Snapshot:

Using snapshot, we can copy the content of one server to anther (we install nginx in one server using snapshot we can copy the nginx in anther server without install it run in anther server)

You can back up the data on your Amazon EBS volumes to Amazon S3 by taking point-in-time snapshots. Snapshots are *incremental* backups, which means that only the blocks on the device that have changed after your most recent snapshot are saved. This minimizes the time required to create the snapshot and saves on storage costs by not duplicating data.

When we create snapshot AMI (amazon machine image) also create automatically

[]EC2 dashboard

[] select snapshot

[] create snapshot

[] instance

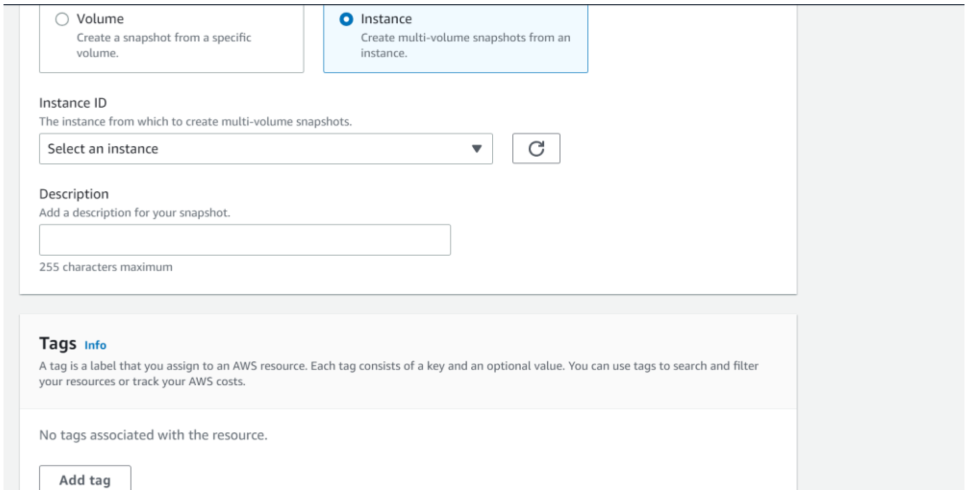
[] in instance ID select which instance we want

[] Description whatever

[] in volumes

[] copy tags

[] create snapshot



○ Volume
Create a snapshot from a specific volume.

● Instance
Create multi-volume snapshots from an instance.

Instance ID
The instance from which to create multi-volume snapshots.
Select an instance

Description
Add a description for your snapshot.

255 characters maximum

Tags Info
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

No tags associated with the resource.

[] in instance

[] select instance **(which sever want to backup**)

[] right click select image and templates

[] create image

[] image names give whatever

[] description

[] create image

[] **check the server we get backup of other server content**

Elastic Ip: if we create Elastic ip it helps us when the instance is stop and start it maintains same public ip

[] EC2

[] in **Network and security**

[] select Elastic ips

[] select allocate Elastic ip address

[] automatically selected (Amazon ‘s pool of ipv4)

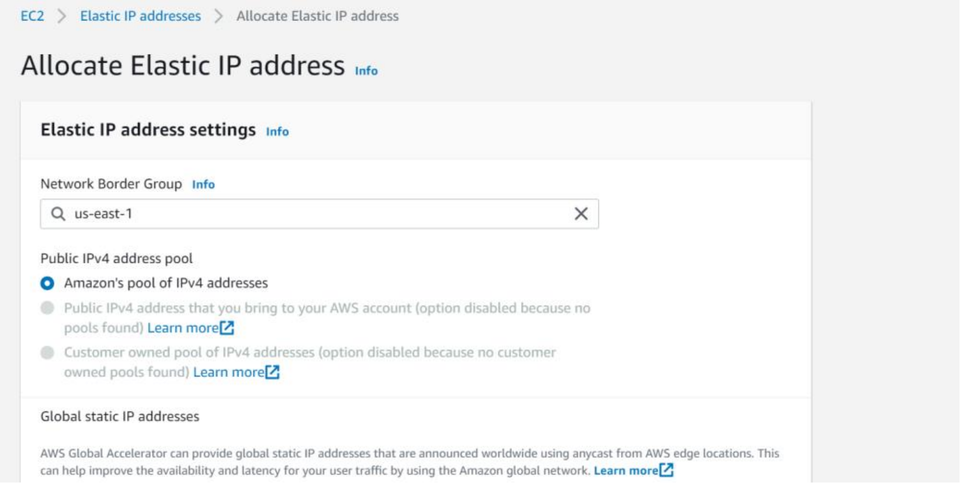
[] in tags – optional

[] add new tag

[] key (give whatever)

