

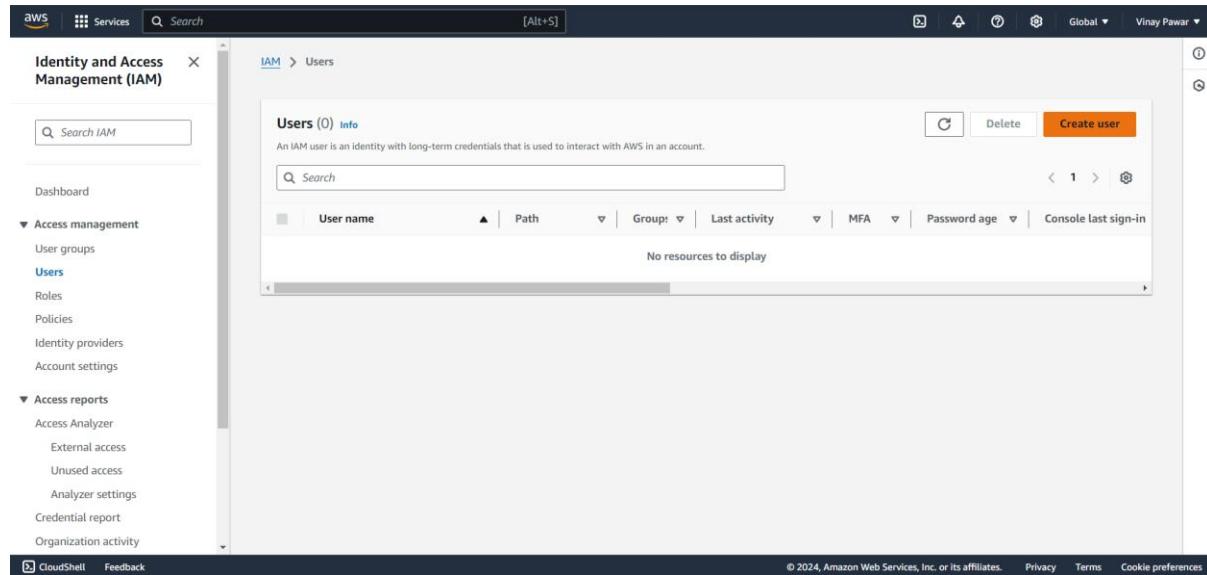
Linux and Cloud Computing Exam

Name: Vinay Jeevan Pawar

ID: 240840325070

1. Create a new IAM user, policy granting EC2 full access.

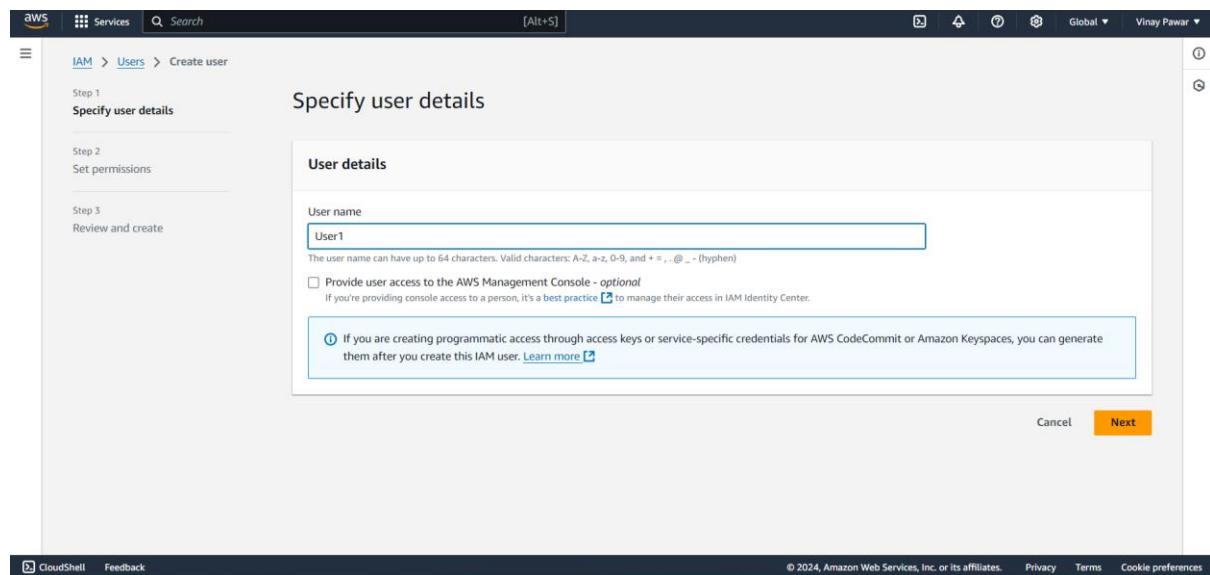
creating IAM user.



The screenshot shows the AWS Identity and Access Management (IAM) service interface. The left sidebar is titled 'Identity and Access Management (IAM)' and contains the following navigation items:

- Dashboard
- Access management
 - User groups
 - Users** (selected)
 - Roles
 - Policies
 - Identity providers
 - Account settings
- Access reports
 - Access Analyzer
 - External access
 - Unused access
 - Analyzer settings
 - Credential report
 - Organization activity

The main content area is titled 'Users (0) Info' and displays the message: 'An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.' A search bar and a table header with columns 'User name', 'Path', 'Group', 'Last activity', 'MFA', 'Password age', and 'Console last sign-in' are visible. Below the table, it says 'No resources to display'. At the top right, there are 'Create user' and 'Delete' buttons. The bottom right corner includes copyright information: '© 2024, Amazon Web Services, Inc. or its affiliates.' and links for 'Privacy', 'Terms', and 'Cookie preferences'.



The screenshot shows the 'Specify user details' step of the IAM User creation wizard. The left sidebar shows the steps: Step 1 (selected), Step 2 (Set permissions), and Step 3 (Review and create). The main form is titled 'User details' and contains a 'User name' field with the value 'User1'. Below the field, a note states: 'The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ _ - (hyphen)'. There is also an optional checkbox: 'Provide user access to the AWS Management Console - optional' with the note: 'If you're providing console access to a person, it's a best practice to manage their access in IAM Identity Center.' A note at the bottom of the form says: '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](#)'.

Setting permission to the IAM user.

The screenshot shows the 'Set permissions' step of the 'Create user' wizard. It includes a sidebar with steps 1-3: 'Specify user details', 'Set permissions', and 'Review and create'. The main area has a 'Permissions options' section with three choices: 'Add user to group', 'Copy permissions', and 'Attach policies directly'. The 'Attach policies directly' option is selected. Below is a 'Permissions policies' table with one policy listed: 'AmazonEC2FullAccess' (AWS managed, 0 matches). A search bar at the top right filters results by 'ec2f'.

Permissions policies (1/1241)

Policy name	Type	Attached entities
AmazonEC2FullAccess	AWS managed	0
AWSEC2FleetServiceRolePolicy	AWS managed	0

The screenshot shows the 'Review and create' step. It displays user details (User name: User1, Console password type: None, Require password reset: No) and a 'Permissions summary' table showing the attached policy. It also includes a 'Tags - optional' section with a note about key-value pairs and a 'Add new tag' button.

