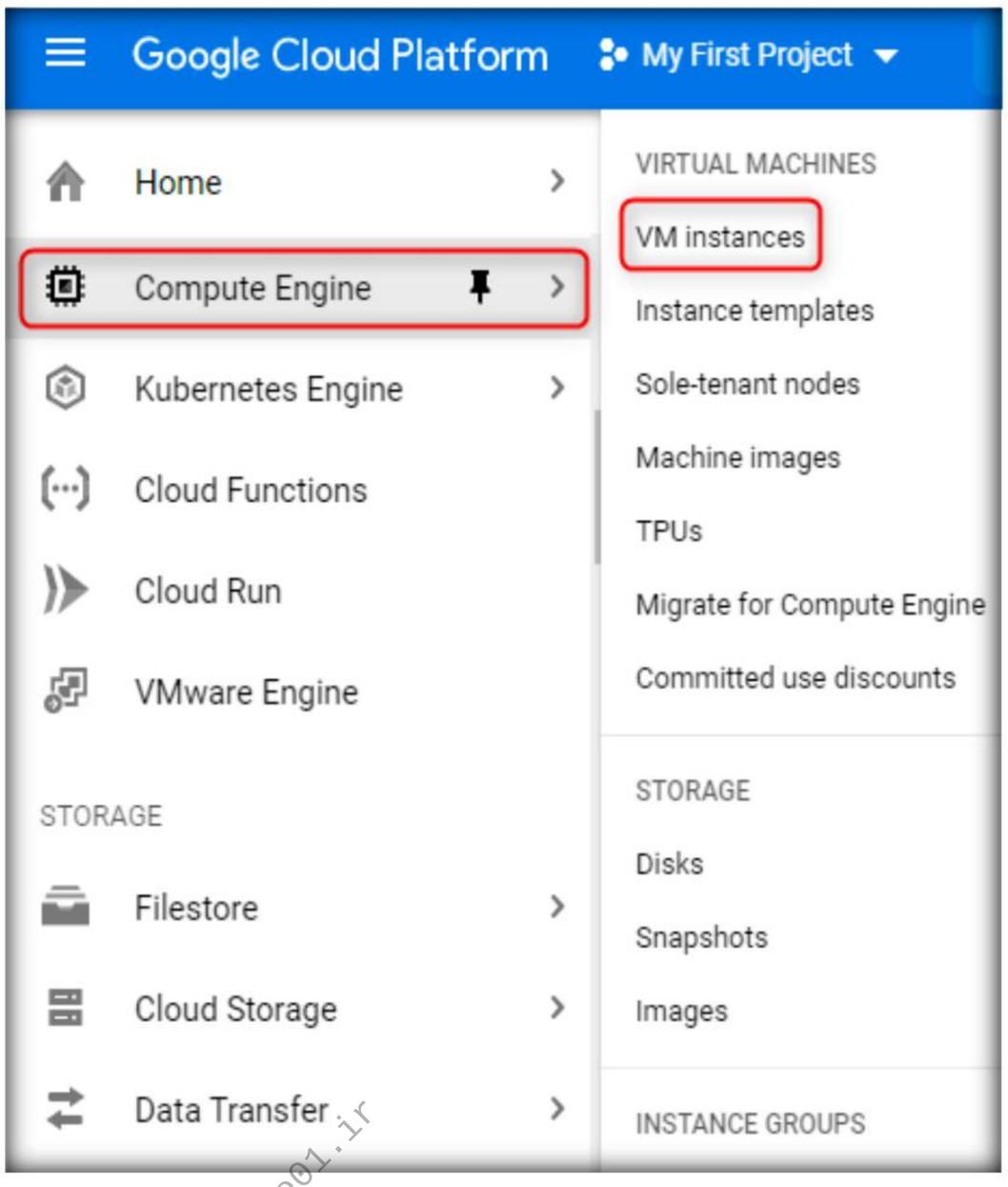


FIGURE 2.10.49: Navigating to VM Instances

56. Scroll to the right of the VM instance and click on **SSH** under **Connect**.

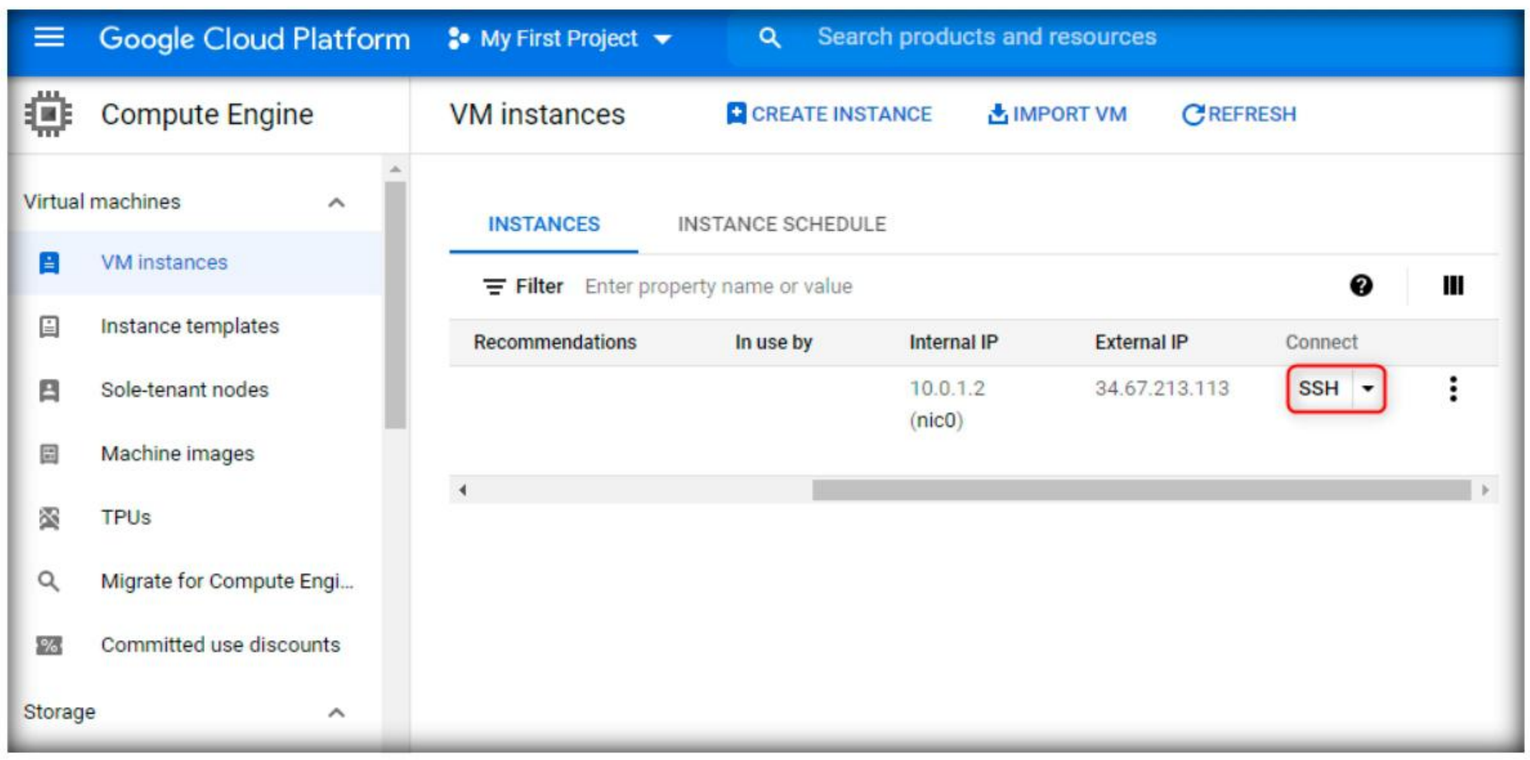


FIGURE 2.10.50: Selecting SSH

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

57. Now, verify whether the instances are connected. In the SSH window, type the following command and press **Enter**.

    ping <internal IP address> (replace <internal IP address> with the internal IP address of the second project instance).

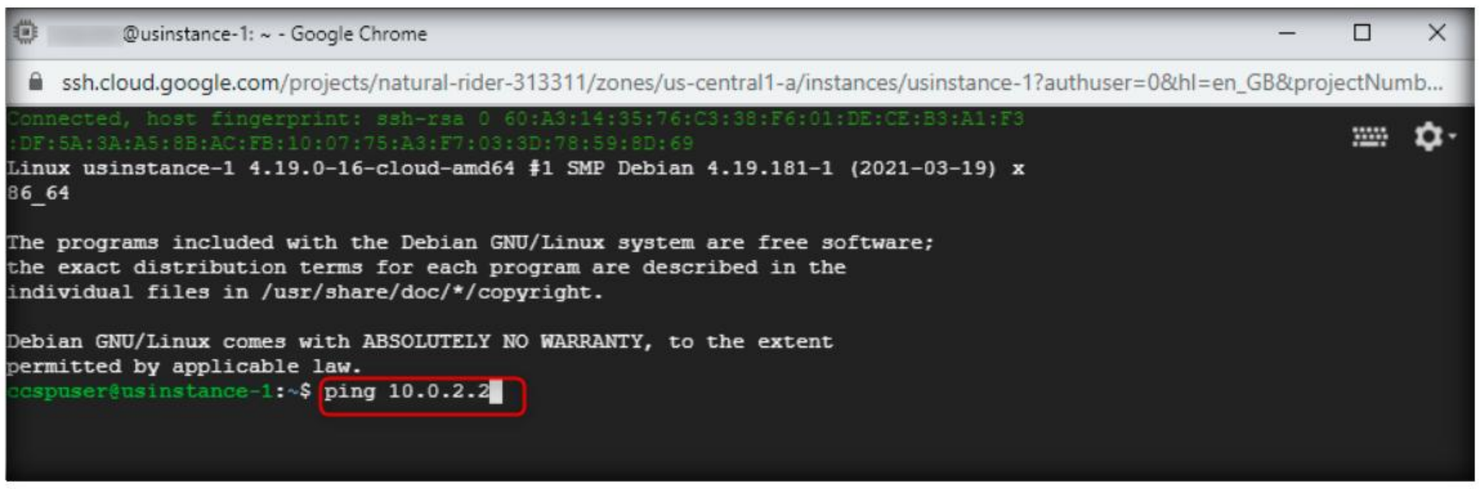


FIGURE 2.10.51: Checking connection to the other instance

58. There is no ping reply, as seen in the screenshot below, which indicates no connection has been established between the instances.

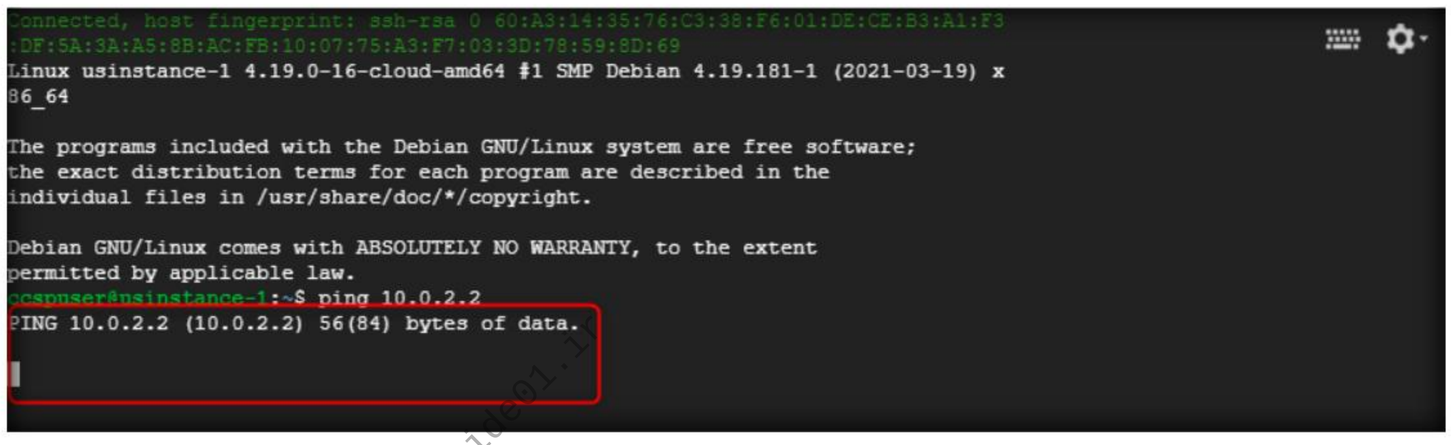


FIGURE 2.10.52: Connection is not established

59. Ensure you are on the first project. Set up **VPC Network Peering** between the instances to establish a secure connection between them. To do this, navigate to **VPC network** and select **VPC network peering**.

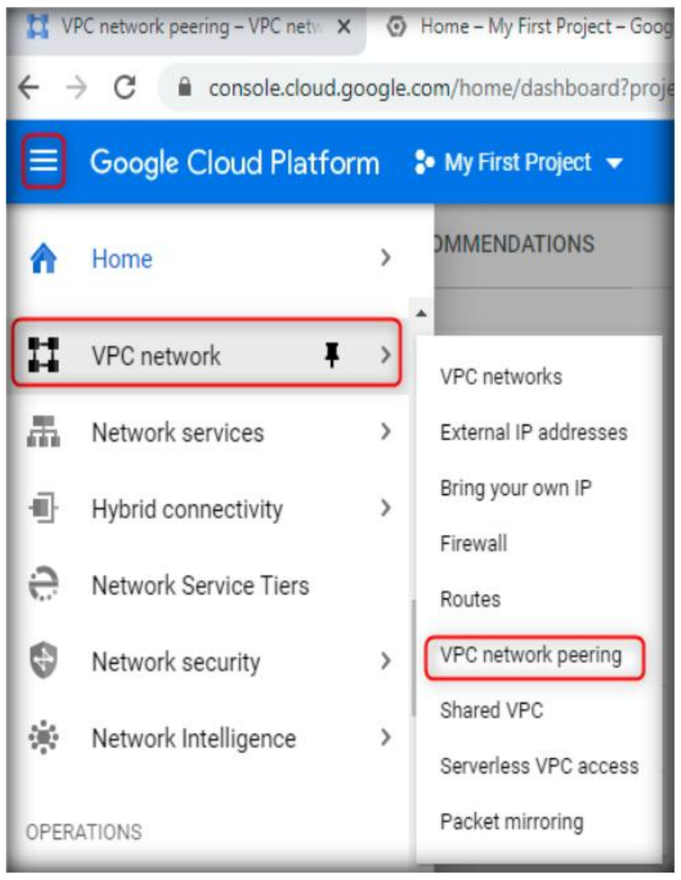


FIGURE 2.10.53: Navigating to VPC network peering

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

60. Click on **CREATE CONNECTION**.

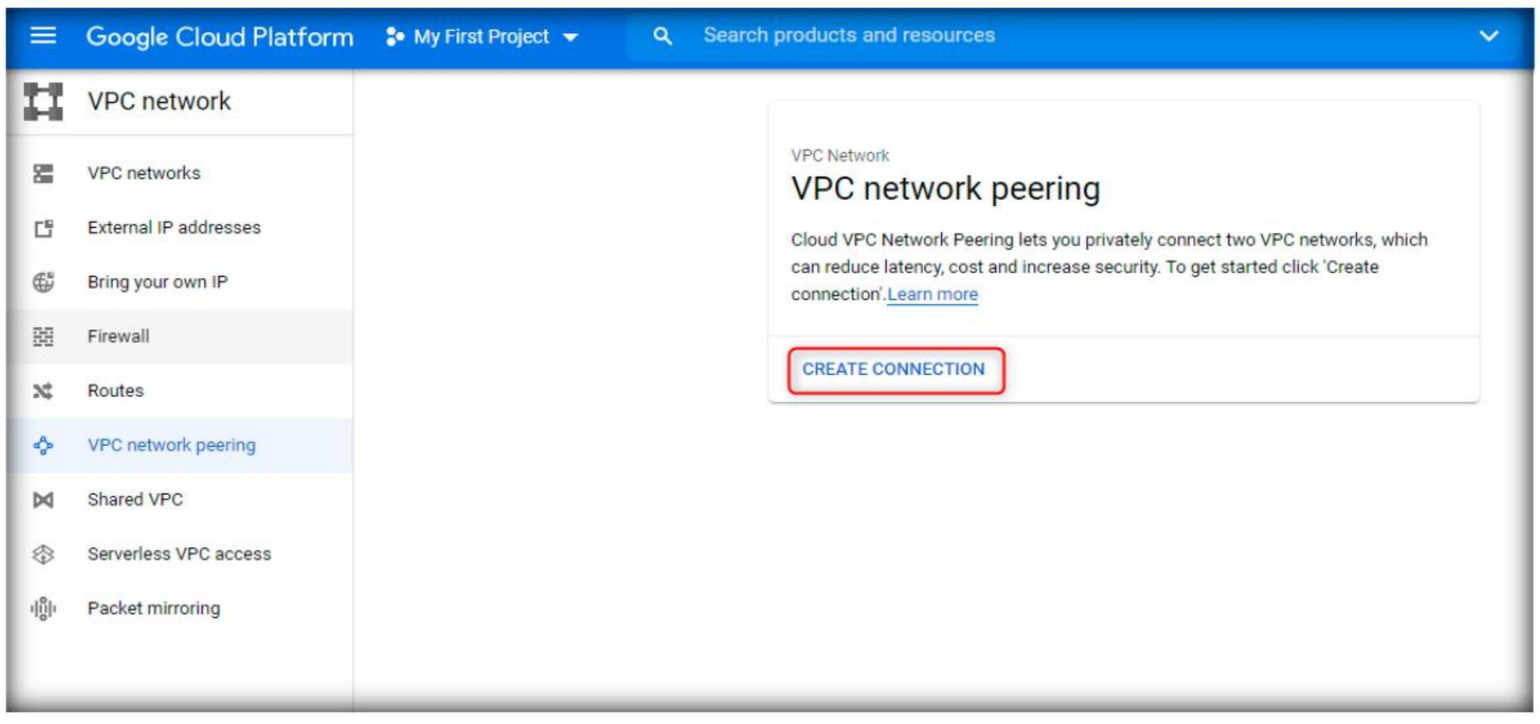


FIGURE 2.10.54: Creating Network peering

61. Click on **CONTINUE.**

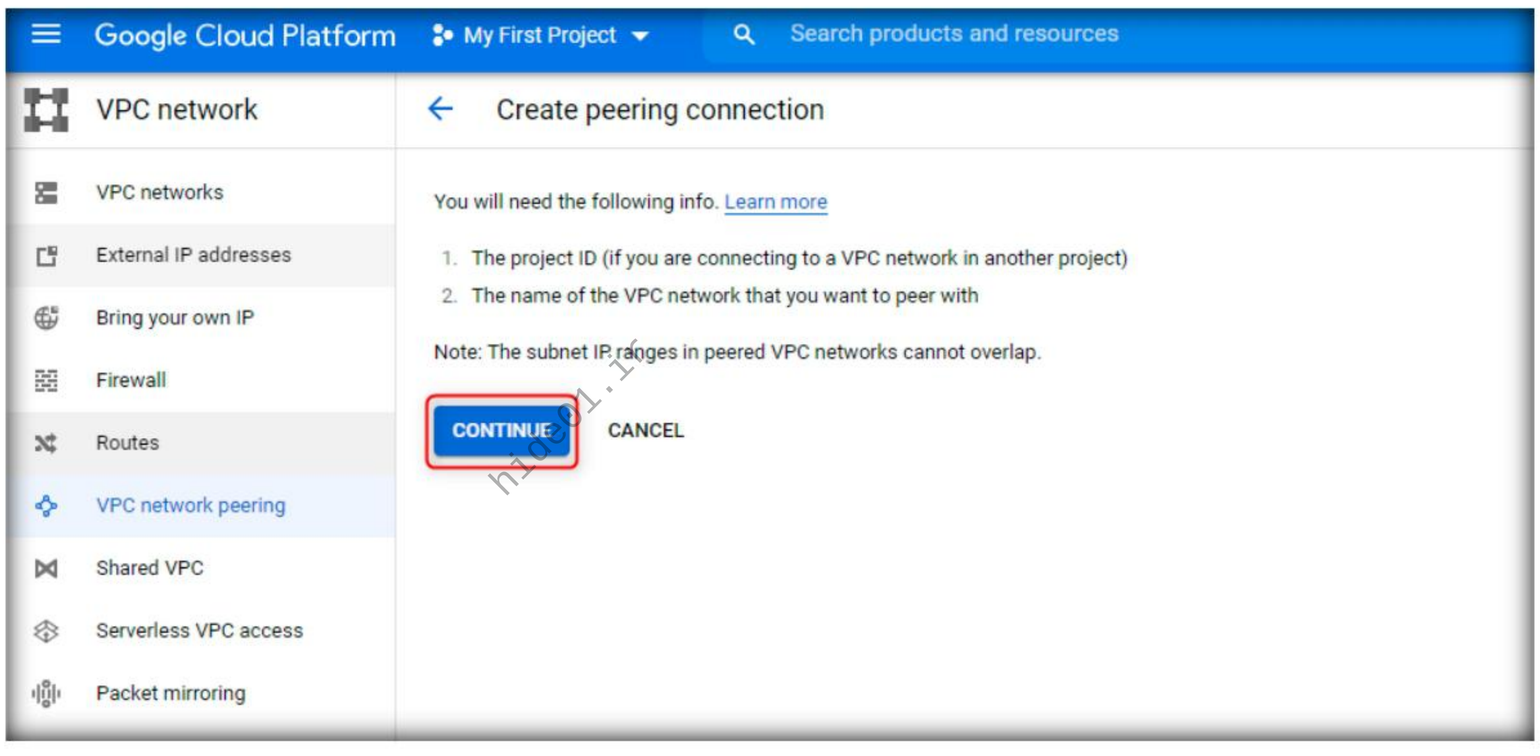


FIGURE 2.10.55: Continue creating the peering connection

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

62. In the **Create Peering Connection** window, provide the appropriate details for the peering connection. In this lab, we have used the following details:

    Name: eccinst1-eccinst2

    Your VPC network: eccvpcnw-1

    Peered VPC Network: In another project

    Project ID: mystic-hull-314109

    VPC network name: eccvpcnw-2

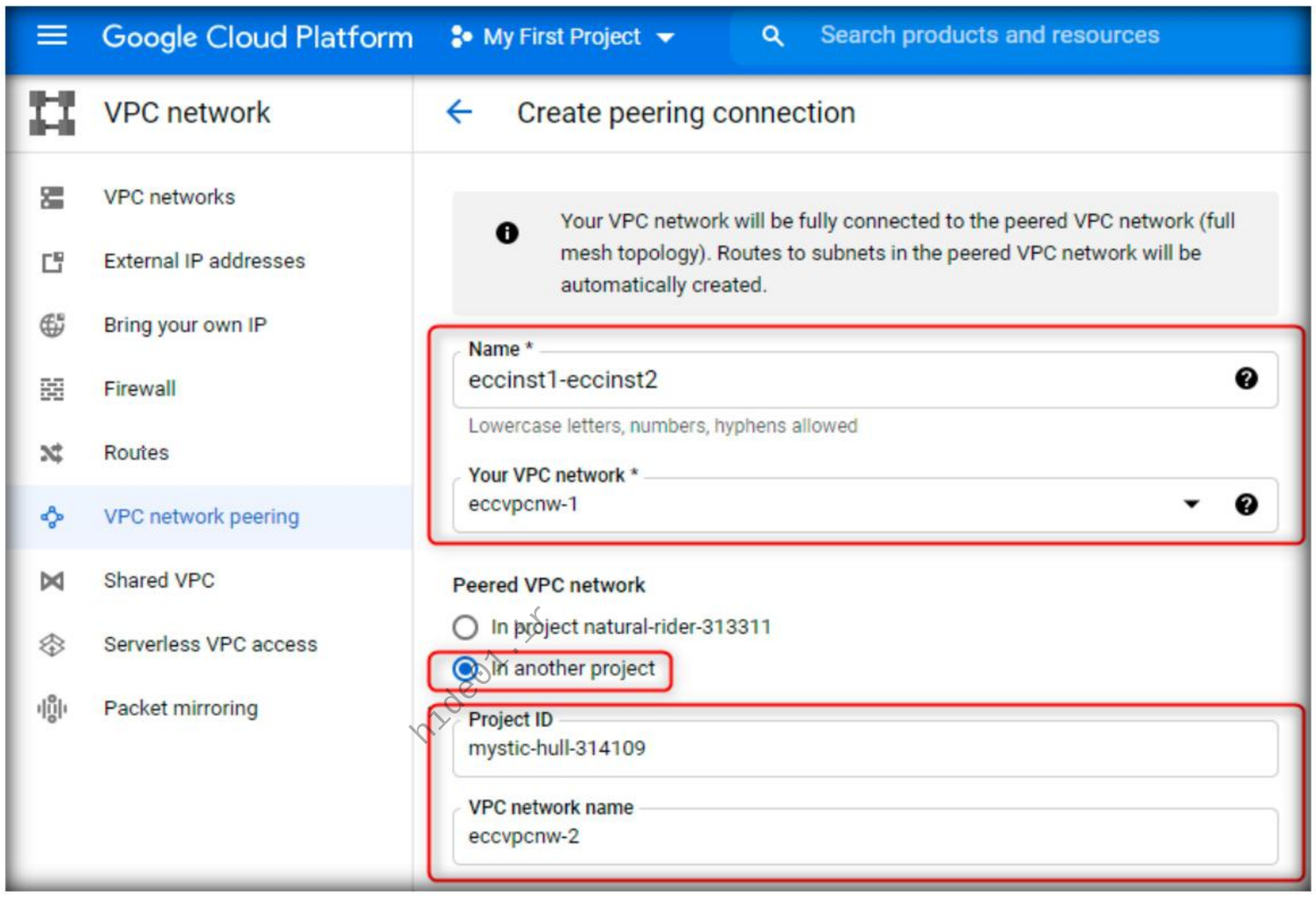


FIGURE 2.10.56: Entering the details for Peering

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

63. Retain the other default settings and click on **CREATE**.

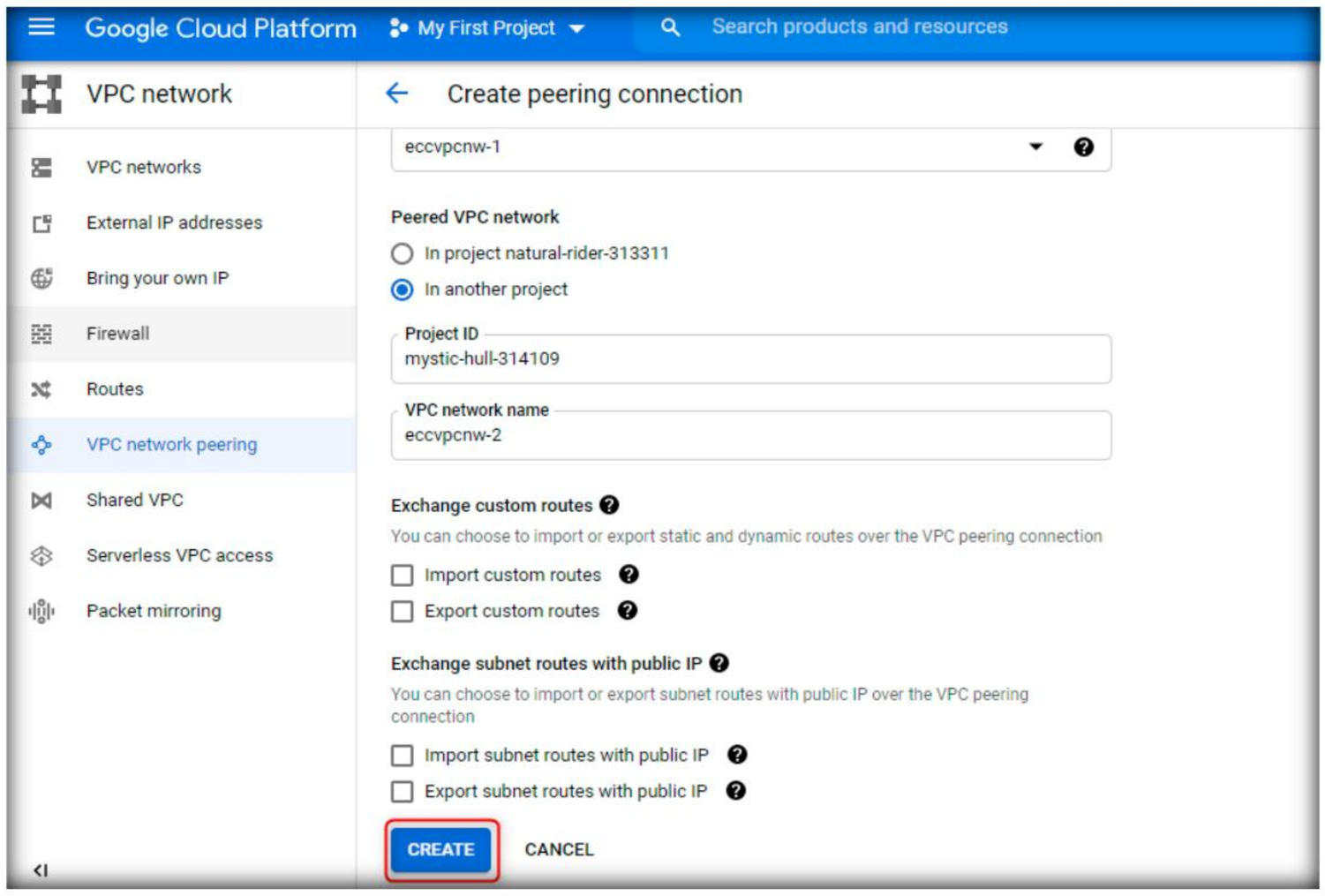


FIGURE 2.10.57: Creating VPC Peering

64. VPC network peering for first project instance has been created successfully.

Note: The status of a VPC becomes active only after configuring the next VPC.

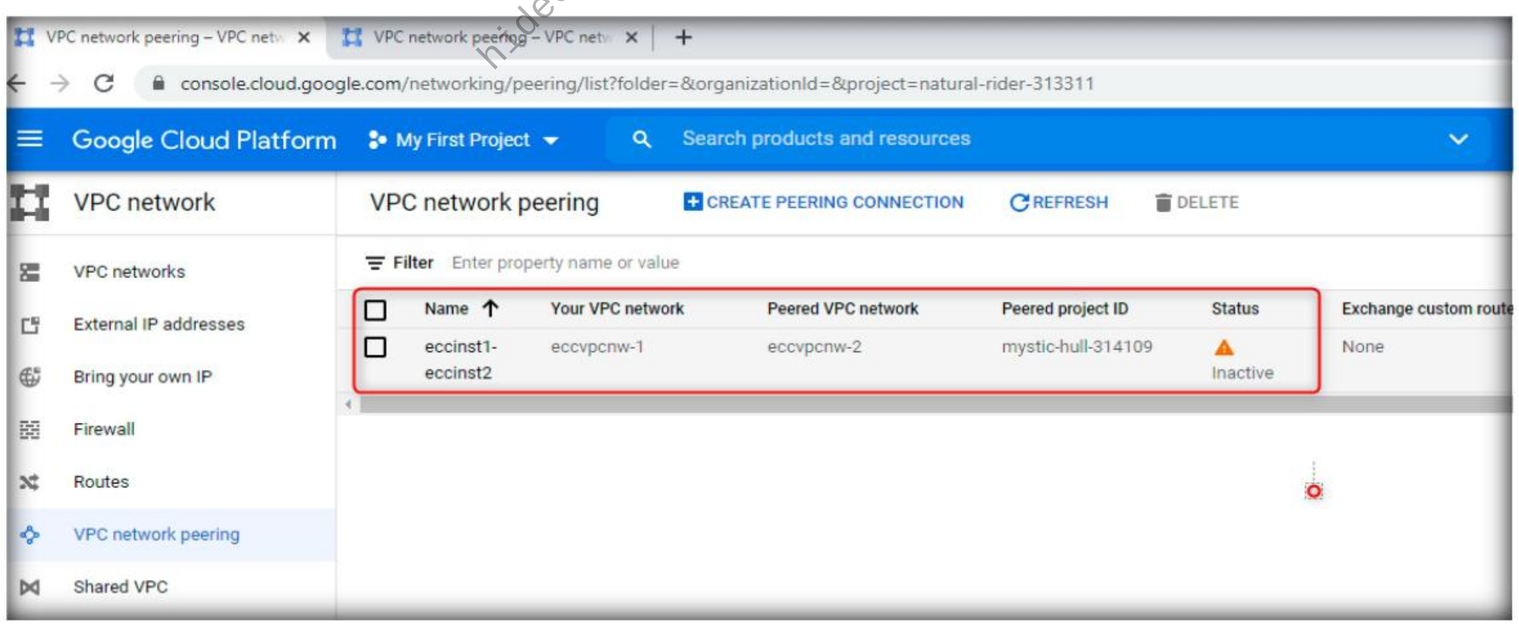


FIGURE 2.10.58: Created VPC for first project

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

65. Next, switch to the second project, navigate to **VPC network**, and select **VPC network peering**.

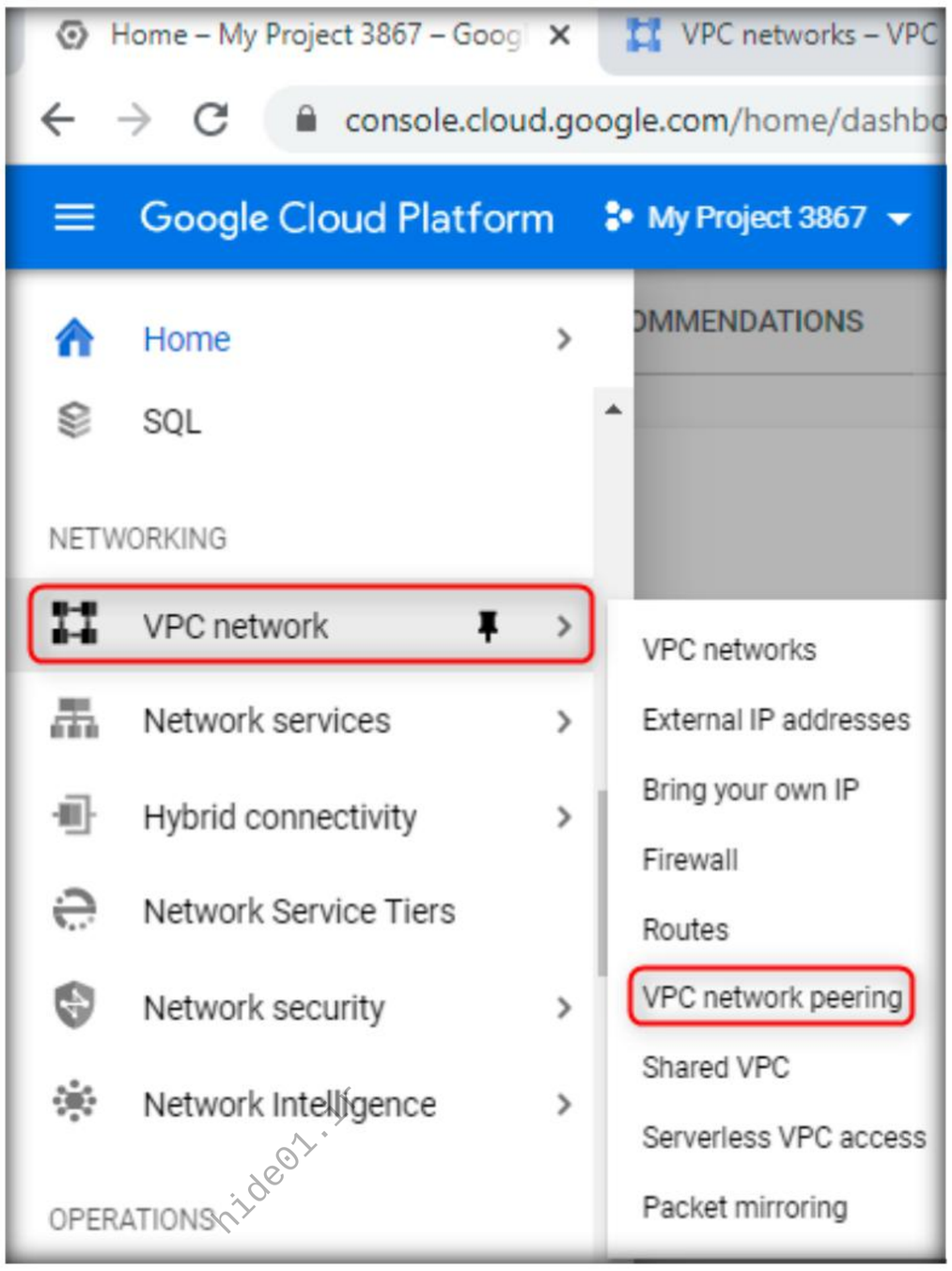


FIGURE 2.10.59: Policy Generator

66. Click on **CREATE CONNECTION**.

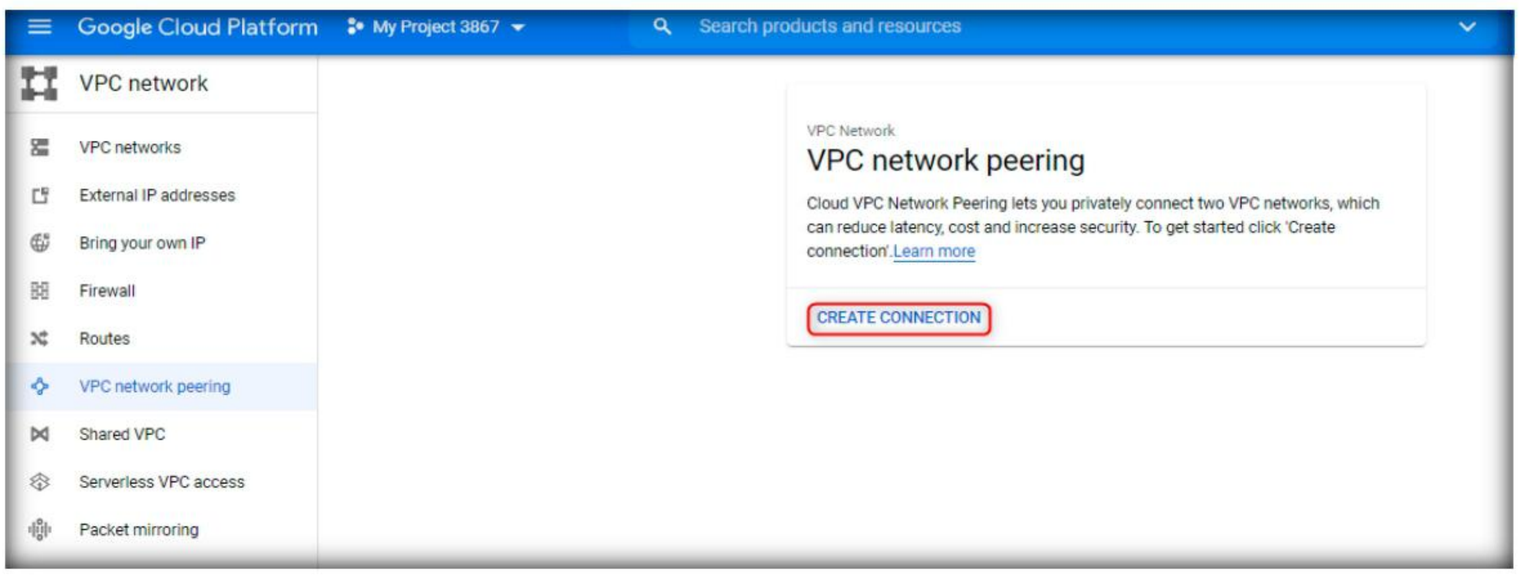


FIGURE 2.10.60: Creating new connection

Certified Cloud Security Engineer Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

67. Click on **CONTINUE**.

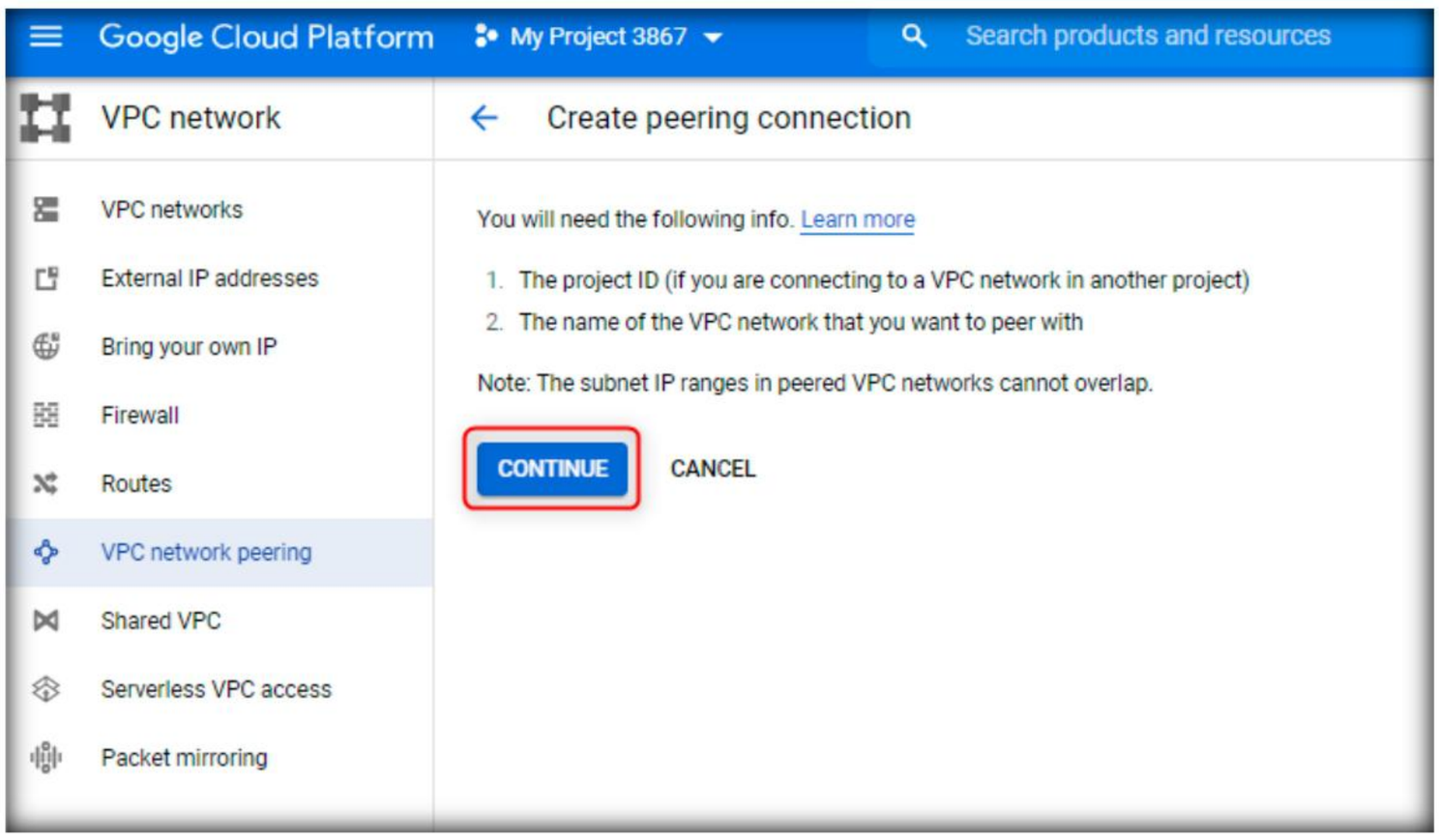


FIGURE 2.10.61: Continue with creating the connection

68. Provide the appropriate details in **Create Peering Connection**. In this lab, we have used the following details:

Name: eccinst2-eccinst2

Your VPC network: eccvpcnw-2

Peered VPC Network: In another project

Project ID: natural-rider-313311

VPC network name: eccvpcnw-1

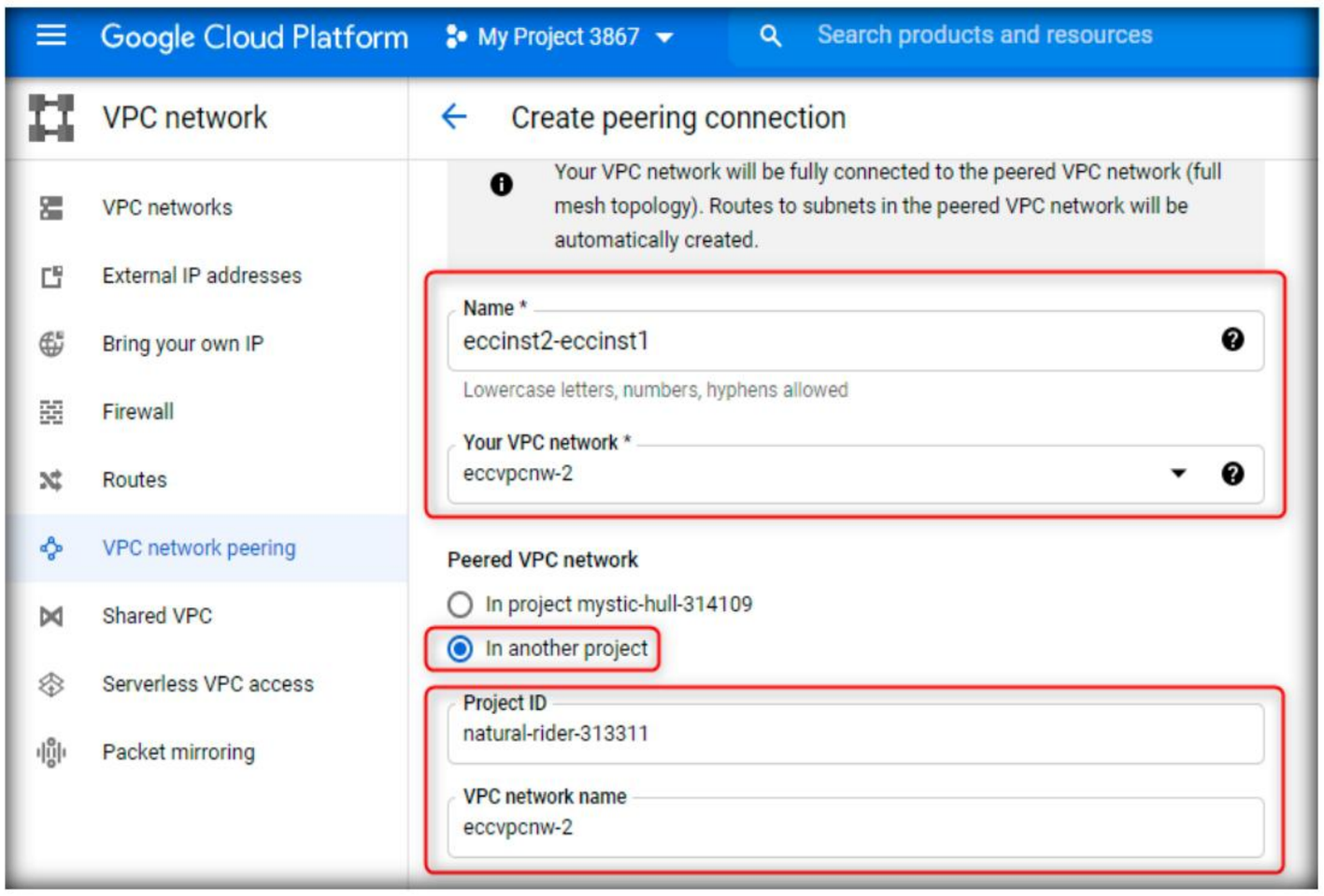


FIGURE 2.10.62: Entering the details

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

69. Retain the other default settings and click on **CREATE**.

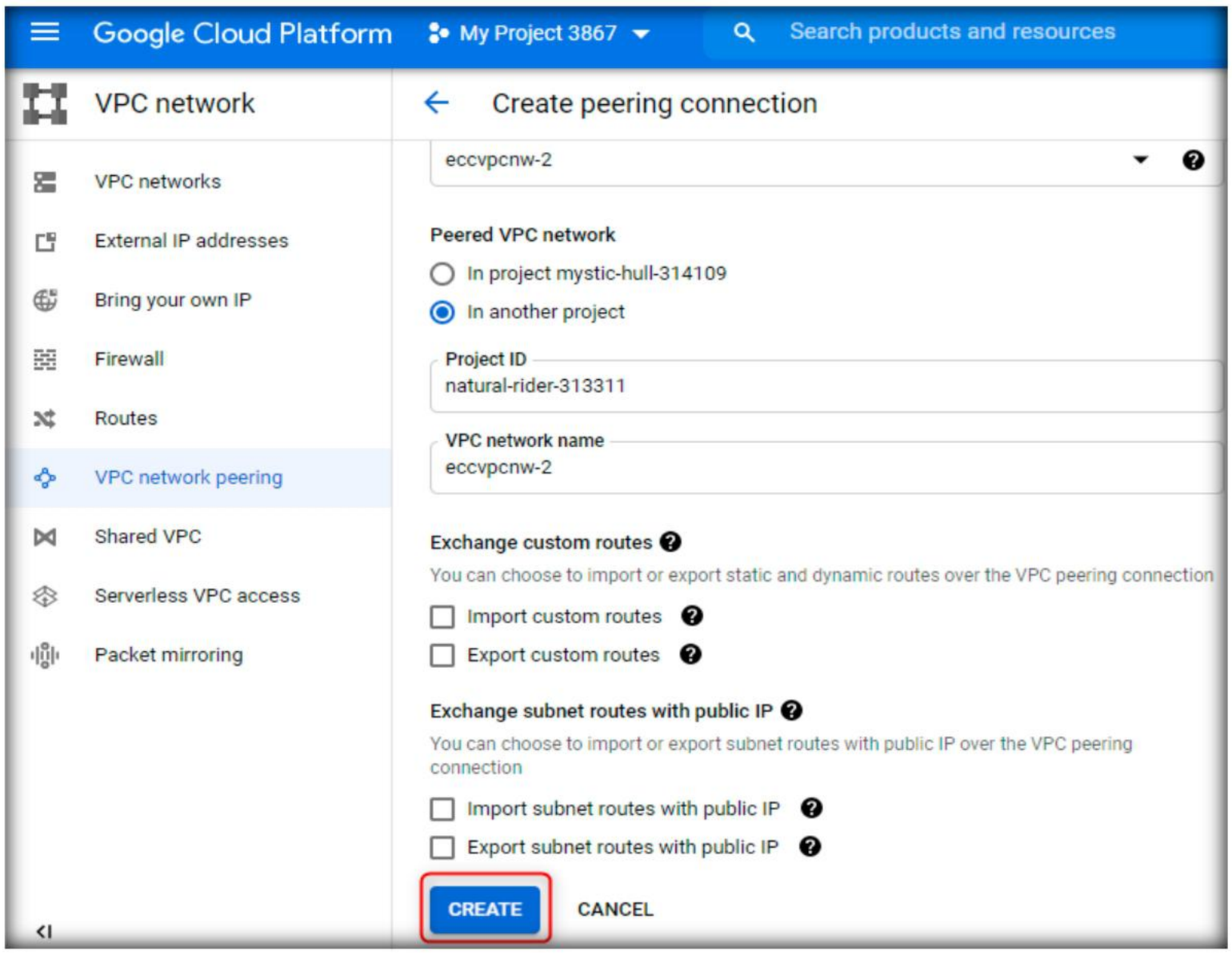


FIGURE 2.10.63: Creating the connection

70. The VPC network peering is now activated, and the status is **Active**.

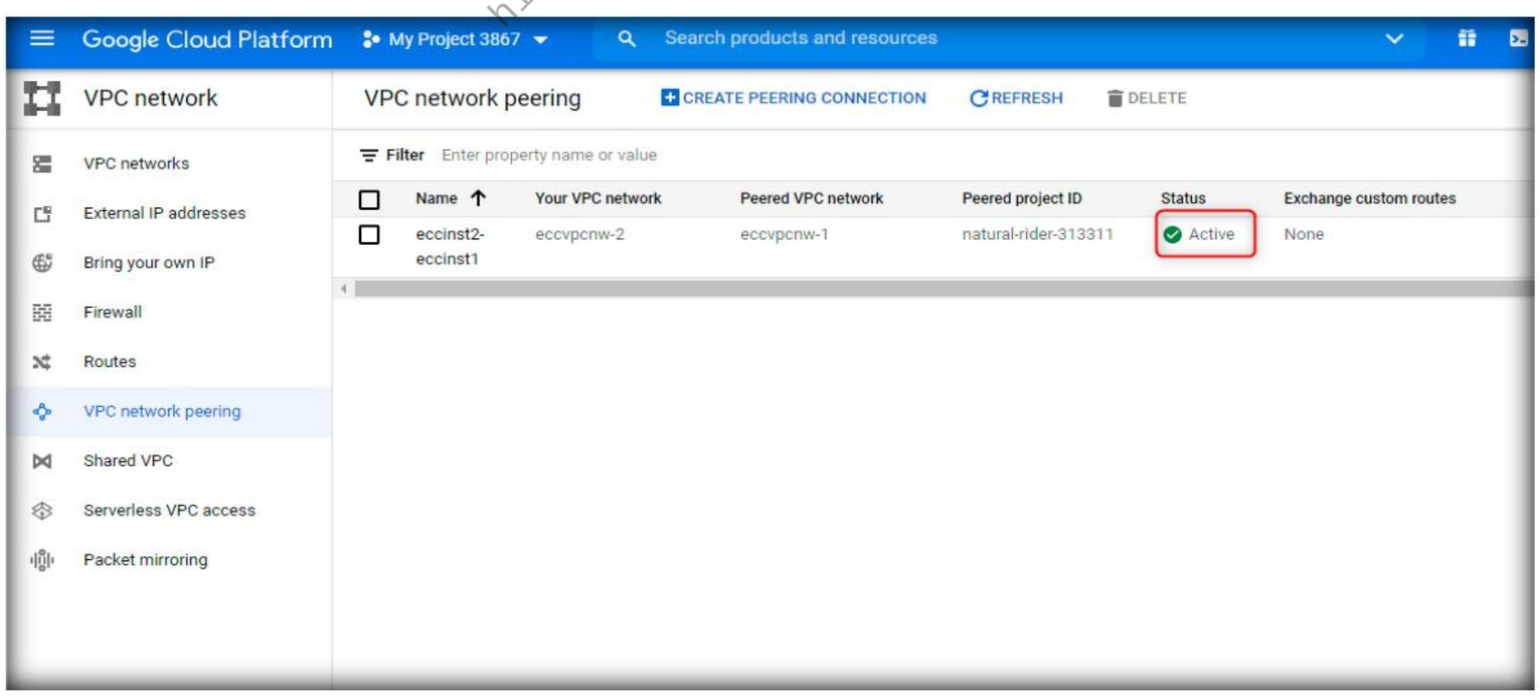


FIGURE 2.10.64: Peering is Active

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

71. Now, go back to the SSH shell of the first project's VM instance, ping the command given below, and press **Enter**.

    `ping <internal IP address>` (Replace internal IP with the internal IP of the second project instance)

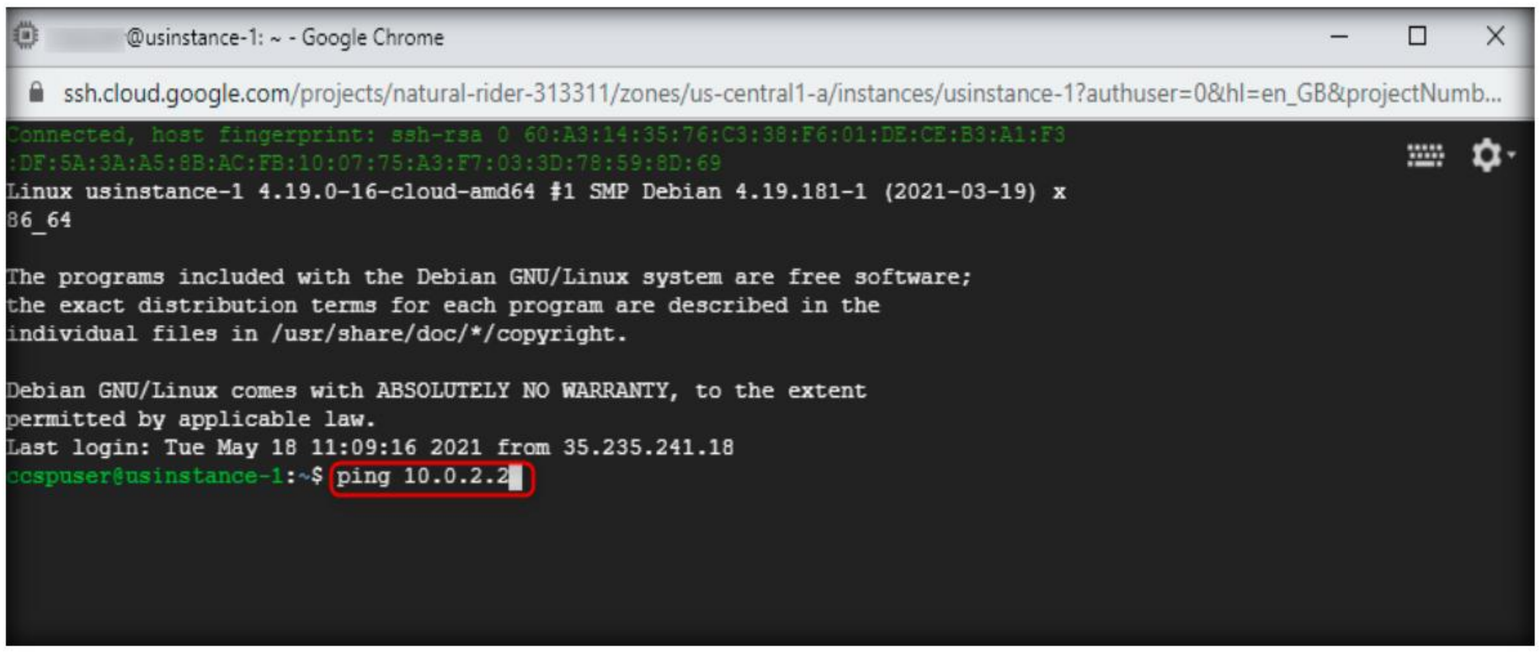


FIGURE 2.10.65: Conducting ping request in SSH shell

72. The connection is successfully established.

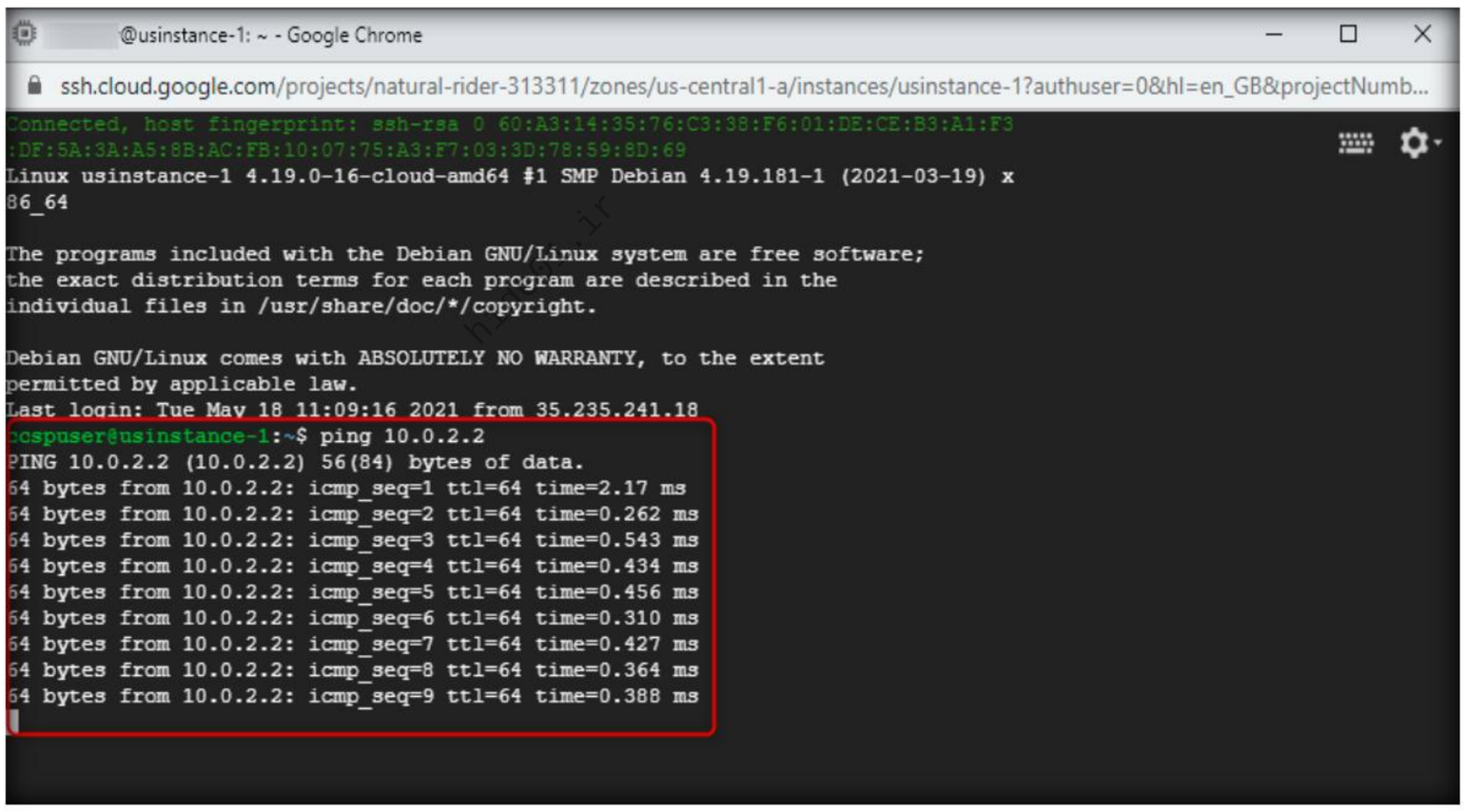


FIGURE 2.10.66: Successfully established the VPC connection

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

73. This way, a cloud security engineer can establish a secure private connection between the instances of different projects.

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

74. Now, to delete the Compute Engine VM instance that you have created for the first project, navigate to the **VM instances** section in **Compute Engine**. Click on the ellipsis, for instance, and click on **Delete**. Repeat the step for deleting the VM instance of the second project. In the pop-up window, click on **DELETE**.

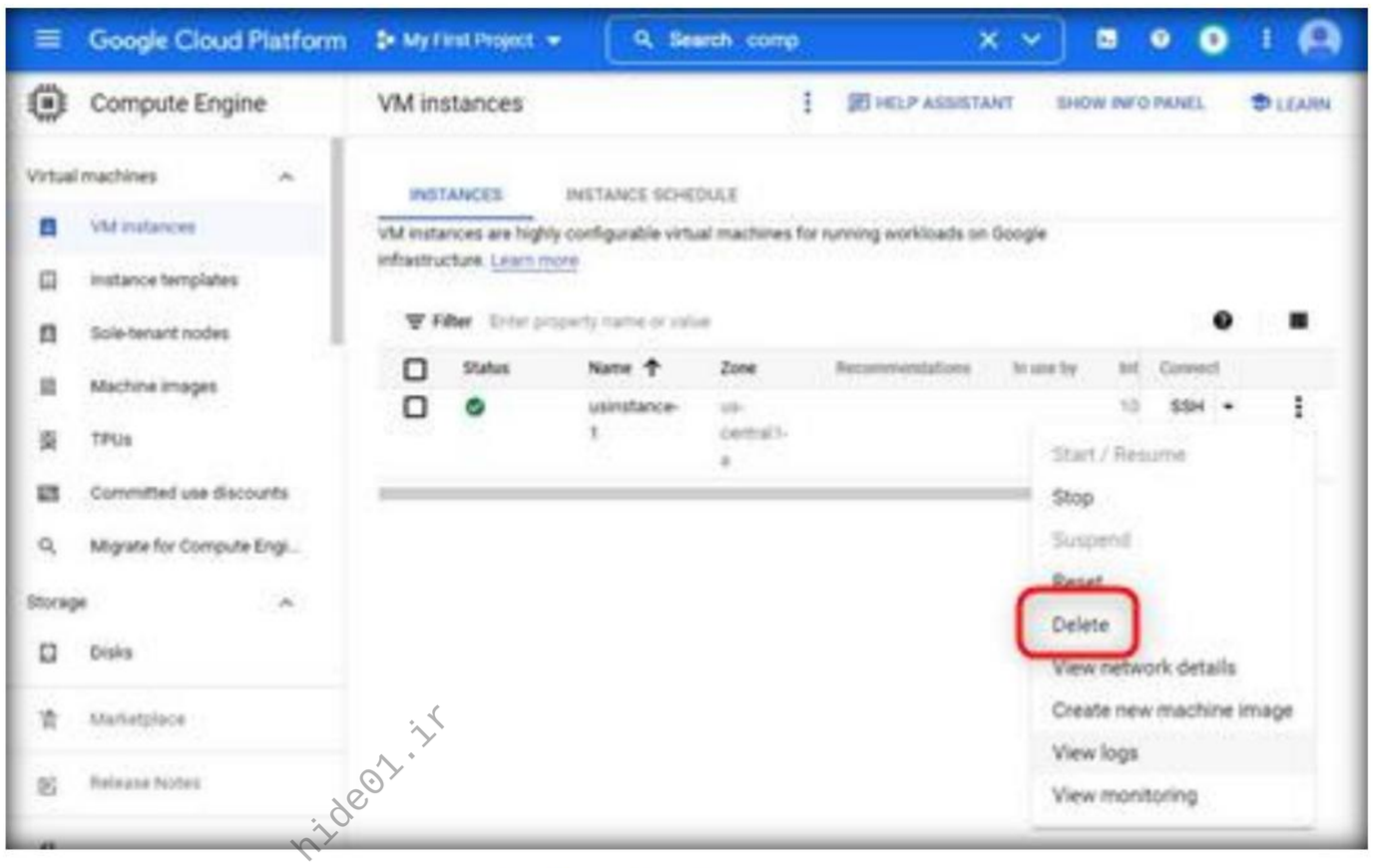


FIGURE 2.10.67: Deleting VM Instance

75. Next, delete VPC network peering. Navigate to the **VPC network peering** section in the VPC network. Click on the ellipsis for the VPC network peering connection you have created and click on **Delete**. Repeat the step for deleting the VPC network peering connection of the second project. In the pop-up window, click on **DELETE**.

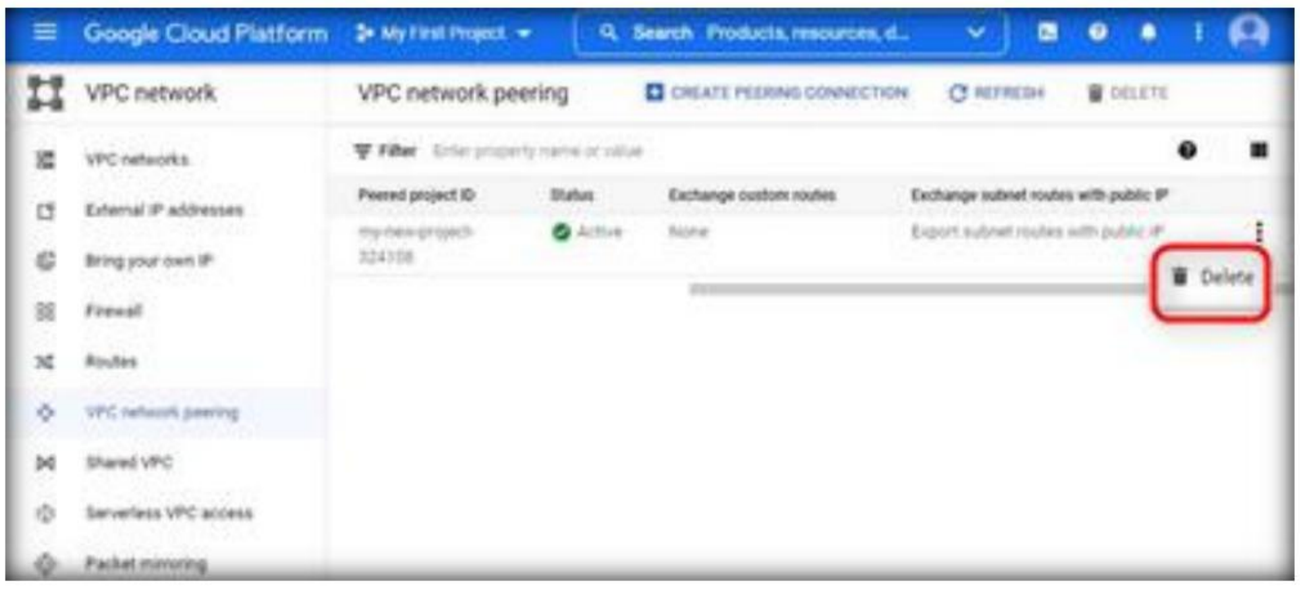


FIGURE 2.10.68: Deleting VPC Network Peering

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

76. Next, to delete the VPC network that you have created for the first project, open the VPC network that you have created and click on **DELETE VPC NETWORK** at the top. Repeat the step for deleting the VPC network of the second project.

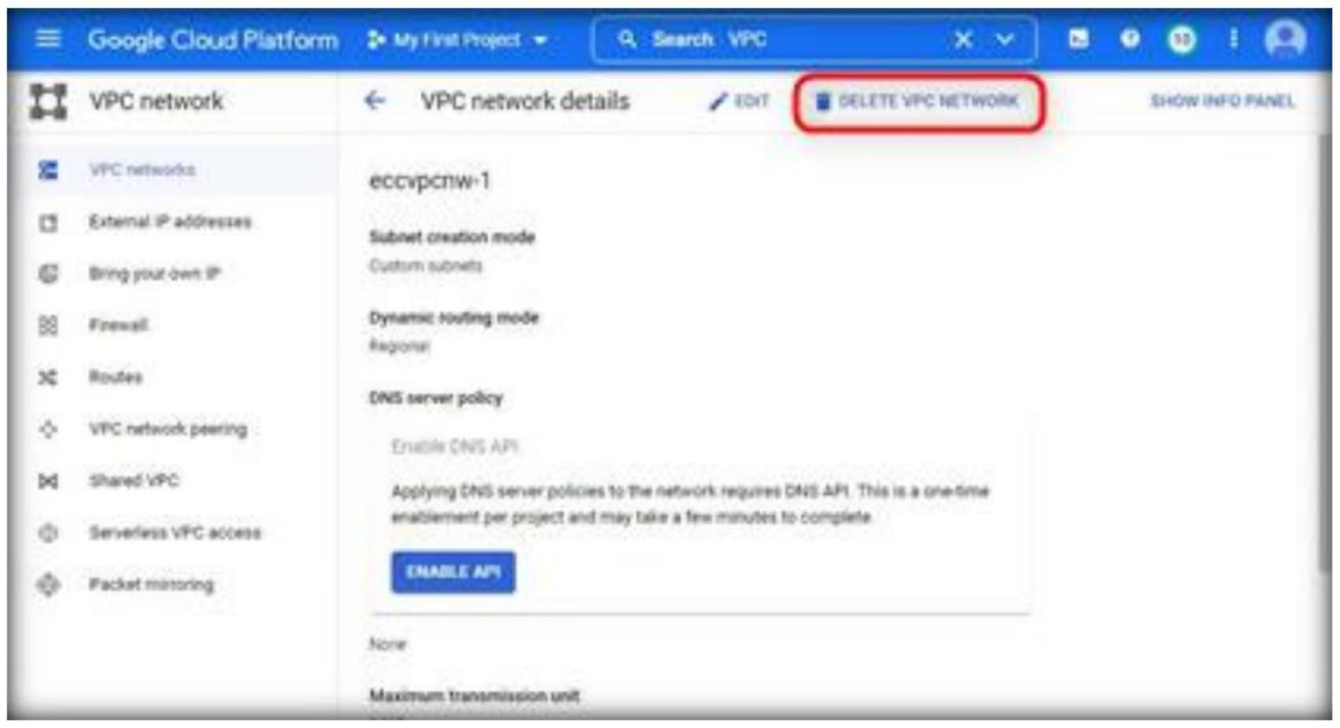


FIGURE 2.10.65: Deleting VPC Network

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.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

This page is intentionally left blank.

hide01.ir

Application Security in Cloud

hide01.ir

Module 03

Caution: Completing the steps in this exercise will require you to sign up for third party services that may incur fees. Be sure to follow proper guidelines for removing billable services from your account before you leave your lab. Deviating from our specific instructions may result in unwanted fees for services from third-party service providers. Be sure to check with your school, instructor, or employer if education accounts are available. If you sign-up and provide your credit card, you will be responsible for any fees related to services you activate. We strongly advise you not to deviate from our explicit instructions while connected to the platforms unless you are fully aware of what the services are and what the respective third-party charges for their use.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 1

Implementing Web Application Firewall in AWS

AWS web application firewall (WAF) protects the applications and APIs from various attacks that can compromise security and downgrade performance by utilizing excessive resources. A cloud professional can easily secure and protect AWS services and resources for AWS users using WAF.

ICON KEY

Valuable information

Test your knowledge

Web exercise

Workbook review

Lab Scenario

AWS WAF offers predefined and custom rules to cloud professionals to help protect AWS services and resources. It enables access rules and permissions for specific applications to manage their accessibility across specific regions or areas. AWS WAF detects and handles incoming threats for cloud professionals against an application.

Lab Objectives

This lab will demonstrate the implementation of WAF and its associated configuration settings.

In this lab, you will learn to do the following:

- Create a web application API
- Protect the API from specific IP addresses with WAF
- Creating WEB ACL in WAF
- Block web API for specific IPs using WAF

Lab Environment

To perform this lab, you need the following:

- **Admin Machine** VM
- **Administrative** privileges
- Registered AWS account

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Duration

Time: 15 minutes

Overview of WAF

AWS WAF protects the applications deployed on AWS from common web exploits such as SQL injection and cross-site scripting to ensure their security and availability is not compromised. AWS WAF utilizes some predefined rules to filter the network traffic. It updates the managed rules for AWS in the face of new security issues. These managed rules can address OWASP Top-10 security risks and common vulnerabilities and exposures (CVEs). Security policies can be updated quickly across the entire infrastructure because the updates take less than a minute. The web requests can be filtered based on features such as IP address, origin country, malicious scripts, malicious SQL code, etc. Rules can be defined to allow or block requests or count them based on some properties.

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., AWS), the application interface may be updated with time. Hence, in case you happen to work on an updated version of AWS, 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.

Module 03 - 1

Note: Before starting this lab, you should create an AWS account using the following link: https://portal.aws.amazon.com/billing/signup. Once the registration is complete, perform the following tasks.

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

TASK 1

Creating WEB API in AWS

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

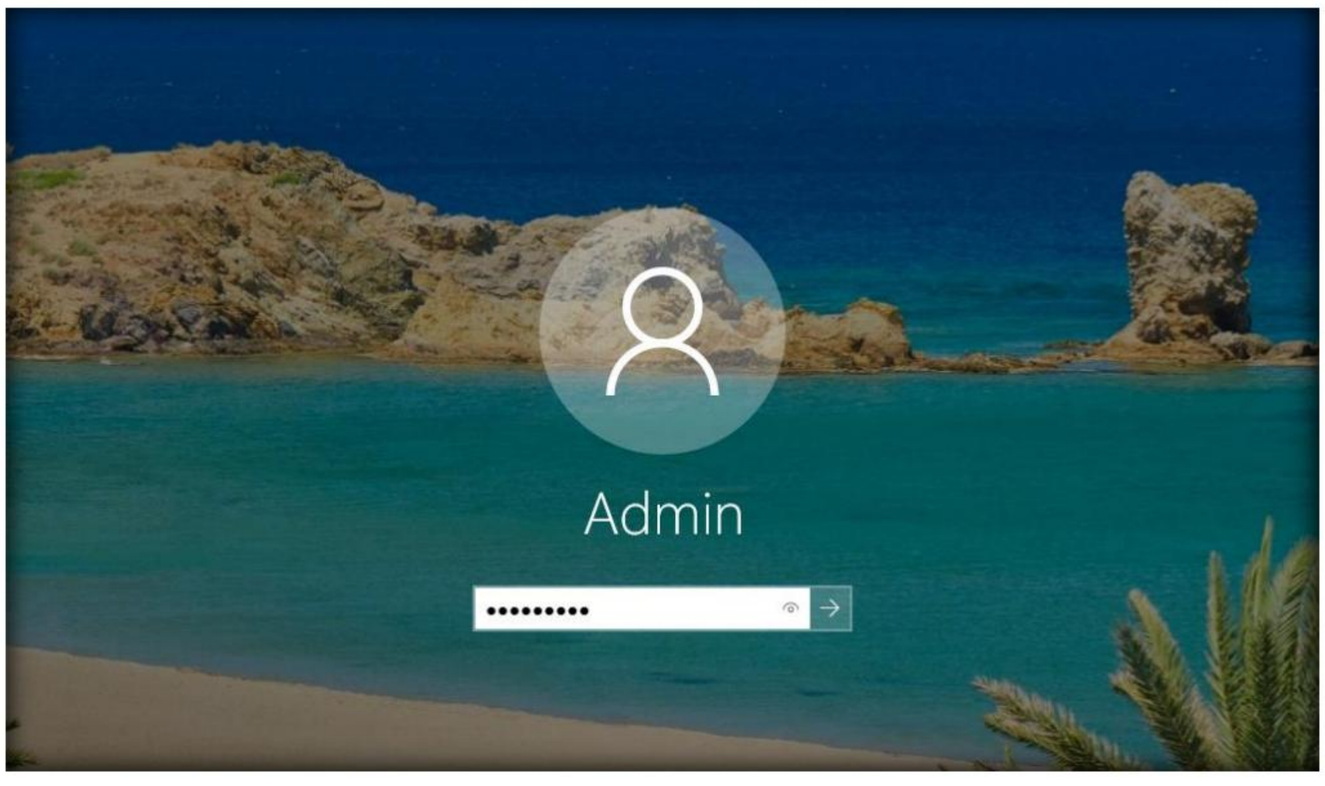


FIGURE 3.1.1: Launch Admin Machine and Log in

Certified Cloud Security Engineer Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

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

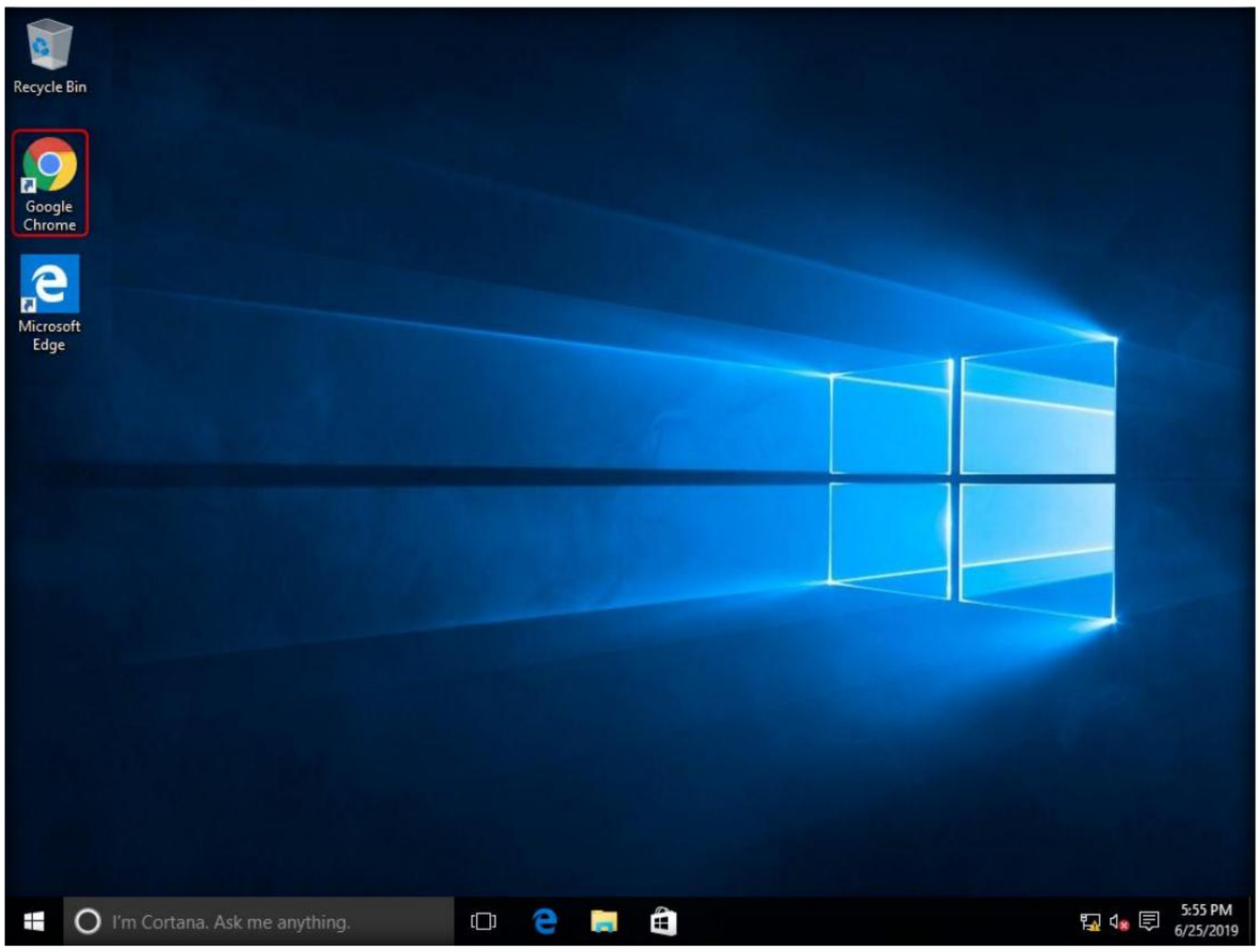


FIGURE 3.1.2: Navigating to the Chrome Browser from Taskbar

3. To login to **AWS Web Services - Cloud Computing Services,** go to the address bar, type **https://aws.amazon.com/**, and press **Enter**.

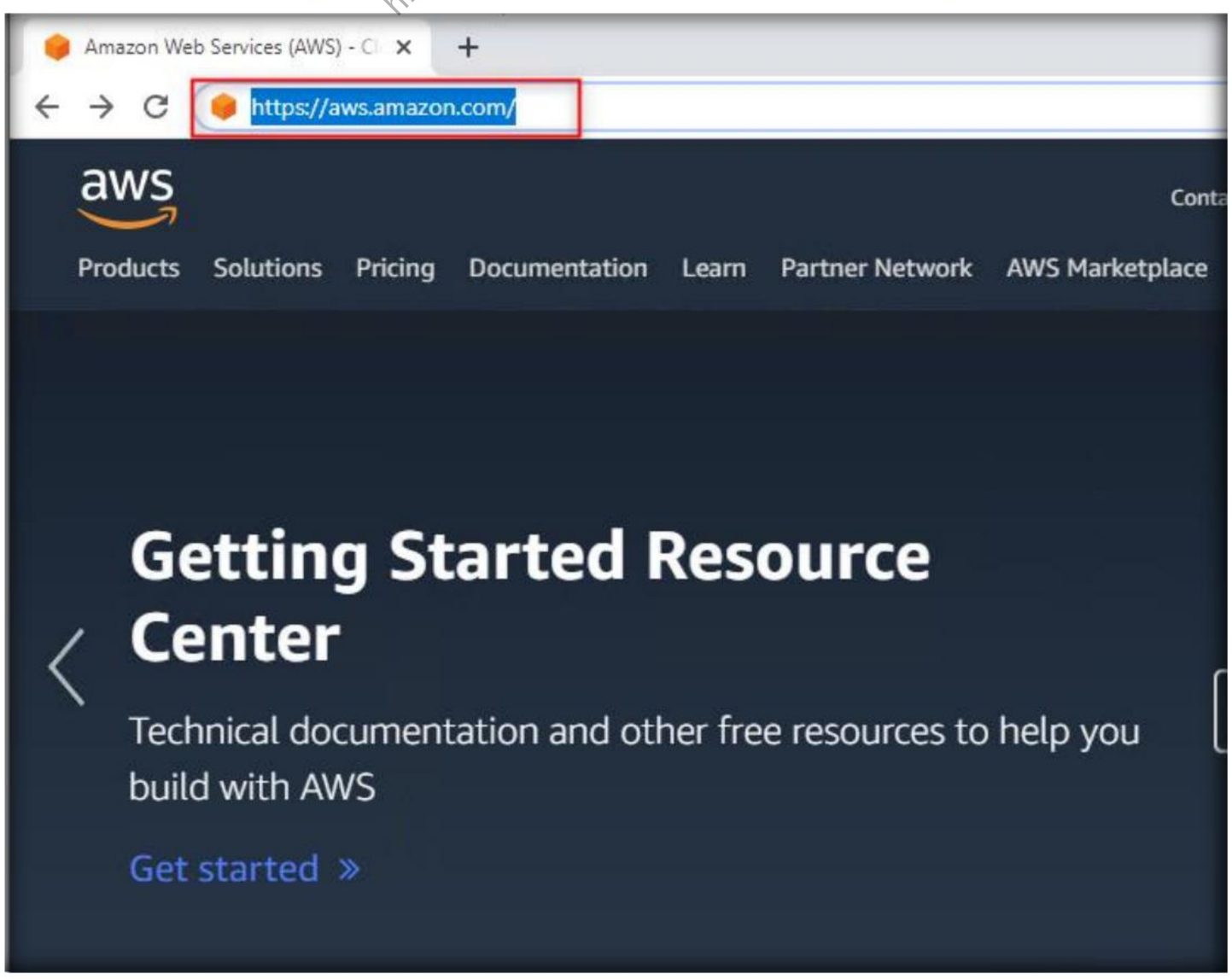


FIGURE 3.1.3: Access AWS in Browser

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

4. The **AWS Web Services - Cloud Computing Services** home page appears. Click on **AWS Management Console** from the **My Account** drop-down menu, as shown in the screenshot below.

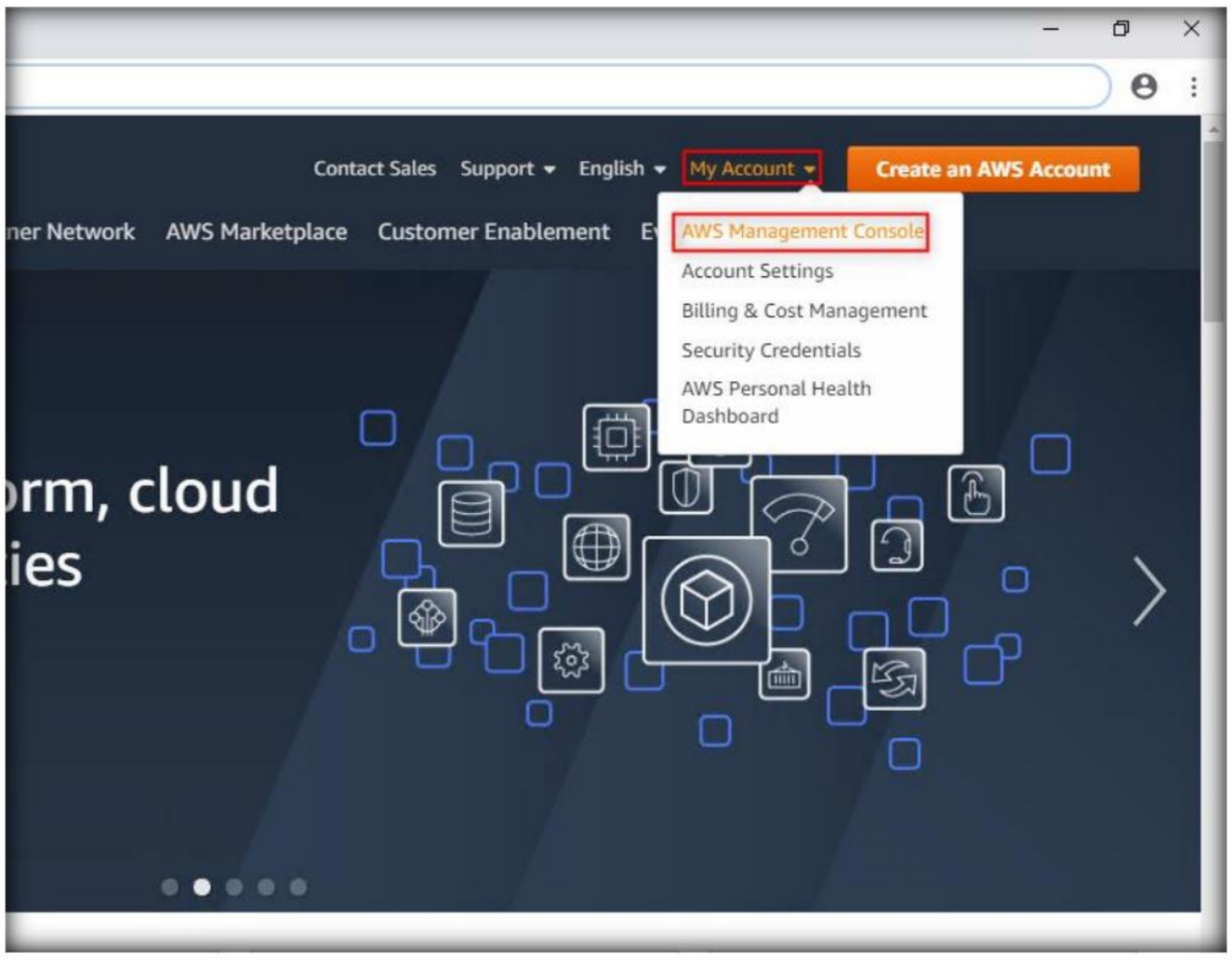


FIGURE 3.1.4: Navigate to AWS Management Console

5. The **AWS Sign-in** page appears. Choose **Root user** and type the AWS administrator account ID (Root user email address), as shown in the screenshot below, and click on **Next**.

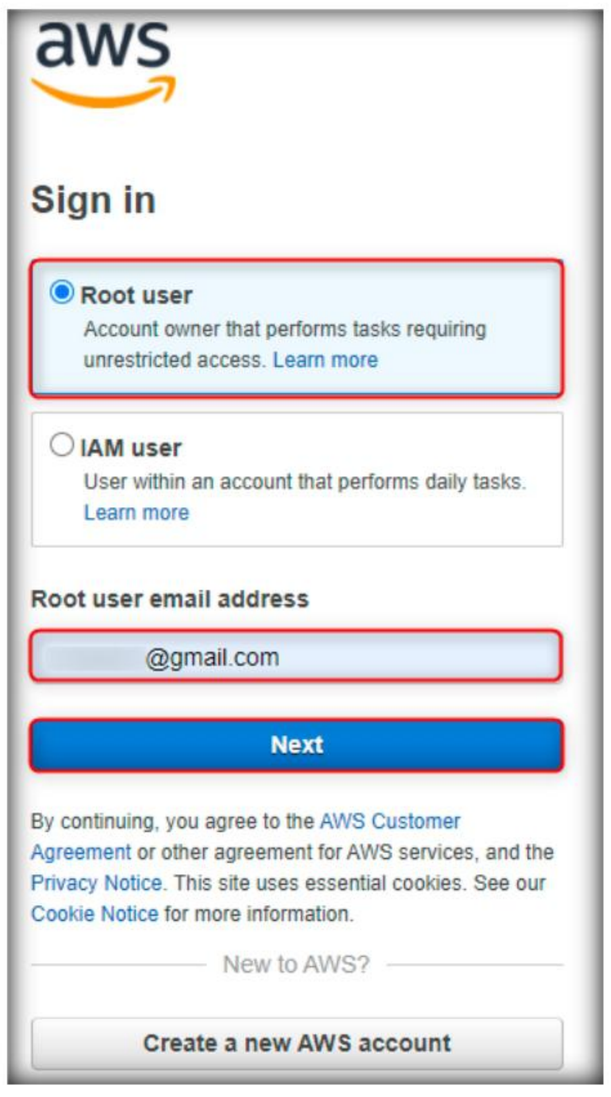


FIGURE 3.1.5: Authentication Window

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

6. On the security check page that appears, type the characters shown in the image and click **Submit.**

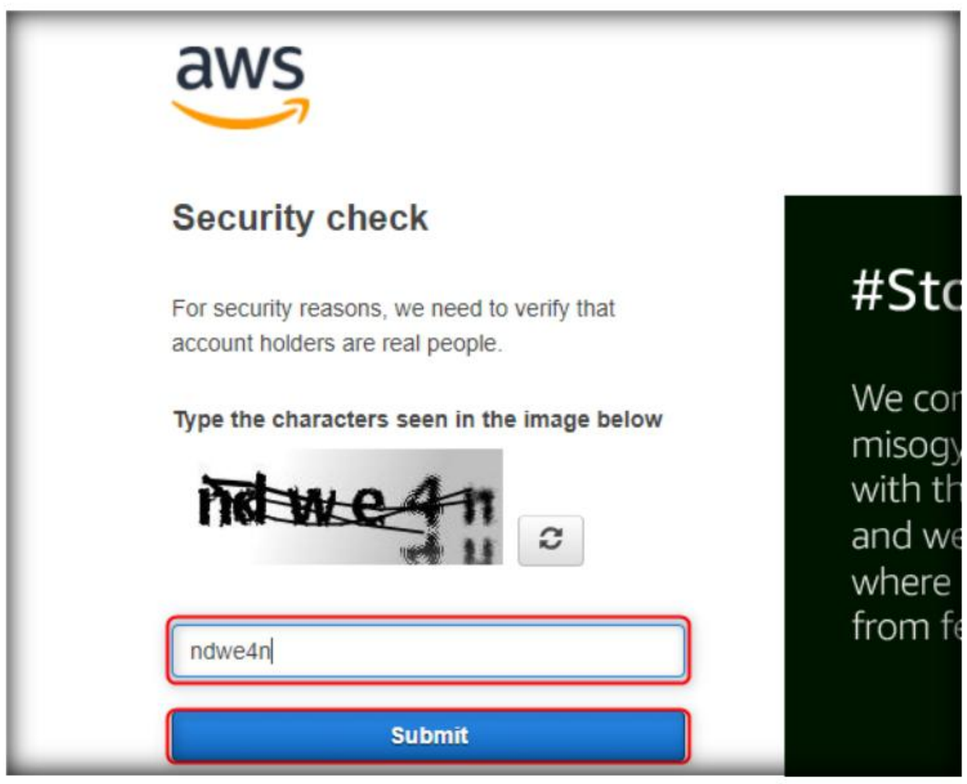


FIGURE 3.1.6: Entering Security Captcha

7. In the **Password** field, type the password, and click on **Sign-in**, as shown in the screenshot below.

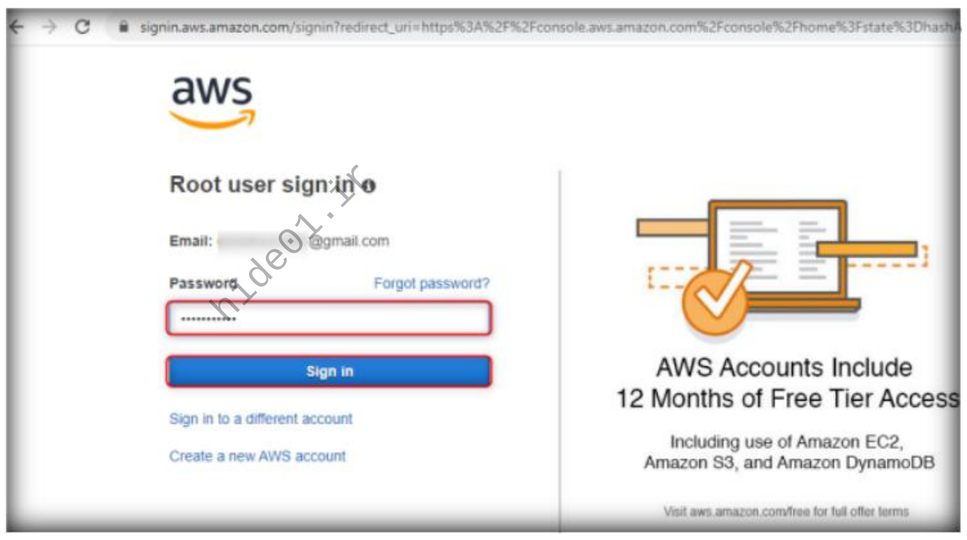


FIGURE 3.1.7: Sign-in to AWS Console

8. To create a WEB API, go to **API Gateway** service, which provides the option for creating and monitoring APIs. Select **Services** from the menu bar and click on **API Gateway** under the **Networking & Content Delivery** section, as shown in the screenshot below.

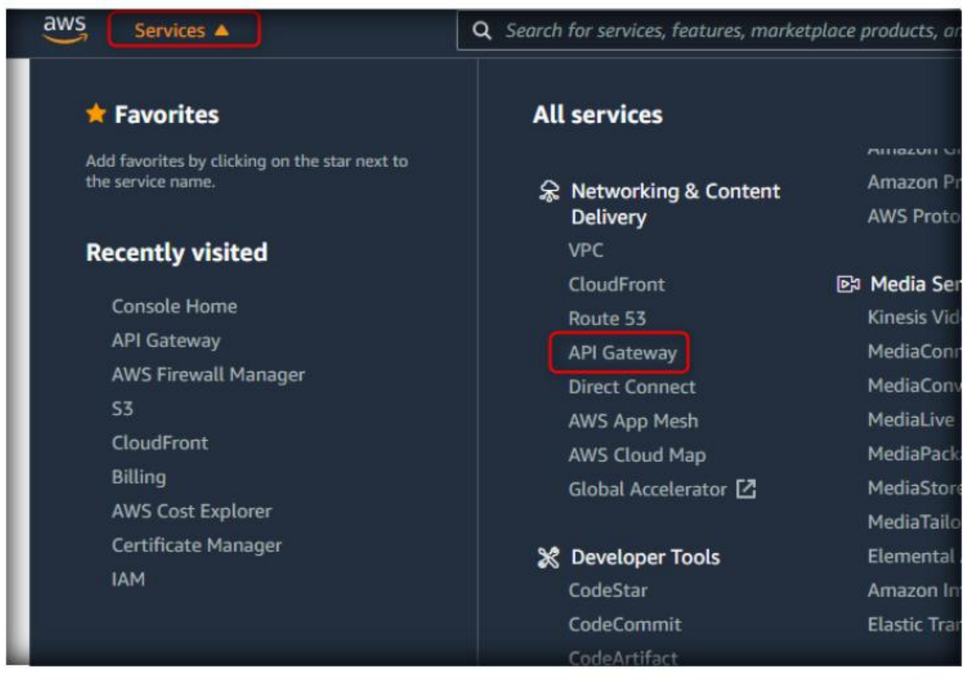


FIGURE 3.1.8: Navigating to API Gateway

Certified Cloud Security Engineer Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

9. To create a **REST API,** go to the **REST API Private** section in the API Gateway page and click on **Build.**

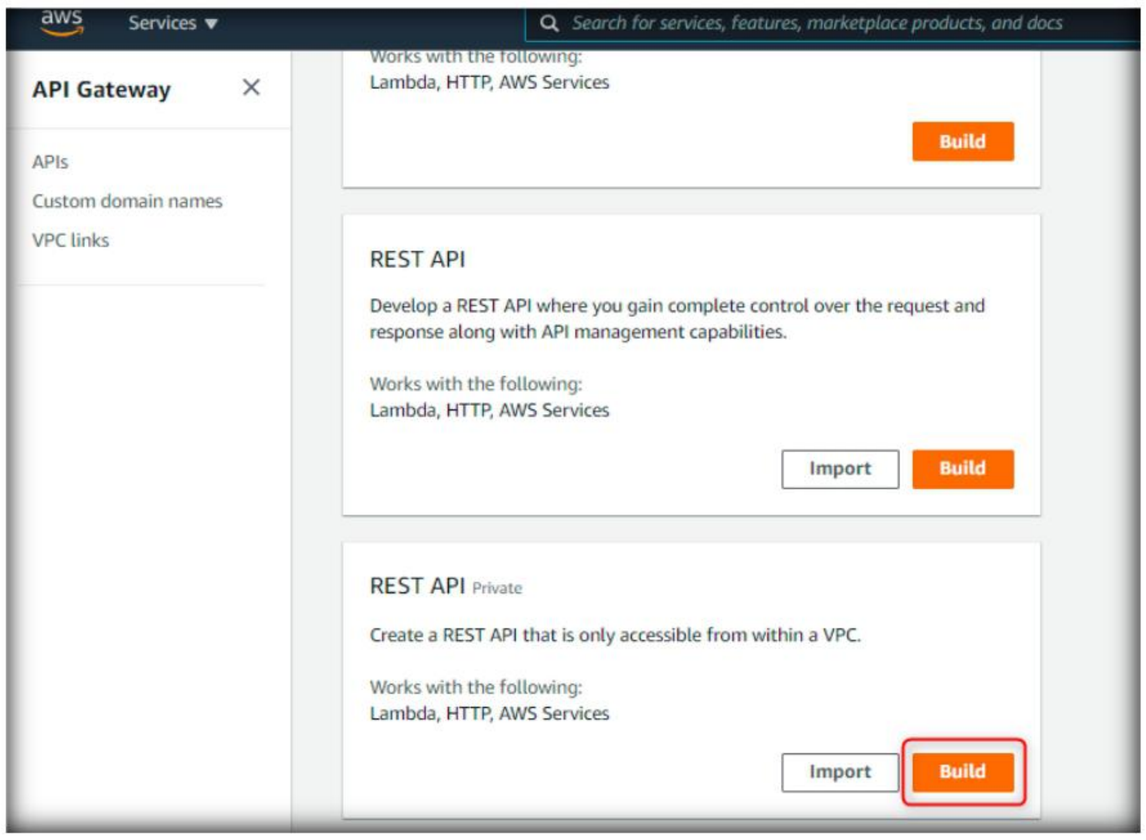


FIGURE 3.1.9: API Gateway Dashboard

10. A **Create your first API** pop-up appears. Click **OK**.

Note: If you have already created a REST API using the account, you may not see the popup.

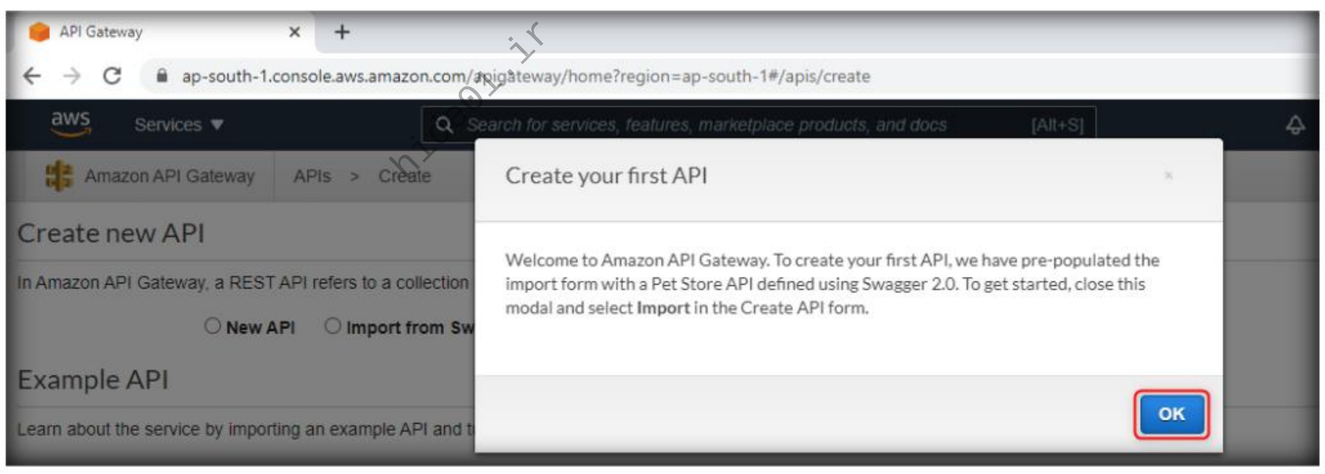


FIGURE 3.1.10: Creating First API pop-up

11. In the **Create new API** section**,** select the **New API** radio button. Under the **Settings** section, provide an API name and description. In this lab, we have used **ECCCloudApi** as the **API name** and **This is REST API** as the **Description.** Now, click on **Create API** to create the API.

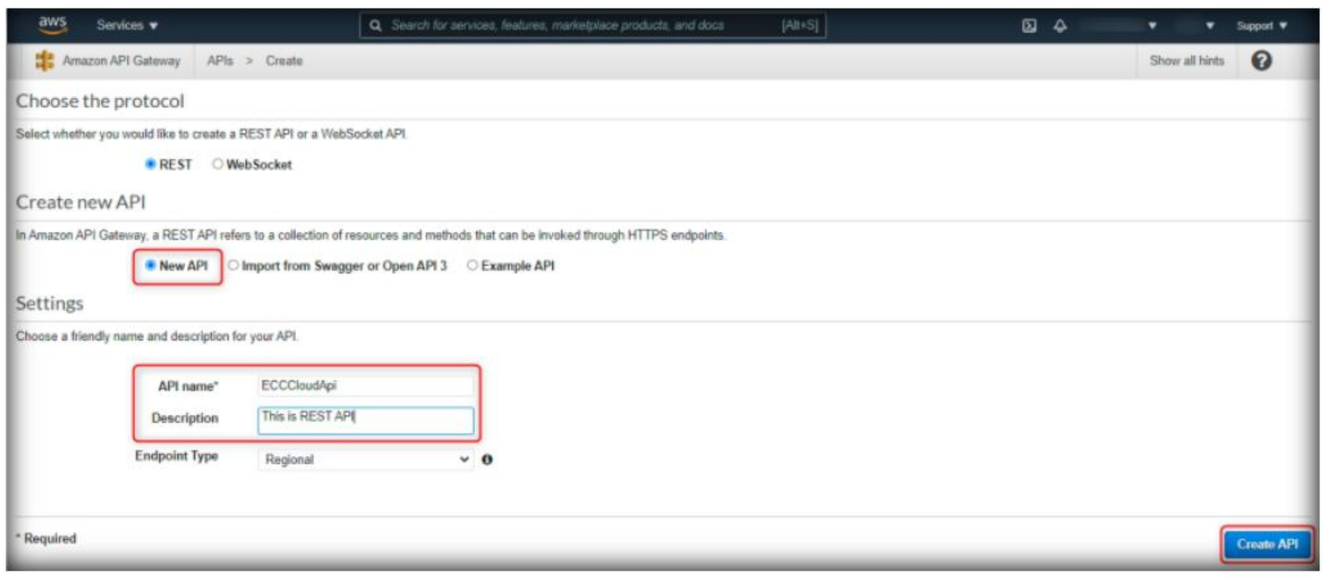


FIGURE 3.1.11: Configuring and creating API

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

12. In the next page, click on the **Actions** dropdown button and select **Create Method** to setup **REST API** methods.

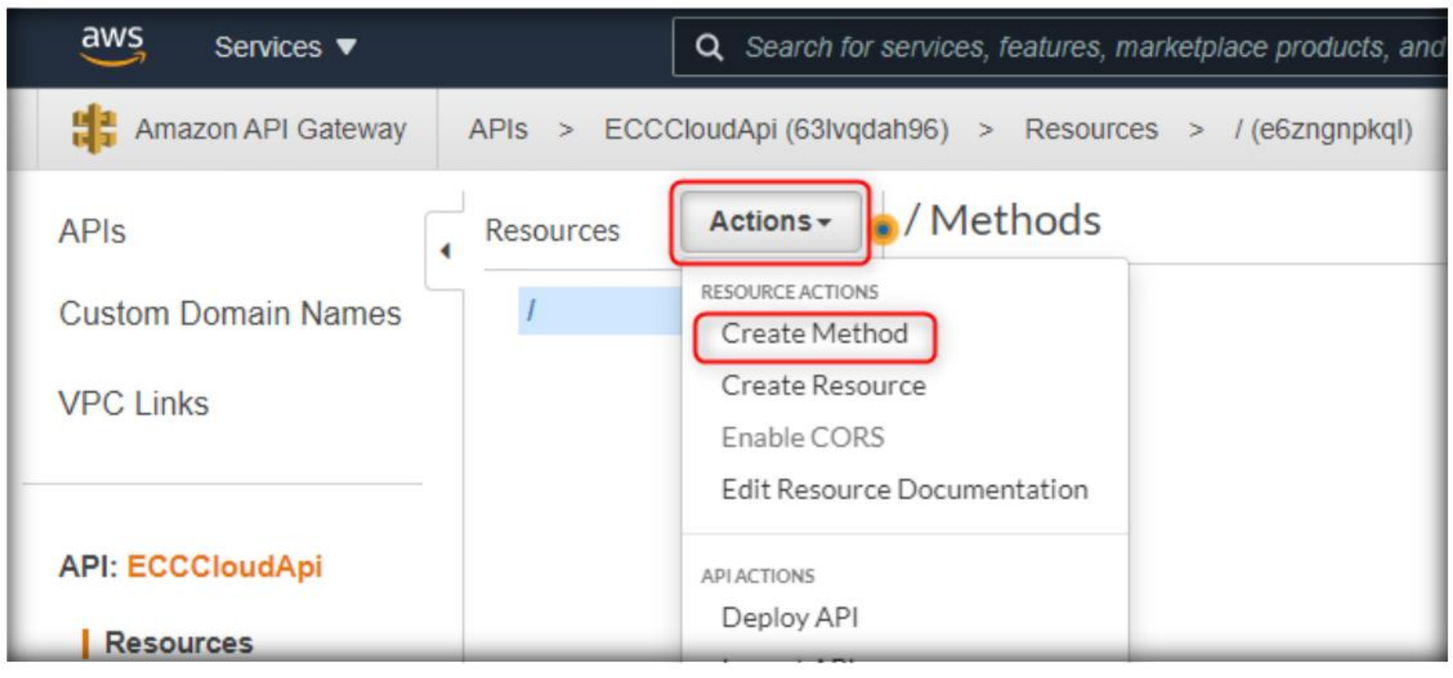


FIGURE 3.1.12: Configuring Resource Actions

13. Click on the empty dropdown list box at the top and select **GET** method from the available list to specify the HTTP method as **GET**.

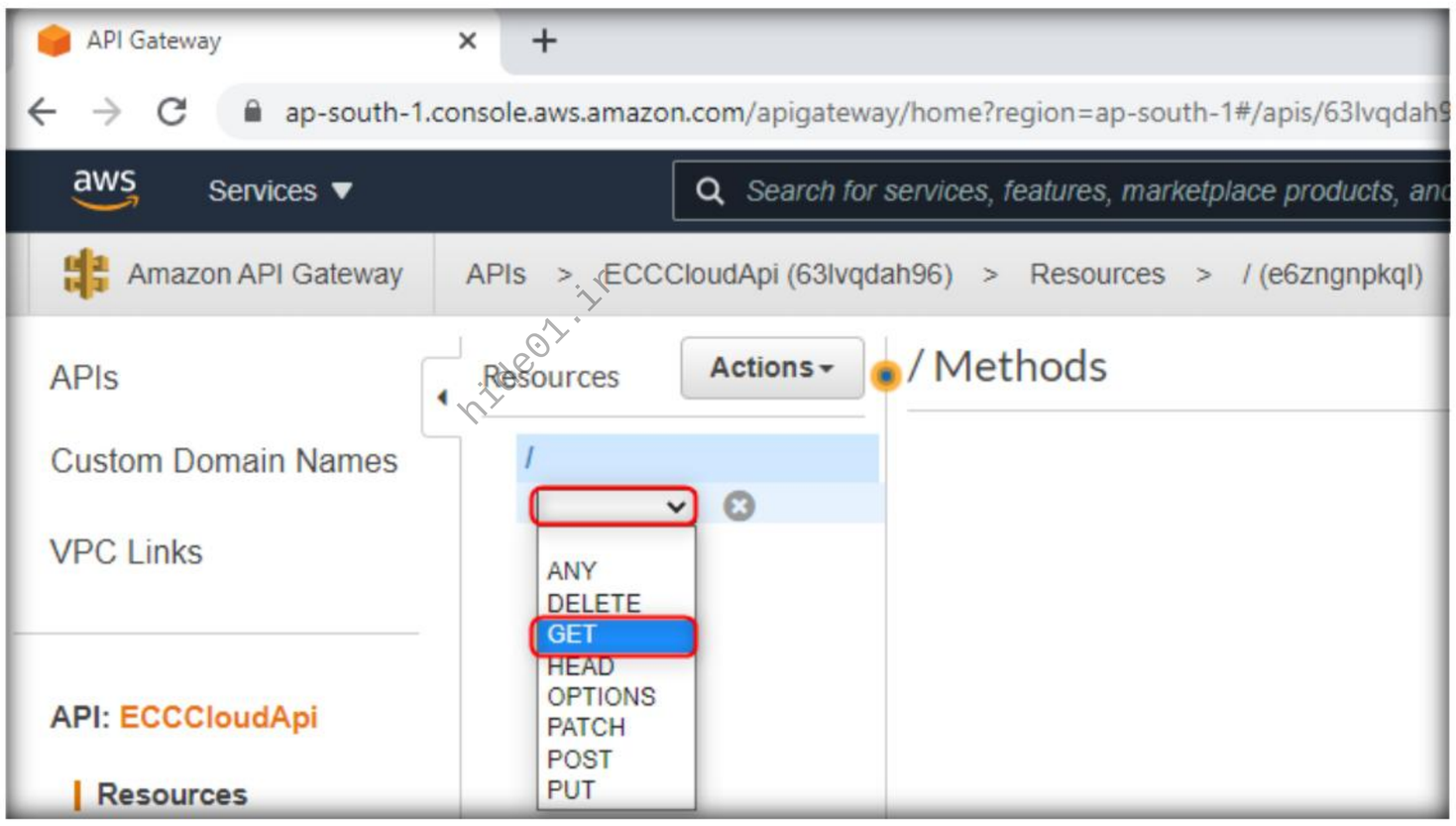


FIGURE 3.1.13: Selecting Action

14. Click on the **Gray tick** button to create the **GET** method.

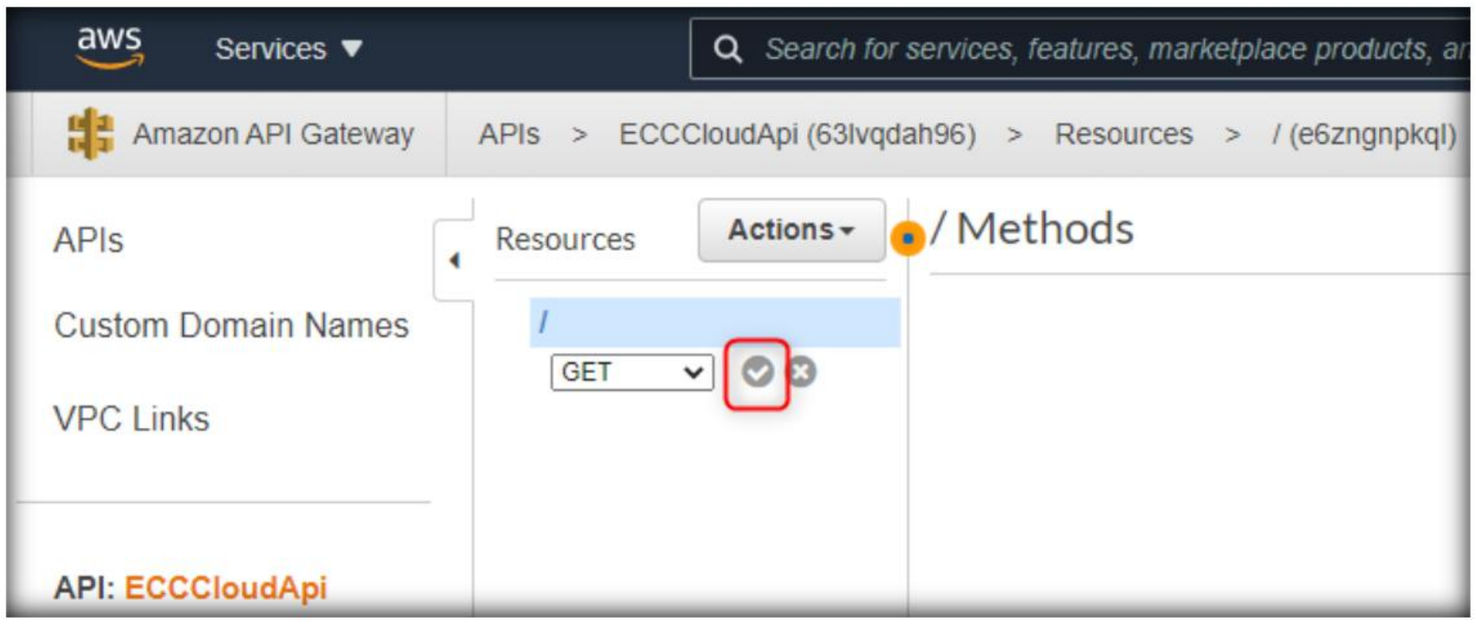


FIGURE 3.1.14: Selecting GET Action

Certified Cloud Security Engineer Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

15. The created method needs to be integrated with an endpoint at the backend. Setting the API integration option as **Mock** will generate API responses directly from API Gateway without any backend integration. Select **Integration** type as **Mock** and click **Save**.

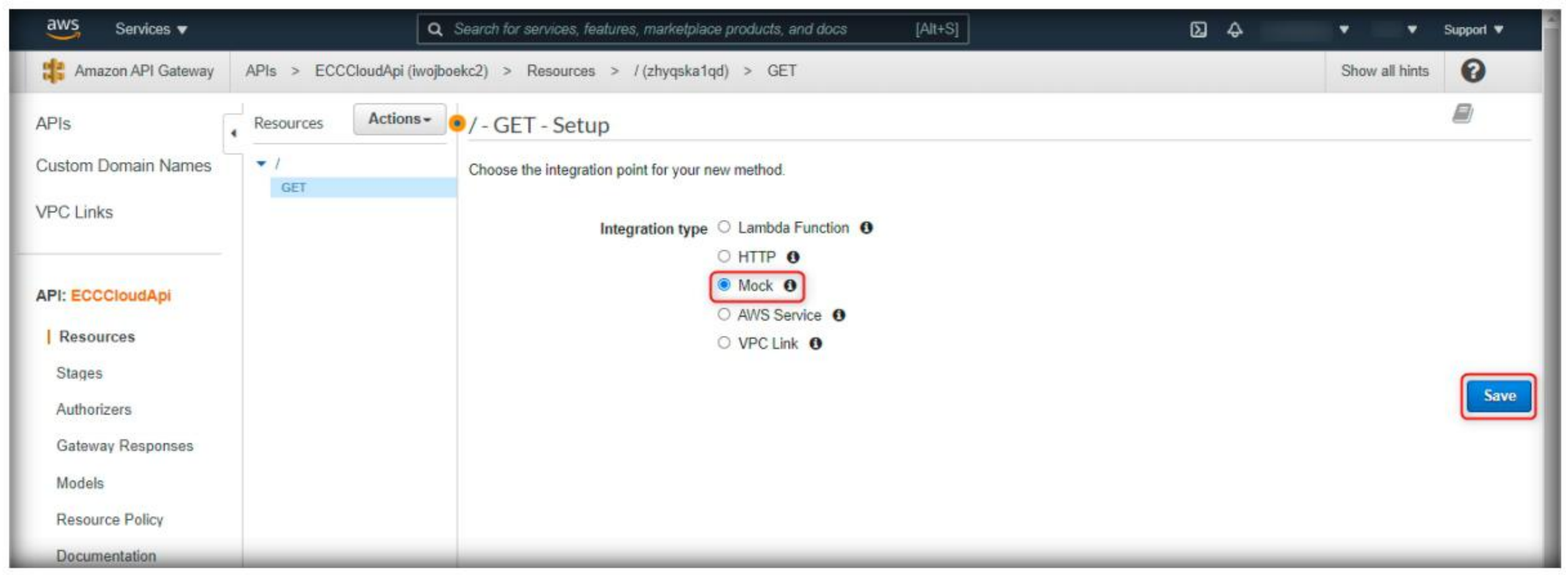


FIGURE 3.1.15: Saving the API Setup

16. You will be redirected to the **GET- Method Execution** page, which displays the details of request and response methods of the **GET** method execution.

17. Click **Integration Response** to set the response from the server to the client.

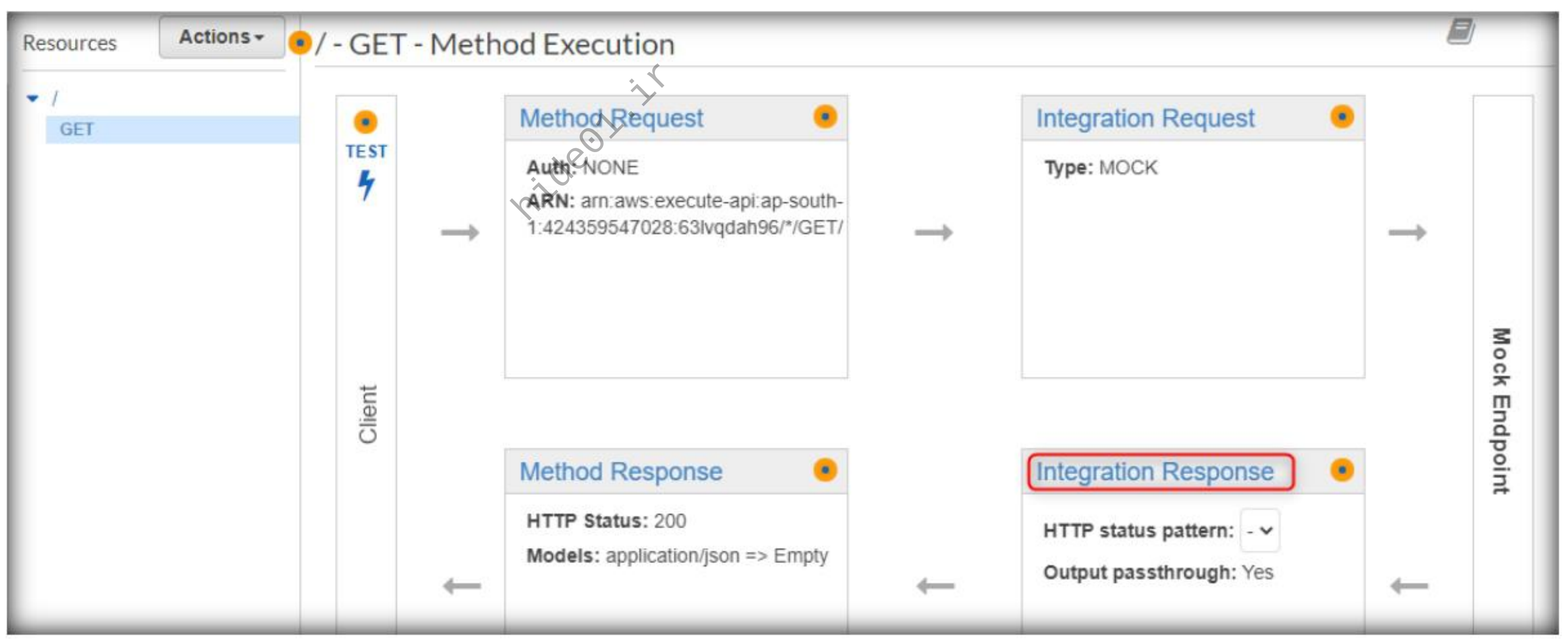


FIGURE 3.1.16: Adding Dummy Data

18. Expand the **arrow** button to add an integration response for the API method.

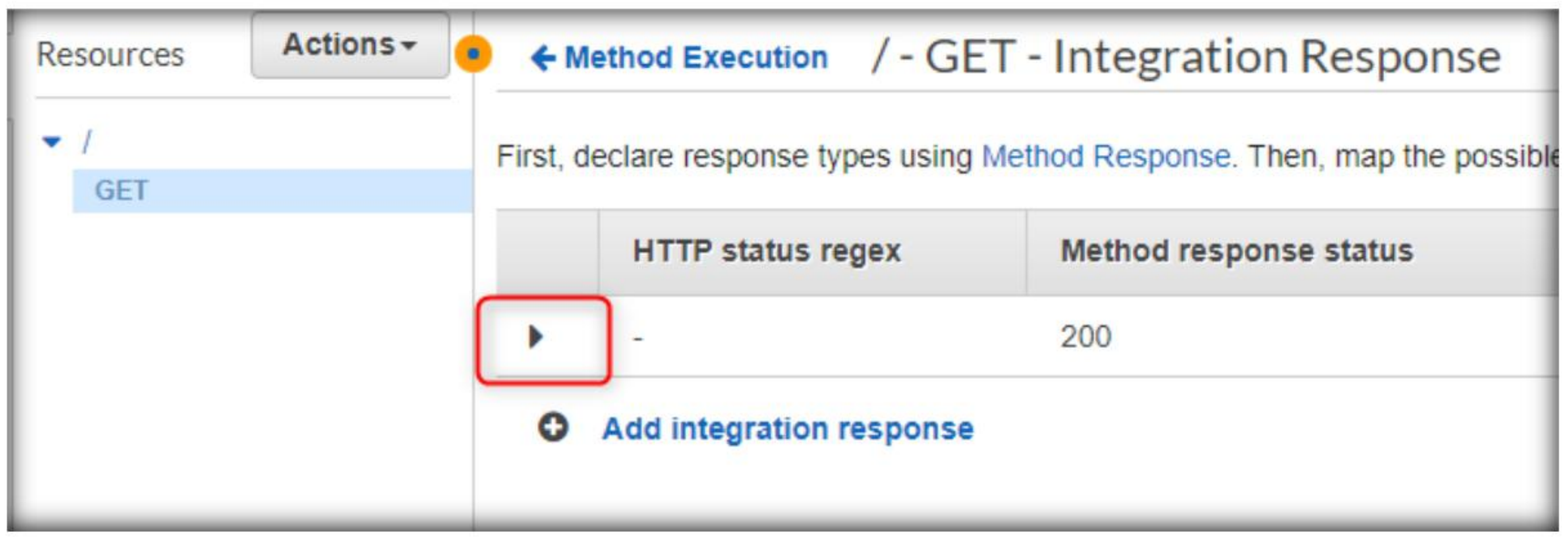


FIGURE 3.1.17: Integration Response Window

Certified Cloud Security Engineer Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

19. Next, expand the **Mapping Templates** and click on **application/json** under **Content-Type** in the **Generate template** editor window that appears.

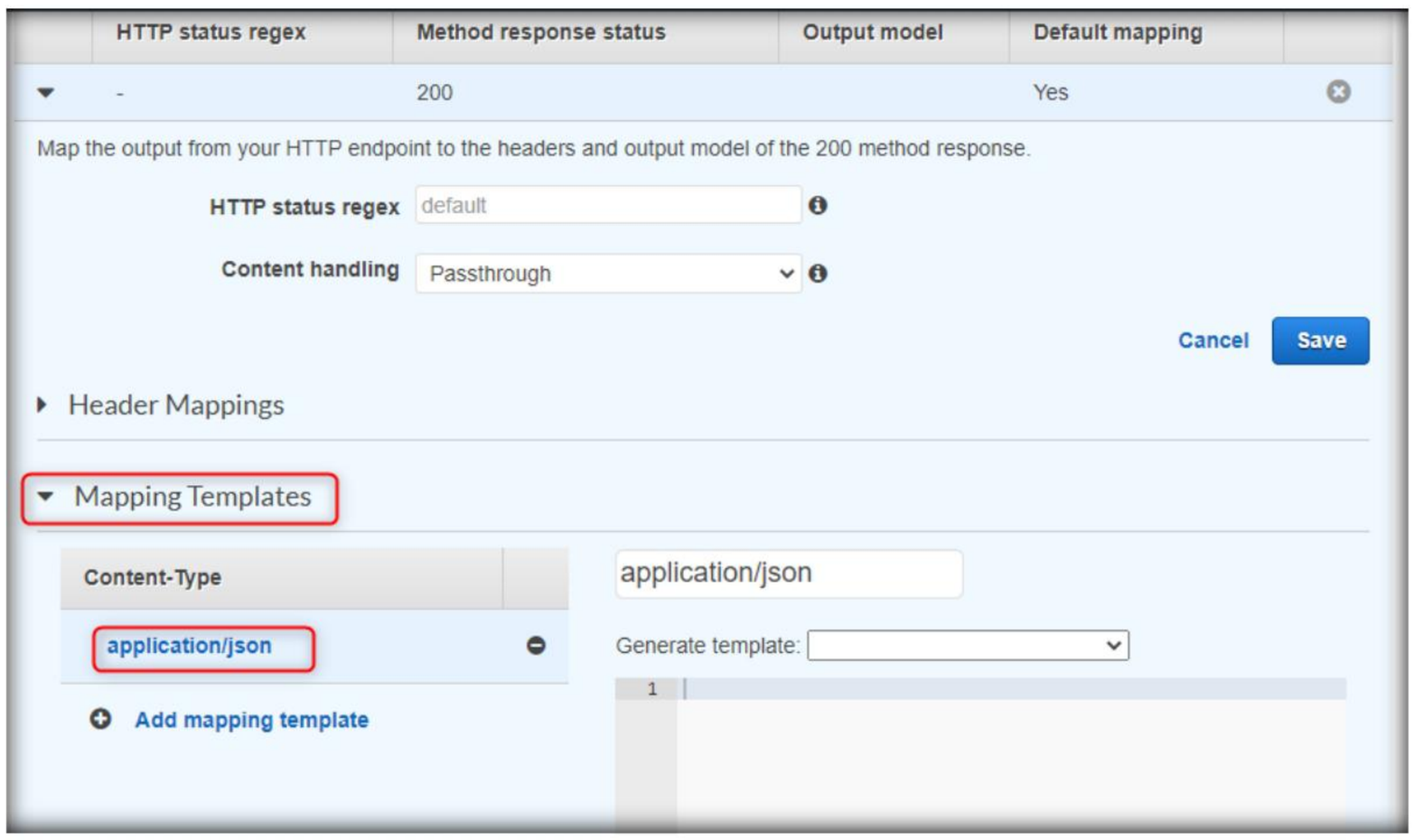


FIGURE 3.1.18: Template Editor Window

20. Type the text given below in the editor and click **Save**.

```
{
"message:"This is ECCcloud Demo api....!""
}
```

hide01.ir

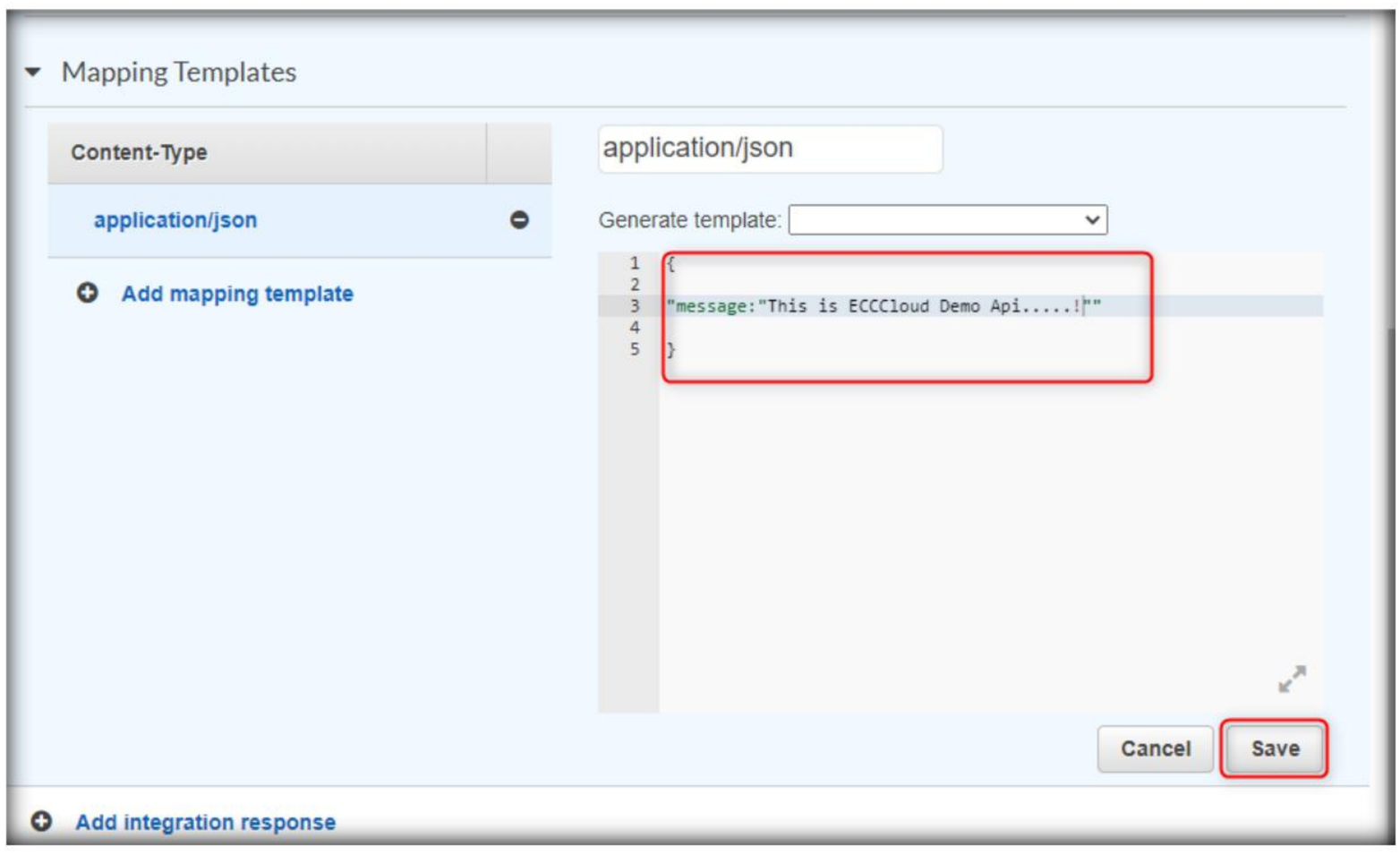


FIGURE 3.1.19: Adding Code in Editor

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

21. Click **Method Execution** at the top to go back.

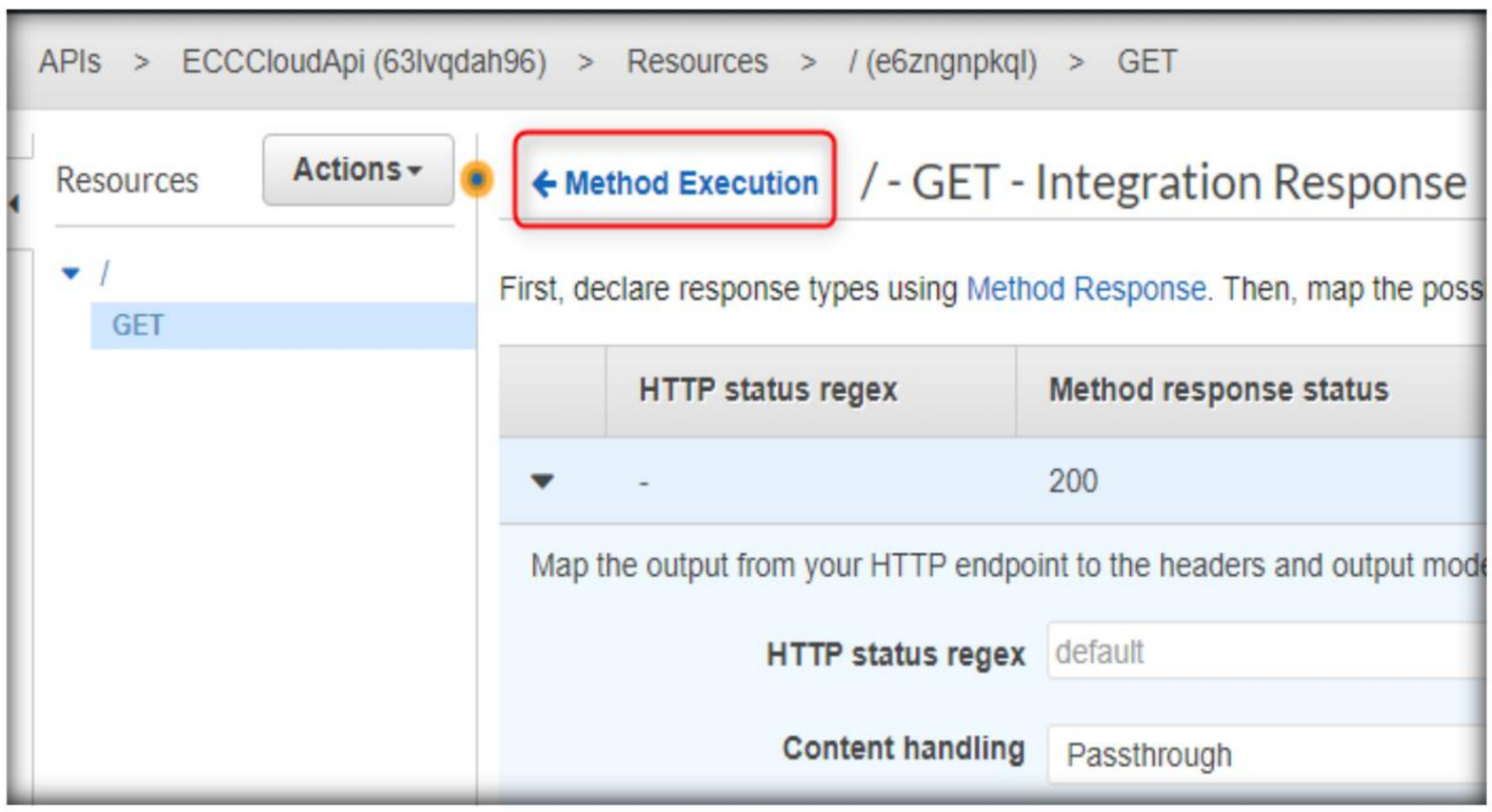


FIGURE 3.1.20: Navigating Back

22. Next, click on the **Actions** dropdown and then on **Deploy API** to deploy the created Web API.

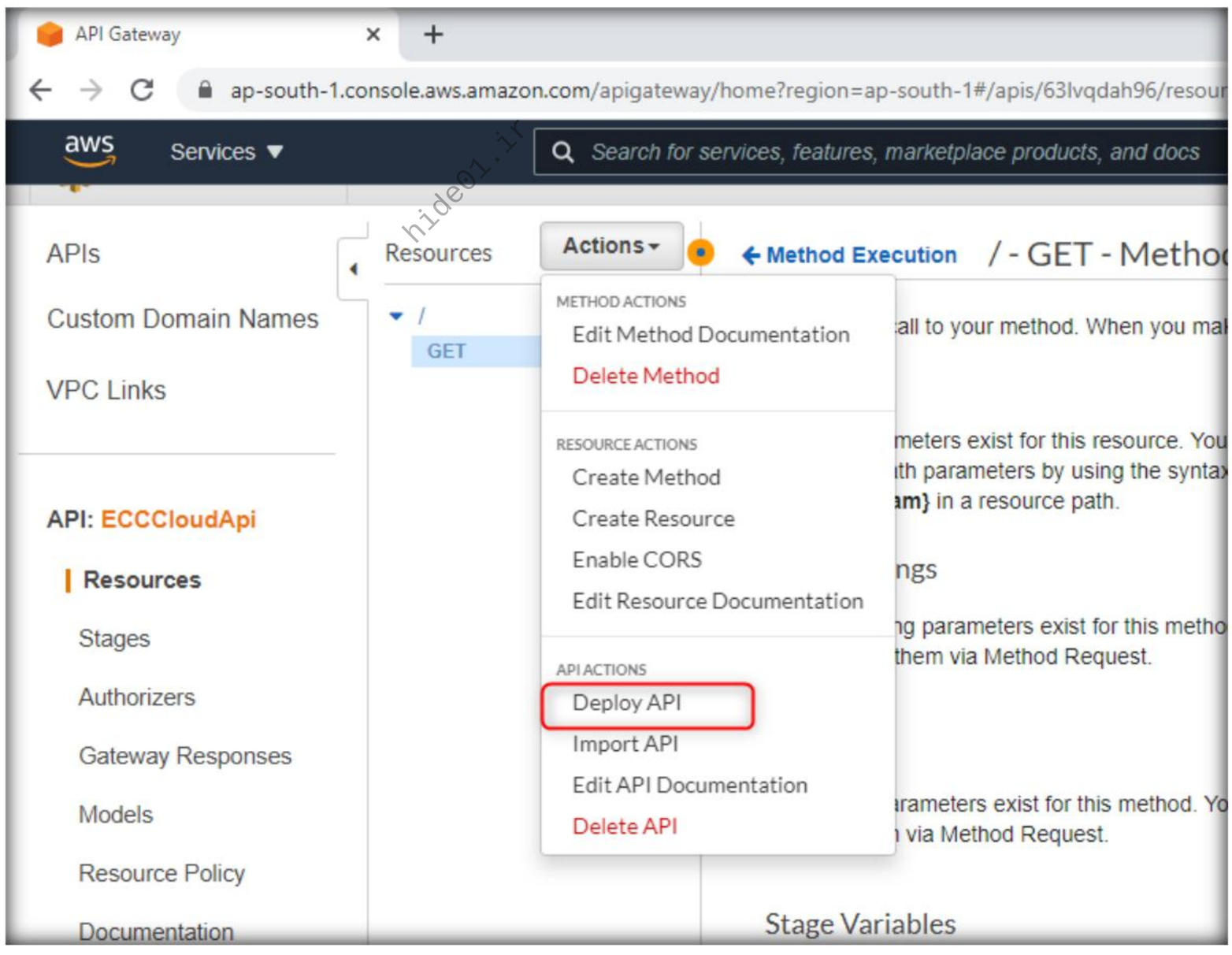


FIGURE 3.1.21: Deploying the API

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

23. To associate the Web API with API stage, select **Deployment stage** as **[New Stage]** and give it a name. In this lab, we have used **test** as the **Stage name.**

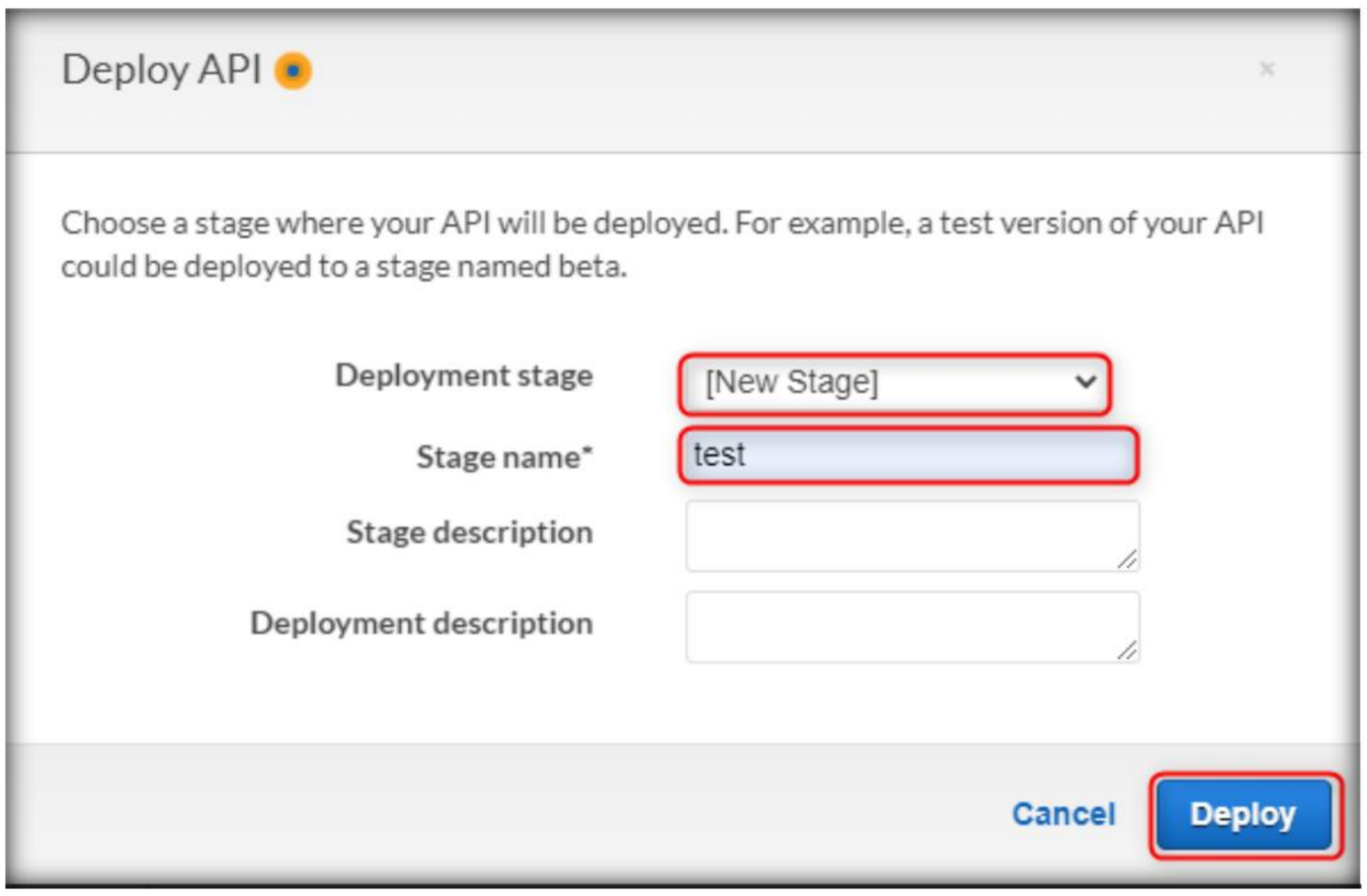
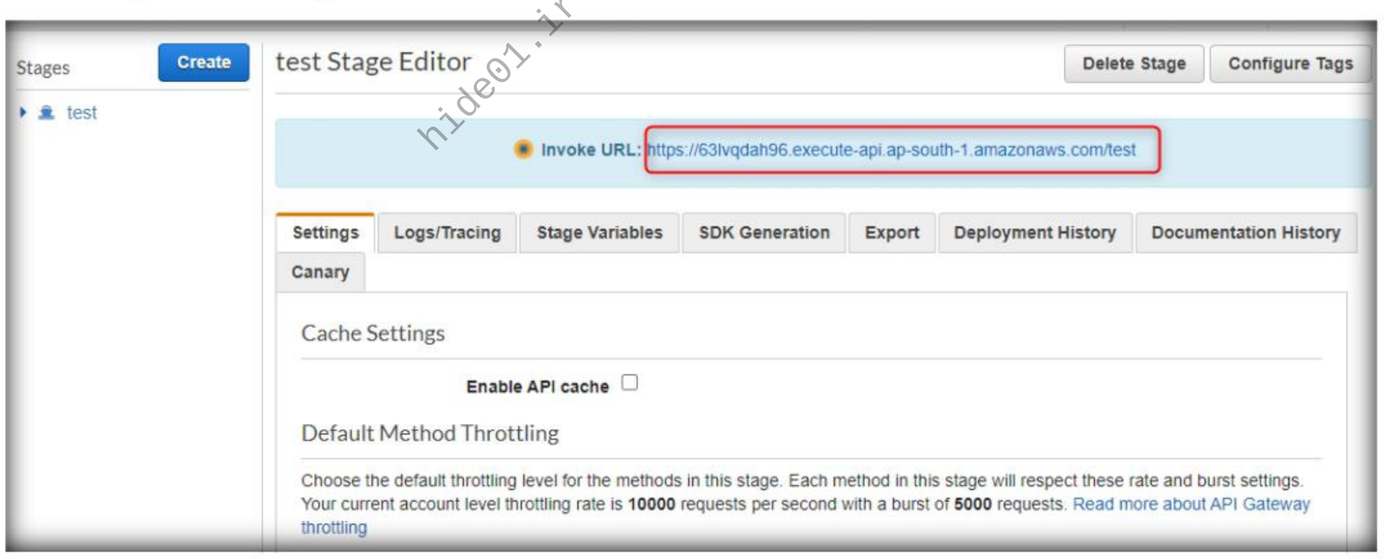


FIGURE 3.1.22: Associate the Web API with API stage

24. Now, you can see the **Invoke URL** of your API. Copy the URL, open notepad, and paste it there.



hide01.ir

FIGURE 3.1.23: Recording the Invoke URL

25. Paste the copied **Invoke URL** in a new browser tab and press **Enter.** You will see the json message as response.

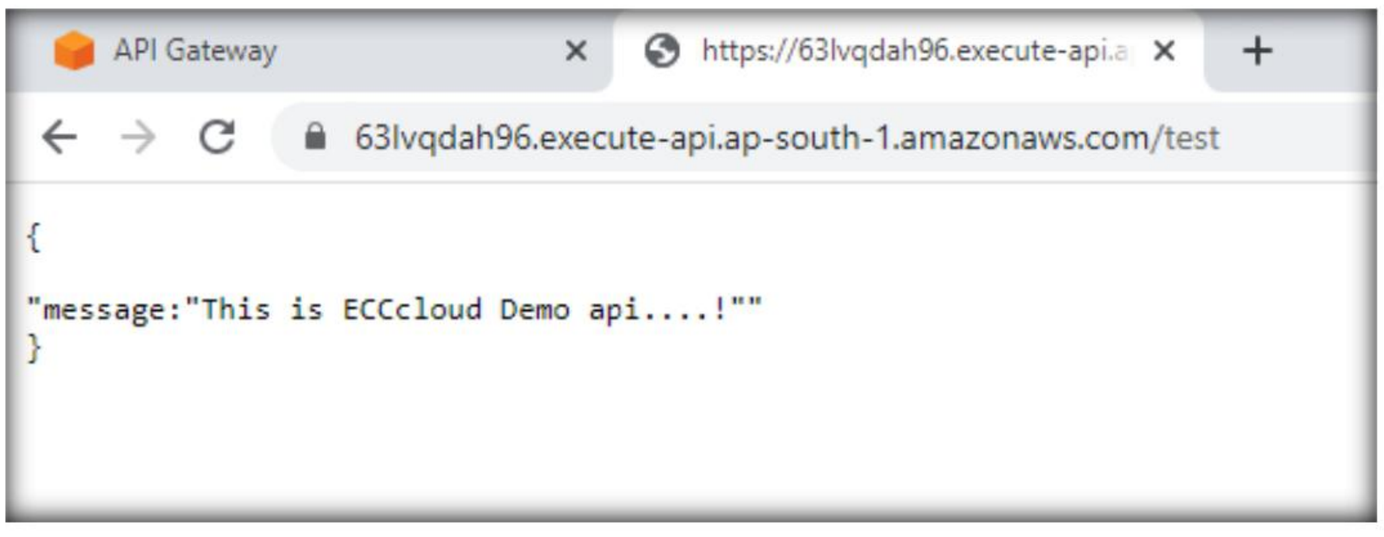


FIGURE 3.1.24: Response Message of API

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 2

Protecting API from Specified IP address with WAF

26. Now you will implement WAF to prevent some IP addresses from accessing the created Web API.
27. To access AWS WAF, click on **Services** and select **AWS Firewall Manager** under **Security Identity & Compliance** in the AWS console.

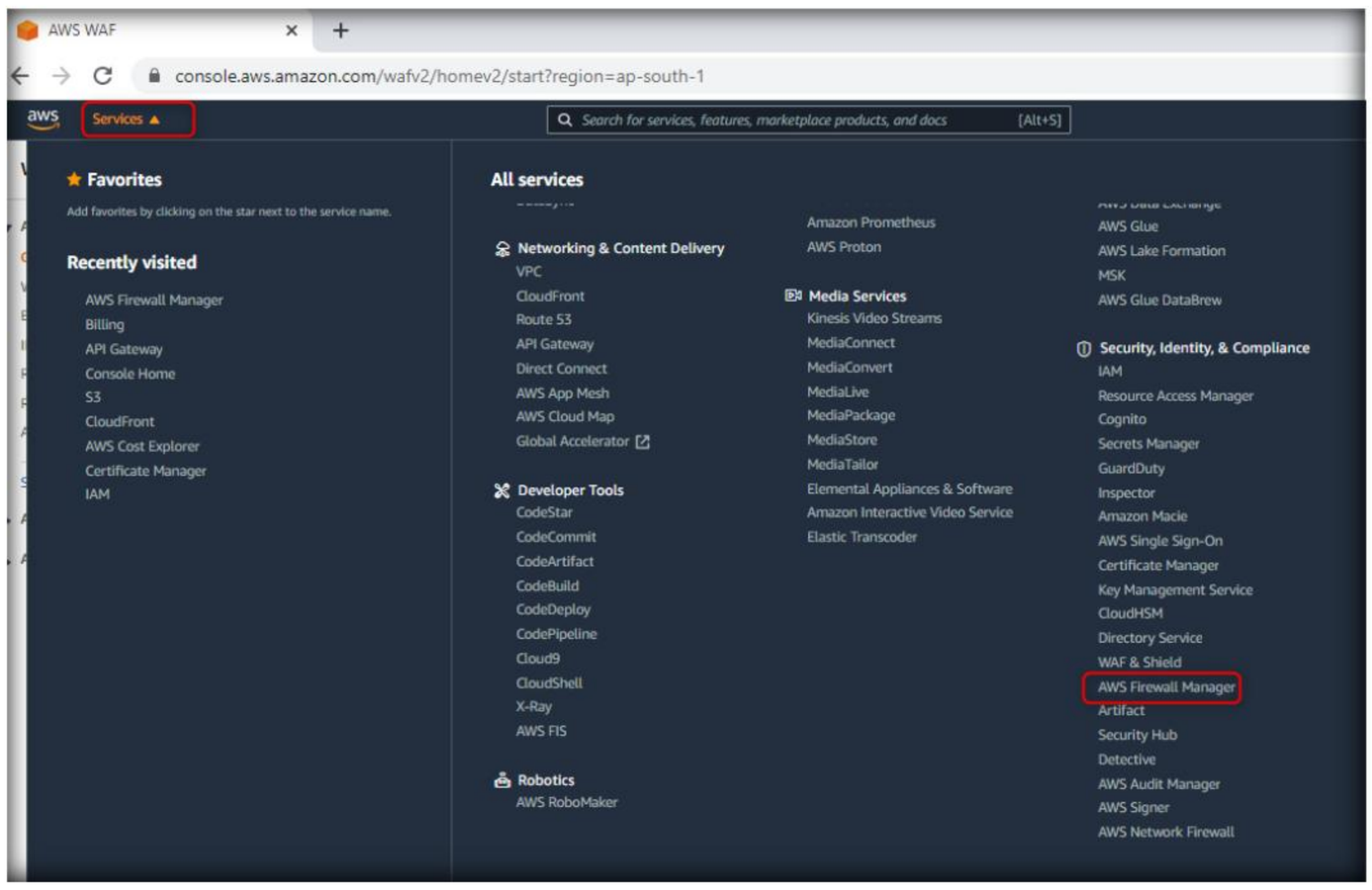


FIGURE 3.1.25: Navigating to AWS Firewall Manager

28. The AWS WAF page appears. Click **IP sets** from the left navigation pane to create an IP set that defines a collection or range of IP addresses for creating WAF rules.

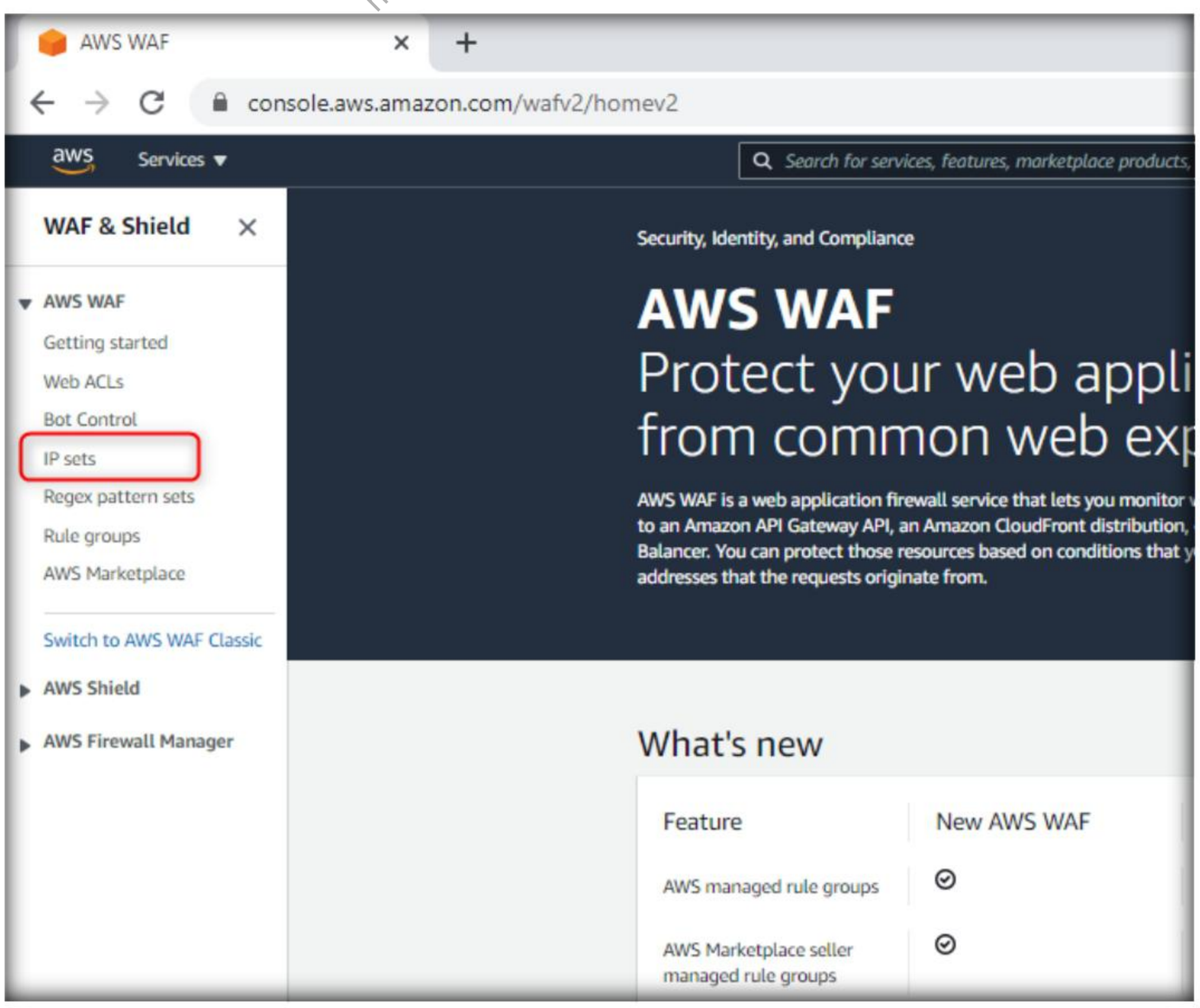


FIGURE 3.1.26: Selecting IP sets

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

29. Next, click on **Create IP set** button.

Note: Make sure you have selected the same region where you created the API.

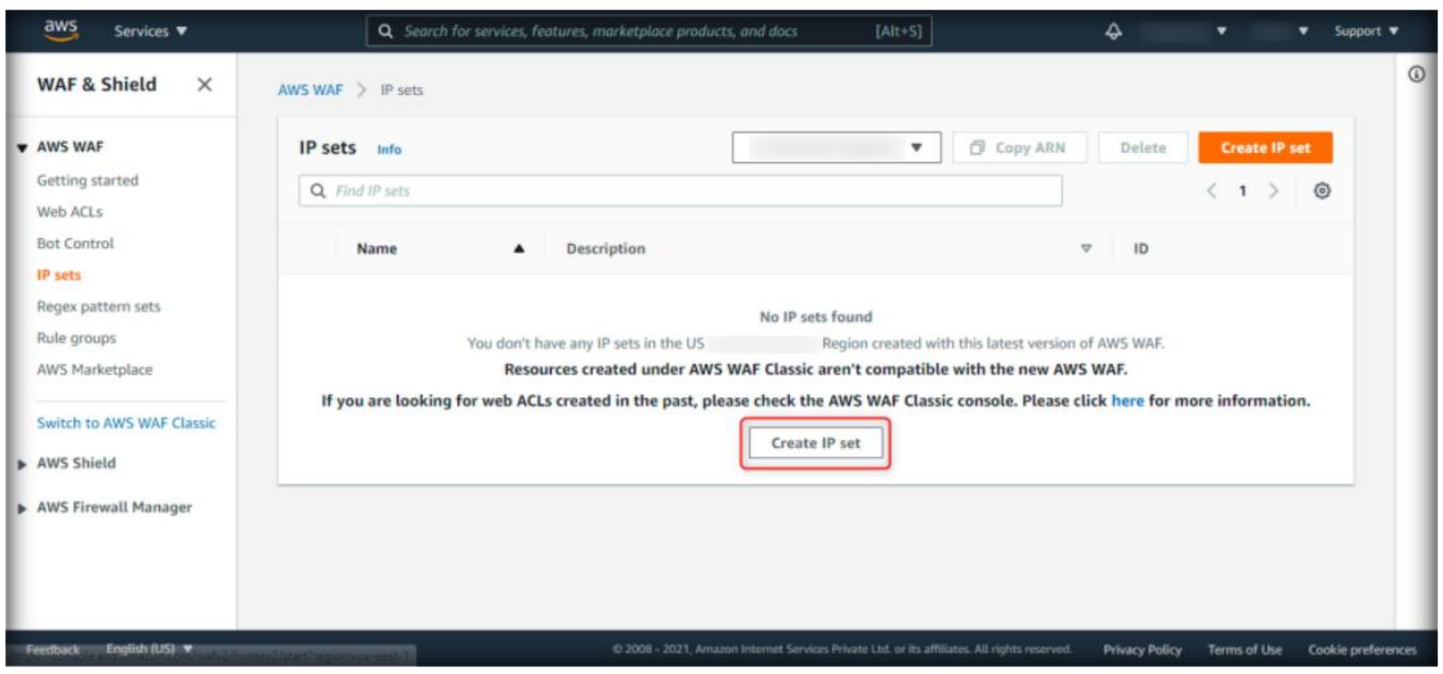


FIGURE 3.1.27: Creating IP set

30. Specify **IP set name** for the new IP set. Retain other default settings. In this lab, we have used **blacklistips** as the IP set name.

Note: Ensure the created Web API and the IP set have the same region.

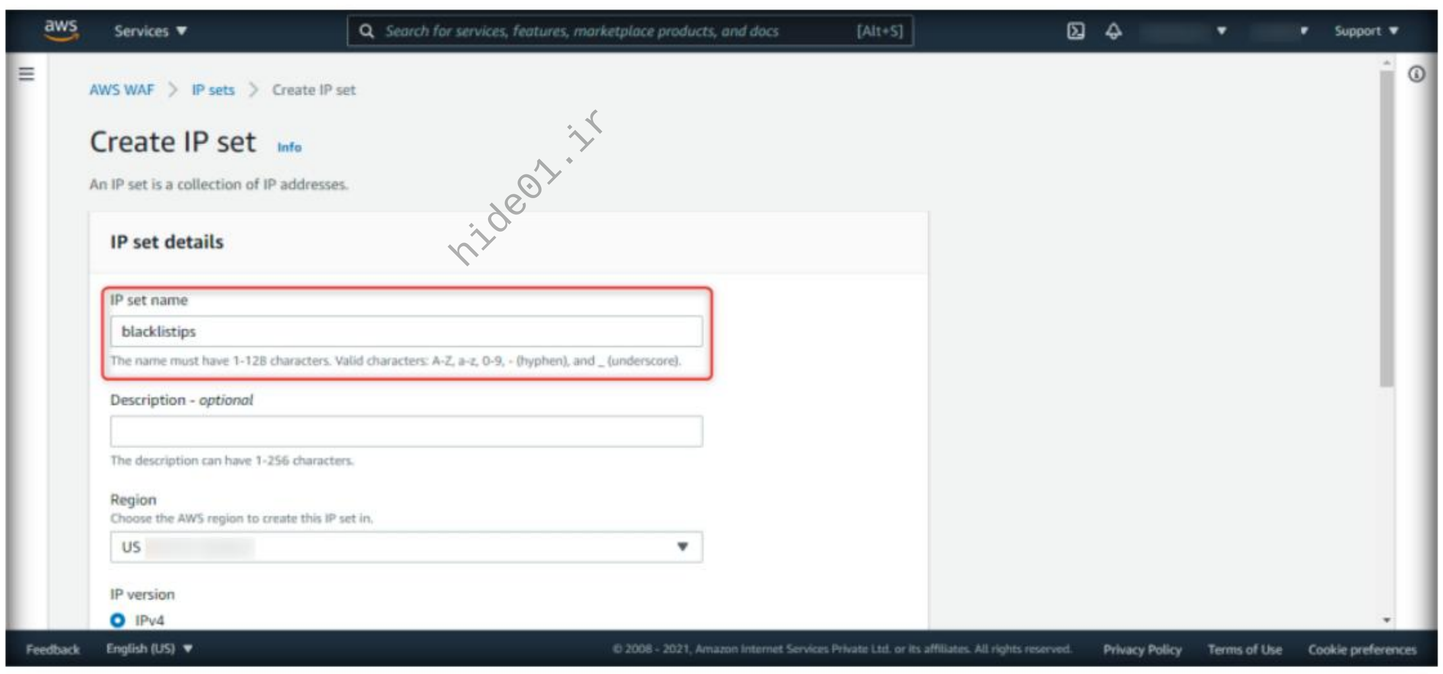


FIGURE 3.1.28: Configuring IP Set



FIGURE 3.1.29: Creating IP Set

Certified Cloud Security Engineer Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

31. Scroll down and click on **Create IP set**.
32. A **"You successfully created the IP set blacklistips"** message will be displayed, indicating the IP set is created. You will see the created IP set details in the list of IP sets.

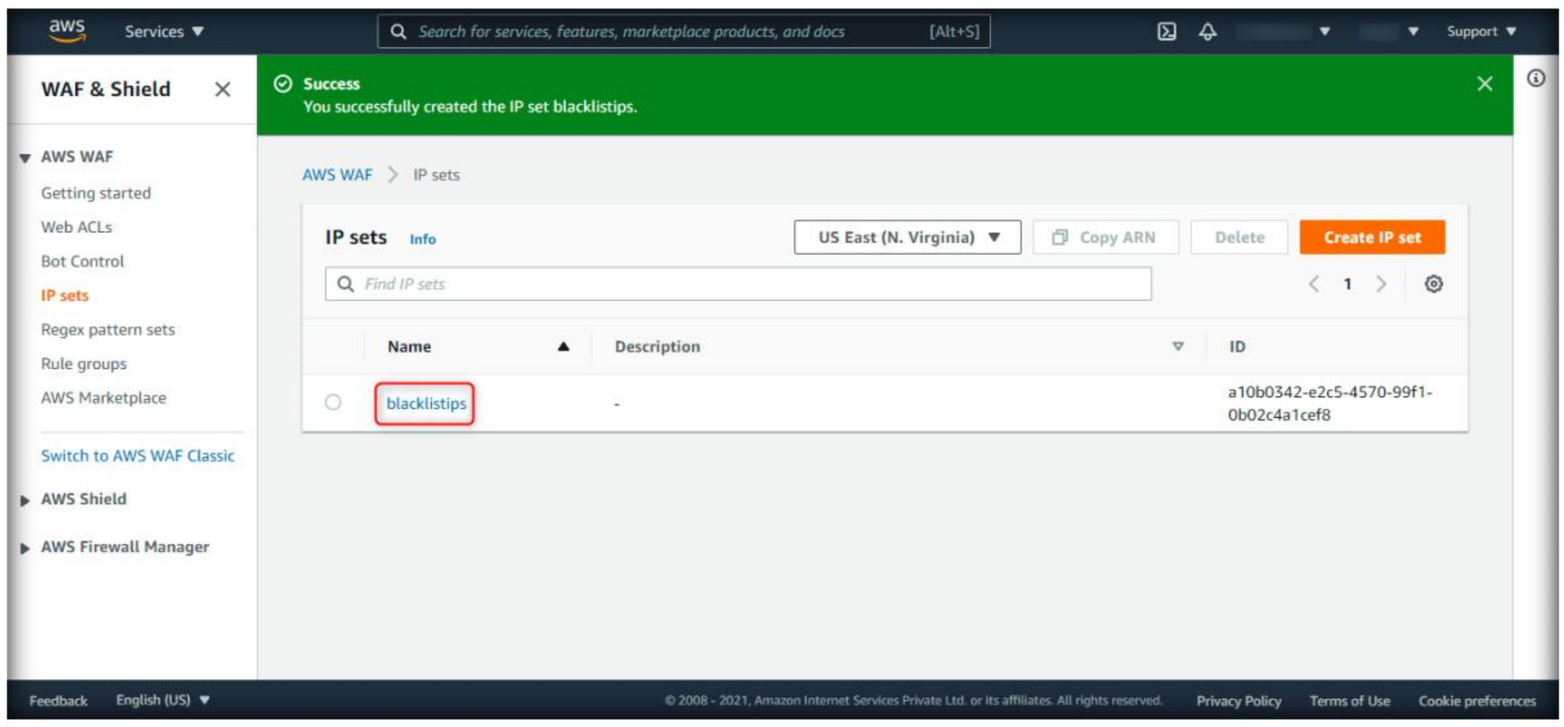


FIGURE 3.1.30: IP Set Created Successfully

33. For this lab, we have used the public IP address of the machine where the lab is being executed. You can include your own public IP address or any other machine IP address for blocking access to the Web API.
34. To test this lab, include your machine's public IPv4 address. To get the IP address of your machine, open a new tab in the browser and browse to https://whatismyipaddress.com/ to find your machine's public IPv4 address. Copy this address.

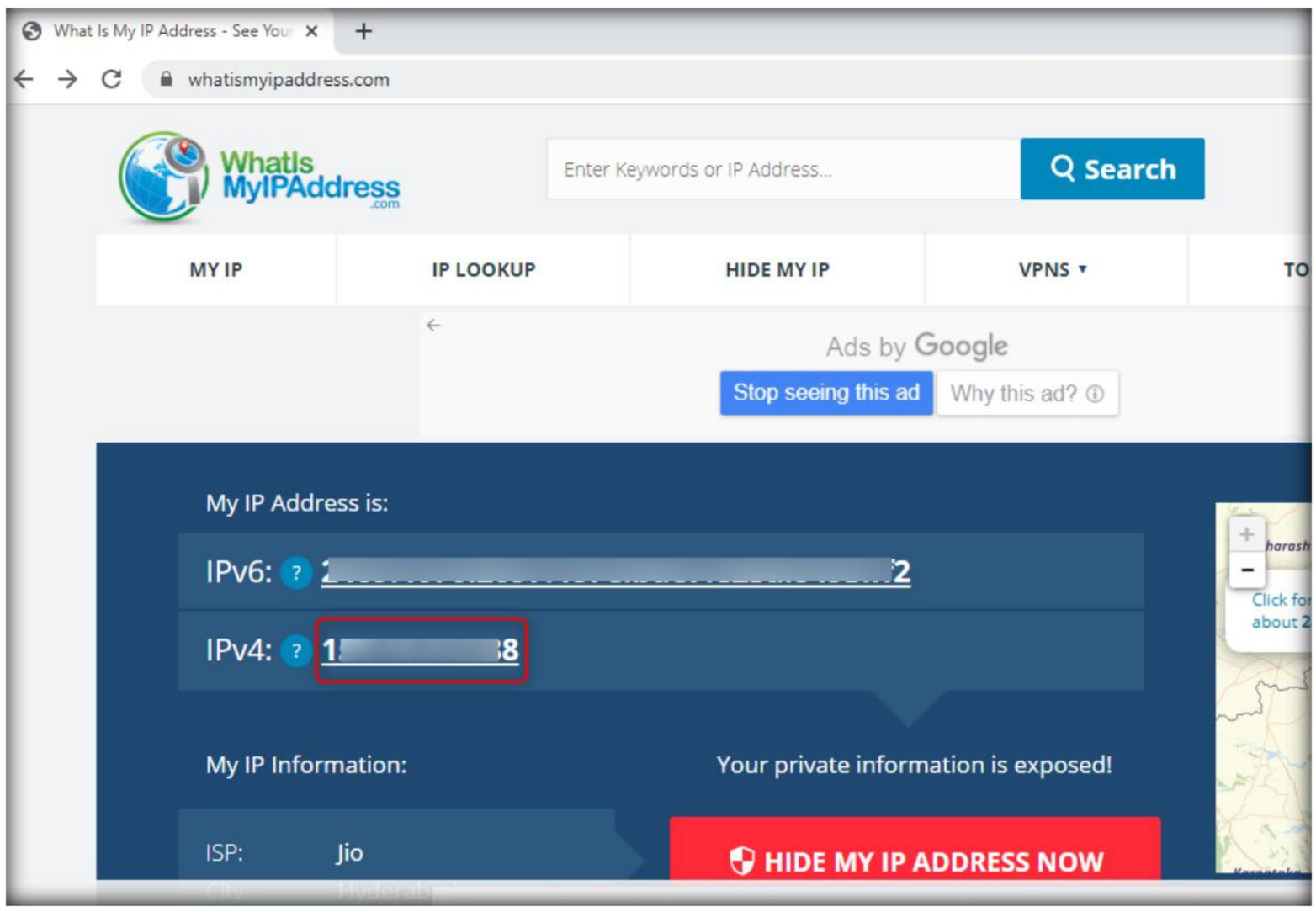


FIGURE 3.1.31: Getting the Public IP Address

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

35. Click on **blacklistips**, the IP set you created.

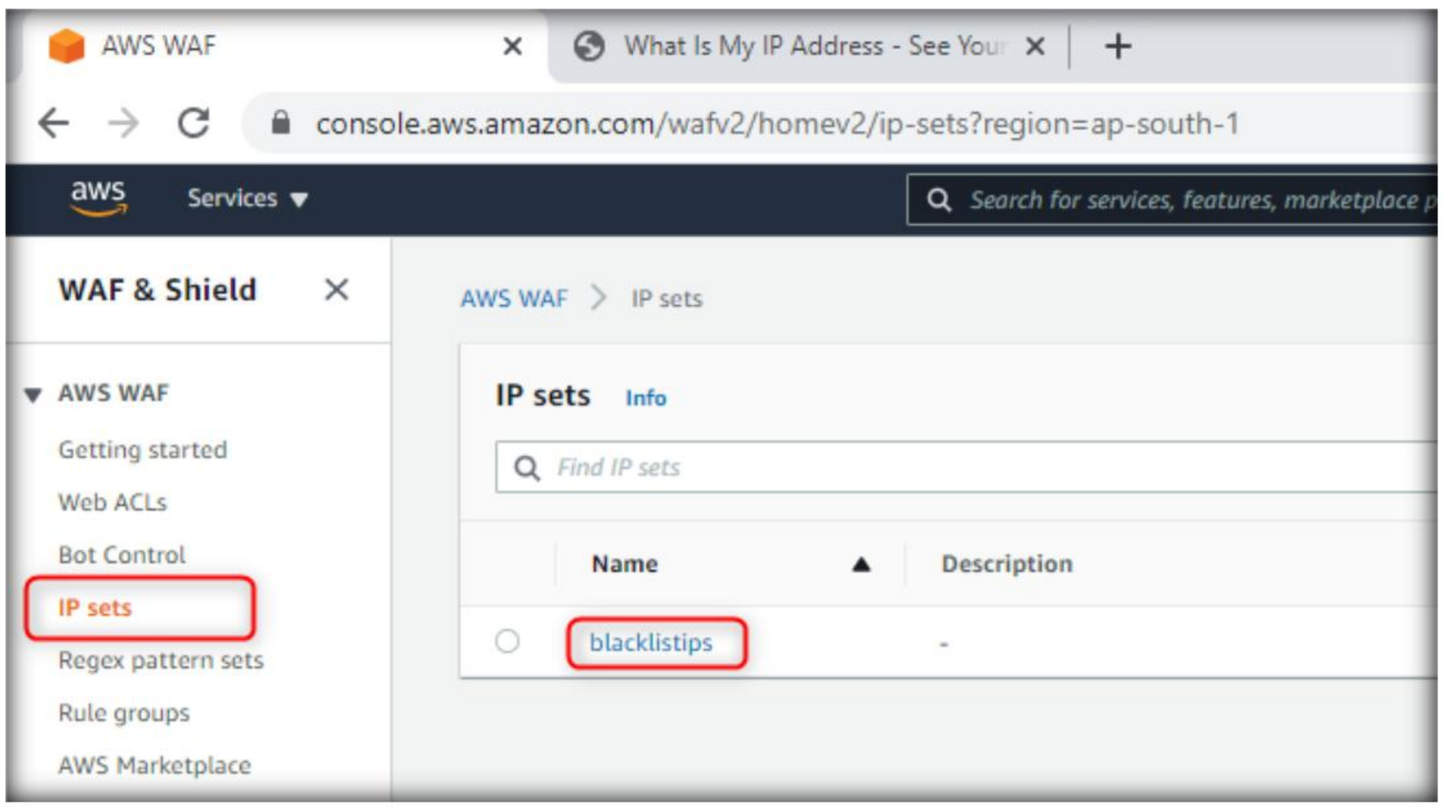


FIGURE 3.1.32: Opening IP Set

36. The **blacklistips** detail page opens. Click **Add IP addresses.**



FIGURE 3.1.33: blacklistips page

37. In the **Add IP addresses to blacklistips** popup window that appears, paste the copied public IPv4 address of your machine and add **/32** after it. Then, click **Add**.

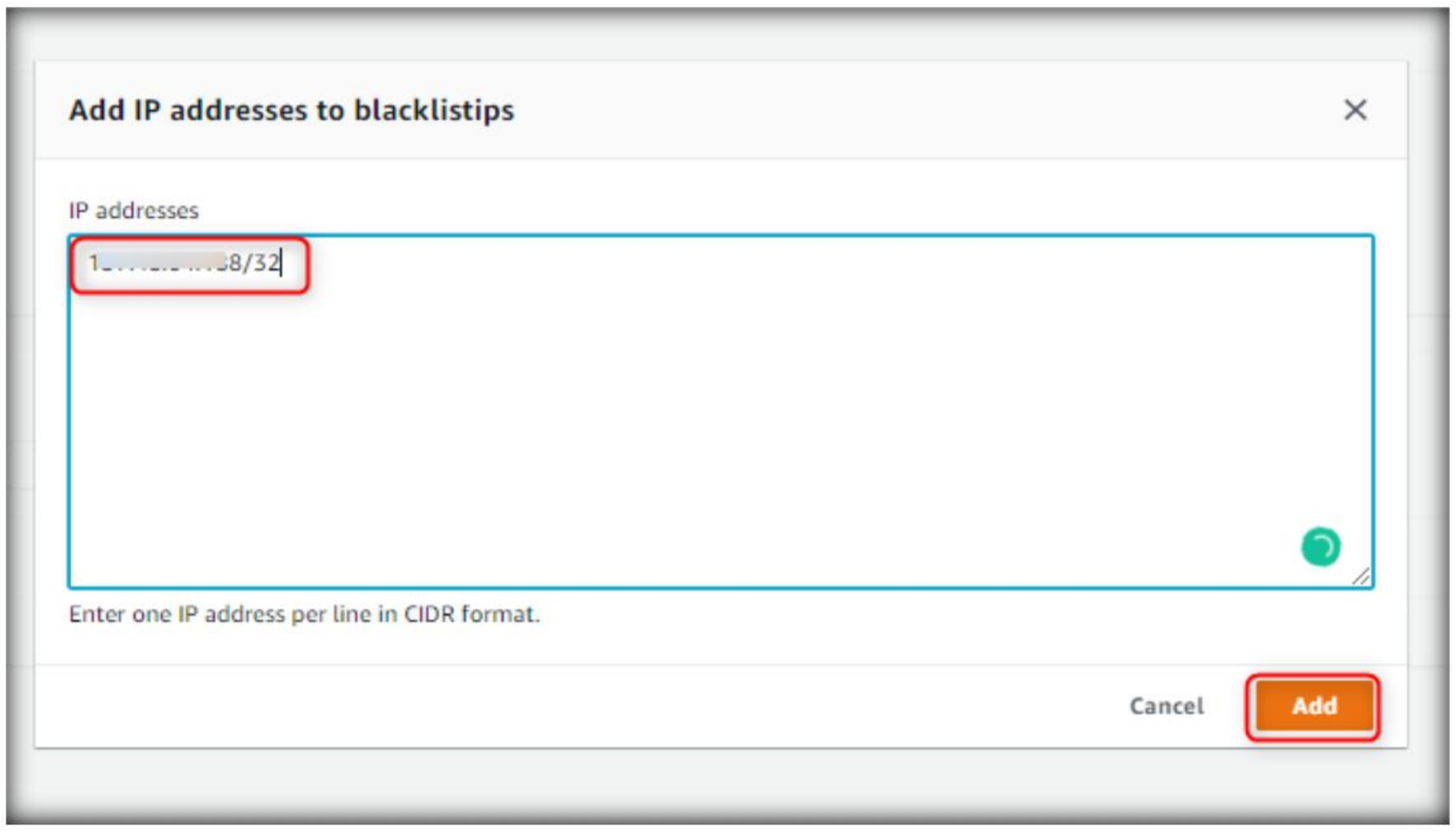


FIGURE 3.1.34: Adding the IP Address

Certified Cloud Security Engineer Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

38. The IP address is added successfully, as shown in following screenshot.

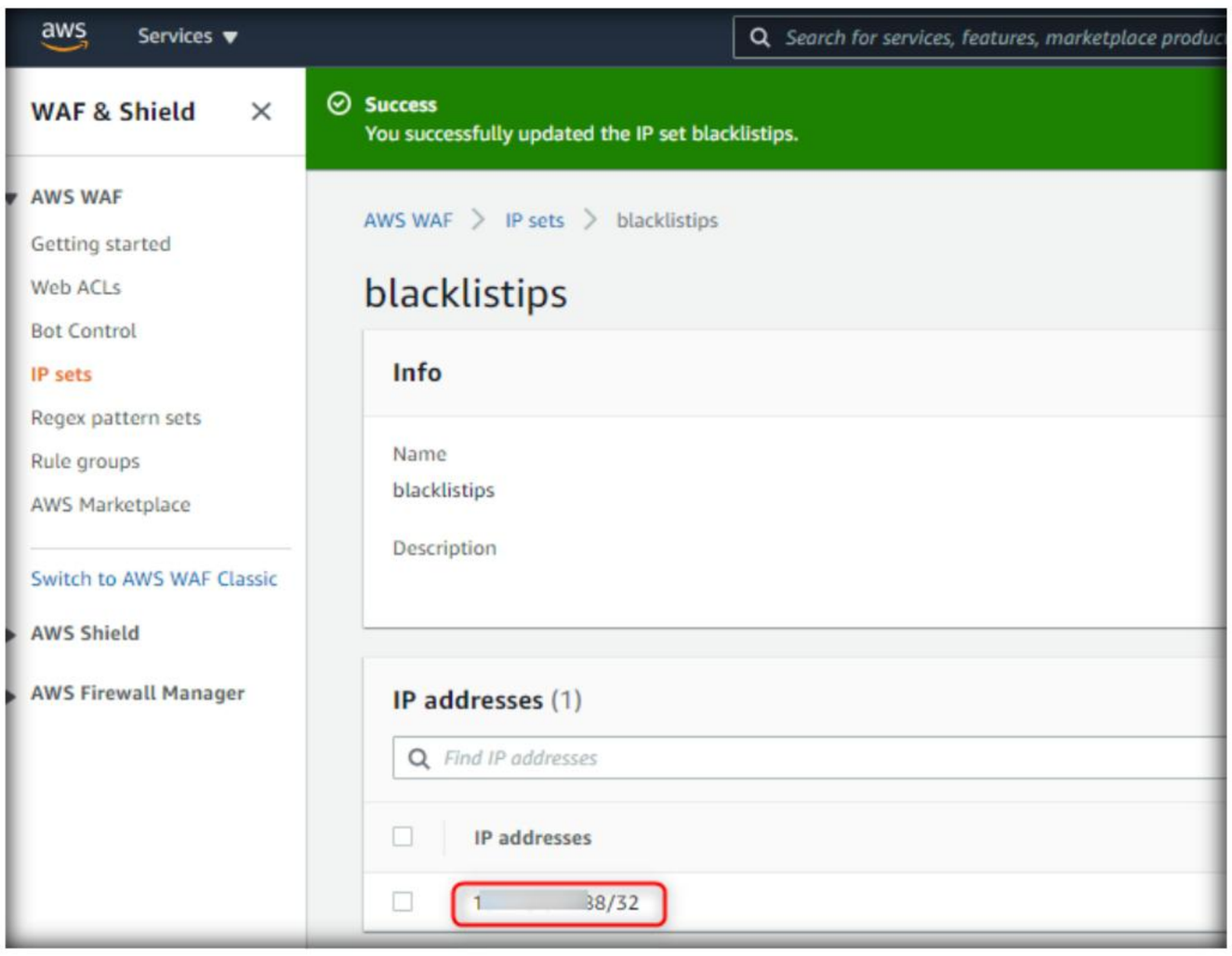


FIGURE 3.1.35: Include System IP address

TASK 3

Creating WEB ACL in WAF

39. Next, create a Web ACL to block requests to the created Web API. Click **Web ACLs** from the left navigation pane.

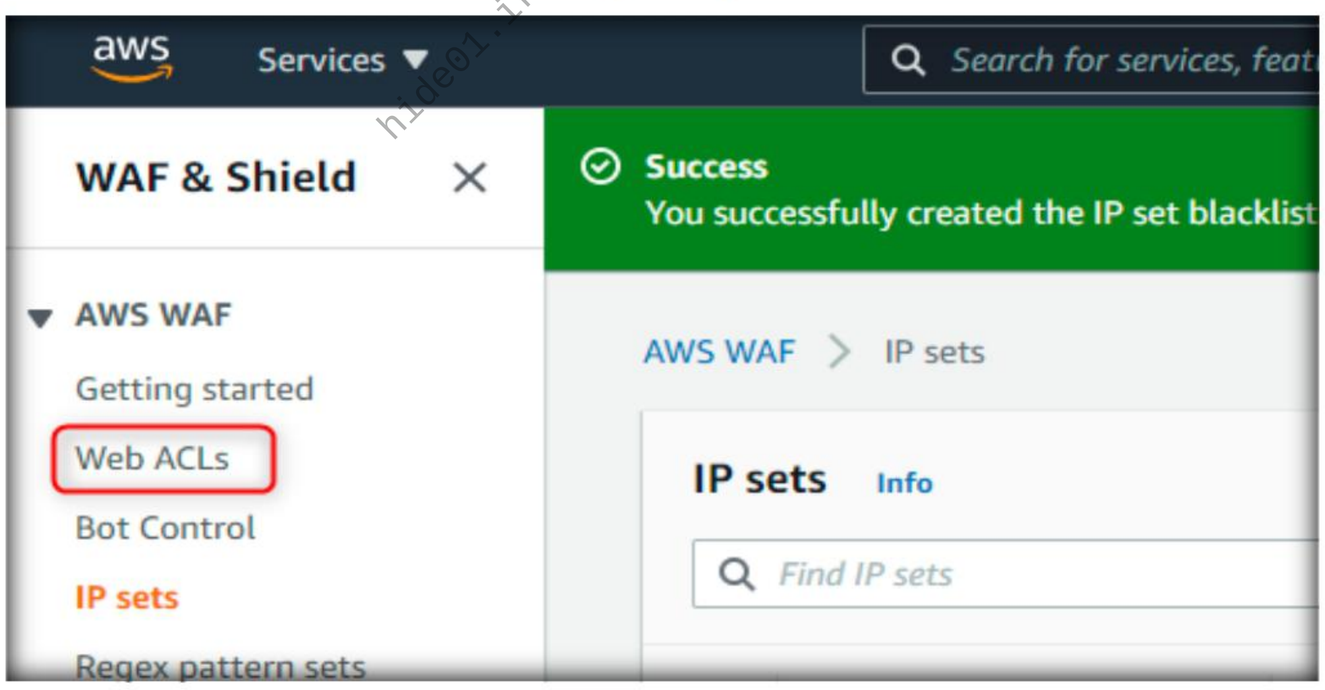


FIGURE 3.1.36: Opening Web ACLs

40. Click the **Create web ACL** button in the **Web ACLs** window.

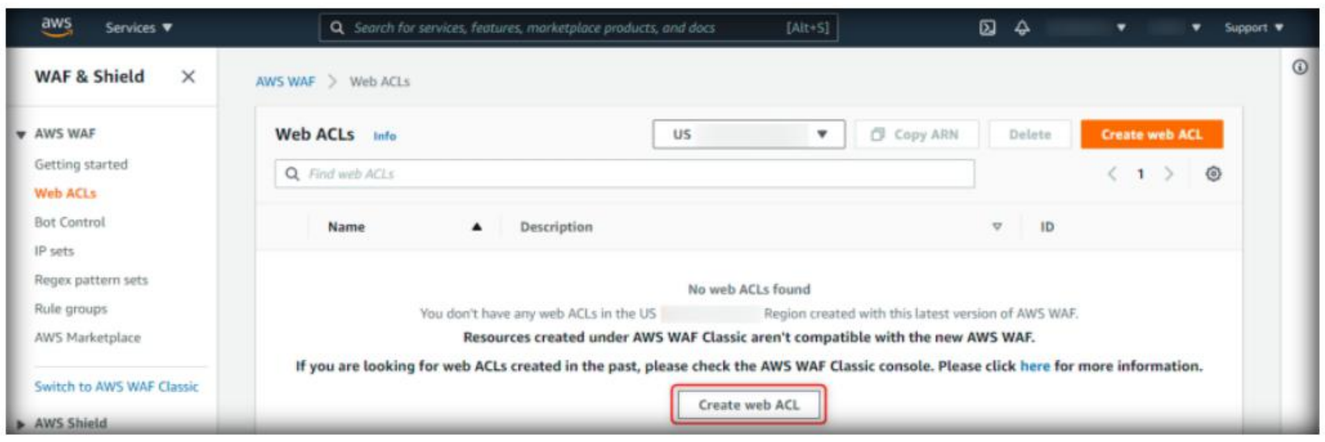


FIGURE 3.1.37: Creating Web ACL

Certified Cloud Security Engineer Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

41. Give a name to the ACL. In this lab, we have used **ECCWeb-ACL** as the ACL name. Now, select **Regional resources** as **Resource type** to associate the ACL with the API Gateway. Next, click on **Add AWS resources** to associate the ACL with the **ECCCloudApi-test** API.

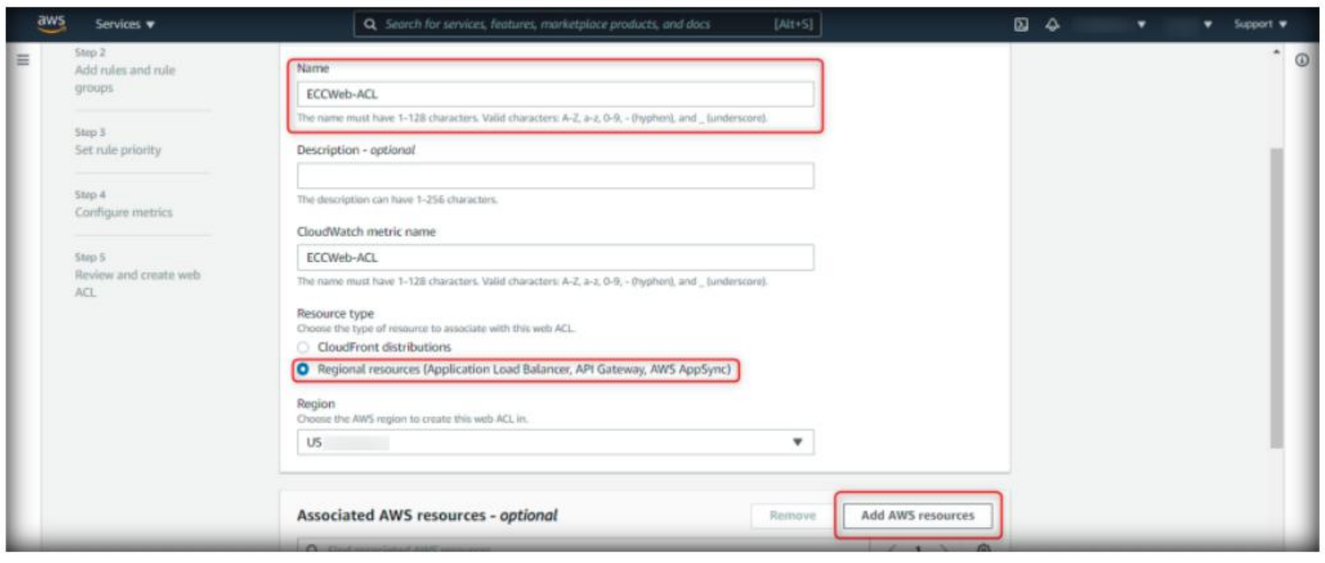


FIGURE 3.1.38: Configuring Web ACL

42. An **Add AWS resources** pop-up appears, and you can see the created API. Now, select **ECCCloudApi-test** and click **Add.**

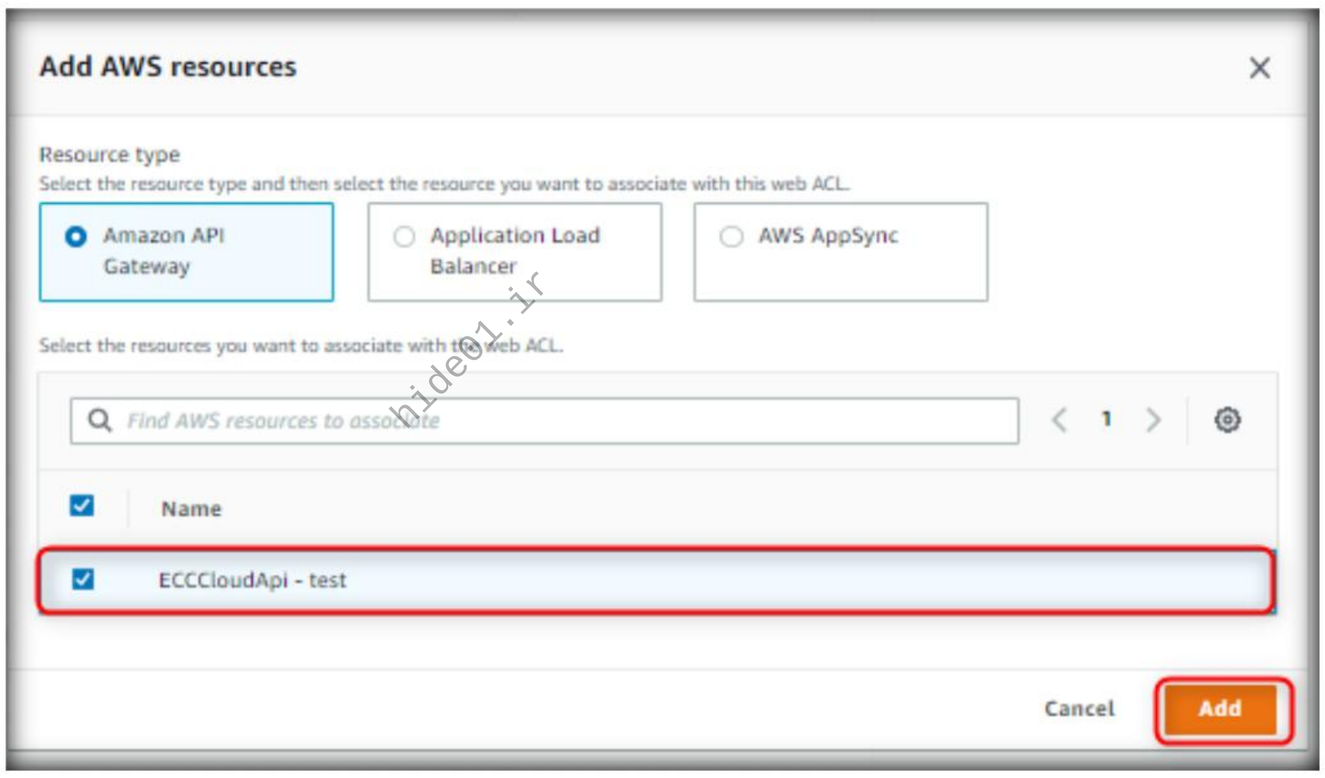


FIGURE 3.1.39: Adding AWS Resources

43. Select the checkbox for **ECCCloudApi-test** under **Associated AWS resources-optional** and click **Next** to continue.

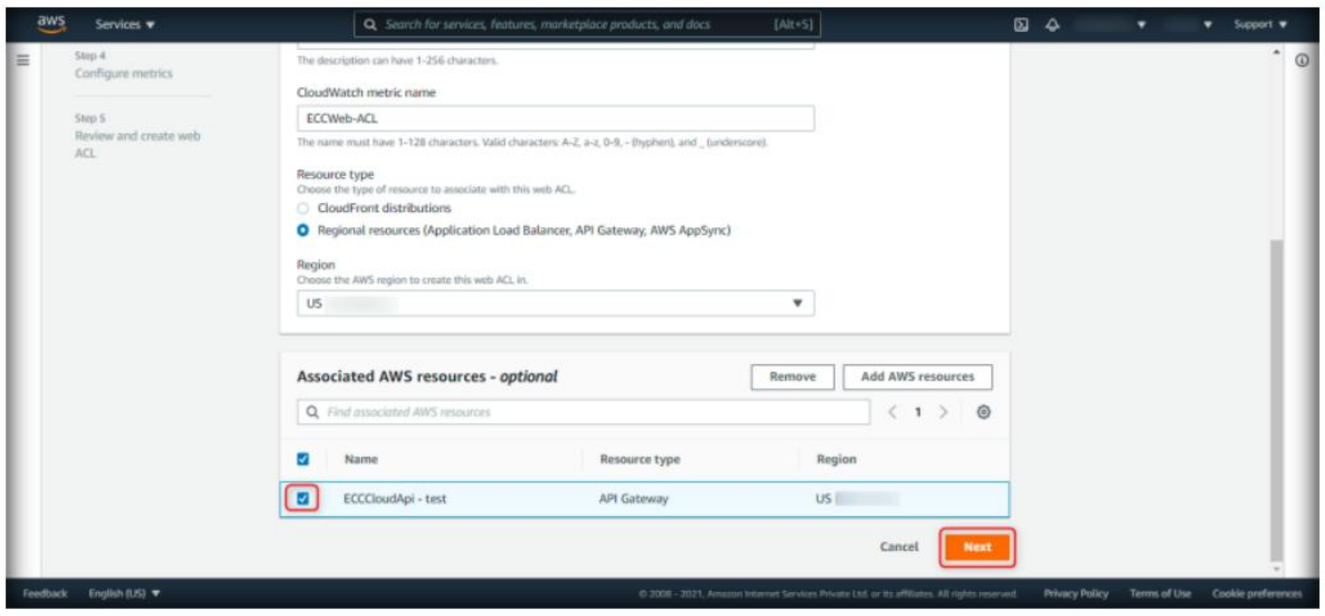


FIGURE 3.1.40: Proceeding with Configuration

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

44. To add rule groups to block web requests, which will be used by the Web ACL, click on the **Add Rules** dropdown in the **Add rules and rule groups** window and select **Add my own rules and role groups**.

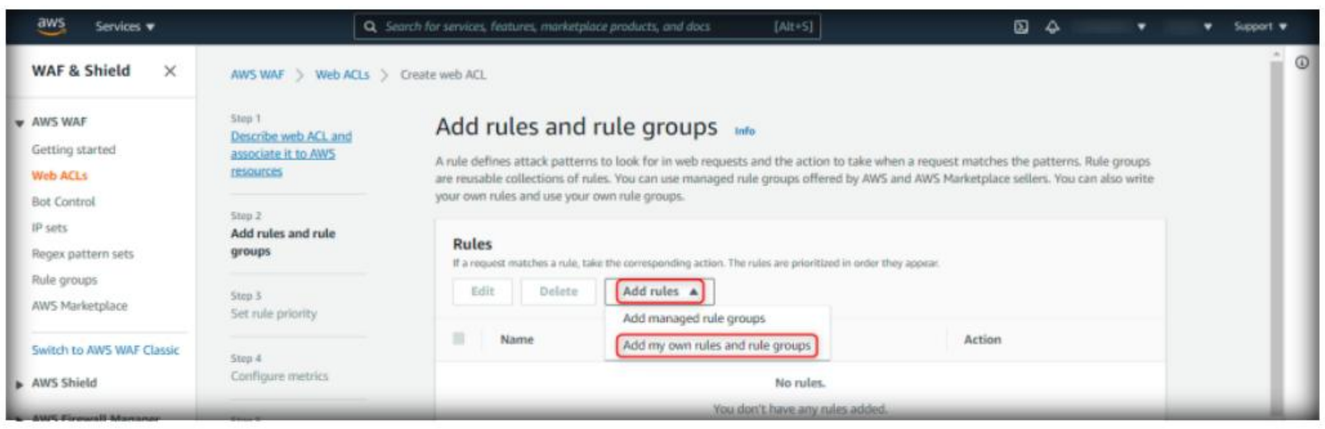
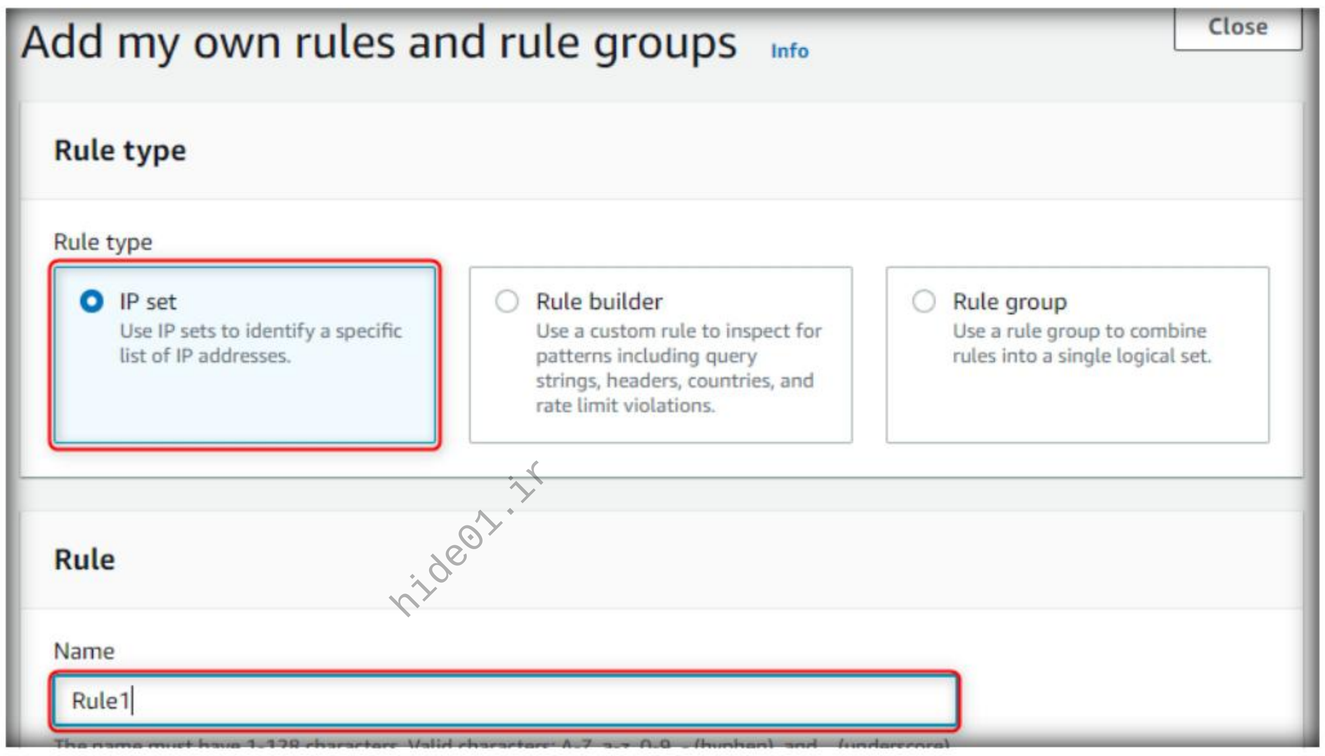


FIGURE 3.1.41: Adding Rules

45. To use the created IP set, select **Rule type** as **IP set** and give a name to the rule. In this lab, we have used **Rule1** as the **Name**.



hide01.ir

FIGURE 3.1.42: Configuring Rules and Rule Groups

46. Select **blacklistips**, the **IP set** you created, from the dropdown and choose **Block** as the **Action** option. Then, click on **Add rule**.

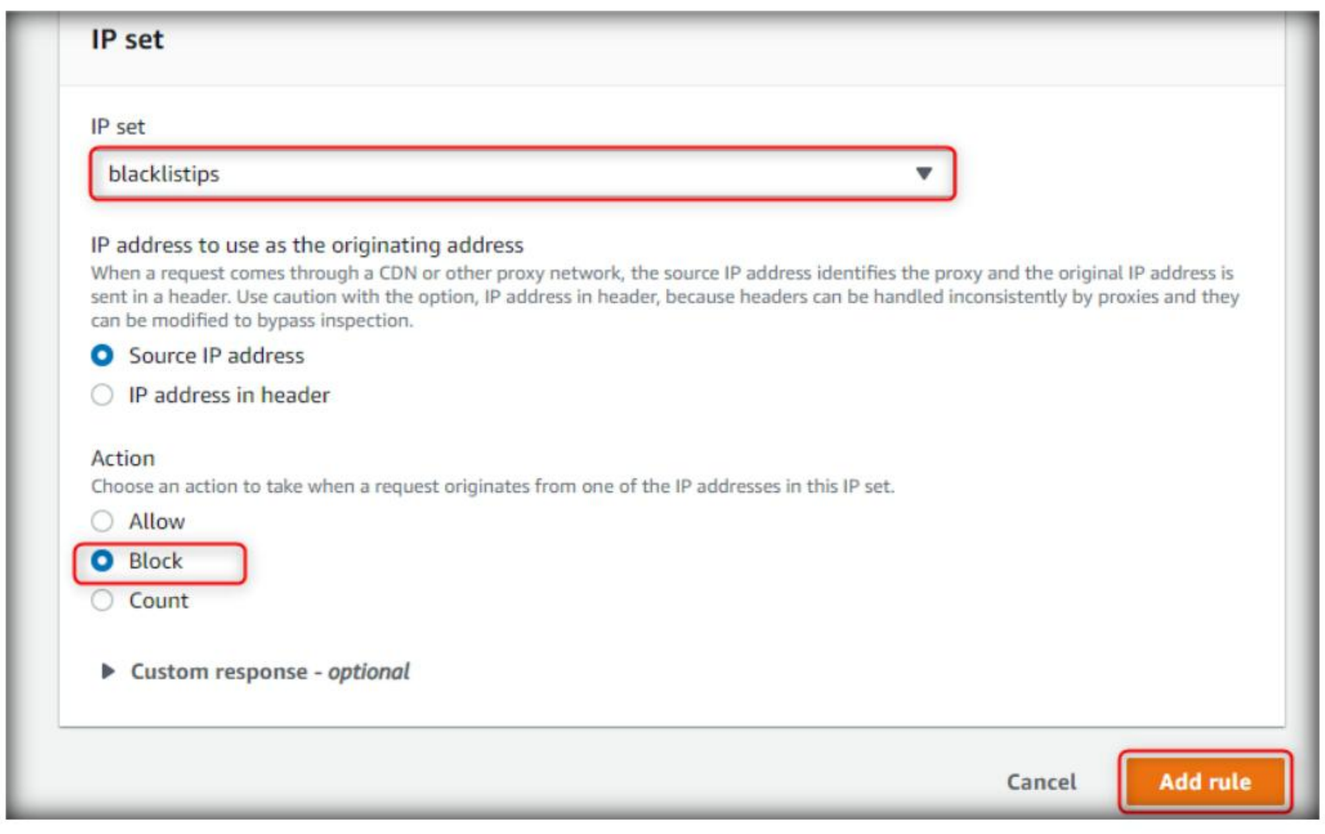


FIGURE 3.1.43: Selecting IP Set and Action

Certified Cloud Security Engineer Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

47. You can see that **Rule1** is added to the list. To enable **Rule1** for the ACL, select the checkbox next to it. Then, click **Next**.

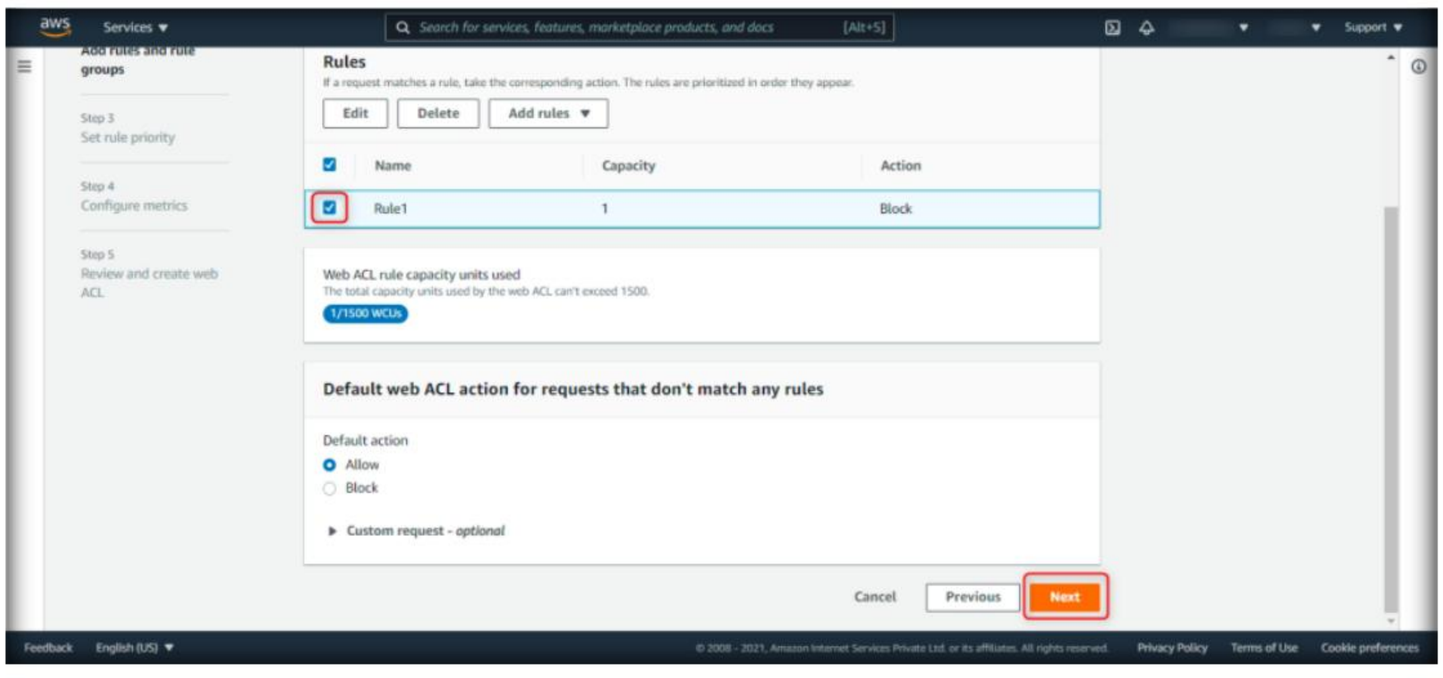


FIGURE 3.1.44: Proceeding with Configuration

48. Next, select **Rule1** in the **Set rule priority** window and click **Next**.

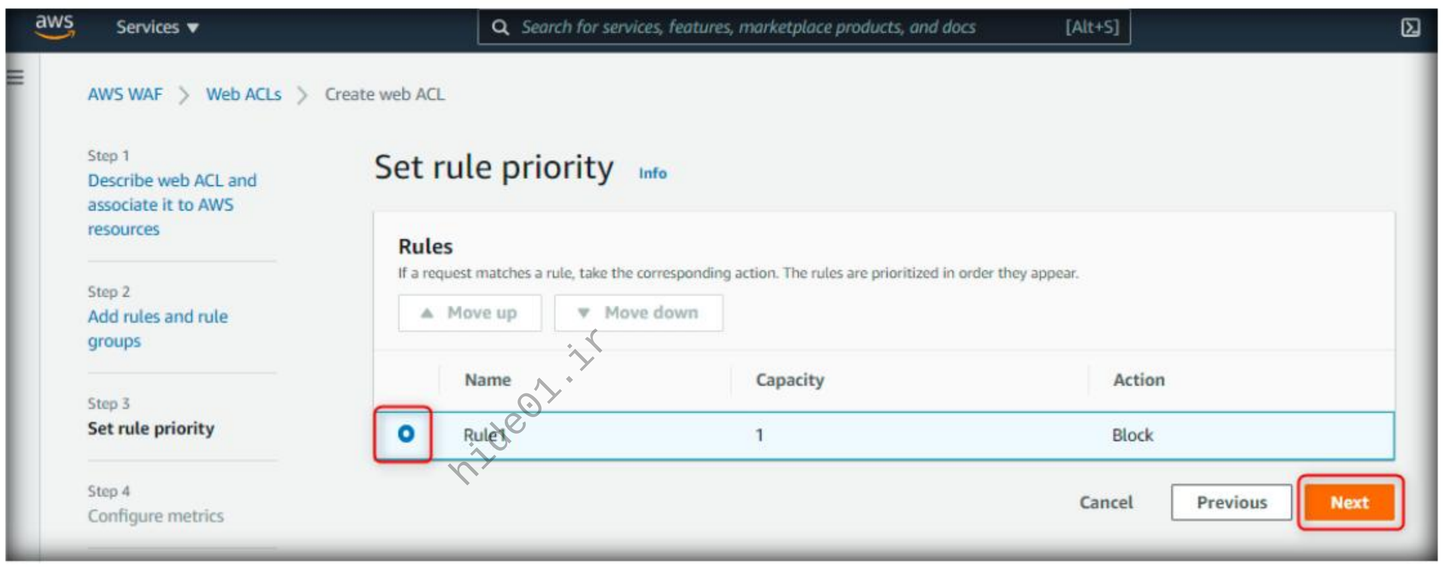


FIGURE 3.1.45: Proceeding with Configuration

49. The **Configure metrics** window enables you to configure the tagging and logging settings for the Web ACL. Click **Next** to continue.

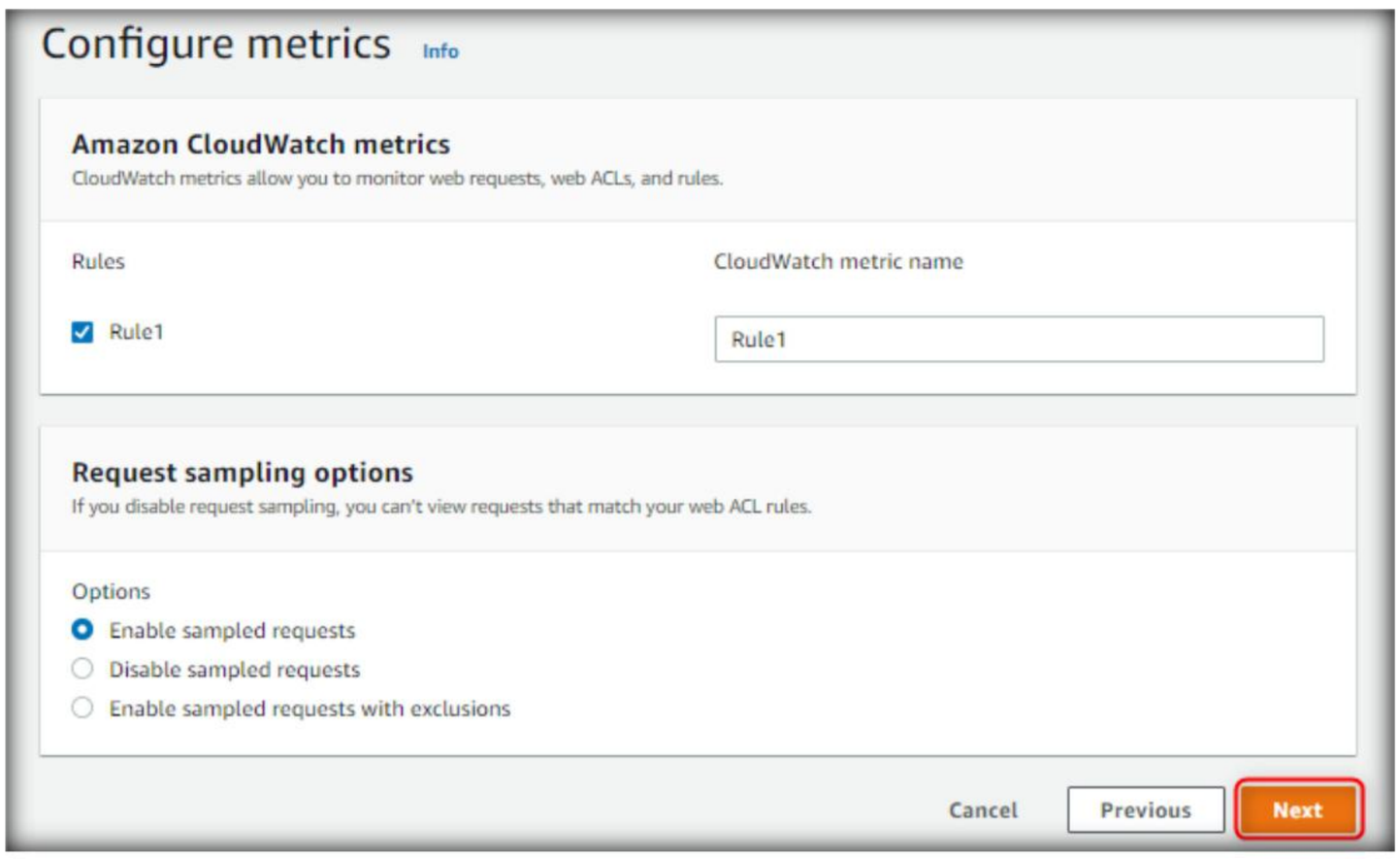


FIGURE 3.1.46: Proceeding with Configuration

Certified Cloud Security Engineer Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

50. Finally, scroll down and click the **Create web ACL** button in the review window.

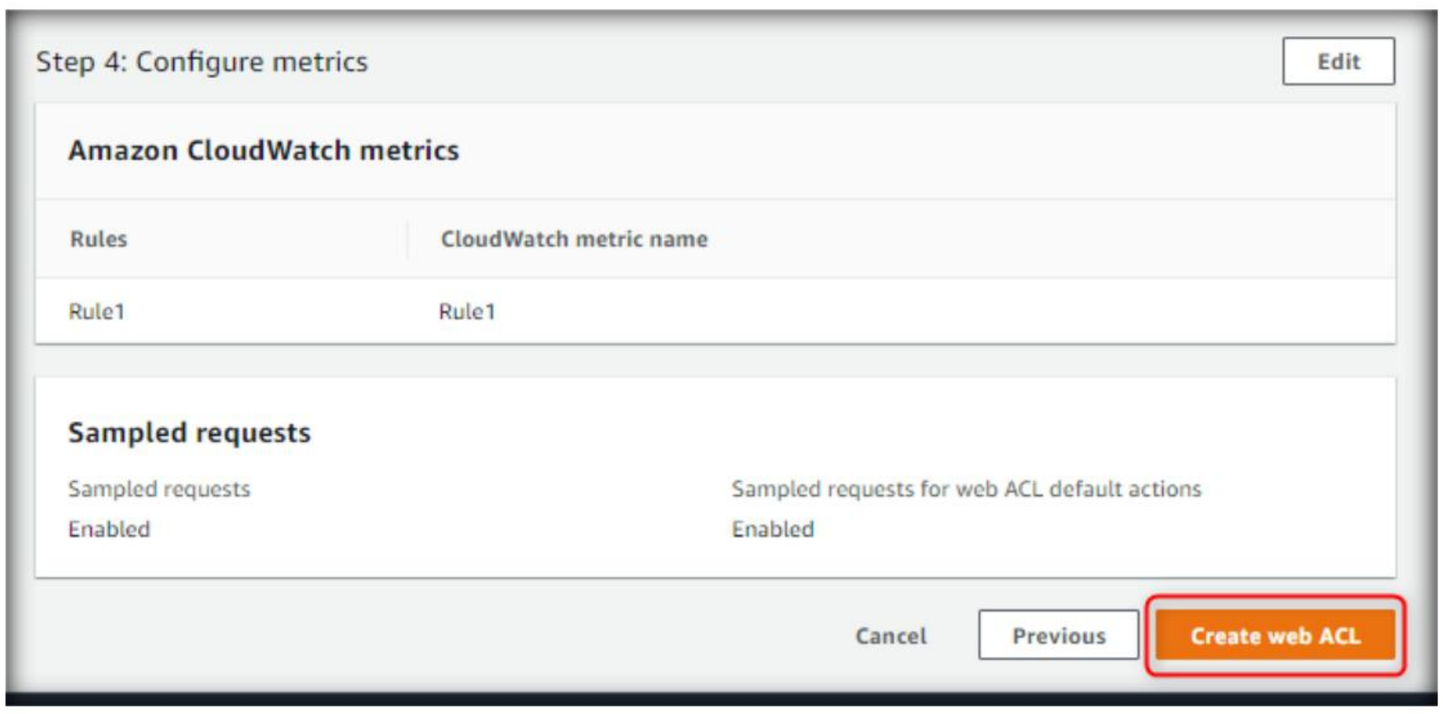
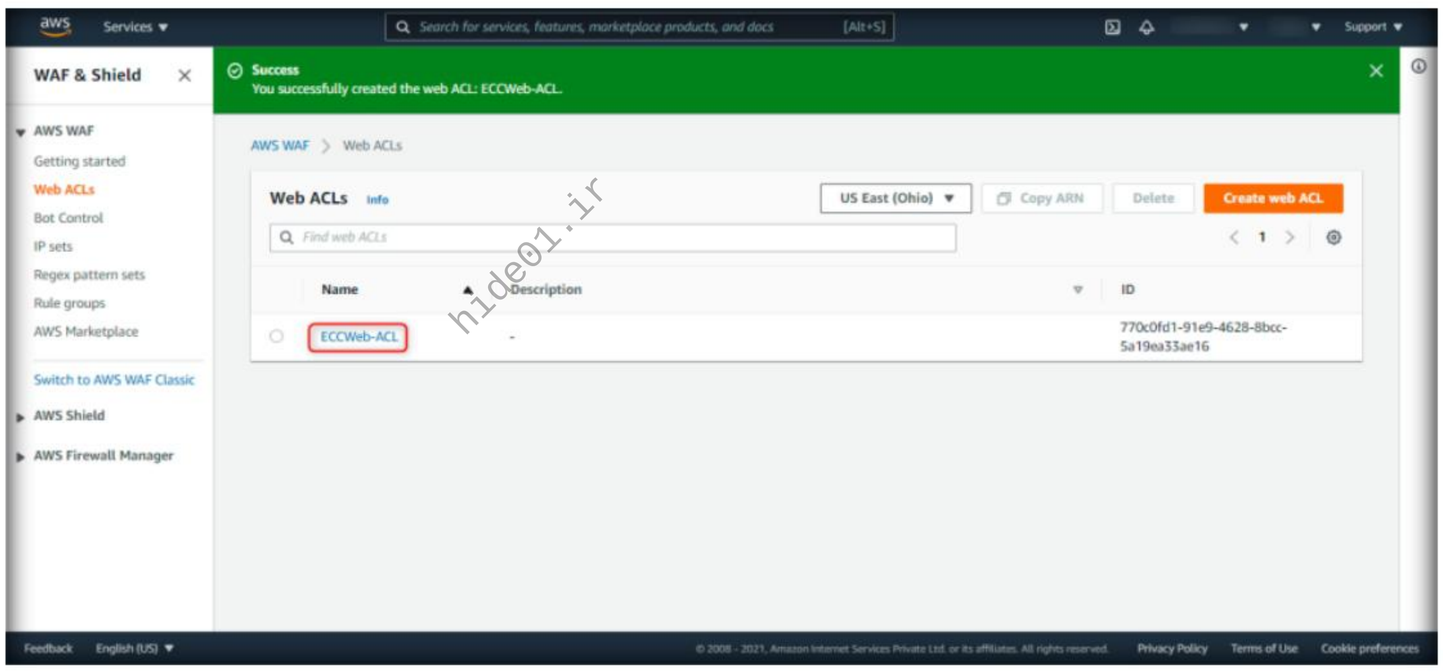


FIGURE 3.1.47: Finish Creating Web ACL

51. Web ACL will be created after a minute or so. Once it is created, you will see a **You successfully created the web ACL: ECCWeb-ACL** message, as seen in the following screenshot.



hide01.ir

FIGURE 3.1.48: Web ACL Created Successfully

TASK 4

Test the configured Web ACL

52. Open a new browser tab and paste the **Invoke URL** you had copied into notepad. Then, press **Enter**. Now, you will see a **Forbidden** message because access is blocked for your machine.

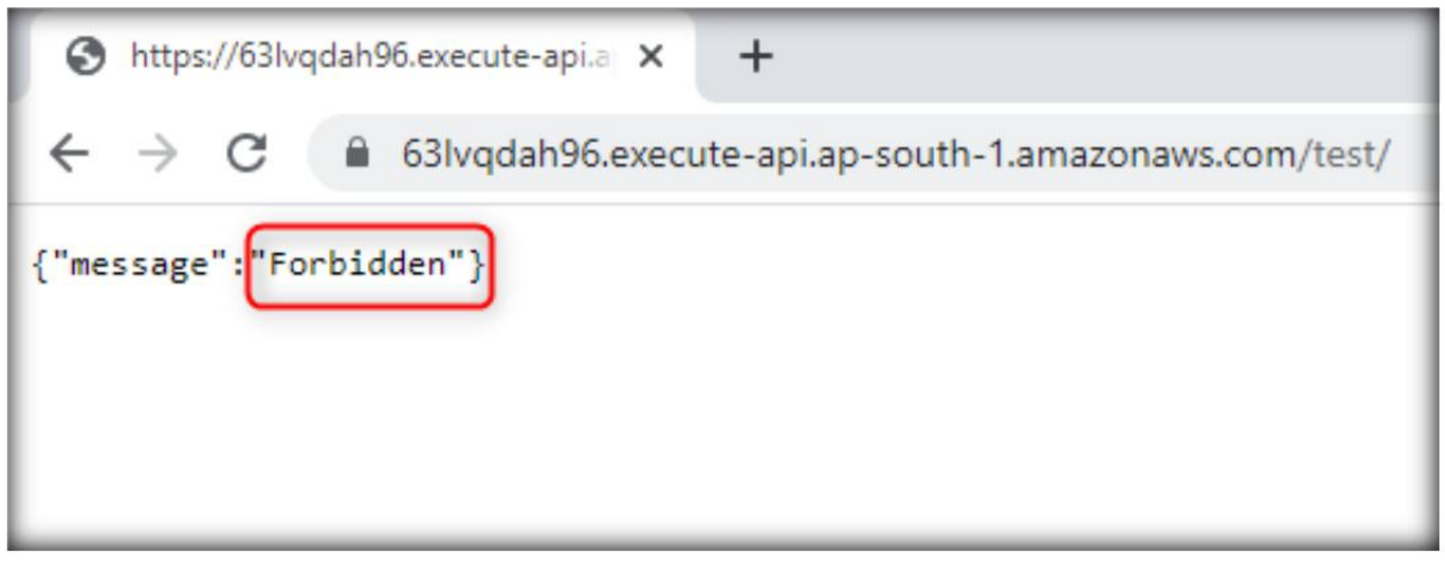


FIGURE 3.1.49: Access gets blocked

Certified Cloud Security Engineer Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

53. This way, a cloud security engineer can use **AWS WAF** to protect the web applications.

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

54. Now, delete the instances created in this lab. Navigate to the **API Gateway** console and select the checkbox of the API created in this lab. Select the **Actions** dropdown and click on **Delete**. In the pop-up window, enter delete and click on the **Delete** button.

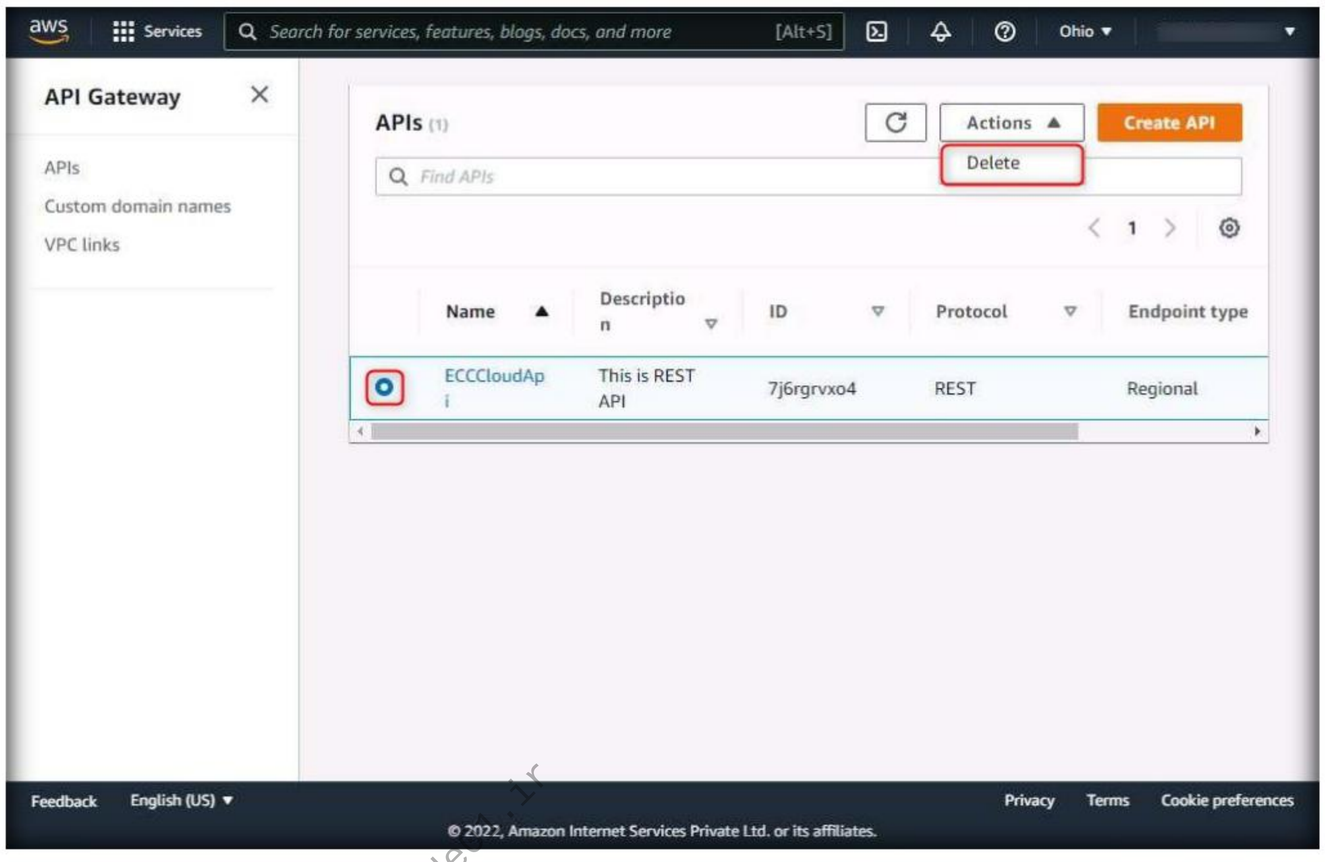


FIGURE 3.1.50: Deleting API Gateway

55. Navigate to **Web ACLs** under AWS Firewall manager and select the check for instance created in this lab (here, **ECCWeb-ACL**). Click on the **Delete** button. In the pop-up window, enter delete and click on the **Delete** button.

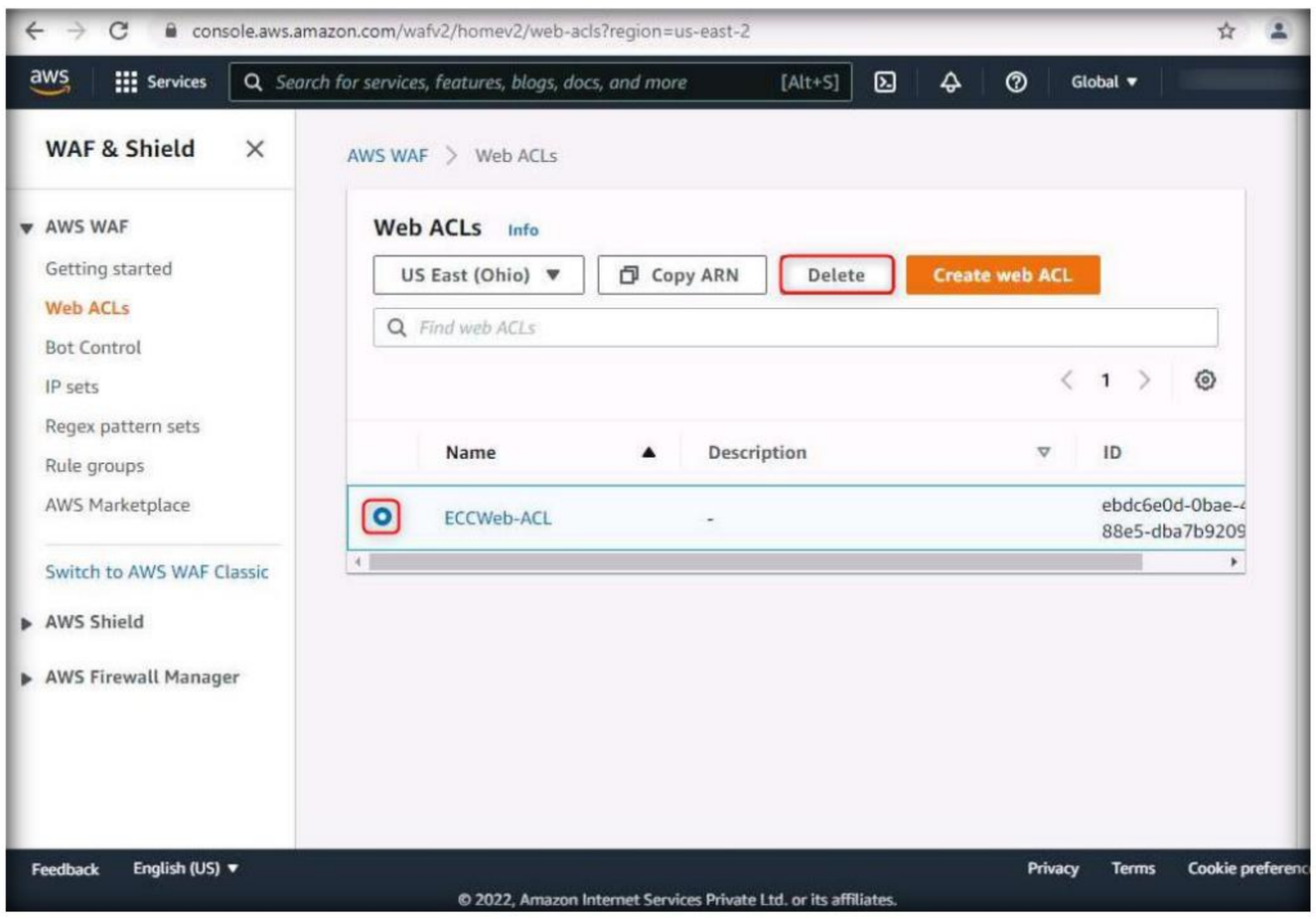


FIGURE 3.1.51: Deleting Web ACL

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

56. Navigate to the **IP sets** under the AWS Firewall Manager console and select the checkbox of the instance created in this lab (here, **blacklistips**). Click on the **Delete** button. In the pop-up window, enter delete and click on the **Delete** button.

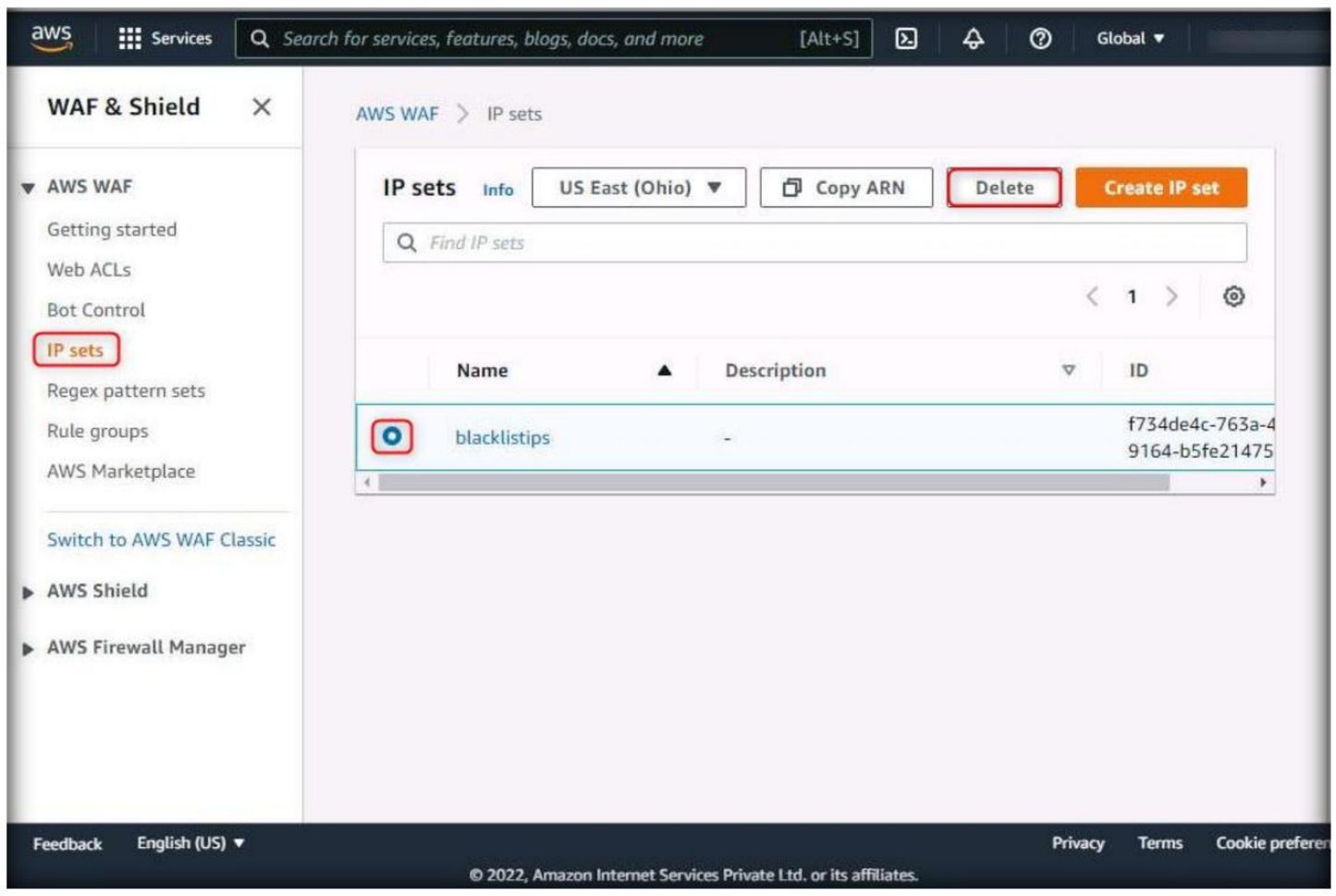


FIGURE 3.1.52: Deleting IP sets

Lab Analysis

hide01.ir

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.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 2

Enforcing Principle of Least Privilege with SAML-based Single Sign-on in Azure

Security assertion markup language (SAML)-based single sign-on in Azure allows users to utilize the same credentials to sign-in and access the limited resources with limited permissions on-premises and in Azure cloud. It helps a cloud security engineer enforce the principle of least privilege to users.

ICON KEY

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

Lab Scenario

hide01.ir

SAML-based single sign-on in Azure for enterprise applications allows a cloud security engineer to enforce the principle of least privilege. It provides security and convenience to users, allows them to utilize the same credentials to sign-in and access the limited resources with limited permissions in Azure cloud and on-premises, and allows them to access SaaS applications based on an organization account in Azure Active Directory (AD).

Lab Objectives

In this lab, you will learn how to create a new user in Azure AD, how to add enterprise application in Azure AD, how to set single sign-on (SSO) with SAML, how to set up AWS SSO, how to add a user to Azure AWS SSO, how to assign a user and create a new permission set, and finally, how to check a new permission set in Azure management console.

In this lab, you will:

- Create a new user in Azure AD
- Add AWS SSOin Azure
- Set up single sign-on with SAML
- Configure AWS SSO
- Enable automatic provisioning in AWS SSO

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Add a user to Azure AWS SSO
- Assign a user and create a new permission set
- Configure AWS account with the new user and permission set
- Perform operations using the new permission set in AWS management console

Lab Environment

To perform this lab, you need the following:

- Admin Machine VM
- Registered AWS account.
- Registered Microsoft Azure account

Lab Duration

Time: 25 minutes

Overview of Azure SAML-based Single Sign-on

Single sign-on refers to accessing multiple applications and resources by signing in only once with a single user account. In Microsoft Azure AD, a seamless single sign-on automatically signs in corporate desktop users connected to a corporate network. The cloud applications can utilize various single sign-on methods, such as OpenID Connect, OAuth, SAML, password-based, etc. SAML-based single sign-on is useful for cloud-based and on-premises applications. Select SAML-based single sign-on for applications that do not utilize OAuth or OpenID Connect. SAML single sign-on will work on applications that authenticate with one of the SAML protocols.

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: You need to have an active AWS account. Create an AWS account using the following URL: **https://portal.aws.amazon.com/billing/signup**. To register the account. you should create a Microsoft Azure account using the following URL: **https://azure.microsoft.com/en-in/free/**. Once you have created your Microsoft Azure account, 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.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1

Creating New User in Azure AD

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

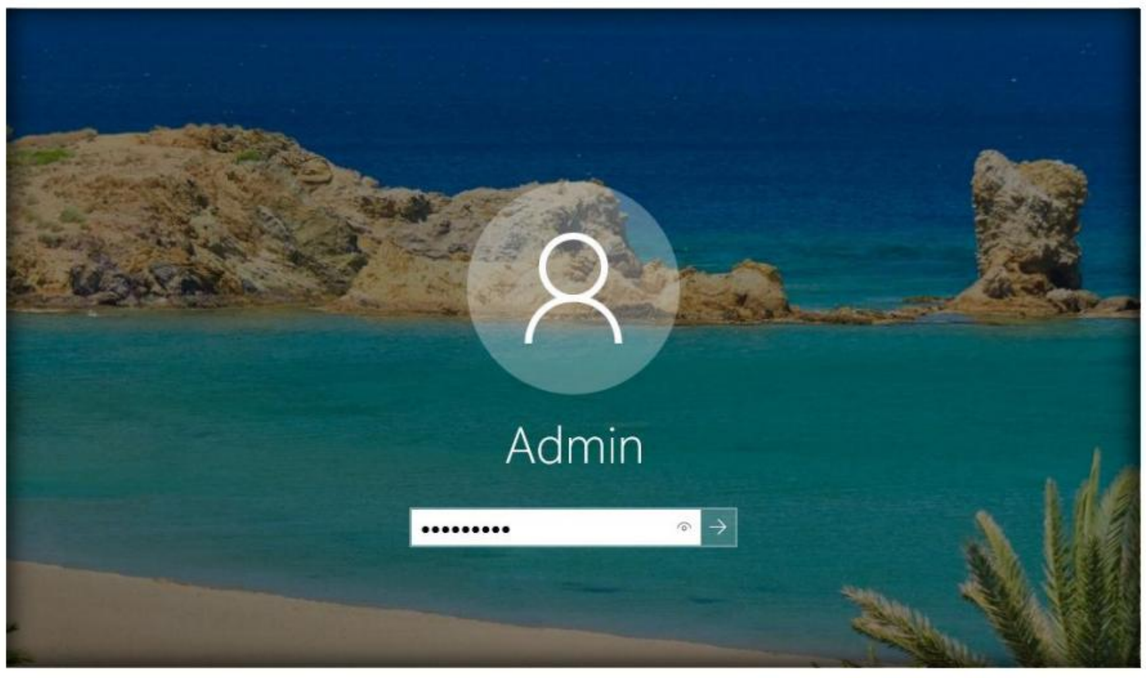


FIGURE 3.2.1: Launch Admin Machine and Log in

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



FIGURE 3.2.2: 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**.

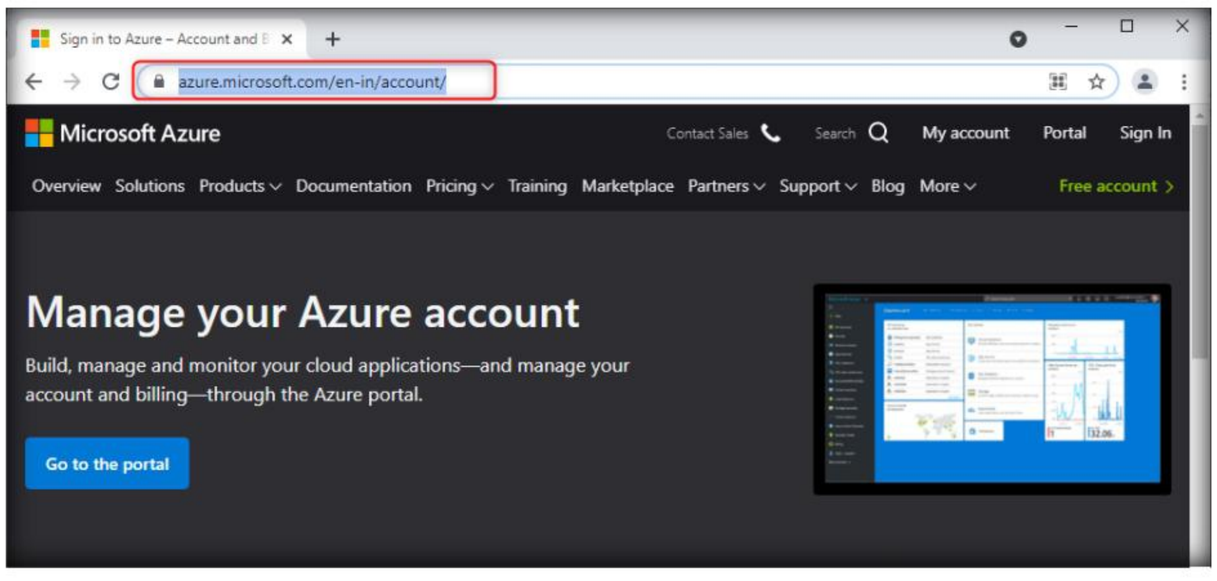


FIGURE 3.2.3: Entering the URL of Microsoft Azure

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

4. The **Microsoft Azure** page will appear. To login to Azure portal, click on **Portal** from the top right menu.

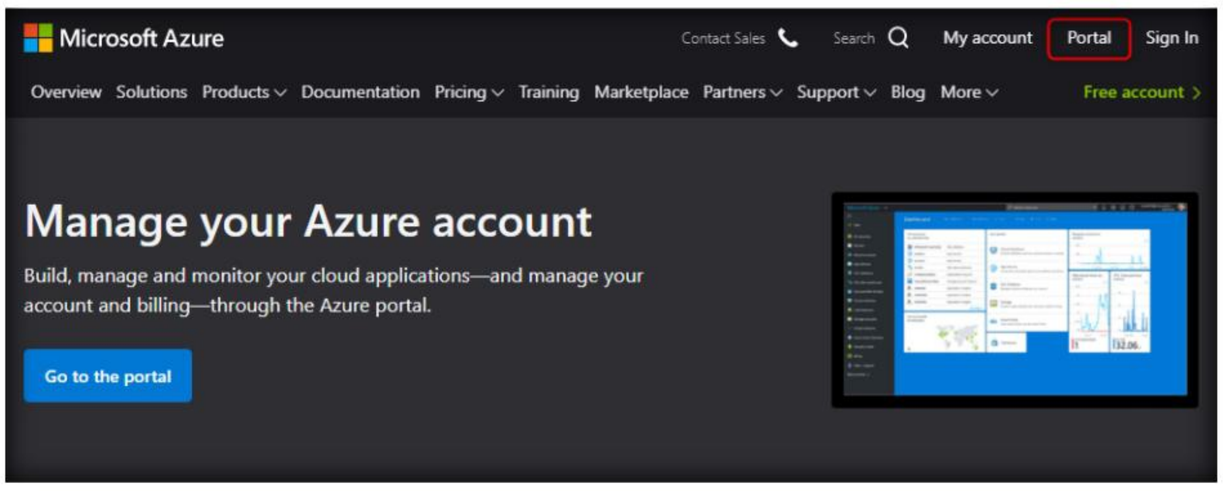


FIGURE 3.2.4: Sign into Azure Portal

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

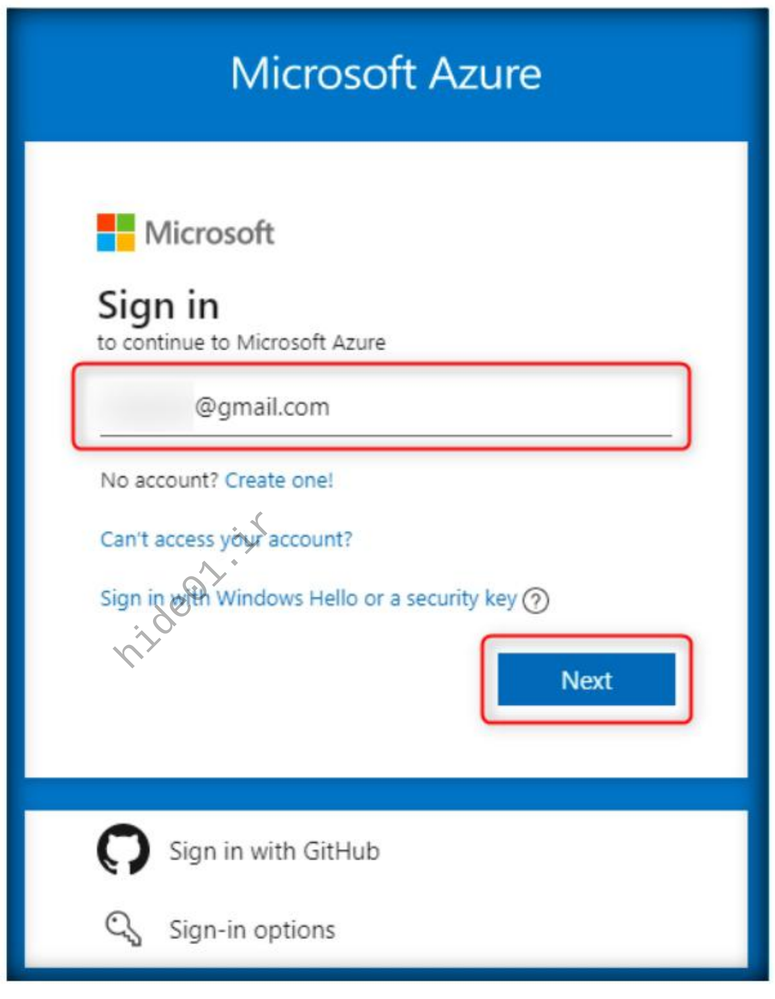


FIGURE 3.2.5: Entering Account ID to continue

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

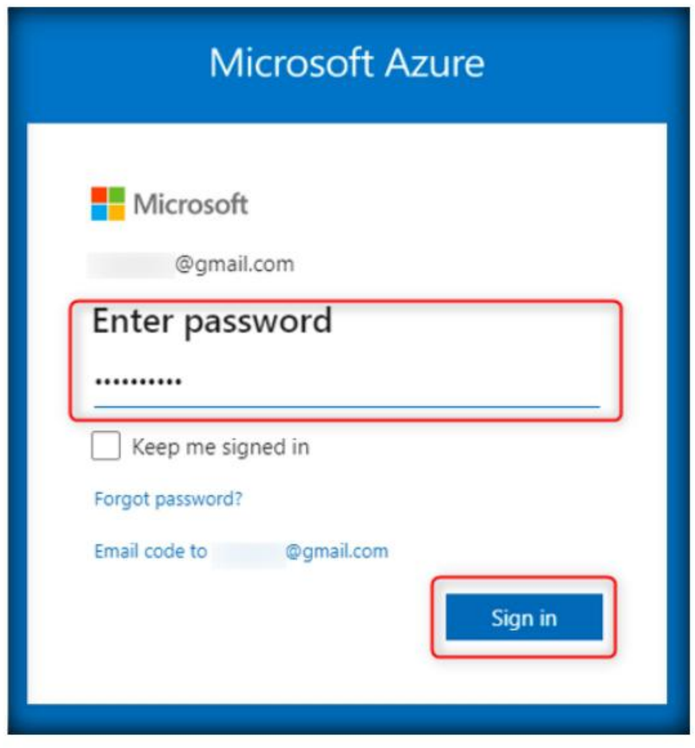


FIGURE 3.2.6: Entering the Log In Password

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

7. You will be successfully logged into **Microsoft Azure portal.**

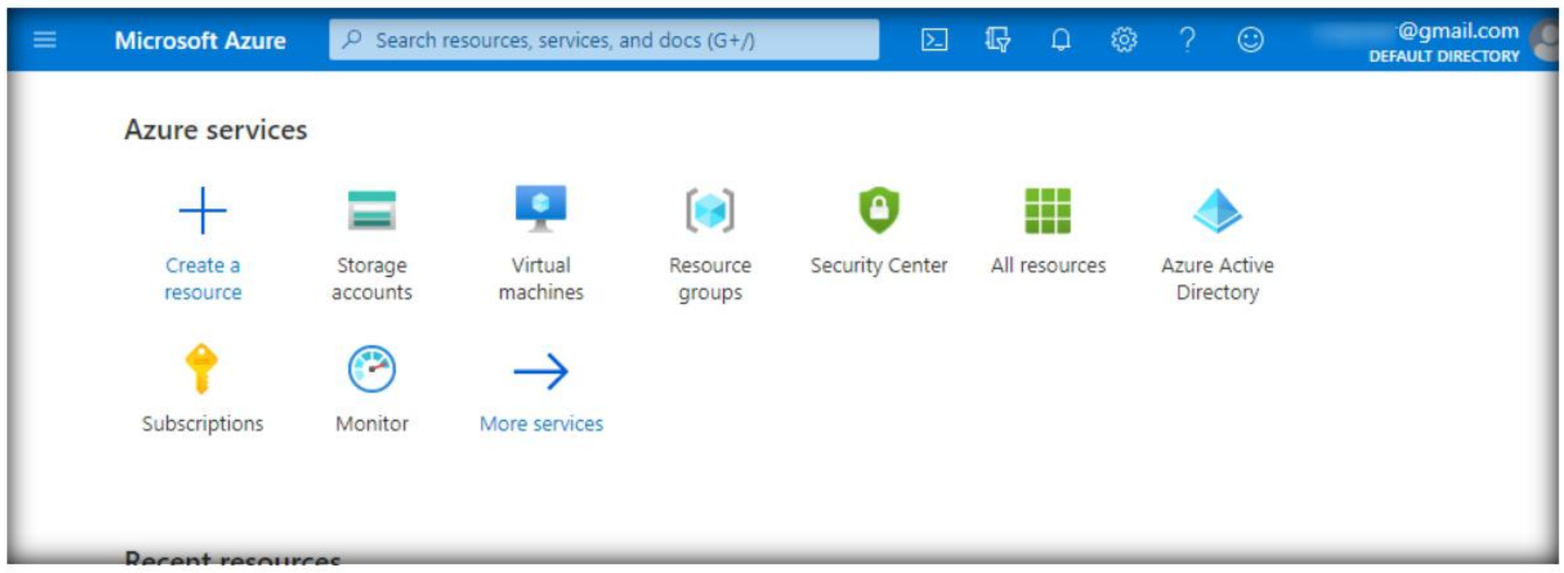


FIGURE 3.2.7: Microsoft Azure Portal

8. Click on the top left pane menu bar, and then navigate and click on **Azure Active Directory** to access the active directory in Azure.

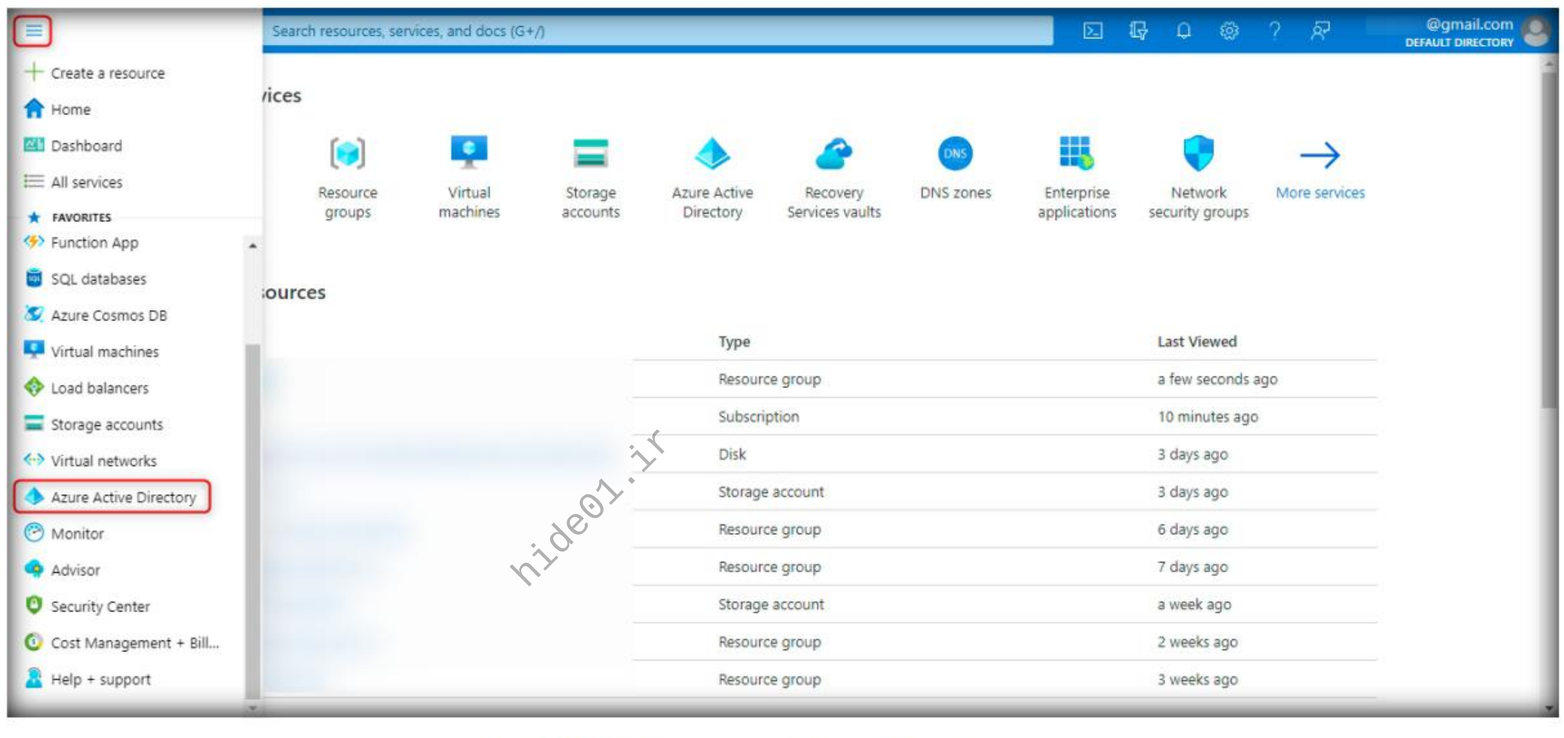


FIGURE 3.2.8: Selecting Azure Active Directory

9. To add a new AD user, click on **Users** under **Manage** in the **Default Directory** window to the left.

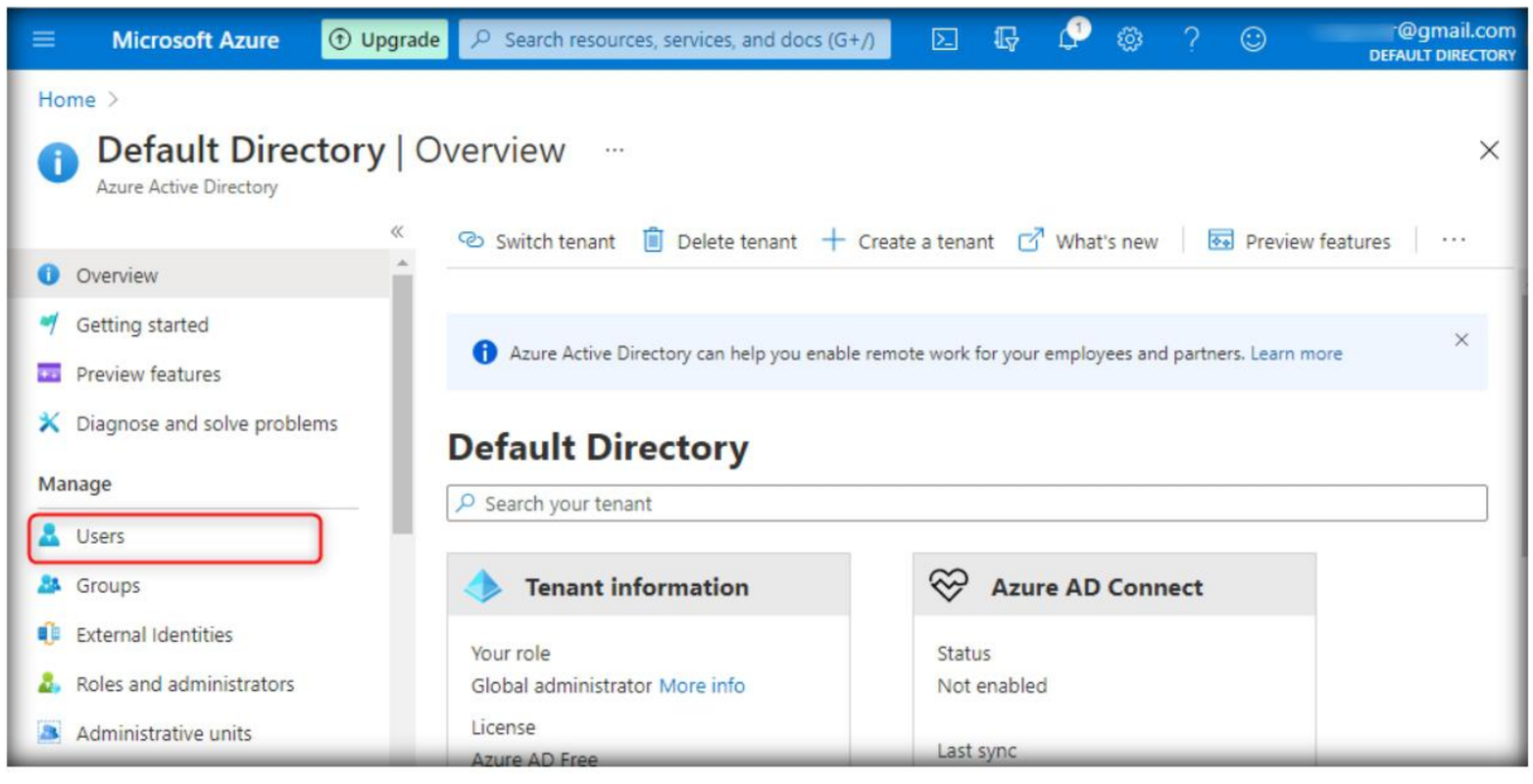


FIGURE 3.2.9: Selecting Users in Azure AD

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

10. Click on **New User**.

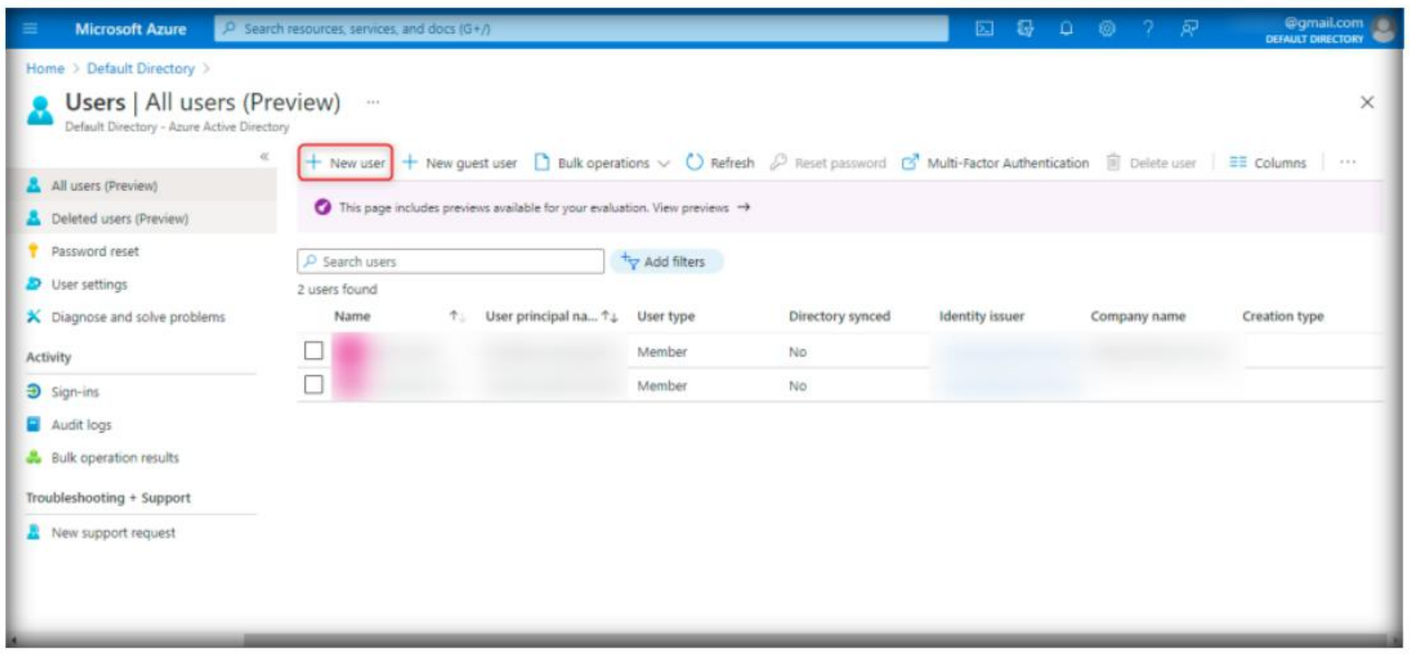


FIGURE 3.2.10: Creating New user

11. Select the **Create user** radio button.

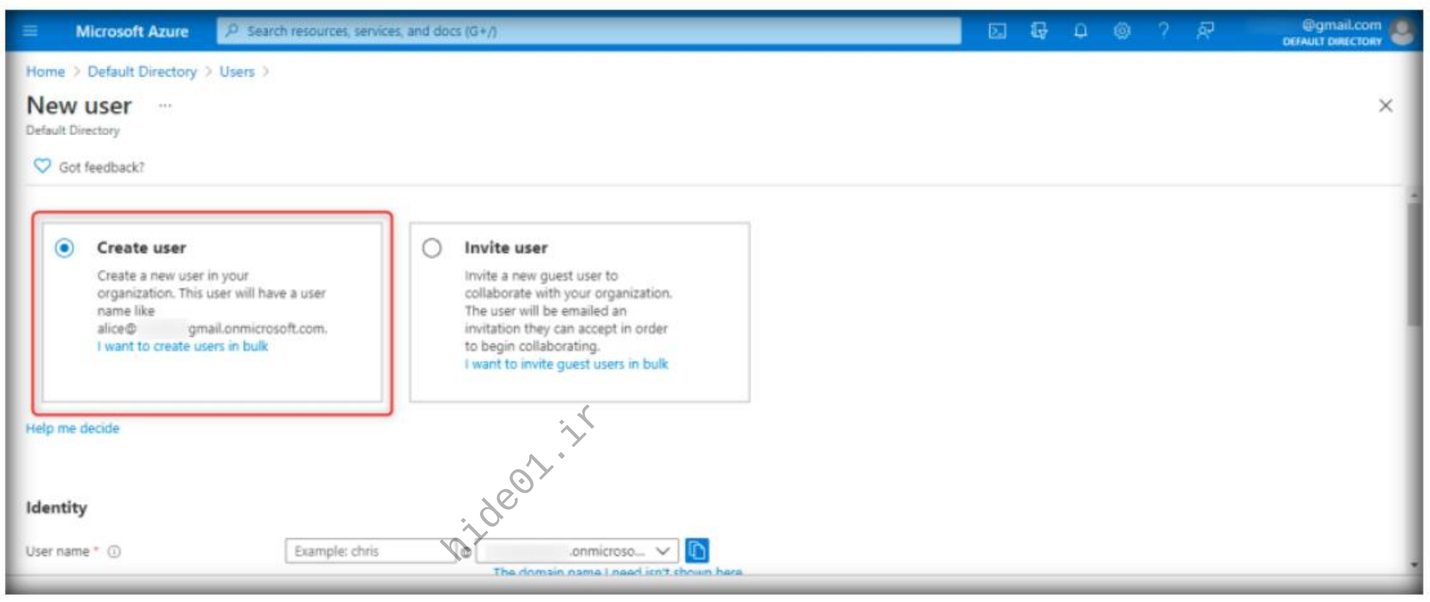


FIGURE 3.2.11: Selecting Create user Radio Button

12. Under **Identity**, enter the following details:

User name: Bob

Name: Bob Green

First name: Bob

Last name: Green

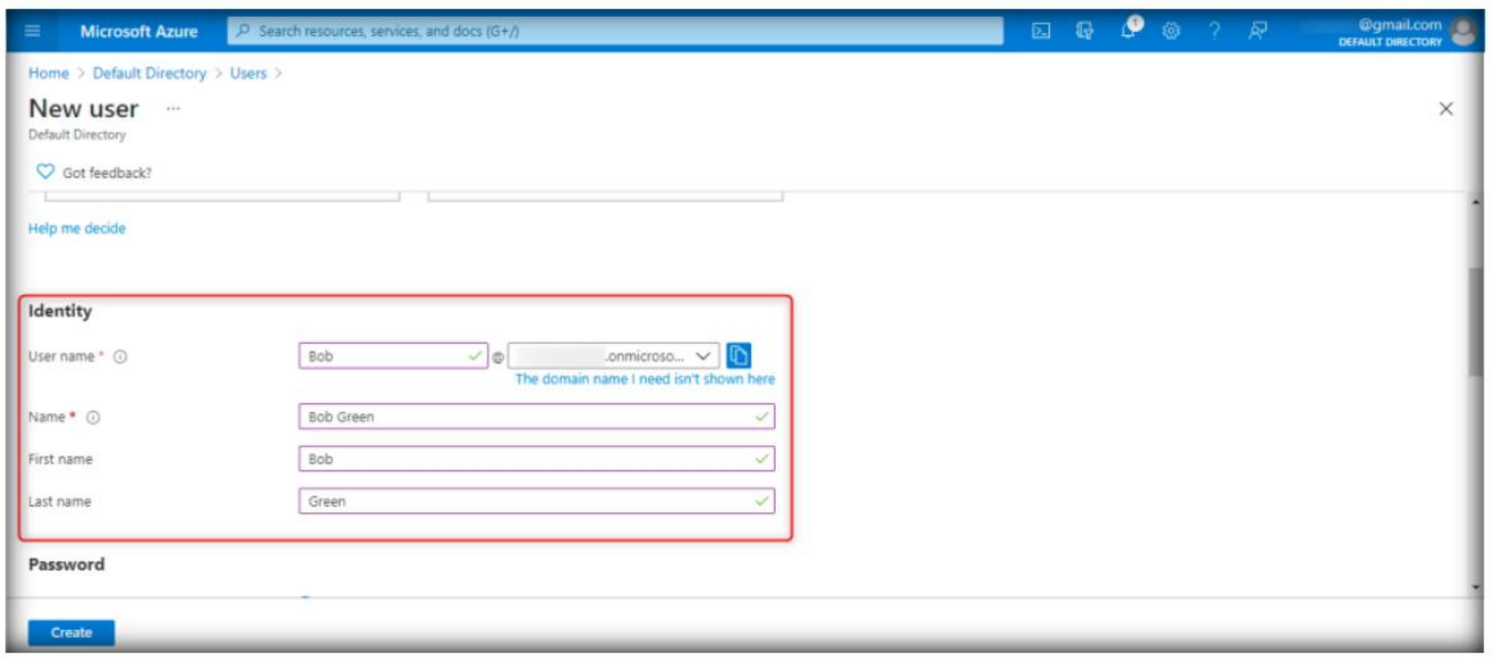


FIGURE 3.2.12: Entering User Details

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

13. In the **Password** section, check the **Let me create the password** radio button and enter **Administrator@789** as the **Initial password.**

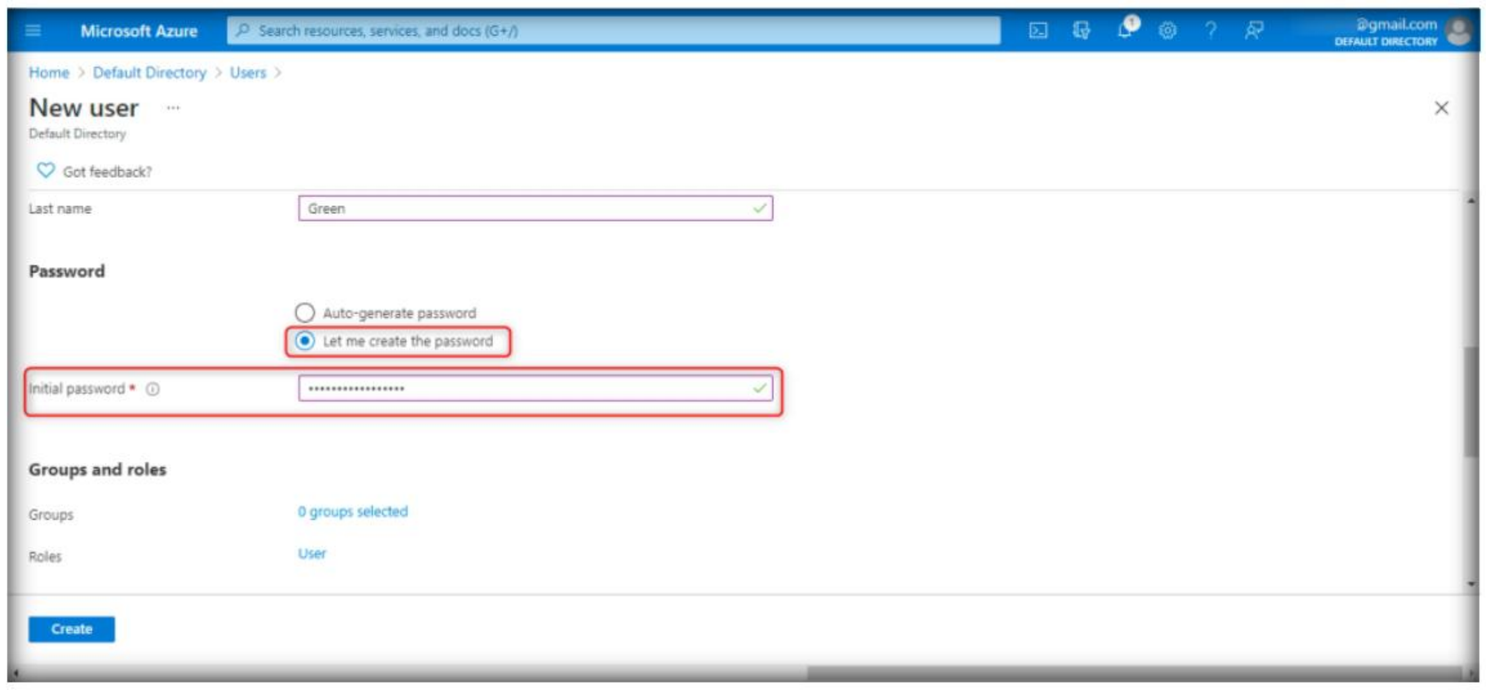


FIGURE 3.2.13: Entering a Password

14. Retain the default settings in the **Settings** section. In the **Job info** section, enter the following:

    Job title: Security Engineer

    Department: Cloud Information Security

    Company name: Global SecTech Pvt. Ltd.

    Then, click on the **Create** button.

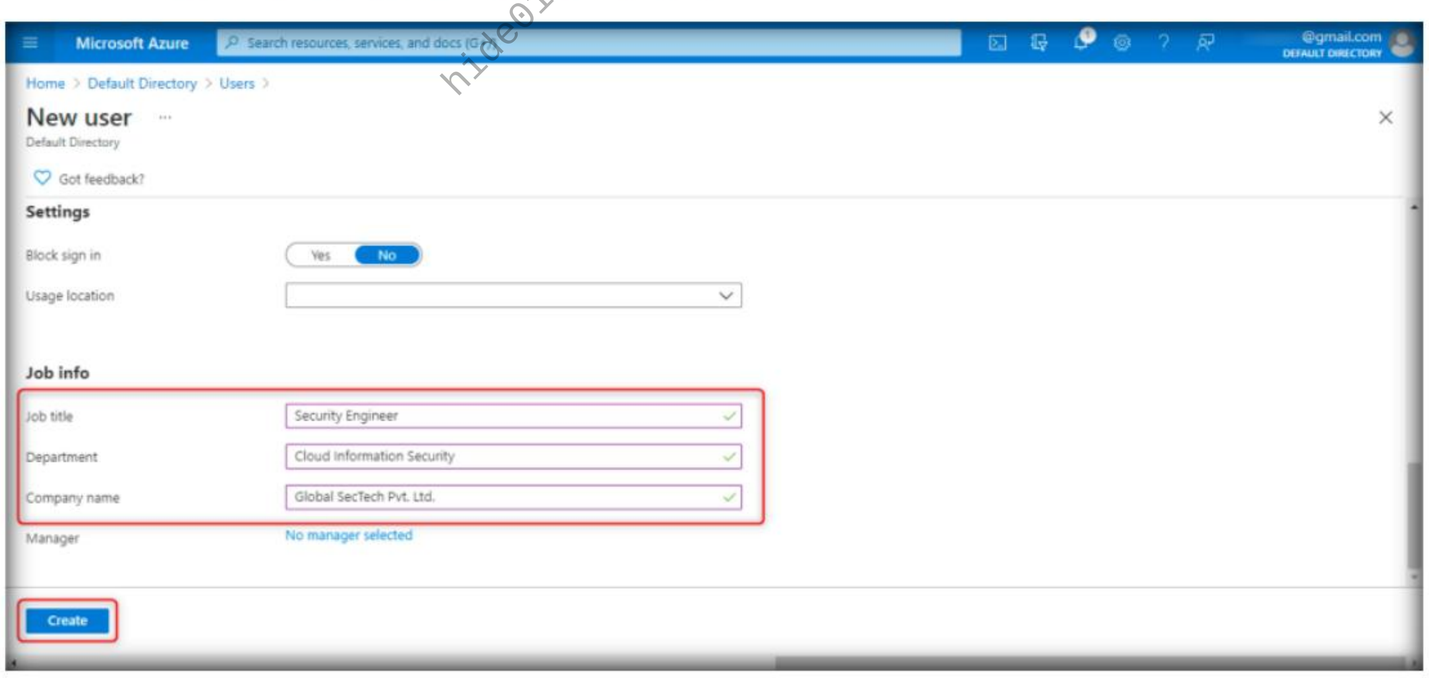


FIGURE 3.2.14: Entering Job Information of the User

15. A new user (**Bob Green**) is successfully created in Azure AD.

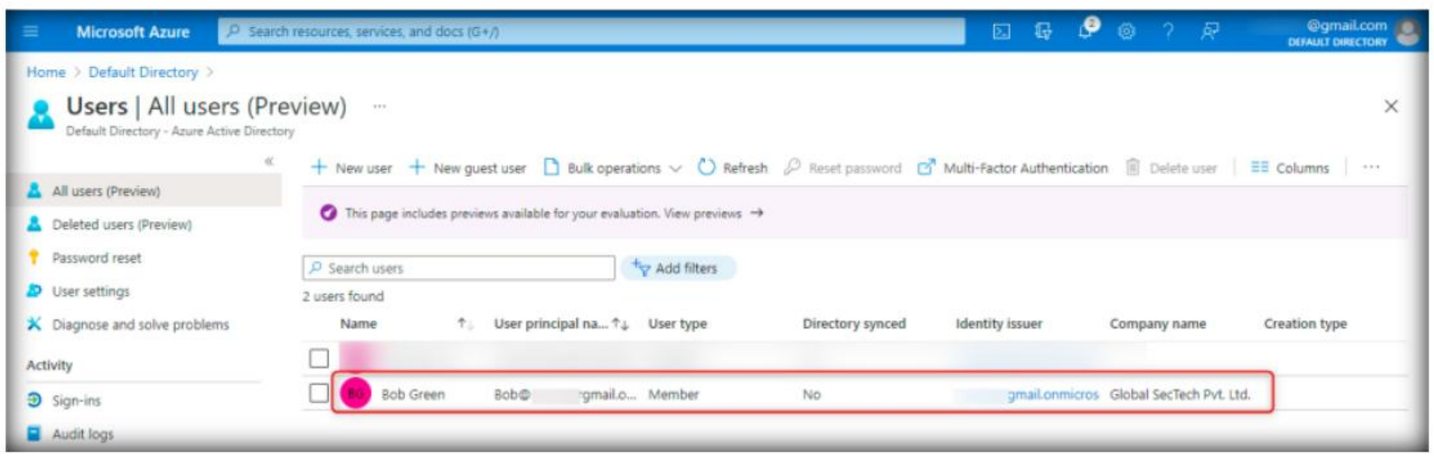


FIGURE 3.2.15: Successful Creation of New User

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 2

Adding AWS Single Sign-on Application in Azure

16. Click on **Home** at the top to go back to Azure portal.

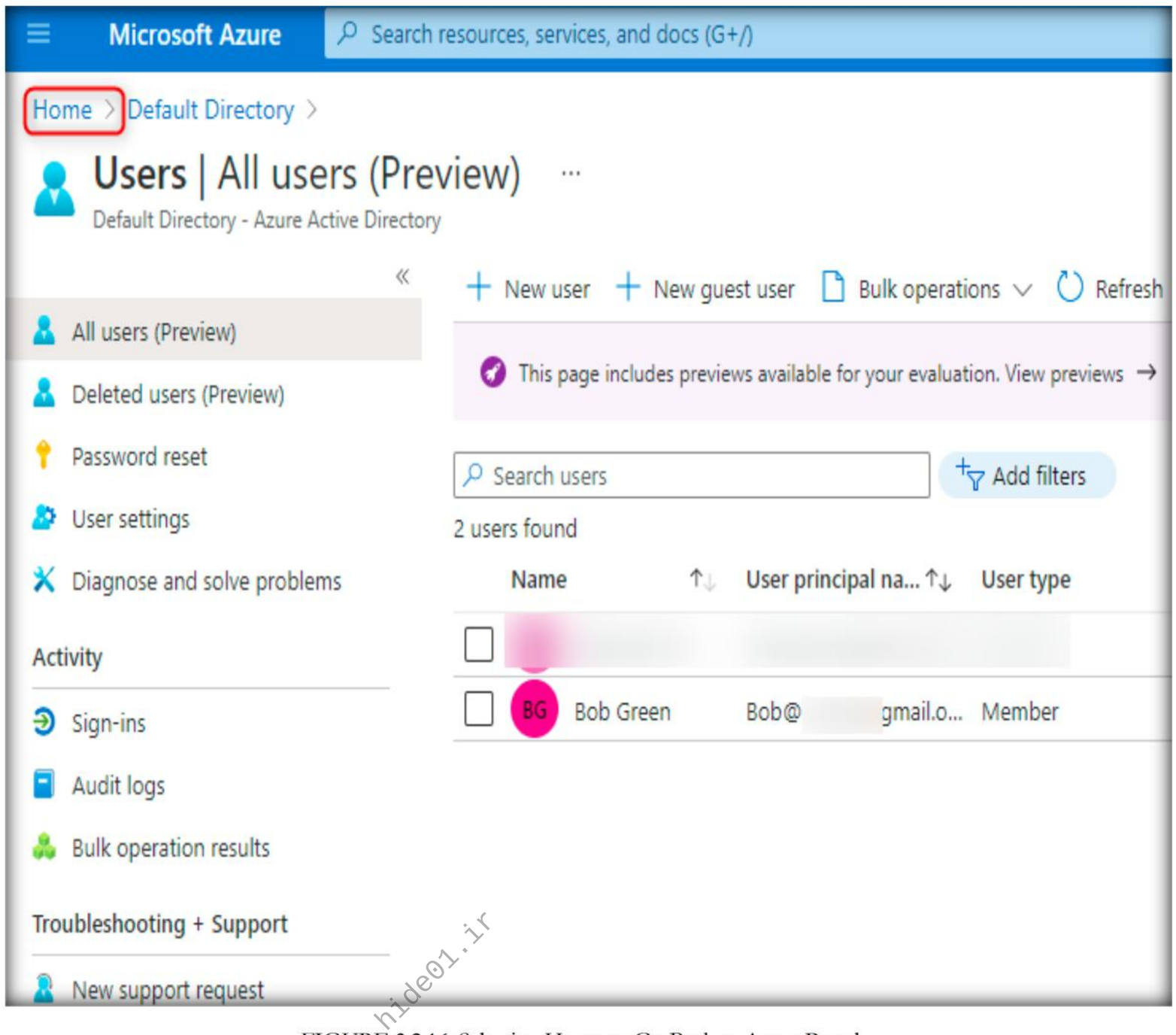


FIGURE 3.2.16: Selecting Home to Go Back to Azure Portal

17. Click on the Azure portal menu at the top left corner. Then, navigate and click on **Azure Active Directory**.

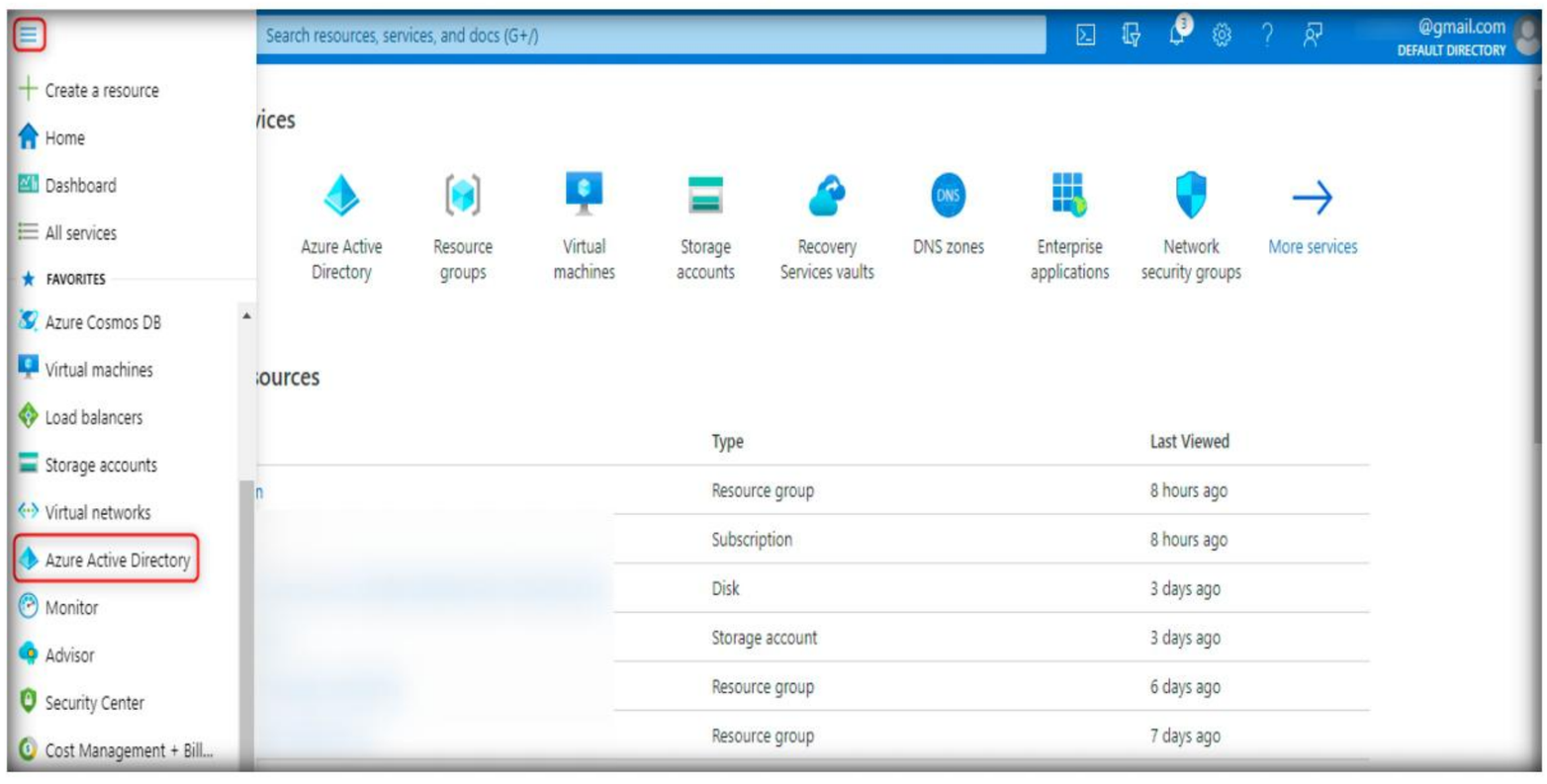


FIGURE 3.2.17: Selecting Azure Active Directory

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

18. In the **Default Directory** window, navigate and click on **Enterprise applications** under **Manage** in the left pane.

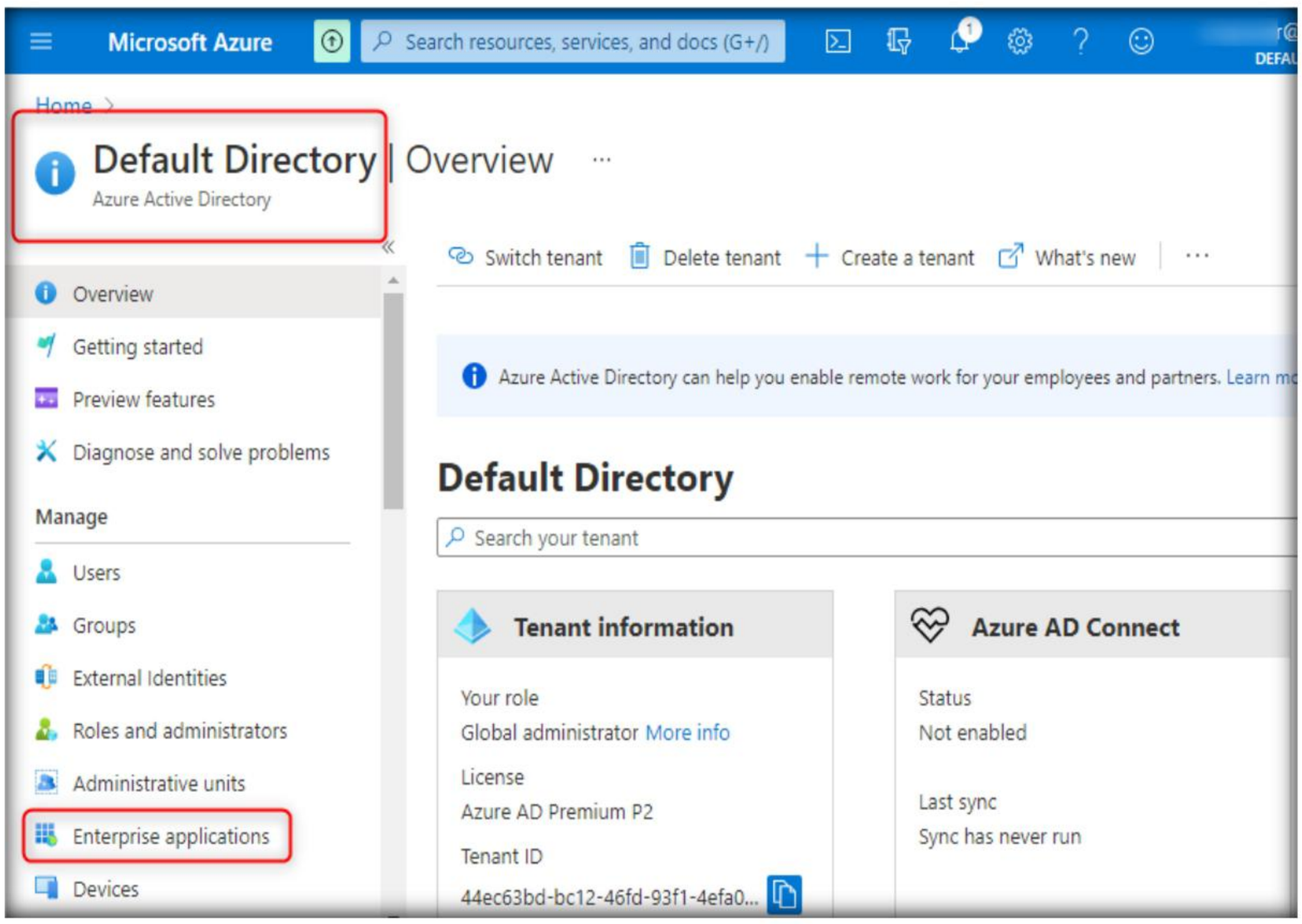


FIGURE 3.2.18: Selecting Enterprise Applications

19. Click on **+ New application** in the main page to create an application that supports SSO.

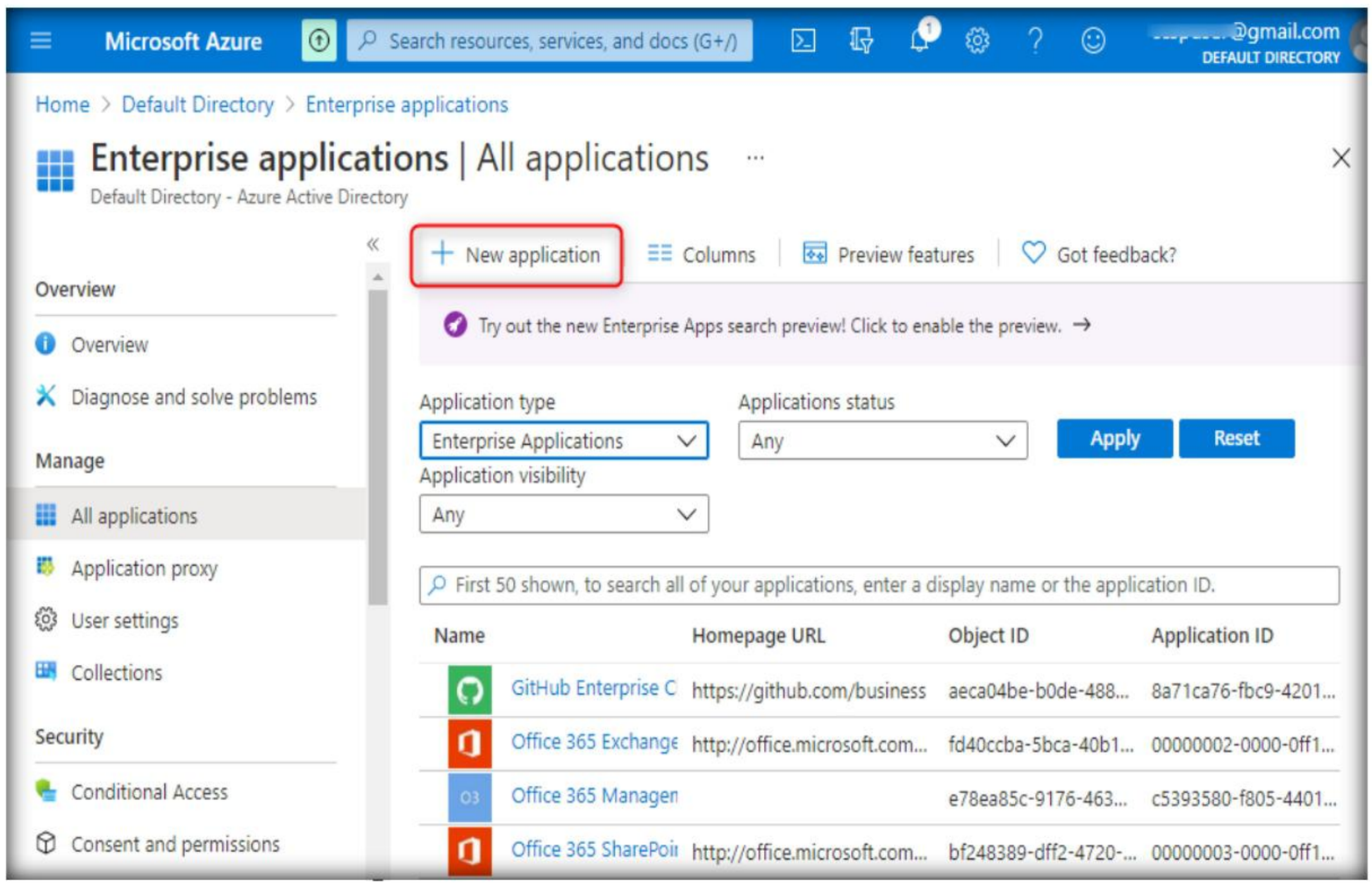


FIGURE 3.2.19: Selecting +New application

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

20. In the **Browse Azure AD Gallery** search box, type **AWS single sign-on**. Then, select **AWS Single Sign-on** from the displayed search results.

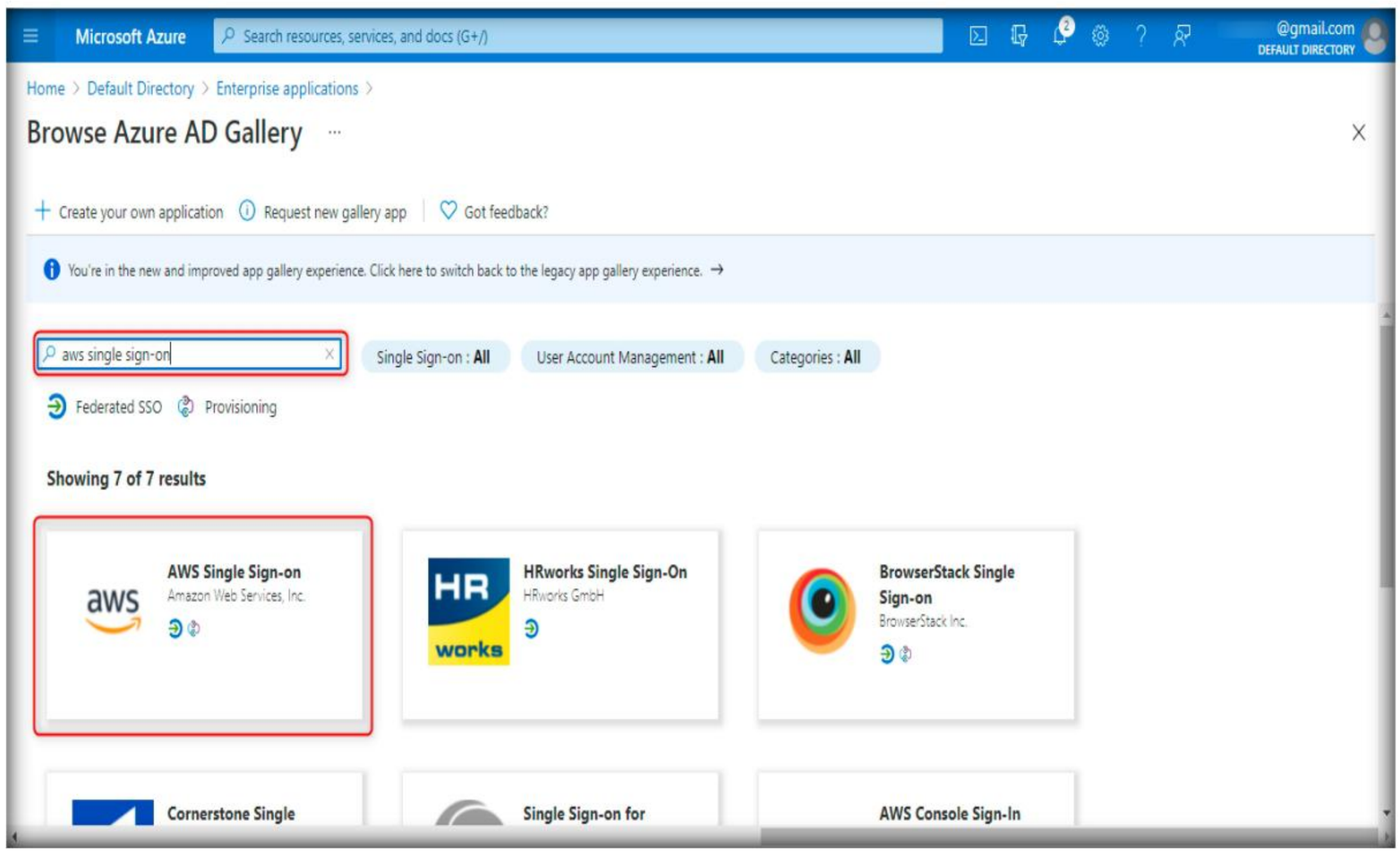


FIGURE 3.2.20: Selecting AWS Single Sign-on Application

21. **AWS Single Sign-on** will appear on the right pane. Now, click on the **Create** button at the bottom.

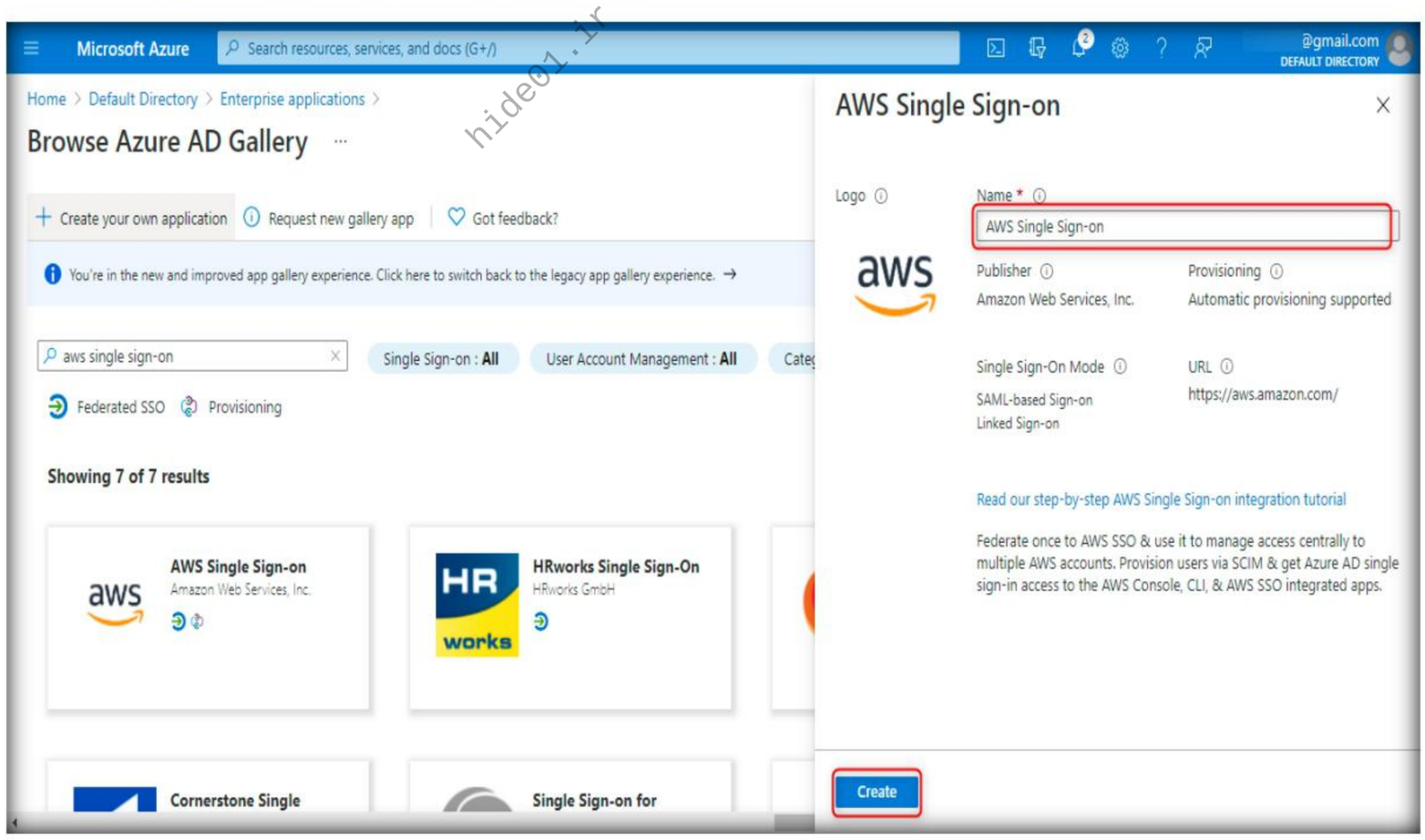


FIGURE 3.2.21: Adding AWS Single Sign-On Application

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

22. After a few seconds, **AWS Single Sign-on** will be successfully added.

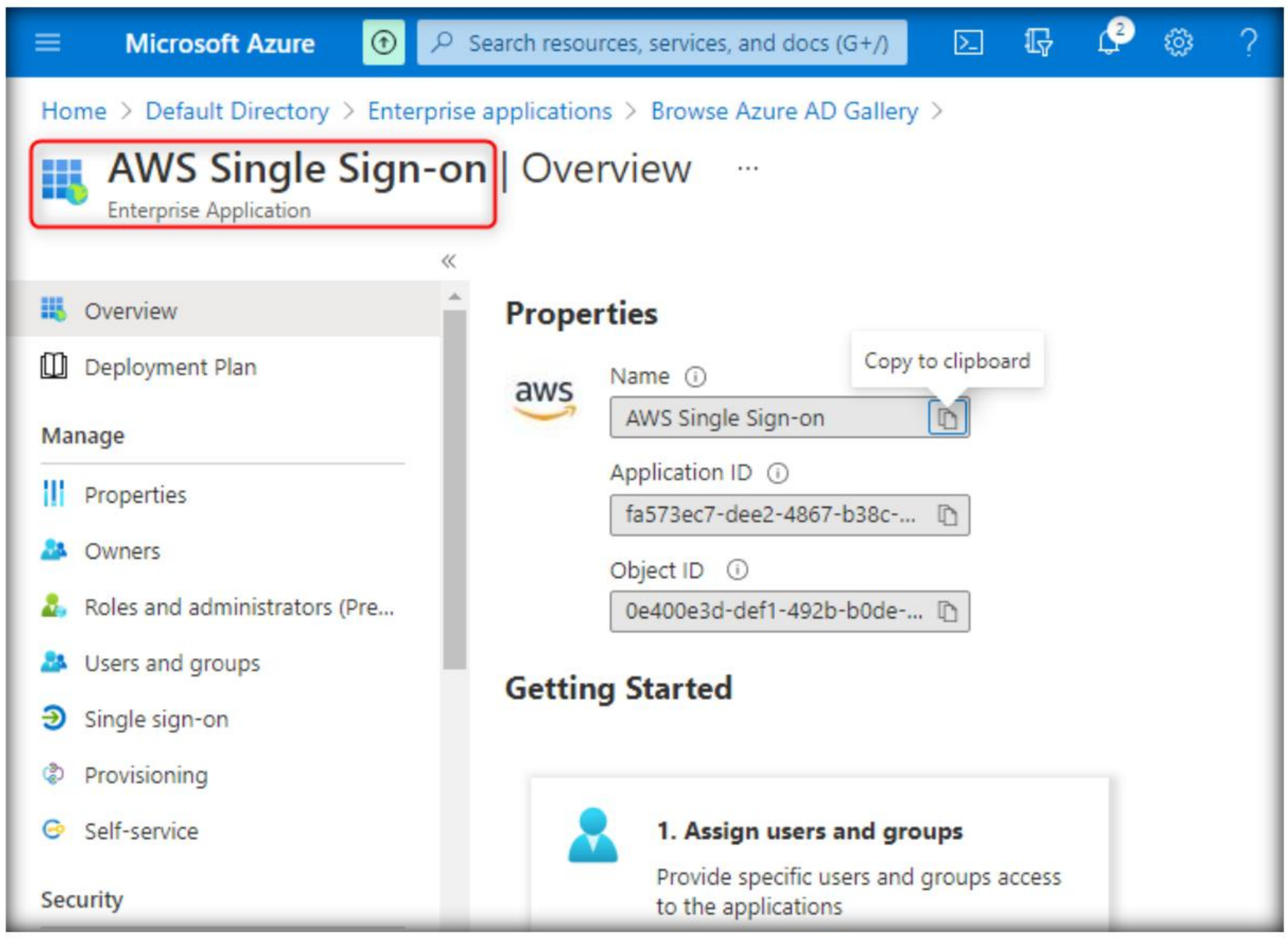


FIGURE 3.2.22: AWS Single-Sign On Successfully Added in Azure AD

TASK 3

Setting Up Single Sign-On with SAML

23. Navigate and click on **Single sign-on** under **Manage** in the left pane. Then, click on **SAML** under **Select a single sign-on method**.

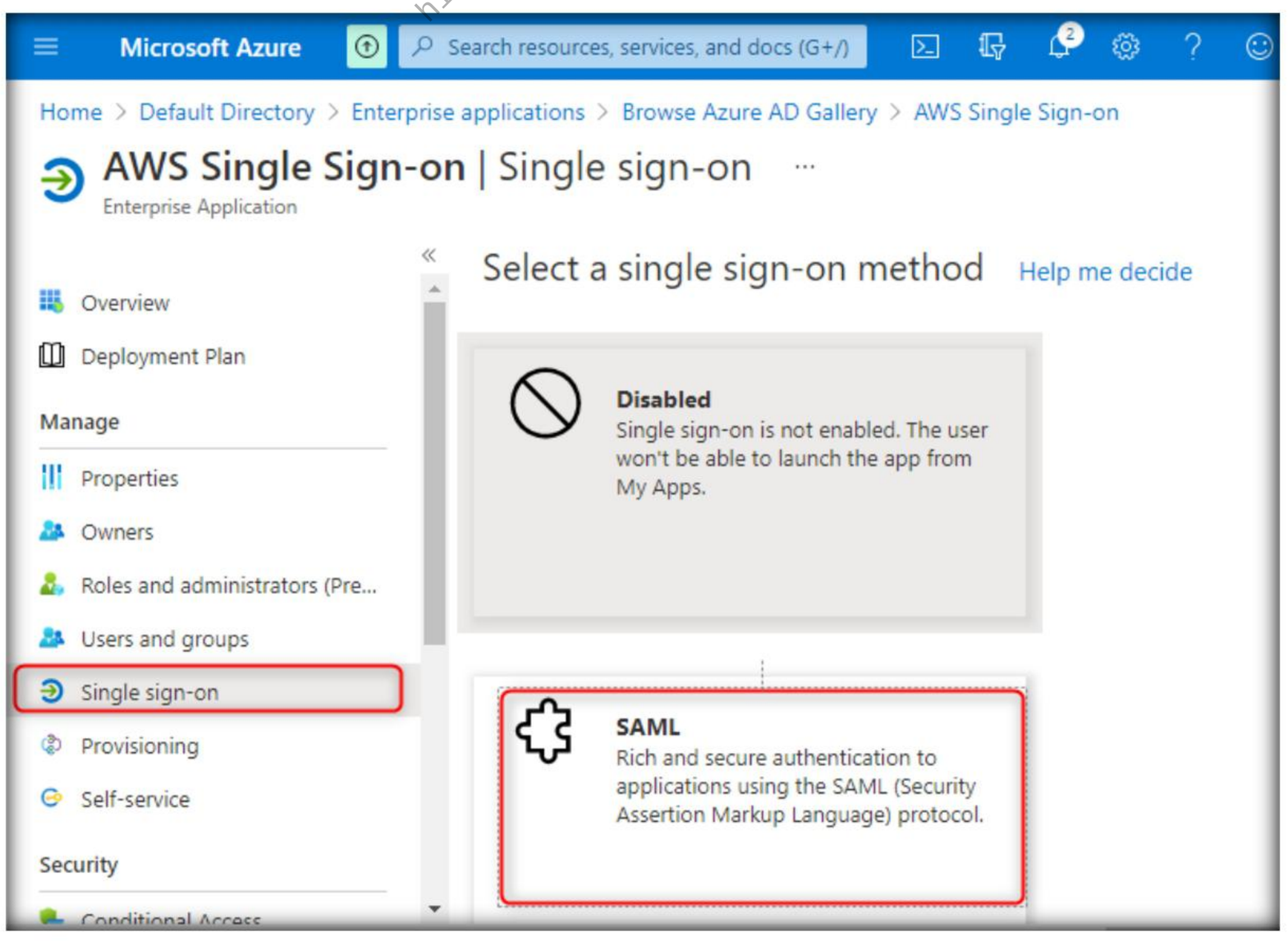


FIGURE 3.2.23: Selecting Single sign-on in AWS Single Sign-on Window

Certified Cloud Security Engineer Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

24. **SAML-based Single Sign-On** set up page will appear, as shown in the screenshot below. Here, **Required** will be seen beside **Identifier (Entity ID)**.

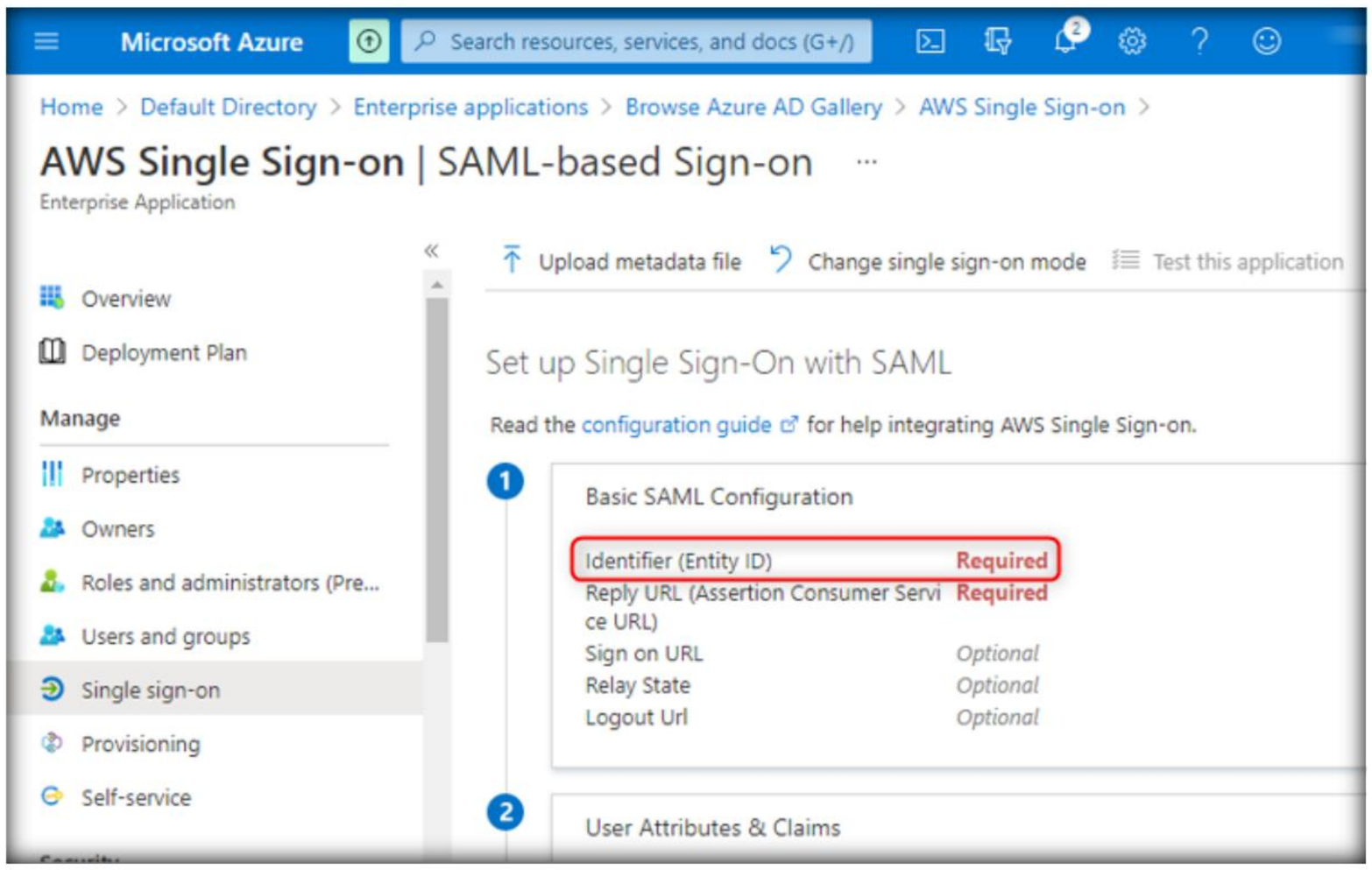


FIGURE 3.2.24: Setting Up Single Sign-On with SAML Window

25. Now, to configure the identity source, open a new tab in the Google Chrome browser, enter the following link: **https://aws.amazon.com/**, and press **Enter**.

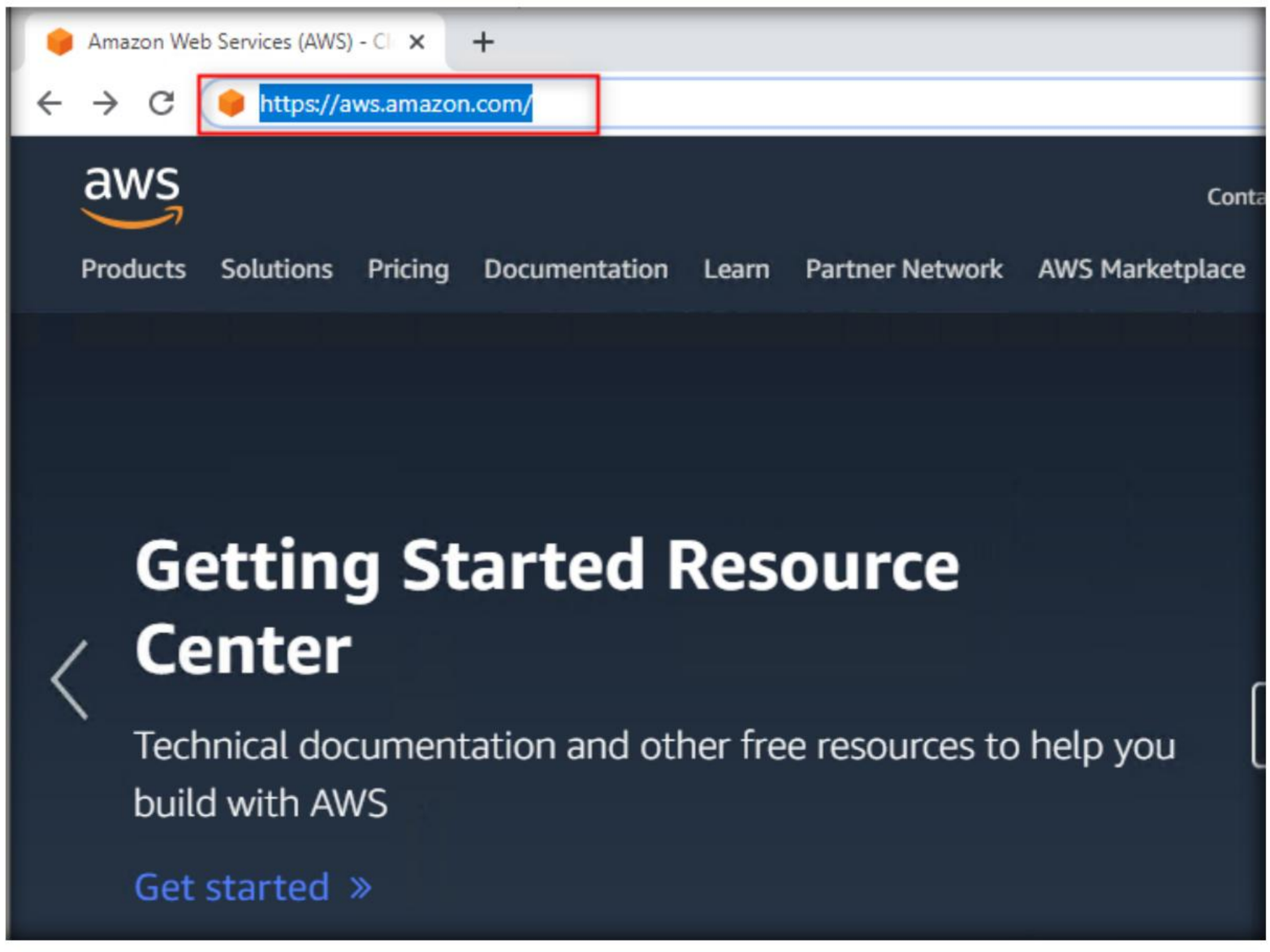
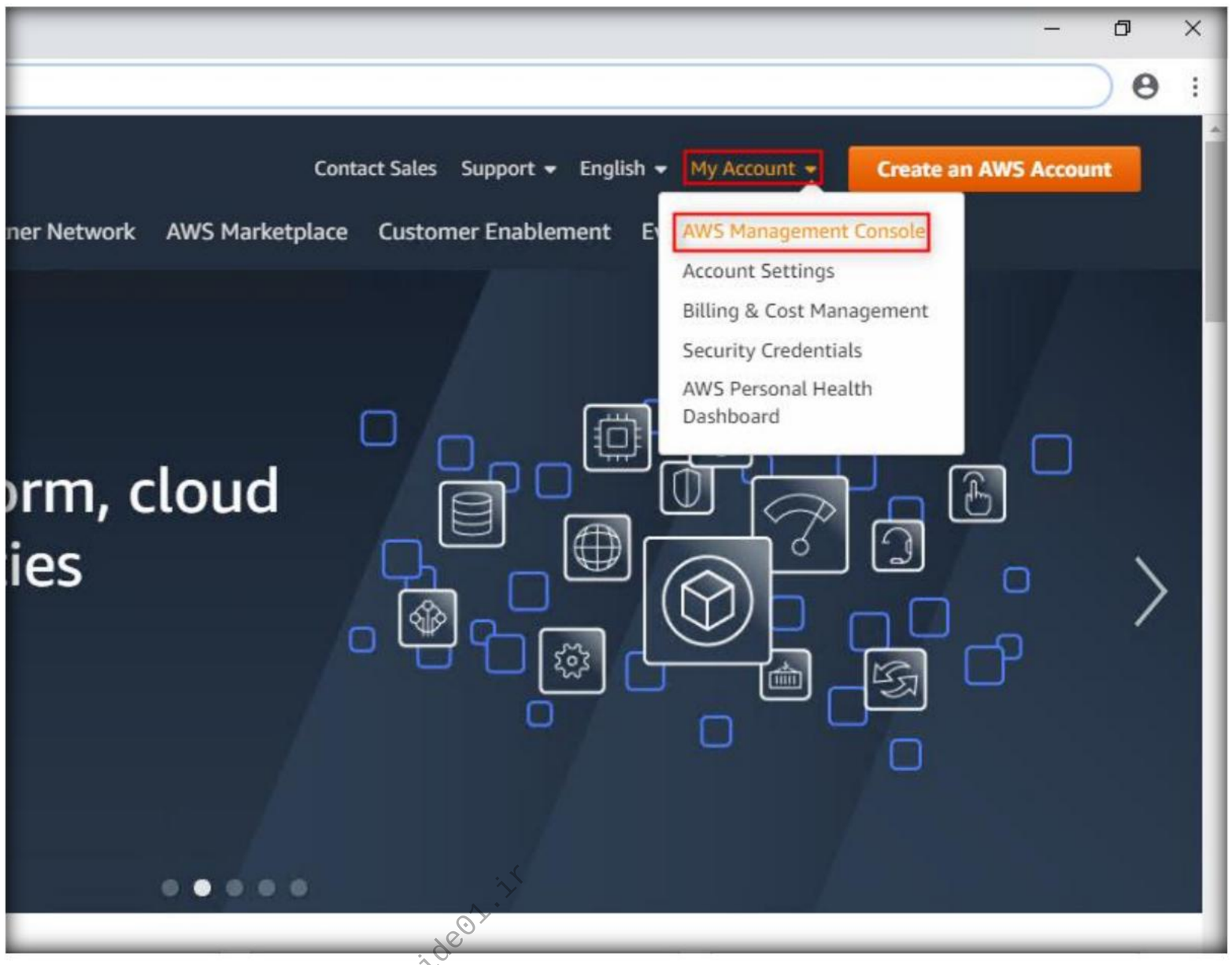


FIGURE 3.2.25: Searching Amazon Management Console in Google

Certified Cloud Security Engineer Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

26. The **AWS Web Services - Cloud Computing Services** page appears. Click on **AWS Management Console** from the **My Account** dropdown, as shown in the screenshot below.



hide01.ir

FIGURE 3.2.26: Opening AWS Management Console

27. Select the **Root user** radio button and enter your AWS login email ID in **Root user email address**. Then, click on **Next**.

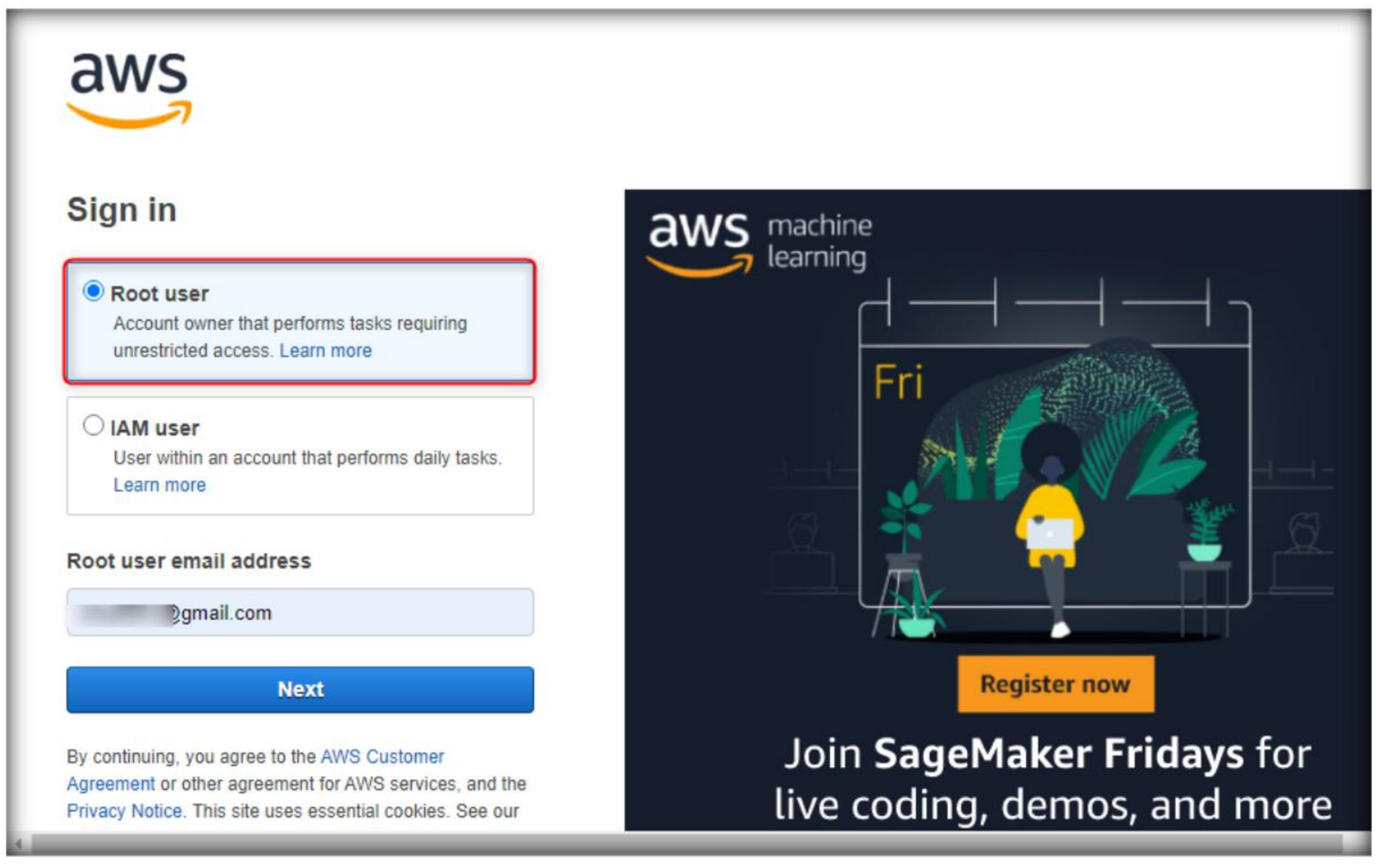


FIGURE 3.2.27: Signing into AWS Using Root User Email Address

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

28. In the **Security check** window, enter the characters shown in your image, and then click on **Submit**.



FIGURE 3.2.28: Entering Captcha

29. In the **Root user sign in** window, enter the AWS Root user log in **Password** and click on **Sign in**.

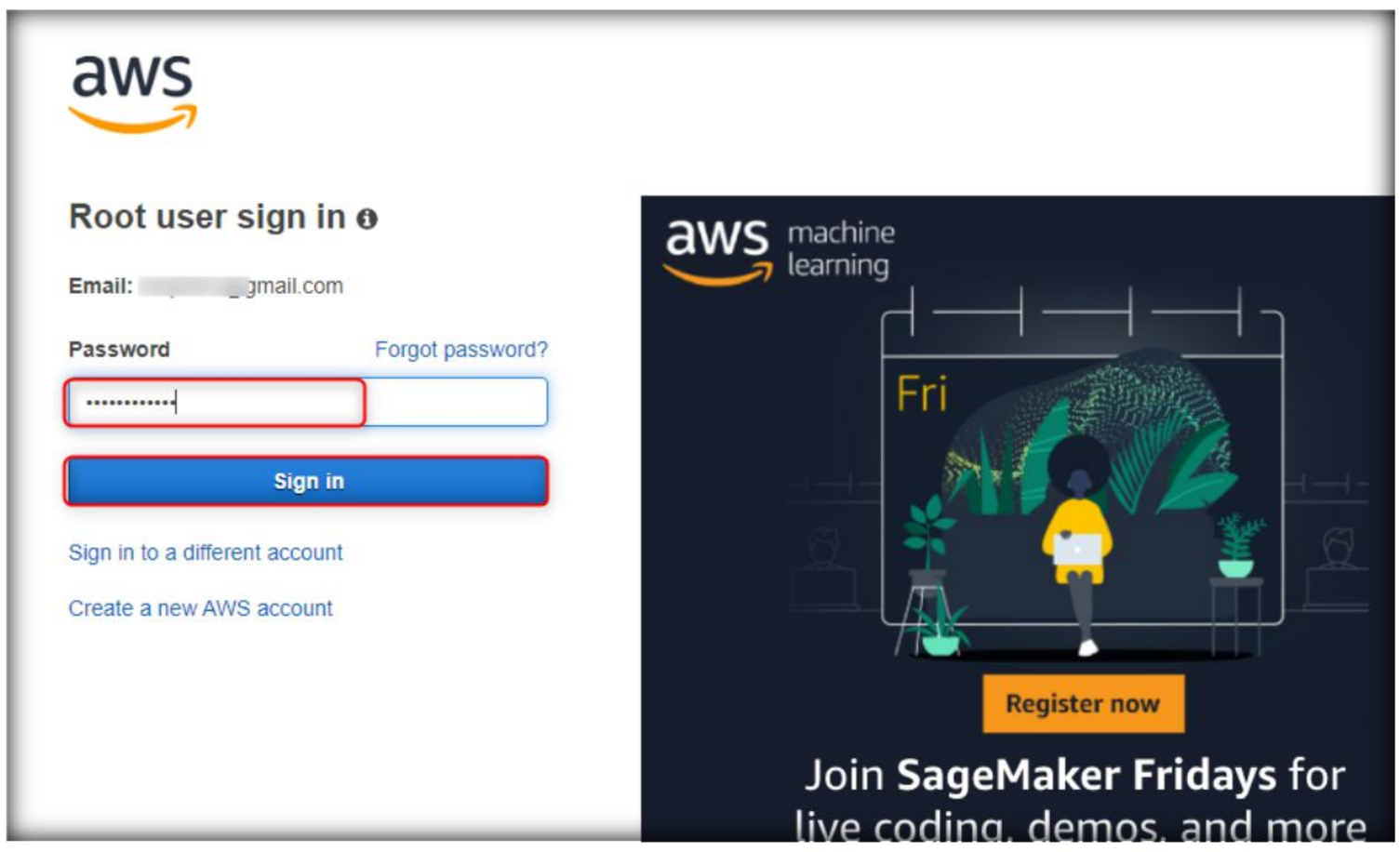


FIGURE 3.2.29: Root User Sign In

Certified Cloud Security Engineer Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

30. In the AWS search box, type **AWS Single Sign-On**, and then navigate and click on **AWS Single Sign-On** under **Services**.

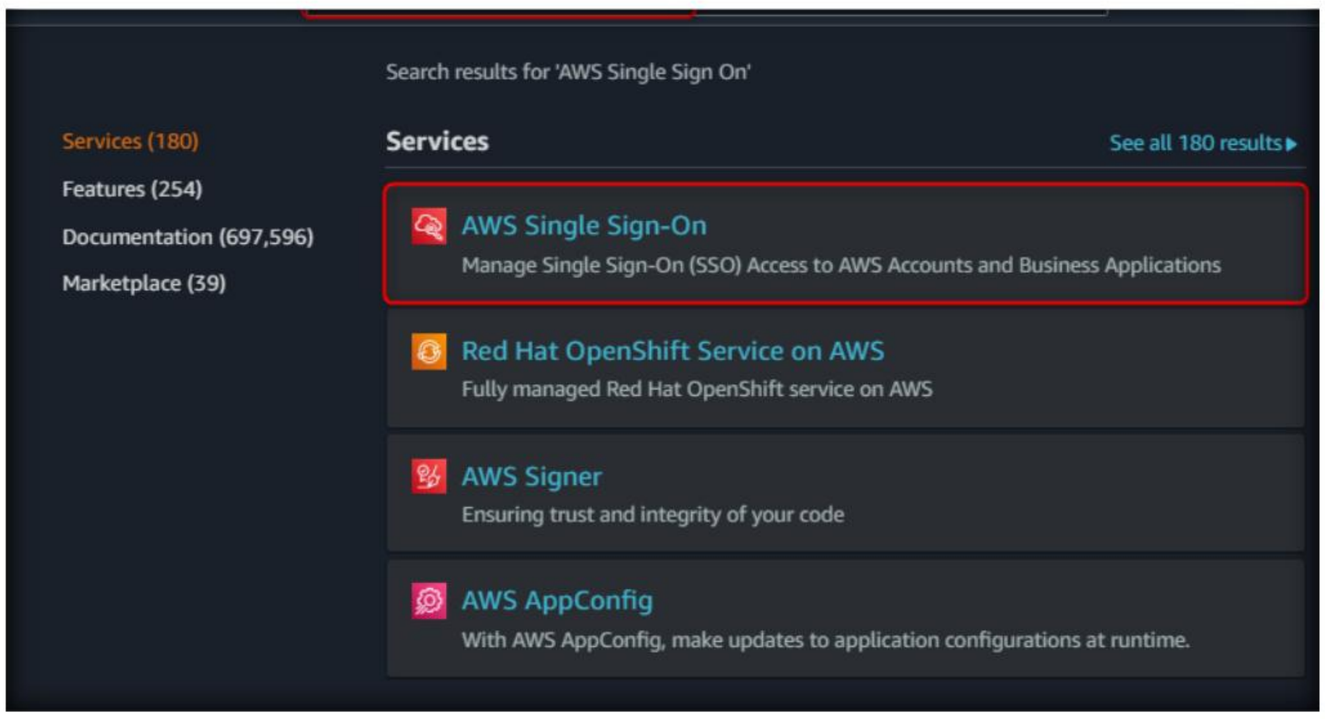


FIGURE 3.2.30: AWS Single Sign-On

31. The **AWS Single Sign-On (SSO)** window appears. Click on **Enable AWS SSO** to enable single sign-on.

    Note: If you have used AWS single sign-on previously, you will not get this window. In that case, you can continue with the subsequent steps.

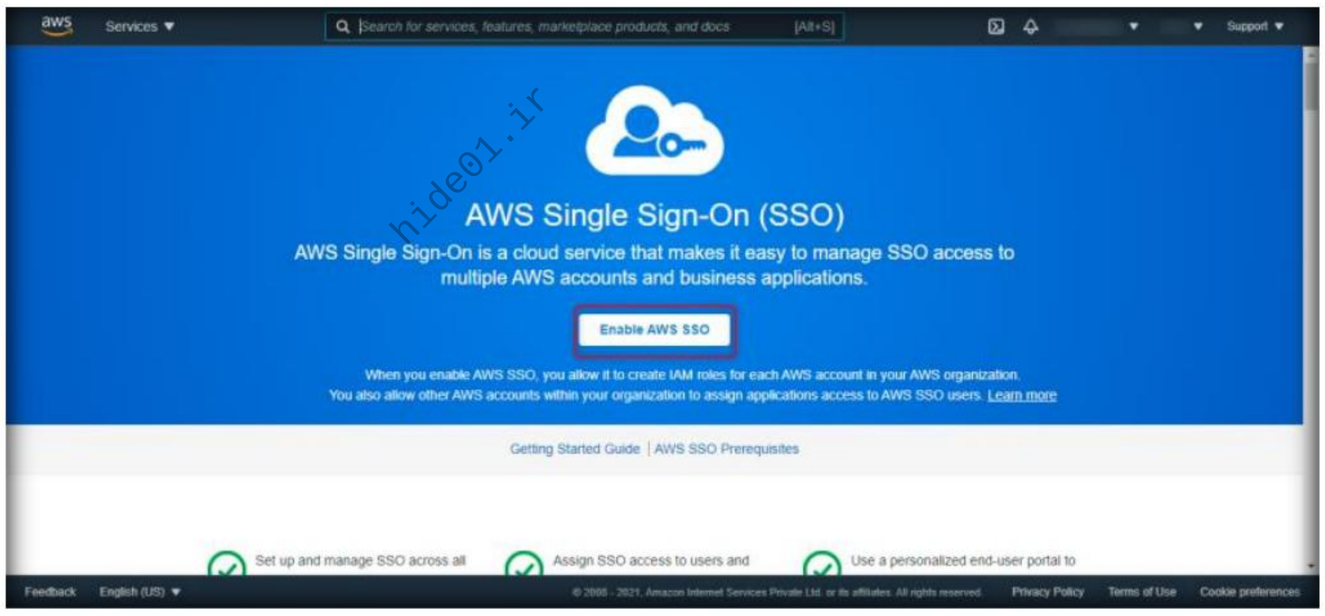


FIGURE 3.2.31: Enabling AWS Single Sign-On

32. An **Enable AWS SSO** popup appears. Click on **Create AWS organization** in the popup.

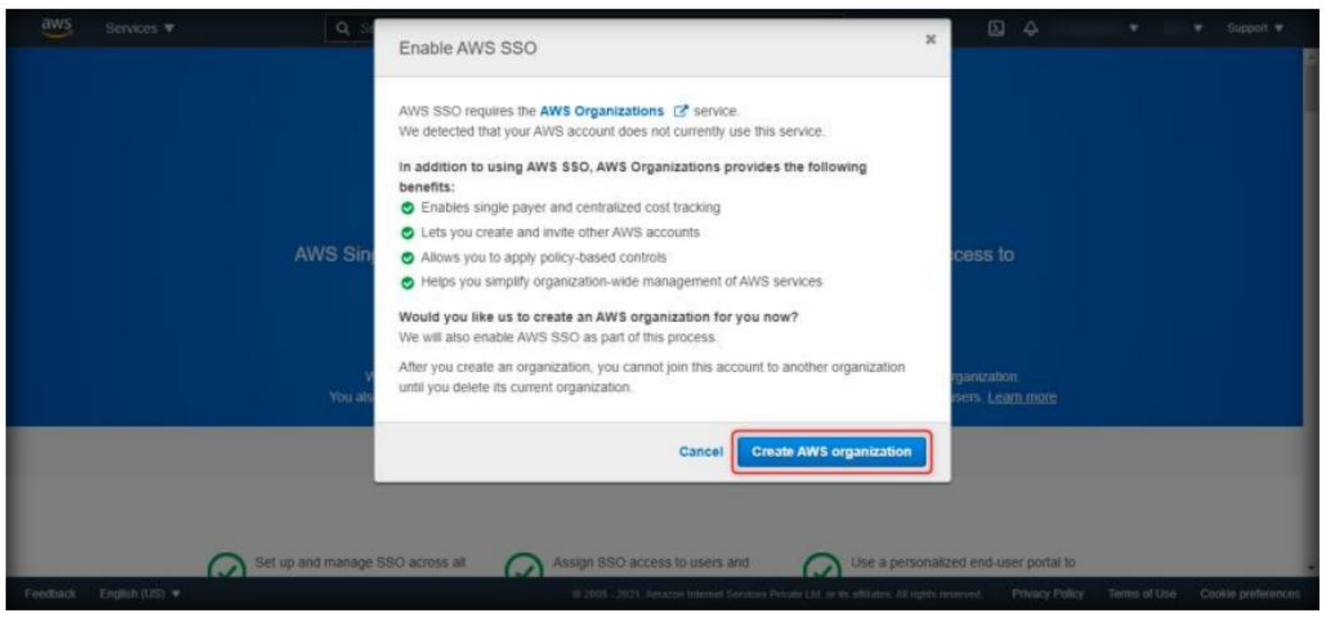


FIGURE 3.2.32: Creating AWS Organization to Enable Single Sign-On

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

33. You will be redirected to **AWS Single Sign-On Dashboard**. In this dashboard, click on **Choose your identity source**.

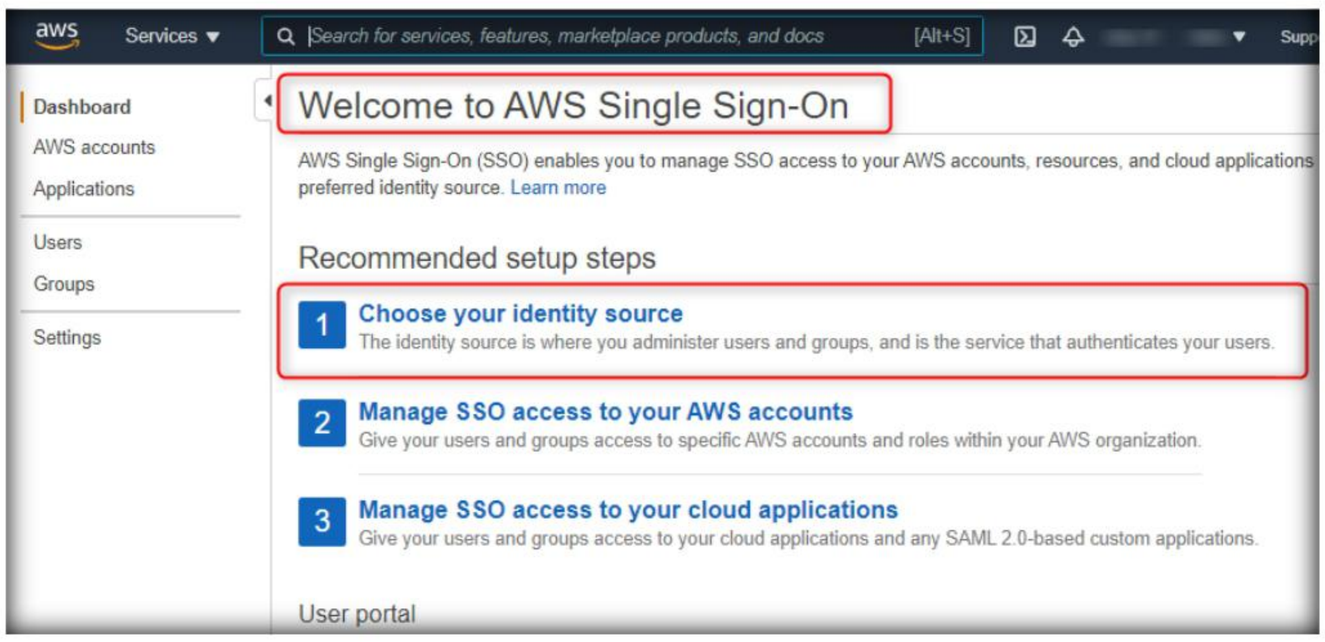


FIGURE 3.2.33: Selecting Identity Source in AWS Window

34. In the **Settings** window, click on **Change** beside **Identity source**.

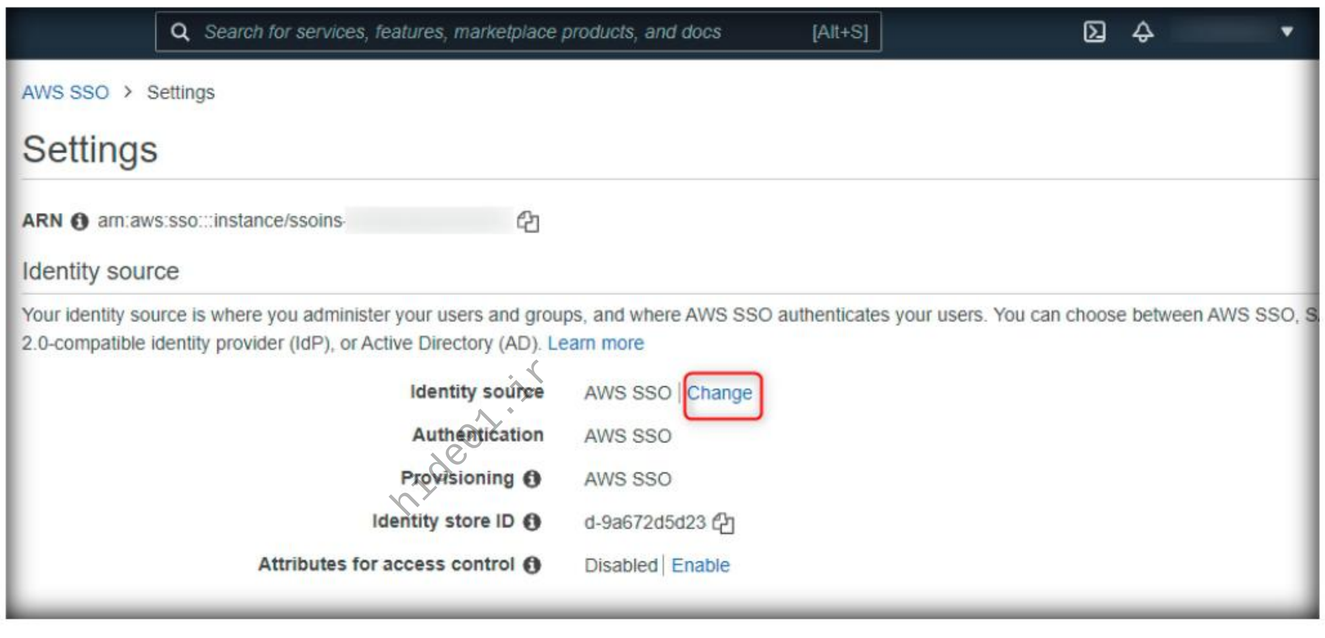


FIGURE 3.2.34: Changing AWS SSO Identity Source

35. A **Change identity source** window will open. Under **Choose where your identities are sourced**, select the **External identity provider** radio button.

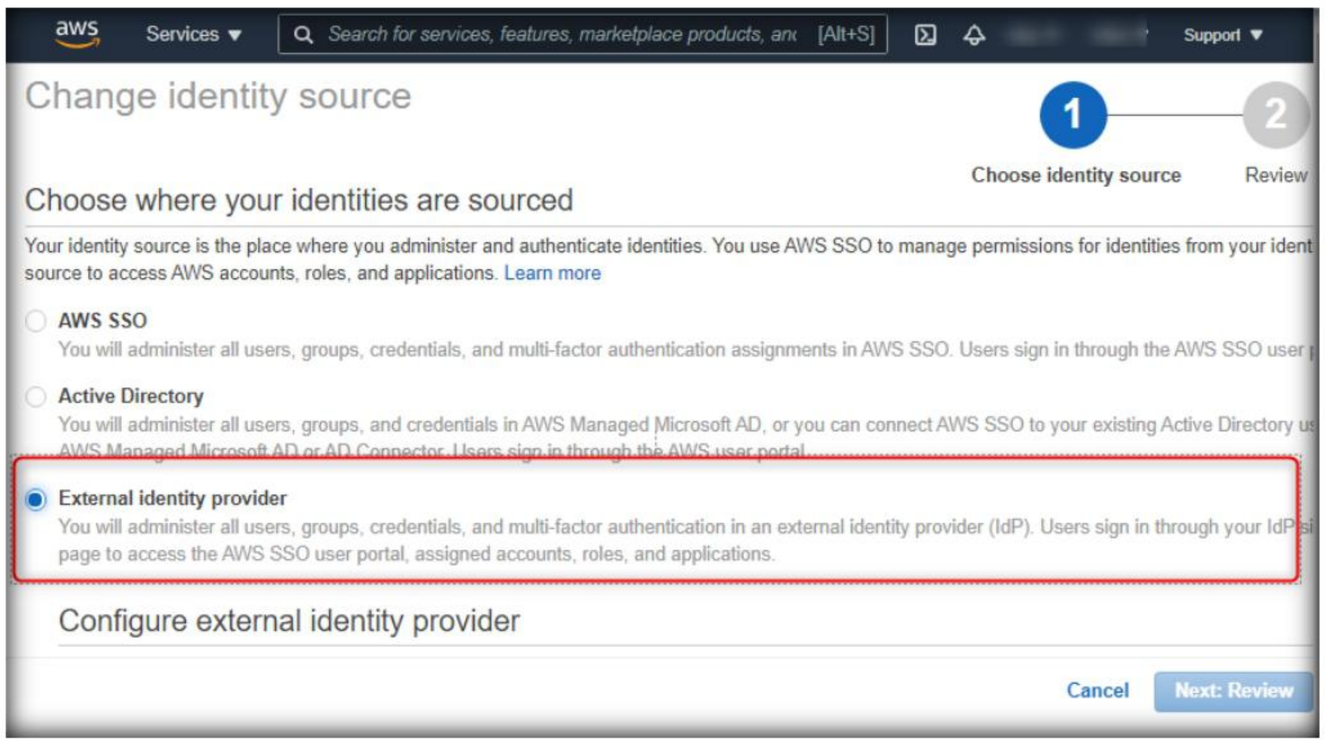


FIGURE 3.2.35: Selecting External Identity Provider

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

36. Scroll down and click on **Download metadata file** under **Service provider metadata**.

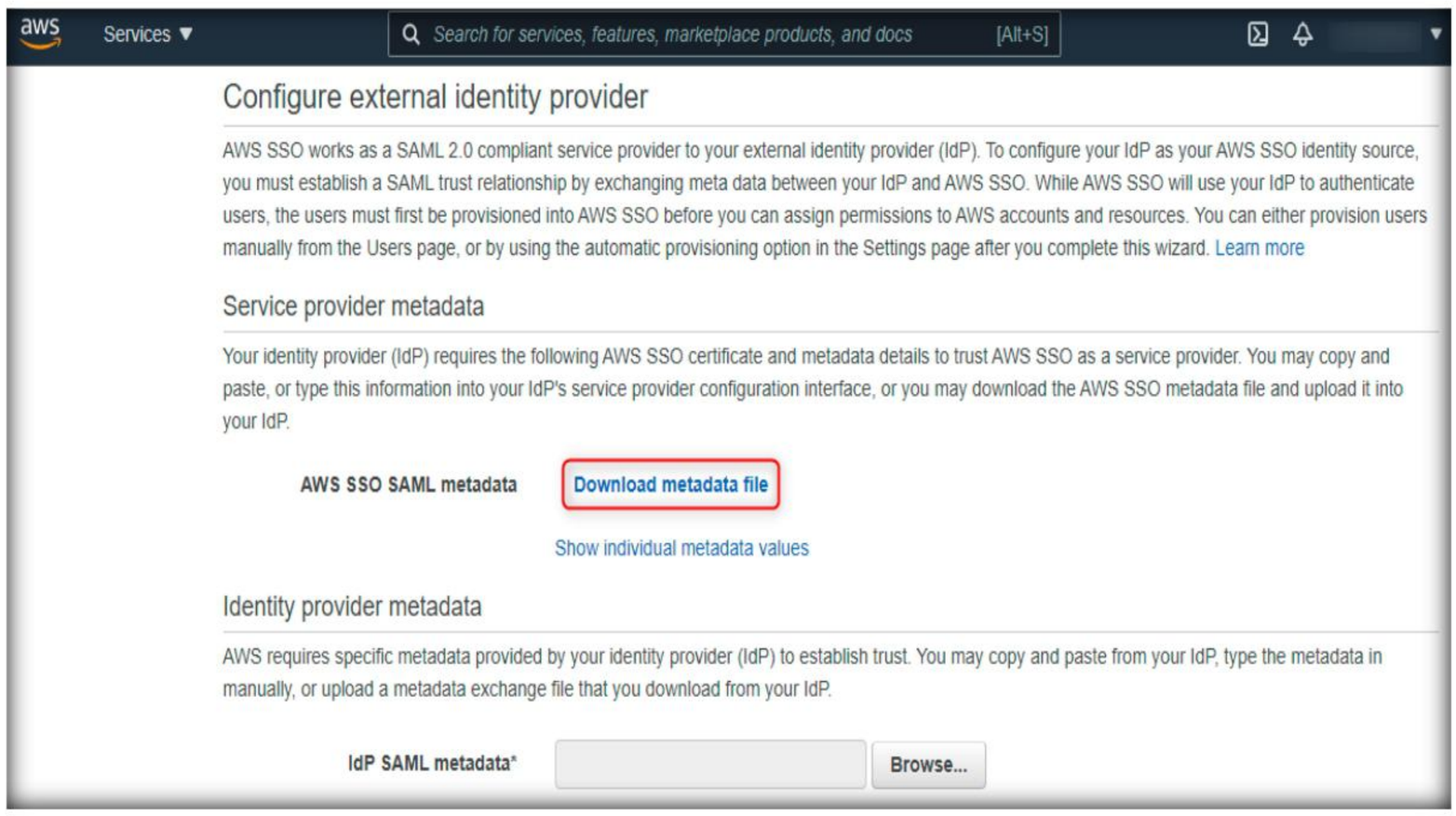


FIGURE 3.2.36: Downloading Metadata File

37. **Metadata file** is successfully downloaded.

    Note: Do not close the AWS window after this step. You can directly go to the next step.

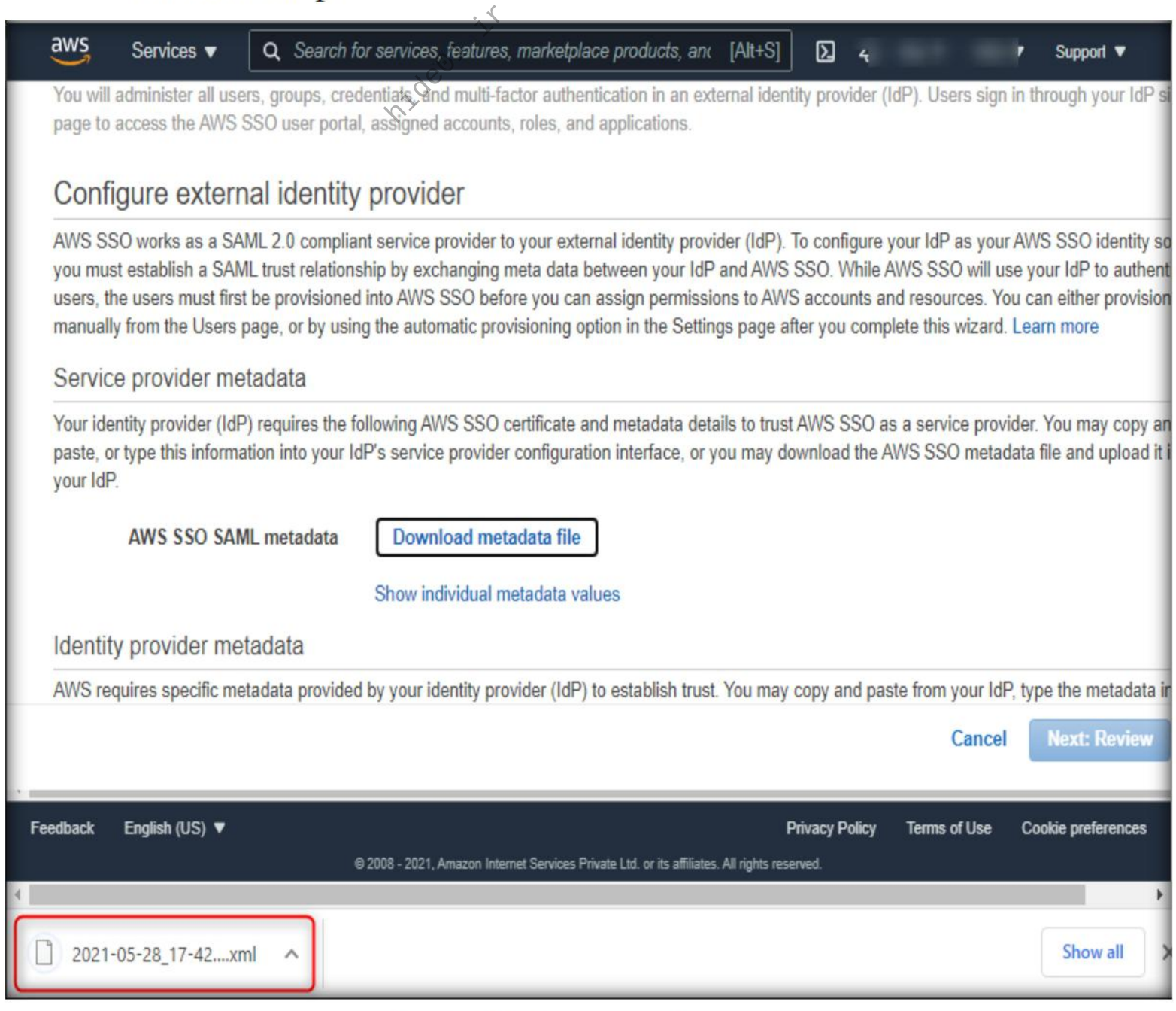


FIGURE 3.2.37: Downloaded Metadata File

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

38. Click on the Azure portal tab that was opened earlier. In the **SAML-based Sign-on** window, click on **Upload metadata file**.

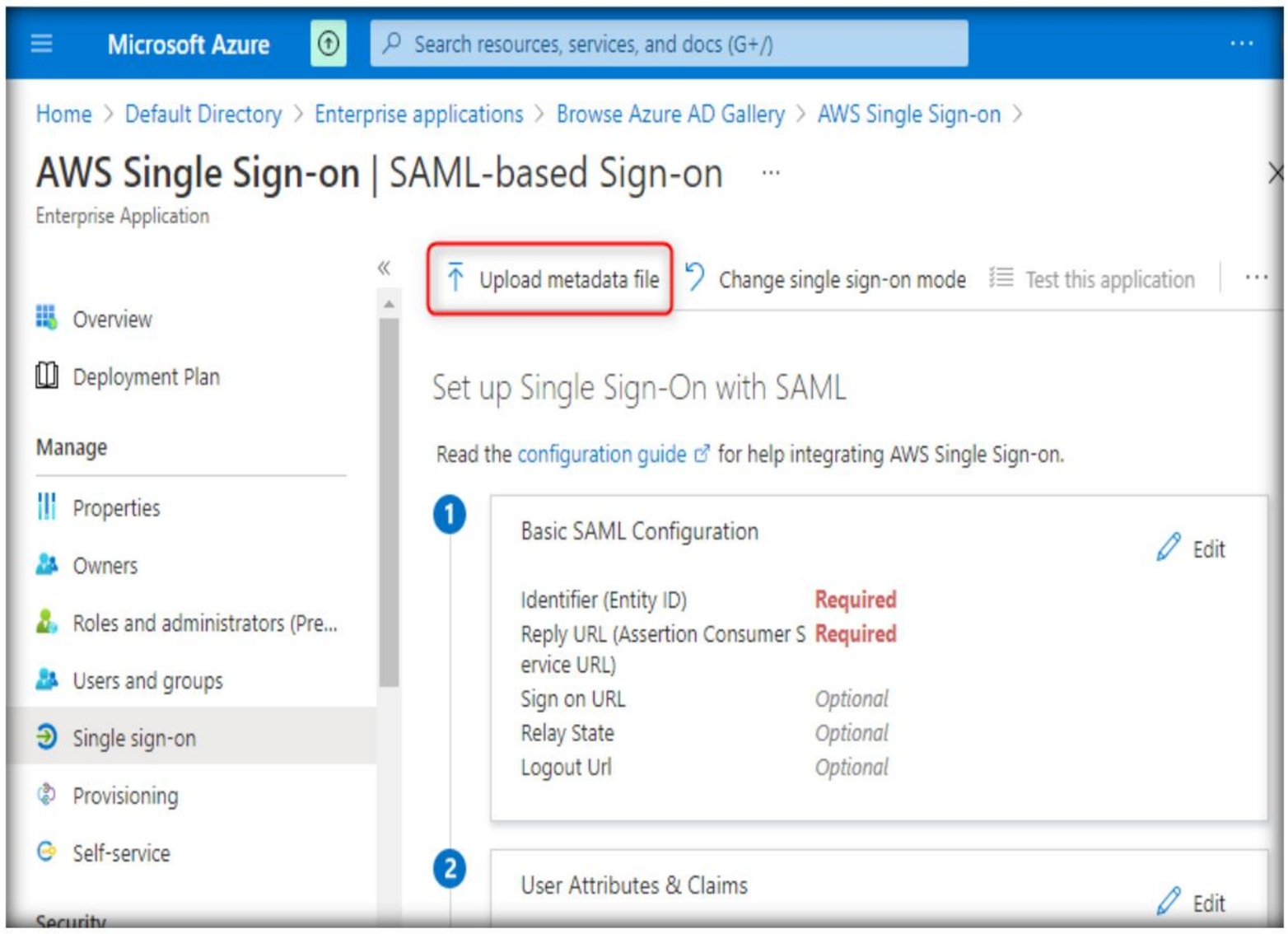


FIGURE 3.2.38: Uploading Metadata File in Microsoft Azure SAML-based Sign-on

39. Click on the **folder** icon on the right side of the **Select a file** field in **Upload metadata file**.

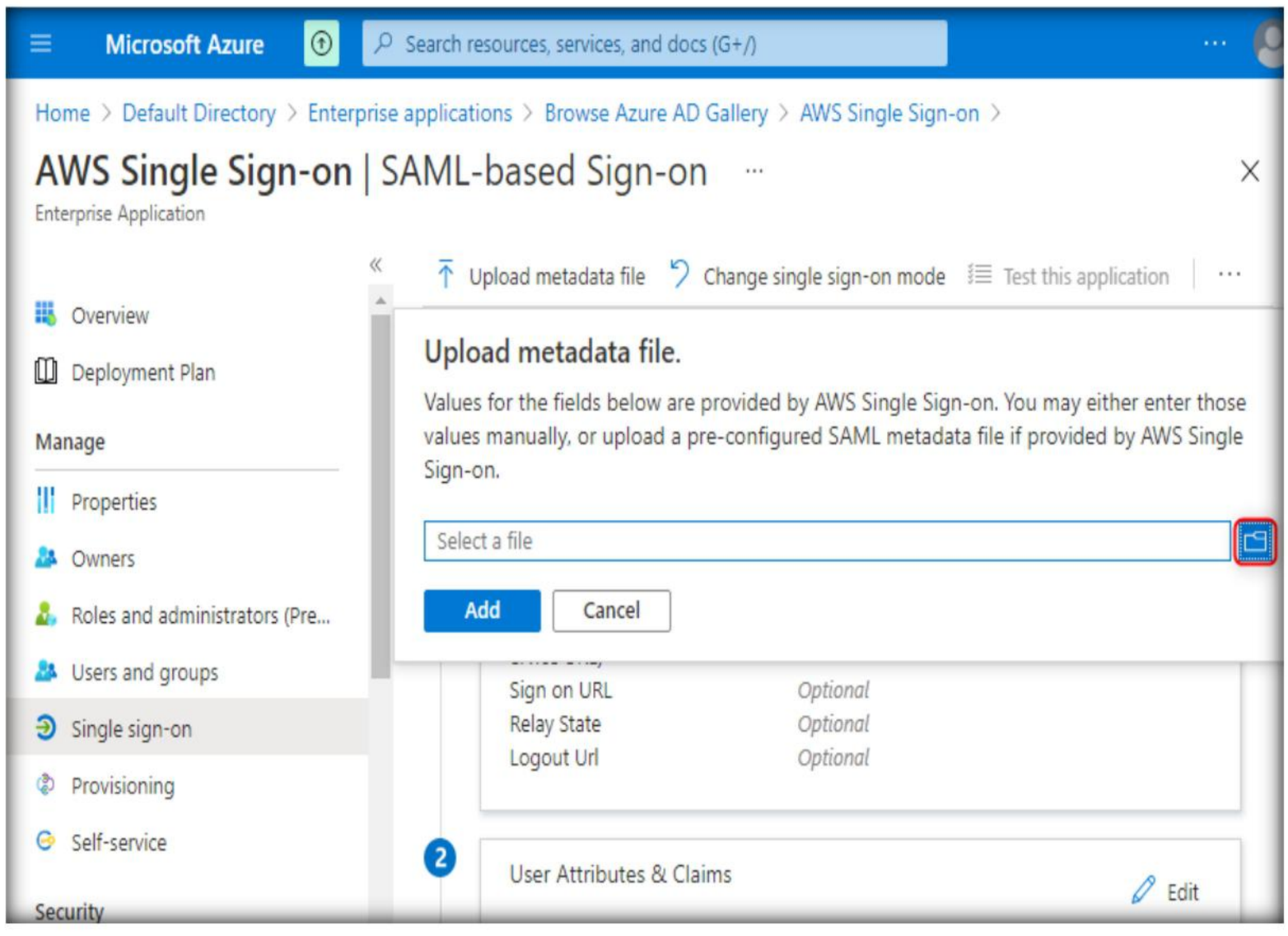


FIGURE 3.2.39: Selecting a File

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

40. In the popup that appears, go to **Downloads** and select the **metadata file** downloaded in the AWS Single Sign-on window.

