(AWS) - PART I

accendnetworks

# A Beginner's Guide to AMAZON WEB SERVICES

Introduction to AWS I AM & Networking and Connectivity

BY: **PAULA WONG**, CEO AND FOUNDER, CEH-MASTER,
CCIE SECURITY AND SWITCHING, C-7 #1086962
AWS CERTIFIED CLOUD PRACTITIONER

## Introduction to AWS I AM



## Networking and Connectivity

# A Comprehensive Guide To Securing Your Aws Root User

At the core of your AWS account lies the root user, the ultimate authority that wields unparalleled power to control every aspect of your AWS environment. It is therefore, no exaggeration to say that the root user is the linchpin of your AWS security. Failing to secure this key account could lead to catastrophic consequences, from data breaches to financial losses, and damage to your organization's reputation.

This article serves as your essential guide to understanding the significance of securing your AWS root user. We will explore the unique risks associated with this account, discuss best practices, and provide practical steps to ensure its robust protection. Let's embark on this crucial voyage toward safeguarding your AWS infrastructure.

# What is a root user?

When you first create an Amazon Web Services (AWS) account, you begin with a single sign-in identity that has complete access to all AWS services and resources in the account. So basically, the identity used for the account creation is the root user. You can sign in as the root user using the email address and password that you used to create the account

The root account is the most privileged AWS account; it has unrestricted access to all resources in the AWS account.

# Security best practices for a root user:

## Avoid the use of root account!

Surprising right? There may be two questions that instantly come up: WHY and HOW?

## WHY to avoid the use of root account?

The root account is the most privileged account with all the access, and hence compromise of a root account potentially means a transfer of ownership, as the attacker has the privilege to change the root password and keep the account.

So, it is recommended to avoid/minimize the use of root account.

# HOW to access the AWS Console then, if not the root account?

One

# IAM User Administrator Account:

Immediately after creating an AWS account, one should start by creating an IAM user account specifically designated as the administrator account. This user should have elevated permissions but not full root access. This strategy minimizes the chances of unintended actions and provides a clear audit trail for all activities.

# The Role of the Admin User:

The administrator user should be responsible for the following tasks:

**Regular Administrative Tasks:** All routine administrative tasks, such as creating, modifying, or deleting user accounts, configuring security policies, and managing resources, should be performed through the administrator account.

**Access Control:** The administrator account can delegate access rights to other users or roles, ensuring proper segregation of duties and limiting the scope of each administrator's responsibility.

**Monitoring and Auditing:**The administrator should regularly review logs, access history, and monitor for any unusual activities within the system, maintaining a high level of vigilance.

# Using the Administrator Account:

To maintain security, administrators should use the IAM administrator account for all their day-to-day activities. Using root access should be reserved for essential system maintenance or configuration changes that cannot be accomplished through the IAM administrator account.

# Setup root account usage alarms.

Using Amazon CloudWatch alarms to detect AWS Root Account usage will help you monitor AWS (root) account activities. You can identify and act on activities which can lead to unauthorised access or other security breaches.

# Delete your root account access keys.

Access keys are long-term credentials for an IAM user or the AWS account root user. You can use access keys to sign programmatic requests to the AWS CLI or AWS API (directly or using the AWS SDK).

# Never share your root user password or access keys with anyone

Always ensure that your root account remain to yourself.

# Monitor and review root user activity

Whenever the root user password or its storage location are accessed, the event should be logged and monitored to verify that your account root user is following best practices. When the root user credentials are used, Amazon CloudWatch Application Insights and AWS CloudTrail record the activity in the log and trail.

# Don't create access keys for the root user

Don’t use highly privileged credentials for programmatic access. Credentials that are stored within applications are an easily exploited attack surface.

