Karthick VM

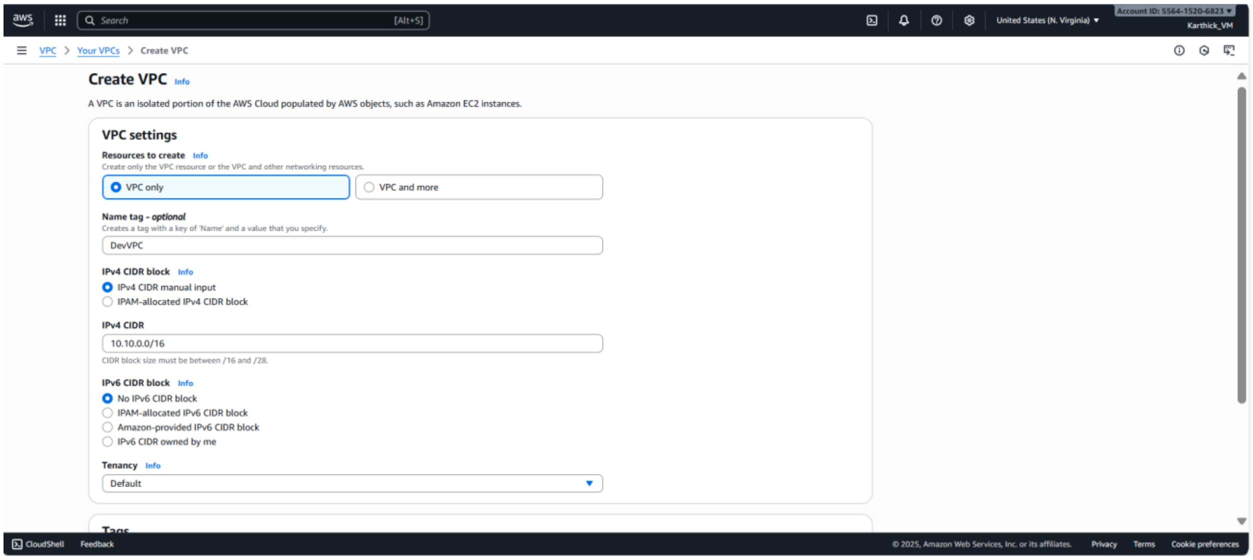
Batch – CIS 1.3

Milestone Assessment 2 – AWS – Set1

You are the AWS Administrator for LTIMindtree organization and your management has decided to implement an infrastructure with the following configurations.

1. Create a VPC
   - VPC Name: DevVPC
   - CIDR Block: 10.10.0.0/16

   Create two Subnets inside DevVPC:
   - Subnet1: 10.10.1.0/24 in AZ1
   - Subnet2: 10.10.2.0/24 in AZ2
     - Creating a VPC with specified requirements


aws
Search [Alt+S]
United States (N. Virginia) ▾
Account ID: 5564-1520-6823 ▾
Karthick_VM
VPC > Your VPCs > Create VPC
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Create VPC Info

A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as Amazon EC2 instances.

VPC settings

Resources to create Info
Create only the VPC resource or the VPC and other networking resources.
● VPC only ○ VPC and more

Name tag - *optional*
Creates a tag with a key of 'Name' and a value that you specify.
DevVPC

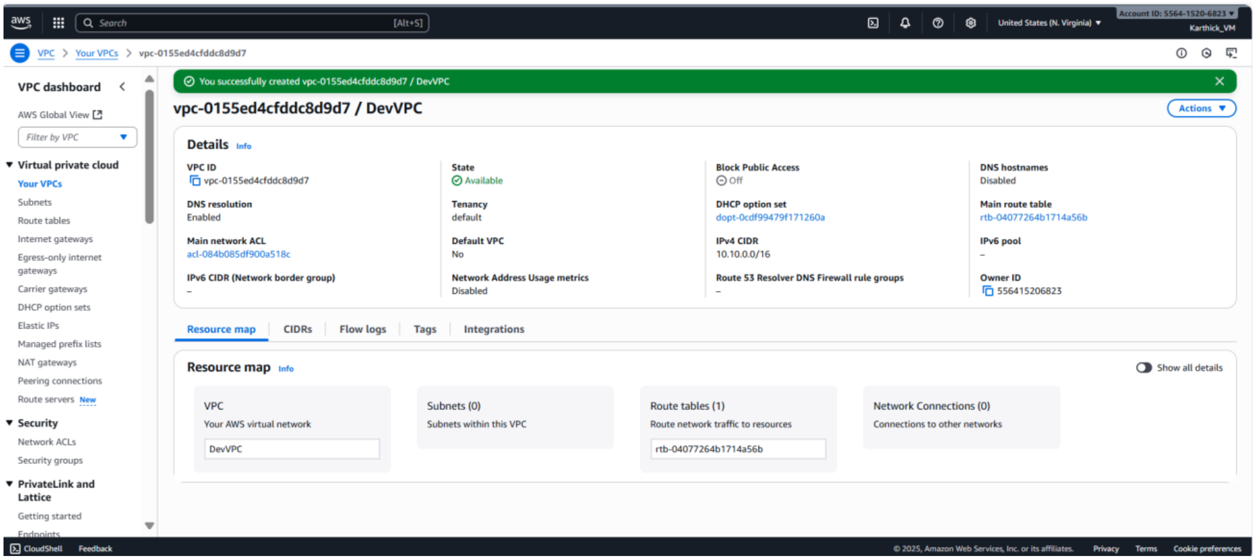
IPv4 CIDR block Info
● IPv4 CIDR manual input
○ IPAM-allocated IPv4 CIDR block

IPv4 CIDR
10.10.0.0/16
CIDR block size must be between /16 and /28.

IPv6 CIDR block Info
● No IPv6 CIDR block
○ IPAM-allocated IPv6 CIDR block
○ Amazon-provided IPv6 CIDR block
○ IPv6 CIDR owned by me

Tenancy Info
Default ▾

Tags



You successfully created vpc-0155ed4cfddc8d9d7 / DevVPC

vpc-0155ed4cfddc8d9d7 / DevVPC

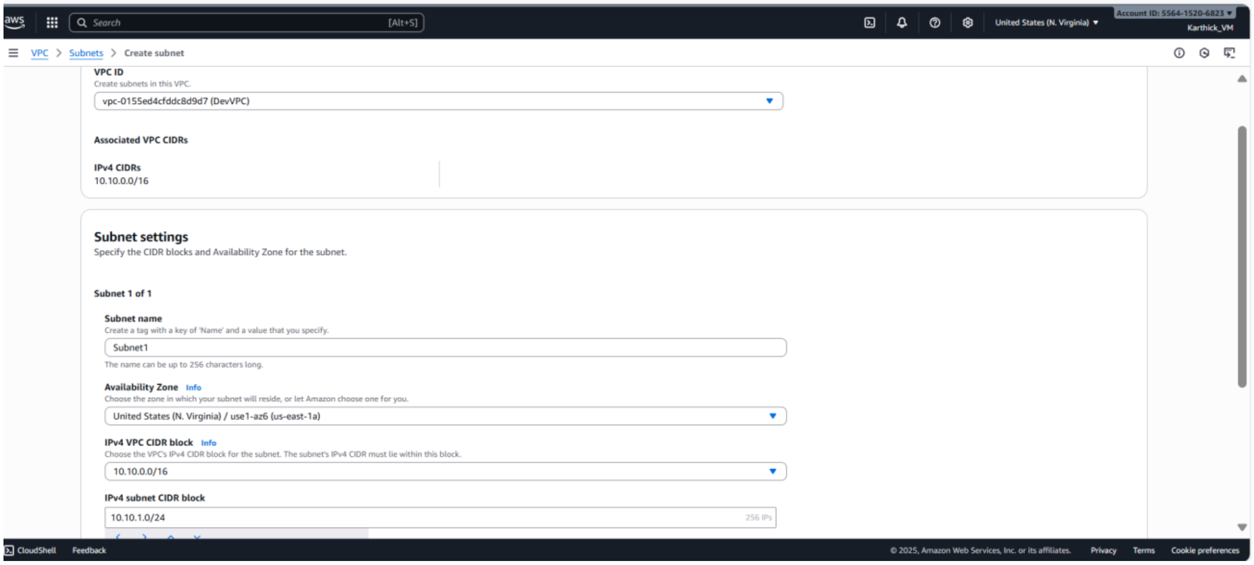
Details Info

VPC ID vpc-0155ed4cfddc8d9d7	**State** ✓ Available	**Block Public Access** Off	**DNS hostnames** Disabled
DNS resolution Enabled	**Tenancy** default	**DHCP option set** dopt-0cdf99479f171260a	**Main route table** rtb-04077264b1714a56b
Main network ACL acl-084b085df900a518c	**Default VPC** No	**IPv4 CIDR** 10.10.0.0/16	**IPv6 pool** –
IPv6 CIDR (Network border group) –	**Network Address Usage metrics** Disabled	**Route 53 Resolver DNS Firewall rule groups** –	**Owner ID** 556415206823

Resource map Info

VPC	Subnets (0)	Route tables (1)	Network Connections (0)
Your AWS virtual network	Subnets within this VPC	Route network traffic to resources	Connections to other networks
DevVPC		rtb-04077264b1714a56b	

- Creating subnet 1 with specified requirements → Zone 1 a


aws
Search [Alt+S]
United States (N. Virginia) ▾
Account ID: 5564-1520-6823 ▾
Karthick_VM
VPC > Subnets > Create subnet
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

VPC ID
Create subnets in this VPC.
vpc-0155ed4cfddc8d9d7 (DevVPC)

Associated VPC CIDRs

IPv4 CIDRs
10.10.0.0/16

Subnet settings
Specify the CIDR blocks and Availability Zone for the subnet.

