

Cloud

The screenshot shows two overlapping windows from the AWS Identity and Access Management (IAM) service.

IAM > Users

This window displays the list of users. The header says "Users (0) Info". A note states: "An IAM user is an identity with long-term credentials that is used to interact with AWS in an account." Below is a search bar and a table with columns: User name, Path, Group, Last activity, MFA, Password age, Console last sign-in, and Access key ID. A message at the bottom says "No resources to display".

IAM > Users > Create user

This window is a step-by-step wizard:

- Step 1: Specify user details**
- Step 2: Set permissions**
- Step 3: Review and create**

The current step is "Specify user details". It has a section titled "User details" with a "User name" field containing "bhas". A note below says: "The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + - . @ _ (hyphen)". There is an optional checkbox: "Provide user access to the AWS Management Console - optional". A note below it says: "If you're providing console access to a person, it's a best practice to manage their access in IAM Identity Center." A callout box provides additional information: "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](#)".

At the bottom right are "Cancel" and "Next" buttons.

IAM > Users > Create user

Step 1
Specify user details

Step 2
Set permissions

Step 3
Review and create

Set permissions

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. [Learn more](#)

Permissions options

- Add user to group

Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.
- Copy permissions

Copy all group memberships, attached managed policies, and inline policies from an existing user.
- Attach policies directly

Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

Permissions policies (2/1246)

Choose one or more policies to attach to your new user.

Filter by Type			
<input type="text" value="s3"/>	All types	12 matches	< 1 >
<input type="checkbox"/> Policy name <input type="text" value="AmazonS3FullAccess"/>	Type	Attached entities	▼
<input type="checkbox"/> AmazonDMSRedshiftS3Role	AWS managed	0	
<input checked="" type="checkbox"/> AmazonS3FullAccess	AWS managed	0	
<input type="checkbox"/> AmazonS3ObjectLambdaExecutionRolePolicy	AWS managed	0	
<input type="checkbox"/> AmazonS3OutpostsFullAccess	AWS managed	0	

[Create policy](#)

User details

User name	Console password type	Require password reset
bhas	None	No

Permissions summary

Name	Type	Used as
AmazonEC2FullAccess	AWS managed	Permissions policy
AmazonS3FullAccess	AWS managed	Permissions policy

Tags - optional

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

No tags associated with the resource.

[Add new tag](#)

You can add up to 50 more tags.

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

Screenshot of the AWS IAM User Details page for user 'bhas'.

Summary

ARN arn:aws:iam::148761676347:user/bhas	Console access Disabled	Access key 1 Create access key
Created October 21, 2024, 16:46 (UTC+05:30)	Last console sign-in -	

Permissions

Permissions policies (2)

Policy name	Type	Attached via
AmazonEC2FullAccess	AWS managed	Directly
AmazonS3FullAccess	AWS managed	Directly

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

Screenshot of the 'Create access key' wizard step 1: Choose use case.

Application running on an AWS compute service

You plan to use this access key to enable application code running on an AWS compute service like Amazon EC2, Amazon ECS, or AWS Lambda to access your AWS account.

Local code

You plan to use this access key to enable application code in a local development environment to access your AWS account.

Third-party service

You plan to use this access key to enable access for a third-party application or service that monitors or manages your AWS resources.

Other

Your use case is not listed here.

Alternative recommended

Assign an IAM role to compute resources like EC2 instances or Lambda functions to automatically supply temporary credentials to enable access. [Learn more](#)

Confirmation

I understand the above recommendation and want to proceed to create an access key.

Cancel Next

IAM > Users > bhas > Create access key

Step 1
[Access key best practices & alternatives](#)

Step 2 - optional
Set description tag

The description for this access key will be attached to this user as a tag and shown alongside the access key.

Description tag value
Describe the purpose of this access key and where it will be used. A good description will help you rotate this access key confidently later.

Maximum 256 characters. Allowed characters are letters, numbers, spaces representable in UTF-8, and: _ . : / = + - @.

Cancel Previous **Create access key**

us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/users/details/bhas/create-access-key

Gmail YouTube Binary Search - Gee... Maps Compilation Proces... News Translate C Program to Copy... Cell splitting techni...

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

IAM > Users > bhas > Create access key

Step 1
[Access key best practices & alternatives](#)

Step 2 - optional
[Set description tag](#)

Step 3
Retrieve access keys

Retrieve access keys [Info](#)

Access key
If you lose or forget your secret access key, you cannot retrieve it. Instead, create a new access key and make the old key inactive.

Access key	Secret access key
<input type="text" value="AKIASFIXDBISLUQTQNKP7"/>	<input style="background-color: #f0f0f0; border: none; width: 100px; height: 20px; vertical-align: middle;" type="text" value="*****"/> Show

Access key best practices

- Never store your access key in plain text, in a code repository, or in code.
- Disable or delete access key when no longer needed.
- Enable least-privilege permissions.
- Rotate access keys regularly.

For more details about managing access keys, see the [best practices](#) for managing AWS access keys.

Download .csv file Done

missions Groups Tags (1) Security credentials Last Accessed

sole sign-in link https://148761676347.signin.aws.amazon.com/console

Multi-factor authentication MFA to increase the security of your users

Type

Enable console access

Enable console access for bhas.

Console password

Autogenerated password

Custom password

User must create new password at next sign-in
Users automatically get the IAMUserChangePassword policy to allow them to change their own password.

Cancel **Enable console access**

access keys (1)

access keys to send programmatic calls to AWS from the AWS CLI, AWS Tools for PowerShell, AWS SDKs, or direct AWS API calls. You can have a maximum of two access keys per user.

us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/users/details/bhas?section=security_credentials

Identity and Access Management (IAM)

Console access enabled.

Console sign-in

Console sign-in URL https://148761676347.signin.aws.amazon.com/console

User name bhas

Console password Show

You have successfully enabled the user's new password.
This is the only time you can view this password. After you close this window, if the password is lost, you must create a new one.