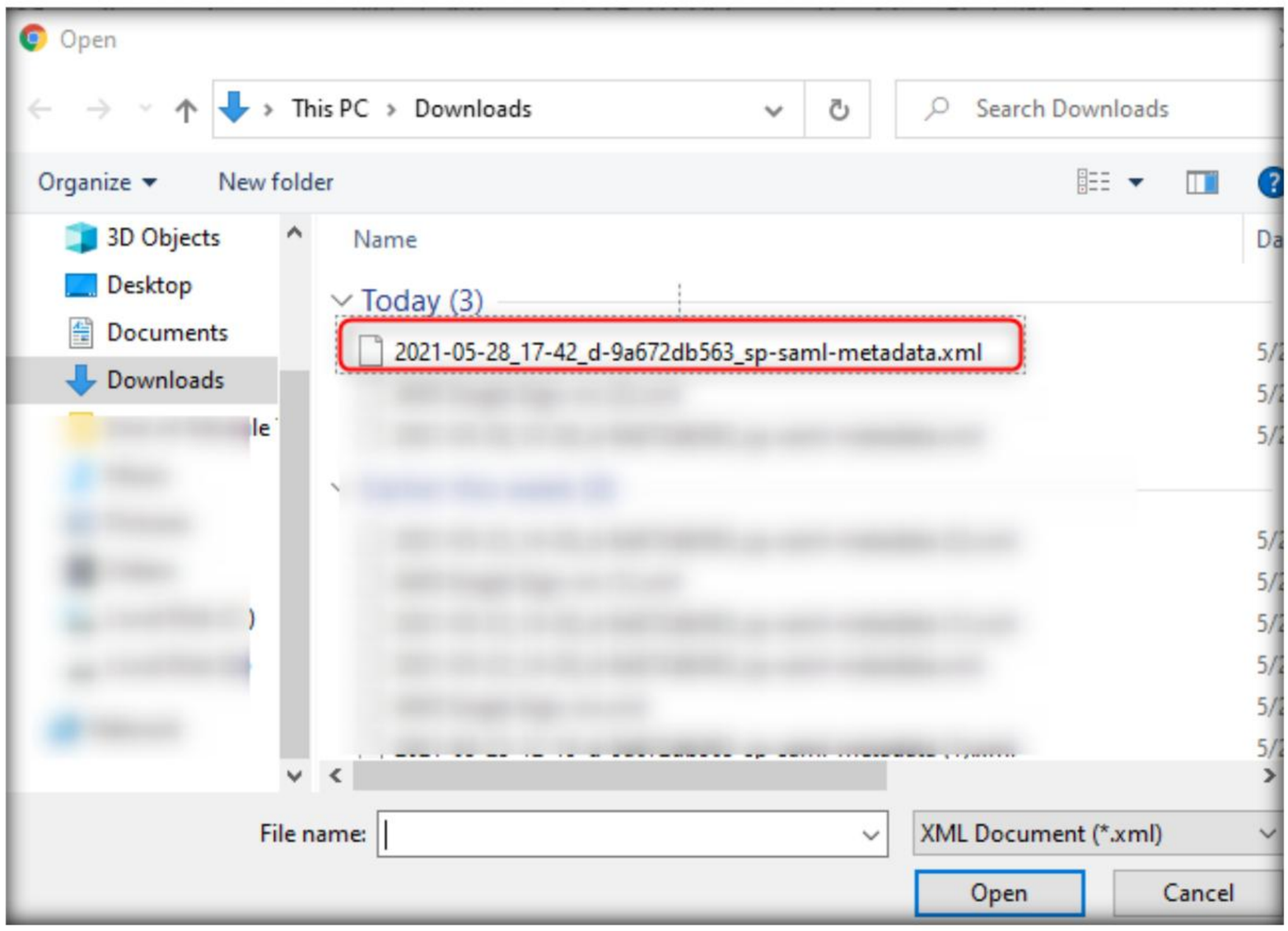


FIGURE 3.2.40: Selecting Metadata File from Downloads

41. Then, click **Open**.

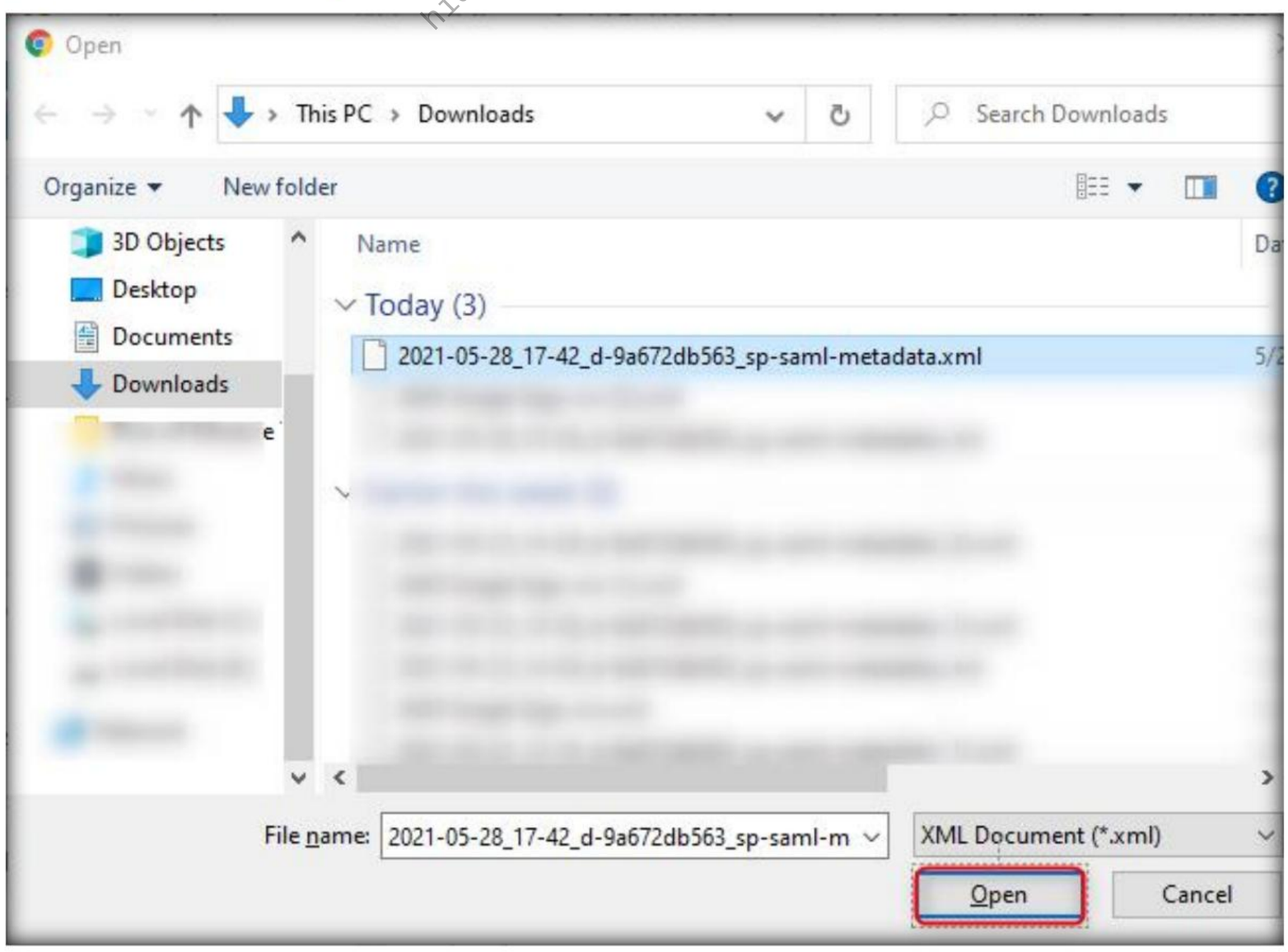


FIGURE 3.2.41: Selecting Open Button

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

42. Click on **Add** under **Upload metadata file.**

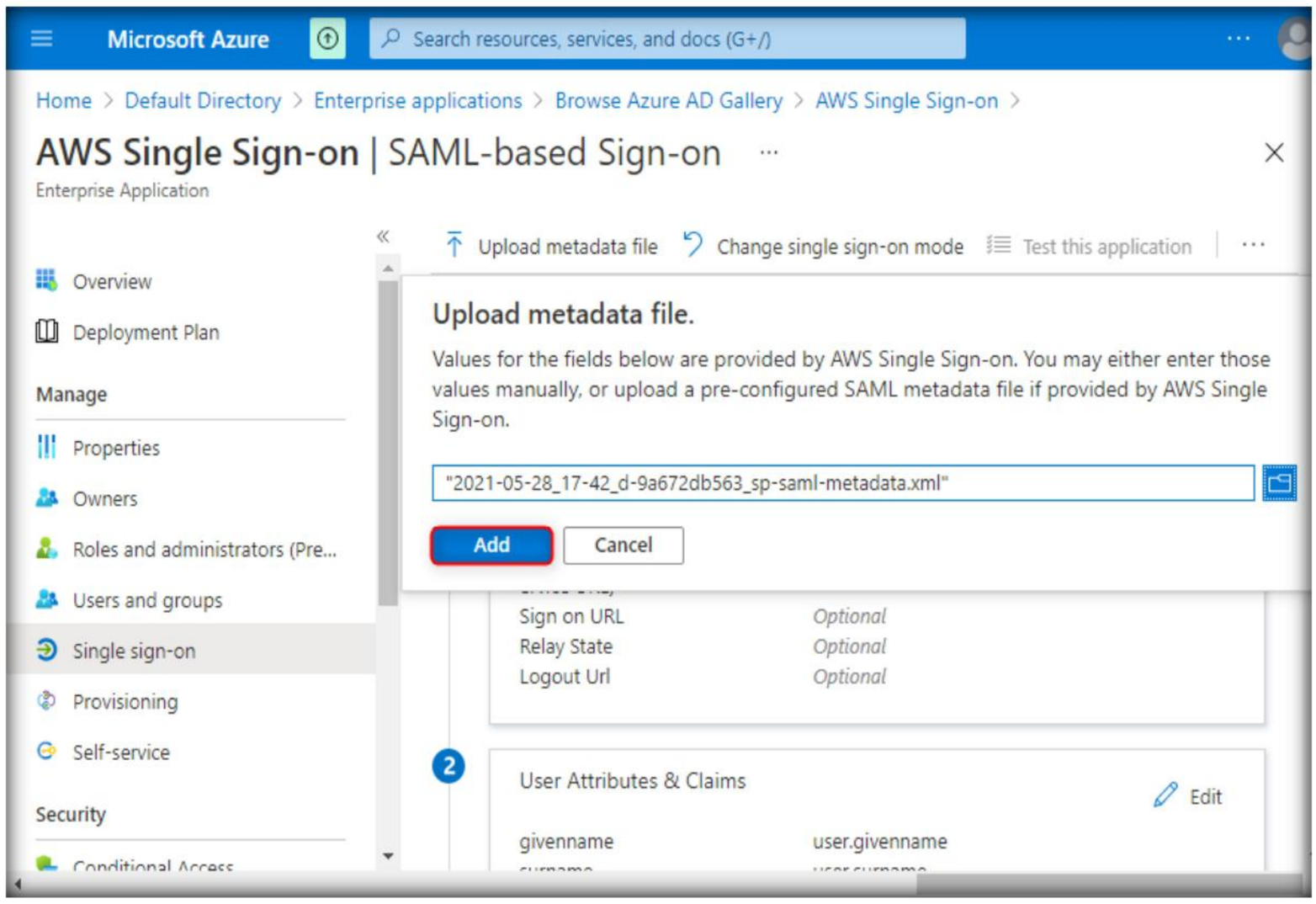


FIGURE 3.2.42: Adding Metadata File

43. A **Basic SAML Configuration** window will open. Now, click on **Save**.

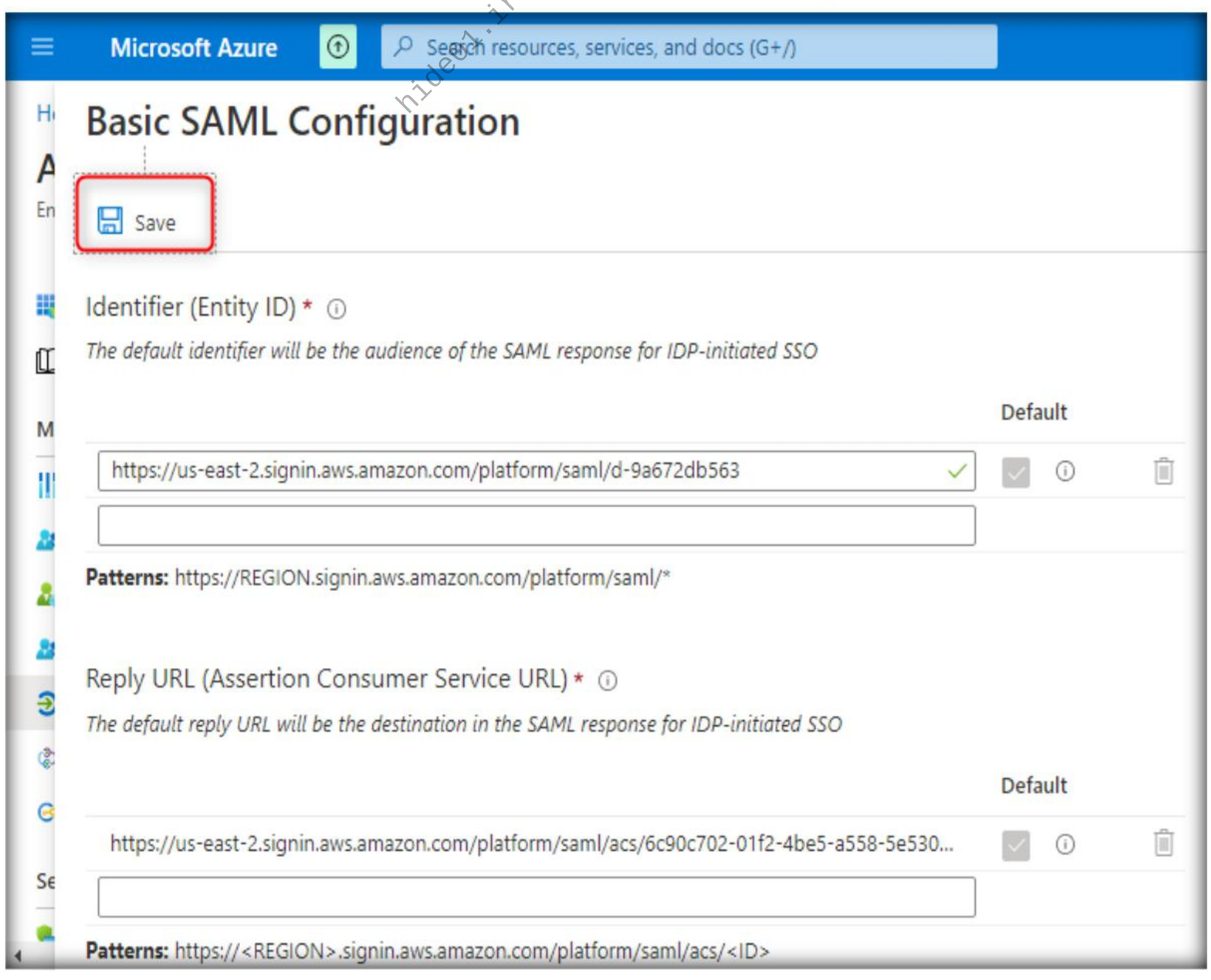


FIGURE 3.2.43: Saving Basic SAML Configuration

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

44. After the **Basic SAML Configuration** is successfully saved, click on the **Close** icon to close the **Basic SAML Configuration** window.

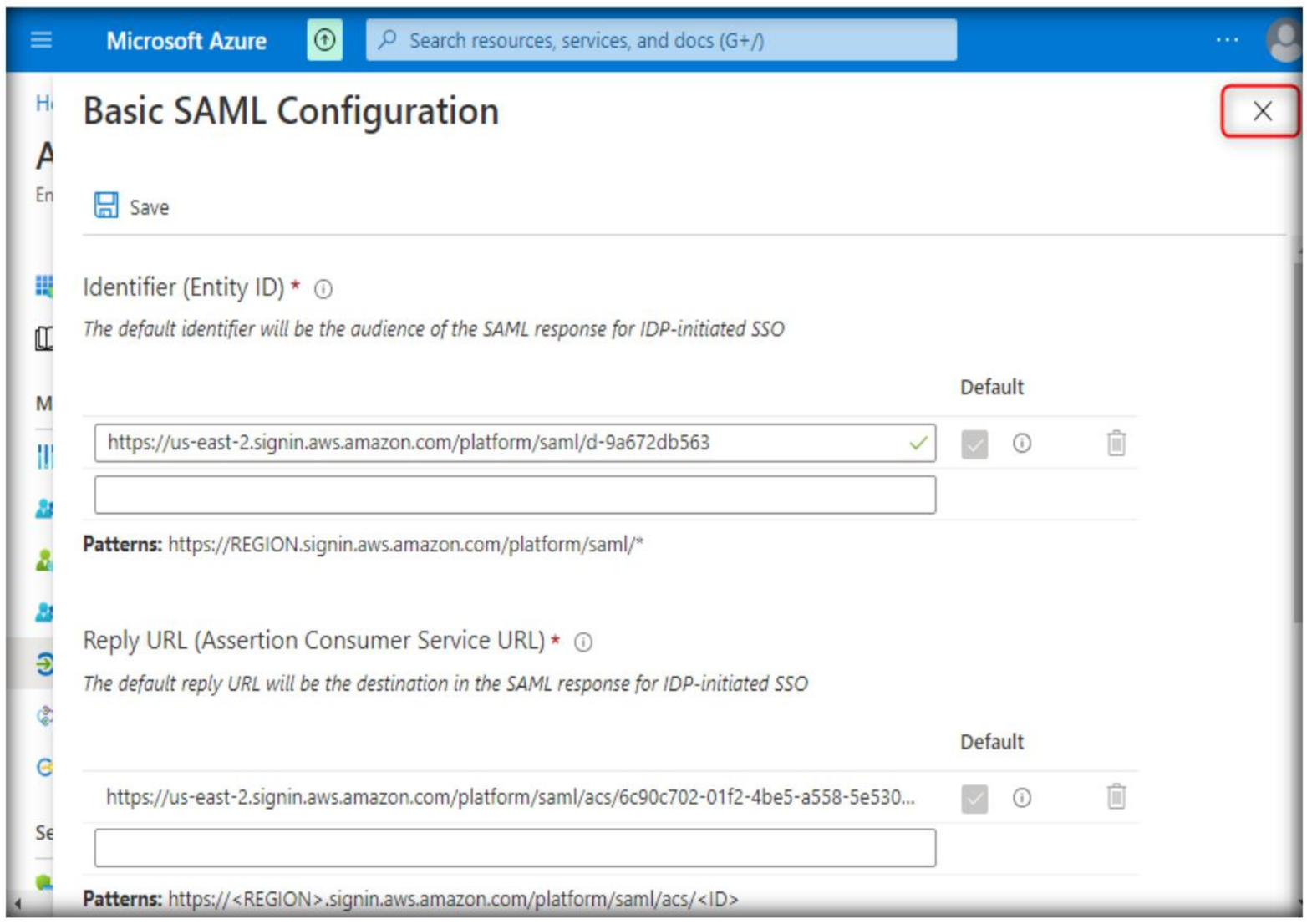


FIGURE 3.2.44: Closing Basic SAML Configuration

45. Under **Basic SAML Configuration**, if **Reply URL** is missing, then click on the following message under **Set up Single Sign-On with SAML**: **The default reply URL is missing from the list of reply URLs. Click here to fix it.**

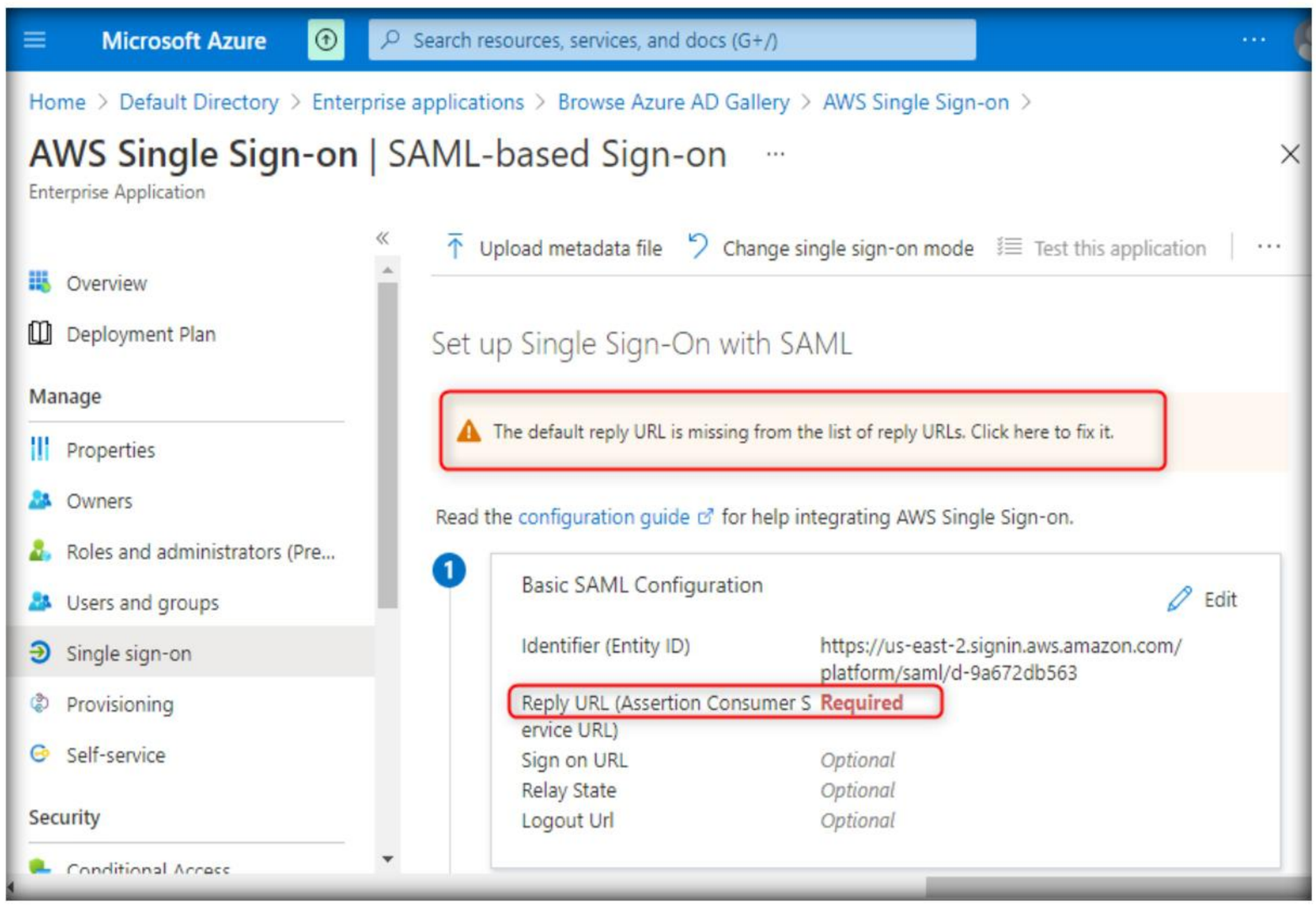


FIGURE 3.2.45: Setting Reply URL

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

46. **Reply URL** will be inserted, and a popup displaying **Single sign-on configuration was saved successfully** will appear.

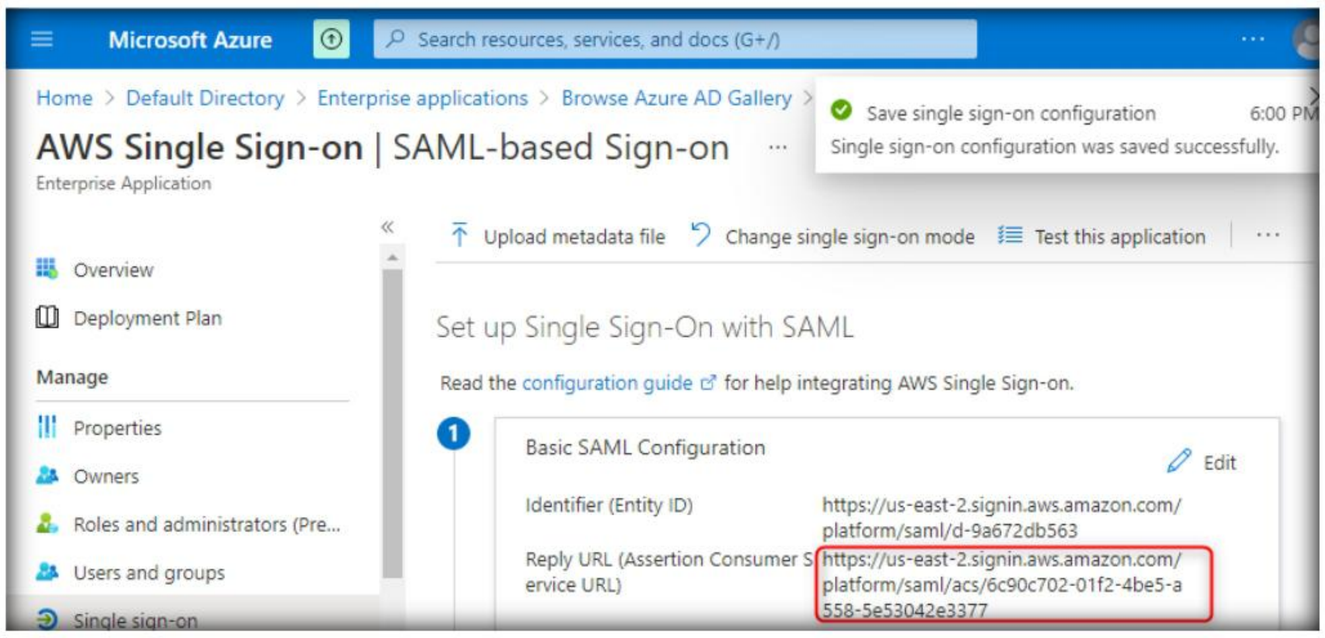


FIGURE 3.2.46: Inserted Reply URL Successfully

47. Scroll down and click on **Download** beside **Federation Metadata XML** under **SAML Signing Certificate**.

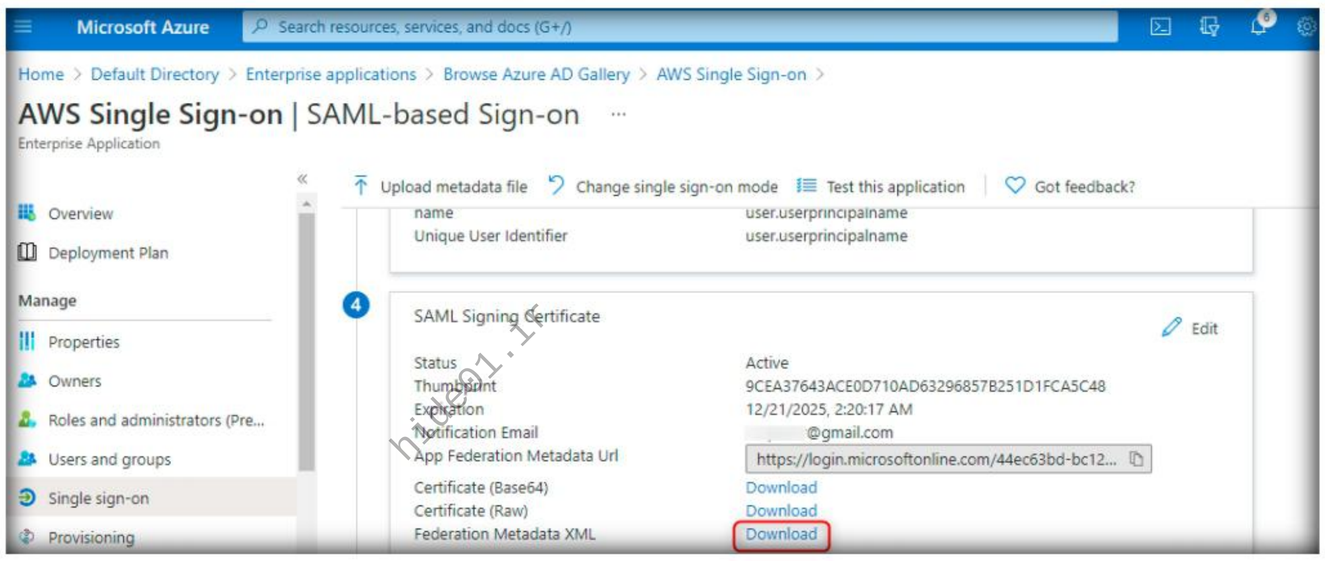


FIGURE 3.2.47: Downloading Federation Metadata XML

48. Federation Metadata XML will be successfully downloaded **as AWS Single Sign-On.xml**.

Note: Do not close this Azure window after this step. Go directly to the next step.

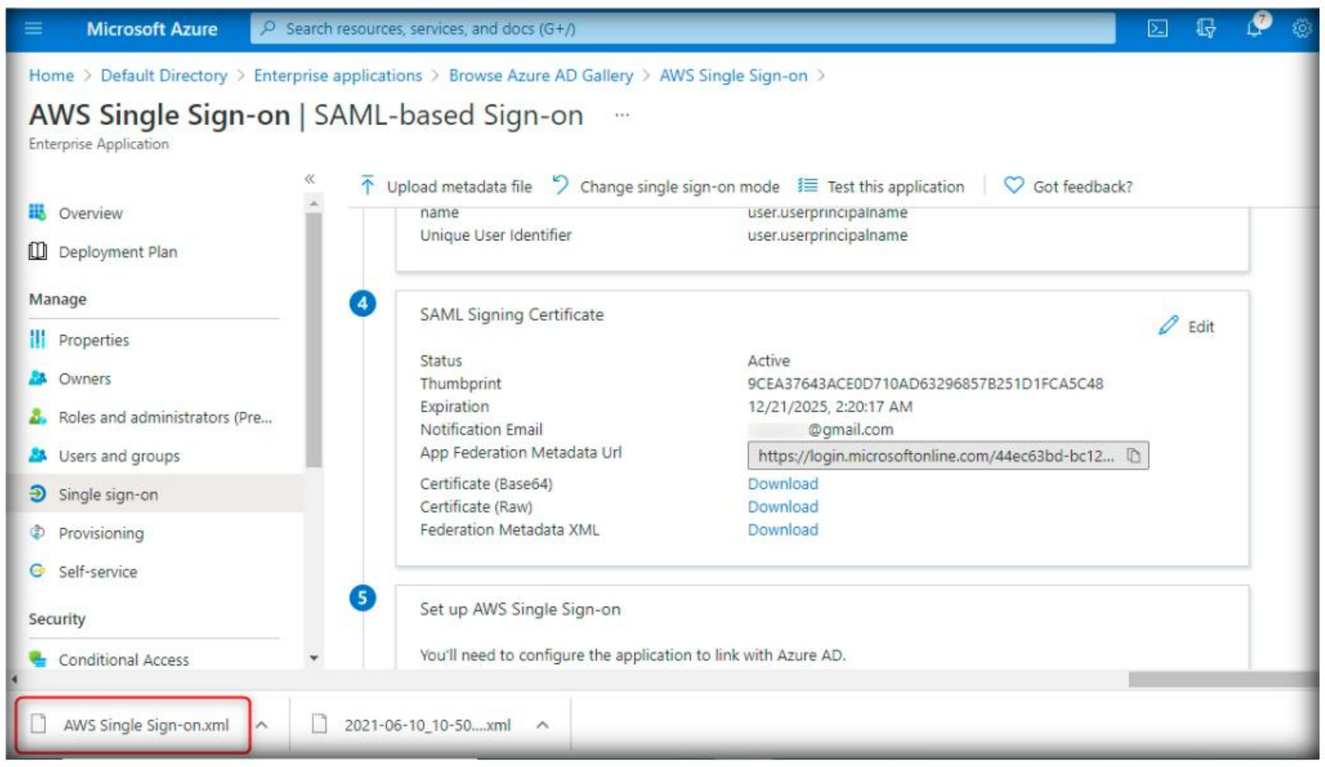


FIGURE 3.2.48: Federated Metadata File Successfully Downloaded

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 4

Configuring AWS SSO

49. Now, go back to the AWS console window in the other tab. Scroll down in the AWS **Change identity source** window. Under the **Identity provider metadata** section, click on the **Browse** button beside **IdP SAML metadata*.**

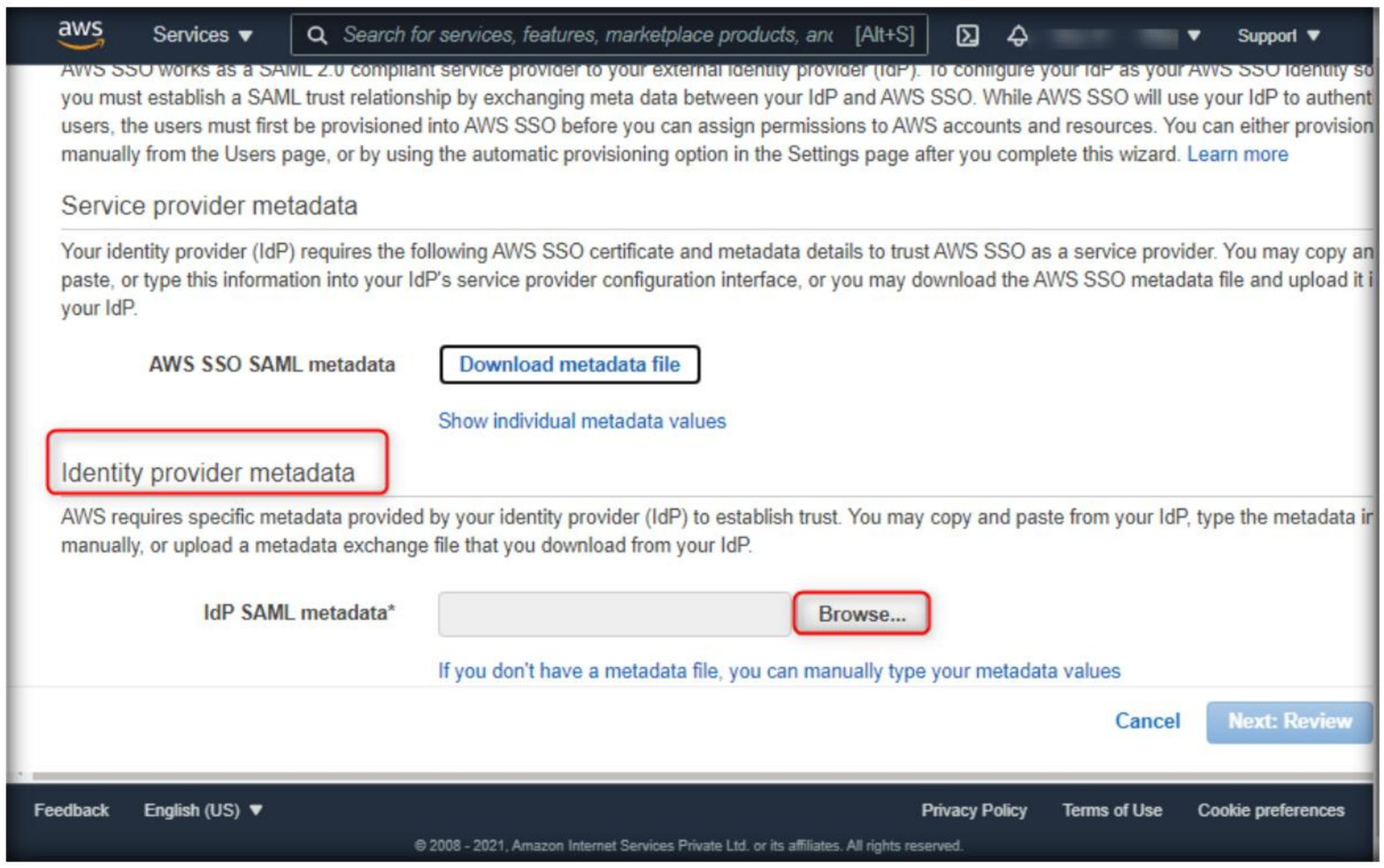


FIGURE 3.2.49: Browsing for Federated Metadata File in AWS

50. In the popup, select the **AWS Single Sign-on.xml** file under Downloads, and then click on **Open**.

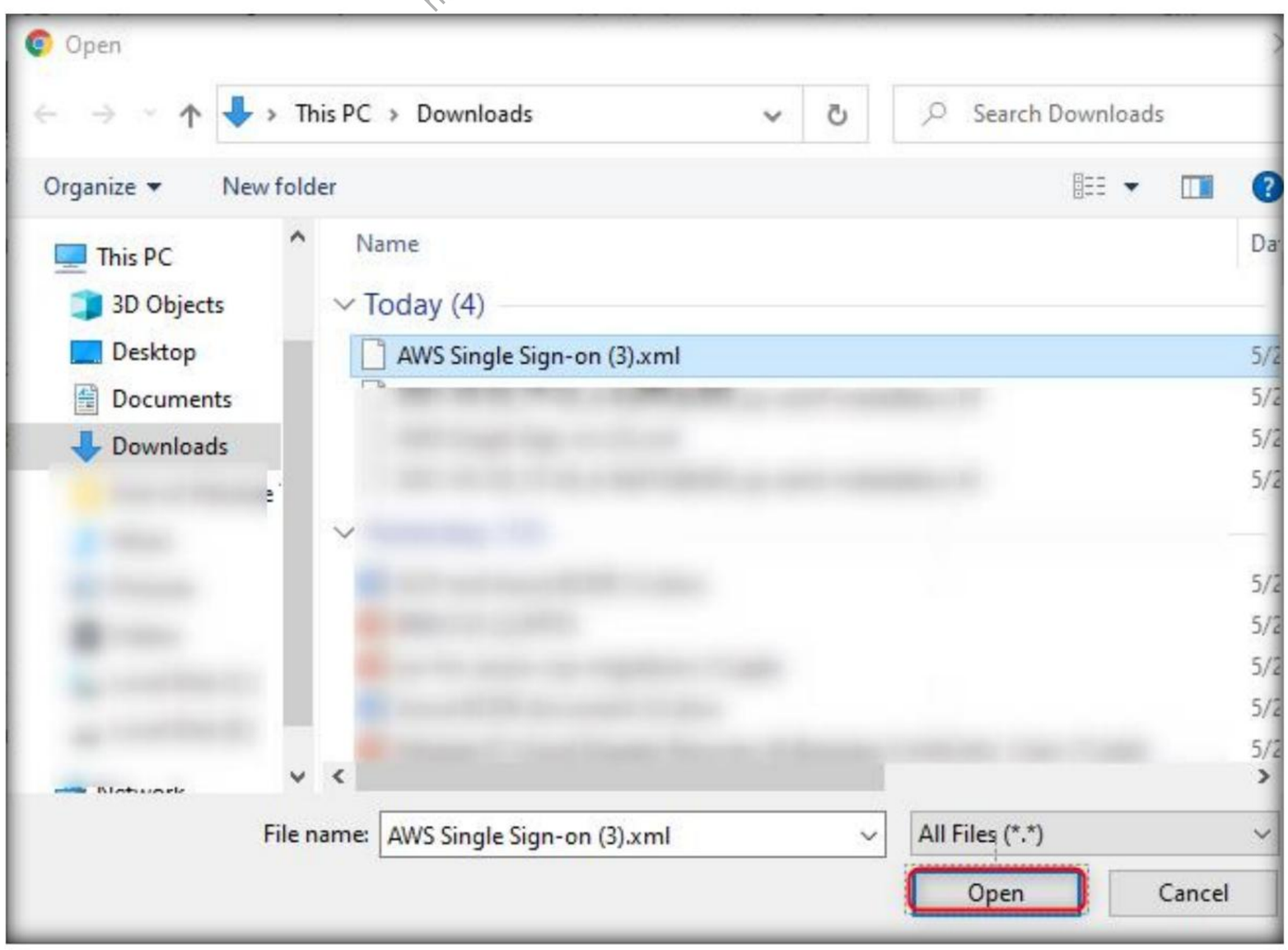


FIGURE 3.2.50: Opening Federated Metadata File

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

51. **AWS Single Sign-on.xml** file is now added. Next, click on **Next: Review** to review the identity source change.

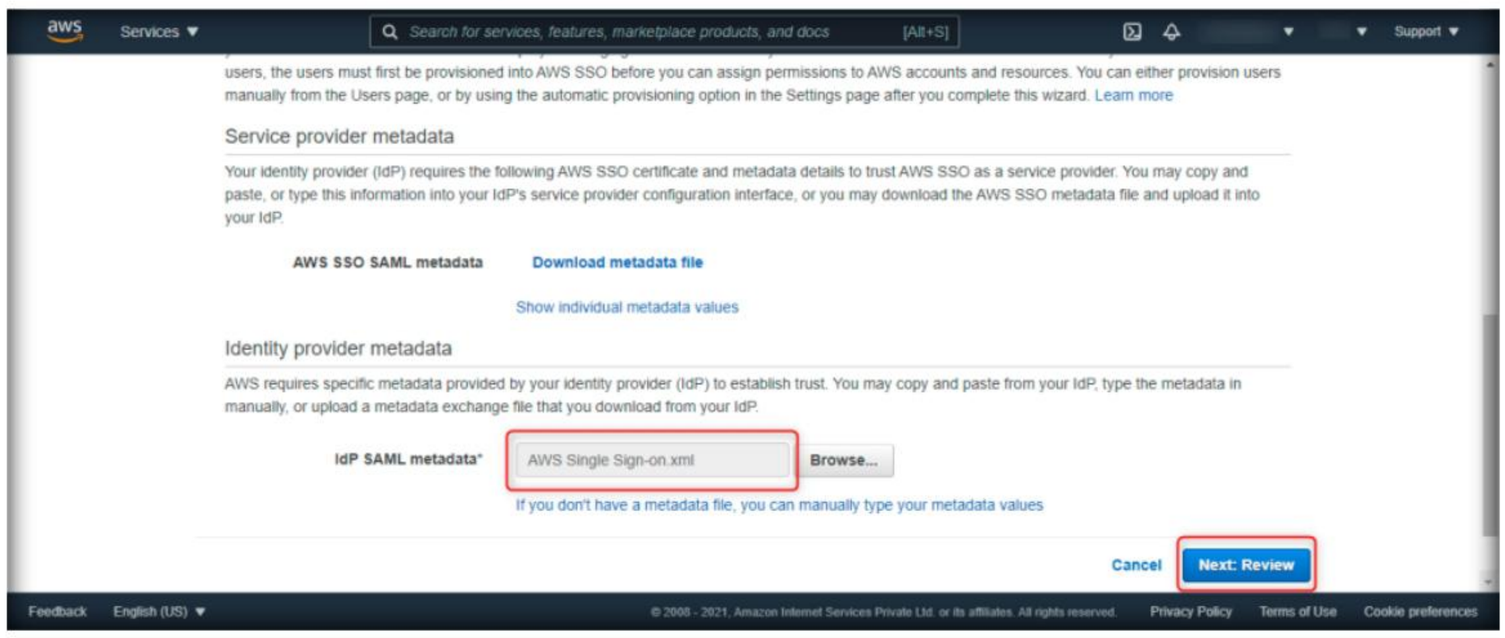


FIGURE 3.2.51: Selecting Next: Review

52. A **Review and confirm** window will open. Type **ACCEPT** in the given field and click on **Change identity source**.

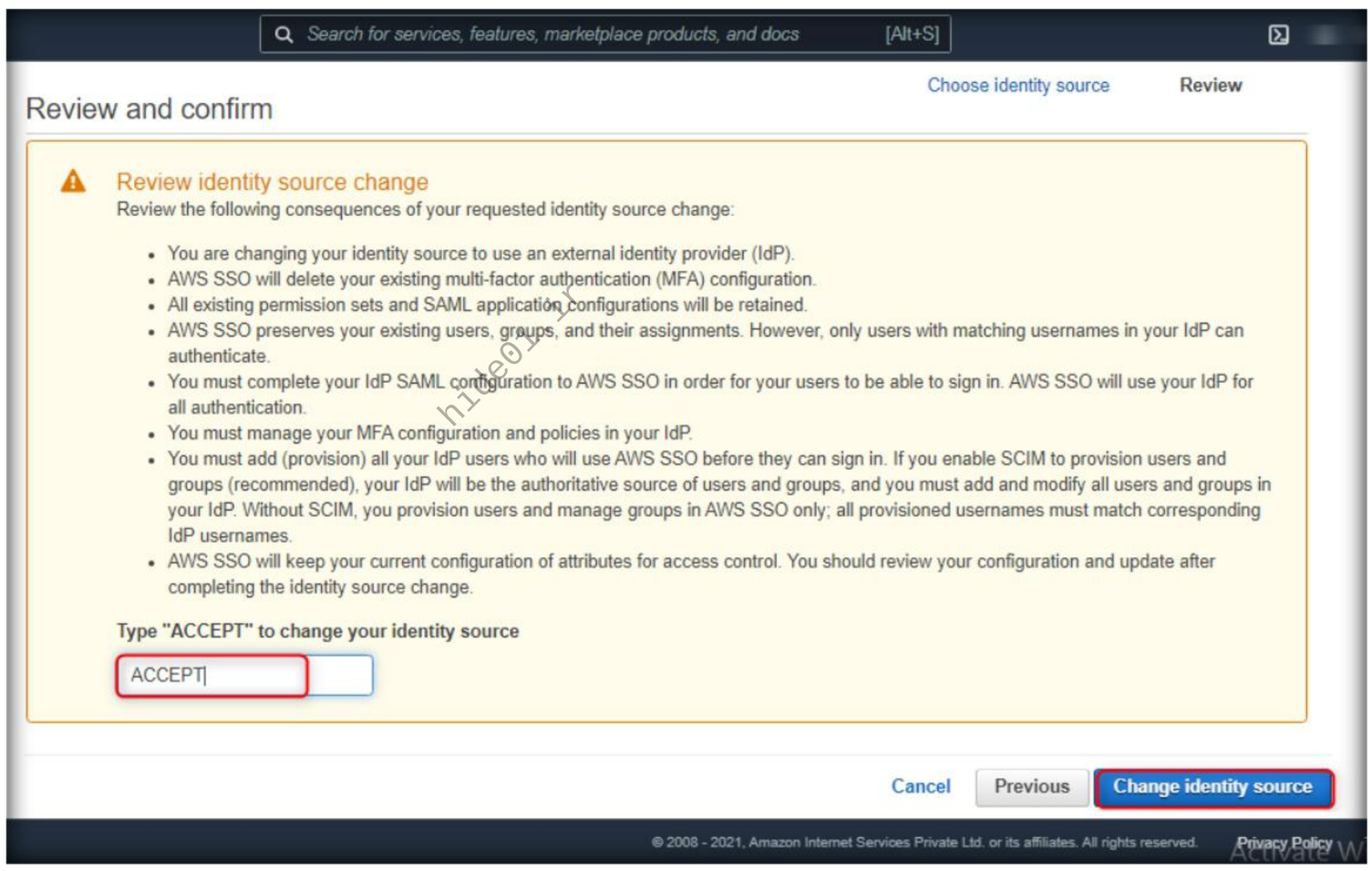


FIGURE 3.2.52: Accepting Review Identity Source Changes

53. After AWS SSO is successfully configured, click on the **Return to settings** button.

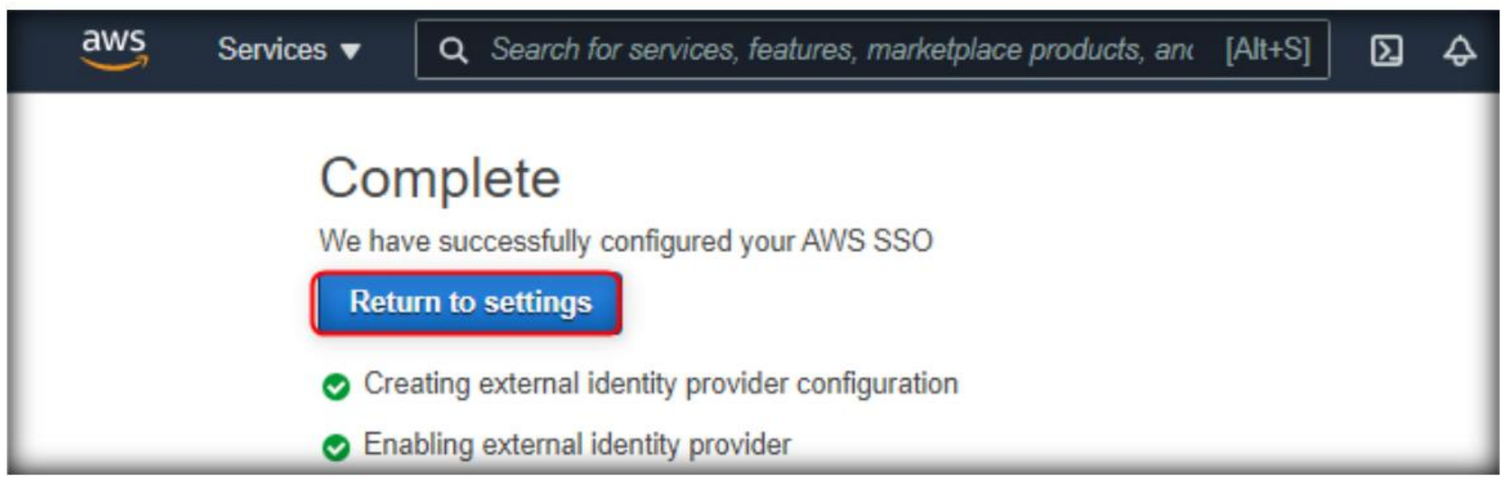


FIGURE 3.2.53: Successfully Configured AWS SSO

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

54. The identity source is successfully changed from AWS SSO to an external identity provider.

    Note: Kindly login to the email account provided during AWS account generation. You may receive an email verification message; click on **Verify your email address** in this email. If you did not receive this email, then continue with the subsequent steps.

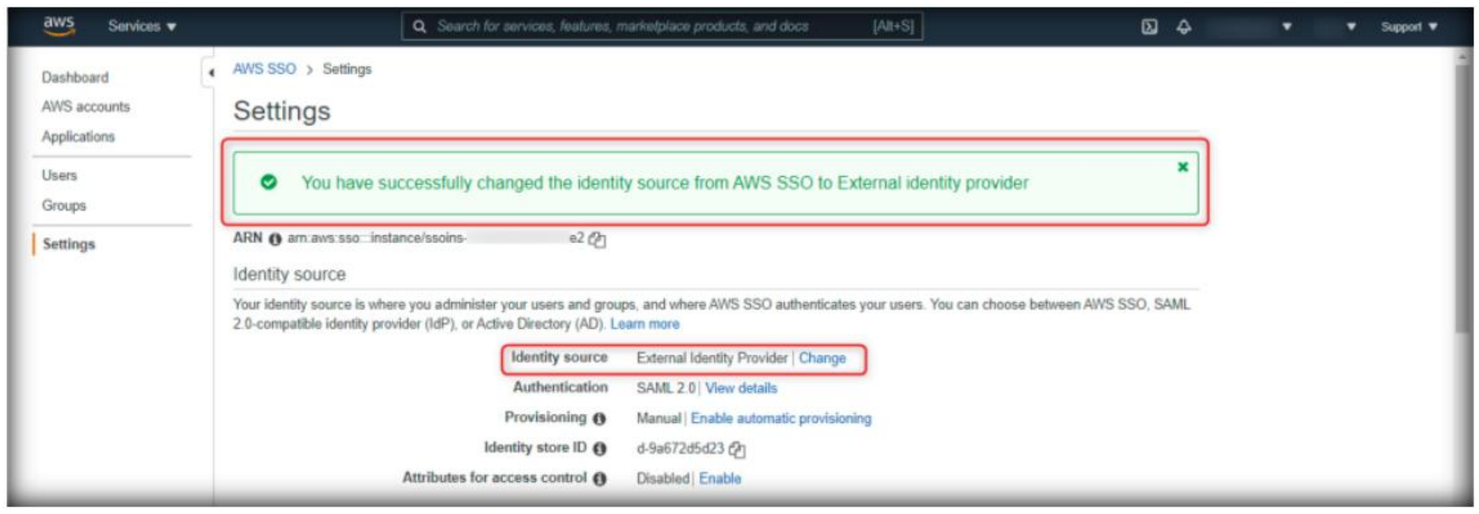


FIGURE 3.2.54: Successfully Changed the Identity Source in AWS

TASK 5

Enabling Automatic Provisioning in AWS SSO

55. Under **Identity source,** click on **Enable automatic provisioning** beside **Provisioning**.

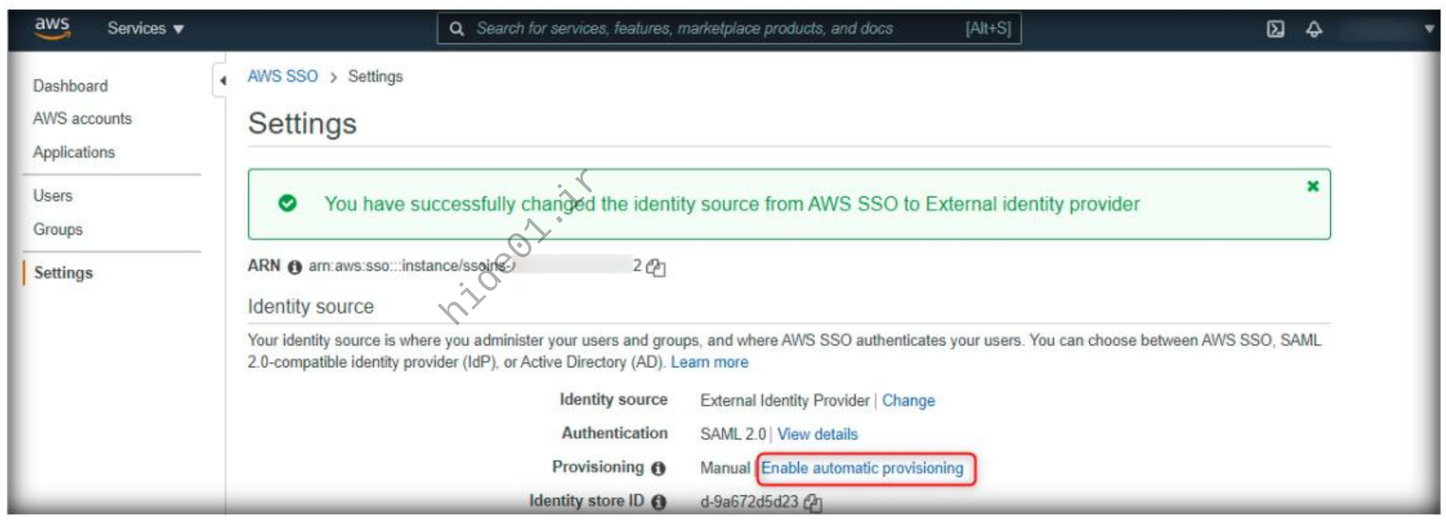


FIGURE 3.2.55: Enabling Automatic Provisioning

56. In the **Inbound automatic provisioning** window, click on **Show token** under **Access token**.

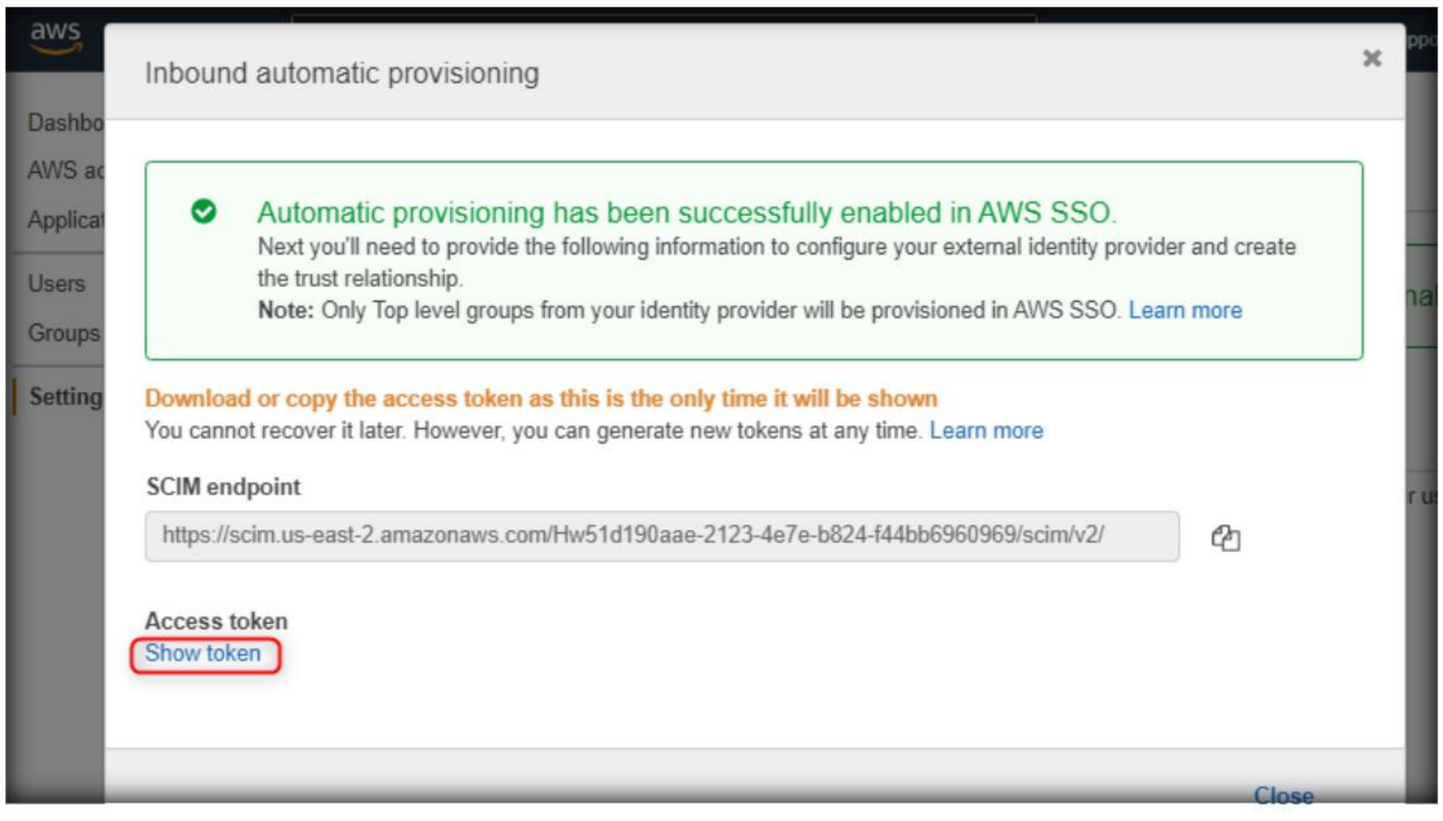
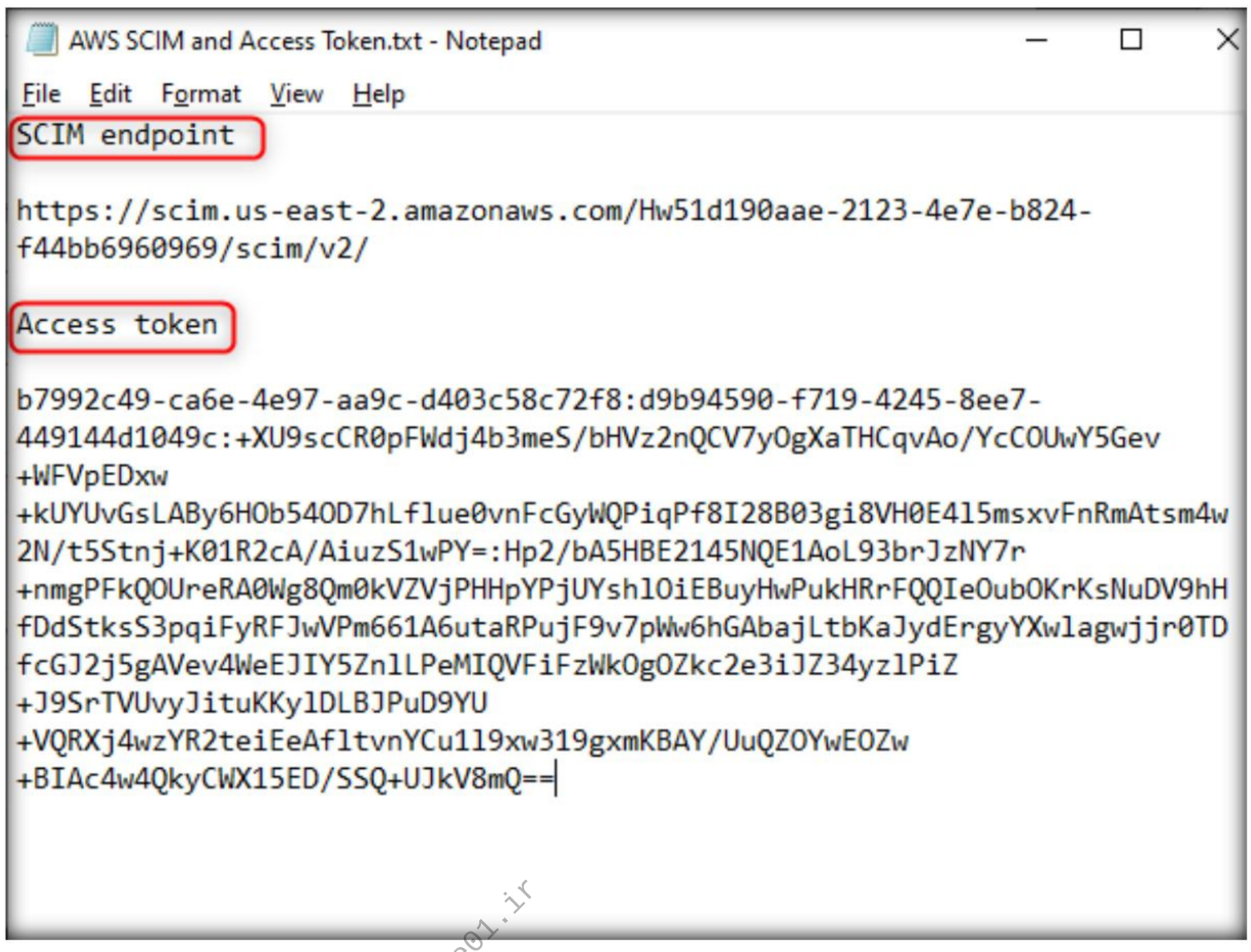


FIGURE 3.2.56: Selecting Show Token

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

57. Open a notepad and copy the **SCIM endpoint** and **Access token**. Further, **save** the notepad on your desktop folder with **AWS SCIM and Access Token.txt** as the file name.



h3de01.ir

FIGURE 3.2.57: Saving SCIM Endpoint and Access Token in Notepad

58. Go back to Azure Portal. In the **AWS SAML-based Sign-on** window, click on **Provisioning** under **Manage** in the left pane.

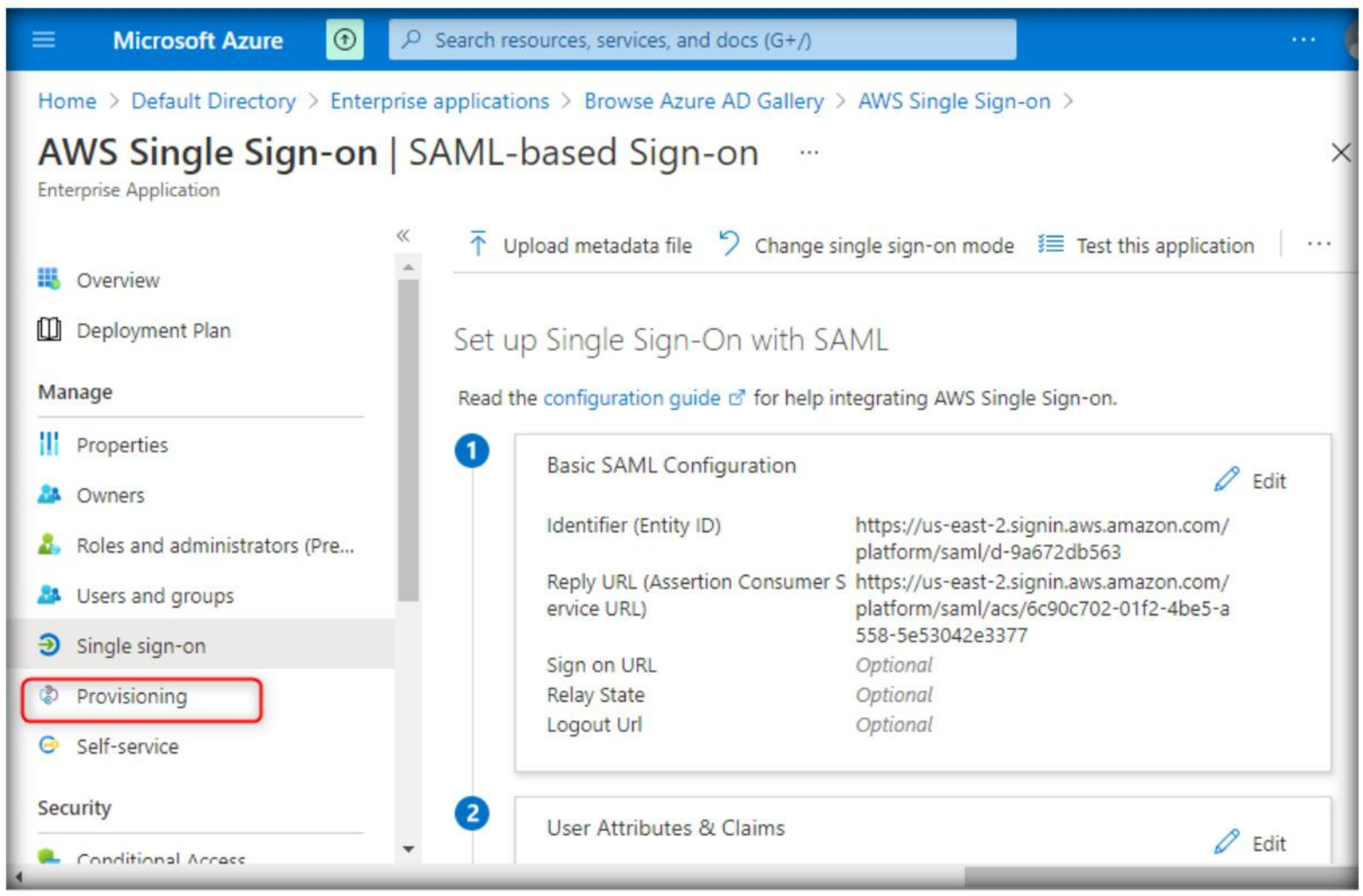


FIGURE 3.2.58: Selecting Provisioning in Azure AWS Single Sign-On

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

59. Then, click on **Get started** in the main page.

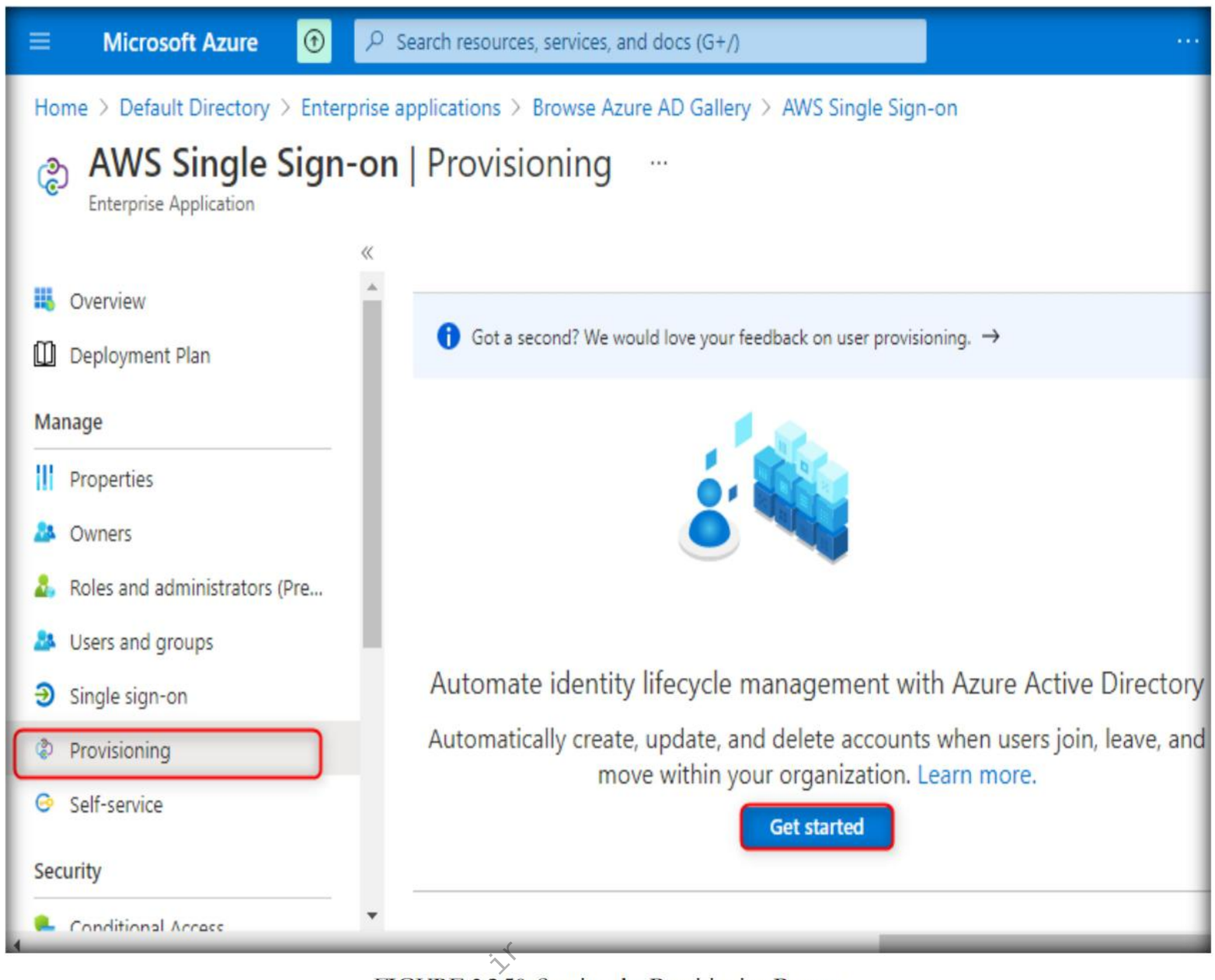


FIGURE 3.2.59: Starting the Provisioning Process

60. In the **Provisioning window** that appears, click on the dropdown under **Provisioning Mode** and select **Automatic.**

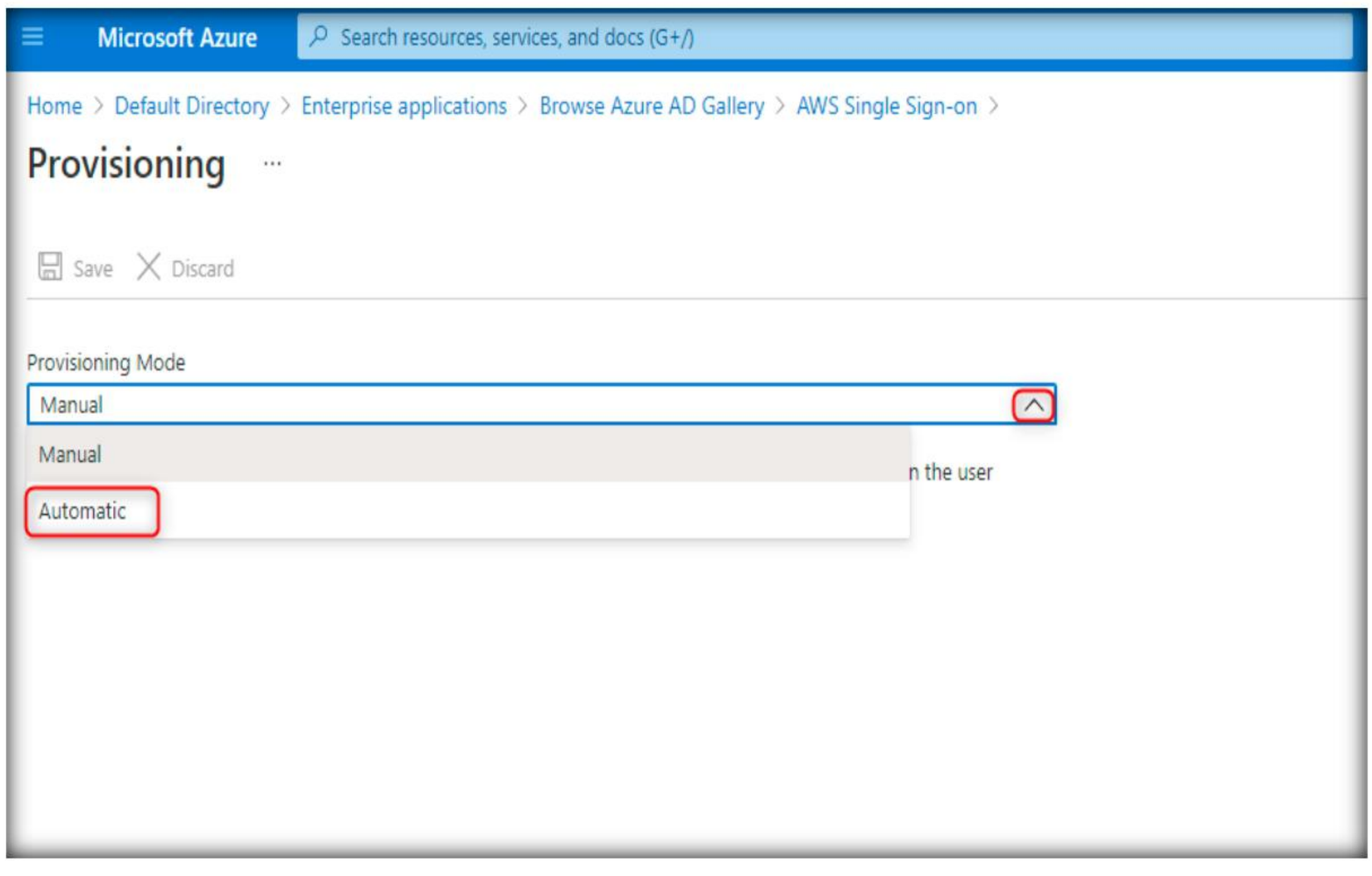


FIGURE 3.2.60: Selecting Automatic Provisioning

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

61. Scroll down. Under **Admin Credentials**, paste the **URL of SCIM endpoint** in the **Tenant URL** field and the **Access token** in the **Secret token** filed from the saved **AWS SCIM and Access Token** notepad file; alternatively, you can copy and paste the same from the **AWS Inbound automatic provisioning** window. Finally, click on **Test Connection**.

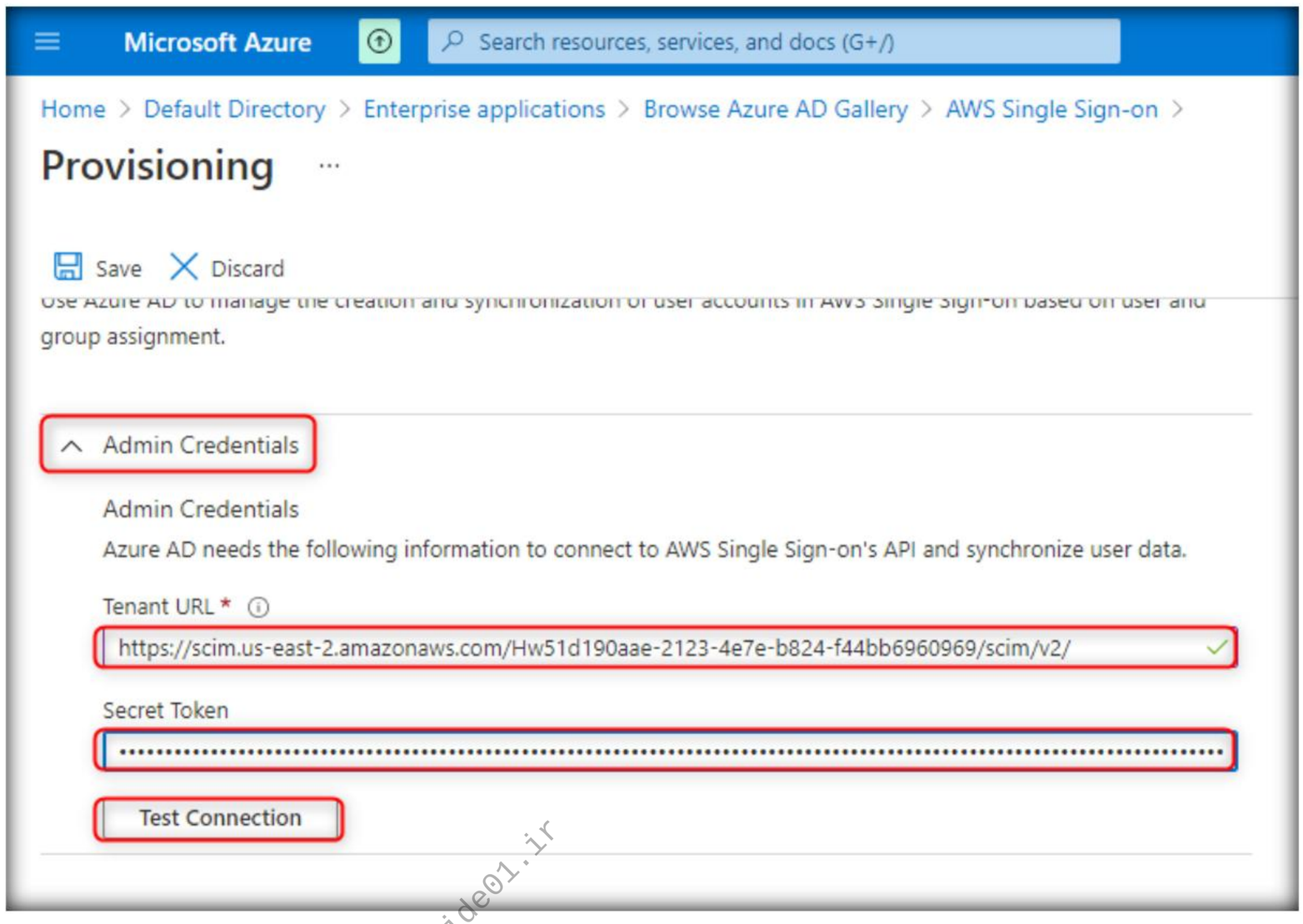


FIGURE 3.2.61: Entering Tenant URL and Secret Token

62. You will see a message stating **The supplied credentials are authorized to enable provisioning**.

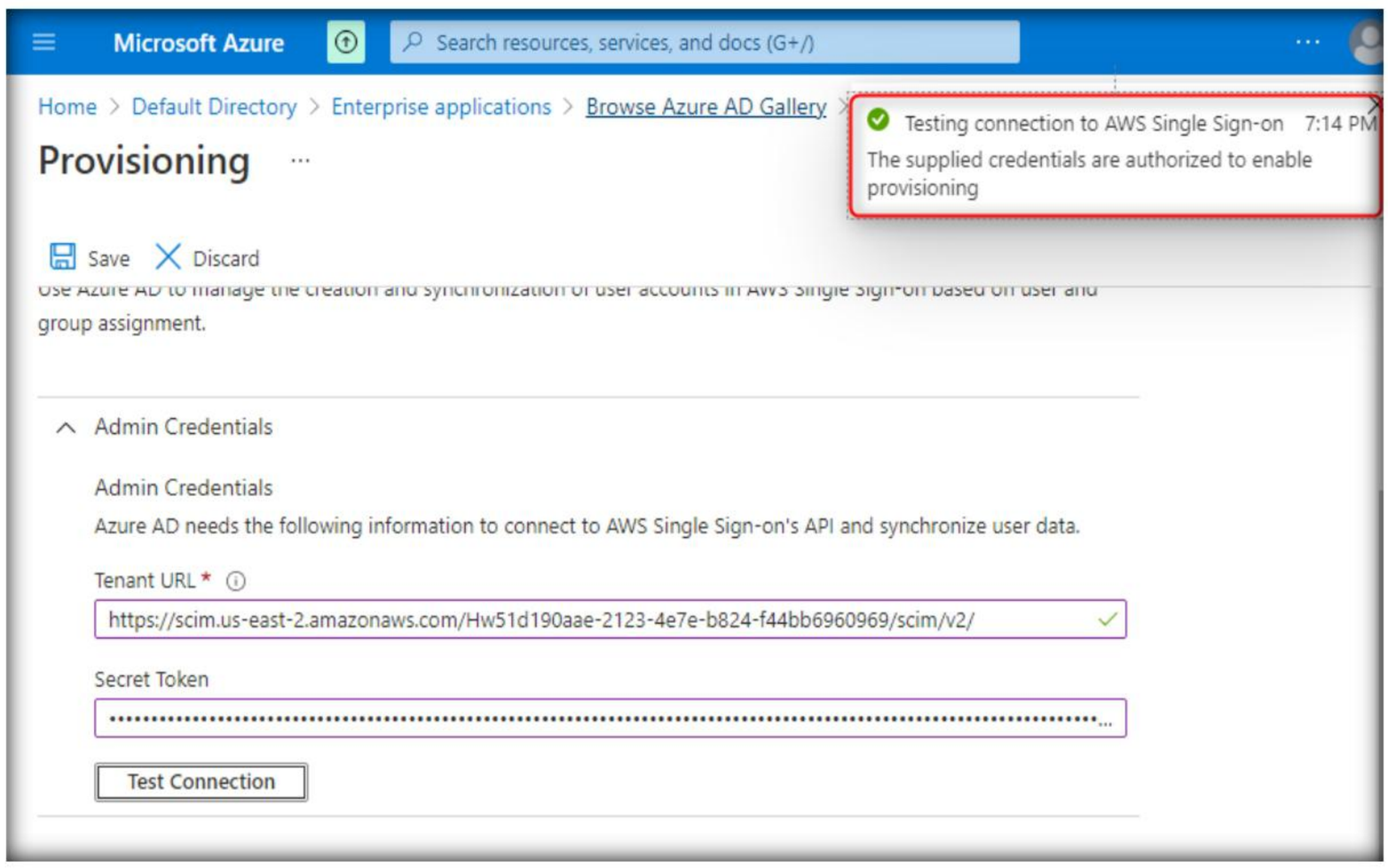


FIGURE 3.2.62: Testing Connection to AWS Single Sign-On

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

63. Click on **Save**.

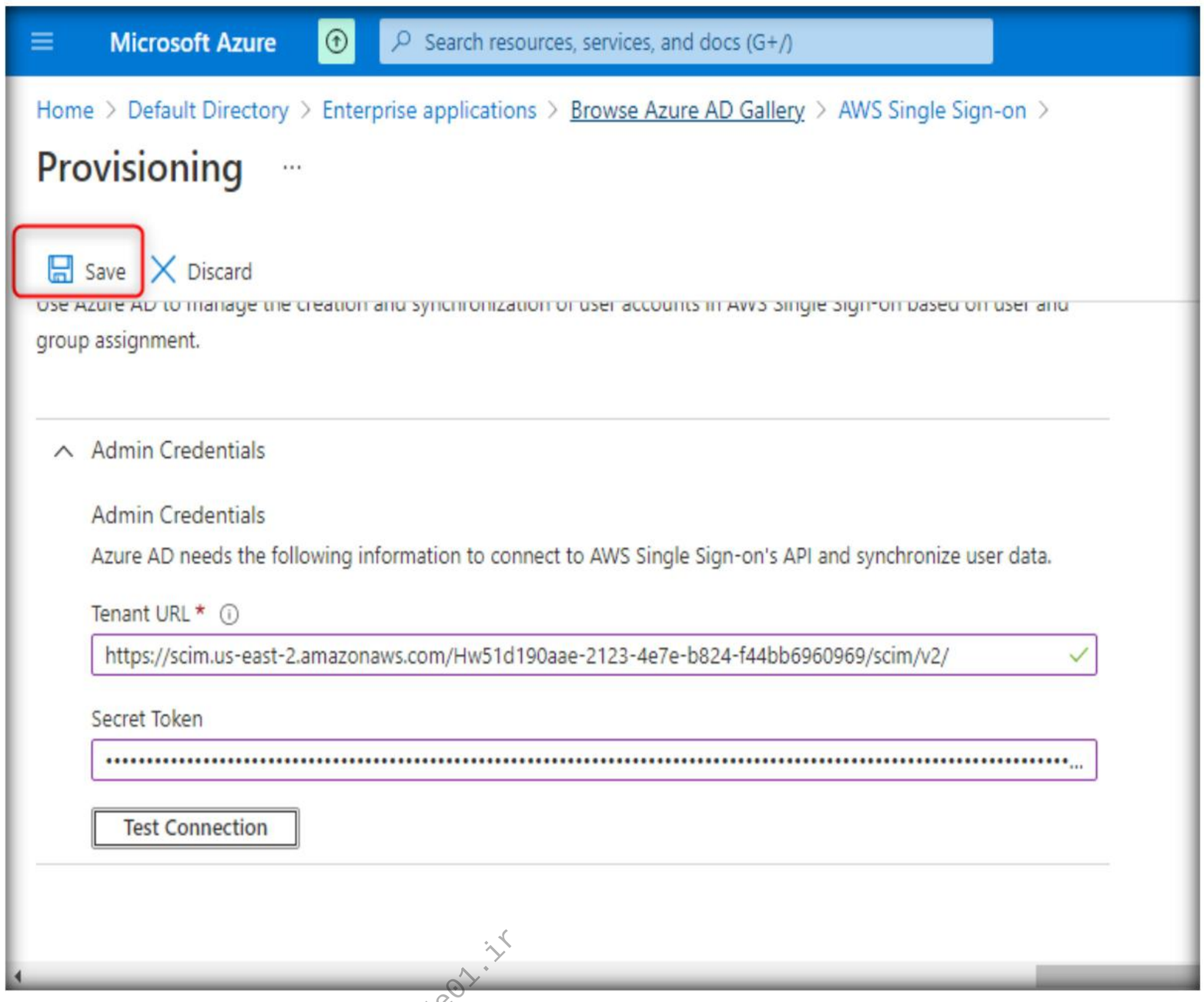


FIGURE 3.2.63: Saving Provisioning Configuration

64. After it is successfully Saved, click on the close symbol.

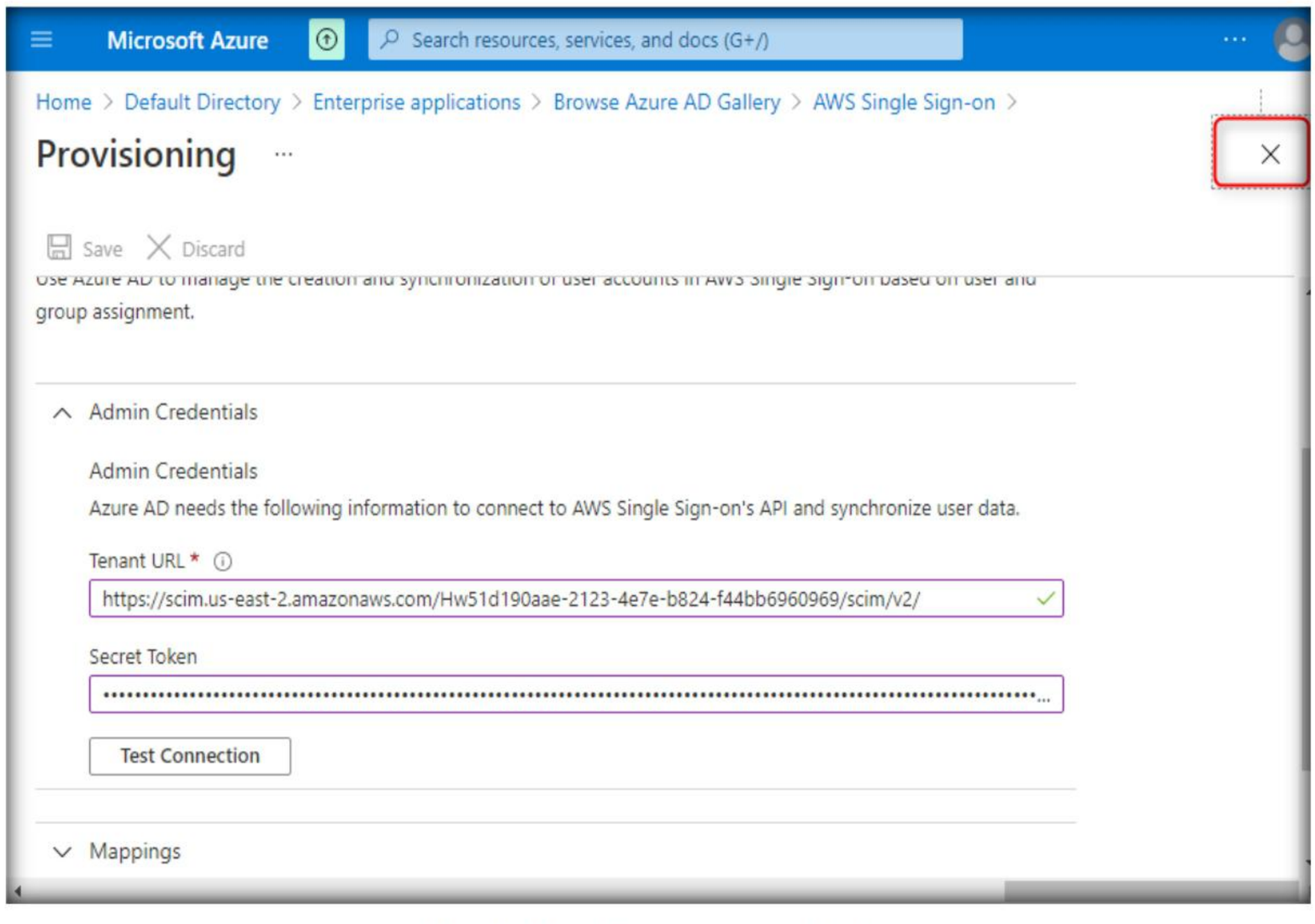


FIGURE 3.2.64: Closing Provisioning Window

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

65. Go back to the AWS tab in the browser. In AWS SSO, **Close** the **Inbound automatic provisioning** window.

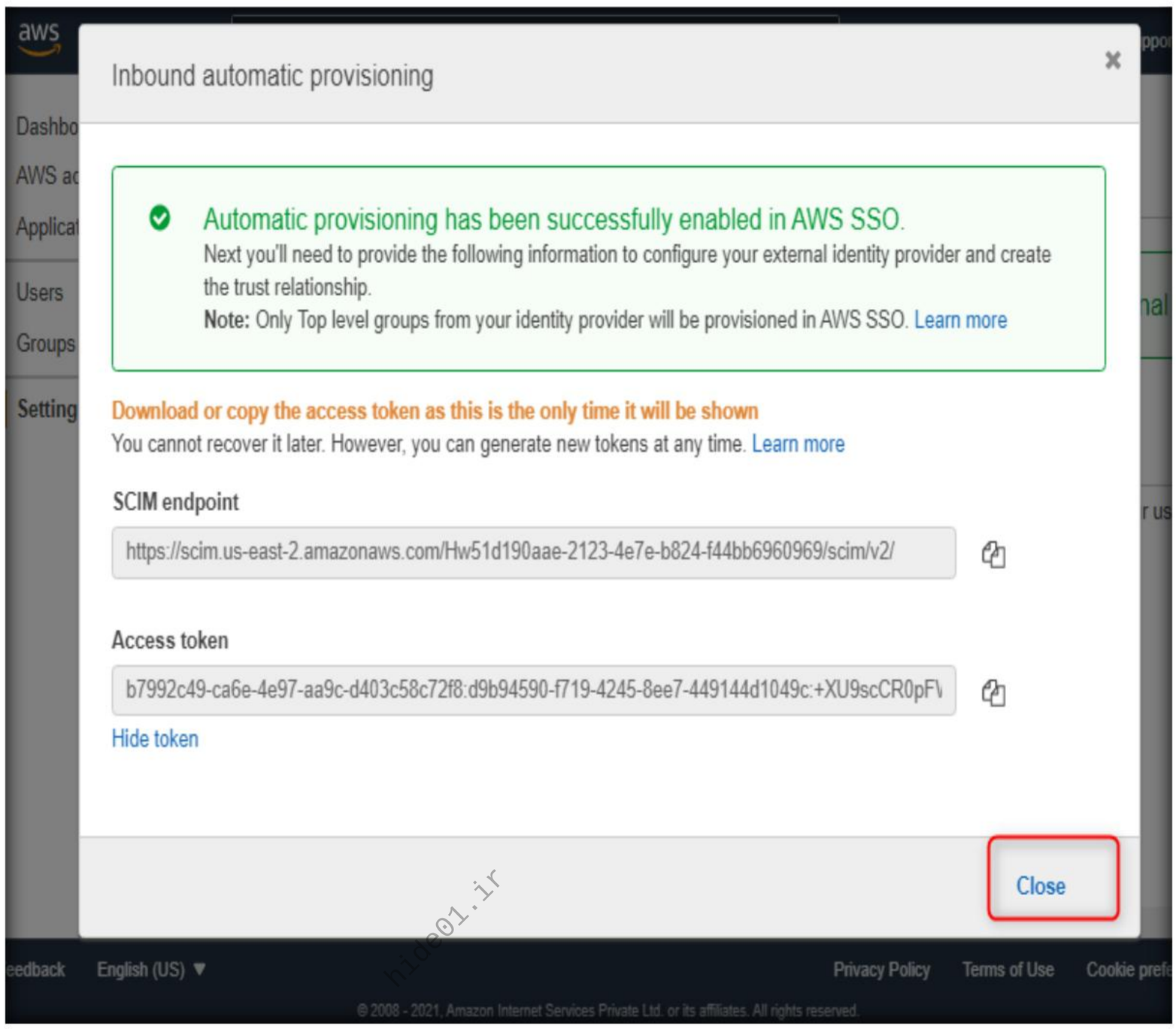


FIGURE 3.2.65: Successfully Enabled Automatic Provisioning in AWS SSO

66. Click on **Users** in the left pane.

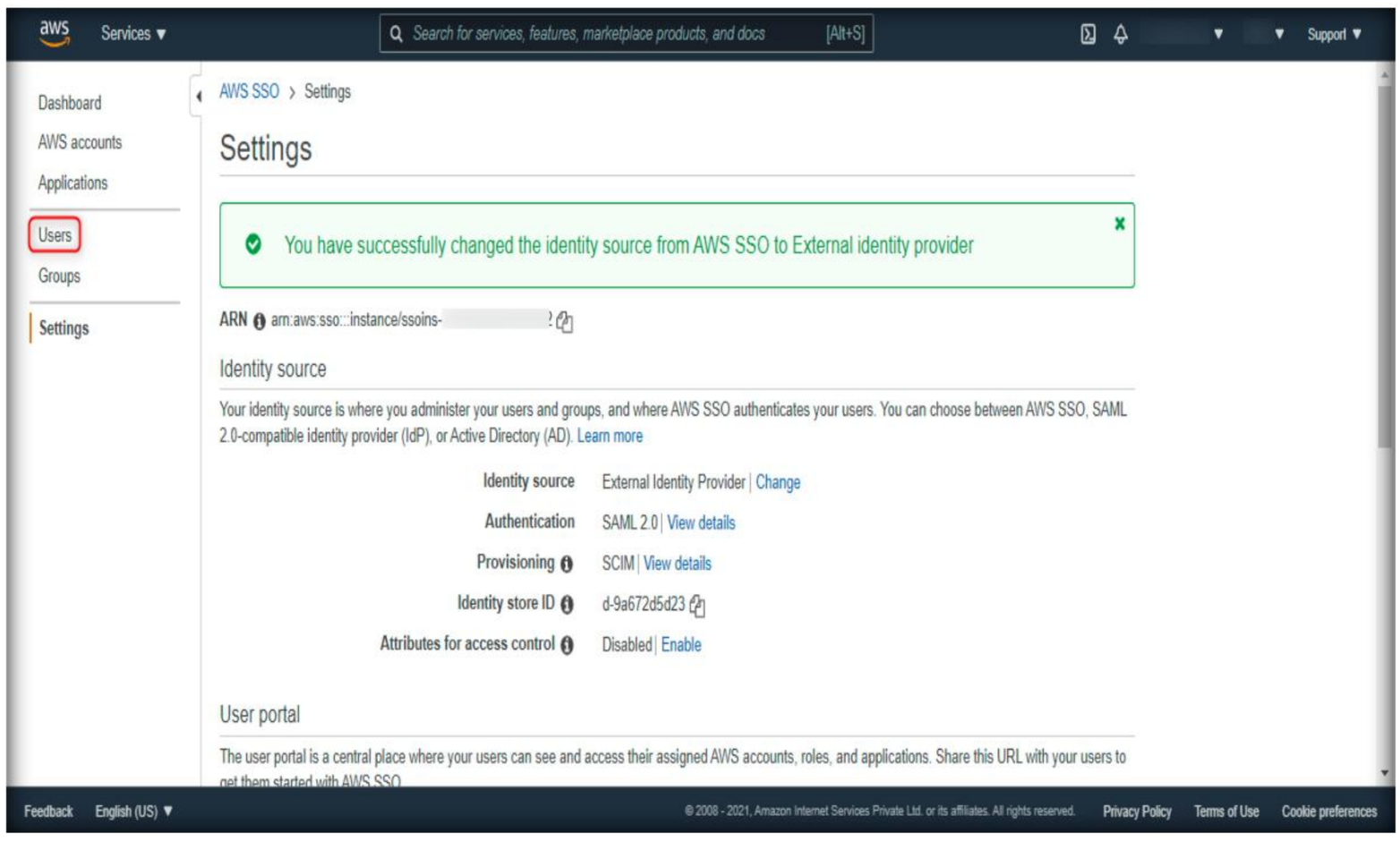


FIGURE 3.2.66: Selecting Users in AWS SSO

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

67. You will observe there are no users at this time.

    Note: Do not close this AWS window after this step. Go directly to the next step.

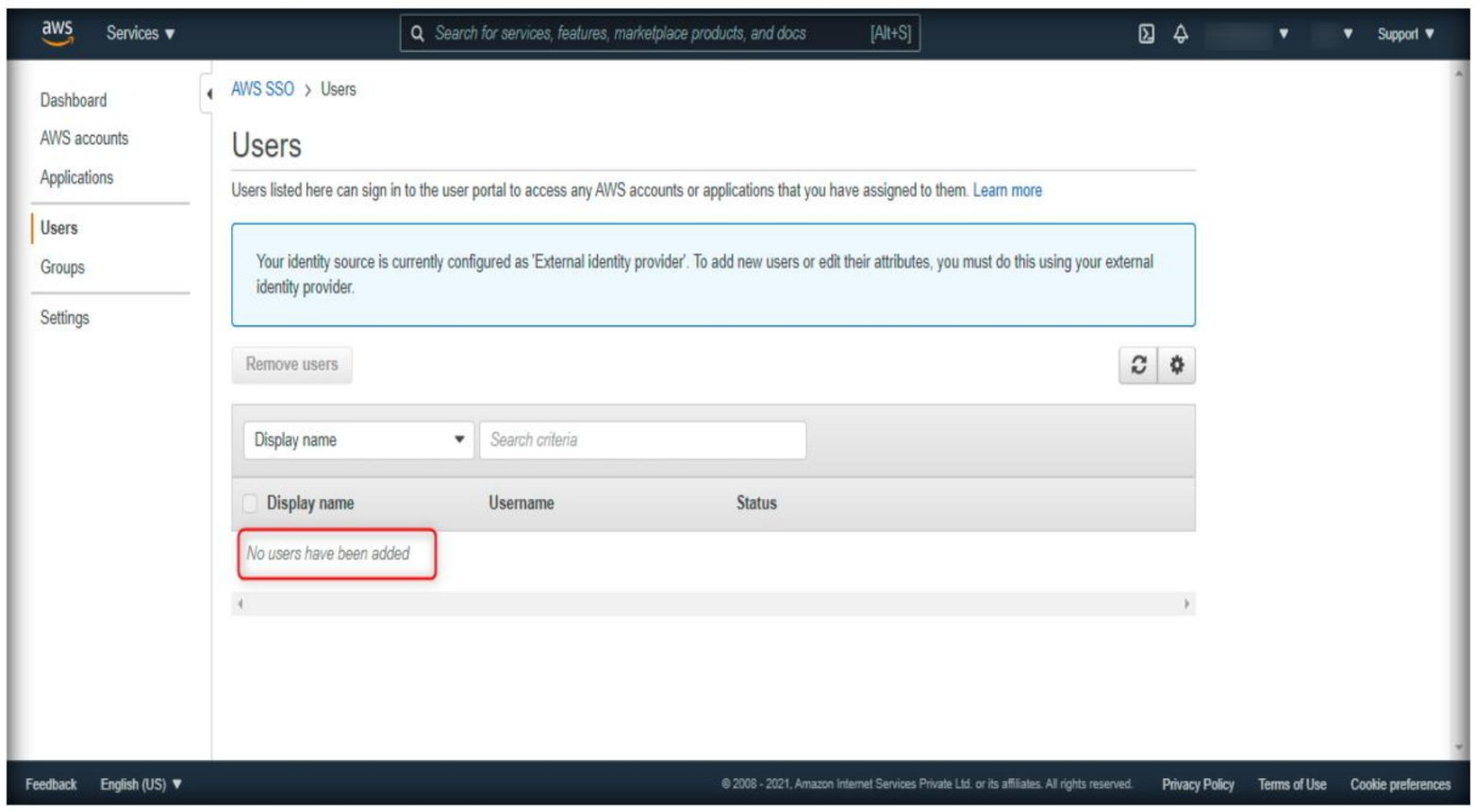


FIGURE 3.2.67: No Users are Listed

68. Go back to Azure Portal. In the **AWS SSO – Provisioning** window in Azure, click on **Start provisioning**.

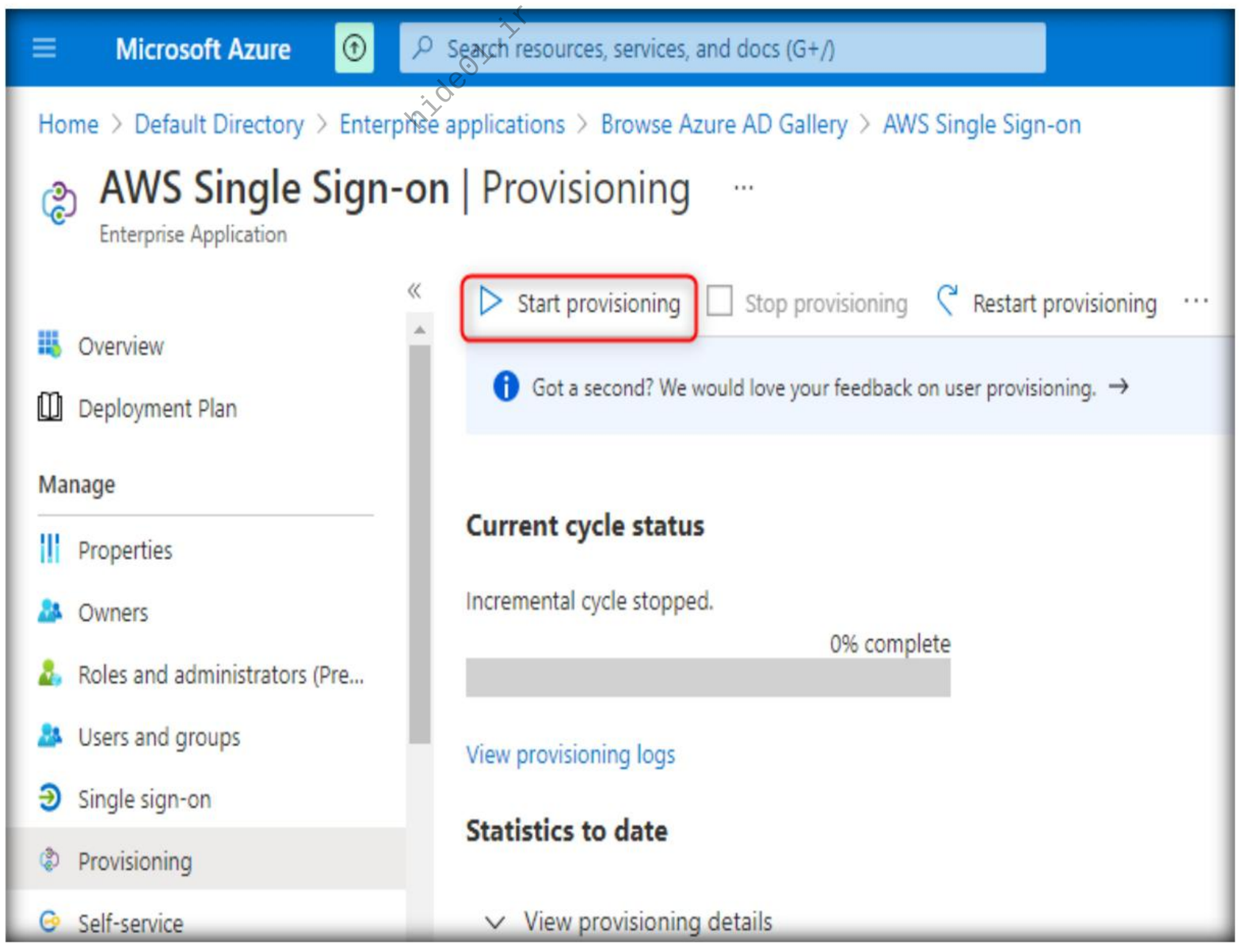


FIGURE 3.2.68: Starting Provisioning in Azure AWS Single Sign-On

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

69. Within 30–60 seconds, you will see a message that the initial cycle will be completed. Click on **View provisioning details** under **Statistics to date.** You can observe that a steady state has been achieved.

    Note: If provisioning is not completed after 60–120 seconds, click on **Stop provisioning**, and then click on **Start provisioning** again.

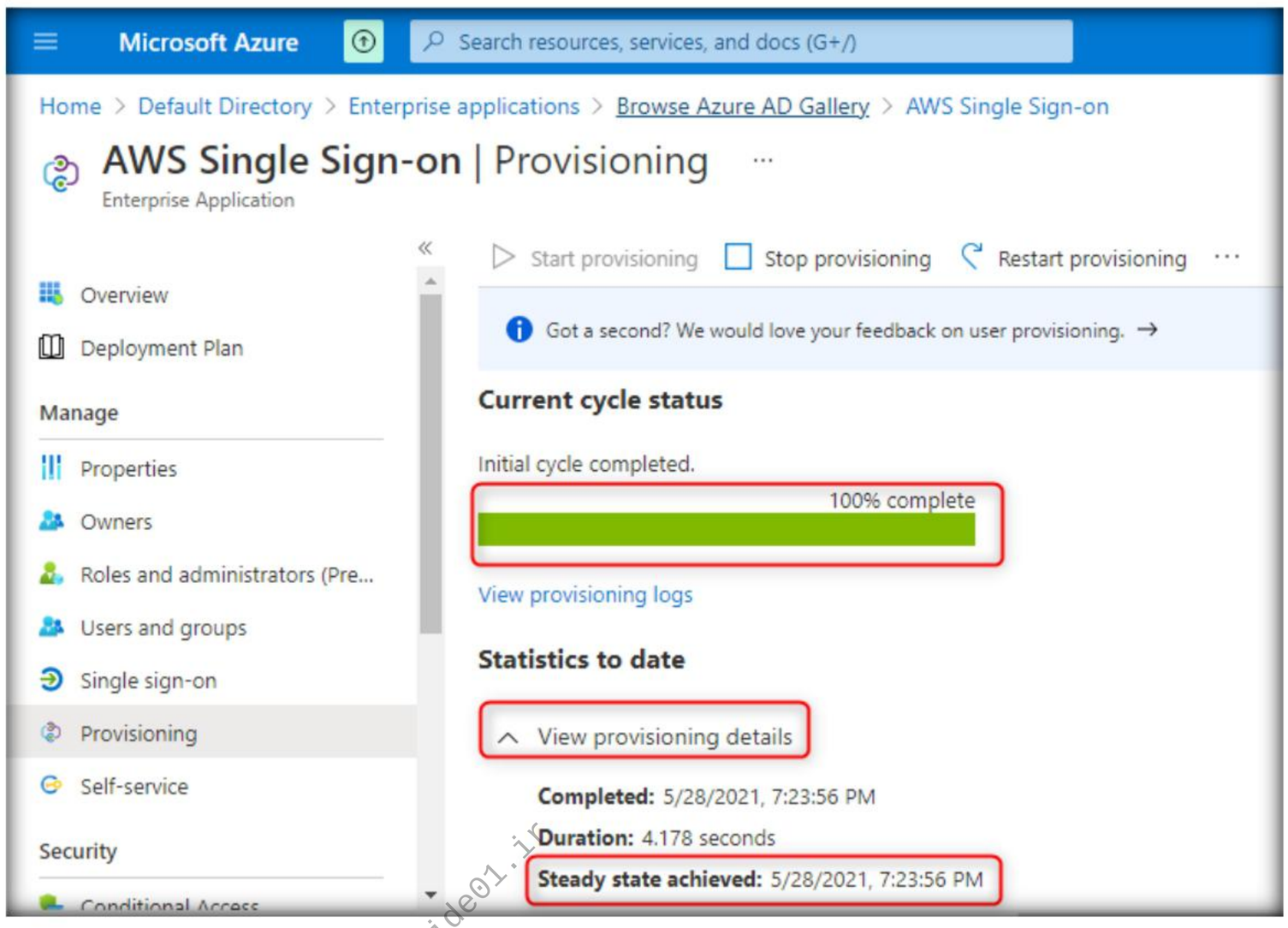


FIGURE 3.2.69: Completion of Initial Provisioning Cycle

70. Now, click on **Users and groups** under **Manage** in the left pane to add a user to Azure **AWS Single Sign-on**.

TASK 6

Adding User to Azure AWS Single Sign-On

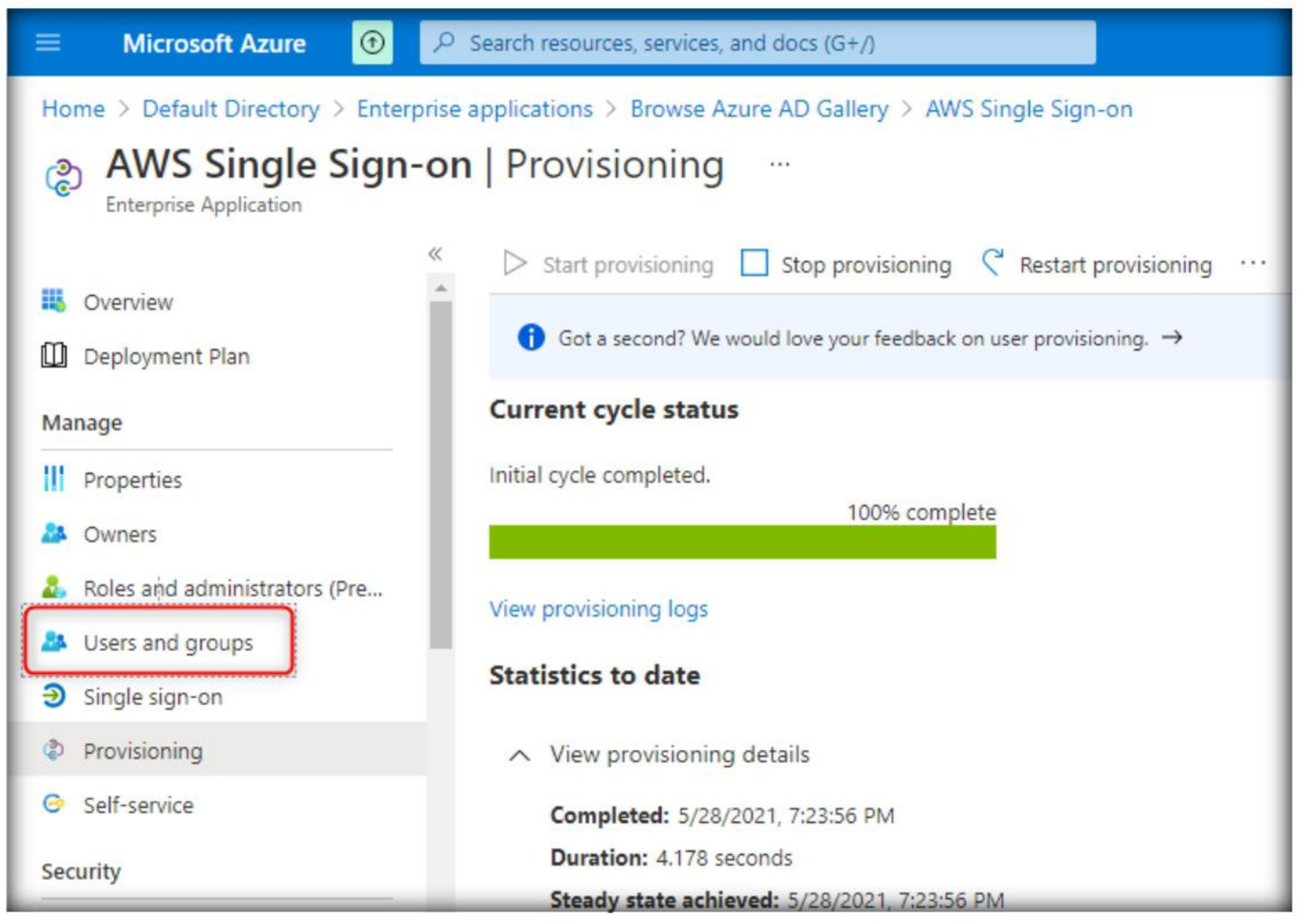


FIGURE 3.2.70: Assigning User

Certified Cloud Security Engineer Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

71. In the **Users and groups** page, click on **+ Add user/group**.

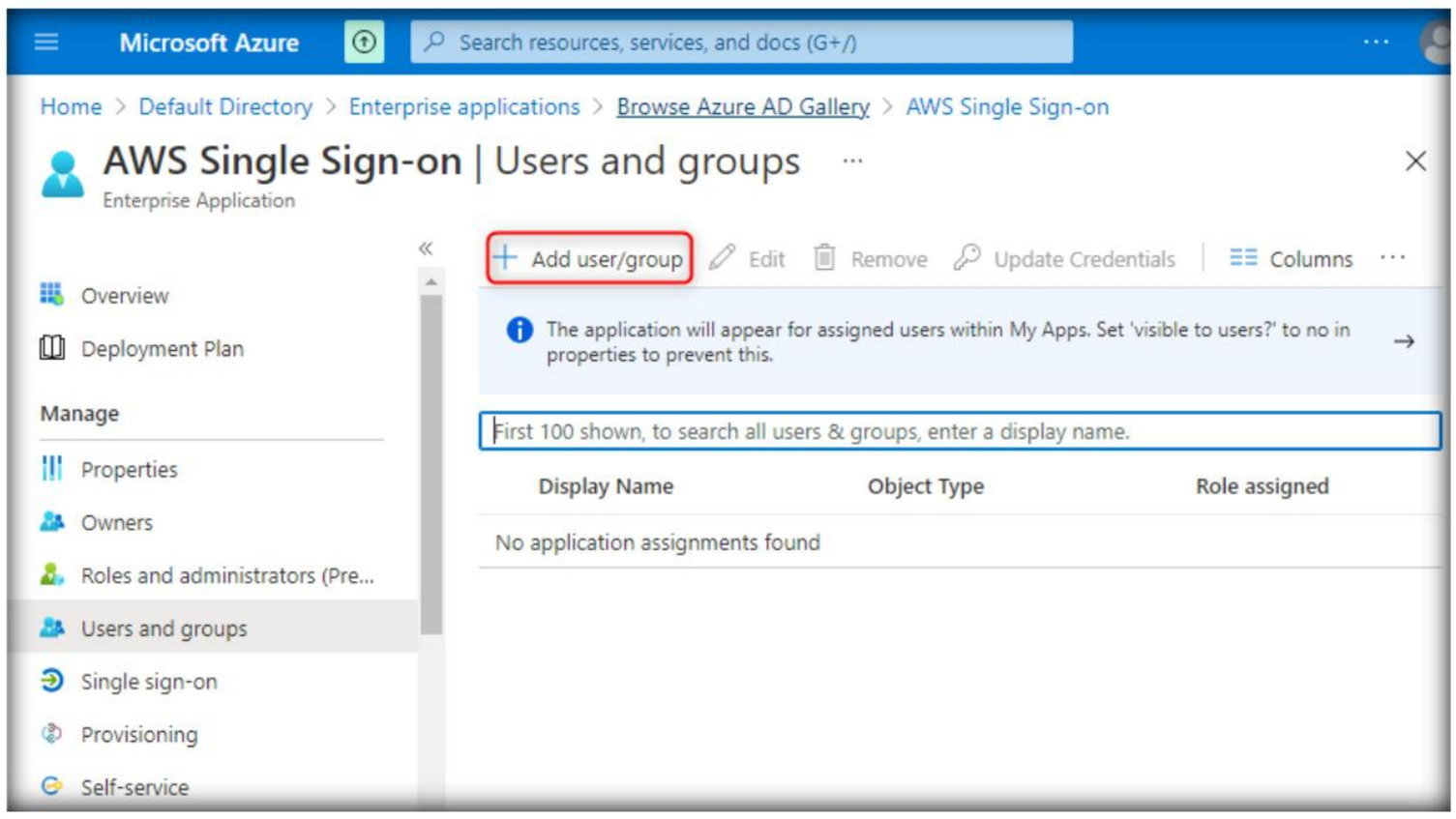


FIGURE 3.2.71: Adding a User

72. In the **Add Assignment** window, click on **None Selected**.

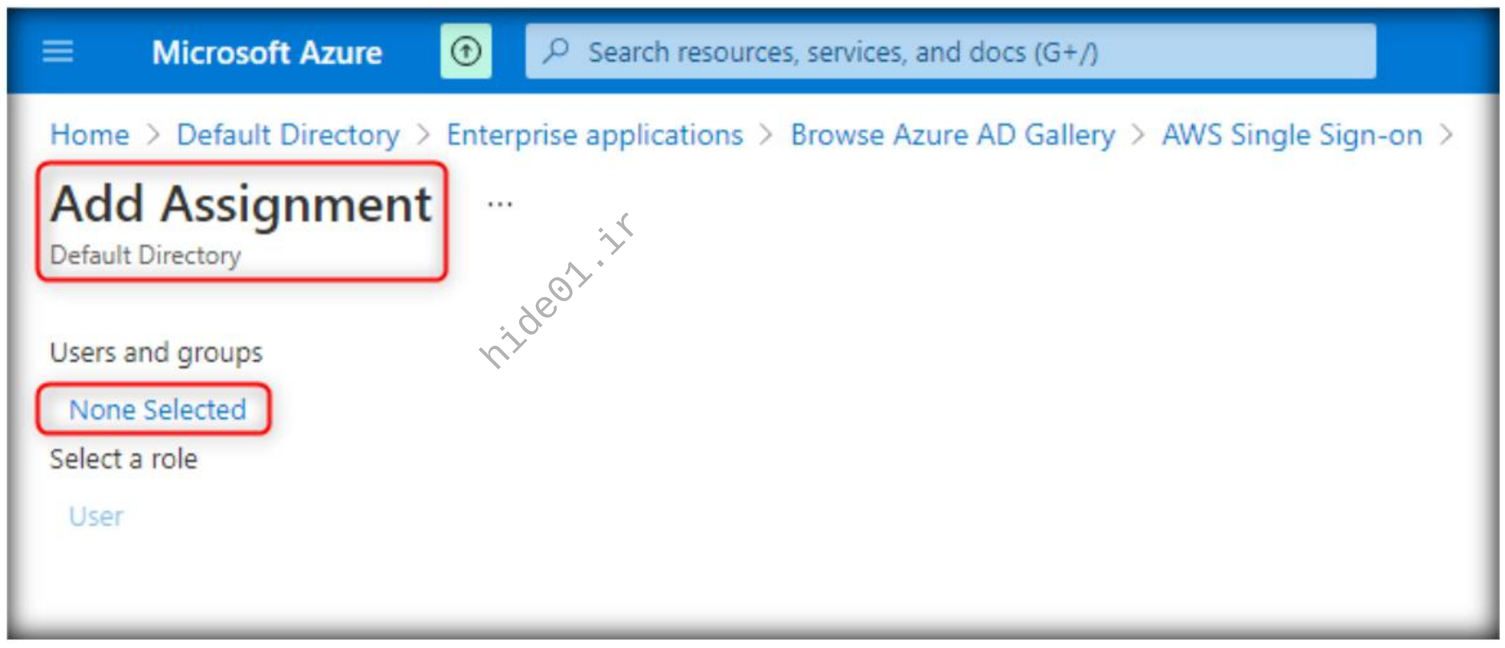


FIGURE 3.2.72: Selecting a User

73. **Users and groups** window will now open on the right pane. Select **Bob Green** user and then click on **Select** at the bottom.

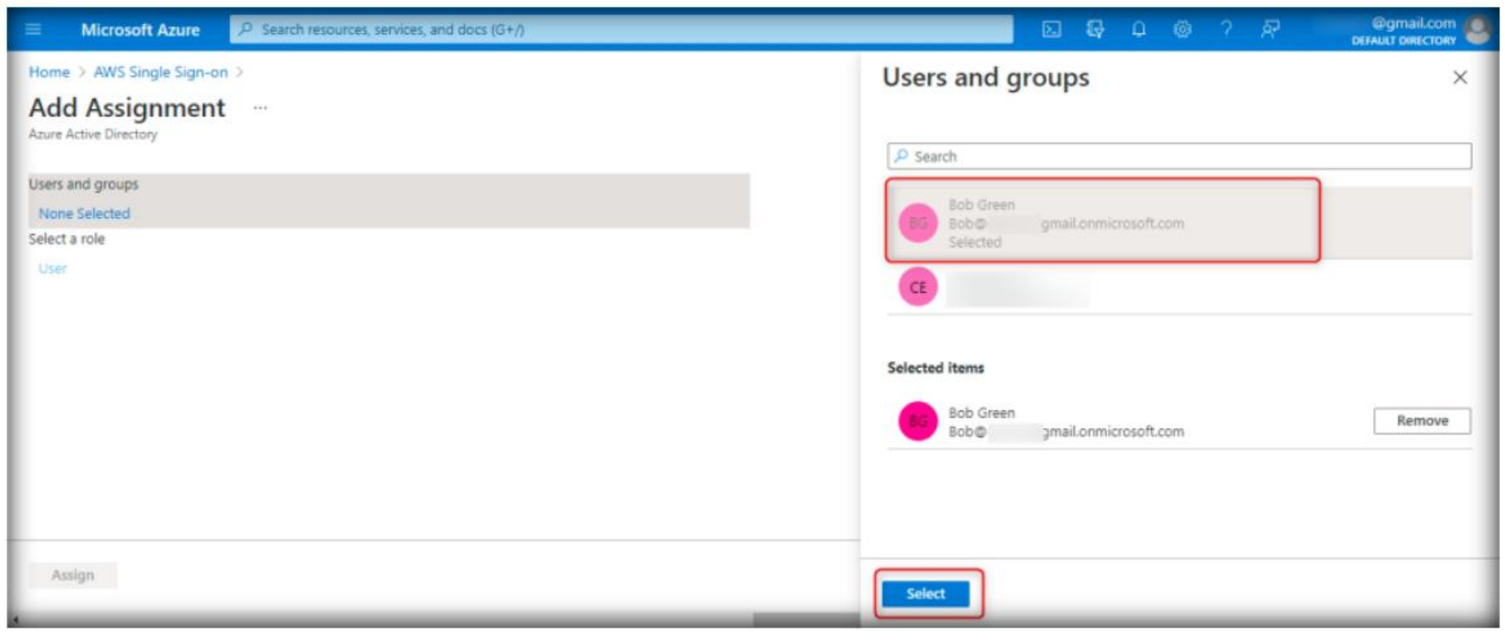


FIGURE 3.2.73: Selecting Bob Green User

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

74. In the **Add Assignment** window, you will see **1 user selected**. Now, click on **Assign**.

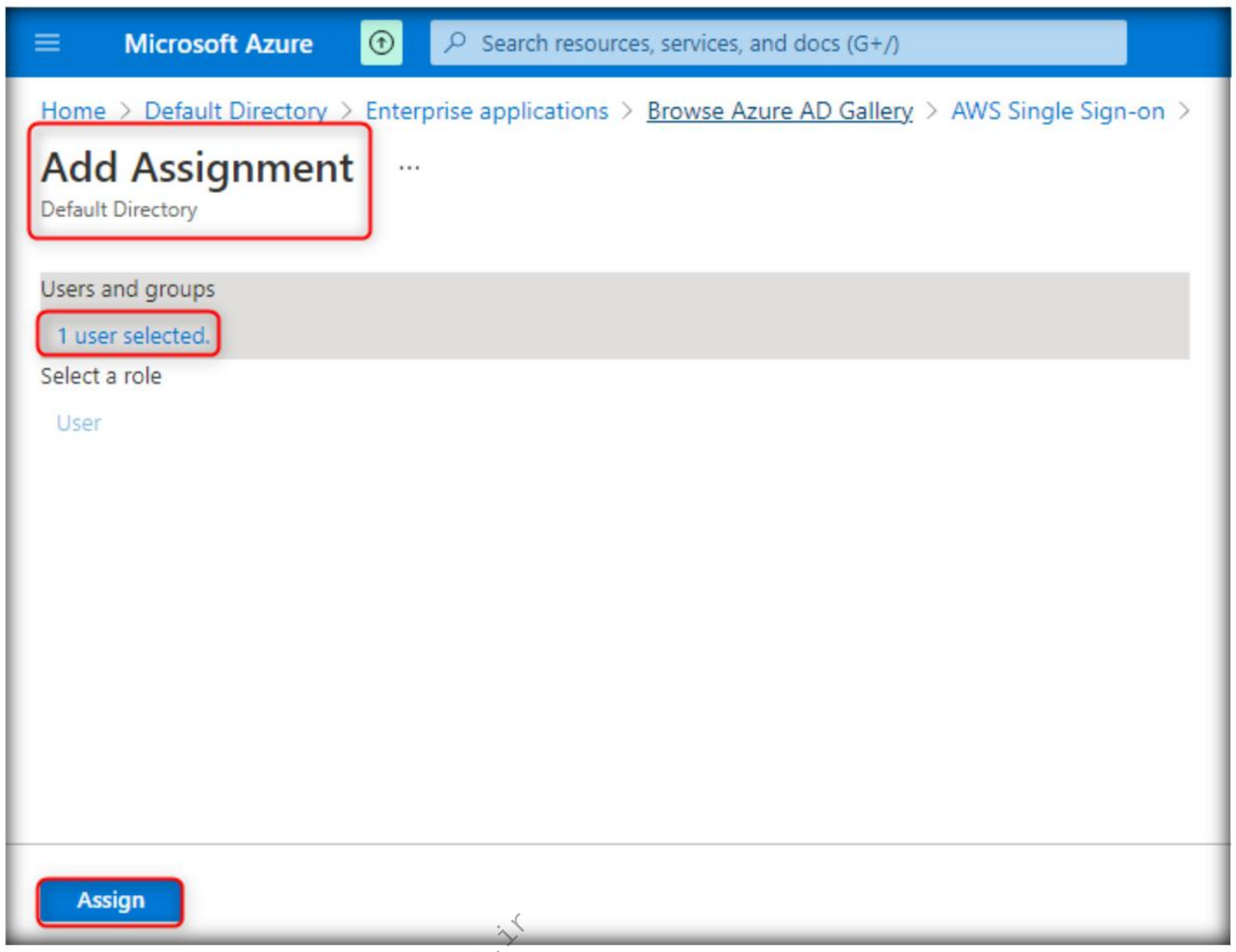


FIGURE 3.2.74: Assigning the User

hide01.ir

75. **Bob Green** is now successfully assigned to the application.

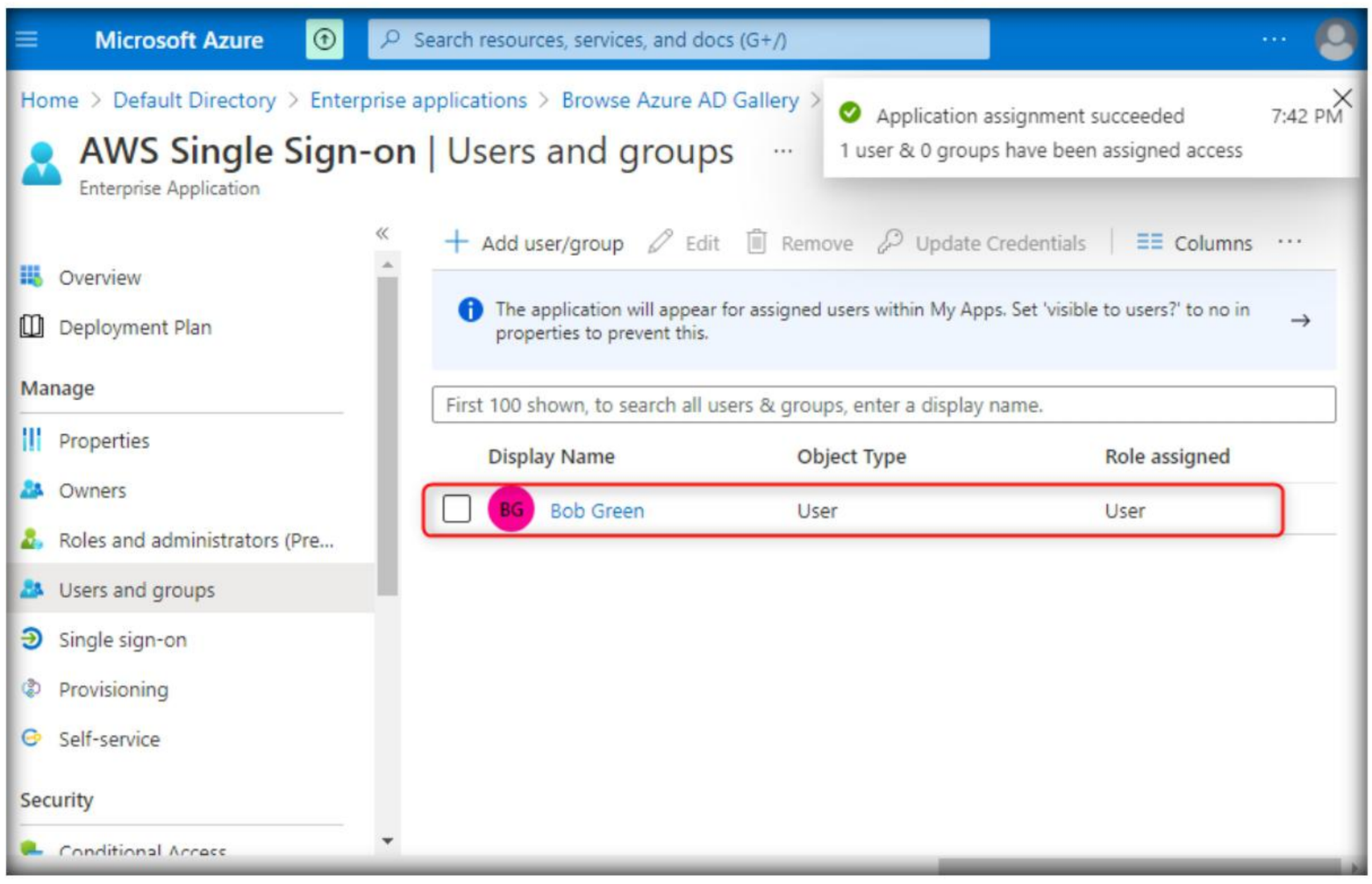


FIGURE 3.2.75: User is Successfully Assigned to Application

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

76. Click on the following notification at the top: **The application will appear for assigned users within My Apps. Set 'visible to users?' to no in properties to prevent this.**

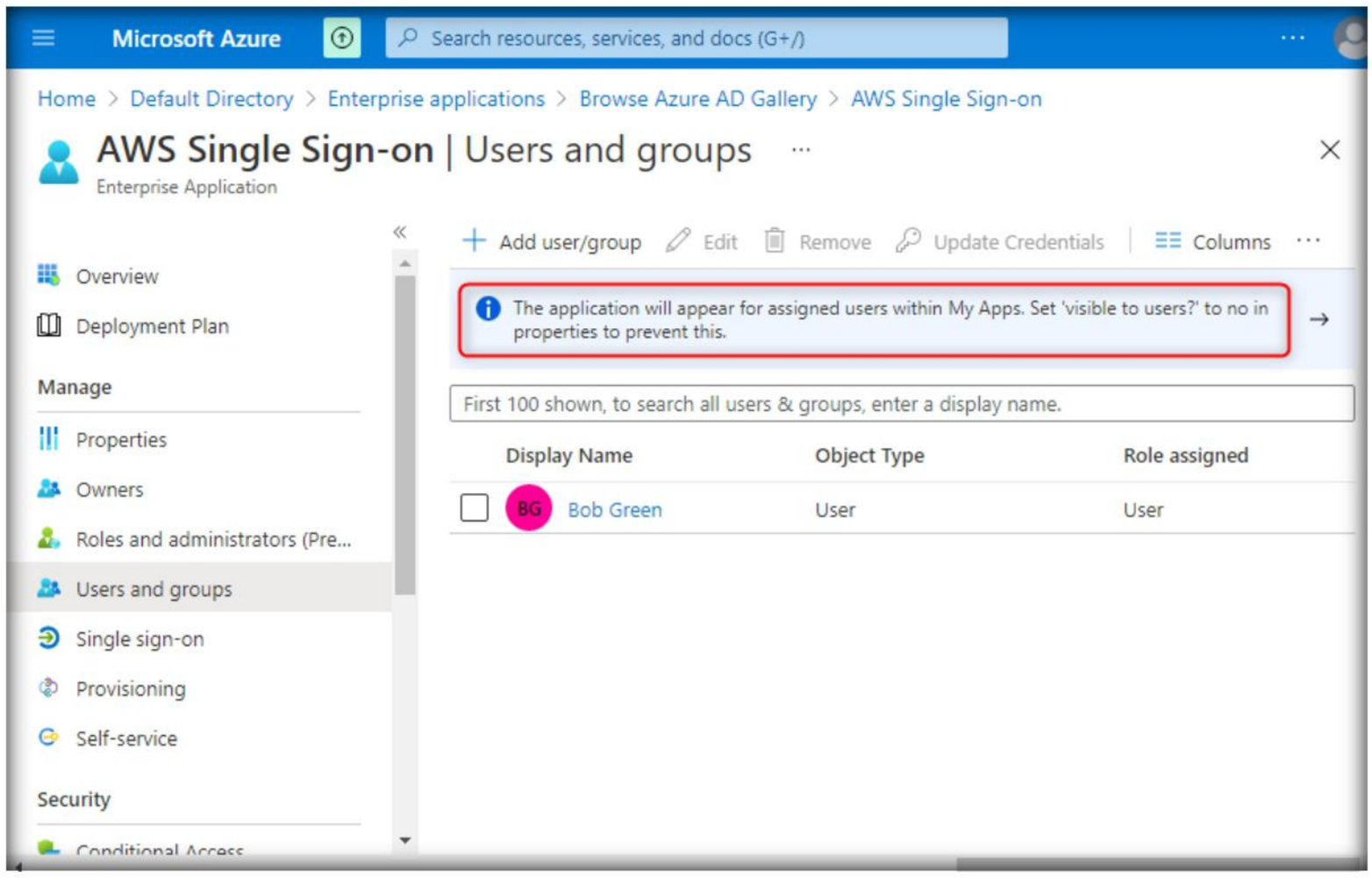


FIGURE 3.2.76: Checking the Notification

77. The **Properties** page will open.

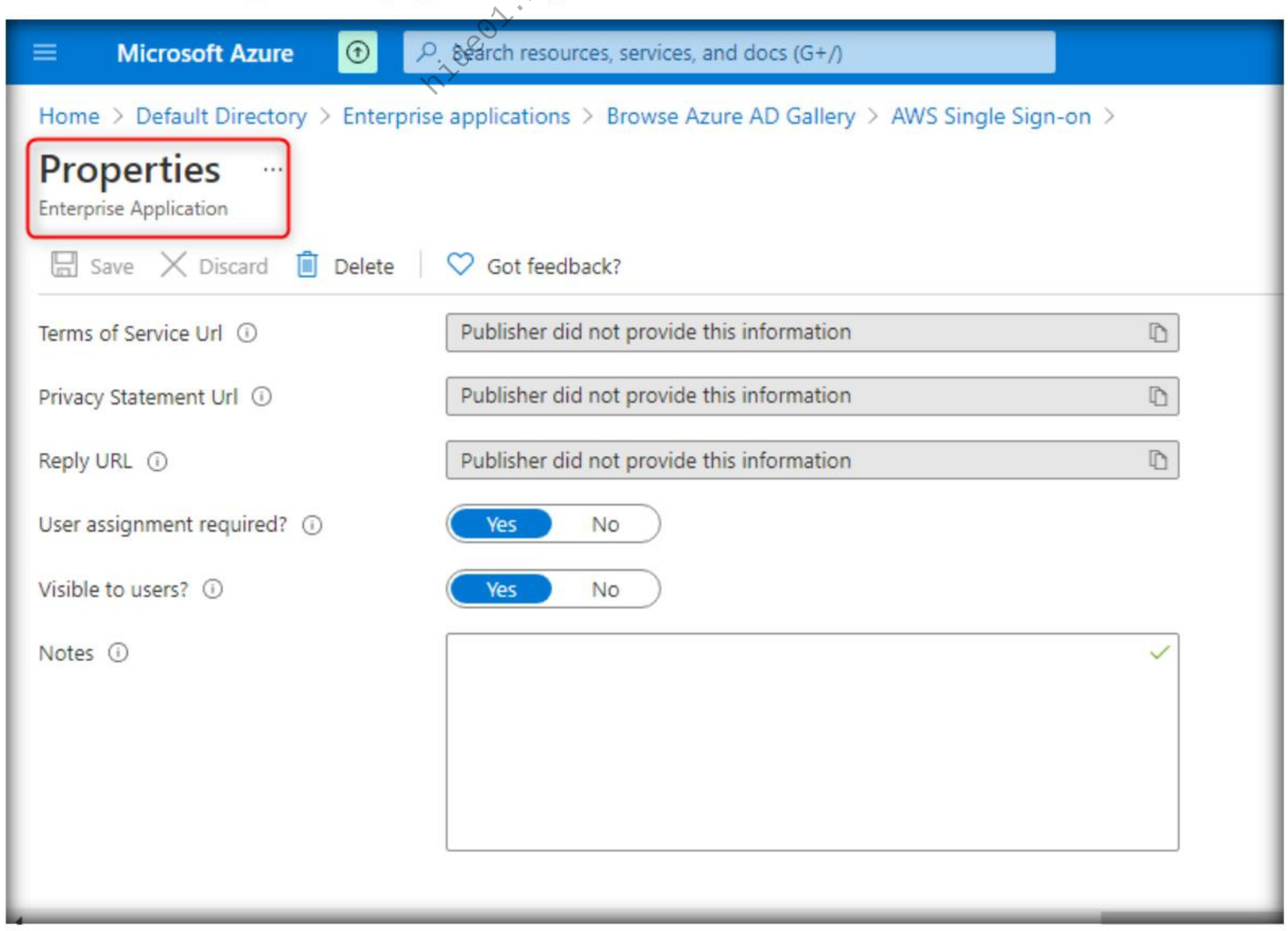


FIGURE 3.2.77: Opening Properties Page

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

78. Scroll down and change the toggle to **No** for **Visible to users?**. Then, click on the **Save** button.

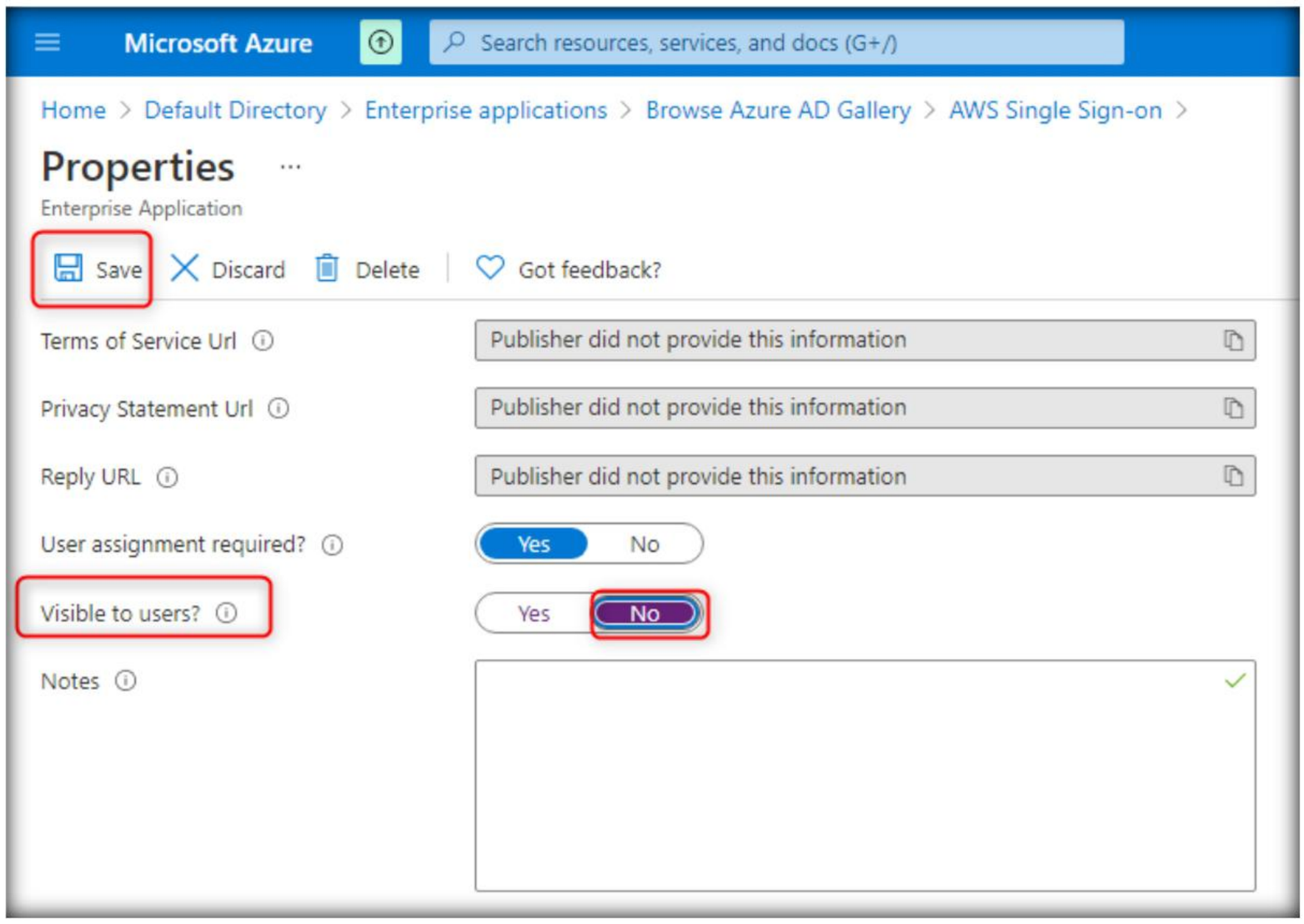


FIGURE 3.2.78: Saving the Settings

79. The application is successfully updated.

Note: Do not close this Azure window after this step. Go directly to the next step.

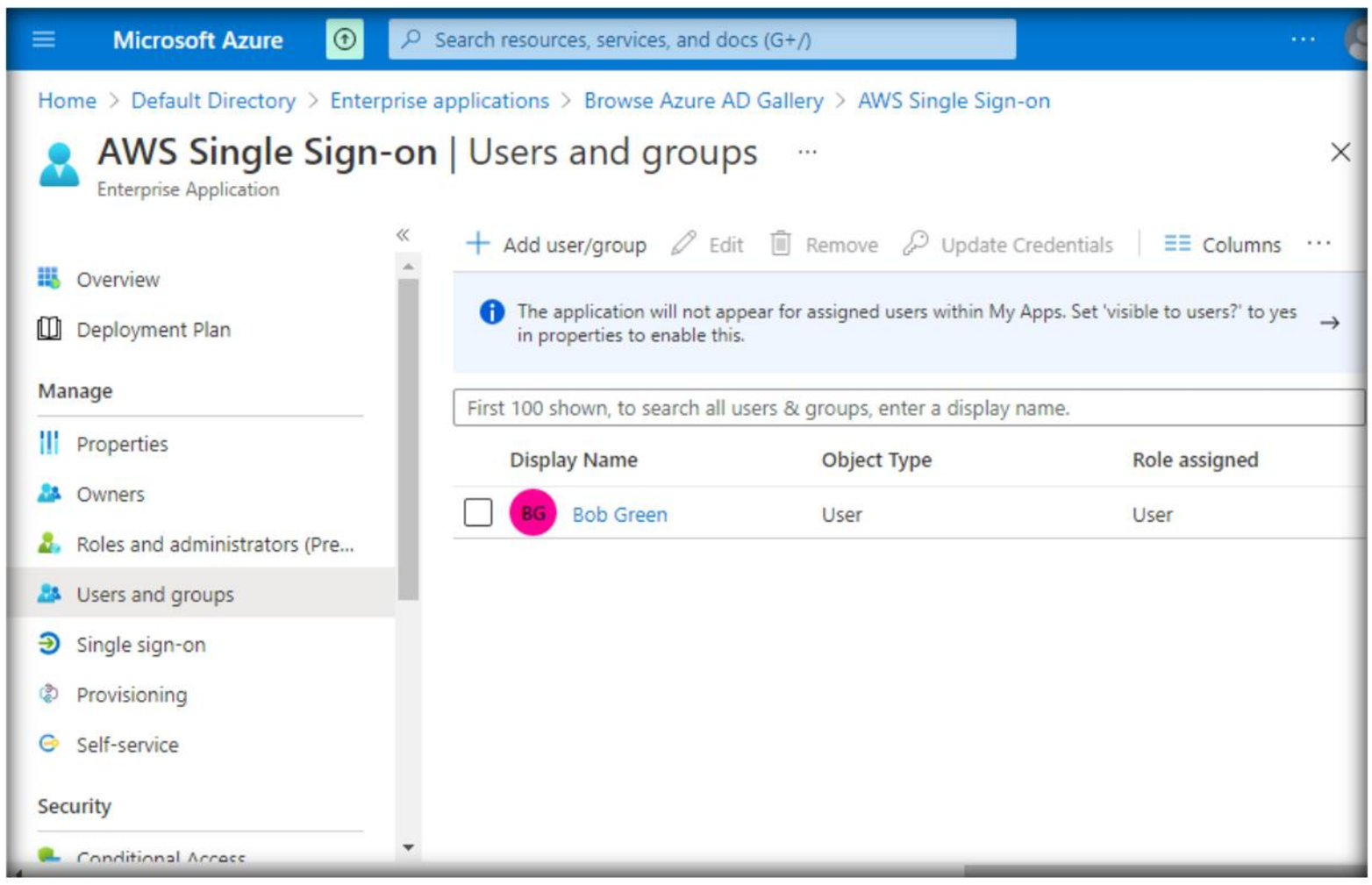


FIGURE 3.2.79: Successfully Updated the Application

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

80. Now, go back to the AWS tab in the browser. In the **AWS SSO Users** window, click on the **refresh** icon.

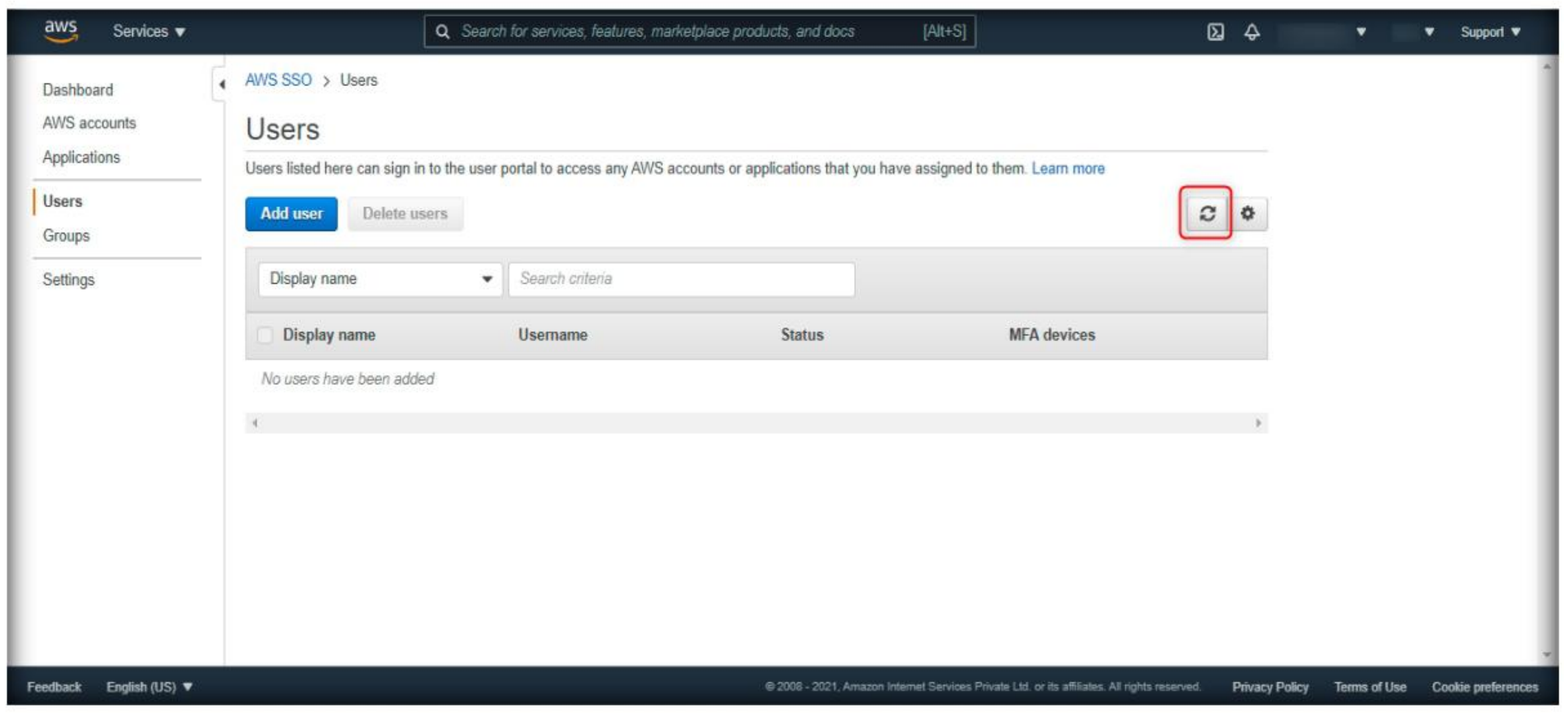


FIGURE 3.2.80: Refreshing AWS SSO Users Window

81. The user **Bob Green** is now successfully enabled in A**WS SSO**.

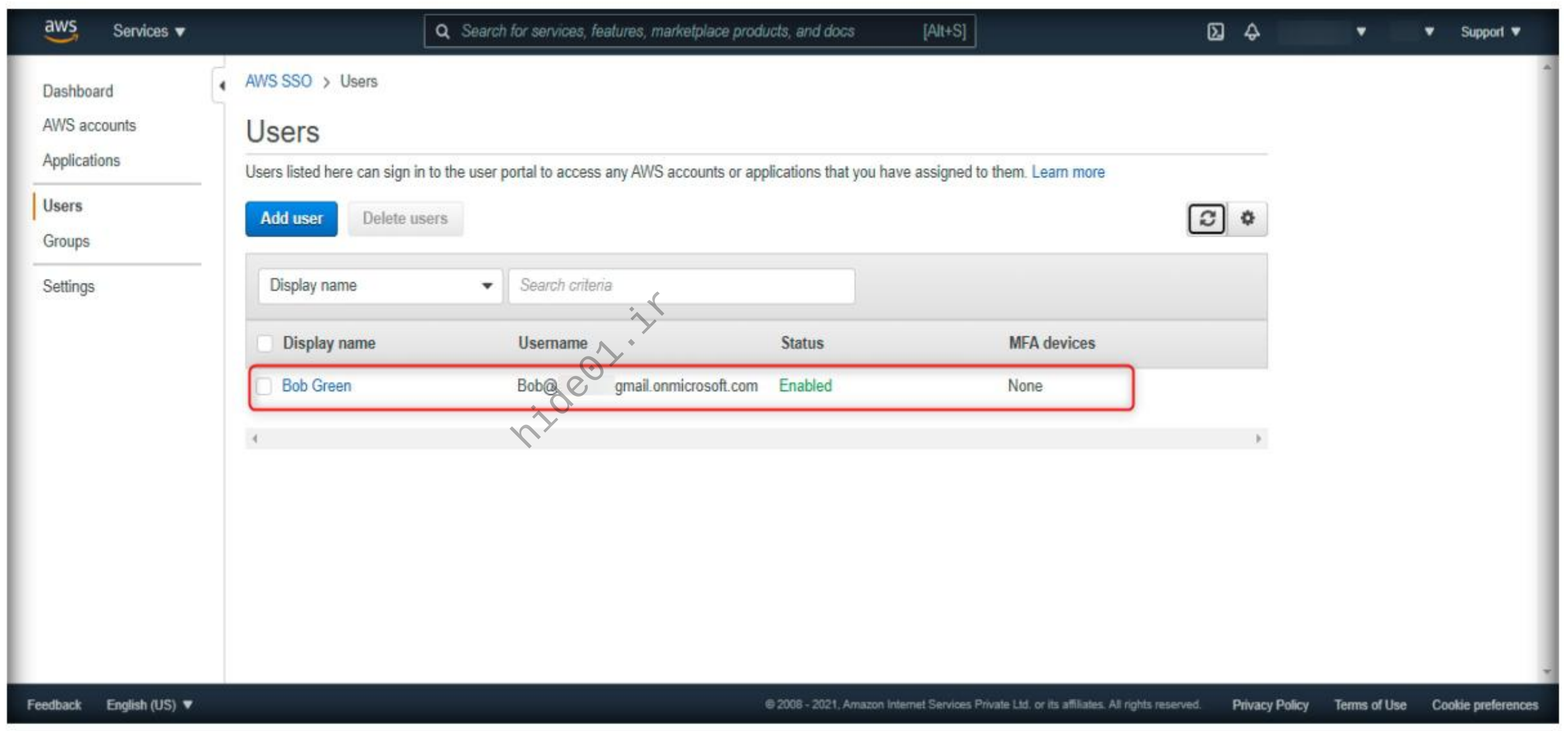


FIGURE 3.2.81: User is Listed in AWS SSO

82. Now, click on **AWS accounts**.

TASK 7

Assigning User and Creating New Permission Set

FIGURE 3.2.82: Selecting AWS accounts in AWS SSO

Certified Cloud Security Engineer Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

83. In **AWS accounts**, select the checkbox for the root user under the **AWS organization** tab, and then click on **Assign users**.

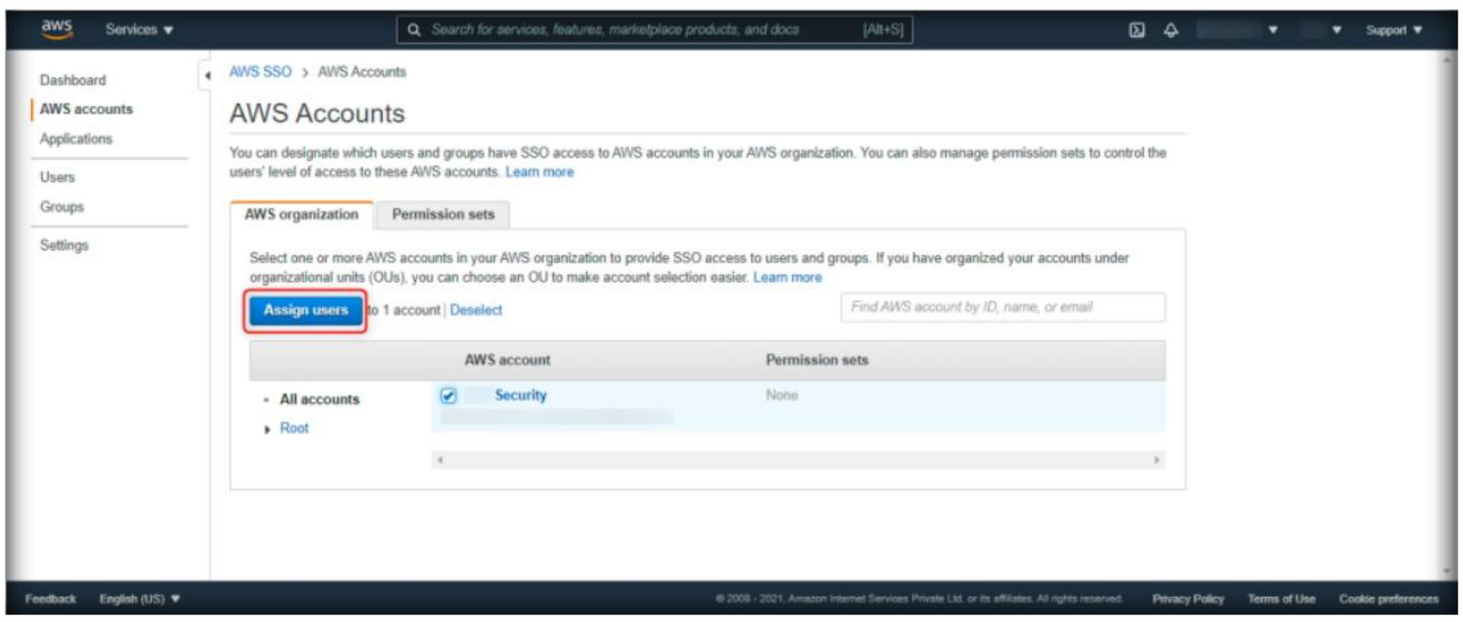


FIGURE 3.2.83: Assigning User in AWS Accounts

84. Select the checkbox for user **Bob Green** and then click on **Next: Permission sets.**

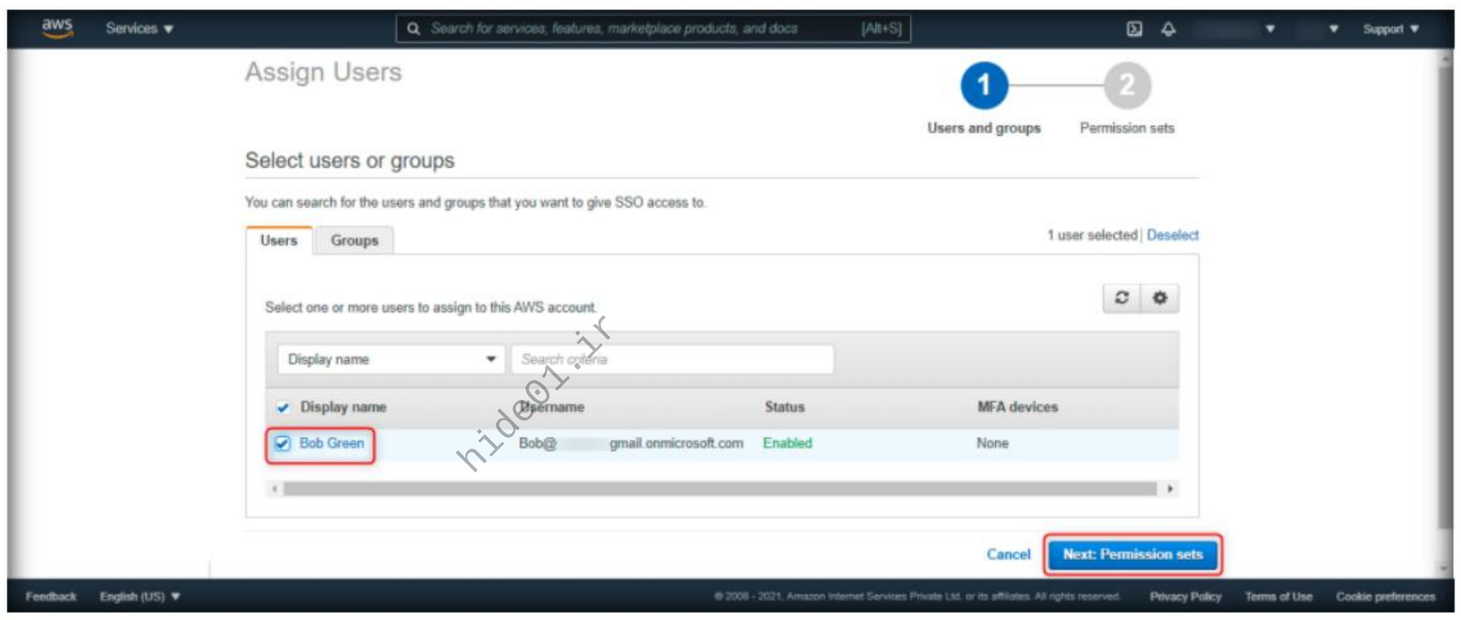


FIGURE 3.2.84: Selecting User and Moving to Permission Sets

85. Click on **Create new permission set.**

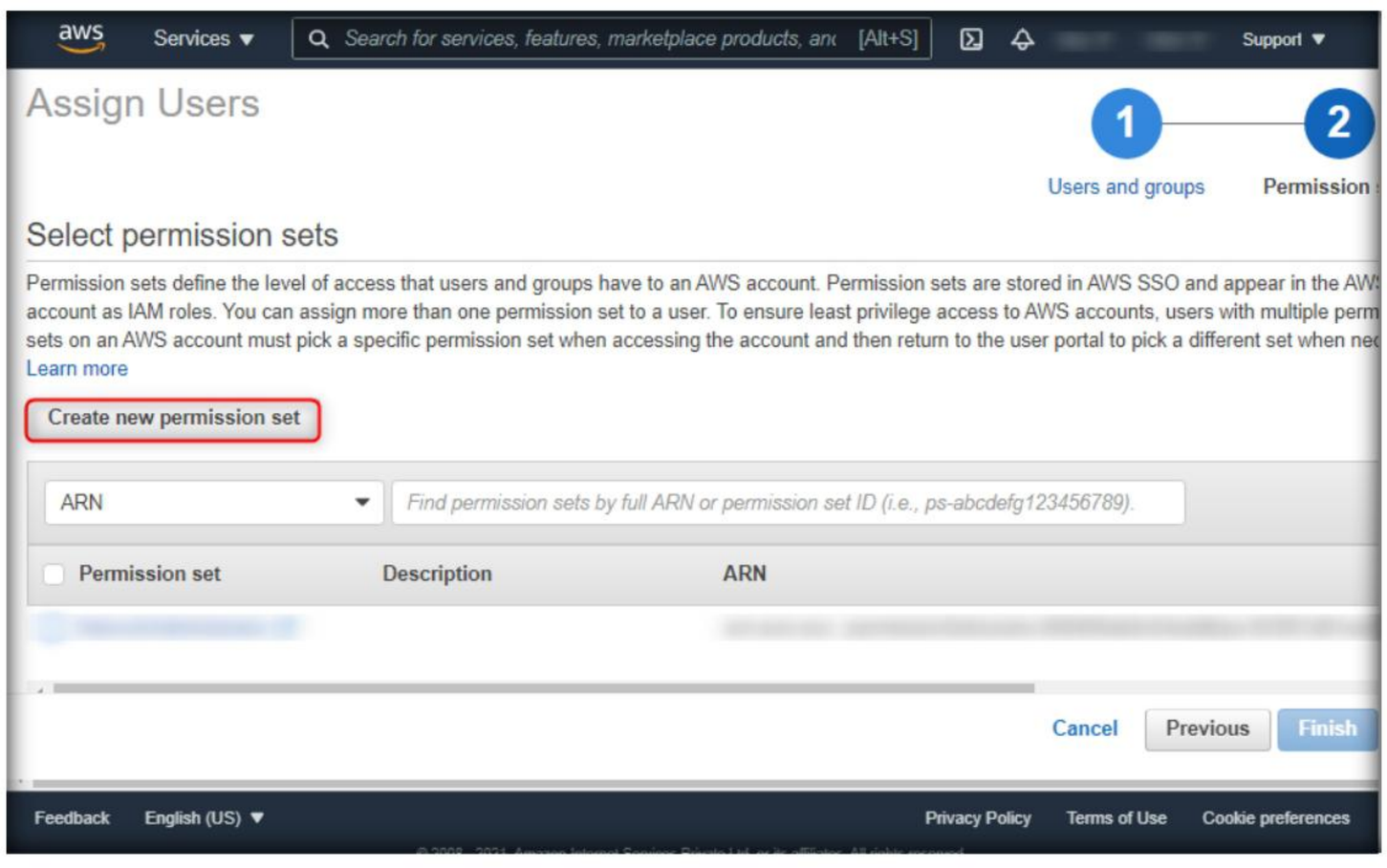


FIGURE 3.2.85: Creating New Permission Set

Certified Cloud Security Engineer Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

86. A new window will open for creating new permissions. Here, select the **Use an existing job function policy** radio button and click on **Next: Details**.

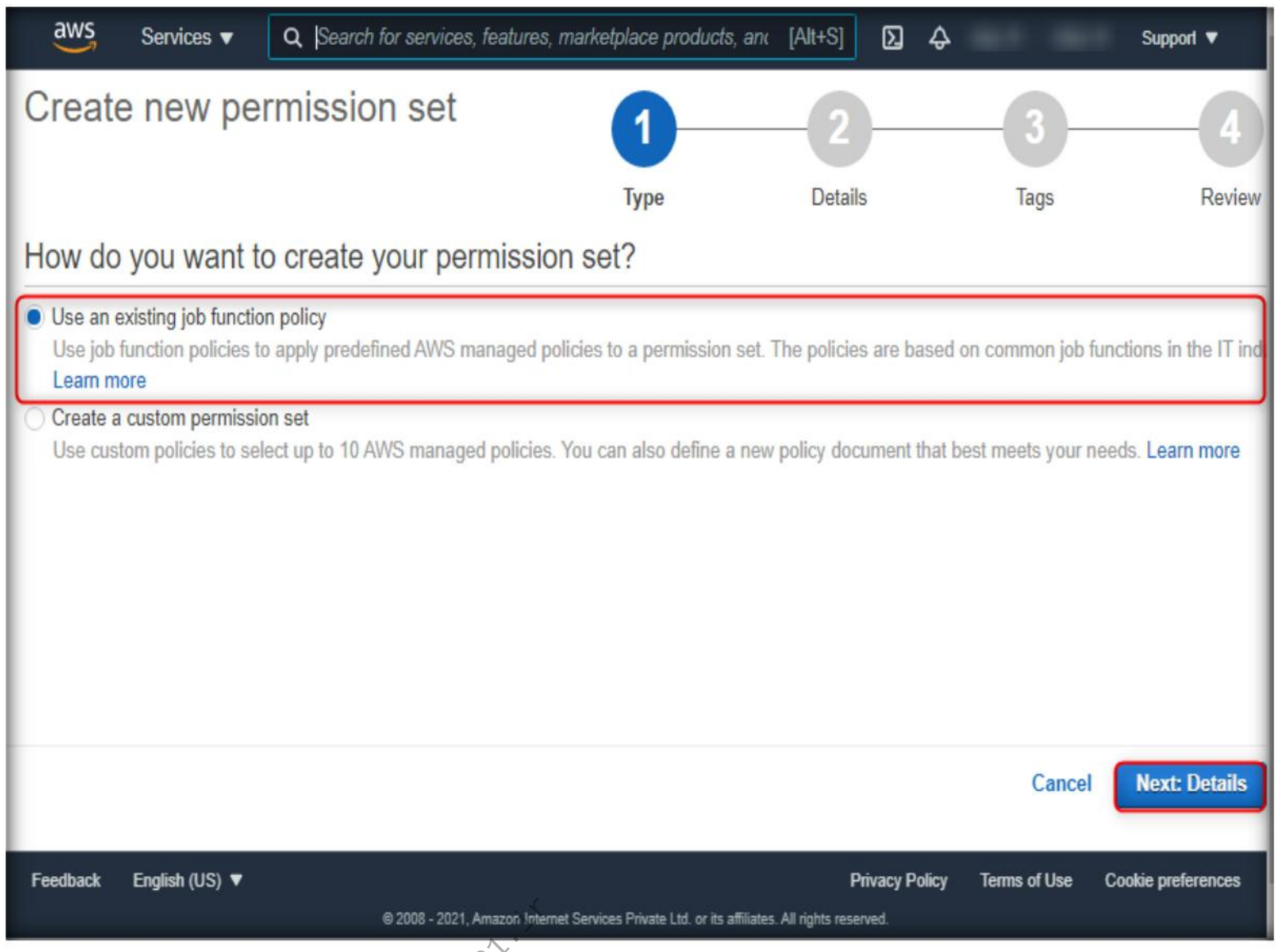


FIGURE 3.2.86: Selecting Use an Existing Job Function Policy

87. Under **Select job function policy**, select **NetworkAdministrator** and click on the **Next: Tags** button.

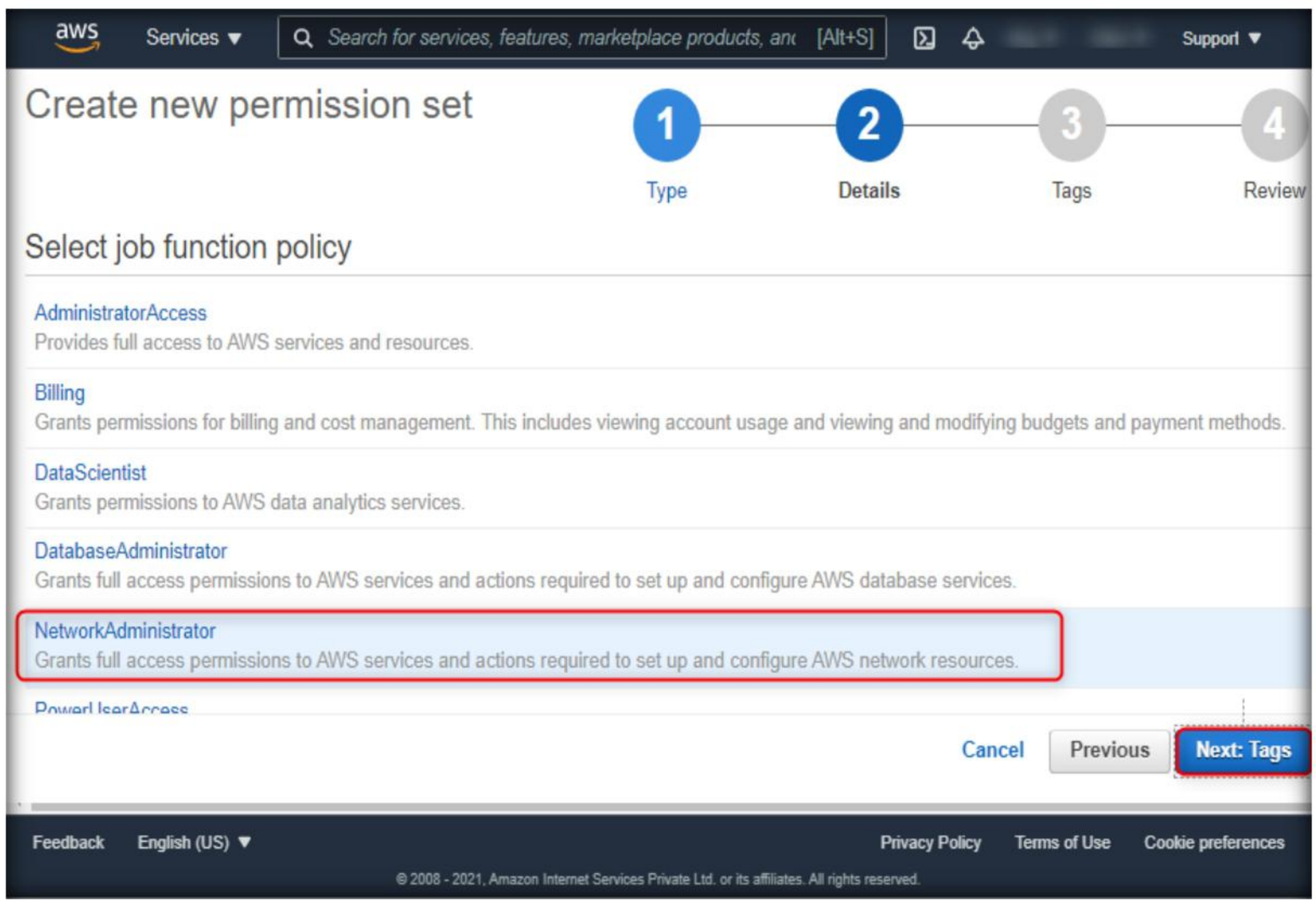


FIGURE 3.2.87: Selecting NetworkAdministrator Role

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

88. Leave **Add tags** in its default state and click on the **Next: Review** button.

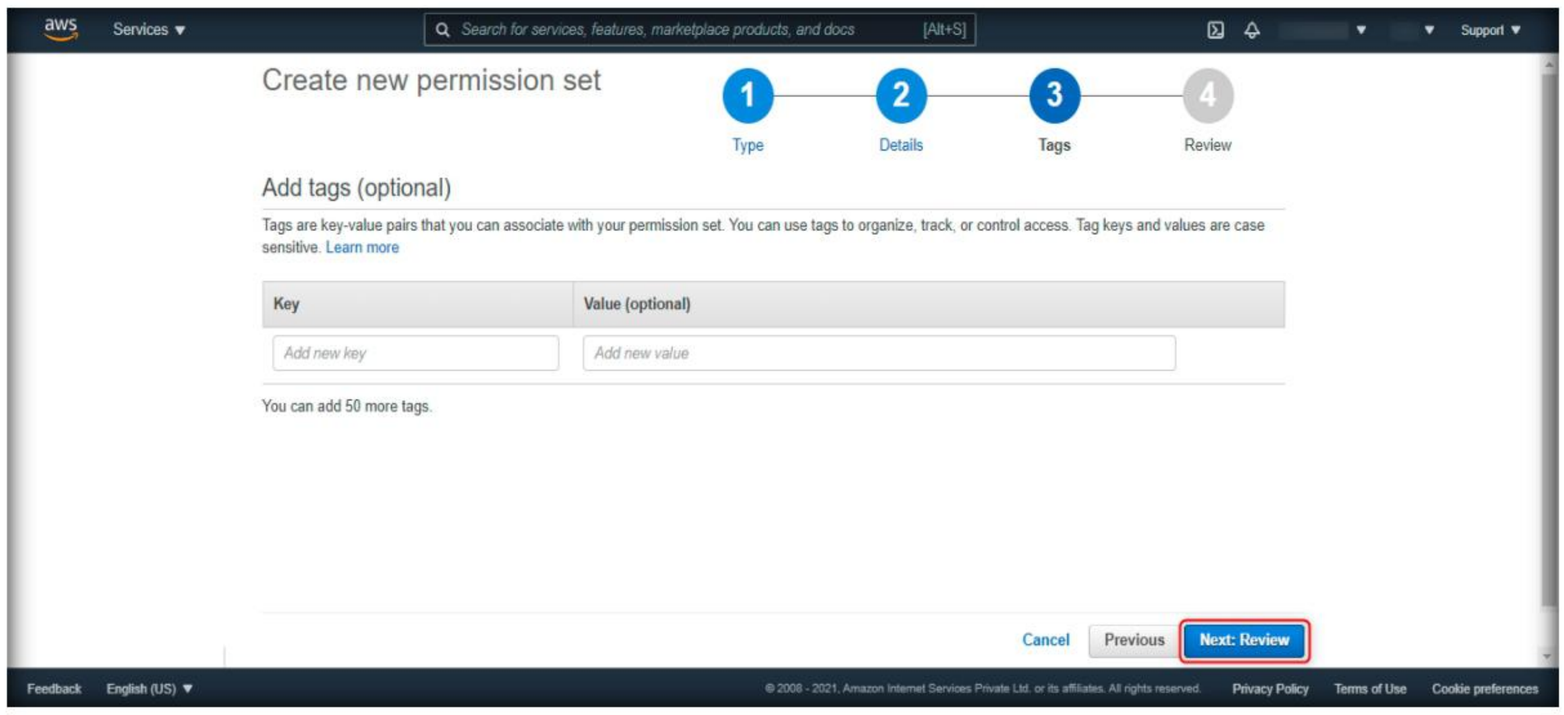
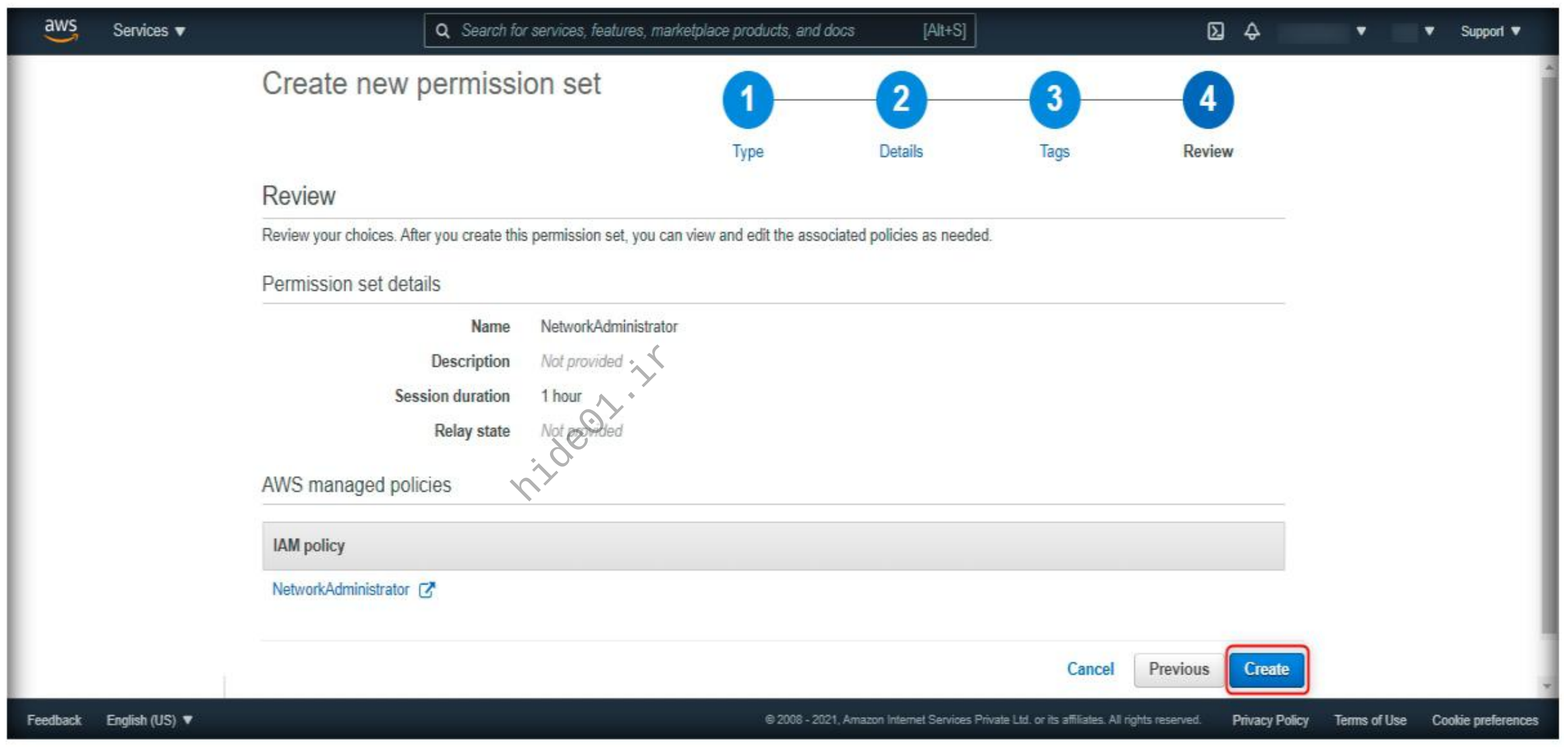


FIGURE 3.2.88: Leaving Add Tags Page in Default State

89. In the **Review** window, click on **Create**.



hide01.ir

FIGURE 3.2.89: Creating New Permission Set

90. The **NetworkAdministrator** permission set is successfully created now.

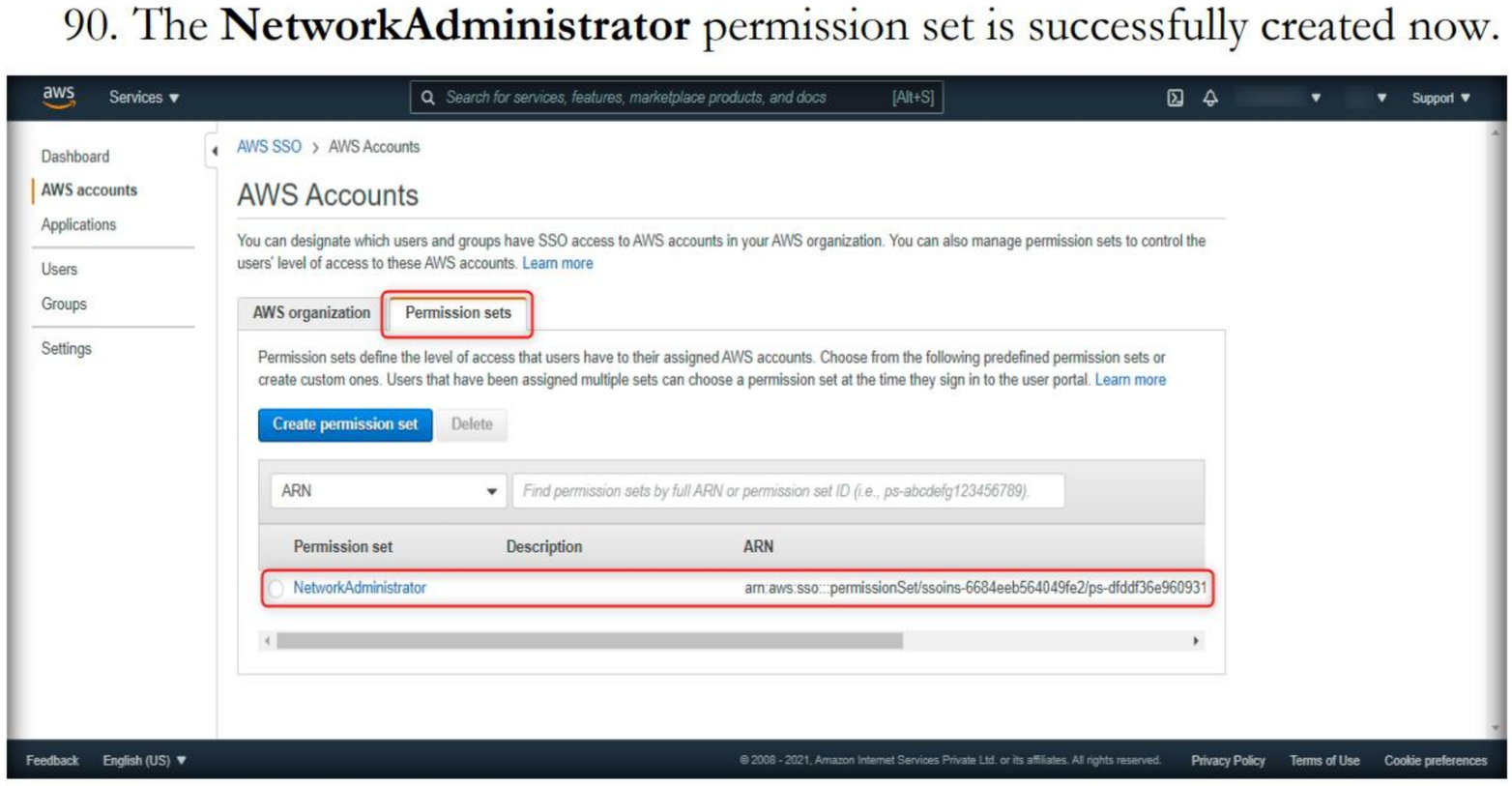


FIGURE 3.2.90: Network Administrator Permission Set is Successfully Created

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

91. Move the horizontal bar. You will observe the permission set is not provisioned yet.

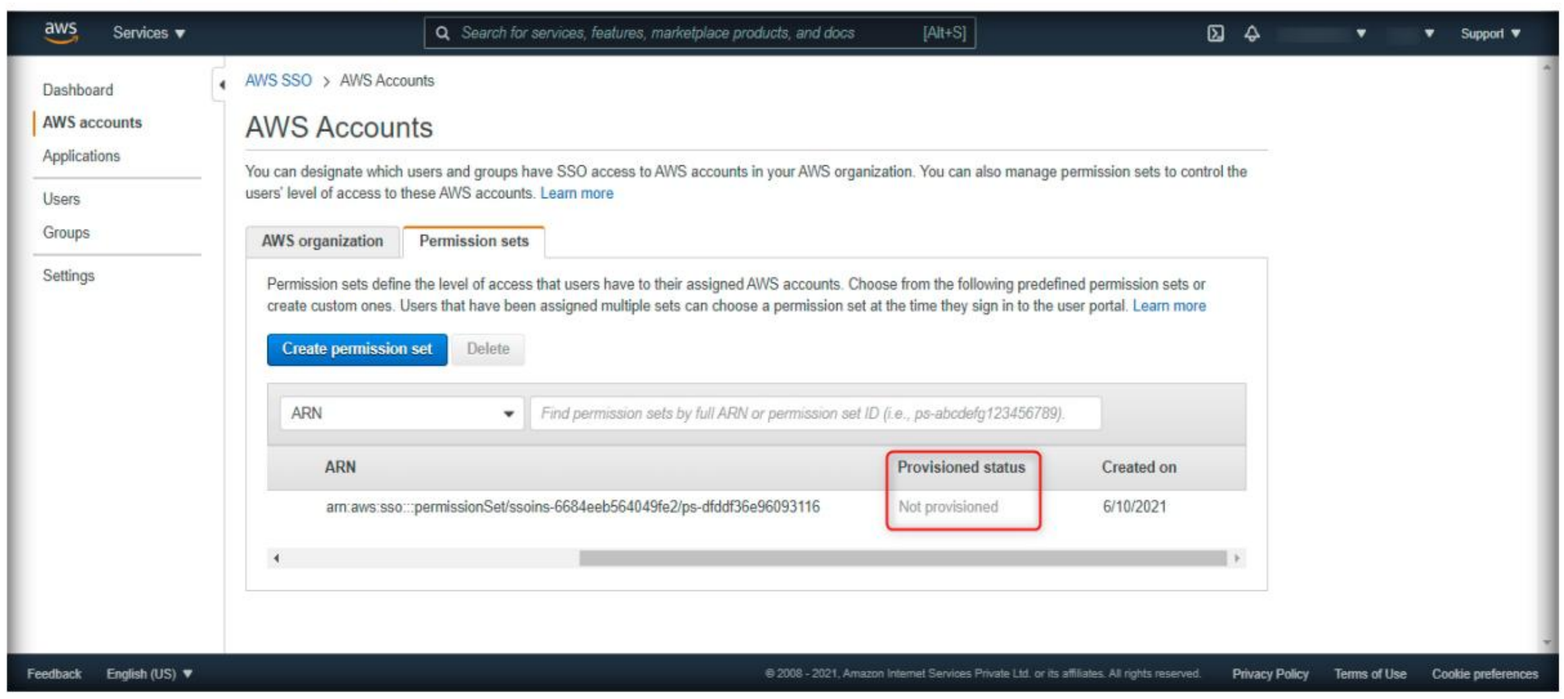


FIGURE 3.2.91: Checking Provisioned Status

92. Next, you need to configure the new user with the permission set. Click on the **AWS organization** tab.

TASK 8

Configuring AWS Account with the New User and Permission Set

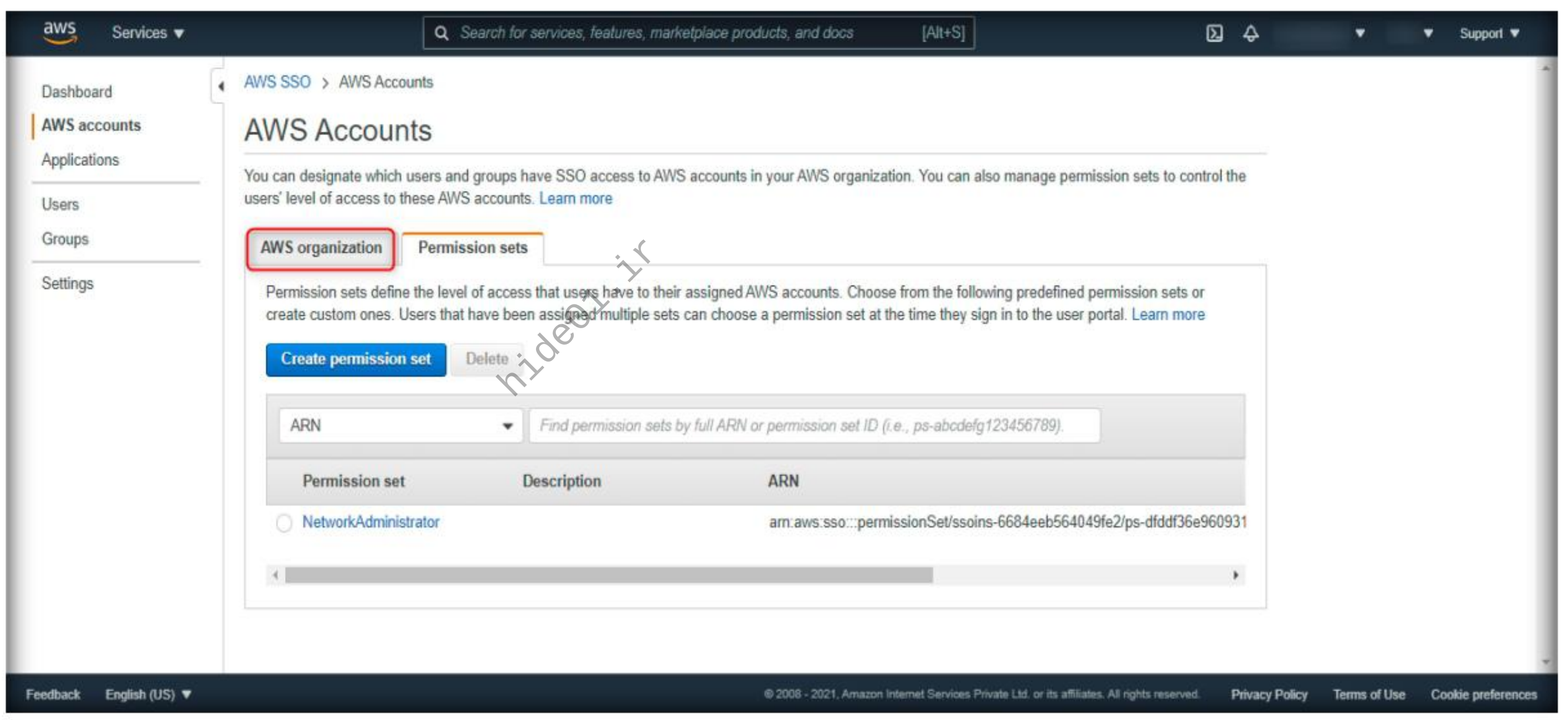


FIGURE 3.2.92: Selecting AWS Organization

93. Select the checkbox for the root user and click on **Assign users**, as shown in the following screenshot.

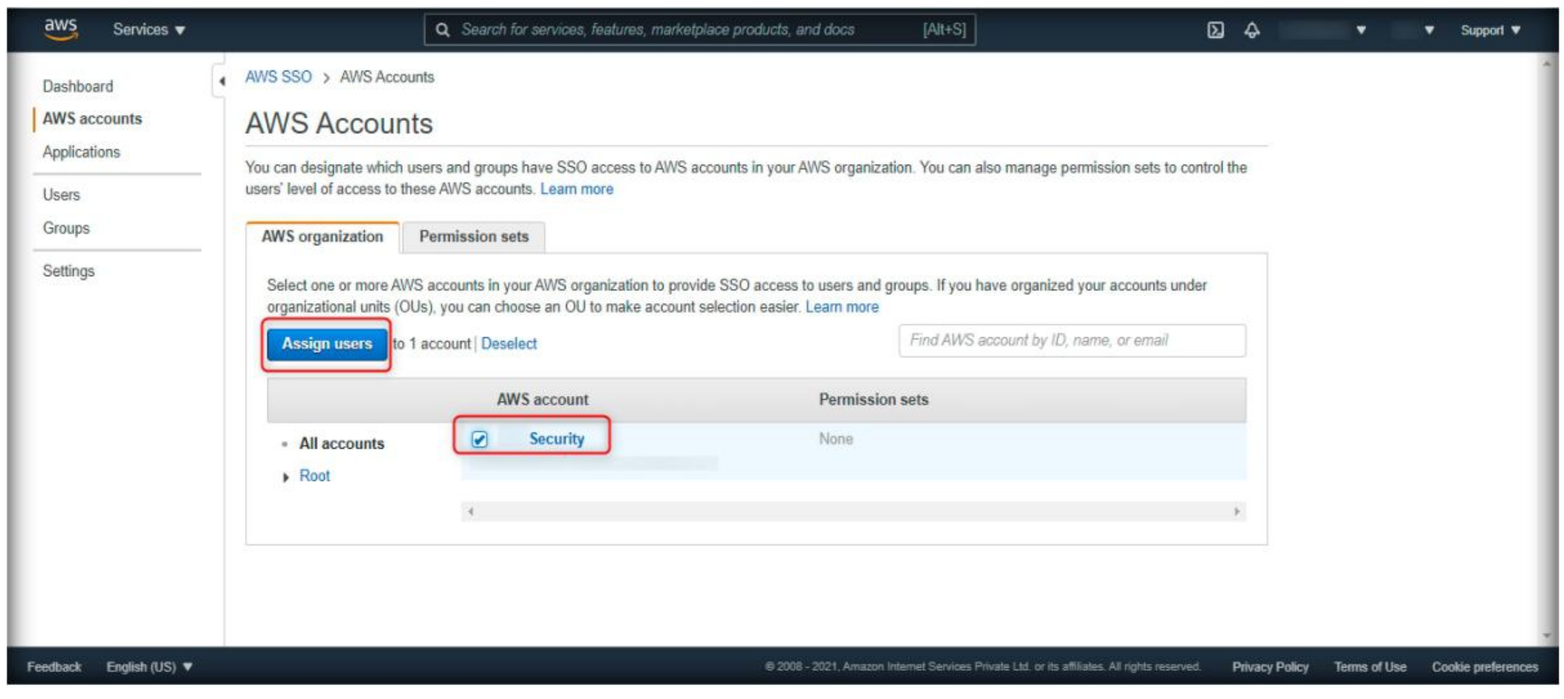


FIGURE 3.2.93: Selecting Root account and Assigning User

Certified Cloud Security Engineer Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

94. Select the checkbox for user **Bob Green** and click on **Next: Permission sets**.

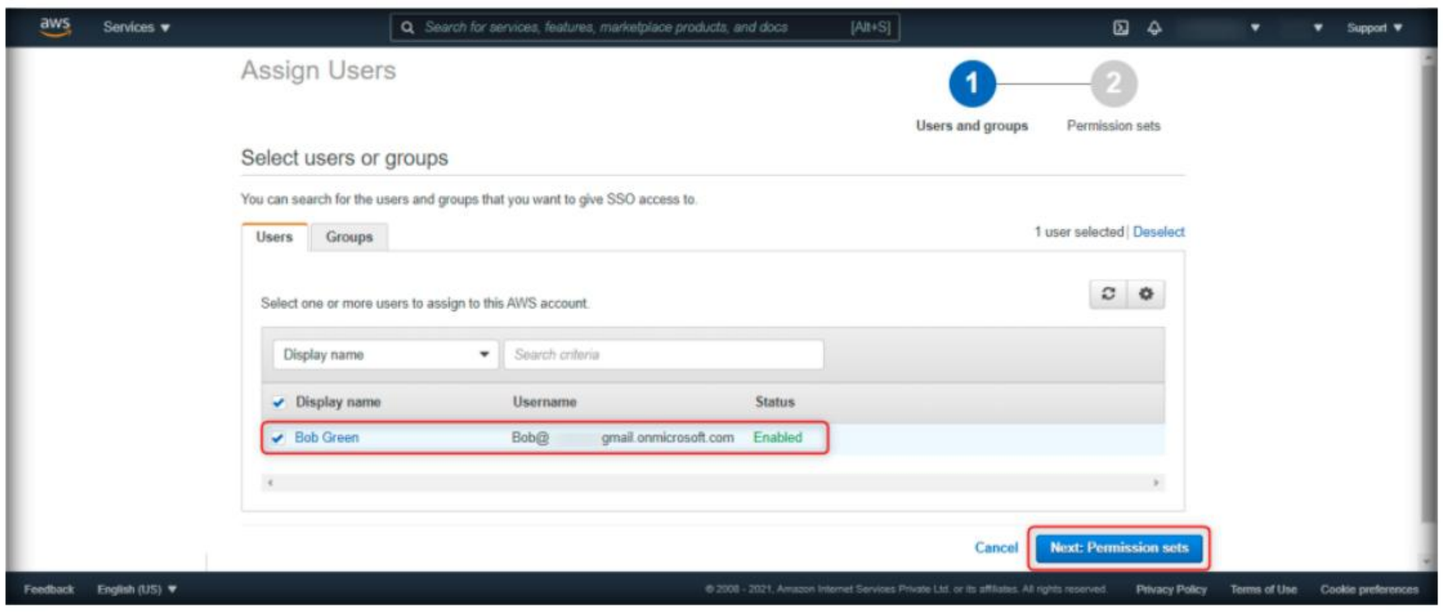


FIGURE 3.2.94: Selecting the User

95. Under **Select permission set,** check **NetworkAdministrator** and click on the **Finish** button.

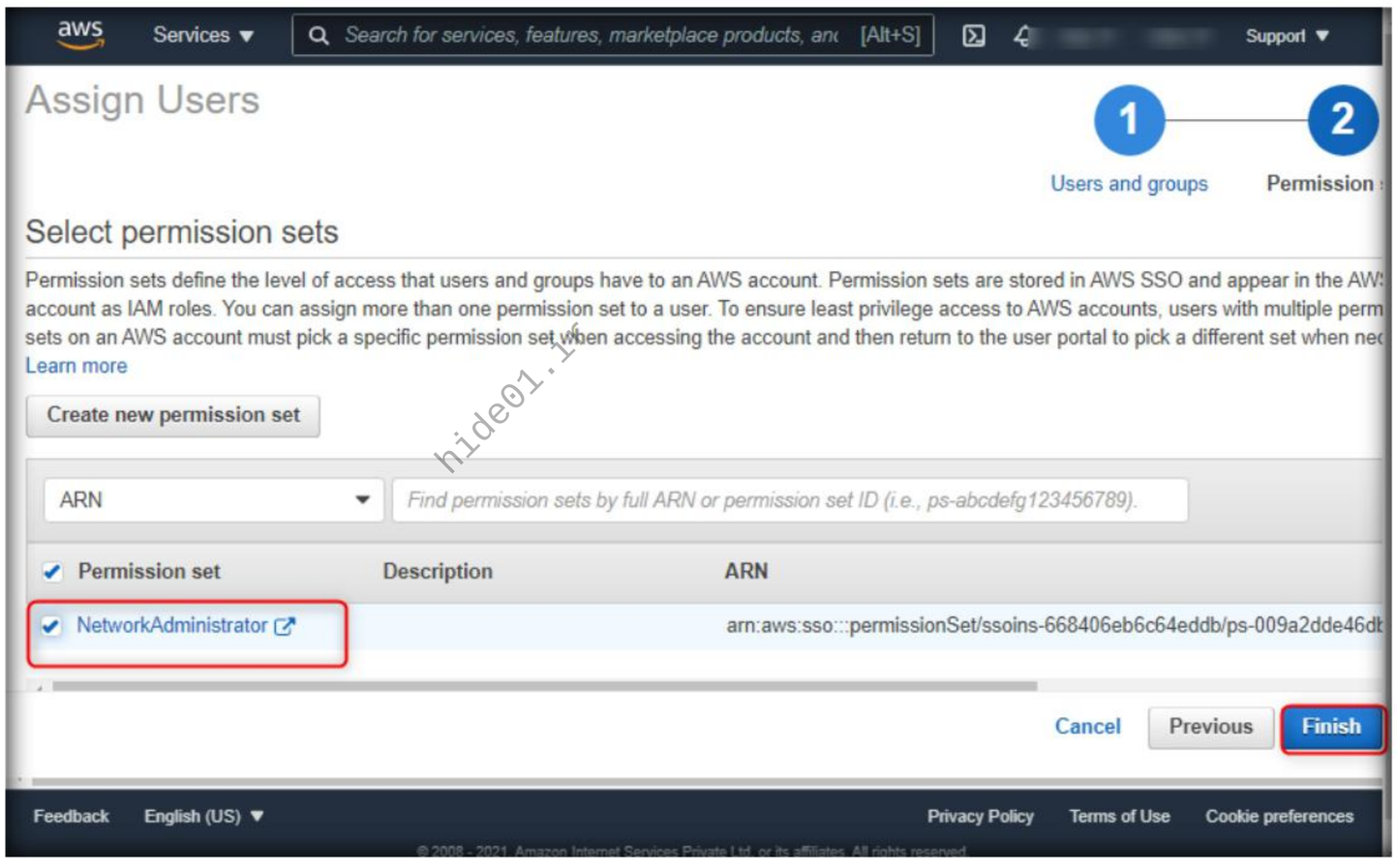


FIGURE 3.2.95: Selecting NetworkAdministrator Permission Set

96. Now, the user **Bob Green** can access the AWS account with the given permission**.** Click on the **Proceed to AWS accounts** button.

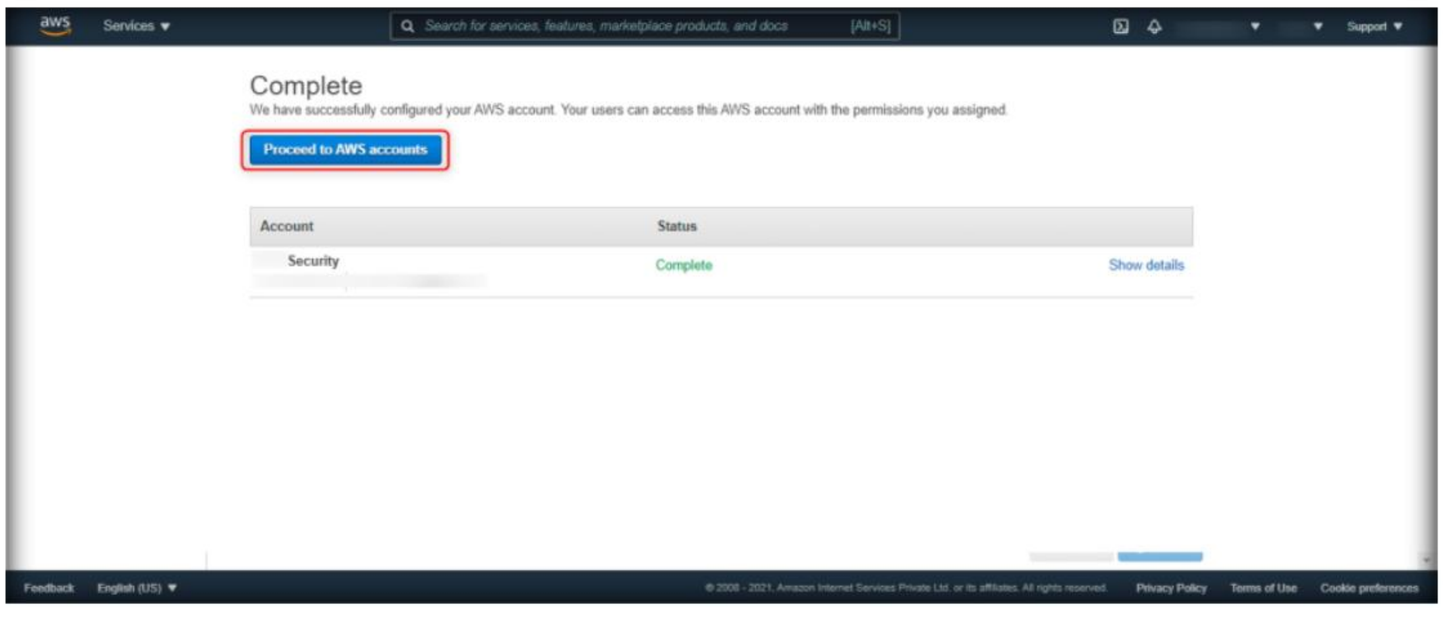


FIGURE 3.2.96: Successfully Configured AWS Account

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

97. Under **Permission sets**, you can see **NetworkAdministrator**.

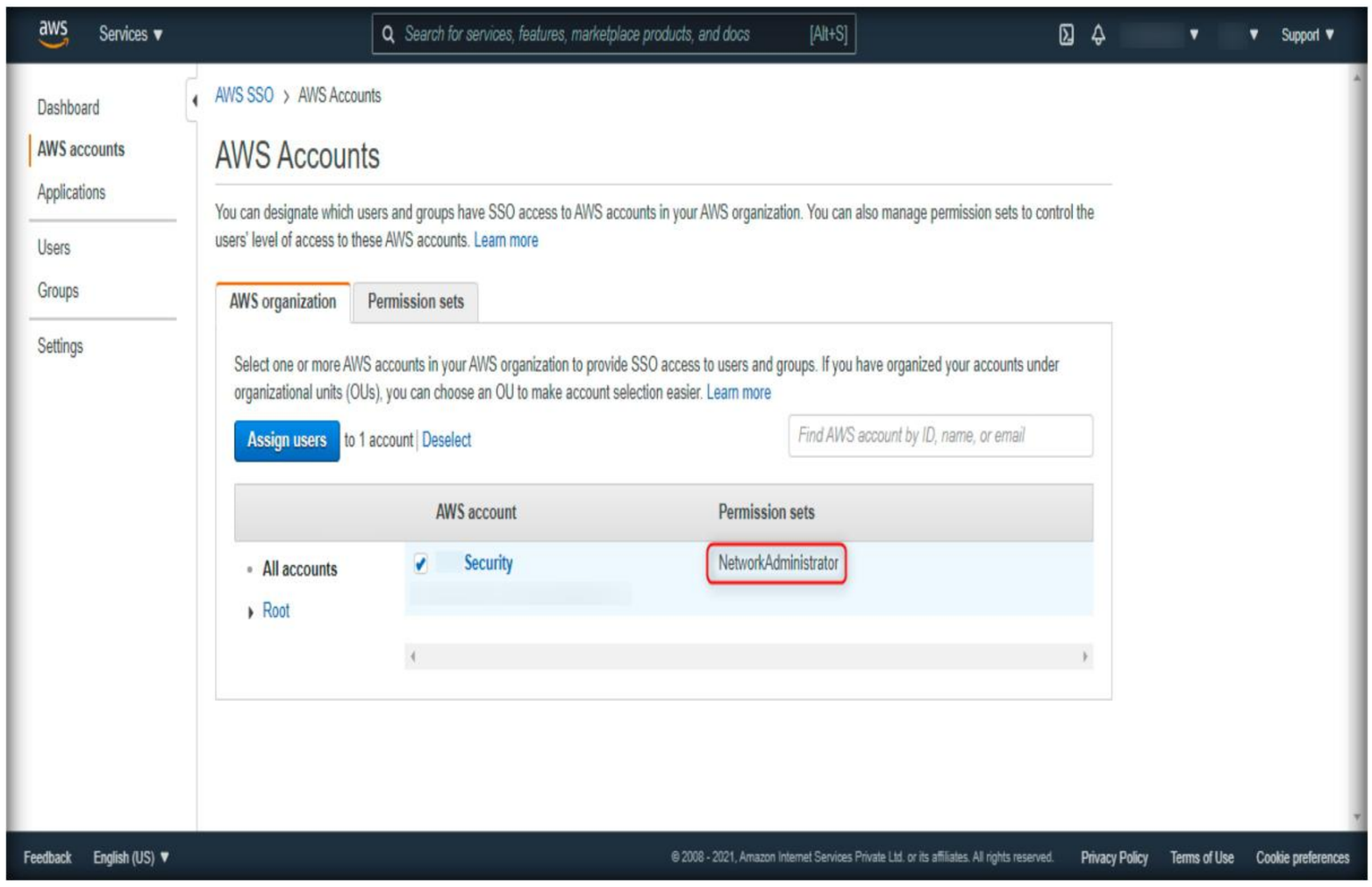


FIGURE 3.2.97: NetworkAdministrator Permission Set is Successfully Assigned

98. Click on the **Permission sets** tab and move the horizontal bar. You will observe the **Provisioned status** as **Provisioned**.

    Note: Do not close this AWS window after this step. Go directly to the next step.

hide01.ir

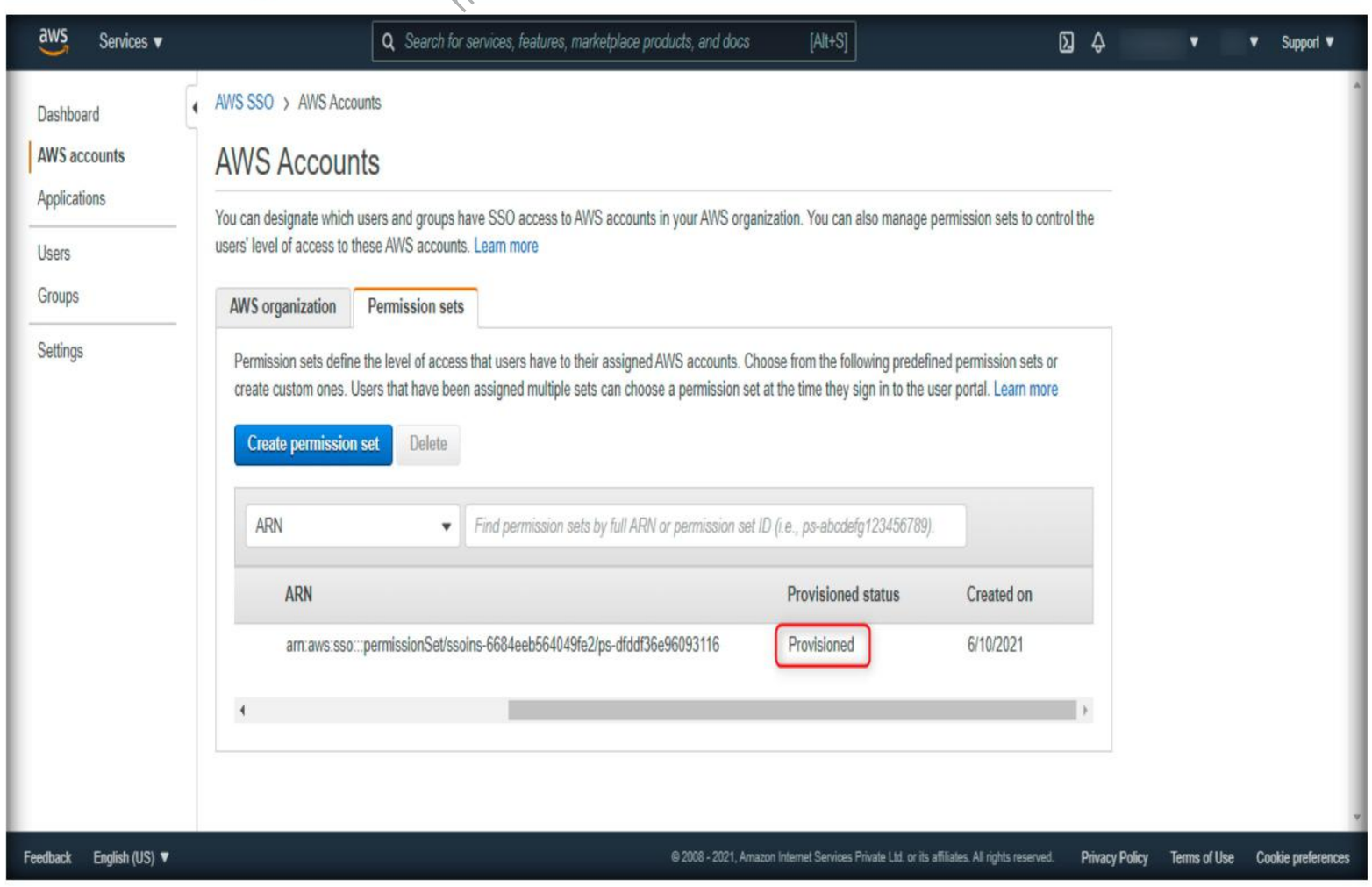


FIGURE 3.2.98: Checking the Provisioned Status

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 9

Performing Operation Using New Permission Set

99. Now, go back to Azure Portal. In the **Azure AWS Single Sign-on** page, click on **Properties** under **Manage** in the left pane.

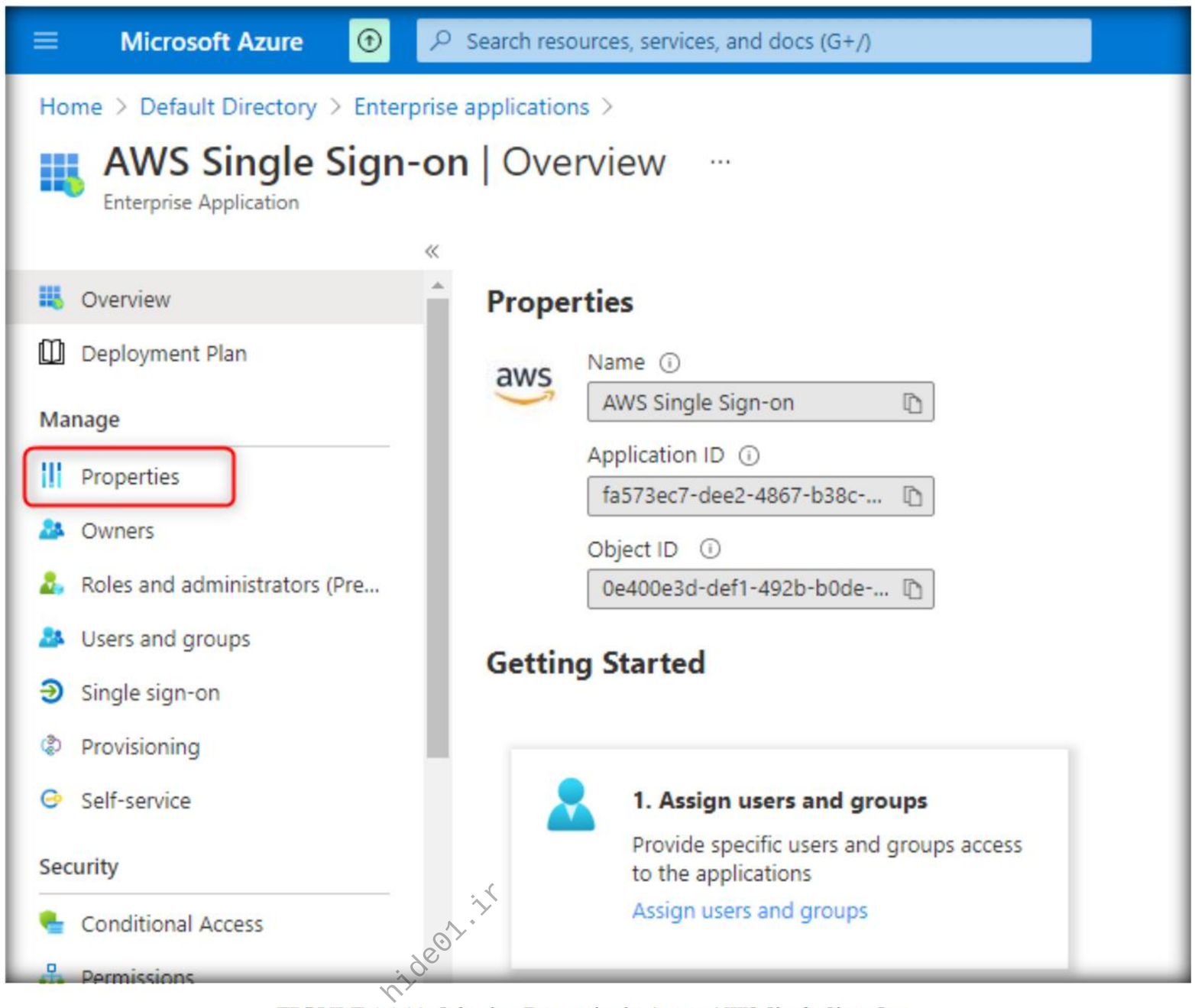


FIGURE 3.2.99: Selecting Properties in Azure AWS Single Sign-On

100. In the AWS Single Sign-on Properties page, change the toggle beside Visible to users? to Yes, and then click on Save.

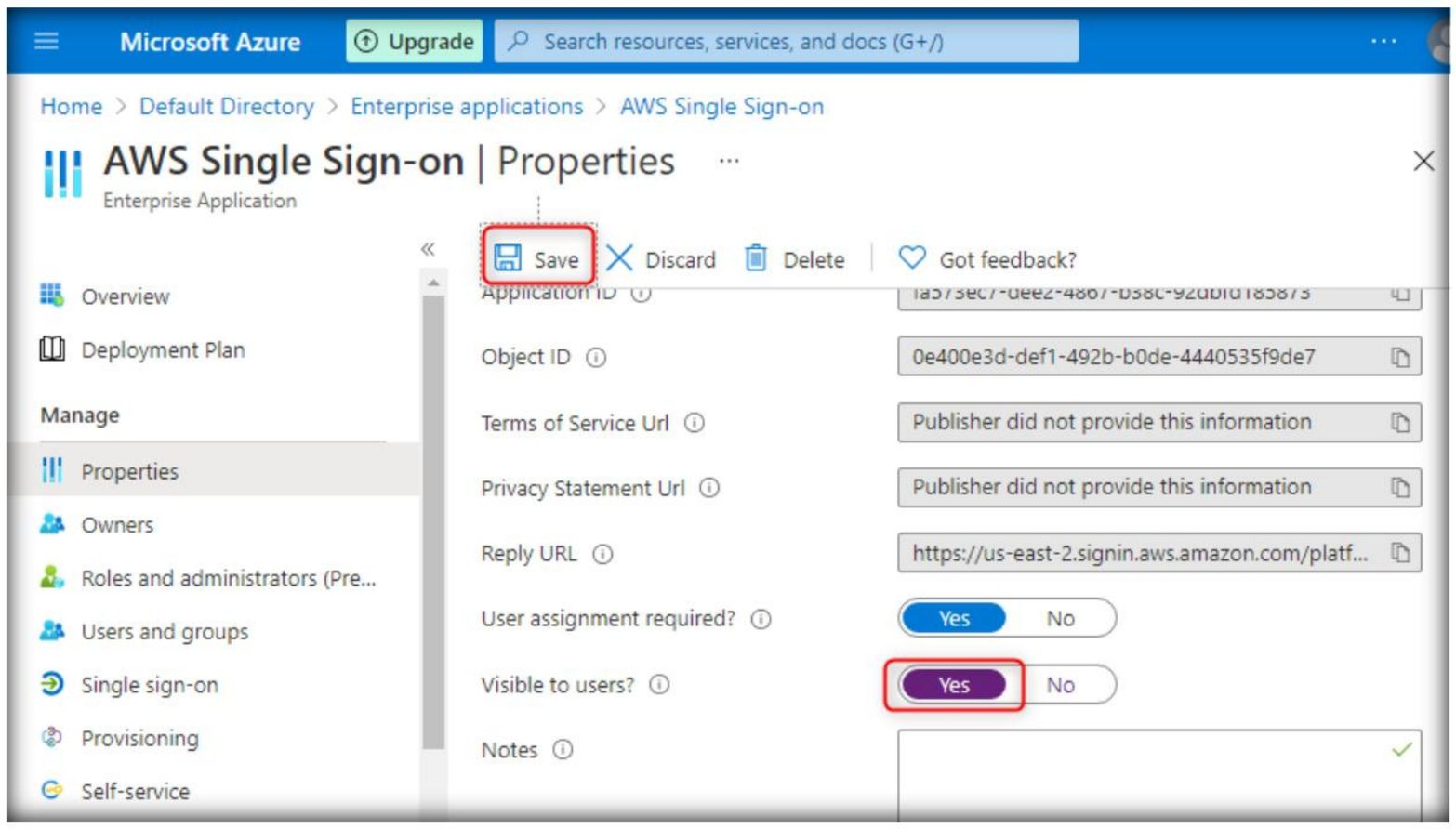


FIGURE 3.2.100: Saving Settings in AWS Single Sign-on Properties Page

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

101. Now, click on **Users and groups** in the left pane.

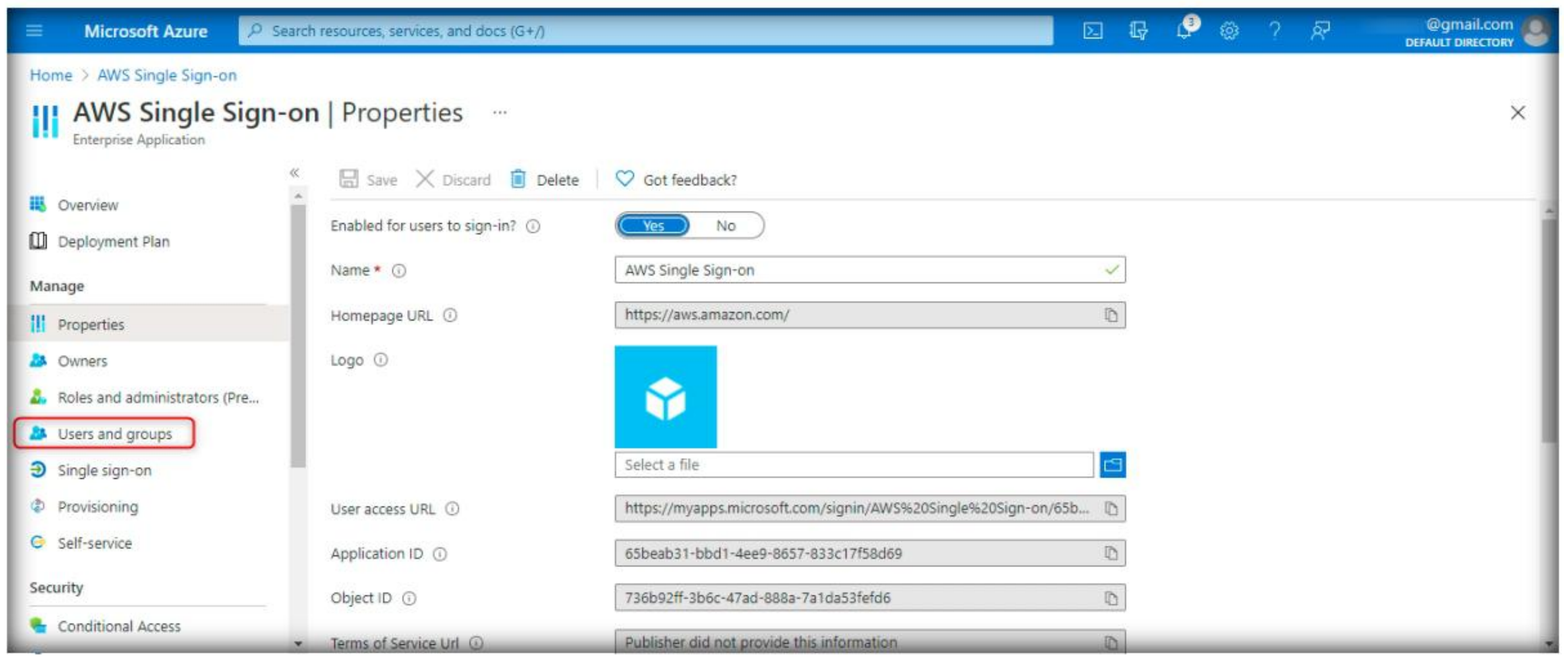


FIGURE 3.2.101: Selecting Users and Groups

102. Click on **Bob Green** under **Display Name**.

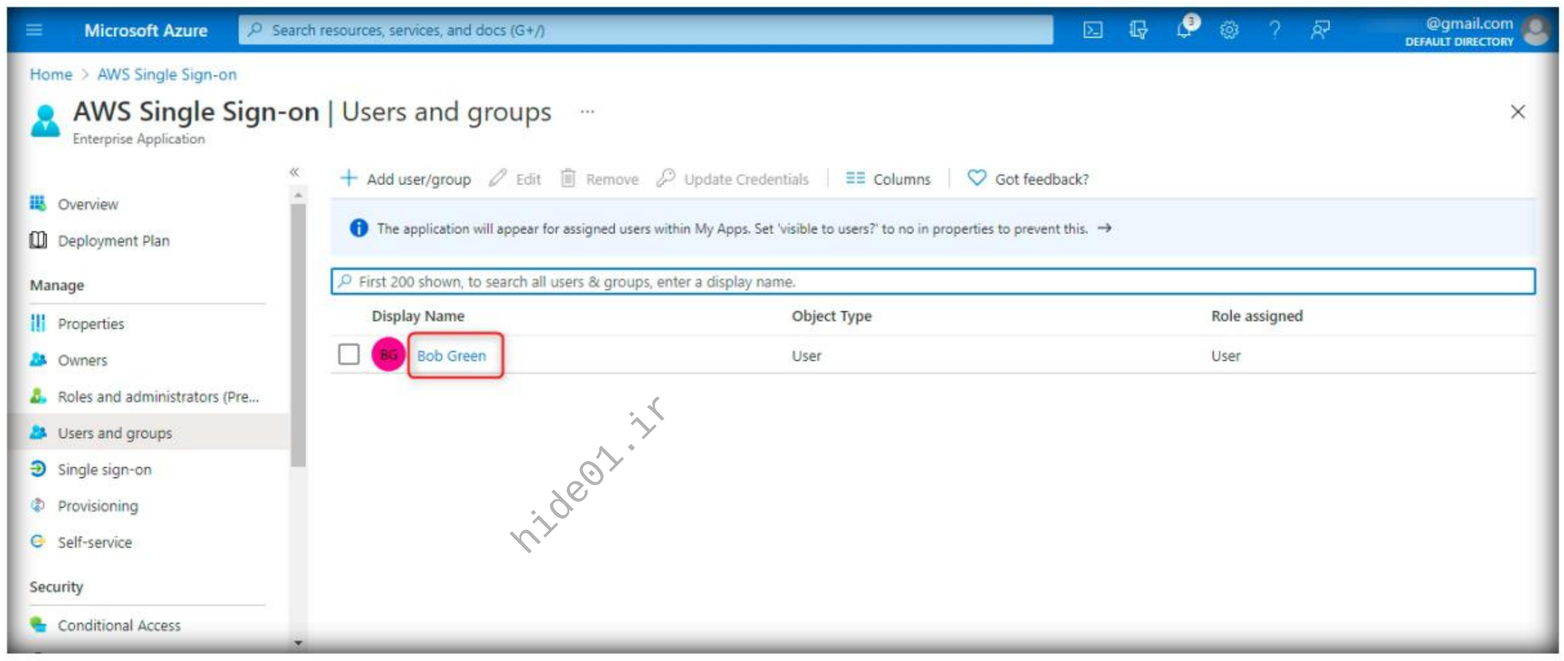


FIGURE 3.2.102: Selecting User

103. In the **Bob Green Profile** window that appears under **Identity**, you can find the **User Principal Name** starting with (**Bob@**). Copy the user principal name and paste it into notepad.

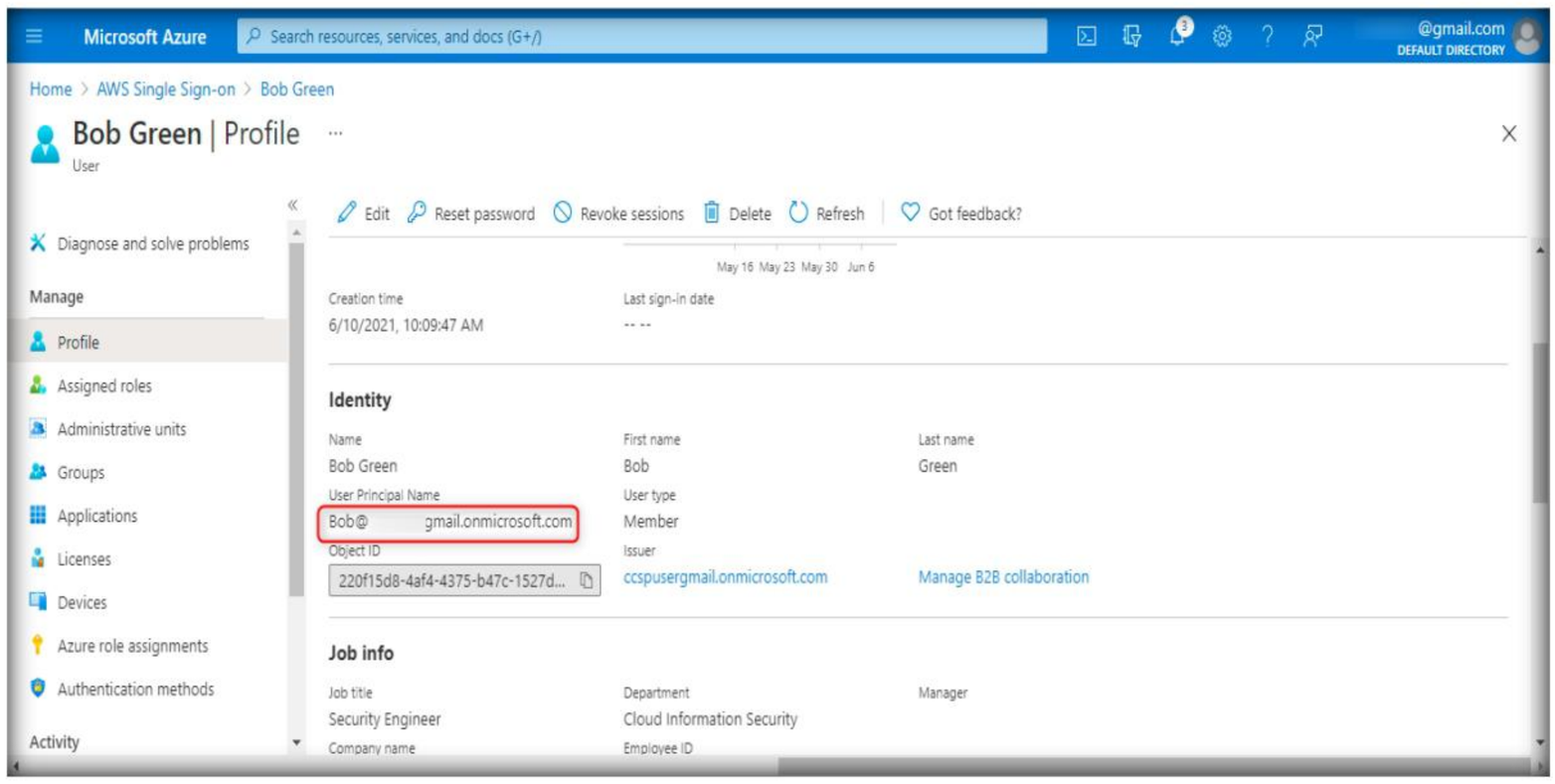


FIGURE 3.2.103: Copying User Principal Name

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

104. Now, go back to AWS console. In the AWS SSO window that you are in, click on **Dashboard** in the left pane.

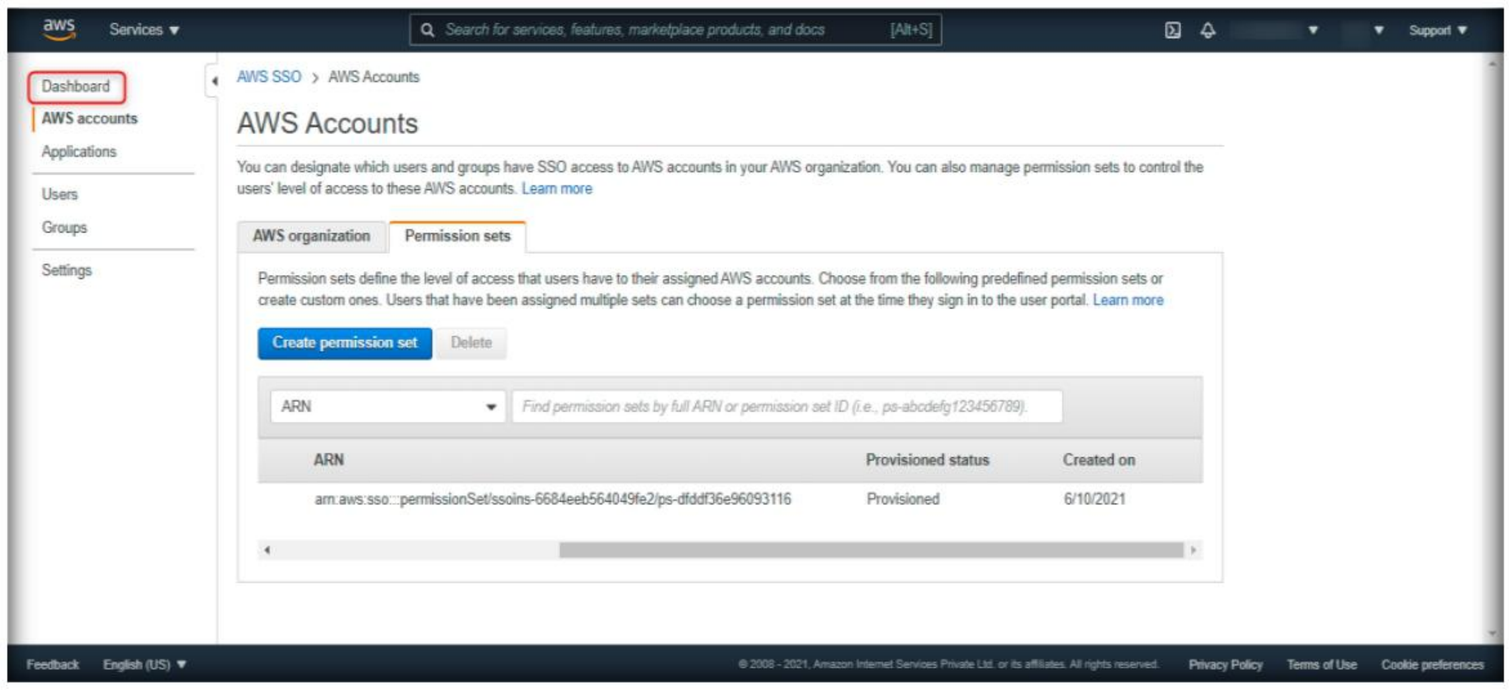


FIGURE 3.2.104: Selecting Dashboard in AWS SSO

105. In the **Dashboard** window, scroll down and right click on **User portal URL** and then select **Open link in incognito window**.

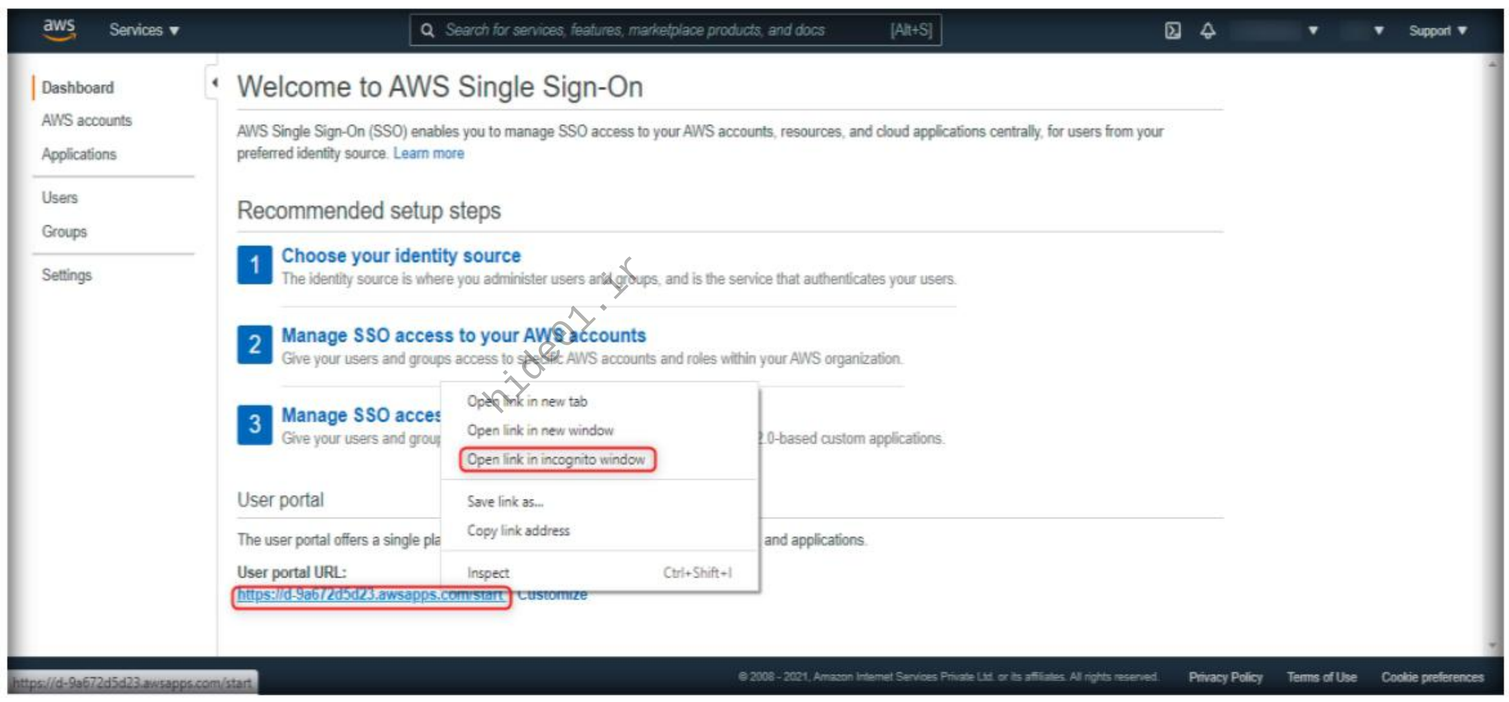


FIGURE 3.2.105: Opening User Portal URL in Incognito Window

106. In the **Microsoft Sign in** window, paste the user login ID you copied to notepad as the principal name and click on the **Next** button.

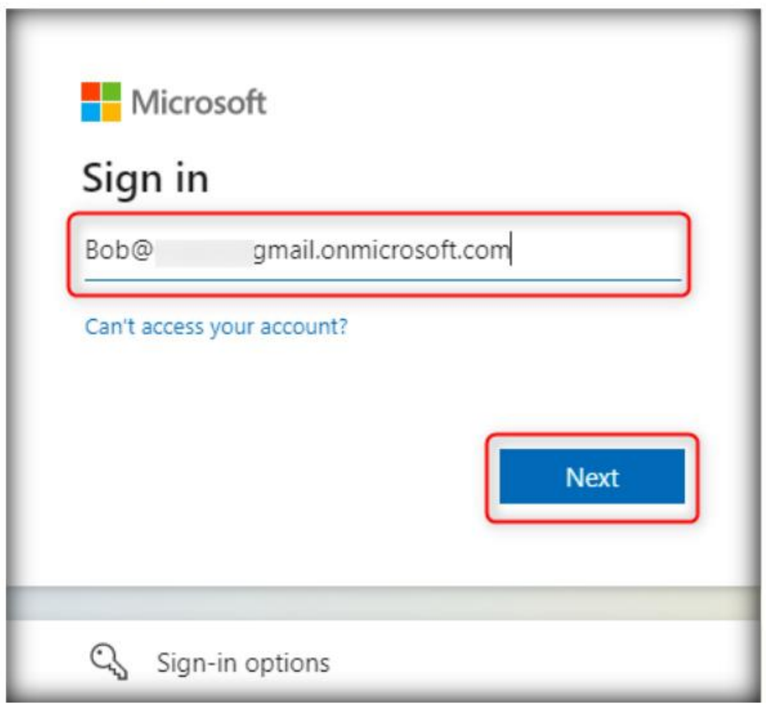


FIGURE 3.2.106: Entering Azure User Name

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

107. Enter the password (Administrator@789) and click Sign in .

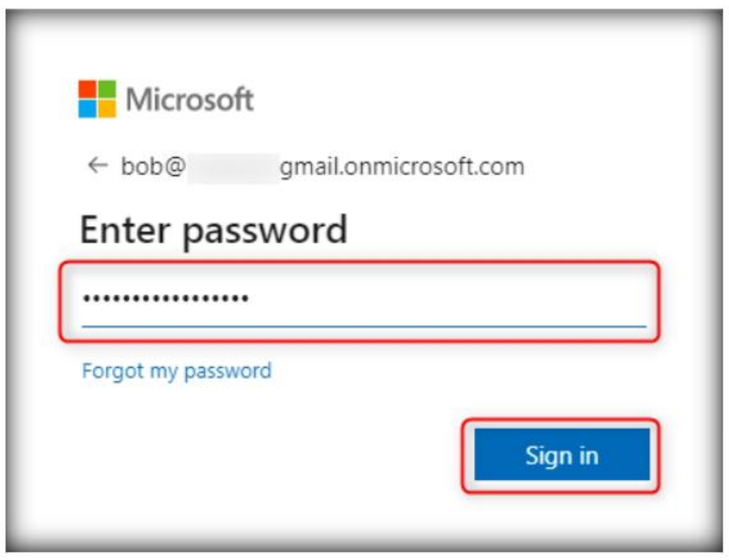


FIGURE 3.2.107: Entering Password

108. In **Update your password** window, enter the **Current password** (**Administrator@789**), and then enter the **New password** (**Administrator@2589**). Finally, fill in the **Confirm password** (**Administrator@2589**) and click on **Sign in**.

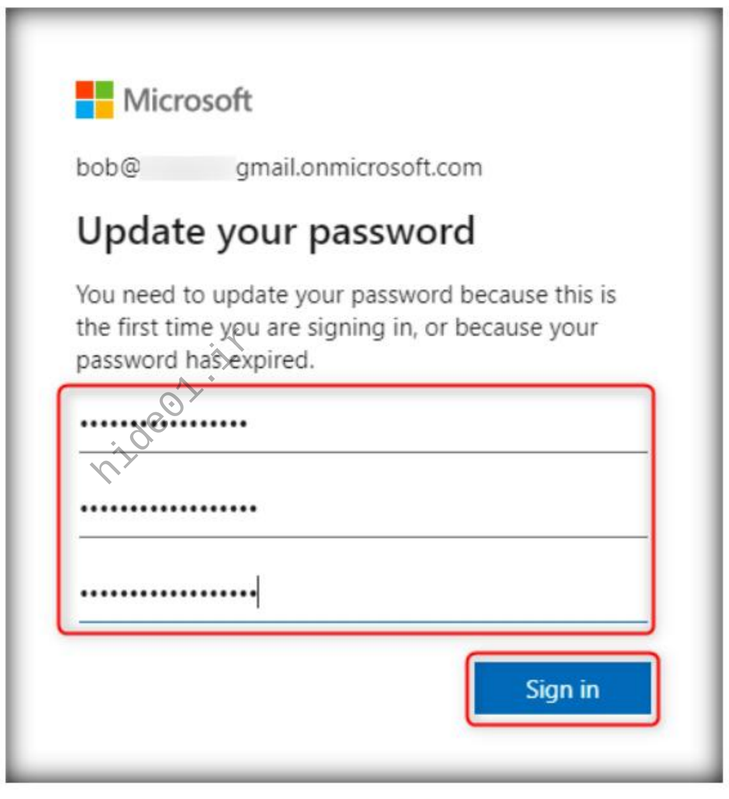


FIGURE 3.2.108: Updating Password

109. In the **Help us protect your account** window, select **Skip for now**.

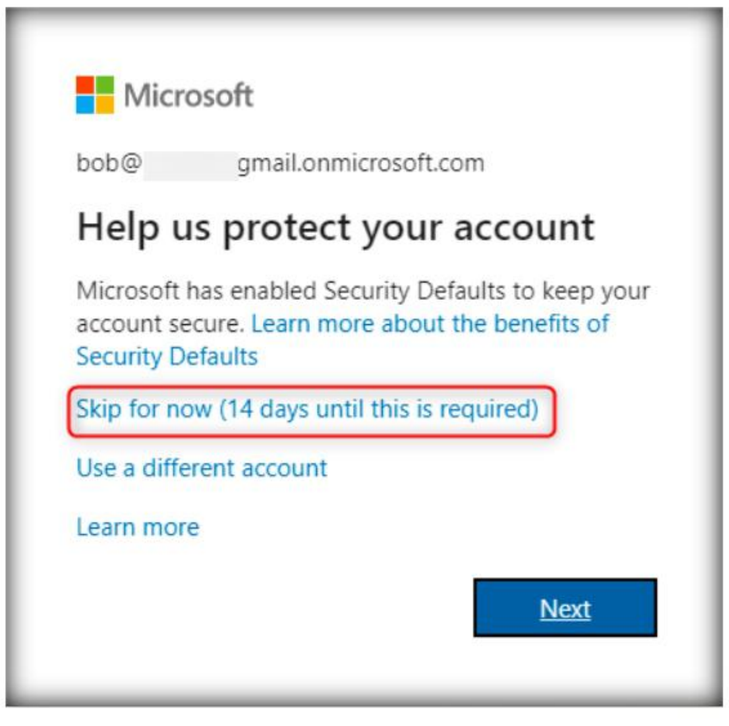


FIGURE 3.2.109: Selecting Skip for now

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

110. In the **Stay signed in** window, click on the **No** button.



FIGURE 3.2.110: Selecting No in Stay Signed In Window

111. In the **Single Sign-On** window, click on **AWS Account**.

Note: If you get an invalid input error, close the incognito window, and try to login again with the updated password by opening the URL in the AWS SSO page in a new incognito window.

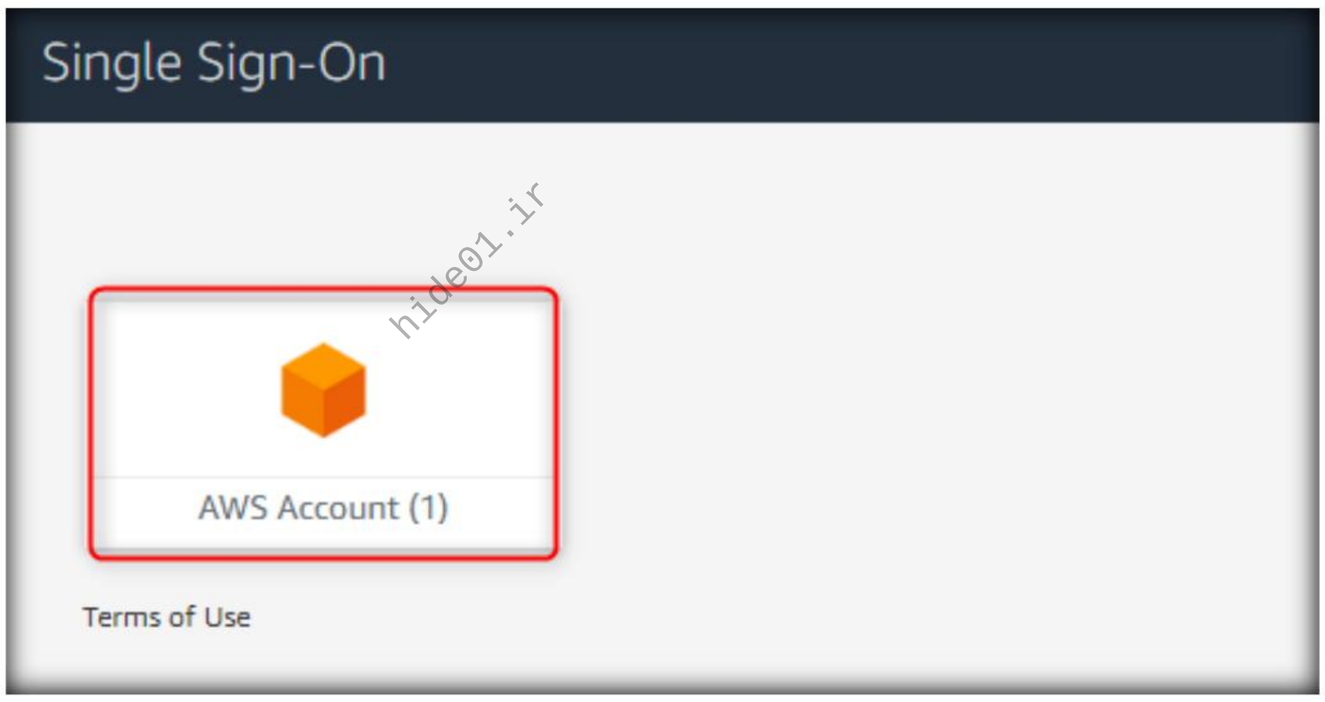


FIGURE 3.2.111: Selecting AWS Account

112. Then, click on the name of the **AWS account** user.

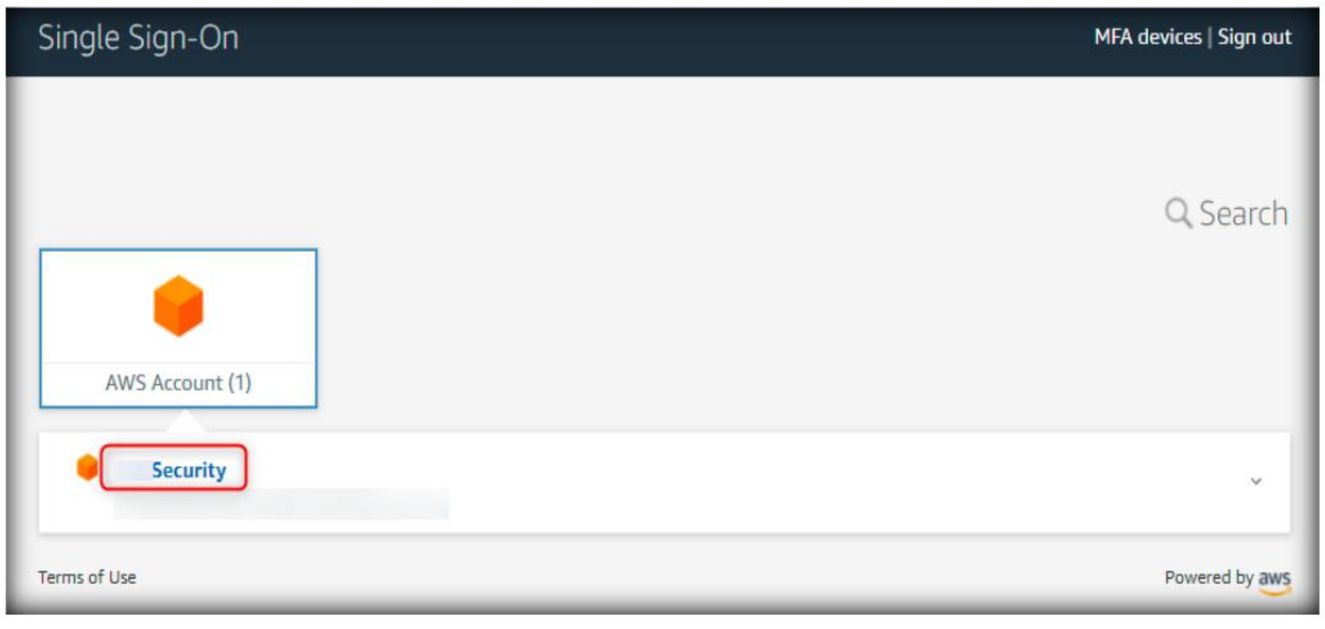


FIGURE 3.2.112: Selecting AWS Account User

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

113. Click on **Management console**.

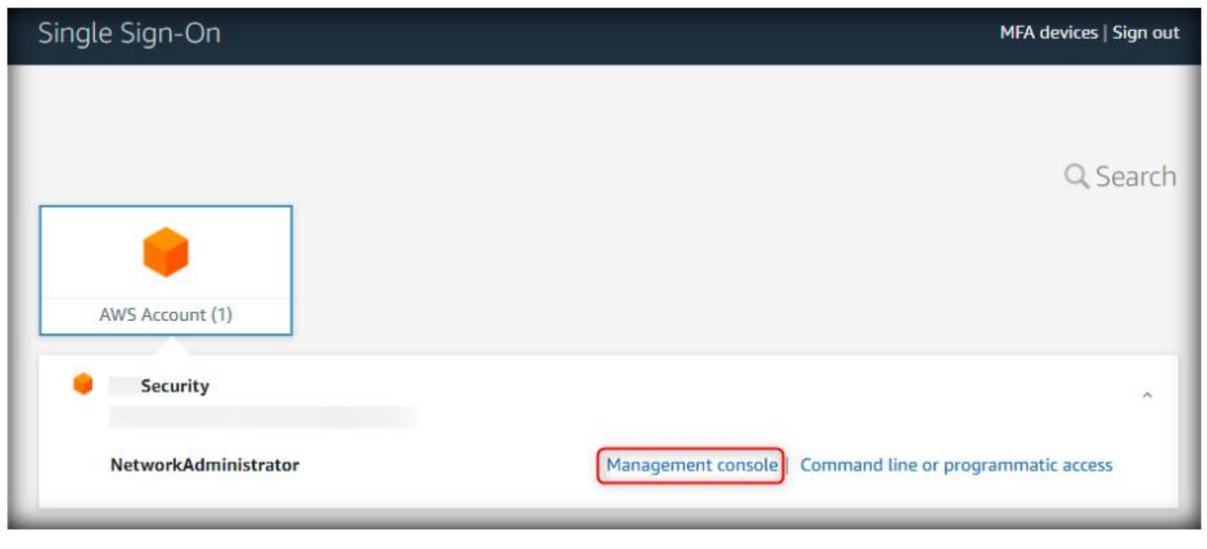


FIGURE 3.2.113: Selecting Management Console

114. In Management console, you will see a NEW! Services popup. Click on **Got it**.

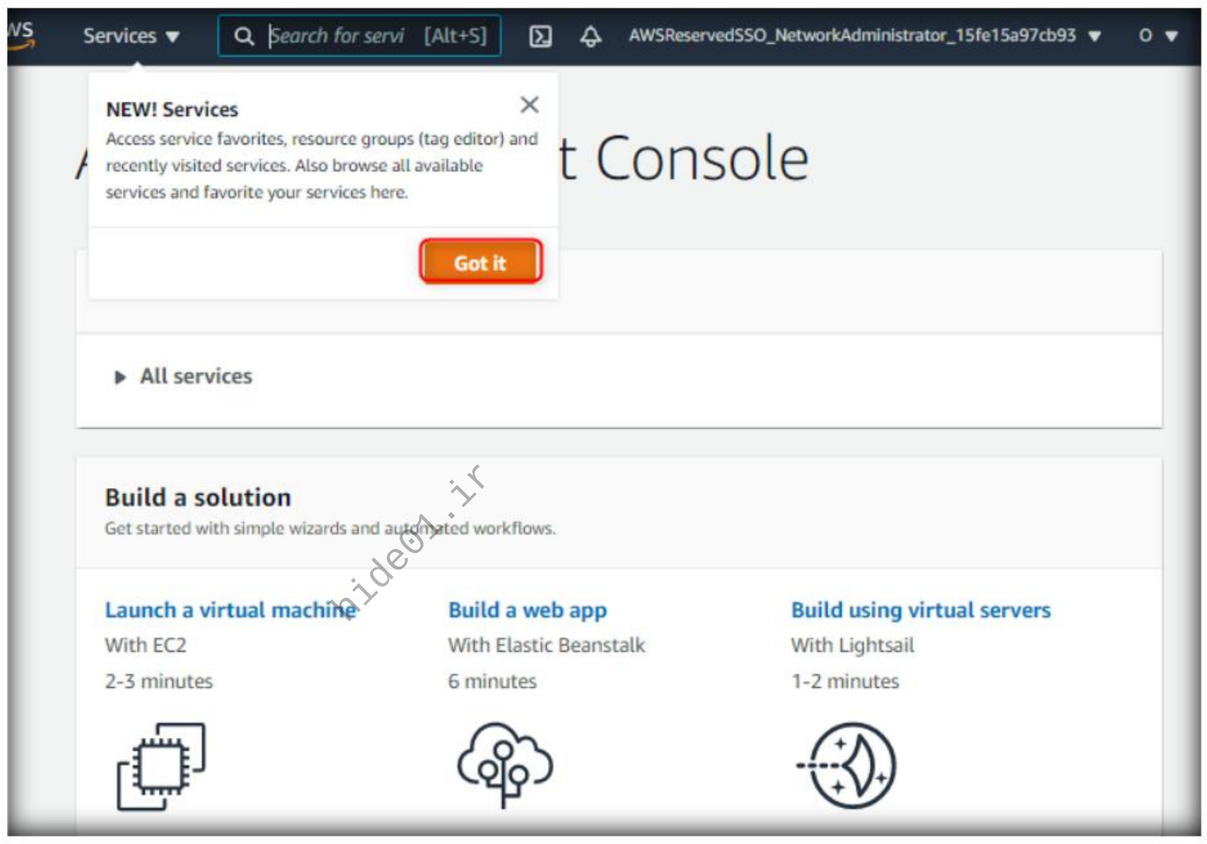


FIGURE 3.2.114: Selecting Got it in Pop--up

115. Click on **All services**.

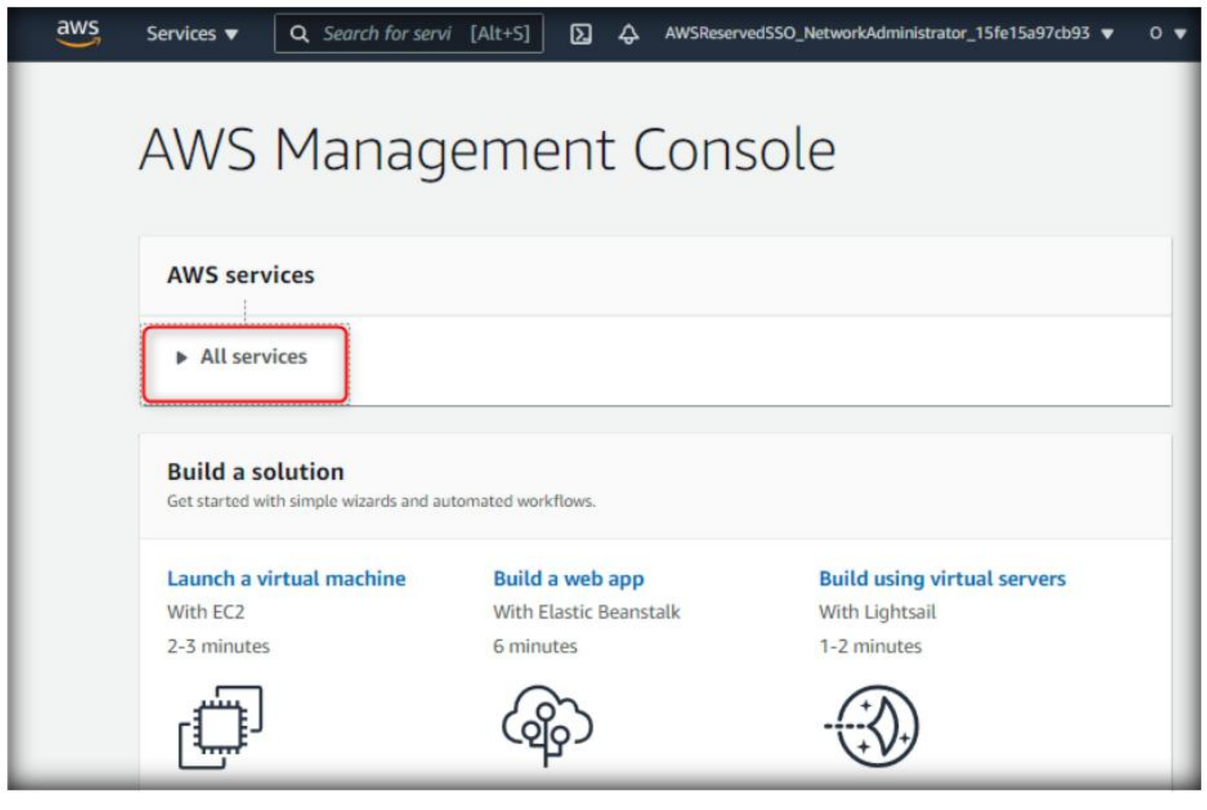


FIGURE 3.2.115: Selecting All Services

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

116. Under **Compute**, click on **EC2**.

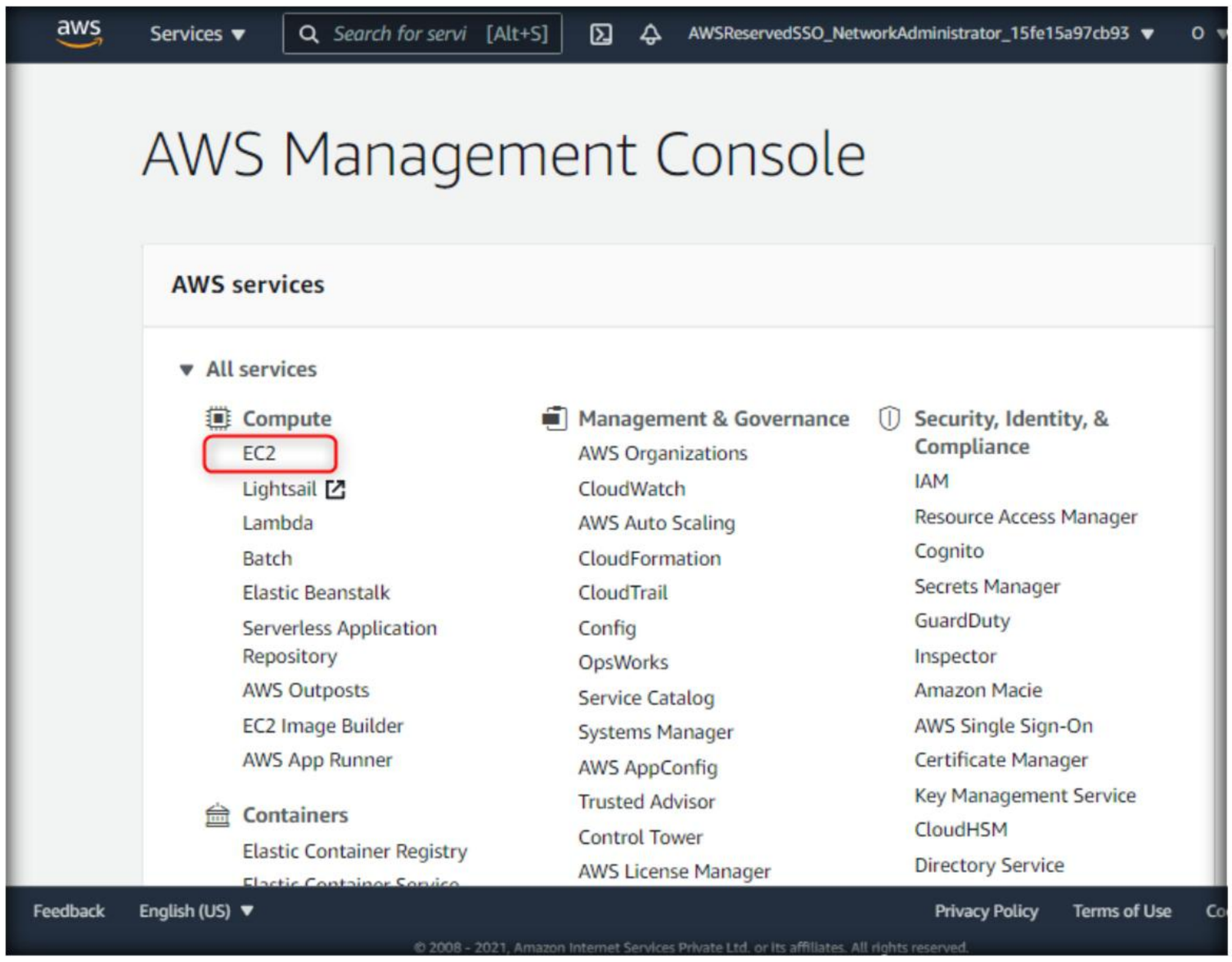


FIGURE 3.2.116: Selecting EC2

117. Now, you can check whether access privileges are implemented with SAML Single Sign-on. In **EC2 Dashboard**, click on the **Launch instance** button.

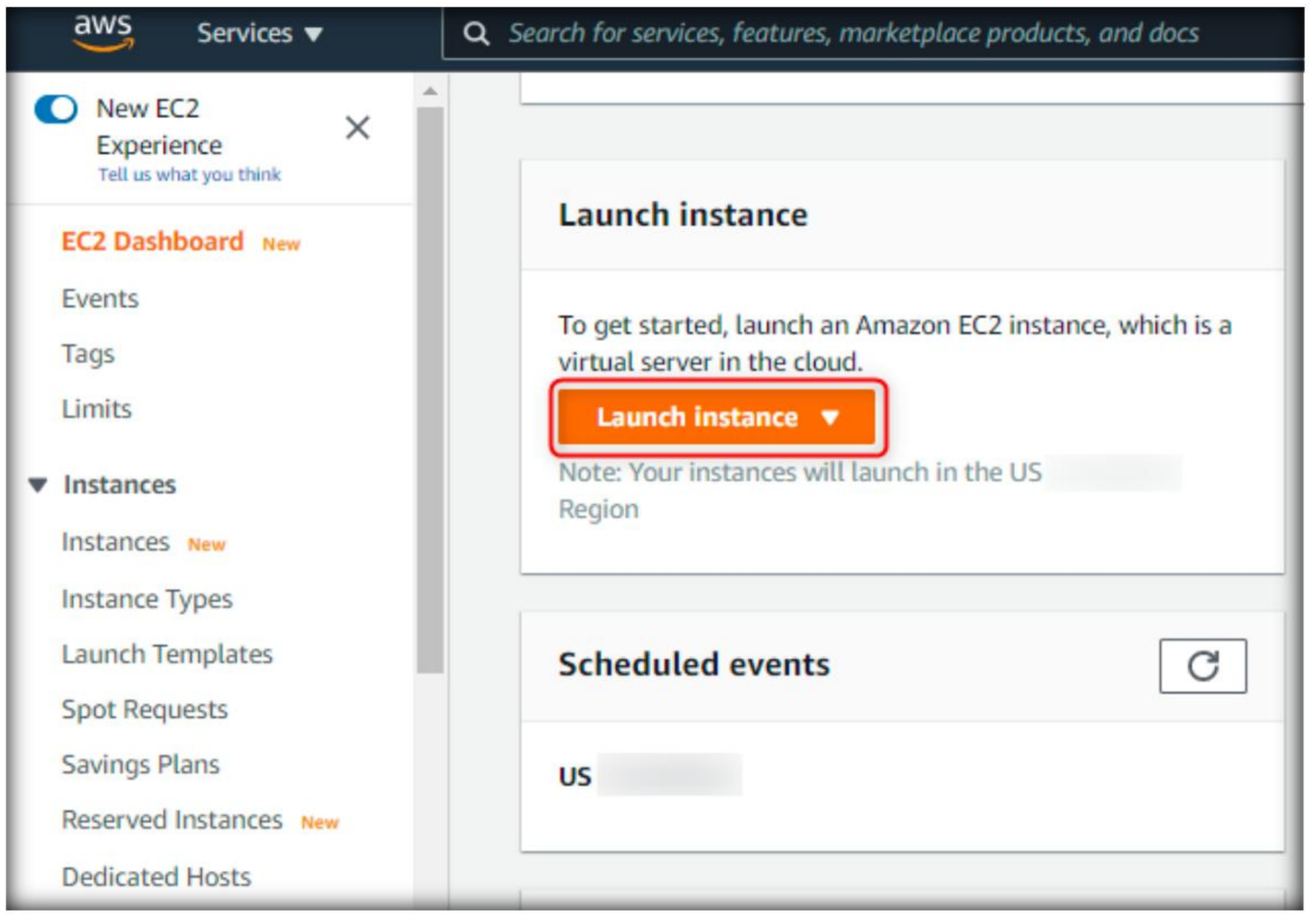


FIGURE 3.2.117: Selecting Launch Instance

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

118. Now, click on **Launch instance** from the dropdown.

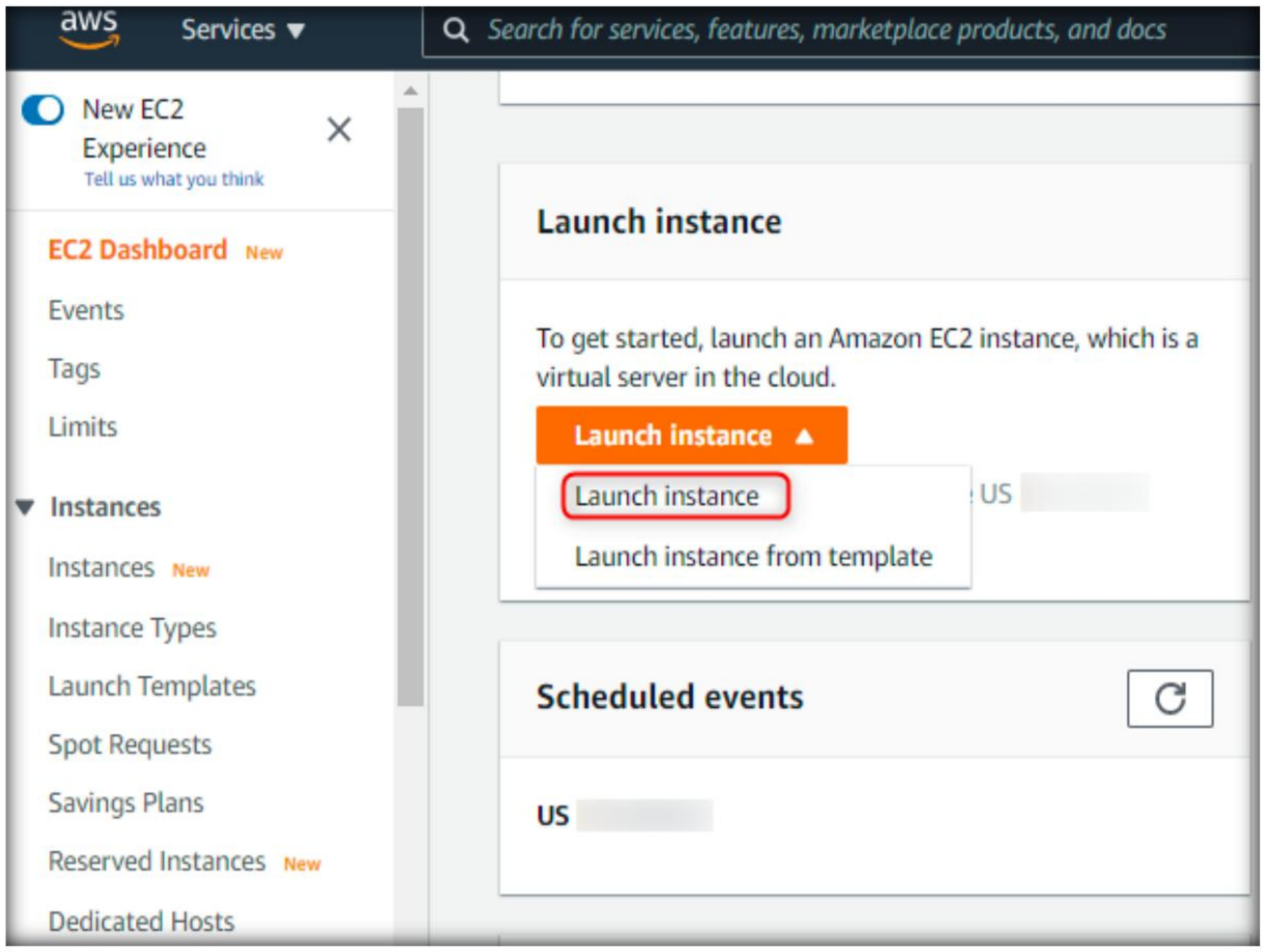


FIGURE 3.2.118: Launching an Instance

119. Click on the **Select** button beside **Amazon Linux 2 AMI**.

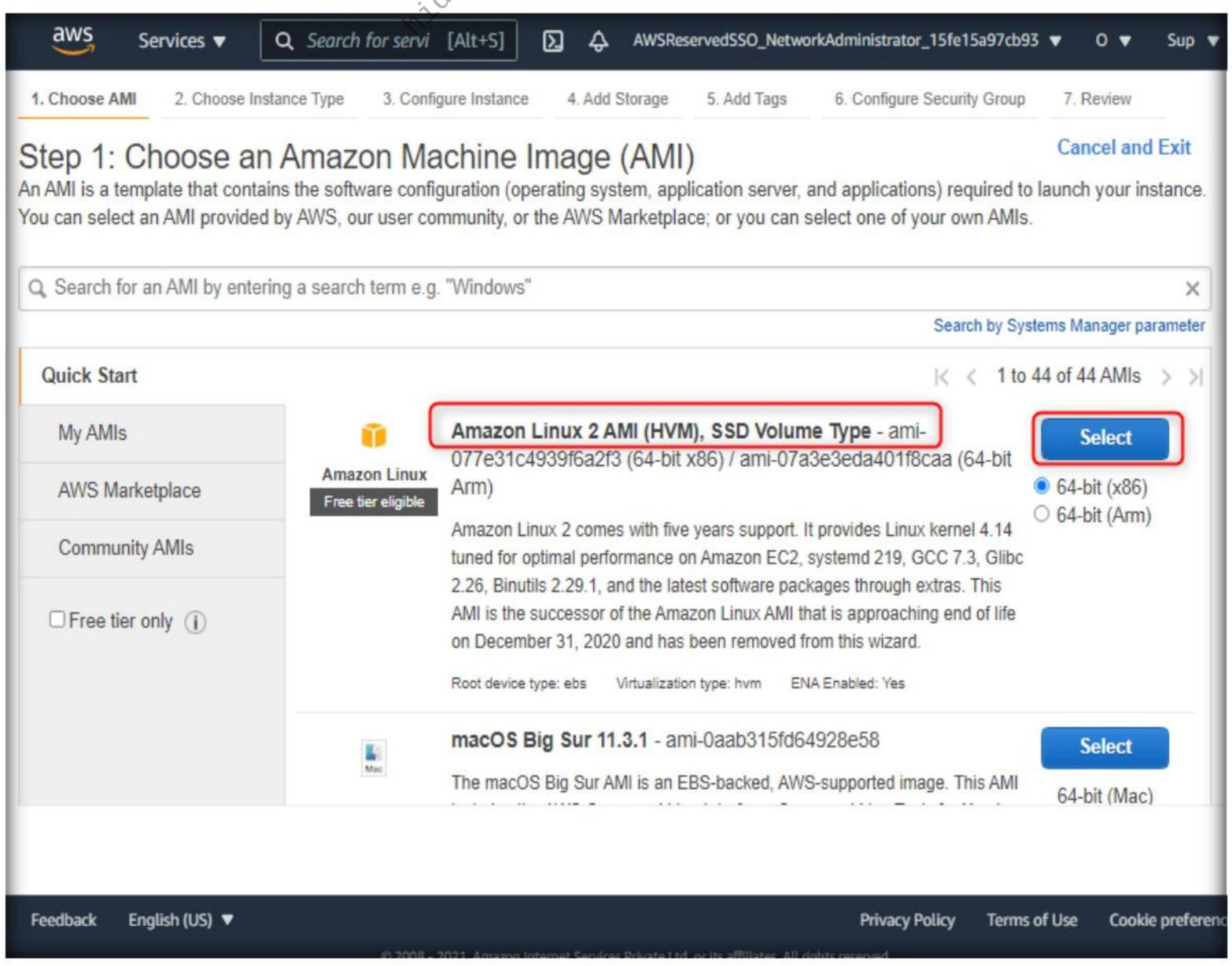


FIGURE 3.2.119: Selecting Amazon Linux 2 AMI Image

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

120. You will see an error because these permissions are not provided to the user.

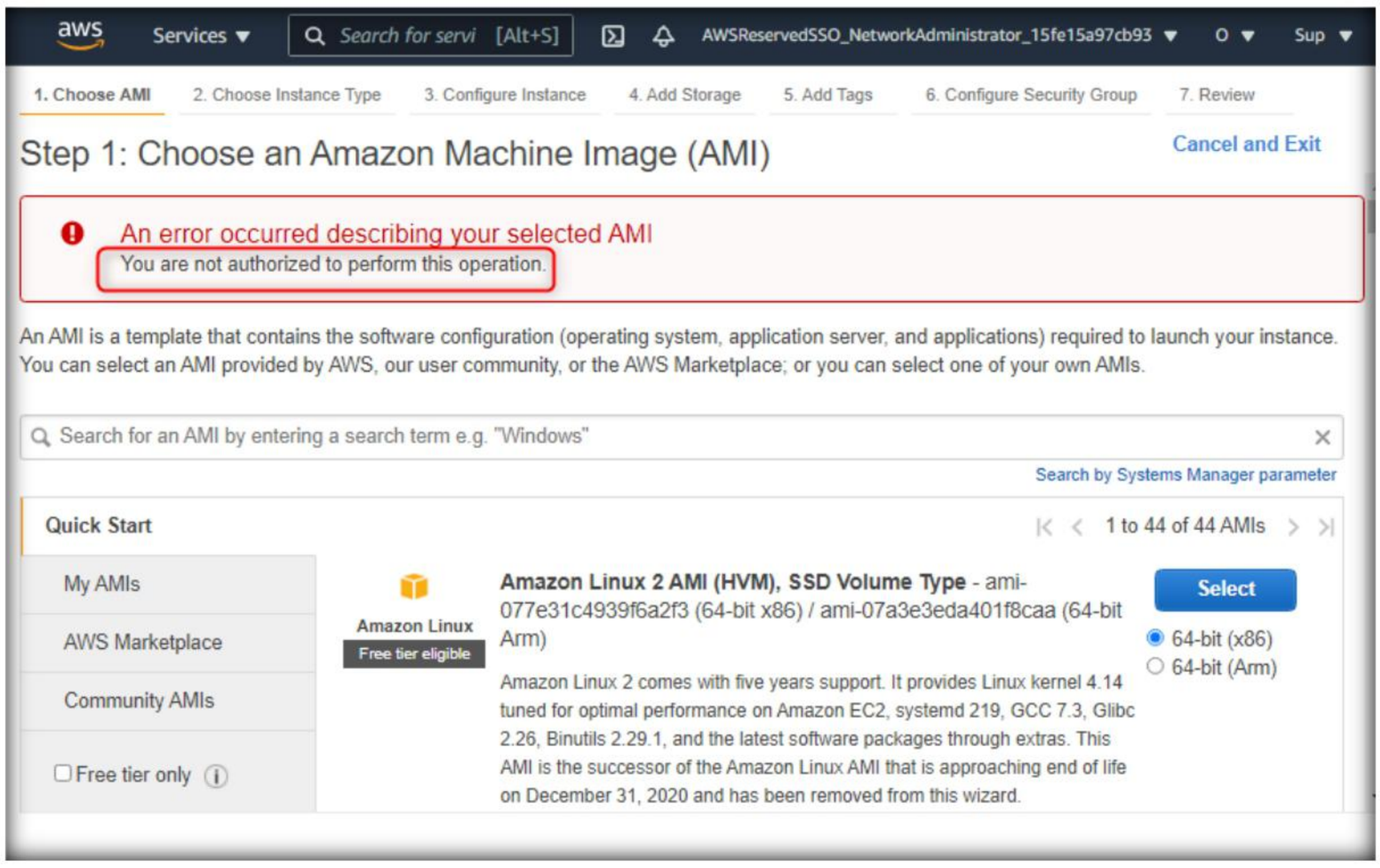


FIGURE 3.2.120: Error in Performing the Operation

121. Thus, with SAML based Single Sign-on service in Azure, a cloud security engineer can implement single sign-on and also enforce the principle of least privilege to restrict access to users and secure the Azure environment.

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

122. To delete the user, go back to Azure and click on **Home**.

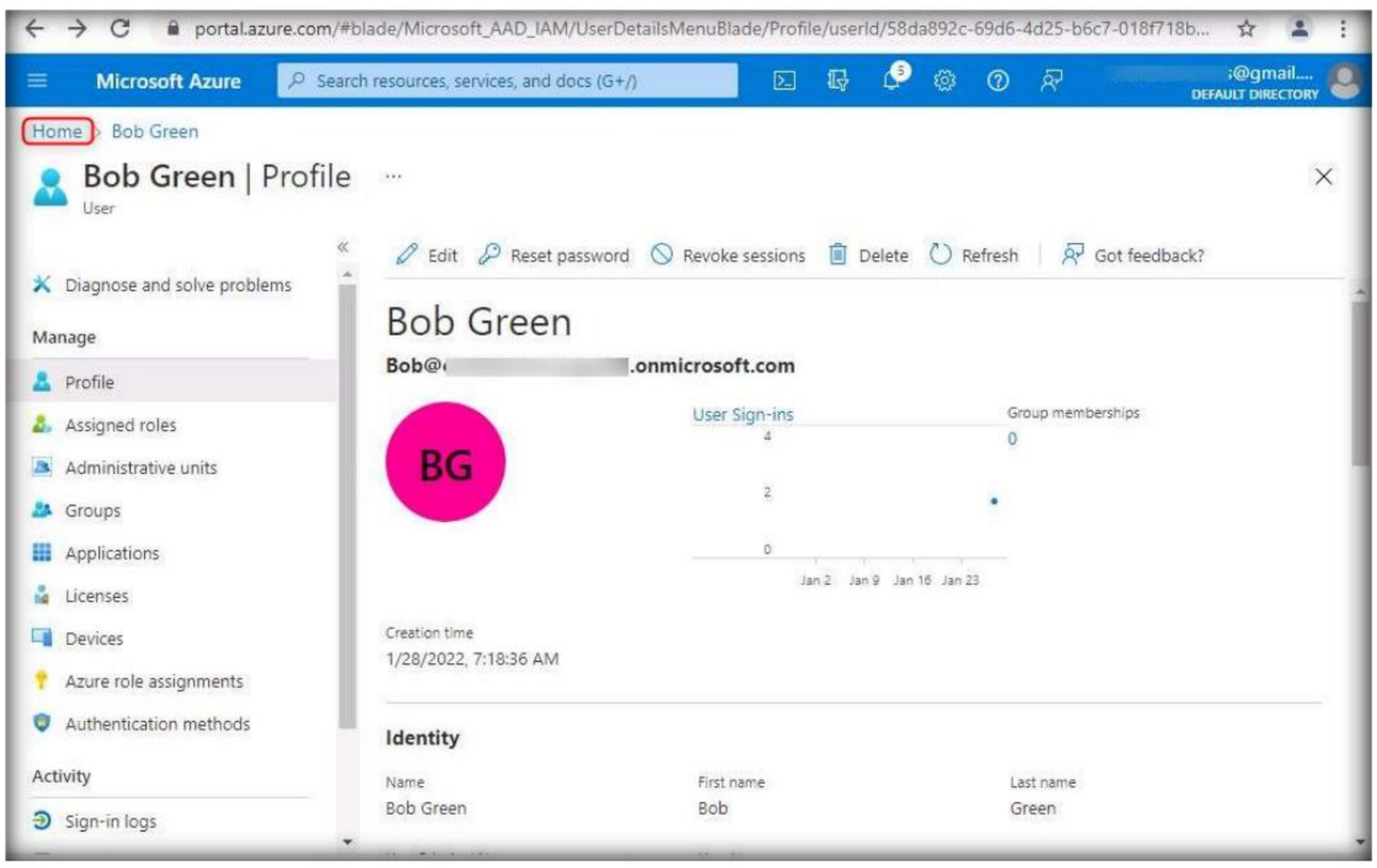


FIGURE 3.2.121: Navigating Back to Azure Portal Home Page

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

123. Click on the Azure portal menu on the left side. Navigate and click on **Azure Active Directory**.

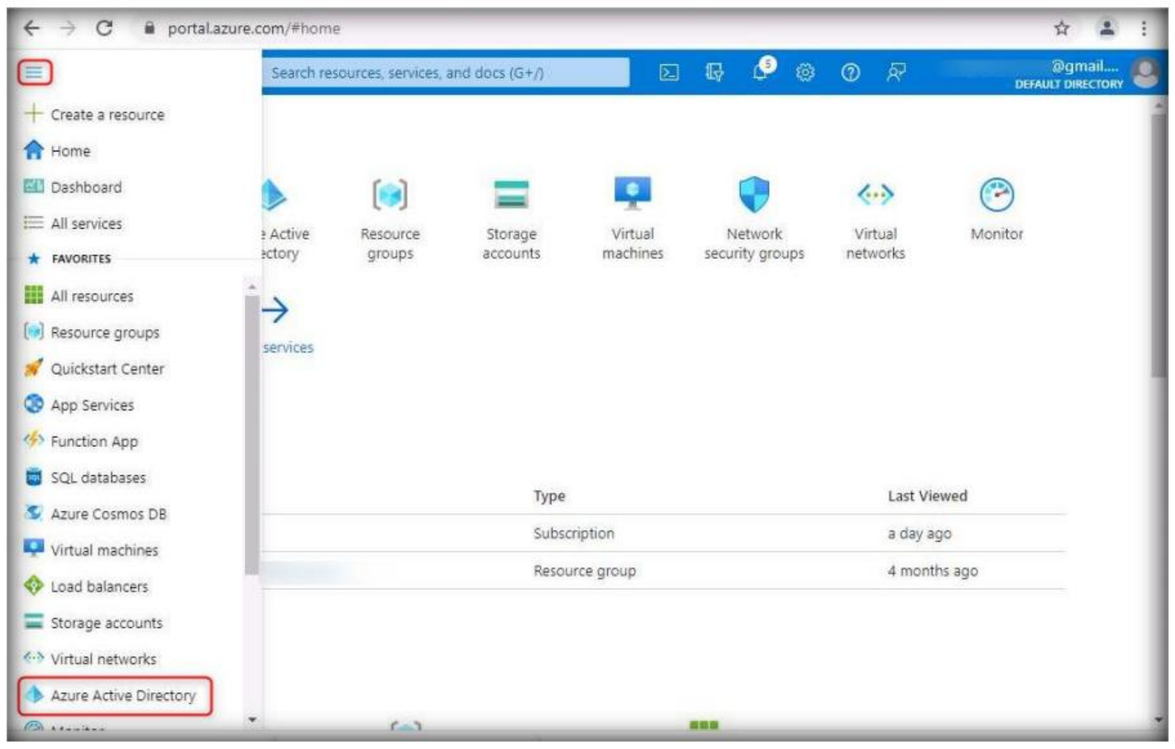


FIGURE 3.2.122: Navigating to Azure Active Directory

124. In the Default Directory window, under Manage, click on Users.

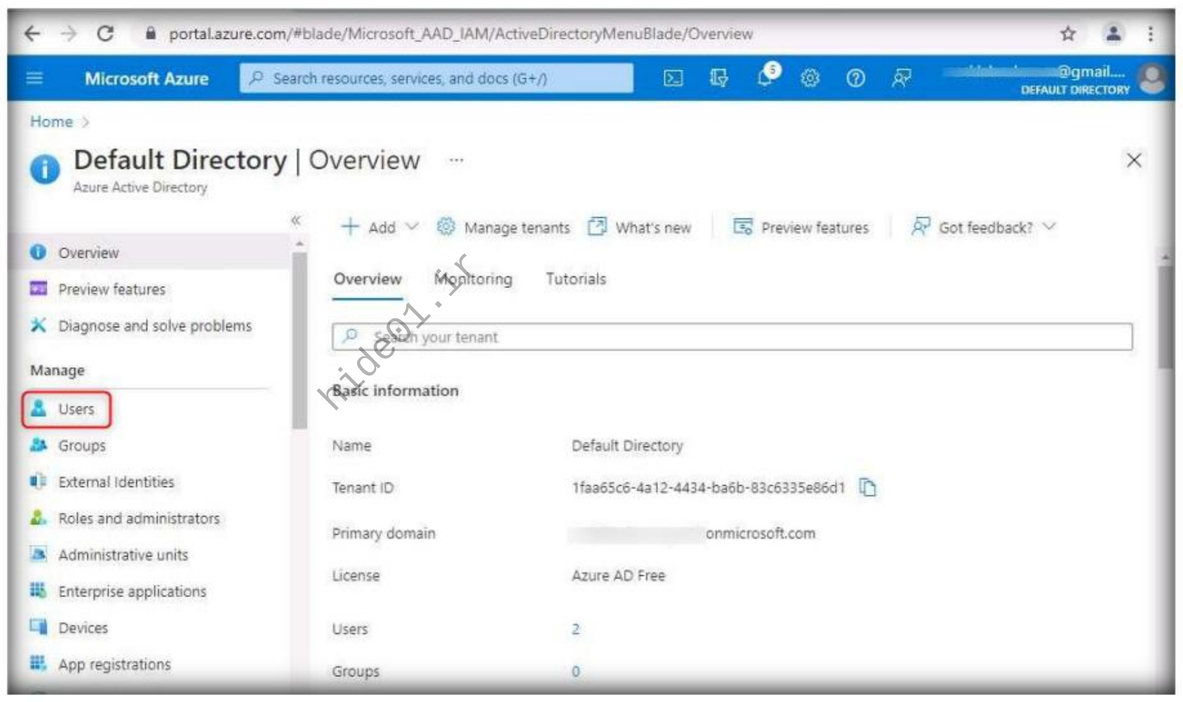


FIGURE 3.2.123: Navigating to Users

125. Select **Bob Green** user, click on the **three dots** present in the **menu bar**, navigate and click on **Delete user**.

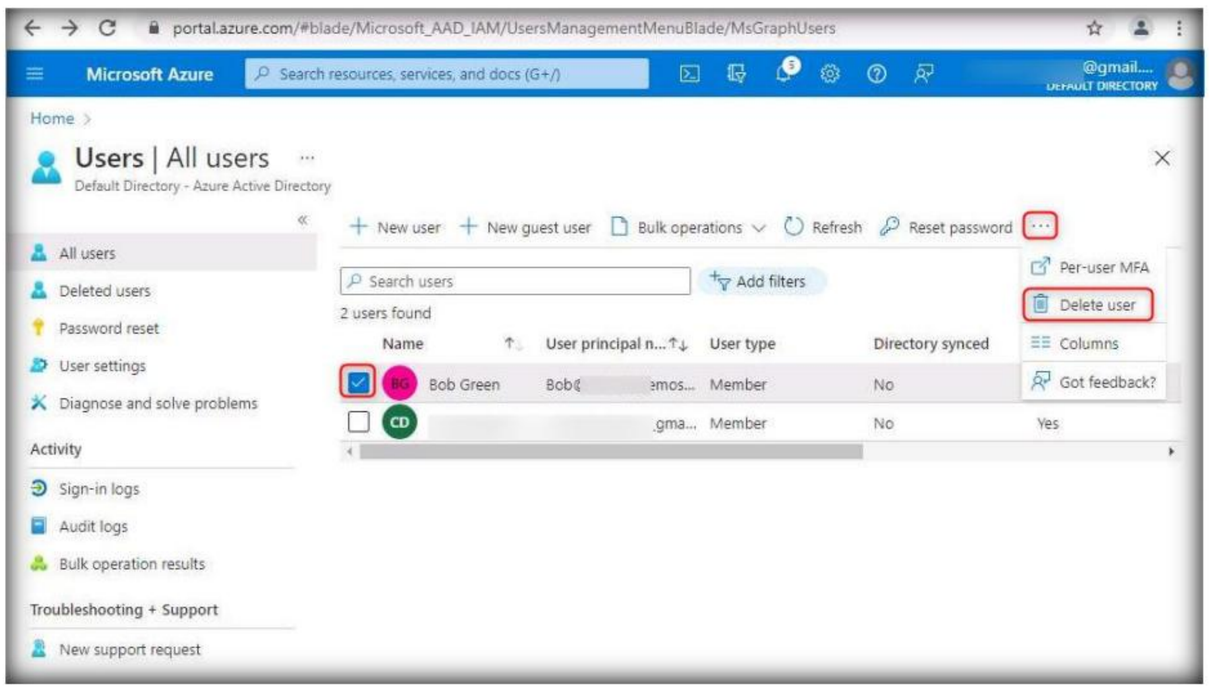


FIGURE 3.2.124: Deleting the User

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

126. Click **OK** button on **Delete selected users** window. The user will be successfully deleted.

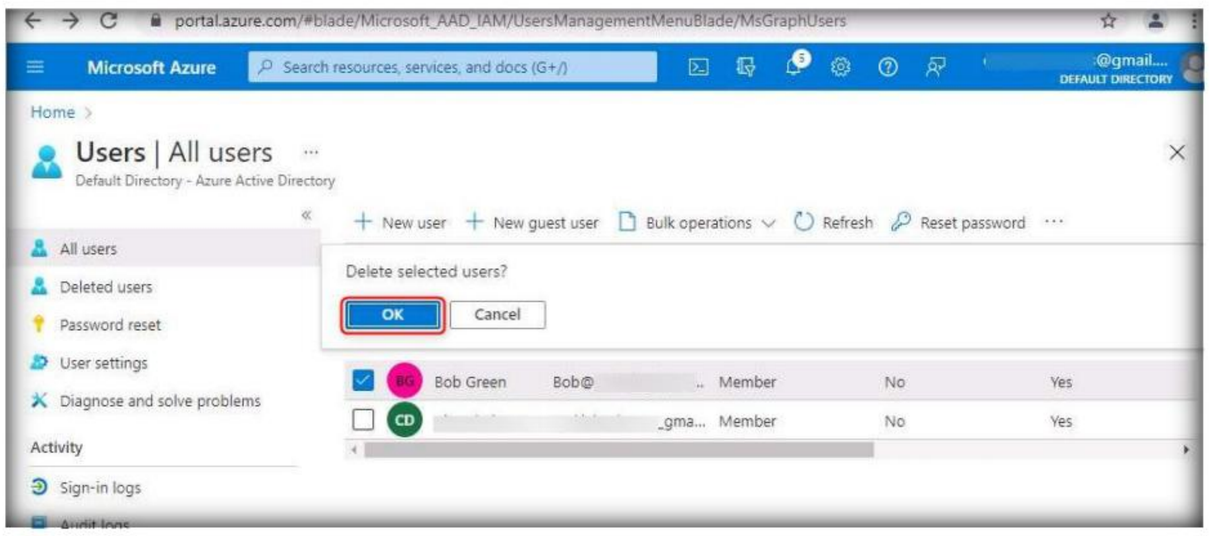


FIGURE 3.2.125: Confirm Deleting the User

127. From the Azure portal, navigate to Azure Active Directory. Click on **Enterprise applications** in the left pane and click on **AWS Single Sign-On**. Click on **Properties** in the left pane and click on **Delete**.

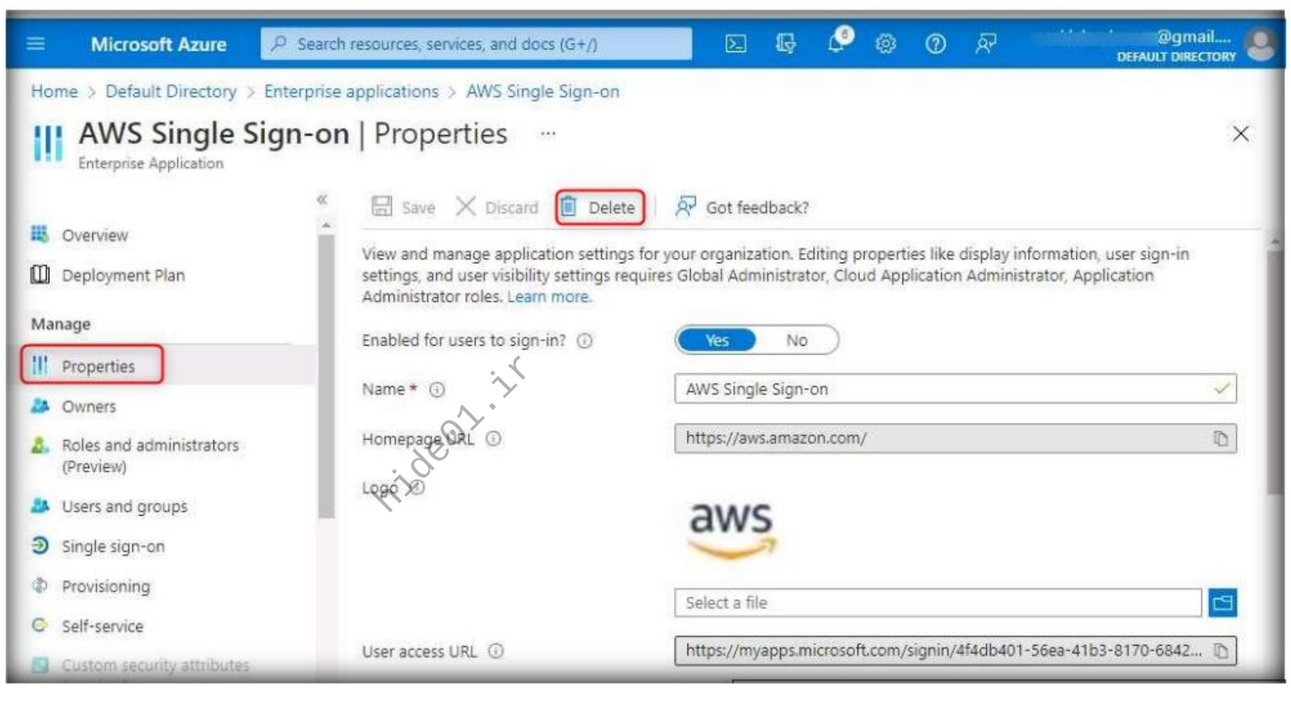


FIGURE 3.2.126: Deleting AWS Single Sign-on

128. Navigate to **AWS SSO** in AWS Management Console. Click **Users** in the left pane and select **Bob Green** user. Click on **Remove users**. Type **REMOVE** and click on **Remove provisioned users**.

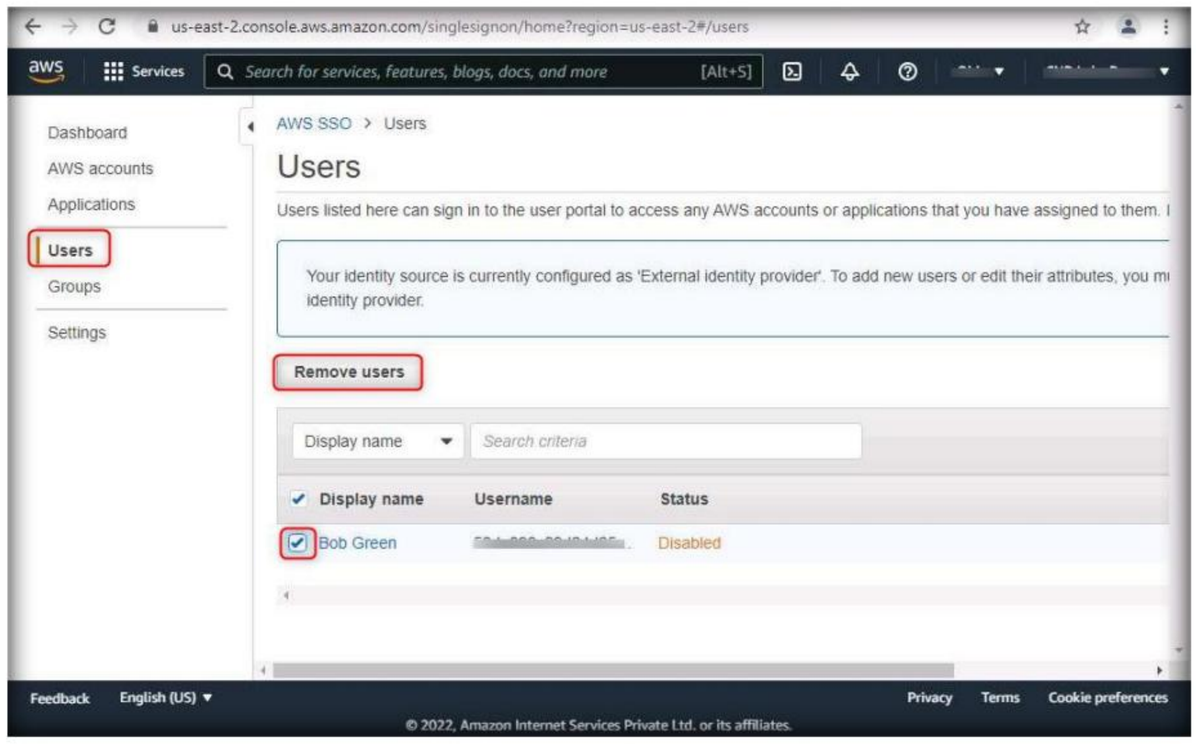


FIGURE 3.2.127: Removing Users from AWS SSO

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

129. In the AWS SSO window, click on **AWS accounts** in the left pane. Click on the name of the root user. Under **Permission sets**, click on **Remove** next to Network Administrator. Click **Remove access**.

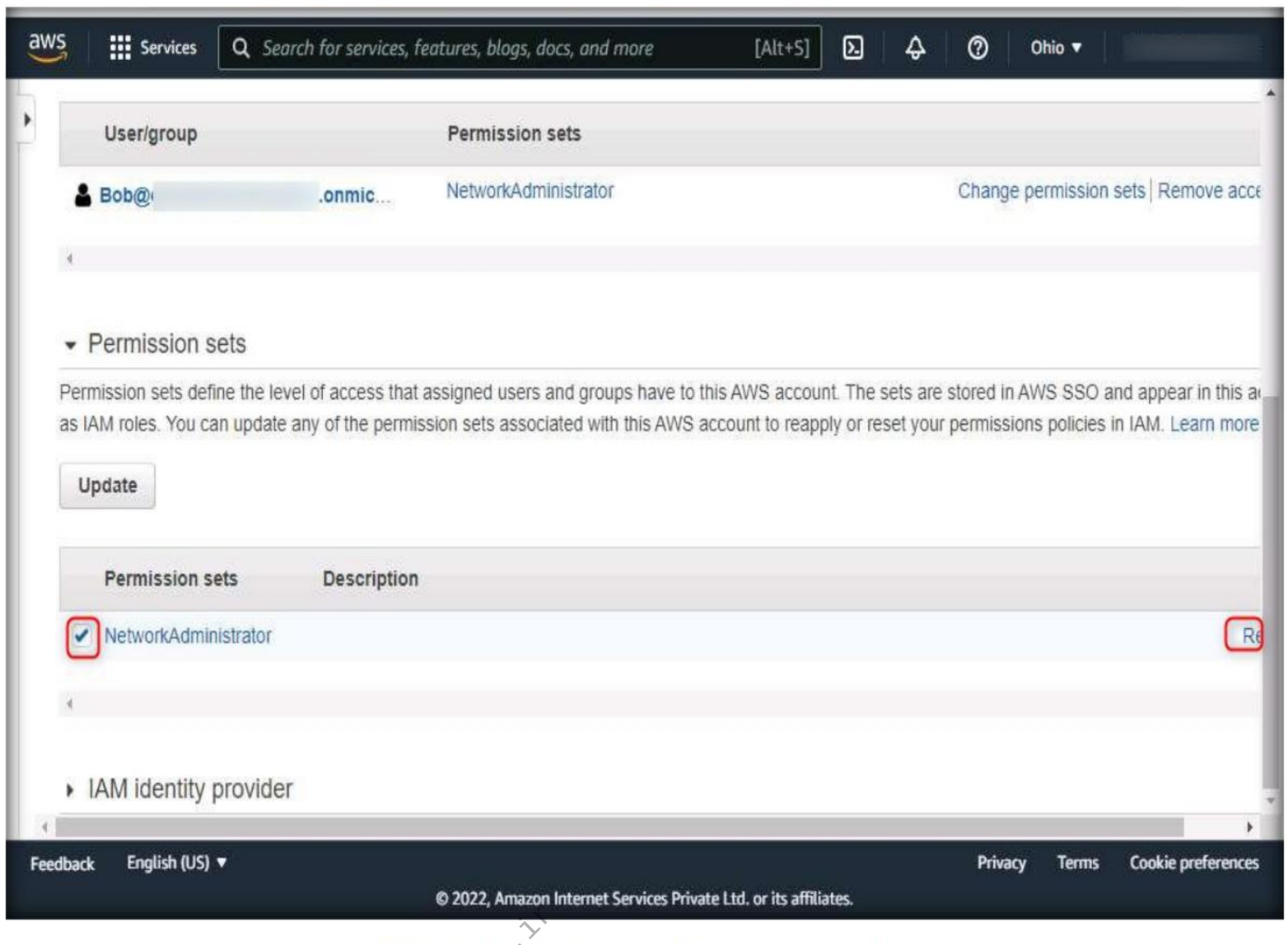


FIGURE 3.2.128: Removing Permission Sets for User

130. Click **AWS accounts** in the left pane. Click on the **Permission sets** tab. Select the radio button for NetworkAdministrator and click on **Delete**.

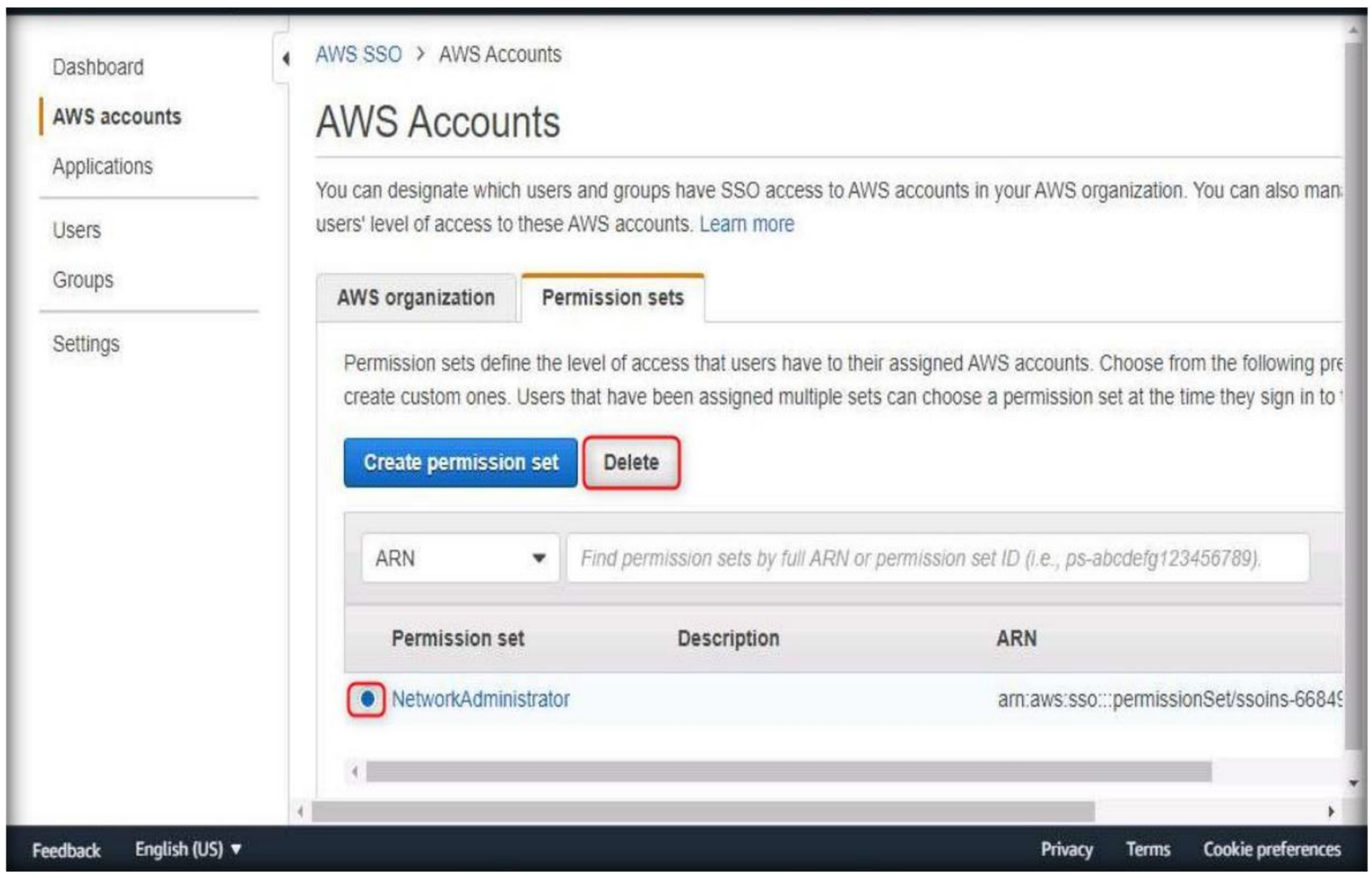


FIGURE 3.2.129: Deleting Permission Set

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

131. Click on **Settings** in the left pane of AWS SSO. Scroll down and click on **Delete AWS SSO configuration**. In the next window, select all the checkboxes and type DELETE. Click on **Delete AWS SSO**.

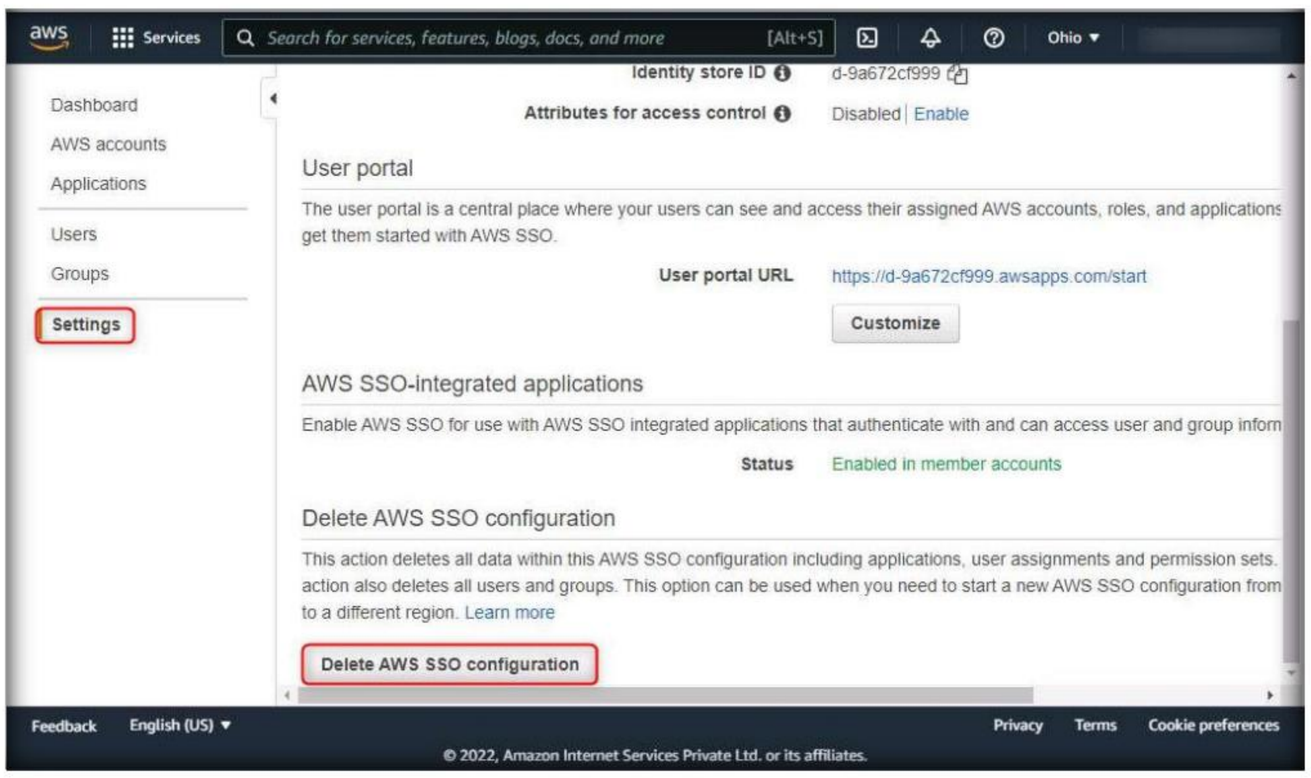


FIGURE 3.2.130: Deleting AWS SSO configuration

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.

hidoo.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab

3

Using Azure AD Multi-Factor Authentication Settings to Block and Unblock Microsoft Azure User

Azure AD offers Multi-Factor Authentication to allow an administrator to block or unblock a user from accessing the system.

ICON KEY

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

Lab Scenario

A cloud security engineer can block and unblock a specific user from receiving Azure Multi-Factor Authentication (MFA) requests using Azure AD MFA settings. Any authentication attempts from the blocked users will be denied automatically.

Lab Objectives

The objective of this lab is to demonstrate how to create a new user in Azure active directory (AD) and block and unblock them using Azure AD MFA.

In this lab you will:

- Create a new user in Azure AD
- Block and unblock the Azure AD user

Lab Environment

To perform this lab, you need the following:

- Admin Machine VM
- Registered Microsoft Azure account

Lab Duration

Time: 10 minutes

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Overview of Azure AD Multi-Factor Authentication

If a user device is stolen or lost, an Azure security administrator can block or unblock that user from receiving Azure MFA requests. The block and unblock features of Azure AD MFA prevent the user from receiving any authentication requests. It will help in safeguarding the Azure user's sensitive information against any unauthorized access. When blocked through Azure AD MFA, the user remained blocked for 90 days; however, an administrator can unblock the user manually at any point in time.

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.

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 New User in Azure AD

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

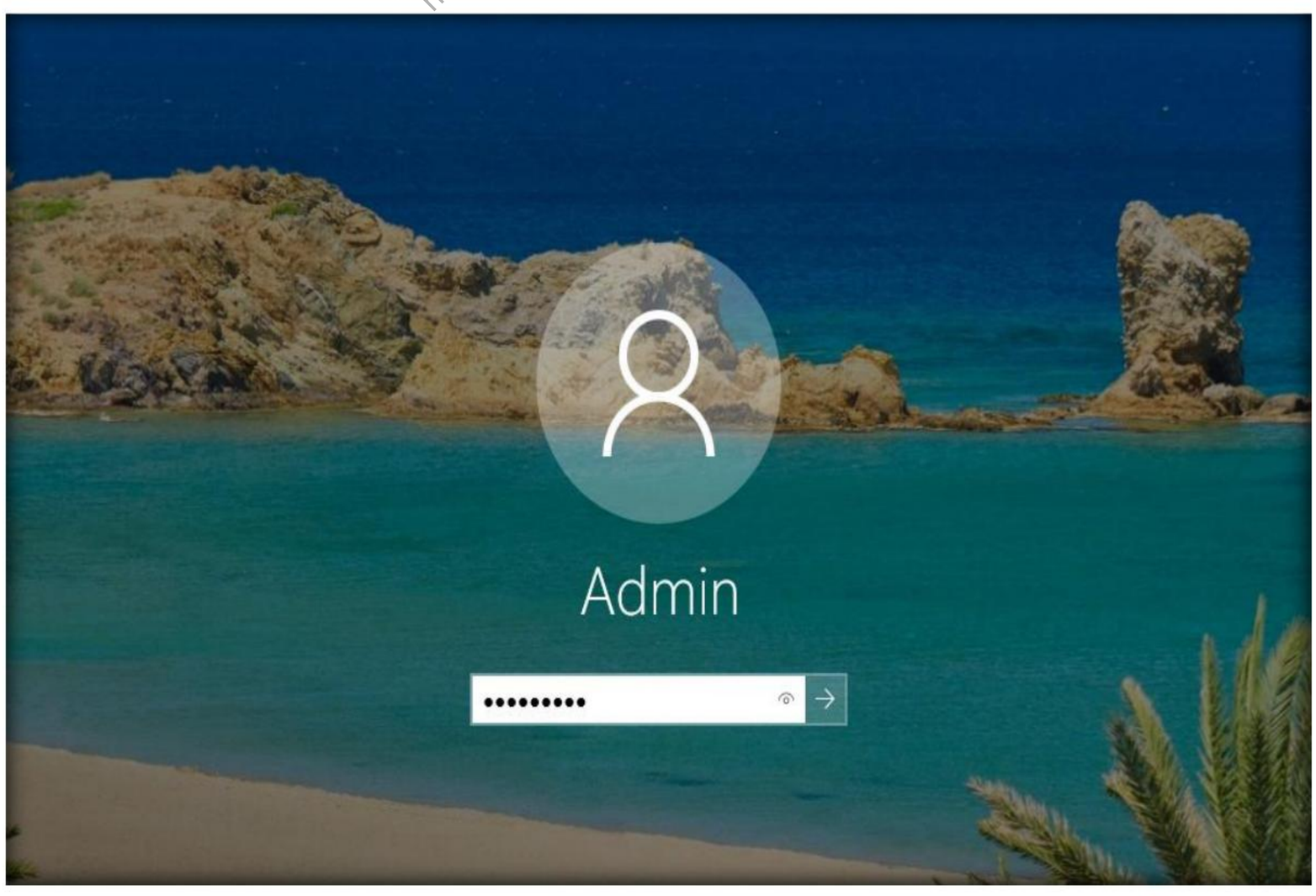


FIGURE 3.3.1: Launch Admin Machine and Log in

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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



FIGURE 3.3.2: 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**.

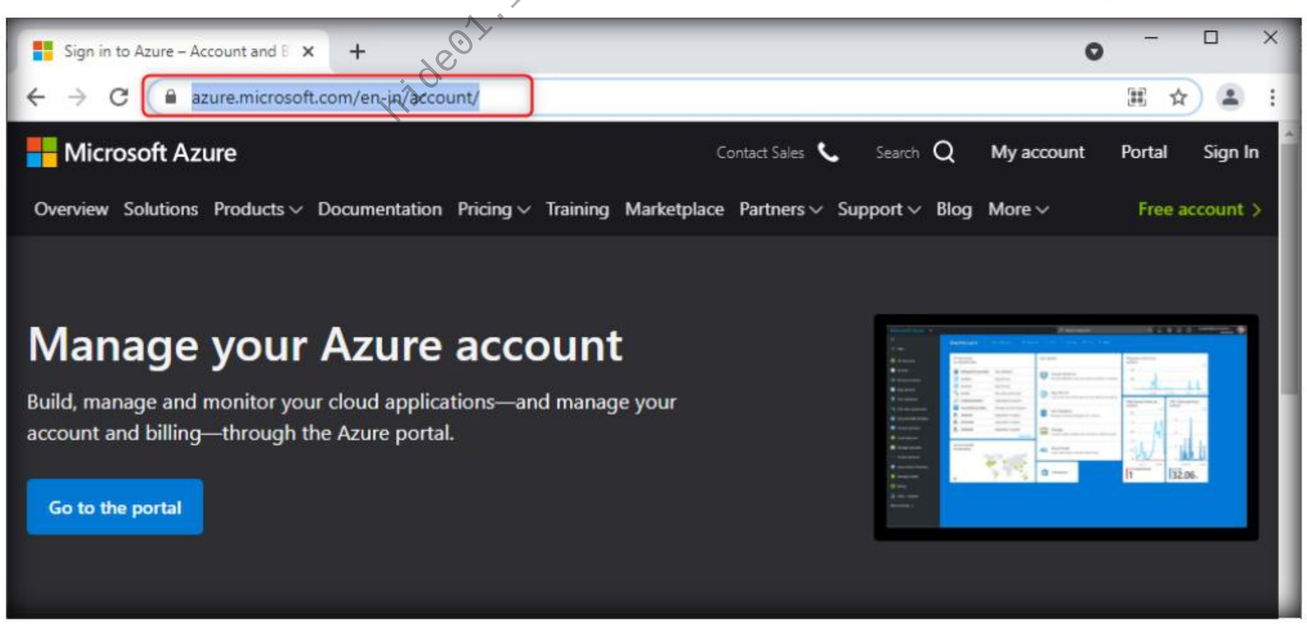


FIGURE 3.3.3: Entering the URL of Microsoft Azure

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

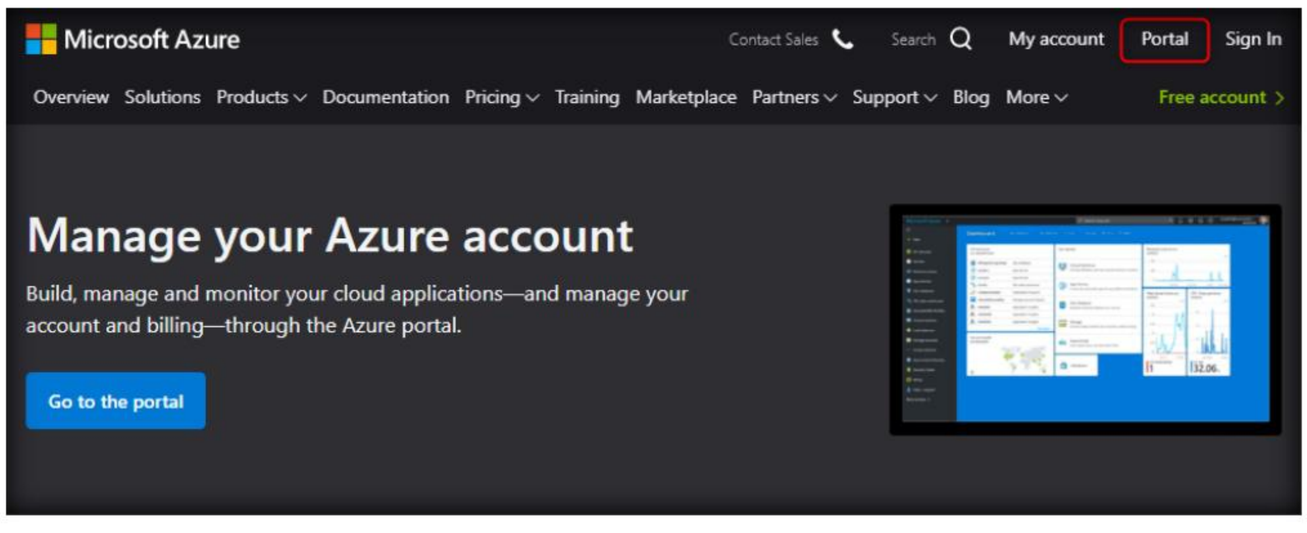


FIGURE 3.3.4: Sign into Azure Portal

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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

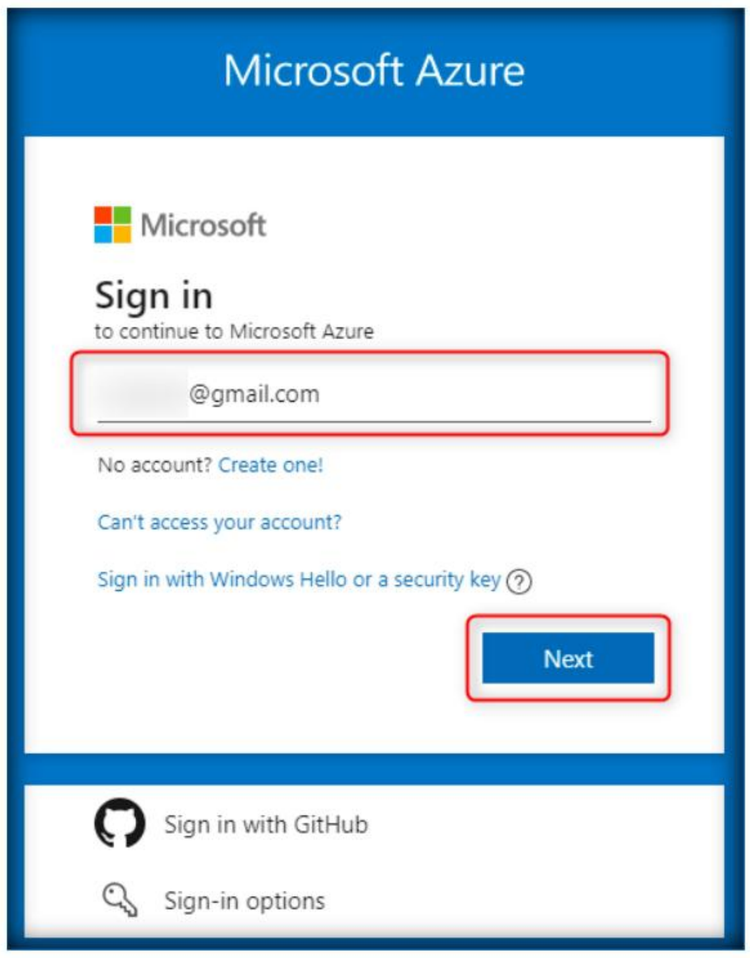


FIGURE 3.3.5: Entering Account ID to continue

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

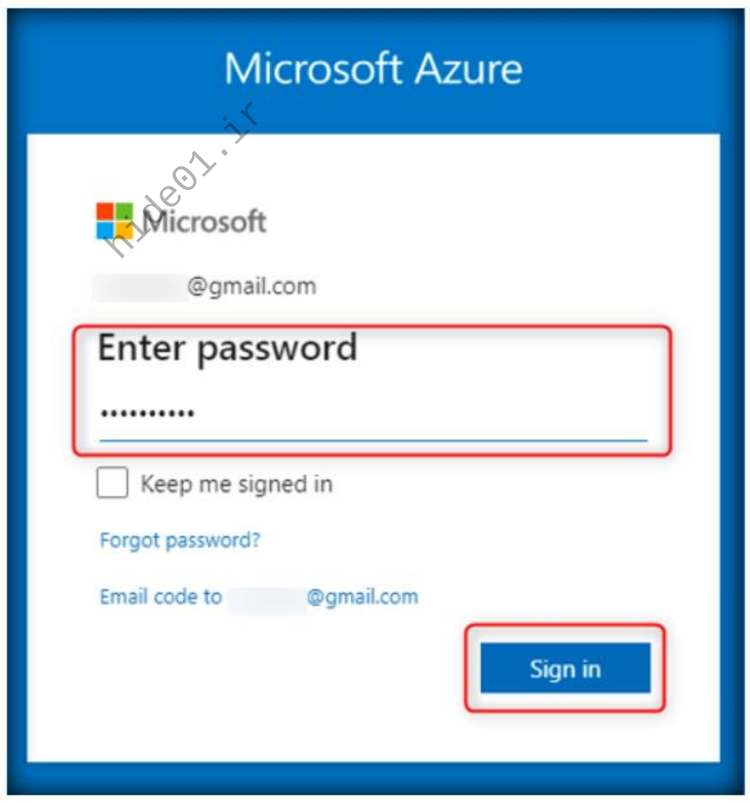


FIGURE 3.3.6: Entering the Log In Password

7. You will be successfully logged in to **Microsoft Azure portal**.

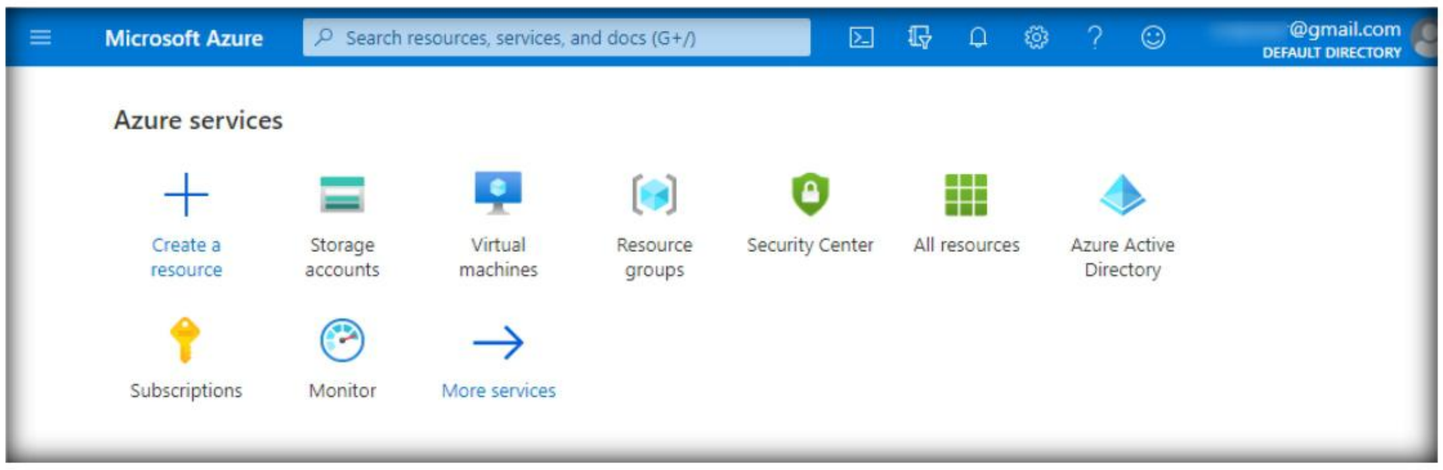


FIGURE 3.3.7: Microsoft Azure Portal

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

8. Click on the top left menu. Then, navigate and click on **Azure Active Directory**.

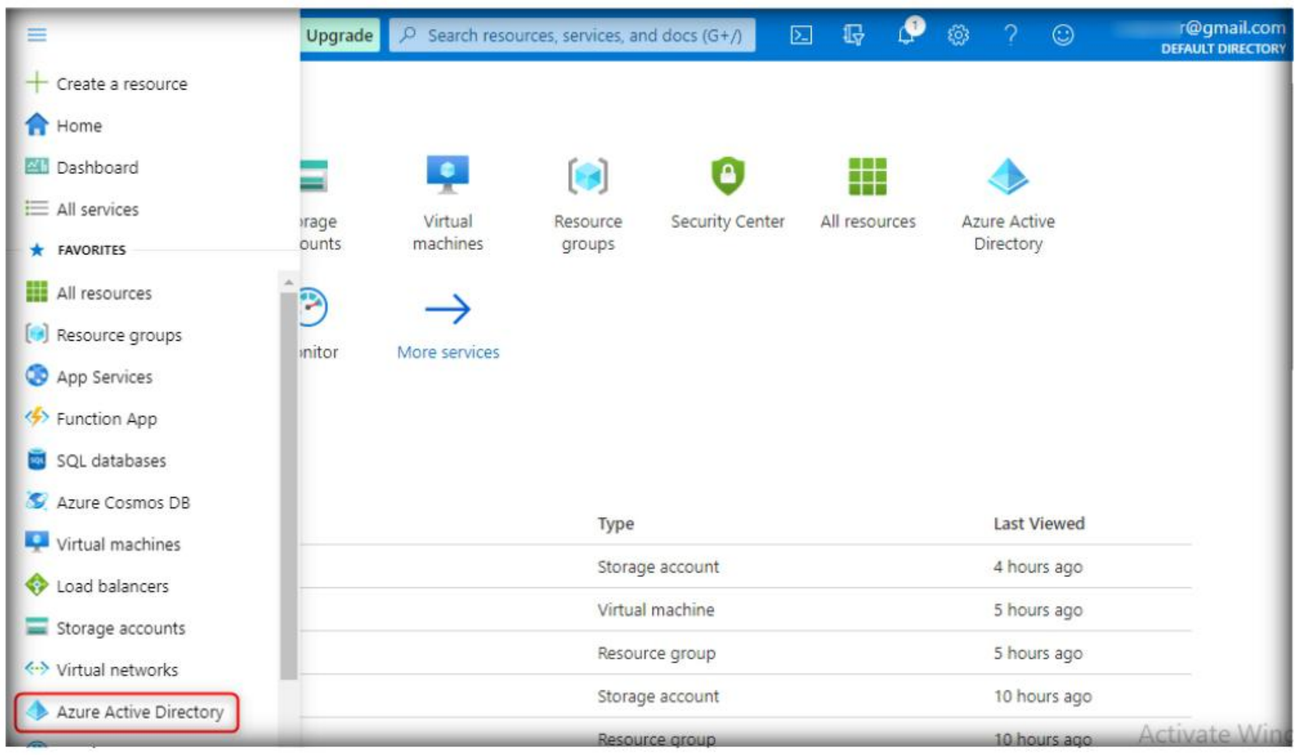


FIGURE 3.3.8: Selecting Azure Active Directory

9. In Azure AD, click on **Users** under **Manage** on the left pane.

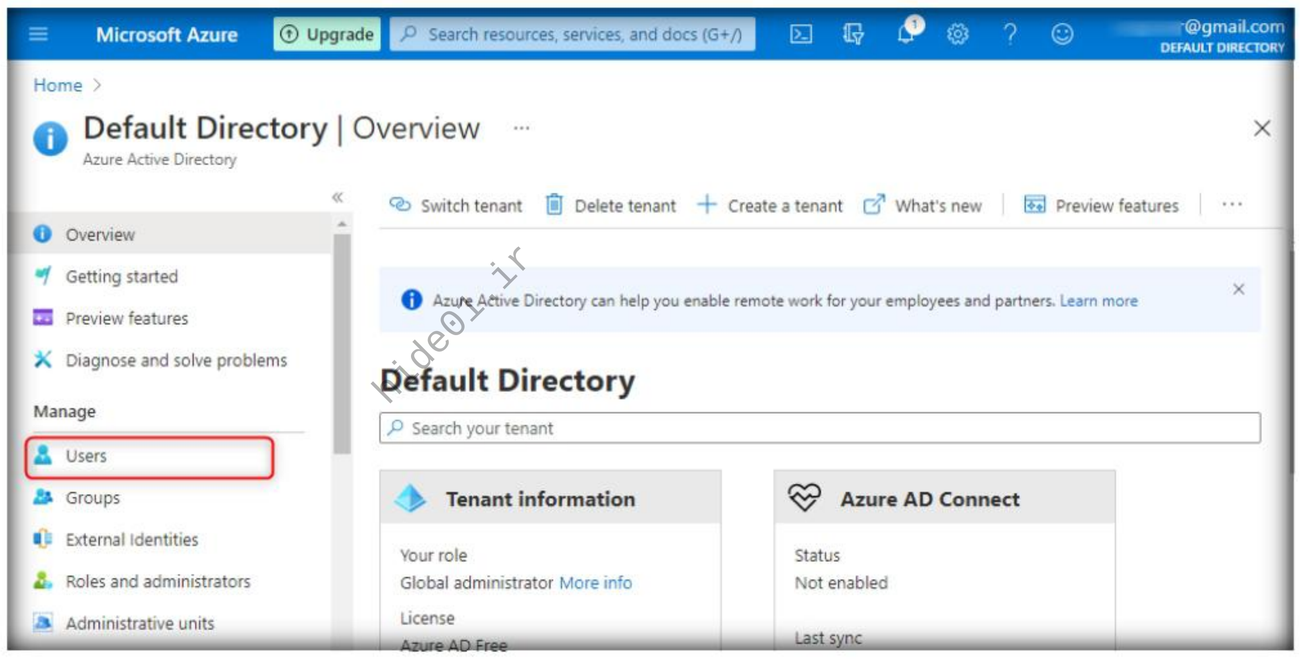


FIGURE 3.3.9: Selecting Users in Azure AD

10. To add a new user, click on **+New User**.

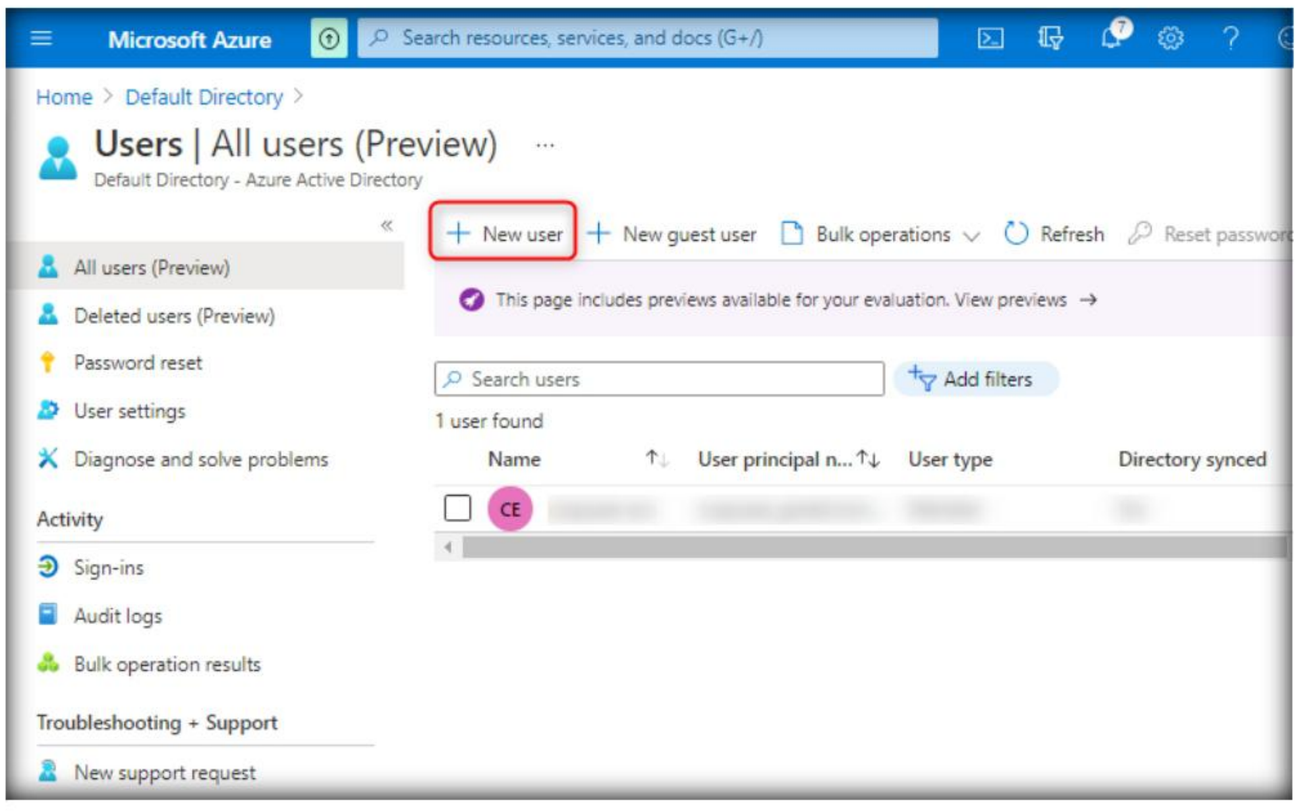


FIGURE 3.3.10: Creating New user

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

11. Select the **Create user** radio button in the **New user Default Directory** panel.

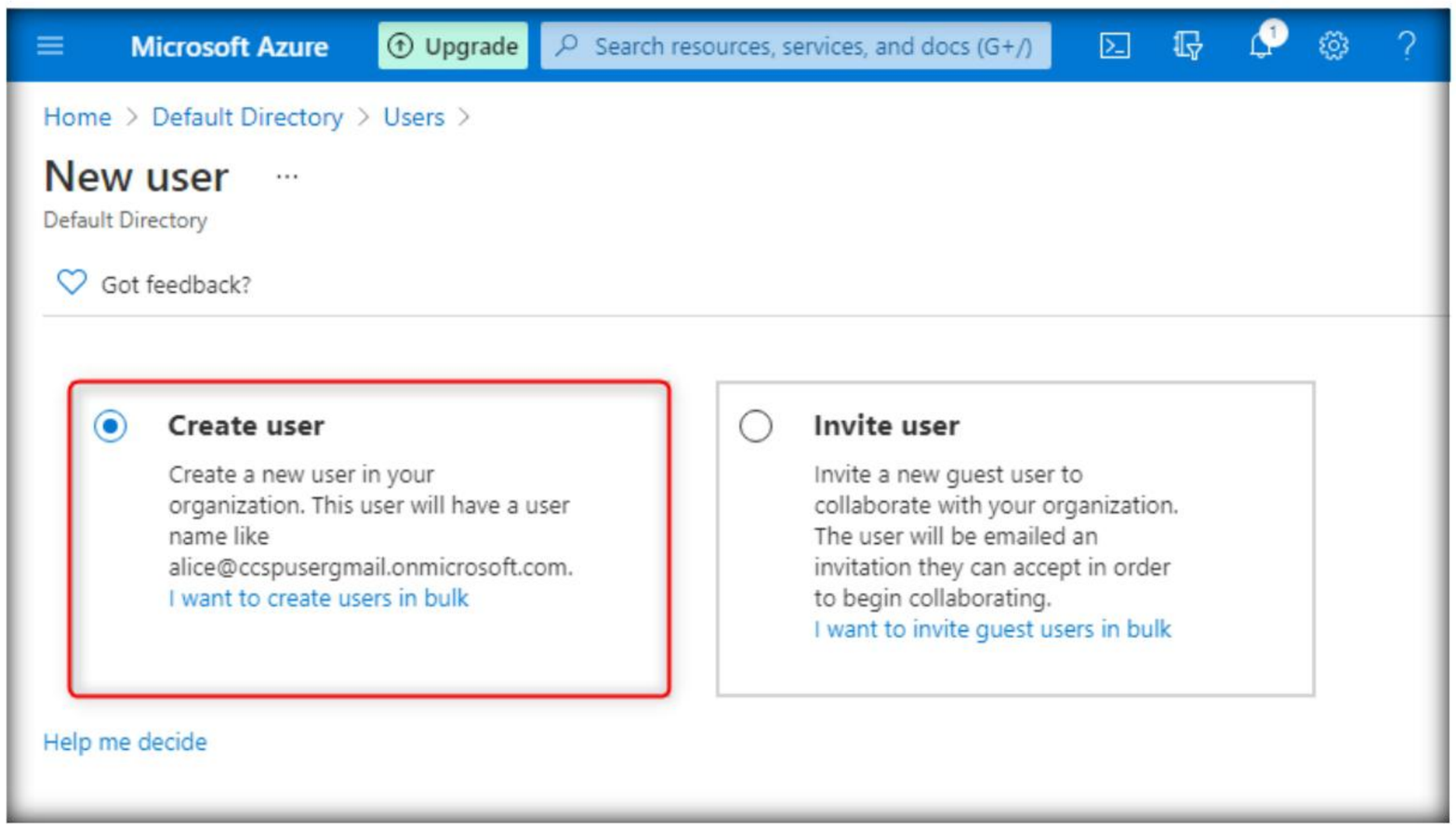


FIGURE 3.3.11: Selecting Create user radio button

12. Under **Identity**, enter the following user details:

    Username: **bob**

    Name: **Bob Watson**

    First name: **Bob**

    Last name: **Watson**

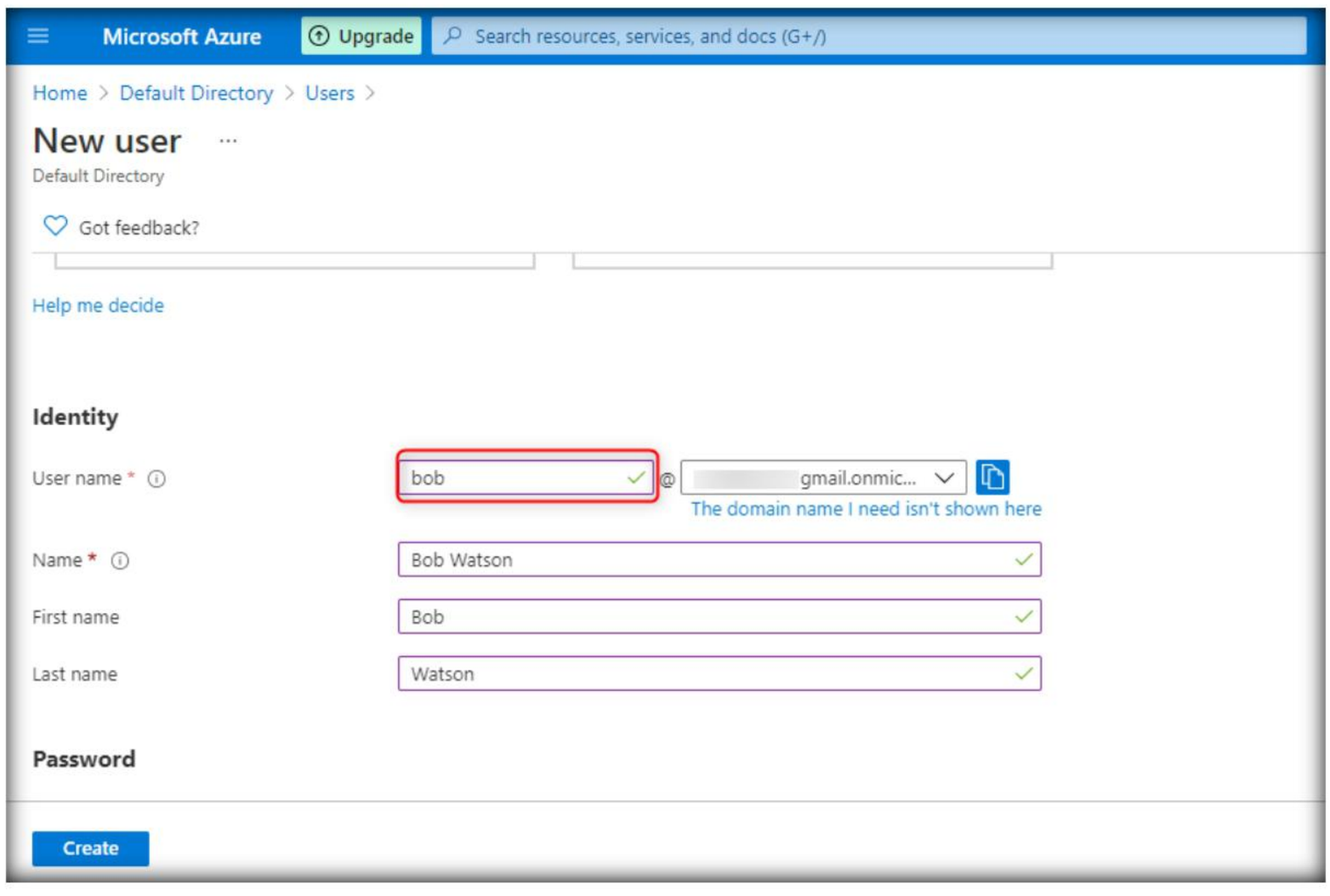


FIGURE 3.3.12: Entering User Details

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

13. Under the **Password** section, check the **Let me create the password** radio button and enter a password in the **Initial password** field. (here, we have entered **Secadmin@123**)

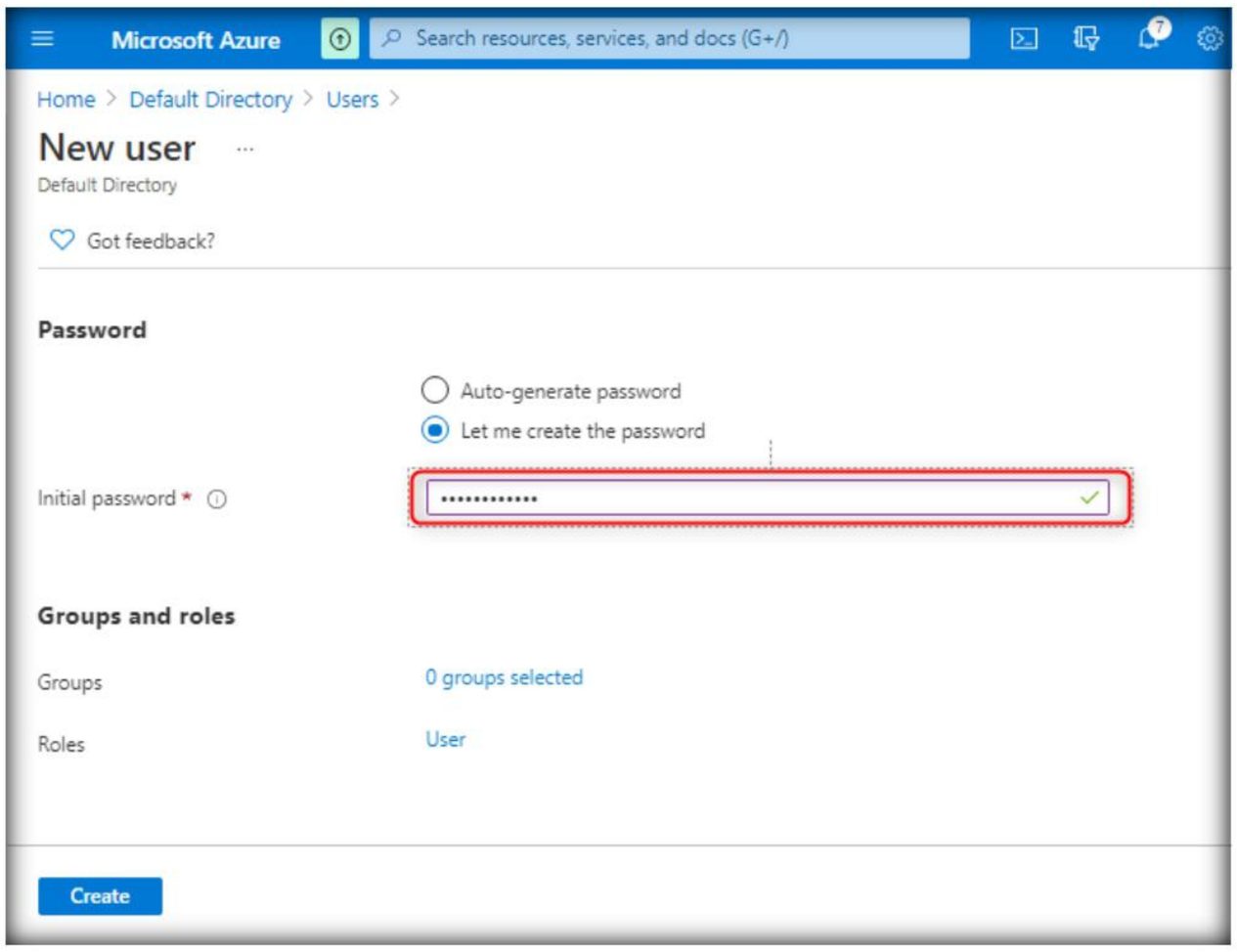


FIGURE 3.3.13: Creating a Password

14. Retain the default settings in the **Settings** section. In the **Job info** section, enter the following details:

Job title: Network administrator

Department: IT

Company name: Global Security Tech Ltd

Then, click on **Create**.

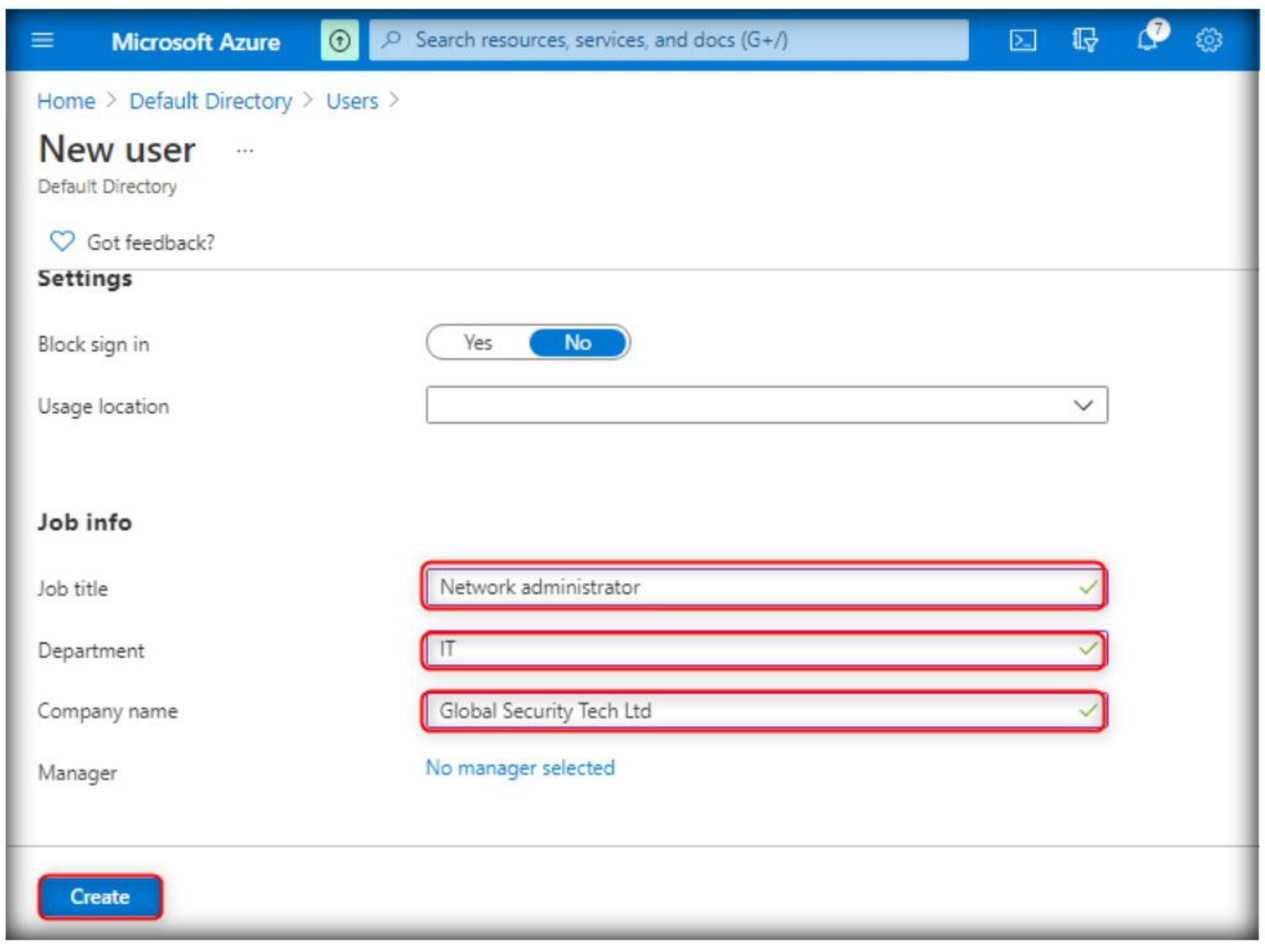


FIGURE 3.3.14: Entering Job Information of the User

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

15. The new user is now successfully created in Azure AD directory.

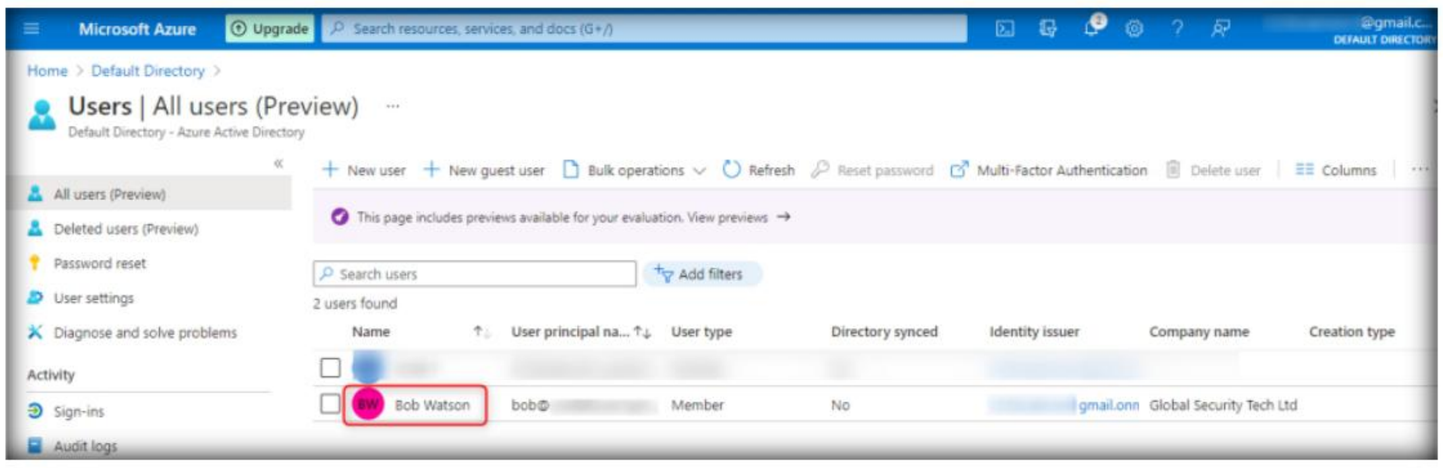


FIGURE 3.3.15: Successful Creation of New User

TASK 2

Blocking and Unblocking the Azure AD User

16. Click on the top left of the Azure portal menu. Then, navigate and click on **Azure Active Directory**.

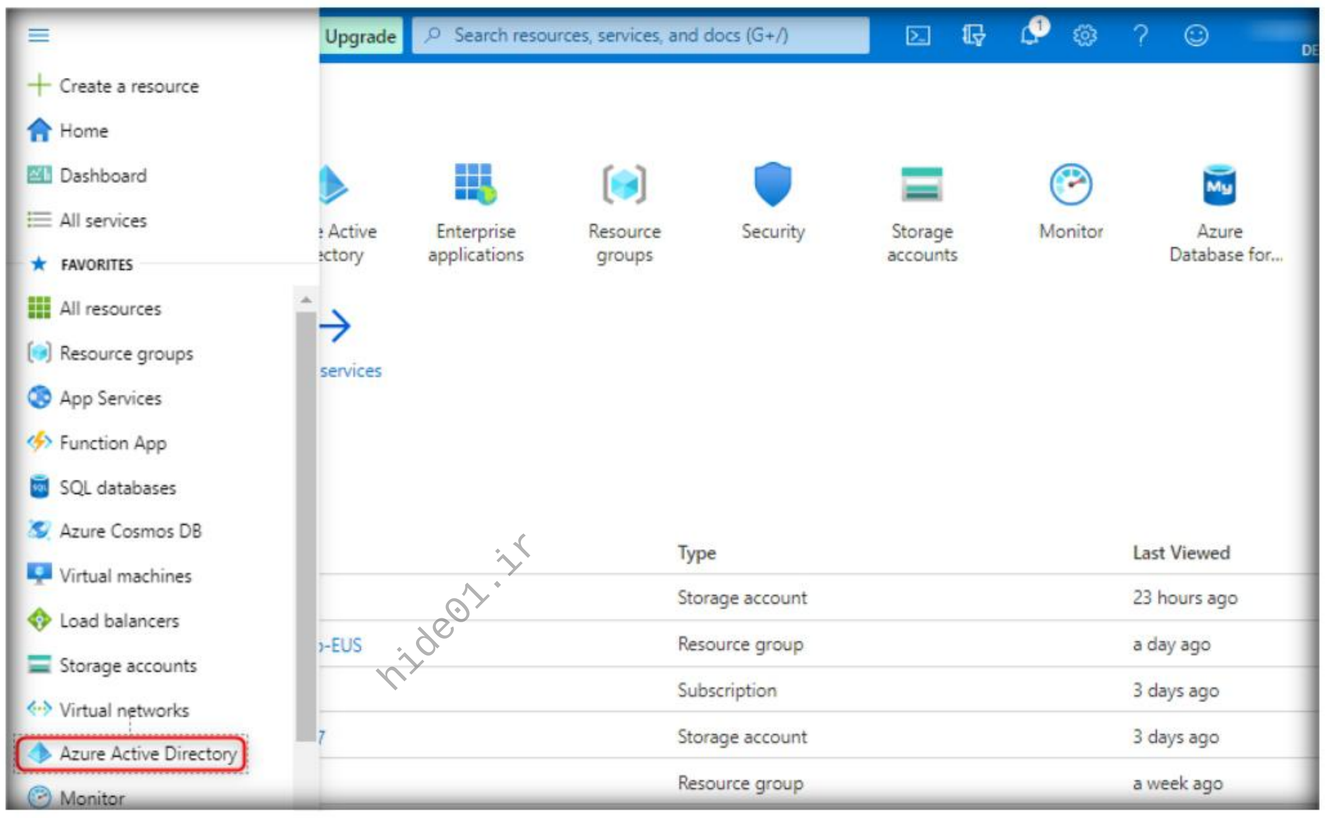


FIGURE 3.3.16: Selecting Azure Active Directory from Azure Portal

17. In the **Default Directory** window, navigate and click on the **Security** option under **Manage**.

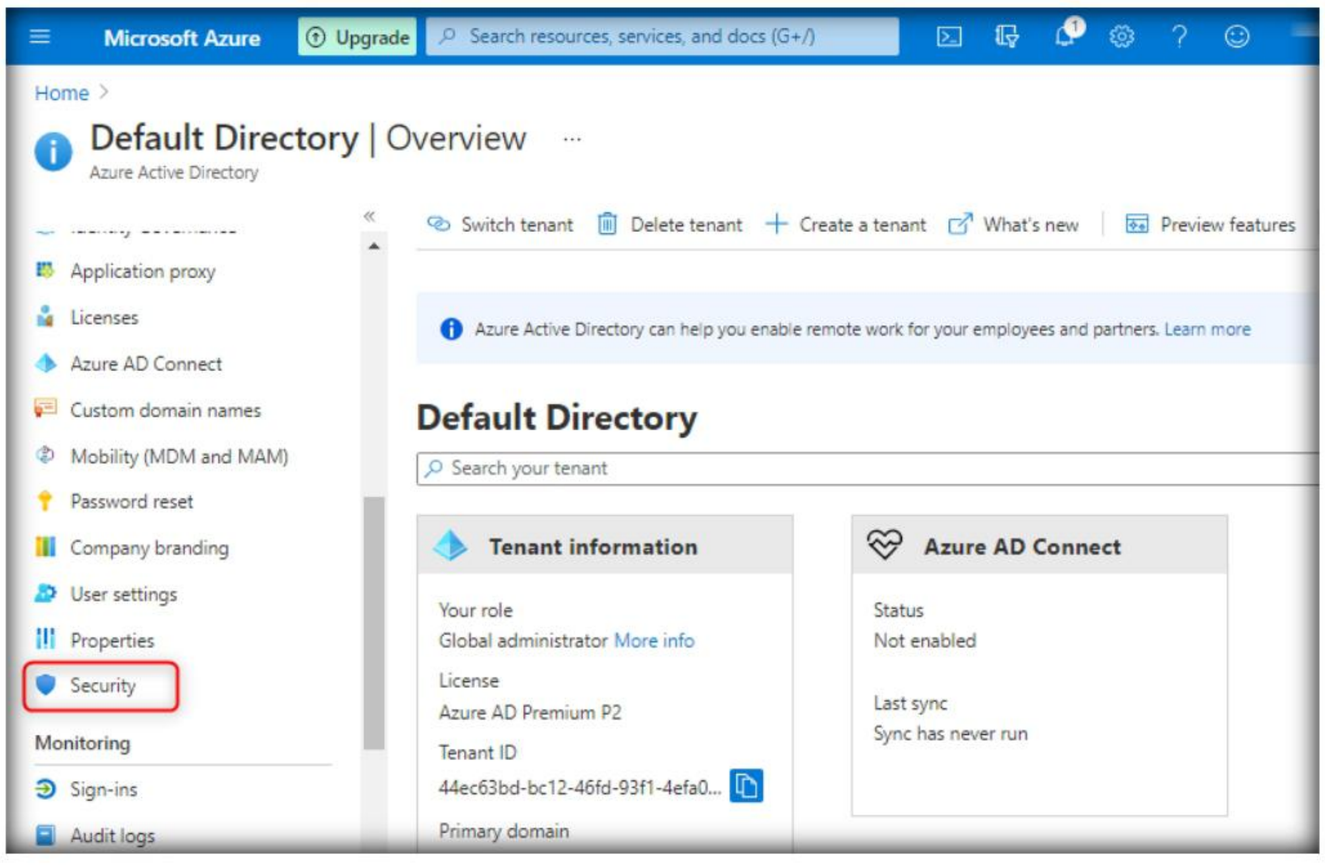


FIGURE 3.3.17: Selecting Security in Default Directory Window

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

18. In the **Security** window, navigate and click on **MFA** under **Manage**.

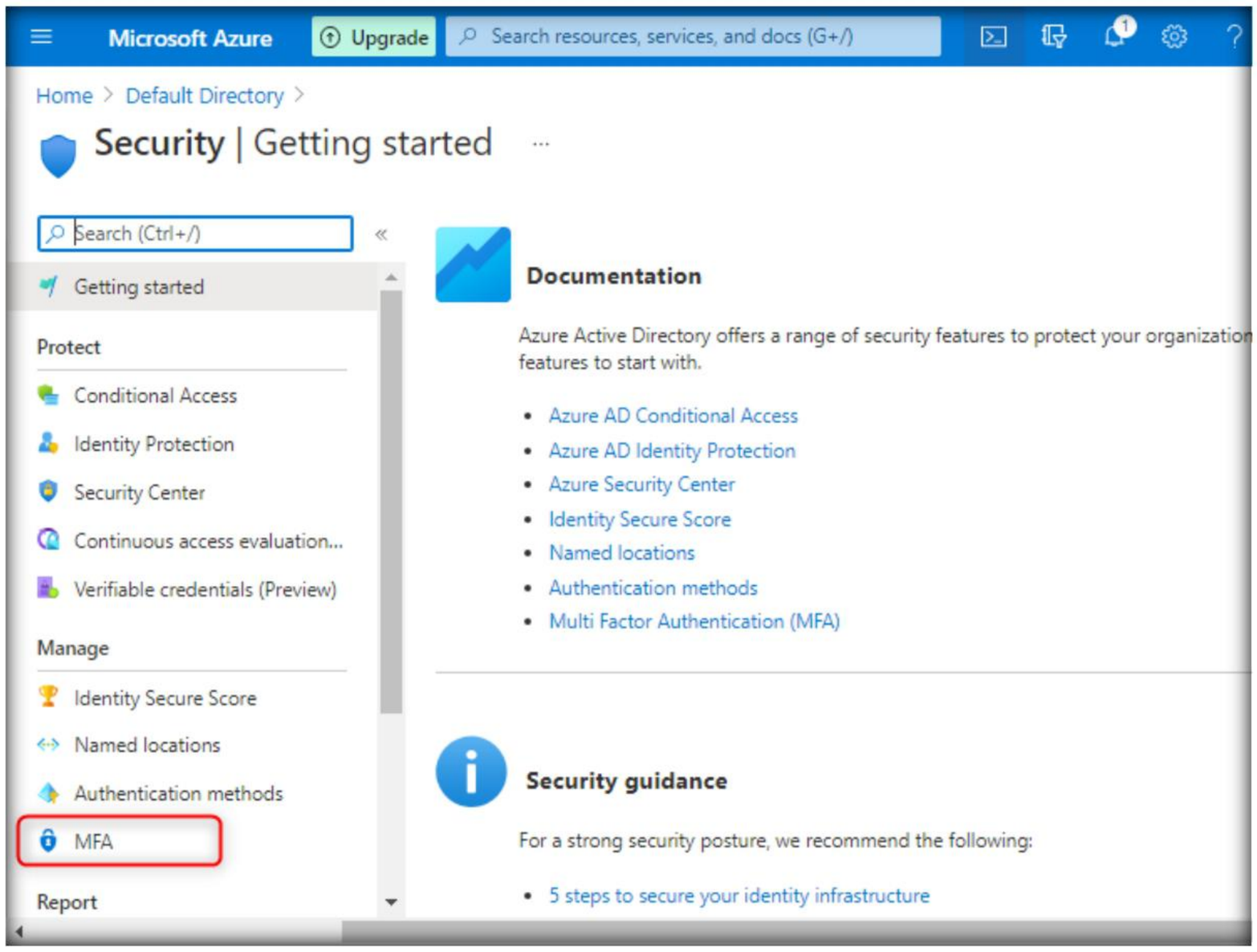


FIGURE 3.3.18: Selecting MFA in Security Window

19. Now, you will see the **Overview window**. Scroll down this window and click on the **Get Free Premium Trial** button.

