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...*

61%

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

Task 6 Security Through Policies

Another method of ensuring cloud security is through enforcing policies & permissions. Policies are a set of guidelines and controls which attach to identities and make permissions. The cloud infrastructure evaluates the permissions defined in the policy to determine whether the request should be allowed or denied whenever an identity requests any service. In a typical cloud environment, there are the following types of policies:

- **Identity-based Policies:** Attached to identities and grant permissions.
- **Resource-based Policies:** These are implemented on resources (data & services) and define who is authorised to access that resource.
- **Session-based Policies:** These temporary policies allow access to specific resources for a particular time.

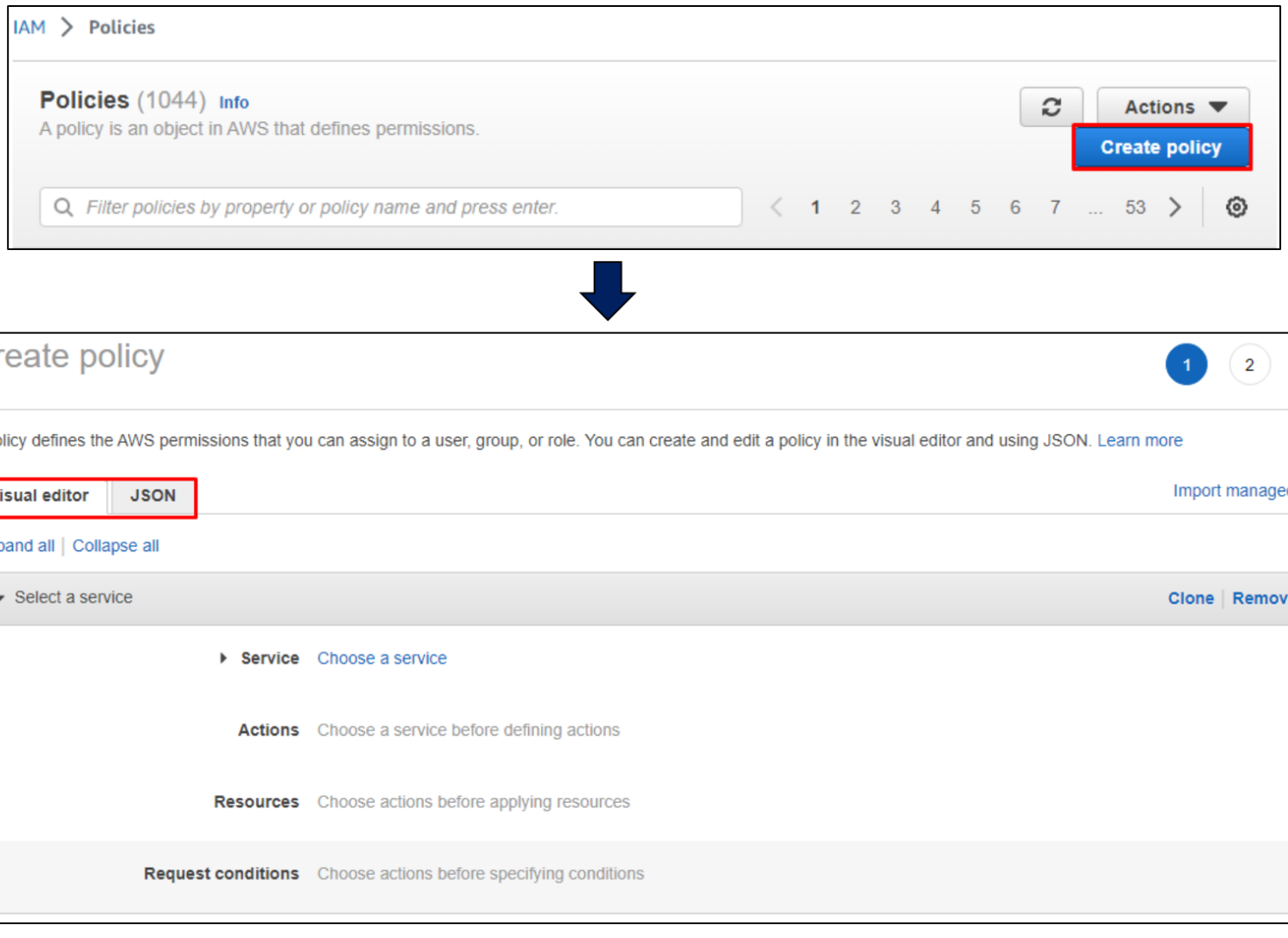
Security through Policies in AWS

In AWS, policies are implemented by AWS IAM. As we have already covered the features of IAM in the previous task, we will directly see how policies are implemented.