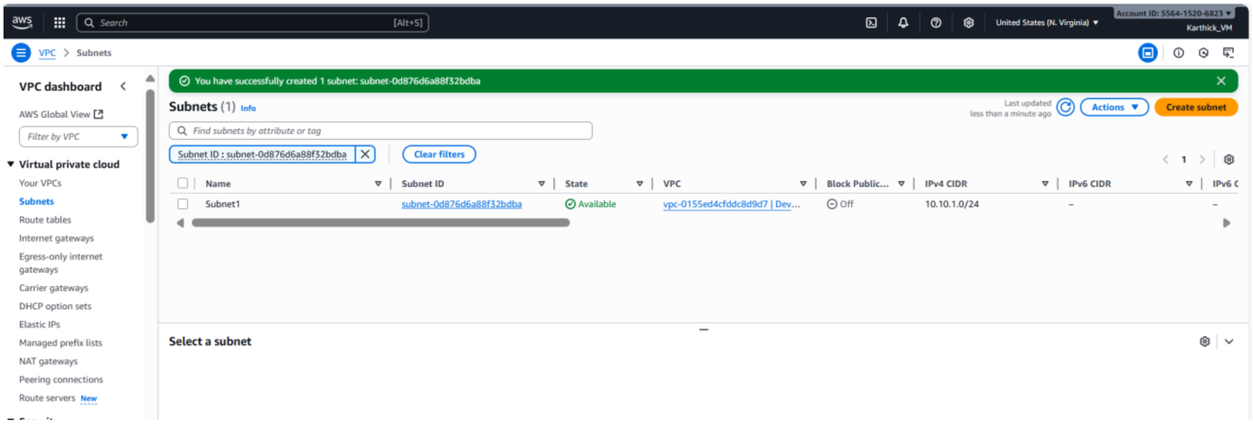
Subnet 1 of 1

Subnet name
Create a tag with a key of 'Name' and a value that you specify.
Subnet1
The name can be up to 256 characters long.

Availability Zone Info
Choose the zone in which your subnet will reside, or let Amazon choose one for you.
United States (N. Virginia) / use1-az6 (us-east-1a)

IPv4 VPC CIDR block Info
Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.
10.10.0.0/16

IPv4 subnet CIDR block
10.10.1.0/24 256 IPs



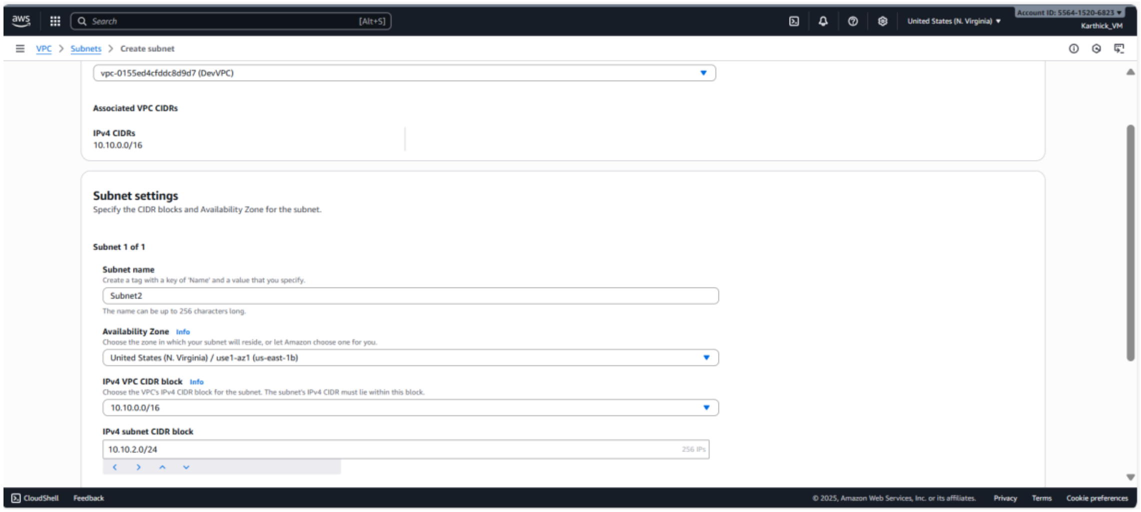
You have successfully created 1 subnet: subnet-0d876d6a88f32bdba

Subnets (1) Info

Subnet ID : subnet-0d876d6a88f32bdba

□	Name	Subnet ID	State	VPC	Block Public...	IPv4 CIDR	IPv6 CIDR	IPv6 C
□	Subnet1	subnet-0d876d6a88f32bdba	✓ Available	vpc-0155ed4cfddc8d9d7 | Dev...	Off	10.10.1.0/24	–	–

- Creating subnet 2 with specified requirements → Zone 1b



VPC > Subnets > Create subnet

vpc-0155ed4cfddc8d9d7 (DevVPC)

Associated VPC CIDRs

IPv4 CIDRs
10.10.0.0/16

Subnet settings
Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

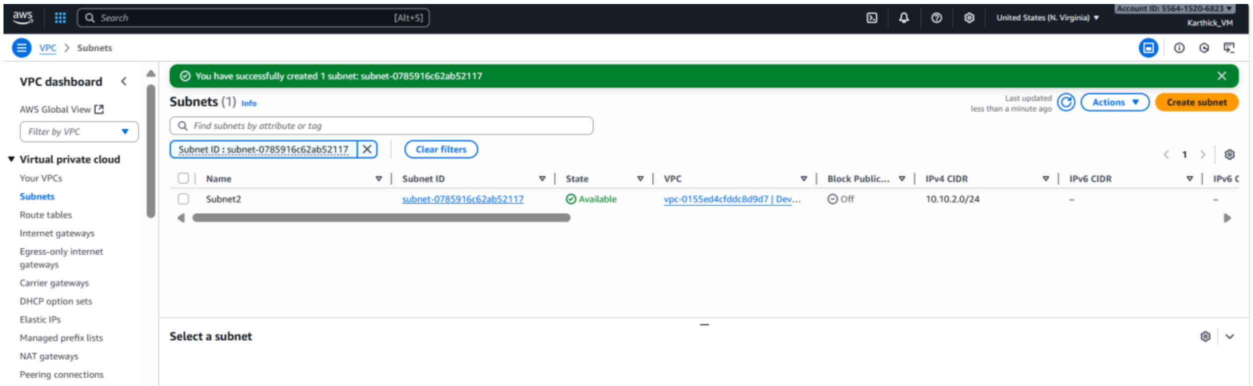
Subnet name
Create a tag with a key of 'Name' and a value that you specify.
Subnet2
The name can be up to 256 characters long.

Availability Zone Info
Choose the zone in which your subnet will reside, or let Amazon choose one for you.
United States (N. Virginia) / use1-az1 (us-east-1b)

IPv4 VPC CIDR block Info
Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.
10.10.0.0/16

IPv4 subnet CIDR block
10.10.2.0/24 256 IPs

aws
Search [Alt+S]
United States (N. Virginia)
Account ID: 5564-1520-6823
Karthick_VM
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences



VPC > Subnets

You have successfully created 1 subnet: subnet-0785916c62ab52117

Subnets (1) Info

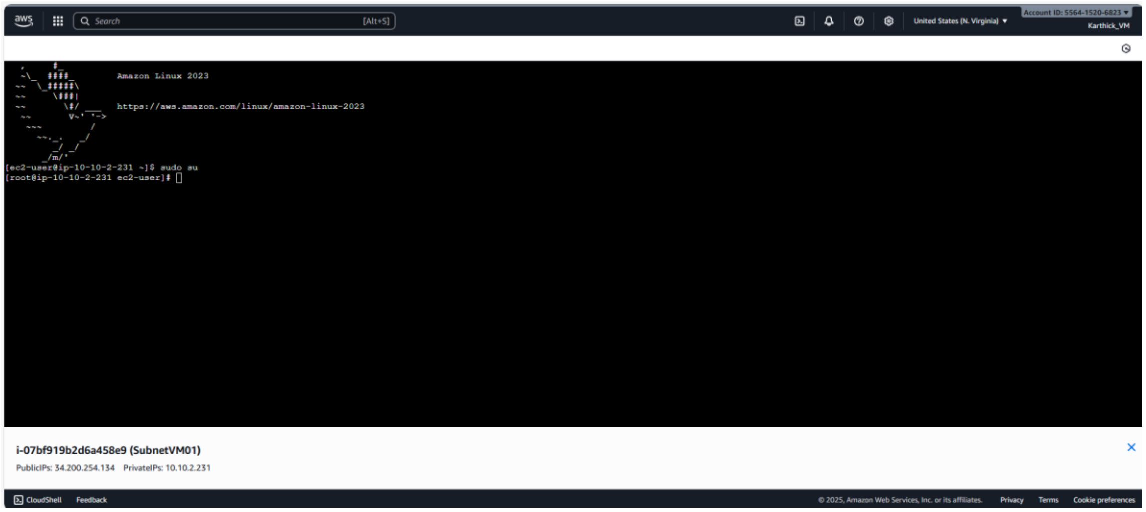
Last updated less than a minute ago

Subnet ID : subnet-0785916c62ab52117

Name	Subnet ID	State	VPC	Block Public...	IPv4 CIDR	IPv6 CIDR	IPv6 C
Subnet2	subnet-0785916c62ab52117	Available	vpc-0155ed4cfddc8d9d7 | Dev...	Off	10.10.2.0/24	–	–

Select a subnet

- Accessing the ec2 instance → i.e connect the instance → To connect via the ec2 console we want to enable ssh connection.



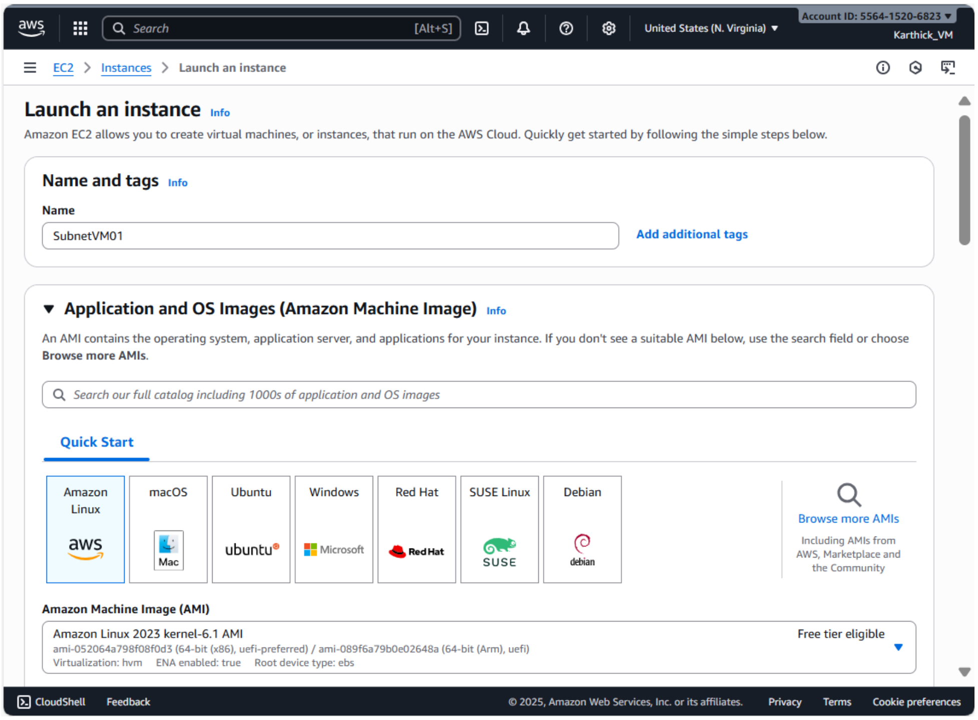
```
   ,     #_
   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\
  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
[ec2-user@ip-10-10-2-231 ~]$ sudo su
[root@ip-10-10-2-231 ec2-user]# 
```

i-07bf919b2d6a458e9 (SubnetVM01)
PublicIPs: 34.200.254.134 PrivateIPs: 10.10.2.231

aws
Search [Alt+S]
United States (N. Virginia)
Account ID: 5564-1520-6823
Karthick_VM
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