Download .csv file **Close**

Manage console access

bhas_credentials (1).csv 109 B • Done

bhas_accessKeys (1).csv 99 B • 6 minutes ago

Created on

Remove Resync Assign MFA device

Assign MFA device

© 2014, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Terms Cookies

Gmail YouTube Binary Search - Gee... Maps Compilation Process... News Translate C Program to Copy... Cell splitting techni...

Try the new sign in UI
See our new improved Amazon Web Services sign in experience before we officially launch.
Enable new sign in

aws

Sign in as IAM user

Account ID (12 digits) or account alias
148761676347

IAM user name
bhas

Password
.....

Remember this account

Sign in

Sign in using root user email
Forgot password?

Amazon Lightsail
Lightsail is the easiest way to get started on AWS
Learn more »

Gmail YouTube Binary Search - Gee... Maps Compilation Process... News Translate C Program to Copy... Cell splitting techni...
aws Services Search [Alt+S] N. Virginia bhas @ 1487-6167-6347

Console Home Info

Recently visited Info

- S3
- CodePipeline
- EC2
- IAM
- Support
- RDS
- Billing and Cost Management
- Amazon SageMaker

View all services

Applications (0) Info

Region: US East (N. Virginia)

Create app

us-east-1 (Current Region) Find applications

Name	Description	Region	Originator
Access denied			

Go to myApplications

Welcome to AWS

Getting started with AWS
Learn the fundamentals and

AWS Health Info

Cost and usage Info

Current month costs
Access denied

Cost breakdown
Access denied

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

Launch an instance [Info](#)

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags [Info](#)

Name: bhas-ec2-iam-instance [Add additional tags](#)

Application and OS Images (Amazon Machine Image) [Info](#)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below.

Search our full catalog including 1000s of application and OS images

Quick Start

Amazon Linux macOS Ubuntu Windows Red Hat SUSE Li [Browse more AMIs](#)

[CloudShell](#) [Feedback](#)

Summary

Number of instances: [Info](#) 1

Software Image (AMI): Amazon Linux 2023 AMI 2023.6.2... [read more](#)
ami-06b21caeaff8cd686

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. [Learn more](#)

[Cancel](#) [Launch instance](#) [Preview code](#)

© 2024, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

t2.micro

Family: t2 - Two vCPU - 1 GiB Memory - Current generation: true
On-Demand Windows base pricing: 0.0162 USD per hour
On-Demand burst credit pricing: 0.01716 USD per hour
On-Demand spot price: 0.0162 USD per hour
On-Demand demand-based reservation price: 0.0116 USD per hour

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 a key pair before you launch the instance.

Key pair name - required

Select: exam-key-pair

Create key pair

Key pair name: exam-key-pair

Key pairs allow you to connect to your instance securely. The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.

Key pair type:

RSA RSA encrypted private and public key pair

ED25519 ED25519 encrypted private and public key pair

Private key file format:

.pem For use with OpenSSH

.ppk For use with PuTTY

When prompted, store the private key in a secure and accessible location on your computer. You will need it later to connect to your instance. [Learn more](#)

[Cancel](#) [Create key pair](#) [Preview code](#)

Screenshot of the AWS Cloud9 interface showing the creation of a new EC2 instance.

Instance Configuration:

- Instance Type:** t2.micro
- AMI:** Amazon Linux 2023 AMI 2023.6.2... (ami-06b21ccaeff8cd686)
- Key pair:** exam-key-pair
- Network settings:** New security group (selected)
- Storage:** 1 volume(s) - 8 GiB

Launch Instance Confirmation:

A modal window displays the following information:

- 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 IP included.
- Launch instance** button (highlighted in orange).
- Preview code** link.

Security Group Configuration:

We'll create a new security group called "launch-wizard-7" with the following rules:

- Allow SSH traffic from Anywhere (0.0.0.0/0)
- Allow HTTPS traffic from the internet
- Allow HTTP traffic from the internet

A note states: Rules 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.

Configure Storage:

1x 8 GiB gp3 Root volume (Not encrypted)

A note states: Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage.

Summary:

Number of instances: 1

Software Image (AMI): Amazon Linux 2023 AMI 2023.6.2... (ami-06b21ccaeff8cd686)

Virtual server type (instance type): t2.micro

Firewall (security group): New security group

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

Screenshot of the AWS EC2 Launch Instance成功 (Success) page.

Message: Successfully initiated launch of instance (i-0ca7bc51567e1957e)

Next Steps:

- Create billing and free tier usage alerts
- Connect to your instance
- Connect an RDS database
- Create EBS snapshot policy
- Manage detailed monitoring
- Create Load Balancer
- Create AWS budget
- Manage CloudWatch alarms

Screenshot of the AWS EC2 Instances page showing the newly launched instance.

Instances (1) Info

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv6 DNS
bhas-ec2-iam-...	i-0ca7bc51567e1957e	Running	t2.micro	Initializing	View alarms +	us-east-1a	ec2-34-228-25-182.co...	34.22

Select an instance

WS Services Search [Alt+S] N. Virginia bhas @ 1487-6167-6347

EC2 Dashboard EC2 > Instances > i-0ca7bc51567e1957e

Instance summary for i-0ca7bc51567e1957e (bhas-ec2-iam-instance) Info Updated less than a minute ago

Instance ID	Public IPv4 address	Private IPv4 addresses
i-0ca7bc51567e1957e	34.228.25.182 open address	172.31.18.209
IPv6 address	Instance state	Public IPv4 DNS
-	Running	ec2-34-228-25-182.compute-1.amazonaws.com open address
Hostname type	Private IP DNS name (IPv4 only)	Elastic IP addresses
IP name: ip-172-31-18-209.ec2.internal	ip-172-31-18-209.ec2.internal	-
Answer private resource DNS name	Instance type	AWS Compute Optimizer finding
IPv4 (A)	t2.micro	User: arnaws:iam::148761676347:user/bhas is not authorized to perform: compute-optimizer:GetEnrollmentStatus on resource: * because no identity-based policy allows the compute-optimizer:GetEnrollmentStatus action
Auto-assigned IP address	VPC ID	Retry
34.228.25.182 [Public IP]	vpc-0843fc796d4048e06	
IAM Role	Subnet ID	Auto Scaling Group name
-	subnet-00879e5df7d9c53bf	-
IMDSv2	Instance ARN	
Required	arnaws:ec2:us-east-1:148761676347:instance/i-0ca7bc51567e1957e	

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

aws Services Search [Alt+S] N. Virginia bhas @ 1487-6167-6347

Amazon S3 > Buckets > Create bucket

Create bucket Info Buckets are containers for data stored in S3.

