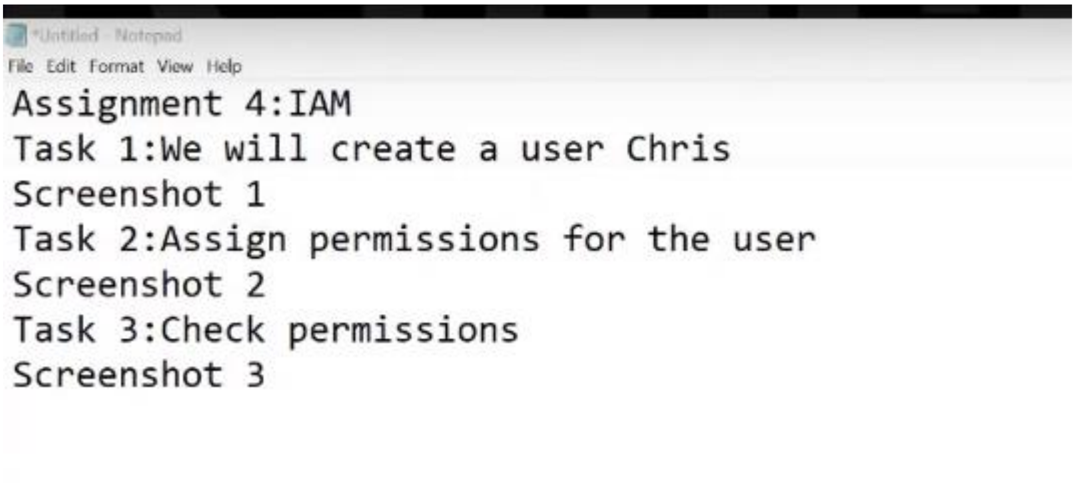
Assignments

Day 4: Assignment 3:

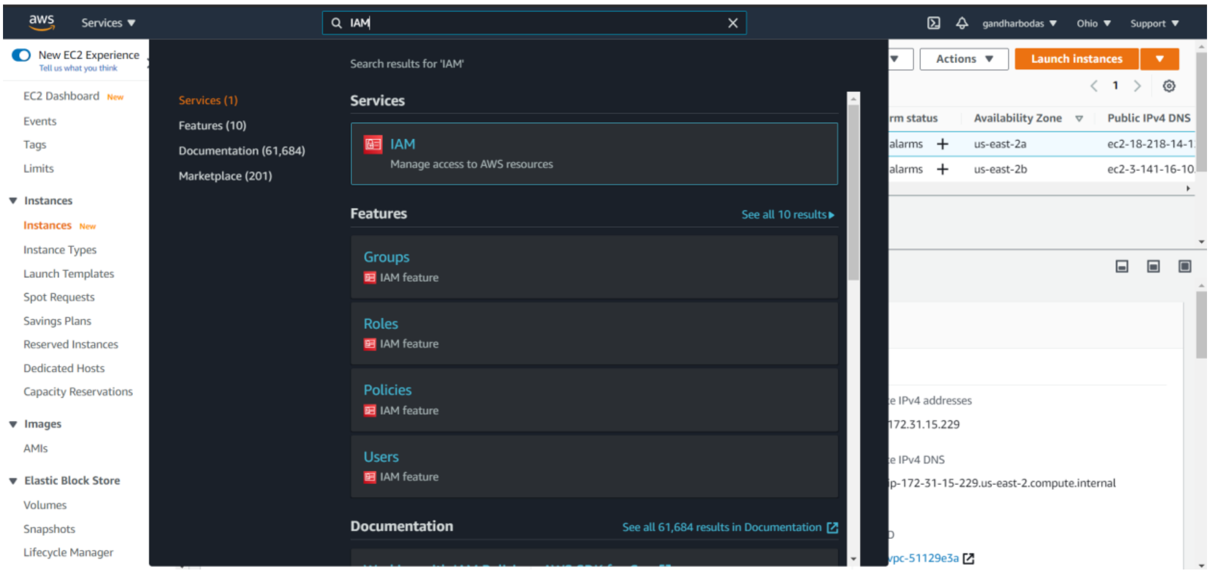


```
Assignment 4:IAM
Task 1:We will create a user Chris
Screenshot 1
Task 2:Assign permissions for the user
Screenshot 2
Task 3:Check permissions
Screenshot 3
```

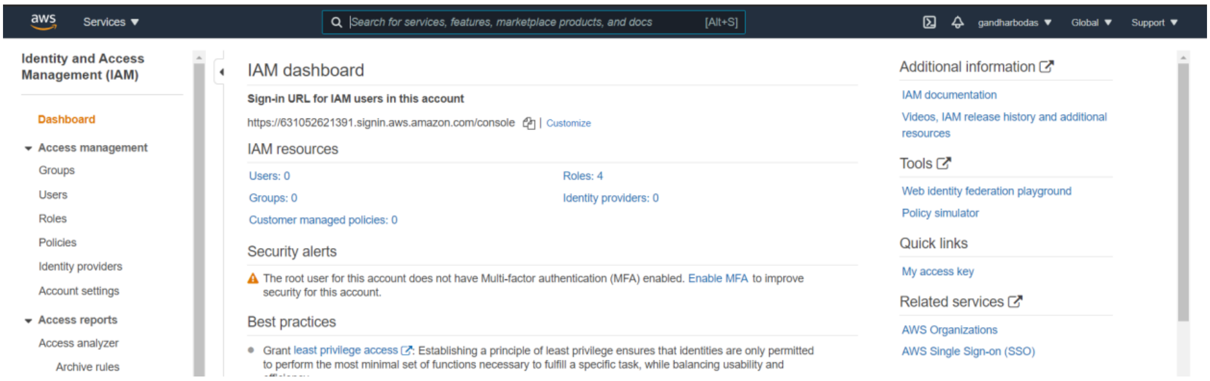
Answer:

Step 1: *We will create a user Chris*

Go to the search engine: IAM and select it.



After selecting: IAM you we get the below page:



aws Services ▼ Search for services, features, marketplace products, and docs [Alt+S] gandharbodas ▼ Global ▼ Support ▼

Identity and Access Management (IAM)

Dashboard

▾ Access management

Groups

Users

Roles

Policies

Identity providers

Account settings

▾ Access reports

Access analyzer

Archive rules

IAM dashboard

Sign-in URL for IAM users in this account

https://631052621391.signin.aws.amazon.com/console | Customize

IAM resources

Users: 0 Roles: 4

Groups: 0 Identity providers: 0

Customer managed policies: 0

Security alerts

⚠ The root user for this account does not have Multi-factor authentication (MFA) enabled. Enable MFA to improve security for this account.

Best practices

- Grant least privilege access: Establishing a principle of least privilege ensures that identities are only permitted to perform the most minimal set of functions necessary to fulfill a specific task, while balancing usability and

Additional information

IAM documentation

Videos, IAM release history and additional resources

Tools

Web identity federation playground

Policy simulator

Quick links

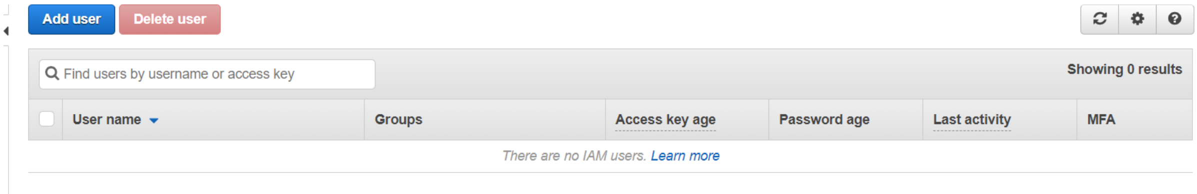
My access key

Related services

AWS Organizations

AWS Single Sign-on (SSO)

Now click on “Users” option which is on Left side of panel” and you will get the page:



Add user Delete user

Find users by username or access key Showing 0 results

□	User name ▾	Groups	Access key age	Password age	Last activity	MFA

There are no IAM users. Learn more

Now, click on “Add user” and Set the user details: User name: user1.

