

AWS, Project 01.

EC2- Based Web Server with S3 Backup

12-08-2025

Tejas Kapade.

1. Launch EC2 Instance,

The screenshot shows the 'Launch an instance' page in the AWS Management Console. At the top, there's a navigation bar with the AWS logo, a search bar, and account information (Asia Pacific (Mumbai), Account ID: 8839-1507-2455, Tejas Kapade). Below the navigation bar, the breadcrumb trail is 'EC2 > Instances > Launch an instance'. A blue banner at the top contains a message: 'It seems like you may be new to launching instances in EC2. Take a walkthrough to learn about EC2, how to launch instances and about best practices'. Below this, the 'Launch an instance' section has a sub-header 'Launch an instance' and a brief description. The main configuration area is divided into two columns. The left column contains 'Name and tags' (Name: project-EC2, Add additional tags), 'Application and OS Images (Amazon Machine Image)' (Search bar, Recents, My AMIs, Quick Start tabs, and a grid of AMIs including Amazon Linux, macOS, Ubuntu, Windows, Red Hat, SUSE Linux, and Debian), and 'Summary'. The right column contains the 'Summary' section with fields for 'Number of instances' (1), 'Software Image (AMI)' (Canonical, Ubuntu, 24.04, amd64...), 'Virtual server type (instance type)' (t3.micro), 'Firewall (security group)' (New security group), and 'Storage (volumes)' (1 volume(s) - 8 GiB). At the bottom right of the summary section are 'Cancel' and 'Launch instance' buttons, along with a 'Preview code' link. The footer includes 'CloudShell', 'Feedback', and copyright information.

2. Create S3 Bucket,

The screenshot shows the 'Create bucket' page in the AWS Management Console. The navigation bar is identical to the previous screenshot. The breadcrumb trail is 'Amazon S3 > Buckets > Create bucket'. The 'Create bucket' section has a sub-header 'Create bucket' and a brief description. The main configuration area is divided into two columns. The left column contains 'General configuration' (AWS Region: Asia Pacific (Mumbai) ap-south-1, Bucket type: General purpose, Bucket name: project01-tejaskapade, Copy settings from existing bucket - optional), and 'Object Ownership'. The right column contains the 'Directory' option. The 'General configuration' section has a 'Bucket type' section with 'General purpose' selected and 'Directory' as an alternative. The 'Bucket name' field is filled with 'project01-tejaskapade'. Below the 'Bucket name' field is a note: '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'. The 'Copy settings from existing bucket - optional' section has a 'Choose bucket' button. The 'Object Ownership' section has a sub-header 'Object Ownership' and a brief description. The footer includes 'CloudShell', 'Feedback', and copyright information.

3. Create an IAM Role for EC2, (We need EC2 to access S3 without storing keys)

The screenshot shows the 'Select trusted entity' step in the AWS IAM console. The left sidebar indicates the current step is 'Select trusted entity'. The main content area has a heading 'Select trusted entity' with an 'Info' link. Below this is a section titled 'Trusted entity type' with five radio button options: 'AWS service' (selected), 'AWS account', 'Web identity', 'SAML 2.0 federation', and 'Custom trust policy'. Each option has a brief description. Below this is a 'Use case' section with the text 'Allow an AWS service like EC2, Lambda, or others to perform actions in this account.' and a 'Service or use case' dropdown menu set to 'EC2'. At the bottom, it says 'Choose a use case for the specified service.' and 'Use case' with 'EC2' selected.

Step 1
● Select trusted entity
○ Step 2
○ Add permissions
○ Step 3
○ Name, review, and create

Select trusted entity [Info](#)

Trusted entity type

- ☒ **AWS service**
Allow AWS services like EC2, Lambda, or others to perform actions in this account.
- ☐ **AWS account**
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.
- ☐ **Web identity**
Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.
- ☐ **SAML 2.0 federation**
Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.
- ☐ **Custom trust policy**
Create a custom trust policy to enable others to perform actions in this account.

Use case
Allow an AWS service like EC2, Lambda, or others to perform actions in this account.

