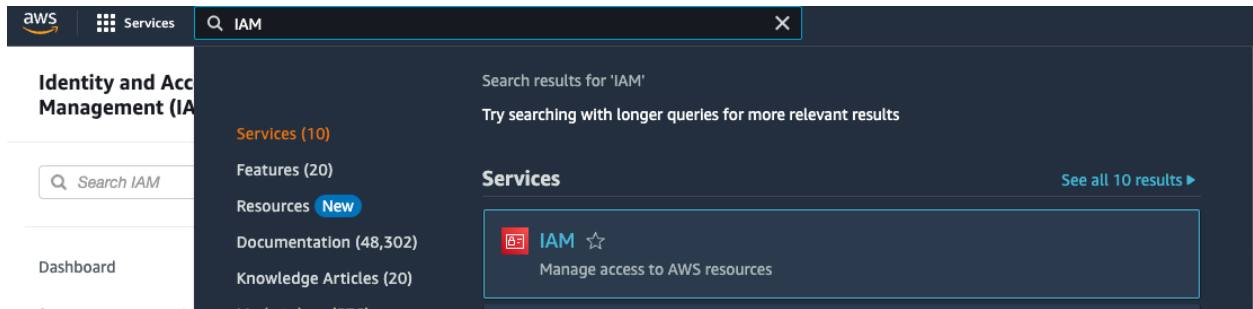
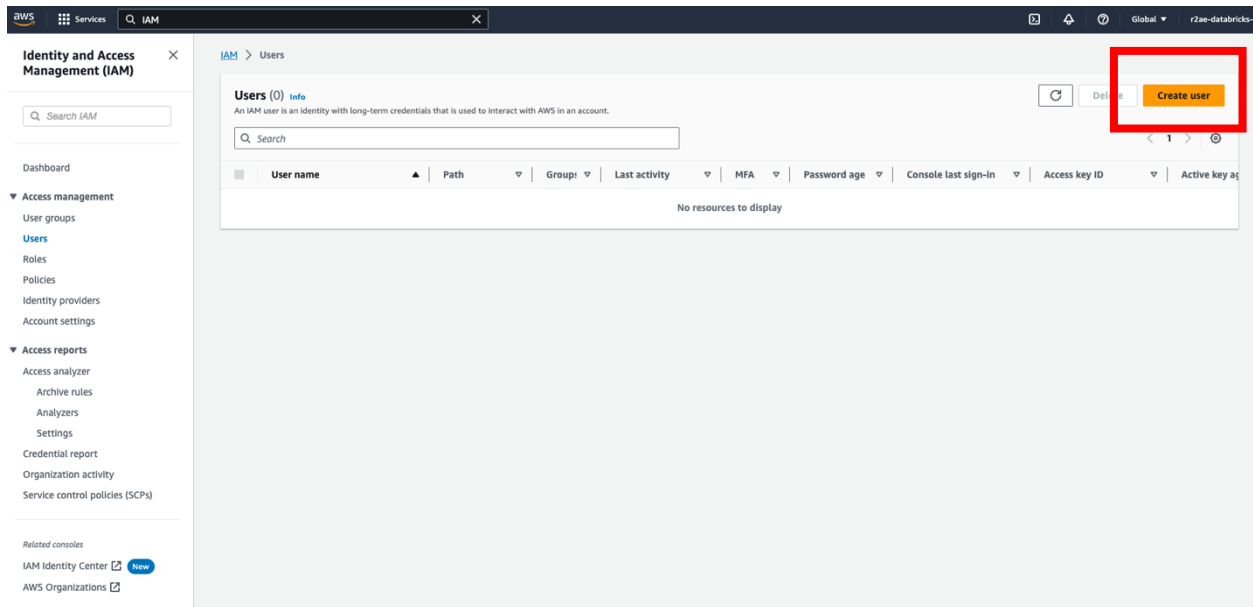