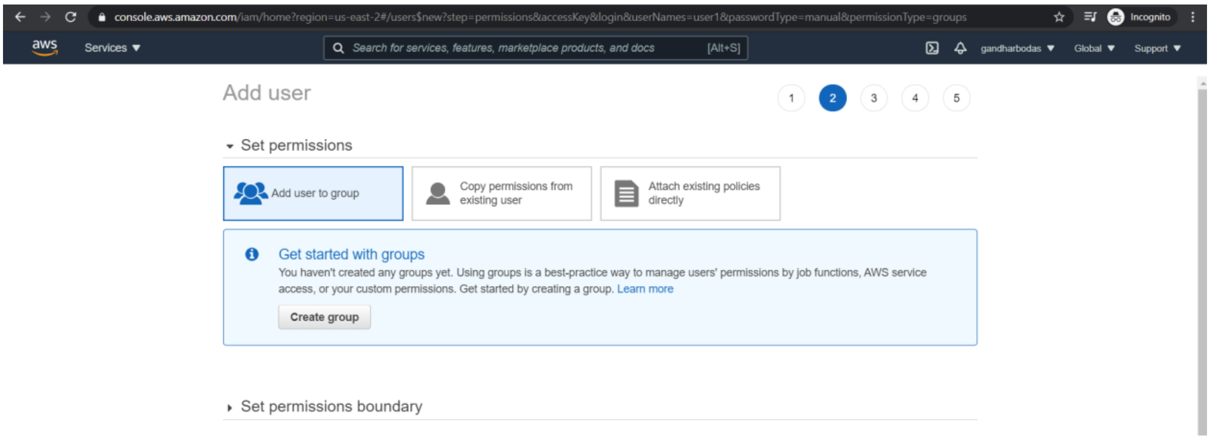
Select AWS access type: Tick on both the check box i.e., select both options:

Access type: Programmatic access and AWS Management Console access.

Set Customer Password: Swami@b19 and

Required password reset: Tick the check box of this. =Yes.

Now, click on “Next: Permission” button and you will get next page as below:



console.aws.amazon.com/iam/home?region=us-east-2#/users$new?step=permissions&accessKey&login&userNames=user1&passwordType=manual&permissionType=groups Incognito

aws Services ▼ Search for services, features, marketplace products, and docs [Alt+S] gandharbodas ▼ Global ▼ Support ▼

Add user 1 2 3 4 5

▾ Set permissions

Add user to group | Copy permissions from existing user | Attach existing policies directly

Get started with groups

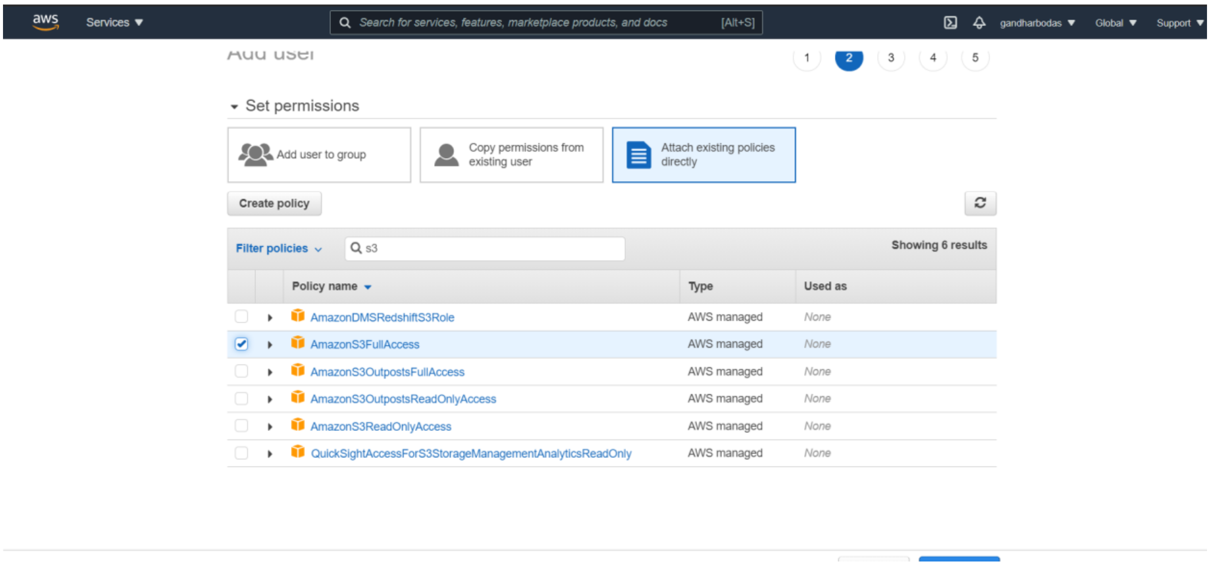
You haven't created any groups yet. Using groups is a best-practice way to manage users' permissions by job functions, AWS service access, or your custom permissions. Get started by creating a group. Learn more

Create group

▸ Set permissions boundary

Step 2: *Assign permission for the user*

Now, select “Attach existing policies directly” option and Filter policies: s3 and select “AmazonS3FullAccess” option and once done these all click on **“Next: Tag’s button”.**


aws
Services ▼
Search for services, features, marketplace products, and docs [Alt+S]
gandharbodas ▼
Global ▼
Support ▼
Add user
1
2
3
4
5
Add user to group
Copy permissions from existing user
Create policy

