Intro to Cloud Security

Show Split View | Cloud Details | Awards | Help

Learn fundamental concepts regarding securing a cloud environment.

Chart | Scoreboard | Discuss | Writeups | More

Difficulty: Easy

Active Machine Information

Loading... *Loading...* *Loading...* *Loading...*

50%

Task 1 Introduction

Task 2 Architectural Concepts of Cloud

Task 3 Cloud Security Concepts

Task 4 Cloud Security Risks Concerning Deployment Models

Task 5 Security Through Access Management

Access management is an important feature that ensures that the "right people" should do the "right job" within the "right set of permissions". Access management has a critical role in cloud security as data is stored over the internet, and due to a plethora of cyber-attacks, it is inherently insecure. In cloud computing, Access Management is implemented through the following measures:

- **Create Identities**: Cloud infrastructure creates "digital identities" that can relate to a person, user, API or service. An entity is a set of properties that can be recorded.
- **Authentication Factors**: Each identity is allocated with a specific set of characteristics unique to that particular identity and helps to distinguish it from other identities. If they are matched, then the essence of that user is confirmed. These characteristics are called "Authentication Factors", which include: username, password, PIN, biometric, certificate, FaceID, etc.
- **Roles**: Each identity has a specific role which defines the domain under which that particular identity functions.

In Amazon, Access Management is implemented through Identity & Access Management (IAM). IAM is considered the "heart of access management" services to configure & perform fine-grained control and access policies to AWS resources. It is a web service that enables Amazon users to grant access to various services & resources to different users.

Features of IAM

- Give rights & permissions of resources in your amazon account to other people without sharing passwords, etc.
- Grant role-based access to users based on their access rights.
- Enable multi-factor authentication.
- Enable and manage permissions and access policies across amazon accounts & resources.

IAM Important Terminologies

To understand IAM, we must be very clear about its important terminologies:

- Resources: These are objects within a particular service; these include users, roles, groups & policies.
- Identities: Represent certain users permitted and authorised to perform specific roles and actions.
- Entities: A subset of resources which are used for authentication purposes. It includes users & roles.
- Principals: A person or some application requesting to use Amazon resources after signing in.

Using Cloud Environment

We will use examples from Amazon Web Services (AWS) throughout the room. Although the room can be completed with the provided text and image content, the practical exercises require an AWS account. Having an AWS account is optional for this room, but if you are interested, you can visit this URL to understand how to create and activate a new AWS account.