## Guideline : Configuring IAM for S3AllAccess Permissions on AWS IAM (By Ad Shane)

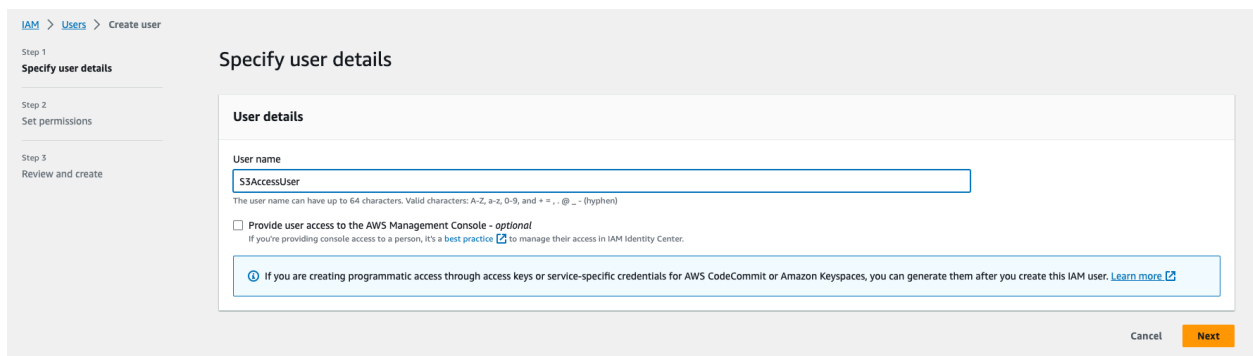
Step 1 : เข้าไปที่หน้า AWS Console แล้ว Search าคำว่า IAM



Step 2 : กดปุ่ม Create user ด้านบนขวาของ Console



Step 3 : ตั้งชื่อ User ตามที่ Configure ตามภาพ S3AccessUser แล้วกด Next



Step 4 : กดเลือก Attach policies directly เพื่อที่จะเลือก Permission Policies = “AmazonS3FullAccess”  
กด Next เพื่อสำเร็จการสร้าง User

[IAM](#) > [Users](#) > Create user

Step 1  
[Specify user details](#)

Step 2  
**Set permissions**

Step 3  
Review and create

### Set permissions

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. [Learn more](#)

**Permissions options**

☐ Add user to group  
Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.

☐ Copy permissions  
Copy all group memberships, attached managed policies, and inline policies from an existing user.

☒ Attach policies directly  
Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

**Permissions policies (1/1121)** [Create policy](#)

Choose one or more policies to attach to your new user.

Filter by Type  
All types 11 matches

<input type="checkbox"/>	Policy name	Type	Attached entities
<input type="checkbox"/>	<a href="#">AmazonDMSRedshiftS3Role</a>	AWS managed	0
<input checked="" type="checkbox"/>	<a href="#">AmazonS3FullAccess</a>	AWS managed	0
<input type="checkbox"/>	<a href="#">AmazonS3ObjectLambdaExecutionRolePolicy</a>	AWS managed	0
<input type="checkbox"/>	<a href="#">AmazonS3OutpostsFullAccess</a>	AWS managed	0
<input type="checkbox"/>	<a href="#">AmazonS3OutpostsReadOnlyAccess</a>	AWS managed	0
<input type="checkbox"/>	<a href="#">AmazonS3ReadOnlyAccess</a>	AWS managed	0
<input type="checkbox"/>	<a href="#">AWSBackupServiceRolePolicyForS3Backup</a>	AWS managed	0
<input type="checkbox"/>	<a href="#">AWSBackupServiceRolePolicyForS3Restore</a>	AWS managed	0
<input type="checkbox"/>	<a href="#">IVSRecordToS3</a>	AWS managed	0
<input type="checkbox"/>	<a href="#">QuickSightAccessForS3StorageManagementAnalyticsR...</a>	AWS managed	0
<input type="checkbox"/>	<a href="#">S3StorageLensServiceRolePolicy</a>	AWS managed	0

► Set permissions boundary - optional

Cancel Previous **Next**

Step 5 : เมื่อ Create User เสร็จแล้ว จะได้ IAM user ดังรูปข้างล่าง

**Identity and Access Management (IAM)** ×

🔍 Search IAM

Dashboard

▼ Access management

- User groups
- Users**
- Roles
- Policies
- Identity providers
- Account settings

▼ Access reports

- Access analyzer
- Archive rules
- Analysers
- Settings
- Credential report
- Organization activity
- Service control policies (SCPs)

Related consoles

- [IAM Identity Center](#) **New**
- [AWS Organizations](#)

**User created successfully** ×

You can view and download the user's password and email instructions for signing in to the AWS Management Console.