Practical Exercise

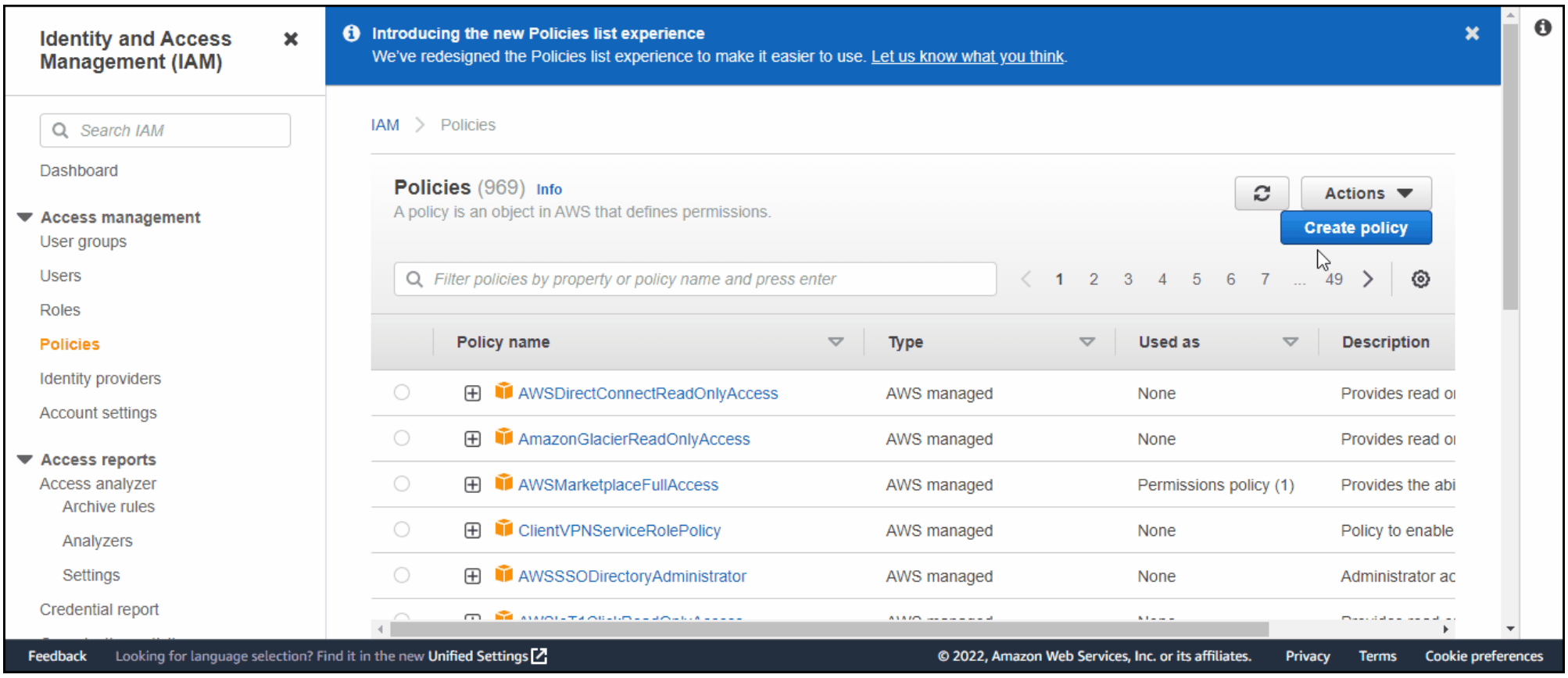
Consider a scenario where a user wants to access resources during a particular date & time.

- Login to your AWS account, Open `IAM` in the services menu and click on `Open Policies` .
- Click on Create Policy - AWS IAM provides two approaches to create a policy, i.e. via **JSON & Visual Editor**.



Click to enlarge the image.

- To define a policy, we first select a service and determine a certain action on a particular resource under a specific condition.



- In the above example, we have selected the service RDS and denied all permissions. We can attach the policy with an identity so the user cannot access the RDS service. The primary idea is to have a granular level of access control through policies to restrict or enable access to a specific resource.

Answer the questions below

In a cloud environment, can we create a policy to enable Database access for a user at a specific time of the day (yea/nay)?

yea — Correct Answer

I have completed the practical exercise.

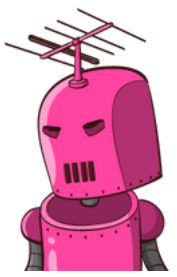
No answer needed — Correct Answer

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.