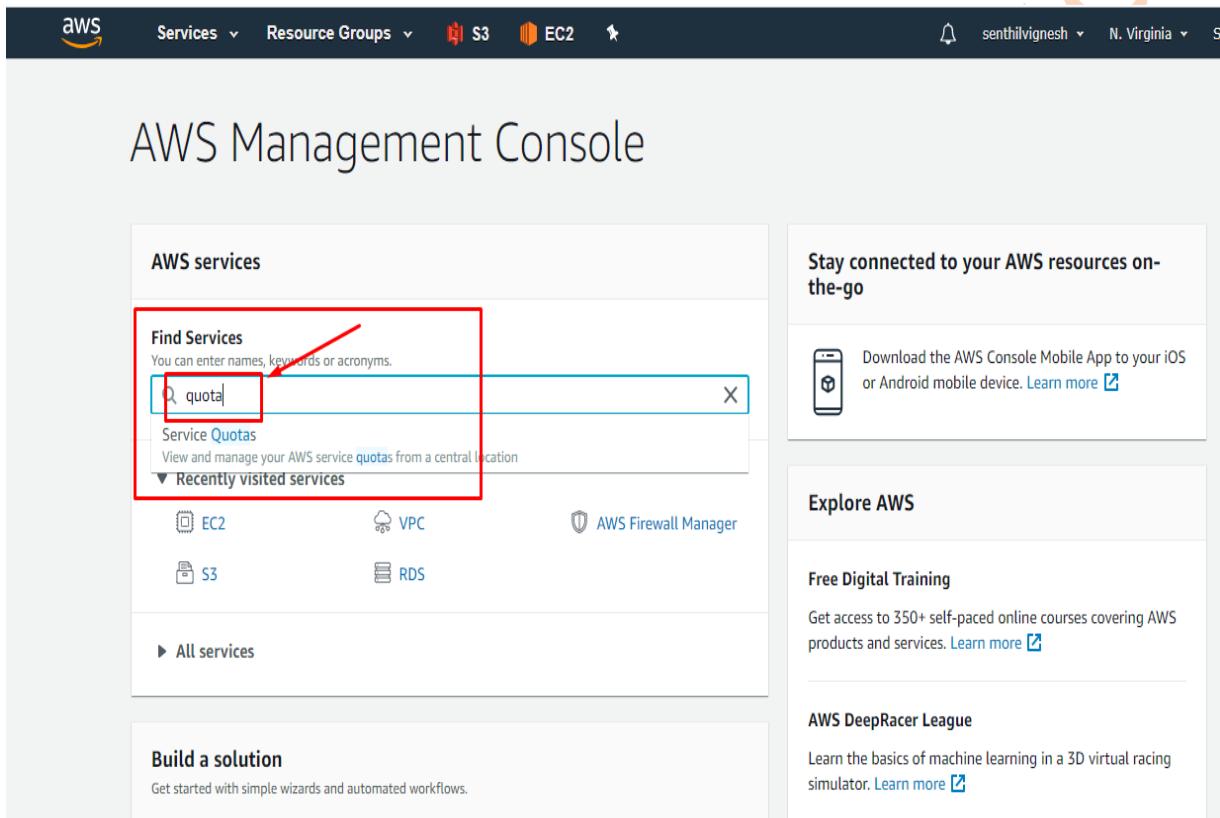


DVS Technologies Aws & Devops

Verifying A/C Limits:

Step1:



The screenshot shows the AWS Management Console homepage. At the top, there's a navigation bar with the AWS logo, 'Services' dropdown, 'Resource Groups' dropdown, 'S3' icon, 'EC2' icon, and a user dropdown for 'senthilvignesh' in 'N. Virginia'. Below the navigation bar, the main title 'AWS Management Console' is displayed. On the left, there's a sidebar titled 'AWS services' with a 'Find Services' search bar containing the text 'quota'. A red box highlights this search bar, and a red arrow points from the text above to it. Below the search bar, there's a 'Service Quotas' section with a link to 'View and manage your AWS service quotas from a central location'. Under 'Recently visited services', there are links for EC2, S3, VPC, RDS, and AWS Firewall Manager. At the bottom of the sidebar, there's a 'Build a solution' section with a link to 'Get started with simple wizards and automated workflows.' To the right of the sidebar, there's a large 'Explore AWS' section with links for 'Free Digital Training' (with a note about 350+ courses) and 'AWS DeepRacer League' (with a note about learning machine learning in a 3D racing simulator). A watermark for 'DV' is visible on the left side of the page.

Step2:

DVS Technologies Aws & Devops

The screenshot shows the AWS Service Quotas dashboard. On the left, there's a sidebar with options like Dashboard, AWS services, Quota request history, Organization, and Quota request template. The main area displays several service quotas in cards:

- Amazon Elastic Compute Cloud (Amazon EC2)**: Total quotas: 73
- Amazon Virtual Private Cloud (Amazon VPC)**: Total quotas: 23
- Amazon Elastic Block Store (Amazon EBS)**: Total quotas: 20
- Amazon Relational Database Service (Amazon RDS)**: Total quotas: 20
- Amazon DynamoDB**: Total quotas: 9
- AWS Key Management Service (AWS KMS)**: Total quotas: 51
- AWS Lambda**: Total quotas: 15
- Amazon Athena**: Total quotas: 4
- AWS CloudFormation**: Total quotas: 21

Below these cards are two sections: "Pending service quota requests (0)" and "Recently resolved service quota requests".

Step3:

The screenshot shows the "Amazon Elastic Compute Cloud (Amazon EC2)" service quota details page. The left sidebar has options for Dashboard, AWS services (which is selected), Quota request history, Organization, and Quota request template. The main content area is titled "Amazon Elastic Compute Cloud (Amazon EC2)" and contains a search bar and a table of service quotas.

Service quota	Applied quota value	AWS default quota value	Adjustable
Running On-Demand Standard (A, C, D, H, I, M, R, T, Z) instances	62	5	Yes

Step4:

DVS Technologies, Opp Home Town, Beside Biryani Zone, Marathahalli, Bangalore Phone: 9632558585 Mobile: 8892499499 Mail : dvs.training@gmail.com Web: www.dvstechnologies.in

DVS Technologies Aws & Devops

Running On-Demand Standard (A, C, D, H, I, M, R, T, Z) instances

Details			
Description Maximum number of vCPUs assigned to the Running On-Demand Standard (A, C, D, H, I, M, R, T, Z) instances.			
Quota code L-1216C47A	Quota ARN arn:aws:servicequotas:us-east-2:907814406801:ec2/L-1216C47A		
Usage 0	Applied quota value 62	AWS default quota value 5	Adjustable Yes

Monitoring
This displays a customizable CloudWatch embedded graph. [Learn more](#)

[Add to dashboard](#) [1h](#) [3h](#) [12h](#) [1d](#) [3d](#) [1w](#) [⟳](#)

Running On-Demand Standard (A, C, D, H, I, M, R, T, Z) instances - (Utilization %)

Step5:

Request quota increase: Running On-Demand Standard (A, C, D, H, I, M, R, T, Z) instances [X](#)

Quota name
Running On-Demand Standard (A, C, D, H, I, M, R, T, Z) instances

Description
Maximum number of vCPUs assigned to the Running On-Demand Standard (A, C, D, H, I, M, R, T, Z) instances.

Utilization
0

Applied quota value
62

AWS default quota value
5

Change quota value:
Enter in the total amount that you want the quota to be. [Learn more](#)

80

Must be a number greater than your current quota value

[Cancel](#) [Request](#)

DVS Technologies Aws & Devops

1. Choosing IAM Service:

Working With IAM :

The screenshot shows the AWS Management Console homepage. A red box highlights the search bar where 'iam' is typed. Below it, another red box highlights the 'IAM' service card, which is described as 'Manage access to AWS resources'. Other services like S3, EC2, and RDS are also visible.

AWS Management Console

AWS services

Find Services
You can enter names, keywords or acronyms.
IAM

IAM
Manage access to AWS resources

Recently visited services

All services

Build a solution
Get started with simple wizards and automated workflows.

Stay connected to your AWS resources on-the-go
Download the AWS Console Mobile App to your iOS or Android mobile device. [Learn more](#)

Explore AWS

AWS DeepRacer League
Learn the basics of machine learning in a 3D virtual racing simulator. [Learn more](#)

Get Up to 40% Better Price Performance in Amazon EC2
Amazon EC2 M6g, C6g, and R6g instances provide the best price performance for cloud native workloads in Amazon EC2. [Learn more](#)

Identity and Access Management (IAM)

Dashboard

Access management

- Groups
- Users
- Roles
- Policies
- Identity providers
- Account settings

Access reports

- Access analyzer
- Archive rules
- Analyzers
- Settings

Credential report
Organization activity

Welcome to Identity and Access Management

IAM users sign-in link:
<https://907814406801.signin.aws.amazon.com/console> [Customize](#)

IAM Resources

Users: 0 Roles: 3
Groups: 0 Identity Providers: 0
Customer Managed Policies: 0

Security Status 1 out of 5 complete.

<input checked="" type="checkbox"/> Delete your root access keys	▼
! Activate MFA on your root account	▼
! Create individual IAM users	▼
! Use groups to assign permissions	▼
! Apply an IAM password policy	▼

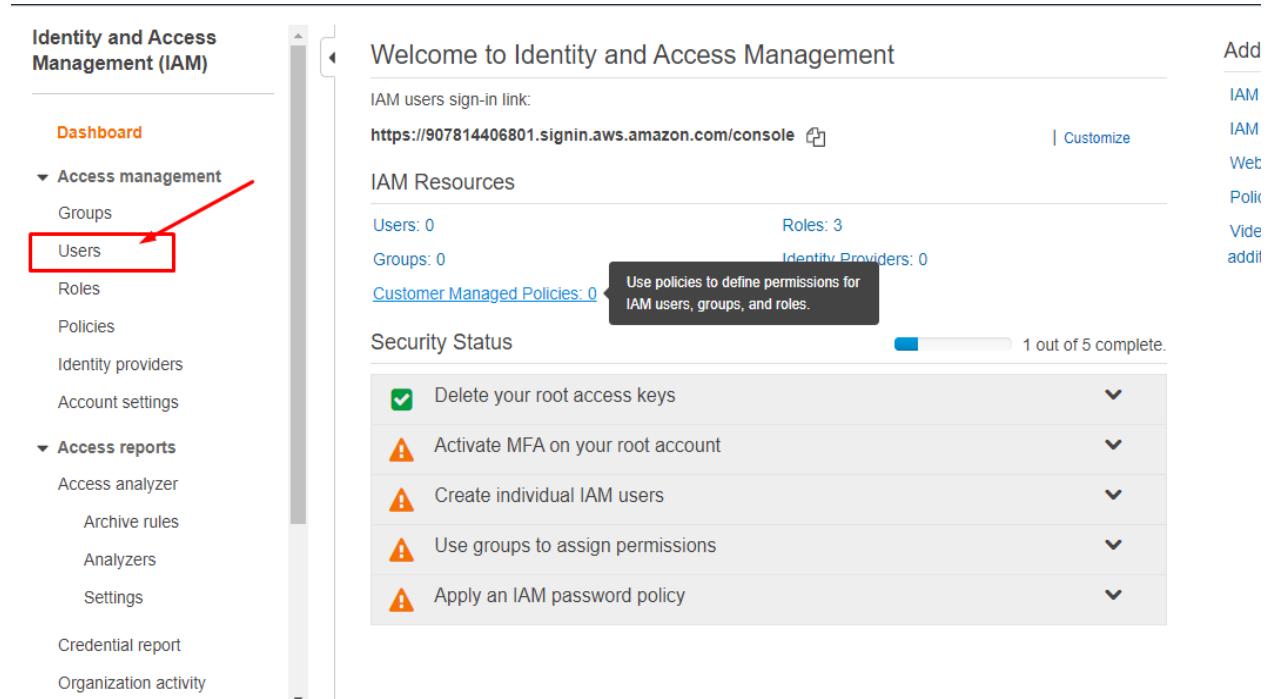
Additional Information

- IAM best practices
- IAM documentation
- Web Identity Federation Play
- Policy Simulator
- Videos, IAM release history
- additional resources

DVS Technologies Aws & Devops

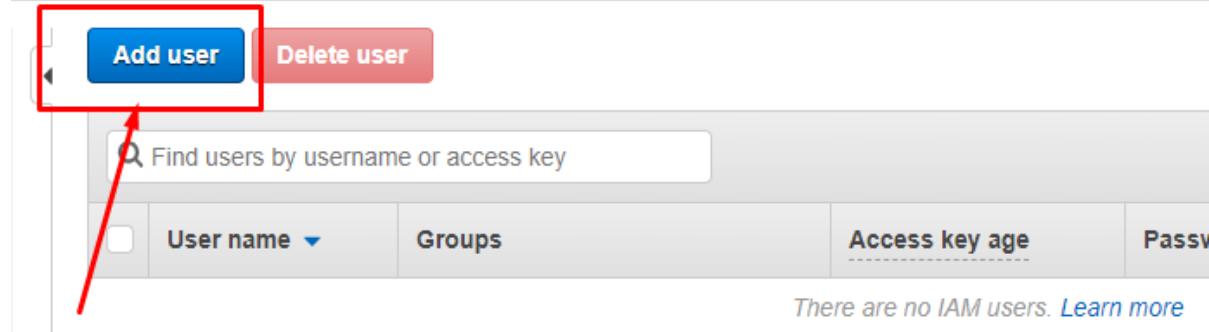
2. Create a New user without any permissions

Step1:



The screenshot shows the AWS Identity and Access Management (IAM) dashboard. On the left, there's a navigation menu with options like Dashboard, Access management (Groups, Users, Roles, Policies), Access reports (Access analyzer, Archive rules, Analyzers, Settings), and Credential report/Organization activity. The 'Users' option under 'Access management' is highlighted with a red box and a red arrow pointing to it. The main panel displays 'Welcome to Identity and Access Management' with links to IAM users sign-in and a customized URL. It shows 'IAM Resources' with 0 users, 0 groups, and 3 roles. A callout box says 'Use policies to define permissions for IAM users, groups, and roles.' Below is a 'Security Status' section with five items: 'Delete your root access keys' (checked), 'Activate MFA on your root account', 'Create individual IAM users', 'Use groups to assign permissions', and 'Apply an IAM password policy'. A progress bar indicates '1 out of 5 complete.'

Step2:



This screenshot shows the 'Users' page in the AWS IAM service. At the top, there are two buttons: 'Add user' (highlighted with a red box and a red arrow) and 'Delete user'. Below them is a search bar labeled 'Find users by username or access key'. The main table has columns for 'User name', 'Groups', 'Access key age', and 'Pass'. A message at the bottom states 'There are no IAM users. Learn more'.

Step3:

DVS Technologies Aws & Devops

User name* [+ Add another user](#)

Select AWS access type
Select how these users will access AWS. Access keys and autogenerated passwords are provided in the last step. [Learn more](#)

Access type* Programmatic access
Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.

AWS Management Console access
Enables a **password** that allows users to sign-in to the AWS Management Console.

Console password* Autogenerated password Custom password
 Show password

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

* Required [Cancel](#) [Next: Permissions](#)

Step4:

Set permissions

i 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](#)

Note:- Don't Select Options

Set permissions boundary

[Cancel](#) [Previous](#) [Next: Tags](#)

Step5:

DVS Technologies Aws & Devops

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
<input type="text" value="Add new key"/>	<input type="text"/>	<input type="button" value="Remove"/>

You can add 50 more tags.

Step6:



Review

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

User details

User name	ramesh
AWS access type	AWS Management Console access - with a password
Console password type	Custom
Require password reset	Yes
Permissions boundary	Permissions boundary is not set

Permissions summary

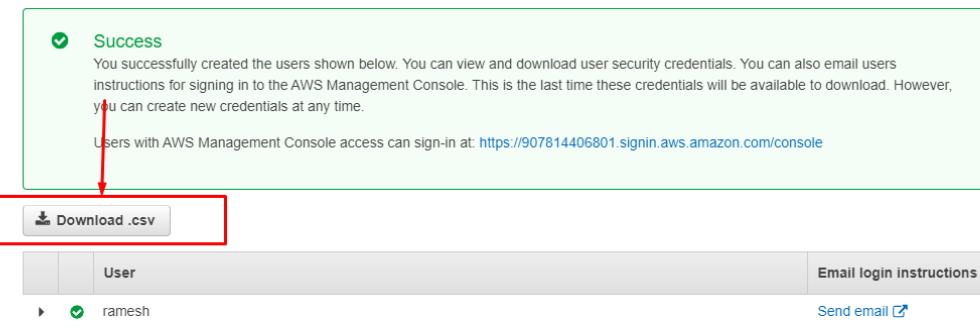
The user shown above will be added to the following groups.