▾ Set permissions

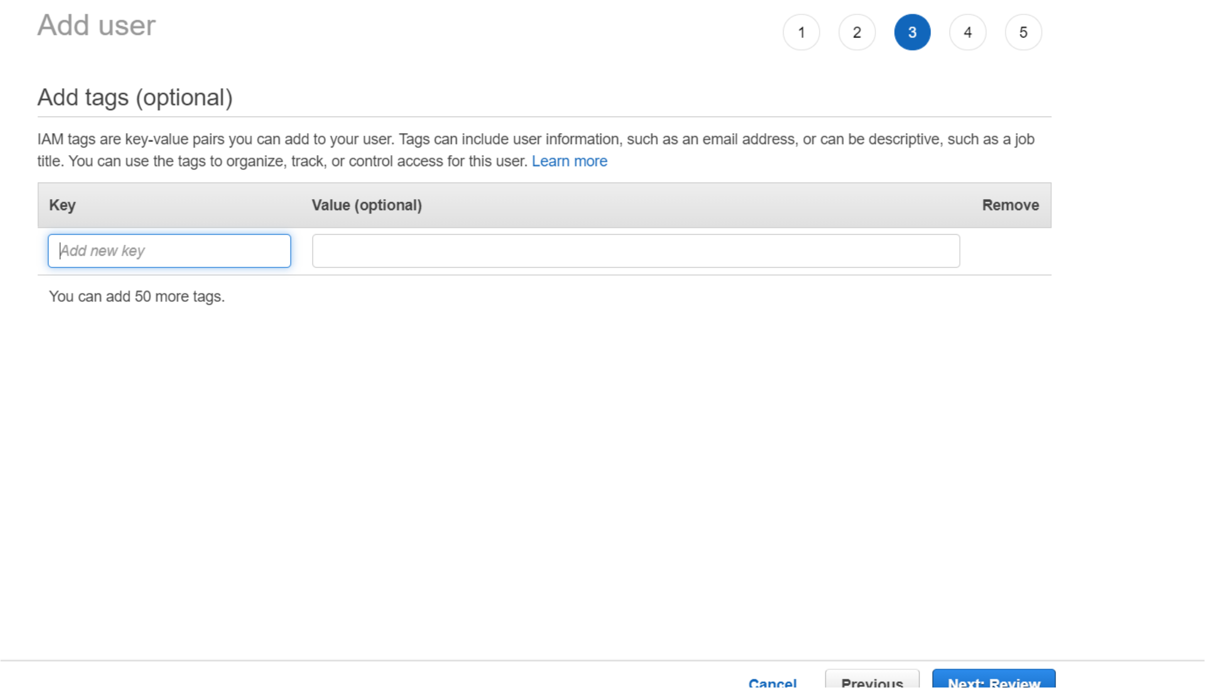
Attach existing policies directly

Filter policies ⌄ s3

Showing 6 results

		Policy name ▾	Type	Used as
□	▸	AmazonDMSRedshiftS3Role	AWS managed	None
☑	▸	AmazonS3FullAccess	AWS managed	None
□	▸	AmazonS3OutpostsFullAccess	AWS managed	None
□	▸	AmazonS3OutpostsReadOnlyAccess	AWS managed	None
□	▸	AmazonS3ReadOnlyAccess	AWS managed	None
□	▸	QuickSightAccessForS3StorageManagementAnalyticsReadOnly	AWS managed	None

Add tages page will get display as below:



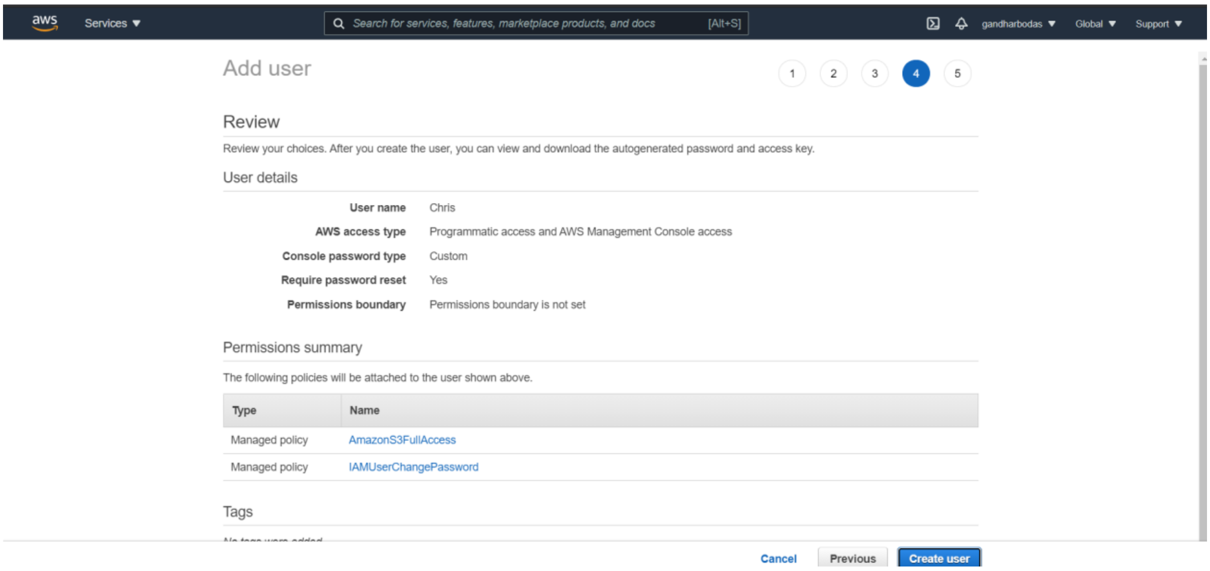
Add tags (optional)

IAM tags are key-value pairs you can add to your user. Tags can include user information, such as an email address, or can be descriptive, such as a job title. You can use the tags to organize, track, or control access for this user. Learn more

Key	Value (optional)	Remove
Add new key		

You can add 50 more tags.

Here, I am going to keep as it is and now click on “Next: Review” button and once clicked the next page will get appear as below:



Add user

Review

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

User details

User name	Chris
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

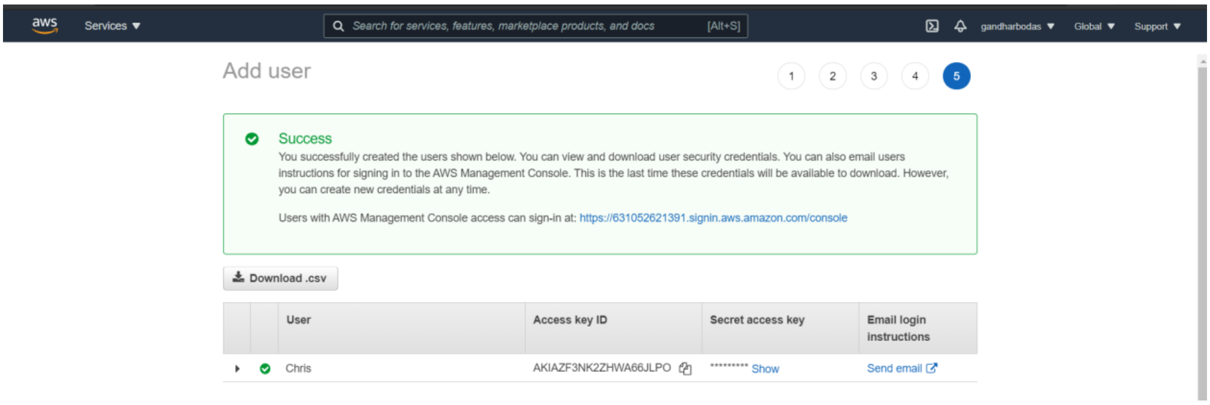
The following policies will be attached to the user shown above.

Type	Name
Managed policy	AmazonS3FullAccess
Managed policy	IAMUserChangePassword

Tags

No tags were added

Now, go ahead and click on “Create user”.


aws
Services ▼
Search for services, features, marketplace products, and docs [Alt+S]
gandharbodas ▼
Global ▼
Support ▼
1 2 3 4 5
Download .csv

Add user

Success

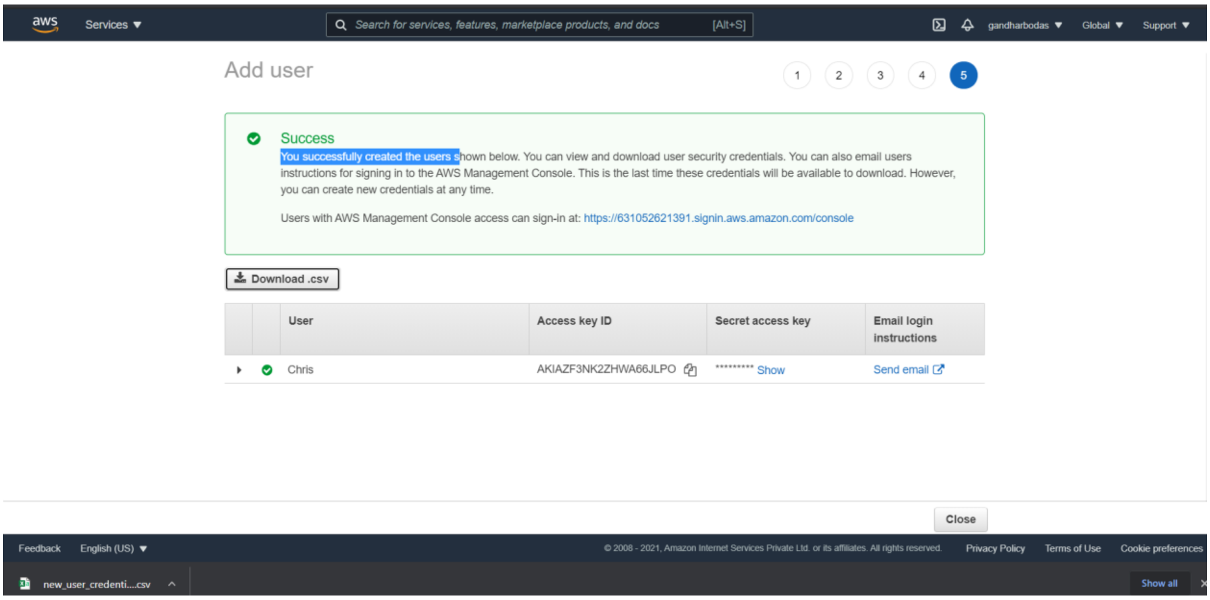
You successfully created the users shown below. You can view and download user security credentials. You can also email users instructions for signing in to the AWS Management Console. This is the last time these credentials will be available to download. However, you can create new credentials at any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

