aws-iam-access-control

Ce projet illustre la gestion des accès AWS IAM en fonction des rôles des utilisateurs. Il simule l'attribution des permissions à trois nouveaux employés pour restreindre leur accès aux ressources AWS (EC2 et S3) en fonction de leur groupe IAM.

🎯 Objectifs

- Créer et gérer des groupes IAM avec des permissions spécifiques.
- Assigner des utilisateurs IAM aux groupes correspondants.
- Appliquer des politiques AWS IAM pour restreindre l'accès aux services AWS (EC2 et S3).
- Vérifier les permissions accordées à chaque utilisateur.

📂 Architecture du projet

L'architecture mise en place est la suivante :

Utilisateur	Groupe IAM	Permissions
user-1	S3-Support	Accès en lecture seule à Amazon S3
user-2	EC2-Support	Accès en lecture seule à Amazon EC2
user-3	EC2-Admin	Voir, démarrer et arrêter les instances Amazon EC2

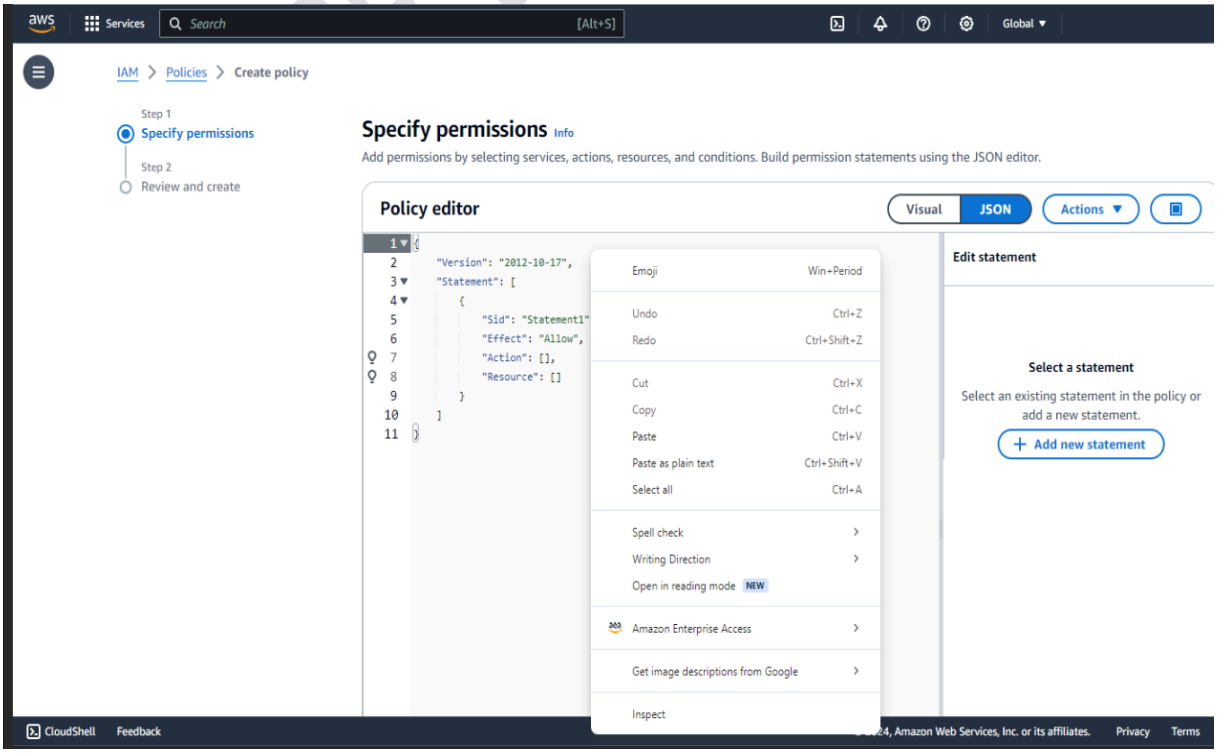
🛠 Prérequis

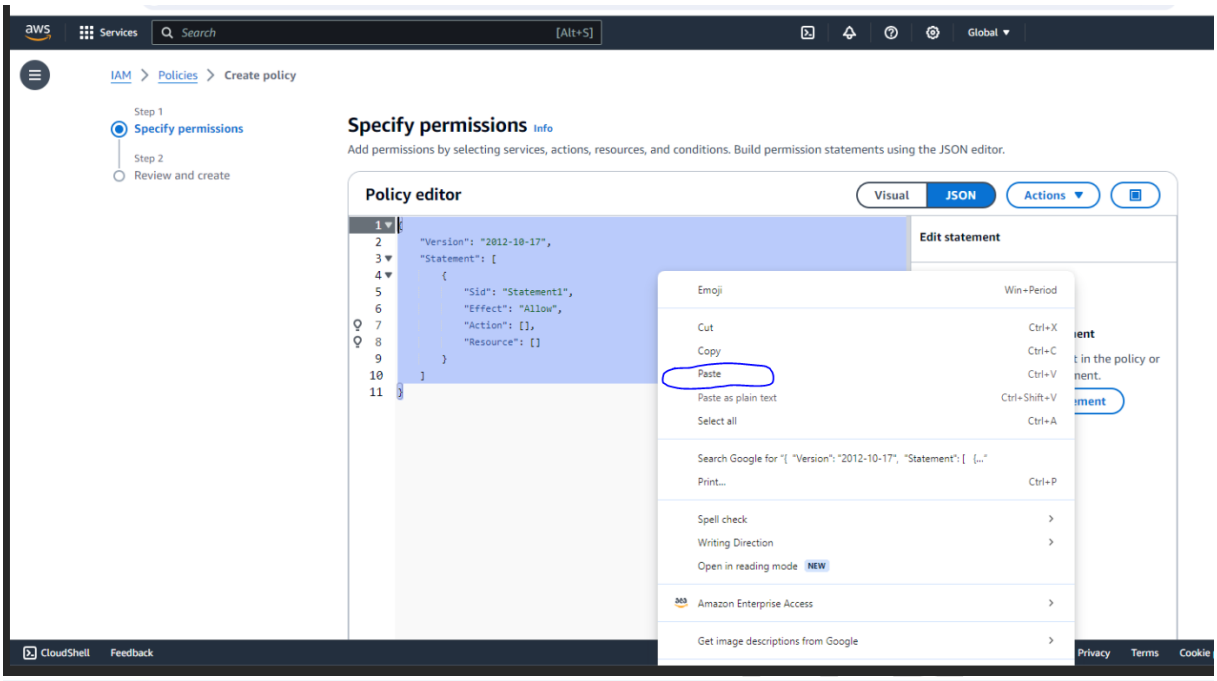
Avoir un compte AWS

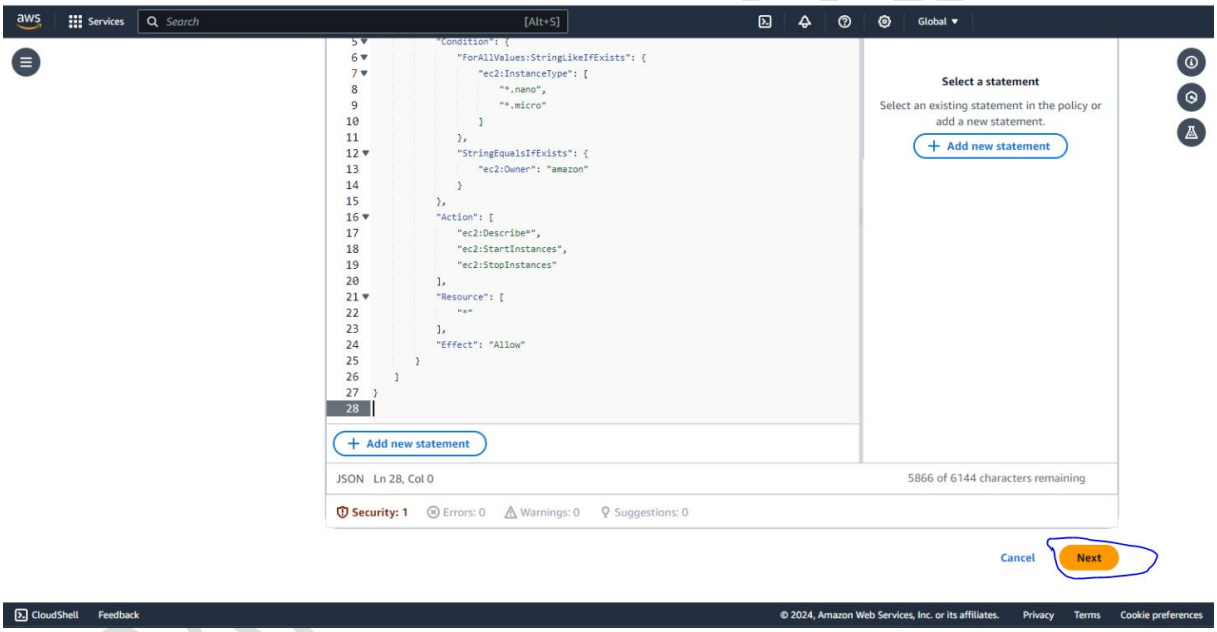
Avoir une instance EC2 déjà créée

Avoir un compartiment S3 déjà crée

Une page web (par exemple un fichier index.html contenant les script html pour notre page web utilisé dans ce Lab).




aws
Services
Search
[Alt+S]
Global
IAM > Policies > Create policy
Step 1
Specify permissions
Step 2
Review and create
Specify permissions Info
Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.
Policy editor
Visual
JSON
Actions
Edit statement
"Version": "2012-10-17",
"Statement": [
"Sid": "Statement1",
"Effect": "Allow",
"Action": [],
"Resource": []
Emoji Win+Period
Cut Ctrl+X
Copy Ctrl+C
Paste Ctrl+V
Paste as plain text Ctrl+Shift+V
Select all Ctrl+A
Search Google for "{ "Version": "2012-10-17", "Statement": [{..."
Print... Ctrl+P
Spell check
Writing Direction
Open in reading mode NEW
Amazon Enterprise Access
Get image descriptions from Google
CloudShell
Feedback
Privacy
Terms


aws
Services
Search
[Alt+S]
Global
"Condition": {
"ForAllValues:StringLikeIfExists": {
"ec2:InstanceType": [
"*.nano",
"*.micro"
]
},
"StringEqualsIfExists": {
"ec2:Owner": "amazon"
}
},
"Action": [
"ec2:Describe*",
"ec2:StartInstances",
"ec2:StopInstances"
],
"Resource": [
"*"
],
"Effect": "Allow"
}
]
}
Select a statement
Select an existing statement in the policy or add a new statement.
Add new statement
Add new statement
JSON Ln 28, Col 0
5866 of 6144 characters remaining
Security: 1
Errors: 0
Warnings: 0
Suggestions: 0
Cancel
Next
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

IAM > Policies > Create policy

Step 1
Specify permissions

Step 2
Review and create

Review and create Info

Review the permissions, specify details, and tags.

Policy details

Policy name
Enter a meaningful name to identify this policy.

EC2-Admin-Policy

Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.

Description - *optional*
Add a short explanation for this policy.

Maximum 1,000 characters. Use alphanumeric and '+=,.@-_' characters.

Permissions defined in this policy Info

Edit

Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it

Search

Allow (1 of 416 services)

Show remaining 415 services

Service	Access level	Resource	Request condition
EC2	Limited: List, Write	All resources	Multiple

Add tags - *optional* Info

Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.

No tags associated with the resource.

Add new tag

You can add up to 50 more tags.

Cancel | Previous | Create policy

Policy EC2-Admin-Policy created. View policy

IAM > Policies

Policies (1228) Info

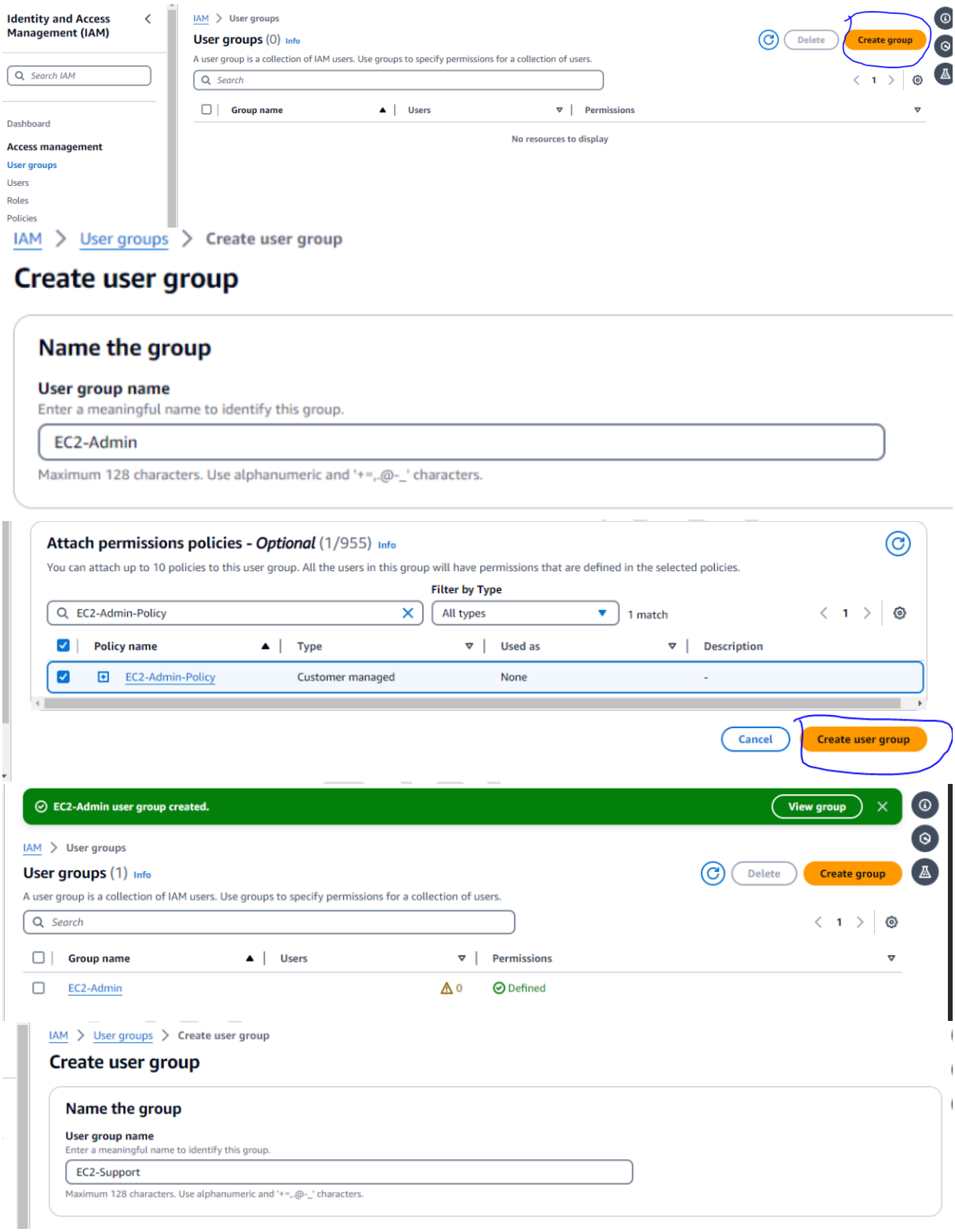
A policy is an object in AWS that defines permissions.

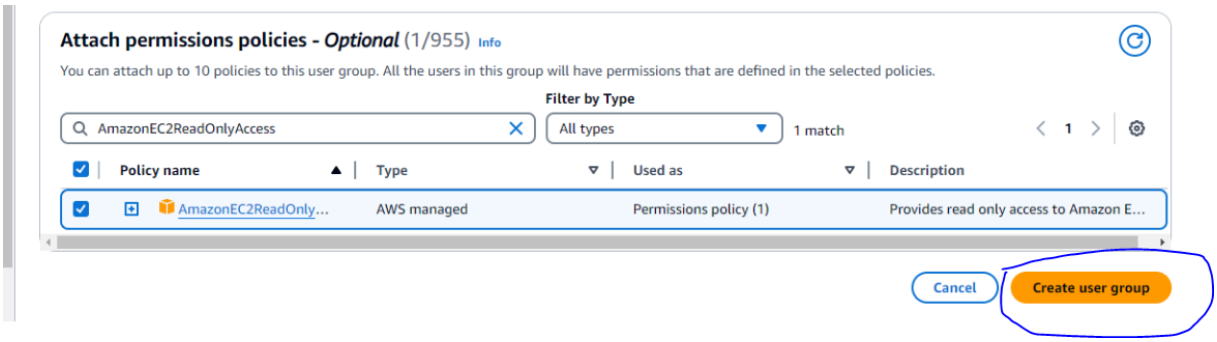
Actions | Delete | Create policy

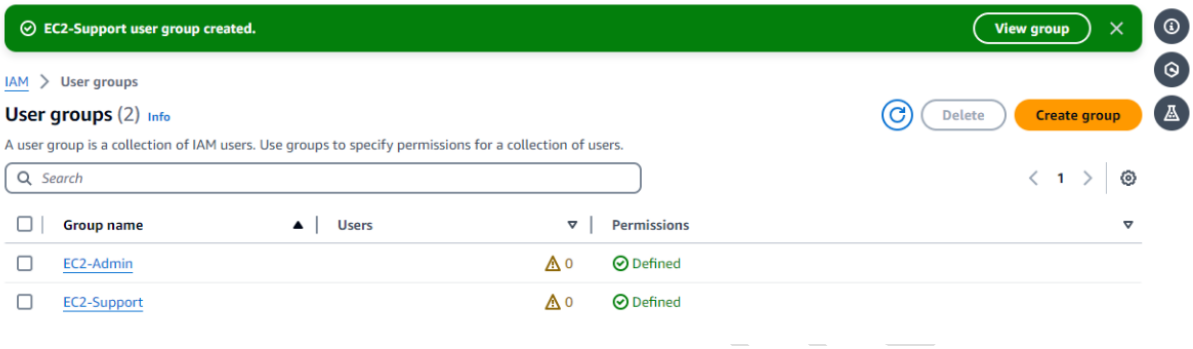
Search | Filter by Type: All types

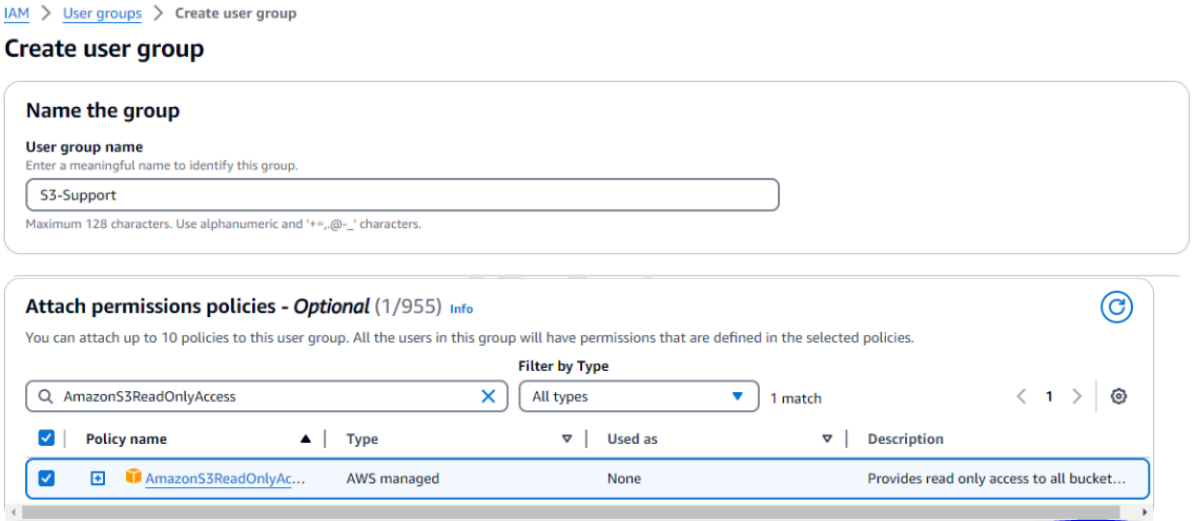
1 2 3 4 5 6 7 ... 62

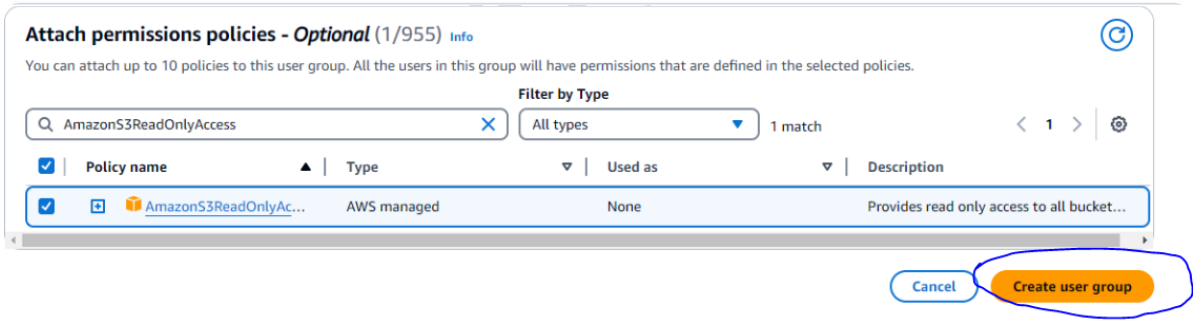
Policy name	Type	Used as	Description
AccessAnalyzerServiceRo...	AWS managed	Permissions policy (1)	Allow Access Analyzer to analyze resou...
AdministratorAccess	AWS managed - job function	Permissions policy (1)	Provides full access to AWS services an...
AdministratorAccess-Am...	AWS managed	Permissions policy (1)	Grants account administrative permiss...
AdministratorAccess-AW...	AWS managed	None	Grants account administrative permiss...