Type	Name
Managed policy	IAMUserChangePassword

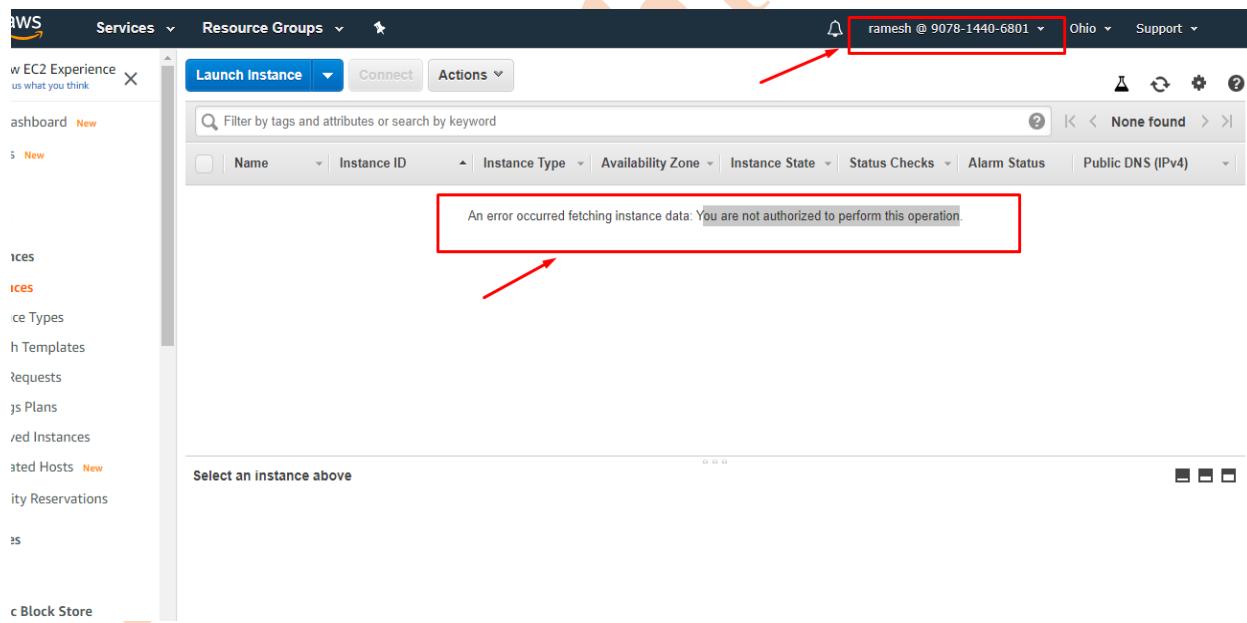
Step7:

DVS Technologies, Opp Home Town, Beside Biryani Zone, Marathahalli, Bangalore Phone: 9632558585 Mobile: 8892499499 Mail : dvs.training@gmail.com Web: www.dvstechnologies.in

DVS Technologies Aws & Devops



3. Granting Access for IAM user



DVS Technologies Aws & Devops

The screenshot shows the AWS Identity and Access Management (IAM) console. At the top, there are navigation links for Resource Groups, S3, EC2, and a user dropdown labeled "harish". A red box highlights the user dropdown, and another red arrow points from the "Users: 1" section in the main content area to the user dropdown.

Welcome to Identity and Access Management

IAM users sign-in link:
<https://907814406801.signin.aws.amazon.com/console> | Customize

IAM Resources

Users: 1	Groups: 0	Roles: 3	Identity Providers: 0
----------	-----------	----------	-----------------------

Customer Managed Policies: 0

Security Status 2 out of 5 complete.

<input checked="" type="checkbox"/> Delete your root access keys	▼
<input type="checkbox"/> Activate MFA on your root account	▼
<input checked="" type="checkbox"/> Create individual IAM users	▼
<input type="checkbox"/> Use groups to assign permissions	▼
<input type="checkbox"/> Apply an IAM password policy	▼

Add user **Delete user**

User name	Groups	Access key age	Password age	Last activity	MFA
ramesh	None	None	Today	Today	Not enabled

DVS Technologies Aws & Devops

arn:partition:service:region:account-id:

partition = aws or aws-cn (for China)
service = the AWS service: s3, ec2, rds, dynamodb
region = region code: us-east-1, ap-southeast-2

And, depending on service, finish with:

resource
resourcetype/resource
resourcetype/resource/qualifier

Users > ramesh

Summary

User ARN: arn:aws:iam::007814406801:user/ramesh

Path: /

Creation time: 2020-07-27 19:20 UTC+0400

Permissions Groups Tags Security credentials Access Advisor

Permissions policies (1 policy applied)

Add permissions Add inline policy

Policy name	Policy type
IAMUserChangePassword	AWS managed policy

Attached directly

Permissions boundary (not set)

DVS Technologies Aws & Devops

Users > ramesh

Summary

Delete user

User ARN arn:aws:iam::907814406801:user/ramesh 

Path /

Creation time 2020-07-27 19:20 UTC+0400

Caller 01 h

Permissions Groups Tags Security credentials Access Advisor

Add inline pol

▼ Permissions policies (1 policy applied)

Add permissions

Policy name ▾	Policy type ▾
IAMUserChangePassword	AWS managed policy

Attached directly

▶ IAMUserChangePassword AWS managed policy

▶ Permissions boundary (not set)

DVS1

DVS Technologies Aws & Devops

Add permissions to ramesh

1 2

Grant permissions

Use IAM policies to grant permissions. You can assign an existing policy or create a new one.

Attach existing policies directly

Create policy

Filter policies ▾ Q ec2

Policy name	Type	Used as
<input checked="" type="checkbox"/> AmazonEC2FullAccess	AWS managed	None
<input type="checkbox"/> AmazonEC2ReadOnlyAccess	AWS managed	None
<input type="checkbox"/> AmazonEC2RoleforAWSCodeDeploy	AWS managed	None
<input type="checkbox"/> AmazonEC2RoleforDataPipelineRole	AWS managed	None
<input type="checkbox"/> AmazonEC2RoleforSSM	AWS managed	None

Showing 22 results

Cancel Next: Review

DVS Technologies Aws & Devops

Summary Delete user ?

User ARN am.aws:iam::907814406801:user/ramesh Copy

Path /

Creation time 2020-07-27 19:20 UTC+0400

Permissions Groups Tags Security credentials Access Advisor

▼ Permissions policies (2 policies applied)

Add permissions Add inline policy

Policy name ▾	Policy type ▾
Attached directly	
▶ AmazonEC2FullAccess	AWS managed policy X
▶ IAMUserChangePassword	AWS managed policy X

▶ Permissions boundary (not set)

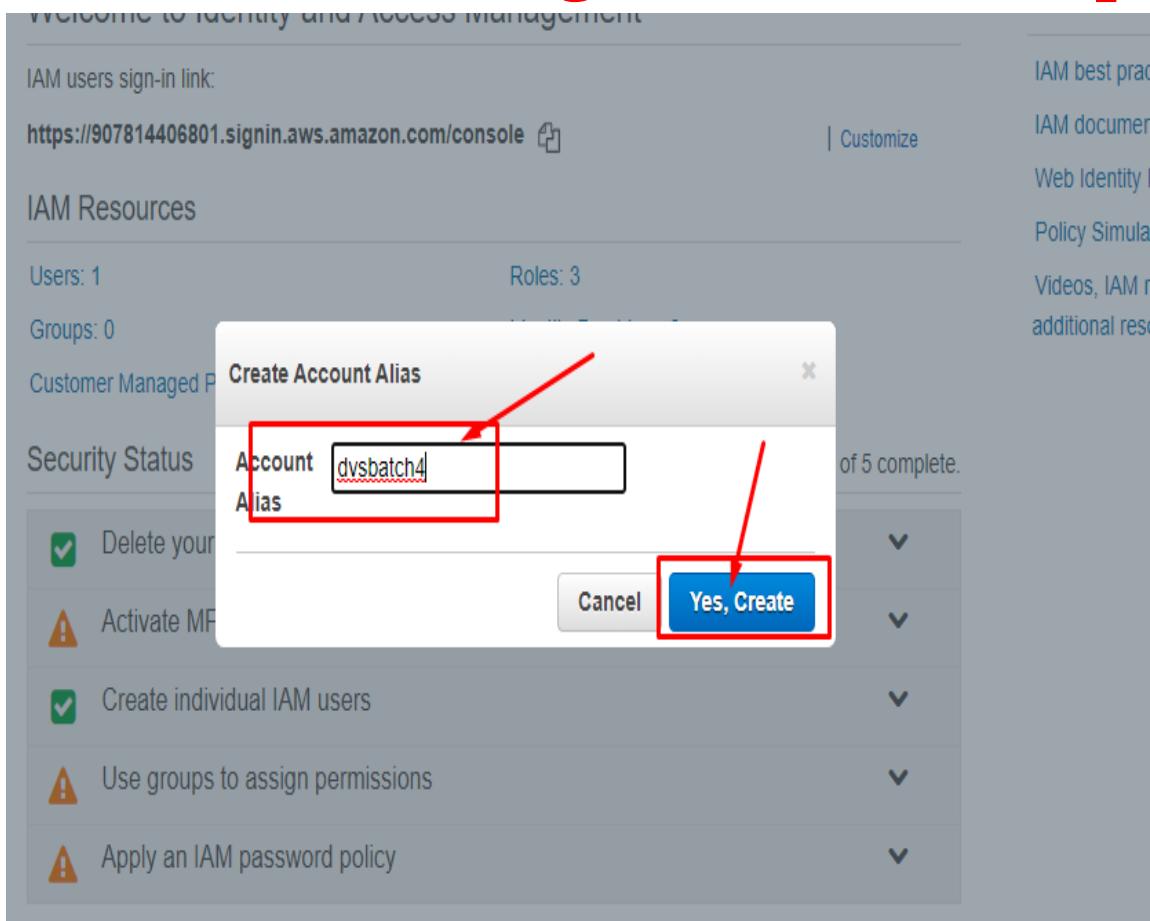


DVS Technologies Aws & Devops

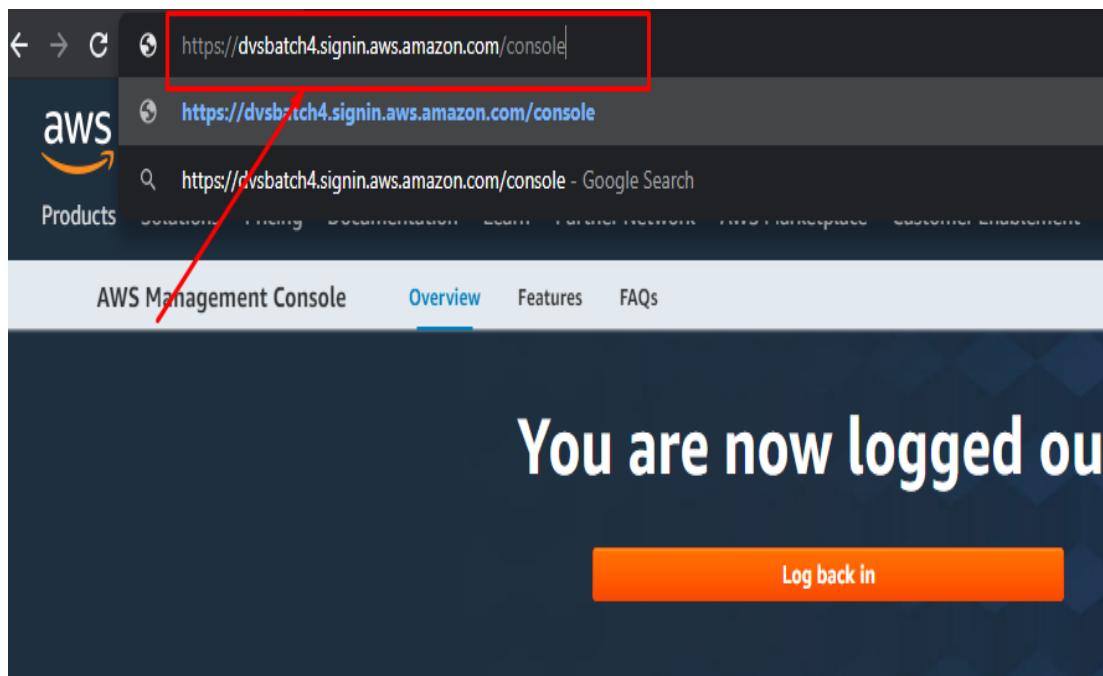
The screenshot shows the AWS EC2 dashboard. At the top, there's a navigation bar with 'Resource Groups' and a user profile section labeled 'ramesh @ 9078-1440-6801'. Below the navigation bar is a toolbar with 'Launch Instance', 'Connect', and 'Actions' buttons. A search bar allows filtering by tags or keywords. The main content area displays a message: 'You do not have any running instances in this region.' It includes a link to the 'Getting Started Guide' and a 'Launch Instance' button. A red box highlights the user profile section, and a red arrow points from the text 'No Entries' to the 'Launch Instance' button.

The screenshot shows the AWS IAM Welcome page. On the left, a sidebar lists 'Identity and Access Management (IAM)' with sub-options: 'Dashboard', 'Access management', 'Groups', 'Users', 'Roles', 'Policies', 'Identity providers', and 'Account settings'. The 'Access management' option is expanded. The main content area is titled 'Welcome to Identity and Access Management'. It features a 'Sign-in' link: 'https://907814406801.signin.aws.amazon.com/console'. Below this, it shows 'IAM Resources' with statistics: 'Users: 1', 'Groups: 0', 'Roles: 3', and 'Identity Providers: 0'. It also lists 'Customer Managed Policies: 0'. A 'Security Status' bar indicates '2 out of 5 complete'. A red box highlights the sign-in link, and another red box highlights the 'Customize' button in the top right corner. A red arrow points from the 'Customize' button towards the sign-in link.