# Use a strong root user password to help protect access

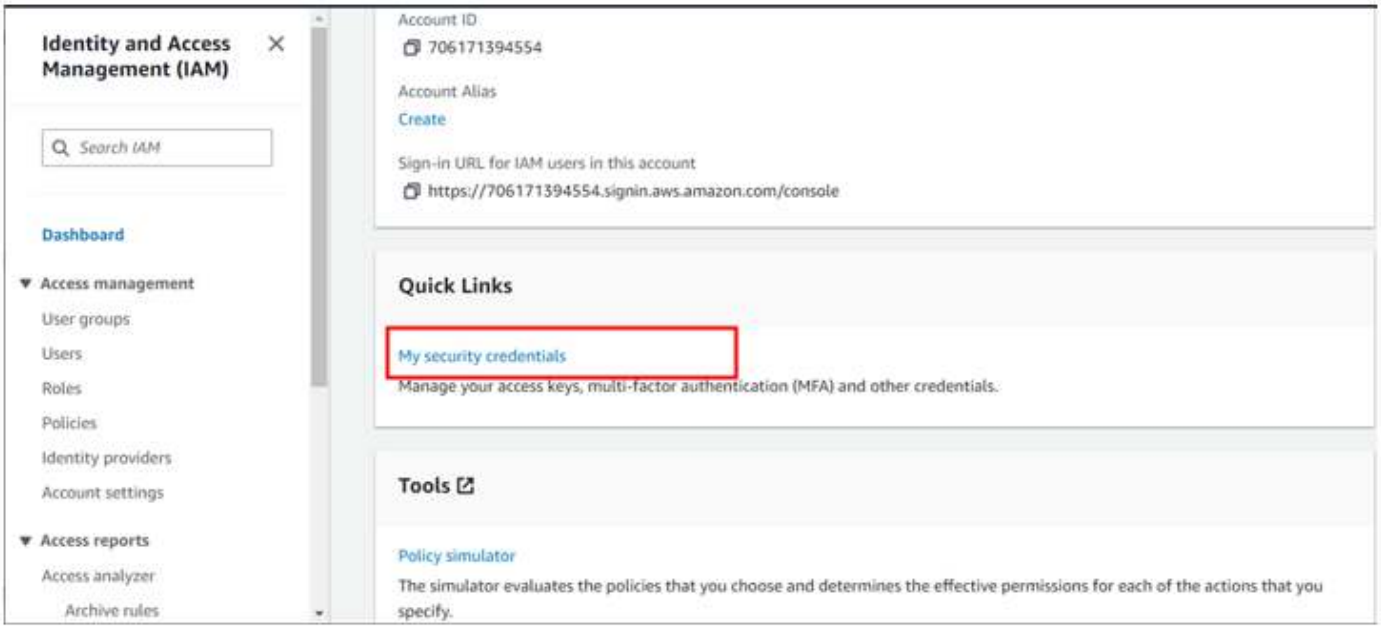
Strong passwords are more difficult to guess or break using brute-force attacks. Have root user passwords follow password complexity guidelines.

# Configuring Security Best Practices for the Root User:

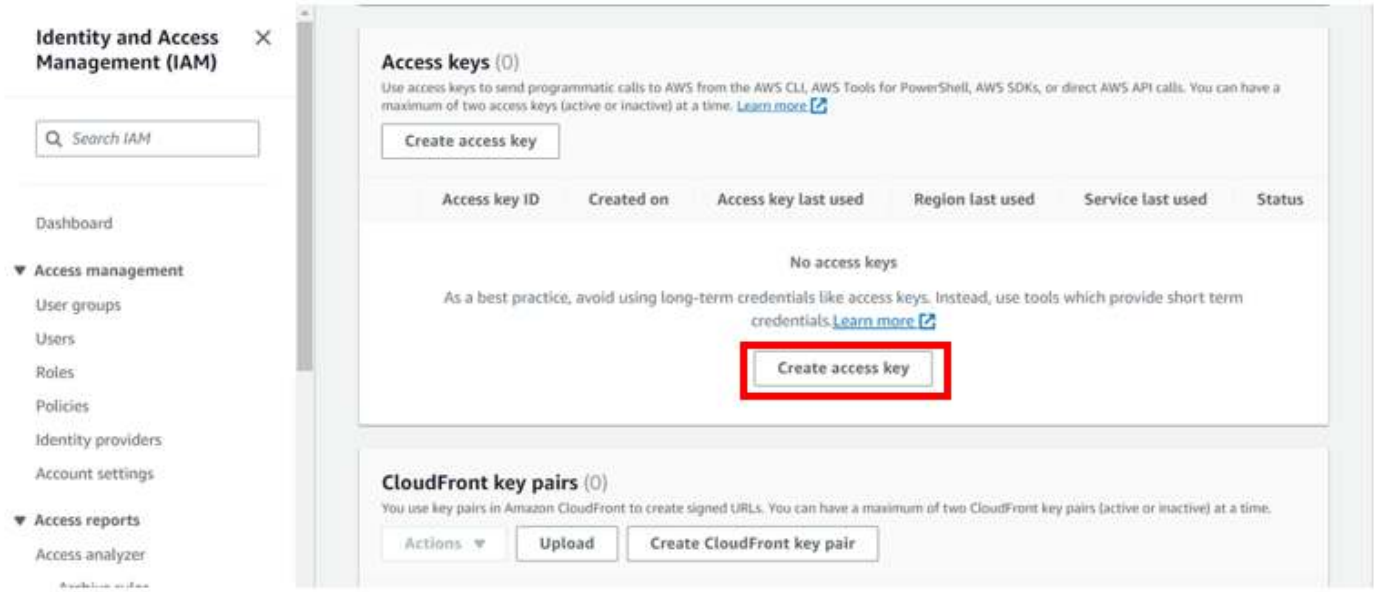
Sign in to the AWS Management Console and open the IAM console at https://console.aws.amazon.com/iam/