2. Create an EC2 Instance
   - Instance Name: SubnetVM01
   - AMI: Windows Server 2019 Base / Amazon Linux 2023 Kernel-6.1 AMI
   - Instance Type: t2.micro(Or t3 micro)
   - Authentication: Create Key-Pair • VPC: DevVPC
   - Subnet: Subnet2
   - Public IP: Enabled
   - Security Group: Basic rules(SSH/HTTP/RDP) : Follow Question 3 for this
   - Region: us-east-1 (N. Virginia) or Allowed Region

- Creating Ec2 with specified requirements



Account ID: 5564-1520-6823

Karthick_VM

EC2 > Instances > Launch an instance

Launch an instance

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

Name: SubnetVM01

Application and OS Images (Amazon Machine Image)

An AMI contains the operating system, application server, and applications for your instance. If you don't see a suitable AMI below, use the search field or choose Browse more AMIs.

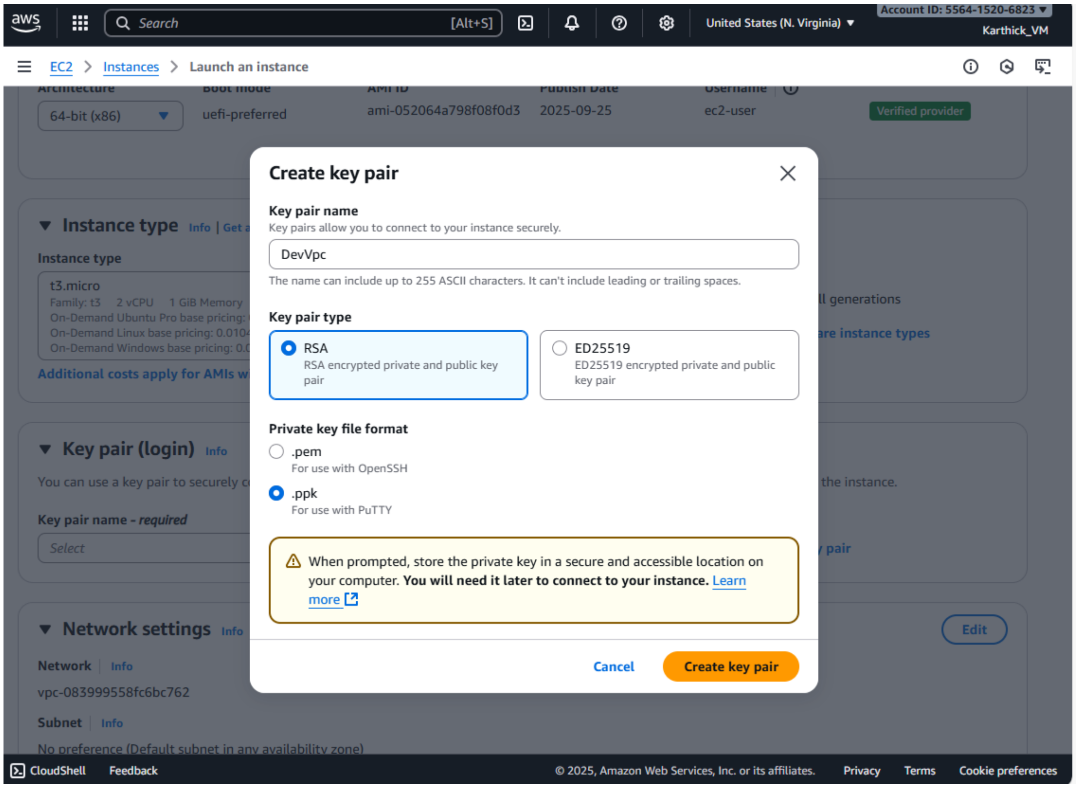
Quick Start: Amazon Linux

Amazon Machine Image (AMI)

Amazon Linux 2023 kernel-6.1 AMI — Free tier eligible
ami-052064a798f08f0d3 (64-bit (x86), uefi-preferred) / ami-089f6a79b0e02648a (64-bit (Arm), uefi)
Virtualization: hvm ENA enabled: true Root device type: ebs

aws
Search
[Alt+S]
United States (N. Virginia)
Info
Add additional tags
Search our full catalog including 1000s of application and OS images
Amazon Linux
macOS
Ubuntu
Windows
Red Hat
SUSE Linux
Debian
Mac
ubuntu
Microsoft
Red Hat
SUSE
debian
Browse more AMIs
Including AMIs from AWS, Marketplace and the Community
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

- Creating a key-pair



aws
Search [Alt+S]
United States (N. Virginia) ▾
Account ID: 5564-1520-6823 ▾
Karthick_VM
EC2 > Instances > Launch an instance

Architecture: 64-bit (x86) | Boot mode: uefi-preferred | AMI ID: ami-052064a798f08f0d3 | Publish Date: 2025-09-25 | Username: ec2-user | Verified provider

Instance type: t3.micro
Family: t3 2 vCPU 1 GiB Memory

Create key pair

Key pair name
Key pairs allow you to connect to your instance securely.

DevVpc

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

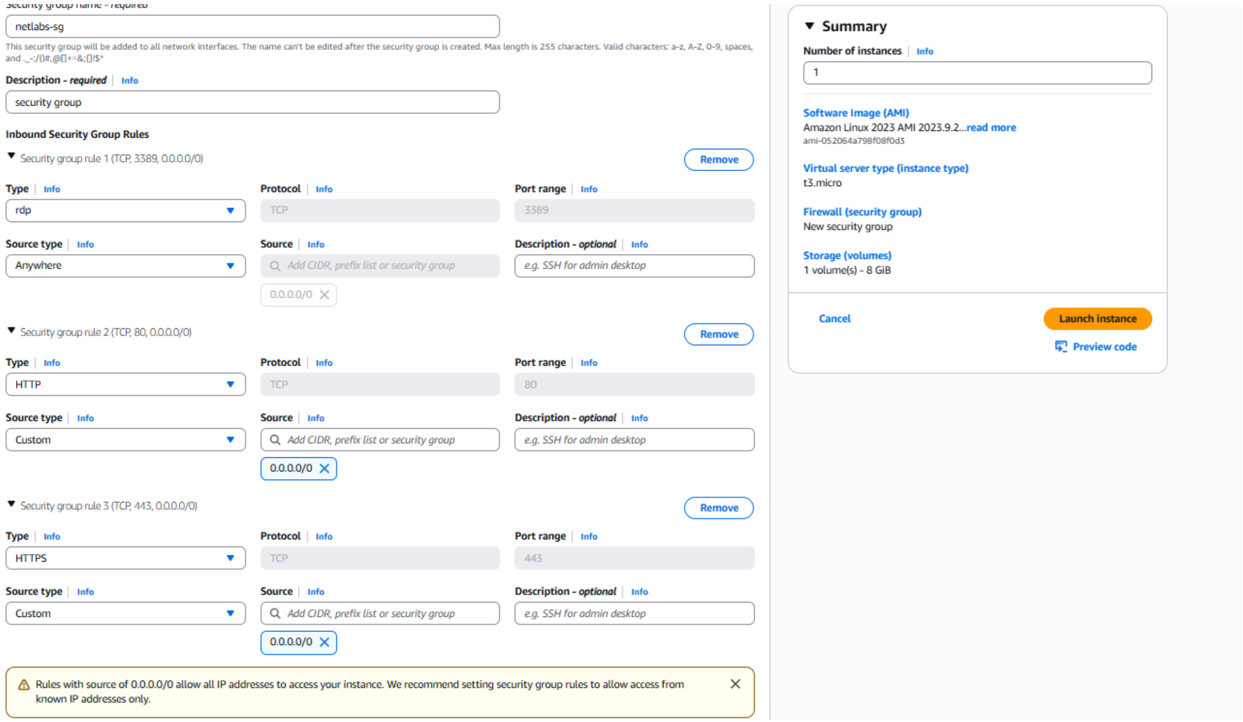
Private key file format

○ .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

- Creating Security group based on Question 3 requirements



Security group name - required
netlabs-sg
This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and ._-:/()#,@[]+=&;{}!$*

Description - required
security group

Inbound Security Group Rules

▼ Security group rule 1 (TCP, 3389, 0.0.0.0/0)

Type	Protocol	Port range
rdp	TCP	3389

Source type	Source	Description - optional
Anywhere	0.0.0.0/0	e.g. SSH for admin desktop

▼ Security group rule 2 (TCP, 80, 0.0.0.0/0)

Type	Protocol	Port range
HTTP	TCP	80

Source type	Source	Description - optional
Custom	0.0.0.0/0	e.g. SSH for admin desktop

▼ Security group rule 3 (TCP, 443, 0.0.0.0/0)

Type	Protocol	Port range
HTTPS	TCP	443

Source type	Source	Description - optional
Custom	0.0.0.0/0	e.g. SSH for admin desktop

⚠ 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: 1

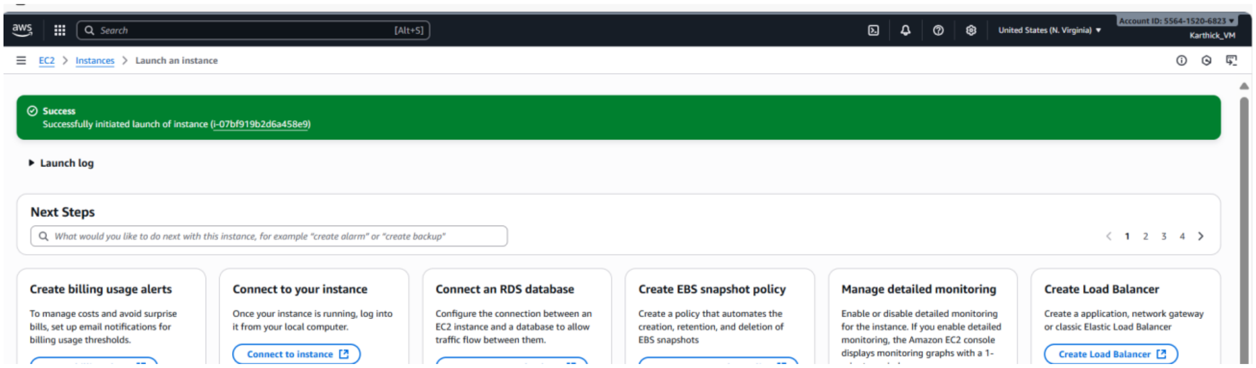
Software Image (AMI)
Amazon Linux 2023 AMI 2023.9.2...read more
ami-052064a798f08f0d3

Virtual server type (instance type)
t3.micro

Firewall (security group)
New security group

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

- Instance is Created successfully.



aws
Search [Alt+S]
United States (N. Virginia) ▾
Account ID: 5564-1520-6823 ▾
Karthick_VM
EC2 > Instances > Launch an instance

Success
Successfully initiated launch of instance (i-07bf919b2d6a458e9)

▸ Launch log

Next Steps

What would you like to do next with this instance, for example "create alarm" or "create backup"

< 1 2 3 4 >

Create billing usage alerts
To manage costs and avoid surprise bills, set up email notifications for billing usage thresholds.

