

IAM

INSTALLED AWS CLI



```
Command Prompt
Microsoft Windows [Version 10.0.19045.3208]
(c) Microsoft Corporation. All rights reserved.

C:\Users\sv199>aws --version
aws-cli/2.13.3 Python/3.11.4 Windows/10 exe/AMD64 prompt/off

C:\Users\sv199>
```

TASK :

- How many policies can attach to one group ?

You can assign IAM users to up to 10 groups. You can also attach up to 10 managed policies to each group, for a maximum of 120 policies.

Creating user

User name

mahi

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.

☒ 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

Permission boundary:

if the user gave permission policies to user which is ec2 full access , s3 full access and vpc full access and then set the Permission boundary for the same user as ec2 full access, and vpc full access . Then, that user won't able to access on s3 Eventhough the user have that permission policy just because we didn't give the permission in set bpdundary permission.

The screenshot shows the AWS IAM console in the 'us-east-1' region, specifically the 'Create user' page. The 'Permissions summary' section displays a table of attached policies and boundaries. The table has three columns: Name, Type, and Used as. The policies listed are AmazonEC2FullAccess, AmazonS3FullAccess, AmazonVPCFullAccess, and IAMUserChangePassword, all of which are AWS managed permissions policies. The AmazonVPCFullAccess policy is also listed as a permissions boundary. Below the table, there is a 'Tags - optional' section with a note that tags are key-value pairs used for identifying and organizing resources. A button labeled 'Add new tag' is present, with a note indicating that up to 50 tags can be added. At the bottom of the page, there are buttons for 'Cancel', 'Previous', and 'Create user'. The bottom of the screenshot shows the Windows taskbar with various application icons and the system clock indicating 12:44 PM on 26-07-2023.

Name	Type	Used as
AmazonEC2FullAccess	AWS managed	Permissions policy
AmazonS3FullAccess	AWS managed	Permissions policy
AmazonVPCFullAccess	AWS managed	Permissions policy
AmazonVPCFullAccess	AWS managed	Permissions boundary
IAMUserChangePassword	AWS managed	Permissions policy

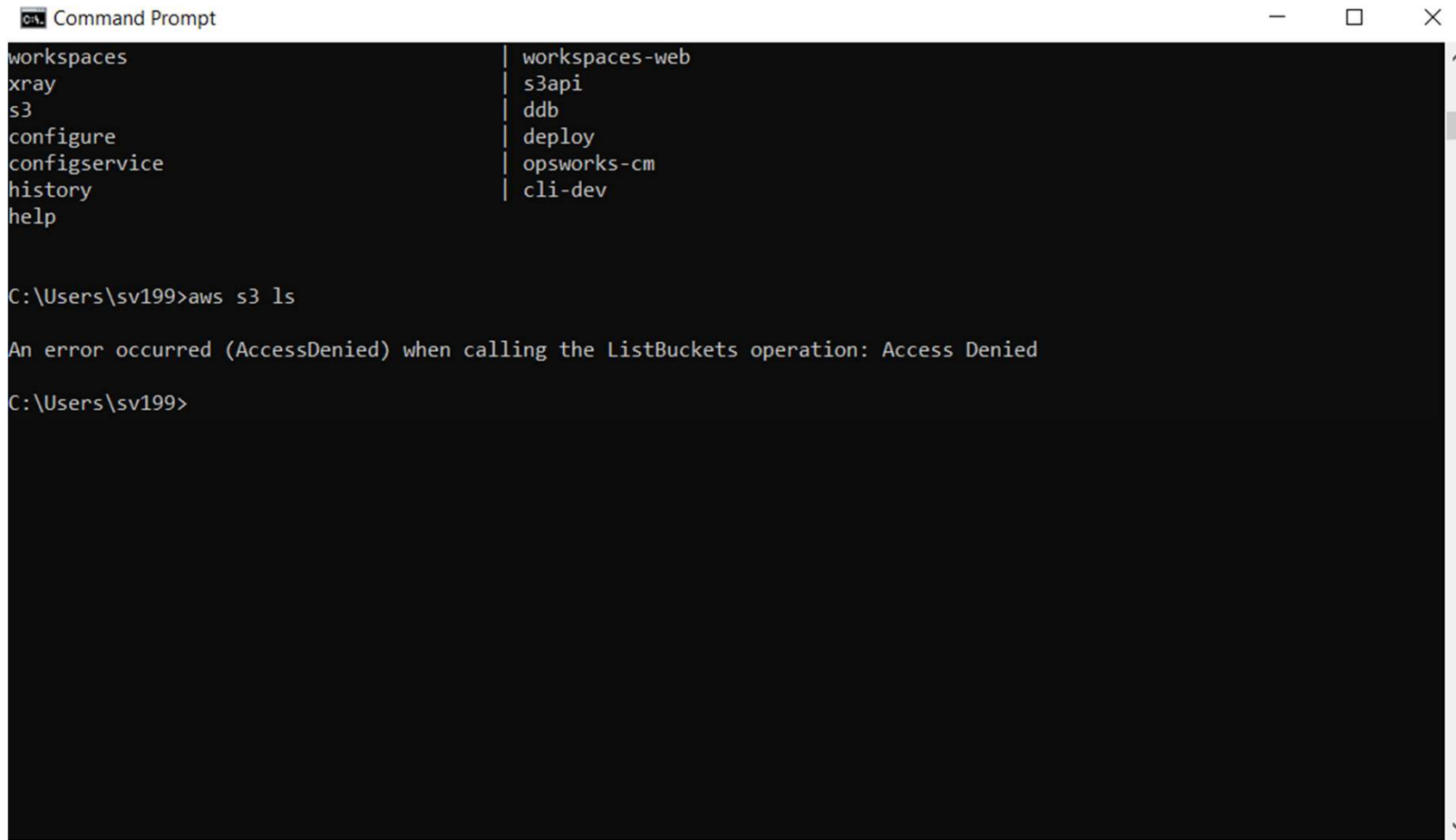
Tags - optional
Tags are key-value pairs you can add to AWS resources to help identify, organize, or search for resources. Choose any tags you want to associate with this user.