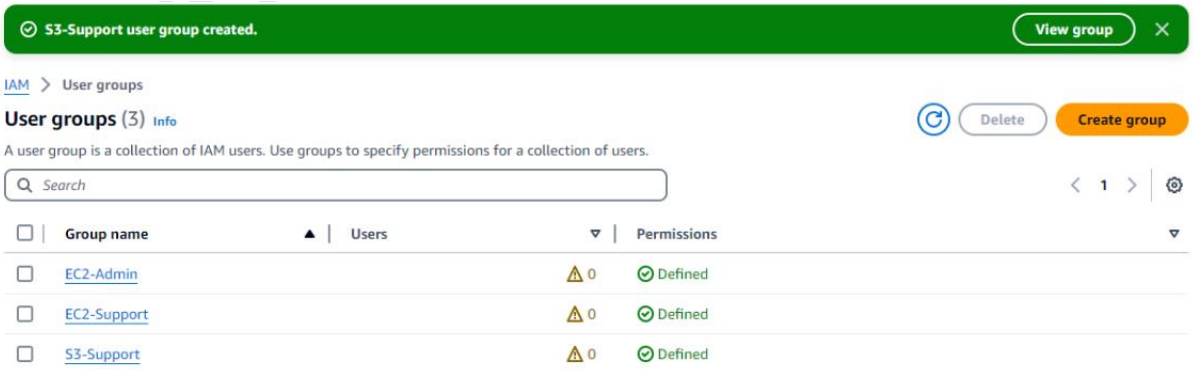

Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
IAM > User groups
User groups (0) Info
A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.
Search
Delete
Create group
Group name
Users
Permissions
No resources to display
IAM > User groups > Create user group
Create user group
Name the group
User group name
Enter a meaningful name to identify this group.
EC2-Admin
Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.
Attach permissions policies - Optional (1/955) Info
You can attach up to 10 policies to this user group. All the users in this group will have permissions that are defined in the selected policies.
Filter by Type
EC2-Admin-Policy
All types
1 match
Policy name
Type
Used as
Description
EC2-Admin-Policy
Customer managed
None
-
Cancel
Create user group
EC2-Admin 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.
Search
Delete
Create group
Group name
Users
Permissions
EC2-Admin
0
Defined
IAM > User groups > Create user group
Create user group
Name the group
User group name
Enter a meaningful name to identify this group.
EC2-Support
Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.

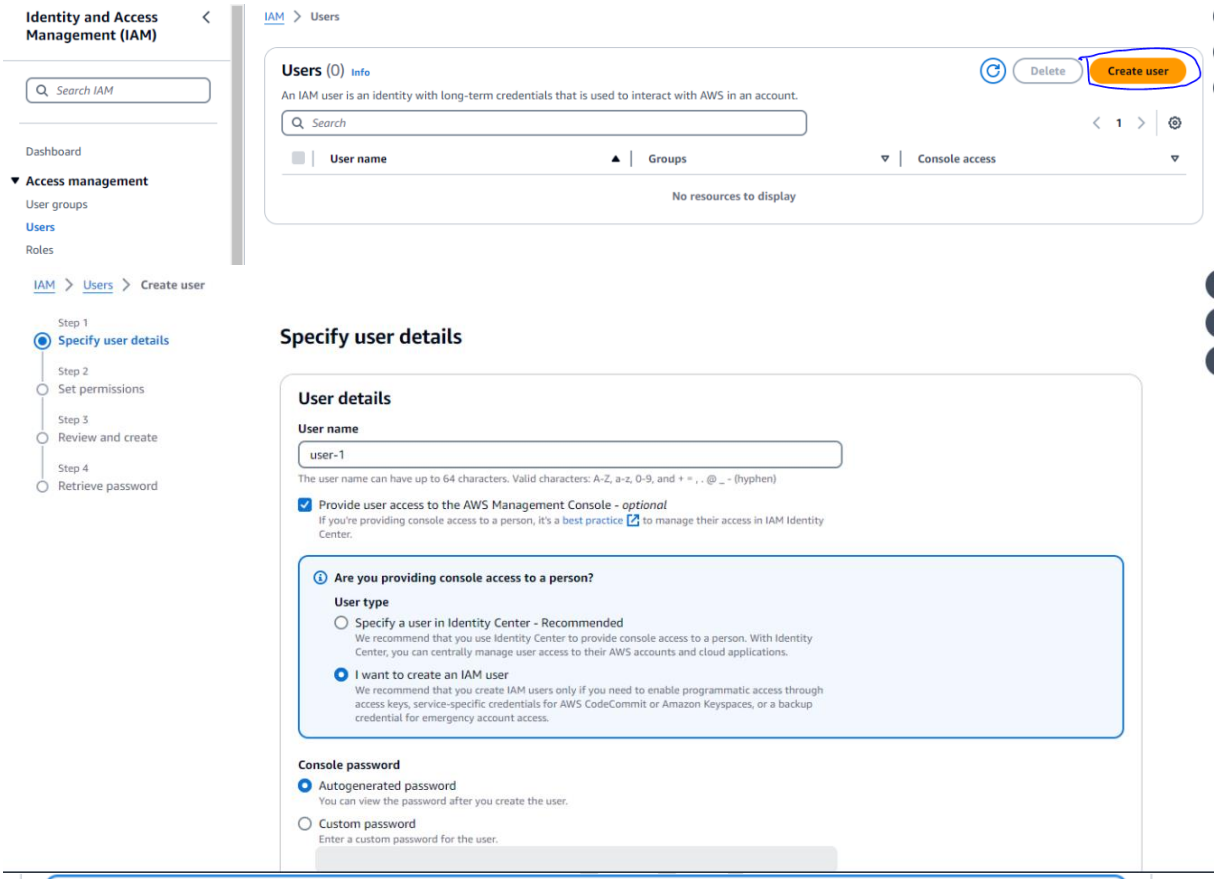

Attach permissions policies - Optional (1/955) Info
You can attach up to 10 policies to this user group. All the users in this group will have permissions that are defined in the selected policies.
Filter by Type
AmazonEC2ReadOnlyAccess
All types
1 match
Policy name
Type
Used as
Description
AmazonEC2ReadOnly...
AWS managed
Permissions policy (1)
Provides read only access to Amazon E...
Cancel
Create user group

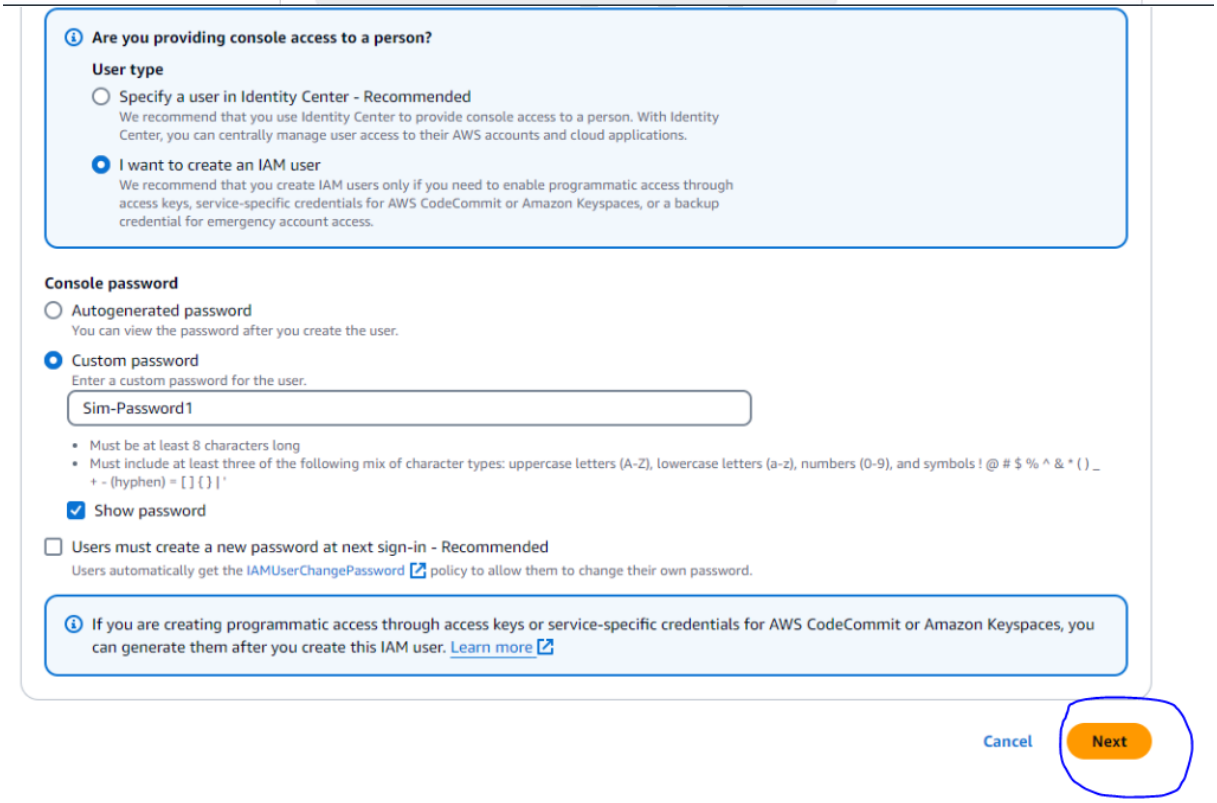

EC2-Support user group created.
View group
IAM > User groups
User groups (2) Info
A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.
Delete
Create group
Search
Group name
Users
Permissions
EC2-Admin
0
Defined
EC2-Support
0
Defined


IAM > User groups > Create user group
Create user group
Name the group
User group name
Enter a meaningful name to identify this group.
S3-Support
Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.


Attach permissions policies - Optional (1/955) Info
You can attach up to 10 policies to this user group. All the users in this group will have permissions that are defined in the selected policies.
Filter by Type
AmazonS3ReadOnlyAccess
All types
1 match
Policy name
Type
Used as
Description
AmazonS3ReadOnlyAc...
AWS managed
None
Provides read only access to all bucket...
Cancel
Create user group


S3-Support user group created.
View group
IAM > User groups
User groups (3) Info
A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.
Delete
Create group
Search
Group name
Users
Permissions
EC2-Admin
0
Defined
EC2-Support
0
Defined
S3-Support
0
Defined


Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
IAM > Users
Users (0) Info
An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.
Delete
Create user
Search
User name
Groups
Console access
No resources to display
IAM > Users > Create user
Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Step 4
Retrieve password
Specify user details
User details
User name
user-1
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.


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.
Sim-Password1
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 or Amazon Keyspaces, you can generate them after you create this IAM user. Learn more
Cancel
Next

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.

User groups (1/3)

Create group

Search

Group name	Users	Attached policies
EC2-Admin	0	EC2-Admin-Policy
EC2-Support	0	AmazonEC2ReadOnlyAccess
S3-Support	0	AmazonS3ReadOnlyAccess

▶ Set permissions boundary - *optional*

Cancel Previous Next

IAM > Users > Create user

Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Step 4
Retrieve password

Review and create

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

User details

User name	Console password type	Require password reset
user-1	Custom password	No

Permissions summary

Name	Type	Used as
S3-Support	Group	Permissions group

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

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 > Create user

Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Step 4
Retrieve password

Retrieve password

You can view and download the user's password below or email users instructions for signing in to the AWS Management Console. This is the only time you can view and download this password.

Console sign-in details

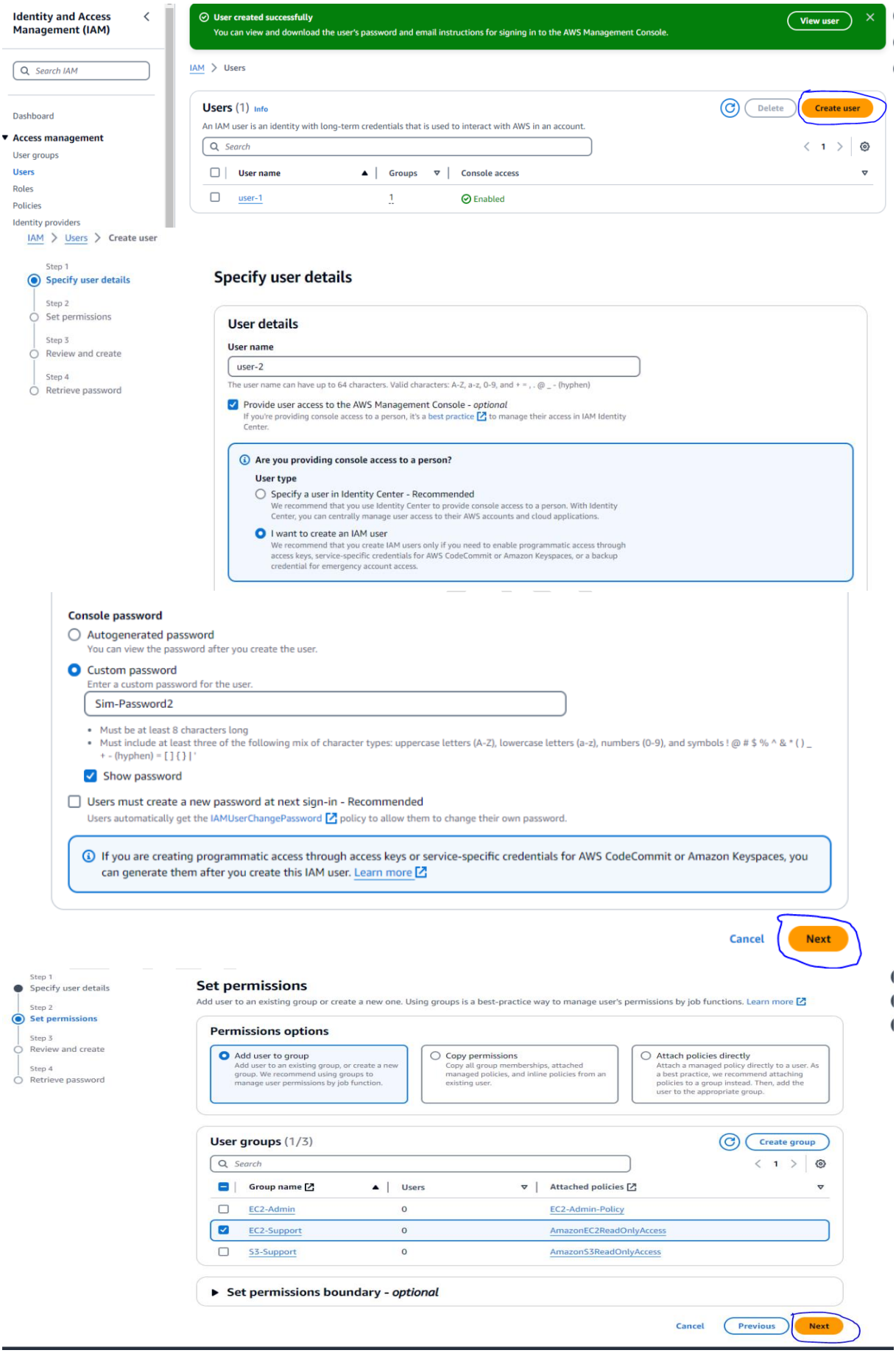
Email sign-in instructions

Console sign-in URL
https://033742928620.signin.aws.amazon.com/console

User name
user-1

Console password
********** Show

Cancel Download .csv file Return to users list


Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
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
An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.
Delete
Create user
Search
User name
Groups
Console access
user-1
1
Enabled
IAM > Users > Create user
Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Step 4
Retrieve password
Specify user details
User details
User name
user-2
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.
Sim-Password2
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 or Amazon Keyspaces, you can generate them after you create this IAM user. Learn more
Cancel
Next
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.
User groups (1/3)
Create group
Search
Group name
Users
Attached policies
EC2-Admin
0
EC2-Admin-Policy
EC2-Support
0
AmazonEC2ReadOnlyAccess
S3-Support
0
AmazonS3ReadOnlyAccess
Set permissions boundary - optional
Cancel
Previous
Next

IAM > Users > Create user

Step 1 Specify user details
Step 2 Set permissions
Step 3 Review and create
Step 4 Retrieve password

Review and create

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

User details

User name	Console password type	Require password reset
user-2	Custom password	No

Permissions summary

Name	Type	Used as
EC2-Support	Group	Permissions group

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

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 > Create user

Step 1 Specify user details
Step 2 Set permissions
Step 3 Review and create
Step 4 Retrieve password

Retrieve password

You can view and download the user's password below or email users instructions for signing in to the AWS Management Console. This is the only time you can view and download this password.

Console sign-in details

Email sign-in instructions

Console sign-in URL
https://033742928620.signin.aws.amazon.com/console

User name
user-2

Console password
********** Show

Cancel | Download .csv file | Return to users list

Continue without viewing or downloading console password?

You haven't viewed or downloaded this user's password. If you continue, you cannot retrieve the password in the future. Instead you must create a new password for the user.

Cancel | Continue

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 (2) Info
An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.
Delete | Create user

Search

User name	Groups	Console access
user-1	1	Enabled
user-2	1	Enabled

IAM > Users > Create user

Step 1 Specify user details
Step 2 Set permissions
Step 3 Review and create
Step 4 Retrieve password

Specify user details

User details

User name
user-3
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.
Sim-Password3
- 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 or Amazon Keyspaces, you can generate them after you create this IAM user. Learn more

Cancel | Next

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.