Connect to your instance
Once your instance is running, log into it from your local computer.
Connect to instance

Connect an RDS database
Configure the connection between an EC2 instance and a database to allow traffic flow between them.

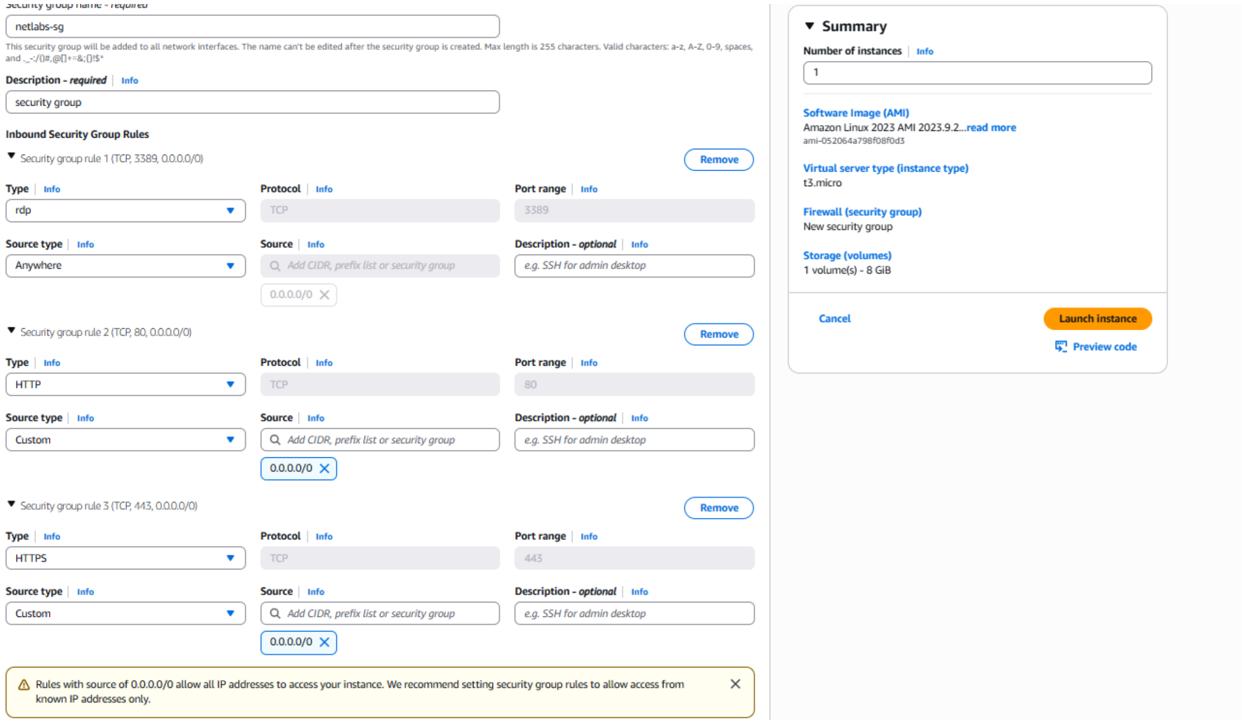
Create EBS snapshot policy
Create a policy that automates the creation, retention, and deletion of EBS snapshots

Manage detailed monitoring
Enable or disable detailed monitoring for the instance. If you enable detailed monitoring, the Amazon EC2 console displays monitoring graphs with a 1-

Create Load Balancer
Create a application, network gateway or classic Elastic Load Balancer
Create Load Balancer

3. Create a Security Group
   - Name: netlabs-sg
   - Define inbound and outbound rules as mentioned below:
     - o Inbound Rules: Allow RDP (3389), HTTP (80), HTTPS (443)
     - o Outbound Rules: Deny HTTP (80) and HTTPS (443)
   - Associate this Security Group with EC2 in Subnet2 you are creating

- Creating Security group based on specified requirements



Security group name - *required*
netlabs-sg
This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and ._-:/()#,@[]+=&;{}!$*

Description - *required* | Info
security group

Inbound Security Group Rules

▾ Security group rule 1 (TCP, 3389, 0.0.0.0/0)   Remove

Type: rdp
Protocol: TCP
Port range: 3389
Source type: Anywhere
Source: Add CIDR, prefix list or security group
0.0.0.0/0 ✕
Description - *optional*: e.g. SSH for admin desktop

▾ Security group rule 2 (TCP, 80, 0.0.0.0/0)   Remove

Type: HTTP
Protocol: TCP
Port range: 80
Source type: Custom
Source: Add CIDR, prefix list or security group
0.0.0.0/0 ✕
Description - *optional*: e.g. SSH for admin desktop

▾ Security group rule 3 (TCP, 443, 0.0.0.0/0)   Remove

Type: HTTPS
Protocol: TCP
Port range: 443
Source type: Custom
Source: Add CIDR, prefix list or security group
0.0.0.0/0 ✕
Description - *optional*: e.g. SSH for admin desktop

⚠ 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
1

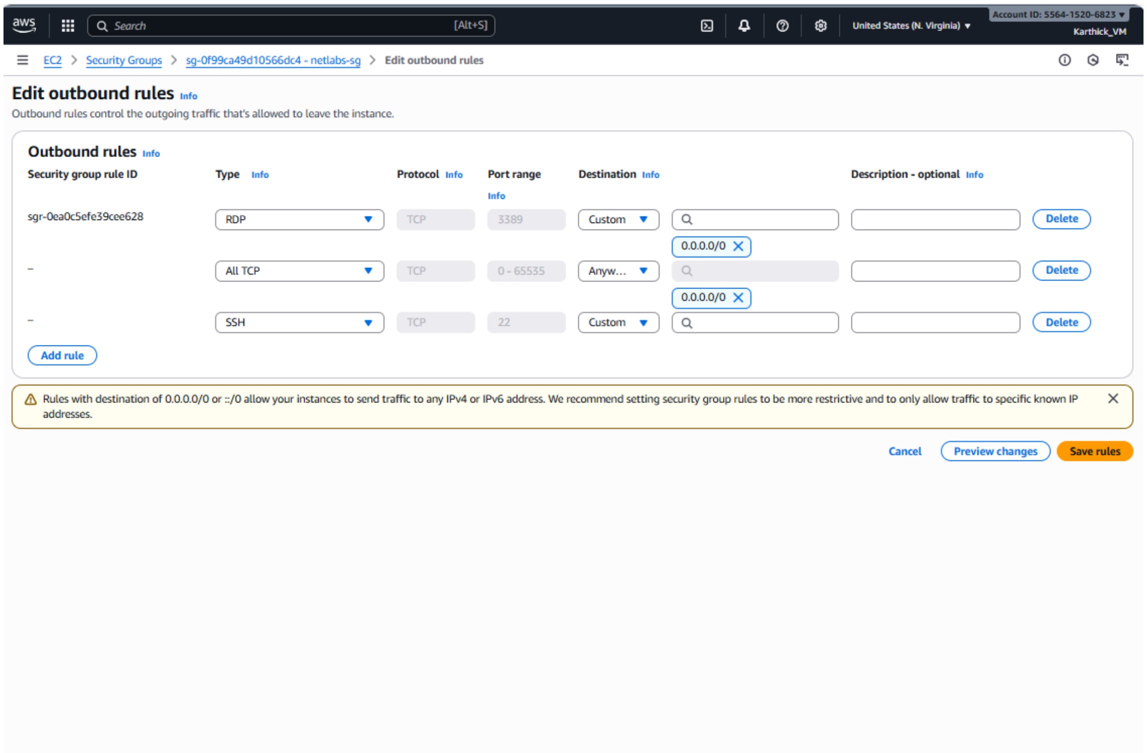
Software Image (AMI)
Amazon Linux 2023 AMI 2023.9.2...read more
ami-052064a798f08f0d3

Virtual server type (instance type)
t3.micro

Firewall (security group)
New security group

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

- Here in outbound rule we specify RDP,TCP and SSh Traffic so it automatically denied the http and https traffic



aws
Search [Alt+S]
United States (N. Virginia) ▾
Account ID: 5564-1520-6823 ▾
Karthick_VM
EC2 > Security Groups > sg-0f99ca49d10566dc4 - netlabs-sg > Edit outbound rules

Edit outbound rules Info

Outbound rules control the outgoing traffic that's allowed to leave the instance.