General configuration

AWS Region: US East (N. Virginia) us-east-1

Bucket type: General purpose Directory

General purpose: Recommended for most use cases and access patterns. General purpose buckets are the original S3 bucket type. They allow a mix of storage classes that redundantly store objects across multiple Availability Zones.

Directory: Recommended for low-latency use cases. These buckets use only the S3 Express One Zone storage class, which provides faster processing of data within a single Availability Zone.

Bucket name: exambucket1

Bucket name must be unique within the global namespace and follow the bucket naming rules. See rules for bucket naming

Copy settings from existing bucket - optional
Only the bucket settings in the following configuration are copied.
Choose bucket

Format: s3://bucket/prefix

Object Ownership Info

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

Object Ownership

Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.

ACLs disabled (recommended)
All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.

ACLs enabled
Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.

⚠️ We recommend disabling ACLs, unless you need to control access for each object individually or to have the object writer own the data they upload. Using a bucket policy instead of ACLs to share data with users outside of your account simplifies permissions management and auditing.

Object Ownership

Bucket owner preferred
If new objects written to this bucket specify the bucket-owner-full-control canned ACL, they are owned by the bucket owner. Otherwise, they are owned by the object writer.

Object writer
The object writer remains the object owner.

ⓘ If you want to enforce object ownership for new objects only, your bucket policy must specify that the bucket-owner-full-control canned ACL is required for object uploads. [Learn more](#)

Block Public Access settings for this bucket

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

Block all public access

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

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

Block public access to buckets and objects granted through any access control lists (ACLs)
S3 will ignore all ACLs that grant public access to buckets and objects.

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

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

⚠️ 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

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore

Screenshot of the AWS S3 Bucket Creation wizard - Step 2: Set Bucket Encryption.

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 (DSS-E-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

[Info](#) After creating the bucket, you can upload files and folders to the bucket, and configure additional bucket settings.

[Cancel](#) [Create bucket](#)

Screenshot of the AWS S3 Buckets list after bucket creation.

Successfully created bucket "exambucket1"

To upload files and folders, or to configure additional bucket settings, choose [View details](#).

[View Storage Lens dashboard](#)

[Amazon S3](#) > [Buckets](#)

Account snapshot - updated every 24 hours [All AWS Regions](#)
Storage lens provides visibility into storage usage and activity trends. [Learn more](#)

[General purpose buckets](#) [Directory buckets](#)

General purpose buckets (1) [Info](#) [All AWS Regions](#)

Buckets are containers for data stored in S3.

Name	AWS Region	IAM Access Analyzer	Creation date
exambucket1	US East (N. Virginia) us-east-1	View analyzer for us-east-1	October 21, 2024, 17:06:01 (UTC+05:30)

[Create bucket](#)

[CloudShell](#) [Feedback](#)

© 2024, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

EC2 > Instances > i-0ca7bc51567e1957e (bhas-ec2-iam-instance) Info

Updated 4 minutes ago

Instance ID	i-0ca7bc51567e1957e
IPv6 address	-
Hostname type	IP name: ip-172-31-18-209.ec2.internal
Answer private resource DNS name	IPv4 (A)
Auto-assigned IP address	34.228.25.182 [Public IP]
IAM Role	-
IMDSv2	Required

Public IPv4 address copied
54.228.25.182 | open address

Private IP4 address
ip-172-31-18-209.ec2.internal

Instance state
Running

Private IP DNS name (IPv4 only)
ip-172-31-18-209.ec2.internal

Instance type
t2.micro

VPC ID
vpc-0843fc796d4048e06

Subnet ID
subnet-00879e5df7d9c53bf

Instance ARN
arn:aws:ec2:us-east-1:148761676347:instance/i-0ca7bc51567e1957e

Private IPv4 addresses
172.31.18.209

Public IPv4 DNS
ec2-34-228-25-182.compute-1.amazonaws.com | open address

Elastic IP addresses
-

AWS Compute Optimizer finding
User: armawsiam:148761676347:user/bhas is not authorized to perform: compute-optimizer:GetEnrollmentStatus on resource: * because no identity-based policy allows the compute-optimizer:GetEnrollmentStatus action

Retry

Auto Scaling Group name
-

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

EC2 > Instances > i-0ca7bc51567e1957e (bhas-ec2-iam-instance) Info

Updated 5 minutes ago

Instance ID	i-0ca7bc51567e1957e
IPv6 address	-
Hostname type	IP name: ip-172-31-18-209.ec2.internal
Answer private resource DNS name	IPv4 (A)
Auto-assigned IP address	34.228.25.182 [Public IP]
IAM Role	-
IMDSv2	Required

PUTTY Configuration

Category: Session

Basic options for your PuTTY session

Specify the destination you want to connect to:

Host Name (or IP address): 34.228.25.182

Port: 22

Connection type: SSH

Load, save or delete a stored session

Saved Sessions: Default Settings

Close window on exit: Always, Never, Only on clean exit

About, Help, Open, Cancel

Auto Scaling Group name
-

EC2 > Instances > i-0ca7bc51567e1957e (bhas-ec2-iam-instance) Info

Updated 6 minutes ago

Instance ID	i-0ca7bc51567e1957e	Public IPv4 address	34.228.25.182 open address
IPv6 address	-	Instance state	Running
Hostname type	IP name: ip-172-31-18-209.ec2.internal	Private IP DNS name (IPv4 only)	ip-172-31-18-209.ec2.internal
Answer private resource DNS name	IPv4 (A)	Instance type	t2.micro
Auto-assigned IP address	34.228.25.182 [Public IP]	VPC ID	vpc-0843fc796d4048e06
IAM Role	-	Subnet ID	subnet-00879e3df7d9c53bf
IMDSv2	Required	Instance ARN	arn:aws:ec2:us-east-1:148761676347:instance/i-0ca7bc51567e1957e