Note: If AD MFA is already enabled, you may not see the activation screen and can directly go to **Step 23**.

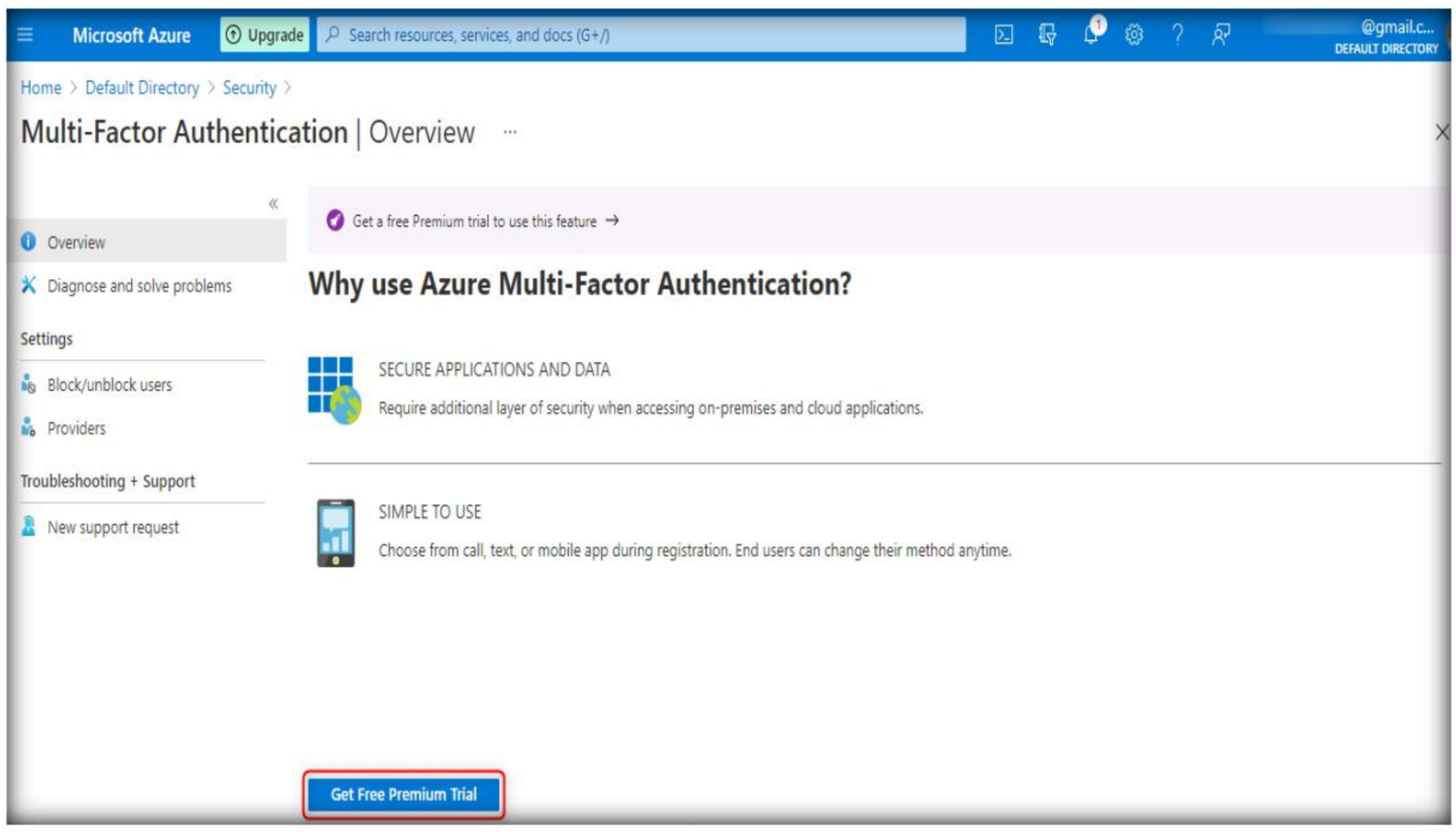


FIGURE 3.3.19: Selecting Get Free Premium Trial

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

20. An **Activate** window will appear now. You will have to activate both options step by step. Click on **Free trial** to expend the **ENTERPRISE MOBILITY + SECURITY ES** option.

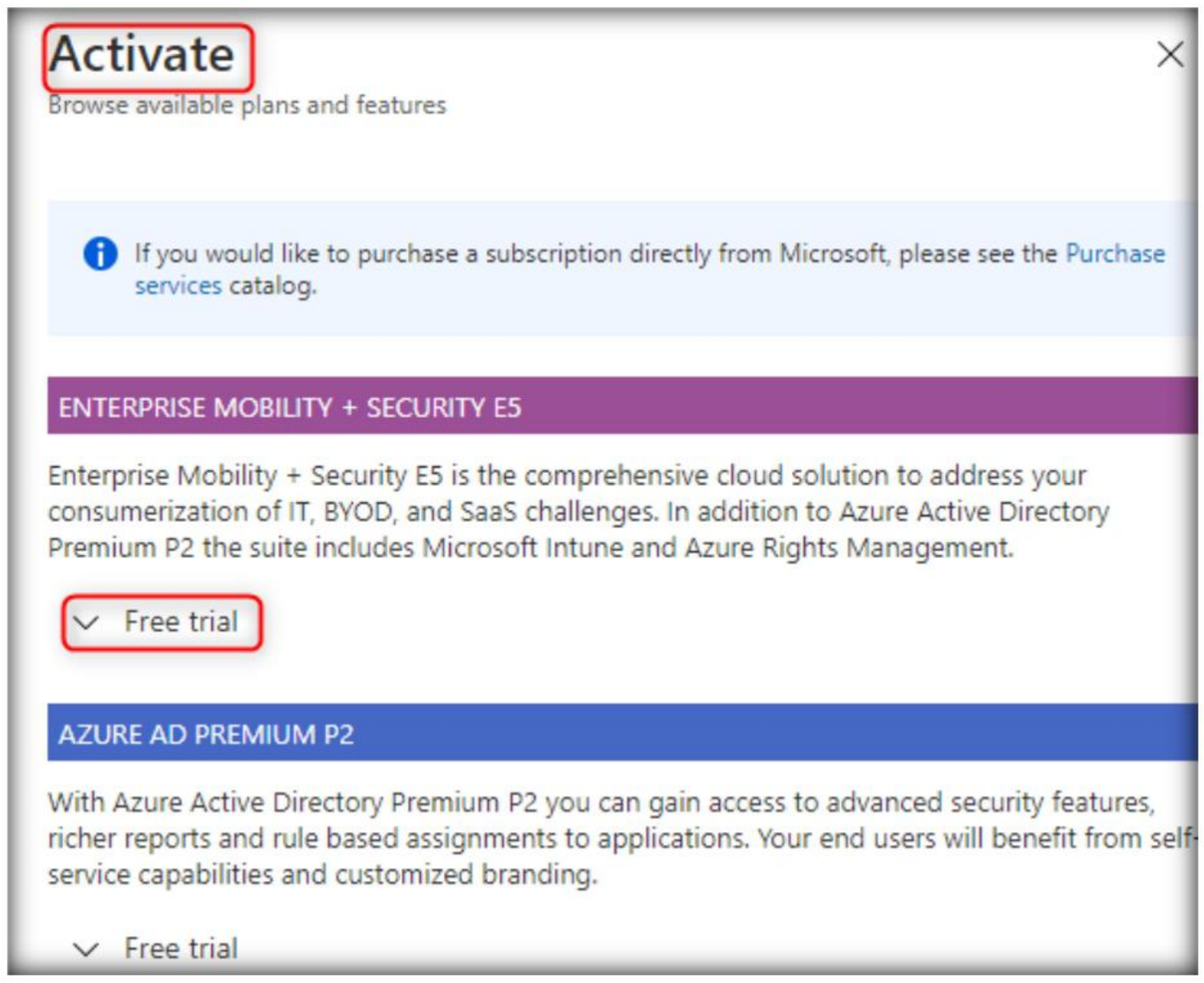


FIGURE 3.3.20: Selecting Activate window

21. Click on the **Activate** button.

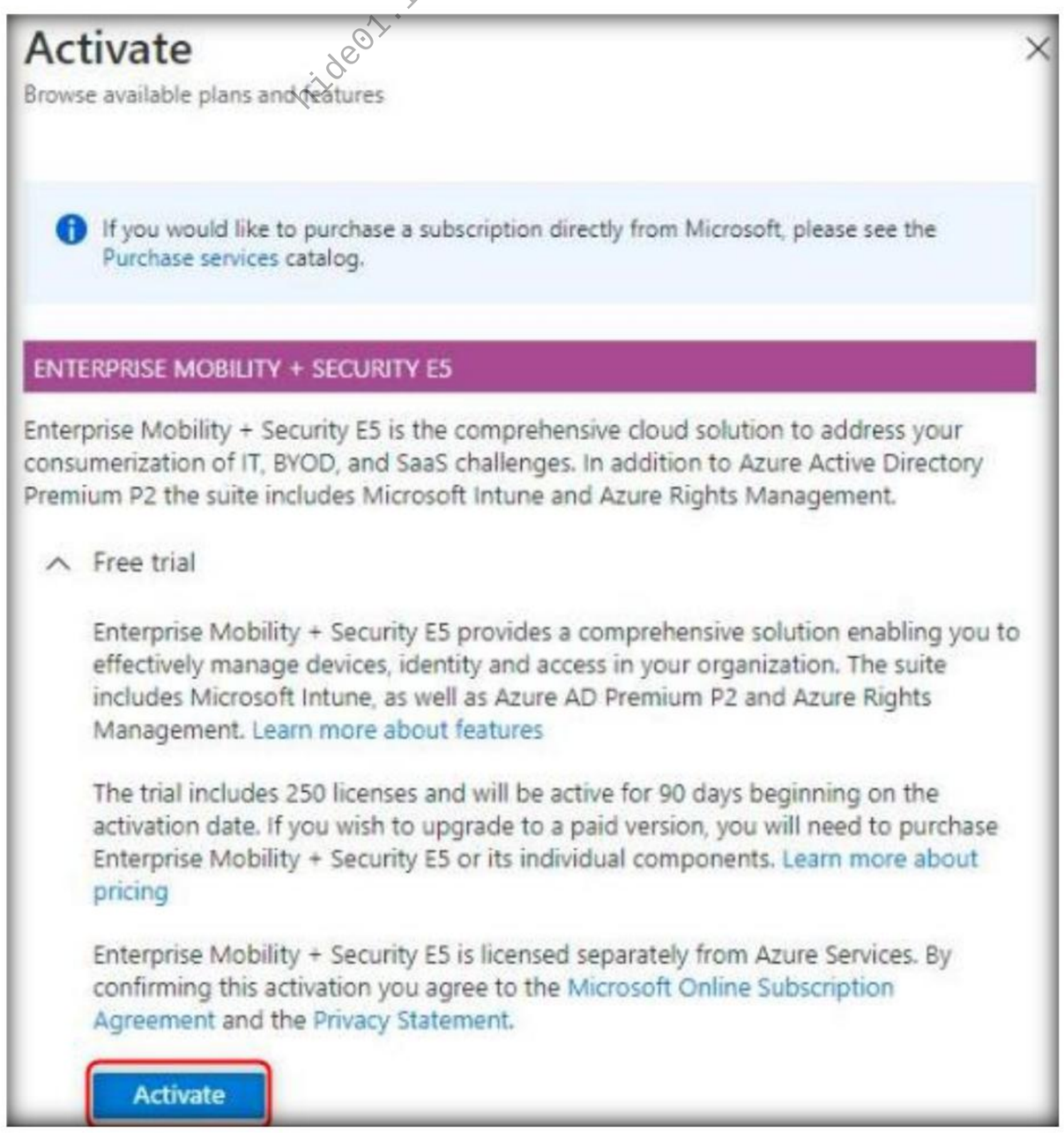
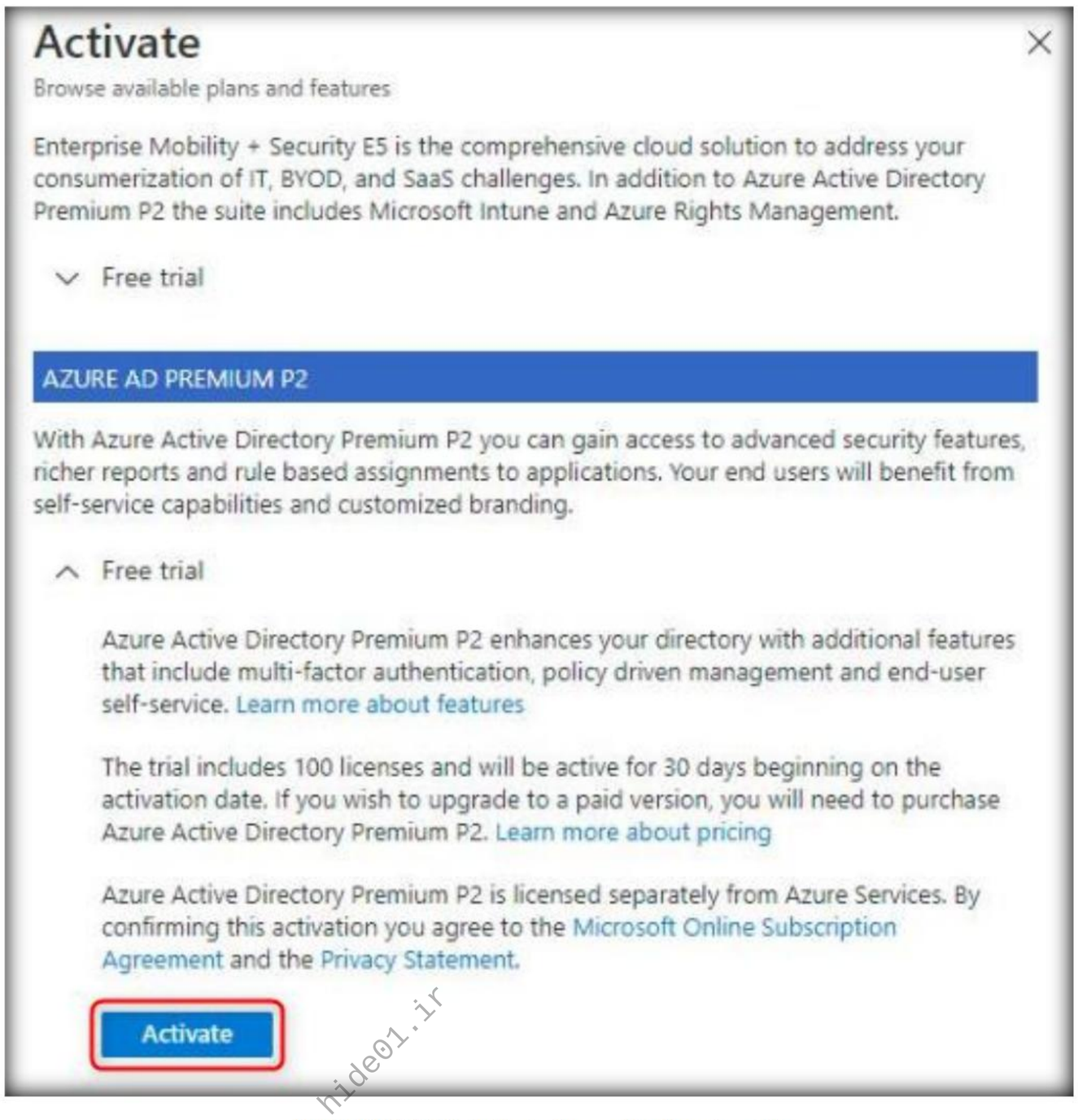


FIGURE 3.3.21: Activate Enterprise mobility+ security ES.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

22. Again click on the **Activate** button.



hide01.ir

FIGURE 3.3.22: Activate Azure AD Premium P2

23. Refresh the MFA page, and navigate and click on **Block/unblock users** under **Settings**.

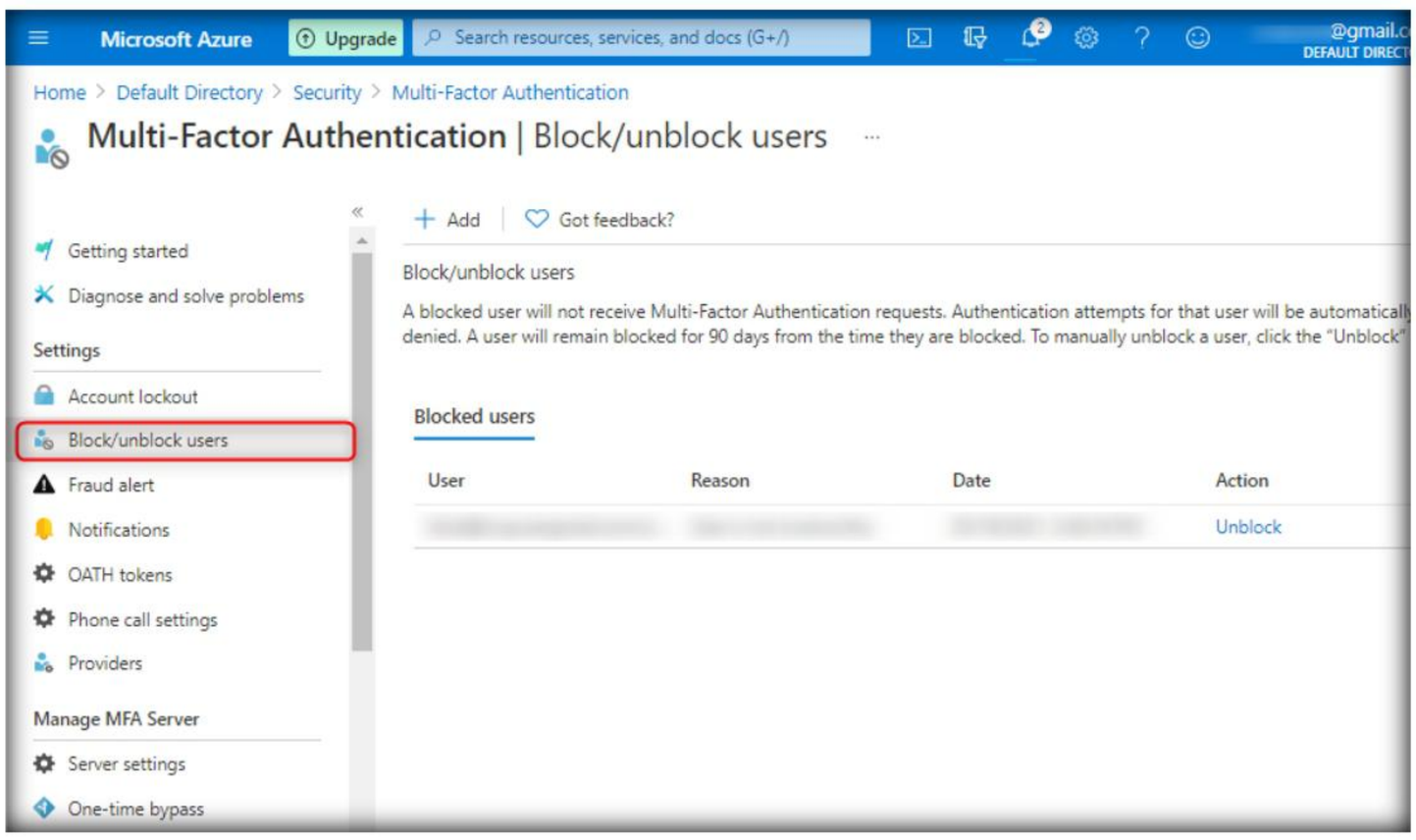


FIGURE 3.3.23: Selecting Block/unblock users option in Multi-Factor Authentication Window

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

24. Click on **+Add.** A **Block a user** window will appear on the left pane.

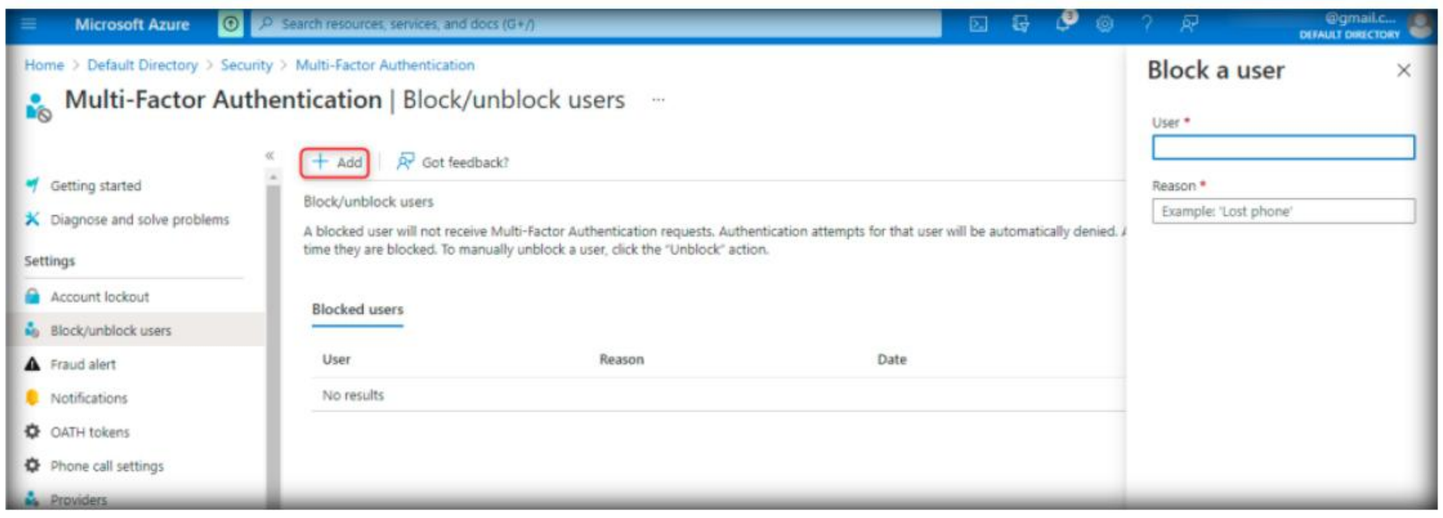


FIGURE 3.3.24: Blocking a User

25. In the **user** field, select the name of the user you wish to block. In this lab, we are blocking the user **bob@****.onmicrosoft.com.** In the **Reason** field, enter a reason of your choice (here, we have entered **Lost Laptop**).

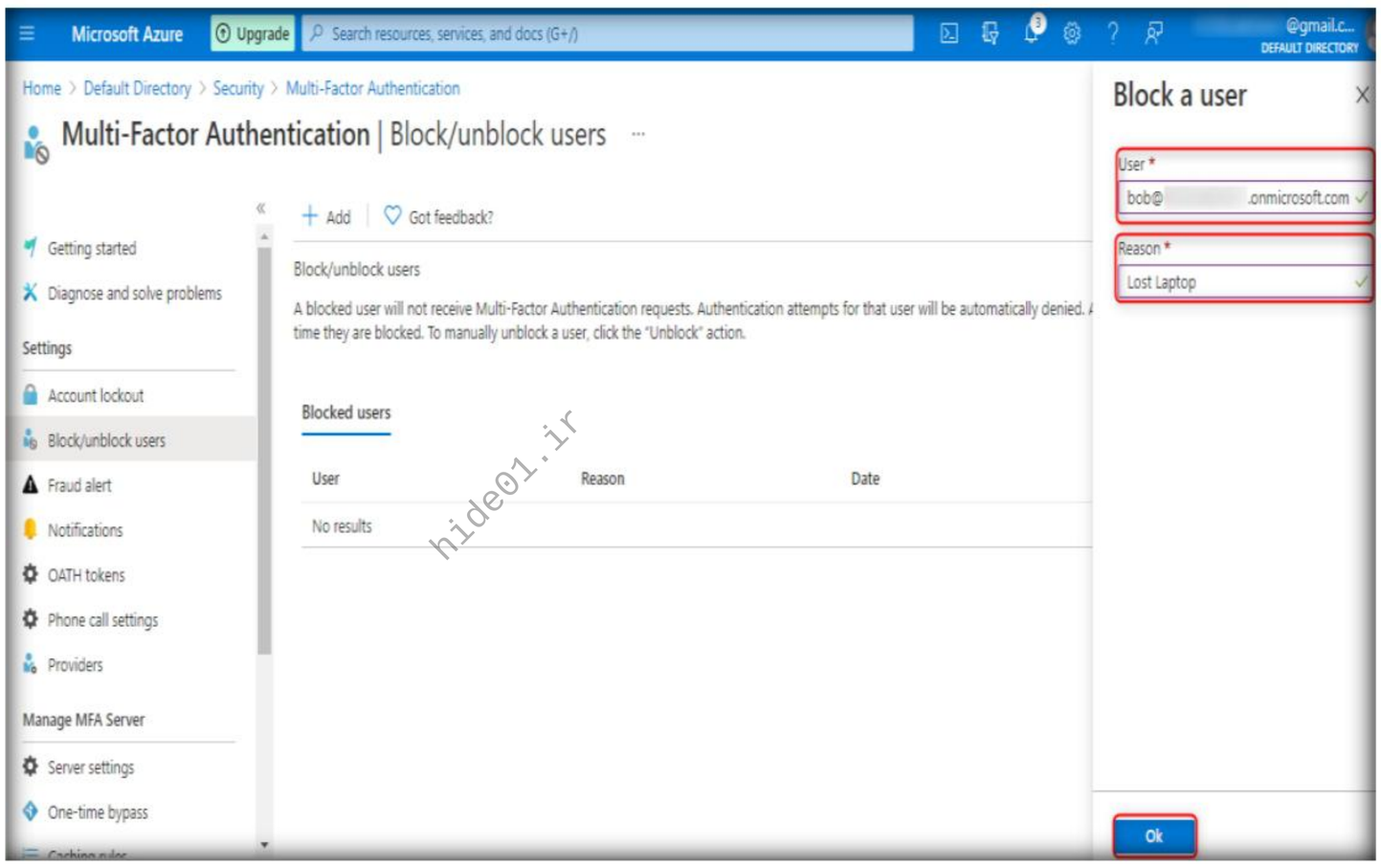


FIGURE 3.3.25: Entering the User Azure Login ID and Reason for Blocking

26. The user will be successfully blocked.

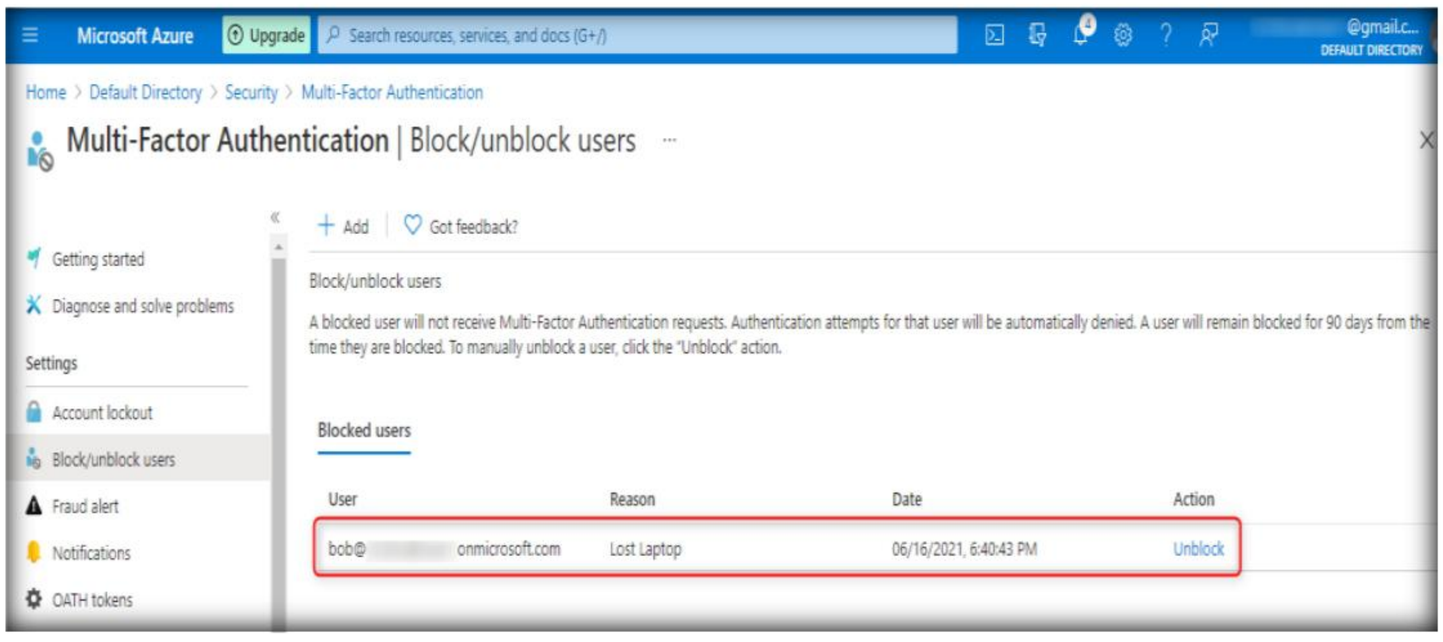


FIGURE 3.3.26: Successfully Blocking the User

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

27. To unblock the blocked user, click on **Unblock** under **Action**.

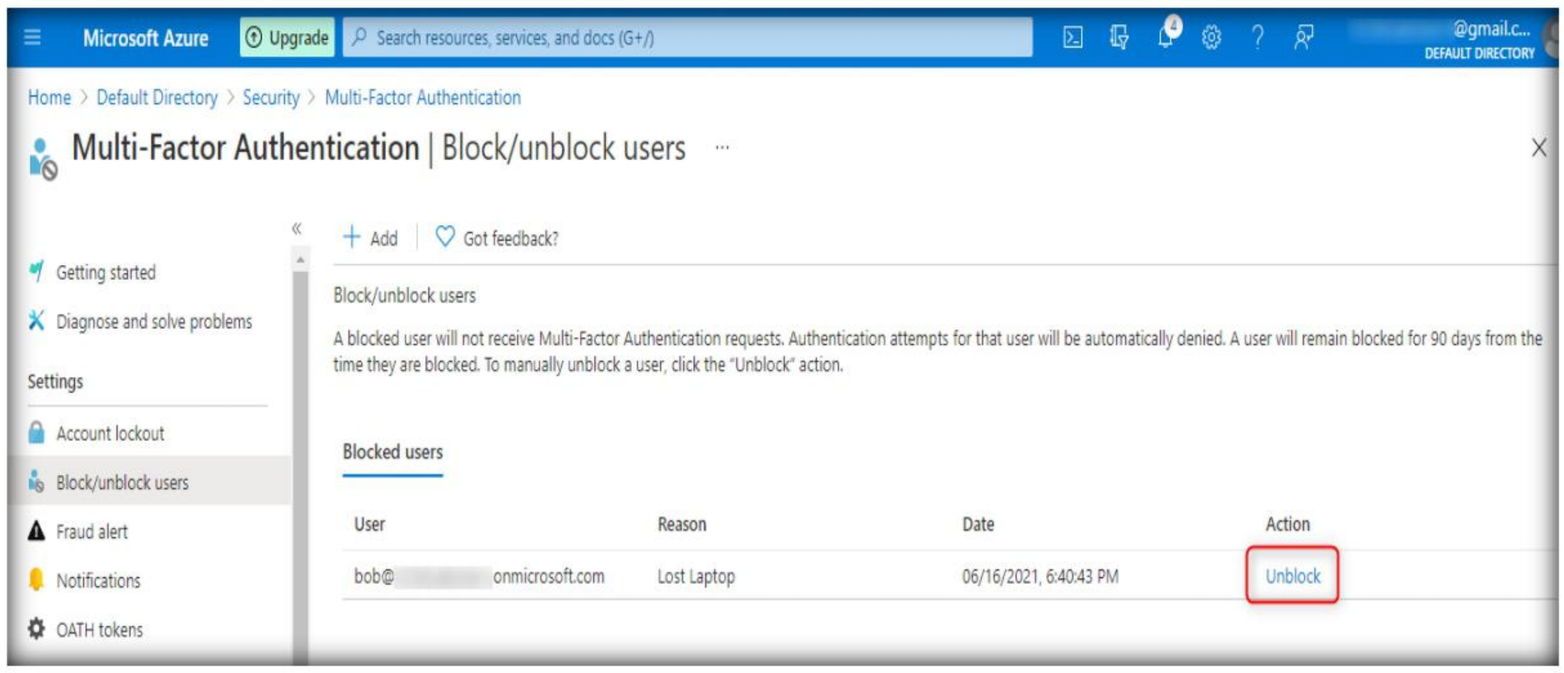


FIGURE 3.3.27: Successfully Blocking the User

28. A **Unblock a user** window will appear. Enter the **Reason for unblocking** (here, we have entered **Trusted User**). Then, click on **OK**.

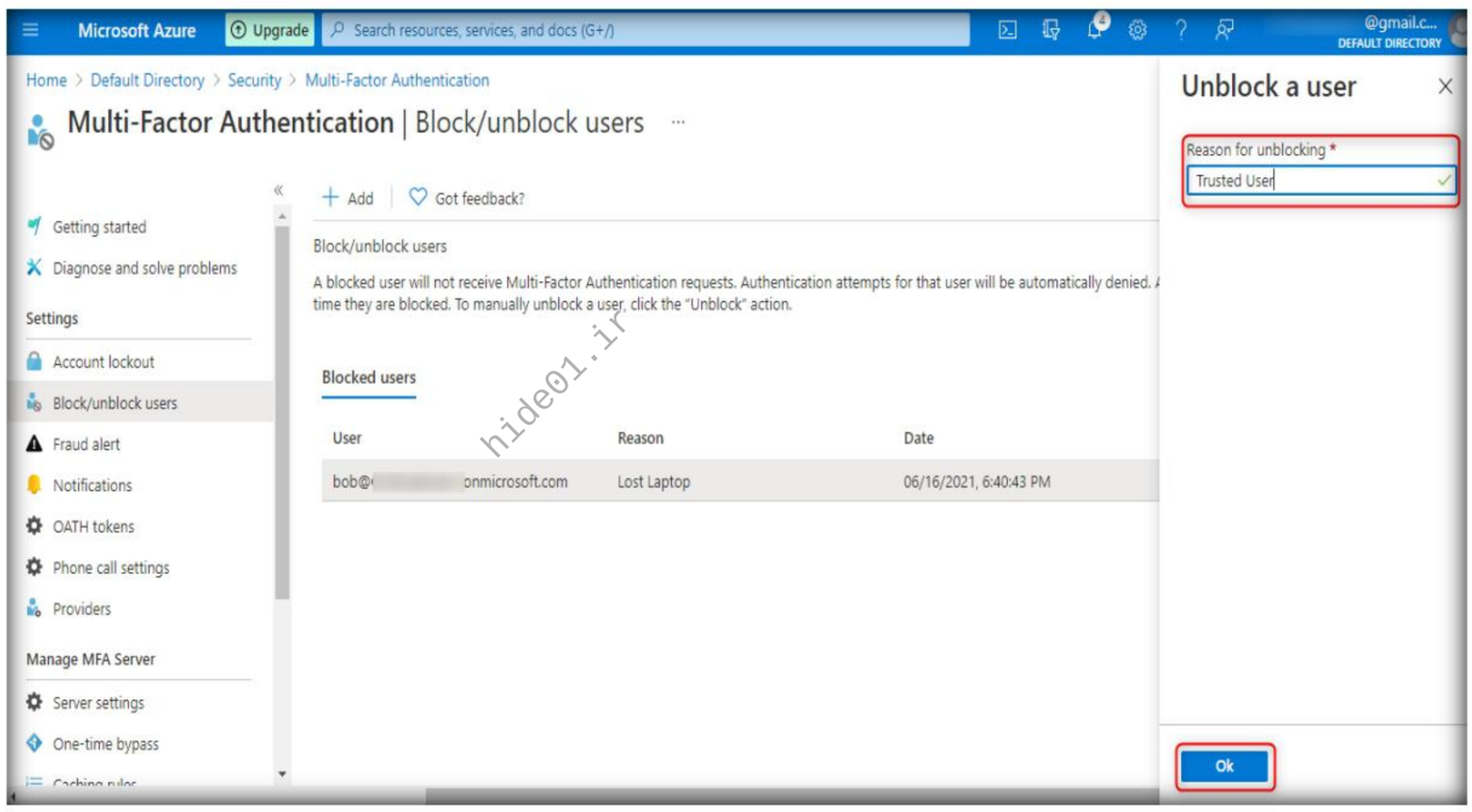


FIGURE 3.3.28: Unblocking the User

29. The user will be successfully **unblocked** and removed from the blocked user list.

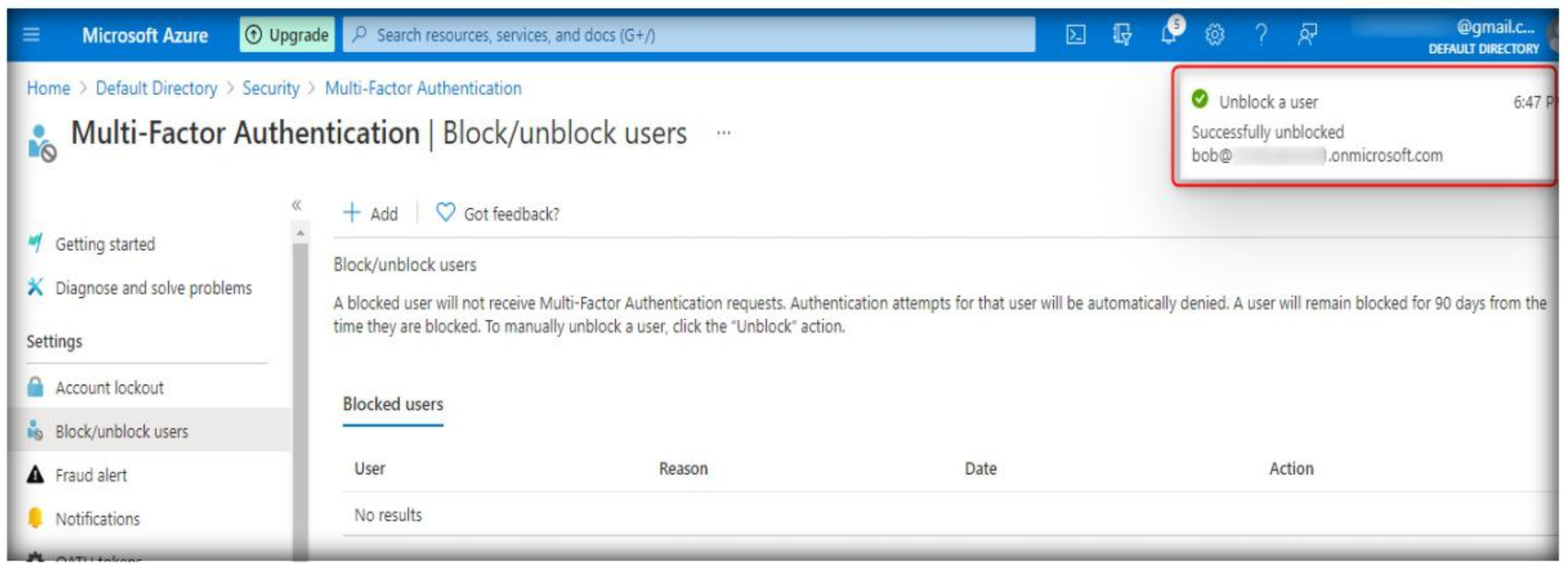


FIGURE 3.3.29: User Successfully Unblocked

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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

30. In the Azure portal, navigate and click on **Azure Active Directory**. Click on **Users** under **Manage** on the left pane. Click on the user's name (**Bob Watson**) to view the user profile window. Click on **Delete** at the top.

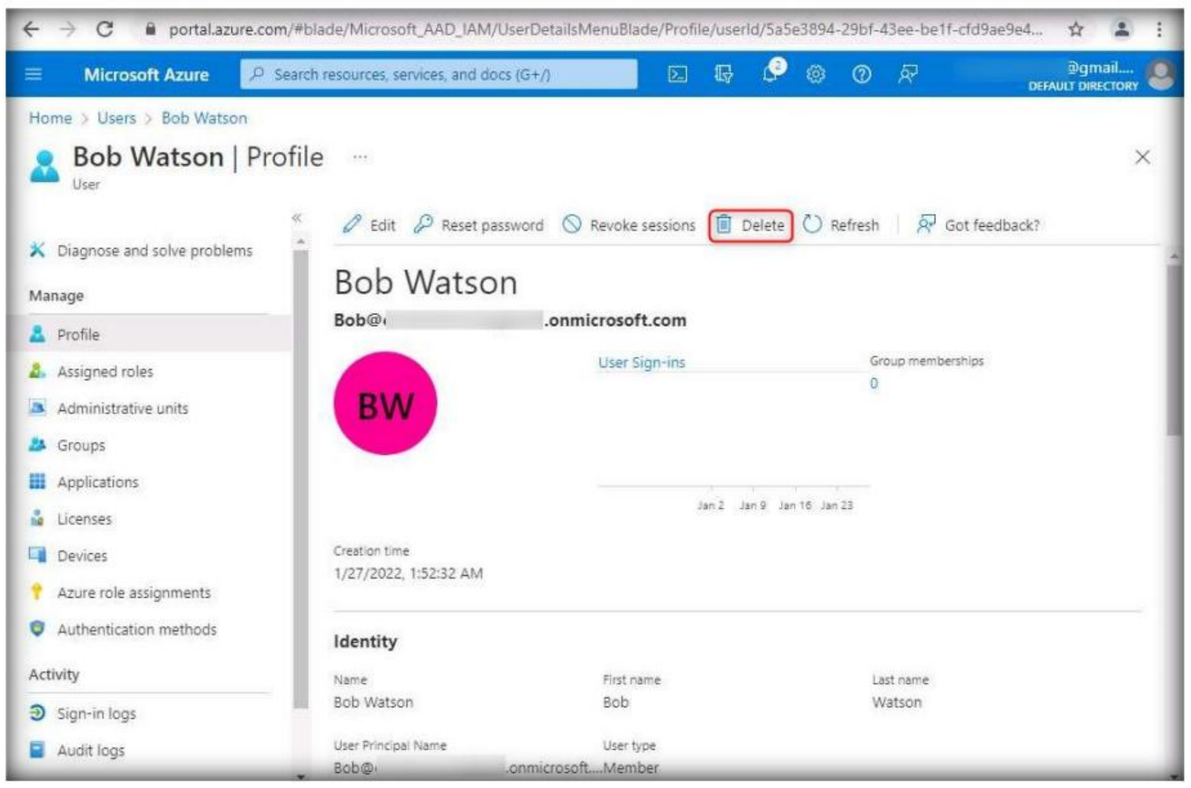


FIGURE 3.3.30: Deleting User

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.

hidel.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab

4

Restricting Access to App Engine Applications in GCP with Cloud IAP

Google Cloud Identity Aware Proxy (IAP) allows the cloud security administrators to control access to applications and resources running on Google Cloud.

ICON KEY

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

Lab Scenario

Google Cloud IAP enforces access controls to applications and resources. IAP can be used for implementing an application-level access control. With IAP, a cloud security engineer can restrict access for users to an application by implementing a fine-grained access control without the need for a VPN.

hide01ir

Lab Objectives

This lab demonstrates how to restrict access to App Engine applications and verify a configuration.

In this lab, you will learn to do the following:

- Create a new project in Google Cloud Console
- Deploy an application to App Engine in Cloud Shell
- Restrict access by enabling Cloud IAP
- Access an application

Lab Environment

To perform this lab, you need the following:

- **Admin Machine** VM
- **Administrative** privileges
- Registered GCP account

Lab Duration

Time: 15 minutes

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Overview of Cloud IAP

Cloud IAP allows the cloud administrators to enforce a central access control to applications accessed by HTTPS. When an application is secured by IAP, authentication and authorization checks are performed when a user tries to access it. For IAP-enabled App Engine applications, information regarding a secured application is sent to the IAP authentication server, which includes the GCP project number, URL, and IAP credentials in the request headers or cookies. Then, IAP checks the browser credentials of the user; if none exists, the users are redirected to the OAuth 2.0 Google account sign-in flow, which stores a browser cookie. If the request credentials turn out to be valid, they will be used by the authentication server to get the identity of the user (email address and user ID). The user's IAM role is verified by the authentication server using this identity along with whether the user has been granted access to the resource.

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., GCP), the application interface may be updated with time. Hence, in case you happen to work on an updated version of GCP, 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 GCP account using the following link: **https://console.cloud.google.com**. Once the registration is complete, perform the following tasks.

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

TASK 1

Creating a New Project in Google Cloud Console

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

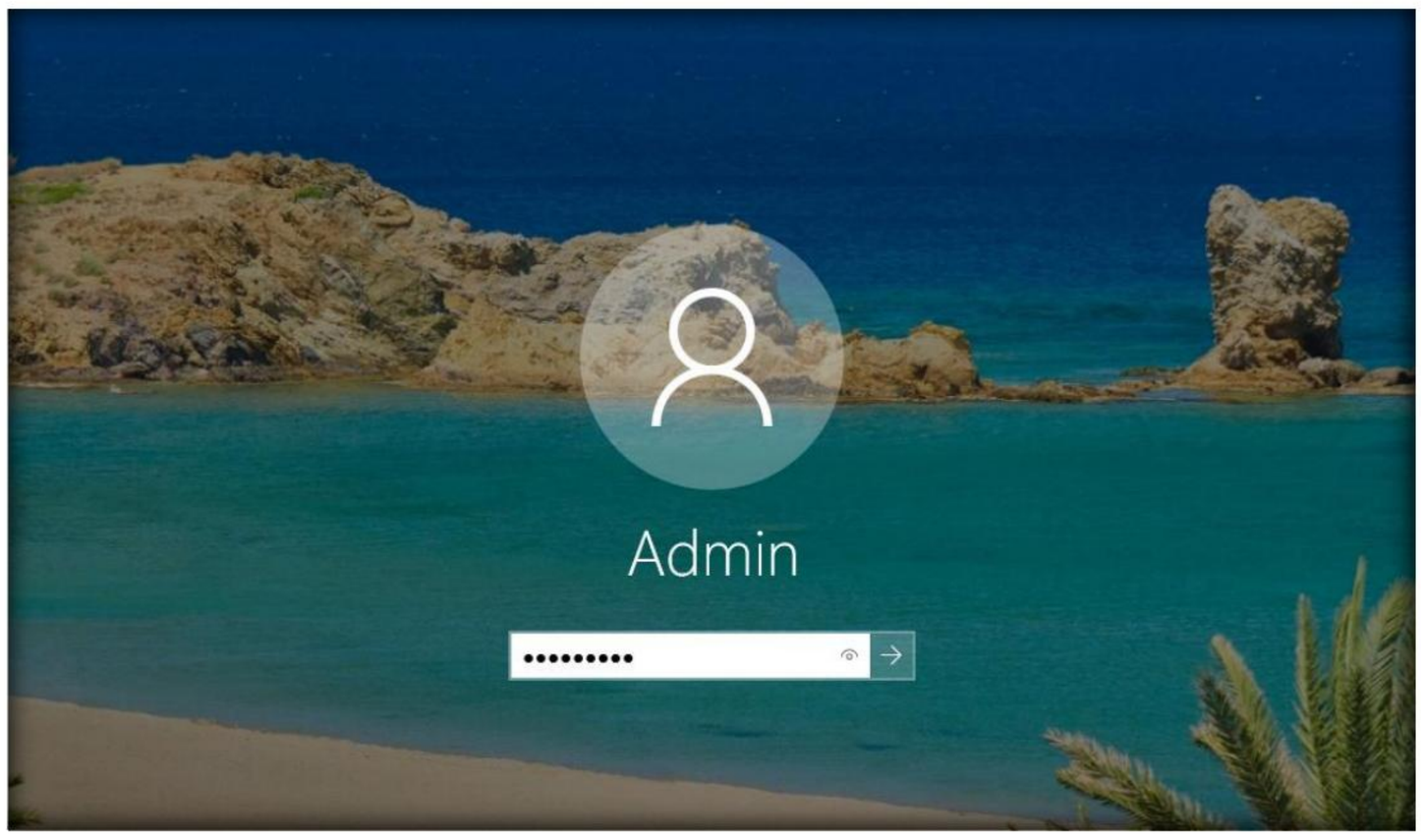


FIGURE 3.4.1: Launch Admin Machine and Log in

Certified Cloud Security Engineer Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

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

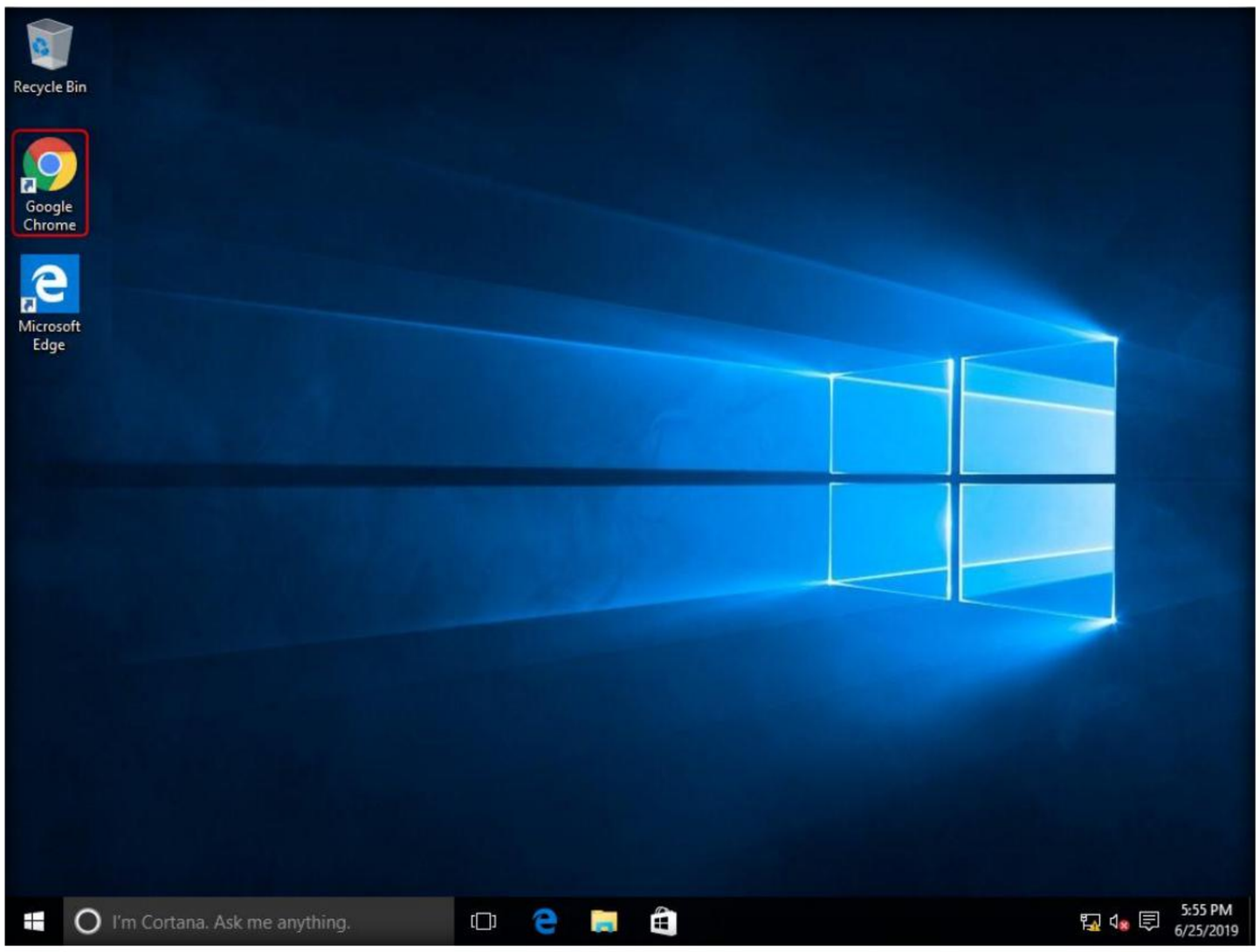


FIGURE 3.4.2: Navigating to the Chrome Browser from Taskbar

hide01.ir

3. Go to the address bar, type **https://console.cloud.google.com/**, and press **Enter**.
4. In the Sign in page, enter the **Email or phone** and click **Next** to login into **Google Cloud Platform**.

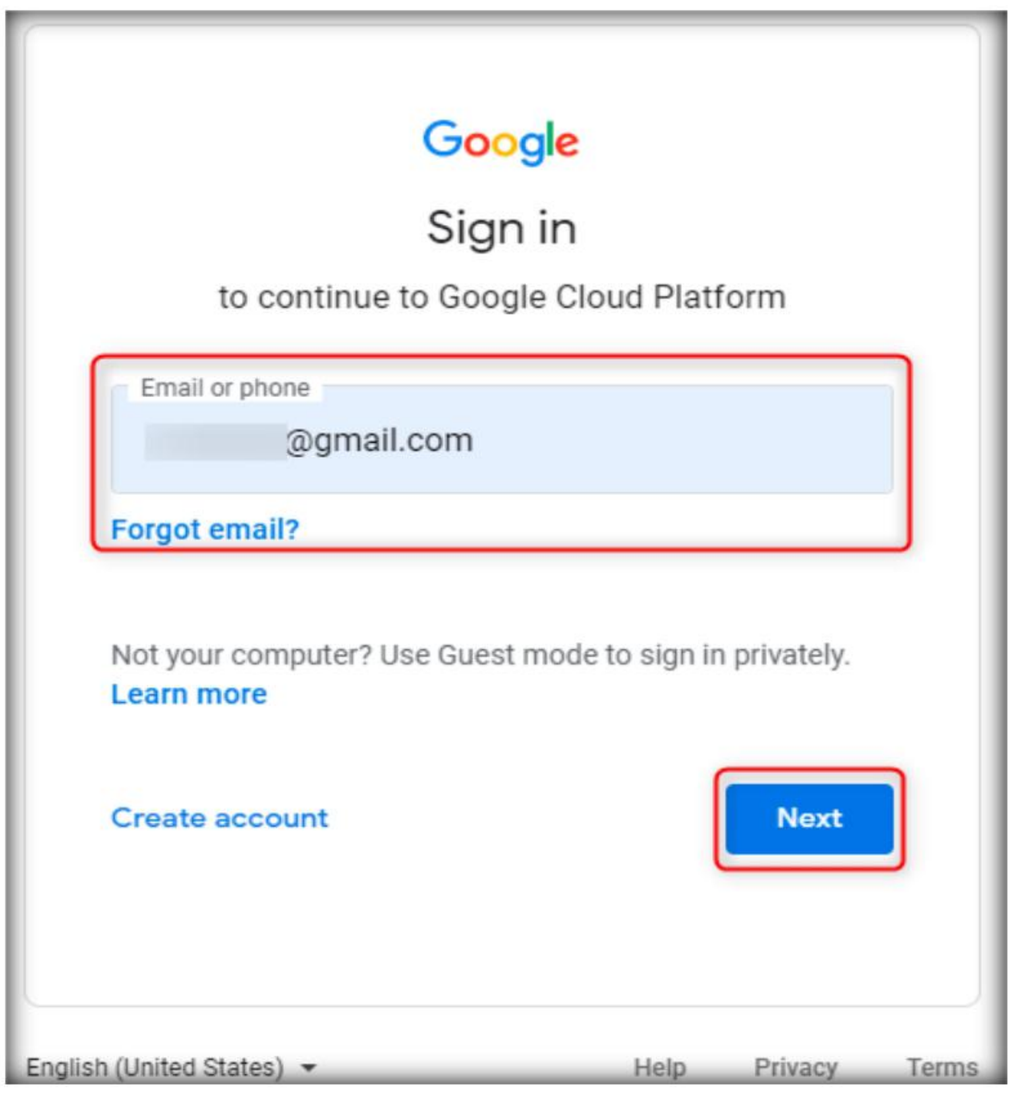
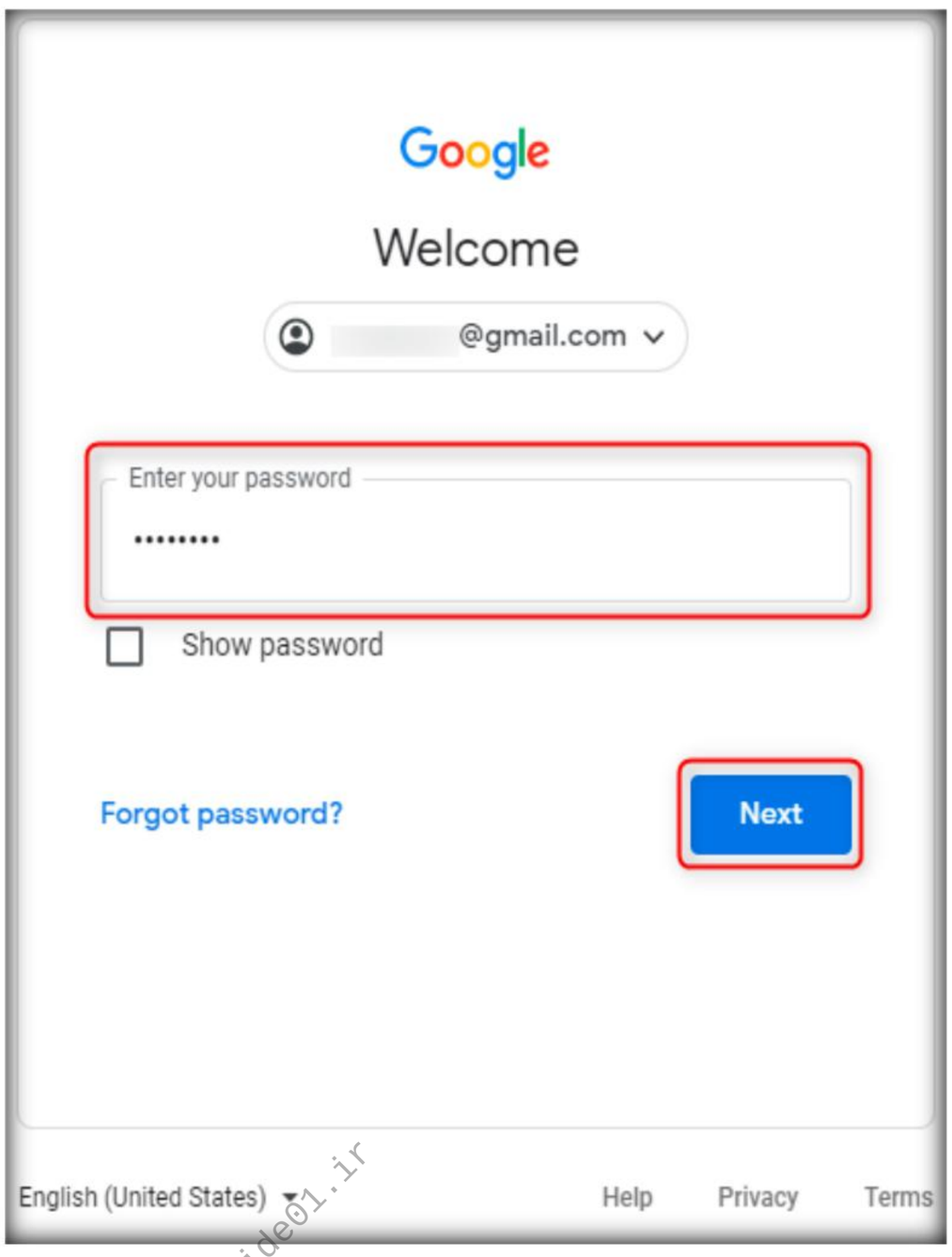


FIGURE 3.4.3: Access GCP in Browser

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

5. Enter the **password** and click on **Next**.



hide01.ir

FIGURE 3.4.4: Signing in into GCP console

6. On top left corner, you will have a dropdown. If **My First Project** is the default selected project, then skip **Steps 7–16** and go to **Step 17**.

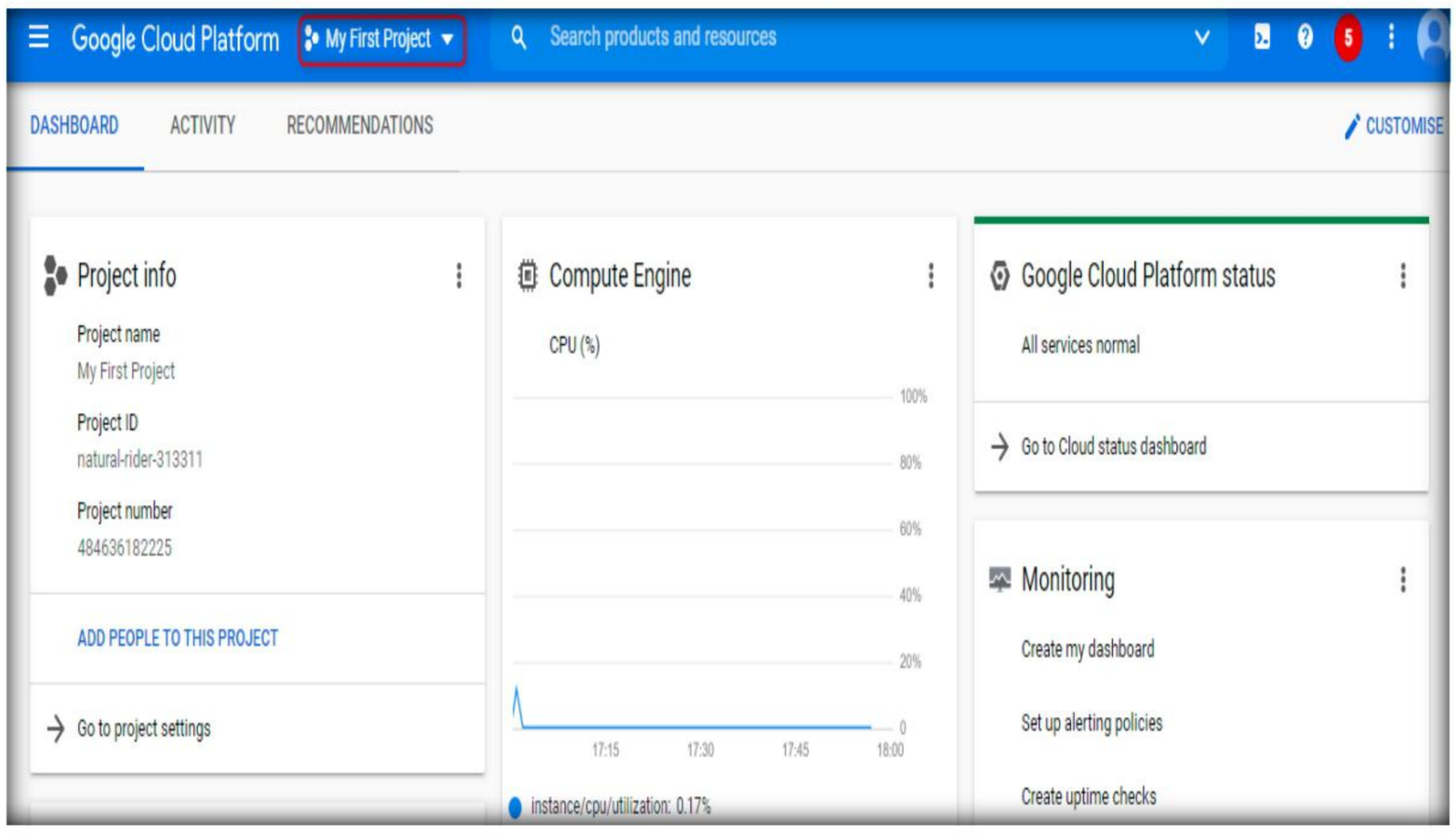


FIGURE 3.4.5: Create new Project

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

7. On the top left corner, in the dropdown, if you see **Select a Project** with an empty dashboard, then click on **CREATE PROJECT** in the empty dashboard to create a new project.

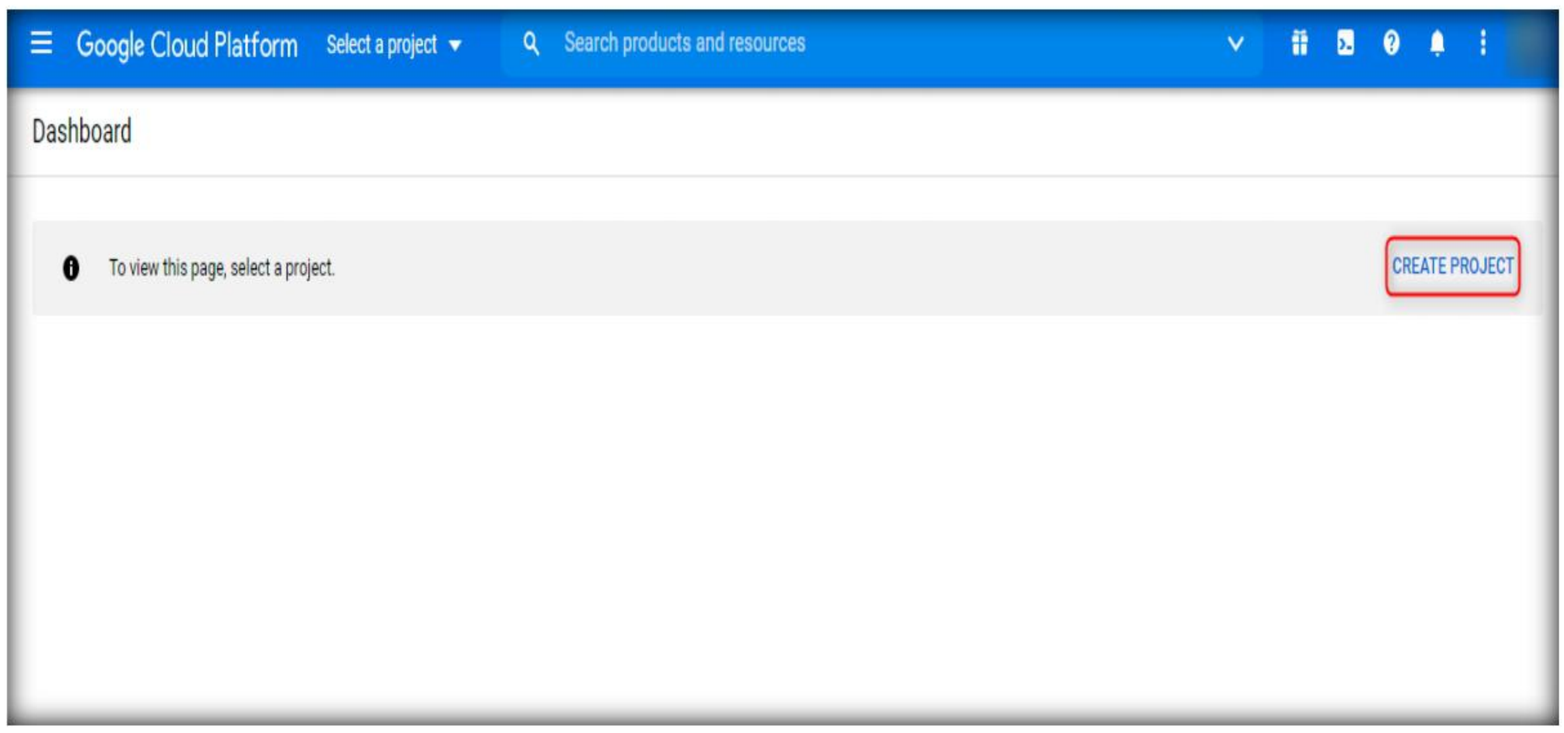


FIGURE 3.4.6: Creating Project

8. In the **New Project** window that opens, type the **Project name** as **My First Project**. Then, click on **CREATE**.

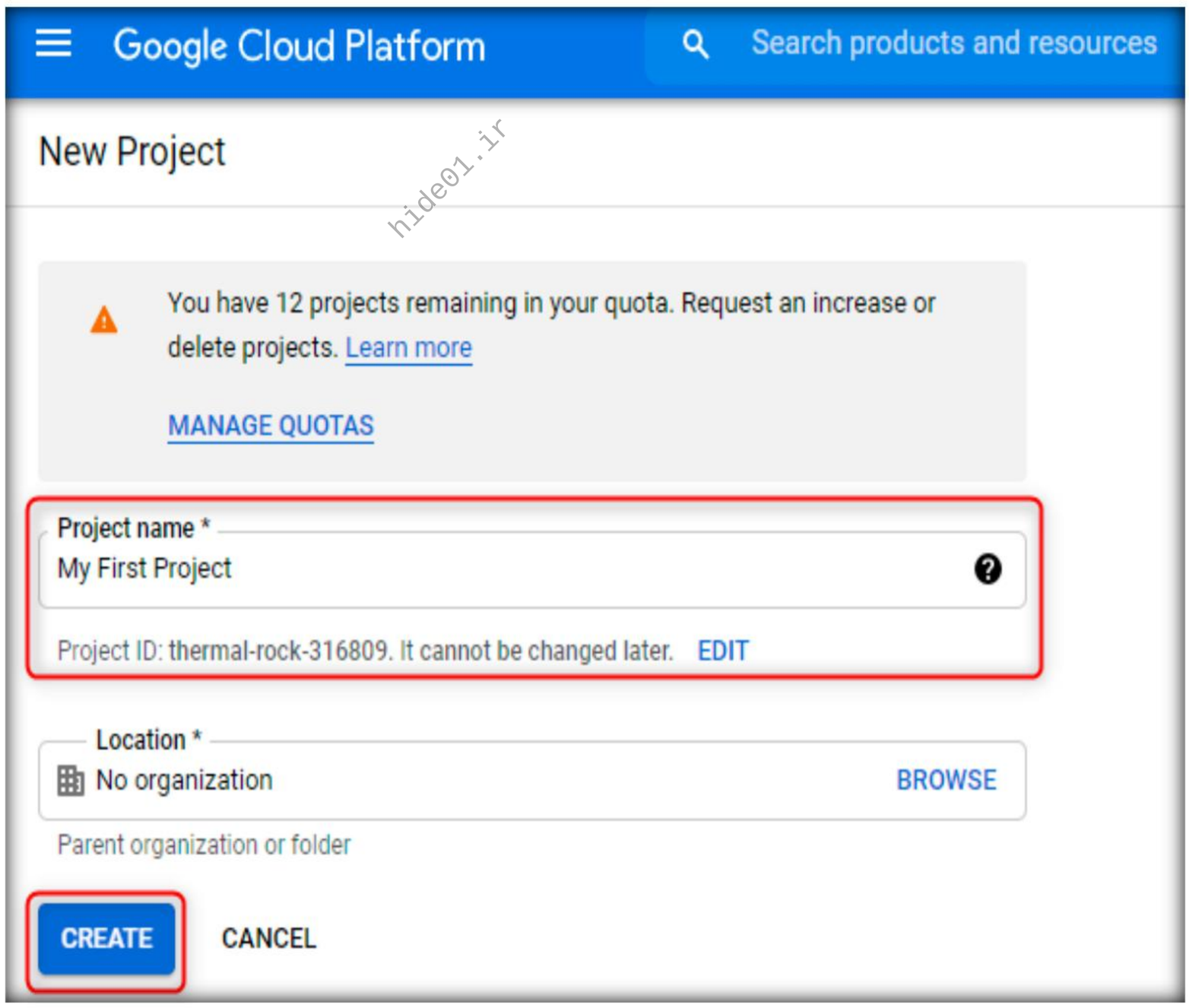


FIGURE 3.4.7: Configuring New Project

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

9. Your project will be successfully created. You can see the new project at the top of the window, **My New Project** is selected by default as the current project.

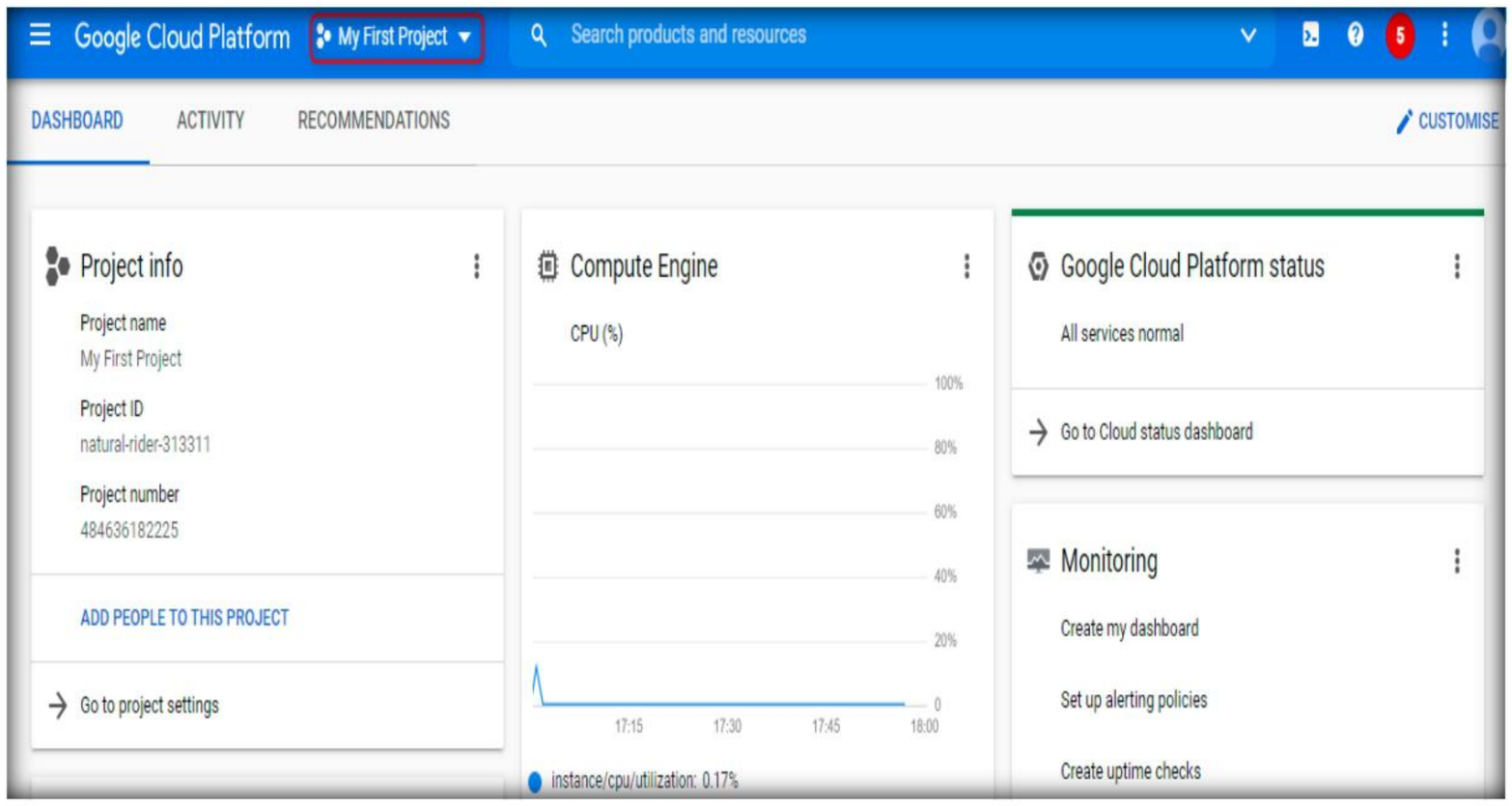


FIGURE 3.4.8: My First Project Selected as Default

10. On the top left corner, if the dropdown displays a different project other than **My First Project** by default, click on the dropdown.

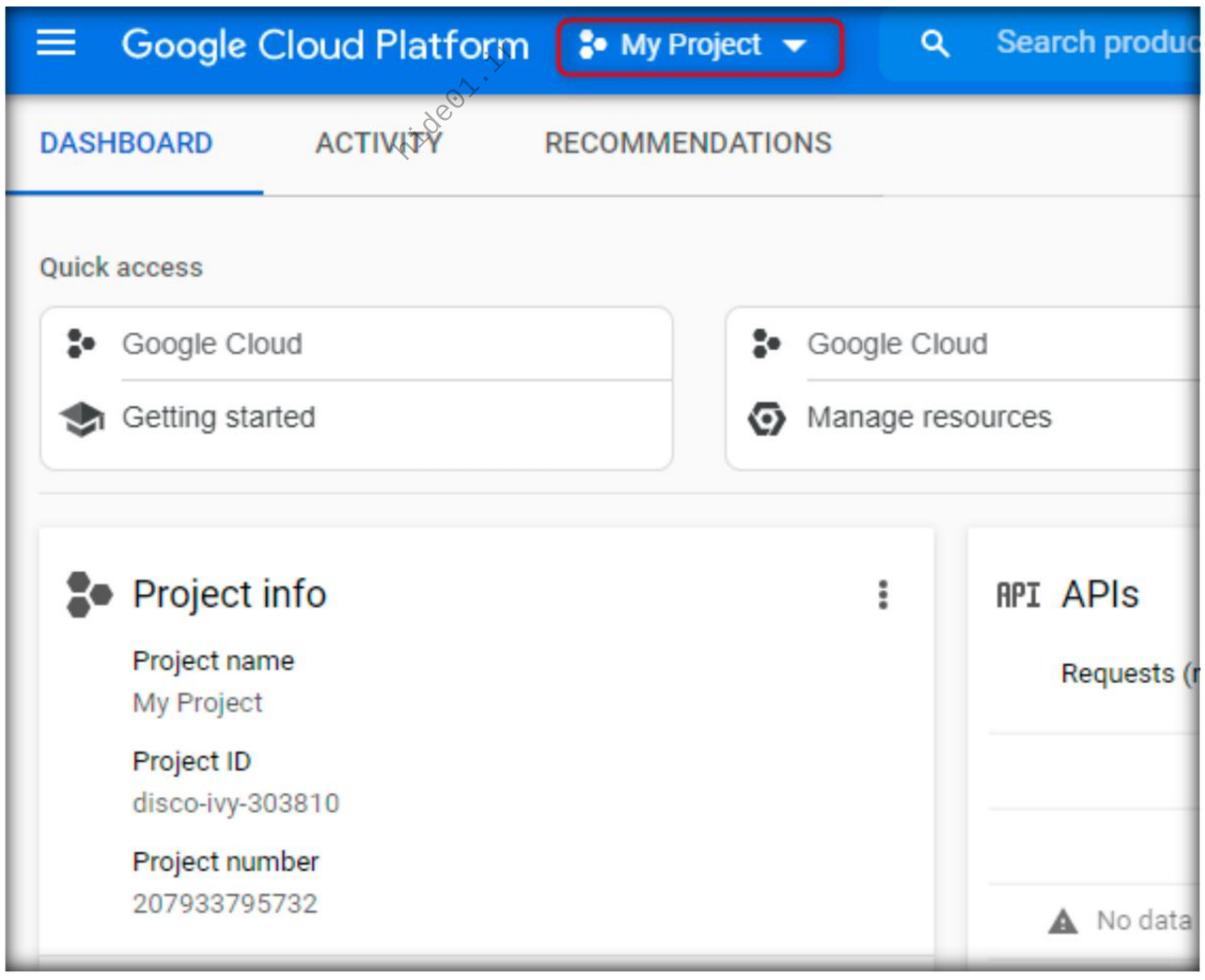


FIGURE 3.4.9: Selecting Project Dropdown

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

11. A **Select a project** window opens, which displays all existing projects. A **Search projects and folders** option is also provided to search for an existing project. Select **My First Project** from the displayed list of existing projects.

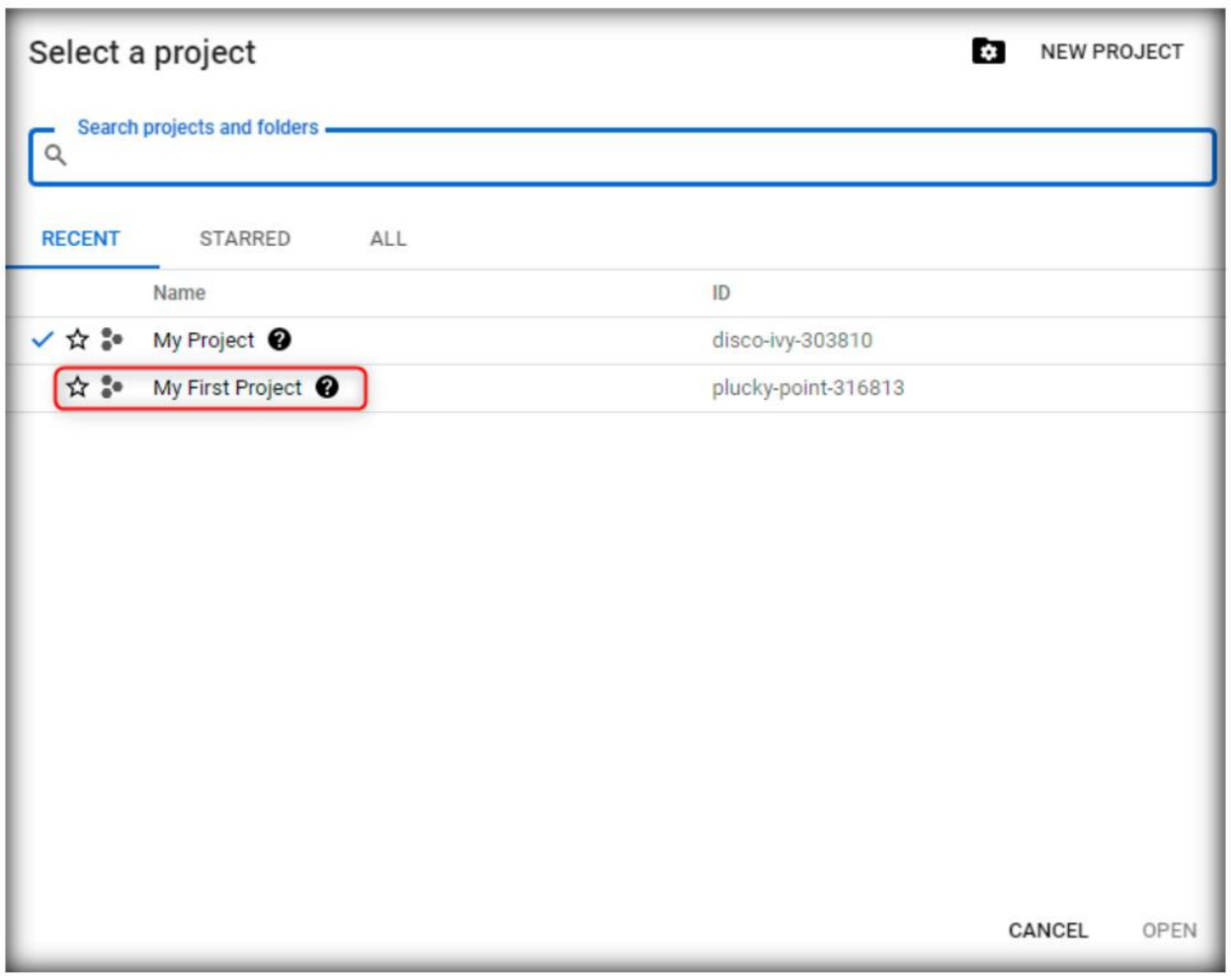


FIGURE 3.4.10: Selecting My First Project

12. Now, if **My New Project** is not in the list, click on the **NEW PROJECT** option to create a new project named **My First Project**.

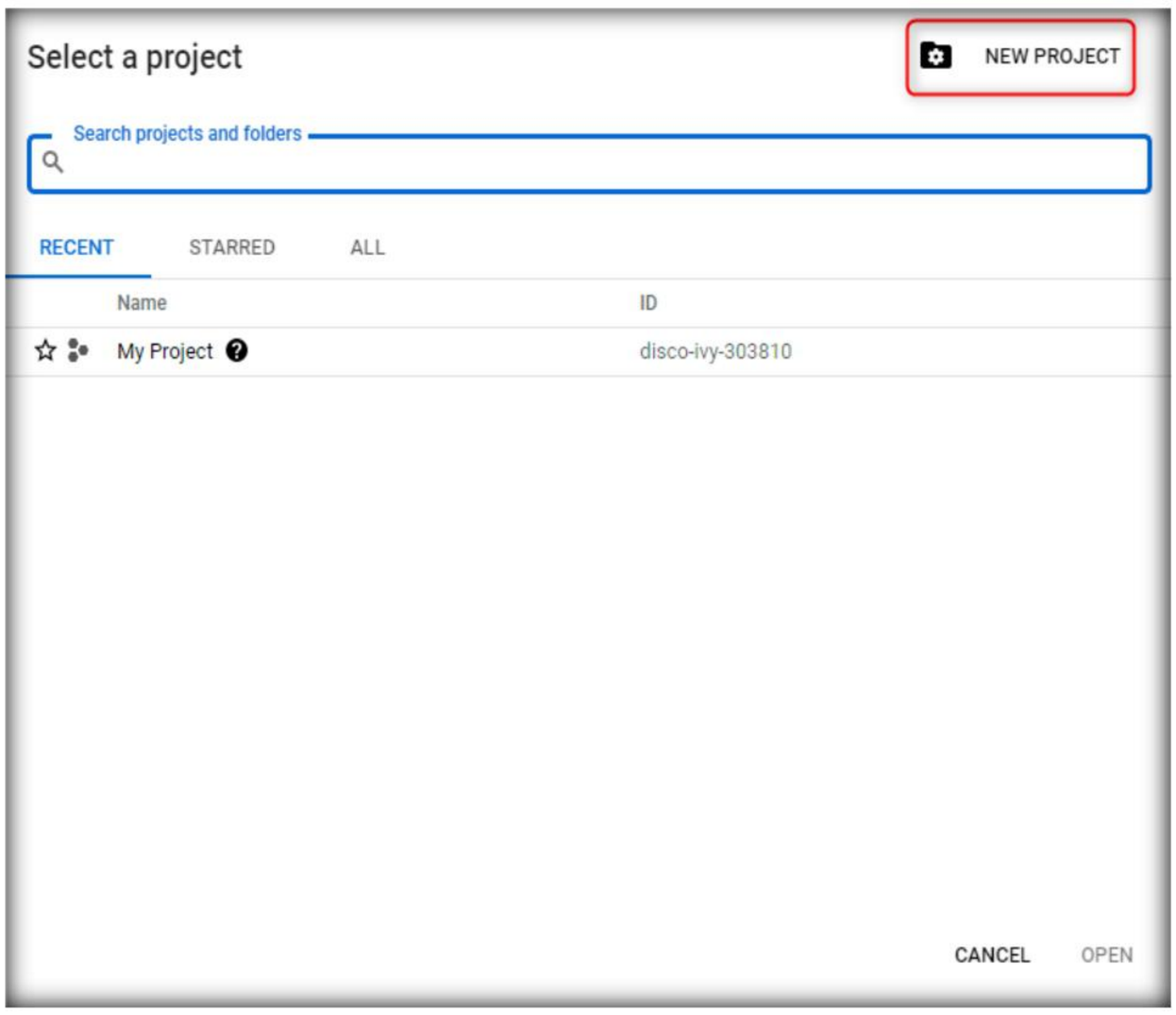


FIGURE 3.4.11: Creating New Project

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

13. The **New project** window opens. Type the **Name** of the project as **My First Project** and click on **CREATE**, as shown in the screenshot below.

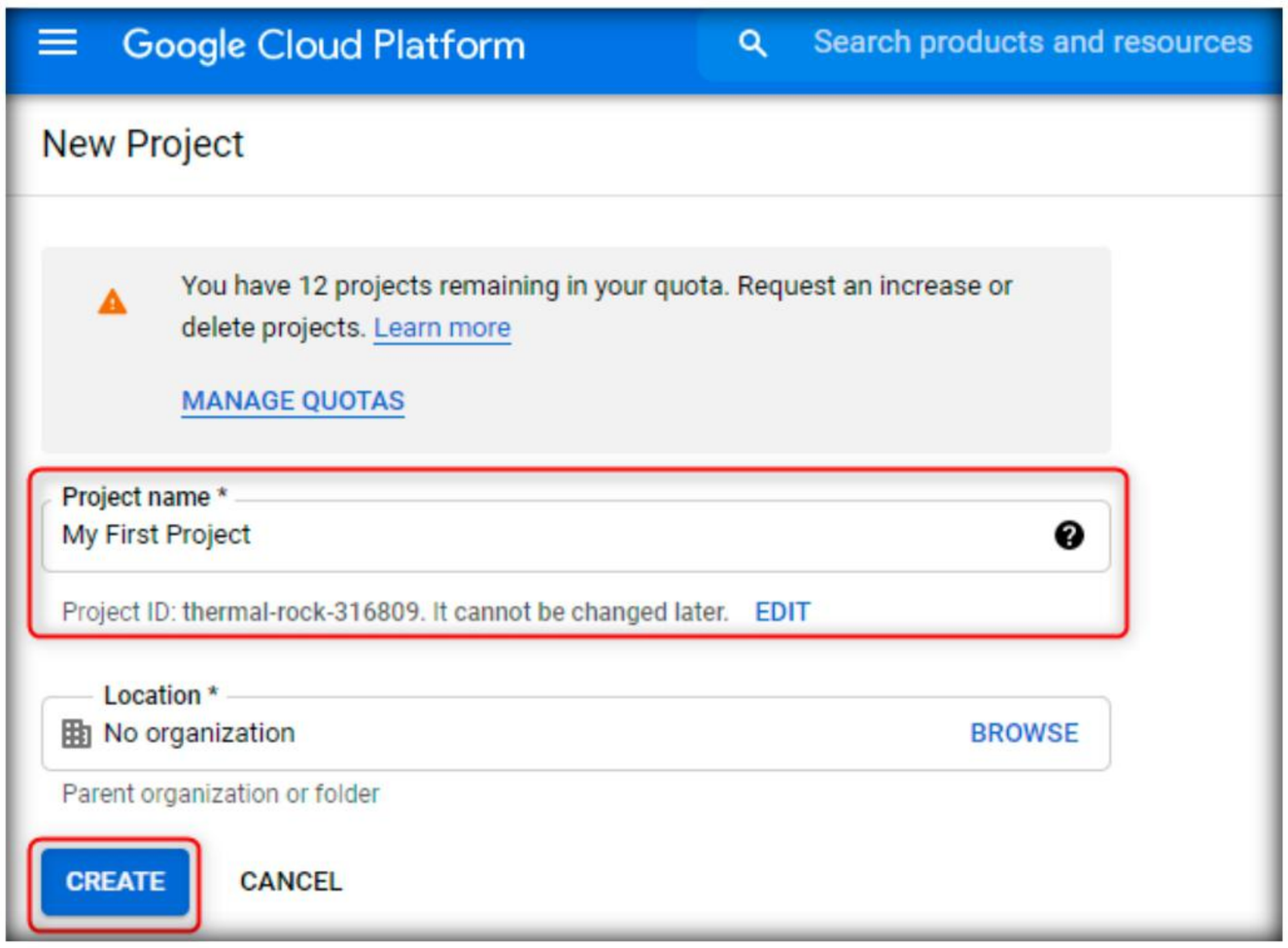


FIGURE 3.4.12: Creating My First Project

14. **My First Project** will be created. Next, you need to select **My First Project** as the default project. Now, click on the project dropdown at the top left corner.

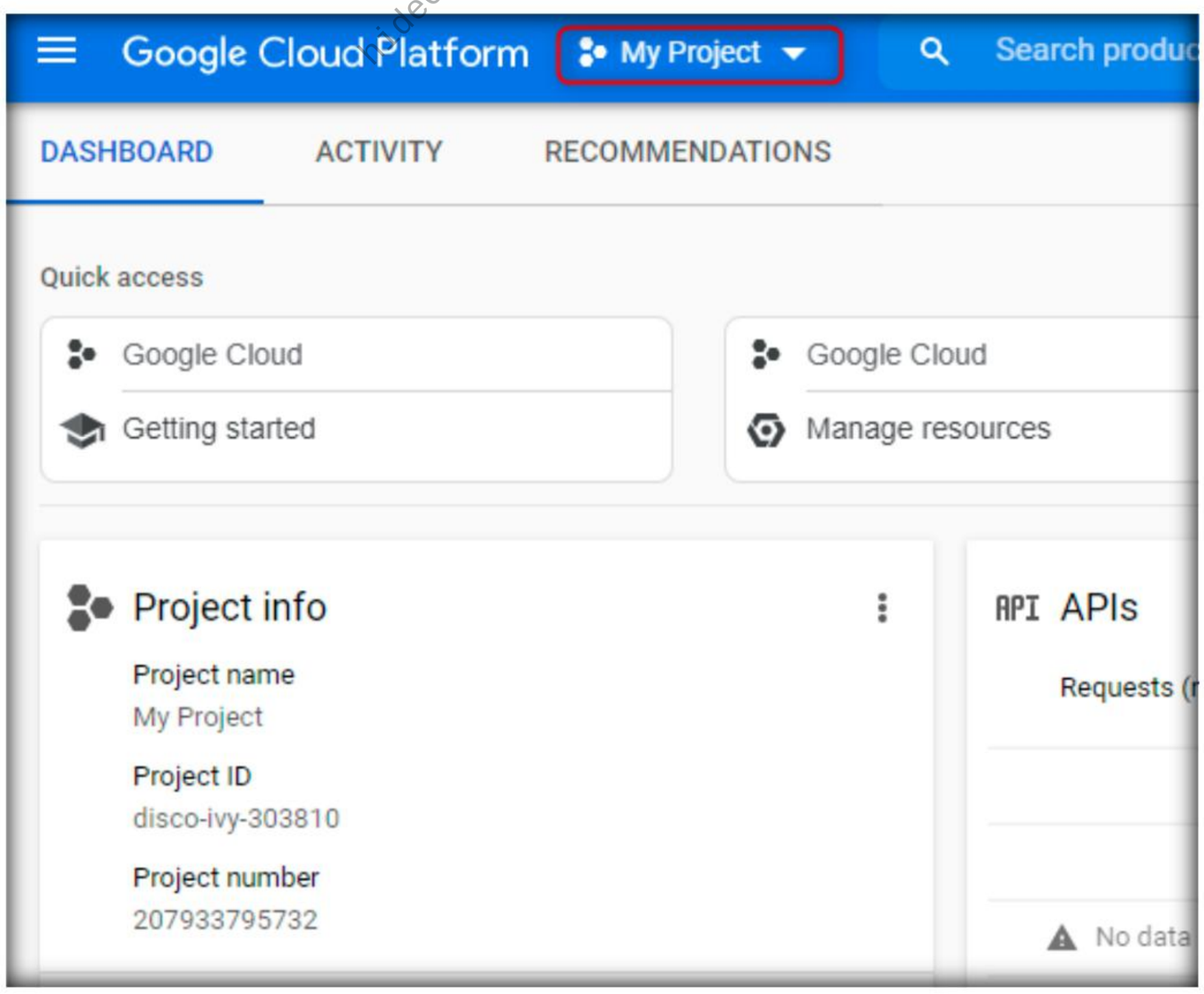


FIGURE 3.4.13: Selecting Project Dropdown

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

15. Select **My First Project** from the list of projects.
16. **My First Project** will be selected as the default project.

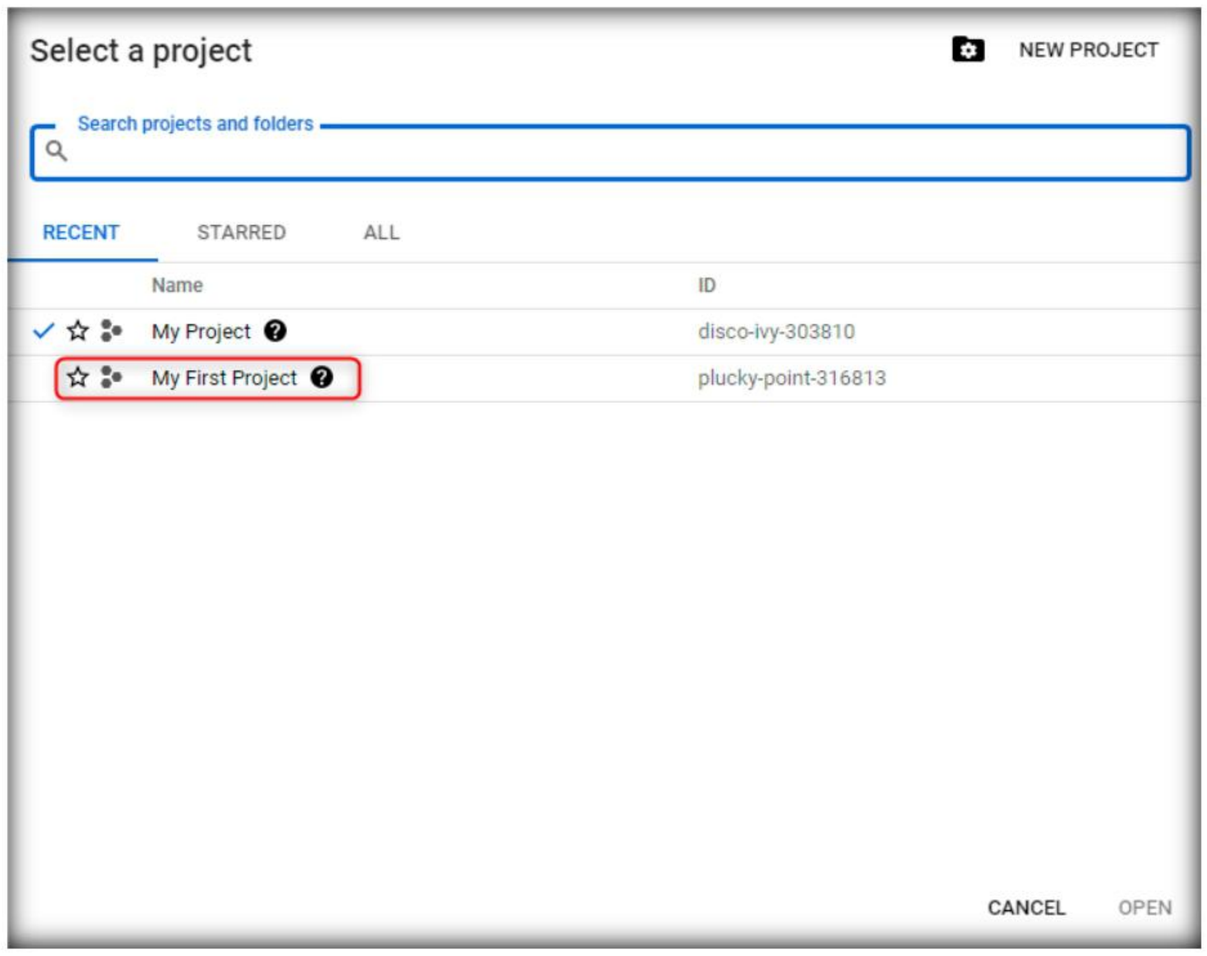


FIGURE 3.4.14: Selecting My First Project

TASK 2

Deploying an App Engine Application Using Cloud Shell

17. To deploy an App Engine application, open Cloud Shell. Click on the Cloud Shell icon at the top right corner of the console.

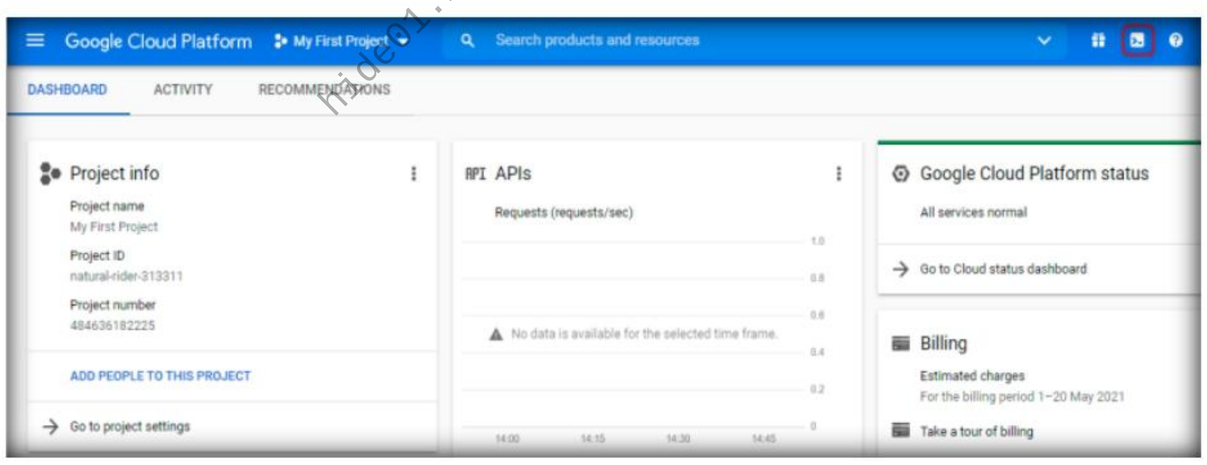


FIGURE 3.4.15: Opening Cloud Shell

18. Now, click on the icon at the top right corner of the Cloud Shell editor to open it in a new window.

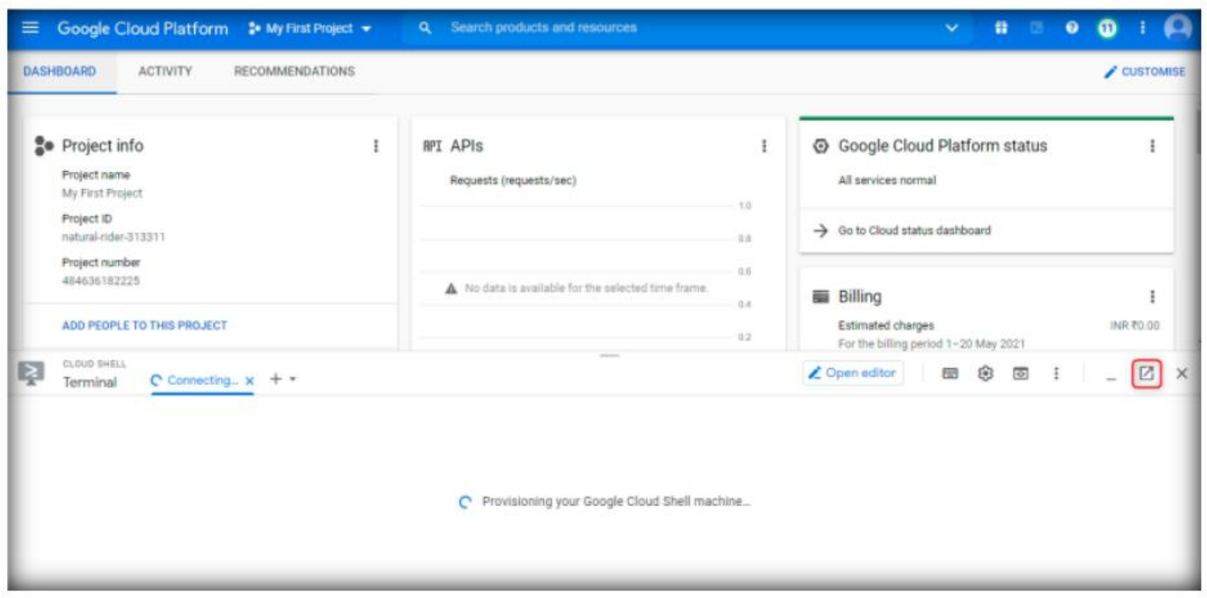


FIGURE 3.4.16: Expanding Cloud Shell Window

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

19. Now, to set **My First Project** in the current Cloud Shell session, we need to know the project id. Run the following command to list all projects and their respective **PROJECT_IDs**.

    `gcloud projects list`

    Note: If a window pops up for **Authorise Cloud Shell**, click on **Authorise**.

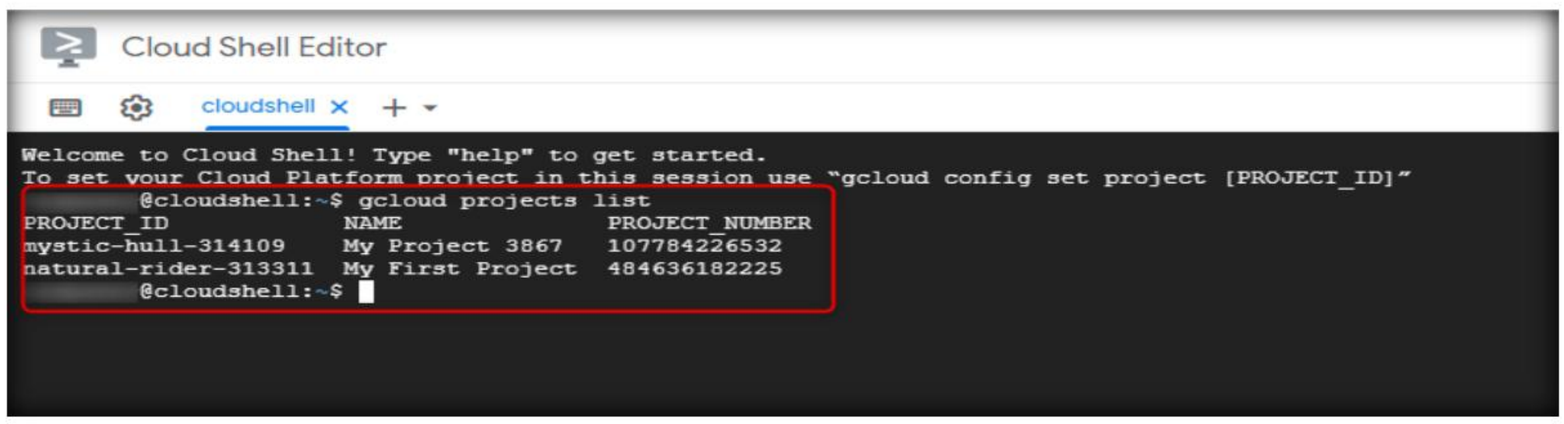


FIGURE 3.4.17: Listing the Projects

20. Now, to set **My First Project** in the current Cloud Shell session, type the following command and press **Enter**.

    `gcloud config set project [project_ID]` (replace `[project-ID]` with the project ID of **My First Project**)

    In this case, we have used the following command:

    `gcloud config set project natural-rider-313311`

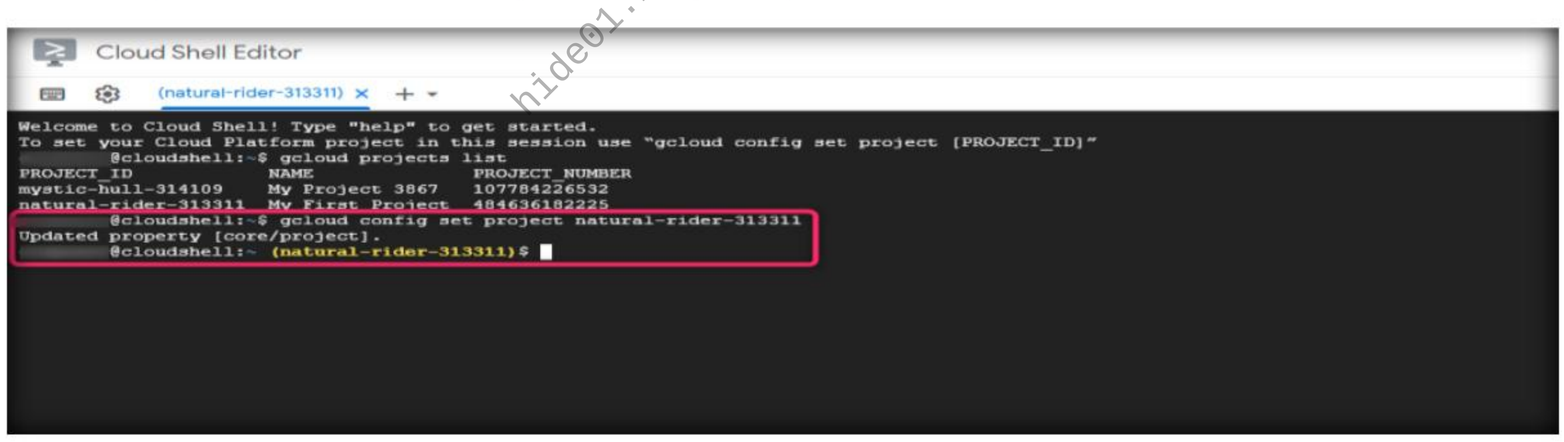


FIGURE 3.4.18: Setting GCP Project

21. Now, to download the sample application code from https://github.com/GoogleCloudPlatform/python-docs-samples.git to your local system, type the following command and press **Enter**.

    `git clone https://github.com/GoogleCloudPlatform/python-docs-samples.git`

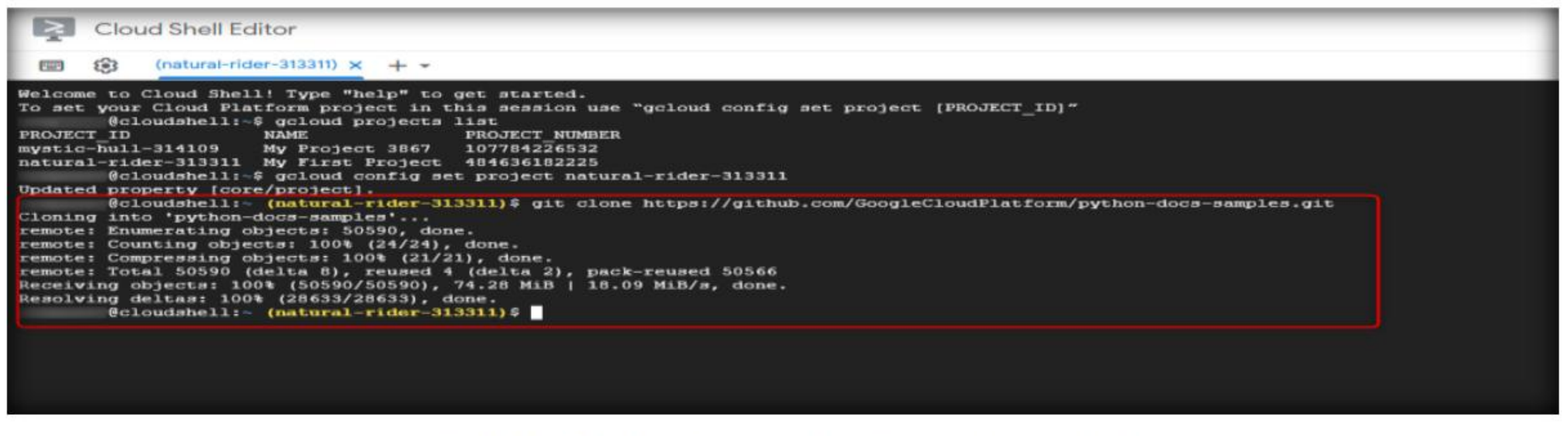


FIGURE 3.4.19: Fetching sample application from GitHub

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

22. After the application code is fetched from GitHub, type the following command and press **Enter** to navigate to the directory containing the sample application.

```
cd python-docs-
samples/appengine/standard/users/
```

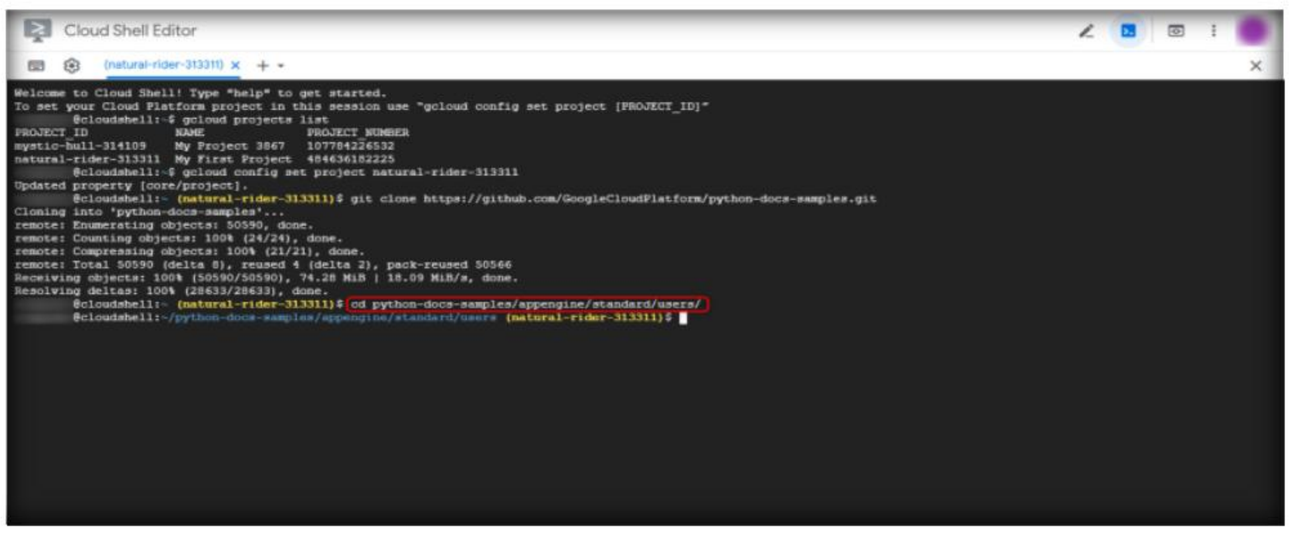


FIGURE 3.4.20: Changing Directory

23. Now, for deploying the sample application to App Engine standard environment, type the following command and press **Enter**.

```
gcloud app deploy
```

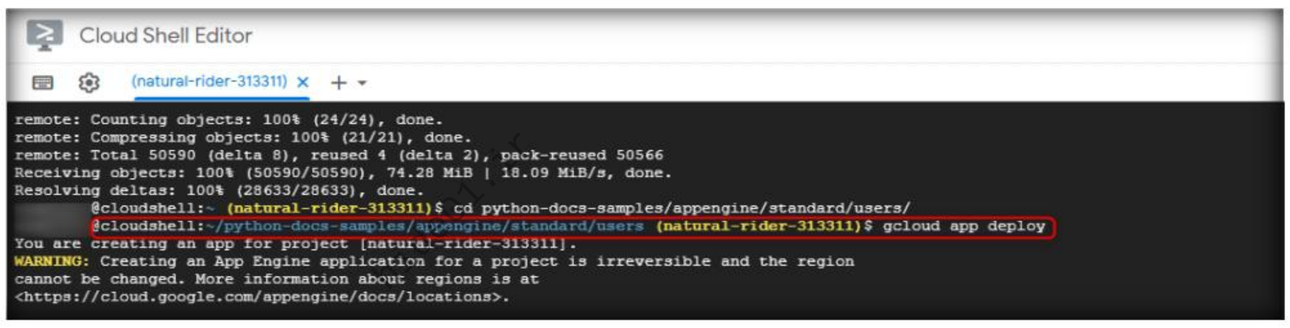


FIGURE 3.4.21: Deploying Application

24. Now, it will list the locations available for deploying the application under **Please choose the region where you want your App Engine application located:**. In **Please enter your numeric choice:**, give the appropriate location number and press **Enter**. In this lab, we have set the location to **us-east1** by typing 16.

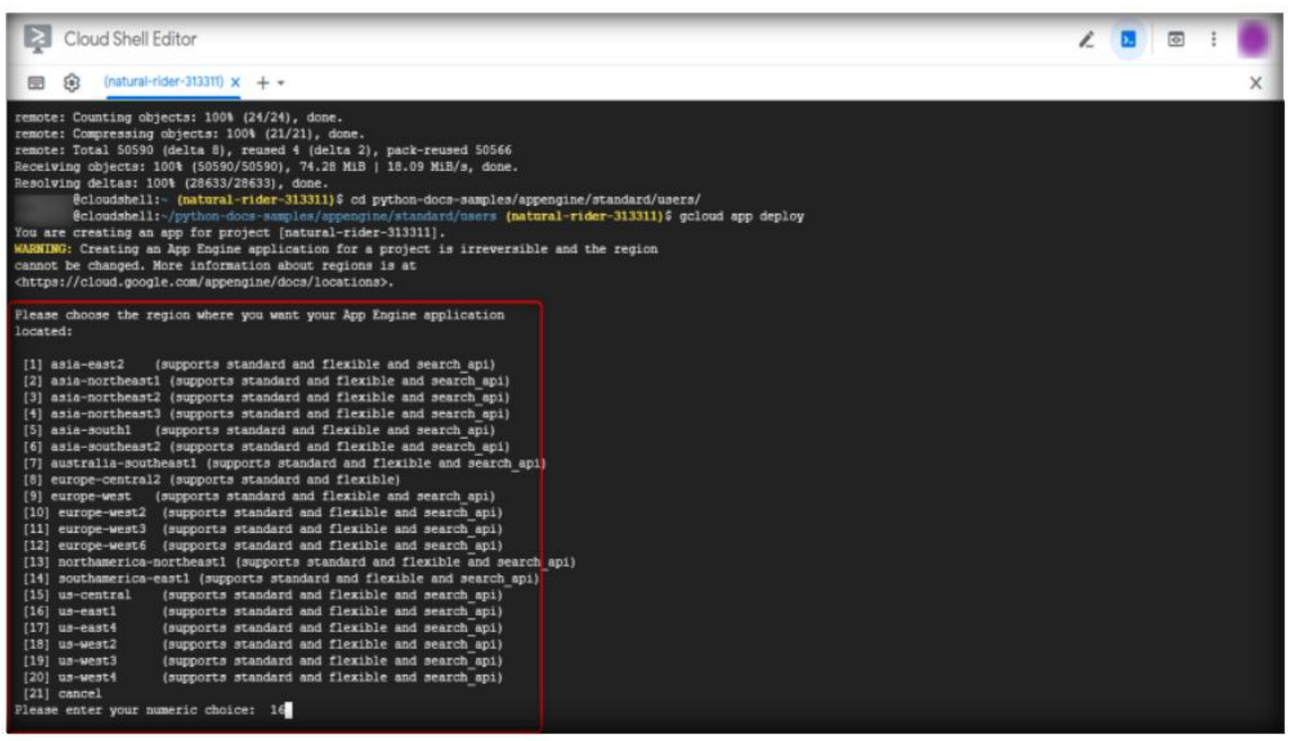


FIGURE 3.4.22: Choosing Location

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

25. For **Do you want to continue (Y/n)?**, type **Y** and press **Enter**.

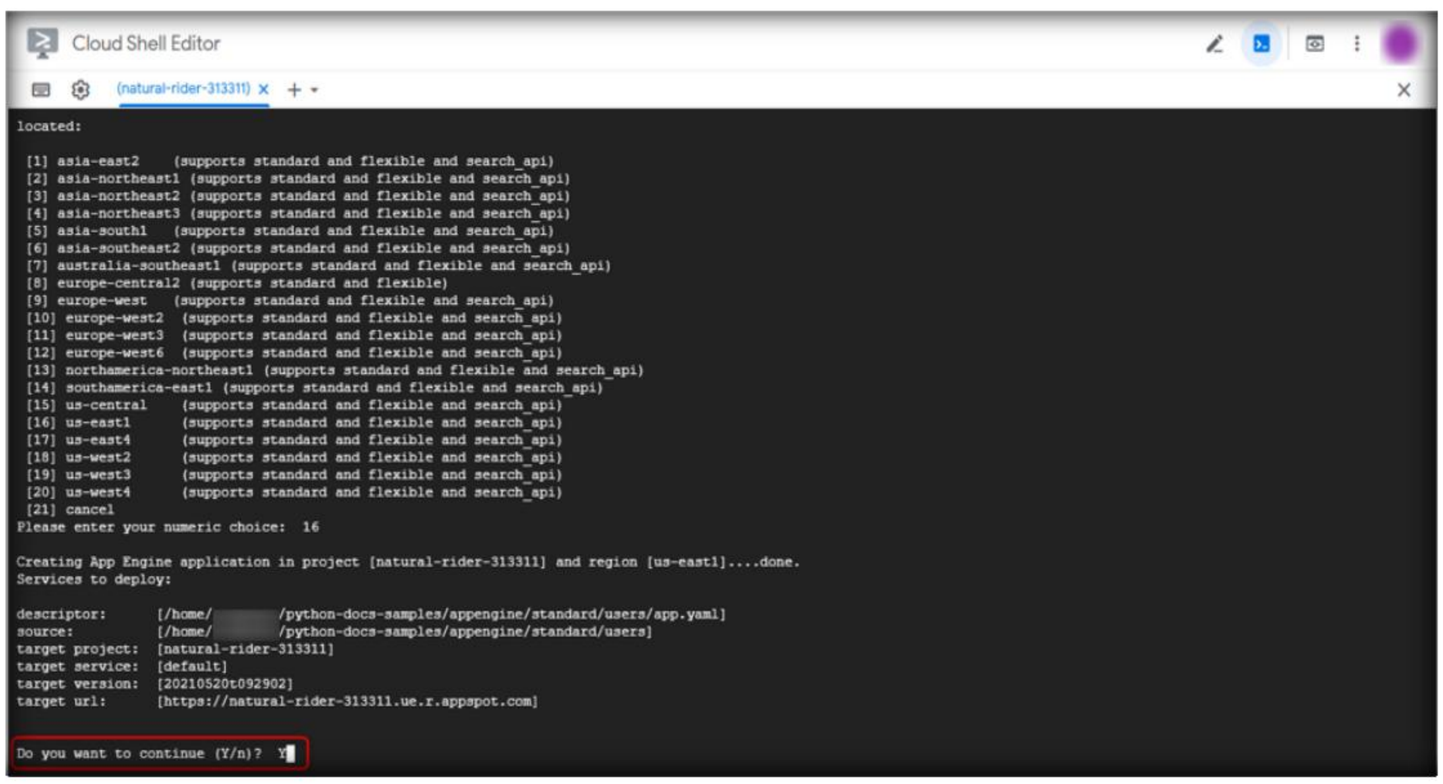


FIGURE 3.4.23: Confirming the deployment

26. Your **App Engine sample application** will be successfully created. Copy the **target url** (URL for accessing the sample application) and paste it in notepad for future use.

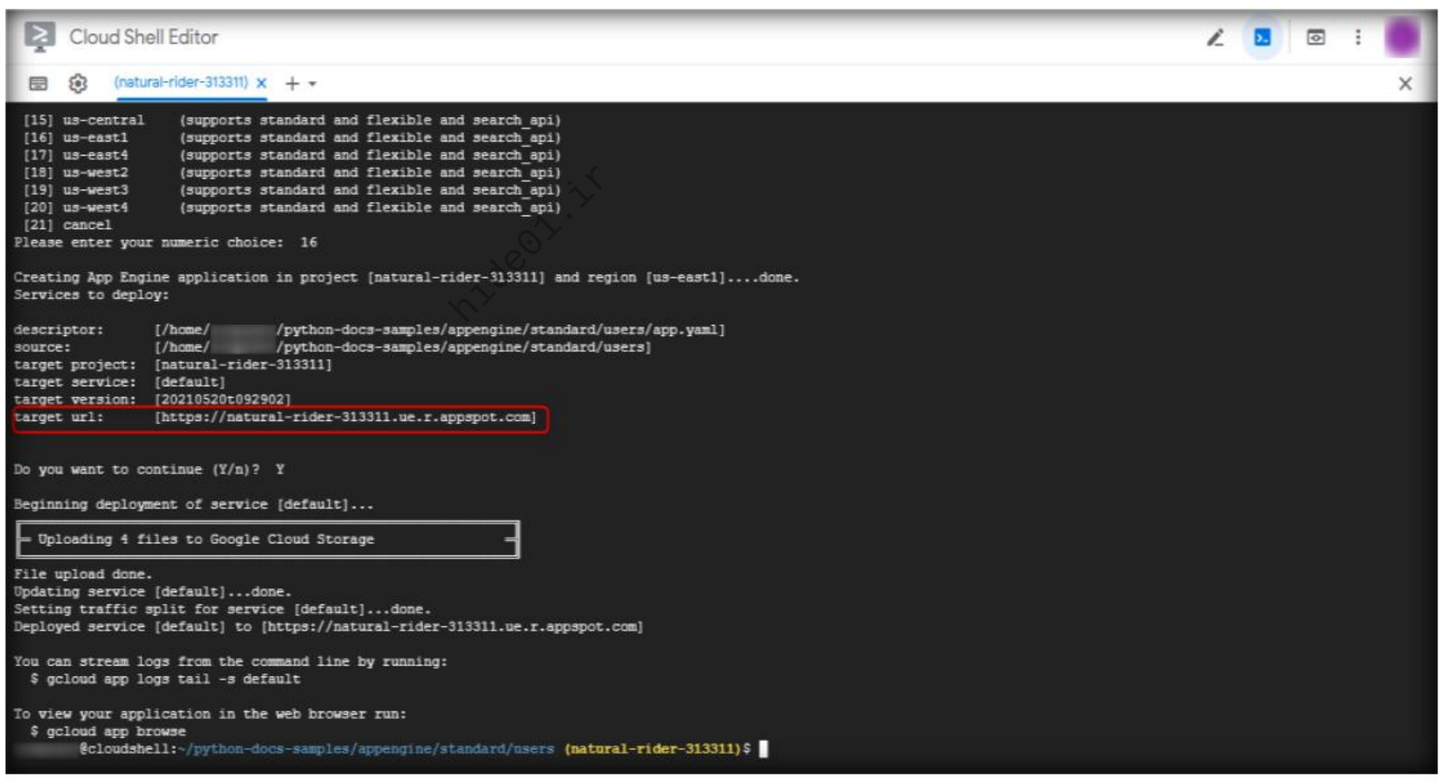


FIGURE 3.4.24: Application Deployed Successfully

27. Now, open a new tab in the **Google Chrome** browser window and paste the **target url** in its address bar to access the sample application. Press **Enter**. The sample application will open in the browser; click on **Sign in**.

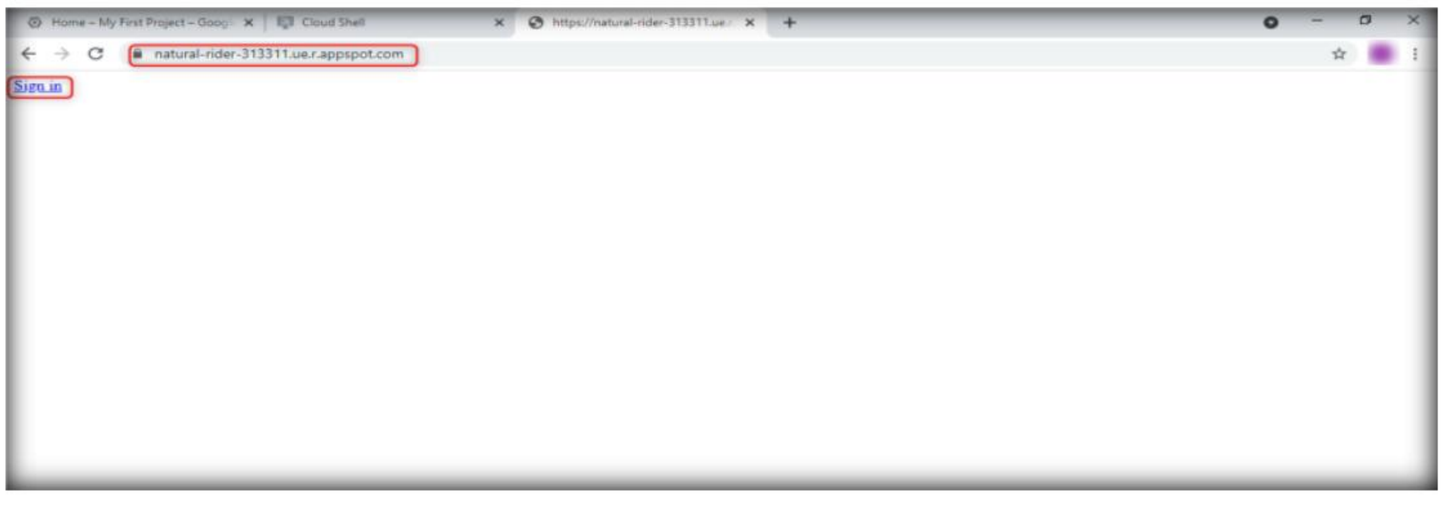


FIGURE 3.4.25: Accessing the application

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

28. Click on **Next** to continue authentication.

Note: In this page, the Google account with which you are currently logged in to the GCP console will be automatically selected for signing in.

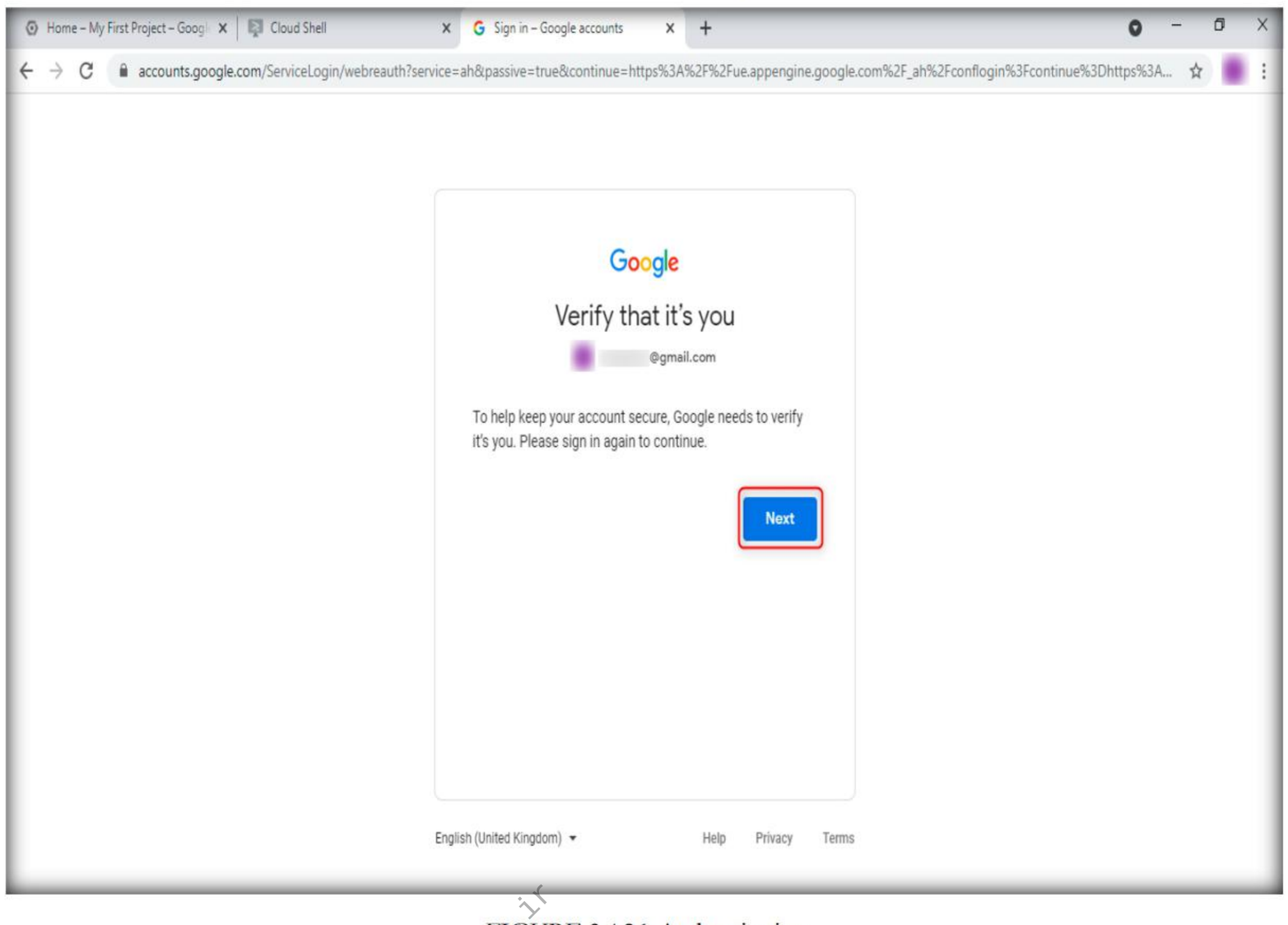


FIGURE 3.4.26: Authentication

29. Enter the password and click on **Next**.

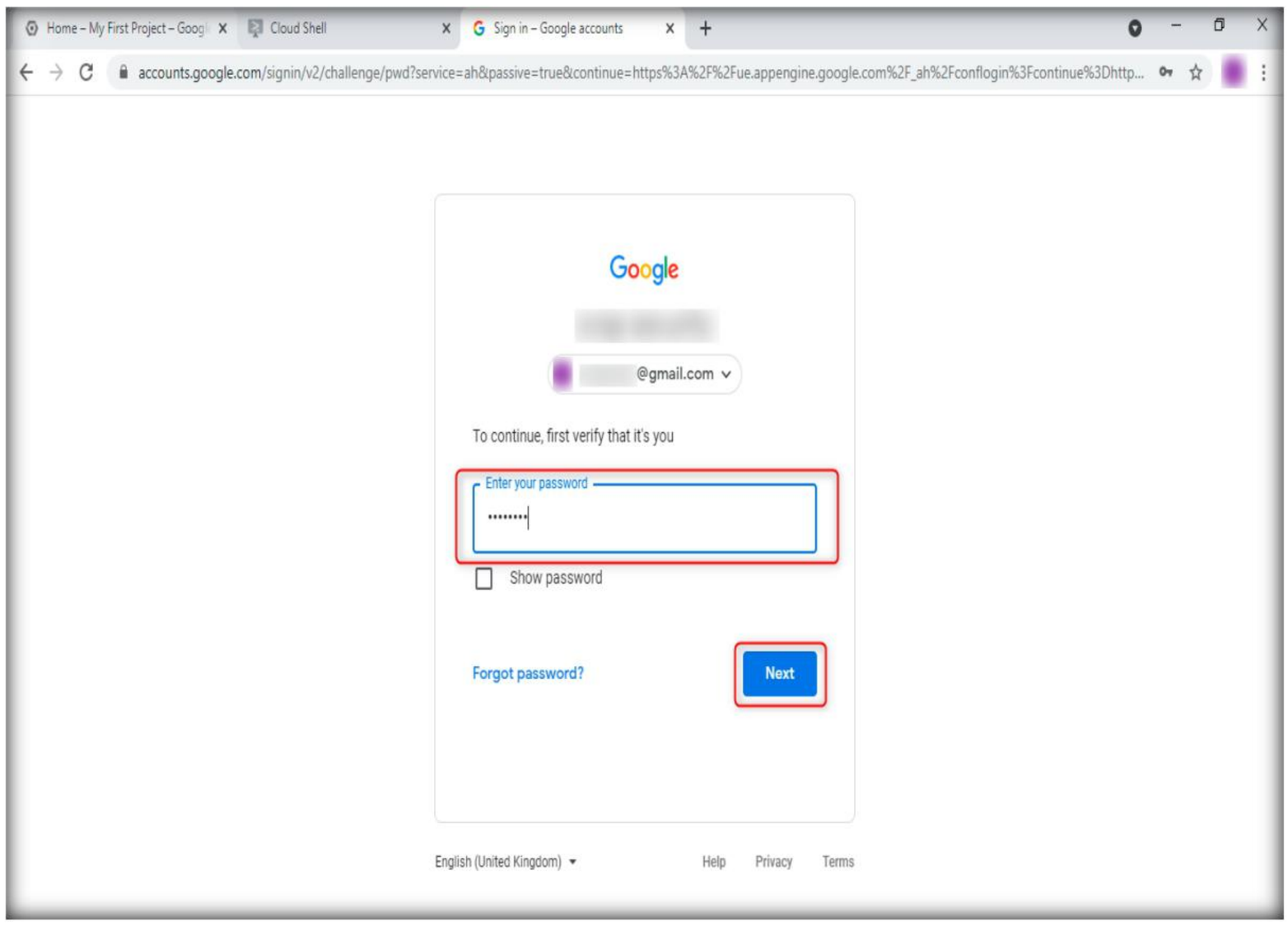


FIGURE 3.4.27: Authenticating to the application

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

30. You will see a **Welcome** message with your Google account username. This way, anyone with a Google account can easily login to the deployed sample application.

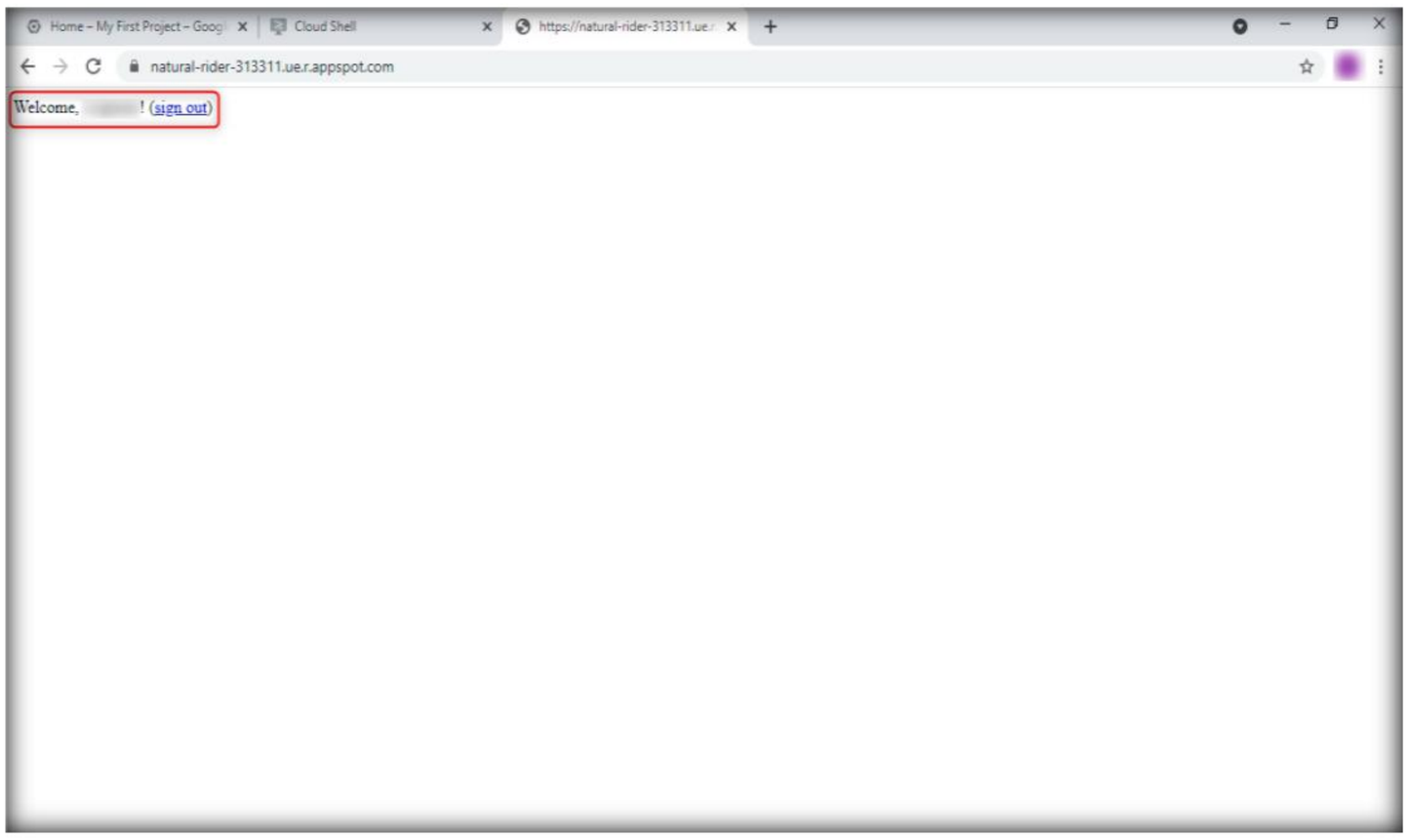


FIGURE 3.4.28: Accessed the Web Page

TASK 3

Implementing IAP for the Application

31. Now, to implement **Identity-Aware Proxy** to restrict access to the App Engine sample application, go to the main GCP menu in the top left corner. Navigate to **Security** and select **Identity-Aware Proxy** from console.

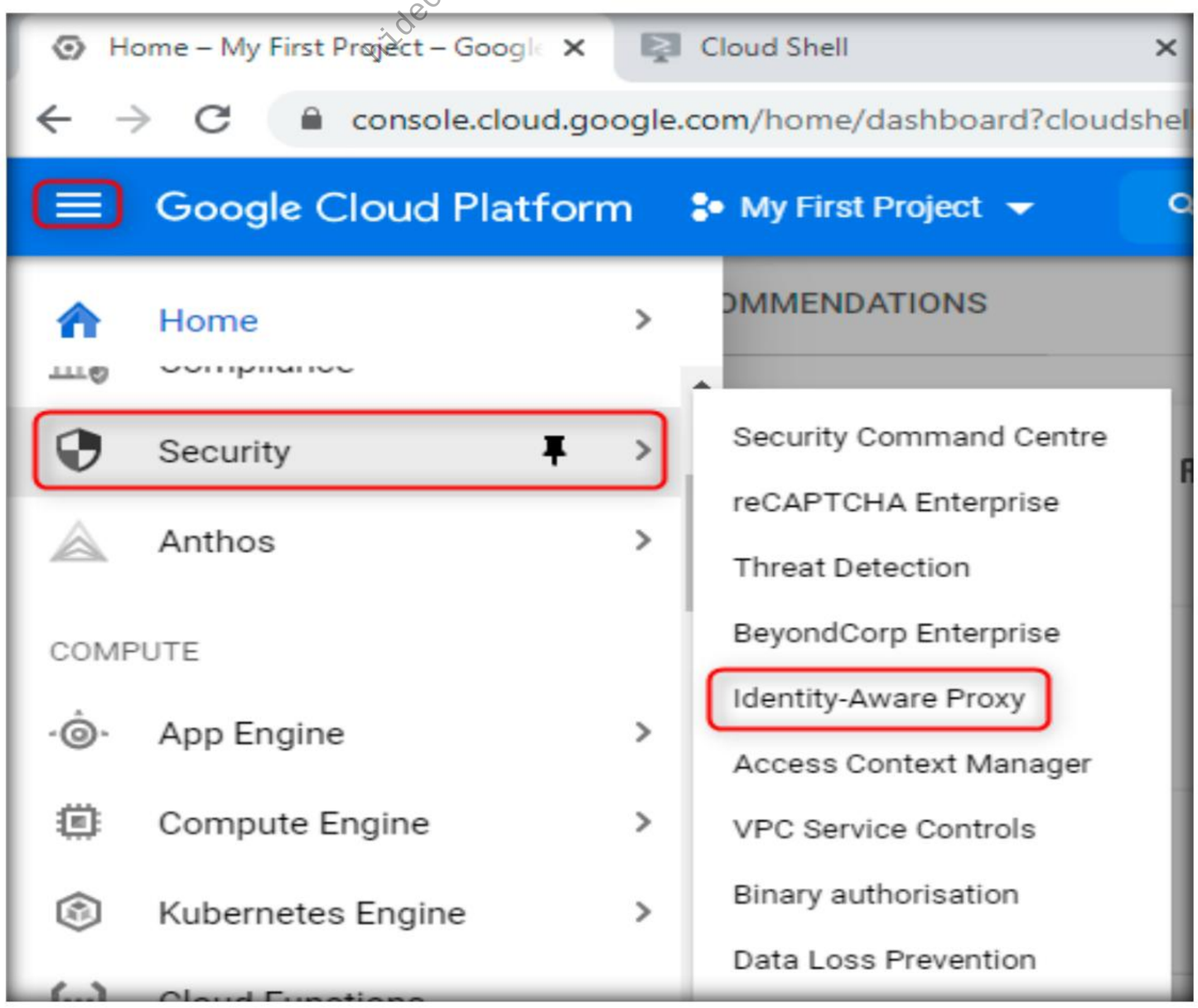


FIGURE 3.4.29: Navigating to Identity-Aware Proxy

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

32. In the **Identity-Aware Proxy** window that appears, click on **ENABLE API**. Wait for it to be enabled.

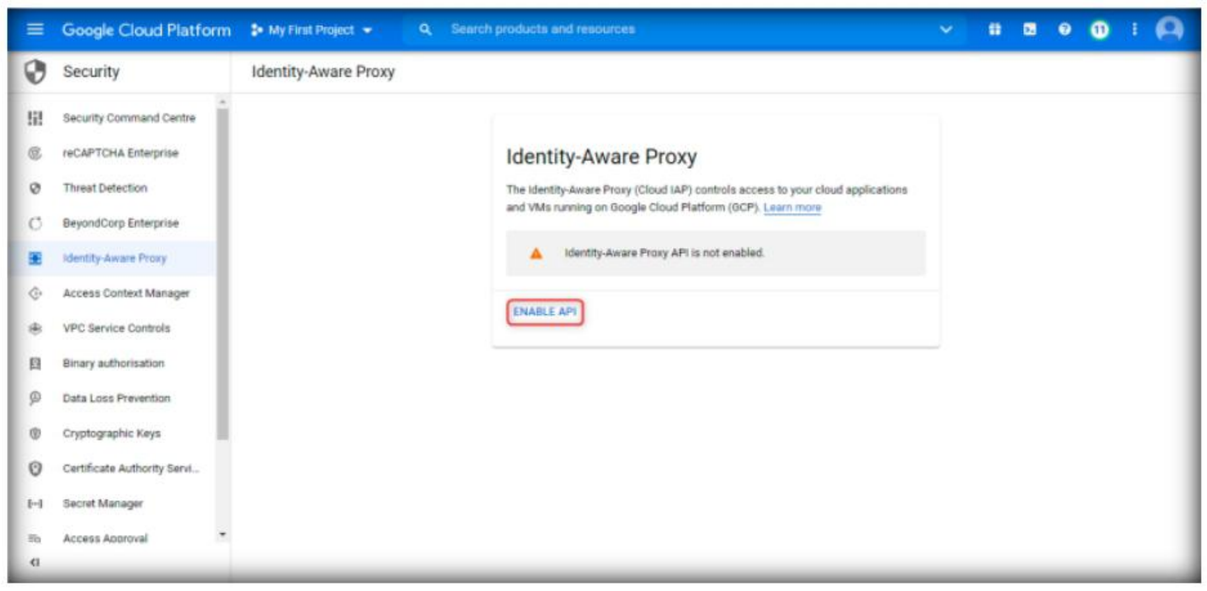
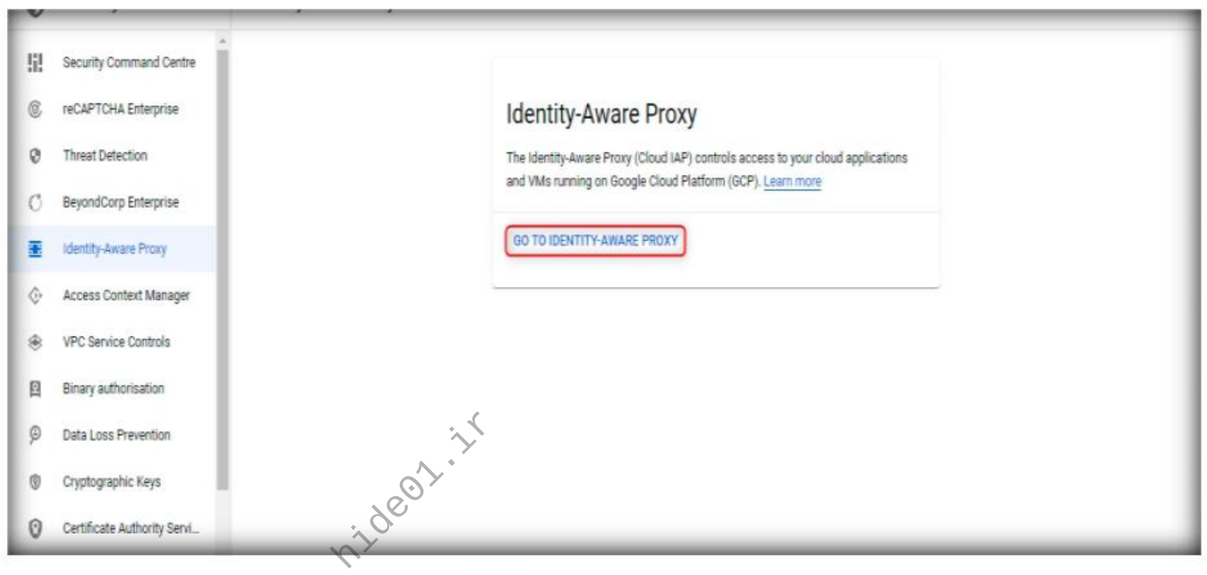


FIGURE 3.4.30: Enabling IAP

33. Once IAP is enabled, click on **GO TO IDENTITY-AWARE PROXY**.



hide01.ir

FIGURE 3.4.31: Opening IAP

34. Now, to start using IAP, first, you should configure the OAuth consent screen, which is a prompt that informs users requesting data access. Click on **CONFIGURE CONSENT SCREEN** to configure the OAuth consent screen.

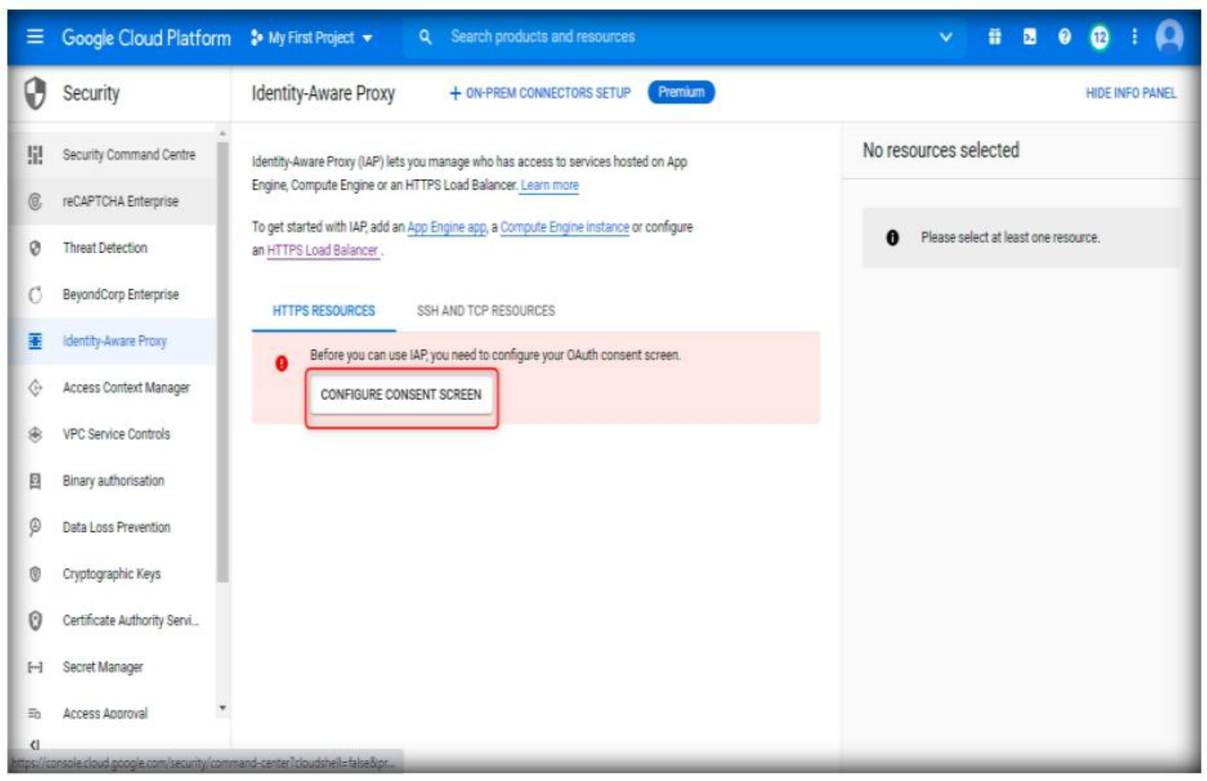


FIGURE 3.4.32: Configuring OAuth consent screen

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

35. In the **OAuth consent screen** page that opens subsequently, select **User Type** as **External** to configure application access to any user with a Google account. Then, click on **CREATE**.

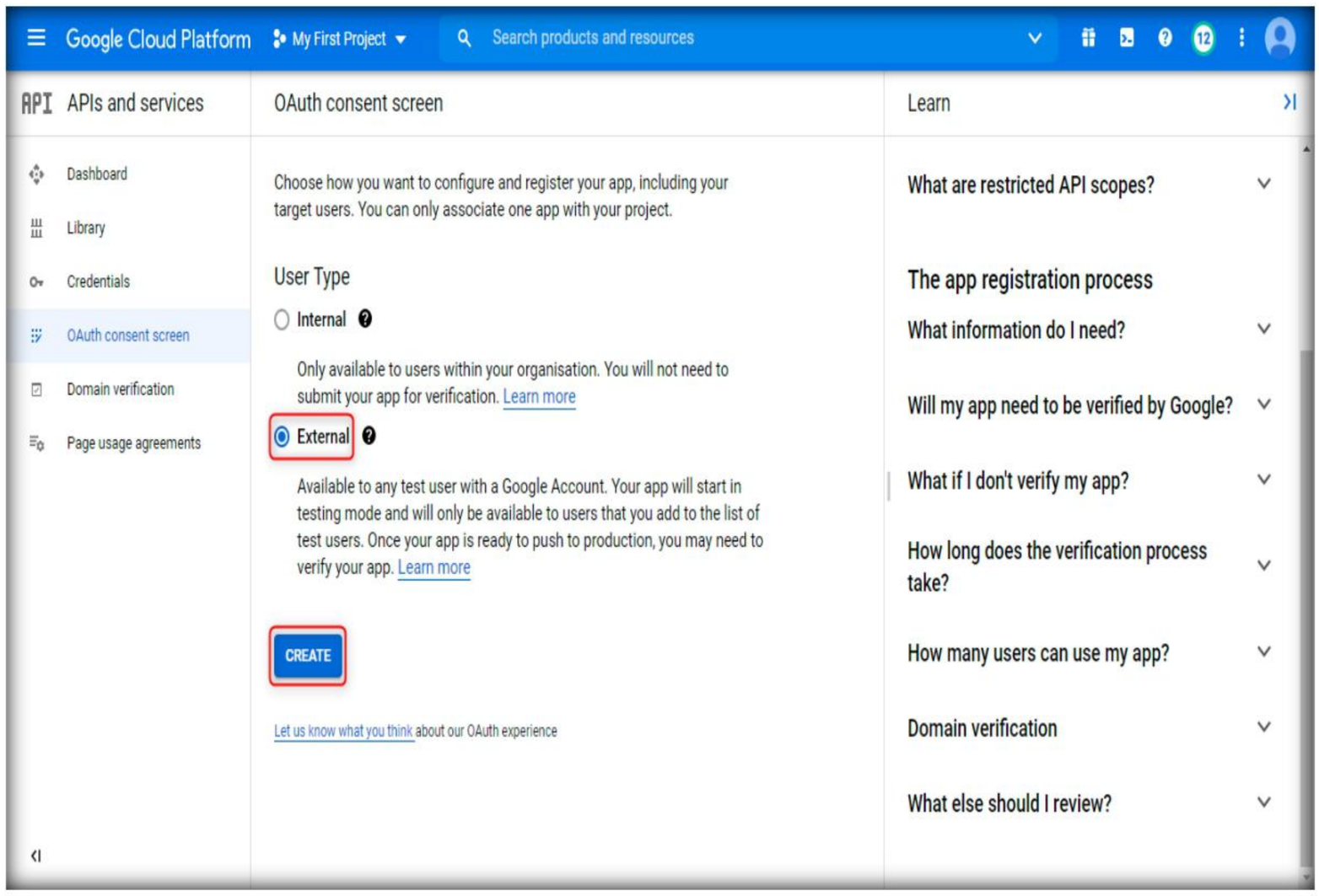


FIGURE 3.4.33: Configuration of OAuth consent screen

36. In the subsequent window for **App information**, enter **eccwebapp-1** in **App name**. In **User support email**, type your GCP account Gmail id. This email ID is added for user support in case of any problems.

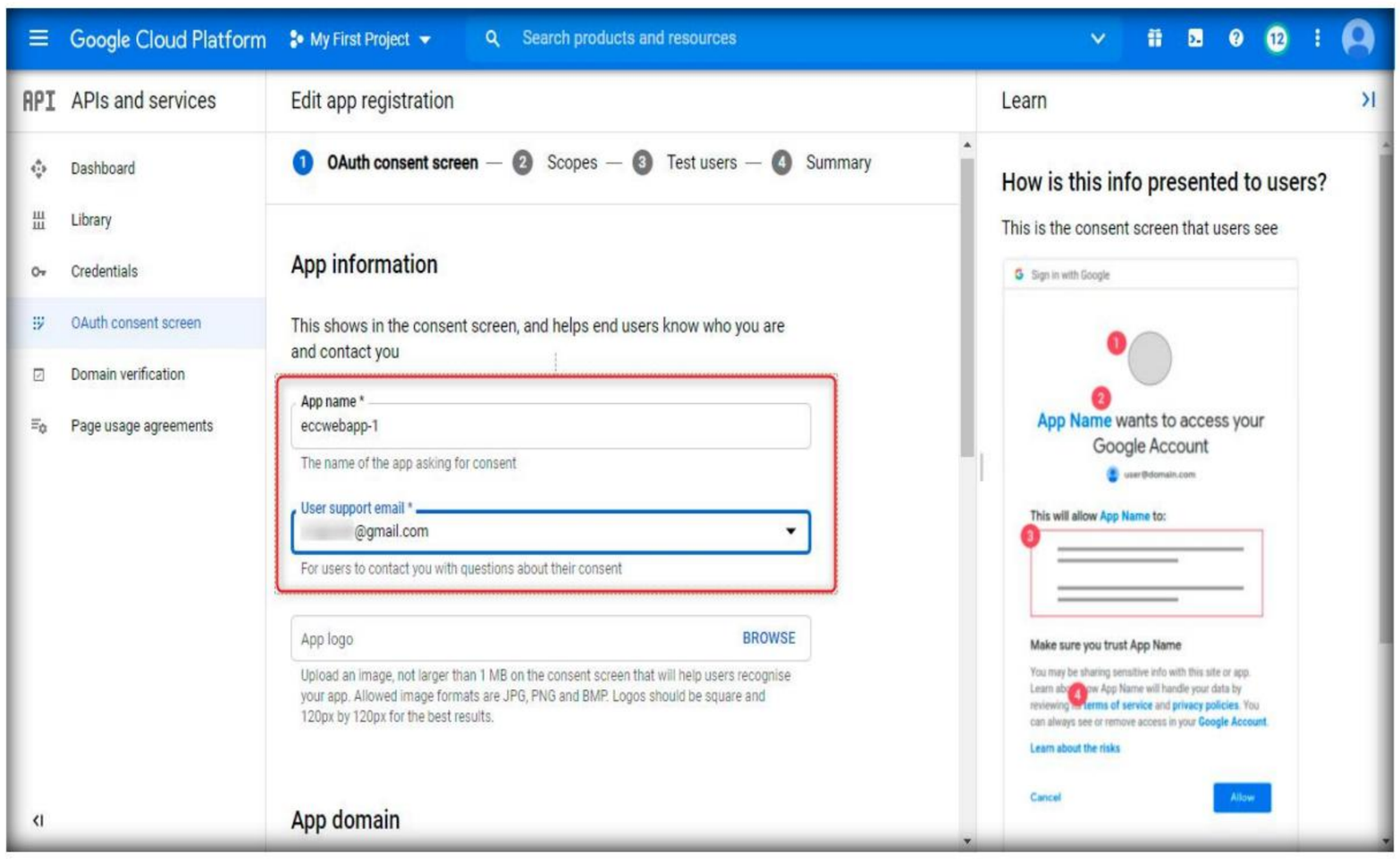


FIGURE 3.4.34: Entering other information

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

37. Scroll down to the bottom. In **Developer contact information** under **Email addresses,** enter your GCP account email ID. Any changes in your project will be notified by Google to this email ID. Click on **SAVE AND CONTINUE.**

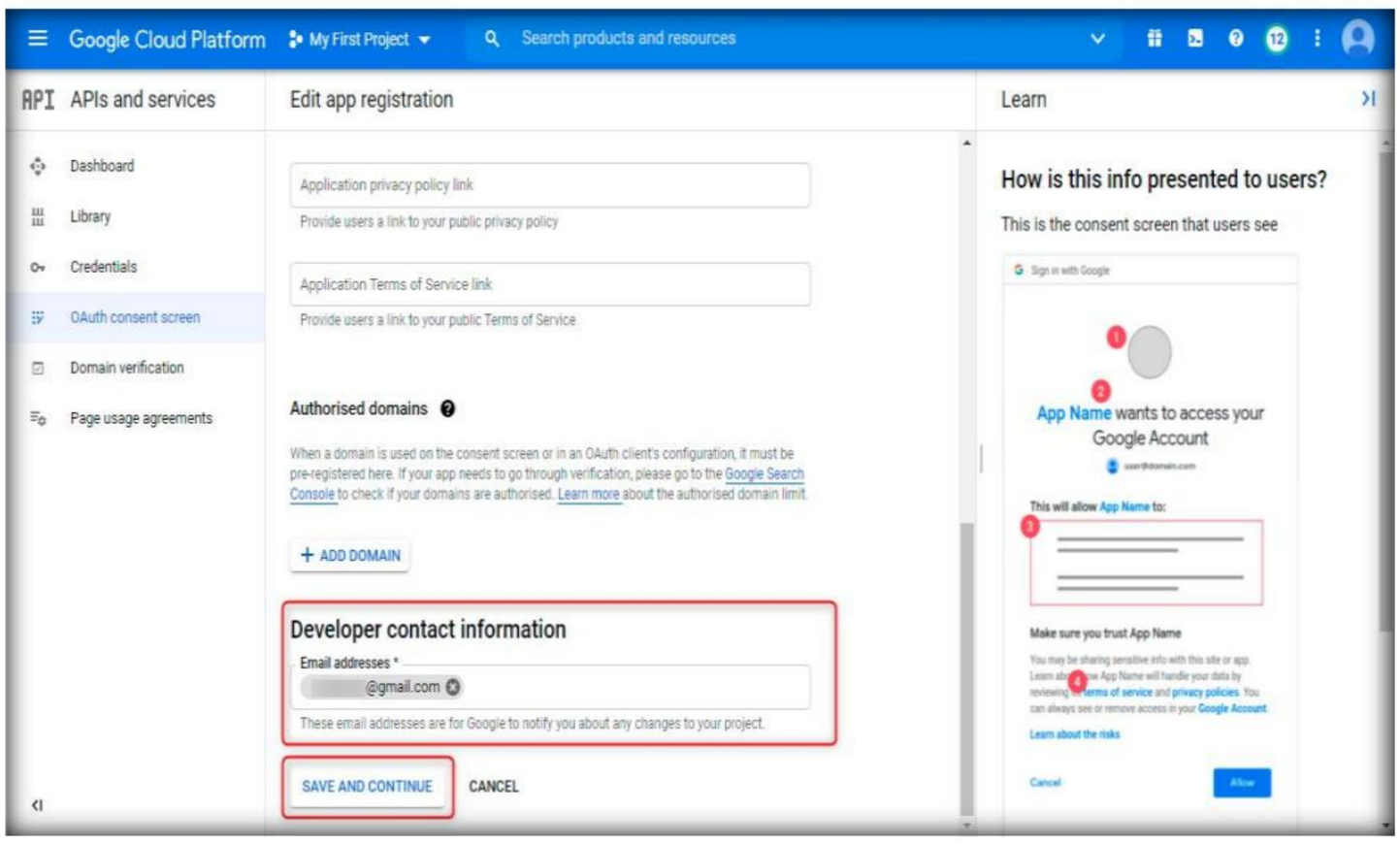


FIGURE 3.4.35: Saving OAuth configuration

38. After the OAuth consent screen is configured, click on the main menu in the top left corner, navigate to **Security,** and select **Identity-Aware Proxy** in the console.

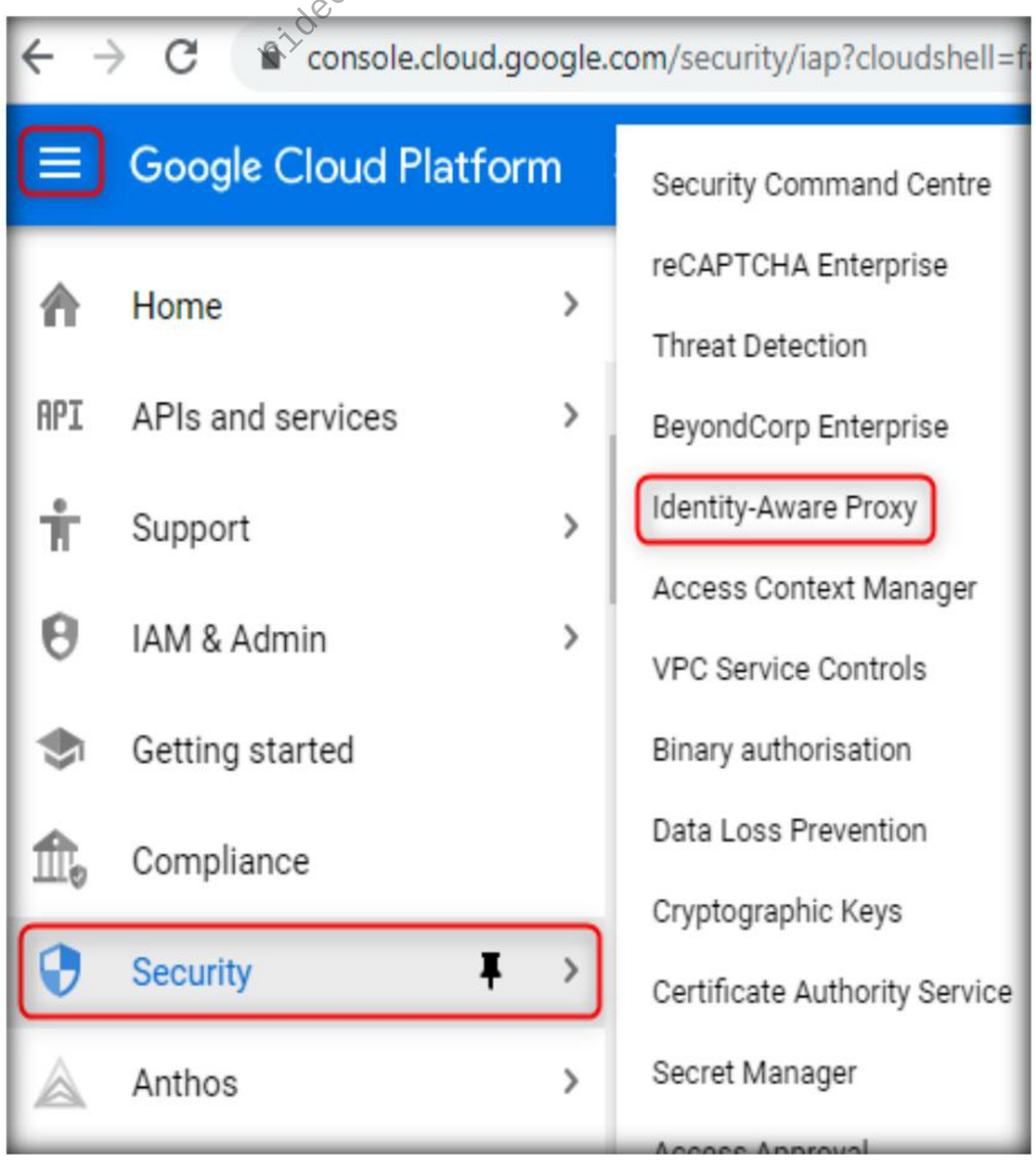


FIGURE 3.4.36: Navigating to Cloud IAP

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

39. First, select the checkbox for **App Engine app** having the published URL of the sample application. To assign permissions to users, click on **ADD MEMBER** to the right.

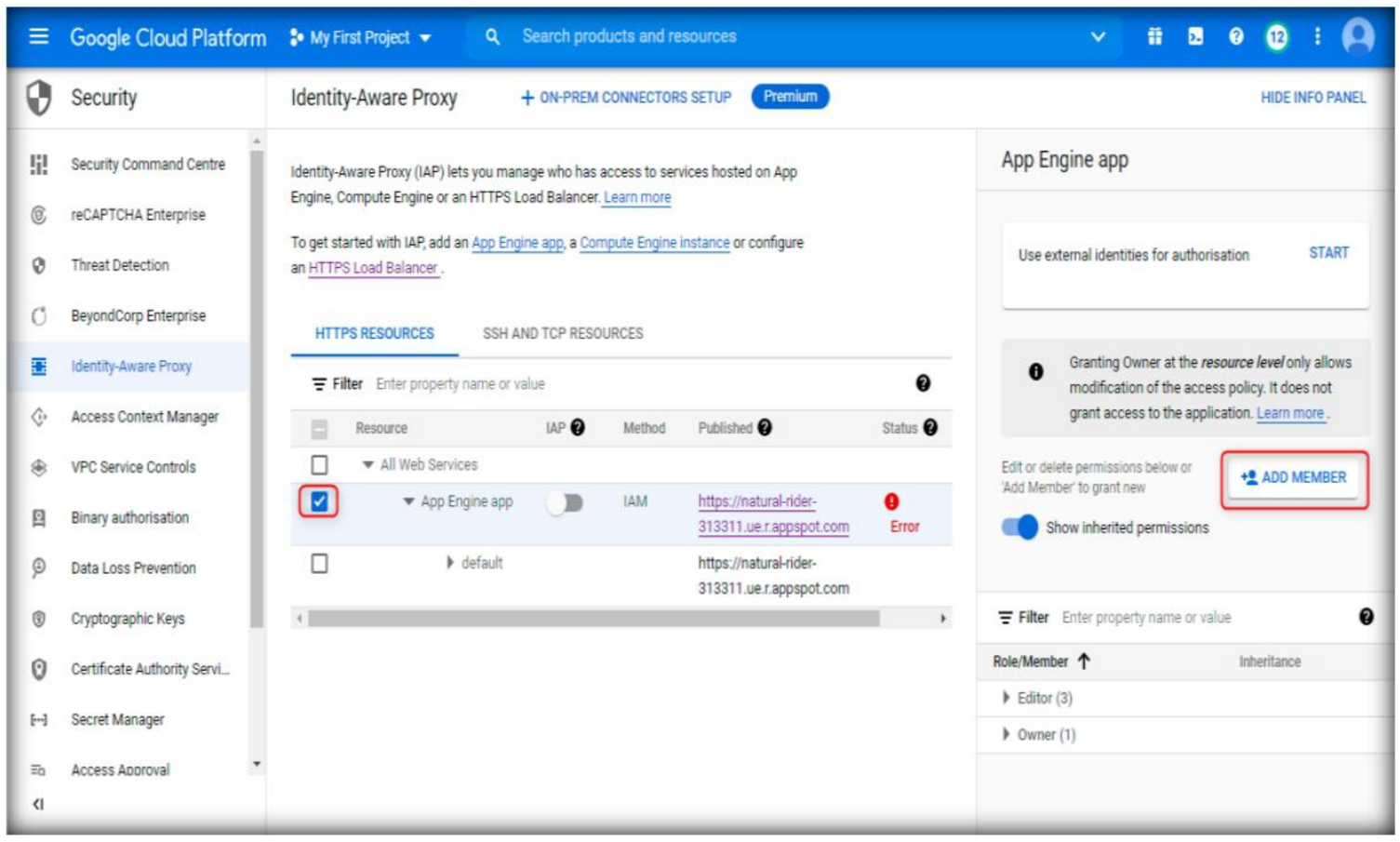


FIGURE 3.4.37: Selecting the app and adding members

40. In the **Add members to App Engine app** window that opens, you have to add the members to whom access should be granted. Under **New members,** add any active Gmail account. Now, to configure the Cloud IAP role of the added user, click on **Select a role**. Under **All roles**, select **Cloud IAP,** and then select **IAP-secured Web App user**.

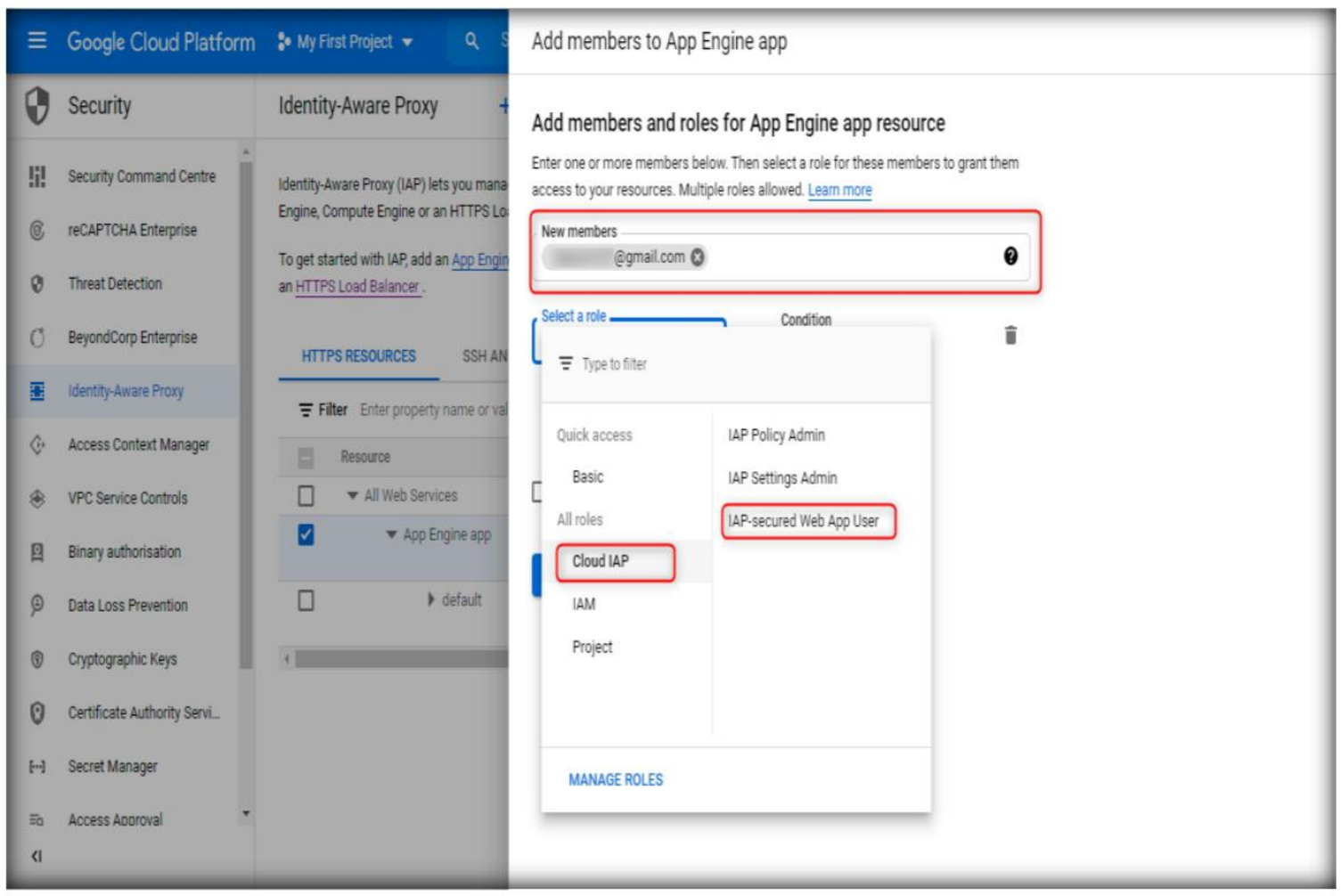


FIGURE 3.4.38: Adding User and Roles

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

41. Click **SAVE** to save the new member and the Cloud IAP role.

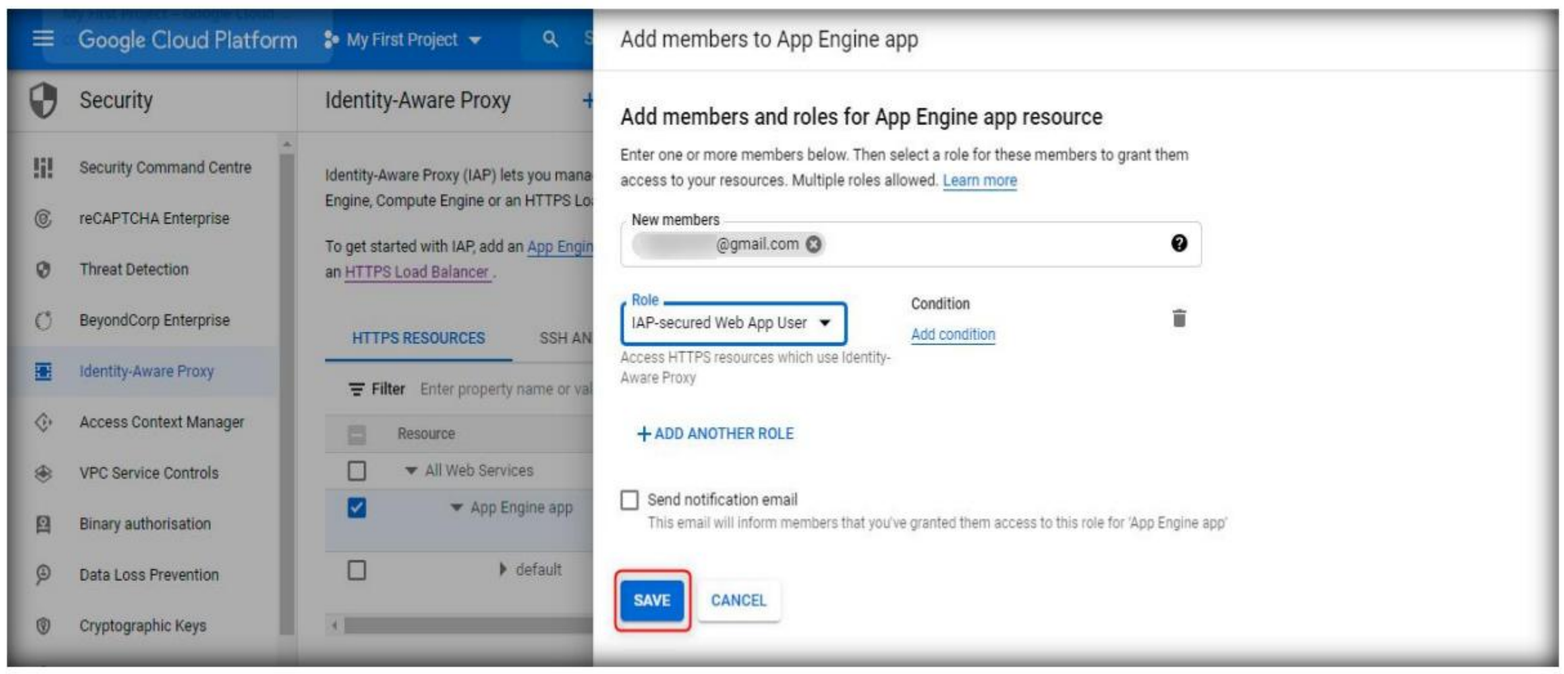


FIGURE 3.4.39: Saving the Policy

42. Now, turn on IAP by moving the slider under **IAP** for the **App Engine app**.

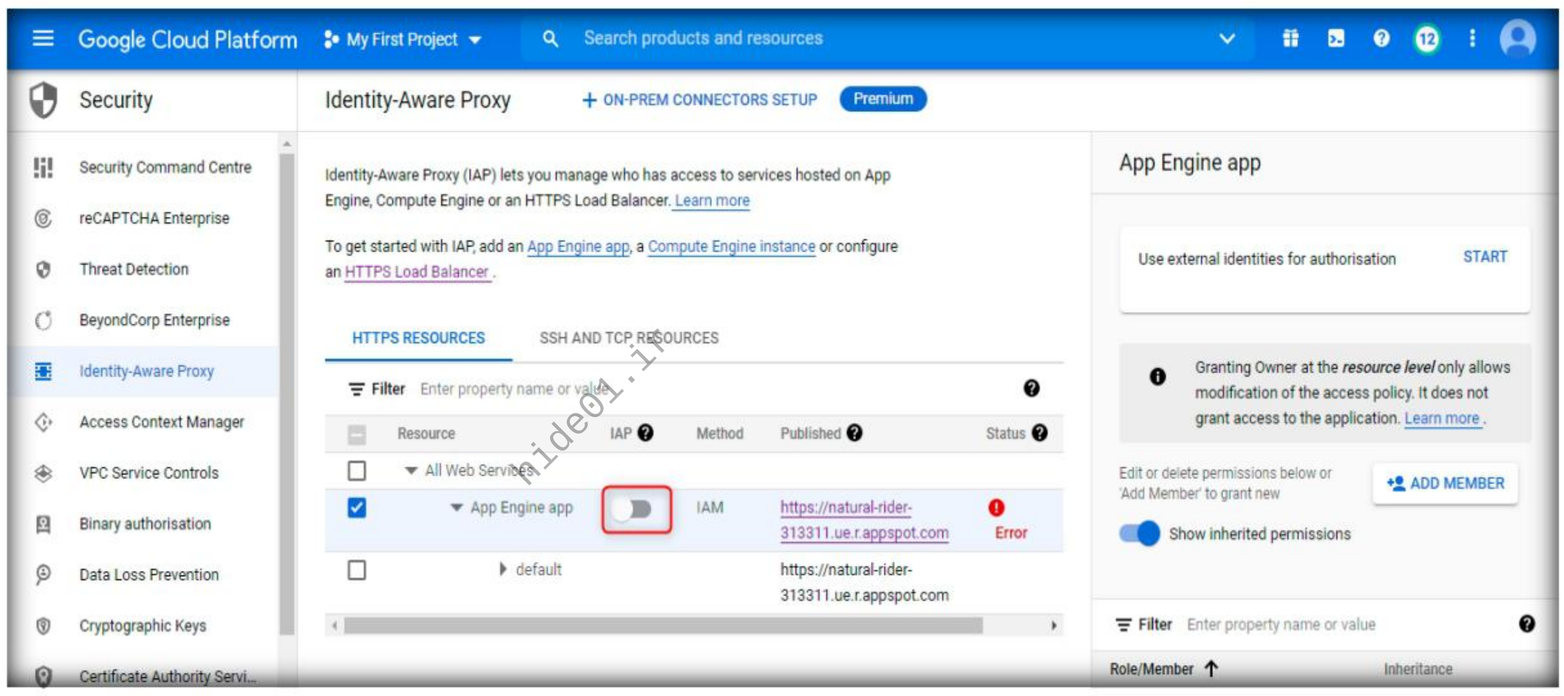


FIGURE 3.4.40: Turning on IAP

43. In the popup window that appears, click on **TURN ON**.

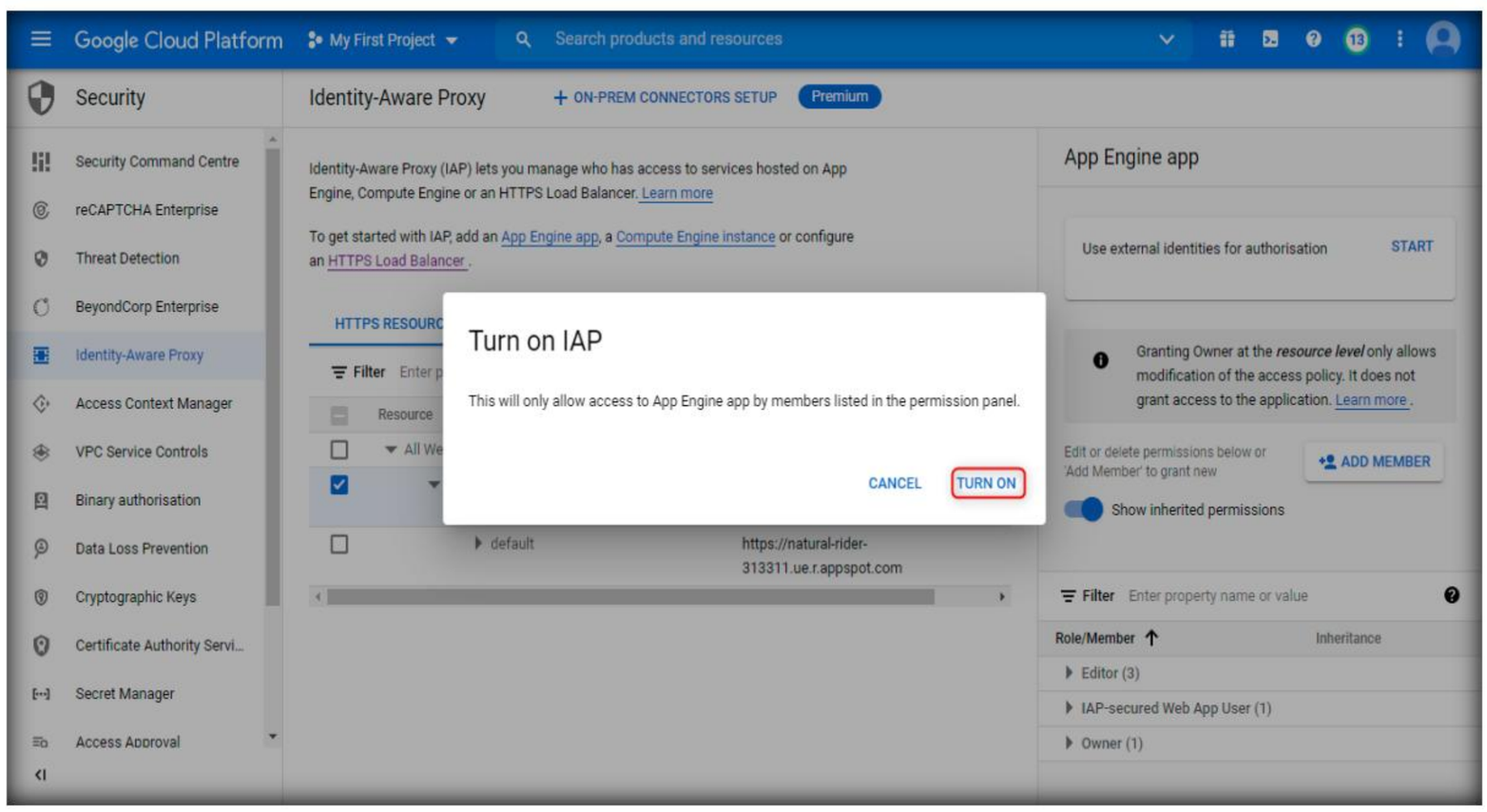


FIGURE 3.4.41: Turning on IAP for the App

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 4

Testing Access to the Application

44. IAP will be turned on successfully and **Status** will be marked as **OK**. Now, to test access to the application after enabling Cloud IAP, click on the application link under **Published** for **App Engine app**.

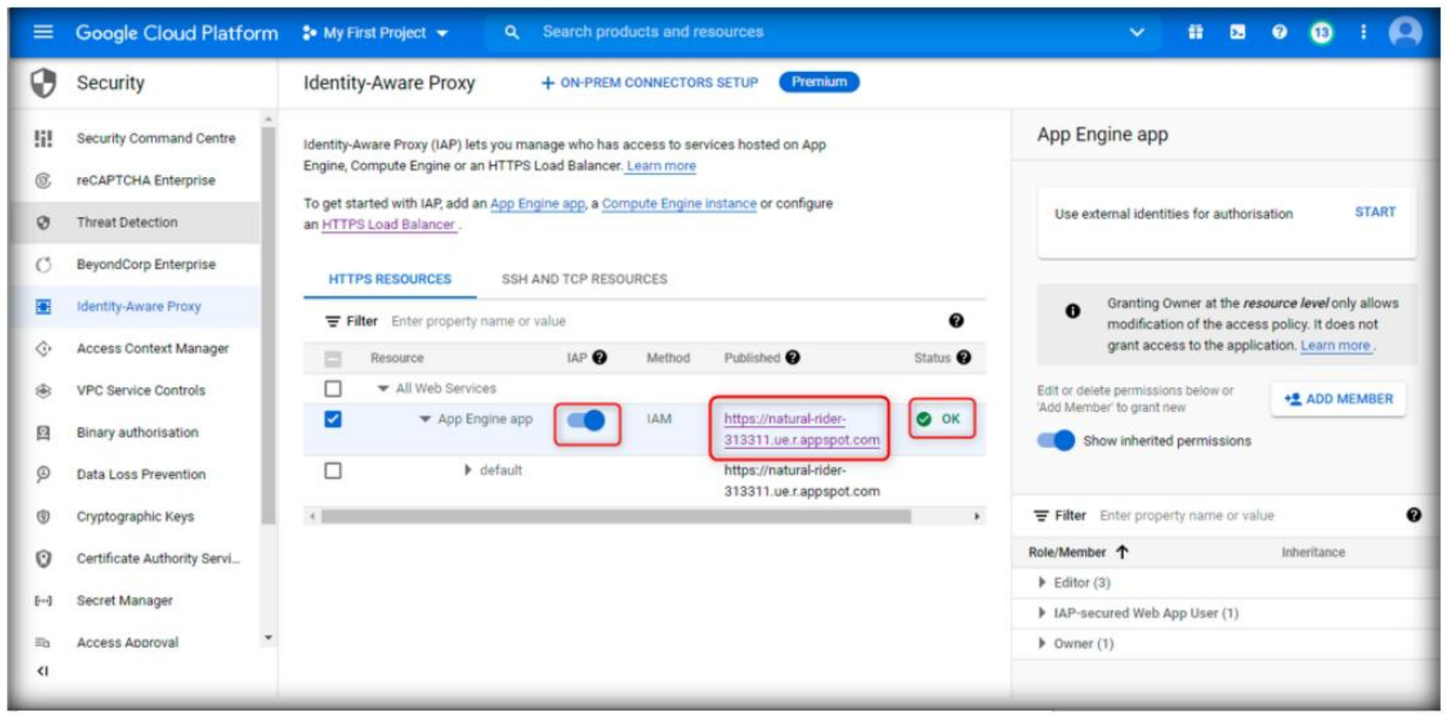


FIGURE 3.4.42: Opening the Application Link

45. In the application web page that opens, click on **Sign in**.



hide01.ir

FIGURE 3.4.43: Accessing the App Engine application

46. Enter the **Email address** of the user to which you granted access for the Cloud IAP role and click on **Next**.

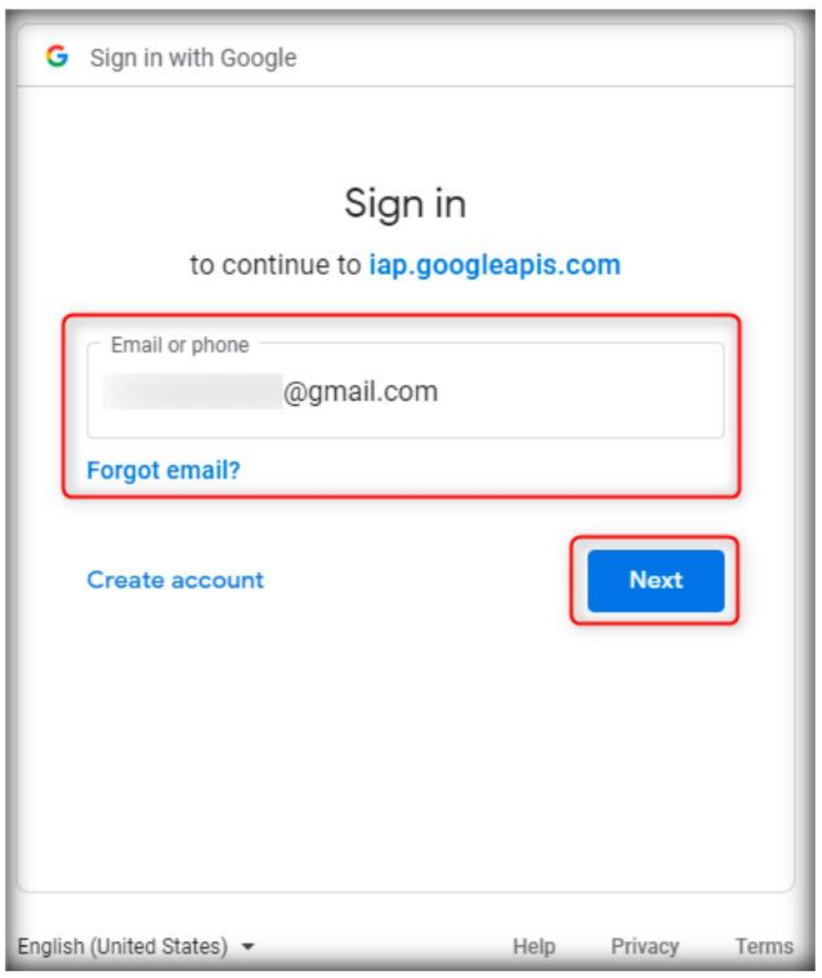


FIGURE 3.4.44: Authentication to the application

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

47. Enter the account **password** and click on **Next**.

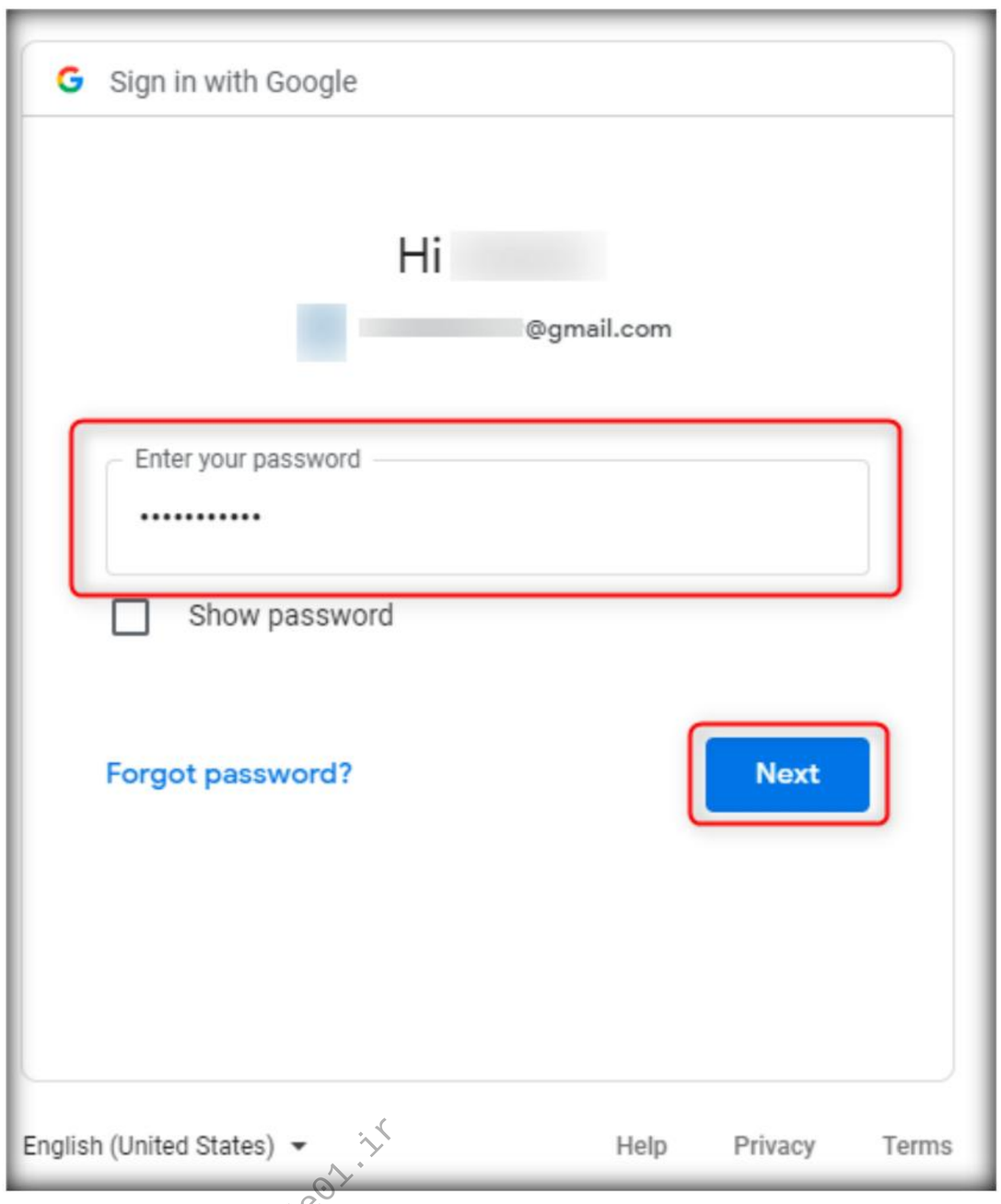


FIGURE 3.4.45: Authentication to the application

hide01.ir

48. You will get a **Welcome** message with the username of the email address. Click **sign out.** Do not close the tab.



FIGURE 3.4.46: Authenticated to the application

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

49. Now, delete the role assigned to the user account and then try to access the application to confirm that Cloud IAP is enabled. To do this, go back to GCP console, navigate to **Security,** and select **Identity-Aware Proxy** in the console.

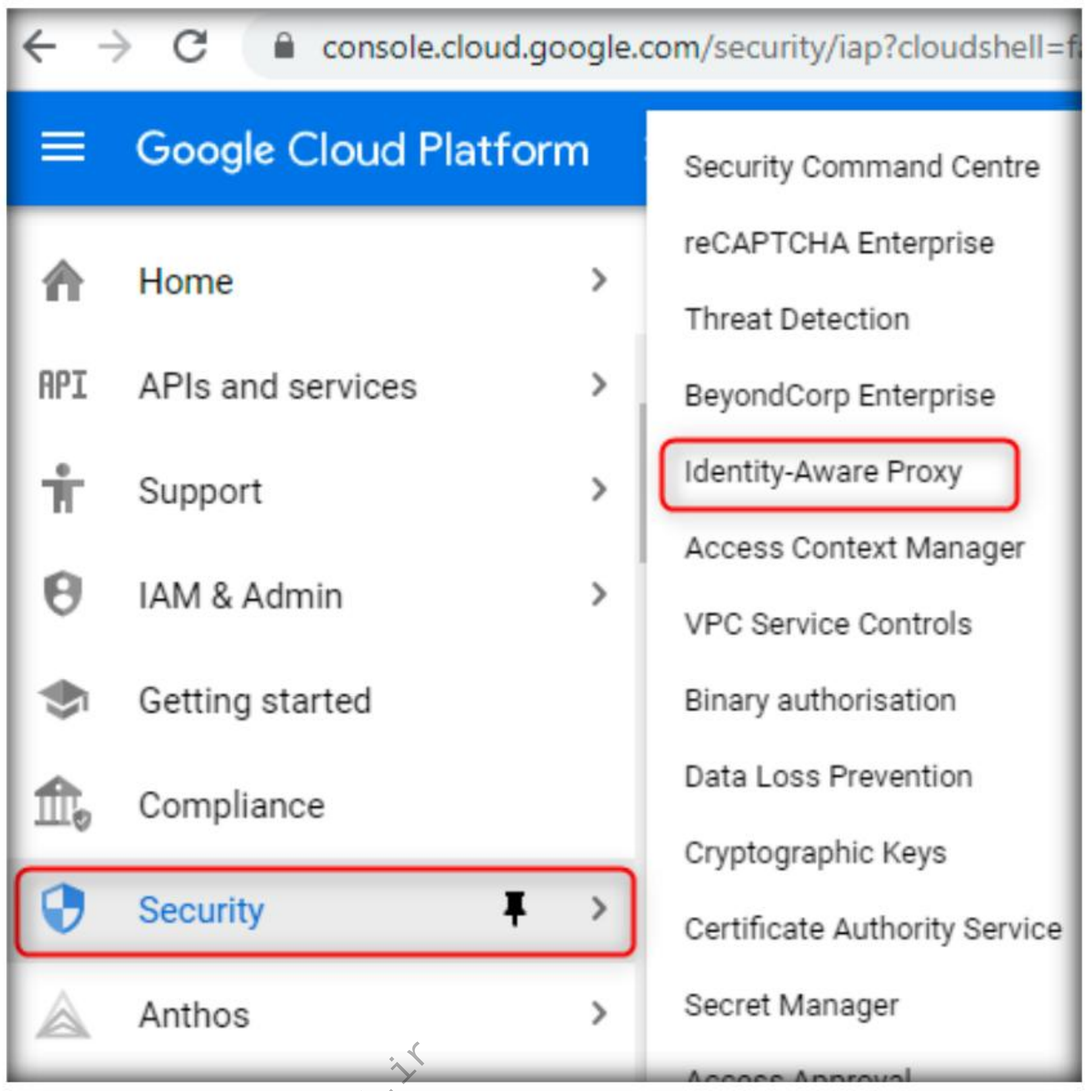


FIGURE 3.4.47: Navigating to IAP

50. Select the checkbox for **App Engine app**. To delete the user and the IAP role, expand **IAP-secured Web App User** at the bottom right corner of the screen under **Role/Member**. Click on the **delete icon** on the right side of the username.

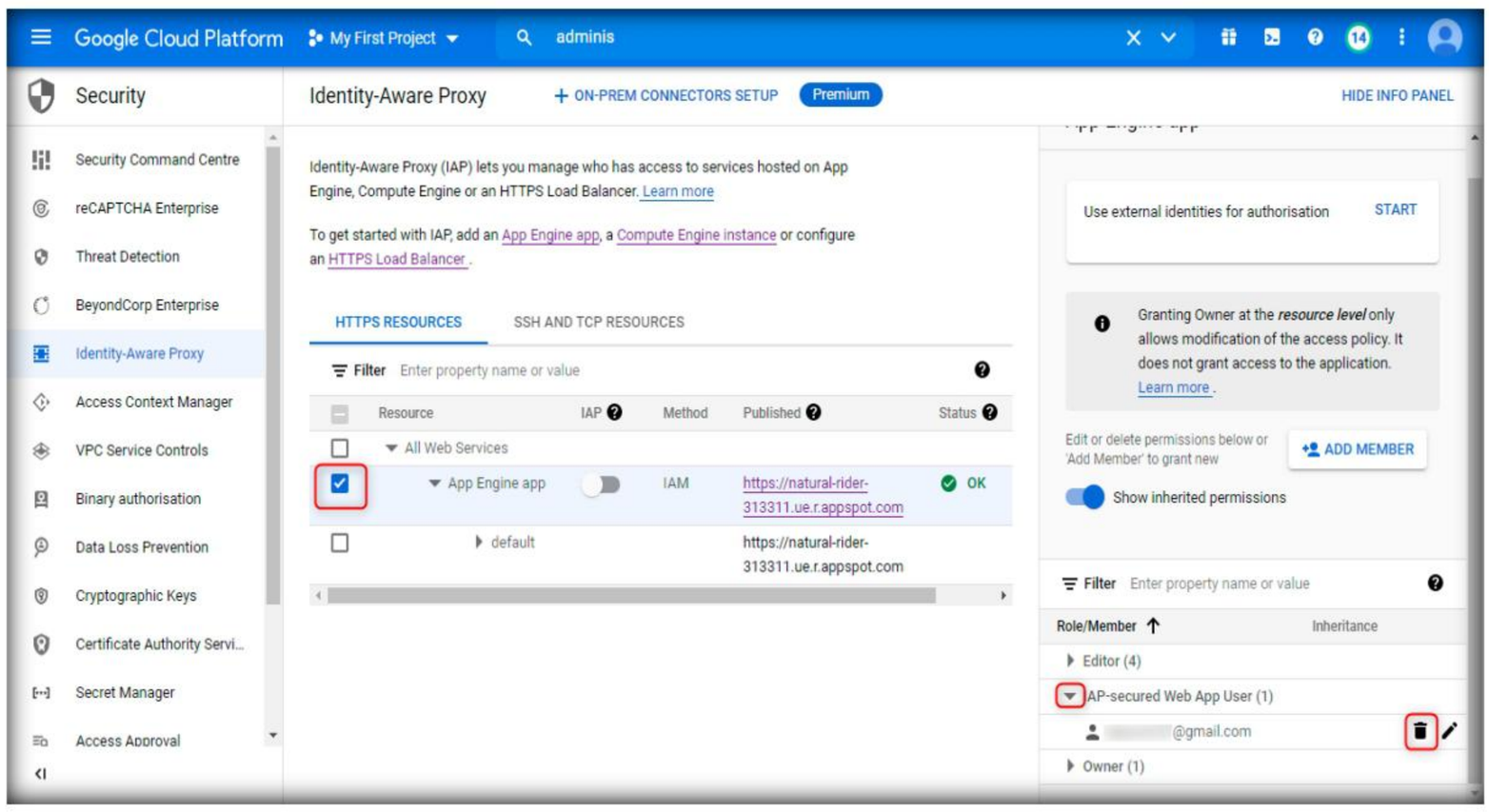


FIGURE 3.4.48: Deleting Roles

Certified Cloud Security Engineer Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

51. In the **Remove role from member** popup that opens, select the checkbox for **Remove the user account from all roles on this resource** to confirm the deletion of **IAP-secured Web App User Role**. Click on **REMOVE**.

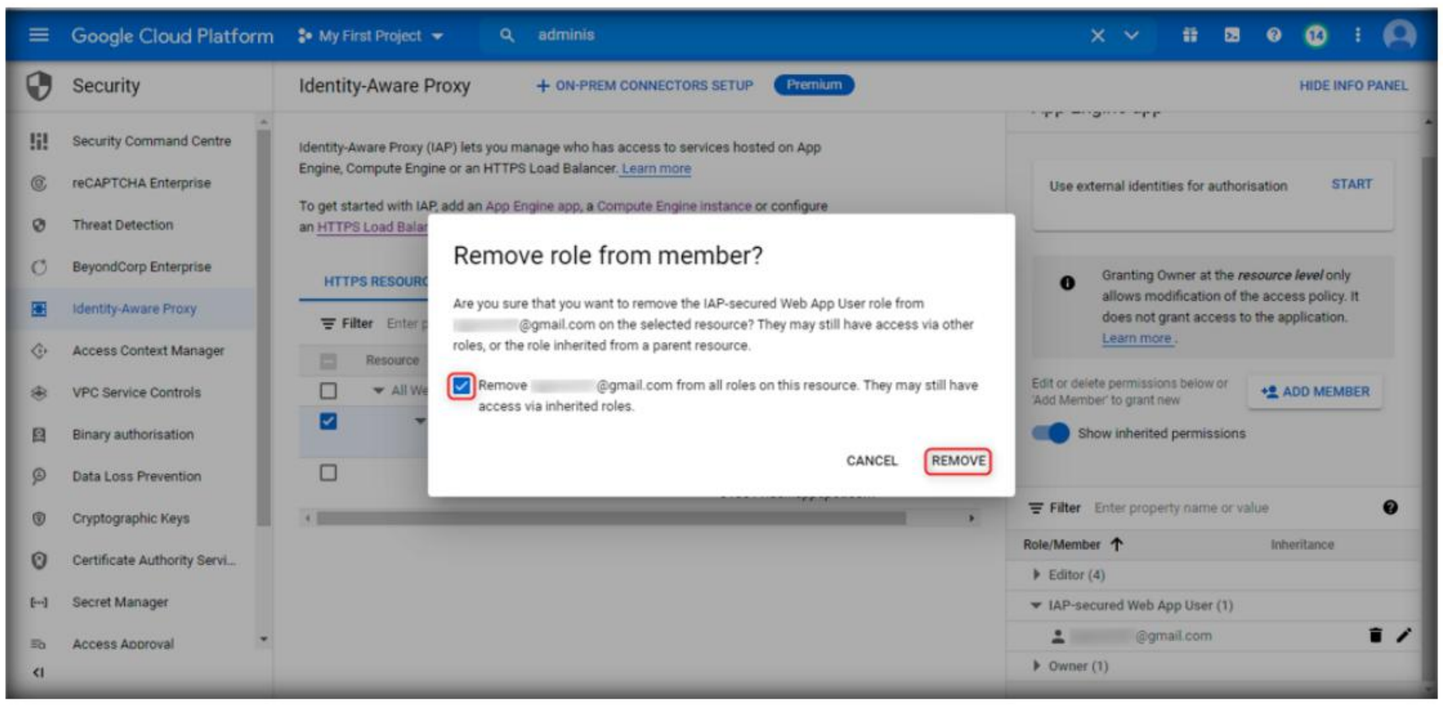


FIGURE 3.4.49: Confirm Deletion

52. Now, try to authenticate to the application again. Go back to the App Engine application in the browser window and click on **Sign in**.



FIGURE 3.4.50: Sign in to the App Engine application

53. Enter the same user's **Email ID** with which you logged in after the IAP role was granted, but whose access has been revoked. Click **Next**.

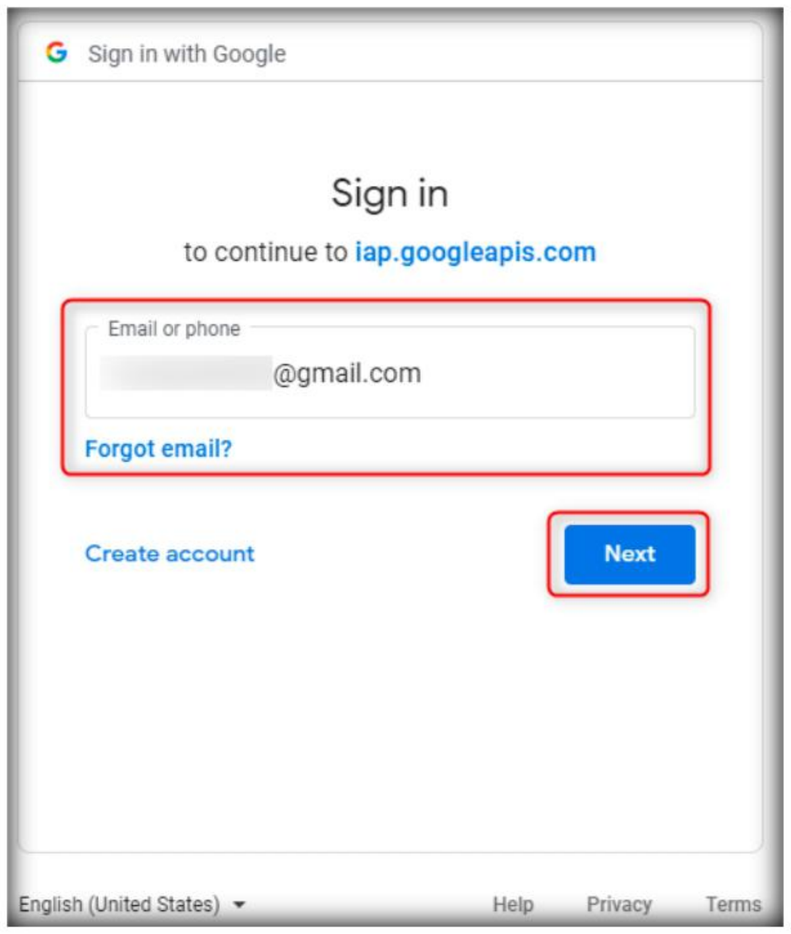


FIGURE 3.4.51: Entering Email

Certified Cloud Security Engineer Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

54. Type the password and click **Next**.

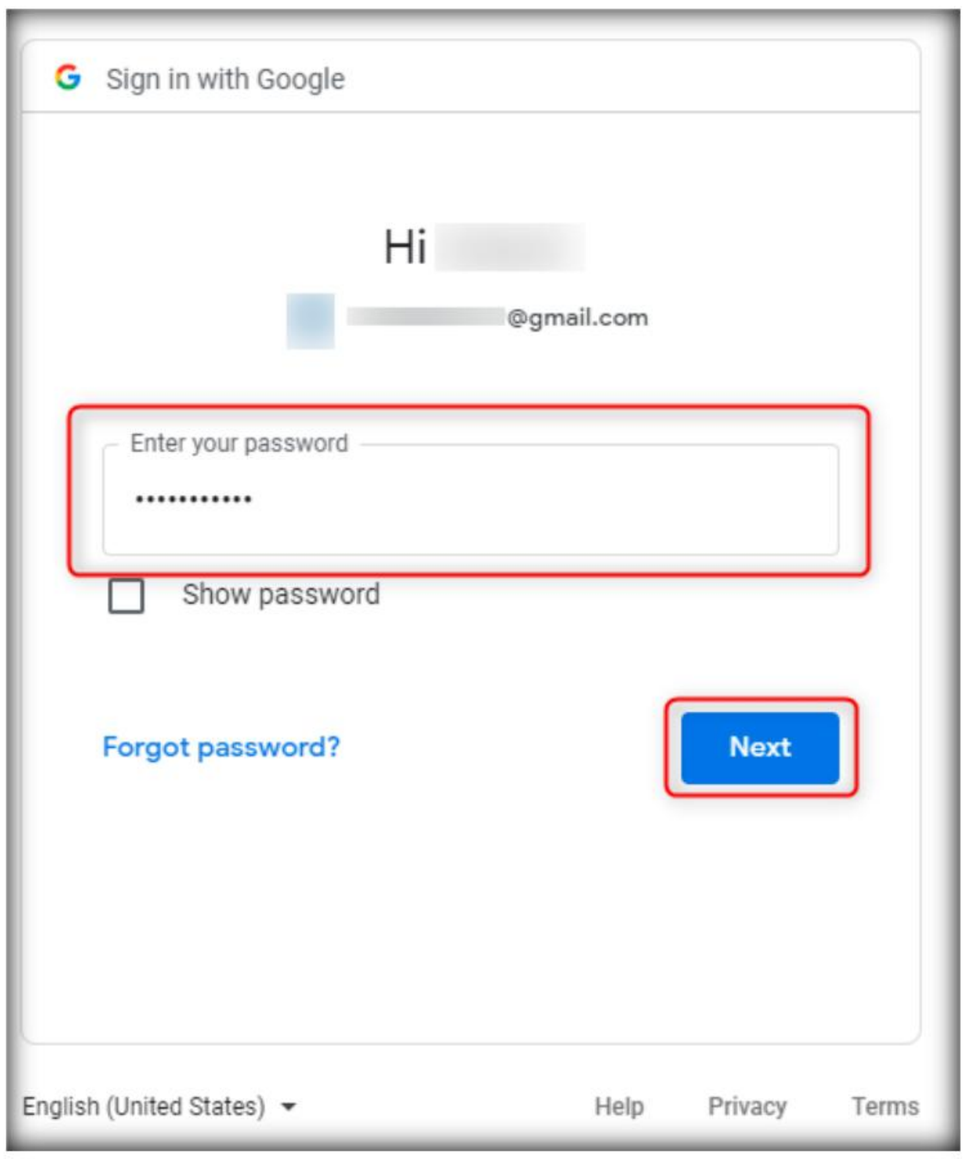


FIGURE 3.4.52: Entering Password

55. You will get a **You don't have access** message because access to the user has been revoked by IAP.

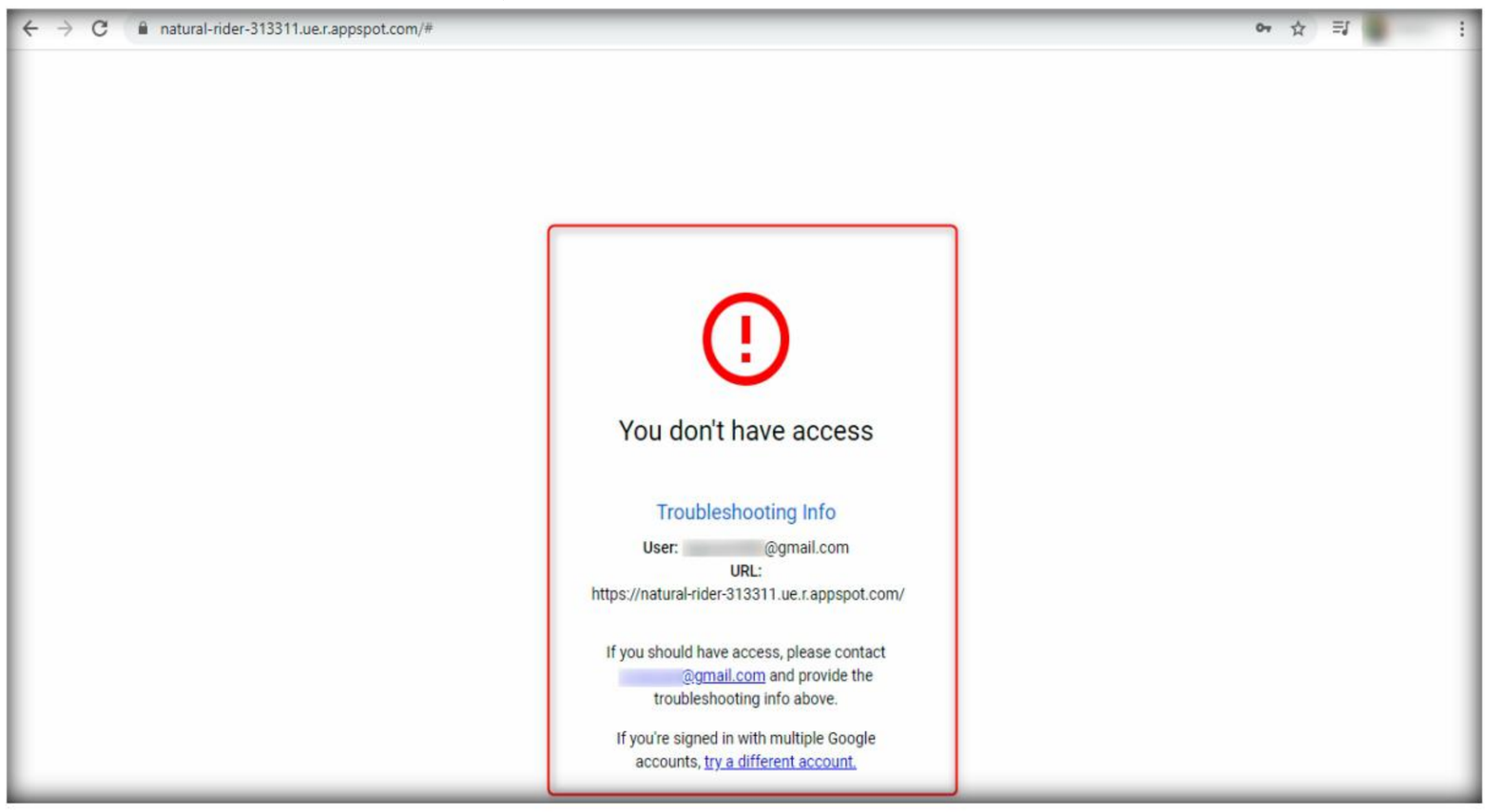


FIGURE 3.4.53: Access Denied Message

56. This way, a cloud security engineer can use Cloud IAP to restrict any unauthorized access to App Engine applications.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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

57. Now, navigate to **App Engine** and click on **Settings** in the left pane to disable the application you have deployed. Click on **Disable application** to disable the application to prevent further charges. In the pop-up window, type the application ID and click **Disable**.

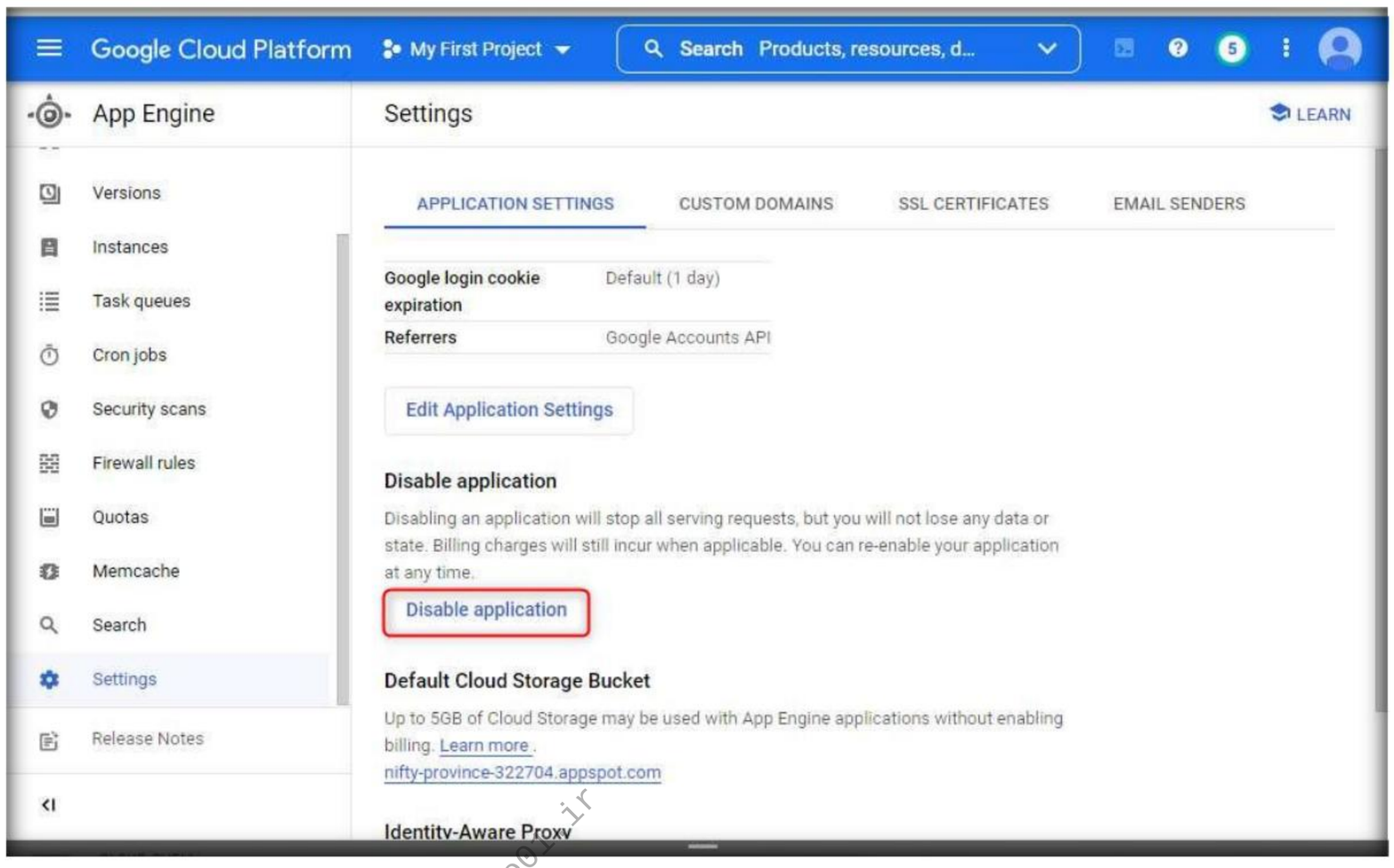


FIGURE 3.4.54: Disabling App Engine Application

58. To delete the cloned repository and the associated folders, type the following command and press **Enter**.

```
rm -rf python-docs-samples.git
```

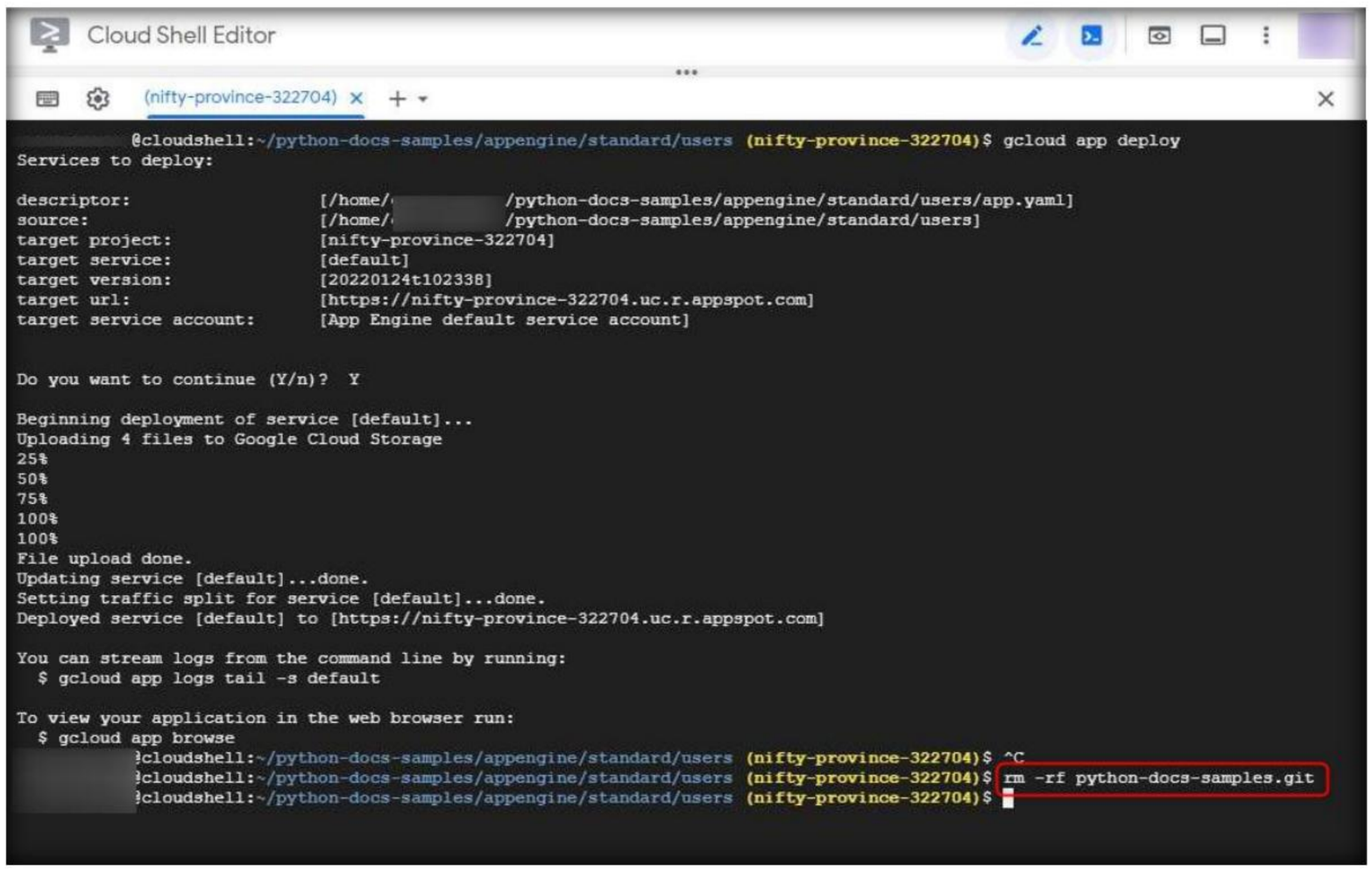


FIGURE 3.4.55: Deleting Cloned Repository

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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.

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Data Security in Cloud

hide01.ir

Module 04

Caution: Completing the steps in this exercise will require you to sign up for third party services that may incur fees. Be sure to follow proper guidelines for removing billable services from your account before you leave your lab. Deviating from our specific instructions may result in unwanted fees for services from third-party service providers. Be sure to check with your school, instructor, or employer if education accounts are available. If you sign-up and provide your credit card, you will be responsible for any fees related to services you activate. We strongly advise you not to deviate from our explicit instructions while connected to the platforms unless you are fully aware of what the services are and what the respective third-party charges for their use.

hidefi.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 1

Restricting access to S3 Bucket Object Using CloudFront

AWS CloudFront is the fastest content delivery network that securely delivers content over a network.

Lab Scenario

AWS CloudFront is the fastest content delivery network that securely delivers content over a network. AWS CloudFront has an option to restrict a direct access to content, which adds an extra layer of security. With this restriction on a direct access to content, only specific users can access the data in an Amazon S3 bucket. To protect an Amazon S3 bucket, you can use the origin access identity (OAI) feature of CloudFront. By setting up OAI, a cloud security professional can restrict access to S3 data and deny direct access to S3 objects if a user uses an S3 URL directly.

ICON KEY

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

Lab Objectives

This lab will demonstrate how to restrict access to S3 content using CloudFront.

In this lab, you will learn to do the following:

- Create a new AWS S3 bucket
- Create objects inside the S3 bucket
- Create a distribution inside the CloudFront
- Configure OAI

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Environment

To perform this lab, you need the following:

- **Admin Machine** VM
- **Administrative** privileges to run the tools

Lab Duration

Time: 10 minutes

Overview of AWS CloudFront

Cloud Front is the fastest content delivery service that can deliver data at high speeds and securely without any data loss. Network and application layer DDoS attacks can be prevented as it offers field-level encryption and HTTPS support. Amazon CloudFront can be integrated with AWS Shield, AWS WAF and Route 53 to protect against most web attacks. Amazon CloudFront can work with Amazon EC2, Amazon S3, and elastic load balancing to deliver a seamless experience. It can highly available services to the users at a faster speed; thus, the availability of the CIA Triad can be ensured with CloudFront. CloudFront can be integrated with AWS Shield Advanced and AWS WAF to add extra layers of defense against most CVEs. The content can be delivered securely over the Internet using the following CloudFront options:

- **Signed URLs or cookies**: To serve the content to specific CloudFront users with signed URLs or cookies
- **OAI for Amazon S3 buckets**: The origin access identity (OAI) feature of Amazon CloudFront can be used to secure Amazon S3 content.
- **Application load balancer**: Secure access to the application load balancer with elastic load balancing as an origin is possible with CloudFront.
- **AWS WAF web ACLs**: Access to content can be restricted by creating a web access control list using a web application firewall. CloudFront delivers the content based on a specified web ACL condition.
- **Geo restriction**: CloudFront can also be configured to serve the content to users from a specific location.

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., AWS), the application interface may be updated with time. Hence, in case you happen to work on an updated version of AWS, 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 an AWS Free Tier account using the following link: https://aws.amazon.com/free/, in case you have already not

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

created it for the previous module. Once the registration is complete, perform the following task:

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

TASK 1

Create a New Amazon S3 Bucket

1. If you are already logged into the AWS Web Console, click on **Services**. In the **Search** field, type **KMS**, and then click on **Key Management Service** from the search result.
2. If you are not logged in, first log in to the **Admin Machine** VM with the user **Admin** and password **admin@123**.

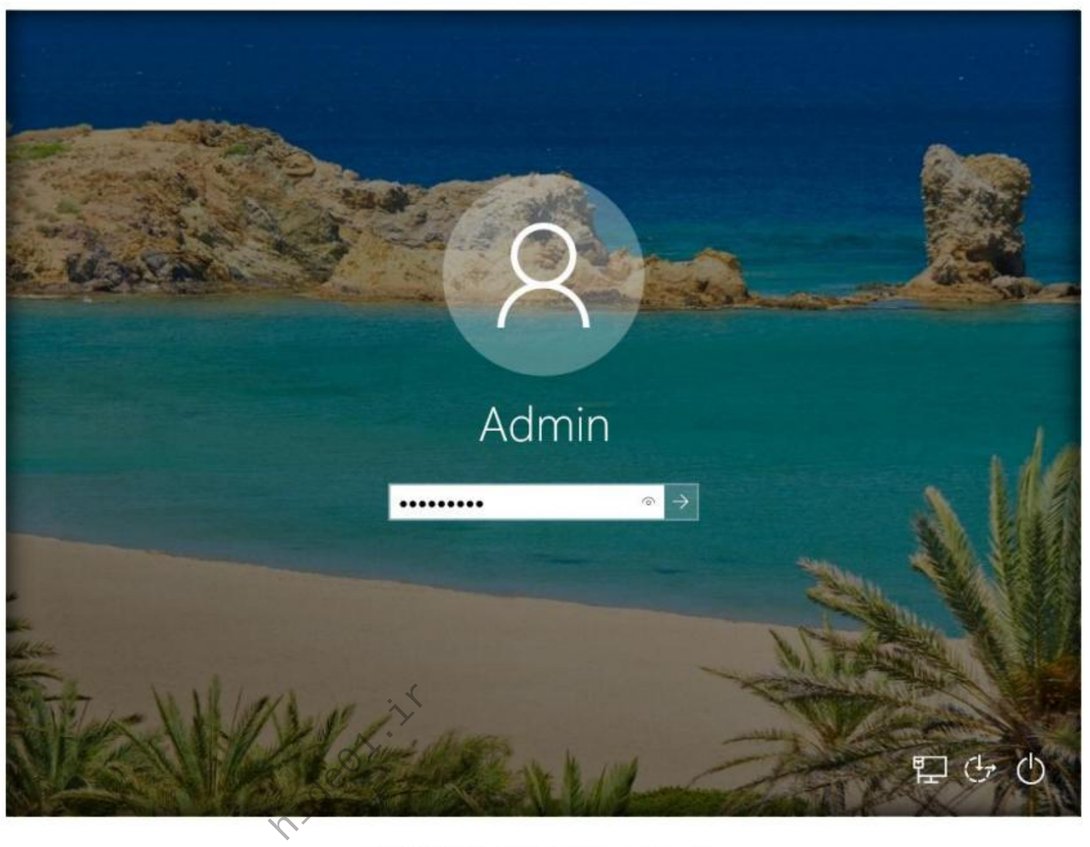


FIGURE 4.1.1: User Login

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



FIGURE 4.1.2: Navigating to the Chrome Browser from Taskbar

4. The **Google Chrome** browser opens. Go to the address bar, type **https://aws.amazon.com/**, and press **Enter.**

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

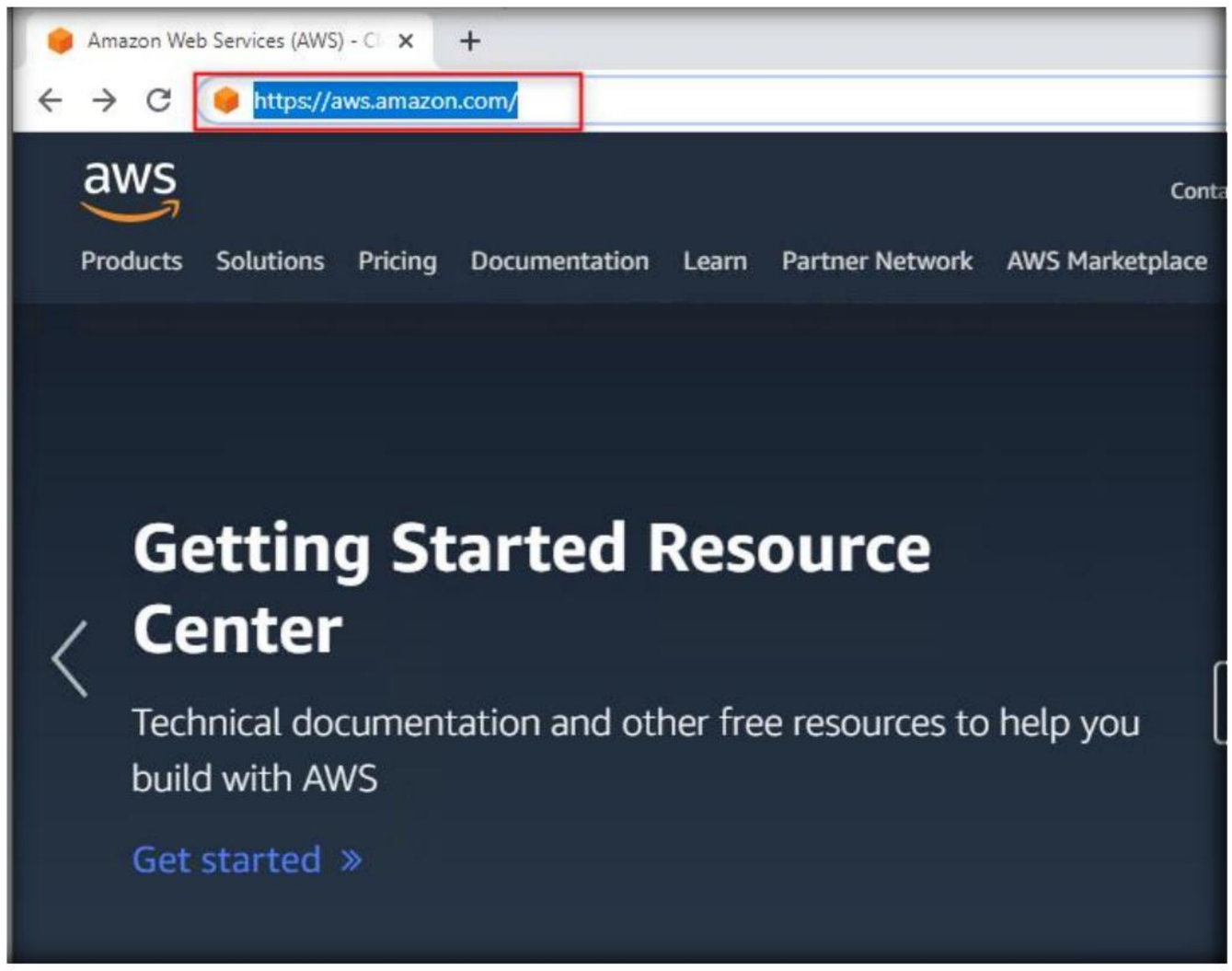


FIGURE 4.1.3: Access AWS in Browser

Note: If you are already logged in, skip the login steps.

5. The **AWS Web Services - Cloud Computing Services** page appears. Click on the **AWS Management Console** from the **My Account** dropdown, as shown in the screenshot below.

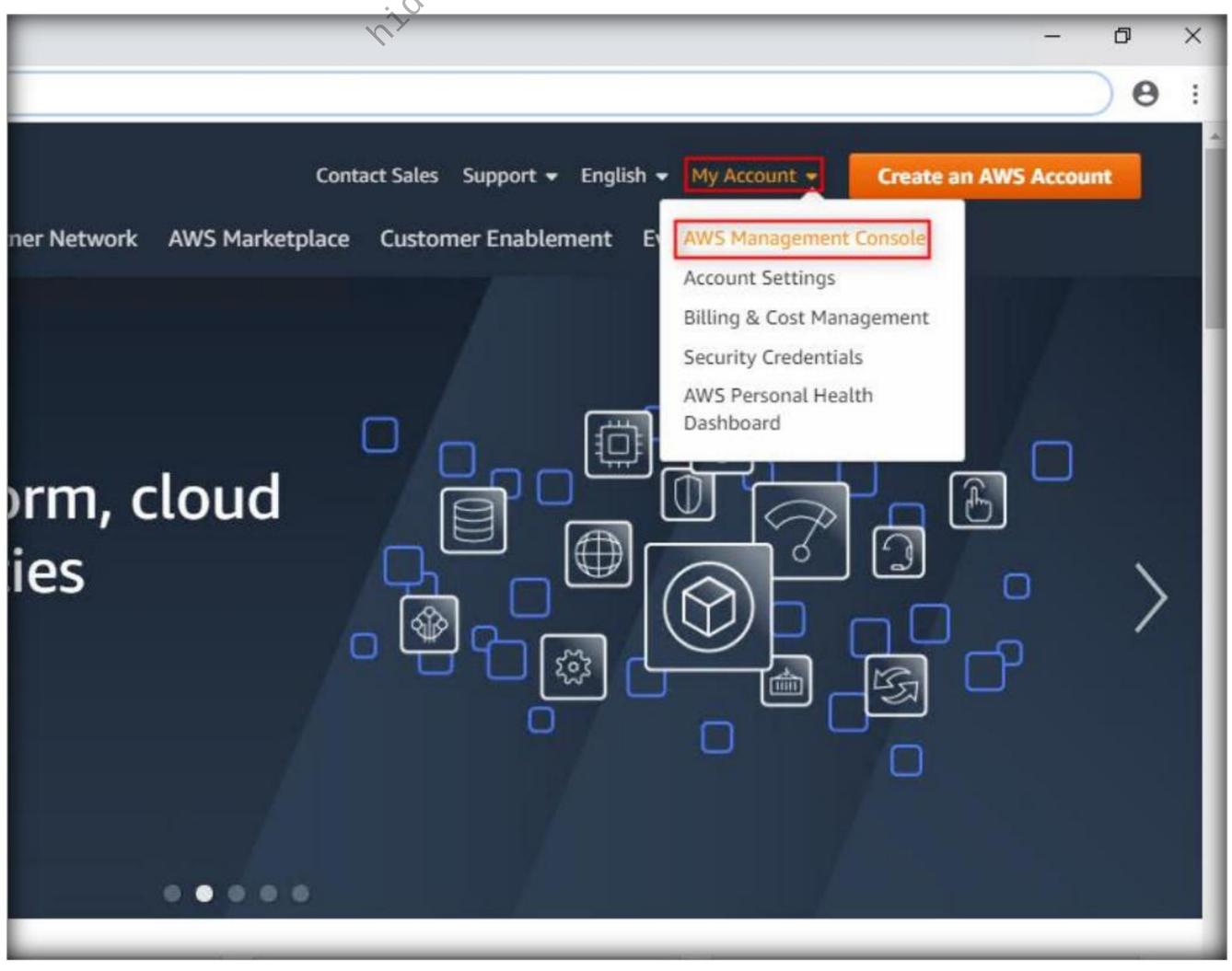


FIGURE 4.1.4: Navigate to AWS Management Console

6. The **AWS Sign-in** page appears. Choose **Root user** and type the AWS administrator account ID (**Root user email address**), as shown in the screenshot below. Then, click on **Next**.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

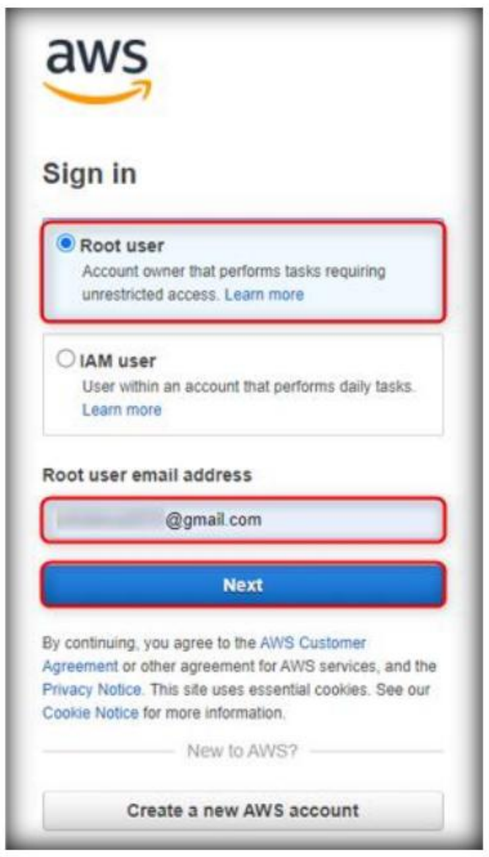


FIGURE 4.1.5: Login Credentials

7. In the security check page that appears, type the characters shown in the image and click **Submit**.



FIGURE 4.1.6: Sign-in to AWS

8. In the **Password** field, type the password, and then click on **Sign-in**, as shown in the screenshot below.

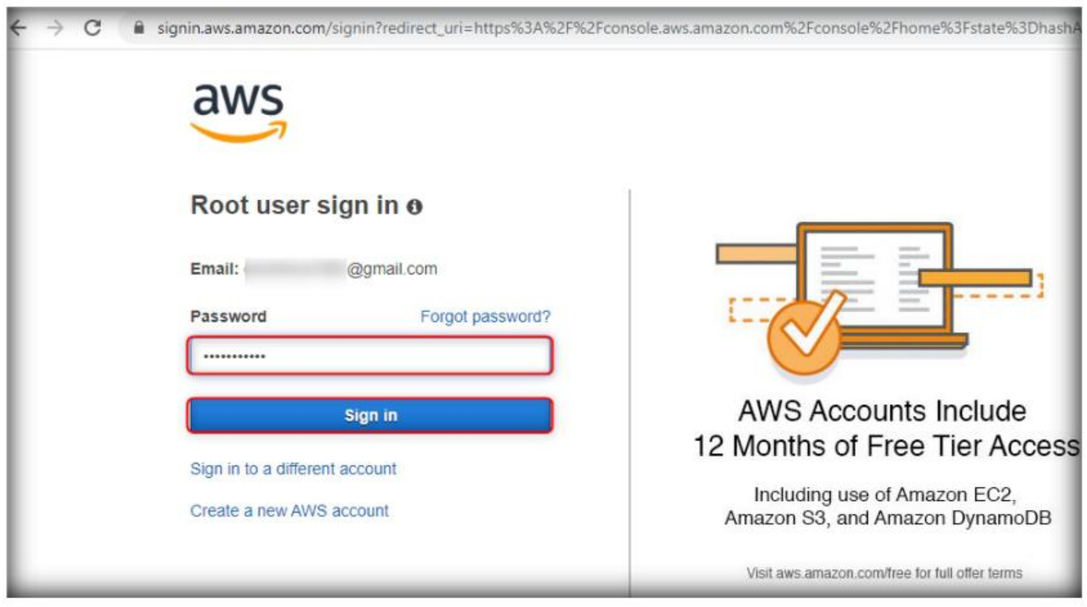


FIGURE 4.1.7: Sign-in to AWS

9. Now, to create an AWS S3 bucket, click on **Services** from the menu bar in the **AWS Management Console** and choose **S3** under **Storage**.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

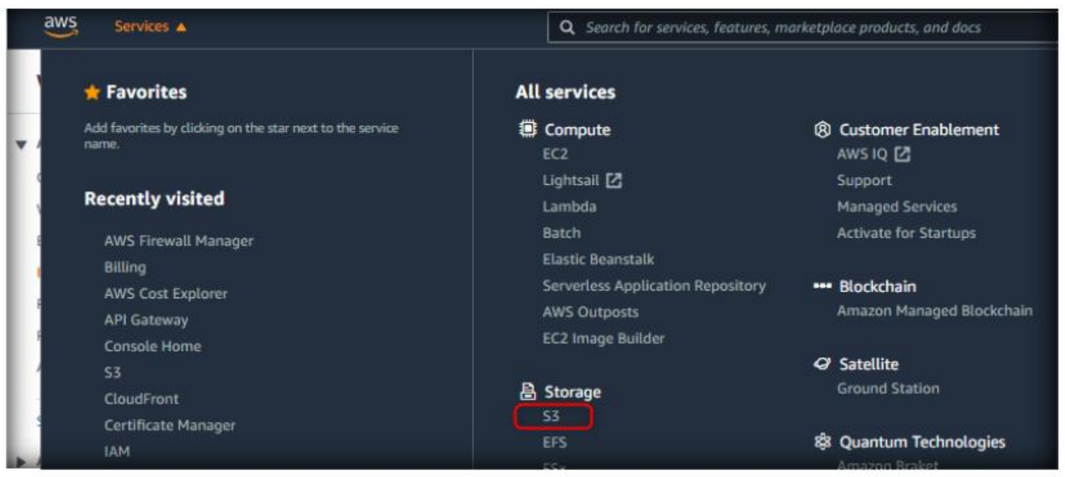


FIGURE 4.1.8: Select S3

10. The **Amazon S3** window appears. Click on **Create bucket** in the **Buckets** section.



FIGURE 4.1.9: Selecting Create bucket

11. The **General Configuration** section appears now. Under **Bucket name**, type a name of your choice (**departmentinfo** in this case) and choose an appropriate **AWS Region** (**Asia Pacific (Mumbai) ap-south-1** in this case).

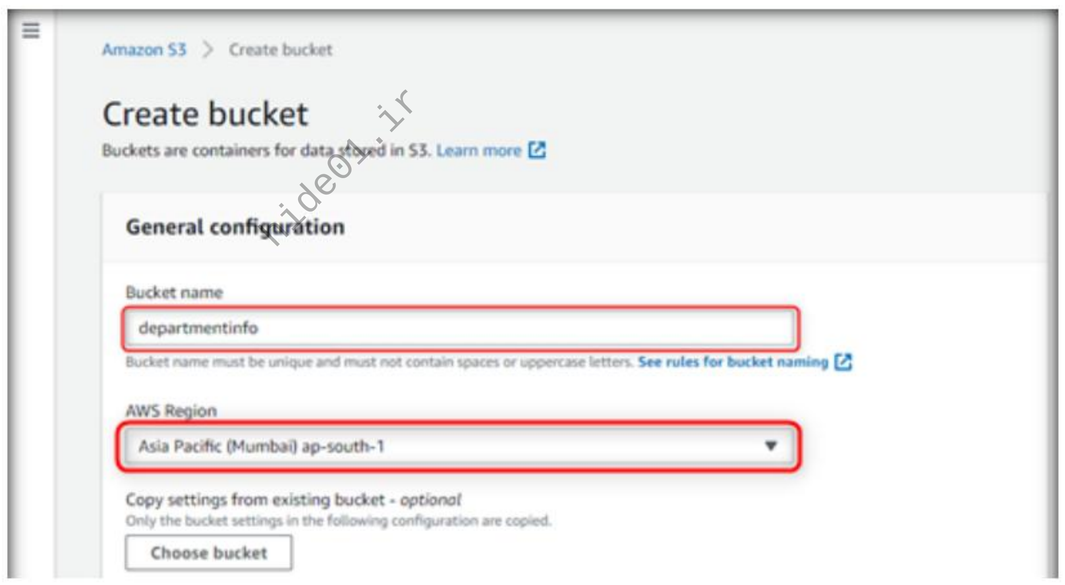


FIGURE 4.1.10: Bucket Configuration

12. Retain the other default settings. Scroll down to the bottom and click on **Create bucket.**

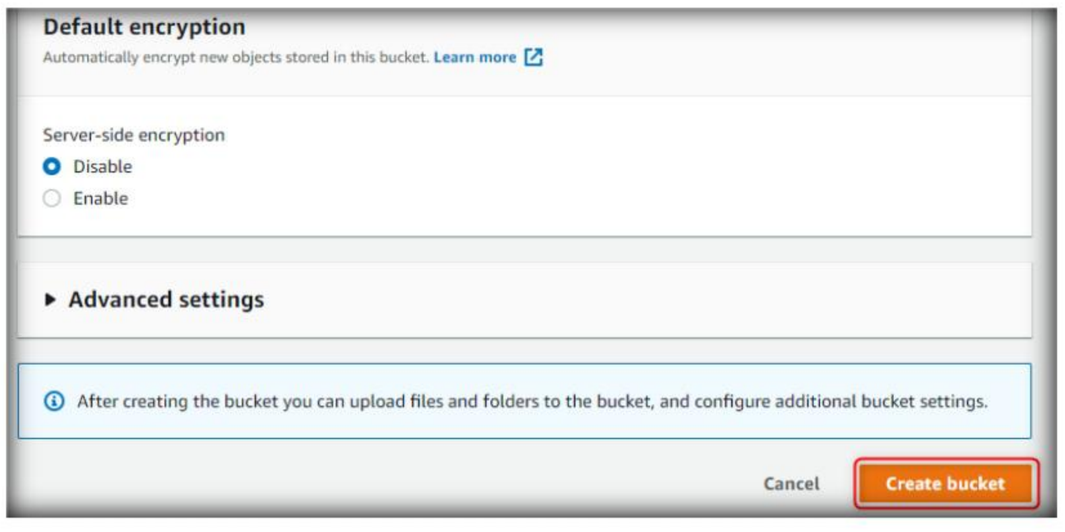


FIGURE 4.1.11: Creating the bucket.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 2

Creating Objects inside the S3 bucket

13. The **departmentinfo** bucket is created now. Next, to create an object inside the S3 bucket, click on the **departmentinfo** bucket.

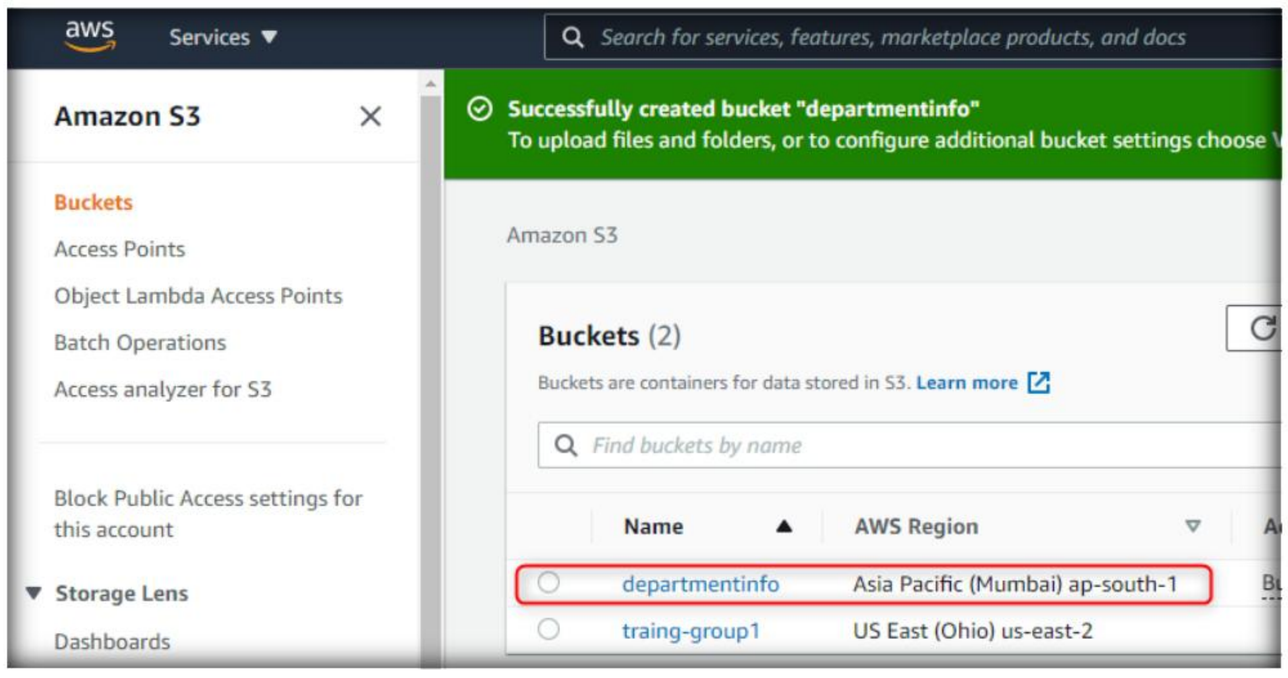


FIGURE 4.1.12: Clicking on the Bucket

14. On the **departmentinfo** bucket page, click on the **Upload** button under **Objects** to upload an **index.html** file.

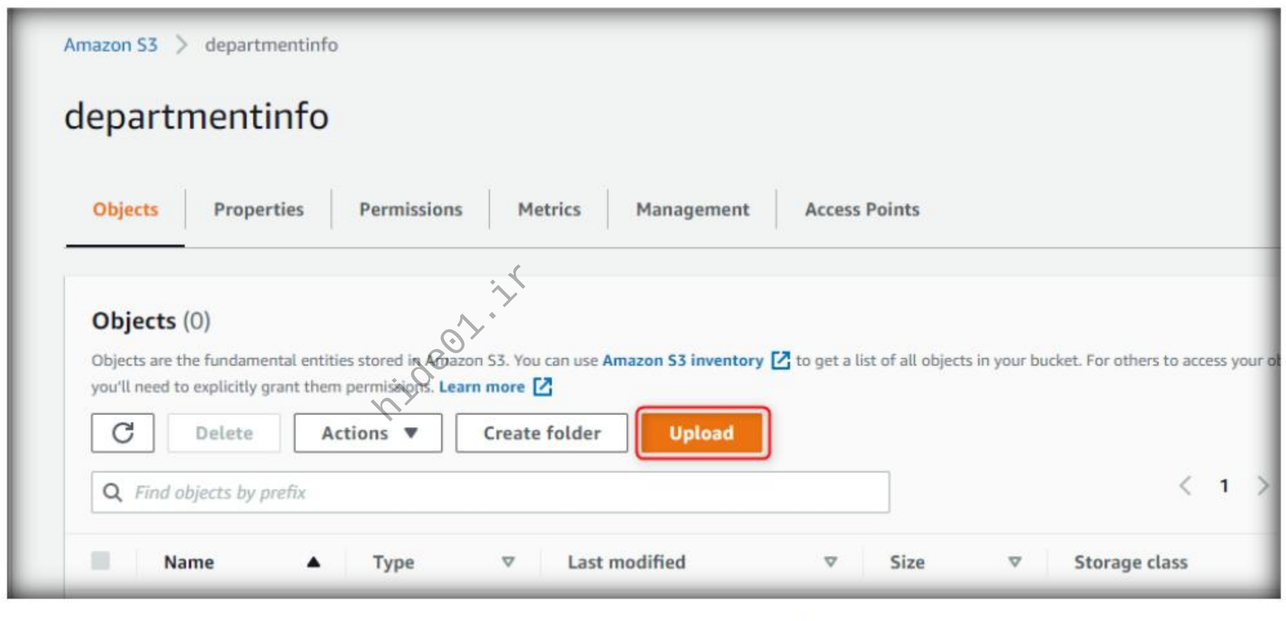


FIGURE 4.1.13: Clicking on Upload

15. When the **Upload** section opens, click on **Add files**.

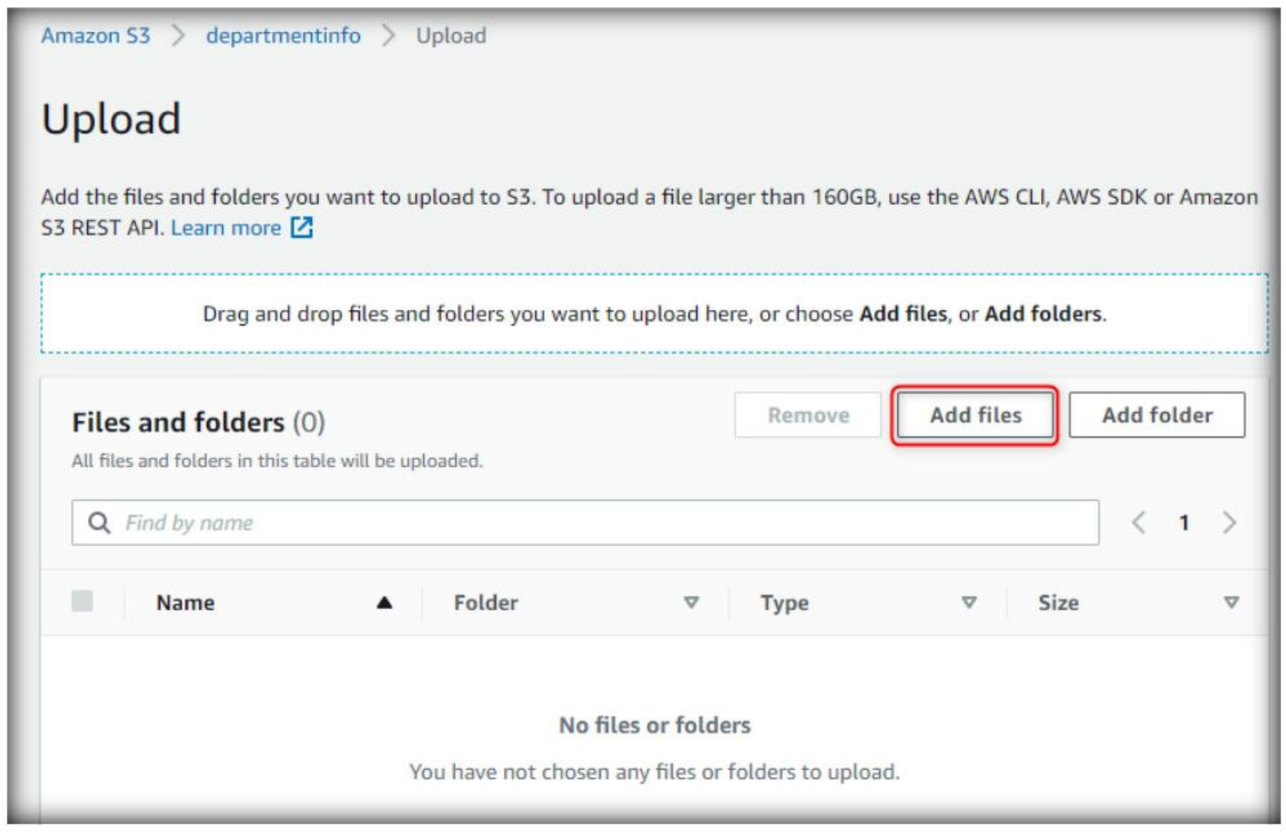


FIGURE 4.1.14: Clicking on Add files

Certified Cloud Security Engineer Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

16. Create an html file (index) and store it on your system. Once the **Open** window appears, navigate to the path where you stored the file on the system**.** Now, select the **index** file and click on **Open**.

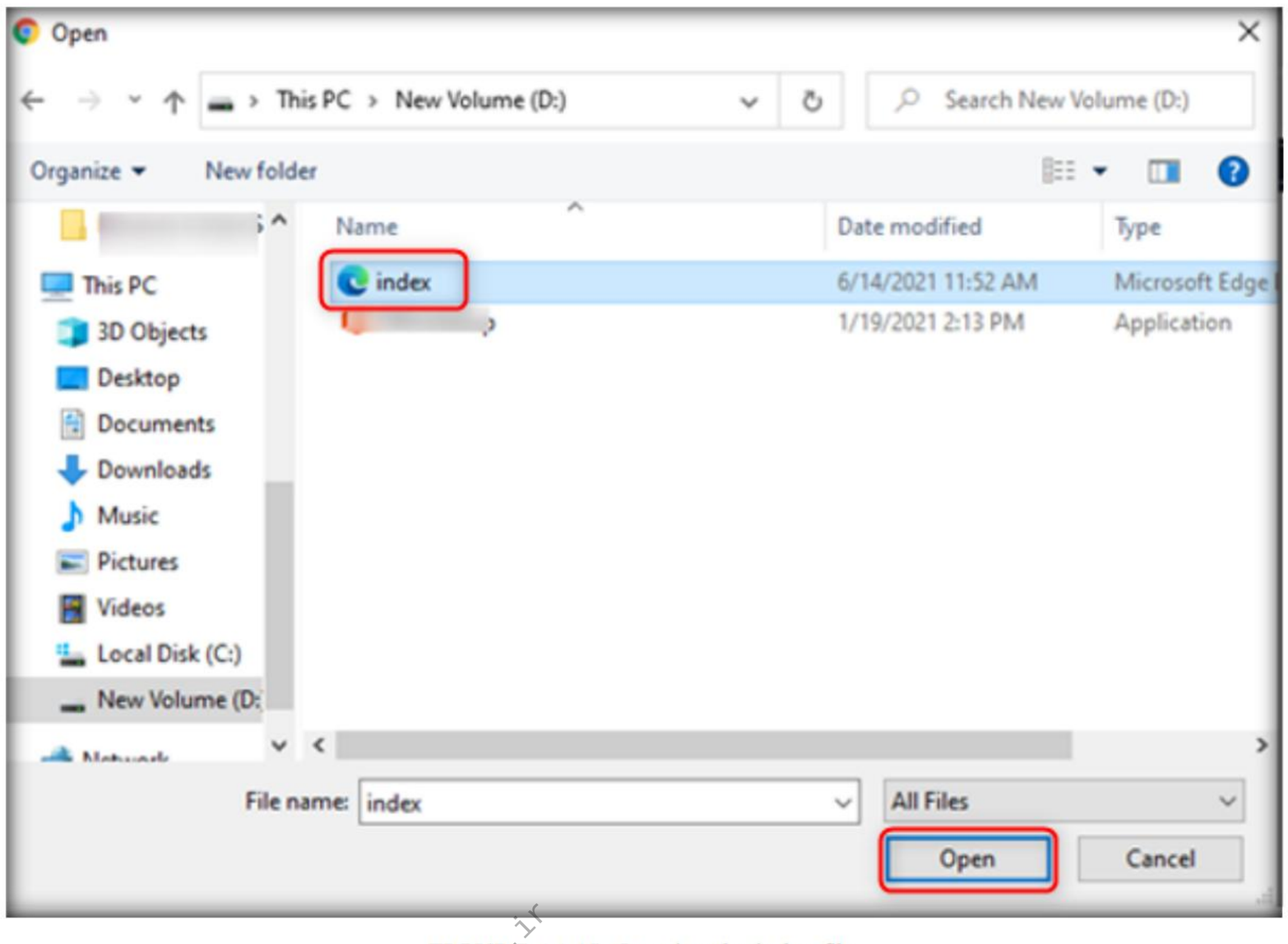


FIGURE 4.1.15: Opening the index file

17. When the file is ready to upload, scroll down and click **Upload**.

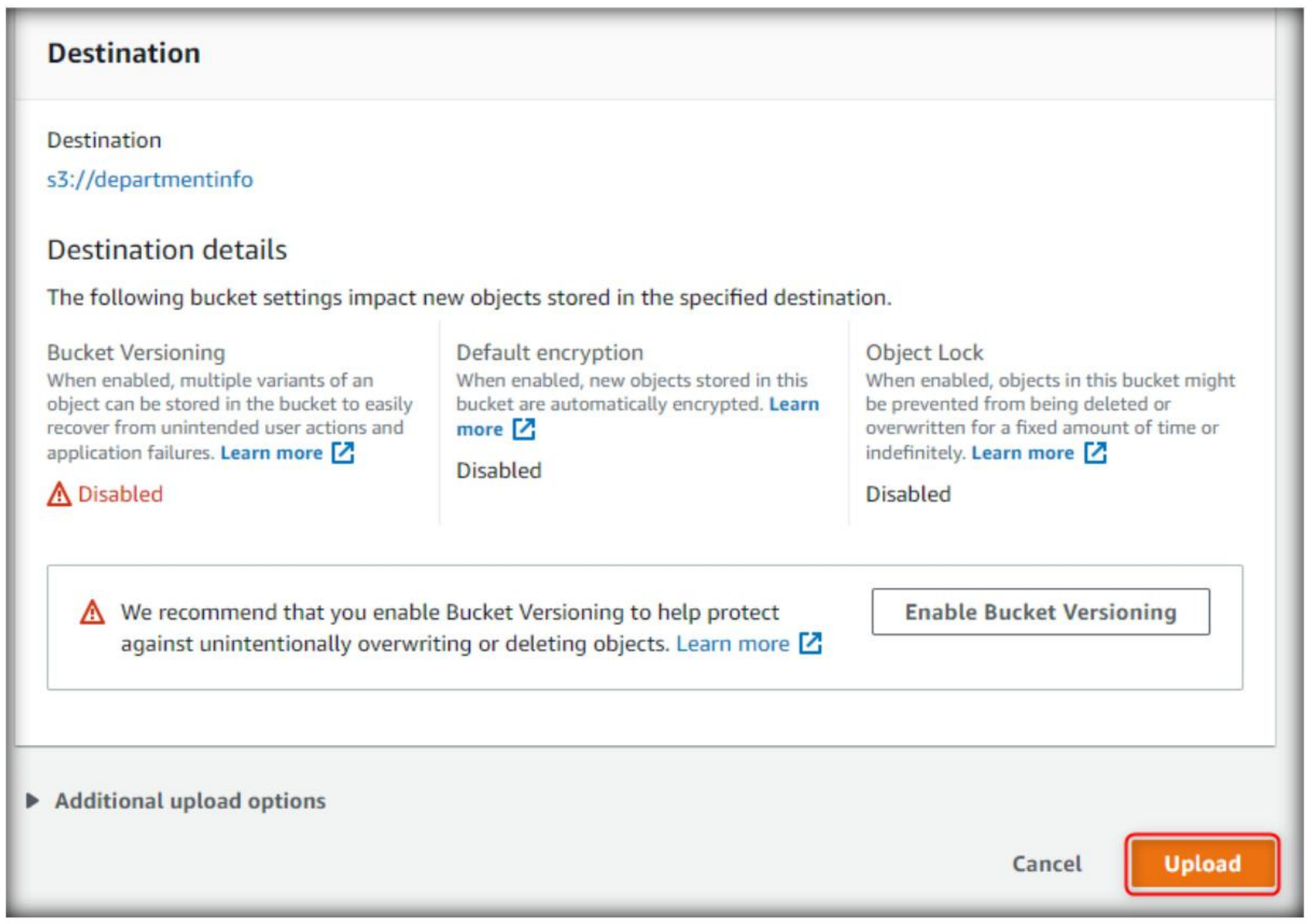


FIGURE 4.1.16: Uploading the file

Certified Cloud Security Engineer Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

18. Once the file is uploaded, click on **index.html** to see its details.

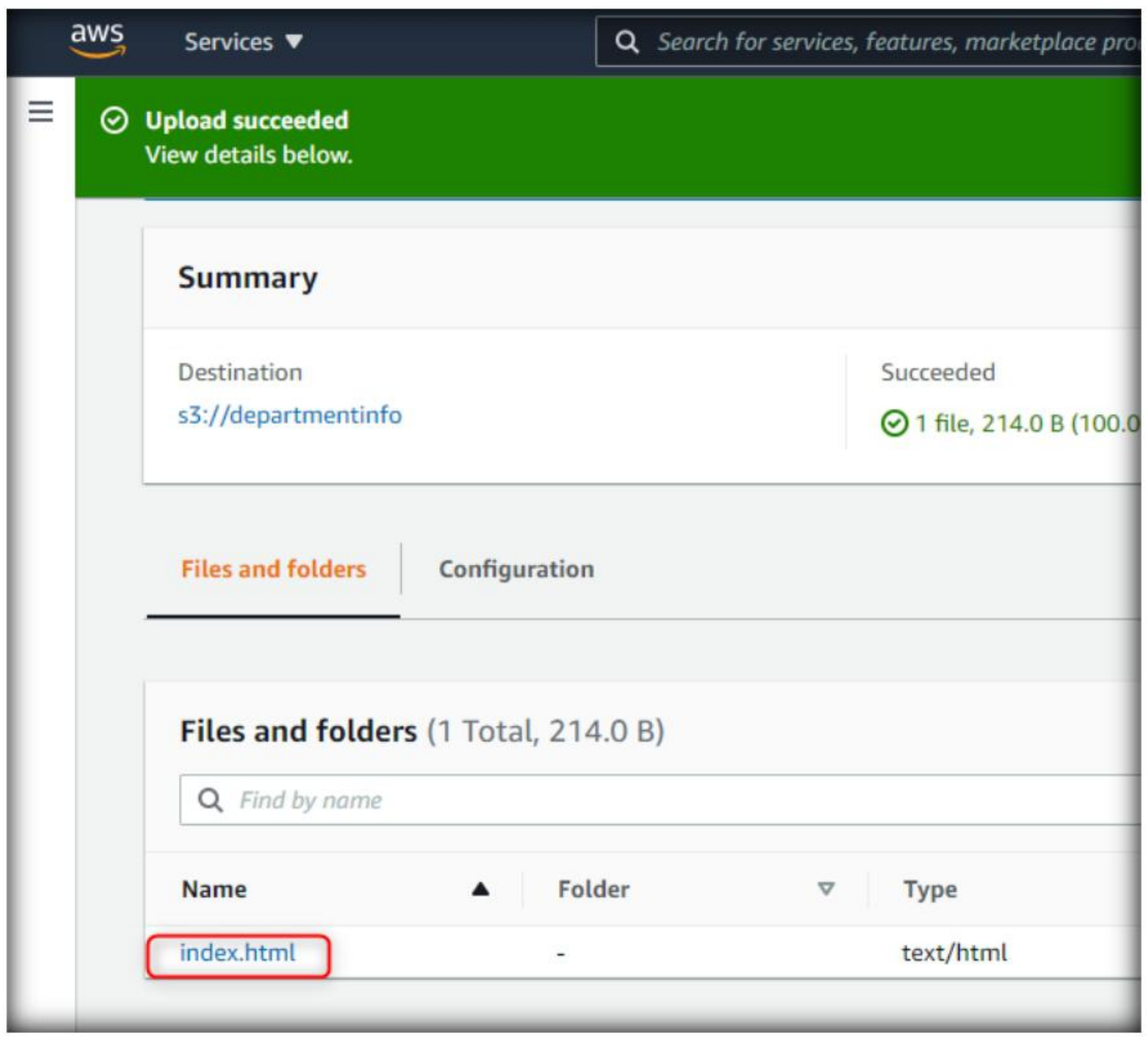


FIGURE 4.1.17: Clicking on the file

19. Under **Object overview**, copy the **Object URL** and paste it into a new browser tab to access the file.

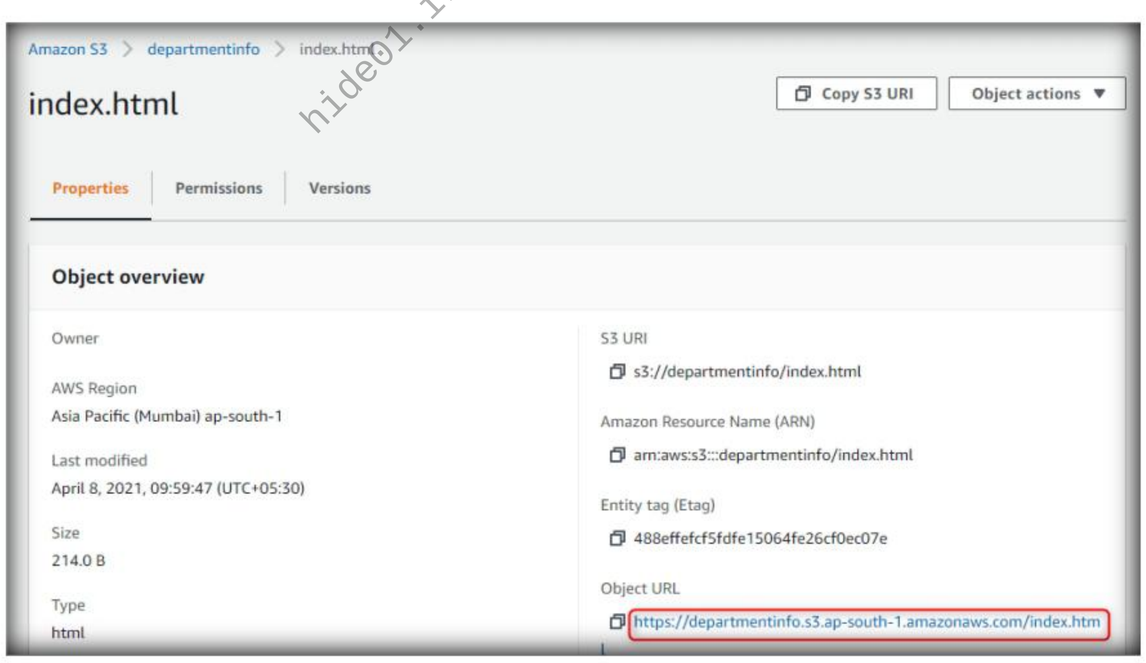


FIGURE 4.1.18: Copying the Object URL

20. You cannot access the file because you do not have a public access for it.

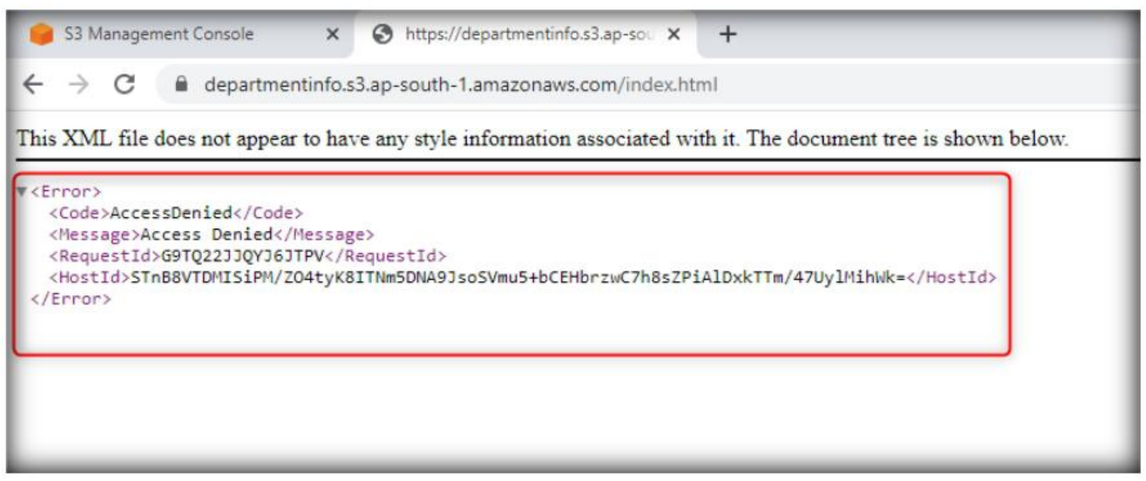


FIGURE 4.1.19: Pasting the link in the new window

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 3

Creating CloudFront Distribution with OAI configured

21. Next, allow specific users with the CloudFront-generated URL address to access the index.html page so that they can access the page only through CloudFront.
22. Click on **Services** and select **CloudFront** under **Networking and Content Delivery**.

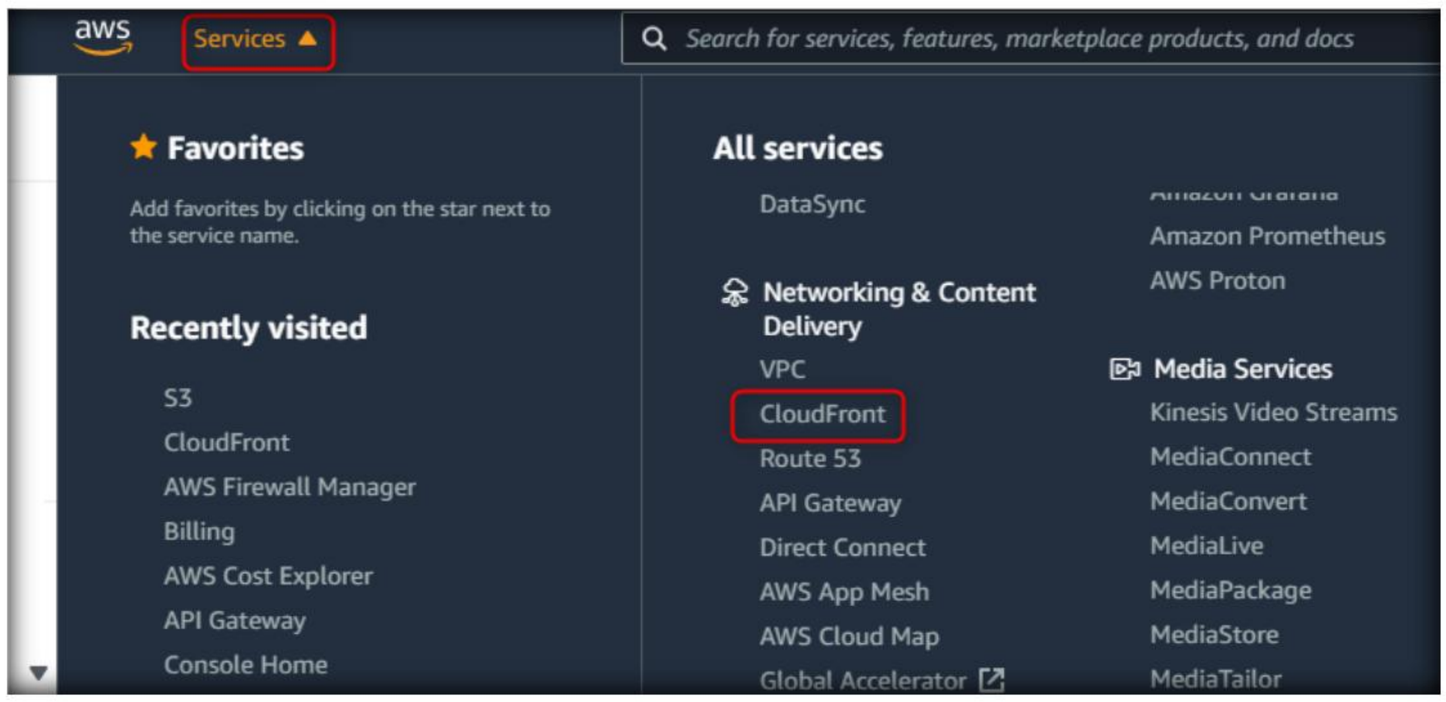


FIGURE 4.1.20: Selecting CloudFront

23. Once the **CloudFront** dashboard opens, click on **Create Distribution**. If you have created any distribution earlier, you will get the **Select a delivery method for your content** window directly.

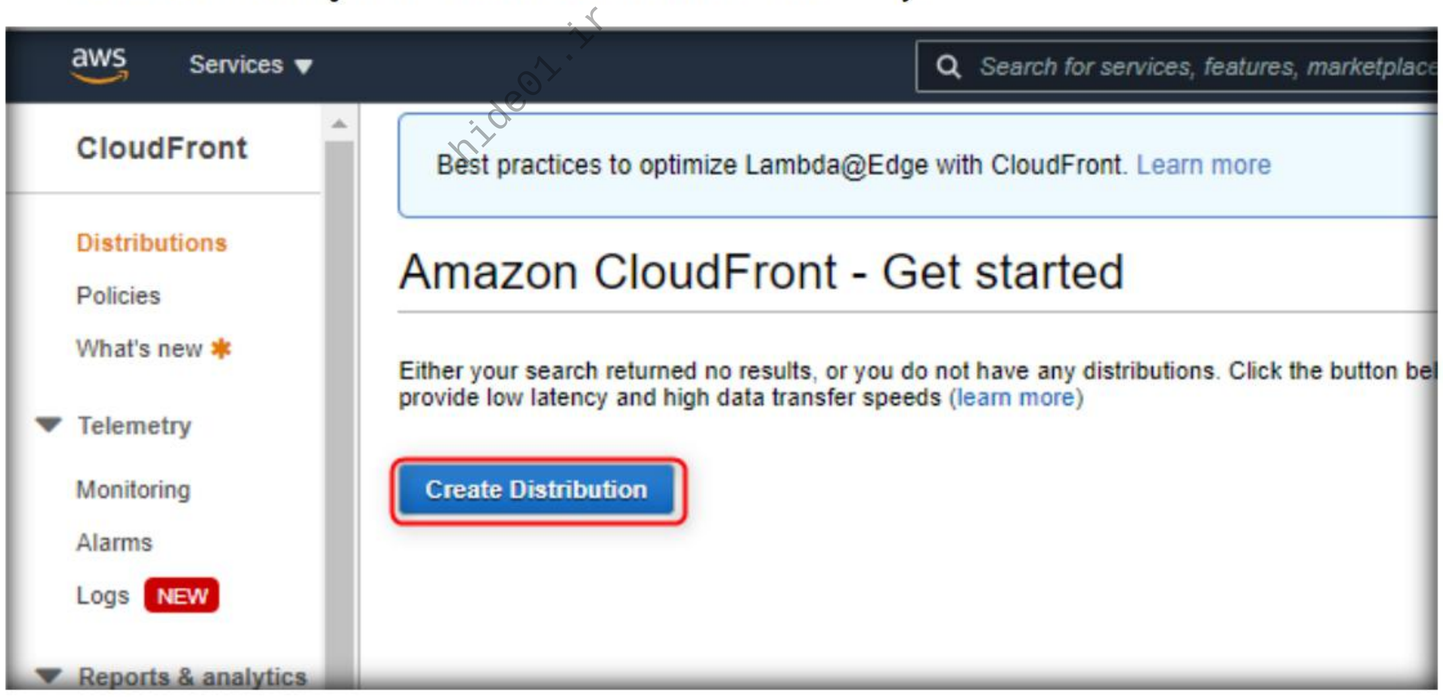


FIGURE 4.1.21: Selecting Create Distribution

24. Click **Get Started** to create the distribution.

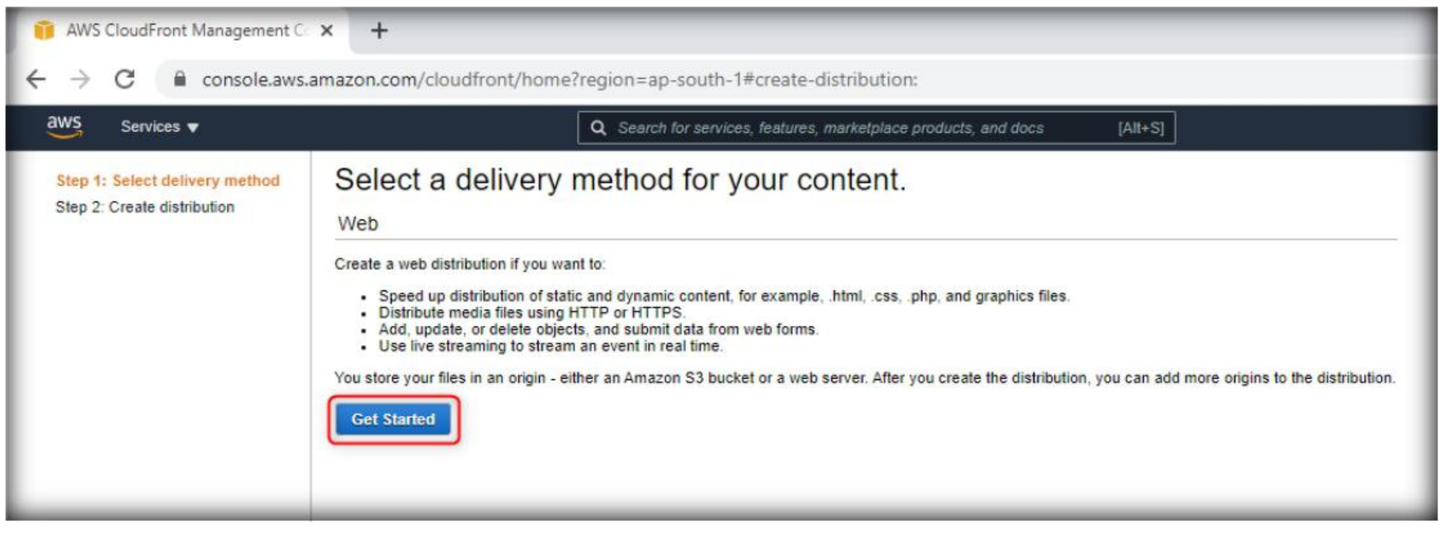


FIGURE 4.1.22: Selecting Get Started

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

25. Now, configure origin access identity (OAI) to setup access to the data. Under the **Origin Settings** on the **Create Distribution** page, select **Origin Domain Name** as **departmentinfo.s3.amazonaws.com**(name will change according to your S3 bucket name) and set the below options before scrolling to the next section:

    - Restrict Block Access**: Yes**
    - Origin Access Identity**: Create a New Identity**
    - Grant Read Permissions on Bucket**: Yes, Update Bucket Policy**

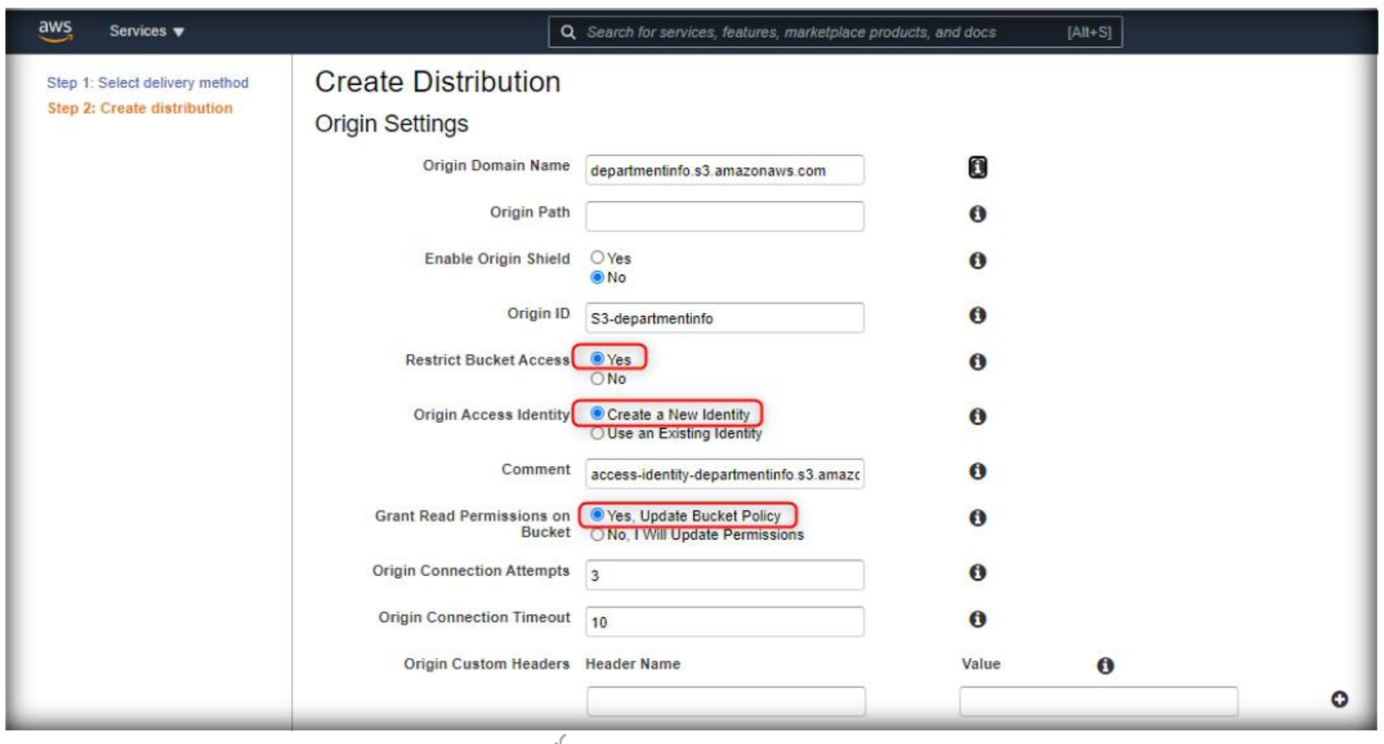


FIGURE 4.1.23: Configuring Origin Settings

26. Next, retain all other default settings and click on **Create Distribution**.

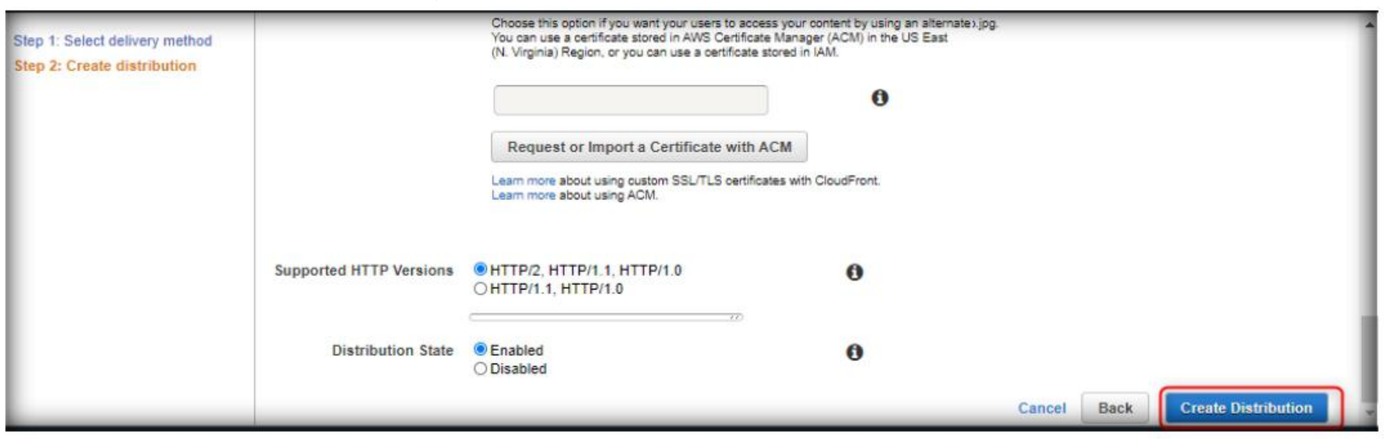


FIGURE 4.1.24: Configuring Origin Settings

27. On the next page, click on **Distributions** to the left side of the navigation pane.

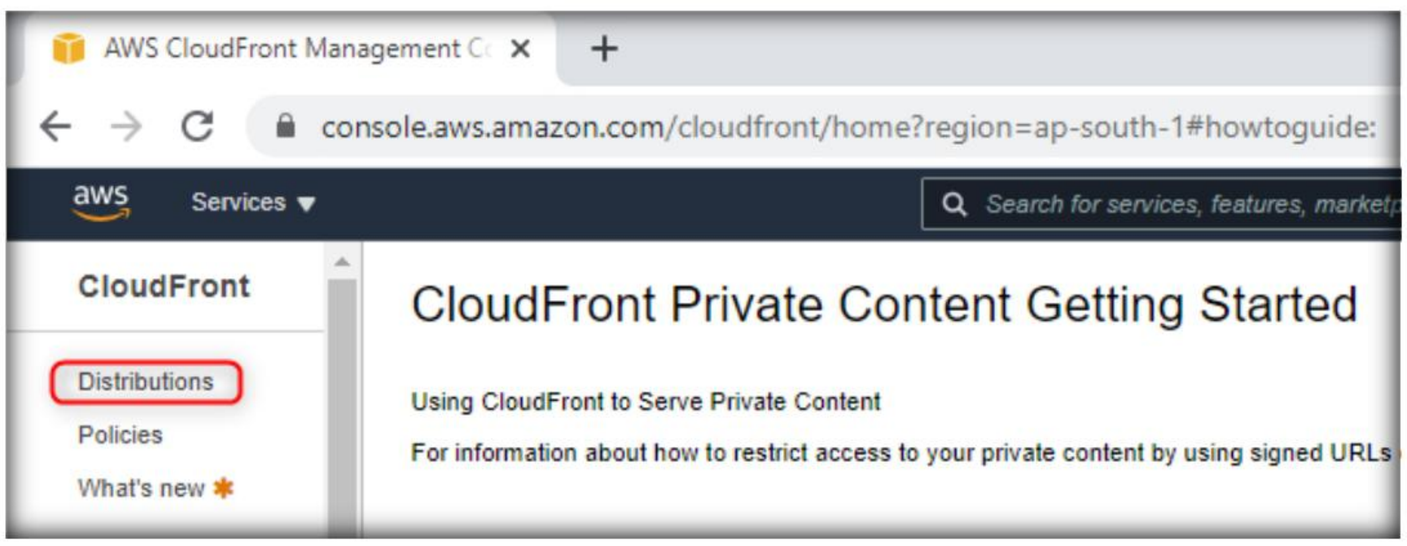


FIGURE 4.1.25: Choose Distribution

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

28. You can see the distribution is created and its status is **In Progress**. Wait for a few minutes to complete the deployment.

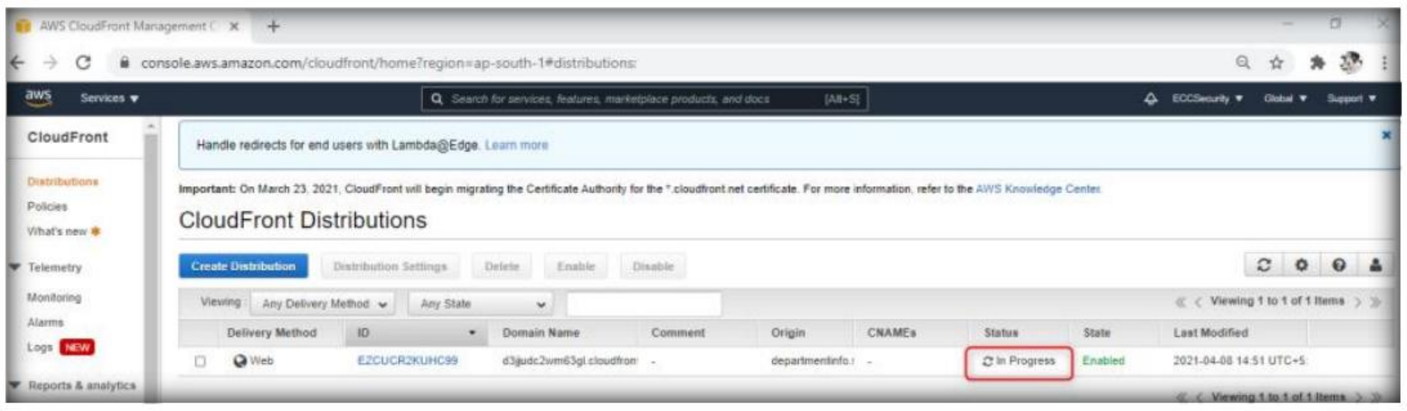


FIGURE 4.1.26: Distribution status

29. Click on the distribution **ID** to check the distribution details.

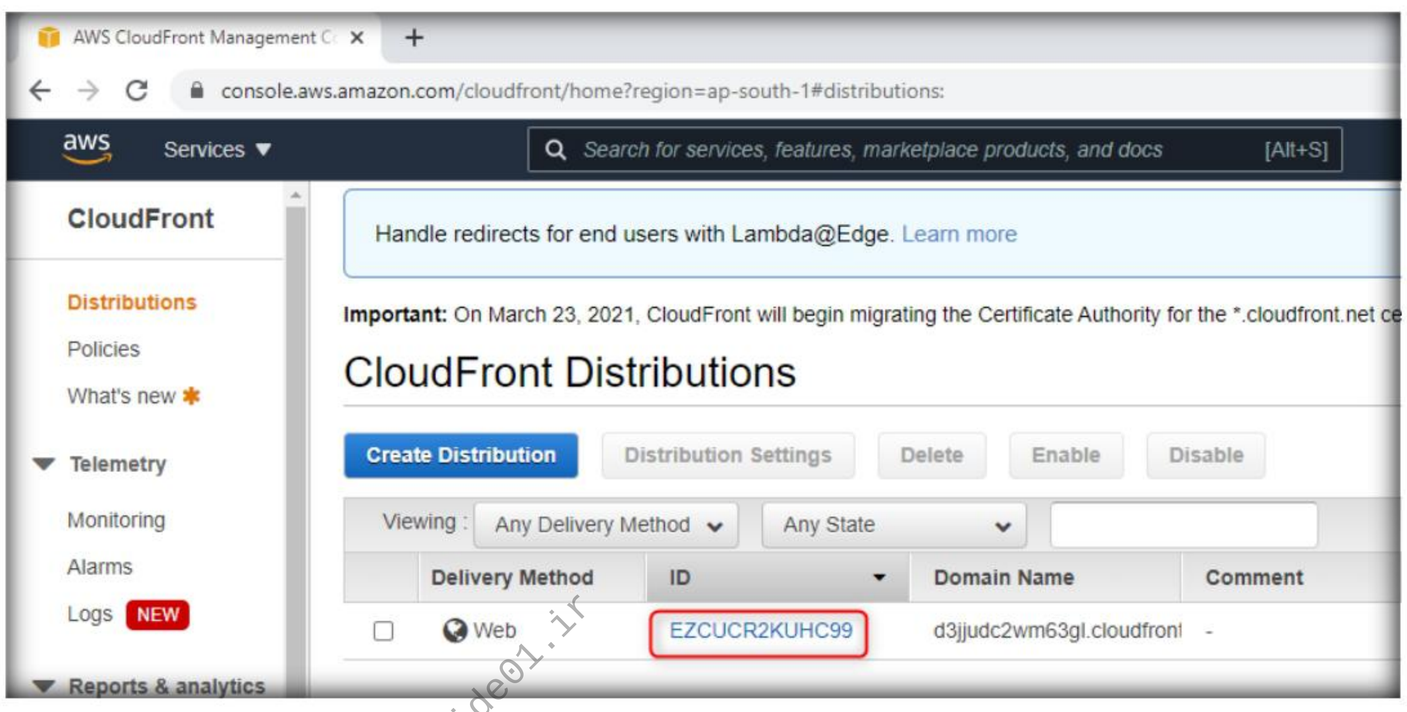


FIGURE 4.1.27: Clicking on the Distribution ID

30. Now, you can see the **Domain Name** of the created S3 bucket, which can be shared with the user to whom you wish to allow access to objects. Copy the domain name.

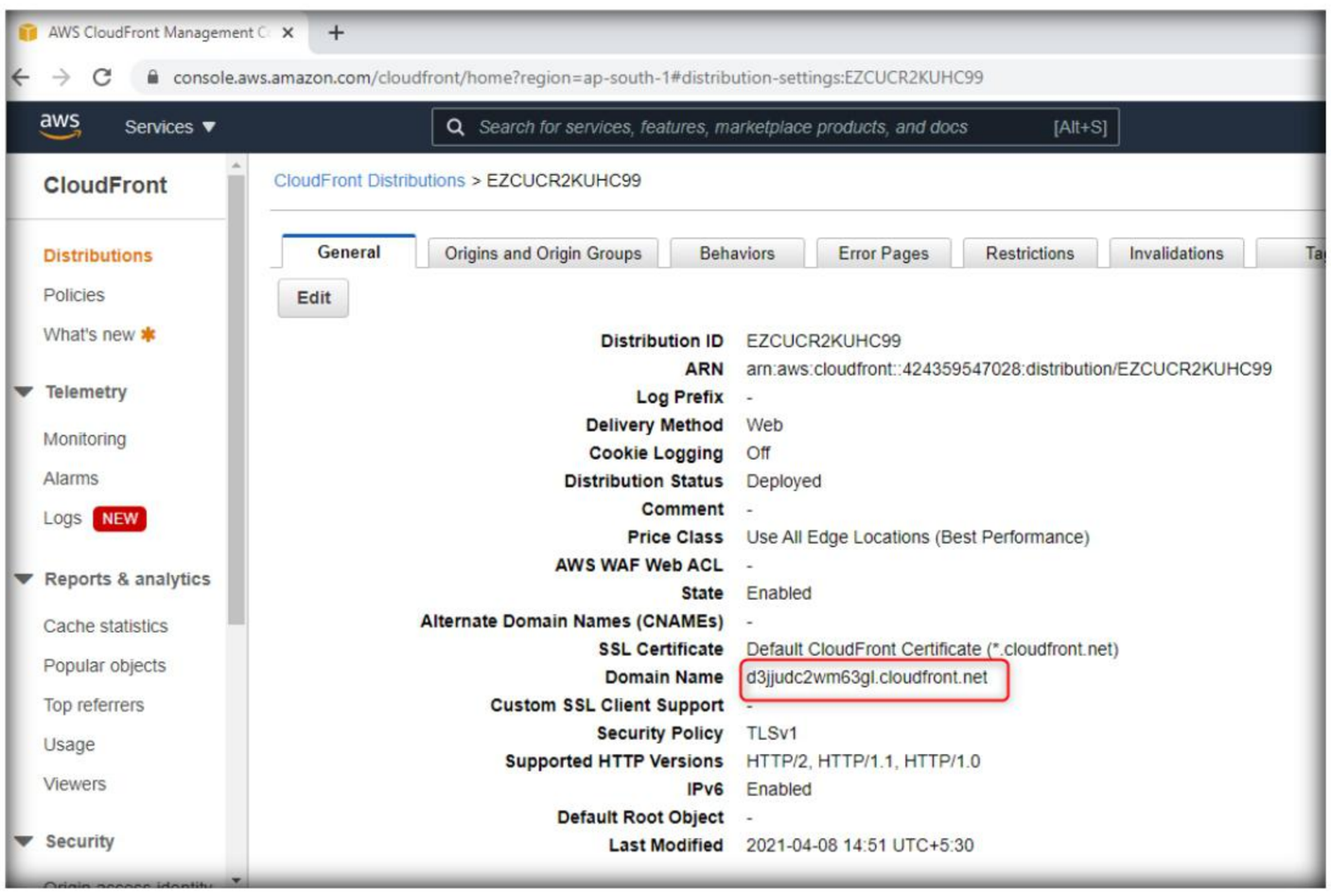


FIGURE 4.1.28: Copying Domain Name

guide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

31. Open a new browser tab and paste the copied URL (**d3jjudc2m63gl.cloudfront.net**), add **/index.html** to the copied URL **(d3jjudc2m63gl.cloudfront.net/index.html**), and then press **Enter**.

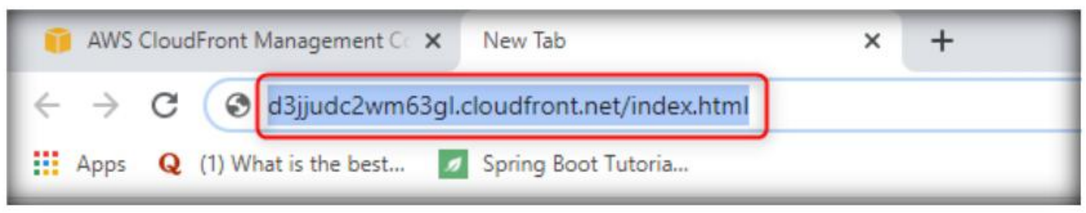


FIGURE 4.1.29: Pasting the copied URL with the file name

32. Now, you can see the content of the S3 object.



FIGURE 4.1.30: Accessing the file content

33. This way, a cloud security engineer can restrict access to S3 content and make the content available only to specific users using AWS CloudFront with OAI configuration.

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

34. Now, delete the instances created in this lab. Navigate to the **Distributions** under CloudFront and select the checkbox created in this lab. Click on the **Disable** button. In the pop-up window, click on **Disable** button.



FIGURE 4.1.31: Disable Distribution

35. Navigate to the **Buckets** under Amazon S3 and select the checkbox, for instance, created in this lab (here, **departmentinfo**). Click on the **Empty** button to empty the bucket before deleting. In the pop-up window, enter permanently delete and click on the **Empty** button.

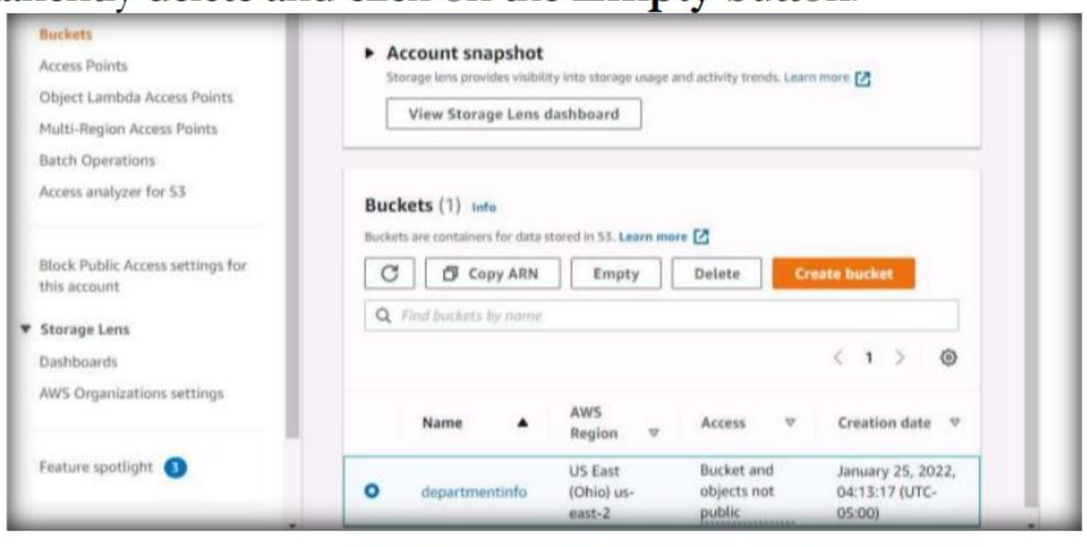


FIGURE 4.1.32: Empty the created Bucket

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

36. Navigate to the **Buckets** under Amazon S3 and select the checkbox for instance created in this lab (here, **departmentinfo**). Click on the **Delete** button. In the pop-up window, enter the bucket's name and click on the **Delete bucket** button.

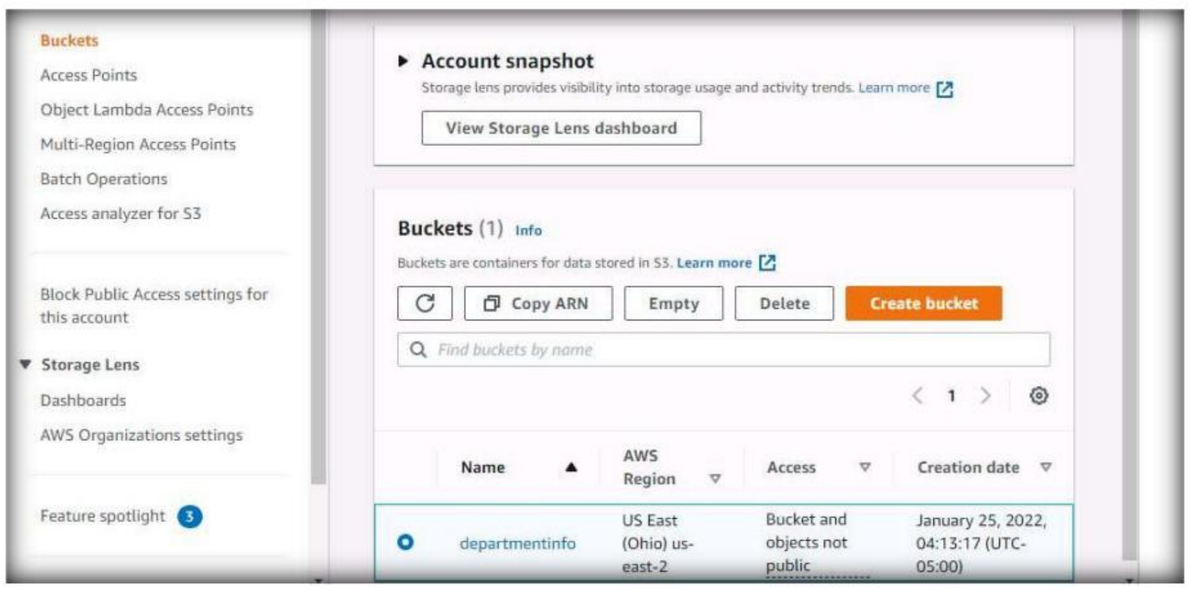


FIGURE 4.1.33: Deleting Bucket

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.

hide01.ir

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

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 2

Restricting Access to AWS S3 Buckets using ACL and Bucket Policy

AWS S3 buckets, when configured with certain bucket policies and ACLs, can restrict access to S3 resources only to the right entities.

Lab Scenario

ICON KEY

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

AWS S3 bucket is the secure storage service in AWS. Public access to an S3 bucket can be granted through access control lists (ACLs), bucket policies, etc. S3 ACL can be used to define the different access types for different AWS accounts or groups. With S3 bucket policies, the specific actions that a user can perform on the bucket can be configured. This lab demonstrates the configuration of ACLs and bucket policies for an S3 bucket.

Lab Objectives

This lab will demonstrate how to configure S3 resources by creating bucket policies and ACLs, to provide access to selected entities.

In this lab, you will learn to do the following:

- Assign permissions to Amazon S3 using an ACL
- Assign permissions to Amazon S3 using a bucket policy

Lab Environment

To perform this lab, you need the following:

- **Admin Machine** VM
- **Administrative** privileges to run the tools
- **Registered AWS account**

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Duration

Time: 10 minutes

Overview of AWS Storage

Amazon S3 allows the uploading and retrieval of data, anytime and anywhere on the Internet. It stores data as objects (text files/photos/videos) within buckets. In their default state, all Amazon S3 buckets can be accessed by authorized users. Access to S3 resources can be configured by combining bucket policies, ACLs, and IAM polices for giving access to the right entities.

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., AWS), the application interface may be updated with time. Hence, in case you happen to work on an updated version of AWS, 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 an AWS Free Tier account using the following link: https://aws.amazon.com/free/, in case you have already not created it for the previous module. Once the registration is complete, perform the following task:

hide01.ir

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

TASK 1

Assign Permissions to Amazon S3 Using Access Control Lists

1. Log in to the **Admin Machine** VM with the username **Admin** and password **admin@123**.

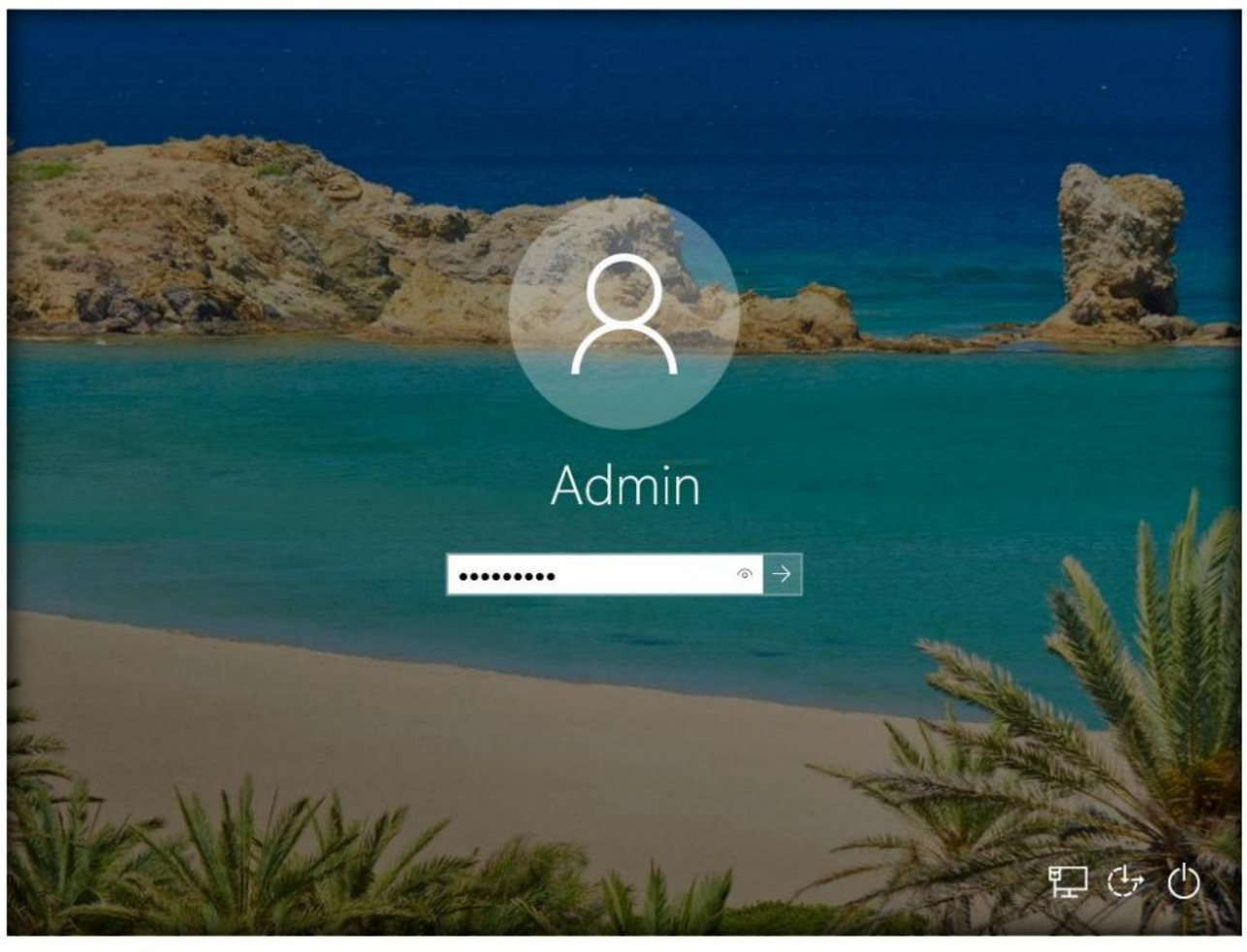


FIGURE 4.2.1: User Login

Certified Cloud Security Engineer Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

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



FIGURE 4.2.2: Navigating to the Chrome Browser from Taskbar

3. The **Google Chrome** browser appears. Go to the address bar, type **https://aws.amazon.com/**, and press **Enter.**

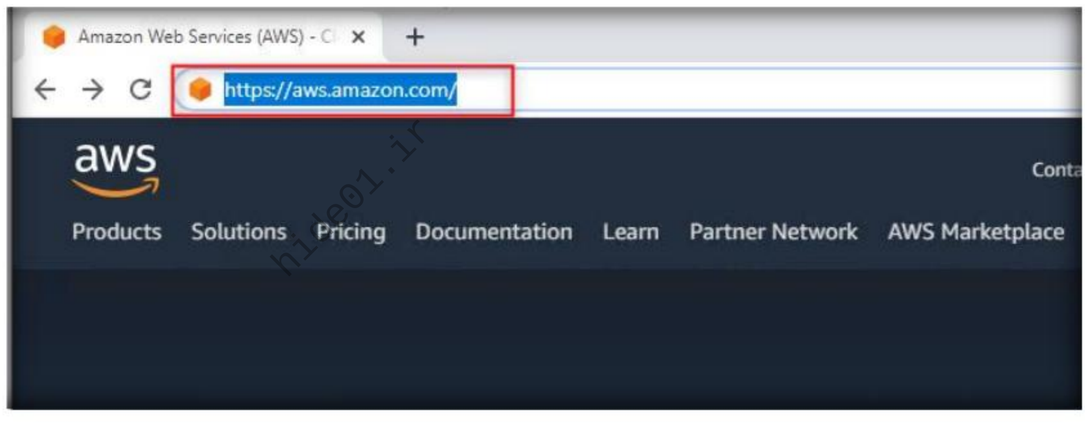


FIGURE 4.2.3: Access AWS in Browser

Note: If you are already logged in, skip the login steps.

4. The **AWS Web Services - Cloud Computing Services** page appears. Click on **AWS Management Console** from the **My Account** dropdown, as shown in the screenshot below.

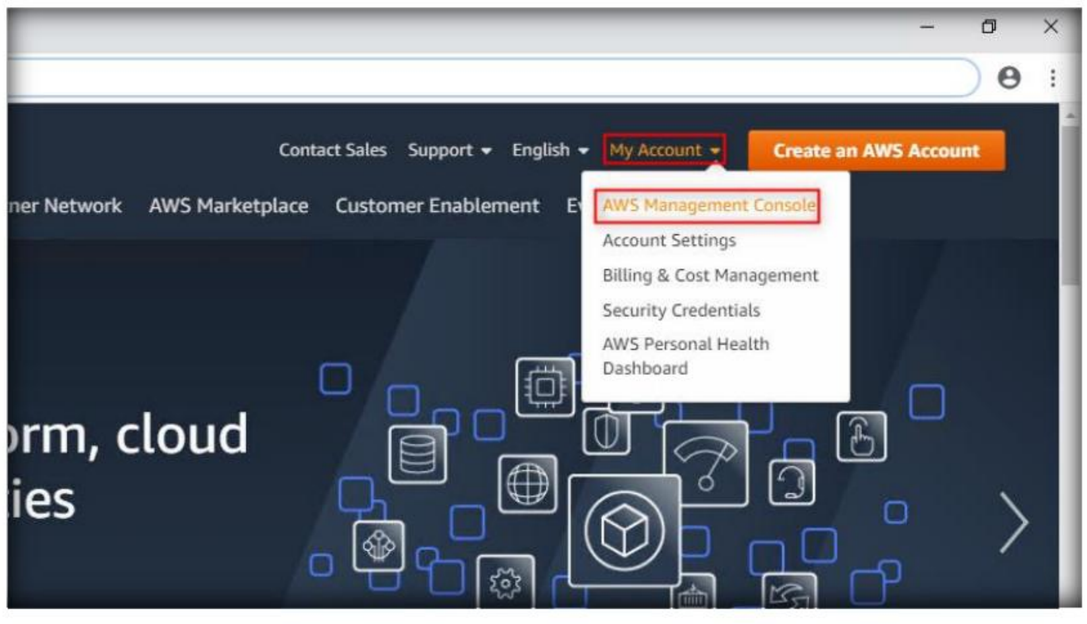


FIGURE 4.2.4: Navigate to AWS Management Console

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

5. The **AWS Web Services Sign-in** page appears. Type the AWS administrator account ID (Root user email address) and click on **Next**.

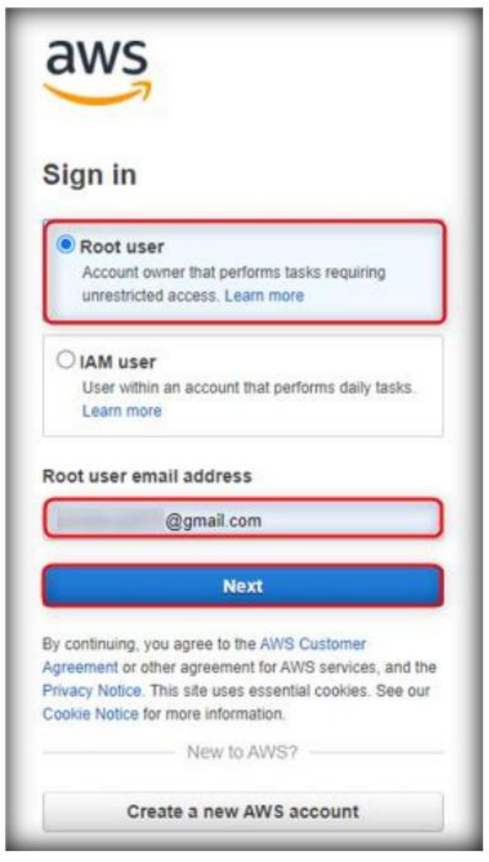


FIGURE 4.2.5: Sign-in to AWS

6. In the security check page that appears, type the characters shown in the image and click **Submit.**

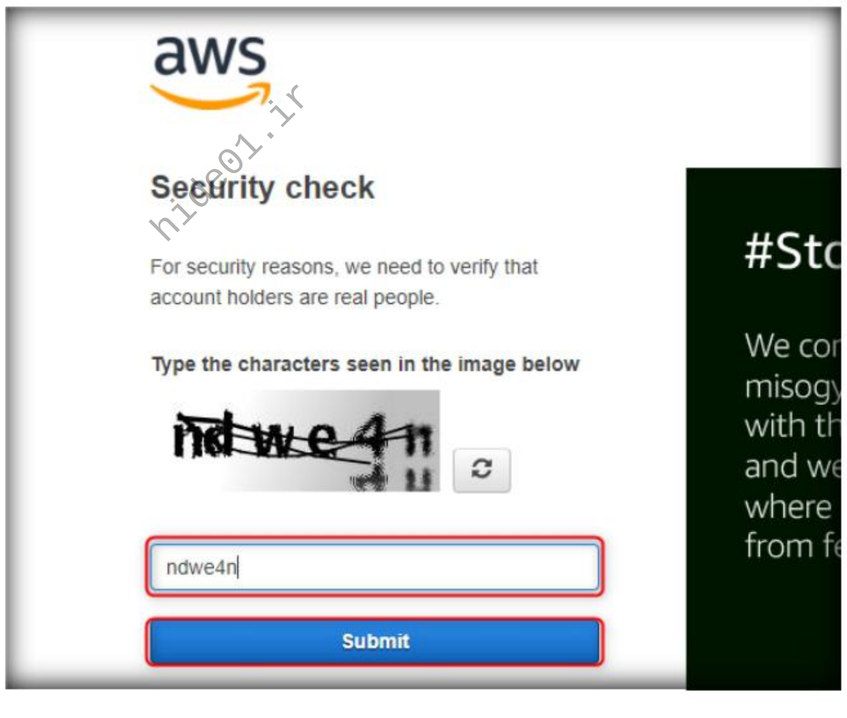


FIGURE 4.2.6: Sign-in to AWS

7. In the **Password** field, type the password and click on **Sign in**.

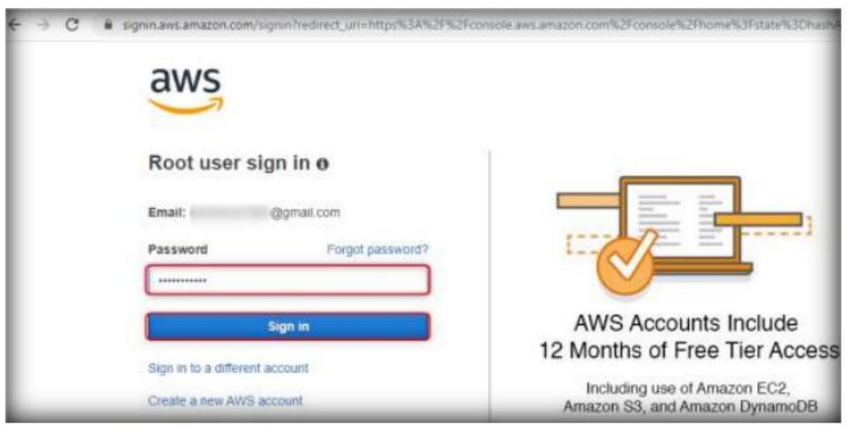


FIGURE 4.2.7: Sign-in to AWS

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

8. Now, to create an S3 bucket, click on **Services**. In the search field, type **S3**, and then click on **S3 Scalable Storage in the Cloud** from the search results.



FIGURE 4.2.8: Selecting S3 Service

9. Click on **Create bucket** in the **Amazon S3** window.

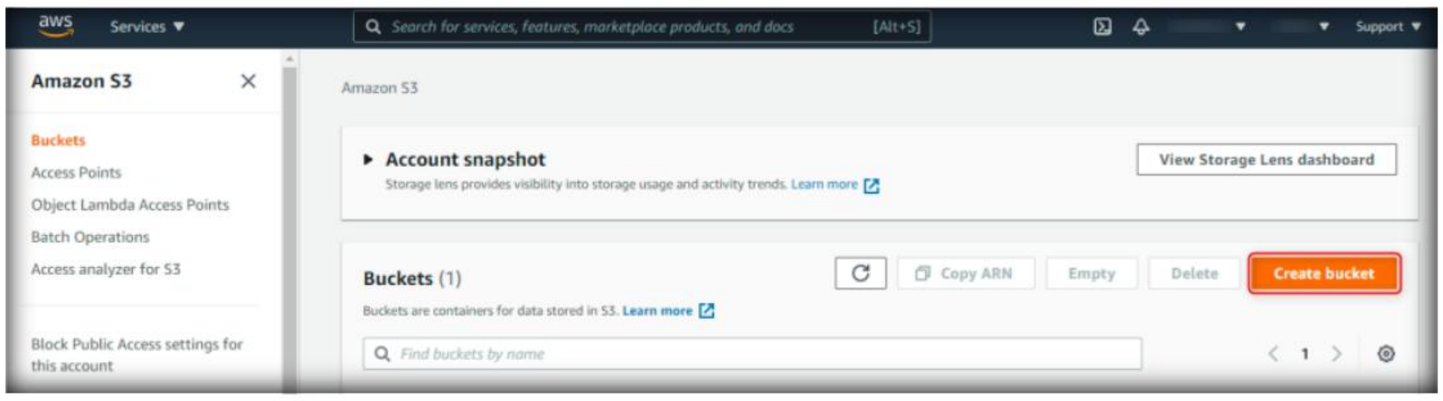


FIGURE 4.2.9: Creating S3 Bucket

10. In the create bucket window that appears, use **training-group001** as the **Bucket name**. Then, select an appropriate region under **AWS Region**.

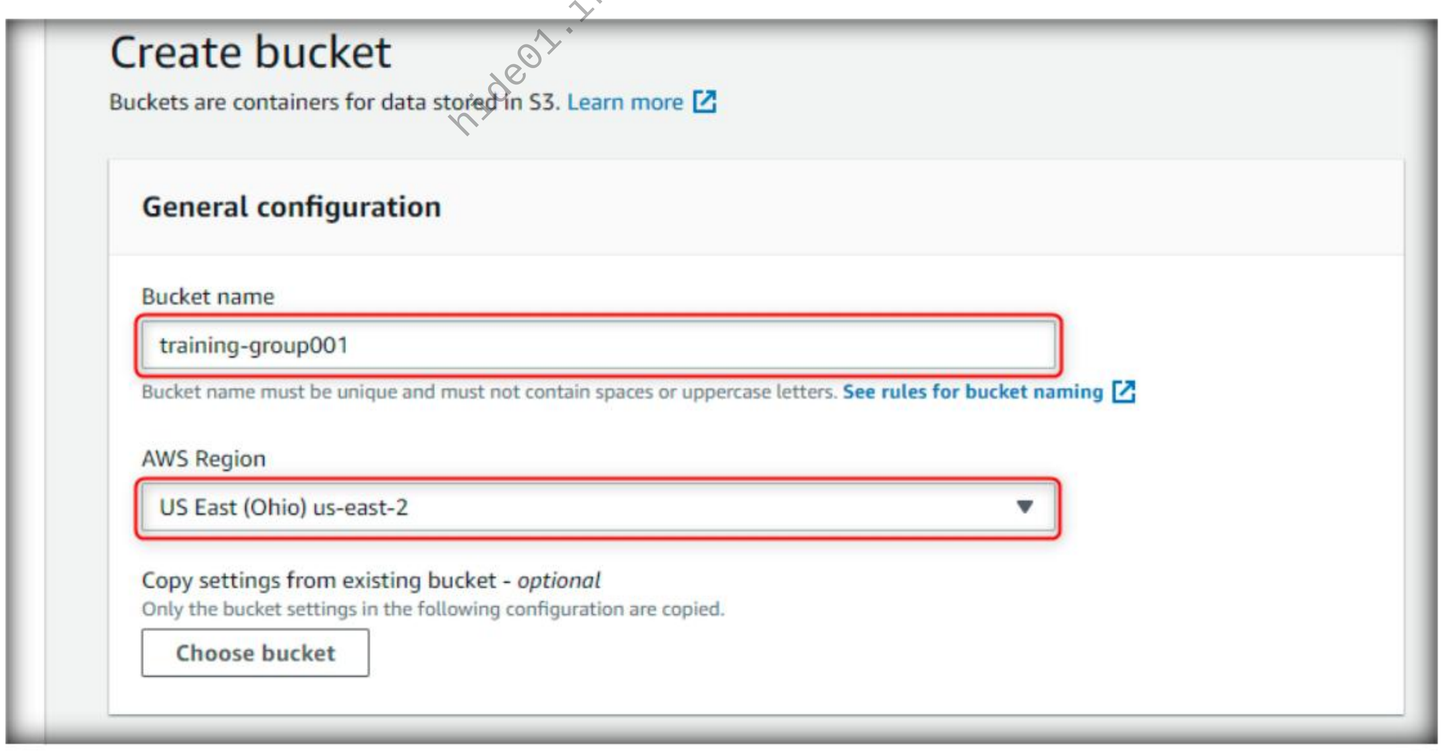


FIGURE 4.2.10: Entering General Configuration Details

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

11. Under Object Ownership, click on ACLs enabled radio button and retain the other default settings. Scroll down to the bottom and click on **Create bucket**.

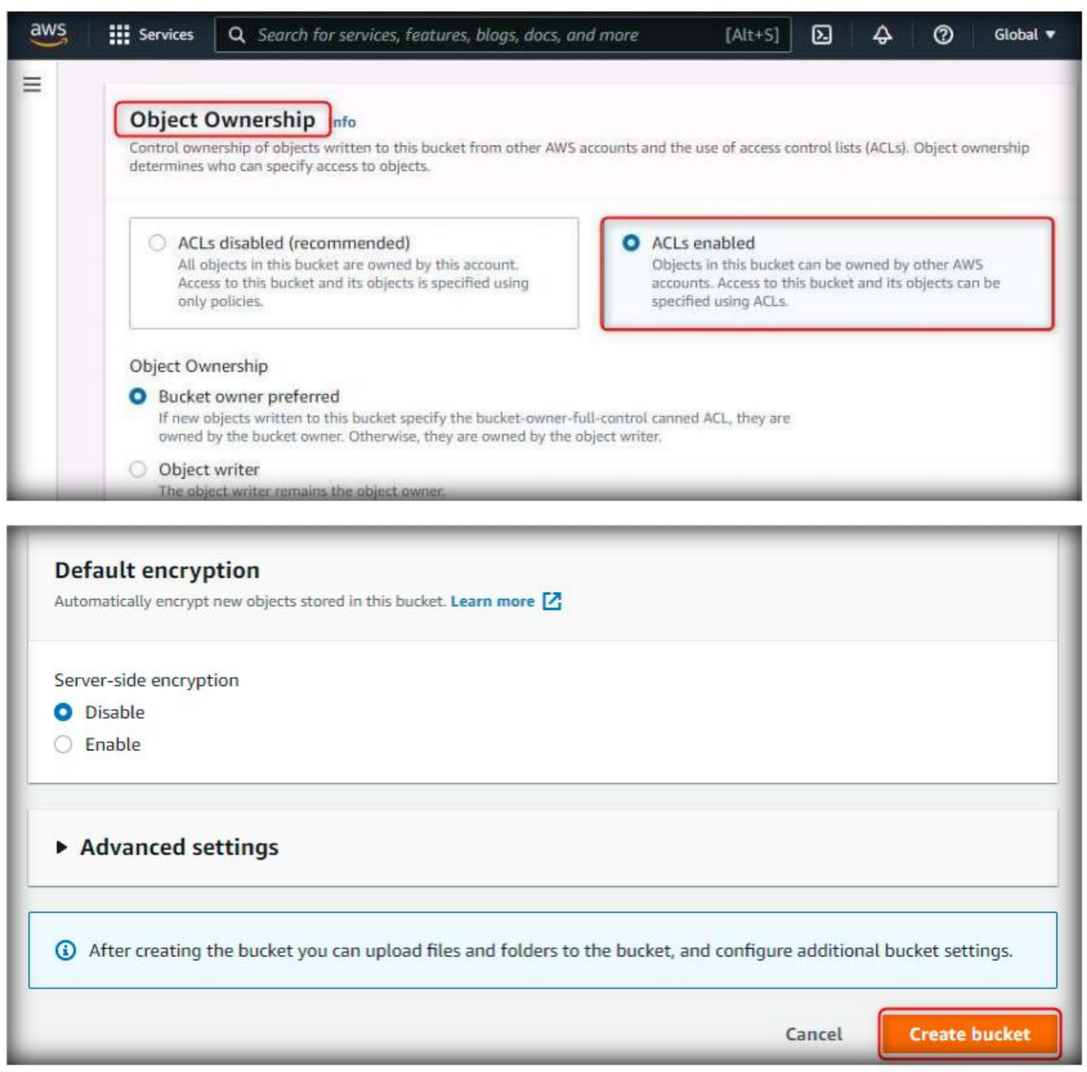


FIGURE 4.2.11: Selecting Create Bucket Button

12. Now, to edit the S3 bucket's public access settings, click on the S3 bucket (here, **training-group001)** that you had created.

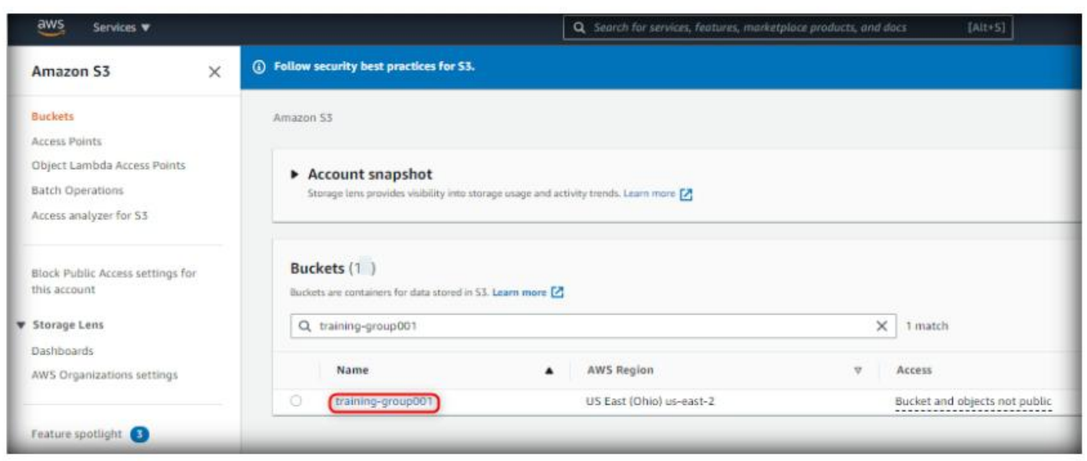


FIGURE 4.2.12: Bucket Selection

13. The **Amazon S3 > training-group001** page appears. Click on the **Permissions** tab.

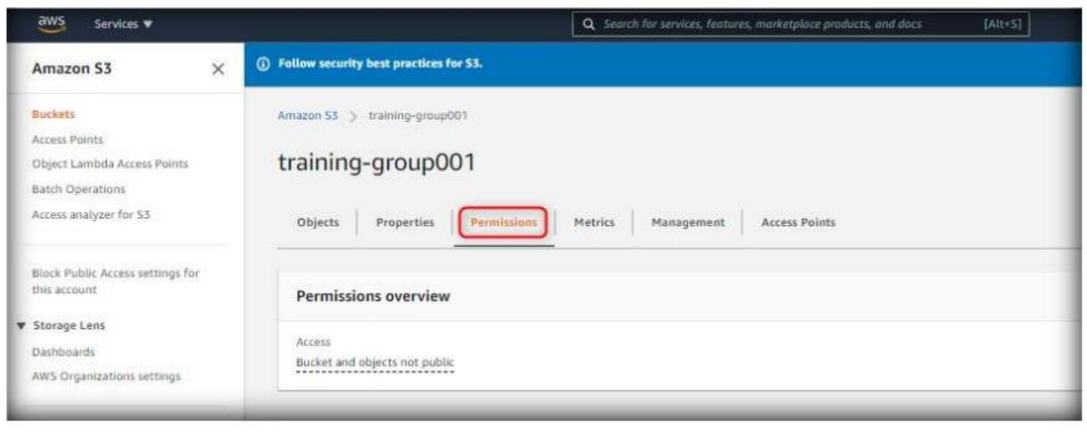


FIGURE 4.2.13: Permissions

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

14. By default, the **Block public access (bucket settings)** tab is selected. Click on **Edit**, as shown in the screenshot below.



FIGURE 4.2.14: Editing Permissions

15. Uncheck **Block all public access** to allow public access to the bucket. Then, click on **Save changes**.

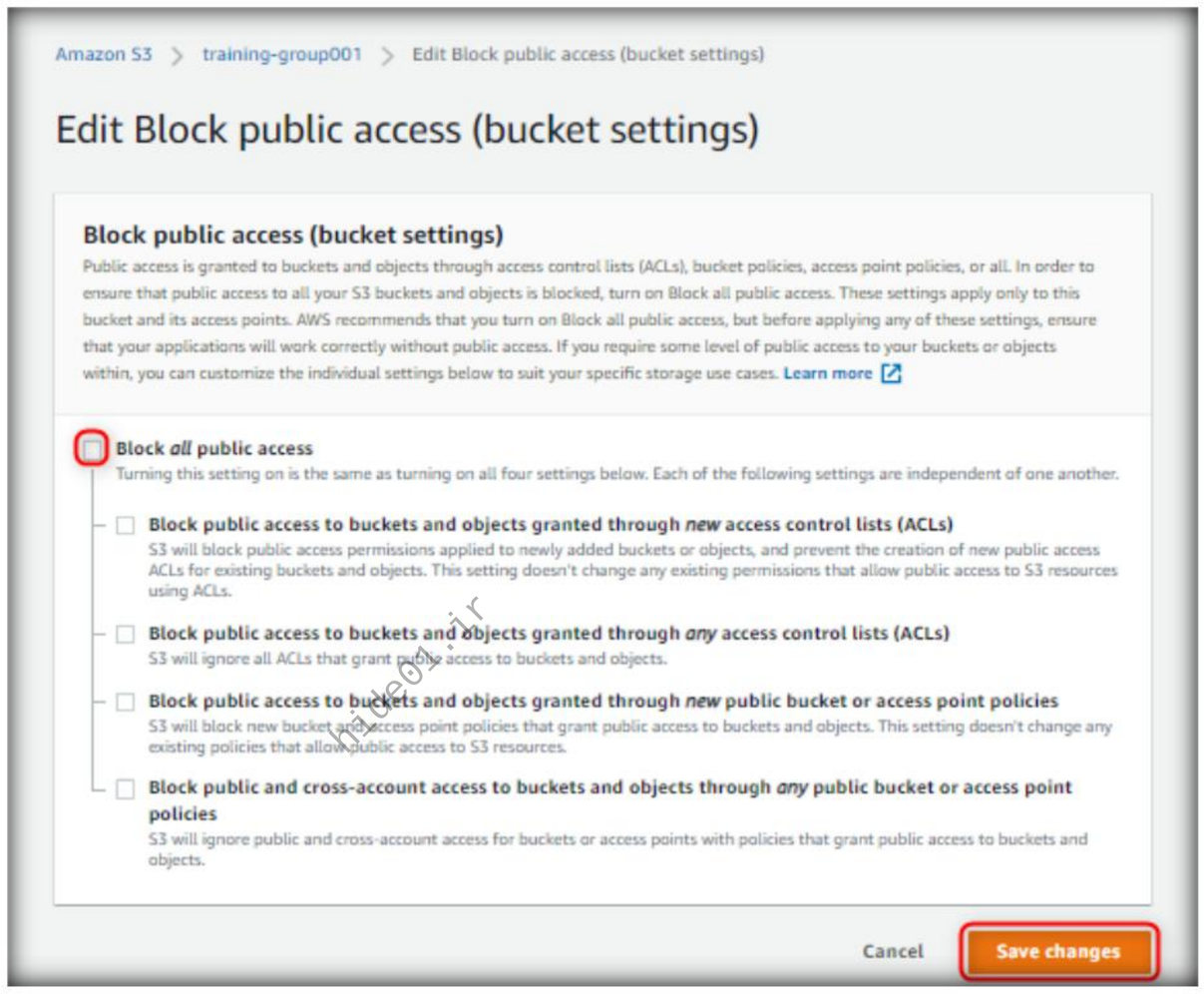


FIGURE 4.2.15: Save Permissions

16. A confirmation dialog appears. Type **confirm**, as shown in the screenshot below, and then click on **Confirm.**

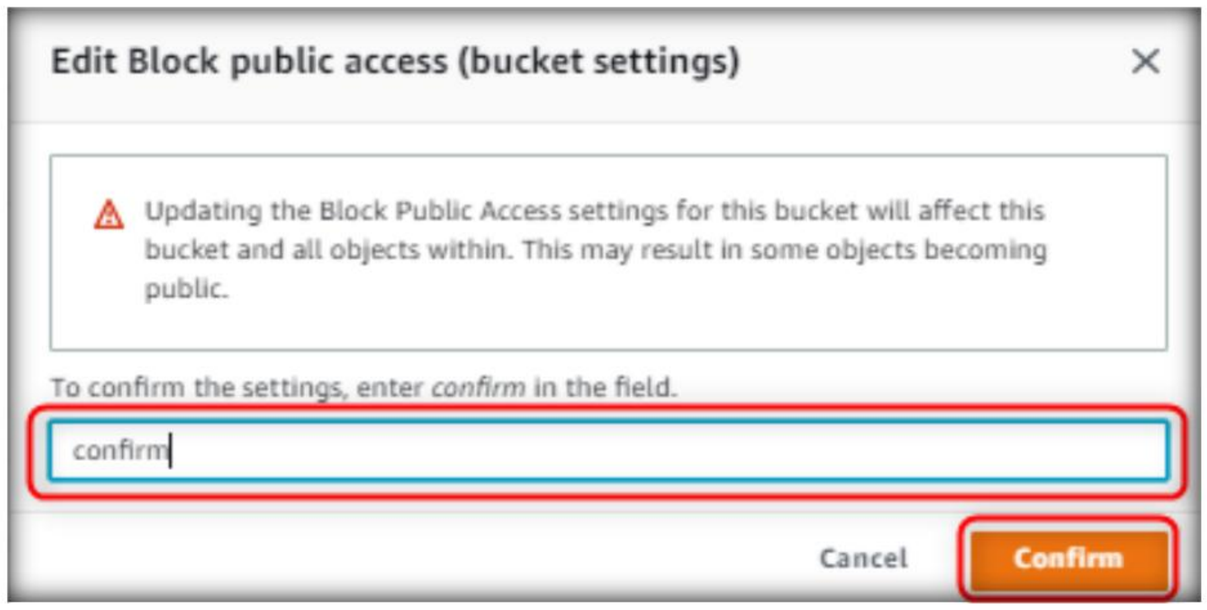


FIGURE 4.2.16: Confirm Settings

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

17. A **Public Access settings updated successfully** message appears.

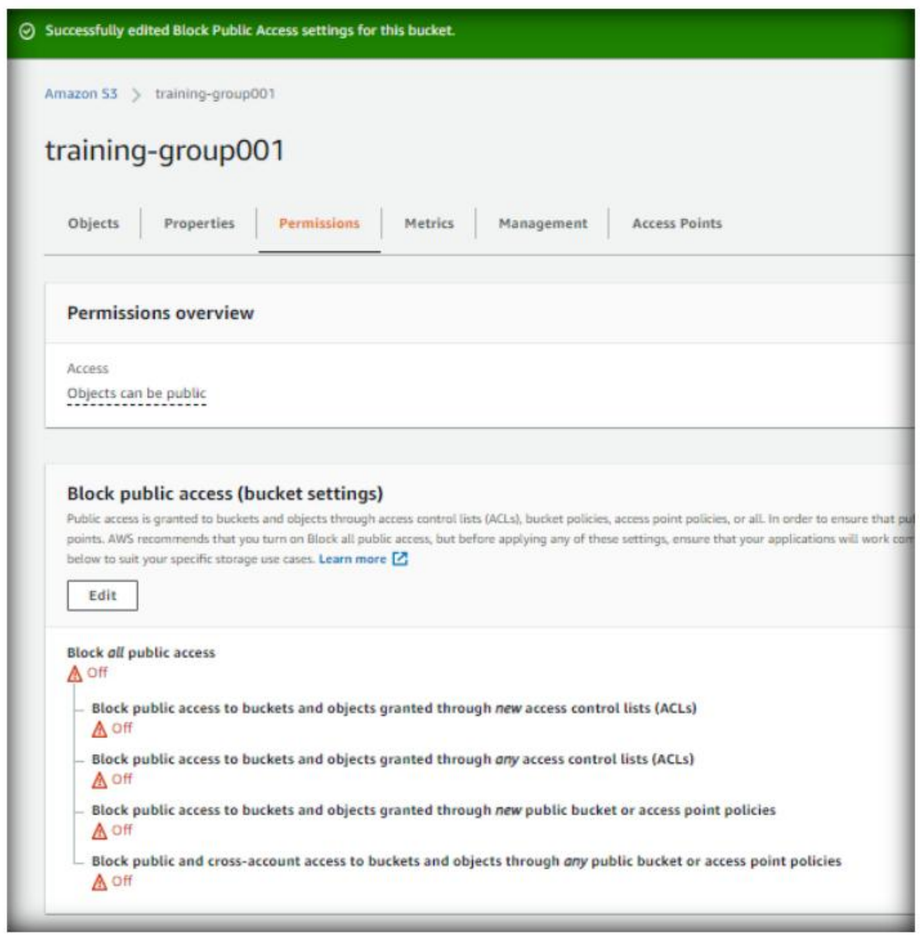


FIGURE 4.2.17: Settings Updated Successfully

18. Scroll down to **Access Control List** on the same **Permissions** tab to edit the read/write permissions of the S3 bucket. Then, click on **Edit**.

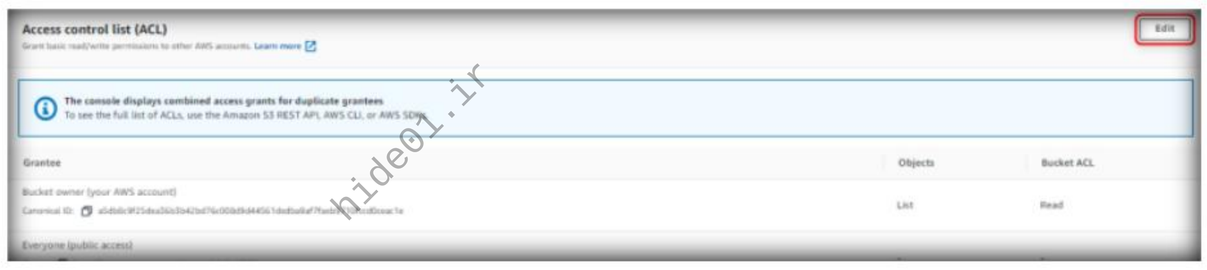


FIGURE 4.2.18: Access Control List

19. On the **Edit access control list (ACL)** page, assign permissions to the S3 bucket under the **Access Control List (ACL)** section for **Bucket owner, Everyone, Authenticated users group**, etc.

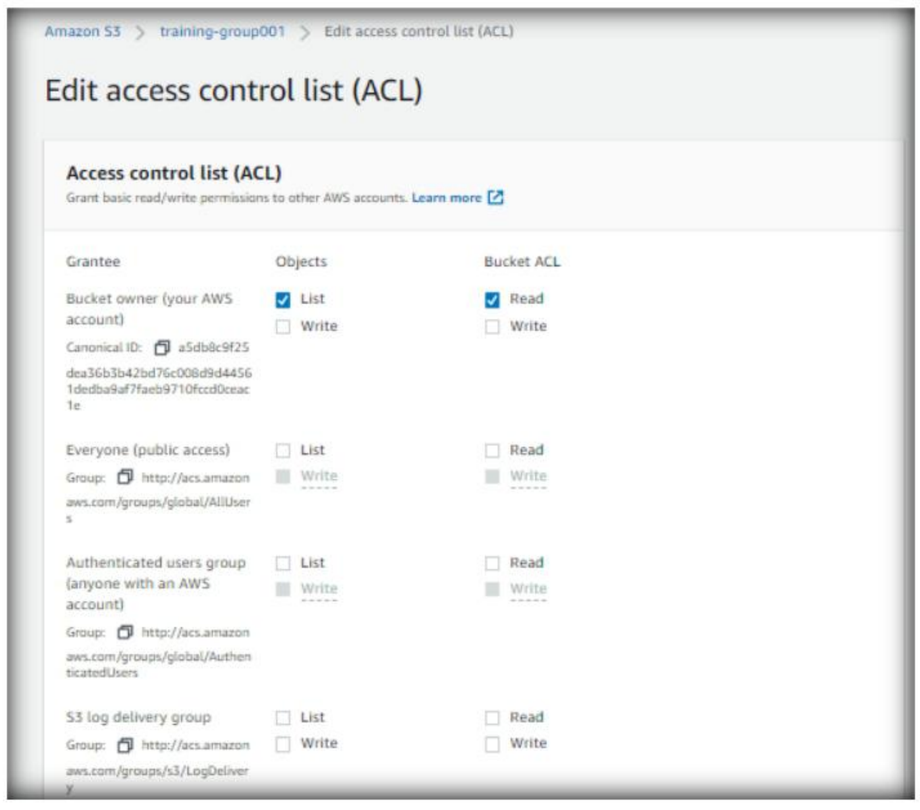


FIGURE 4.2.19: Assigning permissions

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

20. Assign all permissions for the **Bucket owner (your AWS account)** by selecting the checkboxes for **List**, **Write** under **Objects,** and also for **Read** and **Write** under **Bucket ACL**. Then, click on **Save changes**.

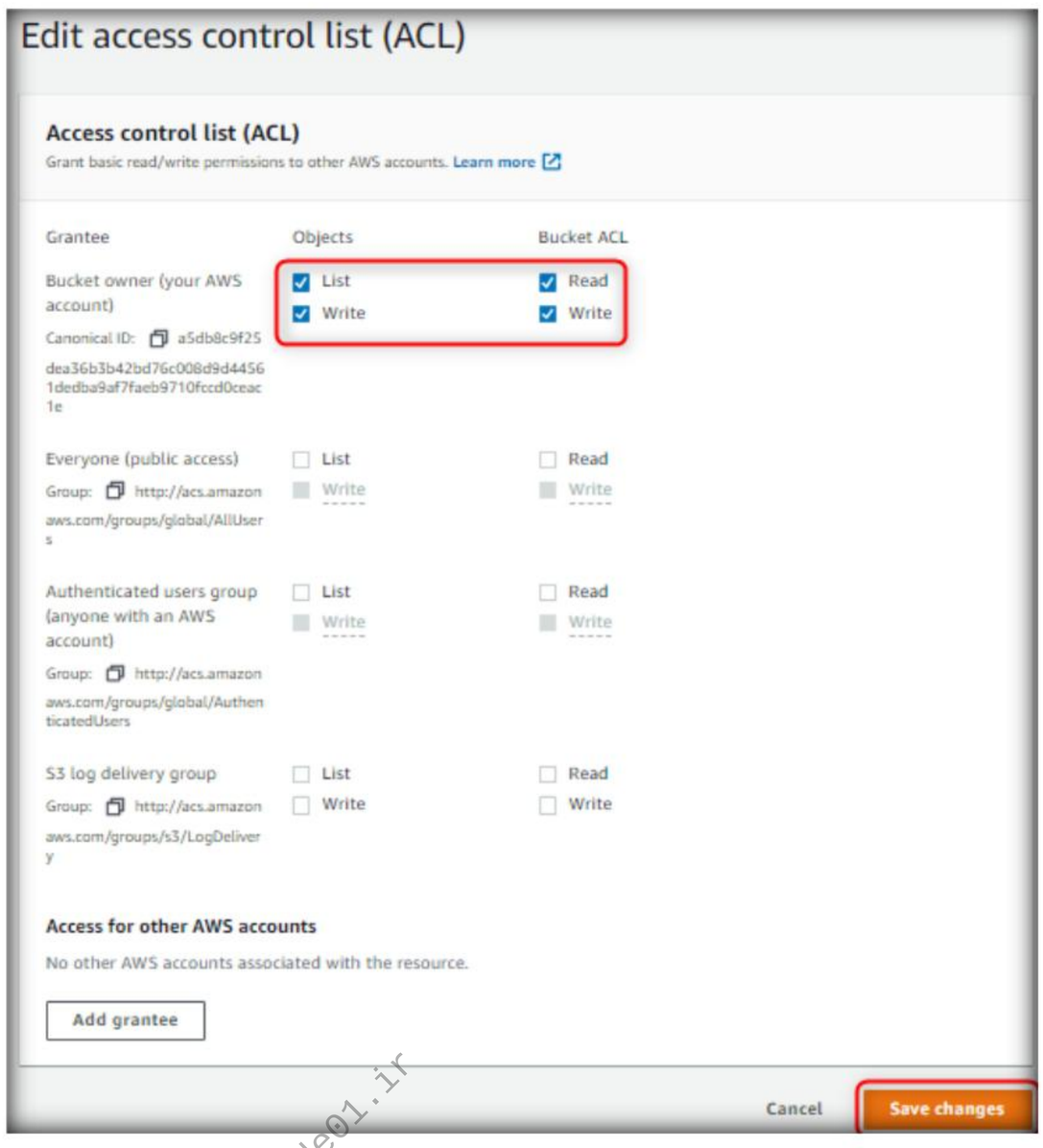


FIGURE 4.2.20: Applying Permissions

21. The public access settings and ACLs have been updated successfully.



FIGURE 4.2.21: Updated Public Access

TASK 2

Assigning Permissions to S3 Buckets Using Bucket Policy

22. To create a bucket policy with the name **training-group001**, you need its ARN. Right-click on **Amazon S3** and click on **Open link in new tab**.

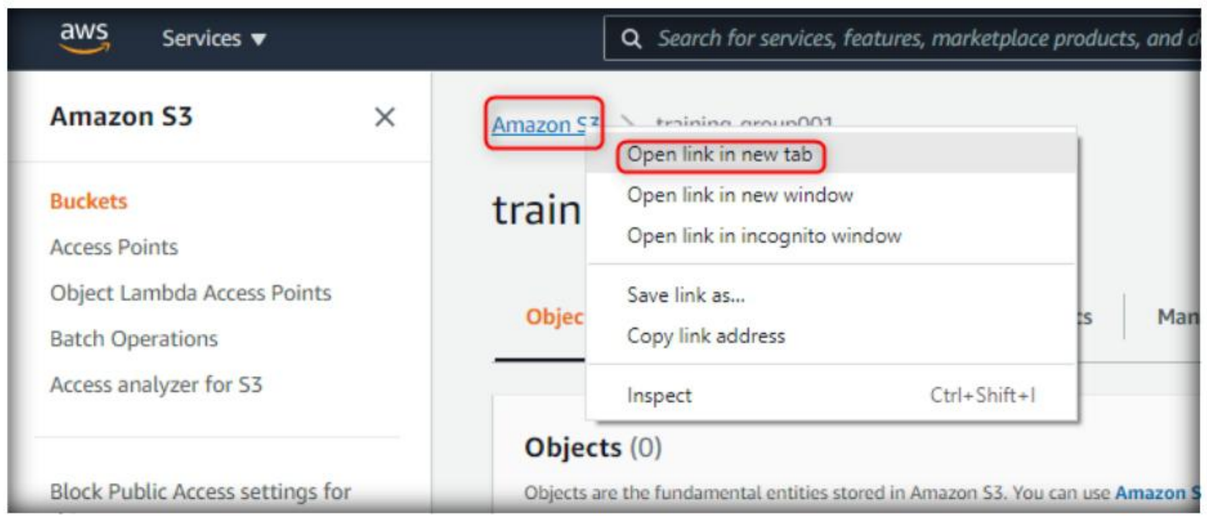


FIGURE 4.2.22: Opening S3 page in a new window

hade01.ir

Certified Cloud Security Engineer Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

23. Check the bucket for which you want to know the ARN number (here, **training-group001**). The details of **training-group001** will appear. Click on **Copy Bucket ARN**, as shown in the screenshot below.