No tags associated with the resource.

[Add new tag](#)
You can add up to 50 more tags.

[Cancel](#) [Previous](#) [Create user](#)

Gave s3-full access permission policy to user mahi but it shows access denied because I set the boundary permission as Vpc-full access.



```
Command Prompt
workspaces      | workspaces-web
xray            | s3api
s3              | ddb
configure       | deploy
configservice  | opsworks-cm
history         | cli-dev
help

C:\Users\sv199>aws s3 ls

An error occurred (AccessDenied) when calling the ListBuckets operation: Access Denied

C:\Users\sv199>
```

Created user and named as mahi

The screenshot shows the AWS IAM console interface. The left sidebar contains the 'Identity and Access Management (IAM)' menu with options like Dashboard, Access management, and Access reports. The main content area displays the 'Users (1)' page, which includes a search bar and a table of users. The table has columns for User name, Groups, Last activity, MFA, Password age, and Active key age. A single user named 'mah' is listed with a password age of '2 minutes ago'.

Users (1) Info

An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

Find users by username or access key

<input type="checkbox"/>	User name	Groups	Last activity	MFA	Password age	Active key age
<input type="checkbox"/>	mah	None	Never	None	2 minutes ago	-

Access key and secret access key generated

The screenshot shows the AWS IAM console interface. At the top, there's a navigation bar with the AWS logo, a search bar, and a user profile dropdown. The main content area is titled 'Retrieve access keys' and includes a green banner stating 'Access key created'. Below this, there's a table showing the generated Access key and Secret access key. The Access key is 'AKIASQEXODK3XLDEVEVN' and the Secret access key is 'Uh4On1DPs5c+Nd5LhpuEuyEonHMAGPm9Z01uoG8'. A 'Hide' link is next to the secret key. Below the table, there's a section titled 'Access key best practices' with a list of recommendations: 'Never store your access key in plain text, in a code repository, or in code.', 'Disable or delete access key when no longer needed.', 'Enable least-privilege permissions.', and 'Rotate access keys regularly.' At the bottom of the console, there's a 'Download .csv file' button and a 'Done' button. The bottom of the image shows a Windows taskbar with various application icons and a system tray displaying the date and time.

WhatsApp IAM > Users > mahi > Create acc... what is set permission boundary... how many policies can attach to... +

us-east-1.console.aws.amazon.com/iamv2/home?region=eu-north-1#/users/details/mahi/create-access-key

Services Search [Alt+S]

EC2 IAM

Access key created
This is the only time that the secret access key can be viewed or downloaded. You cannot recover it later. However, you can create a new access key any time.

