

AWS: Amazon Web Services Lab Practice Guide

Document has been prepared for lab practice only not for production deployments

Prepared for:
Public

Prepared by:
Ankam Ravi Kumar

Follow Me on Social Networking Sites

[Facebook](#) | [Google Plus](#) | [Twitter](#) | [Reddit](#) | [LinkedIn](#) | [Website](#) | [Blog](#) | [YouTube](#)

Reach me over Email: aravikumar48@gmail.com or aravi@server-computer.com

If you think this document helped a lot [Donate](#) a dollar as complementary

Table of Contents

1. About Author	4
2. Services we provide to our customers	5
3. Cloud Computing Models	6
3.1. Infrastructure as a Service (IaaS):	6
3.2. Platform as a Service (PaaS):	6
3.3. Software as a Service (SaaS):	6
4. Amazon Free Tier Account Creation	7
5. Enabling Multi-Factor Authentication to Secure Your Access	11
6. Creating First Linux Instance	15
7. Create your First EC2 windows instance	20
8. Assigning Elastic IP Addresses to Instance (Static IP Address)	24
9. Launching RDS Instance	25
10. Accessing MySQL Instance Using Workbench	33
11. AWS S3 Bucket	38
11.1. AWS S3 Lifecycle Management	40
11.2. S3 Bucket Replication to Cross-Region	43
11.3. S3 Bucket Policies to control Access	44
12. VPC – Virtual Private Cloud (isolated Network)	45
12.1. Create subnets	48
12.2. Create Internet gateway and attach to VPC	49
12.3. Create Virtual Private Gateway and Attach to VPC	49
12.4. Create route tables and attach to subnets	50
13. AWS Elastic Load Balancer (ELB)	53
14. AWS CloudTrail – Enable Governance and Auditing	57
14.1. How to Create CloudTrail	57

1. About Author

Ankam Ravi Kumar has more than 10+ years of experience in Information Technology Operations and production support streams. He served more than 5 companies in his career and still continuing.

We provide server and data center related services from purchasing of underlying hardware to provisioning the applications.

Solid industry experience in Infrastructure Management/Customer Support/Operations and Training Domains. I love to help people by sharing my knowledge and skills. I always believe “Power is gained by Sharing Knowledge not hoarding it”.

- Operating System Management Such has Linux Different Flavors, Red hat, Fedora, Ubuntu, AIX, Solaris and Windows
- Enterprise Server Management
- Installing and configuring Blade Servers
- Core Storage Management Dell-EMC, IBM and NetApp
- Database Management MSSQL, POSTGRESQL, MariaDB and MySQL
- Process Management ITIL
- Virtualization management RHEV, vSphere, VMware, KVM, Hyper-V and XEN
- Backup and Recovery Management NetVault, Commvault and Symantec Backup Exec
- Application Server Management and Storage Cluster Management
- Data Center Management and Hosting Solutions
- Programming Languages such as PHP and HTML
- Scripting Languages Shell, Perl and Python

Specialized in managing and building the Teams for IT services delivery and Service Support, Training and Operations in both smaller and larger companies. Rich experience and strong exposure in IT Infrastructure & Data Center Management.

Implementation of monitoring solutions for Enterprise, Using Tools Nagios, NagiosXI, Cacti, Solarwinds and LogicMonitor.

2. Services we provide to our customers



Data Storage

Any type of storage categories like DAS, NAS, SAN and Unified. Like Netapp, Dell-EMC, IBM, HP, Hitachi, Pure storage and Synology.



Backup and Recovery

We provide solutions for Online and Offline data backup. RPO and RTO less than ~5Minutes for any disaster recovery.



Networking

Switching and routing. Specialized in Paloalto firewall configurations and VPN. Spam filtering and proxy configurations.



Servers

Starting from server hardware configuration, requirement gathering to installing and configuring. Racking, Operating system and application to production. All brands.



Tape Libraries

We do provide tape library with backup software's. starting from LTO3, LTO4, LTO5, LTO6 and LTO7. Qualstar, Dell, Quantum, HP and IBM.



Telecommunication

Like PRI Lines, SIP, VoIP Services. Software and Hardware solutions for Inband and outband.



Virtualization

Virtualization environment implementation, configurations and migrations. Vmware, Hyper-V and RHEV.



Web Applications

Web application development. web designing and web development.



Application Migrations

We handle a large number of application migrations, data migrations from on-frame to cloud and cloud to on-frame. Any kind of old systems data CIFS shares, User data migrations we will handle with care.

3. Cloud Computing Models

There are three main models for cloud computing. Each model represents a different part of the cloud computing stack.

3.1. Infrastructure as a Service (IaaS):

Infrastructure as a Service, sometimes abbreviated as IaaS, contains the basic building blocks for cloud IT and typically provide access to networking features, computers (virtual or on dedicated hardware), and data storage space. Infrastructure as a Service provides you with the highest level of flexibility and management control over your IT resources and is most similar to existing IT resources that many IT departments and developers are familiar with today.

3.2. Platform as a Service (PaaS):

Platforms as a service remove the need for organizations to manage the underlying infrastructure (usually hardware and operating systems) and allow you to focus on the deployment and management of your applications. This helps you be more efficient as you don't need to worry about resource procurement, capacity planning, software maintenance, patching, or any of the other undifferentiated heavy lifting involved in running your application.