User details

User name	Console password type	Require password reset
User1	None	No

Permissions summary

Name	Type	Used as
AmazonEC2FullAccess	AWS managed	Permissions policy

Tags - optional

No tags associated with the resource.

Add new tag

User created successfully.

The screenshot shows the AWS IAM dashboard. A green success message box says 'User created successfully' with a link to 'View user'. The main area shows a 'Users (1) info' table with one row for 'User1'. The sidebar contains links for Identity and Access Management (IAM), 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), and CloudShell/Feedback.

Identity and Access Management (IAM)

Users (1) info

User name	Path	Groups	Last activity	MFA	Password age	Console last sign-in
User1	/	0	-	-	-	-

2. Using aws cli configured with this IAM user's credentials, list all EC2 instances and perform start/stop operations on EC2 instance that you launched.

Going under users → Security credentials →

The screenshot shows the AWS Identity and Access Management (IAM) console. On the left, there is a navigation sidebar with the following menu items:

- Identity and Access Management (IAM)
- Dashboard
- Access management
 - User groups
 - Users** (selected)
 - Roles
 - Policies
 - Identity providers
 - Account settings
- Access reports
 - Access Analyzer
 - External access
 - Unused access
 - Analyzer settings
 - Credential report
 - Organization activity

The main content area displays the details for a user named "User1". The "Summary" tab is selected, showing the following information:

ARN	Console access	Access key 1
arn:aws:iam::831926607414:user/User1	Disabled	Create access key
Created October 21, 2024, 14:07 (UTC+05:30)	Last console sign-in -	

Below the summary, there are tabs for "Permissions", "Groups", "Tags", "Security credentials" (which is selected), and "Last Accessed".

The "Console sign-in" section contains a "Console sign-in link" (https://831926607414.signin.aws.amazon.com/console) and a "Console password" status (Not enabled). There is also a "Enable console access" button.

The "Multi-factor authentication (MFA) (0)" section has buttons for "Remove", "Resync", and "Assign MFA device".

At the bottom of the page, there are links for "CloudShell", "Feedback", and copyright information: "© 2024, Amazon Web Services, Inc. or its affiliates.", "Privacy", "Terms", and "Cookie preferences".

users → Security credentials → Access Key →

The screenshot shows the AWS Identity and Access Management (IAM) service interface. On the left, there's a sidebar with navigation links like Dashboard, Access management, and Access reports. The main content area is titled 'Access keys (0)' and contains a message: 'No access keys. As a best practice, avoid using long-term credentials like access keys. Instead, use tools which provide short term credentials.' Below this is a large 'Create access key' button. At the bottom of the page, there's a section for 'SSH public keys for AWS CodeCommit (0)' with a similar 'Create access key' button.

users → Security credentials → Access Key → create access key → Command line interface

This screenshot shows the second step of the 'Create Access Key' wizard. It asks the user to choose a use case for the new access key. The 'Command Line Interface (CLI)' option is selected and highlighted with a blue border. Other options include Local code, Application running on an AWS compute service, Third-party service, Application running outside AWS, and Other. At the bottom of the page, there's a section for 'Alternatives recommended'.

Set any description tag here ‘ec2instance’

The screenshot shows the 'Set description tag - optional' step in the AWS IAM 'Create access key' wizard. The 'Description tag value' field contains 'ec2instance'. The 'Create access key' button is highlighted in orange at the bottom right.

Save access key and secret access key

The screenshot shows the 'Access key created' confirmation message: 'This is the only time that the secret access key can be viewed or downloaded. You cannot recover it later. However, you can create a new access key any time.' Below this, the 'Access key' section shows the key 'AKIA4DMVQTY3C2Q55LHW' and the secret key 'We+PMuCKWhHnley2Yxnj3aNbKfhkftXgMavgz/T' with a 'Hide' link. A green box indicates the secret key has been copied. The 'Access key best practices' section lists several guidelines. At the bottom are 'Download .csv file' and 'Done' buttons.

Launch an EC2 instance

The screenshot shows the 'Launch an instance' wizard in the AWS Management Console. The current step is 'Name and tags'. A modal window titled 'Summary' is open, showing the configuration details:

- Number of instances: 1
- Software Image (AMI): Amazon Linux 2023 AMI (ami-04a57924ffe27da53)
- Virtual server type (instance type): t2.micro
- Firewall (security group): New security group
- Storage (volumes): 1 volume(s) - 8 GiB

A tooltip for the 'Free tier' badge indicates: "Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 750 hours of public IPv4 address usage per month, 30 GiB of EBS storage, 2 million I/Os, 1 GiB of snapshots, and 1 million AWS Lambda executions."

Select amazon linux free tier eligible.

The screenshot shows the AWS Marketplace search results for AMIs. The search bar contains "Search for an AMI by entering a search term e.g. "Windows"" and the results are filtered by "Free tier eligible".

Refine results filters include:

- Clear all filters
- Free tier only
- OS category: All Linux/Unix, All Windows
- Architecture: 64-bit (Arm), 32-bit (x86), 64-bit (x86), 64-bit (Mac)

The results table shows three items:

- Amazon Linux 2023 AMI (ami-04a57924ffe27da53)
 - Description: Amazon Linux 2023 is a modern, general purpose Linux-based OS that comes with 5 years of long term support. It is optimized for AWS and designed to provide a secure, stable and high-performance execution environment to develop and run your cloud applications.
 - Platform: amazon
 - Root device type: ebs
 - Virtualization: hvm
 - ENAs enabled: Yes
 - Options: Select (button), 64-bit (x86), uefi-preferred, 64-bit (Arm), uefi
- Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type (ami-0e0e417dfa2028266)
 - Description: Amazon Linux 2 comes with five years support. It provides Linux kernel 5.10 tuned for optimal performance on Amazon EC2, systemd 219, GCC 7.3, Glibc 2.26, Binutils 2.29.1, and the latest software packages through extras. This AMI is the successor of the Amazon Linux AMI that is now under maintenance only mode and has been removed from this wizard.
 - Platform: amazon
 - Root device type: ebs
 - Virtualization: hvm
 - ENAs enabled: Yes
 - Options: Select (button), 64-bit (x86), 64-bit (Arm)
- macOS Sonoma (ami-0009ef477047d07a97)
 - Description: macOS Sonoma
 - Platform: macos
 - Root device type: ebs
 - Virtualization: hvm
 - ENAs enabled: Yes
 - Options: Select (button)

The screenshot shows the AWS AMI Catalog interface. On the left, a search bar and navigation tabs (AMI from catalog, Recents, Quick Start) are visible. A specific AMI, "Amazon Linux 2023 AMI", is selected, indicated by a green "Verified provider" button and a blue "Free tier eligible" button. The AMI details include its name, description (a modern, general purpose Linux-based OS), image ID (ami-04a37924ffe27da53), and a sample username (ec2-user). A table provides metadata: Catalog (Quick Start AMIs), Published (2024-10-11T16:52:38.000Z), Architecture (x86_64), Virtualization (hvm), Root device type (ebs), and ENA Enabled (Yes). On the right, the "Summary" section shows 1 instance selected. It includes fields for Software Image (AMI), Firewall (security group), and Storage (volumes). A tooltip for the Free tier indicates it covers 750 hours of t2.micro usage per month. The bottom navigation bar includes CloudShell, Feedback, and various AWS service icons.