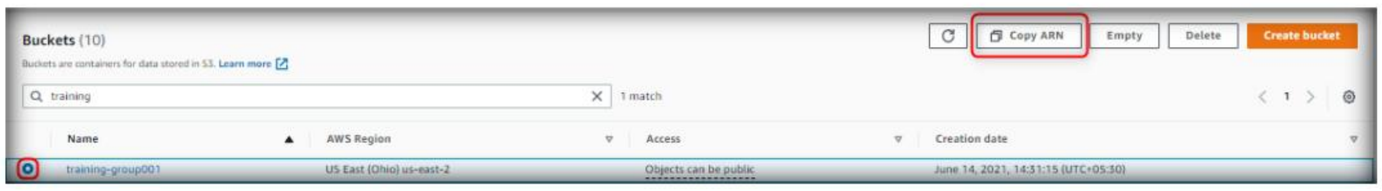


FIGURE 4.2.23: Copying Bucket ARN

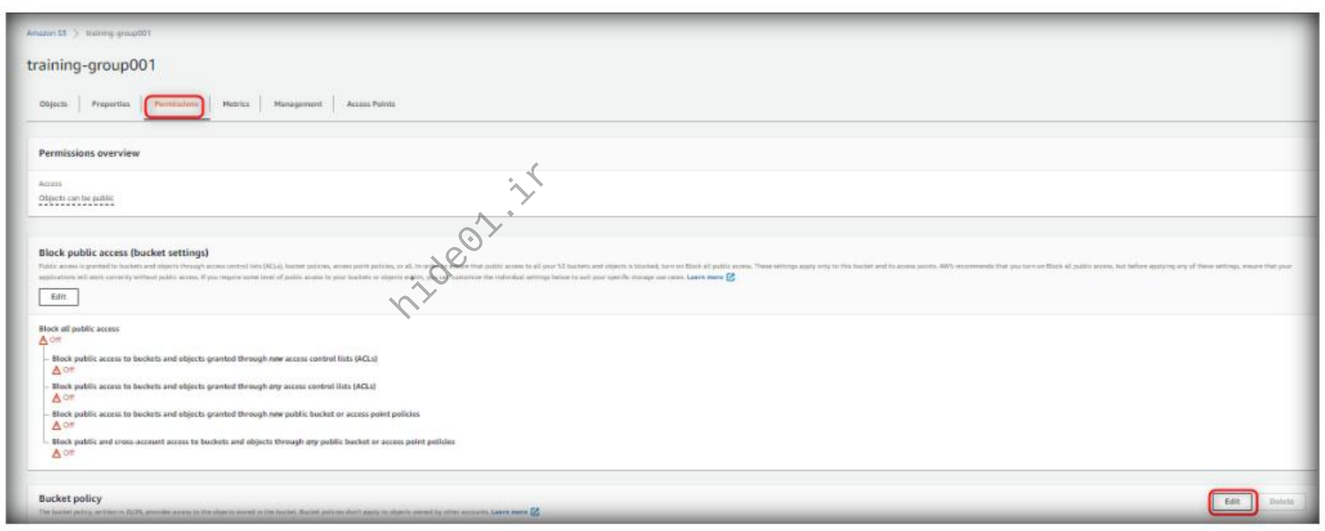
24. Open **Notepad** and paste the copied ARN into it.



FIGURE 4.2.24: Copying to Notepad

25. Switch to the browser and close the second browser tab. You will return to the first browser tab.

26. Now, to configure the bucket policy for the S3 bucket, select **Permissions** on the **training-group001** page. Scroll down to **Bucket Policy** under the **Permissions** tab and click on **Edit**.



hide01.ir

FIGURE 4.2.25: Bucket Policy

27. Scroll down the page and click on the **Policy generator** link, as shown in the screenshot below. A new browser tab opens. Switch to the new tab.



FIGURE 4.2.26: Click on Policy Generator

28. The **AWS Policy Generator** tab appears, as shown in the screenshot below. Set **Select Type of Policy** to **S3 Bucket Policy** from the dropdown. To allow access, set **Effect** to **Allow**. In the **Principal** field,

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

specify a wildcard (*) to grant permissions to everyone. Set **AWS Service** to **Amazon S3** from the dropdown.

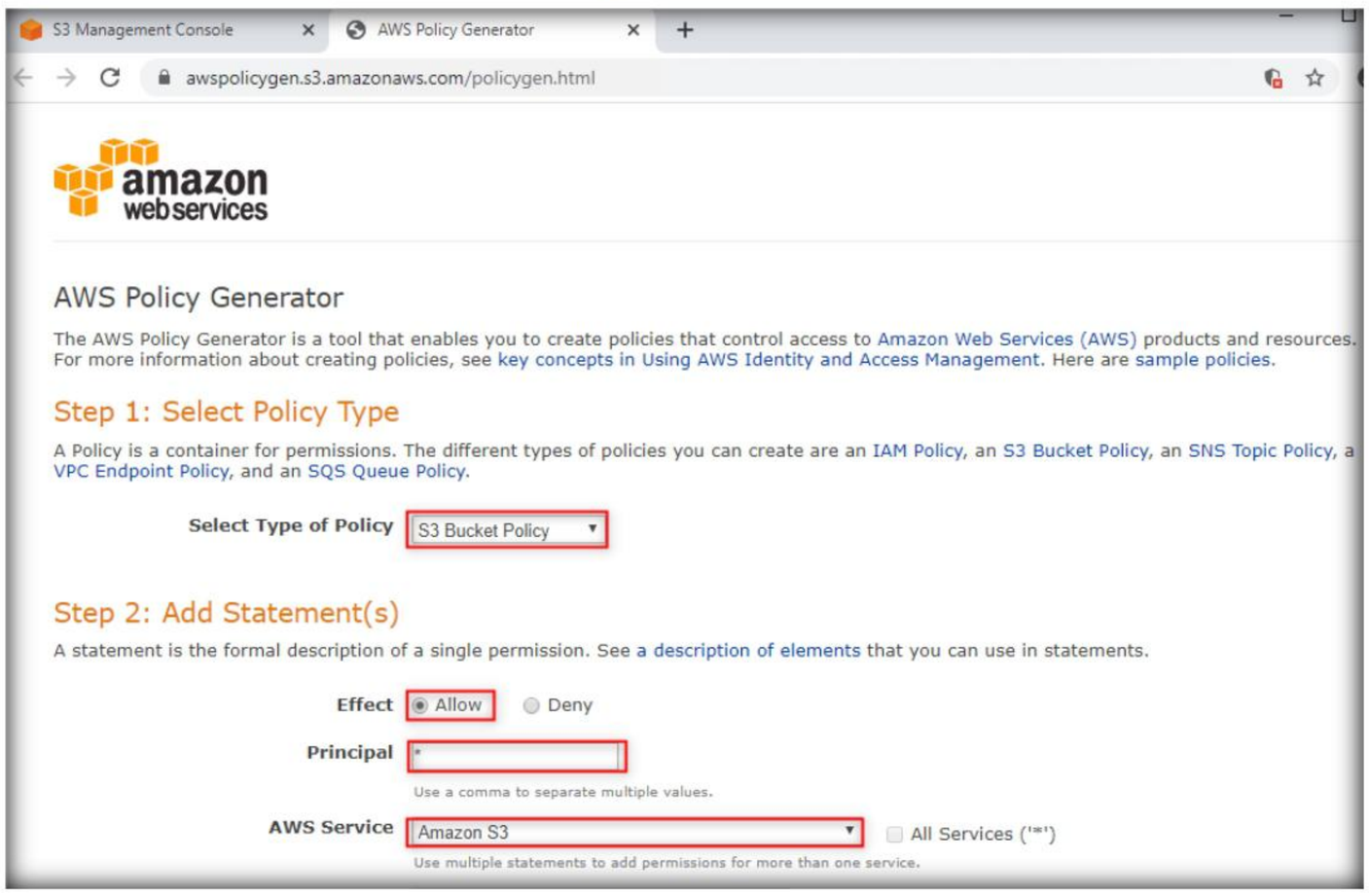


FIGURE 4.2.27: AWS Policy Generator Settings

29. Switch to **Notepad** and copy the ARN that you had copied. Check the **All Actions** checkbox and paste the copied ARN in the **Amazon Resource Name (ARN)** field. Then, click on **Add Statement**.

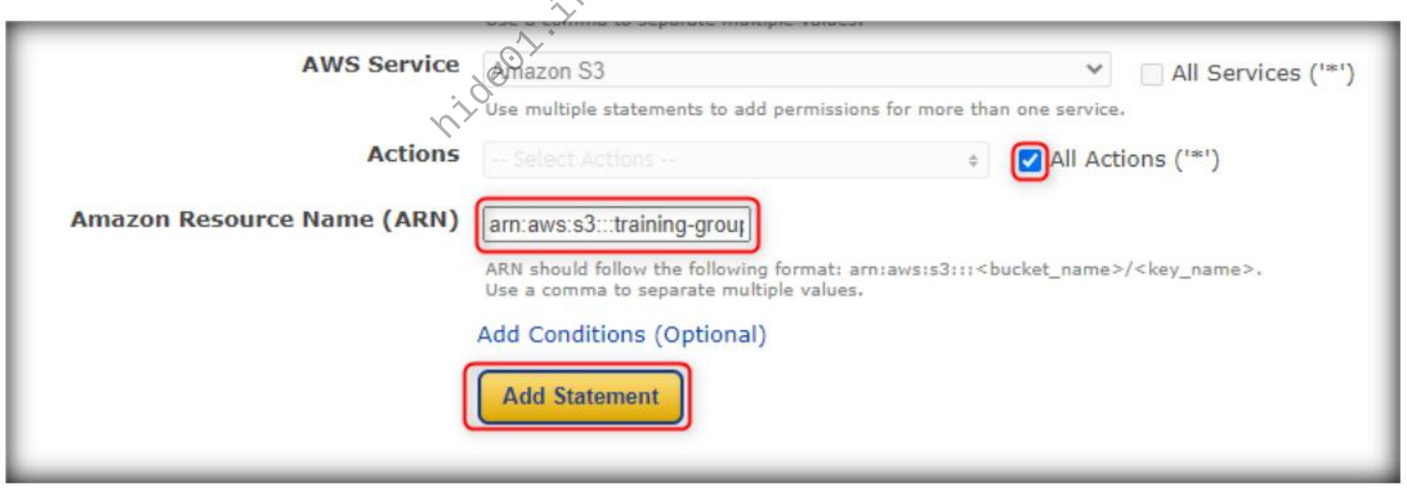


FIGURE 4.2.28: Adding Statement

30. Once the statement is added, click on **Generate Policy** in under **Step 3: Generate Policy**.



FIGURE 4.2.29: Generating Policy

31. A **Policy JSON Document** pop-up appears along with the generated JSON code. Copy the code, as shown in the screenshot below, and click on **Close**.

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

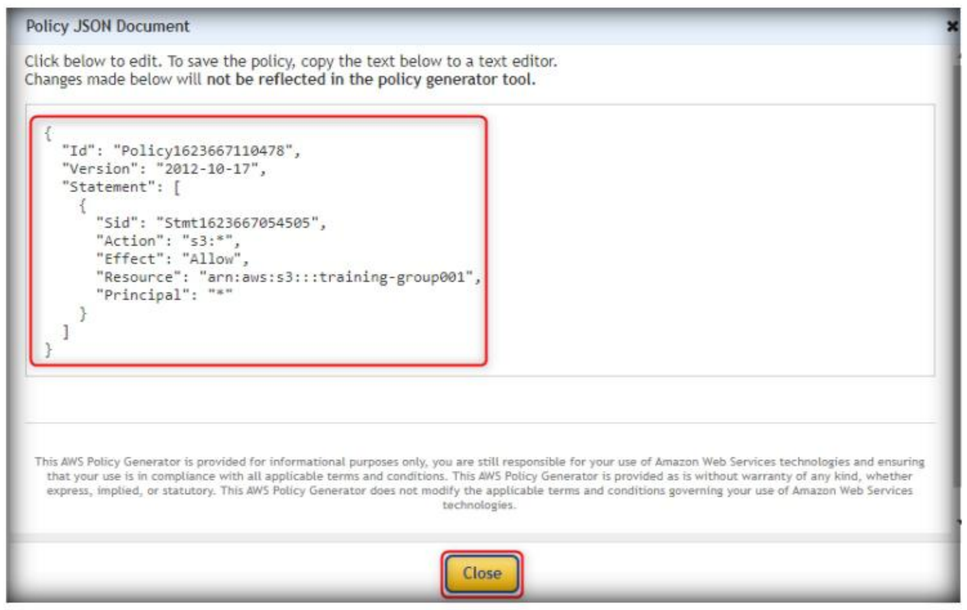


FIGURE 4.2.30: JSON Code

32. Switch to the first tab of the browser (**Edit bucket policy**) to configure **Bucket Policy**. Paste the copied JSON code in the **Bucket policy** editor under **Policy.** Then, click on **Save changes**.

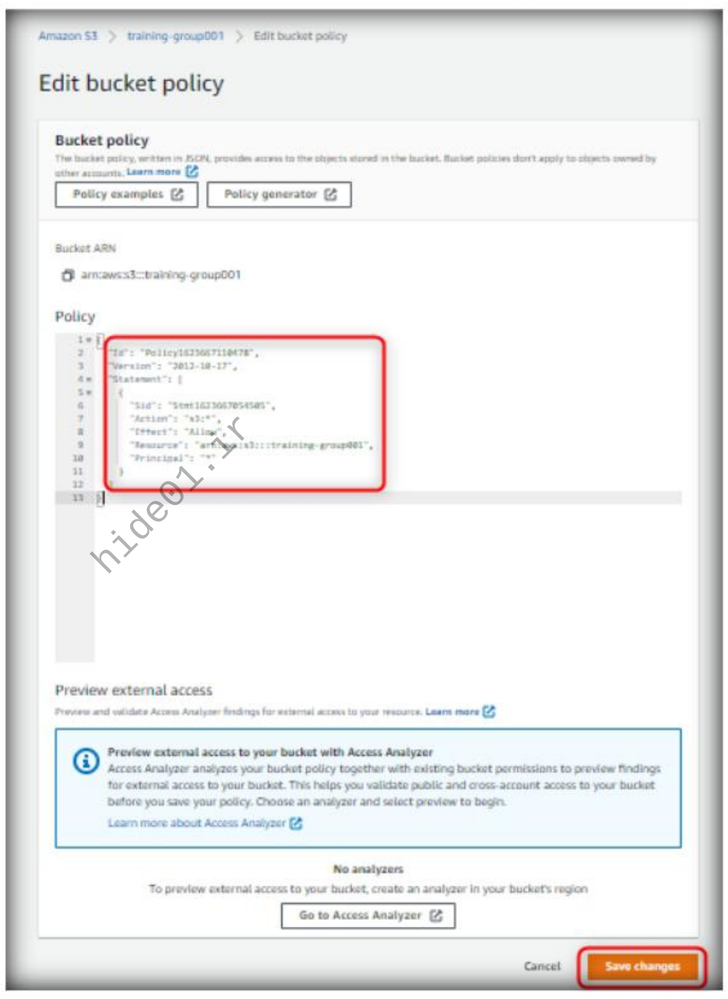


FIGURE 4.2.31: Bucket Policy Editor

33. Now, the bucket has public access.

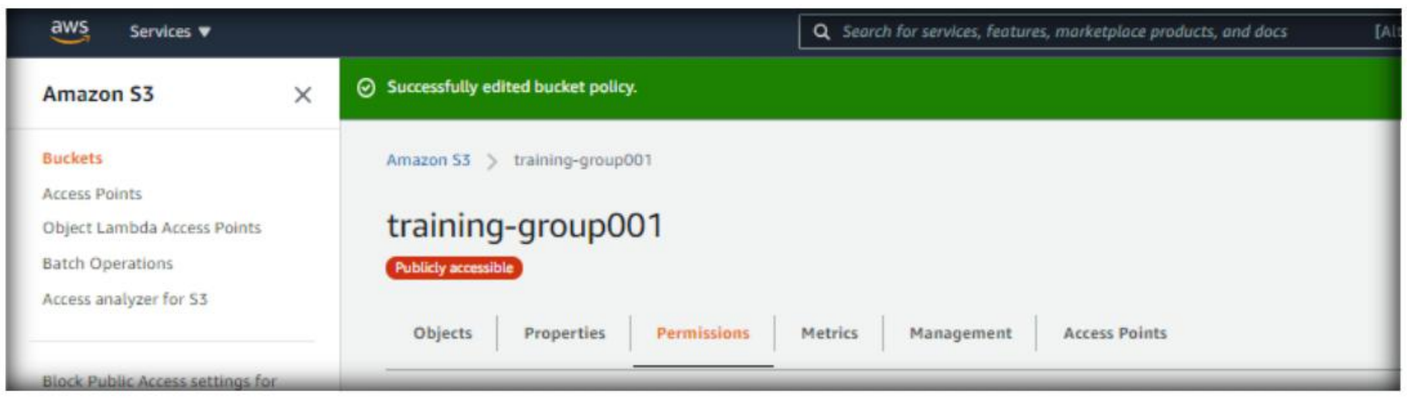


FIGURE 4.2.32: Bucket Access

34. This way, a cloud security engineer can assign permissions to S3 buckets in AWS using ACLs and bucket policies.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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

35. Now, delete the instances created in this lab. Navigate to **Buckets** under the Amazon S3 and select the checkbox for the bucket you want to delete (here, **training-group002**). Click on the **delete** button. In the pop-up window, enter the bucket's name and click on the **Delete bucket** button.

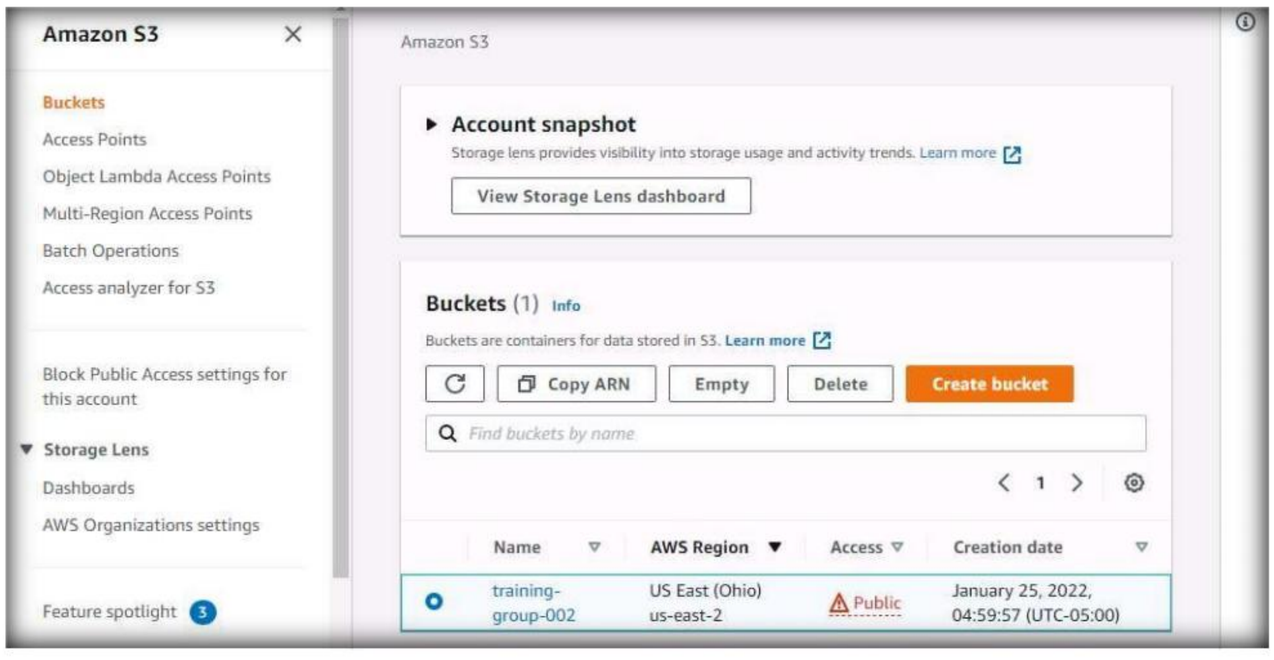


FIGURE 4.2.33: Deleting Bucket

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.

vidoo1.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 3

Restricting Non-SSL Access for S3 Objects using Bucket Policies

Bucket policies can be configured to implement data-in-transit encryption for objects stored in an Amazon S3 bucket.

Lab Scenario

ICON KEY

Valuable information

Test your knowledge

Web exercise

Workbook review

Amazon S3 objects include files and their metadata. Access to the S3 objects can be secured by defining policies. Amazon S3 uses the HTTPS protocol to ensure the data in transit is encrypted. Policies can be defined to secure S3 objects to block non-SSL access and allow only SSL access.

Lab Objectives

This lab will demonstrate how to restrict non-SSL (insecure) access for S3 objects.

In this lab, you will learn to do the following:

- Create an object inside a bucket
- Configure permissions for an object
- Verify public access for the object over the Internet
- Configure a secure connection for the object using a bucket policy
- Verify the secure connection publicly for an object over the Internet

Lab Environment

To perform this lab, you need the following:

- **Admin Machine** VM
- **Administrative** privileges to run the tools

Lab Duration

Time: 15 minutes

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Overview of AWS Storage Objects

Amazon S3 allows the uploading and retrieval of data anytime from anywhere on the Internet. It stores data such as objects (text files/photos/videos) within buckets. Amazon S3 is a container that stores the objects securely. In their default state, all Amazon S3 buckets can be accessed by authorized users. If access restrictions are to be imposed on objects in Amazon S3, bucket policies need to be configured. The security of the data in transit can be ensured with Amazon S3 because it uses the HTTPS protocol. Policies can be configured for the objects to allow only HTTPS connections and deny HTTP connections. Man-in-the-middle attacks can be prevented when http connections are blocked for S3 objects.

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., AWS), the application interface may be updated with time. Hence, in case you happen to work on an updated version of AWS, 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 an AWS Free Tier account using the following link: https://aws.amazon.com/free/, in case you have already not created it for the previous module. Once the registration is complete, perform the following task:

ide01.ir

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

TASK 1

Creating Object inside Bucket

1. Log in to the **Admin Machine** VM with username **Admin** and password **admin@123**.

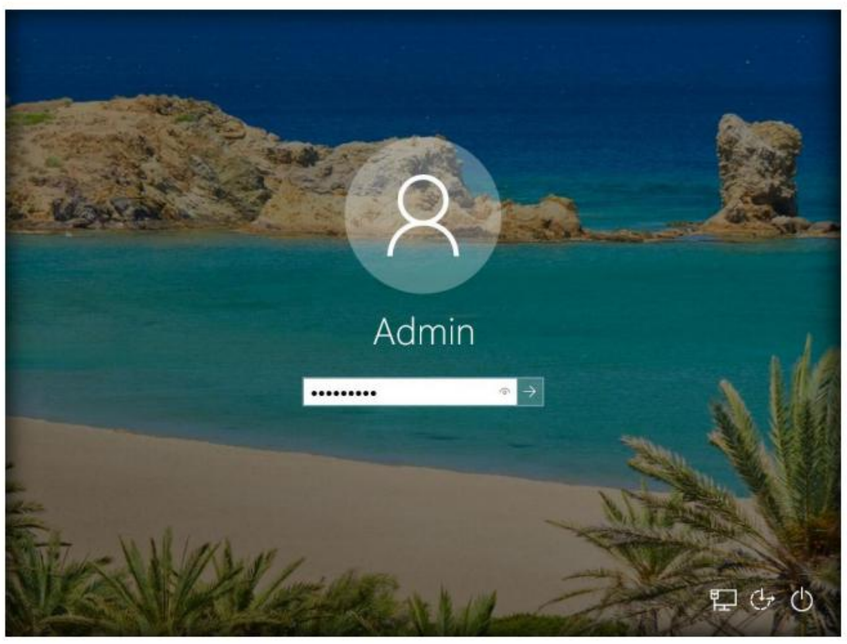


FIGURE 4.3.1: User Login

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

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



FIGURE 4.3.2: Navigating to the Chrome Browser from Taskbar

3. The **Google Chrome** browser appears. Go to the address bar, type **https://aws.amazon.com/**, and press **Enter.**

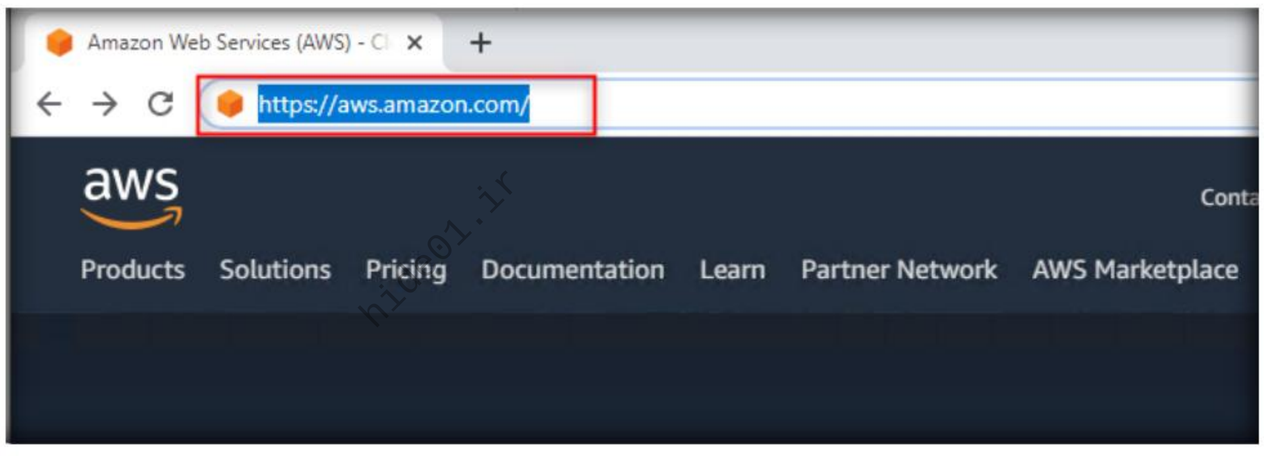


FIGURE 4.3.3: Access AWS in Browser

Note: If you are already logged in, skip the login steps.

4. The **AWS Web Services - Cloud Computing Services** page appears. Click on the **AWS Management Console** from the **My Account** dropdown, as shown in the screenshot below.

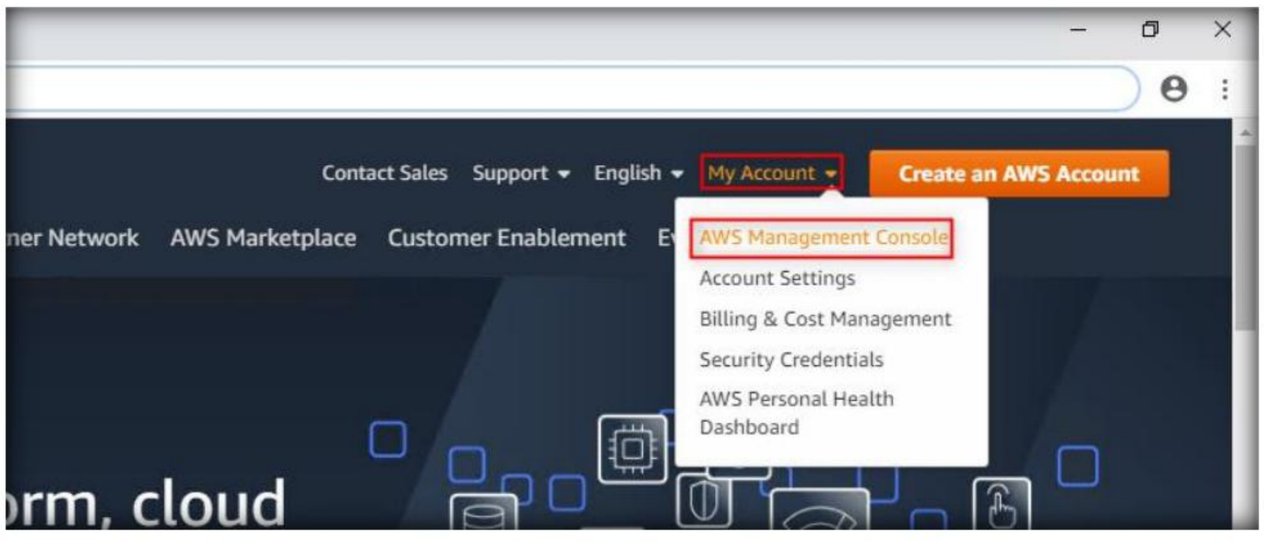


FIGURE 4.3.4: Navigate to AWS Management Console

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

5. The **AWS Web Services Sign-in** page appears. Type the AWS administrator account ID (**Root user email address**) and click on **Next**.

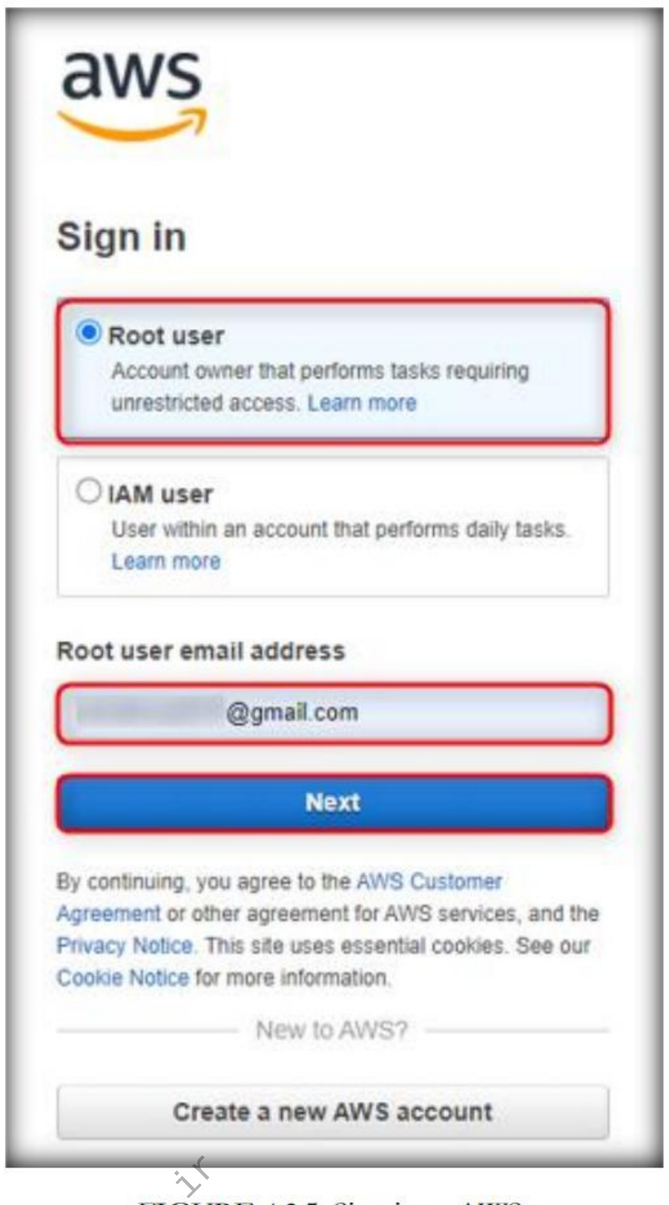


FIGURE 4.3.5: Sign-in to AWS

6. In the security check page that appears, type the characters shown in the image and click **Submit**.

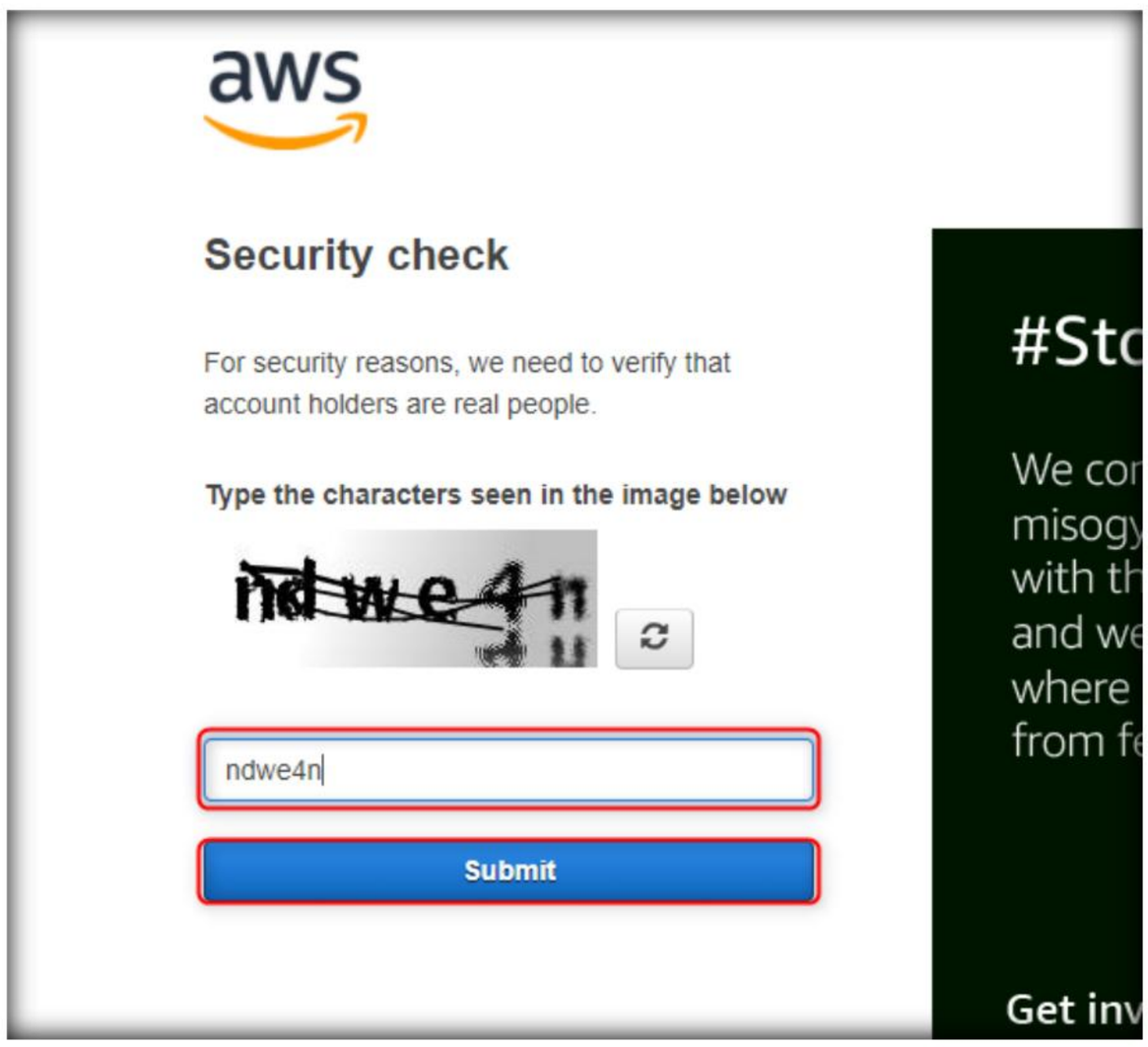


FIGURE 4.3.6: Sign-in to AWS

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

7. In the **Password** field, type the password and click on **Sign in**.

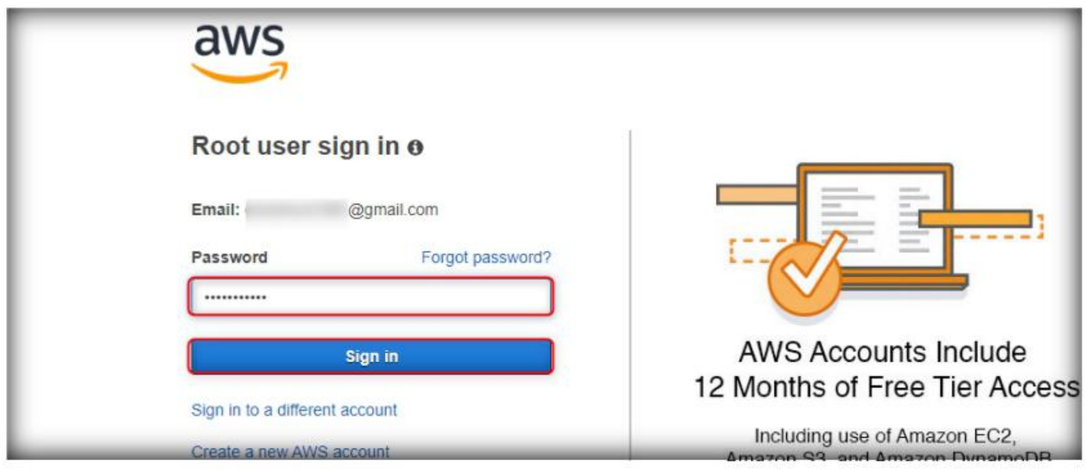


FIGURE 4.3.7: Sign in to AWS

8. Now, to add objects to the S3 bucket, click on **Services**. Then, click on **S3** under **Storage**.

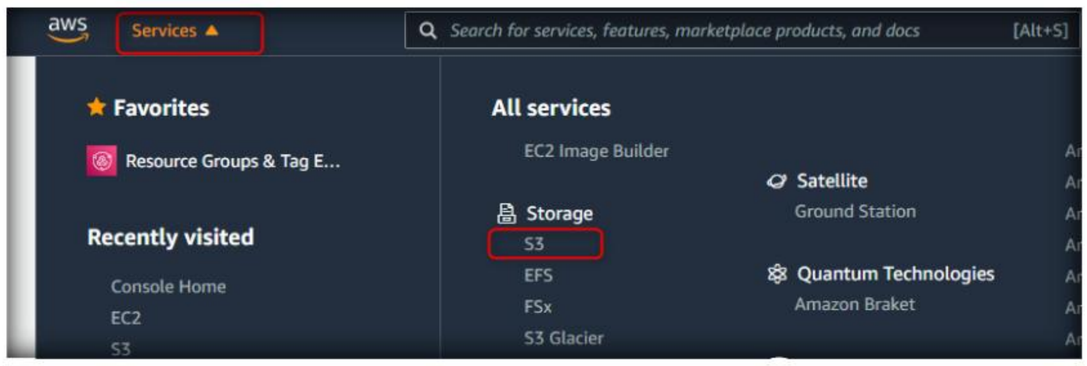


FIGURE 4.3.8: Selecting Service

9. You can see the bucket you had created in the previous lab (**training-group001**). Create a new object under the **training-group001** bucket by clicking on it.

Note: If you have deleted the **training-group001** S3 bucket, create a new S3 bucket by following **Steps 8–10** in the previous lab.

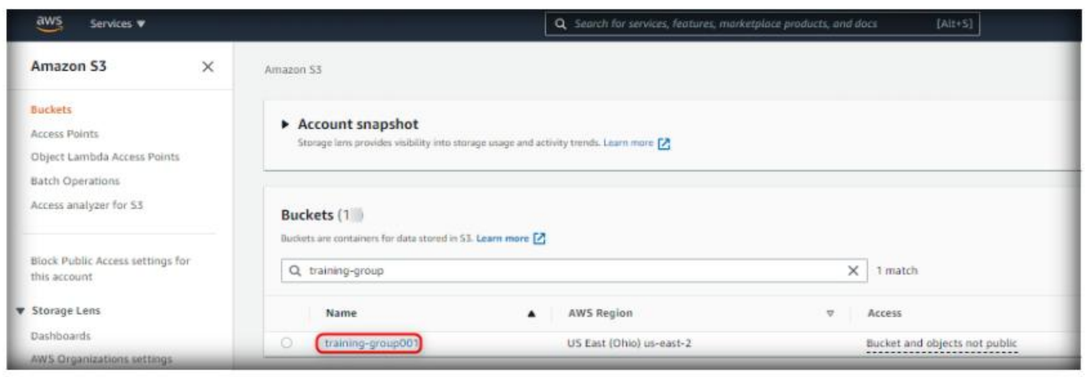


FIGURE 4.3.9: Bucket Selection

10. Next, upload a webpage as the object to the S3 bucket that can be publicly accessed. Then, click the **Upload** button.

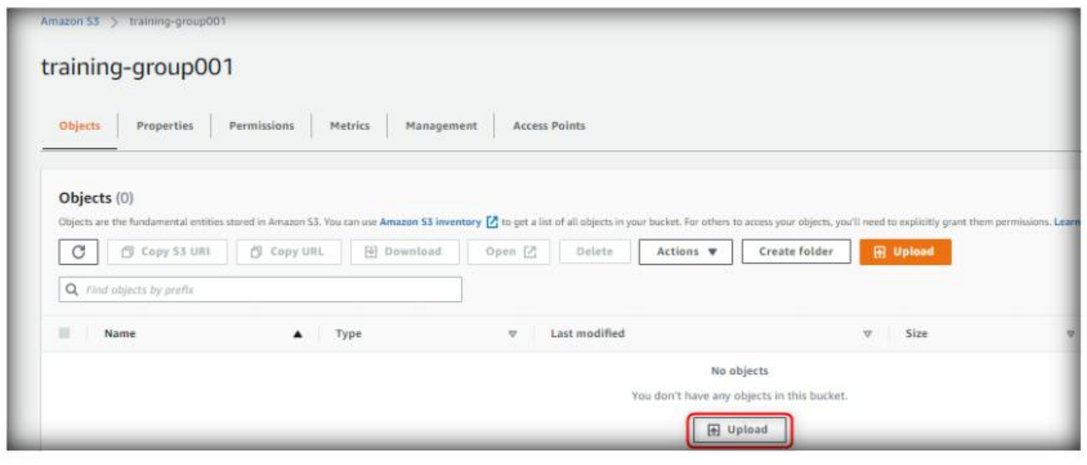


FIGURE 4.3.10: Selecting Upload

Certified Cloud Security Engineer Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

11. Once the **Upload** section opens, click the **Add files** button to add the file.

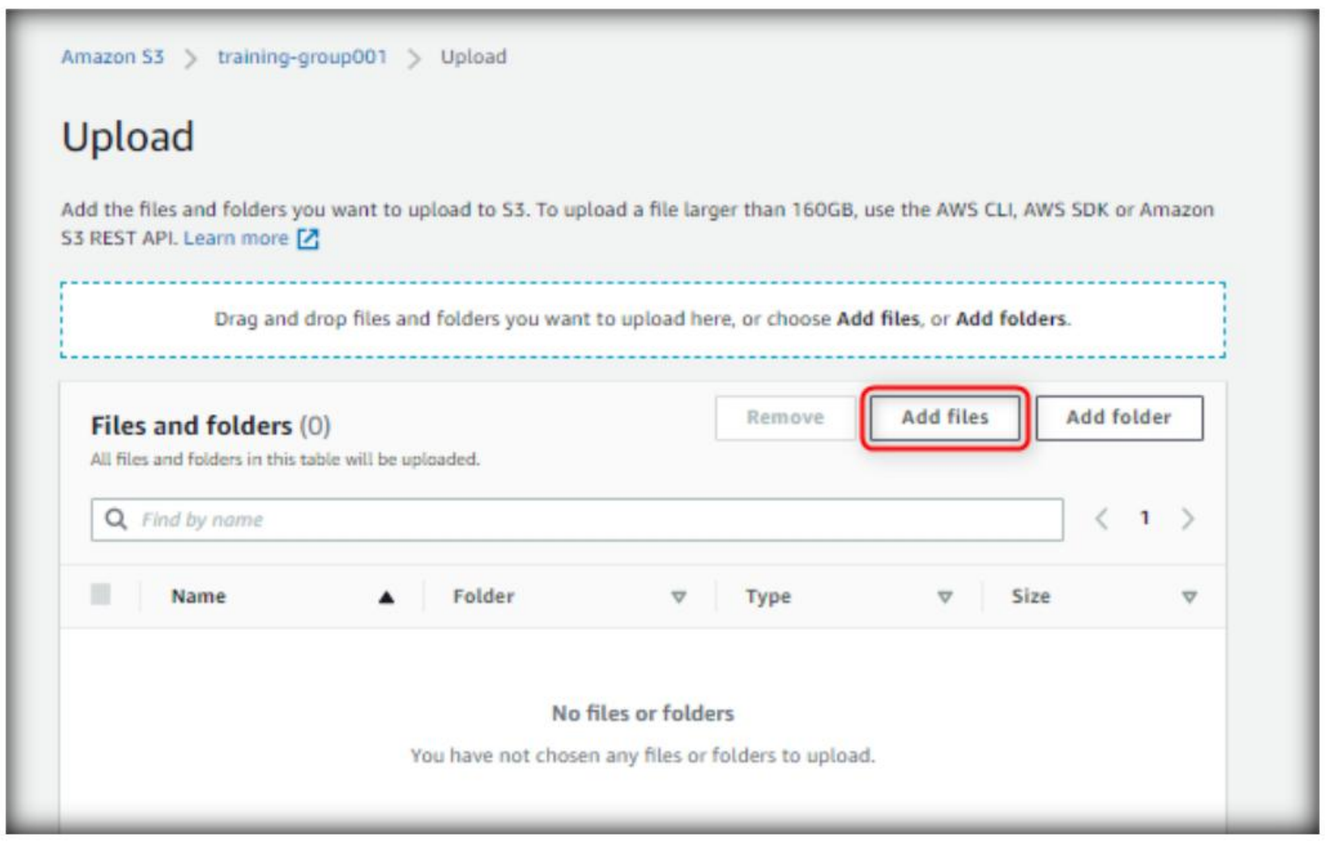


FIGURE 4.3.11: Clicking on Add files

12. Now, open notepad to create an html file (e.g., **WebApp**) on your host machine. Enter the text **"Welcome to the Web Application"** inside notepad.



hide01.ir

FIGURE 4.3.12: Creating an HTML File

13. Save the file name with a .html extension (**e.g., WebApp.html**) and click **Save**.

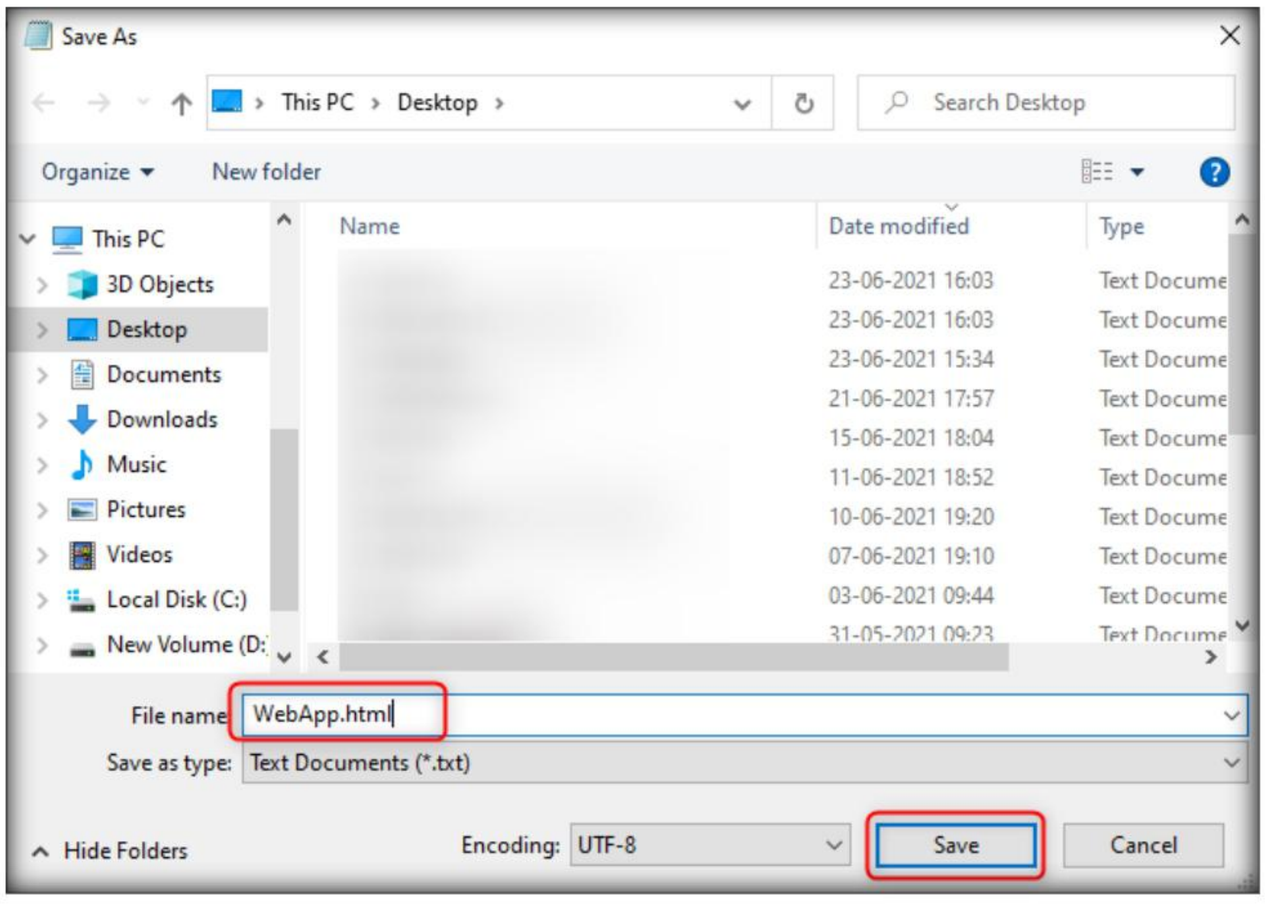


FIGURE 4.3.13: Saving HTML File

14. Once the **Open** window appears, navigate to the file location, select it, and click the **Open** button.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

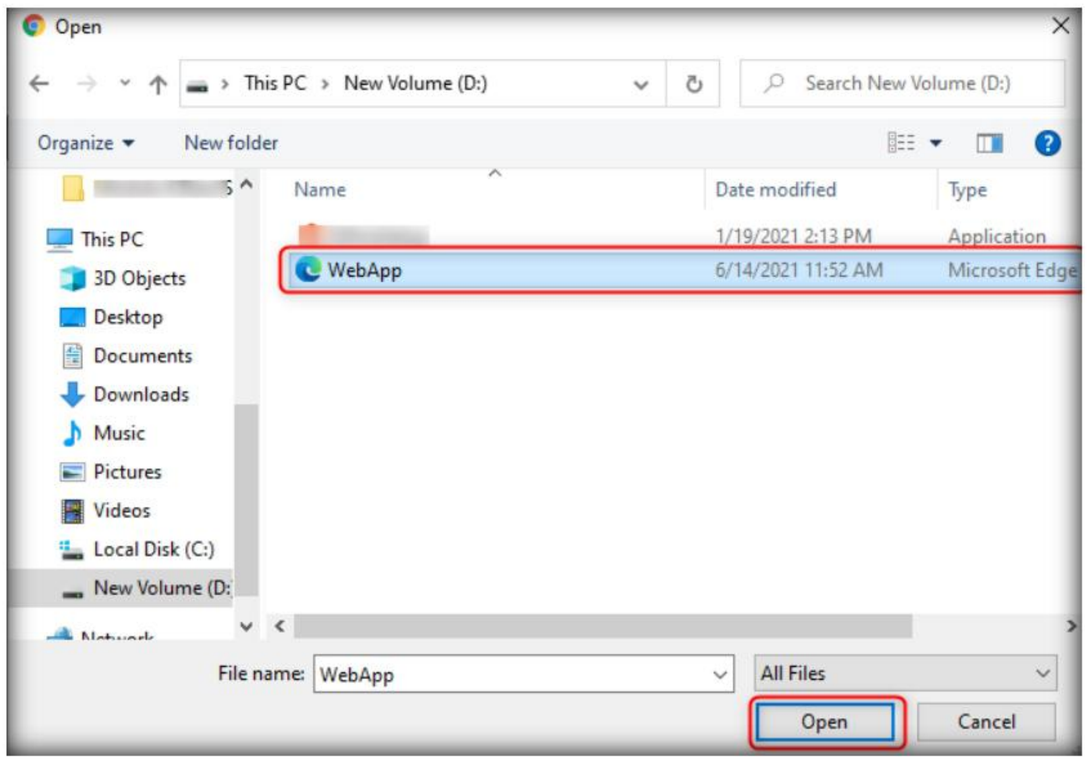


FIGURE 4.3.14: Opening WebApp

15. The **WebApp.html** file will be added. Scroll down and click on **Upload** to upload the file.

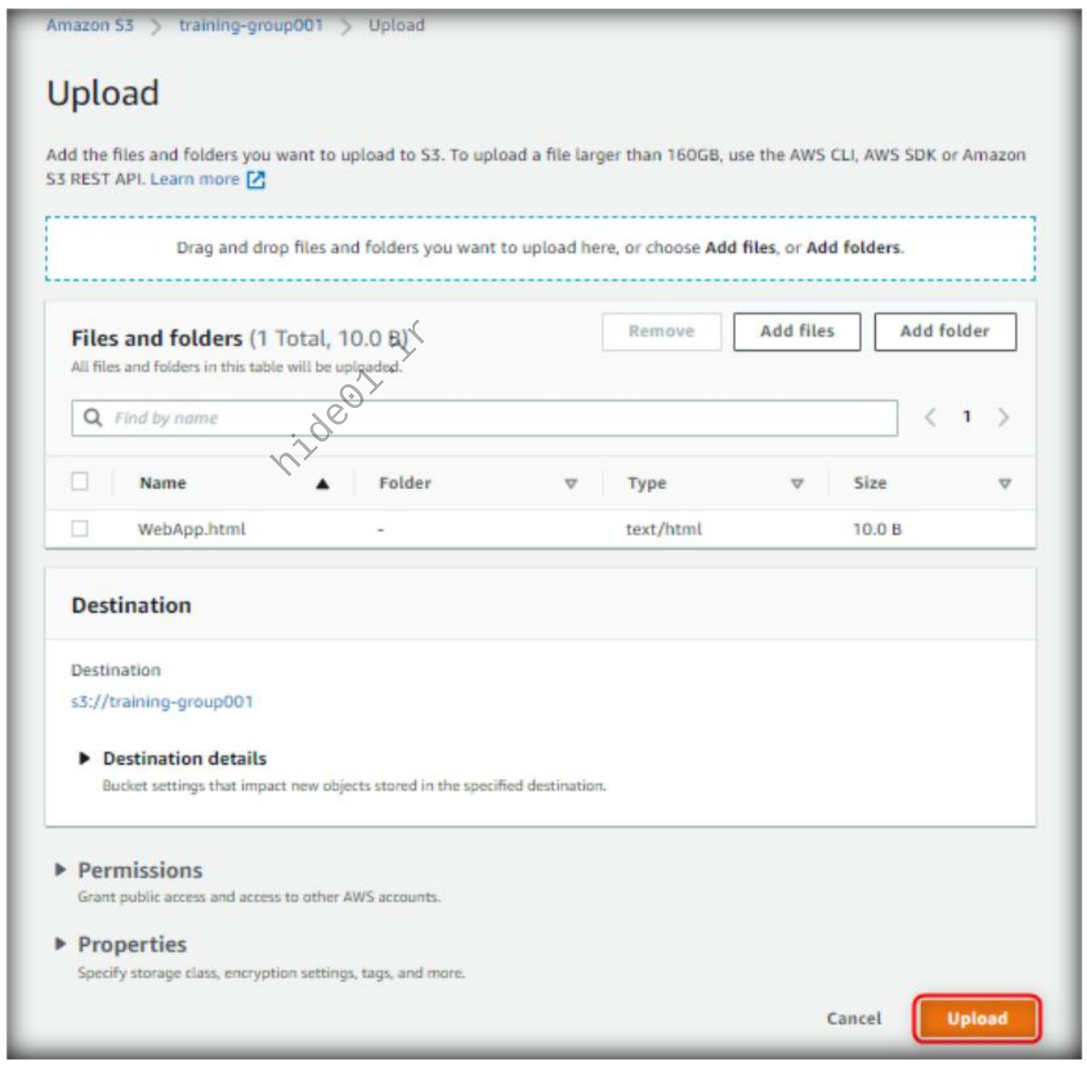


FIGURE 4.3.15: Uploading the file

16. After a few seconds, you will see the **upload succeeded** message. Then, click on **Close**.

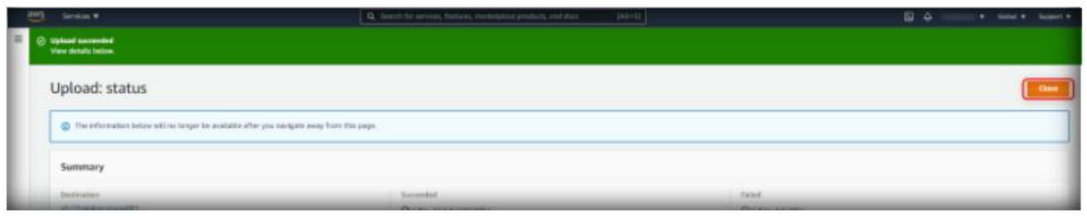


FIGURE 4.3.16: Upload Status

17. Next, you will be returned to the **training-group001** bucket page.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

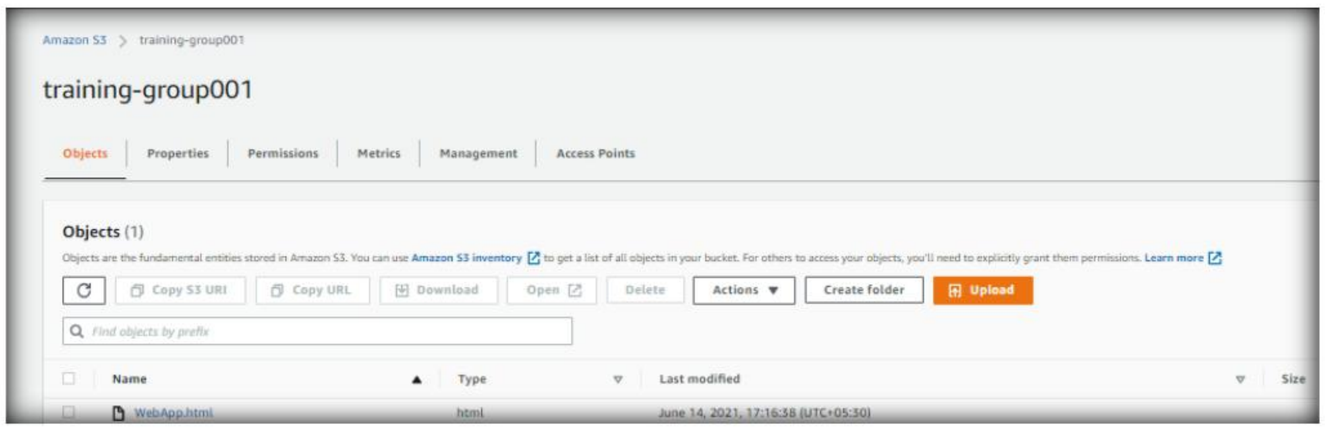


FIGURE 4.3.17: **training-group001** Bucket Page

TASK 2

Configuring Permissions for object

18. To make the web page publicly accessible, select the checkbox for **WebApp.html** object. Then, click on the **Actions** dropdown button and select the **Make public** option from the list.

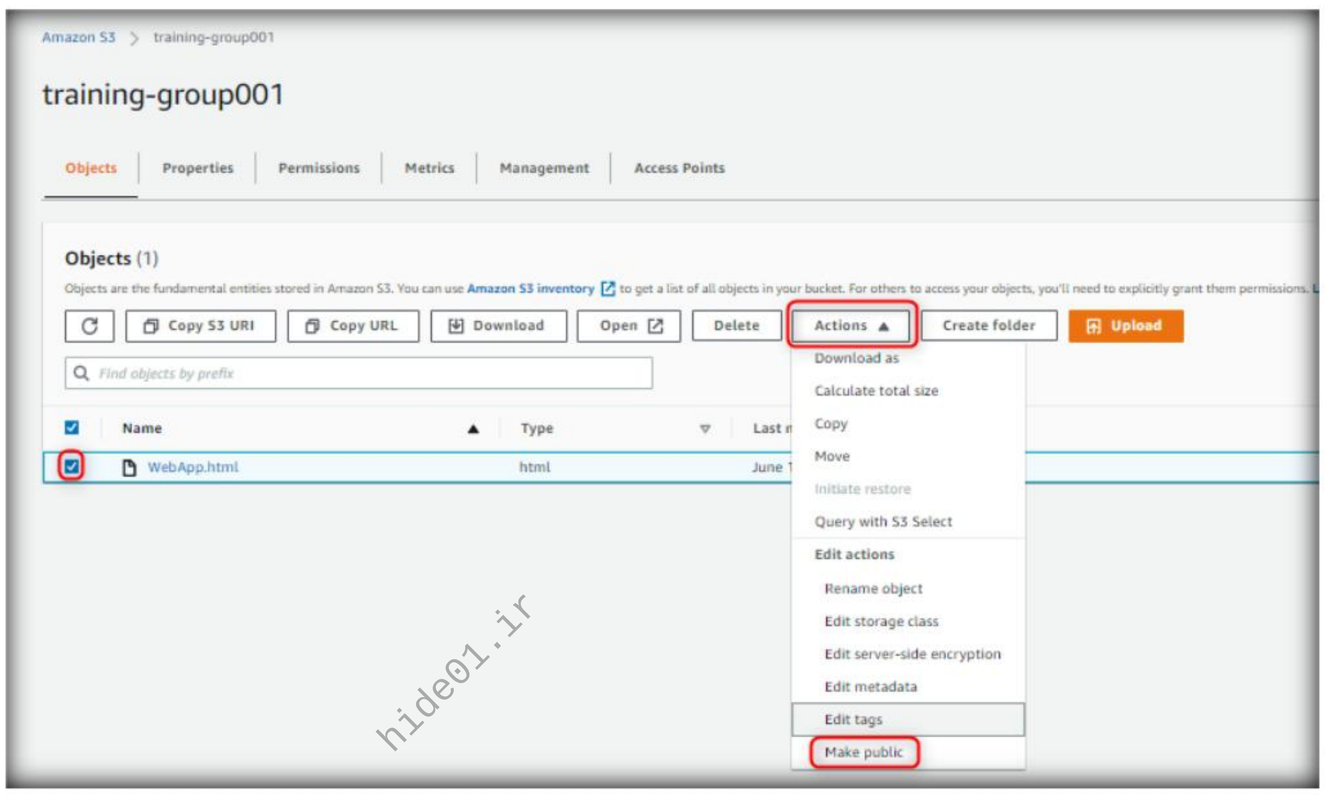


FIGURE 4.3.18: Setting WebApp permissions

19. In the **Make public** section that appears, click on the **Make public** button to continue.

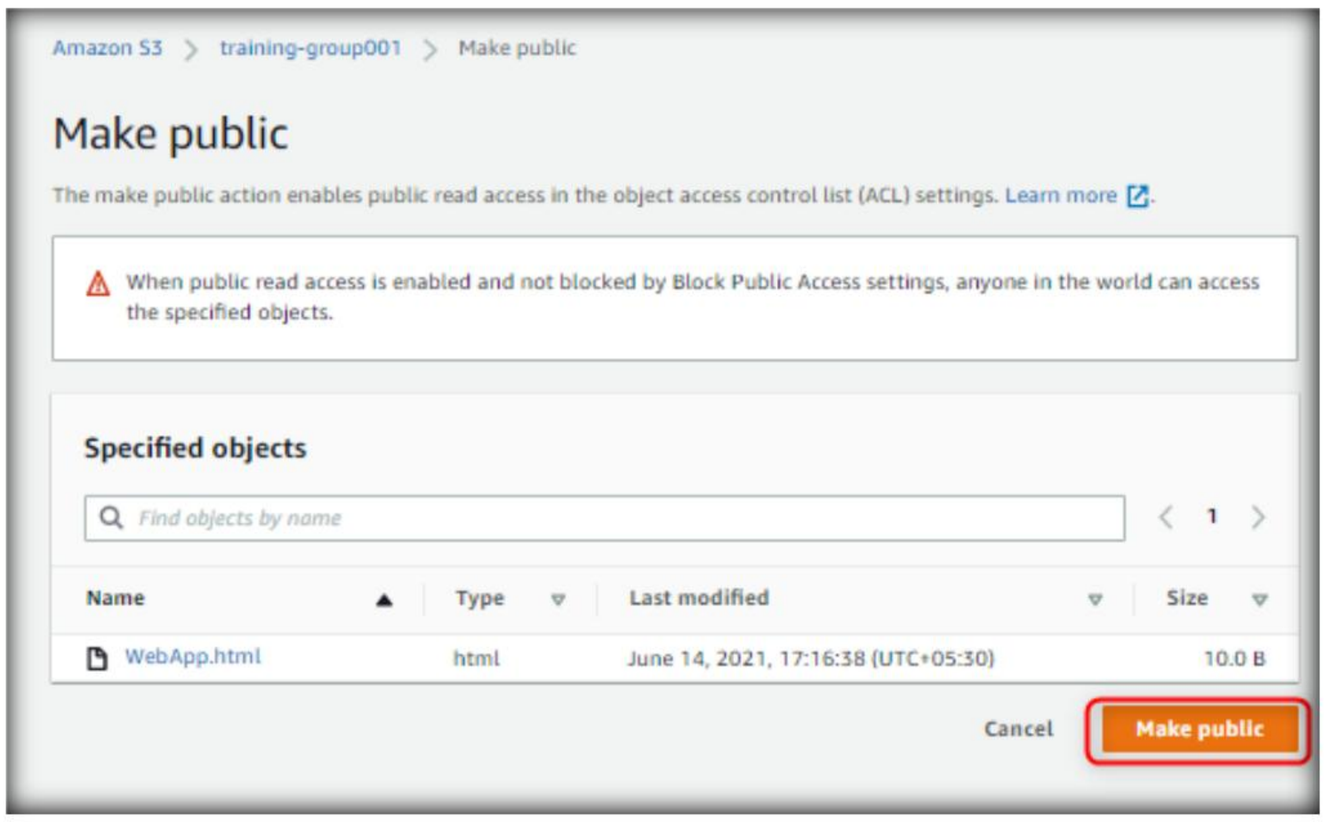


FIGURE 4.3.19: Updated Public Access

20. After the **Successfully edited public access** message appears, click on **Close**.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

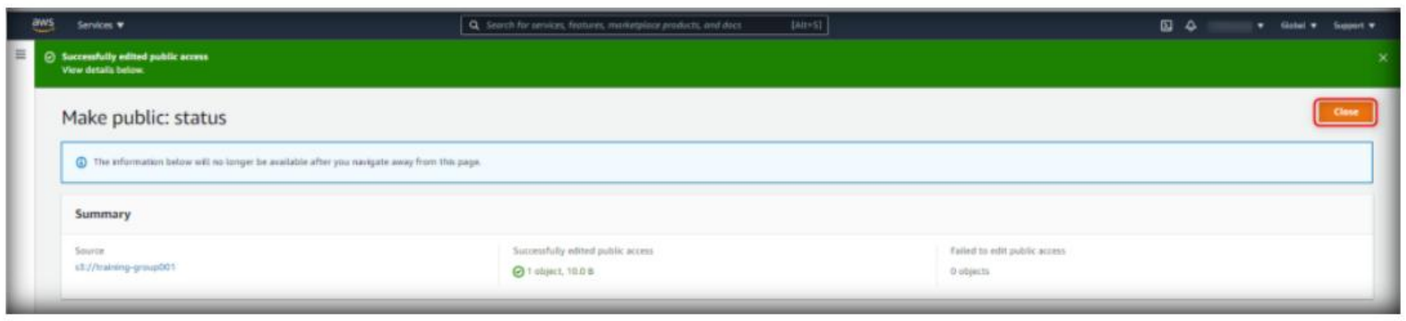


FIGURE 4.3.20: Make public: status

TASK 3

Verifying public access for the object Over the internet

21. Next, you will be returned to the **training-group001** bucket page. Click on the **WebApp.html** object under **Objects**.

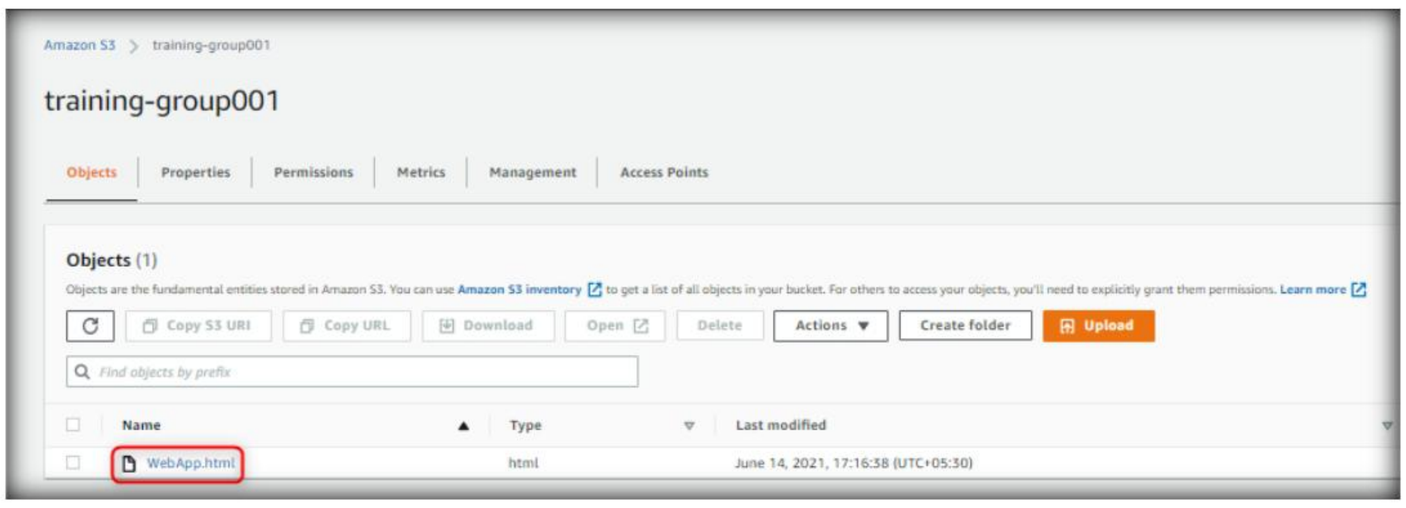


FIGURE 4.3.21: Selecting WebApp object

22. After the **WebApp.html** object page opens, you will see the **Object URL** which can be publicly accessed. Copy the URL.



FIGURE 4.3.22: Copying the Object URL

23. Open a new browser tab, paste the copied **Object URL** in the address bar, and press **Enter** to see the web page content.

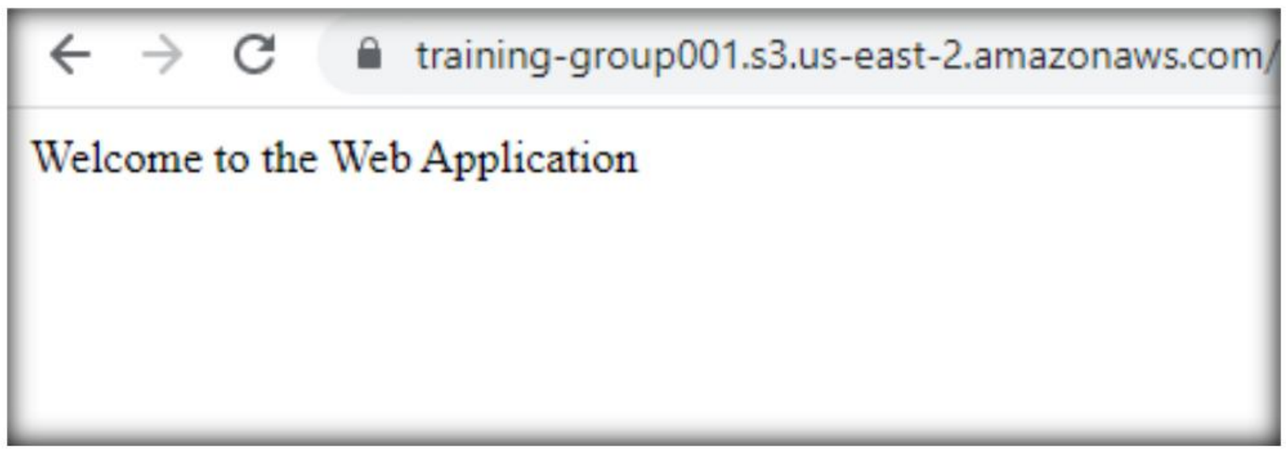


FIGURE 4.3.23: WebApp content

24. Observe the URL in the address bar. the lock icon in the URL indicates the page can be securely accessed.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

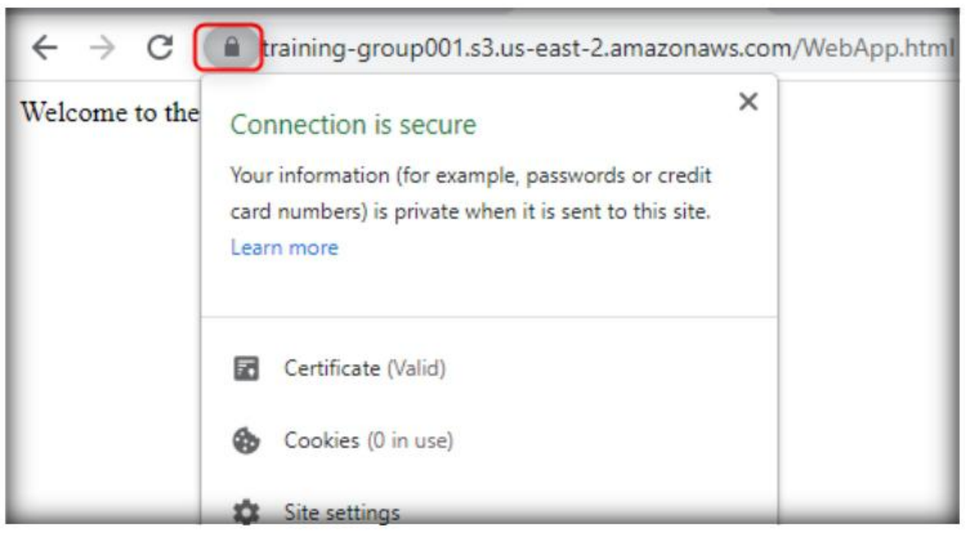


FIGURE 4.3.24: Secure Connection

25. Modify the URL from the **https** request to a **http** request and press **Enter**.

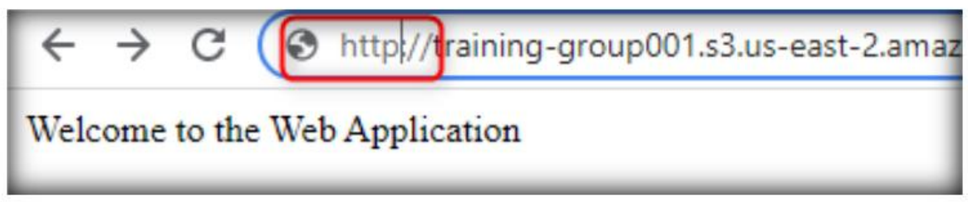


FIGURE 4.3.25: Making connection insecure

26. You will see the following page, which indicates the connection is not secure.

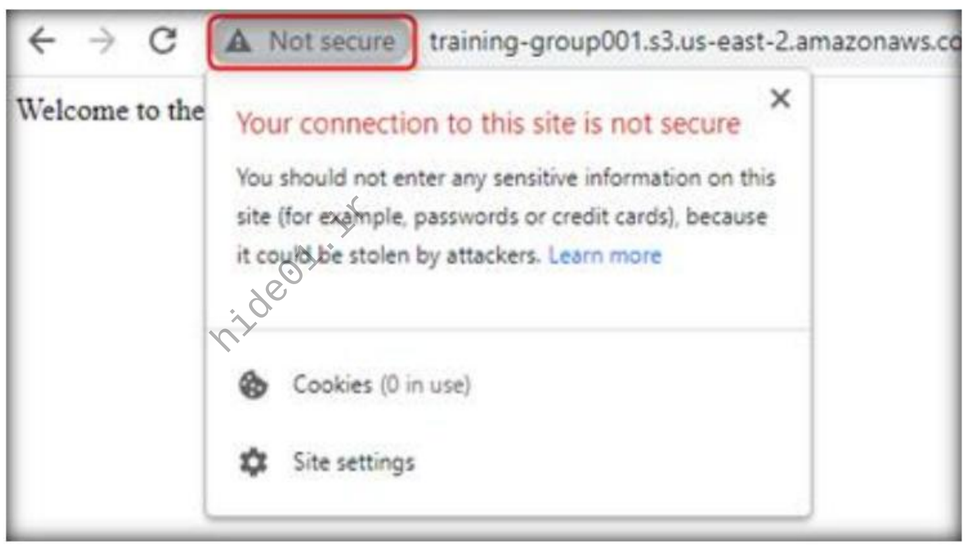


FIGURE 4.3.26: Insecure connection

TASK 4

Setting Secure Connection for the Object using bucket Policy

27. Now, implement a bucket policy that allows only secure connections (https) for publicly accessing the object.
28. Switch to the **Amazon S3** console and click on the **training-group001** bucket.

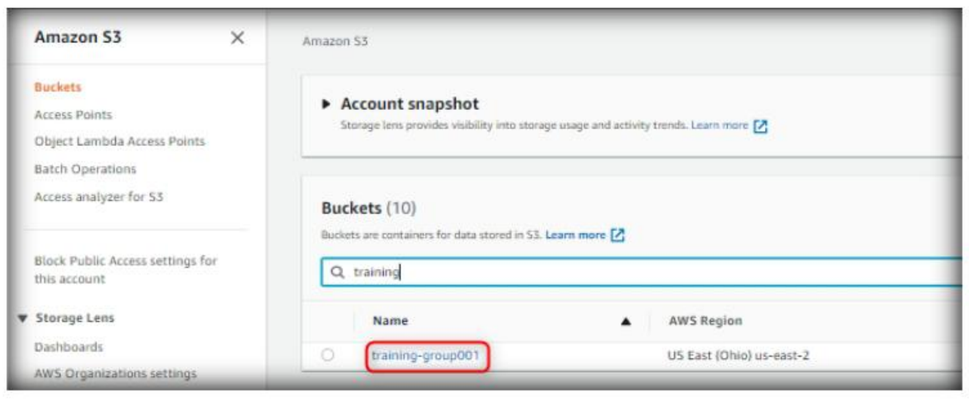


FIGURE 4.3.27: Choosing the bucket

Certified Cloud Security Engineer Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

29. Once the **training-group001** bucket page opens, click on the **Permissions** tab.

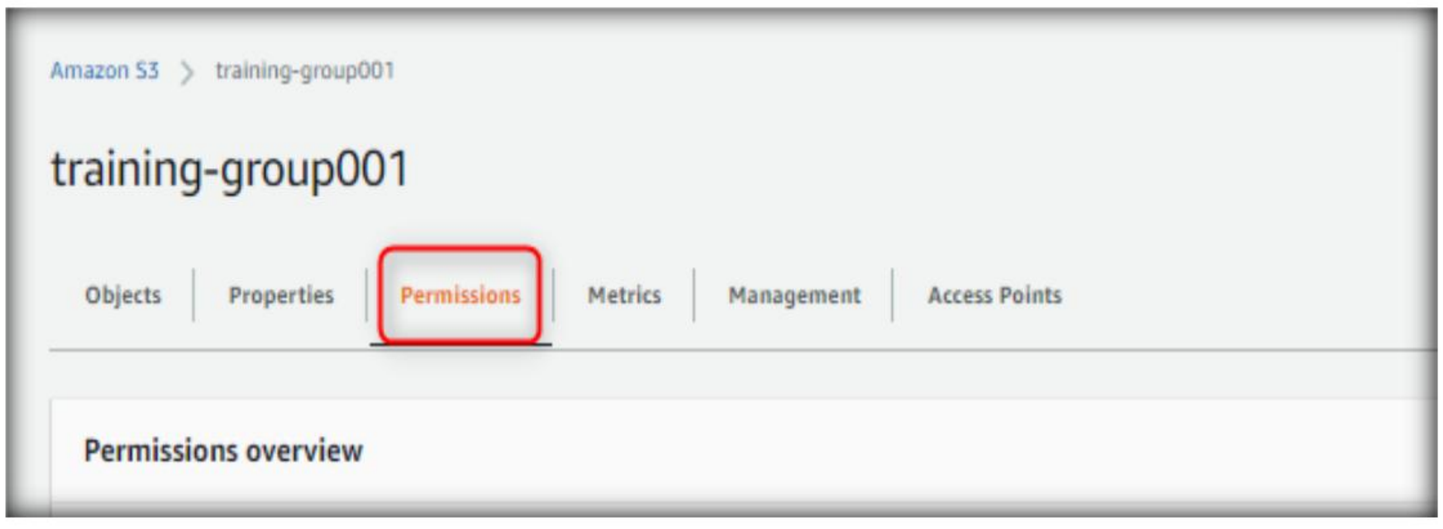


FIGURE 4.3.28: Selecting Permissions

30. Scroll down and click on **Edit** under **Bucket policy** section.



FIGURE 4.3.29: Editing Bucket policy

31. Copy the policy written below for the **training-group001** bucket and paste it in the **bucket policy editor**. Then, scroll down and click on **Save changes**.

```
{
   "Statement":[
      {
         "Action": "s3:*",
         "Effect":"Deny",
         "Principal": "*",
         "Resource":"arn:aws:s3:::training-group001/*",
         "Condition":{
            "Bool":
            { "aws:SecureTransport": false }
         }
      }
   ]
}
```


Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

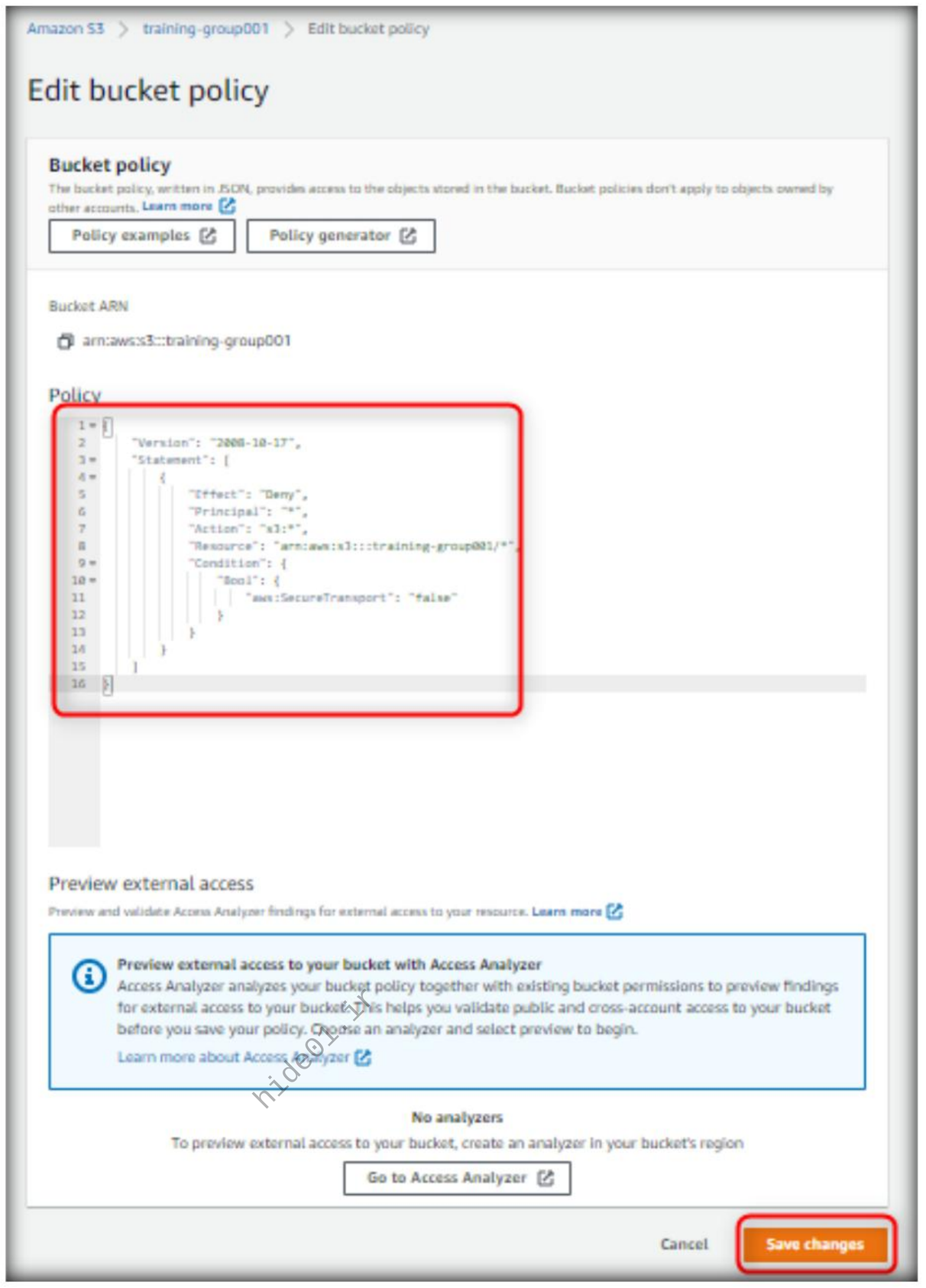


FIGURE 4.3.30: Editing bucket policy

32. The **Successfully edited bucket policy** message appears now.

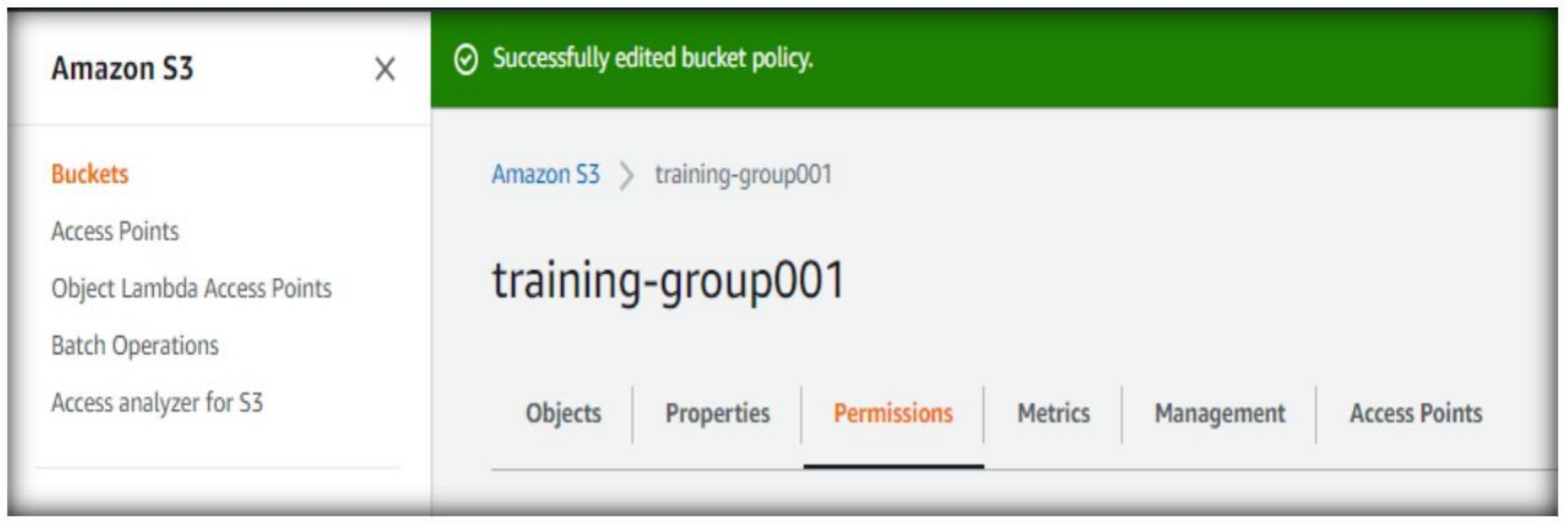


FIGURE 4.3.31: Bucket Policy Status

33. Next, verify the publicly accessible object's secure connection by repeating the **Steps 19–23**.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 5

Verifying Secure Connection for the Object over the Internet publicly

34. This time, you cannot view the content with a http connection because the access is denied.



FIGURE 4.3.32: Insecure Connection

35. If you access the content with a secure connection (**https**), then you can view the content. Type https:// in the beginning of the URL and press **Enter**.

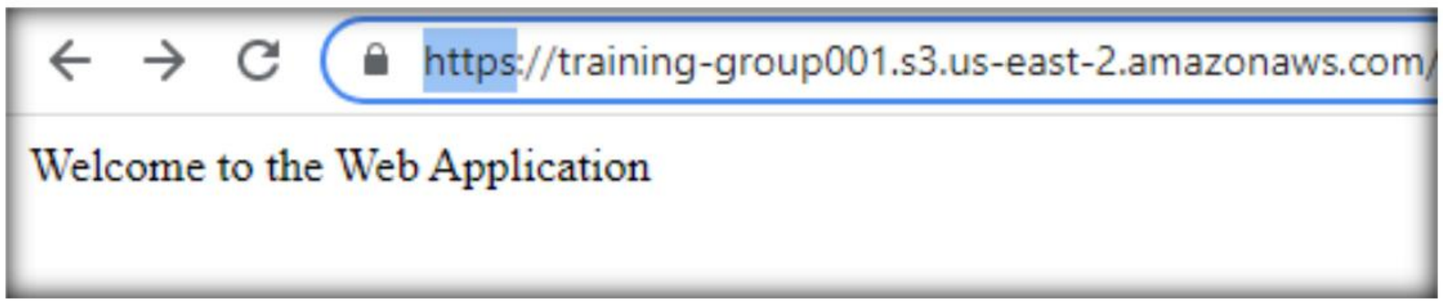


FIGURE 4.3.33: Secure Connection

36. This way, a cloud security engineer can restrict http connections to the objects in a S3 bucket using a bucket policy.

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

37. Now, delete the instances created in this lab. Navigate to **Buckets** under Amazon S3 and select the checkbox for the bucket created in this lab (here, **training-group002**). Click on the **Empty** button to empty the bucket before deleting it. In the pop-up window, enter permanently delete and click on the **Empty** button.

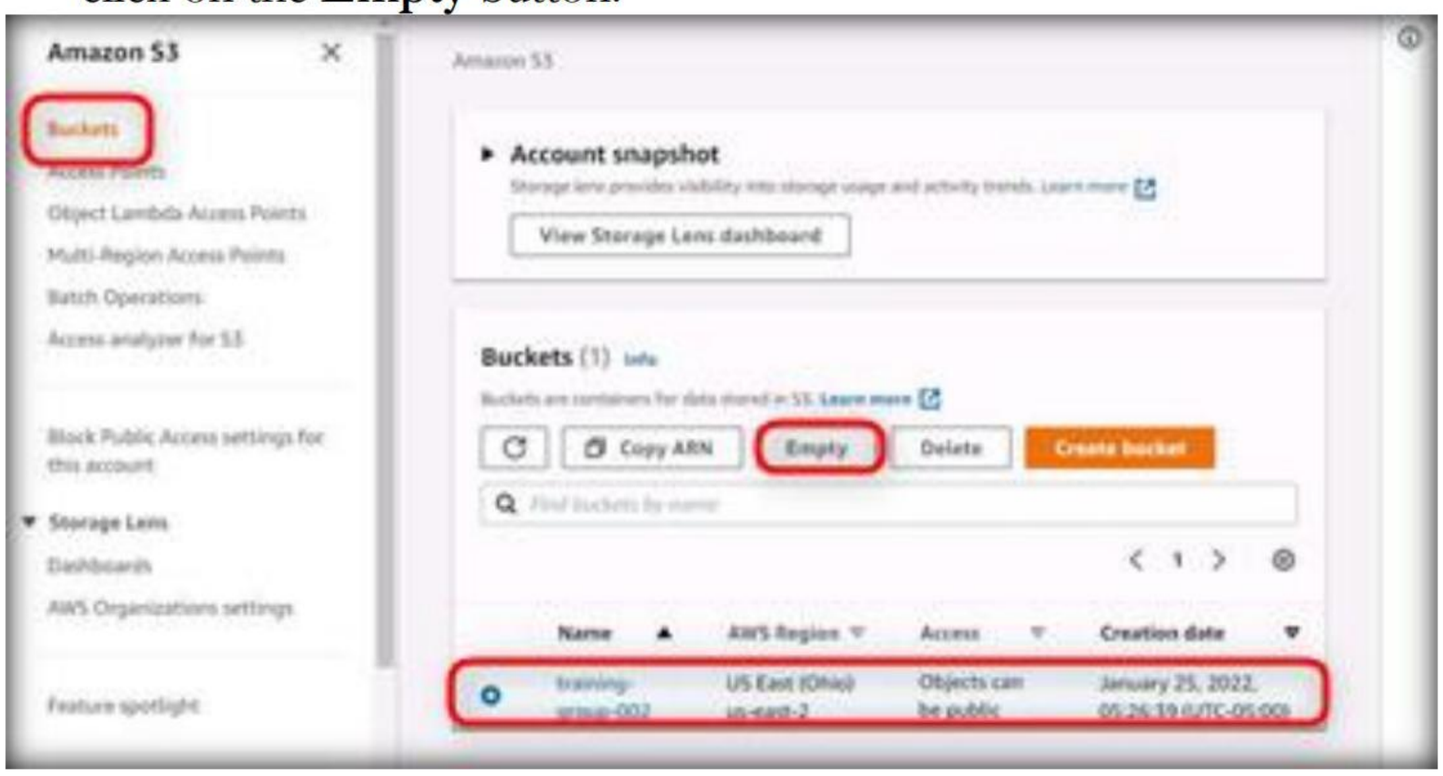


FIGURE 4.3.34: Empty Bucket

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

38. Navigate to **Buckets** under Amazon S3 and select the checkbox for the bucket created in this lab (here, **training-group002**). Click on the **Delete** button. In the pop-up window, enter the bucket's name and click on the **Delete** button.

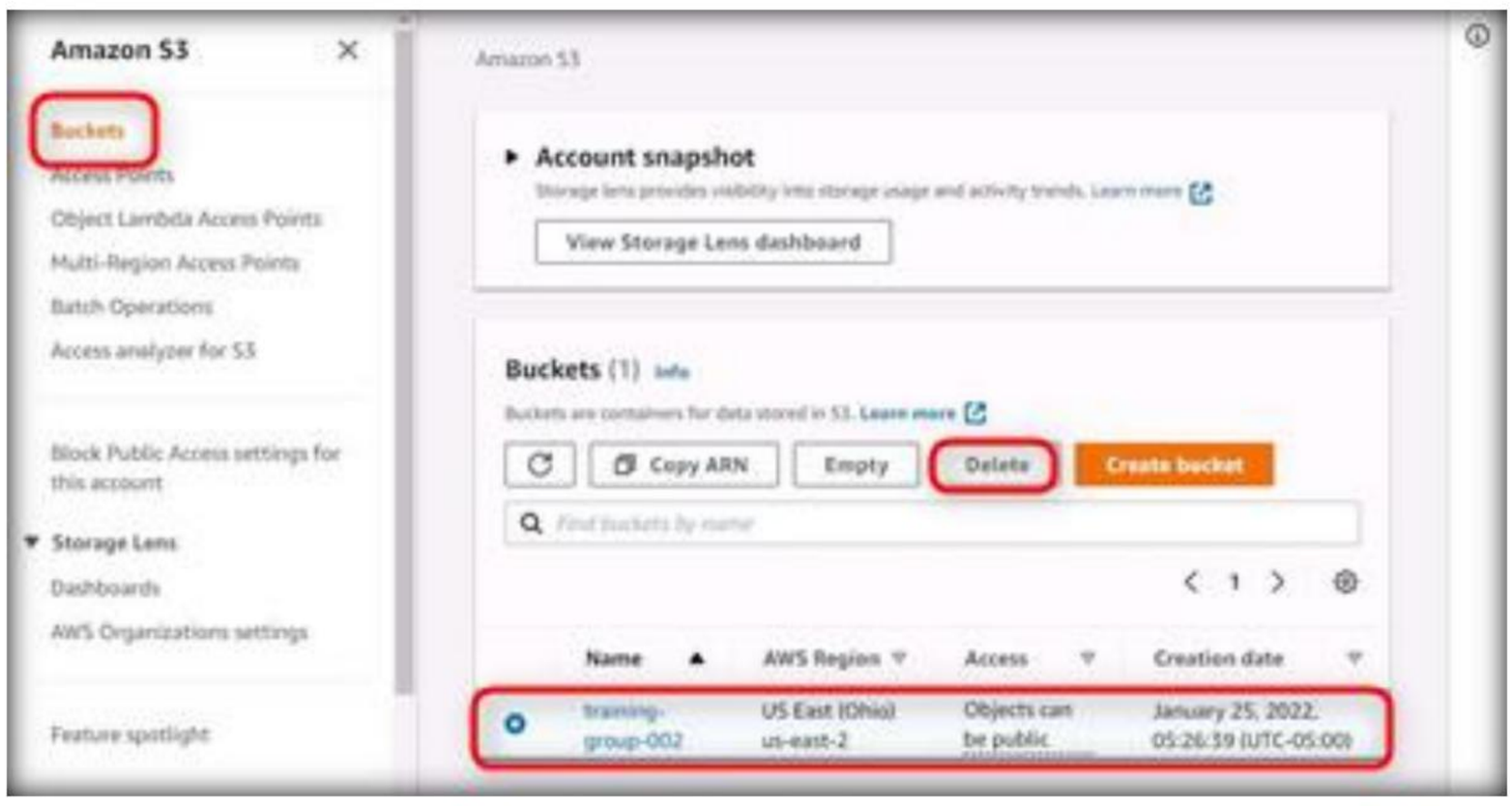


FIGURE 4.3.33: Deleting Bucket

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.

hi@01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 4

Securing Amazon RDS from Accidental Deletion

Amazon relational database service (RDS) can be protected from any accidental deletion by enabling the deletion protection feature while creating the database. Creating a snapshot of the database helps in disaster recovery.

Lab Scenario

ICON KEY

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

Amazon relational database service (RDS) can be used by a cloud security engineer to create a secure relational database in the cloud. To ensure the security of the relational database, a cloud security engineer should configure the RDS with the available features. Amazon RDS provides an accidental deletion feature, which can be enabled while creating a database. A cloud security engineer can also take a snapshot of the database, which can be used for disaster recovery. This lab demonstrates how to enable and verify the accidental deletion feature of Amazon RDS. This lab also includes the creation of a database snapshot for disaster recovery.

Lab Objectives

This lab will demonstrate how to secure Amazon RDS by enabling deletion protection and create database snapshots.

In this lab, you will learn to do the following:

- Create a MySQL database in Amazon RDS with deletion protection
- Create an Amazon RDS snapshot
- Verify deletion protection of the RDS

Lab Environment

To perform this lab, you need the following:

- **Admin Machine** VM
- **Administrative** privileges to run the tools
- Registered AWS account

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Duration

Time: 10 minutes

Overview of Amazon RDS

Amazon relational database service (RDS) can be used by a cloud security engineer to create a secure relational database in the cloud. Amazon RDS ensures better security and availability for the applications. Amazon RDS provides database engines such as Amazon Aurora, PostgreSQL, MySQL, MariaDB, Oracle Database, and SQL Server for the users. The database instances can be isolated with Amazon RDS by running them in Amazon virtual private cloud (VPC). Disaster recovery can be implemented by creating a snapshot of the Amazon RDS. Amazon RDS has encryption features for securing the database and snapshots. Accidental deletion of database snapshots by a cloud security engineer or any other user can also be prevented by enabling the deletion protection feature when creating a database.

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., AWS), the application interface may be updated with time. Hence, in case you happen to work on an updated version of AWS, 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.

Module 01 - 1

Note: Before starting this lab, you should create an AWS Free Tier account using the following link: https://aws.amazon.com/free/, in case you have already not created it for the previous module. Once the registration is complete, perform the following task:

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

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1

Creating a MySQL Database in Amazon RDS with Deletion **Protection**

1. Log in to the **Admin Machine** VM with the user **Admin** and password **admin@123**.

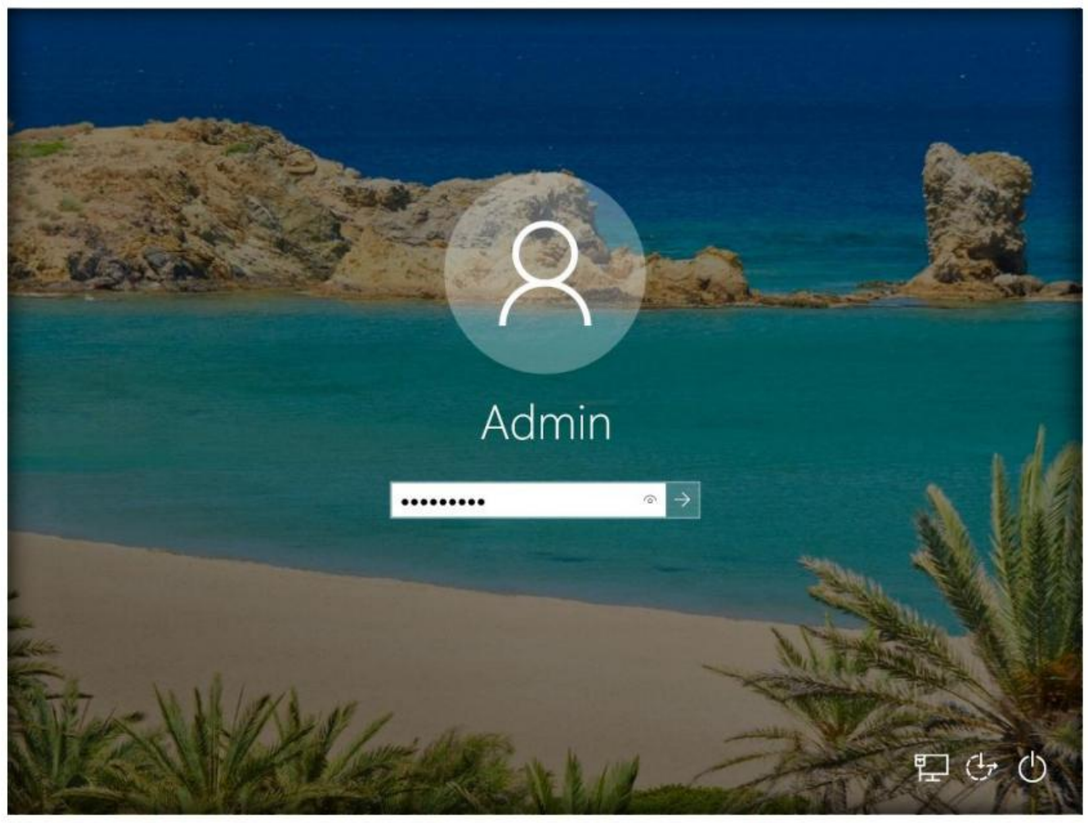


FIGURE 4.4.1: User Login

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



FIGURE 4.4.2: Navigating to the Chrome Browser from Taskbar

3. The **Google Chrome** browser appears. Go to the address bar, type **https://aws.amazon.com/**, and press **Enter.**

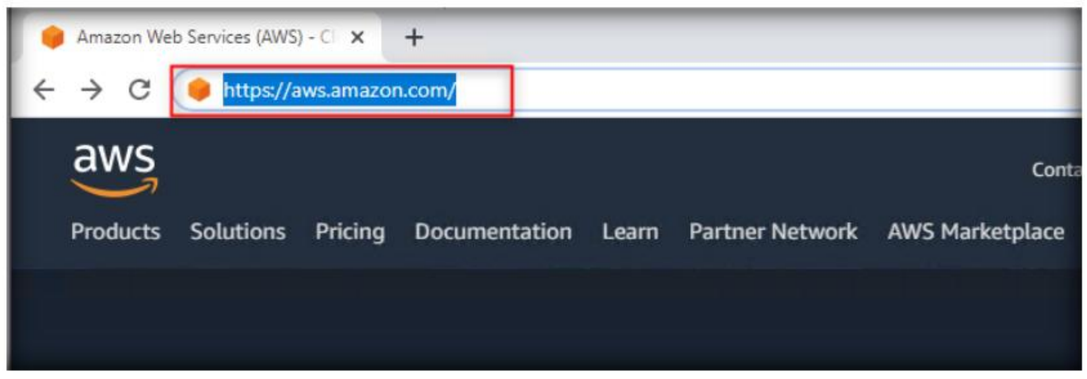


FIGURE 4.4.3: Access AWS in Browser

Note: If you are already logged in, skip the login steps.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

4. The **AWS Web Services - Cloud Computing Services** page appears. Click on the **AWS Management Console** from the **My Account** dropdown, as shown in the screenshot below.

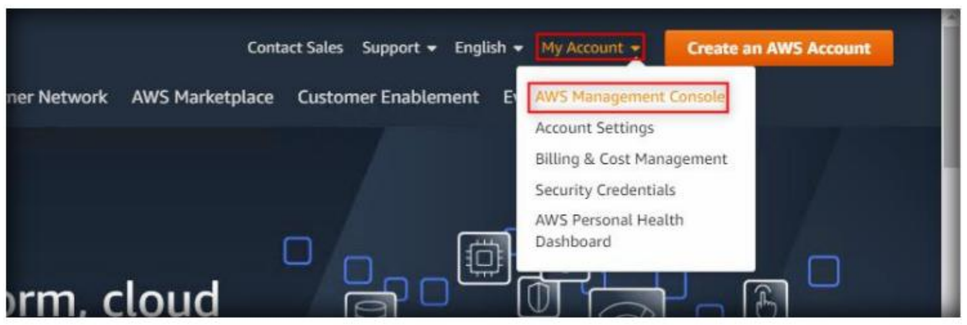


FIGURE 4.4.4: Navigate to AWS Management Console

5. The **AWS Web Services Sign-in** page appears. Choose **Root user** and type the AWS administrator account ID (Root user email address), as shown in the screenshot below, and then click on **Next**.

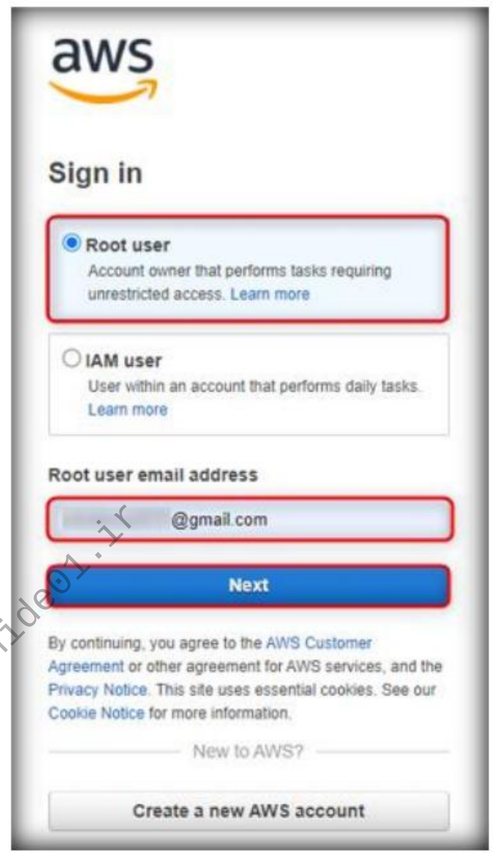


FIGURE 4.4.5: Sign-in to AWS

6. In the security check page that appears, type the characters shown in the image and click **Submit**.

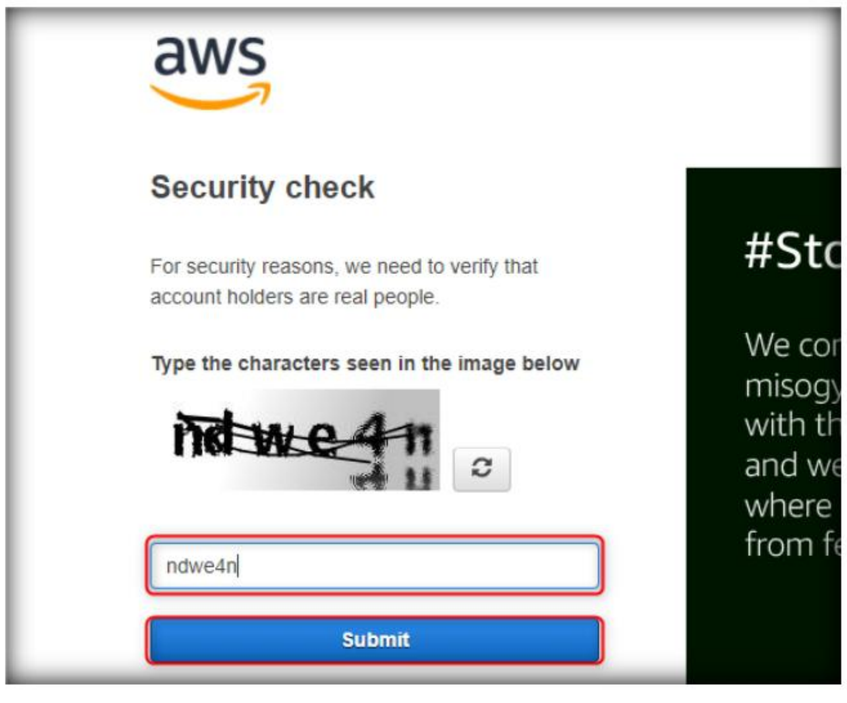


FIGURE 4.4.6: Typing the Characters for Security Check

7. In the **Password** field, type the password and click on **Sign in**.

Certified Cloud Security Engineer Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

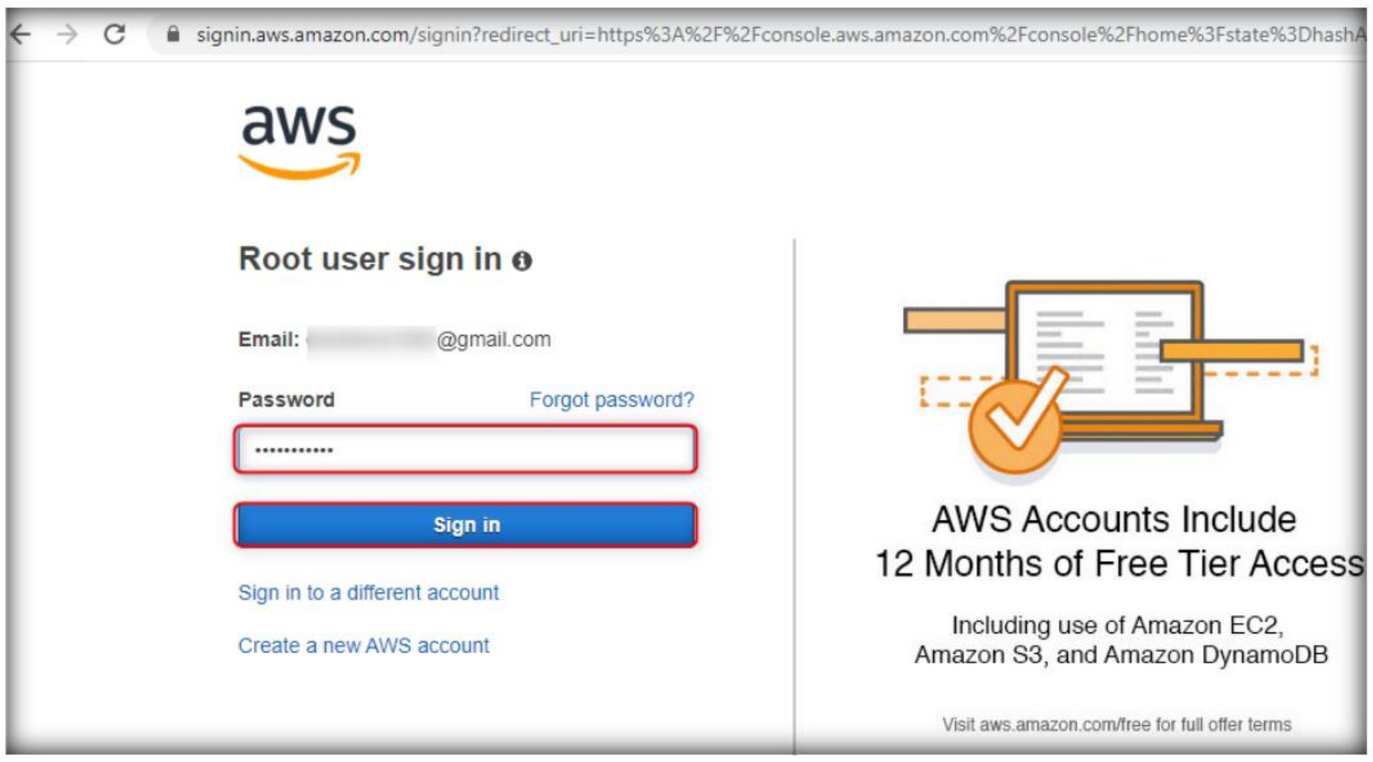


FIGURE 4.4.7: Sign-in to AWS

8. Now, to create a MySQL database in Amazon RDS, click on **Services**. In the services pane that opens, click on **RDS** under the **Database** section.

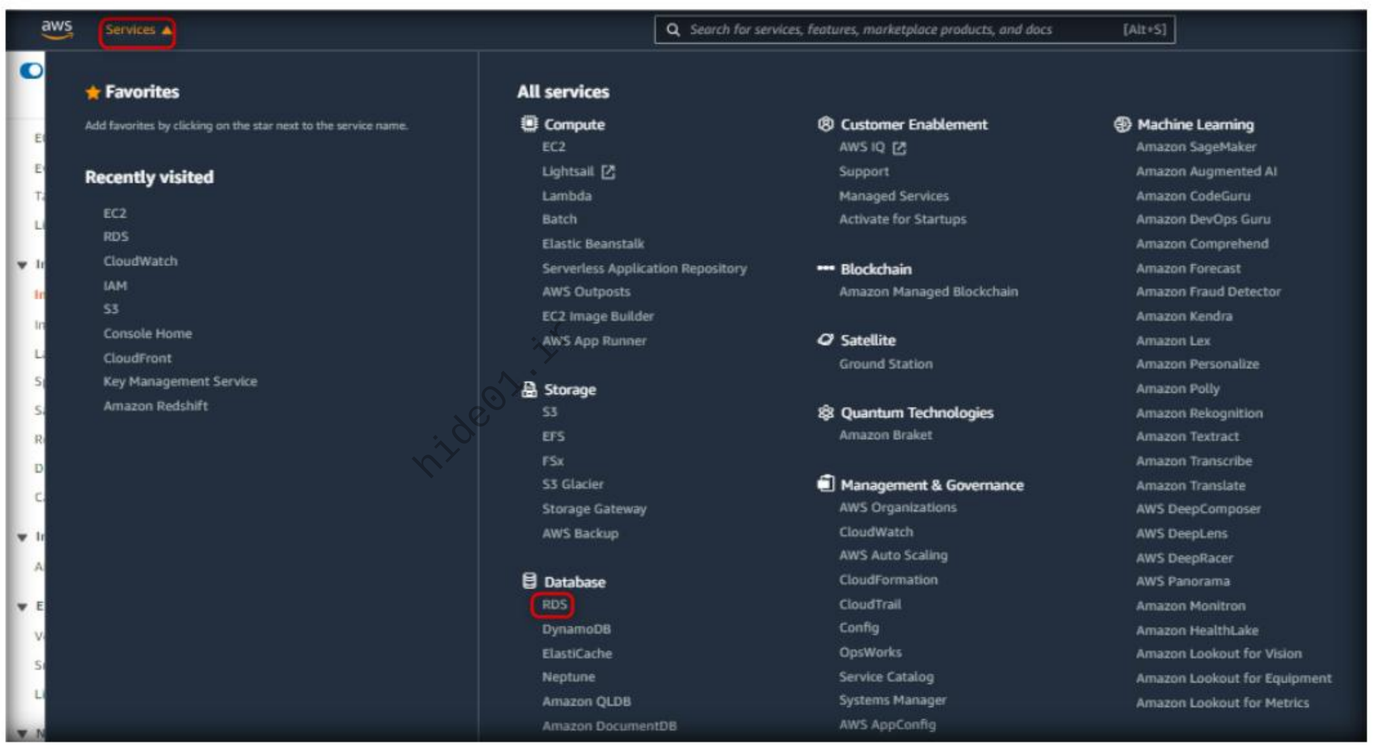


FIGURE 4.4.8: Selecting Service

9. In the **Amazon RDS** window, click **Create database**.

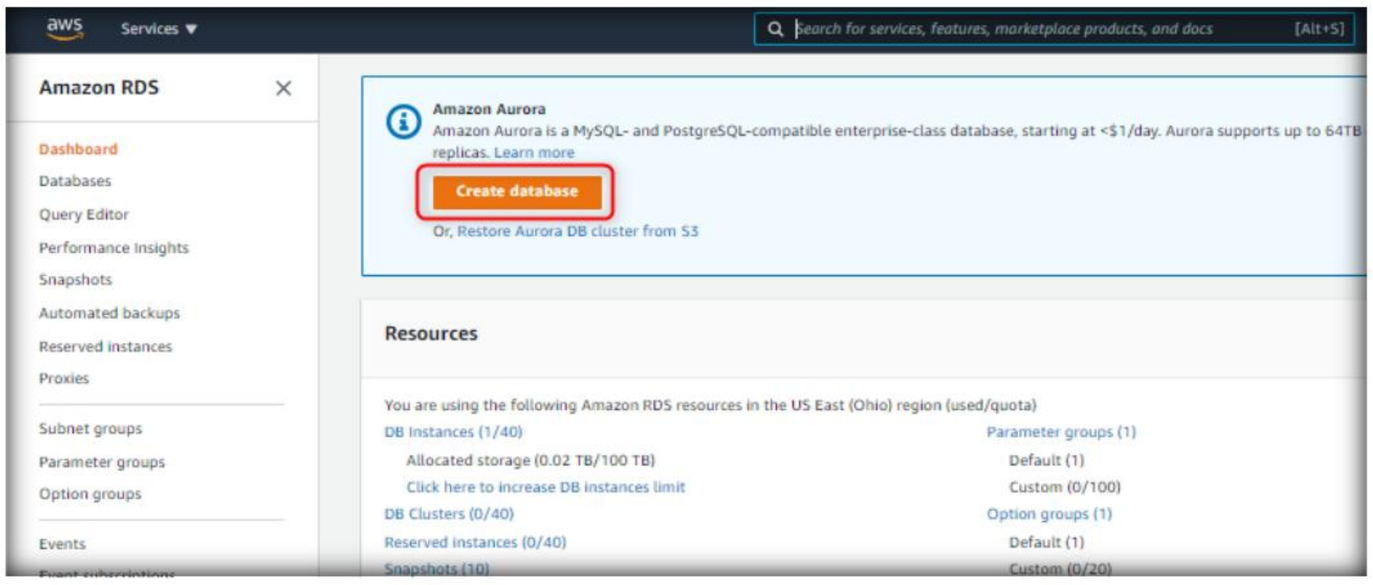


FIGURE 4.4.9: Select Create database

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

10. Once the **Create database** window appears, choose the database creation method as **Standard create**. For **Engine Option,** select the radio button for **MySQL** to select MySQL as the RDS database engine.

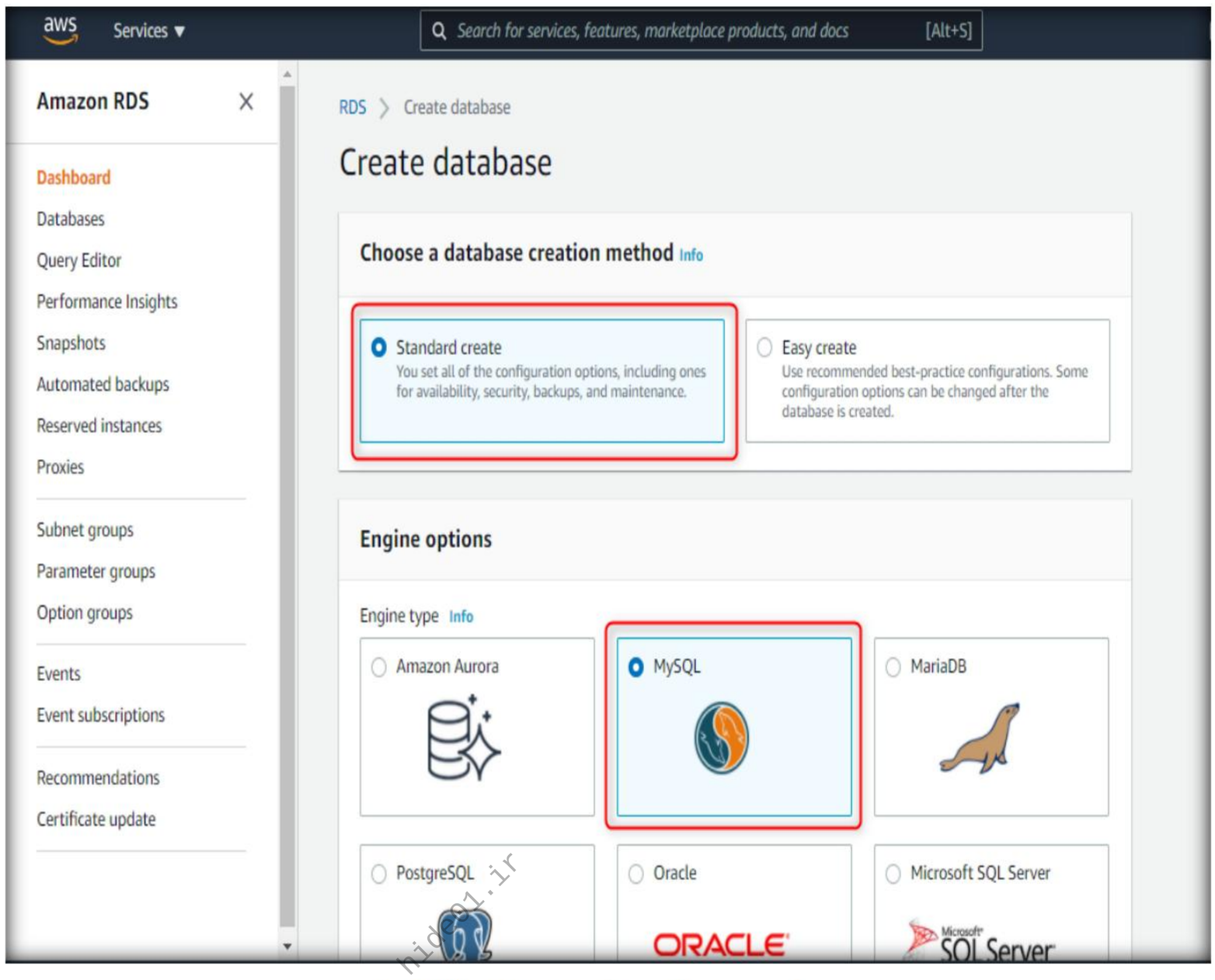


FIGURE 4.4.10: Configure database settings

11. Scroll down to the **Templates** section and select **Free tier**.

Note: The Production option gives some extra features but also entails some costs. Therefore, choose the **Free tier** option here.

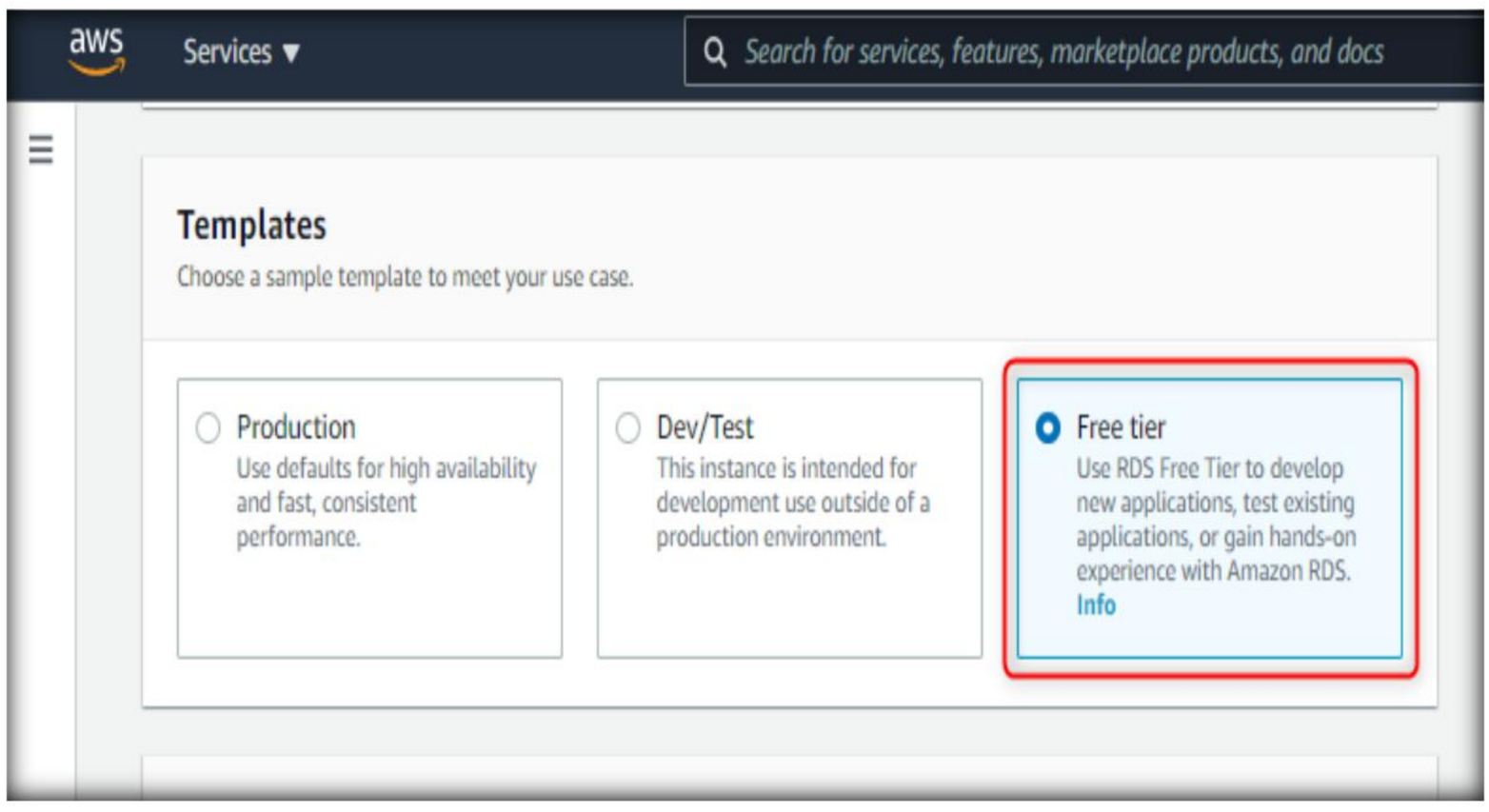


FIGURE 4.4.11: Configure database settings

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

12. Next, scroll down to the **Settings** section and type **eccblogdb** as the DB instance identifier**.** Under **Credentials Settings,** type a **Master username** (here, **admin**) and a strong password (here, **Qzxcvqwerty**) under **Master password**.

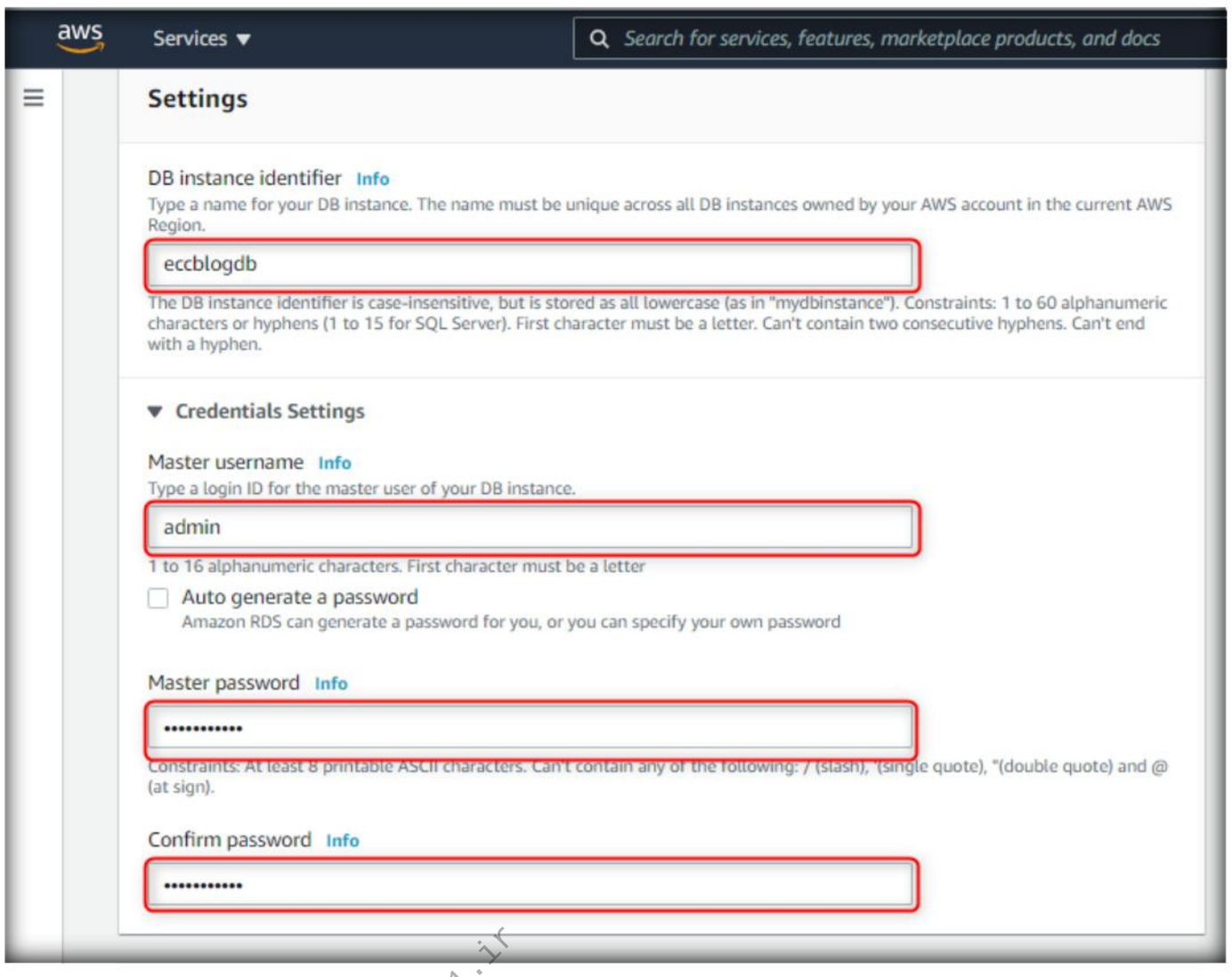


FIGURE 4.4.12: Configure database settings

13. Scroll down to the **Connectivity** section. To disable public access for the database, select the **No** radio button for **Public access**. If the database is publicly accessible, several tools can be used to scan the DB ports in a public network and your data may be compromised.

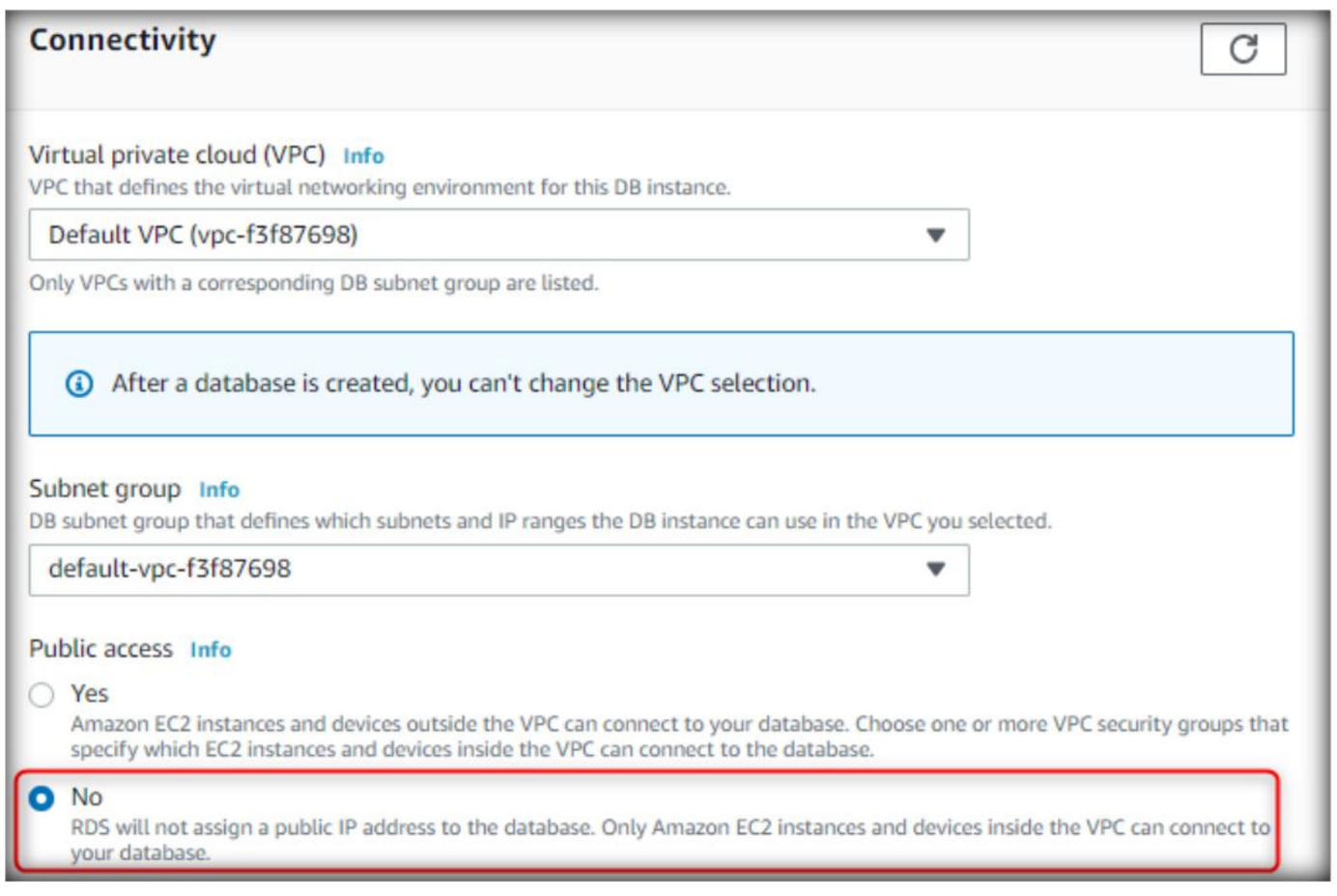


FIGURE 4.4.13: Configure database settings

hidoo1.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

14. Now, restrict access to the DB using a VPC security group. Scroll down and select the radio button for **Create new** under the **VPC security group** section. Type a name (here, **eccusersecuritygroup**) under **New VPC security group name**.

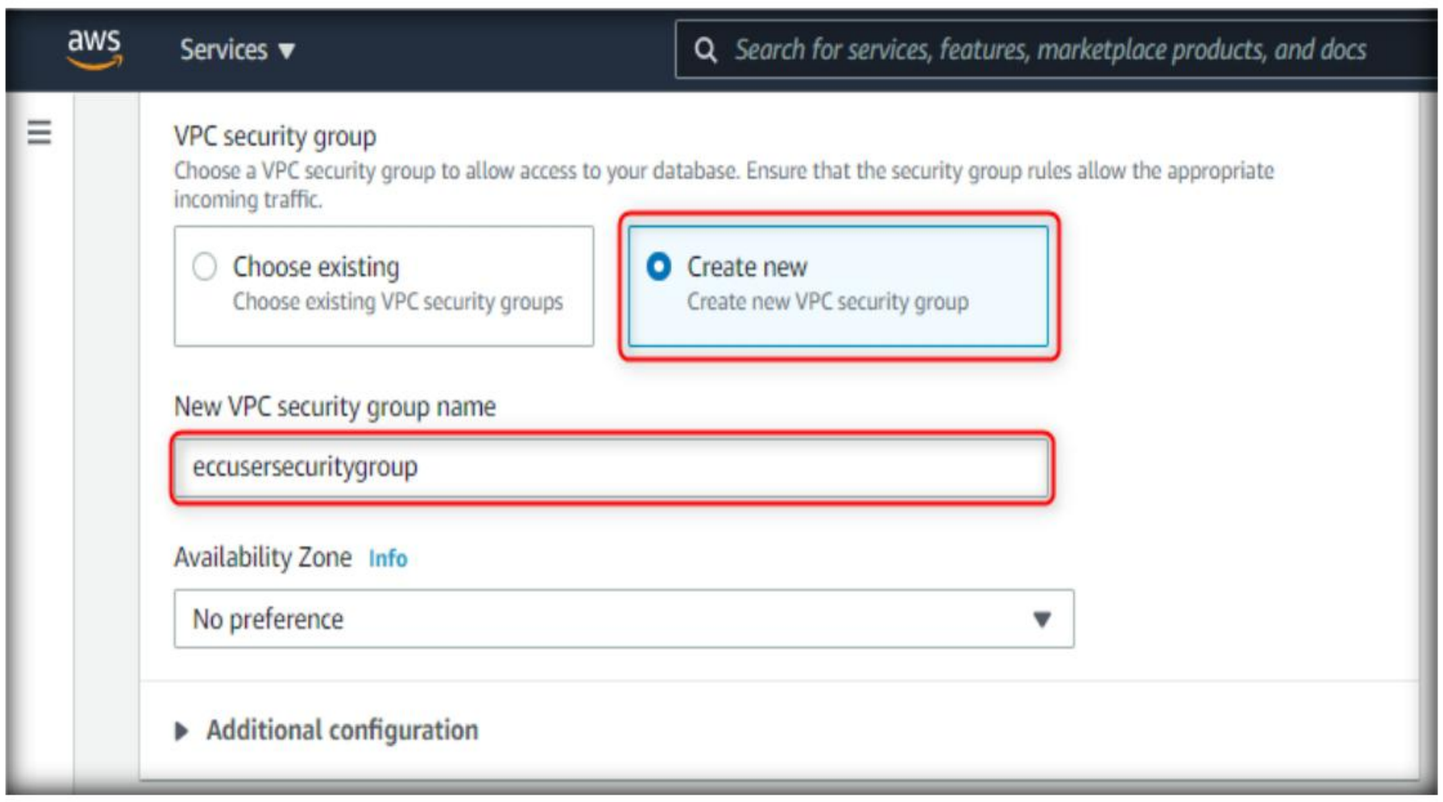


FIGURE 4.4.14: Configure database settings

15. Next, scroll down to the **Additional configuration** section and expand it. Type a name (here, **eccblogdb**) under **Initial database name.** To create a snapshot of the database, select **Enable automatic backups** for **Backup**.

hide01.ir

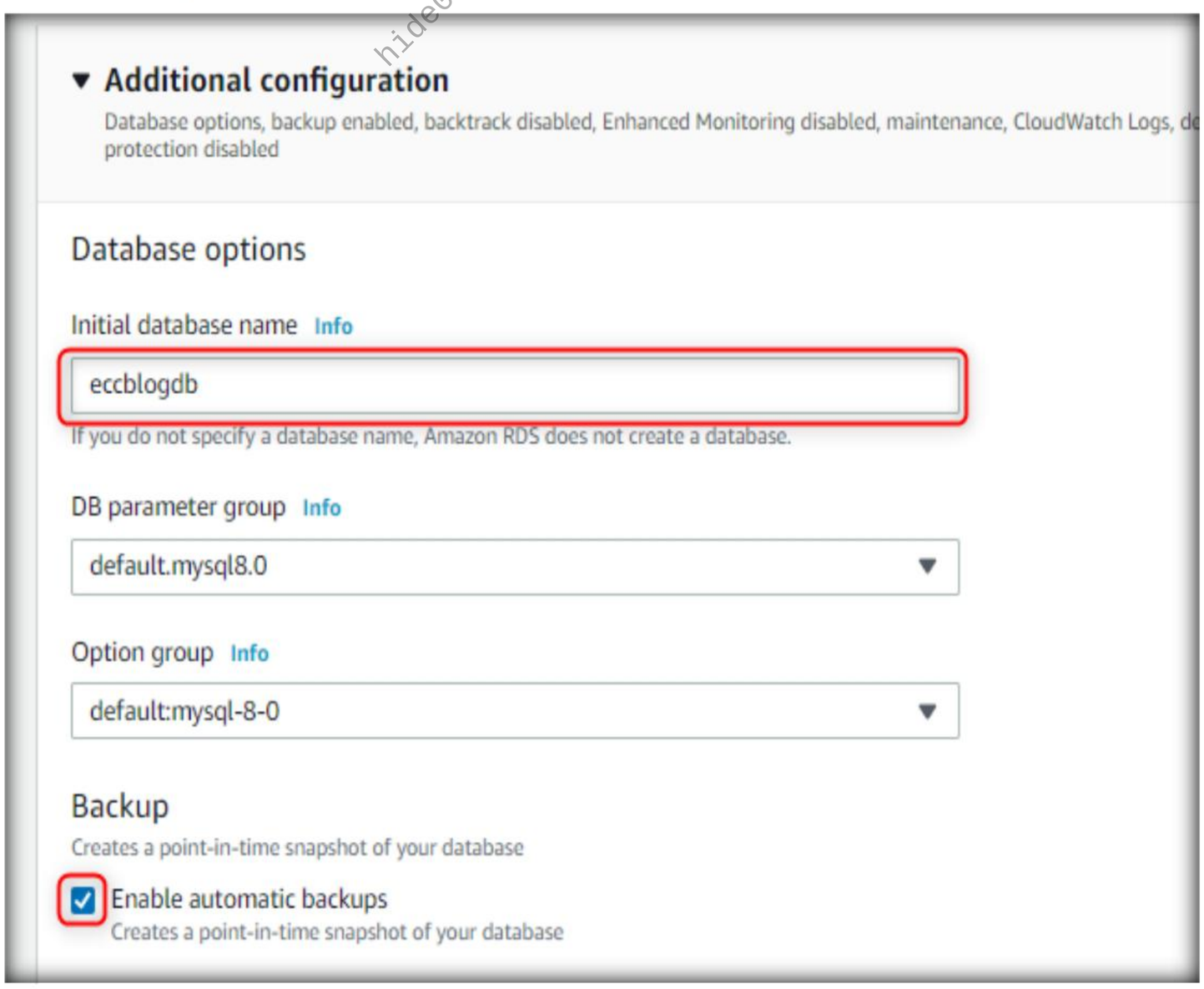


FIGURE 4.4.15: Configure database settings

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

16. Now, to protect the database from accidental deletion, scroll down and select the checkbox for **Enable deletion protection** under **Deletion protection**. Then, click on **Create database**.

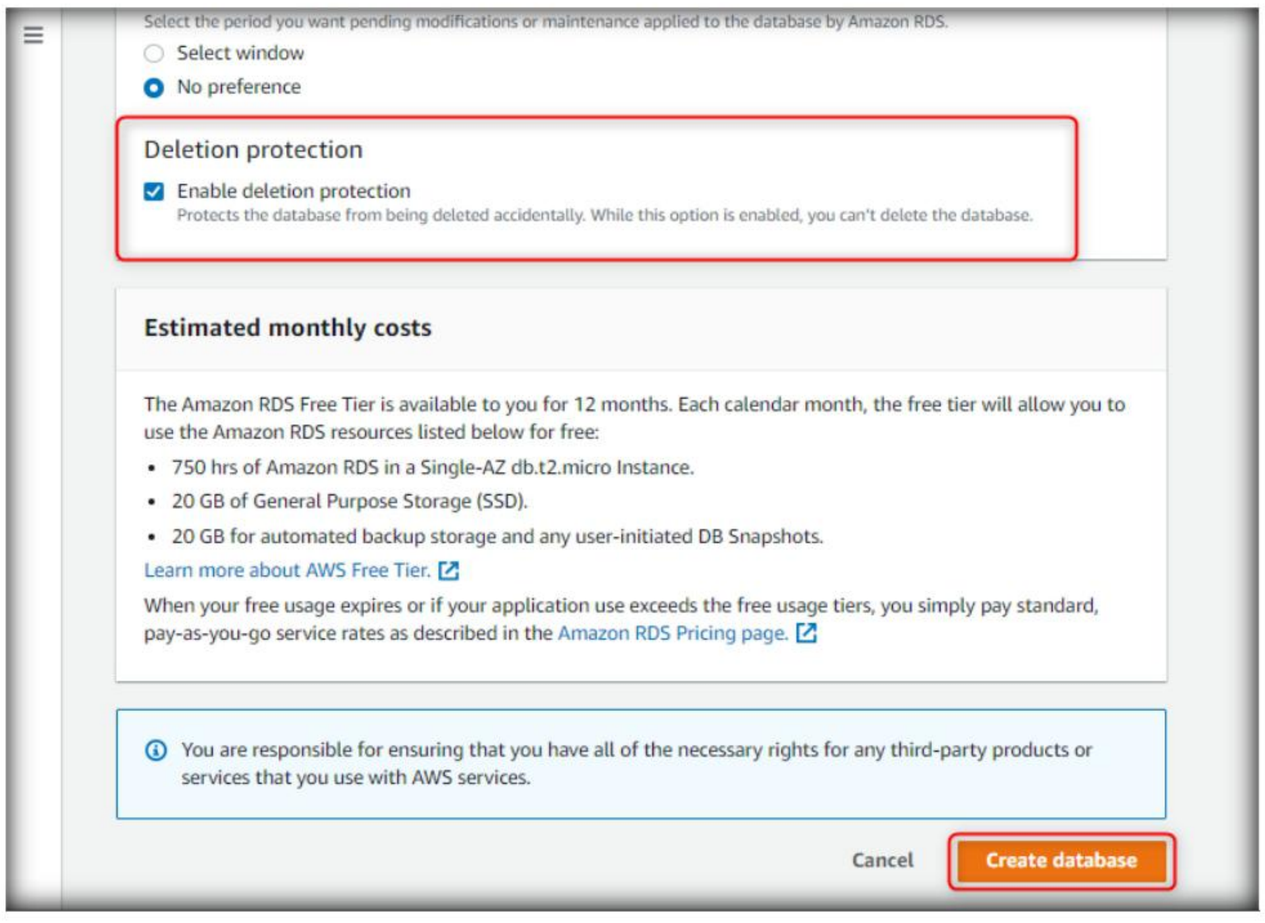


FIGURE 4.4.16: Configure database settings

17. Wait for a few seconds for the database to be created.

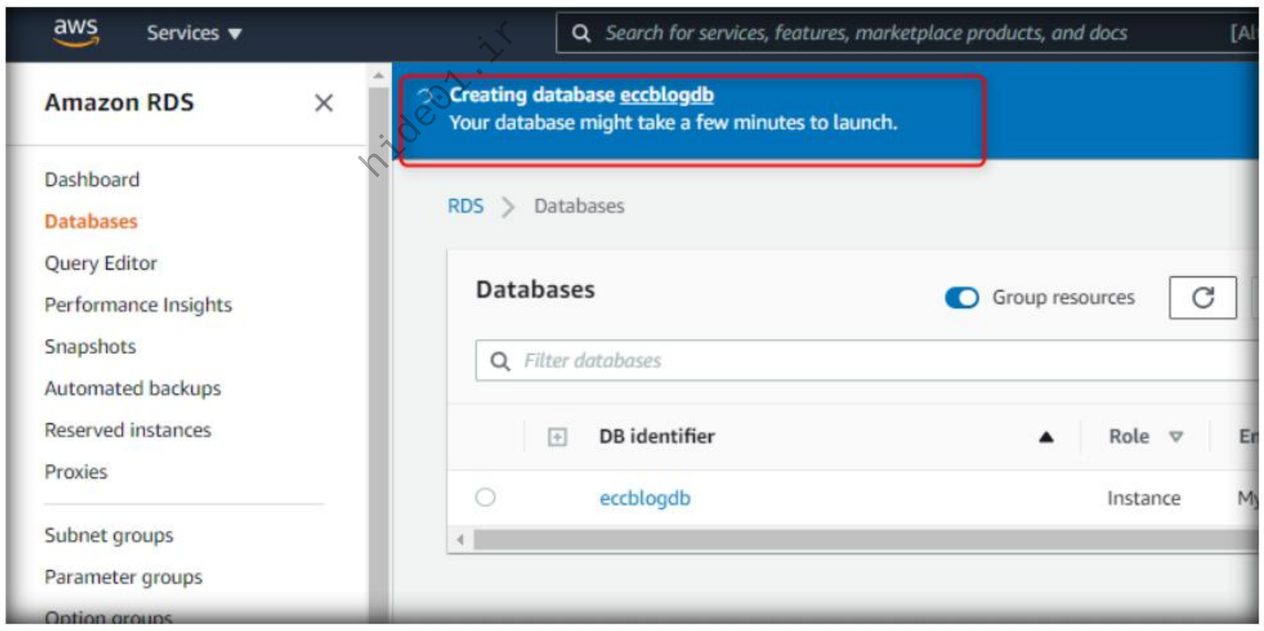


FIGURE 4.4.17: Database Creation in Progress

18. After a few minutes, the database will be created, as shown in the following screenshot.

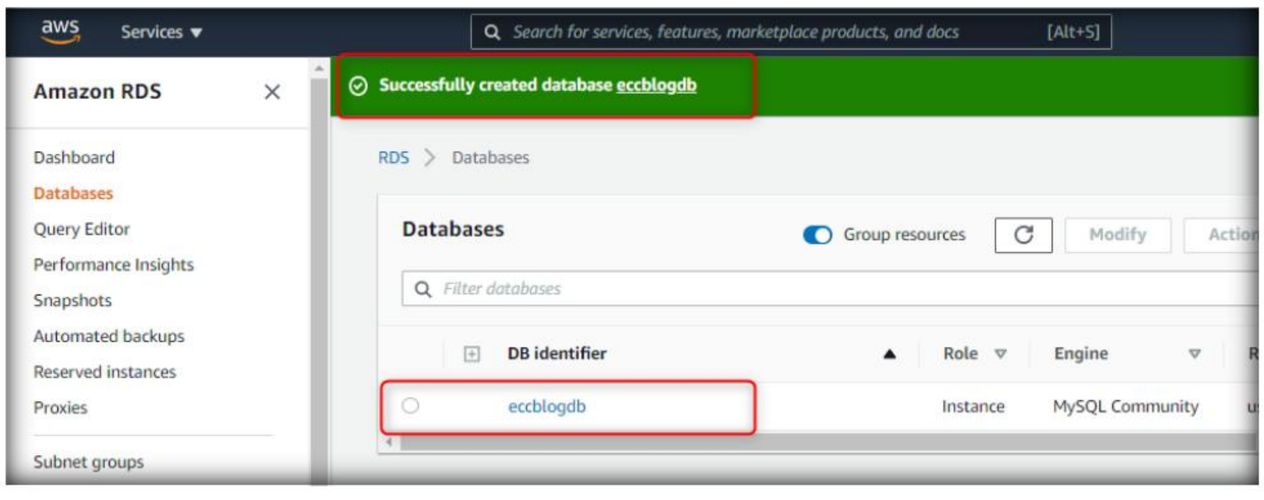


FIGURE 4.4.18: Database Created

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 2

Creating Amazon RDS Snapshots

19. Next, to create a snapshot of the database (**ecclogdb**), select the radio button for the database **(eccblogdb)** you created. Then, click on the **Actions** dropdown button and choose **Take Snapshot**.

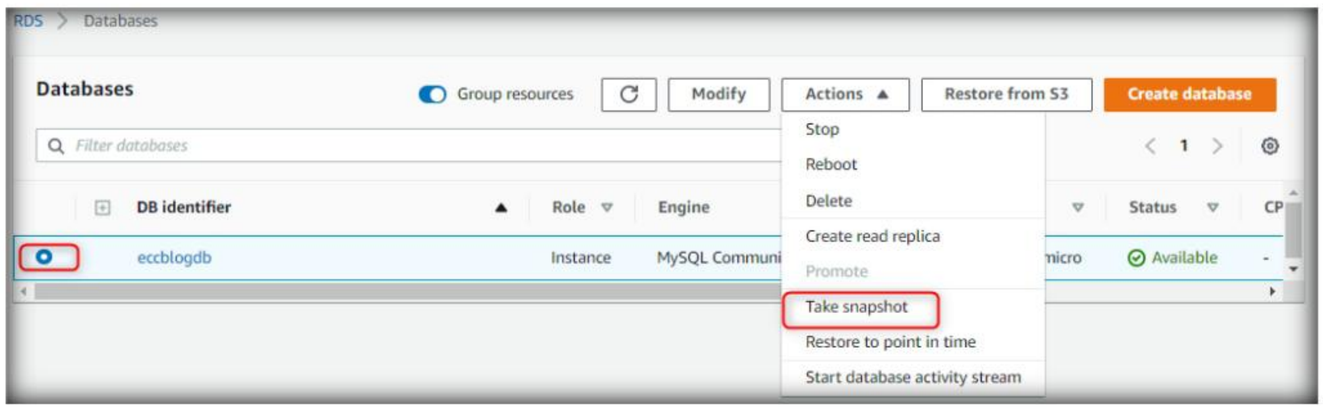


FIGURE 4.4.19: Choosing Take snapshot

20. Under Settings, type an appropriate snapshot name (here, **snap-eccblogdb)** and click **Take snapshot**.

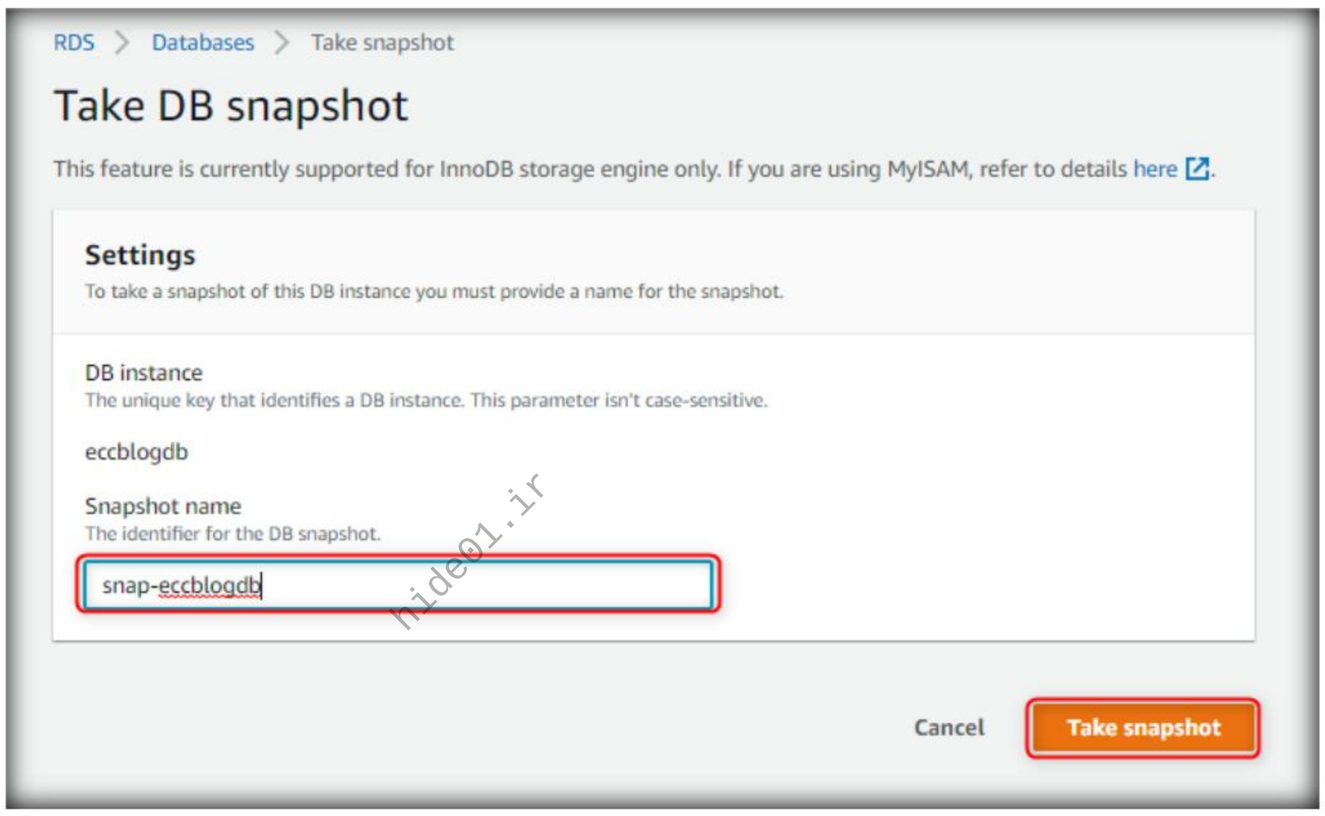


FIGURE 4.4.20: Taking Database Snapshot

21. An Amazon RDS snapshot will be created, as shown in the following screenshot.

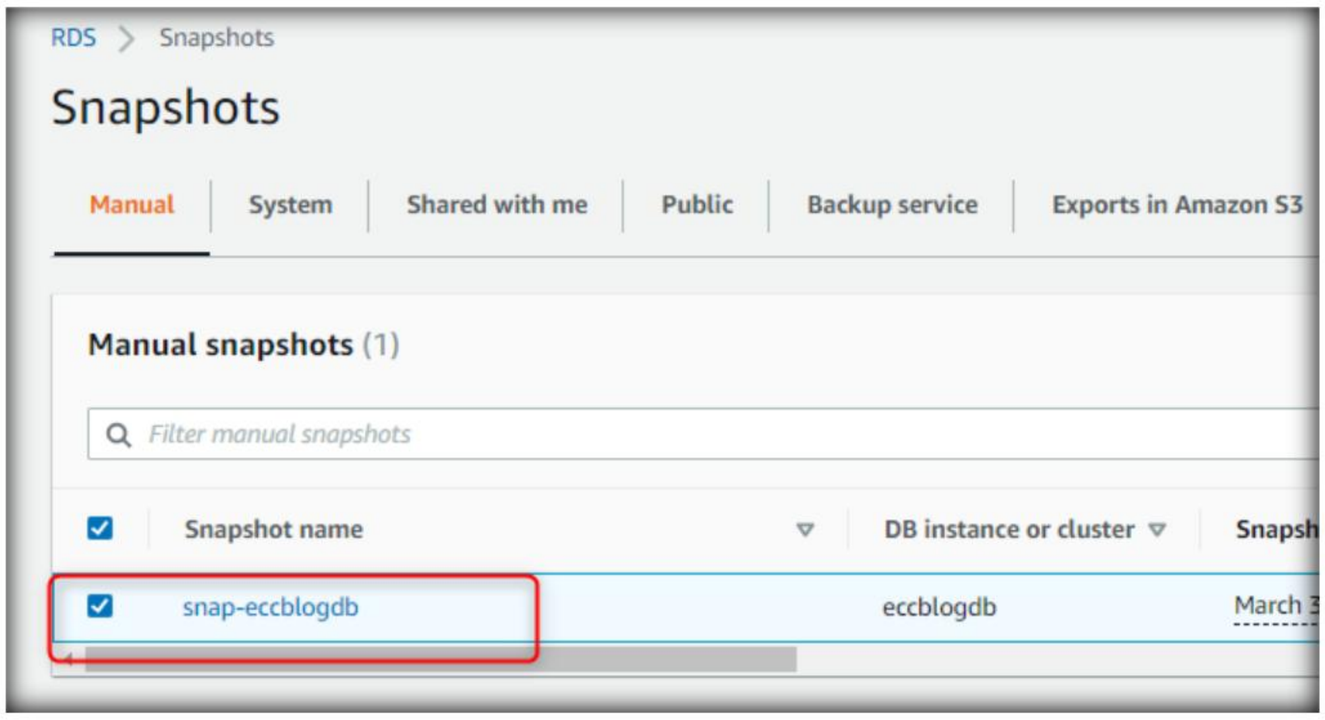


FIGURE 4.4.21: RDS Snapshot Created

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

22. After waiting for a few minutes, you can enable encryption and create a copy of the snapshot. To do this, select the checkbox for the newly created snapshot (**snap-eccblogdb**). Then, click on the **Actions** dropdown and choose **Copy snapshot**.

    Note: If the options are disabled in the **Actions** dropdown, wait for a few minutes and then refresh.

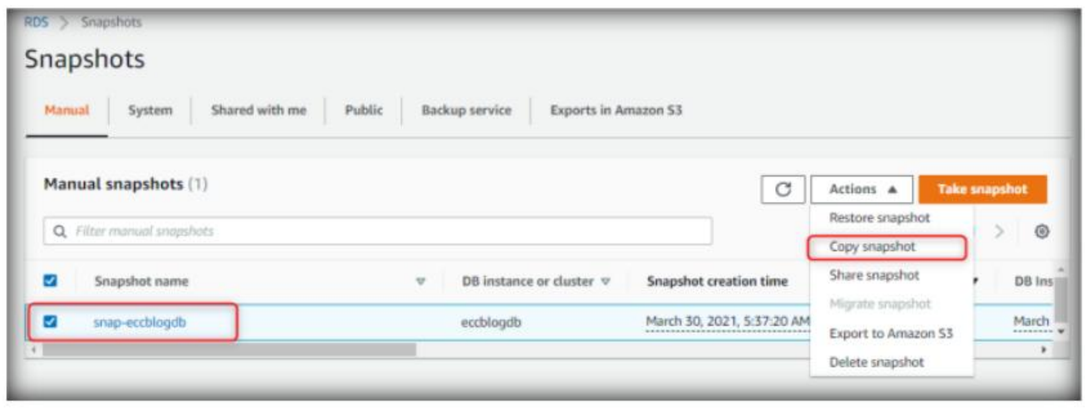


FIGURE 4.4.22: Copying Snapshot

23. On the **Copy snapshot** page, type a name for **New DB Snapshot Identifier** (here, **eccblog-snp-cpy1**) and scroll down.

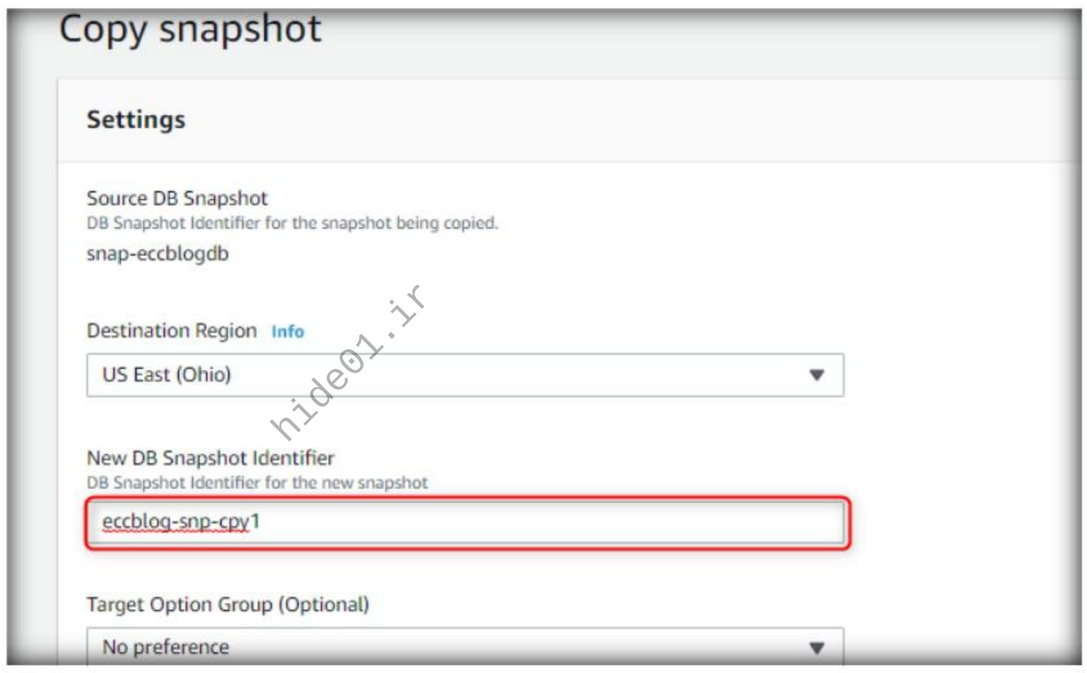


FIGURE 4.4.23: Configure settings

24. Under the **Encryption** section, check the **Enable Encryption** option to enable encryption for the copy of the DB snapshot. Keep the **Master key** as **(default) aws/rds** and then click on **Copy snapshot**.

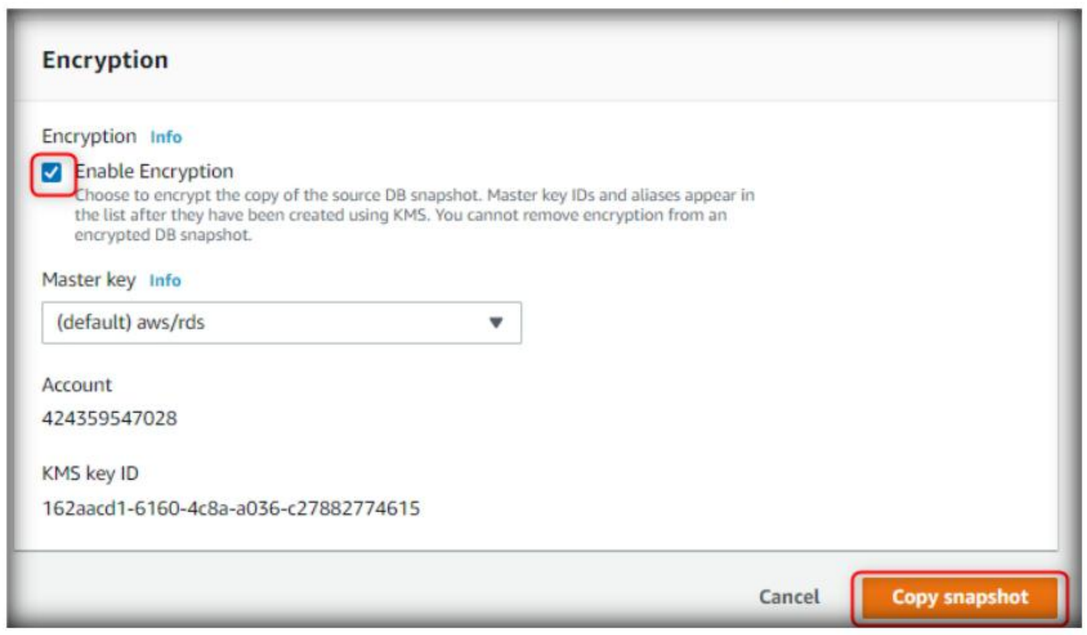


FIGURE 4.4.24: Configure settings

Certified Cloud Security Engineer Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

25. Now, wait for a few minutes for the snapshot copy to be created. Once done, you will have the encrypted Amazon RDS snapshot.

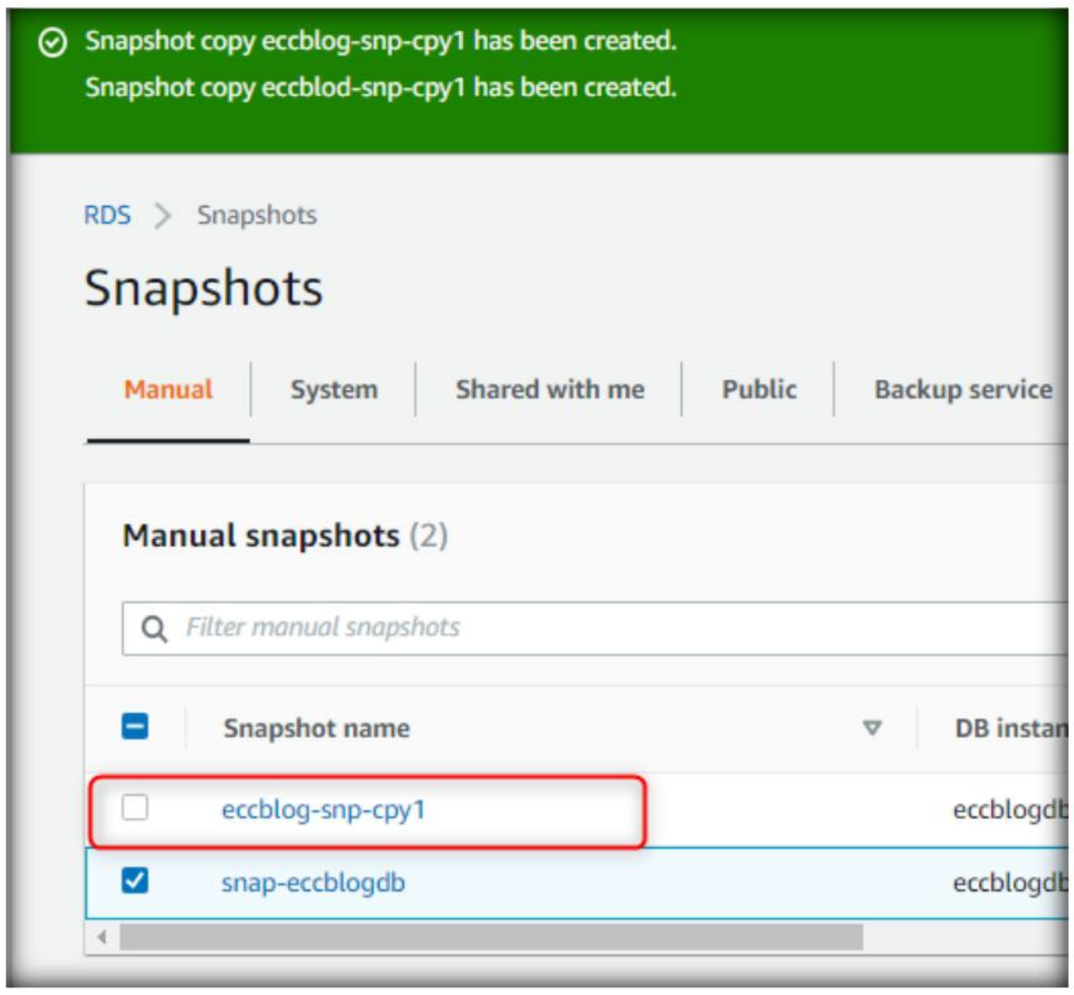


FIGURE 4.4.25: Snapshot Copy Created

TASK 3

Verifying Deletion Protection of the RDS

26. Next, you can check if deletion protection is enabled for the Amazon RDS. In case any unauthorized user tries to access your database, then they will not be able to delete it without editing or modifying the database instance.

27. Click **Databases** from the **Amazon RDS** left panel.

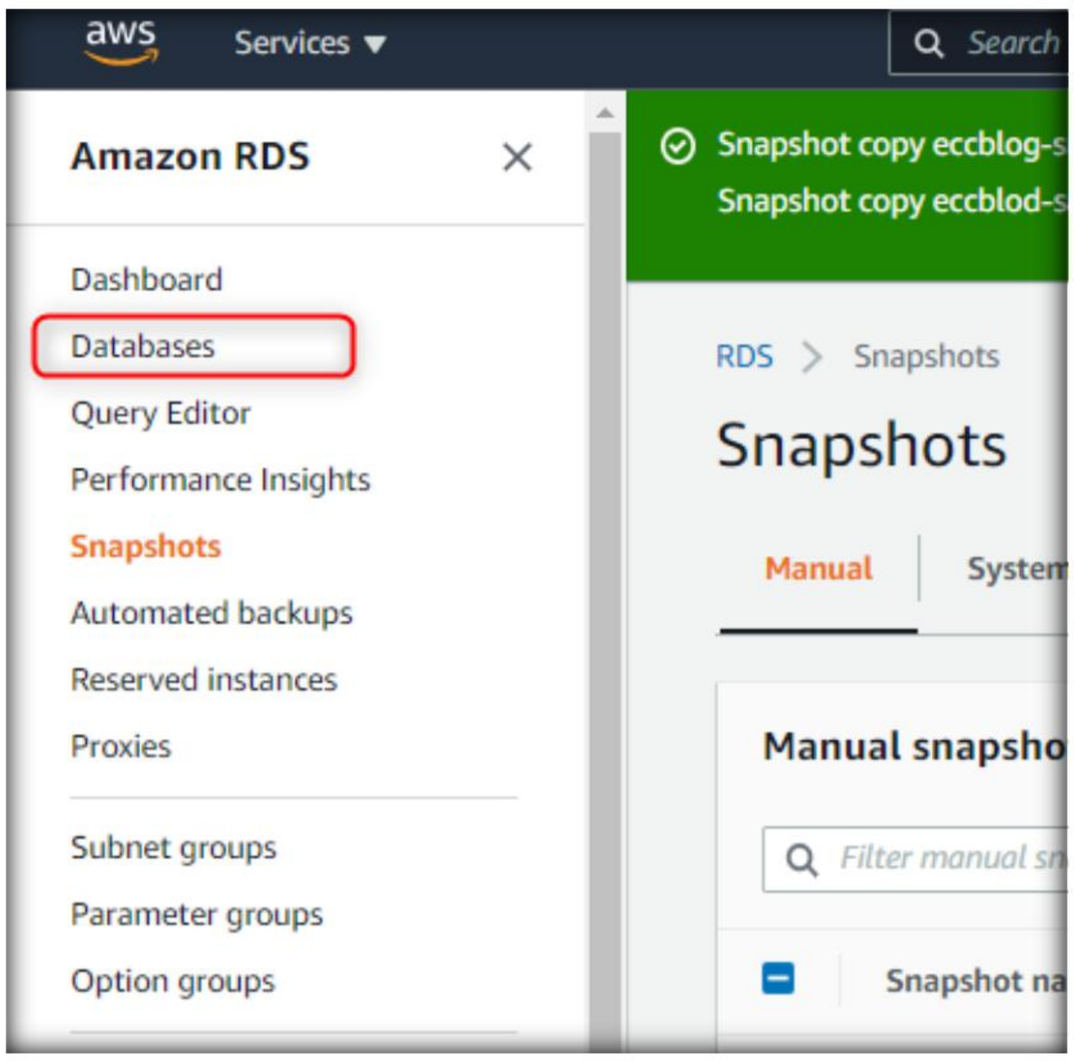


FIGURE 4.4.26: Clicking on Databases

Certified Cloud Security Engineer Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

28. Select the checkbox for the database you created (**eccblogdb**). Click on the **Actions** dropdown and select **Delete** from the menu.

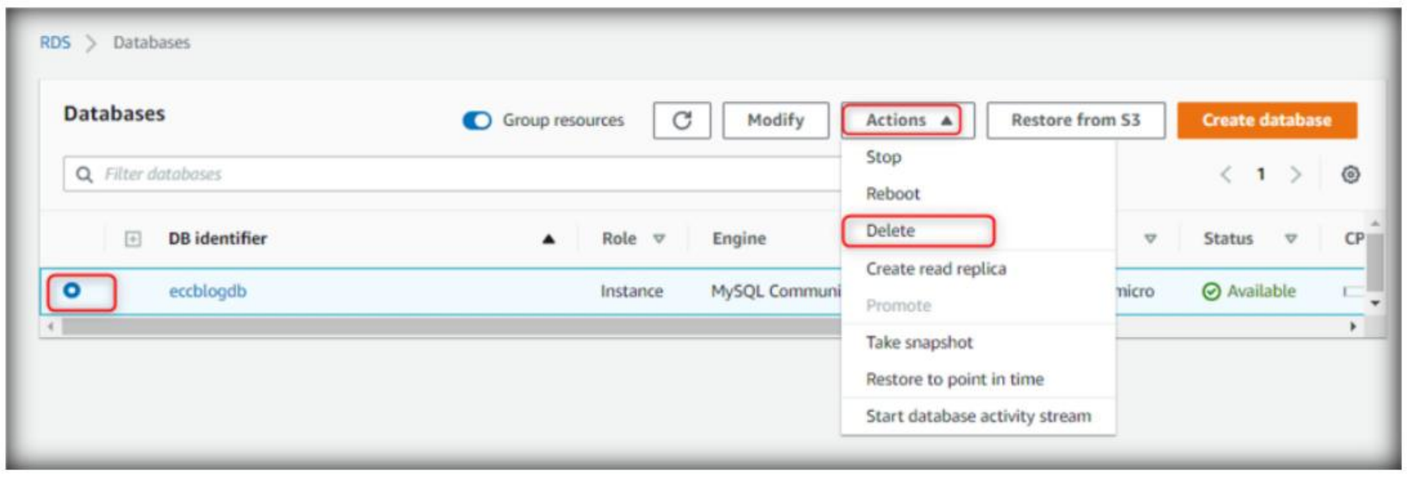


FIGURE 4.4.27: Trying to Delete the Database

29. As soon as you click on **Delete**, you will see a pop-up that says, **"This database has deletion protection option enabled."** Now, click on **Close**.

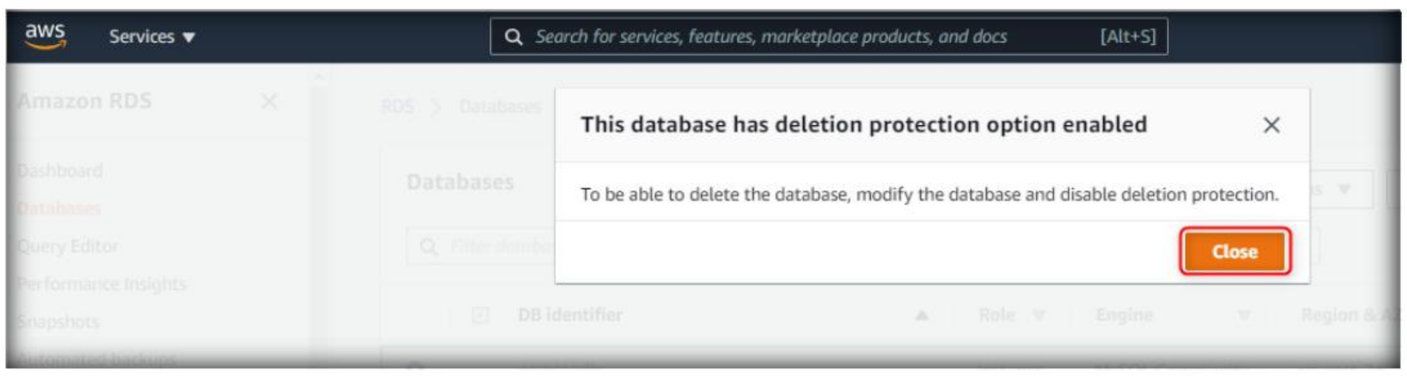


FIGURE 4.4.28: Database is Protected from Deletion

30. This way, a cloud security engineer can secure databases in Amazon RDS by enabling deletion protection and also by creating a database snapshot.

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

31. Now delete all the instances created in this lab. Navigate to the **Snapshots** under Amazon RDS and select the checkbox for the instances created in this lab (here, **snap-eccblogdb** and **eccblog-snp-cpy1**). In the pop-up window, click on the **Delete** button.

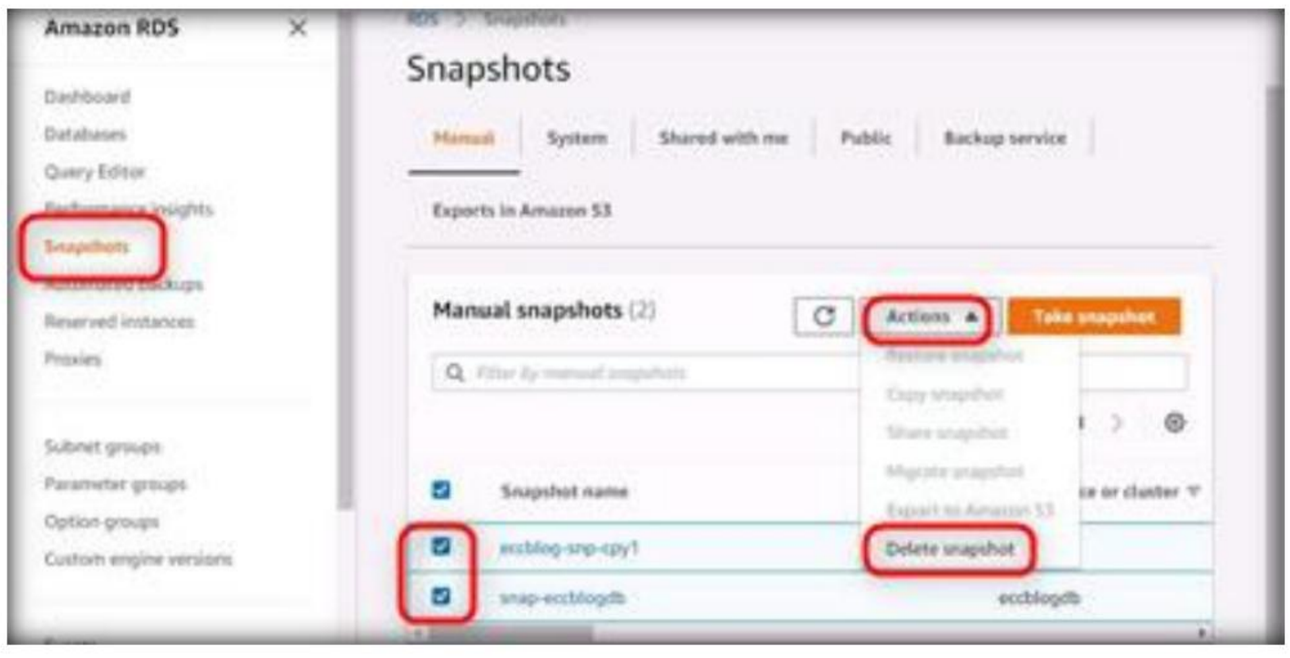


FIGURE 4.4.29:Deleting Snapshot

Certified Cloud Security Engineer Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

32. Navigate to **Databases** under Amazon RDS and select the checkbox created in this lab (here, **eccblogdb**). Select the **Modify** button and uncheck the **Enable delete protection** under **Deletion** protection. Click on Continue.

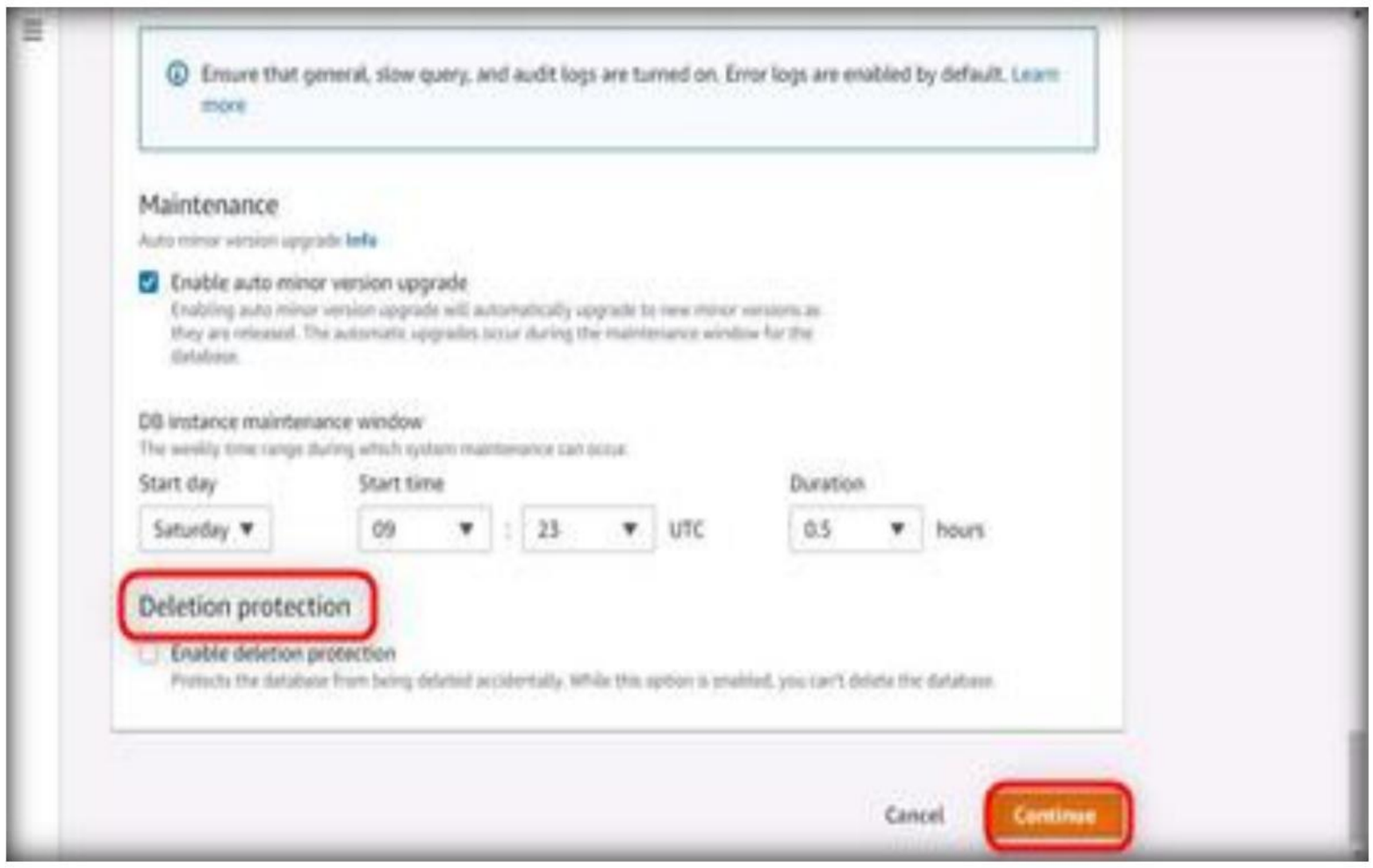


FIGURE 4.4.30: Disble Delete Protection

33. In the next window, click on **Apply immediately** radio button for **Scheduling of modifications** and select **Modify DB instance**.

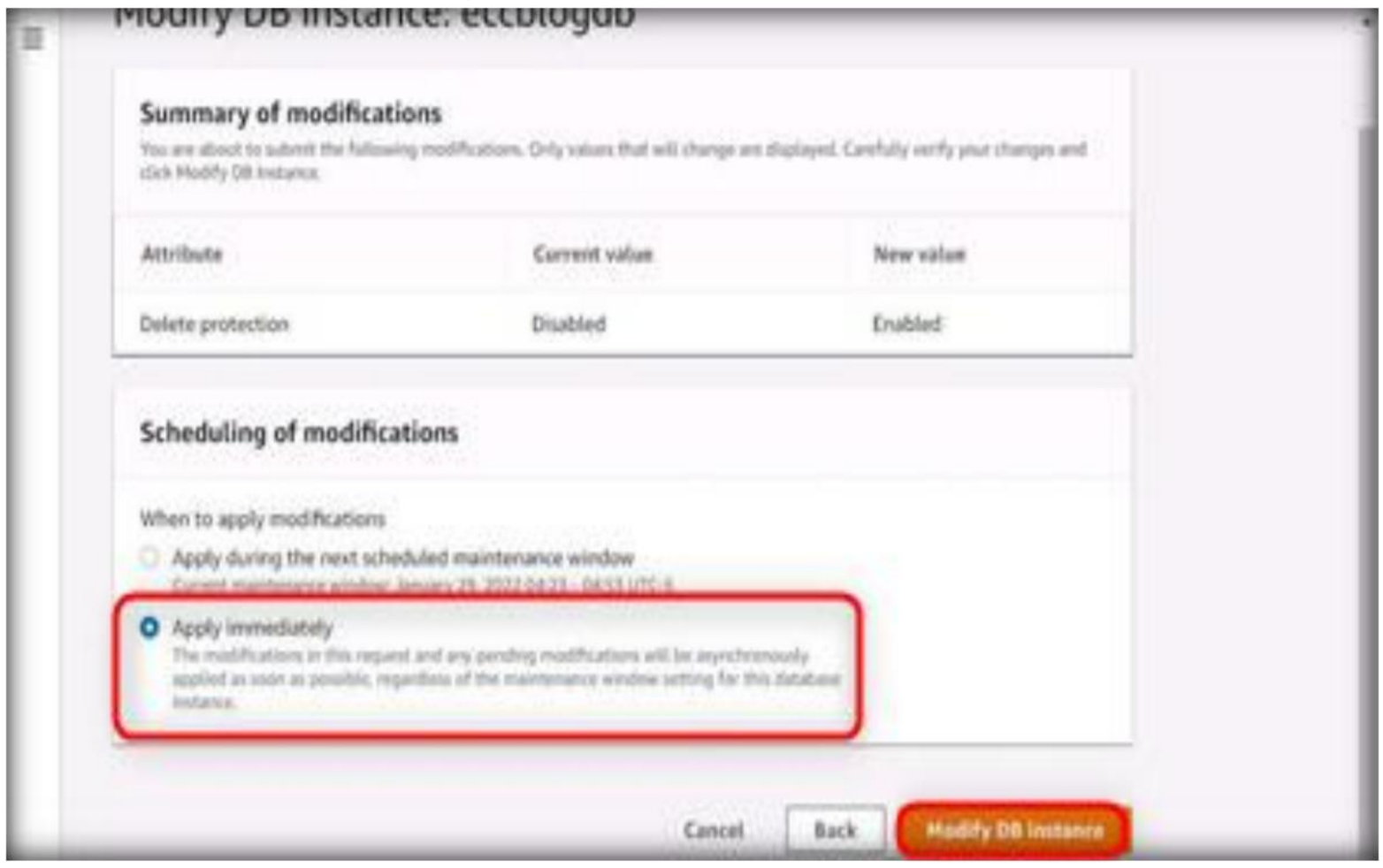


FIGURE 4.4.31: Modifyibg DB Instance

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

34. Navigate to **Databases** under Amazon RDS and select the checkbox for database instance created in this lab (here, **eccblogdb**). Click on the **Delete** button. In the pop-up window, acknowledge the checkbox, enter delete me, and click on the **Delete** button.

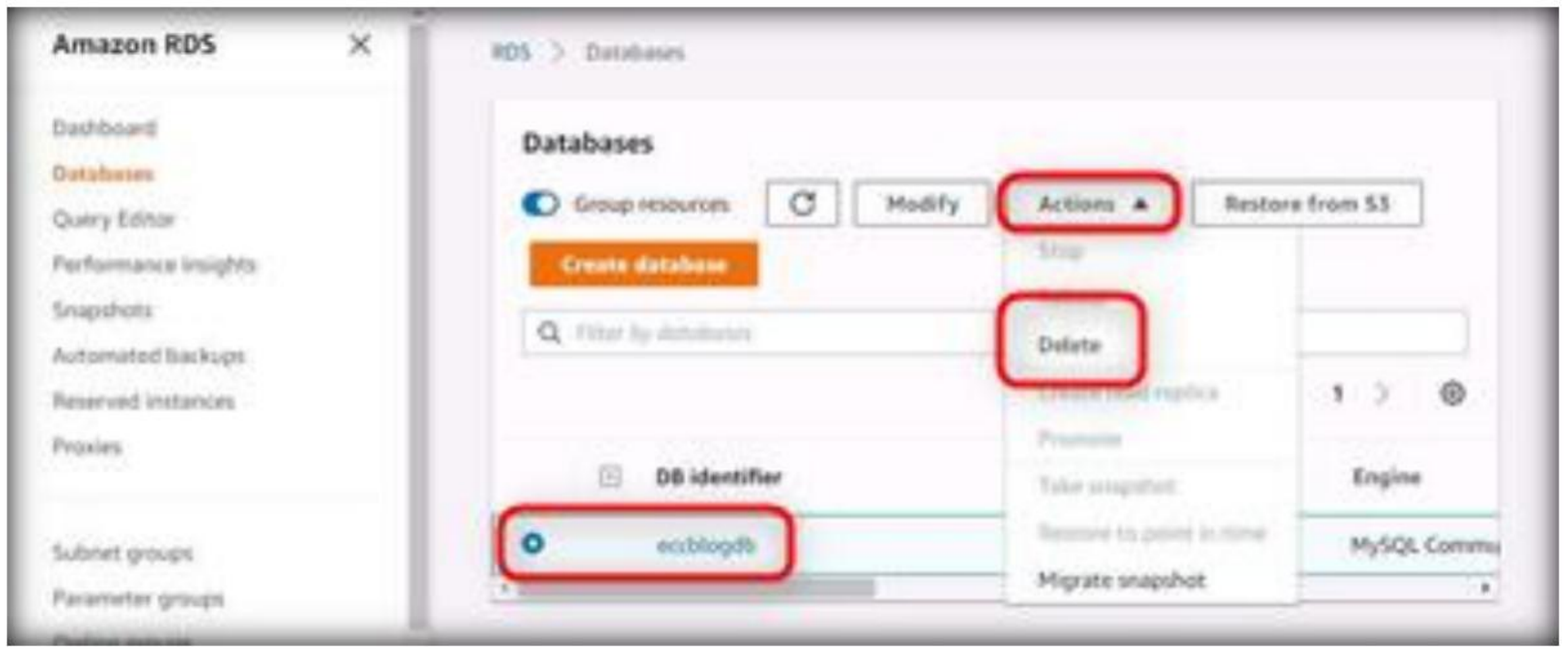


FIGURE 4.4.32: Deleting Database

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.

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 5

Preventing Deletion of Backups Using an Amazon Backup Vault Resource-based Access Policy

By using resource-based access policies with AWS backup vault, a cloud security engineer can specify who can access the backup in the vault and what actions they can perform to prevent any unauthorized access.

ICON KEY

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

Lab Scenario

With AWS Backup, a cloud security administrator can assign policies to the backup vault and its related resources. By using resource-based access policies with AWS backup vault, the administrator can specify who can access the backup in the vault and what actions they can perform. Using these policies, the administrator can also restrict users from deleting a backup in the vault.

Lab Objectives

This lab will demonstrate how to create backups and prevent their deletion by creating an Amazon backup vault resource-based access policy.

In this lab, you will learn to do the following:

- Create an IAM user in AWS with access to backups
- Create an Amazon backup vault resource-based access policy
- Verify the restricted access policy

Lab Environment

To perform this lab, you need the following:

- **Admin Machine** VM
- **Administrative** privileges
- Registered AWS account

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Duration

Time: 15 minutes

Overview of Amazon Backup Vault Resource-based Access Policy

AWS Backup provides complete data protection and can be used to configure backup policies for an insight into events that use AWS resources. A backup vault in AWS is a container that can be used to store backups. With AWS backup, a cloud security administrator can assign policies to the backup vault and its related resources. These policies provide access to users for creating backup plans and can also restrict their ability to delete the recovery points.

By using resource-based access policies with AWS backup vault, the administrator can specify who can access the backup in the vault and what actions they can perform. Using these policies, the administrator can also restrict the users from deleting a backup in the vault.

The use of resource-based access policies in Amazon backup ensures the backups are protected and can be accessed only by the right users.

Lab Tasks

video.ir

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., AWS), the application interface may be updated with time. Hence, in case you happen to work on an updated version of AWS, 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 an AWS Free Tier account using the following link: https://aws.amazon.com/free/, in case you have already not created it for the previous module. Once the registration is complete, perform the following task:

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

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1

Creating an IAM User with access to AWS Backups

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

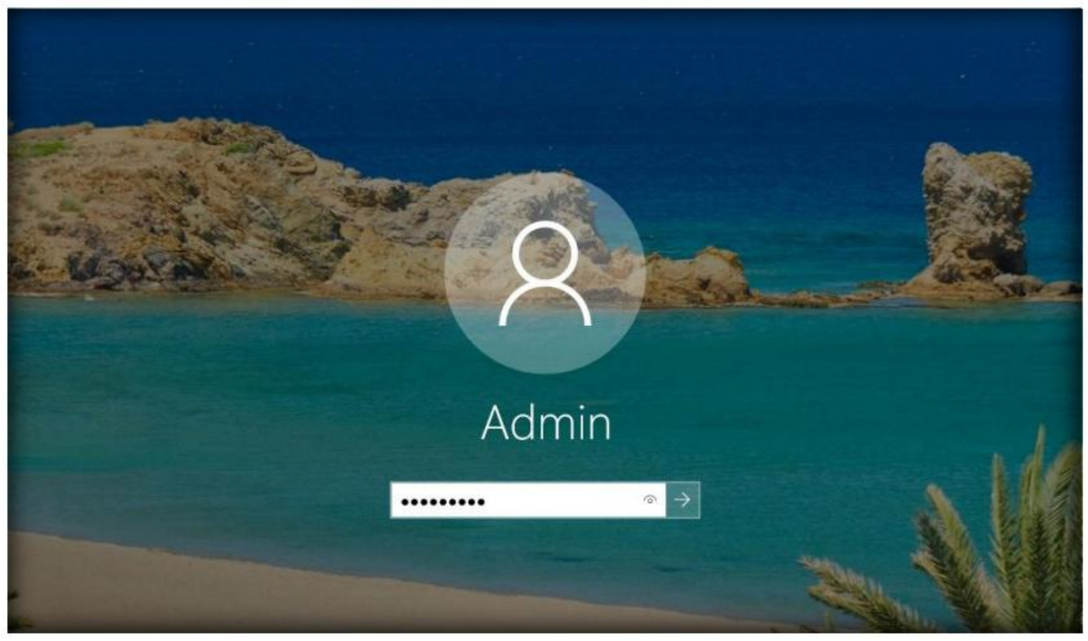


FIGURE 4.5.1: Launch Admin Machine and Log in

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



FIGURE 4.5.2: Navigating to the Chrome Browser from Taskbar

3. The **Google Chrome** browser opens. In the address bar, type **https://aws.amazon.com/** and press **Enter**.

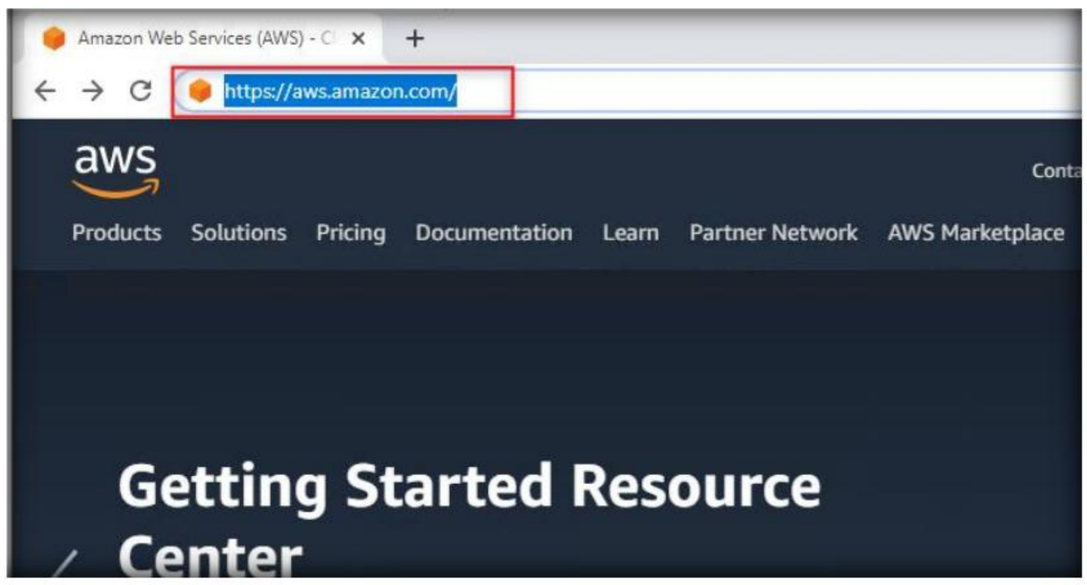


FIGURE 4.5.3: Access AWS in Browser

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

4. The **AWS Web Services - Cloud Computing Services** page appears. Click on **AWS Management Console** from the **My Account** dropdown, as shown in the screenshot below.

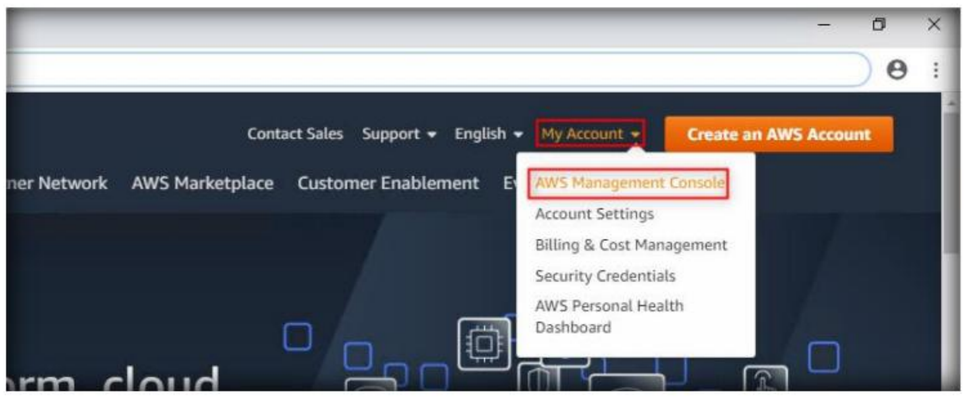


FIGURE 4.5.4: Navigate to AWS Management Console

5. The **AWS Web Services Sign-in** page appears. Choose **Root user**, type the AWS administrator account ID (Root user email address), as shown in the screenshot below, and click on **Next**.

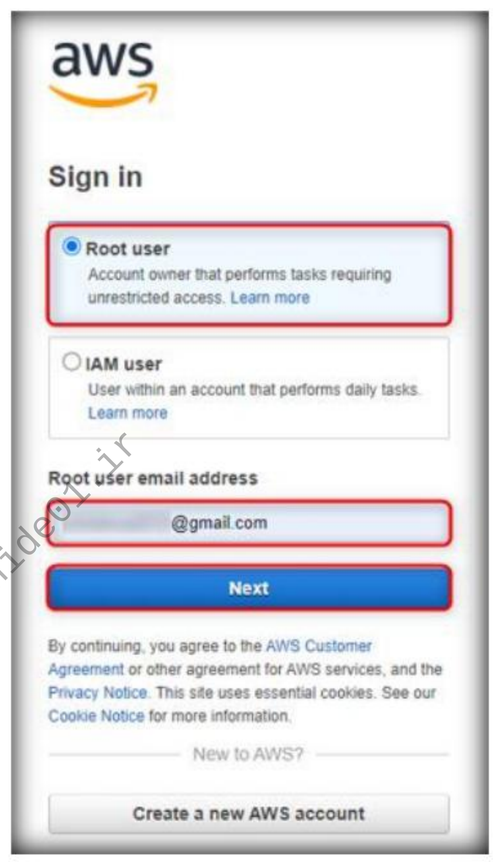


FIGURE 4.5.5: AWS Sign-in

6. In the security check page that appears, type the characters shown in the image and click on **Submit**.



FIGURE 4.5.6: AWS Sign-in Security Check

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

7. In the **Password** field, type the password and click on **Sign in**, as shown in the screenshot below.

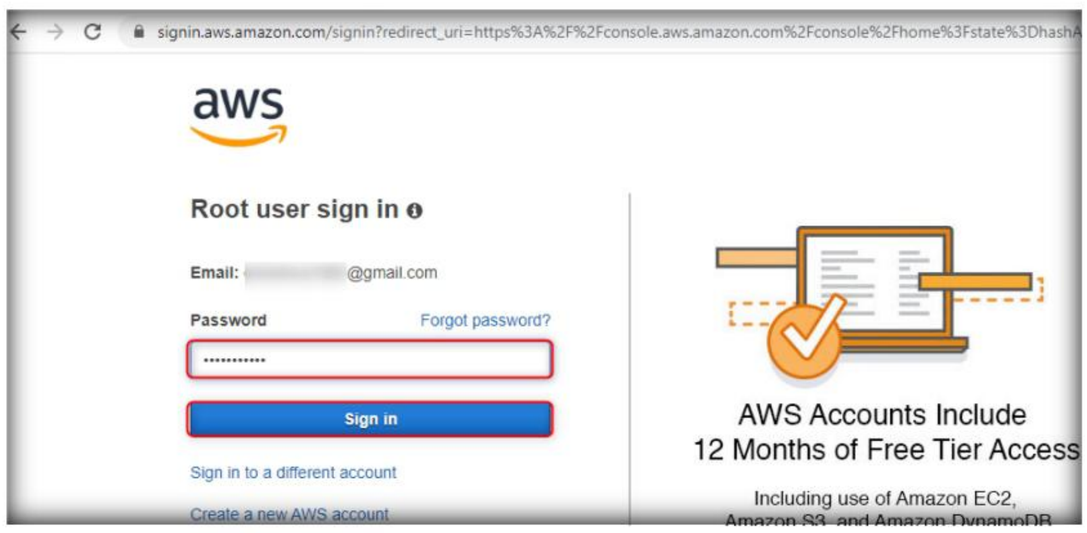


FIGURE 4.5.7: Sign-in to AWS

8. Now, to create an IAM user, select **Services** from the menu bar and click on **IAM** under the **Security, Identity, & Compliance** section, as shown in the screenshot below.

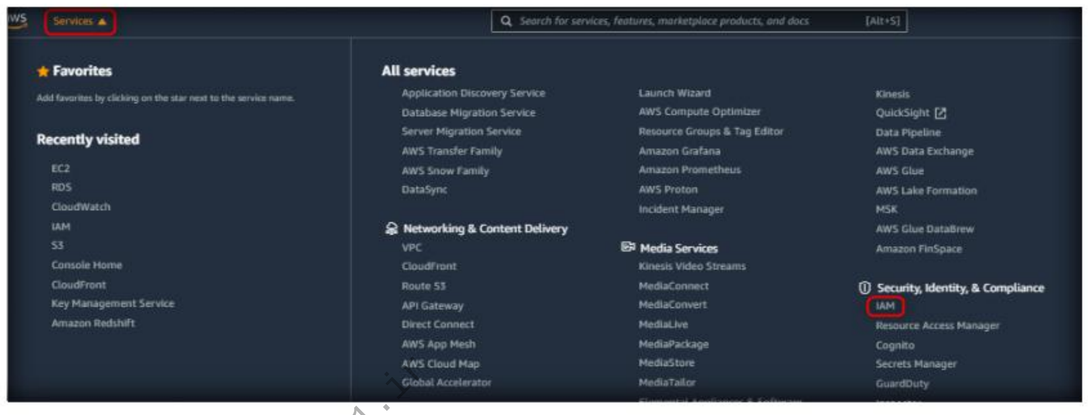


FIGURE 4.5.8: Navigate to IAM

9. On the **IAM dashboard**, select **Users** in the left pane from the **Identity and Access Management (IAM)** section.

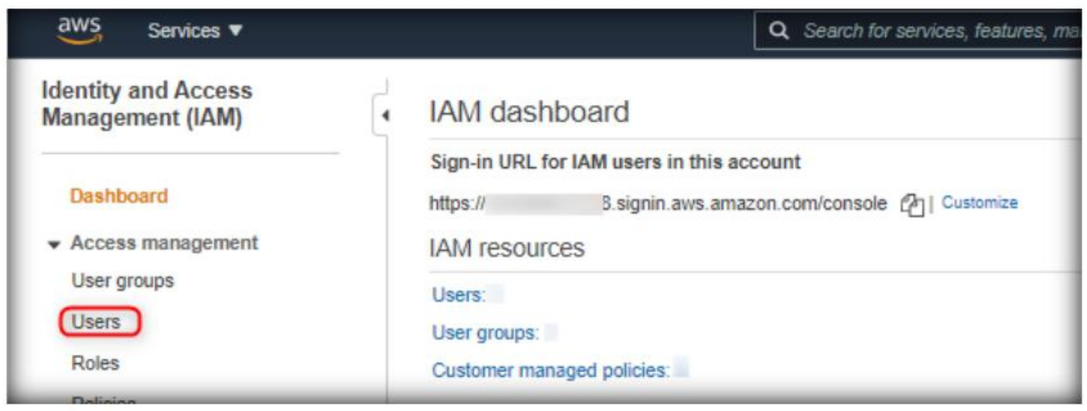


FIGURE 4.5.9: Navigate to Users

10. Click on **Add user**, as shown in the screenshot below, to create a new user.

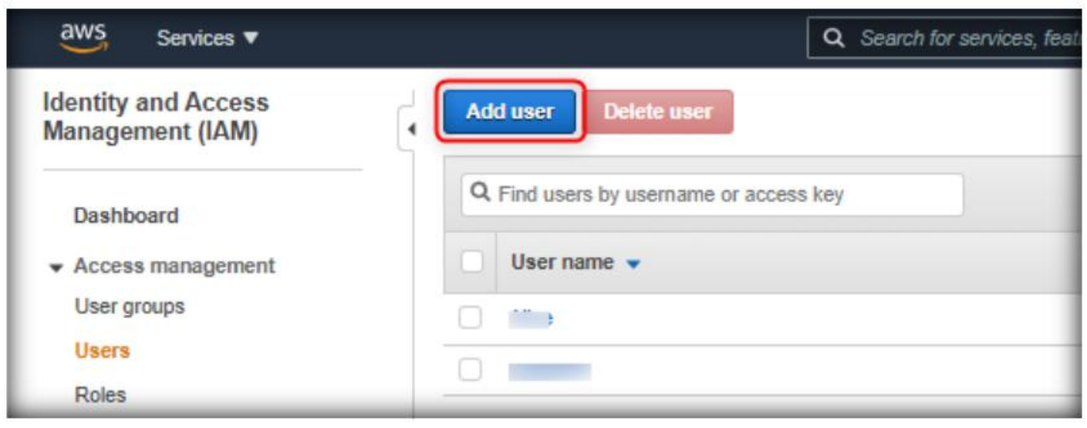


FIGURE 4.5.10: Adding a New User

Certified Cloud Security Engineer Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

11. The **Add user** page appears. In the **Username** field, provide any name (here, the username is **John**). Check **AWS Management Console access and Programmatic access** under **Access type** in the **Select AWS access type** section. Choose the **Custom password** radio button and type the password (**user@123**) in the password field, as shown in the screenshot below. **Require password reset** is optional; however, uncheck this setting. Now, click on **Next: Permissions**.

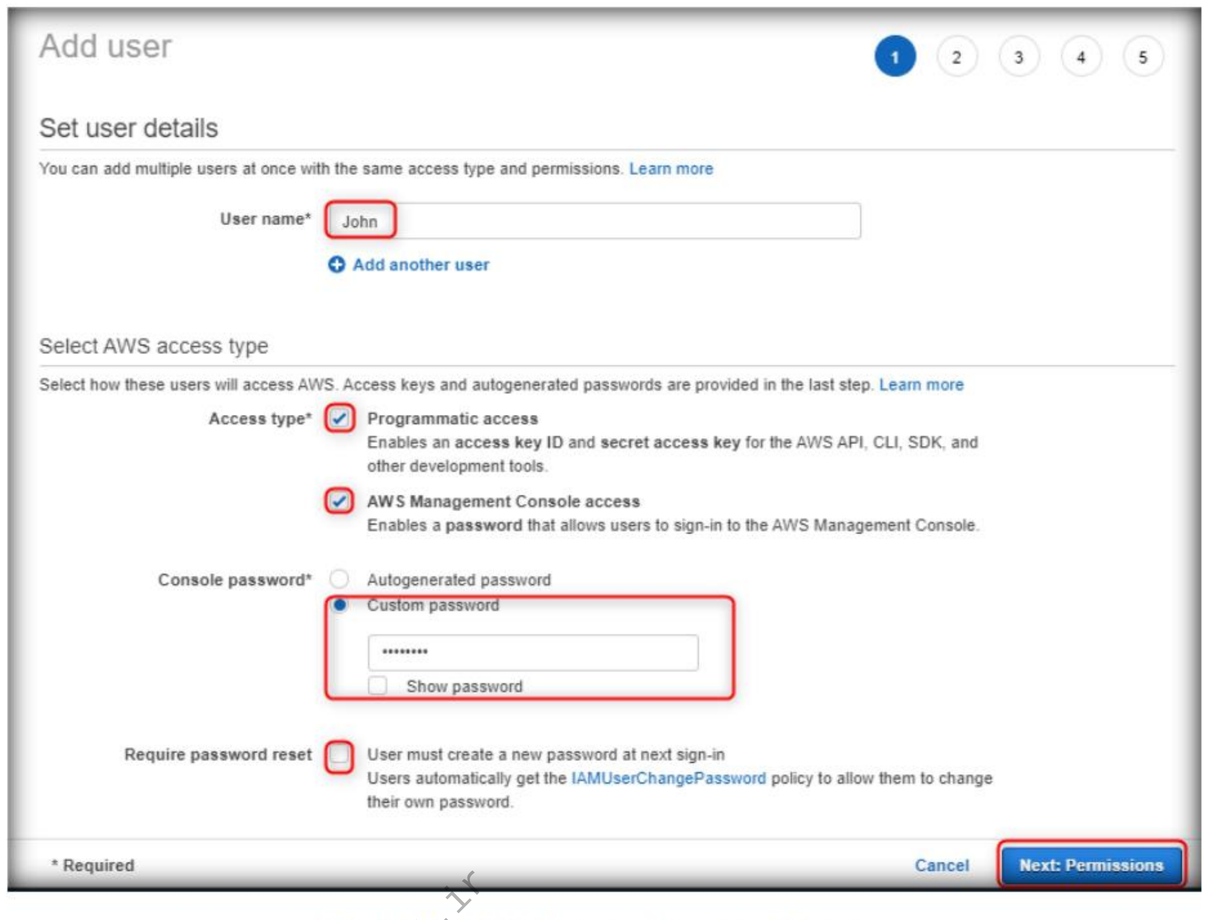


FIGURE 4.5.11: Entering New User Details

12. In the **Set permissions** section, click on **Attach existing policies directly**. In the **Filter policies** field, search for **AWSBackupFullAccess** and select the checkbox for **AWSBackupFullAccess** from the search results. Now, click on **Next: Tags**.

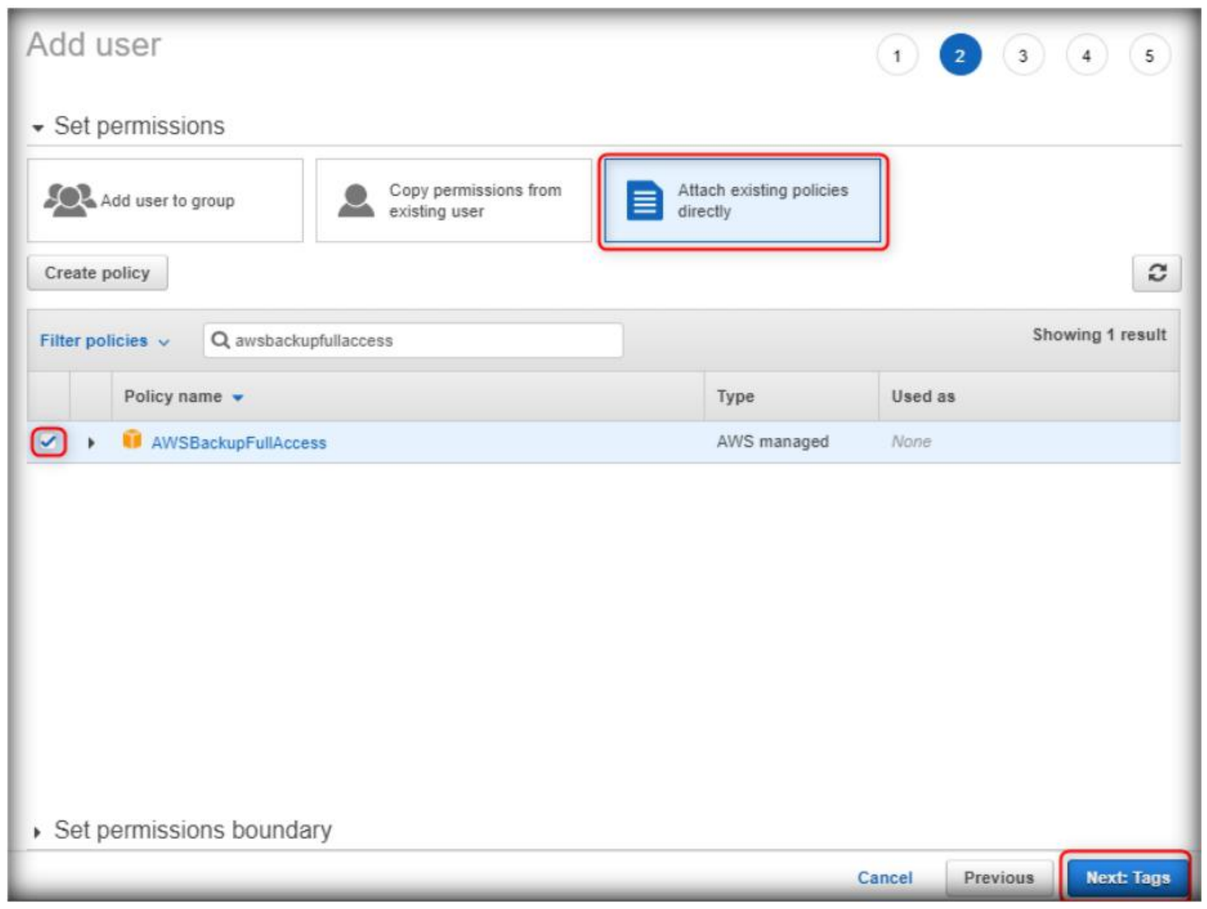


FIGURE 4.5.12: Attaching Policy

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

13. Tags are optional; however, tagging will help you later in easily searching for tag keys. Then, click on **Next: Review** to review the IAM user creation.

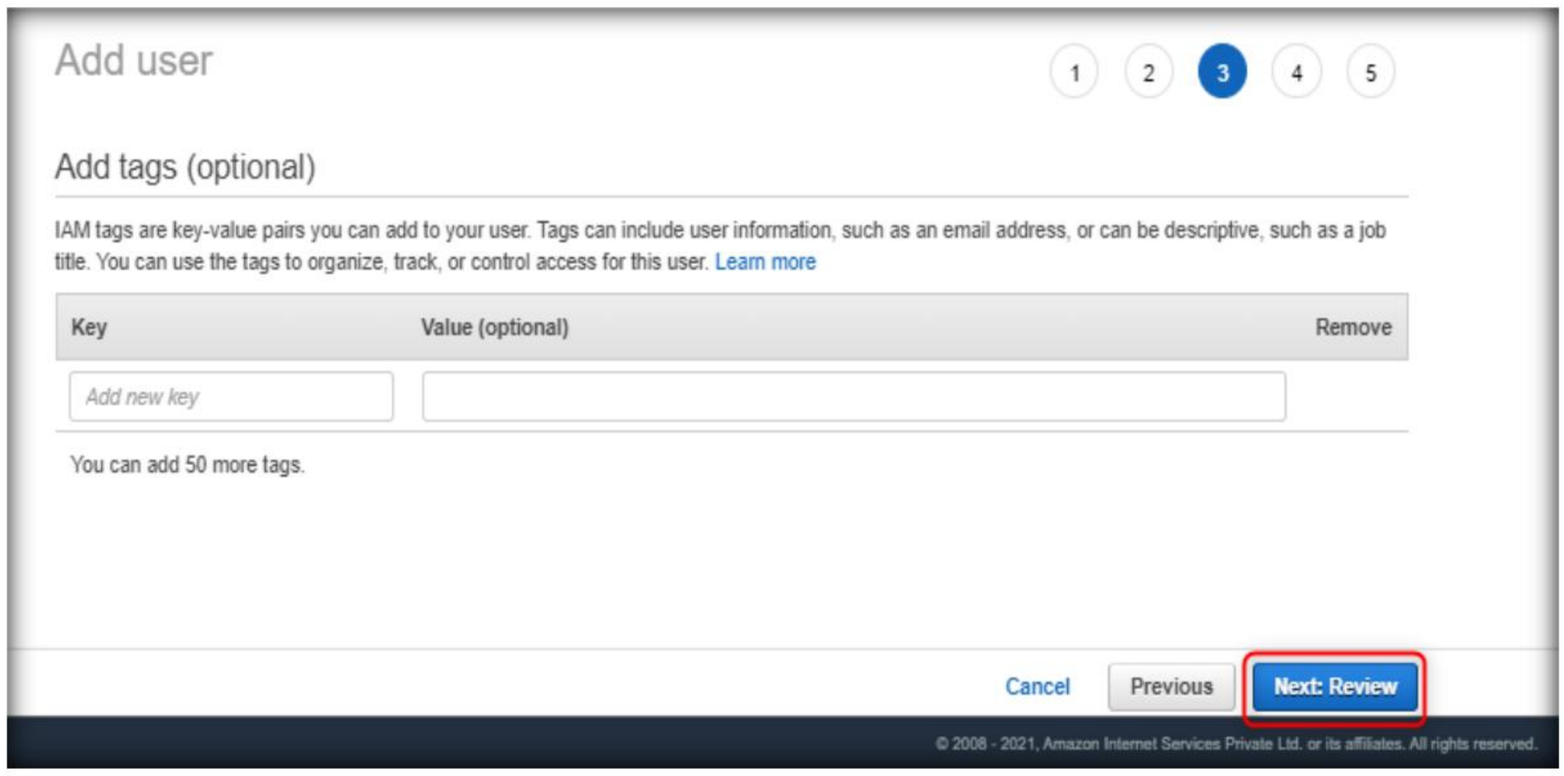


FIGURE 4.5.13: Adding Tag for User

14. On the **Review** page, view the settings and IAM user details before creating the user. Once you have verified the settings, click on **Create user**.

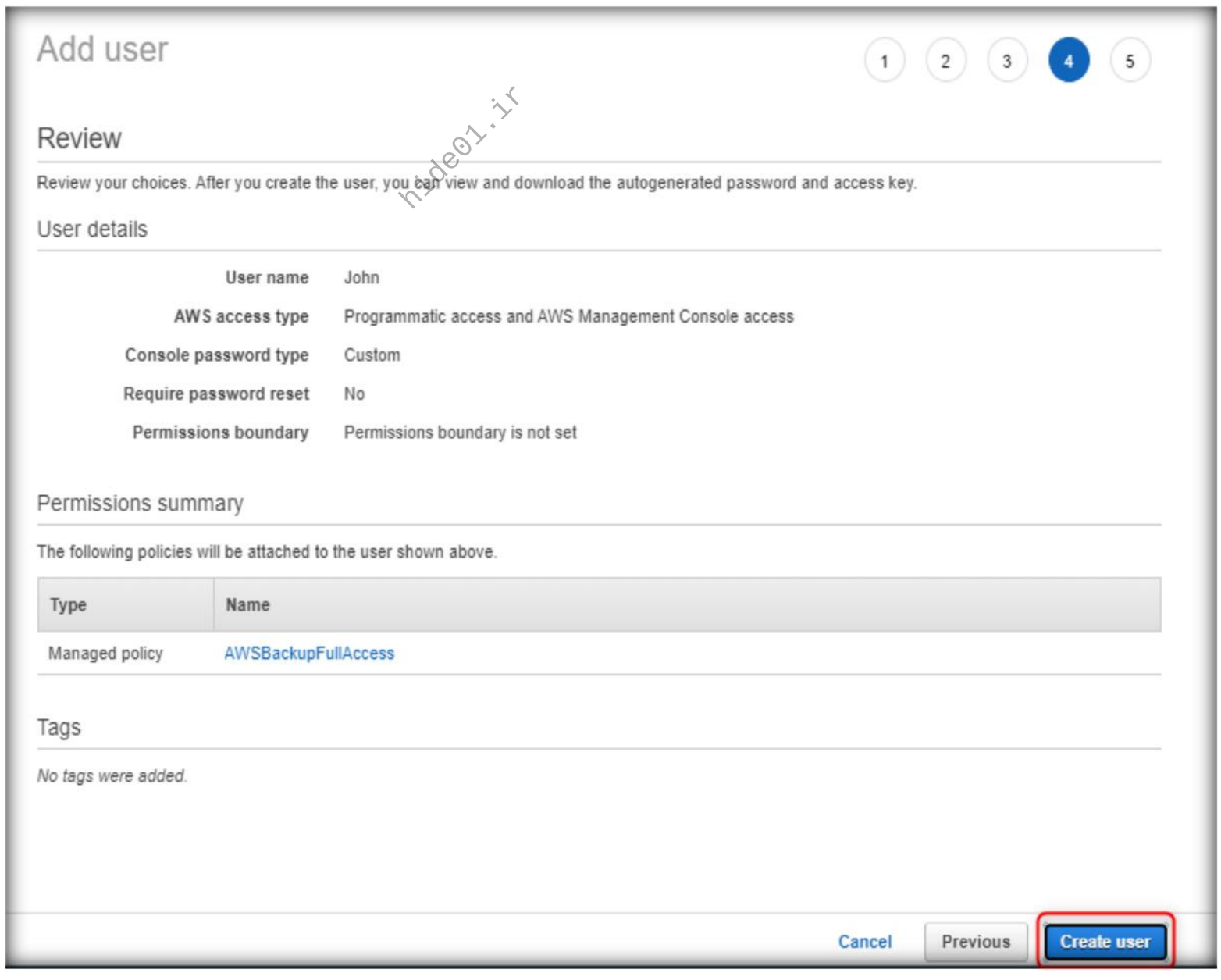


FIGURE 4.5.14: Reviewing New User Details

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

15. After you click on **Create user**, a **Success** message is displayed, as shown in the screenshot below. You have an option to **Send Email** to get the login instructions for the newly created IAM user. Click on **Close** (lower right corner of the page) to return to the IAM page. It will redirect you to the **Users** page.

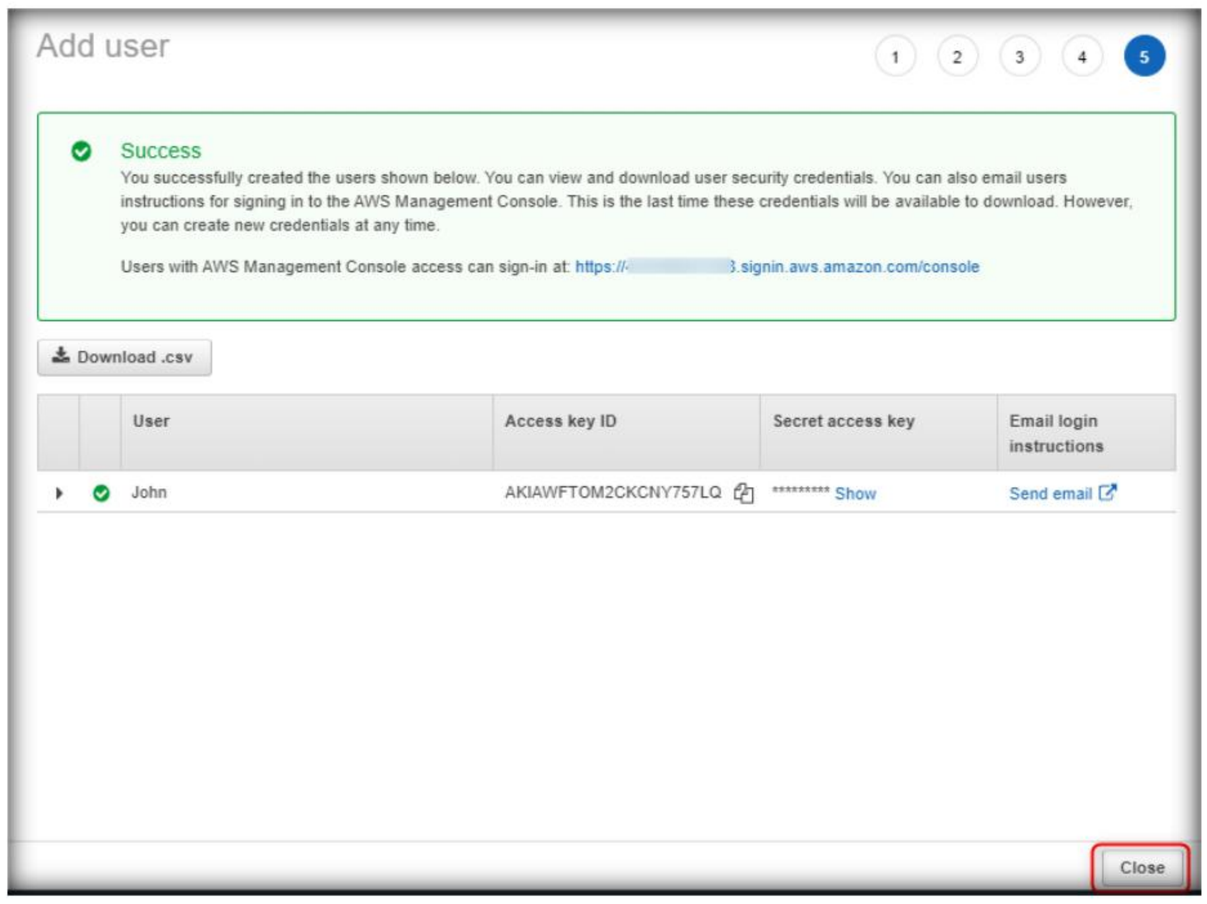


FIGURE 4.5.15: New User Added Successfully

16. You will be redirected to the **Users** page. On this page, click on the name of the user (**John**) you created.

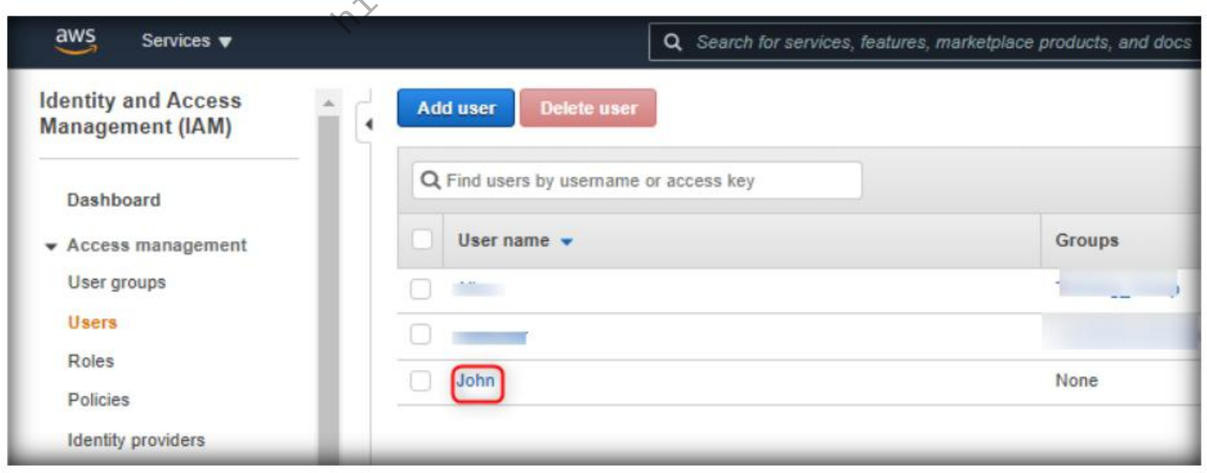


FIGURE 4.5.16: Selecting the User

17. The **Summary** page appears now. To assign a policy to the user, the **User ARN** (for **John**) is required. Copy the **User ARN** and paste it in notepad.

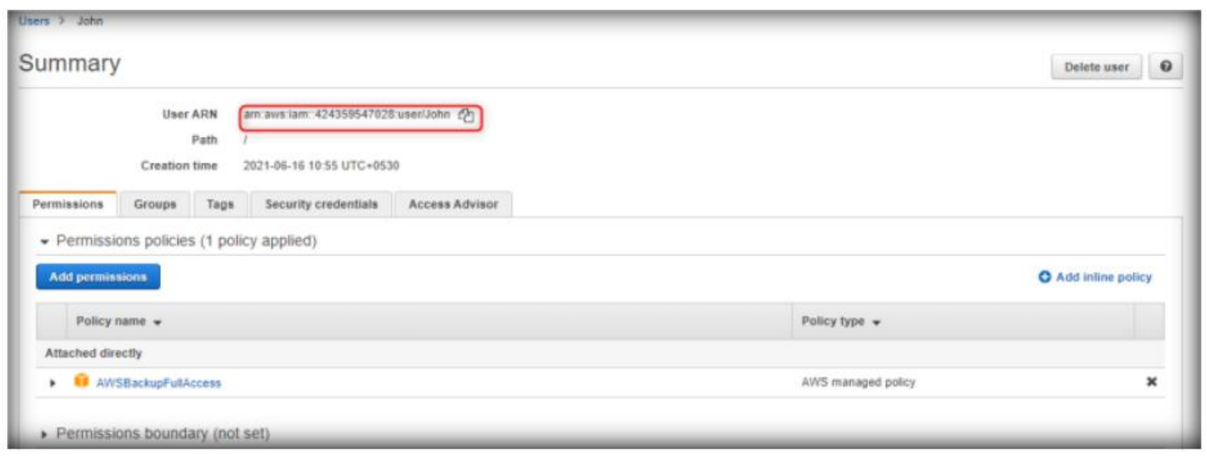


FIGURE 4.5.17: Copying ARN

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 2

Creating AWS Backup Vault

18. To create an AWS backup vault, click on the **Services** menu and select **AWS Backup** under **Storage**.

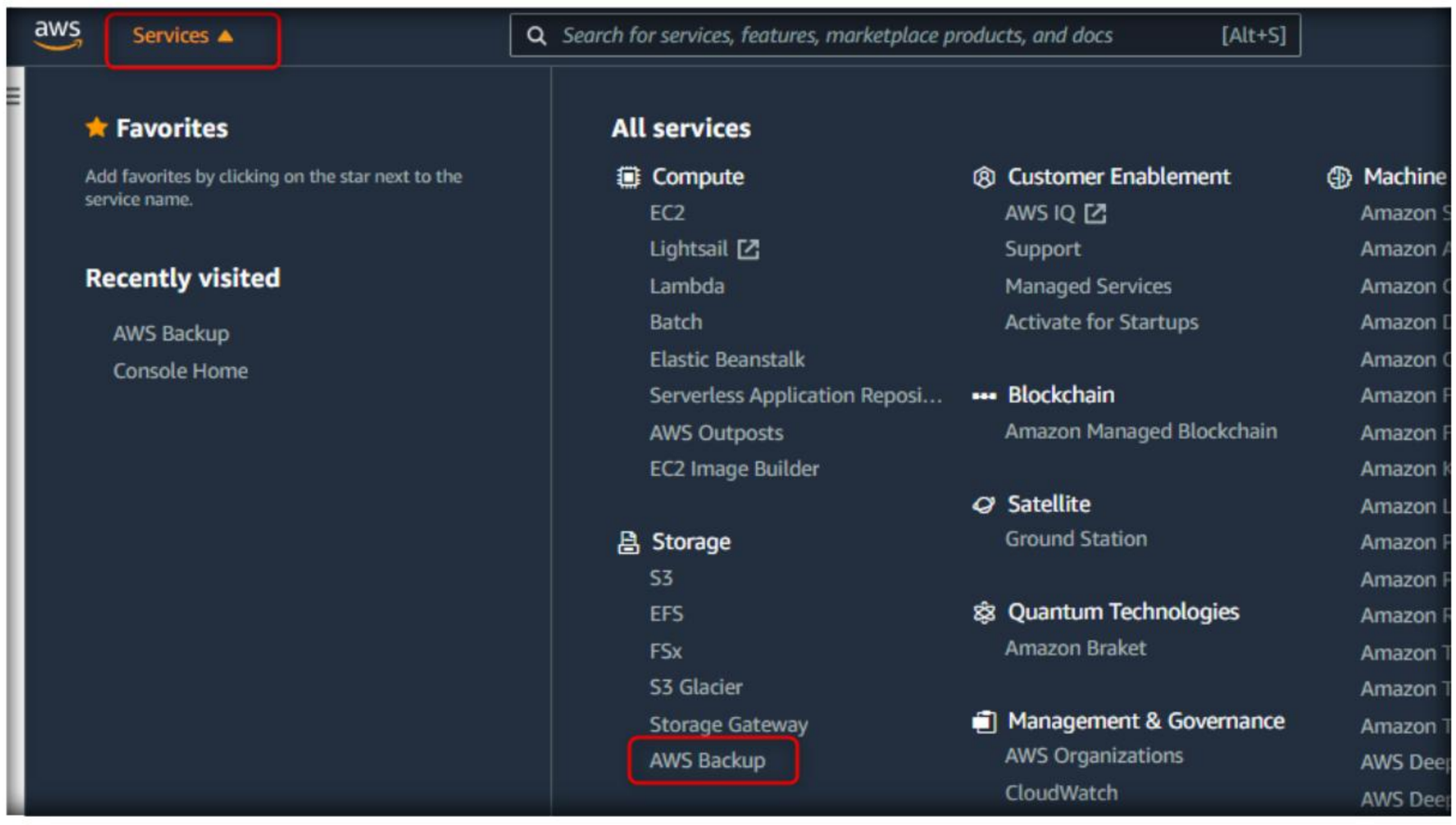


FIGURE 4.5.18: Selecting AWS Backup Service

19. Once the **AWS Backup Console** opens, click on the **Backup vaults** option from the left pane. If the menu is not visible, click on the **ellipsis** at the top left corner to view it, and then select **Backup Vault**.



FIGURE 4.5.19: Backup Vault

20. To create a backup vault, click on **Create Backup vault** in the **Backup vaults** window.

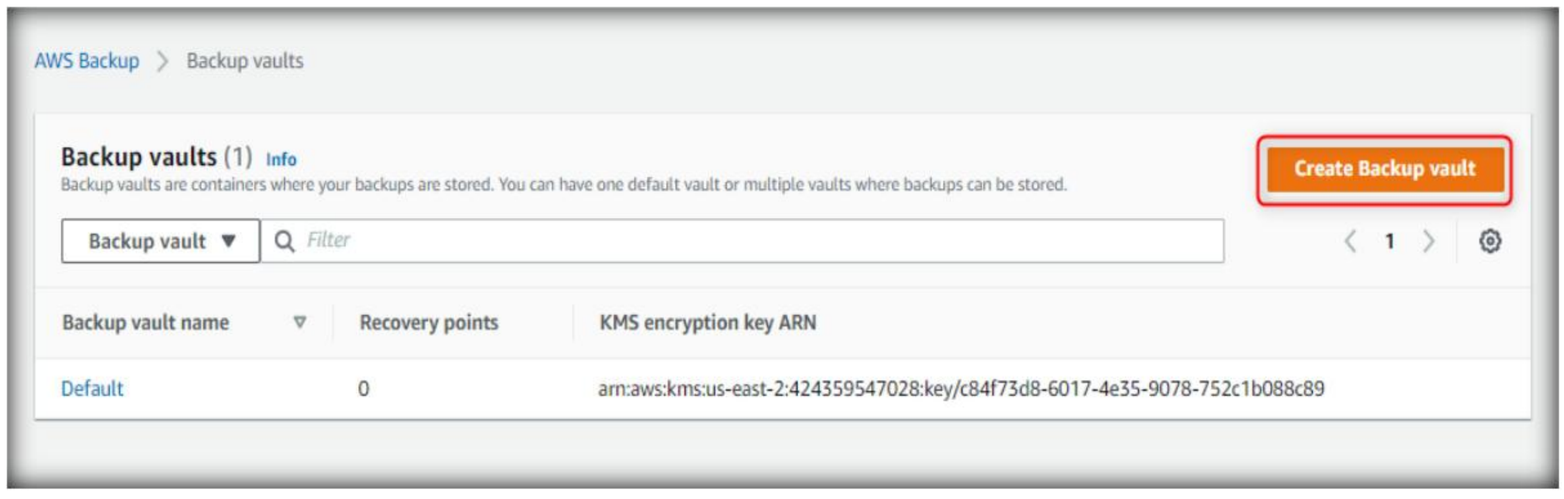


FIGURE 4.5.20: Clicking on Create Backup

Certified Cloud Security Engineer Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

21. In the **Create Backup vault** section, type a suitable name under **Backup vault name** (here, **AwsBackup1**) and select **Encryption key** as **default aws/backup**. Then, click on **Create Backup vault**.

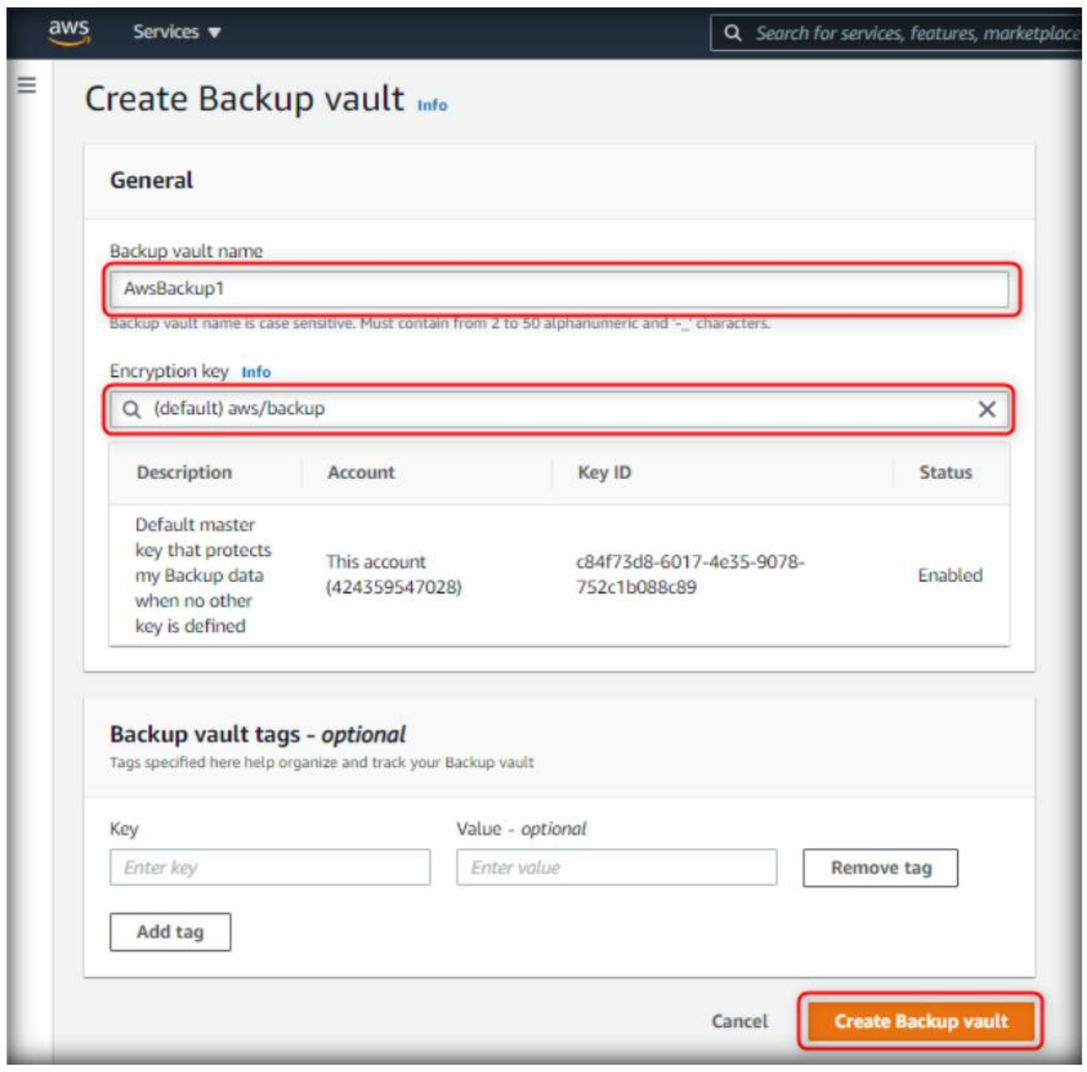


FIGURE 4.5.21: Creating Backup vault

22. The **AwsBackup1** is created, as shown in the following screenshot.

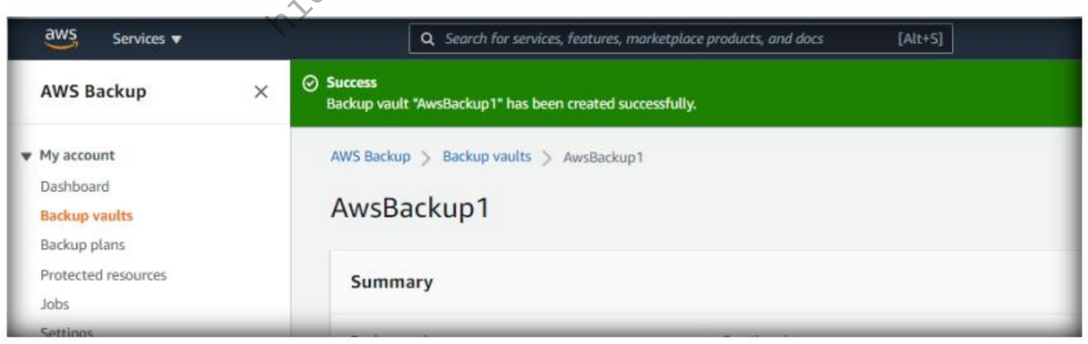


FIGURE 4.5.22: AwsBackup1 Created

23. Repeat **Steps 19–21** to create another backup vault with the following name: **AwsBackup2_imp**.

24. Now, there are two backup vaults: **AwsBackup1** and **AwsBackup2_imp**.

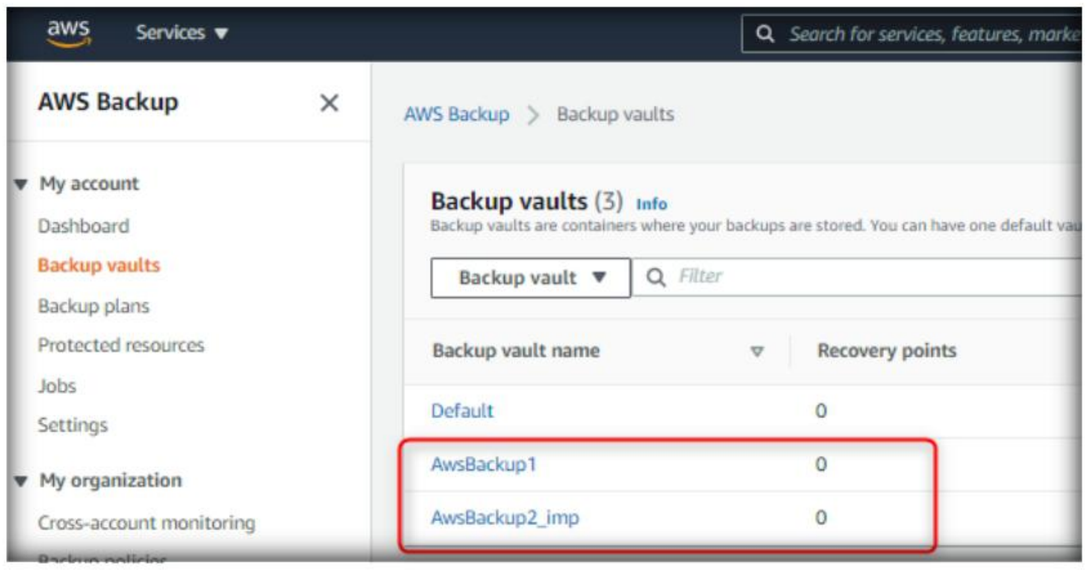


FIGURE 4.5.23: Backup vaults

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 3

Creating Amazon Backup Vault Resource- Based Access Policy

25. Next, to deny the deletion action to the user (**John**) for the backup vault named **AwsBackup2_imp**, create an Amazon backup vault resource-based access policy.
26. Now, to copy the backup vault ARN for **AWSBackup2_imp**, which is required for writing the policy, click on **AwsBackup2_imp** on the **Backup vaults** page.

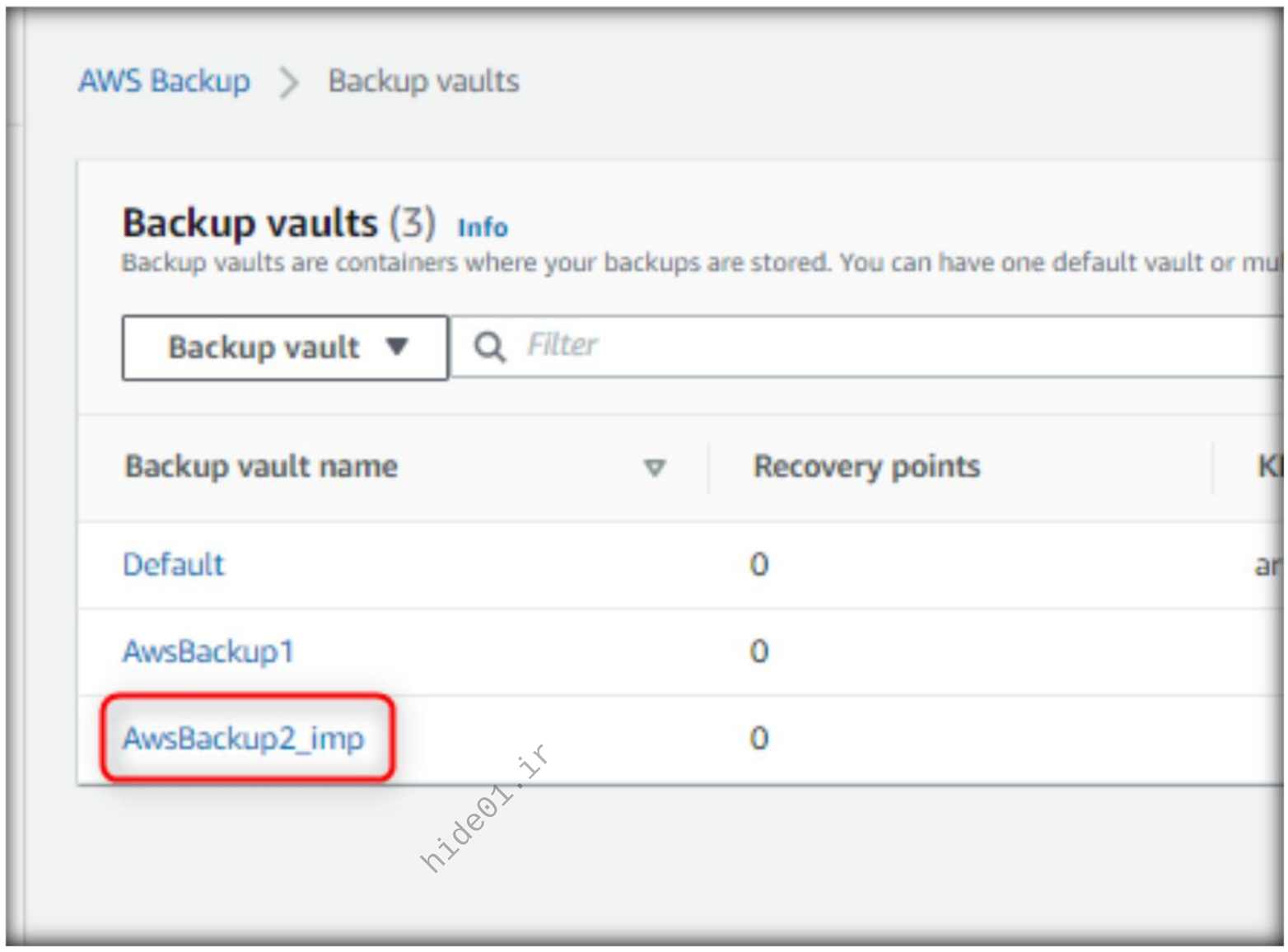


FIGURE 4.5.24: Selecting the vault

27. The **AwsBackup2_imp** section opens. Copy the **Backup vault ARN** and paste into notepad. Click **Edit** under the **Access policy** section.

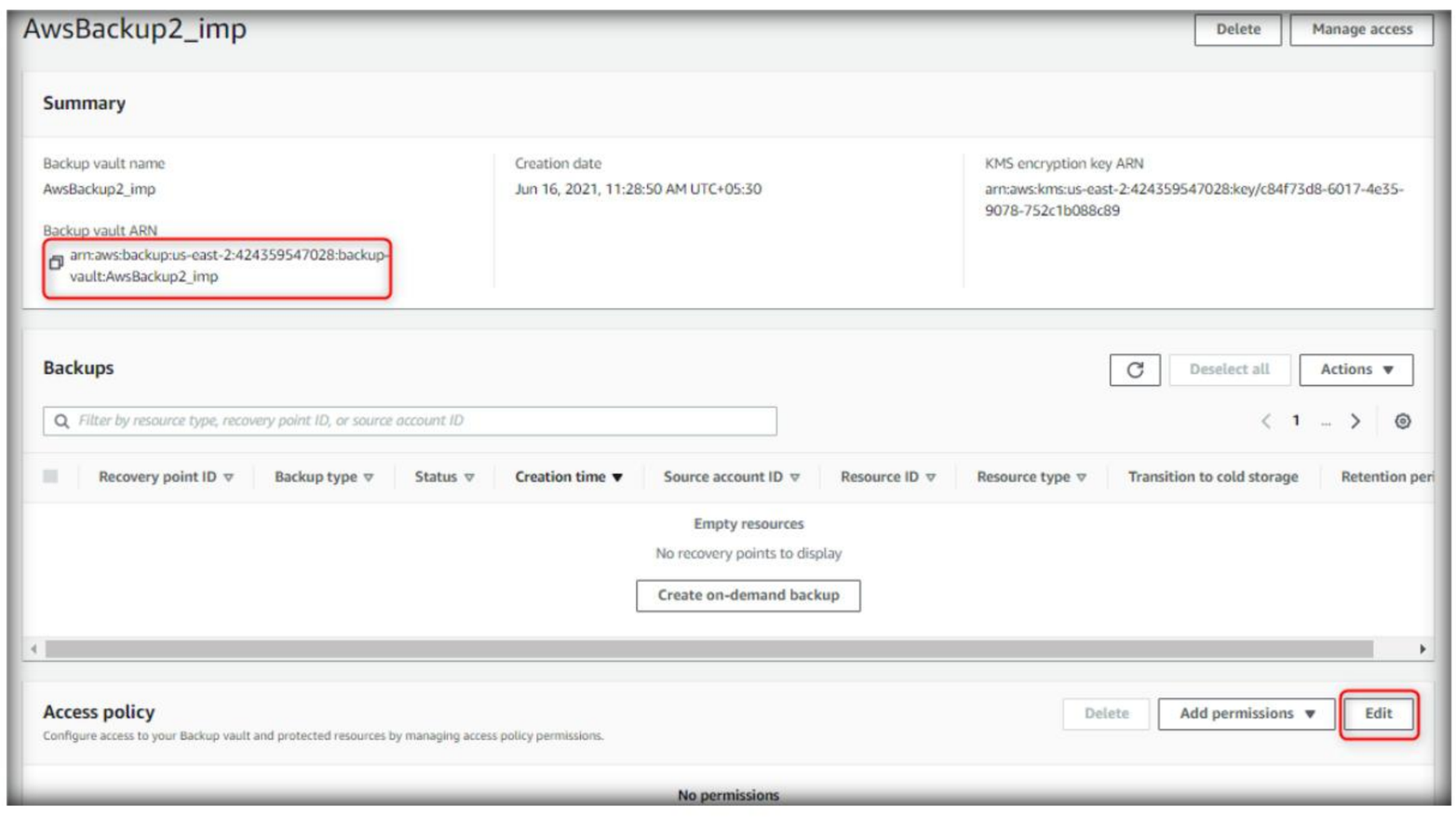


FIGURE 4.5.25: Vault page

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

28. The **Edit Access Policy** window opens now. Inside the policy editor window, paste the below JSON policy code, which denies access to the resources for the user (John). Click on **Save policy**.

    Note: Replace the **Principal** AWS ARN value you copied into the notepad in **Step 17** and replace the **Resource** ARN value you copied into notepad in **Step 27.**