User groups (3)

Create group

Search

Group name	Users	Attached policies
EC2-Admin	0	EC2-Admin-Policy
EC2-Support	0	AmazonEC2ReadOnlyAccess
S3-Support	0	AmazonS3ReadOnlyAccess

▶ Set permissions boundary - *optional*

Cancel | Previous | Next

Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Step 4
Retrieve password

Review and create

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

User details

User name	Console password type	Require password reset
user-3	Custom password	No

Permissions summary

Name	Type	Used as
No resources		

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

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 > Create user

Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Step 4
Retrieve password

Retrieve password

You can view and download the user's password below or email users instructions for signing in to the AWS Management Console. This is the only time you can view and download this password.

Console sign-in details

Email sign-in instructions

Console sign-in URL
https://033742928620.signin.aws.amazon.com/console

User name
user-3

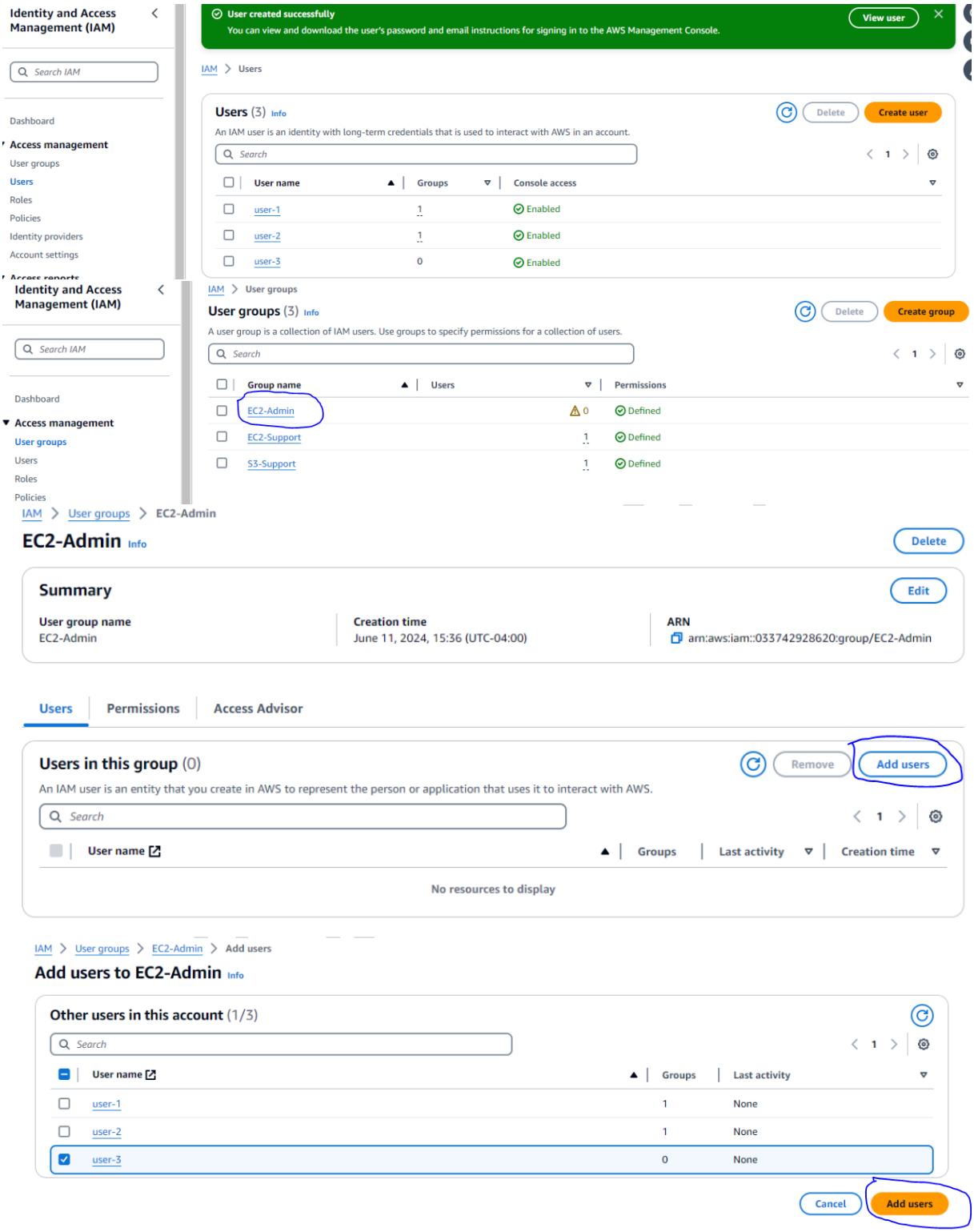
Console password
********** Show

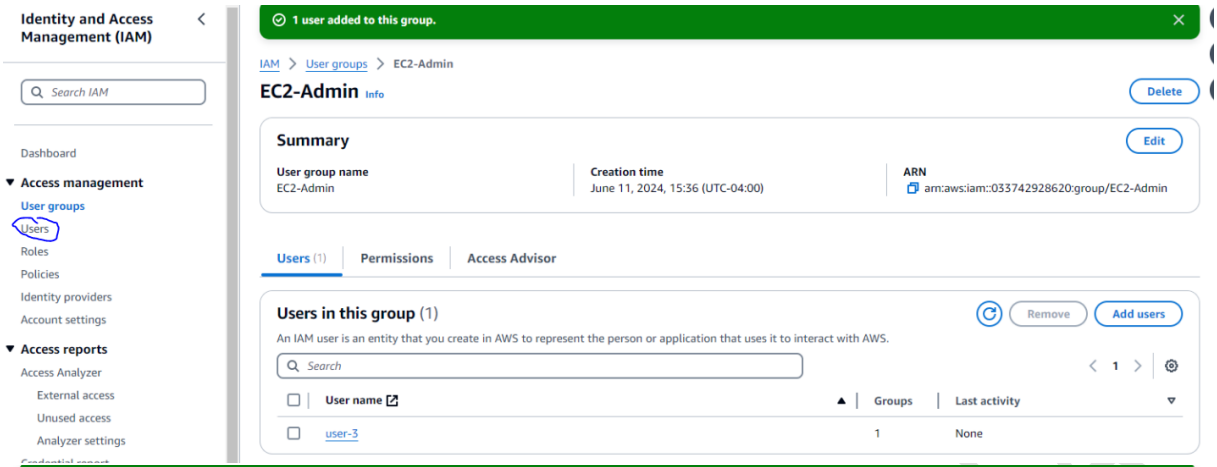
Cancel | Download .csv file | Return to users list

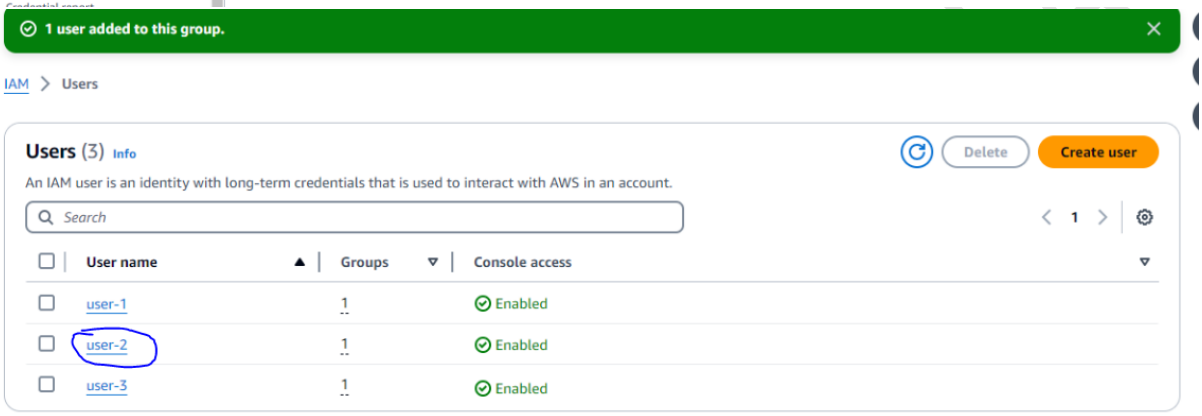
Continue without viewing or downloading console password?

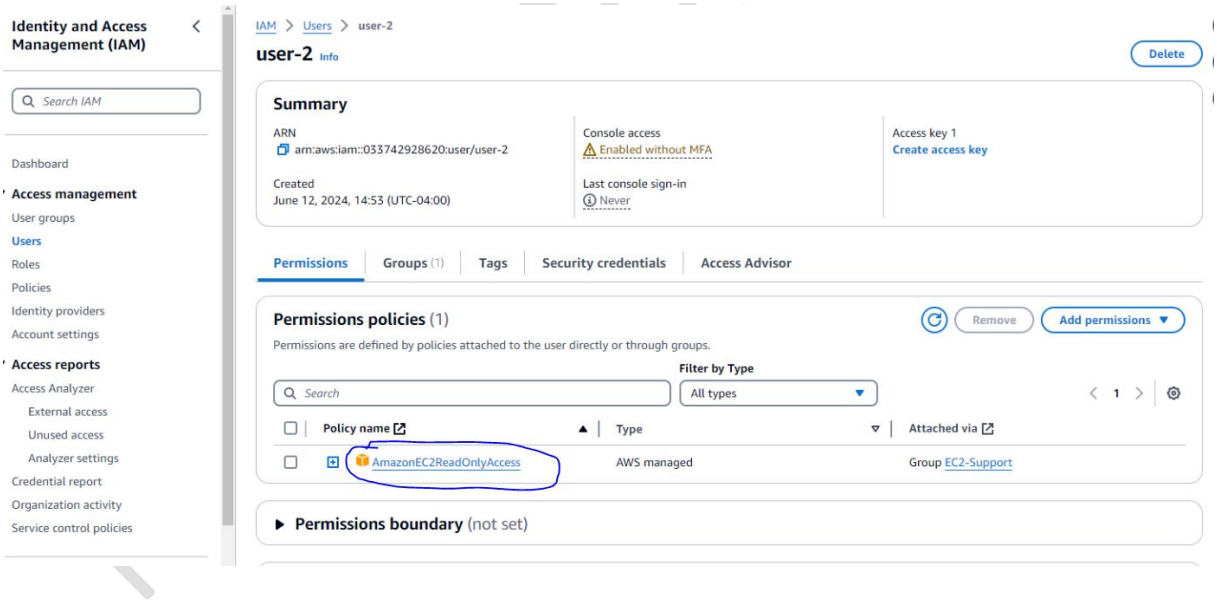
You haven't viewed or downloaded this user's password. If you continue, you cannot retrieve the password in the future. Instead you must create a new password for the user.

Cancel | Continue


Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
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 (3) Info
An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.
Delete
Create user
Search
User name
Groups
Console access
user-1
1
Enabled
user-2
1
Enabled
user-3
0
Enabled
IAM > User groups
User groups (3) Info
A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.
Create group
Group name
Users
Permissions
EC2-Admin
0
Defined
EC2-Support
1
Defined
S3-Support
1
Defined
IAM > User groups > EC2-Admin
EC2-Admin Info
Delete
Summary
Edit
User group name
EC2-Admin
Creation time
June 11, 2024, 15:36 (UTC-04:00)
ARN
arn:aws:iam::033742928620:group/EC2-Admin
Users
Permissions
Access Advisor
Users in this group (0)
An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.
Remove
Add users
User name
Groups
Last activity
Creation time
No resources to display
IAM > User groups > EC2-Admin > Add users
Add users to EC2-Admin Info
Other users in this account (1/3)
User name
Groups
Last activity
user-1
1
None
user-2
1
None
user-3
0
None
Cancel
Add users


Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access Analyzer
External access
Unused access
Analyzer settings
1 user added to this group.
IAM > User groups > EC2-Admin
EC2-Admin Info
Delete
Summary
Edit
User group name
EC2-Admin
Creation time
June 11, 2024, 15:36 (UTC-04:00)
ARN
arn:aws:iam::033742928620:group/EC2-Admin
Users (1)
Permissions
Access Advisor
Users in this group (1)
Remove
Add users
An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.
Search
User name
Groups
Last activity
user-3
1
None


1 user added to this group.
IAM > Users
Users (3) Info
Delete
Create user
An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.
Search
User name
Groups
Console access
user-1
1
Enabled
user-2
1
Enabled
user-3
1
Enabled


Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access Analyzer
External access
Unused access
Analyzer settings
Credential report
Organization activity
Service control policies
IAM > Users > user-2
user-2 Info
Delete
Summary
ARN
arn:aws:iam::033742928620:user/user-2
Created
June 12, 2024, 14:53 (UTC-04:00)
Console access
Enabled without MFA
Last console sign-in
Never
Access key 1
Create access key
Permissions
Groups (1)
Tags
Security credentials
Access Advisor
Permissions policies (1)
Remove
Add permissions
Permissions are defined by policies attached to the user directly or through groups.
Filter by Type
Search
All types
Policy name
Type
Attached via
AmazonEC2ReadOnlyAccess
AWS managed
Group EC2-Support
Permissions boundary (not set)

IAM > Policies > AmazonEC2ReadOnlyAccess

AmazonEC2ReadOnlyAccess Info

Provides read only access to Amazon EC2 via the AWS Management Console.

Policy details

Type	Creation time	Edited time	ARN
AWS managed	February 06, 2015, 13:40 (UTC-05:00)	February 14, 2024, 13:43 (UTC-05:00)	arn:aws:iam::aws:policy/AmazonEC2ReadOnlyAccess

Permissions | Entities attached | Policy versions (2) | Access Advisor

Permissions defined in this policy Info

Summary | JSON

Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it

Search

Allow (5 of 416 services)

Show remaining 411 services

Service	Access level	Resource	Request condition
CloudWatch	Limited: List, Read	All resources	None
EC2	Limited: List	All resources	None
EC2 Auto Scaling	Full: Read Limited: List	All resources	None
ELB	Full: List, Read	All resources	None

user-2 | IAM | Global | AmazonEC2ReadOnlyAccess |

us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/policies/details/arn%3Aaws%3Aiam%3A%3Aaws%3Apolicy%2FAmazonEC2ReadOnlyAccess?section=permissions&view=...

Services | Search [Alt+S] | Global

Identity and Access Management (IAM)

Search IAM

- Dashboard
- Access management
  - User groups
  - Users
  - Roles
  - Policies
  - Identity providers
  - Account settings
- Access reports
  - Access Analyzer
    - External access
    - Unused access
    - Analyzer settings
  - Credential report
  - Organization activity
  - Service control policies

Policy details

Type	Creation time	Edited time	ARN
AWS managed	February 06, 2015, 13:40 (UTC-05:00)	February 14, 2024, 13:43 (UTC-05:00)	arn:aws:iam::aws:policy/AmazonEC2ReadOnlyAccess

