



Security Best Practices for Creating an AWS Account


© 2020 Amazon Web Services, Inc. or its affiliates. All rights reserved.

DO NOT COPY
bufetekaye.22@gmail.com

What you will learn

At the core of the lesson

You will learn how to describe best practices to use when you create an AWS account.



2



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.

Best practice (1 of 4): Day One with AWS

1. Stop using the AWS account root user as soon as possible.

The account root user has *unrestricted* access to your resources.

To stop using the account root user, take the following steps:

1. With the account root user, create an AWS Identity and Access Management (IAM) user for yourself.
2. Create an IAM group:
 - a) Give the group full administrator permissions.
 - b) Add the IAM user to the group.
3. Sign in with your IAM user credentials.
4. Store your account root user credentials in a secure place.
5. If you have account root user access keys, disable and remove them.

3

aws re/start

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:

1. With the account root user, create an AWS Identity and Access Management (IAM) user for yourself.
2. Create an IAM group, give it full administrator permissions, and add the IAM user to the group.
3. 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 [Creating your first IAM admin user and group](#) in the *AWS Identity and Access Management User Guide*.

Best practice (2 of 4): Day One with AWS

2. Require multi-factor authentication (MFA) for access.

1. Require MFA for your AWS account root user and all IAM users.
2. Use MFA to control access to AWS service application programming interfaces (APIs).

Software MFA

- AWS virtual MFA
- Google Authenticator
- Authy Authenticator (Windows Mobil app)
- Short Message Service (SMS) notification

Hardware MFA

- Gemalto key fob or display card

4

aws re/start

For more information about Gemalto, see [Multi-Factor Authentication \(MFA\)](#) on the Thales website.

Best practice (3 of 4): Day One with AWS

3. Enable AWS CloudTrail.

AWS CloudTrail logs all API requests to resources in your account:

1. On the CloudTrail console, 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 the logs will be stored.
2. Ensure that the S3 bucket that you use for CloudTrail has its access restricted to only those who require access, such as administrators.

5

aws re/start

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

Here is how to enable AWS CloudTrail:

1. 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.
2. 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](#)).

DO NOT COPY
bufetekaye.22@gmail.com

Best practice (4 of 4): Day One with AWS

4. Enable a billing report, such as the AWS Cost and Usage Report:

- 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.
- 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.

6

aws re/start


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*.

IAM best practices

- Delete AWS account (root) access keys.
- IAM users
 - Create individual IAM users.
 - Remove unnecessary users and credentials.
- Use groups to assign permissions to IAM users.
- IAM roles
 - Use roles for applications that run on Amazon EC2 instances.
 - Delegate by using roles instead of by sharing credentials.
- Harden access control
 - Grant access based on least privilege.
 - Configure a strong password policy.
 - Enable MFA for privileged users.
 - Use policy conditions for extra security.
 - Rotate credentials regularly.
 - Monitor activity in your AWS account.



7

aws re/start

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



© 2020 Amazon Web Services, Inc. or its affiliates. All rights reserved.

8

- 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.

aws re/start

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.