PuTTY Configuration

Category: Logging Terminal Keyboard Bell Features Window Appearance Behaviour Translation Selection Colours Connection Data Proxy SSH Kex Hostkeys Cipher Auth Credentials GSSAPI TTY X11 Tunnels

Credentials to authenticate with
Public-key authentication
Private key file for authentication: C:\Users\hp\Downloads\exam-key-pair.ppk
Browse...
Certificate to use with the private key (optional):
Browse...
Plugin to provide authentication responses
Plugin command to run

Open Cancel

aws Services s3

EC2 Dashboard

Instances

- Instances
- Instance Types
- Launch Templates
- Spot Requests
- Savings Plans
- Reserved Instances
- Dedicated Hosts
- Capacity Reservations **New**

Images

- AMIs
- AMI Catalog

Elastic Block Store

- Volumes
- Snapshots
- Lifecycle Manager

34.228.25.182 - PuTTY

PuTTY Security Alert

The host key is not cached for this server.
34.228.25.182 (port 22)
You have no guarantee that the server is the computer you think it is.
The server's ssh-ed25519 key fingerprint is:
ssh-ed25519 255 SHA256:Gx8Y5RemBBCDiatSVq2A4jUS8V6SXguYJl/mGJkp0M
If you trust this host, press "Accept" to add the key to PuTTY's cache and carry on connecting.
If you want to carry on connecting just once, without adding the key to the cache, press "Connect Once".
If you do not trust this host, press "Cancel" to abandon the connection.

Help More info... Accept Connect Once Cancel

Private IPv4 addresses
172.31.18.209
Public IPv4 DNS
ec2-34-228-25-182.compute-1.amazonaws.com | open address

Subnet ID
subnet-00879e3df7d9c53bf

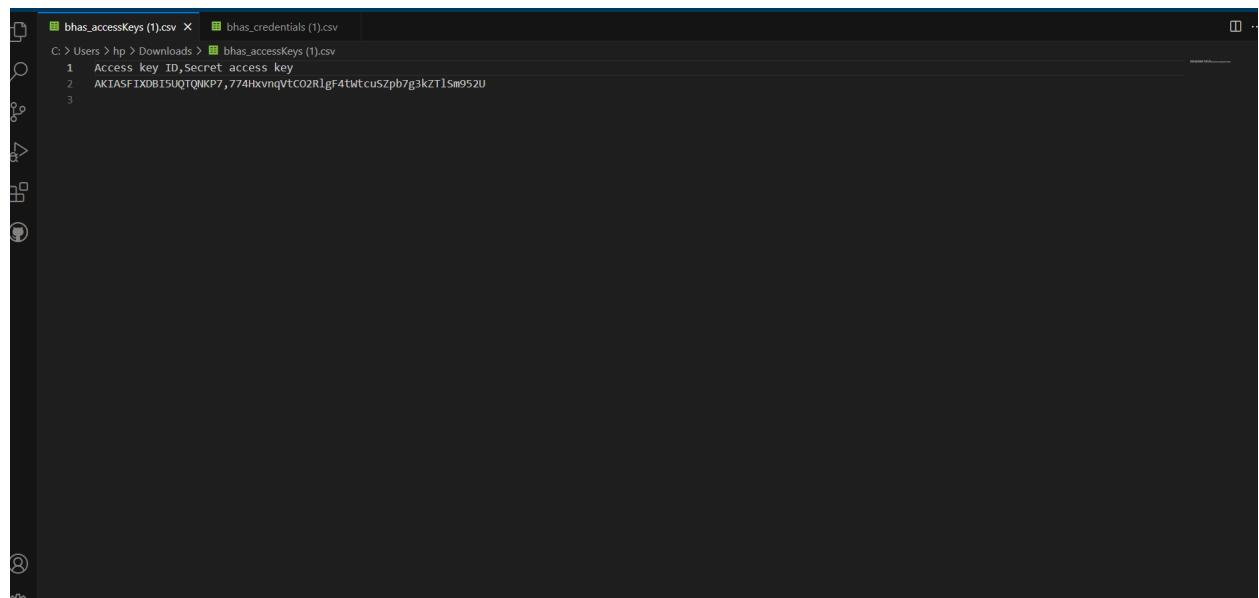
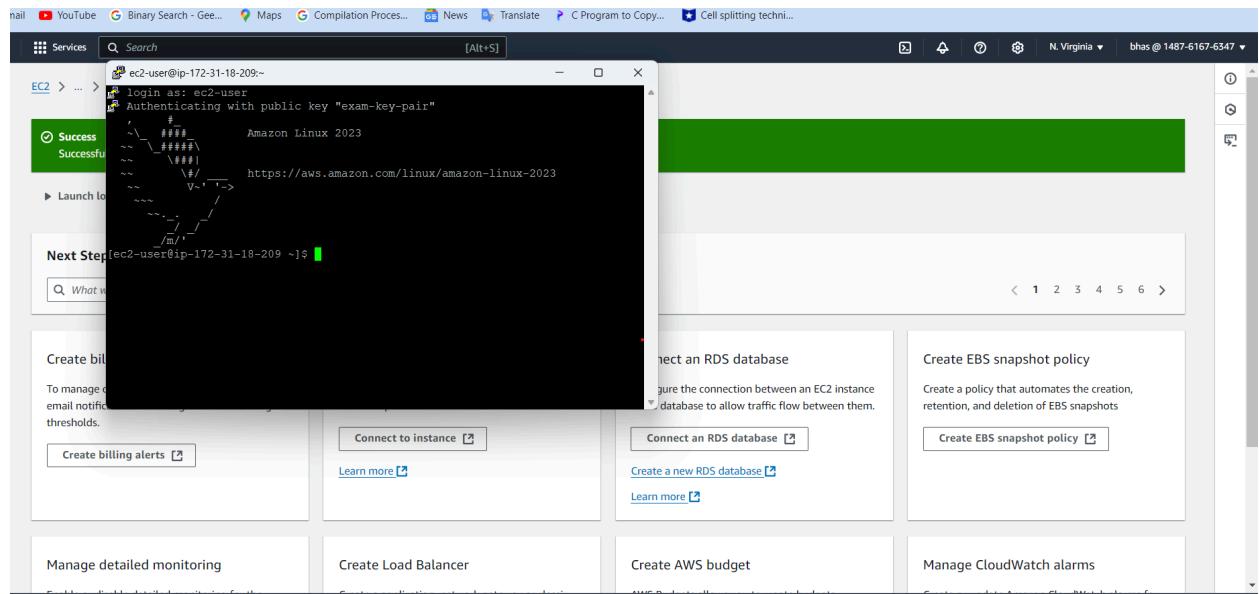
Instance ARN
arn:aws:ec2:us-east-1:148761676347:instance/i-0ca7bc51567e1957e