[]value (give whatever)

[] allocate



EC2 > Elastic IP addresses > Allocate Elastic IP address

Allocate Elastic IP address Info

Elastic IP address settings Info

Network Border Group Info

us-east-1

Public IPv4 address pool

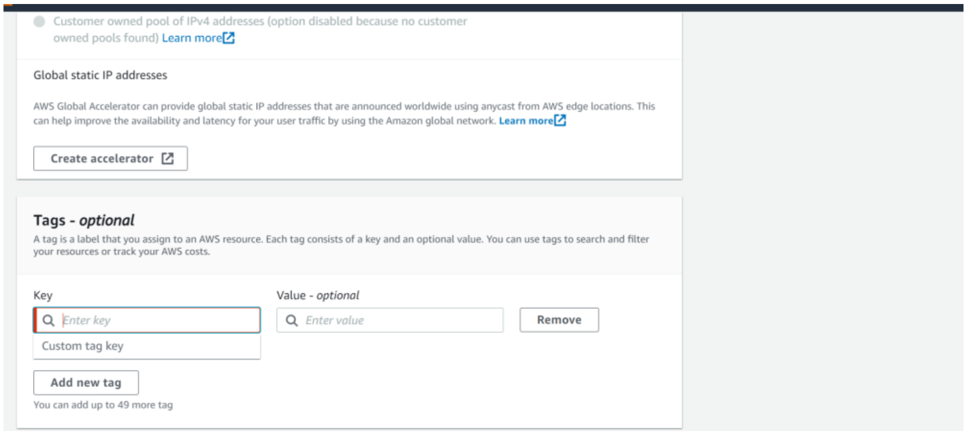
● Amazon's pool of IPv4 addresses

○ Public IPv4 address that you bring to your AWS account (option disabled because no pools found) Learn more

○ Customer owned pool of IPv4 addresses (option disabled because no customer owned pools found) Learn more

Global static IP addresses

AWS Global Accelerator can provide global static IP addresses that are announced worldwide using anycast from AWS edge locations. This can help improve the availability and latency for your user traffic by using the Amazon global network. Learn more



○ Customer owned pool of IPv4 addresses (option disabled because no customer owned pools found) Learn more

Global static IP addresses

AWS Global Accelerator can provide global static IP addresses that are announced worldwide using anycast from AWS edge locations. This can help improve the availability and latency for your user traffic by using the Amazon global network. Learn more

Tags - *optional*

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key: *Enter key*

Custom tag key

Value - *optional*: *Enter value*

You can add up to 49 more tag

[] **in Actions**

[] select Associate Elastic Ip address

[] in resource type

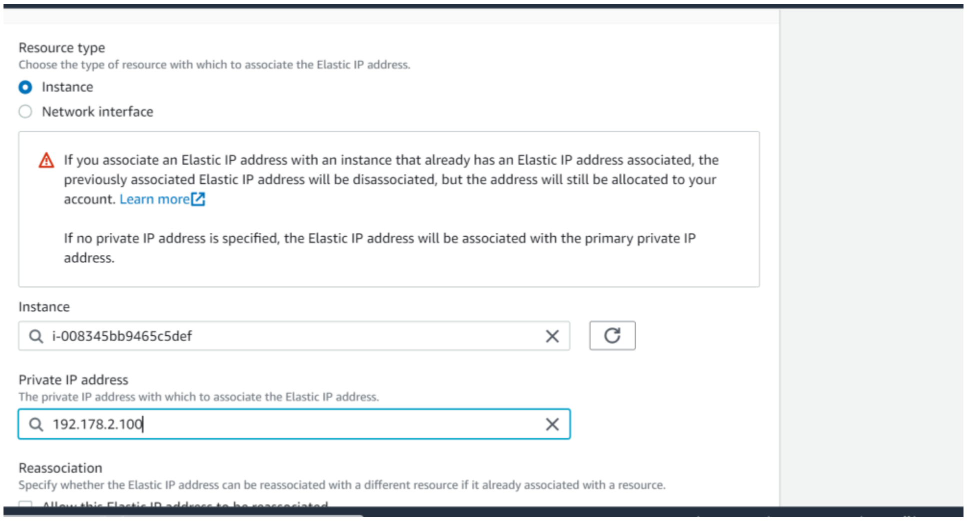
[] automatically selected (instance)