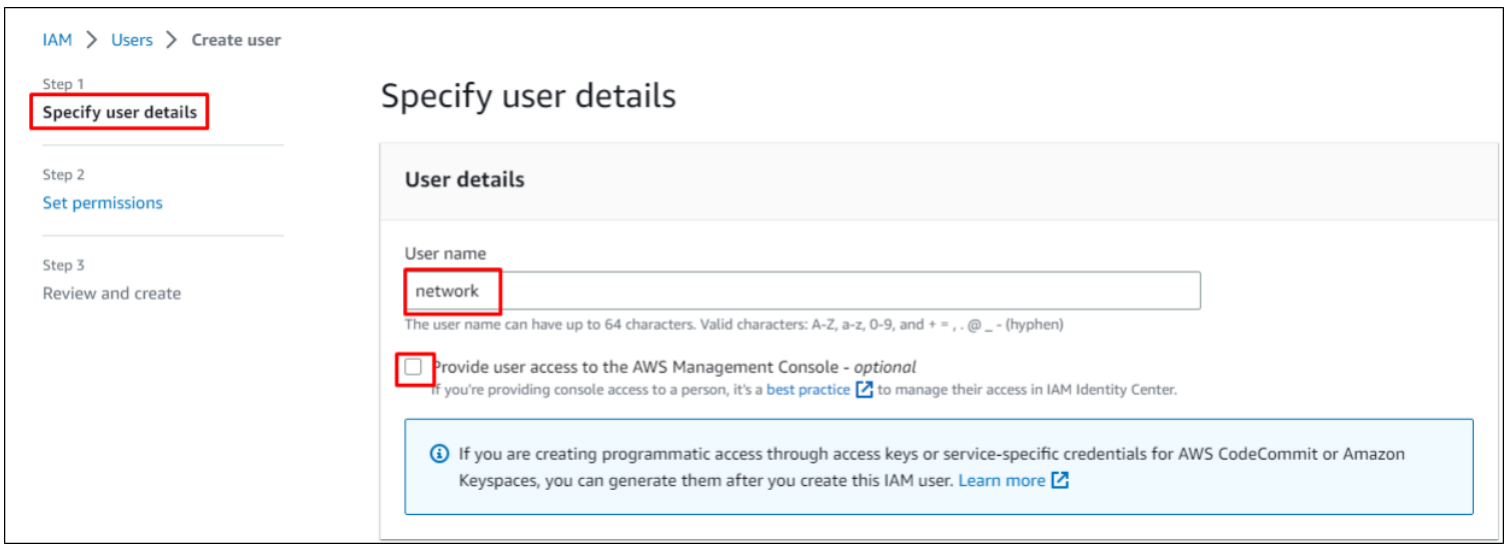
Practical Exercise

Create an IAM user account with administrative privileges in your AWS account. IAM users with administrative privileges will have complete access to AWS resources. Moreover, it can grant permissions to other users as well.

- Login to your AWS account by visiting `console.aws.amazon.com` and navigating "IAM" in the services menu.
- Go to "Users" in the navigation pane and click `Add users` .

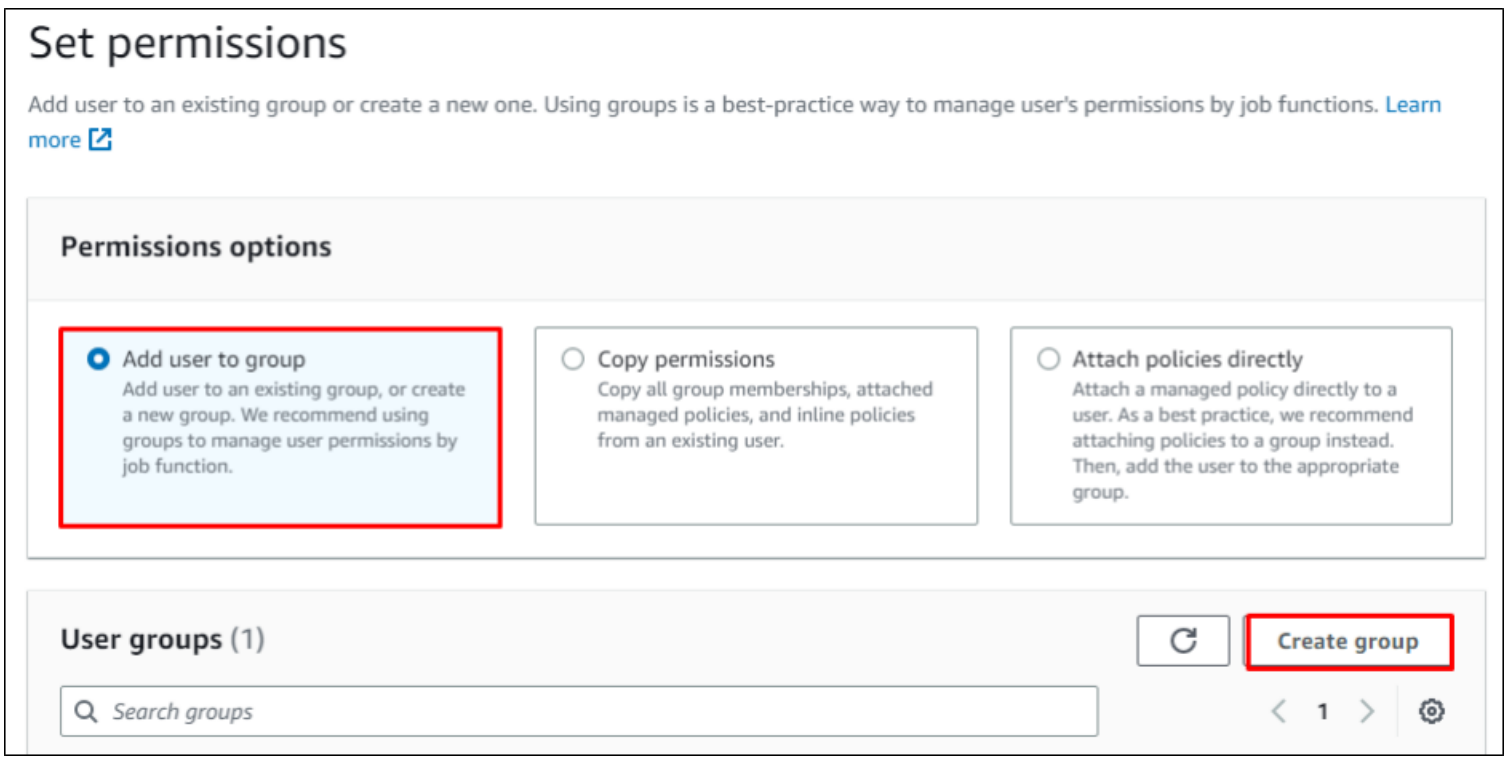
Click to enlarge the image.