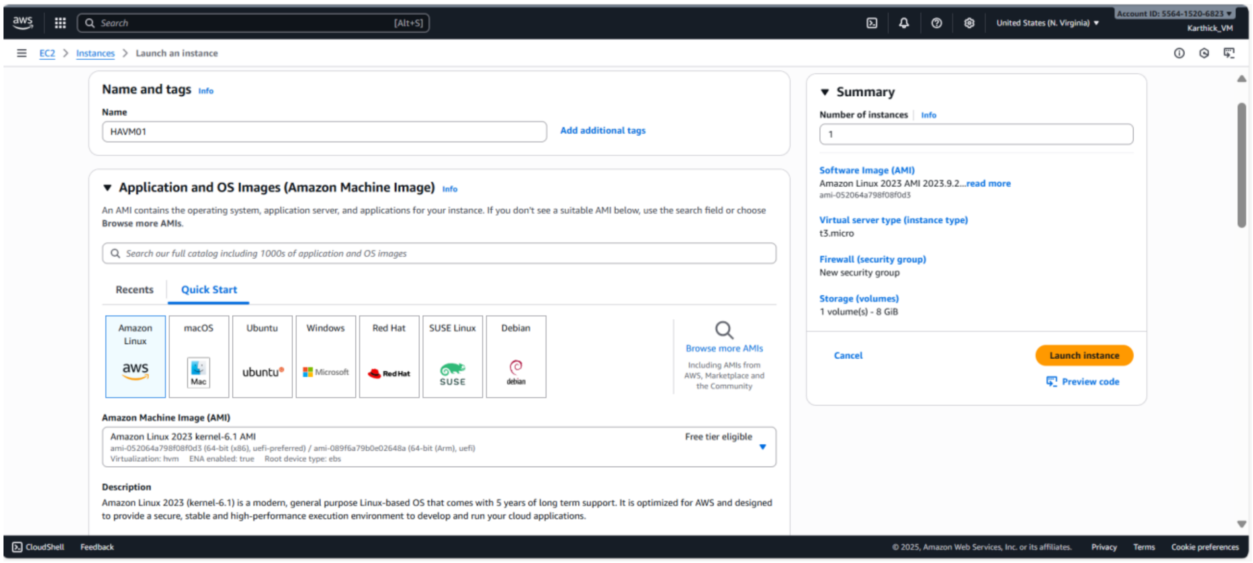
Outbound rules Info

Security group rule ID	Type Info	Protocol Info	Port range Info	Destination Info		Description - optional Info	
sgr-0ea0c5efe39cee628	RDP	TCP	3389	Custom	0.0.0.0/0		Delete
–	All TCP	TCP	0 - 65535	Anyw...	0.0.0.0/0		Delete
–	SSH	TCP	22	Custom			Delete

⚠ Rules with destination of 0.0.0.0/0 or ::/0 allow your instances to send traffic to any IPv4 or IPv6 address. We recommend setting security group rules to be more restrictive and to only allow traffic to specific known IP addresses.

4. Create an Availability Zone Setup
   • Availability Option: Availability Set equivalent in AWS → Launch multiple instances in different Availability Zones.
   • Instance Name: HAVM01
   • AMI: Windows Server 2019 Base / Amazon Linux 2023 Kernel-6.1 AMI
   • Instance Type: t2.micro(Or t3 micro)
   • Authentication: Create Key-Pair
   • VPC: DevVPC • Subnet: Subnet2
   • Public IP: Enabled
   • Security Group: Basic rules(SSH/HTTP/RDP) : Follow Question 3 for this
   • Region: us-east-1 (N. Virginia) or Allowed Region
   • Placement: Choose two different Availability Zones in us-east-1 i.e. Subnet1 of selected region for high availability.

- Creating a Ec2 Instance with specified requirements



EC2 > Instances > Launch an instance

Name and tags

Name: HAVM01

Application and OS Images (Amazon Machine Image)

An AMI contains the operating system, application server, and applications for your instance. If you don't see a suitable AMI below, use the search field or choose Browse more AMIs.

Quick Start: Amazon Linux

Amazon Machine Image (AMI)
Amazon Linux 2023 kernel-6.1 AMI — Free tier eligible
ami-052064a798f08f0d3 (64-bit (x86), uefi-preferred) / ami-089f6a79b0e02648a (64-bit (Arm), uefi)
Virtualization: hvm ENA enabled: true Root device type: ebs

Description
Amazon Linux 2023 (kernel-6.1) 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.

Summary

Number of instances: 1

Software Image (AMI): Amazon Linux 2023 AMI 2023.9.2...read more
ami-052064a798f08f0d3

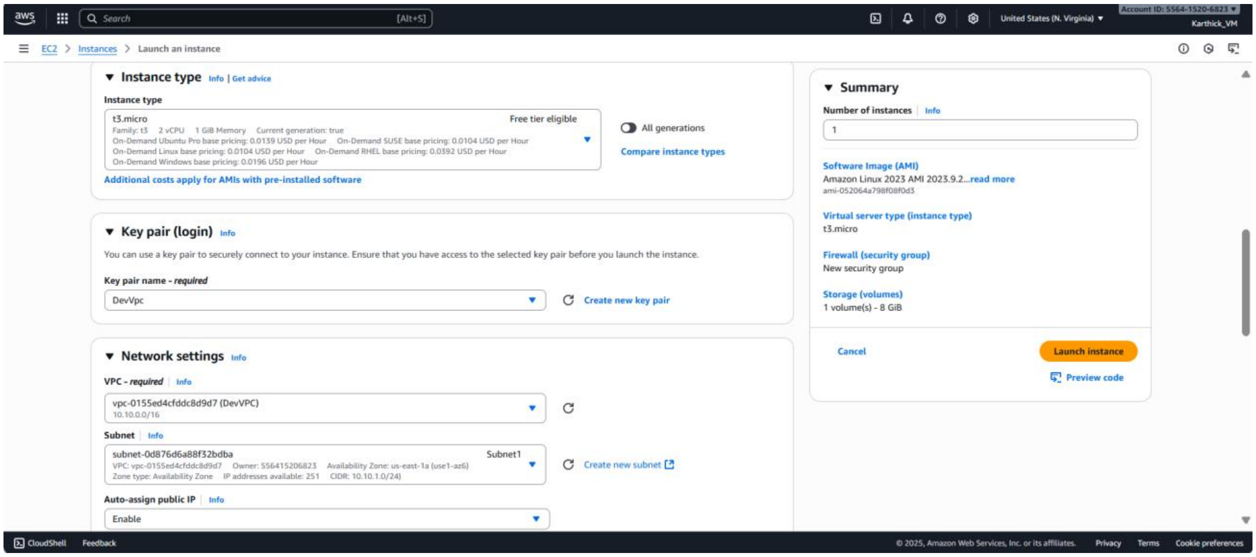
Virtual server type (instance type): t3.micro

Firewall (security group): New security group

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

Search
[Alt+S]
United States (N. Virginia)
Account ID: 5564-1520-6823
Karthick_VM
Info
Add additional tags
Search our full catalog including 1000s of application and OS images
Recents
Quick Start
Amazon Linux
macOS
Ubuntu
Windows
Red Hat
SUSE Linux
Debian
Browse more AMIs
Including AMIs from AWS, Marketplace and the Community
Cancel
Launch instance
Preview code
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

- Here we specify this ec2 in subnet 1 so it will be created in availability zone 1a , whereas the ec2 which is created using subnet 2 will be created in availability zone 1b.



EC2 > Instances > Launch an instance

Instance type

Instance type: t3.micro — Free tier eligible
Family: t3 2 vCPU 1 GiB Memory Current generation: true
On-Demand Ubuntu Pro base pricing: 0.0139 USD per Hour On-Demand SUSE base pricing: 0.0104 USD per Hour
On-Demand Linux base pricing: 0.0104 USD per Hour On-Demand RHEL base pricing: 0.0392 USD per Hour
On-Demand Windows base pricing: 0.0196 USD per Hour

Additional costs apply for AMIs with pre-installed software

Key pair (login)

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*: DevVpc

Network settings

VPC - *required*: vpc-0155ed4cfddc8d9d7 (DevVPC)
10.10.0.0/16

Subnet: subnet-0d876d6a88f32bdba — Subnet1
VPC: vpc-0155ed4cfddc8d9d7 Owner: 556415206823 Availability Zone: us-east-1a (use1-az6)
Zone type: Availability Zone IP addresses available: 251 CIDR: 10.10.1.0/24)

Auto-assign public IP: Enable

Summary

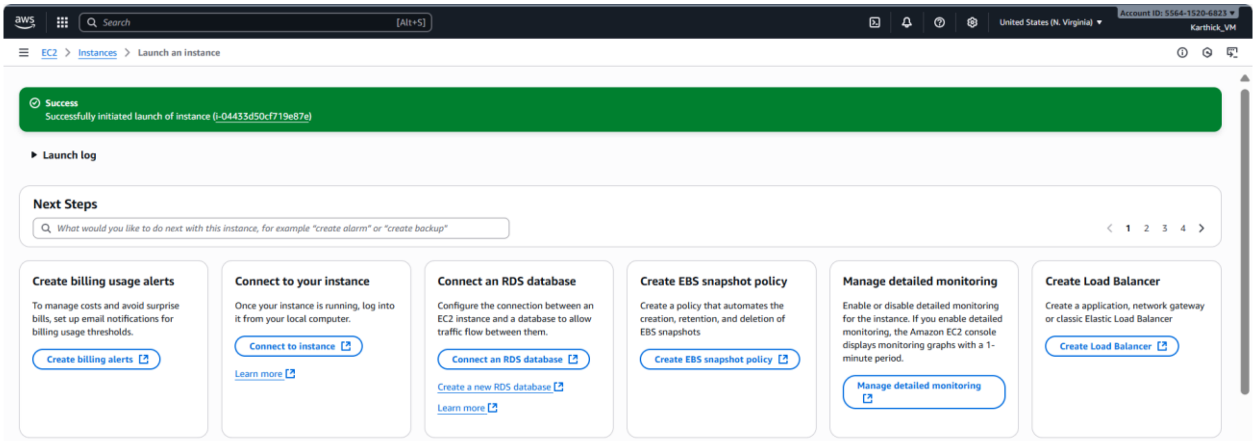
Number of instances: 1

Software Image (AMI): Amazon Linux 2023 AMI 2023.9.2...read more
ami-052064a798f08f0d3

Virtual server type (instance type): t3.micro

Firewall (security group): New security group

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



Success
Successfully initiated launch of instance (i-04433d50cf719e87e)

Launch log

Next Steps

What would you like to do next with this instance, for example "create alarm" or "create backup"

Create billing usage alerts
To manage costs and avoid surprise bills, set up email notifications for billing usage thresholds.
Create billing alerts

Connect to your instance
Once your instance is running, log into it from your local computer.
Connect to instance
Learn more

Connect an RDS database
Configure the connection between an EC2 instance and a database to allow traffic flow between them.
Connect an RDS database
Create a new RDS database
Learn more