Select instance type t2.micro and key pair also.

aws Services Search [Alt+S]

Instance type [Info](#) | [Get advice](#)

Instance type

t2.micro Free tier eligible

Family: t2 1 vCPU 1 GiB Memory Current generation: true

On-Demand Linux base pricing: 0.017 USD per Hour

On-Demand Windows base pricing: 0.017 USD per Hour

On-Demand RHEL base pricing: 0.0288 USD per Hour

On-Demand SUSE base pricing: 0.0124 USD per Hour

All generations [Compare instance types](#)

Additional costs apply for AMIs with pre-installed software

Key pair (login) [Info](#)

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - required [Create new key pair](#)

Network settings [Info](#)

Network [Info](#)

vpc-0d3b55152378b1148

Summary

Number of instances [Info](#)

Software Image (AMI)
Amazon Linux 2023 AMI
ami-04a37924ffe27da53

Virtual server type (instance type)
t2.micro

Firewall (security group)
New security group

Storage (volumes)
1 volume(s) - 8 GiB

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 750 hours of public IPv4 address usage per month, 30 GiB of EBS storage, 2 million IOs, 1 GB of snapshots, and

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences ENG IN 21-10-2024

allow ssh , https, http.

aws Services Search [Alt+S]

Network settings [Info](#)

Network [Info](#)

vpc-0d3b55152378b1148

Subnet [Info](#)

No preference (Default subnet in any availability zone)

Auto-assign public IP [Info](#)

Enable

Additional charges apply when outside of **free tier allowance**

Firewall (security groups) [Info](#)

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

[Create security group](#) [Select existing security group](#)

We'll create a new security group called 'launch-wizard-9' with the following rules:

Allow SSH traffic from Helps you connect to your instance

Allow HTTPS traffic from the internet To set up an endpoint, for example when creating a web server

Allow HTTP traffic from the internet To set up an endpoint, for example when creating a web server

Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

Summary

Number of instances [Info](#)

Software Image (AMI)
Amazon Linux 2023 AMI
ami-04a37924ffe27da53

Virtual server type (instance type)
t2.micro

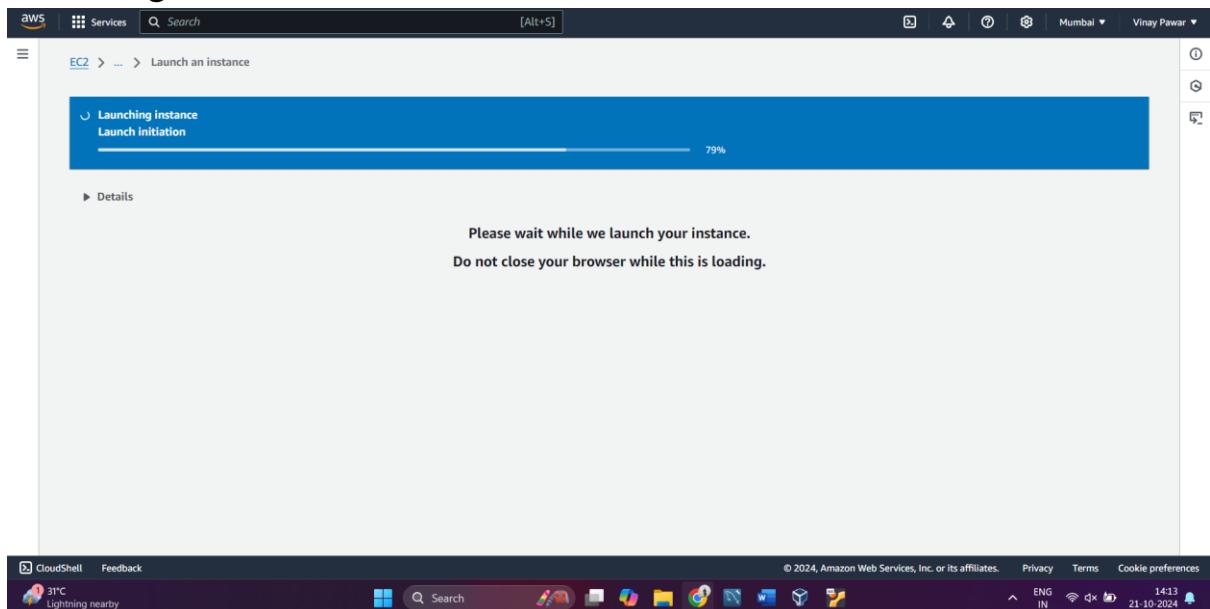
Firewall (security group)
New security group

Storage (volumes)
1 volume(s) - 8 GiB

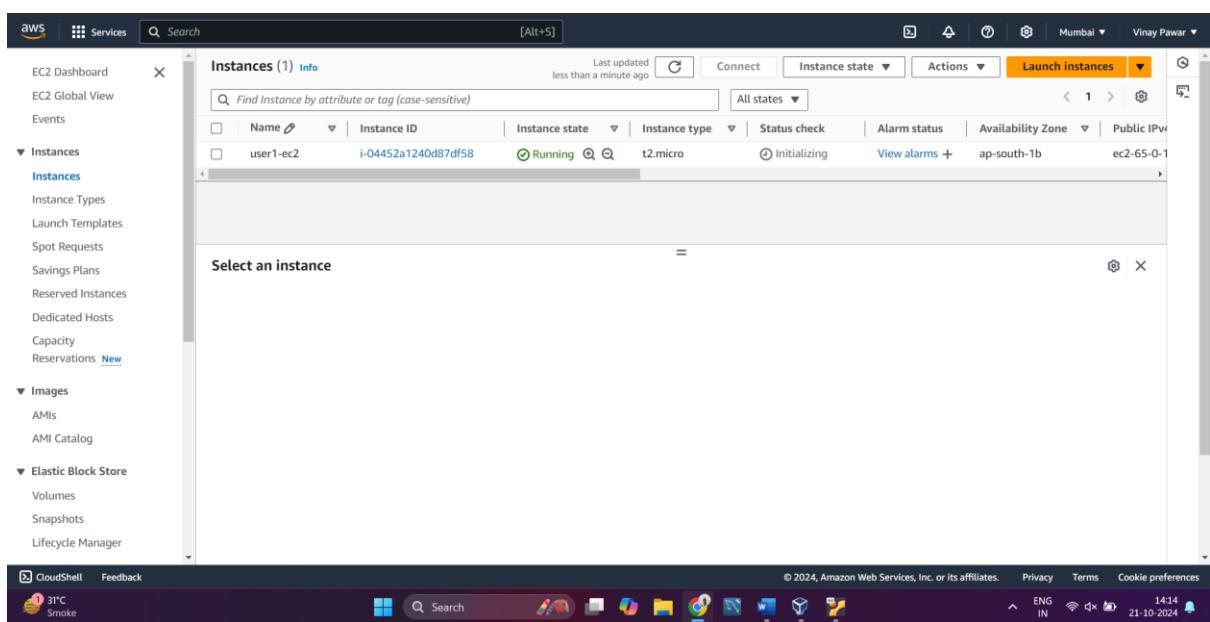
Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 750 hours of public IPv4 address usage per month, 30 GiB of EBS storage, 2 million IOs, 1 GB of snapshots, and

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences ENG IN 21-10-2024

Launching instance.