Service or use case
EC2

Choose a use case for the specified service.
Use case
☒ EC2

The screenshot shows the 'Add permissions' step in the AWS IAM console. The left sidebar indicates the current step is 'Add permissions'. The main content area has a heading 'Add permissions' with an 'Info' link. Below this is a section titled 'Permissions policies (1/1069)' with an 'Info' link. It says 'Choose one or more policies to attach to your new role.' There is a search bar with 'amazons3' entered and a 'Filter by Type' dropdown set to 'All types', showing '8 matches'. Below this is a table of permissions policies. The first policy, 'AmazonS3FullAccess', is selected with a checkbox. The table has columns for 'Policy name', 'Type', and 'Description'.

Step 1
○ Select trusted entity
● Add permissions
○ Step 3
○ Name, review, and create

Add permissions [Info](#)

Permissions policies (1/1069) [Info](#)

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

Search: amazons3 [X](#) Filter by Type: All types 8 matches

<input checked="" type="checkbox"/>	Policy name ?	Type	Description
<input checked="" type="checkbox"/>	AmazonS3FullAccess	AWS managed	Provides full access to all buckets via t...
<input type="checkbox"/>	AmazonS3ObjectLambdaExecutionRolePolicy	AWS managed	Provides AWS Lambda functions permi...
<input type="checkbox"/>	AmazonS3OutpostsFullAccess	AWS managed	Provides full access to Amazon S3 on ...
<input type="checkbox"/>	AmazonS3OutpostsReadOnlyAccess	AWS managed	Provides read only access to Amazon S...
<input type="checkbox"/>	AmazonS3ReadOnlyAccess	AWS managed	Provides read only access to all bucket...
<input type="checkbox"/>	AmazonS3TablesFullAccess	AWS managed	Provides full access to all S3 table buc...
<input type="checkbox"/>	AmazonS3TablesLakeFormationServiceRole	AWS managed	This managed policy grants AWS Lake ...
<input type="checkbox"/>	AmazonS3TablesReadOnlyAccess	AWS managed	Provides read only access to all S3 tabl...

aws

Search

[Alt+S]

Global

Account ID: 8839-1507-2455

Tejas Kapade

IAM

Roles

Create role

Step 1

Select trusted entity

Step 2

Add permissions

Step 3

Name, review, and create

Name, review, and create

Role details

Role name
Enter a meaningful name to identify this role.

Maximum 64 characters. Use alphanumeric and '+=, @-./[]!#\$%^&*()_{}~`' characters.

Description
Add a short explanation for this role.

Maximum 1000 characters. Use letters (A-Z and a-z), numbers (0-9), tabs, new lines, or any of the following characters: +=, @-./[]!#\$%^&*()_{}~`'.

Step 1: Select trusted entities

Trust policy

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Action": [
```

CloudShell

Feedback

© 2025, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

aws

Search

[Alt+S]

Global

Account ID: 8839-1507-2455

Tejas Kapade

IAM

Roles

Create role

Step 1

Select trusted entity

Step 2

Add permissions

Step 3

Add tags

Step 1: Select trusted entities

Trust policy

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Action": [
7         "sts:AssumeRole"
8       ],
9       "Principal": {
10        "Service": [
11          "ec2.amazonaws.com"
12        ]
13      }
14    }
15  ]
16 }
```

Step 2: Add permissions

Permissions policy summary

Policy name	Type	Attached as
AmazonS3FullAccess	AWS managed	Permissions policy

Step 3: Add tags

CloudShell

Feedback

© 2025, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

4. Attach IAM Role to EC2 Instance,

The image shows two screenshots from the AWS Management Console. The top screenshot displays the 'Instance summary' for an EC2 instance with ID `i-0a0caaff9950e1f65`. The instance is in a 'Running' state. A dropdown menu is open under the 'Actions' button, showing options like 'Change security groups', 'Get Windows password', and 'Modify IAM role'. The bottom screenshot shows the 'Modify IAM role' page for the same instance. It allows selecting an existing IAM role or creating a new one. The role 'Project01-EC2-S3' is currently selected.