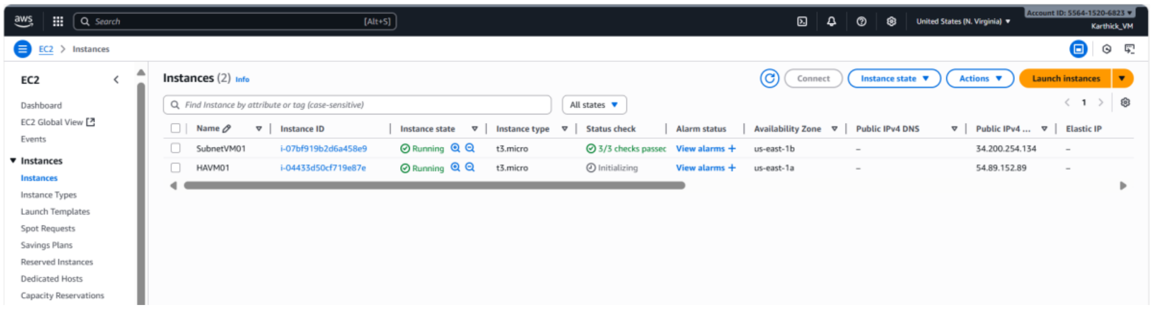
Create EBS snapshot policy
Create a policy that automates the creation, retention, and deletion of EBS snapshots
Create EBS snapshot policy

Manage detailed monitoring
Enable or disable detailed monitoring for the instance. If you enable detailed monitoring, the Amazon EC2 console displays monitoring graphs with a 1-minute period.
Manage detailed monitoring

Create Load Balancer
Create a application, network gateway or classic Elastic Load Balancer
Create Load Balancer

aws
Search [Alt+S]
United States (N. Virginia)
Account ID: 5564-1520-6823
Karthick_VM
EC2 > Instances > Launch an instance
1 2 3 4

- Here you can clearly see that the instance created in subnet 1 is created in availability zone 1a and the instance created in subnet2 is created in availability zone 1b



Instances (2)

	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP
□	SubnetVM01	i-07bf919b2d6a458e9	Running	t3.micro	3/3 checks passec	View alarms +	us-east-1b	–	34.200.254.134	–
□	HAVM01	i-04433d50cf719e87e	Running	t3.micro	Initializing	View alarms +	us-east-1a	–	54.89.152.89	–

5. Create an S3 Bucket and Generate Pre-Signed URL

   • Create a private S3 bucket (Do not make it Public).

   • Enable ACL

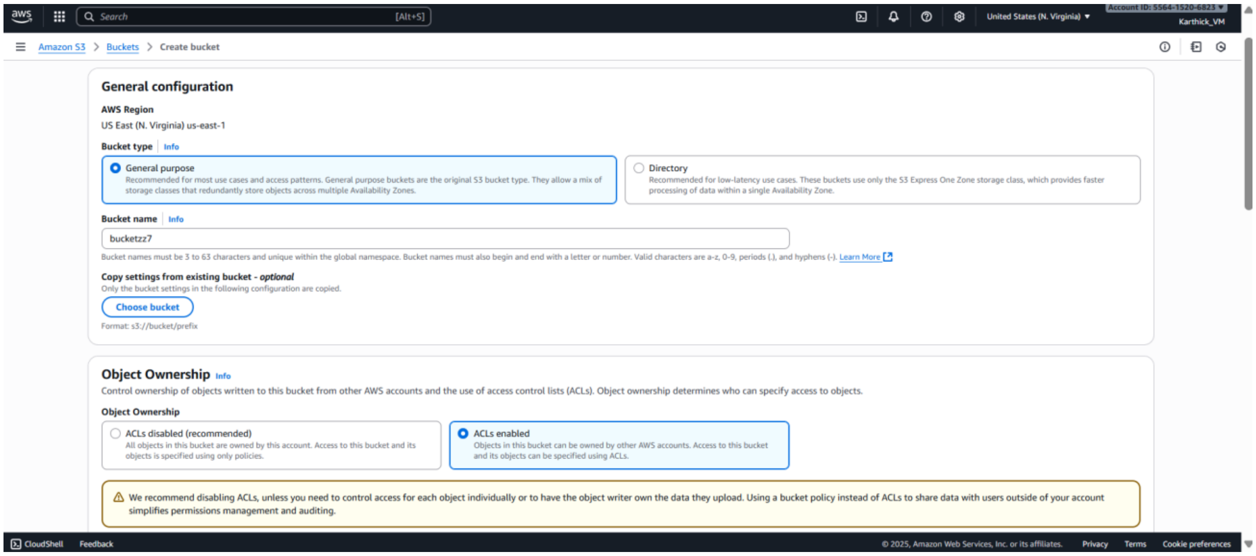
   • Create Folder name it container

   • Upload a file into a container (folder) inside the bucket.

   • Use Object Url and check whether you can see it or not, if No. How can you see with object ACL enablement.

   • Ensure that the bucket and objects are private by default

- Creating a s3 bucket with specified requirements


aws
Search [Alt+S]
United States (N. Virginia) ▼
Account ID: 5564-1520-6823 ▼
Karthick_VM
Amazon S3 > Buckets > Create bucket
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

General configuration

AWS Region

US East (N. Virginia) us-east-1

Bucket type | Info

● 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 | Info

bucketzz7

Bucket names must be 3 to 63 characters and unique within the global namespace. Bucket names must also begin and end with a letter or number. Valid characters are a-z, 0-9, periods (.), and hyphens (-). Learn More

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

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.

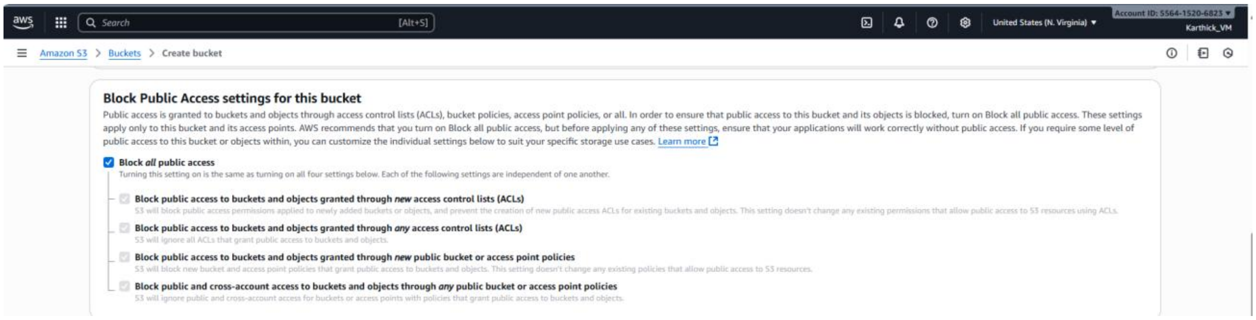
Object Ownership

○ 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.

- Blocking the public access to the bucket so that it will remain private.


aws
Search [Alt+S]
United States (N. Virginia) ▼
Account ID: 5564-1520-6823 ▼
Karthick_VM
Amazon S3 > Buckets > Create bucket

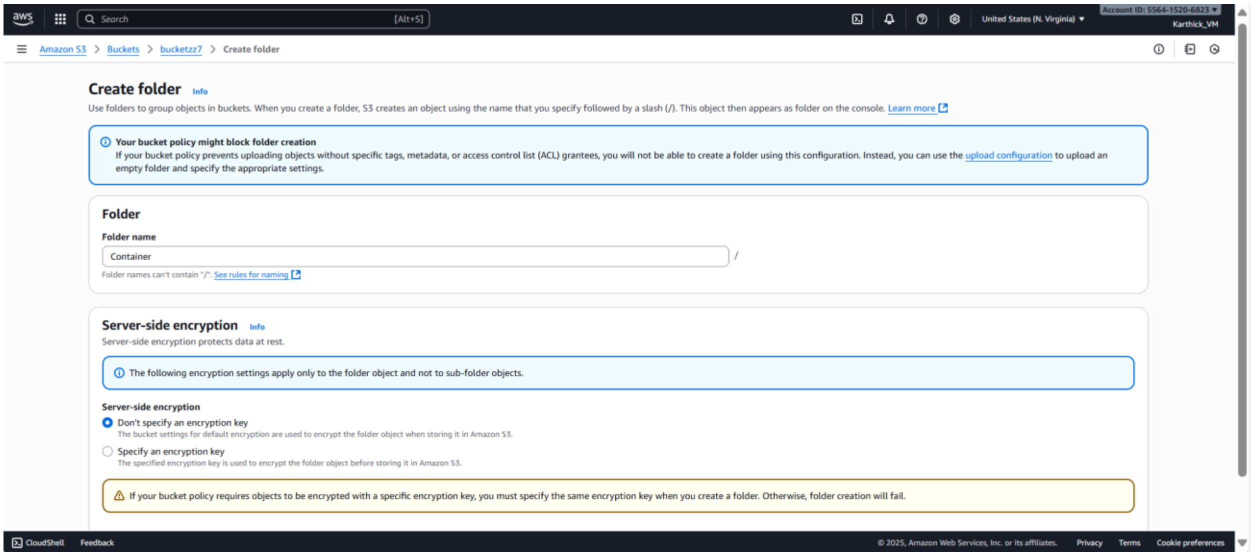
Block Public Access settings for this bucket

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

☑ **Block *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.

- Creating folder named ‘Container’


aws
Search [Alt+S]
United States (N. Virginia) ▼
Account ID: 5564-1520-6823 ▼
Karthick_VM
Amazon S3 > Buckets > bucketzz7 > Create folder
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Create folder Info

Use folders to group objects in buckets. When you create a folder, S3 creates an object using the name that you specify followed by a slash (/). This object then appears as folder on the console. Learn more

ⓘ **Your bucket policy might block folder creation**
If your bucket policy prevents uploading objects without specific tags, metadata, or access control list (ACL) grantees, you will not be able to create a folder using this configuration. Instead, you can use the upload configuration to upload an empty folder and specify the appropriate settings.

Folder

Folder name

Container /

Folder names can't contain "/". See rules for naming

Server-side encryption Info

Server-side encryption protects data at rest.

ⓘ The following encryption settings apply only to the folder object and not to sub-folder objects.