DVS Technologies Aws & Devops



DVS Technologies Aws & Devops



DVS Technologies Aws & Devops

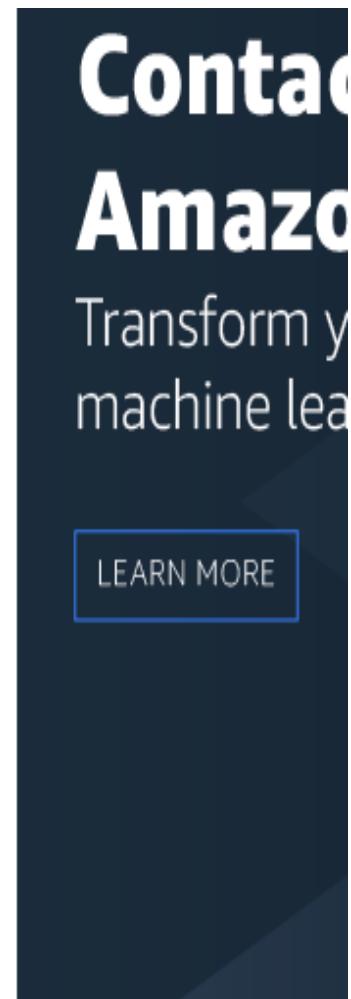
Account ID (12 digits) or account alias

IAM user name

Password

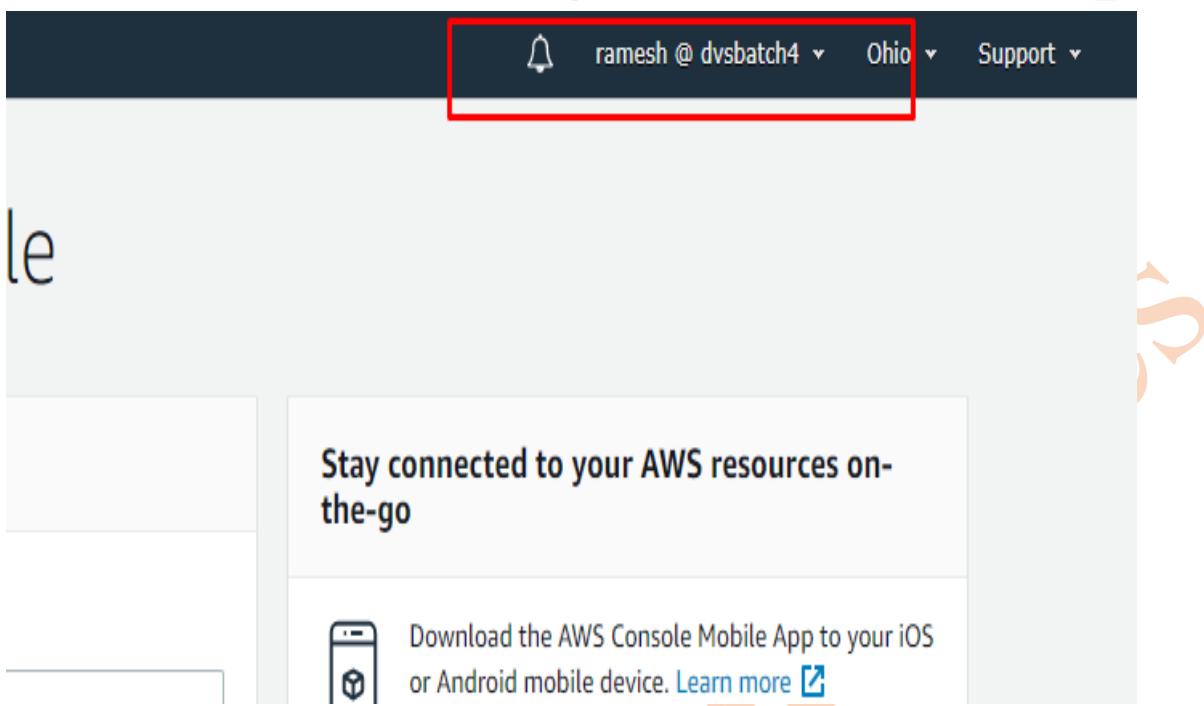
[Sign in using root user email](#)

[Forgot password?](#)



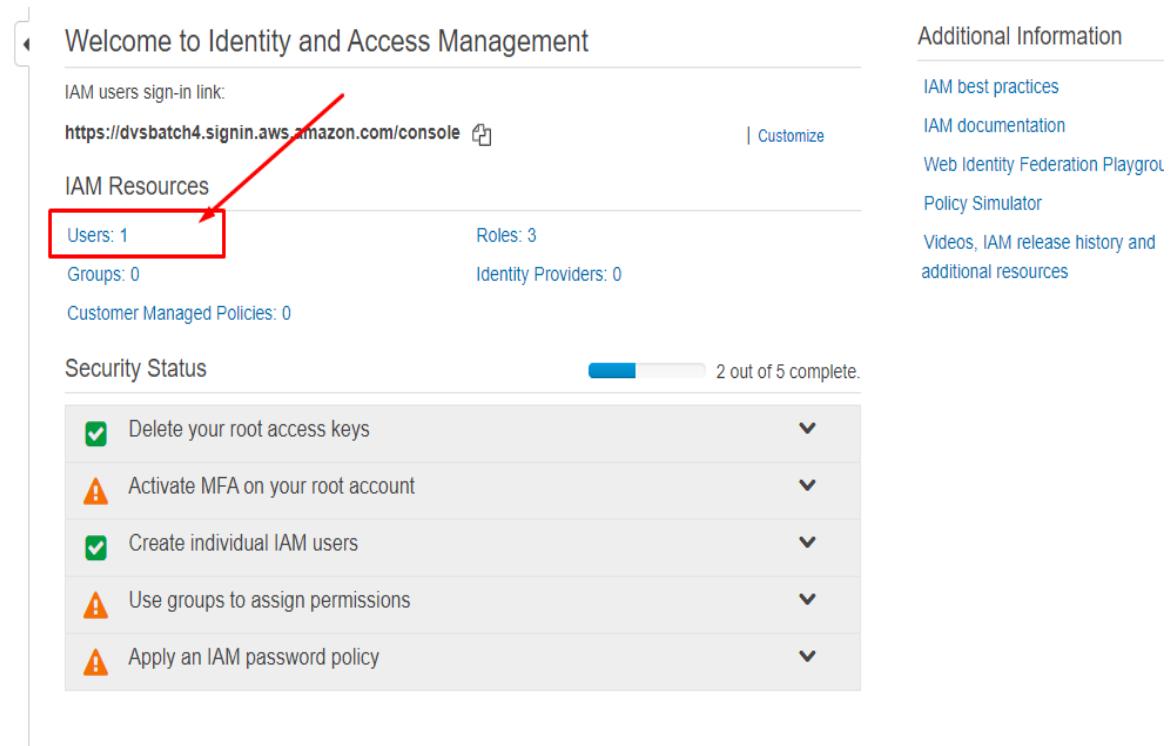
DVS'Y

DVS Technologies Aws & Devops



The screenshot shows the AWS Home page. At the top, there's a dark header bar with a bell icon, the email 'ramesh @ dvsbatch4' with a dropdown arrow, 'Ohio' with a dropdown arrow, and 'Support' with a dropdown arrow. Below the header, there's a large orange banner with the text 'Stay connected to your AWS resources on-the-go'. Underneath the banner, there's a mobile phone icon and the text 'Download the AWS Console Mobile App to your iOS or Android mobile device. Learn more' with a blue link. To the right of the banner, there's a large orange 'HN' watermark.

4. Reset user password



The screenshot shows the AWS Identity and Access Management (IAM) Home page. It features a left sidebar with a navigation tree and a main content area. In the main content area, there's a section titled 'Welcome to Identity and Access Management' with a 'Sign-in' link. Below that is an 'IAM Resources' section showing 'Users: 1' (which is highlighted with a red box and has a red arrow pointing to it), 'Groups: 0', and 'Customer Managed Policies: 0'. To the right of the resources is an 'Additional Information' sidebar with links to 'IAM best practices', 'IAM documentation', 'Web Identity Federation Playgrou...', 'Policy Simulator', and 'Videos, IAM release history and additional resources'. Below the resources is a 'Security Status' section with a progress bar showing '2 out of 5 complete.' and a list of five items with checkboxes and dropdown arrows. The first item is checked ('Delete your root access keys').

DVS Technologies Aws & Devops

The screenshot shows a user management interface with the following elements:

- Add user** and **Delete user** buttons.
- A search bar labeled "Find users by username or access key".
- A filter dropdown set to "User name".
- A table with columns: User name, Groups, Access key age, Password age, and Last activity.
- A single row is visible in the table, corresponding to the user "ramesh".
- The "User name" column for "ramesh" has a checked checkbox.
- The "Groups" column for "ramesh" shows "None".
- The "Access key age" column for "ramesh" shows "None".
- The "Password age" column for "ramesh" shows "Today".
- The "Last activity" column for "ramesh" shows "Today".

A red box highlights the "User name" column for the user "ramesh", and a red arrow points from the text "Select user" to this highlighted area.

DVS Technologies Aws & Devops

Summary

[Delete user](#)

User ARN [arn:aws:iam::907814406801:user/ramesh](#)

Path /

Creation time 2020-07-27 19:20 UTC+0400

Permissions Groups Tags **Security credentials** Access Advisor

Sign-in credentials

Summary • Console sign-in link: <https://dvsbatch4.signin.aws.amazon.com/console>

Console password Enabled (last signed in Today) | [Manage](#)

Assigned MFA device Not assigned | [Manage](#)

Signing certificates None [Edit](#)

Access keys

Use access keys to make secure REST or HTTP Query protocol requests to AWS service APIs. For your protection, you should never share your secret key with anyone. As a best practice, we recommend frequent key rotation. [Learn more](#)

DVS Technologies Aws & Devops

Manage console access

Manage ramesh's AWS console access and password

Console access Enable Disable
Disabling will remove pre-existing password.

Set password* Keep existing password Autogenerated password Custom password
 Show password

Require password reset User must create a new password at next sign-in

Use keys to make secure REST or HTTP Query protocol requests to AWS service APIs. For your protection, you

Sign in as IAM user

Account ID (12 digits) or account alias

dvsbatch4

IAM user name

ramesh

Password

.....

[Sign in using root user email](#)

[Forgot password?](#)

Amazon FSx for Windows File Server

Scale and simplify your file storage

[LEARN MORE](#)



DVS Technologies Aws & Devops

5. Working with MFA

Activating MFA for Root Account:

IAM users sign-in link:
<https://dvsbatch4.signin.aws.amazon.com/console> | Customize

IAM Resources

Users: 1 Roles: 3
Groups: 0 Identity Providers: 0
Customer Managed Policies: 0

Security Status
2 out of 5 complete.

- Delete your root access keys
- Activate MFA on your root account
- Create individual IAM users
- Use groups to assign permissions
- Apply an IAM password policy

Activate multi-factor authentication (MFA) on your AWS root account to add another layer of protection to help keep your account secure. [Learn More](#)

[Manage MFA](#)

IAM best practices
IAM documentation
Web Identity Federation Playgrou
Policy Simulator
Videos, IAM release history and
additional resources

Your Security Credentials

Use this page to manage the credentials for your AWS account. To manage credentials for AWS Identity and Access Management (IAM) users, use the To learn more about the types of AWS credentials and how they're used, see [AWS Security Credentials](#) in AWS General Reference.

▲ Password

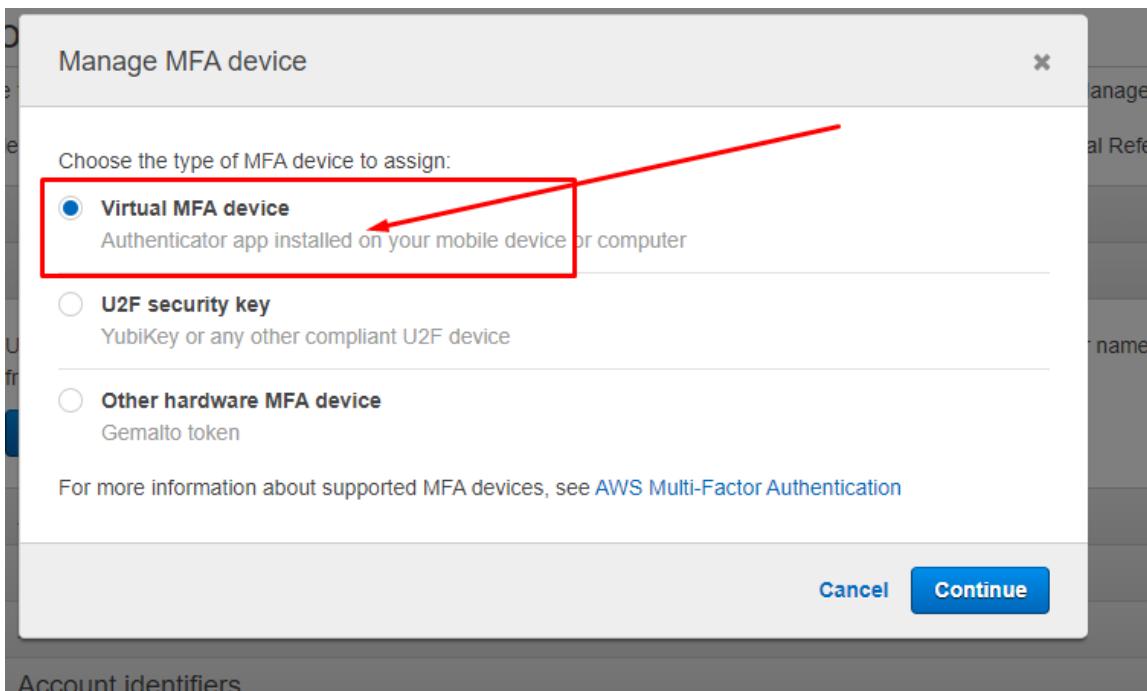
▼ Multi-factor authentication (MFA)

Use MFA to increase the security of your AWS environments. Signing in to MFA-protected accounts requires a user name, password, and an author from an MFA device.

[Activate MFA](#)

▲ Access keys (access key ID and secret access key)
▲ CloudFront key pairs
▲ X.509 certificate
▲ Account identifiers

DVS Technologies Aws & Devops



DVS Technologies Aws & Devops

Set up virtual MFA device

x

1. Install a compatible app on your mobile device or computer

See a [list of compatible applications](#)

2. Use your virtual MFA app and your device's camera to scan the QR code



x

Scan this code.

Alternatively, you can type the secret key. [Show secret key](#)

DVSTechY

DVS Technologies Aws & Devops

Set up virtual MFA device



Alternatively, you can type the secret key. [Show secret key](#)

3. Type two consecutive MFA codes below

MFA code 1 404901

MFA code 2 889319

first code

second code

from mobile

Cancel Previous Assign MFA

Set up virtual MFA device

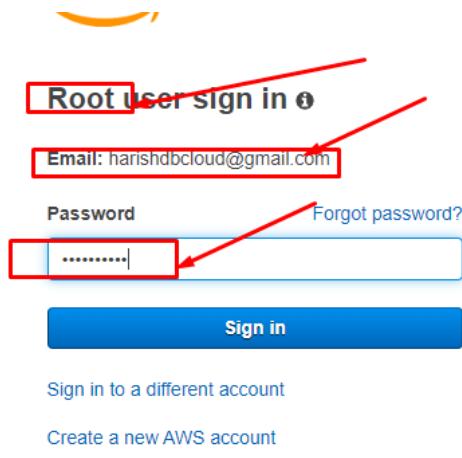
You have successfully assigned virtual MFA

This virtual MFA will be required during sign-in.

[Close](#)

DVS Technologies Aws & Devops

Verification:



A screenshot of the AWS sign-in page. A red box highlights the 'Root user sign in' link. Another red box highlights the 'Email' field containing 'harishdbcloud@gmail.com'. A third red box highlights the 'Password' field. A blue arrow points from the 'Password' field to the 'Forgot password?' link. Below the form are links for 'Sign in to a different account' and 'Create a new AWS account'.



**AWS Accounts Include
12 Months of Free Tier Access**

Including use of Amazon EC2,
Amazon S3, and Amazon DynamoDB

Visit aws.amazon.com/free for full offer terms

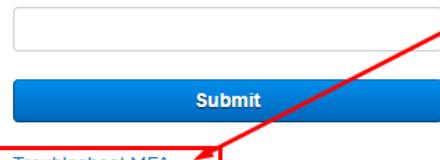
Troubleshooting MFA:

Multi-factor authentication

Your account is secured using multi-factor authentication (MFA). To finish signing in, turn on or view your MFA device and type the authentication code below.

Email address: harishdbcloud@gmail.com

MFA code



A screenshot of the MFA troubleshooting page. A red box highlights the 'Submit' button. A blue arrow points from the 'Submit' button to the 'Troubleshoot MFA' link. Below the form are links for 'Cancel'.

Amazon FSx for Windows File Server

Scale and simplify your file storage

[LEARN MORE](#)



DVS Technologies Aws & Devops



Troubleshoot your authentication device

Re-sync with AWS servers

If your multi-factor authentication (MFA) device appears to be functioning properly, and you are not able to sign in, then the device might be out of sync.

[Re-sync MFA device](#)

Sign in using alternative factors of authentication

If your multi-factor authentication (MFA) device is lost, damaged, or not working, you can sign in using alternative factors of authentication. You must verify your identity using the email and phone registered with this account.

[Sign in using alternative factors](#)

[Sign in to a different account](#)

Deactivate MFA :

Root user sign in ⓘ

Email: harishdbcloud@gmail.com

Password

Forgot password?

.....

[Sign in](#)

[Sign in to a different account](#)

[Create a new AWS account](#)

Build Mobile and Web Apps Fast

Add authentication and data sync with AWS Amplify in just a few lines of code.

[LEARN MORE](#)



DVS Technologies Aws & Devops

Multi-factor authentication

Your account is secured using multi-factor authentication (MFA). To finish signing in, turn on or view your MFA device and type the authentication code below.

Email address: harishdbcloud@gmail.com

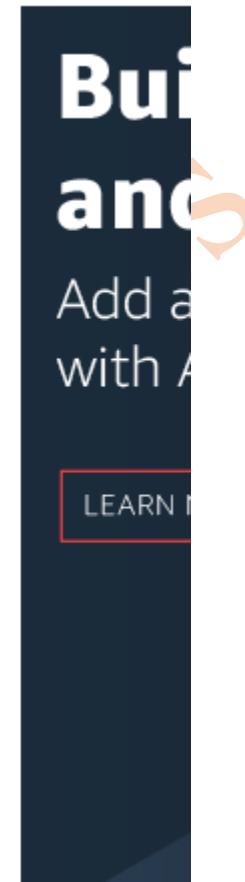
MFA code

471615

Submit

[Troubleshoot MFA](#)

[Cancel](#)



DVS'S

DVS Technologies Aws & Devops

IAM Resources

Users: 1

Roles: 3

Groups: 0

Identity Providers: 0

Customer Managed Policies: 0

Security Status

3 out of 5 complete.