- Enter the new username and the user's sign-in name, and Select if you want the user to access AWS Management Console.



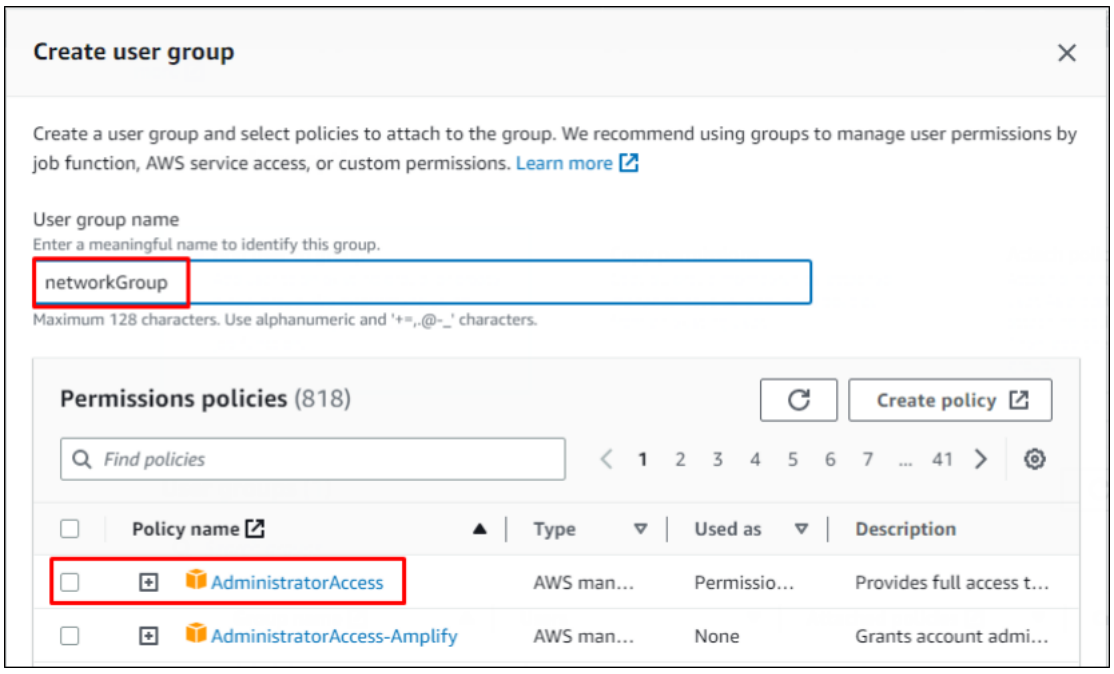
Click to enlarge the image.

- Choose “Next” to go to permissions. Since no group is created, so click on `Create Group` .