3.3. Software as a Service (SaaS):

Software as a Service provides you with a completed product that is run and managed by the service provider. In most cases, people referring to Software as a Service are referring to end-user applications. With a SaaS offering you do not have to think about how the service is maintained or how the underlying infrastructure is managed; you only need to think about how you will use that particular piece software. A common example of a SaaS application is web-based email where you can send and receive email without having to manage feature additions to the email product or maintaining the servers and operating systems that the email program is running on.

4. Amazon Free Tier Account Creation

Read these conditions before creating a free tier account.

- Amazon Elastic Cloud computer EC2 Linux t2.micro 750Hours per month
- 750 Hours t2.micro windows instance per month
- 2000 Put requests of Amazon S3 (single PUT Request max 5GB)
- 20000 Get requests of Amazon S3 (Each request Get request)
- Amazon RDS MySQL DB instance with t2.micro 5GB storage
- MSSQL Express version t2.micro with 20GB GP-SSD Free tier

<https://aws.amazon.com/free/>

Prerequisites:

- Credit card with minimum 1\$ available balance
- Reachable mobile number for verification

<https://aws.amazon.com/console/>

Click on

Create an AWS Account

Create an AWS account

Email address
aravikumar48@gmail.com

Password
.....

Confirm password
.....

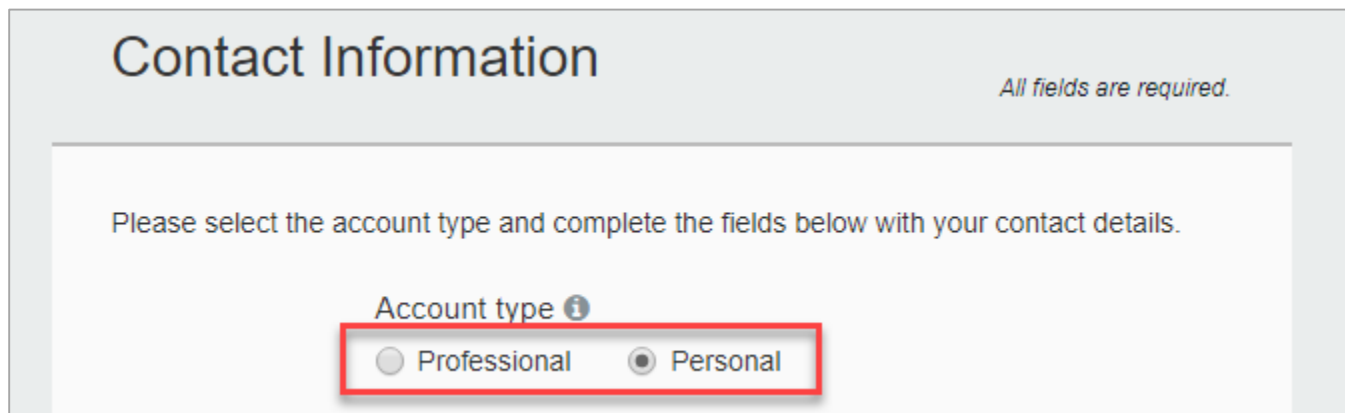
AWS account name ⓘ
Server-Computer

Continue

[Sign in to an existing AWS account](#)

© 2018 Amazon Web Services, Inc. or its affiliates.
All rights reserved.
[Privacy Policy](#) | [Terms of Use](#)

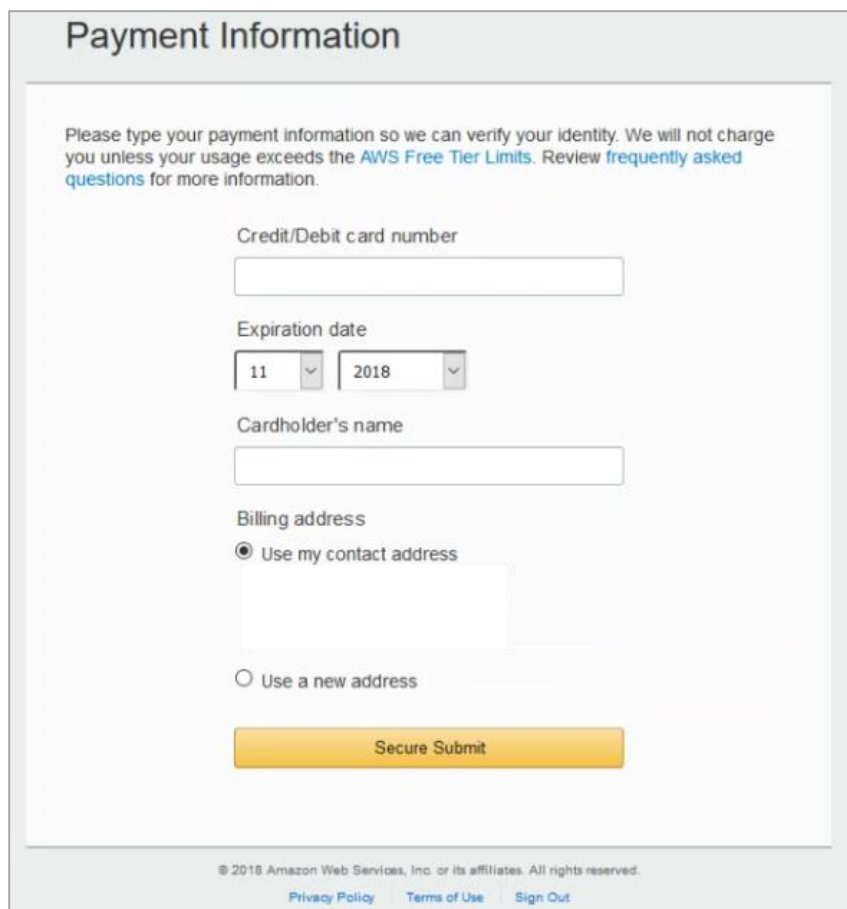
Fill the details example is shown above and **click continue**