Delete your root access keys

Activate MFA on your root account

Activate multi-factor authentication (MFA) on your AWS root account to add another layer of protection to help keep your account secure. [Learn More](#)

[Manage MFA](#)

Create individual IAM users

Use groups to assign permissions

Apply an IAM password policy

▲ Password

▼ Multi-factor authentication (MFA)

Use MFA to increase the security of your AWS environments. Signing in to MFA-protected accounts requires a user name, password, and an authenticator from an MFA device.

Device type	Serial number	Actions
Virtual	arn:aws:iam::907814406801:mfa/root-account-mfa-device	Manage

▲ Access keys (access key ID and secret access key)

▲ CloudFront key pairs

▲ X.509 certificate

▲ Account identifiers

DVS Technologies Aws & Devops

Manage MFA device

Choose an action to perform on the MFA device for user :

Remove

This user will no longer be required to provide MFA during sign-in.

Resync

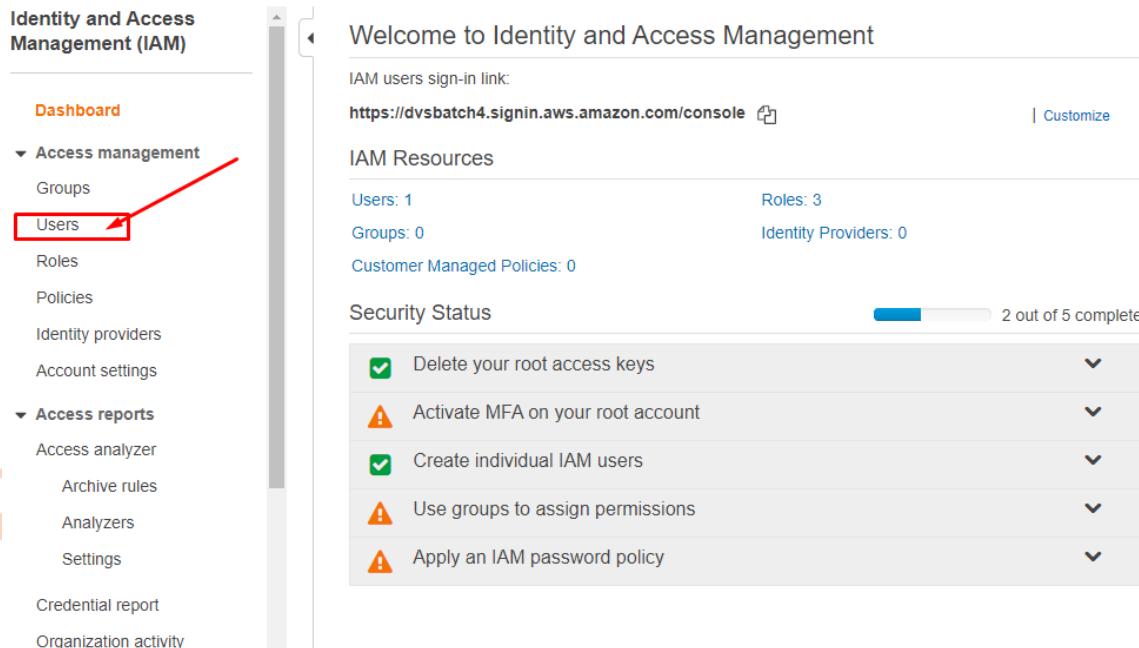
This option is not available for U2F security keys.

Cancel

Remove

Post above changes try to login to the console again with your mail id and password & check the results.

Activate MFA for IAM Users:



The screenshot shows the AWS Identity and Access Management (IAM) service dashboard. On the left, there's a navigation pane with several sections: 'Identity and Access Management (IAM)', 'Dashboard', 'Access management' (which is expanded, showing 'Groups', 'Users' [highlighted with a red box], 'Roles', 'Policies', 'Identity providers', and 'Account settings'), 'Access reports' (which is also expanded, showing 'Access analyzer', 'Archive rules', 'Analyzers', and 'Settings'), 'Credential report', and 'Organization activity'. The main content area is titled 'Welcome to Identity and Access Management' and includes a 'Sign-in link' (https://dvsbatch4.signin.aws.amazon.com/console). It also displays 'IAM Resources' such as 'Users: 1', 'Groups: 0', 'Roles: 3', 'Identity Providers: 0', and 'Customer Managed Policies: 0'. Below this is a 'Security Status' section with a progress bar showing '2 out of 5 complete.' and a list of five items with checkboxes and dropdown arrows: 'Delete your root access keys' (checked), 'Activate MFA on your root account' (warning icon), 'Create individual IAM users' (checked), 'Use groups to assign permissions' (warning icon), and 'Apply an IAM password policy' (warning icon).

DVS Technologies Aws & Devops

Add user Delete user

User name		Groups	Access key age	Password age
<input checked="" type="checkbox"/>	ramesh	None	None	Yesterday

Users > ramesh

Summary

Delete us

User ARN arn:aws:iam::907814406801:user/ramesh

Path /

Creation time 2020-07-27 19:20 UTC+0400

Permissions Groups Tags Security credentials Access Advisor

Sign-in credentials

Summary • Console sign-in link: https://dvsbat14.sigin.aws.amazon.com/console

Console password

Enabled (last signed in Yesterday) | Manage

Assigned MFA device

Not assigned | Manage

Signing certificates

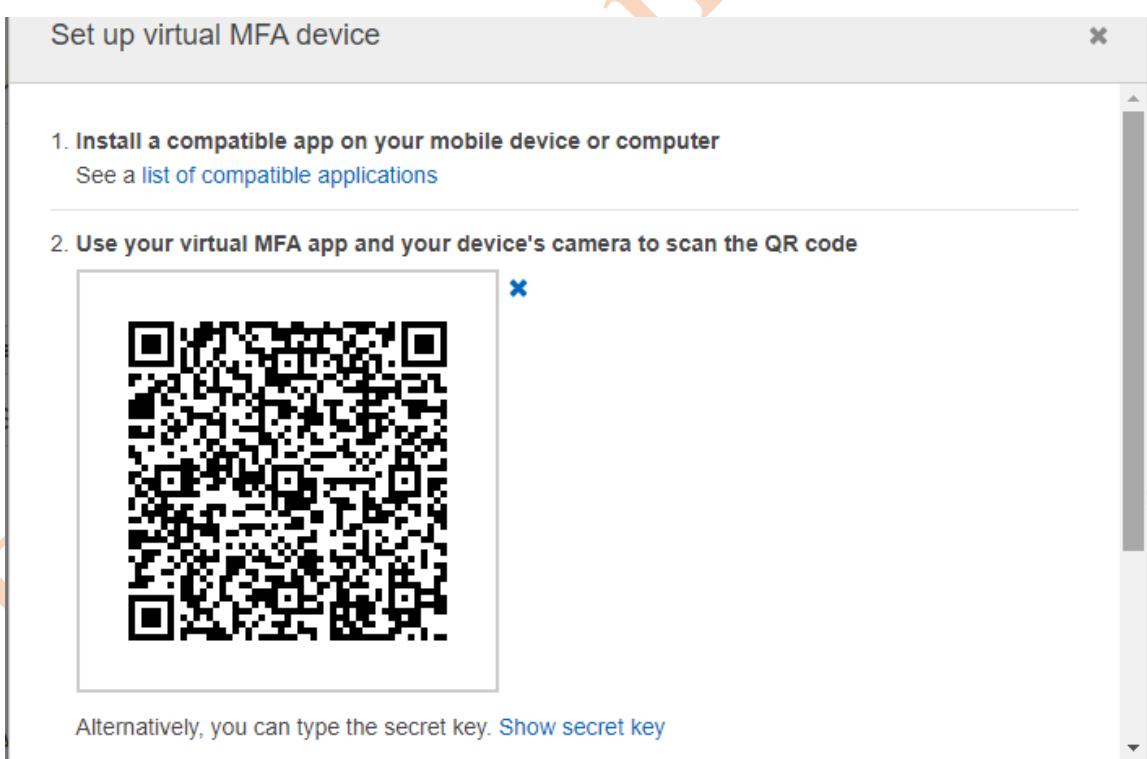
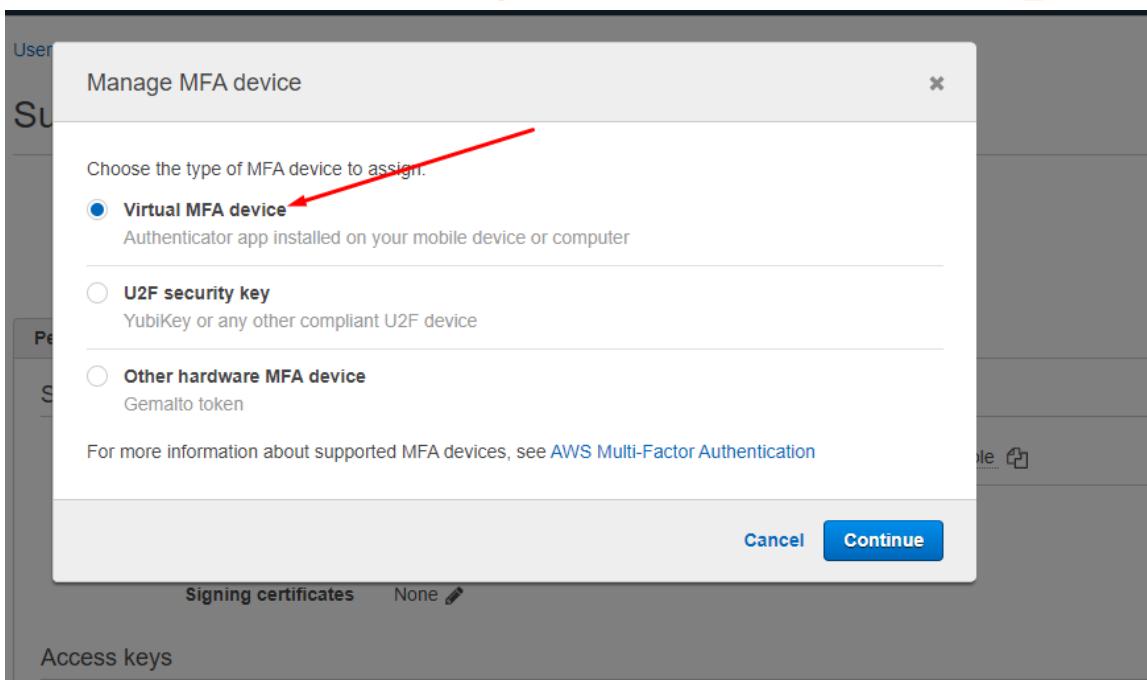
None

Access keys

Use access keys to make secure REST or HTTP Query protocol requests to AWS service APIs. For your protection, you should never share your sec



DVS Technologies Aws & Devops



DVS Technologies Aws & Devops



Alternatively, you can type the secret key. [Show secret key](#)

3. Type two consecutive MFA codes below

MFA code 1 821094

MFA code 2 130592

[Cancel](#) [Previous](#) [Assign MFA](#)

Set up virtual MFA device

You have successfully assigned virtual MFA

This virtual MFA will be required during sign-in.

[Close](#)

Permissions Groups Tags Security credentials Access Advisor

DVS

DVS Technologies Aws & Devops

Verification:

Sign in as IAM user

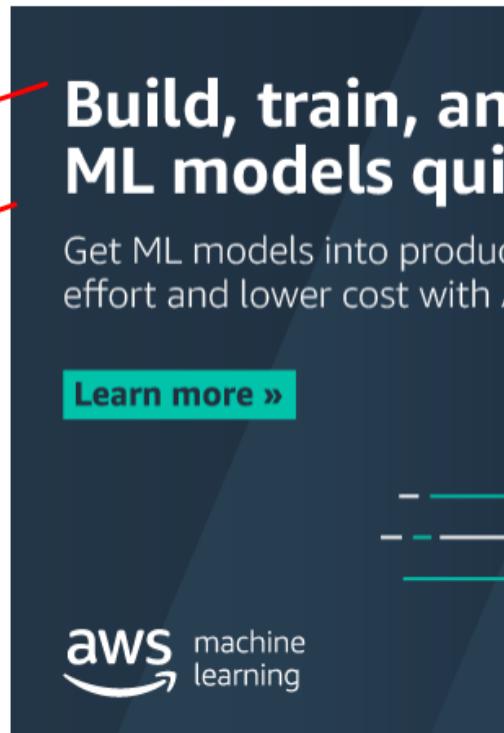
Account ID (12 digits) or account alias

IAM user name

Password

[Sign in using root user email](#)

[Forgot password?](#)



DVS

DVS Technologies Aws & Devops

Multi-factor Authentication

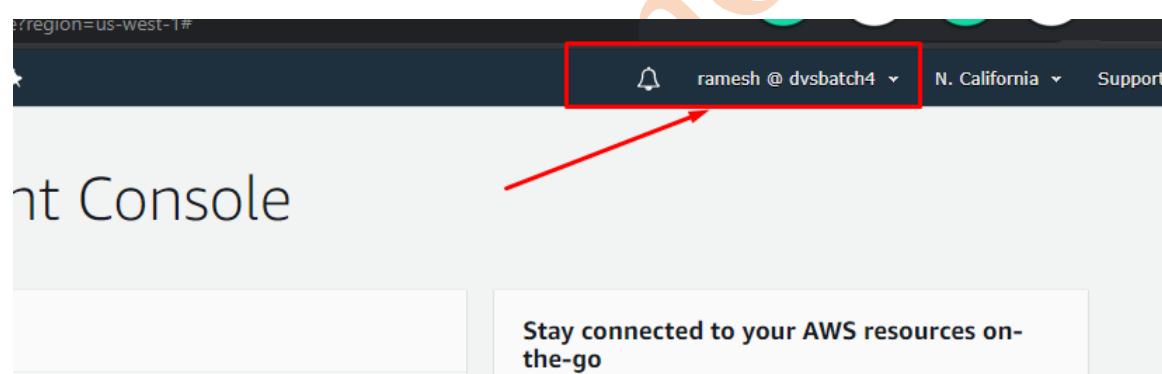
Enter an MFA code to complete sign-in.

MFA Code:

888342

Submit

[Cancel](#)



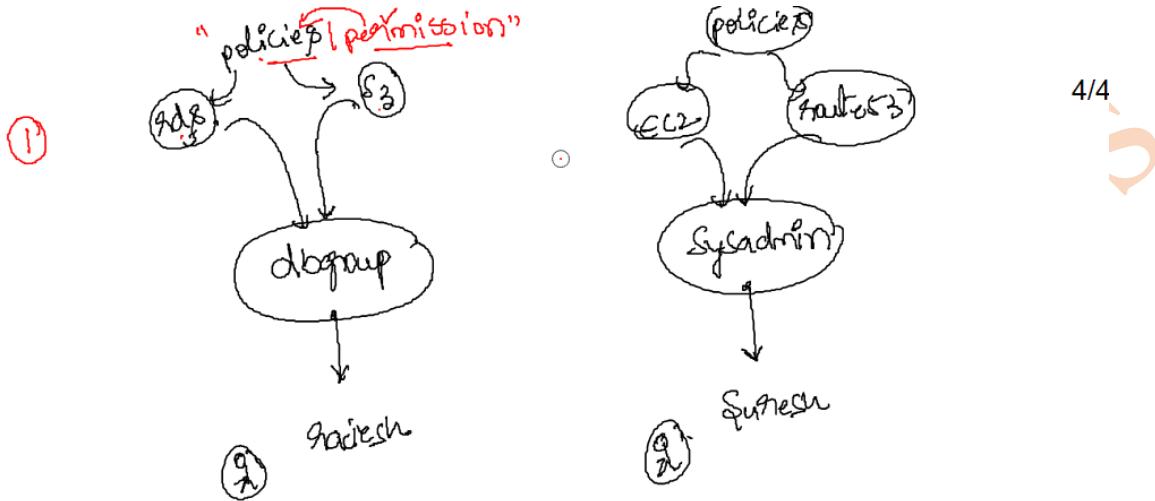
Stay connected to your AWS resources on-the-go

DVS

DVS Technologies Aws & Devops

6. Working with Groups

Requirement:



DVS Technologies Aws & Devops

The screenshot shows the AWS Management Console with the search bar set to "iam". The main search results are displayed under the "IAM" category, which includes "Manage access to AWS resources". Other services listed include EC2, Lightsail, Lambda, Batch, Elastic Beanstalk, Serverless Application Repository, AWS Outposts, and EC2 Image Builder. Below the search results, there are sections for "Storage" and "Management & Governance". On the left sidebar, under the "Identity and Access Management (IAM)" section, the "Groups" link is highlighted with a red box and an arrow pointing to it from the main search area.