[] in instance (select which instance want)

[] in private Ip address (select which private Ip for selected above instance)

[] associate

(Check the instance it gives same public Ip to turn on and off the instance)



Resource type

Choose the type of resource with which to associate the Elastic IP address.

● Instance

○ Network interface

If you associate an Elastic IP address with an instance that already has an Elastic IP address associated, the previously associated Elastic IP address will be disassociated, but the address will still be allocated to your account. Learn more

If no private IP address is specified, the Elastic IP address will be associated with the primary private IP address.

Instance

i-008345bb9465c5def

Private IP address

The private IP address with which to associate the Elastic IP address.

192.178.2.100

Reassociation

Specify whether the Elastic IP address can be reassociated with a different resource if it already associated with a resource.

□ Allow this Elastic IP address to be reassociated

To release/delete the Elastic ip

[] Elastic IPs

[] Actions

[] click on IP (below of allocated IPv4)

[] Action

[] select disassociated

[] then Action release elastic IPs

Creating AMI using snapshot:

[]EC2 dashboard

[] select snapshot

[] create snapshot

[] instance

[] in instance ID select which instance we want

[] Description whatever

[] in volumes

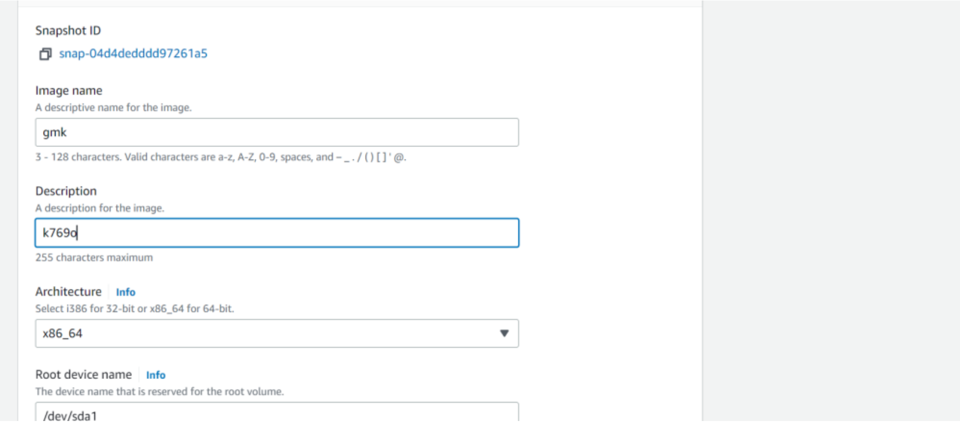
[] copy tags

[] create snapshot

[] in **actions**

[] select create image from snapshot

[] follow below

[] 

Snapshot ID

snap-04d4dedddd97261a5

Image name

A descriptive name for the image.

gmk

3 - 128 characters. Valid characters are a-z, A-Z, 0-9, spaces, and – _ . / ( ) [ ] ' @.

Description

A description for the image.

k769o

255 characters maximum

Architecture

Select i386 for 32-bit or x86_64 for 64-bit.

x86_64 ▼

Root device name

The device name that is reserved for the root volume.