Step 1
Access key best practices & alternatives

Step 2 - optional
Set description tag

Step 3
Retrieve access keys

Retrieve access keys [Info](#)

Access key	Secret access key
AKIASQEXODK3XLDEVEVN	Uh4On1DPs5c+Nd5LhpuEuyEonHMAGPm9Z01uoG8 Hide

Access key best practices

- Never store your access key in plain text, in a code repository, or in code.
- Disable or delete access key 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](#).

[Download .csv file](#) [Done](#)

CloudShell Feedback Language © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

mahi_credentials (1).csv AWS & EC2 intro (1).txt EC2 ADVANCE (1).txt [Show all](#)

Type here to search 28°C 01:01 PM 26-07-2023

Command prompt

```
Command Prompt
Microsoft Windows [Version 10.0.19045.3208]
(c) Microsoft Corporation. All rights reserved.

C:\Users\sv199>aws --version
aws-cli/2.13.3 Python/3.11.4 Windows/10 exe/AMD64 prompt/off

C:\Users\sv199>aws configure
AWS Access Key ID [*****G23N]: AKIASQEX0DK32OUGG23N
AWS Secret Access Key [*****lBme]: Ai4n14HBs7qmSyTkNxaD4B9oHPRbEr1RkVrx1Bme
Default region name [eu-west-2]: eu-west-2
Default output format [json]: json

C:\Users\sv199>aws s3 ls

An error occurred (AccessDenied) when calling the ListBuckets operation: Access Denied

C:\Users\sv199>aws ec2 ls

usage: aws [options] <command> <subcommand> [<subcommand> ...] [parameters]
To see help text, you can run:

    aws help
    aws <command> help
    aws <command> <subcommand> help

aws: error: argument operation: Invalid choice, valid choices are:

accept-address-transfer | accept-reserved-instances-exchange-quote
accept-transit-gateway-multicast-domain-associations | accept-transit-gateway-peering-attachment
accept-transit-gateway-vpc-attachment | accept-vpc-endpoint-connections
```


user group created

The screenshot displays the AWS IAM console interface. At the top, a green banner indicates 'ec2-permission user group created.' with a 'View group' button. The left sidebar shows the 'Identity and Access Management (IAM)' menu with options like Dashboard, Access management, and Access reports. The main content area shows the 'User groups (1)' page. A table lists the user group 'ec2-permission' with 1 user and 'Defined' permissions. The bottom of the screen shows a Windows taskbar with various application icons and system information.

us-east-1.console.aws.amazon.com/iamv2/home?region=eu-north-1#/groups

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
- Analyzers
- Settings

ec2-permission user group created. View group

IAM > User groups

User groups (1) Info

A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.

Filter User groups by property or group name and press enter

<input type="checkbox"/>	Group name	Users	Permissions	Creation time
<input type="checkbox"/>	ec2-permission	1	Defined	Now

CloudShell Feedback Language

© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

mahi_credentials (1).csv AWS & EC2 intro (1).txt EC2 ADVANCE (1).txt Show all

Type here to search

29°C

01:23 PM 26-07-2023

Role created: ec2-s3-fullaccess

The screenshot displays the AWS IAM console in the 'us-east-1' region. The left sidebar shows the 'Identity and Access Management (IAM)' section with options like Dashboard, Access management, and Access reports. The main content area is titled 'IAM > Roles' and shows a list of roles. The role 'ec2-s3-fullaccess' is highlighted. Below the list, there is a section for 'Roles Anywhere' with options like 'Access AWS from your non AWS workloads', 'X.509 Standard', and 'Temporary credentials'.

Role name	Trusted entities	Last activity
AWSServiceRoleForSupport	AWS Service: support (Service-Linked Role)	5 days ago
AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor (Service-Linked Role)	-
ec2-s3-fullaccess	AWS Service: ec2	-

Instance created with withrole and without role:

```
root@ip-172-31-18-127:~  
login as: ec2-user  
Authenticating with public key "mykey"  
#  
~\#### Amazon Linux 2023  
~~\#####\  
~~\###|  
~~\#/ https://aws.amazon.com/linux/amazon-linux-  
~~V~'-'>  
~~~  
~~.  
~-./-/-/-/  
~/m/'
```

[ec2-user@ip-172-31-18-127 ~]\$ sudo -i
[root@ip-172-31-18-127 ~]#

[illegible]

root@ip-172-31-18-127:~

```
[root@ip-172-31-18-127 ~]# aws s3 ls
```

2023-07-26 08:27:43 26-07-23

```
[root@ip-172-31-18-127 ~]#
```

root@ip-172-31-23-132:~

```
login as: ec2-user
```

```
Authenticating with public key "mykey"
```

```
      #_
     _###_      Amazon Linux 2023
    _####_
   _#####_
  _#####_
 _#####_
_#####_
V~'-'>

```

<https://aws.amazon.com/linux/amazon-linux-2023>

Last login: Wed Jul 26 08:35:58 2023 from 223.187.119.249

```
[ec2-user@ip-172-31-23-132 ~]$ sudo -i
```

```
[root@ip-172-31-23-132 ~]# aws s3 ls
```

Unable to locate credentials. You can configure credentials by running "aws configure".