AWS Services

Resource Groups

S3

EC2

History

Console Home

IAM

EC2

Billing

S3

VPC

iam

IAM

Manage access to AWS resources

EC2

Lightsail

Lambda

Batch

Elastic Beanstalk

Serverless Application Repository

AWS Outposts

EC2 Image Builder

Amazon Managed Block

Satellite

Ground Station

Quantum Technologies

Amazon Braket

Storage

Management & Governance

Identity and Access Management (IAM)

Dashboard

Access management

Groups

Users

Roles

Policies

Identity providers

Account settings

Access reports

Access analyzer

Archive rules

Analyzers

Settings

Credential report

Organization activity

Welcome to Identity and Access Management

IAM users sign-in link: <https://dvsbatch4.signin.aws.amazon.com/console>

IAM Resources

Users: 1 Roles: 3

Groups: 0 Identity Providers: 0

Customer Managed Policies: 0

Security Status: 2 out of 5 complete.

Additional Links

- IAM best practices
- IAM documentation
- Web Identity
- Policy Simulator
- Videos, IAI
- additional r

Groups

Delete your root access keys

Activate MFA on your root account

Create individual IAM users

Use groups to assign permissions

Apply an IAM password policy

DVS Technologies Aws & Devops

Create New Group

Group Actions ▾

Search

No records found.

Group Name Users Inline F

Set Group Name

Specify a group name. Group names can be edited any time.

Group Name:

Example: Developers or ProjectAlpha
Maximum 128 characters

Cancel Next Step

DVS Technologies Aws & Devops

Attach Policy

Select one or more policies to attach. Each group can have up to 10 policies attached.

Showing 4 results

	Policy Name	Attached Entities	Creation Time
<input type="checkbox"/>	AmazonDMSRedshiftS3Role	0	2016-04-20 21:05 UTC+...
<input checked="" type="checkbox"/>	AmazonS3FullAccess	0	2015-02-06 22:40 UTC+...
<input type="checkbox"/>	AmazonS3ReadOnlyAccess	0	2015-02-06 22:40 UTC+...
<input type="checkbox"/>	QuickSightAccessForS3StorageManagementAnalyticsReadOnly	0	2017-06-12 22:18 UTC+...

Cancel Previous Next Step

Attach Policy

Select one or more policies to attach. Each group can have up to 10 policies attached.

Showing 10 results

	Policy Name	Attached Entities	Creation Time
<input type="checkbox"/>	AmazonRDSDataFullAccess	0	2018-11-21 01:29 UTC+...
<input type="checkbox"/>	AmazonRDSDirectoryServiceAccess	0	2016-02-26 06:02 UTC+...
<input type="checkbox"/>	AmazonRDSEnhancedMonitoringRole	0	2015-11-11 23:58 UTC+...
<input checked="" type="checkbox"/>	AmazonRDSFullAccess	0	2015-02-06 22:40 UTC+...
<input type="checkbox"/>	AmazonRDSReadOnlyAccess	0	2015-02-06 22:40 UTC+...
<input type="checkbox"/>	AWSBeanstalkRoleRDS	0	2020-06-06 01:46 UTC+...
<input type="checkbox"/>	AWSQuickSightDescribeRDS	0	2015-11-11 03:24 UTC+...
<input type="checkbox"/>	CloudWatchAutomaticDashboardsAccess	0	2019-07-23 14:01 UTC+...
<input type="checkbox"/>	RDSCloudHsmAuthorizationRole	0	2015-02-06 22:41 UTC+...

Cancel Previous Next Step

DVS Technologies Aws & Devops

Review

Review the following information, then click **Create Group** to proceed.

Group Name: dbgroup

Policies: arn:aws:iam::aws:policy/AmazonS3FullAccess
arn:aws:iam::aws:policy/AmazonRDSFullAccess

Edit Group Name | Edit Policies | Create Group

Create New Group | Group Actions ▾

Search

<input checked="" type="checkbox"/>	Group Name	Users	Inline Policy
<input checked="" type="checkbox"/>	dbgroup	0	

DVS Technologies Aws & Devops

IAM > Groups > dbgroup

Summary

Group ARN: arn:aws:iam::907814406801:group/dbgroup

Users (in this group): 0

Path: /

Creation Time: 2020-07-30 19:02 UTC+0400

Users Permissions Access Advisor

Managed Policies

The following managed policies are attached to this group. You can attach up to 10 managed policies.

Attach Policy

Policy Name	Actions
AmazonRDSFullAccess	Show Policy Detach Policy Simulate Policy
AmazonS3FullAccess	Show Policy Detach Policy Simulate Policy

Inline Policies

Creating rajesh user:

Identity and Access Management (IAM)

Dashboard

Access management

Groups

Users

Roles

Policies

Identity providers

Account settings

Access reports

Access analyzer

Archive rules

Analyzers

Add user Delete user

Find users by username or access key

User name	Groups	Access key age	Password age	Last activity
ramesh	None	None	Today	Today

DVS Technologies Aws & Devops

You can add multiple users at once with the same access type and permissions. [Learn more](#)

User name* [+ Add another user](#)

Select AWS access type

Select how these users will access AWS. Access keys and autogenerated passwords are provided in the last step. [Learn more](#)

Access type* Programmatic access
Enables an access key ID and secret access key for the AWS API, CLI, SDK, and other development tools.

AWS Management Console access
Enables a password that allows users to sign-in to the AWS Management Console.

Console password* Autogenerated password
 Custom password

***** [Show password](#)

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

* Required

Cancel

Next: Permissions

Add user

1 2 3 4 5

▼ Set permissions



Copy permissions from existing user

Attach existing policies directly

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](#)

Add user to group

[Create group](#) [Refresh](#)

Search

Showing 1 result

Group ▾

Attached policies

dbgroup

AmazonRDSFullAccess and 1 more

Cancel

Previous

Next: Tags

DVS Technologies Aws & Devops

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
<input type="text" value="Add new key"/>	<input type="text"/>	<input type="button" value="Remove"/>

You can add 50 more tags.

[Cancel](#) [Previous](#) [Next: Review](#)

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

User details

User name	<input type="text" value="rajesh"/>
AWS access type	AWS Management Console access - with a password
Console password type	Custom
Require password reset	No
Permissions boundary	Permissions boundary is not set

Permissions summary

The user shown above will be added to the following groups.

Type	Name
Group	dbgroup

Tags

No tags were added.

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

DVS Technologies Aws & Devops

The screenshot shows the AWS IAM 'Users' page. At the top, there are 'Add user' and 'Delete user' buttons. A search bar is present. Below it is a table with columns: 'User name', 'Group', 'Access key age', 'Password age', 'Last activity', and 'MFA'. Two users are listed: 'rajes' (grouped in 'dbgroup') and 'ramesh' (no group). Red boxes highlight the 'User name' and 'Group' columns for the first row.

Summary

This screenshot shows the 'rajes' user details page. It includes fields for 'User ARN' (arn:aws:iam::907814406801:user/rajes), 'Path' (/), and 'Creation time' (2020-07-30 19:11 UTC+0400). Below these are tabs for 'Permissions', 'Groups (1)', 'Tags', 'Security credentials', and 'Access Advisor'. The 'Permissions' tab is selected, showing a list of applied policies: 'Attached from group' (AmazonRDSFullAccess and AmazonS3FullAccess) and 'AWS managed policy from group dbgroup' (two entries). A red box highlights the 'Attached from group' section, and another red box highlights the 'AWS managed policy from group dbgroup' section. A blue 'Add inline policy' button is also visible.

Note: Please replicate same for "sysadmin group" & "Suresh" user:

DVS Technologies Aws & Devops

Replicating access from existing user:

Set user details

You can add multiple users at once with the same access type and permissions. [Learn more](#)

User name* somesh

[Add another user](#)

Select AWS access type

Select how these users will access AWS. Access keys and autogenerated passwords are provided in the last step. [Learn more](#)

Access type* Programmatic access
Enables an access key ID and secret access key for the AWS API, CLI, SDK, and other development tools.

AWS Management Console access
Enables a password that allows users to sign-in to the AWS Management Console.

Console password* Autogenerated password Custom password
 Show password

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

* Required Cancel [Next: Permissions](#)

Set permissions

[Add user to group](#) [Copy permissions from existing user](#) [Attach existing policies directly](#)

Select an existing user from which to copy policies and group membership.

[Copy permissions from existing user](#)

Showing 3 results

User name	Groups	Attached policies
rajesh	dbgroup	None
ramesh	None	AmazonEC2FullAccess and 1 more
suresh	sysadmin	None

[Cancel](#) [Previous](#) [Next: Tags](#)

DVS Technologies Aws & Devops

Review

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

User details

User name	somesh
AWS access type	AWS Management Console access - with a password
Console password type	Custom
Require password reset	No
Permissions boundary	Permissions boundary is not set

Permissions summary

The following groups and policies will be copied from the selected existing user and attached to the user shown above.

Type	Name
Group	dbgrou

Cancel

Previous

Create user

Add user Delete user

Find users by username or access key				
	User name	Groups	Access key age	Password age
<input type="checkbox"/>	rajesh	dbgrou	None	Today
<input type="checkbox"/>	ramesh	None	None	Yesterday
<input checked="" type="checkbox"/>	somesh	dbgrou	None	Today
<input type="checkbox"/>	suresh	sysadmin	None	Today

DVS Technologies Aws & Devops

Summary

[Delete user](#)

User ARN: arn:aws:iam::907814406801:user/somesh [Edit](#)

Path: /

Creation time: 2020-07-30 19:30 UTC+0400

Permissions Groups (1) Tags Security credentials Access Advisor

▼ Permissions policies (2 policies applied)

[Add permissions](#) [Add inline policy](#)

Policy name	Policy type
Attached from group	AWS managed policy from group dbgroup
▶ AmazonRDSFullAccess	x
▶ AmazonS3FullAccess	x
▶ Permissions boundary (not set)	

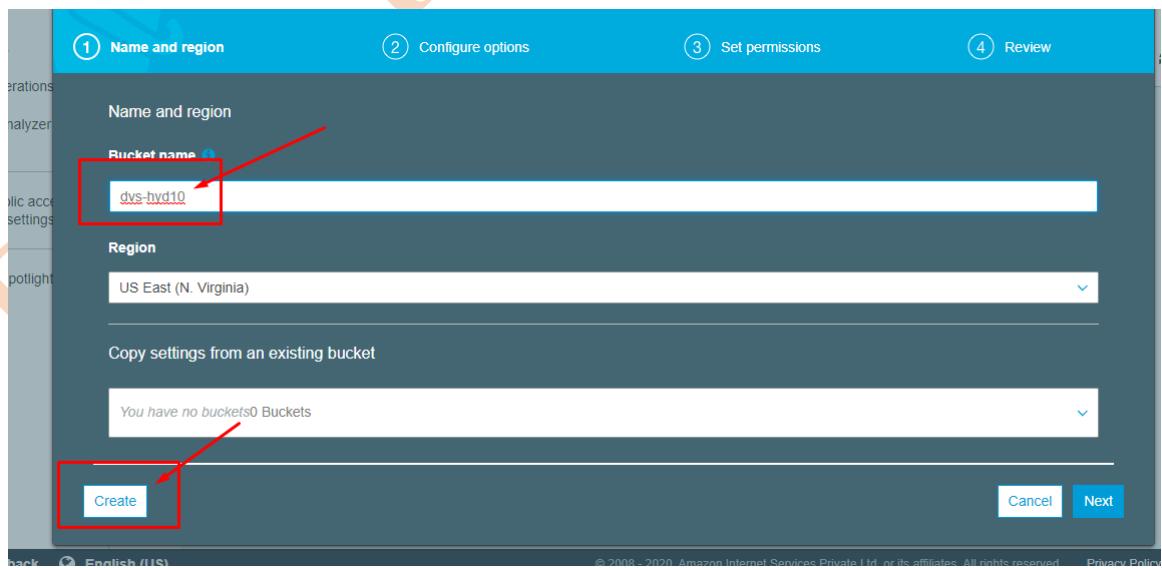
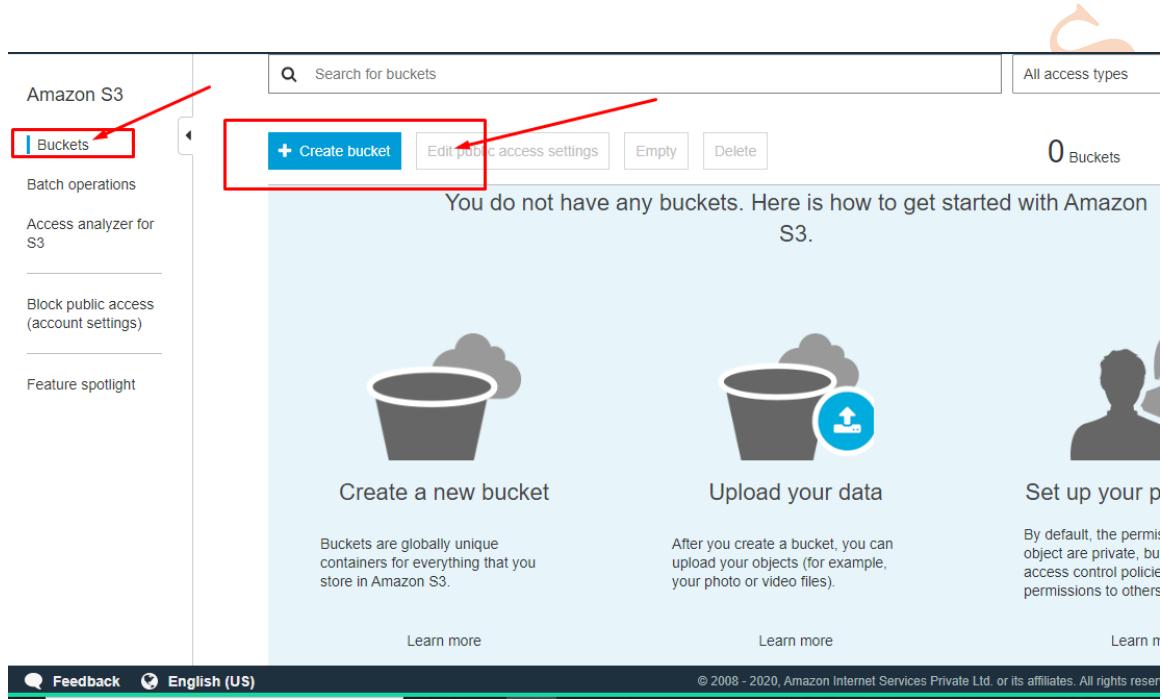
DVSTechin

DVS Technologies Aws & Devops

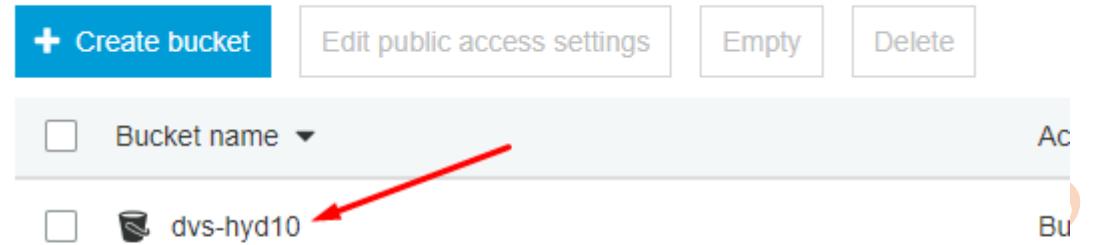
7. Custom Policies

1. Requirement:

Working with Custom policies perform the steps as below.



