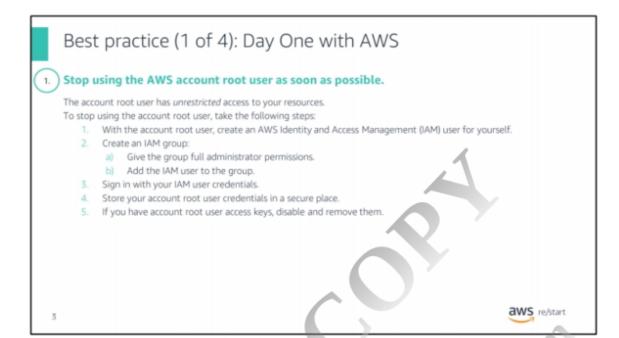




What are the best practices for setting up a new AWS account? This lesson collates security practices, and provides insight into Day One best practices that every account should follow.

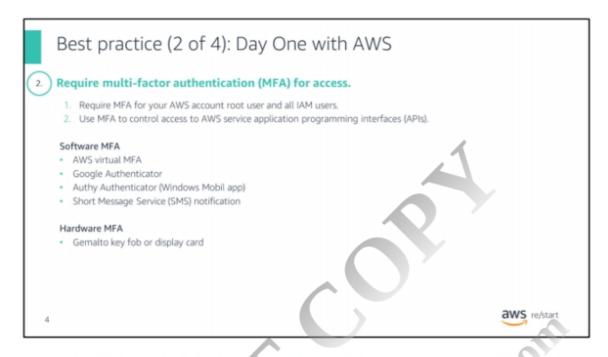


AWS recommends that if you have access keys for your account root user, remove them. Before you remove the access keys, confirm that they are not being used anywhere in your applications.

To stop using the account root user, follow these steps:

- With the account root user, create an AWS Identity and Access Management (IAM) user for yourself.
- Create an IAM group, give it full administrator permissions, and add the IAM user to the group.
- Sign in with your IAM user credentials.
- 4. Store your account root user credentials in a secure place.

For more information about setting up your first IAM user and administrators group, see <u>Creating your first IAM admin user and group</u> in the *AWS Identity and Access Management User Guide*.



For more information about Gemalto, see <u>Multi-Factor Authentication (MFA)</u>" on the Thales website.



CloudTrail logs all application programming interface (API) requests to resources in your account.

Here is how to enable AWS CloudTrail:

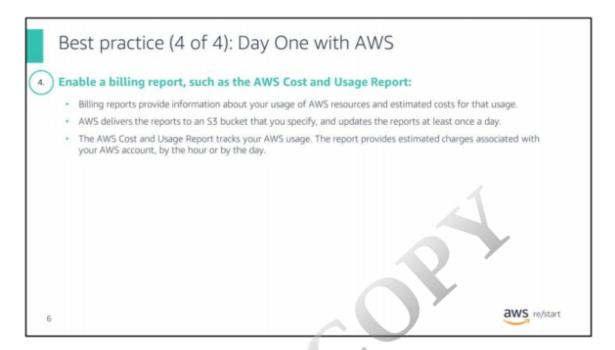
- Create a trail:
 - a) Give the trail a name.
 - b) Apply the trail to all Regions.
 - c) Enter a name for the new Amazon Simple Storage Service (Amazon S3) bucket where logs will be stored.
- Ensure that the Amazon S3 bucket you use for CloudTrail has its access restricted to only those who require access, such as administrators.

CloudTrail is now enabled by default for all users. It provides visibility into the past 7 days of account activity. It removes the need to configure a trail in the service to get started. When CloudTrail is enabled, you can view, search, and download the account activity through the CloudTrail Event History.

For more information, see "Creating a trail" in the AWS CloudTrail User Guide (http://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-create-

a-trail-using-the-console-first-time.html).



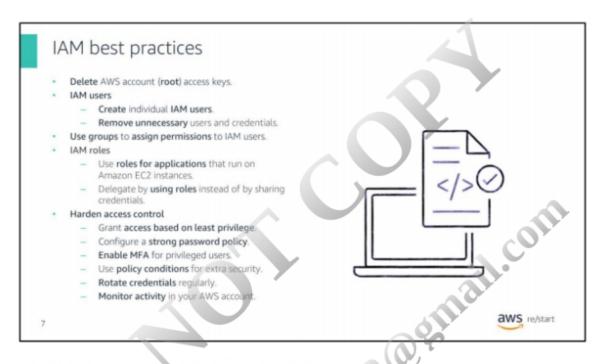


Billing reports provide information about your usage of AWS resources and estimated costs for that usage. AWS delivers the reports to an S3 bucket that you specify and updates the reports at least once a day.

For example, the AWS Cost and Usage Report tracks your AWS usage. The report provides estimated charges associated with your AWS account, by the hour or by the day.

For more information, refer to What are AWS Cost and Usage Reports? in the Cost and Usage Report User Guide.

Printed by: bufetekaye.22@gmail.com. Printing is for personal, private use only. No part of this book may be reproduced or transmitted without publisher's prior permission. Violators will be prosecuted.



In summary, here are some best practices to follow with IAM.

For more information, see Security best practices in IAM in the AWS Identity and Access Management User Guide.



Key takeaways from this lesson include:

- The AWS account root user is the email address that you use to set up the AWS account. It has full administrator access.
 - Do not give the root user credentials to anyone.
 - Delete the AWS account root user access keys after login.
- Create an IAM user for each individual in the organization.
- · Always secure your AWS account with MFA.
- Enable AWS CloudTrail to log and Billing Reports to collect usage and cost information in your AWS account.