Auto Scaling Group name
-

Elastic IP addresses
-

AWS Compute Optimizer finding
User: arn:aws:iam::148761676347:user/bhas is not authorized to perform: compute-optimizer:GetEnrollmentStatus on resource: * because no identity-based policy allows the compute-optimizer:GetEnrollmentStatus action

Retry



```
[ec2-user@ip-172-31-18-209 ~]$ aws s3 ls
[ec2-user@ip-172-31-18-209 ~]$ aws configure
AWS Access Key ID [None]: AKIASFIIXDB15UQTQNKP7
AWS Secret Access Key [None]: 774HxvnqVtCO2RlgF4tWtcuSZpb7g3kZTlSm952U
Default region name [None]: us-east-1
Default output format [None]: none
[ec2-user@ip-172-31-18-209 ~]$ aws s3 ls
2024-10-21 11:36:01 exambucket1
[ec2-user@ip-172-31-18-209 ~]$ nano hallo.html
[ec2-user@ip-172-31-18-209 ~]$
```

```
Hello, welcome to my page."
```

```

ec2-user@ip-172-31-18-209:~$ login as: ec2-user
Authenticating with public key "exam-key-pair"
'__ _#
~\_\#\#\#_ Amazon Linux 2023
~~ \#\#\#\\
~~ \|##|
~~ \|#/
~~ V~' '-->
~~ .-
~~ /-
/m/-
[ec2-user@ip-172-31-18-209 ~]$ aws s3 ls
Unable to locate credentials. You can configure credentials by running "aws configure".
[ec2-user@ip-172-31-18-209 ~]$ aws configure
AWS Access Key ID [None]: AKIASFIXXDBI5UQTQNKP7
AWS Secret Access Key [None]: 774HxvnqVtCO2RlgF4tWtcuSzb7g3kZTlSm952U
Default region name [None]: us-east-1
Default output format [None]: none
[ec2-user@ip-172-31-18-209 ~]$ aws s3 ls
2024-10-21 11:36:01 exambucket1
[ec2-user@ip-172-31-18-209 ~]$ nano hallo.html
[ec2-user@ip-172-31-18-209 ~]$ nano hallo.html
[ec2-user@ip-172-31-18-209 ~]$ cat hallo.html
"Hello, welcome to my page."
[ec2-user@ip-172-31-18-209 ~]$ aws s3 cp hallo.html s3://exambucket1
upload: ./hallo.html to s3://exambucket1/hallo.html
[ec2-user@ip-172-31-18-209 ~]$ 

```

The screenshot shows the AWS S3 console interface. On the left, there's a navigation sidebar with links like 'Buckets', 'Access Grants', 'Object Lambda Access Points', etc. The main area shows the 'exambucket1' bucket details. The 'Objects' tab is selected, displaying a single file named 'hallo.html'. The file details are as follows:

Name	Type	Last modified	Size	Storage class
hallo.html	html	October 21, 2024, 17:15:17 (UTC+05:30)	29.0 B	Standard

Properties	Permissions	Versions
Object overview		
Owner	S3 URI	
barefox400	s3://exambucket1/hallo.html	
AWS Region	Amazon Resource Name (ARN)	
US East (N. Virginia) us-east-1	arn:aws:s3:::exambucket1/hallo.html	
Last modified	Entity tag (Etag)	
October 21, 2024, 17:15:17 (UTC+05:30)	4bb847afc4bcb5e1807e04f52c7cb5e8	
Size	Object URL	
29.0 B	https://exambucket1.s3.amazonaws.com/hallo.html	
Type		
html		
Key		
hallo.html		

Amazon S3 > Buckets > exambucket1 > hallo.html > Edit access control list

Edit access control list [Info](#)

Access control list (ACL)
Grant basic read/write permissions to AWS accounts. [Learn more](#).

Grantee	Objects	Object ACL
Object owner (your AWS account)	<input checked="" type="checkbox"/> Read <input checked="" type="checkbox"/> Write	
Canonical ID: 4c36dec890e47b71d985732f74410e2f5ae9e29882ad168466799fa642756e10		
Everyone (public access) Group: http://acs.amazonaws.com/groups/global/AllUsers	<input checked="" type="checkbox"/> Read <input type="checkbox"/> Write	<input checked="" type="checkbox"/> Read <input type="checkbox"/> Write
Authenticated users group (anyone with an AWS account) Group: http://acs.amazonaws.com/groups/global/AuthenticatedUsers	<input checked="" type="checkbox"/> Read <input type="checkbox"/> Write	<input checked="" type="checkbox"/> Read <input type="checkbox"/> Write

⚠️ When you grant access to the Everyone or Authenticated users group grantees, anyone in the world can access this object.

Authenticated users group ⚠️ Read
(anyone with an AWS account)

Group:
 <http://acs.amazonaws.com/groups/global/AuthenticatedUsers>

⚠️ When you grant access to the Everyone or Authenticated users group grantees, anyone in the world can access this object.