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Deny",
         "Principal": {
            "AWS": "arn:aws:iam::424359547028:user/John"
         },
         "Action": [
                  "backup:DeleteBackupVault"
               ],
         "Resource":  "arn:aws:backup:us-east-2:424359547028:backup-vault:AwsBackup2_imp"
      }
   ]
}
```

h10901.ir

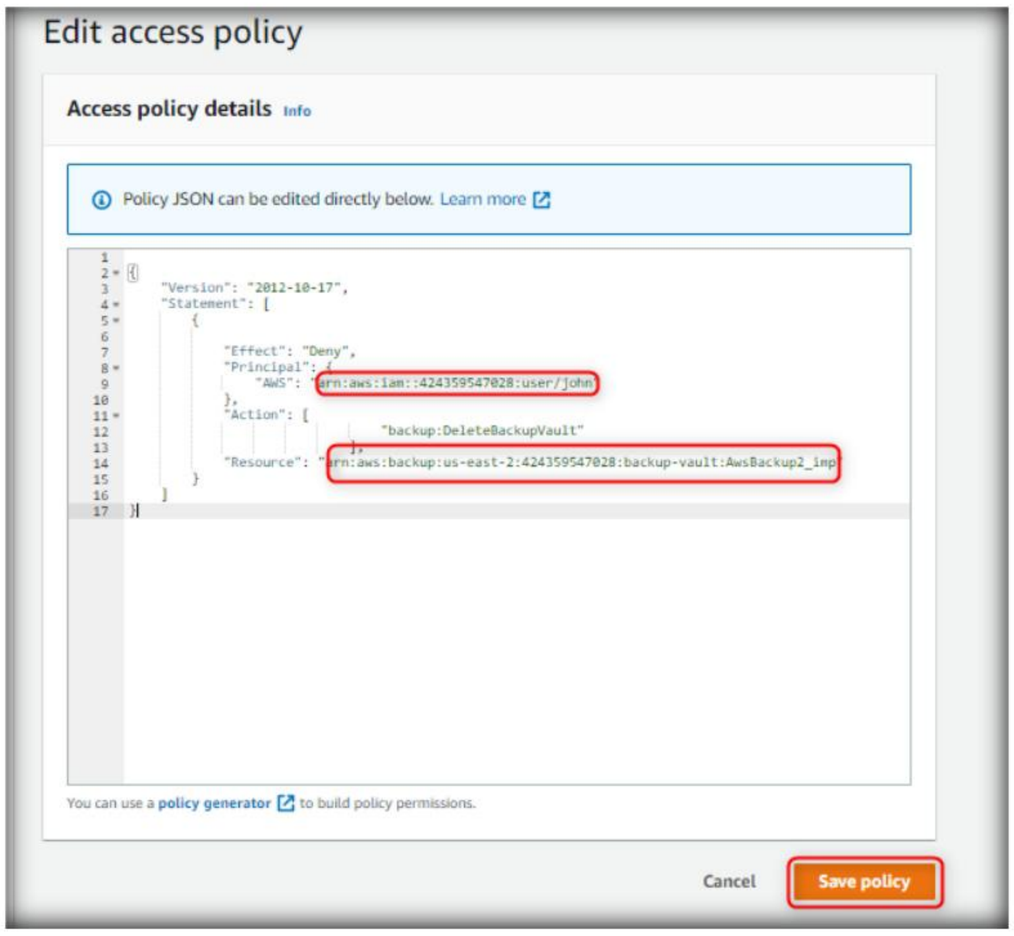


FIGURE 4.5.26: Saving Policy

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

29. The policy is updated successfully.

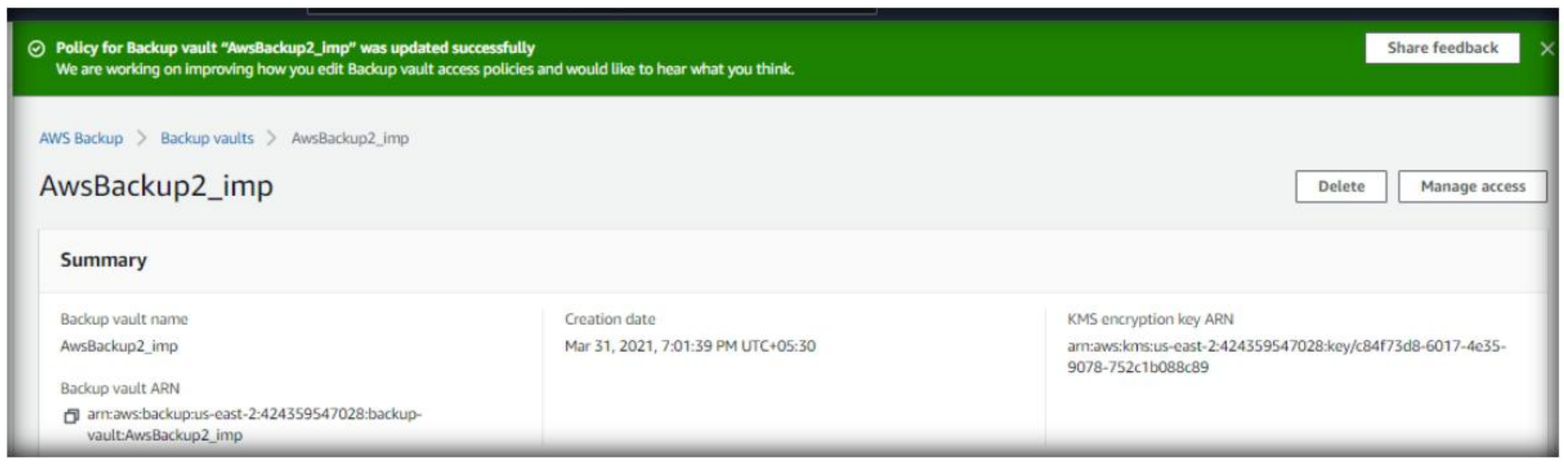


FIGURE 4.5.27: Policy Attached to the Vault

TASK 3

Verification of the Restricted Access Policy

30. Now, **John** cannot delete the Backup resources. Now, verify the applied restricted resources access policy. To do this, click on the **Services** menu and then on **IAM** under the **Recently visited** section.

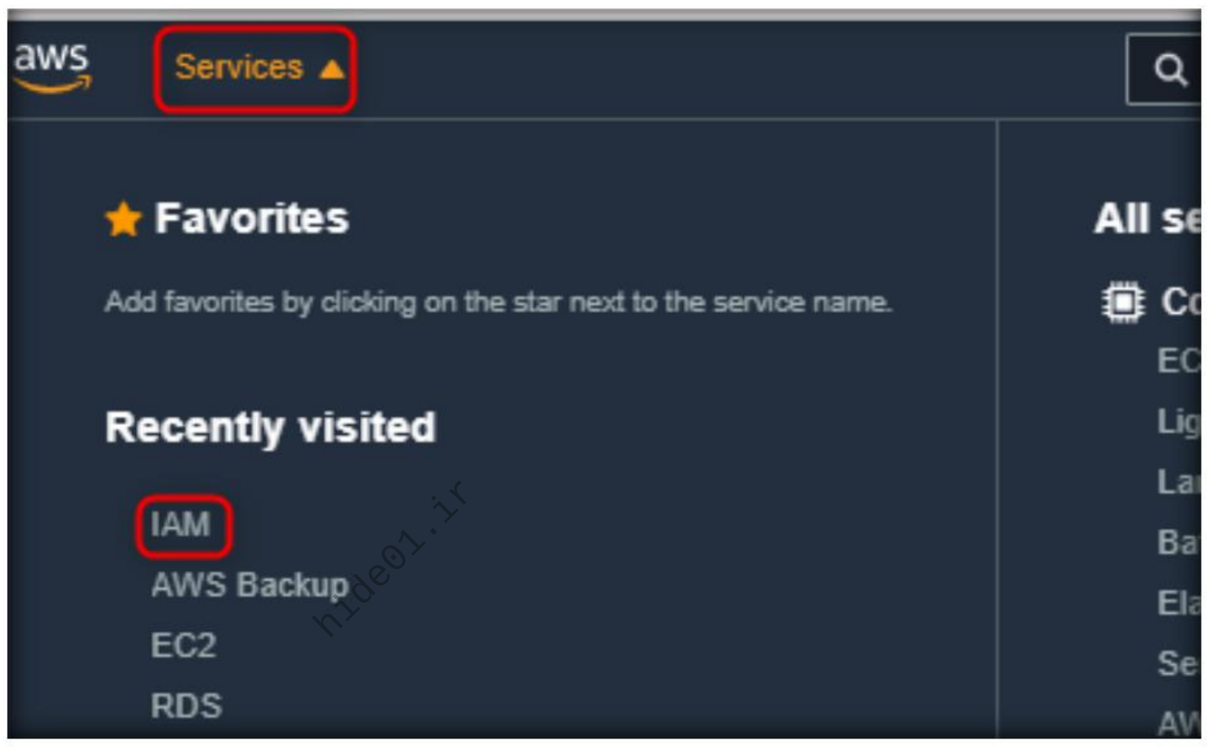


FIGURE 4.5.28: Selecting IAM

31. In the **IAM dashboard**, copy the link under **Sign-in URL for IAM users in this account**.

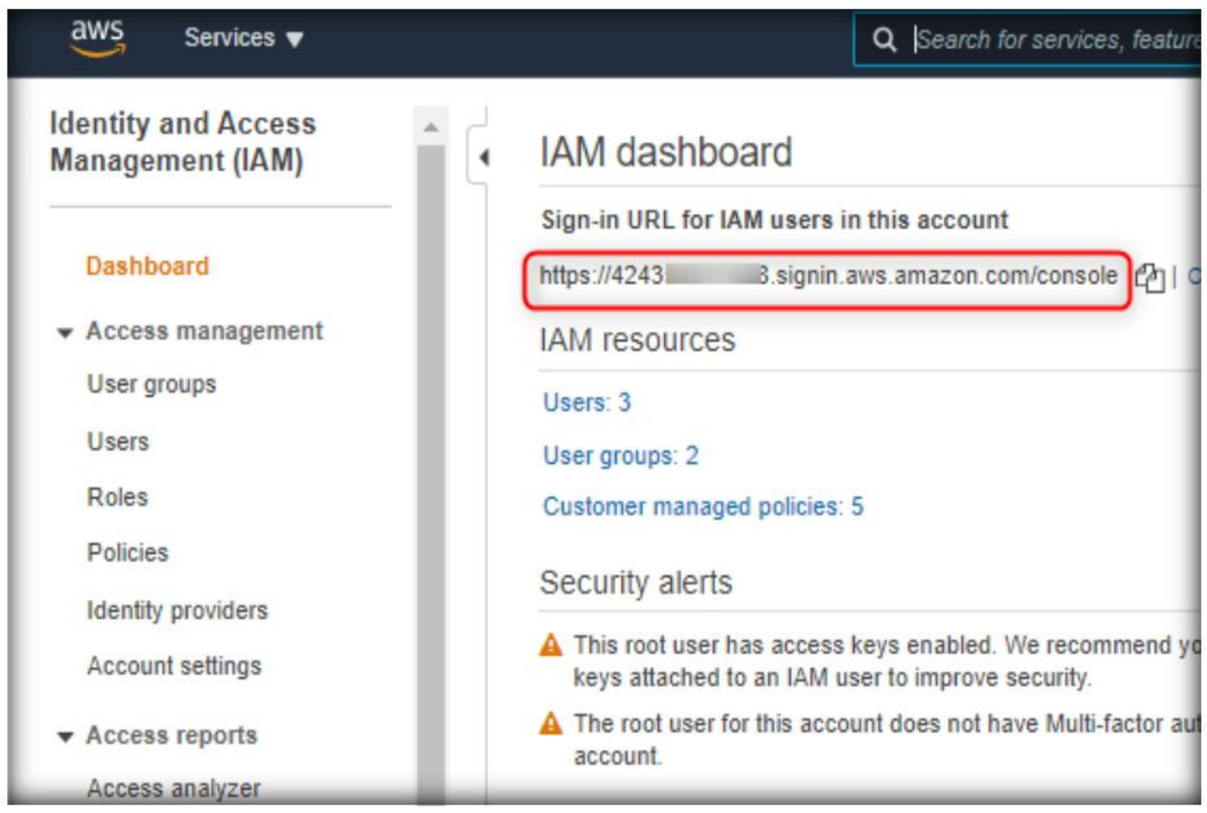


FIGURE 4.5.29: Copying IAM User link

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

32. To login to AWS as a user, open a new incognito Chrome window and paste the copied URL. You will be redirected to **AWS Sign in as IAM user** page; here, type IAM username as the user (**John**) you created and password as **user@123,** and then click on **Sign in**.



FIGURE 4.5.30: Signing into AWS

33. Now, to delete the backup vault, click on the **Services** menu and select **AWS Backup** under **Storage**.

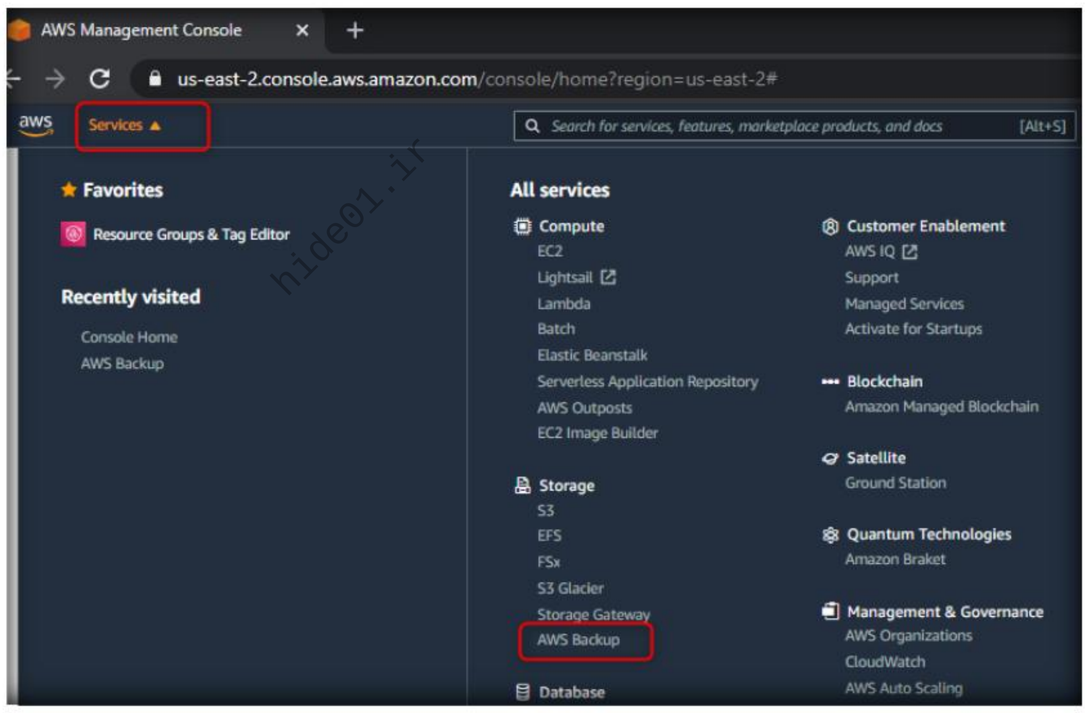


FIGURE 4.5.31: Selecting the AWS Backup Service

34. On the **AWS Backup** page, click on **Backup vaults** from the left navigation pane.

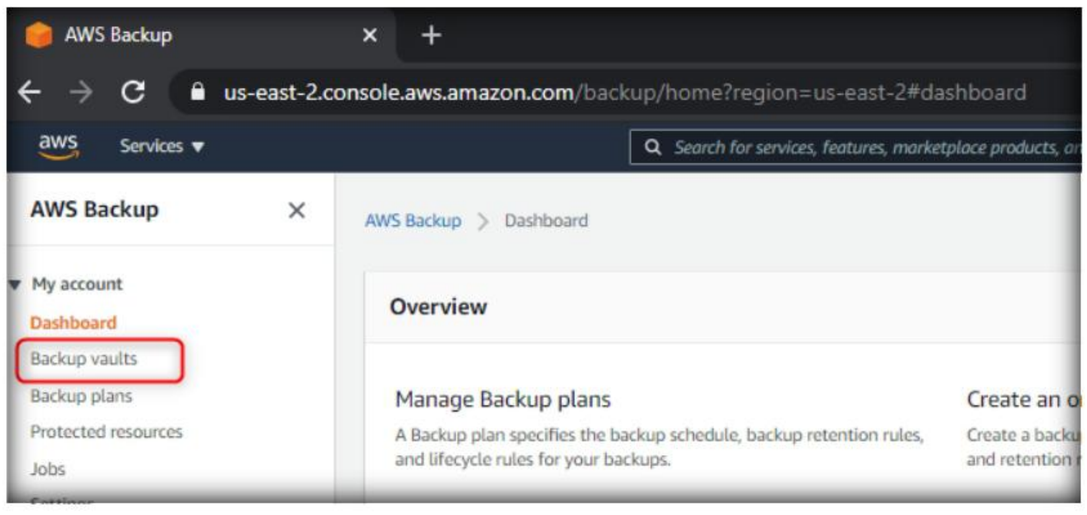


FIGURE 4.5.32: AWS Backup page

35. You can see three backup vaults under **Backup vaults**.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

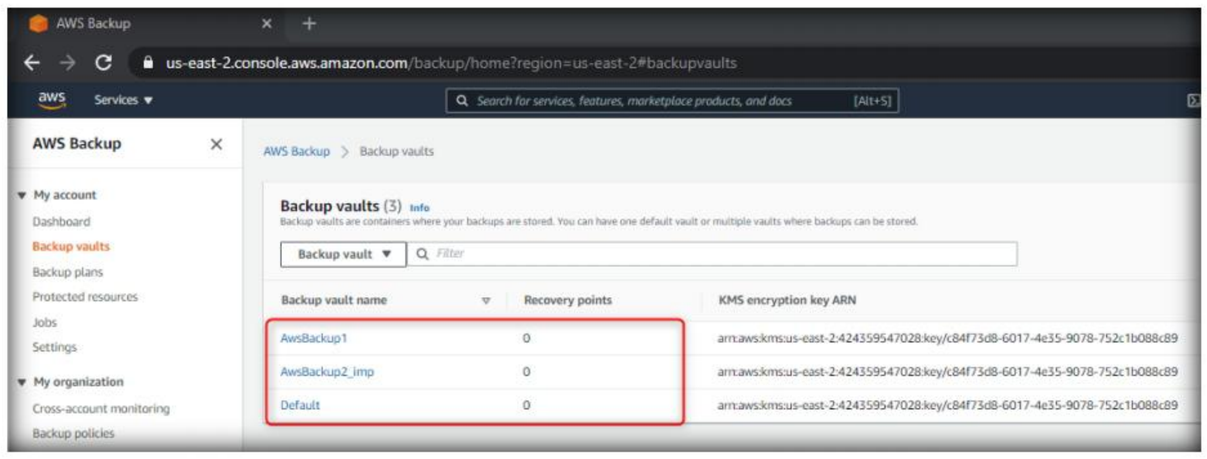


FIGURE 4.5.33: AWS Backup vaults

36. Click on **AwsBackup2_imp**. On the **AwsBackup2_imp** backup vault page, click on **Delete**, as shown in the following screenshot.



FIGURE 4.5.34: Backup vault page

37. In the **Delete backup vault** window, type **AwsBackup2_imp** as the backup vault name to confirm deletion. Then, click the **Delete backup vault** button.

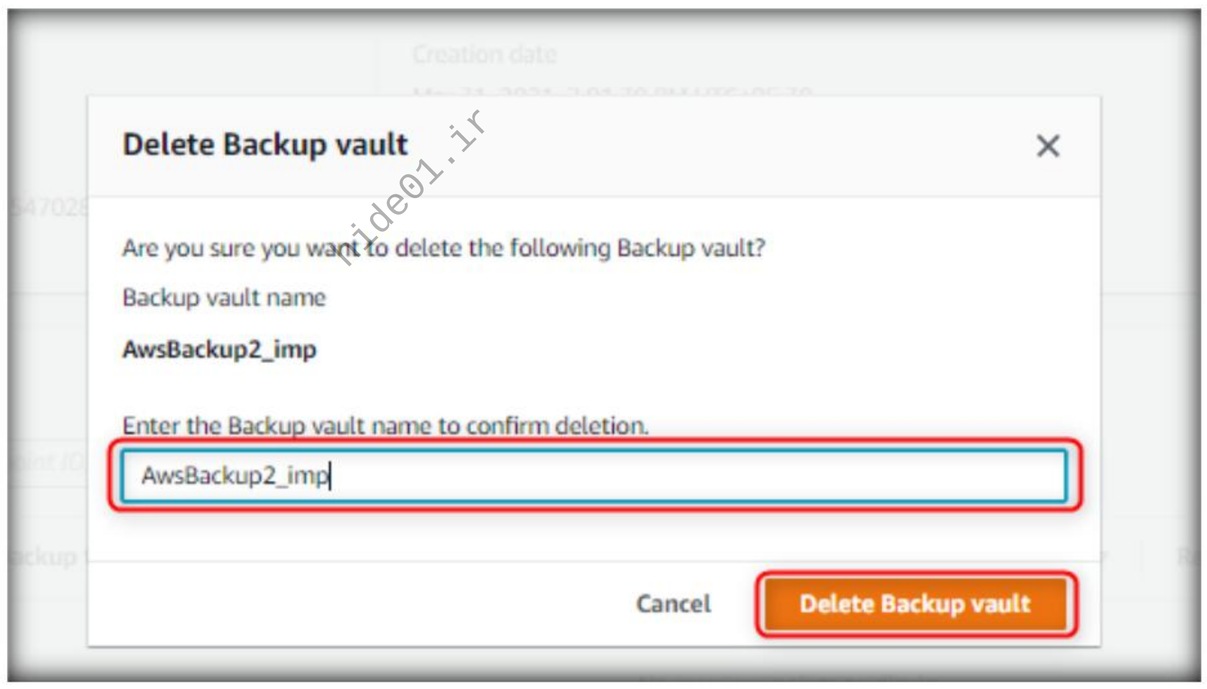


FIGURE 4.5.35: Delete Backup vault page

38. As soon as you click the **Delete Backup vault** button, you will see an **Access Denied** message, as shown in following screenshot.

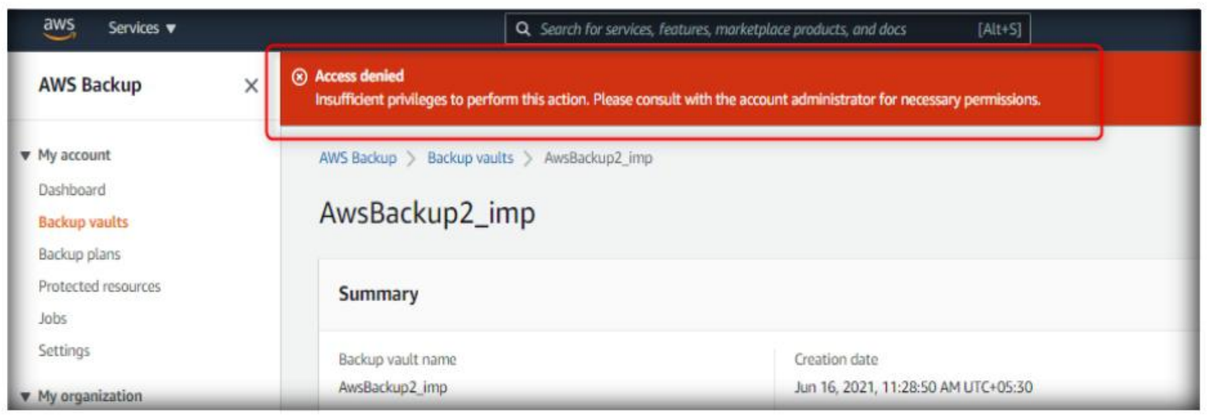


FIGURE 4.5.36: Backup vault cannot be deleted

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

39. The **AwsBackup2_imp** backup vault resource is now restricted by the administrator as you have applied the **DenyBackupvault** policy for the user (**John**).
40. Next, try to delete the **AwsBackup1** backup vault. Click on **Backup vaults** in the left pane to switch to the **Backup vaults** section, and then click on **AwsBackup1**.

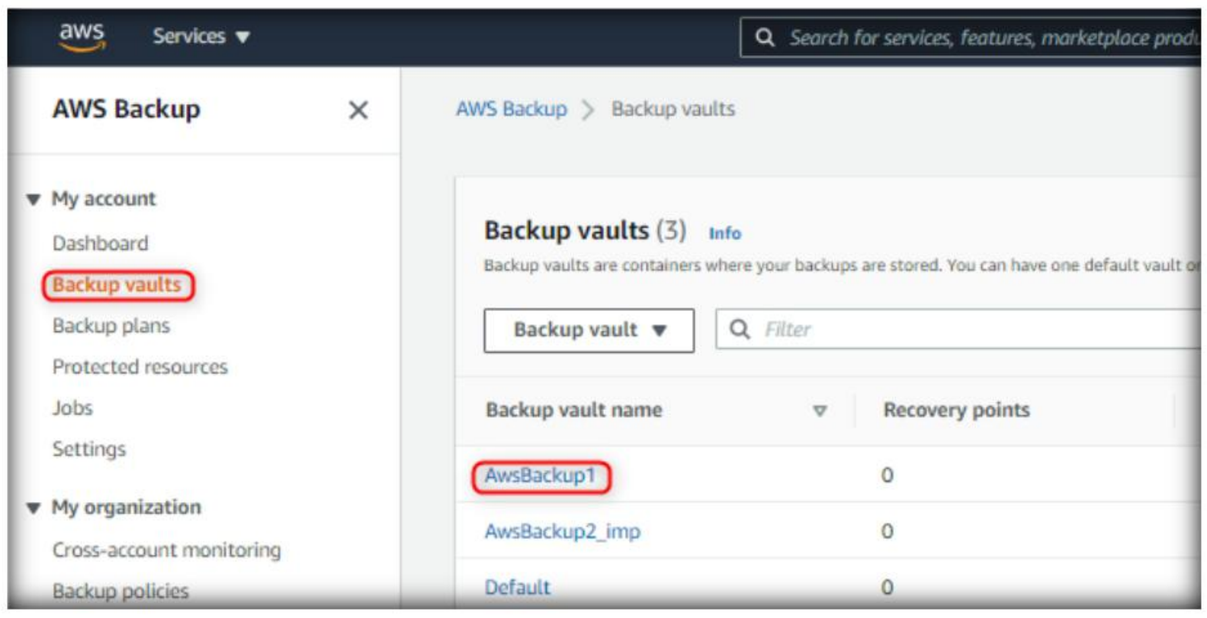


FIGURE 4.5.37: Selecting Backup vault

41. On the **AwsBackup1** page, click on **Delete**.



FIGURE 4.5.38: Backup vault page

42. In the **Delete backup vault** window, type **AwsBackup1** to confirm deletion. Then, click on **Delete backup vault**.

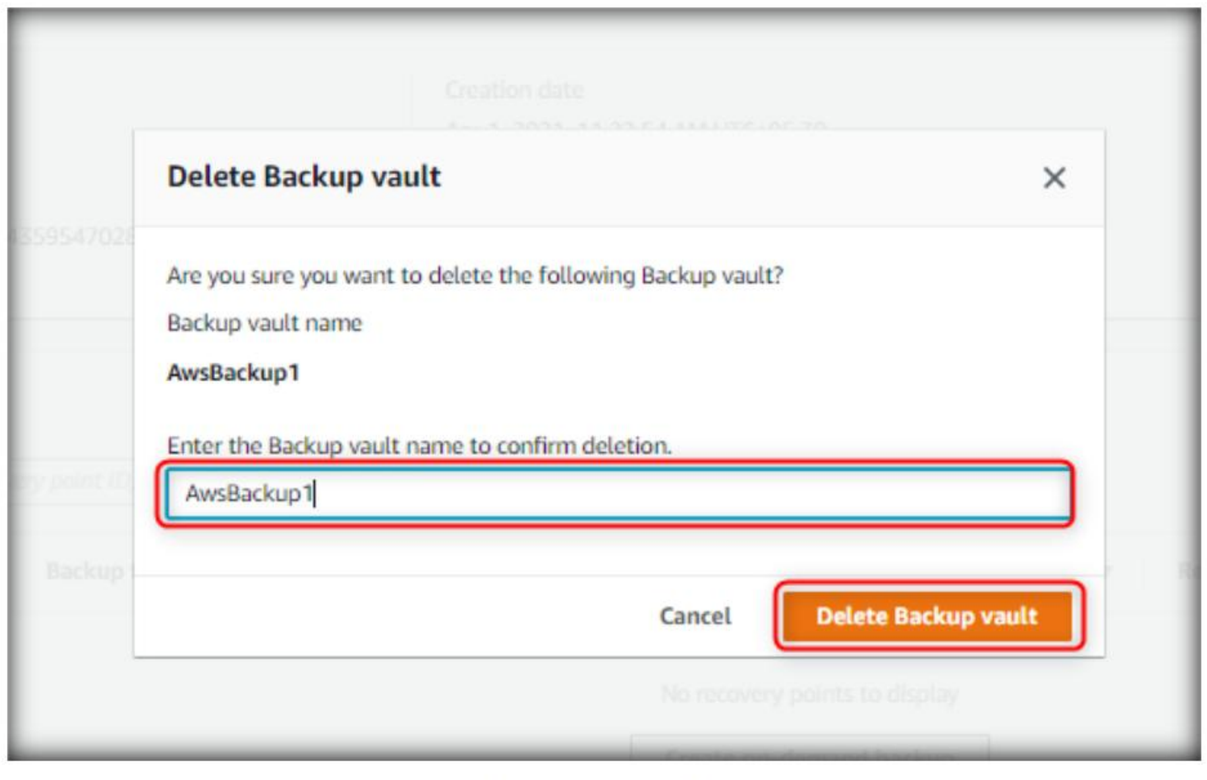


FIGURE 4.5.39: Delete Backup vault page

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

43. The **AwsBackup1** backup vault gets deleted because you have applied the restricted resources policy to **AwsBackup2_imp** only. Therefore, the user can delete the **AwsBackup1** backup vault resource but not the **AwsBackup2_imp** backup vault.

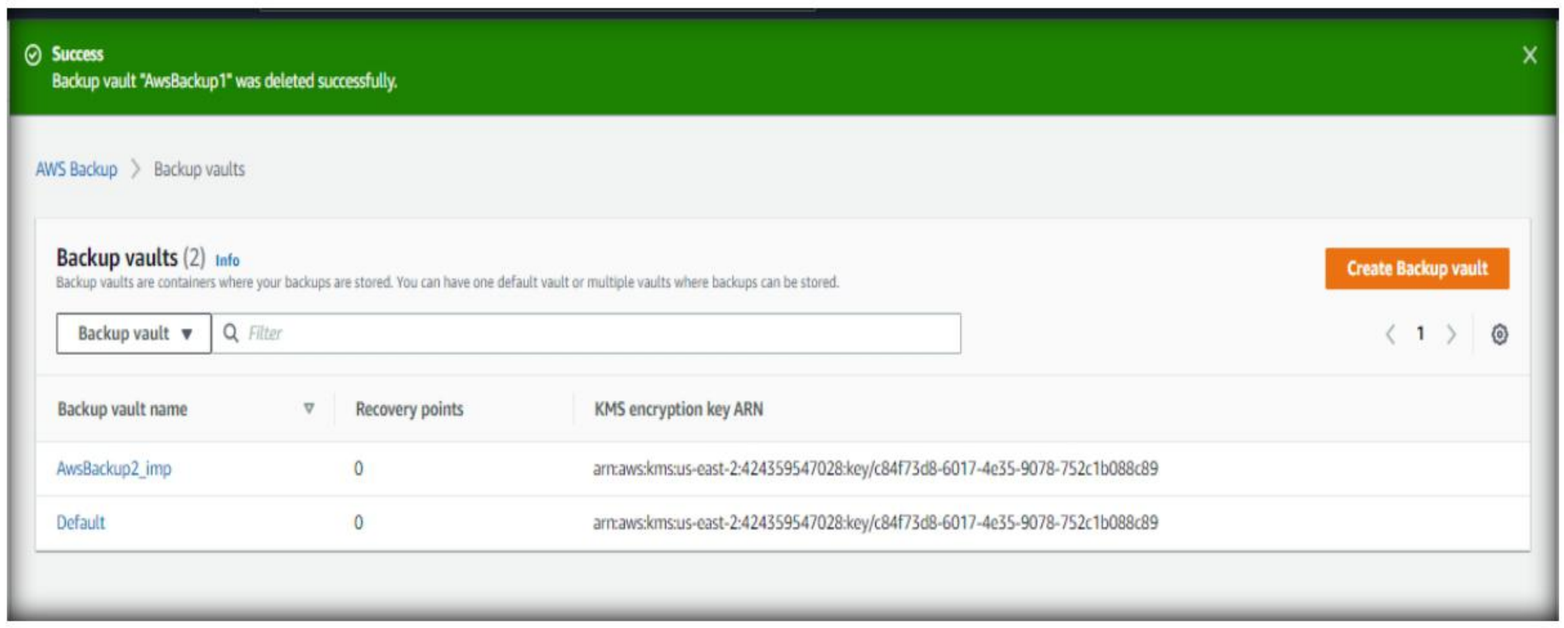


FIGURE 4.5.40: Backup vault Deleted

44. This way, a cloud security engineer can apply a restricted resources policy for specific users and/or specific resources.

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

45. Now, delete the instances created in this lab. Navigate to the **Backup vaults** under AWS Backup in the AWS console and click on the instance created in this lab (here, **AwsBackup2_imp**). Click on the **Delete** button. In the pop-up window, enter the vault's name and click on **Delete Backup vault****.

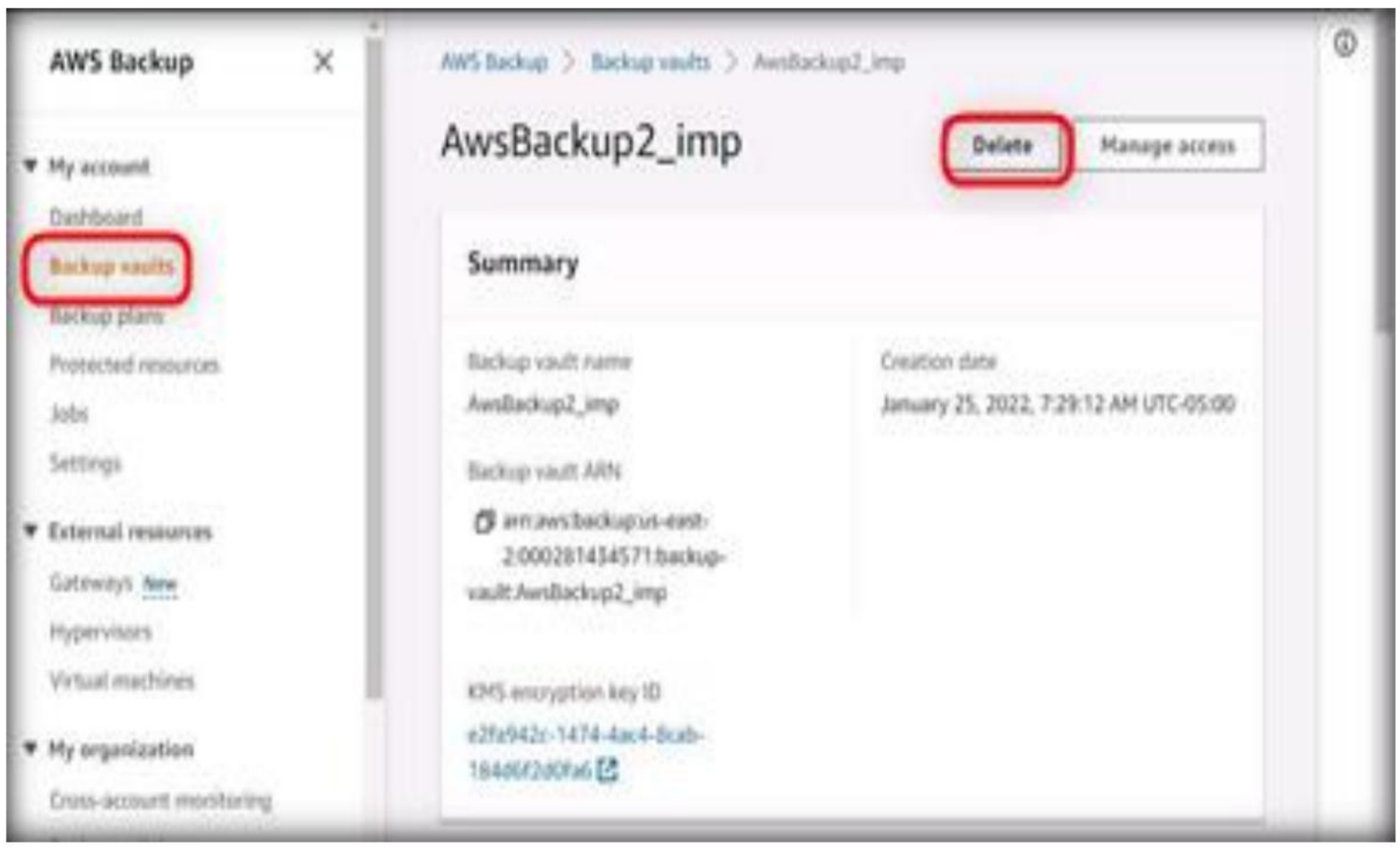


FIGURE 4.5.41: Deleting Backup Vault

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

46. Navigate to **Users** under the IAM console and select the user created in this lab (here, **John**). Select the checkbox and click on the **Delete** button. In the pop-up window, enter the user's name and click on **Delete**.



FIGURE 4.5.42: Deleting User

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.

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab

6

Preventing Accidental Deletion and Modification of S3 Objects using S3 Object Lock

The Amazon S3 Object Lock feature can be used to retain objects for a specific amount of time without being accidentally deleted or modified.

ICON KEY

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

Lab Scenario

If an organization needs to store S3 objects for a certain period and prevent it from getting deleted accidentally, cloud security engineers can use the S3 Object Lock feature. When the S3 Object Lock compliance mode is enabled for S3 objects for a certain period, even the root user cannot delete these objects during that period. This prevents the accidental deletion of S3 objects and satisfies compliance requirements. This lab demonstrates how to enable S3 Object Lock for a certain period to prevent the accidental deletion of objects.

Lab Objectives

This lab demonstrates how to create an S3 bucket with object lock enabled, upload objects, enable object lock, and verify S3 Object Lock.

In this lab, you will learn the following:

- Creating an S3 bucket with object lock enabled
- Uploading objects and enabling compliance mode retention
- Verifying the configuration

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Environment

To perform this lab, you need the following:

- Admin Machine VM
- Administrative privileges
- Registered AWS account

Lab Duration

Time: 10 minutes

Overview of Amazon S3 Object Lock

Amazon S3 has an object lock feature which can be used by cloud security engineers to retain S3 objects for a period or permanently without being accidentally deleted. In this period, the S3 object cannot be deleted or overwritten. S3 Object Lock is a write-once-read-many (WORM) feature, i.e., an information once written cannot be modified. Apart from protecting objects from accidental deletion, the object lock feature helps to meet regulatory compliance requirements for objects that require retention for a certain period and it also prevents ransomware threats. S3 Object Lock provides two modes of retention, namely governance mode and compliance mode. When governance mode is enabled, only IAM users with special permissions or the root user can delete S3 objects. In compliance mode, even the root user cannot delete or overwrite S3 objects. Moreover, when compliance mode is enabled, the retention mode cannot be changed and the retention period cannot be reduced before this period ends.

guide01.ir

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., AWS), the application interface may be updated with time. Hence, when working on an updated version of AWS, the user interface may differ from that shown in the lab. Consequently, the steps and screenshots demonstrated in this lab might also differ.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Note: Before starting this lab, you should create an AWS Free Tier account using the following link: https://aws.amazon.com/free/, in case you have already not created it for the previous module. Once the registration is complete, perform the following task:

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

TASK 1

Creating S3 bucket with Object Lock enabled

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

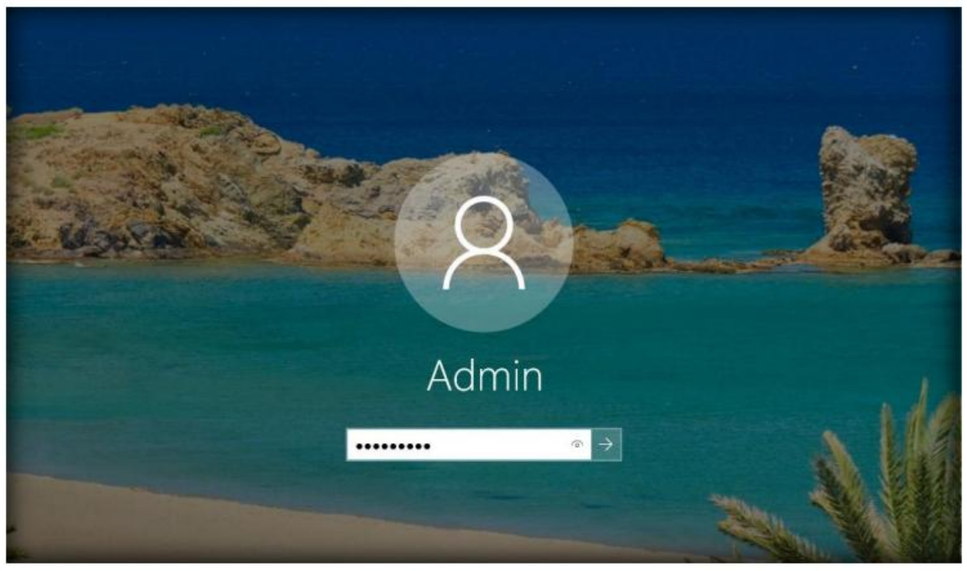


FIGURE 4.6.1: Launch Admin Machine and Log in

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



FIGURE 4.6.2: Navigating to the Chrome Browser from Taskbar

3. The **Google Chrome** browser opens. Go to the address bar, type **https://aws.amazon.com/**, and press **Enter**.

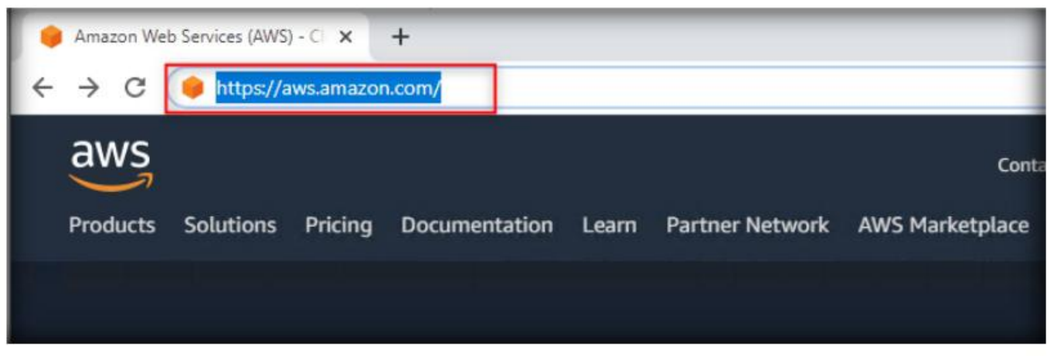


FIGURE 4.6.3: Access AWS in Browser

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

4. The **AWS Web Services – Cloud Computing Services** page appears. Click on **AWS Management Console** from the **My Account** drop-down menu, as shown in the screenshot below.

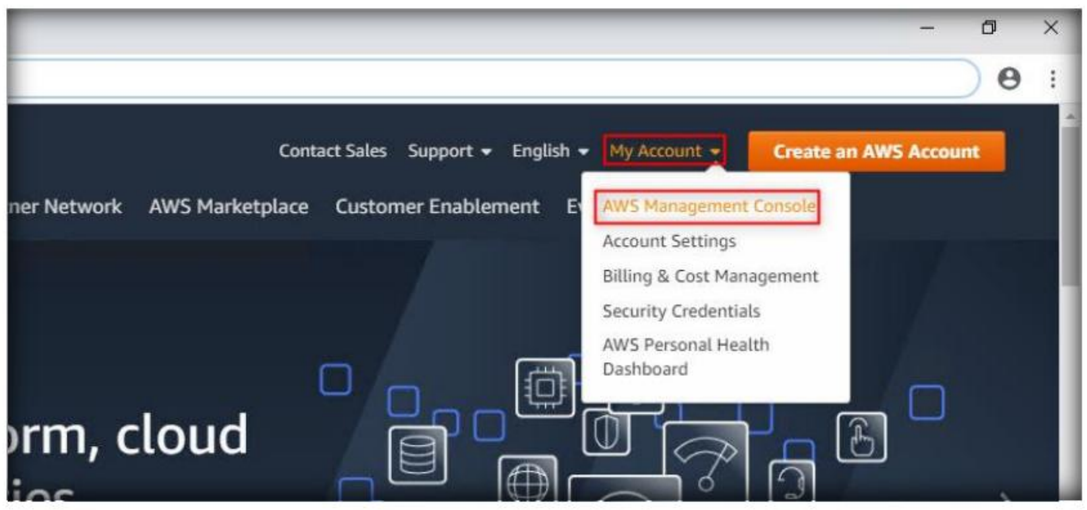


FIGURE 4.6.4: Navigate to AWS Management Console

5. The **AWS Web Services Sign in** page appears. Select **Root user** and type the AWS administrator account ID (root user email address), as shown in the screenshot below, and click on **Next**.



FIGURE 4.6.5: Sign in to AWS

6. The **Security check** page appears; type the characters shown in the image and click on **Submit.**

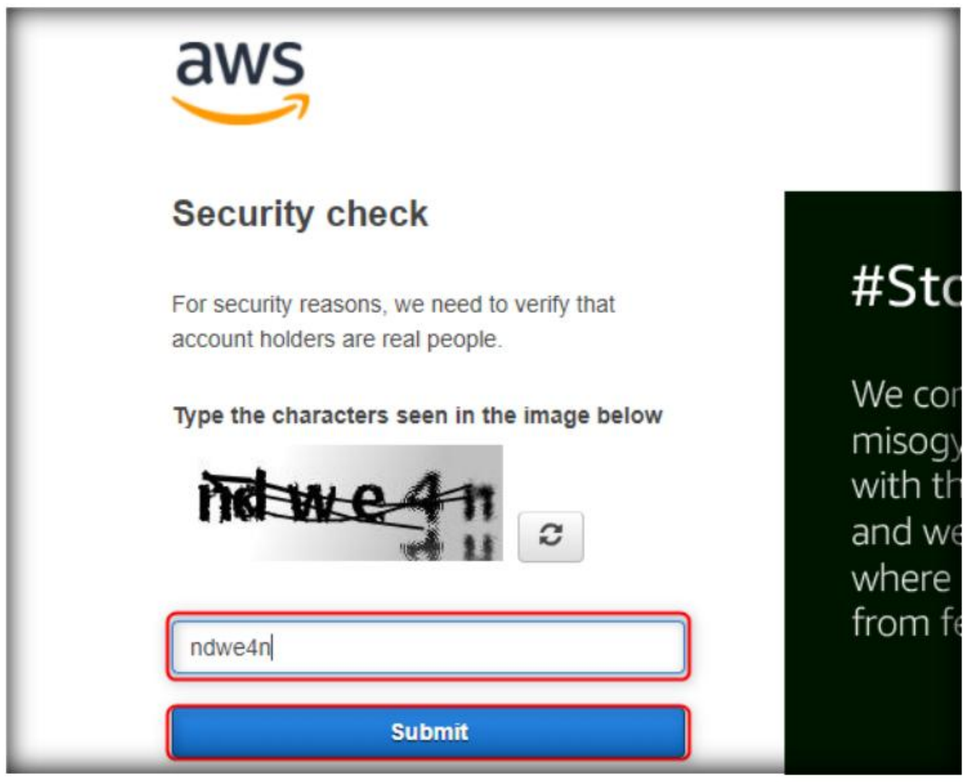


FIGURE 4.6.6: Typing the Characters for Security Check

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

7. In the **Password** field, type the password and click on **Sign in**, as shown in the screenshot below.



FIGURE 4.6.7: Sign in to AWS

8. Now, to create an S3 bucket, select **Services** from the menu bar and click on **S3** under **Storage**.

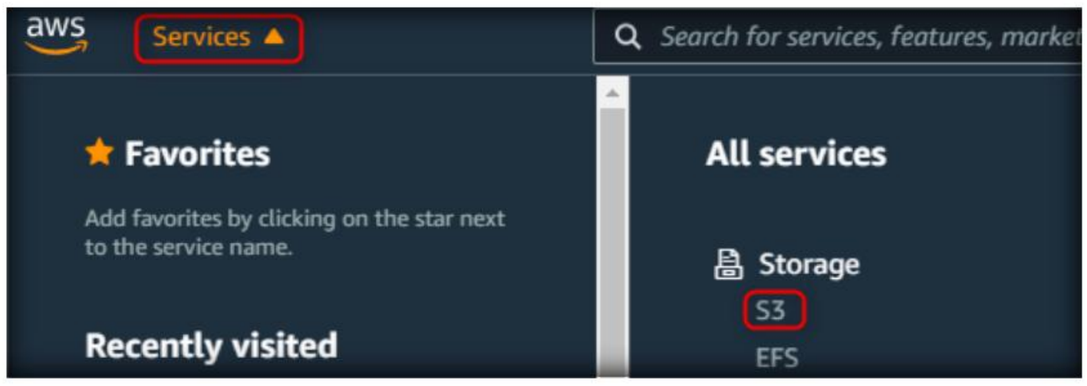


FIGURE 4.6.8: Navigating to AWS S3

9. In the **Amazon S3** window, click on **Create bucket.**

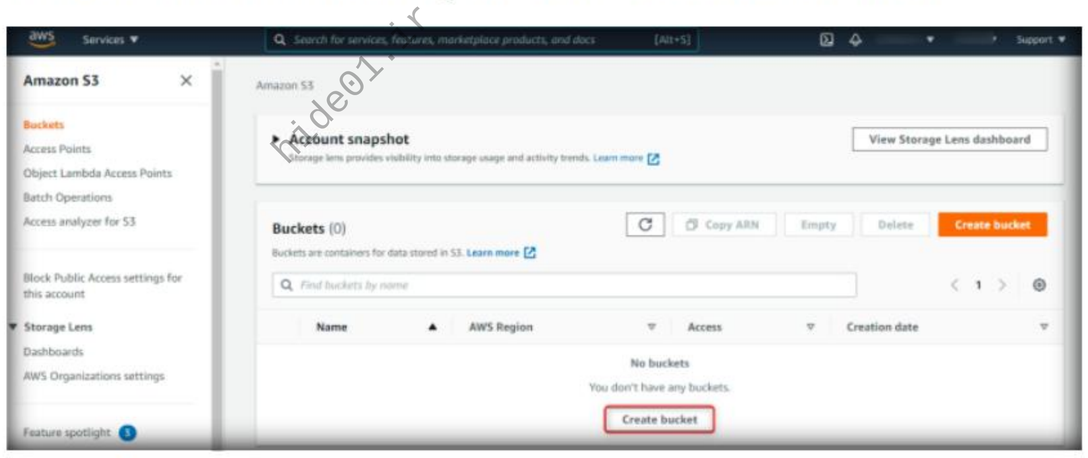


FIGURE 4.6.9: Creating S3 Bucket

10. In the **Create bucket** window, enter a name under **Bucket name**; here, we used **ecc-demobucket**. Under **AWS Region**, select an appropriate region; here, we selected **us-east-1**.

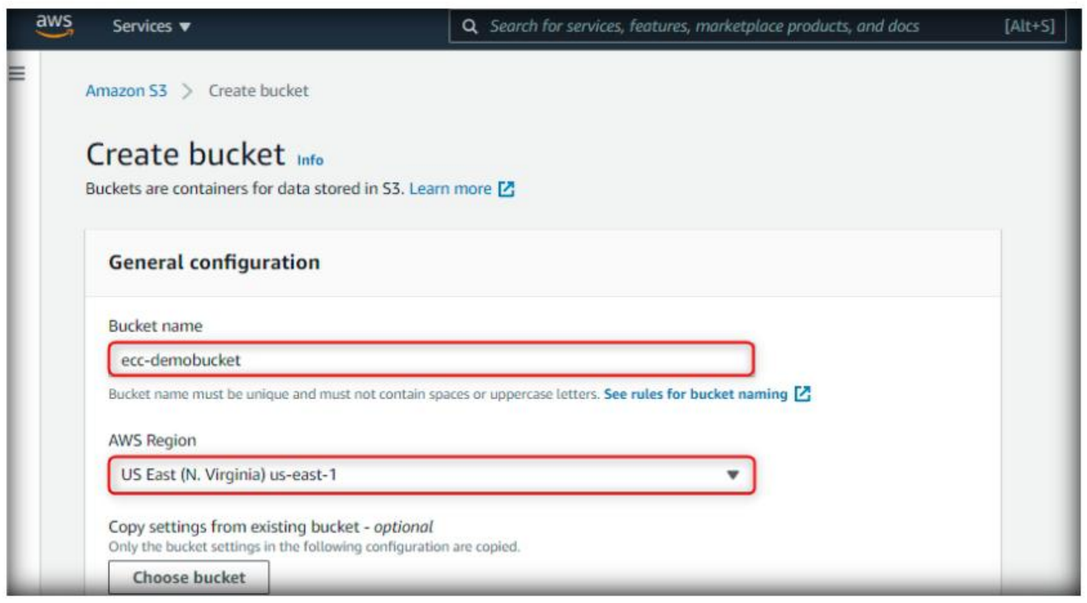
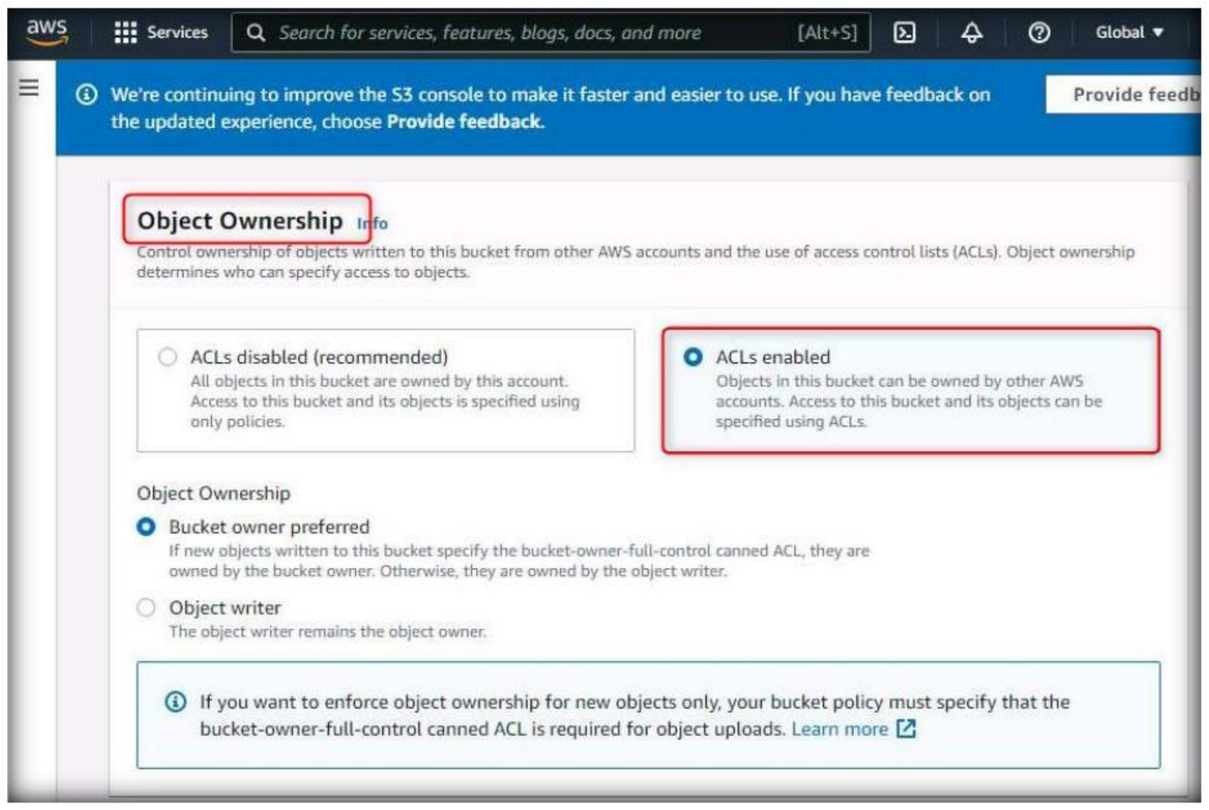


FIGURE 4.6.10: Configuring Bucket

Certified Cloud Security Engineer Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

11. Scroll down to **Object Ownership** and click on **ACLs enabled**, then navigate to **Bucket Versioning**. Because S3 Object Lock only works with versioned buckets, enable bucket versioning for this S3 bucket. Select the radio button for **Enable** under **Bucket Versioning**.



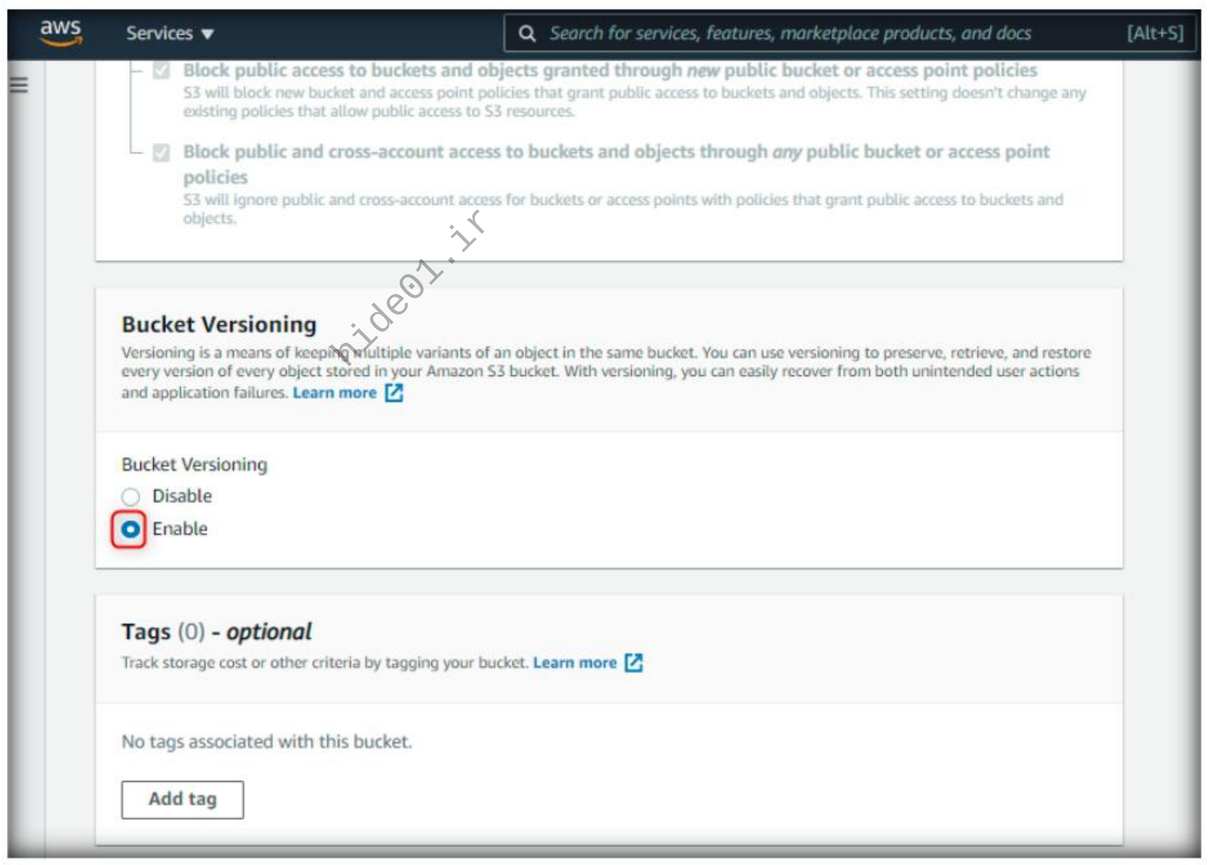


FIGURE 4.6.11: Enabling Bucket Versioning

12. Scroll down and expand **Advanced settings**. To enable object lock for an S3 bucket, select the radio button for **Enable** under **Object Lock**.

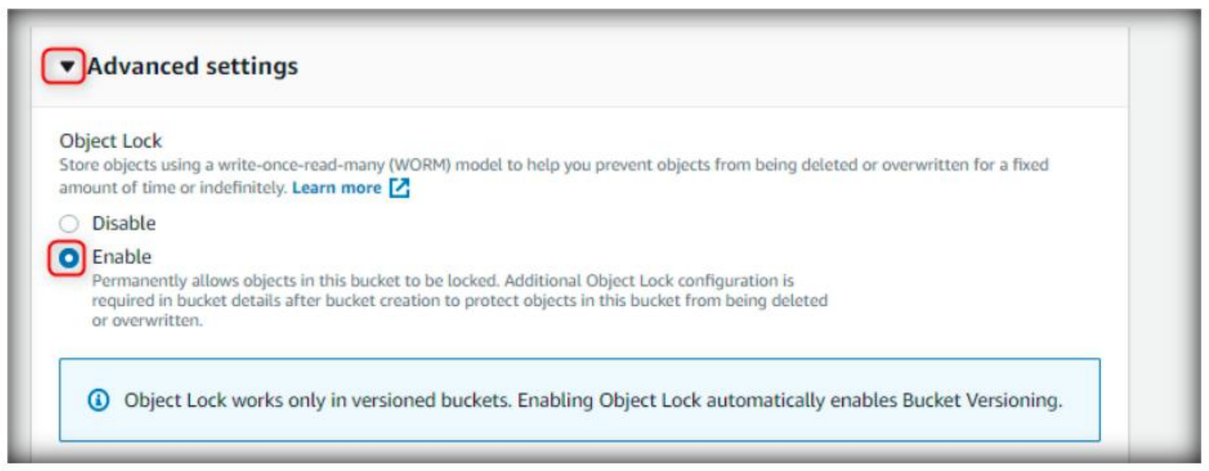


FIGURE 4.6.12: Enabling Object Lock

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

13. Select the checkbox for acknowledgment. Click on **Create bucket**.

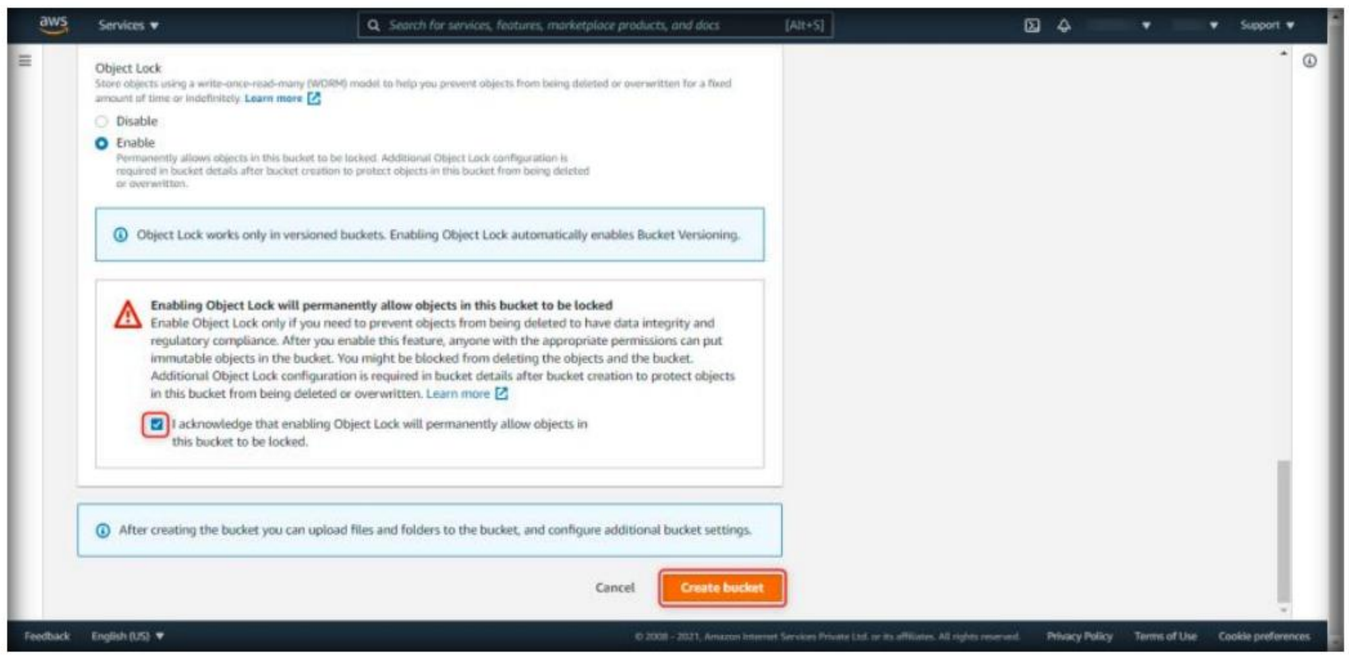


FIGURE 4.6.13: Selecting Acknowledgment and Creating Bucket

14. A message is displayed at the top stating that the bucket has been successfully created.

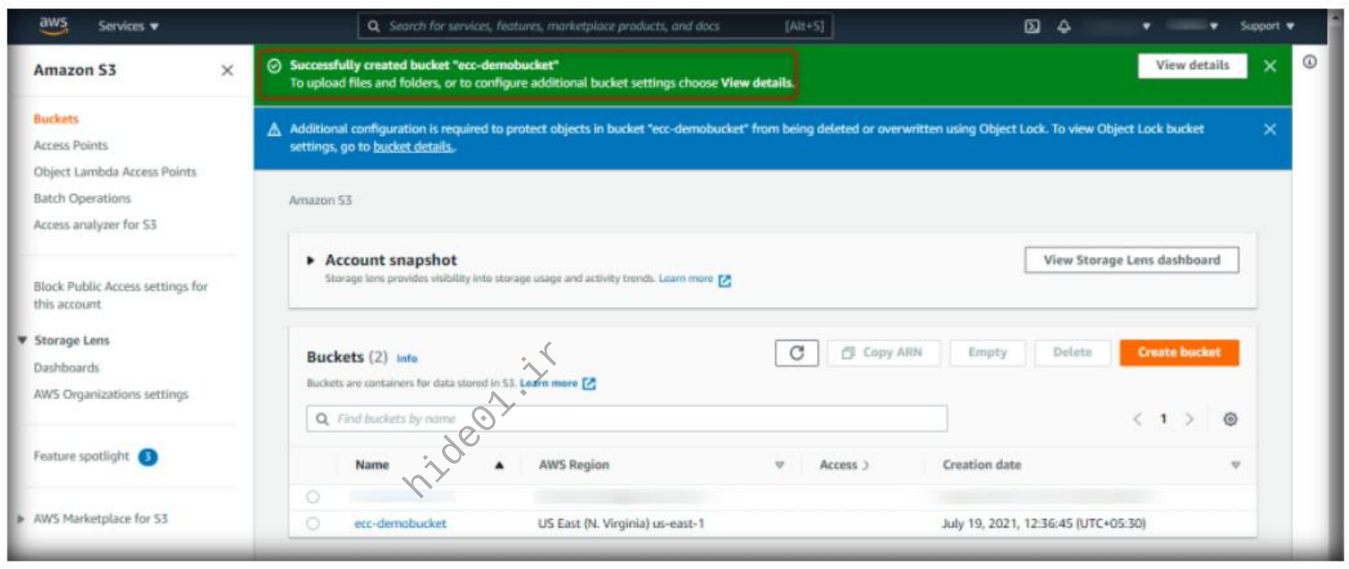


FIGURE 4.6.14: Bucket Created Successfully

TASK 2

Uploading object and enabling compliance mode retention

15. Now, upload an object into the S3 bucket and enable object lock. To upload an object into the S3 bucket, click on the S3 bucket name (**ecc-demobucket**) to open the bucket info page.

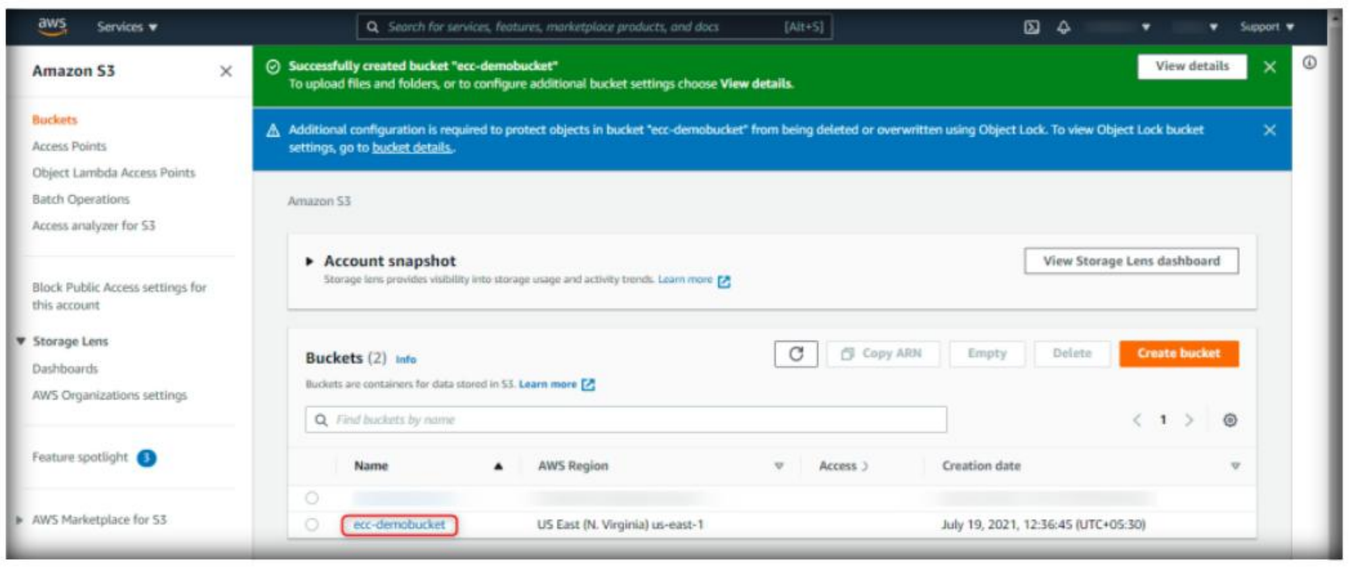


FIGURE 4.6.15: Opening the Bucket Info Page

16. Before you start uploading objects into the S3 bucket, create a text file on the desktop and upload it as the object. Here, we created a text file on the desktop named **test-OL.txt**.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

17. Click on **Upload** to upload the object into the S3 bucket.

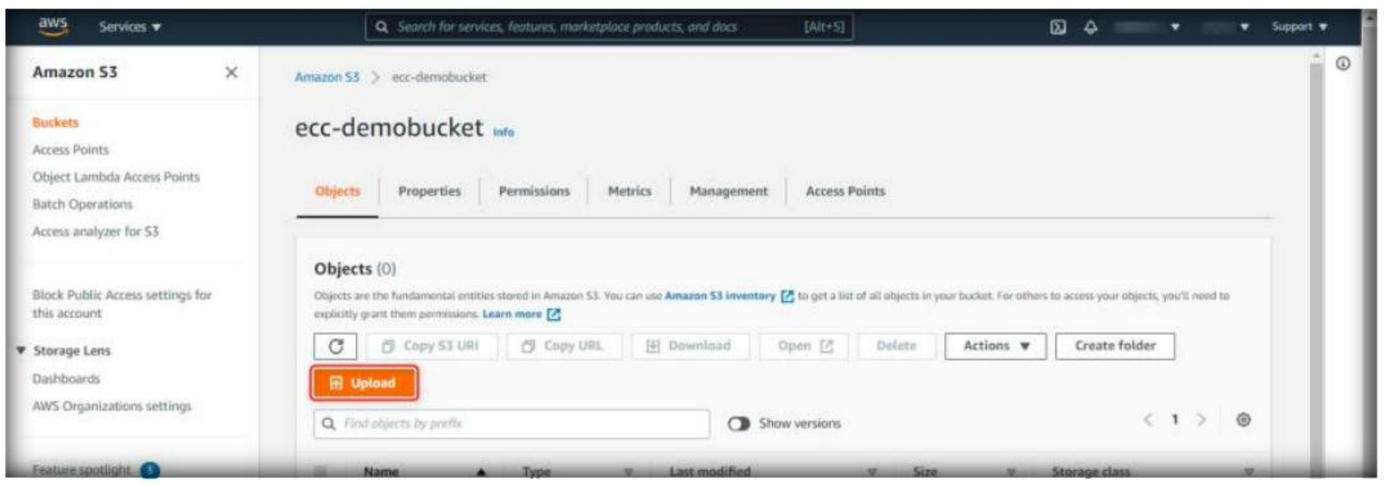
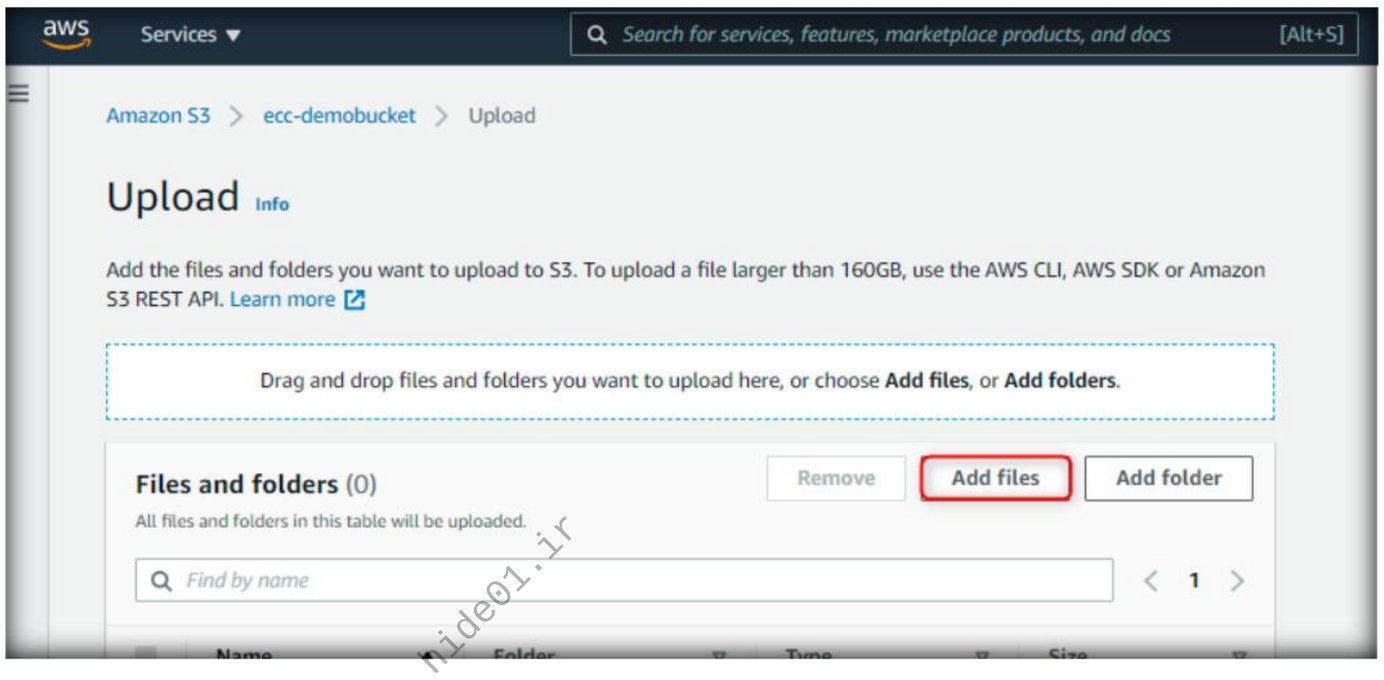


FIGURE 4.6.16: Click Upload

18. The **Upload** window opens. To add files to upload into the S3 bucket, click on **Add files**.



nide01.ir

FIGURE 4.6.17: Click on Add Files

19. Select the text file (**test-OL.txt**) created by you on the desktop to upload as the S3 object. Click on **Open**.

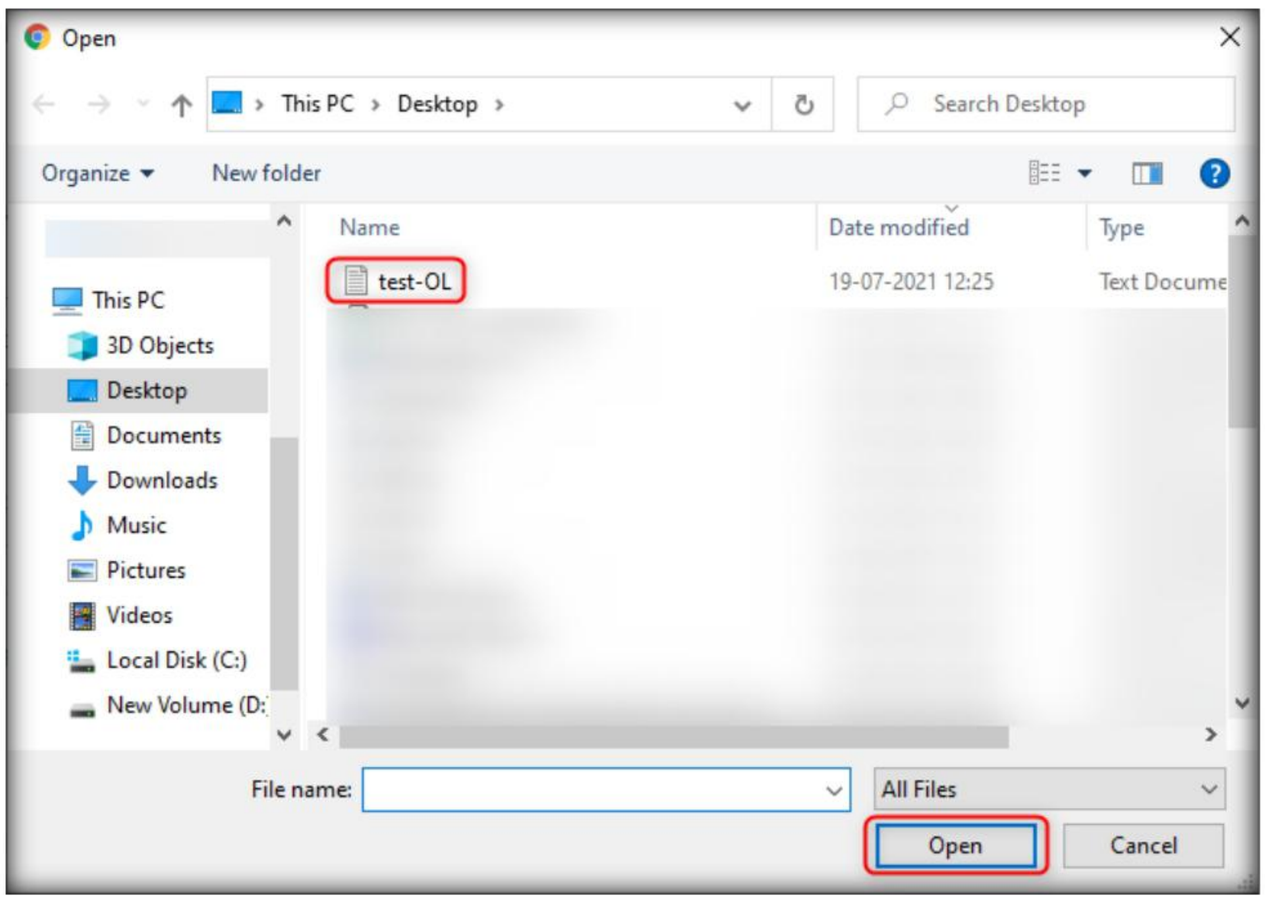


FIGURE 4.6.18: Selecting the File to Add

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

20. The text file gets added successfully. To upload the text file as an S3 object, scroll down and click on **Upload**.

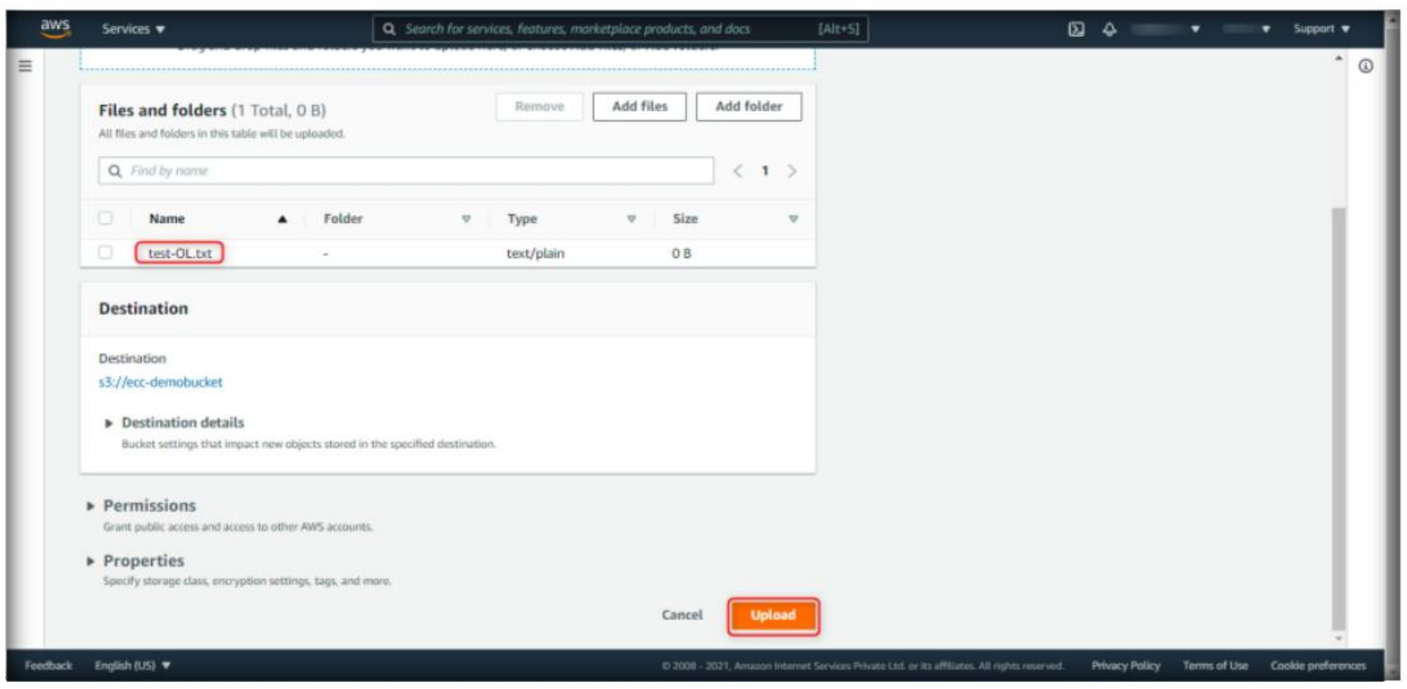
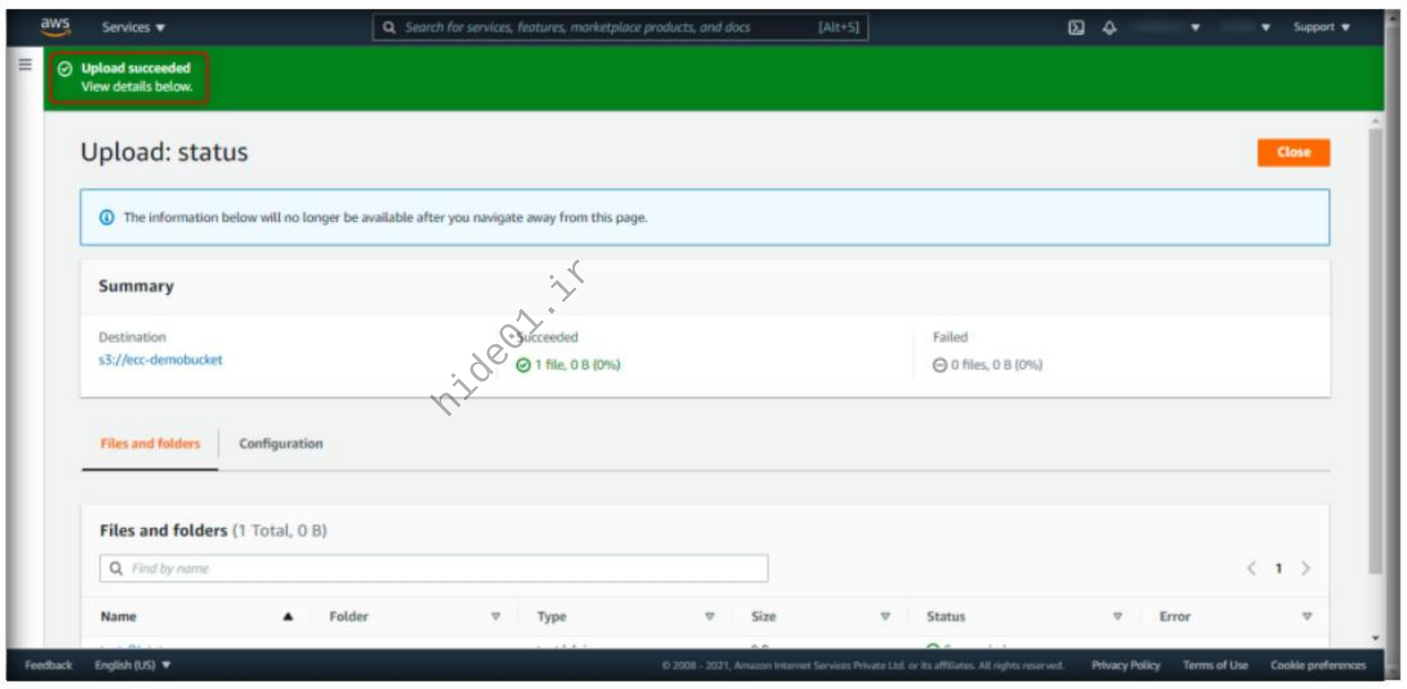


FIGURE 4.6.19: Click on Upload to Upload Objects

21. A message is displayed at the top stating that the file has been uploaded successfully. Click on **Close** to exit the window.



hide01.ir

FIGURE 4.6.20: File Uploaded Successfully

22. Now, you will be in the S3 bucket info window. Enable the compliance mode of object lock for the object. To enable object lock, click on the name of the object to open the object info window.

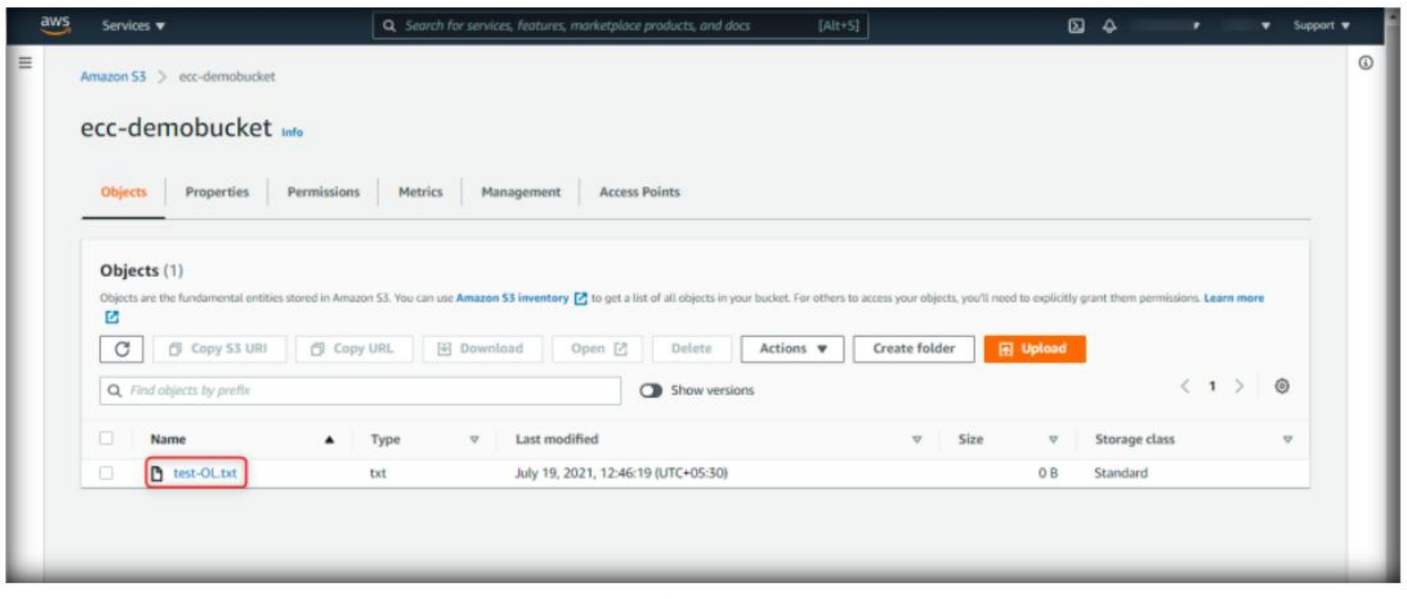


FIGURE 4.6.21: Click on Object Name to Open Info Window

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

23. In the object info window, scroll down to **Object Lock retention**. Click on **Edit** next to **Object Lock retention**.

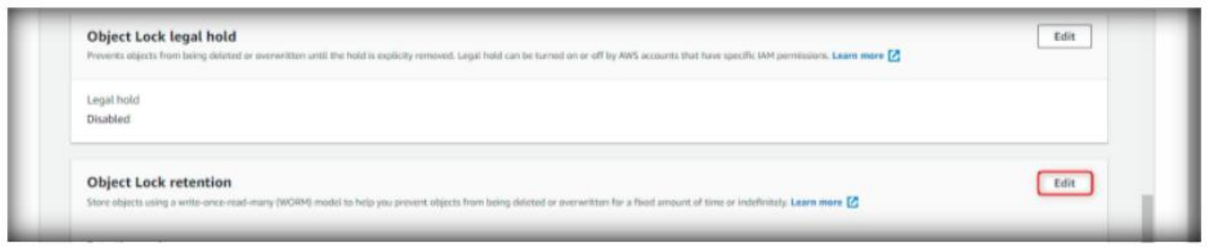


FIGURE 4.6.22: Editing Object Lock Retention

24. The **Edit Object Lock retention** window opens. For **Retention**, select the radio button for **Enable**. Subsequently, more configuration options appear. Now, to enable complete protection of the S3 object from deletion or modification, select the radio button for **Compliance mode** under **Retention mode**. For **Retain until date**, specify a date up to which the object should be retained.

Note: For lab purposes, select the nearest date, preferable the next day, under **Retain until date** because the object cannot even be deleted by the root user if compliance mode is enabled.

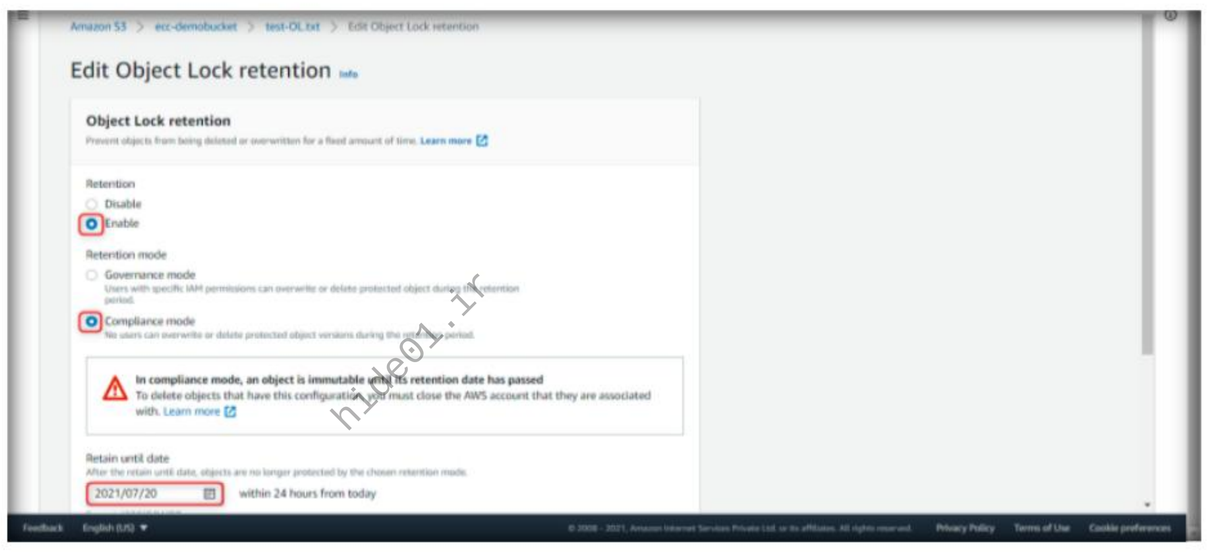


FIGURE 4.6.23: Configuring Object Lock Retention Settings

25. Scroll down to the bottom. To save the retention configuration, click on **Save changes**.

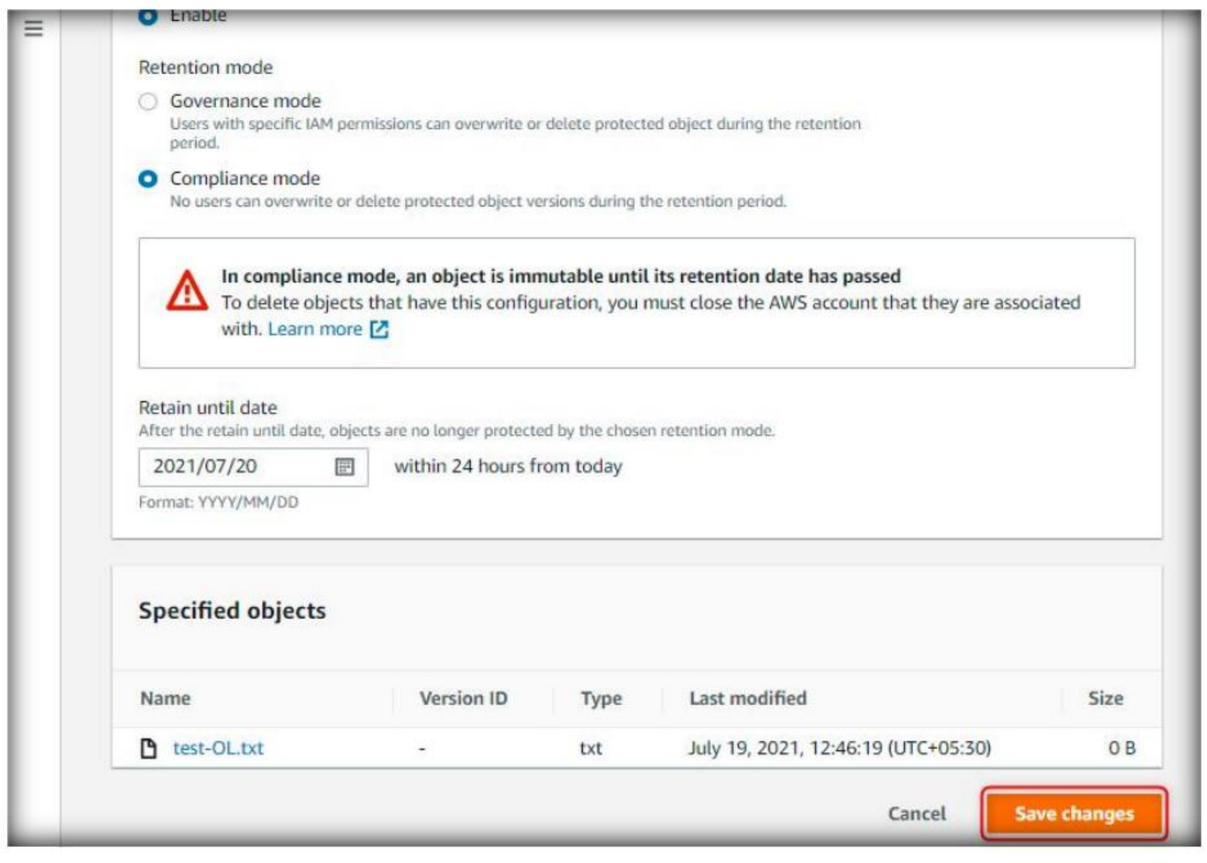


FIGURE 4.6.24: Click on Save Changes to Save the Configuration

Certified Cloud Security Engineer Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

26. A message is displayed at the top stating that Object Lock retention for the object has been edited.

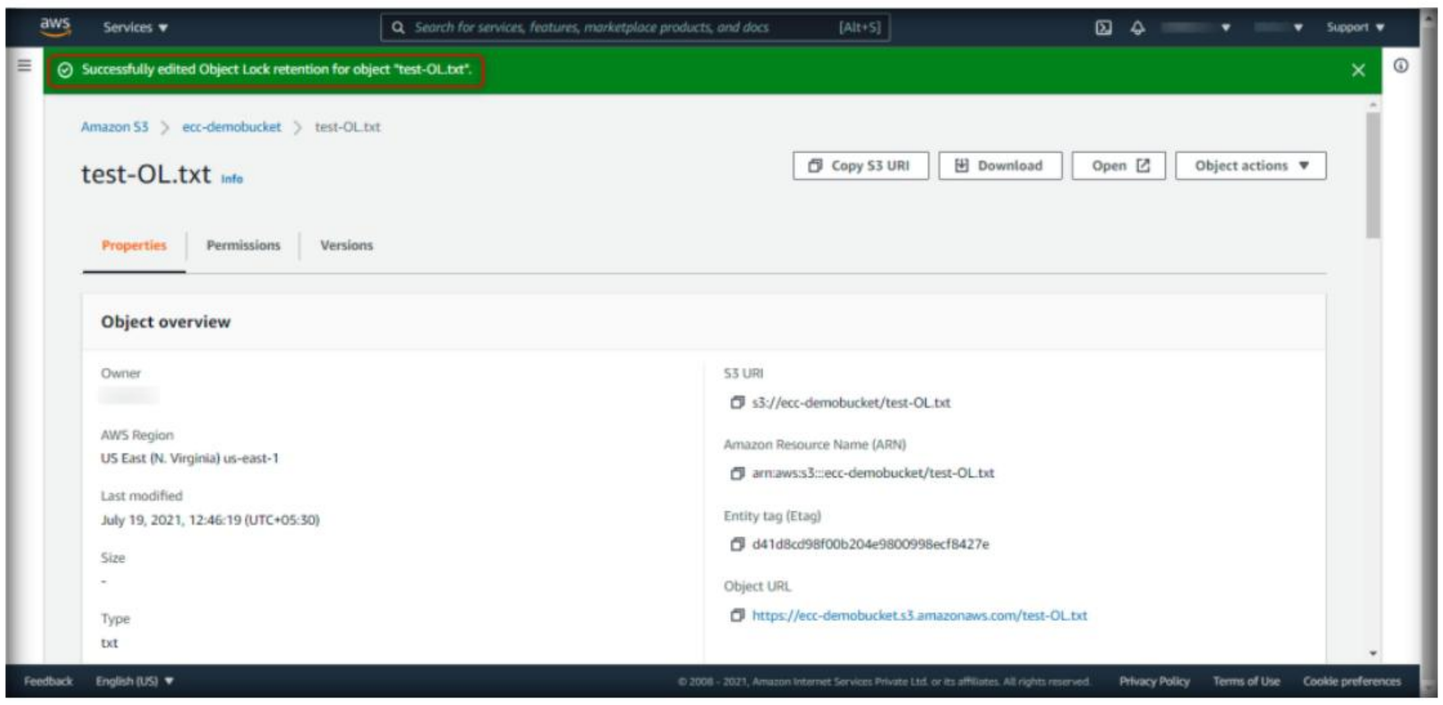


FIGURE 4.6.25: Successfully Edited Object Lock Retention

27. Click on the name of the bucket (**eccdemo-bucket**) at the top to go back to the bucket information window.

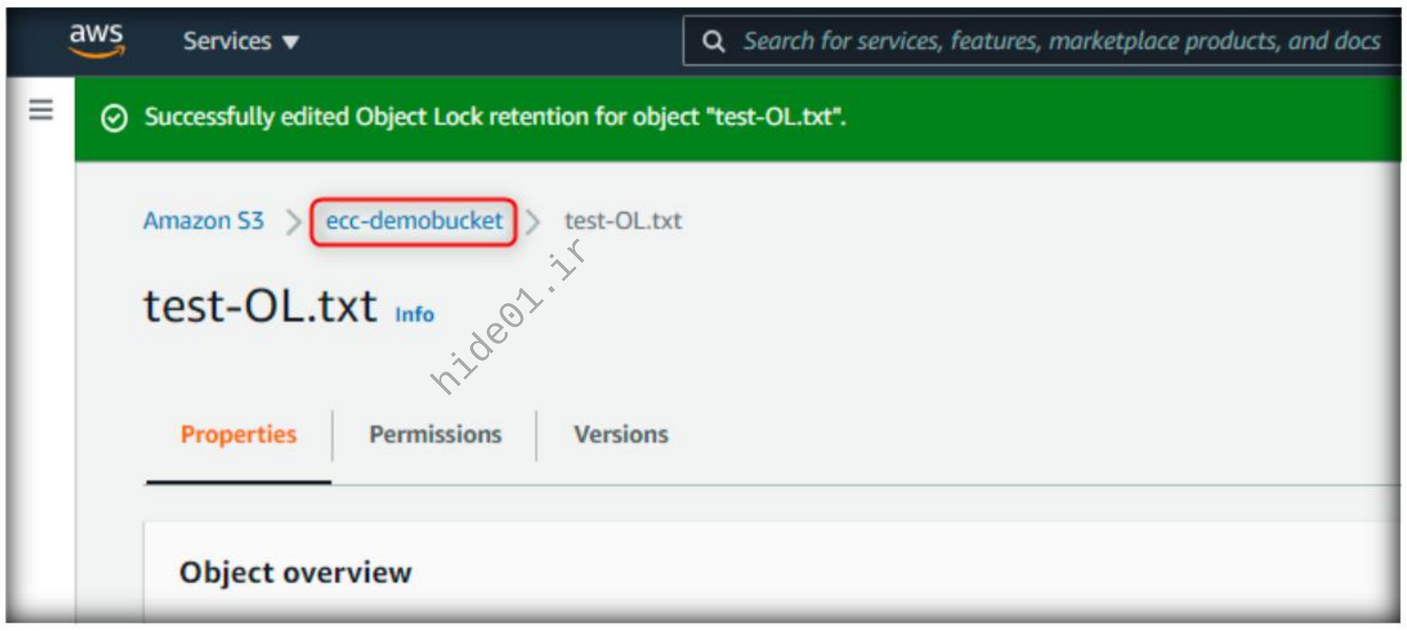


FIGURE 4.6.26: Click on Bucket Name to Go Back to Bucket Info Window

TASK 3

Verifying the object lock configuration

28. Now, verify whether the retention mode can be changed. Click on the name of the S3 object (**test-OL.txt**) to open the object info window.

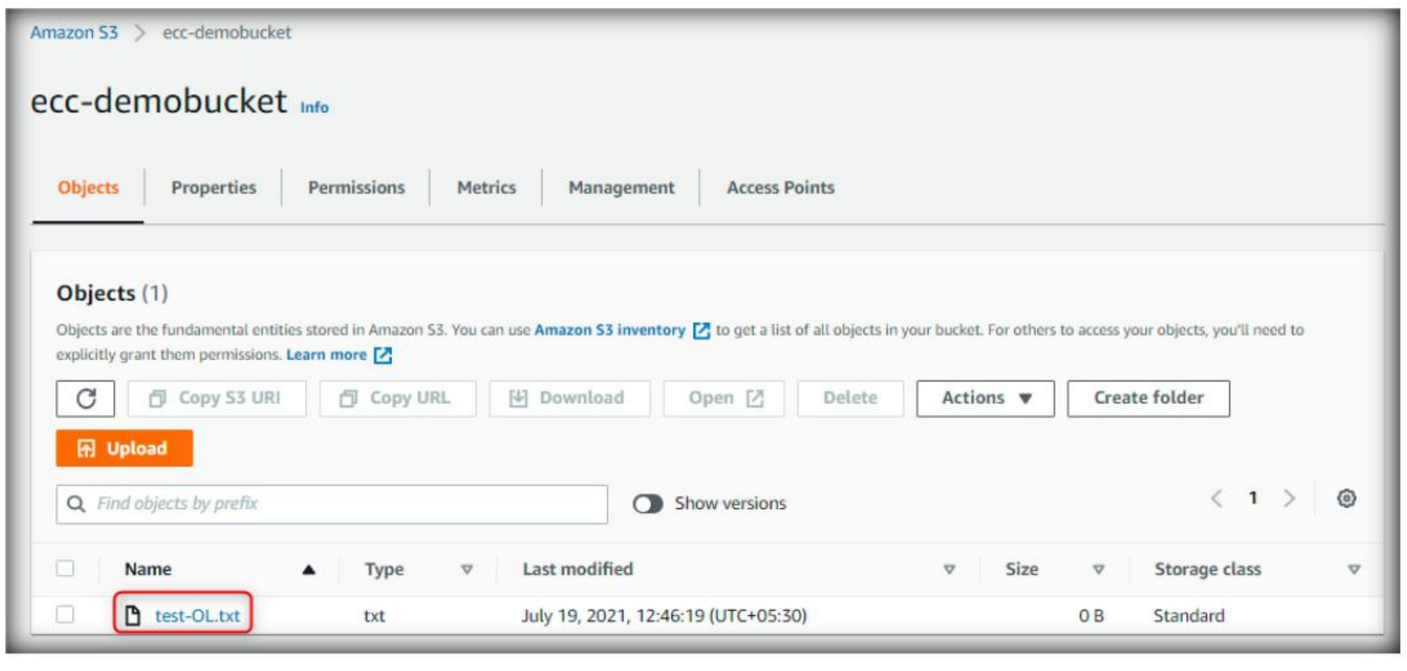


FIGURE 4.6.27: Select Object Name to Open Info Window

Certified Cloud Security Engineer Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

29. In the object info page, scroll down to **Object Lock retention**. Click on **Edit**.



FIGURE 4.6.28: Editing Object Lock Retention

30. You can see that the **Disable** option for **Retention** is not active. Additionally, the **Governance mode** under **Retention mode** is not active. You can make changes to Object Lock retention only after the retention date.

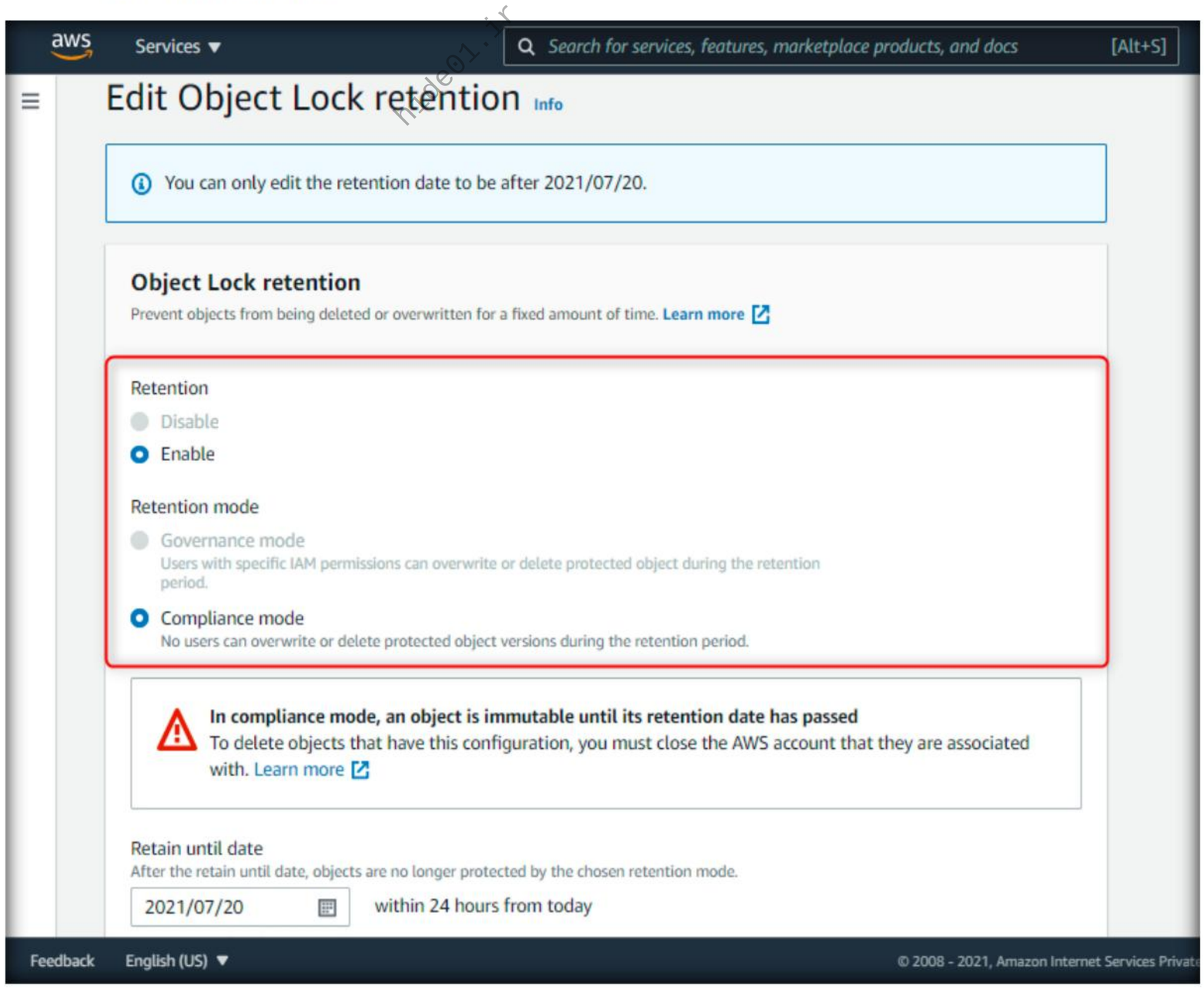


FIGURE 4.6.29: Object Lock Retention

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

31. Now, click on the name of the S3 bucket (**eccdemo-bucket**) at the top to go back to the bucket info window.

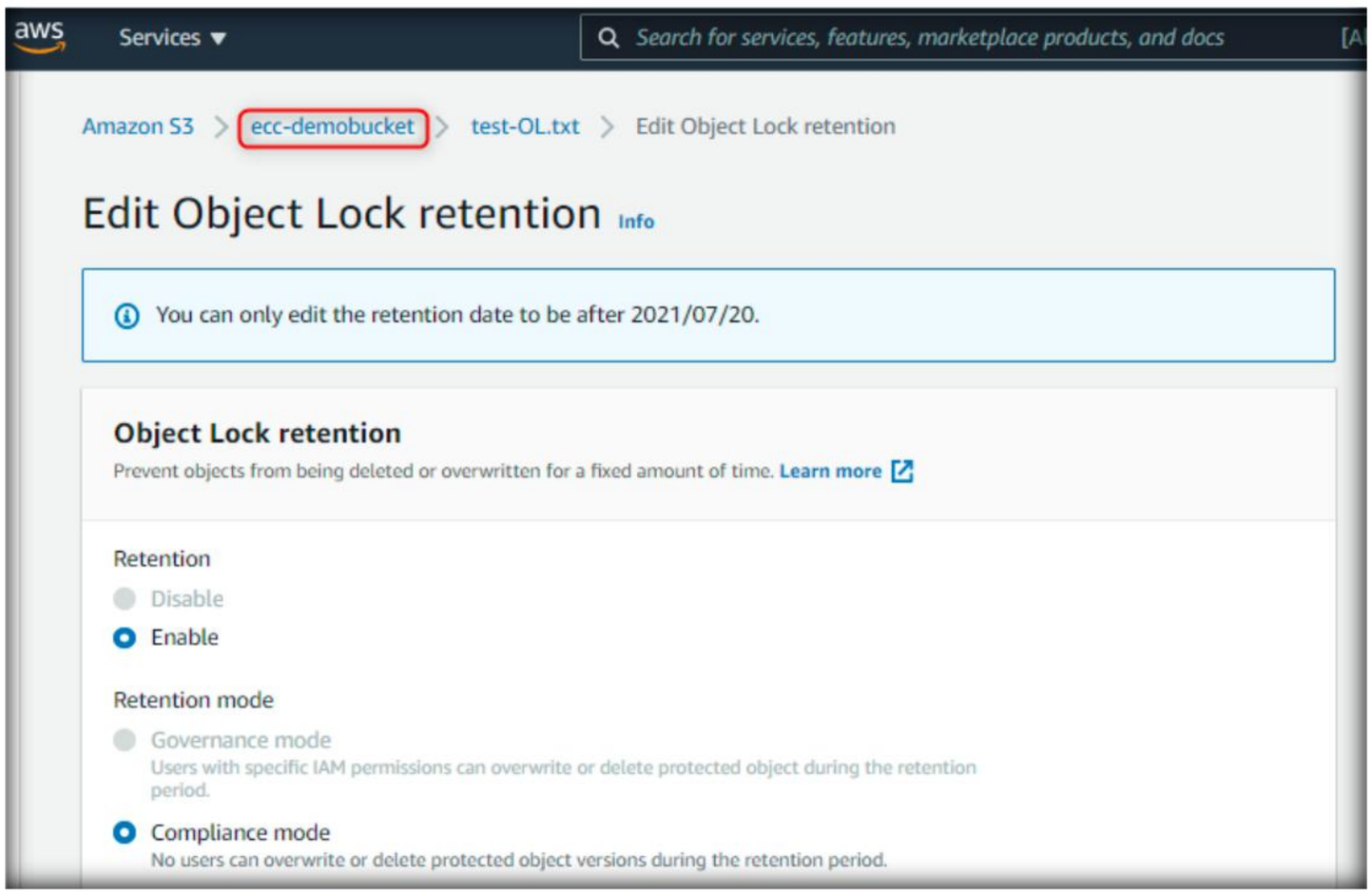


FIGURE 4.6.30: Navigating Back to Bucket Info Window

32. For versioning enabled buckets, to list the object versions, show versions should be turned on. Toggle on **Show versions** to list all versions of the S3 object.

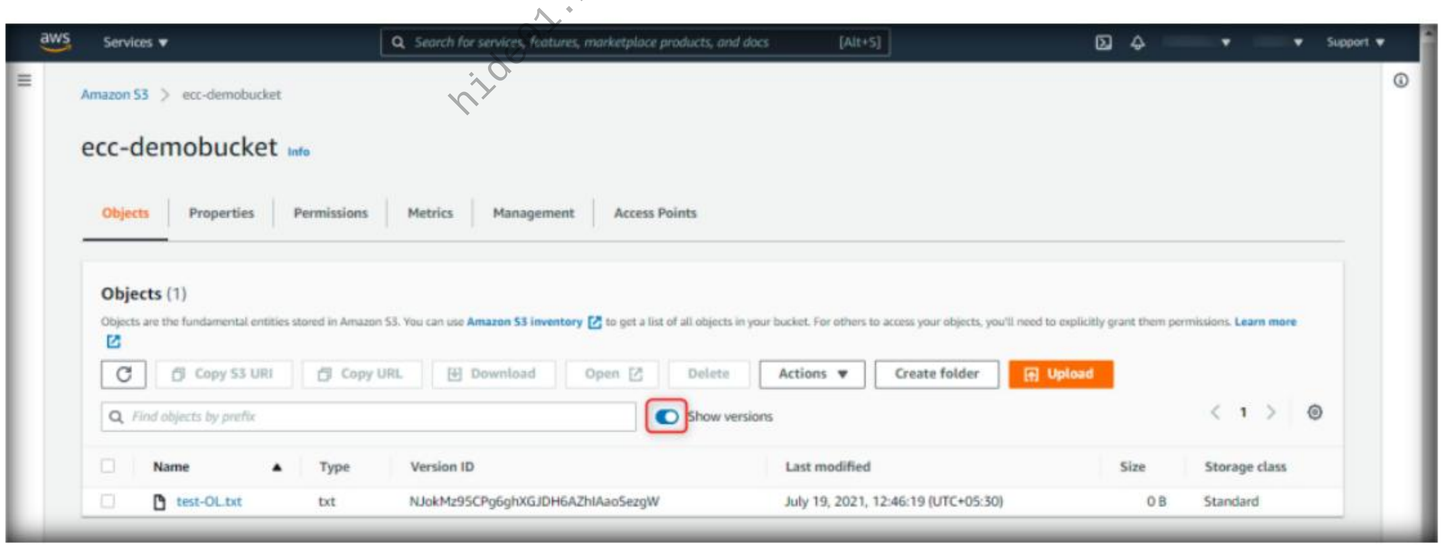


FIGURE 4.6.31: Toggle on Show Versions

33. Now, try to delete the object to verify S3 Object Lock. Select the checkbox for the object (**test-OL.txt**) and click on **Delete**.

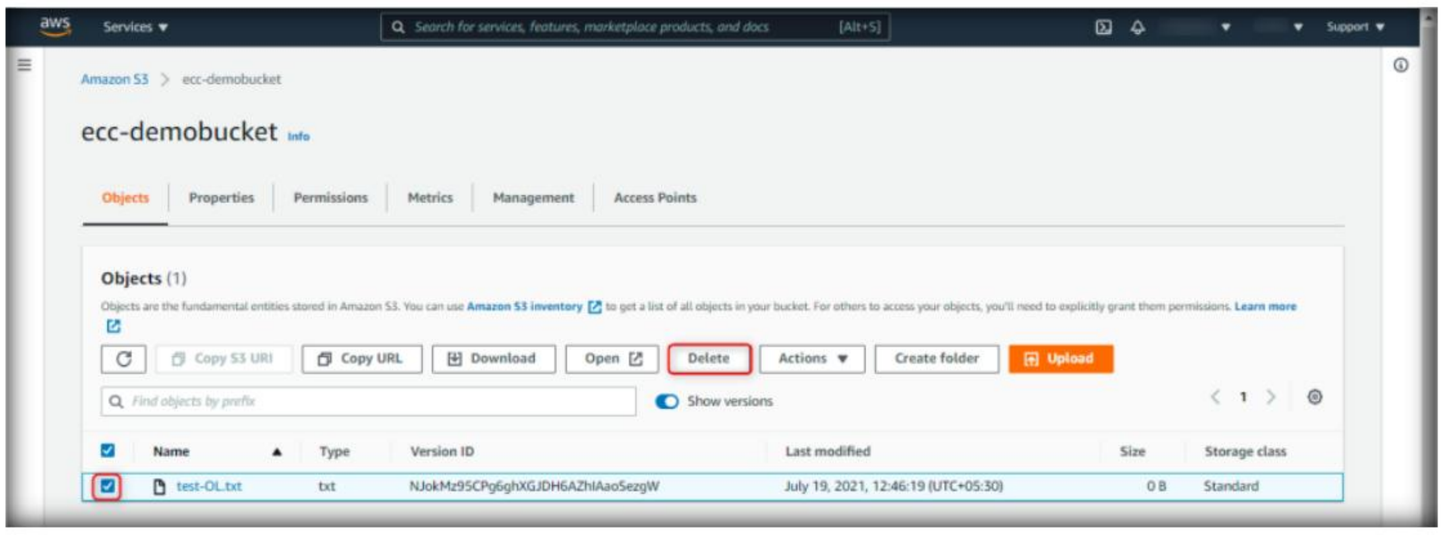


FIGURE 4.6.32: Selecting the Object to Delete

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

34. The **Delete objects** window opens. To confirm deletion, under the field for **Permanently delete objects?**, type **permanently delete**. Click on **Delete objects**.

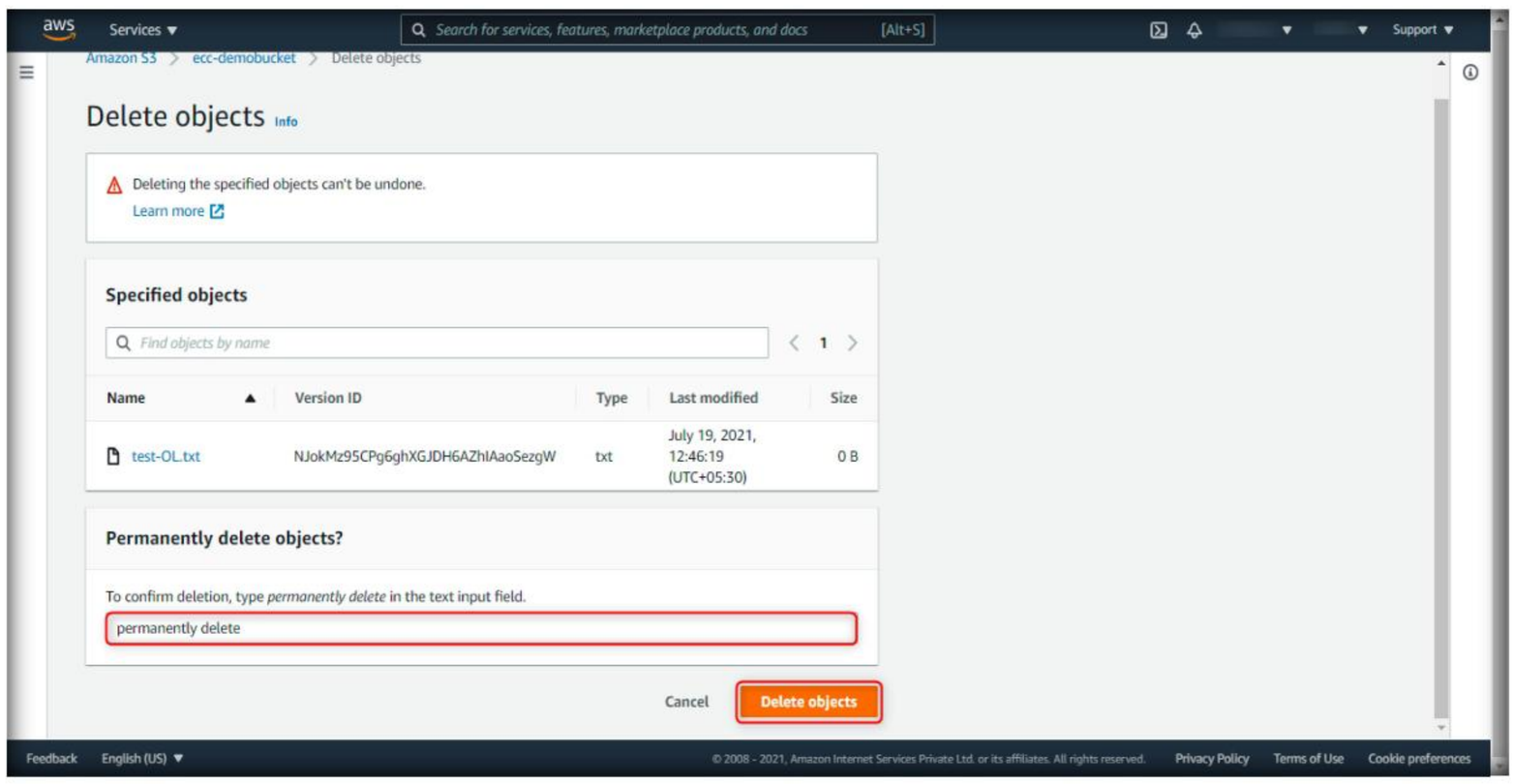


FIGURE 4.6.33: Confirming Deletion

35. The **Delete objects: status** window opens. It can be observed that one object could not be deleted. Under the **Failed to delete** section, you will see an **Error** message, "**Access denied**," as shown in the screenshot below, because compliance mode retention for Object Lock is enabled for the S3 object.

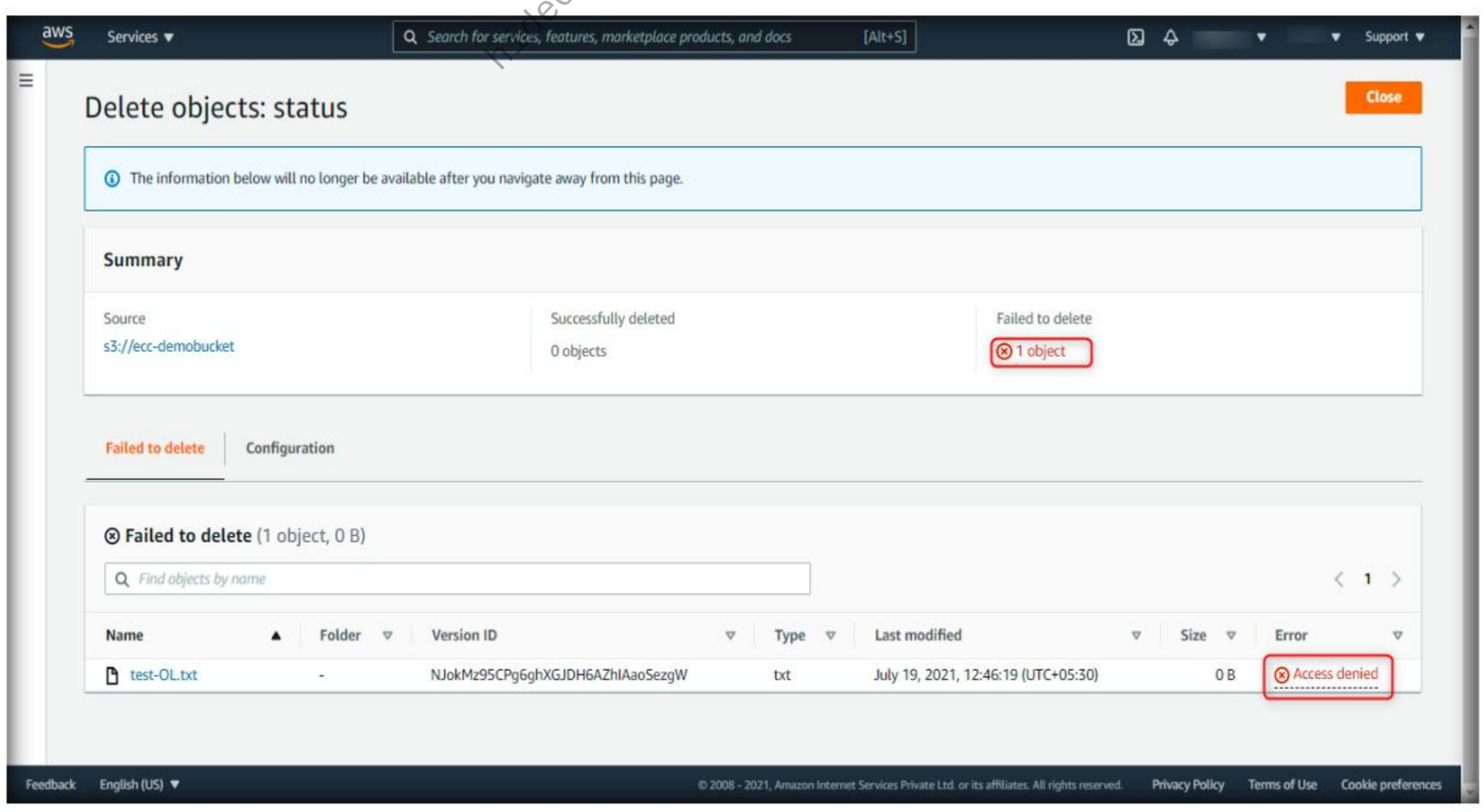


FIGURE 4.6.34: Access Denied Status for Deletion

36. Thus, a cloud security engineer can protect S3 objects from accidental deletion or modification and ransomware threats and ensure compliance requirements for objects by enabling the Object Lock feature of S3 buckets along with the compliance mode retention configuration.

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

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

37. Now, delete the instances created in this lab. Navigate to Buckets under Amazon S3 and select the checkbox of the instance you want to delete (here, ecc-demo-bucket). Click on the Empty button to empty the bucket before deleting. In the pop-up window, enter permanently delete and click on the Empty button.

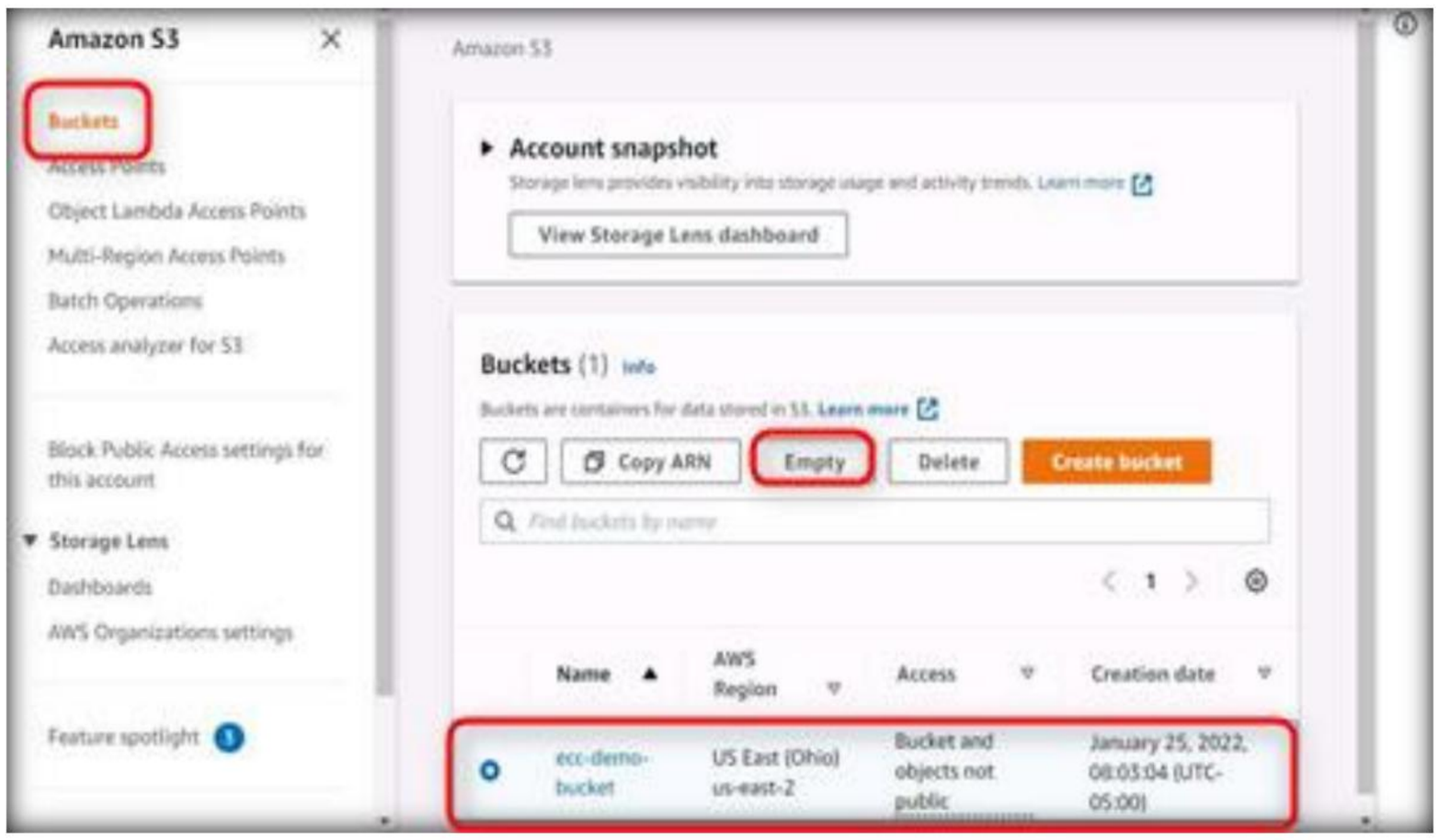


FIGURE 4.6.35: Empty S3 Bucket

38. Navigate to Buckets under Amazon S3 and select the checkbox of the instance you want to delete (here, ecc-demo-bucket). Click on the Delete button. In the pop-up window, enter the bucket's name and click on the Delete button.

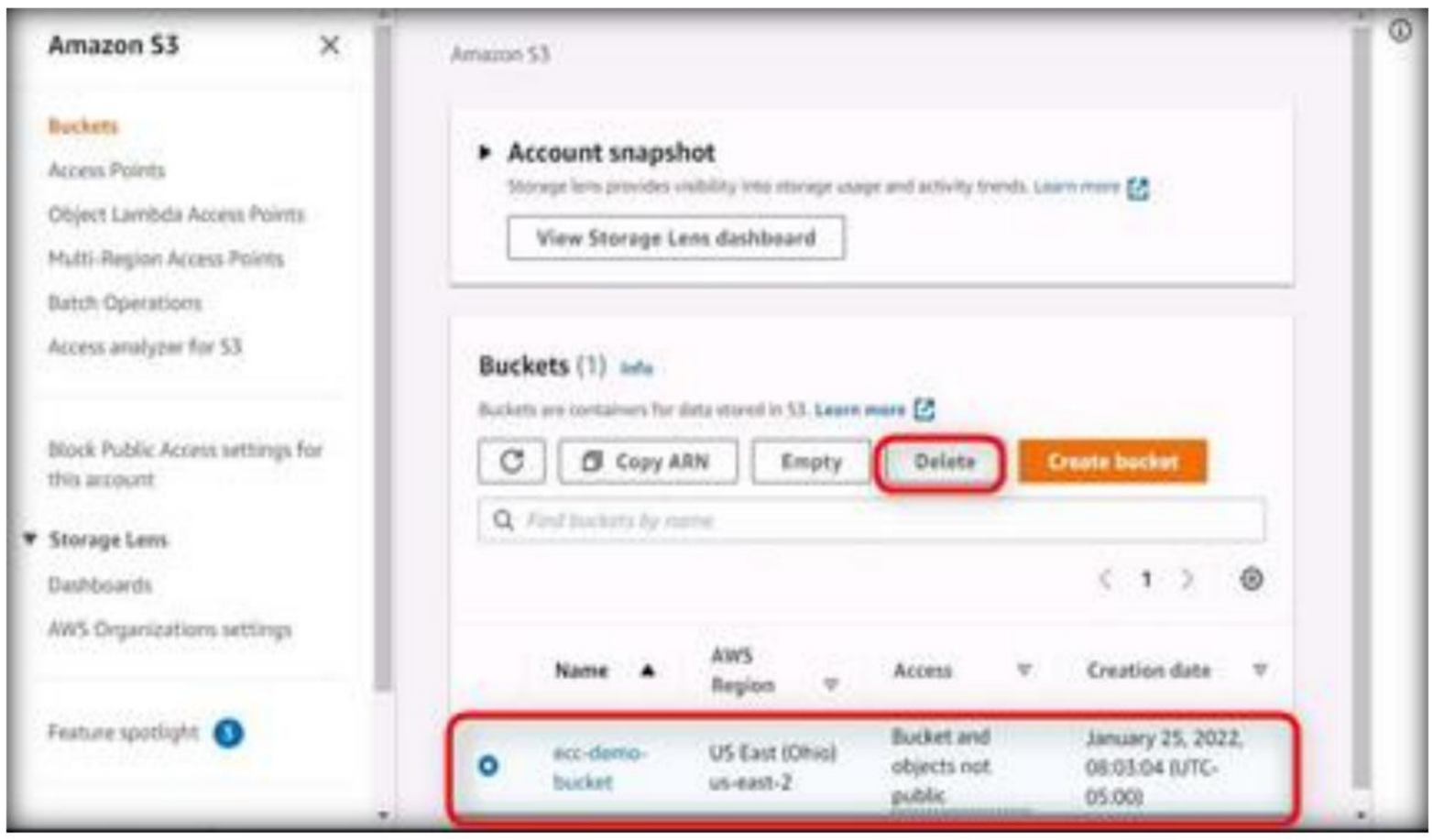


FIGURE 4.6.36: Deleting Bucket

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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.

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 7

Restricting Access to Azure Storage Account Using Shared Access Signature (SAS)

Shared access signature utilizes a URL to grant restricted access to Azure resources for a limited time period.

ICON KEY

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

Lab Scenario

Shared access signature enables the implementation of a fine-grained access control to an Azure storage account. It also helps in restricting access to an Azure storage account. A user with a SAS can only access a specific storage account within a limited timeframe.

Lab Objectives

In this lab, you will learn how to create a new storage account; how to generate a SAS connection string, token, and URL that can be utilized to restrict access to the storage account; how to install Azure Storage Explorer, and how to regulate access to an Azure storage account using SAS.

In this lab you will:

- Create a new storage account
- Generate a SAS token to restrict access to an Azure storage account
- Install Azure Storage Explorer
- Restrict access to an Azure storage account using SAS URI

Lab Environment

To perform this lab, you need the following:

- Admin Machine VM
- Registered Microsoft Azure account

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Duration

Time: 20 minutes

Overview of SAS

Shared access signature is a uniform resource identifier (URI) that provides restricted access to Azure storage resources. Cloud security engineers can not only provide a SAS to clients or users who cannot be trusted with the storage account key, but also delegate access to specific storage account resources. By providing a SAS URI to these individuals, access to specific resources can be granted a particular time period.

A shared access signature (SAS) helps in providing a fine-grained access control over an Azure storage account. A SAS token helps you control the data that can be shared with a client. SAS is recommended over storage access keys for configuring Azure storage 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.

hide01.ir

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 New Storage Account in Azure

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

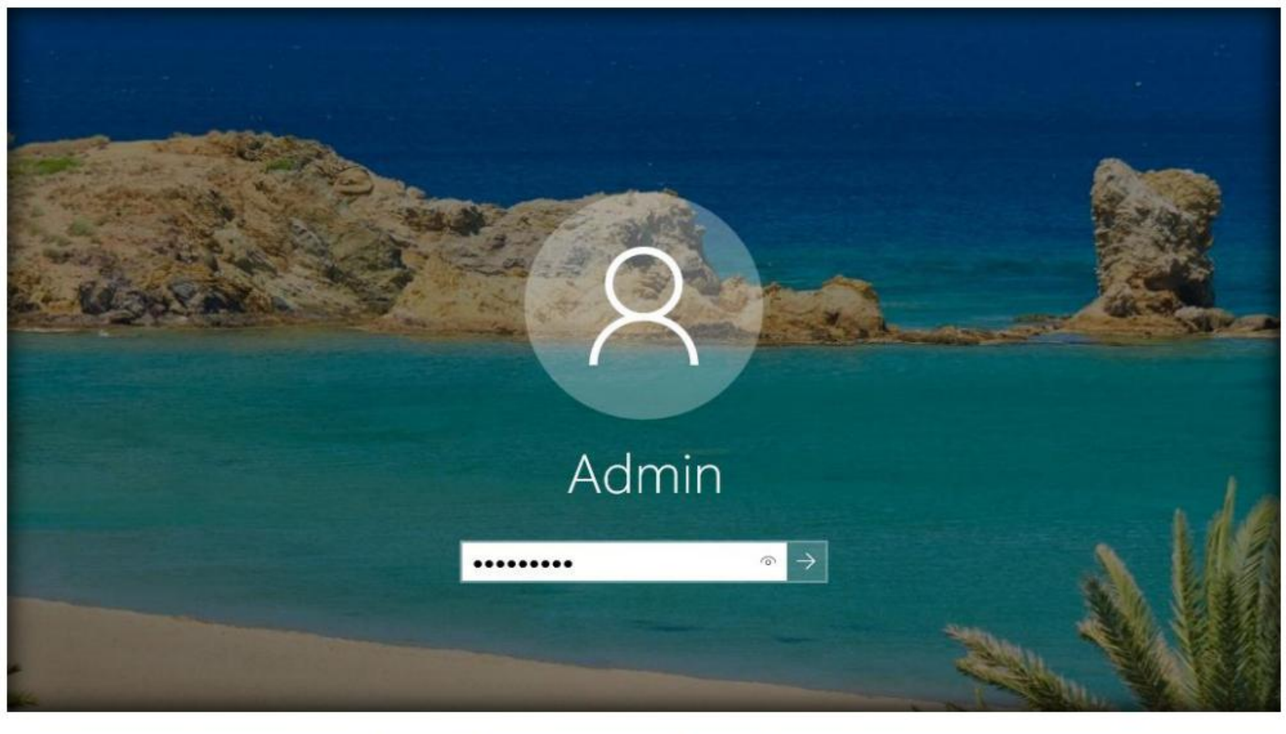


FIGURE 4.7.1: Launch Admin Machine and Log in

Certified Cloud Security Engineer Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

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

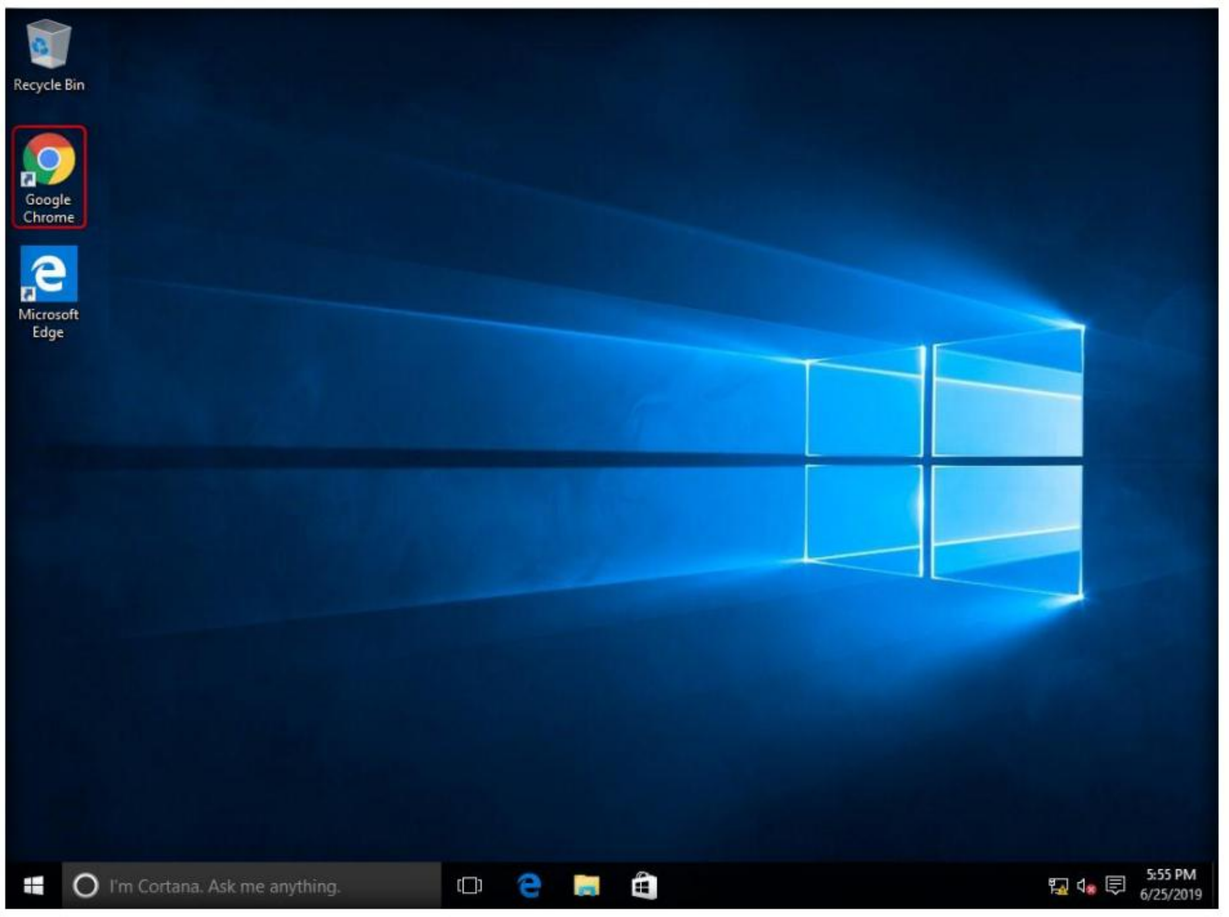


FIGURE 4.7.2: Navigating to the Chrome Browser from Taskbar

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

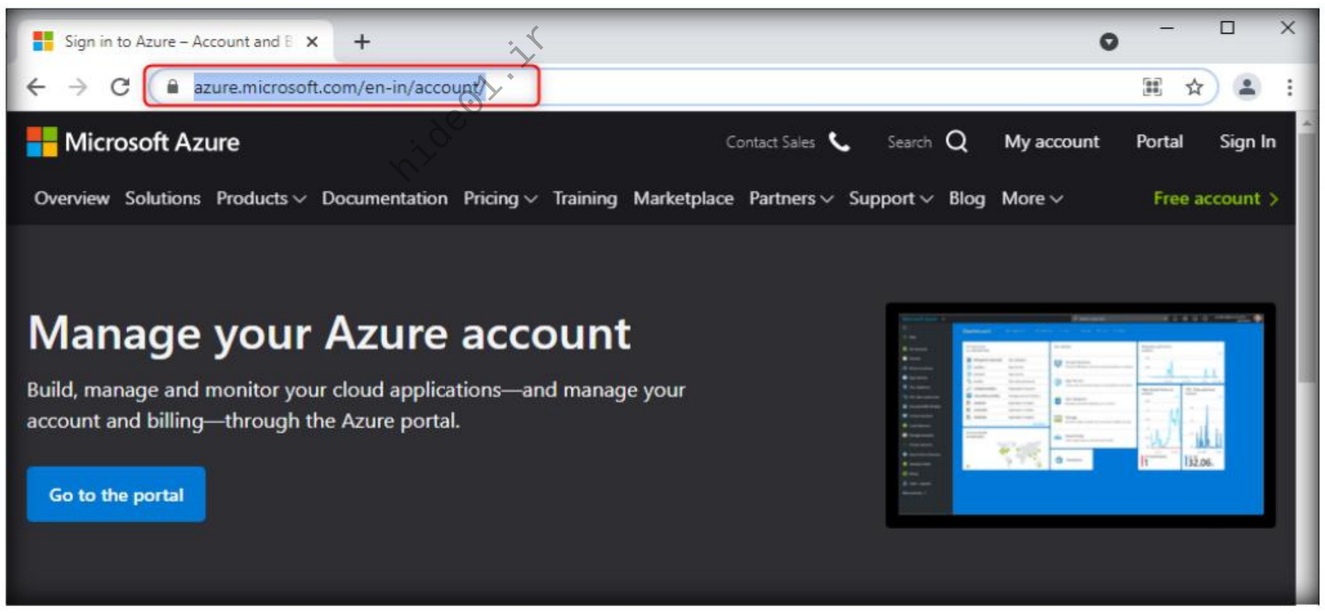


FIGURE 4.7.3: Entering the URL of Microsoft Azure

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

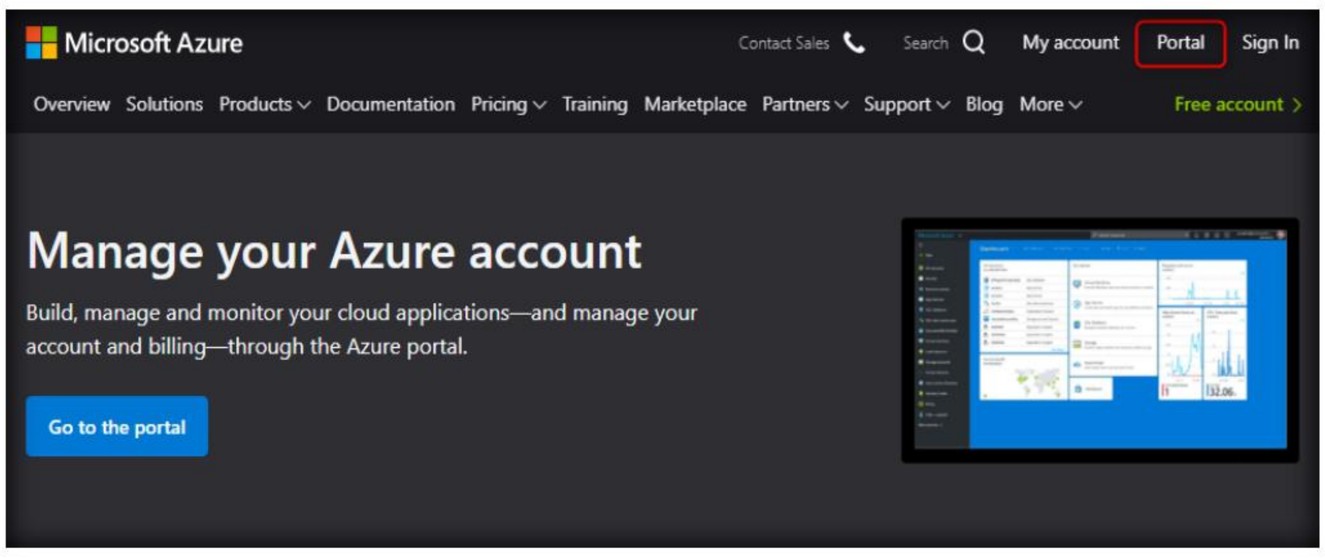


FIGURE 4.7.4: Sign in to Azure Portal

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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

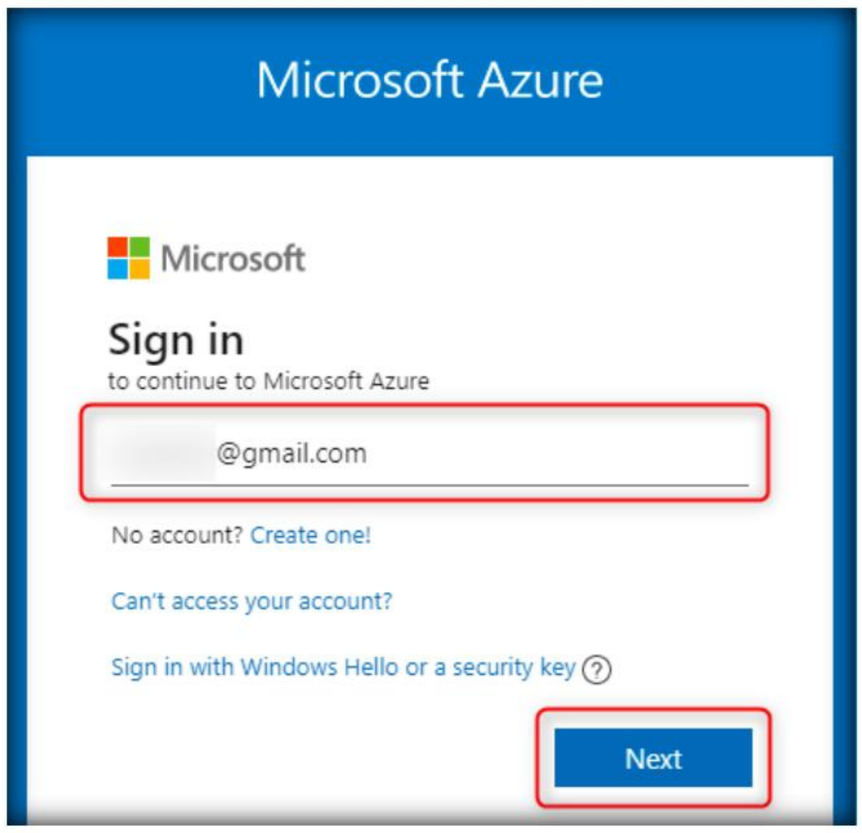


FIGURE 4.7.5: Entering Account ID to continue

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

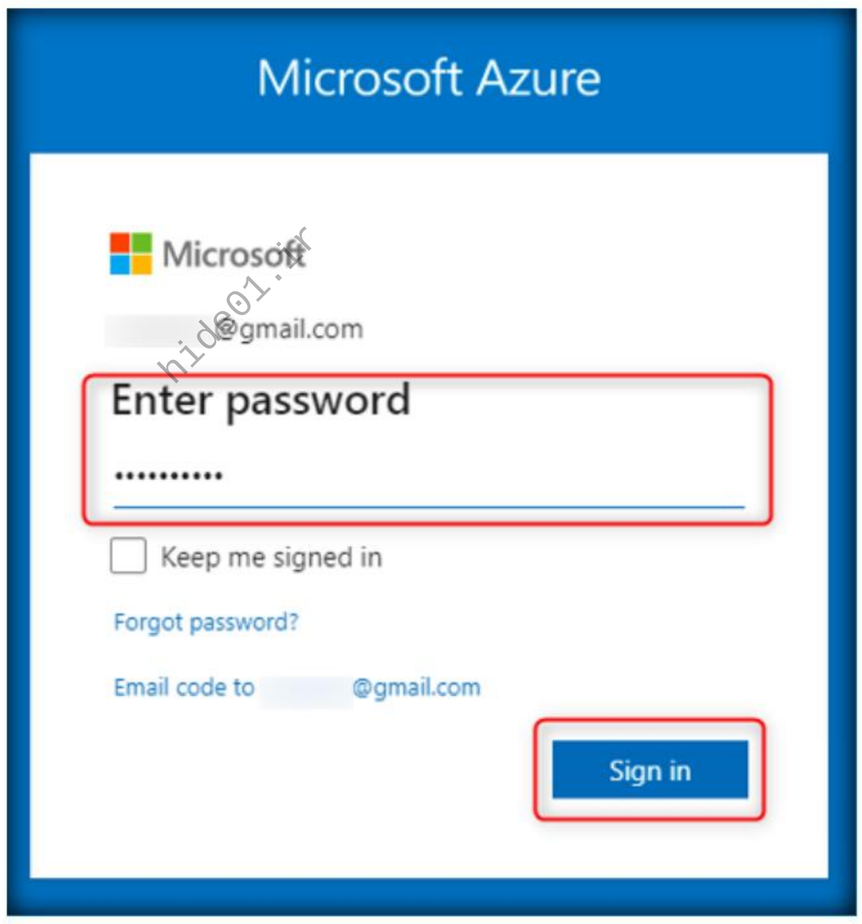


FIGURE 4.7.6: Sign in to Azure Account

7. Microsoft Azure portal will appear now. Click on **Resource groups** under Azure services.



FIGURE 4.7.7: Selecting Resource group in Azure portal

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

8. Under the **Resource groups** pane, click on the **+Create** button.

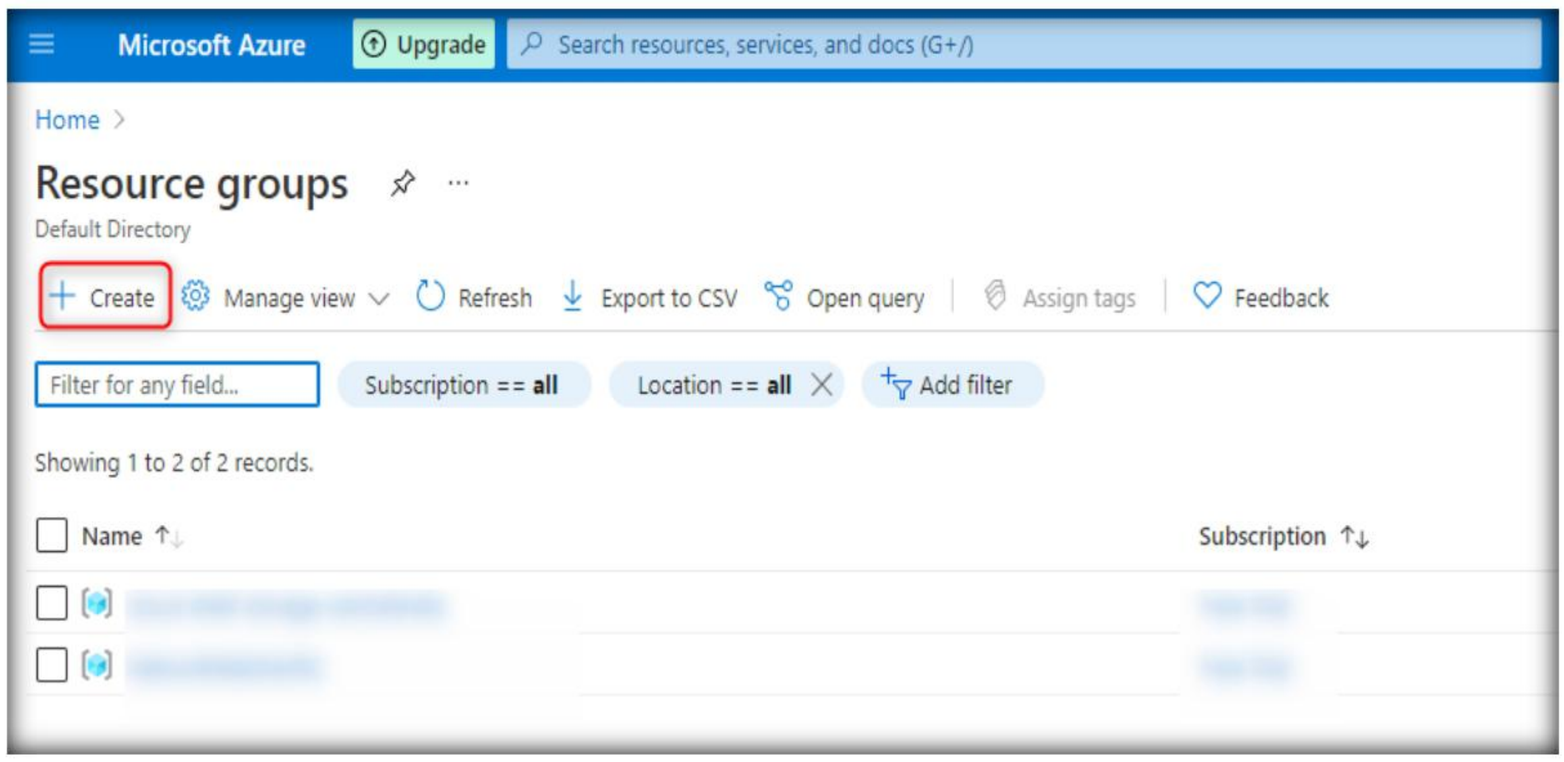


FIGURE 4.7.8: Click on +Create

9. **Create a resource group** page will open now. In the **Resource group** field, enter a **Resource group** name (**SAStestRG** in this lab), and in the **Region** field, enter a **Region** name (**(US) East US** in this lab). Now, click on the **Next: Tags>** button.

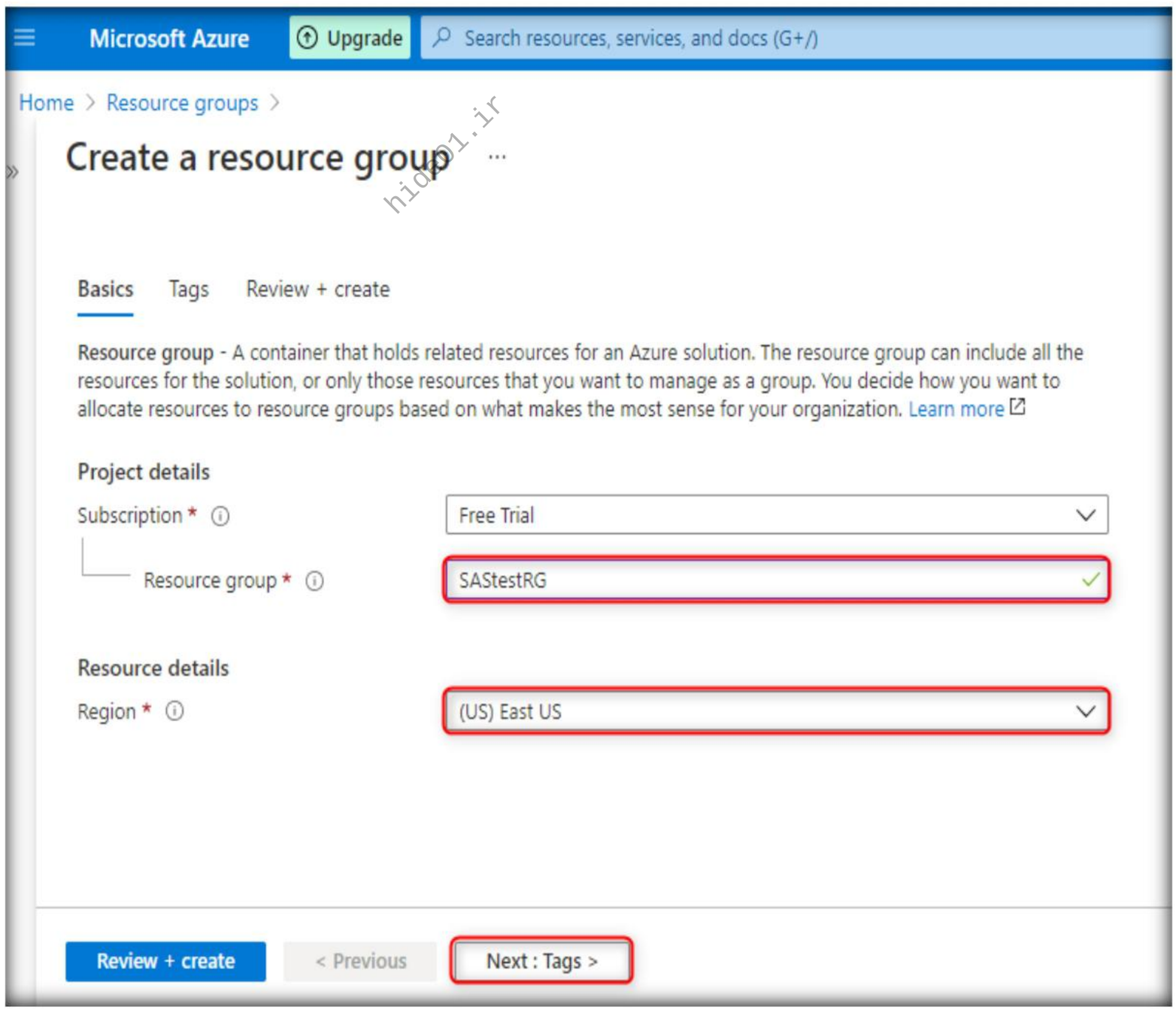


FIGURE 4.7.9: Entering Resource Group Name and Location

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

10. Retain the default **Tags** tab settings and click on the **Next: Review + create** button.

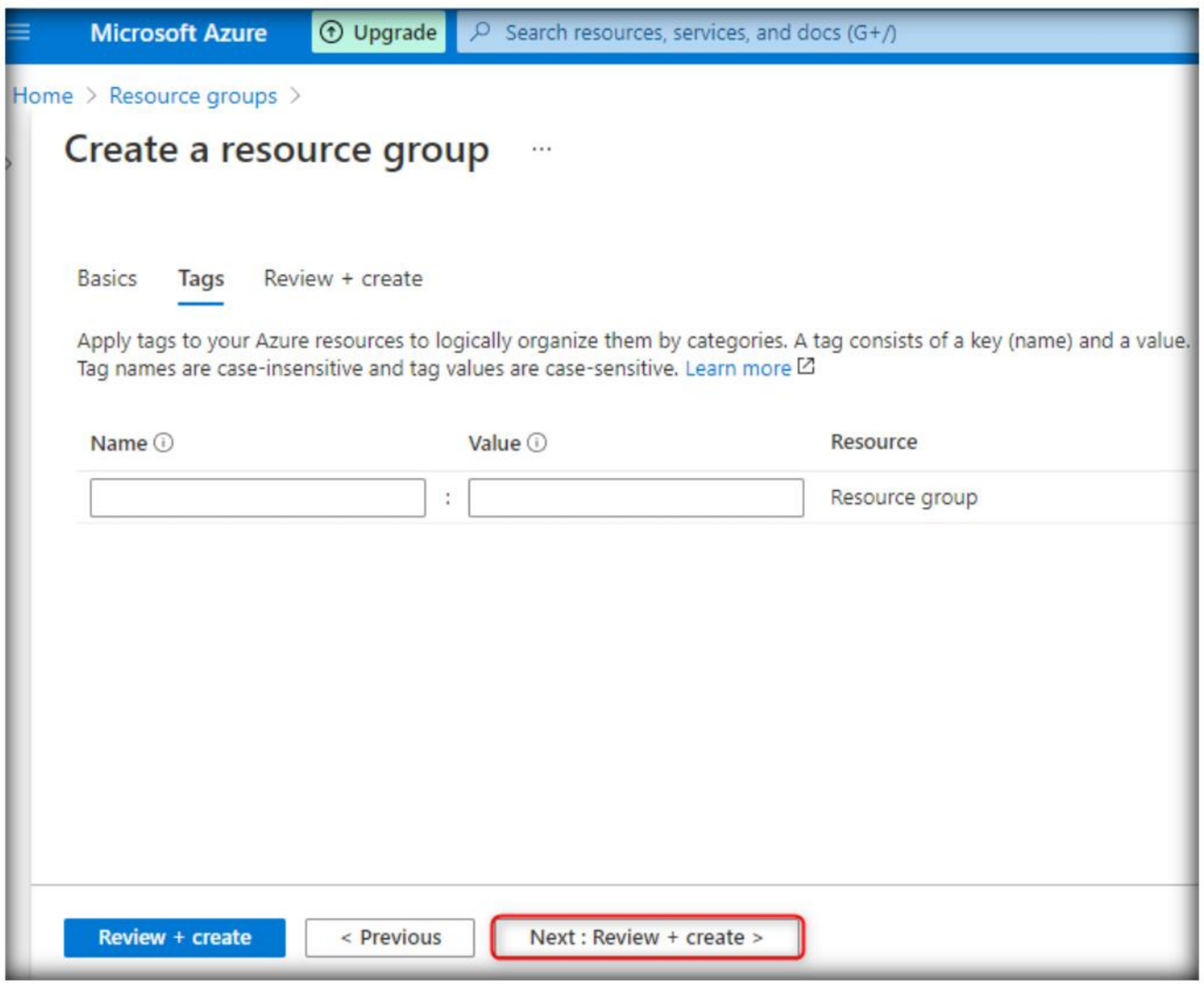


FIGURE 4.7.10: Reviewing and Creating Resource Group

11. **A Review + create** page will appear. Wait for the **Validation passed** message and then click on **Create**.

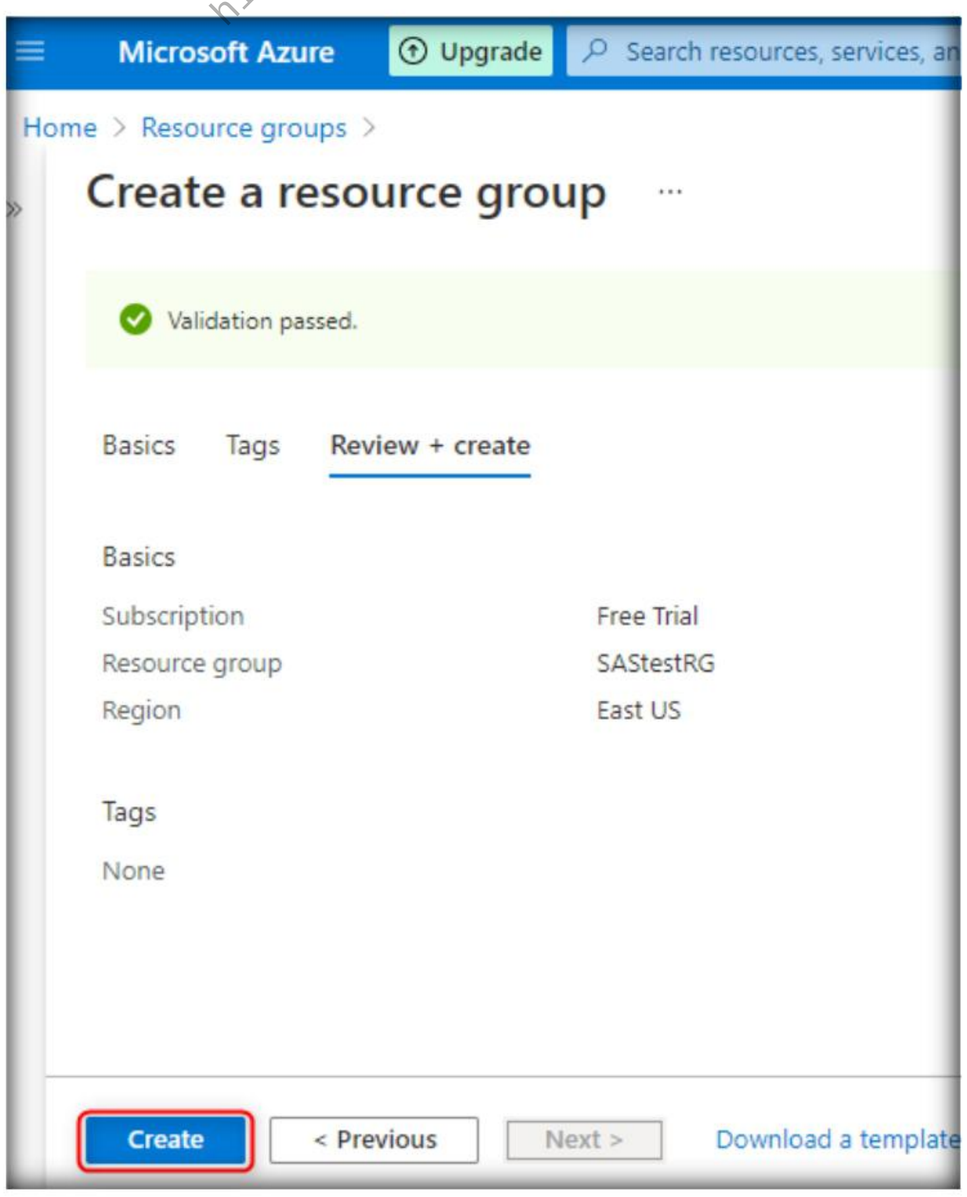


FIGURE 4.7.11: Validation Passed for Creating a Resource Group

Certified Cloud Security Engineer Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

12. Resource group name **SAStestRG** is successfully created now.

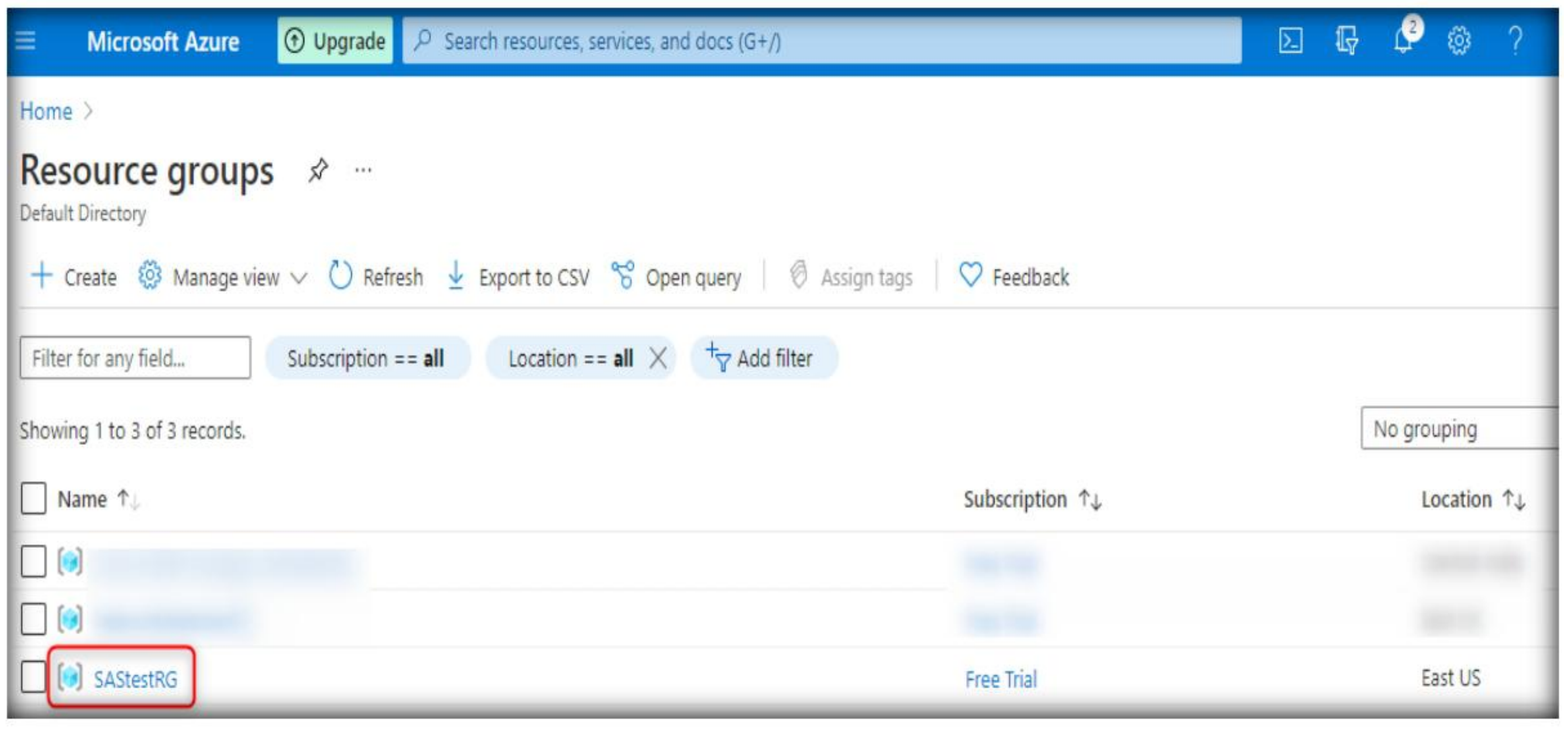


FIGURE 4.7.12: Successfully Creating Resource Group

13. Now, to create a storage account, click on **Storage accounts** under **Azure services**.



FIGURE 4.7.13: Selecting Storage accounts in Azure portal

14. In the **Storage accounts** window, click on **+Create**.

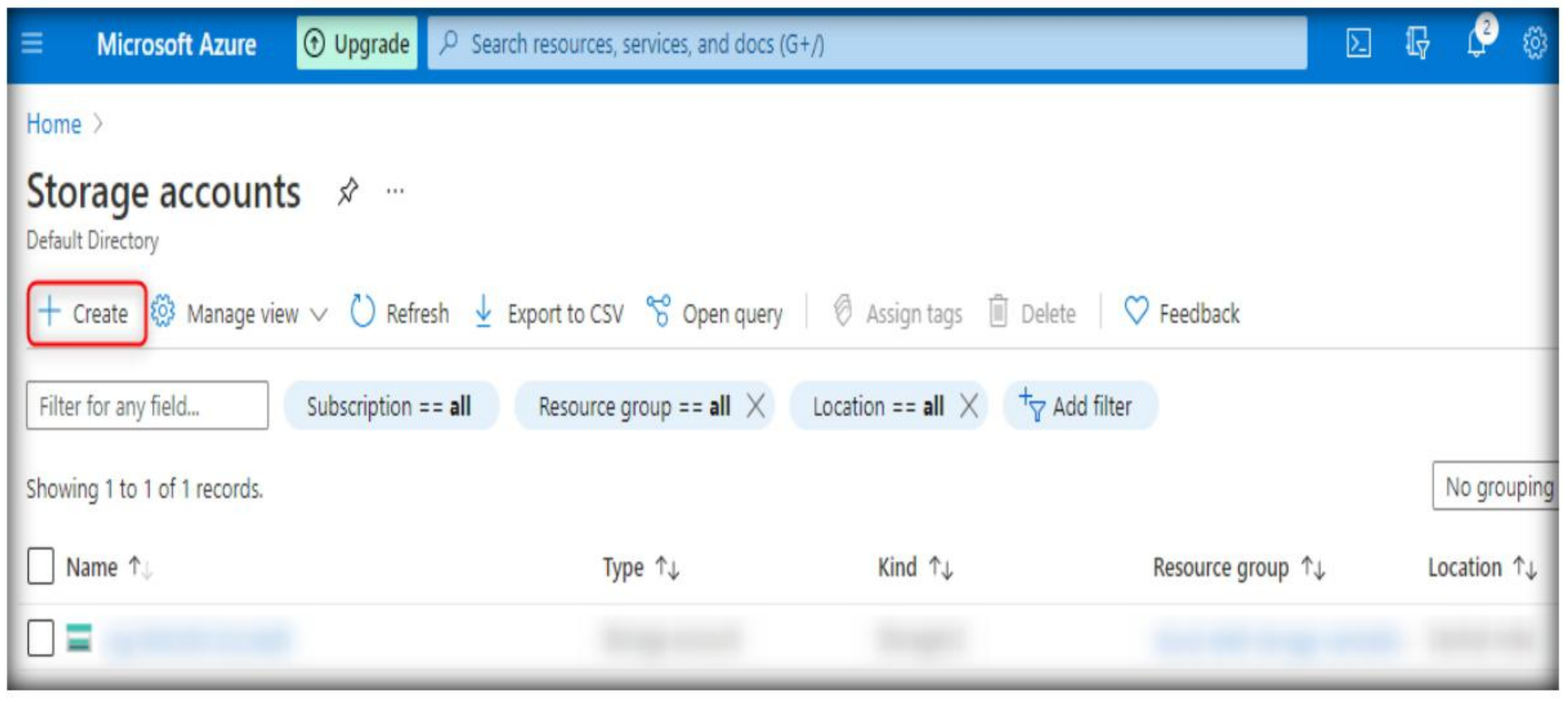


FIGURE 4.7.14: Creating a New Storage Account

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

15. A **Create a storage account** window will appear now; select the **Resource group** you have created (here, we have selected **SAStestRG**).

    Note: For this lab, we are keeping all parameters in their default state. You can change them according to your requirements.

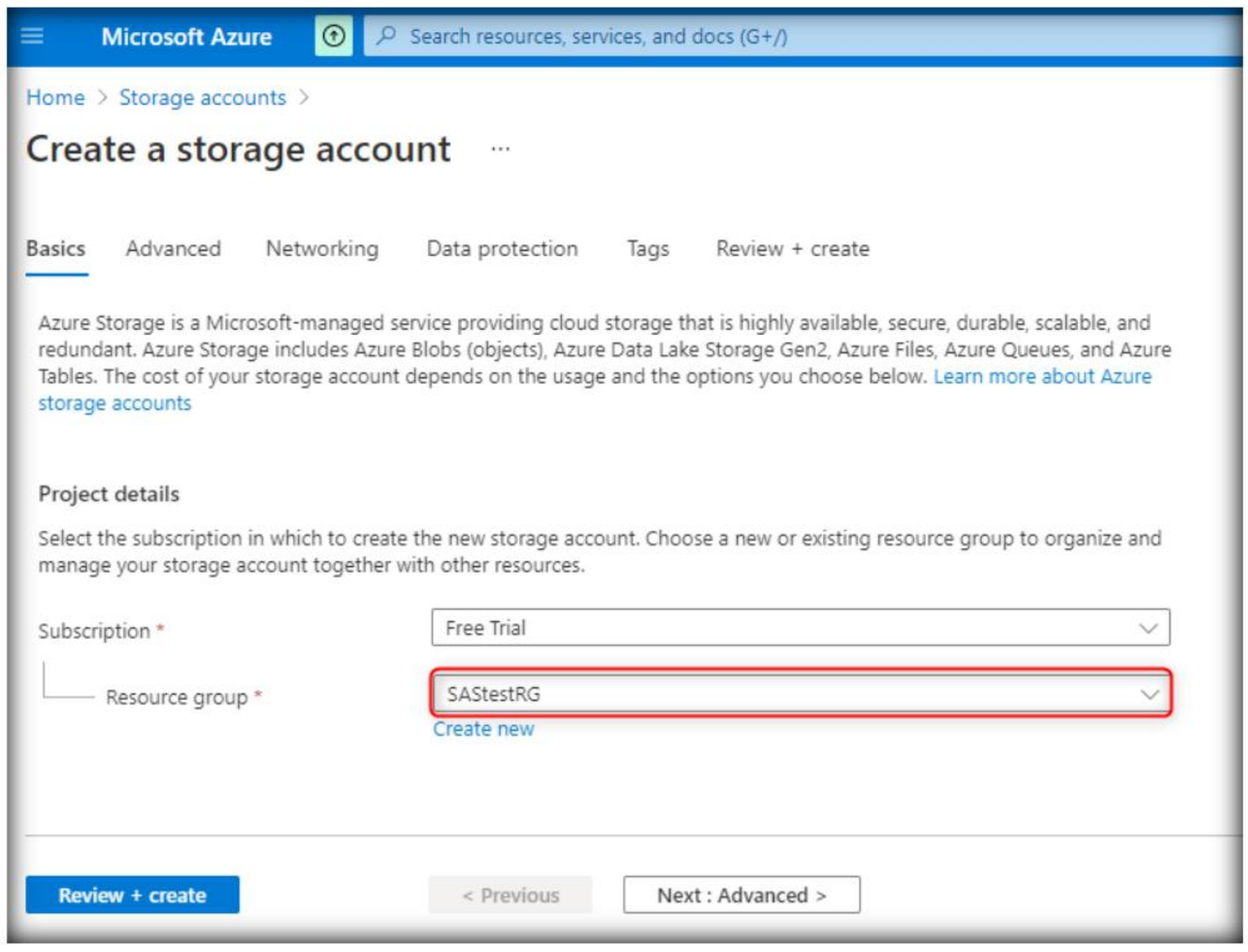


FIGURE 4.7.15: Entering Resource Group Name

16. Scroll down. Under **Instance details**, type the storage account name (here, we have entered **sasdatastorage**). Leave the **Region**, **Performance** and **Redundancy** fields in their default state. Then, click on the **Next: Advanced>** button.

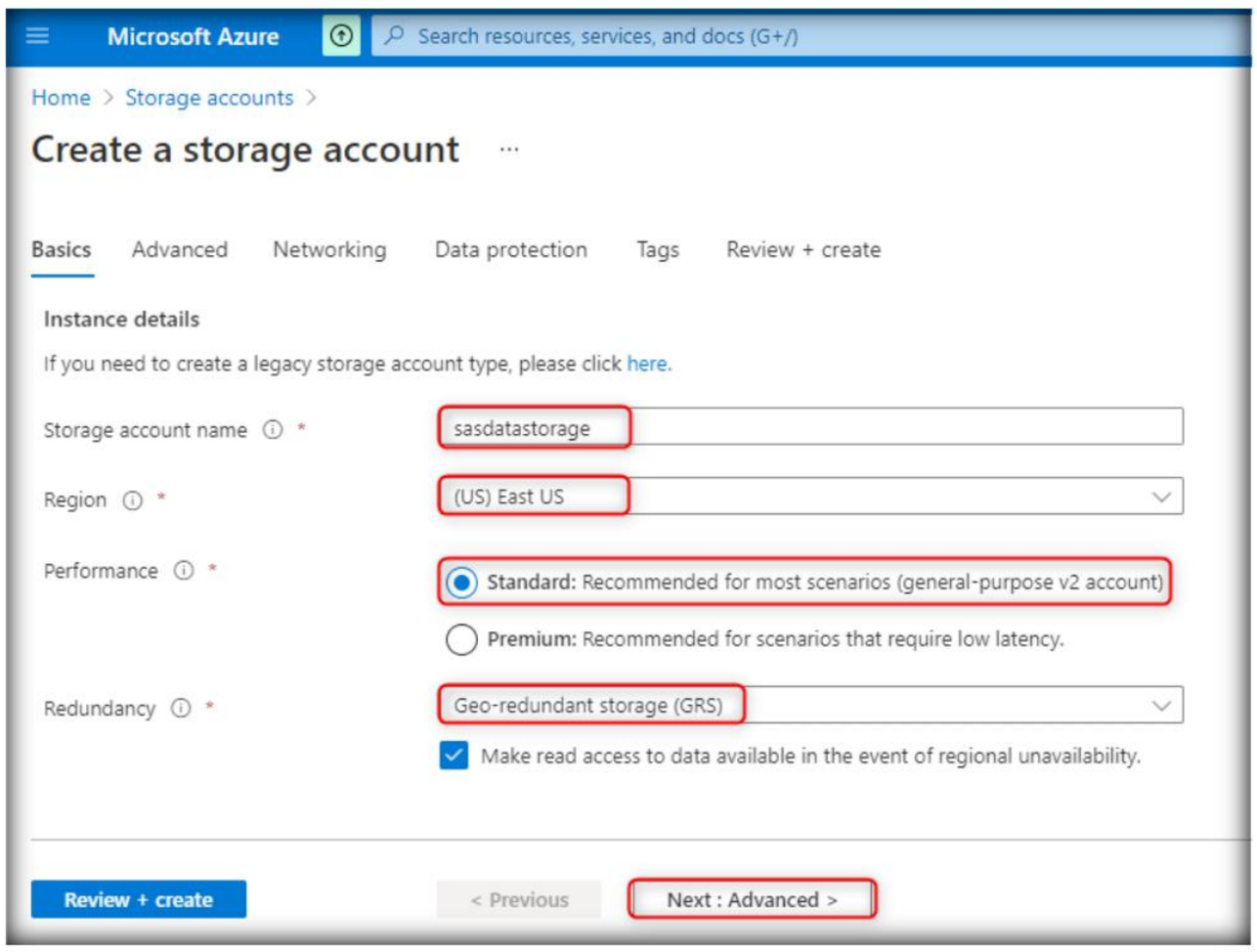


FIGURE 4.7.16: Entering Storage account name and Region details

Certified Cloud Security Engineer Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

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

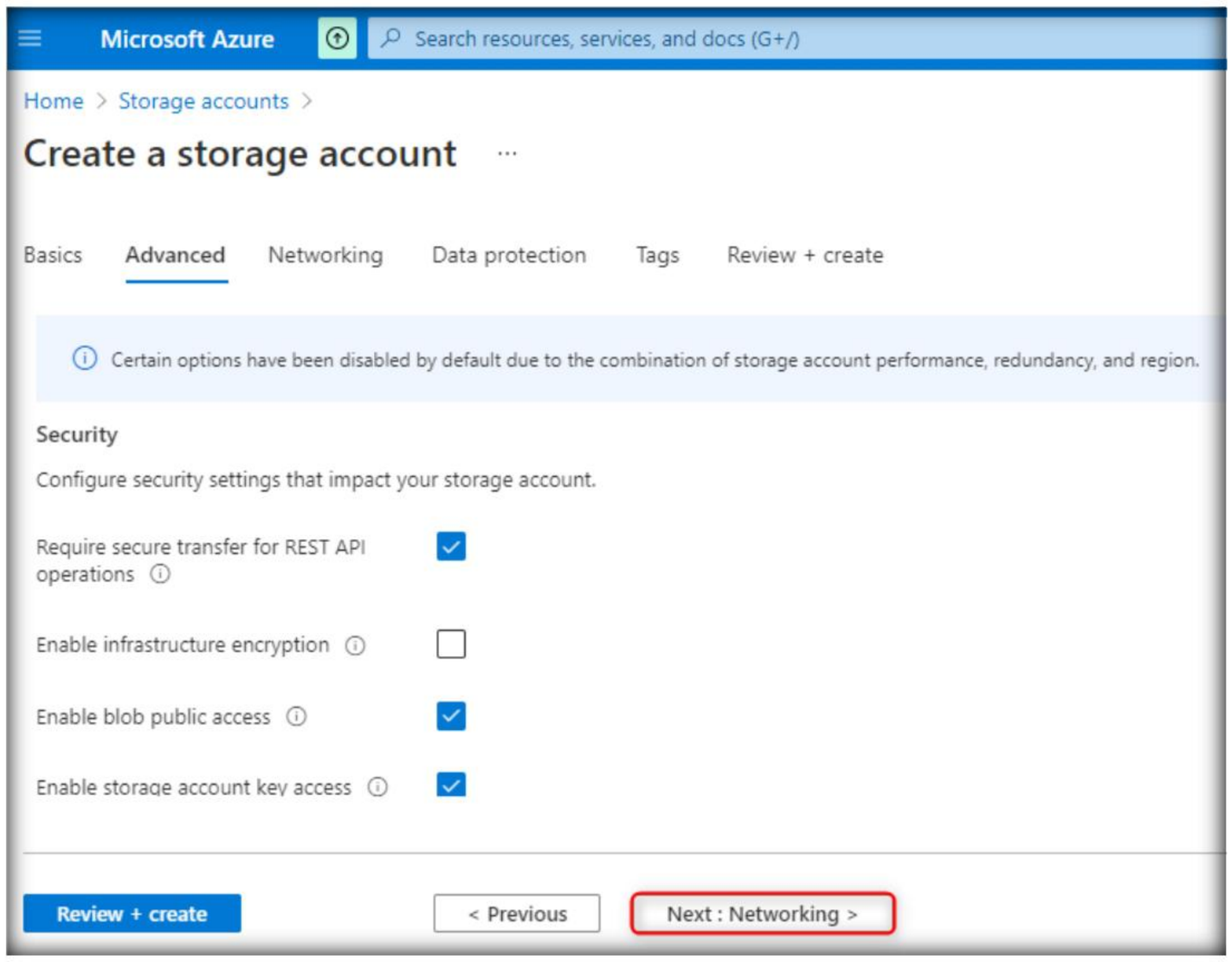


FIGURE 4.7.17: Leaving Everything in Default State in Advanced Tab

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

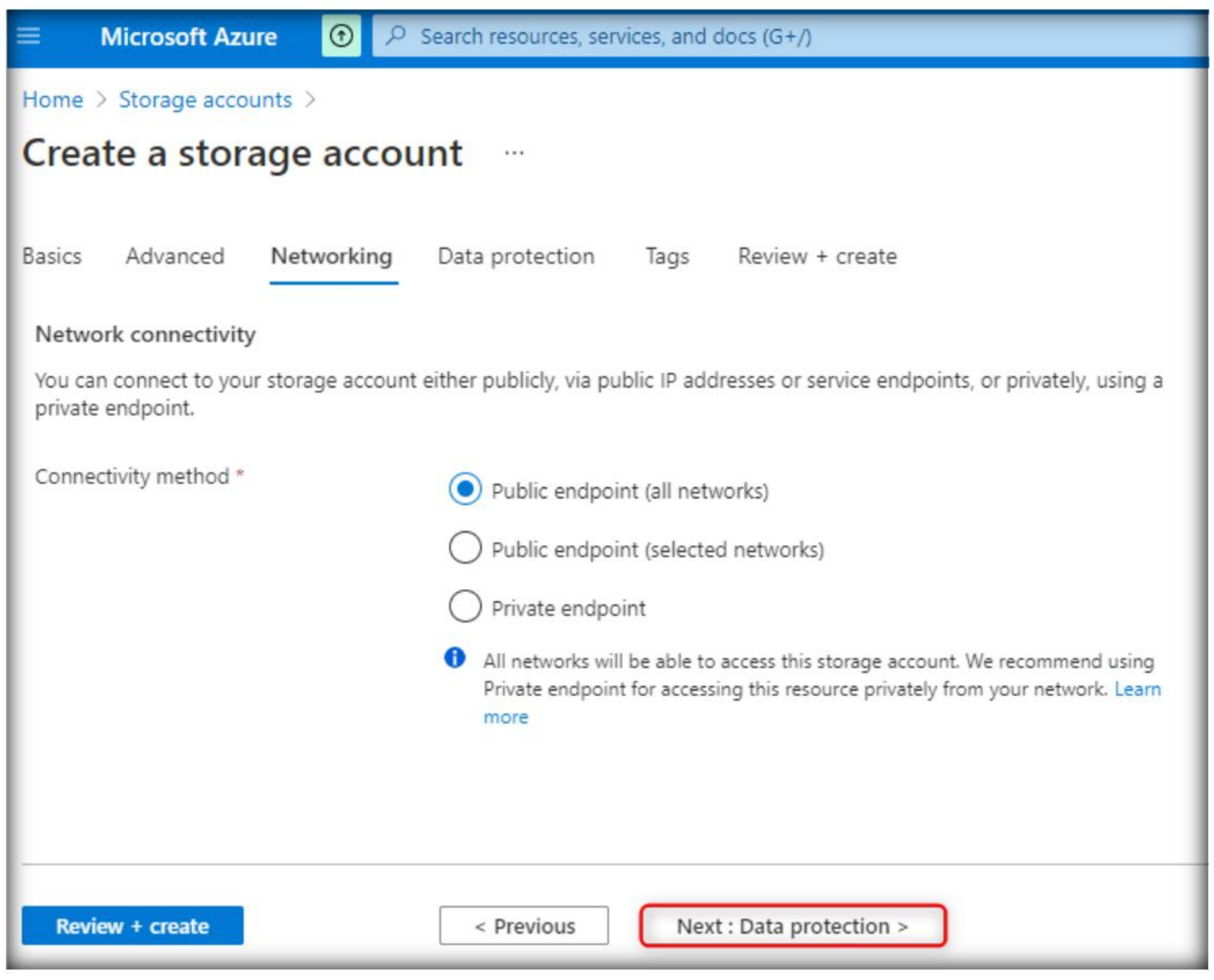


FIGURE 4.7.18: Leaving Everything in Default State in Networking Tab

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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

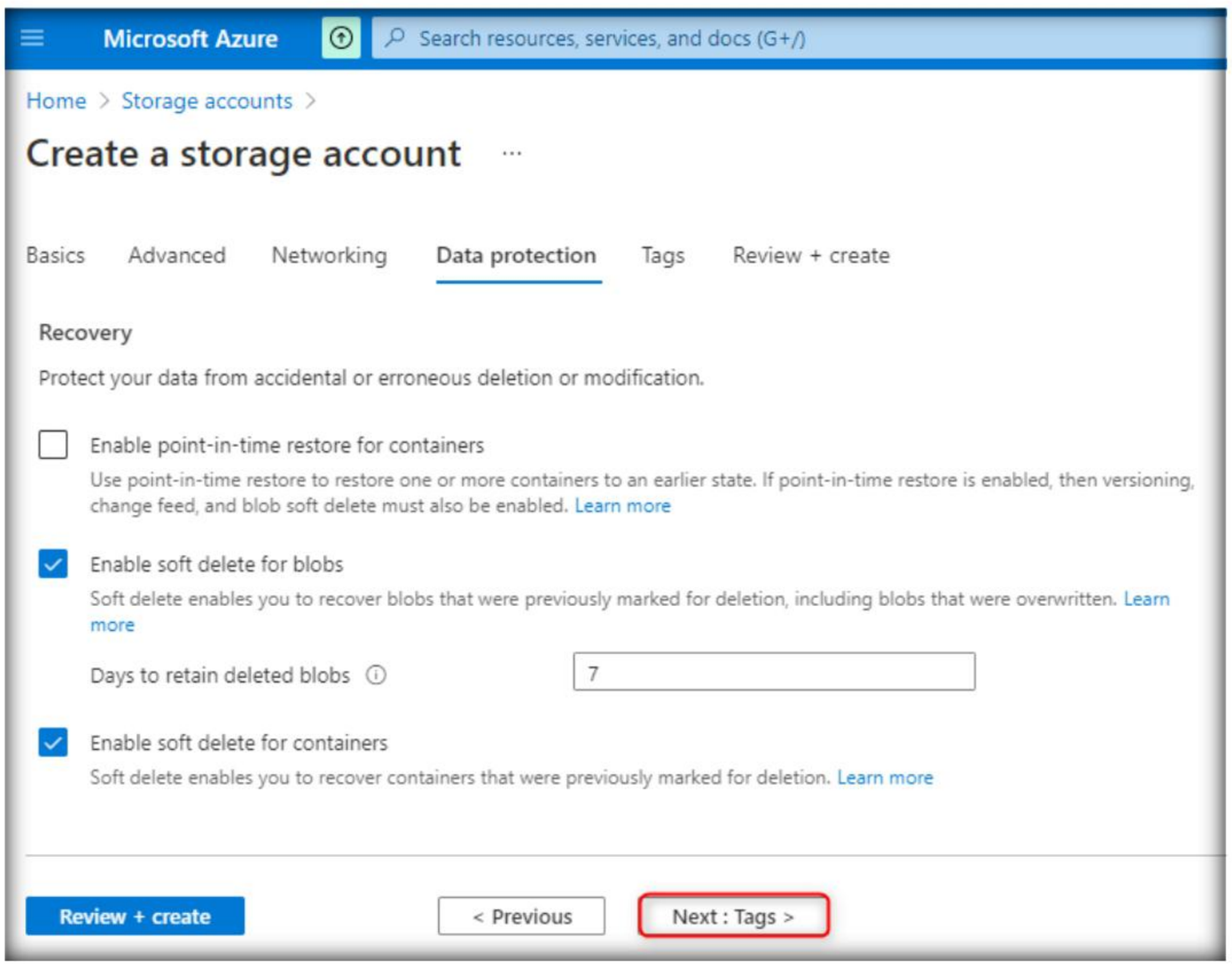


FIGURE 4.7.19: Leaving Everything in Default State in Data Protection Tab

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

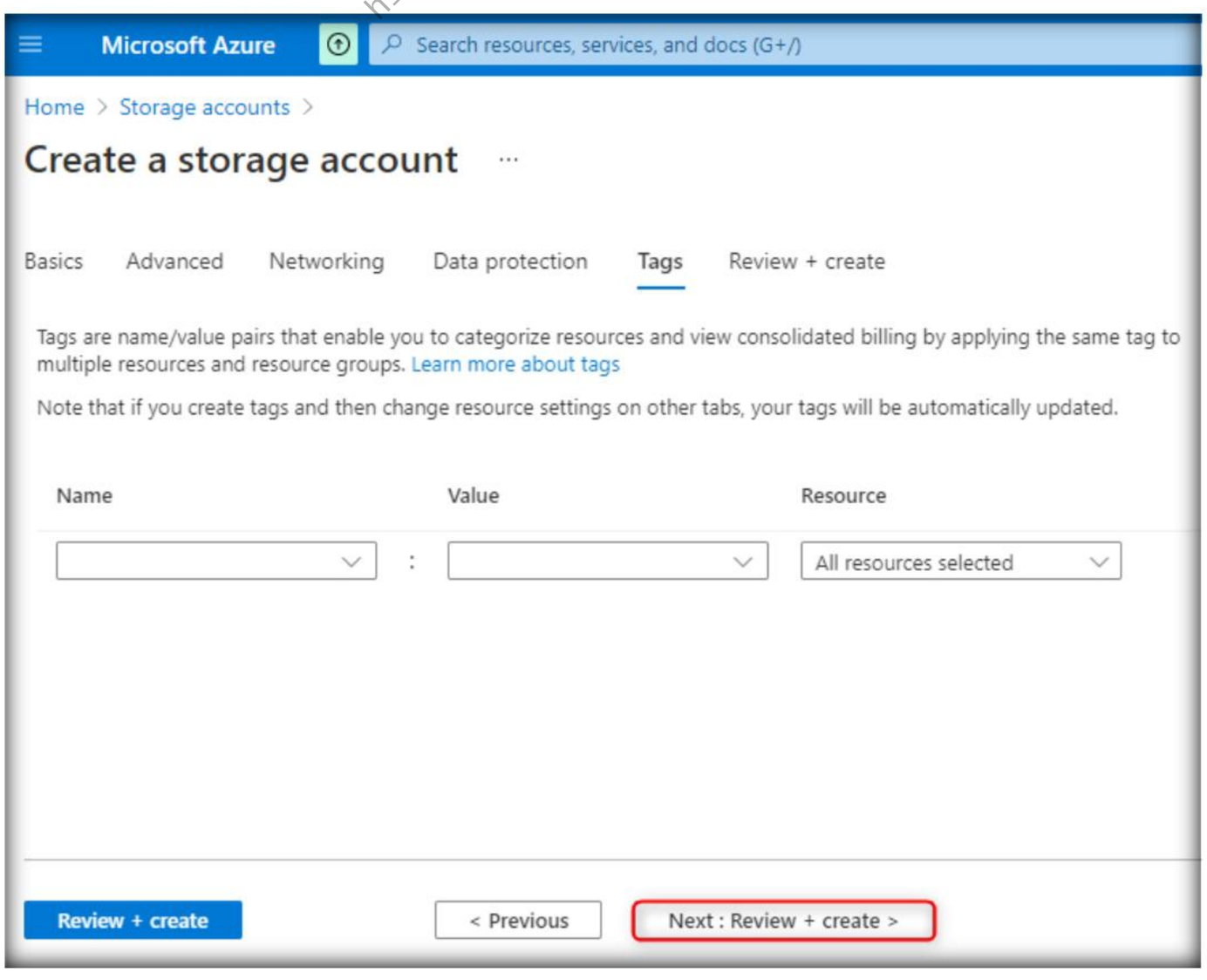


FIGURE 4.7.20: Leaving Everything in Default State in Tags Tab

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

21. After the **Validation passed** message, click on **Create**.

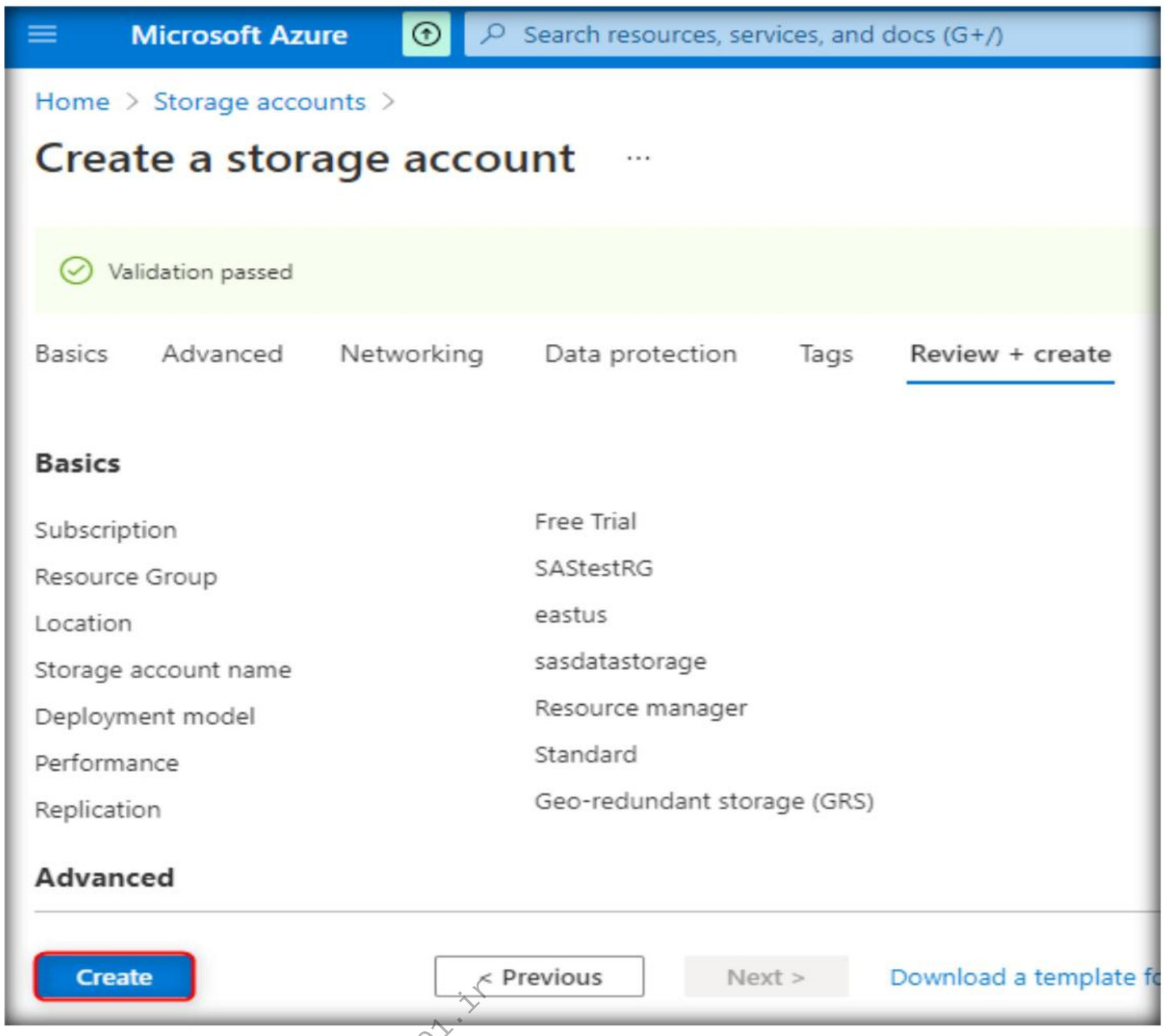


FIGURE 4.7.21: Storage Account Passing the Validation

22. Wait for a few seconds. After the completion of deployment, click on the **Go to resource** button.

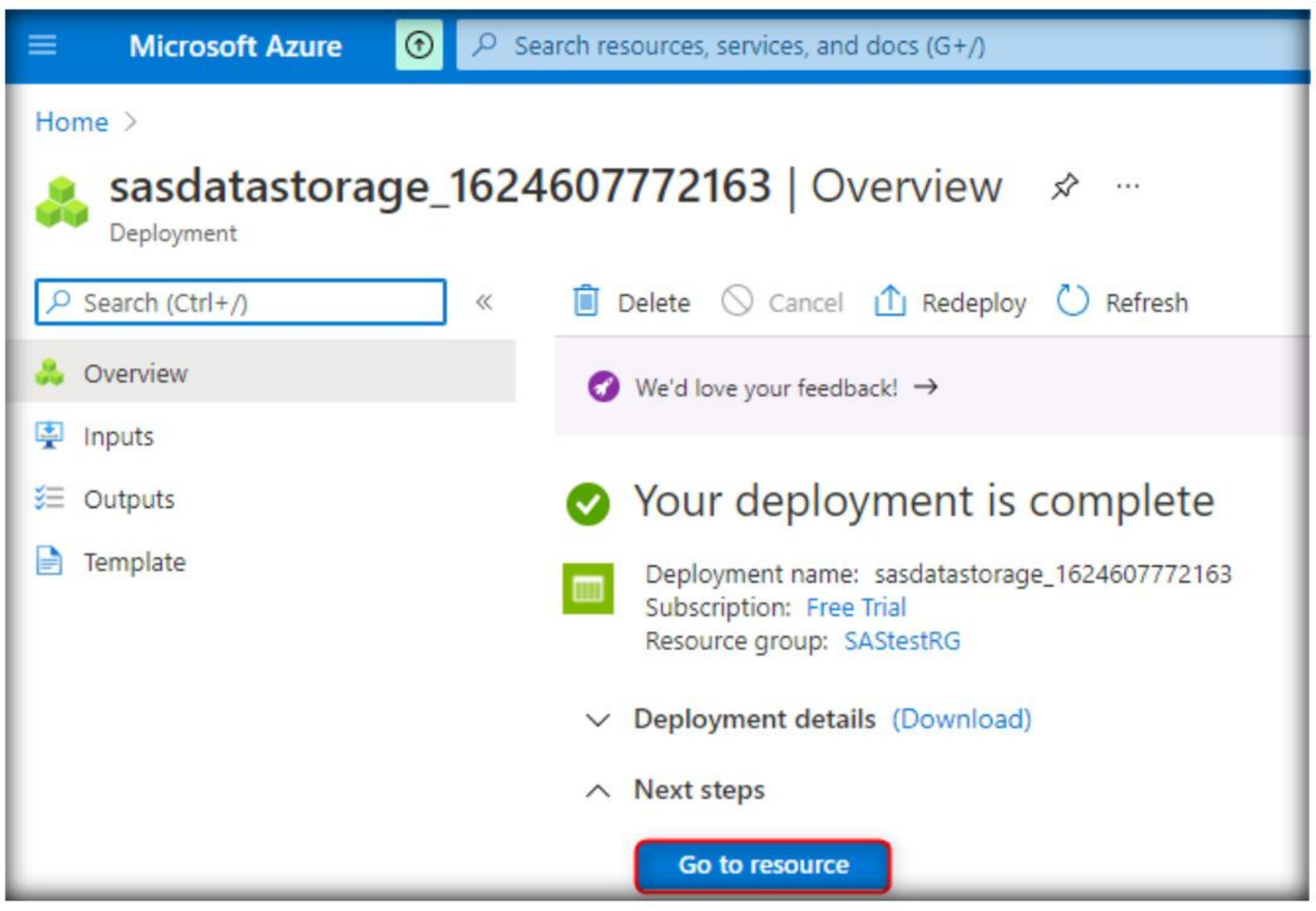


FIGURE 4.7.22: Deployment of Storage Account

Certified Cloud Security Engineer Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

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

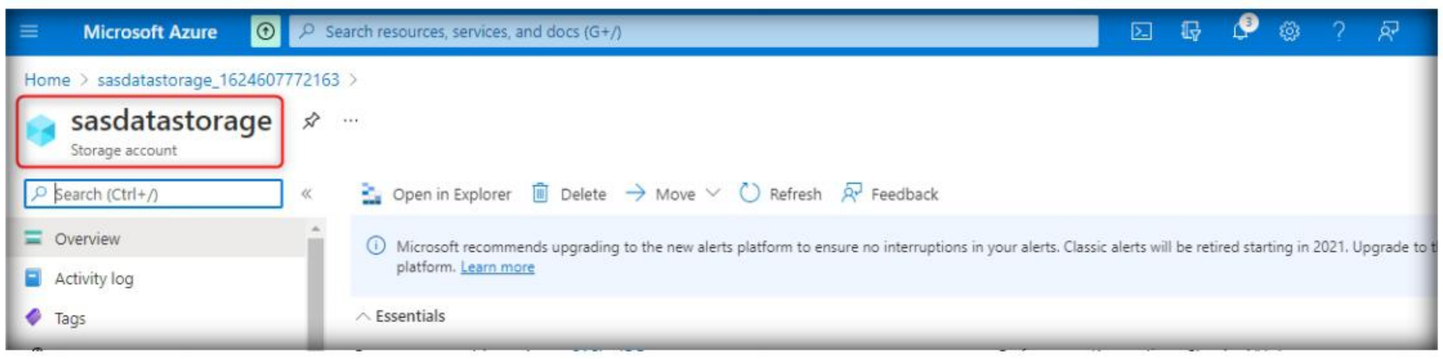
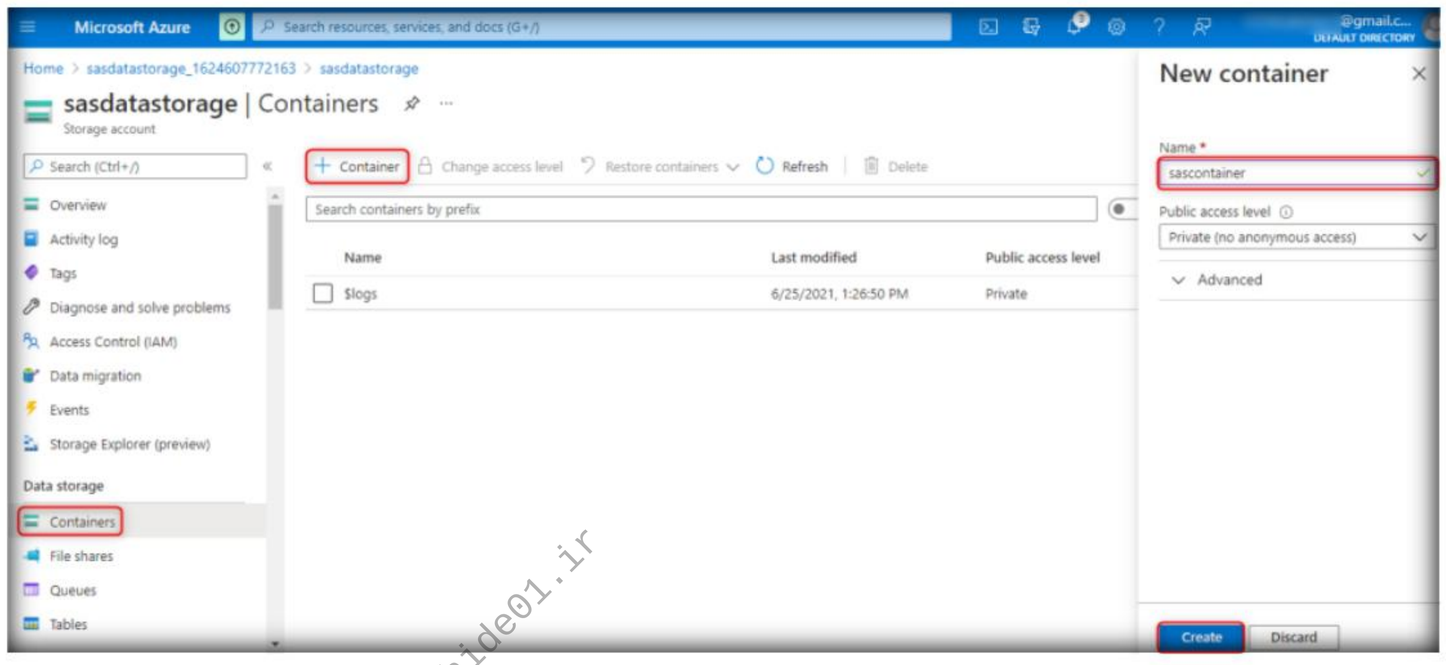


FIGURE 4.7.23: Successful Creation of New Storage Account

TASK 2

Generating SAS token to Restrict Access to Azure Storage Account

24. Now, to create a container in the storage account, click on **Containers** under **Data storage** in the left pane. Then, click on **+ Container** in the main page. In the **New container** side bar, enter the name of the container (**sascontainer** in this lab) and then click on **Create**.



hide01.ir

FIGURE 4.7.24: Creating a Container in Storage Account

25. Container **sascontainer** is successfully created now. Click on it.

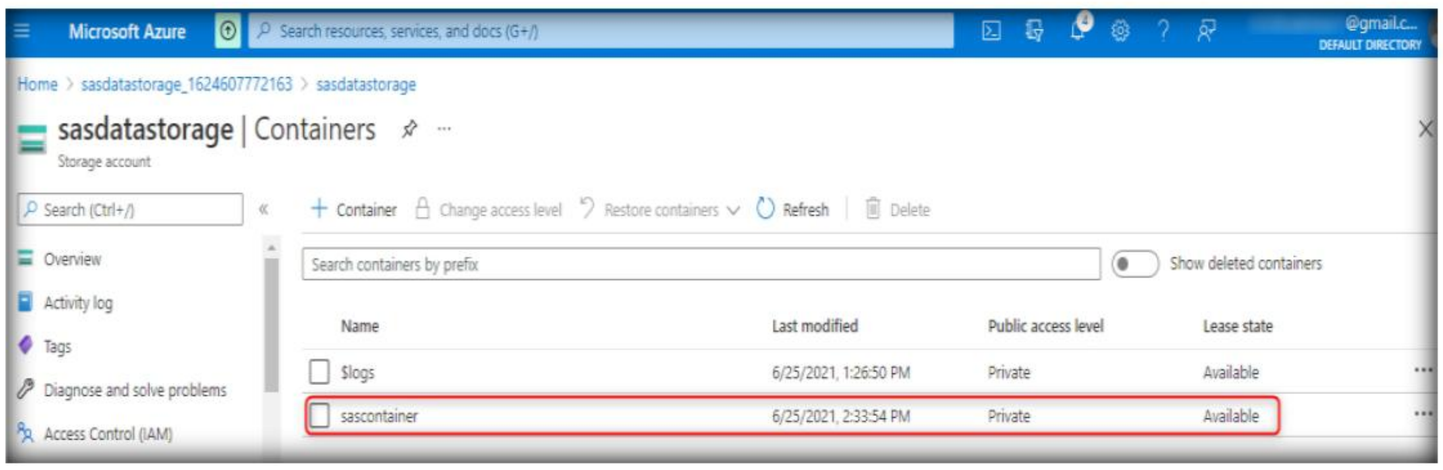


FIGURE 4.7.25: Container is Successfully Created

26. To upload some files into the container, click on **Upload** in the **sascontainer** window.

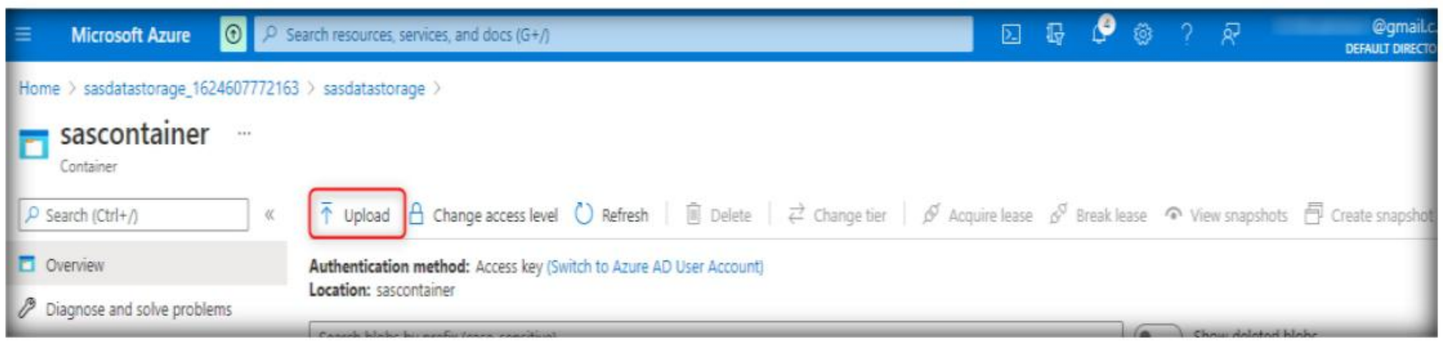


FIGURE 4.7.26: Selecting the Upload button

Certified Cloud Security Engineer Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

27. In the left pane, an **Upload blob** window will appear. Here, click on the folder icon, browse and select some random files, and then click on the **Upload** button.

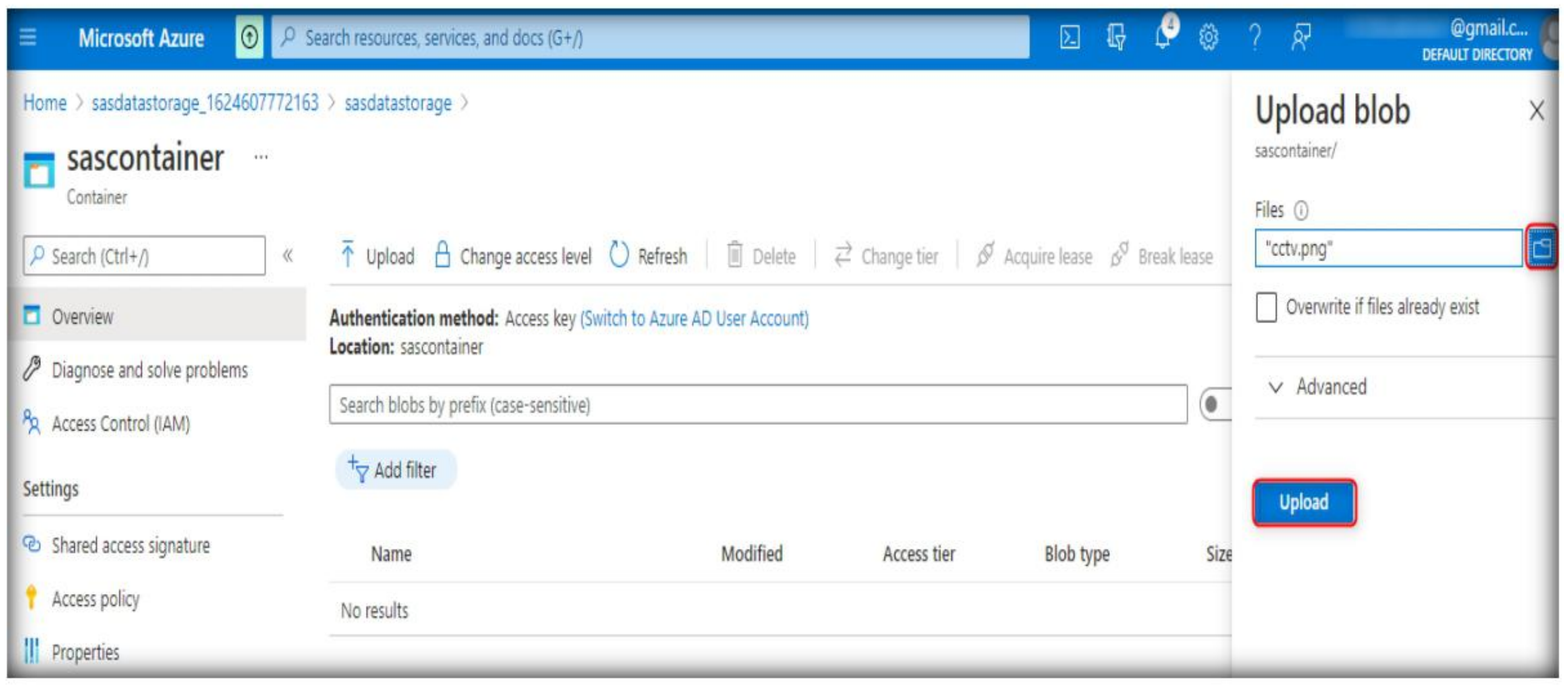


FIGURE 4.7.27: Browsing and Uploading a File

28. The file will be successfully added to the container.

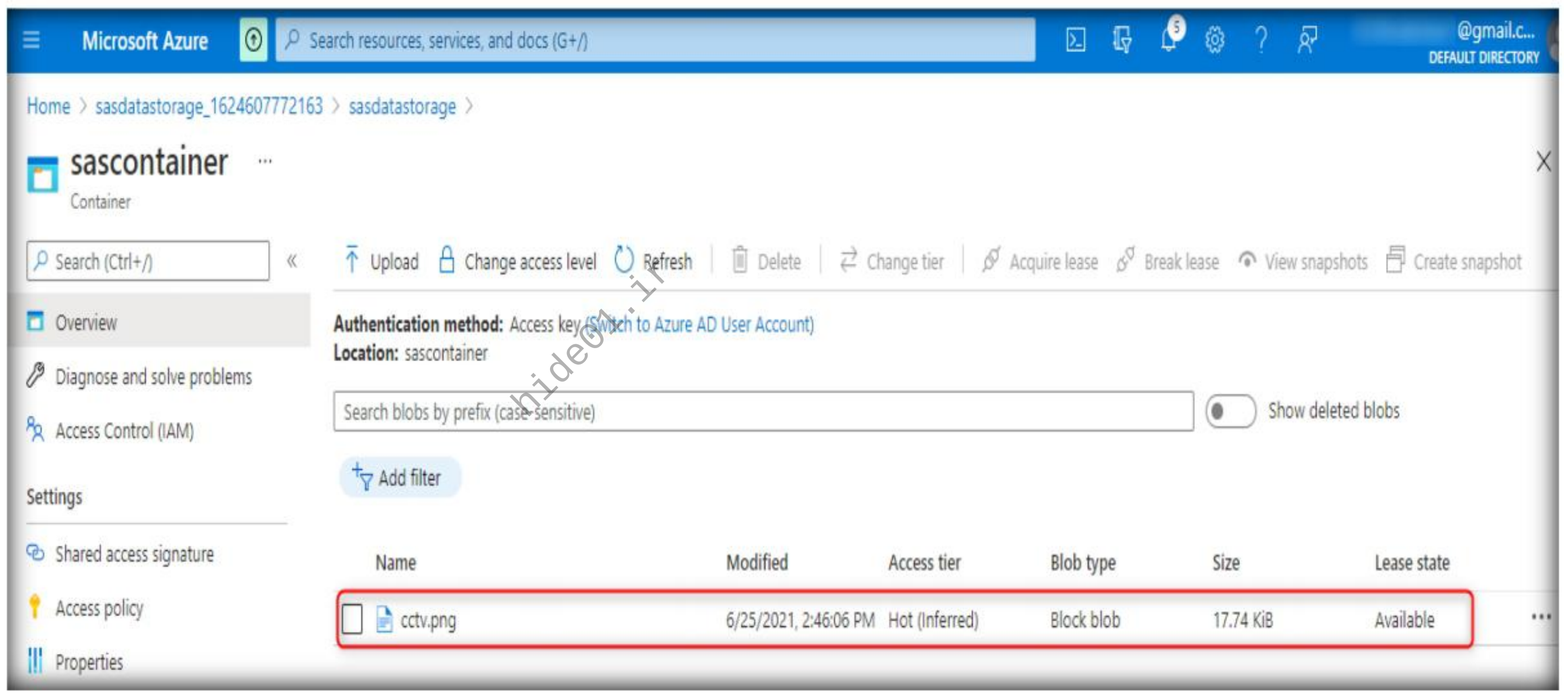


FIGURE 4.7.28: File Successfully Uploaded in the Container

29. Similarly, add another file to the container by repeating **Steps 26–28**.

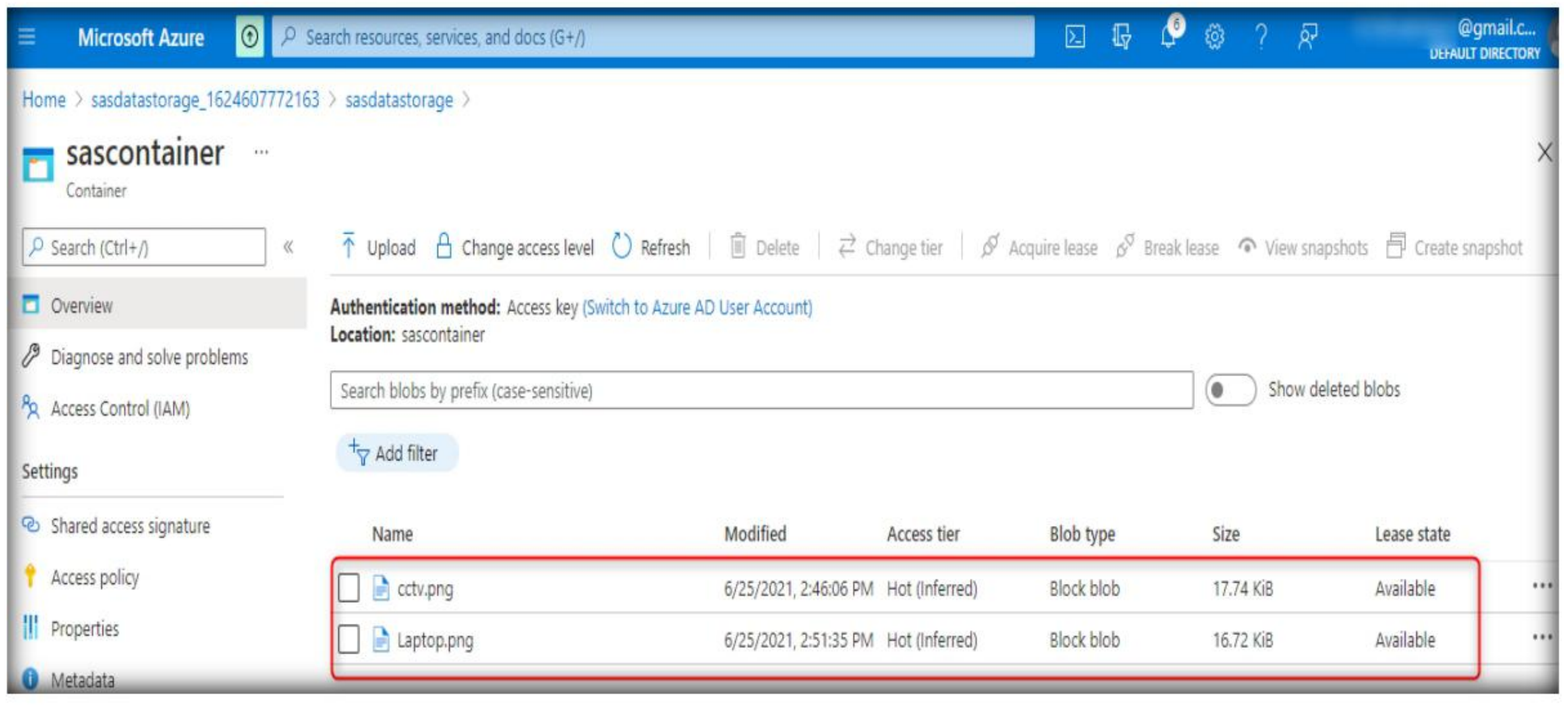


FIGURE 4.7.29: Successfully Uploading Another File in the Container

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

30. Now, to generate a SAS token and connection string, go back to the Azure portal and click on **Storage accounts** under **Azure services**.



FIGURE 4.7.30: Selecting Storage accounts in Azure Portal

31. A list of storage accounts will be displayed. Select the storage account (**sasdatastorage**) to which you want to generate a shared access signature.

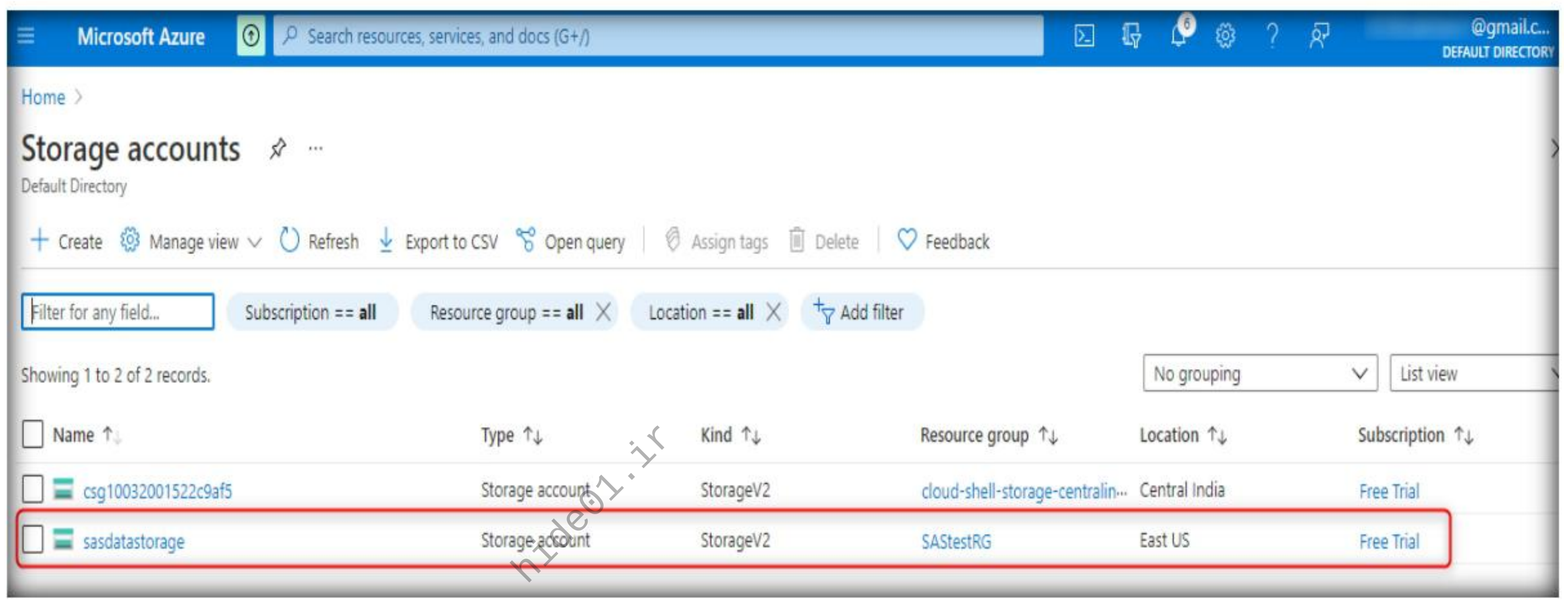


FIGURE 4.7.31: List of Storage Accounts

32. Under **Security + networking** in the left pane, click on **Shared access signature**.

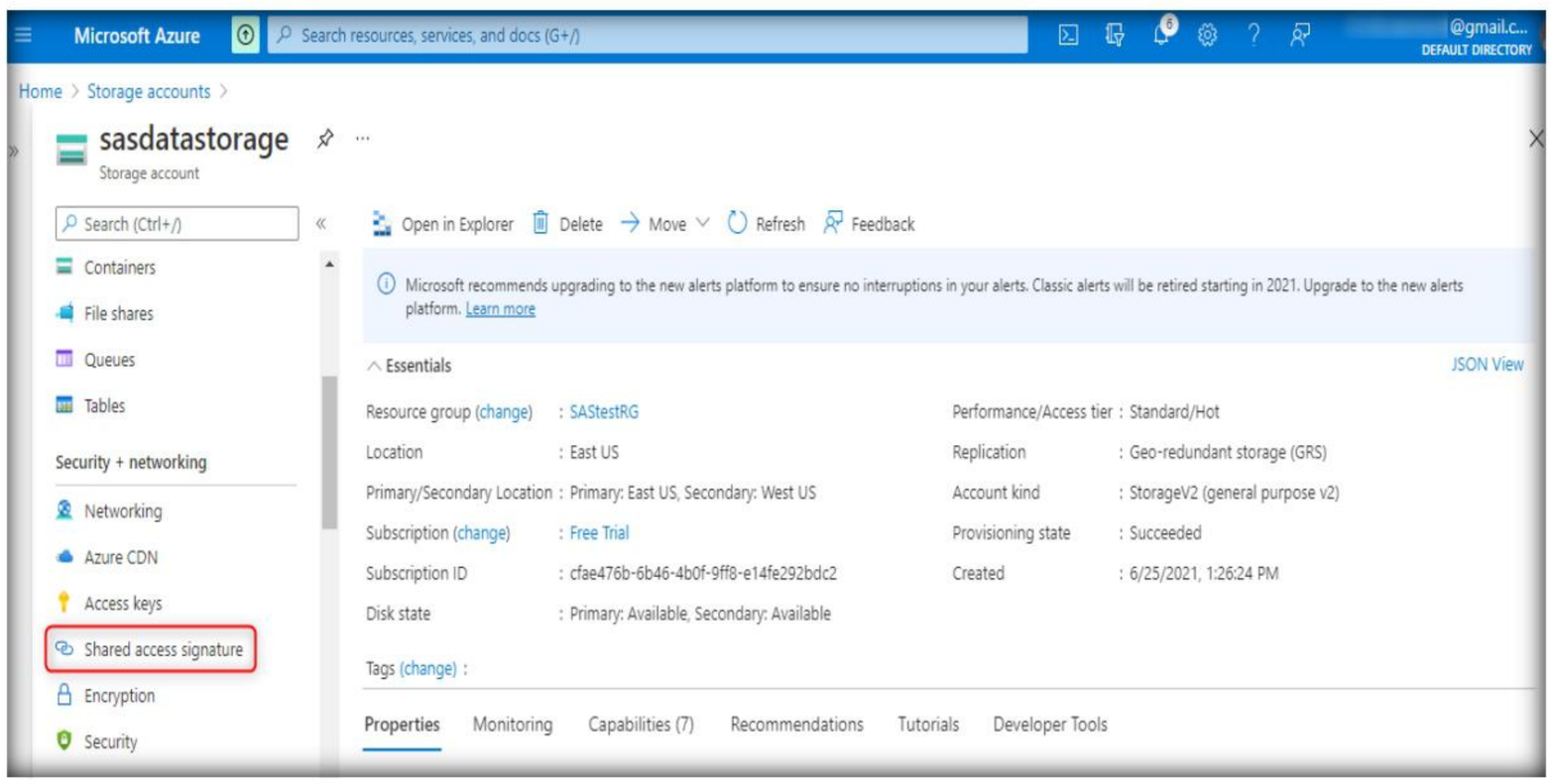


FIGURE 4.7.32: Selecting Shared access signature

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

33. Select the **Allowed services** that you want to allow access to (here, we have selected **Blob**). Select **Allowed resource types** as per your requirement (here, we have selected **Service** and **Container**). Select the necessary **Allowed permissions** for the users or clients (here, we have selected **Read** and **List**). Leave **Blob versioning permissions** in its default state.

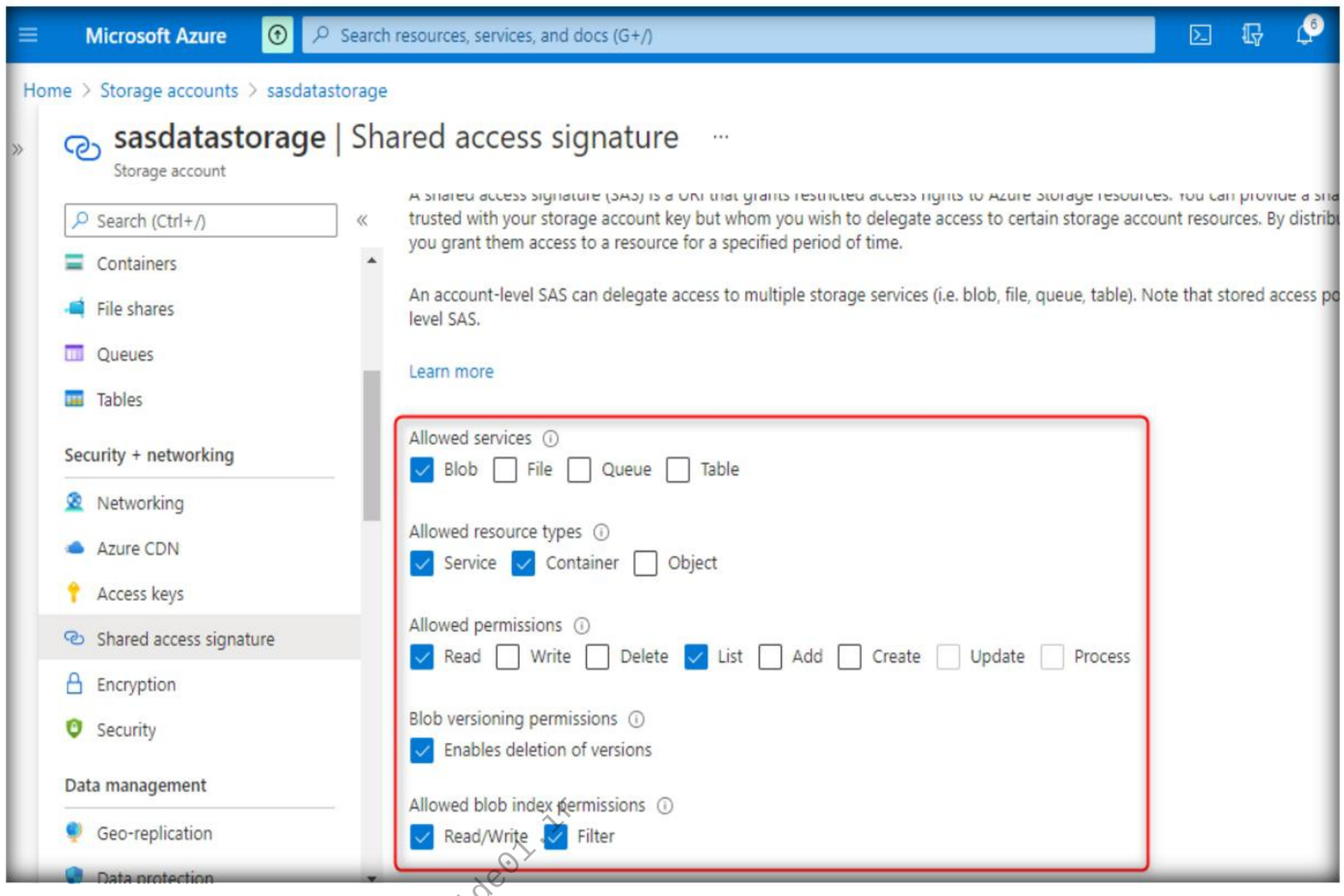


FIGURE 4.7.33: Selecting Allowed Services, Resources, and Permissions for SAS

34. Enter the **Start and expiry date/time** in their respective fields. For **Allowed protocols**, select the **HTTPS only** radio button. Leave **Preferred routing tier** as **Basic (default)**. Then, click on **Generate SAS and connection string** to generate tokens.

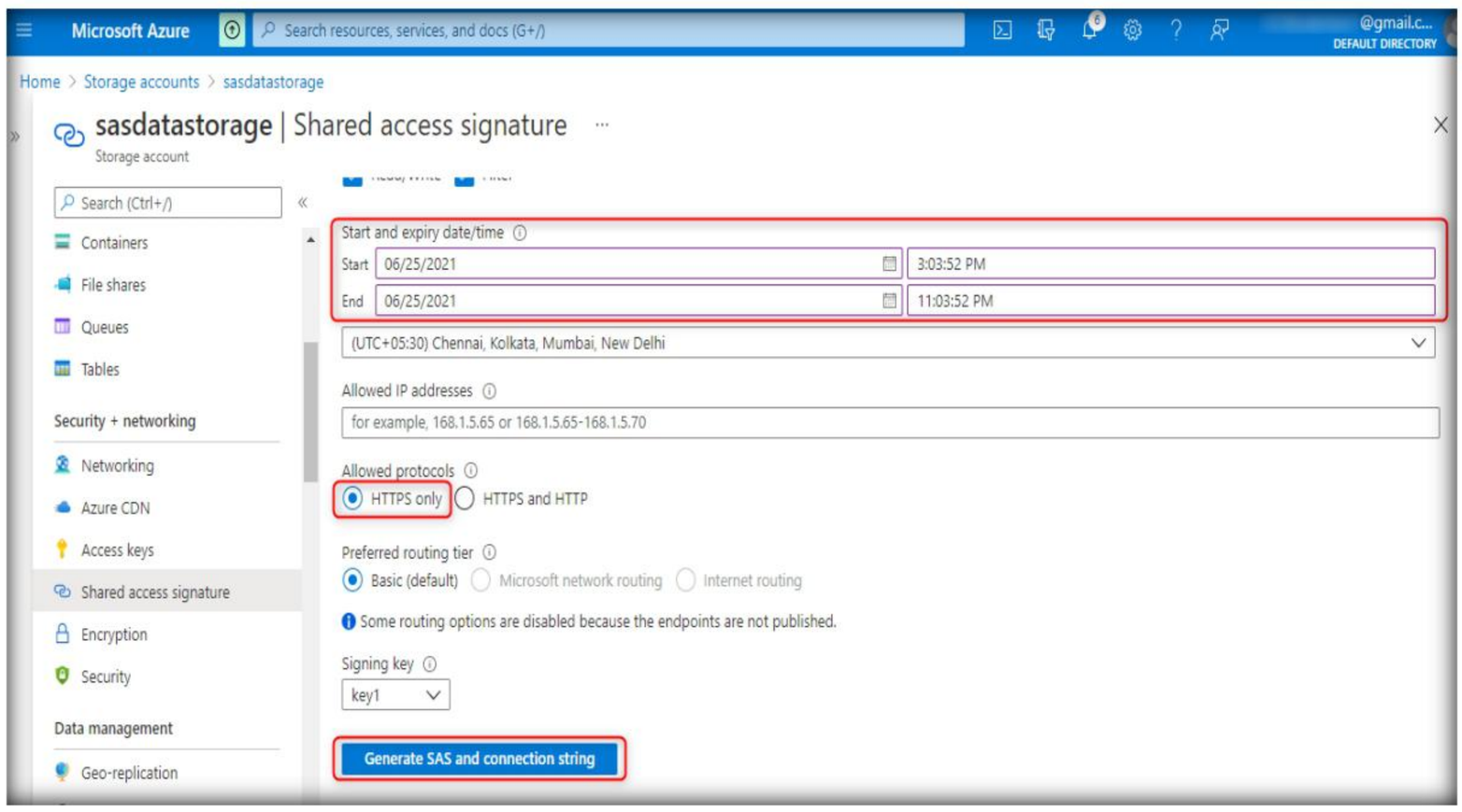


FIGURE 4.7.34: Generating SAS and connection string

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

35. The SAS token and connection string will be successfully generated. This will be used by the users or a client to access the storage account.

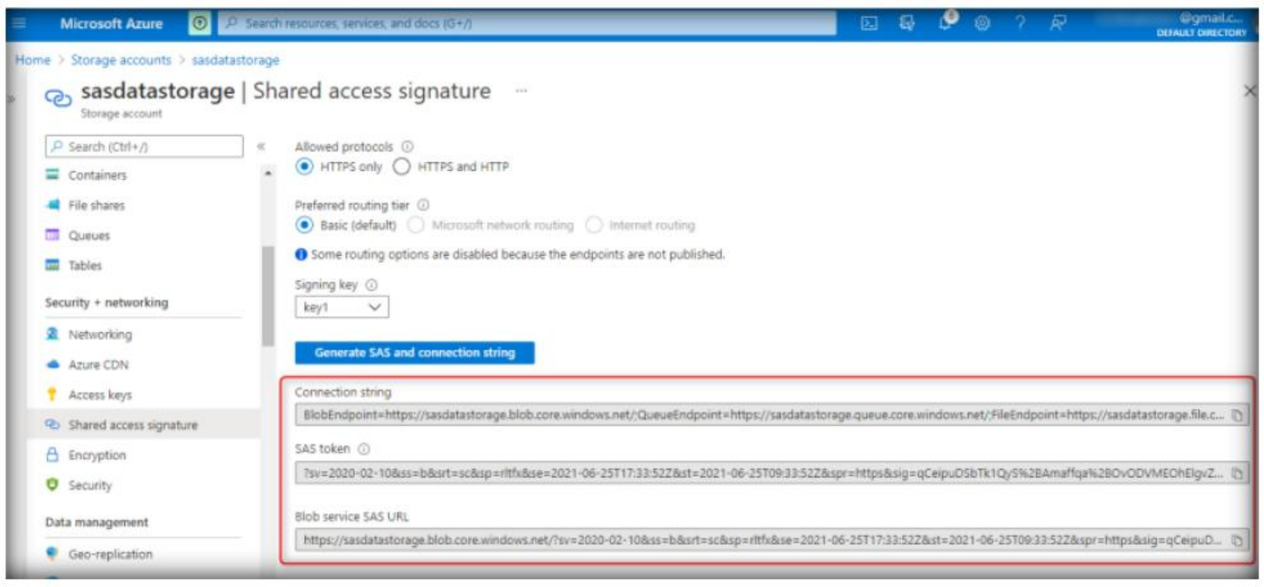


FIGURE 4.7.35: Successful Generation of SAS URI

36. Open Notepad and copy the **SAS URIs**. Then, save the notepad file on your desktop.



FIGURE 4.7.36: Successful Generation of SAS URI

TASK 3

Installing Azure Storage Explorer

37. A cloud security administrator can use this SAS token to restrict access to Azure storage account.

    To use the SAS token, a cloud security engineer needs to install Azure storage explorer on your VM. To install Azure storage explorer, open the Chrome browser and type Google in the address bar. Then, type **Azure Storage Explorer** in the Google search bar.



FIGURE 4.7.37: Searching for Azure Storage Explorer in Google

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

38. Click on the **Azure Storage Explorer – cloud storage management** link.

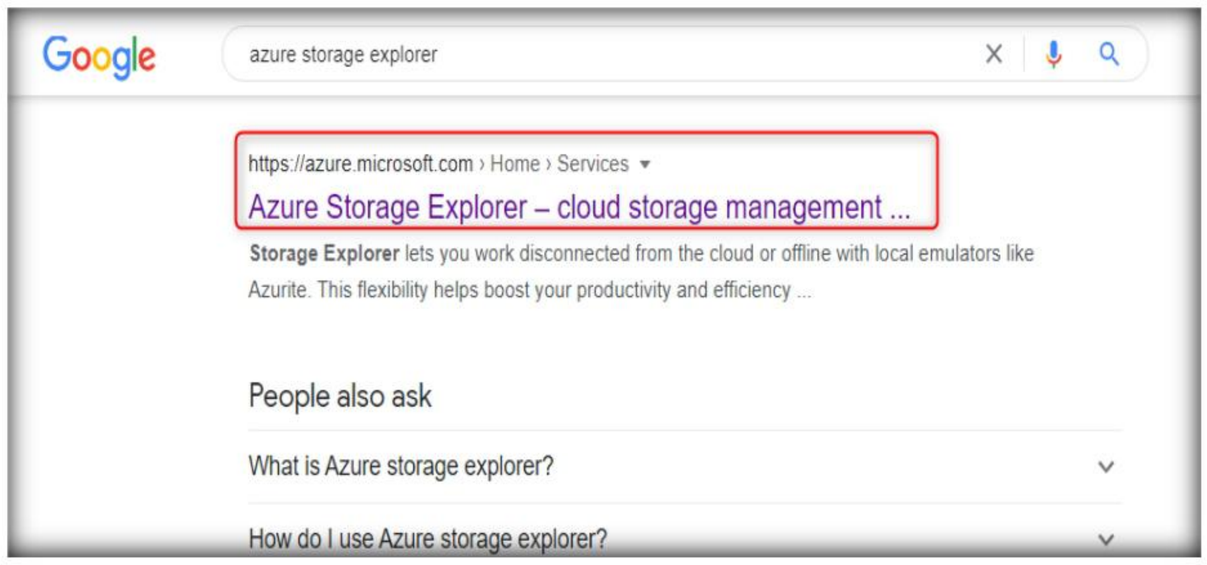


FIGURE 4.7.38: Opening the link of Azure Storage Explorer

39. In the **Operating system** dropdown, select **Windows** and then click on the **Download now** button.

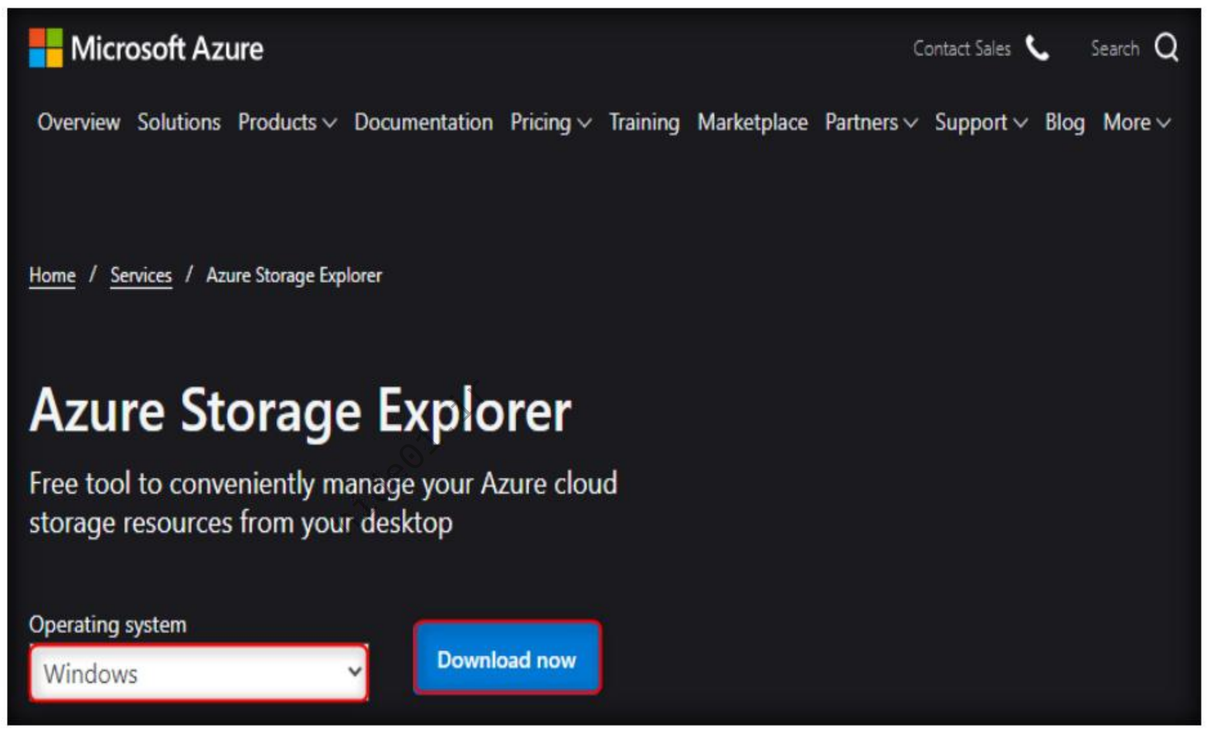


FIGURE 4.7.39: Downloading Azure Storage Explorer Application

40. **StorageExplorer.exe** file will be downloaded now. Run this file by clicking on it.

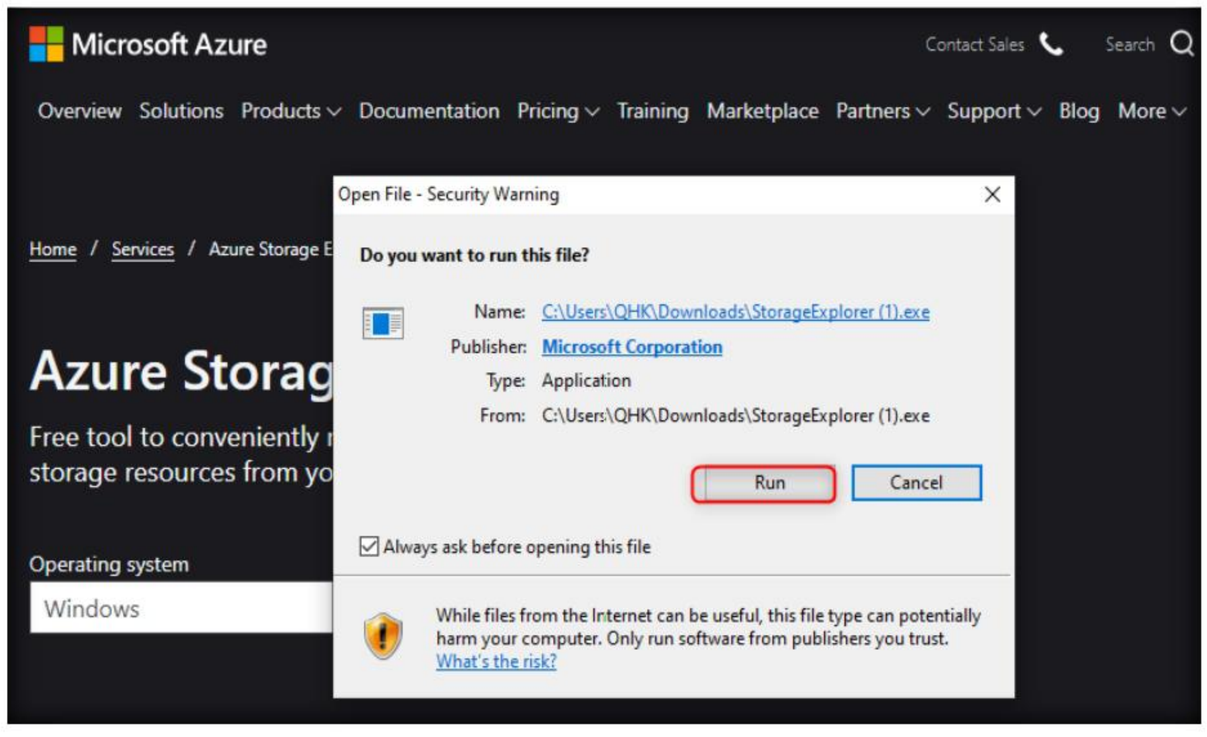


FIGURE 4.7.40: Running Azure Storage Explorer Application

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

41. A **Select Install Mode** window will now appear. Click on **Install for me only**.

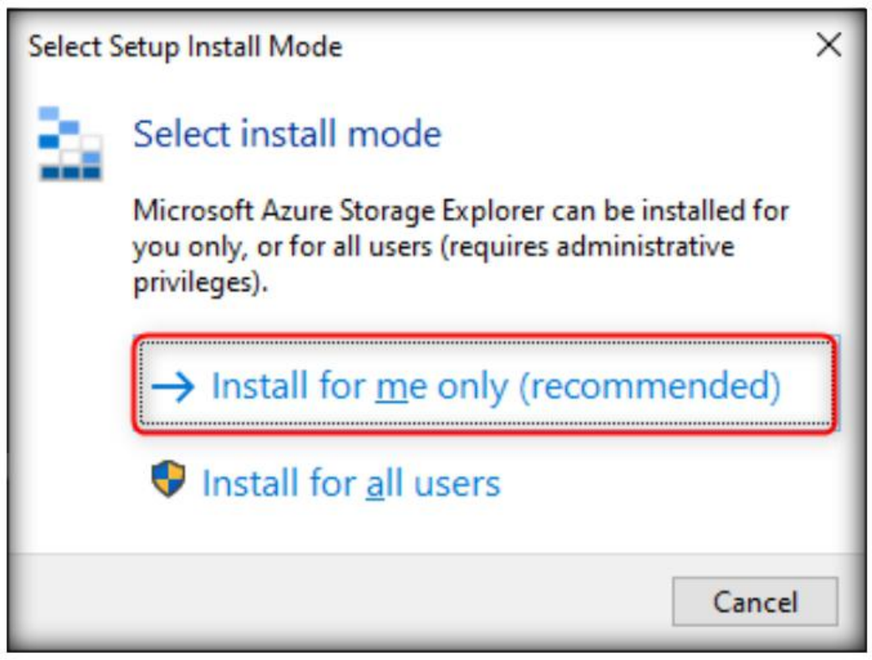


FIGURE 4.7.41: Selecting the Installation Mode

42. A **License Agreement** window will appear now. Select **I accept the agreement** radio button and then click on the **Install** button.

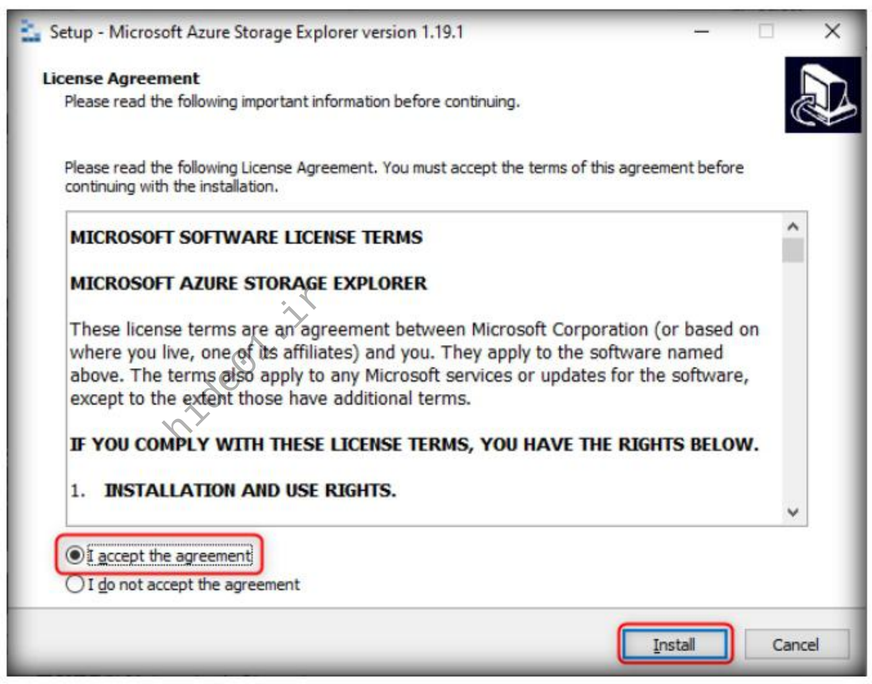


FIGURE 4.7.42: Accepting the License Agreement

43. Select the location where you want to install **Microsoft Azure Storage Explorer** and then click on **Next**.

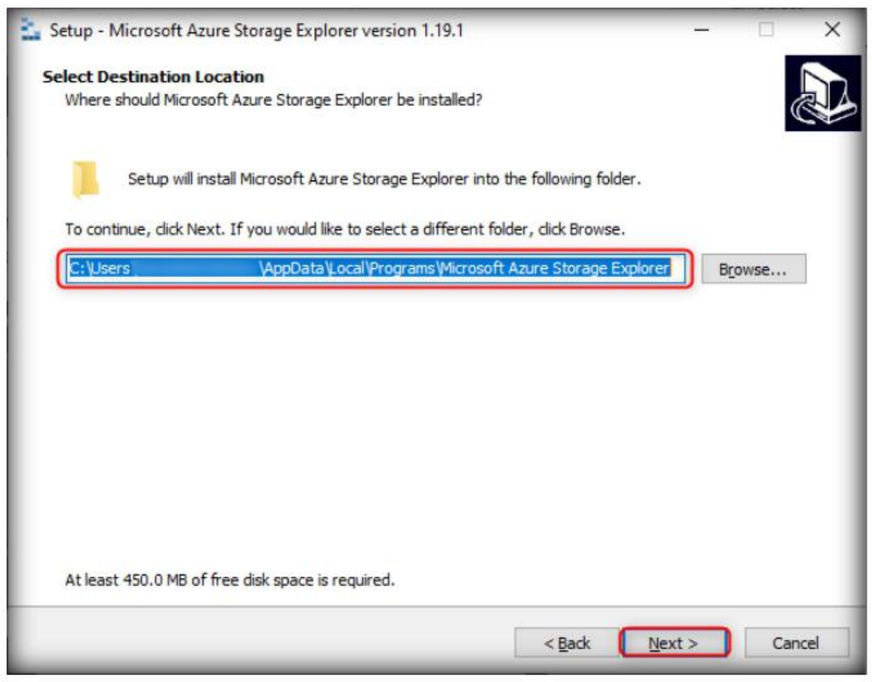


FIGURE 4.7.43: Choosing the location for Azure Storage Explorer

Certified Cloud Security Engineer Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

44. A **Select Start Menu Folder** window will appear now. Leave it in its default state and click on **Next**.

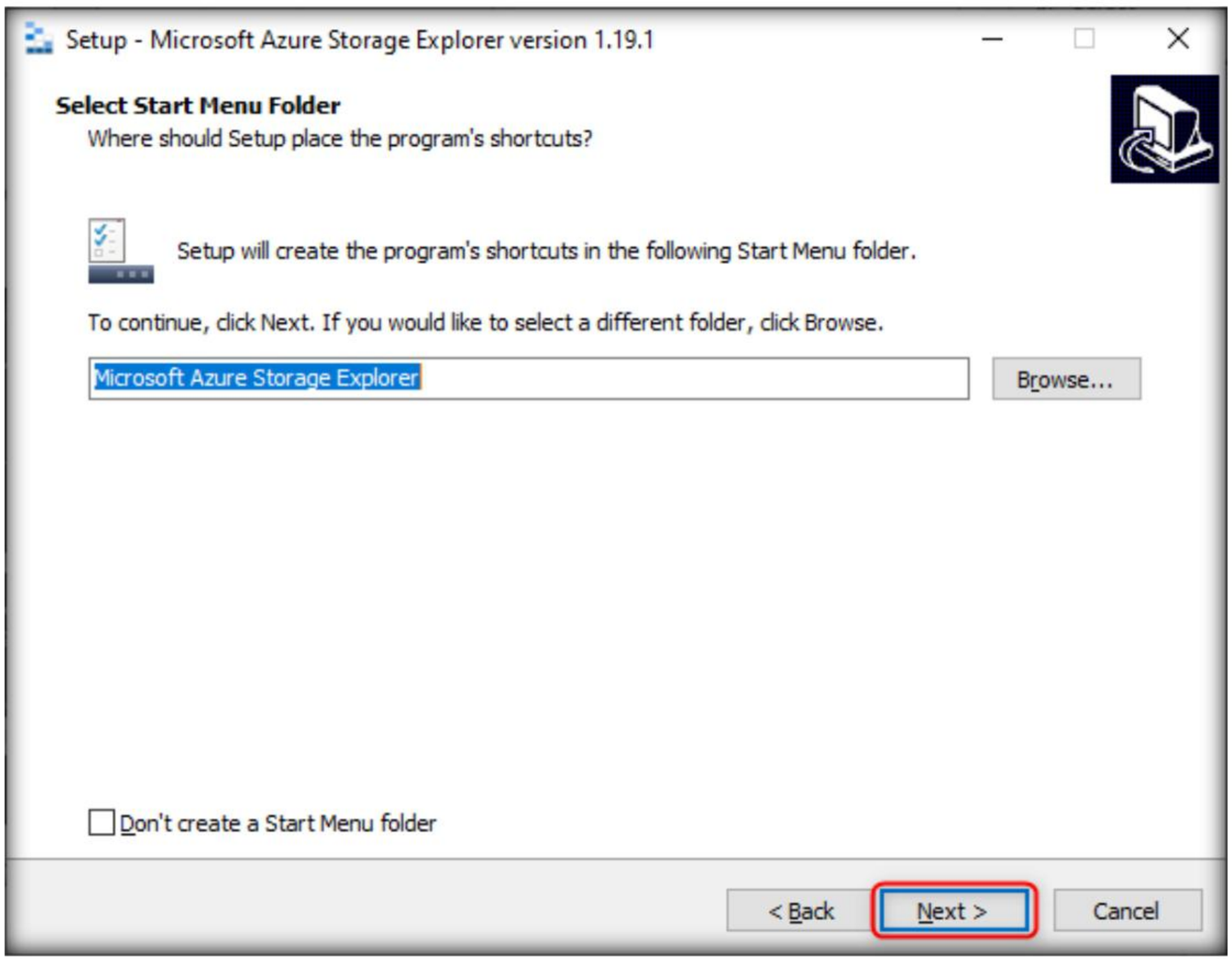


FIGURE 4.7.44: Start Menu Window Selection

45. Wait for a few seconds for the installation to complete.

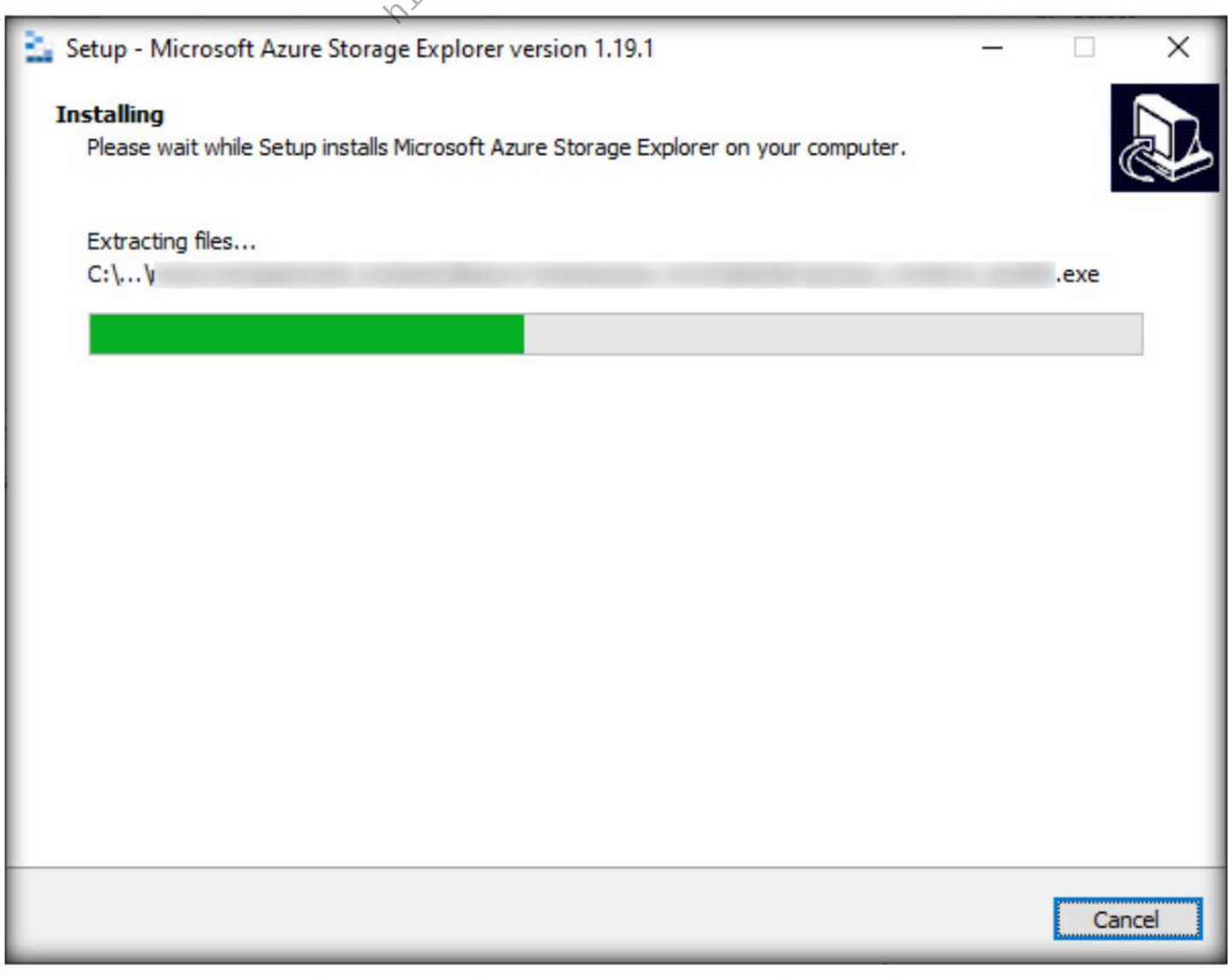
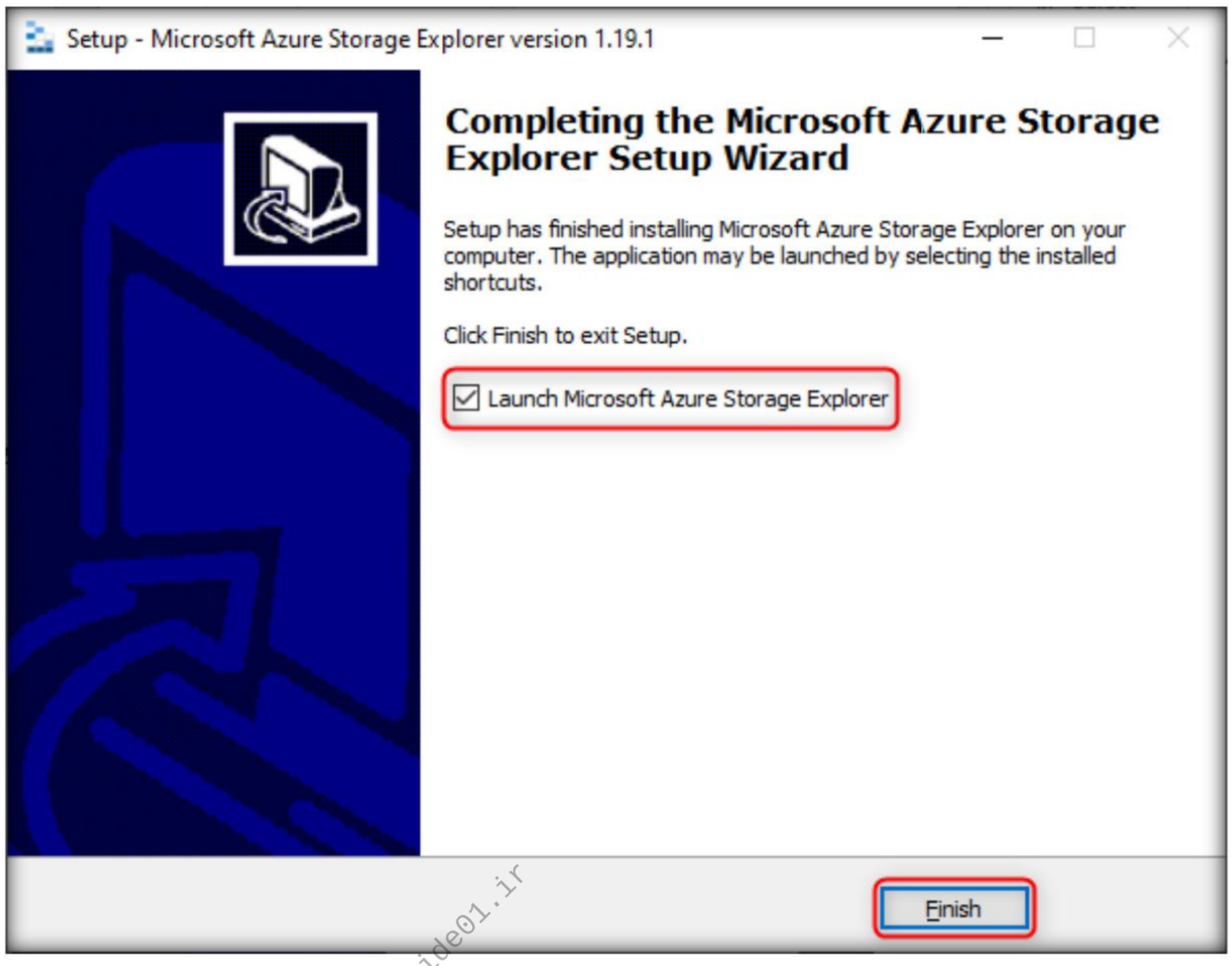


FIGURE 4.7.45: Progress of Azure Storage Explorer Installation

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

46. A **Completing the Microsoft Azure Storage Explorer Setup Wizard** window will appear now. Check the **Launch Microsoft Azure Storage Explorer** option and then click on **Finish**.



hide01.ir

FIGURE 4.7.46: Azure Storage Explorer Installation Completion

47. **Microsoft Azure Storage Explorer** will be launched in a few seconds.

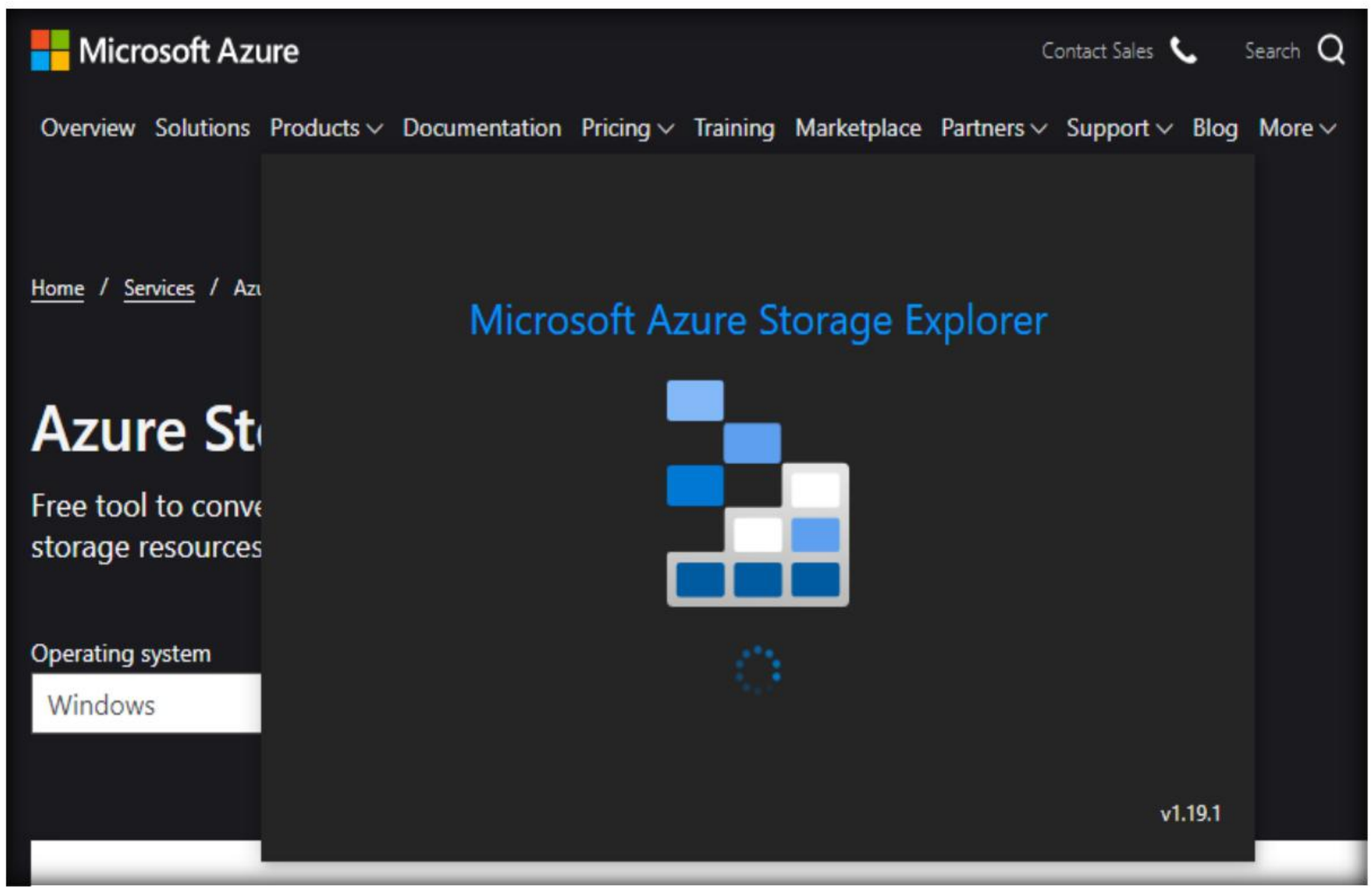


FIGURE 4.7.47: Launching of Azure Storage Explorer

Certified Cloud Security Engineer Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

48. **Azure Storage Explorer** application dashboard will be displayed now.

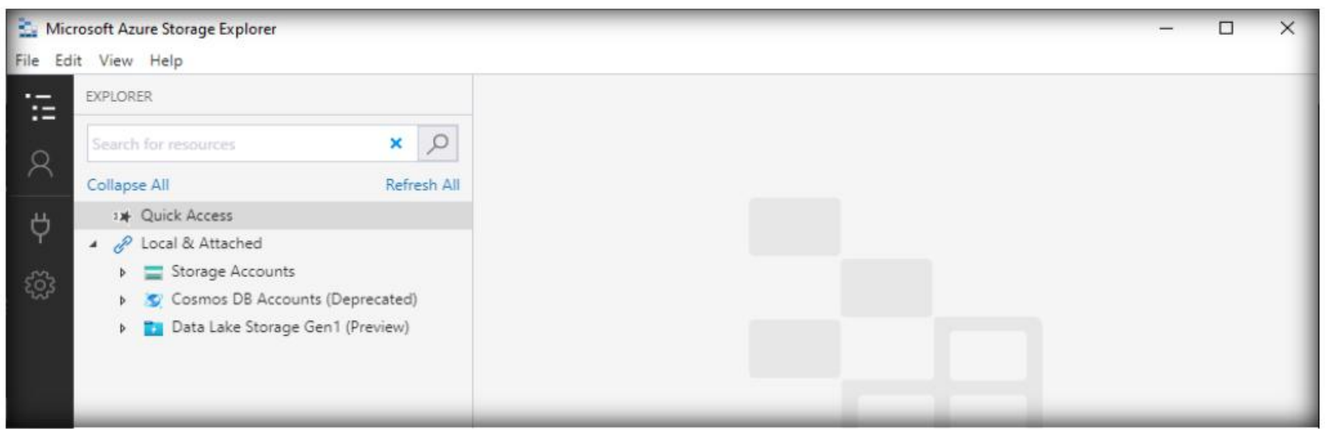


FIGURE 4.7.48: Dashboard of Azure Storage Explorer

TASK 4

Restricting Access to the Azure storage account using the SAS URI

49. A security administrator can allow access to clients or users with a SAS token for the storage account. A client or user without a SAS token or with an expired SAS token cannot access the storage account. Thus, a security administrator can regulate the activities on a storage account with a SAS token.

In the **Microsoft Azure Storage Explorer** dashboard, click on the **Manage Account** icon and then click on **Add an account….**



FIGURE 4.7.49: Adding Storage Account in Azure Storage Explorer

50. In the **Select Resource** window that appears, navigate and click on **Storage account or service**.

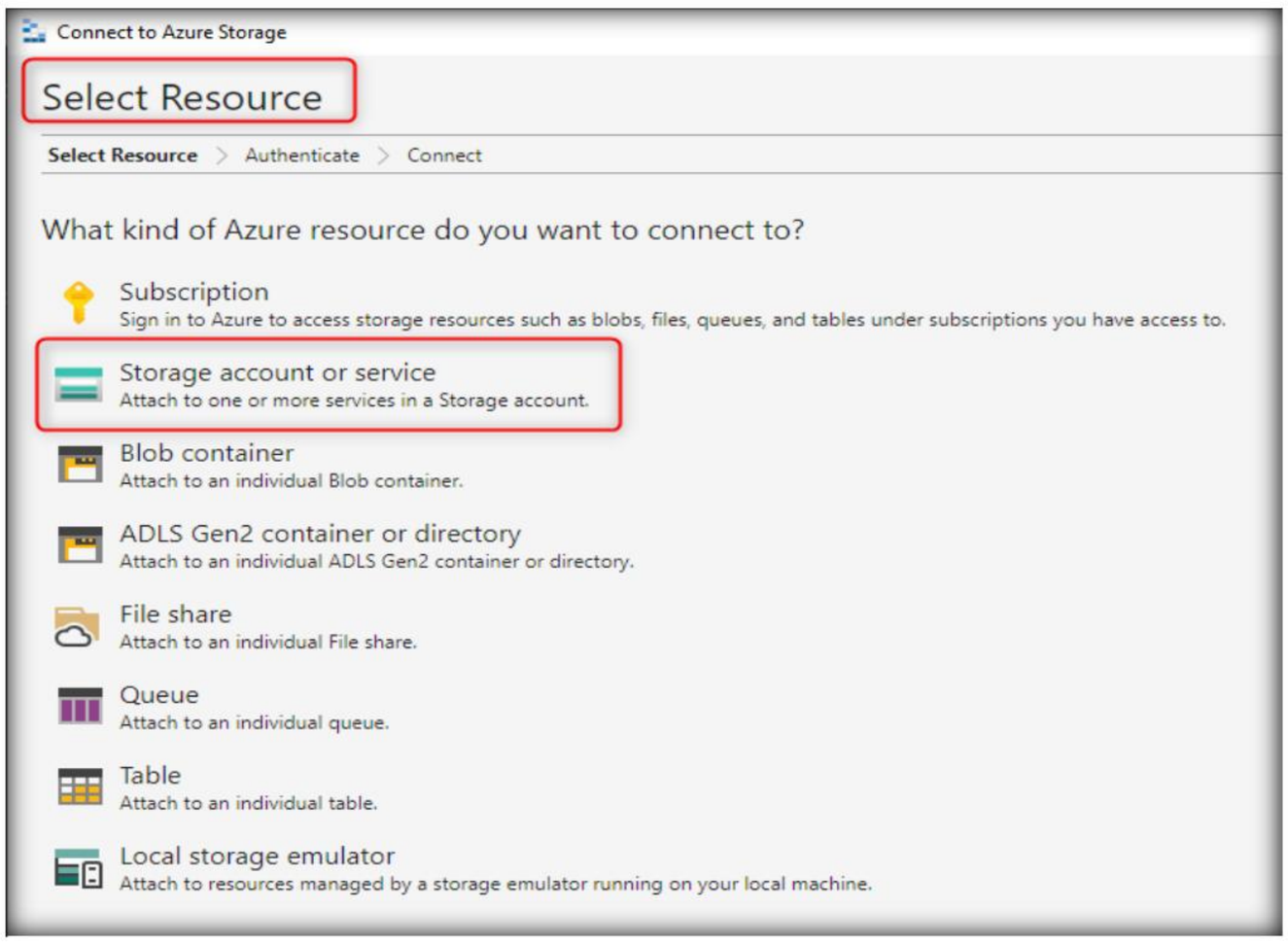


FIGURE 4.7.50: Selecting Storage Account or Service in Azure Storage Explorer

Certified Cloud Security Engineer Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

51. The **Select Connection Method** window will appear now. Select **Shared access signature URL (SAS)** and then click on **Next**.

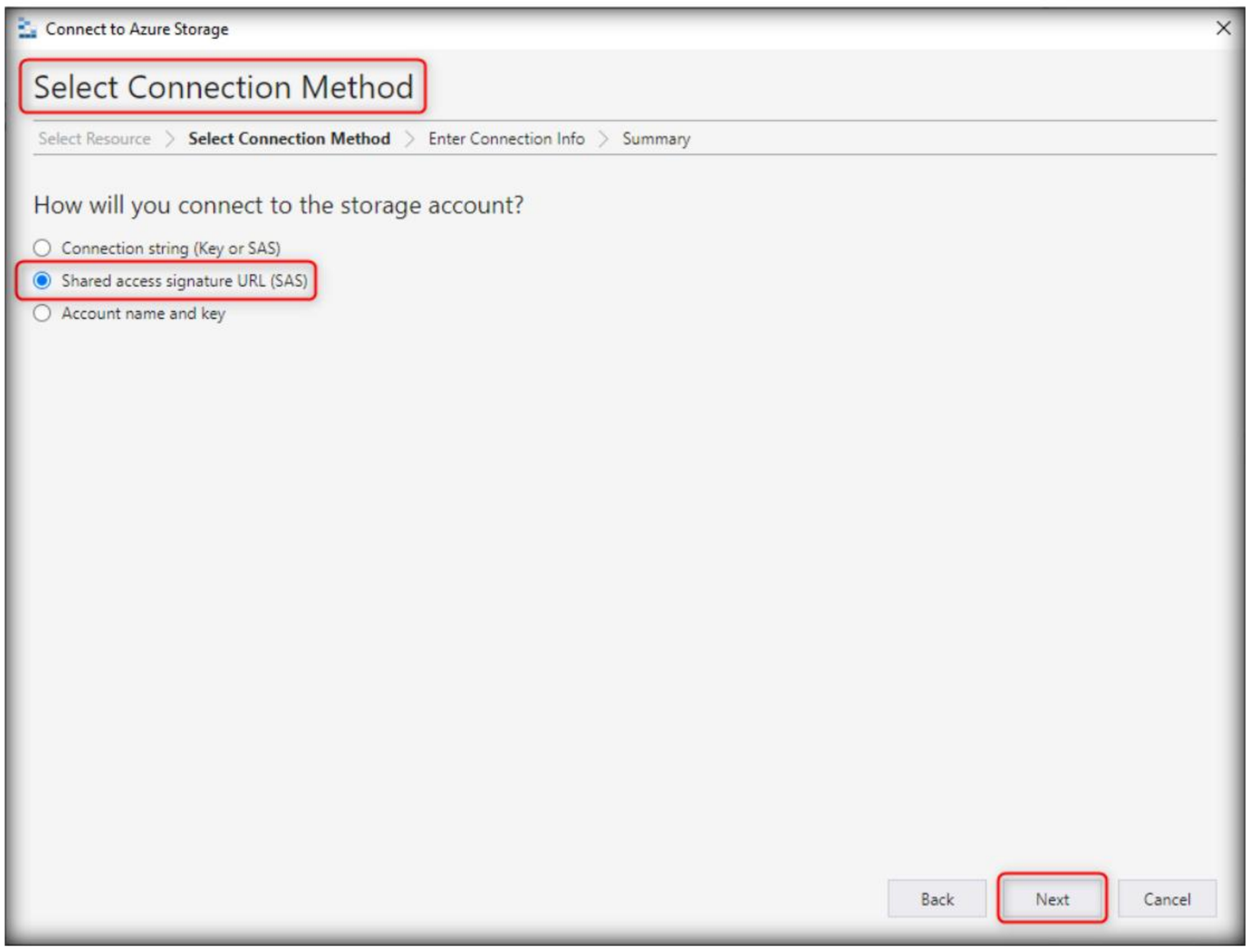


FIGURE 4.7.51: Selecting the radio button of Shared access signature URL

52. The **Enter Connection info** window will appear now. In the **Service URL** box, paste the **SAS URL** that was copied in **Step 30** and click on the **Next** button.

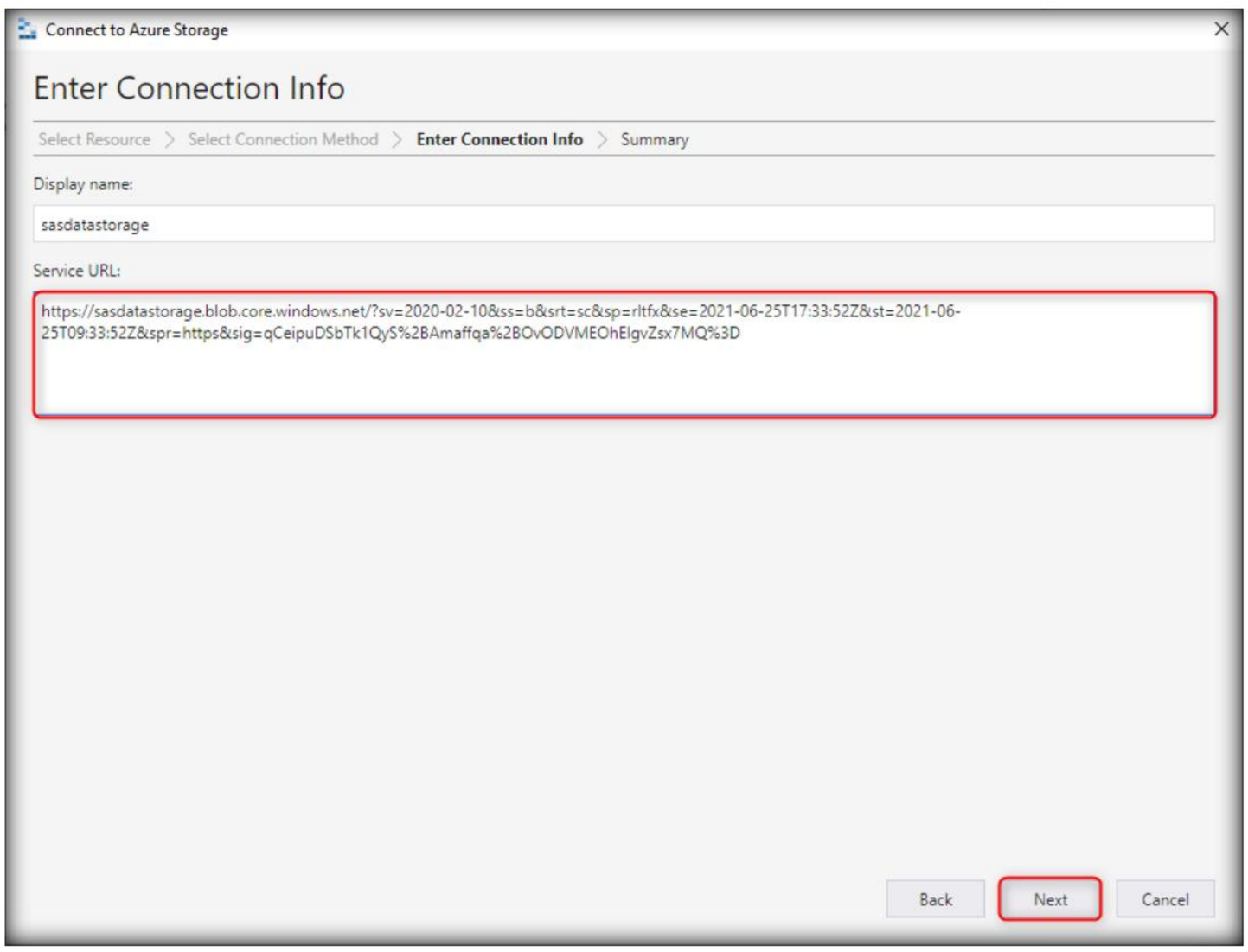


FIGURE 4.7.52: Pasting the SAS URL

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

53. In the **Summary** window that appears, click on the **Connect** button.

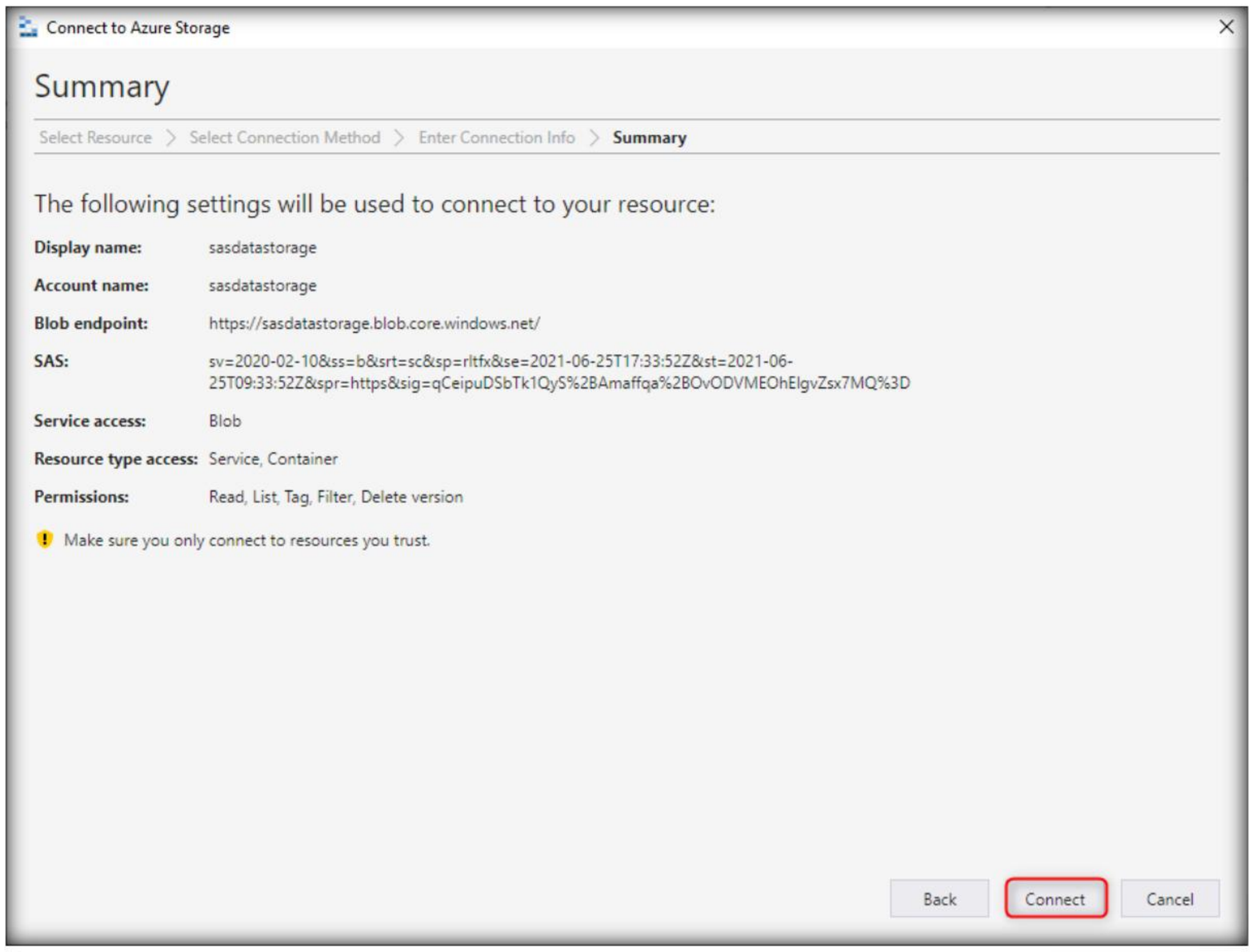


FIGURE 4.7.53: Connecting with Azure Storage Account

54. The new connection will be added successfully to the storage account.

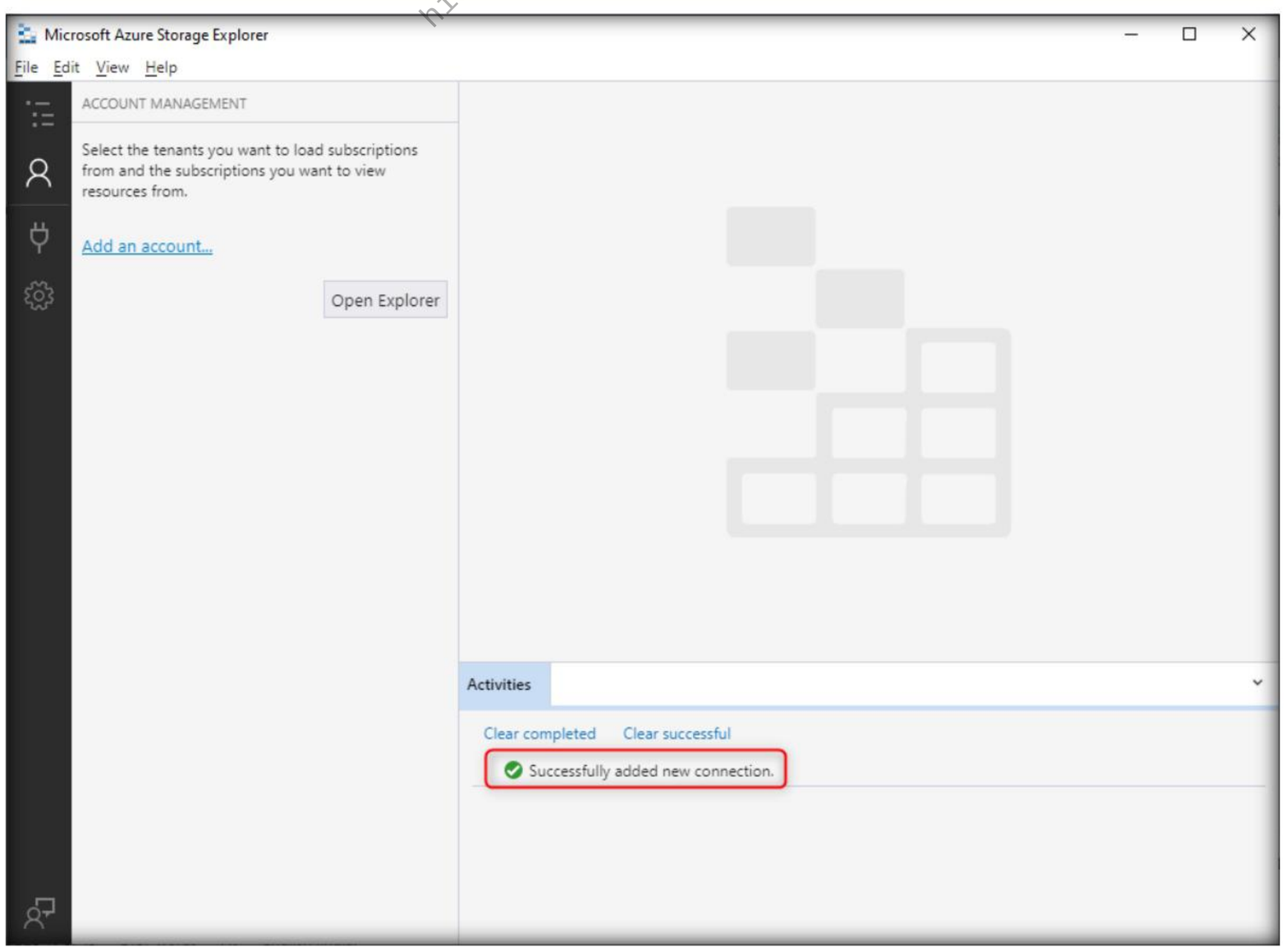


FIGURE 4.7.54: Successfully Establishing the Connection with Azure Storage Account

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

55. Click on **Microsoft Azure Storage Explorer**, navigate and expand **Storage Accounts** and then the **sasdatastorage (SAS)** account, and finally click on the **sascontainer** container. You will observe the files present in the container.

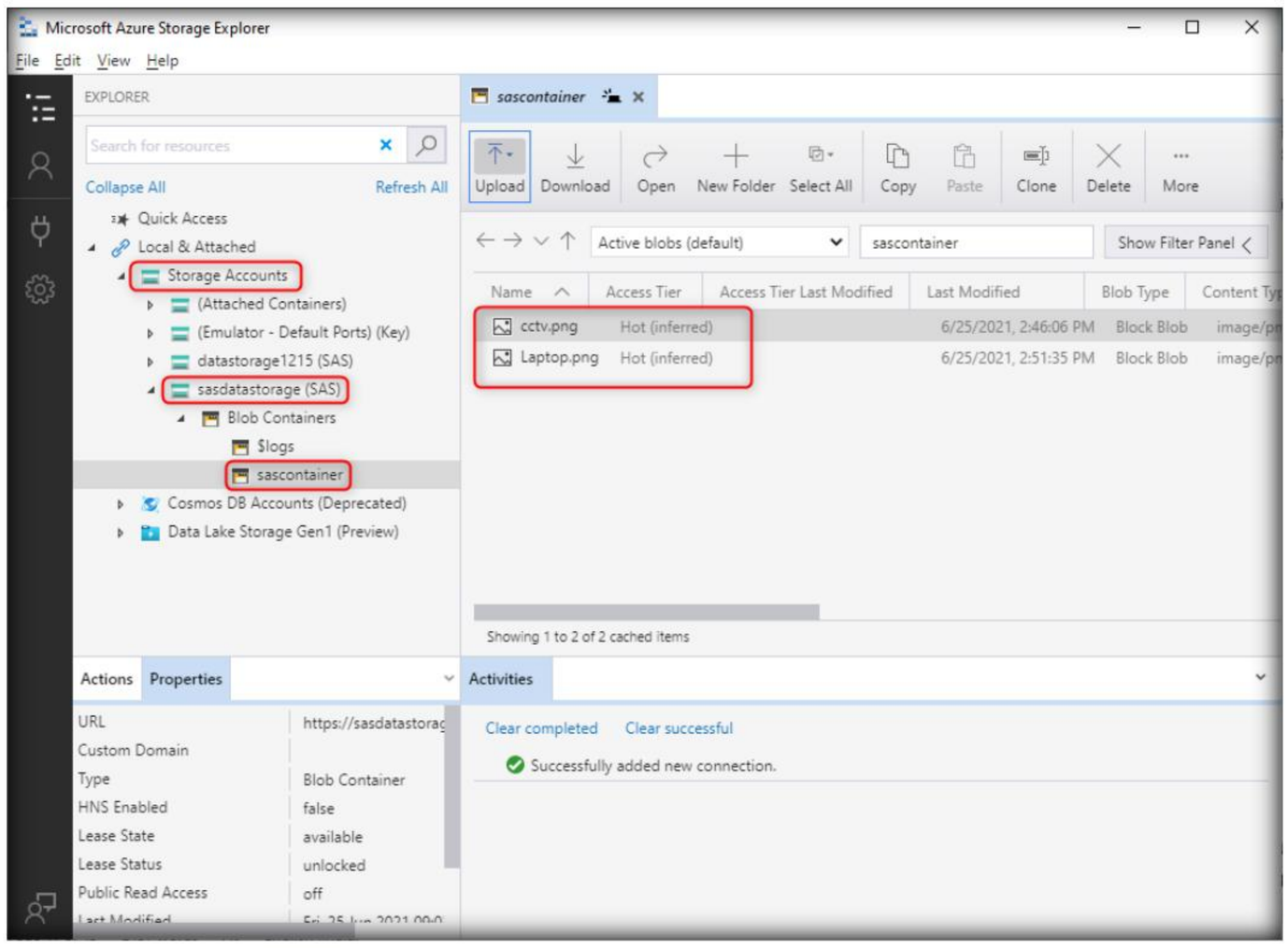


FIGURE 4.7.55: Checking the Container of Azure Storage Account in Azure Storage Explorer

56. The client or the user is allowed to read and list the content of the storage account. They are not allowed to delete or upload any content on the storage account. Now, if you try to download the file, it will be downloaded.

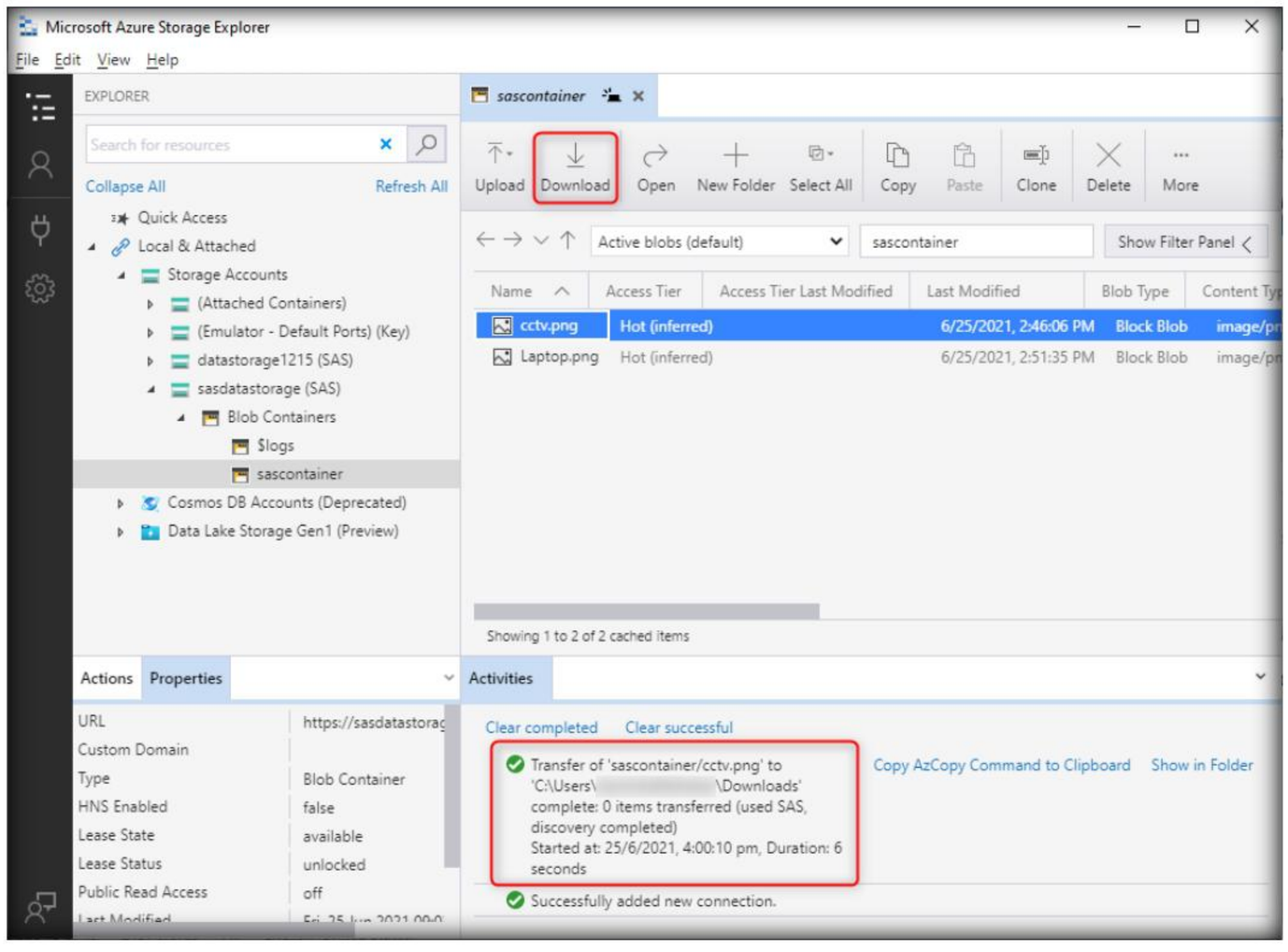


FIGURE 4.7.56: Downloading File from the Container of Azure Storage Account

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

57. Click on **Delete** at the top right corner. The client or user will not be able to delete the file as the delete permission has not been given to them.

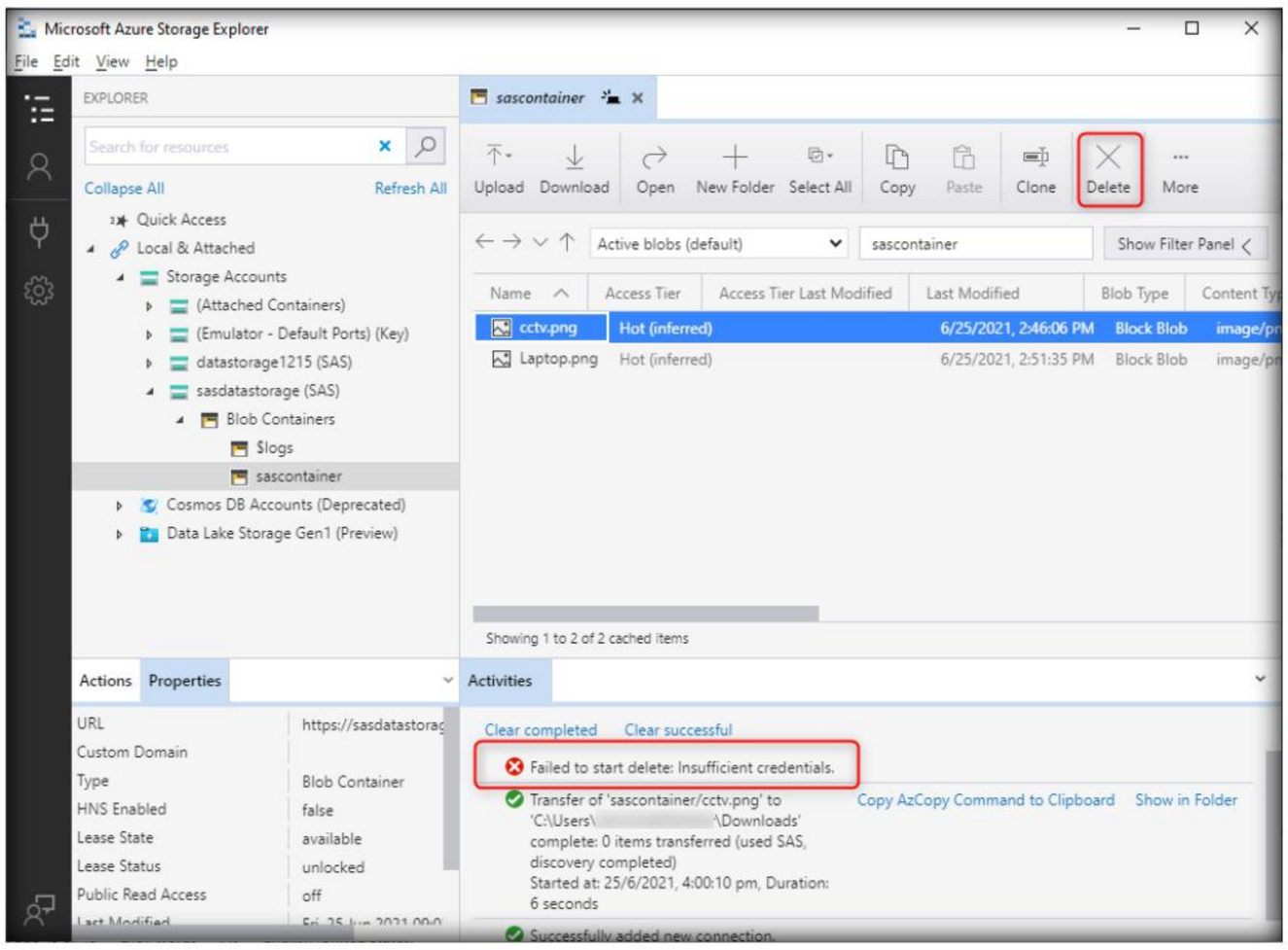


FIGURE 4.7.57: Failed to Delete File from the Container of Azure Storage Account

58. This way, a cloud security administrator can stringently regulate the access to a storage account. Based on the requirements, an administrator can give or restrict access to users or clients through shared access signature.

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

59. Navigate to **Storage accounts** in Azure Portal. Click on the name of the storage account (**sasdatastorage**) to open the **Overview** window. Click on **Delete** at the top. Type the storage account name in the **Delete storage account** window and click on **Delete**.

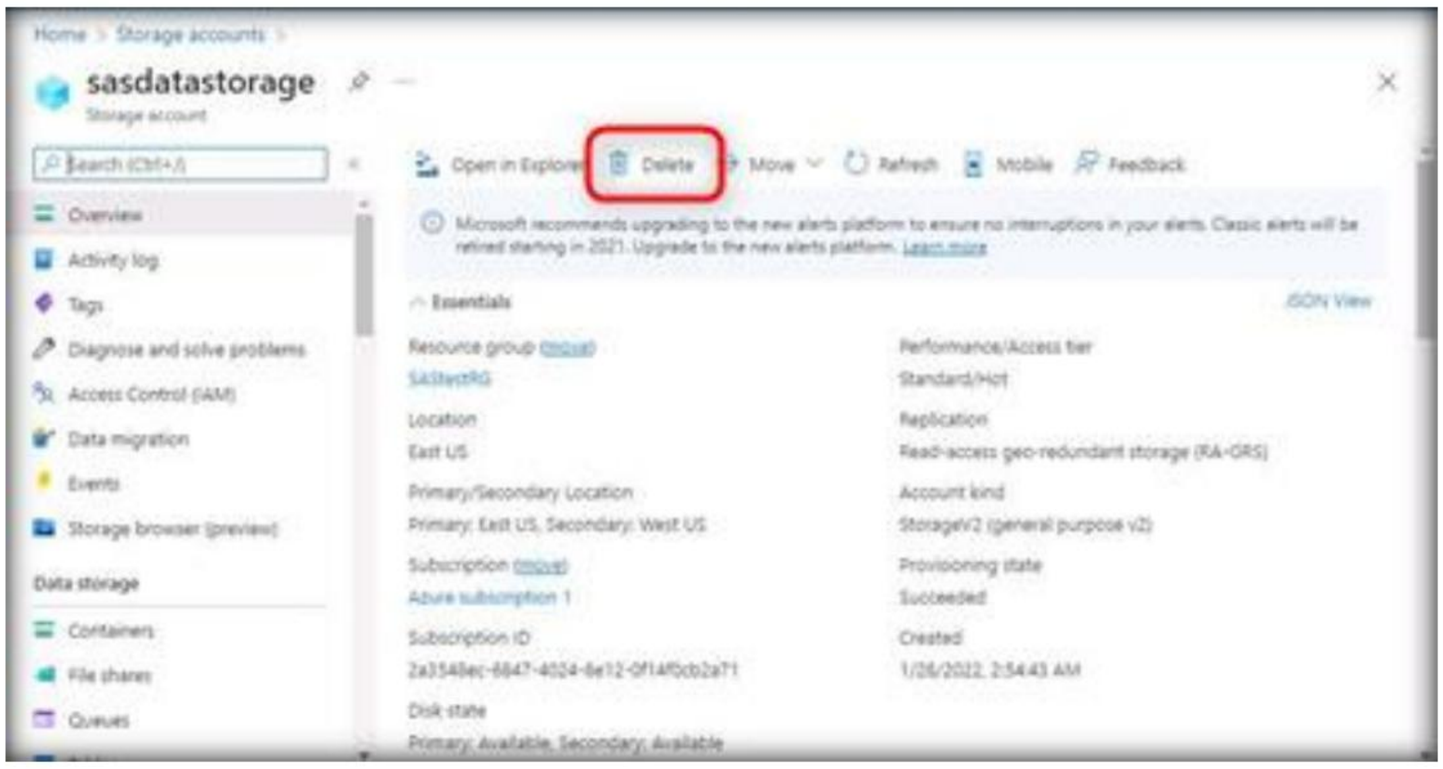


FIGURE 4.7.58: Deleting Storage Account

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

60. Navigate to **Resource groups** in the Azure portal. Click on the name of the resource group (**SastestRG**) to open the **Overview** window. Click on **Delete resource group**. In the **Delete resource group** window, type the name of the resource group and click on **Delete**.

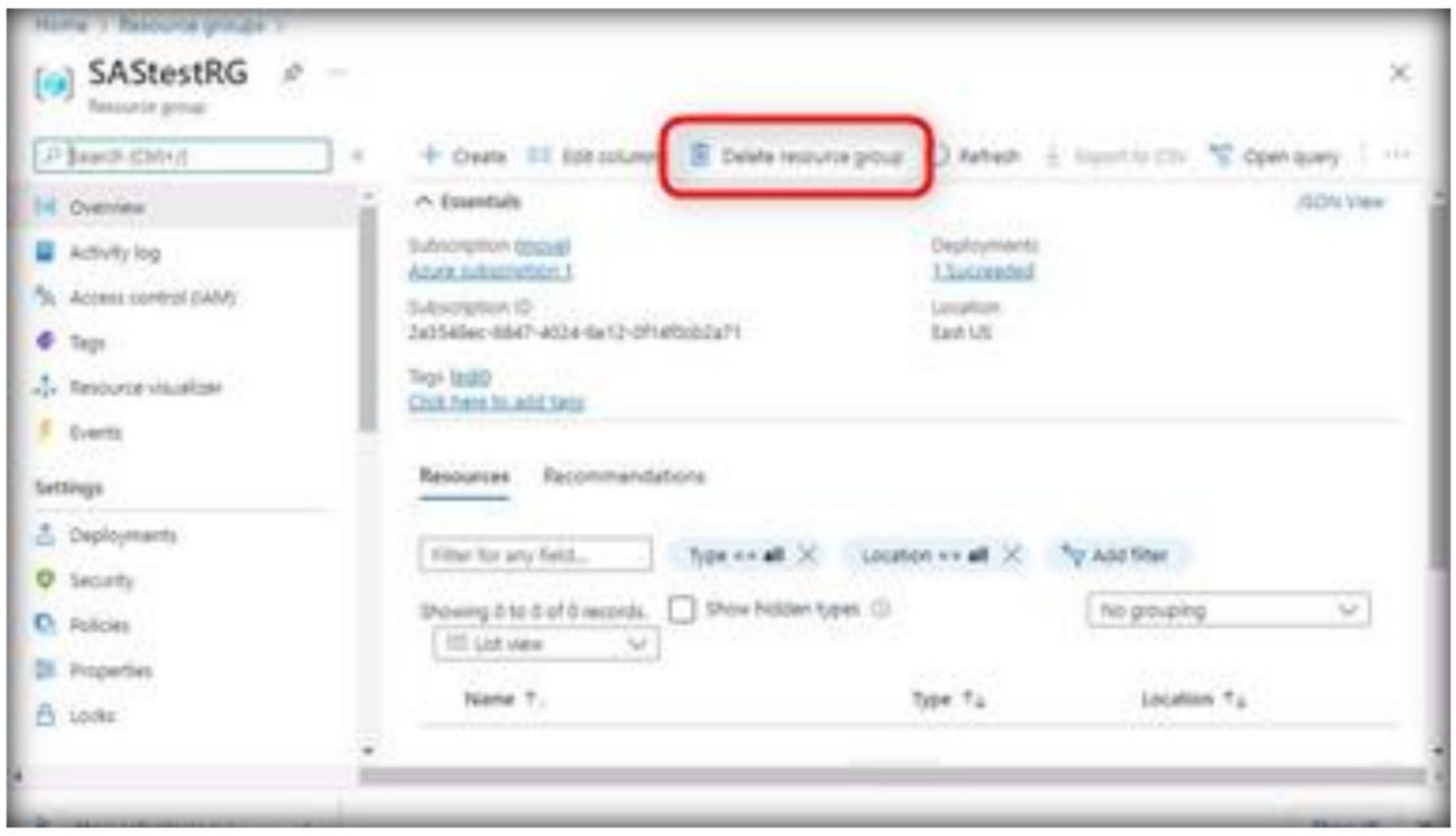


FIGURE 4.7.57: Deleting Resource Group

Lab Analysis

hide01.ir

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.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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.

hide01.ir

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

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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**.

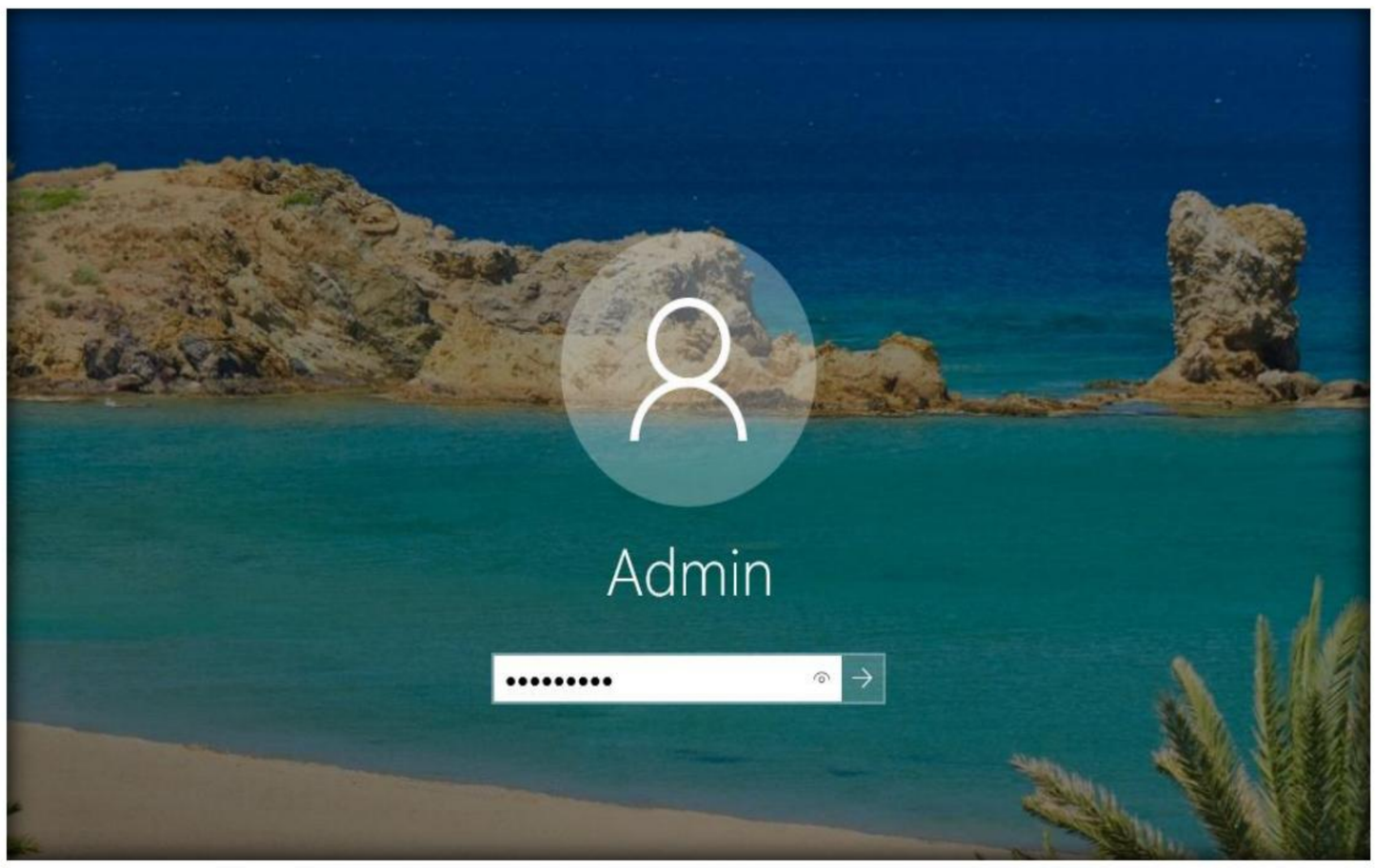


FIGURE 4.9.1: Launch Admin Machine and Log in

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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**.

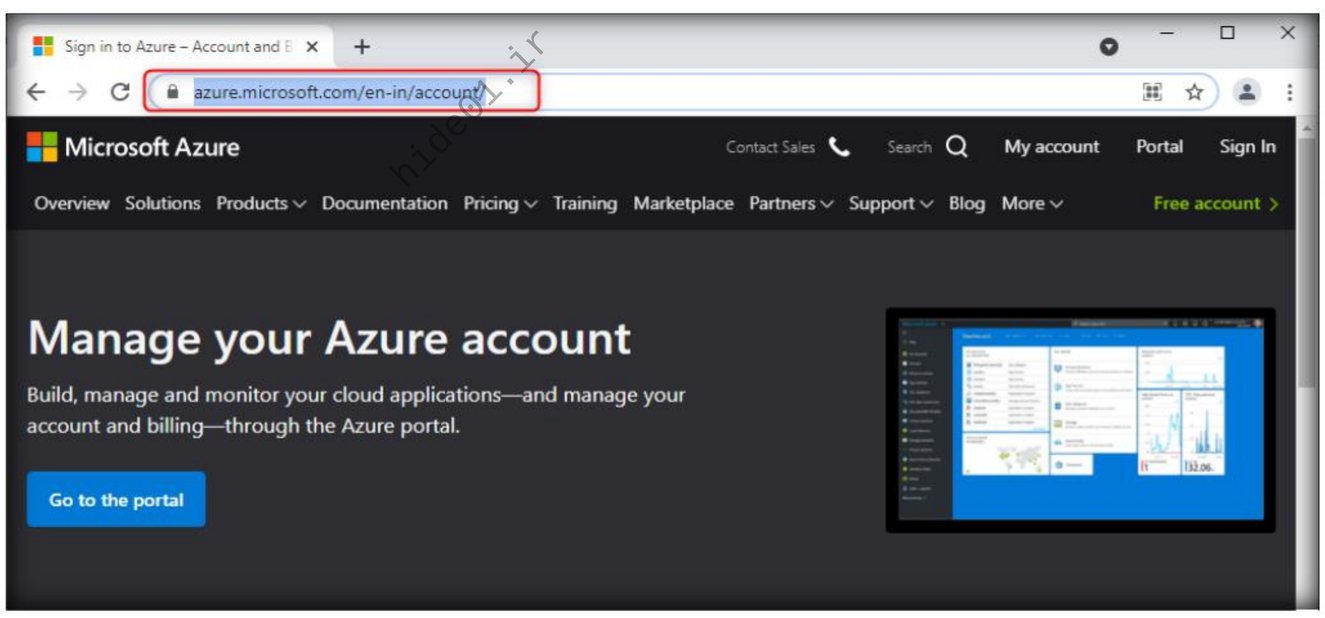


FIGURE 4.9.3: Entering the URL of Microsoft Azure

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

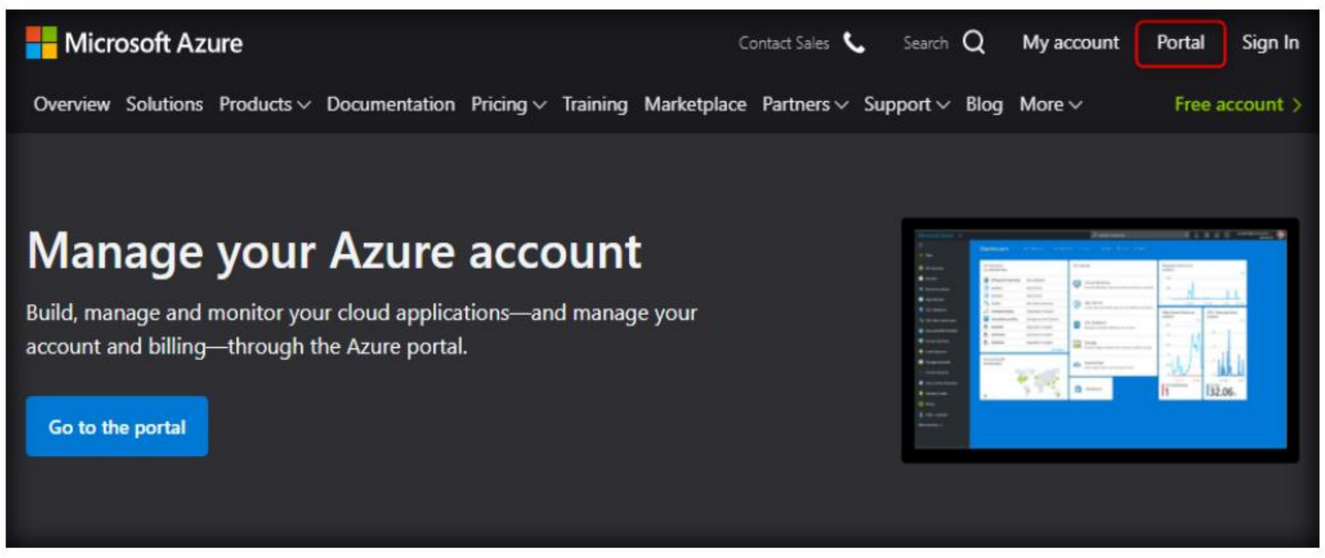


FIGURE 4.9.4: Sign into Azure Portal

Certified Cloud Security Engineer Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

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

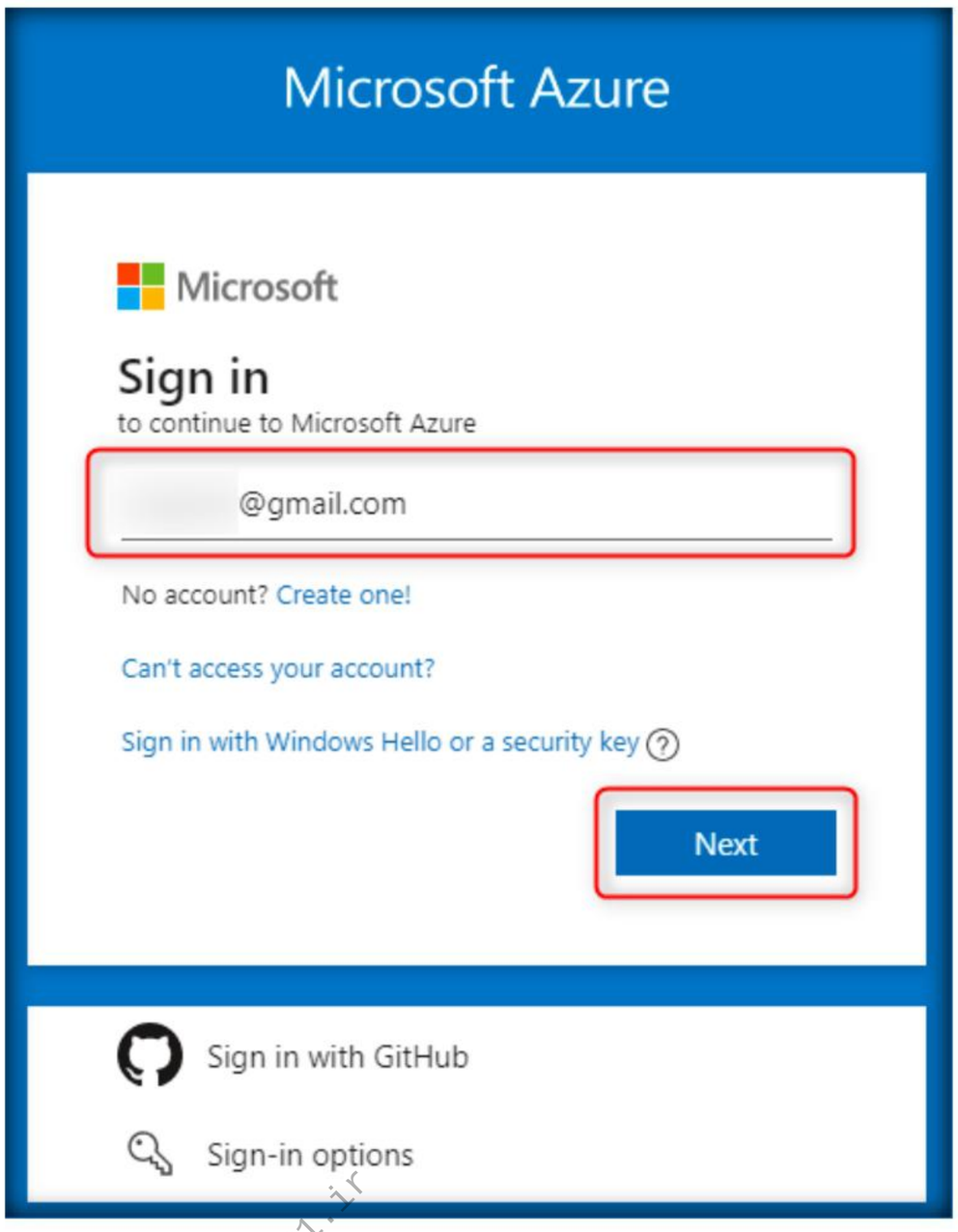


FIGURE 4.9.5: Entering Account ID to continue

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

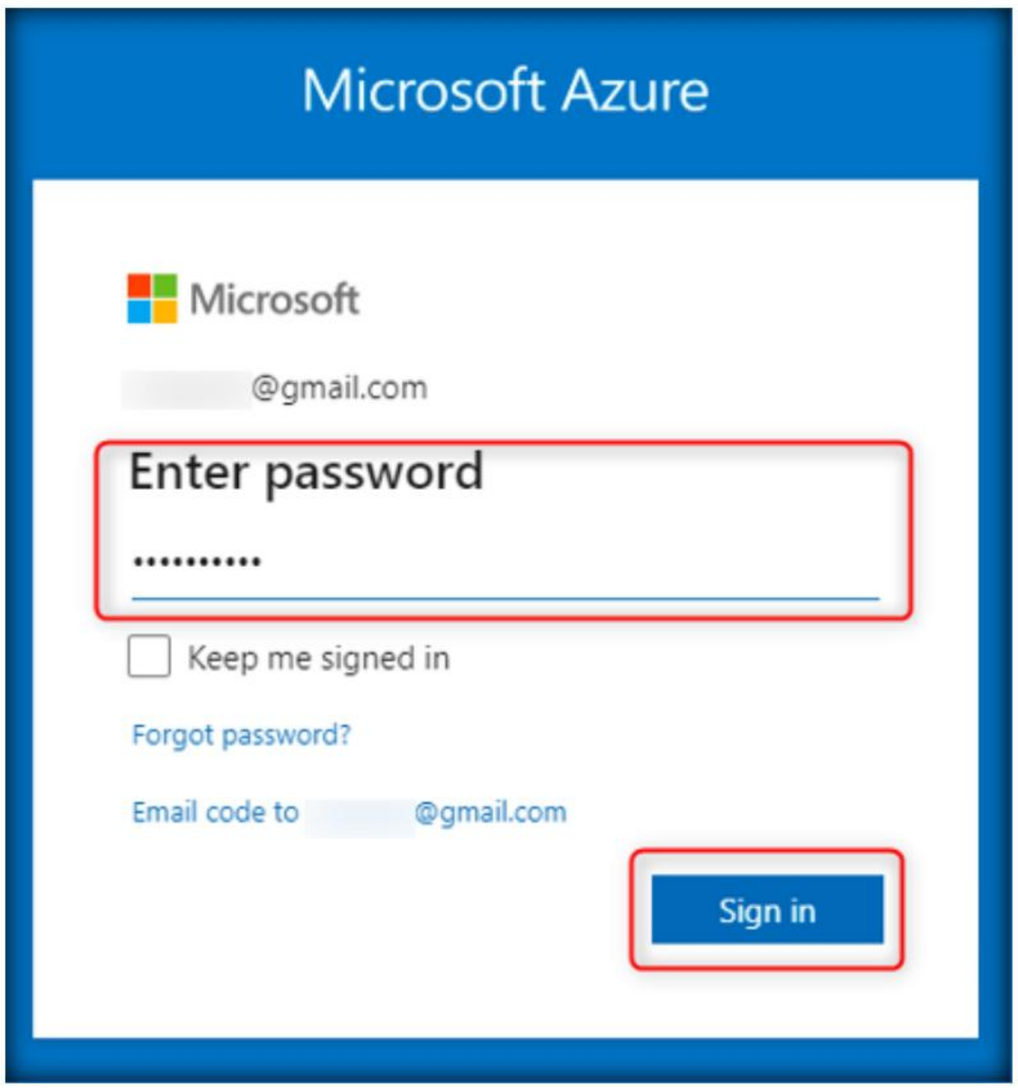


FIGURE 4.9.6: Sign in to Azure Account

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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

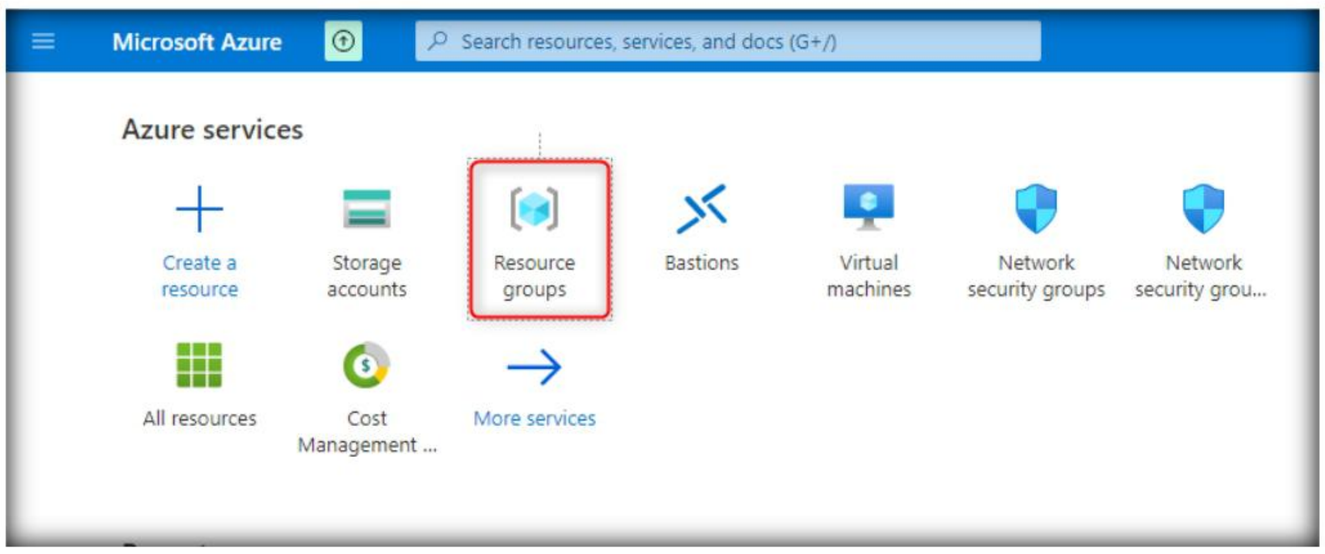


FIGURE 4.9.7: Selecting Resource Groups

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

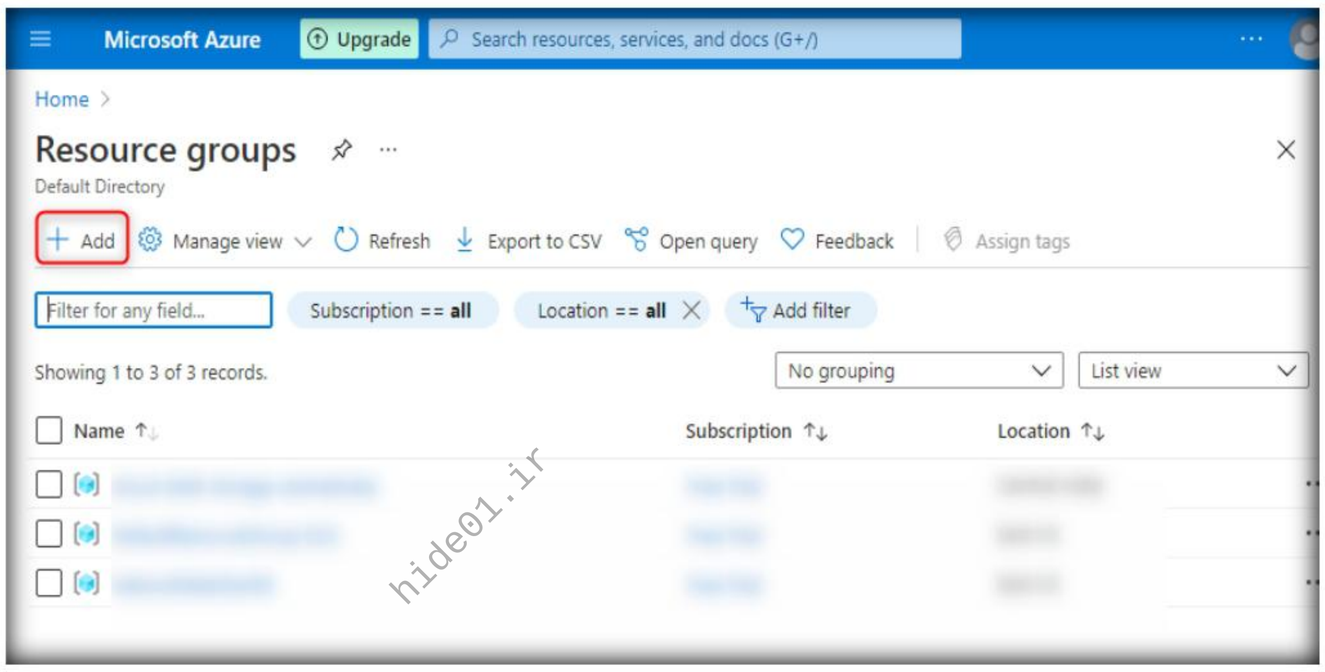


FIGURE 4.9.8: Adding New Resource Group

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.

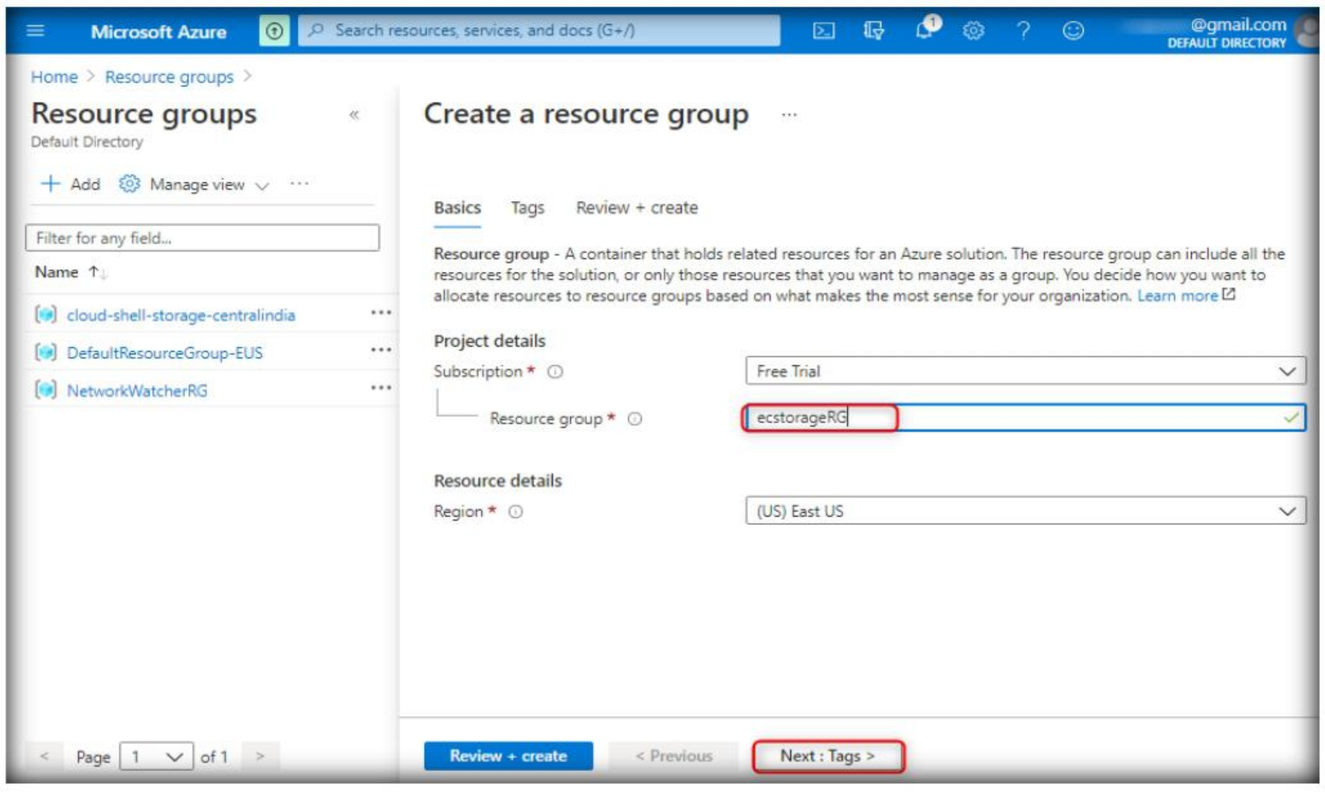


FIGURE 4.9.9: Entering Resource Group Name and Location

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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

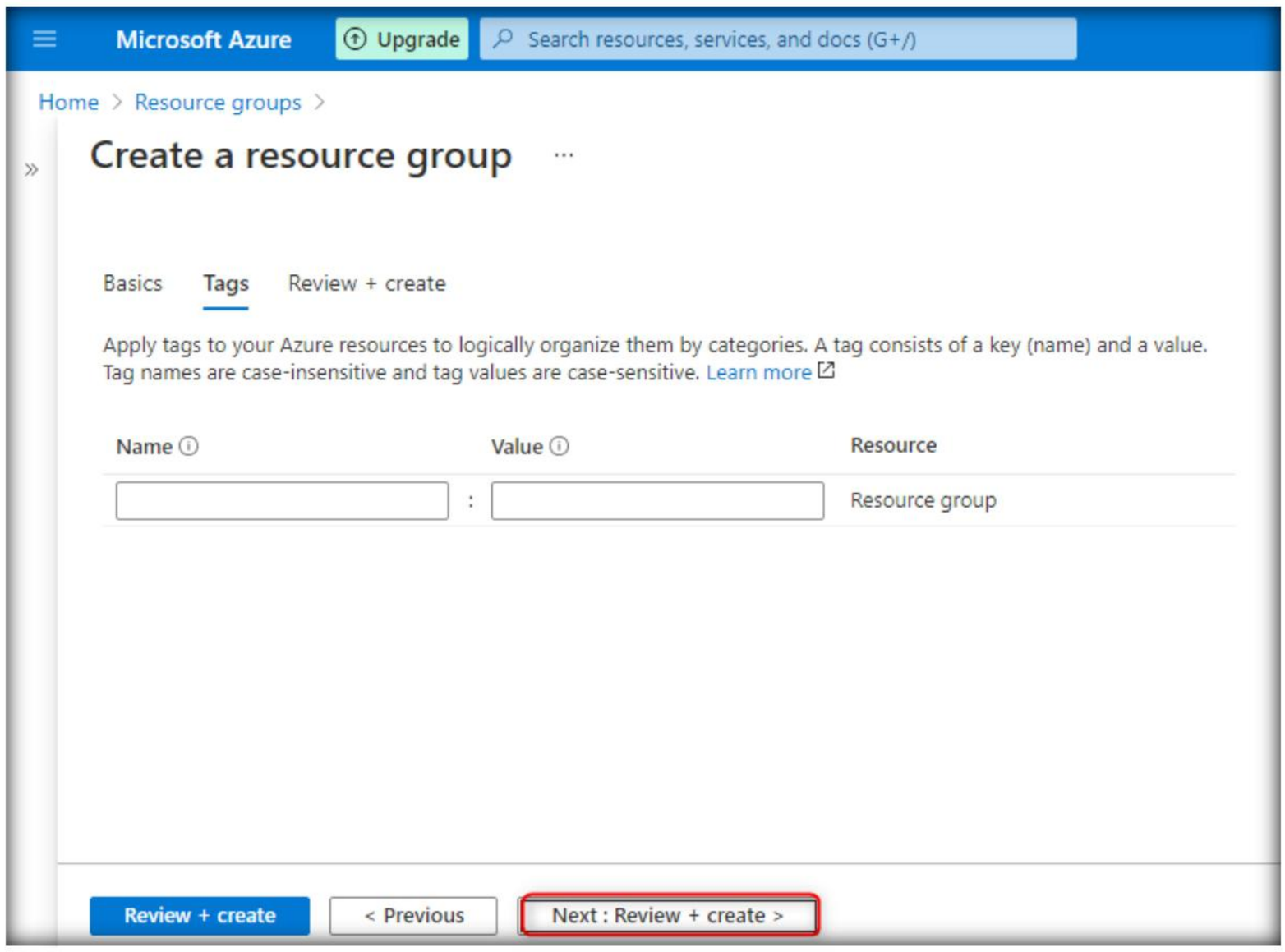


FIGURE 4.9.10: Reviewing and Creating Resource Group

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

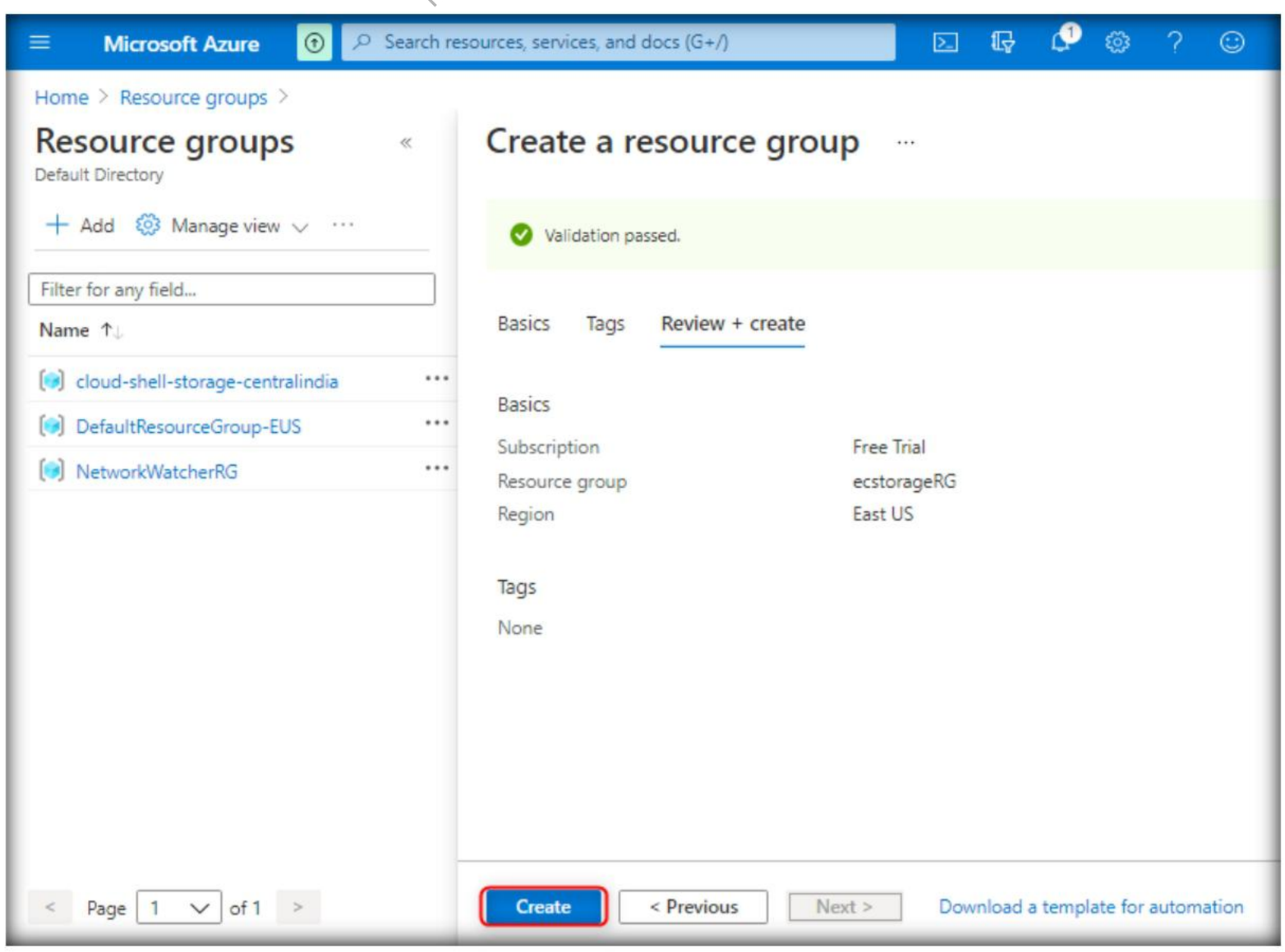


FIGURE 4.9.11: Validation Passed for Creating a Resource Group

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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

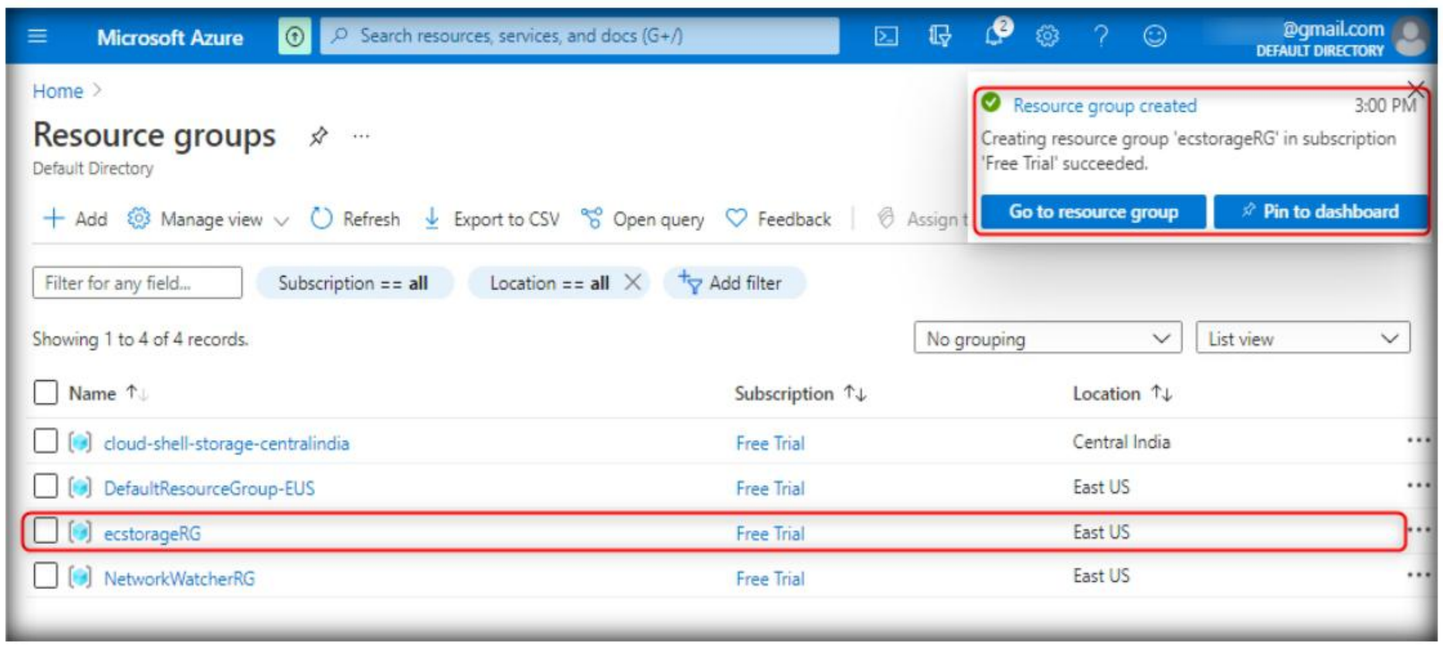


FIGURE 4.9.12: Successfully Creating Resource Group

TASK 2

Creating a Storage Account in the Resource Group

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

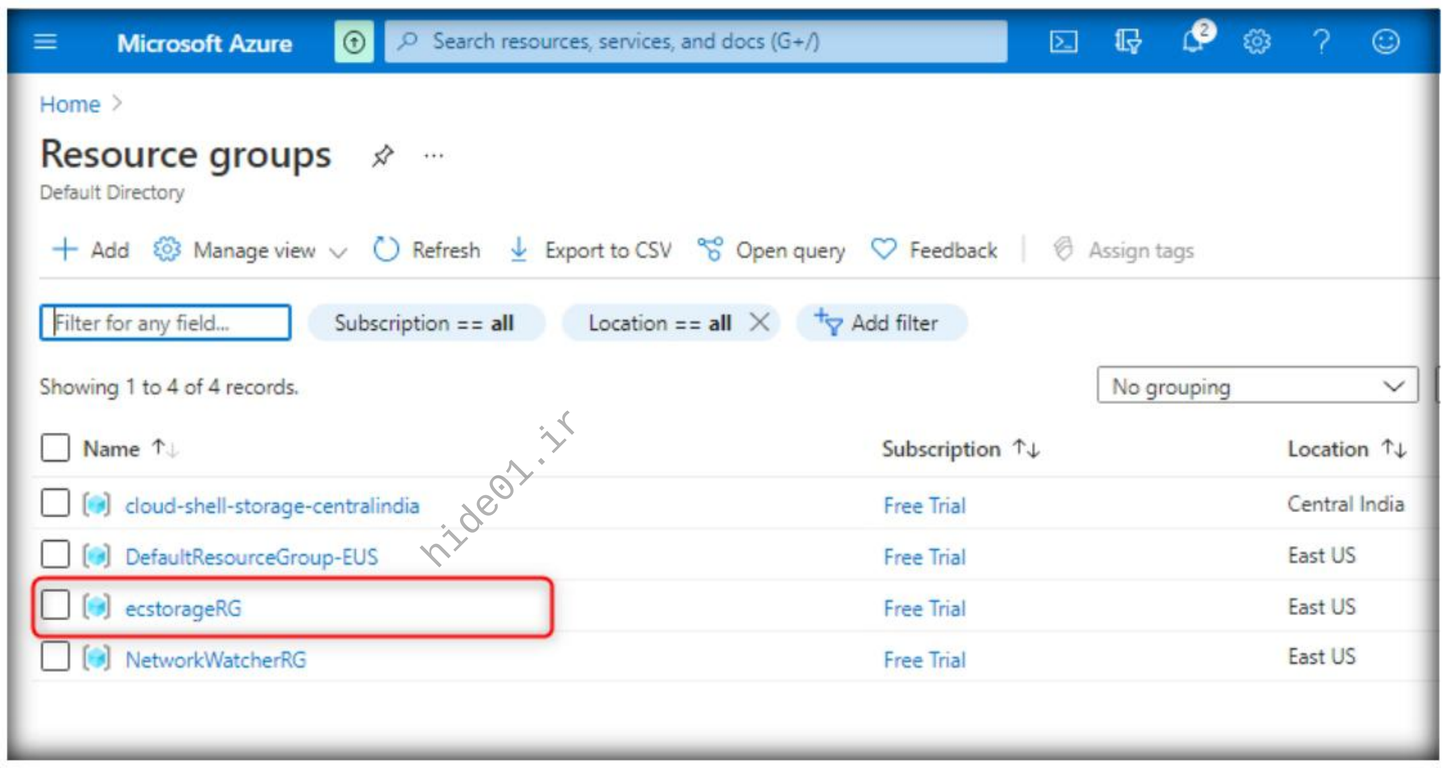


FIGURE 4.9.13: Selecting Resource Group

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

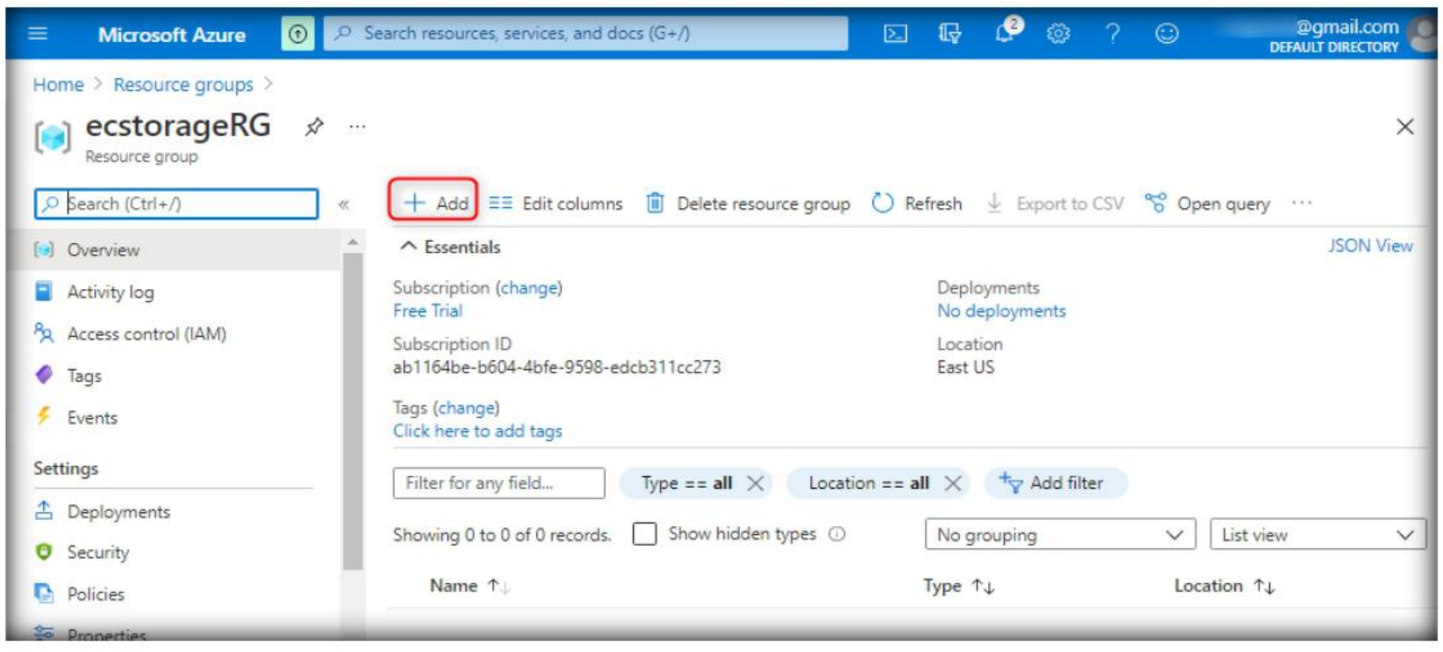


FIGURE 4.9.14: Creating a New Storage Account

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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

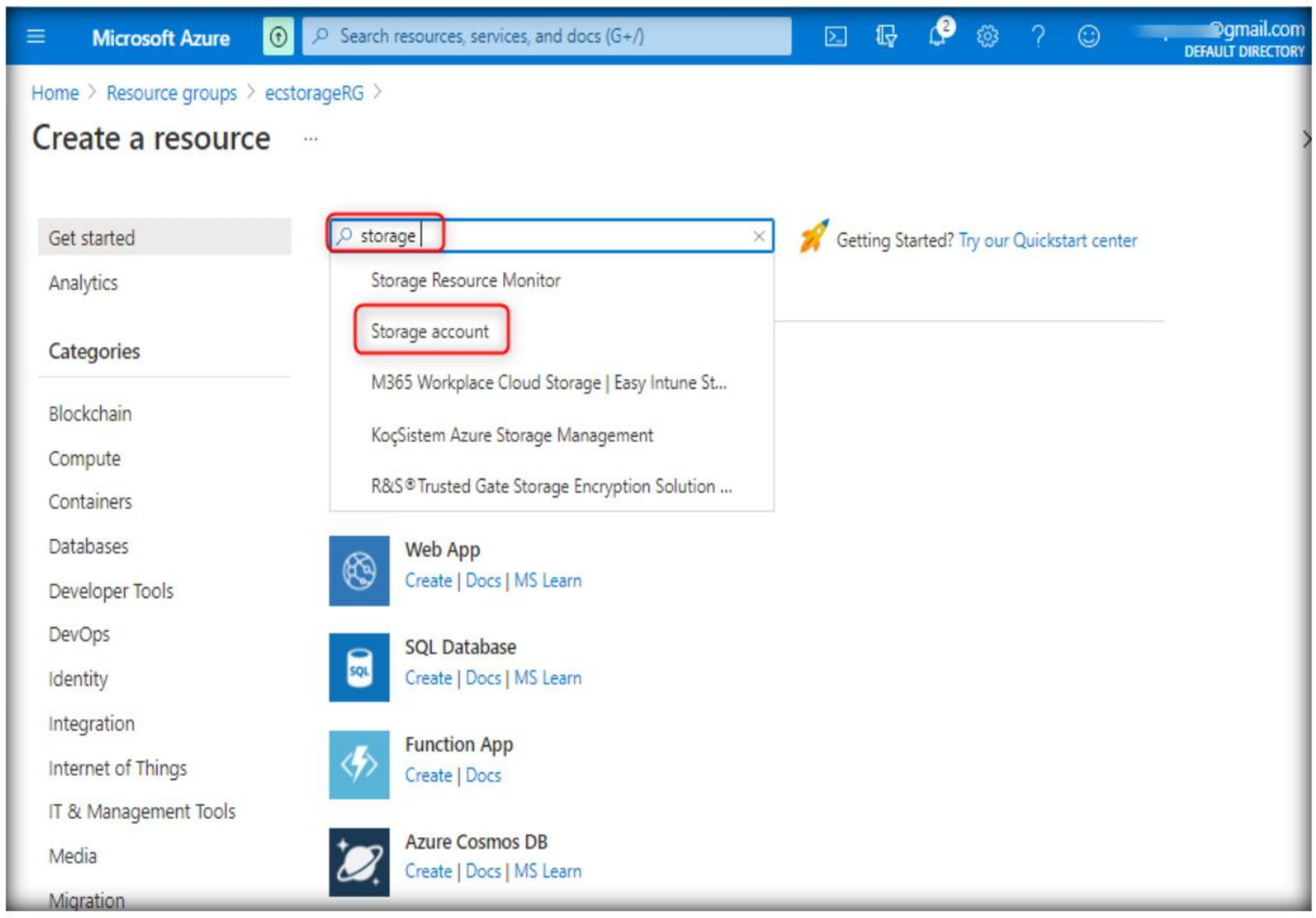


FIGURE 4.9.15: Searching and Selecting Storage Account

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

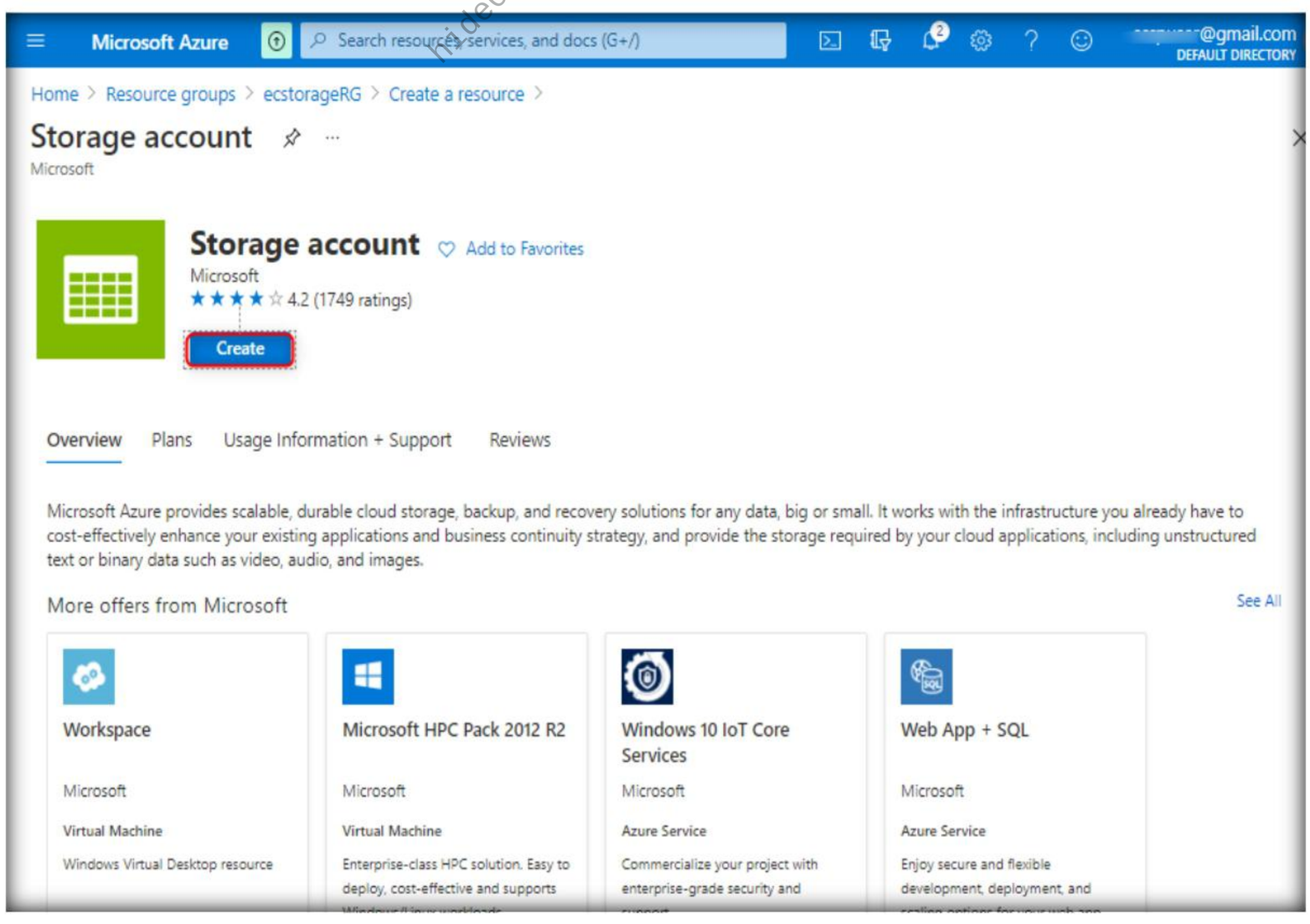


FIGURE 4.9.16: Creating a Storage Account

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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

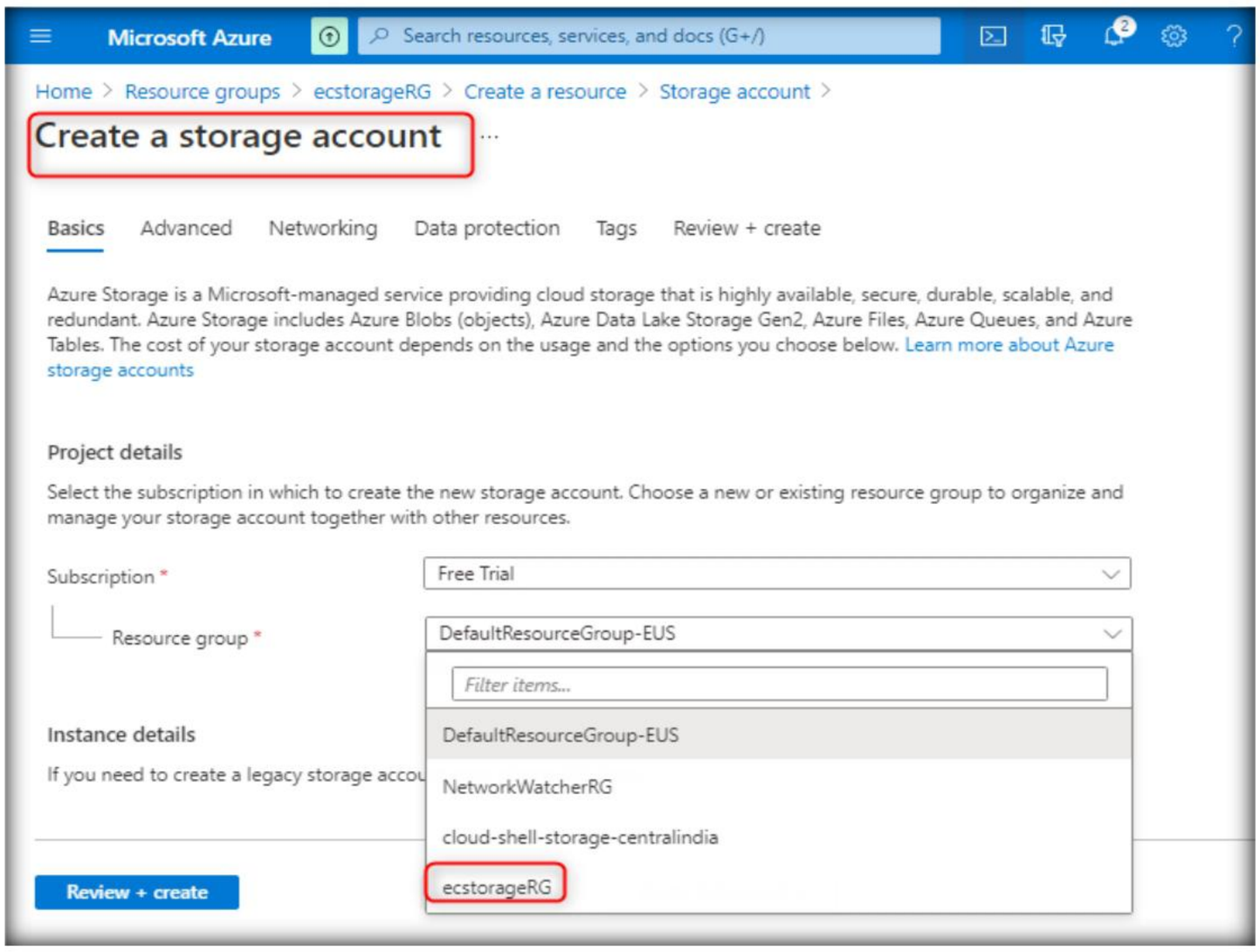


FIGURE 4.9.17: Selecting Resource Group for Storage Account

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.

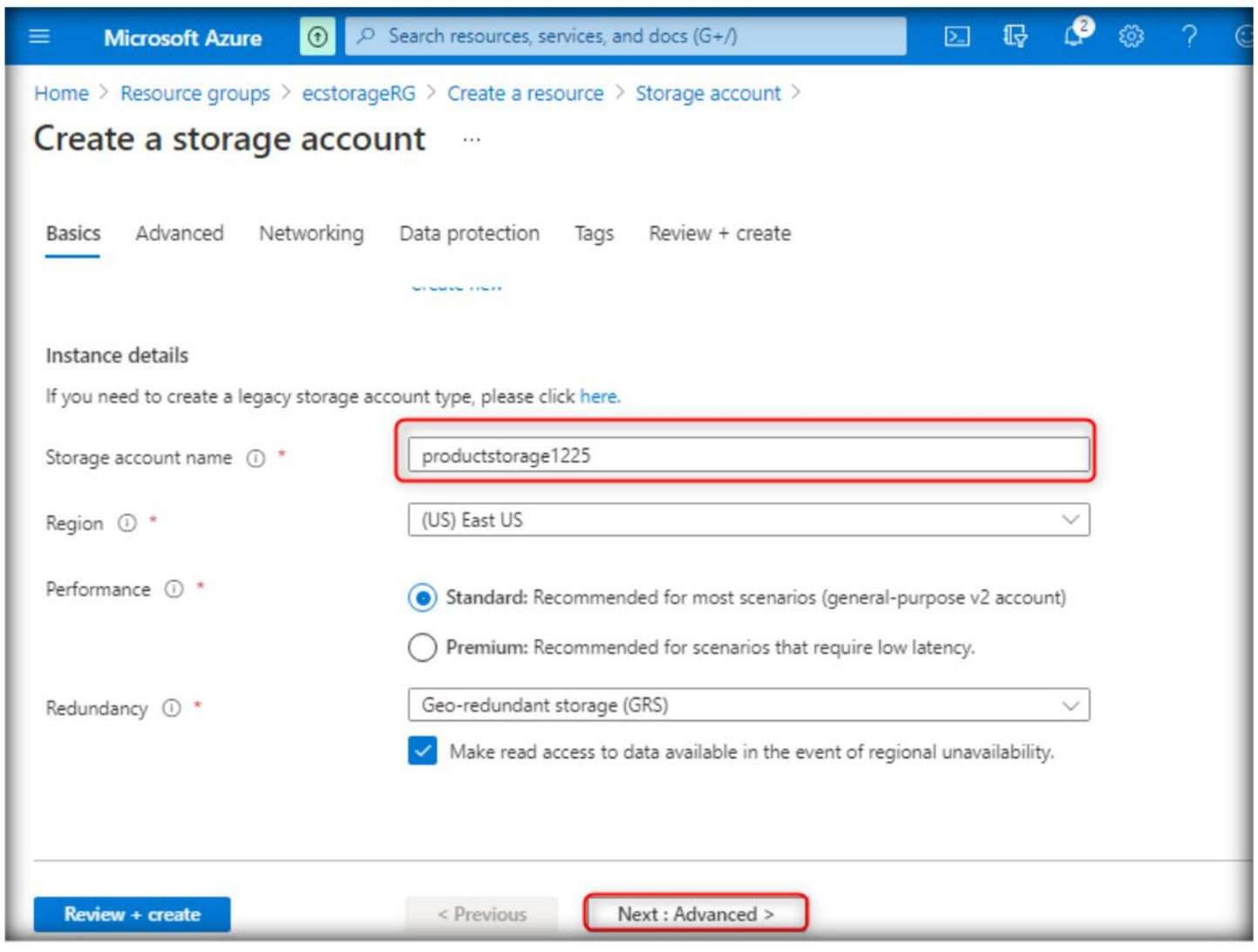


FIGURE 4.9.18: Entering the Name of the Storage Account

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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

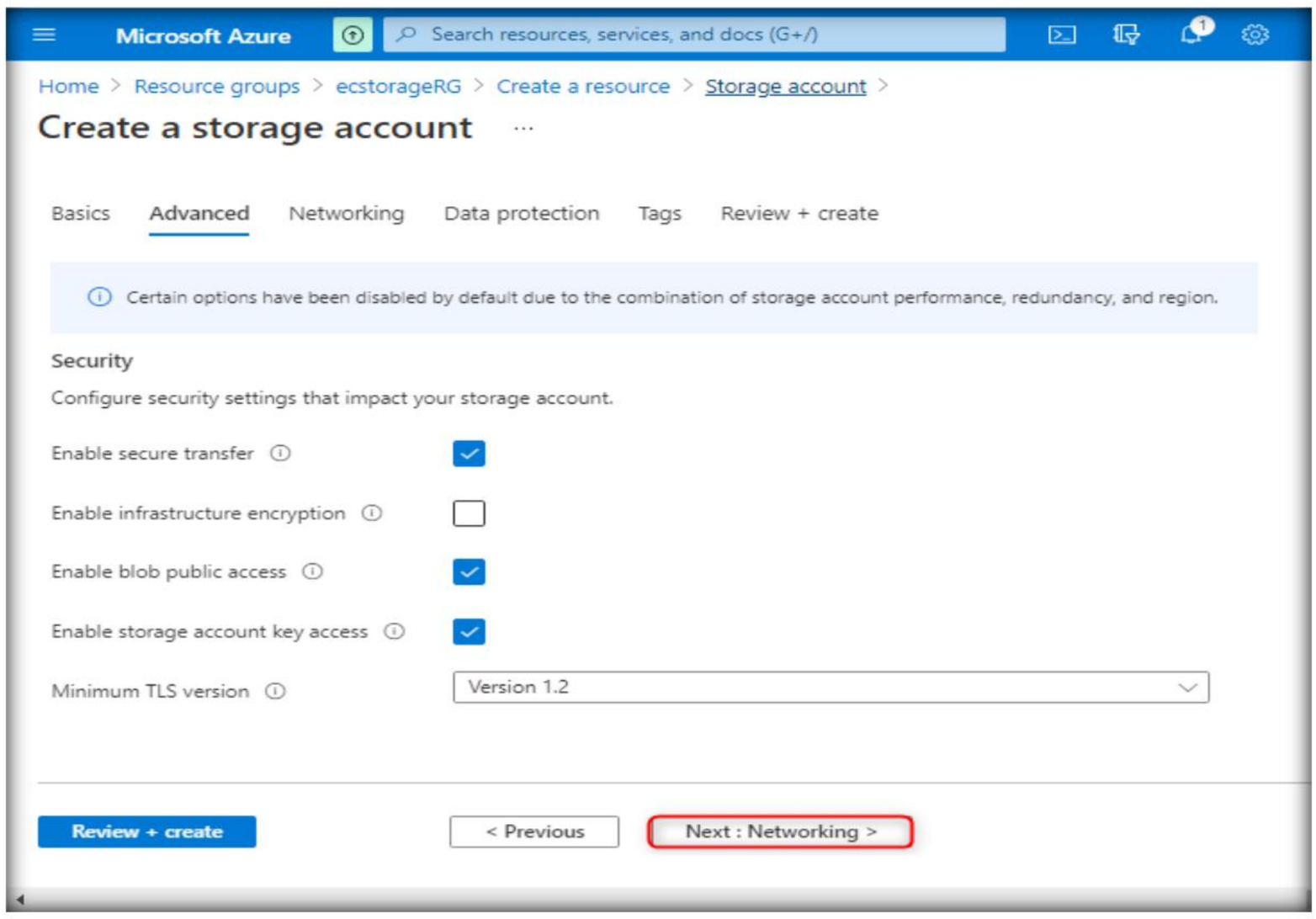


FIGURE 4.9.19: Leaving Everything in Default State in Advanced Tab

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

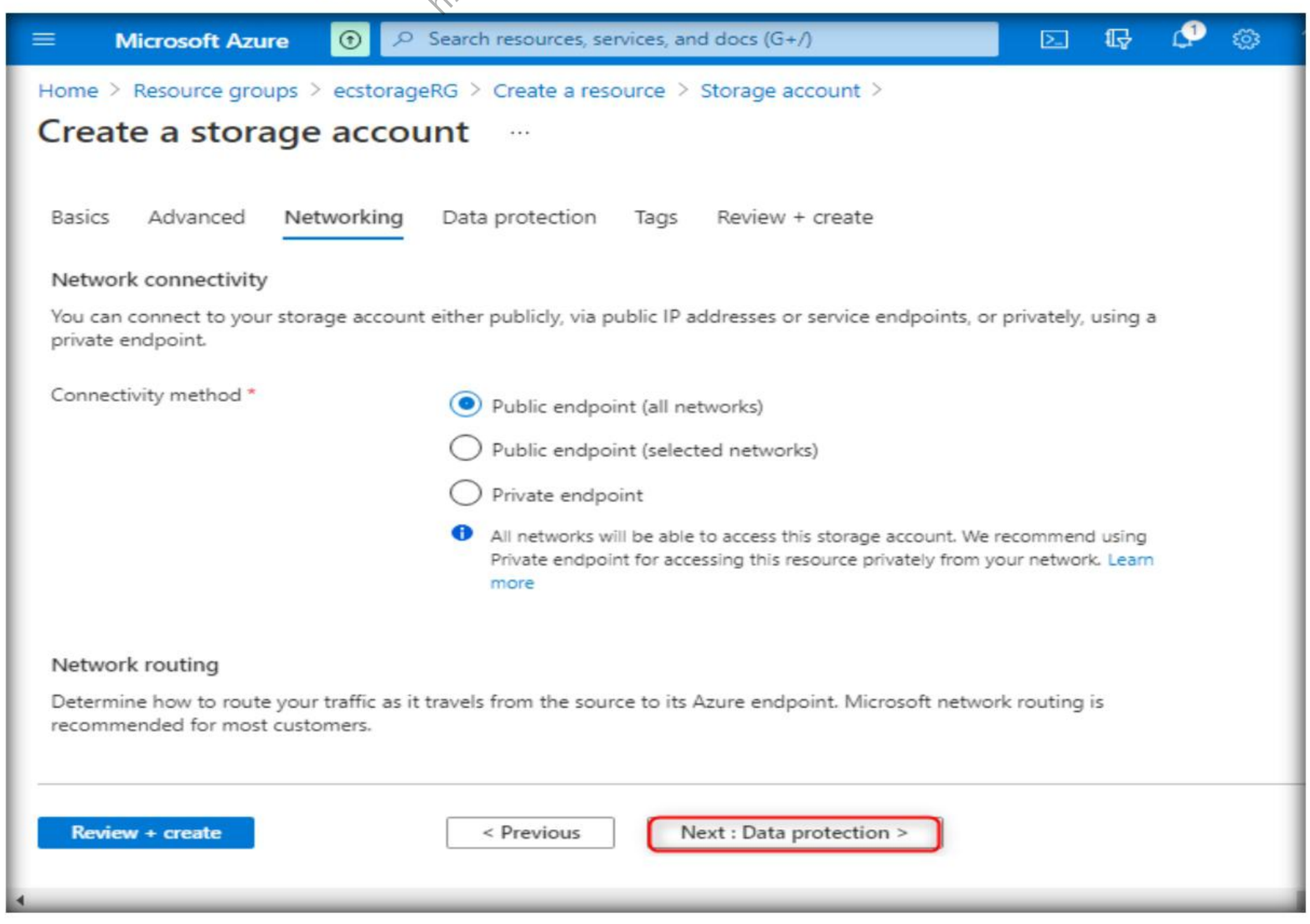


FIGURE 4.9.20: Leaving Everything in Default State in Networking Tab

Certified Cloud Security Engineer Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

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

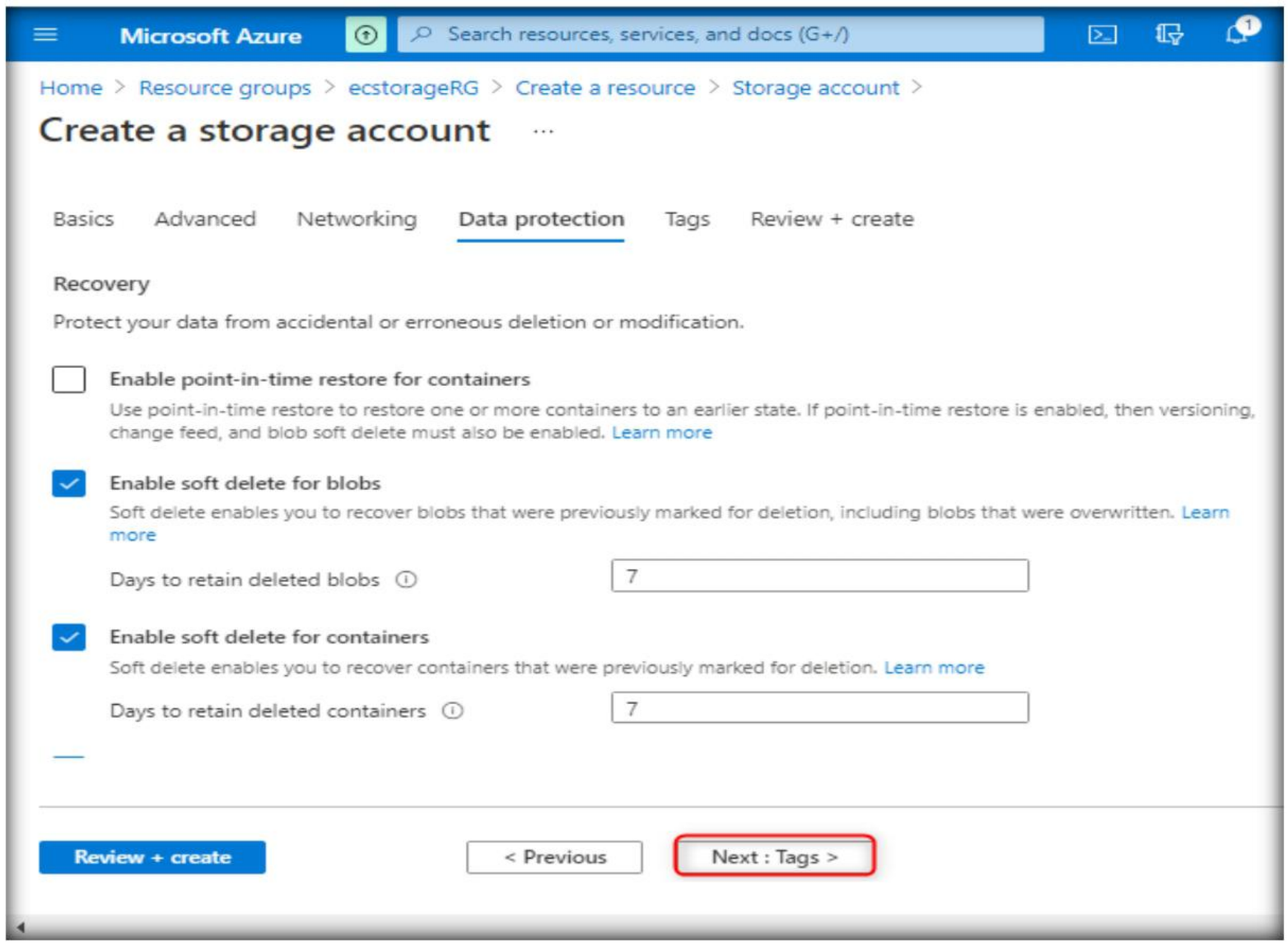


FIGURE 4.9.21: Leaving Everything in Default State in Data Protection Tab

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

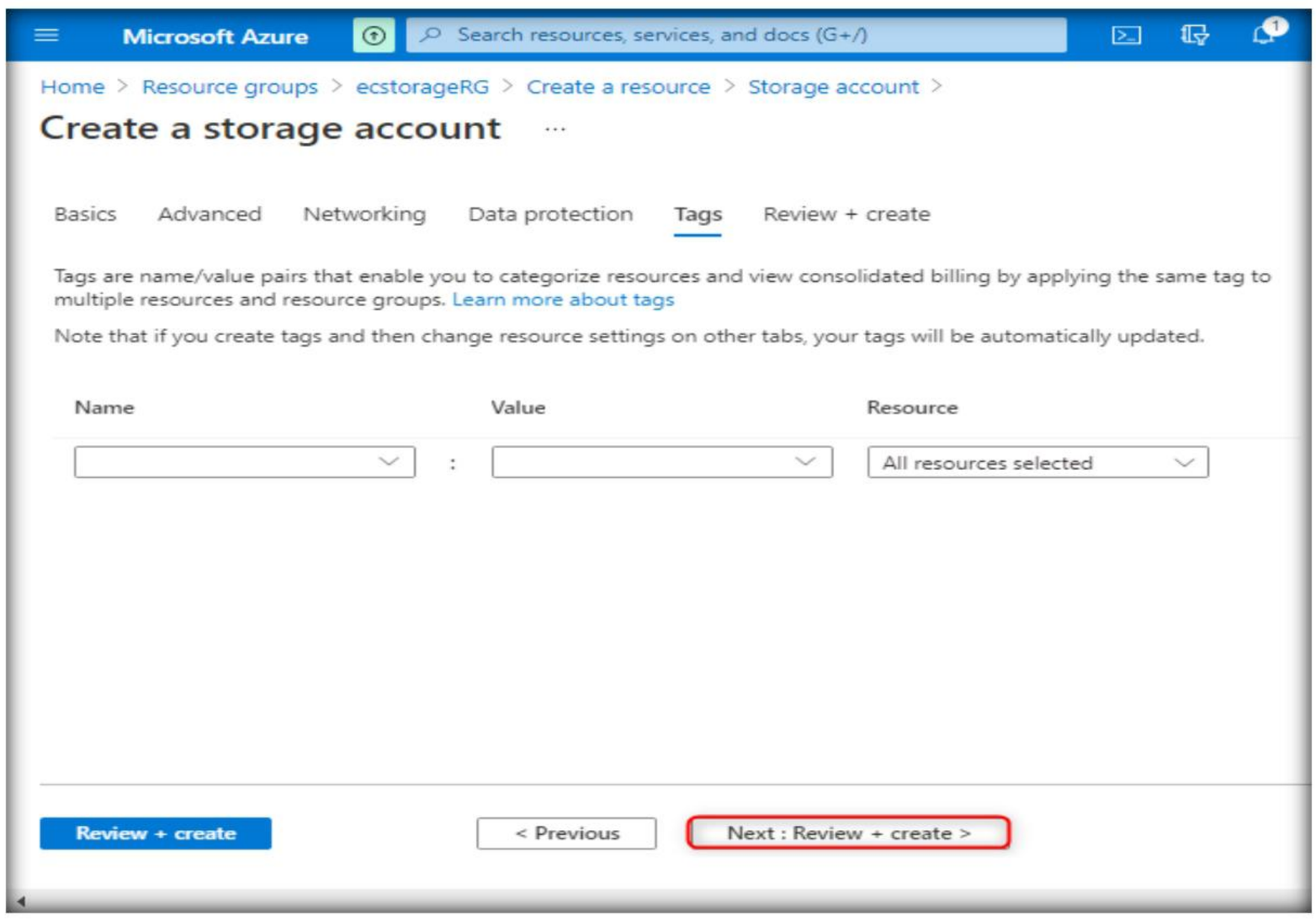


FIGURE 4.9.22: Leaving Everything in Default State in Tags Tab

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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

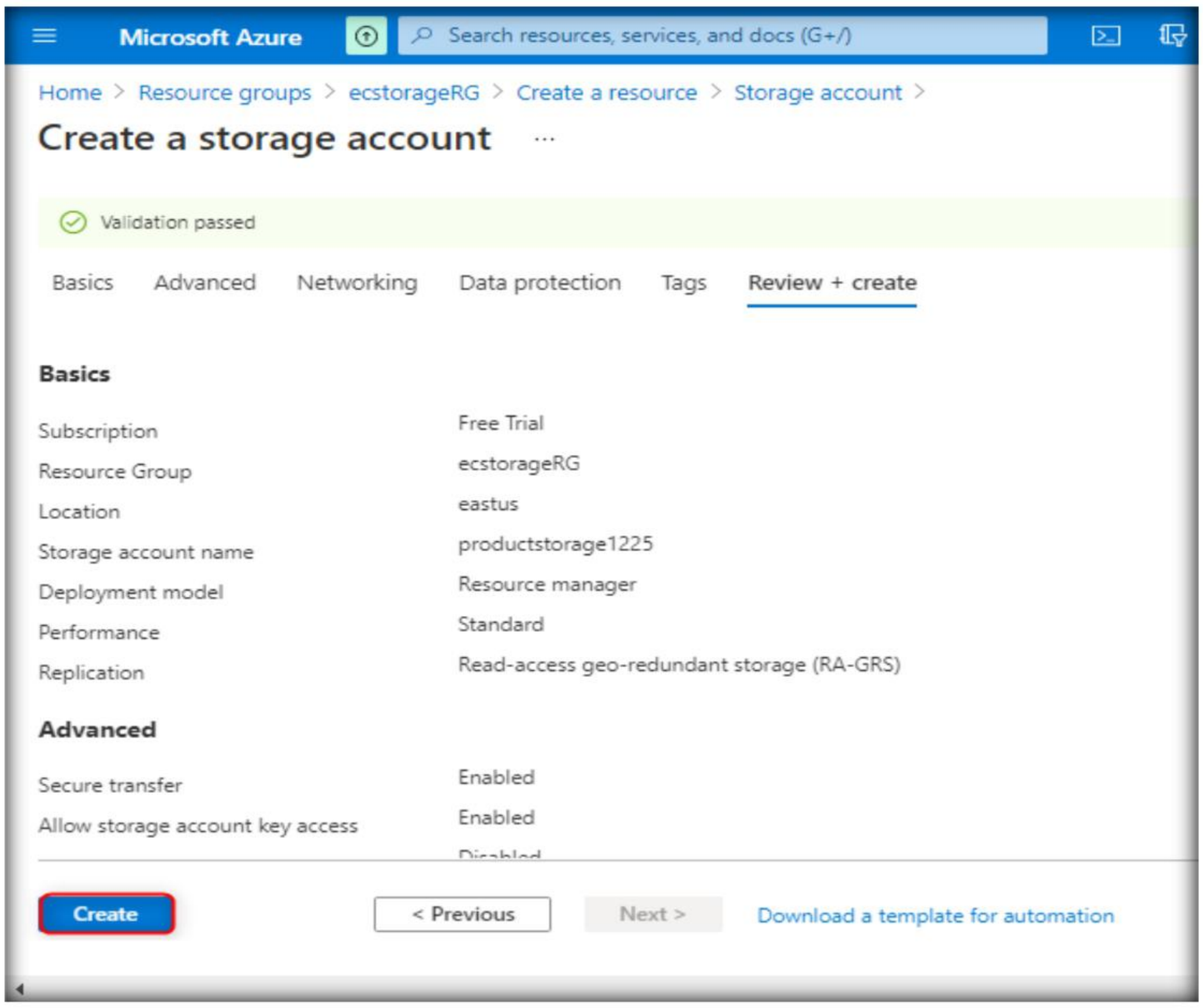


FIGURE 4.9.23: Passing the Validation

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

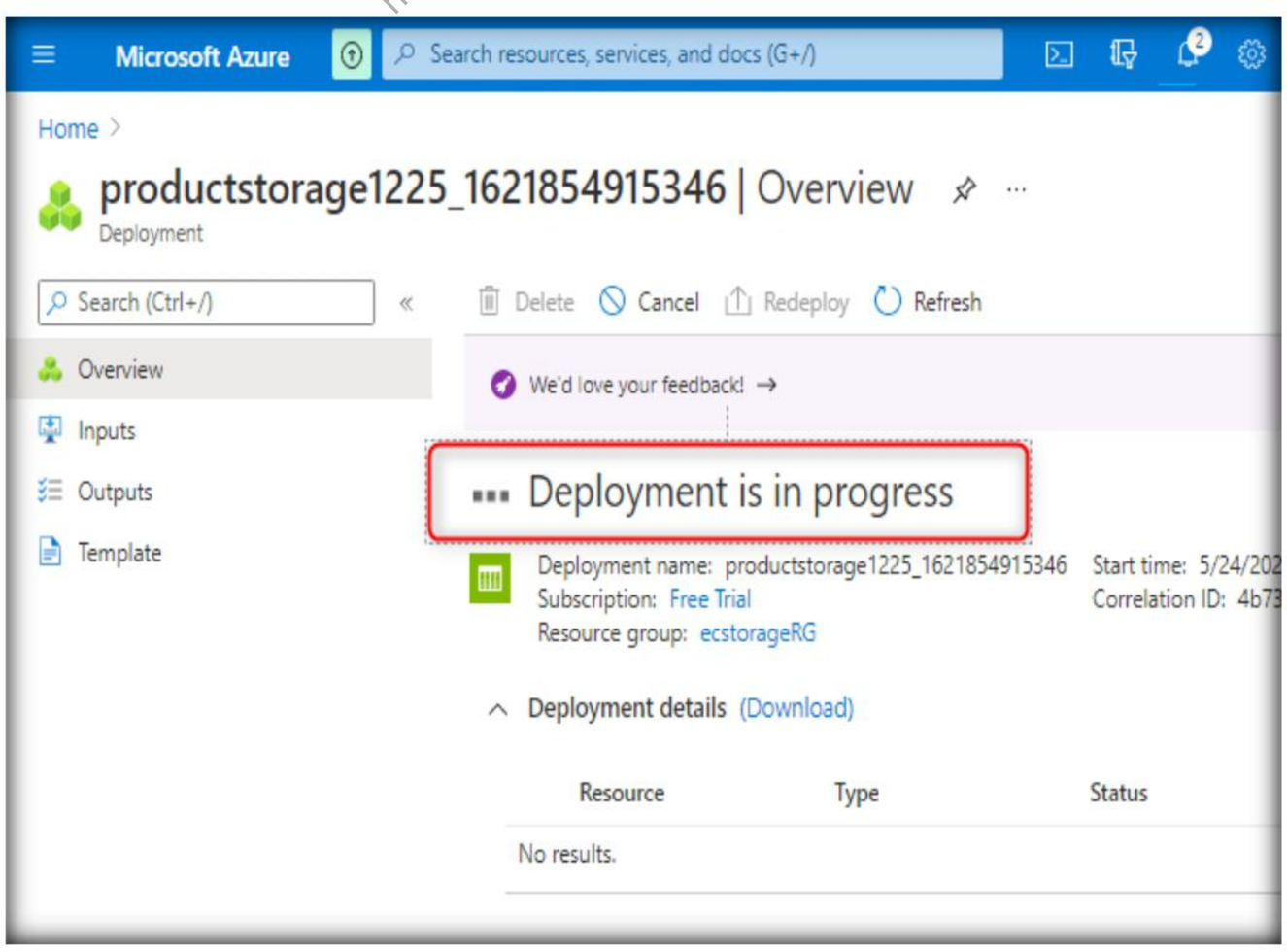


FIGURE 4.9.24: Storage Account Deployment Status

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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

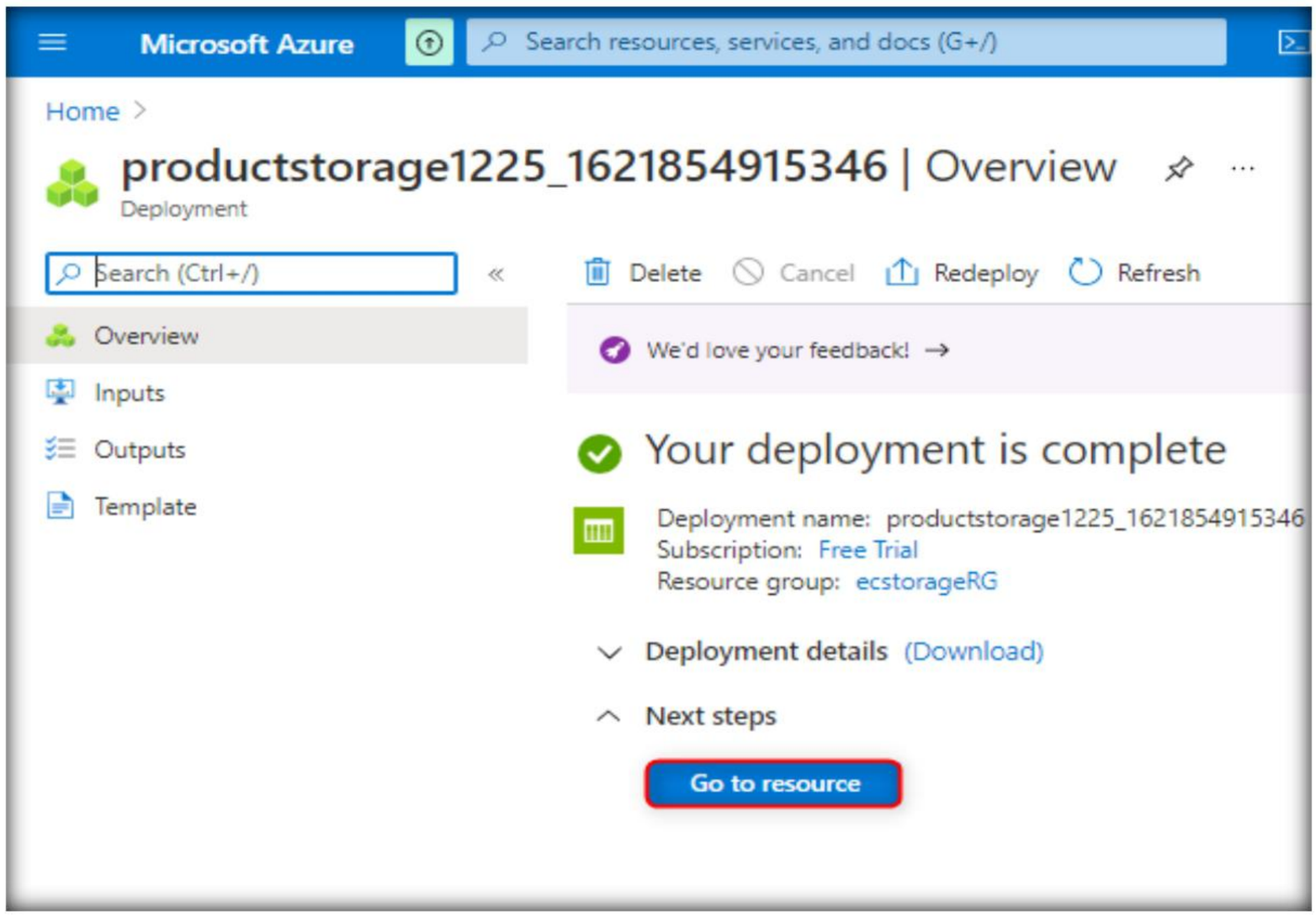


FIGURE 4.9.25: Successful Deployment of Storage Account

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

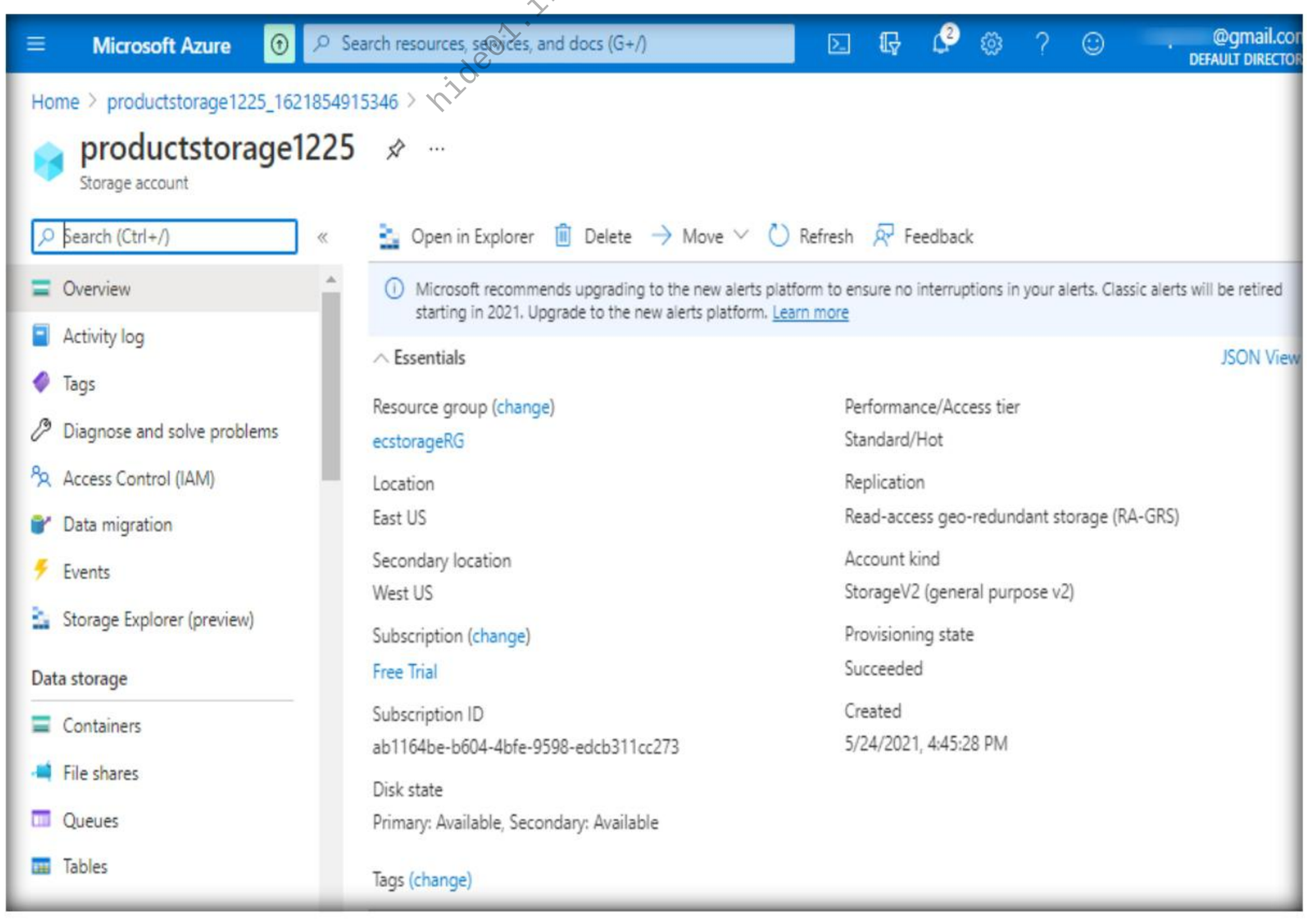


FIGURE 4.9.26: Successfully Creation of New Storage Account

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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**.

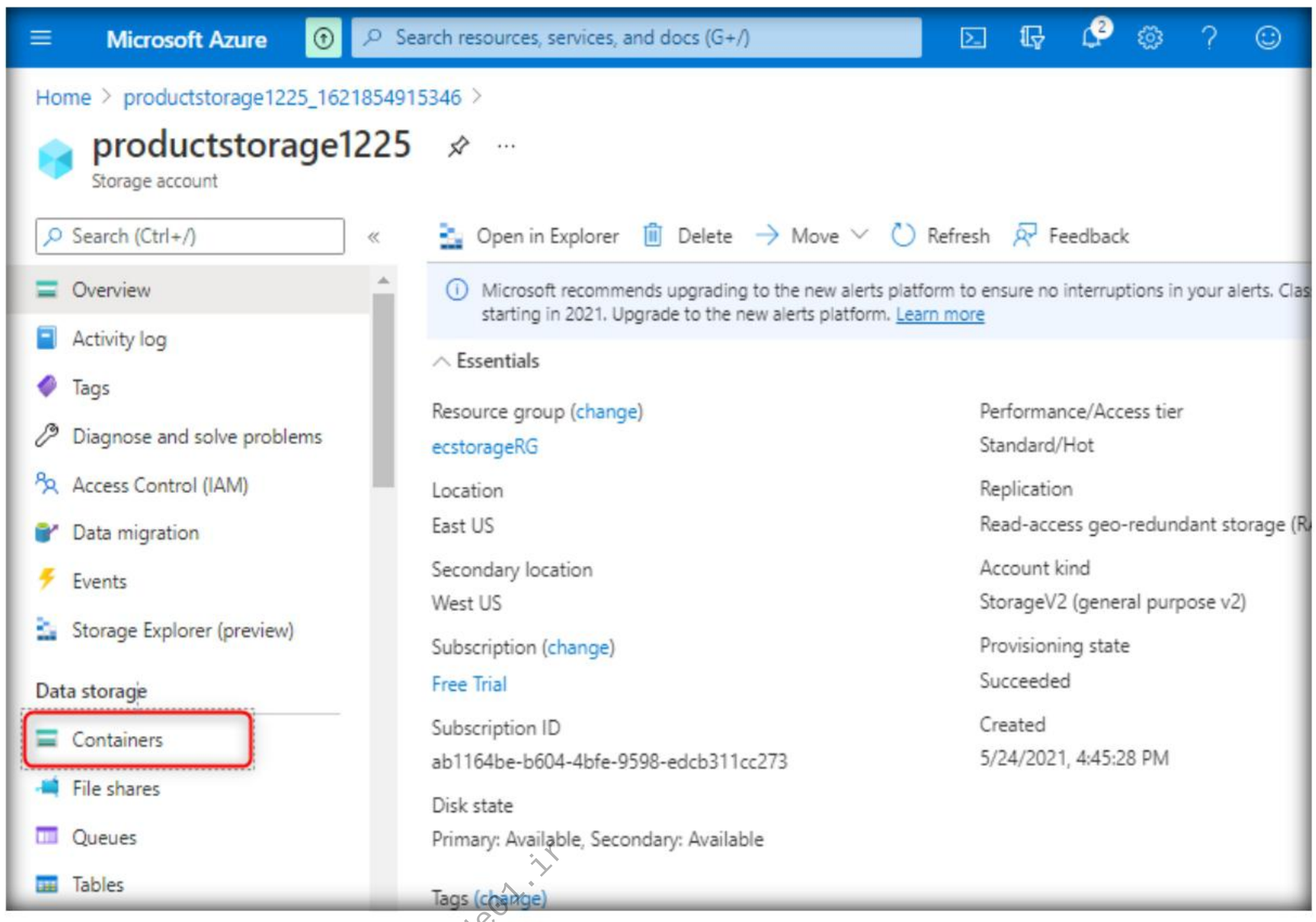


FIGURE 4.9.27: Selecting Containers in Storage Account

28. Click on **+ Container**.

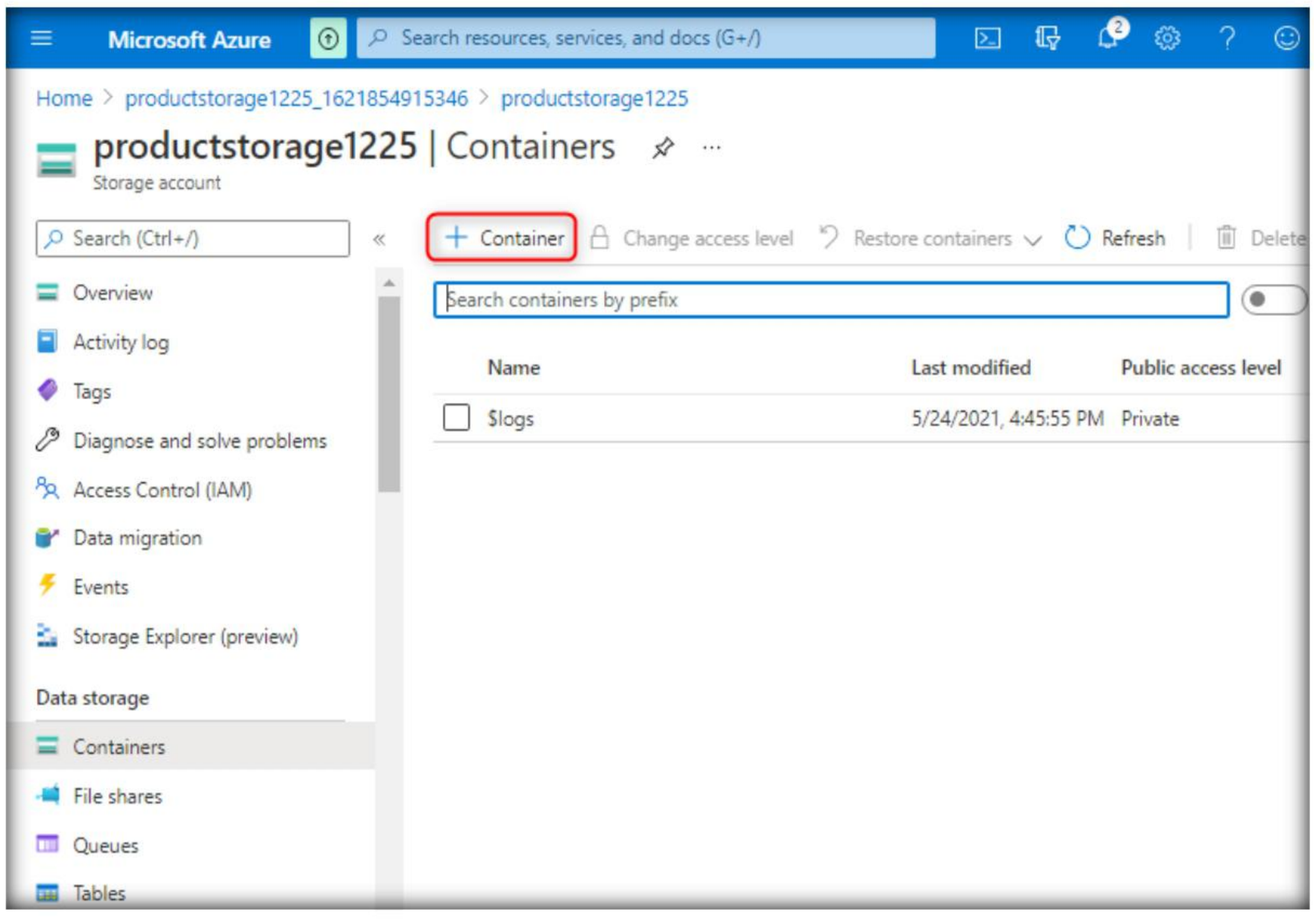


FIGURE 4.9.28: Creating a New Container

Certified Cloud Security Engineer Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

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.

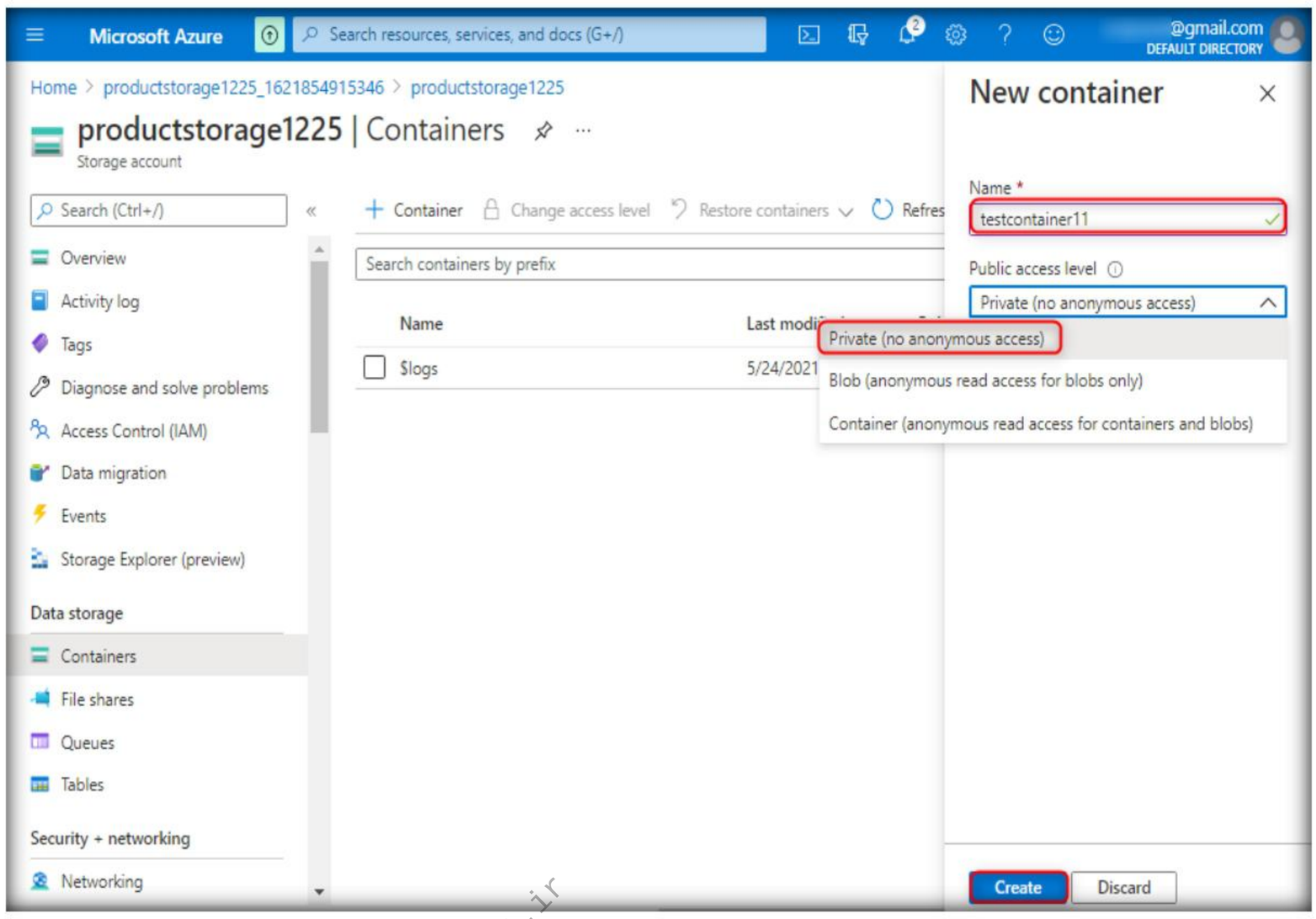


FIGURE 4.9.29: Filling Container Details in New Container Window

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

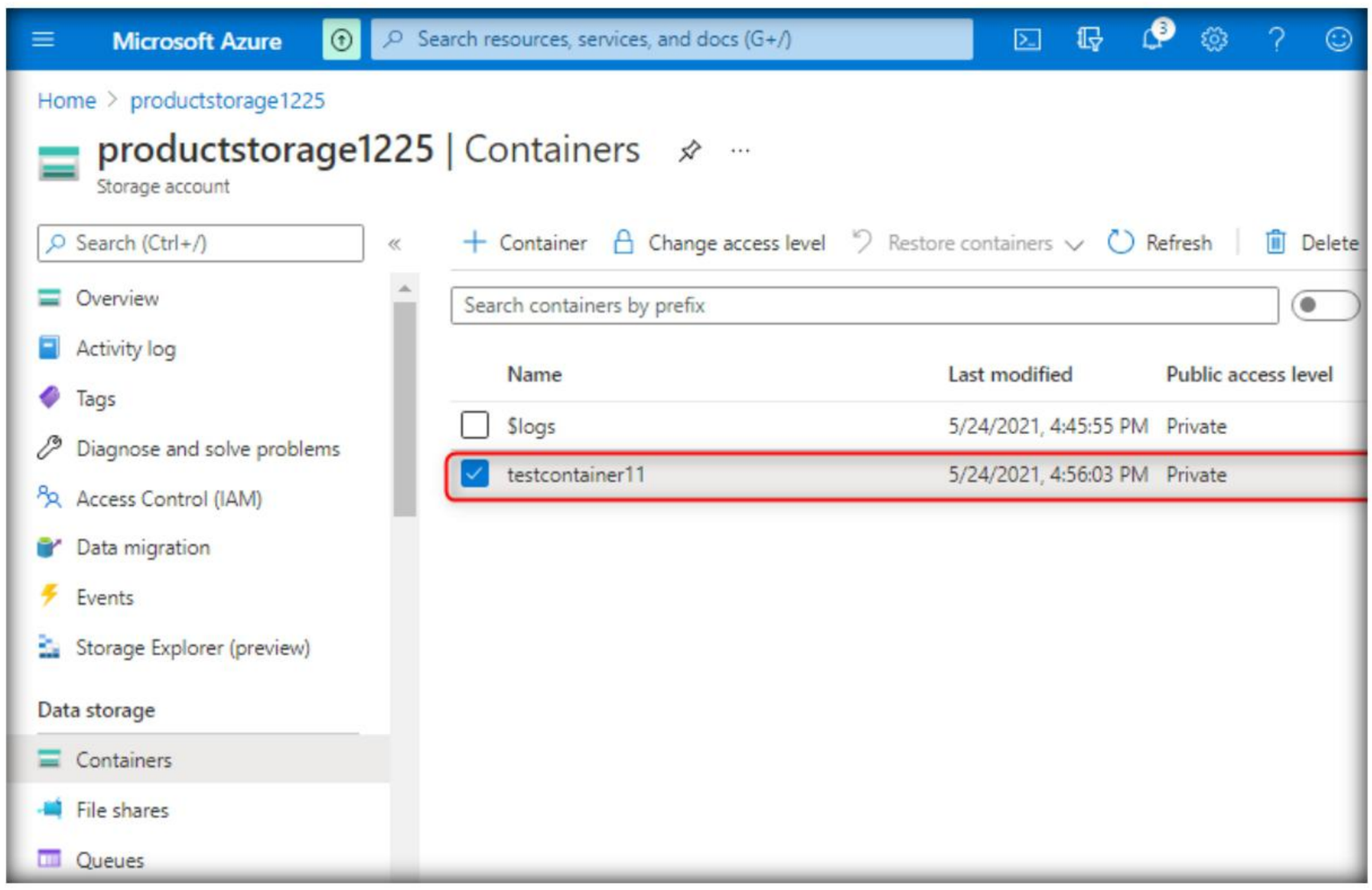


FIGURE 4.9.30: Successfully Creating Container with No Anonymous Access

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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.

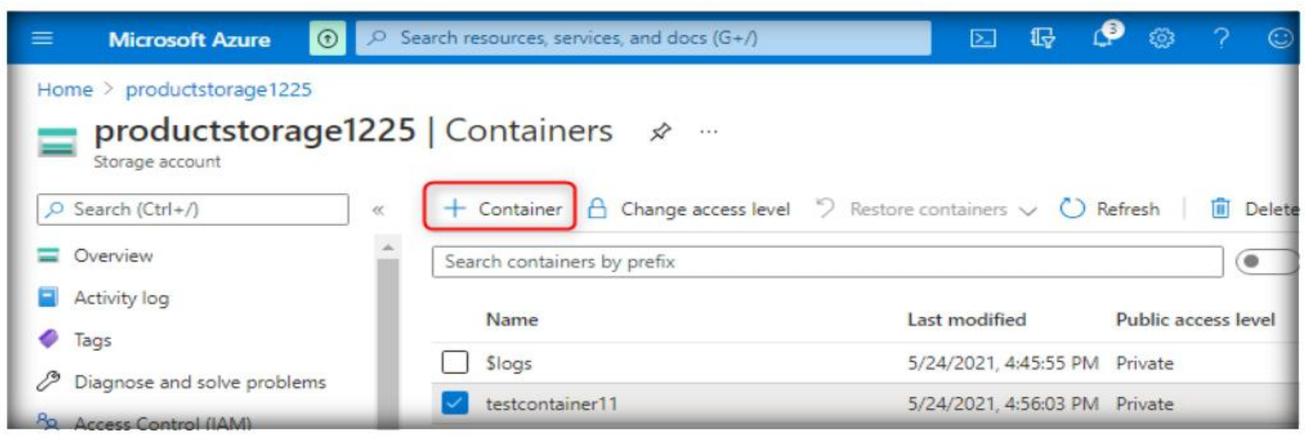


FIGURE 4.9.31: Creating a New Container

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)**.

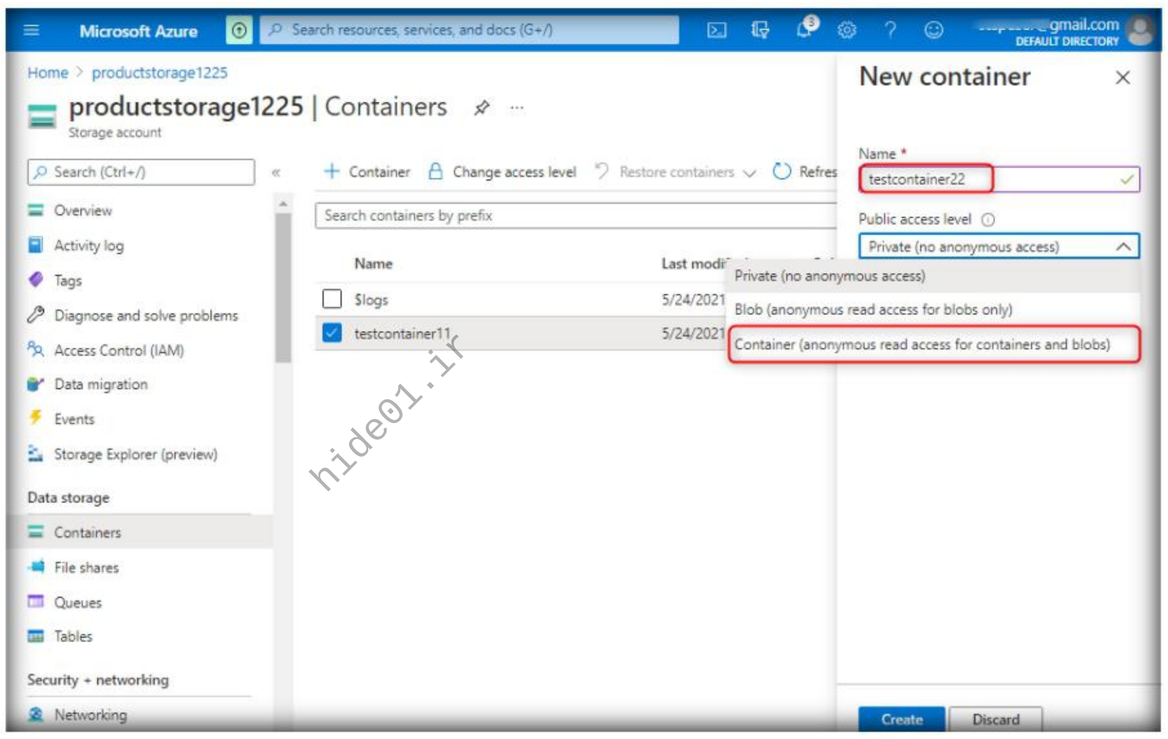


FIGURE 4.9.32: Entering Details in New Container Window

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

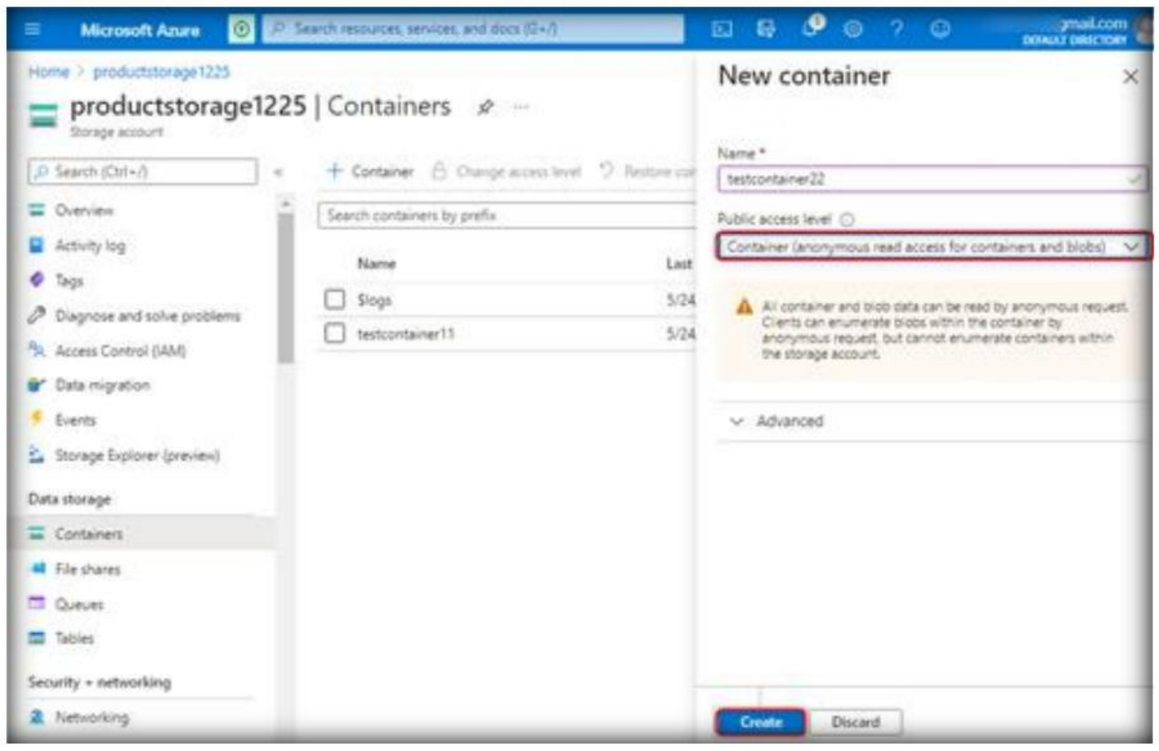


FIGURE 4.9.33: Creating Container with Anonymous Access

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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

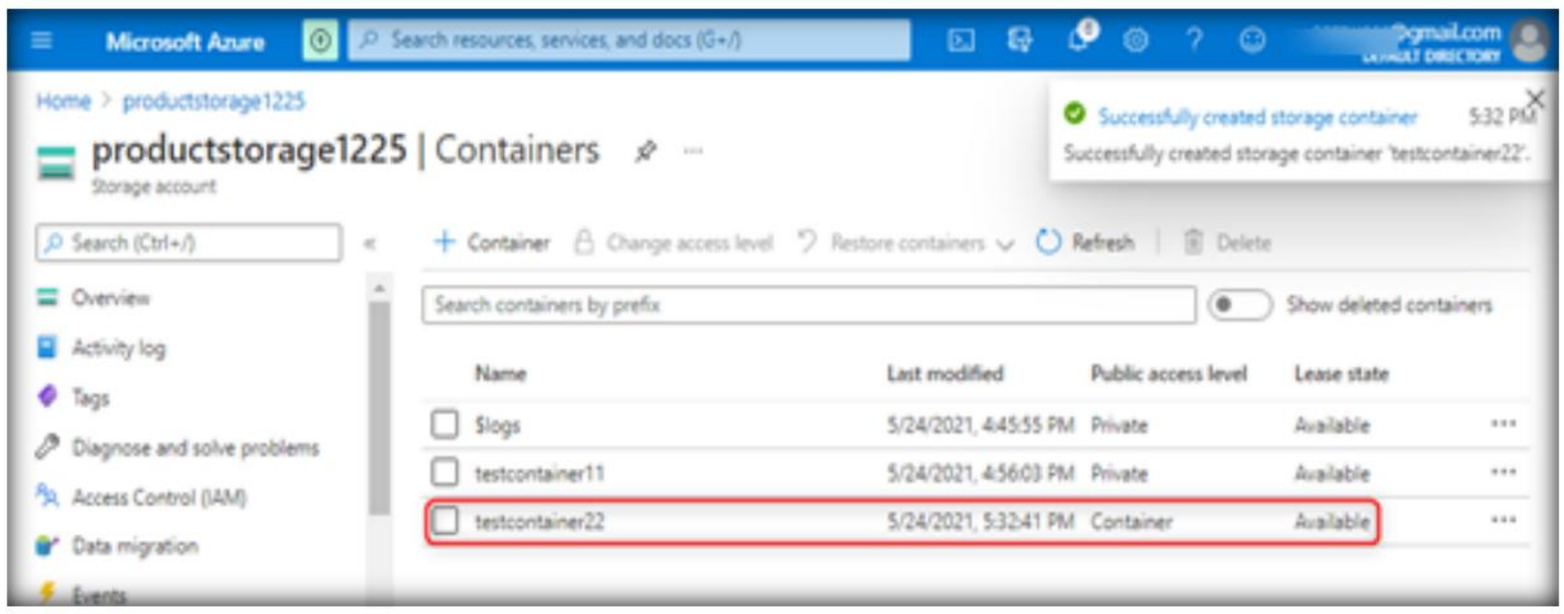


FIGURE 4.9.34: Successfully Created a Container Having Anonymous Read Access

TASK 5

Changing Access Level of the Container from Public to Private

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

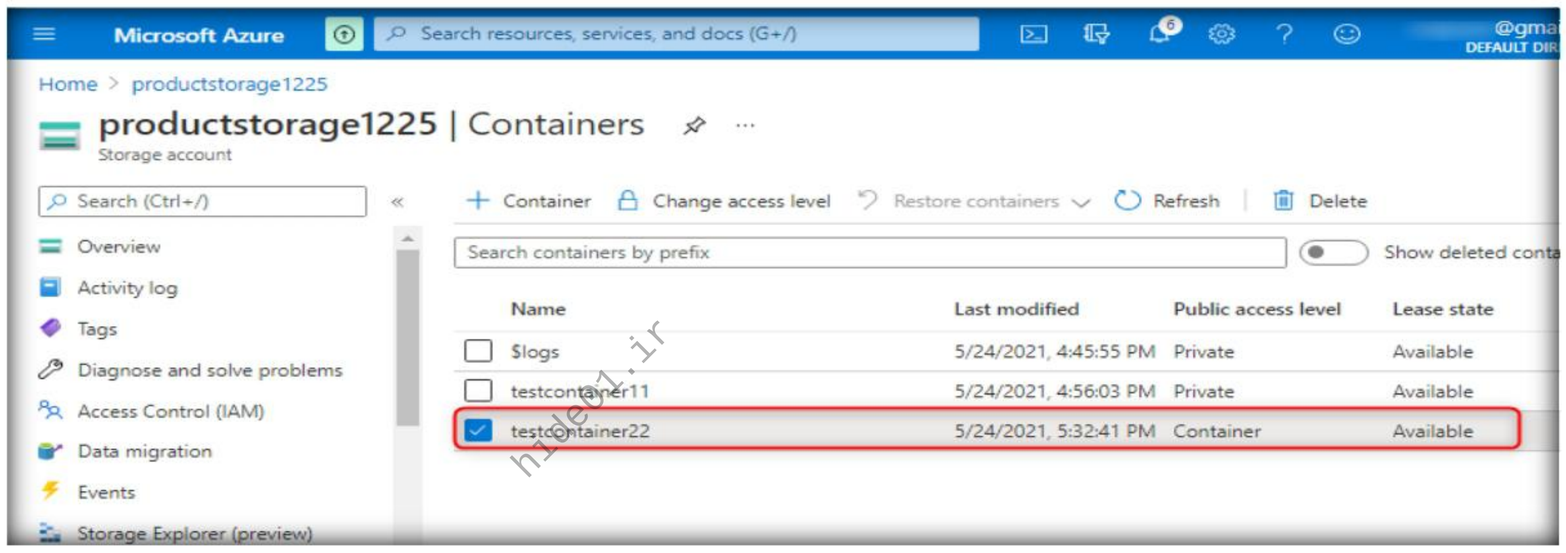


FIGURE 4.9.35: Selecting the Container with Public Access

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

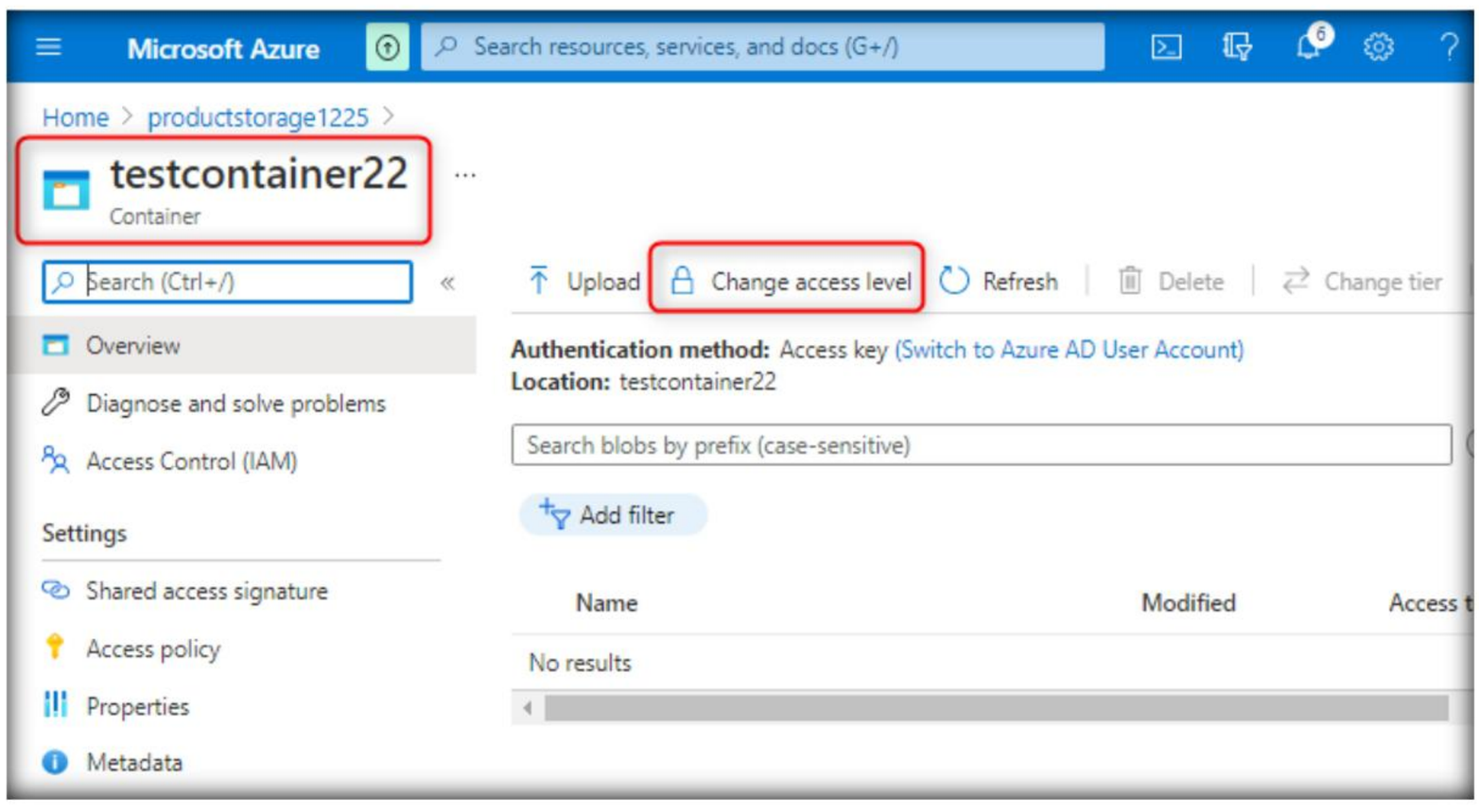


FIGURE 4.9.36: Changing Access Level

Certified Cloud Security Engineer Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

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

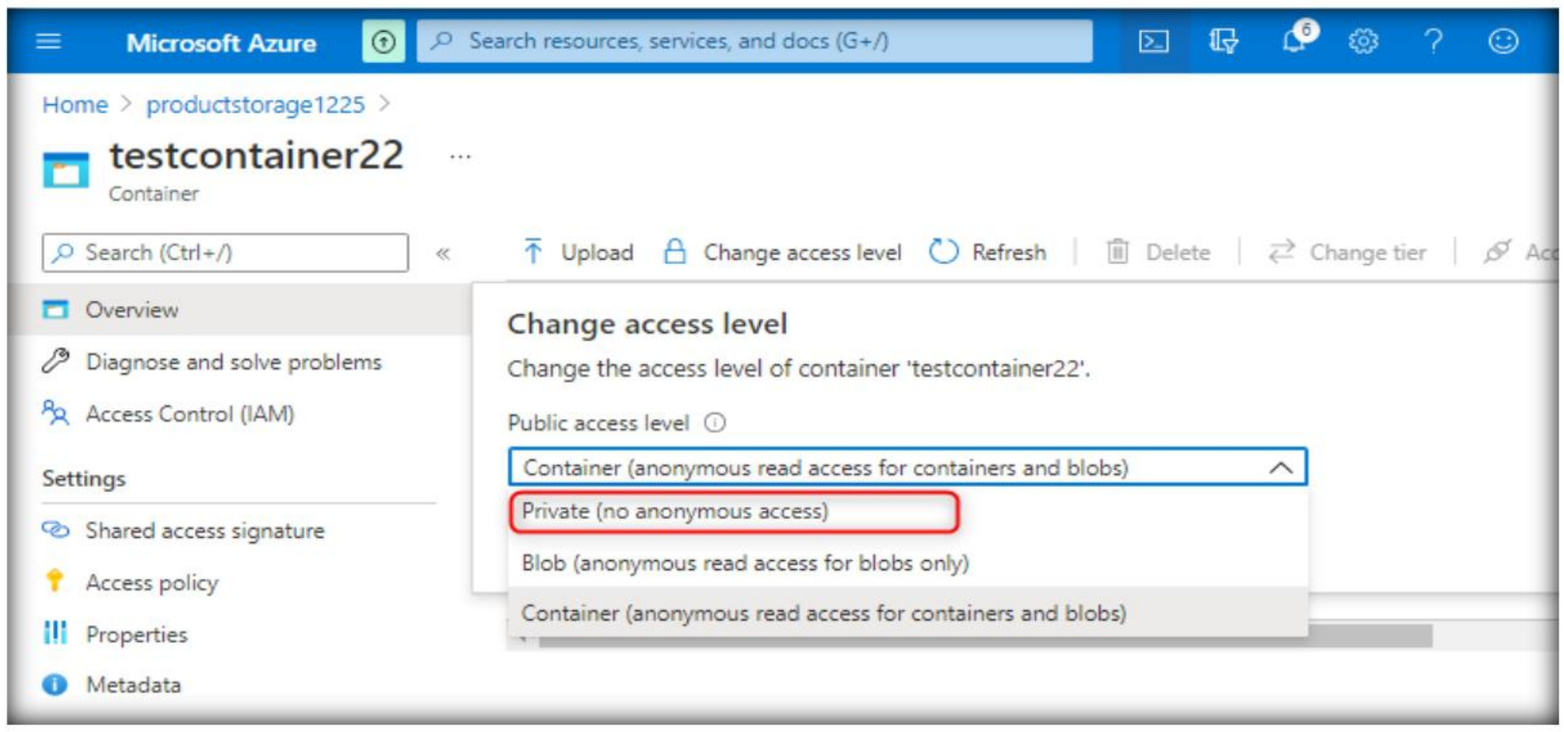


FIGURE 4.9.37: Selecting Private (no anonymous access) for the Container

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

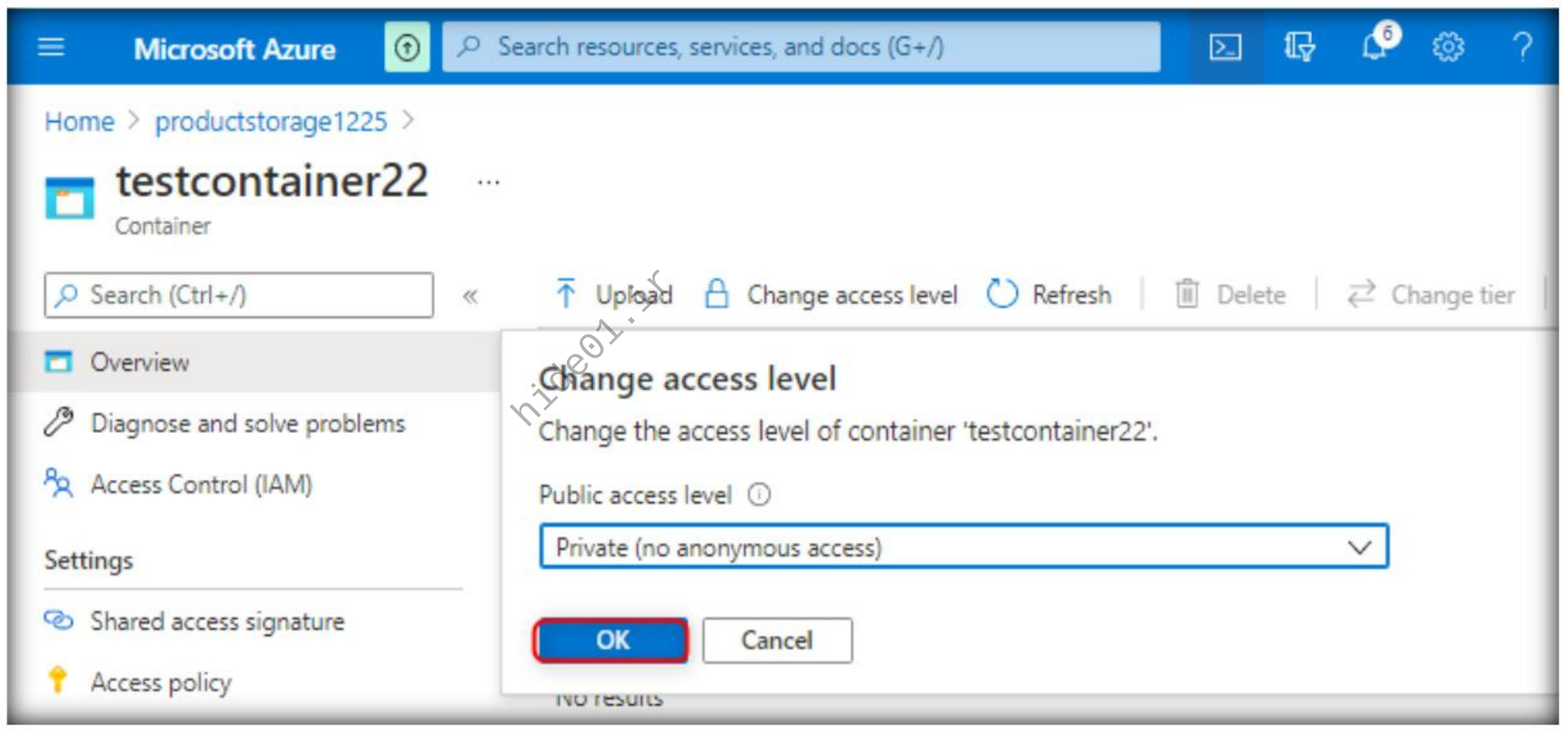


FIGURE 4.9.38: Confirming Change in Access Level

39. Click on **productstorage1225**.

FIGURE 4.9.39: Going Back to Storage Account

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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

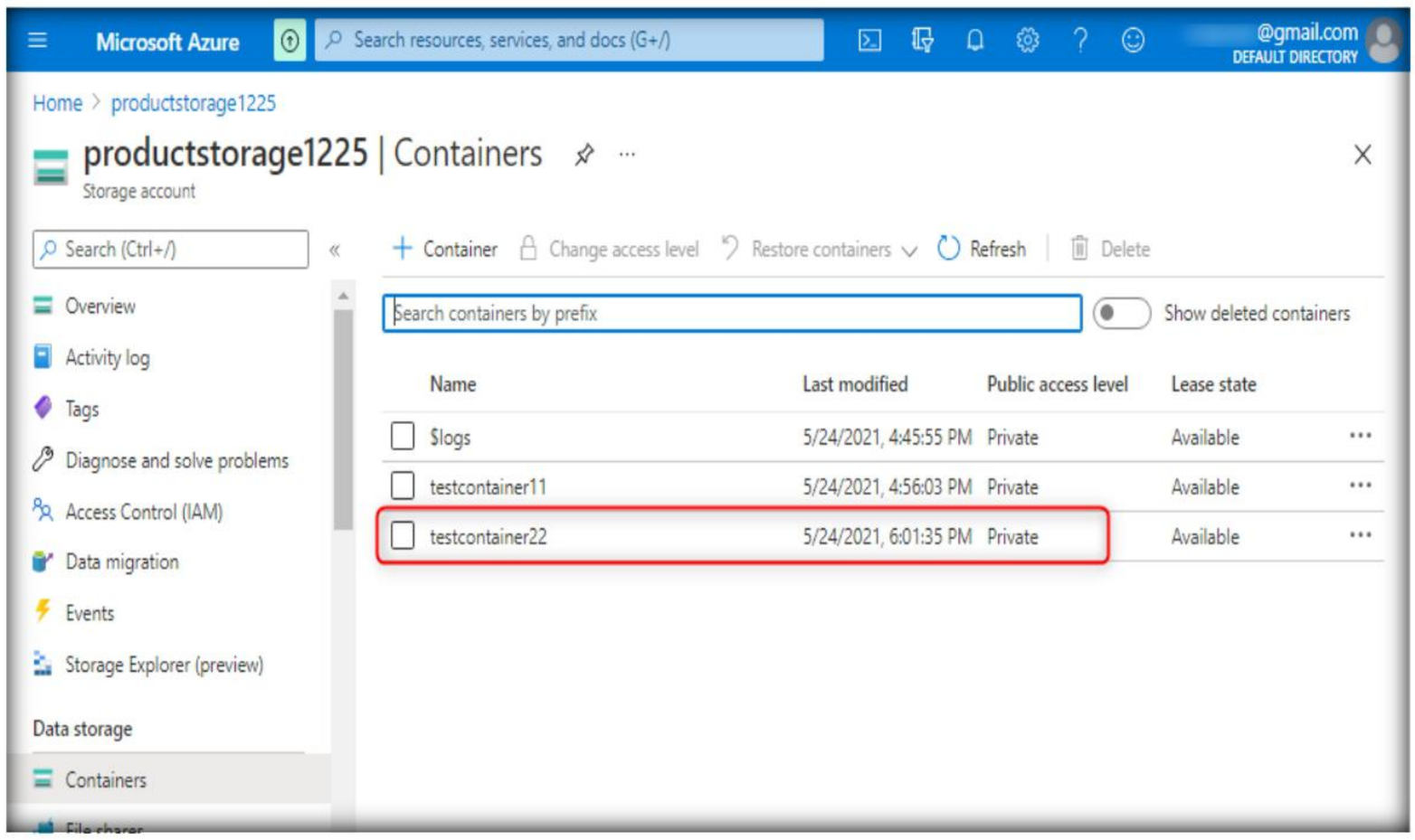


FIGURE 4.9.40: Checking the Change in Access Level

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.

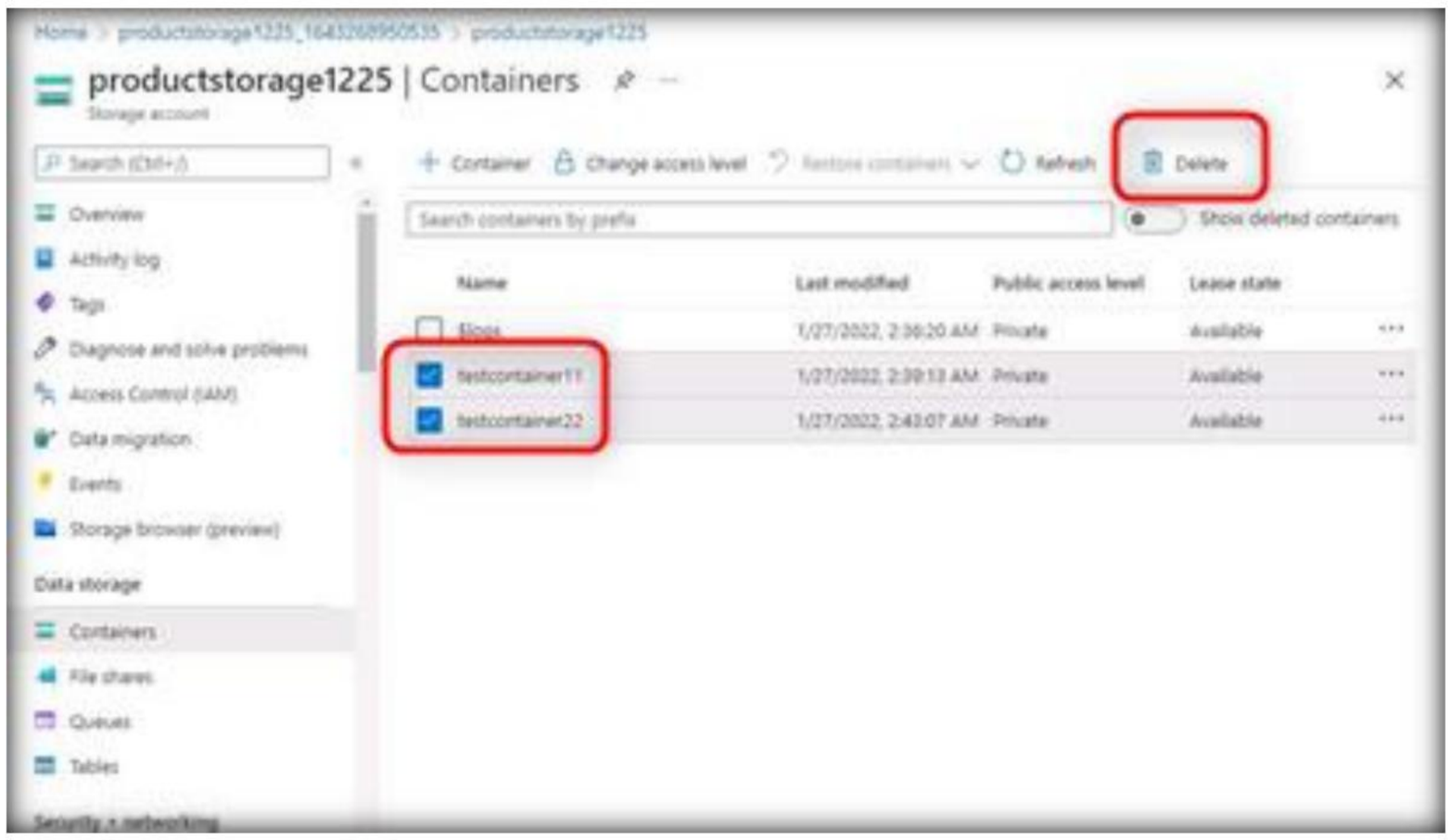


FIGURE 4.9.41: Deleting Container

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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.

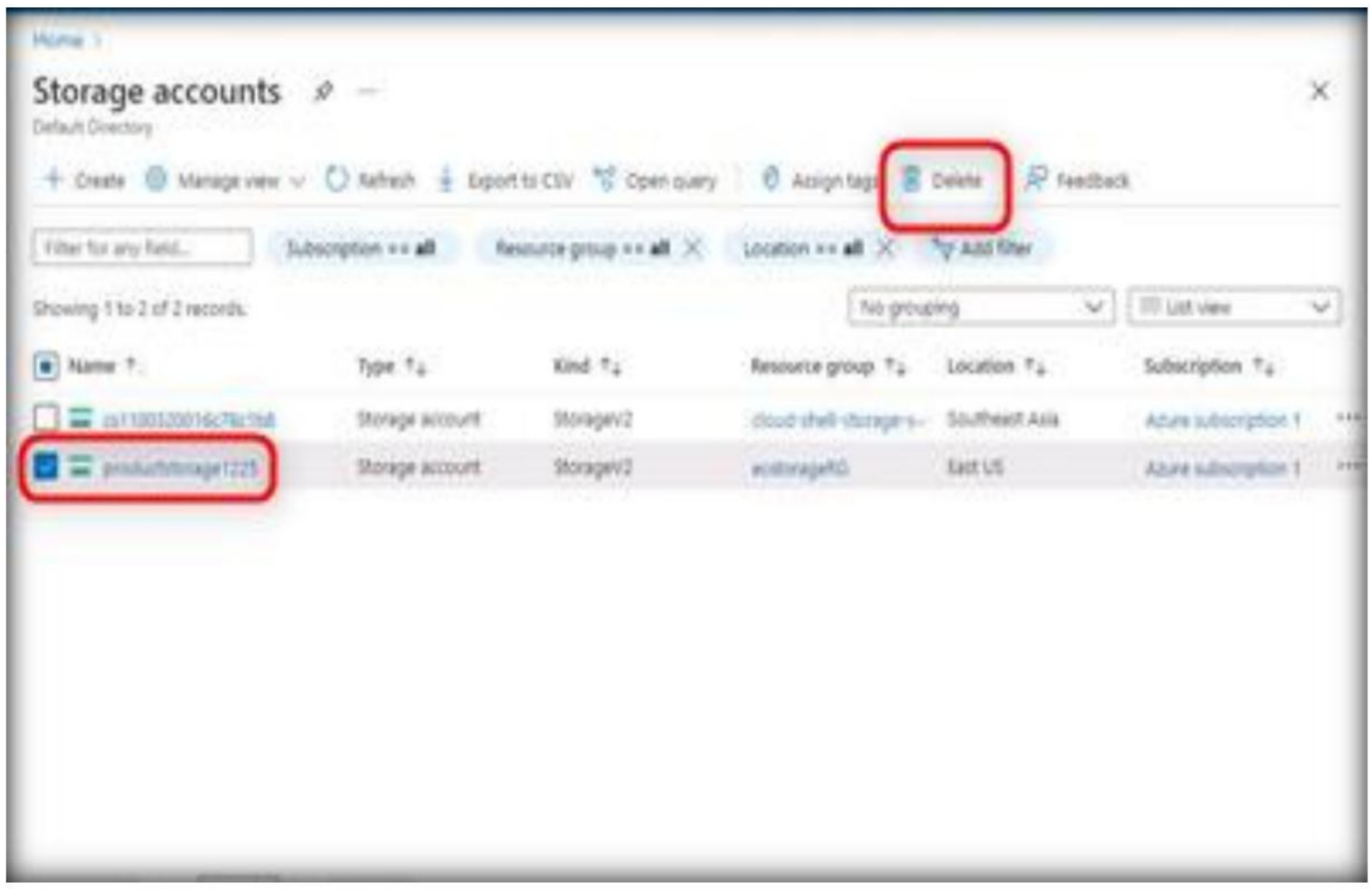


FIGURE 4.9.42: Deleting Storage Account

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.

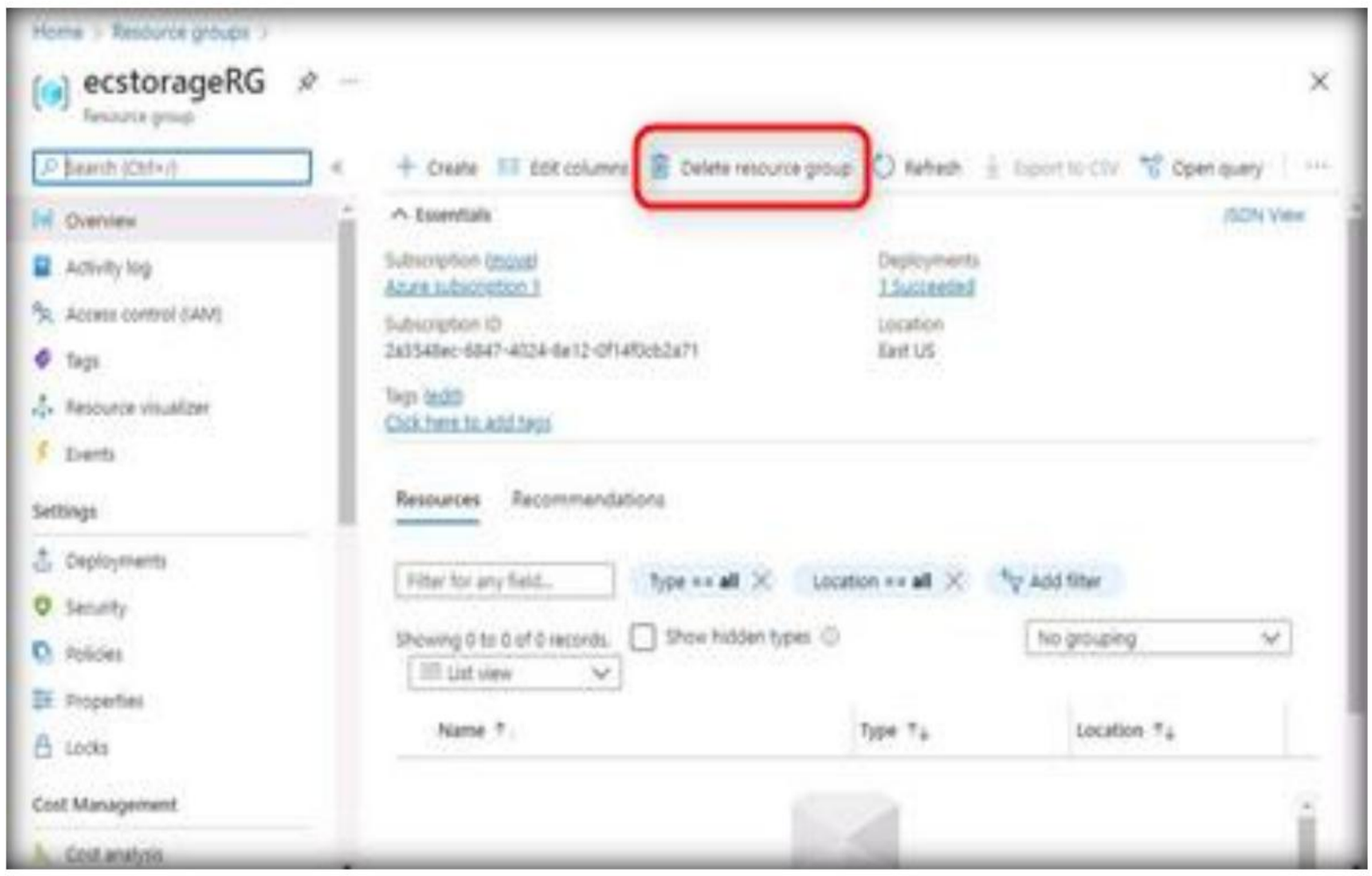


FIGURE 4.9.43: Deleting Resource Group

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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.

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 9

Preventing Accidental Deletion of Resources Using Azure Resource Locking

Azure Resource Locking helps to protect the resources deployed in Azure from accidental deletion. Resource Locking can be applied to individual resources or resource groups.

ICON KEY

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

Lab Scenario

hide01.ir

Azure RBAC (Role-Based Access Control) is used to prevent access to the resources in Microsoft Azure. Implementing RBAC restricts access, but it is not that effective in all situations. If a user with full access accidentally deletes any critical resources, it will affect the cloud operations. To prevent accidental deletion, malicious changes, or modification to the critical resources, you should lock the Azure resource group or resource. In this lab, you will learn how to lock the Azure Resource Group to protect it from accidental deletion.

Lab Objectives

In this lab, you will learn how to create a Resource Group and Resource, lock the Resource Group, lock the Resource, try to delete the resource after the lock is enabled, delete Lock on the Resource Group, and then delete the Resource using Azure PowerShell.

In this lab, you will:

- Create a Resource Group and Resource in the form of a Virtual Machine
- Lock the Resource Group and Resource
- Unlock Resource Group and try to delete the Resource

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Environment

To perform this lab, you need the following:

- Admin Machine VM
- Registered Microsoft Azure account.

Lab Duration

Time: 15 minutes

Overview of Azure Resource Locking

Azure Resource Locking adds an extra layer of security by preventing the accidental deletion of the resources. Azure Resource Lock can be applied to resources or resource groups. The two types of Azure Resource Locks are

- **CanNotDelete**: In this type of lock, modifications can be performed on the resources, but the resources cannot be deleted.
- **ReadOnly**: In this type of resource lock, both modification and deletion of resources cannot be done.

To safeguard the resource group or resource from accidental deletion or modification in Azure, the cloud security engineer should lock the resource group or resource. The lock that is applied on the parent scope will be inherited to all the resources that are within that scope. If you add any resource later, then the resource will inherit the lock from the parent. You can apply the lock at the resource group level or the resource level. Once the lock is applied to the resources or resource groups, it can only be deleted once the resource lock is removed, thus preventing accidental deletion. As a part of the Azure Governance Strategy, you can use the resource lock to safeguard your cloud resources. It is recommended to apply the lock at the resource group level.

Lab Tasks

TASK 1

Creating a Resource Group and Resource

Note: Web applications using cloud environments may undergo frequent updates. For this lab, since we are working on a cloud-based environment (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 an Azure Free Account using the following link: https://azure.microsoft.com/free, in case you have already

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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.

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

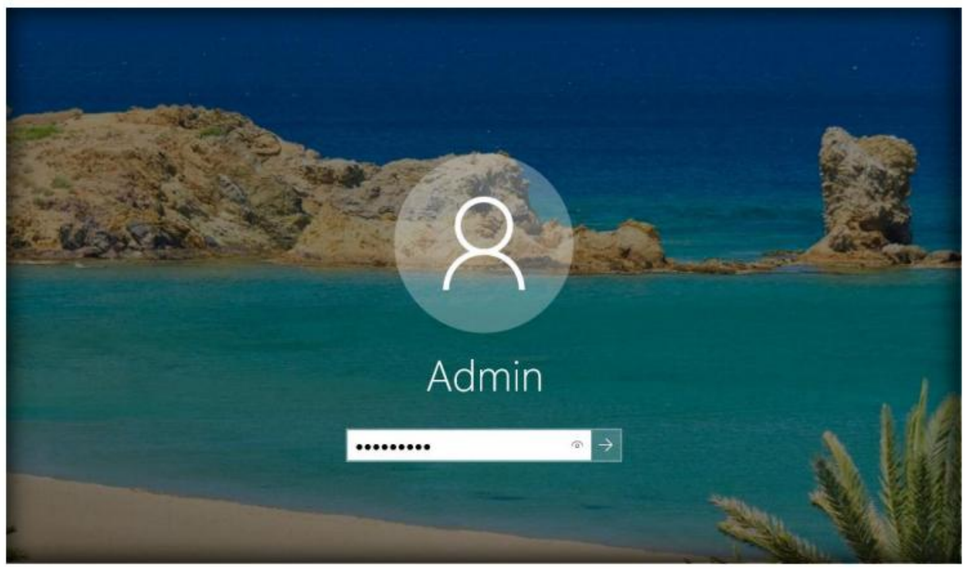


FIGURE 4.9.1: Launch Admin Machine and Log in

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. Go to the address bar, type **https://azure.microsoft.com/en-in/account/**, and press **Enter**.

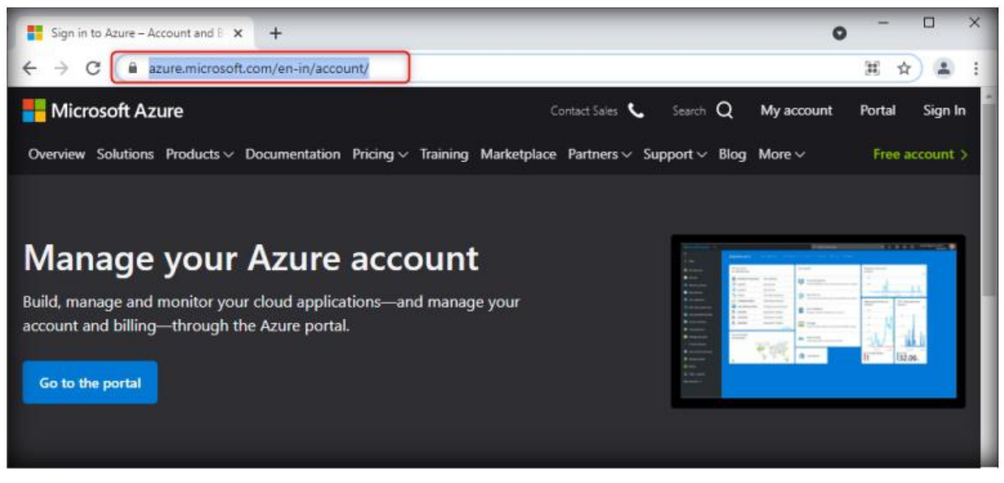


FIGURE 4.9.3 Entering the URL of Microsoft Azure

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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

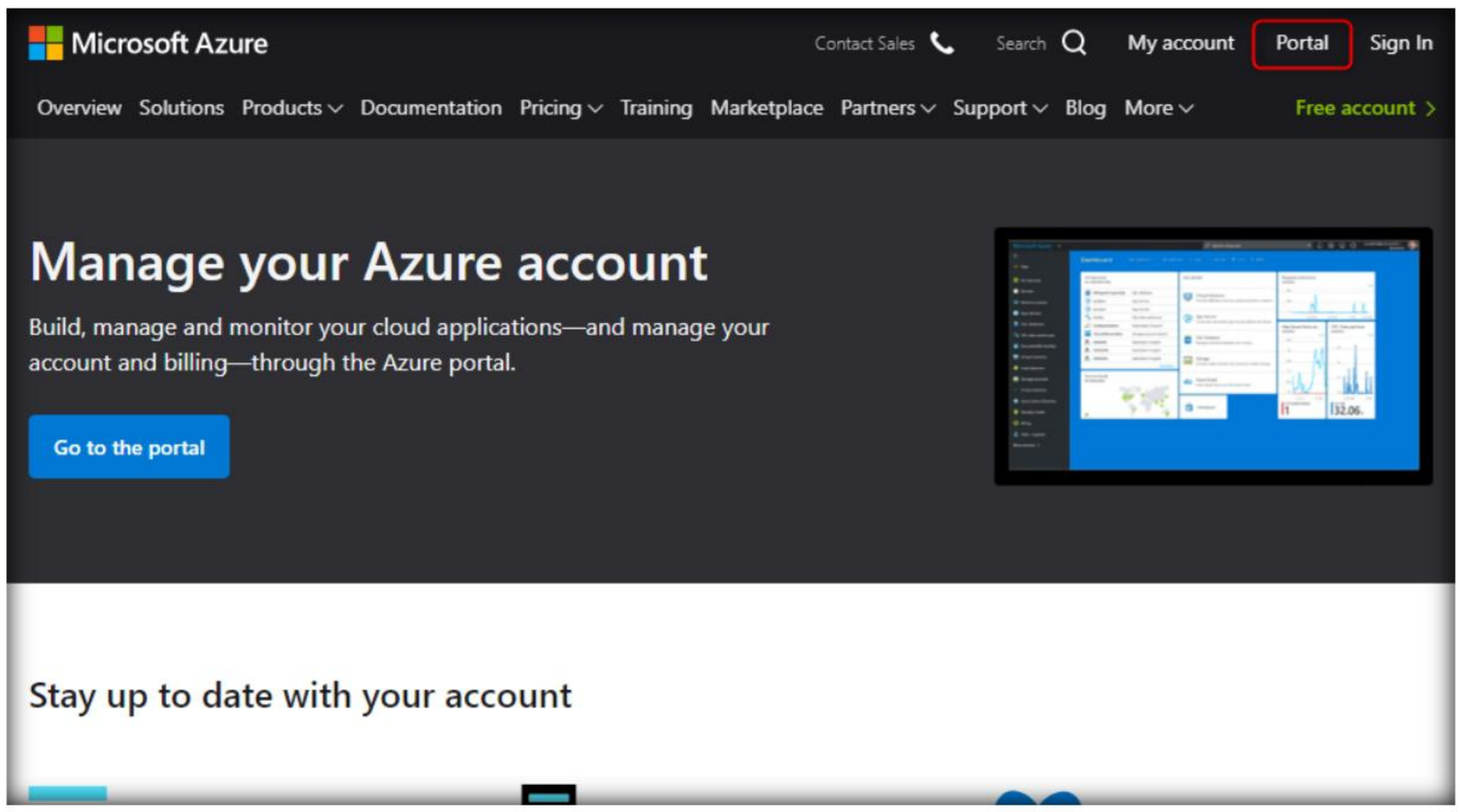


FIGURE 4.9.4:: Sign in to Azure Portal

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

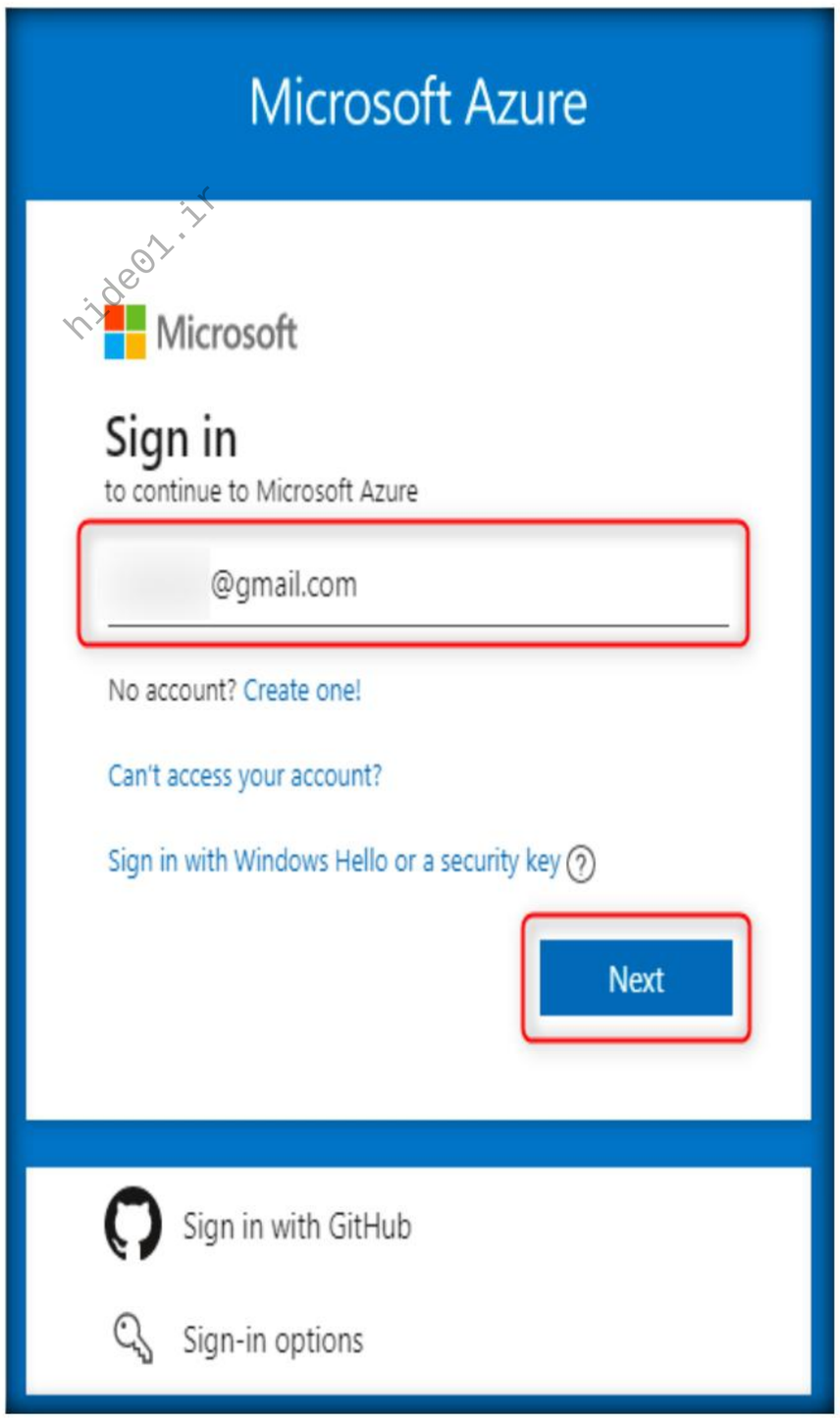


FIGURE 4.9.5: Entering Account ID to continue

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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

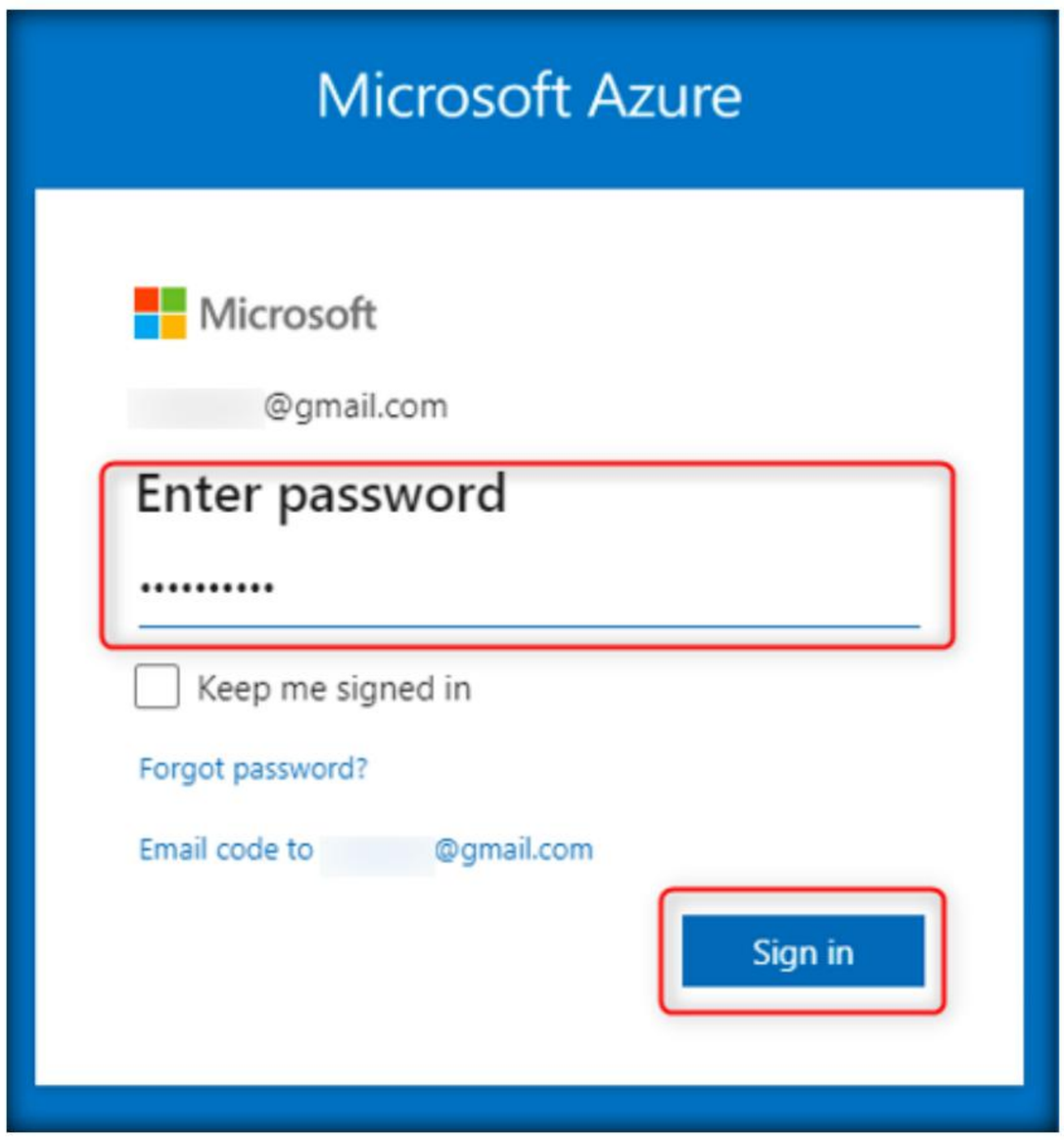


FIGURE 4.9.6: Entering the login Password

7. In the Azure portal, click on the **Cloud Shell** button in the top navigation bar.

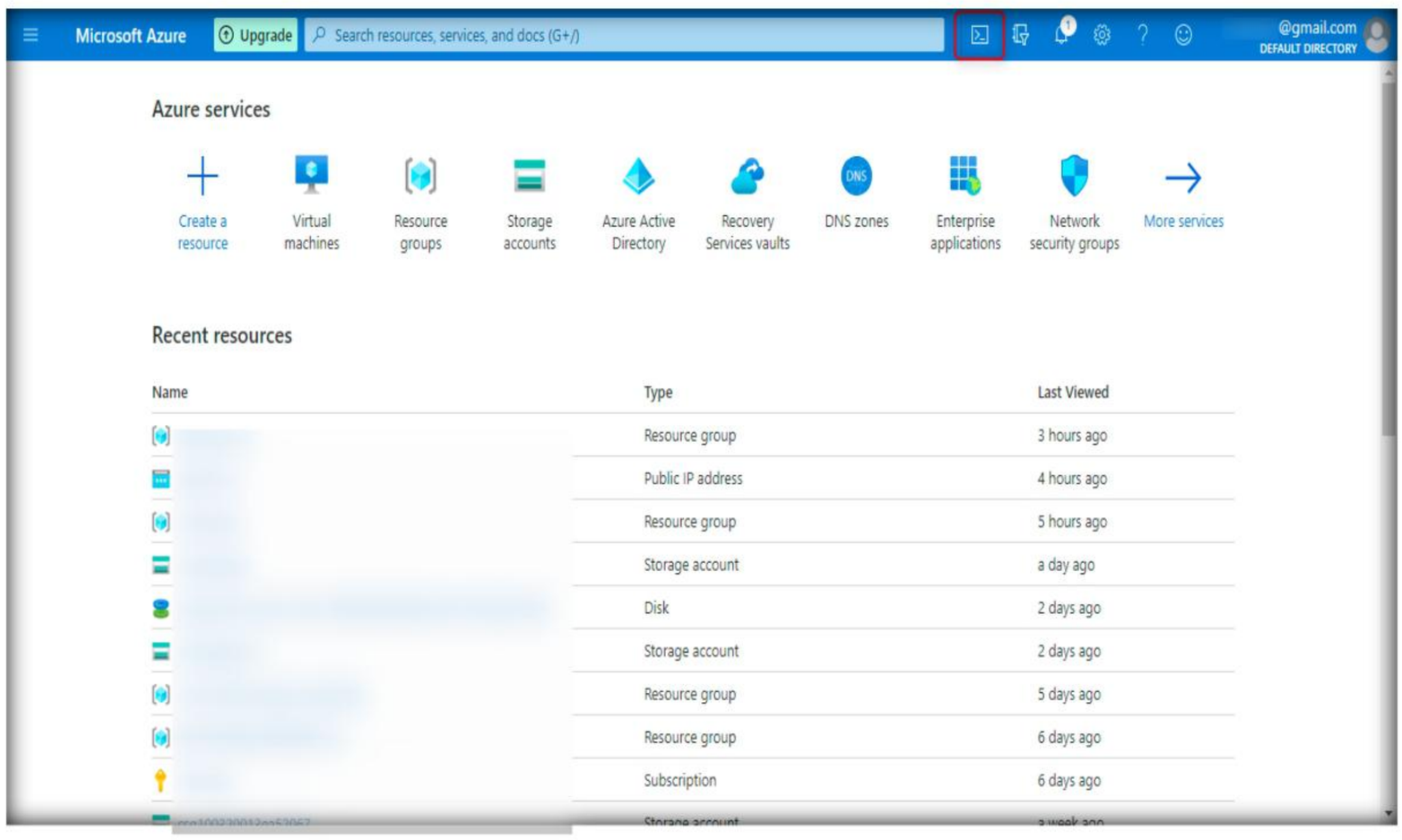


FIGURE 4.9.7: Selecting Cloud Shell in Azure Portal

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

8. Select the **PowerShell** environment from the dropdown in the top left side of the cloud shell.

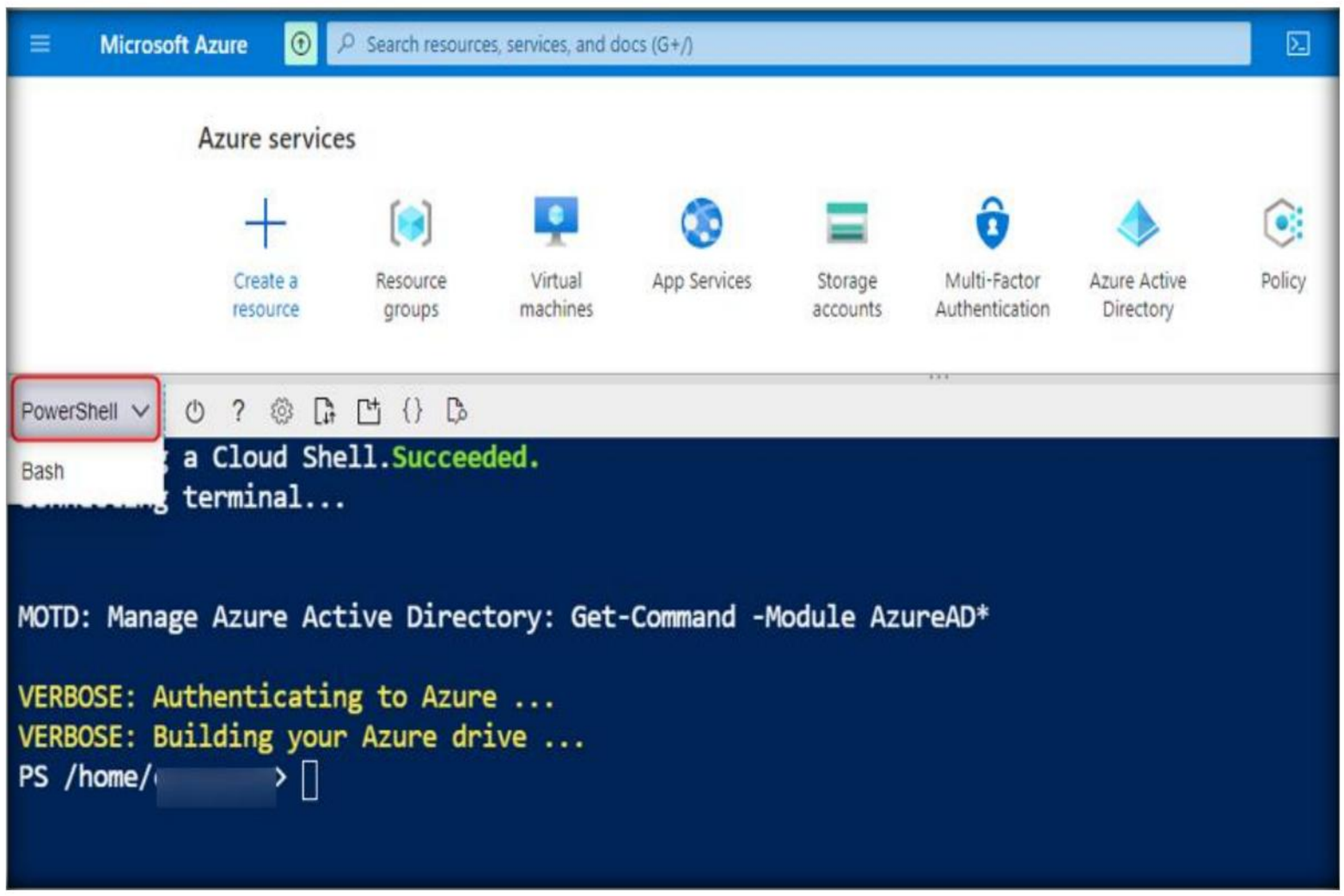


FIGURE 4.9.8: Choosing PowerShell Environment

9. Run the following command to create a new resource group.