The 'Contact Information' form has a title 'Contact Information' and a note 'All fields are required.' Below the title, it says 'Please select the account type and complete the fields below with your contact details.' Under 'Account type', there are two radio buttons: 'Professional' and 'Personal'. The 'Personal' radio button is selected and highlighted with a red rectangle.

Click on radio button

- Professional is for company
- Personal is for single person



The 'Payment Information' form has a title 'Payment Information' and a note: 'Please type your payment information so we can verify your identity. We will not charge you unless your usage exceeds the [AWS Free Tier Limits](#). Review [frequently asked questions](#) for more information.' The form contains several input fields: 'Credit/Debit card number' (a text box), 'Expiration date' (two dropdown menus showing '11' and '2018'), 'Cardholder's name' (a text box), and 'Billing address' (a text box). Below the 'Billing address' field, there are two radio buttons: 'Use my contact address' (which is selected) and 'Use a new address'. At the bottom of the form is a yellow 'Secure Submit' button. The footer of the form includes copyright information: '© 2018 Amazon Web Services, Inc. or its affiliates. All rights reserved.' and links for 'Privacy Policy', 'Terms of Use', and 'Sign Out'.

Provide your credit card details correctly, Card Number, Expiry Date and Card Holder Name

Click on **Secure Submit**

Phone Verification

AWS will call you immediately using an automated system. When prompted, enter the 4-digit number from the AWS website on your phone keypad.

Provide a telephone number




Please enter your information below and click the "Call Me Now" button.

Country/Region code

India (+91)

Phone number Ext

Security Check

Please type the characters as shown above

© 2018 Amazon Web Services, Inc. or its affiliates. All rights reserved.

[Privacy Policy](#) [Terms of Use](#) [Sign Out](#)

It will ask you to enter phone number, Security check then click on **Call Me Now**

Call in progress...

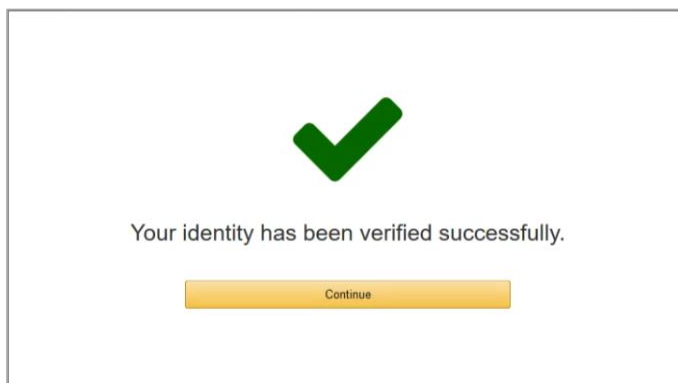
Please answer the call from AWS and, when prompted, enter the 4-digit number on your phone keypad.

2 9 0 2

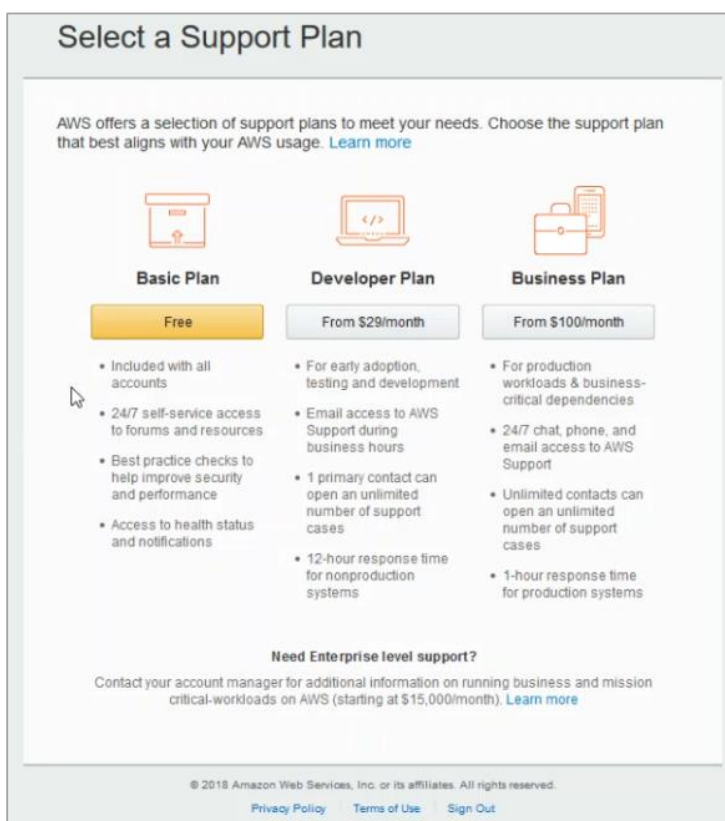
You will receive a call from AWS tele communication and ask you to enter the code displayed on screen.