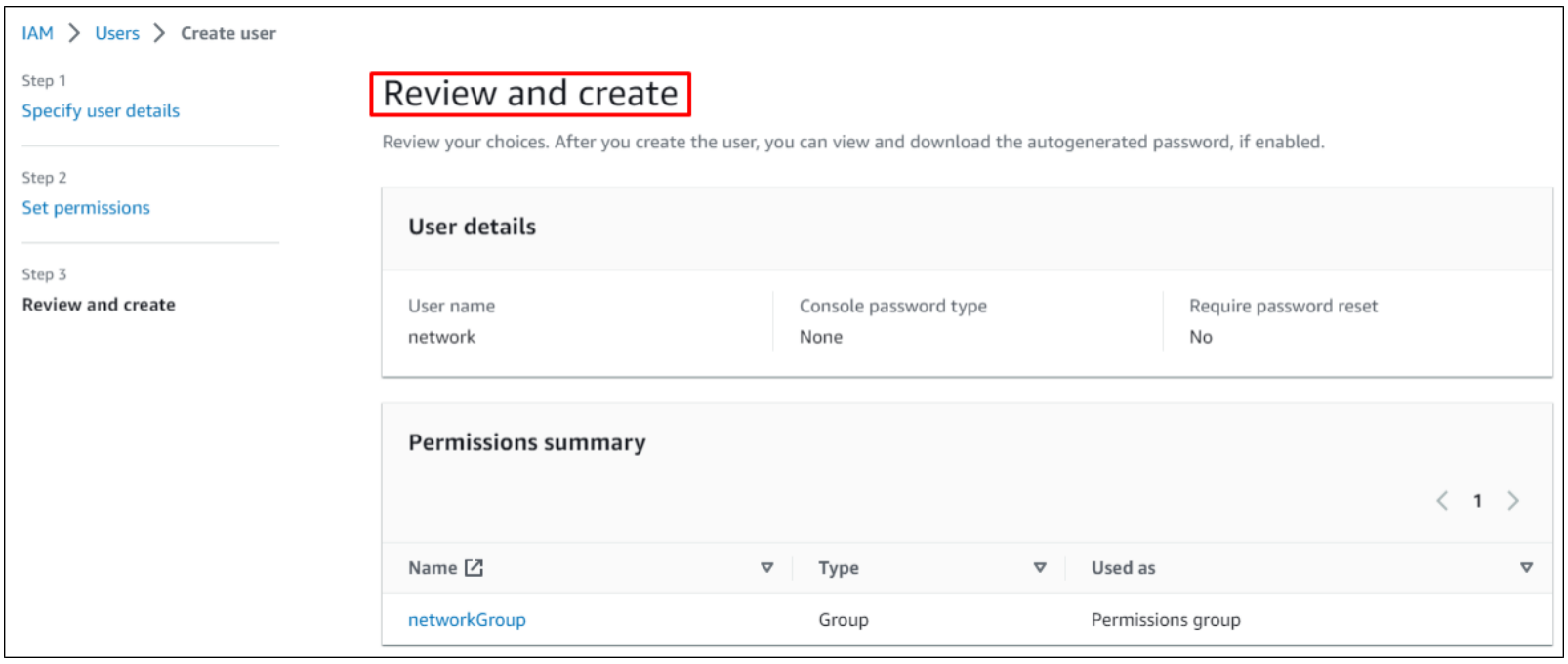
Click to enlarge the image.

- Enter the group name & check `AdministratorAccess` Policy.



Click to enlarge the image.

- Click `Create Group` and then `Review` to go through the settings. If everything is up to the mark, then click **Create User**.



Click to enlarge the image.

- The user has been created. Save the essential details such as username, Password, etc.

Answer the questions below

Are FaceID and biometric types of Authentication factors (yea/nay)?

yea

Correct Answer

I have completed the practical exercise.

No answer needed

Correct Answer

Task 6 ○ Security Through Policies

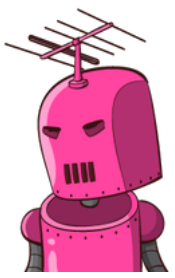
Task 7 ○ Security Through Network Management

Task 8 ○ Security Through Storage Management

Task 9 ○ Cloud Security - Some Additional Concepts

Task 10 ○ Conclusion

Created by 

tryhackme and  1337rce

Only subscribers can deploy virtual machines in this room! Go to your profile page to subscribe (if you have not already). 2037 users are in here and this room is 9 days old.