/dev/sda1

[] check in AMIs image is created

[] to delete snapshot first we need to delete AMIs right click on image you get option to delete

[] in snapshot select action in that delete snapshot

Identity and Access Management (IAM):

IAM used to create user and police

[] IAM (search iam in search bar)

[] select users

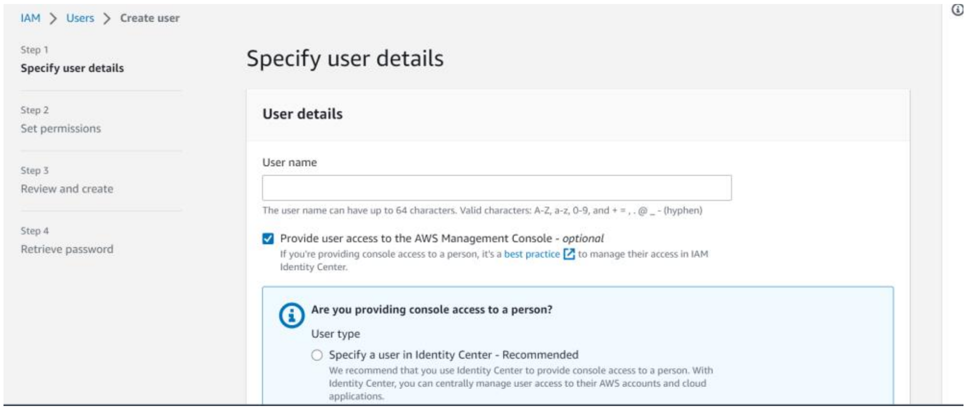
[] user name

[] select provide user access to the AWS management console

[] select I want to create an IAM user

[] select custom password (give whatever)

[] Next



Specify user details

User details

User name

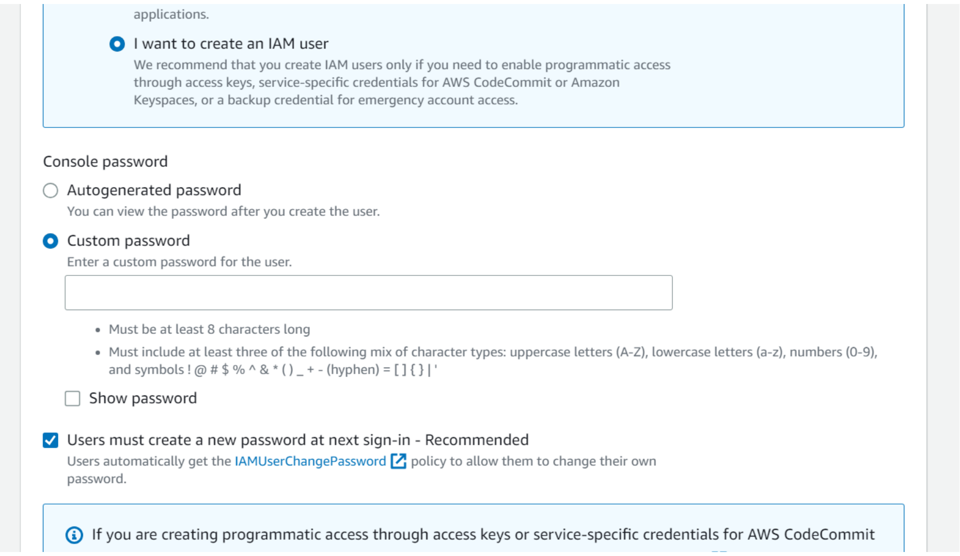
The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ _ - (hyphen)

☑ Provide user access to the AWS Management Console - *optional*
If you're providing console access to a person, it's a best practice to manage their access in IAM Identity Center.

Are you providing console access to a person?

User type

○ Specify a user in Identity Center - Recommended
We recommend that you use Identity Center to provide console access to a person. With Identity Center, you can centrally manage user access to their AWS accounts and cloud applications.



applications.

● I want to create an IAM user
We recommend that you create IAM users only if you need to enable programmatic access through access keys, service-specific credentials for AWS CodeCommit or Amazon Keyspaces, or a backup credential for emergency account access.

Console password

○ Autogenerated password
You can view the password after you create the user.

● Custom password
Enter a custom password for the user.