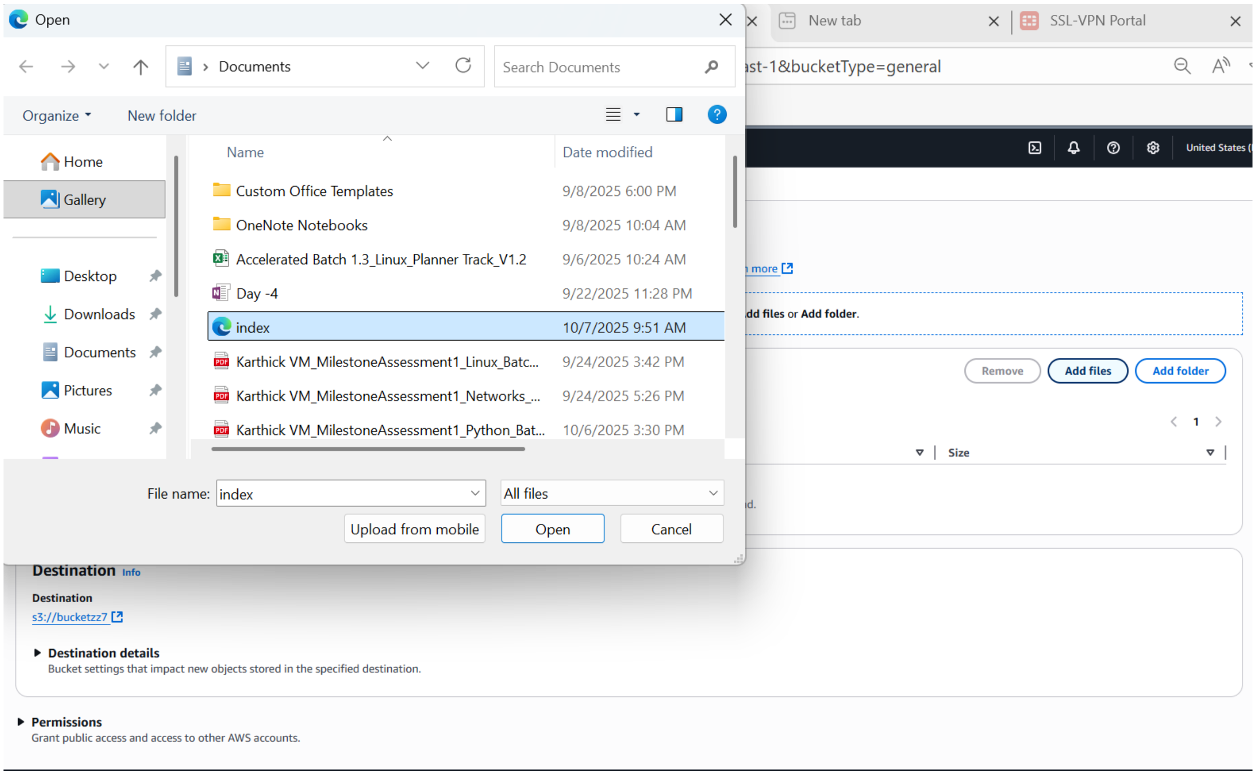
Server-side encryption

● Don't specify an encryption key
The bucket settings for default encryption are used to encrypt the folder object when storing it in Amazon S3.

○ Specify an encryption key
The specified encryption key is used to encrypt the folder object before storing it in Amazon S3.

⚠ If your bucket policy requires objects to be encrypted with a specific encryption key, you must specify the same encryption key when you create a folder. Otherwise, folder creation will fail.

- Upload files in the bucket



Name	Date modified
Custom Office Templates	9/8/2025 6:00 PM
OneNote Notebooks	9/8/2025 10:04 AM
Accelerated Batch 1.3_Linux_Planner Track_V1.2	9/6/2025 10:24 AM
Day -4	9/22/2025 11:28 PM
index	10/7/2025 9:51 AM
Karthick VM_MilestoneAssessment1_Linux_Batc...	9/24/2025 3:42 PM
Karthick VM_MilestoneAssessment1_Networks_...	9/24/2025 5:26 PM
Karthick VM_MilestoneAssessment1_Python_Bat...	10/6/2025 3:30 PM

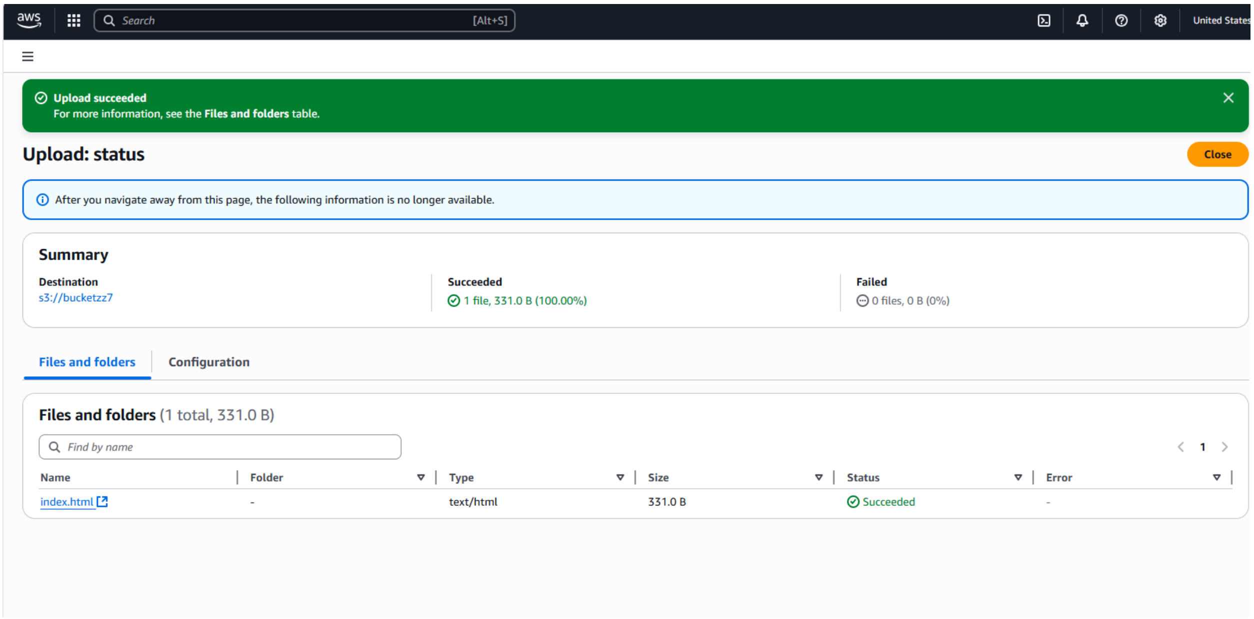
File name: index
All files
Upload from mobile · Open · Cancel

Destination Info

Destination
s3://bucketzz7

▸ Destination details
Bucket settings that impact new objects stored in the specified destination.

▸ Permissions
Grant public access and access to other AWS accounts.



Upload succeeded
For more information, see the **Files and folders** table.

Upload: status

After you navigate away from this page, the following information is no longer available.

Summary

Destination	Succeeded	Failed
s3://bucketzz7	✓ 1 file, 331.0 B (100.00%)	0 files, 0 B (0%)

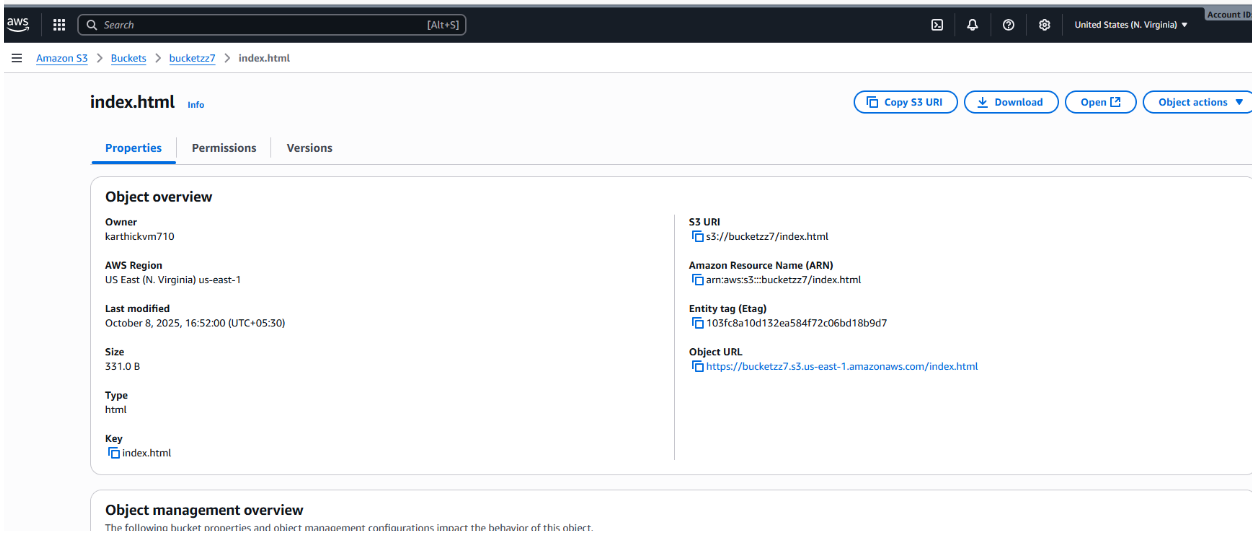
Files and folders | Configuration

Files and folders (1 total, 331.0 B)

Find by name

Name	Folder	Type	Size	Status	Error
index.html	-	text/html	331.0 B	✓ Succeeded	-

- Go to the file and there you can be able to see object url of the file → try to access it.



index.html Info

Object overview

Owner
karthickvm710

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

Last modified
October 8, 2025, 16:52:00 (UTC+05:30)

Size
331.0 B

Type
html

Key
index.html

S3 URI
s3://bucketzz7/index.html

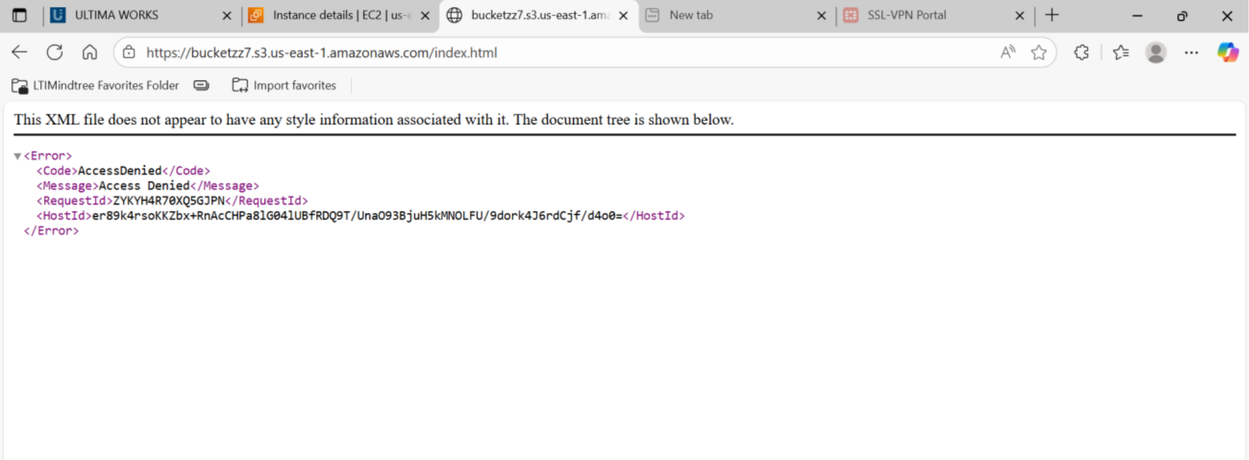
Amazon Resource Name (ARN)
arn:aws:s3:::bucketzz7/index.html

Entity tag (Etag)
103fc8a10d132ea584f72c06bd18b9d7

Object URL
https://bucketzz7.s3.us-east-1.amazonaws.com/index.html

Object management overview
The following bucket properties and object management configurations impact the behavior of this object.