Note: Listen All the Details carefully and proceed by entering code displayed on screen.

After successful verification



Continue

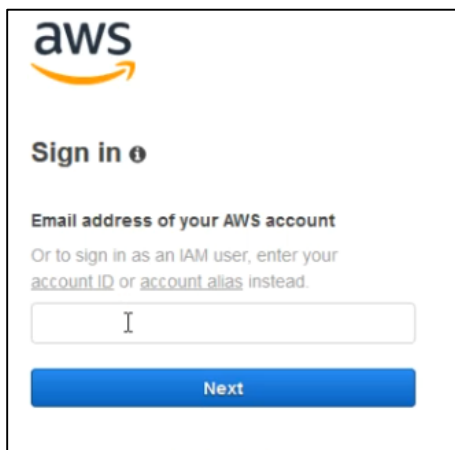


Select Support plan in this case select **Free**



You successfully completed Free Tier Account Creation. Login and Enjoy AWS Free Tier.

AWS Console



The image shows the AWS Sign in page. At the top is the AWS logo. Below it is the text "Sign in" with a help icon. Underneath is the prompt "Email address of your AWS account" followed by a smaller line of text: "Or to sign in as an IAM user, enter your account ID or account alias instead." There is a text input field with a cursor. Below the input field is a blue "Next" button.

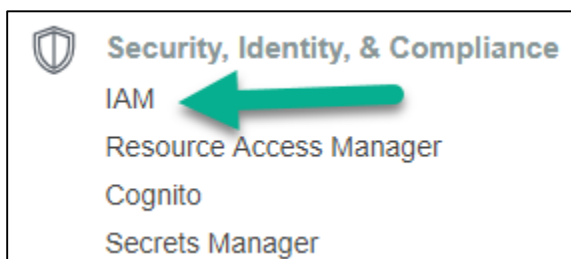


The image shows the AWS Root user sign in page. At the top is the AWS logo. Below it is the text "Root user sign in" with a help icon. Underneath are two input fields: "Email:" and "Password:". To the right of the password field is a link "Forgot password?". Below the input fields is a blue "Sign in" button. At the bottom, there are two links: "Sign in to a different account" and "Create a new AWS account".

Provide your email address and password to **Sign In**

5. Enabling Multi-Factor Authentication to Secure Your Access

Go To IAM Services → Security, Identify & Compliance → IAM



Click on Users → Add User

Add user 1 2 3 4 5

Set user details

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

User name* administrator

[Add another user](#)

Select AWS access type

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

Access type*

- ☐ **Programmatic access**
Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.
- ☒ **AWS Management Console access**
Enables a **password** that allows users to sign-in to the AWS Management Console.

Console password*

- ☐ Autogenerated password
- ☒ Custom password

☐ Show password

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

* Required

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

Provide user name, select access type

- Programmatic Access – Required for automation, run any operation using programs
- AWS Management Console Access – User will have web console access

Click **Next Permissions**

Add user 1 2 3 4 5

▼ **Set permissions**

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

[Create policy](#)

Filter policies Search Showing 375 results

	Policy name	Type	Used as	Description
<input checked="" type="checkbox"/>	AdministratorAccess	Job function	Permissions policy (1)	Provides full access to AWS services and...
<input type="checkbox"/>	AlexaForBusinessD...	AWS managed	None	Provide device setup access to AlexaFor...
<input type="checkbox"/>	AlexaForBusinessF...	AWS managed	None	Grants full access to AlexaForBusiness r...
<input type="checkbox"/>	AlexaForBusinessG...	AWS managed	None	Provide gateway execution access to Ale...
<input type="checkbox"/>	AlexaForBusinessR...	AWS managed	None	Provide read only access to AlexaForBus...
<input type="checkbox"/>	AmazonAPIGatewa...	AWS managed	None	Provides full access to create/edit/delete ...
<input type="checkbox"/>	AmazonAPIGatewa...	AWS managed	None	Provides full access to invoke APIs in Am...
<input type="checkbox"/>	AmazonAPIGatewa...	AWS managed	None	Allows API Gateway to push logs to user'...

► **Set permissions boundary**

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

Click **Next: Tags**

Add tags whatever required to identify user

Add user

12**3**45

[www.server-computer.com](#)

Add tags (optional)

IAM tags are key-value pairs you can add to your user. Tags can include user information, such as an email address, or can be descriptive, such as a job title. You can use the tags to organize, track, or control access for this user. [Learn more](#)

Key	Value (optional)	Remove
Created Date:	25th Oct 2018	×
Description	Administrator for My ABC Client	×
Add new key		

You can add 48 more tags.