Users with AWS Management Console access can sign-in at: https://631052621391.signin.aws.amazon.com/console

		User	Access key ID	Secret access key	Email login instructions
▸	✓	Chris	AKIAZF3NK2ZHWA66JLPO	******** Show	Send email

You successfully created the users.

Now, download the .csv excel file in which you will get User name, Access key ID, secret access key and Console login link.


aws
Services ▼
Search for services, features, marketplace products, and docs [Alt+S]
gandharbodas ▼
Global ▼
Support ▼
1
2
3
4
5
Close
Feedback
English (US) ▼
© 2008 - 2021, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
Cookie preferences
new_user_credenti....csv
Show all

Add user

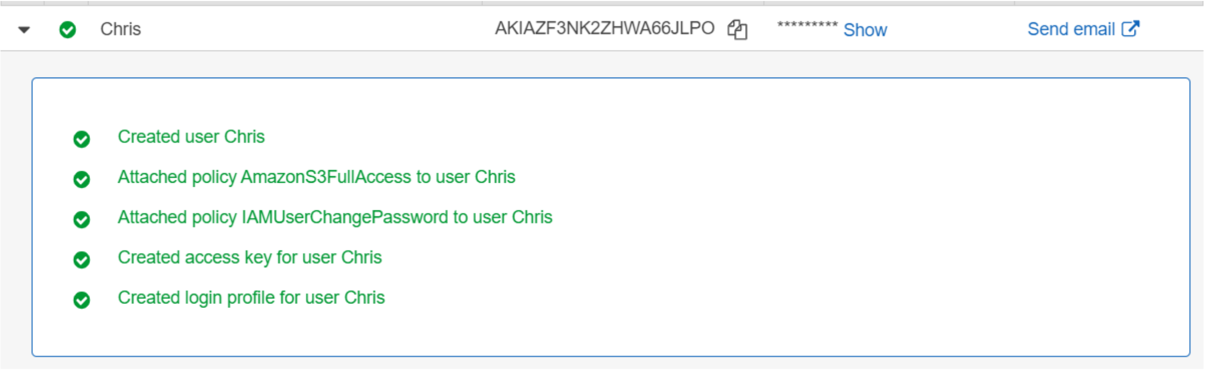
Success

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://631052621391.signin.aws.amazon.com/console

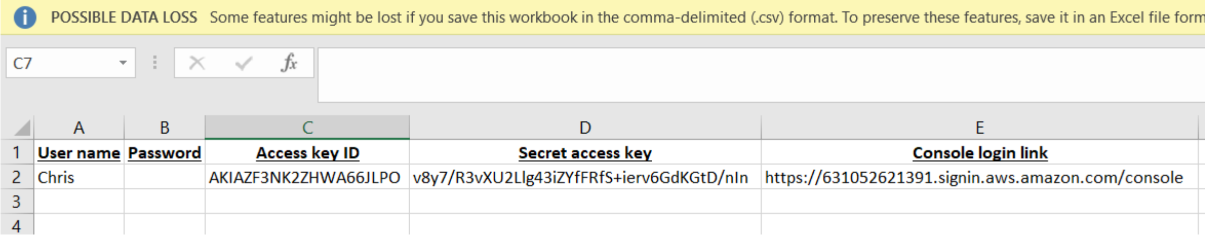
Download .csv

		User	Access key ID	Secret access key	Email login instructions
▸	✓	Chris	AKIAZF3NK2ZHWA66JLPO	********* Show	Send email



▾	✓	Chris	AKIAZF3NK2ZHWA66JLPO	********* Show	Send email

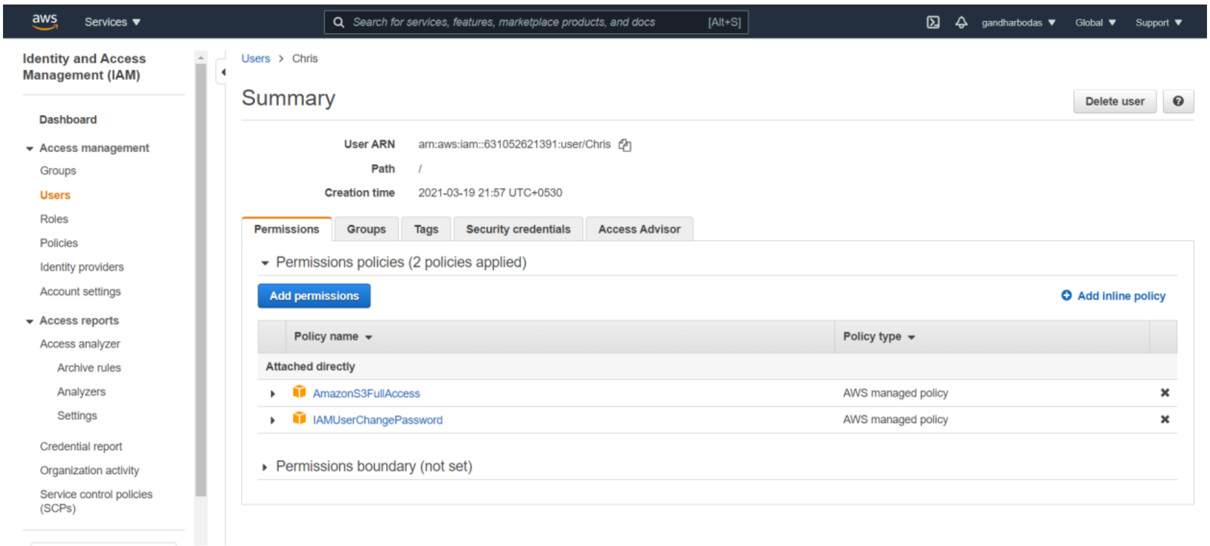
- ✓ Created user Chris
- ✓ Attached policy AmazonS3FullAccess to user Chris
- ✓ Attached policy IAMUserChangePassword to user Chris
- ✓ Created access key for user Chris
- ✓ Created login profile for user Chris



POSSIBLE DATA LOSS Some features might be lost if you save this workbook in the comma-delimited (.csv) format. To preserve these features, save it in an Excel file form

	A	B	C	D	E
1	User name	Password	Access key ID	Secret access key	Console login link
2	Chris		AKIAZF3NK2ZHWA66JLPO	v8y7/R3vXU2Llg43iZYfFRfS+ierv6GdKGtD/nIn	https://631052621391.signin.aws.amazon.com/console
3					
4					

Now, let’s go back and click on user: Chris:



Summary

User ARN arn:aws:iam::631052621391:user/Chris

Path /

Creation time 2021-03-19 21:57 UTC+0530

Permissions policies (2 policies applied)