DVS Technologies Aws & Devops



A screenshot of the AWS S3 console. At the top, there are buttons for '+ Create bucket', 'Edit public access settings', 'Empty', and 'Delete'. Below these are two input fields: 'Bucket name' and 'Access'. The 'Bucket name' field contains 'dvs-hyd10' with a red arrow pointing to it. The 'Access' dropdown shows 'Bucket and objects not public'. A large orange watermark 'DVC' is visible across the center of the screen.

DVS Technologies Aws & Devops

Name and region

Bucket name i

dvs-blr10

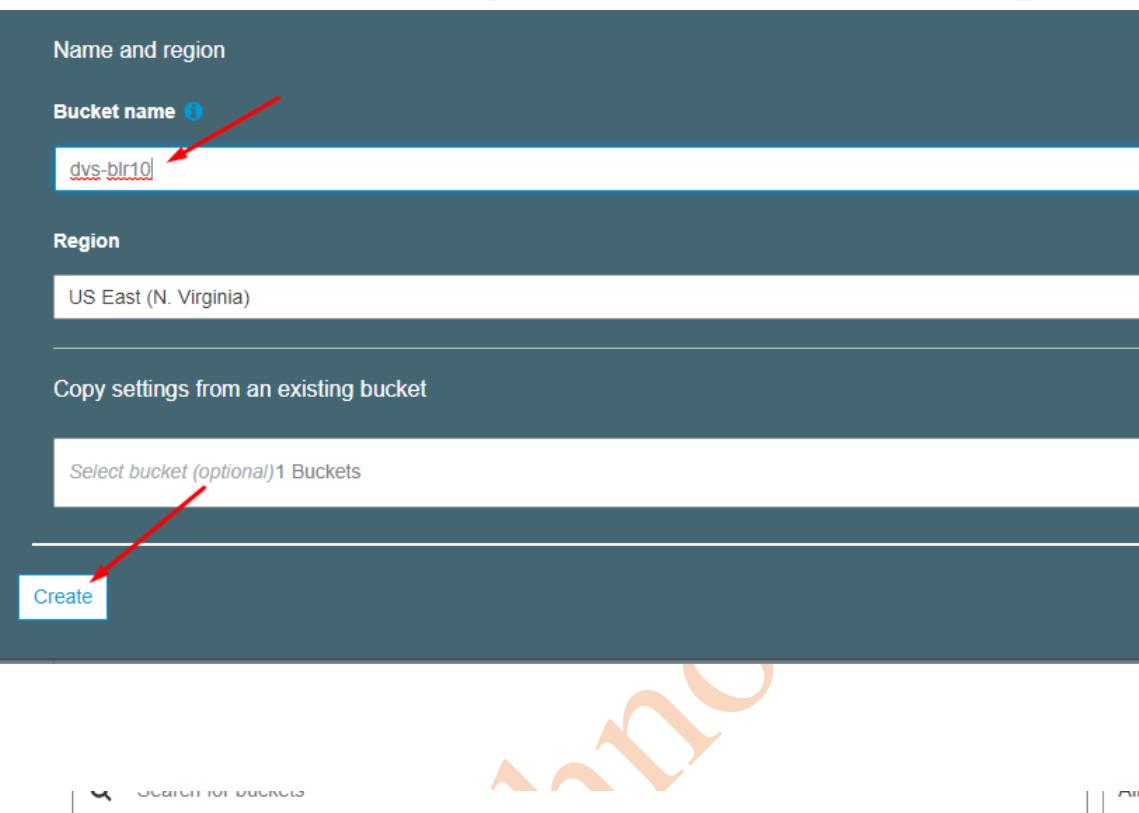
Region

US East (N. Virginia)

Copy settings from an existing bucket

Select bucket (optional) 1 Buckets

Create



+ Create bucket		Edit public access settings	Empty	Delete
<input type="checkbox"/>	Bucket name i		Access i ▼	Region i ▼
<input type="checkbox"/>	 dvs-blr10		Bucket and objects not public	US Ea
<input type="checkbox"/>	 dvs-hyd10		Bucket and objects not public	US Ea

DVS Technologies Aws & Devops

The screenshot shows the AWS Identity and Access Management (IAM) console. On the left sidebar, under 'Access management', the 'Users' option is selected. A red arrow points to this selection. On the right, the 'Add user' page is displayed. At the top, there are 'Add user' and 'Delete user' buttons. Below them is a search bar labeled 'Find users by username or access key'. A table lists four existing users: rajesh, ramesh, somesh, and suresh, each with their respective group assignments, access key age, password age, and last activity date.

You can add multiple users at once with the same access type and permissions. [Learn more](#)

User name* [Add another user](#)

Select AWS access type

Select how these users will access AWS. Access keys and autogenerated passwords are provided in the last step. [Learn more](#)

Access type* **AWS Management Console access**
Enables a password that allows users to sign-in to the AWS Management Console.

Console password* Custom password
 [Show password](#)

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

* Required [Cancel](#) [Next: Permissions](#)

DVS Technologies Aws & Devops

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](#)

Add user to group

[Create group](#) [Refresh](#)

Showing 2 results

Group	Attached policies
<input type="checkbox"/> dbgroup	AmazonRDSFullAccess and 1 more
<input type="checkbox"/> sysadmin	AmazonEC2FullAccess and 1 more

Cancel Previous **Next: Tags**

1 2 3 4 5

Review

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

⚠ This user has no permissions
You haven't given this user any permissions. This means that the user has no access to any AWS service or resource. Consider returning to the previous step and adding some type of permissions.

User details

User name	dvsbatch4
AWS access type	AWS Management Console access - with a password
Console password type	Custom
Require password reset	No
Permissions boundary	Permissions boundary is not set

Tags

No tags were added.

Cancel Previous **Create user**

DVS Technologies Aws & Devops

User Management			
Actions		Add user	Delete user
<input type="text"/> Find users by username or access key			
User name	Groups	Access Type	Last Sign In
<input type="checkbox"/> dvsbatch4	None	No	2023-09-18 10:30:00
<input type="checkbox"/> rajesh	dbgroup	No	2023-09-18 10:30:00
<input type="checkbox"/> ramesh	None	No	2023-09-18 10:30:00
<input type="checkbox"/> somesh	dbgroup	No	2023-09-18 10:30:00
<input type="checkbox"/> suresh	sysadmin	No	2023-09-18 10:30:00

Verifying dvsbatch4 access for s3 buckets:

Welcome to Identity and Access Management

IAM users sign-in link: <https://907814406801.signin.aws.amazon.com/console>

Customize

IAM Resources

Users: 5 Roles: 3
Groups: 2 Identity Providers: 0
Customer Managed Policies: 0

Security Status: 3 out of 5 complete.

Checklist:

- Delete your root access keys
- Activate MFA on your root account
- Create individual IAM users
- Use groups to assign permissions

Additional Information:

- IAM best practices
- IAM documentation
- Web Identity Federation
- Policy Simulator
- Videos, IAM release notes
- additional resources

DVS Technologies Aws & Devops

Sign in as IAM user

Account ID (12 digits) or account alias
907814406801

IAM user name
dvsbatch4

Password
.....|

Sign in

Sign in using root user email

Forgot password?



ent Console

dvsbatch4 @ 9078-1440-6801 ▾ Ohio ▾ Sup

Stay connected to your AWS resources on-the-go

Download the AWS Console Mobile App to your iOS or Android mobile device. [Learn more](#)

DVS Technologies Aws & Devops

AWS Management Console

AWS services

Find Services You can enter names, keywords or acronyms.

S3 Scalable Storage in the Cloud

S3 Glacier Archive Storage in the Cloud

AWS Snow Family Large Scale Data Transport

AWS Transfer Family Fully managed support for SFTP, FTPS and FTP

Athena Query Data in S3 using SQL

Amazon Transcribe Accurate speech recognition

Stay connected to your AWS resources on-the-go

Download the AWS Console Mobile App to your iOS or Android mobile device. Learn more

Explore AWS

Amazon SageMaker Resources Learn about SageMaker's features, use cases, and available workshops. Learn more

Amazon DocumentDB (with MongoDB compatibility)

How to optimize your costs on S3. [Learn more »](#)

Documentation

We've temporarily re-enabled the previous version of the S3 console while we continue to improve the new S3 console experience. [Switch to the new console.](#)

S3 buckets

Discover the console

Search for buckets All access types

+ Create bucket Edit public access settings Empty Delete Buckets 0 Regions

Error Access Denied

Bucket name Access Region Date created

© 2008 - 2020, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. [Privacy Policy](#) [Terms of Use](#)

DVS Technologies Aws & Devops

Now lets work on custom policies:

aws policy generator

About 7,040,000 results (0.45 seconds)

awspolicygen.s3.amazonaws.com › policygen › **AWS Policy Generator**

The AWS Policy Generator is a tool that enables you to create policies that control access to Amazon Web Services (AWS) products and resources. For more ... You've visited this page 5 times. Last visit: 6/17/20

aws.amazon.com › blogs › aws › aws-policy-generator › **AWS Policy Generator | AWS News Blog**

Jan 4, 2011 - The new AWS Policy Generator simplifies the process of creating policy ... I chose to create an IAM policy to regulate access to Route 53.

Videos

Step 1: Select Policy Type

A Policy is a container for permissions. The different types of policies you can create are an **IAM Policy**, an **S3 Bucket Policy**, an **SNS Topic Policy**, a **VPC Endpoint Policy**, and an **SQS Queue Policy**.

Select Type of Policy **IAM Policy**

Step 2: Add Statement(s)

A statement is the formal description of a single permission. See a description of elements that you can use in statements.

Effect **Allow** Deny

AWS Service **Amazon S3** All Services (*)

Actions **1 Action(s) Selected** All Actions (*)

Amazon Resource Name (ARN) **arn:aws:s3::***

Add Conditions (Optional)

Add Statement

DVS Technologies Aws & Devops

You added the following statements. Click the button below to Generate a policy.

Effect	Action	Resource	Conditions
Allow	• s3>ListAllMyBuckets	arn:aws:s3:::*	None

Step 3: Generate Policy

A *policy* is a document (written in the [Access Policy Language](#)) that acts as a container for one or more statements.

[Generate Policy](#) [Start Over](#)

This AWS Policy Generator is provided for informational purposes only, you are still responsible for your use of Amazon Web Services technologies and ensuring that your use is in compliance with all applicable terms and conditions. This AWS Policy Generator is provided as is without warranty of any kind, whether express, implied, or statutory. This AWS Policy

Policy JSON Document

Click below to edit. To save the policy, copy the text below to a text editor. Changes made below will **not be reflected in the policy generator tool**.

```
{ "Version": "2012-10-17", "Statement": [ { "Sid": "Stmt1596208319726", "Action": [ "s3>ListAllMyBuckets" ], "Effect": "Allow", "Resource": "arn:aws:s3:::*" } ] }
```

This AWS Policy Generator is provided for informational purposes only, you are still responsible for your use of Amazon Web Services technologies and ensuring that your use is in compliance with all applicable terms and conditions. This AWS Policy Generator is provided as is without warranty of any kind, whether express, implied, or statutory. This AWS Policy Generator does not modify the applicable terms and conditions governing your use of Amazon Web Services technologies.

[Close](#)

DVS Technologies Aws & Devops

Creating Custom Policy:

The screenshot shows the AWS IAM Policies page. On the left, there's a sidebar with 'Identity and Access Management (IAM)' selected. Under 'Access management', 'Policies' is also selected. A red arrow points from the 'Policies' link in the sidebar to the 'Create policy' button at the top of the main content area. The main content area displays a table of existing policies with columns for 'Policy name', 'Type', 'Used as', and 'Description'. A search bar and filter dropdown are also present.

The screenshot shows the 'Create policy' visual editor. At the top, there are tabs for 'Visual editor' and 'JSON', with 'JSON' selected. Below the tabs, there's a code editor containing a JSON policy document. The code is as follows:

```
2 "Version": "2012-10-17",
3 "Statement": [
4     {
5         "Sid": "Stmt1596208319726",
6         "Action": [
7             "s3>ListAllMyBuckets"
8         ],
9         "Effect": "Allow",
10        "Resource": "arn:aws:s3:::/*"
11    }
12 ]
13 }
```

Below the code editor, it says 'Character count: 144 of 6,144.' In the bottom right corner, there are 'Cancel' and 'Review policy' buttons. A red arrow points from the 'Review policy' button to the button itself.

DVS Technologies Aws & Devops

Name* dvsbatch4s3policy
Use alphanumeric and '+,-,@-' characters. Maximum 128 characters.

Description dvsbatch4s3policy
Maximum 1000 characters. Use alphanumeric and '+,-,@-' characters.

Summary This policy does not grant any permissions. To grant access, policies must have an action that has an applicable resource or condition. For details, choose Show remaining. Learn more

Service	Access level	Resource	Request condition
Allow (0 of 235 services) Show remaining 235			

Cancel Previous Create policy

Attaching Policy to user:

Add user Delete user

User name	Groups	Access key age	Password age
<input checked="" type="checkbox"/> dvsbatch4	None	None	Today
<input type="checkbox"/> rajesh	dbgroup	None	Yesterday
<input type="checkbox"/> ramesh	None	None	Yesterday
<input type="checkbox"/> somesh	dbgroup	None	Today
<input type="checkbox"/> suresh	sysadmin	None	Yesterday

AWS account ID: 907814406801

DVS Technologies Aws & Devops

The screenshot shows the AWS IAM User Summary page for a user named 'dvsbatch4'. The user ARN is arn:aws:iam::907814406801:user/dvsbatch4, the path is /, and it was created on 2020-07-31 18:56 UTC+0400. The 'Permissions' tab is selected. A red arrow points from the 'Users' link in the left sidebar to the 'Users' link in the top navigation bar of the summary page.

Summary

User ARN: arn:aws:iam::907814406801:user/dvsbatch4
Path: /
Creation time: 2020-07-31 18:56 UTC+0400

Permissions Groups Tags Security credentials Access Advisor

Get started with permissions
This user doesn't have any permissions yet. Get started by adding the user to a group, copying permissions from another user, or attach policy directly. [Learn more](#)

Add permissions + Add inline policies

Permissions boundary (not set)

Grant permissions

Use IAM policies to grant permissions. You can assign an existing policy or create a new one.