Instance is created successfully.



Assigning MFA device:

The screenshot shows the AWS IAM 'Select MFA device' configuration interface. In the 'MFA device name' field, the value 'iamec2' is entered. Under 'Device options', the 'Passkey or security key' option is selected, with a sub-instruction: 'Authenticate using your fingerprint, face, or screen lock. Create a passkey on this device or use another device, like a FIDO2 security key.' A modal window titled 'Create a passkey to sign in to aws.amazon.com?' is displayed, asking if the user wants to use a passkey for faster sign-in across devices. It includes fields for 'User' and 'Passkey', and buttons for 'Save another way', 'Create', and 'Cancel'. Below the modal, the steps are outlined: Step 1 of 2: Create a passkey on this device or if you're using another device, connect it now. Step 2 of 2: Follow instructions from your browser. The status bar at the bottom indicates 'Loading'.

Pass-Key is: 123456

The screenshot shows the AWS Identity and Access Management (IAM) service. In the top navigation bar, there is a message: "Passkey MFA device assigned As a security best practice, we encourage registering multiple devices in the case that your primary method is lost, disabled, or unavailable. Choose any of your MFA devices to use to sign in to your AWS account." Below this, the "User1" details page is displayed. The "Summary" section shows the ARN (arn:aws:iam::831926607414:user/User1), Console access status (Disabled), and two Access keys. The "Security credentials" tab is selected. Below the summary, there is a "Console sign-in" section with fields for "Console sign-in link" and "Console password". At the bottom of the page, there are tabs for "Permissions", "Groups", "Tags (2)", and "Security credentials". The left sidebar lists various IAM management options like Access management, User groups, and Access reports.

Aws CLI –

For scripting in AWS CLI we need to use cmd ,

The screenshot shows a Microsoft Command Prompt window running on a Windows operating system. The command history shows the user executing the following commands:

```
C:\Users\vinay>aws --version
aws-cli/2.18.10 Python/3.12.6 Windows/11 exe/AMD64
C:\Users\vinay>aws configure
AWS Access Key ID [*****KYNW]: AKIA4DMVQTY3C2Q55LHW
AWS Secret Access Key [*****ibZN]: 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
Default region name [ap-south-1]: ap-south-1
Default output format [json]: json
```

The background shows the AWS IAM service interface with the "Security credentials" tab selected for the "User1" user. The left sidebar of the IAM interface is visible, showing options like Access management, User groups, and Access reports.

Under cmd “aws --version” this command is used to check out version of current aws cli.

After that “aws configure” this command is used to configure your aws setting and it will connect your IAM user to the AWS CLI,

This will need the AWS access key id which is generated under access key generator.

After creating AWS access key it will provide AWS access key id and AWS secret access key.

After that it will ask for region.

And Default output format.

After providing all the details it will connect with the user.

Creating role.

The screenshot shows the AWS IAM Roles page. On the left sidebar, under 'Access management' > 'Roles', there are three listed:

- Role name: AWSServiceRoleForSupport
- Role name: AWSServiceRoleForTrustedAdvisor
- Role name: (unnamed)

Below the table, there are three sections: 'Access AWS from your non AWS workloads', 'X.509 Standard', and 'Temporary credentials'.

Take aws service and Use case as EC2.

The screenshot shows the 'Trusted entity type' step of the AWS IAM Create New Role wizard. Under 'Service or use case', 'EC2' is selected. Under 'Use case', 'EC2' is also selected.

Add permission of AmazonEC2FullAccess.

The screenshot shows the 'Add permissions' step of creating a new role in AWS IAM. The 'Permissions policies' section lists the 'AmazonEC2FullAccess' policy, which is selected and highlighted in blue. The policy description indicates it provides full access to Amazon EC2. Below the list is a note about setting a permissions boundary, which is marked as optional. At the bottom right of the dialog are 'Cancel', 'Previous', and 'Next' buttons, with 'Next' being highlighted in orange.

Give role name here 'ec2instance'.

The screenshot shows the 'Name, review, and create' step of creating a new role. In the 'Role details' section, the 'Role name' field contains 'ec2instance'. The 'Description' field contains the text 'Allows EC2 instances to call AWS services on your behalf.' In the 'Step 1: Select trusted entities' section, the 'Trust policy' field displays a JSON-based policy document:

```
1. {  
2.     "Version": "2012-10-17",  
3.     "Statement": [  
4.         {  
5.             "Effect": "Allow",  
6.             "Principal": "*"  
7.         }  
8.     ]  
9. }
```

At the bottom right of the dialog are 'Edit' and 'Next' buttons, with 'Next' being highlighted in orange. The system status bar at the bottom shows 'CloudShell Feedback' and the date '21-10-2024'.

Role has been created successfully.

The screenshot shows the AWS Identity and Access Management (IAM) service. In the top navigation bar, there is a green banner that says "Role ec2instance created." Below this, the "Roles" section displays three roles: "AWSServiceRoleForSupport", "AWSServiceRoleForTrustedAdvisor", and the newly created "ec2instance". The "ec2instance" role is listed under the "AWS Service: ec2" category. On the right side of the screen, there are sections for "Roles Anywhere" and "Temporary credentials". The status bar at the bottom indicates the user is in the "BAN - SA" region, and the date and time are 21-10-2024 14:31.

Go under EC2 dashboard. And go on Actions.

The screenshot shows the AWS EC2 Dashboard. In the "Instances" section, one instance named "user1-ec2" is listed. The instance is running, has an instance type of t2.micro, and 2/2 checks passed. On the right side of the instance card, there is a vertical "Actions" menu. The "Actions" menu is expanded, showing options like "Connect", "View details", "Manage instance state", "Instance settings", "Networking", "Security", "Image and templates", and "Monitor and troubleshoot". The status bar at the bottom indicates the user is in the "Mumbai" region, and the date and time are 21-10-2024 14:33.

Actions → Security → Modify IAM role

The screenshot shows the AWS EC2 Instances page. A single instance, 'user1-ec2' (i-04452a1240d87df58), is listed as 'Running'. The 'Actions' dropdown menu is open, and the 'Modify IAM role' option is highlighted.

Select just created role and assign it to the EC2 instance. After that Update IAM role.