[View user](#)

[IAM](#) > [Users](#)

**Users (1)** [info](#) [Refresh](#) [Delete](#) [Create user](#)

Search

<input type="checkbox"/>	User name	Path	Group	Last activity	MFA	Password age	Console last sign-in	Access key ID	Active key age
<input type="checkbox"/>	<a href="#">S3AccessUser</a>	/	0	C	-	-	-	-	-

Step 6 : Click ที่ User ที่เพิ่งสร้างขึ้นมานี้ใหม่ จากนั้น กด create access key มุมขวบน

[IAM](#) > [Users](#) > [S3AccessUser](#)

## S3AccessUser [Info](#)

[Delete](#)

Summary		
ARN arn:aws:iam::773735718714:user/S3AccessUser	Console access Disabled	Access key 1 <a href="#">Create access key</a>
Created August 22, 2023, 18:27 (UTC+07:00)	Last console sign-in -	

[Permissions](#) | [Groups](#) | [Tags](#) | [Security credentials](#) | [Access Advisor](#)

Step 7 : เลือก Application running outside AWS

[IAM](#) > [Users](#) > [S3AccessUser](#) > Create access key

Step 1  
**Access key best practices & alternatives**

Step 2 - optional  
Set description tag

Step 3  
Retrieve access keys

### Access key best practices & alternatives [Info](#)

Avoid using long-term credentials like access keys to improve your security. Consider the following use cases and alternatives.

**Use case**

☐ **Command Line Interface (CLI)**  
You plan to use this access key to enable the AWS CLI to access your AWS account.

☐ **Local code**  
You plan to use this access key to enable application code in a local development environment to access your AWS account.

☐ **Application running on an AWS compute service**  
You plan to use this access key to enable application code running on an AWS compute service like Amazon EC2, Amazon ECS, or AWS Lambda to access your AWS account.

☐ **Third-party service**  
You plan to use this access key to enable access for a third-party application or service that monitors or manages your AWS resources.

☒ **Application running outside AWS**  
You plan to use this access key to enable an application running on an on-premises host, or to use a local AWS client or third-party AWS plugin.

☐ **Other**  
Your use case is not listed here.

**It's okay to use an access key for this use case, but follow the best practices:**

- Never store your access key in plain text, in a code repository, or in code.
- Disable or delete access keys when no longer needed.
- Enable least-privilege permissions.
- Rotate access keys regularly.

For more details about managing access keys, see the [best practices for managing AWS access keys](#).

[Cancel](#) [Next](#)

## Step 8 : กด Create Access Key

IAM > Users > S3AccessUser > Create access key

Step 1  
[Access key best practices & alternatives](#)

Step 2 - optional  
**Set description tag**

Step 3  
Retrieve access keys

### Set description tag - *optional* [info](#)

The description for this access key will be attached to this user as a tag and shown alongside the access key.

Description tag value  
Describe the purpose of this access key and where it will be used. A good description will help you rotate this access key confidently later.

Maximum 256 characters. Allowed characters are letters, numbers, spaces representable in UTF-8, and: \_ . : / = + - @

Cancel Previous **Create access key**

## Step 9 : กด Access key และ Secret access key เอาไว้ในโน้ตข้างนอกเพื่อนำไปใช้ต่อ

### Retrieve access keys [info](#)

**Access key**  
If you lose or forget your secret access key, you cannot retrieve it. Instead, create a new access key and make the old key inactive.

Access key	Secret access key
AKIA3UR6D45PEACU4A	***** <a href="#">Show</a>

## Step 10 : Create เสร็จสิ้นจะได้ Set-up ดังรูปข้างล่าง

Identity and Access Management (IAM)

Q Search IAM

Dashboard

Access management

User groups

**Users**

Roles

Policies

Identity providers

Account settings

Access reports

Access analyzer

Archive rules

Analizers

Settings

Credential report

Organization activity

Service control policies (SCPs)

Related consoles

IAM Identity Center

AWS Organizations

IAM > Users > S3AccessUser

S3AccessUser [info](#) [Delete](#)

### Summary

ARN arn:aws:iam::773735718714:user/S3AccessUser	Console access Disabled	Access key 1 AKIA3UR6D45PEACU4A - Active Never used. Created today.
Created August 22, 2023, 18:27 (UTC+07:00)	Last console sign-in -	Access key 2 <a href="#">Create access key</a>

Permissions Groups Tags **Security credentials** Access Advisor

### Console sign-in

[Enable console access](#)

Console sign-in link https://773735718714.signin.aws.amazon.com/console	Console password Not enabled
--	---------------------------------

### Multi-factor authentication (MFA) (0)

Use MFA to increase the security of your AWS environment. Signing in with MFA requires an authentication code from an MFA device. Each user can have a maximum of 8 MFA devices assigned. [Learn more](#)

[Remove](#) [Resync](#) [Assign MFA device](#)

Device type	Identifier	Certifications	Created on
No MFA devices. Assign an MFA device to improve the security of your AWS environment			

[Assign MFA device](#)