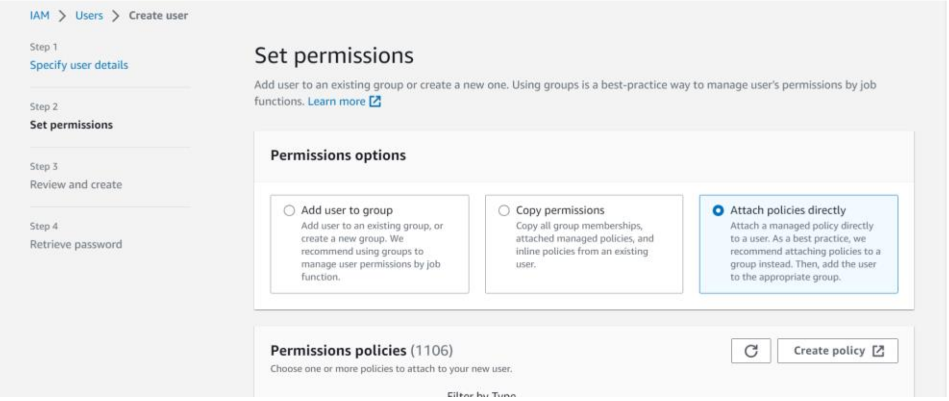
- Must be at least 8 characters long
- Must include at least three of the following mix of character types: uppercase letters (A-Z), lowercase letters (a-z), numbers (0-9), and symbols ! @ # $ % ^ & * ( ) _ + - (hyphen) = [ ] { } | '

□ Show password

☑ Users must create a new password at next sign-in - Recommended
Users automatically get the IAMUserChangePassword policy to allow them to change their own password.

ⓘ If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit

In permissions options:



IAM > Users > Create user

Step 1
Specify user details

Step 2
Set permissions

Step 3
Review and create

Step 4
Retrieve password

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 (1106)
Choose one or more policies to attach to your new user.

[] based on the requirement we select the options (**add user to group for if we have group then we use. 2) copy permissions this is used when we already gave permission to other group, we can copy same permission to other no need to create 3) attach police using this we can select which permission we want)**

[] next

[] create users

[] return to users

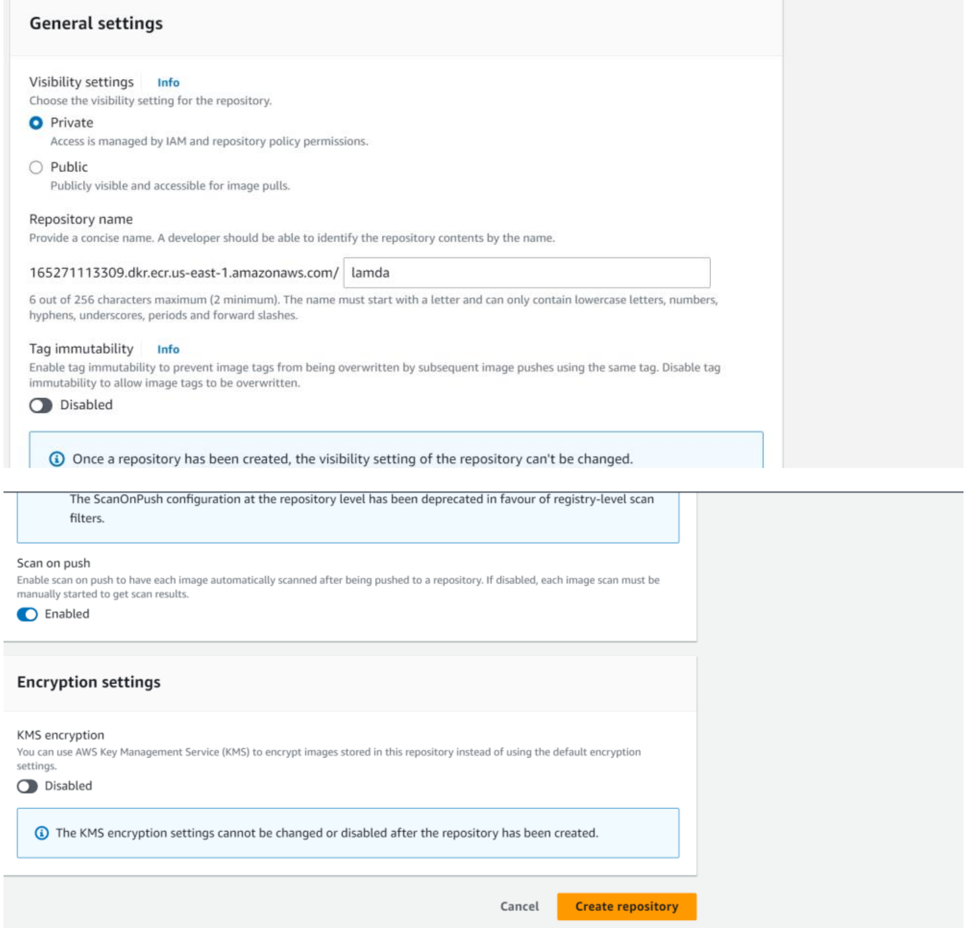
ECR (Amazon Elastic container registry): all AWS developers to **save configurations** and quickly move them into a production environment, thus reducing overall workloads.