- When you try to access the file using the url you will be displayed with a error message stating access denied because , The bucket and object are private by default.

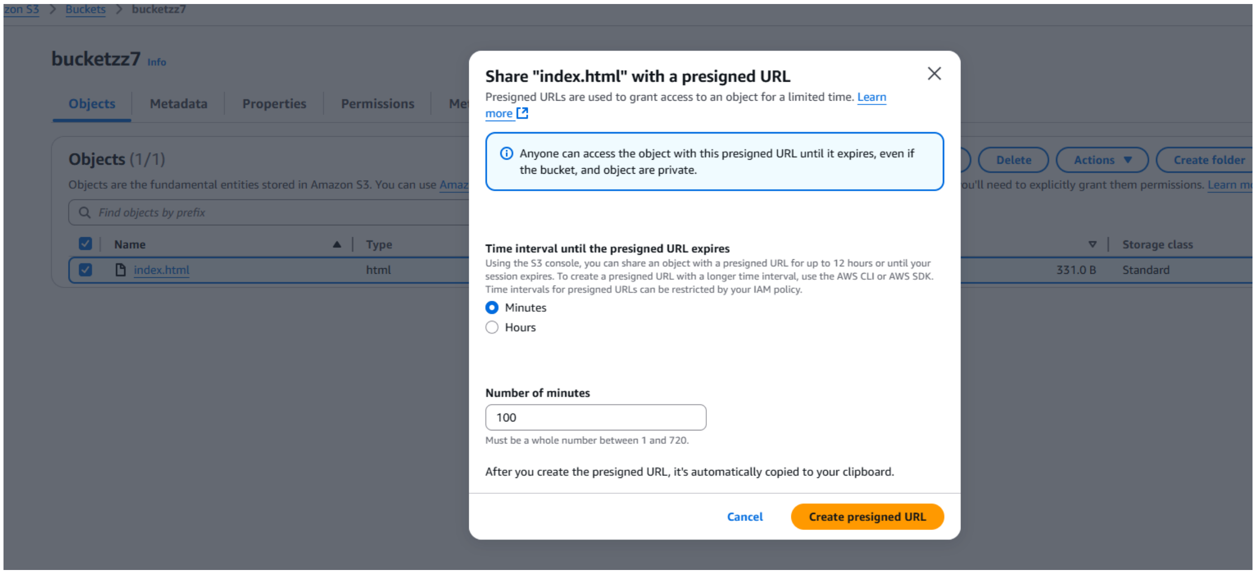


ULTIMA WORKS
Instance details | EC2 | us-
bucketzz7.s3.us-east-1.am
New tab
SSL-VPN Portal
https://bucketzz7.s3.us-east-1.amazonaws.com/index.html
LTIMindtree Favorites Folder
Import favorites

This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
▼<Error>
   <Code>AccessDenied</Code>
   <Message>Access Denied</Message>
   <RequestId>ZYKYH4R70XQ5GJPN</RequestId>
   <HostId>er89k4rsoKKZbx+RnAcCHPa8lG04lUBfRDQ9T/UnaO93BjuH5kMNOLFU/9dork4J6rdCjf/d4o0=</HostId>
 </Error>
```

- Now come back to the bucket page and click the file and click ‘actions’ there click ‘share file with presigned url’ and specify time duration.



Share "index.html" with a presigned URL

Presigned URLs are used to grant access to an object for a limited time. Learn more

Anyone can access the object with this presigned URL until it expires, even if the bucket, and object are private.

Time interval until the presigned URL expires

Using the S3 console, you can share an object with a presigned URL for up to 12 hours or until your session expires. To create a presigned URL with a longer time interval, use the AWS CLI or AWS SDK. Time intervals for presigned URLs can be restricted by your IAM policy.

● Minutes

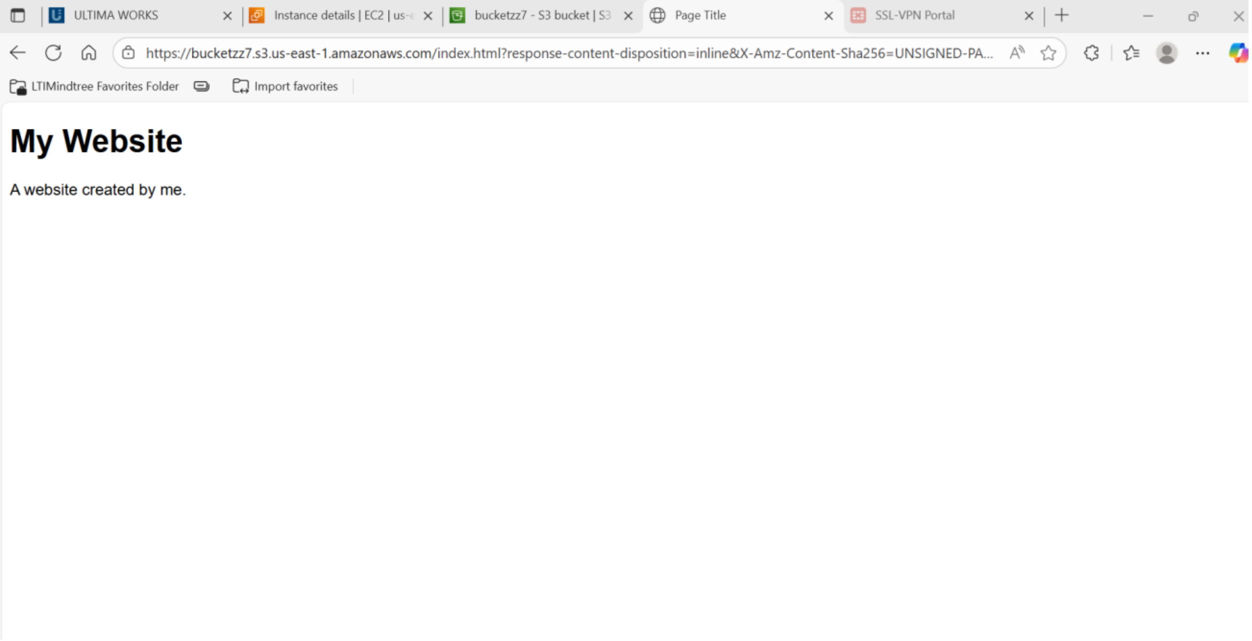
○ Hours

Number of minutes: 100

Must be a whole number between 1 and 720.

After you create the presigned URL, it's automatically copied to your clipboard.

- Now you can be able to access the file using the presigned url.



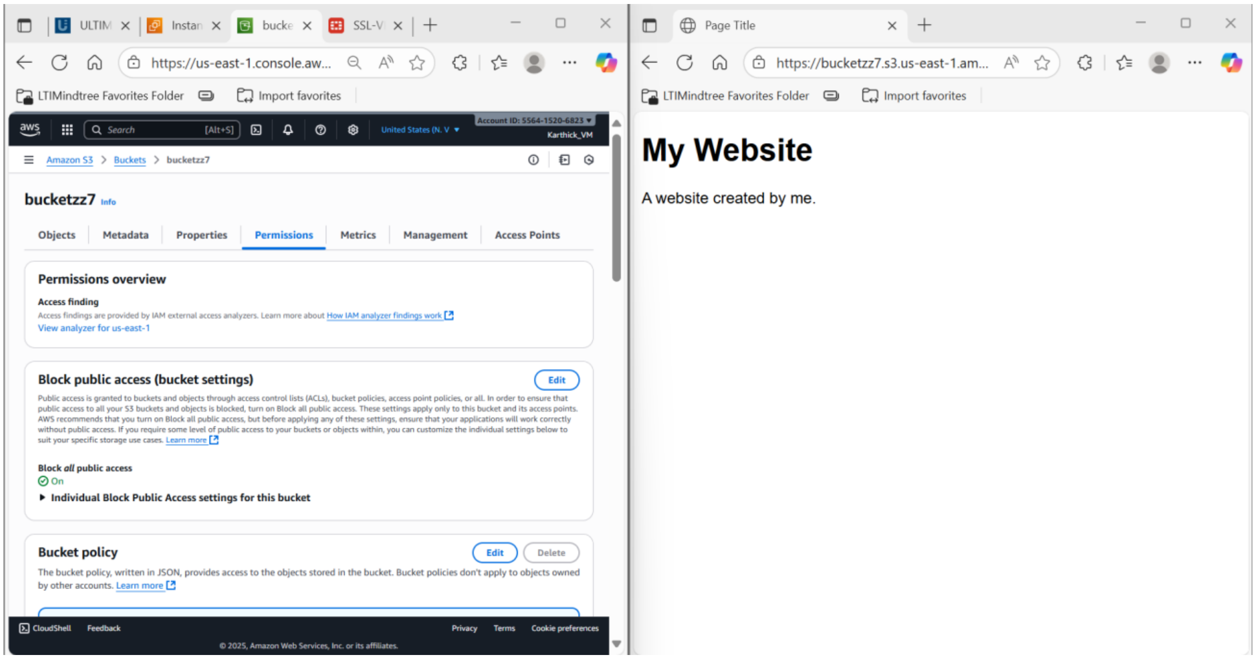
ULTIMA WORKS
Instance details | EC2 | us-
bucketzz7 - S3 bucket | S3
Page Title
SSL-VPN Portal
LTIMindtree Favorites Folder
Import favorites

https://bucketzz7.s3.us-east-1.amazonaws.com/index.html?response-content-disposition=inline&X-Amz-Content-Sha256=UNSIGNED-PA...

My Website

A website created by me.

- Here you can clearly see that the permissions of the bucket still blocks the public access i.e the bucket still remains private but on the other hand we can able to access the file content in it which is because of the presigned url.



bucketzz7 Info

Permissions overview

Access finding

Access findings are provided by IAM external access analyzers. Learn more about How IAM analyzer findings work

View analyzer for us-east-1

Block public access (bucket settings)

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and 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 your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. Learn more

Block *all* public access

✓ On

▸ Individual Block Public Access settings for this bucket

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

© 2025, Amazon Web Services, Inc. or its affiliates.

My Website

A website created by me.