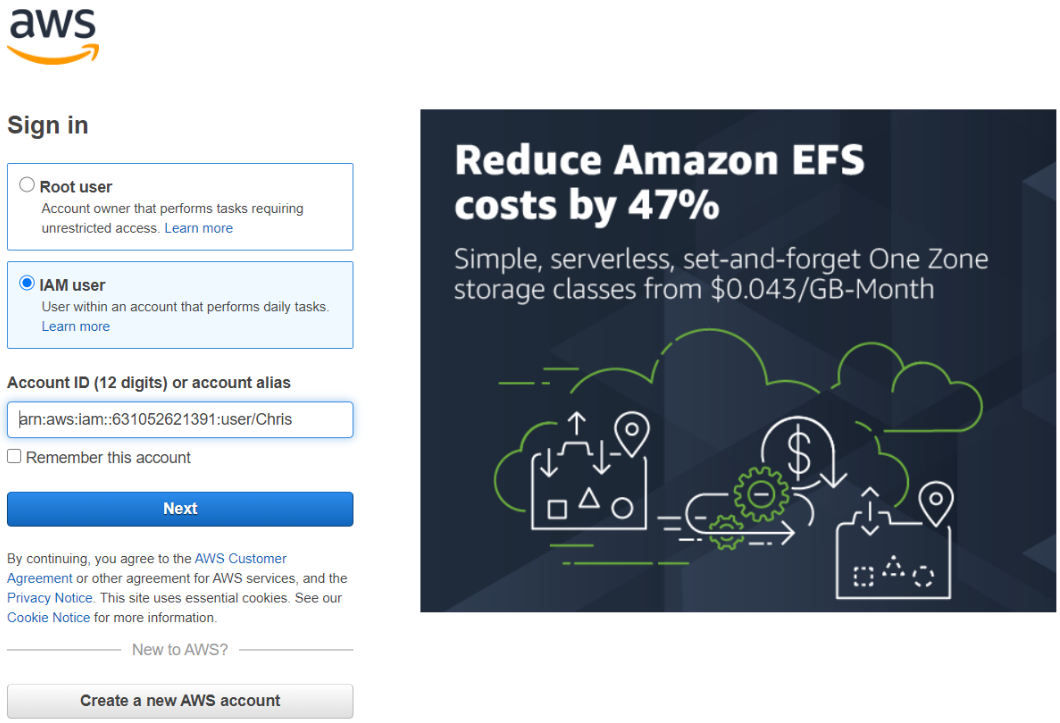
Policy name	Policy type
Attached directly	
AmazonS3FullAccess	AWS managed policy
IAMUserChangePassword	AWS managed policy

Permissions boundary (not set)

Step 3: *Logged in to the User: Chris*

Now copy ARN (Amazon Resource Name): arn:aws:iam::631052621391:user/Chris

Logout from existing root user and then logged in as IAM user as below:


aws
Reduce Amazon EFS costs by 47%
Simple, serverless, set-and-forget One Zone storage classes from $0.043/GB-Month

Sign in

○ Root user
Account owner that performs tasks requiring unrestricted access. Learn more

● IAM user
User within an account that performs daily tasks. Learn more

Account ID (12 digits) or account alias

arn:aws:iam::631052621391:user/Chris

□ Remember this account

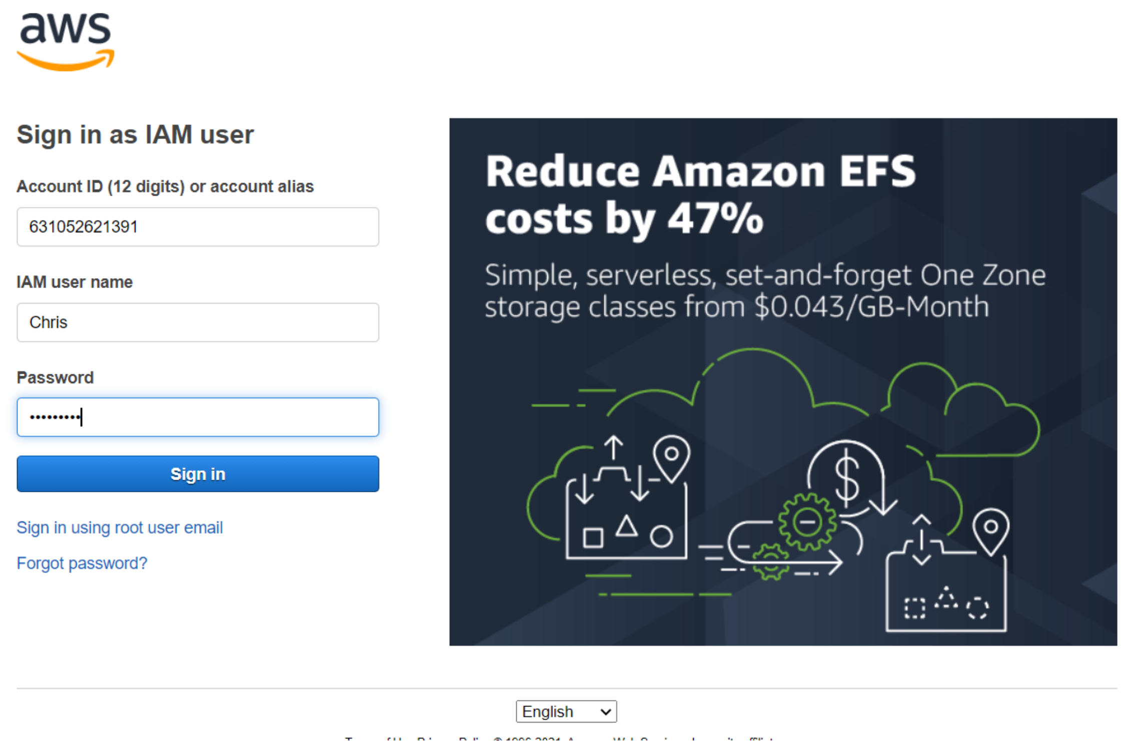
Next

By continuing, you agree to the AWS Customer Agreement or other agreement for AWS services, and the Privacy Notice. This site uses essential cookies. See our Cookie Notice for more information.

New to AWS?

Create a new AWS account

Now insert the Account ID, Username and Password as below:



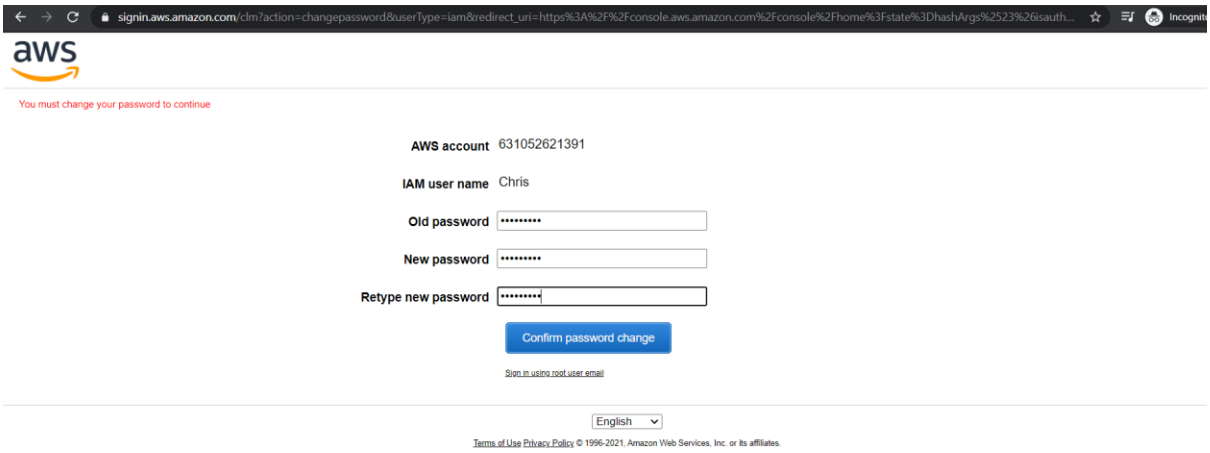
Sign in as IAM user

Account ID (12 digits) or account alias: 631052621391

IAM user name: Chris

Password: •••••••••

Now here, you have to set new password for user: Chris as below and then click on Confirm password change.



signin.aws.amazon.com/clm?action=changepassword&userType=iam&redirect_uri=https%3A%2F%2Fconsole.aws.amazon.com%2Fconsole%2Fhome%3Fstate%3DhashArgs%2523%26isauth...