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

Create policy

Filter policies v dvsbat Showing 1 result

Policy name	Type	Used as
<input checked="" type="checkbox"/> dvsbatch4s3policy	Customer managed	None

Cancel Next: Review

DVS Technologies Aws & Devops

Add permissions to dvsbatch4

1 2

Permissions summary

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

Type	Name
Managed policy	dvsbatch4s3policy

Cancel Previous Add permissions

Identity and Access Management (IAM)

Users > **dvsbatch4**

Summary

User ARN: arn:aws:iam::907814406801:user/dvsbatch4

Path: /

Creation time: 2020-07-31 18:56 UTC+0400

Permissions Groups Tags Security credentials Access Advisor

Permissions policies (1 policy applied)

Add permissions + Add inline policy

Policy name: **dvsbatch4s3policy**

Attached directly: Managed policy

Permissions boundary (not set)

DVS Technologies Aws & Devops

We've temporarily re-enabled the previous version of the S3 console while we continue to improve the new S3 console experience. [Switch to console.](#)

S3 buckets

Search for buckets

All access types

Create bucket Edit public access settings Empty Delete

Bucket name	Access	Region	Date created
dvs-blr10	Error	US East (N. Virginia)	Jul 31 PM G
dvs-hyd10	Error	US East (N. Virginia)	Jul 31 PM G

Upload some data to buckets:

Discover the console

S3 buckets

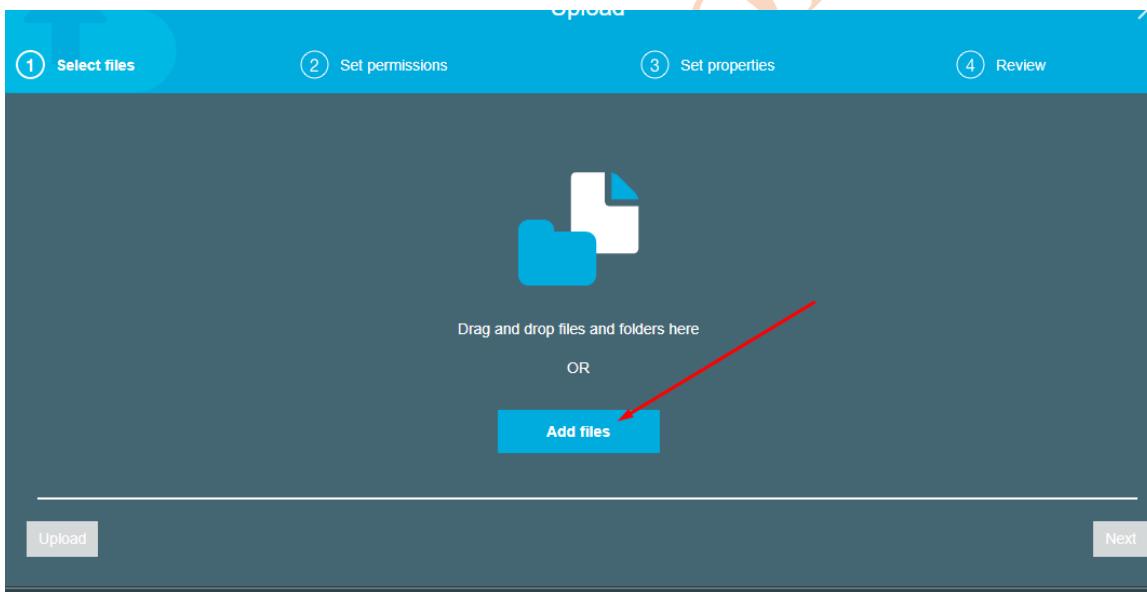
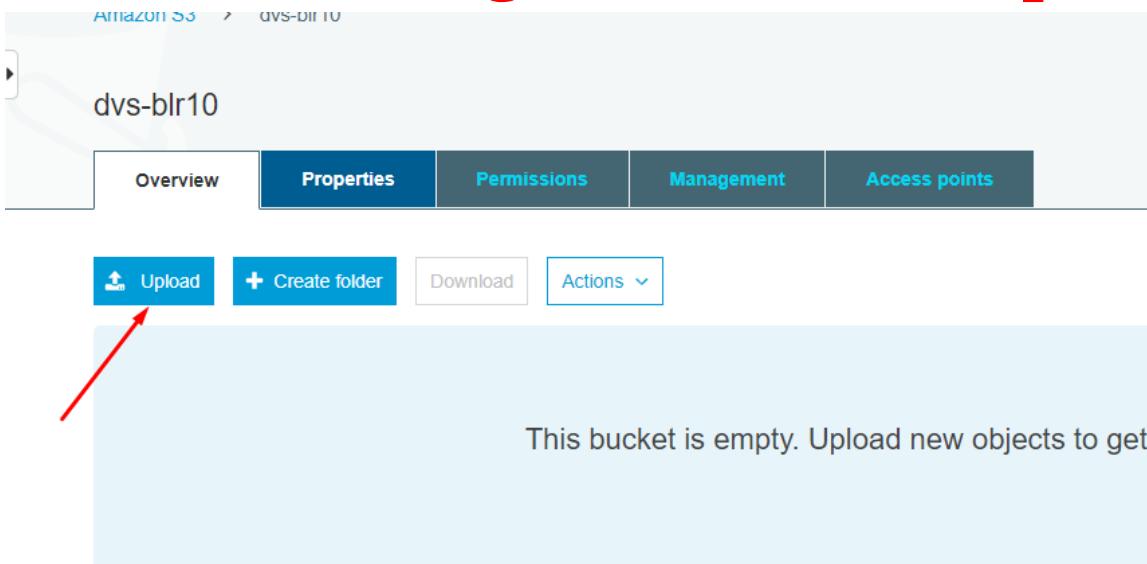
Search for buckets

All access types

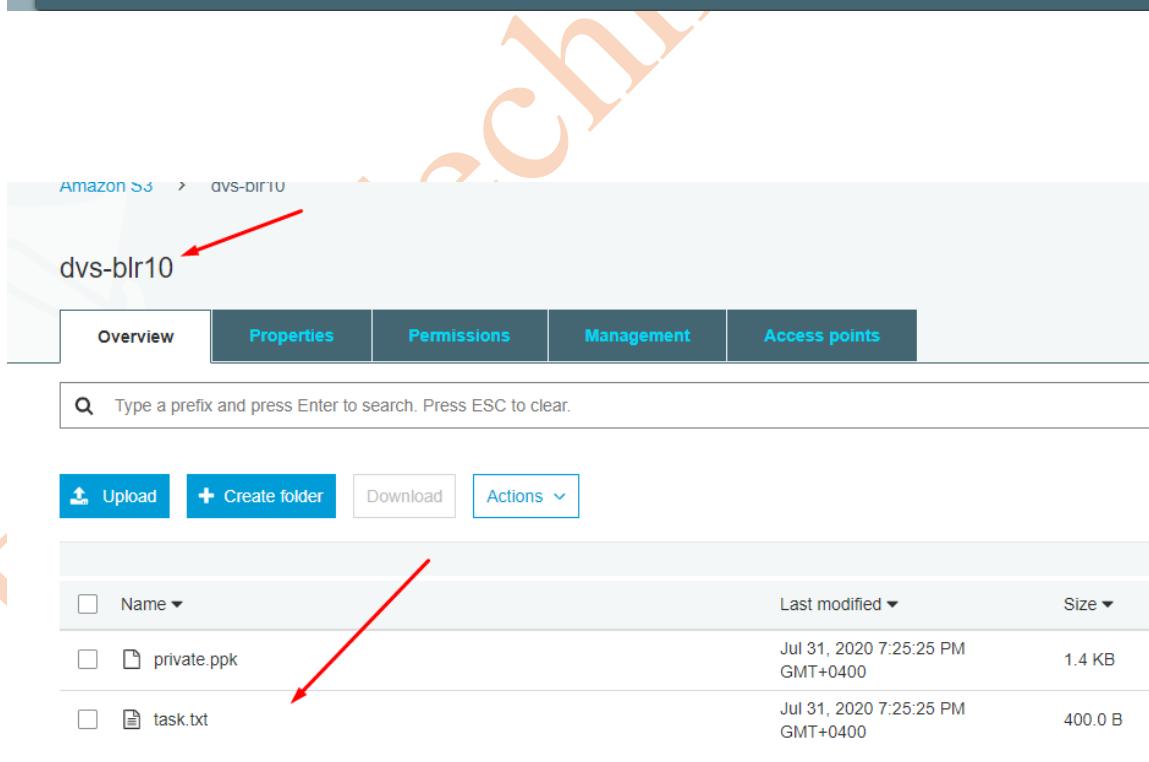
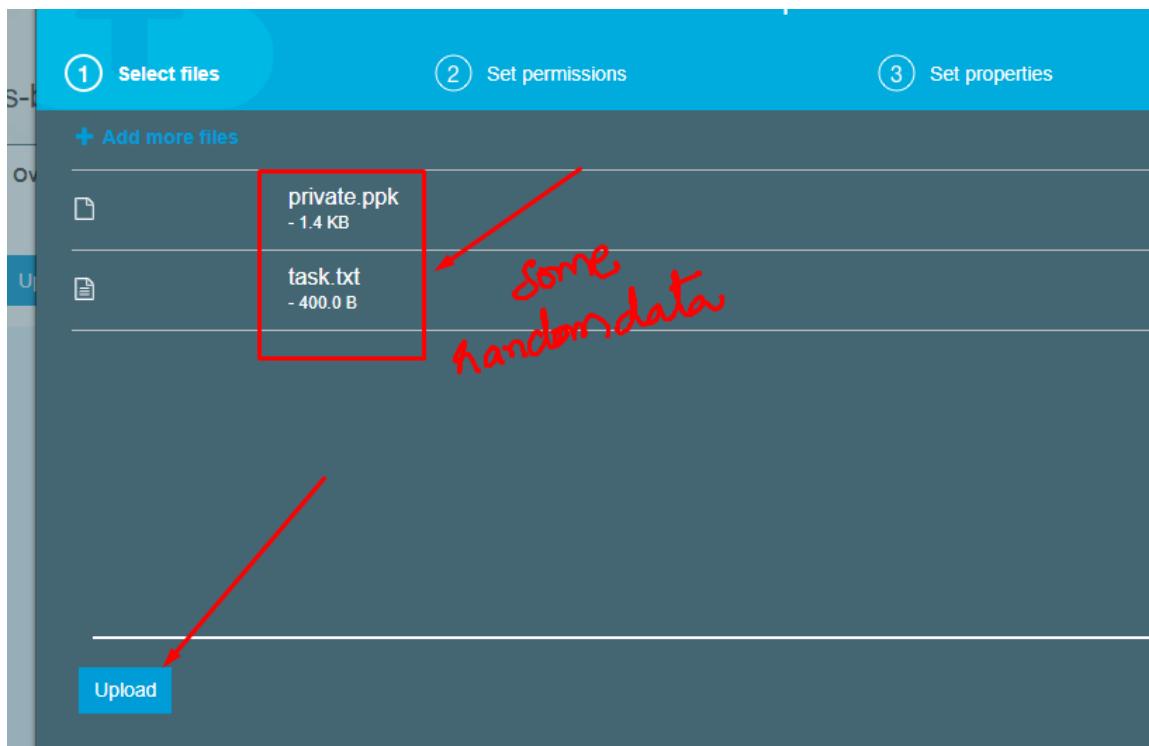
Create bucket Edit public access settings Empty Delete

Bucket name	Access	Region	Date created
dvs-blr10	Bucket and objects not public	US East (N. Virginia)	Jul 31, 2020 6:54:30 PM GMT+0400
dvs-hyd10	Bucket and objects not public	US East (N. Virginia)	Jul 31, 2020 6:53:24 PM GMT+0400

DVS Technologies Aws & Devops



DVS Technologies Aws & Devops



Note: Do the same for other bucket

DVS Technologies Aws & Devops

8. Extending Customized Policies

Granting the permission for a user to a particular buckets data

Step 2: Add Statement(s)

A statement is the formal description of a single permission. See a [description of elements](#) that you can use in statements.

Effect Allow Deny

AWS Service All Services (*)

Actions All Actions (*)

Amazon Resource Name (ARN) ARN should follow the following format: arn:aws:s3:::<bucket_name>/<key_name>. Use a comma to separate multiple values.

Add Conditions (Optional)

You added the following statements. Click the button below to Generate a policy.

Effect	Action	Resource	Conditions
Allow	s3>ListAllMyBuckets	arn:aws:s3:::*	None

Step 3: Generate Policy

You added the following statements. Click the button below to Generate a policy.

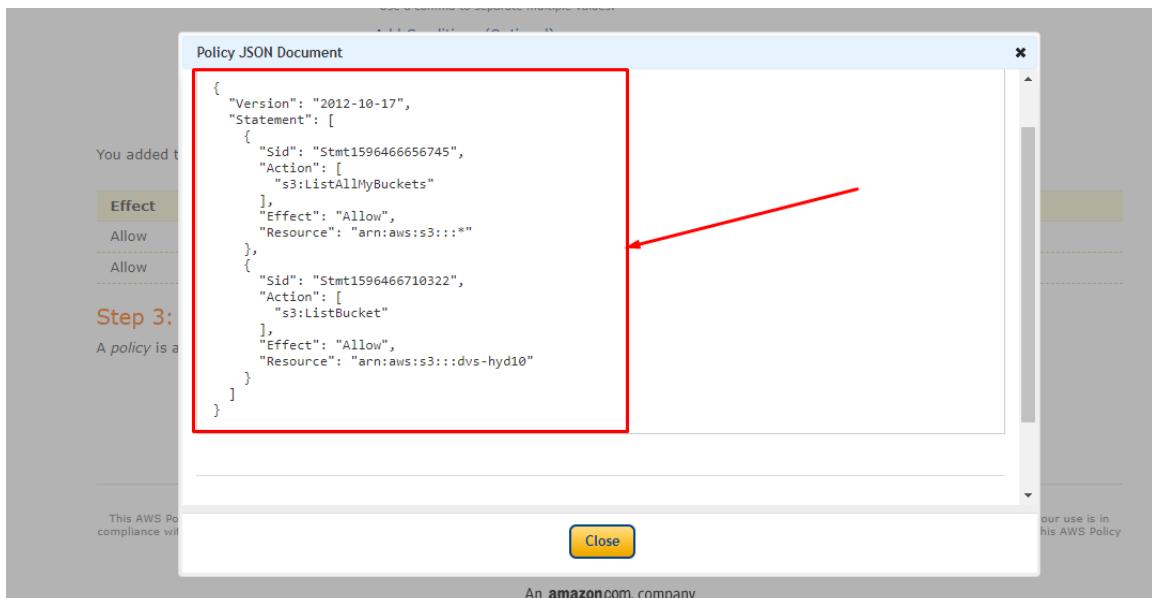
Effect	Action	Resource	Conditions
Allow	s3>ListAllMyBuckets	arn:aws:s3:::*	None
Allow	s3>ListBucket	arn:aws:s3:::dvs-hyd10	None

Step 3: Generate Policy

A policy is a document (written in the Access Policy Language) that acts as a container for one or more statements.

This AWS Policy Generator is provided for informational purposes only, you are still responsible for your use of Amazon Web Services technologies and ensuring that your use is in compliance with all applicable terms and conditions. This AWS Policy Generator is provided **as is** without warranty of any kind, whether express, implied, or statutory. This AWS Policy

DVS Technologies Aws & Devops



The screenshot shows the 'Summary' page for the user 'dvsbatch4'. The left sidebar is expanded to show 'Policies' under 'Users'. A red arrow points from the sidebar to the 'Policies' link. The main summary table includes:

User ARN	arn:aws:iam::907814406801:user/dvsbatch4
Path	/
Creation time	2020-07-31 18:56 UTC+0400

The 'Permissions' tab is selected, showing one policy applied:

- Permissions policies (1 policy applied)
- Add permissions
- Attached directly: dvsbatch4s3policy (Managed policy)

DVS Technologies Aws & Devops

Create policy

Policy actions ▾

Filter policies ▾

Search

Policy name ▾

Type

Used as

Loading...

Visual editor JSON Import managed policy

1: {
2: "Version": "2012-10-17",
3: "Statement": [
4: {
5: "Sid": "Stmt1596466856745",
6: "Action": [
7: "s3>ListAllMyBuckets"
8:],
9: "Effect": "Allow",
10: "Resource": "arn:aws:s3:::/*"
11: },
Character count: 252 of 6,144.

Cancel Review policy

paste your policy here

DVS Technologies Aws & Devops

Name* Use alphanumeric and '+=_-' characters. Maximum 128 characters.

Description Maximum 1000 characters. Use alphanumeric and '+=_-' characters.

Summary
This policy defines some actions, resources, or conditions that do not provide permissions. To grant access, policies must have an action that has an applicable resource or condition. For details, choose Show remaining. [Learn more](#)

Service	Access level	Resource	Request condition
S3	Limited: List	BucketName string like dvs-hyd10	None

Cancel Previous **Create policy**

red

Sales (US)

AWS Services Resource Groups S3 EC2 haris

Groups Users **Policies** Roles Policies Identity providers Account settings

Access reports Access analyzer Archive rules Analyzers Settings Credential report Organization activity Service control policies (SCPs)

Search IAM

dvsbatch4newS3Policy has been created.

Create policy Policy actions

Policy name	Type	Used as	Description
AccessAnalyzerServiceRole...	AWS managed	None	Allow Access Analyzer to analyze i
AdministratorAccess	Job function	None	Provides full access to AWS servic
AlexaForBusinessDeviceSe...	AWS managed	None	Provide device setup access to Alk
AlexaForBusinessFullAccess	AWS managed	None	Grants full access to AlexaForBusi
AlexaForBusinessGateway...	AWS managed	None	Provide gateway execution access
AlexaForBusinessLifesizeD...	AWS managed	None	Provide access to Lifesize AVS de
AlexaForBusinessNetworkP...	AWS managed	None	This policy enables Alexa for Busir
AlexaForBusinessPolyDele...	AWS managed	None	Provide access to Poly AVS device
AlexaForBusinessReadOnly...	AWS managed	None	Provide read only access to Alexa
AmazonAPIGatewayAdmini...	AWS managed	None	Provides full access to create/edit/

DVS Technologies Aws & Devops

Users > dvsbatch4

Summary

User ARN: arn:aws:iam::907814406801:user/dvsbatch4
Path: /
Creation time: 2020-07-31 18:56 UTC+0400

Permissions Groups Tags Security credentials Access Advisor

▼ Permissions policies

Get started with permissions: This user doesn't have any permissions yet. Get started by adding the user to a group, copying permissions from another user, or attaching a policy directly. Learn more

Add permissions Add inline policy

Permissions boundary (not set)

Add permissions to dvsbatch4

Grant permissions

Use IAM policies to grant permissions. You can assign an existing policy or create a new one.