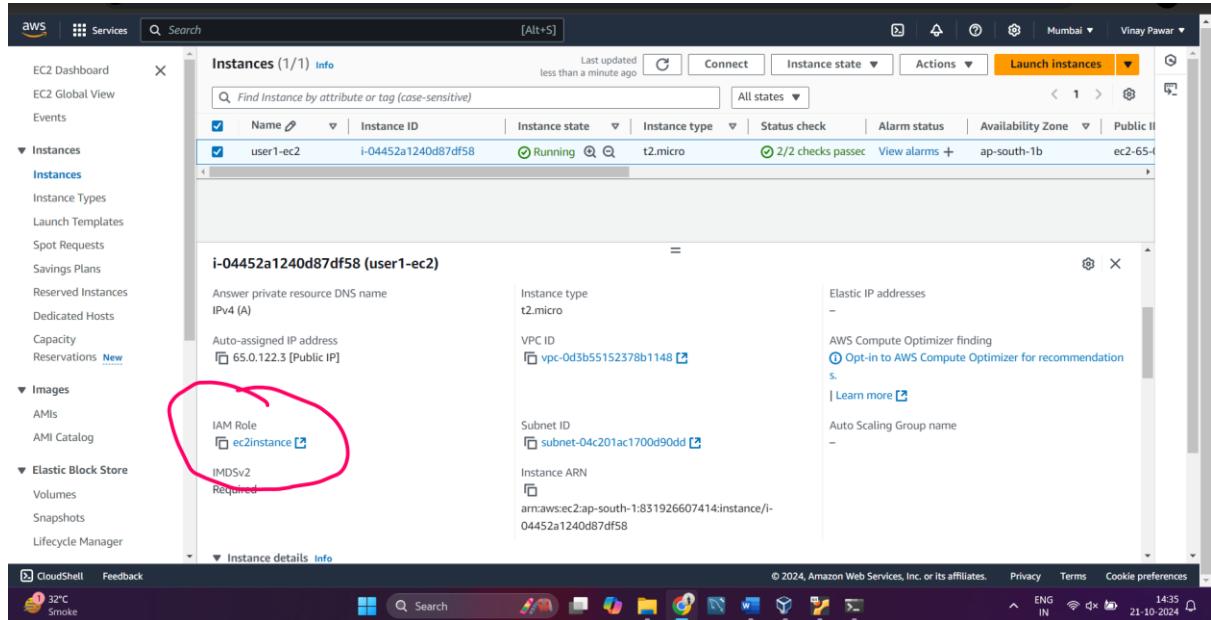
The screenshot shows the 'Modify IAM role' configuration dialog. It displays the instance ID 'i-04452a1240d87df58 (user1-ec2)' and a dropdown menu for selecting an IAM role. A warning message states: '⚠ If you choose No IAM Role, any IAM role that is currently attached to the instance will be removed. Are you sure you want to remove from the selected instance?'. At the bottom are 'Cancel' and 'Update IAM role' buttons.

The screenshot shows the 'Modify IAM role' page in the AWS IAM console. At the top, the navigation path is EC2 > Instances > i-04452a1240d87df58 > Modify IAM role. The main section is titled 'Modify IAM role' with a link to 'Info'. Below it, a sub-instruction says 'Attach an IAM role to your instance.' A dropdown menu is open, showing 'ec2instance' selected. To the right of the dropdown is a button labeled 'Create new IAM role'. At the bottom right of the dialog is an 'Update IAM role' button.

Role attached to ec2instance successfully

The screenshot shows the 'Instances' page in the AWS EC2 Dashboard. The left sidebar lists various EC2 services like EC2 Global View, Events, Instances, Images, and Elastic Block Store. The main content area displays a table for 'Instances (1/1)'. The table has columns for Name, Instance ID, Instance state, Instance type, Status check, Alarm status, Availability Zone, and Public IP. One row is shown, indicating 'user1-ec2' with Instance ID 'i-04452a1240d87df58' is 'Running' on 't2.micro' type, with 2/2 checks passed, in 'ap-south-1b' zone, and Public IP 'ec2-65-0-1'. At the bottom of the page, the instance details are summarized as 'i-04452a1240d87df58 (user1-ec2)'.

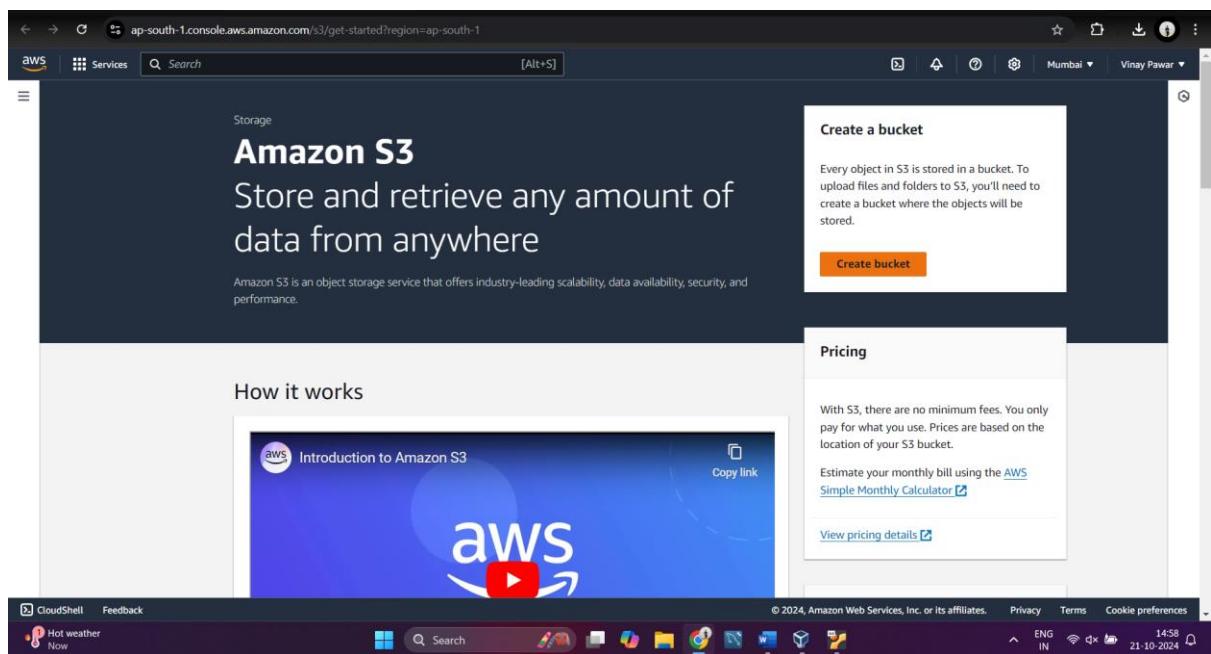
Here our IAM role is successfully attached to the EC2 instance.



The screenshot shows the AWS EC2 Instances page. On the left, there's a navigation sidebar with options like EC2 Dashboard, EC2 Global View, Events, Instances (with 'Instances' selected), Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Capacity, and Reservations. Below that are sections for Images (AMIs, AMI Catalog) and Elastic Block Store (Volumes, Snapshots, Lifecycle Manager). The main area displays a table of instances. One row is selected, showing details for 'user1-ec2' (Instance ID: i-04452a1240d87df58). The 'IAM Role' field contains 'ec2instance' and is circled in red. Other visible details include Instance type: t2.micro, Status check: 2/2 checks passed, and VPC ID: vpc-0d3b55152378b1148.