You must change your password to continue

AWS account: 631052621391

IAM user name: Chris

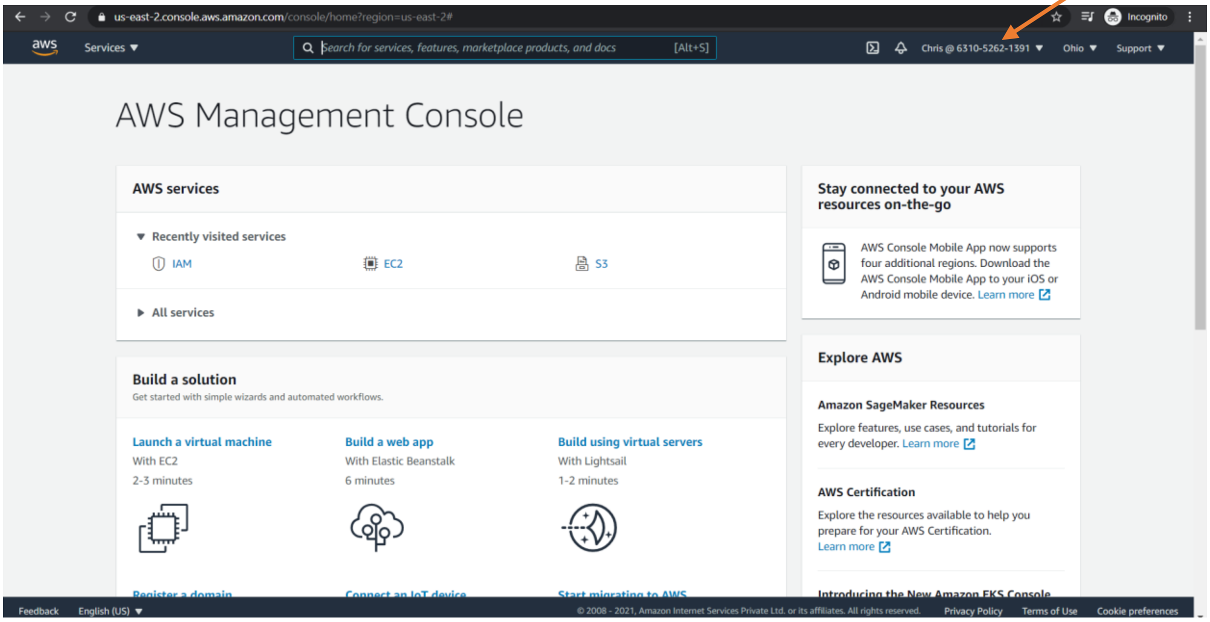
Old password: •••••••••

New password: •••••••••

Retype new password: •••••••••

Terms of Use Privacy Policy © 1996-2021, Amazon Web Services, Inc. or its affiliates.

Once new password set the next page will get appear as below:



This one user name: Chris

us-east-2.console.aws.amazon.com/console/home?region=us-east-2#

aws Services ▼ Search for services, features, marketplace products, and docs [Alt+S] Chris @ 6310-5262-1391 ▼ Ohio ▼ Support ▼

AWS Management Console

AWS services

▼ Recently visited services

IAM EC2 S3

▶ 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 Connect an IoT device Start migrating to AWS

Stay connected to your AWS resources on-the-go

AWS Console Mobile App now supports four additional regions. Download the AWS Console Mobile App to your iOS or Android mobile device. Learn more

Explore AWS

Amazon SageMaker Resources

Explore features, use cases, and tutorials for every developer. Learn more

AWS Certification

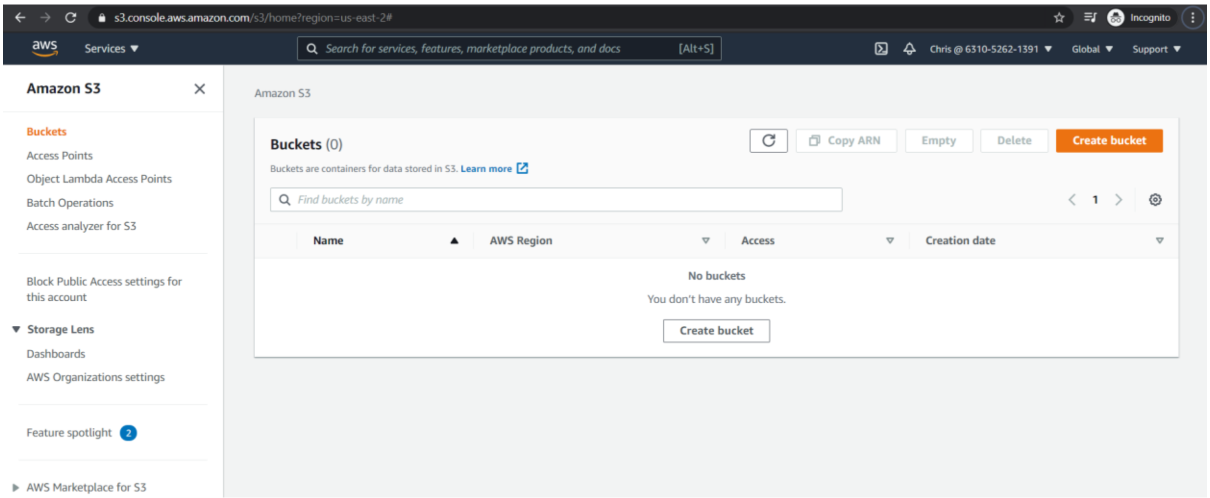
Explore the resources available to help you prepare for your AWS Certification. Learn more

Introducing the New Amazon EKS Console

Feedback English (US) ▼ © 2008 - 2021, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use Cookie preferences

Step 4: *Check permissions on user: Chris*

Go to the Services--→S3-→ he will be able to see the below screen:



s3.console.aws.amazon.com/s3/home?region=us-east-2#

aws Services ▼ Search for services, features, marketplace products, and docs [Alt+S] Chris @ 6310-5262-1391 ▼ Global ▼ Support ▼

Amazon S3 ✕

Buckets
Access Points
Object Lambda Access Points
Batch Operations
Access analyzer for S3