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

Create policy

Filter policies v Q dvsbatch4 Showing 2 results

Policy name	Type	Used as
<input checked="" type="checkbox"/> dvsbatch4newS3Policy	Customer managed	None
<input type="checkbox"/> dvsbatch4s3policy	Customer managed	None

Cancel Next: Review

CLICK ON ADD PERMISSIONS

DVS Technologies Aws & Devops

Amazon S3 > dvs-hyd10

Properties Permissions Management Access points

Type a prefix and press Enter to search. Press ESC to clear.

Upload Create folder Download Actions

Name	Last modified	Size	Storage class
private.ppk	Jul 31, 2020 7:26:29 PM GMT+0400	1.4 KB	Standard
task.txt	Jul 31, 2020 7:26:29 PM GMT+0400	400.0 B	Standard

US East (N. Virginia) Viewing 1 to 2

Amazon S3 > dvs-blr10

Properties Permissions Management Access points

Type a prefix and press Enter to search. Press ESC to clear.

Upload Create folder Download Actions

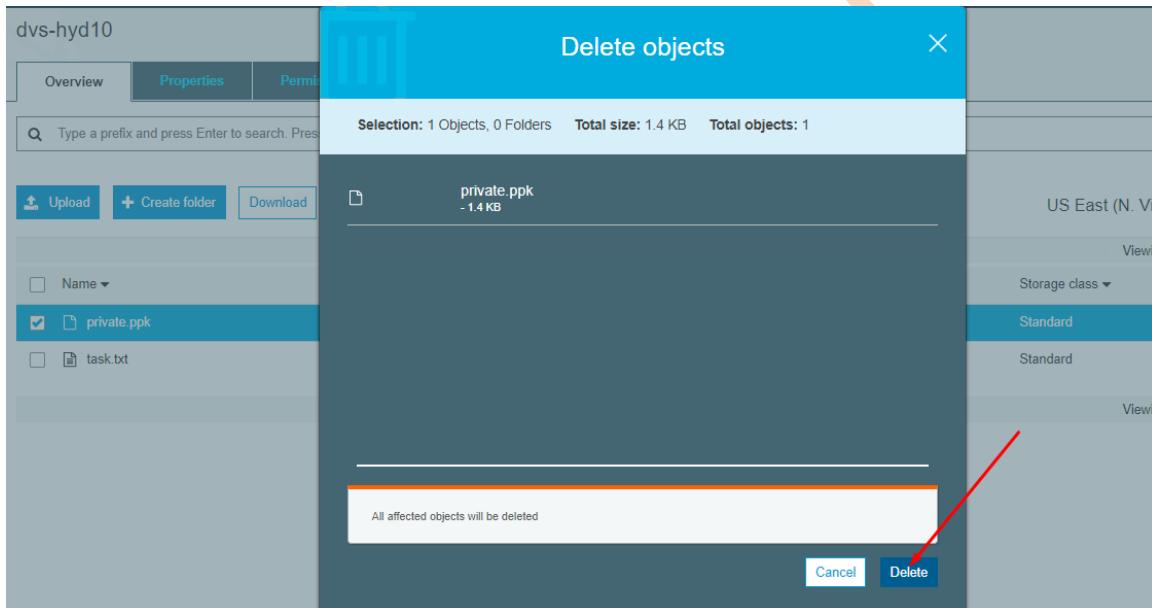
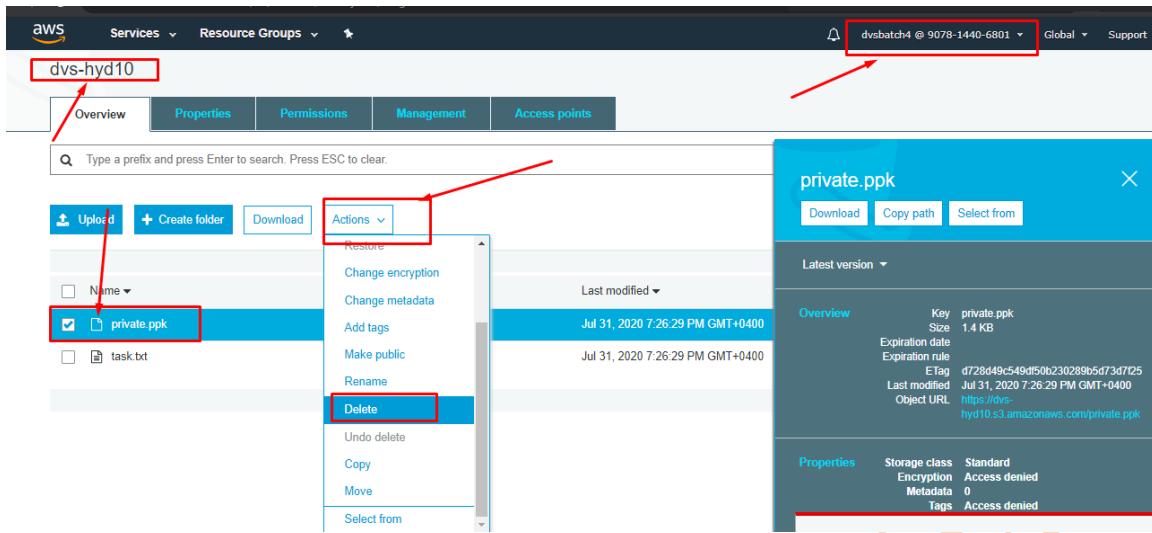
Error
Access Denied

Name	Last modified	Size	Storage class

US East (N. Virginia)

Let's try to delete the object via dvsbatch4 user and let's see if he can delete the data or not

DVS Technologies Aws & Devops



DVS Technologies Aws & Devops

The screenshot shows the AWS S3 console interface. At the top, the bucket name 'dvs-hyd10' is highlighted with a red box. Below the navigation bar, there's a search bar and a row of buttons: Upload, Create folder, Download, and Actions (with a dropdown arrow). The main content area lists two objects: 'private.ppk' and 'task.txt', both modified on Jul 31, 2020. To the right, it says 'US East (N. Virginia)' and 'Viewing 1 to 2'. A red arrow points from the 'Actions' dropdown to a modal window titled 'Delete objects' which shows a progress bar at 100% Failed.

User dvsbatch4 failed to delete the data which is there in dvs-hyd10 bucket

Step 2: Add Statement(s)

A statement is the formal description of a single permission. See a [description of elements](#) that you can use in statements.

The screenshot shows the 'Add Statement' step of the IAM policy editor. It has fields for Effect (Allow), AWS Service (Amazon S3), Actions (s3>ListBucket), and Amazon Resource Name (ARN) (arn:aws:s3:::dvs-hyd10/*). A note below the ARN field specifies the format: arn:aws:s3:::<bucket_name>/<key_name>. Use a comma to separate multiple values. A red arrow points from the 'Add Conditions (Optional)' link to the 'Add Statement' button, which is highlighted with a yellow box.

You added the following statements. Click the button below to Generate a policy.

Effect	Action	Resource	Conditions
Allow	• s3>ListAllMyBuckets	arn:aws:s3:::*	None
Allow	• s3>ListBucket	arn:aws:s3:::dvs-hyd10	None

Step 3: Generate Policy

A *policy* is a document (written in the [Access Policy Language](#)) that acts as a container for one or more statements.

[Generate Policy](#) [Start Over](#)

DVS Technologies Aws & Devops

ARN should follow the following format: arn:aws:s3:::<bucket_name>/<key_name>.

Policy JSON Document
Changes made below will **not be reflected in the policy generator tool**.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "Stmt1596468046560",  
            "Action": [  
                "s3:DeleteObject"  
            ],  
            "Effect": "Allow",  
            "Resource": "arn:aws:s3:::dvs-hyd10/*"  
        }  
    ]  
}
```

This AWS Policy Generator is provided for informational purposes only, you are still responsible for your use of Amazon Web Services technologies and ensuring that your use is in compliance with all applicable terms and conditions. This AWS Policy Generator is provided as is without warranty of any kind, whether express, implied, or statutory. This AWS Policy Generator does not modify the applicable terms and conditions governing your use of Amazon Web Services technologies.

Policies > dvsbatch4newS3Policy

Summary Delete policy

Policy ARN: arn:aws:iam::907814406801:policy/dvsbatch4newS3Policy Edit

Description: dvsbatch4newS3Policy

Permissions Policy usage Policy versions Access Advisor

Policy summary { } JSON Edit policy ?

```
1 {  
2     "Version": "2012-10-17",  
3     "Statement": [  
4         {  
5             "Sid": "Stmt1596466656745",  
6             "Action": [  
7                 "s3>ListAllMyBuckets"  
8             ],  
9             "Effect": "Allow",  
10            "Resource": "arn:aws:s3:::/*"  
11        },  
12        {  
13            "Sid": "Stmt1596466710322",  
14            "Action": [  
15                "s3>ListBucket"  
16            ]  
17        }  
18    ]  
19}
```

DVS Technologies Aws & Devops

A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a policy in the visual editor and using JSON. [Learn more](#)

Visual editor **JSON** Import managed policy

```
1 {  
2     "Version": "2012-10-17",  
3     "Statement": [  
4         {  
5             "Sid": "Stmt1596466656745",  
6             "Action": [  
7                 "s3>ListAllMyBuckets"  
8             ],  
9             "Effect": "Allow",  
10            "Resource": "arn:aws:s3:::/*"  
11        },  
12        {  
13            "Sid": "Stmt1596466710322",  
14            "Action": [  
15                "s3>ListBucket"  
16            ]  
17        }  
18    ]  
19}
```

Paste your new policy data

Character count: 359 of 6,144.

Cancel **Review policy**

AWS Services Resource Groups ★ dvsbatch4 @ 9078-1440-6801 Global

Amazon S3 dvs-hyd10

dvs-hyd10

Overview Properties Permissions Management Access points

Type a prefix and press Enter to search. Press ESC to clear.

Upload Create folder Download Actions

Name private.ppk task.txt

Last modified Size Storage class

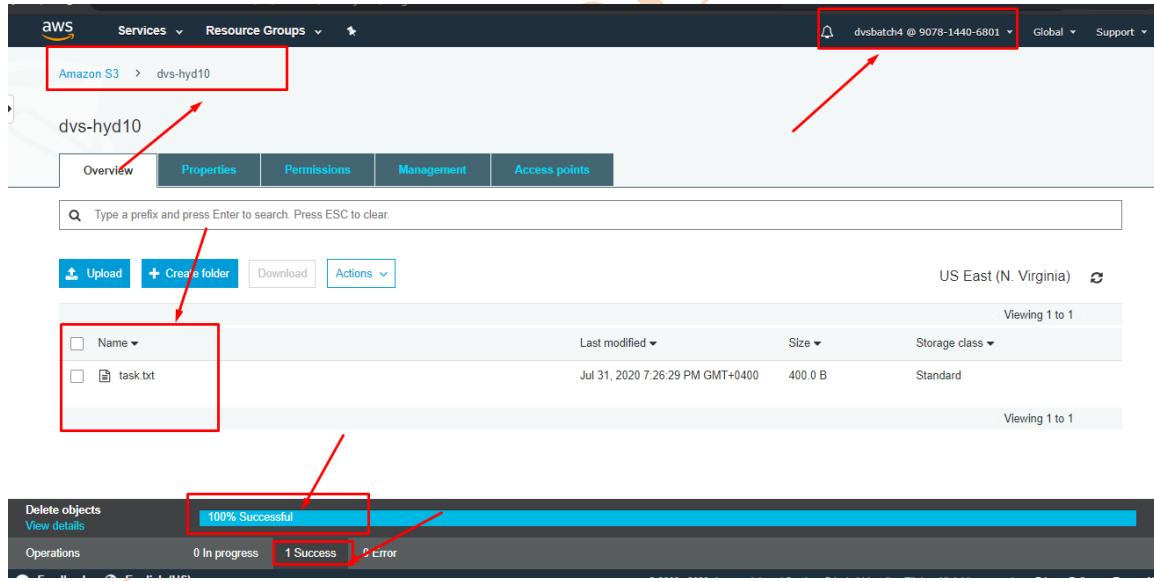
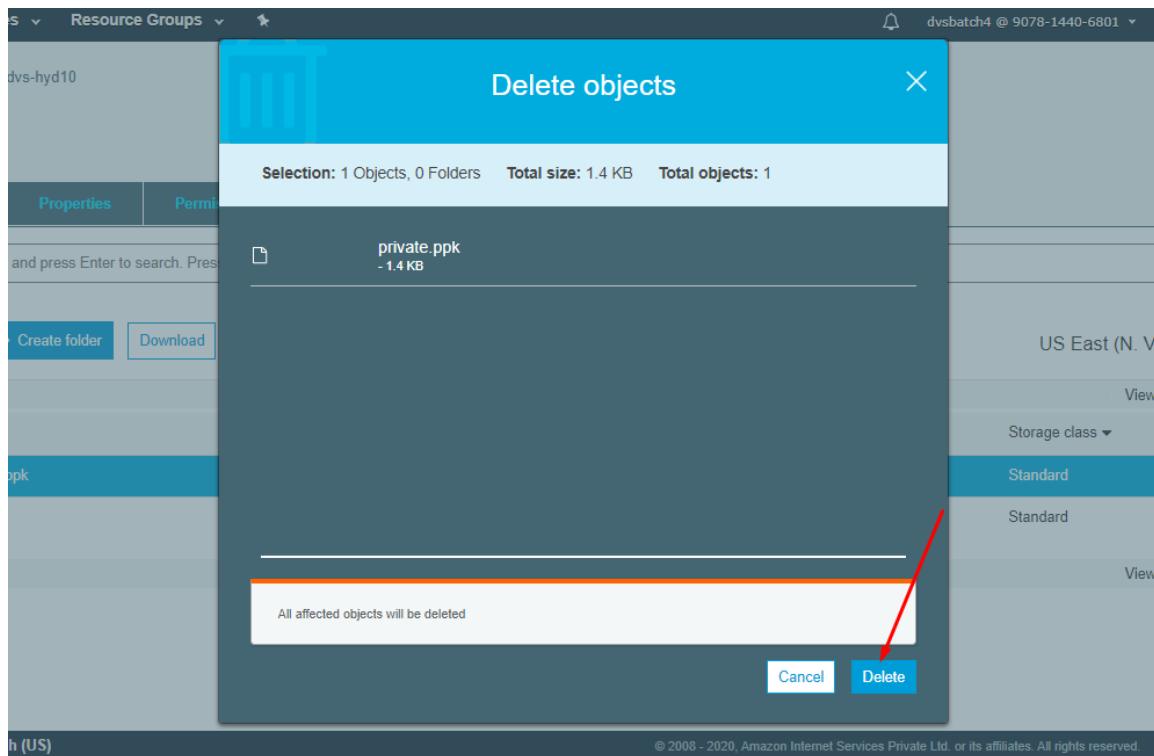
	Last modified	Size	Storage class
private.ppk	Jul 31, 2020 7:26:29 PM GMT+0400	1.4 KB	Standard
task.txt	Jul 31, 2020 7:26:29 PM GMT+0400	400.0 B	Standard

US East (N. Virginia) Viewing 1 to 2

Restore Change encryption Change metadata Add tags Make public Rename Delete Undo delete Copy

Viewing 1 to 2

DVS Technologies Aws & Devops



DVS Technologies Aws & Devops

9. Password Policy

The screenshot shows the AWS IAM console. The left sidebar is titled 'Identity and Access Management (IAM)' and includes sections for Dashboard, Access management, Access reports, and Account settings. The 'Account settings' section is highlighted with a red arrow. The main content area is titled 'Password policy' and contains a sub-section for 'Security Token Service (STS)'. A red box surrounds the 'Set password policy' button. Below it, a paragraph explains what a password policy is. The 'Select your account password policy requirements:' section contains several checkboxes with red arrows pointing to them. These requirements include: Enforce minimum password length (set to 6 characters), Require at least one uppercase letter from Latin alphabet (A-Z), Require at least one lowercase letter from Latin alphabet (a-z), Require at least one number, Require at least one non-alphanumeric character (!@#\$%^&*()_+=[]{}'), and Enable password expiration (checked). Below these requirements, there is a field to set password expiration to 30 days. At the bottom right, there are 'Cancel' and 'Save changes' buttons.