[] in ECR

[] select create repository

[] repository name (whatever)

[] in scan on push enabled



General settings

Visibility settings Info

Choose the visibility setting for the repository.

● Private

Access is managed by IAM and repository policy permissions.

○ Public

Publicly visible and accessible for image pulls.

Repository name

Provide a concise name. A developer should be able to identify the repository contents by the name.

165271113309.dkr.ecr.us-east-1.amazonaws.com/ lamda

6 out of 256 characters maximum (2 minimum). The name must start with a letter and can only contain lowercase letters, numbers, hyphens, underscores, periods and forward slashes.

Tag immutability Info

Enable tag immutability to prevent image tags from being overwritten by subsequent image pushes using the same tag. Disable tag immutability to allow image tags to be overwritten.

Disabled

Once a repository has been created, the visibility setting of the repository can't be changed.

The ScanOnPush configuration at the repository level has been deprecated in favour of registry-level scan filters.

Scan on push

Enable scan on push to have each image automatically scanned after being pushed to a repository. If disabled, each image scan must be manually started to get scan results.

Enabled

Encryption settings

KMS encryption

You can use AWS Key Management Service (KMS) to encrypt images stored in this repository instead of using the default encryption settings.

Disabled

The KMS encryption settings cannot be changed or disabled after the repository has been created.

AWS_ACCESS_KEY_ID: & AWS_SECRET_ACESS_KEY:

[] in iam

[] select users

[] select which user want

[] select security credentials

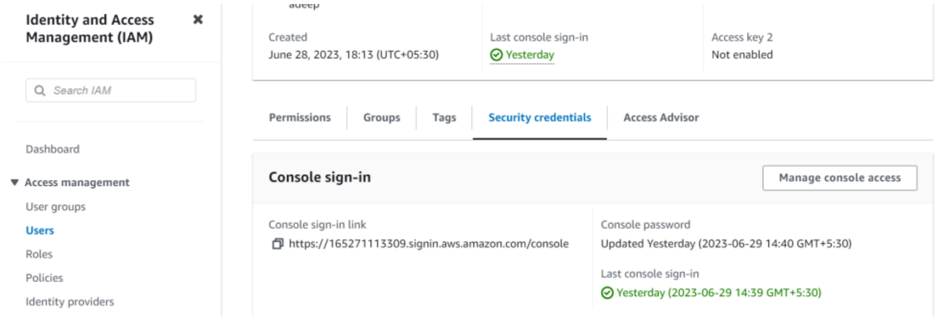
[] scroll down

[] select **create access key**

[] select **command line interface**

[] select confirm

[] next



Created
June 28, 2023, 18:13 (UTC+05:30)