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

Click **Next: Review**

Add user

123**4**5

[www.server-computer.com](#)

Review

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

User details

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

Permissions summary

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

Type	Name
Managed policy	AdministratorAccess

Tags

The new user will receive the following tags

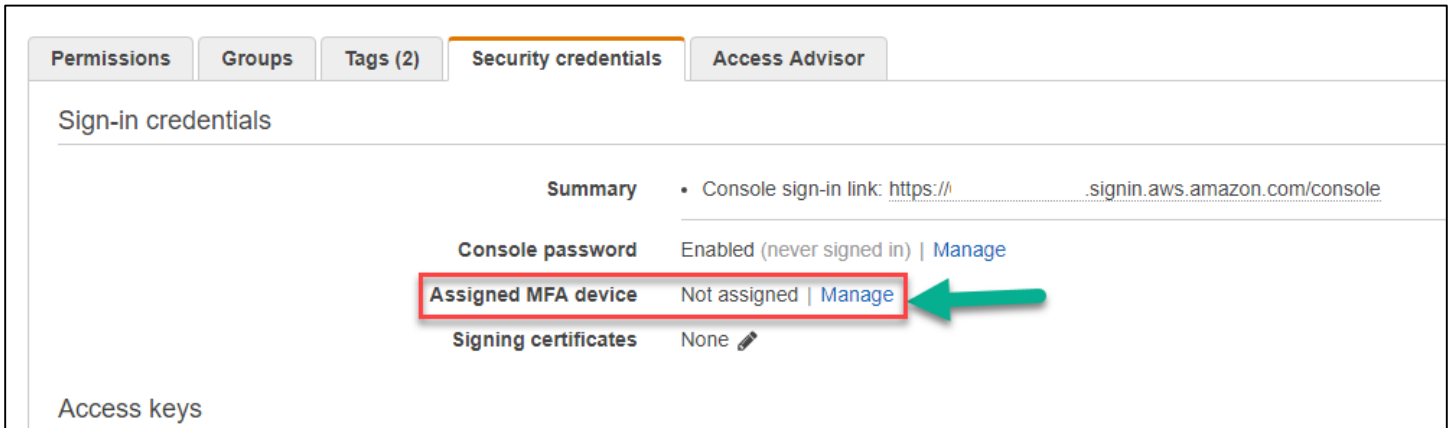
Key	Value
Created Date:	25th Oct 2018
Description	Administrator for My ABC Client

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

Click **Create User**

User creation has been completed successfully now you will get on access URL with your account number. Note the URL.

Now Click on User name → Security credentials (TAB)

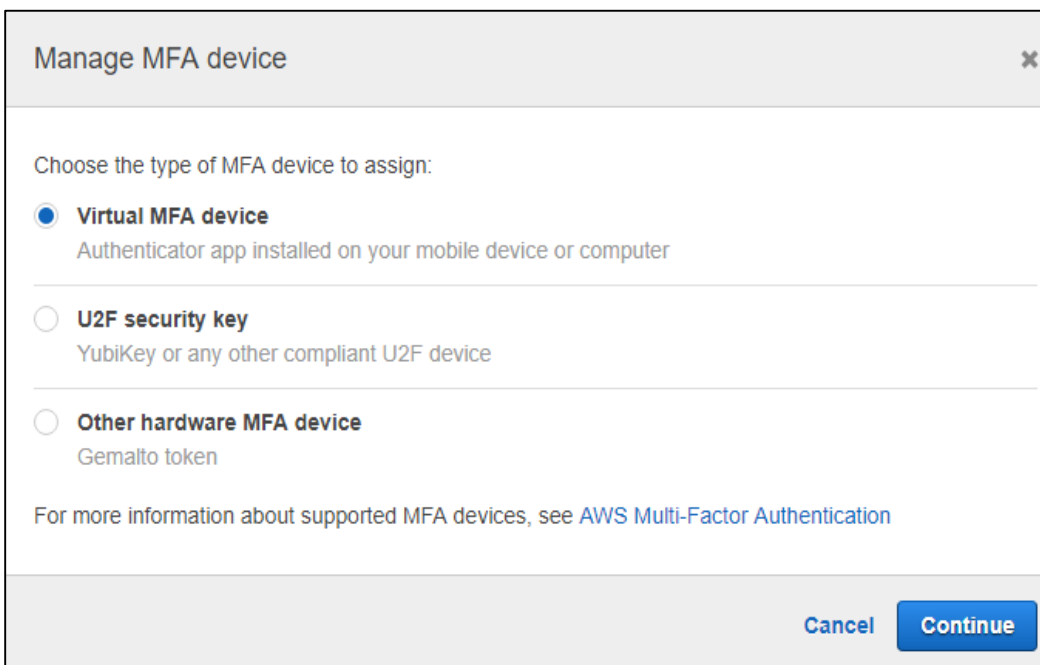


The screenshot shows the 'Security credentials' tab in the AWS IAM console. It displays the 'Sign-in credentials' section with a summary of the user's security settings. The 'Assigned MFA device' row is highlighted with a red box, and a green arrow points to the 'Manage' link next to it.