Instance summary for i-0a0caaff9950e1f65 (project-EC2)

Updated less than a minute ago

Instance ID
i-0a0caaff9950e1f65

IPv6 address
-

Hostname type
IP name: ip-172-31-14-104.ap-south-1.compute.internal

Answer private resource DNS name
IPv4 (A)
13.201.98.31 [Public IP]

Auto-assigned IP address
13.201.98.31 [Public IP]

IAM Role
-

IMDSv2
Required

Operator
-

Public IPv4 address
13.201.98.31 | open address

Instance state
Running

Private IP DNS name (IPv4 only)
ip-172-31-14-104.ap-south-1.compute.internal

Instance type
t3.micro

VPC ID
vpc-0cd504adea6fa8c5c

Subnet ID
subnet-0e522ba0dc37163a1

Instance ARN
arn:aws:ec2:ap-south-1:883915072455:instance/i-0a0caaff9950e1f65

Private IPv4 addresses
172.31.14.104

Elastic IP addresses
-

AWS Compute Optimizer finding
Opt-in to AWS Compute Optimizer for recommendations. | Learn more

Auto Scaling Group name
-

Managed
false

Actions
Instance diagnostics
Instance settings
Networking
Security
Image and templates
Monitor and troubleshoot

Modify IAM role

Attach an IAM role to your instance.

Instance ID
i-0a0caaff9950e1f65 (project-EC2)

IAM role
Select an IAM role to attach to your instance or create a new role if you haven't created any. The role you select replaces any roles that are currently attached to your instance.

Project01-EC2-S3

Create new IAM role

Cancel Update IAM role

Successfully attached Project01-EC2-S3 to instance i-0a0caaff9950e1f65

Instances (1/1) Info Last updated less than a minute ago [Connect](#) [Instance state](#) [Actions](#) [Launch instances](#)

Find Instance by attribute or tag (case-sensitive) [All states](#)

<input checked="" type="checkbox"/>	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4
<input checked="" type="checkbox"/>	project-EC2	i-0a0caaff9950e1f65	Running	t3.micro	3/3 checks passed	View alarms	ap-south-1b	ec2-13-201-

i-0a0caaff9950e1f65 (project-EC2)

[Details](#) [Status and alarms](#) [Monitoring](#) [Security](#) [Networking](#) [Storage](#) [Tags](#)

▼ Instance summary Info

Instance ID i-0a0caaff9950e1f65	Public IPv4 address 13.201.98.31 open address	Private IPv4 addresses 172.31.14.104
IPv6 address -	Instance state Running	Public DNS ec2-13-201-98-31.ap-south-1.compute.amazonaws.com open address
Hostname type IP name: ip-172-31-14-104.ap-south-1.compute.internal	Private IP DNS name (IPv4 only) ip-172-31-14-104.ap-south-1.compute.internal	Elastic IP addresses
Answer private resource DNS name	Instance type	

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

5. Install Apache on EC2,

```
ubuntu@ip-172-31-14-104: ~$
System information as of Tue Aug 12 05:31:20 UTC 2025

System load:  0.0          Temperature:    -273.1 C
Usage of /:   25.4% of 6.71GB  Processes:      107
Memory usage: 22%          Users logged in: 0
Swap usage:   0%            IPv4 address for ens5: 172.31.14.104

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-172-31-14-104:~$
```

```
root@ip-172-31-14-104: /home/ubuntu#  
root@ip-172-31-14-104: /home/ubuntu#  
root@ip-172-31-14-104: /home/ubuntu#  
root@ip-172-31-14-104: /home/ubuntu# apt install apache2  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
The following additional packages will be installed:  
  apache2-bin apache2-data apache2-utils libapr1t64 libaprutil1-dbd-sqlite3 libaprutil1-ldap libaprutil1t64  
  liblua5.4-0 ssl-cert  
Suggested packages:  
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom www-browser  
The following NEW packages will be installed:  
  apache2 apache2-bin apache2-data apache2-utils libapr1t64 libaprutil1-dbd-sqlite3 libaprutil1-ldap libaprutil1t64  
  liblua5.4-0 ssl-cert  
0 upgraded, 10 newly installed, 0 to remove and 105 not upgraded.  
Need to get 2086 kB of archives.  
After this operation, 8090 kB of additional disk space will be used.  
Do you want to continue? [Y/n]
```

