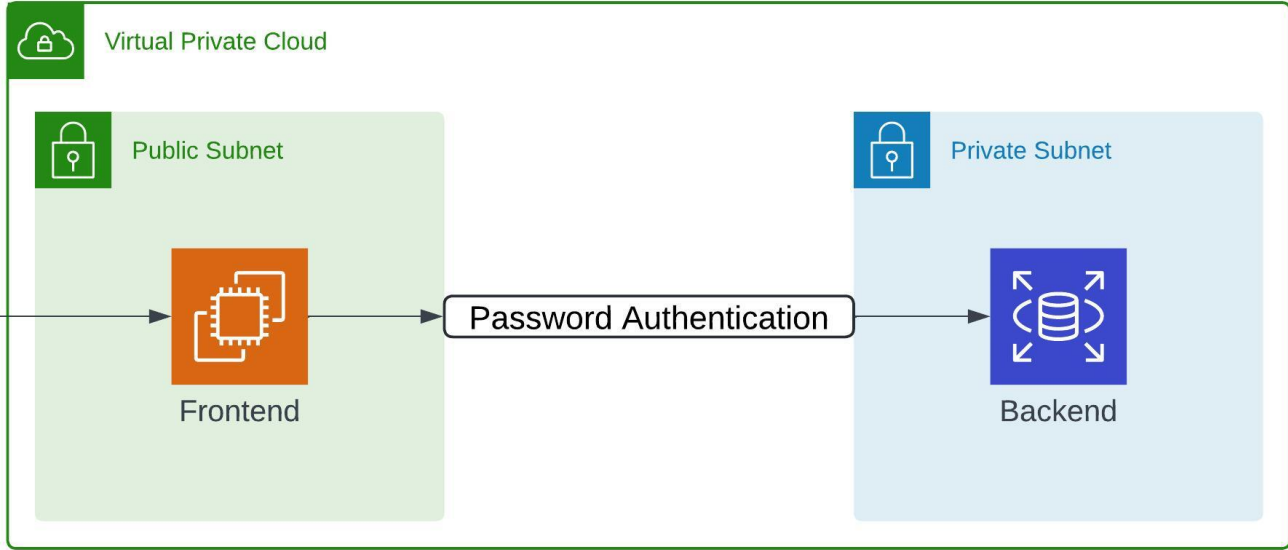


1



Password Authentication

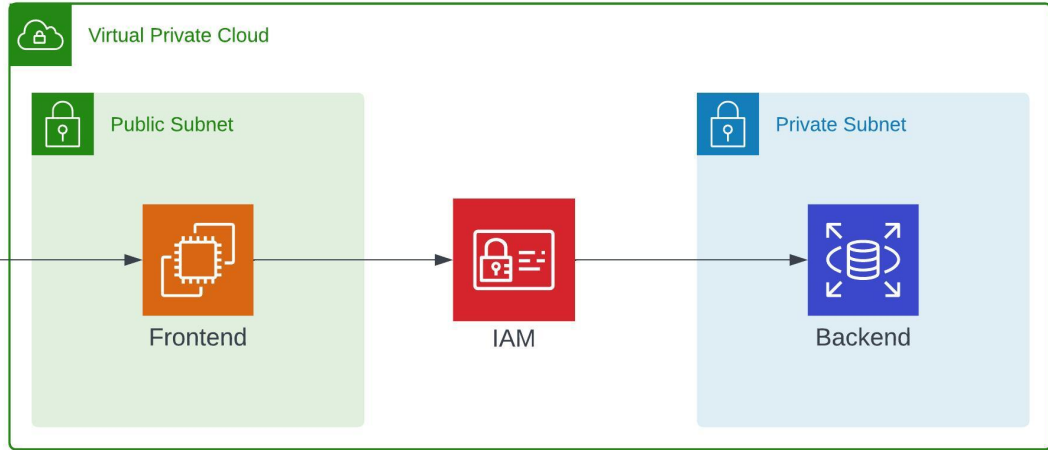
1 Overview

- 1 This is the most basic and commonly used method for authenticating access to a database
- 2 Users connect using a username and password, which the database verifies against its internal user database.

3 Use Case

- 1 Imagine a small company developing a new inventory management application.
- 2 During the development phase, the application is only accessible to the developers within the company network (internal use only).
- 3 To test the app's database functions, developers set up the database using password authentication.
- 4 This setup allows them to quickly access and test the database using simple credentials without needing to configure complex security features.
- 5 Since the application is still under development and not exposed to the internet, this method is efficient and appropriate

2



Password and IAM Database Authentication

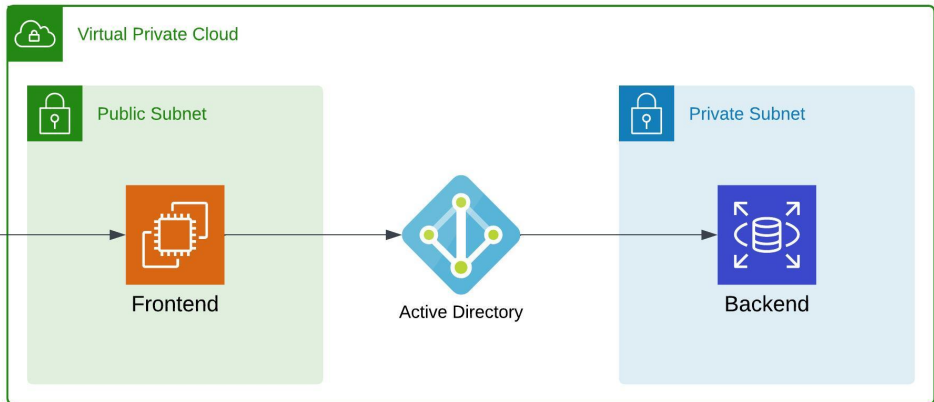
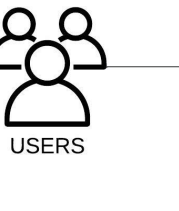
1 Overview

- 1 Combines traditional password authentication with AWS IAM for improved security, using temporary tokens instead of long-term passwords.
- 2 It enables centralized access control and integrates seamlessly with existing IAM policies.

3 Use Case

- 1 A medium-sized company manages multiple environments (development, testing, and production) for their e-commerce application.
- 2 They want to ensure that developers only access the production database when absolutely necessary.
- 3 By using IAM database authentication, they can issue temporary tokens for developers who need to troubleshoot or test specific features.
- 4 This approach minimizes risk, as tokens automatically expire, and access can be easily controlled and monitored through IAM policies.

3



Password and Kerberos Authentication

1 Overview

- 1 Integrates AWS RDS with an existing Active Directory setup using the Kerberos protocol.
- 2 It allows centralized, secure database access management, typically used in enterprise environments with Single Sign-On (SSO) systems

3 Use Case

- 1 A large organization has multiple applications and services, all using centralized authentication through Active Directory.
- 2 The company wants employees to use a single login to access various resources, including their financial management database.
- 3 By using Kerberos authentication, they integrate the AWS RDS database with their existing Active Directory setup.
- 4 Employees log in once with their company credentials, and the system grants them secure, consistent access to the database, aligning with their overall security policies.