```
New-AzResourceGroup -Name "myResourceGroup2556"
-Location "EastUS"
```

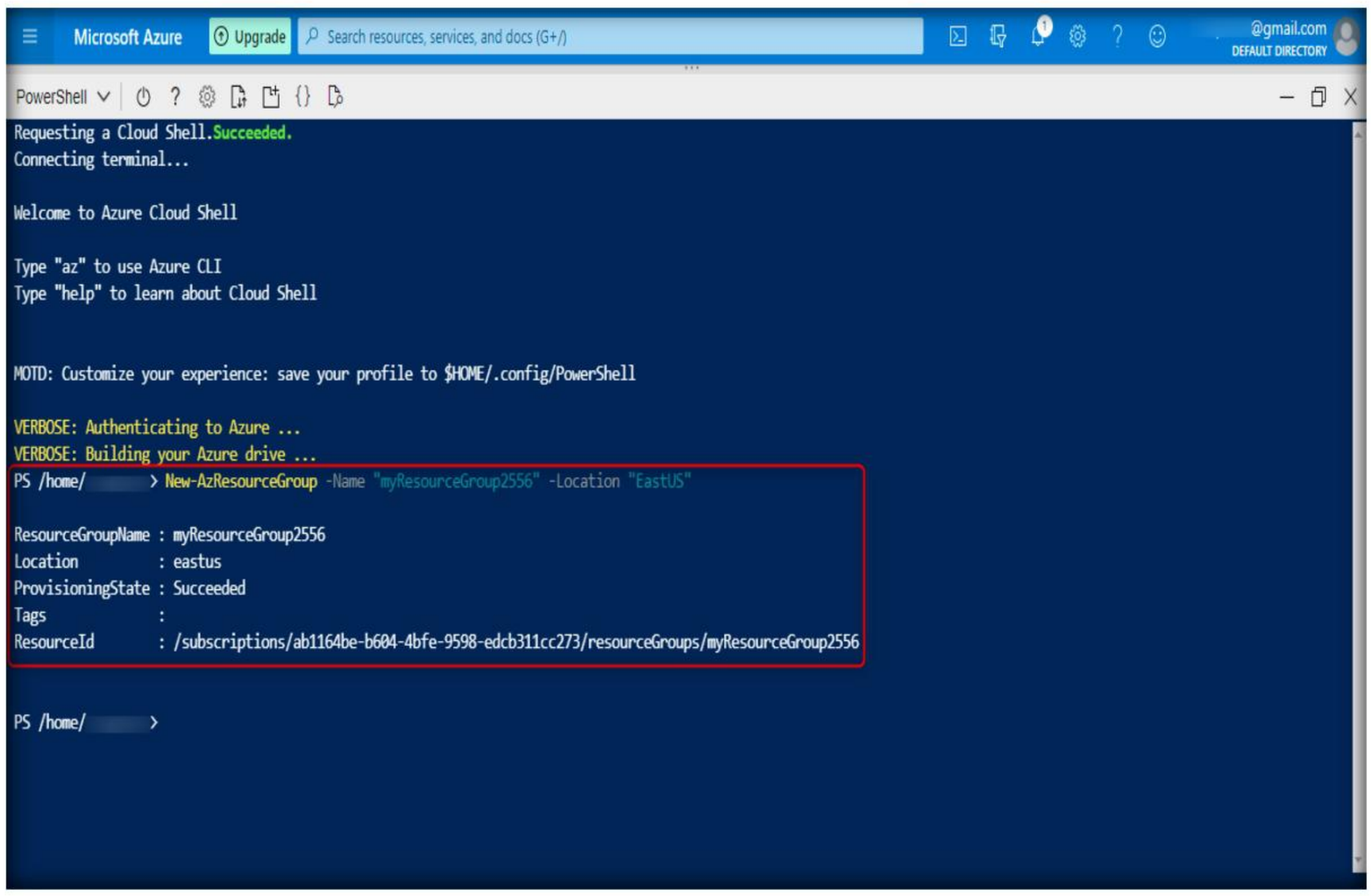


FIGURE 4.9.9: Creating a Resource Group

Certified Cloud Security Engineer Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

10. To create a resource i.e., virtual machine, enter the following command.

```
New-AzVm `
    -ResourceGroupName "myResourceGroup2556" `
    -Name "myVM2556" `
    -Location "East US" `
    -VirtualNetworkName "myVnet" `
    -SubnetName "mySubnet" `
    -SecurityGroupName "myNetworkSecurityGroup"
`
    -PublicIpAddressName "myPublicIpAddress" `
    -OpenPorts 80,3389
```

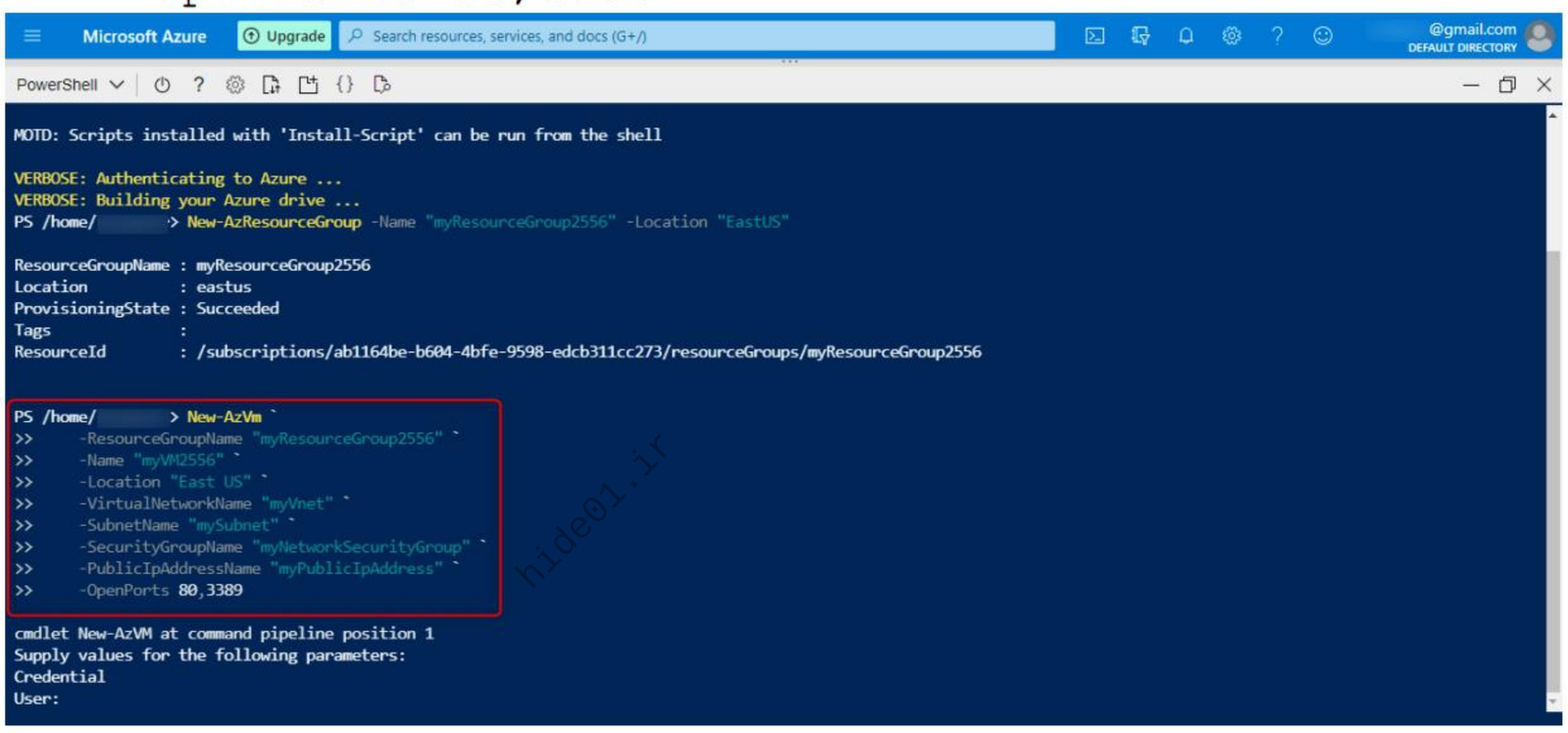


FIGURE 4.9.10: Creating a VM

11. You will have to enter a user name and password for the VM. Enter the User as **ccseuser** and a **Password** of your choice and press **Enter**.

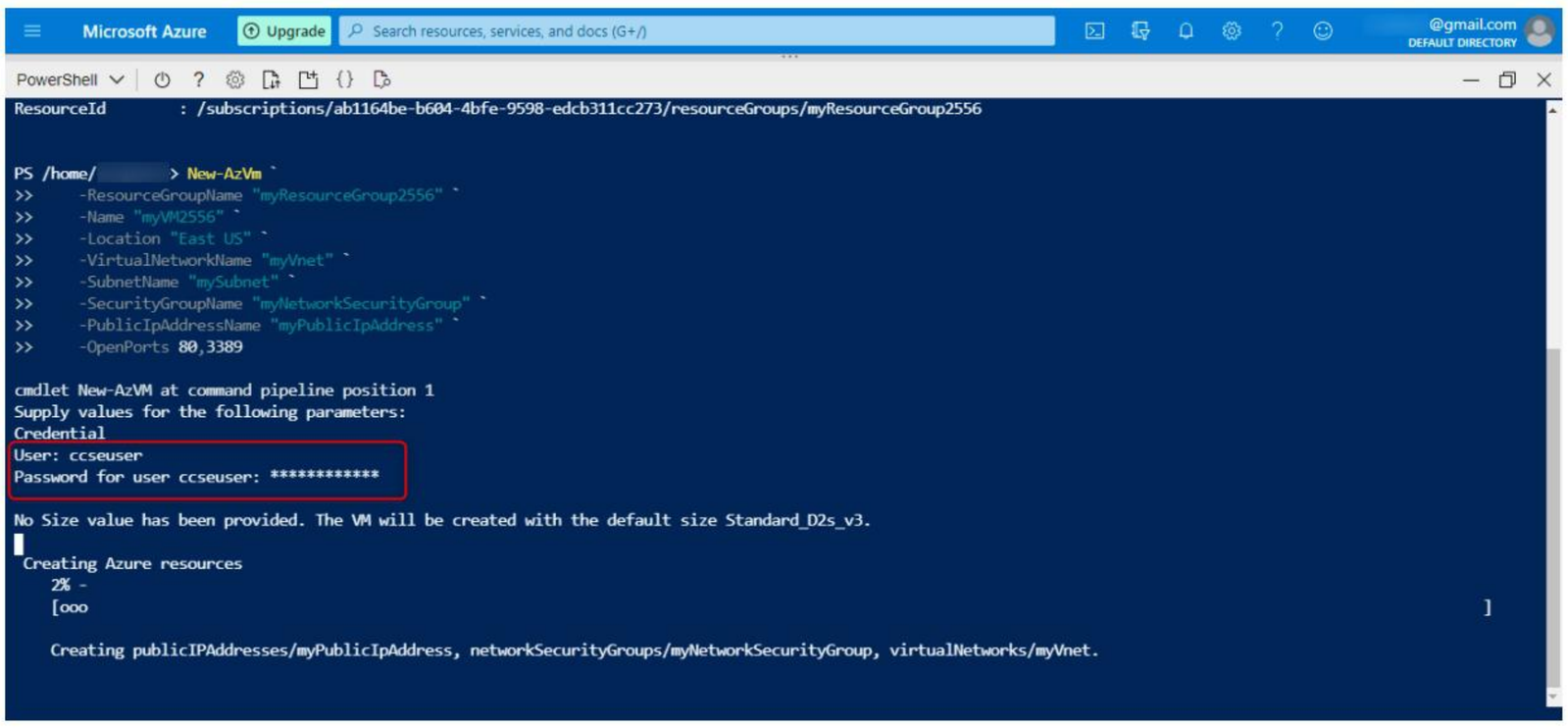


FIGURE 4.9.11: Entering the User and Password

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

12. After few minutes, your VM will get deployed successfully.

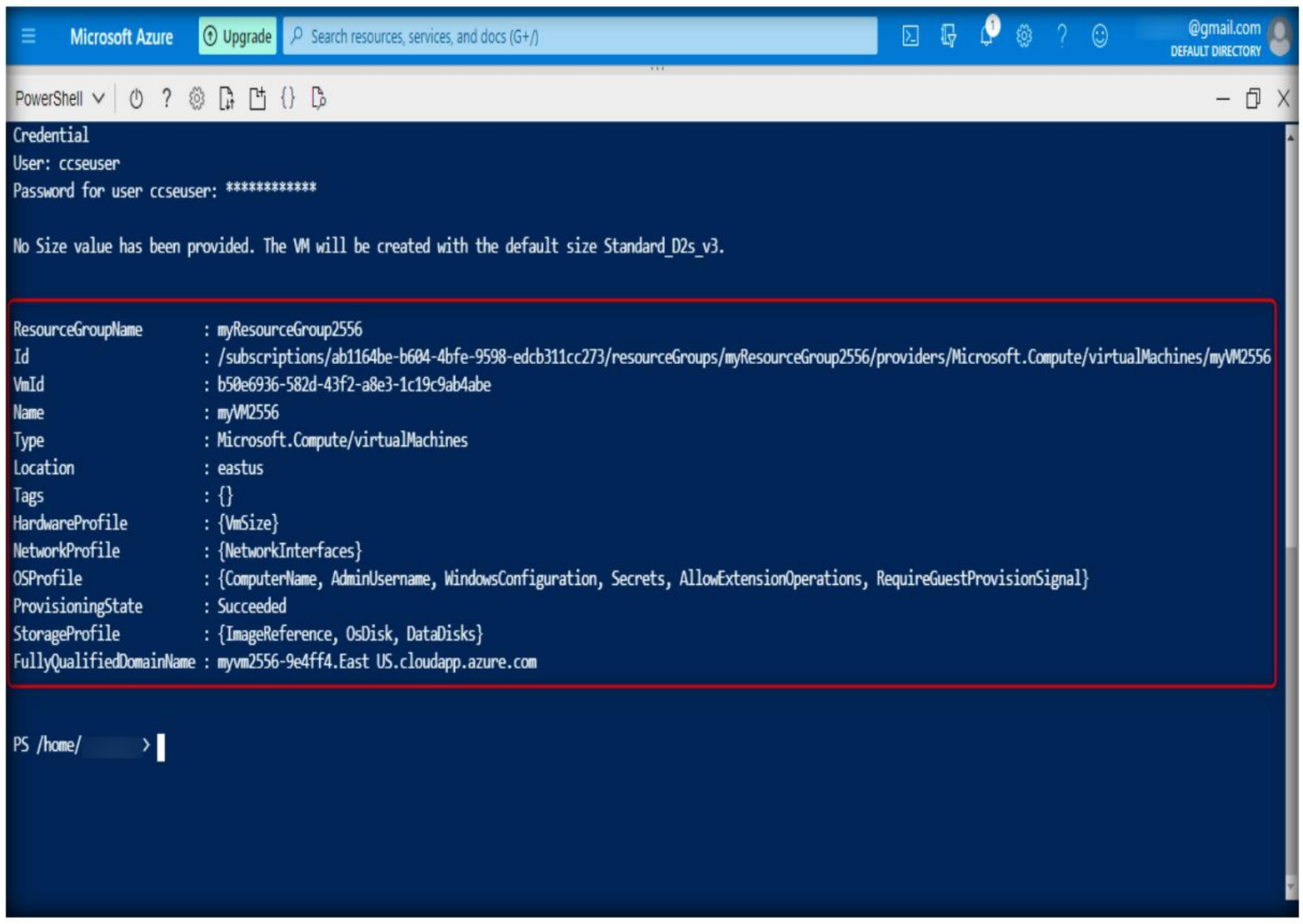


FIGURE 4.9.12: Successful Deployment of VM

13. Now, run the following command to determine the type of resource.

```
Get-AzResource
```

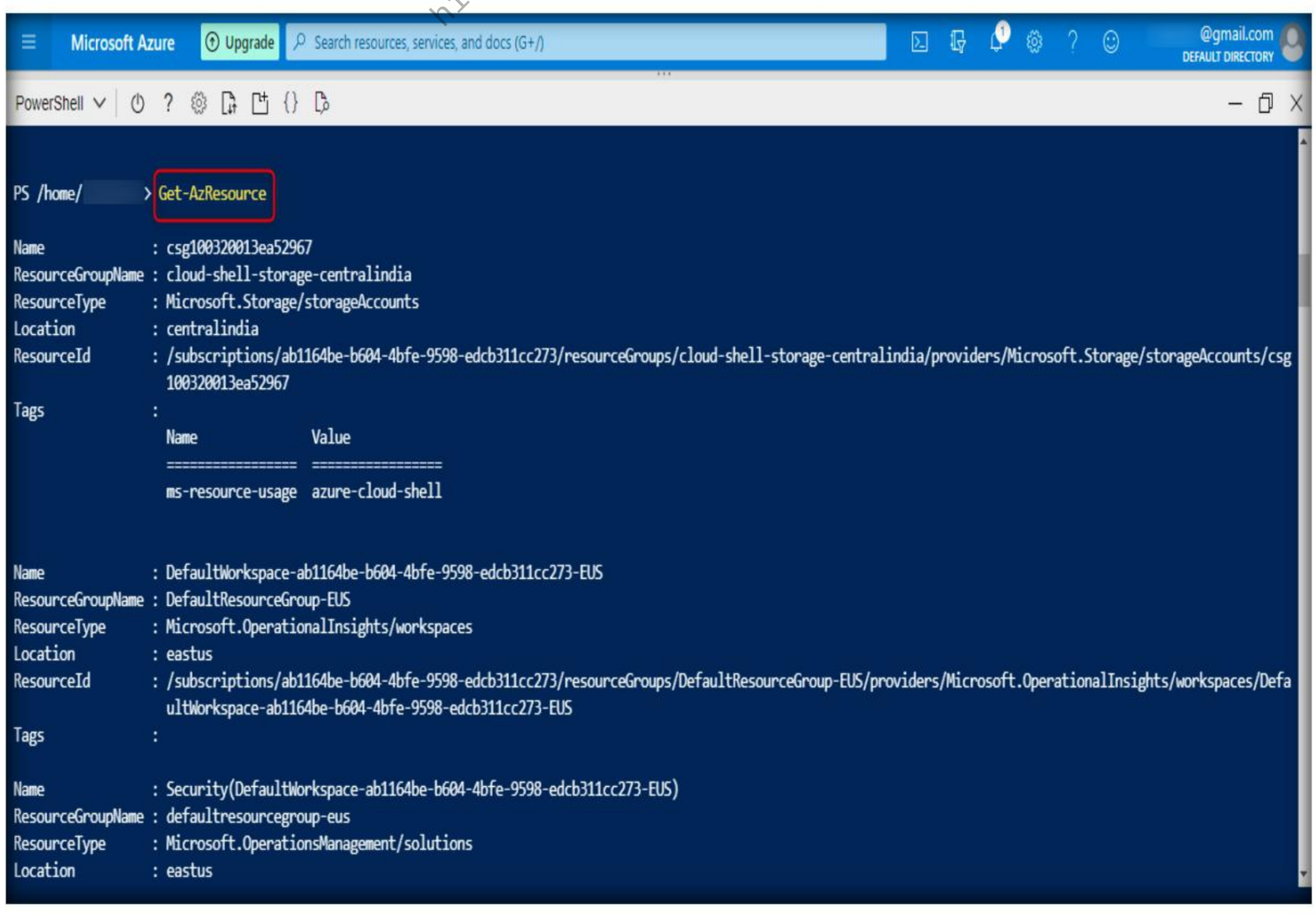


FIGURE 4.9.13: Fetching all the Resources in Azure

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

14. Scroll down and find the **Name** of the resource you have just created (**myVM2566**) and the **Resource Type** as **Microsoft.Compute/virtualMachines**, as shown in the screenshot. Copy the Name of the resource (**myVM2556**),ResourceGroupName (**myResourceGroup2556**), and ResourceType (**Microsoft.Compute/virtualMachines**) and paste in notepad.

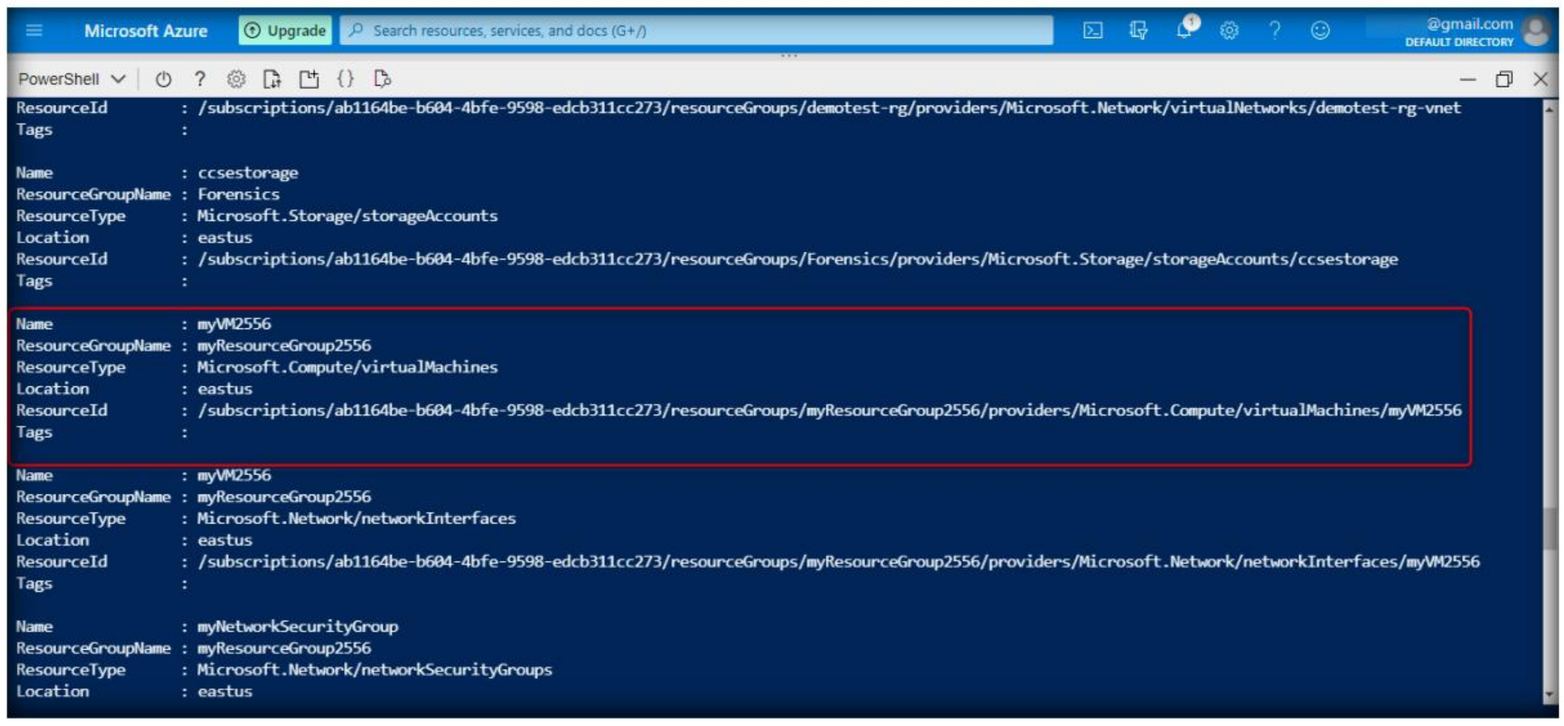


FIGURE 4.9.14: Determining the Type of Resource

TASK 2

Lock the Resource Group and Resource

15. Now, to lock the resource, you need the resource's name, resource type, and resource group that you have copied to notepad in the previous step. First, lock the resource with the **CanNotDelete** lock level. Run the following command to lock the resource.

```
New-AzResourceLock -LockLevel CanNotDelete -
LockName LockSite -ResourceName myVM2556 -
ResourceType
Microsoft.Compute/virtualMachines -
ResourceGroupName myResourceGroup2556
```

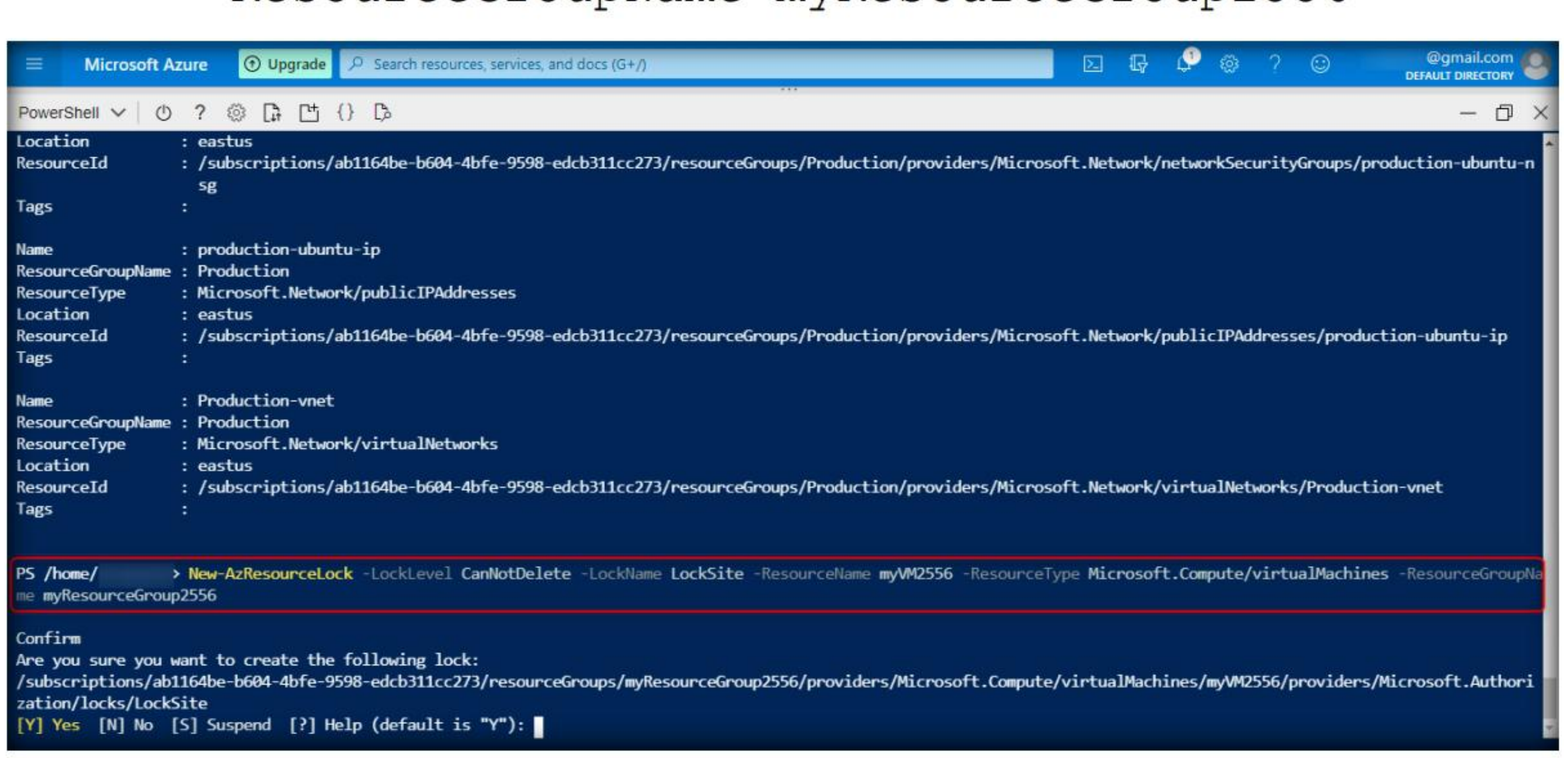


FIGURE 4.9.15: Locking the Resource

Certified Cloud Security Engineer Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

16. Type **Y** and press the **enter** button. The resource gets successfully locked.

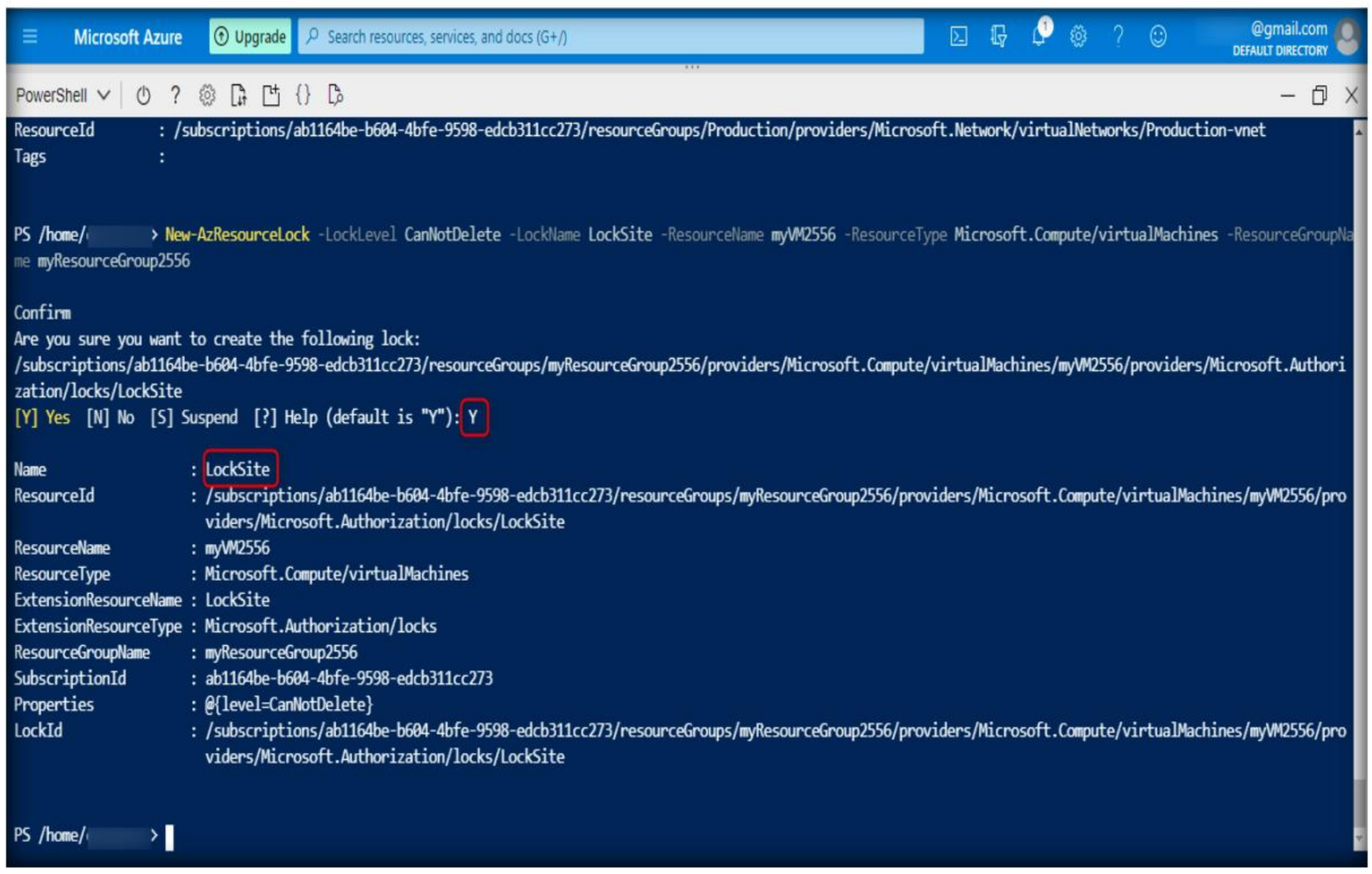


FIGURE 4.9.16: Resource is Successfully Locked

17. Next, you need to lock the resource group. Run the following command to lock the resource group with **CanNotDelete** lock level.

```
New-AzResourceLock -LockName LockGroup -
LockLevel CanNotDelete -ResourceGroupName
myResourceGroup2556
```

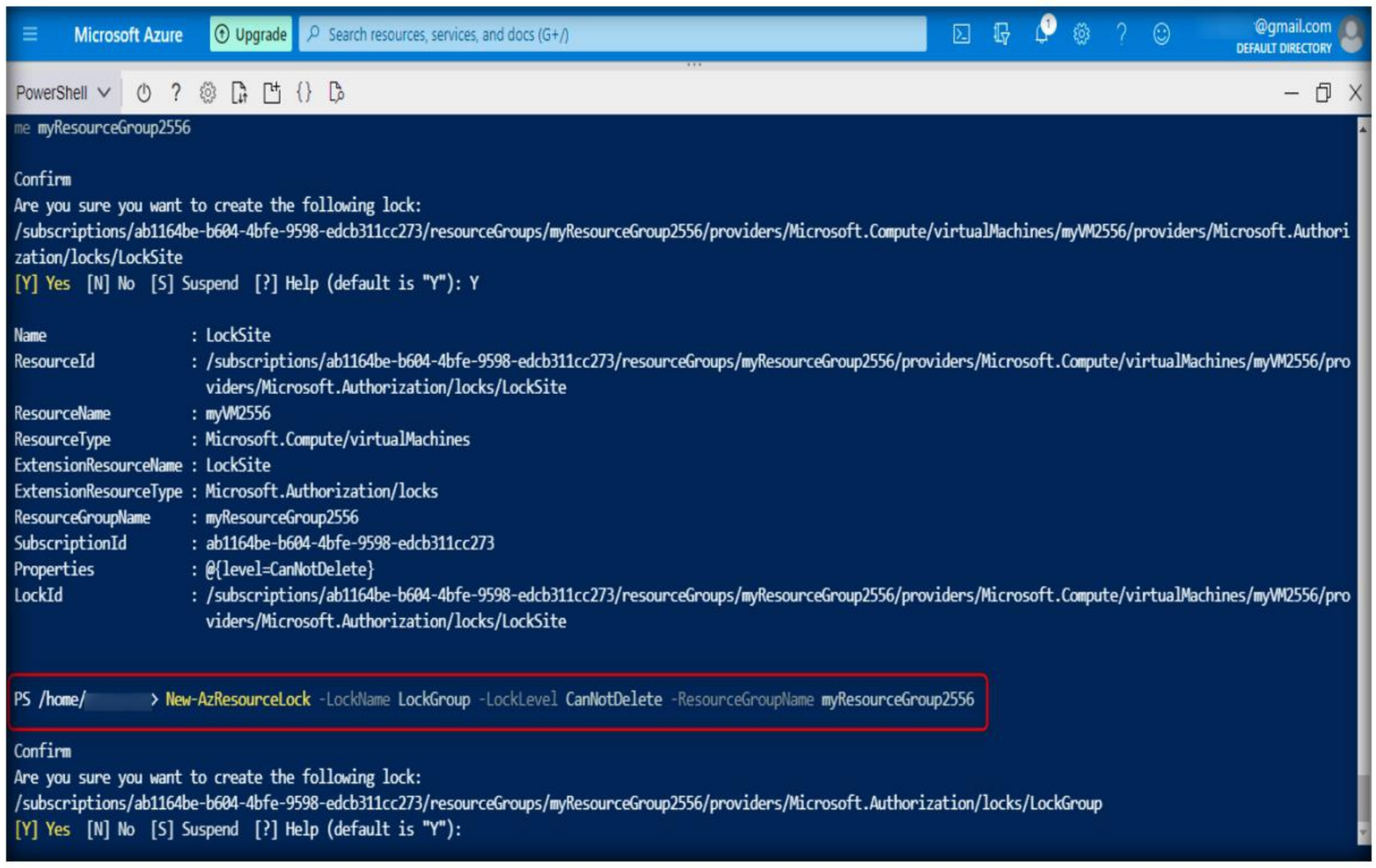


FIGURE 4.9.17: Locking the Resource Group

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

18. Type **Y** and press the **enter** button. Your resource group gets successfully locked.

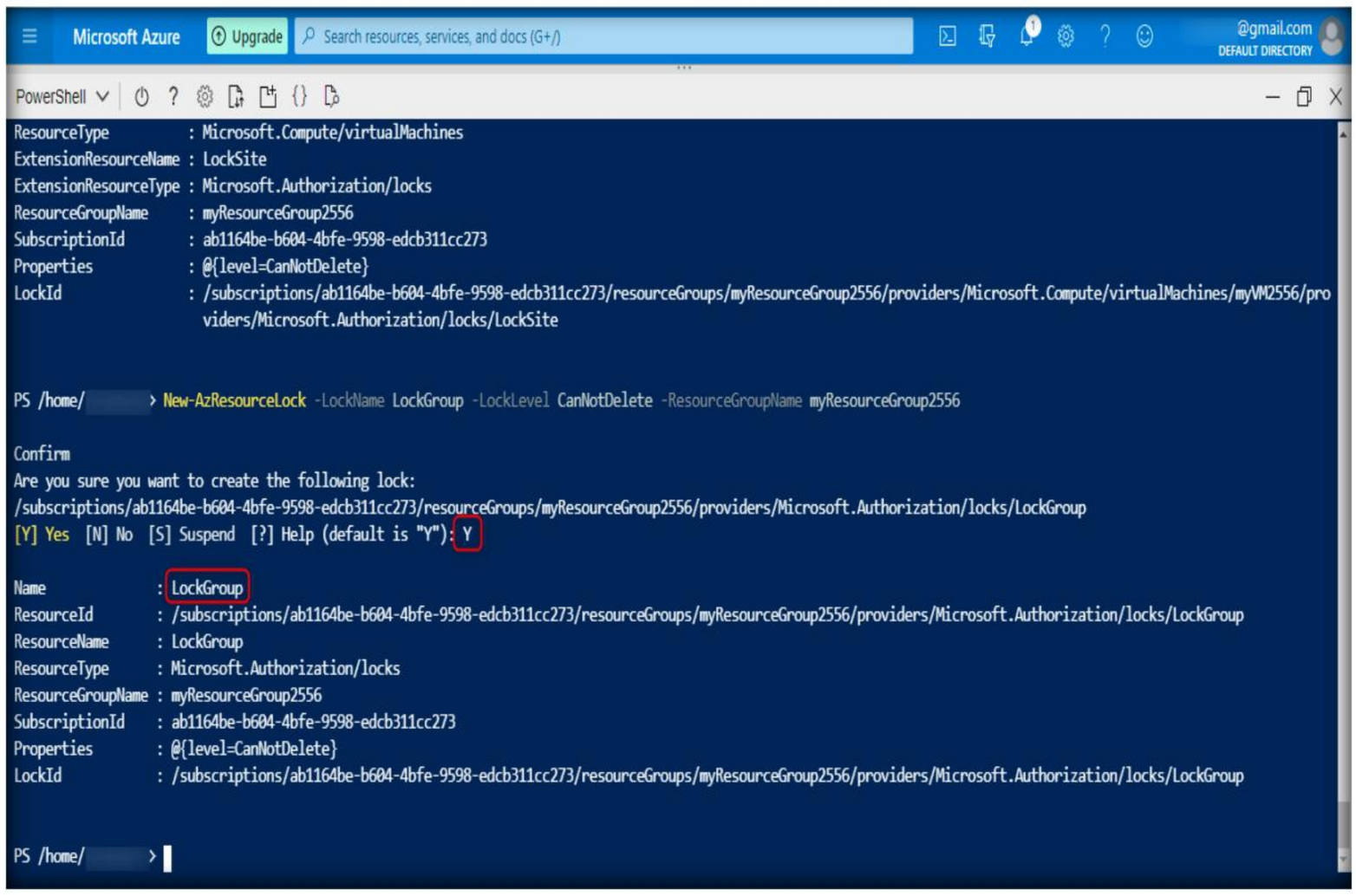


FIGURE 4.9.18: Resource Group is Successfully Locked

19. Run the following command to get information about all the locks in your subscription.

```
Get-AzResourceLock
```

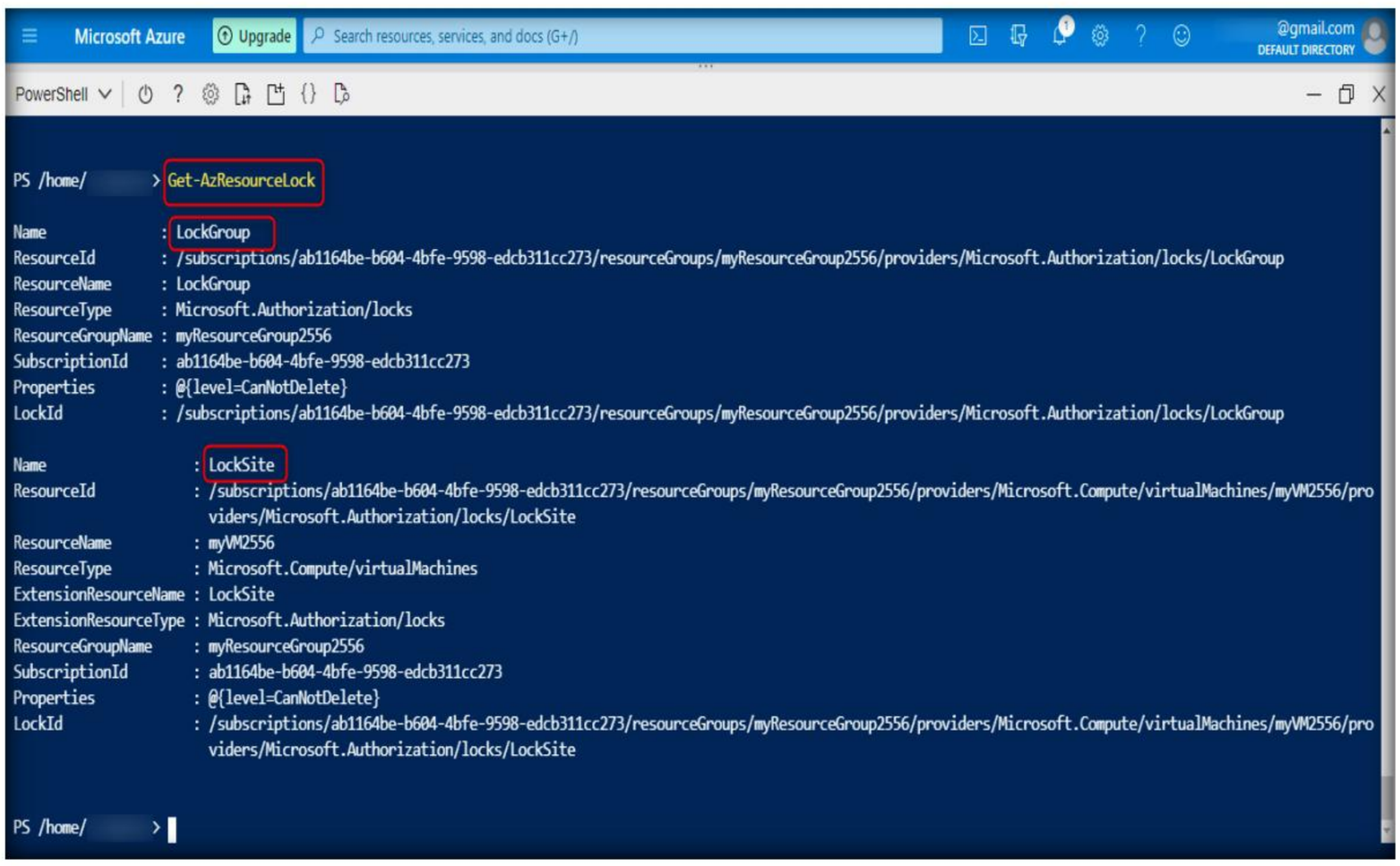


FIGURE 4.9.19: Fetching Information about all the Locks in the Subscription

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

20. Now you can try to delete the VM which you have locked to confirm whether the deployed resource and resource group lock is functioning. Run the following command to delete the VM that we have locked.
`Remove-AzVM -ResourceGroupName "myResourceGroup2556" -Name "myVM2556"`

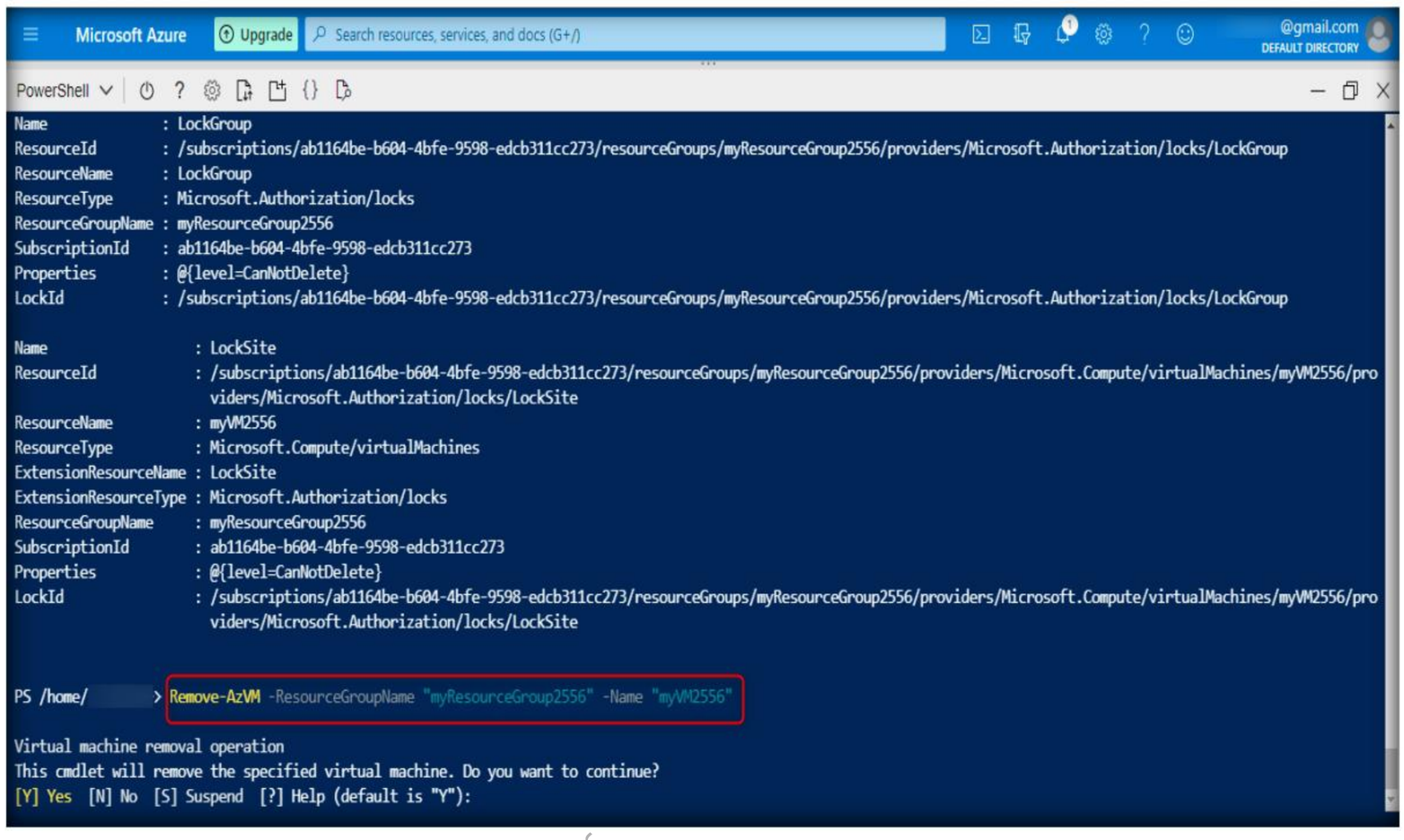


FIGURE 4.9.20: Deleting the VM

21. Type **Y** to confirm the removal of the virtual machine. You will observe an **error** in removal.

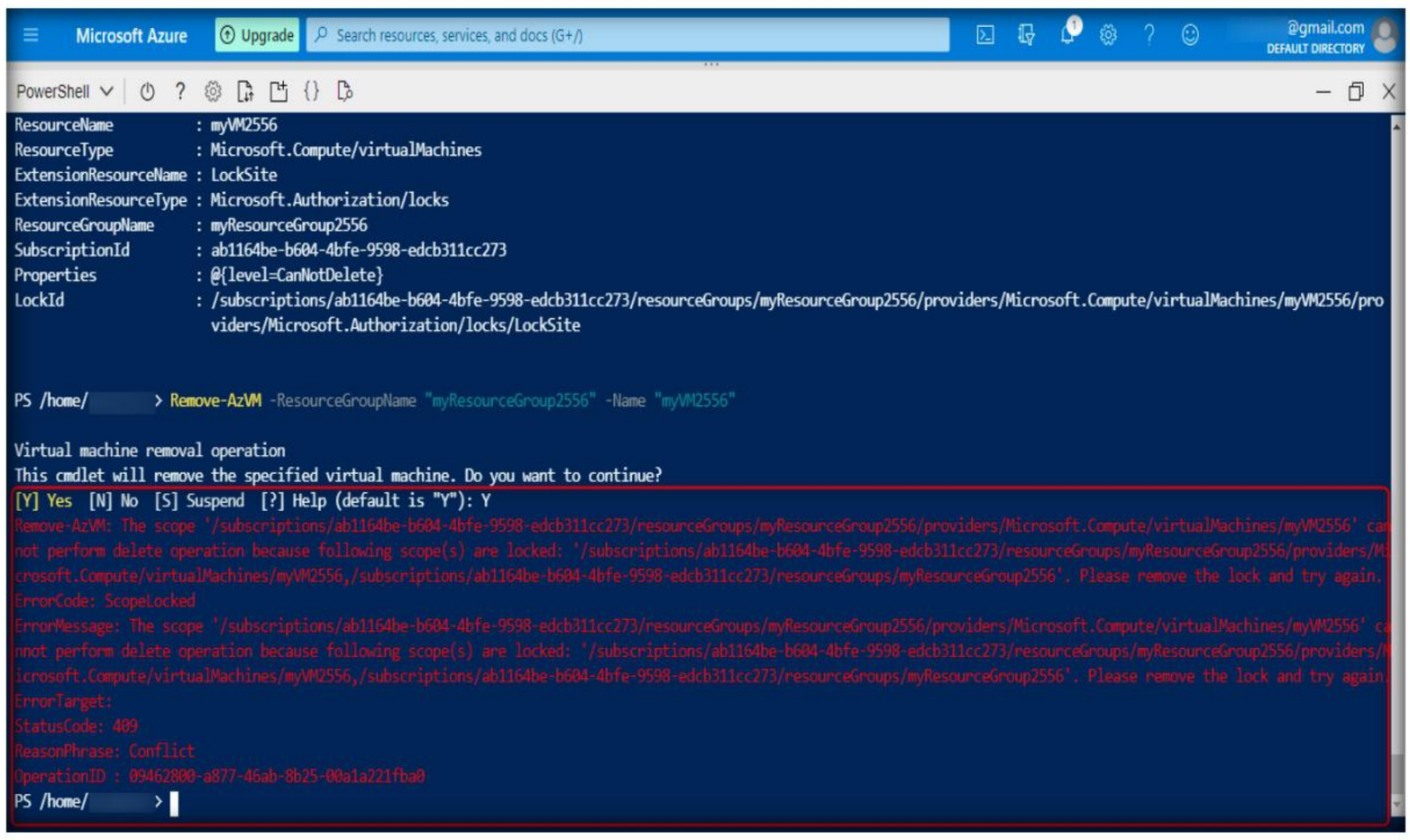


FIGURE 4.9.21: Error in VM Deletion

22. Thus, the resource group and resources cannot be deleted since they are locked, even by the administrator.

h1le01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 3

Unlock the Resource Group and Delete the Resource

23. Now, you can delete the lock on the resource group to remove the lock on all the resources in that resource group. Run the following commands to delete the lock.

```
$rgName = "myResourceGroup2556"

Get-AzResourceLock | Where-Object
ResourceGroupName -eq $rgName | Remove-
AzResourceLock -Force
```

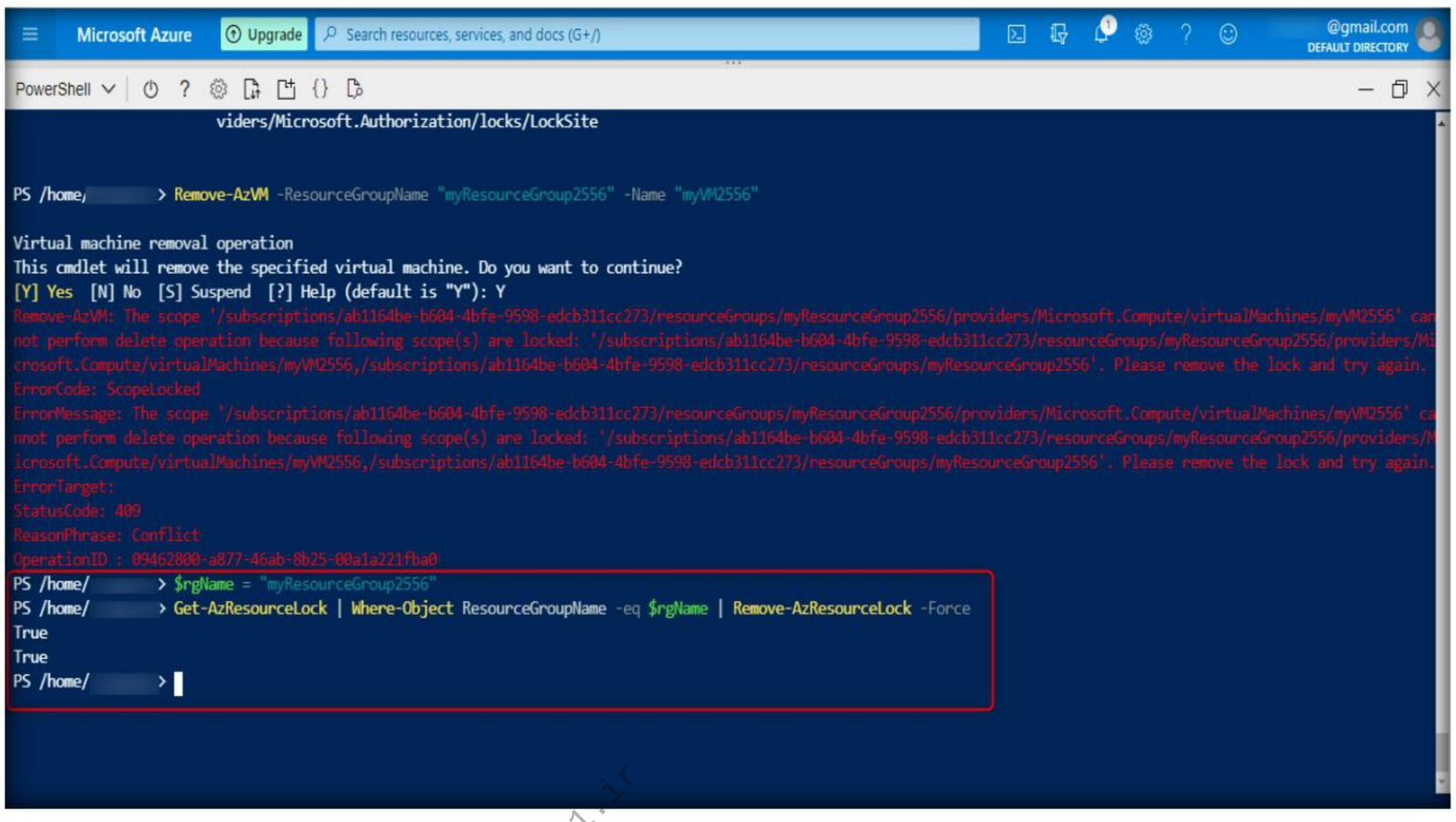


FIGURE 4.9.22: Deleting Lock of Resource Group

24. After removing the lock on the resource group, you can remove the VM, which was earlier not removed, since it was locked. Run the following command to delete the VM.

```
Remove-AzVM -ResourceGroupName
"myResourceGroup2556" -Name "myVM2556"
```

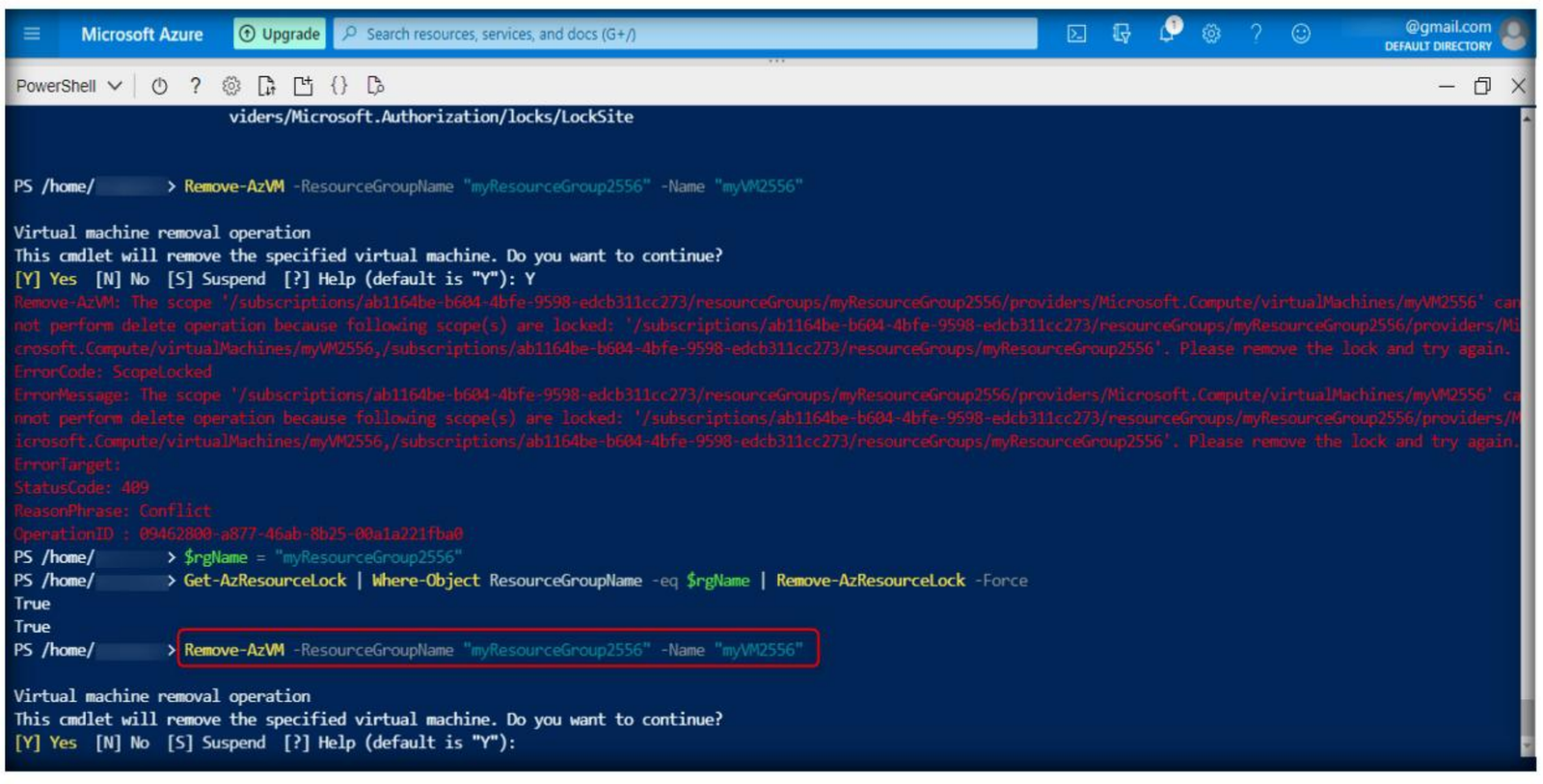


FIGURE 4.9.23: Removing the VM

hidn01.ir

Certified Cloud Security Engineer Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

25. Type **Y** and press **Enter** to confirm the removal of the virtual machine. You will see that the VM gets successfully removed.

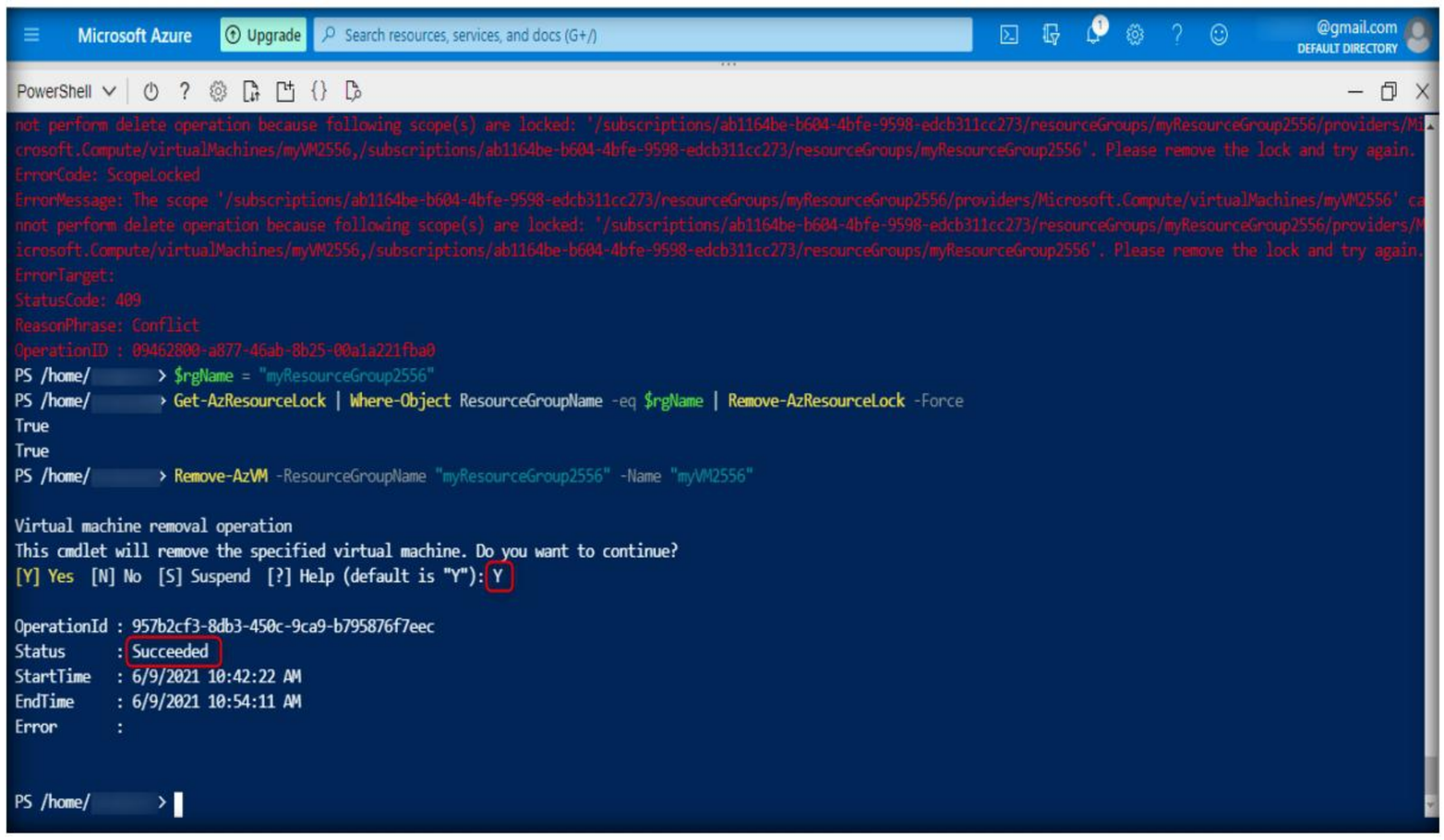


FIGURE 4.9.24: Successful Removal of the VM

26. Thus, a cloud security engineer can prevent the accidental deletion of critical resources in Azure by locking the resource and resource group.

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

27. From the Azure portal, navigate to Resource groups and click on the name of the resource group (myResourceGroup2556). In the Overview window for the resource group, click on Delete resource group at the top.

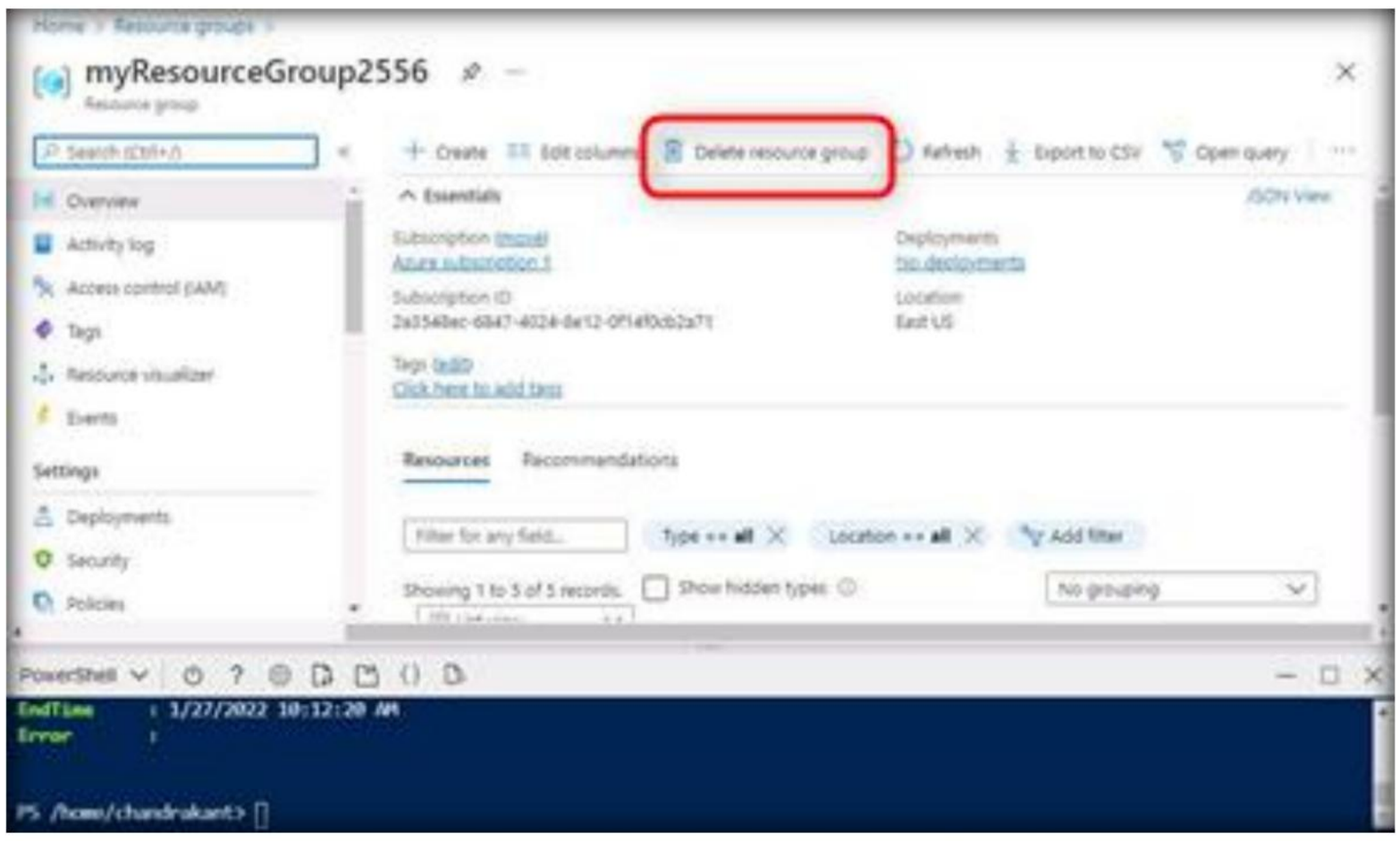


FIGURE 4.9.25: Deleting Resource Group

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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.

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 10

Restricting Network Access to Azure Storage Account Using Virtual Network Service Endpoints

Virtual network service endpoints offer a direct and secure connection to Azure services using an optimized route over the Azure backbone network.

ICON KEY

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

Lab Scenario

Virtual network service endpoints limit network access to Azure service resources in a virtual network subnet. To safeguard an Azure storage account from unauthorized access, you can restrict network access using virtual network service endpoints.

Lab Objectives

In this lab, you will learn how to create a resource group, virtual network, network security group, and Azure storage account, and also to create a file share, restrict network access to a subnet, create a VM, etc.

In this lab you will:

- Create a resource group
- Create a virtual network
- Enable a service endpoint
- Restrict network access for a subnet
- Create an Azure storage account
- Create a file share in Azure storage account
- Restrict network access to a subnet
- Create virtual machines
- Confirm access to a storage account
- Confirm a denied access to a storage account

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Environment

To perform this lab, you need the following:

- Admin Machine VM
- Registered Microsoft Azure account

Lab Duration

Time: 30 minutes

Overview of Virtual Network Service Endpoints

An Azure virtual network service endpoint helps Azure resources connect and communicate directly and securely over the Azure backbone (instead of connecting over the Internet). A cloud security administrator can use the virtual network service endpoints to secure and directly connect the Azure service resources through an optimized route in the Azure backbone.

In a virtual network, the service endpoints enable the private IP addresses to reach the Azure service's endpoint, ruling out the need for a public IP address. An administrator can restrict the service resource to accept traffic only from a subnet linked to the service endpoint. Using a network security group (NSG), the administrator can lock down or restrict the virtual network to only allow outbound traffic to the desired Azure service and block all other outbound traffic.

hide01.ir

Suppose a VM in a virtual network wants to communicate with a storage account in Azure. The administrator can club the storage account, a service endpoint, and NSG to ensure the traffic from a VM in a private subnet does not use the Internet to reach the storage account. All traffic to the storage account is blocked unless it is from this subnet and outbound traffic to the Internet from this subnet is restricted by NSG.

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 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.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1

Creating a Resource Group

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

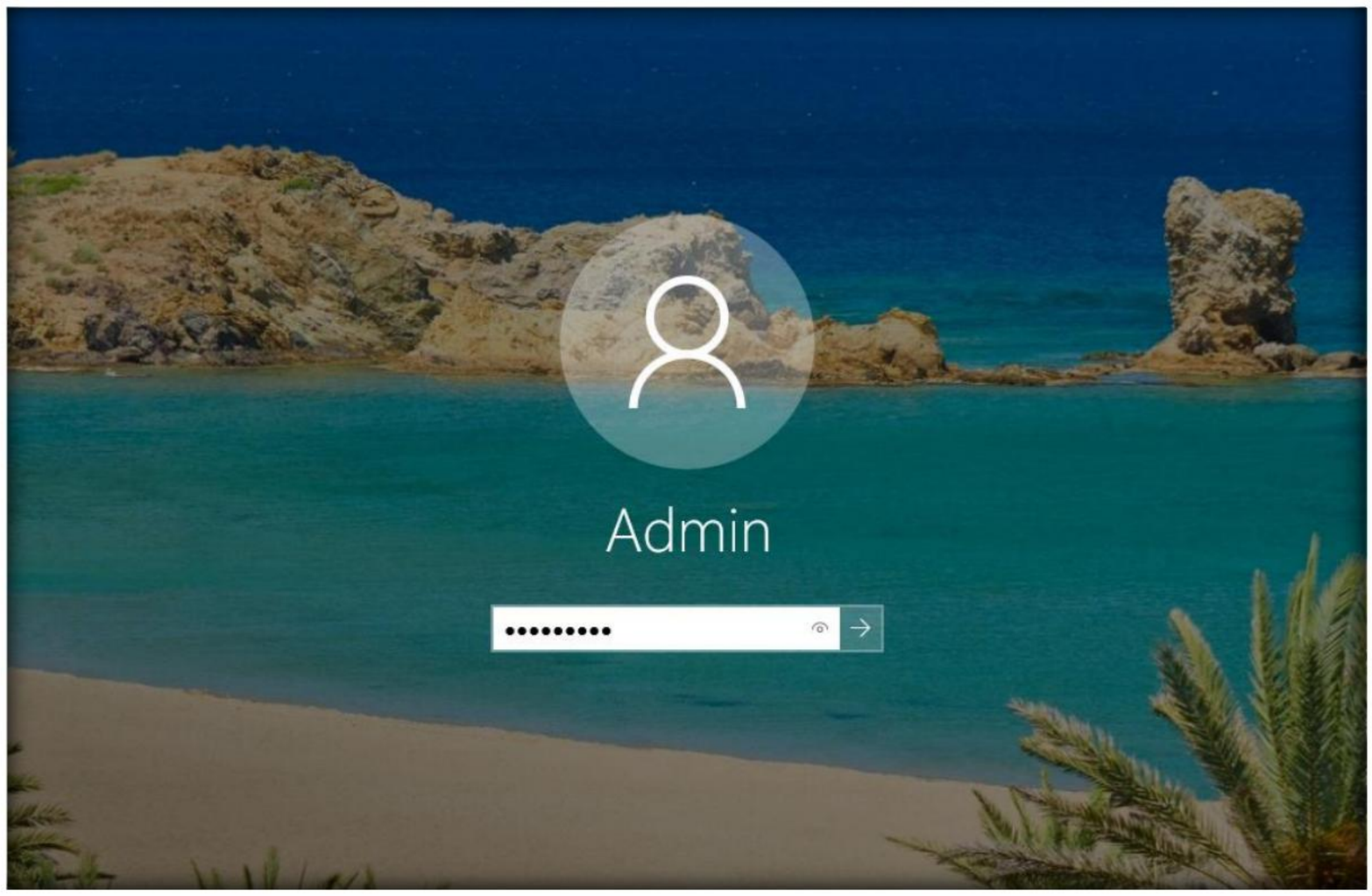


FIGURE 4.10.1: Launch Admin Machine and Log in

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

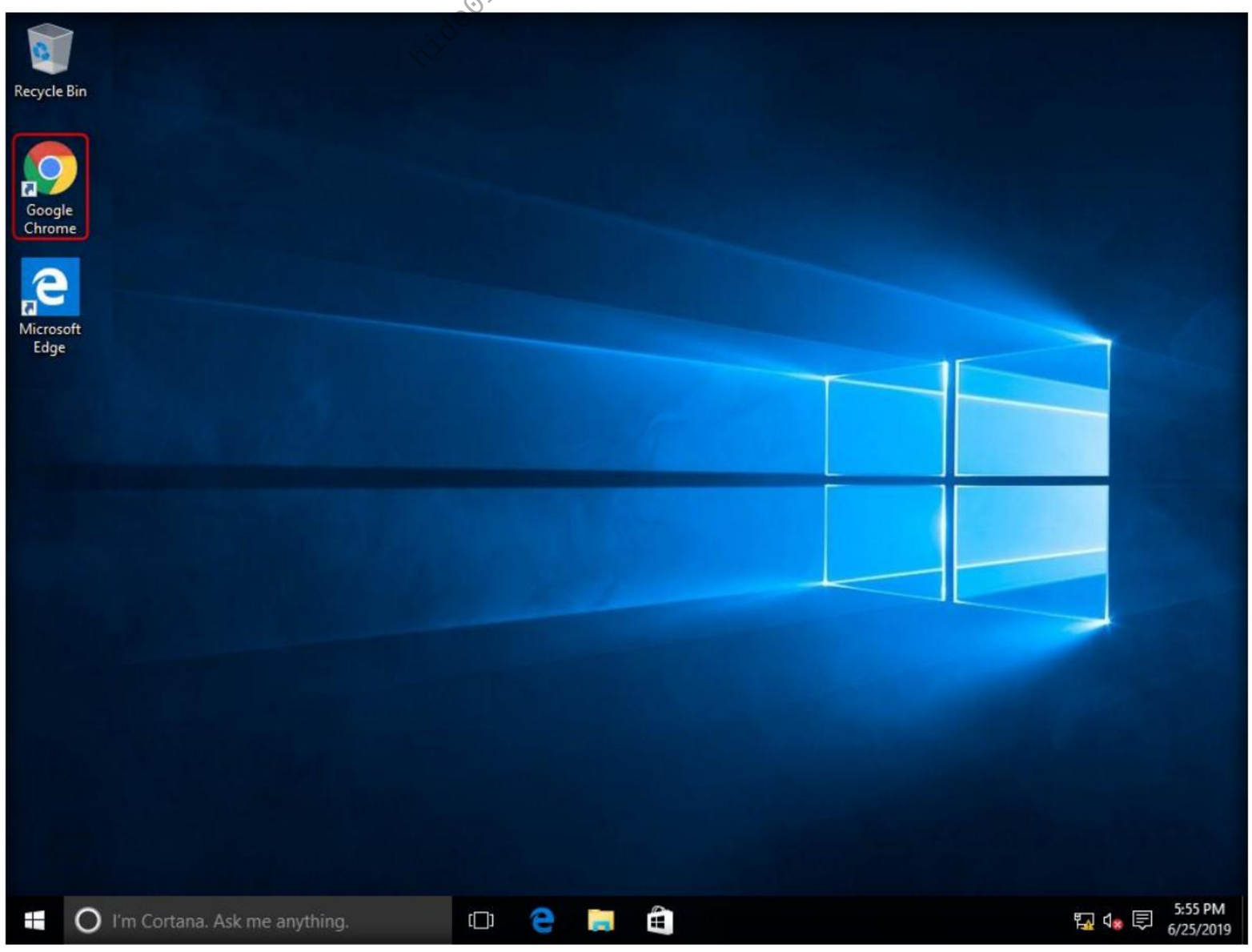


FIGURE 4.10.2: Navigating to the Chrome Browser from Taskbar

Certified Cloud Security Engineer Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

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

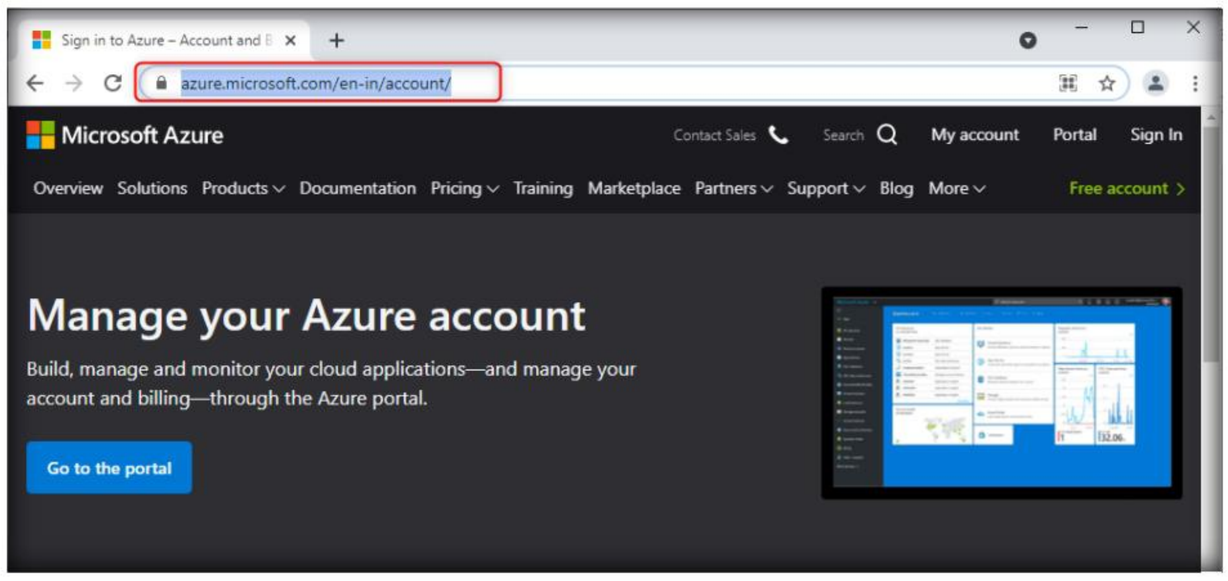


FIGURE 4.10.3: Entering the URL of Microsoft Azure

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

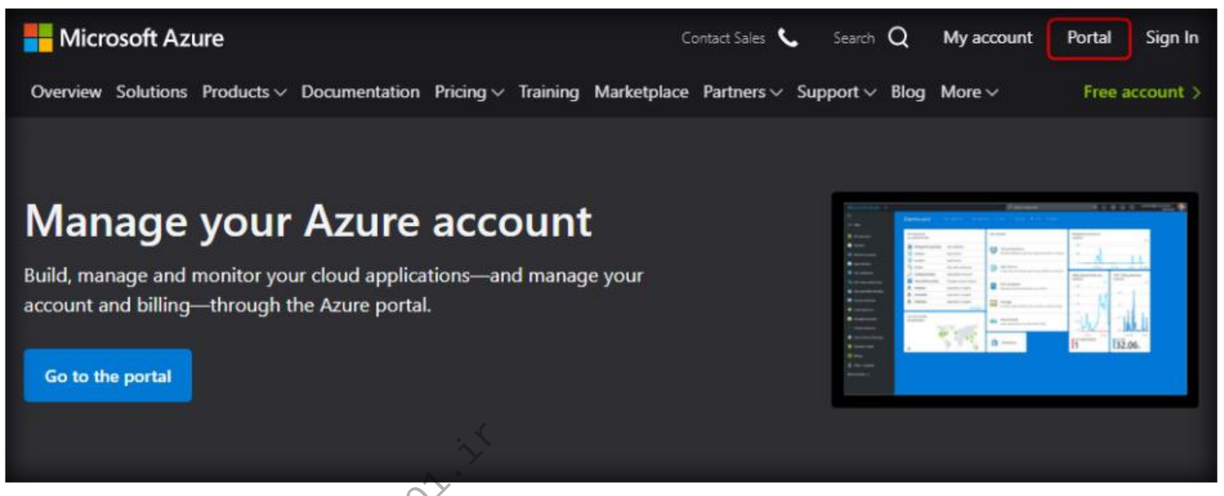


FIGURE 4.10.4: Sign in to Azure Portal

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

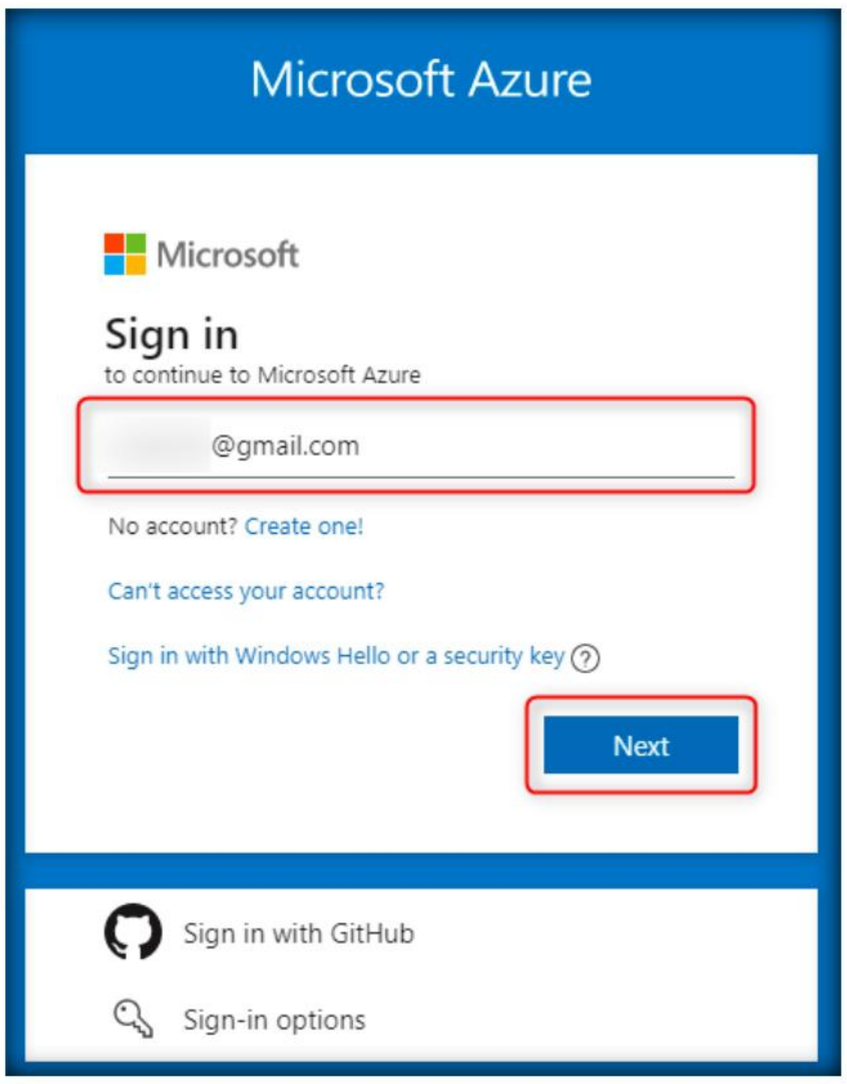


FIGURE 4.10.5: Entering Account ID to continue

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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

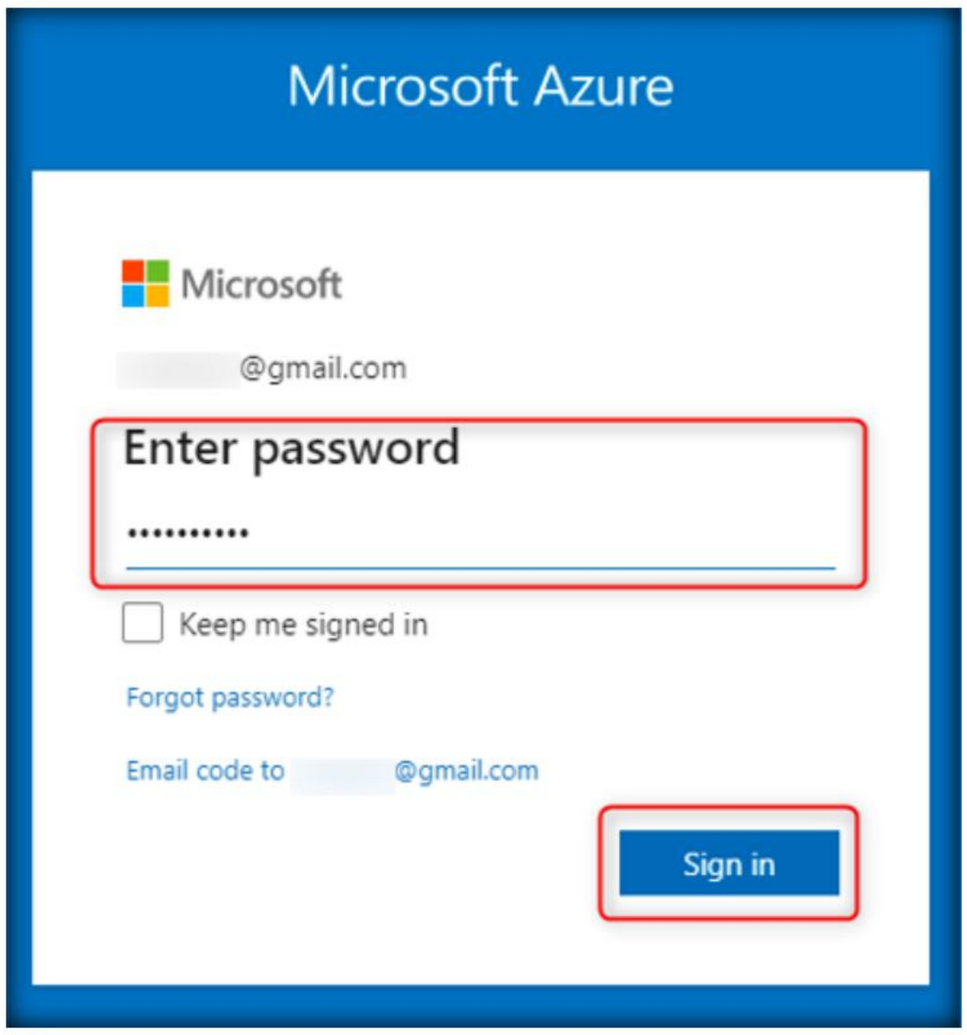


FIGURE 4.10.6: Sign in to Azure Account

7. You will be successfully logged in **Microsoft Azure portal**. Now, to create a resource group, click on **Resource groups**.

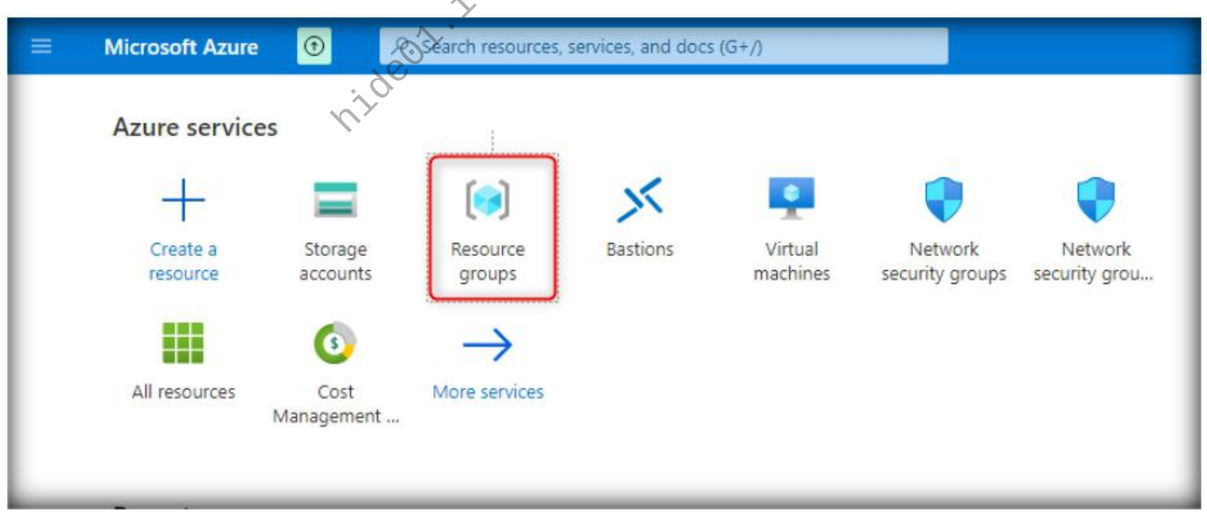


FIGURE 4.10.7: Selecting Resource Groups

8. In the **Resource groups** page, click on **+Add**.

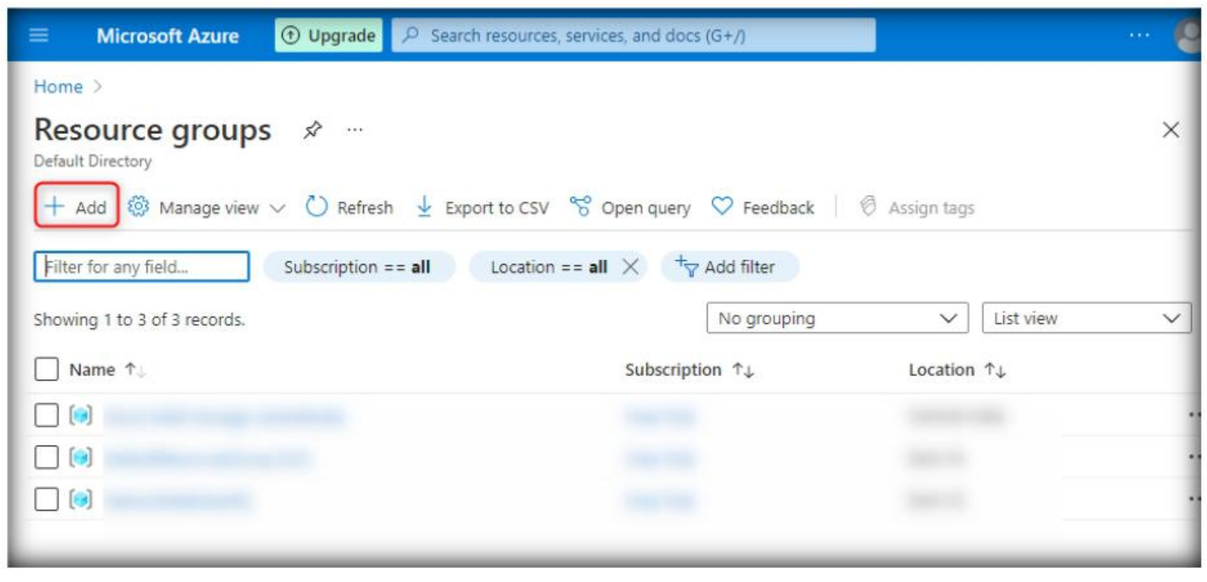


FIGURE 4.10.8: Adding New Resource Group

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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

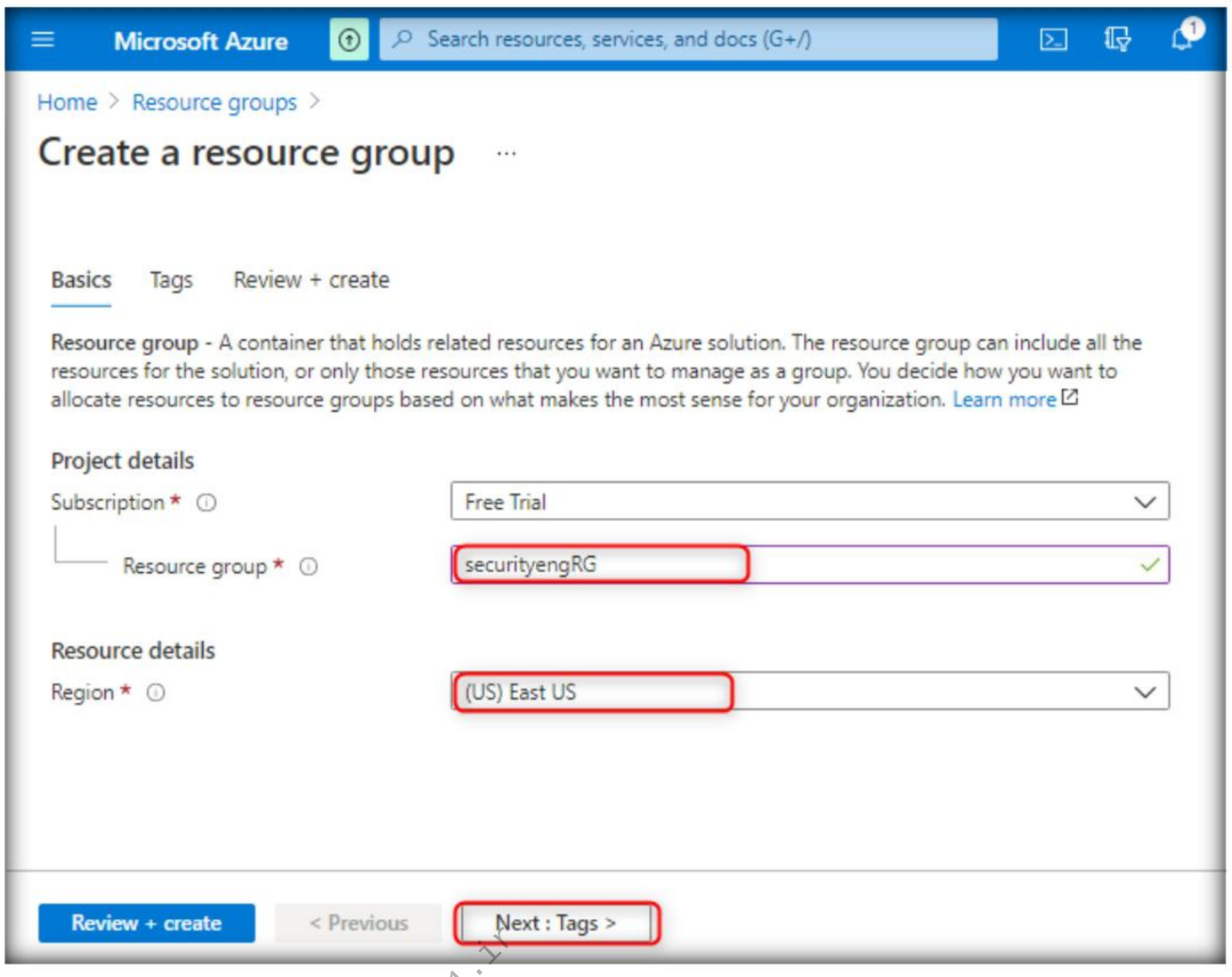


FIGURE 4.10.9: Entering Resource Group Name and Location

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

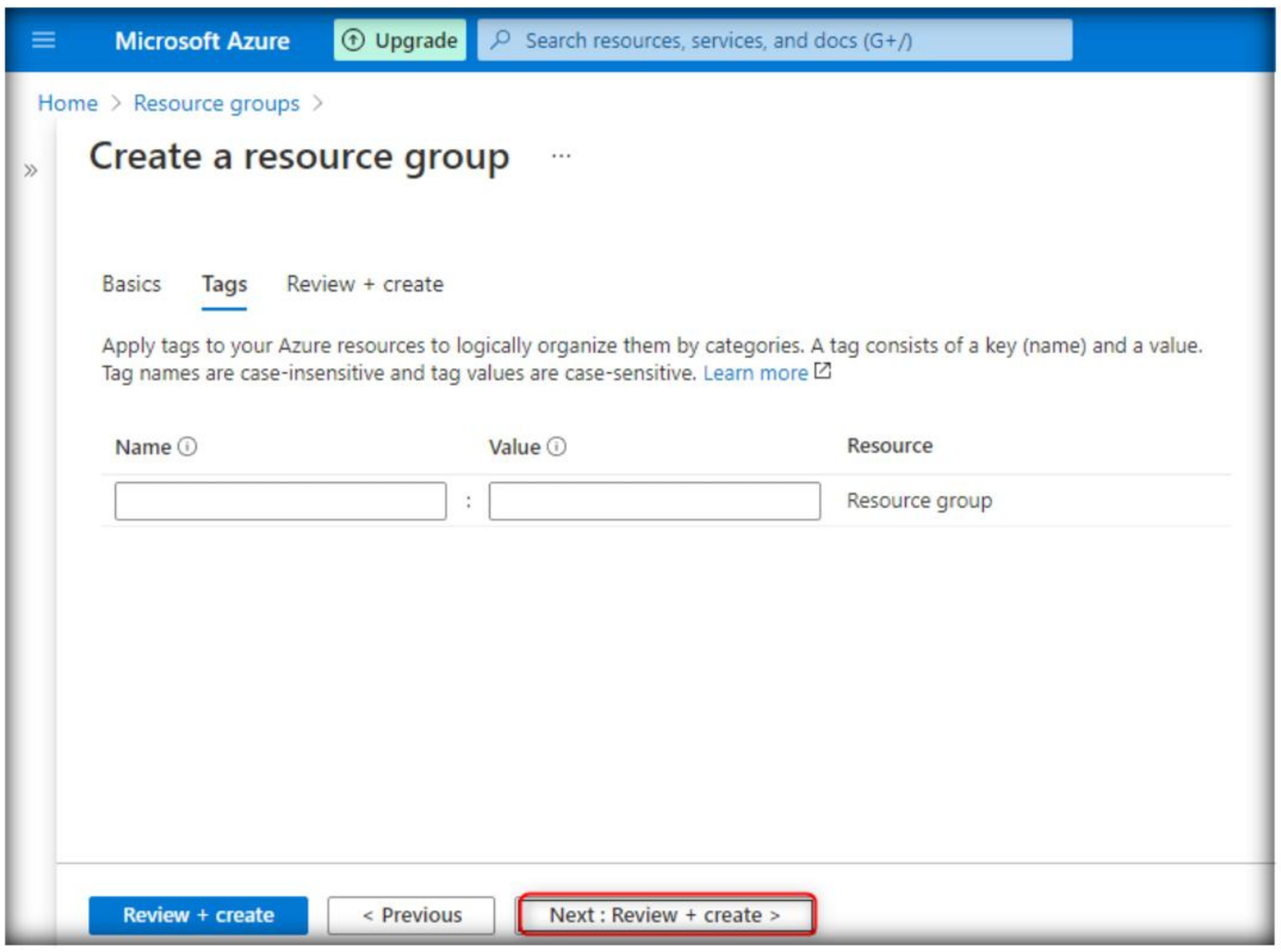


FIGURE 4.10.10: Leaving Tags Tab in Default State

Certified Cloud Security Engineer Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

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

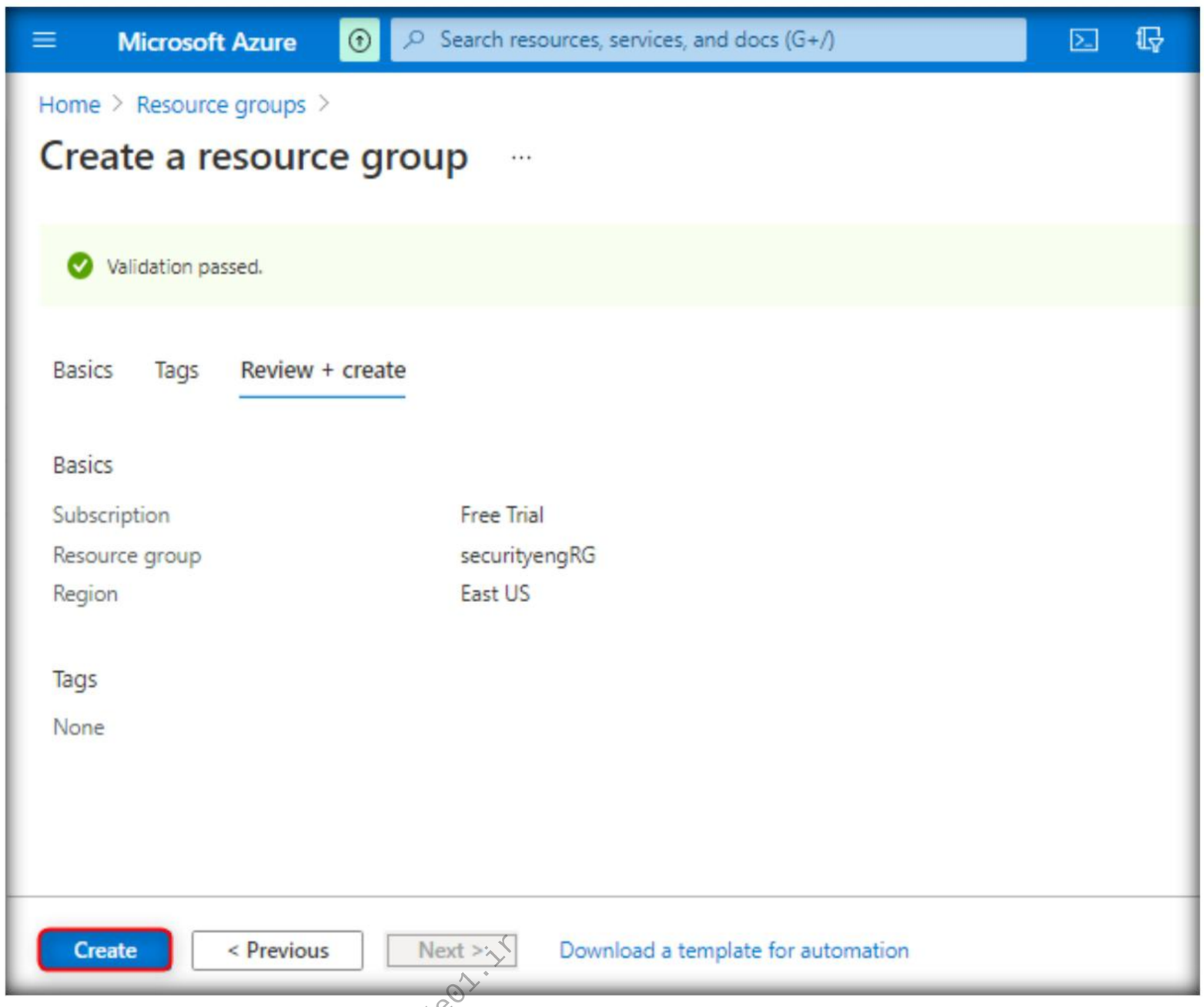


FIGURE 4.10.11: Validation Passed for Creating a Resource Group

12. The **securityengRG** resource group has been successfully created.

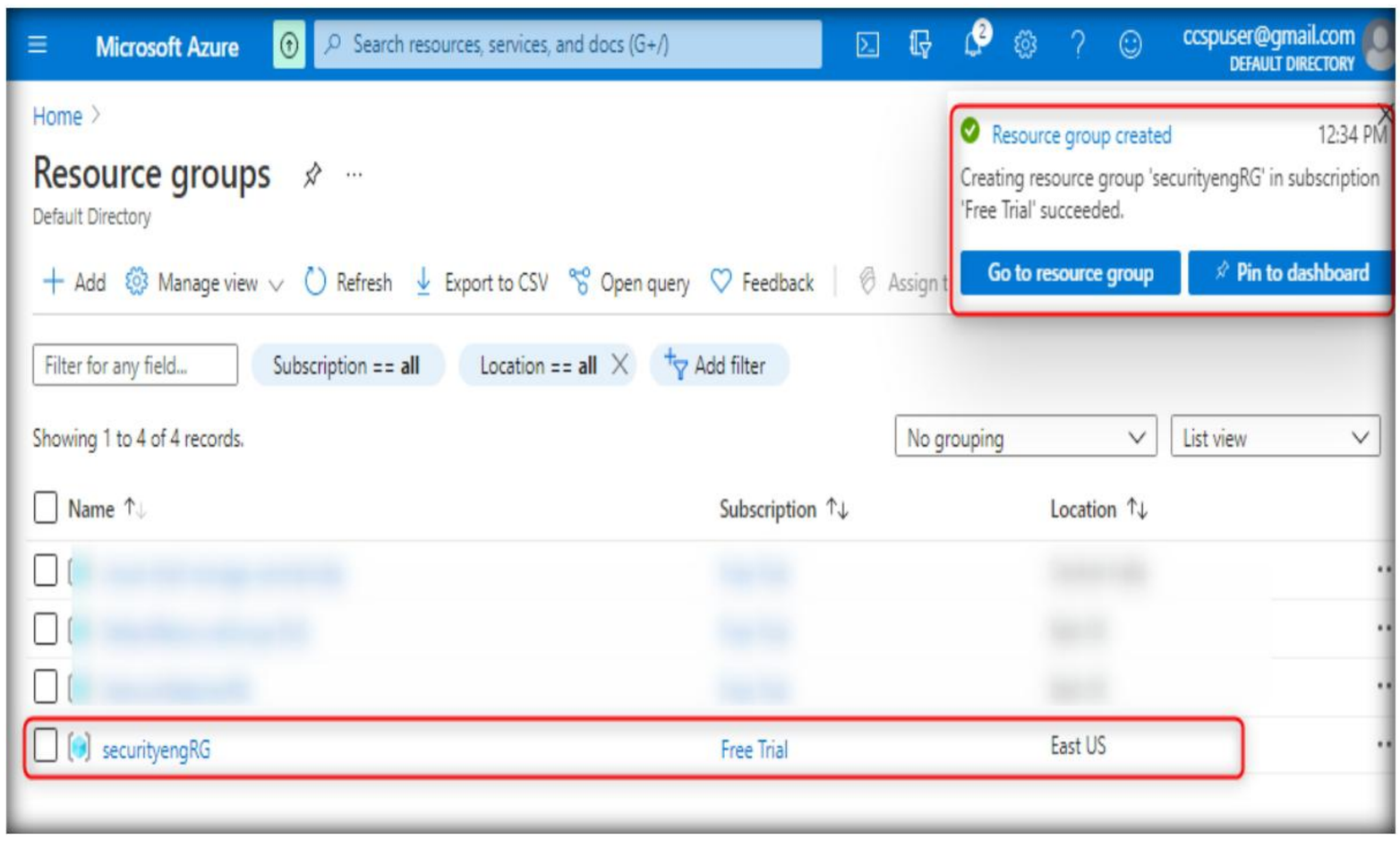


FIGURE 4.10.12: Successfully Creating Resource Group

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 2

Create a Virtual Network

13. Next, to create a virtual network in the resource group (**securityengRG**), go back to Azure portal, type **virtual networks** in the portal search box, and select **Virtual networks**.

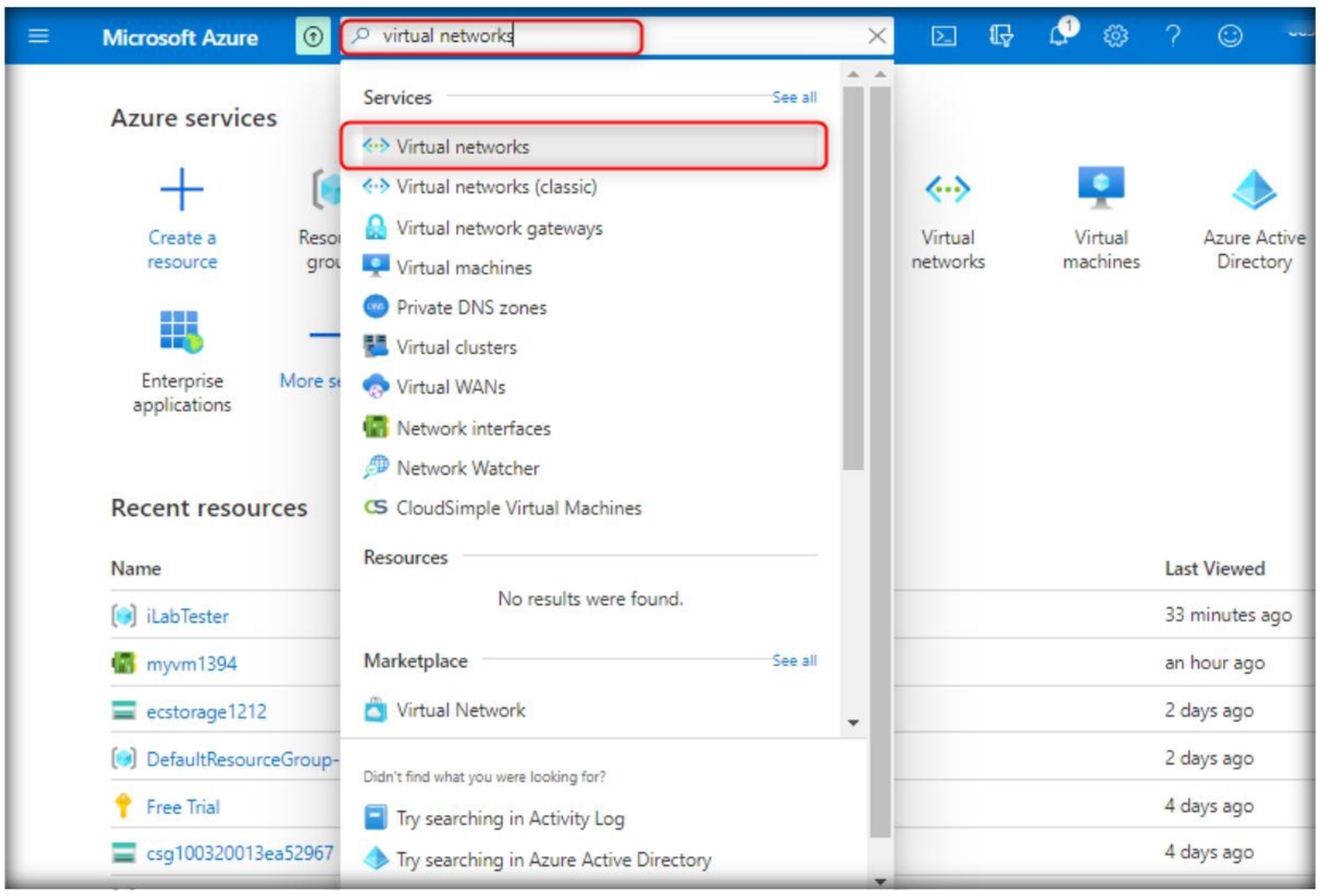


FIGURE 4.10.13: Selecting Virtual Network in Azure Portal

14. In the **Virtual networks** window, click on the **Create virtual network** button.

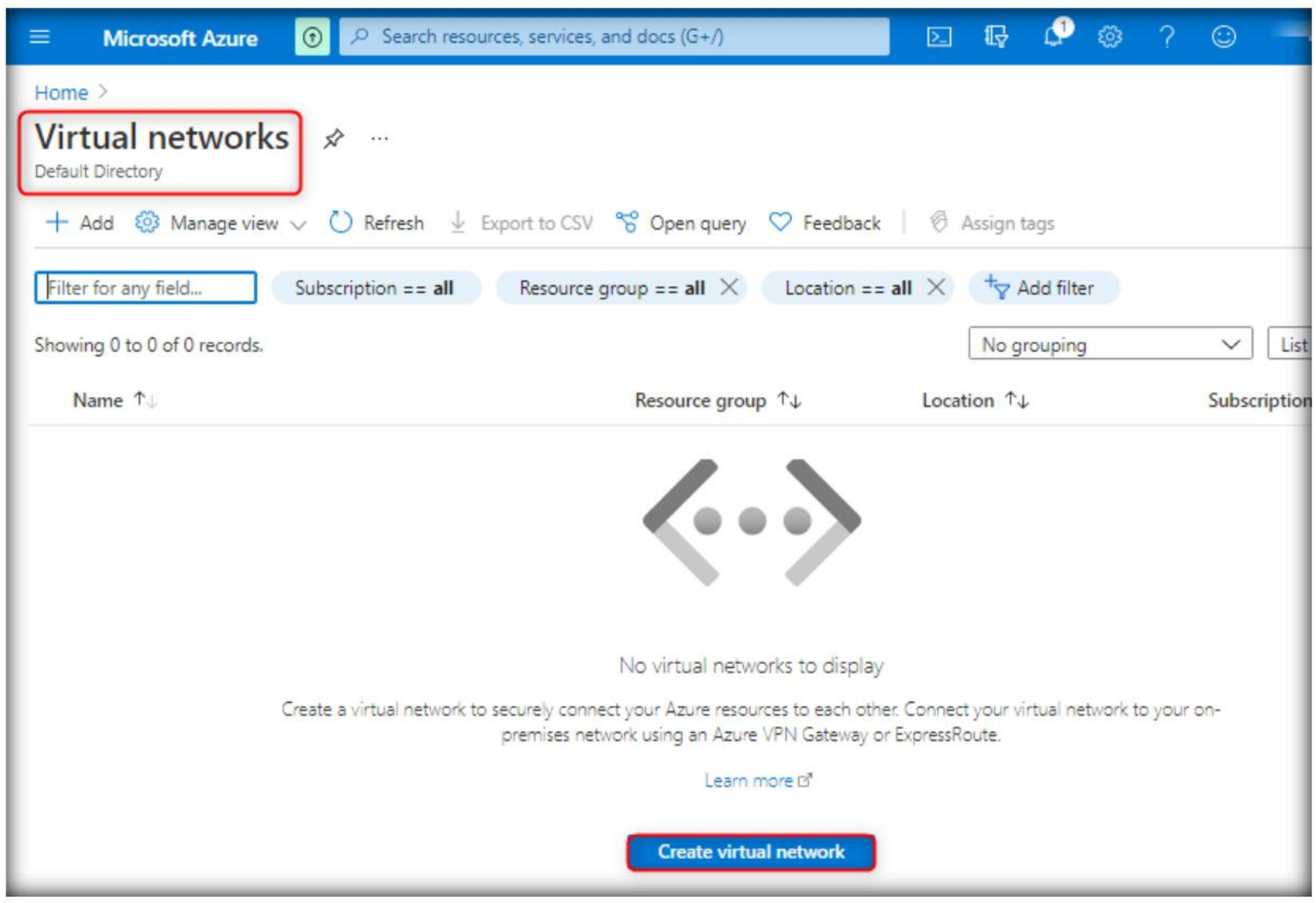


FIGURE 4.10.14 Creating a New Virtual Network

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

15. In the **Create virtual network** window, select the **Resource group** (here, we have selected **securityengRG**) and enter the name of the virtual network in the **Name** field (here, we have used **SecEng-VNET**). Then, click on **Next: IP Addresses >**.

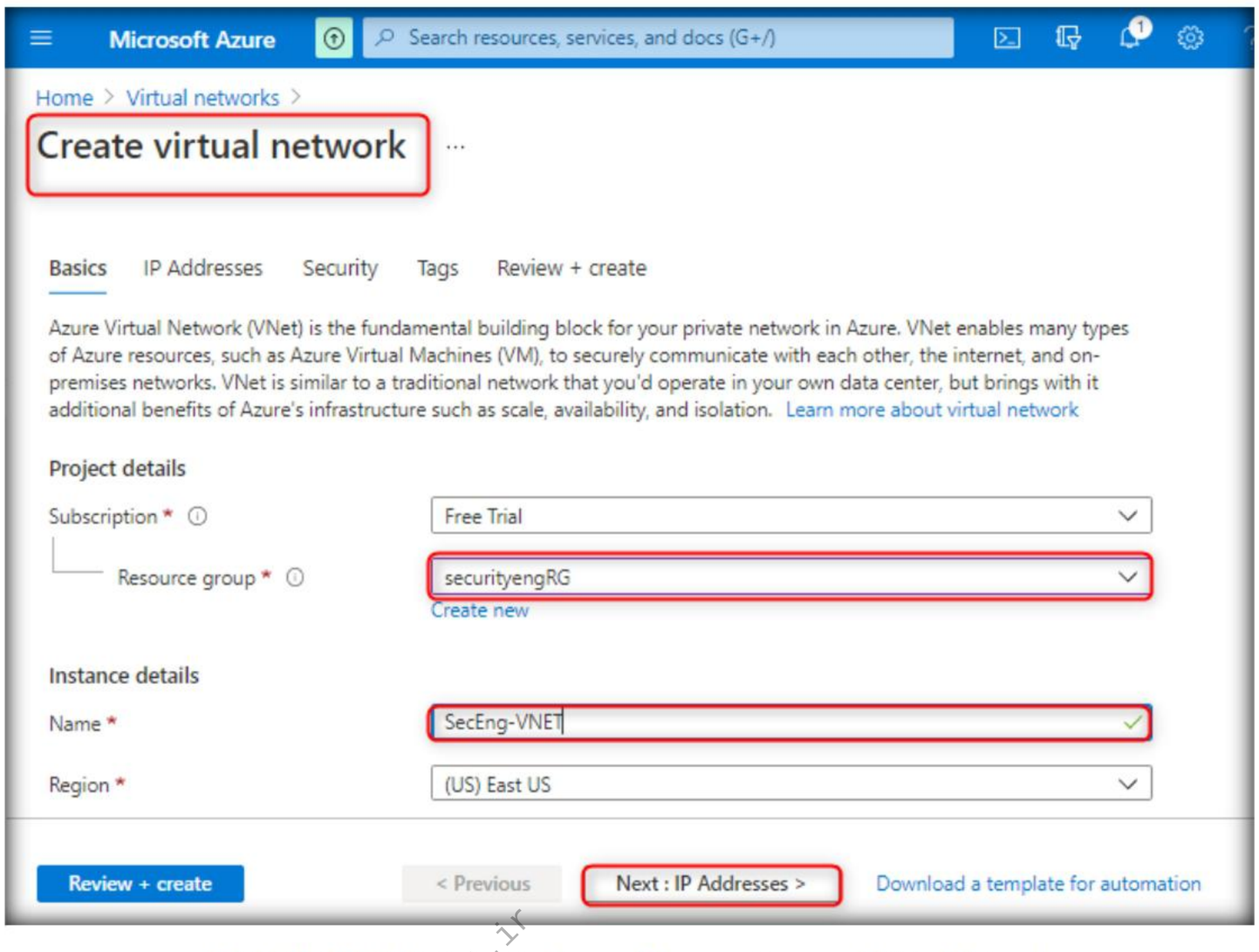


FIGURE 4.10.15: Entering the Name of Resource Group and Virtual Network

16. Keep **IP4 address space** as **4.12.0.0.0/16**. In the **IP addresses** tab, select the **default** option. An **Edit subnet** pane will open on the left side. Enter the Subnet name as **Public,** leave everything else in their default state, and then click on the **Save** button.

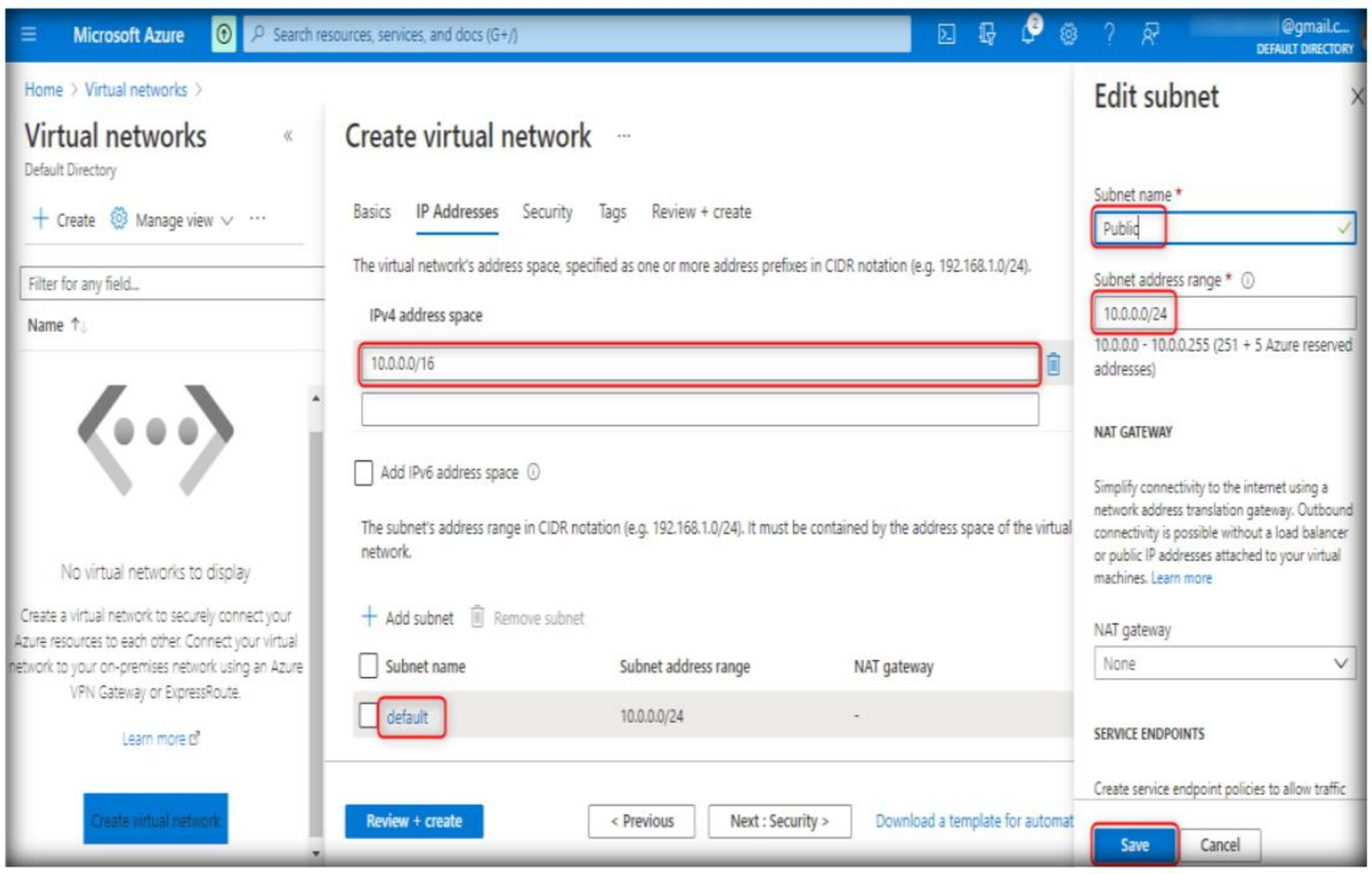


FIGURE 4.10.16: Entering Subnet Details

17. Click on the **Next: Security >** button.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

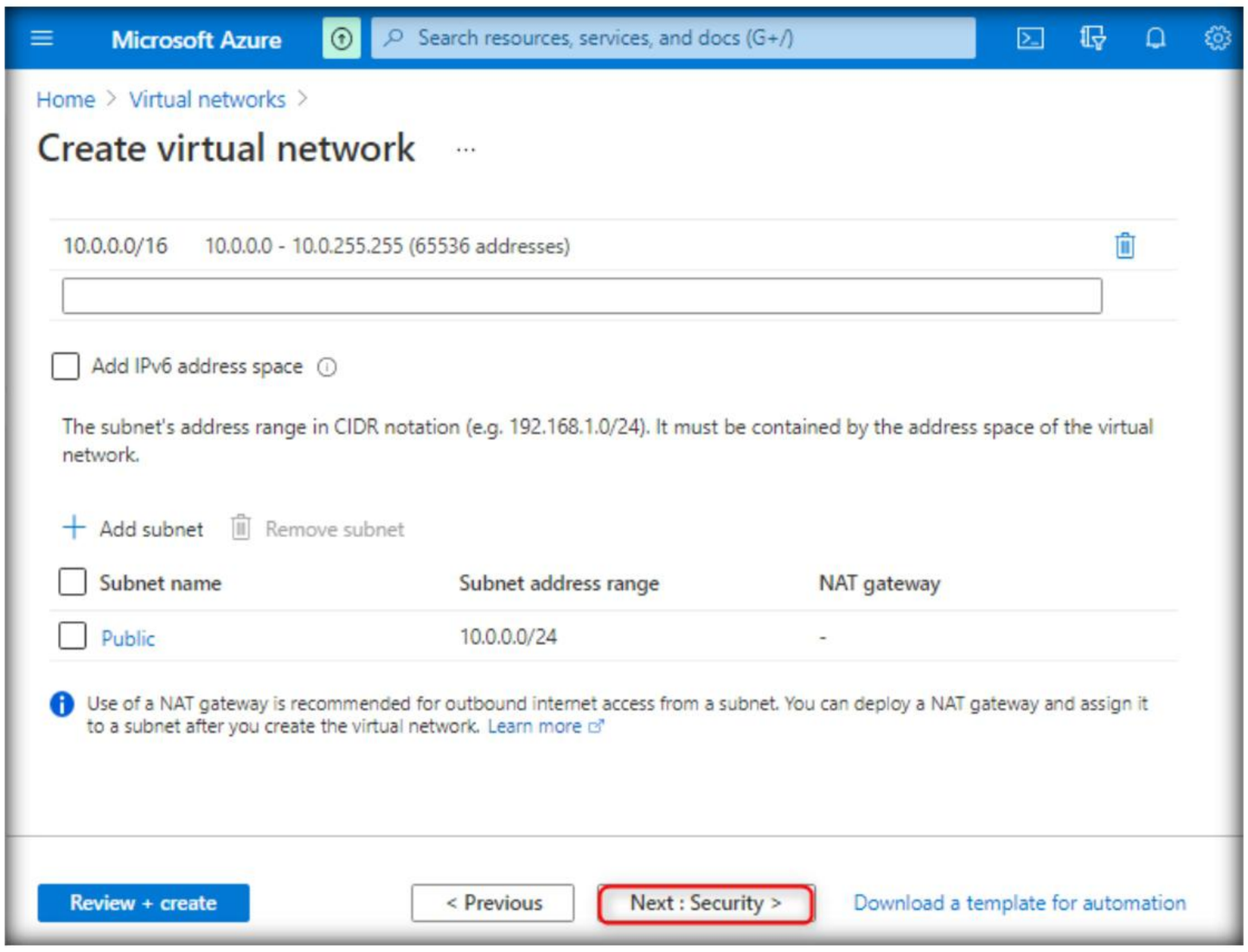


FIGURE 4.10.17: Selecting Security Button

18. In the Security tab, leave everything in their default state, and click on the **Next: Tags >** button.

hide01.ir

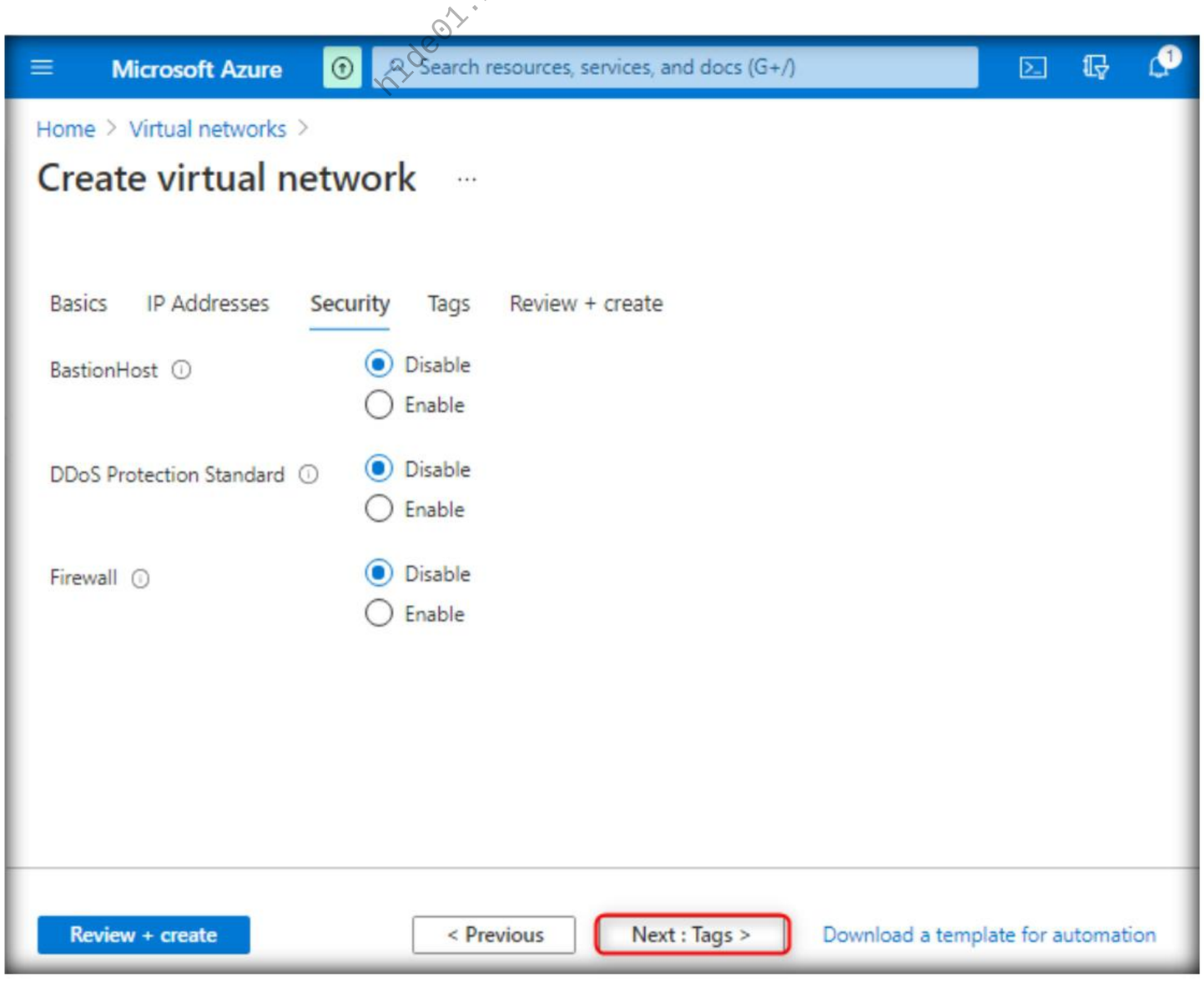


FIGURE 4.10.18: Leaving Security Tab in Default State

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

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



FIGURE 4.10.19: Leaving Tags Tab in Default State

Certified Cloud Security Engineer Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

20. After seeing the **Validation passed** message, click on the **Create** button.

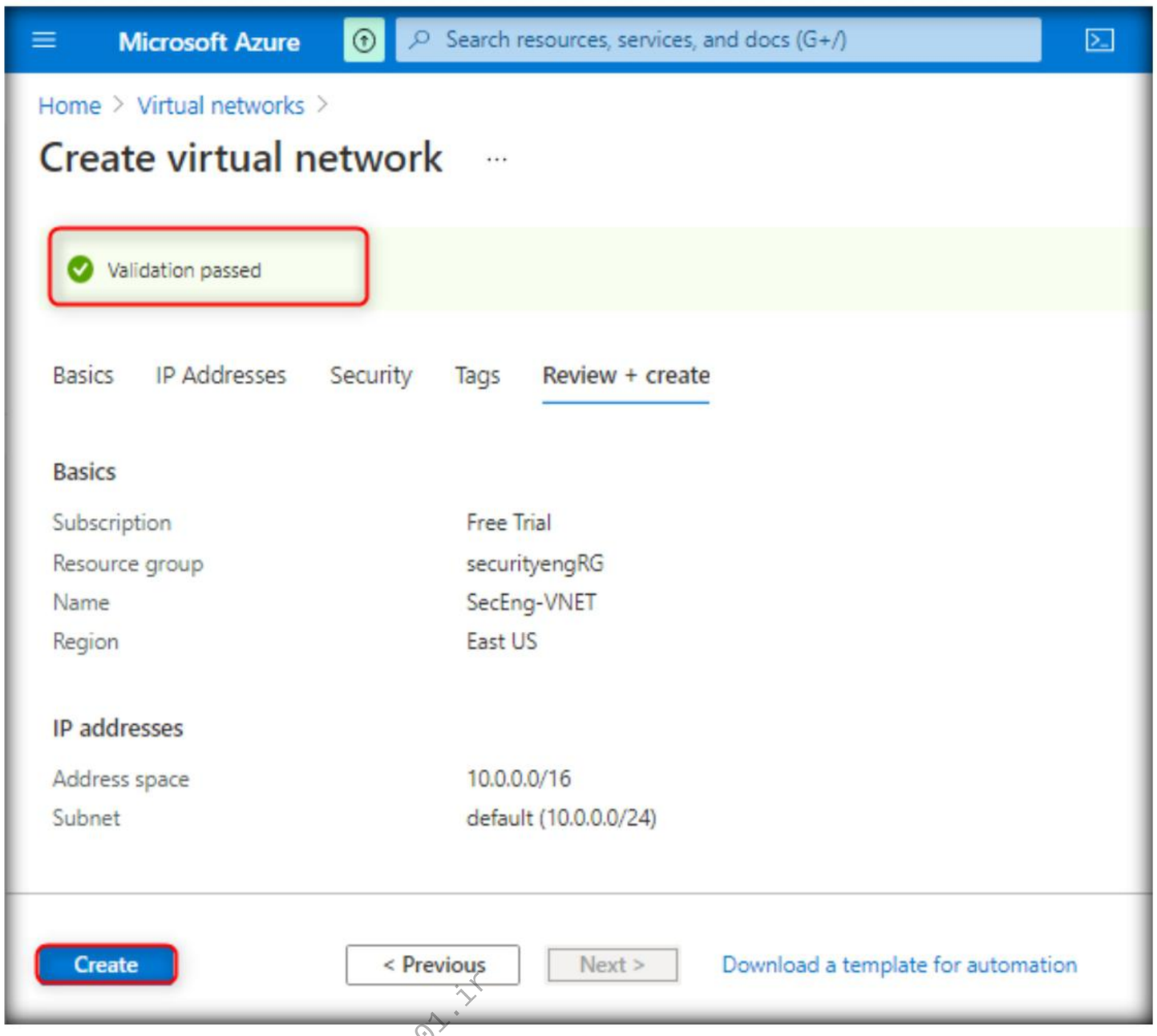


FIGURE 4.10.20: Creating a Virtual Network after Passing the Validation

hi1e01.ir

21. After the successful deployment of the virtual network, click on the **Go to resource** button.

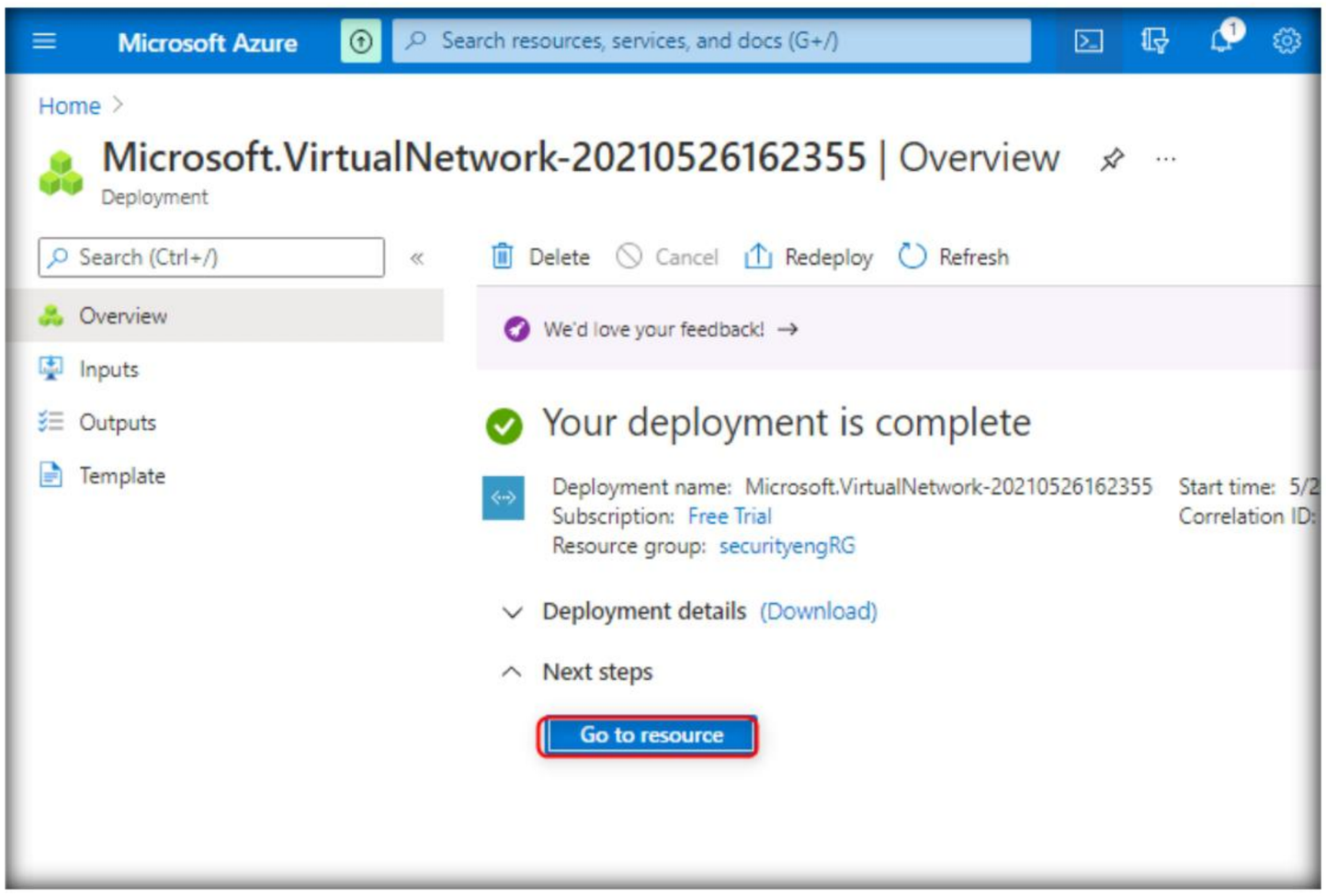


FIGURE 4.10.21: Successful Deployment of Virtual Network

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 3

Enable a Service Endpoint

22. A **SecEng-VNET** window will open. Here, navigate and click on **Subnets** under **Settings** to add a private subnet.

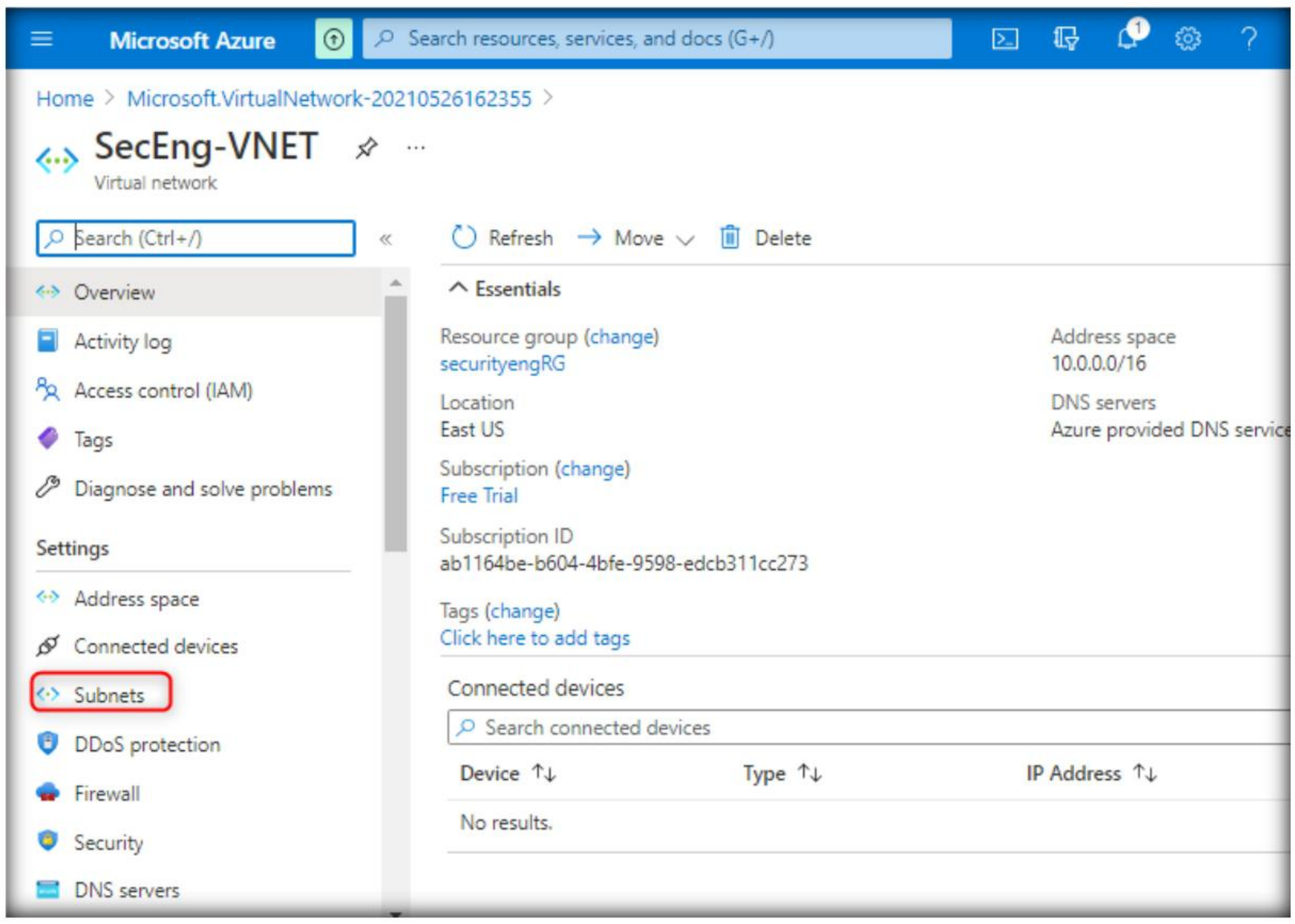


FIGURE 4.10.22: Selecting Subnets in SecEng-VNET

23. Click on **+ Subnet**. An **Add subnet** pane will open on the left side. Here, enter the **Name** of the Subnet as **Private**.

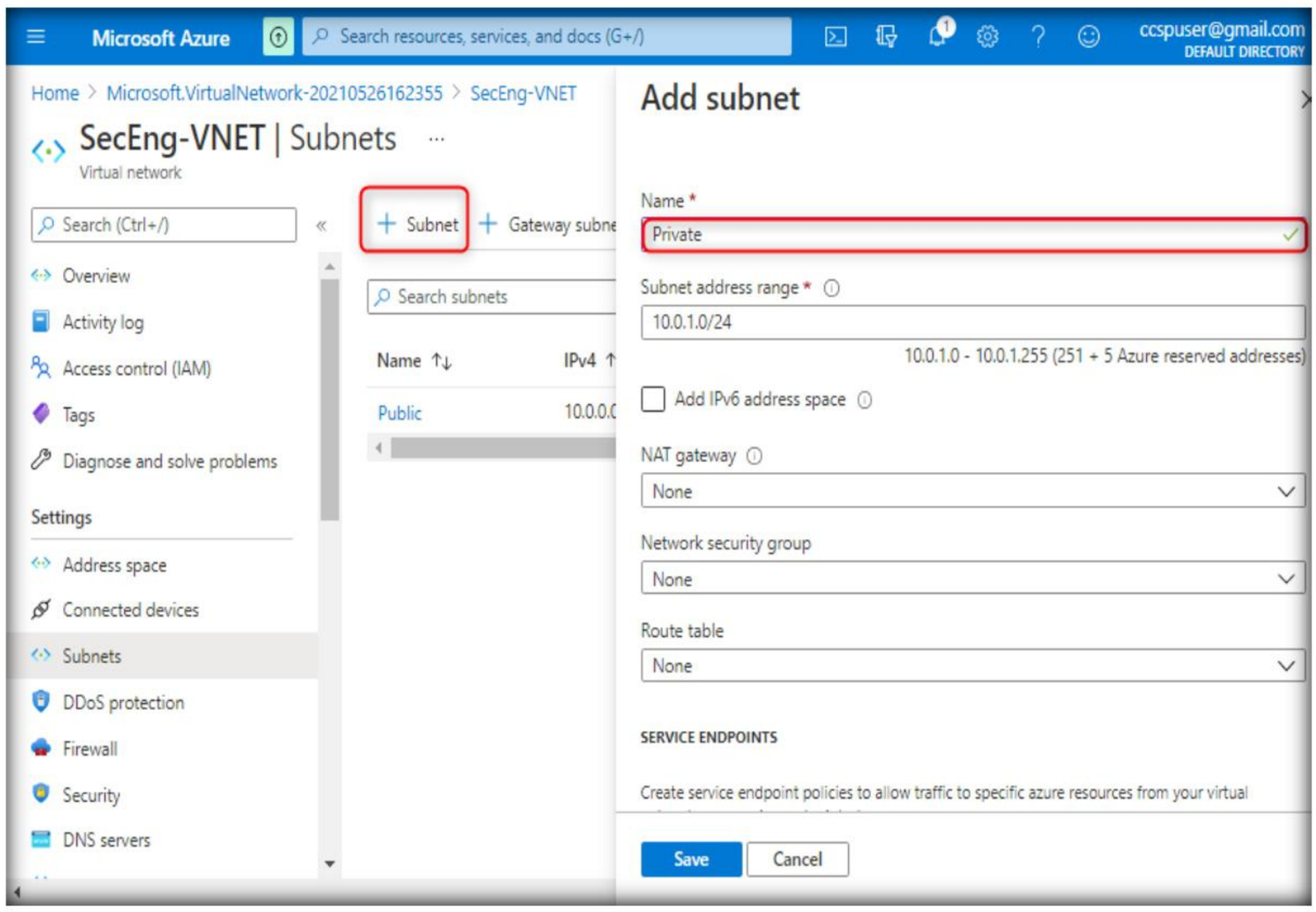


FIGURE 4.10.23: Adding Subnet Details

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

24. Leave the other fields in their default state. Under **SERVICE ENDPOINTS**, click on the **Services** dropdown and select **Microsoft.Storage**. Then, click on the **Save** button.

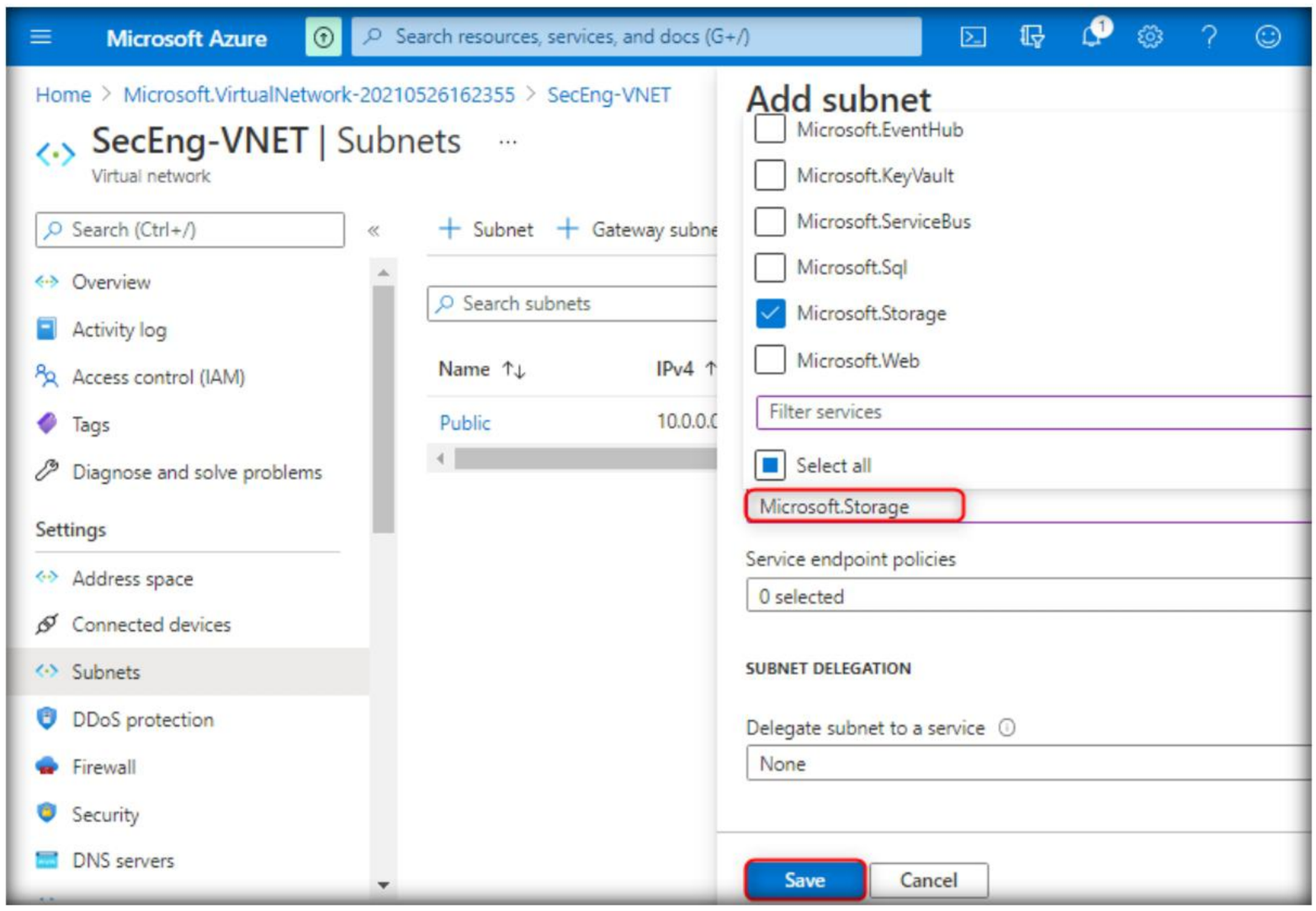


FIGURE 4.10.24: Selecting Service Endpoints

25. **Private** subnet is successfully added to the **SecEng-VNET** virtual network.

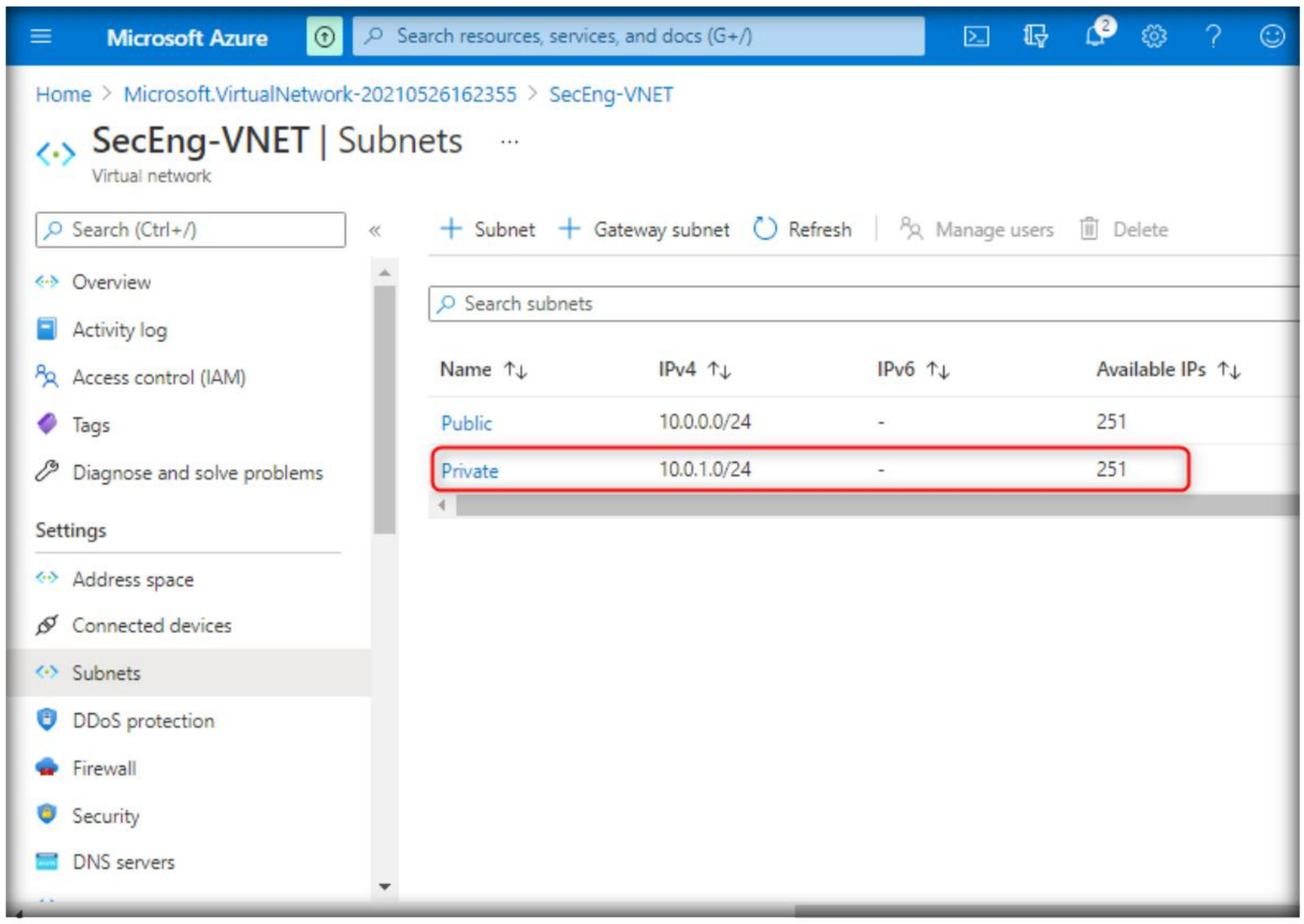


FIGURE 4.10.25: Addition of Private Subnet to SecEng-VNET

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 4

Restrict Network Access for a Subnet

26. Click on **Home** in the **SecEng-VNET** window to go back to Azure portal.

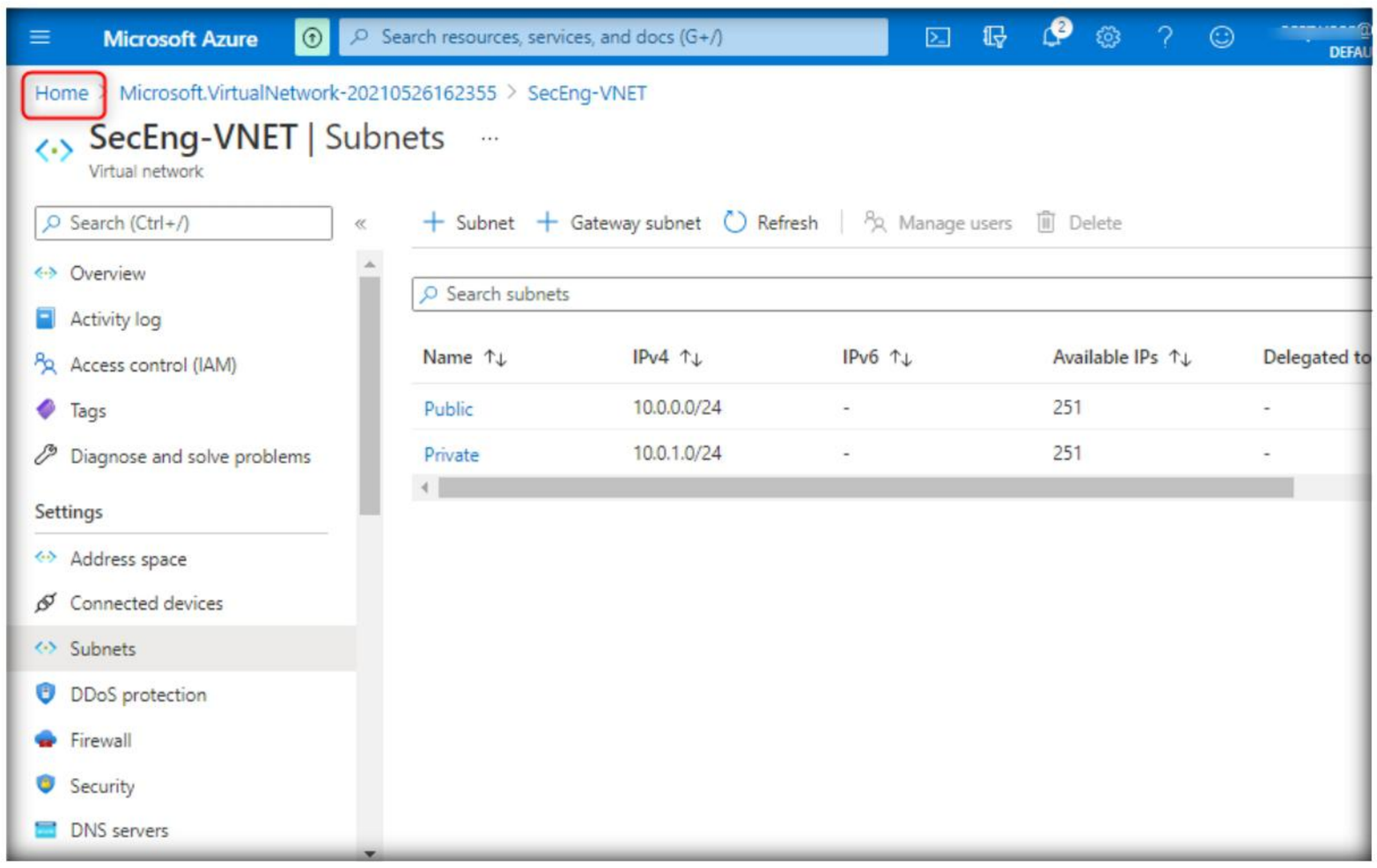


FIGURE 4.10.26: Going Back to Azure Portal

27. Now, to create a network security group, type **network security group** in the Azure portal search box and select **Network security groups**.

(**Note:** Do not select **Network security groups (classic)**)

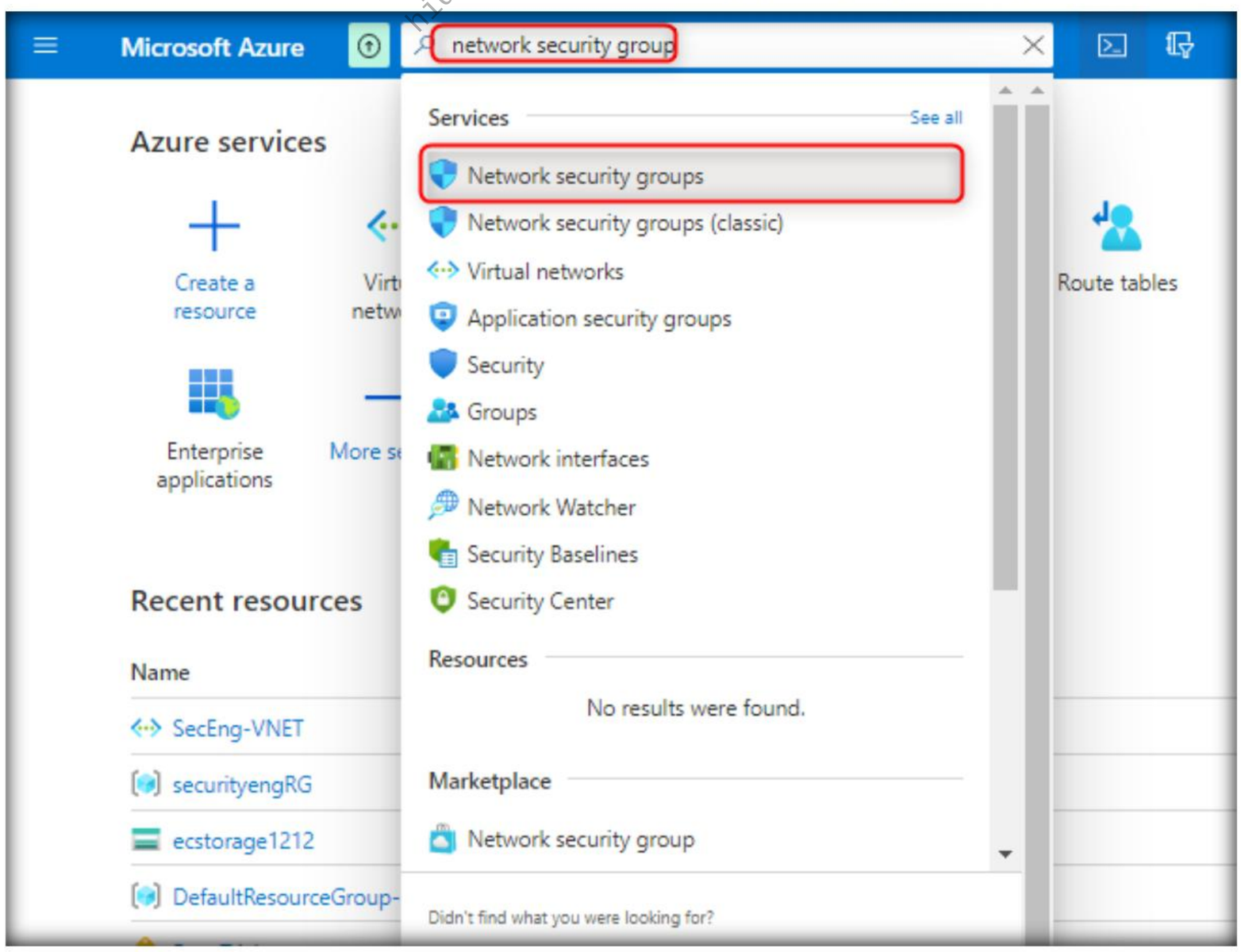


FIGURE 4.10.27: Selecting Network Security Groups

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

28. In the **Network Security groups** window, click on the **Create network security group** button.

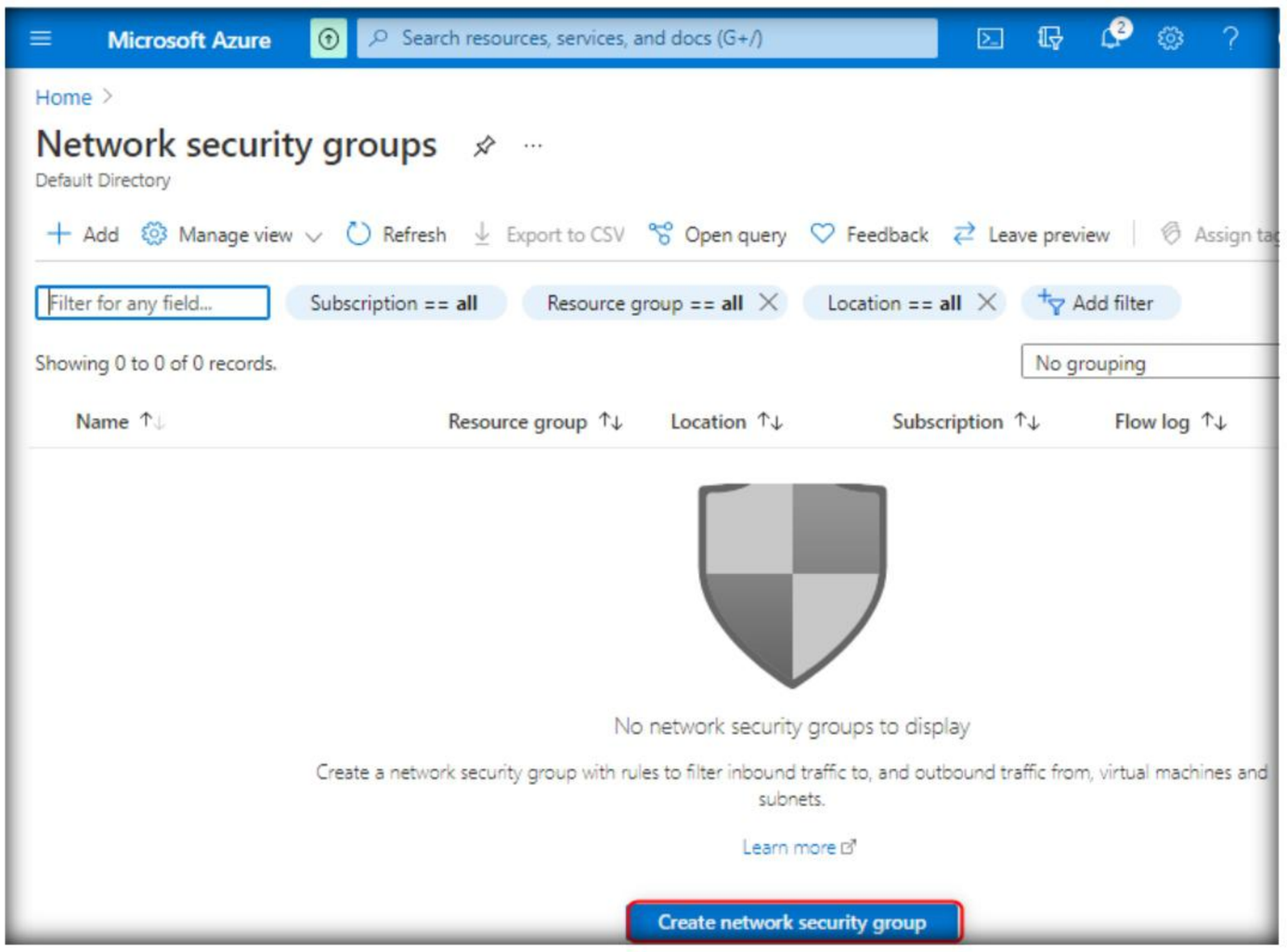


FIGURE 4.10.28: Creating Network Security Group

29. A **Create network security group** window will open. In the **Resource group** field, select **securityengRG** resource group from the dropdown. In the **Name** field, enter **SecEng-NSG**. Then, click on the **Next: Tags >** button.

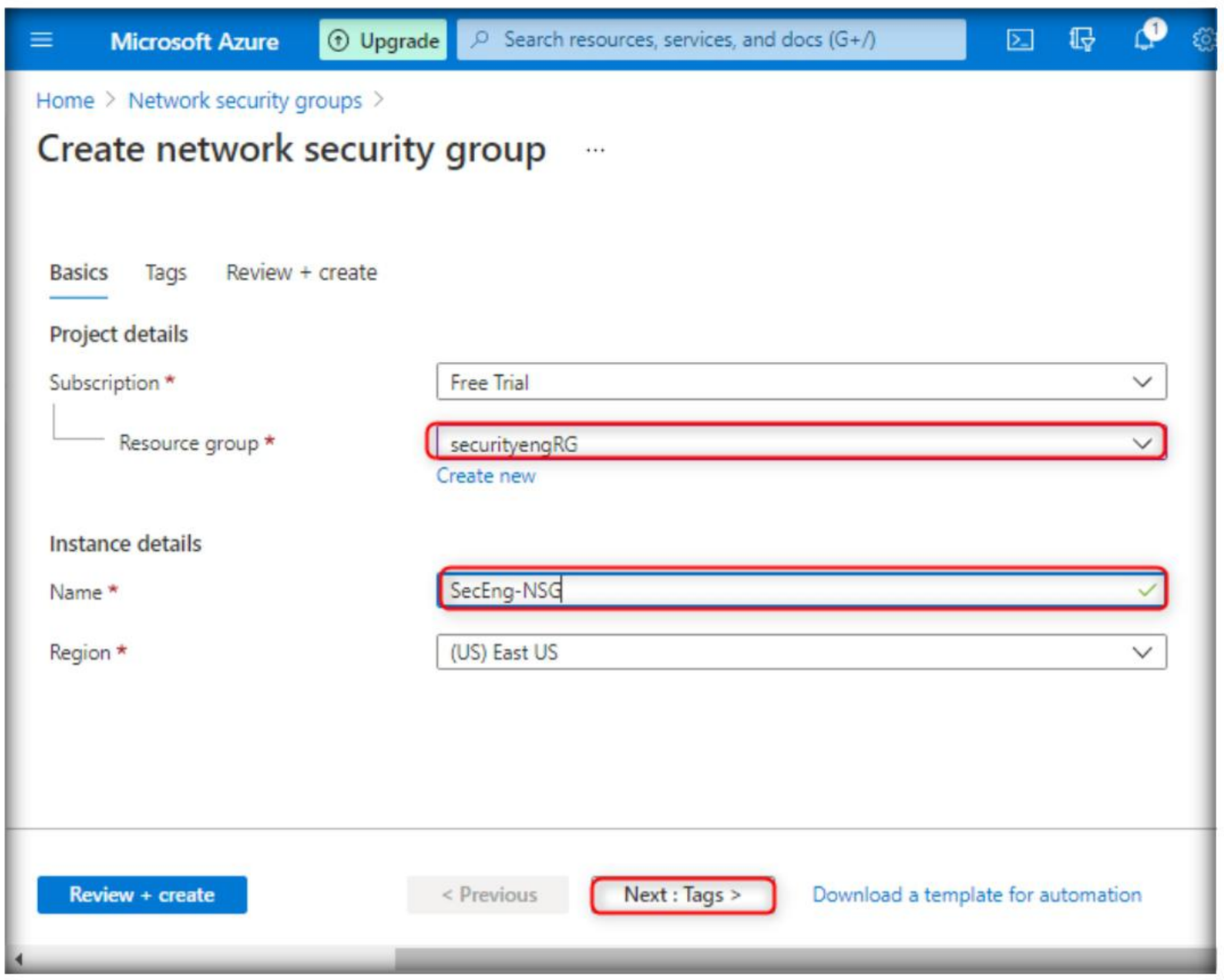


FIGURE 4.10.29: Selecting Resource Group and Entering the Name of the NSG

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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

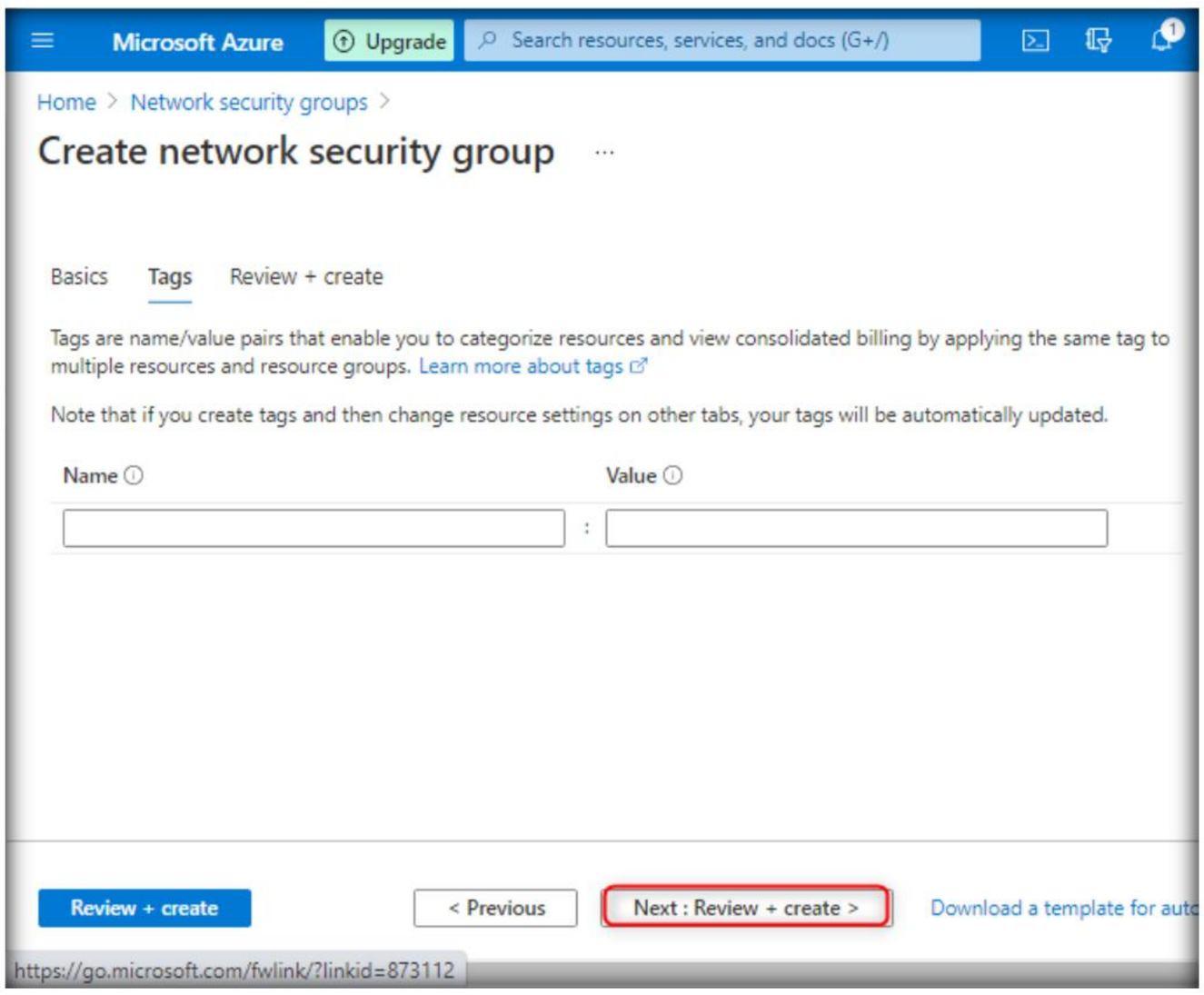


FIGURE 4.10.30: Leaving Tags Tab in Default State

31. After receiving the **Validation passed** message, click on the **Create** button.

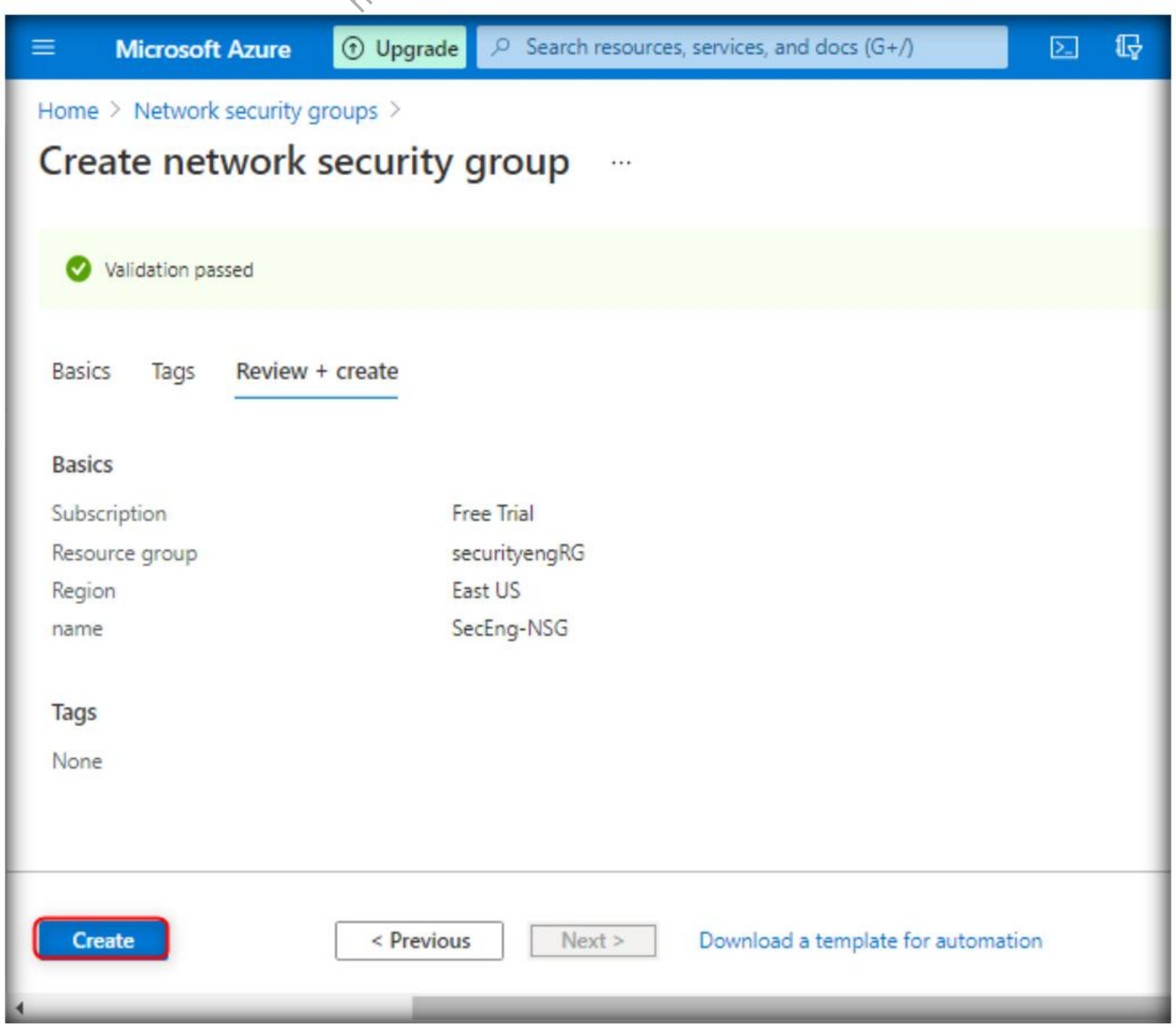


FIGURE 4.10.31: Creating Network Security Group

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

32. After a successful deployment of the network security group, click on the **Go to resource** button.

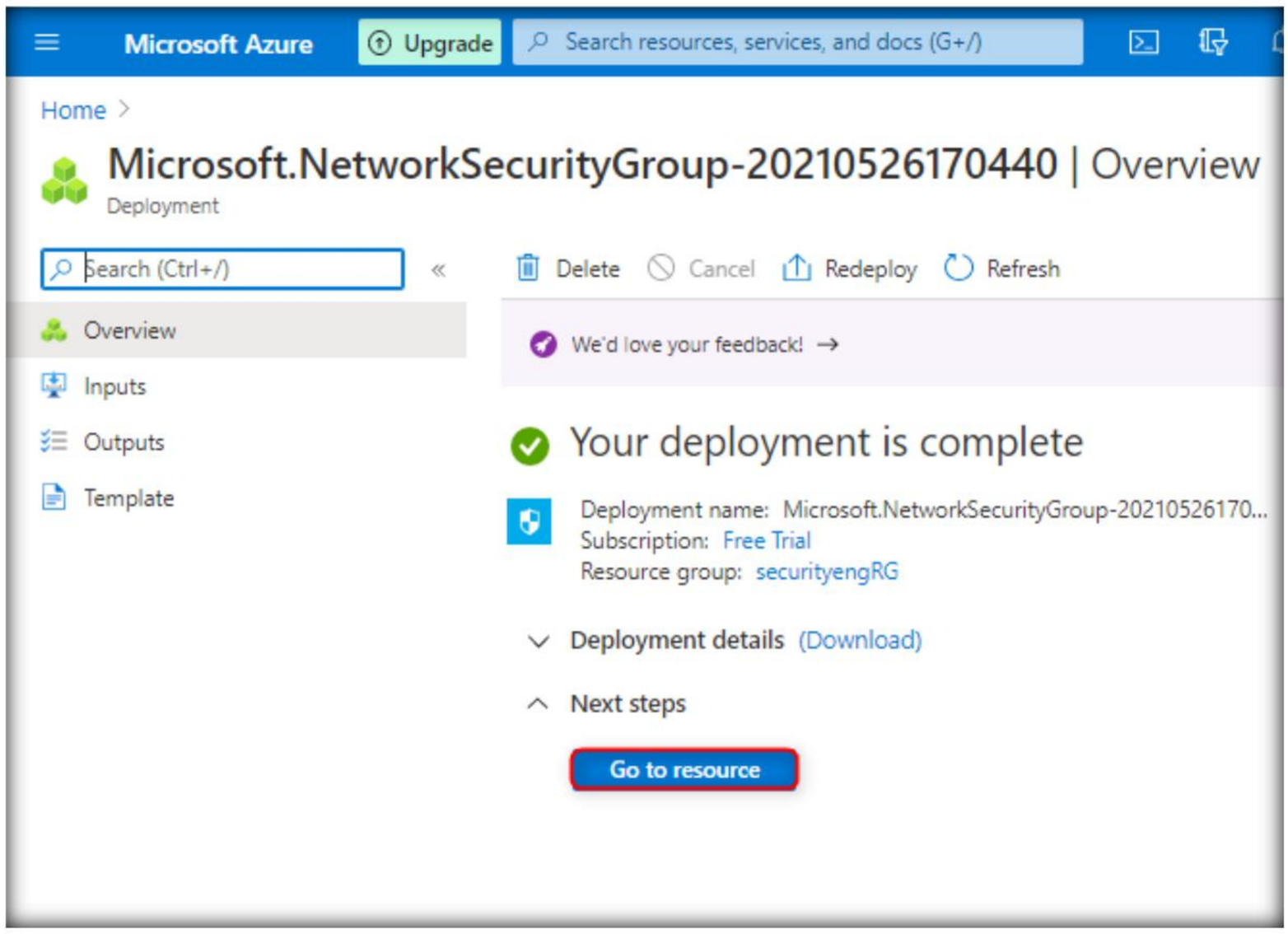


FIGURE 4.10.32: Successful Deployment of Network Security Group

33. A **SecEng-NSG** window will open. Next, you will restrict network access for your created subnet. To do this, navigate and click on **Outbound security rules** under **Settings**.

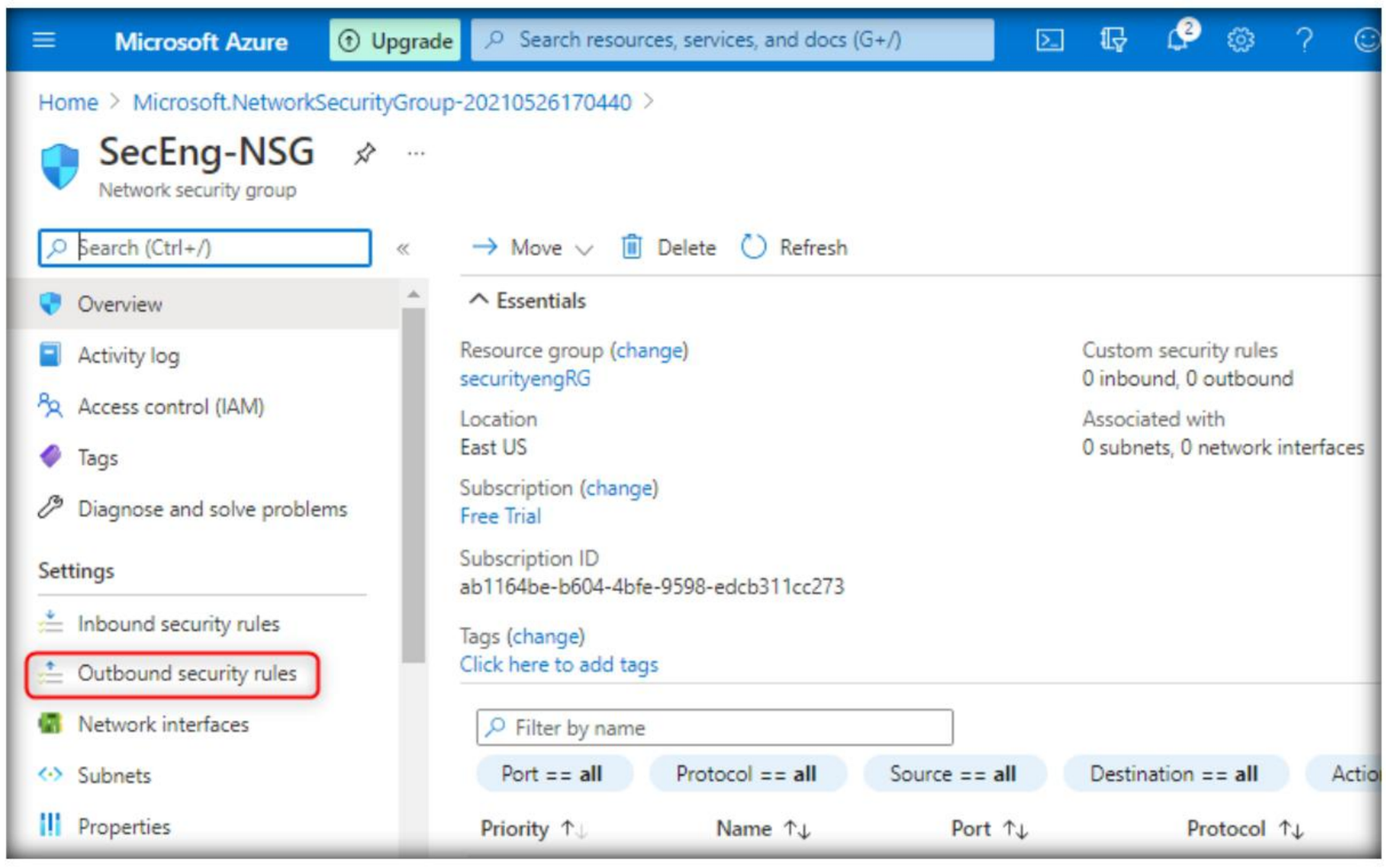


FIGURE 4.10.33: Selecting Outbound Security Rules

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

34. Click on **+Add.** An **Add outbound security rule** pane will open on the left side. Select the following:

    Source: Virtual Network

    Destination: Service Tag

    Destination service tag: Storage

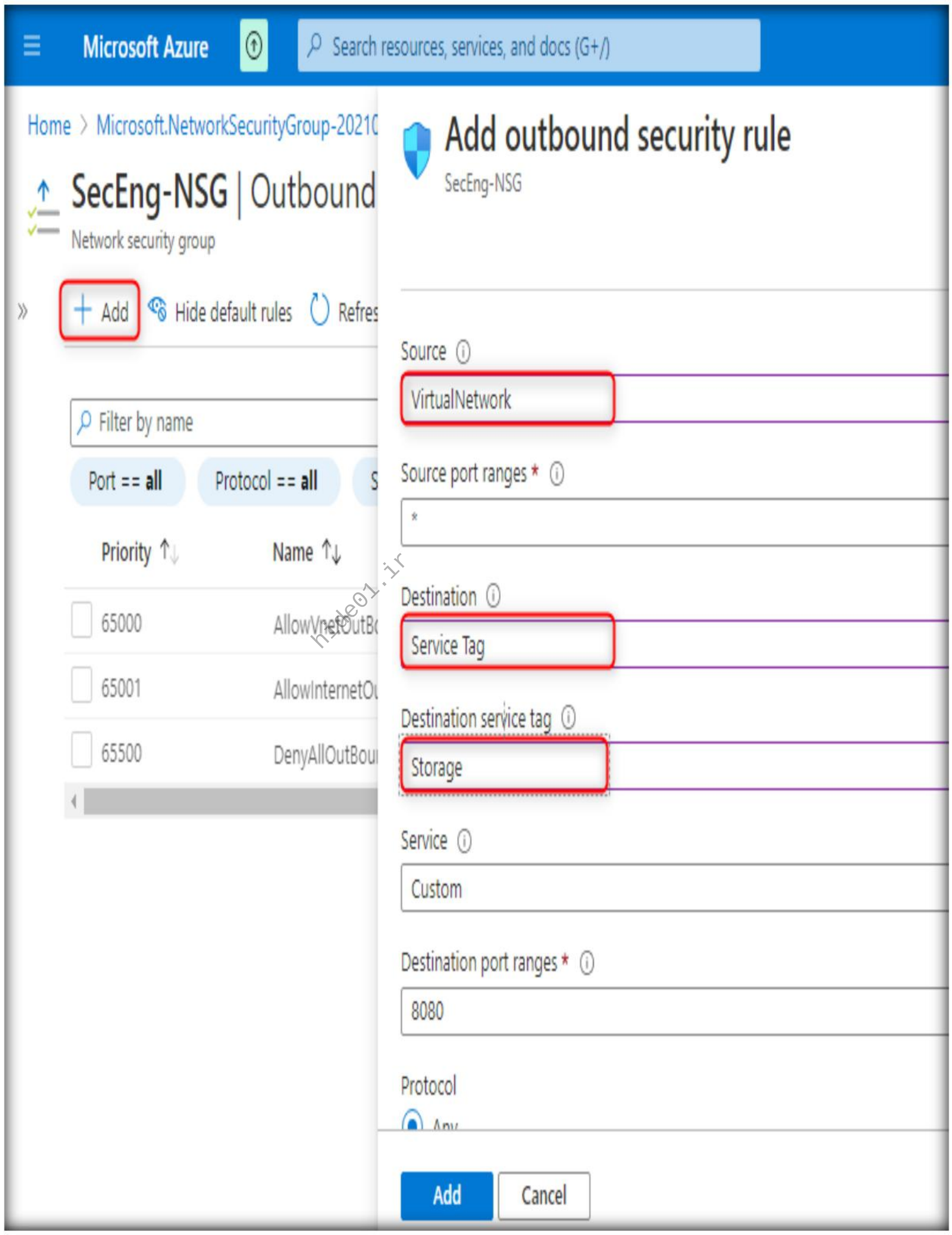


FIGURE 4.10.34: Adding Source, Destination, and Destination Service Tag

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

35. Scroll down the **Add outbound security rule** pane and select the following:

    Destination port range: *

    Protocol: Any

    Action: Allow

    Priority: 100

    Name: Allow-Storage-All

    Then, click on the **Add** button.

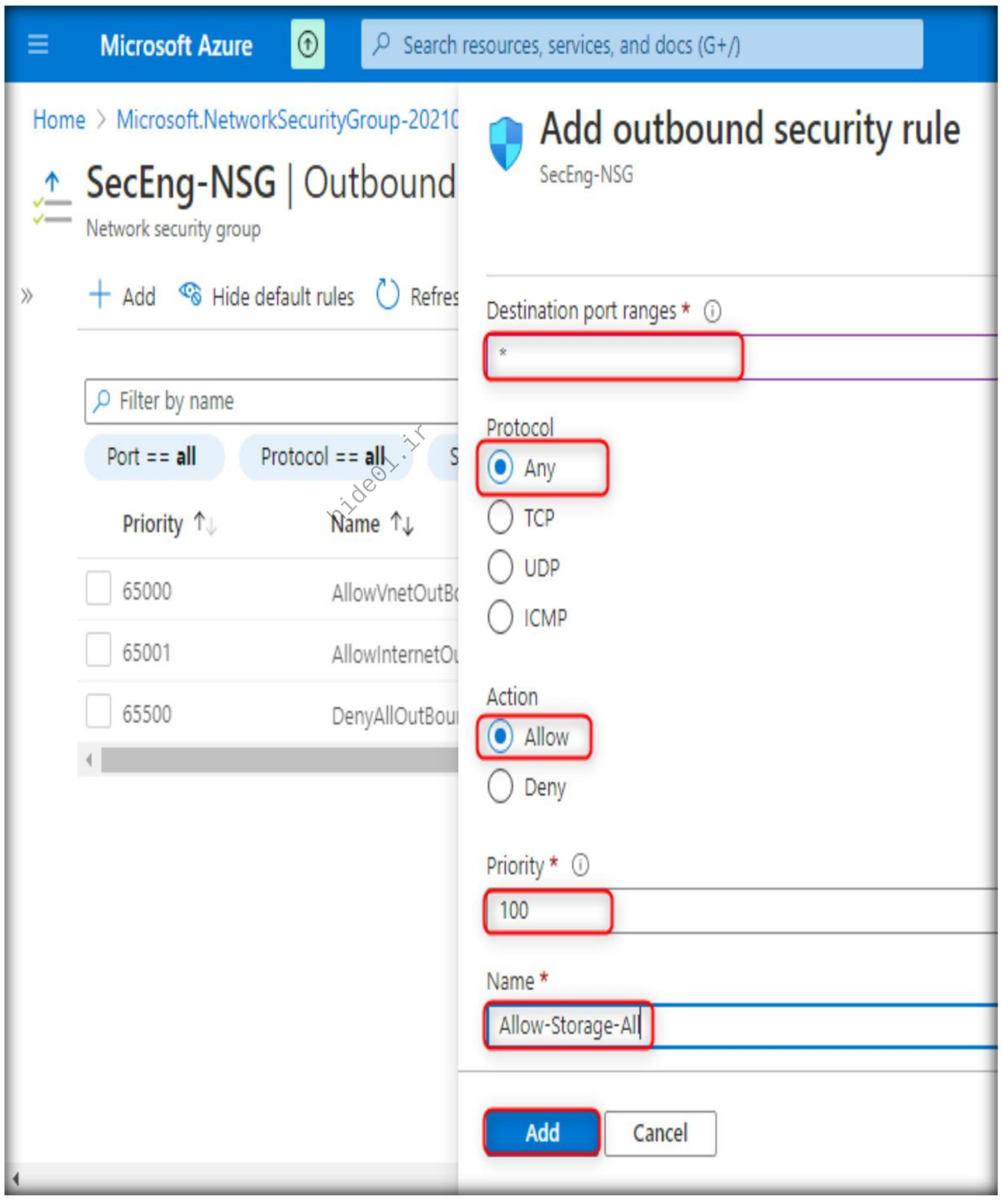


FIGURE 4.10.35: Adding Destination Port Ranges, Protocol, Action, Priority, and Name

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

36. The outbound security rule **Allow-Storage-All** is successfully created now.

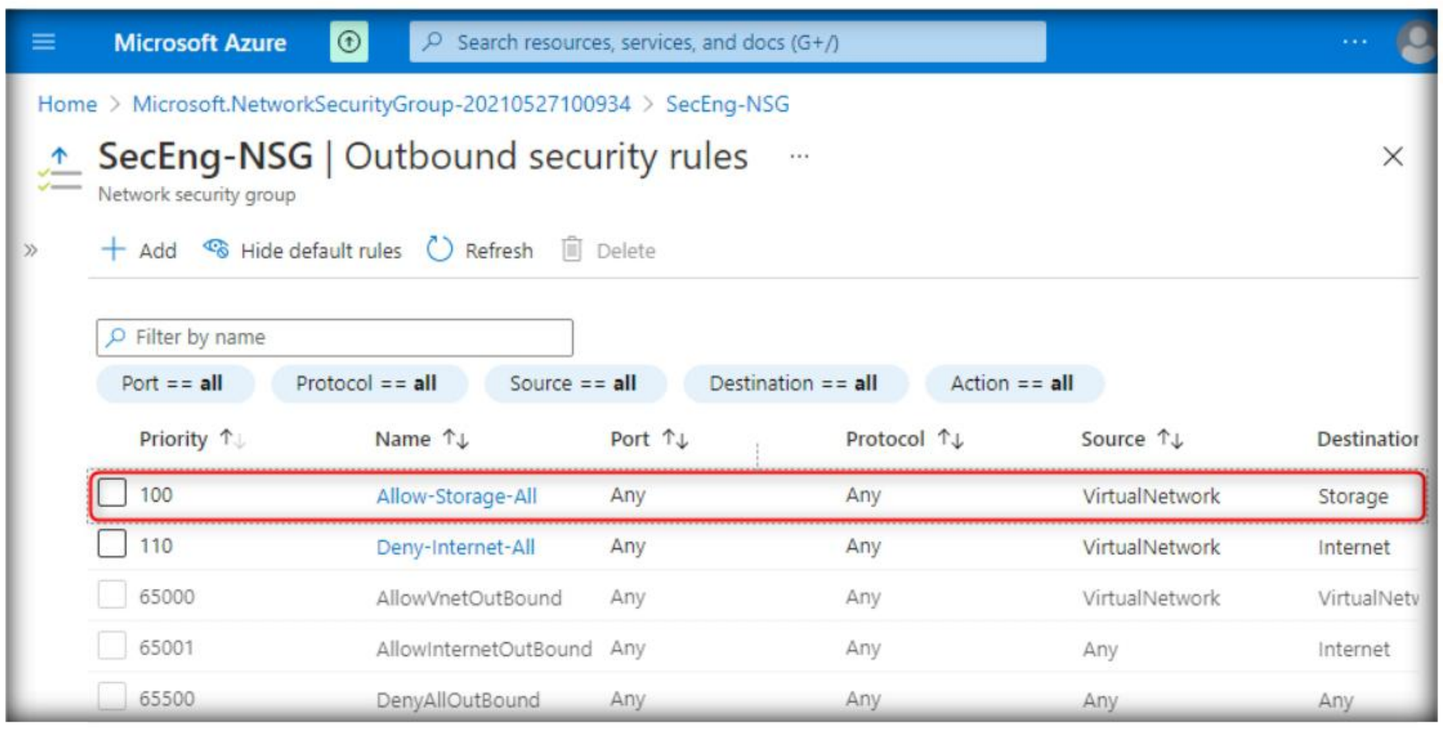


FIGURE 4.10.36: Allow-Storage-All Rule is Created

37. We will create another outbound security rule that denies a communication with the Internet. Click on the **+Add** button and select the following:

    Source: Virtual Network

    Destination: Service Tag

    Destination service tag: Internet

    Destination port ranges: *

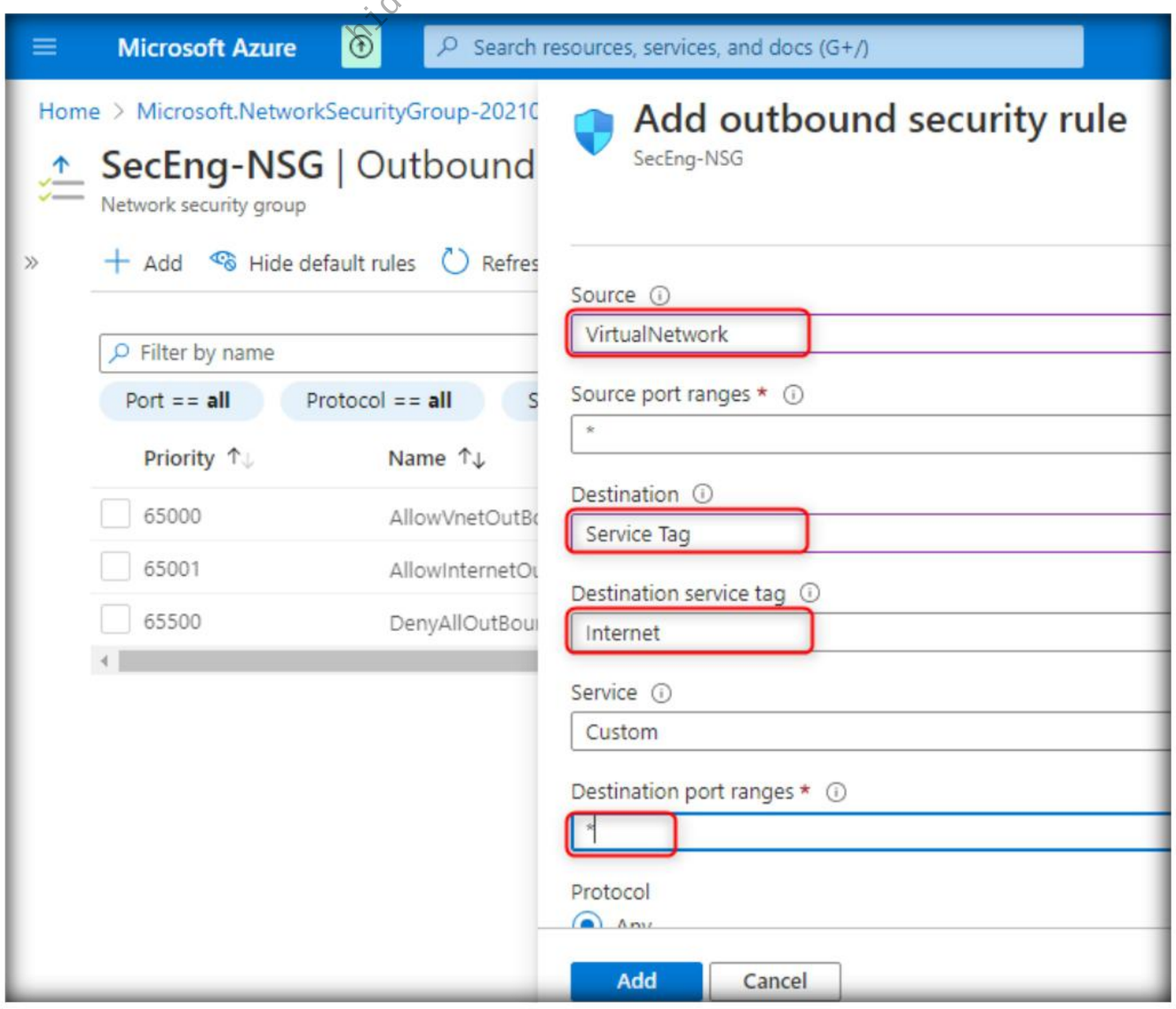


FIGURE 4.10.37: Adding Source, Destination, Destination Service Tag, and Destination Port Ranges

Certified Cloud Security Engineer Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

38. Scroll down the **Add outbound security rule** pane and select the following:

    Protocol: Any

    Priority: 110

    Name: Deny-Internet-All

    Click the **Add** button.

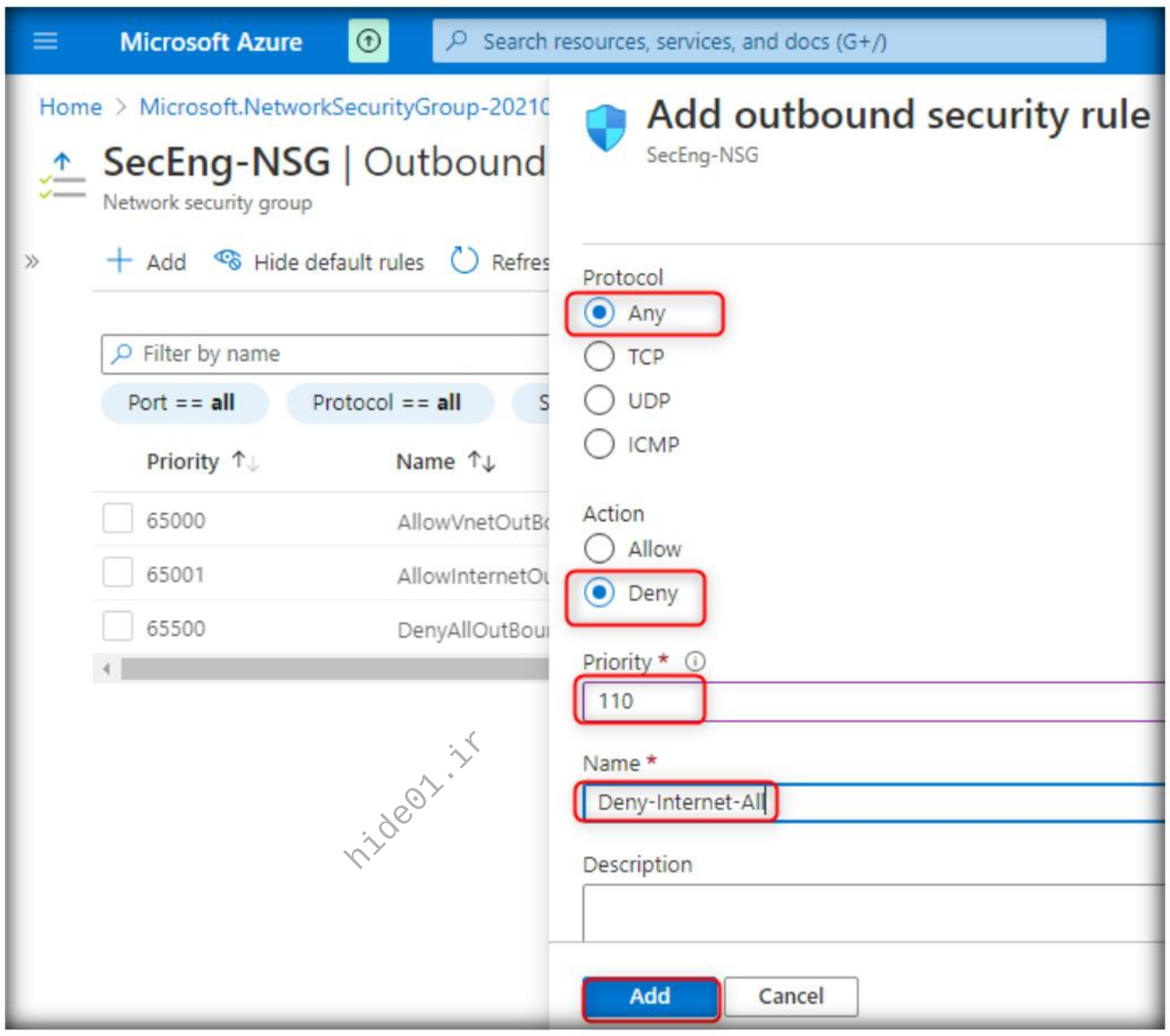


FIGURE 4.10.38: Selecting Protocol, Action, Priority, and Name

39. Click the **Refresh** button. The outbound security rule **Deny-Internet-All** has been successfully created.

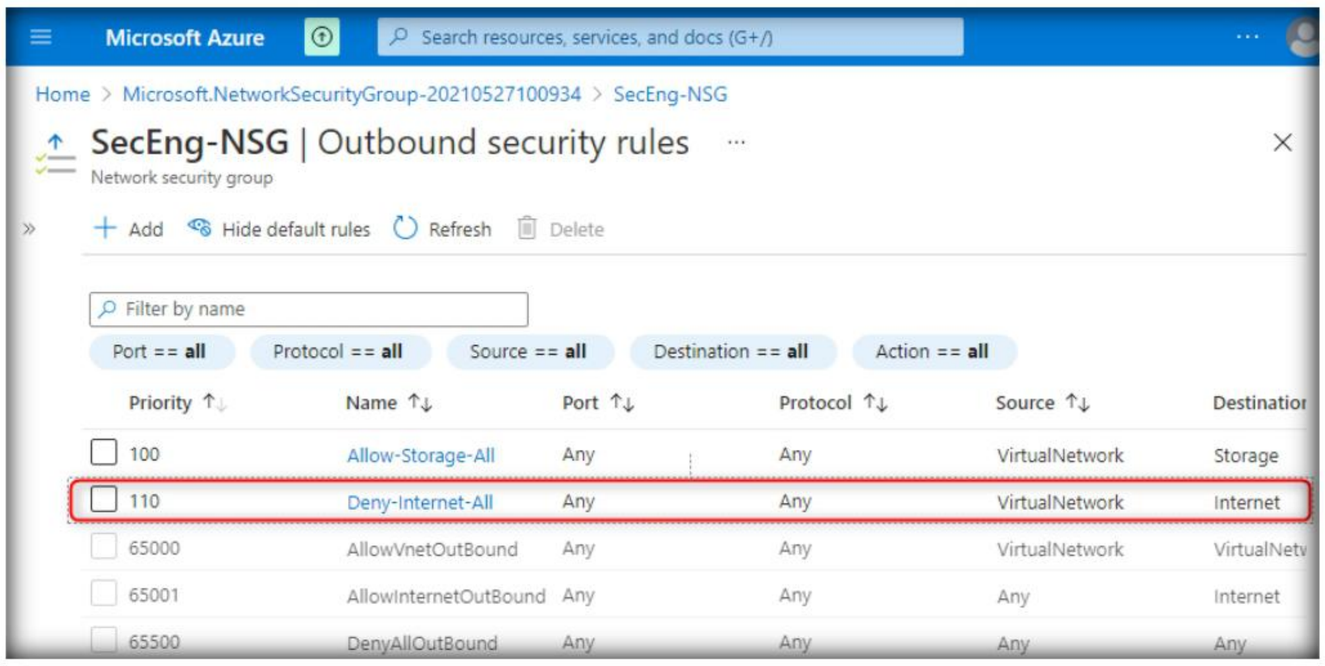


FIGURE 4.10.39: Deny-internet-All Rule is Created

Certified Cloud Security Engineer Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

40. Click on **Inbound security rules** under **Settings**.

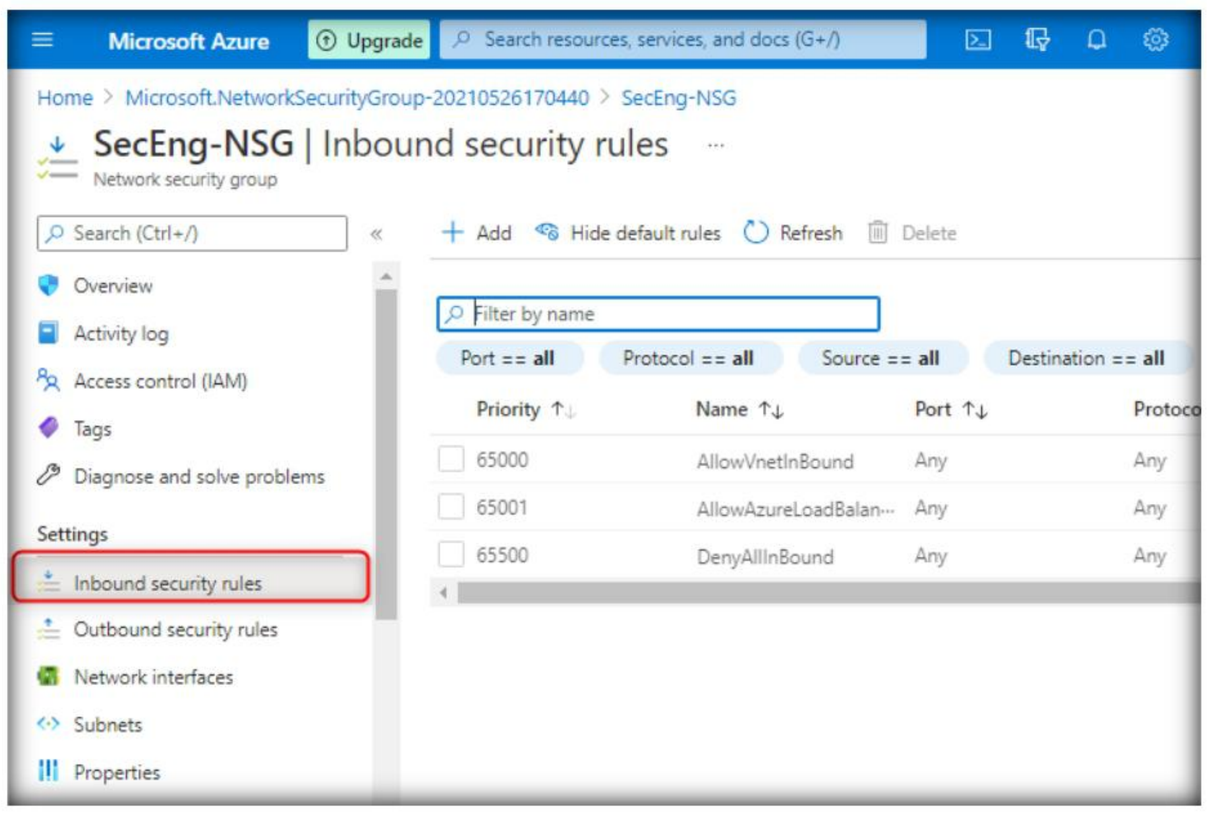


FIGURE 4.10.40: Selecting Inbound Security Rules

41. Click on **+Add**, and select the following under the **Add inbound security rule** window:

Source: Any

Source port ranges: *

Destination: VirtualNetwork

Destination port ranges: 3389

Protocol: Any

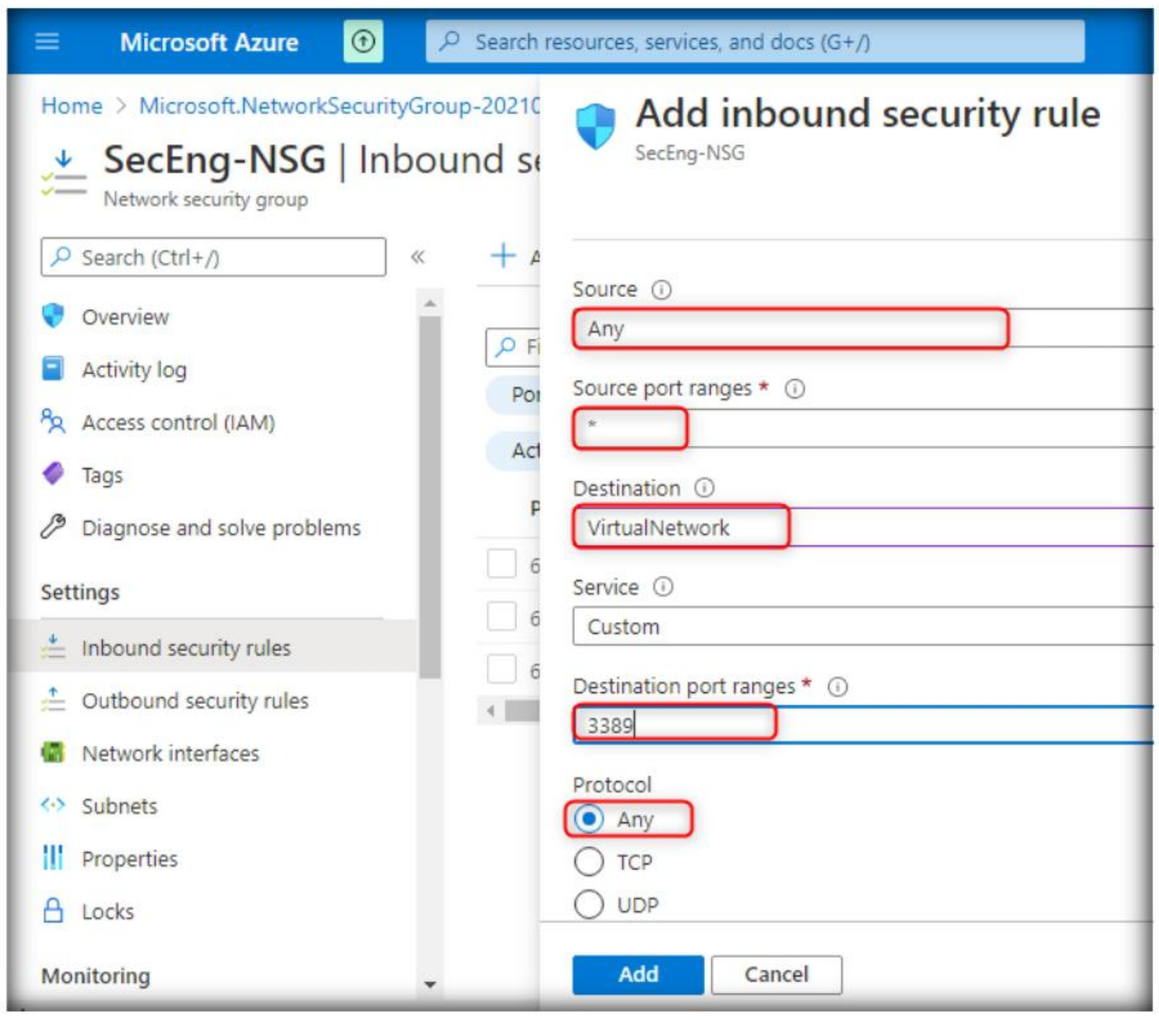


FIGURE 4.10.41: Adding Source, Source Port Ranges, Destination, and Destination Port Ranges, and Selecting Protocol

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

42. Scroll down the **Add inbound security rule** pane and select the following:

    Action: Allow

    Priority: 120

    Name: Allow-RDP-All

    Then, click on **Add** button.

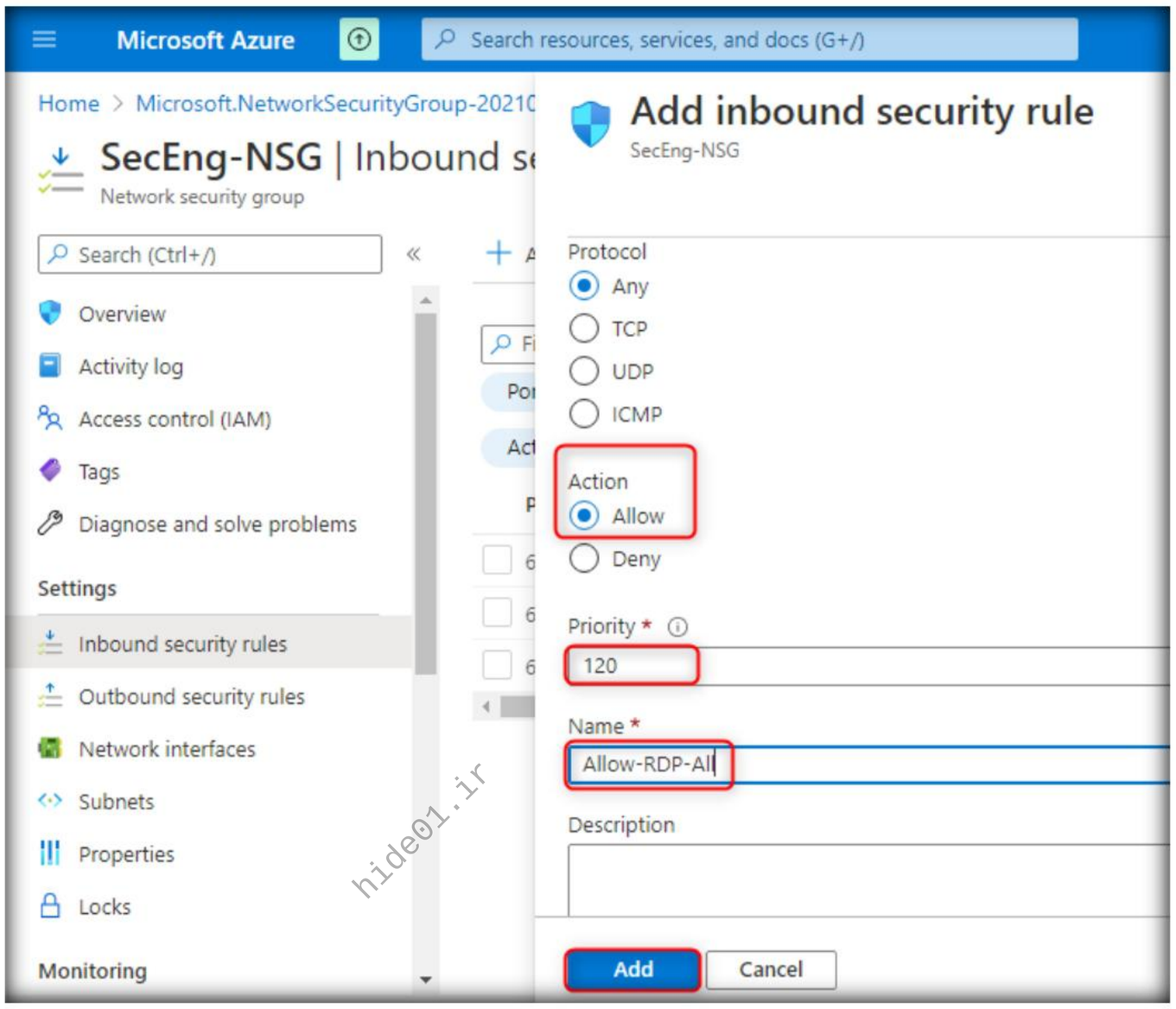


FIGURE 4.10.42: Selecting Action and Adding Priority and Name

43. Click **Refresh** button. The inbound security rule **Allow-RDP-All** is successfully created now.

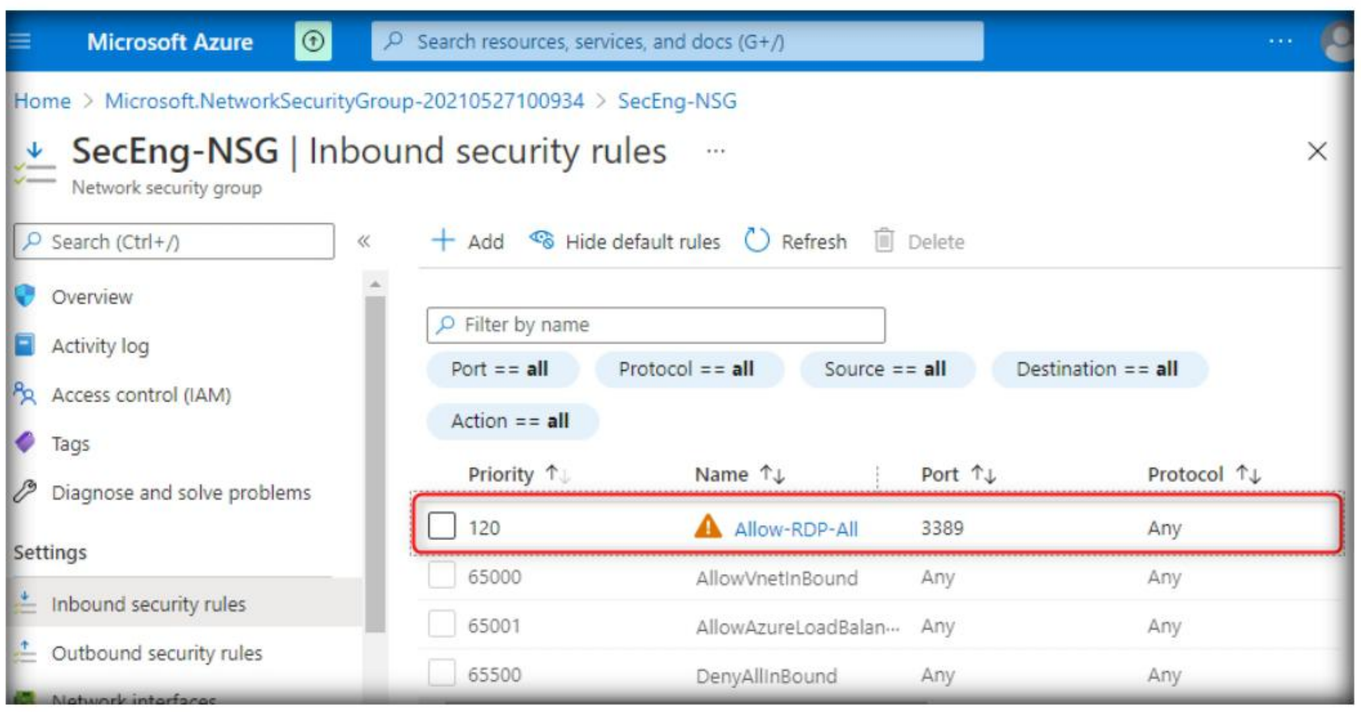


FIGURE 4.10.43: Inbound Security Rule is Created

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

44. Click on **Subnets** under **Settings**, and then click on **+Associate**.

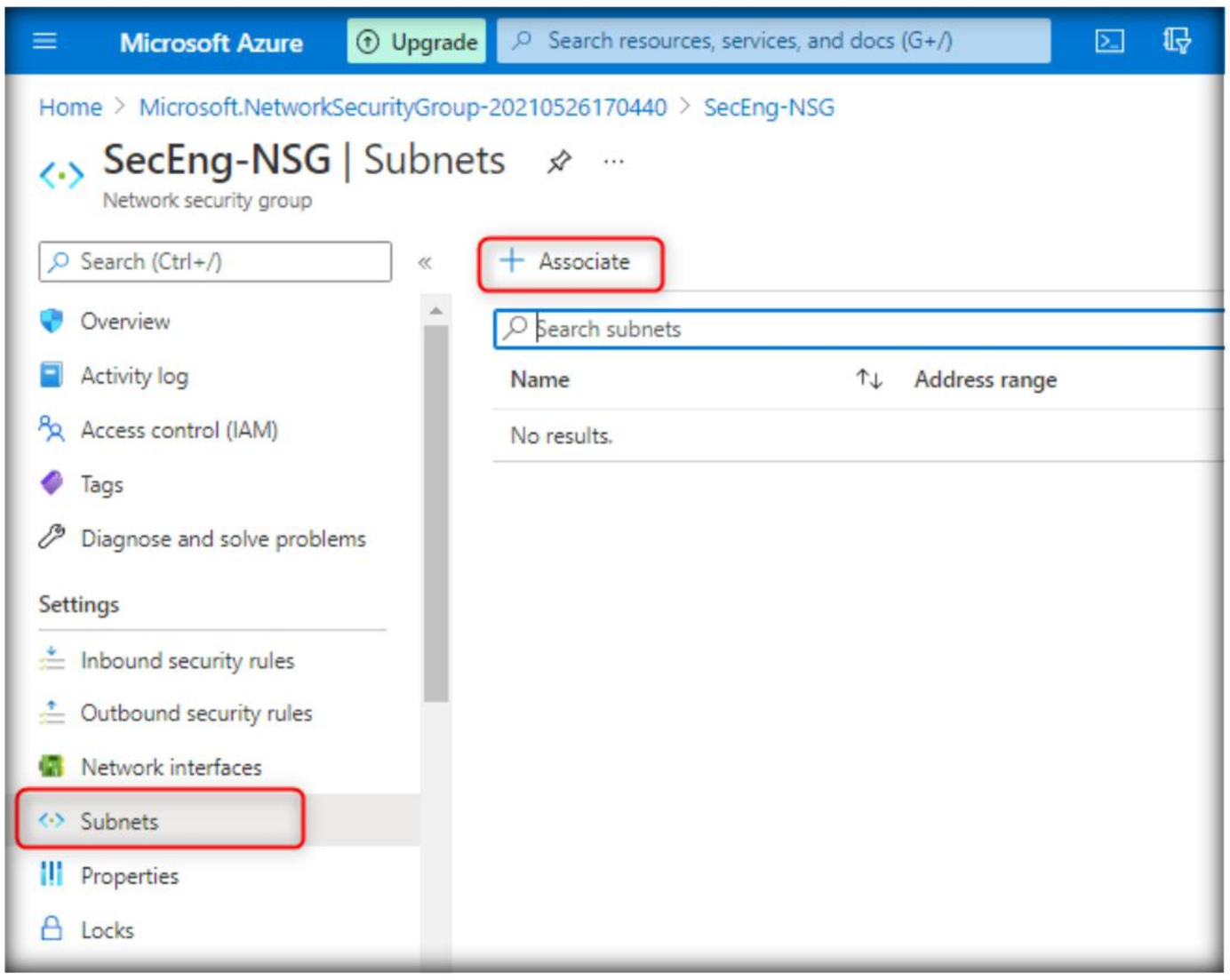


FIGURE 4.10.44: Selecting Subnets

45. An **Associate subnet** pane will open on the left side. Select **SecEng-VNET**, in the **Virtual network** dropdown and **Private** in the **Subnet** field. Then, click on **OK** button.

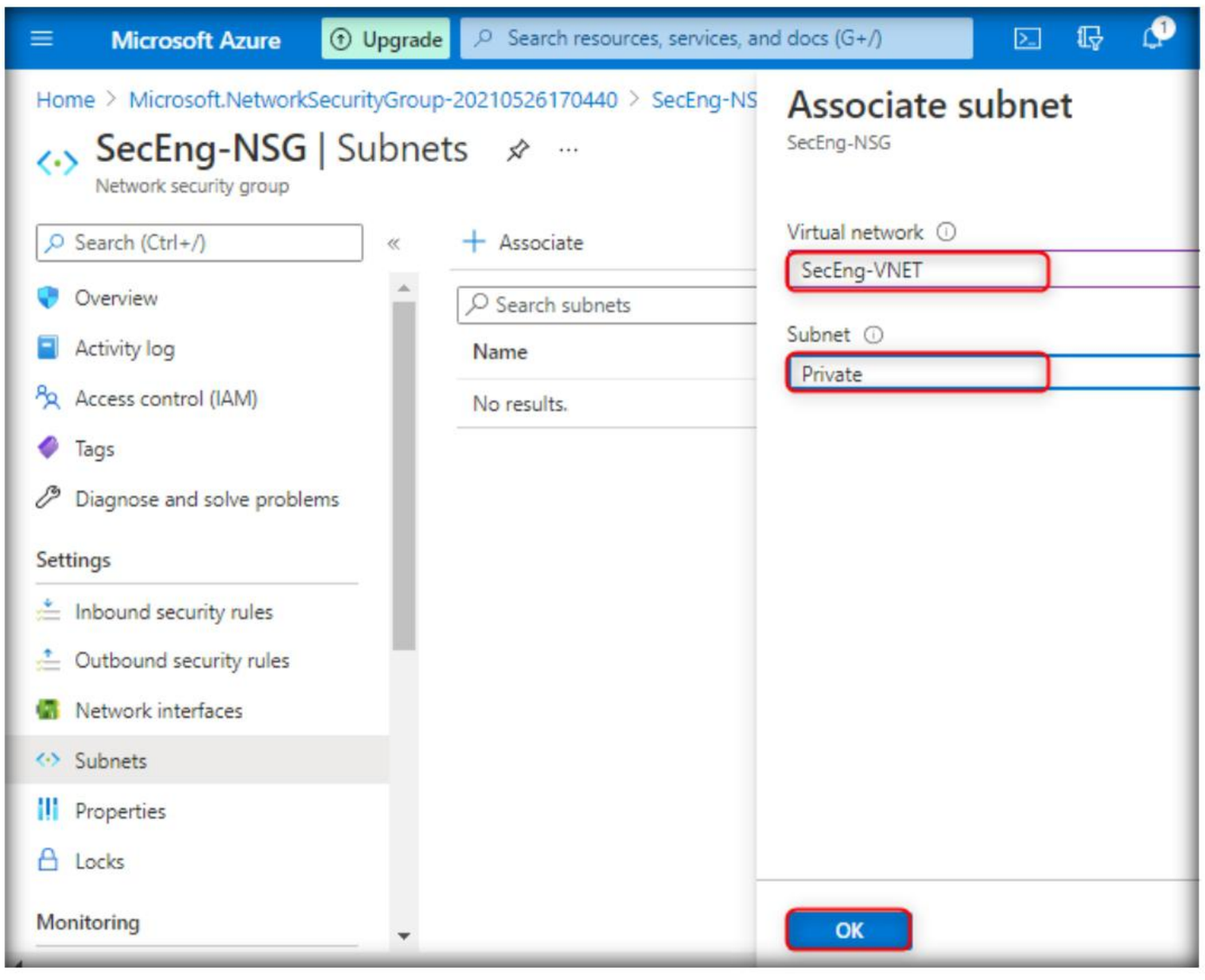


FIGURE 4.10.45: Associating Subnet

Certified Cloud Security Engineer Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

46. The NSG is successfully saved for the **Private** subnet.

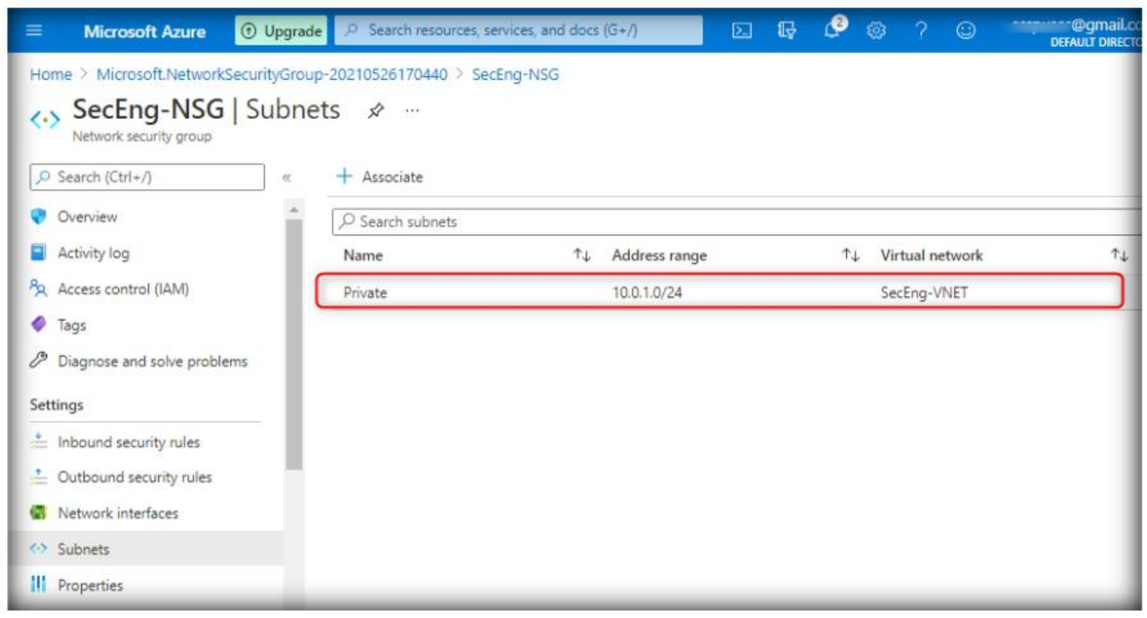


FIGURE 4.10.46: Private Subnet Successfully Associated with NSG

TASK 5

Create Azure Storage Account

47. Click on **Home** to go back to Azure portal.

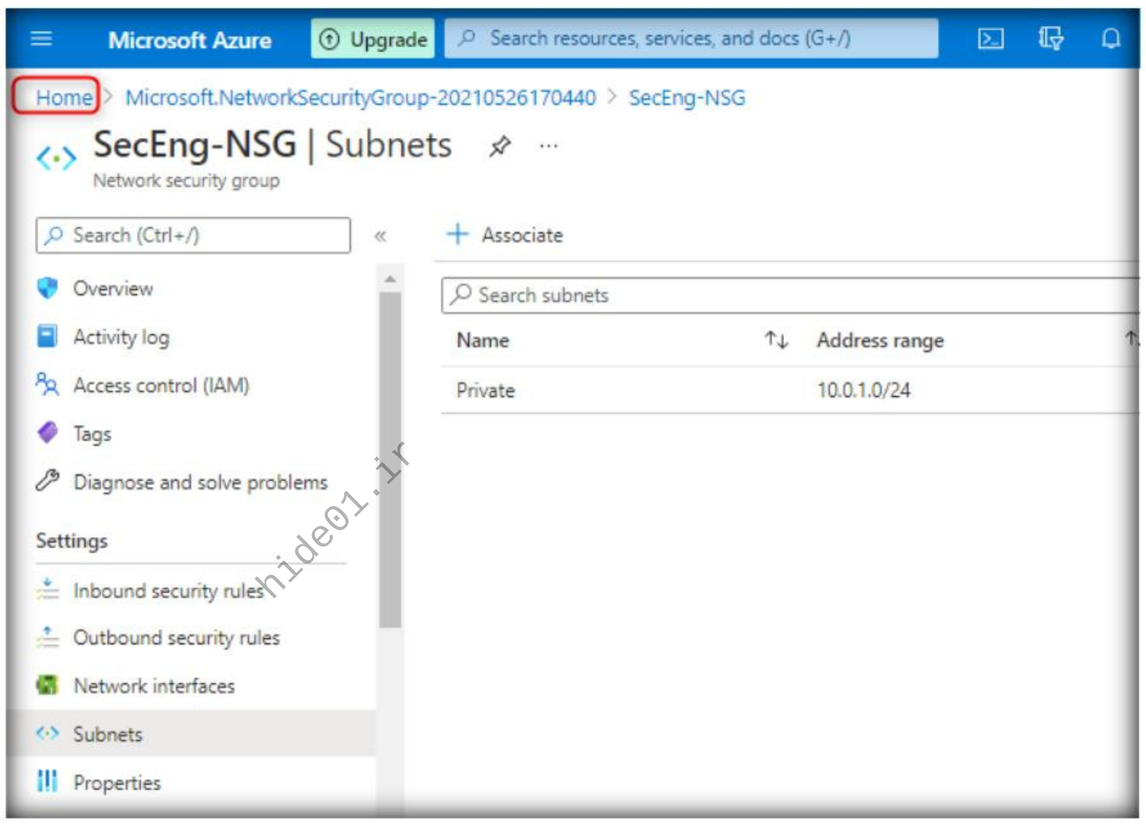


FIGURE 4.10.47: Going Back to Azure Portal

48. Now, create an Azure storage account. To do this, click on the Azure portal menu, and navigate and click on **Storage accounts.**

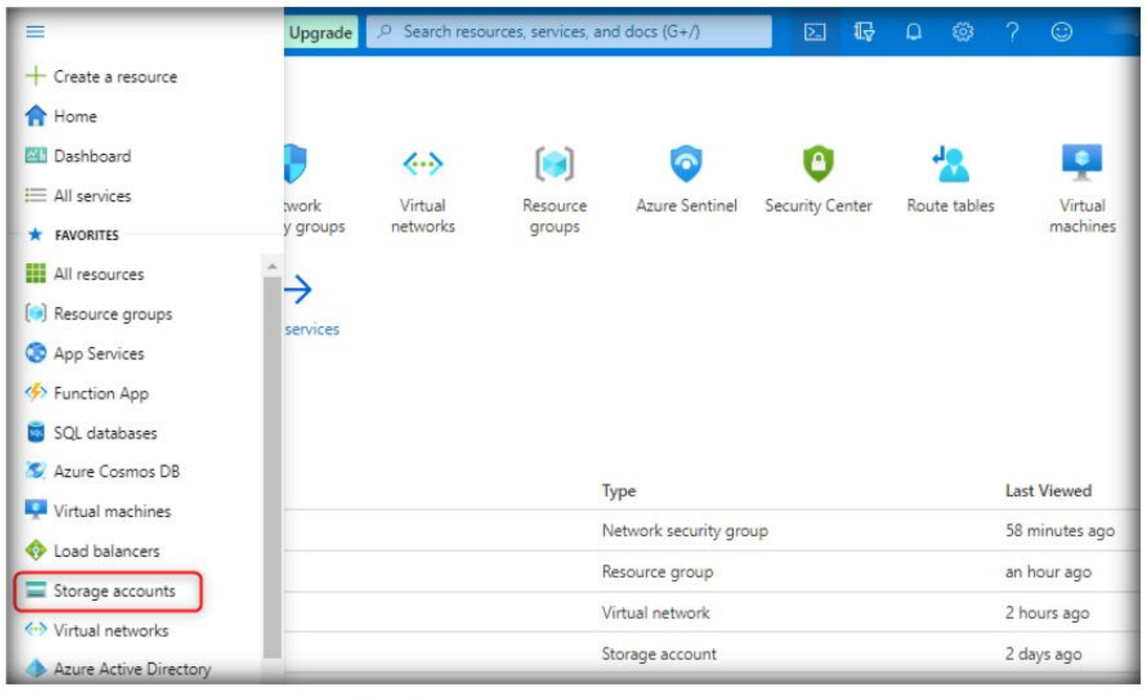


FIGURE 4.10.48: Selecting Storage Accounts

Certified Cloud Security Engineer Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

49. In the **Storage account** window, click **+Add**.

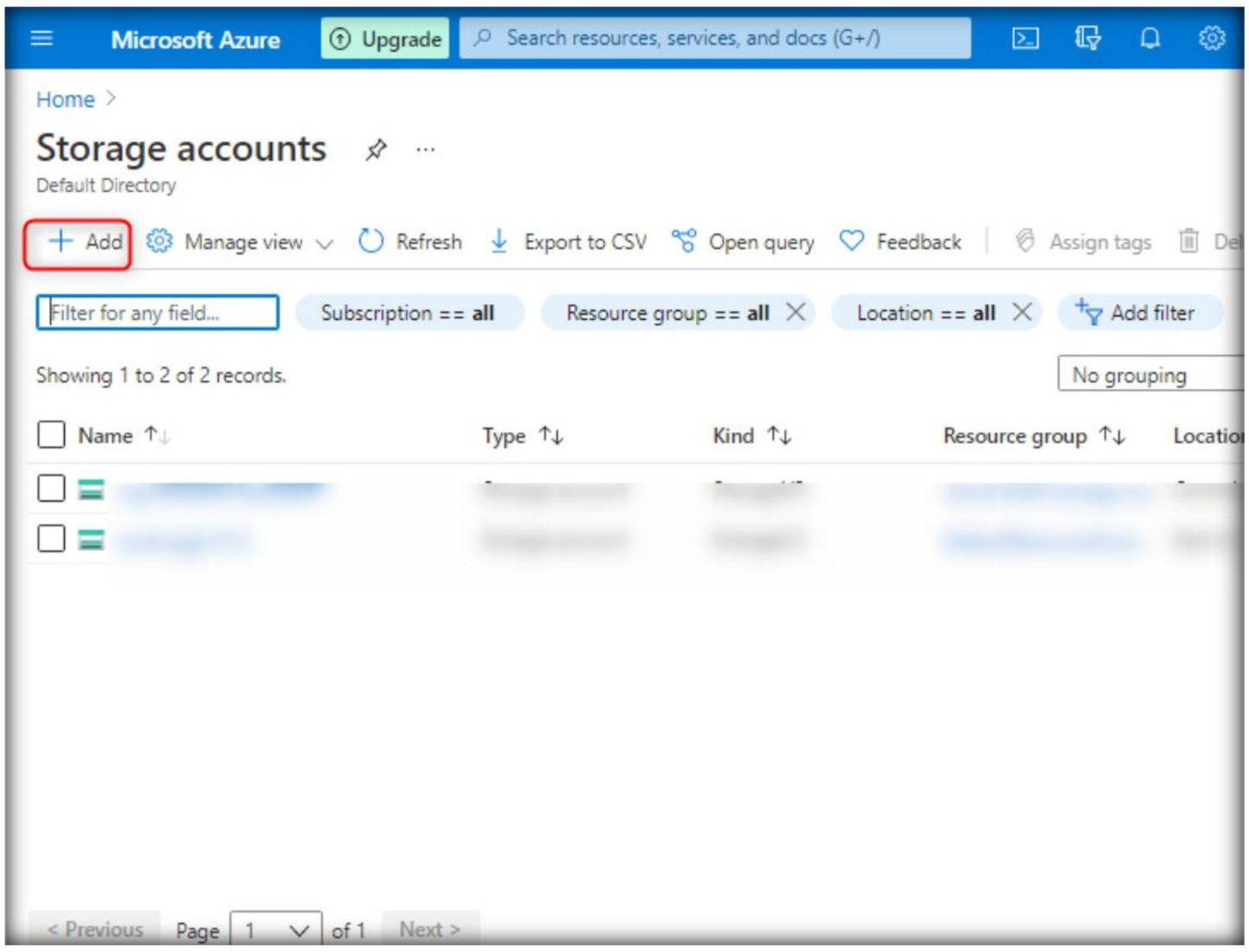


FIGURE 4.10.49: Adding a Storage Account

50. A **Create a storage account** window will open. In the **Resource group** field, select **securityengRG**.

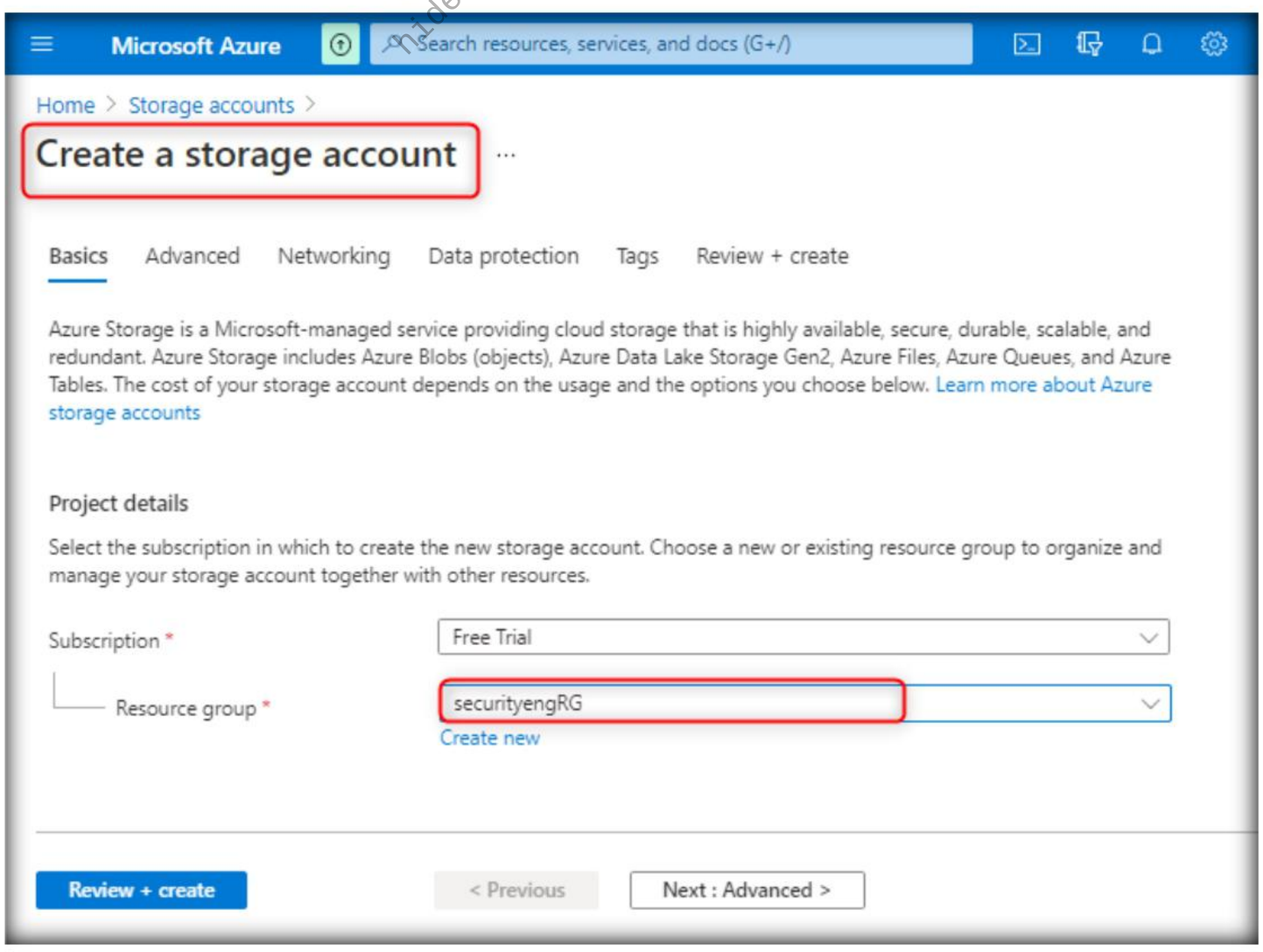


FIGURE 4.10.50: Selecting Resource Group for Storage Account

Certified Cloud Security Engineer Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

51. Scroll down the **Create a storage account** window. In the **Storage account name** field, enter the name of the storage account (here, we have used **mystorage25**) and then click on the **Next: Advanced >** button.

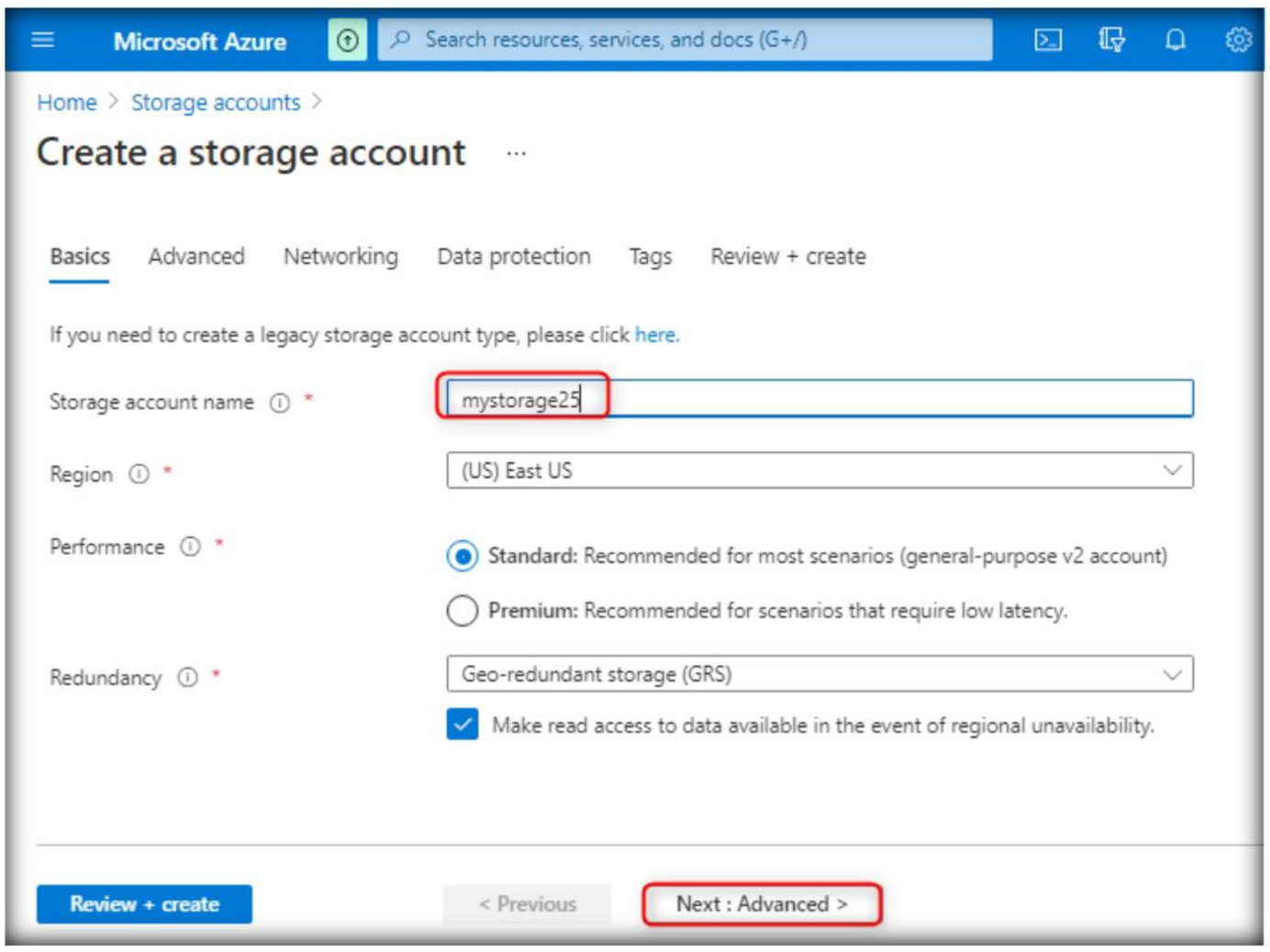


FIGURE 4.10.51: Entering Storage Account Name

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

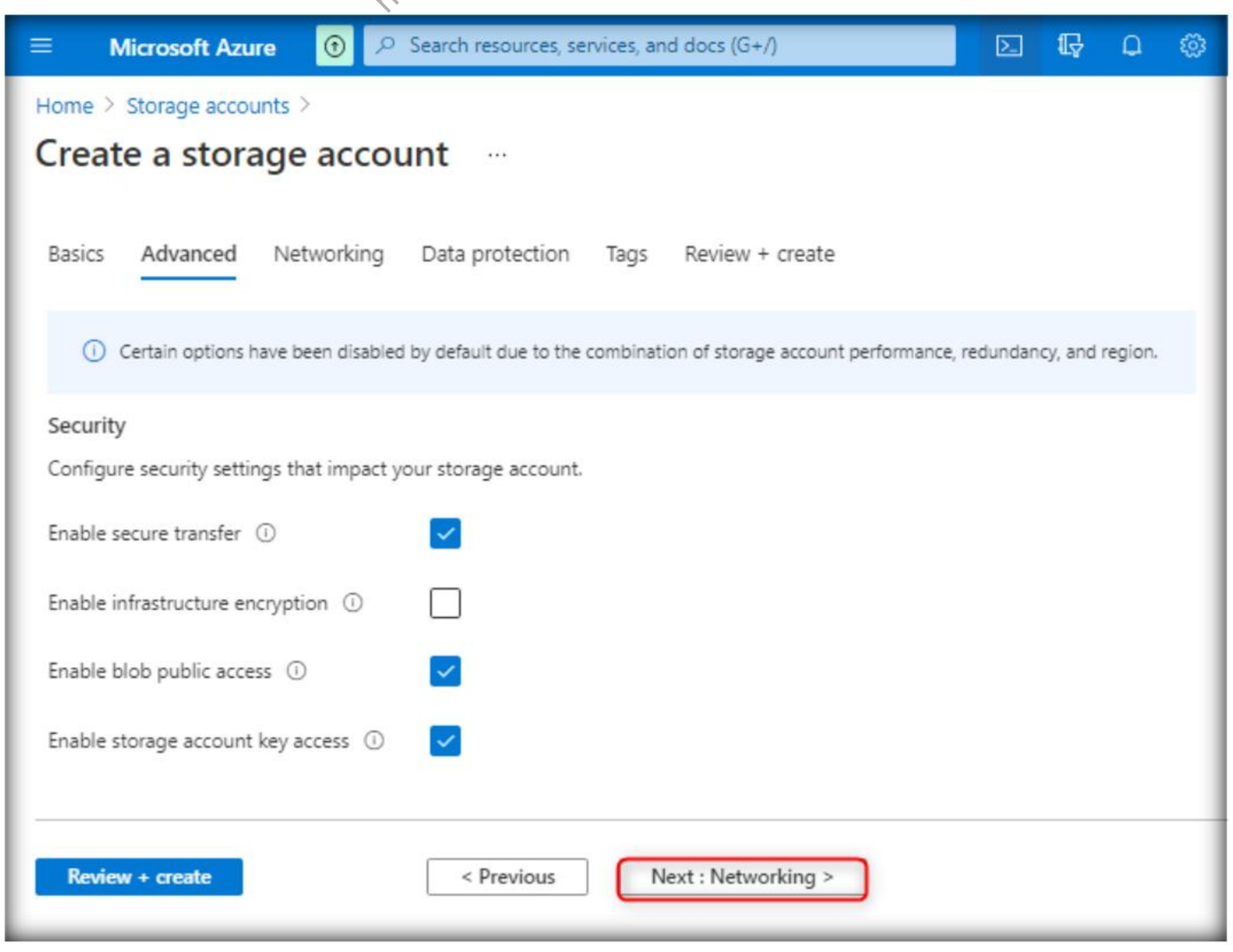


FIGURE 4.10.52: Leaving Advanced Tab in Default State

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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

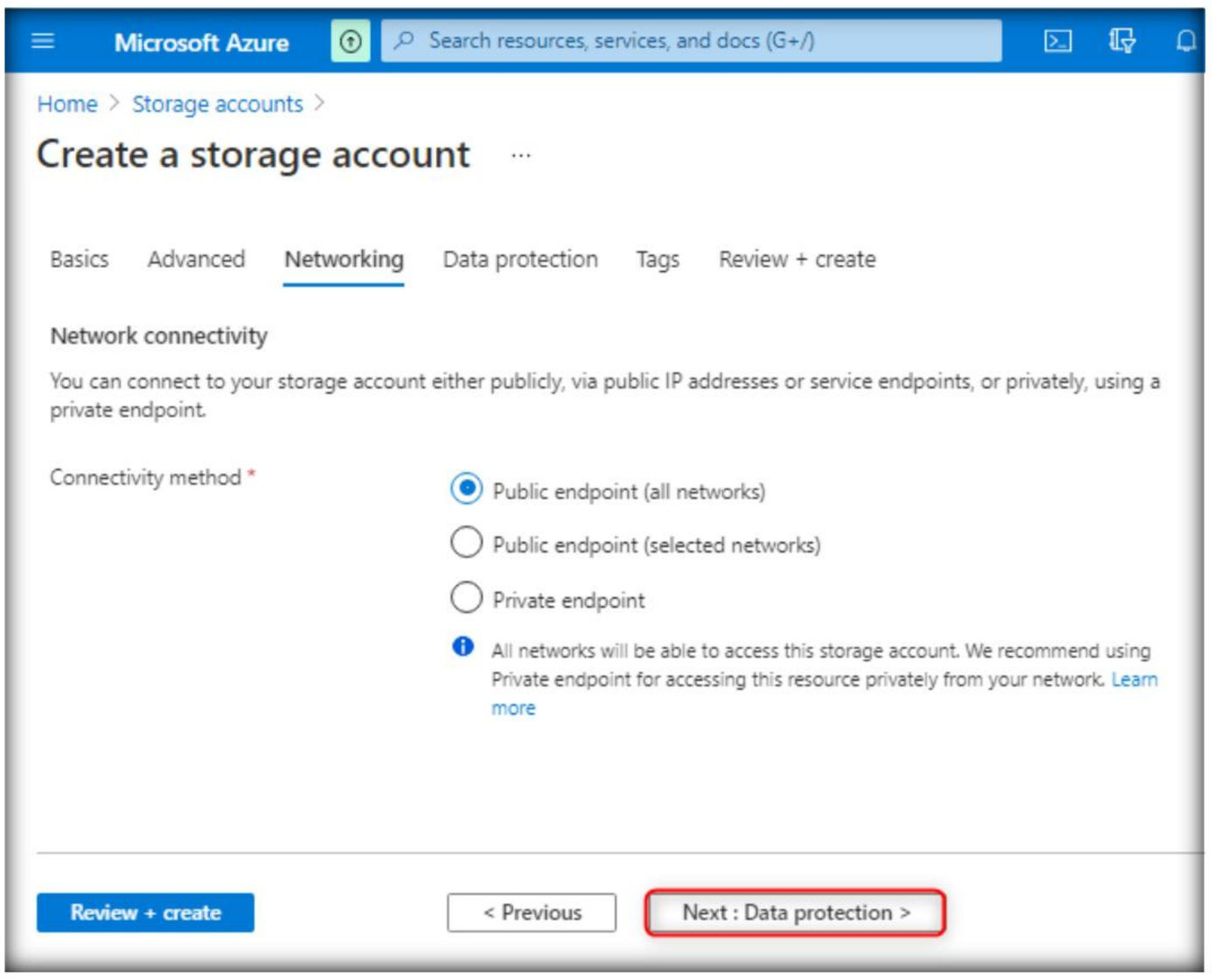


FIGURE 4.10.53: Leaving Networking Tab in Default State

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

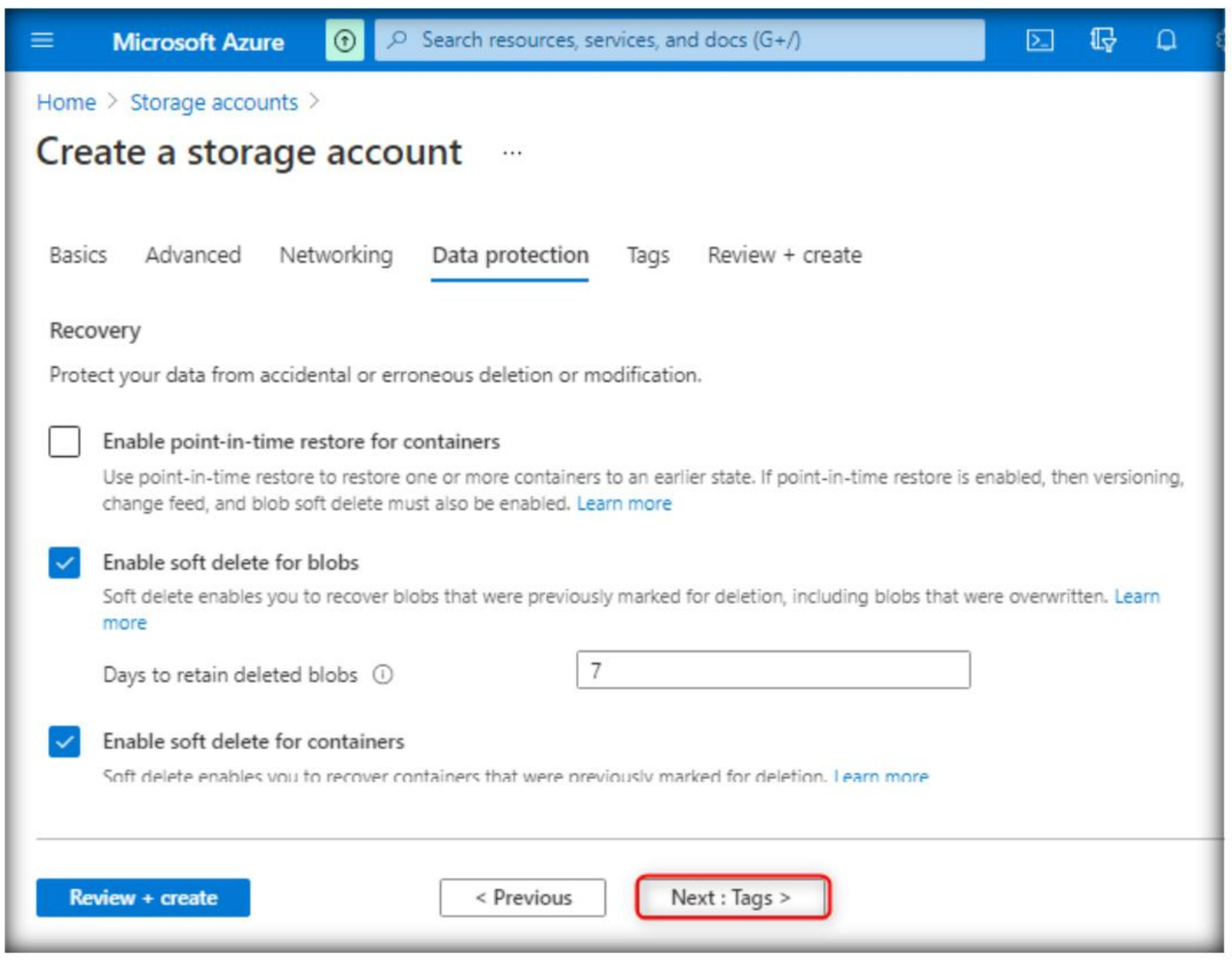


FIGURE 4.10.54: Leaving Data protection Tab in Default State

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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

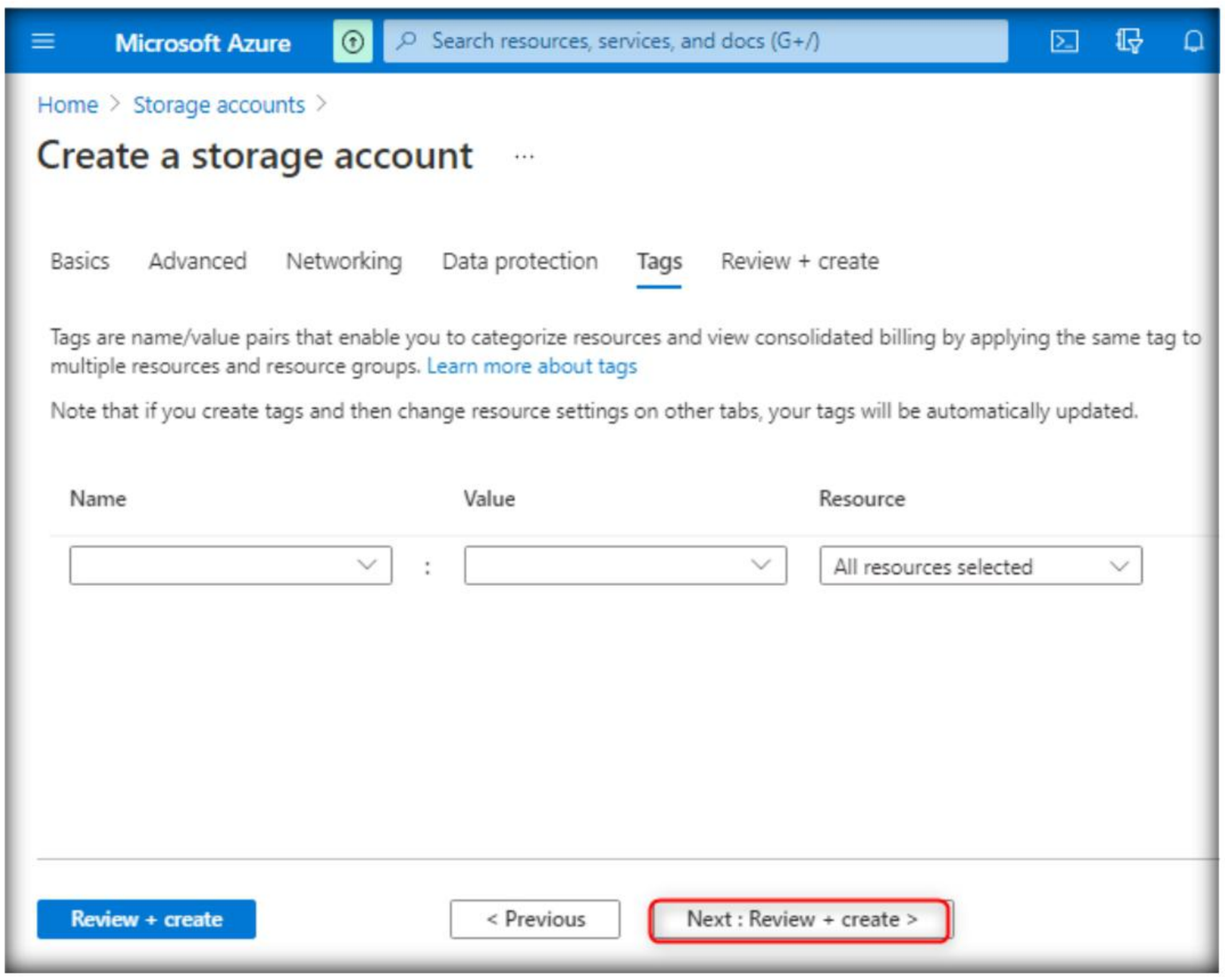


FIGURE 4.10.55: Leaving Tags Tab in Default State

56. After viewing the **Validation passed** message, click on the **Create** button.

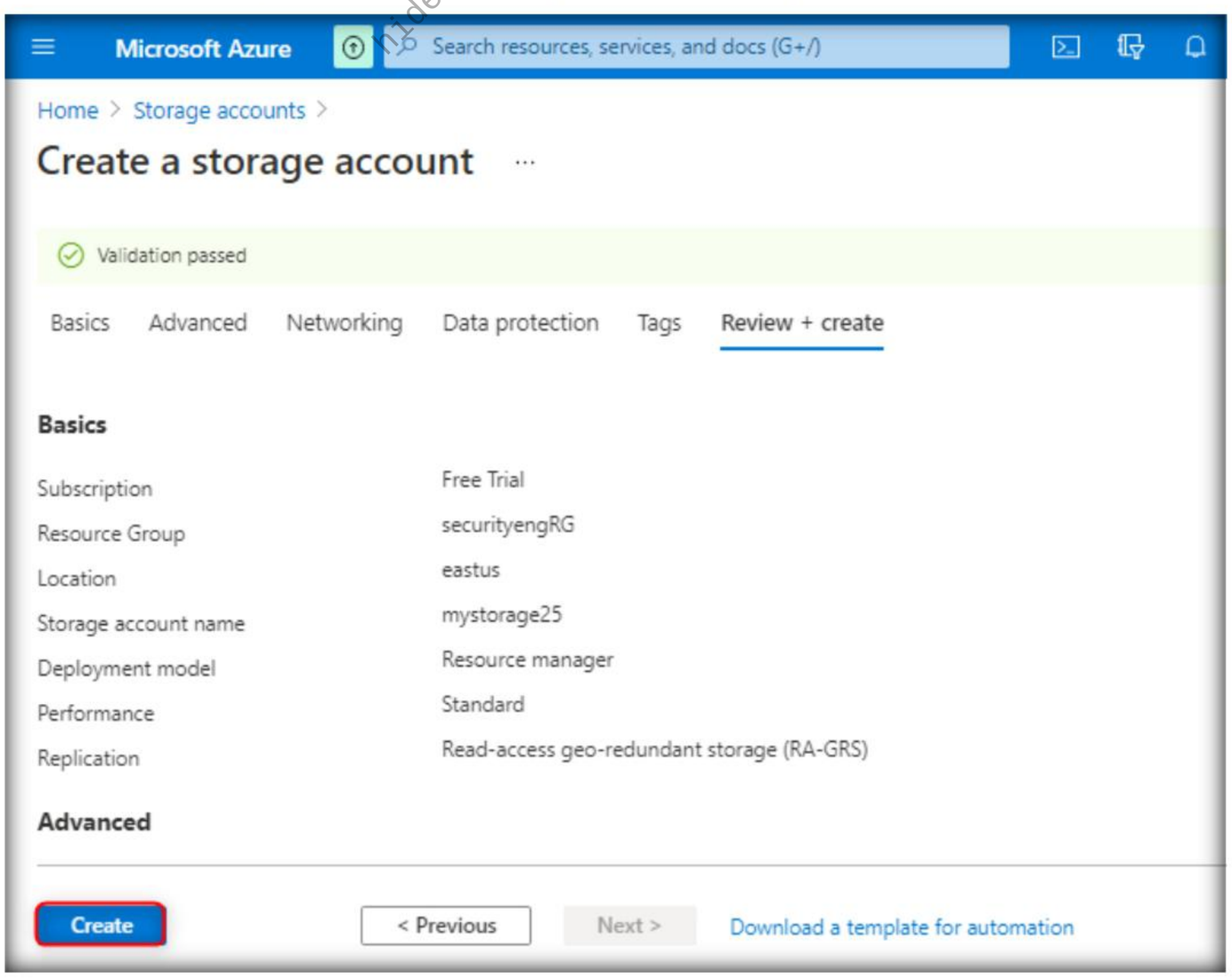


FIGURE 4.10.56: Creating Storage Account after Validation Passed

Certified Cloud Security Engineer Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

57. Wait for few seconds for the deployment to complete.

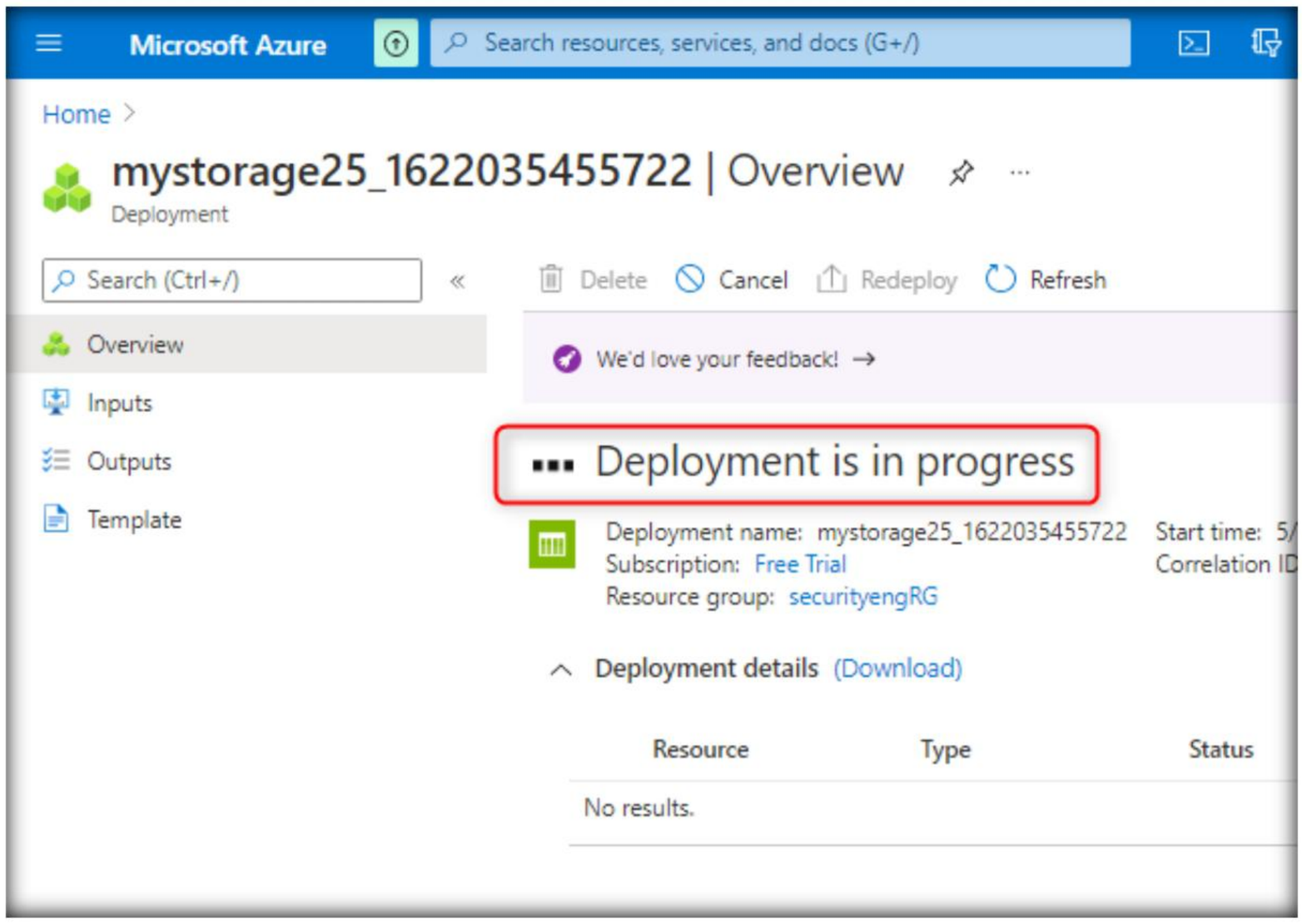


FIGURE 4.10.57: Storage Account Deployment in Progress

58. After the successful deployment of the storage account, click on the **Go to resource** button.

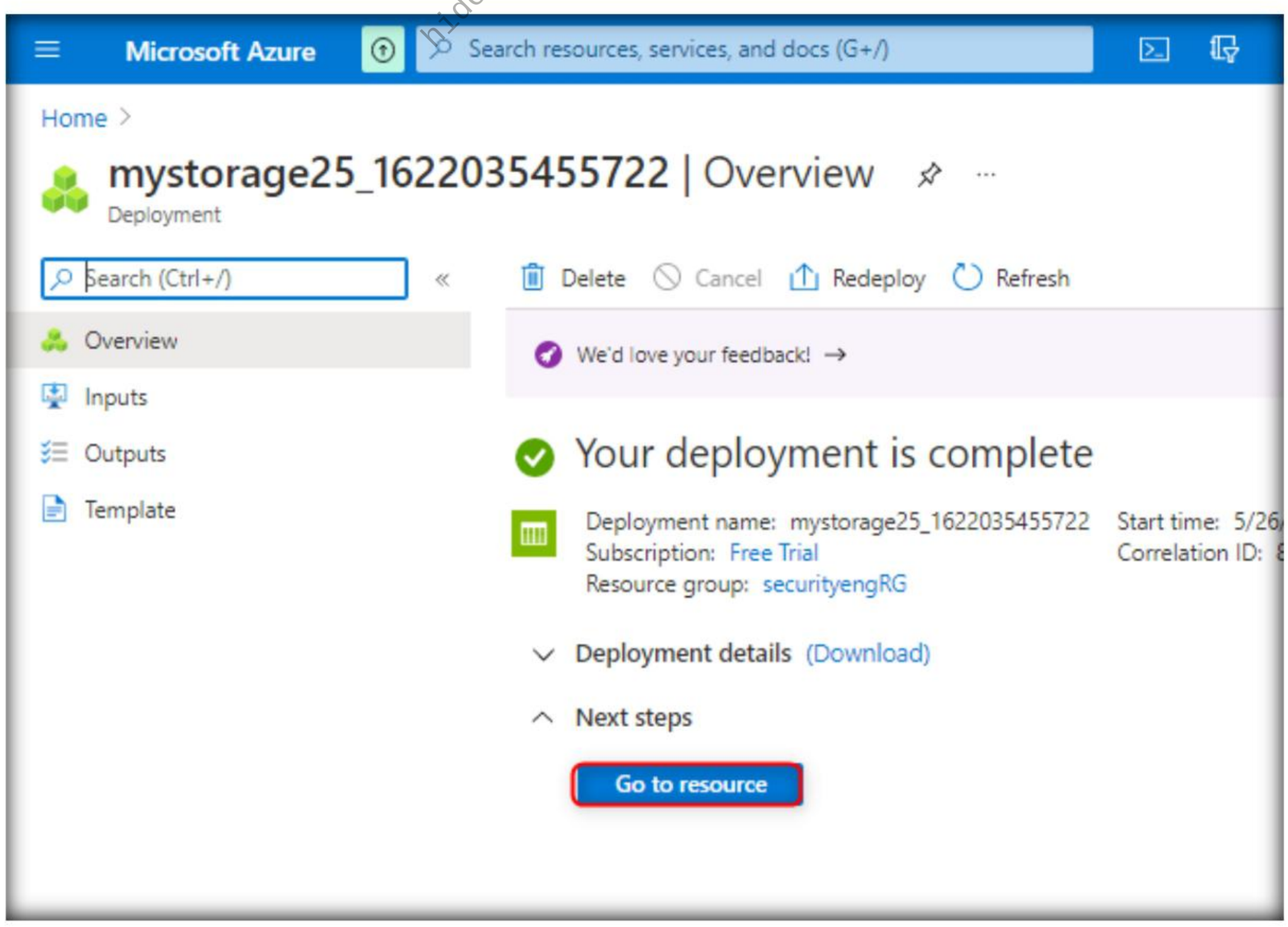


FIGURE 4.10.58: Storage Account Successfully Deployed

Certified Cloud Security Engineer Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 6

Create a File Share in Azure Storage Account

59. Now, create a file share in the Azure storage account you have created. In the storage account (**mystorage25**), navigate and click on **File shares** under **Data Storage**.

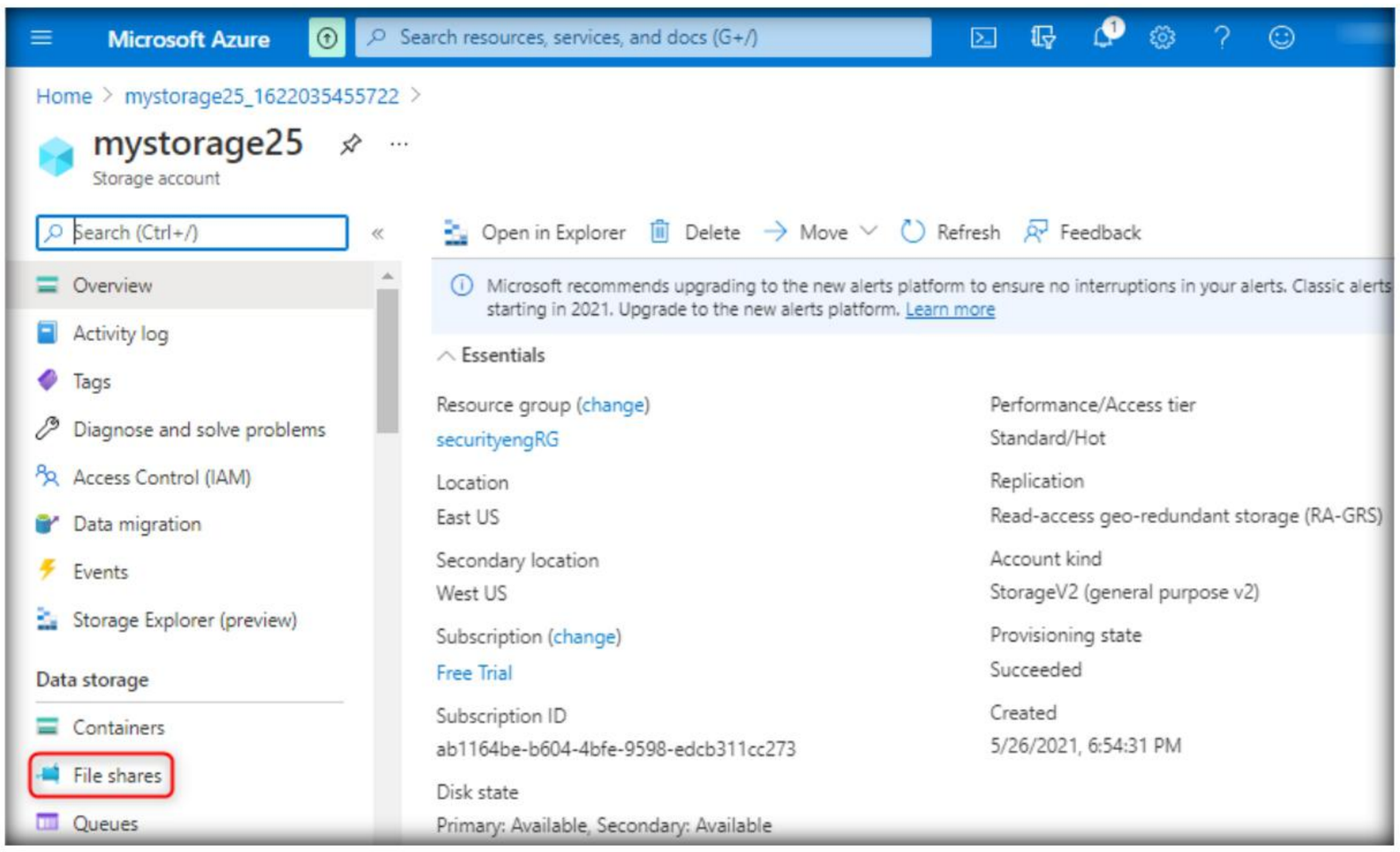


FIGURE 4.10.59: Selecting File shares in Storage Account

60. Click on **+ File share**. A **New file share** pane will open to the left side. In the **Name** field, enter **my-file-share** and click on the **Create** button.

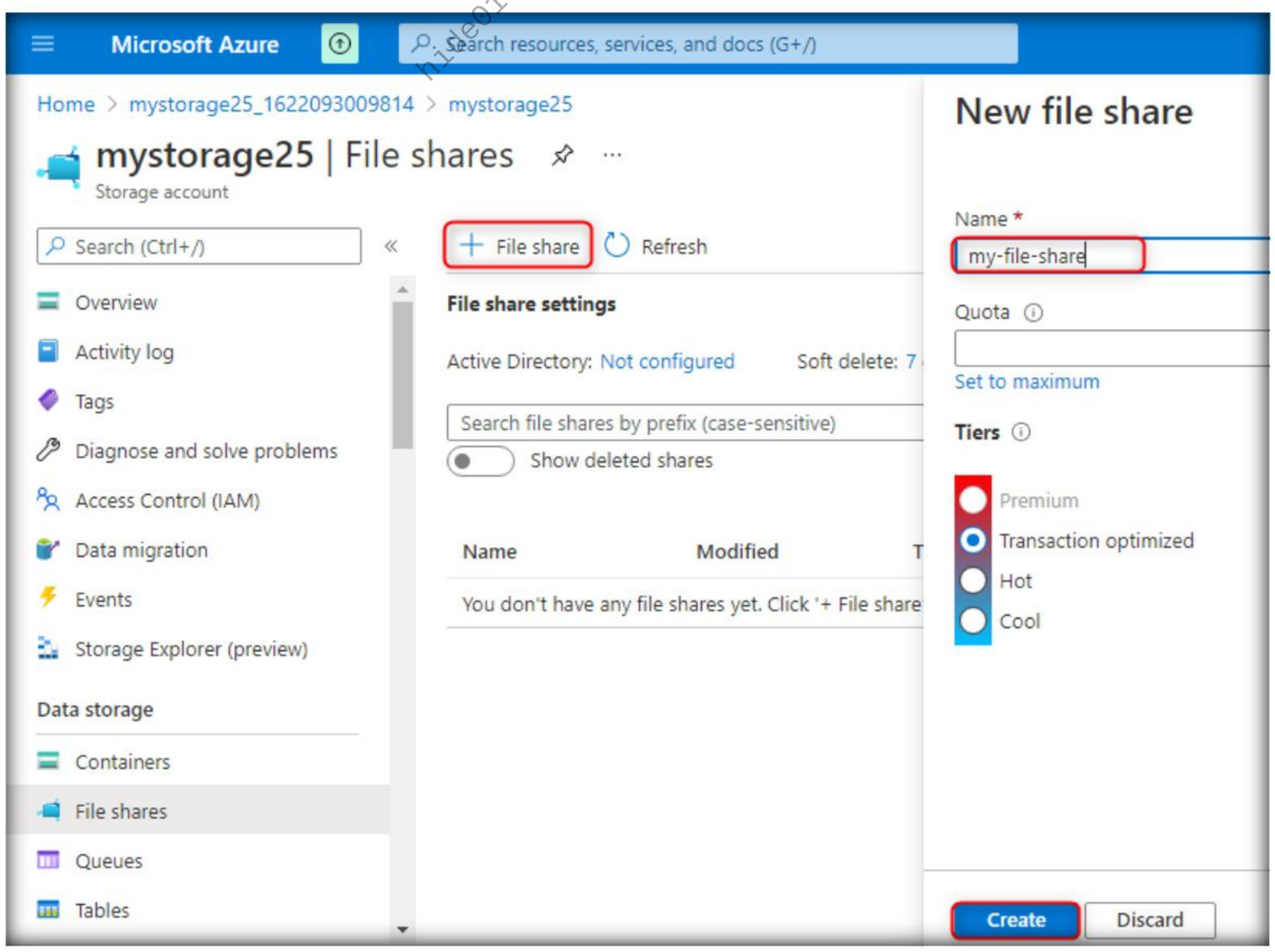


FIGURE 4.10.60: Entering Name of the File Share

Certified Cloud Security Engineer Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

61. The storage file share is successfully created now.

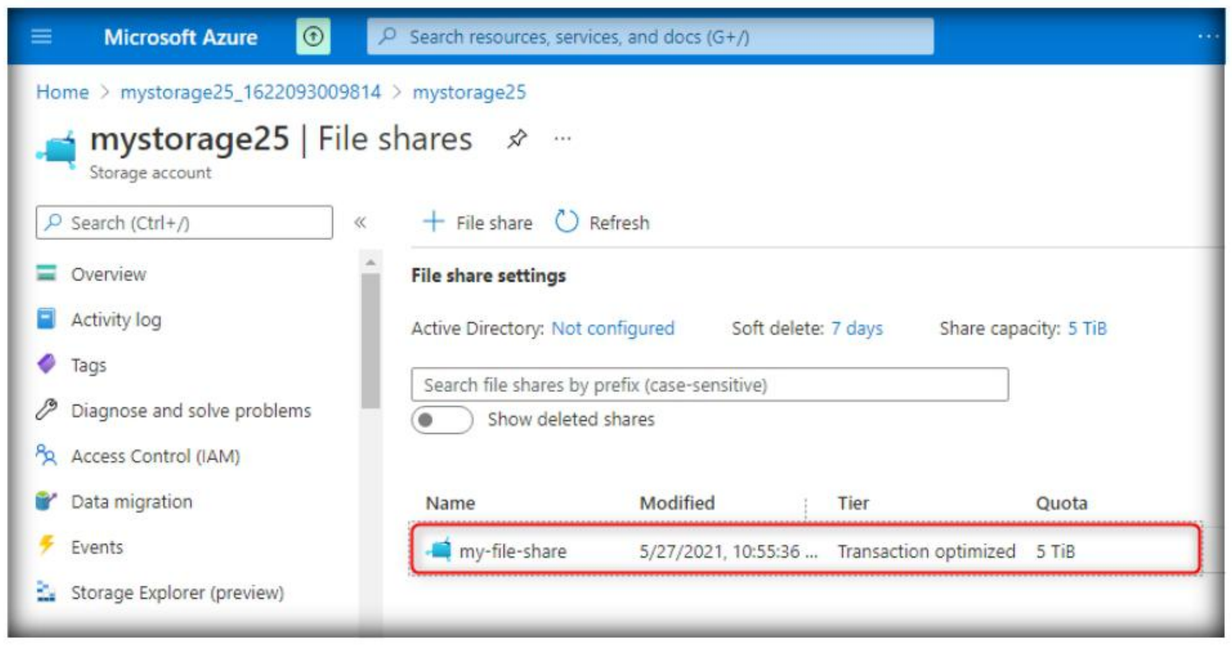


FIGURE 4.10.61: my-file-share is created

62. Click on **mystorage25** to go back to the storage account.

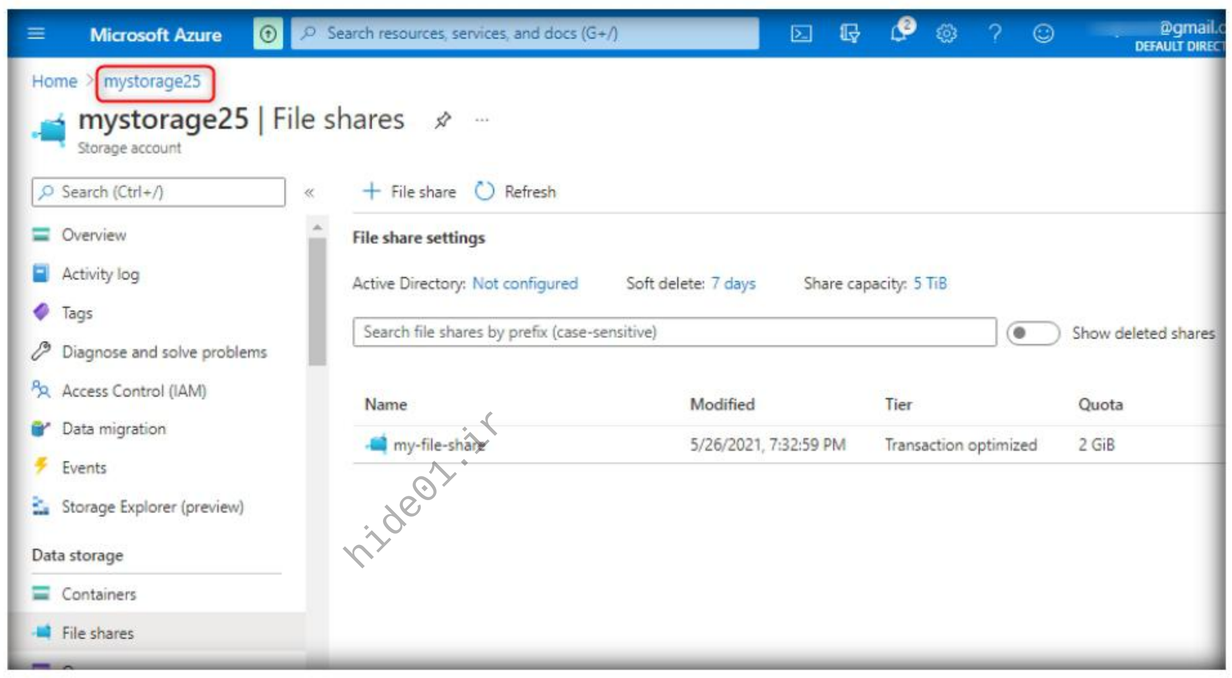


FIGURE 4.10.62: Going Back to Storage Account

63. In the **mystorage25** window, navigate and click on **Networking** under **Security + networking**.

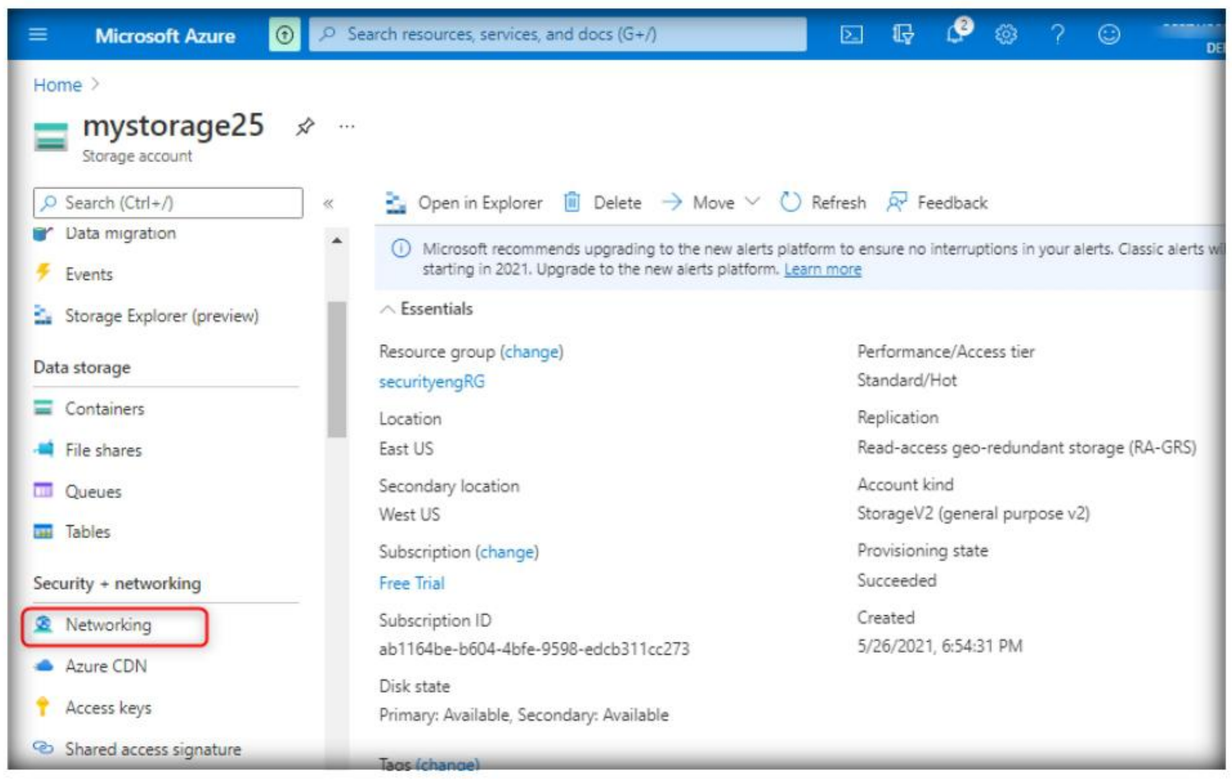


FIGURE 4.10.63: Selecting Networking in Storage Account

TASK 7

Restrict Network Access to a Subnet

Certified Cloud Security Engineer Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

64. Select the **Firewalls and virtual networks** tab.

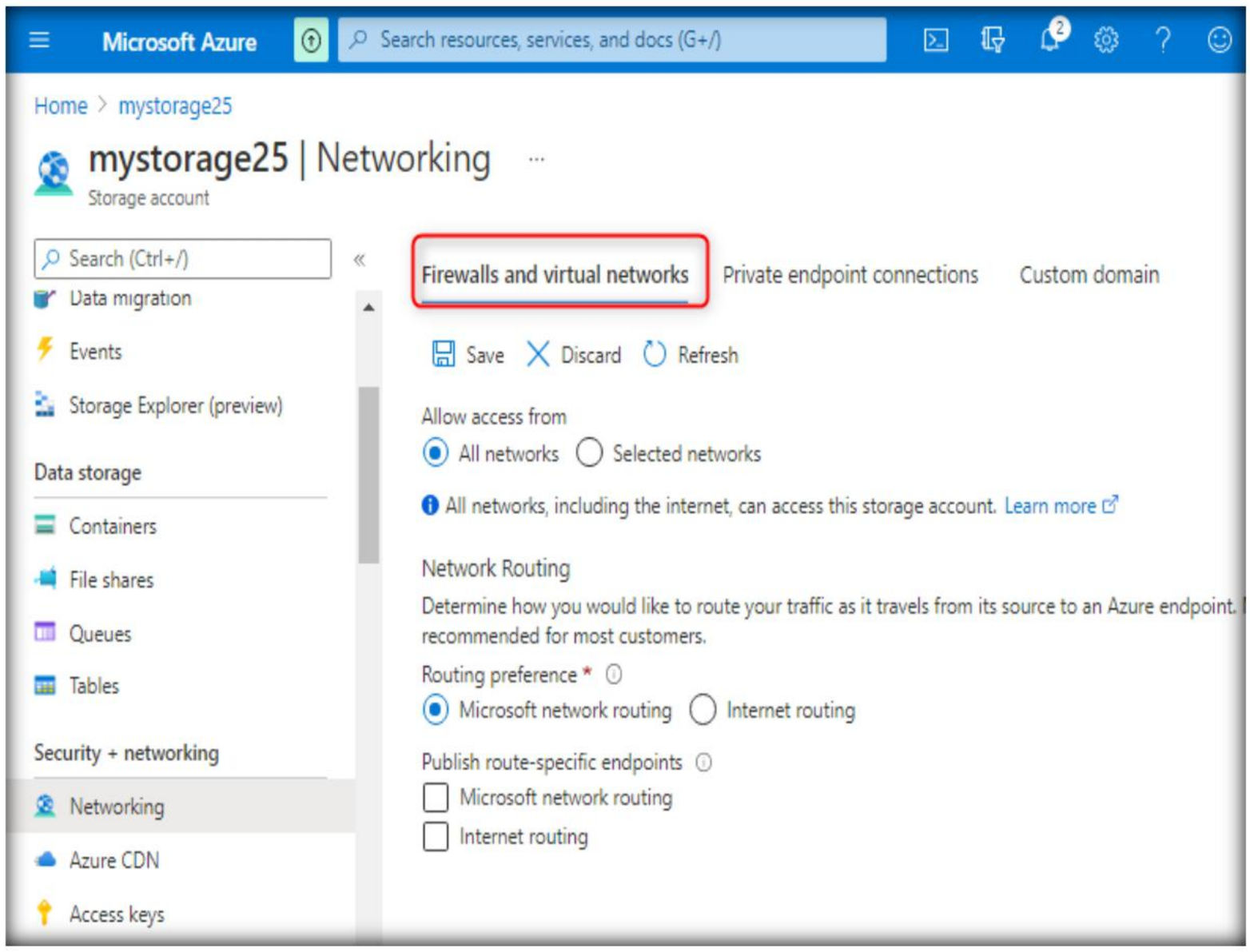


FIGURE 4.10.64: Selecting Firewalls and Virtual Networks Tab

65. Under **Allow access from**, choose the **Selected networks** radio button. Then, click on **+Add existing virtual network** under **Virtual networks.** An **Add networks** pane will open on the left side.

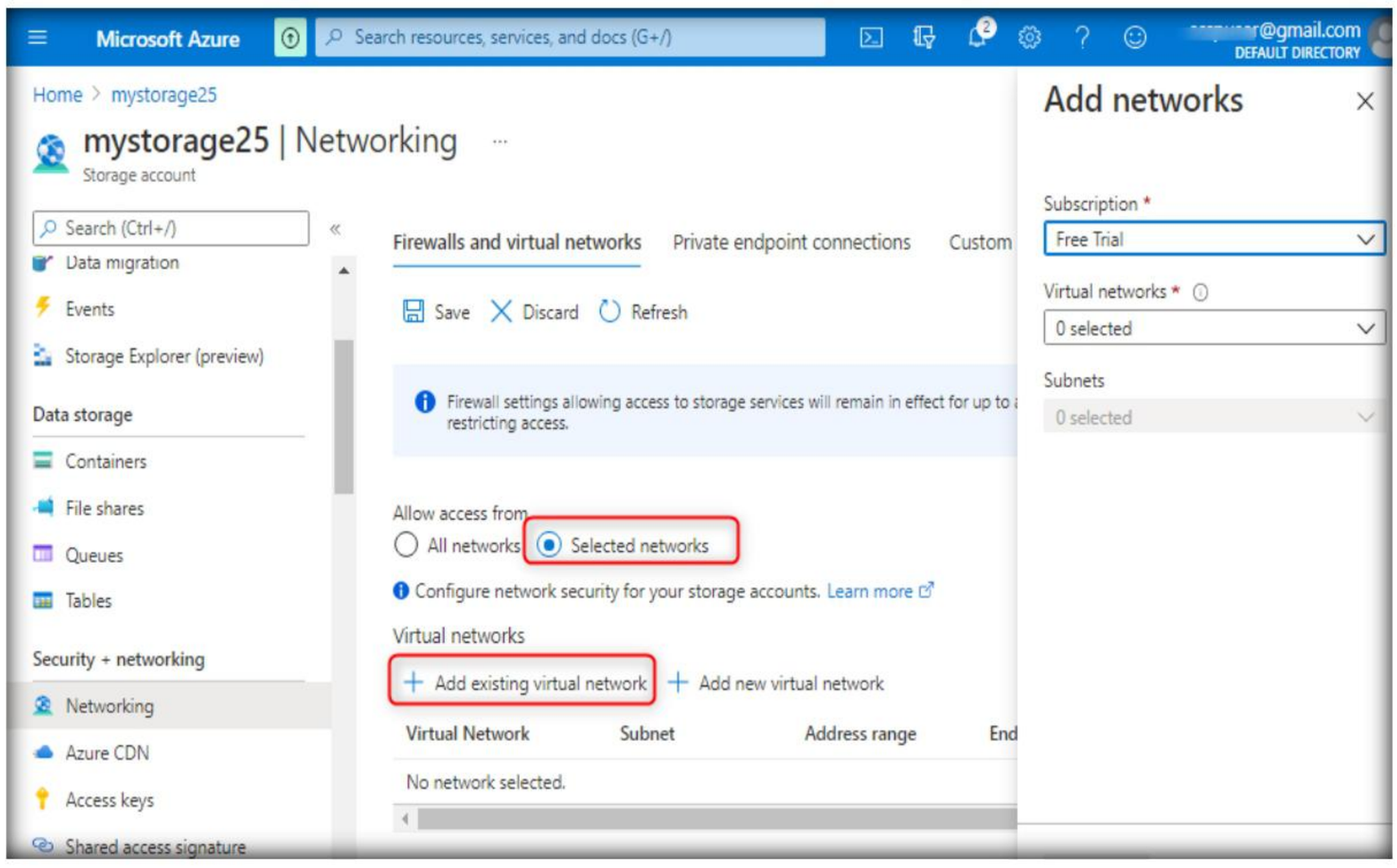


FIGURE 4.10.65: Adding an Existing Virtual Network

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

66. In the **Add networks** pane, select **SecEng-VNET** under **Virtual networks** and **Private** under **Subnets**. Then, click on the **Add** button.

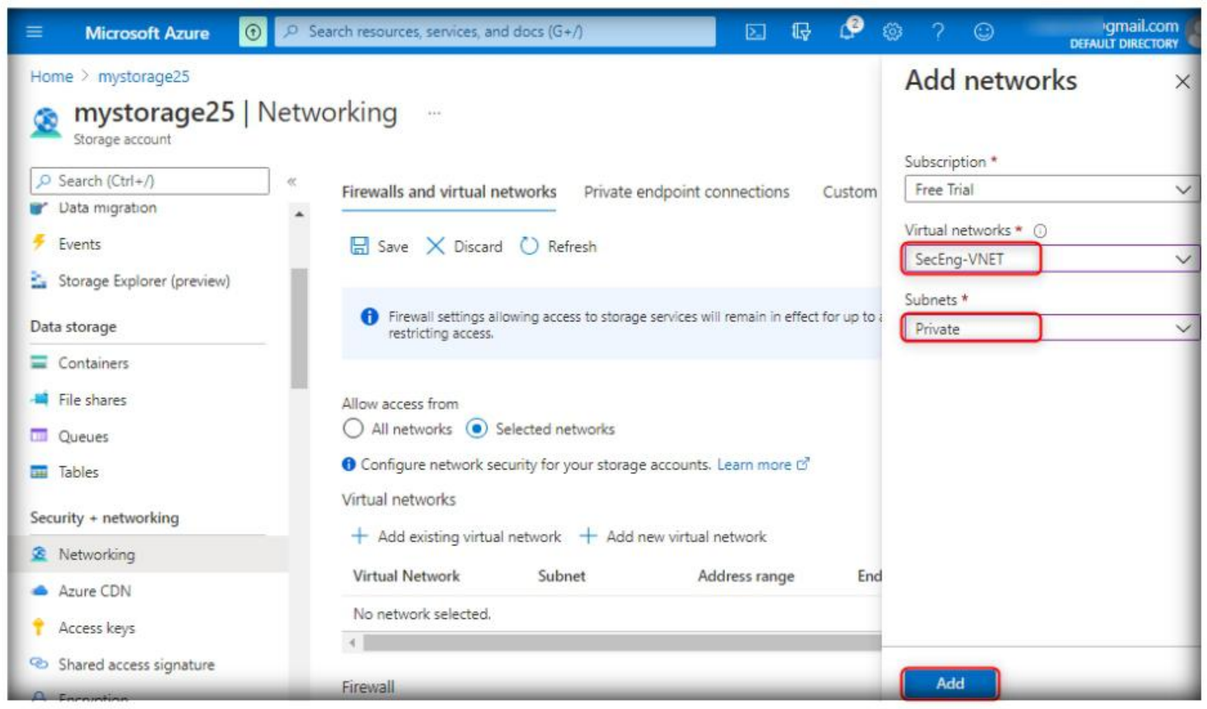


FIGURE 4.10.66: Adding Networks Details

67. The virtual network has been successfully added. Now, click on **Save** to save the settings.

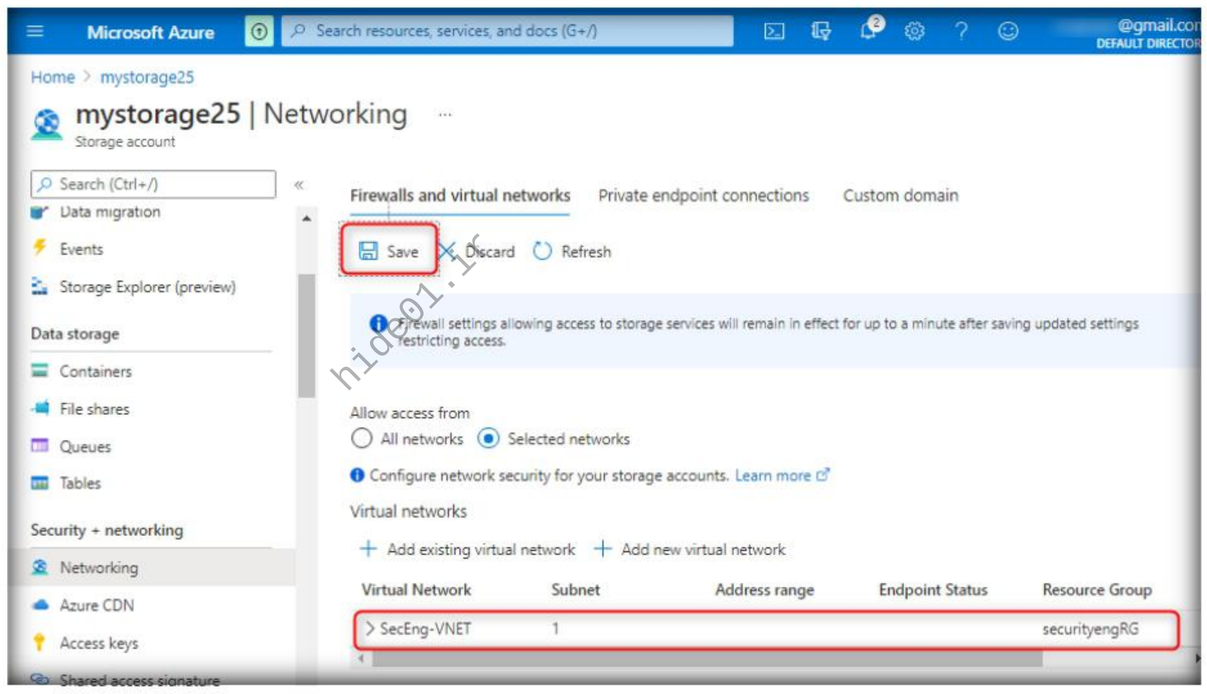


FIGURE 4.10.67: Saving the Virtual Networks

68. The firewall and virtual network settings for the selected storage have been successfully updated.

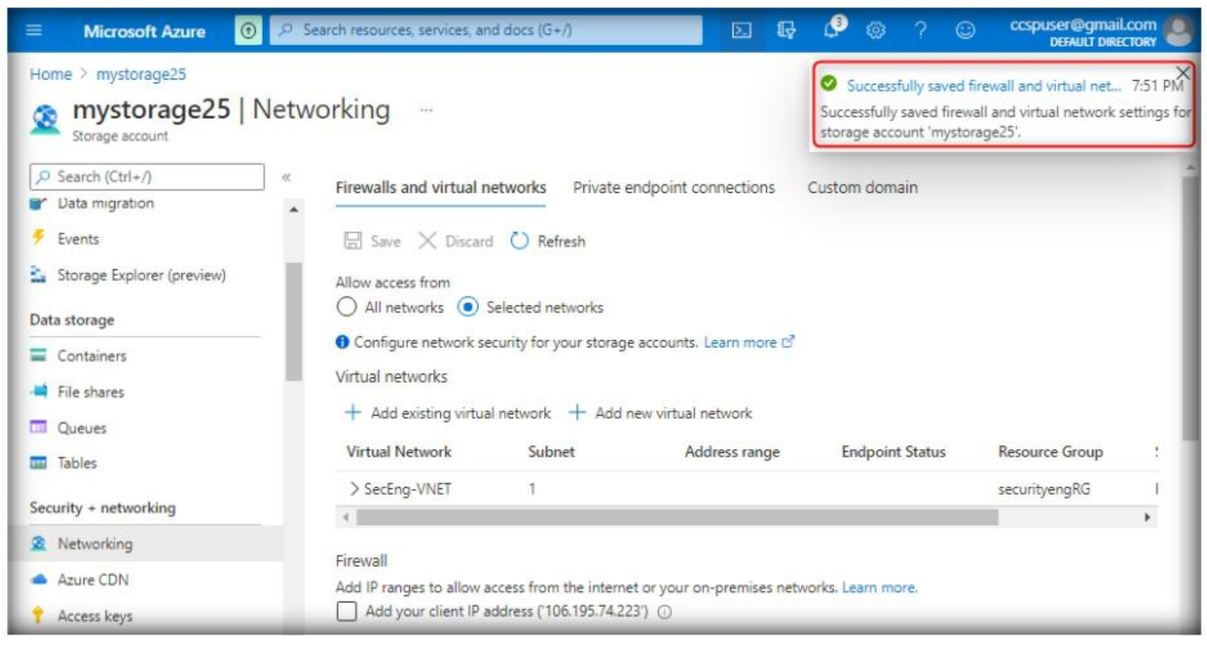


FIGURE 4.10.68: Successfully Saved Firewalls and Virtual Networks

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

69. In **mystorage25**, click on **Access Keys** under **Security + networking**.

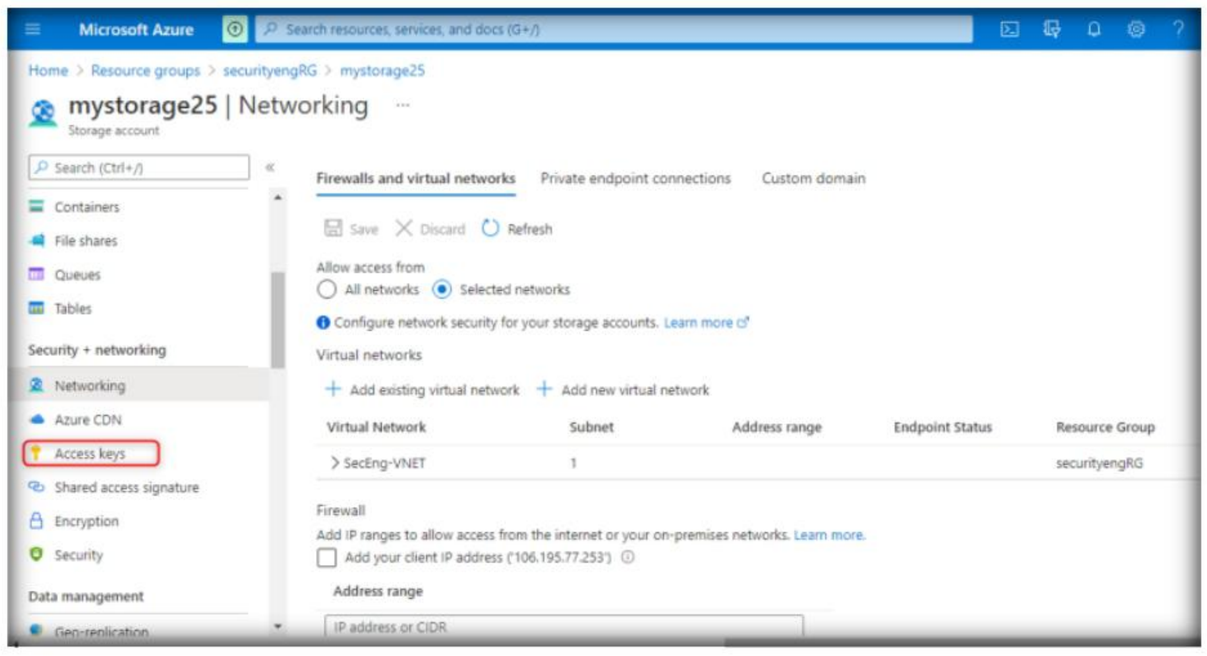


FIGURE 4.10.69: Selecting Access Keys in Storage Account

70. Note down the storage account name (here, **mystorage25**), and then click on the **Hide keys** button.

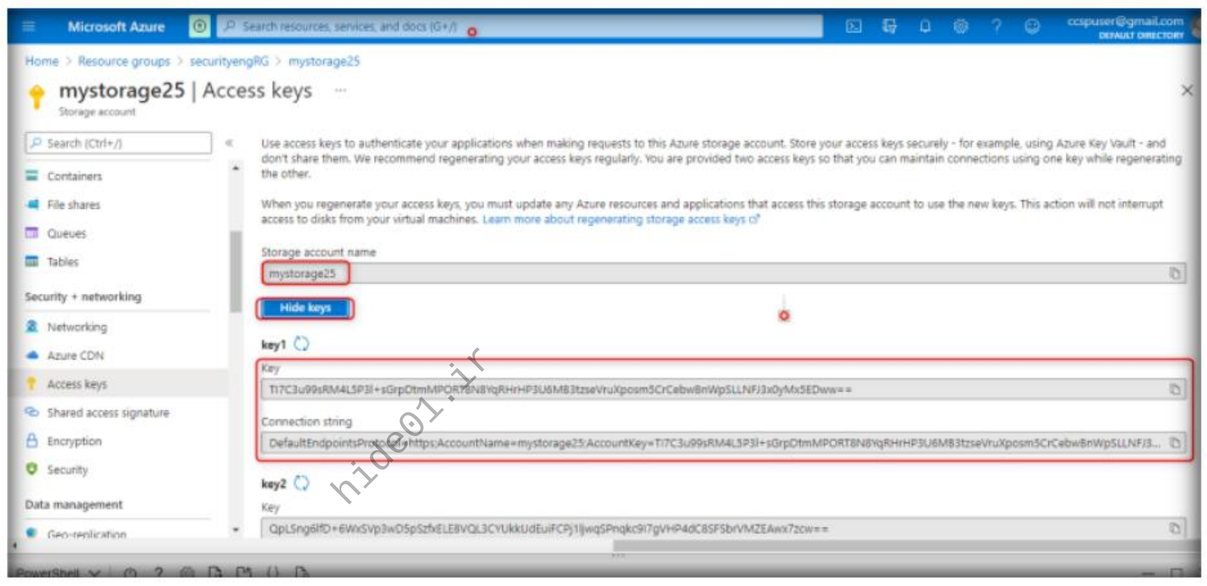


FIGURE 4.10.70: Storage Account Key1

71. Copy the **Key** and **Connection string** in **notepad** and **Save** it on your desktop.

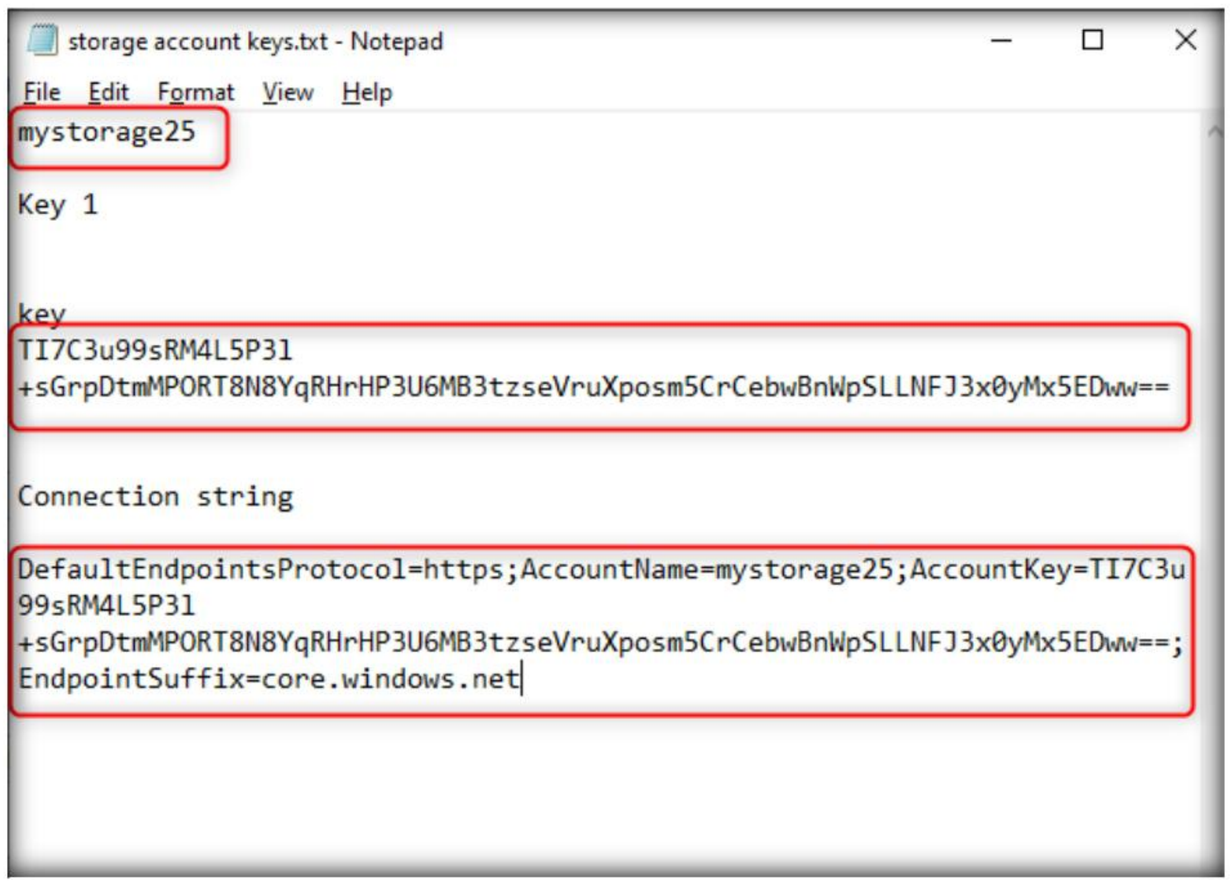


FIGURE 4.10.71: Saving the Storage Account Key1 in Notepad

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 8

Create Virtual Machines

72. You need to create two virtual machines. First, create a virtual machine that will be deployed in a public subnet.

In **mystorage25**, click on **Home** to go back to the Azure portal.

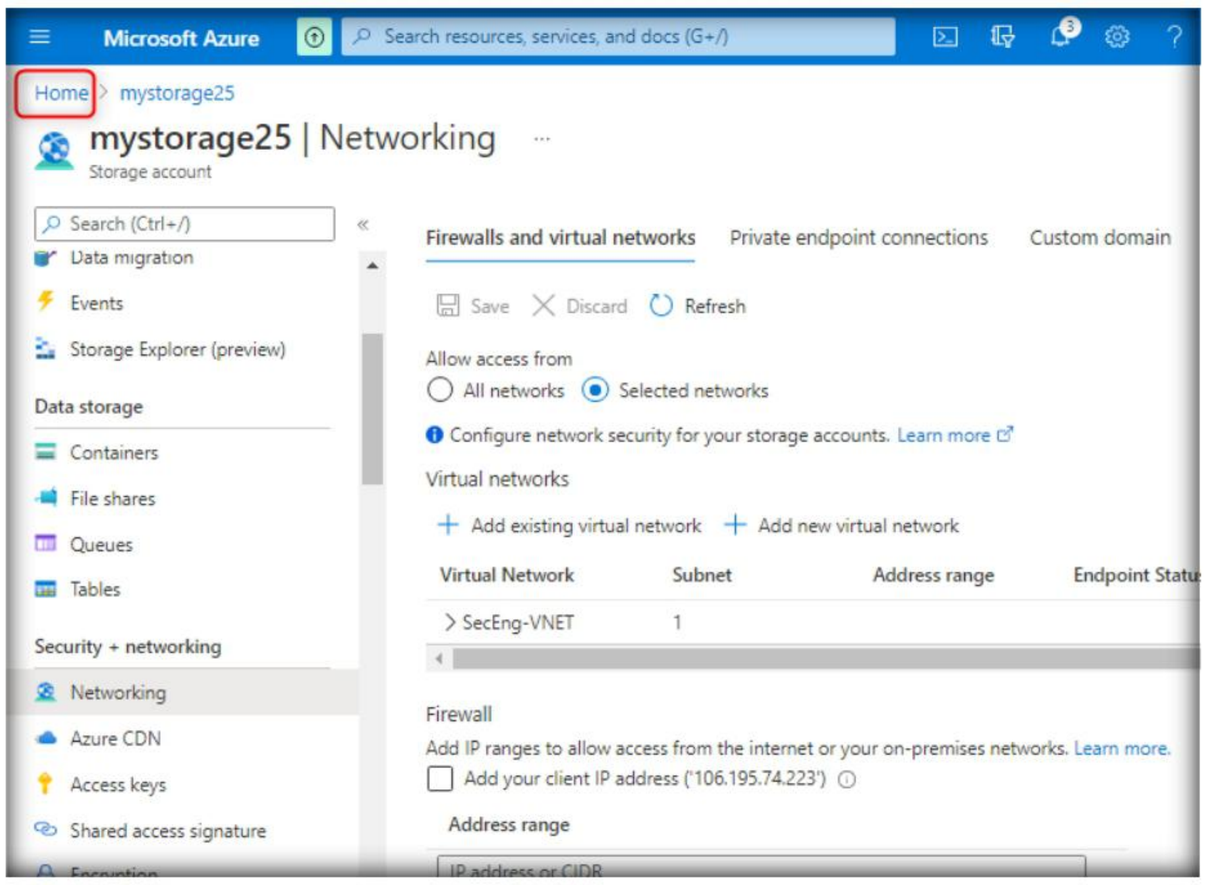


FIGURE 4.10.72: Go Back to Azure Portal

73. Click on **Virtual machines**.

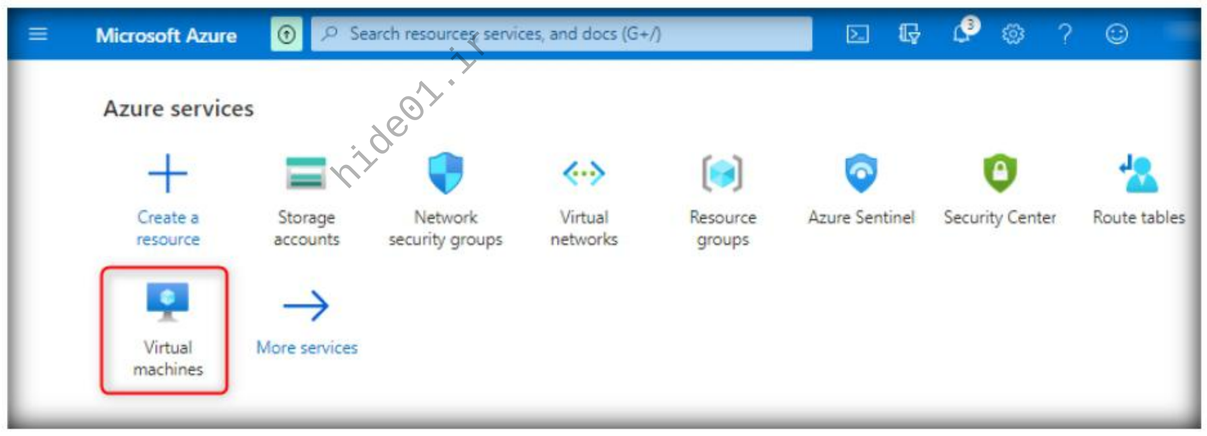


FIGURE 4.10.73: Selecting Virtual Machines

74. Click on **+Add** and then click on **+ Virtual machine**.

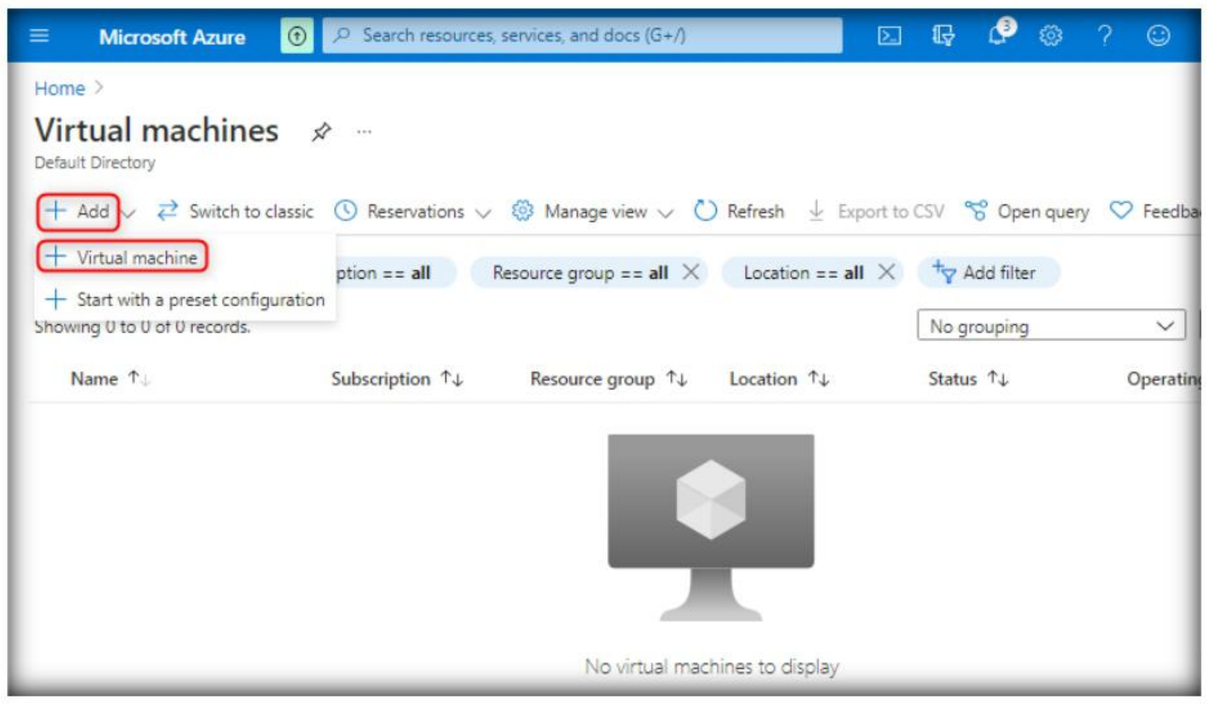


FIGURE 4.10.74: Adding Virtual Machine

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

75. A **Create a virtual machine** window will open. Select **securityengRG** from the dropdown in **Resource group**. In **Virtual machine name**, type **myVMPublic**.

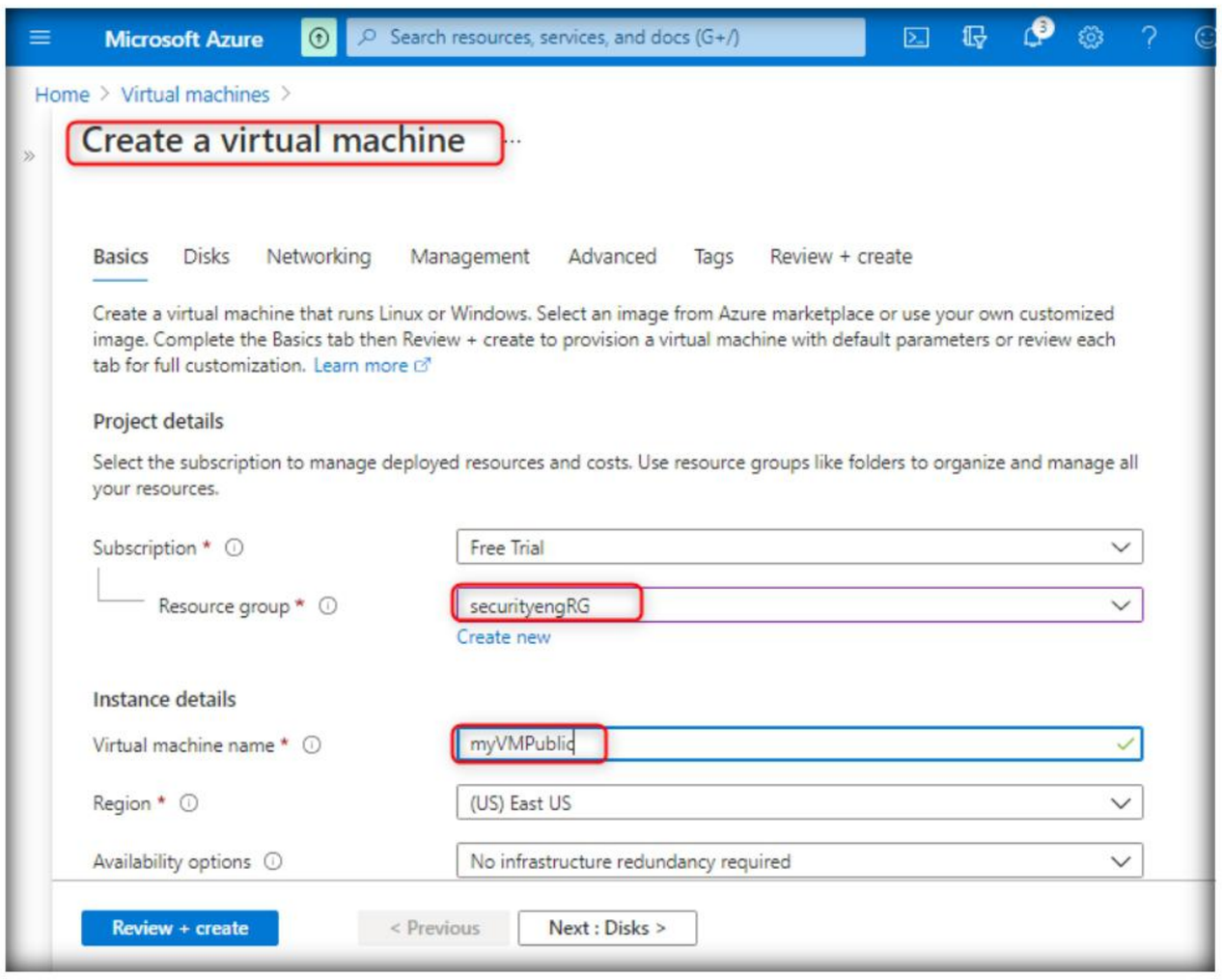


FIGURE 4.10.75: Entering Resource Group and Virtual Machine Name

76. In the **Image** field, select **Window Server 2016 Datacenter – Gen 1**. Under **Administrator account**, type **Username** as **CCSEtester1** and **Password** as **Administrator@321** and confirm the same password. Then, click on **Next: Disks >**.

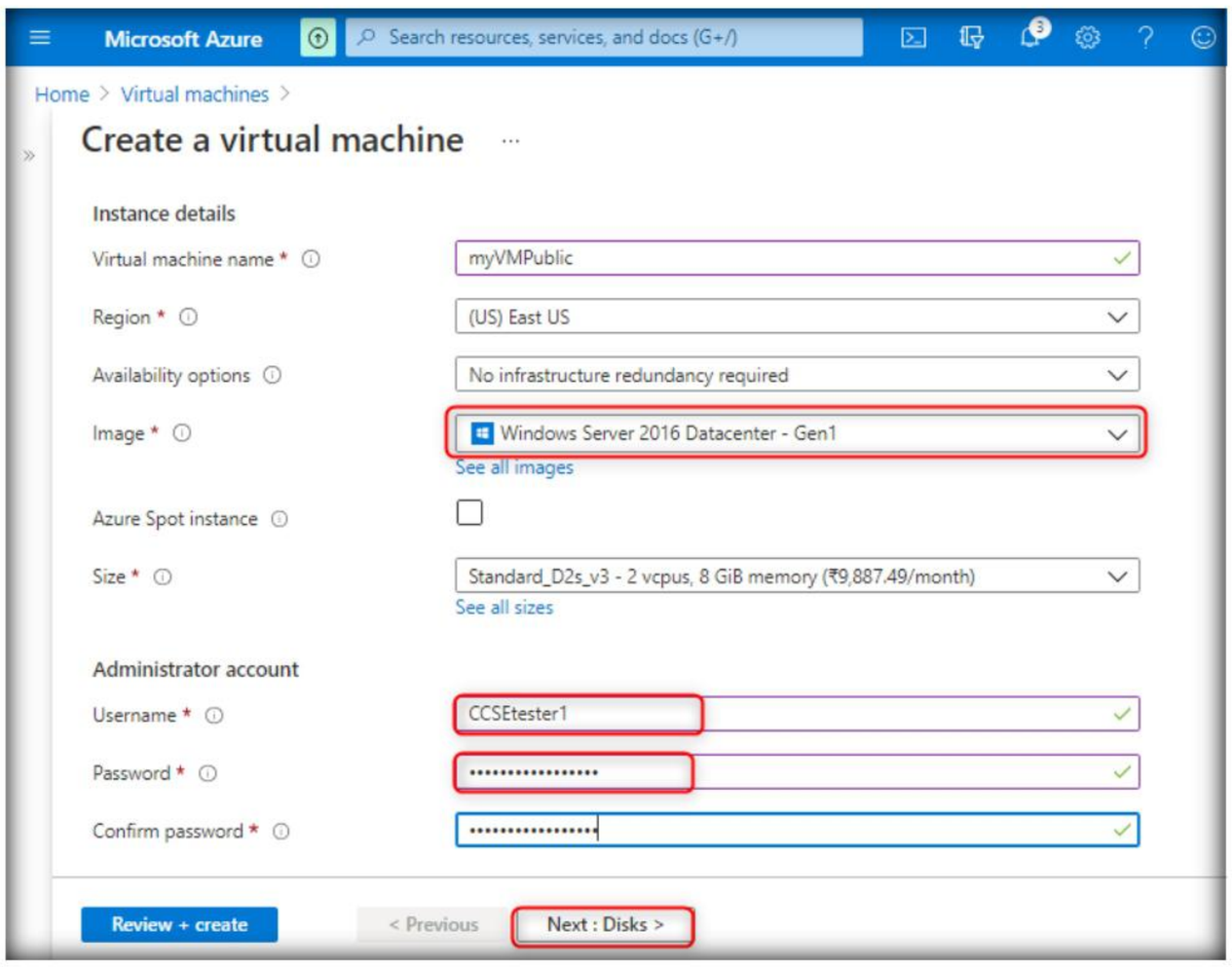


FIGURE 4.10.76: Selecting Image and Filling Login Credentials for VM

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

77. In the **Disks** tab, leave everything in their default state and click on **Next: Networking >**.

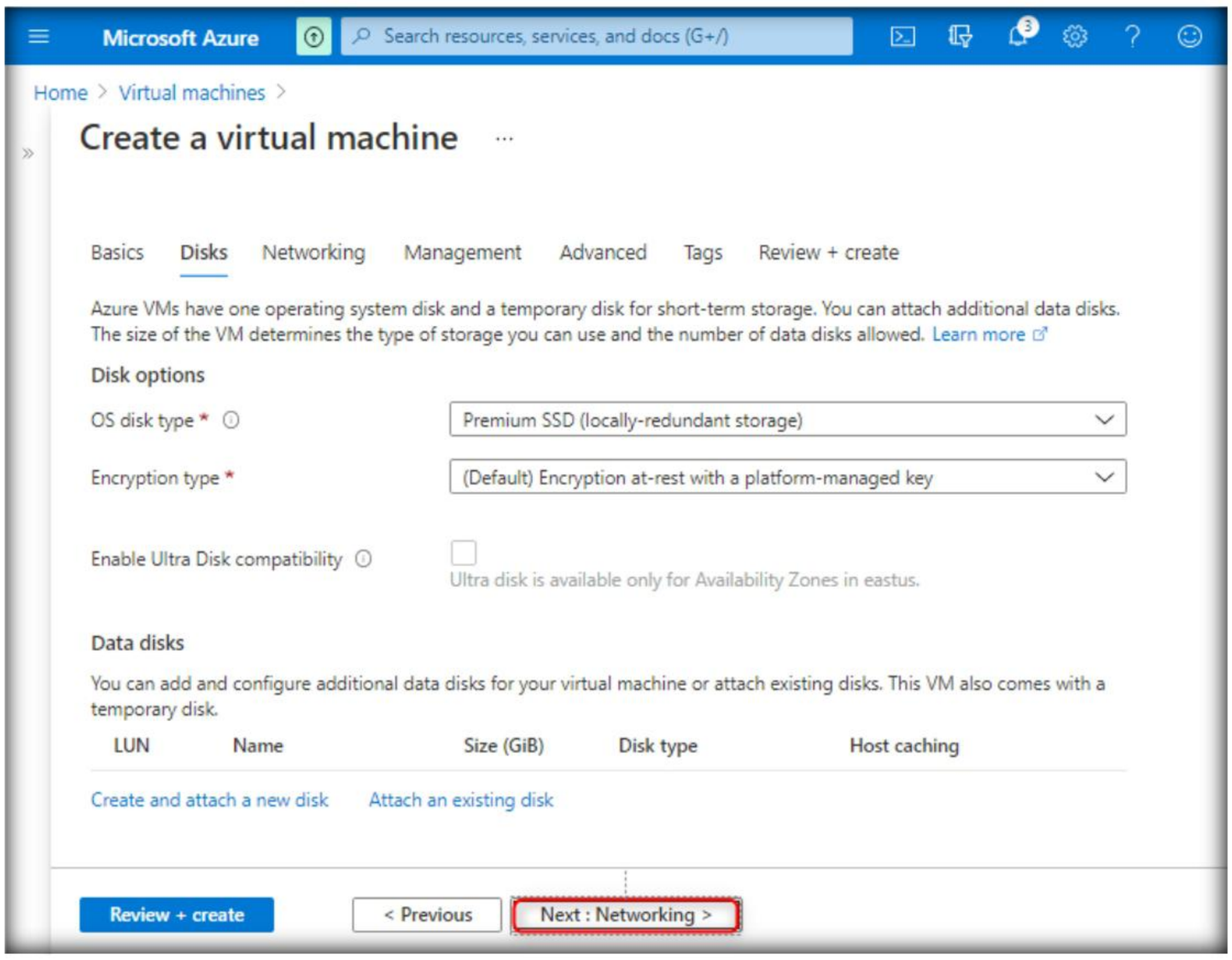


FIGURE 4.10.77: Leaving Disk Tab in Default State

78. In the **Networking** tab, select **Subnet** as **Public**, **NIC network security group** as **Basic**, and **Select inbound ports** as **RDP (3389)**. Then, click on **Next: Management >**.

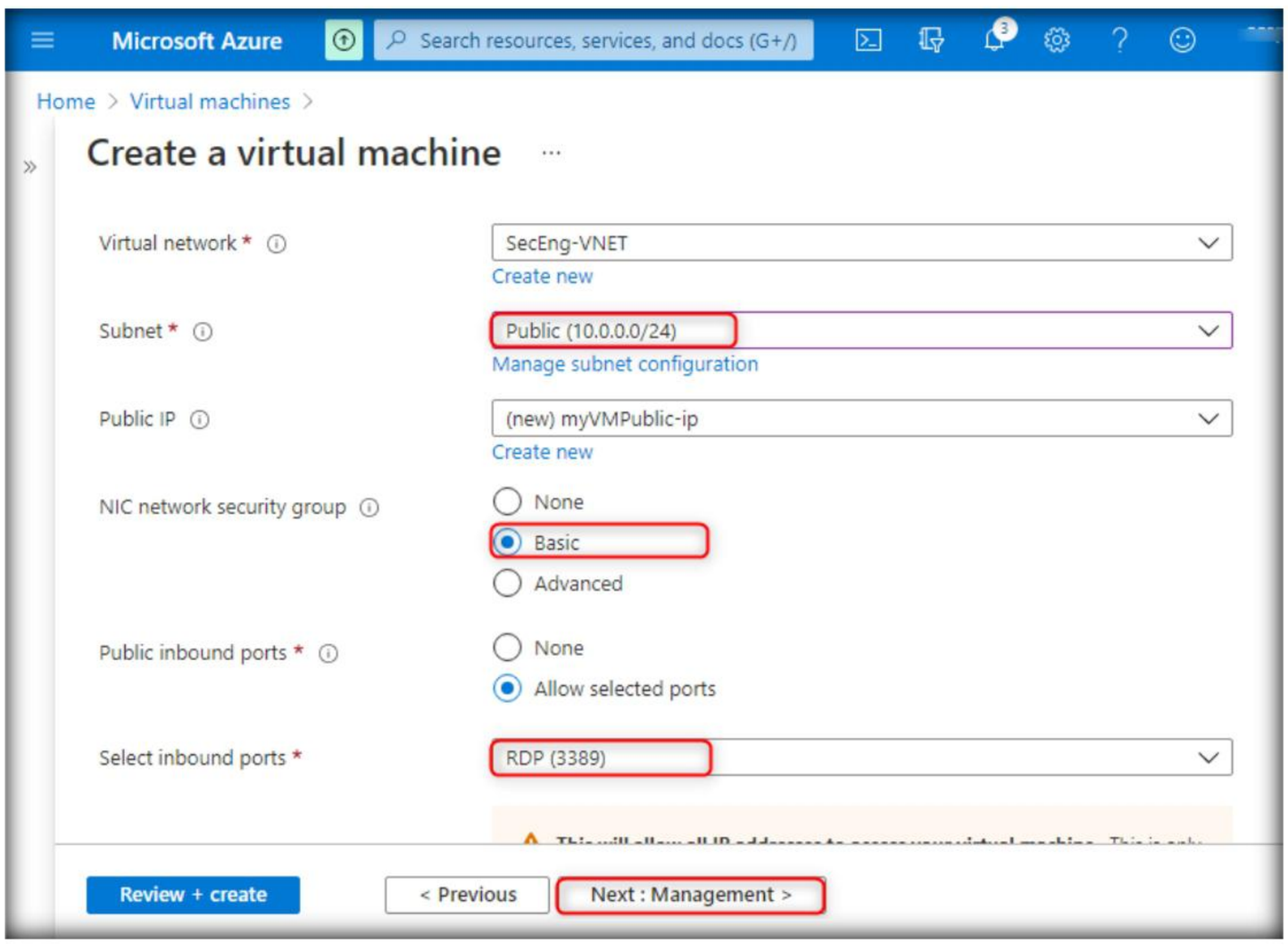


FIGURE 4.10.78: Selecting Subnet, NIC network Security Group, and Inbound Ports

Certified Cloud Security Engineer Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

79. In the **Management** tab, select the **Disable** radio button under **Boot diagnostics**. Then, click on **Next: Advanced >**.

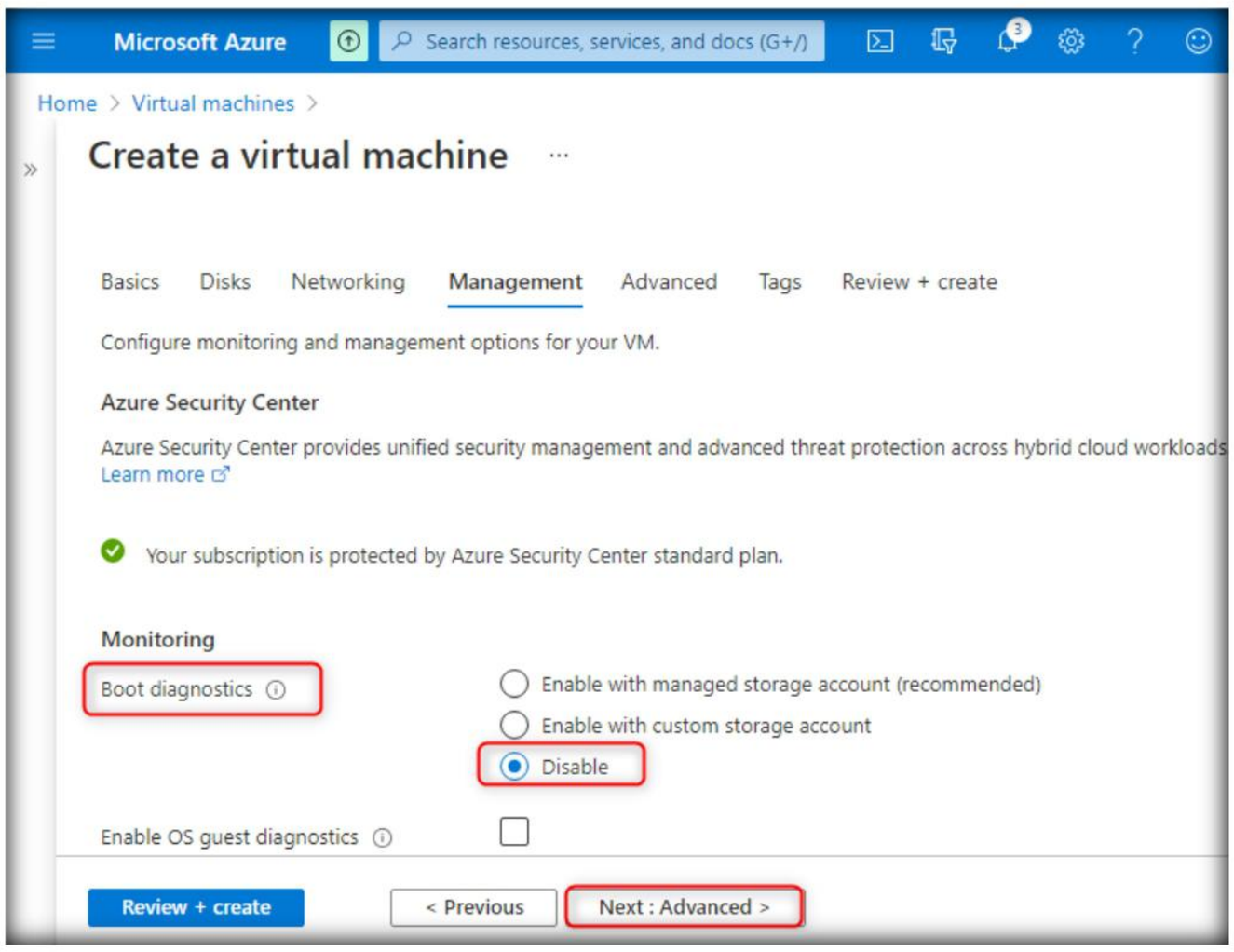


FIGURE 4.10.79: Selecting Disable Radio Button for Boot Diagnostics

80. In the **Advanced** tab, leave everything in their default state and click on the **Next: Tags** button.

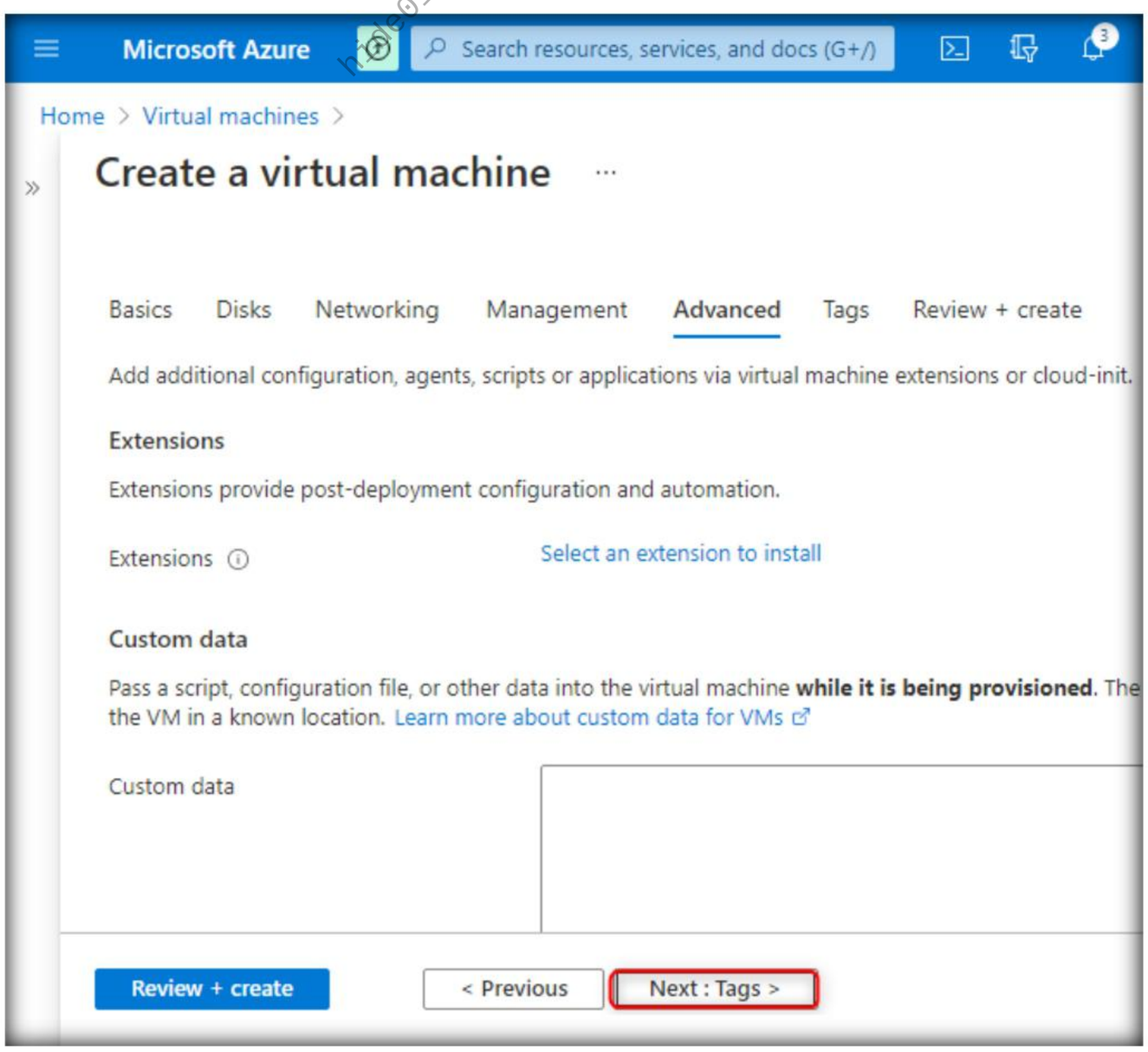


FIGURE 4.10.80: Leaving Advanced Tab in Default State

Certified Cloud Security Engineer Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

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

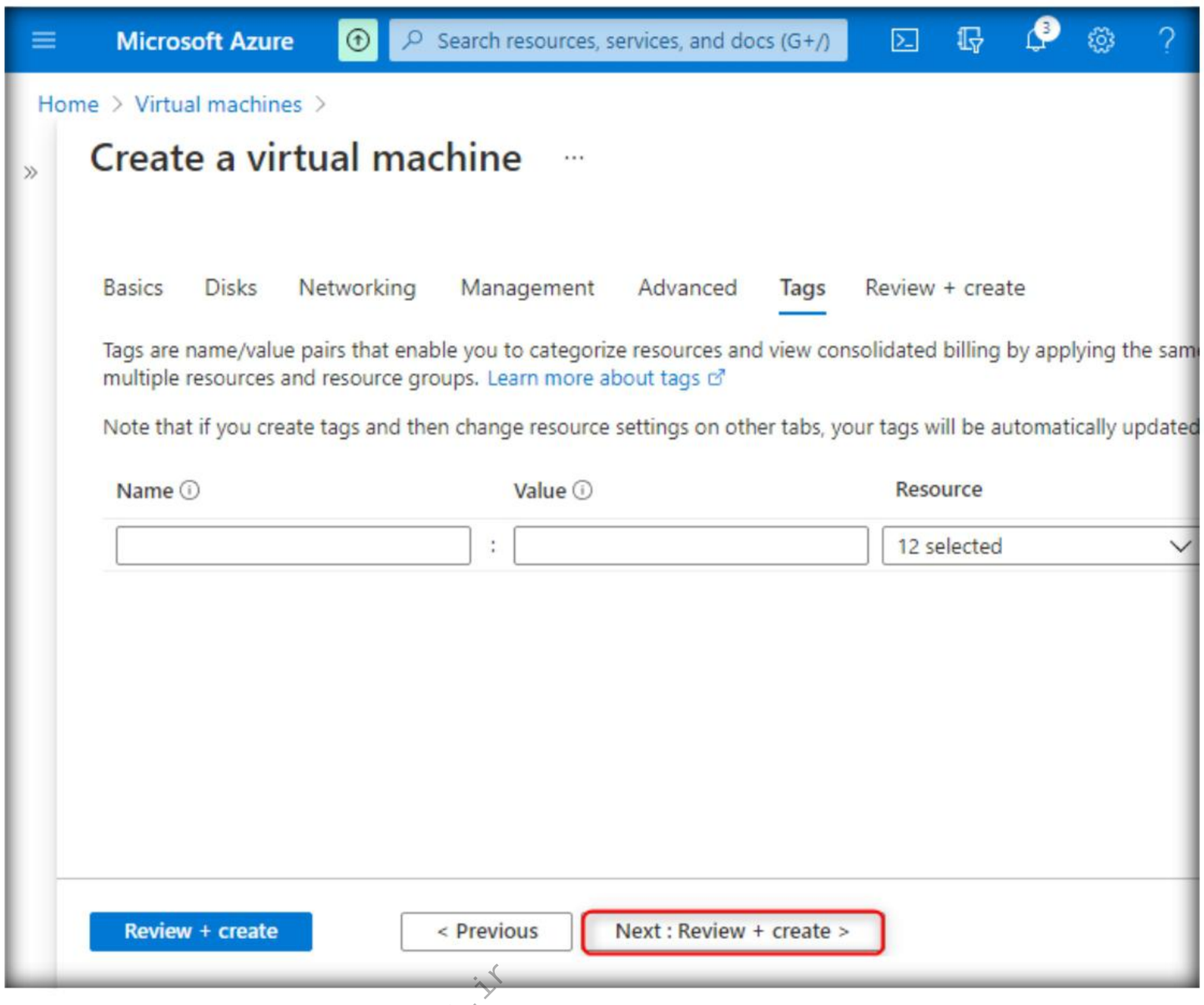


FIGURE 4.10.81: Leaving Tags Tab in Default State

82. After seeing the **Validation passed** message, click on **Create**.

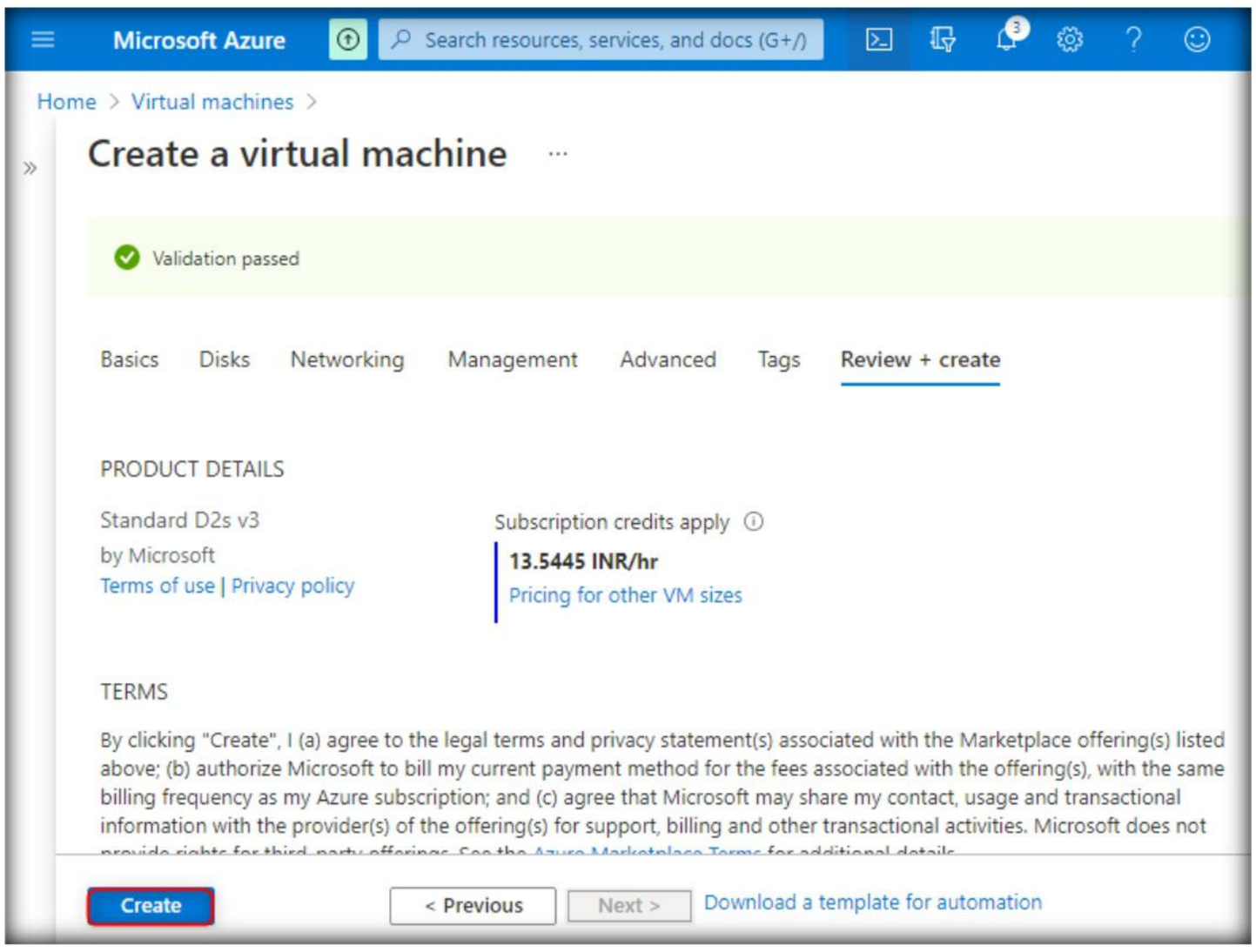


FIGURE 4.10.82: Creating a VM after Validation Passed

Certified Cloud Security Engineer Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

83. After the successful deployment of the virtual machine, click on the **Go to resource** button.

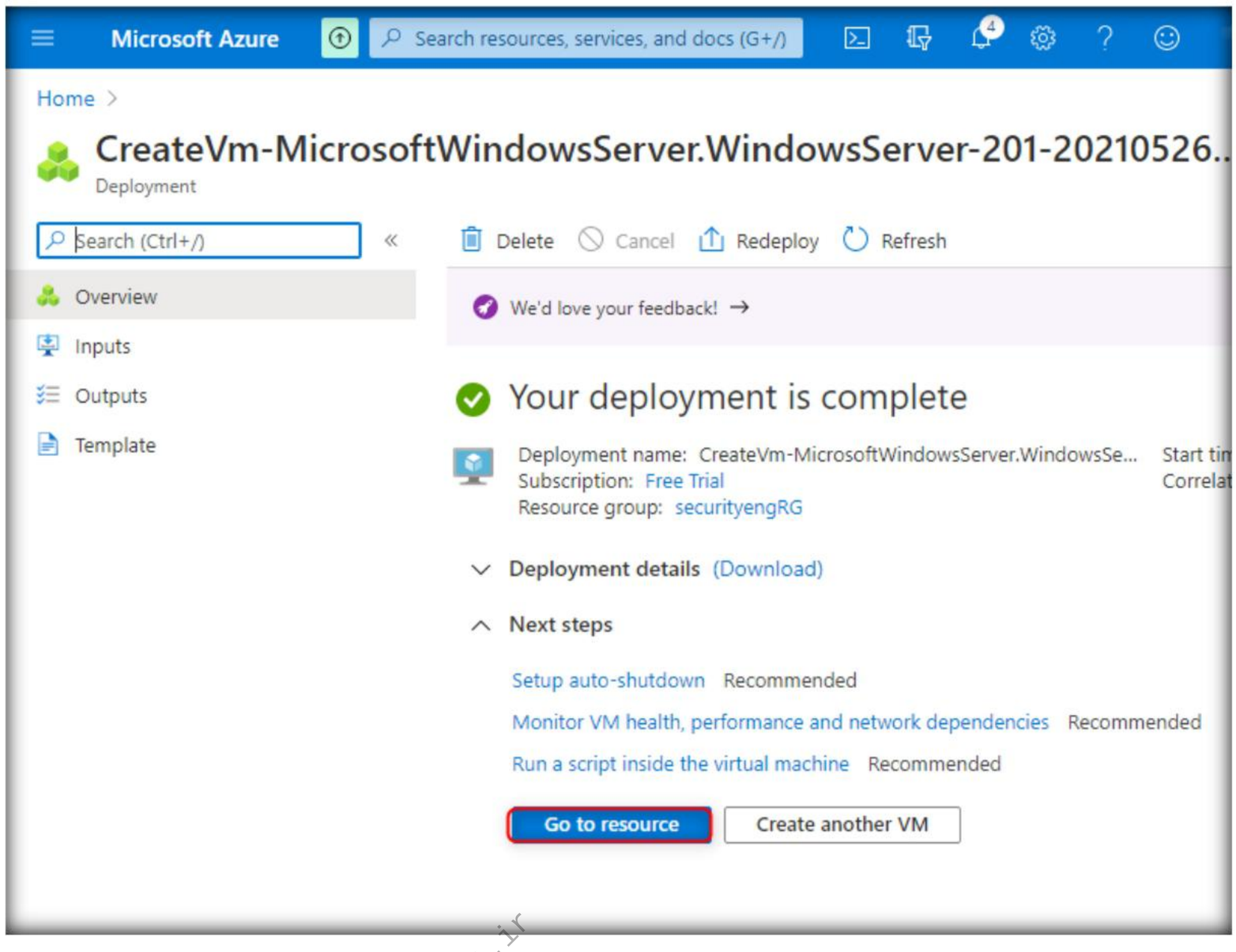


FIGURE 4.10.83: Successful Deployment of VM

84. **myVMPublic** virtual machine has been successfully created.

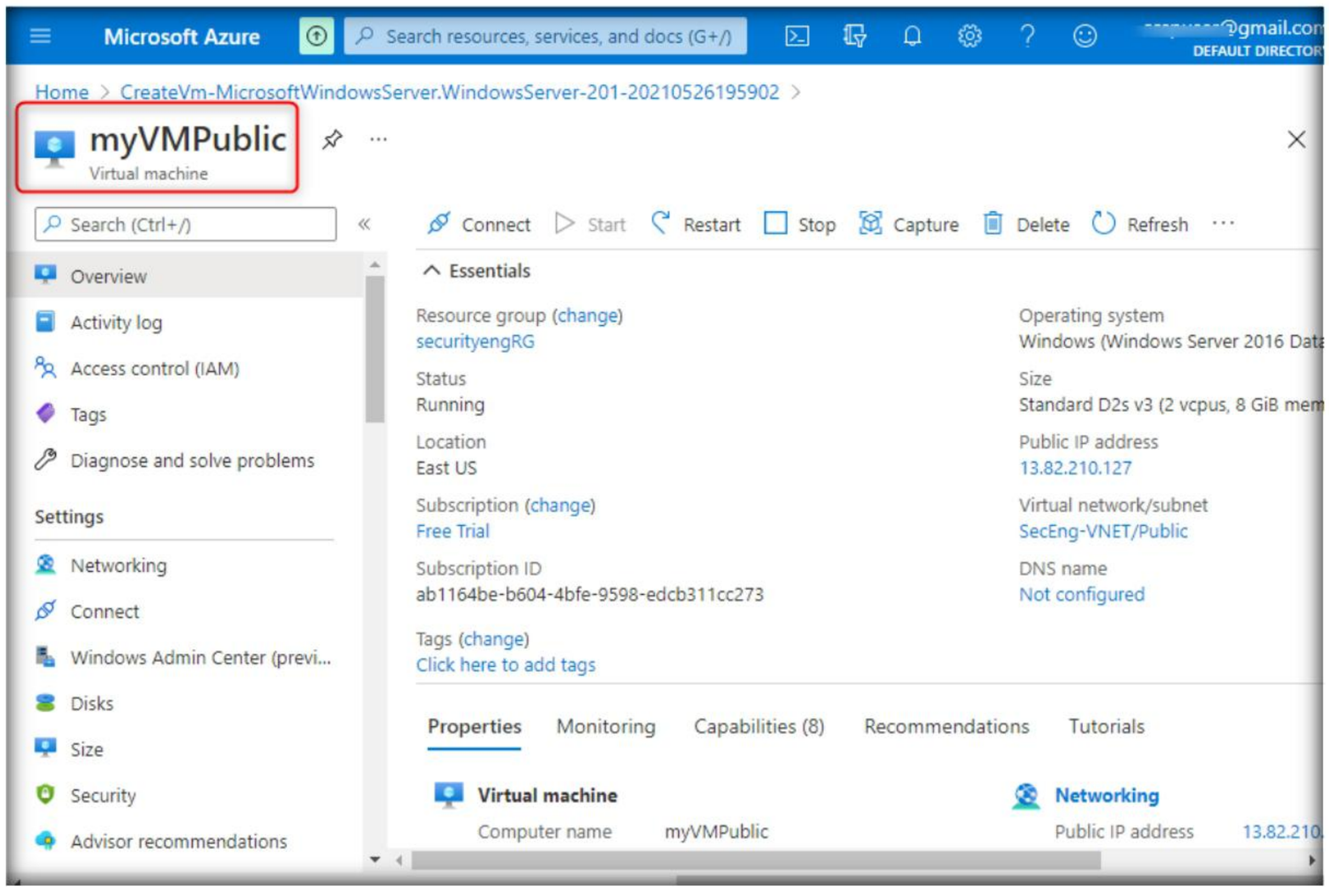


FIGURE 4.10.84: Successful Creation of myVMPublic Virtual Machine

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

85. Now, you will create a second virtual machine. Click on **Home** to go back to the Azure portal.

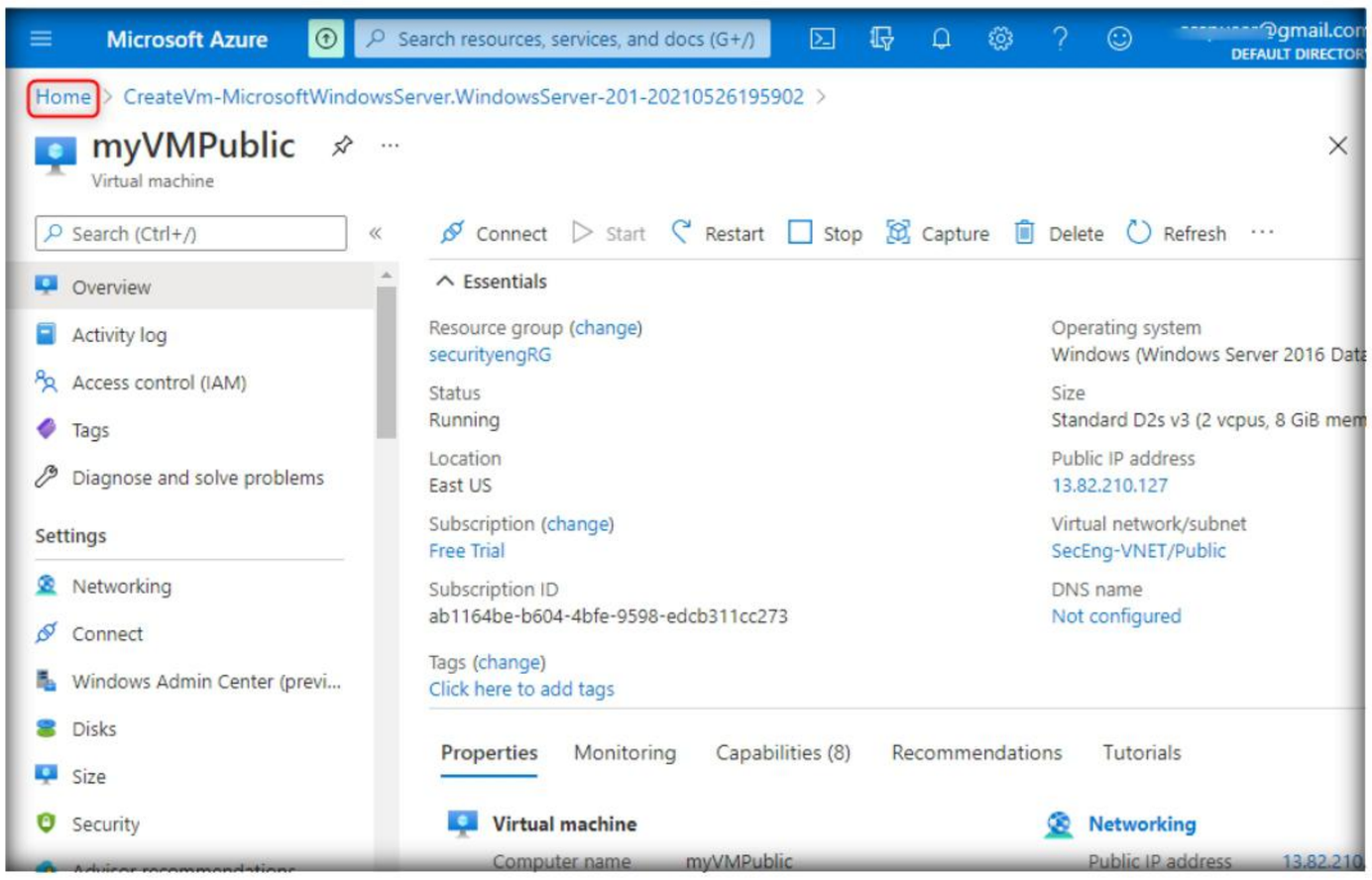


FIGURE 4.10.85: Selecting Home to Go Back to Azure Portal

86. Click on **Virtual machines**.

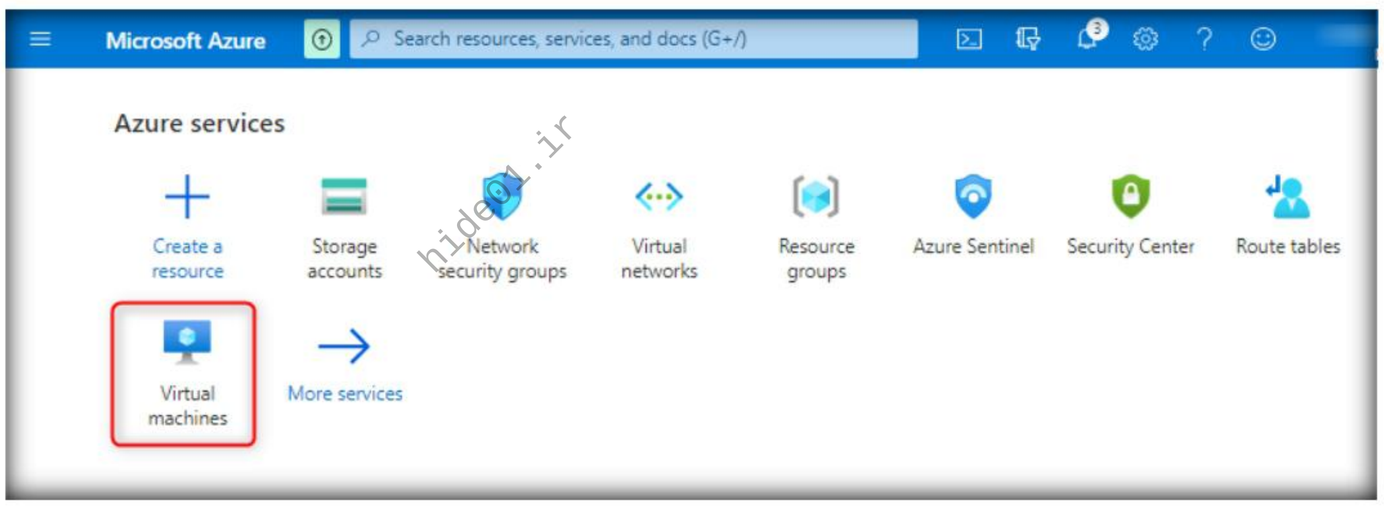


FIGURE 4.10.86: Selecting Virtual Machines

87. Click on **+Add** and then on **+ Virtual machine**.

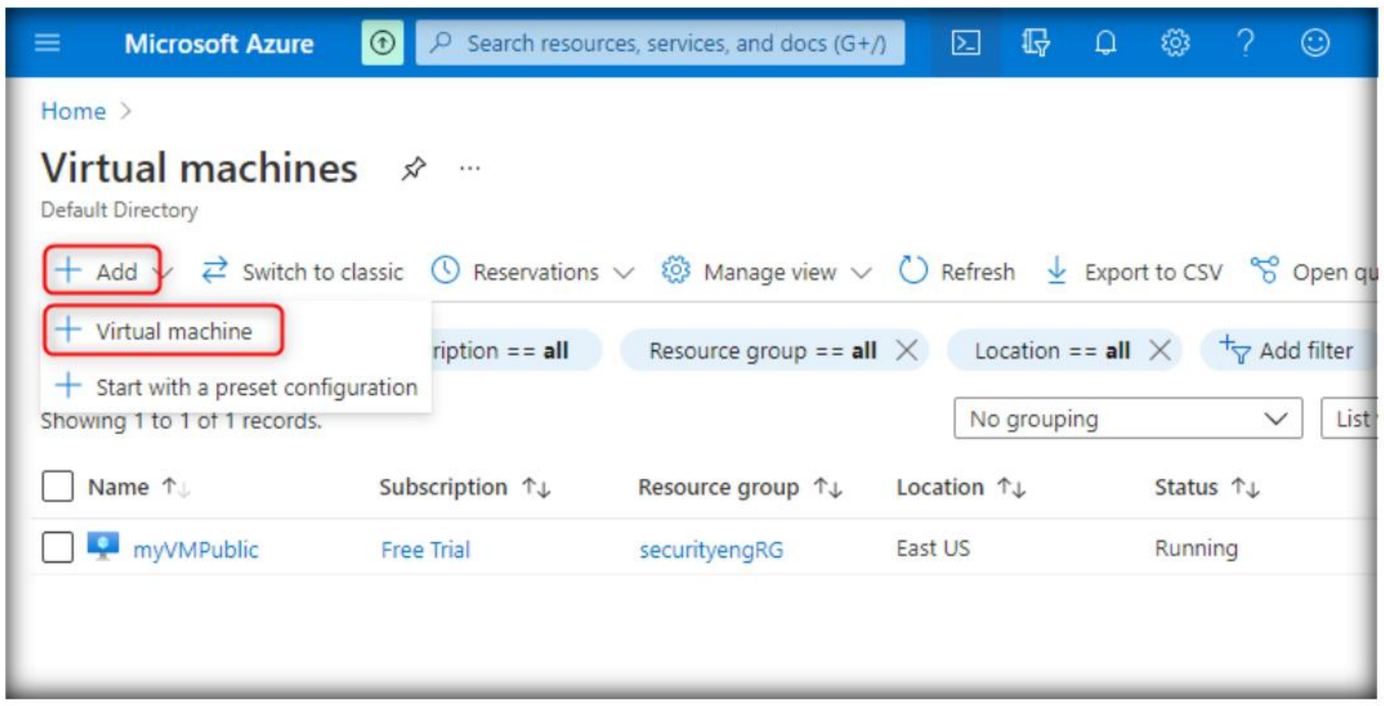


FIGURE 4.10.87: Adding Virtual Machine

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

88. A **Create a virtual machine** window will open. In the **Resource group** field, select **securityengRG** from the dropdown. In the **Virtual machine name** field, type **myVMPrivate**.

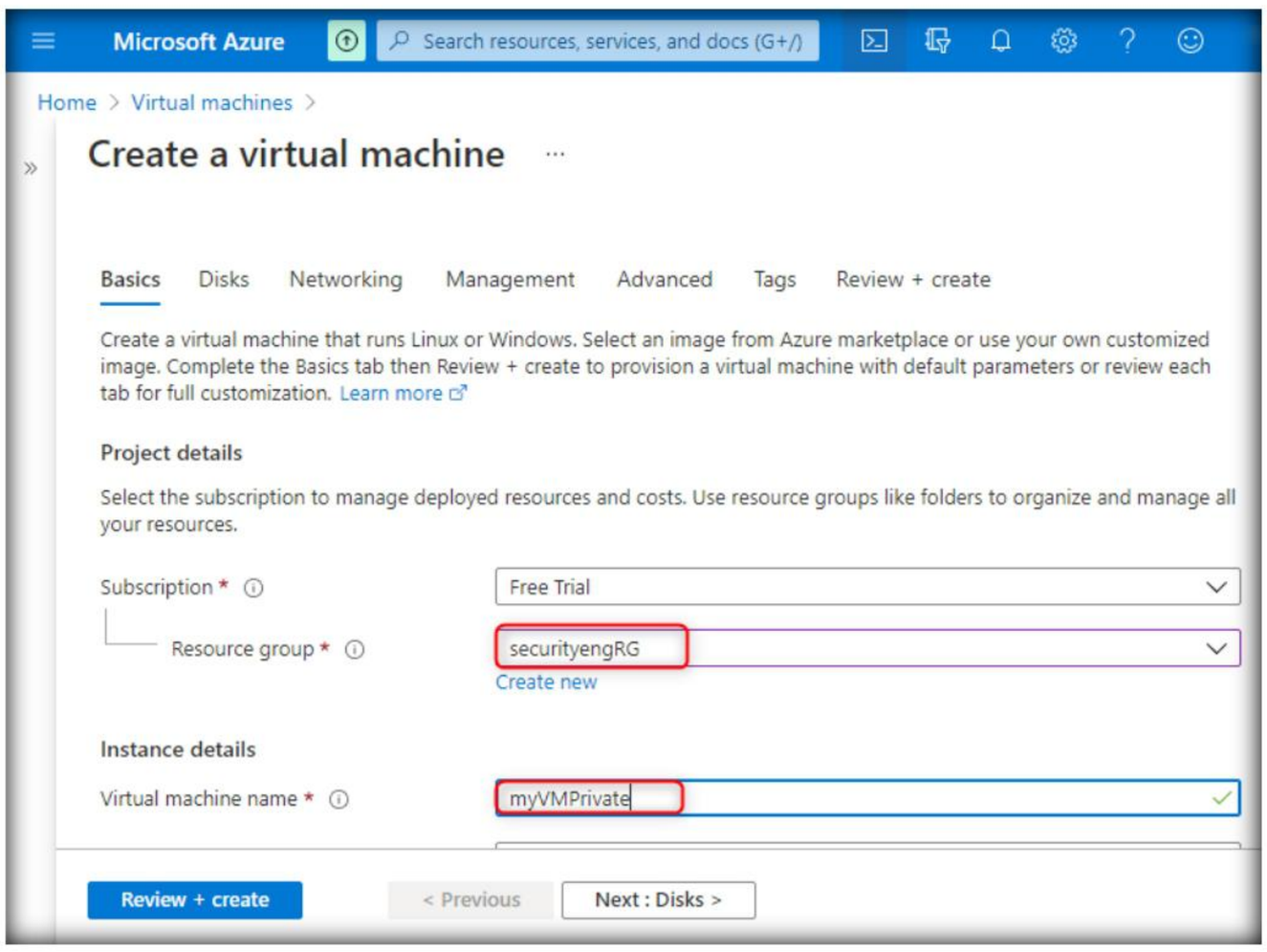


FIGURE 4.10.88: Entering Resource Group and Virtual Machine Name

89. For the Image field, select **Window Server 2016 Datacenter – Gen 1**. Under **Administrator account**, type **Username** as **CCSEtester2** and **Password** as **Administrator@456**, and then confirm the same password. Then, click on **Next: Disks >**.

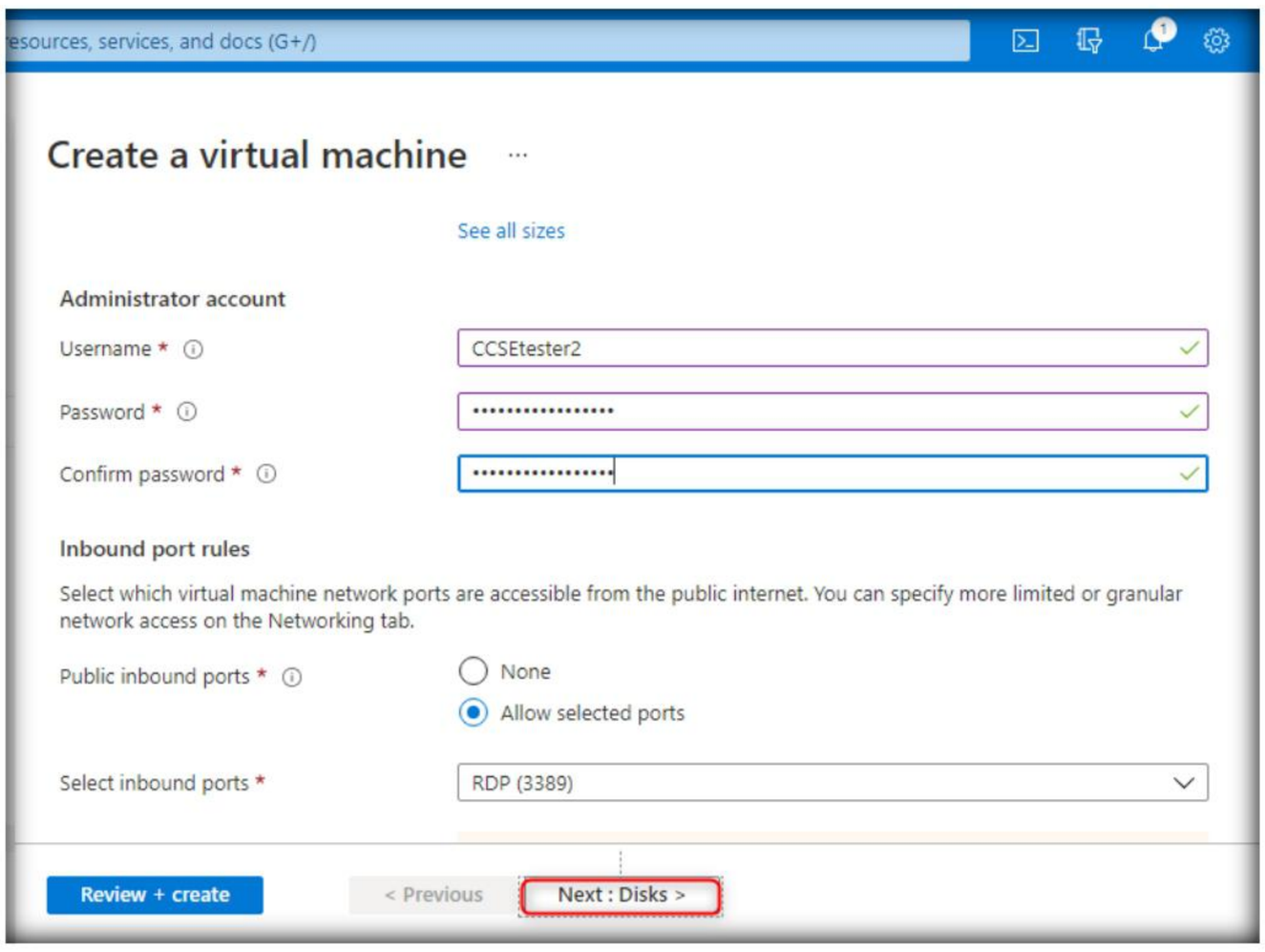


FIGURE 4.10.89: Entering Login Credentials for VM

90. In the **Disks** tab, leave everything in their default state and click on **Next: Networking >**.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

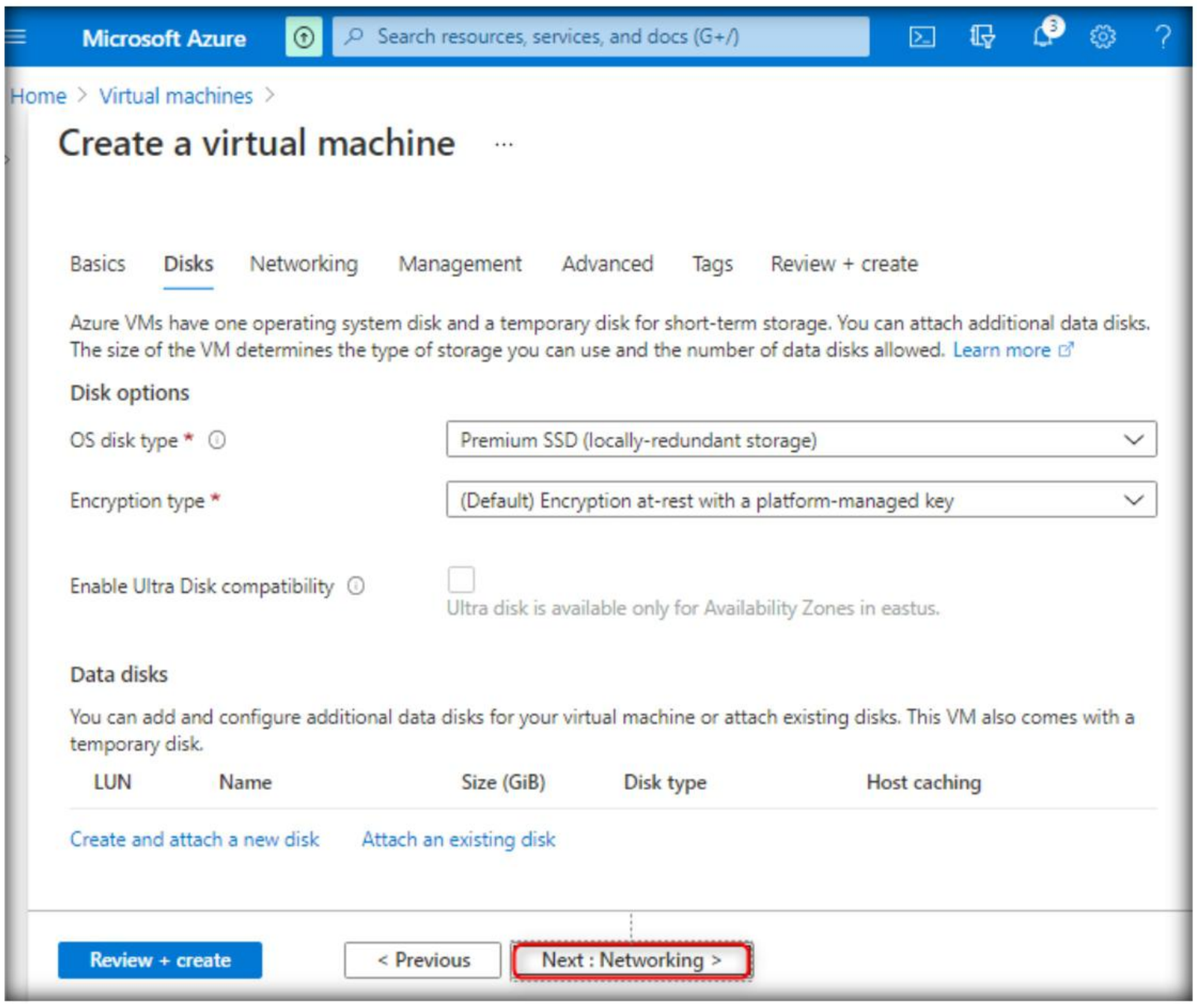


FIGURE 4.10.90: Leaving Disk Tab in Default State

91. In the **Networking** tab, select **Subnet** as **Private,** and in **NIC network security group,** select the **Basic** radio button.

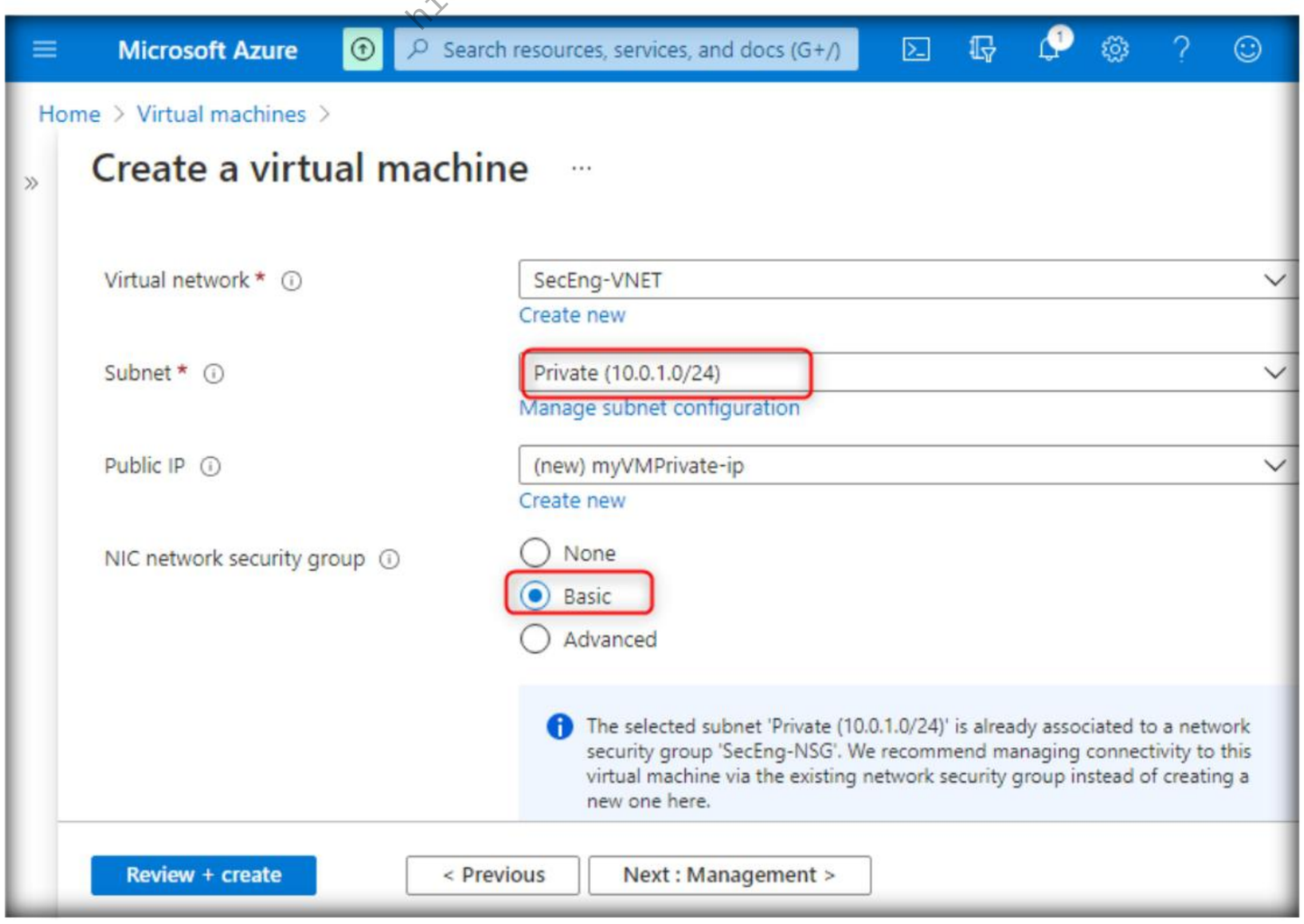


FIGURE 4.10.91: Selecting Subnet and NIC network Security Group

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

92. In **Public inbound ports**, select the **Allow selected ports** radio button. In the **Select inbound ports** field, select **RDP (3389)**. Then, click on **Next: Management >**.

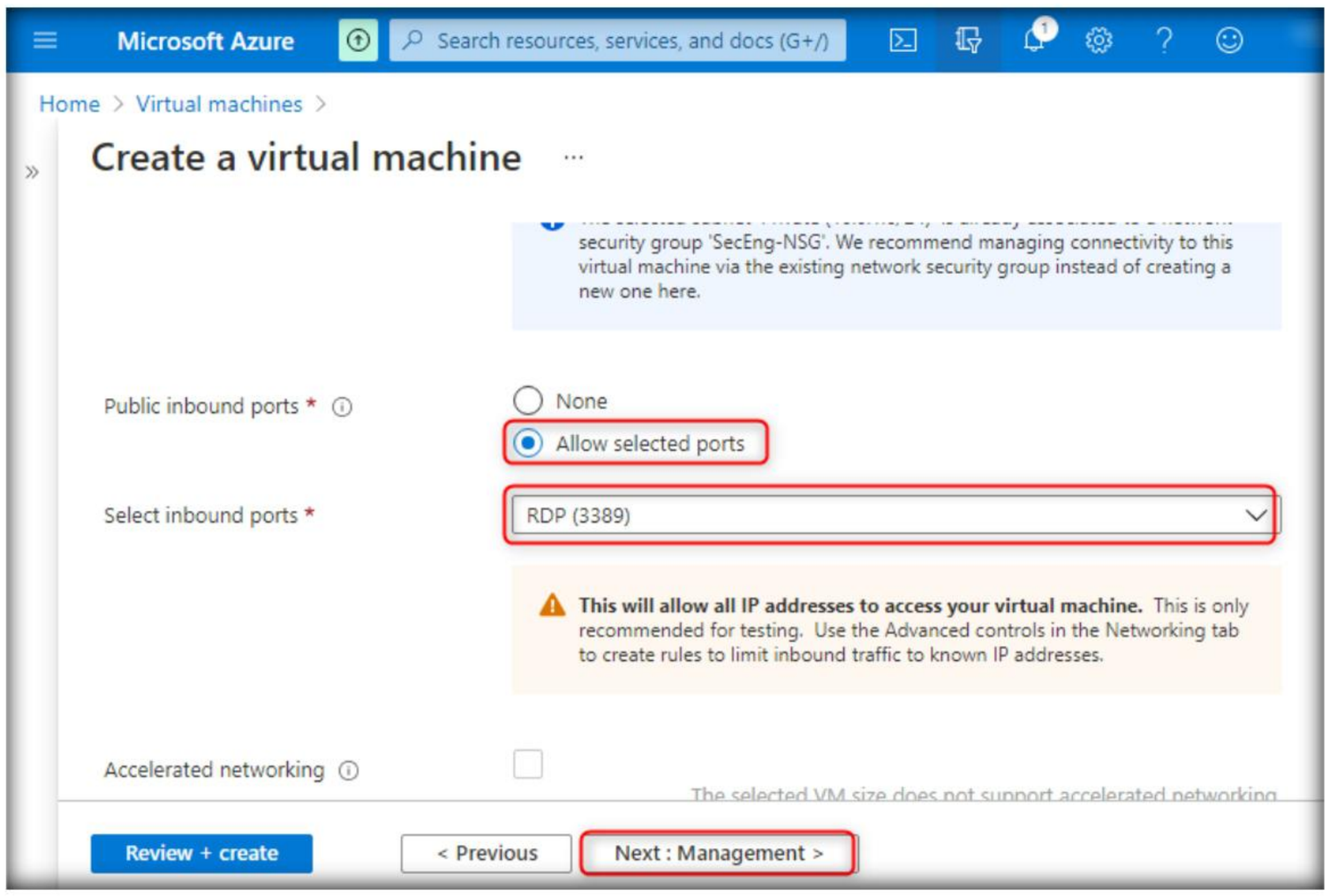


FIGURE 4.10.92: Selecting Inbound Ports

93. In the **Management** tab, select the **Disable** radio button under **Boot diagnostics**. Then, click on **Next: Advanced >**.

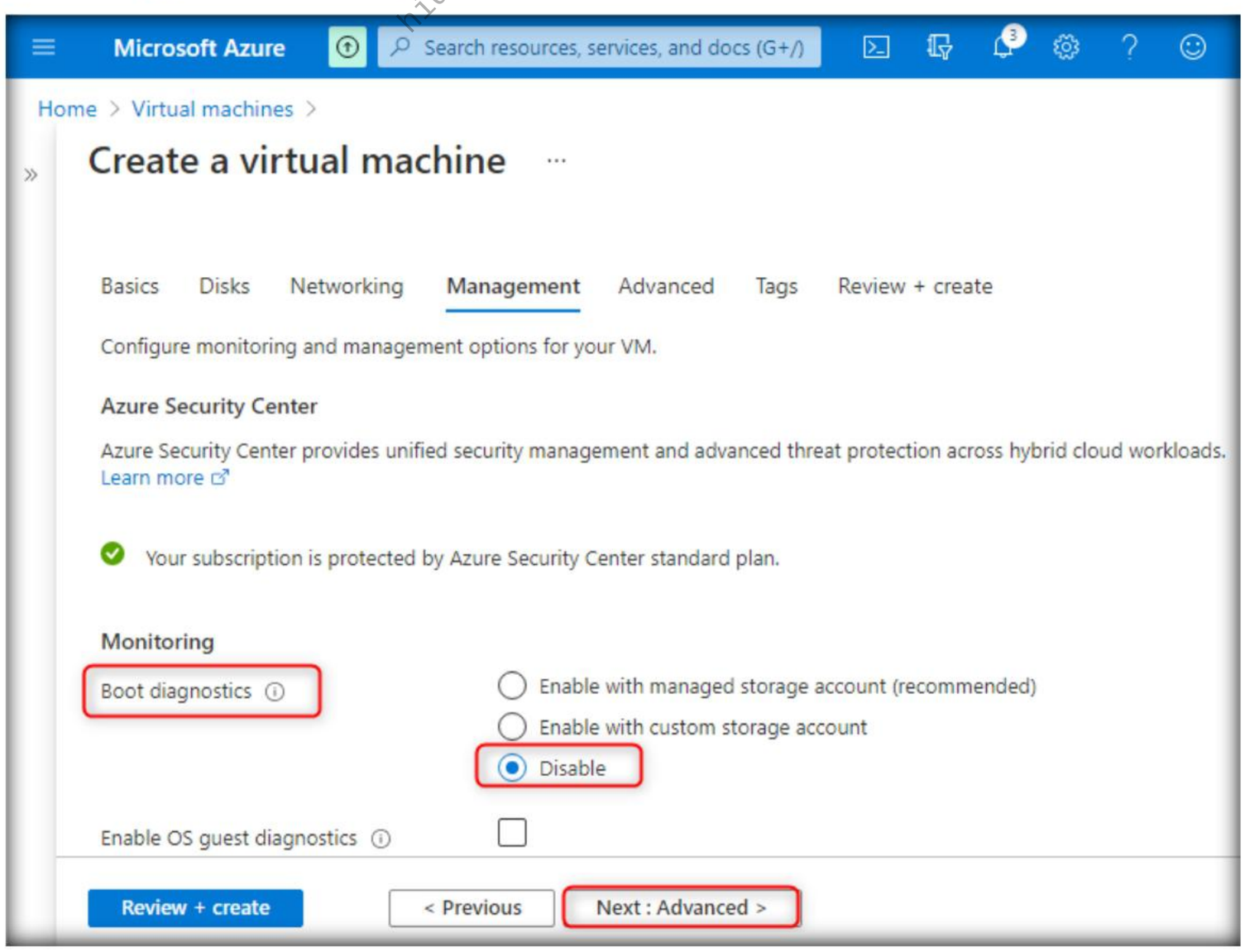


FIGURE 4.10.93: Selecting Disable Radio Button for Boot Diagnostics

Certified Cloud Security Engineer Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

94. In the **Advanced** tab, leave everything in their default state and click on the **Next: Tags** button.

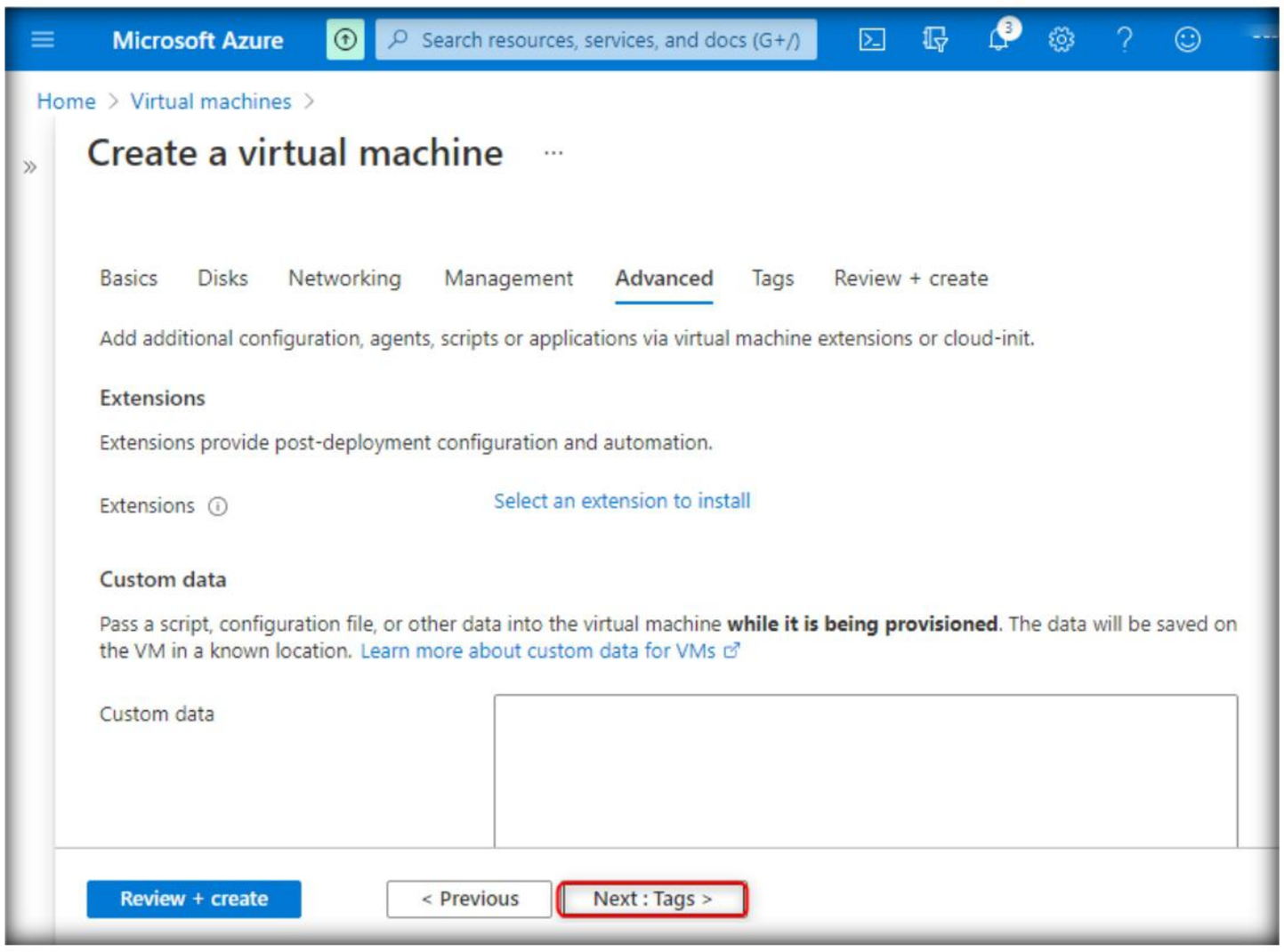


FIGURE 4.10.94: Leaving Advanced Tab in Default State

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

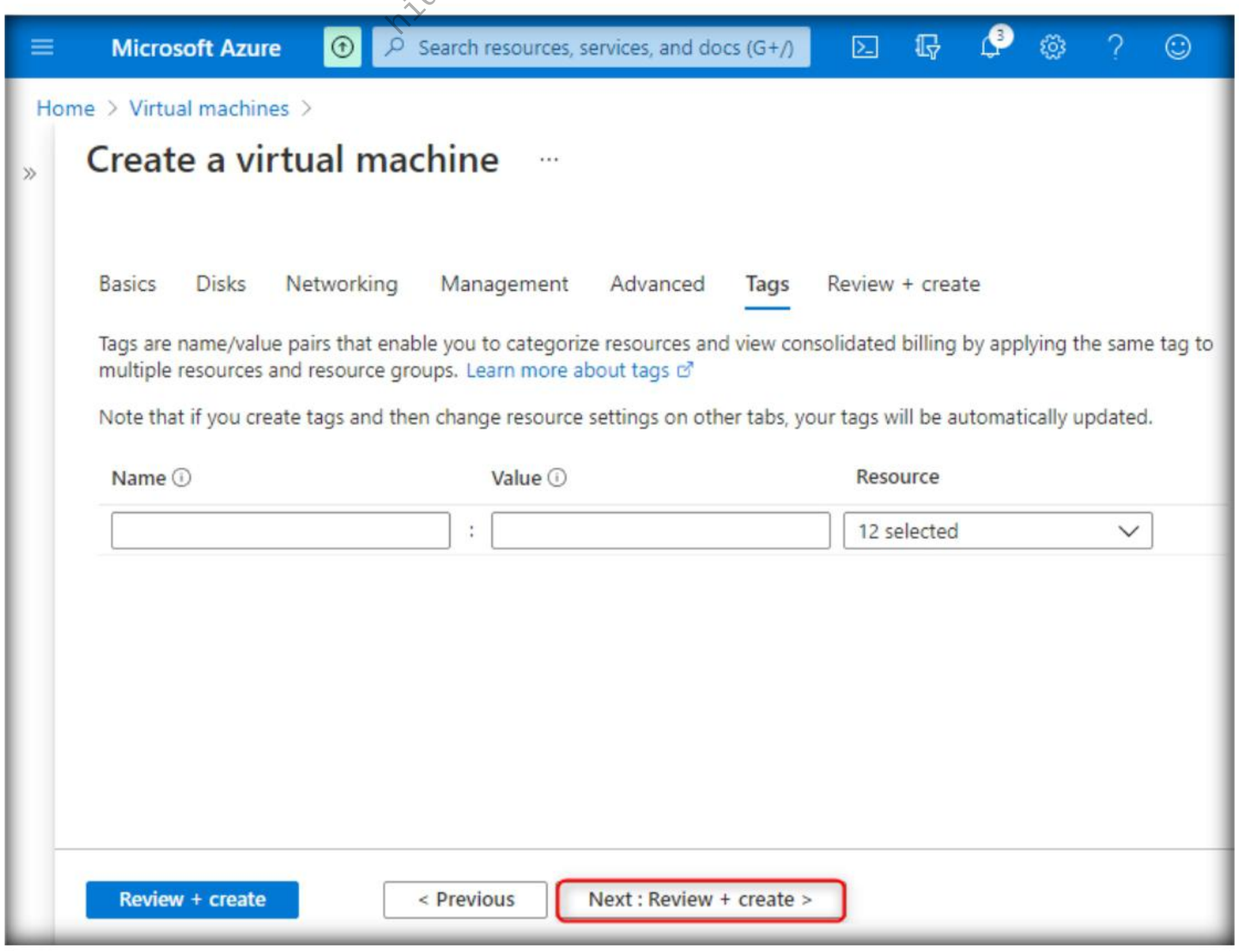


FIGURE 4.10.95: Leaving Tags Tab in Default State

Certified Cloud Security Engineer Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

96. After seeing the **Validation passed** message, click on the **Create** button.

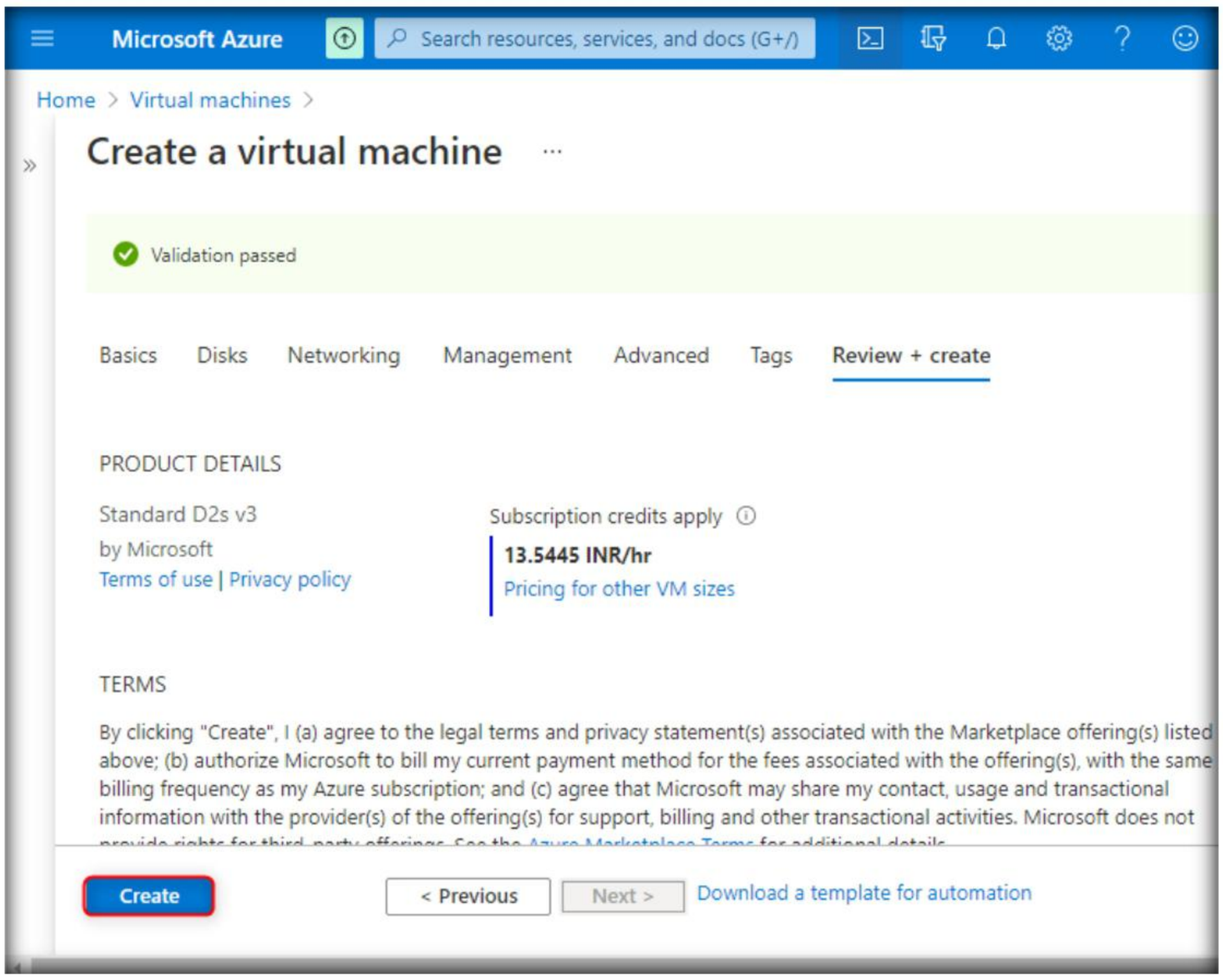


FIGURE 4.10.96: Creating a VM after Validation Passed

97. After the successful deployment of the virtual machine, click on the **Go to resource** button.

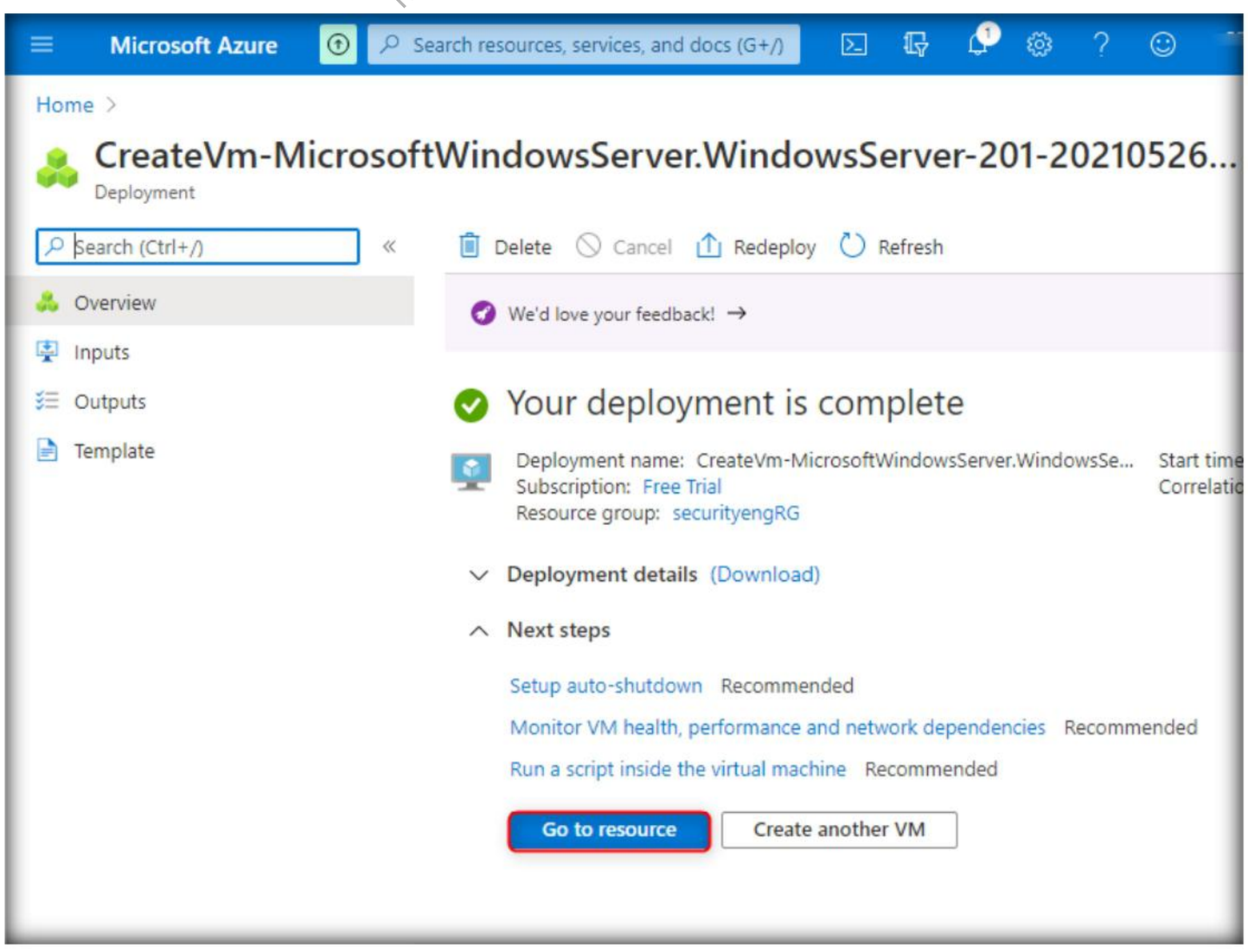


FIGURE 4.10.97: Successful Deployment of VM

Certified Cloud Security Engineer Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

98. **myVMPrivate** virtual machine has been successfully created.

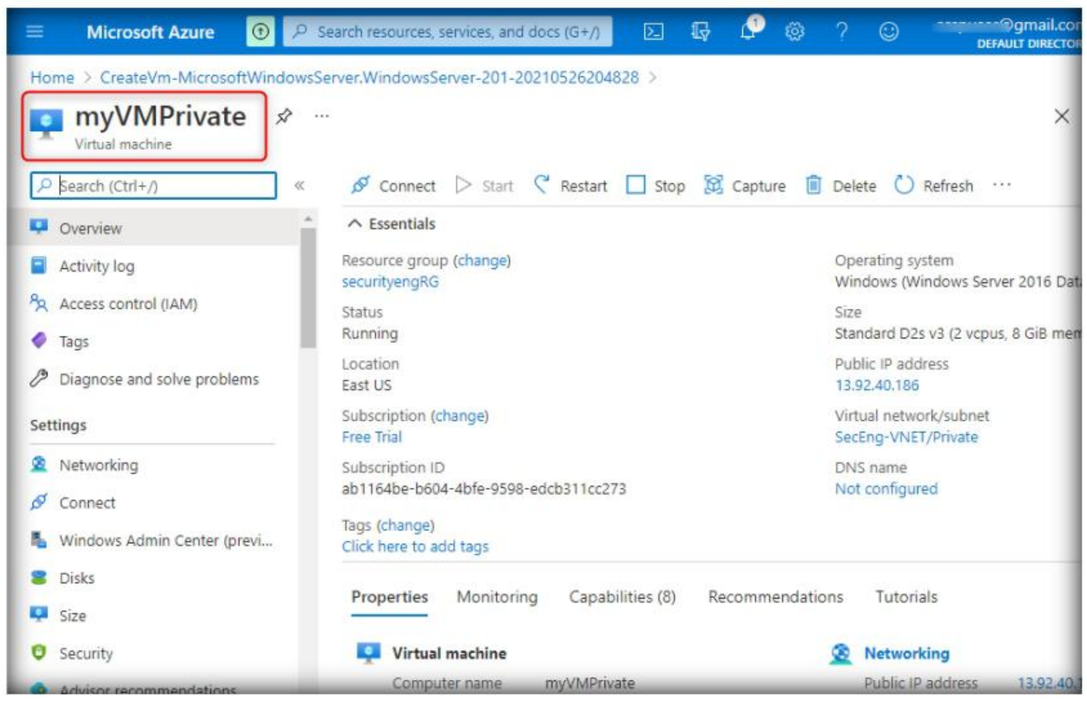


FIGURE 4.10.98: Successful Creation of myVMPublic Virtual Machine

TASK 9

Confirming access to storage account

99. Next, you will confirm access to the storage account. In **myVMPrivate** virtual machine, navigate and click on **Connect**, and then on **RDP**. Under **Connect with RDP**, click on **Download RDP File**.

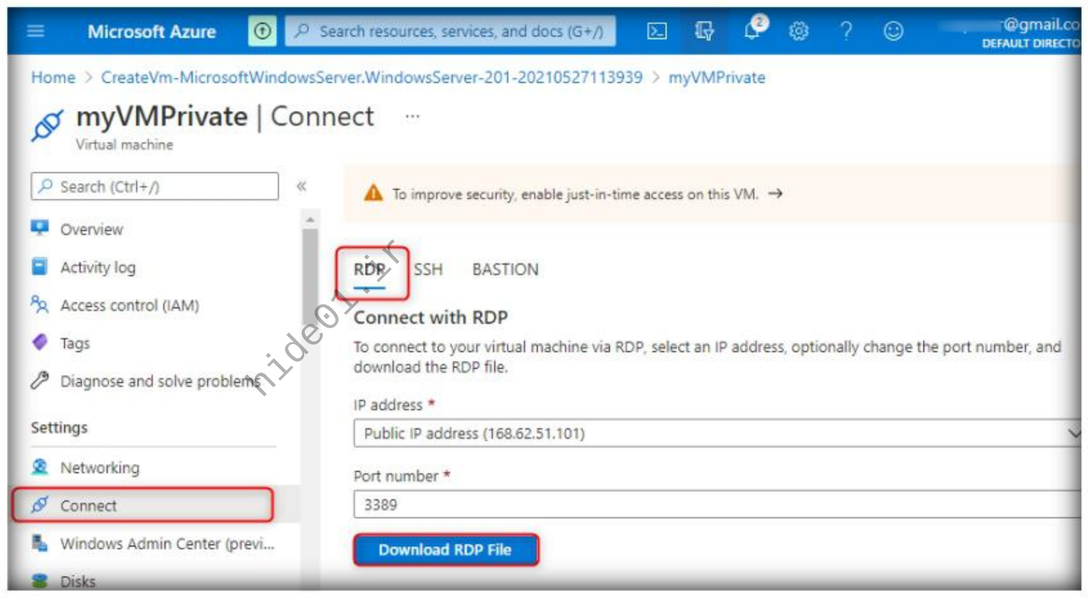


FIGURE 4.10.99: Connecting VM with RDP

100. We will be connecting to **myVMPrivate** virtual machine using remote desktop connection (RDP). Click on the RDP file after it is successfully downloaded.

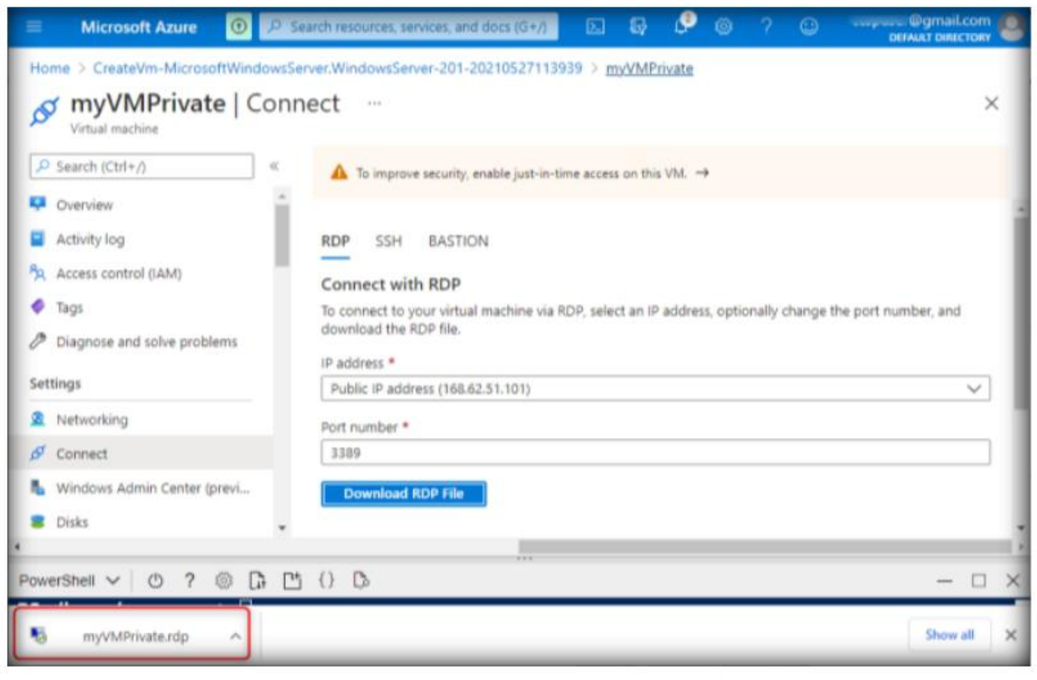


FIGURE 4.10.100: myVMPrivate RDP File is Downloaded

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

101. In the **Remote Desktop Connection** window, click on the **Connect** button.

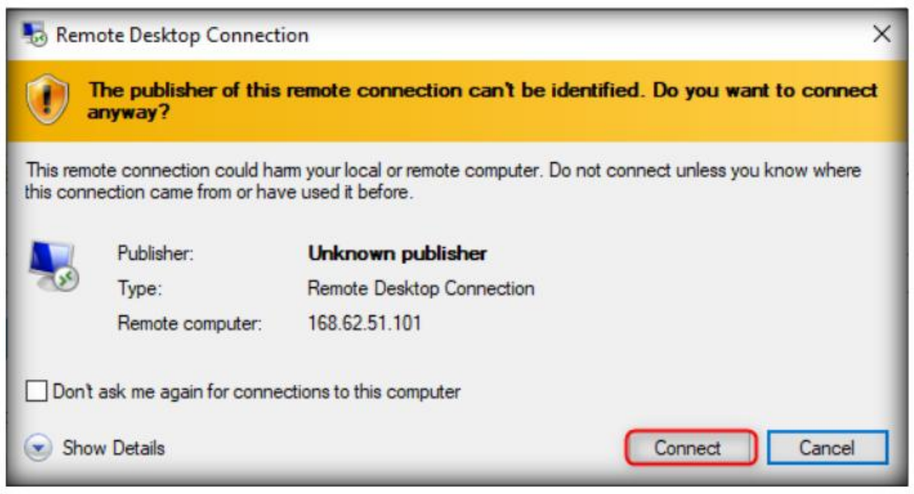


FIGURE 4.10.101: Connecting to myVMPrivate Virtual Machine

102. A **Windows Security Enter your credentials** window will open. Enter **myVMPrivate** virtual machine **Username** (here, **CCSEtester2)** and **Password** (**Administrator@456**). Then, click on the **OK** button.

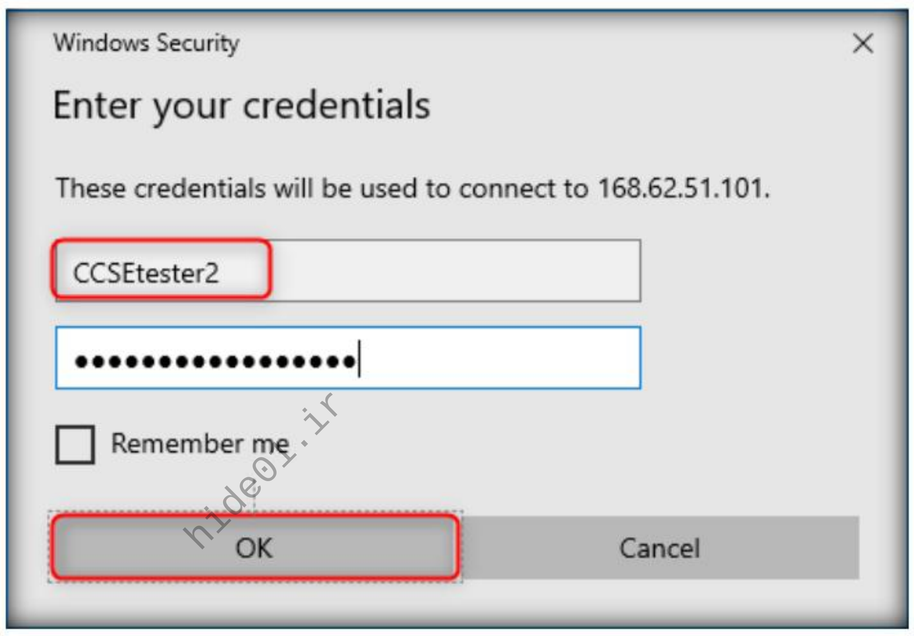


FIGURE 4.10.102: Entering VM Login Credentials

103. The **Remote Desktop Connection** certificate will appear, indicating **Certificate errors.** Click on the **Yes** button.

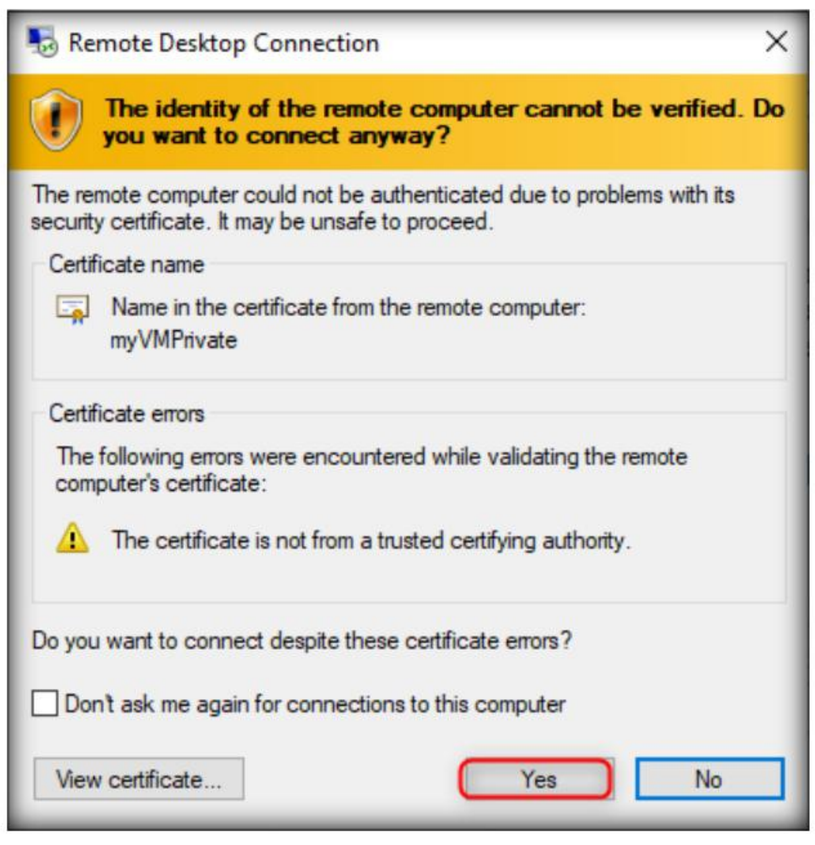


FIGURE 4.10.103: Certification Error

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

104. **myVMPrivate** virtual machine will be successfully connected now. In the **Networks** window, click on the **Yes** button.

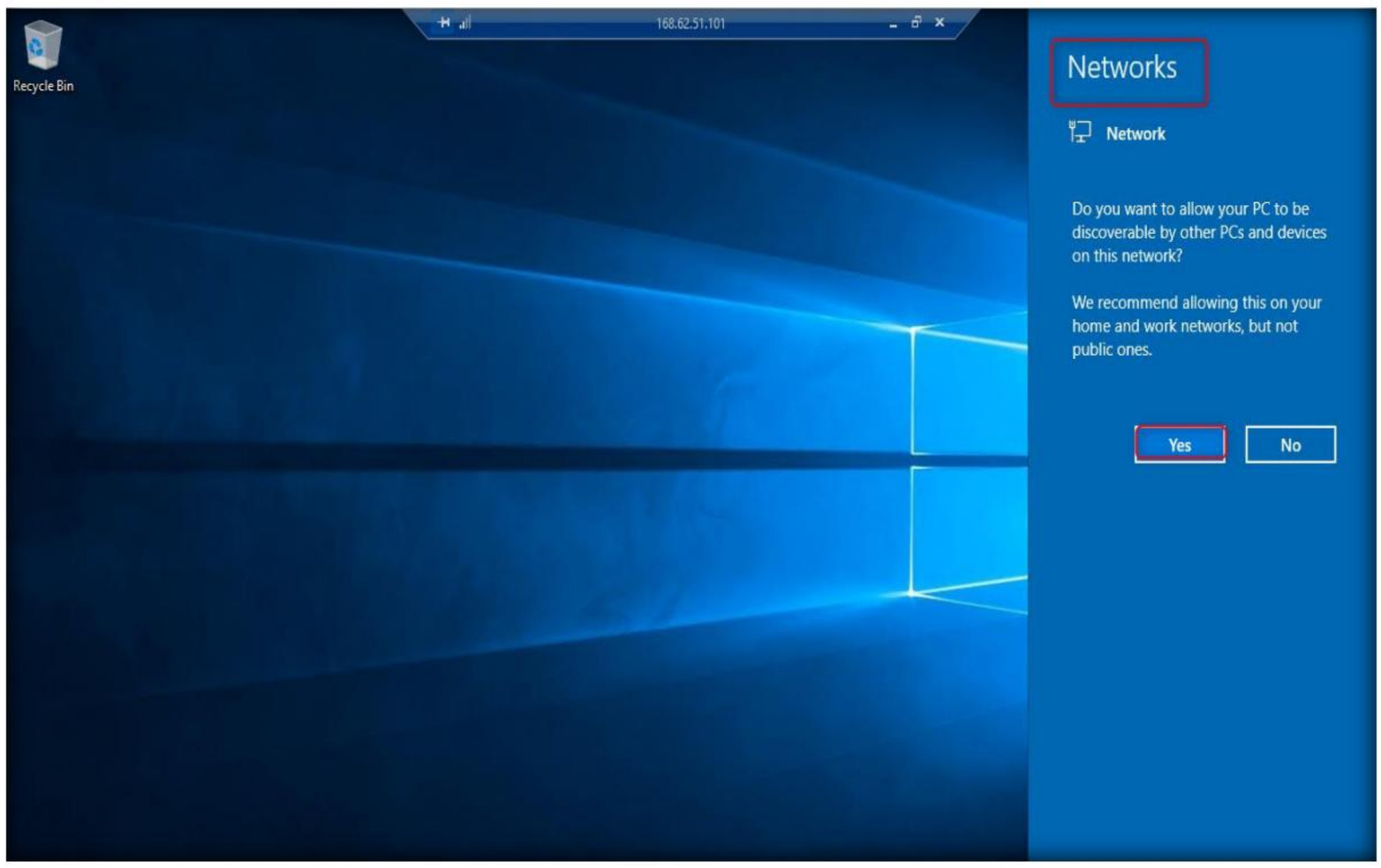


FIGURE 4.10.104: Selecting Yes in Networks Window

105. In the **myVMPrivate** VM search box, type **power shell**. **Windows PowerShell** will appear as the best match. Click on it.

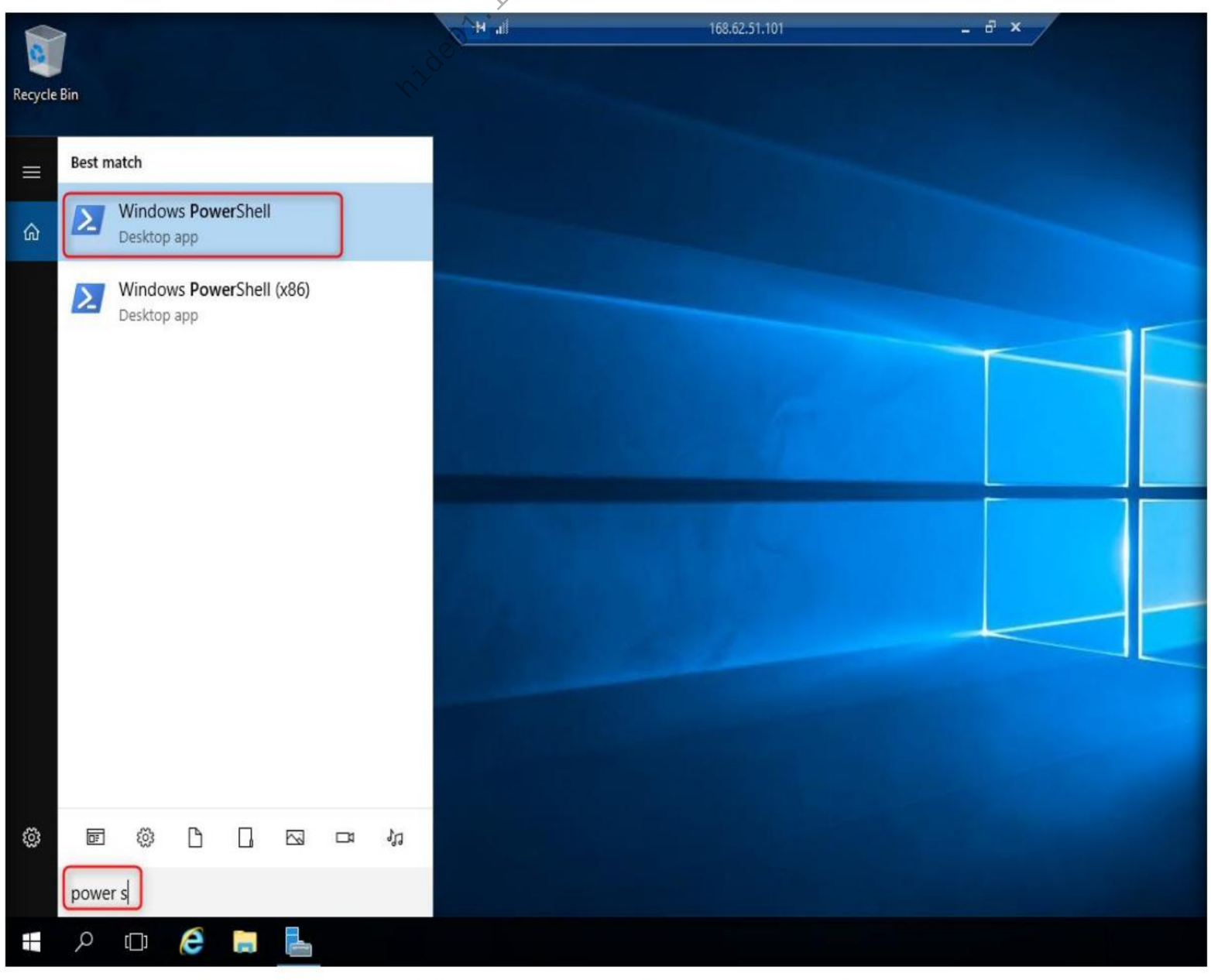


FIGURE 4.10.105: Selecting Windows PowerShell

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

106. In **myVMPrivate** VM, use **PowerShell** to map the Azure file share utilizing drive Z using the following commands sequentially:

```
$acctKey = ConvertTo-SecureString -String
"<storage-account-key>" -AsPlainText -Force

$credential = New-Object
System.Management.Automation.PSCredential -
ArgumentList "Azure\<storage-account-name>",
$acctKey

New-PSDrive -Name Z -PSProvider FileSystem -
Root "\\<storage-account-
name>.file.core.windows.net\my-file-share" -
Credential $credential
```

Note: Before running the above command, replace the <storage-account-key> and <storage-account-name> with those you saved in the notepad at the time of creating a storage account.

Note: You will have a different key. Ensure you input the correct key in the command line.

Note: Type the command, minimize the remote desktop connection, copy the key from the notepad, go to the command line and delete **storage-account-key along with > and < symbols**, paste the key between inverted commas.

hide01.ir

```
$acctKey = ConvertTo-SecureString -String
"TI7C3u99sRM4L5P3l+sGrpDtmMPORT8N8YqRHrHP3U6MB3
tzseVruXposm5CrCebwBnWpSLLNFJ3x0yMx5EDww==" -
AsPlainText -Force

$credential = New-Object
System.Management.Automation.PSCredential -
ArgumentList "Azure\mystorage25", $acctKey

New-PSDrive -Name Z -PSProvider FileSystem -Root
"\\mystorage25.file.core.windows.net\my-file-
share" -Credential $credential
```

Azure file share has been successfully mapped to Z drive.

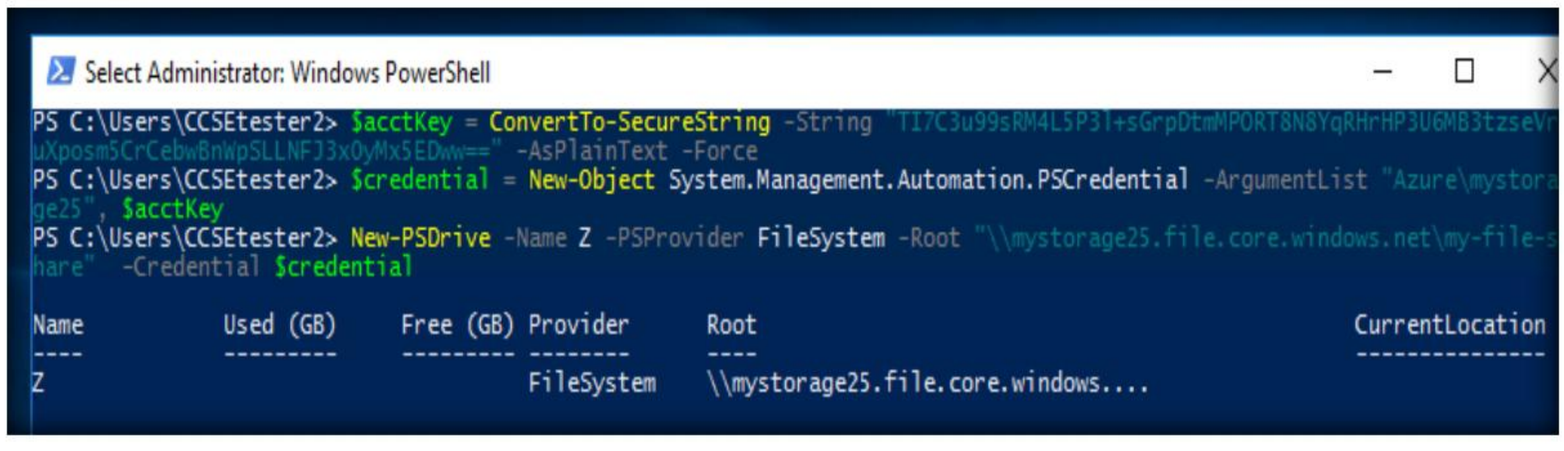


FIGURE 4.10.106: Command to Map the Azure file share utilizing drive Z

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

107. Use the following command to confirm that **myVMPrivate** VM does not have an outbound connectivity with the Internet.

```
ping bing.com
```

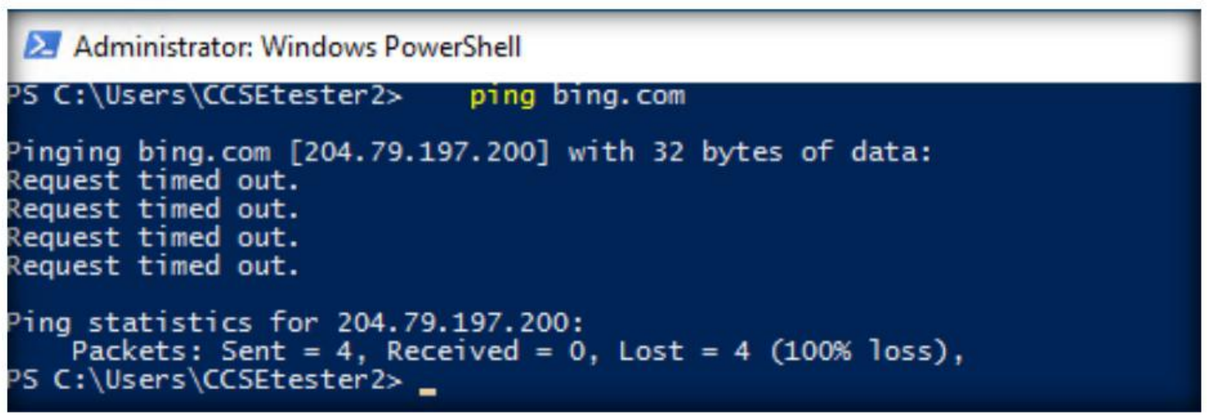


FIGURE 4.10.107: Command to Check the VM Outbound Connectivity with Internet

You will not receive any reply as the NSG associated with **Private** subnet will not allow an outbound access to the Internet.

108. Now, close **Windows PowerShell**. Right click on **Windows** icon, click on **Shut down or sign out**, and then click on **Disconnect** to close **myVMPrivate** VM.

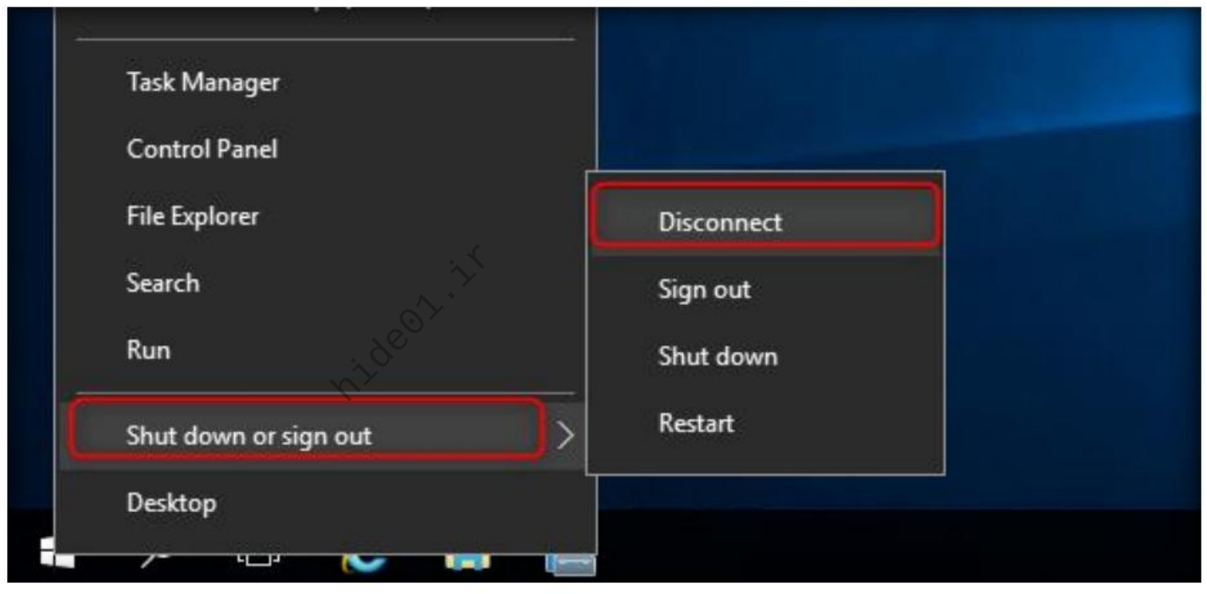


FIGURE 4.10.108: Disconnecting VM

109. If you are in the **myVMPrivate** window, click on **Home** to go back to the Azure portal.

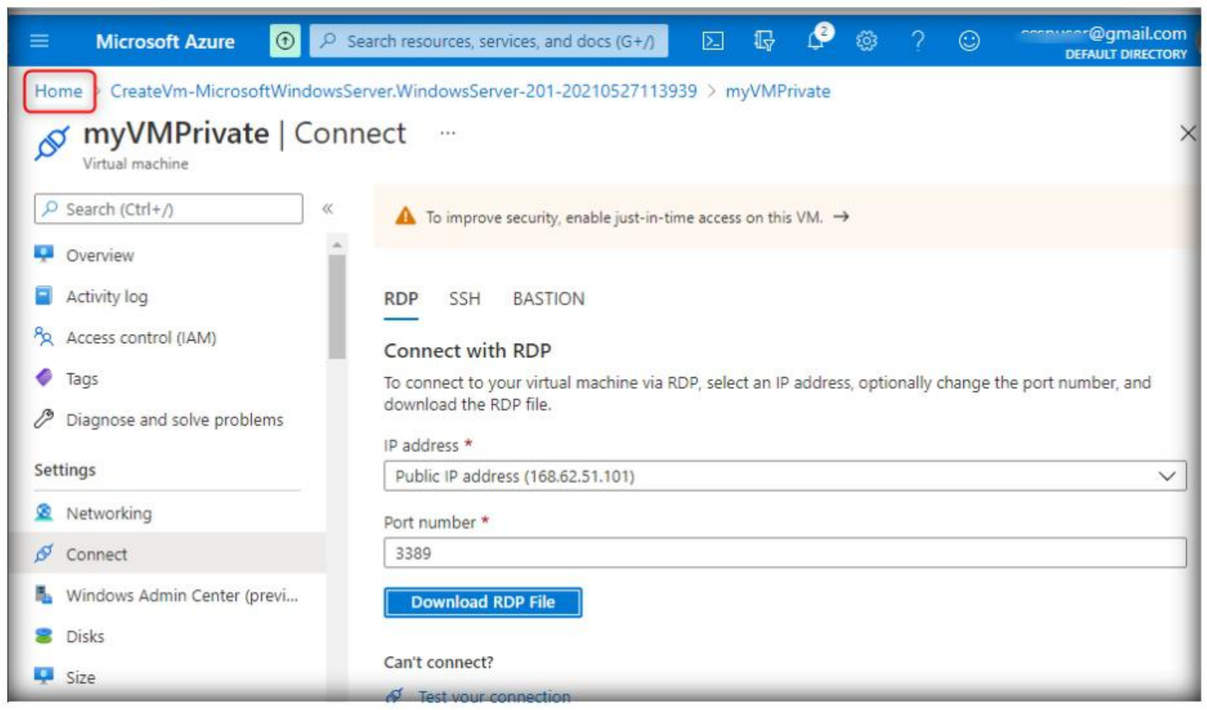


FIGURE 4.10.109: Selecting Home to Go Back to Azure Portal

TASK 10

110. From Azure portal, click on **Resource groups**.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Confirming Access is Denied to Storage Account

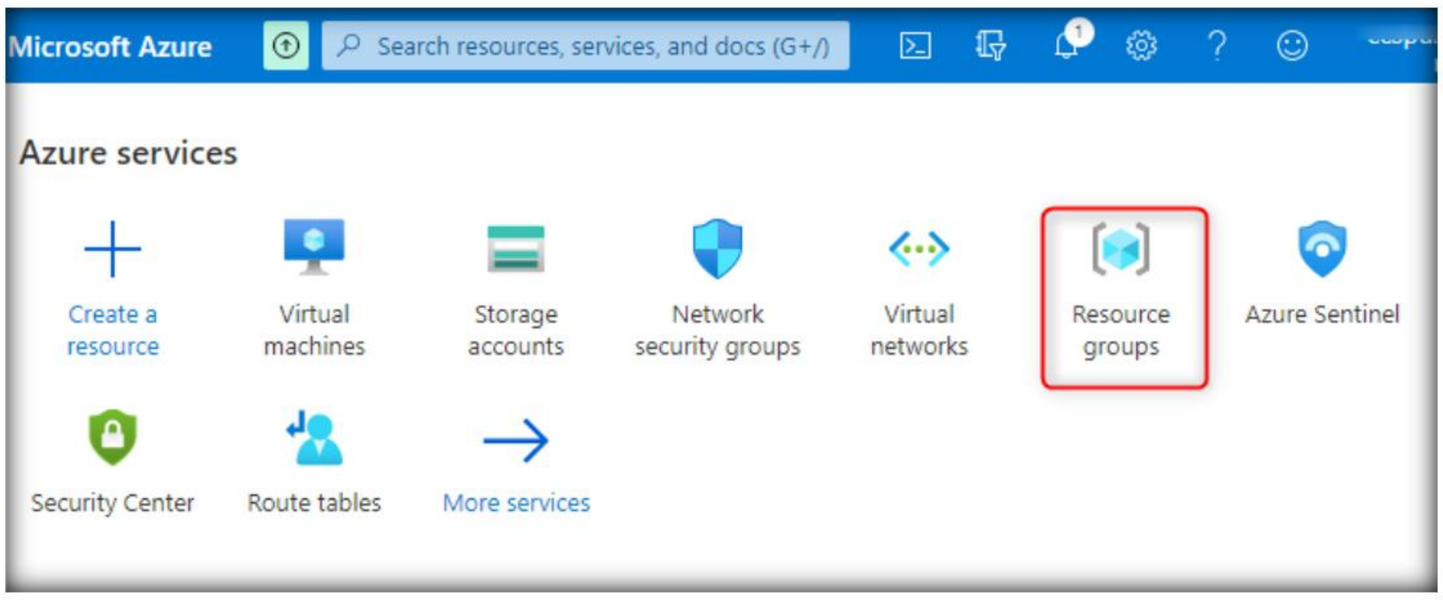


FIGURE 4.10.110: Selecting Resource Groups

111. In **Resource groups**, click on **securityengRG**.

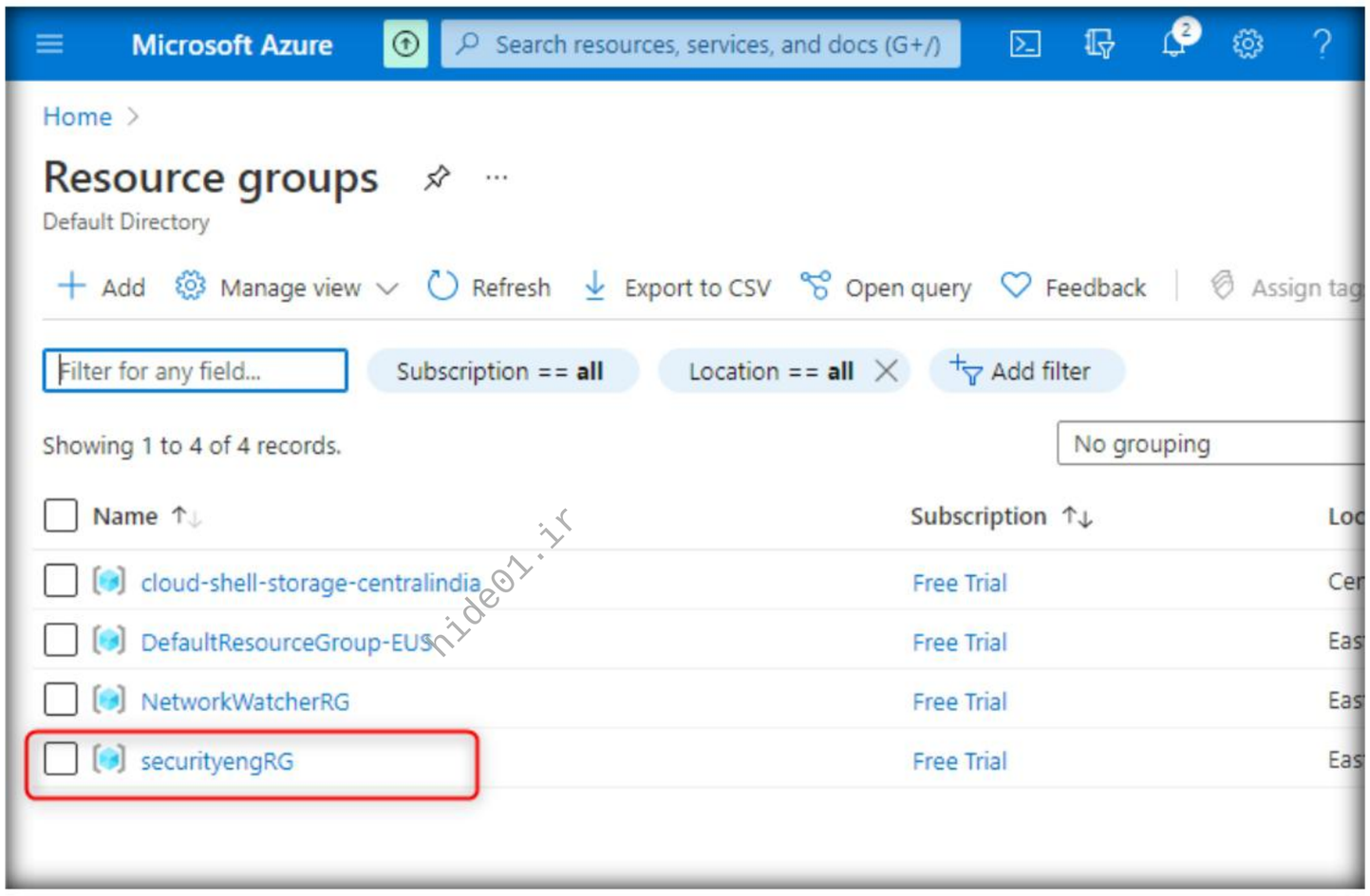


FIGURE 4.10.111: Selecting securityengRG Resource Group

112. In **securityengRG**, click on **myVMPublic** virtual machine.

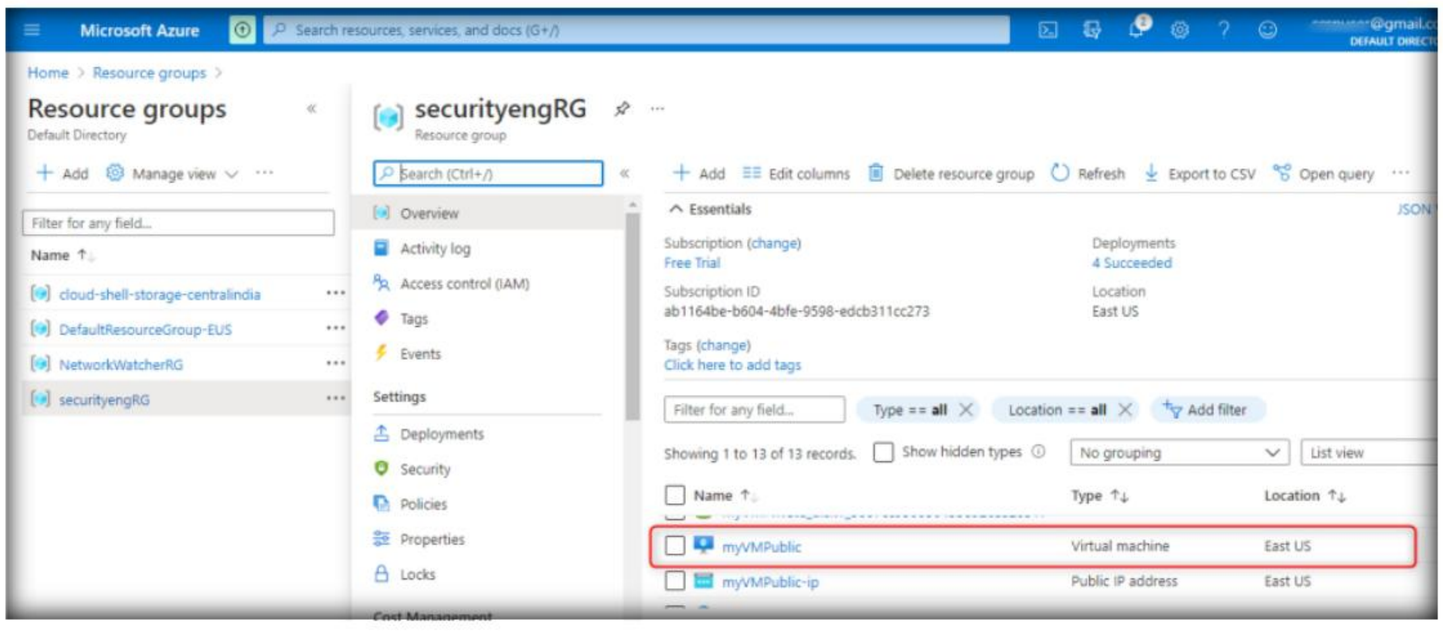


FIGURE 4.10.112: Selecting myVMPublic Virtual Machine

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

113. **myVMPublic** virtual machine will open now. Click on **Connect** and then on **RDP**.

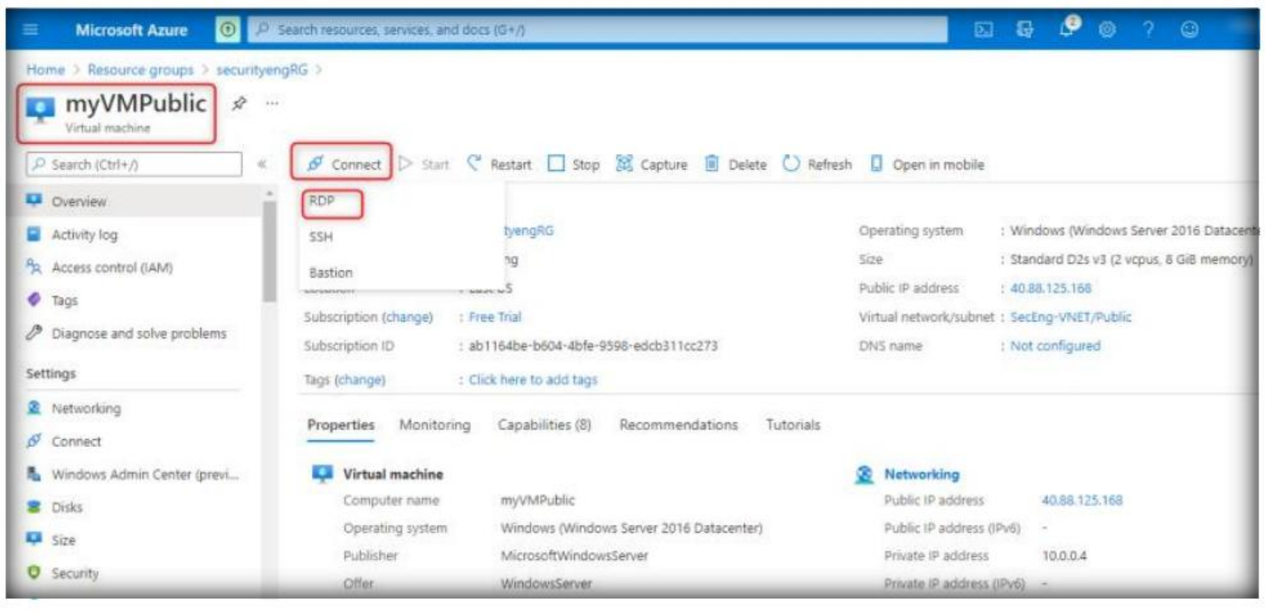


FIGURE 4.10.113: Connecting myVMPublic with RDP

114. Under **Connect with RDP**, click on **Download RDP File**.

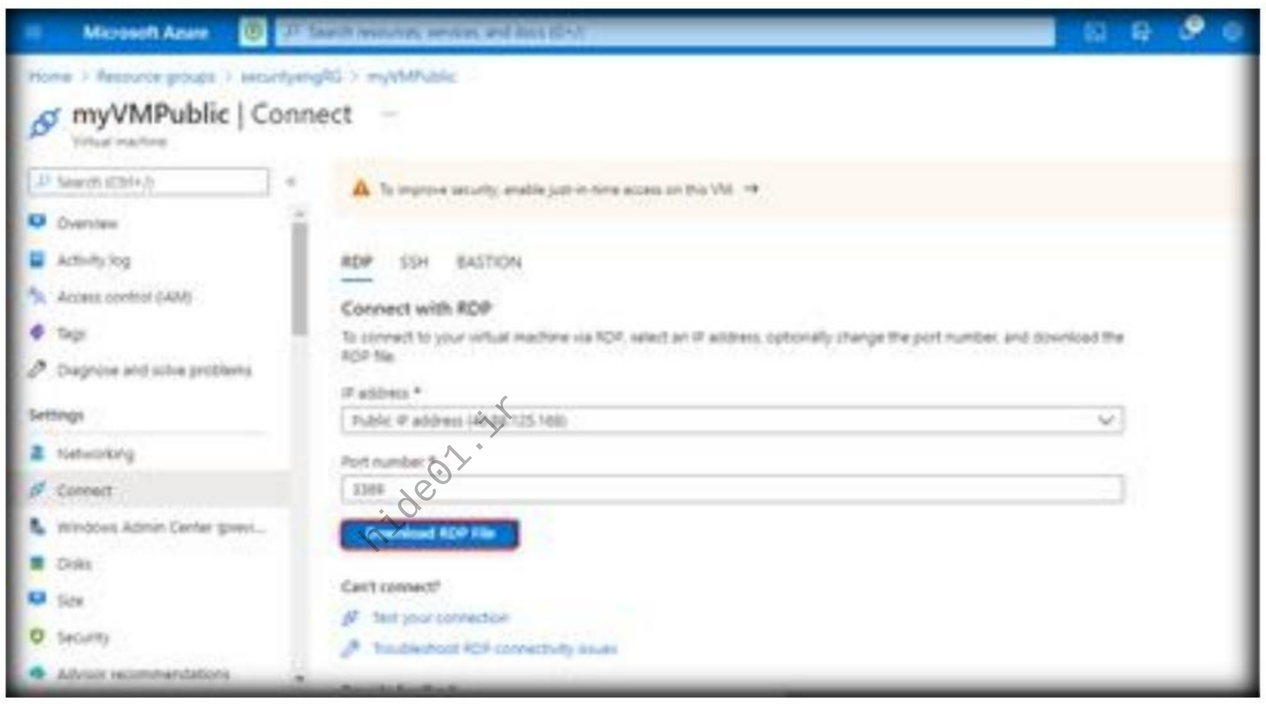


FIGURE 4.10.114: Downloading RDP File

115. Click on the **myVMPublic** RDP file after it is successfully downloaded.

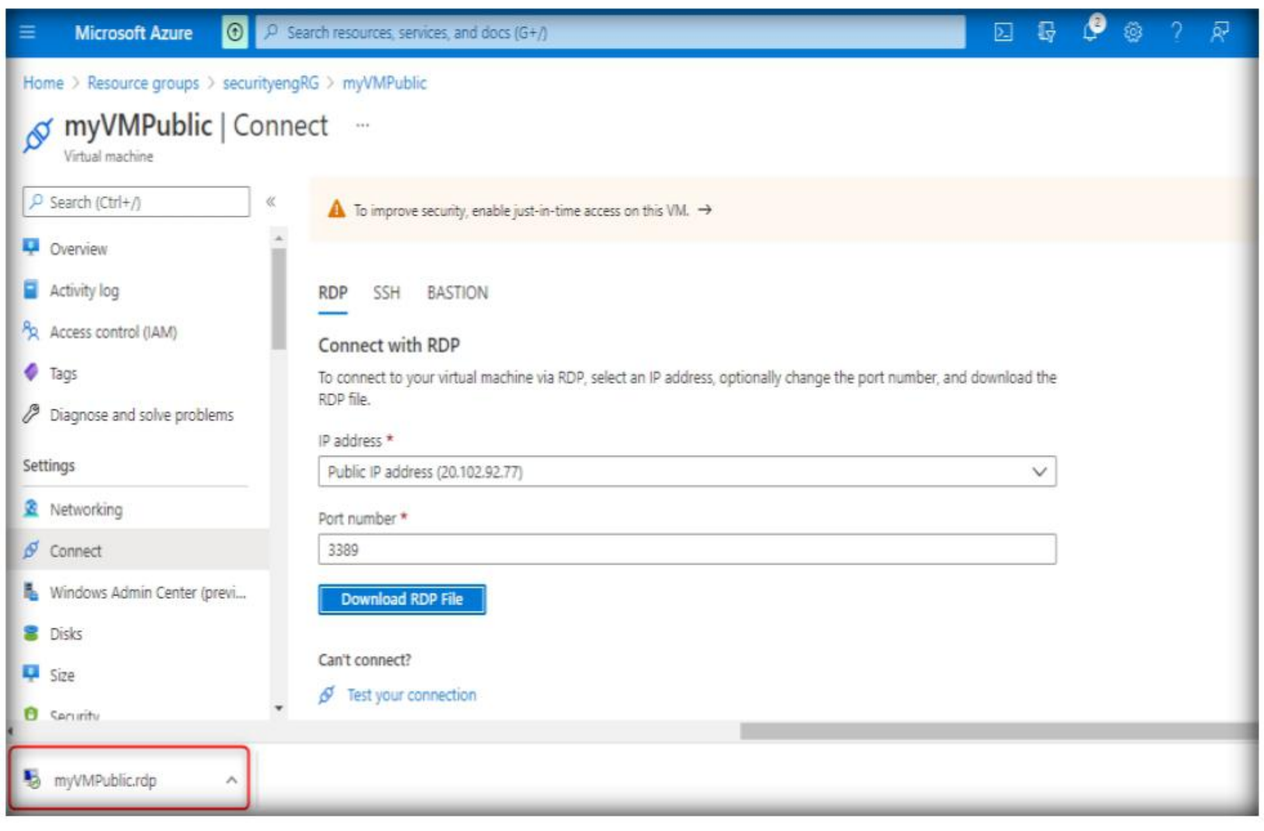


FIGURE 4.10.115: Opening myVMPublic RDP File

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

116. In the **Remote Desktop Connection** window, click on the **Connect** button.

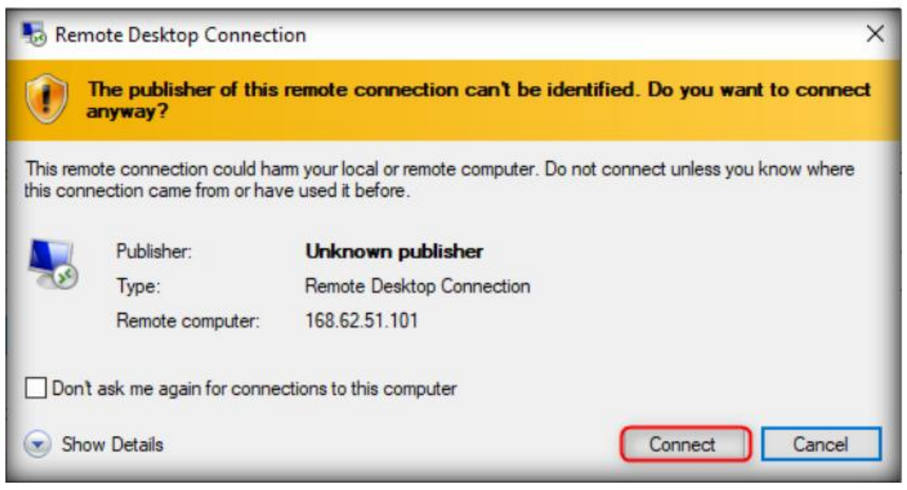


FIGURE 4.10.116: Connecting myVMPublic Virtual Machine

117. A **Windows Security Enter your credentials window** will open. Enter **myVMPublic** virtual machine **Username** (here, **CCSEtester1)** and **Password** (**Administrator@321**). Then, click **OK**.

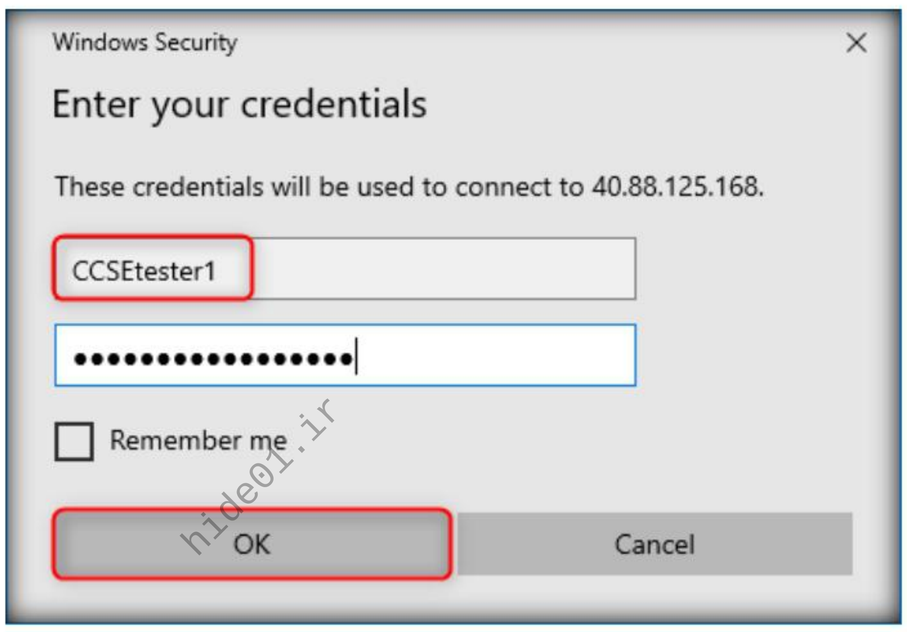


FIGURE 4.10.117: Entering Login Credentials of myVMPublic

118. A **Remote Desktop Connection** certificate will appear, indicating **Certificate errors**. Click on the **Yes** button.

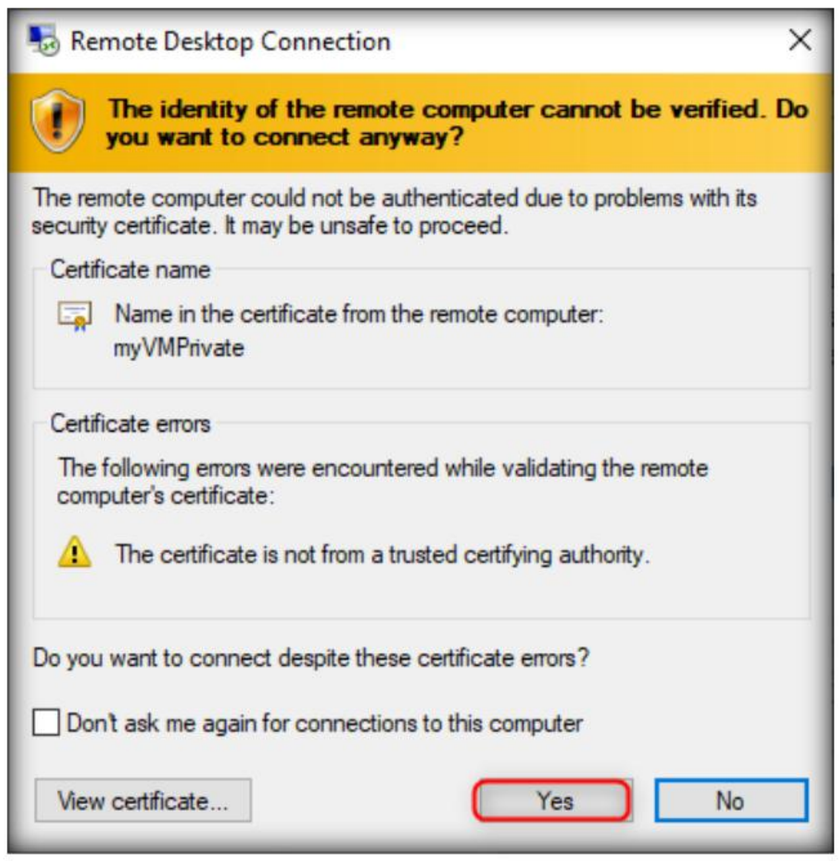


FIGURE 4.10.118: Certificate Errors

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

119. **myVMPublic** virtual machine will be successfully connected now. In the **Networks** window, click on the **Yes** button.

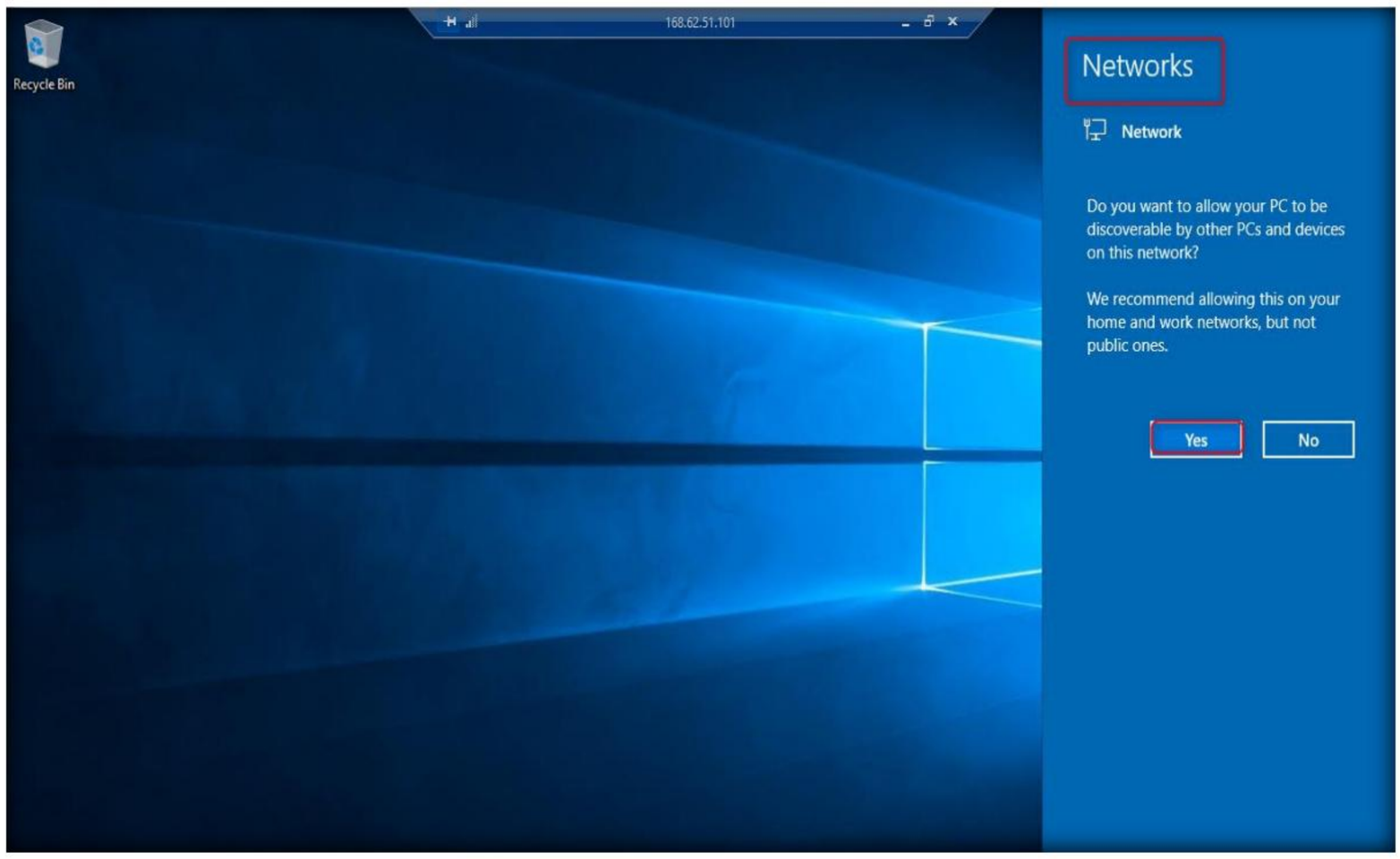


FIGURE 4.10.119: Selecting Yes in Networks Window

120. In the **myVMPrivate** VM search box, type **power shell**. **Windows PowerShell** will appear as the best match. Now, click on **Windows PowerShell**.

hide01.ir

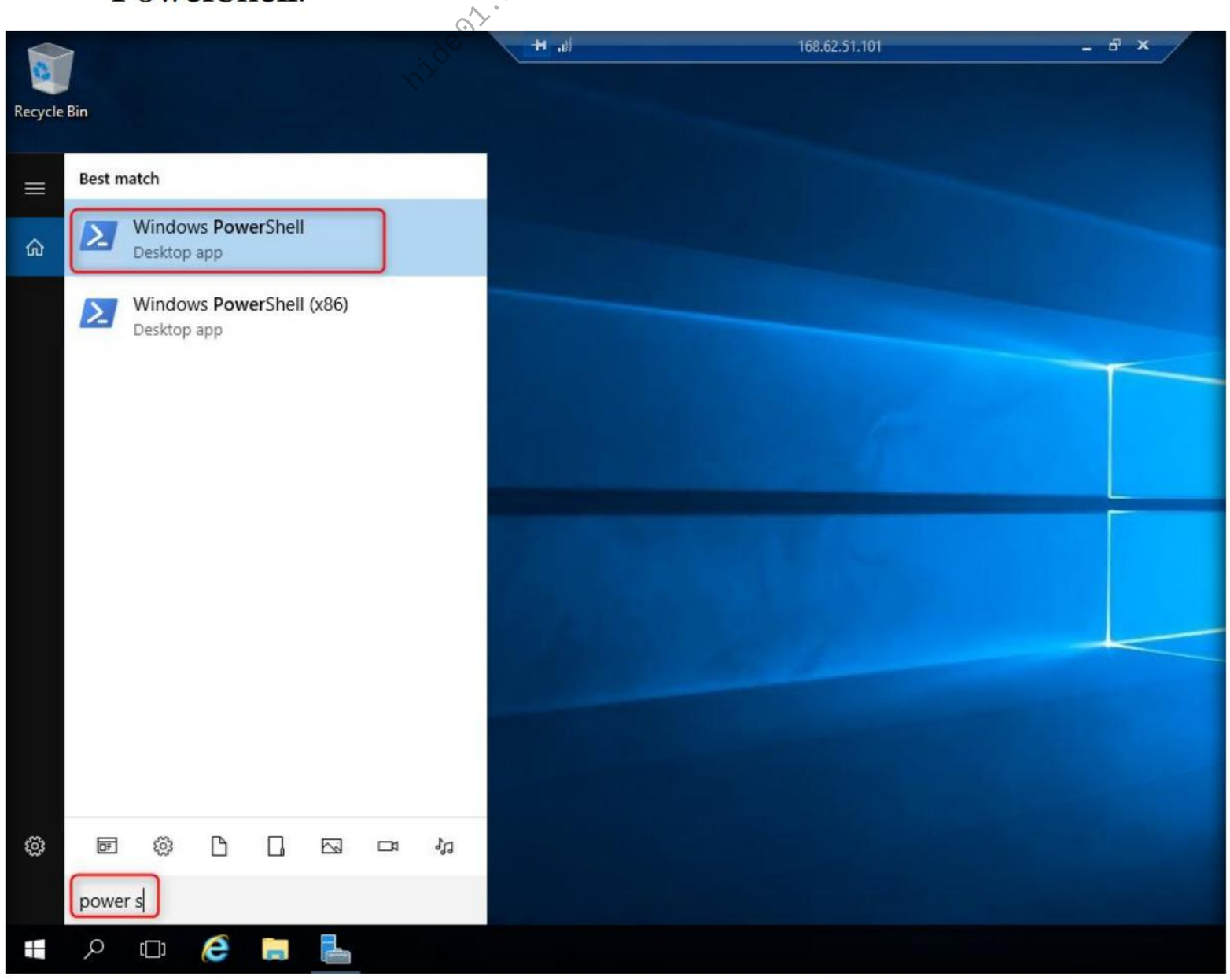


FIGURE 4.10.120: Opening Windows PowerShell

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

121. In **myVMPublic** VM, use PowerShell to map the Azure file share utilizing drive Z using the following commands:

```
$acctKey = ConvertTo-SecureString -String
"<storage-account-key>" -AsPlainText -Force

$credential = New-Object
System.Management.Automation.PSCredential -
ArgumentList "Azure\<storage-account-name>",
$acctKey

New-PSDrive -Name Z -PSProvider FileSystem -
Root "\\<storage-account-
name>.file.core.windows.net\my-file-share" -
Credential $credential
```

Note: Before running the above command, replace the `<storage-account-key>` and `<storage-account-name>` with those you saved in the notepad at the time of creating a storage account.

Note: You would have a different key. Ensure you input the correct key in the command line.

```
$acctKey = ConvertTo-SecureString -String
"TI7C3u99sRM4L5P3l+sGrpDtmMPORT8N8YqRHrHP3U6MB3
tzseVruXposm5CrCebwBnWpSLLNFJ3x0yMx5EDww==" -
AsPlainText -Force

$credential = New-Object
System.Management.Automation.PSCredential -
ArgumentList "Azure\mystorage25", $acctKey

New-PSDrive -Name Z -PSProvider FileSystem -Root
"\\mystorage25.file.core.windows.net\my-file-
share" -Credential $credential
```

hide01.ir

You will receive a `New-PSDrive: Access is denied` error.

The access is denied because we have deployed **myVMPublic** virtual machine in the public subnet,. The public subnet does not have any service endpoints enabled for Azure storage. The Azure storage account allows network access only from the private subnet.

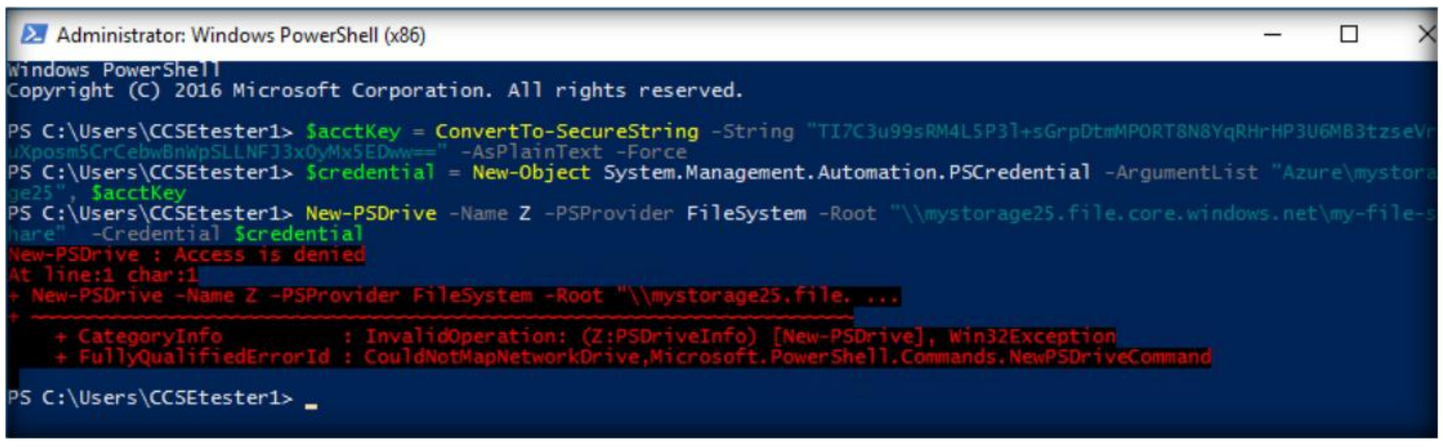


FIGURE 4.10.121: Access is Denied Error

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

122. Close **Windows PowerShell**. Right click on the **Windows** icon, click on **Shut down or sign out**, and then click on **Disconnect** to close **myVMPublic** VM.

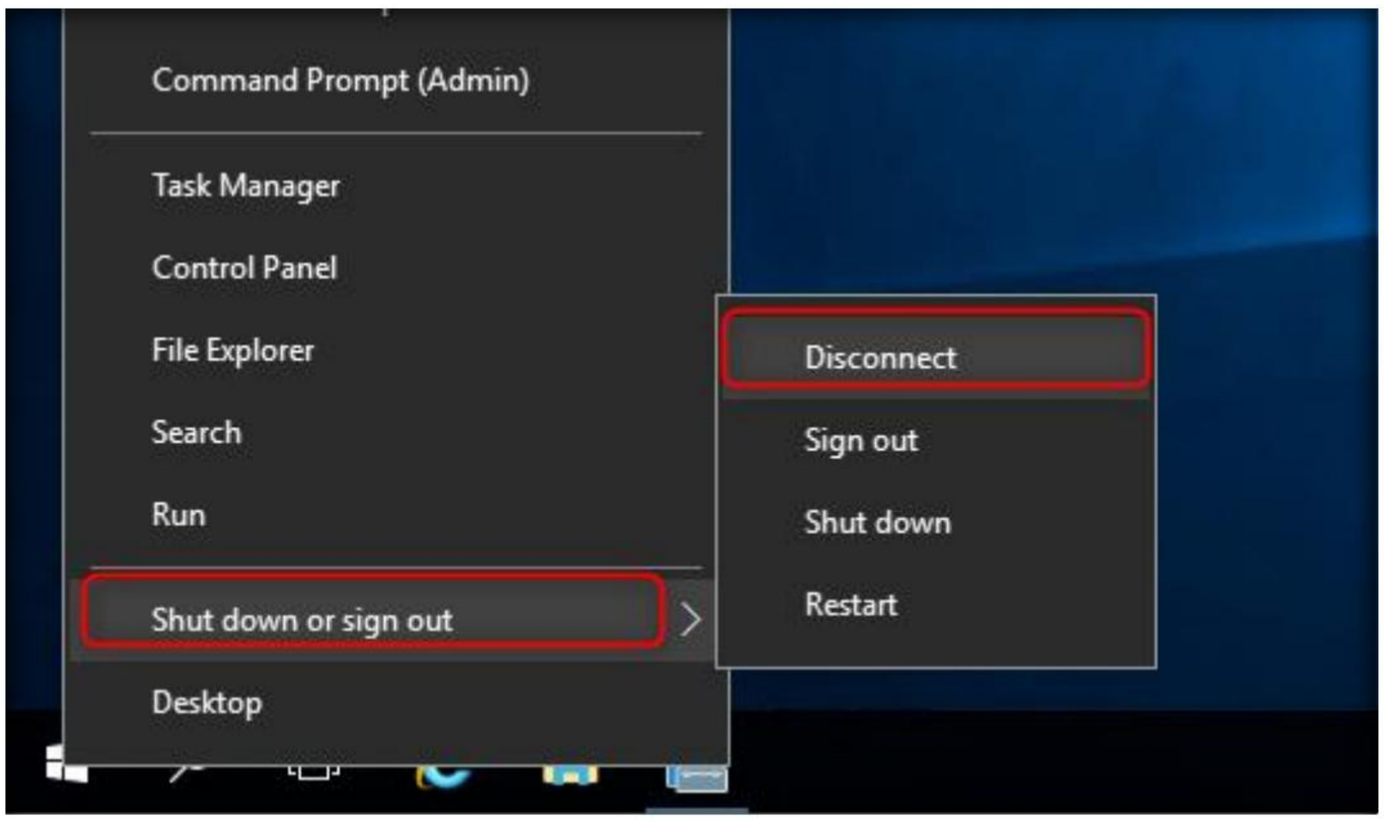


FIGURE 4.10.122: Disconnecting Virtual Machine

123. If you are in **myVMPublic** virtual machine, click on **Home** to go back to Azure portal.

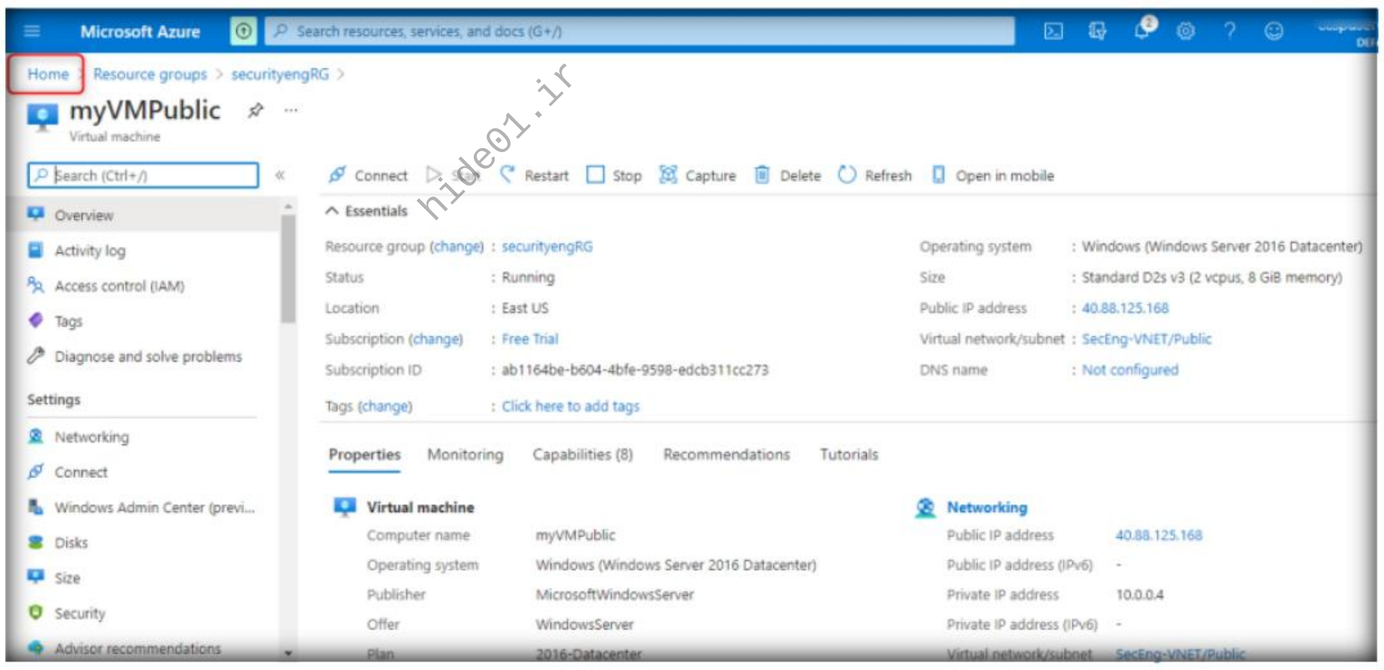


FIGURE 4.10.123: Selecting Home to Go Back to Azure Portal

124. From Azure portal, click on **Resource groups**.

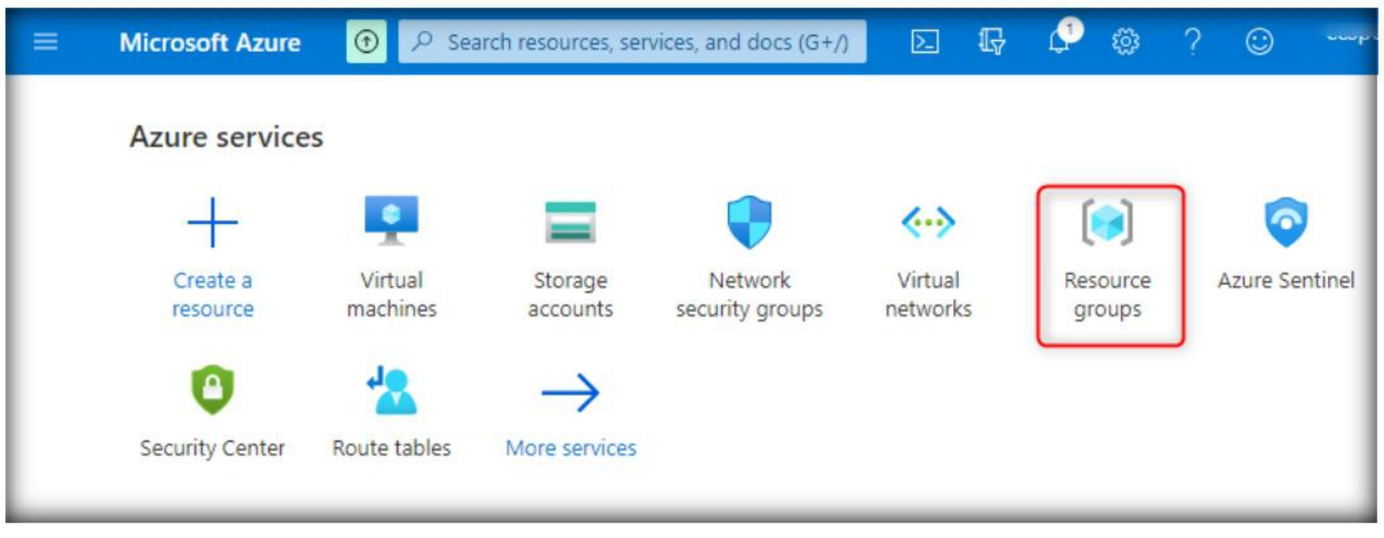


FIGURE 4.10.124: Selecting Resource Group

Certified Cloud Security Engineer Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

125. In **Resource groups**, click **securityengRG**.

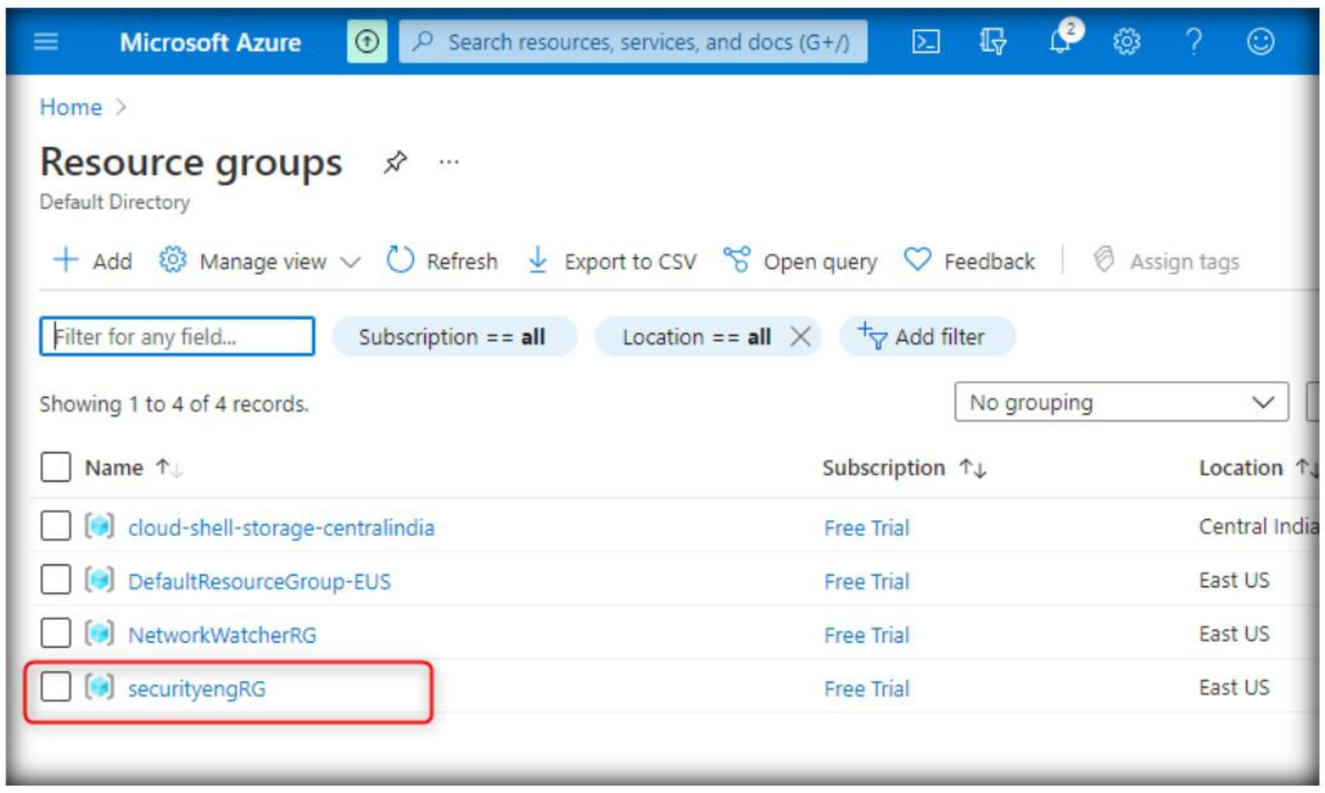


FIGURE 4.10.125: Selecting securityengRG Resource Group

126. In **securityengRG**, click on **mystorage25** storage account.

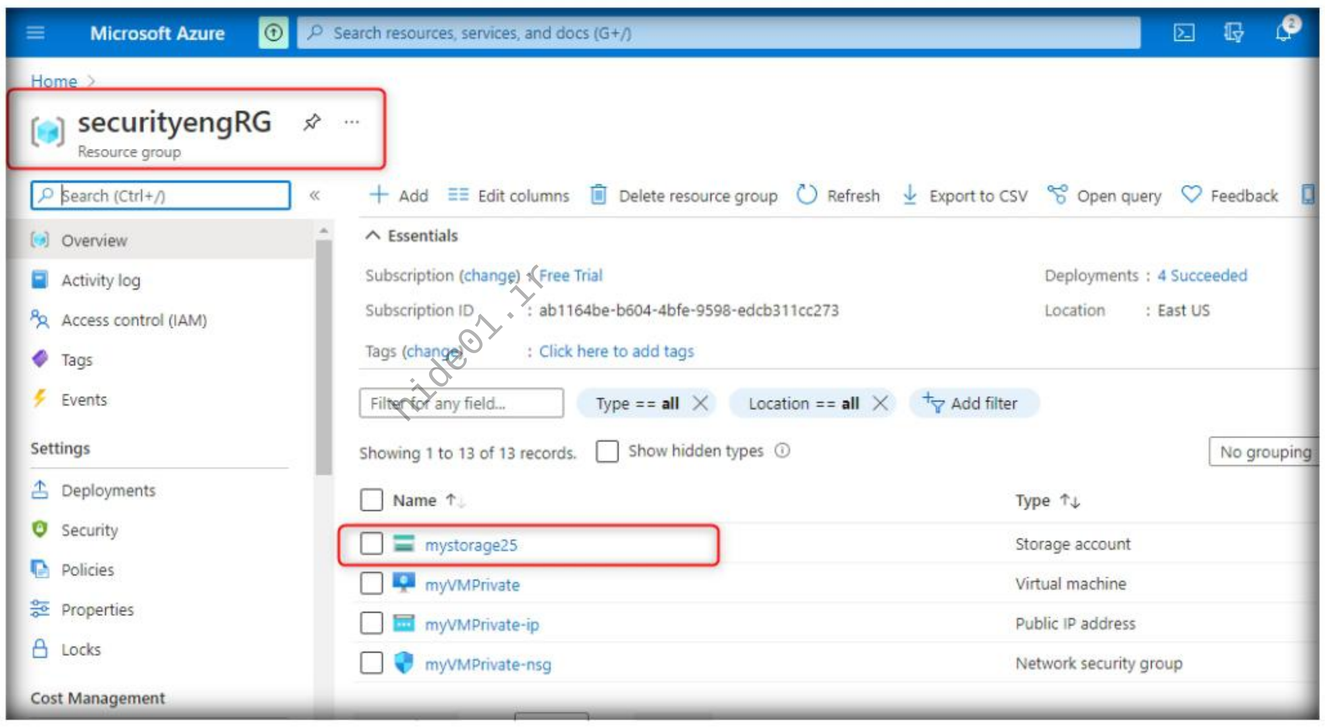


FIGURE 4.10.126: Selecting mystorage25 Storage Account

127. In **mystorage25** storage account, navigate and click on **File shares**.

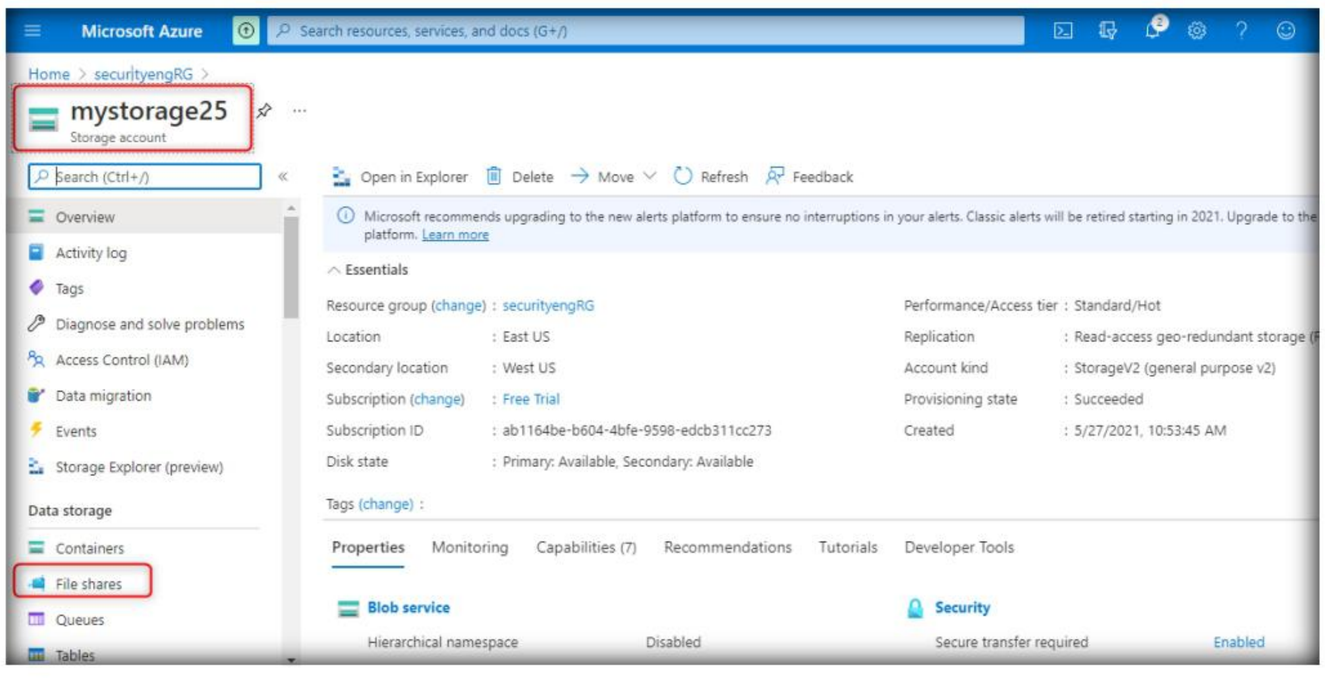


FIGURE 4.10.127: Selecting File Share

128. Then, click on **my-file-share**.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

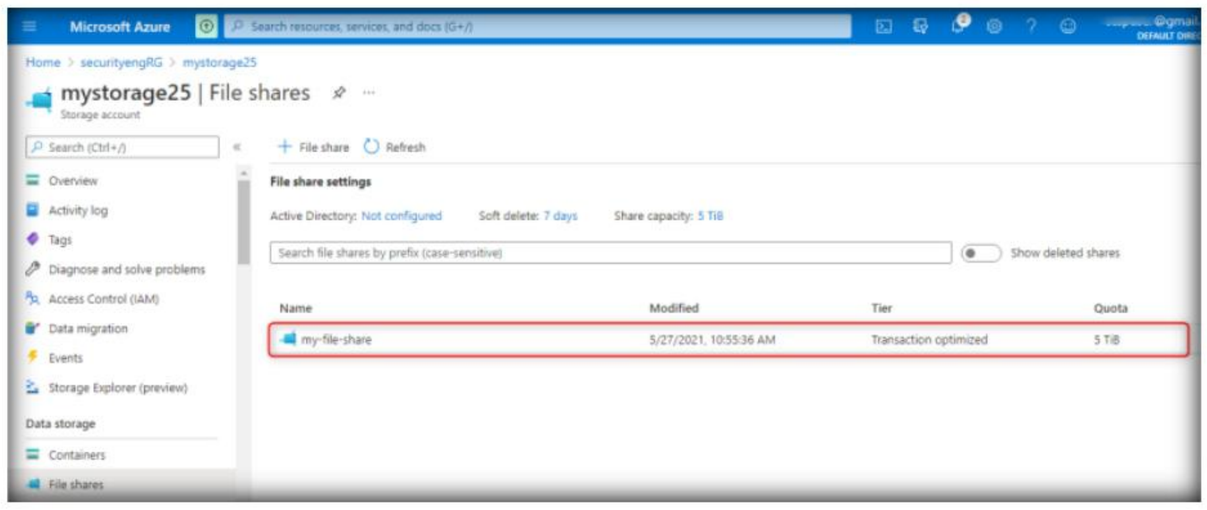


FIGURE 4.10.128: Selecting my-file-share

129. You will observe a message stating **This machine doesn't seem to have access**. The access is denied because your computer is not in the private subnet of the SecEng-VNET virtual network.

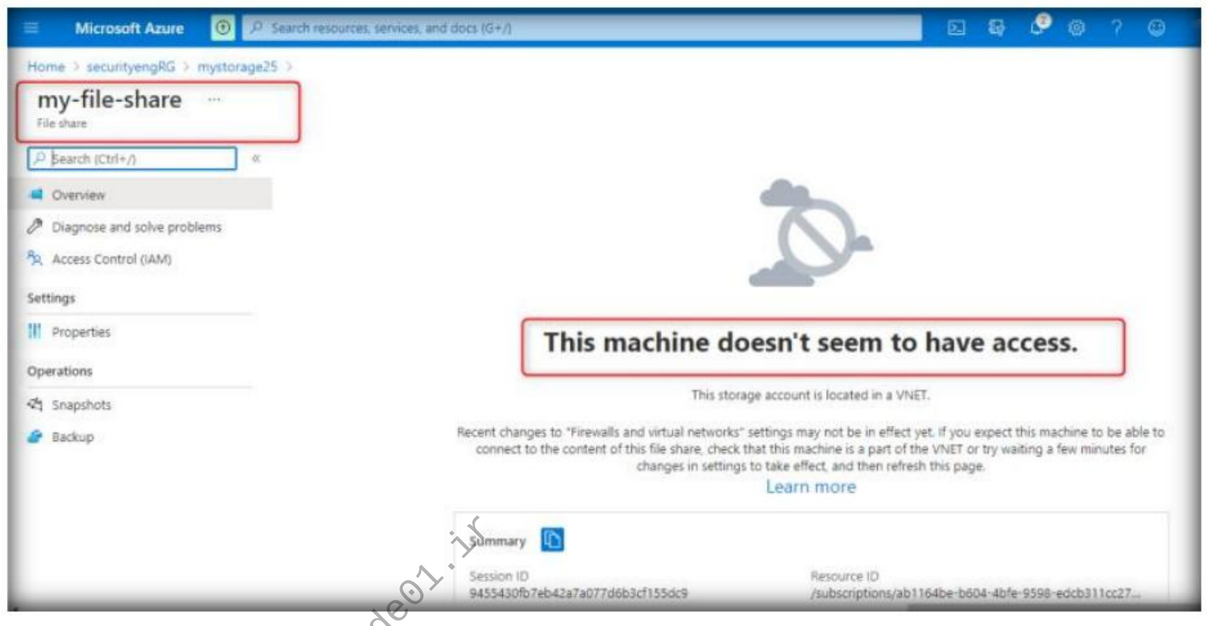


FIGURE 4.10.129: Access is Denied in my-file-share Window

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

130. To delete securityengRG resource group, click on **securityengRG**. You will be redirected to **securityengRG** storage group. In **securityengRG**, click on **Delete resource group**.

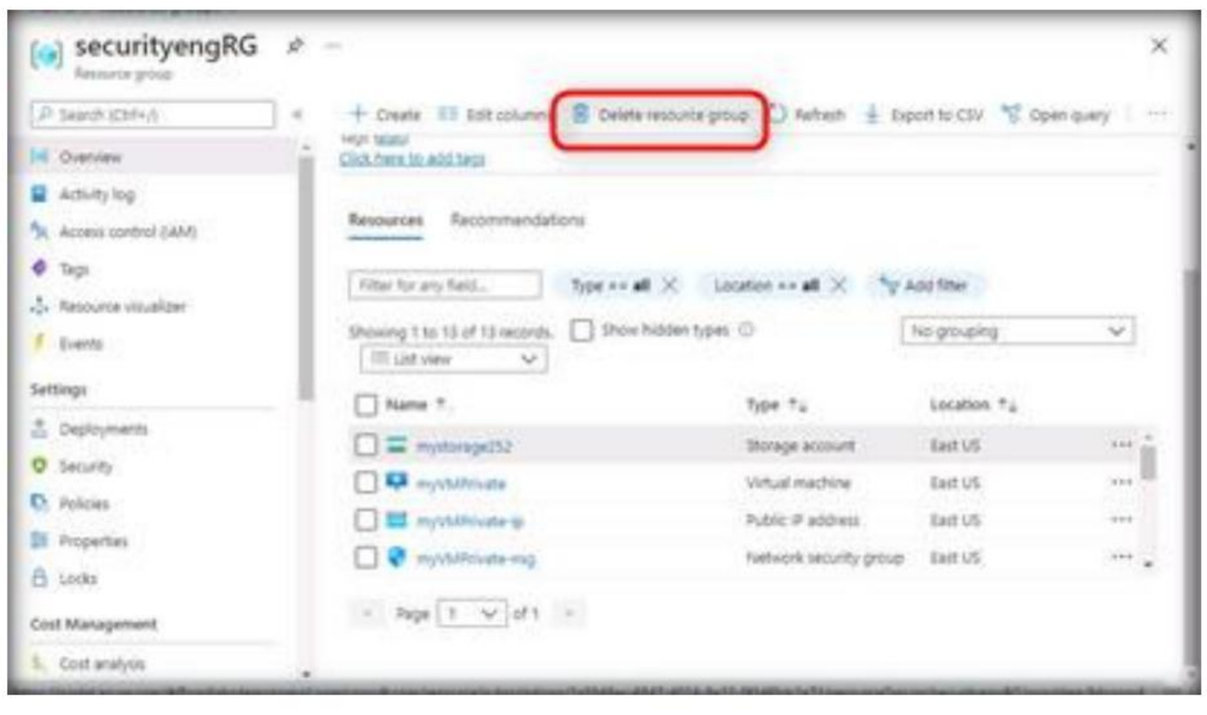


FIGURE 4.10.130: Deleting Resource Group

131. Type the resource group name as **securityengRG** and click on the **Delete** button. After a few minutes, the securityengRG resource group will be successfully deleted.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

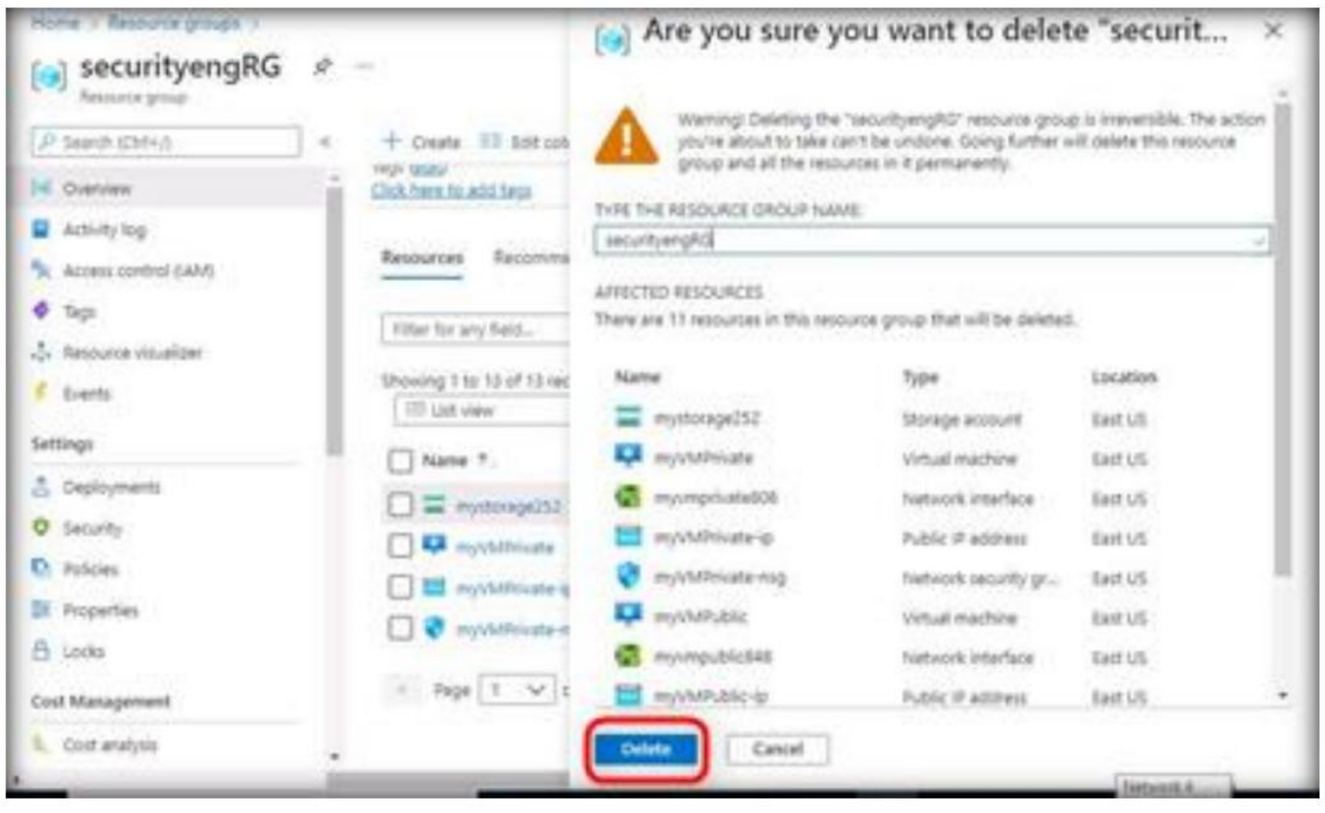


FIGURE 4.10.131: Deleting Resource Group

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.

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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:

hide01.ir

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**".

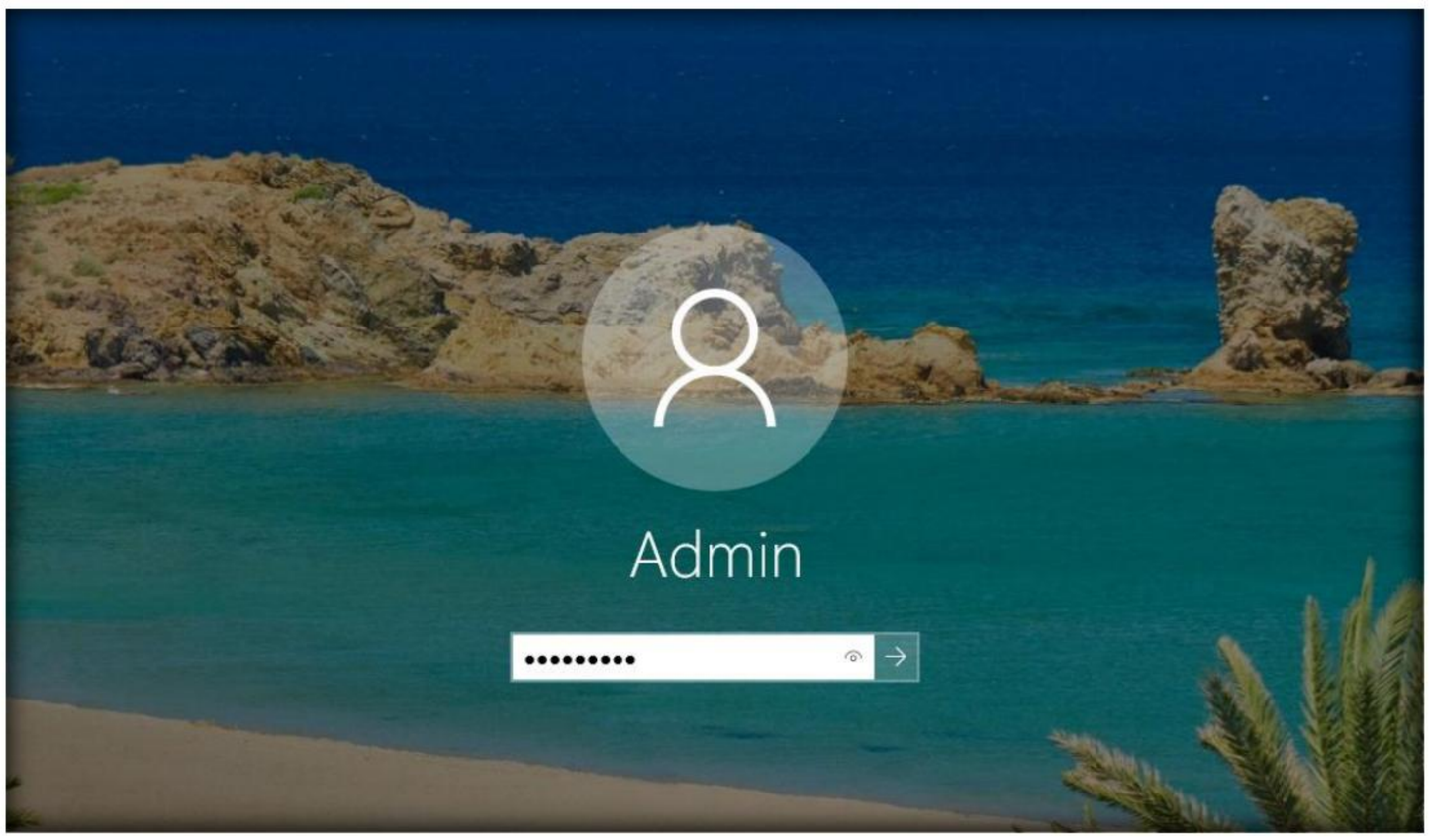


FIGURE 4.11.1: Launch Admin Machine and Log in

Certified Cloud Security Engineer Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

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**.

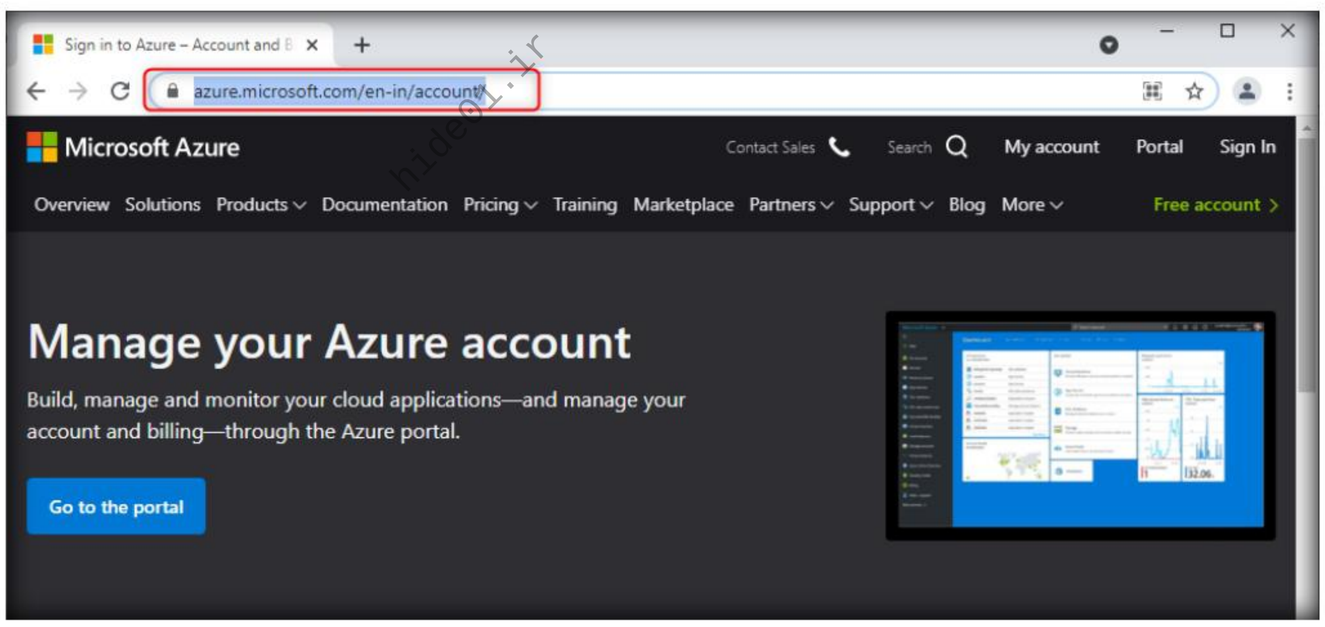


FIGURE 4.11.3: Entering the URL of Microsoft Azure

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

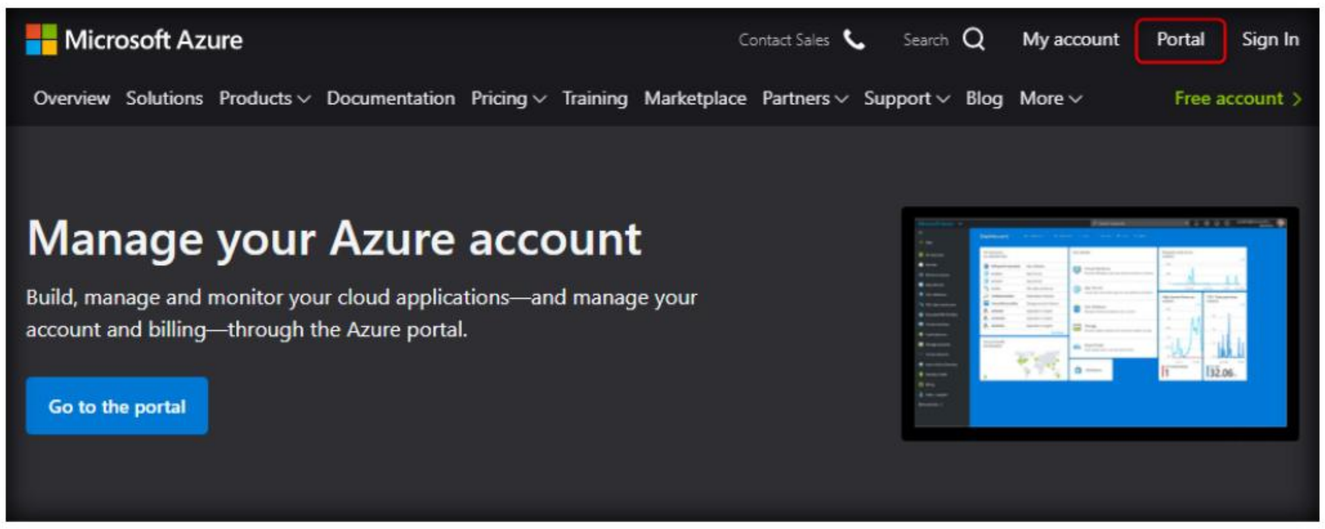


FIGURE 4.11.4: Sign in to Azure Portal

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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

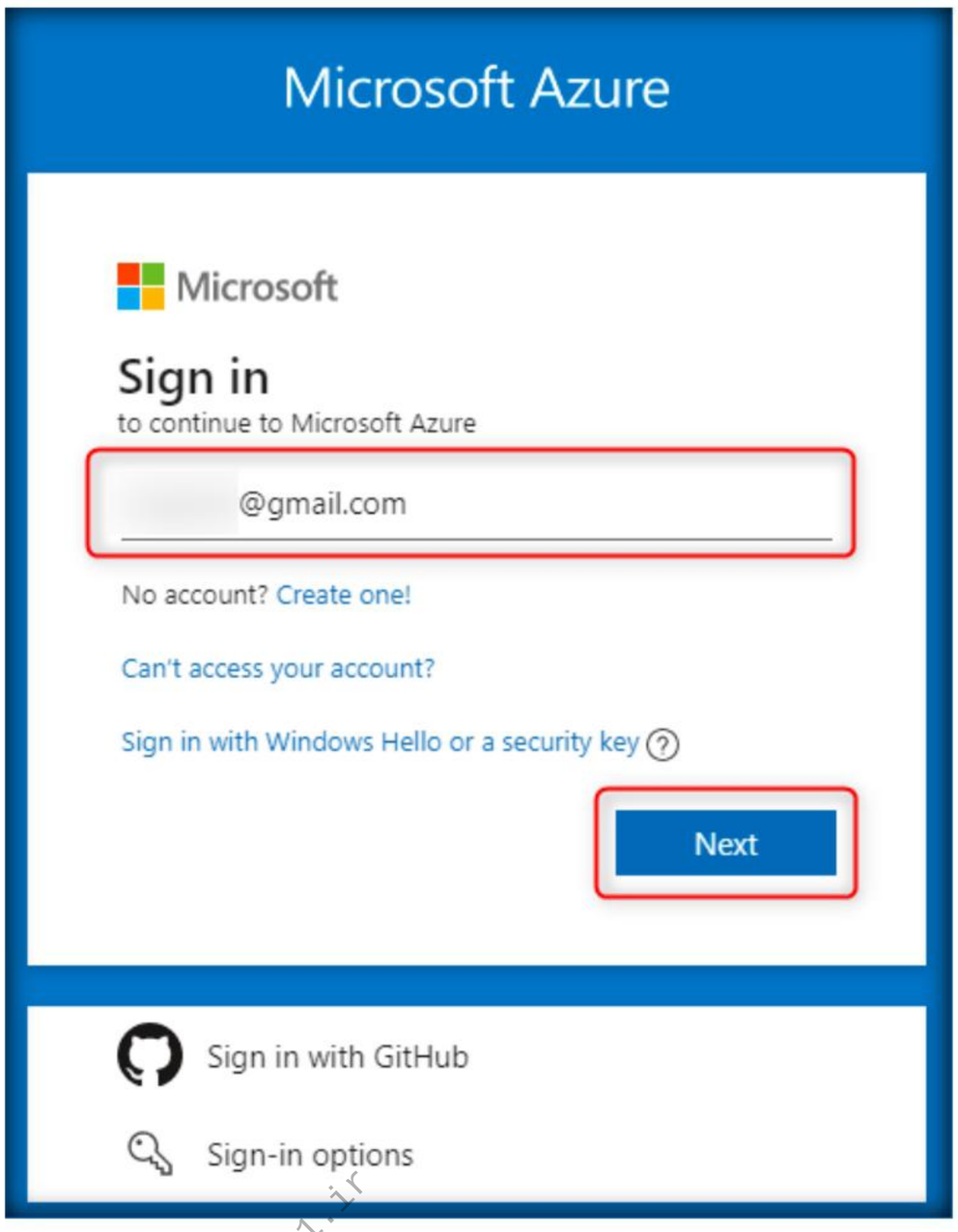


FIGURE 4.11.5: Entering Account ID to continue

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

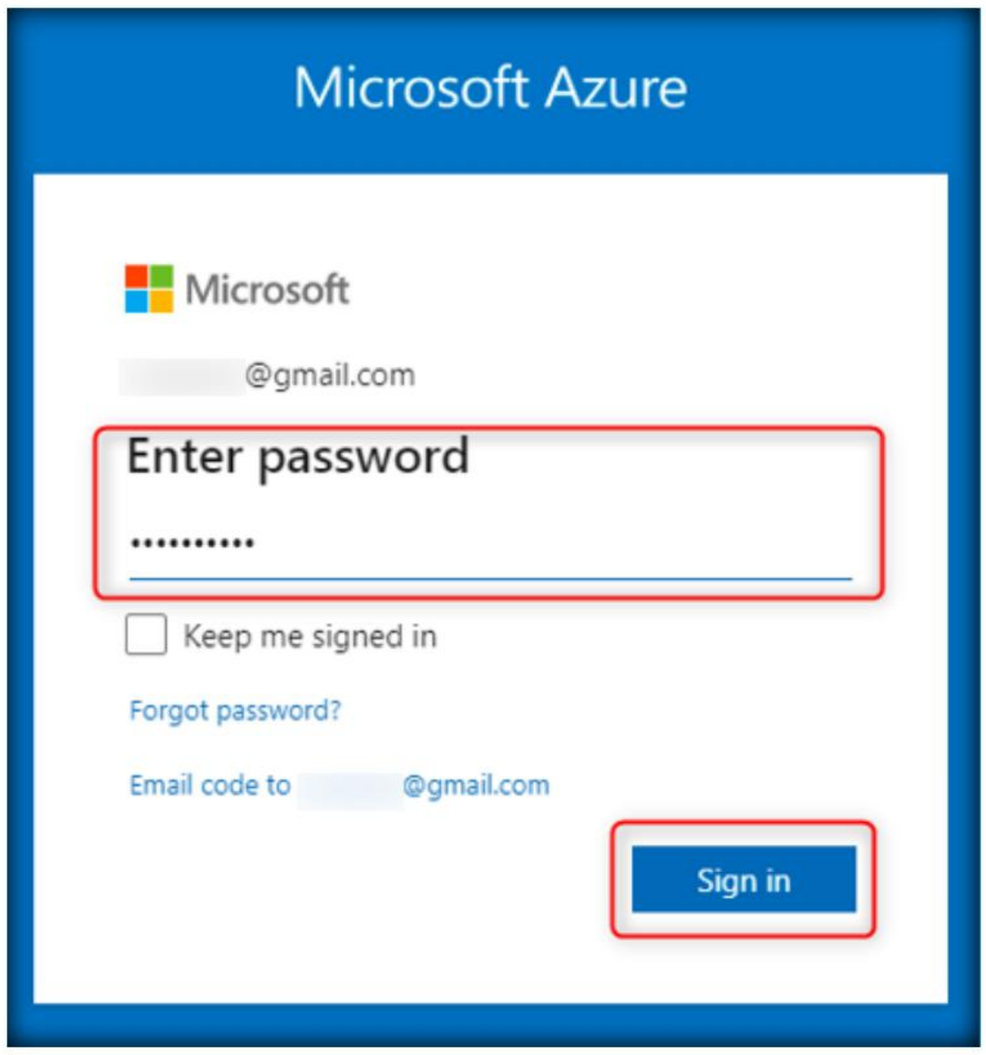


FIGURE 4.11.6: Sign in to Azure Account

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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**.

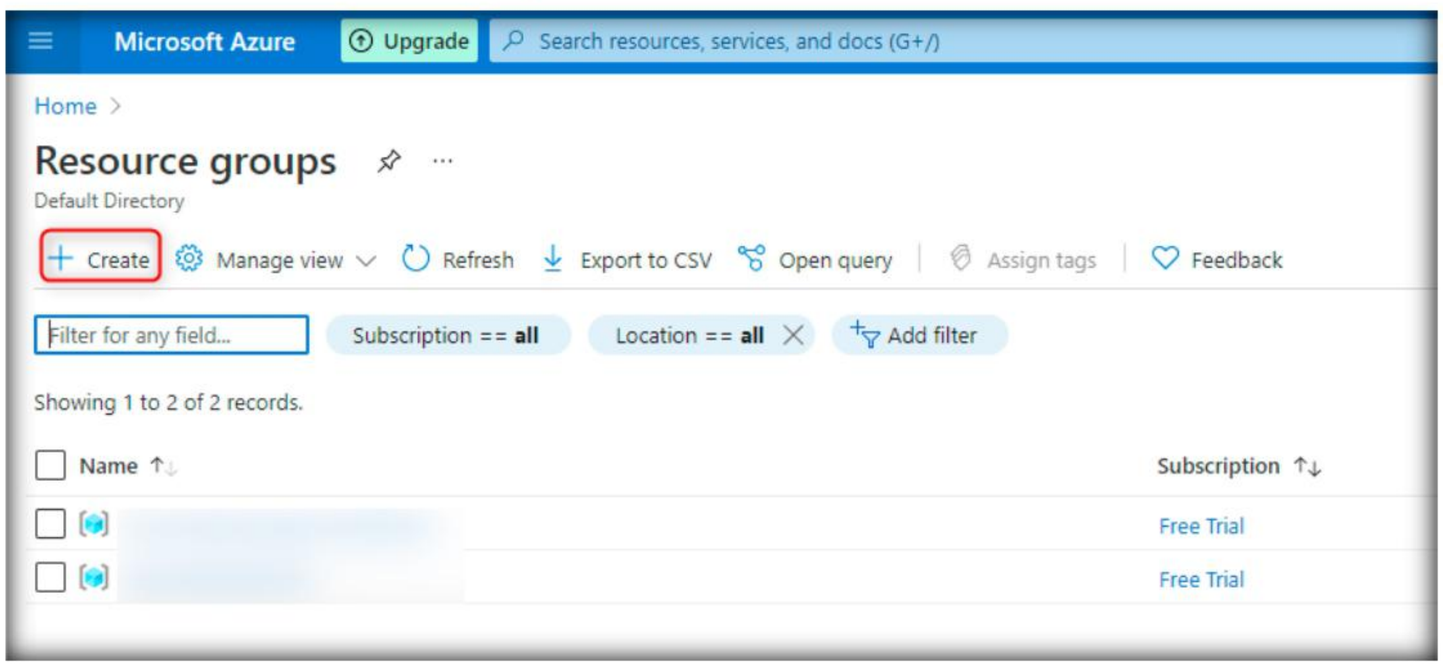


FIGURE 4.11.8: Creating Resource Group

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 >**.

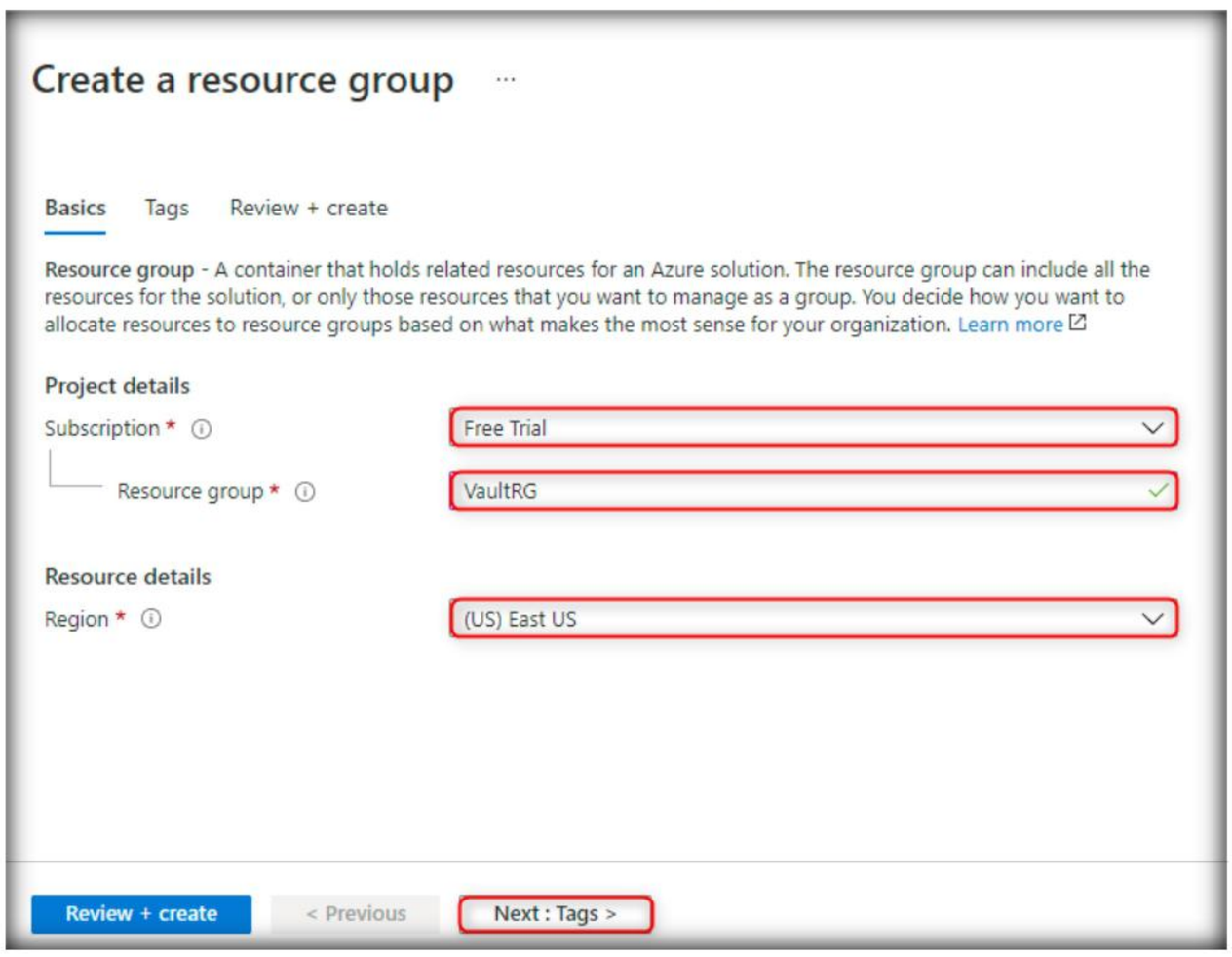


FIGURE 4.11.9: Configuring Resource Group

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

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

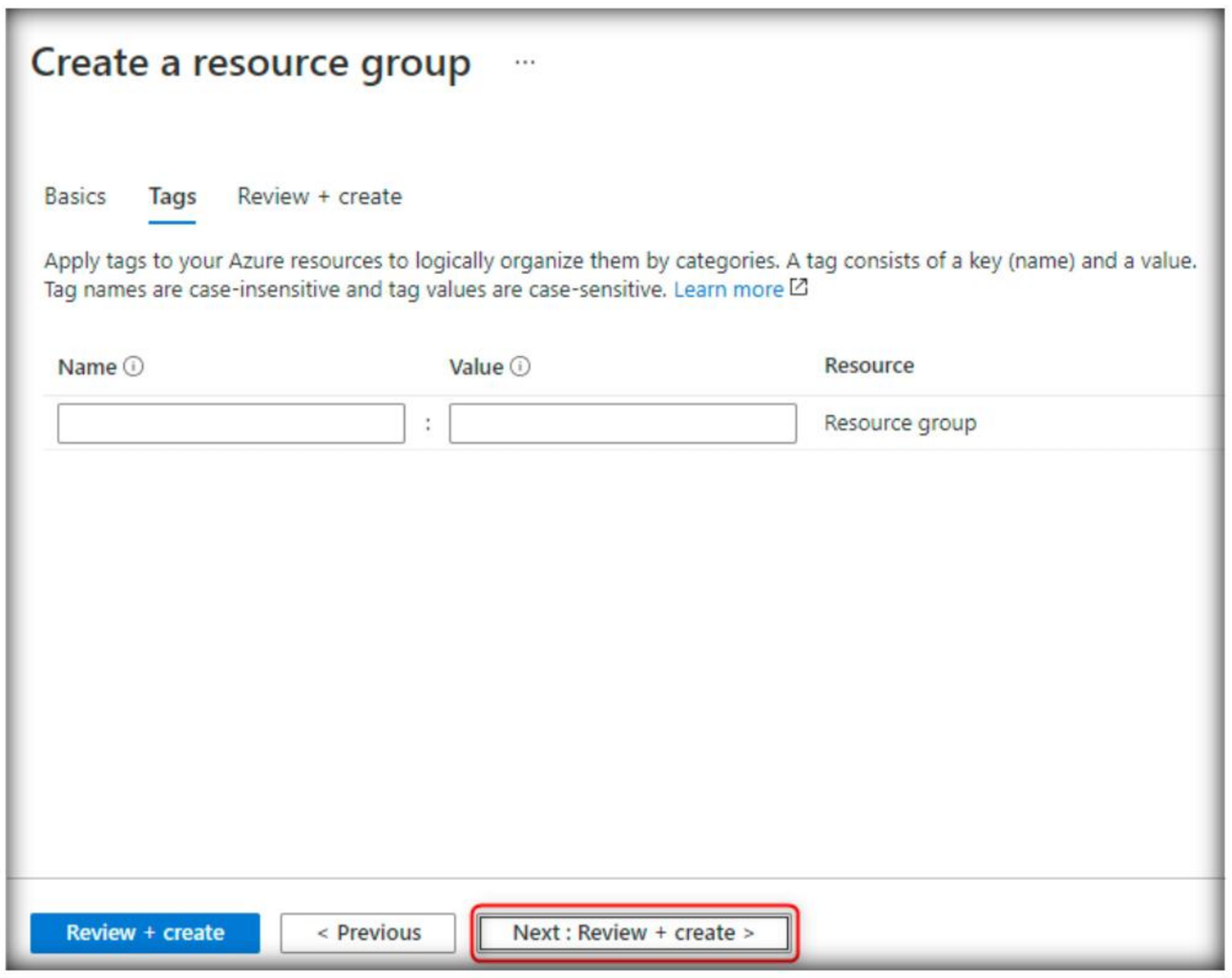


FIGURE 4.11.10: Proceeding with Configuration

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

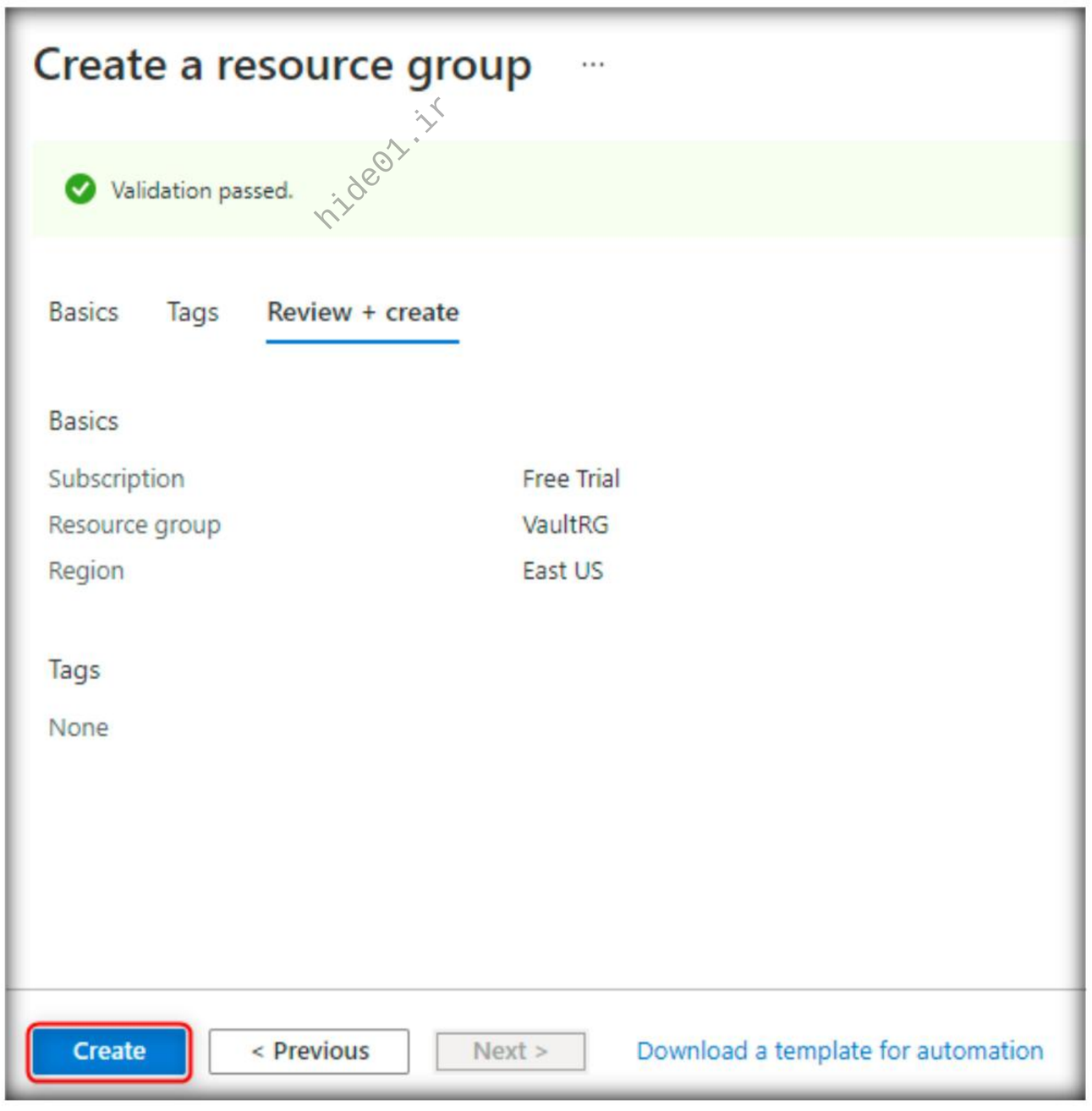


FIGURE 4.11.11: Creating Resource Group

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

12. Thus, the resource group is successfully created.

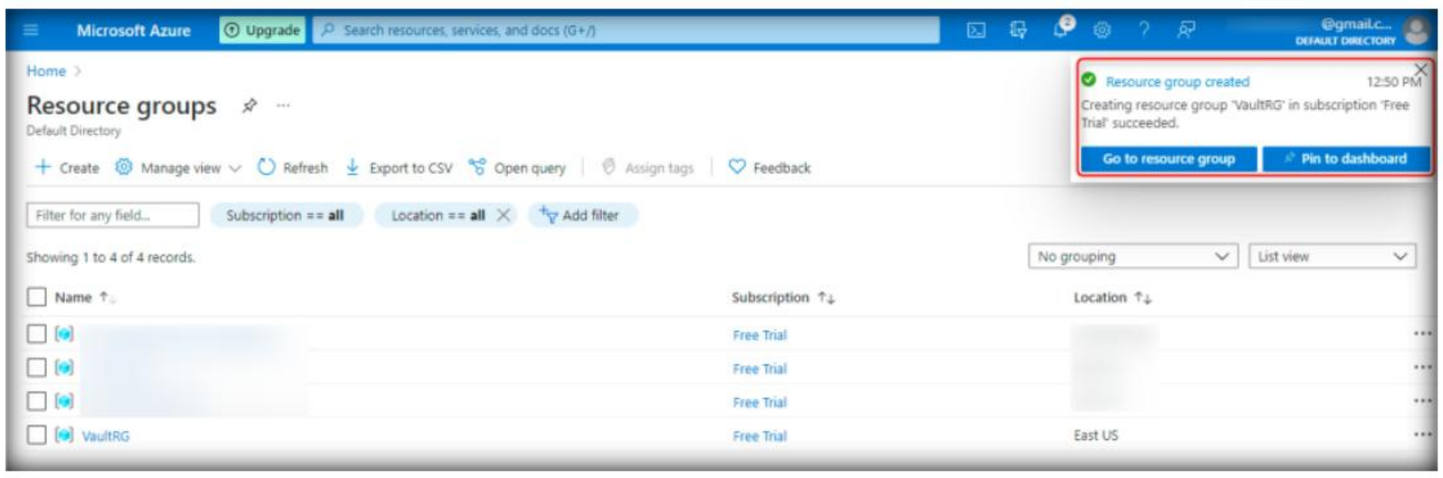


FIGURE 4.11.12: Resource Group Created Successfully

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

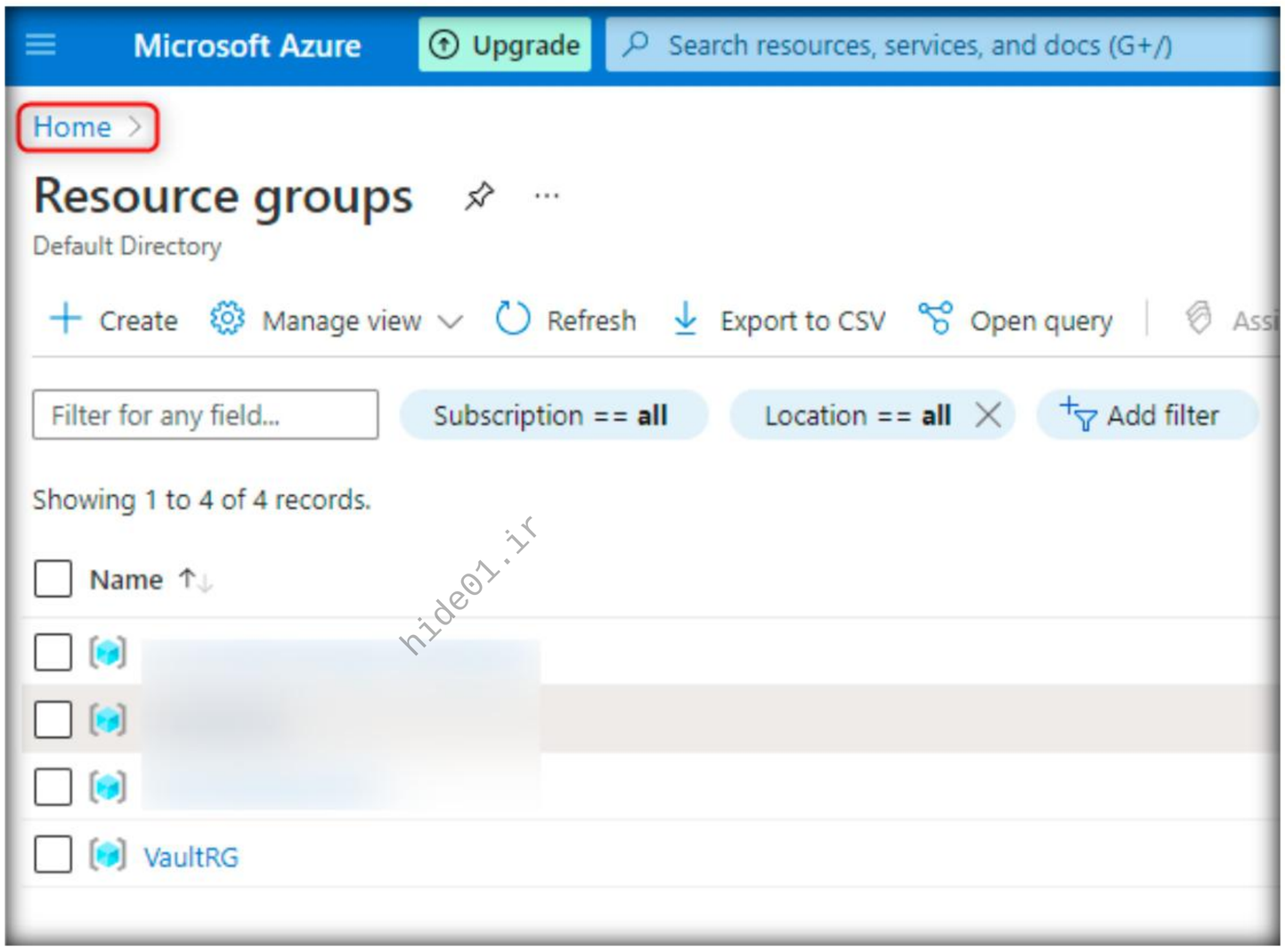


FIGURE 4.11.13: Navigating back to Home Page

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.

TASK 2

Creating an Azure key vault to store passwords

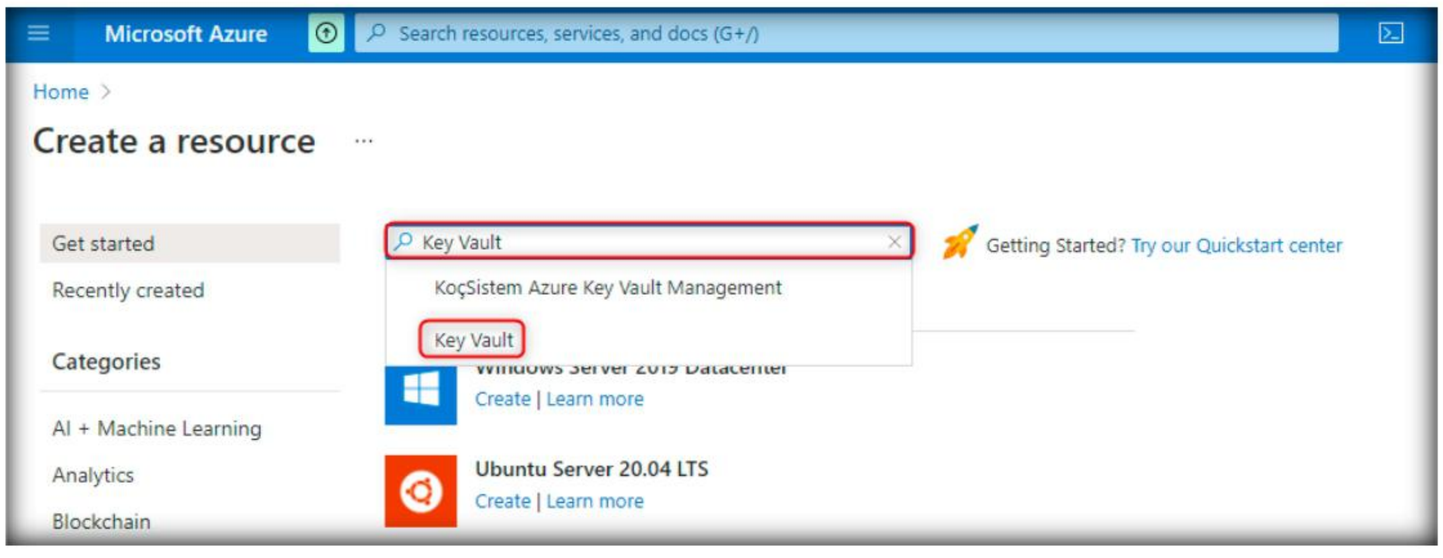


FIGURE 4.11.14: Navigating to Key Vault

Certified Cloud Security Engineer Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

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

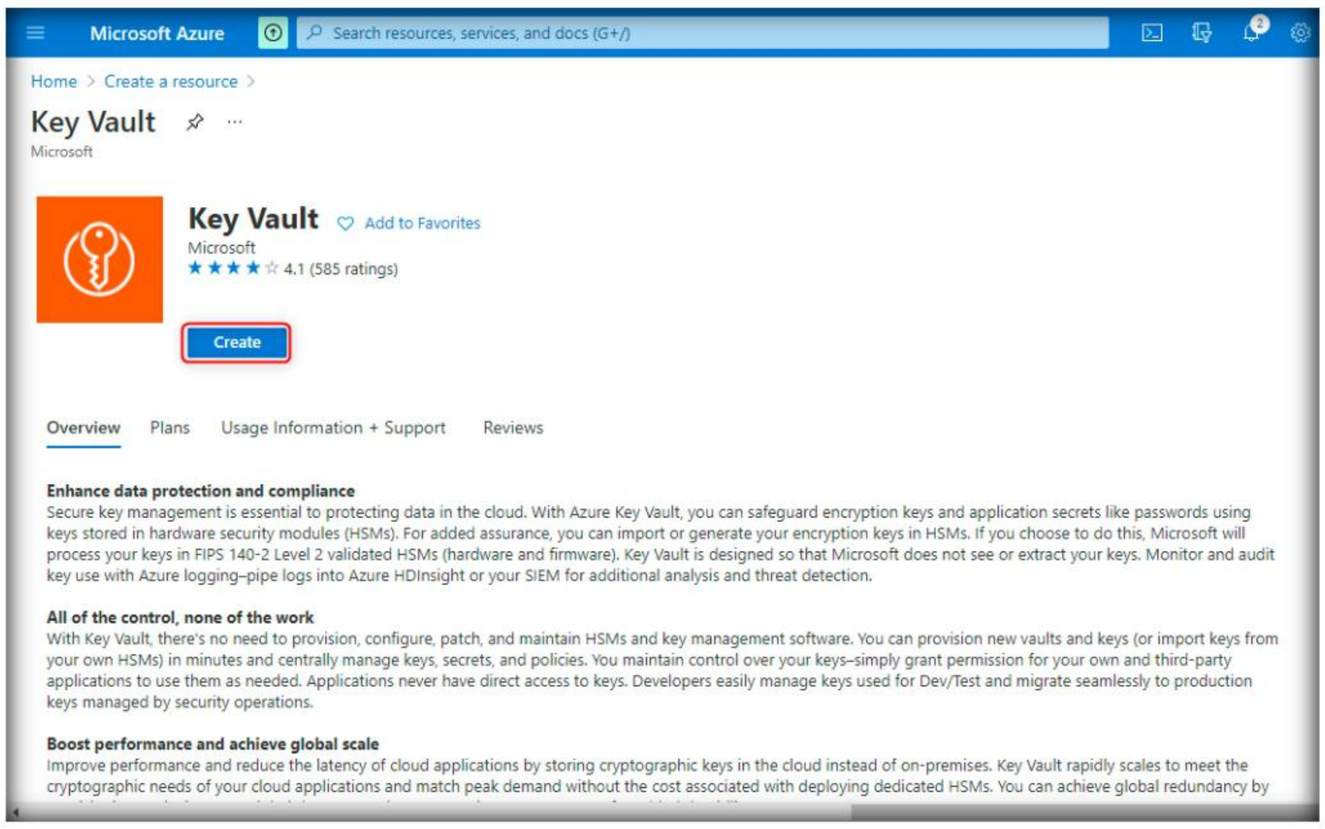


FIGURE 4.11.15: Creating Key Vault

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.

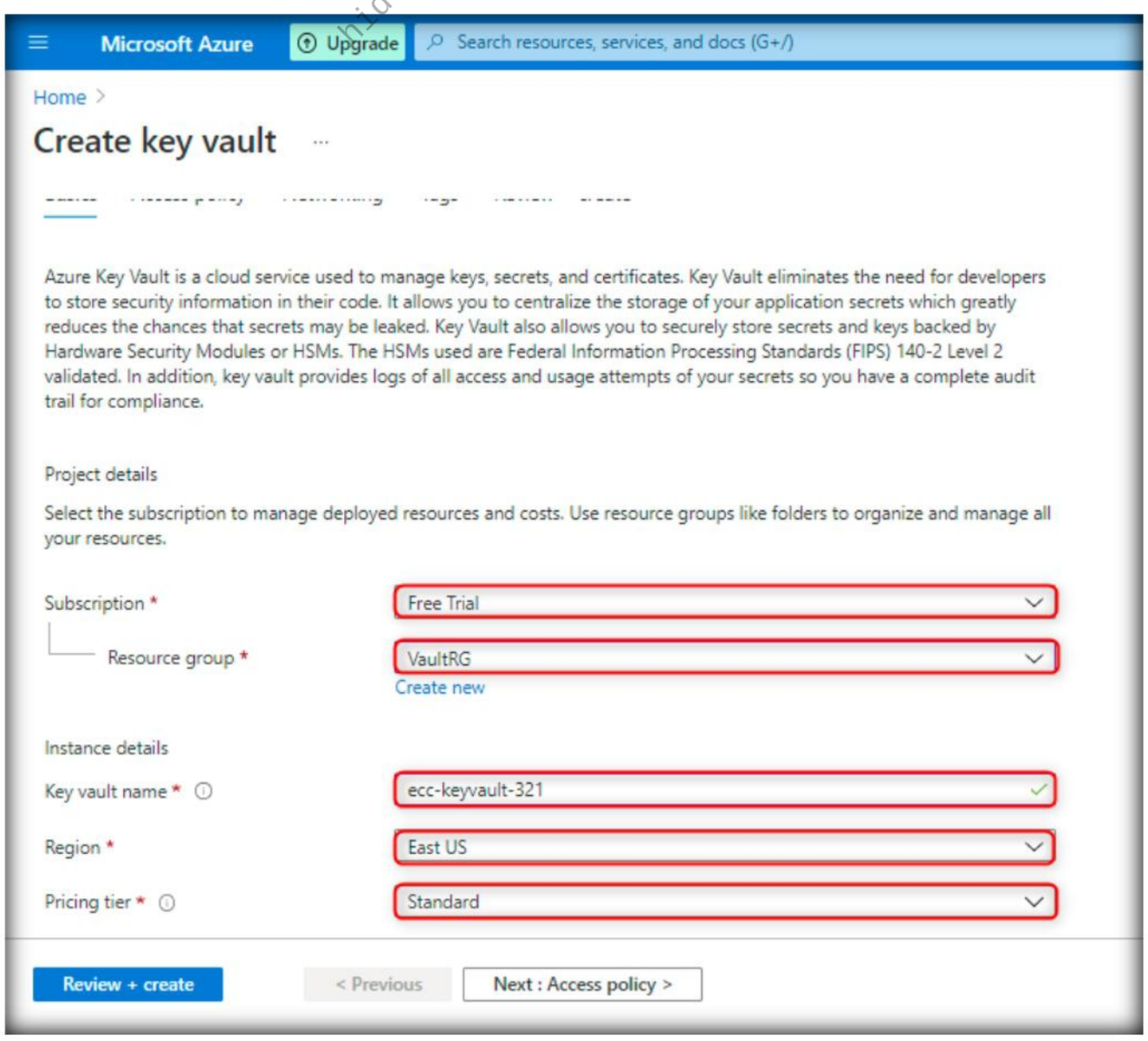


FIGURE 4.11.16: Configuring Key Vault

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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

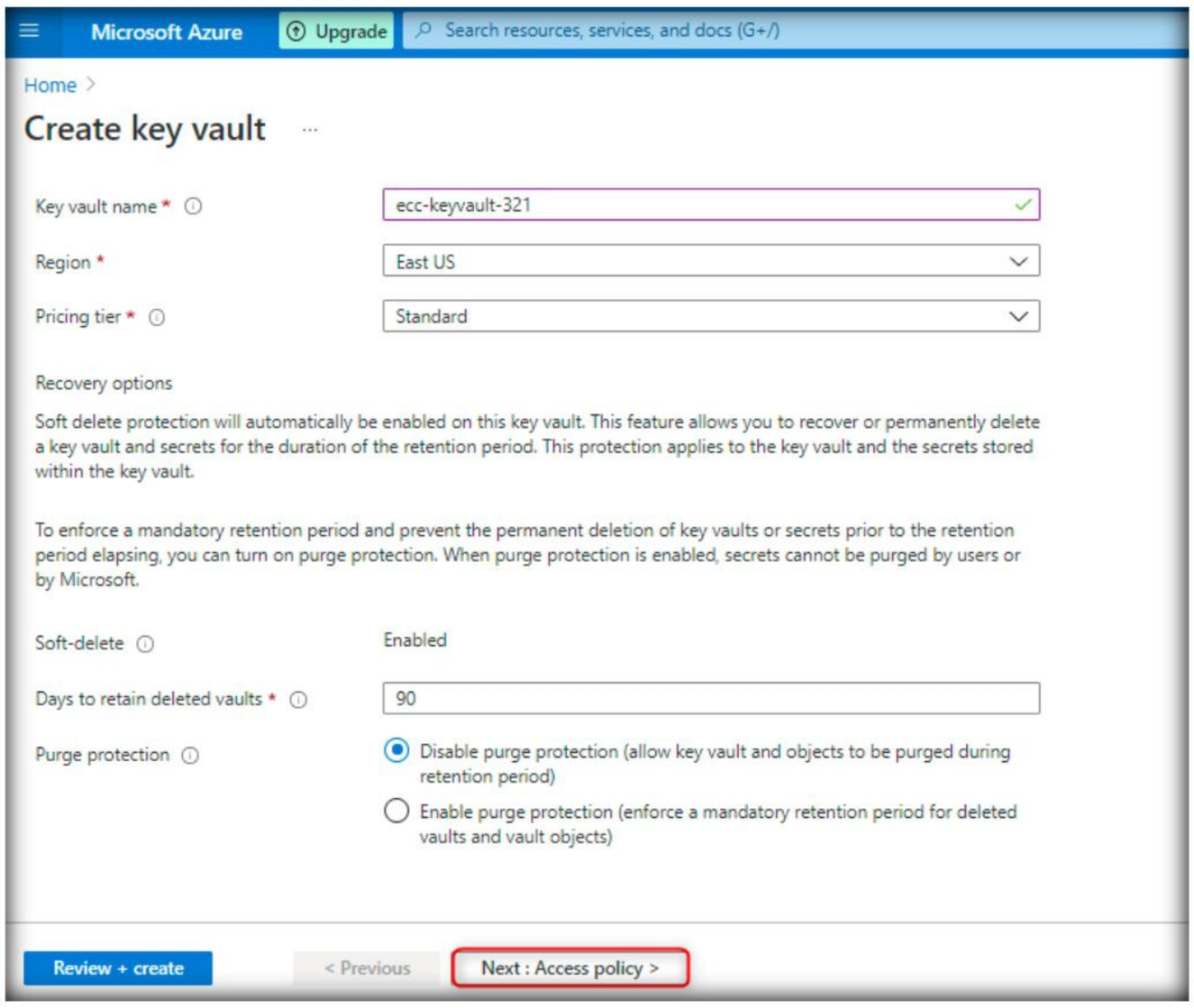


FIGURE 4.11.17: Proceeding with Configuration

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

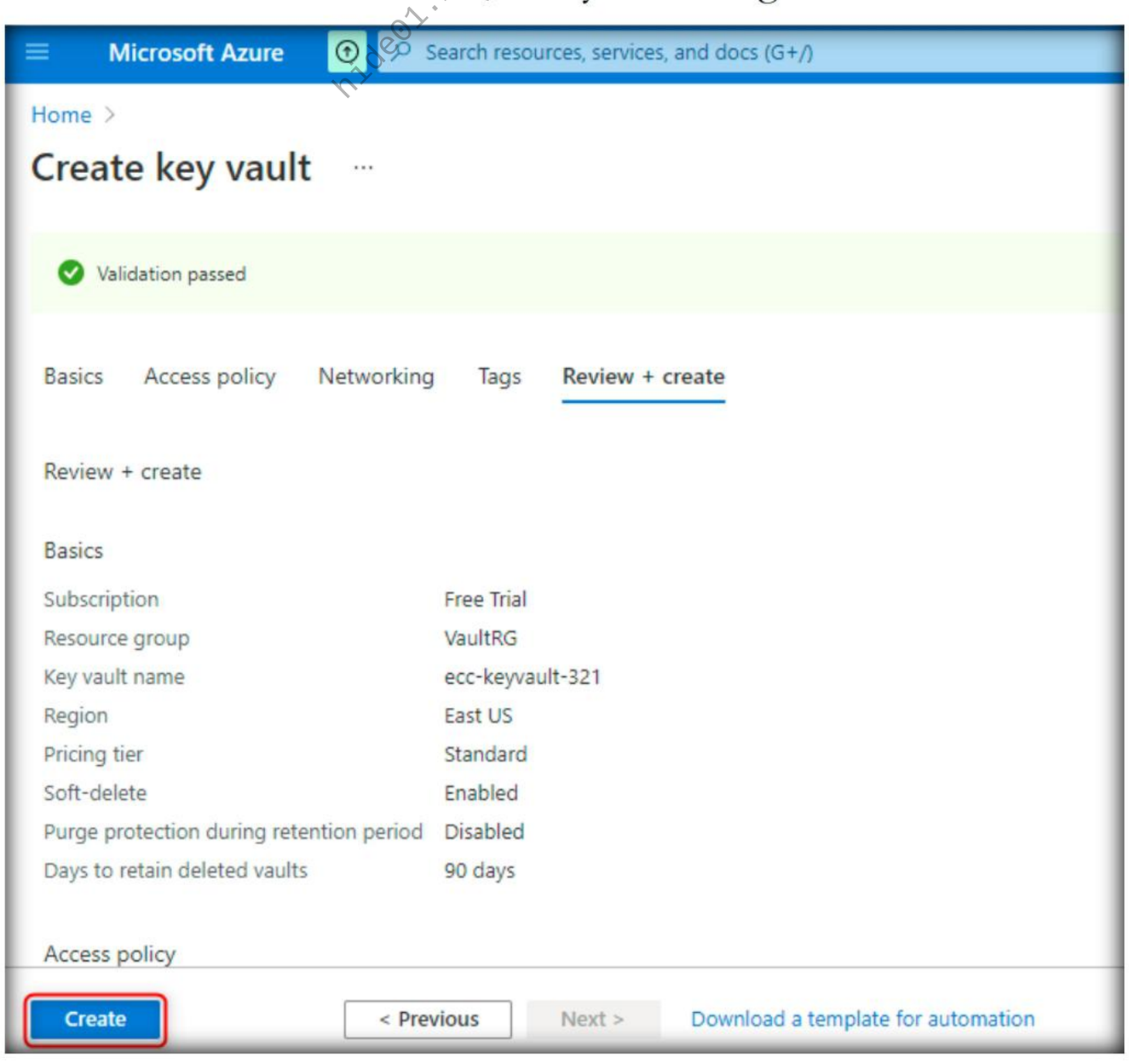


FIGURE 4.11.18: Creating Key Vault

19. Thus, the key vault is successfully created.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

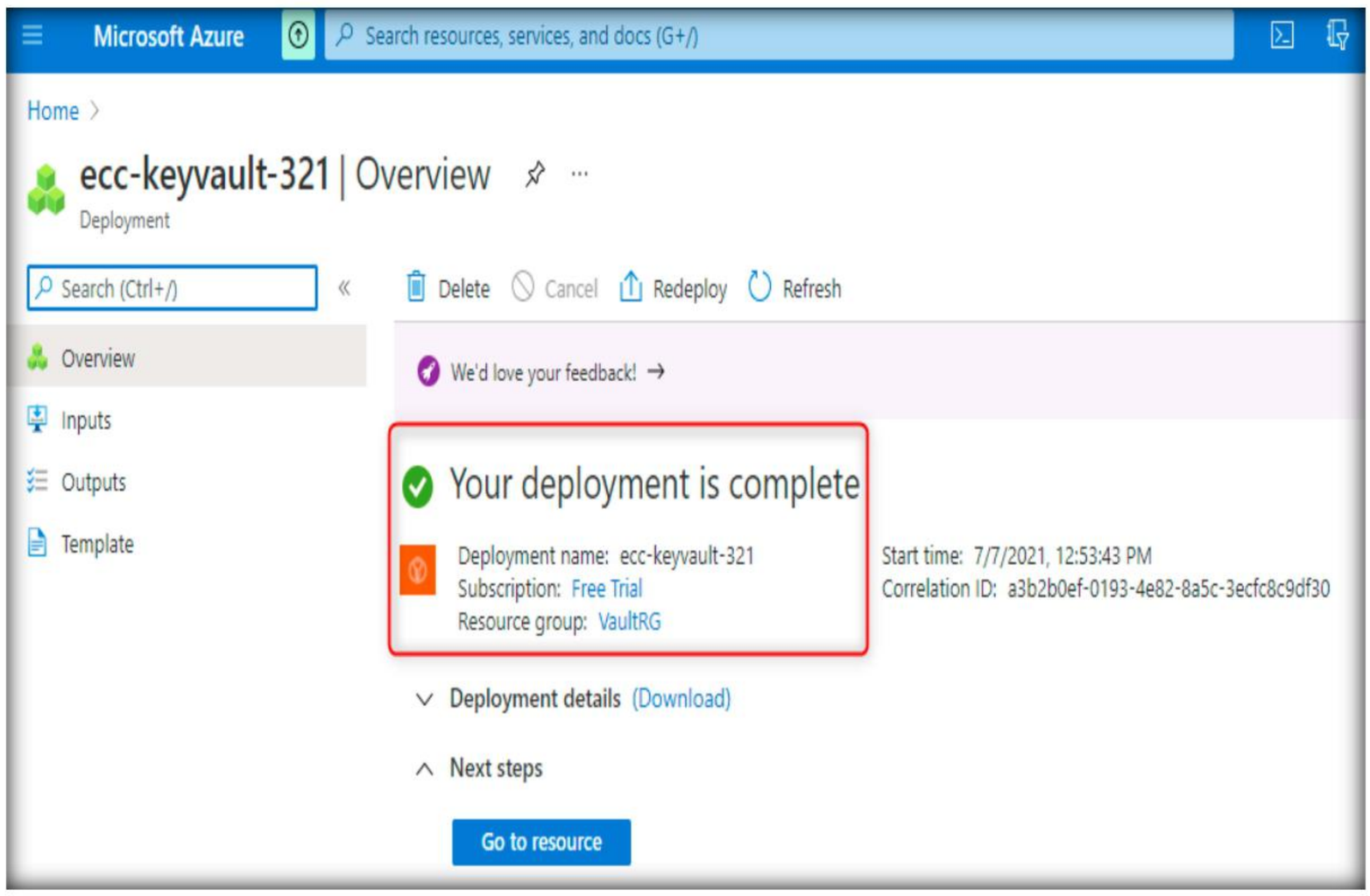


FIGURE 4.11.19: Key Vault Created Successfully

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.

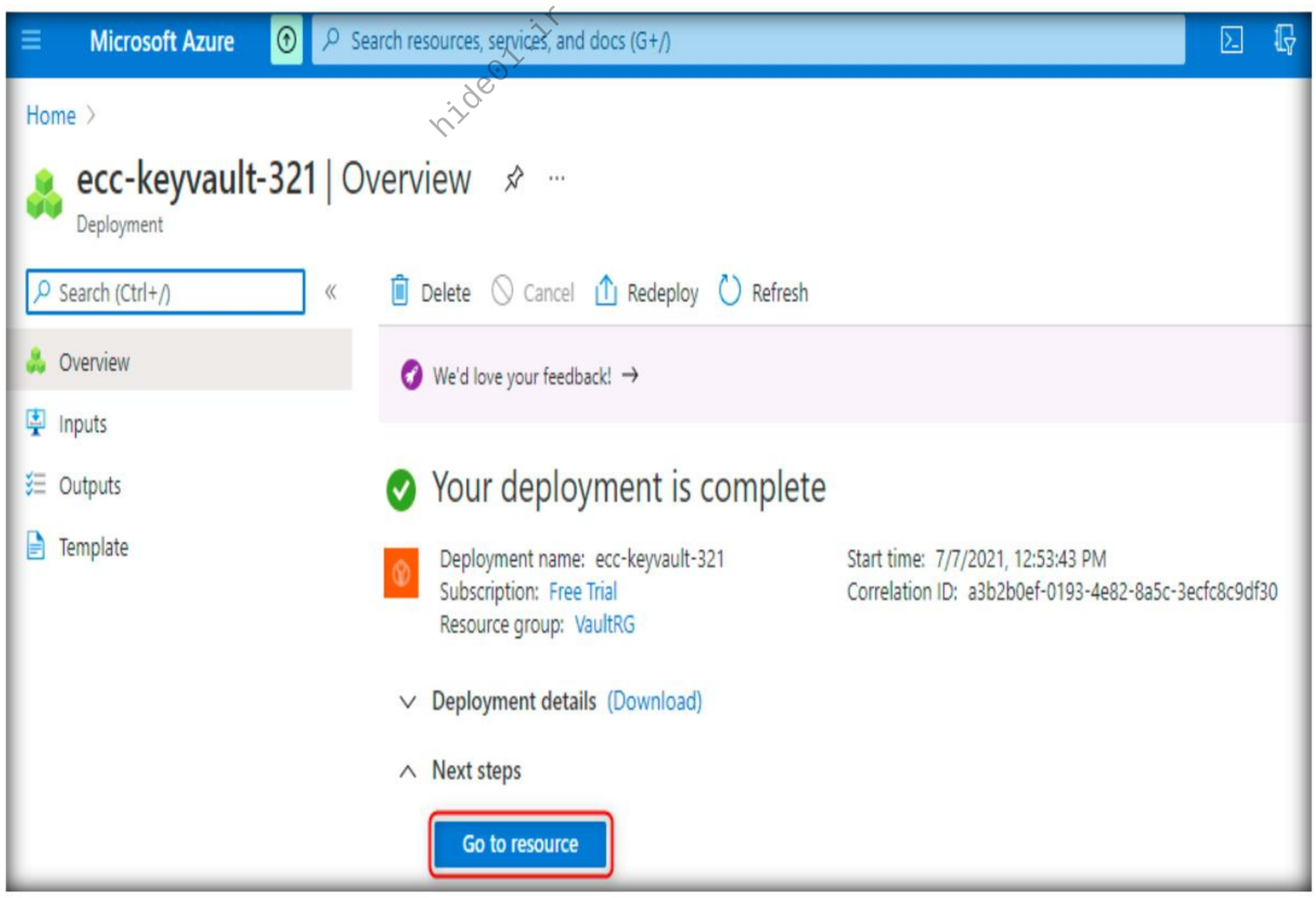


FIGURE 4.11.20: Navigating to the Key Vault

Certified Cloud Security Engineer Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

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

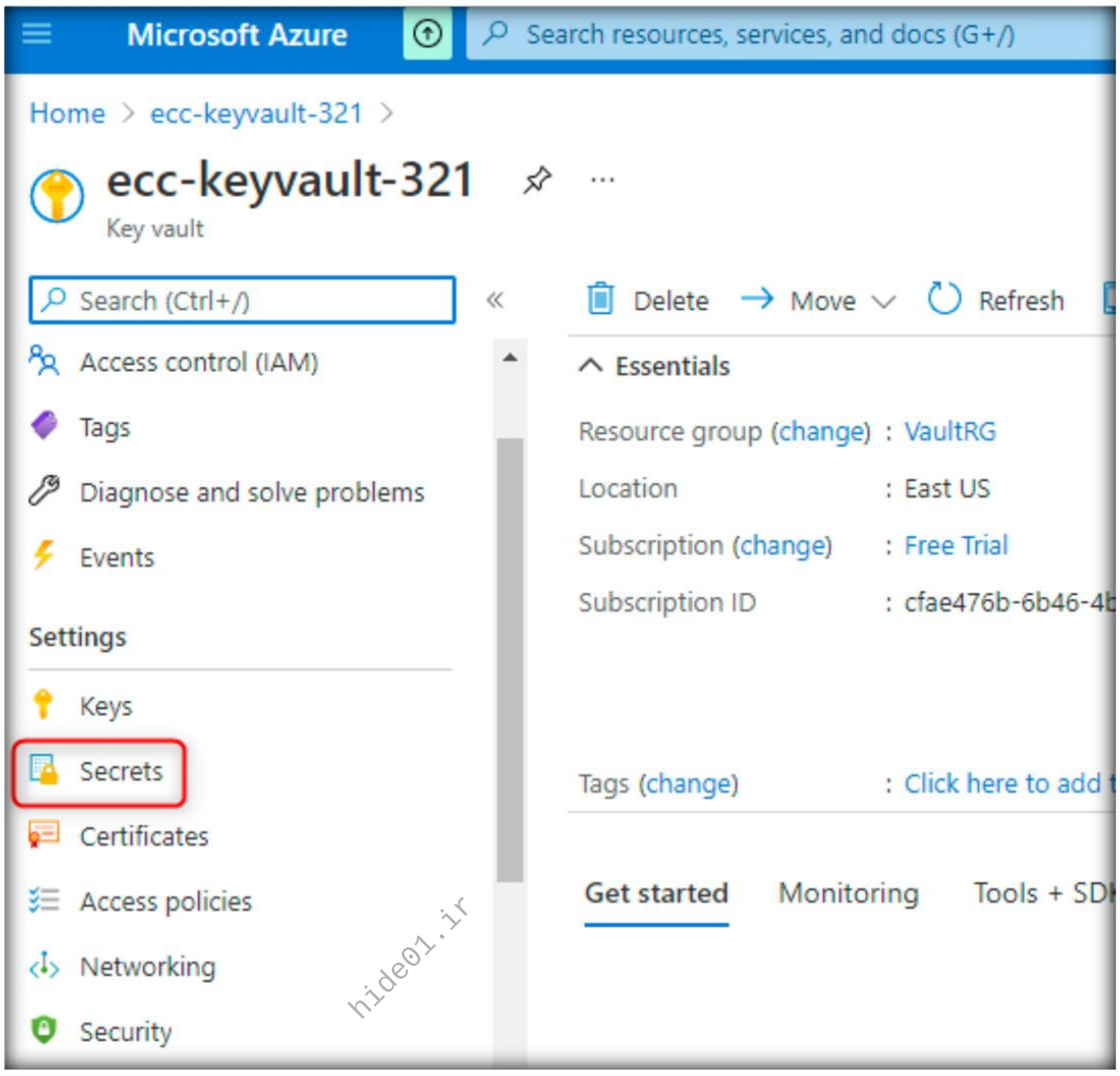


FIGURE 4.11.21: Navigating to Secrets

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

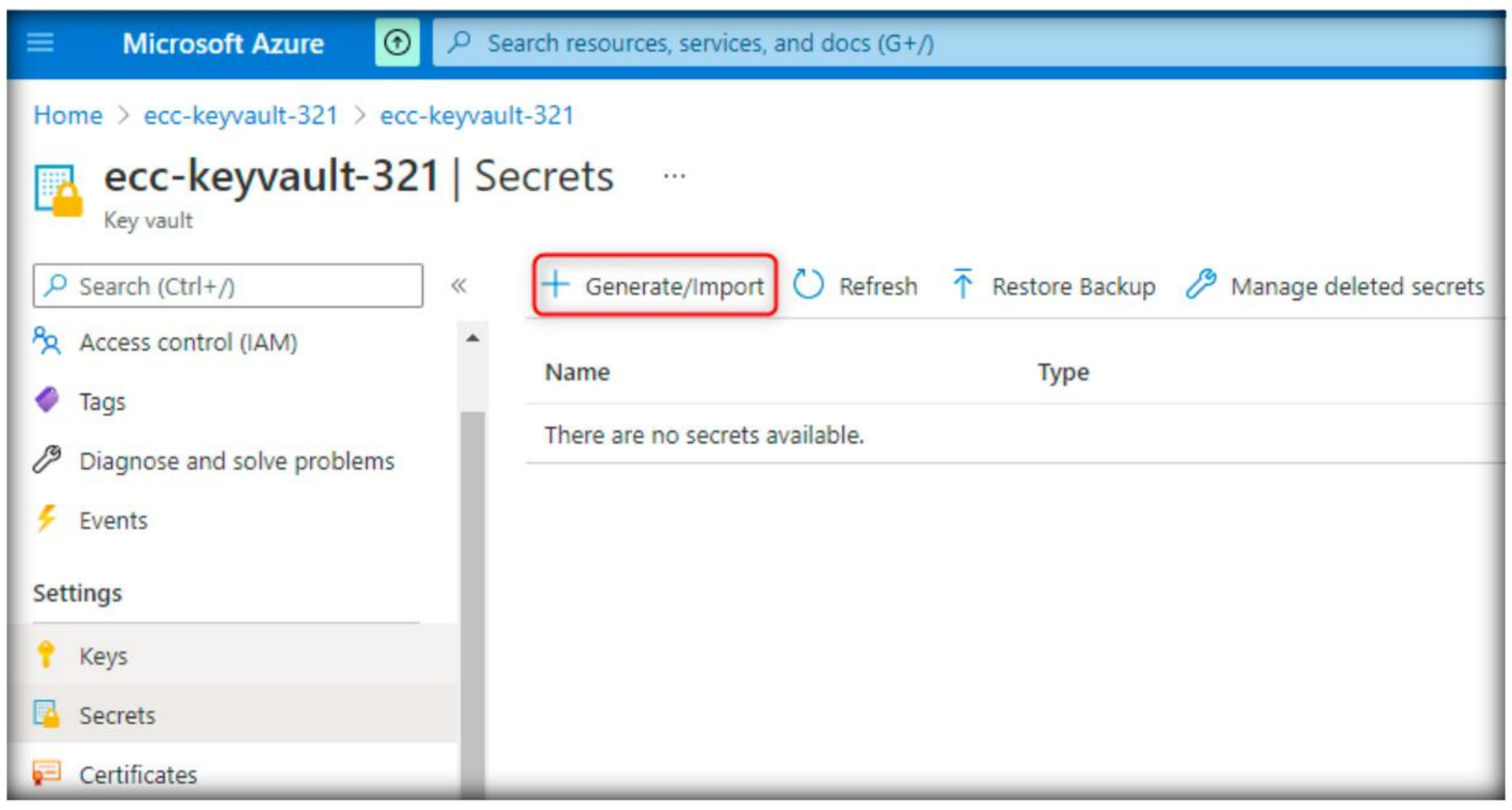


FIGURE 4.11.22: Adding Secret

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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.

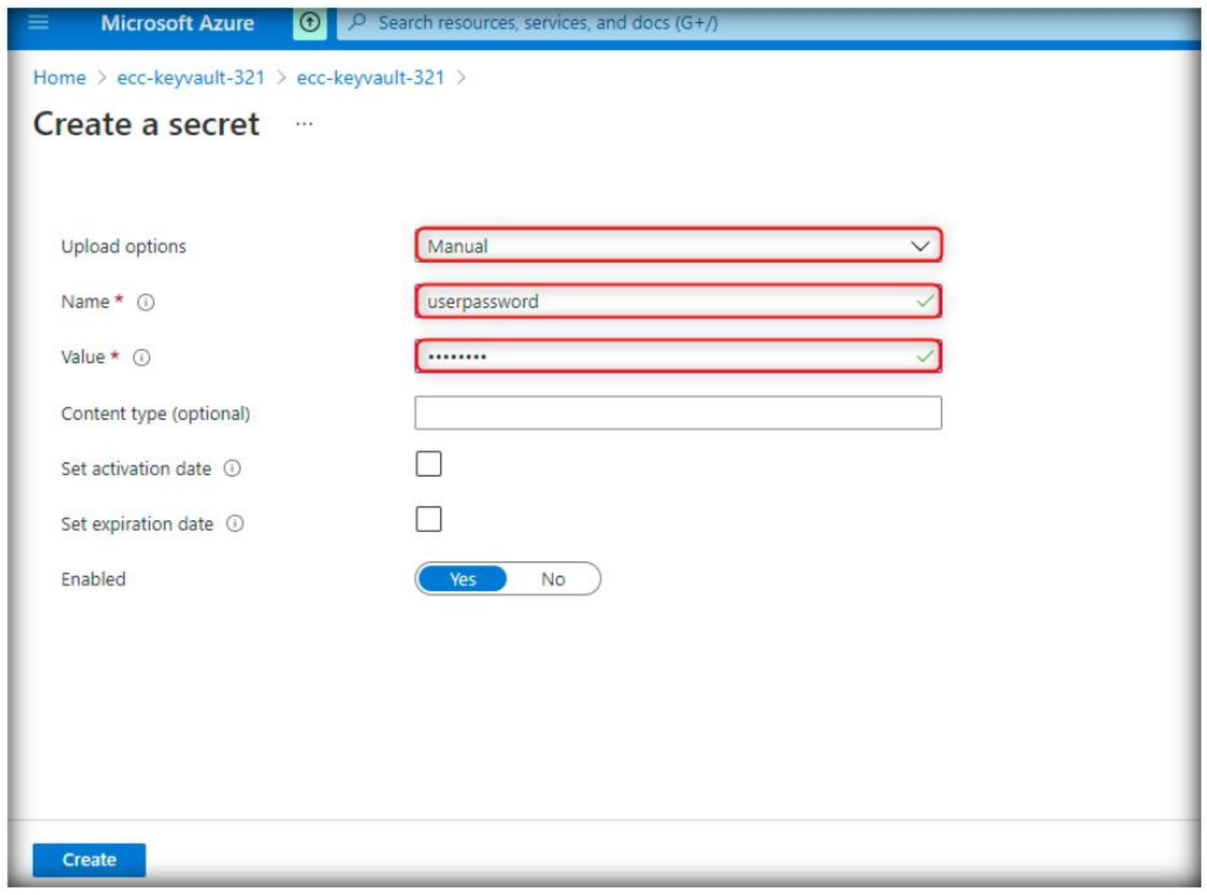


FIGURE 4.11.23: Creating Secret

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.

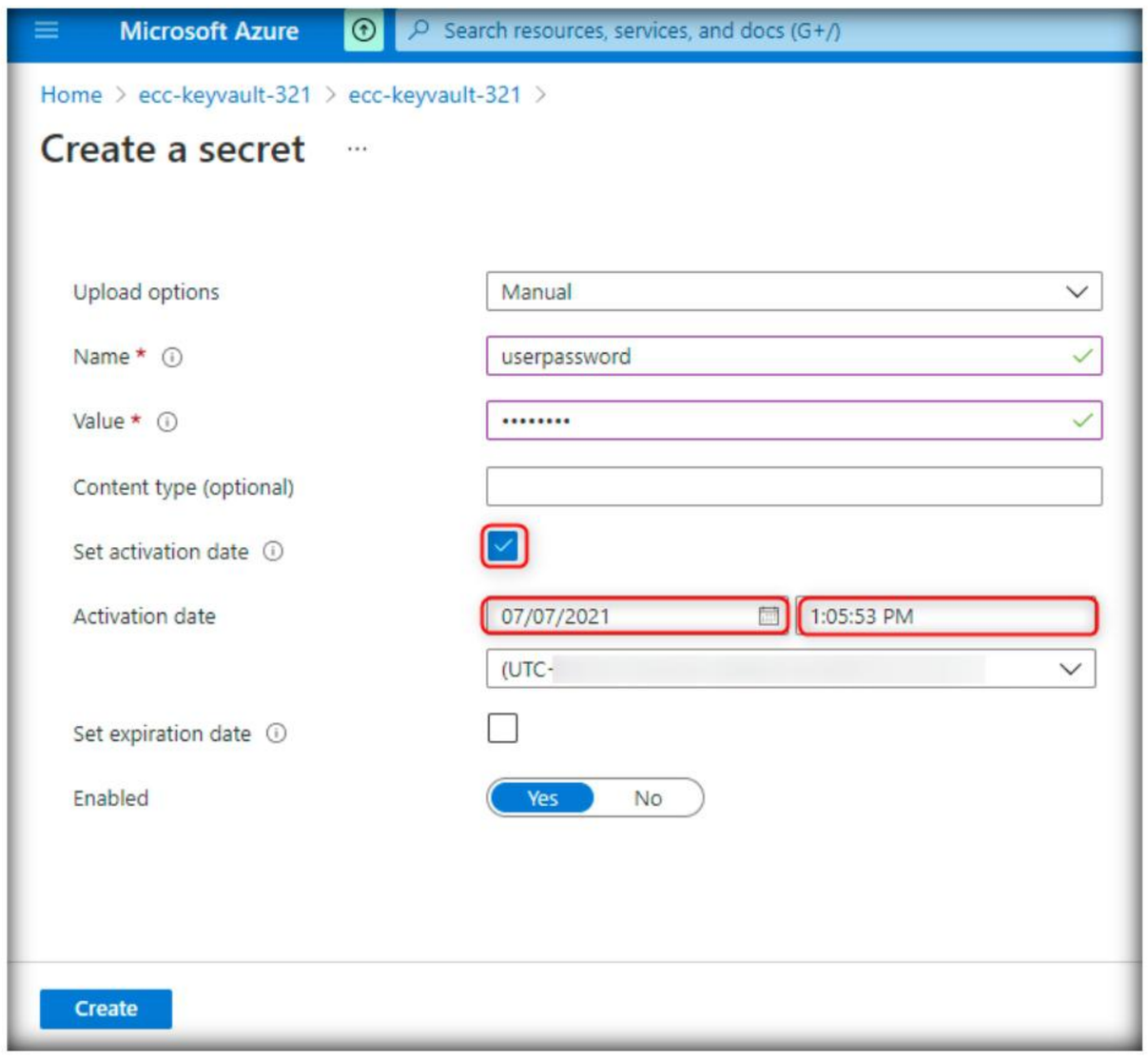


FIGURE 4.11.24: Configuring Activation Date

Certified Cloud Security Engineer Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

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**.

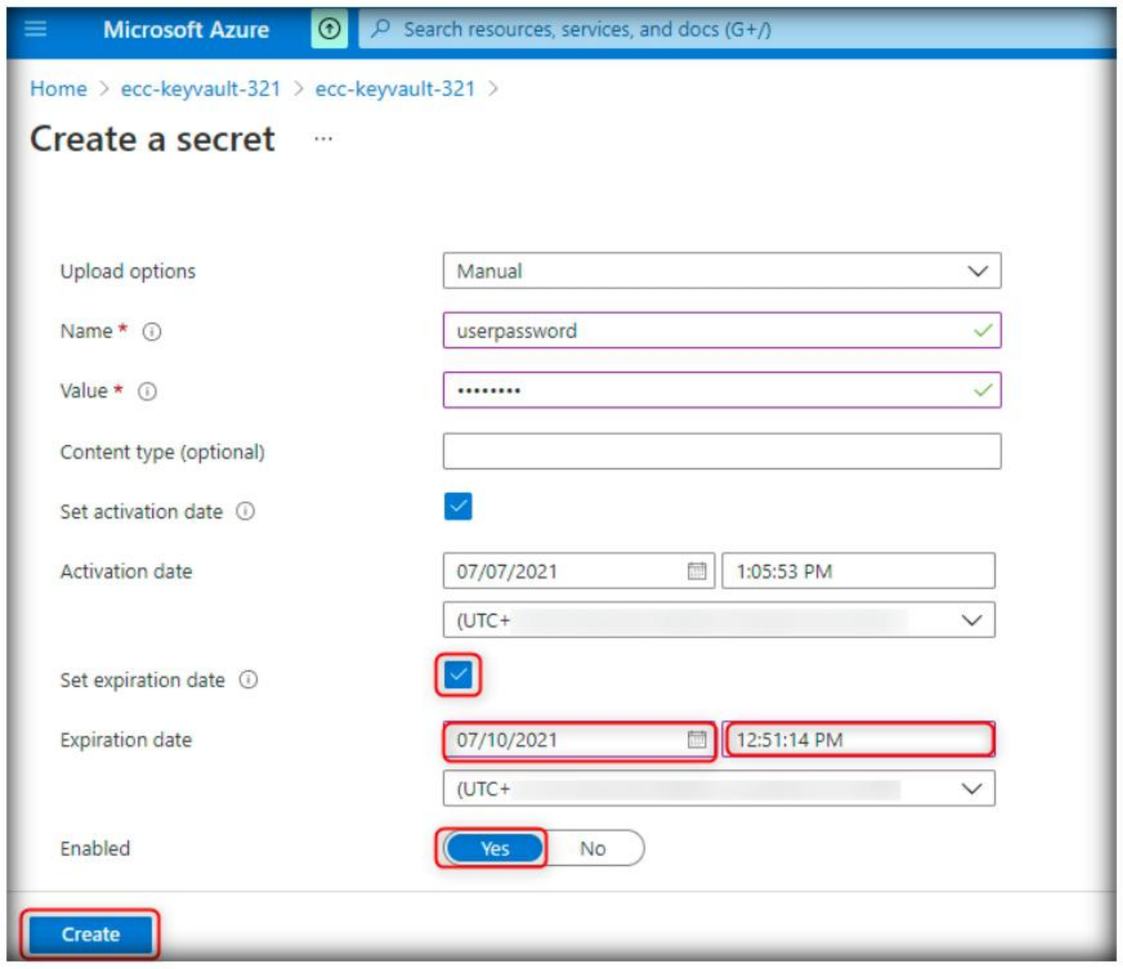


FIGURE 4.11.25: Creating Secret

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

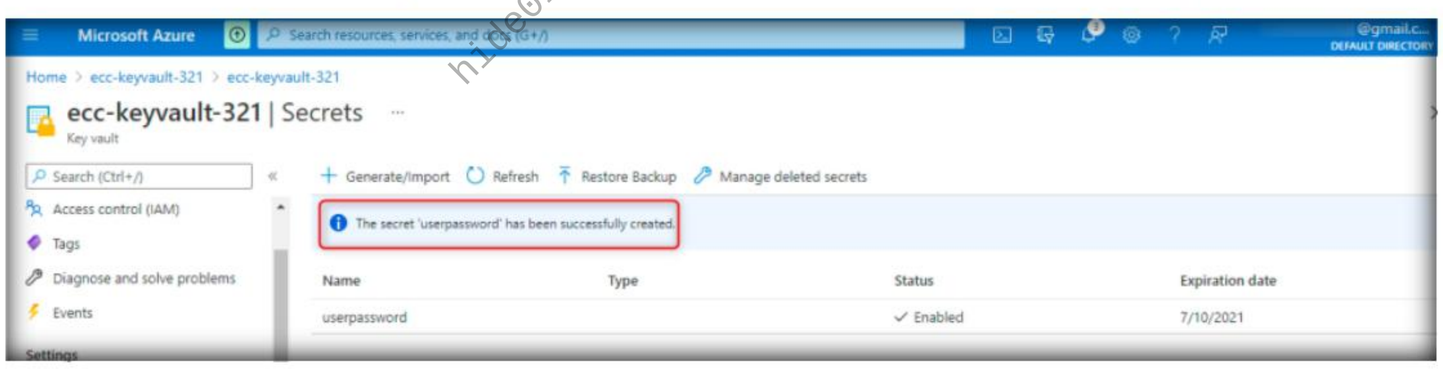


FIGURE 4.11.26: Secret Created Successfully

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.

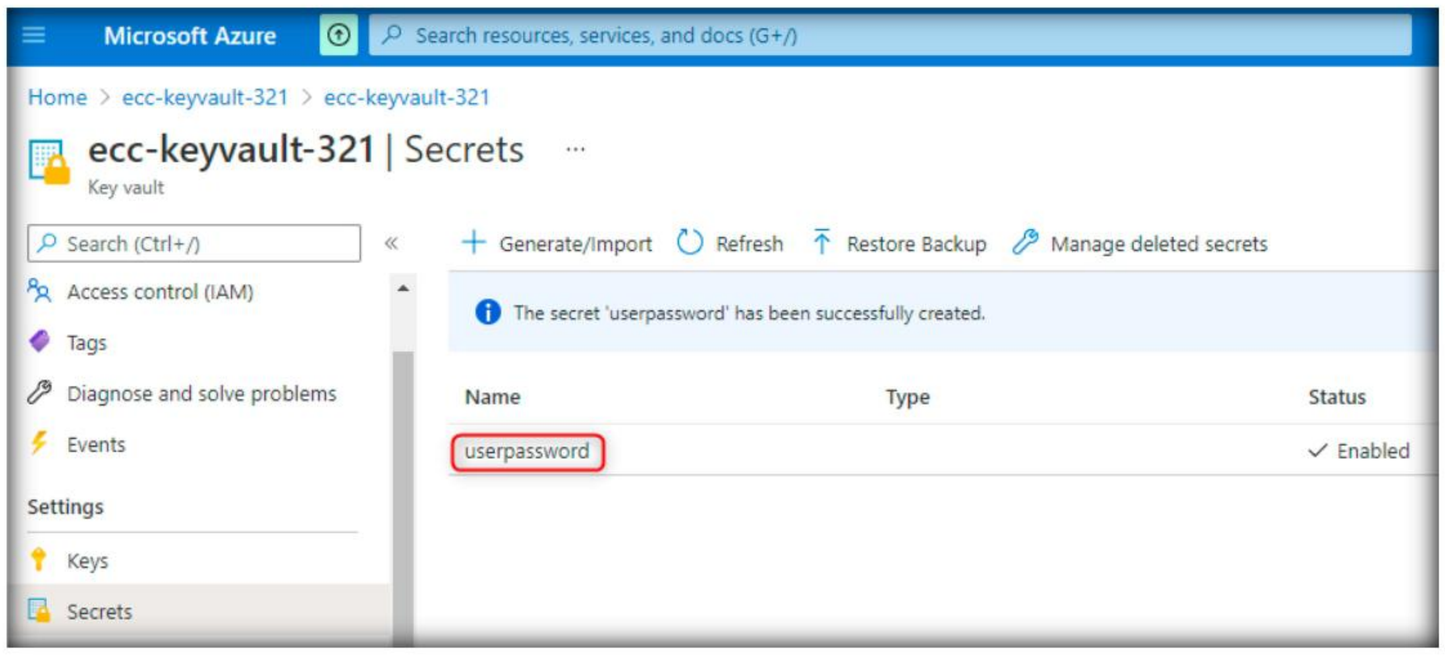


FIGURE 4.11.27: Viewing Secret

Certified Cloud Security Engineer Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

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

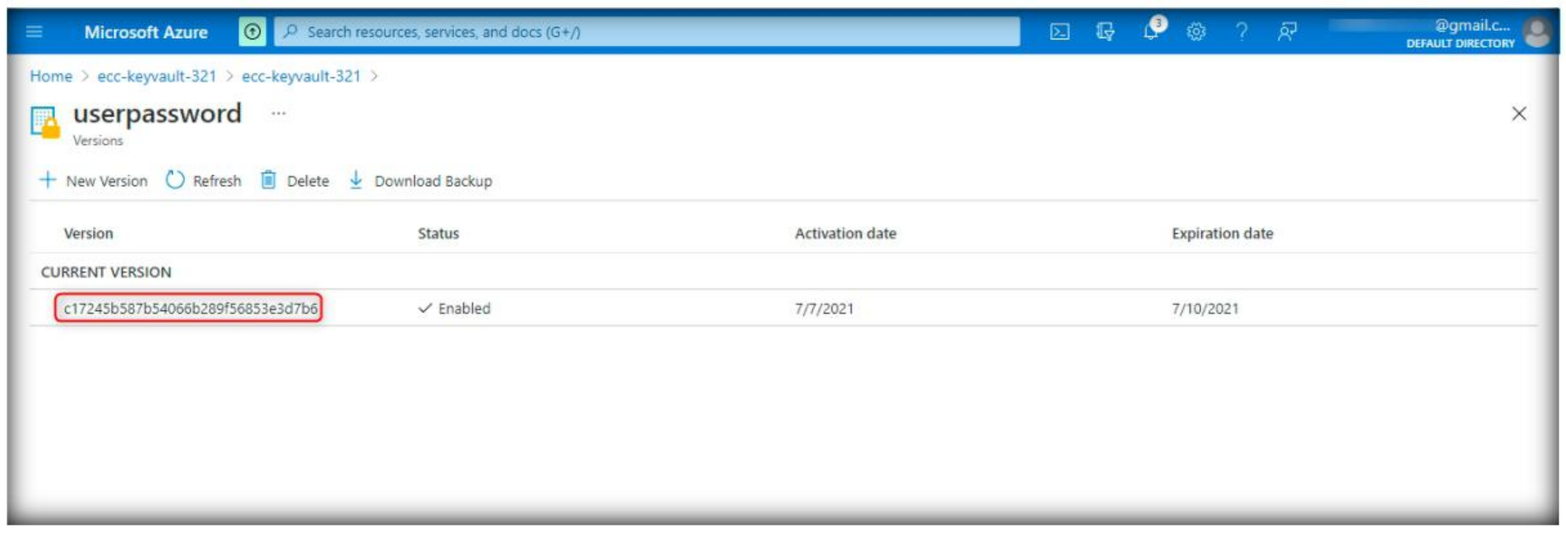


FIGURE 4.11.28: Viewing Secret

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

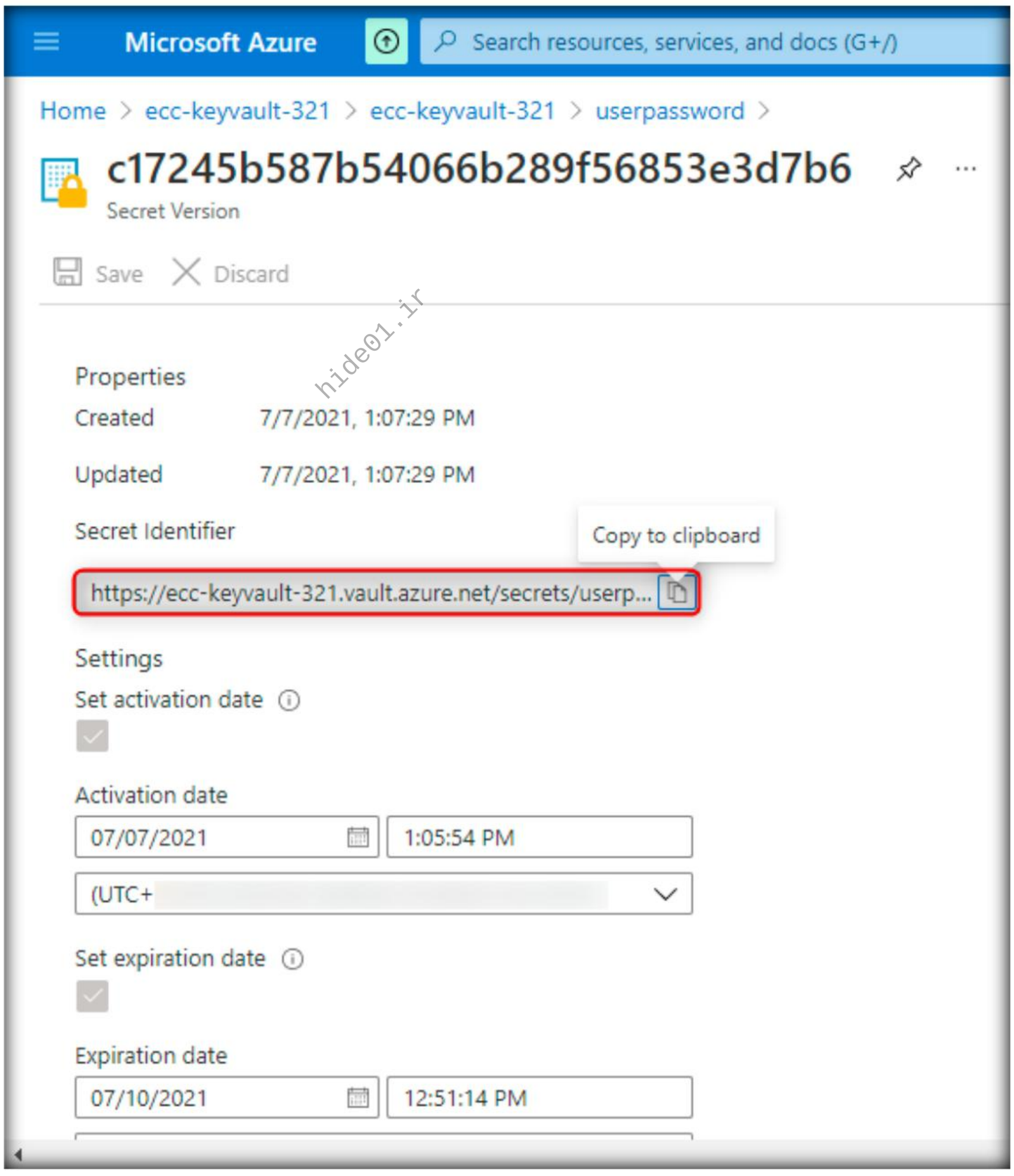


FIGURE 4.11.29: Secret Identifier URI

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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

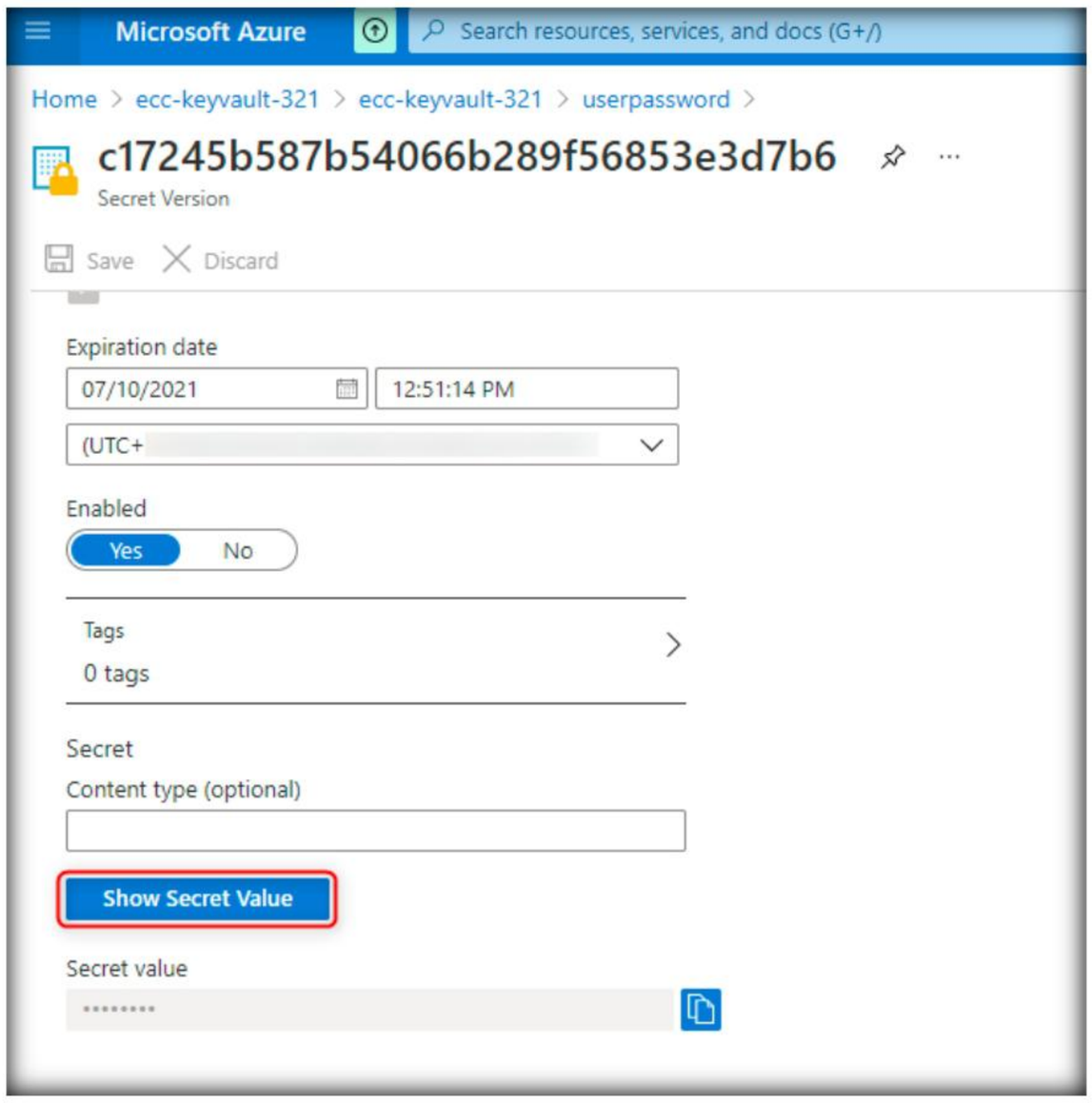


FIGURE 4.11.30: Viewing Secret Value

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

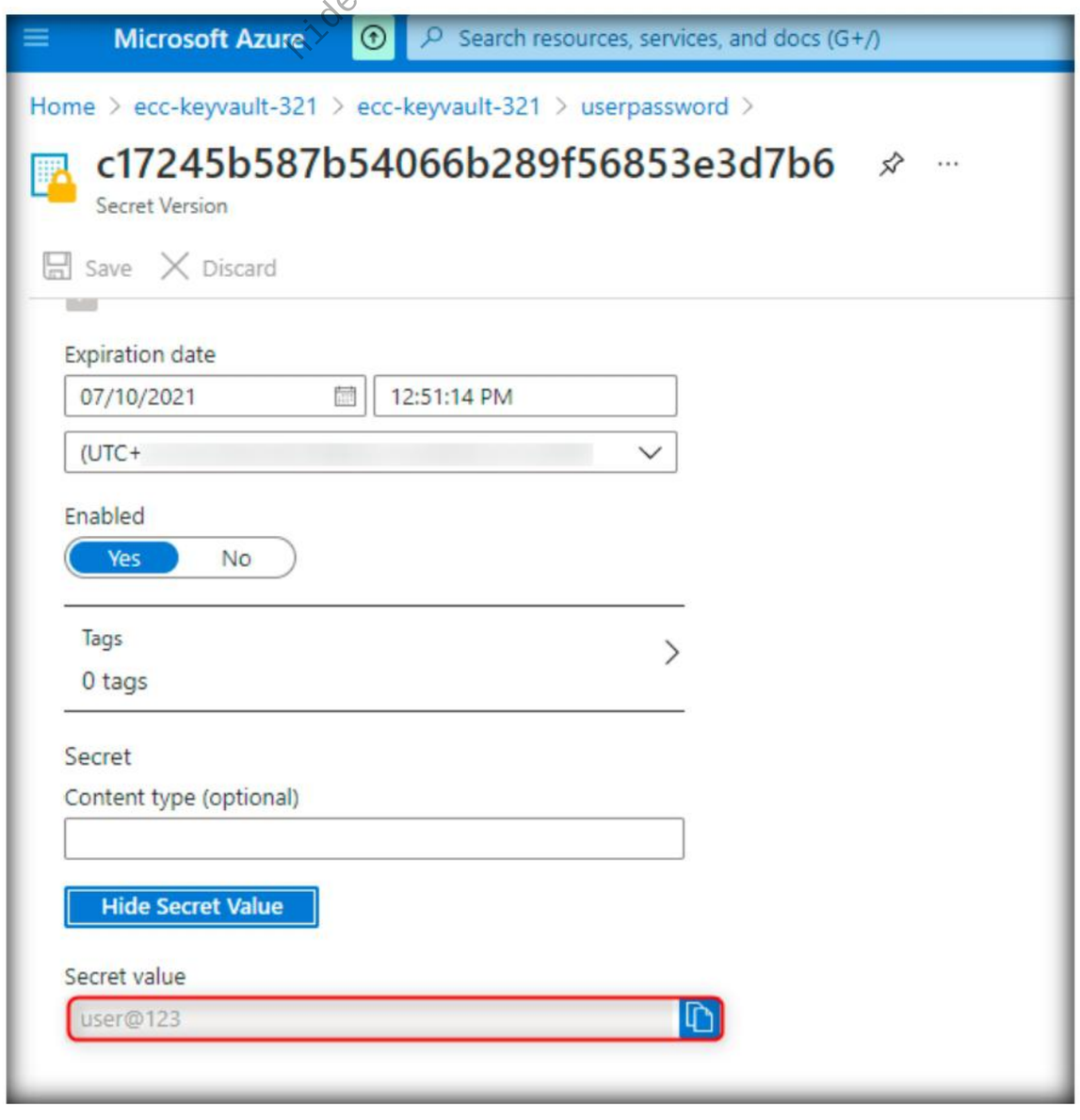


FIGURE 4.11.31: Viewing the Secret

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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

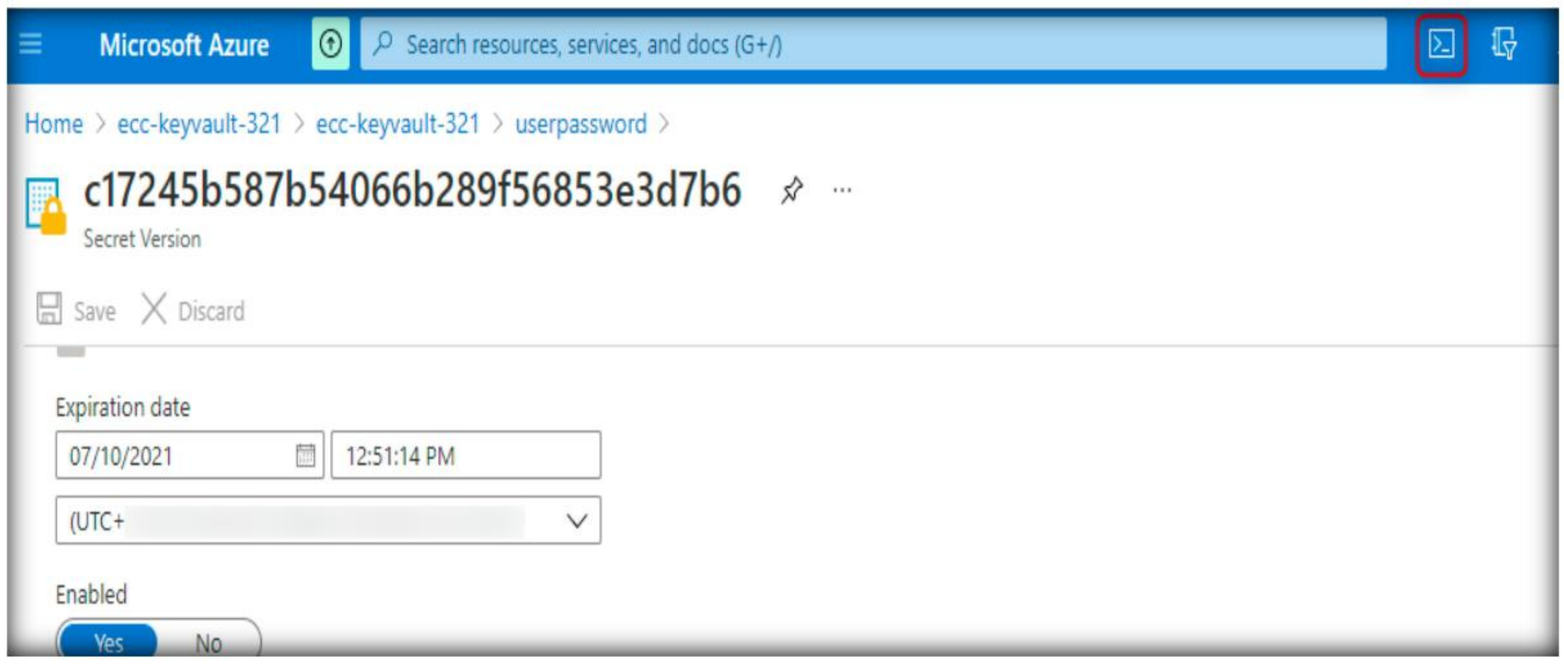


FIGURE 4.11.32: Opening PowerShell

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.

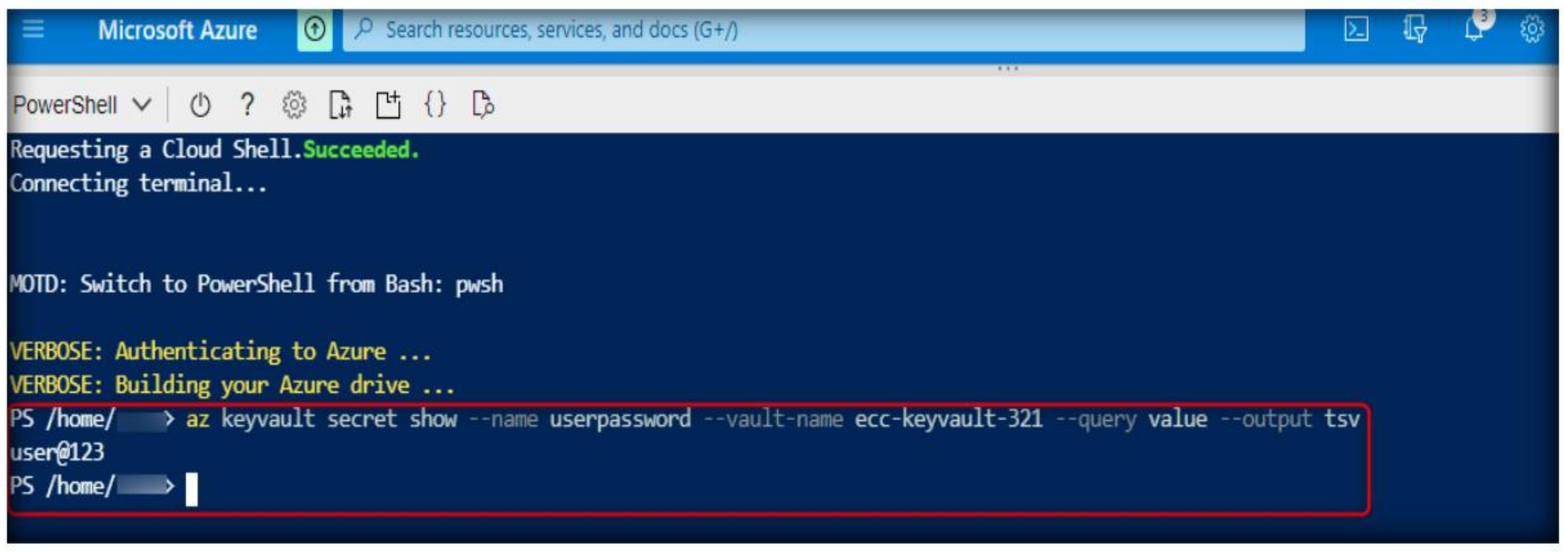


FIGURE 4.11.33: Viewing Secret in PowerShell

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.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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.

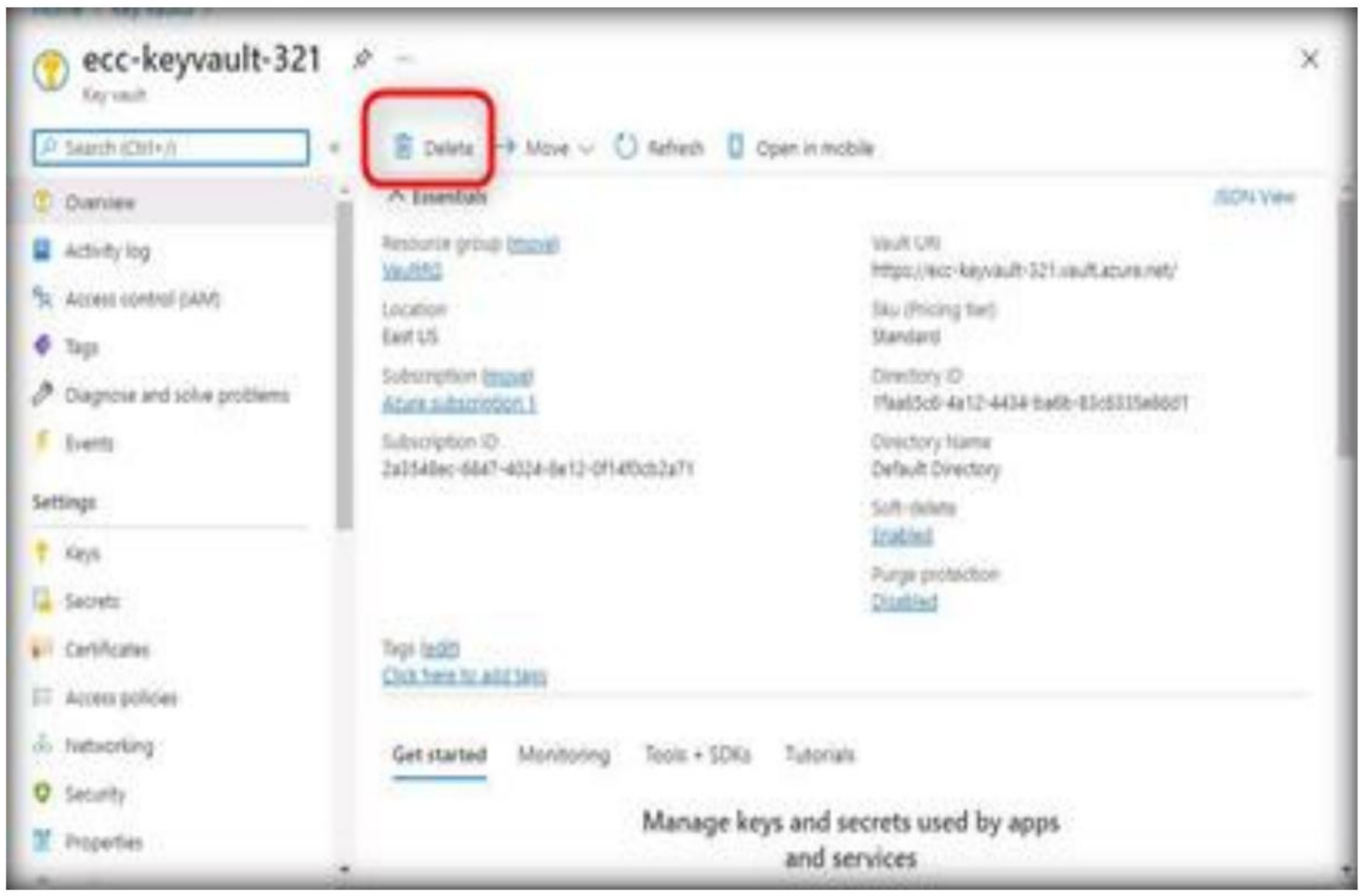


FIGURE 4.11.34: Deleting Key vault

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.

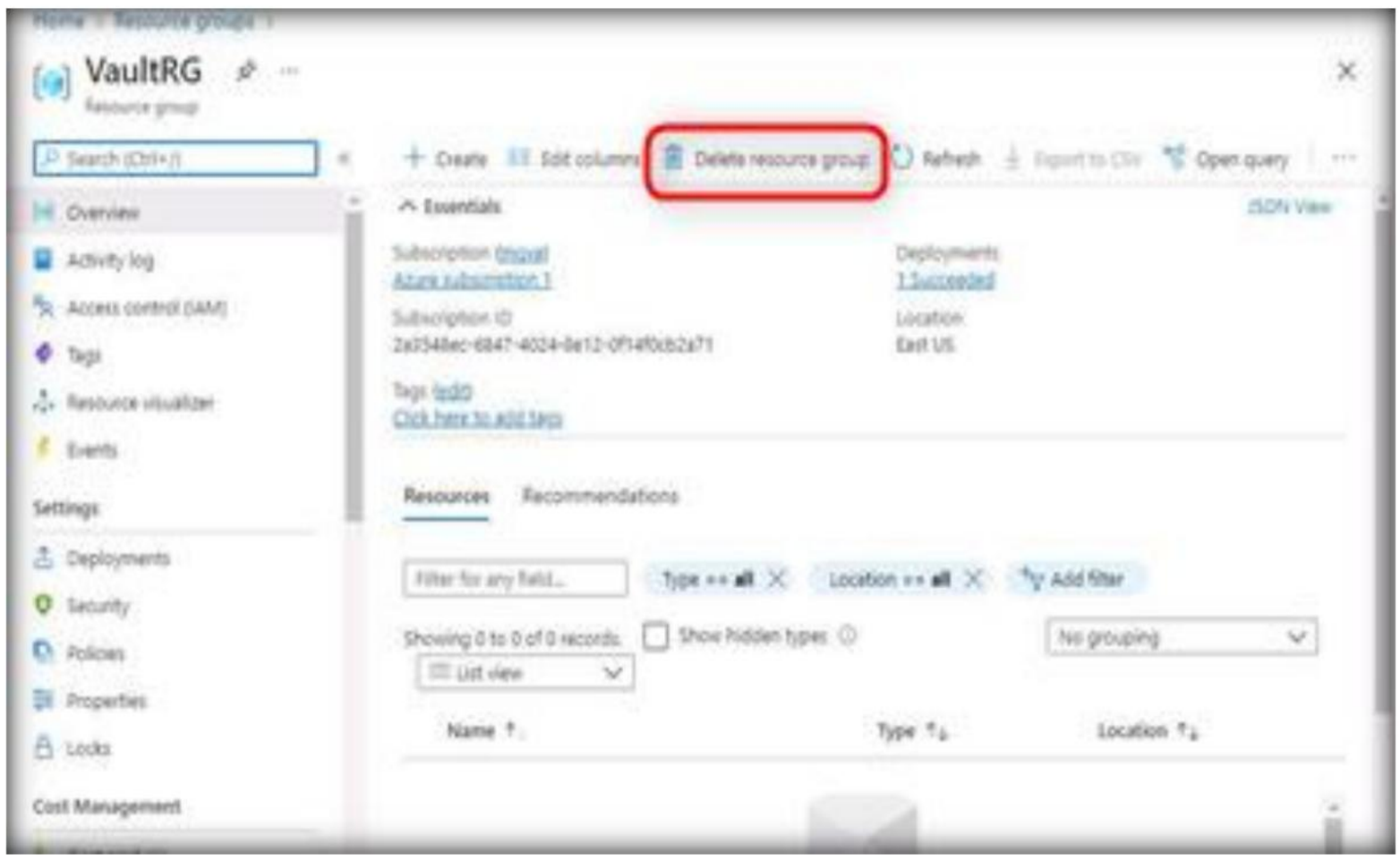


FIGURE 4.11.35: Deleting Resource Group

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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.

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 12

Implementing Encryption and Decryption of Data with Google Cloud KMS

Cloud key management services (KMS) is a centralized key management service that allows cloud security engineers to manage cryptographic keys for cloud operations.

ICON KEY

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

Lab Scenario

Google Cloud KMS is a key management service in cloud that allows cloud security engineers to centrally manage the symmetric and asymmetric cryptographic keys, similar to how an administrator handles such cryptographic keys on-premises. Cloud security professionals can utilize Cloud KMS to create, use, and rotate cryptographic keys. Sensitive data can be encrypted and decrypted using these cryptographic keys. Key rotation can also be performed for symmetric keys to ensure the same key version is not used repeatedly.

Lab Objectives

This lab will demonstrate how to encrypt data and then decrypt it using the symmetric keys created with Cloud KMS.

In this lab, you will learn to do the following:

- Create symmetric key rings and keys
- Encrypt data
- Decrypt data
- Rotate the cryptographic keys

Lab Environment

To perform this lab, you need the following:

- **Admin Machine** VM

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Administrative** privileges
- Registered GCP account

Lab Duration

Time: 20 minutes

Overview of Cloud Key Management Services

Cloud KMS is a centralized key management service. GCP KMS can manage symmetric and asymmetric keys for the cloud services, and it allows cloud security engineers to generate, use, rotate, and destroy cryptographic keys such as RSA 2048, RSA 3072, RSA 4096, AES 256, EC P256, and EC P384. Cloud KMS allows an administrator to manage and monitor permissions on individual keys. Cloud KMS protects data corruption and ensures a successful decryption using periodical scans and backups of the keys and their metadata. KMS also ensures protection against unauthorized key access and can be integrated with IAM and Cloud audit logs. Cloud KMS also helps cloud security engineers setup key rotation to prevent brute-force attacks.

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., GCP), the application interface may be updated with time. Hence, in case you happen to work on an updated version of GCP, 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 GCP Free Trial account using the following link: https://cloud.google.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 GCP account but be aware that it may incur significant charges to your account.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1

Creating Symmetric Key Rings and Keys

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

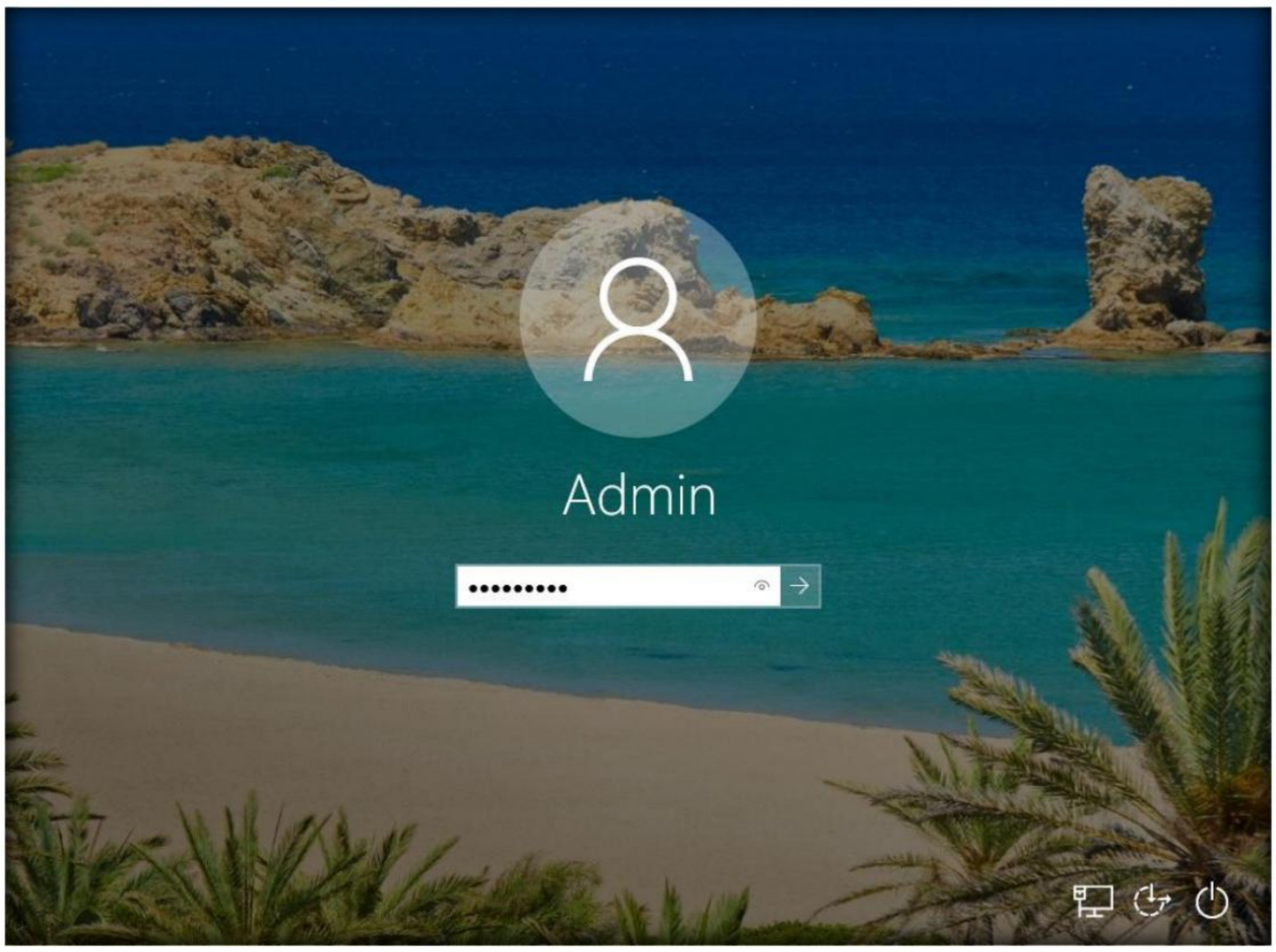


FIGURE 4.12.1: Launch Admin Machine and Log in

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

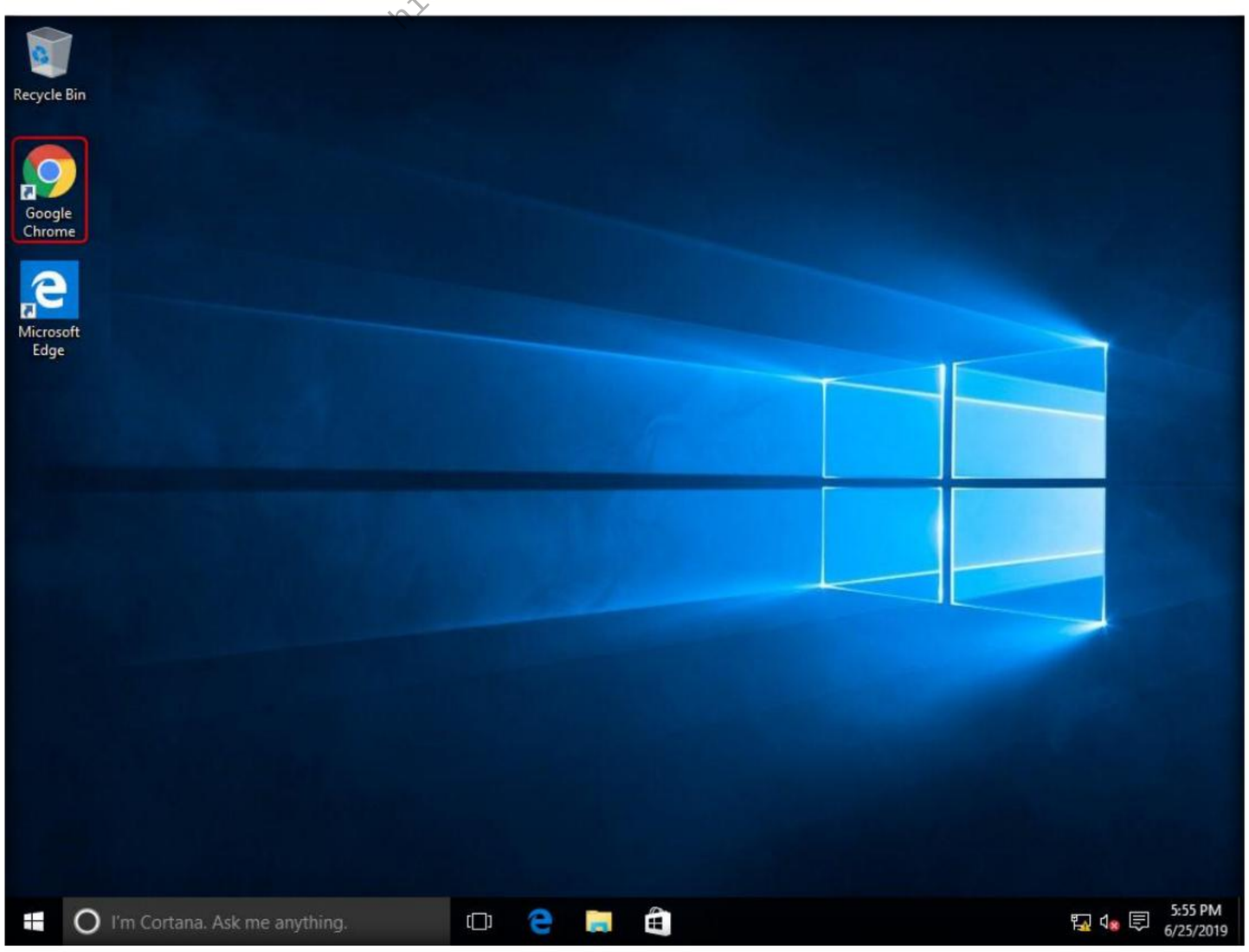


FIGURE 4.12.2: Navigating to the Chrome Browser from Taskbar

Certified Cloud Security Engineer Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

3. The **Google Chrome** browser opens. Go to the address bar, type **https://console.cloud.google.com/**, and press **Enter**.

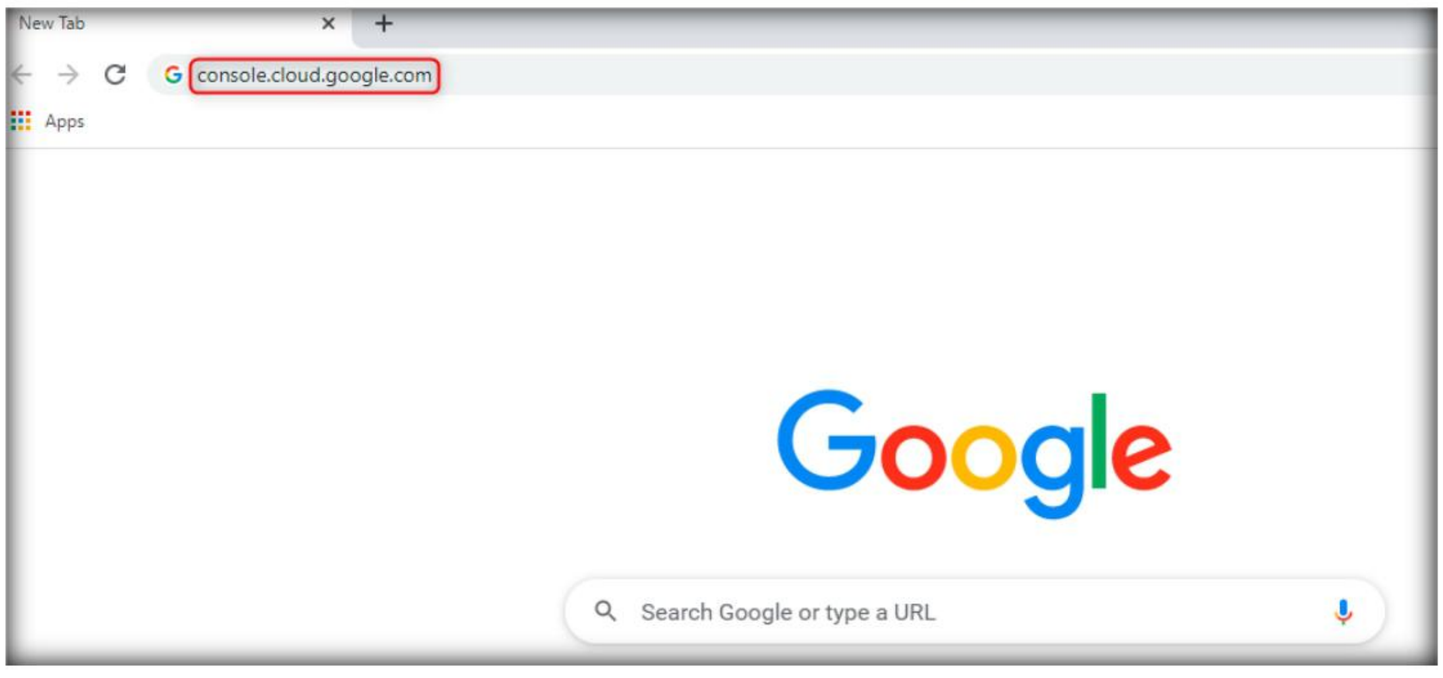


FIGURE 4.12.3: Accessing GCP console from Google chrome

4. Enter the **Email address** to sign into Google Cloud Platform and click **Next**.

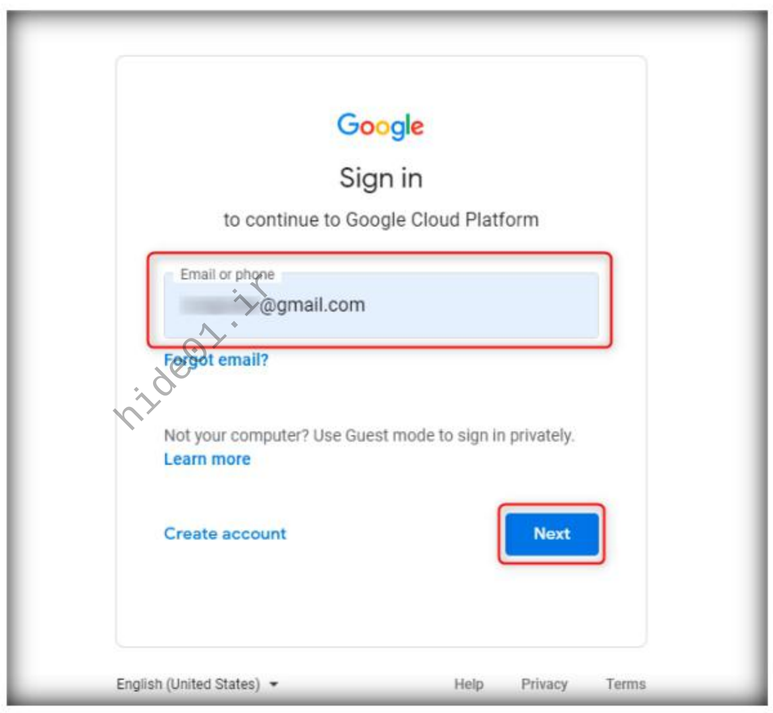


FIGURE 4.12.4: Entering the email address

5. Enter the **password** and click on **Next**.

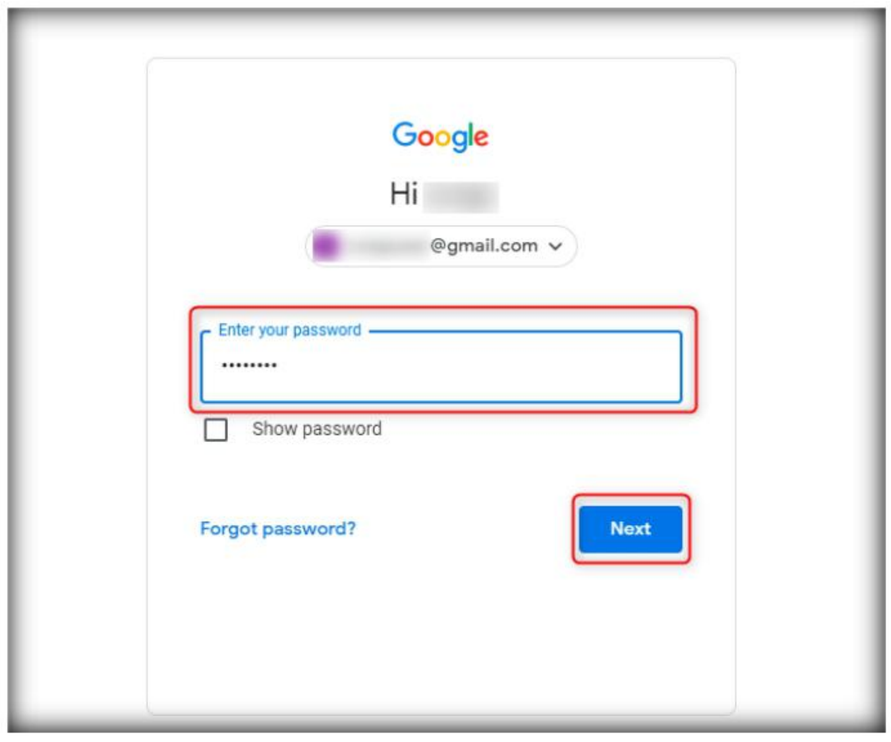


FIGURE 4.12.5: Signing into the console

Certified Cloud Security Engineer Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

6. On top left corner, you will have a dropdown. If **My First Project** is the default selected project, then skip **Steps 7–16** and execute **Step 17**.

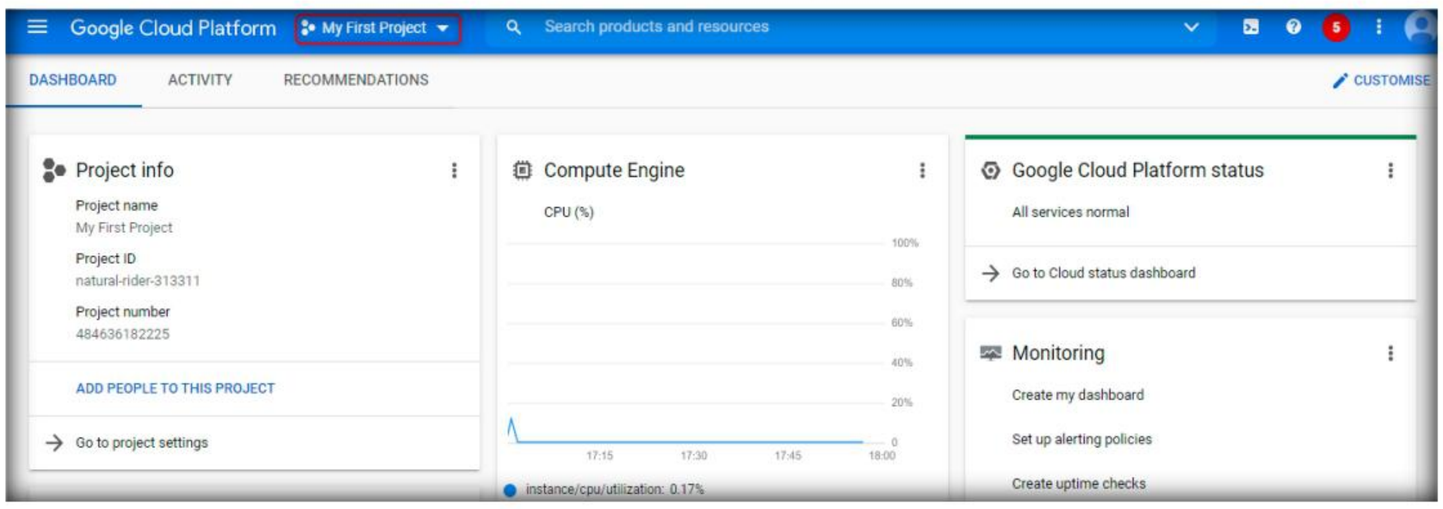
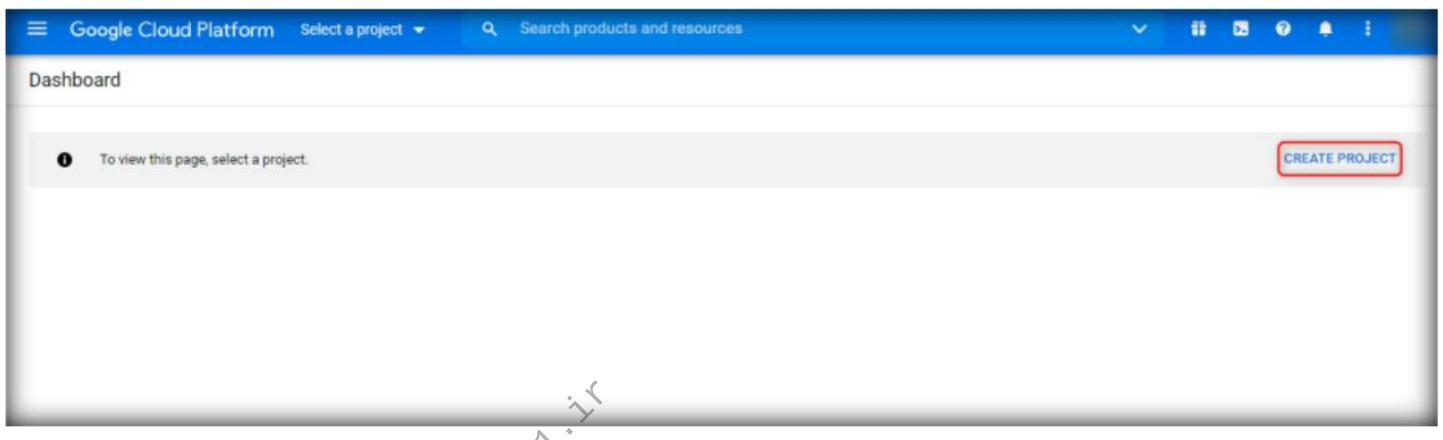


FIGURE 4.12.6: Create new Project

7. In the dropdown on the top left corner, if you see **Select a Project** with an empty dashboard, then click on **CREATE PROJECT** to create a new project.



hide01.ir

FIGURE 4.12.7: Creating Project

8. In the **New Project** window that opens, type **My First Project** as the **Project name**. Then, click on **CREATE**.

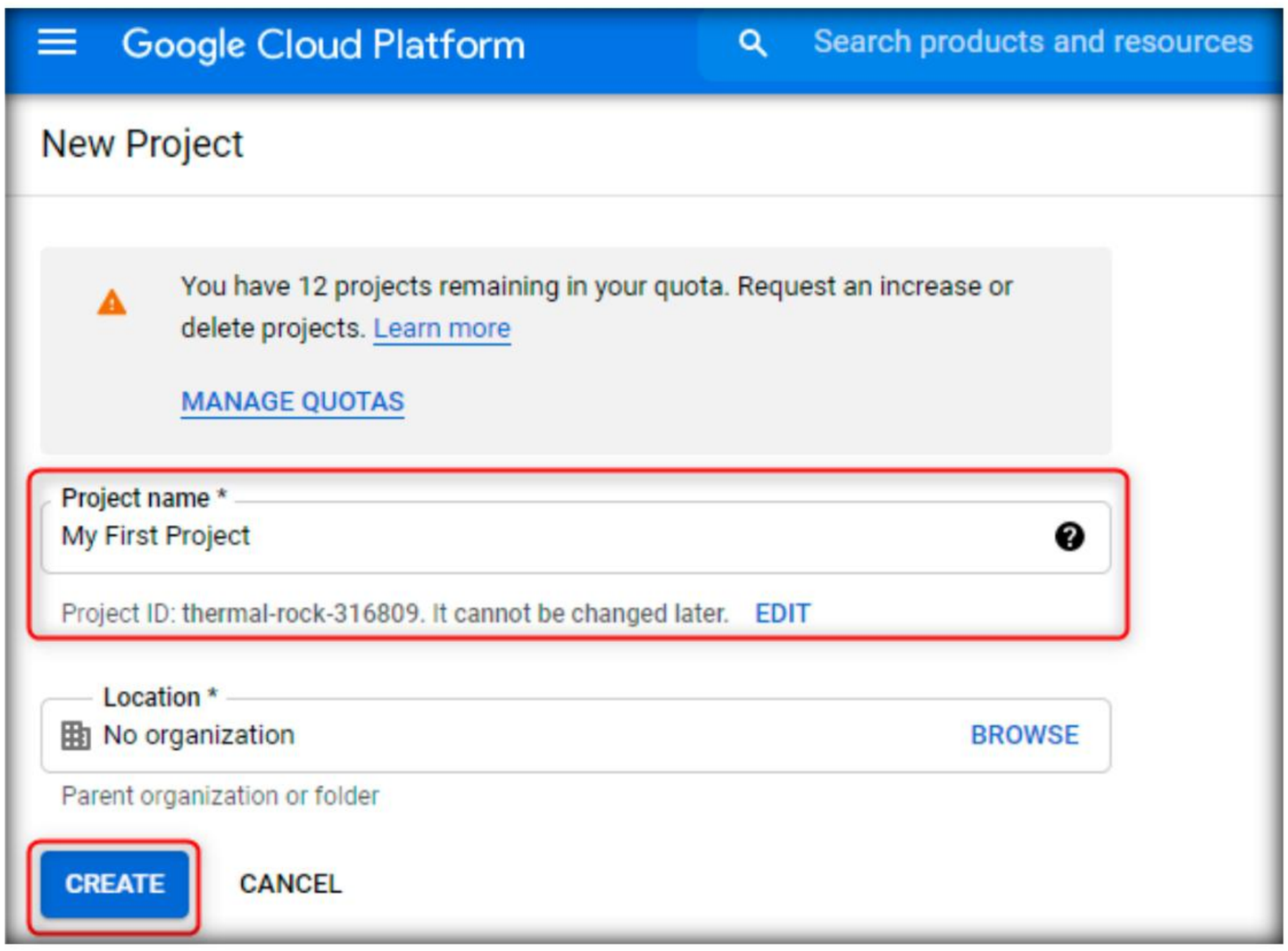


FIGURE 4.12.8: Configuring New Project

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

9. Your project will be successfully created. You will see that in the top of the window, **My New Project** will be selected by default as the current project.

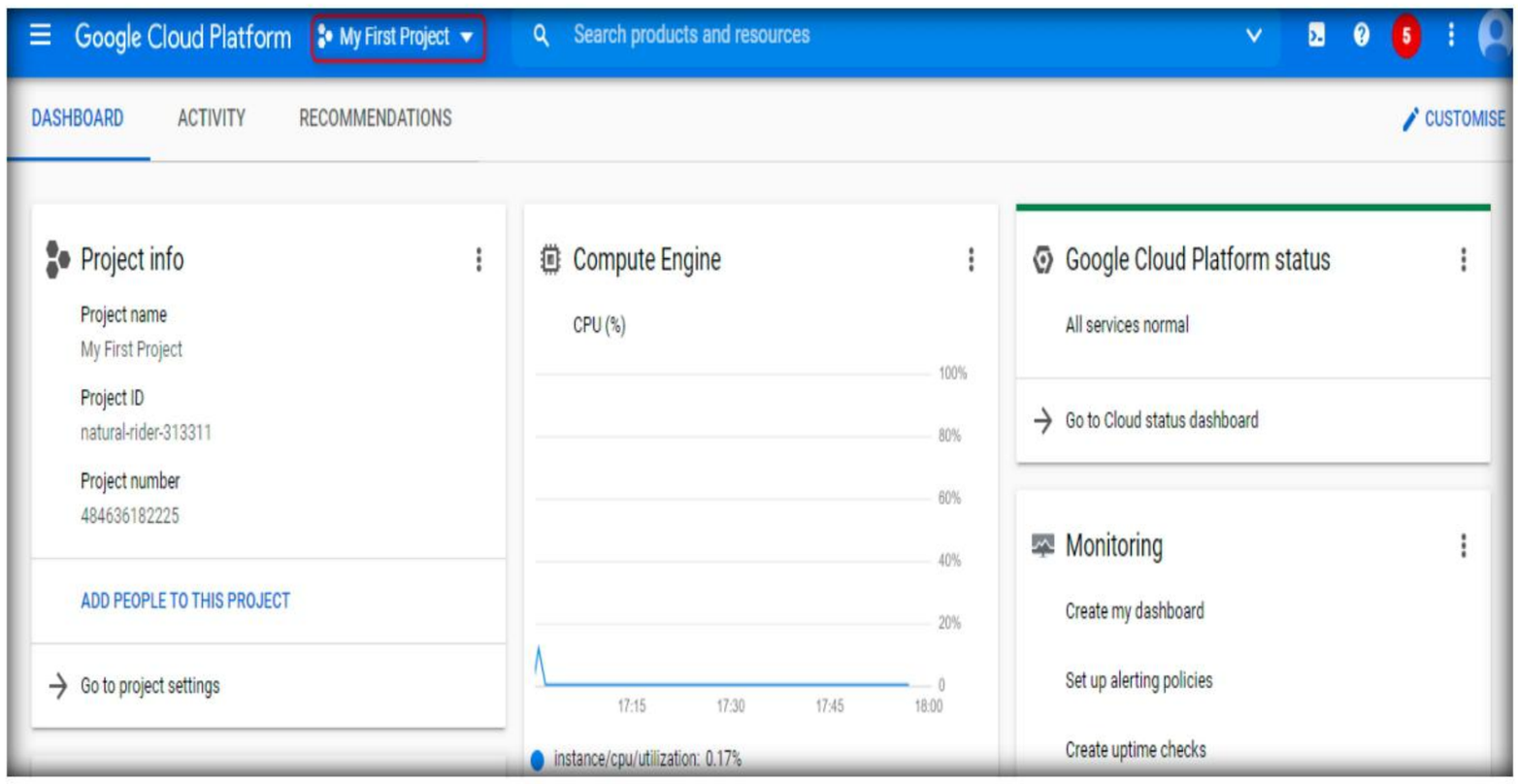


FIGURE 4.12.9: My First Project Selected as Default

10. On the top left corner, if the dropdown displays a different project other than **My First Project** by default, then click on the dropdown.

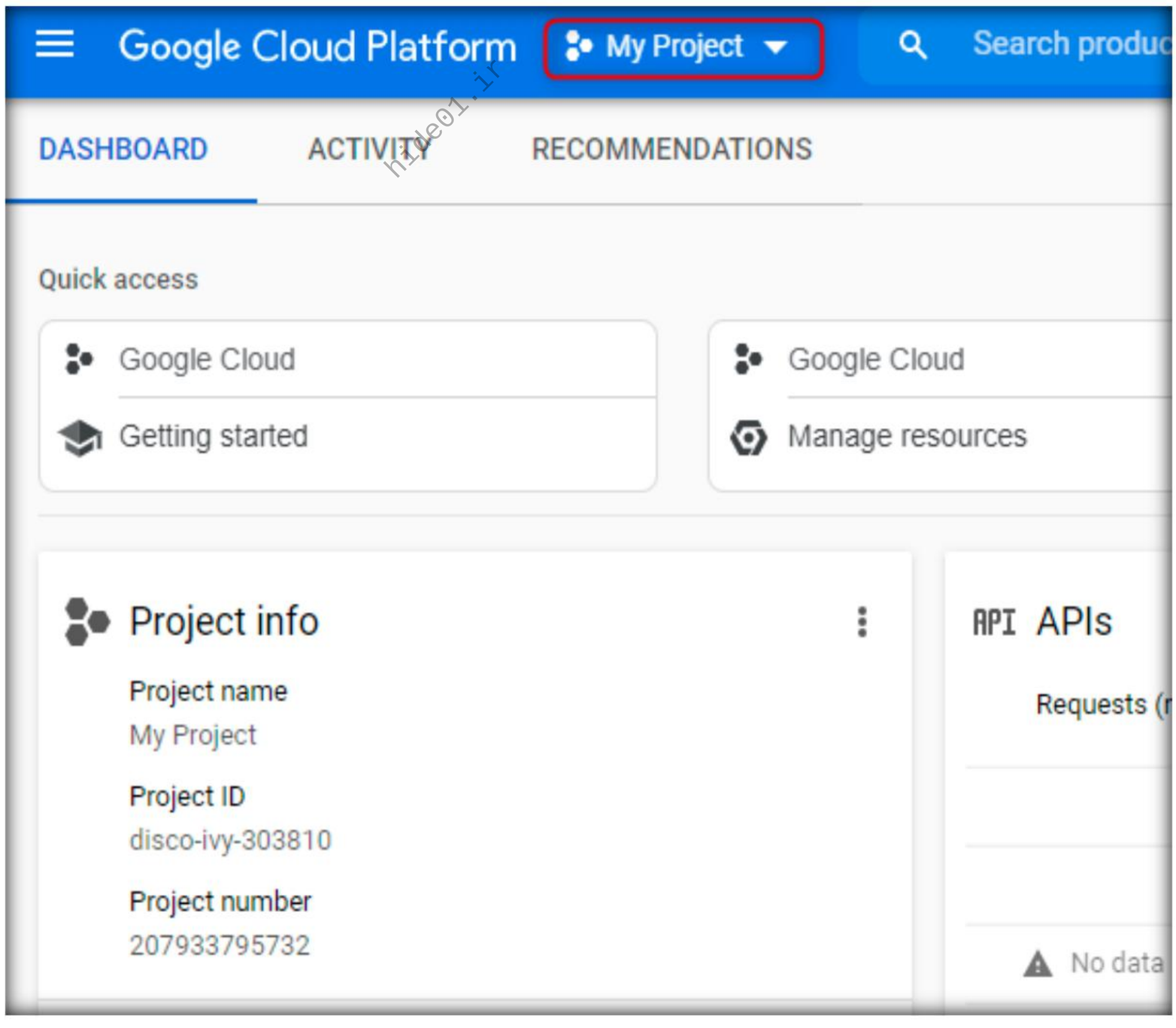


FIGURE 4.12.10: Selecting Project Dropdown

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

11. A **Select a project** window opens, which displays all existing projects. It provides a **Search projects and folders** option to search for an existing project. Select **My First Project** from the displayed list of existing projects.

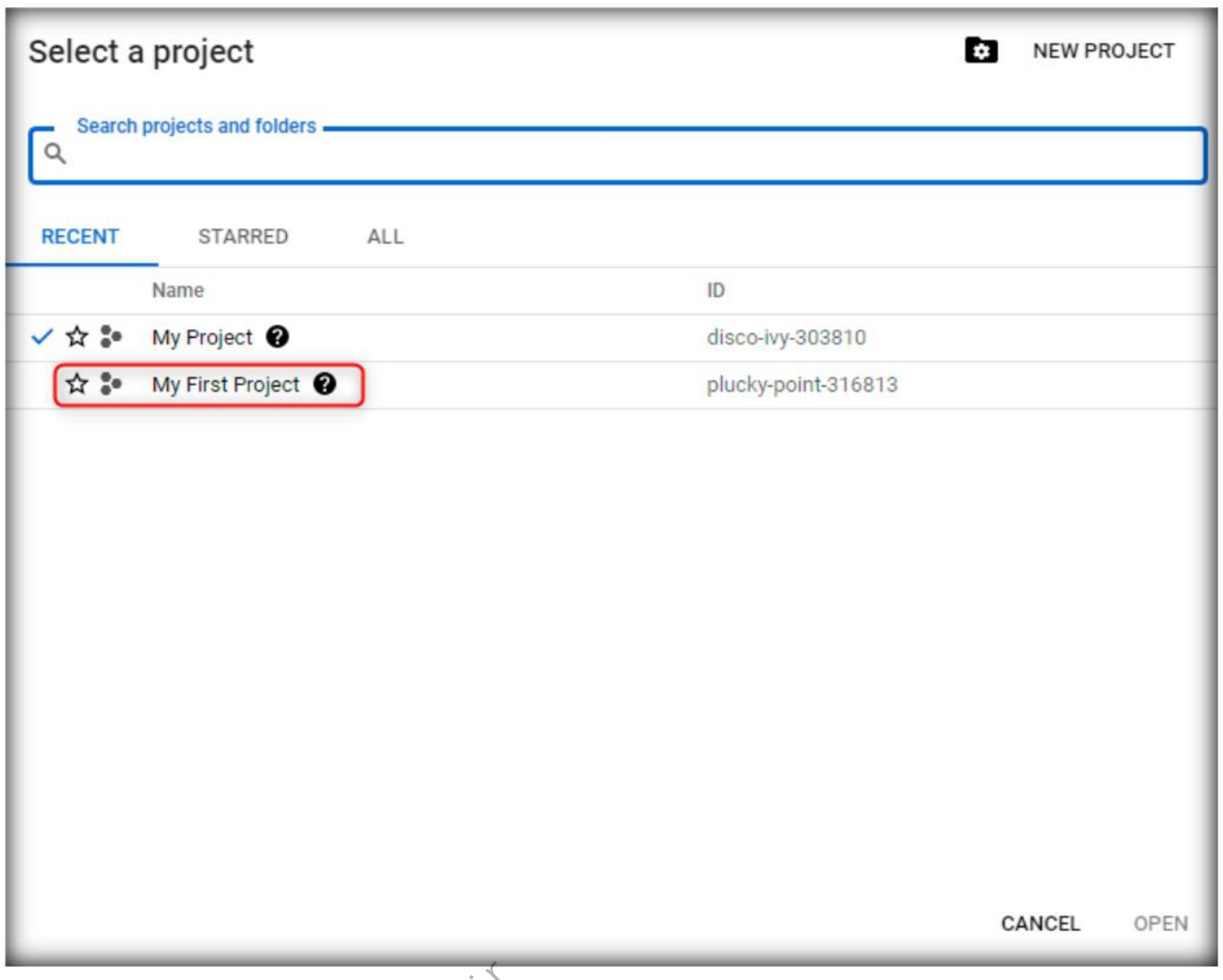


FIGURE 4.12.11: Selecting My First Project

12. Now, if **My New Project** is not in the list, click on **NEW PROJECT** to create a new project named **My First Project**.

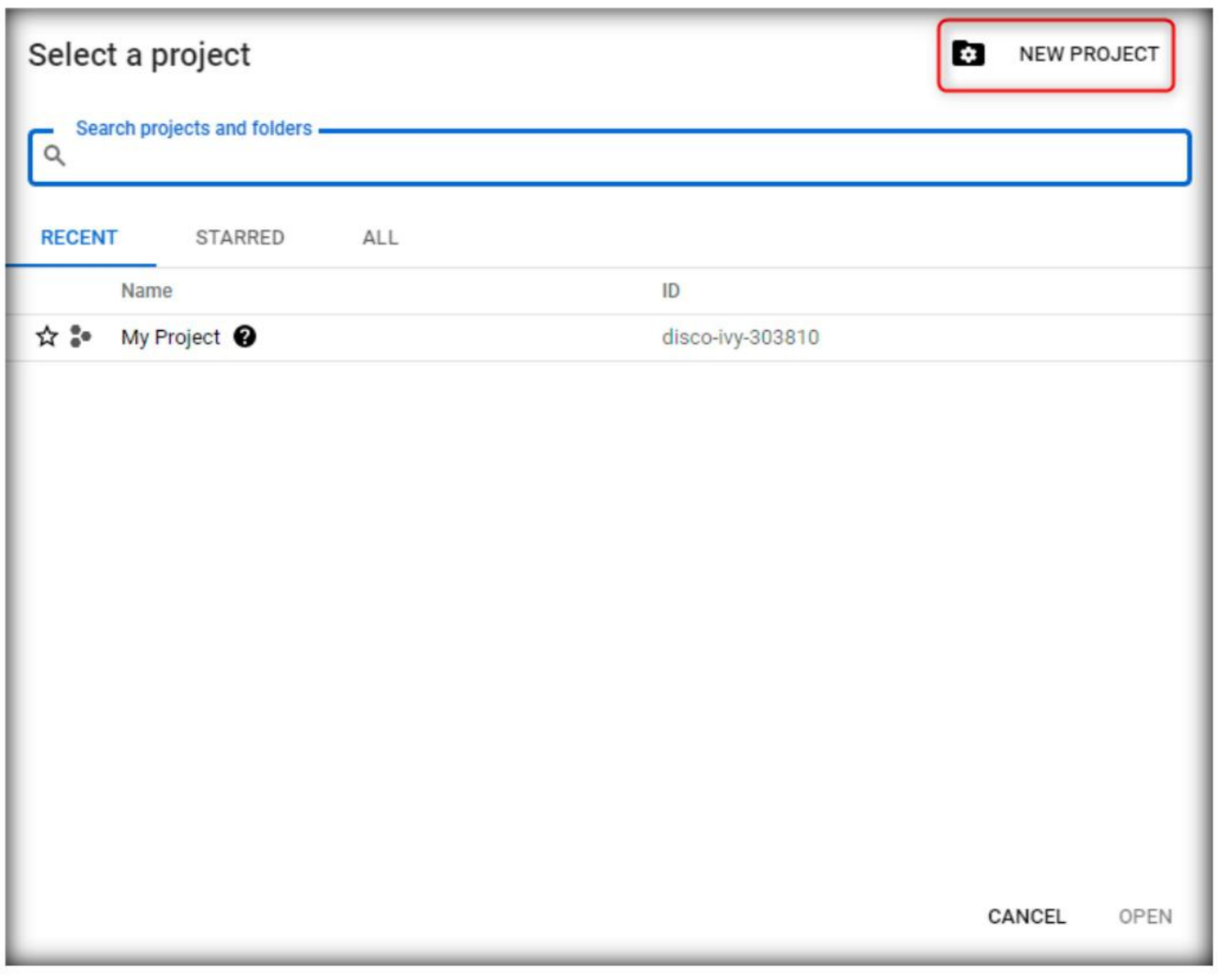


FIGURE 4.12.12: Creating New Project

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

13. The **New project** window opens. Type the **Name** of the project as **My First Project** and click on **CREATE,** as shown in the screenshot below.

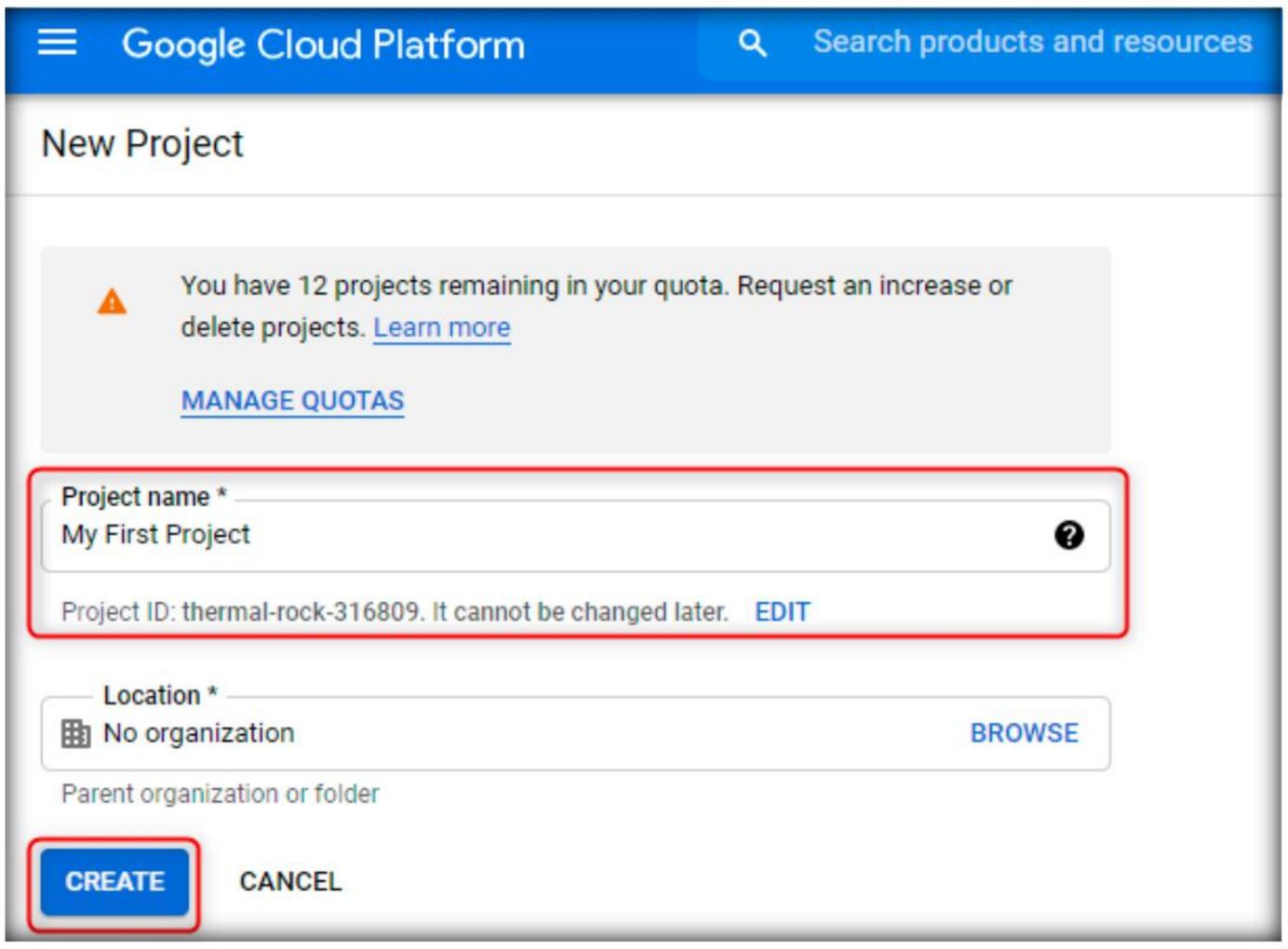


FIGURE 4.12.13: Creating My First Project

14. A new project named **My First Project** will be created. Next, you need to select **My First Project** as the default project. Now, click on the project dropdown at the top left corner.

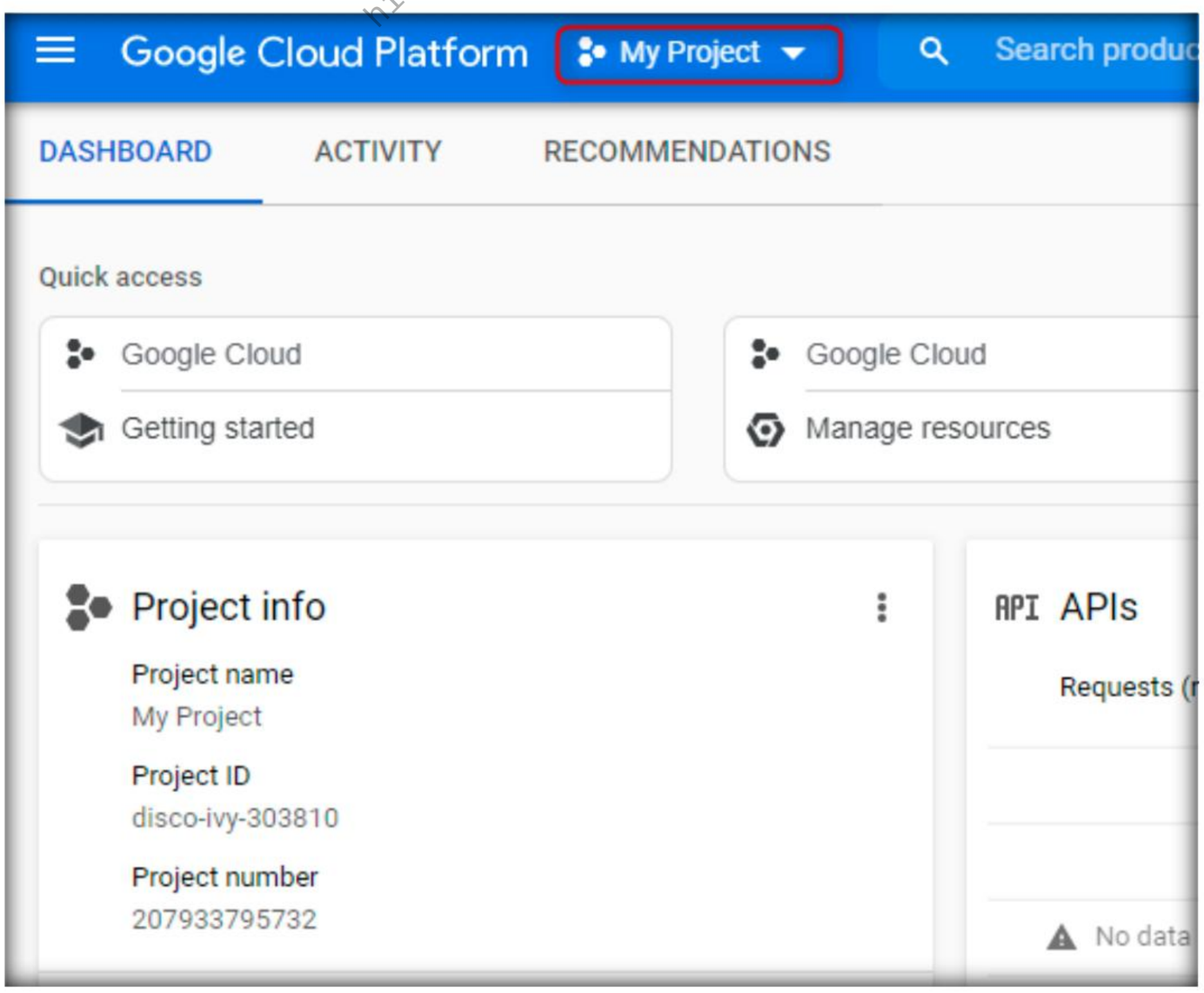


FIGURE 4.12.14: Selecting Project Dropdown

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

15. Select **My First Project** from the list of projects.

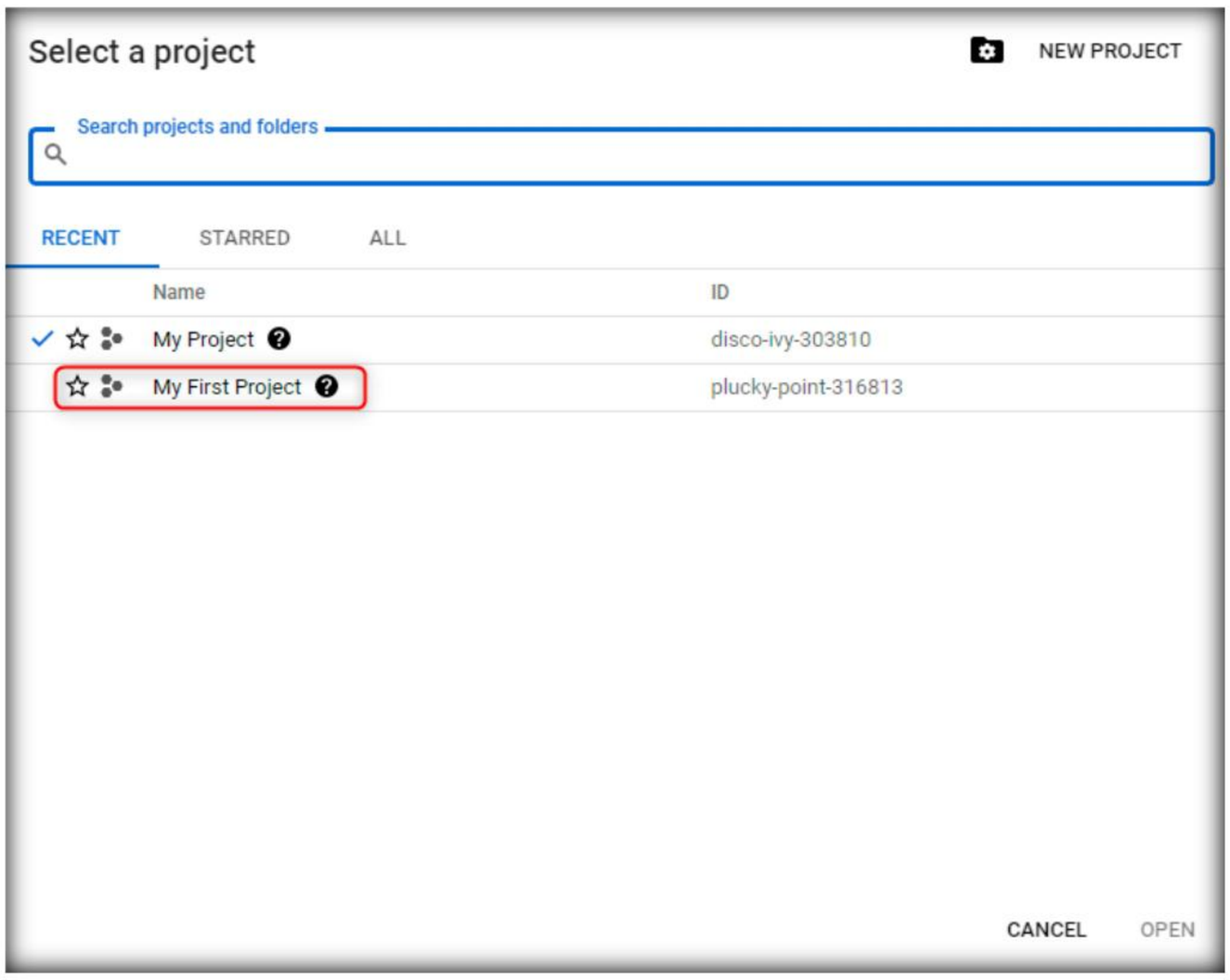


FIGURE 4.12.15: Selecting My First Project

16. **My First Project** will be selected as the default project.
17. After selecting the project, navigate to **Security** and select **Cryptographic Keys** in the console.

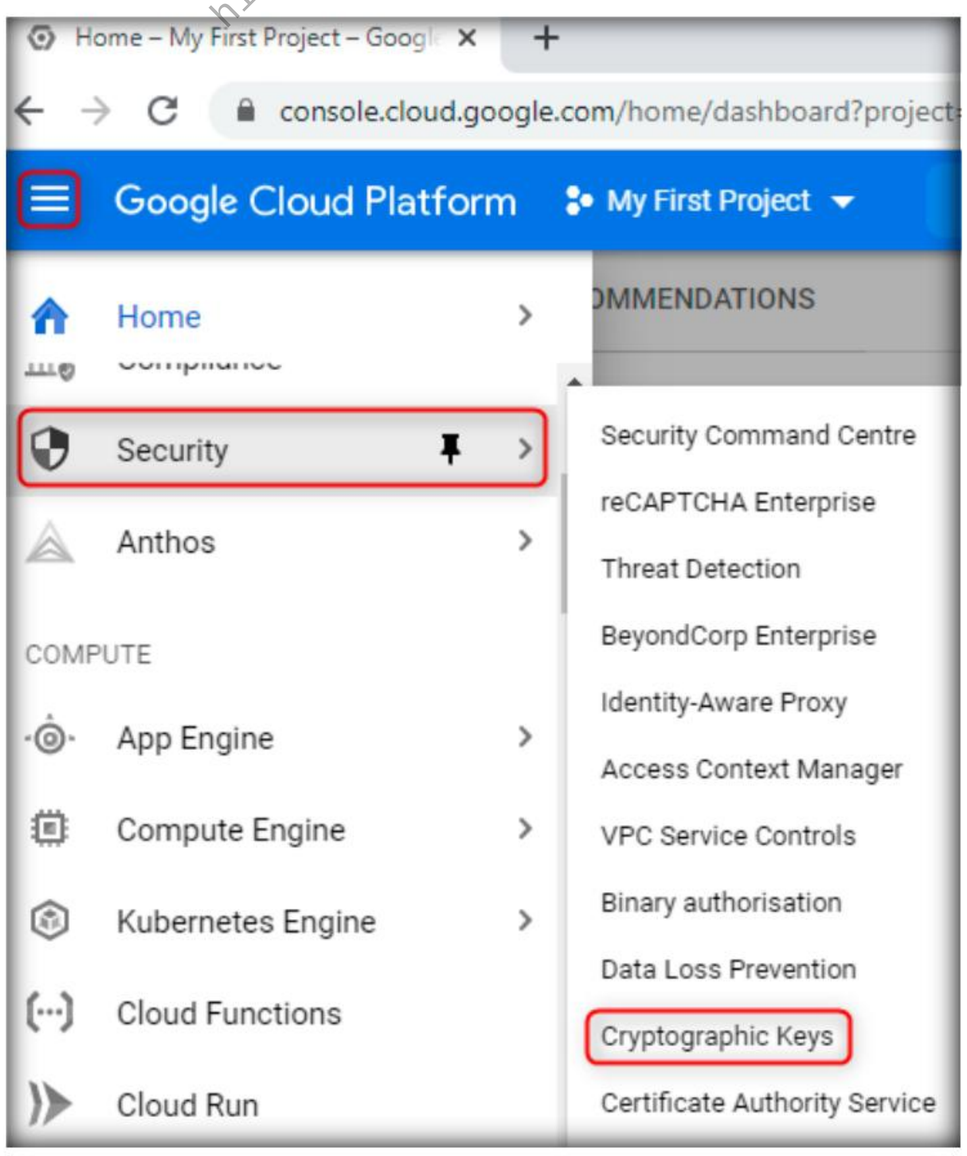


FIGURE 4.12.16: Navigate to Cryptographic Keys in console

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

18. Now, you will create symmetric key rings and keys. If you are creating a key for the first time, you will need to enable the **Cloud Key Management Service (KMS) API**. To do this, click on **ENABLE**. Wait for it to be enabled.

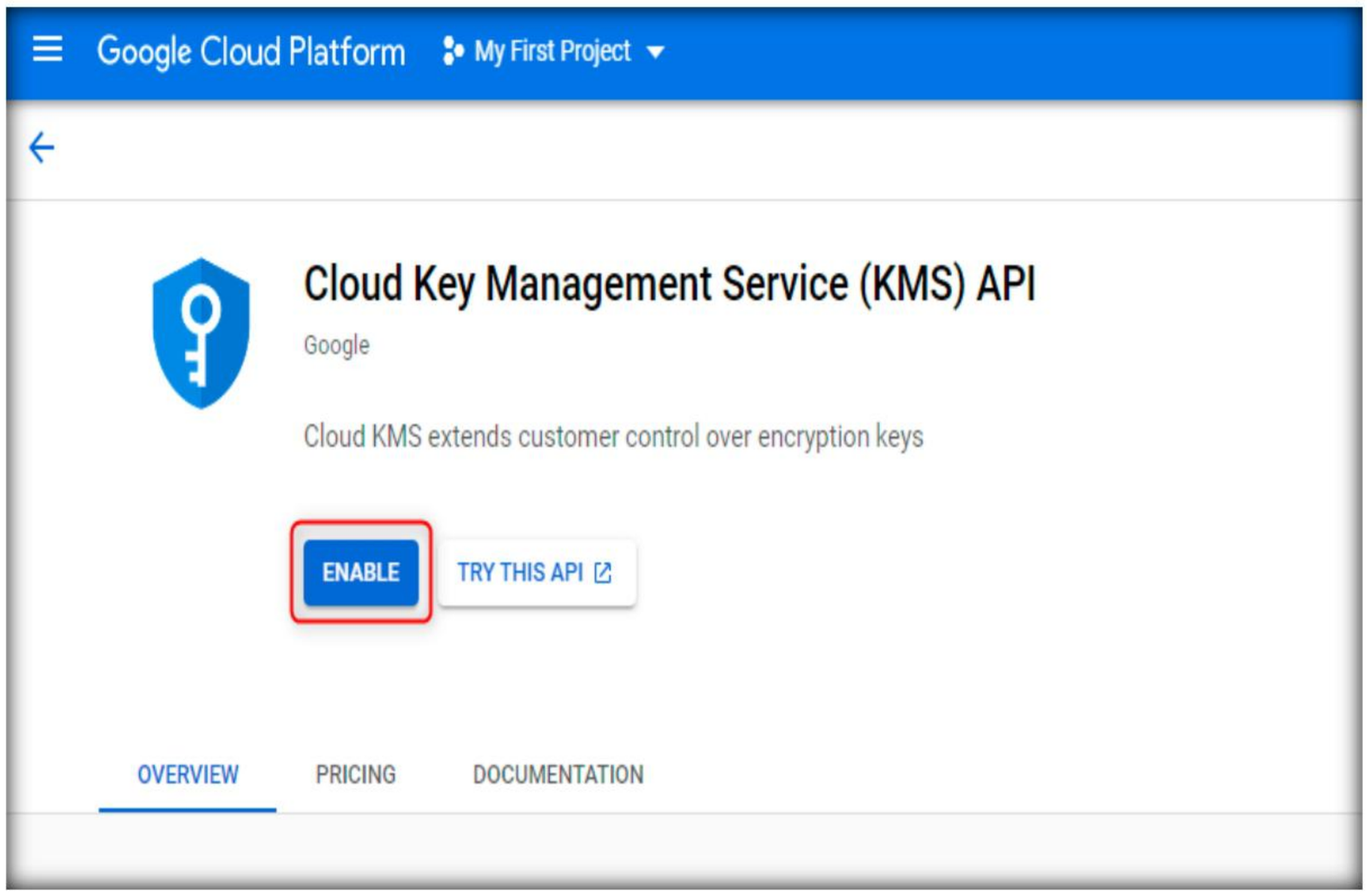


FIGURE 4.12.17: Enabling Cloud KMS

19. After the Cloud KMS services is enabled, click on **CREATE KEY RING** to create your first key ring.

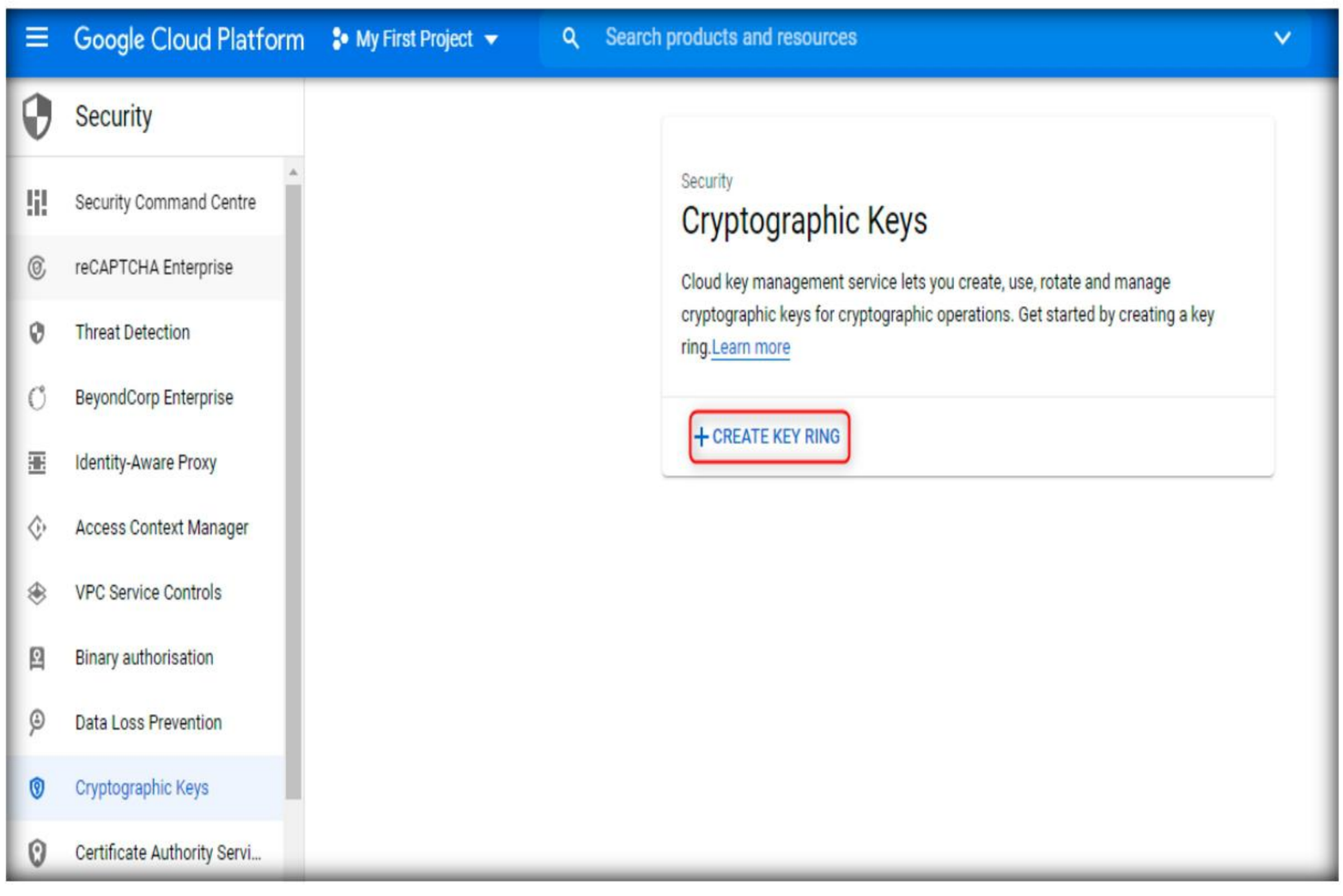


FIGURE 4.12.18: Creating Key Ring

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

20. Give a **Key ring name** and select the **Key ring location**. Then, Click on **CREATE**. Here we have used the following:

    Key ring name: ecckey-1

    Key ring location: global

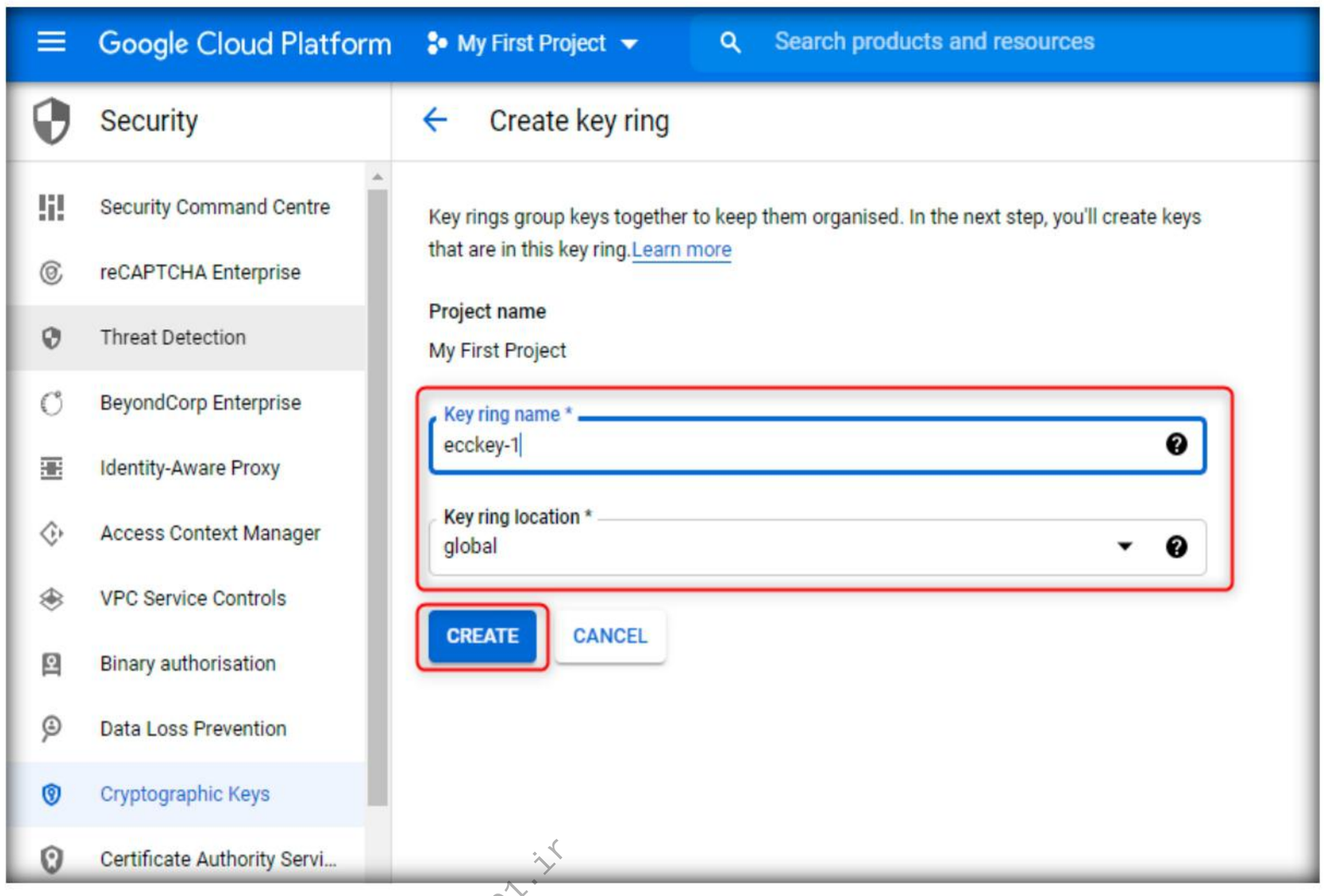


FIGURE 4.12.19: Creating Key Ring

21. Next, to create a key, click on **+CREATE KEY** at the top of the **Key ring details** window that opens.

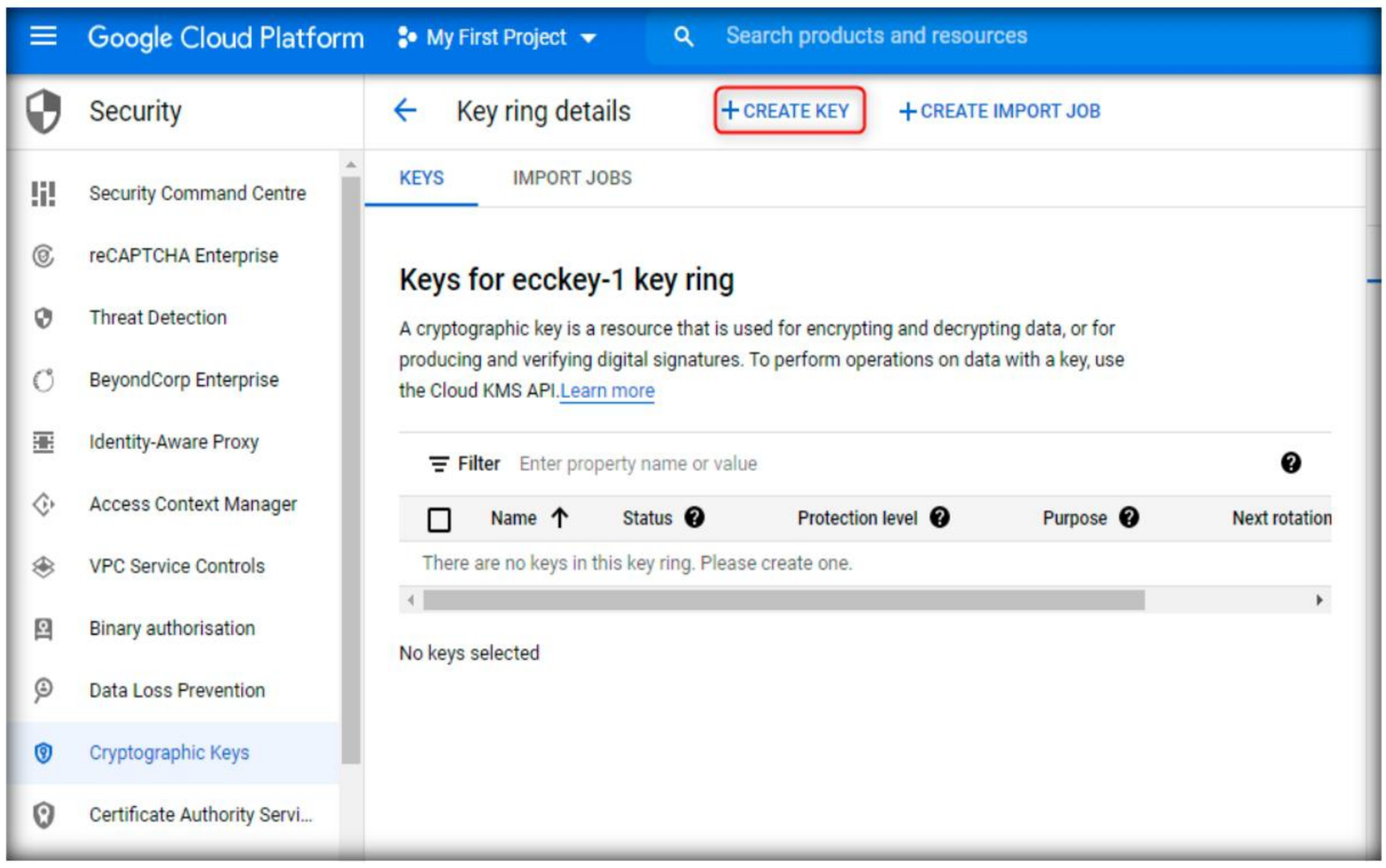


FIGURE 4.12.20: Creating Keys

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

22. In the **Create key** window that opens, under **What type of key do you want to create?**, select **Generated key**. Then, enter the **Key name** and select **Protection level** as **Software** and **Purpose** as **Symmetric encrypt/decrypt**. Here we have used the following

Key name: eccsecuritykey-1

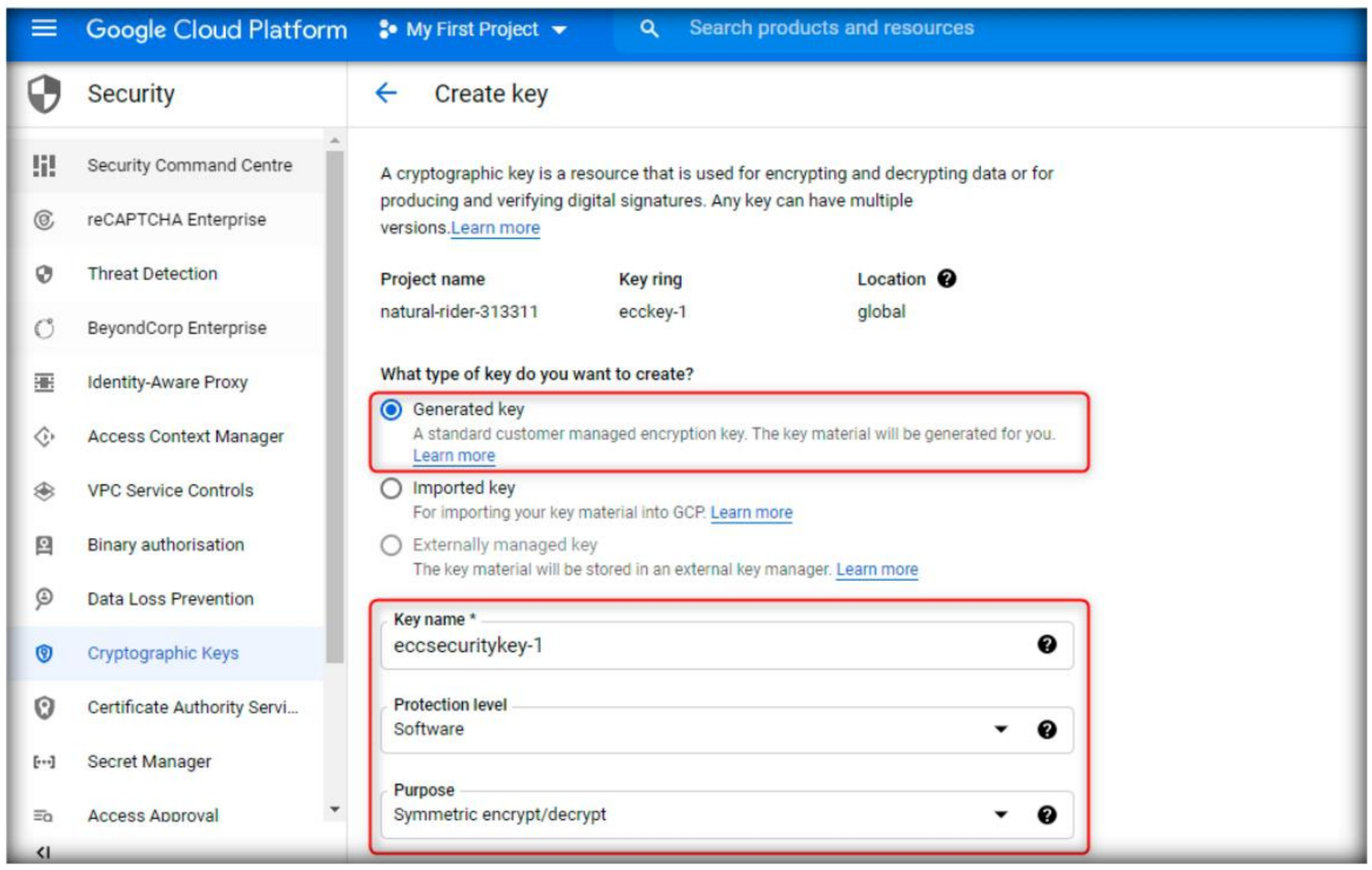


FIGURE 4.12.21: Selecting other Details

23. Retain the other settings and click on **CREATE**.

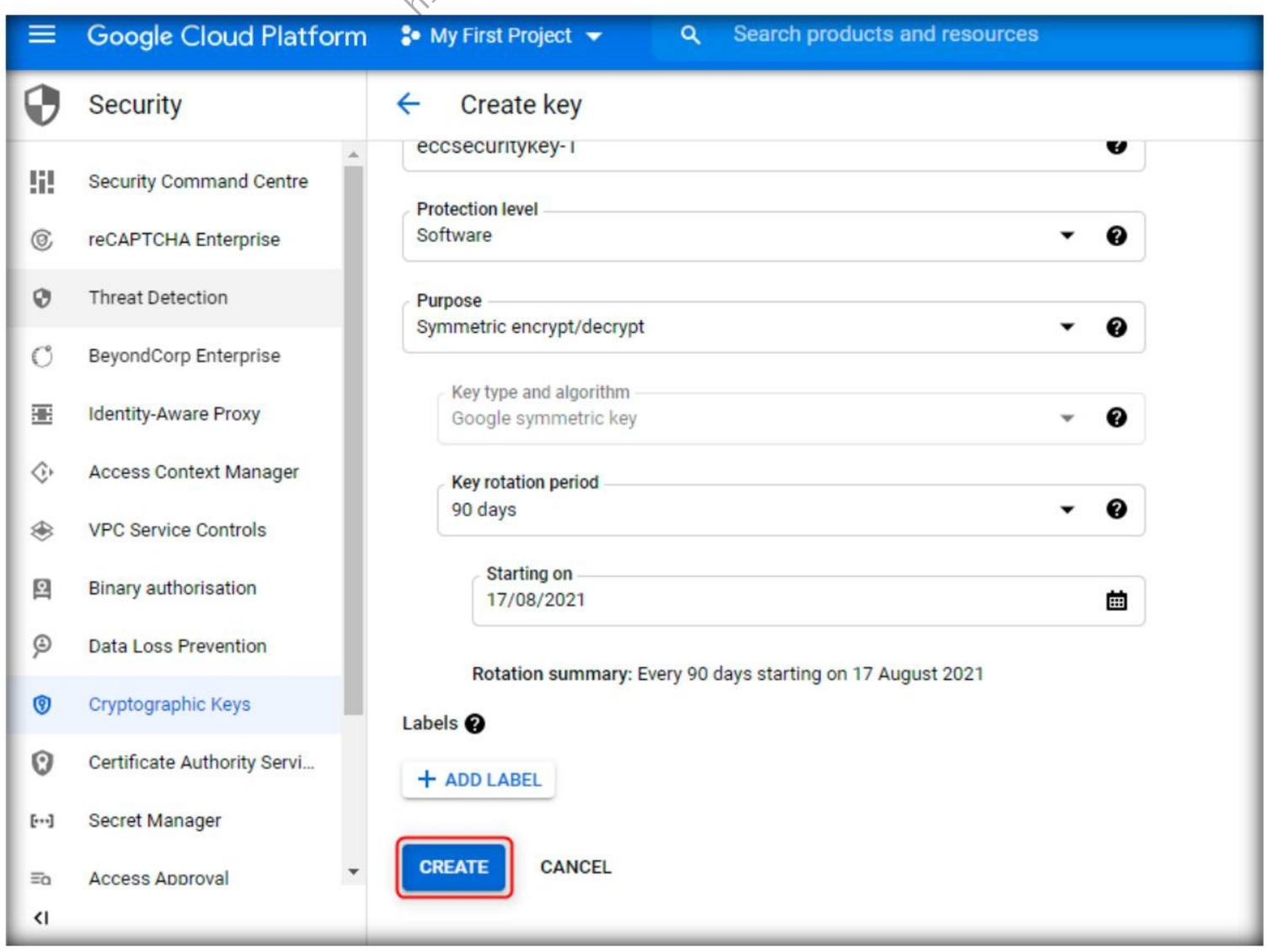


FIGURE 4.12.22: Creating the Key

Certified Cloud Security Engineer Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

24. The key ring and the cryptographic symmetric key will be generated, and the **Status** will become **Available** with a green tick mark.

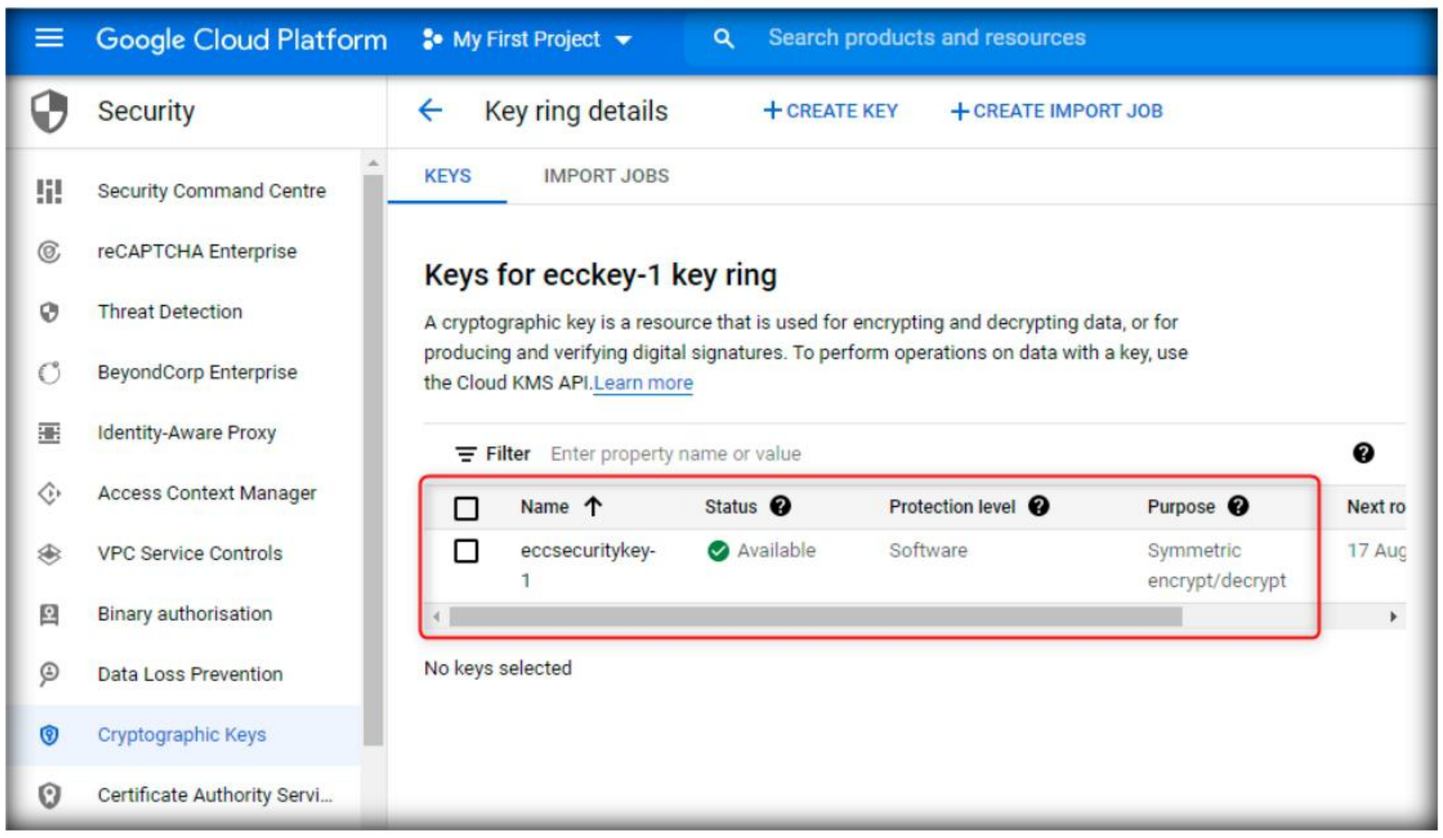


FIGURE 4.12.23: Created Key Ring and Key

TASK 2

Encrypting the Data with the Symmetric Key

25. Now you need to encrypt the data using the symmetric key. To do so, click on the **Cloud Shell icon** on the top right corner of the Google cloud console. Wait for the **Cloud Shell** to open.

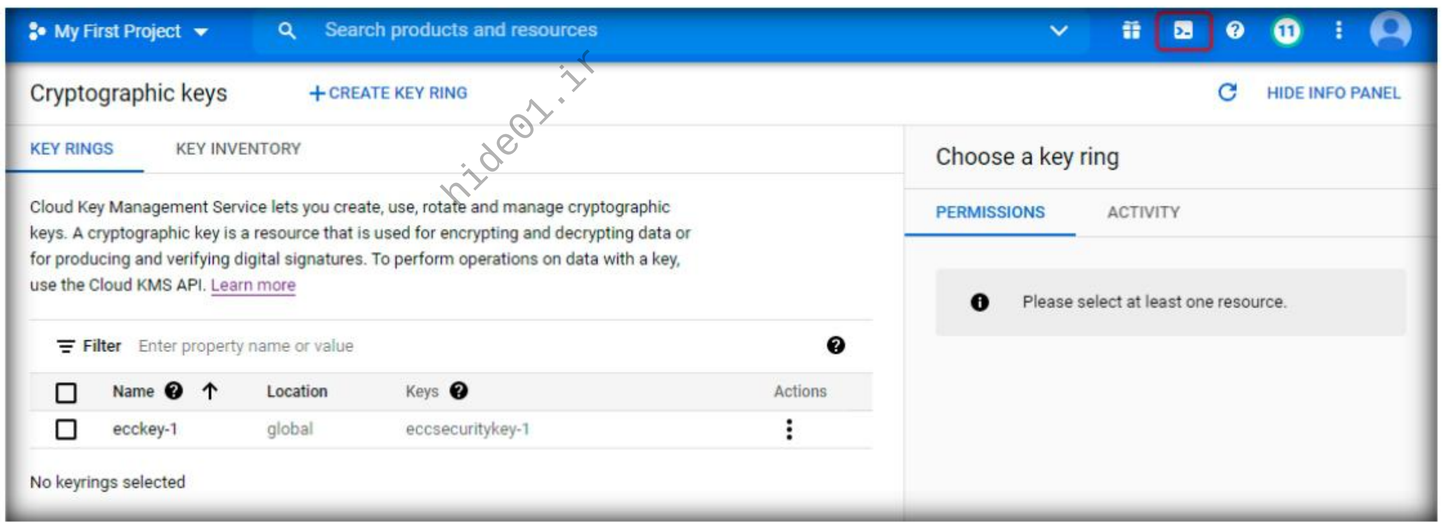


FIGURE 4.12.24: Opening Cloud Shell

26. Now, click on the icon to **open it in new window** at the top right corner of the **CLOUD SHELL** terminal.

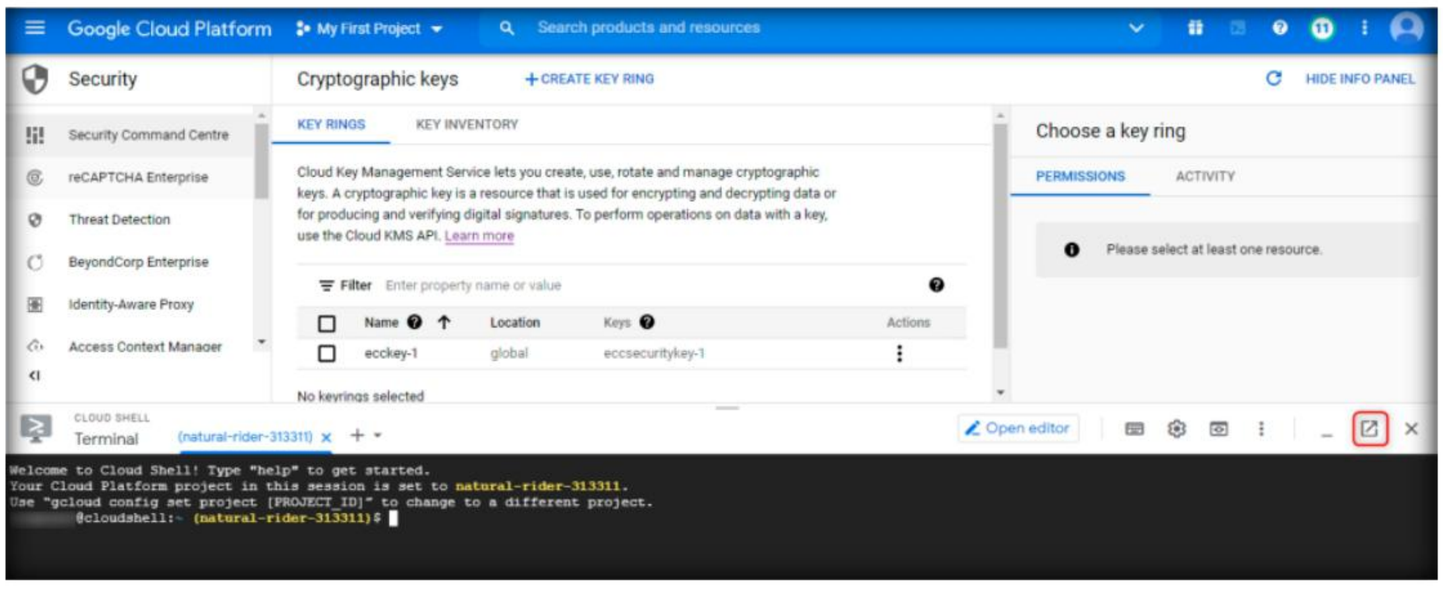


FIGURE 4.12.25: Opening Cloud Shell in new window

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

27. Now, in the **Cloud Shell** window, type the command given below and press **Enter** to list all projects.

    `gcloud projects list`

    Note: If a window pops up for **Authorise Cloud Shell**, click on **Authorise**.

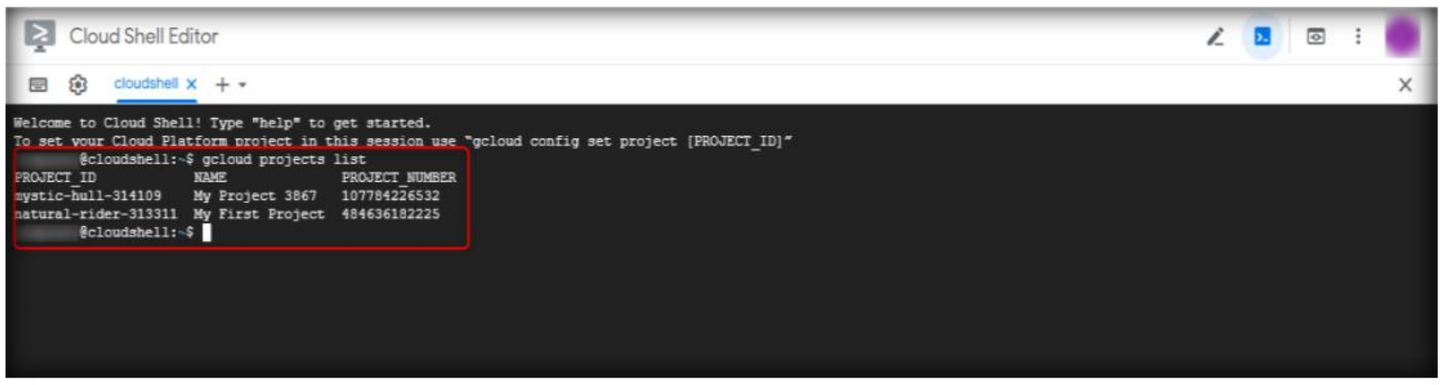


FIGURE 4.12.26: Listing the Projects

28. In the **Cloud Shell** editor window that opens, type the following command to set **My First project** in the current session. Then press **Enter**.

    `gcloud config set project[PROJECT_ID]` (replace `[PROJECT_ID]` with your project ID).

    Here we have used the following command:

    `gcloud config set project natural-rider-313311`

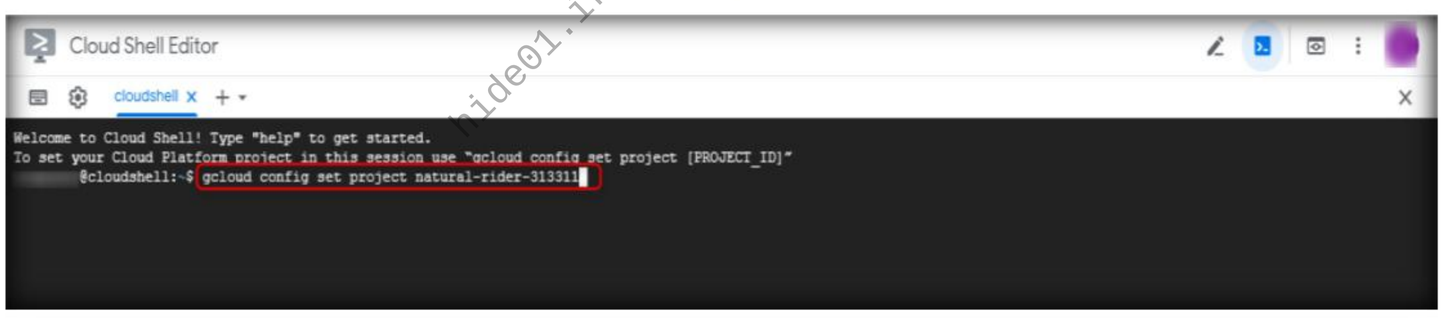


FIGURE 4.12.27: Setting Cloud Platform Project

29. After the **Cloud Shell** is authorized, create a text file that is to be encrypted. Then, type the following command and press **Enter**.

    `echo "<text to be encrypted>" > ./<name of text file.txt>` (replace <text to be encrypted> with your text and <name of text file.txt> with the name of your text file).

    Here, we have used the following command:

    `echo "hackers-are-here-where-are-you" > ./eccdata.txt`

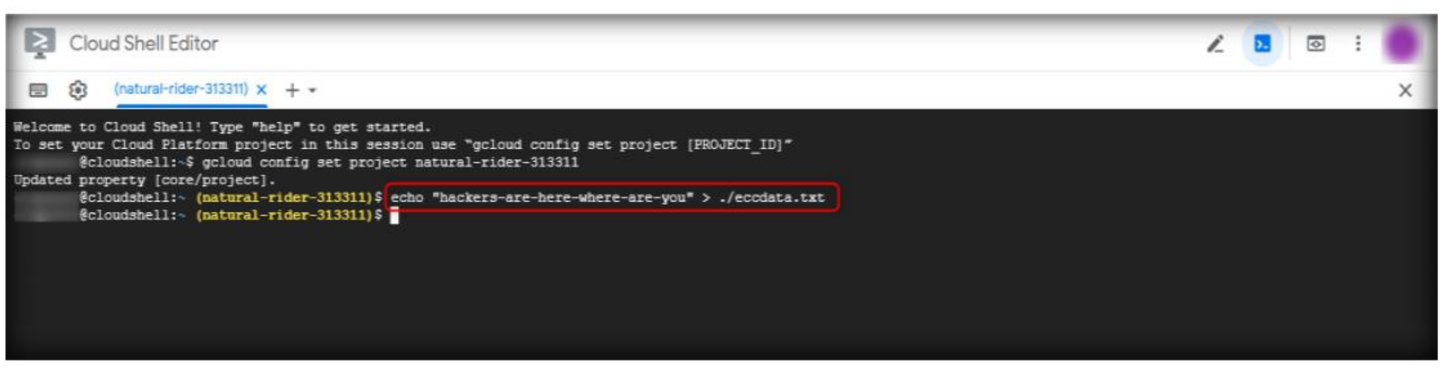


FIGURE 4.12.28: Creating text file

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

30. After the text file is created, encrypt the data in it. To do this, type the following command and press **Enter**.