6. Install AWS CLI on EC2 and test it,

```
root@ip-172-31-14-104: /home/ubuntu#  
root@ip-172-31-14-104: /home/ubuntu#  
root@ip-172-31-14-104: /home/ubuntu# snap install aws-cli --classic  
Download snap "aws-cli" (1543) from channel "v2/stable" 68% 15.2MB/s 1.23s
```

```
root@ip-172-31-14-104: /home/ubunt#  
root@ip-172-31-14-104: /home/ubunt#  
root@ip-172-31-14-104: /home/ubunt# snap install aws-cli --classic  
aws-cli (v2/stable) 2.27.53 from Amazon Web Services (aws✓) installed  
root@ip-172-31-14-104: /home/ubunt#  
root@ip-172-31-14-104: /home/ubunt#  
root@ip-172-31-14-104: /home/ubunt# aws sts get-caller-identity  
{  
  "UserId": "ARO43TLRUPD4535J76IB:i-0a0caaff9950e1f65",  
  "Account": "883915072455",  
  "Arn": "arn:aws:sts::883915072455:assumed-role/Project01-EC2-S3/i-0a0caaff9950e1f65"  
}  
root@ip-172-31-14-104: /home/ubunt#
```

7. Upload Files/Backups to S3,

aws

Search

[Alt+S]

Asia Pacific (Mumbai)

Account ID: 8839-1507-2455

Tejas Kapade

Amazon S3

Buckets

project01-tejaskapade

Upload

Upload

Info

Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDKs or Amazon S3 REST API. [Learn more](#)

Drag and drop files and folders you want to upload here, or choose **Add files** or **Add folder**.

Files and folders (1 total, 2.7 KB)

Remove

Add files

Add folder

All files and folders in this table will be uploaded.

Find by name

< 1 >

<input type="checkbox"/>	Name	Folder	Type	Size
<input type="checkbox"/>	index.html	-	text/html	2.7 KB

Destination

Info

Destination

[s3://project01-tejaskapade](#)

Destination details

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

Permissions

CloudShell

Feedback

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

Privacy

Terms

Cookie preferences

8. We will remove default index.html of apache, and sync our S3 bucket to that file path which is /var/www/html/ and sync our index.html file which is created in S3 bucket.

```
root@ip-172-31-14-104: /home/ubuntu#  
root@ip-172-31-14-104: /home/ubuntu#  
root@ip-172-31-14-104: /home/ubuntu#  
root@ip-172-31-14-104: /home/ubuntu#  
root@ip-172-31-14-104: /home/ubuntu#  
root@ip-172-31-14-104: /home/ubuntu# rm -rf /var/www/html/index.html  
root@ip-172-31-14-104: /home/ubuntu#  
root@ip-172-31-14-104: /home/ubuntu#  
root@ip-172-31-14-104: /home/ubuntu# sudo aws s3 cp s3://project01-tejaskapade/index.html /var/www/html/index.html
```

```
root@ip-172-31-14-104: /home/ubuntu#  
root@ip-172-31-14-104: /home/ubuntu#  
root@ip-172-31-14-104: /home/ubuntu#  
root@ip-172-31-14-104: /home/ubuntu#  
root@ip-172-31-14-104: /home/ubuntu#  
root@ip-172-31-14-104: /home/ubuntu# rm -rf /var/www/html/index.html  
root@ip-172-31-14-104: /home/ubuntu#  
root@ip-172-31-14-104: /home/ubuntu#  
root@ip-172-31-14-104: /home/ubuntu# sudo aws s3 cp s3://project01-tejaskapade/index.html /var/www/html/index.html  
fatal error: An error occurred (404) when calling the HeadObject operation: Key "index.html" does not exist  
root@ip-172-31-14-104: /home/ubuntu#  
root@ip-172-31-14-104: /home/ubuntu#  
root@ip-172-31-14-104: /home/ubuntu# sudo aws s3 cp s3://project01-tejaskapade/index.html /var/www/html/index.html  
download: s3://project01-tejaskapade/index.html to ../../var/www/html/index.html  
root@ip-172-31-14-104: /home/ubuntu# |
```