Last console sign-in
Yesterday

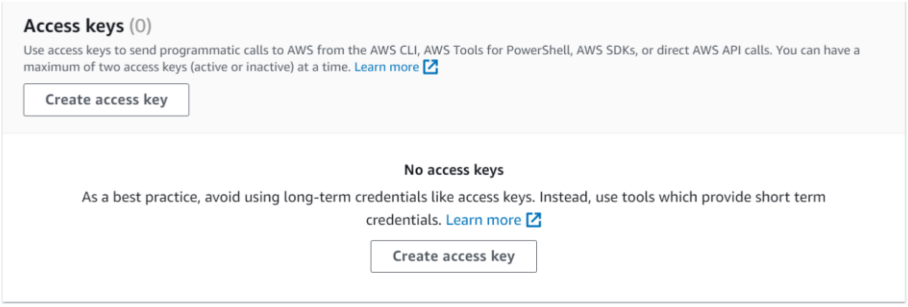
Access key 2
Not enabled

Console sign-in

Console sign-in link
https://165271113309.signin.aws.amazon.com/console

Console password
Updated Yesterday (2023-06-29 14:40 GMT+5:30)

Last console sign-in
Yesterday (2023-06-29 14:39 GMT+5:30)

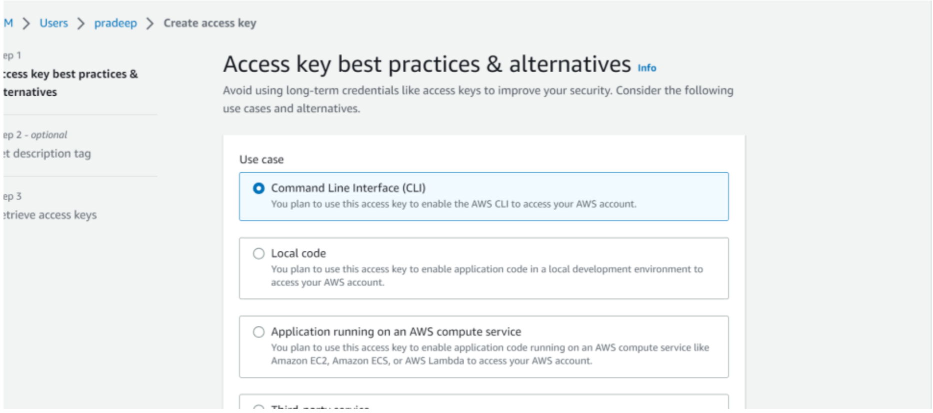


Access keys (0)

Use access keys to send programmatic calls to AWS from the AWS CLI, AWS Tools for PowerShell, AWS SDKs, or direct AWS API calls. You can have a maximum of two access keys (active or inactive) at a time. Learn more

No access keys

As a best practice, avoid using long-term credentials like access keys. Instead, use tools which provide short term credentials. Learn more



M > Users > pradeep > Create access key

ep 1
ccess key best practices & ternatives

ep 2 - *optional*
et description tag

ep 3
etrieve 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

[] type description

[] create access key

we need give ECR full access permission for docker push

[]Open the AWS Management Console and navigate(search) to the IAM service.

[] Locate and select the IAM user to which you want to attach the policy.

[] In the user scroll down to the **"Permissions"** section.

[] in **add permissions** Click on the **"Add inline policy"** button .

In the policy editor, choose the **"JSON"** tab to enter the policy code.

Replace the existing policy code with the JSON code provided earlier

```
{
"Version": "2012-10-17",
"Statement": [
{
"Sid": "Statement1",
"Effect": "Allow",
"Action": [],
```

"Resource": []

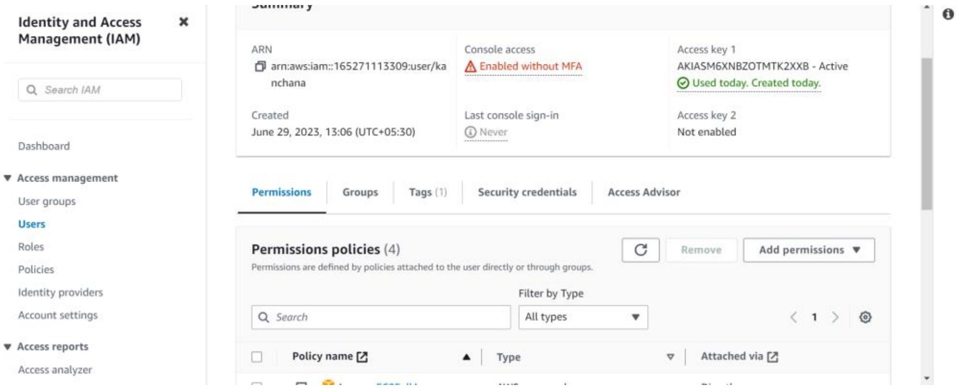
}

]