```
[root@ip-172-31-23-132 ~]#
```

 root@ip-172-31-18-127:~

```
[root@ip-172-31-18-127 ~]# aws s3 ls
2023-07-26 08:27:43 26-07-23
[root@ip-172-31-18-127 ~]# ^C
[root@ip-172-31-18-127 ~]#
```

 root@ip-172-31-23-132:~

```

AWS Access Key ID [None]:
login as: ec2-user
Authenticating with public key "mykey"

#
~\#### Amazon Linux 2023
~~\#####
~~\###|
~~\#/ https://aws.amazon.com/linux/amazon-linux-2023
~~V~' '->
~~~
~~.-.
~/m/' '->

Last login: Wed Jul 26 08:41:17 2023 from 223.187.119.249
[ec2-user@ip-172-31-23-132 ~]$ sudo -i
[root@ip-172-31-23-132 ~]# aws s3 ls

Unable to locate credentials. You can configure credentials by running
"aws configure".
[root@ip-172-31-23-132 ~]# aws configure
AWS Access Key ID [None]: AKIASQEXODK3XLDEVEVN
AWS Secret Access Key [None]: Uh4On1lDPs5c+Nd5LhpuEuyEonHMAGPm9Z01uoG
8
Default region name [None]: eu-west-2
Default output format [None]: json
[root@ip-172-31-23-132 ~]# aws s3 ls

An error occurred (AccessDenied) when calling the ListBuckets operation: Access Denied
[root@ip-172-31-23-132 ~]#

```

```

root@ip-172-31-18-127:~
[root@ip-172-31-18-127 ~]# aws s3 ls
2023-07-26 08:27:43 26-07-23
[root@ip-172-31-18-127 ~]# ^C
[root@ip-172-31-18-127 ~]#
login as: ec2-user
Authenticating with public key "mykey"

#_
##### Amazon Linux 2023
~~\#####\
~~\#####\
~~\###|
~~\#/ https://aws.amazon.com/linux/amazon-linux-
2023
~~ V~' '->
~~~
~~~.
~~~/_m/'
Last login: Wed Jul 26 08:35:30 2023 from 223.187.119.249
[ec2-user@ip-172-31-18-127 ~]$ sudo -i
[root@ip-172-31-18-127 ~]# user add seenu
-bash: user: command not found
[root@ip-172-31-18-127 ~]# useradd seenu
[root@ip-172-31-18-127 ~]# su seenu
[seenu@ip-172-31-18-127 root]$ exit
exit
[root@ip-172-31-18-127 ~]#

```

```

root@ip-172-31-23-132:~
translate | voice-id
waf | waf-regional
wafv2 | wellarchitected
wisdom | workdocs
worklink | workmail
workmailmessageflow | workspaces
workspaces-web | xray
s3api | s3
ddb | configure
deploy | configservice
opsworks-cm | history
cli-dev | help

[root@ip-172-31-23-132 ~]# aws s3 ls

An error occurred (AccessDenied) when calling the ListBuckets oper
on: Access Denied

```

IAM user can reset the password:

Go to IAM page --- > users --- > security credential --- >manage control access --- > enable console access -- > Keep existing password -- > apply (user must create new password at next sign in)

Manage console access [X]

Manage Manoj's AWS console access and password.

Console access

☒ Enable
☐ Disable
Disabling removes the pre-existing password.

Set password

☒ Keep existing password
☐ Autogenerated password
☐ Custom password

☐ User must create new password at next sign-in
Users automatically get the [IAMUserChangePassword](#) policy to allow them to change their own password.

Cancel Apply

Manage console access [X]

Manage Manoj's AWS console access and password.

Console access

☒ Enable
☐ Disable
Disabling removes the pre-existing password.

Set password

☒ Keep existing password
☐ Autogenerated password
☐ Custom password

☒ User must create new password at next sign-in
Users automatically get the [IAMUserChangePassword](#) policy to allow them to change their own password.

Cancel Apply