Permissions | Entities attached | Policy versions (2) | Access Advisor

Permissions defined in this policy Info

Copy | Summary | JSON

Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:Describe*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "elasticloadbalancing:Describe*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "cloudwatch:ListMetrics",
                "cloudwatch:GetMetricStatistics",
                "cloudwatch:Describe*"
            ],
```

Identity and Access Management (IAM)

Search IAM

- Dashboard
- Access management
  - User groups
  - Users
  - Roles
  - Policies
  - Identity providers
  - Account settings

IAM > Users

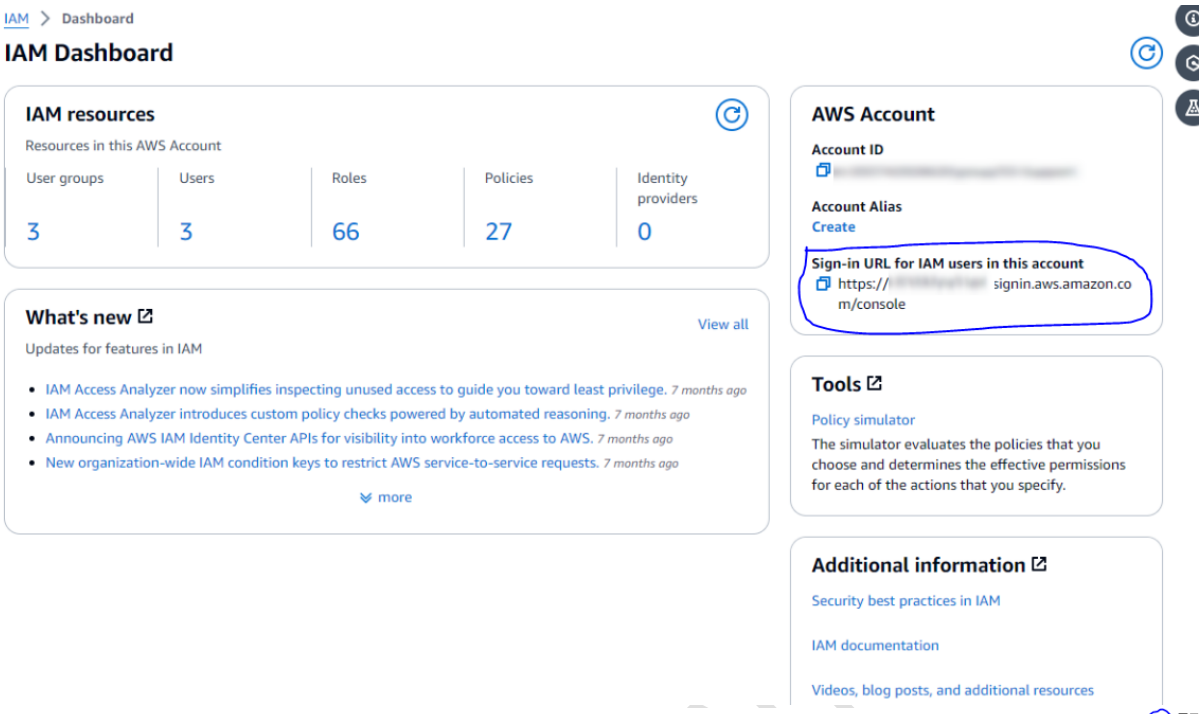
Users (3) Info

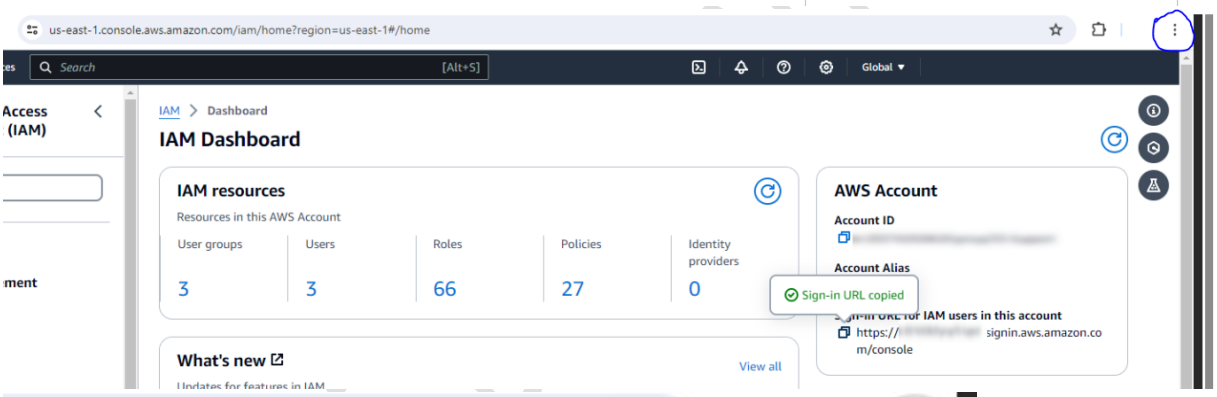
Delete | Create user

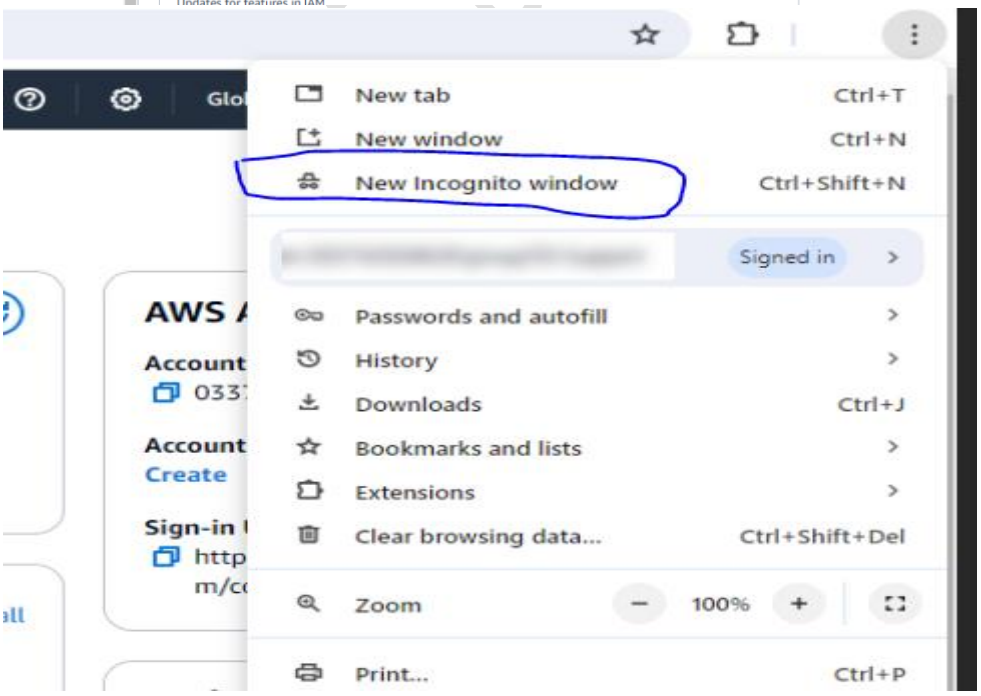
An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

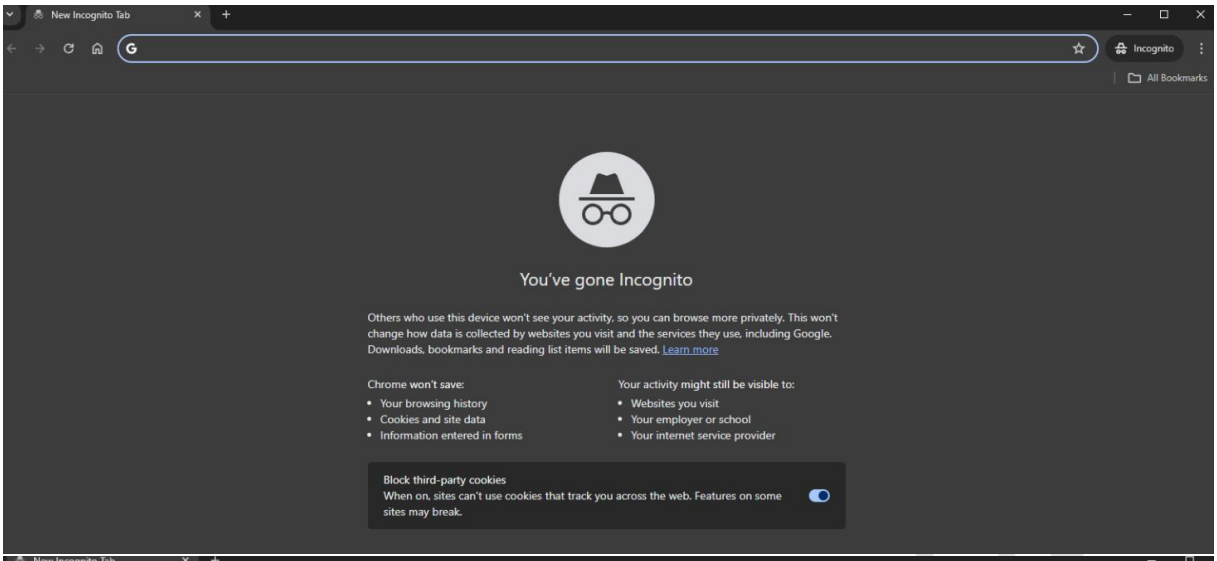
Search

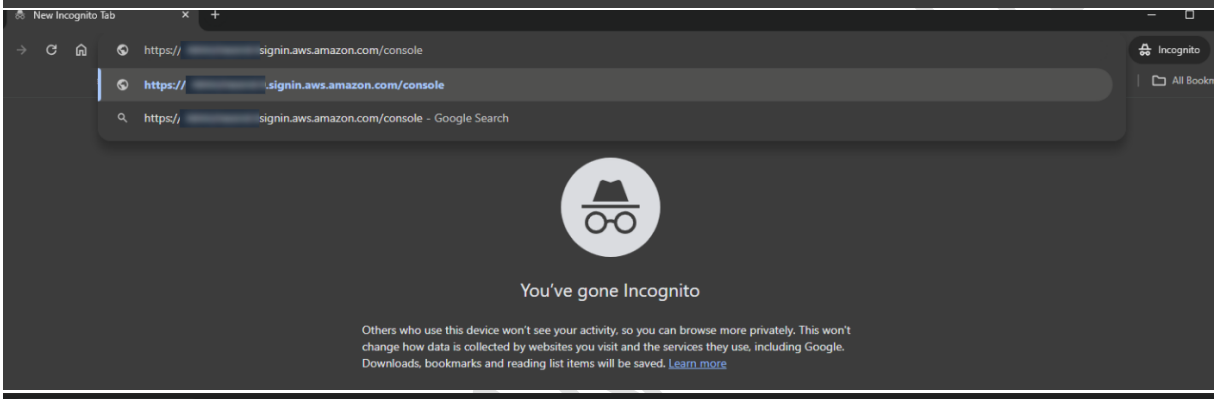
User name	Groups	Console access
user-1	1	Enabled
user-2	1	Enabled
user-3	1	Enabled

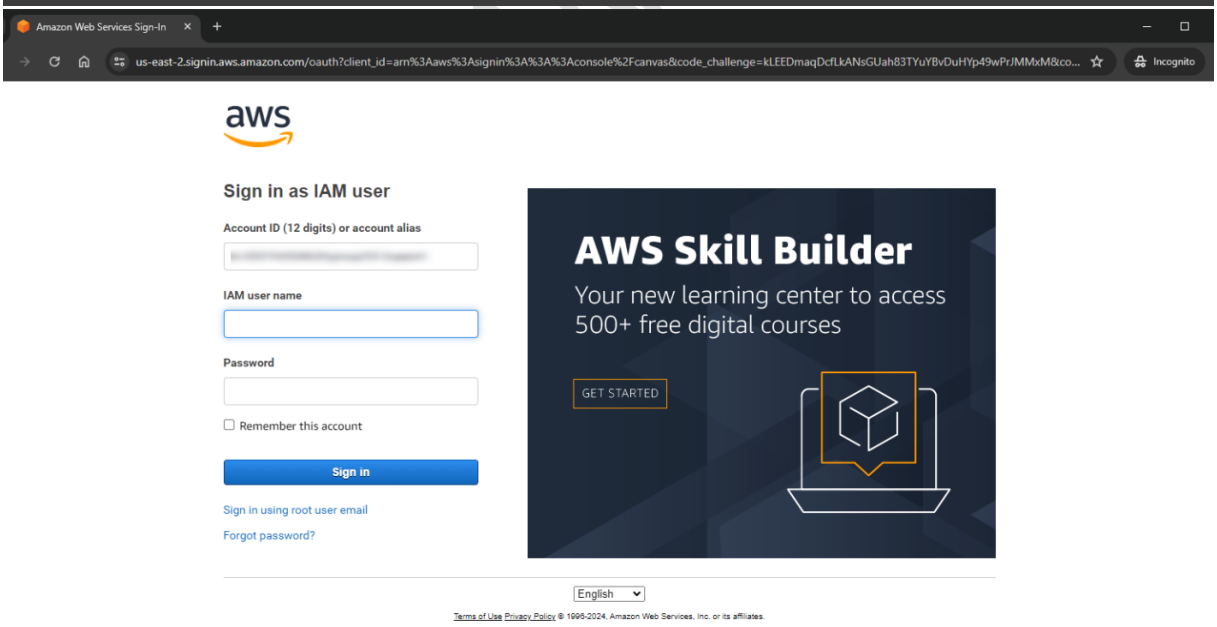

IAM > Dashboard
IAM Dashboard
IAM resources
Resources in this AWS Account
User groups
3
Users
3
Roles
66
Policies
27
Identity providers
0
AWS Account
Account ID
Account Alias
Create
Sign-in URL for IAM users in this account
https:// signin.aws.amazon.com/console
What's new
View all
Updates for features in IAM
IAM Access Analyzer now simplifies inspecting unused access to guide you toward least privilege. 7 months ago
IAM Access Analyzer introduces custom policy checks powered by automated reasoning. 7 months ago
Announcing AWS IAM Identity Center APIs for visibility into workforce access to AWS. 7 months ago
New organization-wide IAM condition keys to restrict AWS service-to-service requests. 7 months ago
more
Tools
Policy simulator
The simulator evaluates the policies that you choose and determines the effective permissions for each of the actions that you specify.
Additional information
Security best practices in IAM
IAM documentation
Videos, blog posts, and additional resources

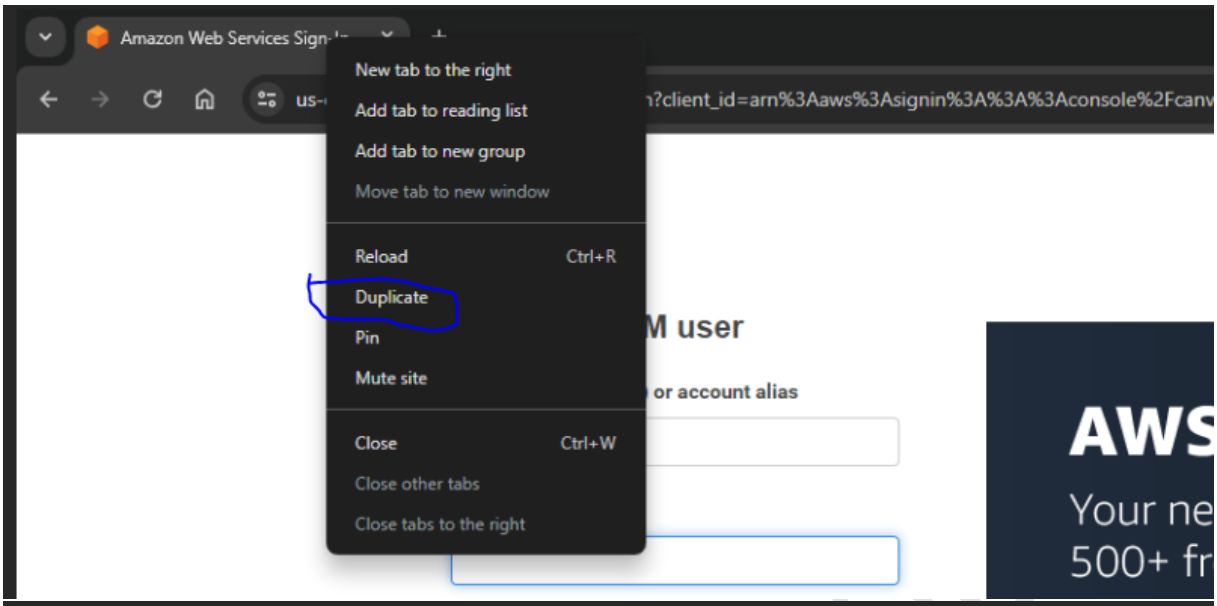

us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/home
Search
[Alt+S]
Global
IAM > Dashboard
IAM Dashboard
IAM resources
Resources in this AWS Account
User groups
3
Users
3
Roles
66
Policies
27
Identity providers
0
AWS Account
Account ID
Account Alias
Sign-in URL copied
https:// signin.aws.amazon.com/console
What's new
View all

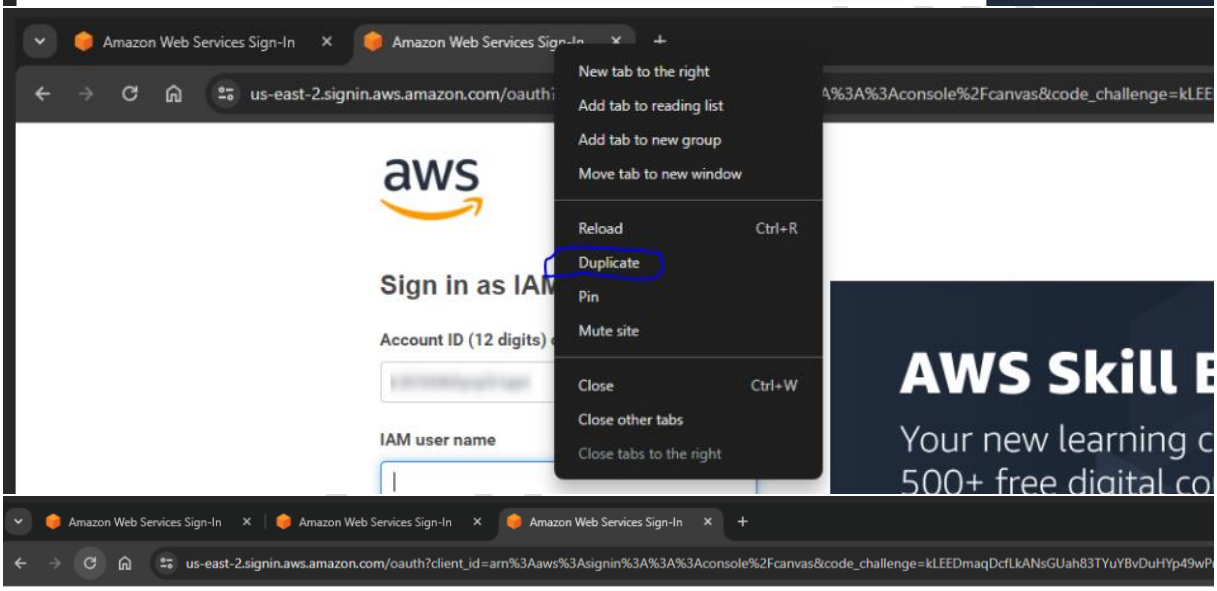

New tab Ctrl+T
New window Ctrl+N
New Incognito window Ctrl+Shift+N
Signed in
Passwords and autofill
History
Downloads Ctrl+J
Bookmarks and lists
Extensions
Clear browsing data... Ctrl+Shift+Del
Zoom 100%
Print... Ctrl+P

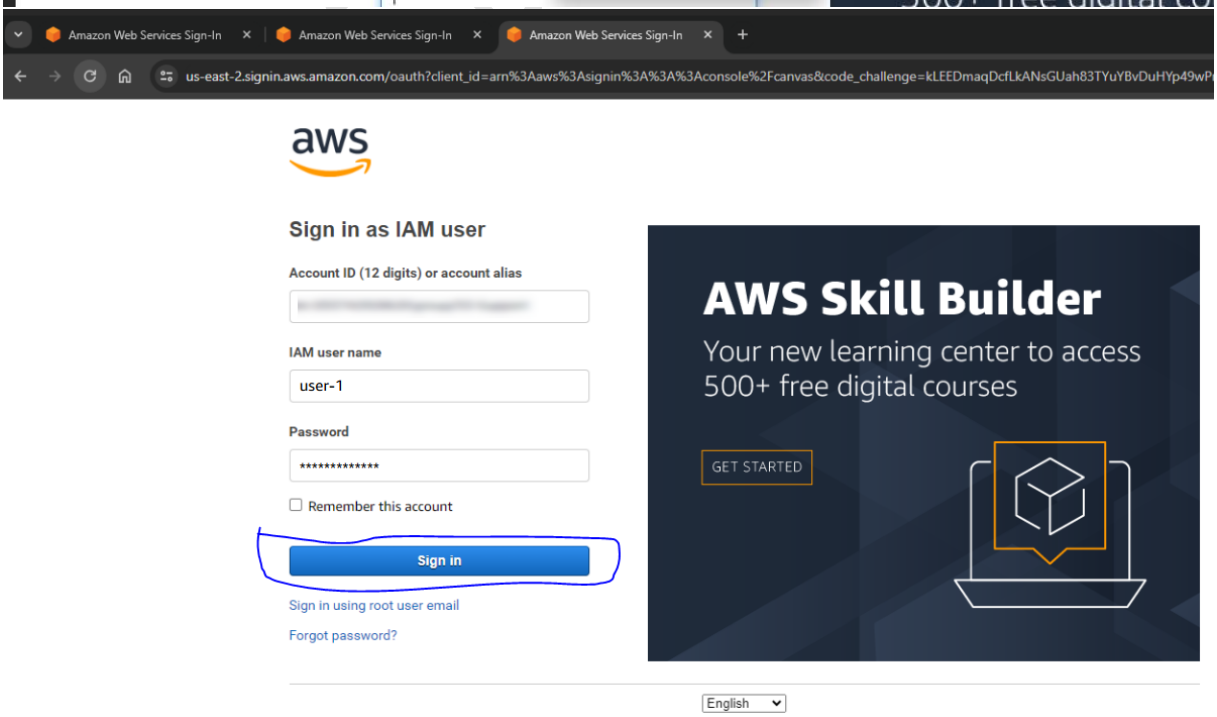

New Incognito Tab
Incognito
All Bookmarks
You've gone Incognito
Others who use this device won't see your activity, so you can browse more privately. This won't change how data is collected by websites you visit and the services they use, including Google. Downloads, bookmarks and reading list items will be saved. Learn more
Chrome won't save:
Your browsing history
Cookies and site data
Information entered in forms
Your activity might still be visible to:
Websites you visit
Your employer or school
Your internet service provider
Block third-party cookies
When on, sites can't use cookies that track you across the web. Features on some sites may break.

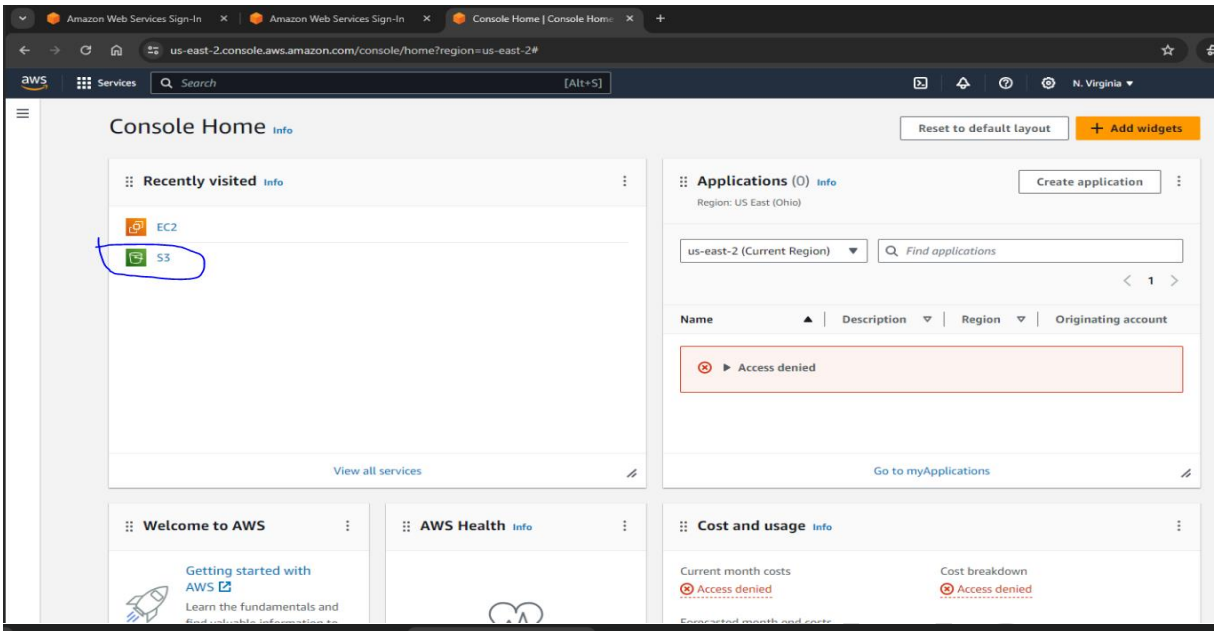

New Incognito Tab
https:// signin.aws.amazon.com/console
https:// .signin.aws.amazon.com/console
https:// signin.aws.amazon.com/console - Google Search
Incognito
You've gone Incognito
Others who use this device won't see your activity, so you can browse more privately. This won't change how data is collected by websites you visit and the services they use, including Google. Downloads, bookmarks and reading list items will be saved. Learn more

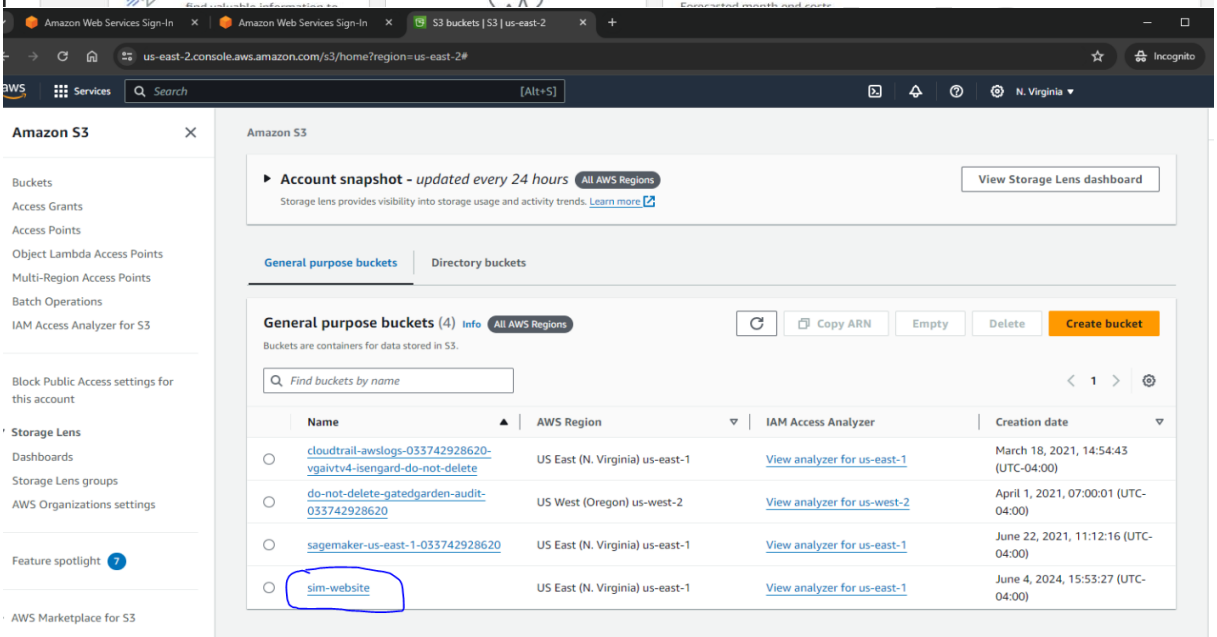

Amazon Web Services Sign-In
us-east-2.signin.aws.amazon.com/oauth?client_id=arn%3Aaws%3Asignin%3A%3A%3Aconsole%2Fcanvas&code_challenge=kLEEDmaqDcfLkANsGUah83TYuYBvDuHYp49wPrJMMxM&co...
Incognito
aws
Sign in as IAM user
Account ID (12 digits) or account alias
IAM user name
Password
Remember this account
Sign in
Sign in using root user email
Forgot password?
AWS Skill Builder
Your new learning center to access 500+ free digital courses
GET STARTED
English
Terms of Use Privacy Policy © 1996-2024, Amazon Web Services, Inc. or its affiliates.

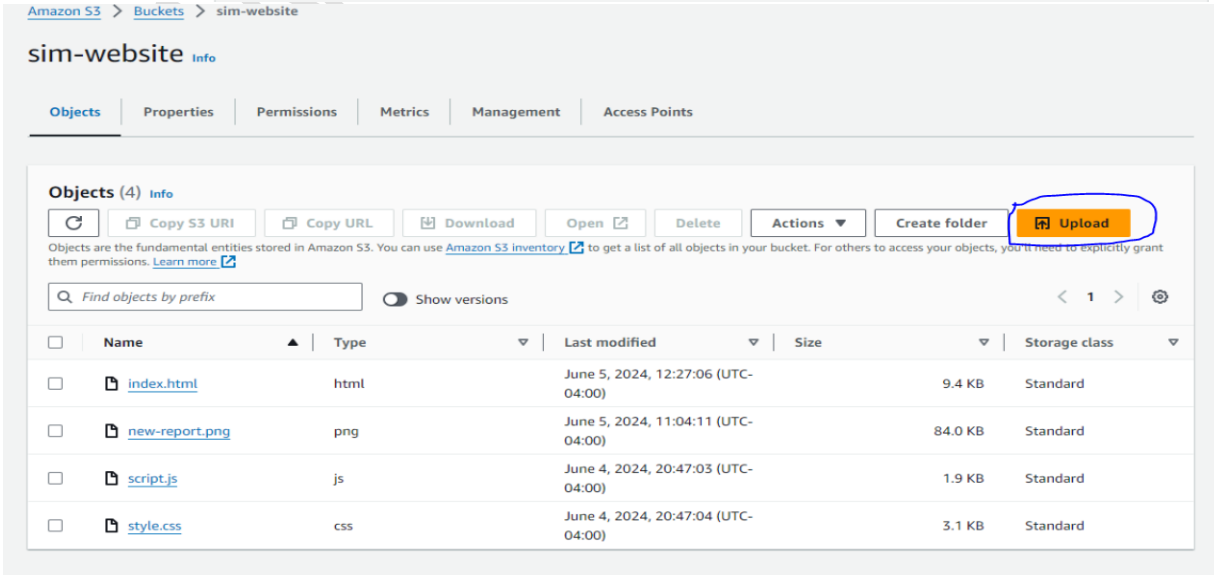

Amazon Web Services Sign-In
New tab to the right