[Learn more](#)

I understand the effects of these changes on this object.

Access for other AWS accounts
No other AWS accounts associated with the resource.

[Add grantee](#)

Specified objects

Name	Type	Version ID	Last modified	Size
 hallo.html	html	-	October 21, 2024, 17:15:17 (UTC+05:30)	29.0 B

[Cancel](#) [Save changes](#)

CloudShell Feedback

SuccessFully edited access control list for object "hallo.html".

Amazon S3 > Buckets > [exambucket1](#) > hallo.html

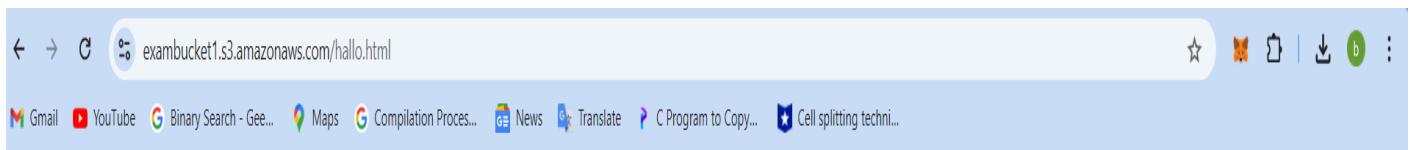
hallo.html [Info](#)

[Copy S3 URI](#) [Download](#) [Open](#) [Object actions](#)

Properties		Permissions	Versions
Object overview			
Owner	barefox400	S3 URI	s3://exambucket1/hallo.html
AWS Region	US East (N. Virginia) us-east-1	Amazon Resource Name (ARN)	arn:aws:s3:::exambucket1/hallo.html
Last modified	October 21, 2024, 17:15:17 (UTC+05:30)	Entity tag (Etag)	4bb847afc4bc5e1807e04f52c7cb5e8
Size	29.0 B	Object URL	https://exambucket1.s3.amazonaws.com/hallo.html
Type	html		
KMS			

Object overview	
Owner	S3 URI
barefox400	s3://exambucket1/hallo.html
AWS Region	Amazon Resource Name (ARN)
US East (N. Virginia) us-east-1	arn:aws:s3:::exambucket1/hallo.html
Last modified	Entity tag (Etag)
October 21, 2024, 17:15:17 (UTC+05:30)	4bb847afc4bcb5e1807e04f52c7cb5e8
Size	Object URL
29.0 B	https://exambucket1.s3.amazonaws.com/hallo.html

<https://exambucket1.s3.amazonaws.com/hallo.html>

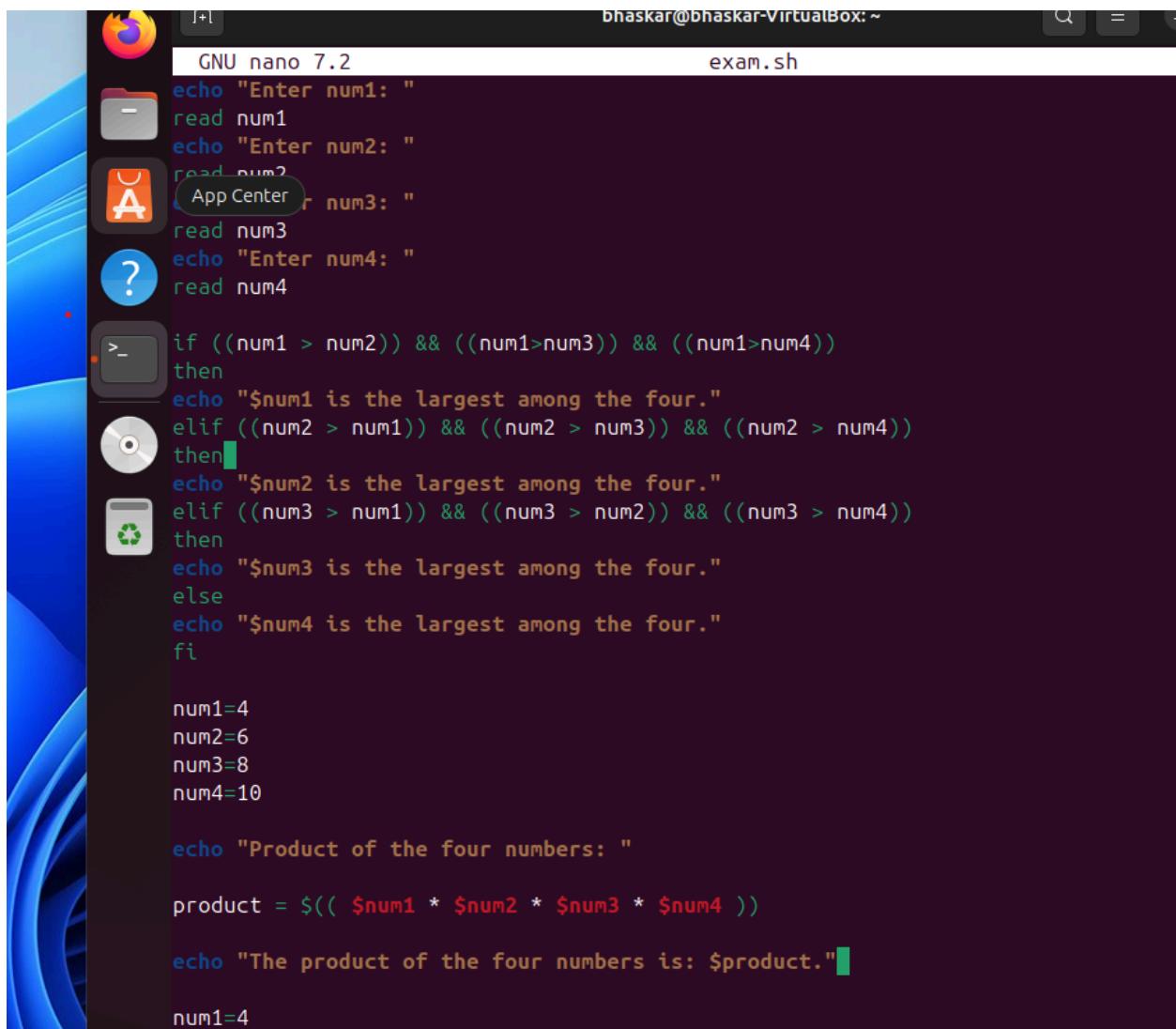


"Hello, welcome to my page."