Sign-in credentials	
Summary	• Console sign-in link: https://...signin.aws.amazon.com/console
Console password	Enabled (never signed in) Manage
Assigned MFA device	Not assigned Manage
Signing certificates	None

Access keys

Click on Assigned MFA Device – Manage



The screenshot shows the 'Manage MFA device' dialog box. It prompts the user to choose the type of MFA device to assign. The 'Virtual MFA device' option is selected, and the 'Continue' button is highlighted.

Manage MFA device

Choose the type of MFA device to assign:

- ☒ **Virtual MFA device**
Authenticator app installed on your mobile device or computer
- ☐ **U2F security key**
YubiKey or any other compliant U2F device
- ☐ **Other hardware MFA device**
Gemalto token

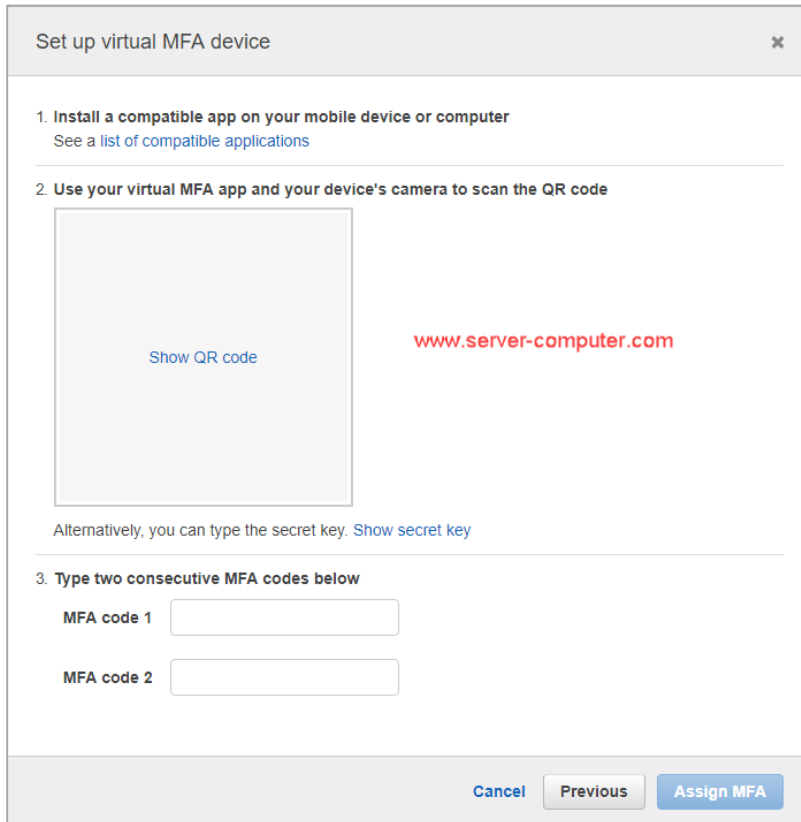
For more information about supported MFA devices, see [AWS Multi-Factor Authentication](#)

[Cancel](#) [Continue](#)

Use any method based on your requirement. Here I am showing Virtual MFA Device method

Install Google Authenticator in your smart phone and ready to pair

Click **Continue**



Set up virtual MFA device

1. Install a compatible app on your mobile device or computer
See a list of compatible applications
2. Use your virtual MFA app and your device's camera to scan the QR code

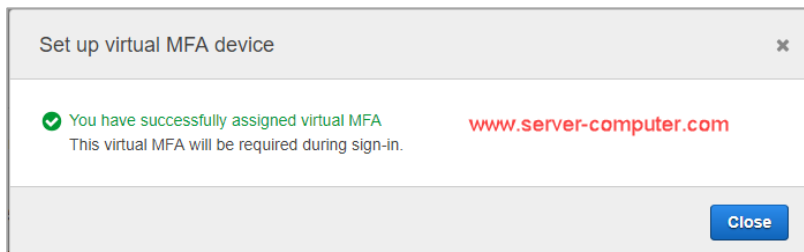
www.server-computer.com

Show QR code

Alternatively, you can type the secret key. [Show secret key](#)
3. Type two consecutive MFA codes below
MFA code 1
MFA code 2

Cancel Previous Assign MFA

Click in **Show QR Code** and scan the same code from your Google authenticator App. It will generate six digit codes enter one code in first MFA code 1 wait 1 minute and second code in MFA Code 2 Click on **Assign MFA**



Set up virtual MFA device

✓ You have successfully assigned virtual MFA
This virtual MFA will be required during sign-in.

www.server-computer.com

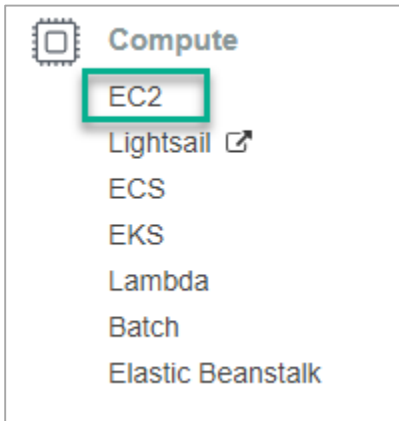
Close

That's it, now you successfully enabled MFA (Multi-Factor Authentication).