Add tab to reading list
Add tab to new group
Move tab to new window
Reload Ctrl+R
Duplicate
Pin
Mute site
Close Ctrl+W
Close other tabs
Close tabs to the right
M user
or account alias
AWS
Your ne
500+ fr

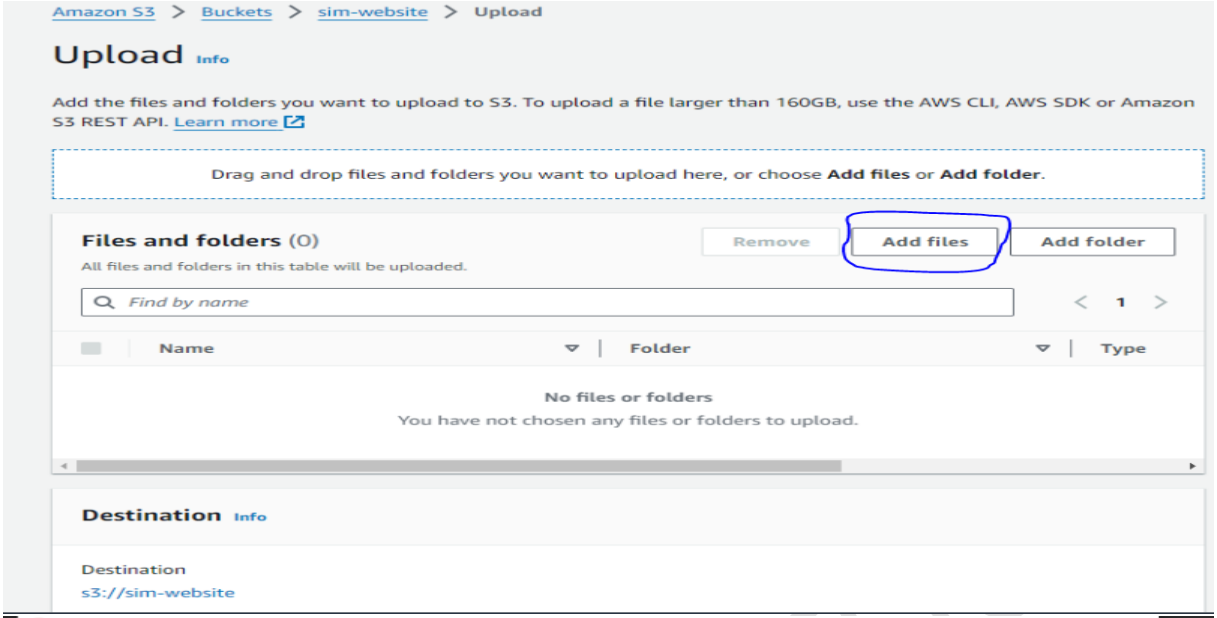

Amazon Web Services Sign-In
Amazon Web Services Sign-In
us-east-2.signin.aws.amazon.com/oauth
New tab to the right
Add tab to reading list
Add tab to new group
Move tab to new window
Reload Ctrl+R
Duplicate
Pin
Mute site
Close Ctrl+W
Close other tabs
Close tabs to the right
aws
Sign in as IAM
Account ID (12 digits)
IAM user name
AWS Skill B
Your new learning c
500+ free digital co

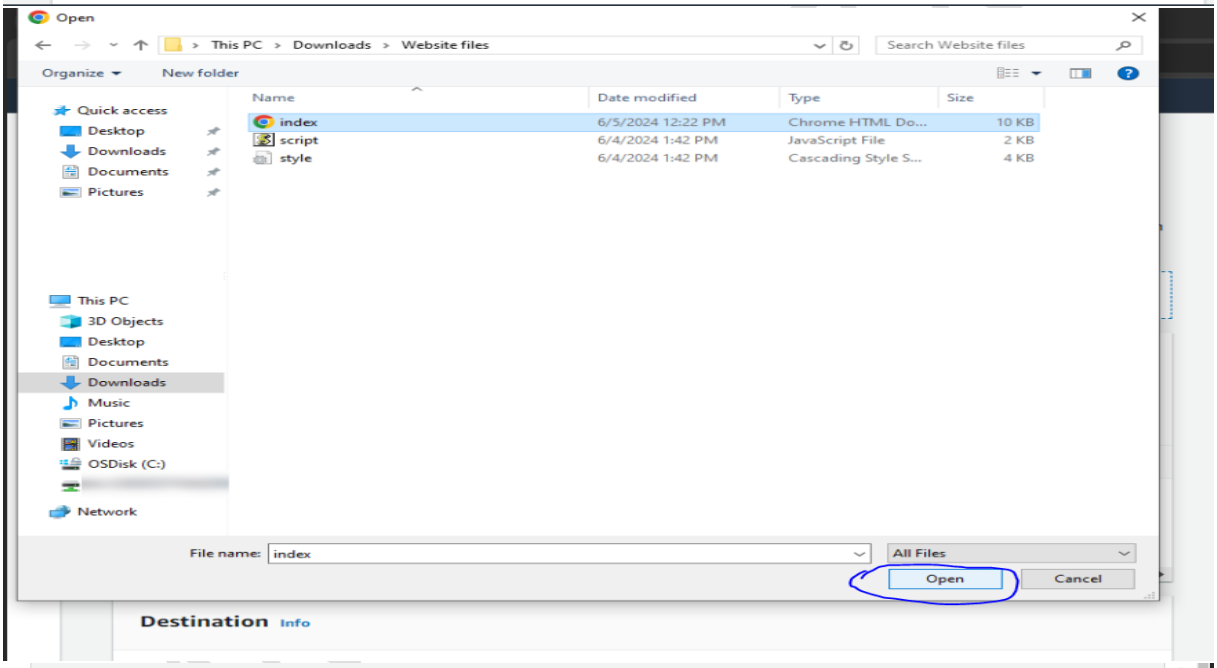

Amazon Web Services Sign-In
Amazon Web Services Sign-In
Amazon Web Services Sign-In
us-east-2.signin.aws.amazon.com/oauth?client_id=arn%3Aaws%3Asignin%3A%3A%3Aconsole%2Fcanvas&code_challenge=kLEEDmaqDcfLkANsGUah83TYuYBvDuHYp49wP
aws
Sign in as IAM user
Account ID (12 digits) or account alias
IAM user name
user-1
Password
Remember this account
Sign in
Sign in using root user email
Forgot password?
AWS Skill Builder
Your new learning center to access
500+ free digital courses
GET STARTED
English

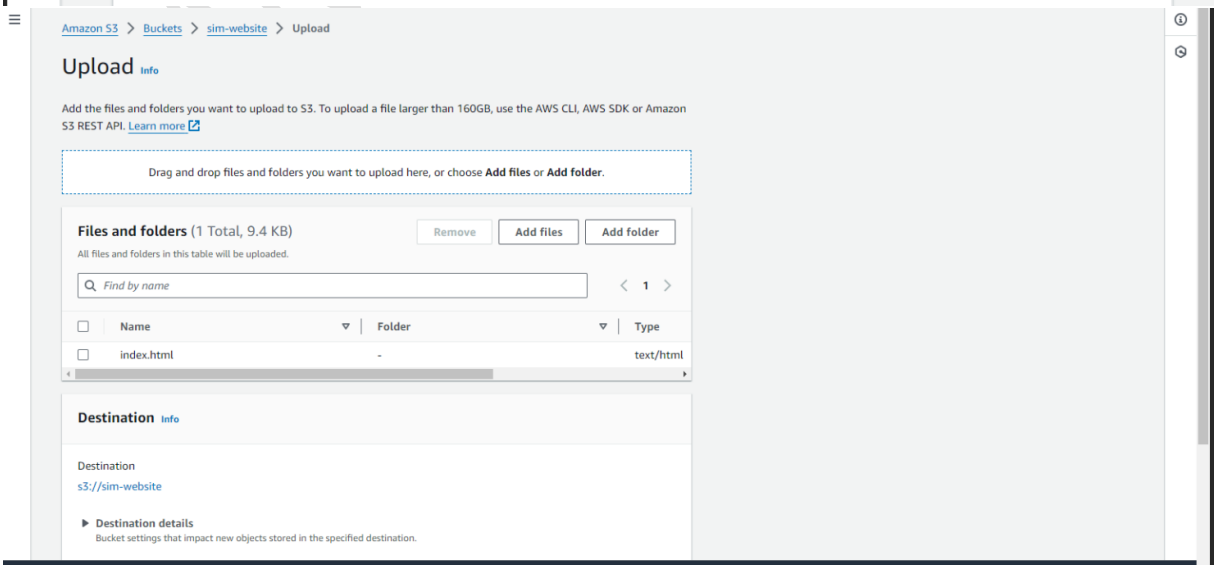

Console Home Info
Reset to default layout
+ Add widgets
Recently visited Info
EC2
S3
View all services
Applications (0) Info
Region: US East (Ohio)
Create application
us-east-2 (Current Region)
Find applications
Name
Description
Region
Originating account
Access denied
Go to myApplications
Welcome to AWS
Getting started with AWS
Learn the fundamentals and
AWS Health Info
Cost and usage Info
Current month costs
Access denied
Cost breakdown
Access denied

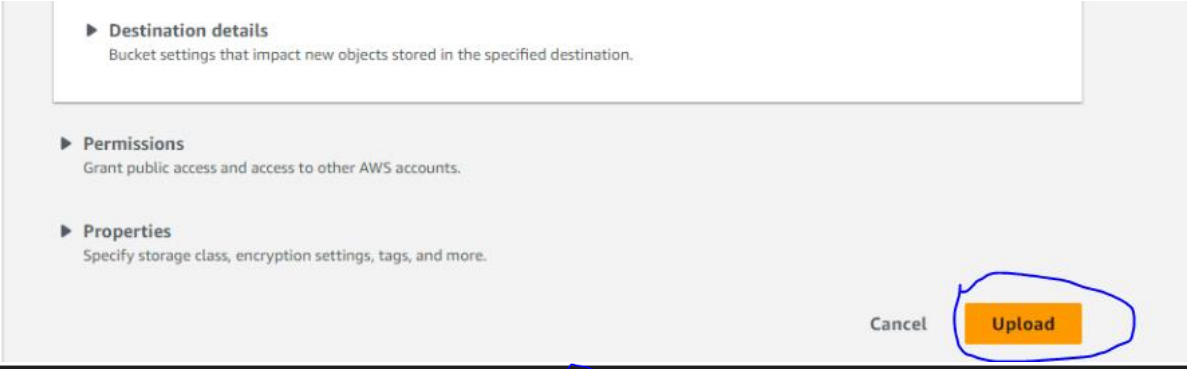

Amazon S3
Buckets
Access Grants
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
Storage Lens groups
AWS Organizations settings
Feature spotlight 7
AWS Marketplace for S3
Account snapshot - updated every 24 hours
All AWS Regions
Storage lens provides visibility into storage usage and activity trends. Learn more
View Storage Lens dashboard
General purpose buckets
Directory buckets
General purpose buckets (4) Info
All AWS Regions
Buckets are containers for data stored in S3.
Copy ARN
Empty
Delete
Create bucket
Find buckets by name
Name
AWS Region
IAM Access Analyzer
Creation date
cloudtrail-awslogs-033742928620-vgaivtv4-isengard-do-not-delete
US East (N. Virginia) us-east-1
View analyzer for us-east-1
March 18, 2021, 14:54:43 (UTC-04:00)
do-not-delete-gatedgarden-audit-033742928620
US West (Oregon) us-west-2
View analyzer for us-west-2
April 1, 2021, 07:00:01 (UTC-04:00)
sagemaker-us-east-1-033742928620
US East (N. Virginia) us-east-1
View analyzer for us-east-1
June 22, 2021, 11:12:16 (UTC-04:00)
sim-website
US East (N. Virginia) us-east-1
View analyzer for us-east-1
June 4, 2024, 15:53:27 (UTC-04:00)

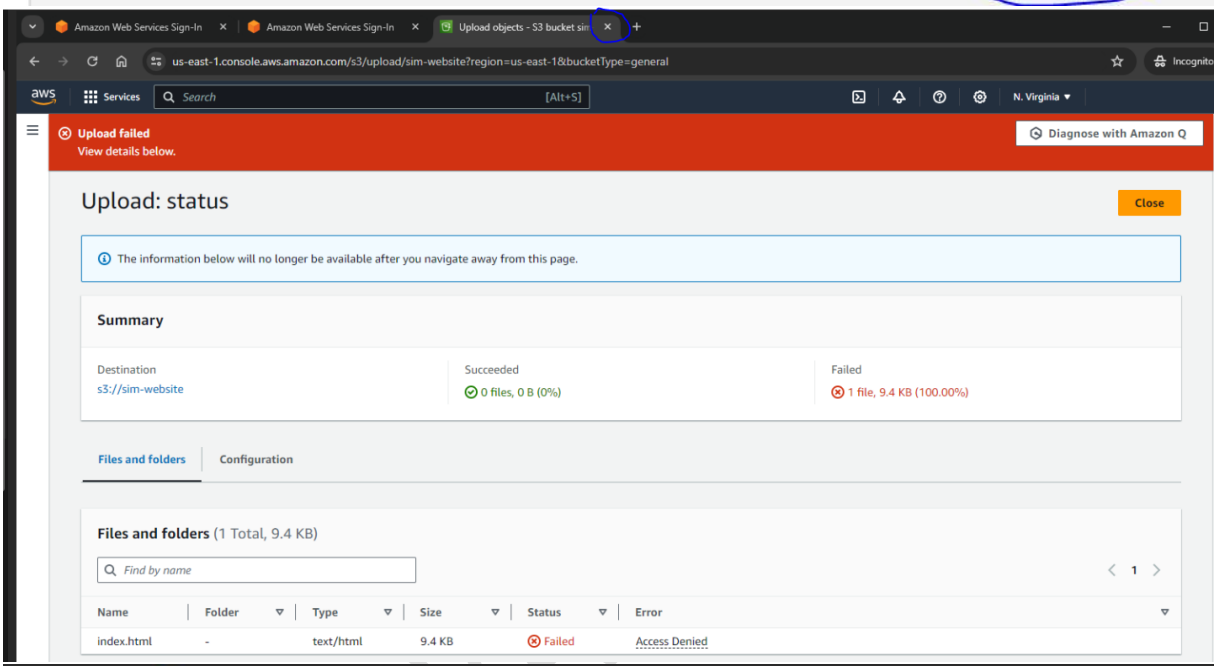

Amazon S3 > Buckets > sim-website
sim-website Info
Objects
Properties
Permissions
Metrics
Management
Access Points
Objects (4) Info
Copy S3 URI
Copy URL
Download
Open
Delete
Actions
Create folder
Upload
Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more
Find objects by prefix
Show versions
Name
Type
Last modified
Size
Storage class
index.html
html
June 5, 2024, 12:27:06 (UTC-04:00)
9.4 KB
Standard
new-report.png
png
June 5, 2024, 11:04:11 (UTC-04:00)
84.0 KB
Standard
script.js
js
June 4, 2024, 20:47:03 (UTC-04:00)
1.9 KB
Standard
style.css
css
June 4, 2024, 20:47:04 (UTC-04:00)
3.1 KB
Standard

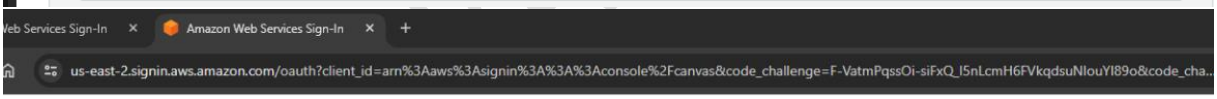

Amazon S3 > Buckets > sim-website > Upload
Upload Info
Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDK or Amazon S3 REST API. Learn more
Drag and drop files and folders you want to upload here, or choose Add files or Add folder.
Files and folders (0)
All files and folders in this table will be uploaded.
Remove
Add files
Add folder
Find by name
Name
Folder
Type
No files or folders
You have not chosen any files or folders to upload.
Destination Info
Destination
s3://sim-website

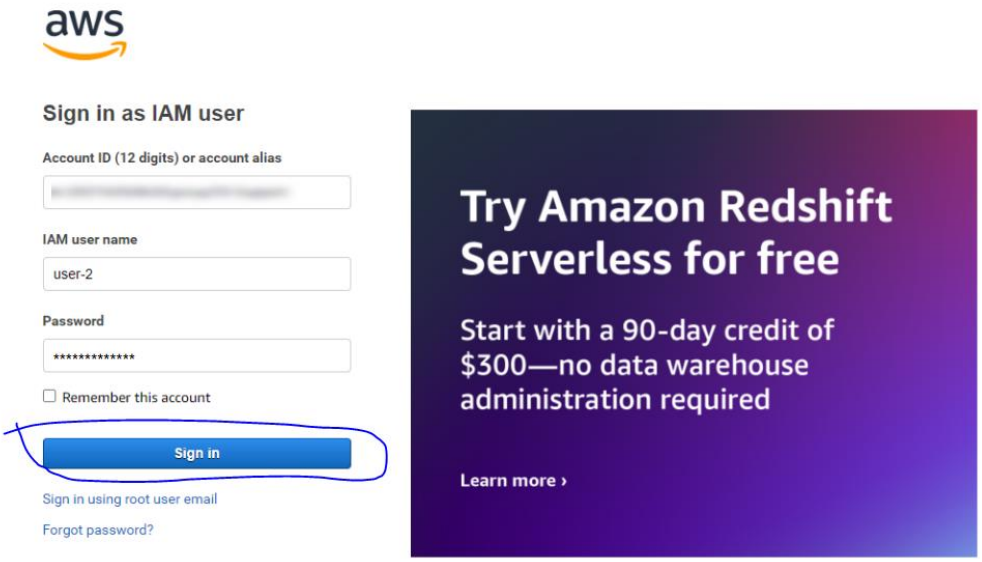

Open
This PC > Downloads > Website files
Search Website files
Organize
New folder
Quick access
Desktop
Downloads
Documents
Pictures
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
OSDisk (C:)
Network
Name
Date modified
Type
Size
index
6/5/2024 12:22 PM
Chrome HTML Do...
10 KB
script
6/4/2024 1:42 PM
JavaScript File
2 KB
style
6/4/2024 1:42 PM
Cascading Style S...
4 KB
File name: index
All Files
Open
Cancel
Destination Info

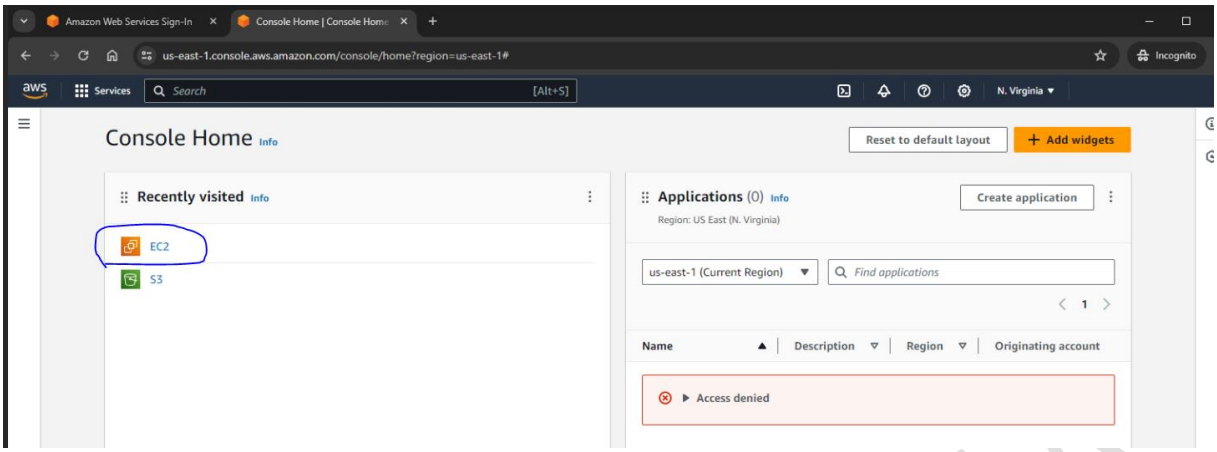

Amazon S3 > Buckets > sim-website > Upload
Upload Info
Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDK or Amazon S3 REST API. Learn more
Drag and drop files and folders you want to upload here, or choose Add files or Add folder.
Files and folders (1 Total, 9.4 KB)
All files and folders in this table will be uploaded.
Remove
Add files
Add folder
Find by name
Name
Folder
Type
index.html
-
text/html
Destination Info
Destination
s3://sim-website
Destination details
Bucket settings that impact new objects stored in the specified destination.

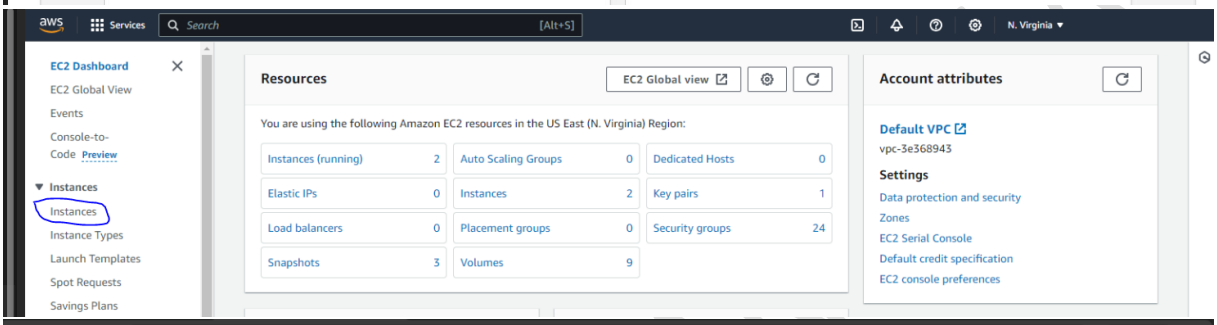

Destination details
Bucket settings that impact new objects stored in the specified destination.
Permissions
Grant public access and access to other AWS accounts.
Properties
Specify storage class, encryption settings, tags, and more.
Cancel
Upload

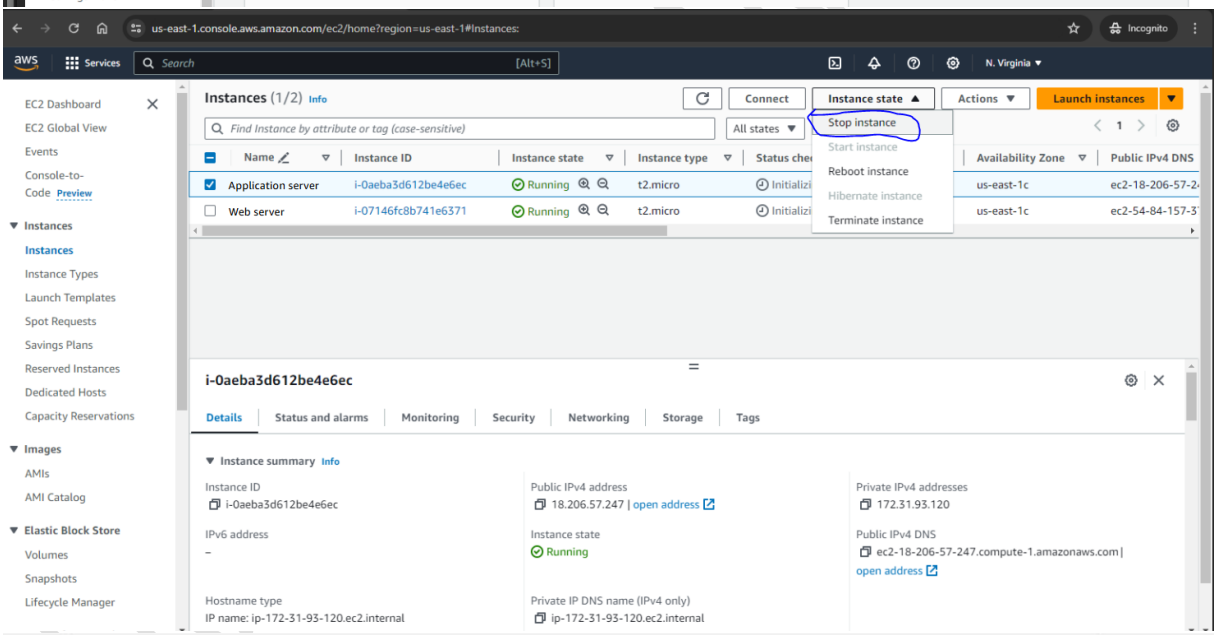

Amazon Web Services Sign-In
Upload objects - S3 bucket sim
us-east-1.console.aws.amazon.com/s3/upload/sim-website?region=us-east-1&bucketType=general
Services
Search
[Alt+S]
N. Virginia
Upload failed
View details below.
Diagnose with Amazon Q
Upload: status
Close
The information below will no longer be available after you navigate away from this page.
Summary
Destination
s3://sim-website
Succeeded
0 files, 0 B (0%)
Failed
1 file, 9.4 KB (100.00%)
Files and folders
Configuration
Files and folders (1 Total, 9.4 KB)
Find by name
Name
Folder
Type
Size
Status
Error
index.html
-
text/html
9.4 KB
Failed
Access Denied


Amazon Web Services Sign-In
us-east-2.signin.aws.amazon.com/oauth?client_id=arn%3Aaws%3Asignin%3A%3A%3Aconsole%2Fcanvas&code_challenge=F-VatmPqssOi-siFxQ_I5nLcmH6FVkqdsuNlouYI89o&code_cha...

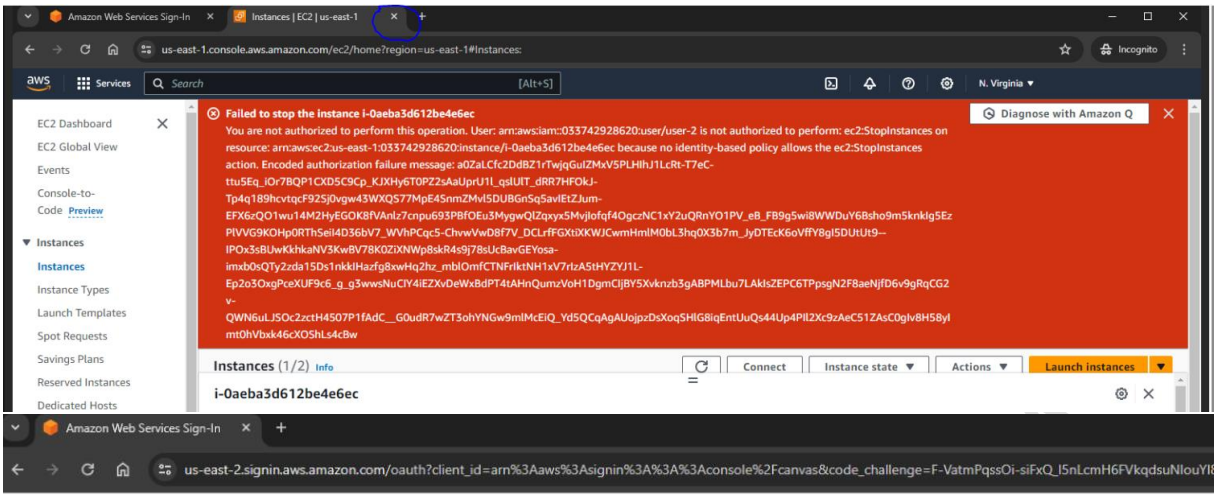

aws
Sign in as IAM user
Account ID (12 digits) or account alias
IAM user name
user-2
Password
****
Remember this account
Sign in
Sign in using root user email
Forgot password?
Try Amazon Redshift Serverless for free
Start with a 90-day credit of $300—no data warehouse administration required
Learn more ›

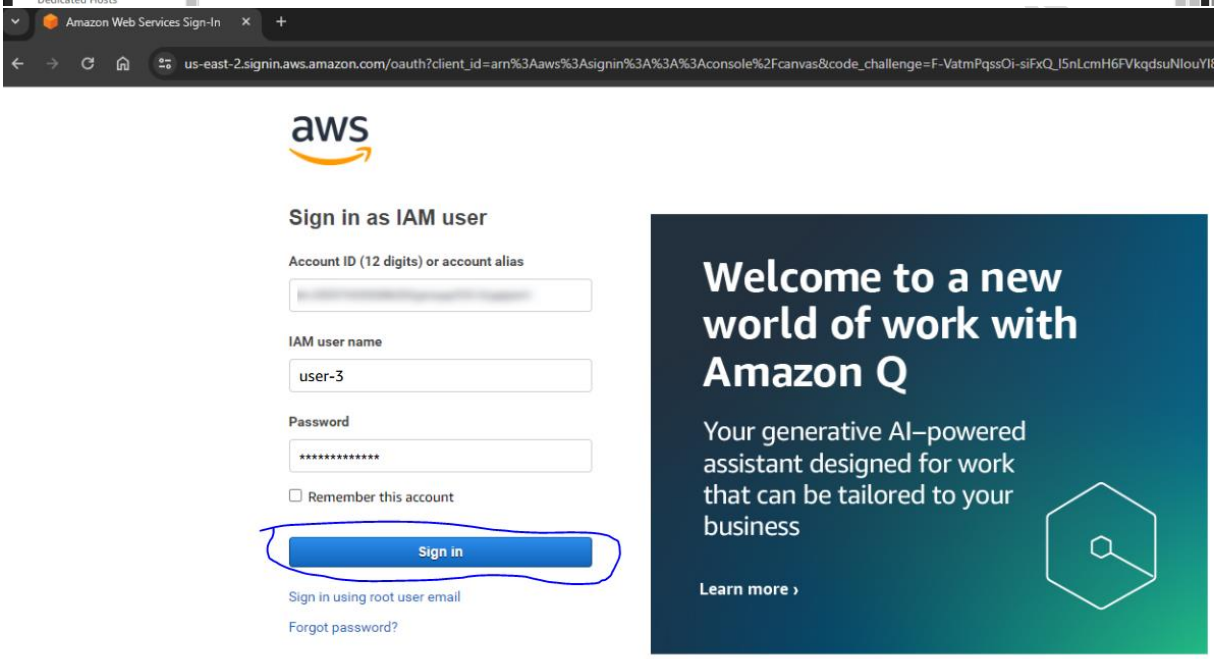

Console Home Info
Reset to default layout
+ Add widgets
Recently visited Info
EC2
S3
Applications (0) Info
Region: US East (N. Virginia)
Create application
us-east-1 (Current Region)
Find applications
Name
Description
Region
Originating account
Access denied

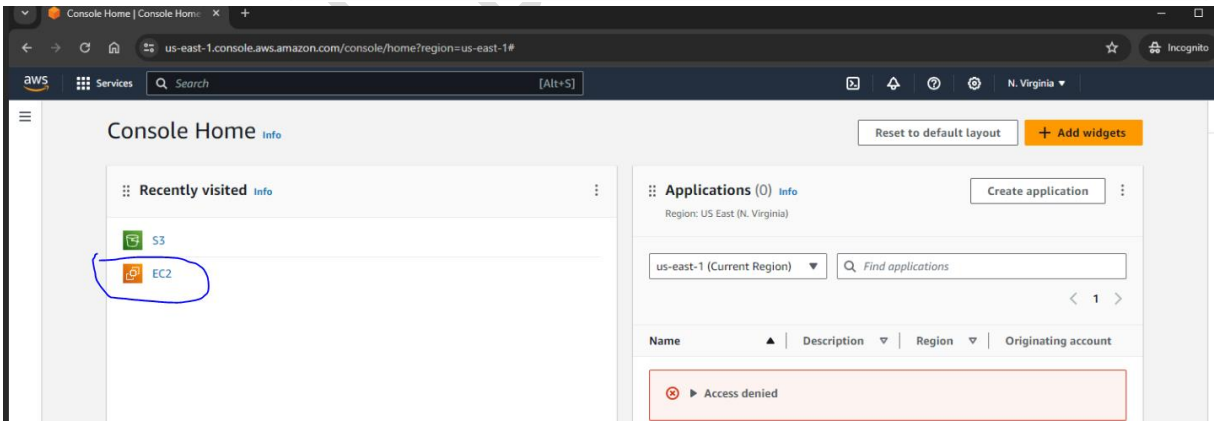

EC2 Dashboard
EC2 Global View
Events
Console-to-Code Preview
Instances
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Resources
EC2 Global view
You are using the following Amazon EC2 resources in the US East (N. Virginia) Region:
Instances (running) 2
Auto Scaling Groups 0
Dedicated Hosts 0
Elastic IPs 0
Instances 2
Key pairs 1
Load balancers 0
Placement groups 0
Security groups 24
Snapshots 3
Volumes 9
Account attributes
Default VPC
vpc-3e368943
Settings
Data protection and security
Zones
EC2 Serial Console
Default credit specification
EC2 console preferences

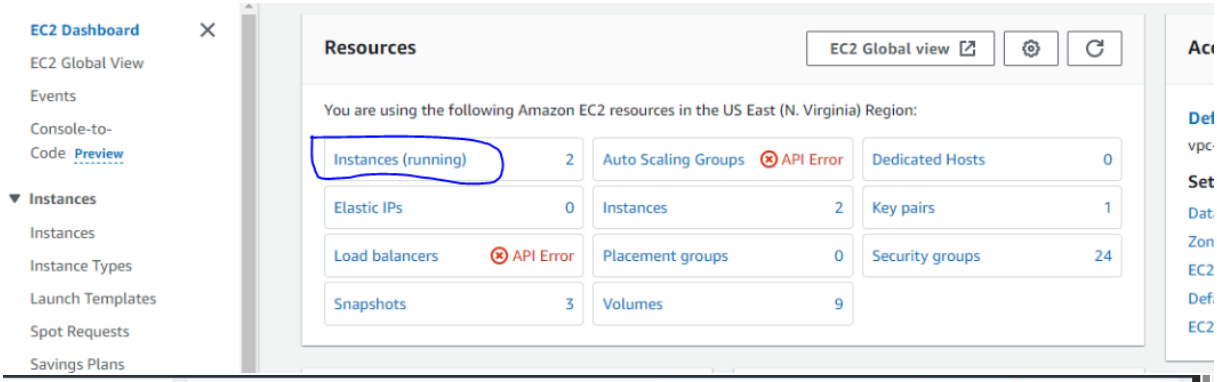

Instances (1/2) Info
Connect
Instance state
Actions
Launch instances
Stop instance
Start instance
Reboot instance
Hibernate instance
Terminate instance
Name
Instance ID
Instance state
Instance type
Availability Zone
Public IPv4 DNS
Application server
i-0aeba3d612be4e6ec
Running
t2.micro
us-east-1c
Web server
i-07146fc8b741e6371
Running
t2.micro
us-east-1c
i-0aeba3d612be4e6ec
Details
Status and alarms
Monitoring
Security
Networking
Storage
Tags
Instance summary Info
Instance ID
i-0aeba3d612be4e6ec
Public IPv4 address
18.206.57.247 | open address
Private IPv4 addresses
172.31.93.120
IPv6 address
Instance state
Running
Public IPv4 DNS
ec2-18-206-57-247.compute-1.amazonaws.com | open address
Hostname type
IP name: ip-172-31-93-120.ec2.internal
Private IP DNS name (IPv4 only)
ip-172-31-93-120.ec2.internal

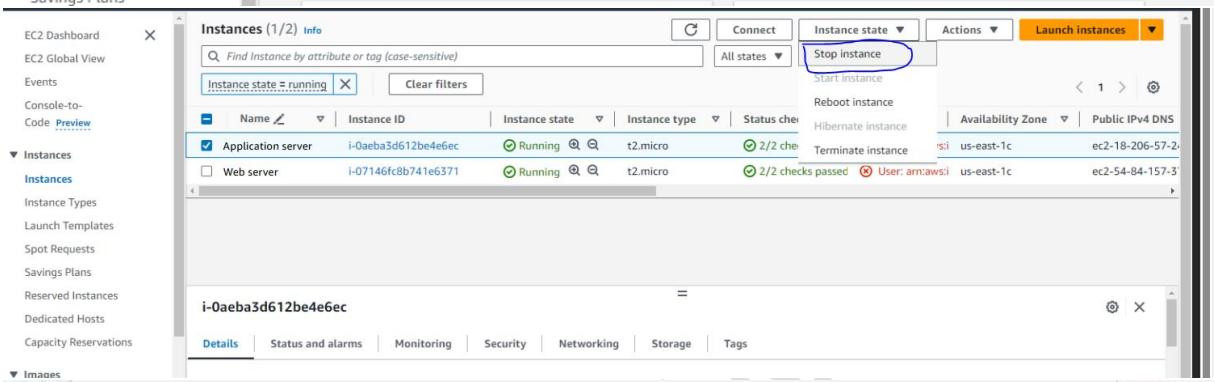
Stop instance?
Instance IDs
i-0aeba3d612be4e6ec
After you stop the instance, you are no longer charged usage or data transfer fees for it. However, you will still be billed for associated resources, such as attached EBS volumes and associated Elastic IP addresses.
To confirm that you want to stop the instance, choose the Stop button below.
Cancel
Stop

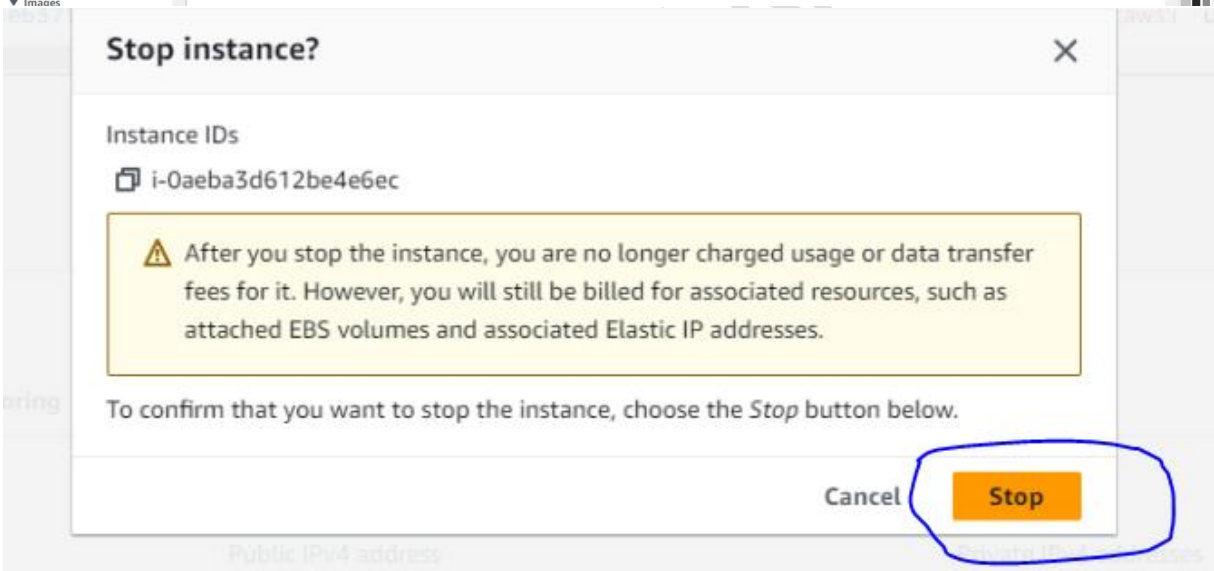

Amazon Web Services Sign-In
Instances | EC2 | us-east-1
us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#Instances:
Services
Search
[Alt+S]
N. Virginia
EC2 Dashboard
EC2 Global View
Events
Console-to-Code Preview
Instances
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Failed to stop the instance i-0aeba3d612be4e6ec