Linux

Q1-

Code-



The screenshot shows a Linux desktop environment with a terminal window open. The terminal window title is "exam.sh" and the command line shows the path "bhaskar@bhaskar-VirtualBox: ~". The terminal content is a shell script named "exam.sh" written in GNU nano 7.2. The script prompts the user to enter four numbers (num1, num2, num3, num4) and then determines which one is the largest. It also calculates the product of all four numbers. The script uses if-else logic and arithmetic expansion. The desktop background is blue, and various icons are visible in the dock.

```
GNU nano 7.2          exam.sh
bhaskar@bhaskar-VirtualBox: ~

echo "Enter num1: "
read num1
echo "Enter num2: "
read num2
echo "Enter num3: "
read num3
echo "Enter num4: "
read num4

if ((num1 > num2)) && ((num1>num3)) && ((num1>num4))
then
echo "$num1 is the largest among the four."
elif ((num2 > num1)) && ((num2 > num3)) && ((num2 > num4))
then
echo "$num2 is the largest among the four."
elif ((num3 > num1)) && ((num3 > num2)) && ((num3 > num4))
then
echo "$num3 is the largest among the four."
else
echo "$num4 is the largest among the four."
fi

num1=4
num2=6
num3=8
num4=10

echo "Product of the four numbers: "

product = $(( $num1 * $num2 * $num3 * $num4 ))

echo "The product of the four numbers is: $product."
num1=4
```

```
echo "$num1 is the largest among the four."
elif ((num2 > num1)) && ((num2 > num3)) && ((num2 > num4))
then
echo "$num2 is the largest among the four."
elif ((num3 > num1)) && ((num3 > num2)) && ((num3 > num4))
then
echo "$num3 is the largest among the four."
else
echo "$num4 is the largest among the four."
fi

num1=4
num2=6
num3=8
num4=10

Product of the four numbers: "
product = $(( $num1 * $num2 * $num3 * $num4 ))
echo "The product of the four numbers is: $product.

num1=4
num2=6
num3=8
num4=10

echo "Average of the four numbers: "
sum = $(( $num1 + $num2 + $num3 + $num4 ))
average = $(( $sum / 4 ))
echo "The average of the four numbers is: $average."
```

Output-

```
Enter num1:
4
Enter num2:
6
Enter num3:
8
Help num4:
10
10 is the largest among the four.
```

Q2 -

```
bhaskar@bhaskar-VirtualBox:~$ mkdir bhas
bhaskar@bhaskar-VirtualBox:~$ ls
bhas          Desktop   Downloads  f2.txt      file2.txt  one.sh      permissions
.sh  Public  Templates t.sh
cliesentials.txt  Documents  exam.sh     file1.txt  Music      one.sh.save  Pictures
    snap    test.sh   Videos
```

```
bhaskar@bhaskar-VirtualBox:~$ ls
bhas          Desktop   Downloads  f2.txt      file2.txt  one.sh      permissions
.sh  Public  Templates t.sh
cliesentials.txt  Documents  exam.sh     file1.txt  Music      one.sh.save  Pictures
    snap    test.sh   Videos
bhaskar@bhaskar-VirtualBox:~$ cd Desktop
bhaskar@bhaskar-VirtualBox:~/Desktop$ pwd
/home/bhaskar/Desktop
bhaskar@bhaskar-VirtualBox:~/Desktop$ cd ..
bhaskar@bhaskar-VirtualBox:~$ mv bhas /home/bhaskar/Desktop
bhaskar@bhaskar-VirtualBox:~$ ls
cliesentials.txt  Documents  exam.sh     file1.txt  Music      one.sh.save  Pictures  sna
p    test.sh   Videos
Desktop          Downloads  f2.txt      file2.txt  one.sh  permissions.sh  Public  Tem
plates t.sh
bhaskar@bhaskar-VirtualBox:~$ cd Desktop
Trash
bhaskar@bhaskar-VirtualBox:~/Desktop$ ls
bhas  cdac-dir  cdac_f1.sh  f2.txt  newhardlink.txt  one.sh
bhaskar@bhaskar-VirtualBox:~/Desktop$ rm bhas
rm: cannot remove 'bhas': Is a directory
bhaskar@bhaskar-VirtualBox:~/Desktop$ rm --info
rm: unrecognized option '--info'
Try 'rm --help' for more information.
bhaskar@bhaskar-VirtualBox:~/Desktop$ rm --help
Usage: rm [OPTION]... [FILE]...
Remove (unlink) the FILE(s).

-f, --force           ignore nonexistent files and arguments, never prompt
-i                   prompt before every removal
-I                   prompt once before removing more than three files, or
                     when removing recursively; less intrusive than -i,
                     while still giving protection against most mistakes
--interactive[=WHEN]  prompt according to WHEN: never, once (-I), or
                     always (-i); without WHEN, prompt always
--one-file-system    when removing a hierarchy recursively, skip any
                     directory that is on a file system different from
                     that of the corresponding command line argument
```

```
--interactive[=WHEN]  prompt according to WHEN: never, once (-I), or
                     always (-i); without WHEN, prompt always
--one-file-system  when removing a hierarchy recursively, skip any
                  directory that is on a file system different from
                  that of the corresponding command line argument
--no-preserve-root  do not treat '/' specially
--preserve-root[=all]  do not remove '/' (default);
                     with 'all', reject any command line argument
                     on a separate device from its parent
-r, -R, --recursive  remove directories and their contents recursively
-d, --dir            remove empty directories
-v, --verbose        explain what is being done
--help              display this help and exit
--version           output version information and exit
```

By default, rm does not remove directories. Use the --recursive (-r or -R) option to remove each listed directory, too, along with all of its contents.

