Day 11/100 AWS

AWS- IAM Accolunt Reot User Overview

Introduction to IAM Account Reot User in AWS:

- A root user is created during the AWS Sign-up process.
- All AWS accounts have a root user (onlyone)
- Has Complete access to all AWS service and resource in the account.
- Permissions can't be restricted by any means (except if Service Control Policy attached to your account).
- Is accessed by signing in with the email address and password that you used to create the account.
- You do not use the root user for your everyday tasks, even the administrative ones.

- Securely lock away the root user Credentials and use them to perform only a few account and Service managment tasks.

When to User root user account

- Modify root user details. This includes changing the root password.

- Change your AWS support plan.

- Change your payment options

- View your account billing information. View Billing tax invoices.

- close an AWS account.

- Sign up for GovCloud.

- Find your AWS account Canonical User ID in the Console. You can view your Canonical user ID from the AWS Management Console only while Signed in as the AWS account root user. You can view your Canonical user ID as an IAM user with the AWS API or AWS CLI.

- Restoring IAM user permissions. If an IAM user accidentally revokes their own per-missions You can sign in as the root user to edit policies and restore these permissions

- Change your account settings using the Billing and Cost Management Consule. You can view & edit your Contact and alternate Contact information, the currency that you pay your bills in, the Regions that you can create resource in, and your tax registration numbers.

- Submit a Reverse DNS for Amazon EC2 request.

- Create CloudFront key pair.

- Configuring an Amazon S3 bucket to enable MFA(multi-factor authentication) Delete.

- Editing and deleting an Amazon S3 bucket policy that includes an invalid. VPC ID or VPC endpoint ID.

- Request removal of the port 25 email throttle on your EC2 instances.

- Change the Amazon EC2 settings for ~~throttle on your~~ longer resource IDs. Changing this setting as the root user affect all users and roles in the account. Changing it as an IAM user or IAM role affects only that user or role.

What can go wrong

- Your account can get Compromised
- Intruder may exposes all your data
- Intruder may even delete all your data and resources
- This can easily lead to lawsuits and heavy financial loss.

IAM Best Practices.

~~#~~ · Active MFA on your root account

- Disable / delete your root access Key
- rotate Credentials.
- Do not share root user Credentials.
- Create IAM user with administrative privilege.