3. Create an s3 bucket with unique name upload static html file containing a message. “Hello, welcome to my page” and configure bucket to serve as a static website.

Create a S3 bucket.



The screenshot shows the AWS S3 Get Started page. The main content area features the heading 'Amazon S3' and the subtext 'Store and retrieve any amount of data from anywhere'. It includes a note about Amazon S3 being an object storage service with industry-leading scalability, data availability, security, and performance. Below this is a section titled 'How it works' with a video thumbnail for 'Introduction to Amazon S3'. To the right, there's a 'Create a bucket' box with the instruction '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.' and a 'Create bucket' button. A 'Pricing' sidebar provides information about no minimum fees and links to a monthly calculator and pricing details. The bottom of the screen shows the standard AWS navigation bar with CloudShell, Feedback, and various icons.

Give a unique name here ‘vinay-s3-bucket-exam’ and give object ownership as ACLs disabled.

The screenshot shows the AWS S3 Bucket creation interface. In the 'Object Ownership' section, the radio button for 'ACLs disabled (recommended)' is selected, indicating that all objects in the bucket are owned by the account and access is controlled by policies. Below this, it says 'Bucket owner enforced'. In the 'Block Public Access settings for this bucket' section, the checkbox for 'Block all public access' is checked, which is highlighted in red. The status message below states: 'Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.' Below this, there are four unchecked checkboxes corresponding to different access control options: 'Block public access to buckets and objects granted through new access control lists (ACLs)', 'Block public access to buckets and objects granted through any access control lists (ACLs)', 'Block public access to buckets and objects granted through new public bucket or access point policies', and 'Block public and cross-account access to buckets and objects through any public bucket or access point policies'.

Here all the access is blocked for public we need to uncheck it because our website is for all the users not for one single user. So we need to give access as a public .

This screenshot shows the 'Block Public Access settings for this bucket' section of the AWS S3 Bucket creation page. The 'Block all public access' checkbox is checked and highlighted in red. Below it, the status message reads: 'Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.' Underneath, four checkboxes are listed: 'Block public access to buckets and objects granted through new access control lists (ACLs)', 'Block public access to buckets and objects granted through any access control lists (ACLs)', 'Block public access to buckets and objects granted through new public bucket or access point policies', and 'Block public and cross-account access to buckets and objects through any public bucket or access point policies'. The first checkbox is checked and highlighted in red, while the others are unchecked.

Here we are unchecking it so that our objects in the bucket will be public.

Block Public Access settings for this bucket

Block all public access

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

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

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

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

⚠️ Turning off block all public access might result in this bucket and the objects within becoming public

AWS recommends that you turn on block all public access, unless public access is required for specific and verified use cases such as static website hosting.

I acknowledge that the current settings might result in this bucket and the objects within becoming public.

Check this box I acknowledge one...



Turning off block all public access might result in this bucket and the objects within becoming public

AWS recommends that you turn on block all public access, unless public access is required for specific and verified use cases such as static website hosting.

I acknowledge that the current settings might result in this bucket and the objects within becoming public.

Bucket Versioning

Make all remaining as a default one.

Default encryption [Info](#)

Server-side encryption is automatically applied to new objects stored in this bucket.

Encryption type [Info](#)

Server-side encryption with Amazon S3 managed keys (SSE-S3)

Server-side encryption with AWS Key Management Service keys (SSE-KMS)

Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)

Secure your objects with two separate layers of encryption. For details on pricing, see [DSSE-KMS pricing](#) on the Storage tab of the [Amazon S3 pricing page](#).

Bucket Key

Using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. S3 Bucket Keys aren't supported for DSSE-KMS. [Learn more](#)

Disable

Enable

Advanced settings

After creating the bucket, you can upload files and folders to the bucket, and configure additional bucket settings.

Create bucket

Here our s3 bucket will be created successfully.

The screenshot shows the AWS S3 service page. A green banner at the top indicates that a bucket named "vinay-s3-bucket-exam" has been successfully created. Below the banner, there's an "Account snapshot" section with a link to "All AWS Regions". Under "General purpose buckets", there is one entry: "vinay-s3-bucket-exam" from the "Asia Pacific (Mumbai) ap-south-1" region, created on October 21, 2024, at 14:59:22 (UTC+05:30). There are buttons for "Copy ARN", "Empty", "Delete", and "Create bucket".

Go under Buckets and go inside created bucket.

The screenshot shows the "Objects" tab of the "vinay-s3-bucket-exam" bucket. It displays a message stating "No objects" and "You don't have any objects in this bucket." There is a prominent "Upload" button at the bottom. The top navigation bar shows the URL as "ap-south-1.console.aws.amazon.com/s3/buckets/vinay-s3-bucket-exam?region=ap-south-1&bucketType=general&tab=objects".

Upload a html file.

The screenshot shows the AWS S3 'Upload' interface. At the top, there's a navigation bar with 'Services' and a search bar. Below it, the path 'Amazon S3 > Buckets > vinay-s3-bucket-exam > Upload' is visible. The main area is titled 'Upload' with a 'Info' link. A note says: '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](#)'.

A large dashed blue box allows users to 'Drag and drop files and folders you want to upload here, or choose Add files or Add folder.' Below this, a table lists 'Files and folders (1 Total, 263.0 B)'. It shows one item: 'index.html' (text/html). There are 'Remove', 'Add files', and 'Add folder' buttons. A search bar labeled 'Find by name' is also present.

The 'Destination' section shows the target bucket as 's3://vinay-s3-bucket-exam'. A 'Destination details' link is available. The bottom of the screen shows the Windows taskbar with various pinned icons like CloudShell, Feedback, and a weather icon for 31°C Haze.

Uploaded successfully.

The screenshot shows the 'Upload: status' interface. A green header bar indicates 'Upload succeeded' with a 'View details below.' link. Below this, the title 'Upload: status' and a note 'The information below will no longer be available after you navigate away from this page.' are displayed.

The 'Summary' section shows the destination as 's3://vinay-s3-bucket-exam'. It lists 'Succeeded' (1 file, 263.0 B (100.0%)) and 'Failed' (0 files, 0 B (0%)).

The 'Files and folders' section shows a table with one item: 'index.html' (text/html, 263.0 B, Status: Succeeded). A 'Find by name' search bar is at the top of the table.

The bottom of the screen shows the Windows taskbar with icons for CloudShell, Feedback, and a weather icon for 31°C Haze.

Click on that file and go under properties.

AWS Services Search [Alt+S] Mumbai Vinay Pawar

Amazon S3 > Buckets vinay-s3-bucket-exam

vinay-s3-bucket-exam [Info](#)

Objects Properties Permissions Metrics Management Access Points

Bucket overview

AWS Region Asia Pacific (Mumbai) ap-south-1	Amazon Resource Name (ARN) arn:aws:s3:::vinay-s3-bucket-exam	Creation date October 21, 2024, 14:59:22 (UTC+05:30)
------------------------------------------------	-----------------------------------------------------------------	---------------------------------------------------------

Bucket Versioning

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. [Learn more](#)

Bucket Versioning
Disabled

Multi-factor authentication (MFA) delete

An additional layer of security that requires multi-factor authentication for changing Bucket Versioning settings and permanently deleting object versions. To modify MFA delete settings, use the AWS CLI, AWS SDK, or the Amazon S3 REST API. [Learn more](#)

Disabled

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences Nifty smicap -1.24% ENG IN 15:12 21-10-2024

Go downside and find static website hosting.