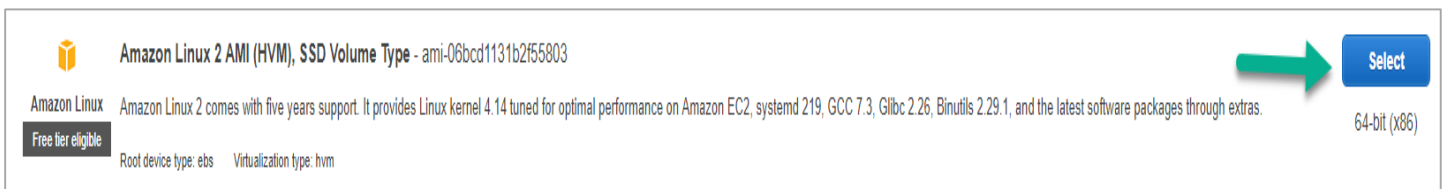
Here after if you want to login, you have to enter credentials and MFA code to Login.

6. Creating First Linux Instance

Login to AWS console, services drop down click on EC2



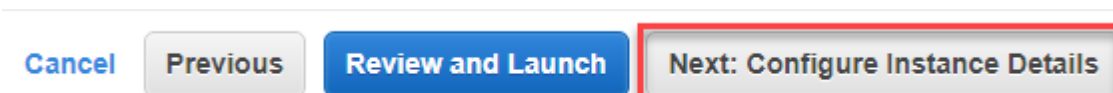
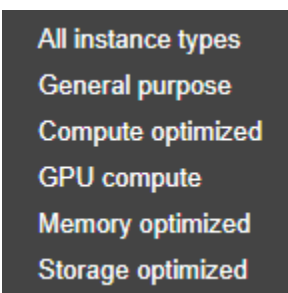
Click on **Launch instance**



I am selecting Free Tier instance Amazon Linux

	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance	IPv6 Support
<input type="checkbox"/>	General purpose	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
<input checked="" type="checkbox"/>	General purpose	t2.micro Free tier eligible	1	1	EBS only	-	Low to Moderate	Yes

We have below types of instances



Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AML, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

Number of instances	1	Launch into Auto Scaling Group
Purchasing option	<input type="checkbox"/> Request Spot instances	
Network	vpc-cbd4f2a3 (default)	Create new VPC
Subnet	No preference (default subnet in any Availability Zone)	Create new subnet
Auto-assign Public IP	Use subnet setting (Enable)	
Placement group	<input type="checkbox"/> Add instance to placement group.	
Capacity Reservation	Open	Create new Capacity Reservation
IAM role	None	Create new IAM role
Shutdown behavior	Stop	
Enable termination protection	<input type="checkbox"/> Protect against accidental termination	
Monitoring	<input type="checkbox"/> Enable CloudWatch detailed monitoring Additional charges apply.	
Tenancy	Shared - Run a shared hardware instance Additional charges will apply for dedicated tenancy.	
T2 Unlimited	<input type="checkbox"/> Enable Additional charges may apply	

[Cancel](#)[Previous](#)[Review and Launch](#)[Next: Add Storage](#)

Step 4: Add Storage

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. [Learn more](#) about storage options in Amazon EC2.

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MB/s)	Delete on Termination	Encrypted
Root	/dev/xvda	snap-00f00b3a3718745e9	8	General Purpose SSD (gp2)	100 / 3000	N/A	<input checked="" type="checkbox"/>	Not Encrypted
Add New Volume								

Add storage – EBS Elastic Block Storage volume will attached to your instance

[Cancel](#)[Previous](#)[Review and Launch](#)[Next: Add Tags](#)

Tags to identify the details about instance (Production/Test/Dev/Client Name)

[Cancel](#)[Previous](#)[Review and Launch](#)[Next: Configure Security Group](#)

Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more](#) about Amazon EC2 security groups.

Assign a security group: ☒ Create a new security group

☐ Select an existing security group

Security group name:

Description:

Type	Protocol	Port Range	Source	Description
SSH	TCP	22	Custom 0.0.0.0/0	e.g. SSH for Admin Desktop

Using security group we can allow/deny any ports

Verify the details and click on Launch

Select an existing key pair or create a new key pair

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. [Learn more](#) about removing existing key pairs from a public AMI.

Create a new key pair

Key pair name



You have to download the **private key file** (*.pem file) before you can continue. **Store it in a secure and accessible location.** You will not be able to download the file again after it's created.