```
gcloud kms encrypt \
    --location <location> \
    --keyring <key ring name> \
    --key <symmetric key name> \
    --plaintext-file ./<text file name> \
    --ciphertext-file ./<encrypted data text file name>
```

In the above command, replace <location> with the location of your key ring, <key ring name> with your key ring name, <symmetric key name> with the name of your symmetric key, <text file name> with the name of text file you created, and <encrypted data text file name> with a name for the encrypted file name with a .enc extension. In this lab, we have used the following command:

```
gcloud kms encrypt \
    --key eccsecuritykey-1 \
    --keyring ecckey-1 \
    --location global \
    --plaintext-file ./eccdata.txt \
    --ciphertext-file ./eccdata.txt.enc
```

hide01.ir

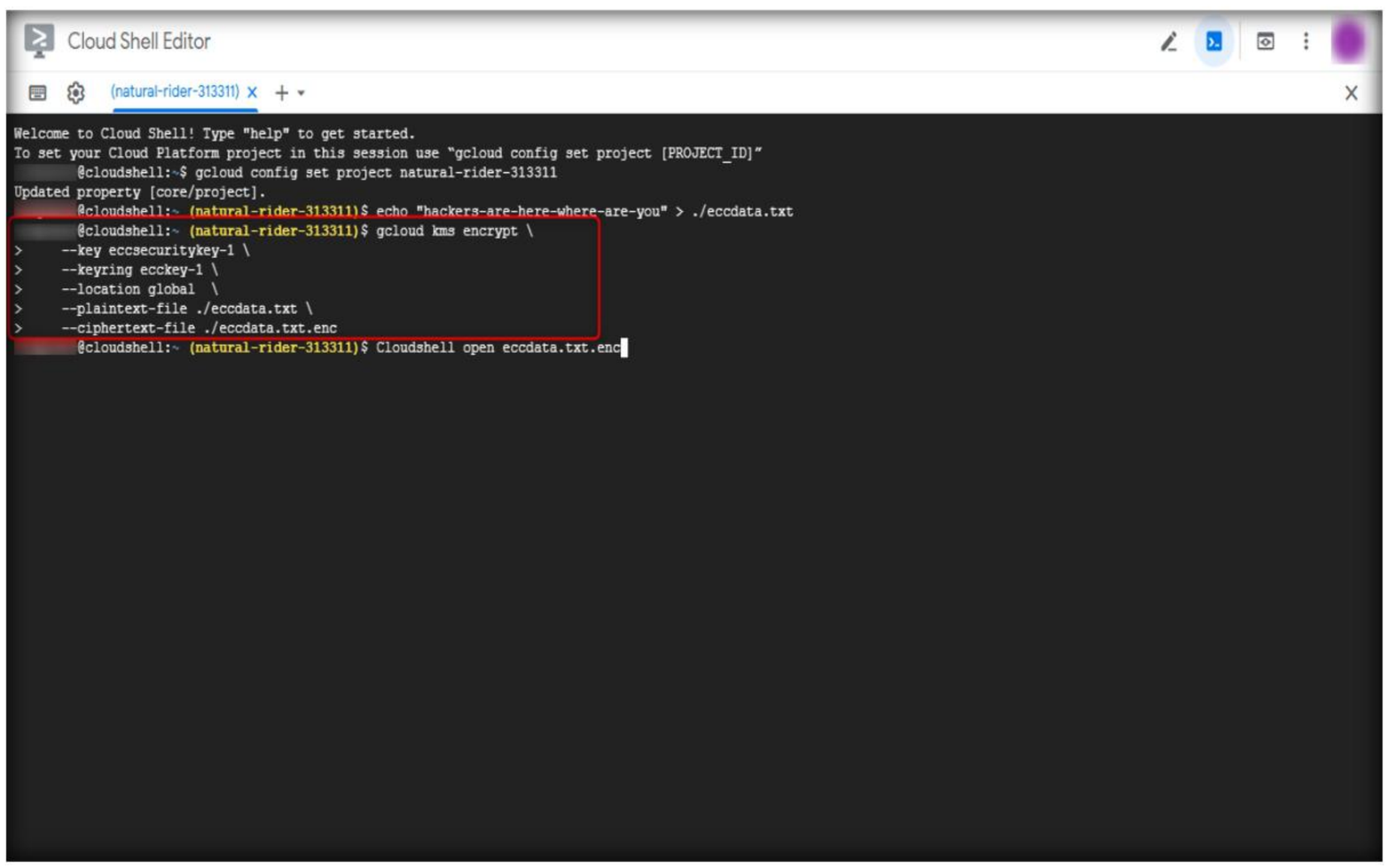


FIGURE 4.12.29: Performing data encryption

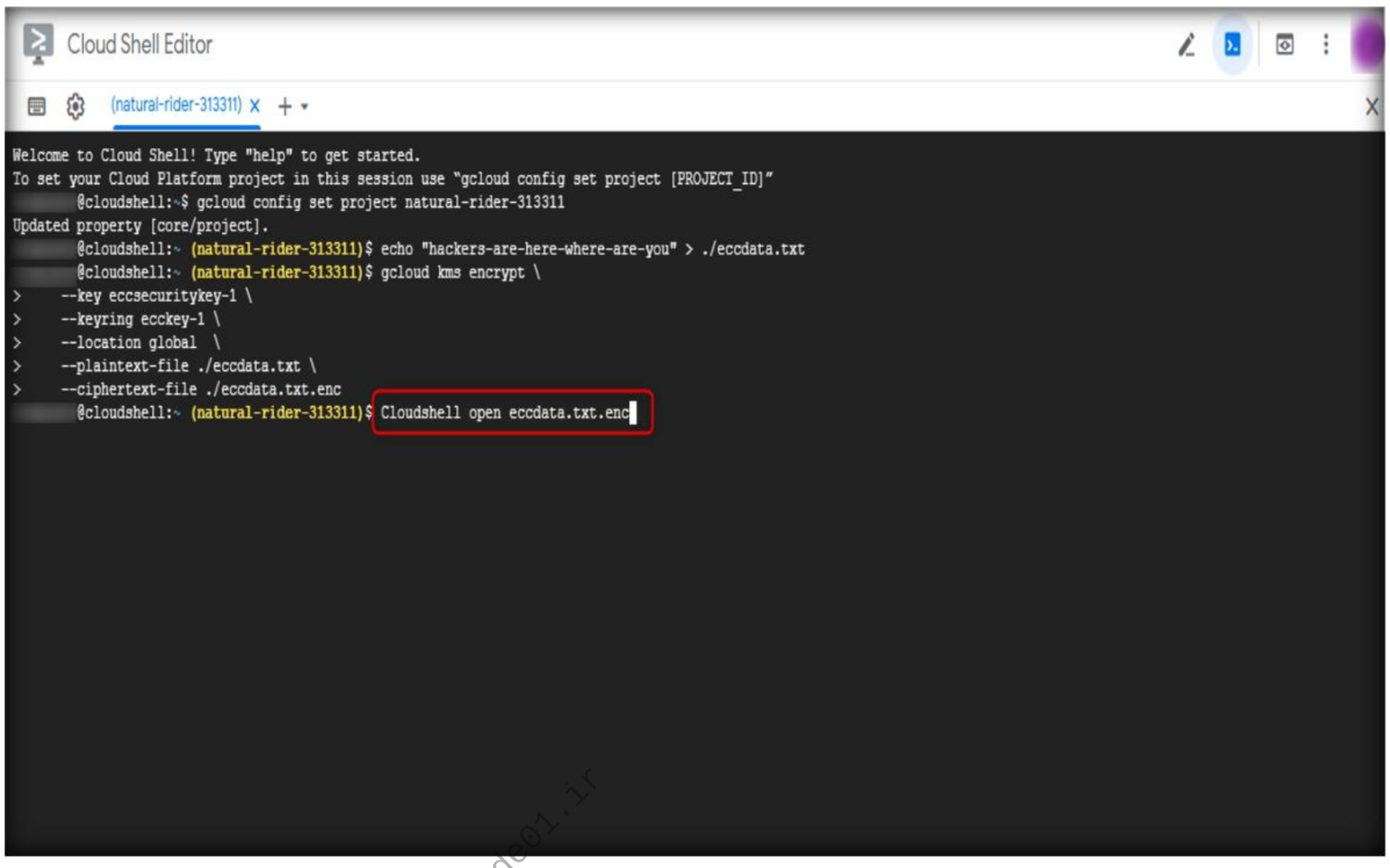
Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

31. Now we need to confirm whether the data has been successfully encrypted. To do this, type the following command and press **Enter**.

    `cloud shell open <name of the encoded text file>`
    (Replace <name of the encoded text file> with your encoded file name)

    In this lab, we have used the following command:

    `cloud shell open eccdata.txt.enc`



hide01.ir

FIGURE 4.12.30: Opening the text file

32. The text file displays strange, unprintable characters, as shown in the screenshot below.

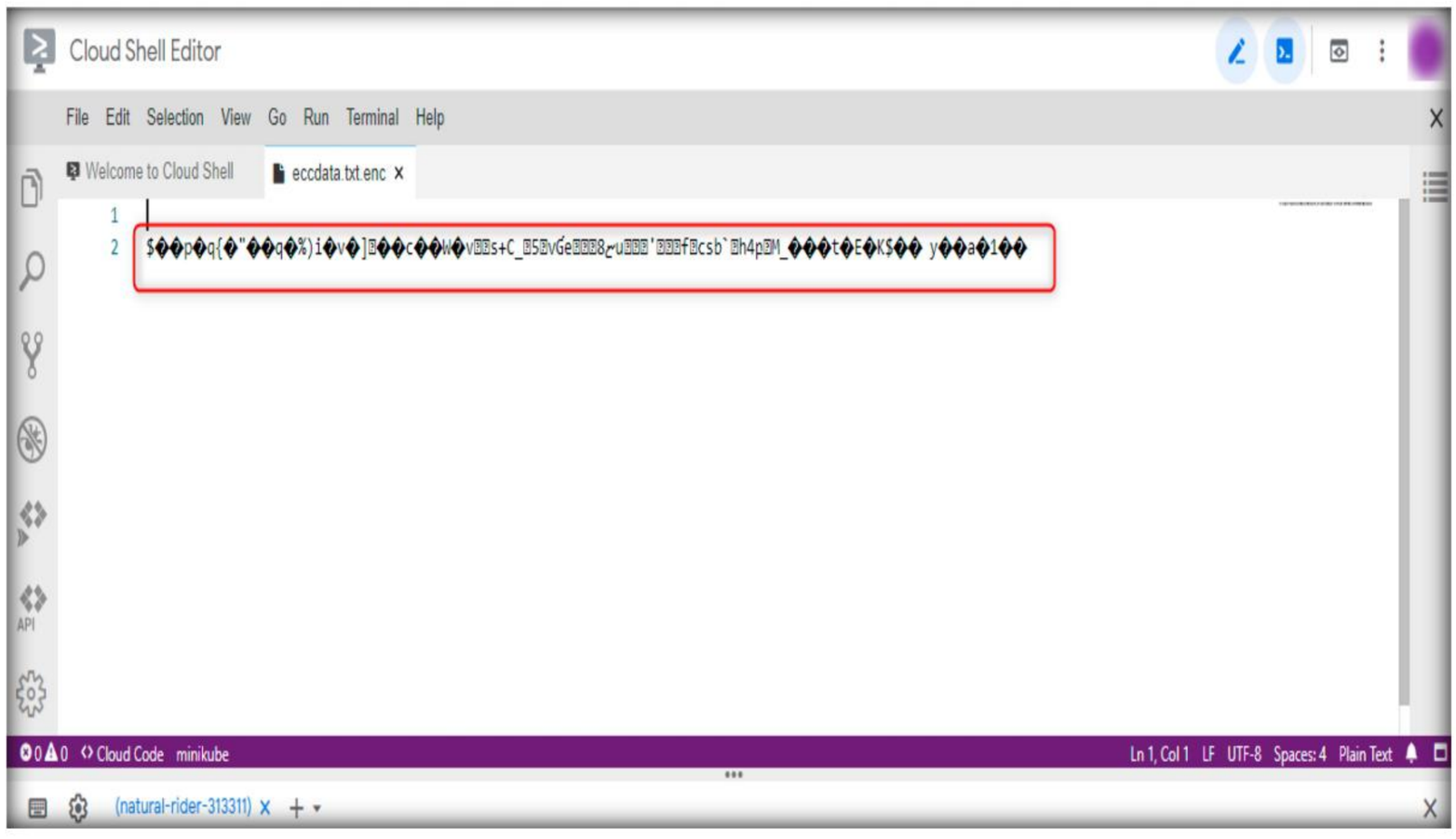


FIGURE 4.12.31: Encrypted text file

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 3

Decrypting the data

33. Next, decrypt the text file. To do so, type the following command and press **Enter**.

```
gcloud kms decrypt \
    --location <location> \
    --keyring <key ring name> \
    --key <key name> \
    --plaintext-file - \
    --ciphertext-file ./<encrypted text file name>
```

In the above command, replace <location> with the location of your key ring, < key ring name> with your key ring name, < key name> with the name of your symmetric key, and <encrypted data text file name> with the name of the encrypted file with a .enc extension. For this lab, we have used the following command:

```
gcloud kms decrypt \
    --location global \
    --keyring ecckey-1 \
    --key eccsecuritykey-1 \
    --plaintext-file - \
    --ciphertext-file ./eccdata.txt.enc
```

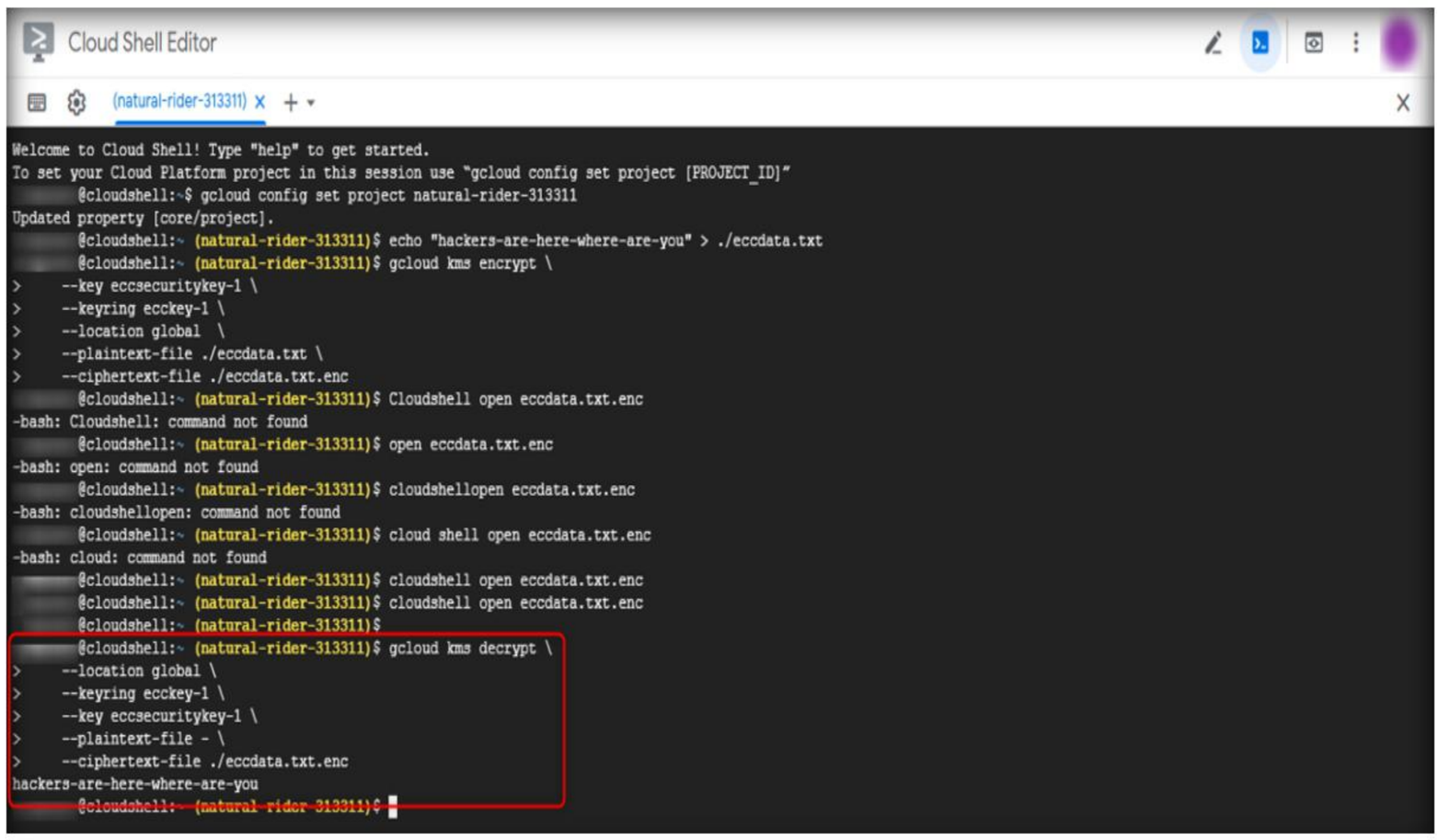


FIGURE 4.12.32: Decrypting the text file

34. The text file is decrypted successfully.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 4

Rotating Keys

35. Next, rotate the keys to limit the number of files encrypted with the same key version to prevent brute-force attacks. To perform a manual key rotation and set it as the primary key version, type the following command and press **Enter**.

```
gcloud kms keys versions create \
     --location <location> \
     --keyring <keyring name> \
     --key <key name> \
     --primary
```

In the above command, replace <location> with the location of your key ring, < keyring name> with your key ring name, and < key name> with the name of your symmetric key. In this lab, we have used the following command:

```
gcloud kms keys versions create \
--location "global" \
--keyring "ecckey-1" \
--key "eccsecuritykey-1" \
--primary
```

hide01.ir

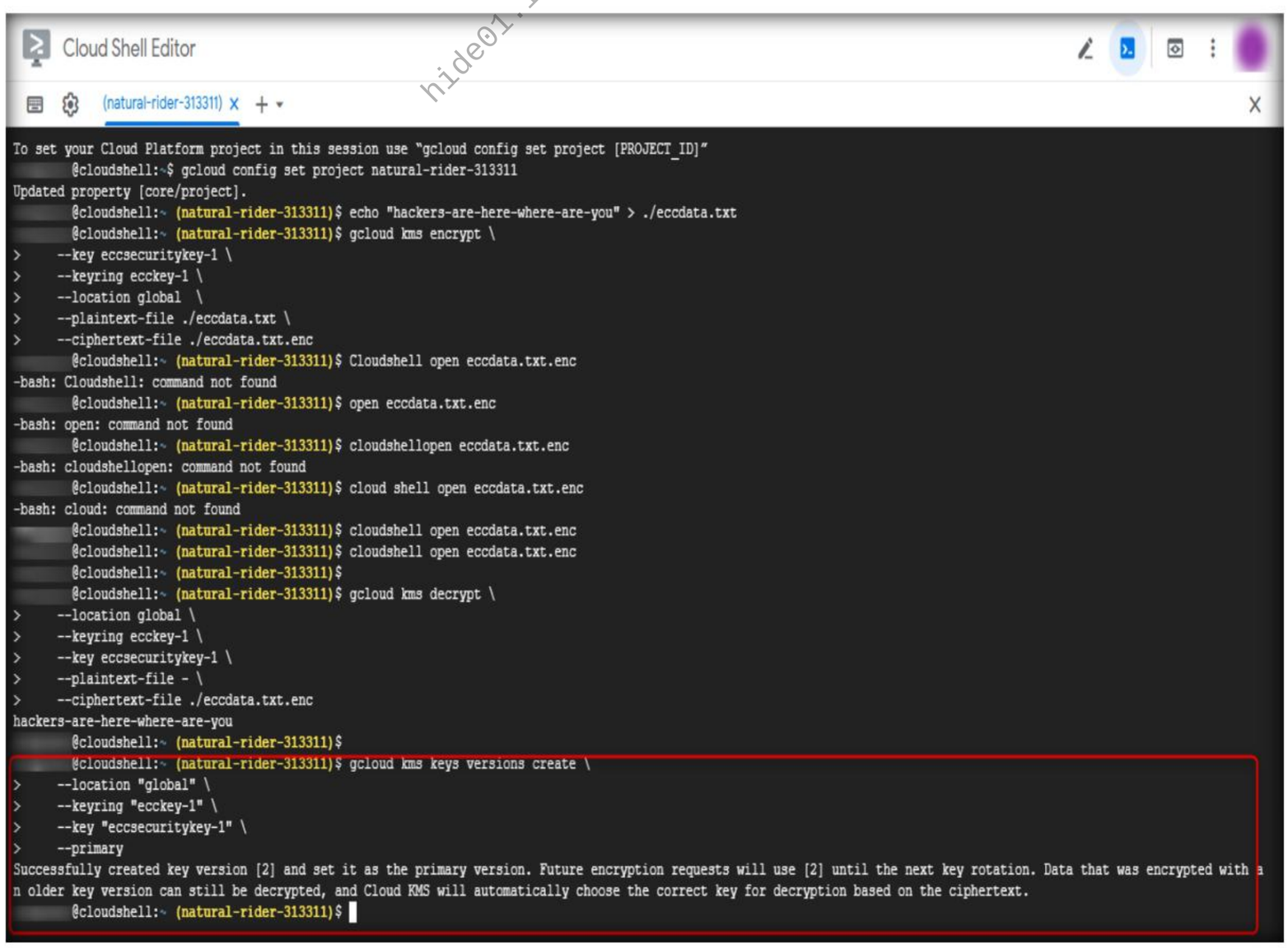


FIGURE 4.12.33: Rotating Keys

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

36. To add more security, disable the key version to prevent the ciphertext values encrypted using an older crypto key version from being decrypted with Cloud KMS. To do so, type the following command and press **Enter.**

```
gcloud kms keys versions disable "1" \
--location "<location>" \
--keyring "<keyring name>" \
--key "<key name>"
```

In the above command, replace <location> with the location of your key ring, < keyring name> with your key ring name, and < key name> with the name of your symmetric key. In this lab, we have used the following command:

```
gcloud kms keys versions disable "1" \
--location "global" \
--keyring "ecckey-1" \
--key "eccsecuritykey-1"
```

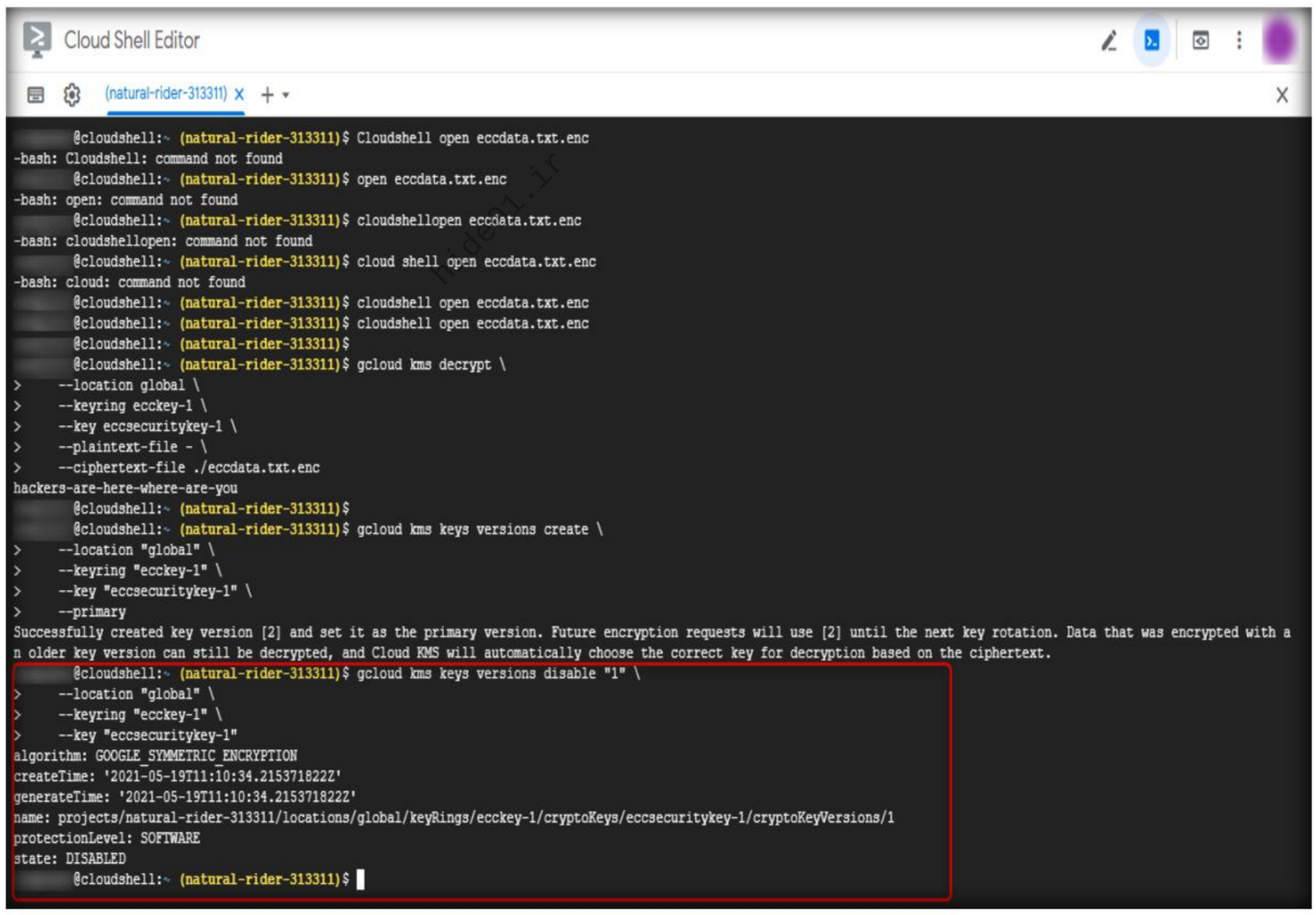


FIGURE 4.12.34: Disabled Keys

37. This way, a cloud security engineer can manage the cryptographic keys for encrypting and decrypting data and ensure data security.

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

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

38. To delete the text file you have created, type the following command and press Enter.

```
rm eccdata.txt
```

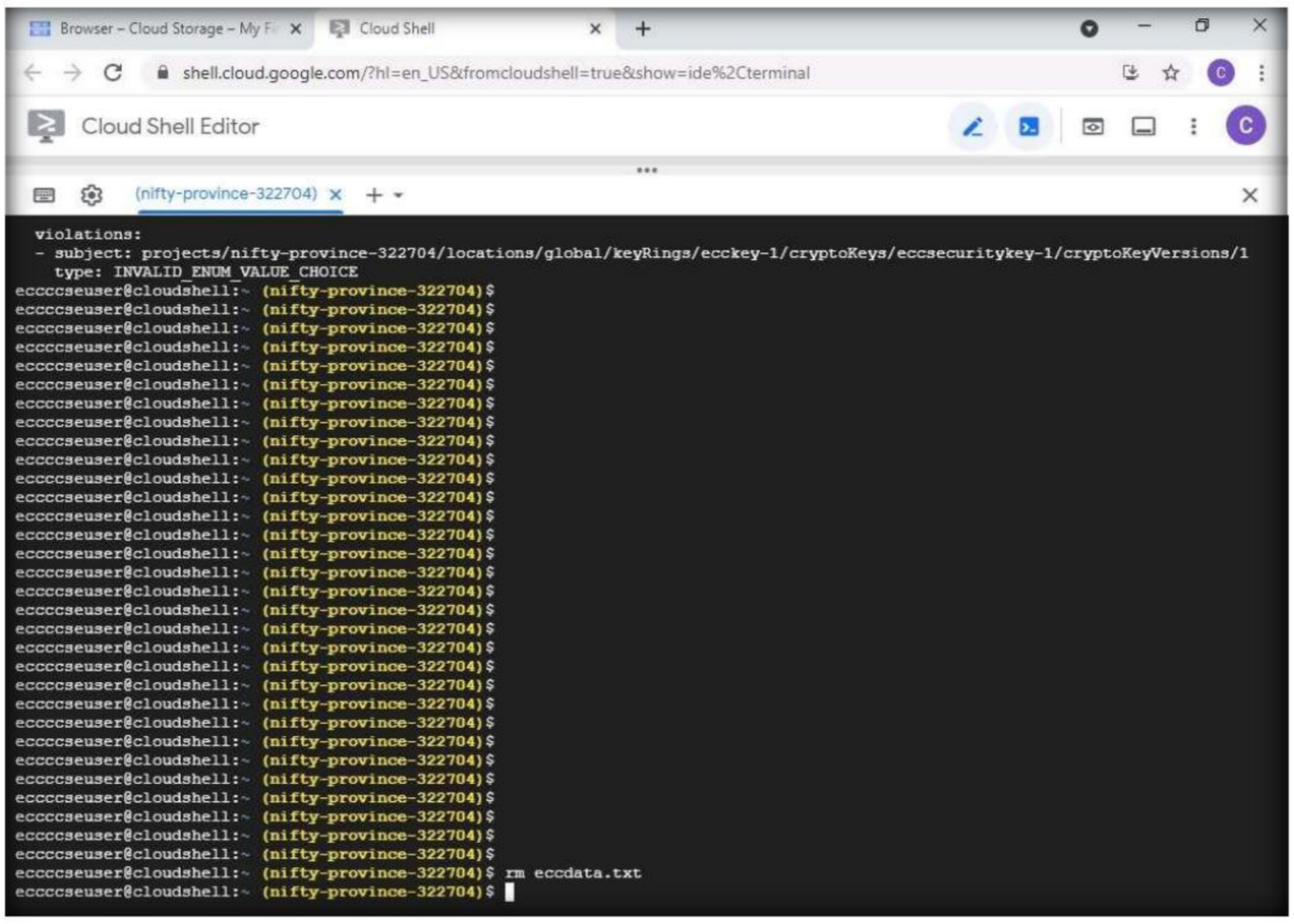


FIGURE 4.12.35: Deleting the Text File

39. Next, to destroy the key (eccsecuritykey-1), navigate to Security, and select Key Management. Open the key ring (ecckey-1). Click on the ellipsis at the end of the key (eccsecuritykey-1) and click on Destroy all key version material. If a pop-up appears, enter the name of the key and click on Schedule destruction.

Caution: The key will get destroyed after 24 hours. You cannot delete the key rings that you have created.

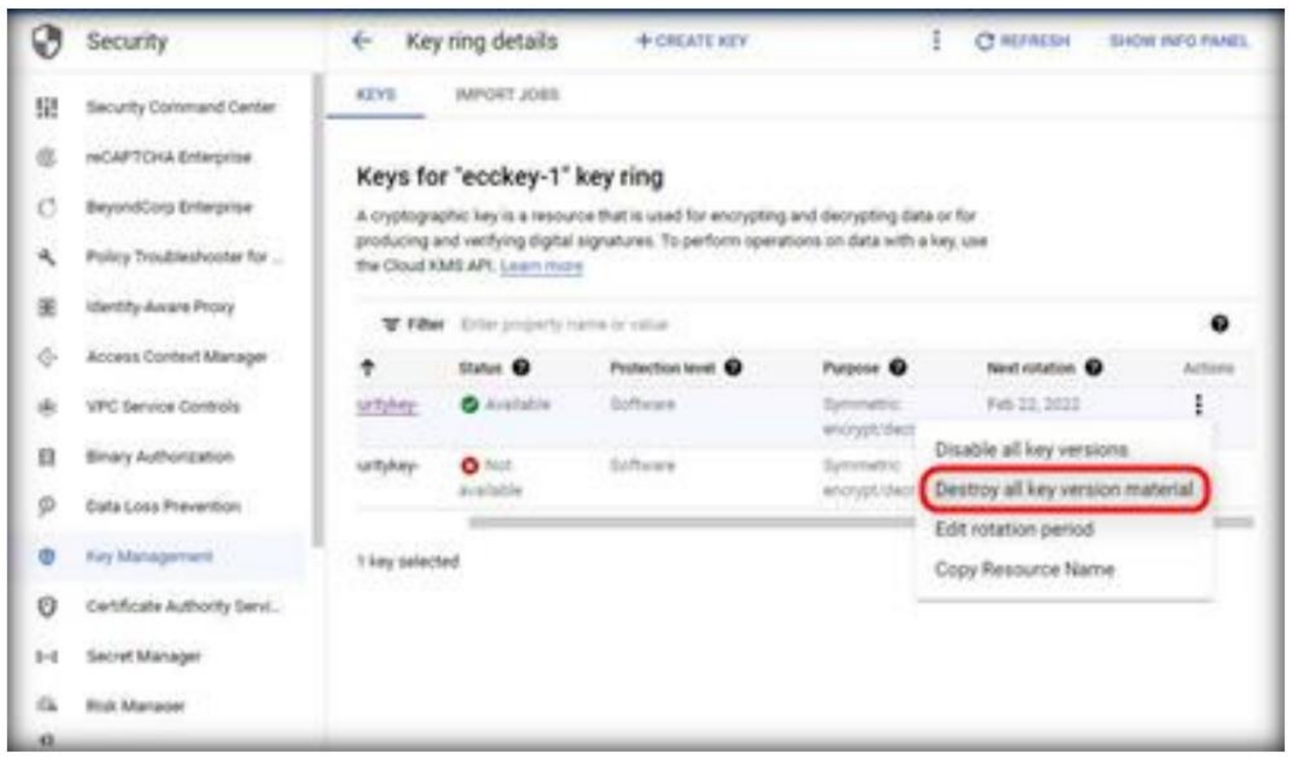


FIGURE 4.12.36: Deleting the Key

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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.

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 13

Inspecting Sensitive Information in GCP with Cloud DLP

Cloud Data Loss Prevention (DLP) service in GCP scans, discovers, protects, and classifies the most sensitive data.

Lab Scenario

Cloud security engineers follow different data security methods to protect sensitive data on cloud. The DLP API in Google Cloud offers access to a detection engine for personally identifiable information (PII) and sensitive data. Cloud DLP provides a fast redaction of the most sensitive data, such as credit card numbers, phone numbers, and passport numbers.

hide01.ir

ICON KEY

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

Lab Objectives

This lab will demonstrate how to set up Cloud DLP, set up an IAM service account, and inspect a string for sensitive information.

In this lab, you will learn to do the following:

- Enable Cloud DLP
- Setup IAM service account for authentication
- Download DLP API files and inspect a string for sensitive information

Lab Environment

To perform this lab, you need the following:

- **Admin Machine** VM
- **Administrative** privileges
- **Registered GCP account**

Lab Duration

Time: 20 minutes

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Overview of Cloud DLP

Cloud DLP helps meet specific compliance requirements by allowing you to understand and manage critical data. Cloud DLP manages sensitive information and personally identifiable information (PII. It prevents the disclosure of sensitive information such as credit card numbers, names, social security numbers, and GCP credentials by offering scalable and fast information classification and redaction. Cloud DLP scans storage buckets, folders, and objects containing sensitive data to meet the security compliance requirements.

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., GCP), the application interface may be updated with time. Hence, in case you happen to work on an updated version of GCP, 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 GCP Free Trial account using the following link: https://cloud.google.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 GCP account but be aware that it may incur significant charges to your account..

hidc01.ir

TASK 1

Enabling Cloud DLP API

1. Log in to the **Admin Machine** VM with the user **Admin** and password **admin@123**.

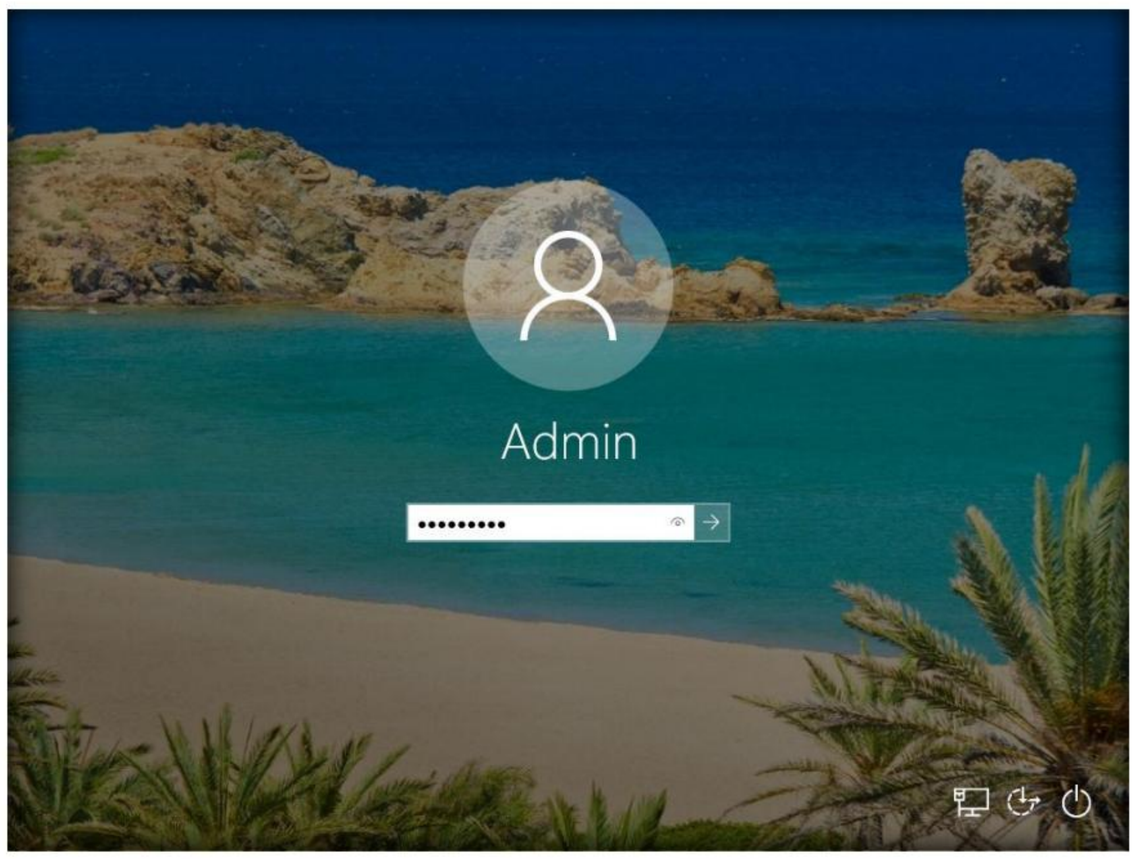


FIGURE 4.13.1: User Login

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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

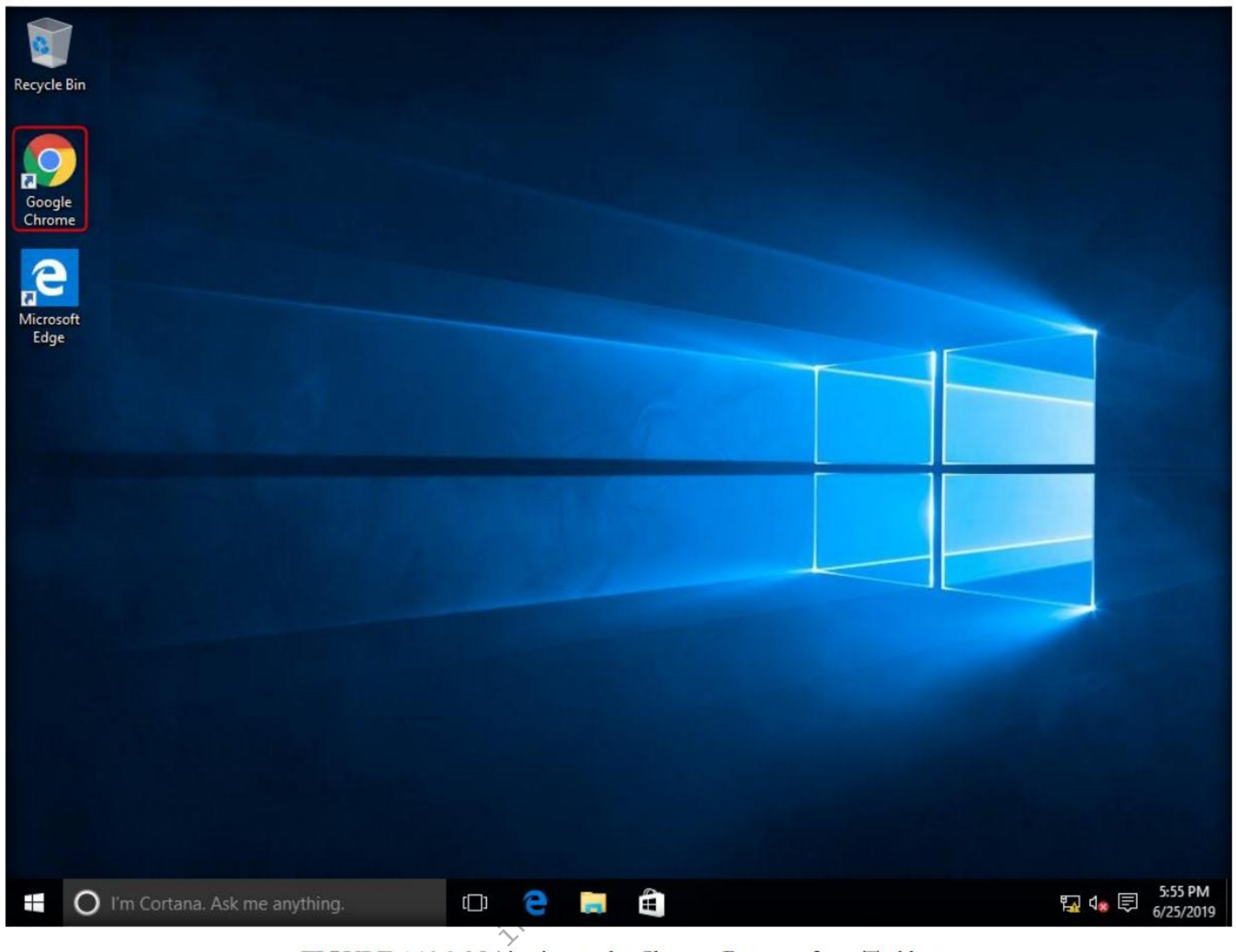


FIGURE 4.13.2: Navigating to the Chrome Browser from Taskbar

3. The **Google Chrome** browser opens. Go to the address bar, type **https://console.cloud.google.com**, and press **Enter.**

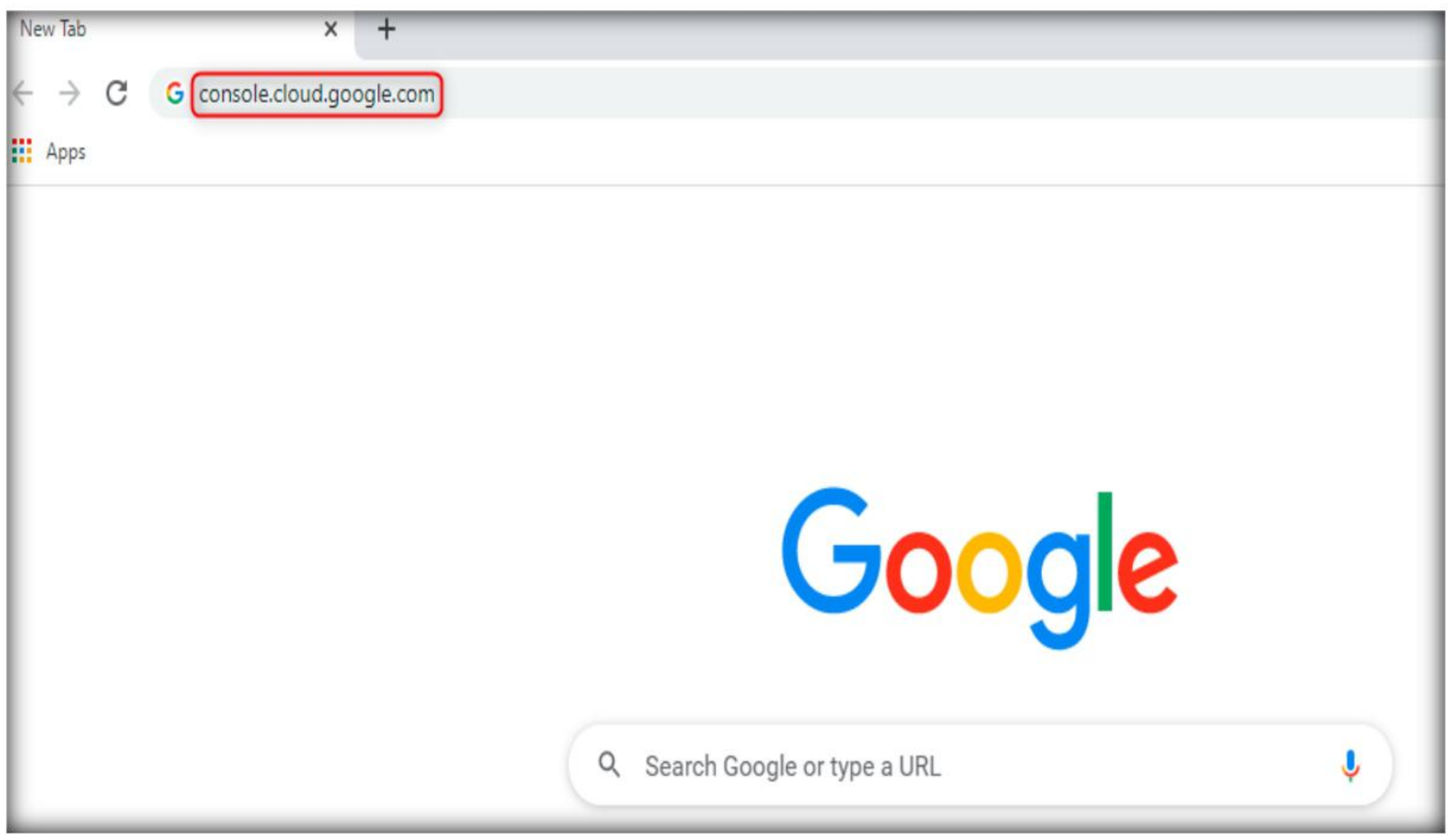


FIGURE 4.13.3: Access GCP in Browser

Note: If you are already logged in, skip the login steps.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

4. Enter the **Email address** to sign into GCP and click **Next**.

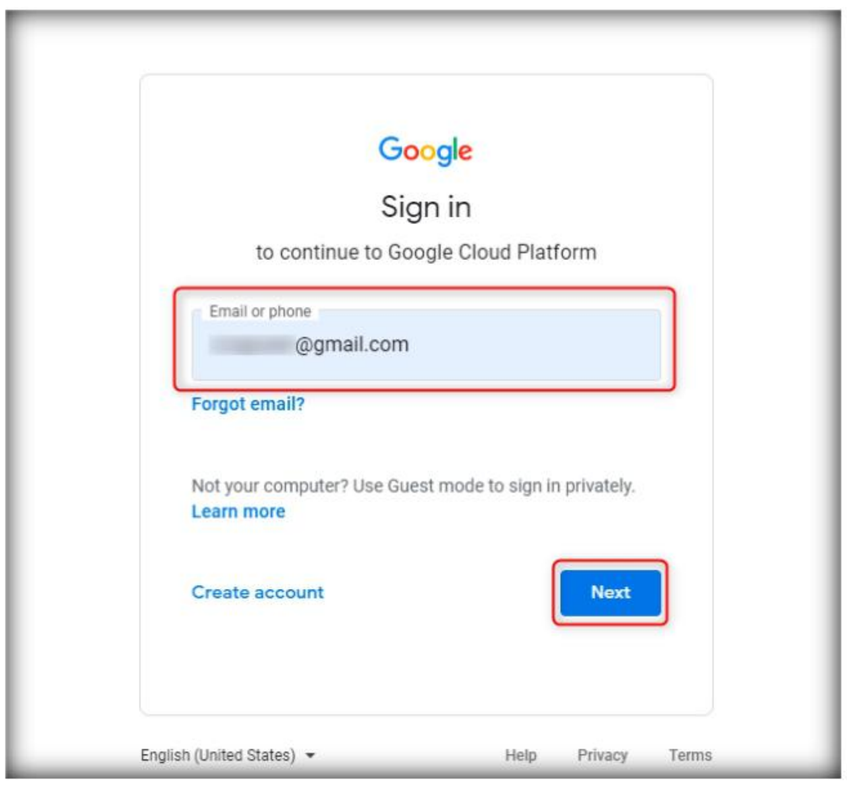


FIGURE 4.13.4: Authentication

5. Enter the **password** and click on **Next**.

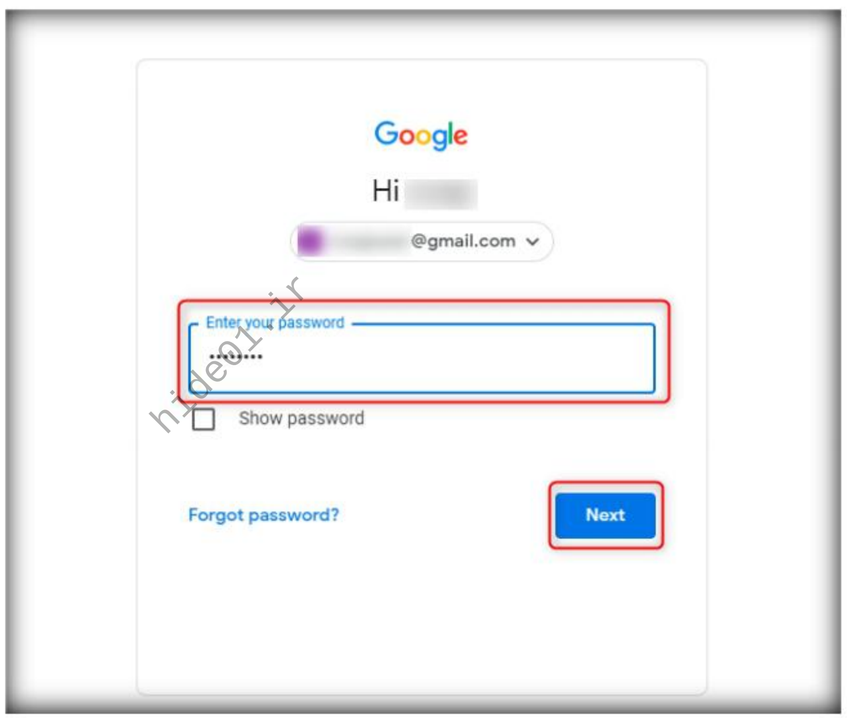


FIGURE 4.13.5: Signing in to the console

6. On the top left corner, you will have a dropdown. Ensure **My First Project** is selected here.

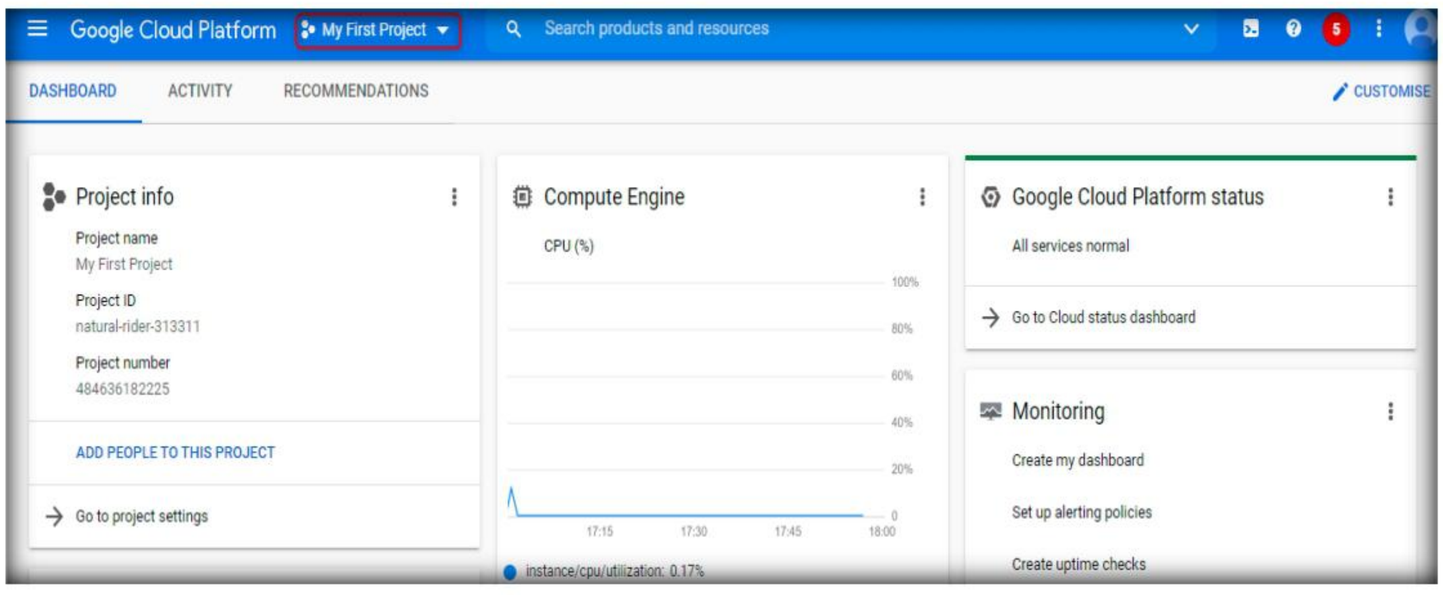


FIGURE 4.13.6: Selecting the Project

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

7. Now, enable **Cloud DLP API** for **My First Project**. To do so, navigate to **Security** and select **Data Loss Prevention** from the console.

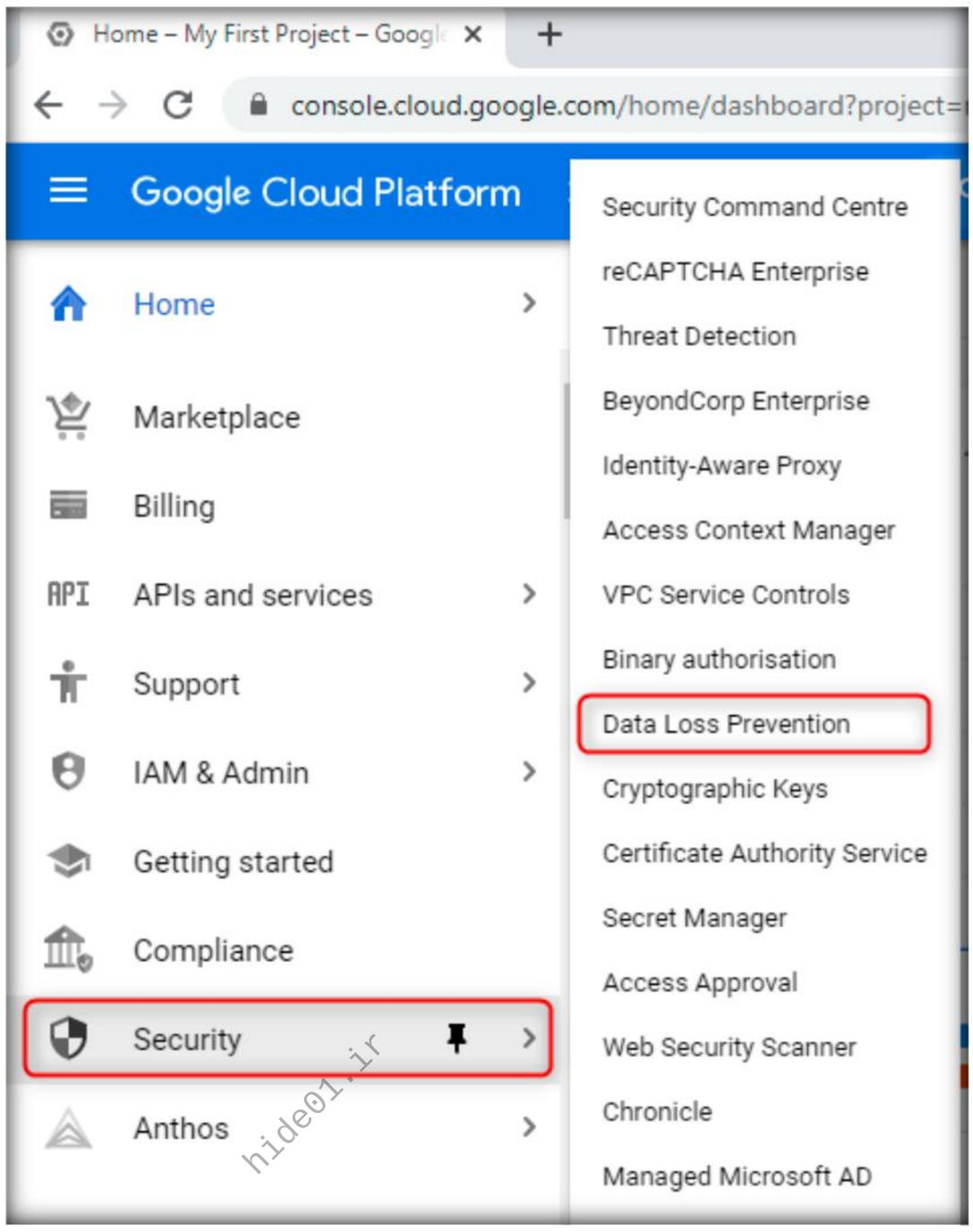


FIGURE 4.13.7: Navigating to Data Loss Prevention in Console

8. Click on **ENABLE** to enable **Cloud DLP** for **My First Project**. Wait for it to be enabled.

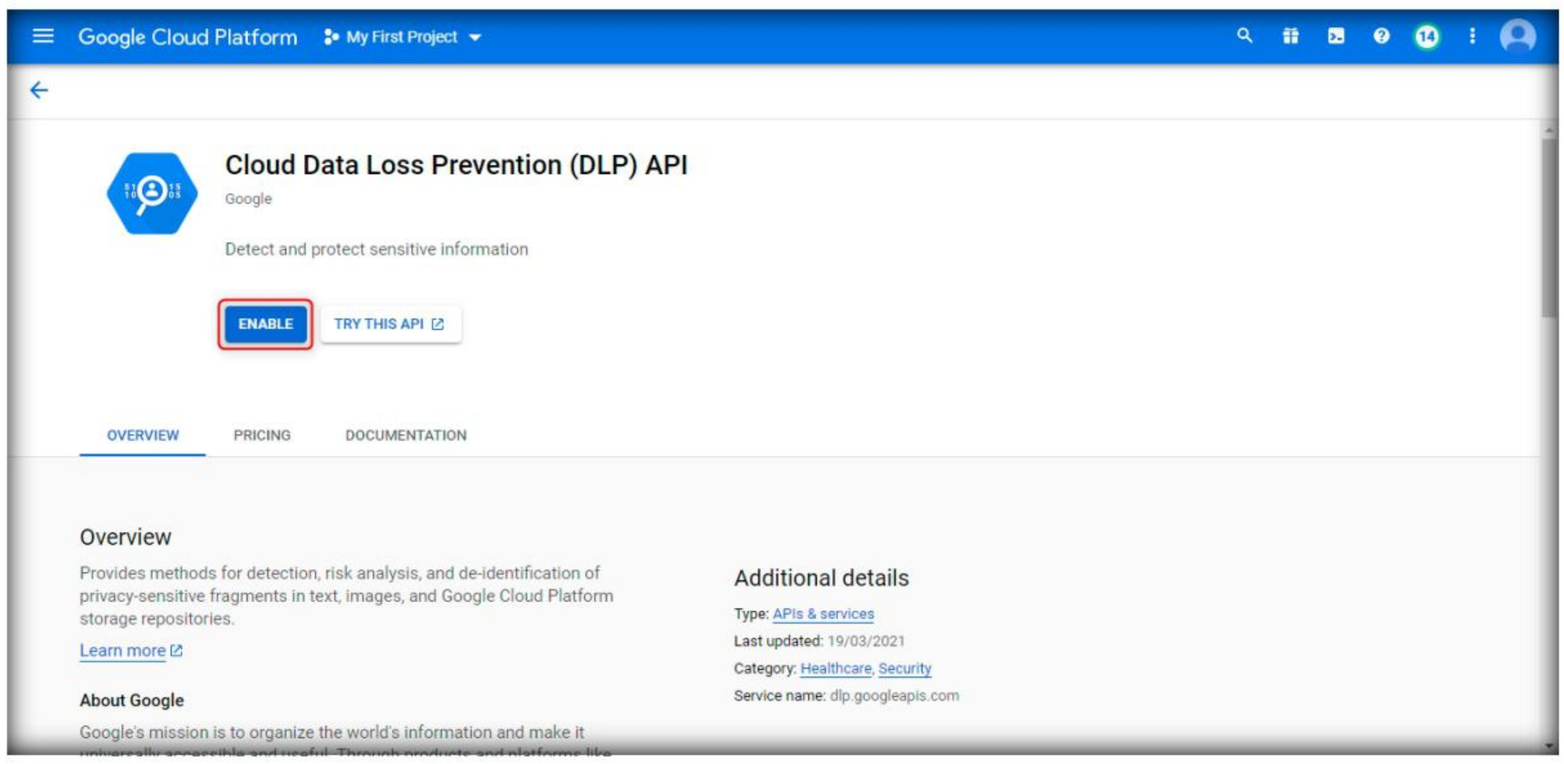


FIGURE 4.13.8: Enabling Cloud DLP API

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 2

Setting up IAM Service Account for Authentication

9. Now, setup an IAM service account for authentication. Navigate to **IAM & Admin** and select **Service Accounts** in the console.

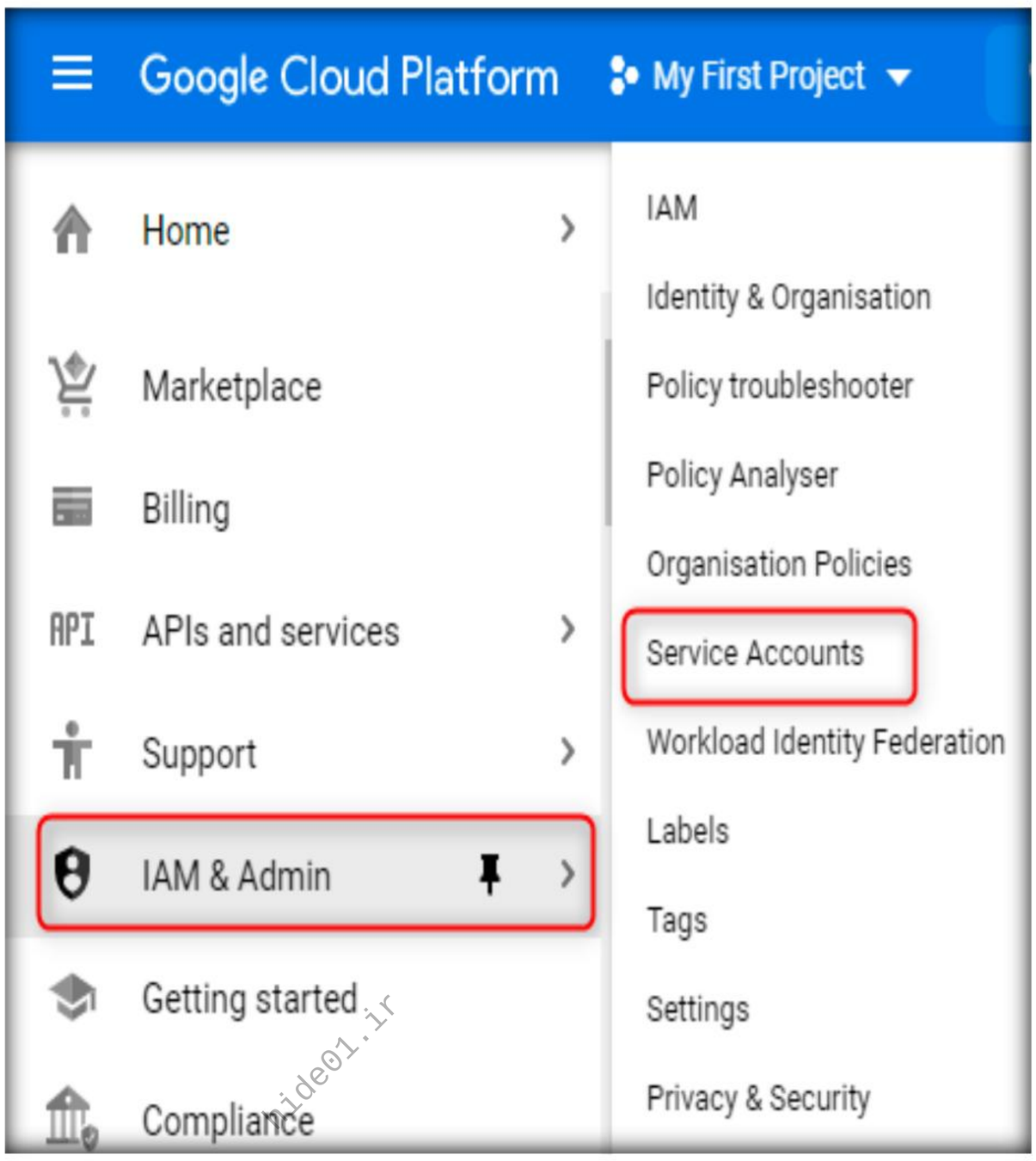


FIGURE 4.13.9: Navigating to Service Accounts

10. To create the service account for Cloud DLP, click on **+CREATE SERVICE ACCOUNT** at the top of the **Service accounts** window.

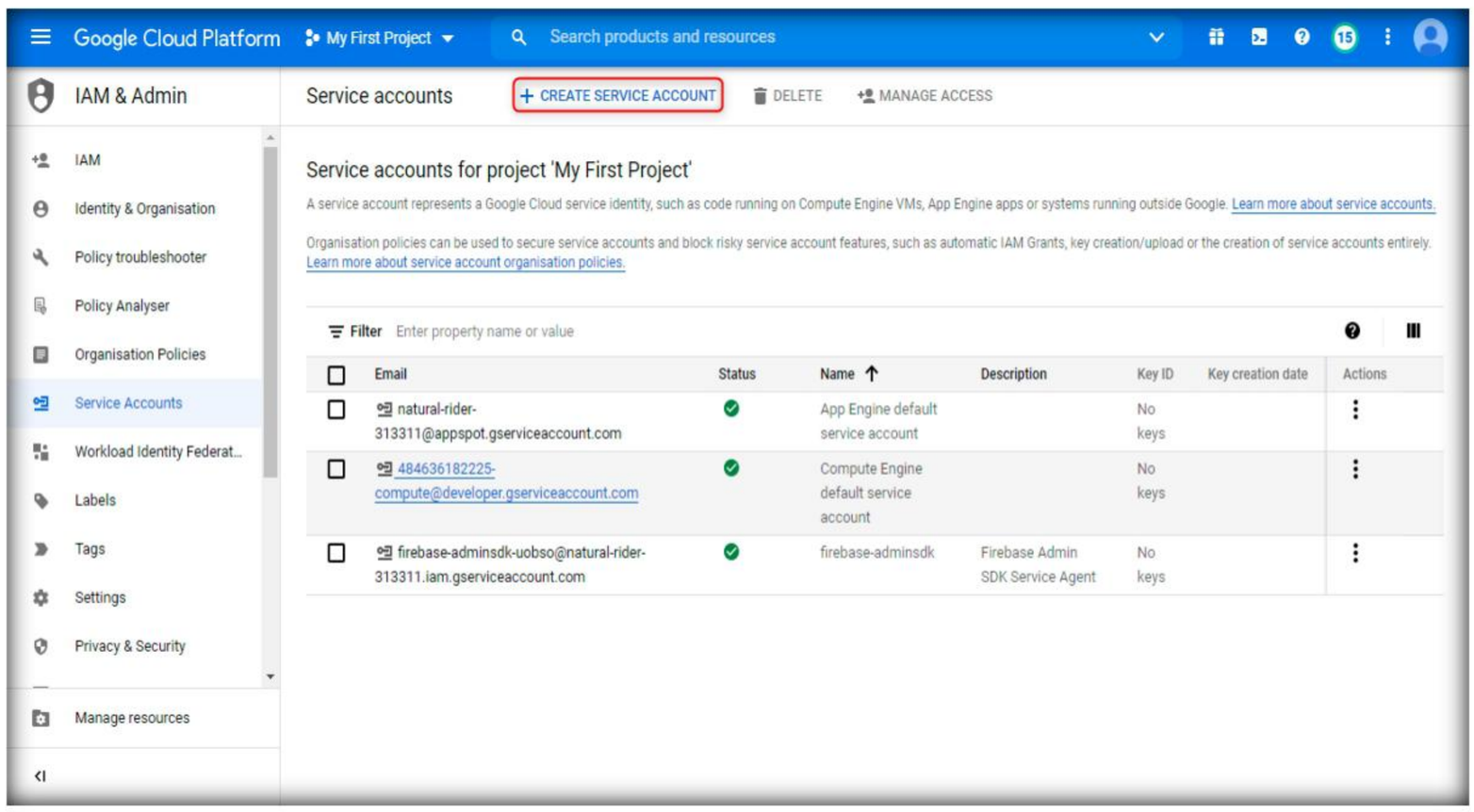


FIGURE 4.13.10: Creating Service account

Certified Cloud Security Engineer Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

11. For **Service account details** under **Service account name**, type a name (**eccservice-1**) and click on **CREATE**.

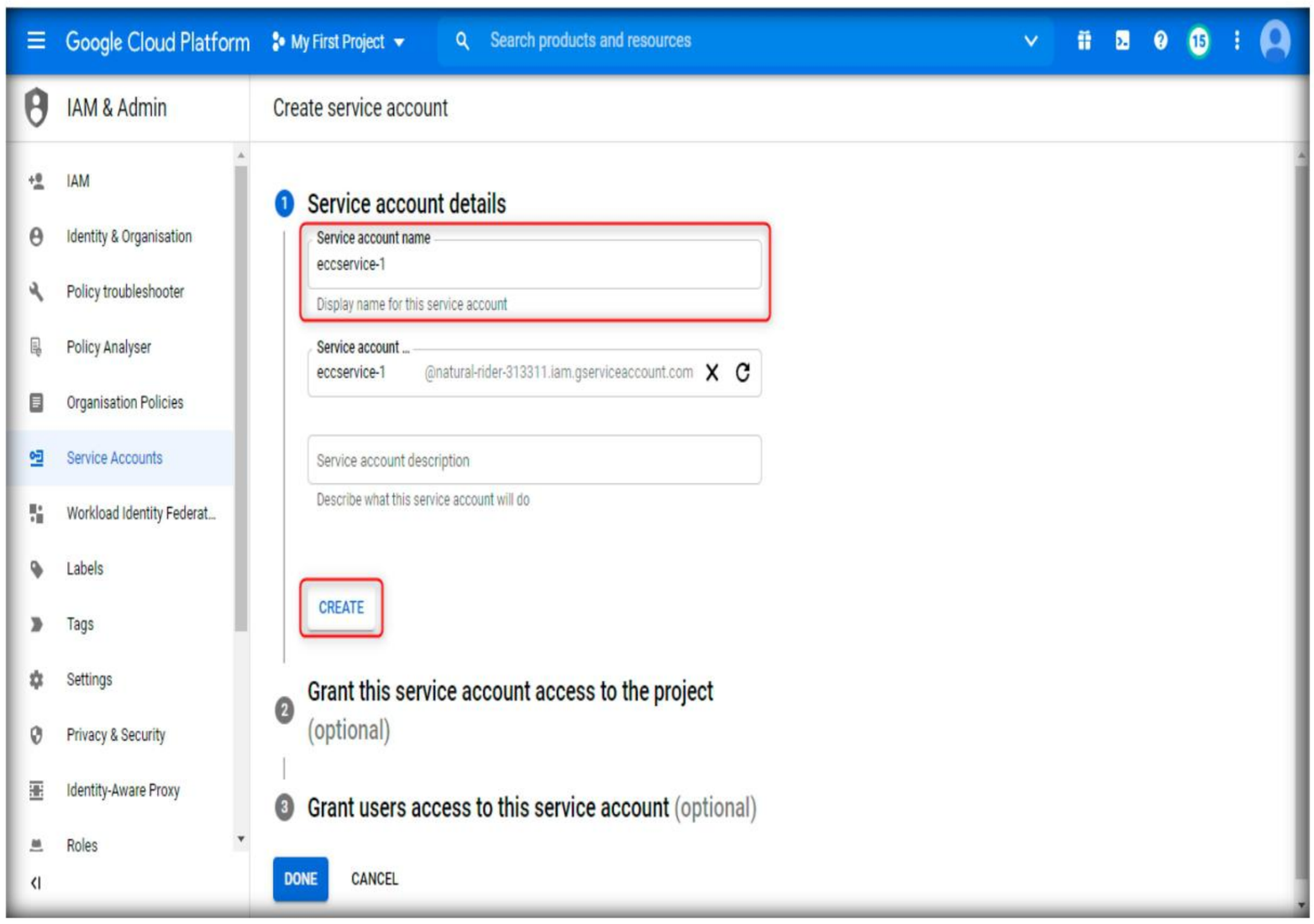


FIGURE 4.13.11: Typing Service Account Details

12. Now, for **Grant this service account access to the project**, click on **Select a role**.

hidegr.ir

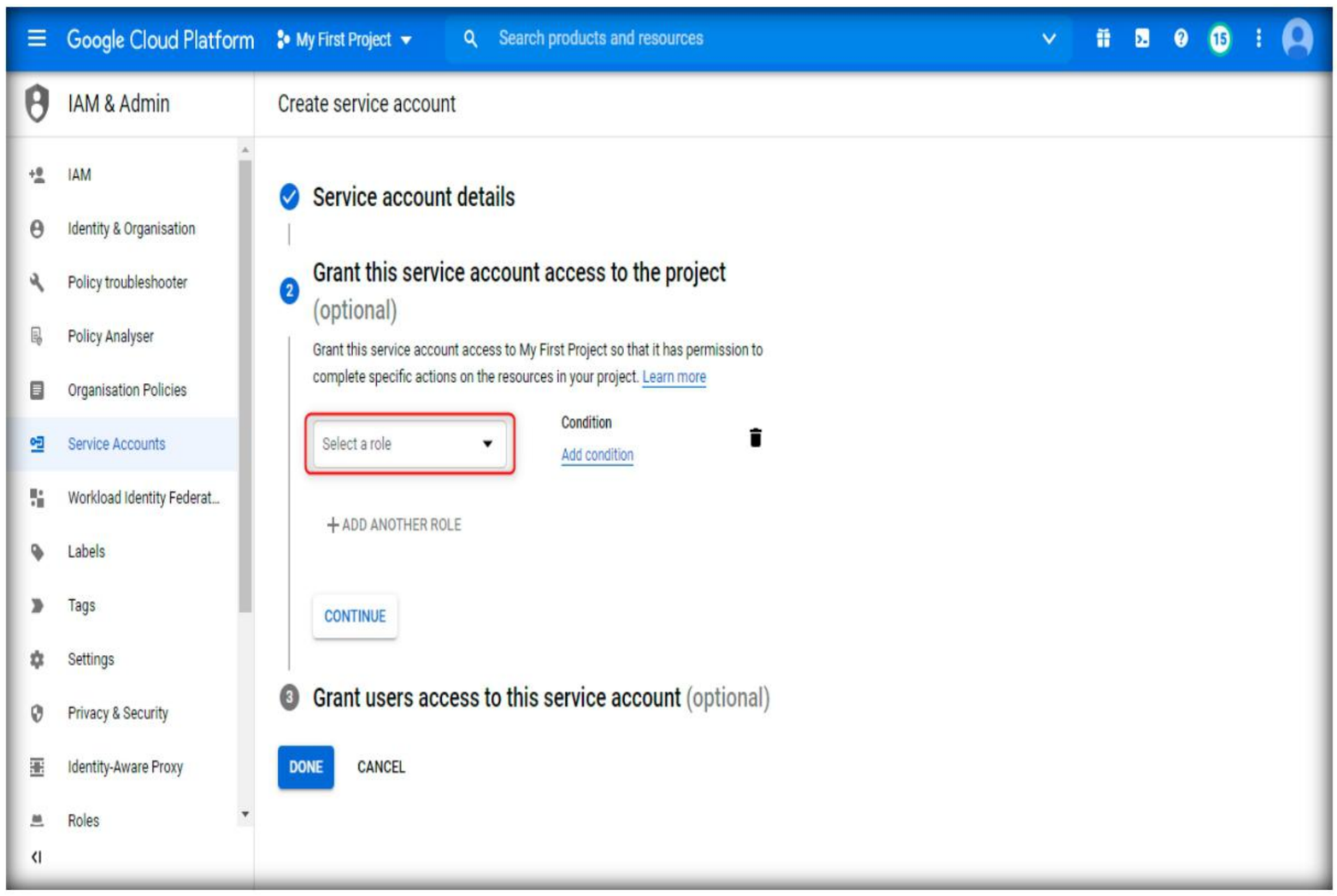


FIGURE 4.13.12: Adding Roles

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

13. Scroll down to the bottom to **Cloud DLP** and select **DLP User** as the role. Click on **CONTINUE.**

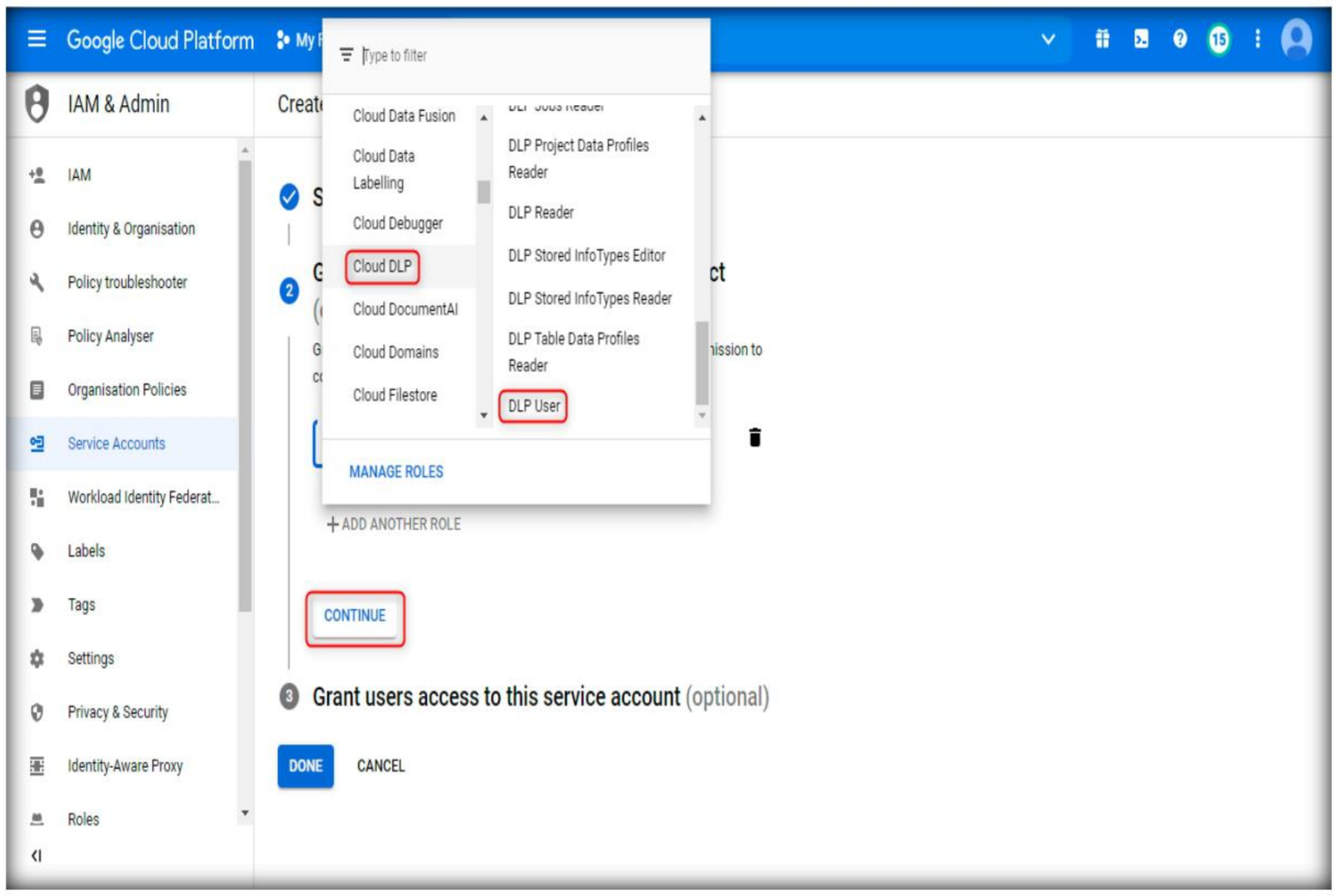


FIGURE 4.13.13: Selecting Cloud DLP Role

14. Retain the other settings and click on **DONE** to create the service account.

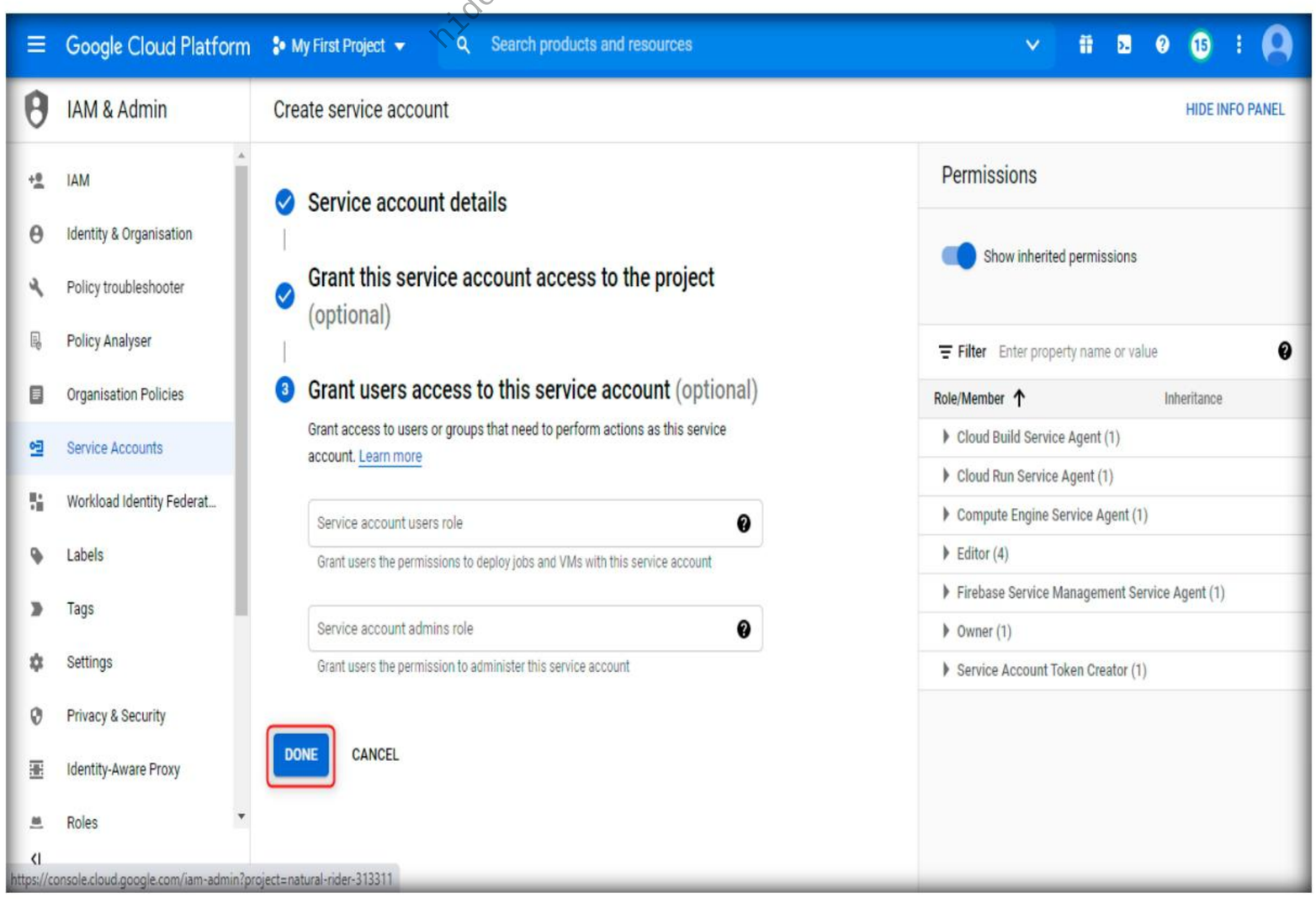


FIGURE 4.13.14: Finish creating service account

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

15. Now, you need to create keys for the service accounts. Click on the **three dots** on the right side of the newly created service account and select **Manage Keys**.

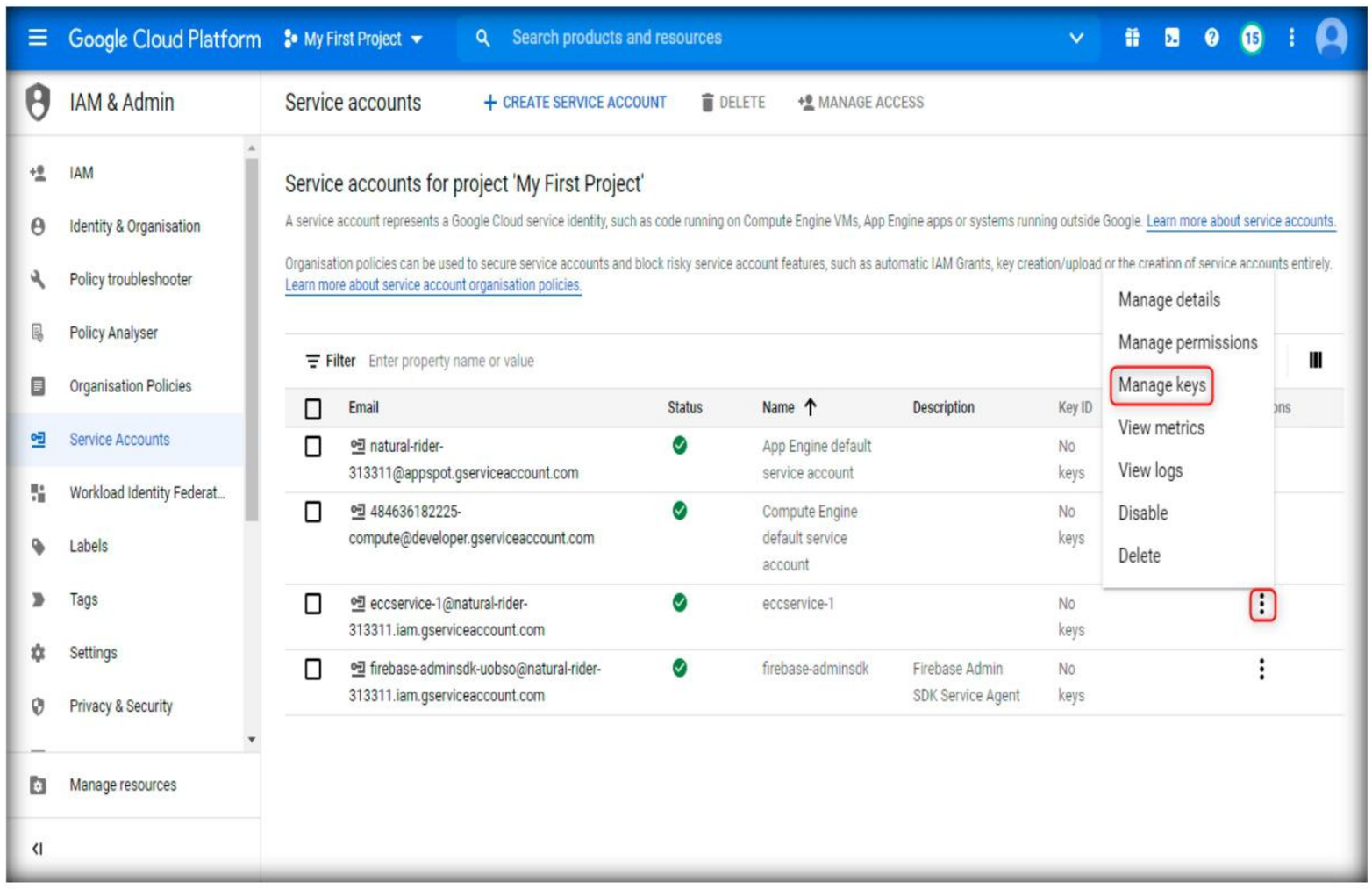


FIGURE 4.13.15: Creating Keys

16. In the **Keys** window that appears, click on **ADD KEY** and select **Create new key**.

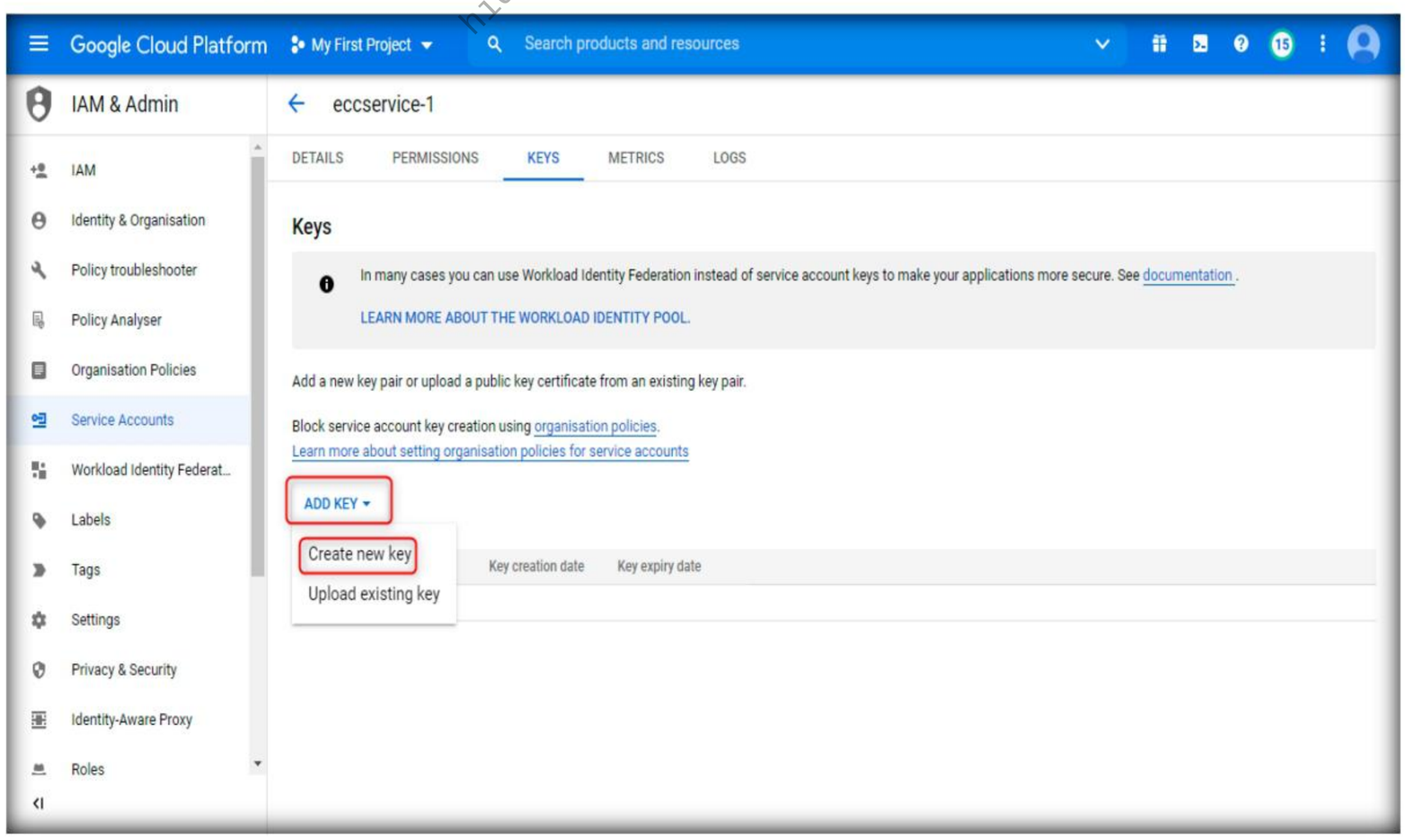


FIGURE 4.13.16: Creating new Key

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

17. A popup window shows **Create private key** for **Key type**. Here, select **JSON** and click on **CREATE**.

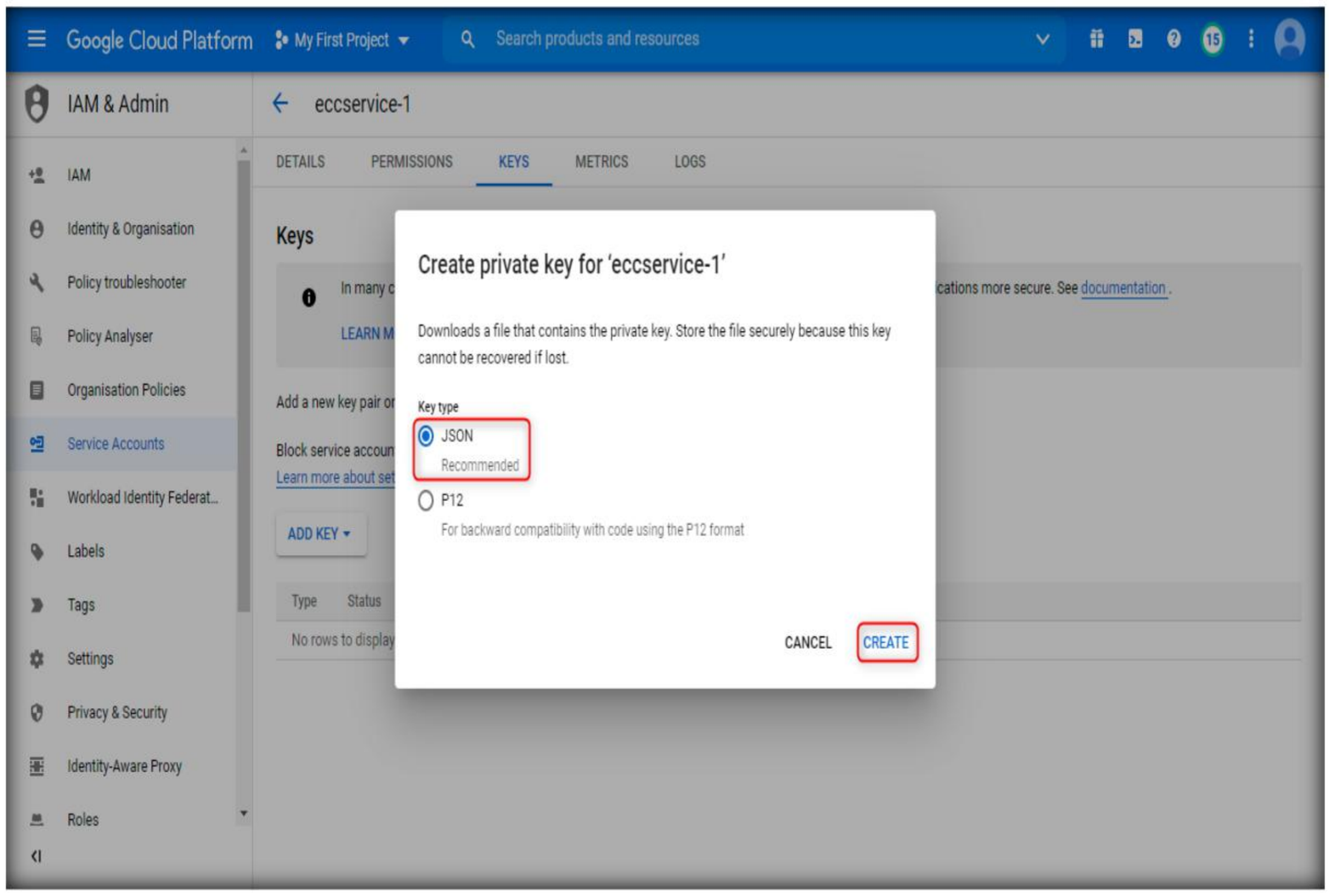


FIGURE 4.13.17: Creating the Private Key

18. A private key will be downloaded to your local machine.

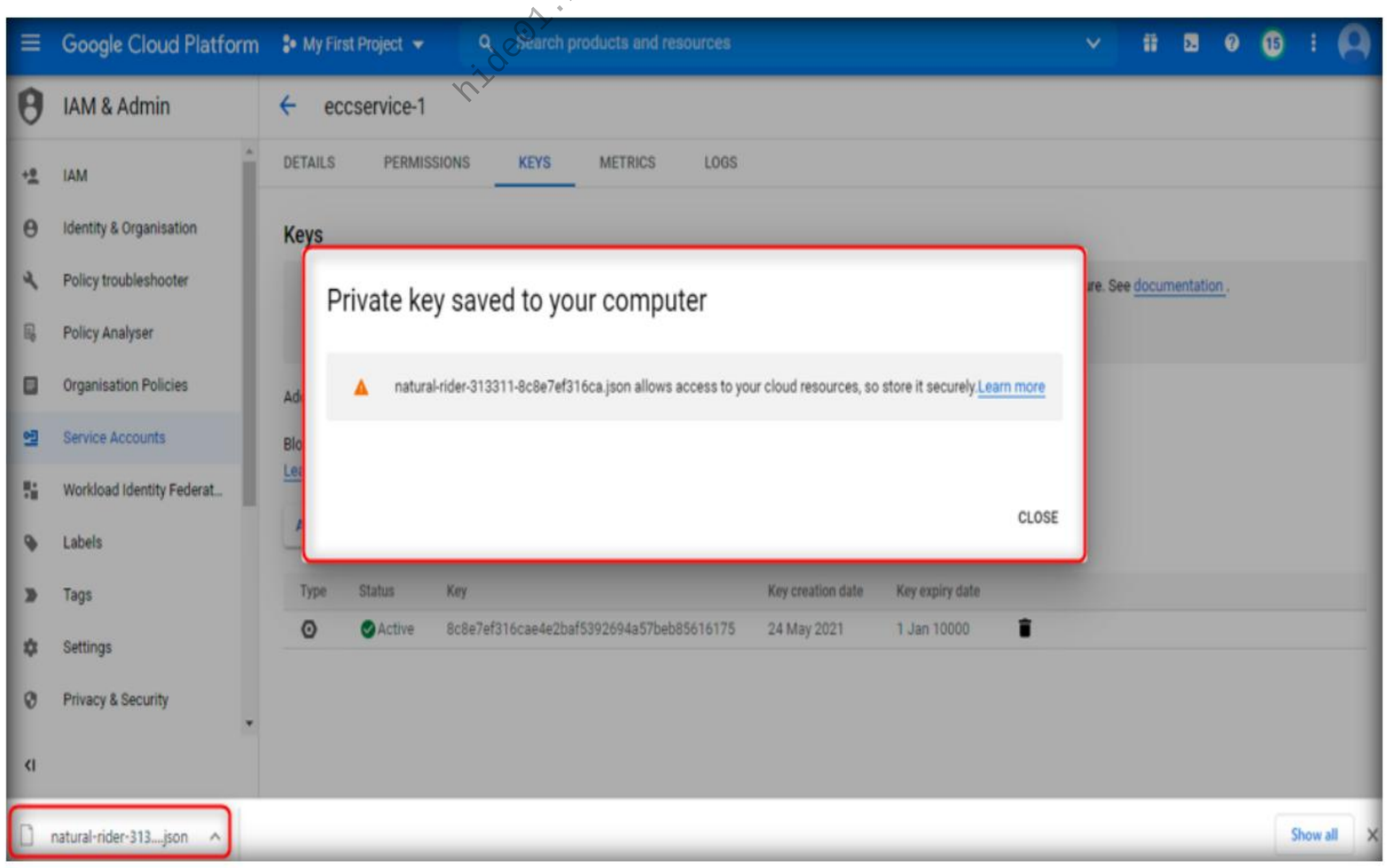


FIGURE 4.13.18: Downloading the Private Key

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 3

Downloading DLP API Files and inspecting string for sensitive information

19. Next, download the DLP API files, install the dependencies, and inspect a string for sensitive information.
20. Click on the **Activate Cloud Shell** icon at the top right corner of the GCP console.

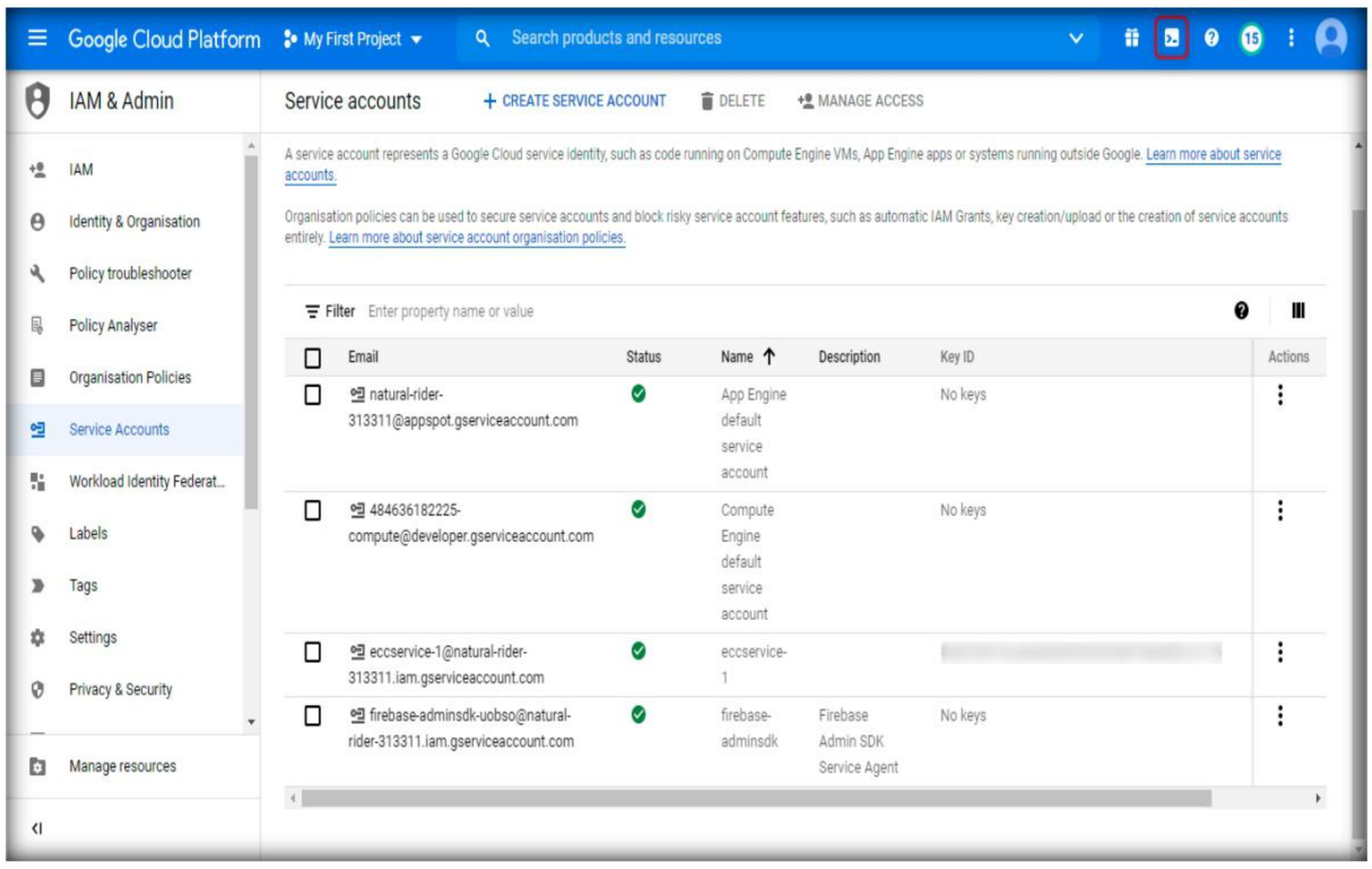


FIGURE 4.13.19: Selecting Service

21. Now, to open **Cloud Shell** in a new window, click on the **Open in new window** icon at the top right corner of **Cloud Shell** terminal.

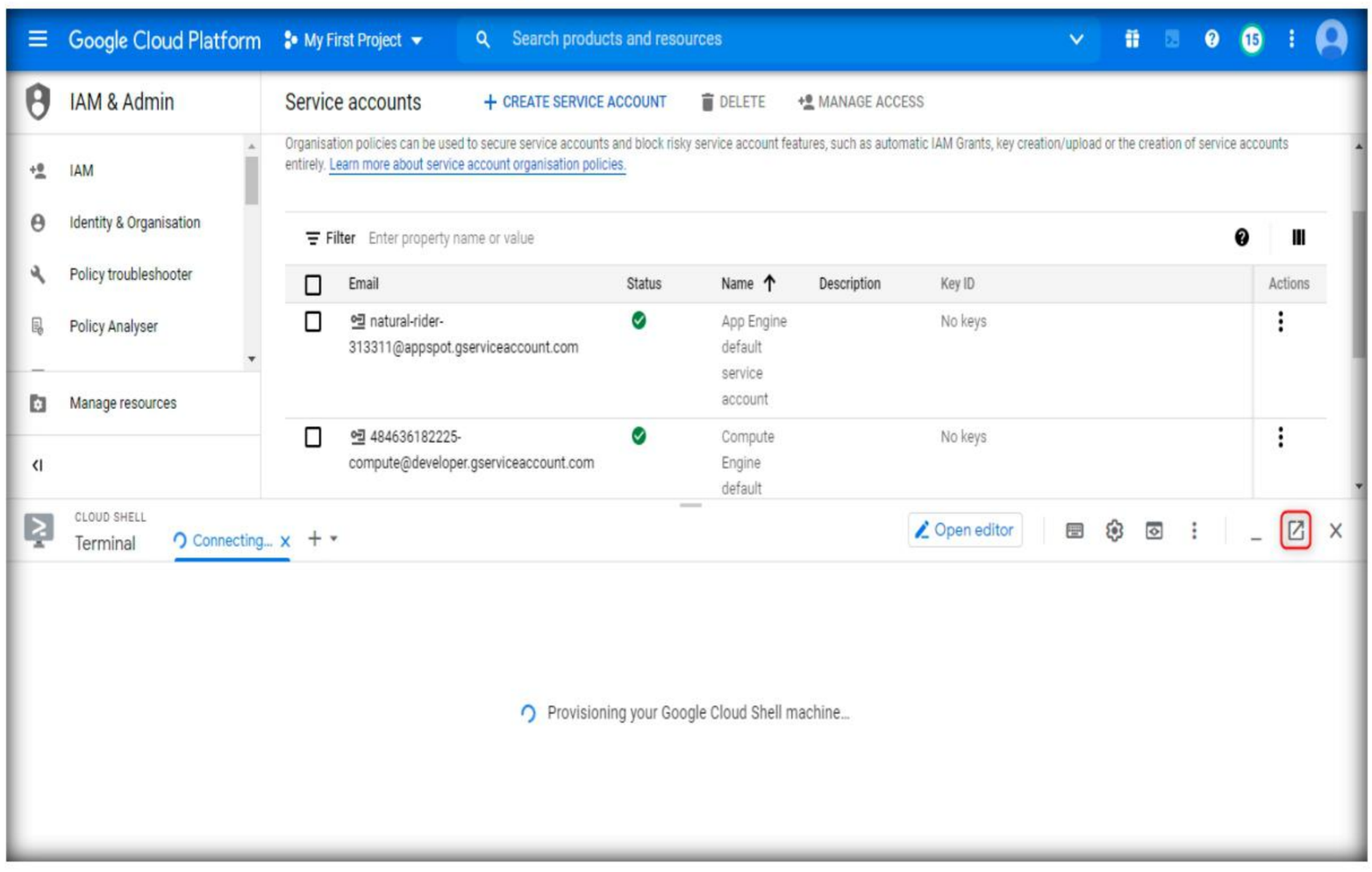


FIGURE 4.13.20: Opening Cloud Shell in new window

Certified Cloud Security Engineer Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

22. Now, in the **Cloud Shell** window, type the following command to list the projects.

    `gcloud projects list`

    Note: If a **Authorise Cloud Shell** window pops up, click on **Authorise**.

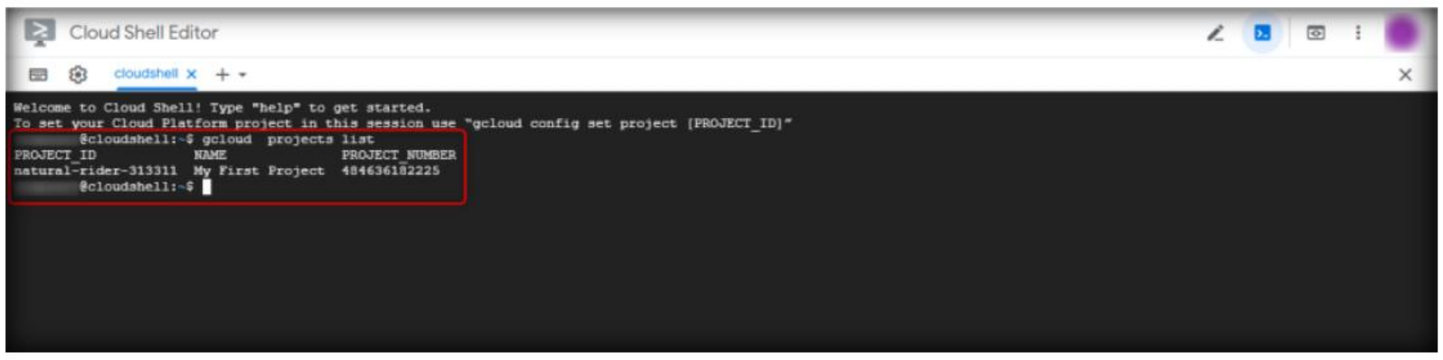


FIGURE 4.13.21: Listing Projects

23. Now, to set the GCP project named **My First Project** in the current session, type the following command and press **Enter**.

    `gcloud config set project [project_ID]` (replace `[project-ID]` with the project ID of your project).

    Here, we have used the following command:

    `gcloud config set project natural-rider-313311`

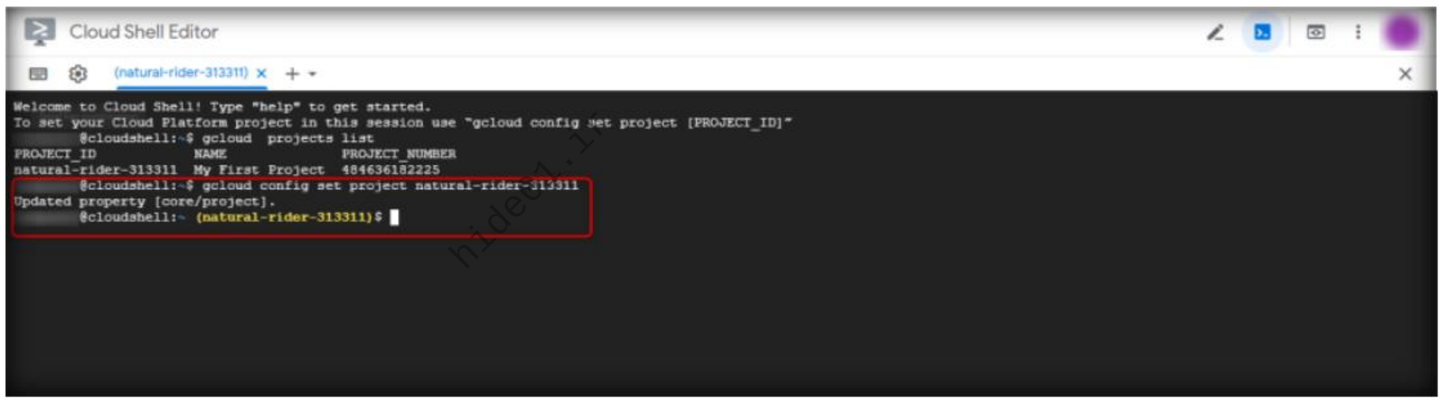


FIGURE 4.13.22: Setting GCP Project

24. Next, upload the JSON private key file you created. To do this, click on the **three dots** on the top right corner of the **Cloud Shell** terminal. Then, select **Upload File**.

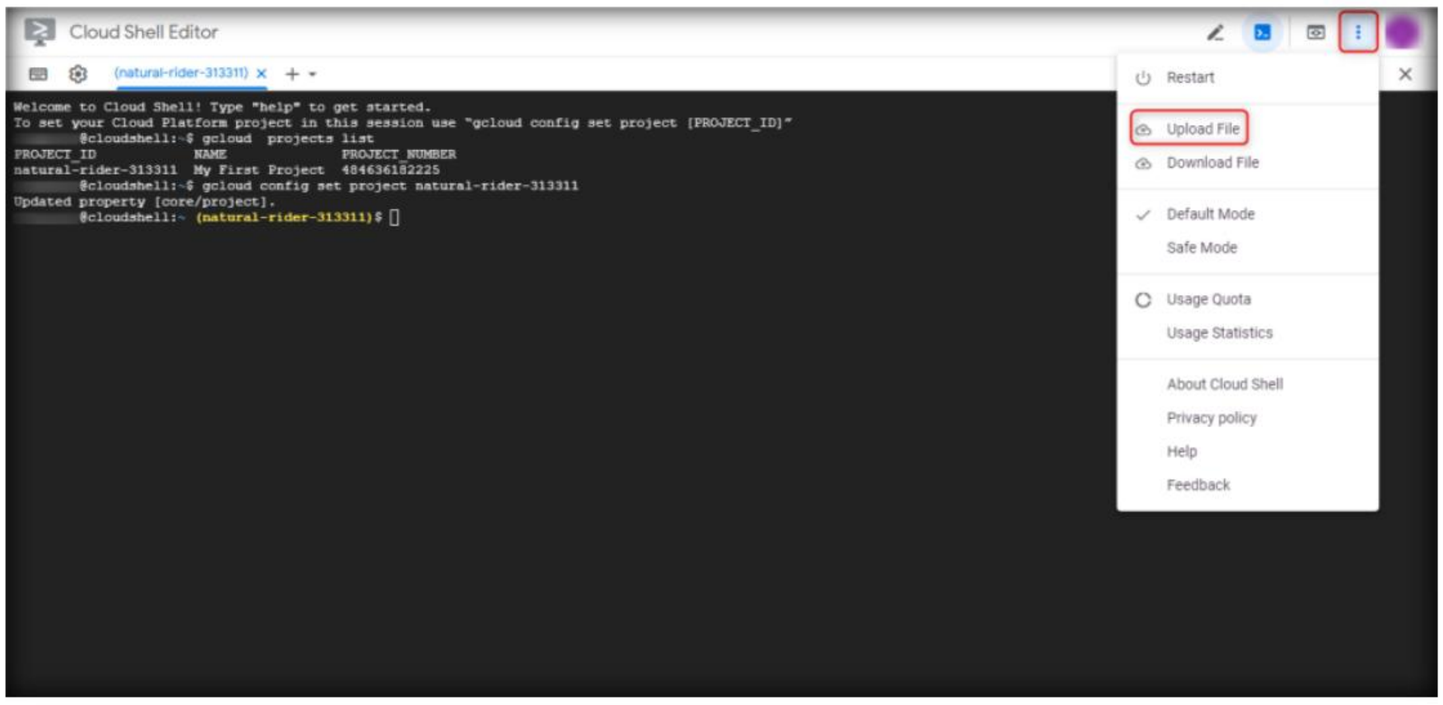


FIGURE 4.13.23: Creating Cluster

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

25. Select the JSON file from the local VM and click **Open**.

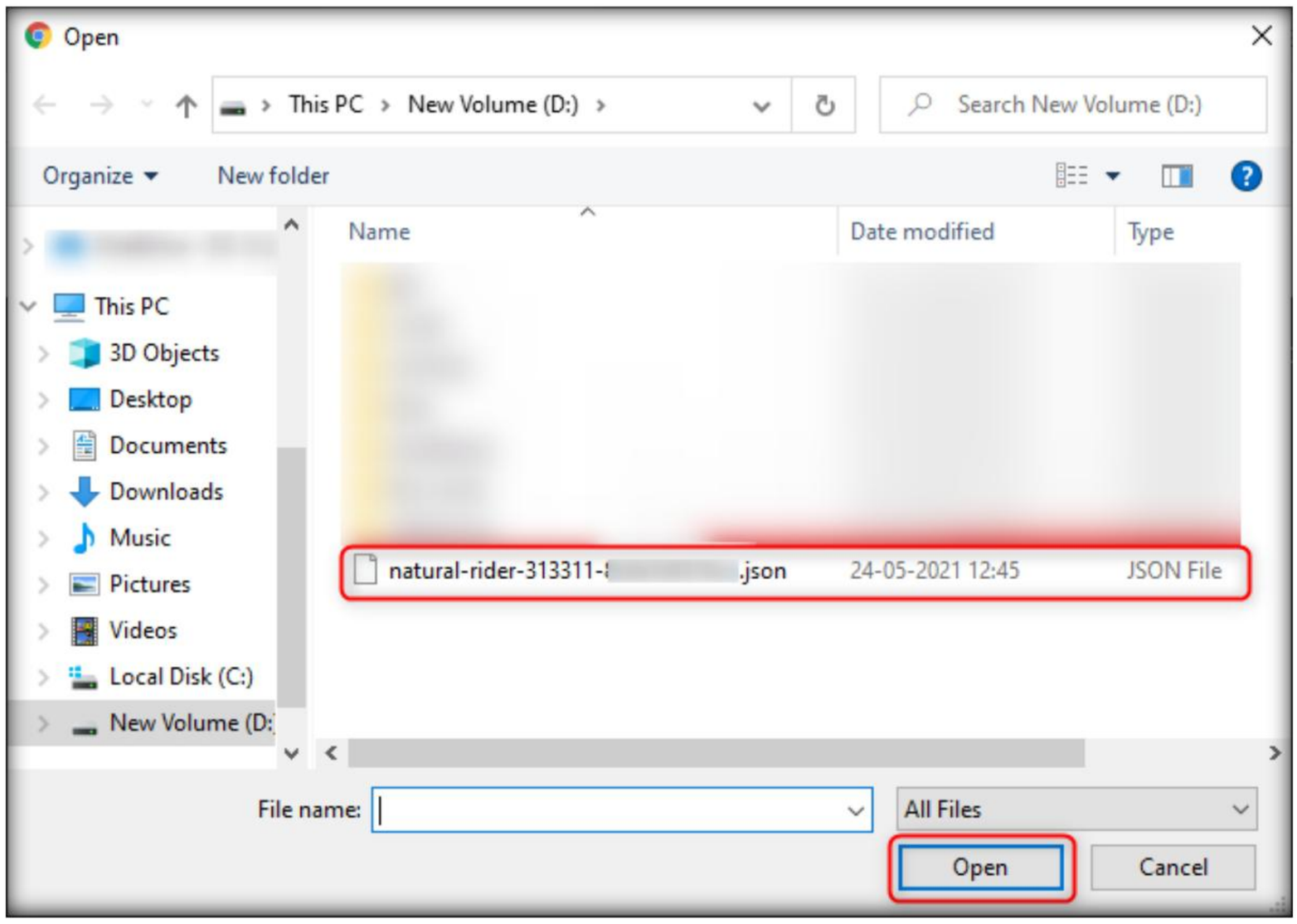


FIGURE 4.13.24: Uploading JSON File

26. Now, set the environment variable to point to the JSON file you uploaded. To do this, type the following command and press **Enter**.

```
export GOOGLE_APPLICATION_CREDENTIALS=~/<name
of JSON file>
```

Note: Replace the `<name of JSON file>` with the name of your JSON file.

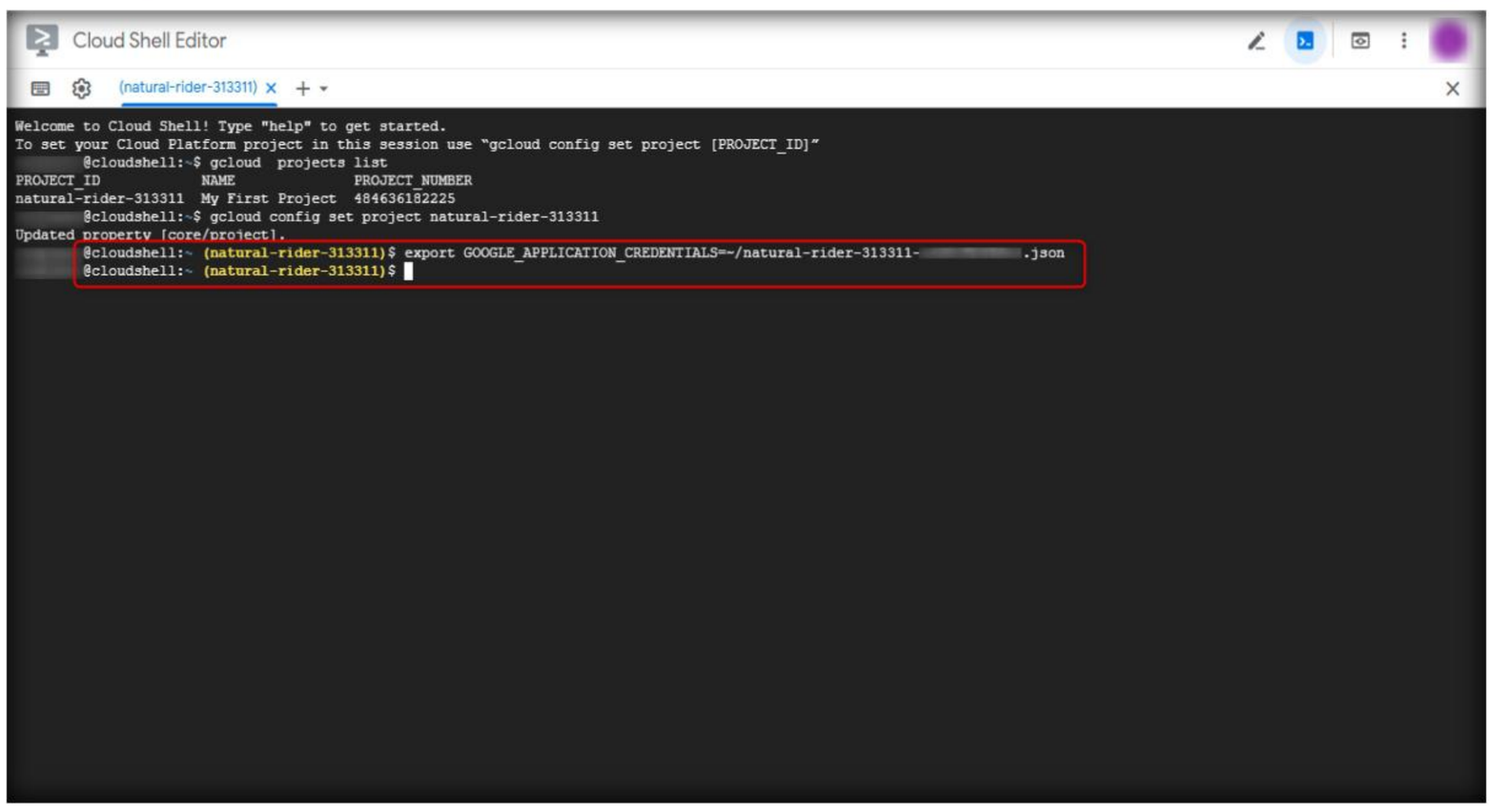


FIGURE 4.13.25: Pointing JSON File

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

27. Next, download the DLP API files. To do this, type the following command to clone the NODE JS DLP repository and press **Enter.**

```
git clone https://github.com/googleapis/nodejs-dlp.git
```

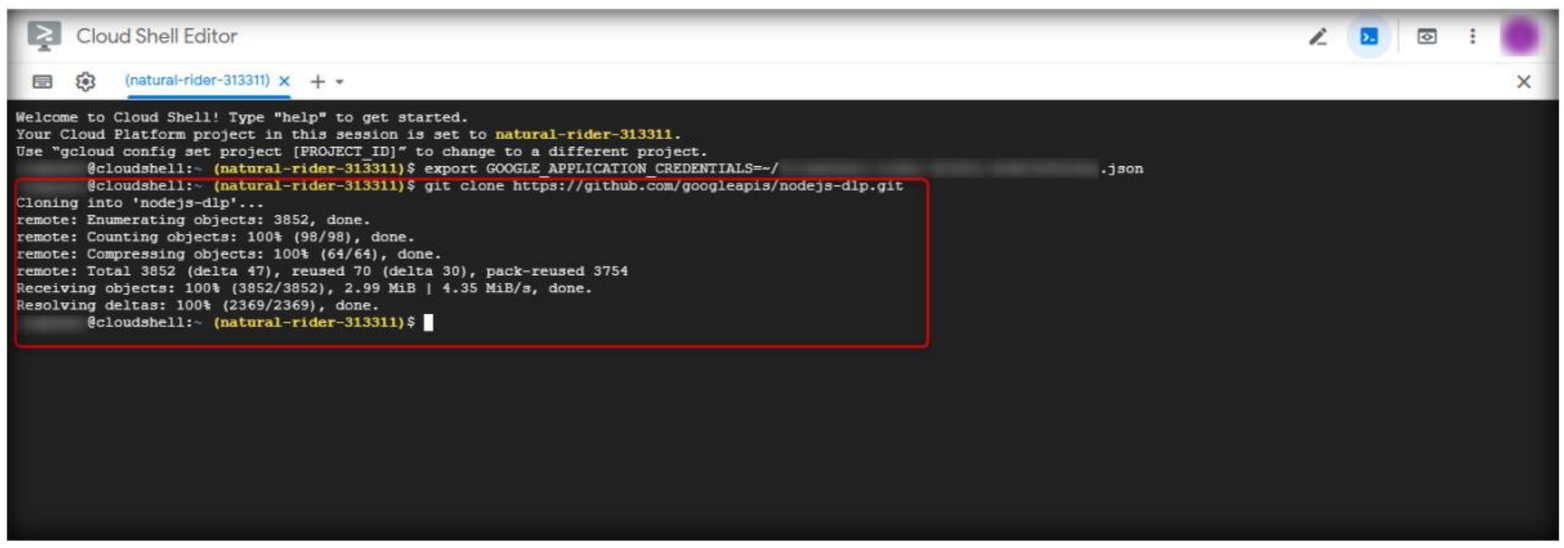


FIGURE 4.13.26: Cloning NODE JS DLP repo

28. Now, to open the directory of **nodejs-dlp/samples**, type the following command and press **Enter**.

```
cd nodejs-dlp/samples
```

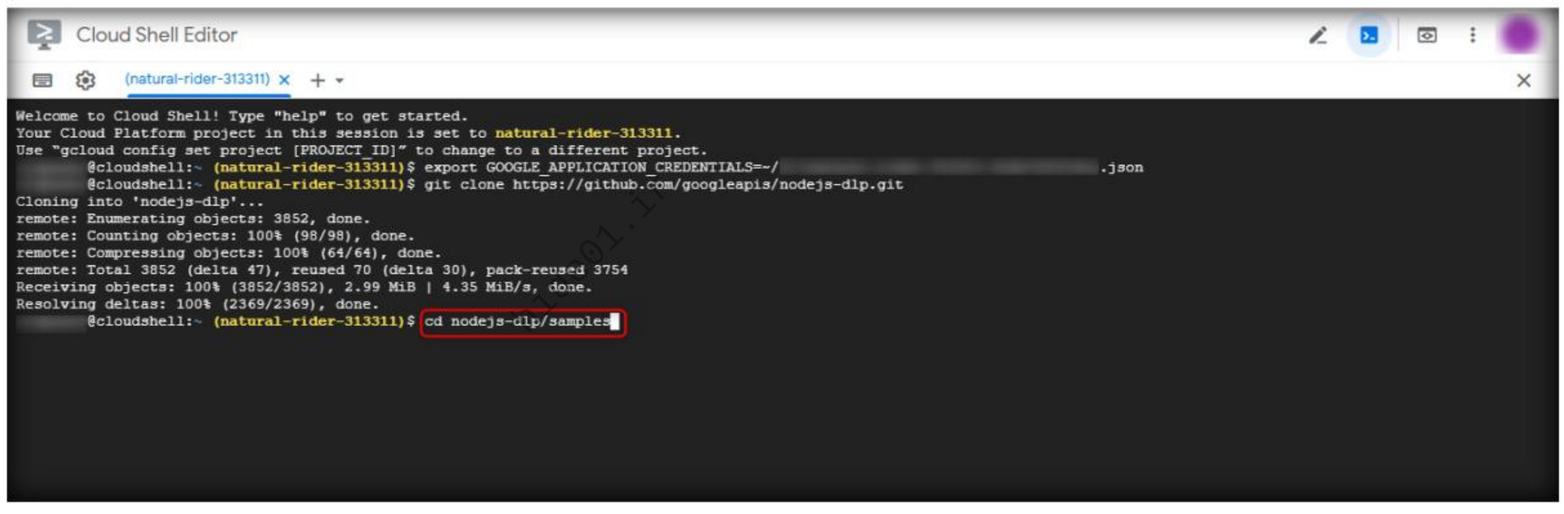


FIGURE 4.13.27: Navigating to the directory

29. Next, install the dependencies. To do this, type the following command and press **Enter**.

```
npm install
```

Note: You can clear the screen at any time by running the **clear** command.



FIGURE 4.13.28: Installing Dependencies

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

a. Next, set the environment variable **GCLOUD_PROJECT** to the **GCP Project ID**. To do this, type the following command and press **Enter** to set the environment variable.

`GCLOUD_PROJECT=<PROJECT_ID>` (replace `<PROJECT_ID>` with your project ID)

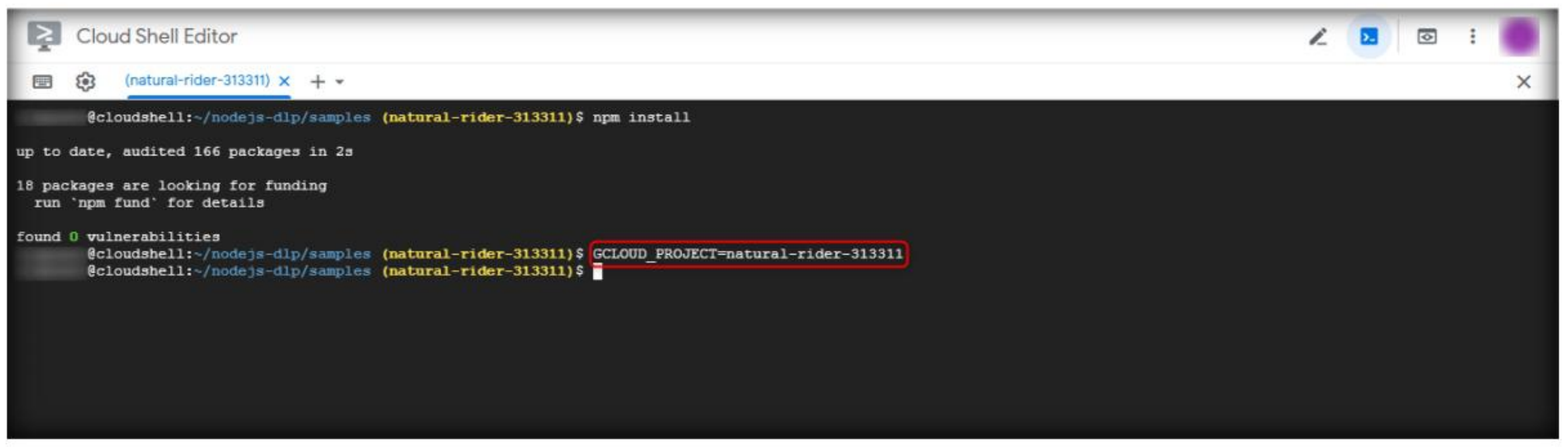


FIGURE 4.13.29: Setting environment Variable

30. Now, you can inspect a string of data for sensitive information. First, you can inspect the string **"My phone number is +9999999999"** for sensitive information. To do this, type the following command and press **Enter**.

`node inspectString.js natural-rider-313311 "My phone number is +9999999999."`

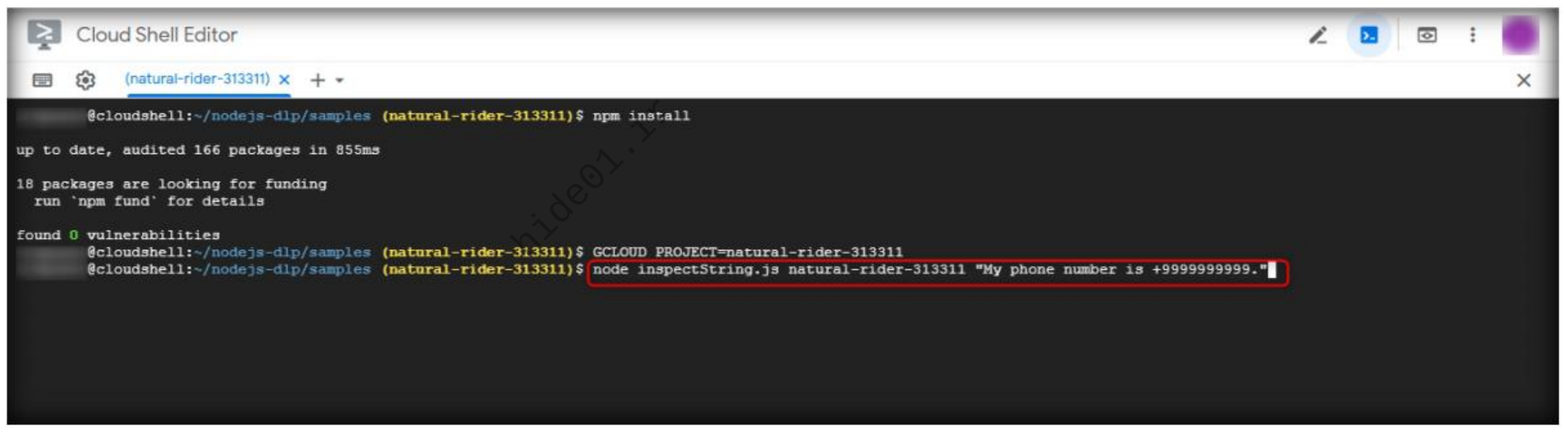


FIGURE 4.13.30: Inspecting the string

31. You will see the **Findings** of the inspected string, which includes info type and match likelihood, as shown below.

`Info type: PHONE_NUMBER` (which indicates there is a telephone number in the given string)

`Likelihood: Likely` (indicating a likelihood that the data matches the PHONE_NUMBER info type)

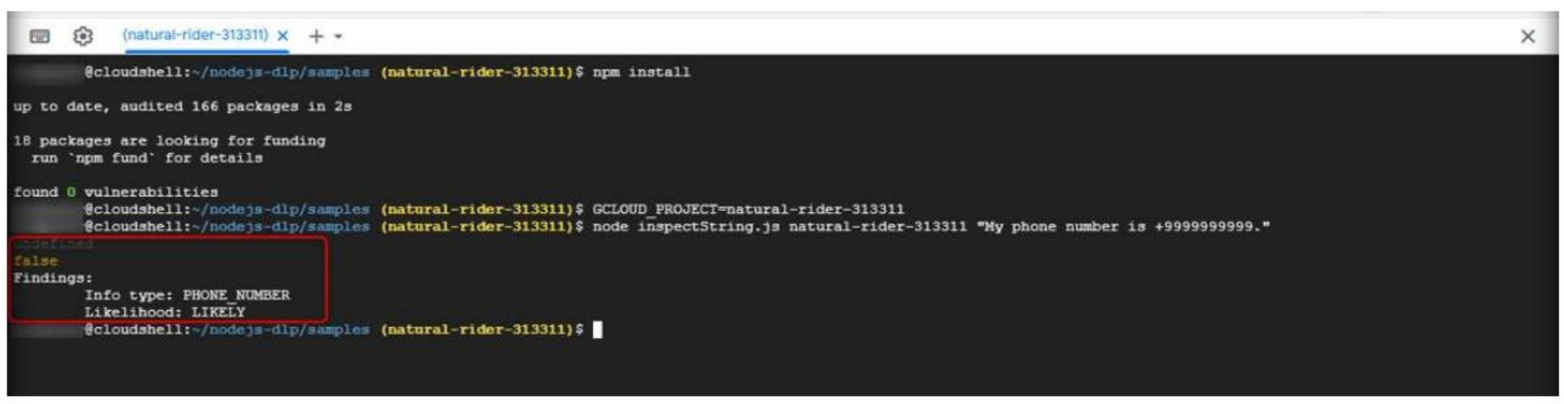


FIGURE 4.13.31: Findings of inspected string

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

32. Next, inspect another string of data for sensitive information. Inspect the string **"My email id is john@eccdemo.com."** for sensitive information by typing the following command and pressing **Enter**.

```
node inspectString.js natural-rider-313311 "My email
id is john@eccdemo.com."
```

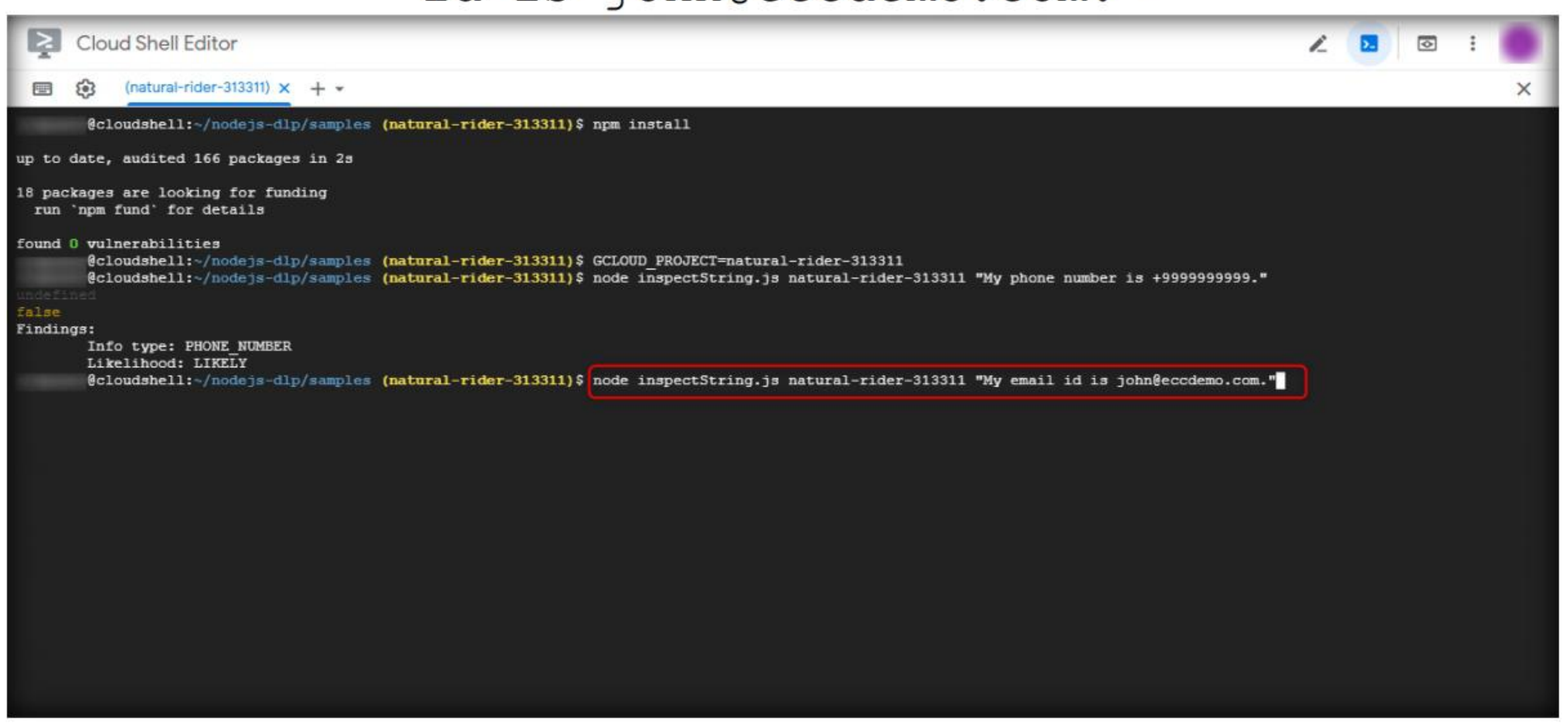


FIGURE 4.13.32: Inspecting for Sensitive Data

33. Here, you will get two types of **Findings,** info type and match likelihood of the string, as shown below.

    `Info type: PERS ON_NAME` (indicating the presence of a person's name in the string)

    `Likelihood: POSSIBLE` (indicating a possible data match for PERSON_NAME info type)

    `Info type: EMAIL_ADDRESS` (indicating an email address is present in the string)

    `Likelihood: VERY_LIKELY` (indicating the data very likely matches the EMAIL_ADDRESS info type)

hadeo1.ir

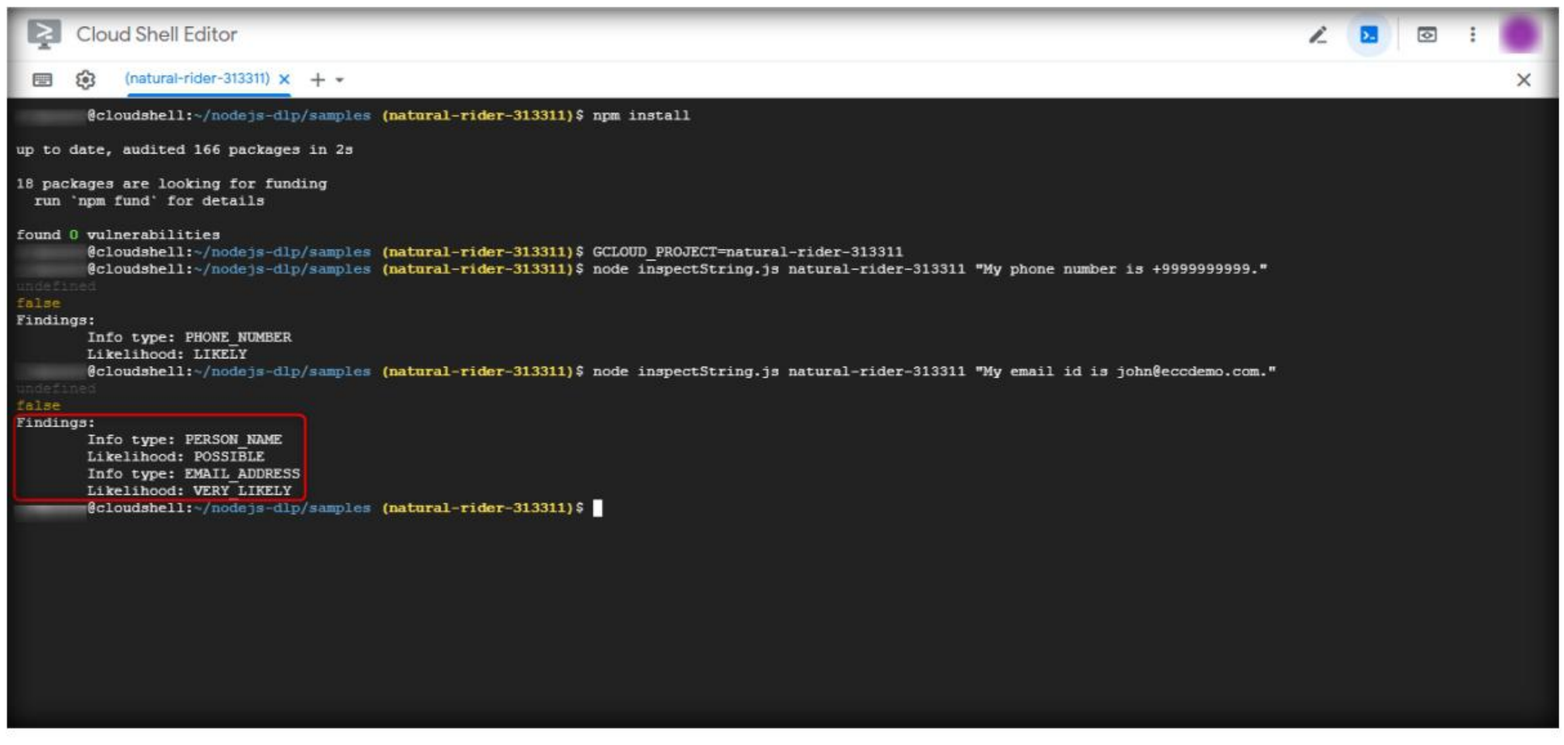


FIGURE 4.13.33: Findings of Inspected String

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

34. As described above, a cloud security professional can scan a string of information for sensitive data using Cloud DLP API.

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

35. To delete the **NODE JS DLP** repository, type the following command and press **Enter**.

```
rm -rf nodejs-dlp.git
```

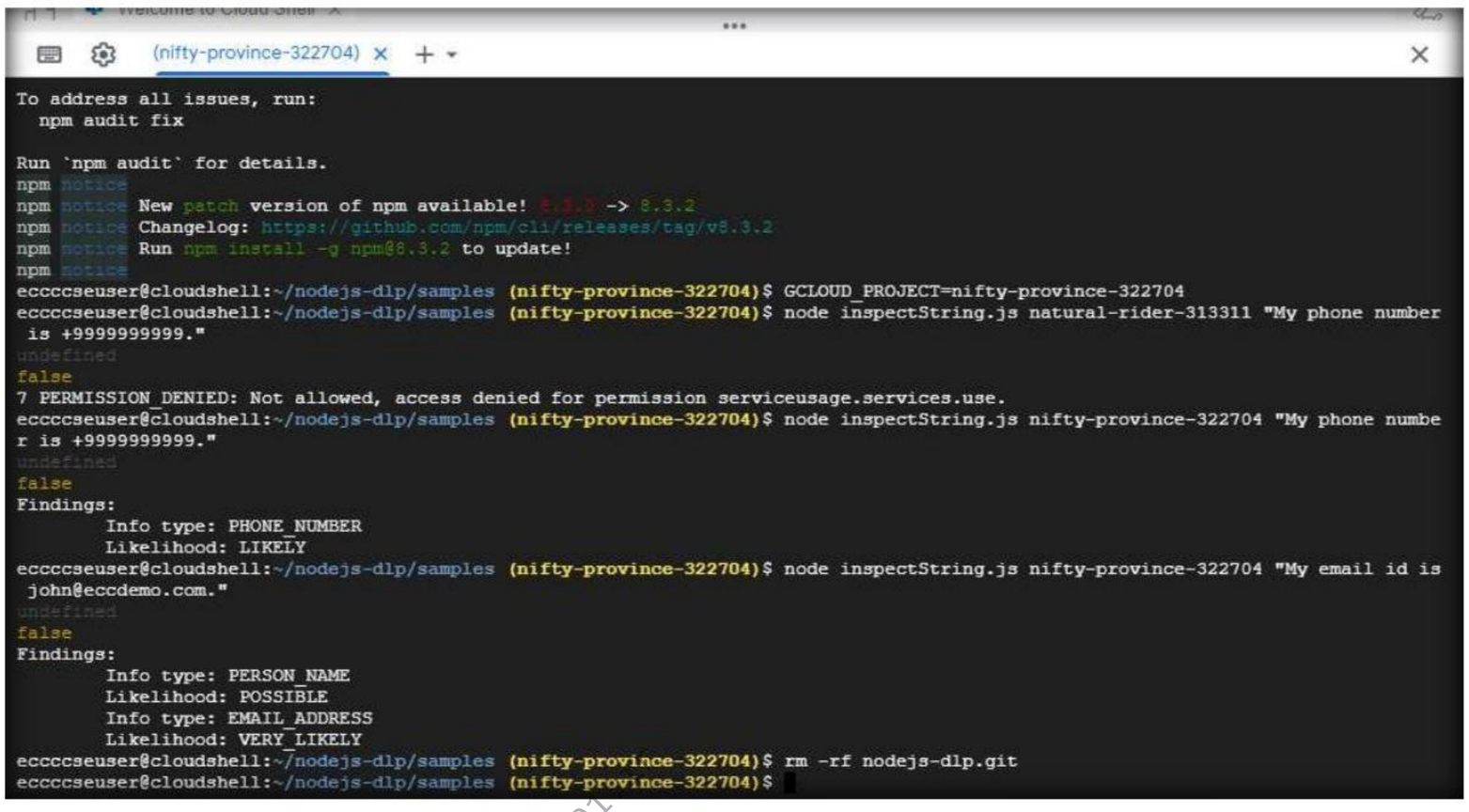


FIGURE 4.13.34: Deleting NODE JS DLP repository

36. Next, to delete the service account for Cloud DLP that you have created, navigate to **IAM & Admin** and select **Service Accounts** in the console. Select the checkbox for the service account (**eccservice-1**) and click on **DELETE**.

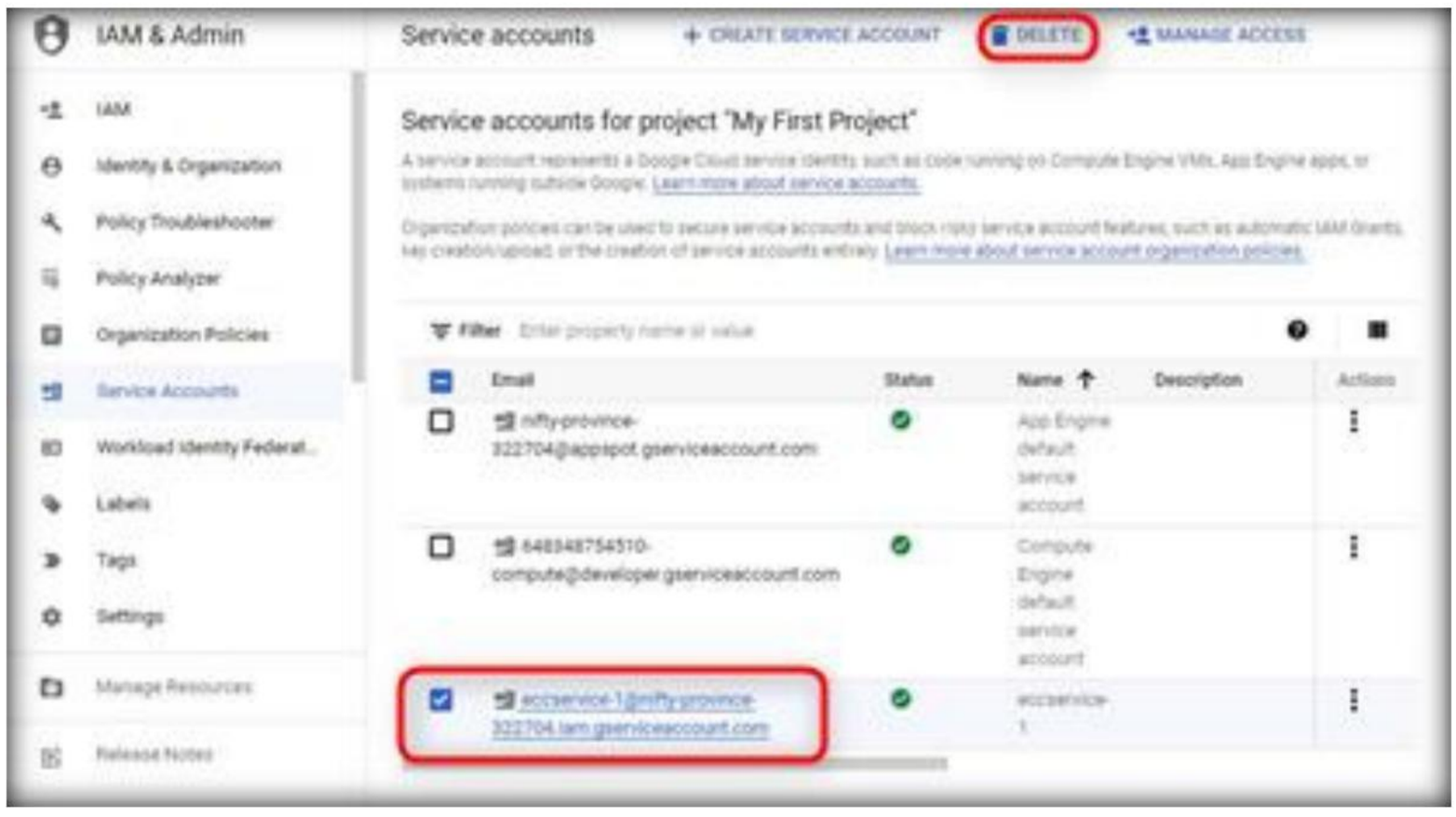


FIGURE 4.13.35: Deleting Service Account

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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.

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

This page is intentionally left blank.

hide01.ir

Security Operations in Cloud

hide01.ir

Module 05

Caution: Completing the steps in this exercise will require you to sign up for third party services that may incur fees. Be sure to follow proper guidelines for removing billable services from your account before you leave your lab. Deviating from our specific instructions may result in unwanted fees for services from third-party service providers. Be sure to check with your school, instructor, or employer if education accounts are available. If you sign-up and provide your credit card, you will be responsible for any fees related to services you activate. We strongly advise you not to deviate from our explicit instructions while connected to the platforms unless you are fully aware of what the services are and what the respective third-party charges for their use.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 1

Discovering Potential Security Issues using Amazon Inspector

Amazon Inspector is a security assessment service by AWS that utilizes automation to assess a cloud deployment for security vulnerabilities and provides the best security recommendations.

Lab Scenario

Amazon Inspector enables cloud security engineers to check for vulnerabilities in the applications deployed on AWS. It can be used to check the network visibility and security vulnerability postures of your EC2 instances.

hide01.ir

ICON KEY

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

Lab Objectives

This lab will demonstrate how to check and discover vulnerabilities in an AWS EC2 instance using the Amazon Inspector API console.

In this lab, you will learn to do the following:

- Create an AWS EC2 instance
- Create an assessment to find security issues

Lab Environment

To perform this lab, you need the following:

- **Admin Machine** VM
- **Administrative** privileges to run the tools

Lab Duration

Time: 15 minutes

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Overview of Amazon Inspector

Amazon Inspector is a security assessment service by AWS that utilizes automation to enhance application security. It can automatically check applications for any type of vulnerabilities or deviations from best practices. Security vulnerabilities are listed according to their severity levels in Amazon Inspector. The entire security of an application can be ensured with Amazon Inspector because it protects the application before deployment and in its running environment. Amazon Inspector provides a functionality to enforce the best security standards and policies for an application. It can check for an application's vulnerabilities or network accessibility issues. AWS Inspector has a database consisting of several rules that can be updated by security researchers.

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., AWS), the application interface may be updated with time. Hence, in case you happen to work on an updated version of AWS, 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 exercise, you should create an AWS account using the following link: https://portal.aws.amazon.com/billing/signup. Once the registration is complete, then perform the following tasks.

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

TASK 1

Creating an AWS EC2 Instance

1. Log in to the **Admin Machine** VM with the user **Admin** and password **admin@123**.

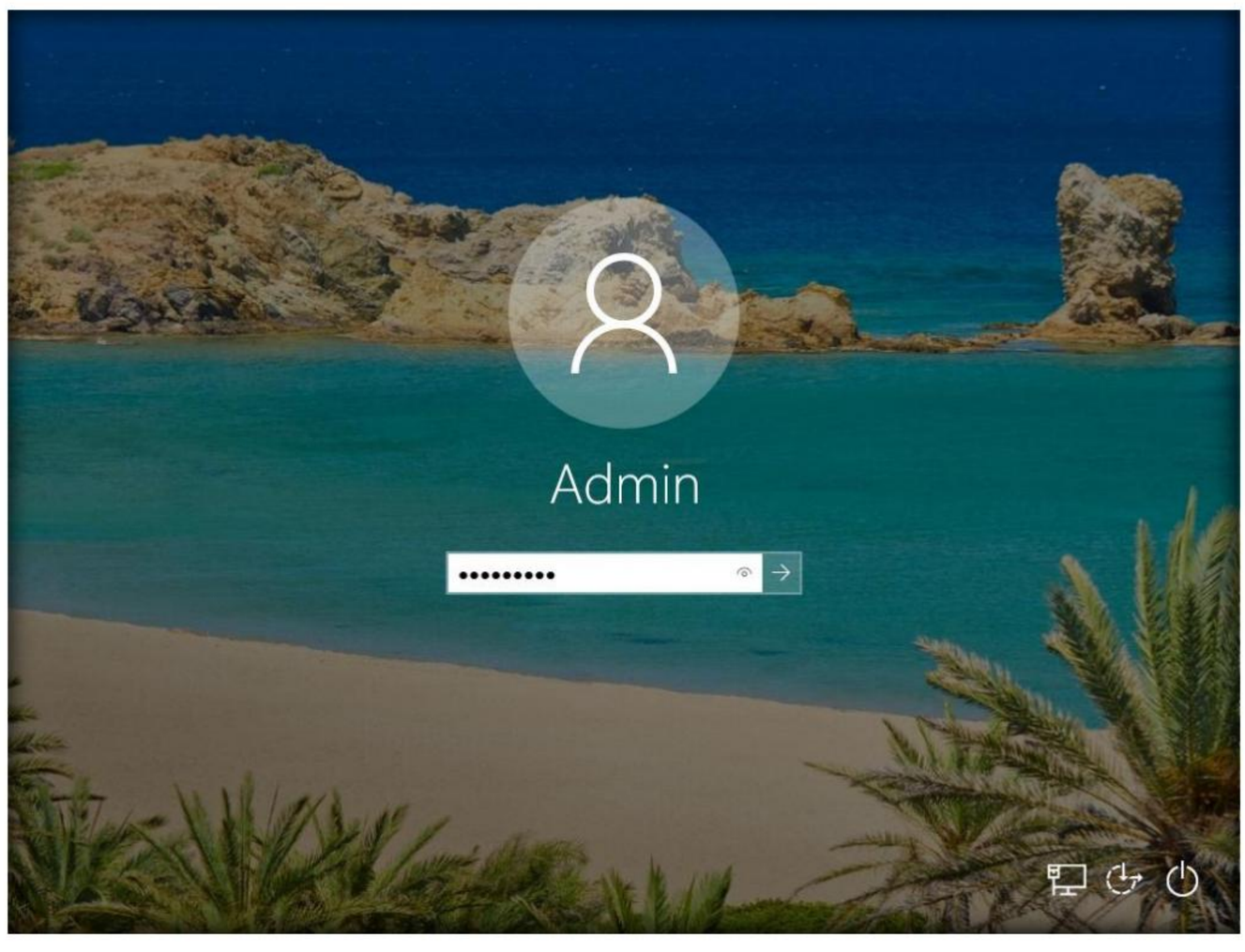


FIGURE 5.1.1: User Login

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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



FIGURE 5.1.2: Navigating to the Chrome Browser from Taskbar

3. The **Google Chrome** browser appears. Go to the address bar, type **https://aws.amazon.com/**, and press **Enter.**

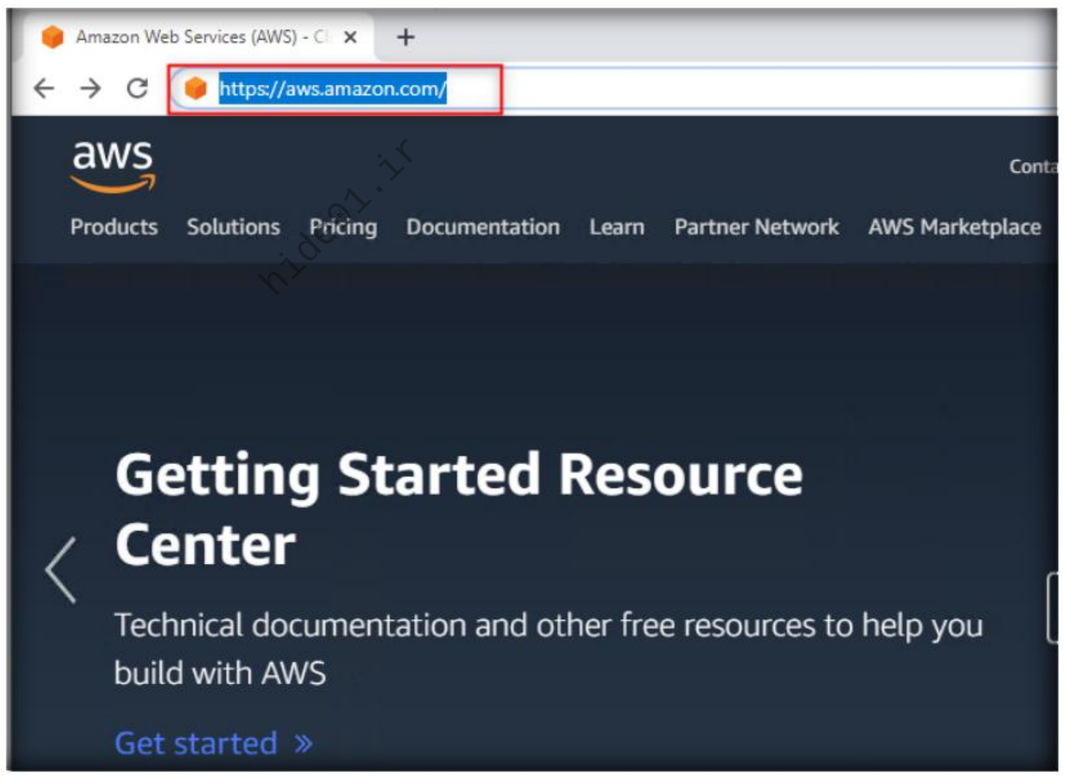


FIGURE 5.1.3: Access AWS in Browser

Note: If you are already logged in, skip the login steps.

4. The **AWS Web Services - Cloud Computing Services** page appears. Click on the **AWS Management Console** from the **My Account** dropdown, as shown in the screenshot below.

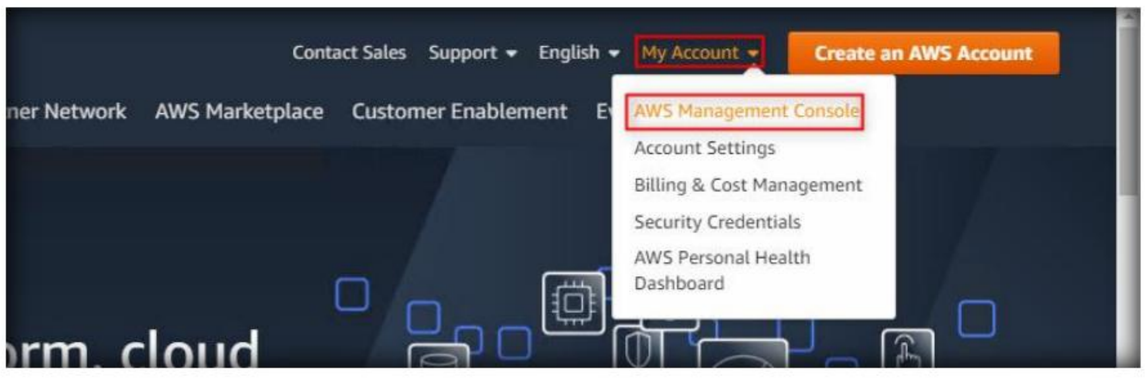


FIGURE 5.1.4: Navigate to AWS Management Console

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

5. The **AWS Web Services Sign-in** page appears. Choose **Root user** and type the AWS administrator account ID (Root user email address), as shown in the screenshot below, and then click on **Next**.

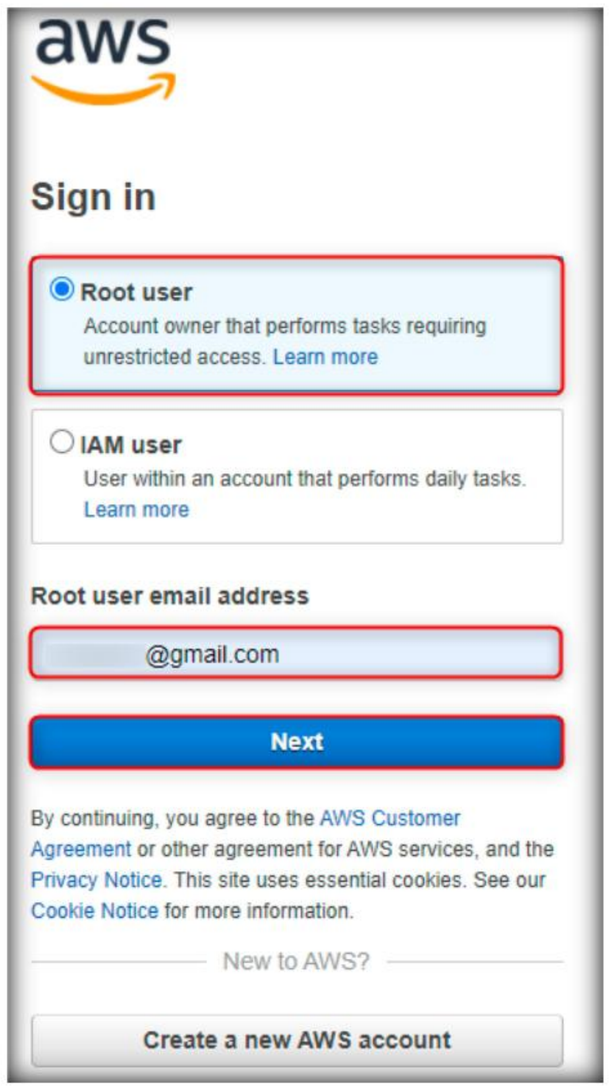


FIGURE 5.1.5: Sign-in to AWS

6. In the security check page that appears, type the characters shown in the image and click **Submit**.

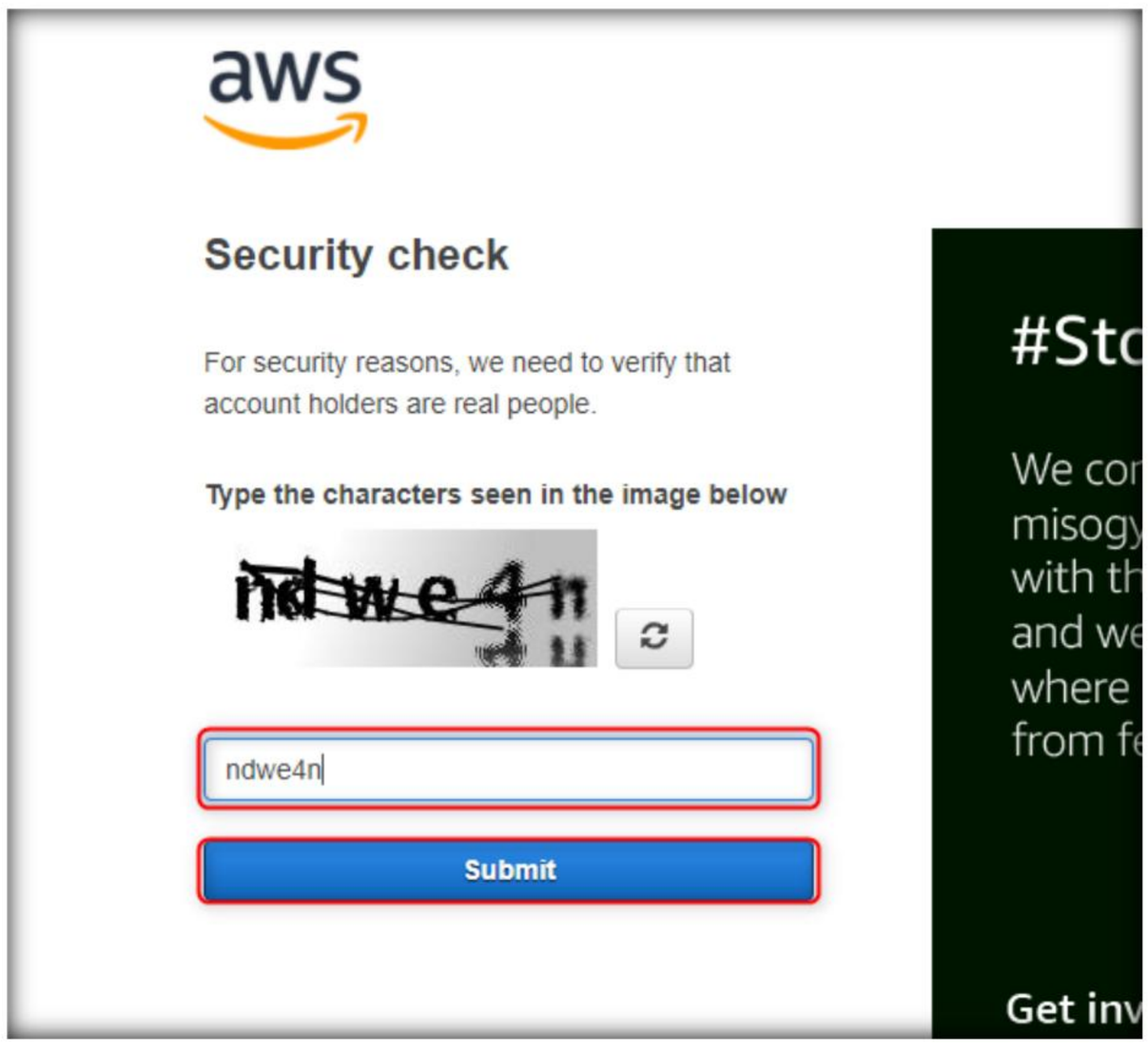


FIGURE 5.1.6: Sign-in to AWS

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

7. In the **Password** field, type the password and click on **Sign in**.

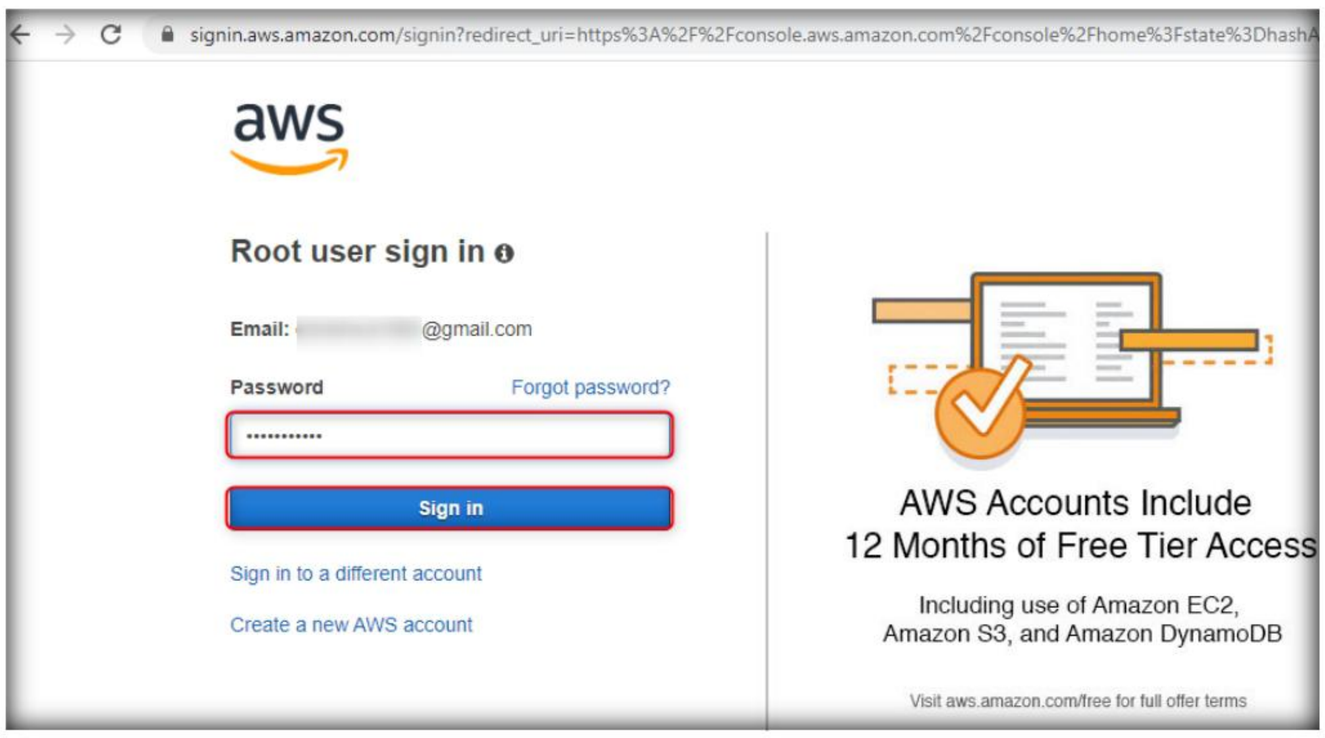


FIGURE 5.1.7: Sign-in to AWS

8. Now, to create an AWS EC2 instance, click on **Services**. Then, select **EC2** under the **Compute** section.

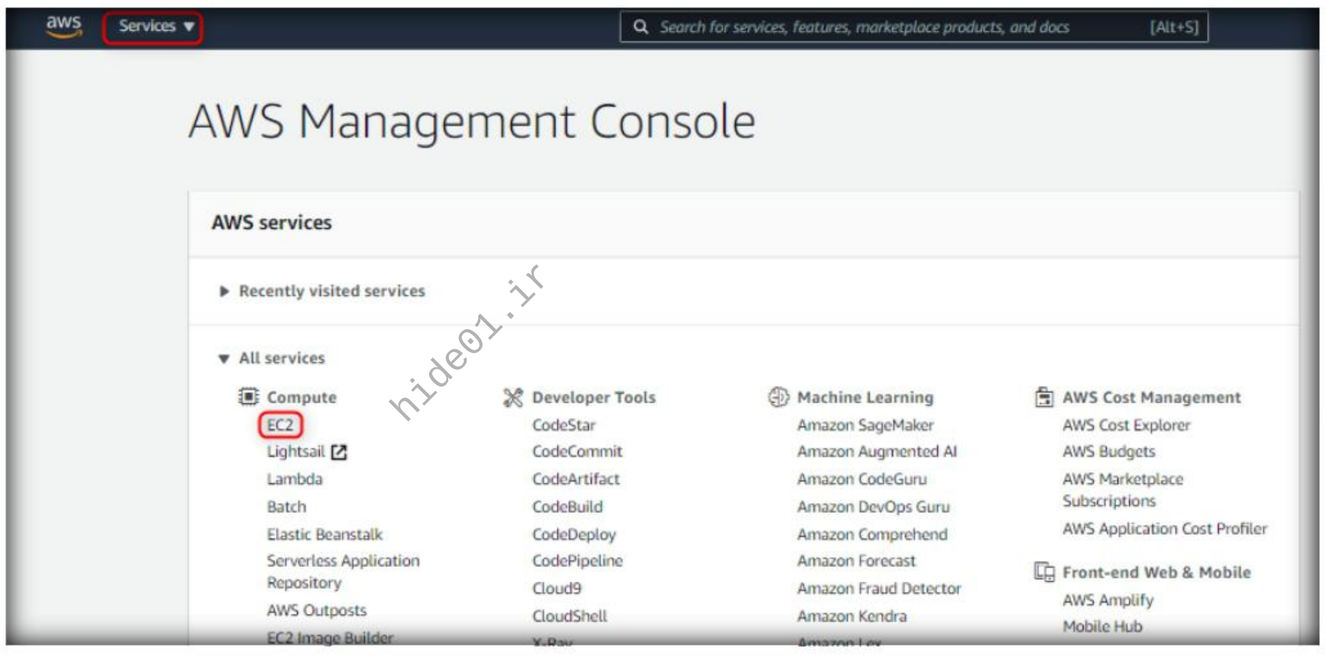


FIGURE 5.1.8: Selecting EC2 Service

9. On the **EC2 Dashboard**, click on **Instances (running)** to create a new EC2 instance.

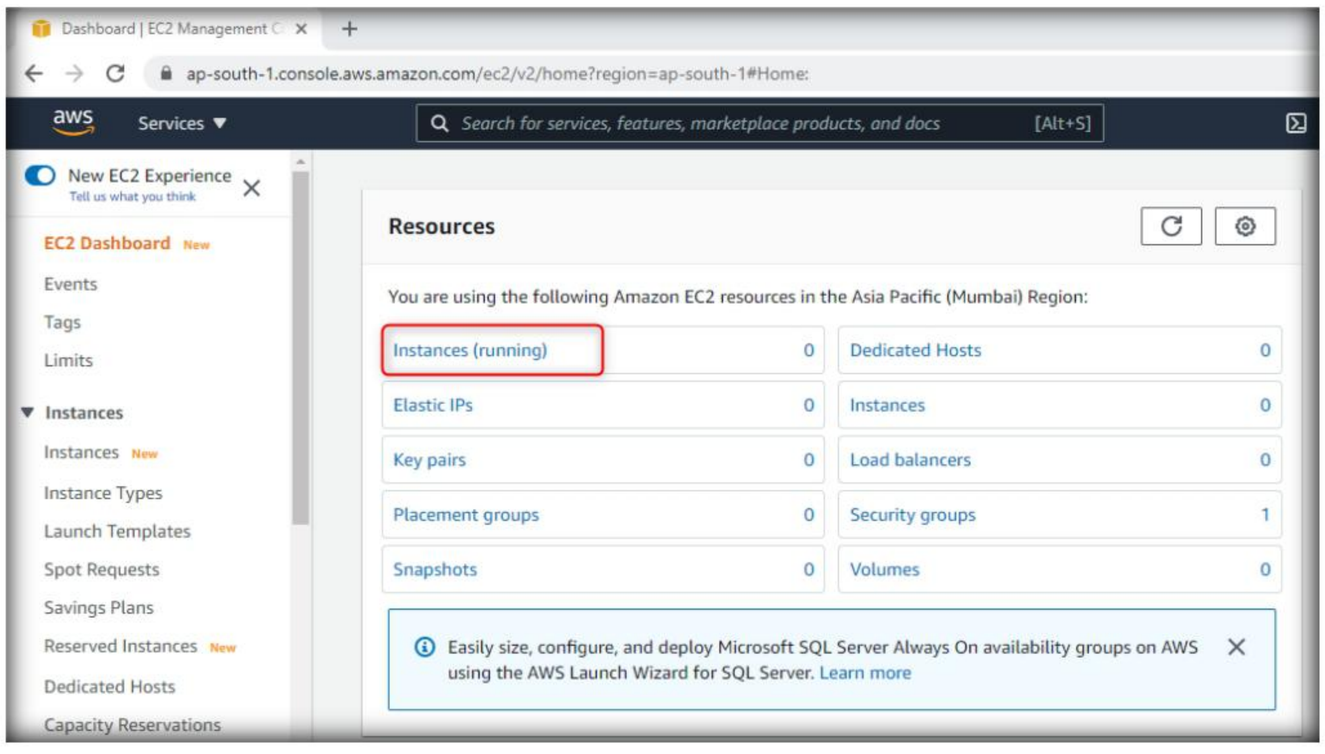


FIGURE 5.1.9: EC2 Dashboard

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

10. On the **Instances** page, click on **Launch instances** to continue.

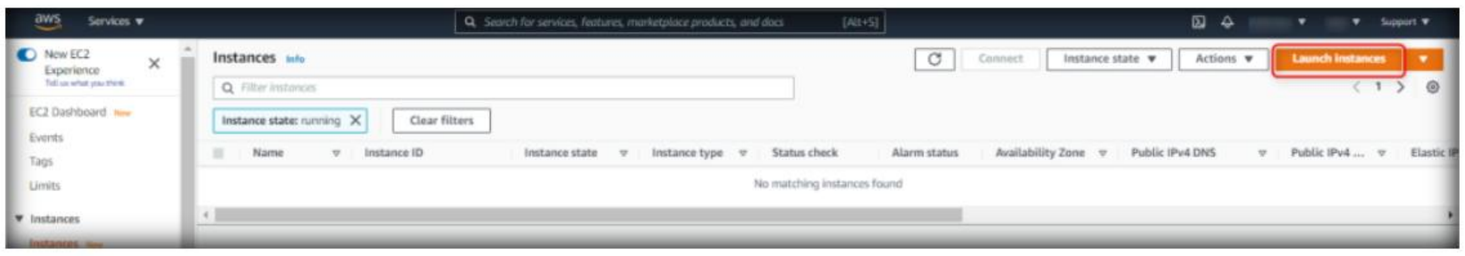


FIGURE 5.1.10: Instances page

11. On the **Choose AMI** page, choose **Amazon Linux 2 AMI (HVM), SSD Volume Type** (as it is eligible for free tier). Click on **Select** to choose Amazon Linux, as shown in the following screenshot.

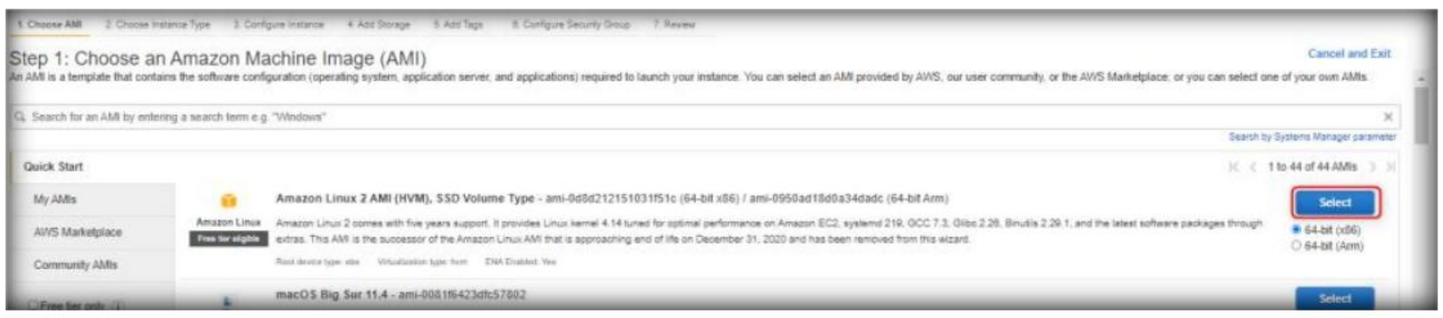


FIGURE 5.1.11: Choosing AMI

12. By default, the instance type is selected on the **Choose Instance Type** page. Click on **Next: Configure Instance Details** to continue.

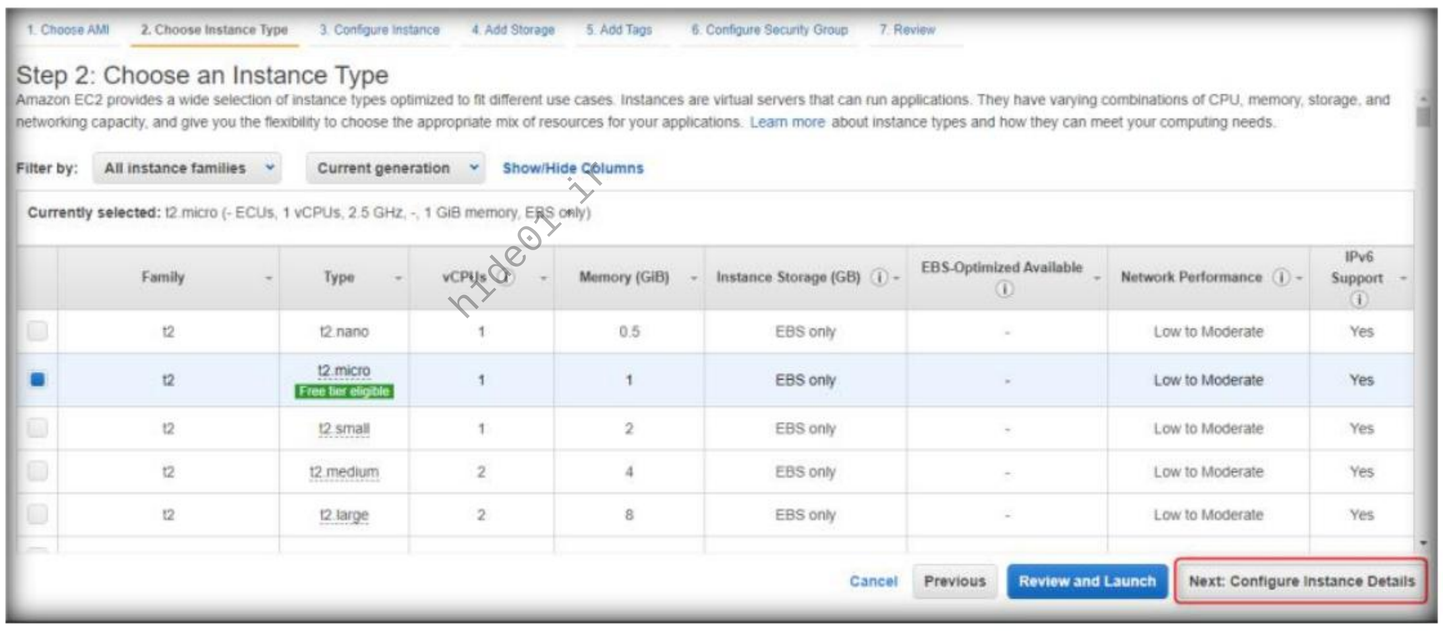


FIGURE 5.1.12: Selecting Instance Type

13. On the **Configure Instance** page, retain all default settings. Then, click on **Next: Add storage**.

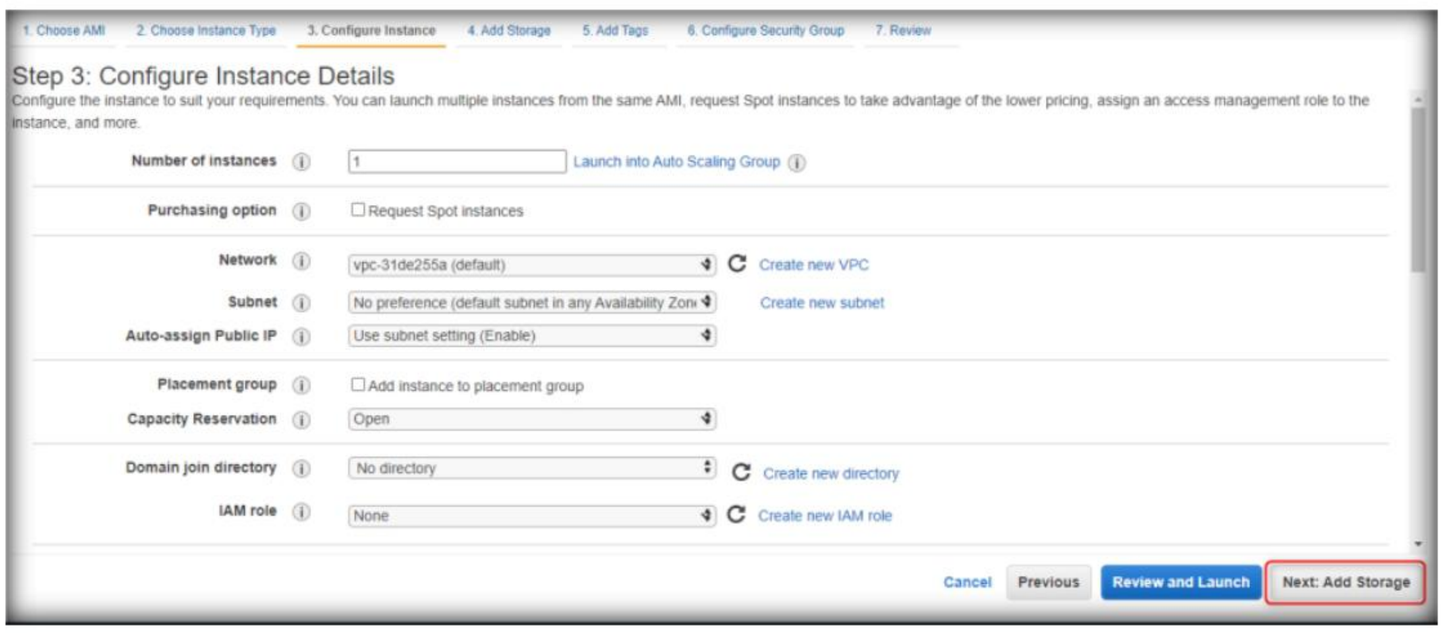


FIGURE 5.1.13: Configuring Instance Details

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

14. In the **Add Storage** step, retain all default settings and click on **Next: Add Tags**.

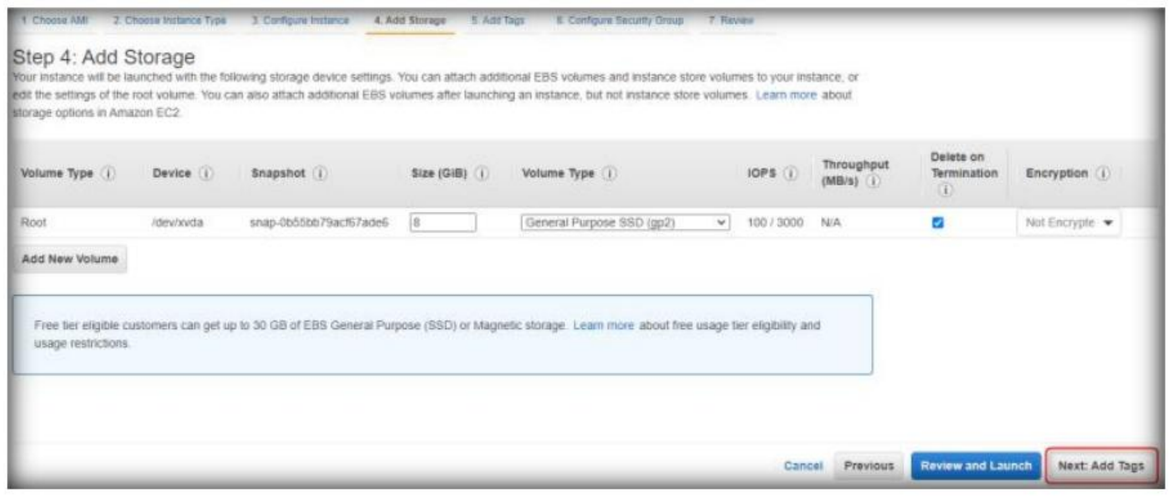


FIGURE 5.1.14: Adding Storage

15. In the **Add Tags** step, click on **Next: Configure Security Group**.

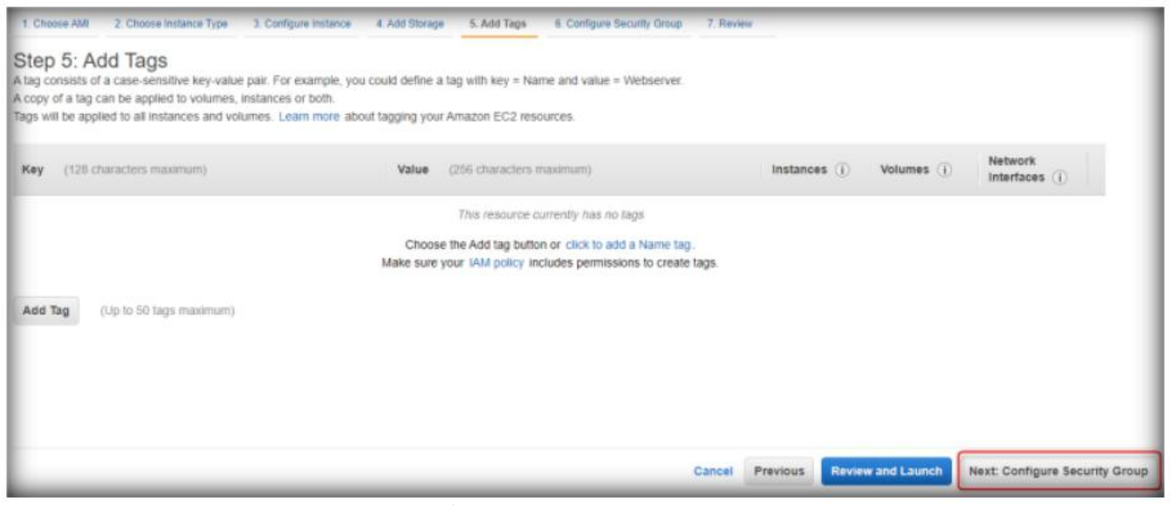


FIGURE 5.1.15: Add Tags page

16. In the **Configure Security Group** step, configure the firewall rules to control the network traffic to the EC2 instance. Give an appropriate **Security group name** (in this lab, we have used **Training_SG** as the **Security group name)** and click on **Add Rule**.



FIGURE 5.1.16: Configuring Security Group

17. For the new rule, select the **Type** as **Custom TCP Rule** from the dropdown. Add the port range as **21** and select source as **Anywhere** from the dropdown. Then, click on **Review and Launch**.

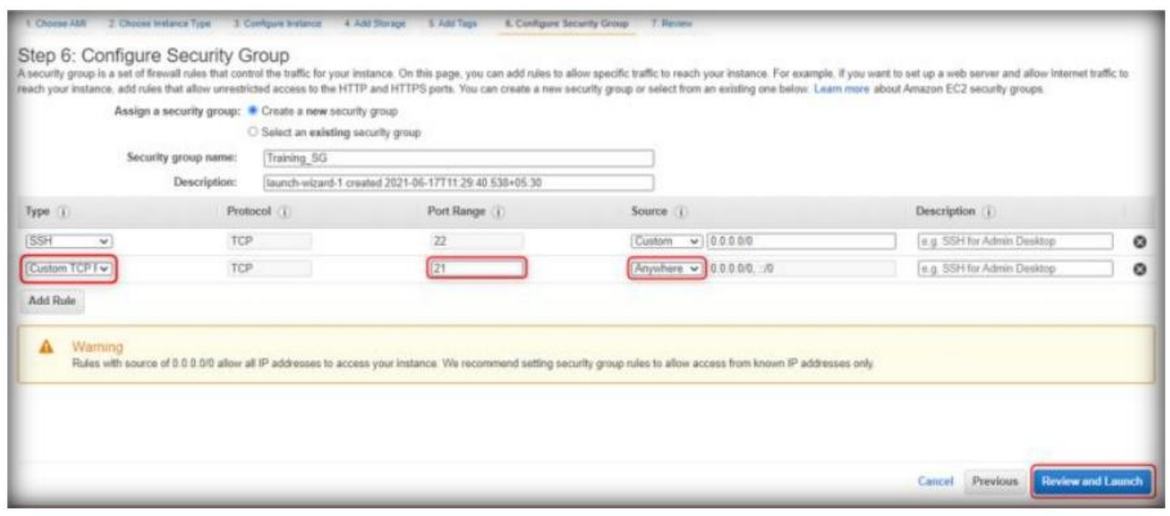


FIGURE 5.1.17: Adding a Rule

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

18. On the **Review Instance Launch** page, view all details and click on **Launch**.

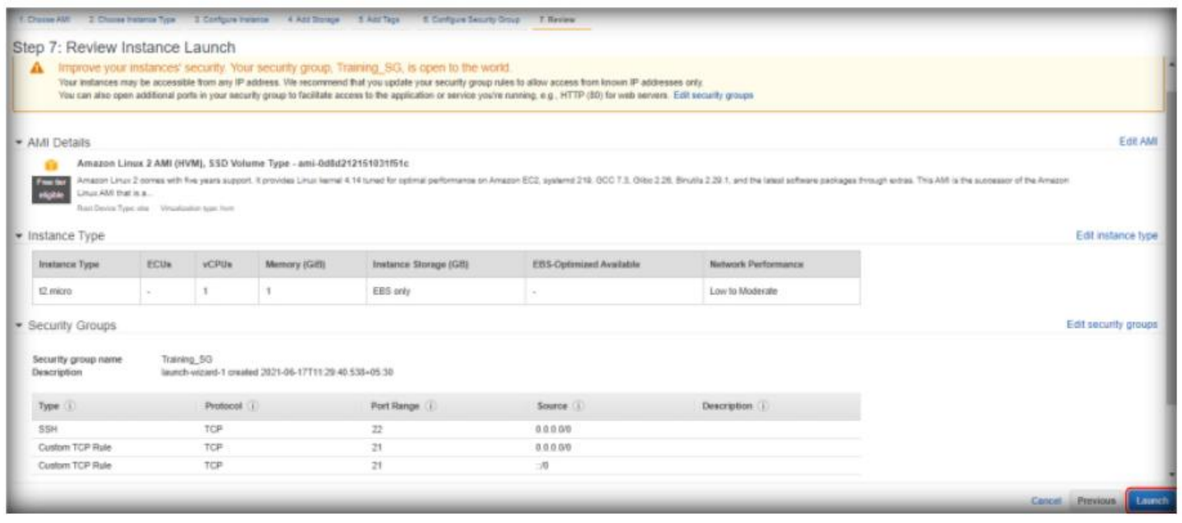


FIGURE 5.1.18: Reviewing Instance Details

19. In the next window that appears for **Select an existing key pair or create a new key pair**, create a key pair that will be used to access the instance publicly. Select **Create a new key pair** and give an appropriate name to the key pair (in this lab, we have used **test_key** as the **Key pair name)**. Click on the **Download Key Pair** button to download your key pair. After the key pair file is downloaded, click on **Launch Instances**.

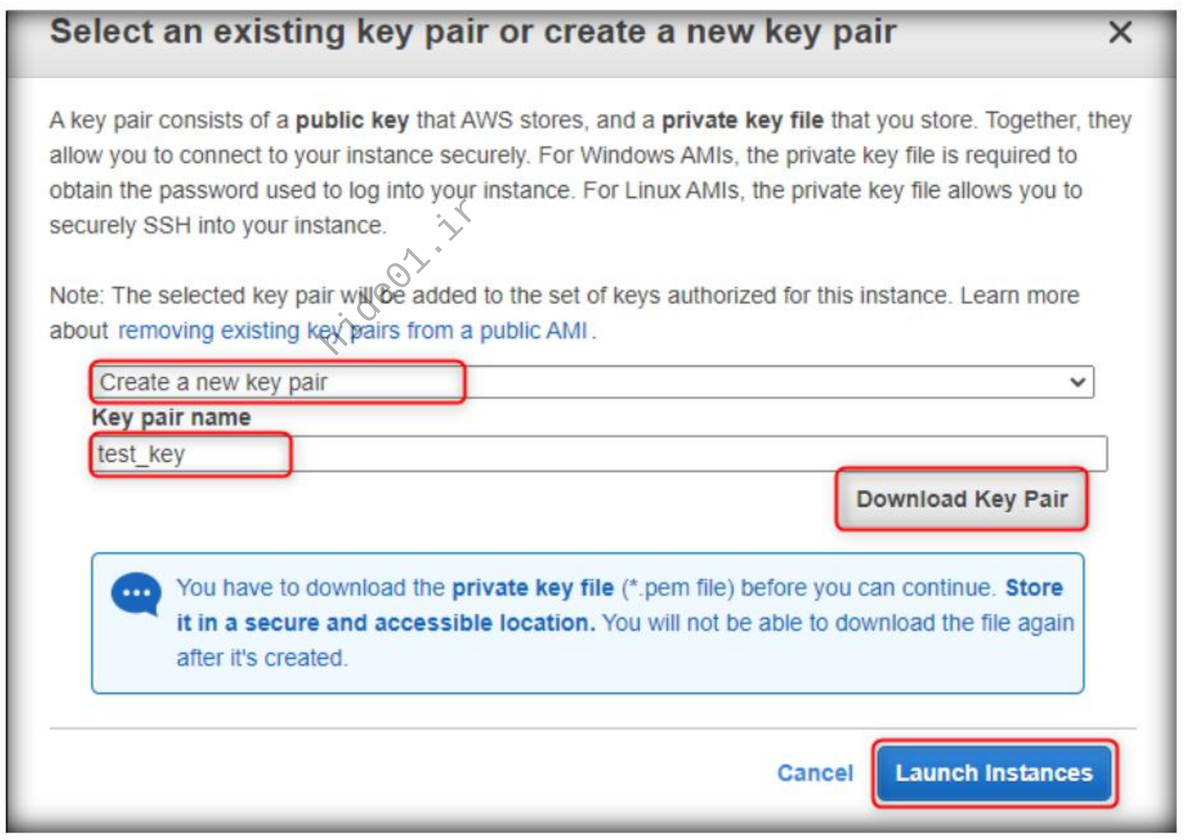


FIGURE 5.1.19: Configuring Key Details

20. On the **Launch Status** page, a message stating **Your instances are now launching** is displayed. Scroll down and click on **View Instances** on the bottom corner to the right.

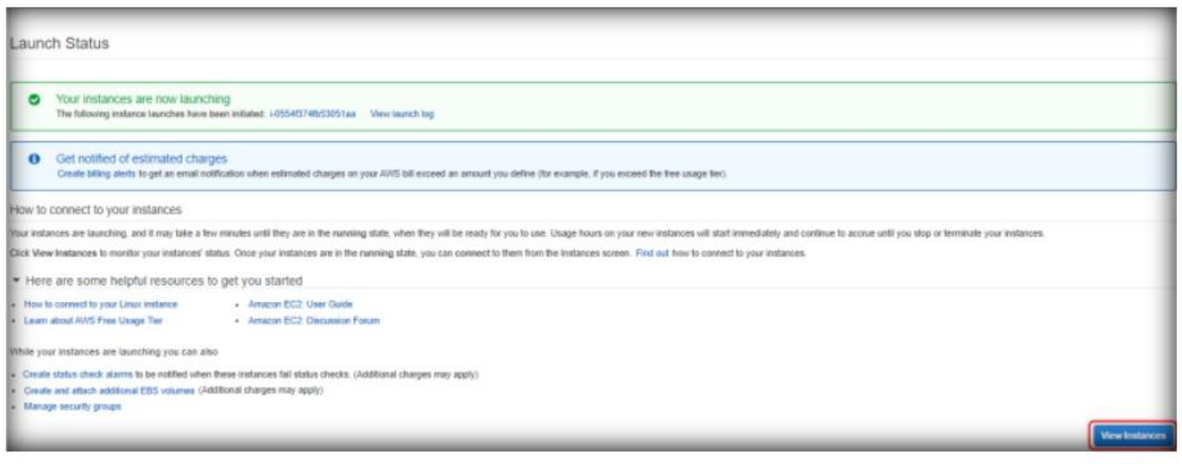


FIGURE 5.1.20: Launch Status

Certified Cloud Security Engineer Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

21. The **Instance state** will display **Running**, indicating that the instance is running.

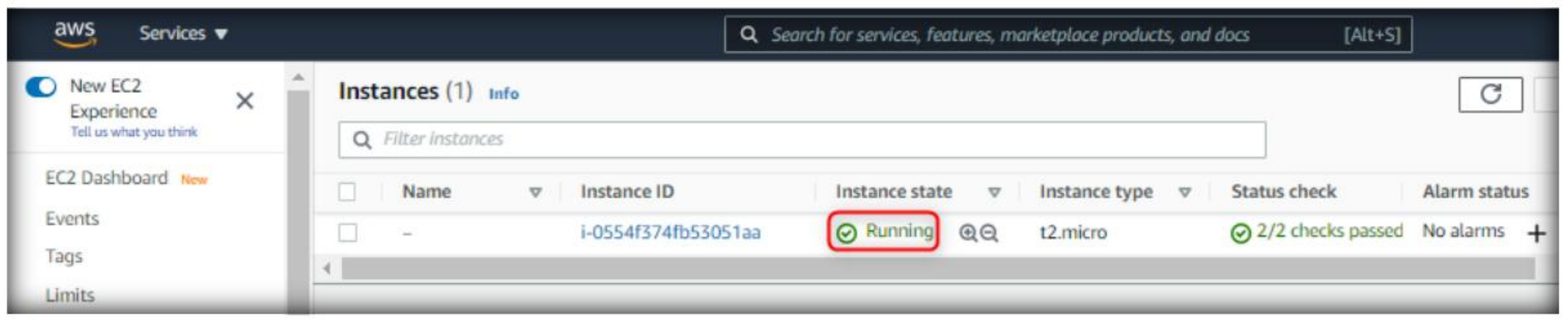


FIGURE 5.1.21: Instance Running

8. Next, you will start an assessment for the target's resources with the help of Amazon Inspector. Click on **Services** and select **Inspector** under **Security, Identity & Compliance**.

TASK 2

Performing Assessment of the EC2 instance with Amazon Inspector

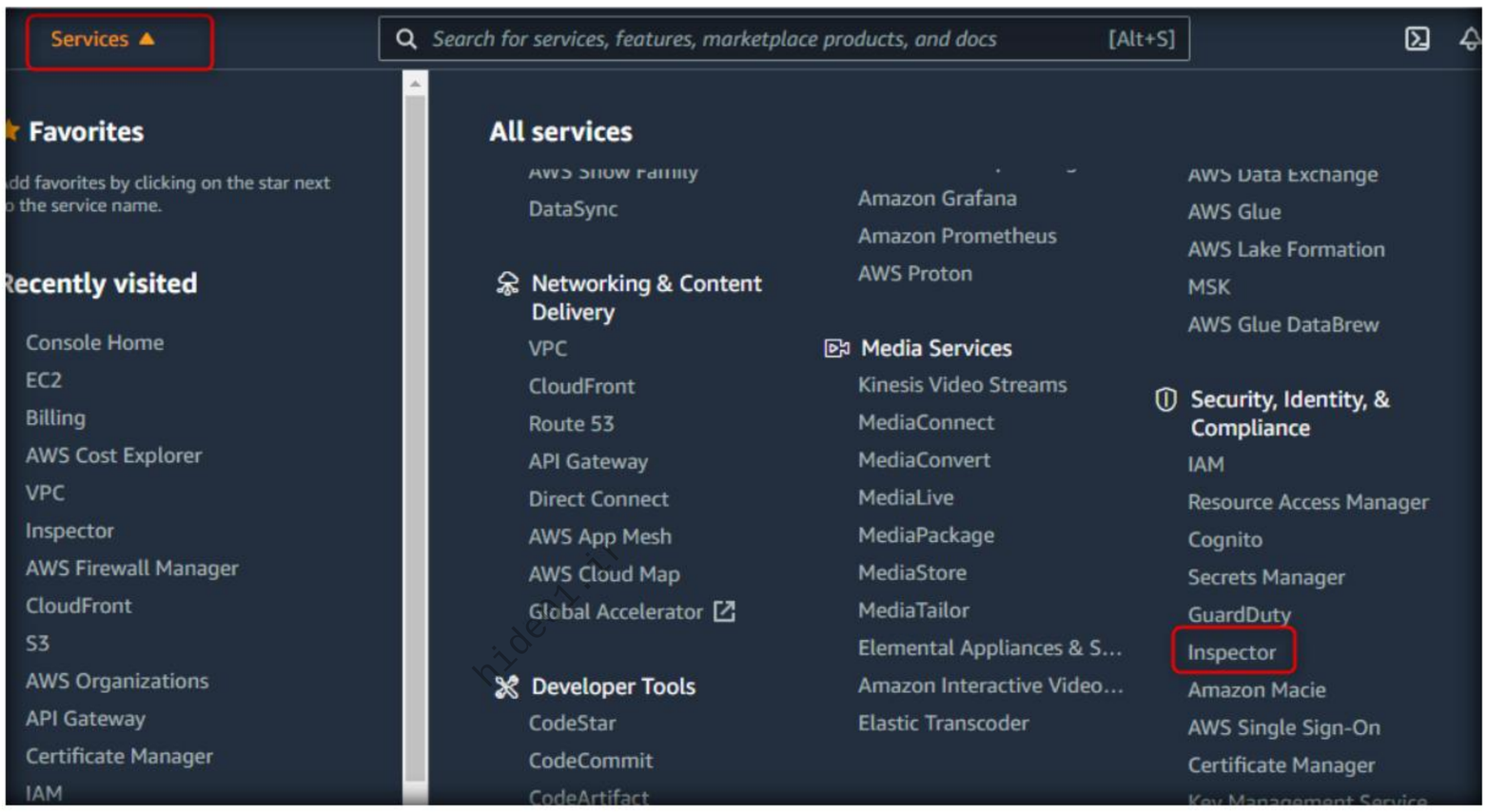


FIGURE 5.1.22: Policy Generator

22. Once the **Amazon Inspector** console opens, click on **Get Started.**

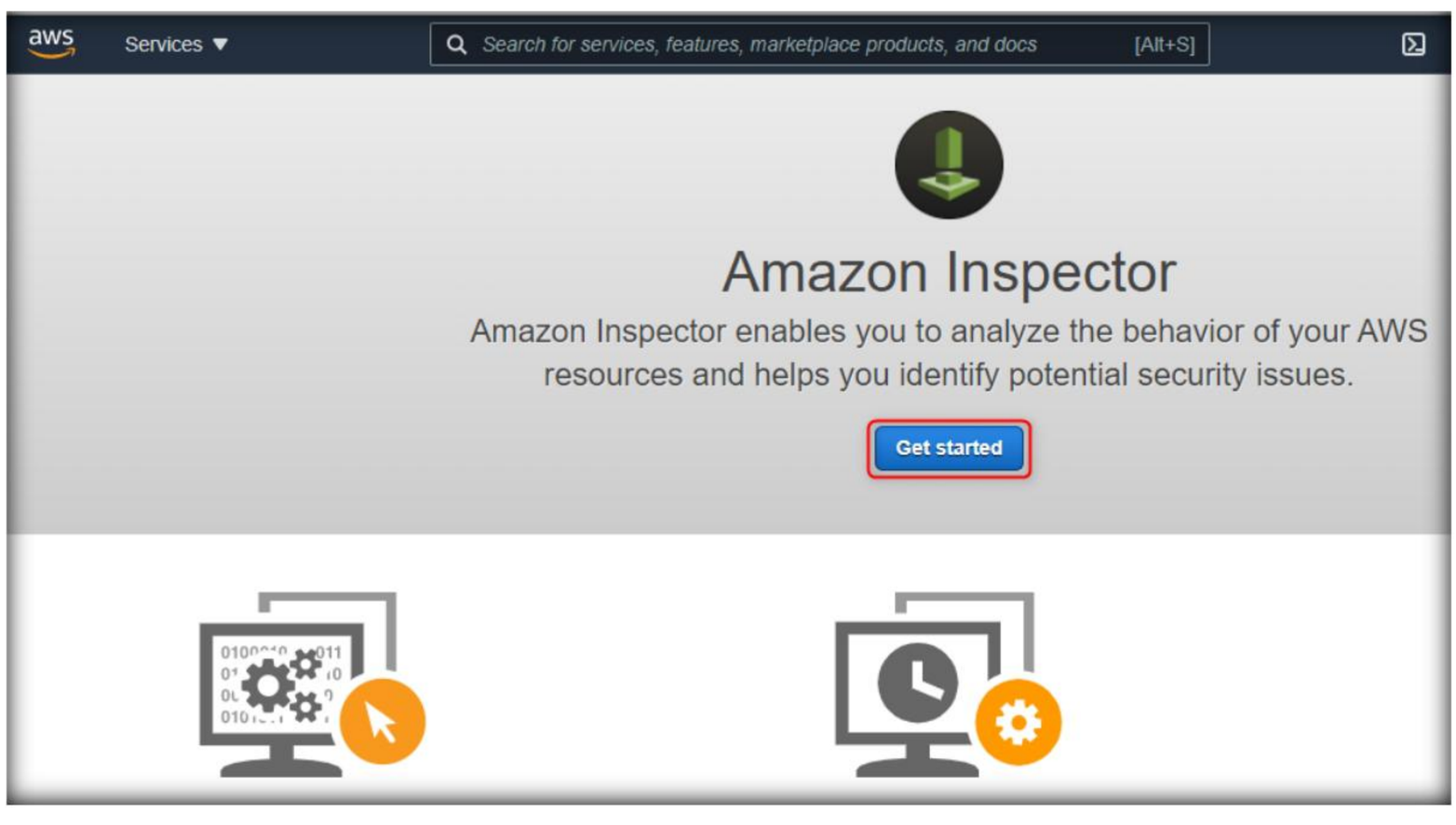


FIGURE 5.1.23: Amazon Inspector

Certified Cloud Security Engineer Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

23. Next, click on **Advanced setup** to continue.

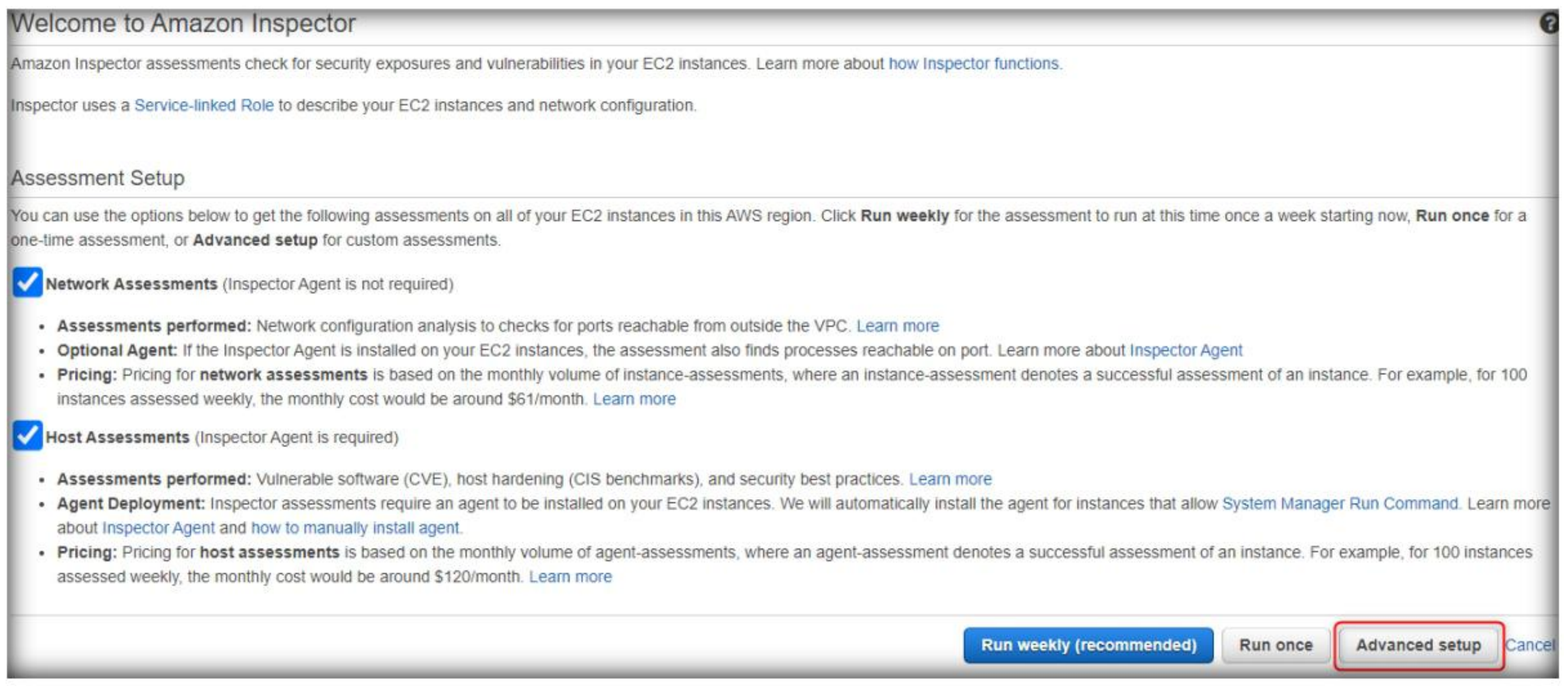


FIGURE 5.1.24: Assessment Setup Settings

24. In **Define an assessment target** step, type **Assessment-Target1** as the **Name** and click **Next**.

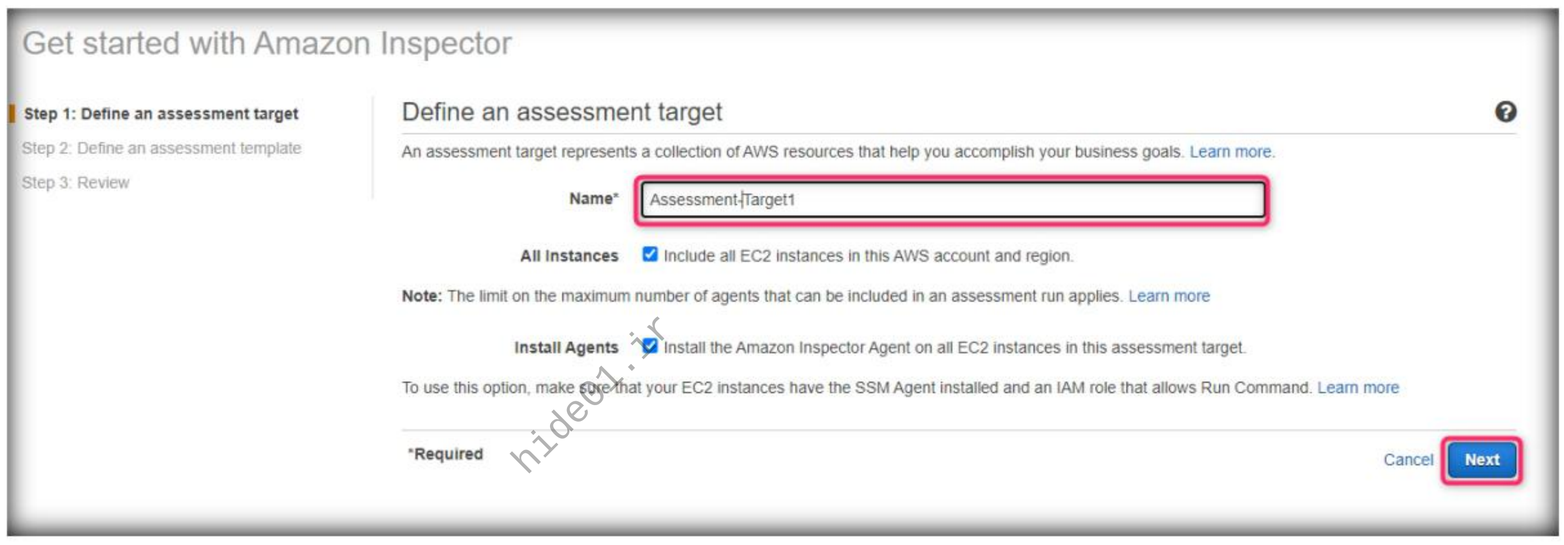


FIGURE 5.1.25: Assessment Setup Details

25. In the **Define an assessment template** step, leave the default template name, select **Duration** as **15 Minutes**, and click on **Next**.

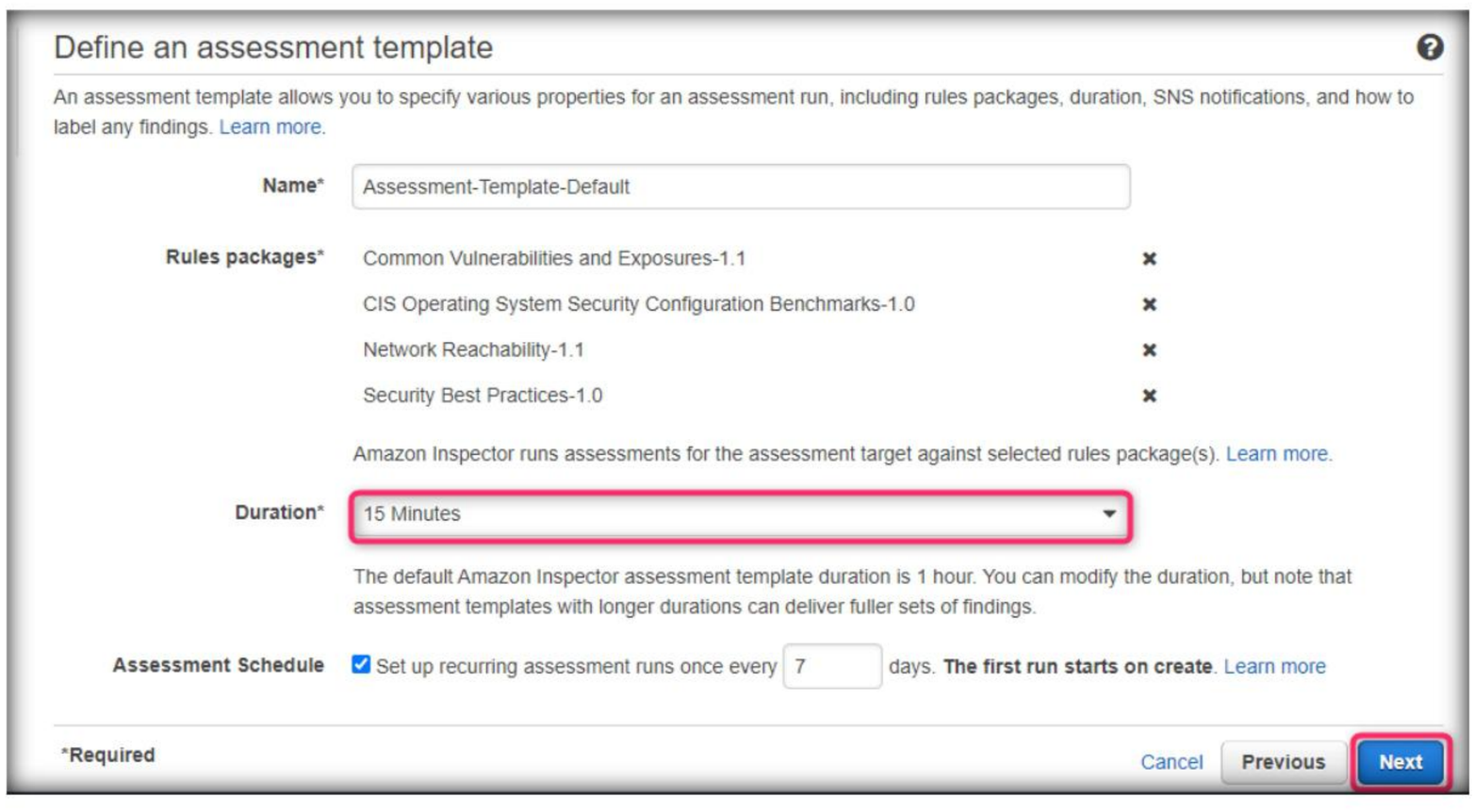


FIGURE 5.1.26: Defining Assessment Template

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

26. Finally, review the assessment details on the **Review** step and click on **Create**.

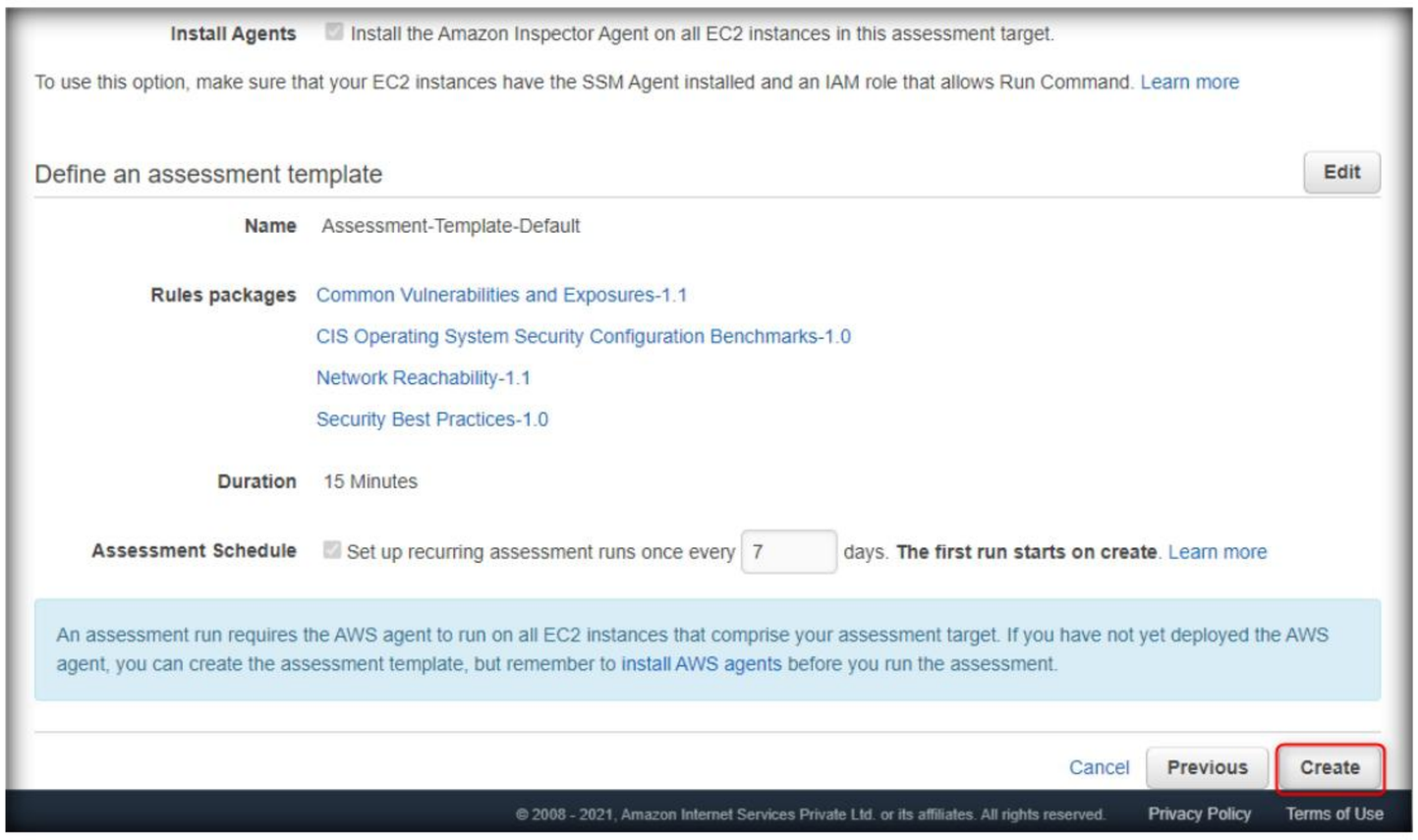


FIGURE 5.1.27: Reviewing Assessment Details

27. You will see a message that says the installation of Amazon Inspector Agent is initiated, as shown in the below screenshot. Now, to view the findings, click on the **Assessment runs** option from the left menu.

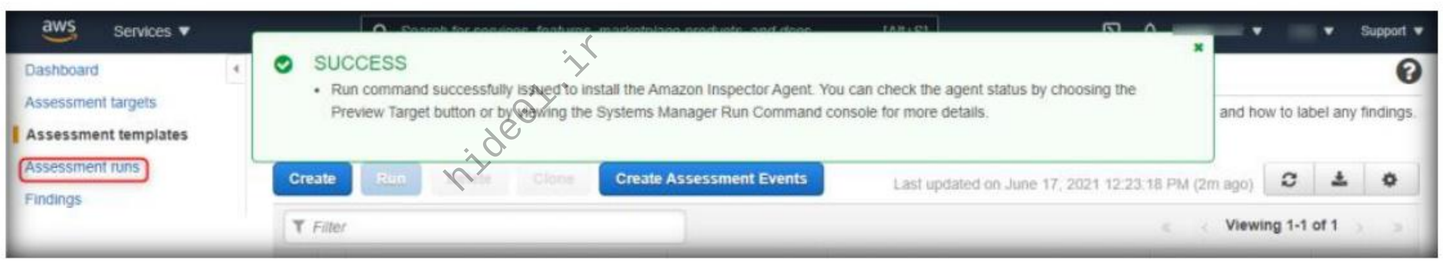


FIGURE 5.1.28: Running Assessment

28. On the **Amazon Inspector – Assessment Runs** page, the assessment details can be seen as in the following screenshot. To check the assessment findings, click on **Findings**.

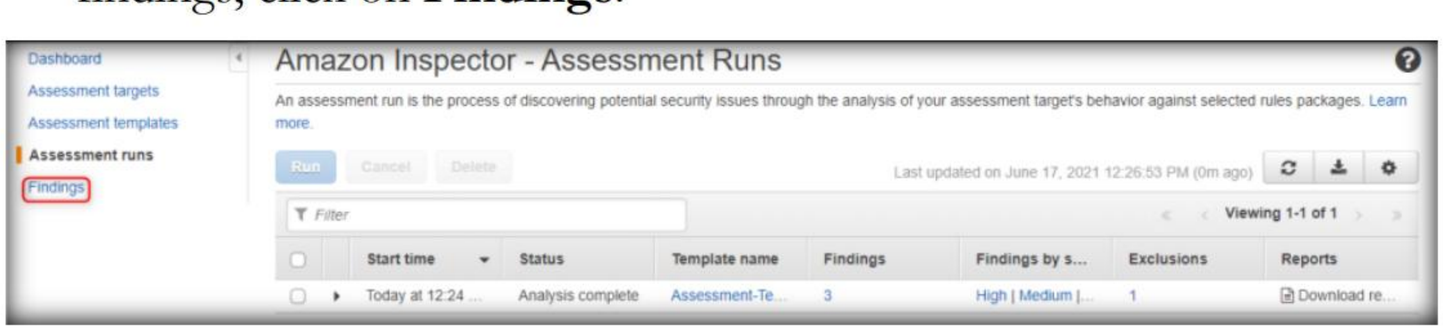


FIGURE 5.1.29: Assessment Result

29. On the **Findings** page, the finding details will be visible.

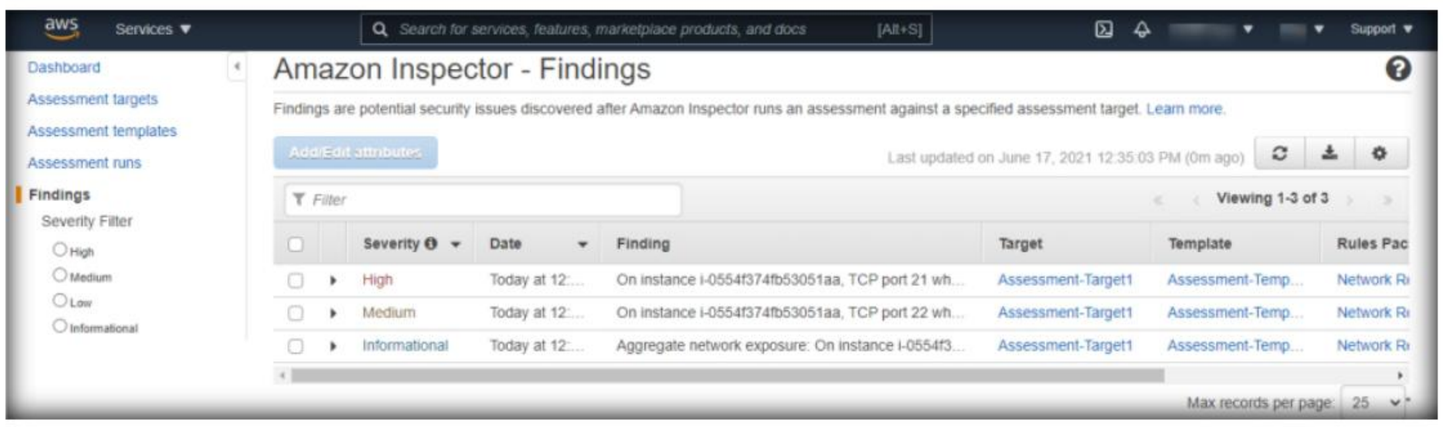


FIGURE 5.1.30: Assessment Findings

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

30. There are different severity levels. Select **High** under **Severity Filter** and expand the available finding for **High** Severity. You can see the details about this severity.

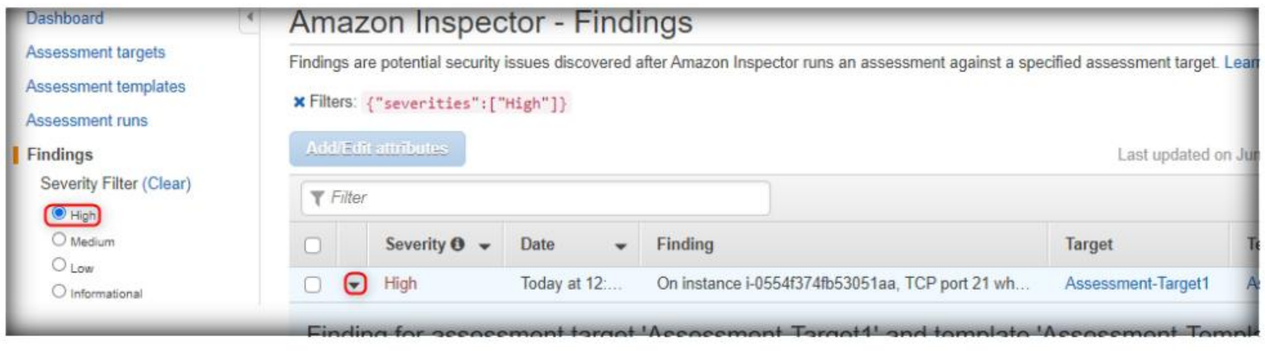


FIGURE 5.1.31: Assessment Finding Details

31. Scroll down the page. You can see the findings and recommendations for the best security practices.

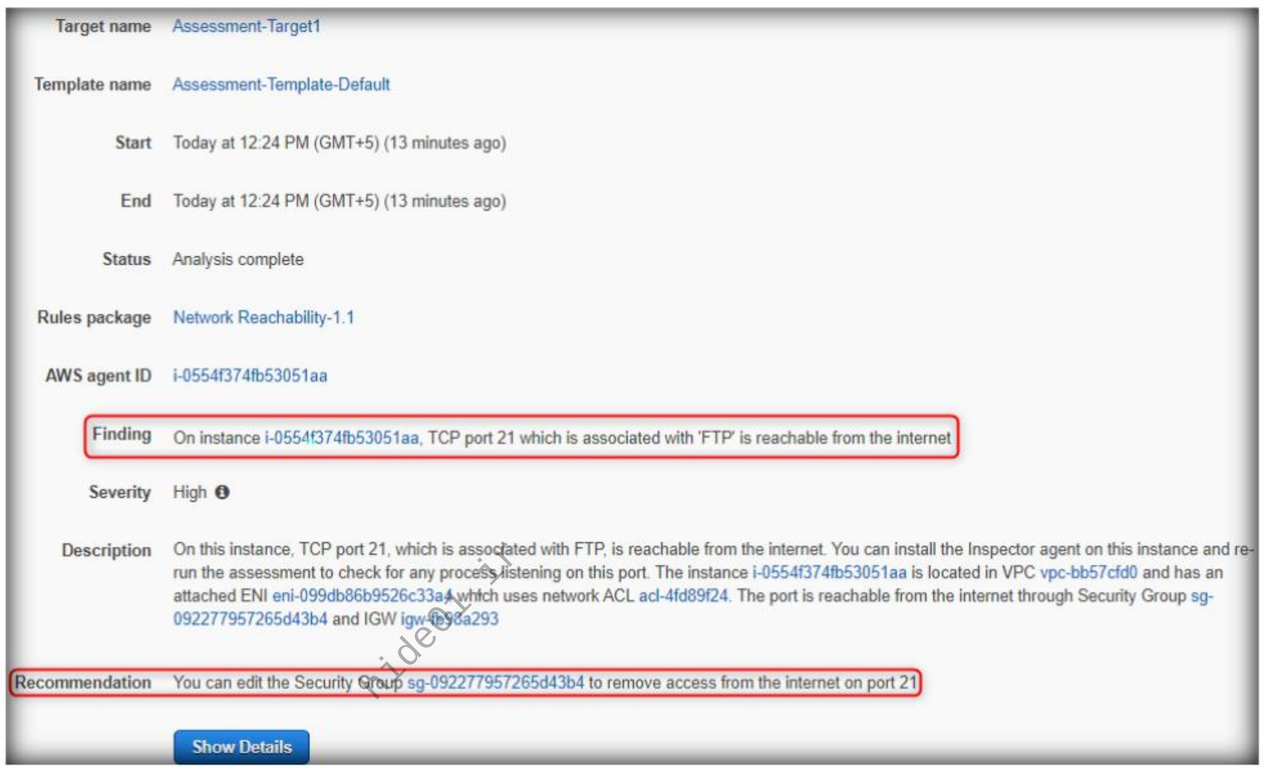


FIGURE 5.1.32: Assessment Finding Details

32. This way, AWS Inspector can assess the instances and recommend the best security practices.

33. The **Recommendation** suggests editing the security group to remove access from the Internet on port 21. Port 21 is associated with FTP protocol, which is generally considered insecure because it uses the clear-text format for data transfer. Click on the security group link provided in **Recommendation** to execute the recommendation, as shown in the following screenshot.

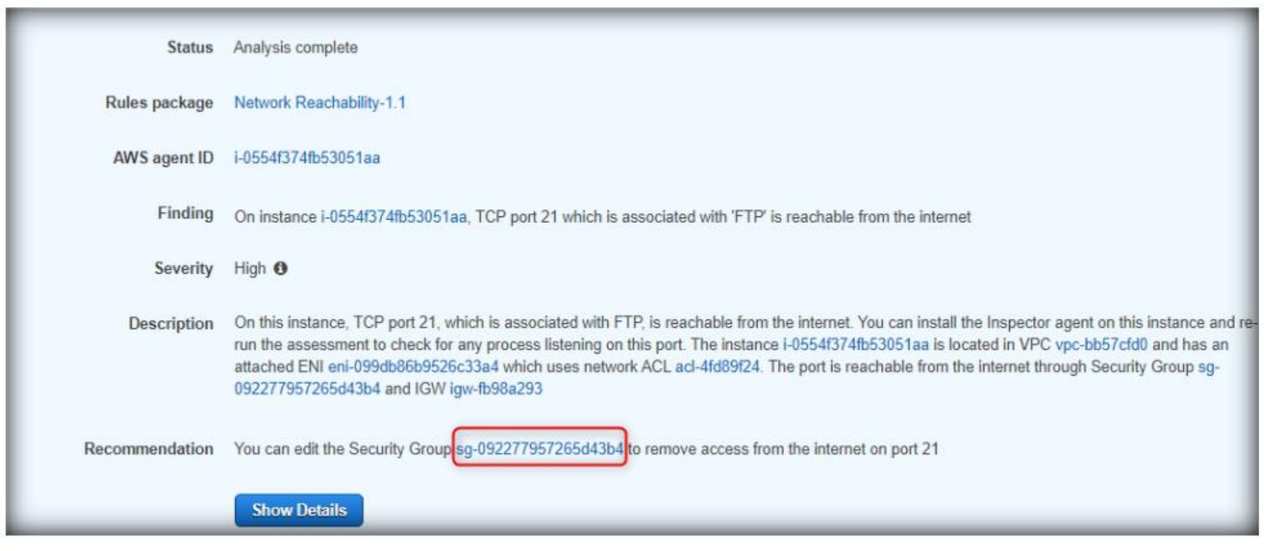


FIGURE 5.1.33: Assessment Recommendation

Certified Cloud Security Engineer Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

34. The **Security Groups** page opens in a new tab. Switch to the newly opened tab and click on the security group id under **Security group ID,** as shown in the screenshot below.

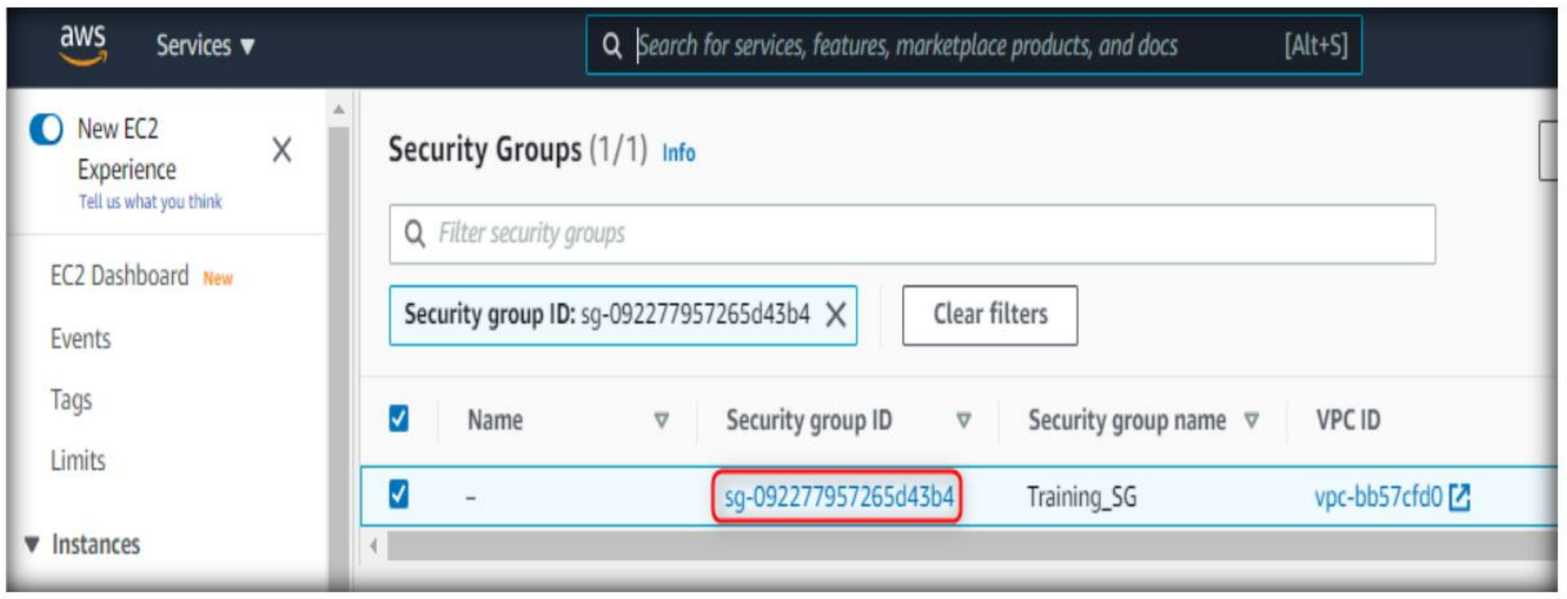


FIGURE 5.1.34: Selecting the Security Group

35. In the **Training_SG** security group section, click on **Edit inbound rules** to remove port 21.

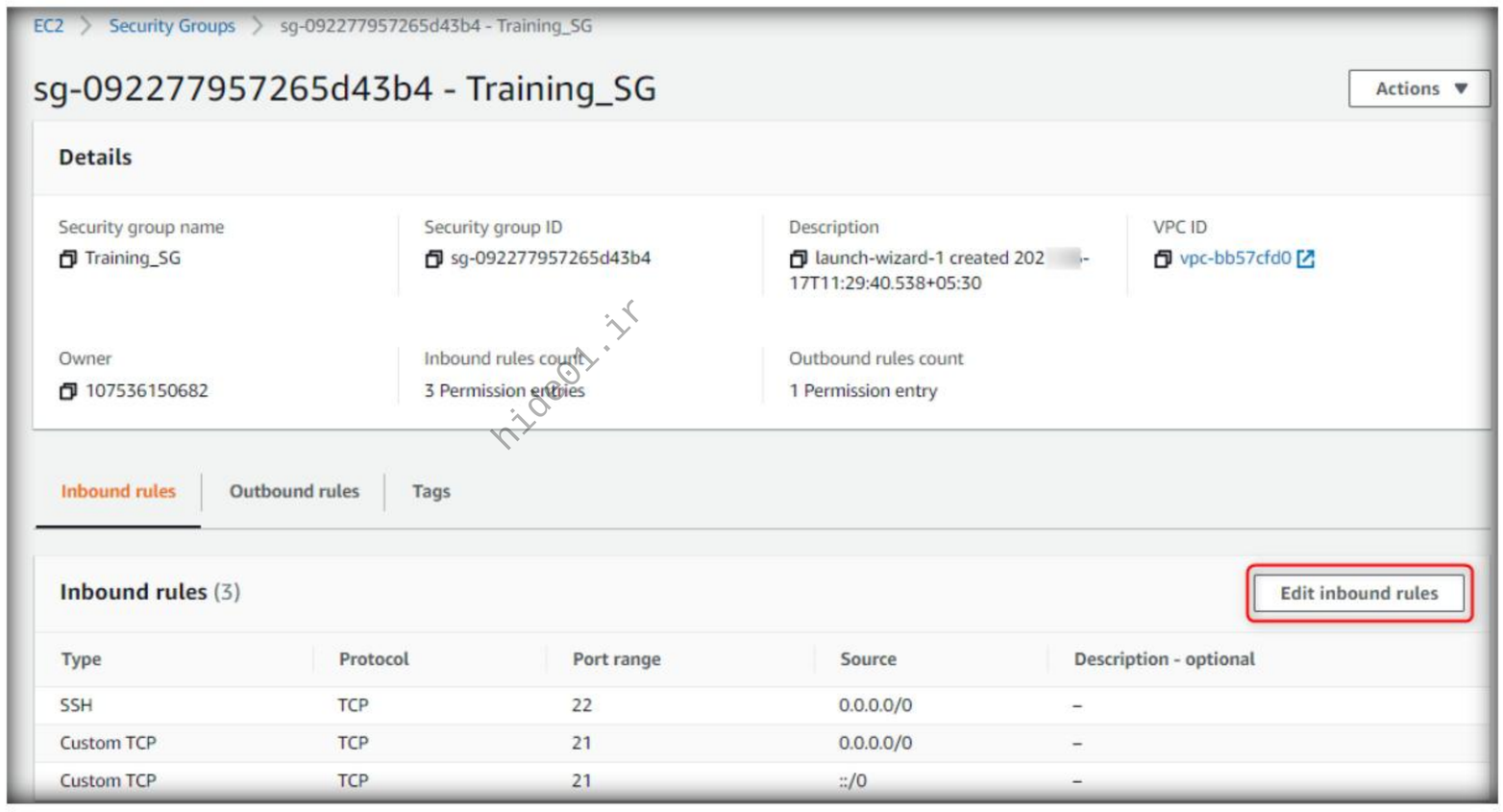


FIGURE 5.1.35: Inbound Rules

36. In the **Inbound rule** window, click on **Delete** to remove the open port **21,** as shown in following screenshot.

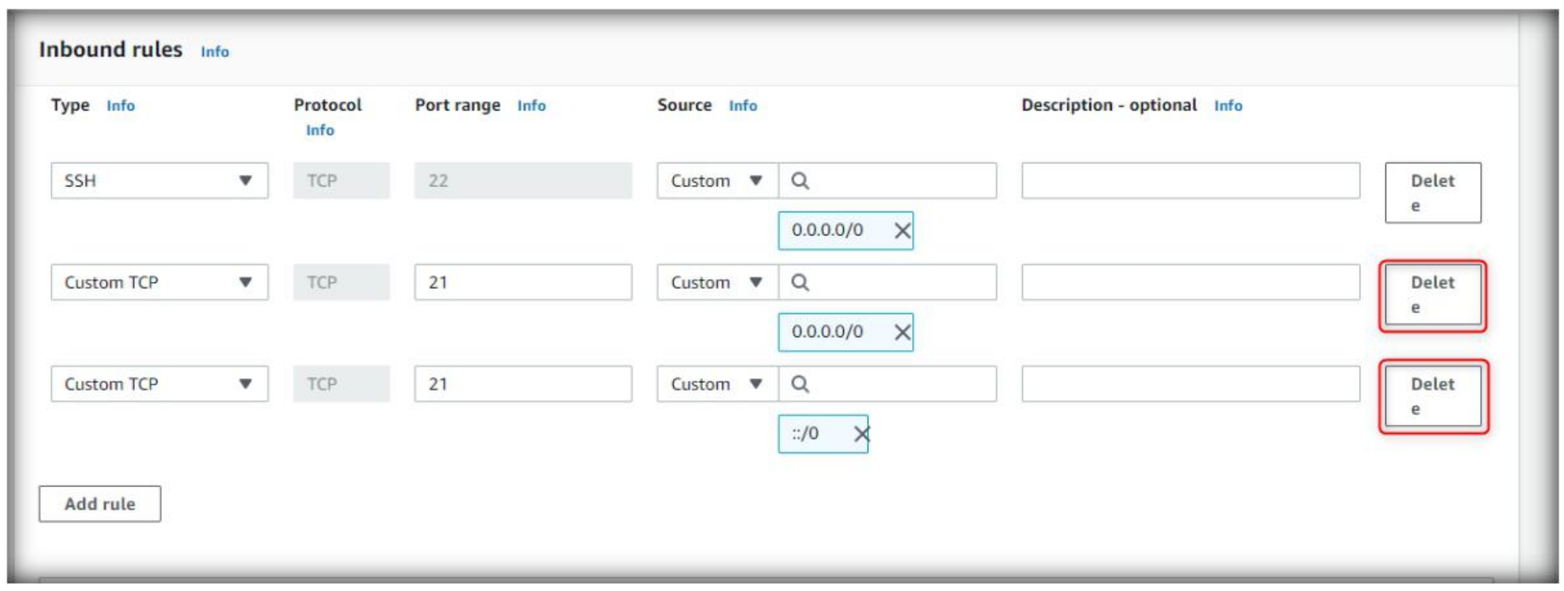


FIGURE 5.1.36: Editing Inbound Rules

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Overview of Cloud Audit Logs

Cloud Audit Logs can be used to maintain audit trails of all activities in GCP to help the security, auditing, and compliance teams. All administrative activities can be stored on a continuously available and highly secure audit trail that cannot be disabled. The types of audit logs recorded by the GCP projects are:

- **Admin activity audit logs**: Admin activity audit logs record administrative changes to resource configurations. Admin activity audit logs can be viewed if you have the IAM logging/logs viewer or project/viewer roles. Admin activity audit logs are enabled by default.
- **System event logs**: System event logs contain information about events that modify resource configurations. System event audit logs can be viewed if you have the logging/logs viewer or project/viewer IAM roles. They are enabled by default.
- **Data access logs**: Data access audit logs record information about the operations that perform ready-only activities. Data access audit logs can be viewed if you have the logging /private logs viewer or project/owner IAM roles. Data access audit logs are disabled by default.
- **Policy denied audit logs**: Policy denied audit logs record information regarding denial of access to GCP services because of security violations. Policy denied audit logs can be viewed if you have the logging/logs viewer or project/viewer IAM roles. They are enabled by default.

hide01.ir

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., GCP), the application interface may be updated with time. Hence, in case you happen to work on an updated version of GCP, 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 an GCP account using the following link: **https://console.cloud.google.com**. Ensure you have activated the account.

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

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1

Creating a New Project in Google Cloud Console

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

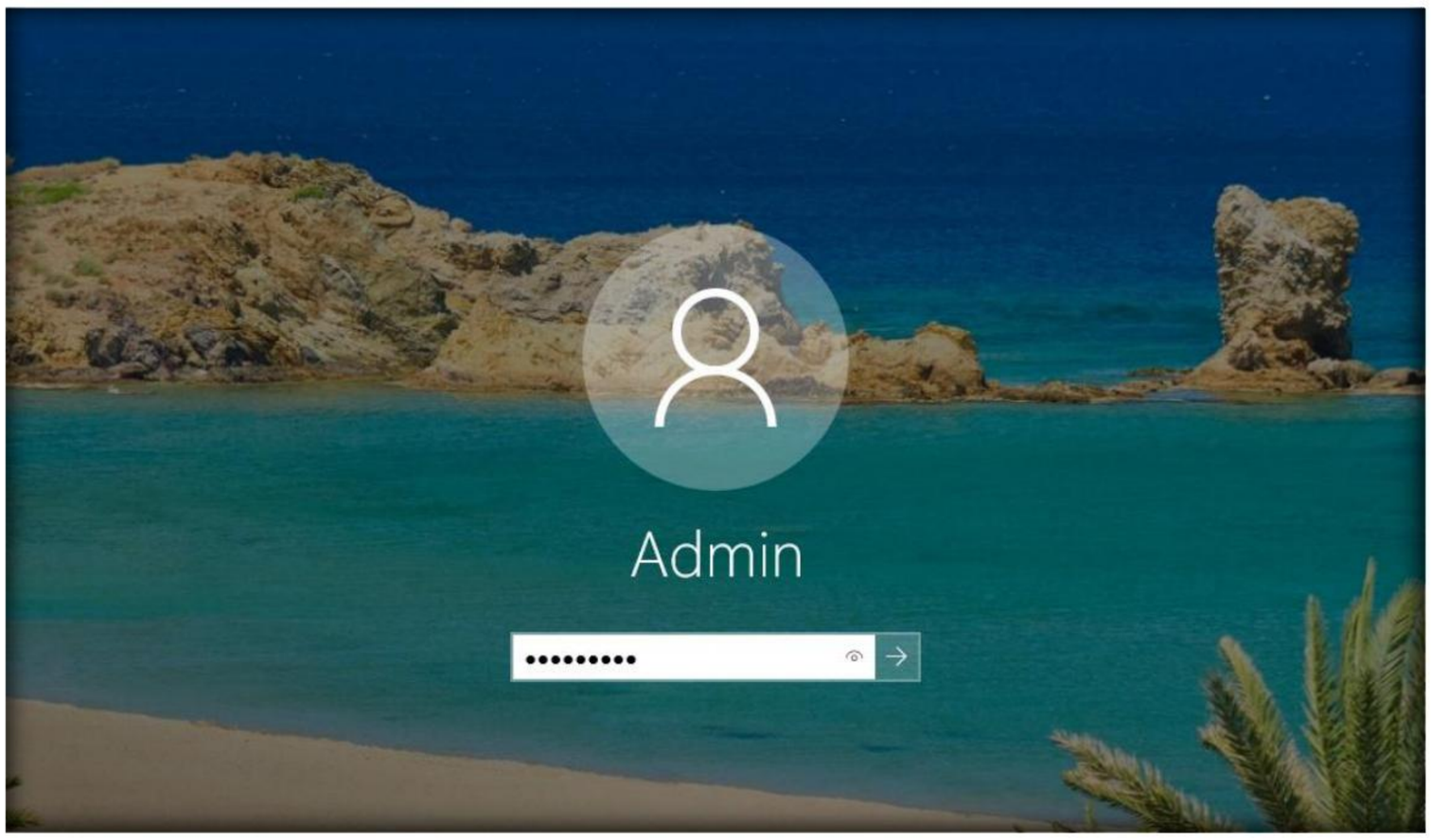


FIGURE 11.3.1: Launch Admin Machine and Log in

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



FIGURE 11.3.2: Navigating to the Chrome Browser from Taskbar

3. Go to the address bar, type **https://console.cloud.google.com/**, and press **Enter.**

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

4. In the Sign in page, enter the **Email or phone** and click **Next** to login into Google Cloud Console.

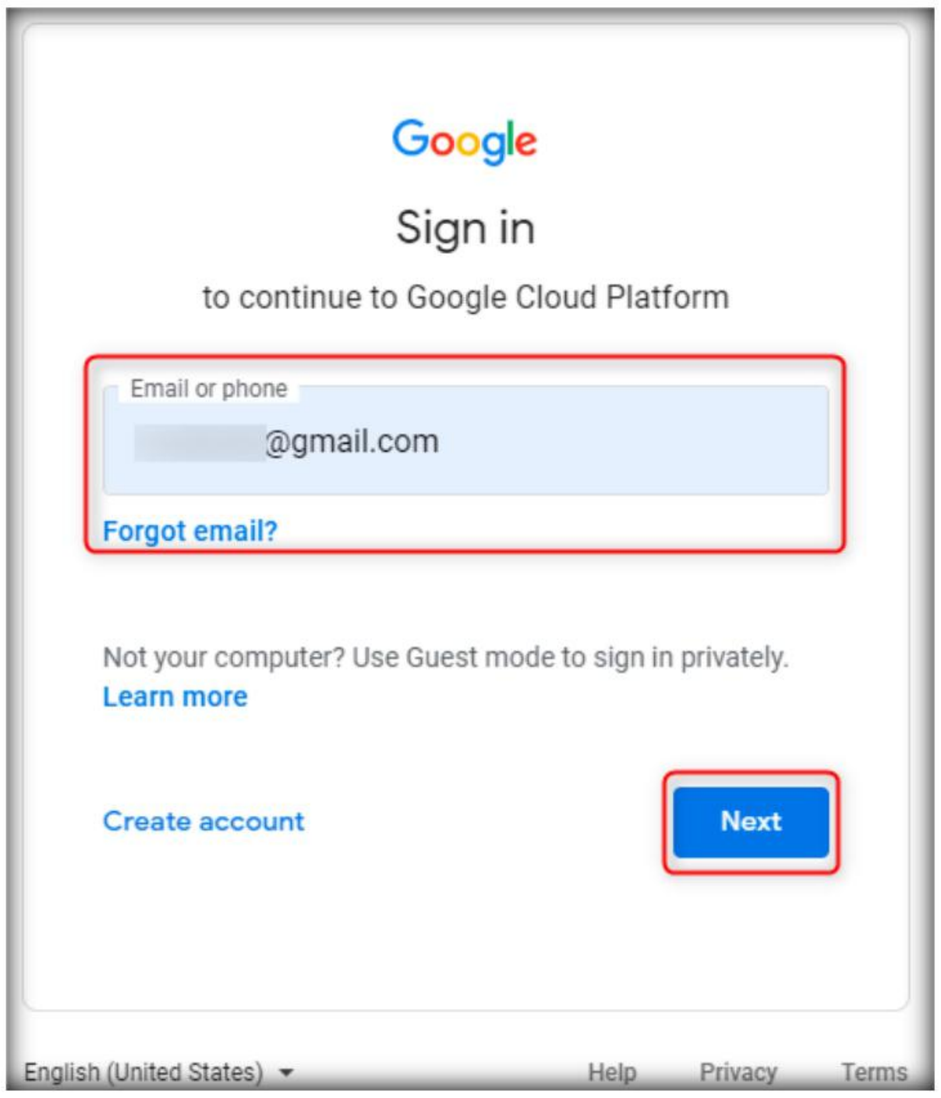


FIGURE 11.3.3: Access GCP in Browser

5. Enter the **password** and click on **Next**.

hide01.ir

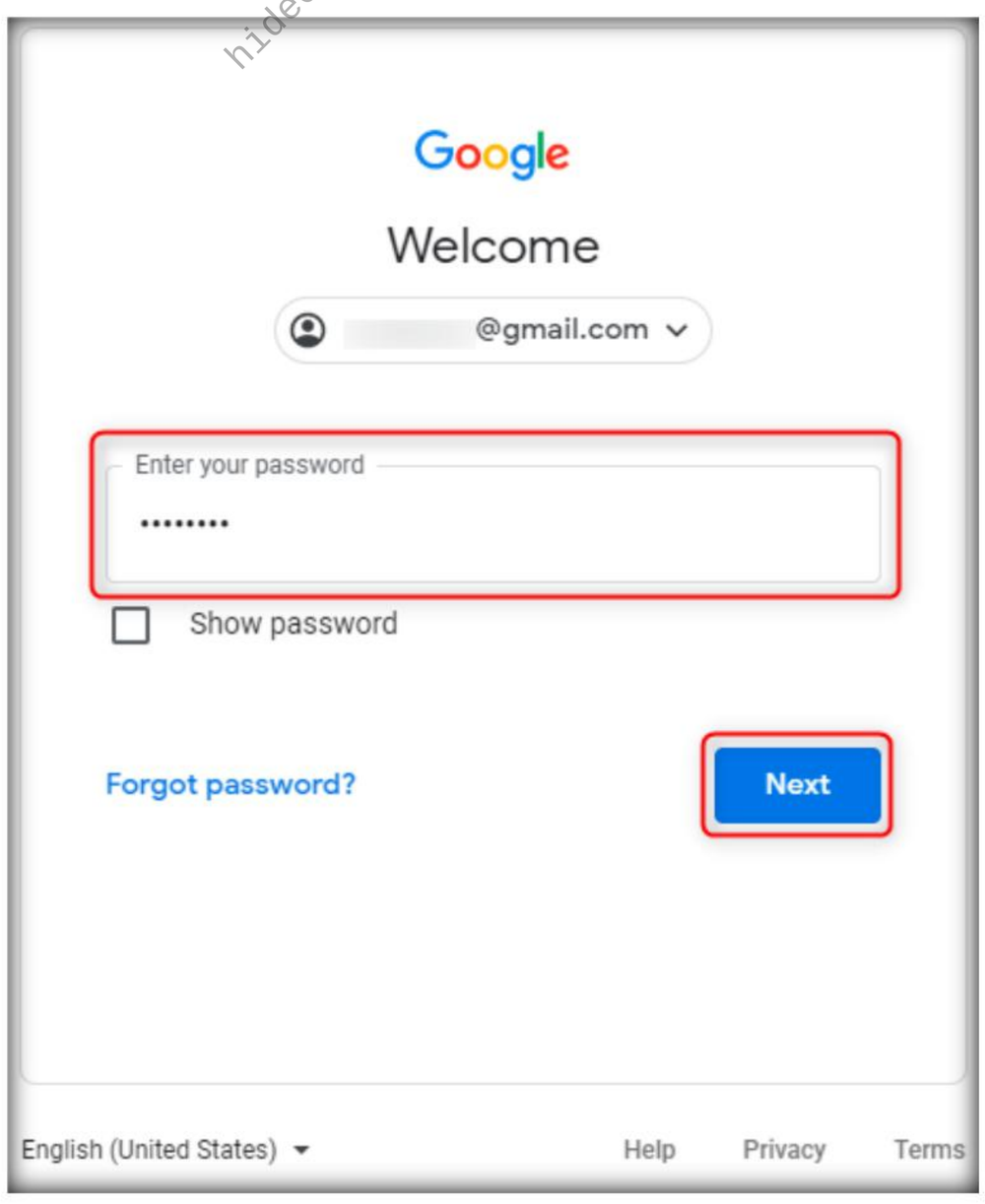


FIGURE 11.3.4: Signing in into GCP console

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

6. On top left corner, you will have a dropdown option. If **My First Project** is the default selected project, then skip **Steps 7–16** and go to **Step 17**.

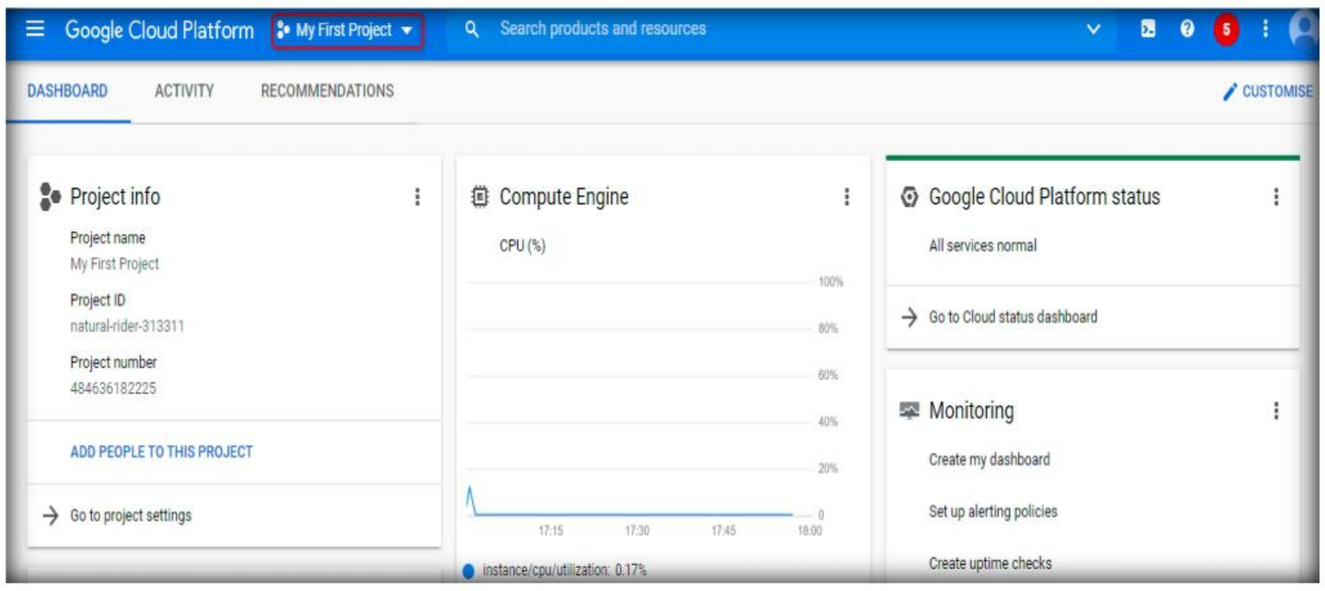
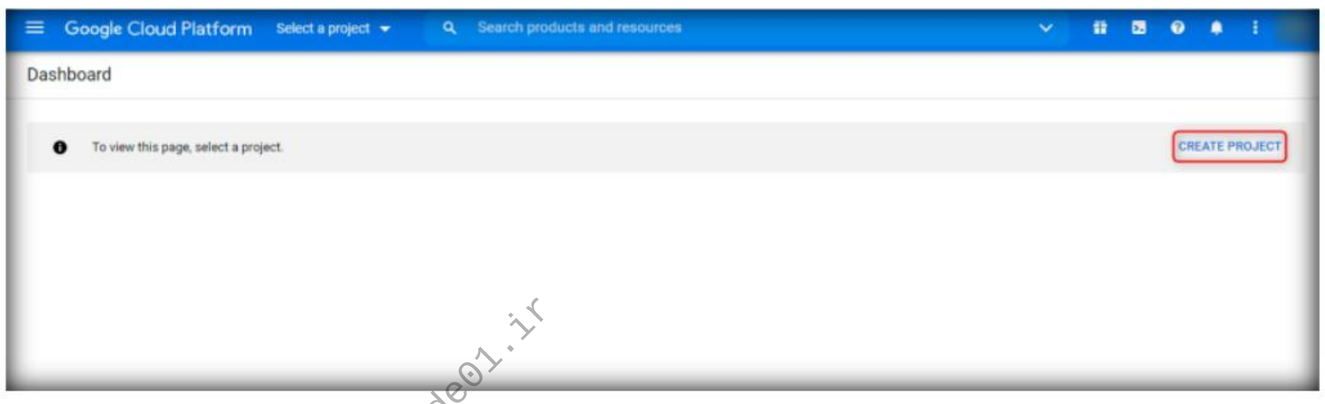


FIGURE 11.3.5: Create new Project

7. On top left corner, if you see **Select a Project** with an empty dashboard in the dropdown, then click on **CREATE PROJECT** to create a new project.



hide01.ir

FIGURE 11.3.6: Creating Project

8. In the **New Project** window that opens, type the **Project name** as **My First Project**. Click on **CREATE**.

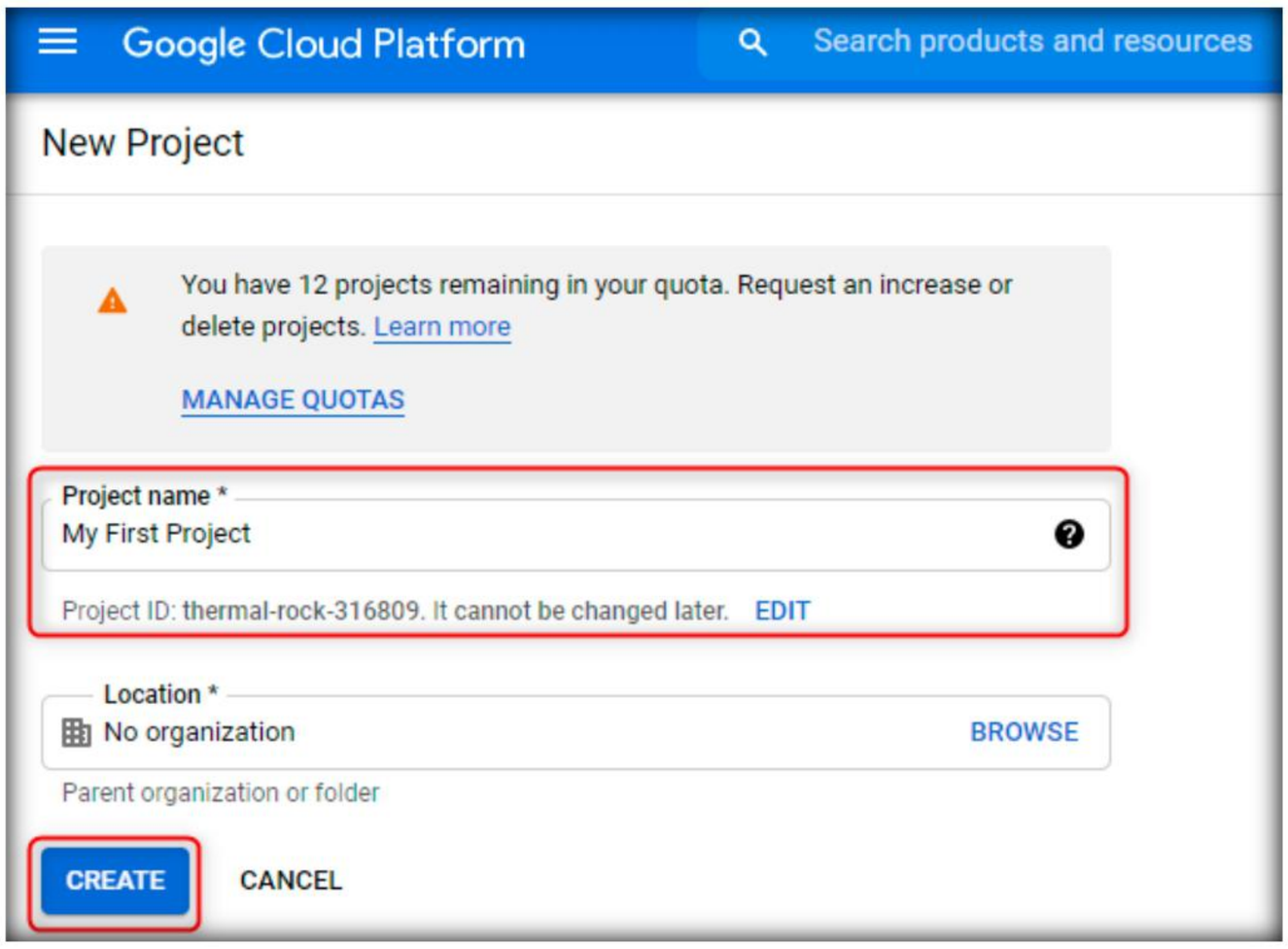


FIGURE 11.3.7: Configuring New Project

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

9. Your project will be successfully created. You can see that in the top of the window, **My New Project** will be selected as the current project by default.

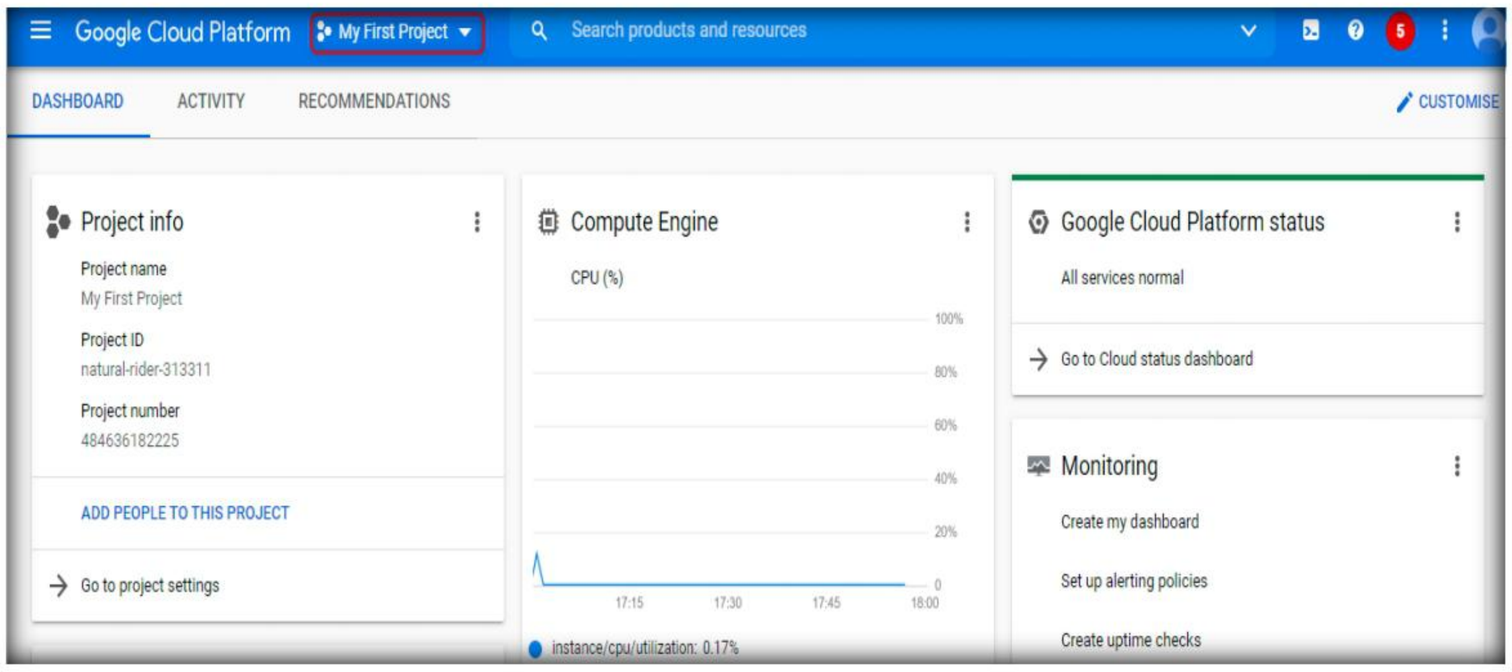


FIGURE 11.3.8: My First Project Selected as Default

10. On top left corner, if the dropdown displays a different project by default other than **My First Project**, then click on it.

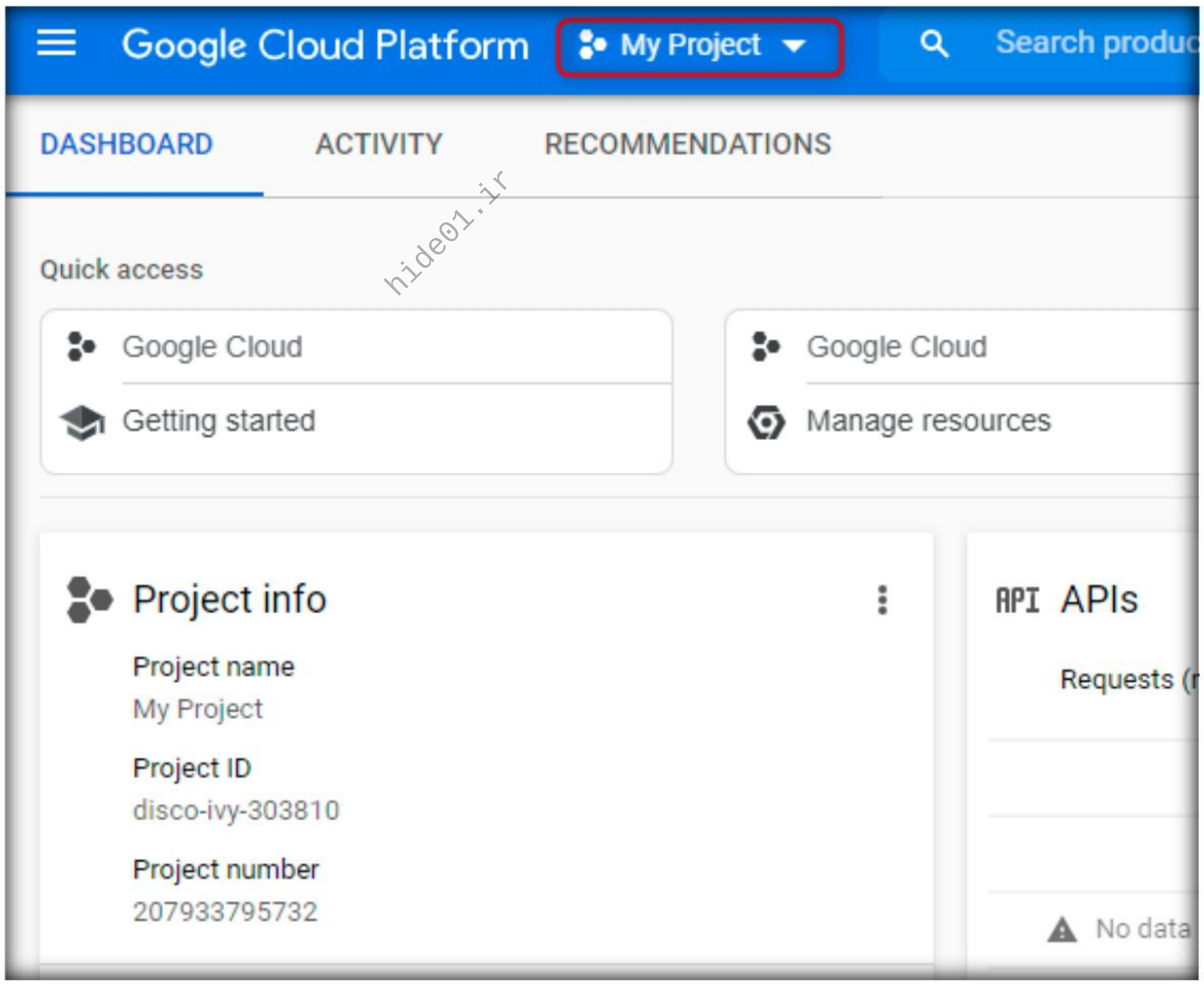


FIGURE 11.3.9: Selecting Project Dropdown

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

11. You will see a **Select a project** window, which displays all existing projects. It also provides a **Search projects and folders** option to search for an existing project. Select **My First Project** from the displayed list of existing projects.

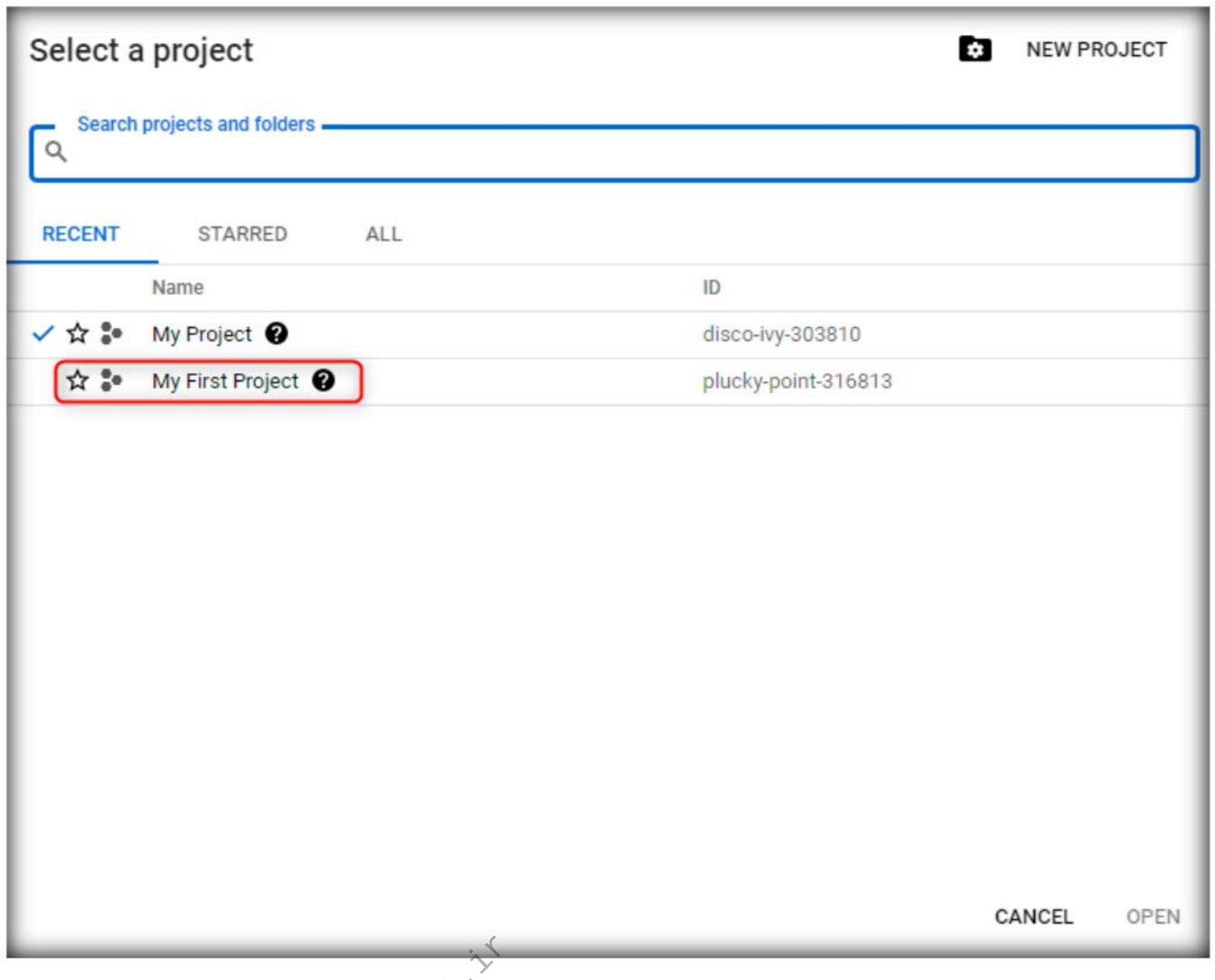


FIGURE 11.3.10: Selecting My First Project

12. Now, if **My New Project** is not in the list, click on the **NEW PROJECT** option to create a new project named **My First Project**.

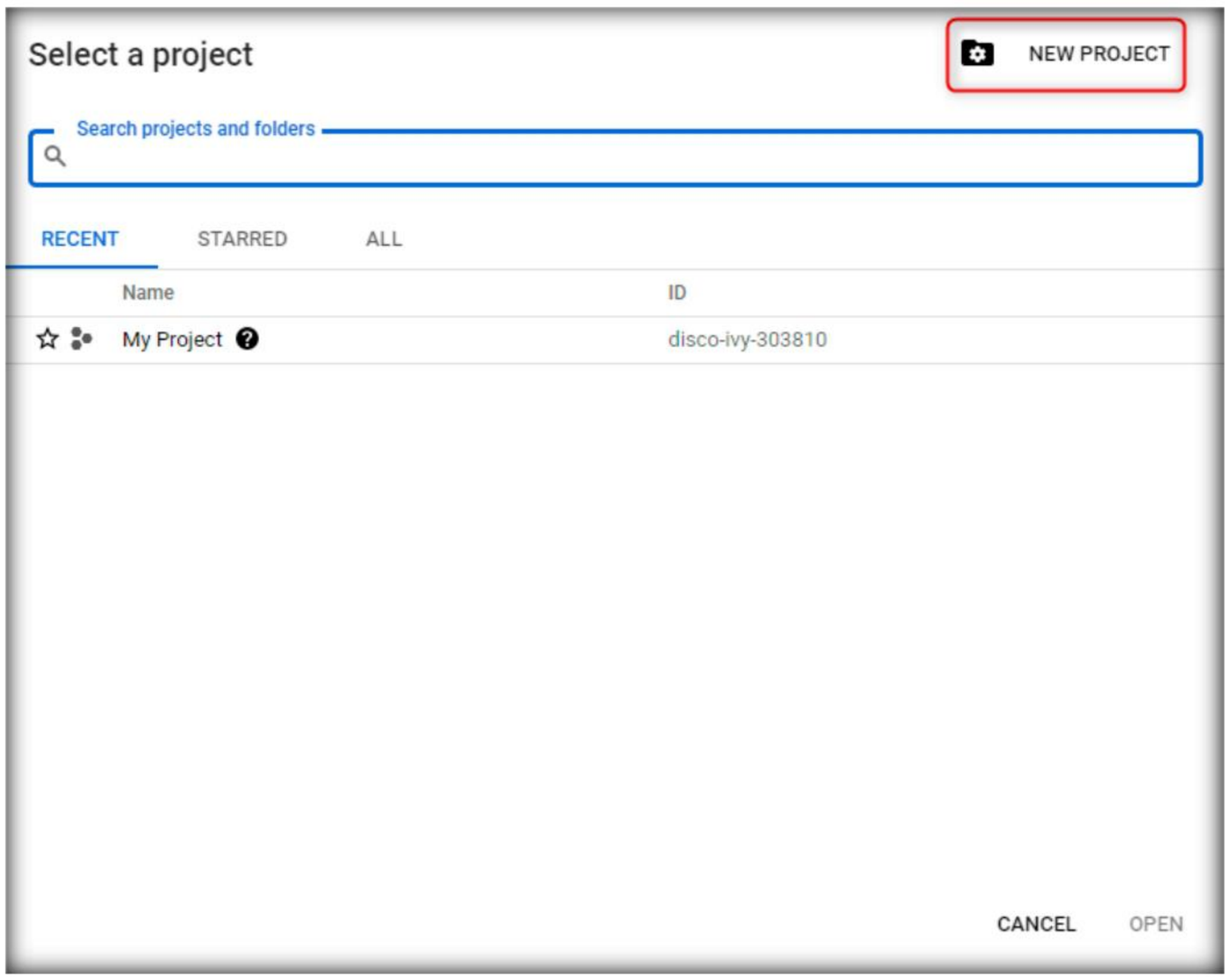


FIGURE 11.3.11: Creating New Project

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

13. The **New project** window opens now. Type the **Name** of the project as **My First Project** and click on **CREATE,** as shown in the following screenshot.

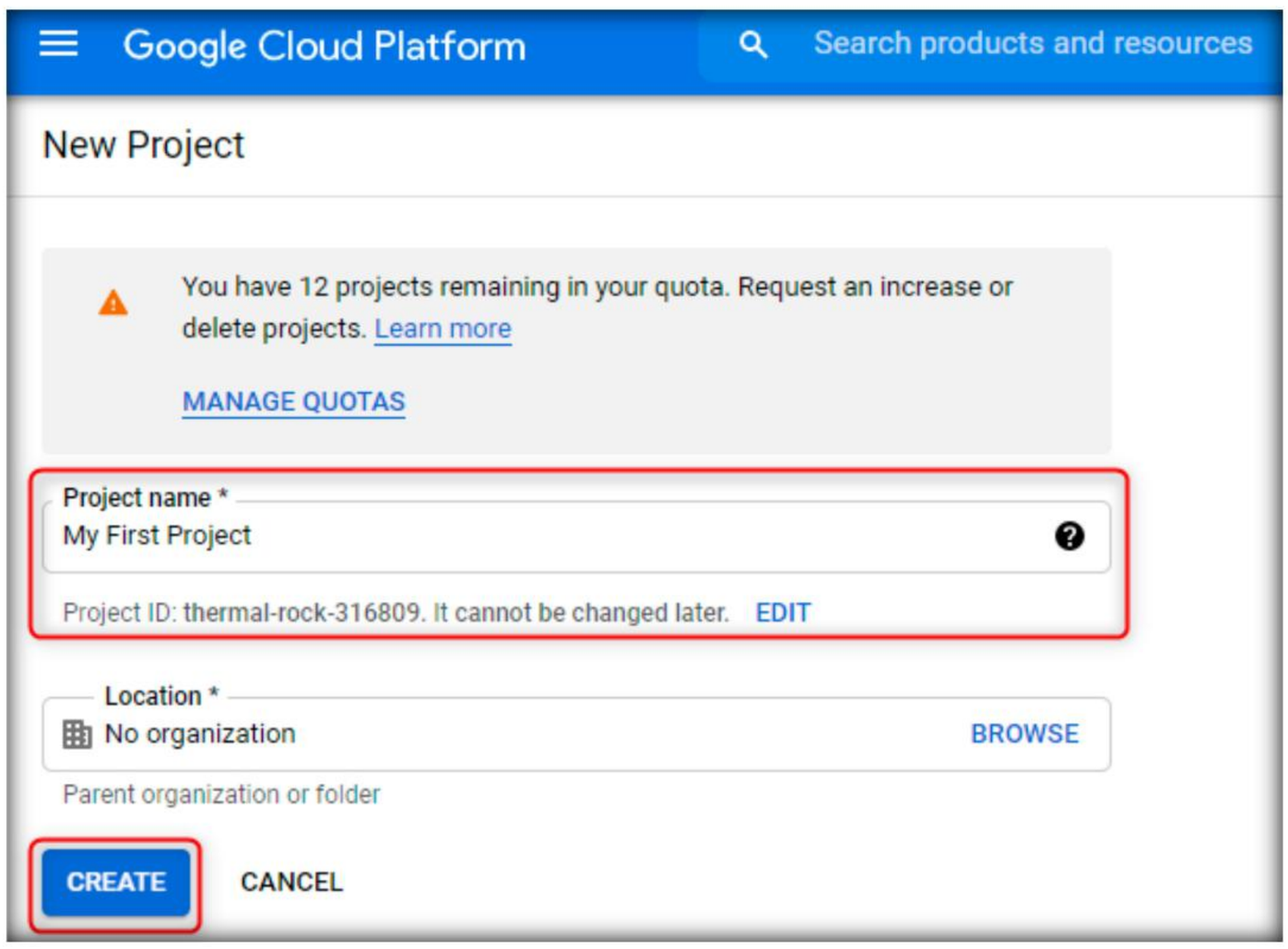


FIGURE 11.3.12: Creating My First Project

14. A new project named **My First Project** will be created. To select **My First Project** as the default project, click on the project dropdown at the top left corner.

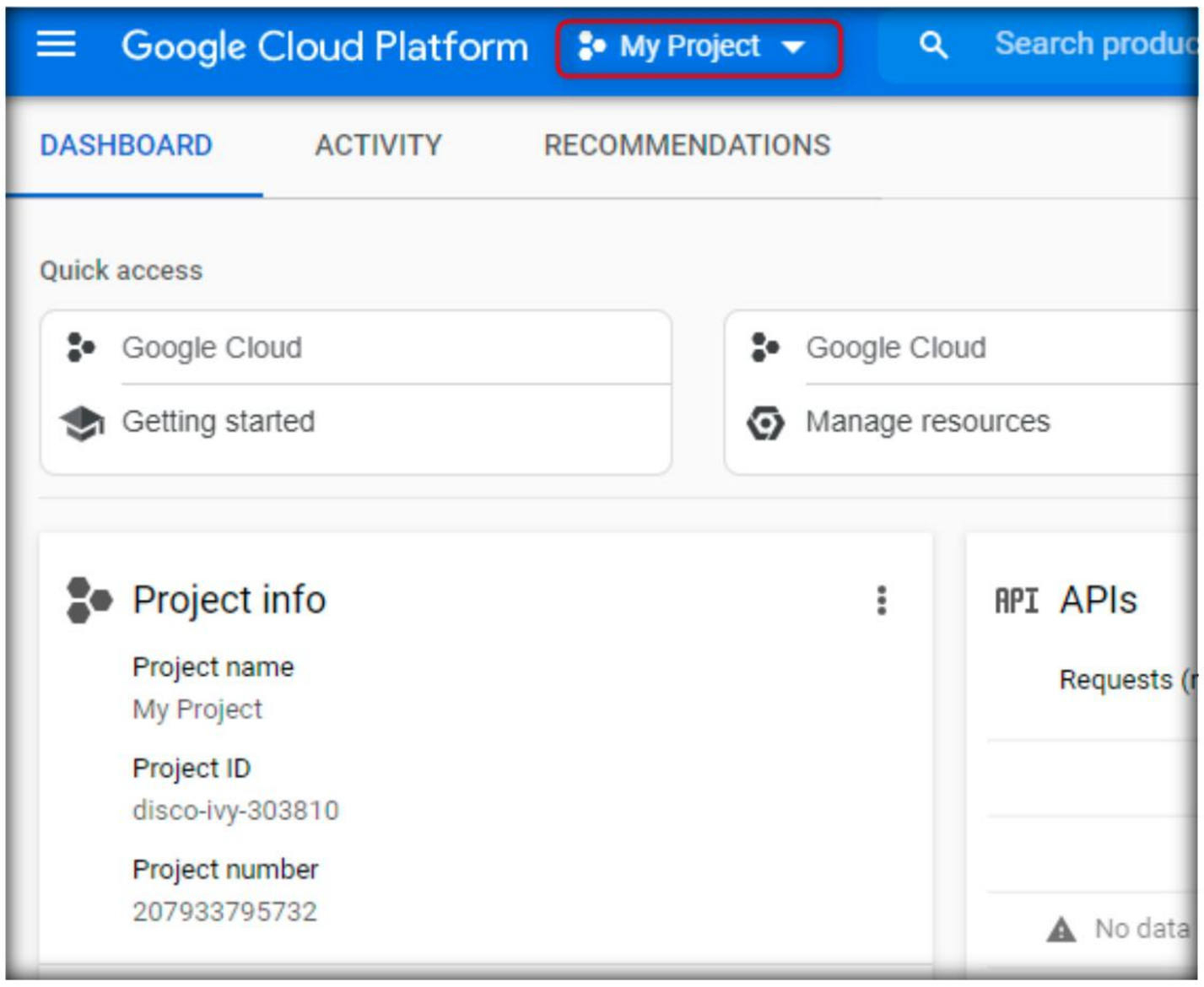


FIGURE 11.3.13: Selecting Project Dropdown

Certified Cloud Security Engineer Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

15. Select **My First Project** from the list of projects.

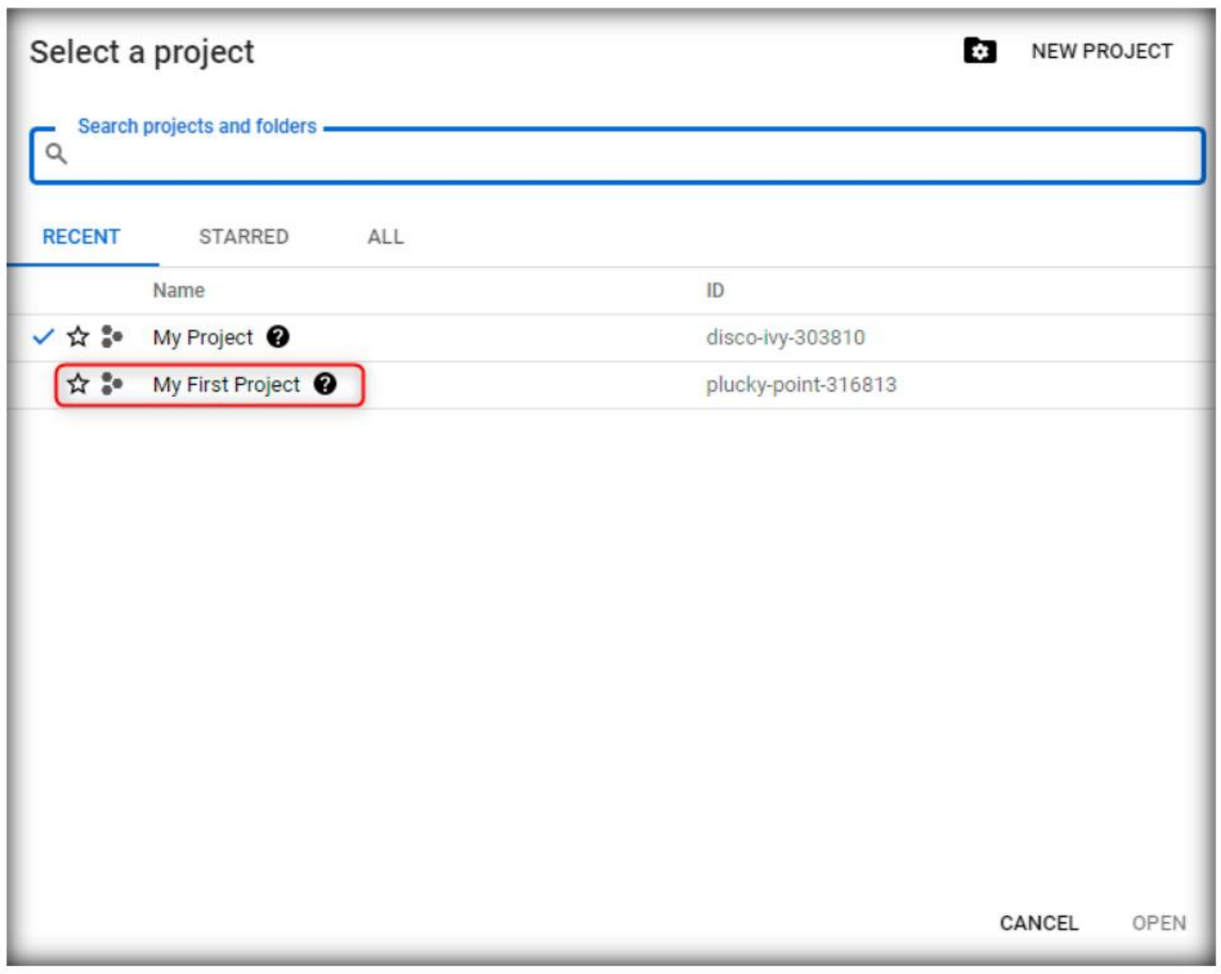


FIGURE 11.3.14: Selecting My First Project

16. **My First Project** will be selected as the default project.

TASK 2

Configuring Cloud Audit Logs for Compute Engine API

17. Auditing of all the admin activities are enabled by default. To enable the auditing of admin logs for specific services, you need to enable it manually. To configure Cloud Audit Logs to enable auditing of Compute Engine API logs, navigate to **IAM &Admin** and click on **Audit Logs** in the console.

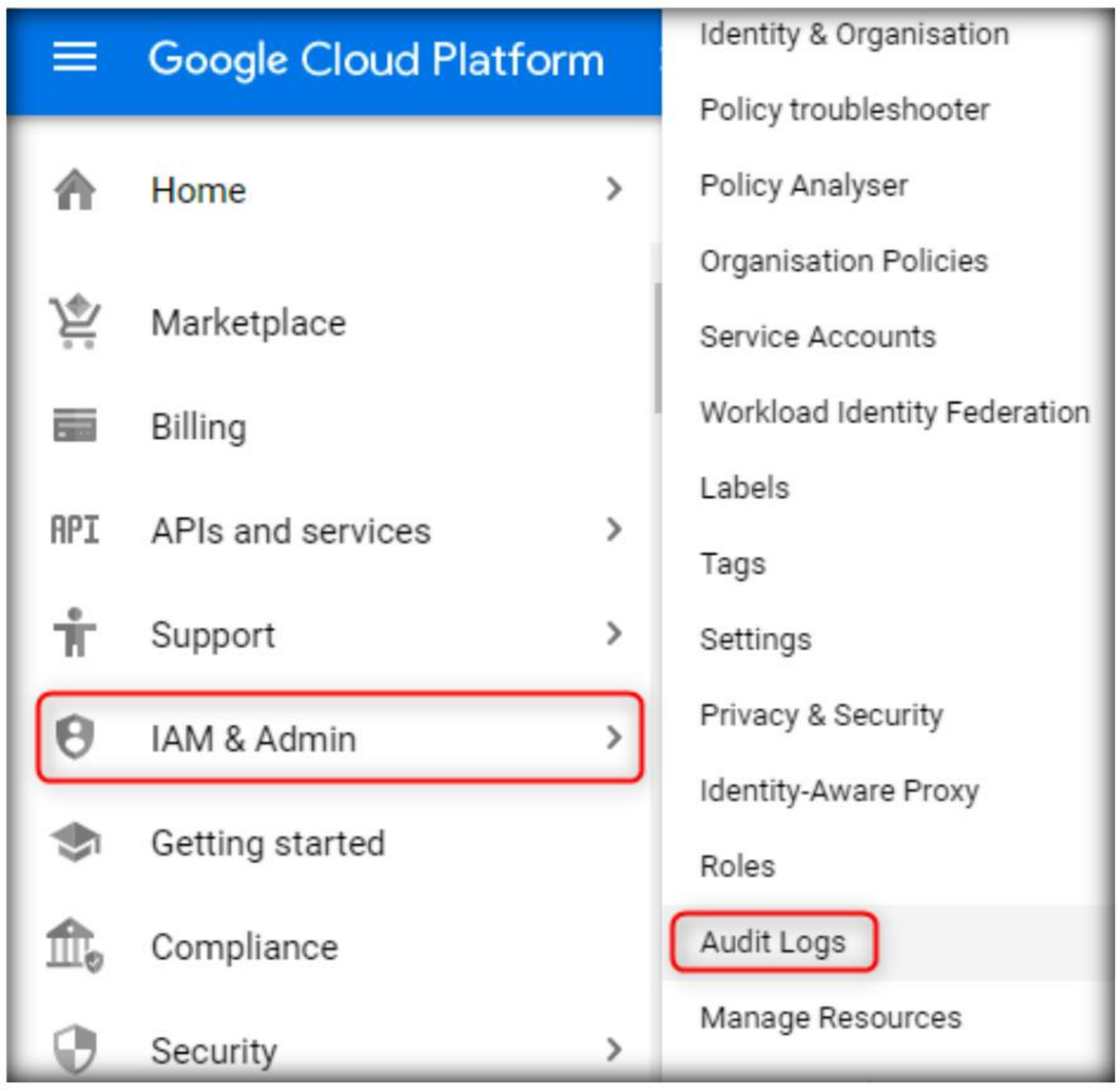


FIGURE 11.3.15: Navigating to Cloud Audit Logs

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

18. You will see a list of services to check/uncheck to enable/disable their **Audit logs.** Scroll down and search **Compute Engine API** service from the list. Check the **Compute Engine API** to enable the audit logs of Compute Engine API service.

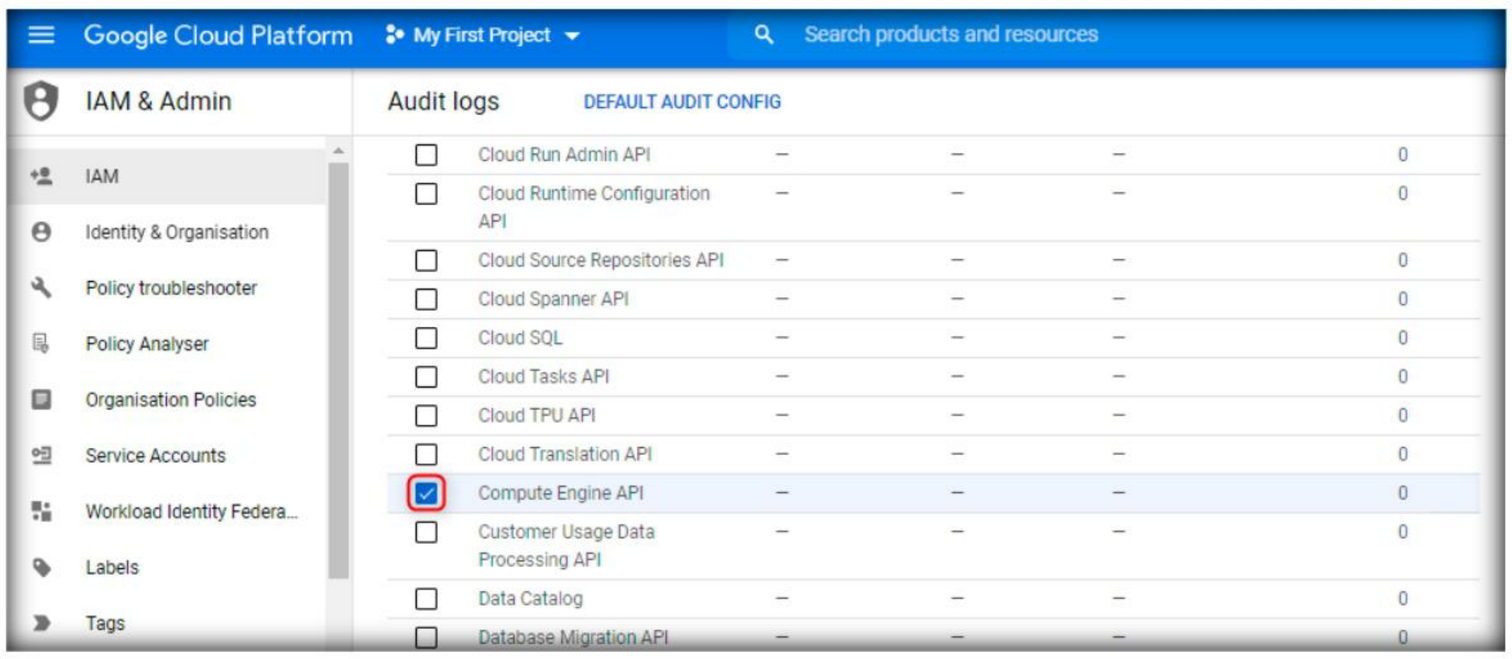


FIGURE 11.3.16: Selecting the Services

19. For turning audit logging on/off for selected services in the Compute Engine API section, select the checkboxes next to **Admin Read, Data Read,** and **Data Write** to turn on the audit logs of **Admin Read, Data Read,** and **Data Write** for the **Compute Engine API** service. Click on **SAVE**.

Note: Admin write is enabled by default.

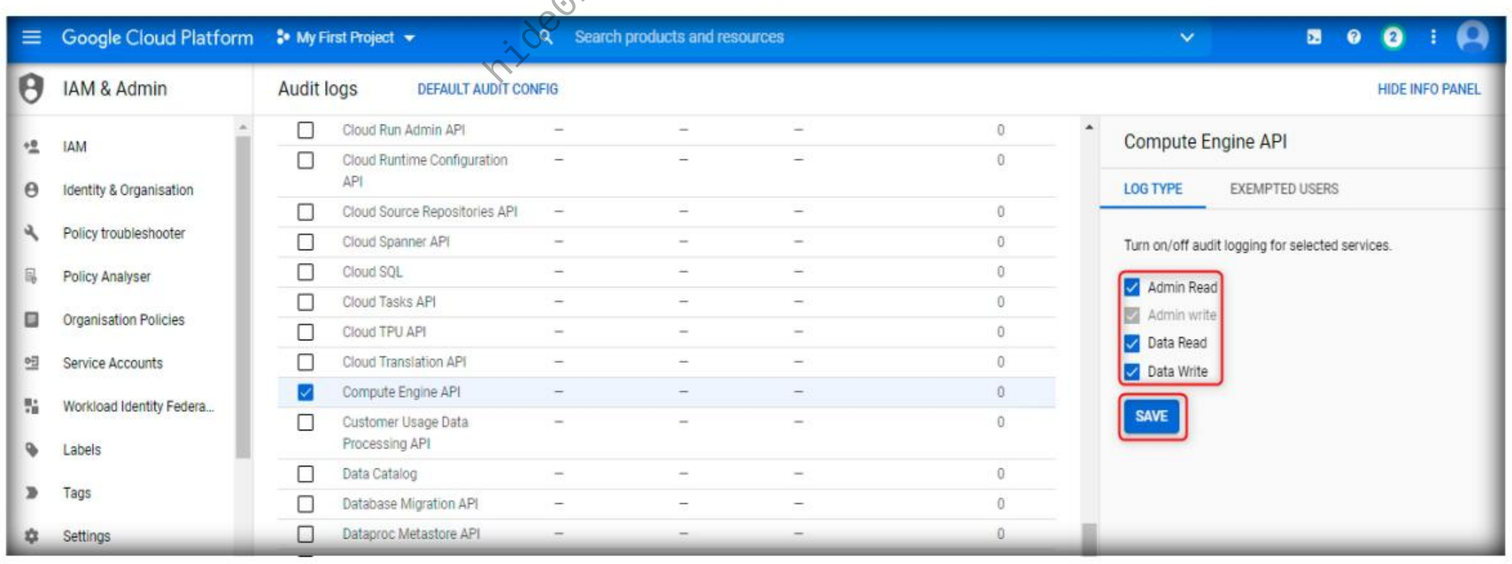


FIGURE 11.3.17: Turning on the audit log services

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 3

Creating a Compute Engine VM instance in GCP

20. Now, the **Compute Engine API** audit logs are enabled. Next, to view the audit logs for Compute Engine events, create a Compute Engine VM instance. To create a Compute Engine VM, Click on the main menu of Google Cloud Console from the top left corner, navigate to **Compute Engine**, and select **VM instances**.

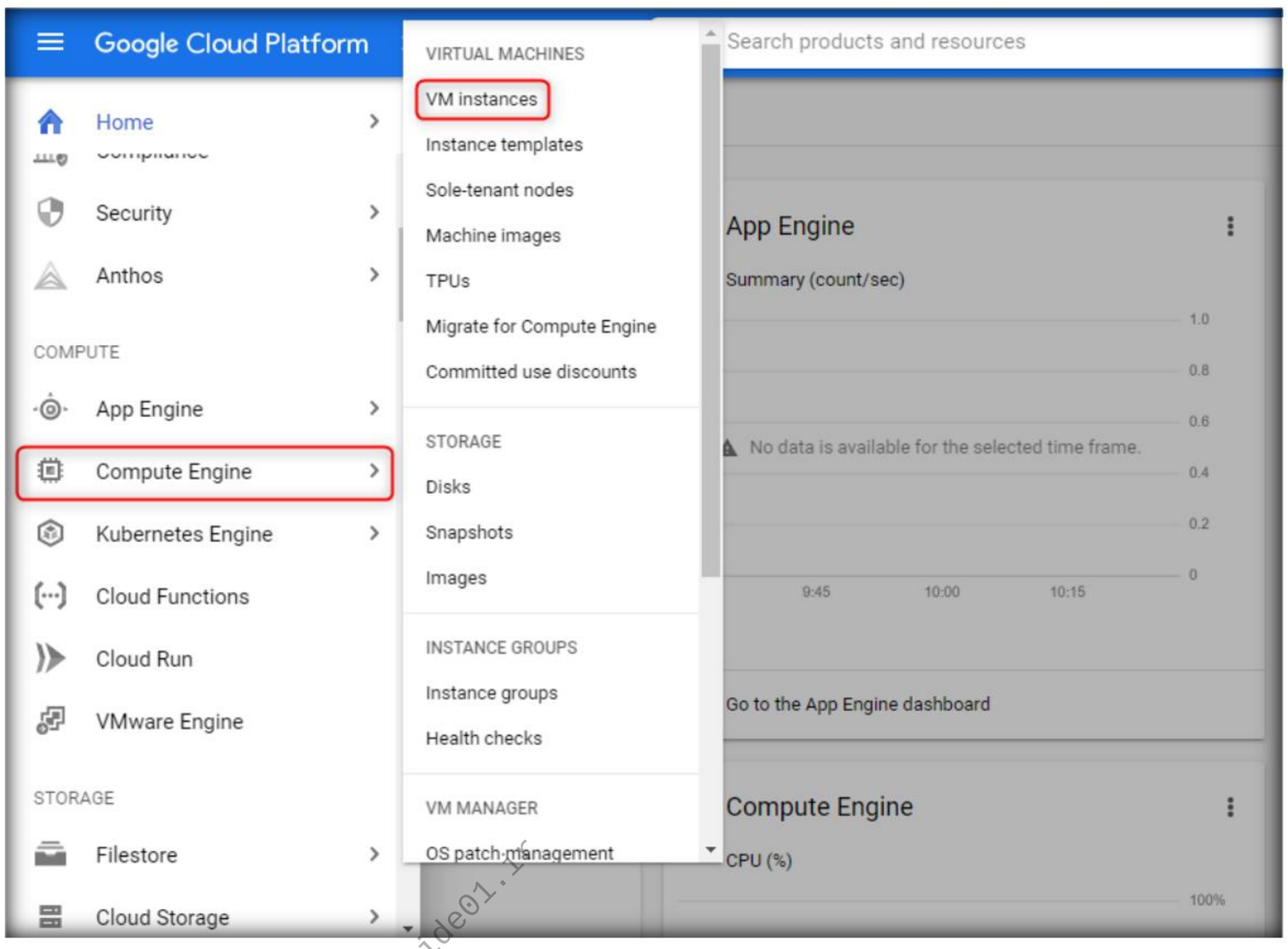


FIGURE 11.3.18: Navigating to VM Instances

21. Next, in the VM instances page, click on **CREATE INSTANCE** to create a new instance.

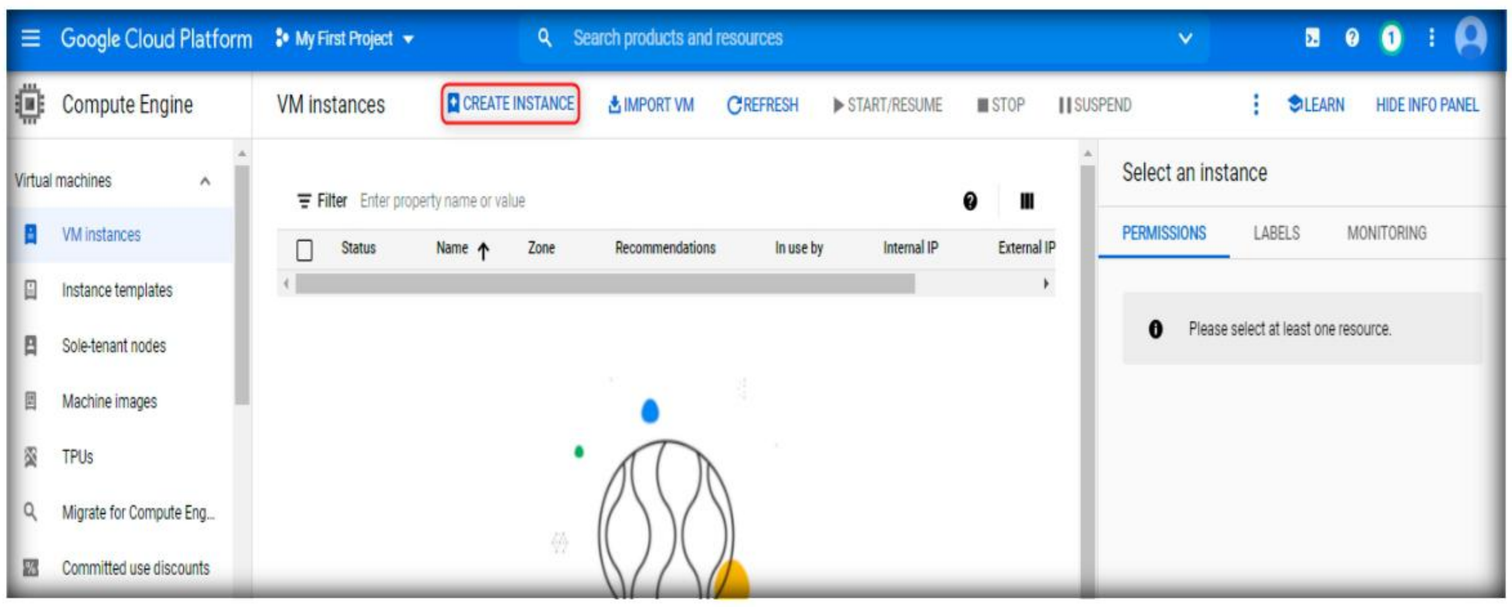


FIGURE 11.3.19: Creating Instance

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

22. Type the **Name** of the instance and select the appropriate **Region** and **Zone**. Here, we are using the following details:

Name: usinstance-1

Region: us-east1

Zone: us-east1-b

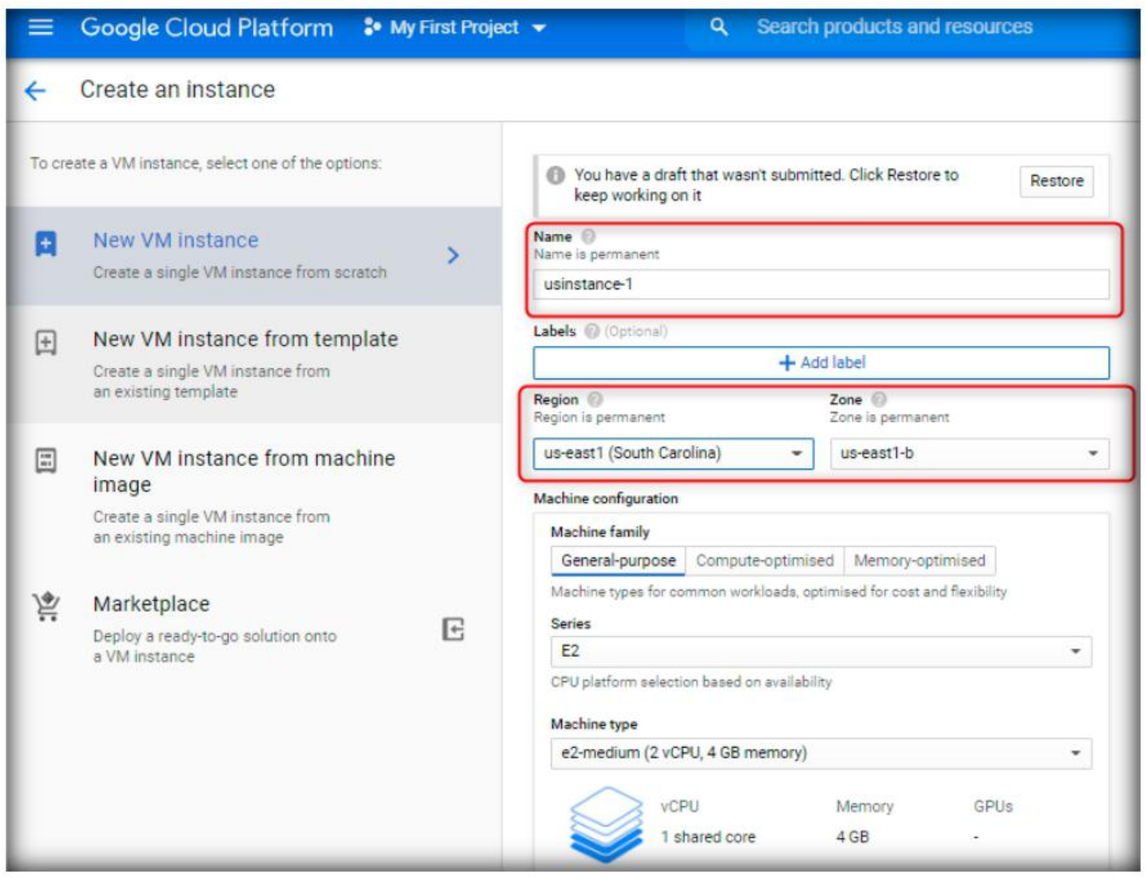


FIGURE 11.3.20: Entering the Name and Selecting the Zone and Region

23. Ensure the **Boot Disk** is **Debian GNU/Linux 10 (buster)**. Retain the other default settings and click on **Create**.

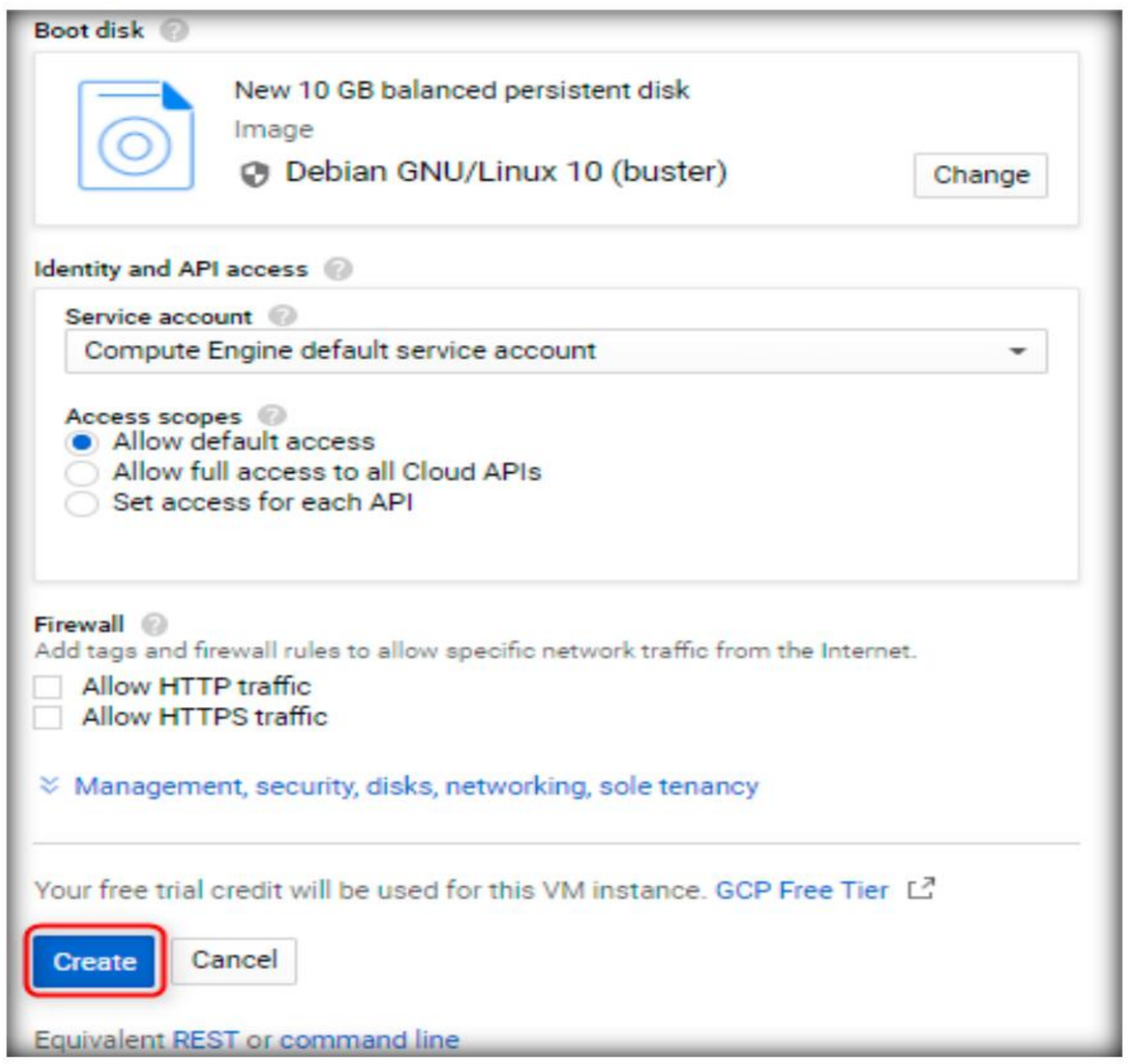


FIGURE 11.3.21: Creating Instance

Certified Cloud Security Engineer Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

24. You can see a green tick mark under **Status,** which confirms the instance is created successfully.

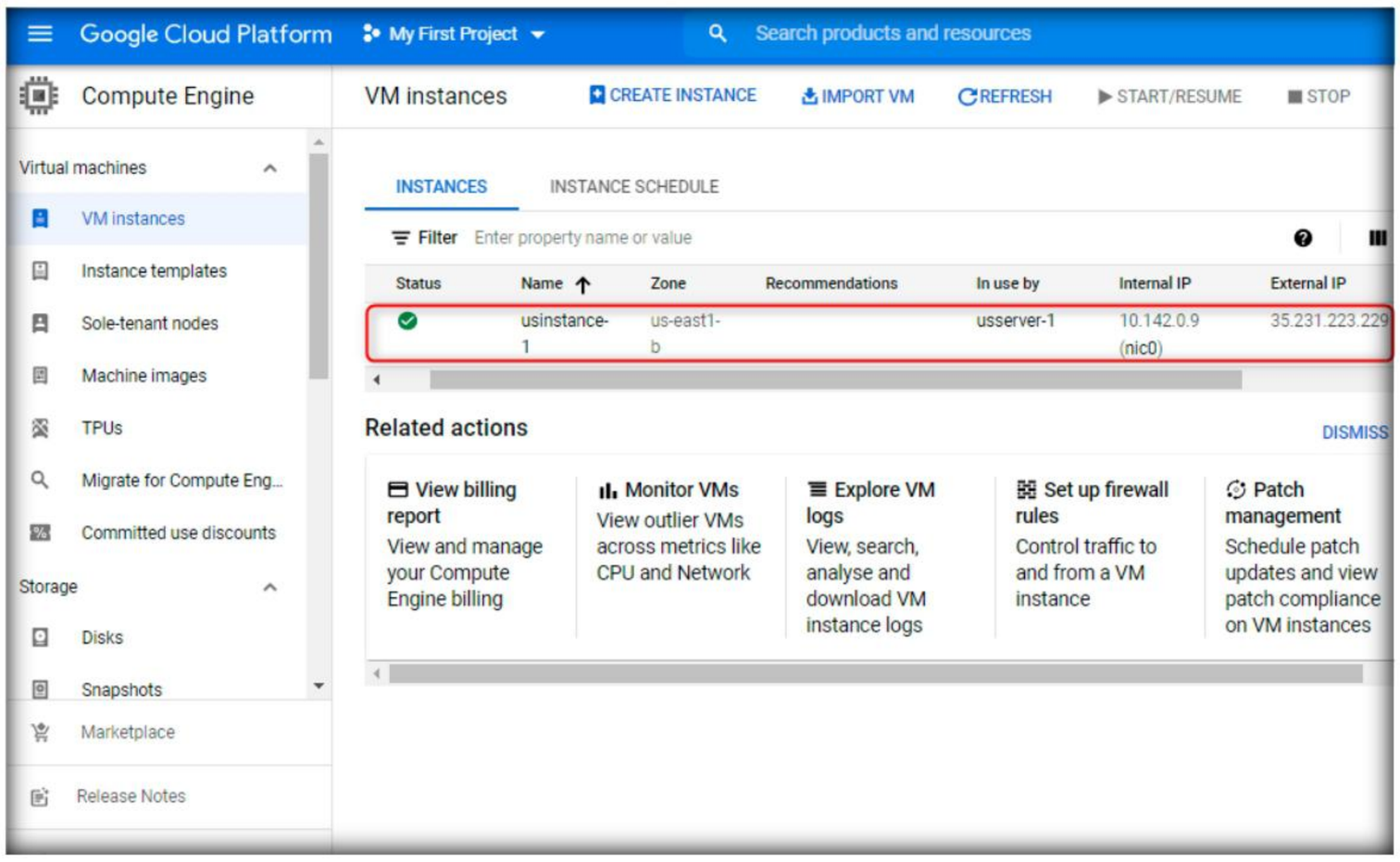


FIGURE 11.3.22: Status of the New Instance as created

TASK 4

Viewing the Audit Logs in Logs explorer

25. Now, after enabling Compute Engine API audit logs and creating a VM instance successfully, we can view the audit logs for a Compute Engine API. To do this, click on the main menu of Google Cloud Console from the top left corner, navigate to **Logging**, and select **Logs Explorer**.

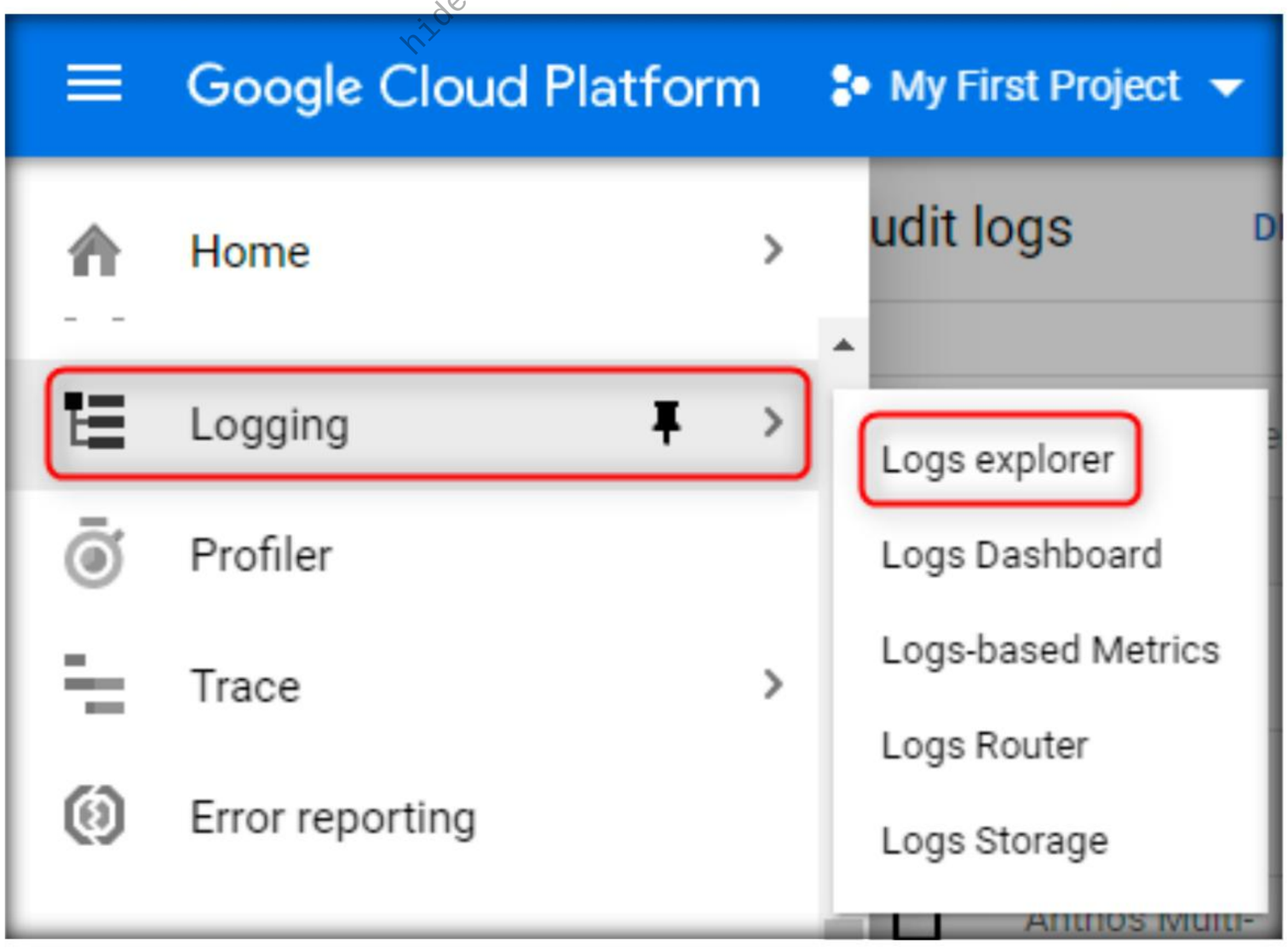


FIGURE 11.3.23: Navigating to Logs Explorer

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

26. You will see the **Logs Explorer** page. Select **Resource** under the **Query** tab**.** Then, scroll down and select **VM Instance**. Select the name of the instance created in the previous task. Then, click **Add**.

    Note: In this lab, we have selected **usinstance-1** to view its audit logs. You can select any VM instance to view its audit logs.

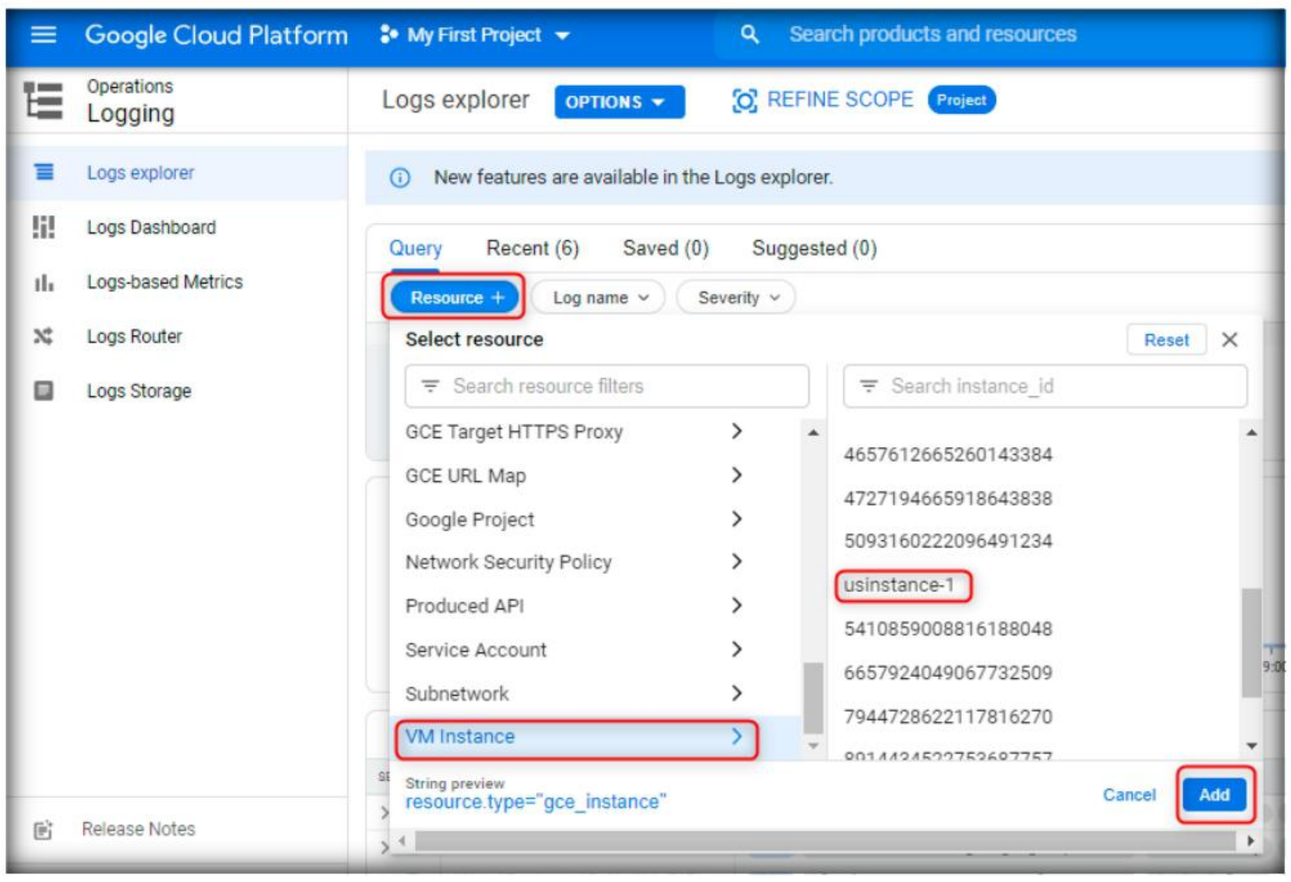


FIGURE 11.3.24: Selecting Resources

27. Next, select **Log Name**. The **Cloud Audit** section displays the types of audit logs. To view the admin activity audit logs, select **activity** and click on **Add**.

    Note: Select the audit log type you want to monitor. Select **data_access** to view data access audit logs and **system_event** to view system event audit logs from the **Cloud Audit** section.

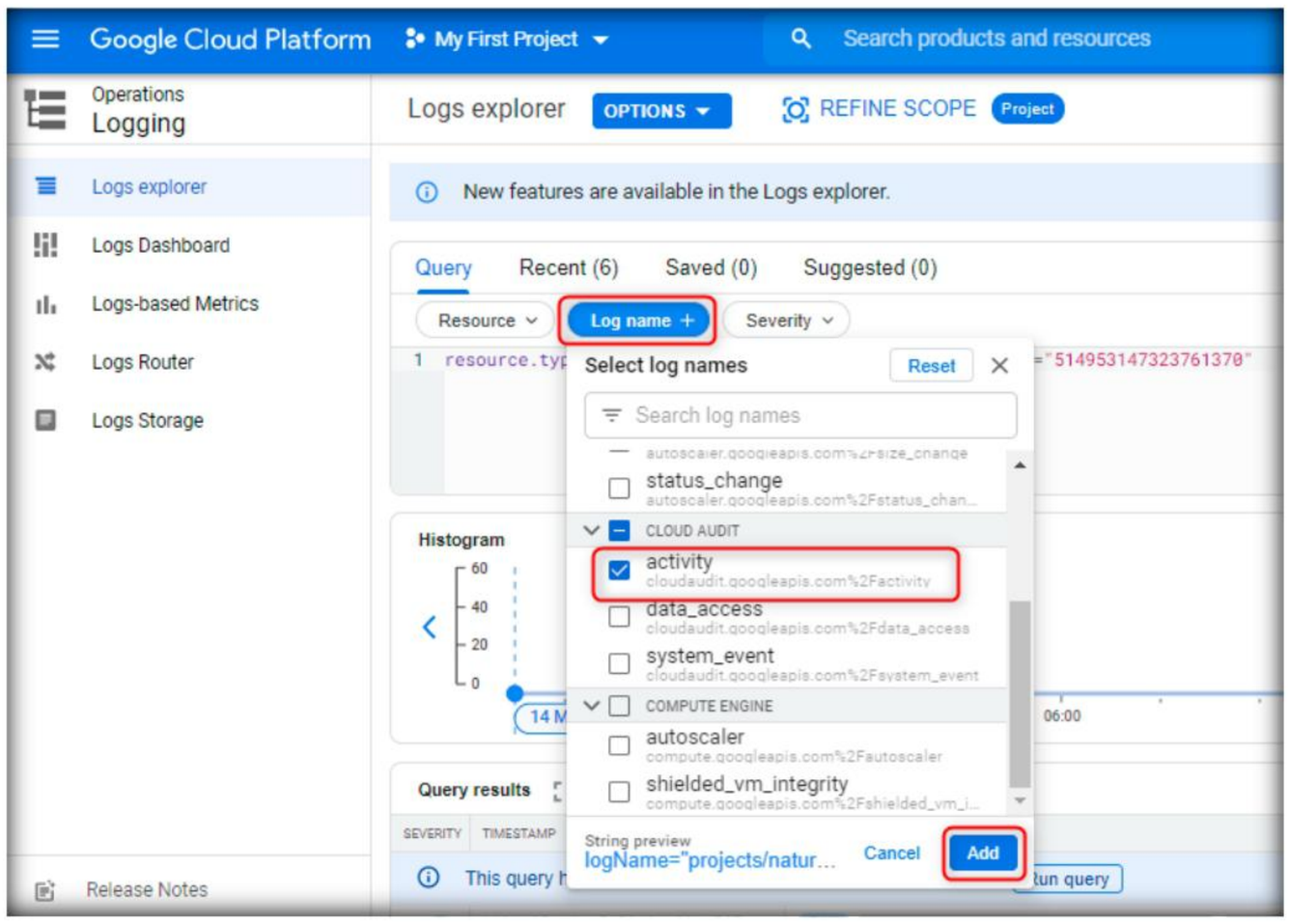


FIGURE 11.3.25: Selecting the type of Audit Logs

hidro1.ir

Certified Cloud Security Engineer Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

28. Click on **Run query** to view the admin activity logs for the selected VM Instance (**usinstance-1)**.

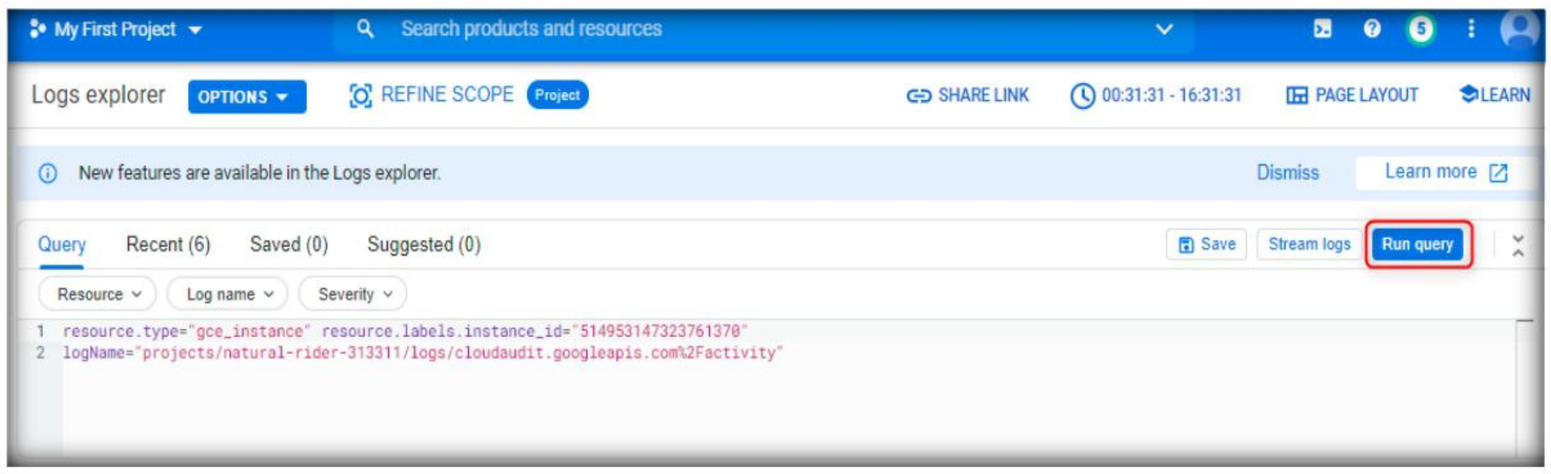
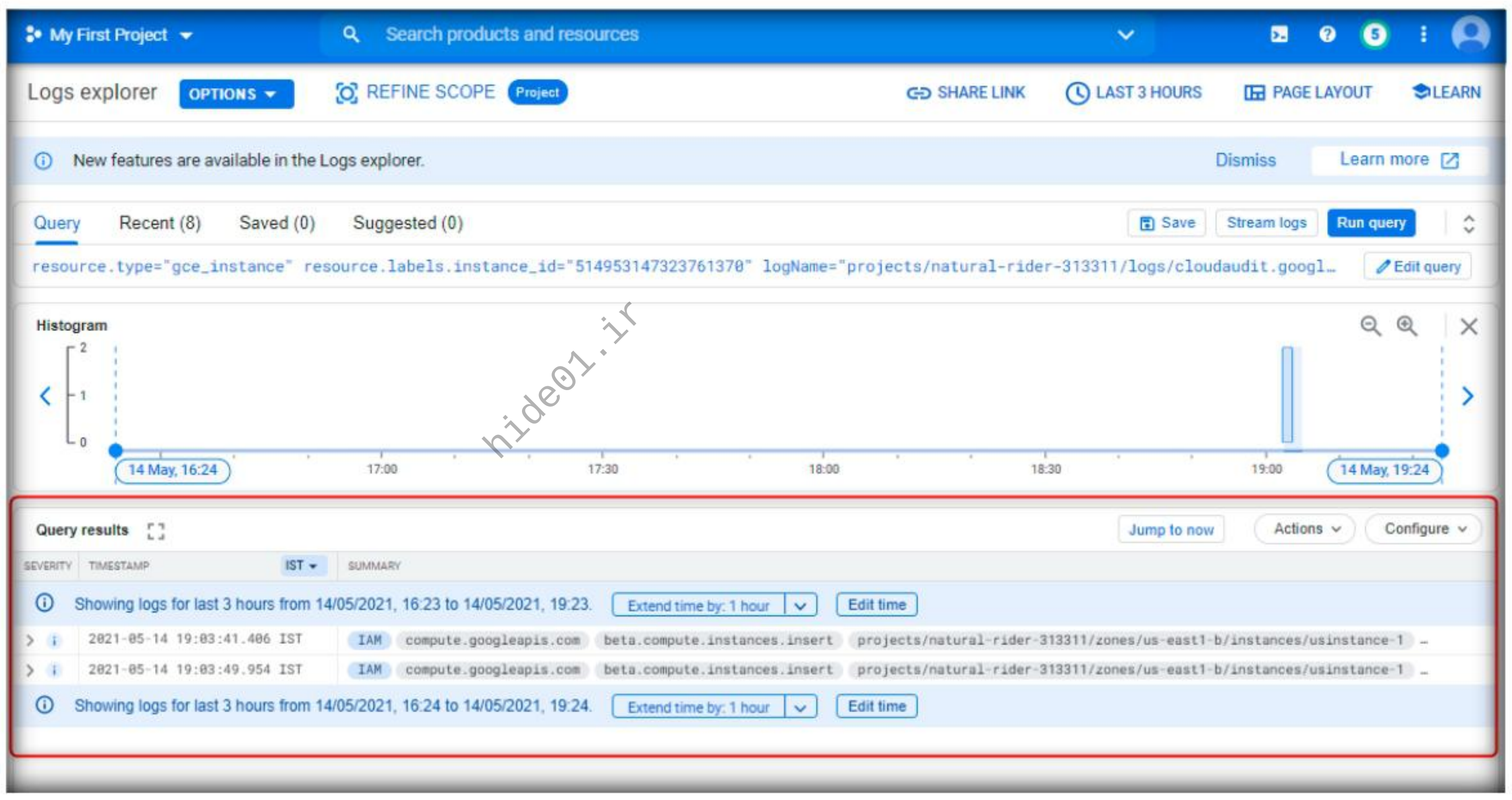


FIGURE 11.3.26: Selecting Run Query

29. In the query results section, you can view the admin activity logs for the selected VM instance (**usinstance-1)**, as shown in the following screenshot. This log shows the details of the events along with their timestamps. You can see events showing admin-created VM instance (**usinstance-1).**



hide01.ir

FIGURE 11.3.27: Viewing the Audit Logs under Query results

30. This way, a cloud security professional can enable and view the audit logs and ensure the compliance requirements of the organization are met.

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

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

31. To delete the VM instance you have created, navigate to **Compute Engine** and select **VM instances** in the left pane. Click on the ellipsis for the VM instance (**usinstance-1**) and click **Delete**. In the pop-up window, click on **Delete**.

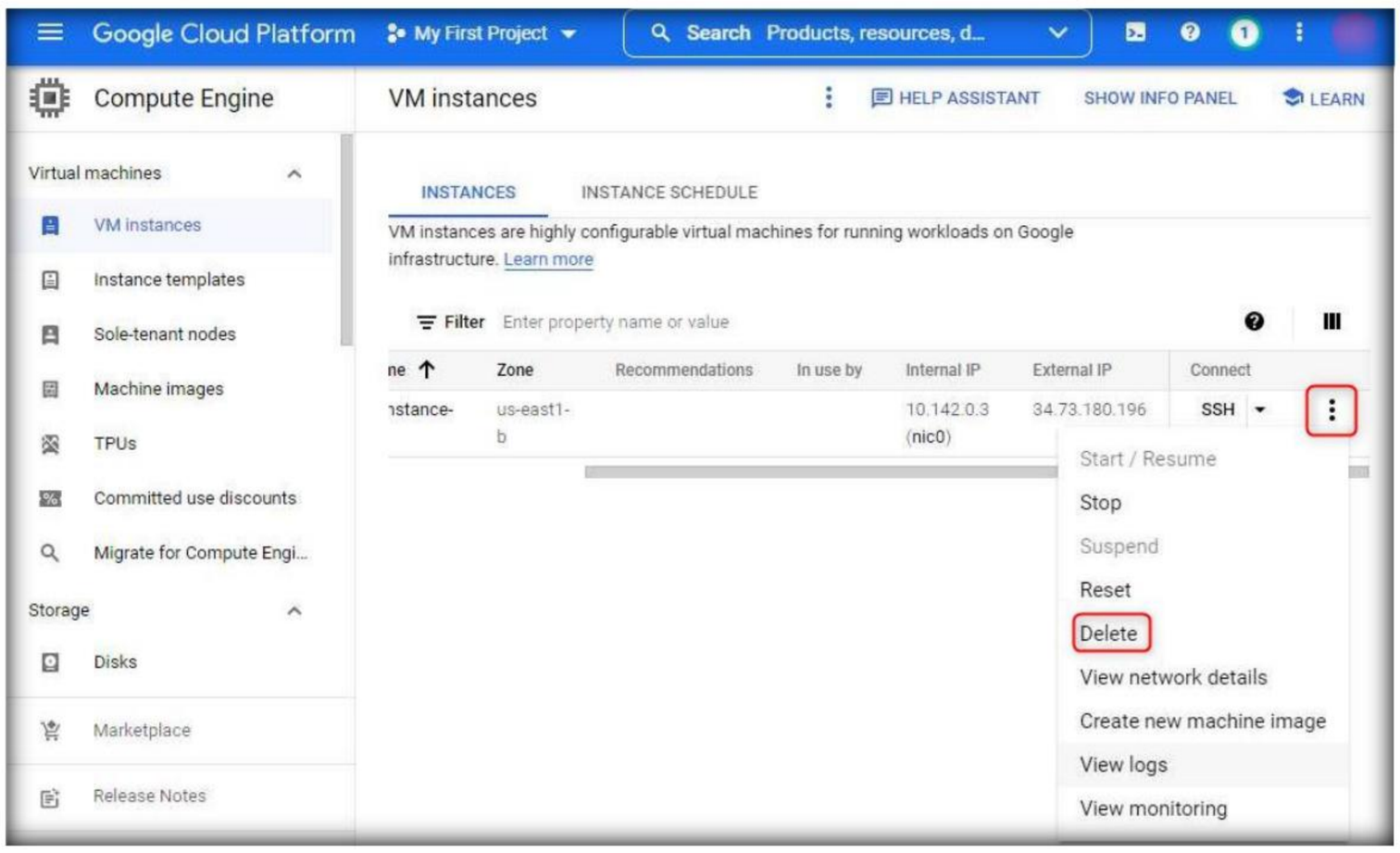


FIGURE 11.3.28: Select the Three Dots for the Instance to Delete it

32. Next, to disable the Compute Engine API logs, navigate to **IAM &Admin** and click on **Audit Logs** in the console. Search **Compute Engine API** service from the list. Check the **Compute Engine API** to disable the audit logs of Compute Engine API service. Uncheck the checkboxes next to **Admin Read**, **Data Read**, and **Data Write**. Click **Save**.

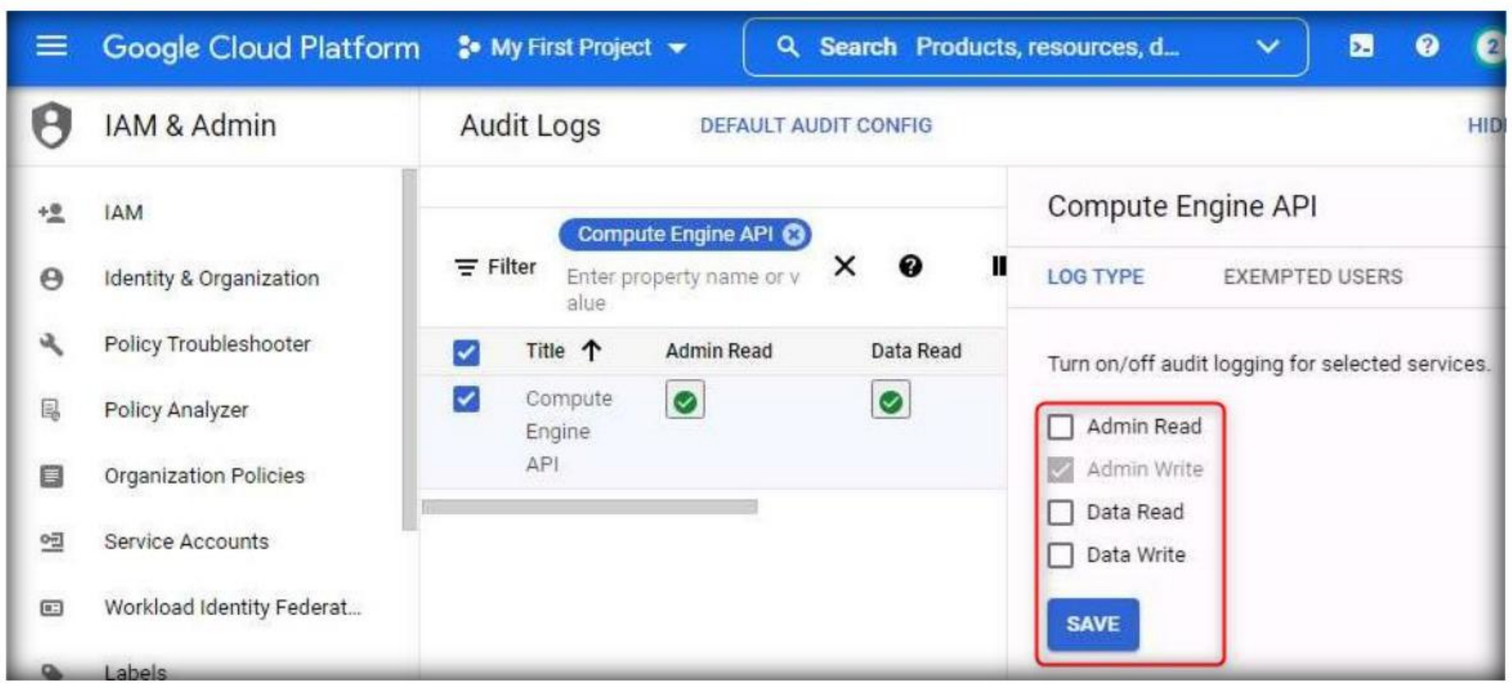


FIGURE 11.3.28: Uncheck the Log Type

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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.

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

This page is intentionally left blank.

hide01.ir