# Deleting Root Access Keys

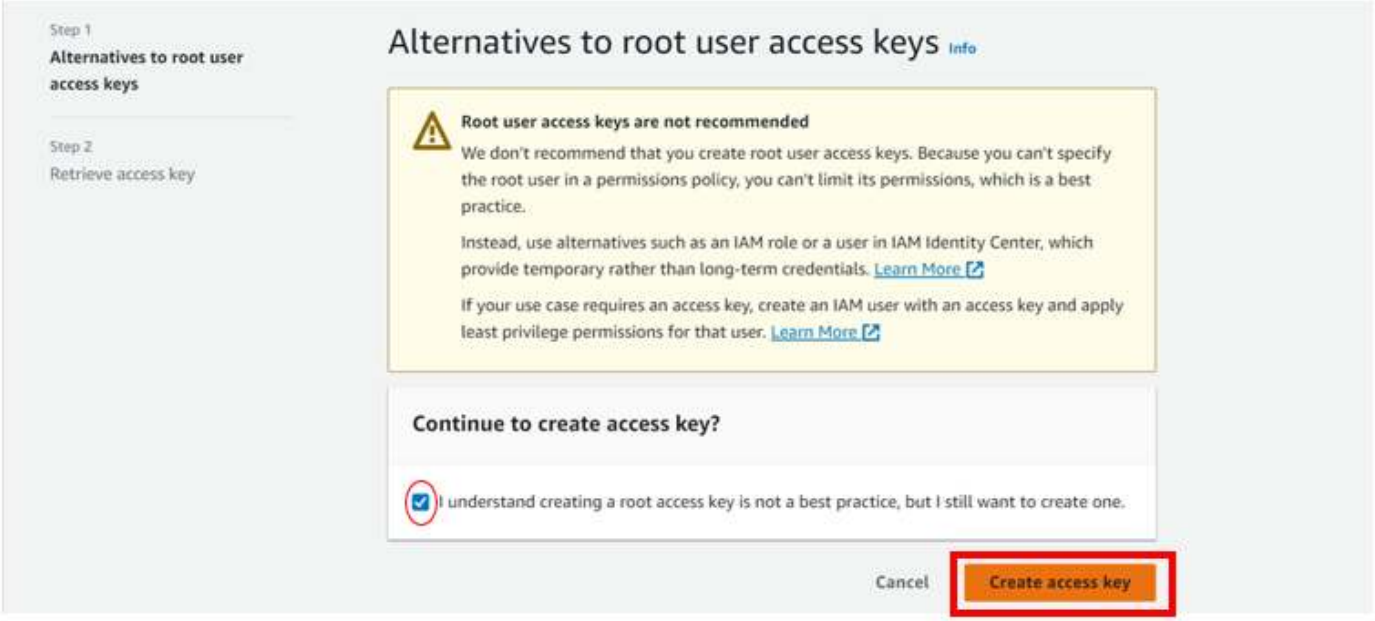
log in as root, click in my security credentials as shown below,




For my case I don't have any access keys for my root account since it's not a best practice, but we will create one for this demo. Under security credentials scroll down to access keys and click create access keys.