}

[] next

[] Provide a name for the policy in the **"Name"** field.
[] Click on **"Review policy"** to verify the policy details.
[]Finally, click on **"Create policy"** or **"Attach policy"** to attach the policy to the IAM user or role



ARN
arn:aws:iam::165271113309:user/kanchana

Console access
Enabled without MFA

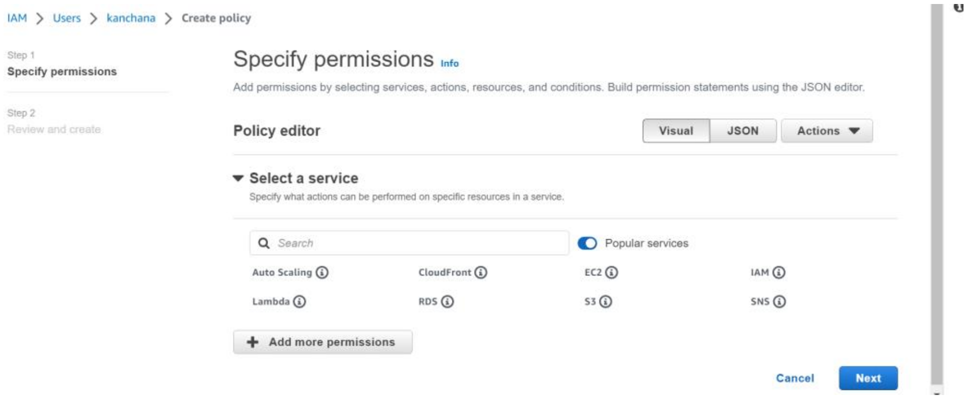
Access key 1
AKIASM6XNBZOTMTK2XXB - Active
Used today. Created today.

Created
June 29, 2023, 13:06 (UTC+05:30)

Last console sign-in
Never

Access key 2
Not enabled

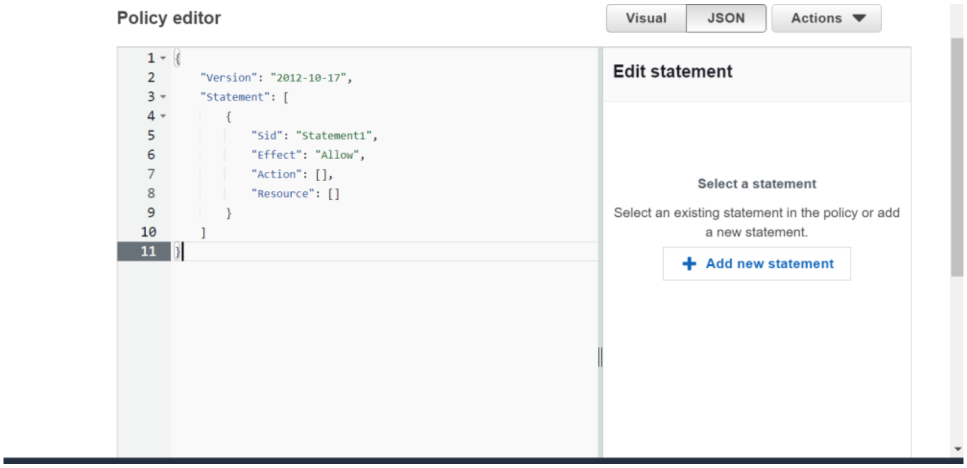
Permissions policies (4)
Permissions are defined by policies attached to the user directly or through groups.



Specify permissions Info
Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.

Policy editor

Select a service
Specify what actions can be performed on specific resources in a service.



```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Statement1",
            "Effect": "Allow",
            "Action": [],
            "Resource": []
        }
    ]
}
```

Edit statement
Select a statement
Select an existing statement in the policy or add a new statement.
+ Add new statement