You are not authorized to perform this operation. User: arn:aws:iam::033742928620:user/user-2 is not authorized to perform: ec2:StopInstances on resource: arn:aws:ec2:us-east-1:033742928620:instance/i-0aeba3d612be4e6ec because no identity-based policy allows the ec2:StopInstances action. Encoded authorization failure message: a0ZaLCfc2DdBZ1rTwjqGulZMxV5PLHlhJ1LcRt-T7eC-ttu5Eq_iOr7BQP1CXD5C9Cp_KJXHy6T0PZ2sAaUprU1l_qslUlT_dRR7HFOkJ-Tp4q189hcvtqcF92Sj0vgw43WXQS77MpE4SnmZMvl5DUBGnSq5avIEtZJum-EFX6zQO1wu14M2HyEGOK8fVAnlz7cnpu693PBfOEu3MygwQlZqxyx5MvjIofqf4OgczNC1xY2uQRnYO1PV_eB_FB9g5wi8WWDuY6Bsho9m5knkIg5EzPlVVG9KOHp0RThSeiI4D36bV7_WVhPCqc5-ChvwVwD8f7V_DCLrfFGXtiXKWJCwmHmlM0bL3hq0X3b7m_JyDTEcK6oVfY8gI5DUtUt9--IPOx3sBUwKkhkaNV3KwBV78K0ZiXNWp8skR4s9j78sUcBavGEYosa-imxb0sQTy2zda15Ds1nkkIHazfg8xwHq2hz_mblOmfCTNFrIktNH1xV7rlzA5tHYZYJ1L-Ep2o3OxgPceXUF9c6_g_g3wwsNuCIY4iEZXvDeWxBdPT4tAHnQumzVoH1DgmCIjBY5Xvknzb3gABPMLbu7LAkIsZEPC6TPpsgN2F8aeNjfD6v9gRqCG2v-QWN6uLJSOc2zctH4507P1fAdC__G0udR7wZT3ohYNGw9mlMcEiQ_Yd5QCqAgAUojpzDsXoqSHlG8iqEntUuQs44Up4PIl2Xc9zAeC51ZAsC0gIv8H58yImt0hVbxk46cXOShLs4cBw
Diagnose with Amazon Q
Instances (1/2) Info
Connect
Instance state
Actions
Launch instances
i-0aeba3d612be4e6ec

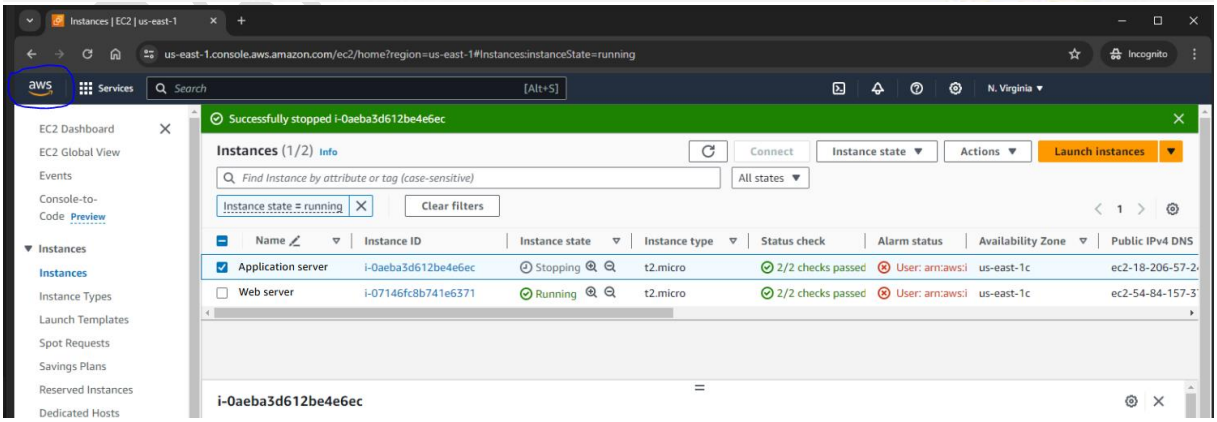

Amazon Web Services Sign-In
us-east-2.signin.aws.amazon.com/oauth?client_id=arn%3Aaws%3Asignin%3A%3A%3Aconsole%2Fcanvas&code_challenge=F-VatmPqssOi-siFxQ_I5nLcmH6FVkqdsuNIouYI
aws
Sign in as IAM user
Account ID (12 digits) or account alias
IAM user name
user-3
Password
****
Remember this account
Sign in
Sign in using root user email
Forgot password?
Welcome to a new world of work with Amazon Q
Your generative AI–powered assistant designed for work that can be tailored to your business
Learn more ›

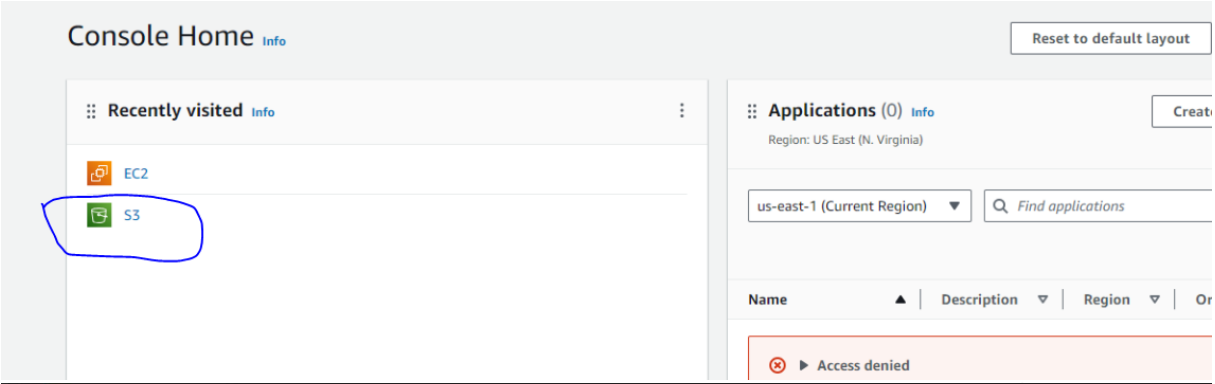

Console Home | Console Home
us-east-1.console.aws.amazon.com/console/home?region=us-east-1#
Services
Search
[Alt+S]
N. Virginia
Console Home Info
Reset to default layout
+ Add widgets
Recently visited Info
S3
EC2
Applications (0) Info
Region: US East (N. Virginia)
Create application
us-east-1 (Current Region)
Find applications
Name
Description
Region
Originating account
Access denied

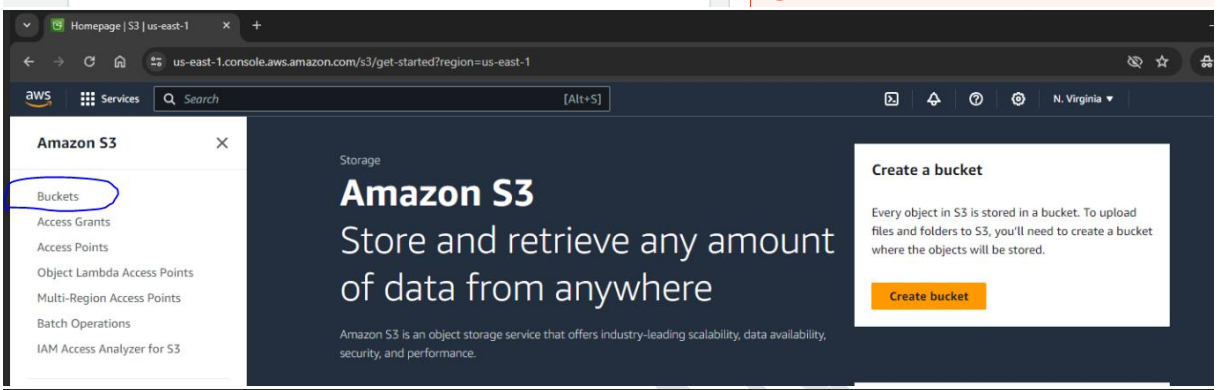

EC2 Dashboard
EC2 Global View
Events
Console-to-Code Preview
Instances
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Resources
EC2 Global view
You are using the following Amazon EC2 resources in the US East (N. Virginia) Region:
Instances (running) 2
Auto Scaling Groups API Error
Dedicated Hosts 0
Elastic IPs 0
Instances 2
Key pairs 1
Load balancers API Error
Placement groups 0
Security groups 24
Snapshots 3
Volumes 9

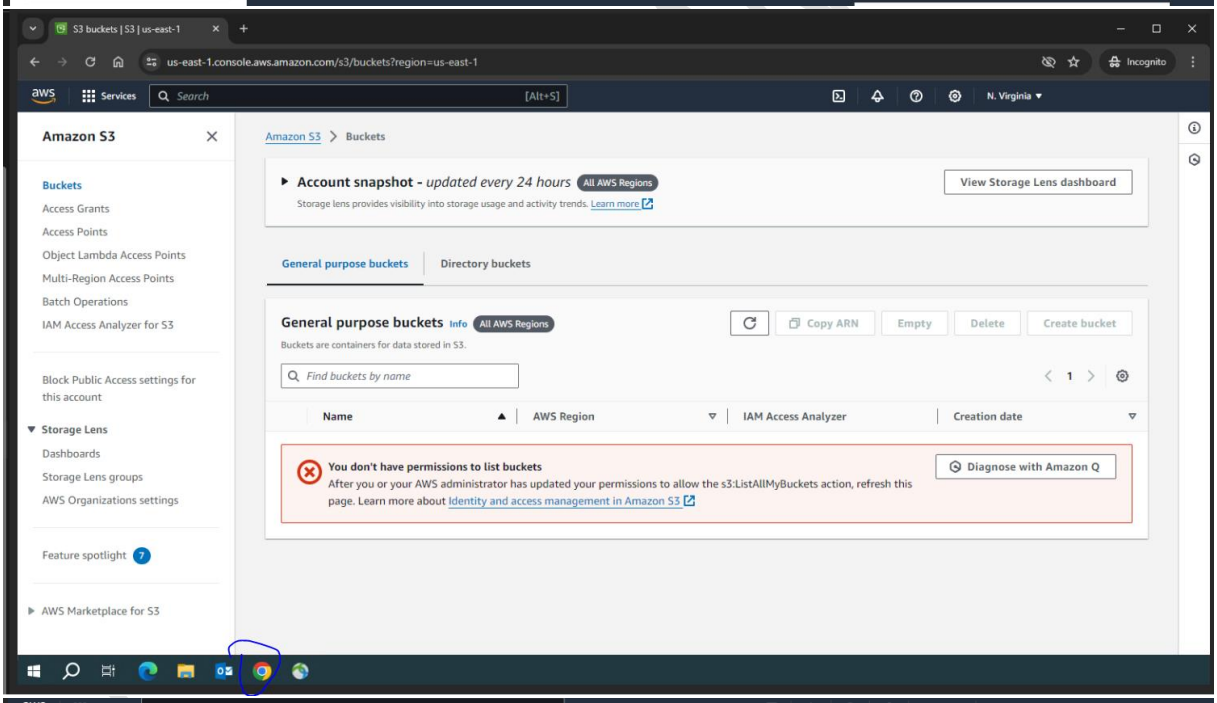

Instances (1/2) Info
Connect
Instance state
Actions
Launch instances
Find Instance by attribute or tag (case-sensitive)
All states
Instance state = running
Clear filters
Stop instance
Start instance
Reboot instance
Hibernate instance
Terminate instance
Name
Instance ID
Instance state
Instance type
Availability Zone
Public IPv4 DNS
Application server
i-0aeba3d612be4e6ec
Running
t2.micro
us-east-1c
Web server
i-07146fc8b741e6371
Running
t2.micro
2/2 checks passed
us-east-1c
i-0aeba3d612be4e6ec
Details
Status and alarms
Monitoring
Security
Networking
Storage
Tags

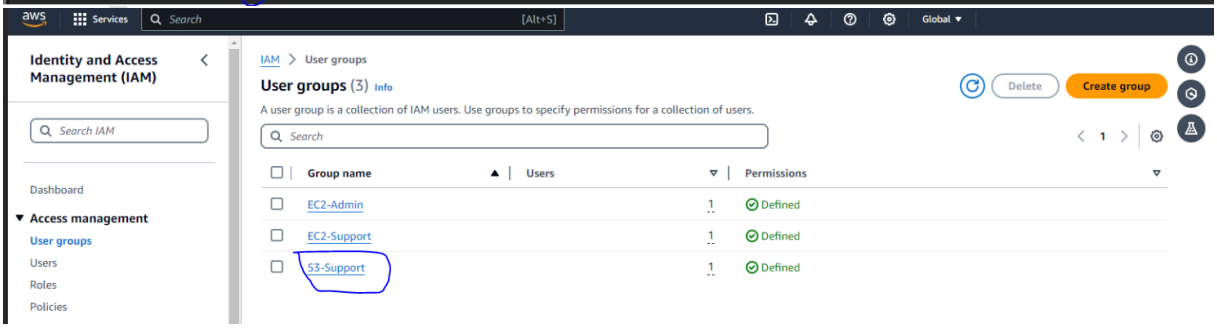

Stop instance?
Instance IDs
i-0aeba3d612be4e6ec
After you stop the instance, you are no longer charged usage or data transfer fees for it. However, you will still be billed for associated resources, such as attached EBS volumes and associated Elastic IP addresses.
To confirm that you want to stop the instance, choose the Stop button below.
Cancel
Stop

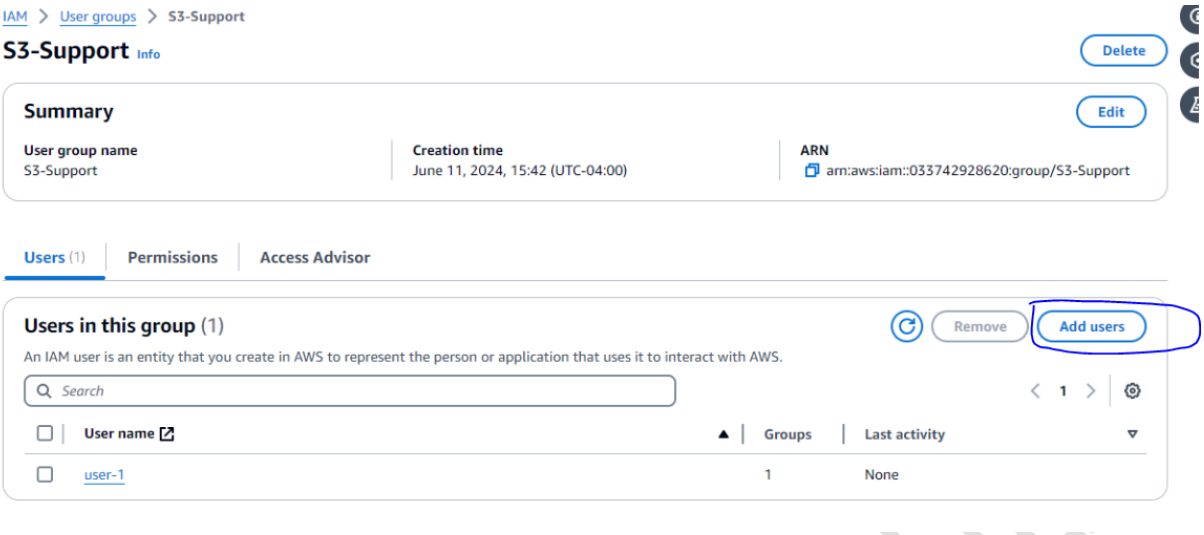

Successfully stopped i-0aeba3d612be4e6ec
Instances (1/2) Info
Connect
Instance state
Actions
Launch instances
Find Instance by attribute or tag (case-sensitive)
All states
Instance state = running
Clear filters
Name
Instance ID
Instance state
Instance type
Status check
Alarm status
Availability Zone
Public IPv4 DNS
Application server
i-0aeba3d612be4e6ec
Stopping
t2.micro
2/2 checks passed
us-east-1c
Web server
i-07146fc8b741e6371
Running
t2.micro
2/2 checks passed
us-east-1c
i-0aeba3d612be4e6ec

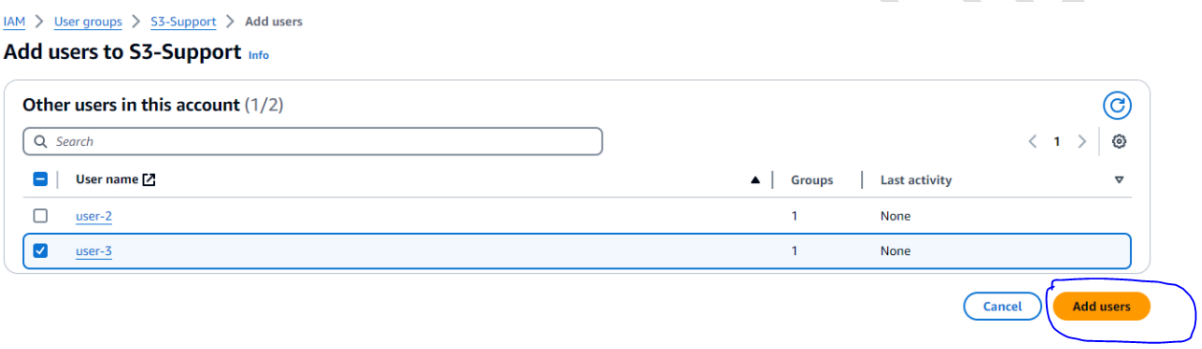

Console Home Info
Reset to default layout
Recently visited Info
EC2
S3
Applications (0) Info
Region: US East (N. Virginia)
us-east-1 (Current Region)
Find applications
Name
Description
Region
Access denied

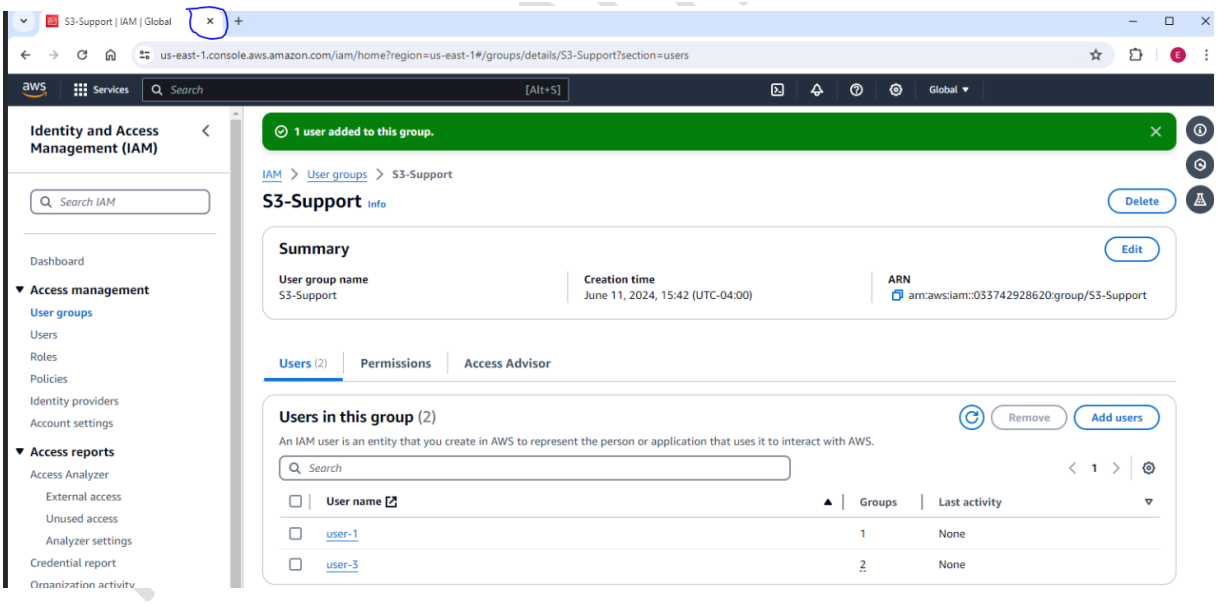

Homepage | S3 | us-east-1
us-east-1.console.aws.amazon.com/s3/get-started?region=us-east-1
Services
Search
[Alt+S]
N. Virginia
Amazon S3
Buckets
Access Grants
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Storage