To remove a file whose name starts with a '-', for example '-foo', use one of these commands:

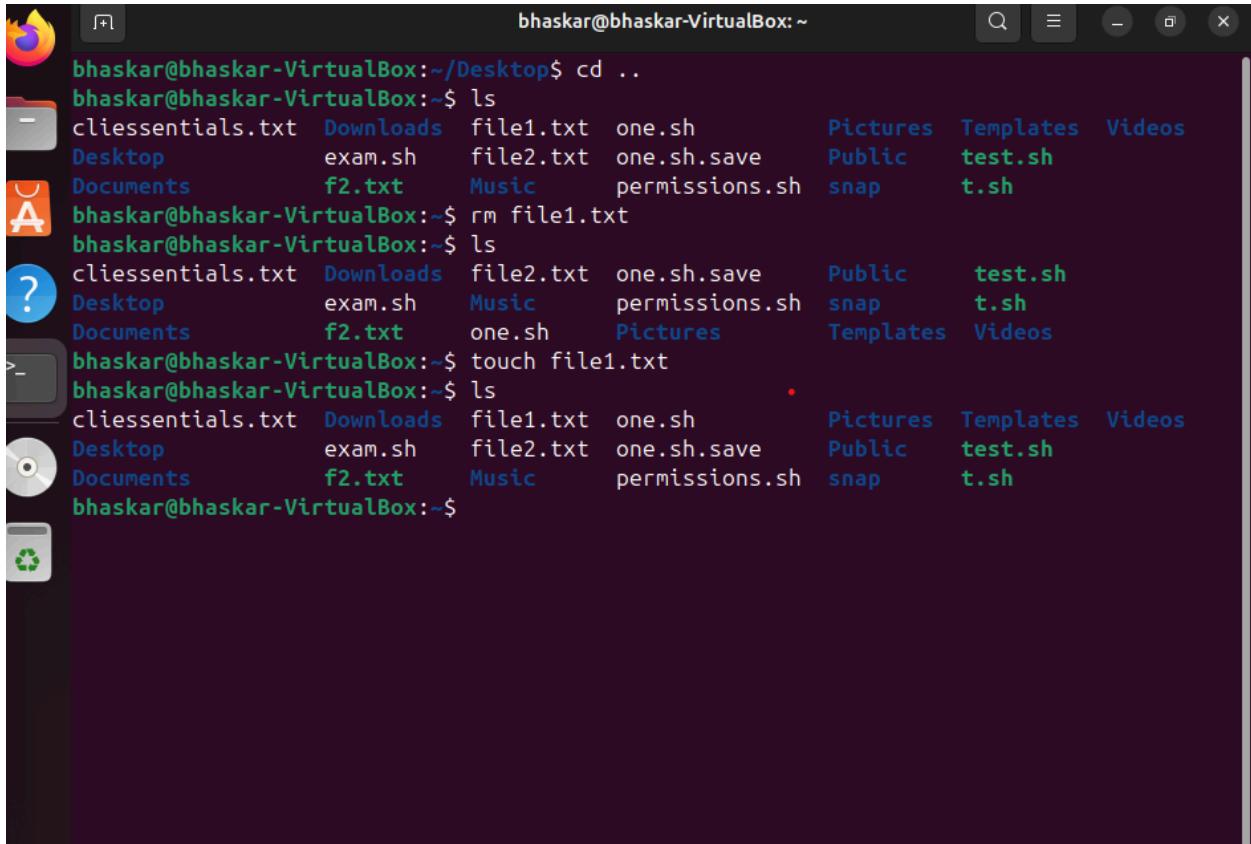
```
rm -- -foo

rm ./-foo
```

Note that if you use rm to remove a file, it might be possible to recover some of its contents, given sufficient expertise and/or time. For greater assurance that the contents are truly unrecoverable, consider using shred(1).

```
GNU coreutils online help: <https://www.gnu.org/software/coreutils/>
Full documentation <https://www.gnu.org/software/coreutils/rm>
or available locally via: info '(coreutils) rm invocation'
bhaskar@bhaskar-VirtualBox:~/Desktop$ rm -d bhas      .
```

```
bhaskar@bhaskar-VirtualBox:~/Desktop$ ls
cdac-dir  cdac_f1.sh  f2.txt  newhardlink.txt  one.sh
bhaskar@bhaskar-VirtualBox:~/Desktop$ █
```

A screenshot of a Linux desktop environment, likely Ubuntu, showing a terminal window. The terminal window has a dark purple background and contains the following command-line session:

```
bhaskar@bhaskar-VirtualBox:~/Desktop$ cd ..
bhaskar@bhaskar-VirtualBox:~$ ls
cliessentials.txt  Downloads  file1.txt  one.sh          Pictures  Templates  Videos
Desktop           exam.sh    file2.txt  one.sh.save    Public    test.sh
Documents         f2.txt    Music     permissions.sh  snap      t.sh
bhaskar@bhaskar-VirtualBox:~$ rm file1.txt
bhaskar@bhaskar-VirtualBox:~$ ls
cliessentials.txt  Downloads  file2.txt  one.sh.save    Public    test.sh
Desktop           exam.sh    Music     permissions.sh  snap      t.sh
Documents         f2.txt    Pictures   Templates       Videos
bhaskar@bhaskar-VirtualBox:~$ touch file1.txt
bhaskar@bhaskar-VirtualBox:~$ ls
cliessentials.txt  Downloads  file1.txt  one.sh          Pictures  Templates  Videos
Desktop           exam.sh    file2.txt  one.sh.save    Public    test.sh
Documents         f2.txt    Music     permissions.sh  snap      t.sh
bhaskar@bhaskar-VirtualBox:~$
```

The desktop environment includes a dock with icons for Dash, Home, Applications, Help, and Recycle Bin.