Amazon Web Services

Password Policy

ankitnarula1991@gmail.com

Password Policy

- We can set a custom password policy on our AWS account to specify complexity requirements and mandatory rotation periods for your IAM users' passwords. The IAM password policy does not apply to the AWS account root user password.

- **Default Password Policy for IAM Users**

- If an administrator does not set a custom password policy, IAM user passwords must meet the default AWS password policy. The default password policy enforces the following conditions:

- Minimum password length of 8 characters and a maximum length of 128 characters.

- Minimum of three of the following mix of character types: uppercase, lowercase, numbers, and ! @ # $ % ^ & * ( ) _ + - = [ ] { } | ' symbols.

- Not be identical to your AWS account name or email address

Password Policy - Custom

- When we configure a custom password policy for your account, we can specify the following conditions:

- Password minimum length: We can specify a minimum of 6 characters and a maximum of 128 characters.

- Password strength: You can select any of the following check boxes to define the strength of your IAM user passwords:

- Require at least one uppercase letter from Latin alphabet (A–Z)

- Require at least one lowercase letter from Latin alphabet (a–z)

- Require at least one number

- Require at least one non alphanumeric character ! @ # $ % ^ & * ( ) _ + - = [ ] { } | '

- Password Expiration: Require users to change the password after some days

- Allow All IAM users to change their own password

- Prevent Password Reuse: You can prevent IAM users from reusing a specified number of previous passwords. You can specify a minimum number of 1 and a maximum number of 24 previous passwords that can't be repeated.

Password Policy

- Go to IAM

- Click on Account Settings

- Click on Change

- We can check the boxes as per our requirement, we need to apply the password policy.

- Click on save changes

Thank You!

ankitnarula1991@gmail.com