

AWS Essentials Assignment -1

Creating IAM user and applying S3FullAccess policy to the user. After that login with the created IAM user and checking with S3, IAM and EC2 consoles in AWS.

➤ **Logged as root user in AWS**

The screenshot displays the AWS Management Console interface. At the top, there is a navigation bar with the AWS logo, a 'Services' dropdown, a search bar containing the text 'Search for services, features, marketplace produc' with an '[Alt+S]' shortcut, and user information including 'SUNEER_AWS', 'Ohio', and a 'Support' link. Below the navigation bar, the main heading 'AWS Management Console' is centered. The interface is divided into two main sections. The first section, 'AWS services', includes a 'Recently visited services' list with 'IAM' listed and an 'All services' link. The second section, 'Build a solution', is subtitled 'Get started with simple wizards and automated workflows.' and contains six solution cards. Each card has a title, a description of the service used, a time estimate, and an icon. The cards are: 'Launch a virtual machine' (With EC2, 2-3 minutes, icon of two server racks), 'Build a web app' (With Elastic Beanstalk, 6 minutes, icon of a cloud with a person), 'Build using virtual servers' (With Lightsail, 1-2 minutes, icon of a cloud with a person and a plus sign), 'Register a domain' (With Route 53, 3 minutes, icon of a cloud with a person), 'Connect an IoT device' (With AWS IoT, 5 minutes, icon of a person with a device), and 'Start migrating to AWS' (With AWS MGN, 1-2 minutes, icon of a cloud with a person and a plus sign).

AWS services

▼ Recently visited services

IAM

► All services

Build a solution

Get started with simple wizards and automated workflows.

Launch a virtual machine
With EC2
2-3 minutes

Build a web app
With Elastic Beanstalk
6 minutes

Build using virtual servers
With Lightsail
1-2 minutes

Register a domain
With Route 53
3 minutes

Connect an IoT device
With AWS IoT
5 minutes

Start migrating to AWS
With AWS MGN
1-2 minutes



➤ IAM console before user creation

The screenshot shows the AWS IAM console interface. The top navigation bar includes the AWS logo, 'Services' dropdown, a search bar, and account information 'SUNEER_AWS'. The left sidebar is titled 'Identity and Access Management (IAM)' and lists various options: Dashboard, Access management (expanded), Users (highlighted), Roles, Policies, Identity providers, Account settings, Access reports, Access analyzer, Archive rules, Analyzers, Settings, and Credential report. The main content area is titled 'IAM > Users'. It shows 'Users (0)' with an 'Info' link and buttons for 'Refresh', 'Delete', and 'Add users'. A description states: 'An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.' Below this is a search bar 'Find users by username or access key'. A table header is visible with columns: 'User name', 'Groups', and 'Last activity'. The table is currently empty, displaying 'No resources to'.

➤ Adding user in IAM

The screenshot shows the 'Add user' wizard in the AWS IAM console. The top navigation bar is identical to the previous screenshot. The wizard has four steps, with the first step 'Add user' being the active one. The section 'Set user details' contains a 'User name*' field with the value 'newuser' and a '+ Add another user' link. The section 'Select AWS access type' contains two checked options: 'Programmatic access' (which enables an access key ID and secret access key) and 'AWS Management Console access' (which enables a password). Under 'Console password*', there are two radio buttons: 'Autogenerated password' and 'Custom password' (which is selected). A password field shows masked characters '.....' and a 'Show password' checkbox is present. At the bottom, the 'Require password reset' checkbox is checked, with a note that users will automatically get the 'IAMUserChangePassword' policy.


➤ Adding S3 Full Access policy to the user


 Services ▾ [Alt+S]  SUNEER_AWS ▾ Global ▾ Support ▾


Add user

12345

▾ Set permissions

 Add user to group








 Copy permissions from existing user

 Attach existing policies directly



Create policy

Filter policies ▾

Showing 7 results

	Policy name ▾	Type	Used as
<input type="checkbox"/>	 AmazonDMSRedshiftS3Role	AWS managed	None
<input checked="" type="checkbox"/>	 AmazonS3FullAccess	AWS managed	None
<input type="checkbox"/>	 AmazonS3ObjectLambdaExecutionRolePolicy	AWS managed	None
<input type="checkbox"/>	 AmazonS3OutpostsFullAccess	AWS managed	None
<input type="checkbox"/>	 AmazonS3OutpostsReadOnlyAccess	AWS managed	None
<input type="checkbox"/>	 AmazonS3ReadOnlyAccess	AWS managed	None
<input type="checkbox"/>	 QuickSightAccessForS3StorageManagementAnalyticsReadOnly	AWS managed	None

➤ Reviewing the user creation

 Services ▾ [Alt+S]  SUNEER_AWS ▾ Global ▾ Support ▾

Add user

12345

Review

Review your choices. After you create the user, you can view and download the autogenerated password and access key.

User details

User name	newuser
AWS access type	Programmatic access and AWS Management Console access
Console password type	Custom
Require password reset	Yes
Permissions boundary	Permissions boundary is not set

Permissions summary


The following policies will be attached to the user shown above.

Type	Name
Managed policy	AmazonS3FullAccess
Managed policy	IAMUserChangePassword

Tags

No tags were added.

➤ User successfully created

 Services ▾

[Alt+S]

SUNEER_AWS ▾

Global ▾

Support ▾

1

2

3

4

5


✓ Success

You successfully created the users shown below. You can view and download user security credentials. You can also email users instructions for signing in to the AWS Management Console. This is the last time these credentials will be available to download. However, you can create new credentials at any time.