Block Public Access settings for this account

▼ Storage Lens
Dashboards
AWS Organizations settings

Feature spotlight 2

▶ AWS Marketplace for S3

Amazon S3

Buckets (0) Copy ARN Empty Delete Create bucket

Buckets are containers for data stored in S3. Learn more

Find buckets by name

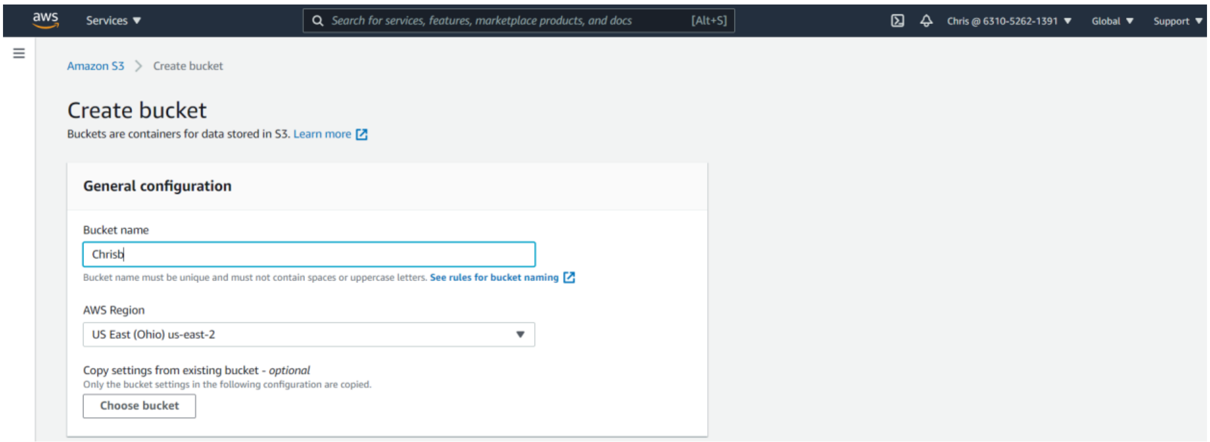
Name ▲	AWS Region ▽	Access ▽	Creation date ▽

No buckets

You don't have any buckets.

Create bucket

He can able to create a bucket, block all public access, etc



aws
Services ▼
Search for services, features, marketplace products, and docs [Alt+S]
Chris @ 6310-5262-1391 ▼
Global ▼
Support ▼
Amazon S3 > Create bucket

Create bucket

Buckets are containers for data stored in S3. Learn more

General configuration

Bucket name

Chrisb

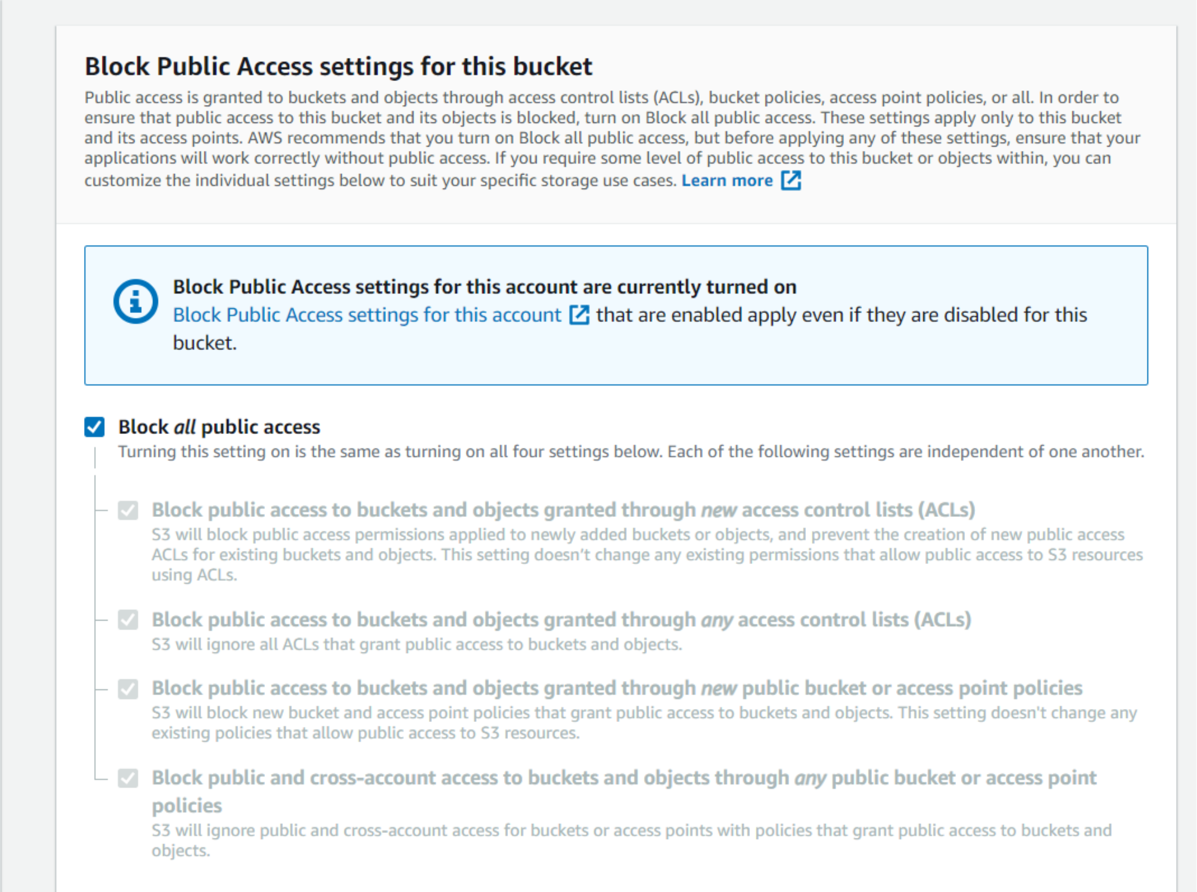
Bucket name must be unique and must not contain spaces or uppercase letters. See rules for bucket naming

AWS Region

US East (Ohio) us-east-2

Copy settings from existing bucket - *optional*

Only the bucket settings in the following configuration are copied.



Block Public Access settings for this bucket

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to this bucket and its objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to this bucket or objects within, you can customize the individual settings below to suit your specific storage use cases. Learn more

Block Public Access settings for this account are currently turned on

Block Public Access settings for this account that are enabled apply even if they are disabled for this bucket.

☑ **Block *all* public access**

Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

- ☑ **Block public access to buckets and objects granted through *new* access control lists (ACLs)**

  S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.

- ☑ **Block public access to buckets and objects granted through *any* access control lists (ACLs)**

  S3 will ignore all ACLs that grant public access to buckets and objects.

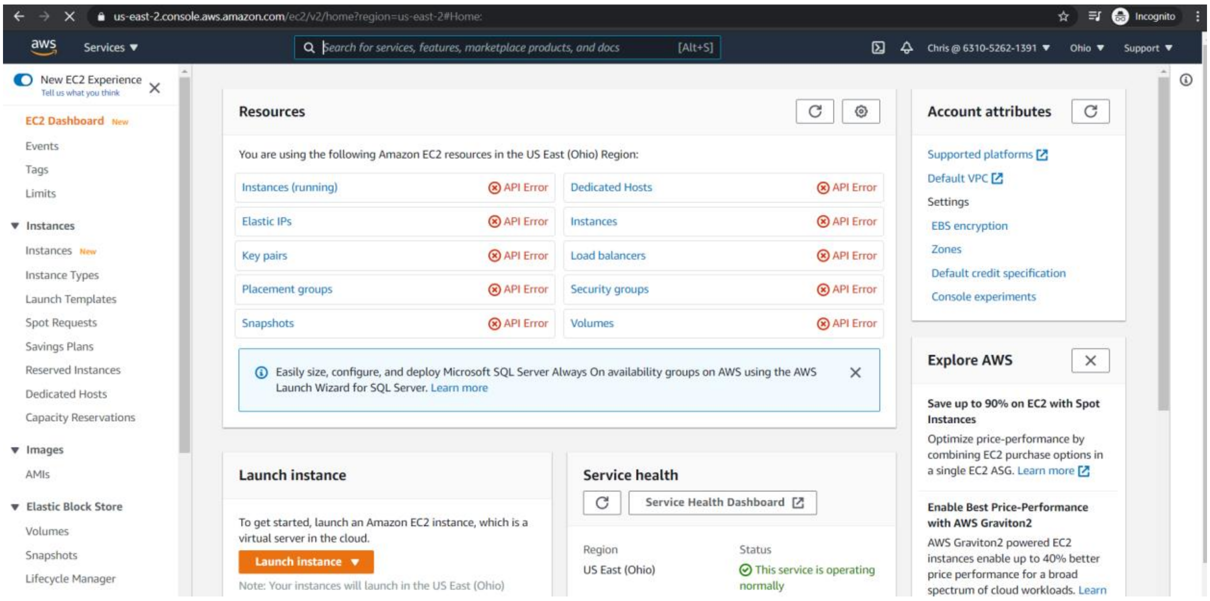
- ☑ **Block public access to buckets and objects granted through *new* public bucket or access point policies**

  S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.