Amazon S3
Store and retrieve any amount of data from anywhere
Amazon S3 is an object storage service that offers industry-leading scalability, data availability, security, and performance.
Create a bucket
Every object in S3 is stored in a bucket. To upload files and folders to S3, you'll need to create a bucket where the objects will be stored.
Create bucket

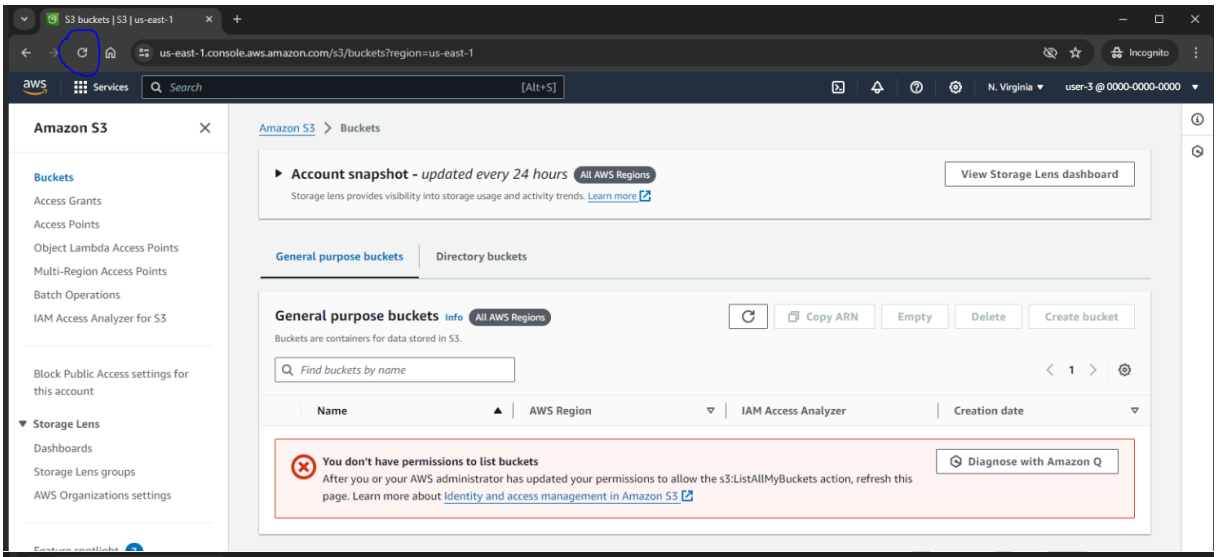

S3 buckets | S3 | us-east-1
us-east-1.console.aws.amazon.com/s3/buckets?region=us-east-1
Incognito
Services
Search
[Alt+S]
N. Virginia
Amazon S3
Buckets
Access Grants
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
Storage Lens groups
AWS Organizations settings
Feature spotlight 7
AWS Marketplace for S3
Amazon S3 > Buckets
Account snapshot - updated every 24 hours
All AWS Regions
Storage lens provides visibility into storage usage and activity trends. Learn more
View Storage Lens dashboard
General purpose buckets
Directory buckets
General purpose buckets Info
All AWS Regions
Buckets are containers for data stored in S3.
Copy ARN
Empty
Delete
Create bucket
Find buckets by name
Name
AWS Region
IAM Access Analyzer
Creation date
You don't have permissions to list buckets
After you or your AWS administrator has updated your permissions to allow the s3:ListAllMyBuckets action, refresh this page. Learn more about Identity and access management in Amazon S3
Diagnose with Amazon Q

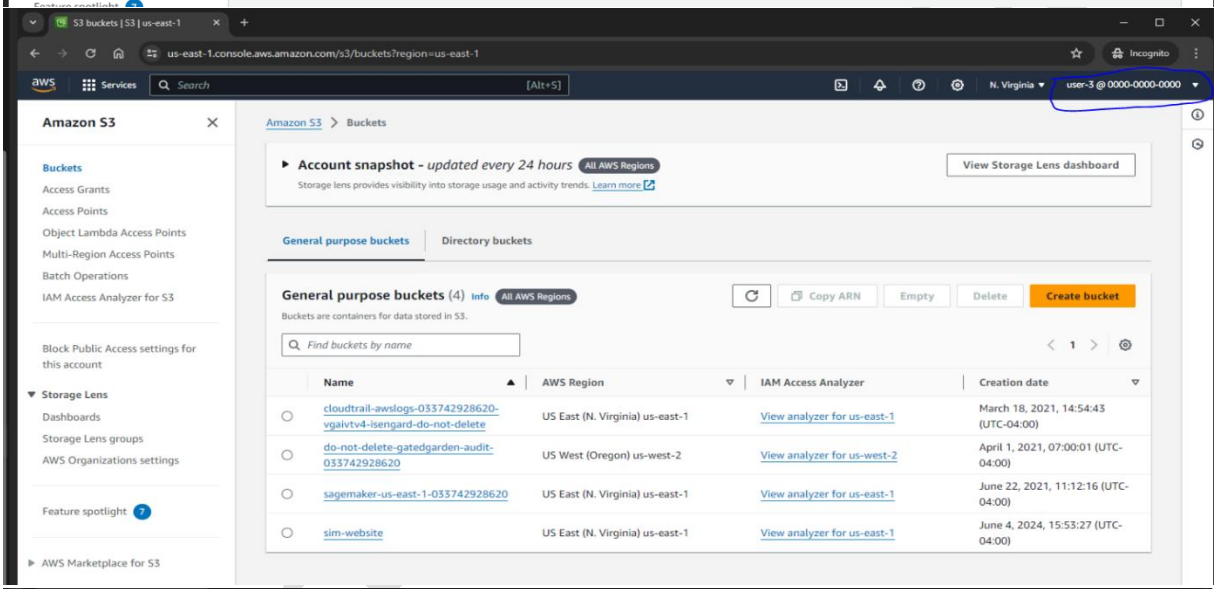

Services
Search
[Alt+S]
Global
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
IAM > User groups
User groups (3) Info
A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.
Delete
Create group
Search
Group name
Users
Permissions
EC2-Admin
EC2-Support
S3-Support
Defined

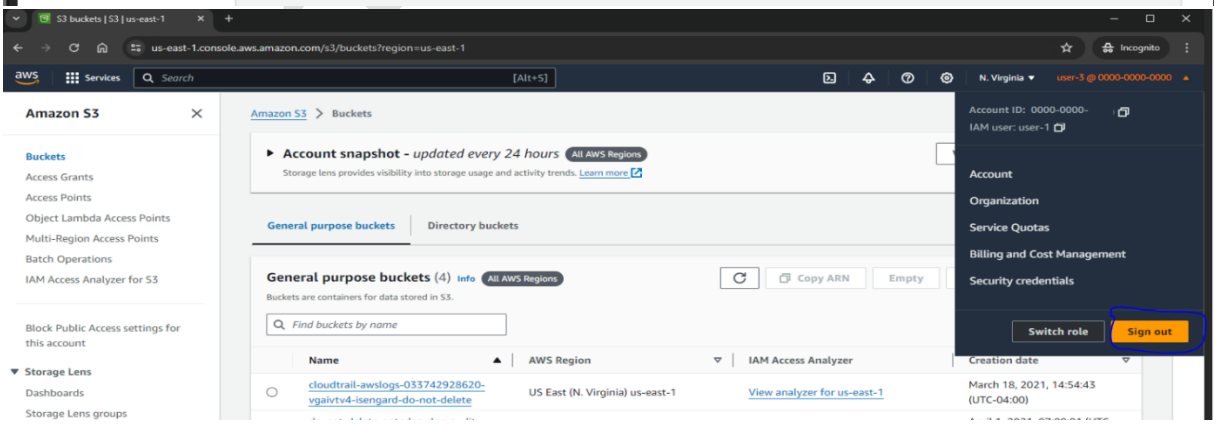

IAM > User groups > S3-Support
S3-Support Info
Delete
Summary
Edit
User group name
S3-Support
Creation time
June 11, 2024, 15:42 (UTC-04:00)
ARN
arn:aws:iam::033742928620:group/S3-Support
Users (1)
Permissions
Access Advisor
Users in this group (1)
Remove
Add users
An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.
Search
User name
Groups
Last activity
user-1
1
None

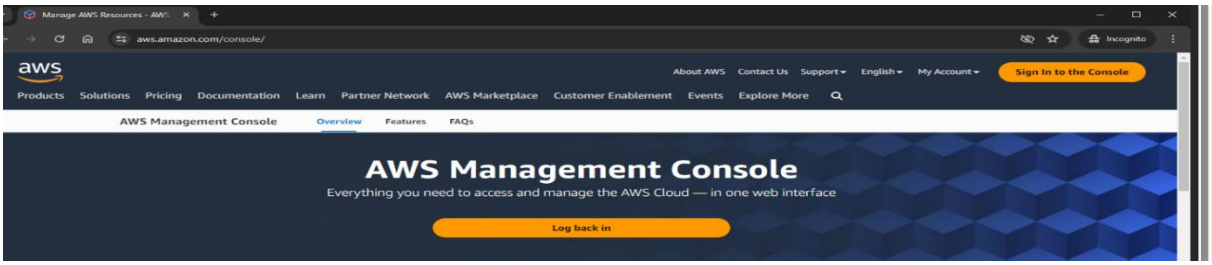

IAM > User groups > S3-Support > Add users
Add users to S3-Support Info
Other users in this account (1/2)
Search
User name
Groups
Last activity
user-2
1
None
user-3
1
None
Cancel
Add users


S3-Support | IAM | Global
us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/groups/details/S3-Support?section=users
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access Analyzer
External access
Unused access
Analyzer settings
Credential report
1 user added to this group.
IAM > User groups > S3-Support
S3-Support Info
Delete
Summary
Edit
User group name
S3-Support
Creation time
June 11, 2024, 15:42 (UTC-04:00)
ARN
arn:aws:iam::033742928620:group/S3-Support
Users (2)
Permissions
Access Advisor
Users in this group (2)
Remove
Add users
An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.
User name
Groups
Last activity
user-1
1
None
user-3
2
None


S3 buckets | S3 | us-east-1
us-east-1.console.aws.amazon.com/s3/buckets?region=us-east-1
Amazon S3
Buckets
Access Grants
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
Storage Lens groups
AWS Organizations settings
Amazon S3 > Buckets
Account snapshot - updated every 24 hours
View Storage Lens dashboard
General purpose buckets
Directory buckets
General purpose buckets
Copy ARN
Empty
Delete
Create bucket
Find buckets by name
Name
AWS Region
IAM Access Analyzer
Creation date
You don't have permissions to list buckets
Diagnose with Amazon Q


Amazon S3 > Buckets
Account snapshot - updated every 24 hours
View Storage Lens dashboard
General purpose buckets
Directory buckets
General purpose buckets (4)
Copy ARN
Empty
Delete
Create bucket
Find buckets by name
Name
AWS Region
IAM Access Analyzer
Creation date
cloudtrail-awslogs-033742928620-vgaivtv4-isengard-do-not-delete
US East (N. Virginia) us-east-1
View analyzer for us-east-1
March 18, 2021, 14:54:43 (UTC-04:00)
do-not-delete-gatedgarden-audit-033742928620
US West (Oregon) us-west-2
View analyzer for us-west-2
April 1, 2021, 07:00:01 (UTC-04:00)
sagemaker-us-east-1-033742928620
June 22, 2021, 11:12:16 (UTC-04:00)
sim-website
June 4, 2024, 15:53:27 (UTC-04:00)
Feature spotlight
AWS Marketplace for S3


Account ID: 0000-0000-
IAM user: user-1
Account
Organization
Service Quotas
Billing and Cost Management
Security credentials
Switch role
Sign out


AWS Management Console
Everything you need to access and manage the AWS Cloud — in one web interface
Log back in