AWS Services Search [Alt+S] Mumbai Vinay Pawar

Amazon S3 > Buckets vinay-s3-bucket-exam

vinay-s3-bucket-exam [Info](#)

Objects Properties Permissions Metrics Management Access Points

Object Lock

Store objects using a write-once-read-many (WORM) model to help you prevent objects from being deleted or overwritten for a fixed amount of time or indefinitely. Object Lock works only in versioned buckets. [Learn more](#)

Object Lock
Disabled

Requester pays

When enabled, the requester pays for requests and data transfer costs, and anonymous access to this bucket is disabled. [Learn more](#)

Requester pays
Disabled

Static website hosting

Use this bucket to host a website or redirect requests. [Learn more](#)

S3 static website hosting
Disabled

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences Nifty smicap -1.24% ENG IN 15:12 21-10-2024

Click on edit. Initially it is disable we need to enable it.

The screenshot shows the AWS S3 Static website hosting configuration interface. At the top, there's a navigation bar with the AWS logo, a search bar, and a 'Services' dropdown. The main content area is titled 'Static website hosting' and contains several configuration sections:

- Static website hosting**: A radio button section where 'Enable' is selected.
- Hosting type**: A radio button section where 'Host a static website' is selected. It includes a note about making content publicly readable and a link to 'Using Amazon S3 Block Public Access'.
- Index document**: A text input field containing 'index.html'.
- Error document - optional**: A text input field containing 'error.html'.
- Redirection rules - optional**: A note about redirection rules, with a link to 'Redirection rules, written in JSON'.

The bottom of the screen shows the Windows taskbar with various pinned icons and the system tray indicating the date and time as 21-10-2024 at 15:12.

Click on save changes it will saved the changes.

The screenshot shows the AWS Lambda function configuration interface. The main area is a JSON editor window with the following content:

```
JSON  Ln 1, Col 1  ⚡ Errors: 0  ⚠ Warnings: 0
```

At the bottom of the editor window, there are two buttons: 'Cancel' and a prominent orange 'Save changes' button.

The bottom of the screen shows the Windows taskbar with various pinned icons and the system tray indicating the date and time as 21-10-2024 at 15:13.

Successfully edited static website hosting.

The screenshot shows the AWS S3 console for a bucket named 'vinay-s3-bucket-exam'. The 'Properties' tab is selected. A green banner at the top says 'Successfully edited static website hosting.' Below it, the 'Bucket overview' section shows the AWS Region as 'Asia Pacific (Mumbai) ap-south-1', the Amazon Resource Name (ARN) as 'arn:aws:s3:::vinay-s3-bucket-exam', and the Creation date as 'October 21, 2024, 14:59:22 (UTC+05:30)'. The 'Bucket Versioning' section is expanded, showing 'Bucket Versioning' is 'Disabled'. An 'Edit' button is visible in the top right corner of this section. At the bottom of the page, there are links for CloudShell, Feedback, and a footer with copyright information and language settings (ENG IN).

Go under permissions and check for bucket policy.

The screenshot shows the AWS S3 console for the same bucket. The 'Permissions' tab is selected. The 'Permissions overview' section includes a note about access findings and a link to view the analyzer for the region. The 'Block public access (bucket settings)' section is expanded, showing 'Block all public access' is set to 'Off'. There is also a note about individual block public access settings for the bucket. An 'Edit' button is visible in the top right corner of this section. At the bottom of the page, there are links for CloudShell, Feedback, and a footer with copyright information and language settings (ENG IN).

The screenshot shows the AWS S3 Bucket Policy settings page. At the top, there is a section titled "Block all public access" with a status of "Off". Below this is a "Bucket policy" section. A note states: "The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. [Learn more](#)". There is a "No policy to display." message, a "Copy" button, and "Edit" and "Delete" buttons.

CloudShell Feedback

BSE smcap -1.21%

CloudShell Search

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

ENG IN 15:13 21-10-2024

The screenshot shows the "Edit bucket policy" page. It includes sections for "Bucket policy", "Bucket ARN" (arn:aws:s3:::vinay-s3-bucket-exam), and "Policy". The policy editor shows a single statement: "1 |". To the right, there is a "Select a statement" dropdown and a "Add new statement" button.

Amazon S3 > Buckets > vinay-s3-bucket-exam > Edit bucket policy

Edit bucket policy [Info](#)

Bucket policy

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. [Learn more](#)

Bucket ARN
arn:aws:s3:::vinay-s3-bucket-exam

Policy

1 |

Select a statement

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

Add new statement

CloudShell Feedback

BSE smcap -1.21%

CloudShell Search

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

ENG IN 15:13 21-10-2024

Screenshot of the AWS S3 Bucket Policy Editor:

The screenshot shows the "Edit bucket policy" page for the bucket "vinay-s3-bucket-exam". The ARN of the bucket is copied to the clipboard. The policy editor interface includes sections for "Bucket policy" and "Policy". A modal window titled "Edit statement" is open, prompting the user to "Select a statement" or "Add new statement".

Screenshot of the AWS Policy Generator:

The screenshot shows the "AWS Policy Generator" interface. It starts with "Step 1: Select Policy Type" (S3 Bucket Policy selected). The next step, "Step 2: Add Statement(s)", is shown with fields for Effect (Allow selected), Principal (*), AWS Service (Amazon S3), Actions (1 Action(s) Selected), and Amazon Resource Name (ARN) (arn:s3:::vinay-s3-bucket-exam). A button "Add Statement" is at the bottom.

Amazon S3

All Services ('*')

Use multiple statements to add permissions for more than one service.

Actions All Actions ('*')

Amazon Resource Name (ARN)

ARN should follow the following format: arn:aws:s3:::\${BucketName}/\${KeyName}.
Use a comma to separate multiple values.

Add Conditions (Optional)

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

Principal(s)	Effect	Action	Resource	Conditions
*	Allow	s3:GetObject	arn:aws:s3:::vinay-s3-bucket-exam	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 Generator does not modify the applicable terms and conditions governing your use of Amazon Web Services technologies.

©2010, Amazon Web Services LLC or its affiliates. All rights reserved.
An [amazon.com](#) company

Amazon S3

All Services ('*')

Use multiple statements to add permissions for more than one service.

Actions All Actions ('*')

Amazon Resource Name (ARN)

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.

```
{
  "Id": "Policy1729503869897",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1729503869897",
      "Action": [
        "s3:GetObject"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::vinay-s3-bucket-exam",
      "Principal": "*"
    }
  ]
}
```

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.