Users with AWS Management Console access can sign-in at: <https://227160538599.signin.aws.amazon.com/console>

 Download .csv

➤ IAM user console after the newuser is created

 Services ▾

[Alt+S]

SUNEER_AWS ▾

Global ▾

Support ▾

Dashboard

▼ Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

▼ Access reports

Access analyzer

Archive rules

Analyzers

Settings

Credential report

Organization activity

Service control policies (SCPs)

Users > newuser

Summary Delete user ?

User ARN

arn:aws:iam::227160538599:user/newuser 

Path

/

Creation time

2021-09-13 00:49 UTC+0300

Permissions

Groups

Tags

Security credentials

Access Advisor

▼ Permissions policies (2 policies applied)

Add permissions




+ Add inline policy

Policy name ▾	Policy type ▾	
Attached directly		
▶  AmazonS3FullAccess	AWS managed policy	✕
▶  IAMUserChangePassword	AWS managed policy	✕

▶ Permissions boundary (not set)

▼ Generate policy based on CloudTrail events

➤ Logged as IAM user in AWS

 Services ▾ [Alt+S]   newuser @ 2271-6053-8599 ▾ Ohio ▾ Support ▾

AWS Management Console

AWS services

▼ Recently visited services

① IAM


► All services

Build a solution

Get started with simple wizards and automated workflows.


Launch a virtual machine

With EC2
2-3 minutes




Build a web app

With Elastic Beanstalk
6 minutes






Build using virtual servers

With Lightsail
1-2 minutes



➤ Checking S3 console in the newuser

 Services ▾ [Alt+S]   newuser @ 2271-6053-8599 ▾ Global ▾ Support ▾

Amazon S3

Buckets

Access Points

Object Lambda Access Points

Multi-Region Access Points

Batch Operations

Access analyzer for S3

Block Public Access settings for this account

▼ **Storage Lens**

Dashboards

AWS Organizations settings

Feature spotlight 3

► AWS Marketplace for S3

Amazon S3





Account snapshot


Storage lens provides visibility into storage usage and activity trends. [Learn more](#)

[View Storage Lens dashboard](#)

Buckets (0) [Info](#)

Buckets are containers for data stored in S3. [Learn more](#)

  Copy ARN  Empty  Delete [Create bucket](#)

< 1 > 

Name ▲	AWS Region ▼	Access ▼	Creation date ▼
No buckets			
You don't have any buckets.			
Create bucket			

➤ Checking IAM console in the newuser

The screenshot shows the AWS IAM console dashboard for a user named 'newuser @ 2271-6053-8599'. The left sidebar contains the 'Identity and Access Management (IAM)' menu with options like Dashboard, Access management, Access reports, and various IAM resources. The main content area is titled 'IAM dashboard' and features a 'Security recommendations' section with three error messages indicating that the user is not authorized to perform certain operations (iam:GetAccountSummary, iam:ListMFADevices, and iam:ListAccessKeys). Below this, the 'IAM resources' section also shows an error message for the iam:ListAccessKeys operation. The top navigation bar includes the AWS logo, Services menu, a search bar, and user information.

Identity and Access Management (IAM)

- Dashboard
- Access management
 - User groups
 - Users
 - Roles
 - Policies
 - Identity providers
 - Account settings
- Access reports
 - Access analyzer
 - Archive rules
 - Analyzers
 - Settings
 - Credential report
 - Organization activity
 - Service control policies (SCPs)

IAM dashboard

Security recommendations

- You do not have the permission required to perform this operation your administrator to add permissions.
User: arn:aws:iam::227160538599:user/newuser is not authorized to perform iam:GetAccountSummary on resource: *
- You do not have the permission required to perform this operation your administrator to add permissions.
User: arn:aws:iam::227160538599:user/newuser is not authorized to perform iam:ListMFADevices on resource: user newuser
- You do not have the permission required to perform this operation your administrator to add permissions.
User: arn:aws:iam::227160538599:user/newuser is not authorized to perform iam:ListAccessKeys on resource: user nullnewuser

IAM resources

- You do not have the permission required to perform this operation your administrator to add permissions.
User: arn:aws:iam::227160538599:user/newuser is not authorized to perform iam:ListAccessKeys on resource: user nullnewuser

➤ Checking EC2 console in the newuser

The screenshot shows the AWS EC2 console dashboard for a user named 'newuser @ 2271-6053-8599'. The left sidebar contains the 'New EC2 Experience' menu with options like EC2 Dashboard, Events, Tags, Limits, Instances, Images, and Elastic Block Store. The main content area is titled 'Resources' and displays a list of Amazon EC2 resources in the US East (Ohio) Region. Each resource is listed with a red 'API Error' icon, indicating that the user is not authorized to perform certain operations on these resources. The top navigation bar includes the AWS logo, Services menu, a search bar, and user information.

New EC2 Experience

- EC2 Dashboard
- Events
- Tags
- Limits
- Instances
 - Instances **New**
 - Instance Types
 - Launch Templates
 - Spot Requests
 - Savings Plans
 - Reserved Instances **New**
 - Dedicated Hosts
 - Capacity Reservations
- Images
 - AMIs
- Elastic Block Store
 - Volumes
 - Snapshots

Resources

You are using the following Amazon EC2 resources in the US East (Ohio) Region:

Instances (running)	API Error
Dedicated Hosts	API Error
Elastic IPs	API Error
Instances	API Error
Key pairs	API Error
Load balancers	API Error
Placement groups	API Error
Security groups	API Error
Snapshots	API Error
Volumes	API Error