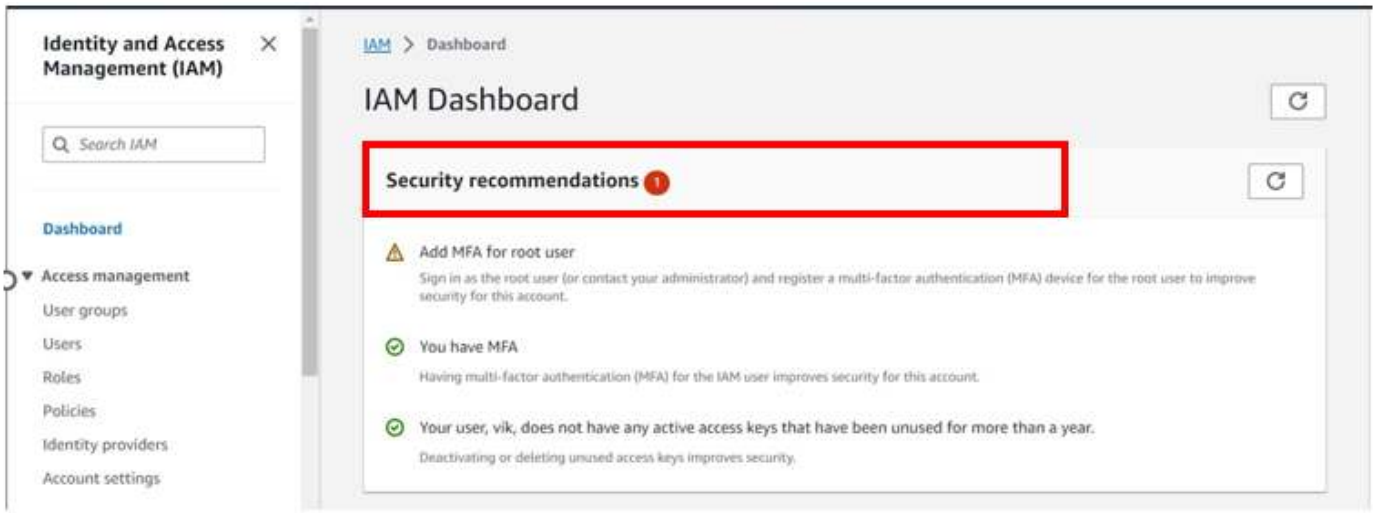



As you can already see the red flag, Root user access keys are not recommended. Check the box down on "I understand creating is not recommended but I still want to create one" then click create access key.



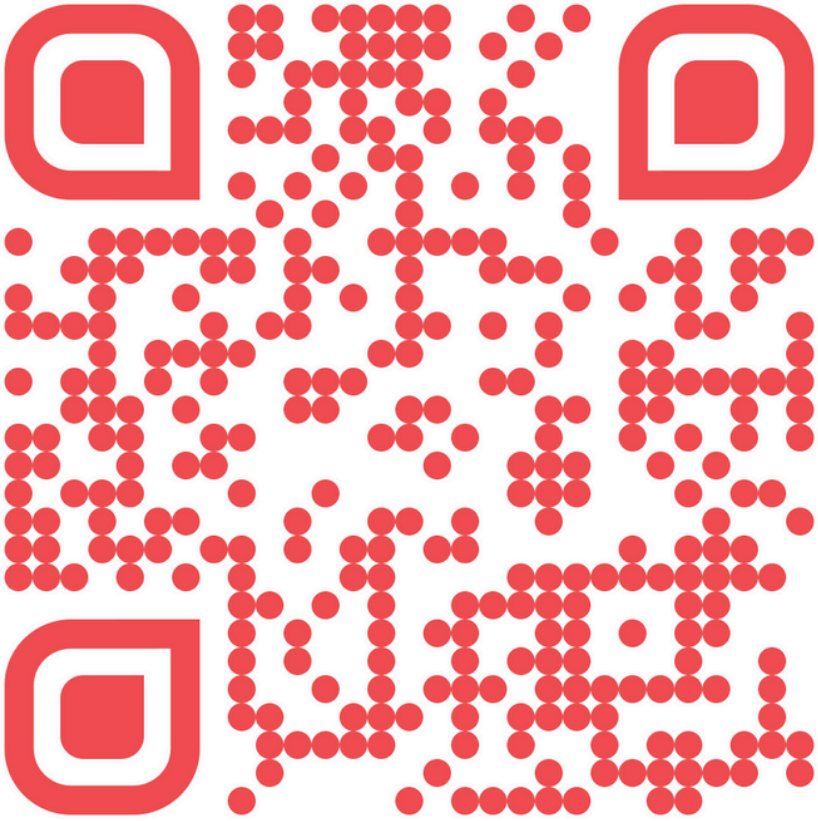

There we go, access keys created and you can download the csv file


Coming back to our I am dashboard, already we can see there is a red flag. we are advised to deactivate or delete access keys for root user. We will now proceed and see how we can delete access keys for root user account.




Select the radio button under access key ID, then select action drop-down button then click deactivate. Remember you must first deactivate an access key before deleting it. When prompted proceed and click deactivate.

accendnetworks



**www.accendnetworks.com**