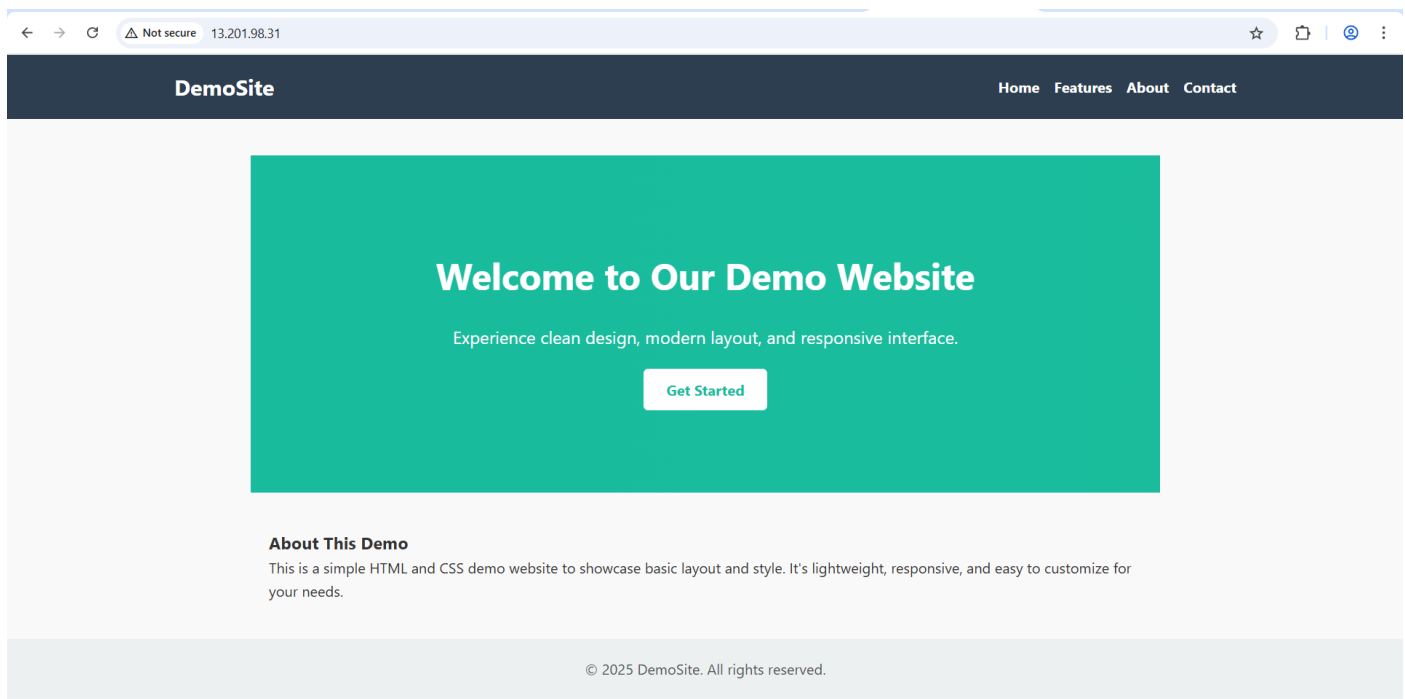
Download success


```
root@ip-172-31-14-104: /var/v x + v
root@ip-172-31-14-104:/home/ubuntu#
root@ip-172-31-14-104:/home/ubuntu#
root@ip-172-31-14-104:/home/ubuntu#
root@ip-172-31-14-104:/home/ubuntu# cd /var/www/html
root@ip-172-31-14-104:/var/www/html#
root@ip-172-31-14-104:/var/www/html# ls
index.html
root@ip-172-31-14-104:/var/www/html#
root@ip-172-31-14-104:/var/www/html#
root@ip-172-31-14-104:/var/www/html# |
```

We can see index.html is now showing.

It was downloaded from our S3 bucket directly, using AWS CLI.

9. Verify: Access EC2 Public IP in Browser -> Website should load



We can see now webpage is available.

What We Done:

1. Created EC2 instance, S3 bucket, Created IAM role for EC2 to give full access to S3 bucket.
2. Installed apache in EC2 removed default webpage, uploaded index.html to S3 bucket.
3. Installed AWS CLI in EC2 instance and through AWS CLI Commands we have done sync/download index.html from S3 bucket directly to out EC2 instance and checked it was visible using Public IP.