©2010, Amazon Web Services LLC or its affiliates. All rights reserved.
An [amazon.com](#) company

AWS Services Search [Alt+S] Bucket ARN Bucket ARN arn:aws:s3:::vinay-s3-bucket-exam

Policy

```
1 {  
2   "Id": "Policy1729503940805",  
3   "Version": "2012-10-17",  
4   "Statement": [  
5     {  
6       "Sid": "Stmt1729503939413",  
7       "Action": [  
8         "s3:GetObject"  
9       ],  
10      "Effect": "Allow",  
11      "Resource": "arn:aws:s3:::vinay-s3-bucket-exam/*",  
12      "Principal": "*"  
13    }  
14  ]  
15 }
```

Edit statement

Select a statement

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

+ Add new statement

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences ENG IN 21-10-2024

AWS Services Search [Alt+S] Bucket ARN Bucket ARN arn:aws:s3:::vinay-s3-bucket-exam

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. [Learn more](#)

Policy

```
1 {  
2   "Id": "Policy1729503940805",  
3   "Version": "2012-10-17",  
4   "Statement": [  
5     {  
6       "Sid": "Stmt1729503939413",  
7       "Action": [  
8         "s3:GetObject"  
9       ],  
10      "Effect": "Allow",  
11      "Resource": "arn:aws:s3:::vinay-s3-bucket-exam/*",  
12      "Principal": "*"  
13    }  
14  ]  
15 }
```

Edit statement Remove Stmt1729503939413

Add actions Choose a service Filter services

Included S3

Available AMP API Gateway API Gateway V2 ASC Access Analyzer Account

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences ENG IN 21-10-2024

The screenshot shows the AWS S3 console. A green banner at the top indicates "Successfully edited bucket policy." Below it, the navigation bar shows "Amazon S3 > Buckets > vinay-s3-bucket-exam". The "Permissions" tab is selected in the top navigation bar. Under "Permissions overview", there is a section for "Access finding" with a link to "How IAM analyzer findings work". Below that is the "Block public access (bucket settings)" section, which includes a "Edit" button and a status indicator "Off". The status is described as "Individual Block Public Access settings for this bucket". The bottom of the screen shows the Windows taskbar with various pinned icons.

4. Ensure that HTML file is publicly accessible...

Go to the s3 bucket → click on permission →

The screenshot shows the AWS S3 buckets page. At the top, there is an "Account snapshot - updated every 24 hours" section with a "View Storage Lens dashboard" button. Below it, there are tabs for "General purpose buckets" and "Directory buckets", with "General purpose buckets" selected. It shows one bucket named "vinay-s3-bucket-exam" with details: Name (vinay-s3-bucket-exam), AWS Region (Asia Pacific (Mumbai) ap-south-1), IAM Access Analyzer (View analyzer for ap-south-1), and Creation date (October 21, 2024, 14:59:22 (UTC+05:30)). There are buttons for "Copy ARN", "Empty", "Delete", and "Create bucket". The bottom of the screen shows the Windows taskbar.

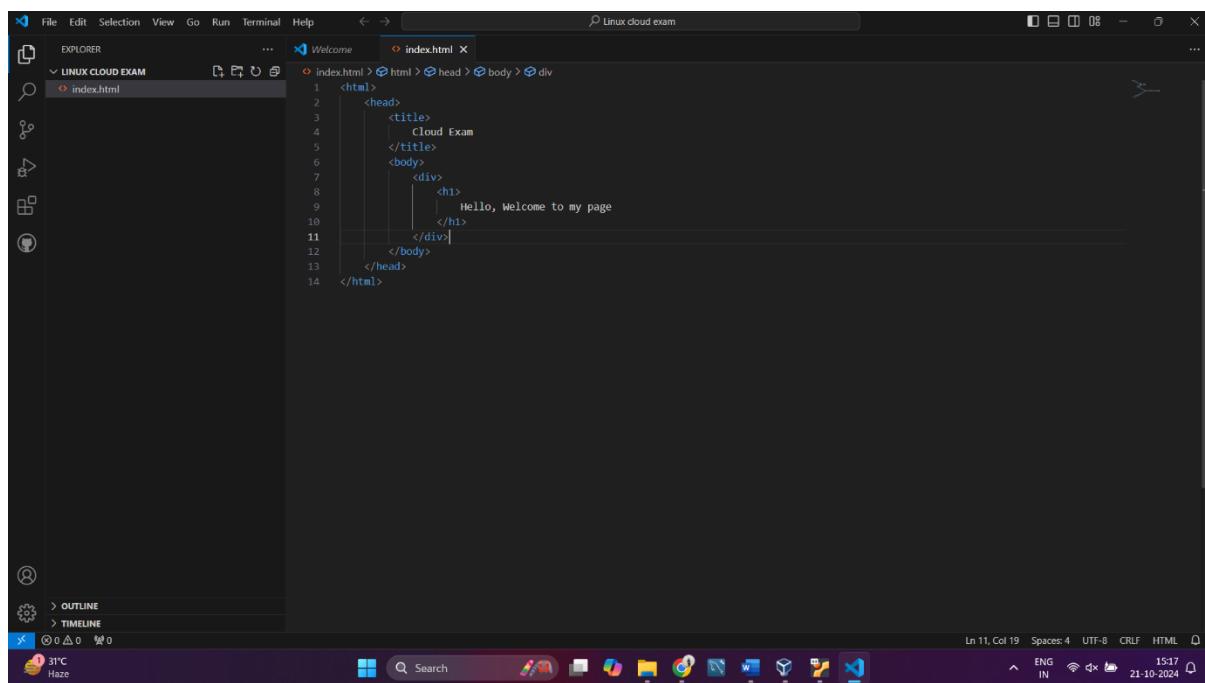
s3 bucket → click on permission → static website hosting → click on that url <http://vinay-s3-bucket-exam.s3-website.ap-south-1.amazonaws.com> this is our website link.

The screenshot shows the AWS S3 Bucket Properties page for 'vinay-s3-bucket-exam'. Under the 'Static website hosting' section, 'Bucket website endpoint' is listed as '<http://vinay-s3-bucket-exam.s3-website.ap-south-1.amazonaws.com>'.

It is hosted successfully and it is open for public also.

The screenshot shows a browser window displaying the static website from the previous step. The title bar reads 'Hello, Welcome to my page'. The status bar at the bottom right shows the date and time as '21-10-2024 15:17'.

This is the html coding of the file.



The screenshot shows a code editor interface with a dark theme. The top bar includes a file menu (File, Edit, Selection, View, Go, Run, Terminal, Help), a search bar, and a tab bar showing "Welcome" and "index.html". The left sidebar has an "EXPLORER" section titled "LINUX CLOUD EXAM" containing "index.html". The main area displays the following HTML code:

```
<html>
  <head>
    <title>
      Cloud Exam
    </title>
  </head>
  <body>
    <div>
      <h1>
        Hello, Welcome to my page
      </h1>
    </div>
  </body>
</html>
```

The status bar at the bottom shows "Ln 11, Col 19" and "Spaces: 4" and "UTF-8" and "CRLF" and "HTML". It also displays the date and time "21-10-2024".