- ☑ **Block public and cross-account access to buckets and objects through *any* public bucket or access point policies**

  S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

Step 5: *Checking is this user has EC2 permissions*



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

Easily size, configure, and deploy Microsoft SQL Server Always On availability groups on AWS using the AWS Launch Wizard for SQL Server. Learn more

Launch instance

To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.

Launch instance ▼

Note: Your instances will launch in the US East (Ohio)

Service health

Service Health Dashboard

Region	Status
US East (Ohio)	This service is operating normally

Account attributes

Supported platforms

Default VPC

Settings

EBS encryption

Zones

Default credit specification

Console experiments

Explore AWS

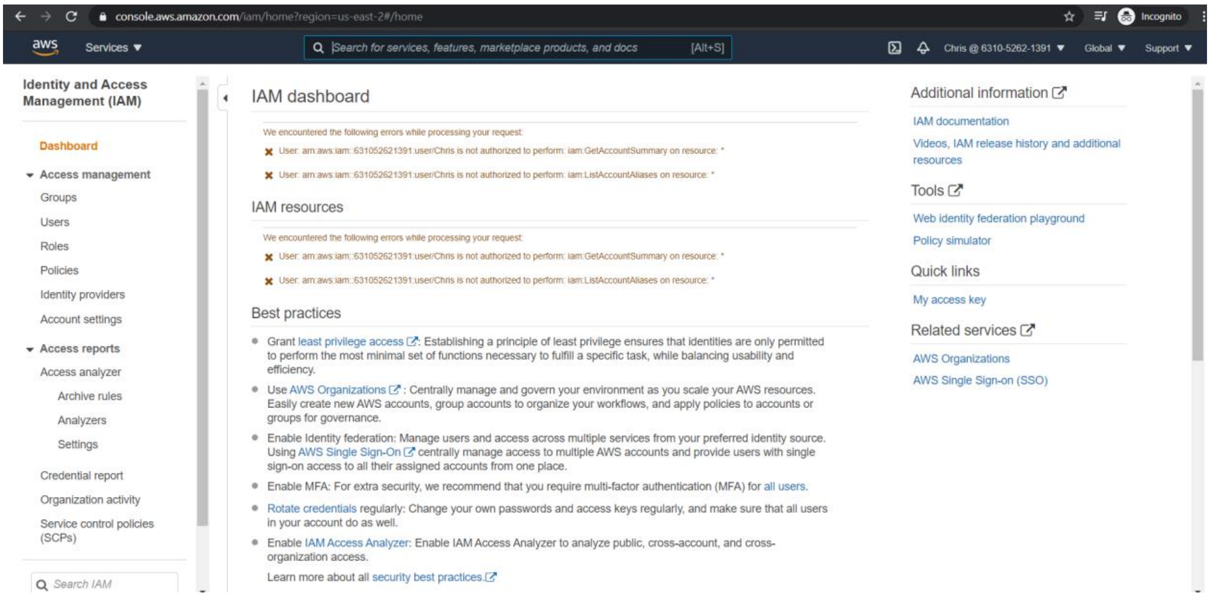
Save up to 90% on EC2 with Spot Instances

Optimize price-performance by combining EC2 purchase options in a single EC2 ASG. Learn more

Enable Best Price-Performance with AWS Graviton2

AWS Graviton2 powered EC2 instances enable up to 40% better price performance for a broad spectrum of cloud workloads. Learn

Step 6: *Checking is this user has IAM permissions*



IAM dashboard

We encountered the following errors while processing your request:

- ✗ User: arn:aws:iam::631052621391:user/Chris is not authorized to perform: iam:GetAccountSummary on resource: *
- ✗ User: arn:aws:iam::631052621391:user/Chris is not authorized to perform: iam:ListAccountAliases on resource: *

IAM resources

We encountered the following errors while processing your request:

- ✗ User: arn:aws:iam::631052621391:user/Chris is not authorized to perform: iam:GetAccountSummary on resource: *
- ✗ User: arn:aws:iam::631052621391:user/Chris is not authorized to perform: iam:ListAccountAliases on resource: *

Best practices

- Grant least privilege access: Establishing a principle of least privilege ensures that identities are only permitted to perform the most minimal set of functions necessary to fulfill a specific task, while balancing usability and efficiency.
- Use AWS Organizations : Centrally manage and govern your environment as you scale your AWS resources. Easily create new AWS accounts, group accounts to organize your workflows, and apply policies to accounts or groups for governance.
- Enable Identity federation: Manage users and access across multiple services from your preferred identity source. Using AWS Single Sign-On centrally manage access to multiple AWS accounts and provide users with single sign-on access to all their assigned accounts from one place.
- Enable MFA: For extra security, we recommend that you require multi-factor authentication (MFA) for all users.
- Rotate credentials regularly: Change your own passwords and access keys regularly, and make sure that all users in your account do as well.
- Enable IAM Access Analyzer: Enable IAM Access Analyzer to analyze public, cross-account, and cross-organization access.

Learn more about all security best practices

Additional information

IAM documentation

Videos, IAM release history and additional resources

Tools

Web identity federation playground

Policy simulator

Quick links

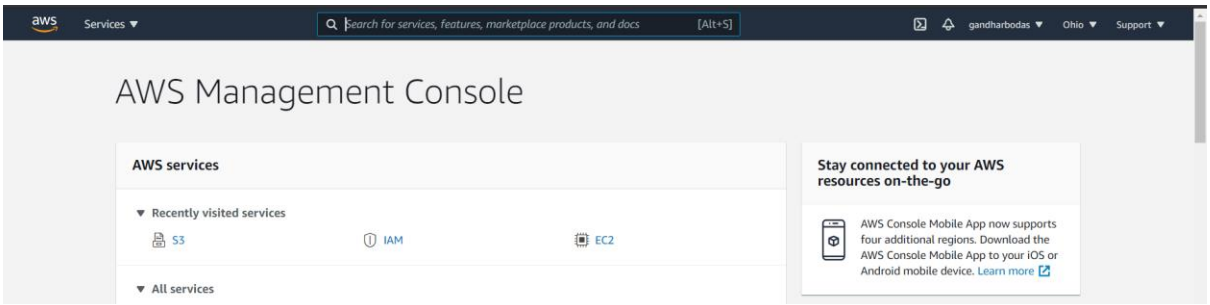
My access key

Related services

AWS Organizations

AWS Single Sign-on (SSO)

Step 7: *Logout from the user: Chris & logged in as the Root user*



AWS Management Console

AWS services

Recently visited services

S3 IAM EC2

All services

Stay connected to your AWS resources on-the-go

AWS Console Mobile App now supports four additional regions. Download the AWS Console Mobile App to your iOS or Android mobile device. Learn more

aws
Services ▼
Search for services, features, marketplace products, and docs
[Alt+S]
gandharbodas ▼
Ohio ▼
Support ▼

END