For the first time you create a new key pair and Download Key Pair

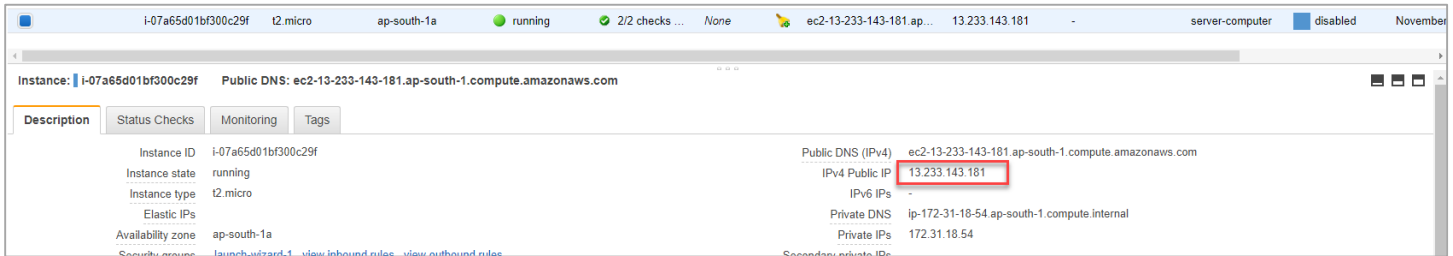
Server-computer.pem file will downloaded, **keep it safe**

Launch Instances

Go to EC2 → See the instances

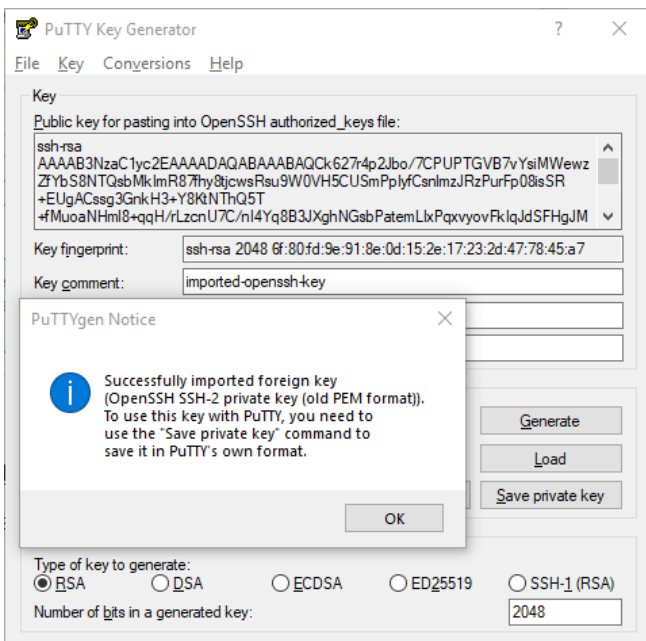
<input type="checkbox"/>	i-07a65d01bf300c29f	t2.micro	ap-south-1a	● running	Initializing	None	ec2-13-233-143-181.ap...	13.233.143.181	-	server-computer	disabled	November
--------------------------	---------------------	----------	-------------	--	--------------	------	--------------------------	----------------	---	-----------------	----------	----------

Click on instance and copy the Public IP Address



Install putty msi installer you will get PuttyGen and Putty for accessing Linux machine

Open puttyGen and load server-computer.pem file

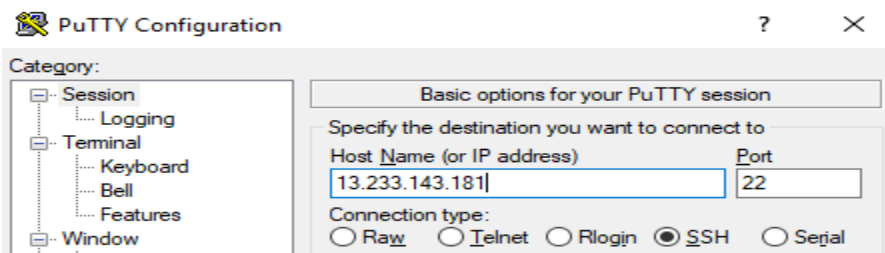


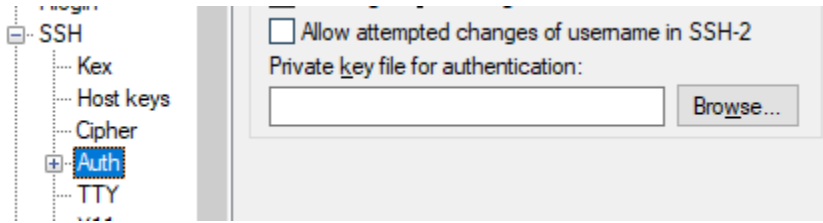
Click Ok.

Save Private Key

In this case, I have used server-computer1.ppk

Open putty application and type IP address as shown below





Expand SSH → Click on Auth → Browse and attach .ppk file

Click on **Open**

```
ec2-user@ip-172-31-18-54:~  
login as: ec2-user  
Authenticating with public key "imported-openssh-key"  
  
  _ |  ( _ | _ )  
  _ |  ( _ | _ ) /   Amazon Linux 2 AMI  
  _ | \ _ | _ |  
  
https://aws.amazon.com/amazon-linux-2/  
[ec2-user@ip-172-31-18-54 ~]$
```

You successfully logged into your Amazon Linux instance

As example, we are going to install web server in Linux server and access using web browser

```
sudo yum update  
sudo yum install httpd  
sudo service httpd start  
sudo service httpd status  
sudo chkconfig httpd on
```

Now go back to your EC2 → Security Groups and Add 80 port



Open browser and type your instance public IP address you can access web-server test page.

7. Create your First EC2 windows instance

Expand services EC2 → Launch Instance

 **Microsoft Windows Server 2016 Base** - ami-0711d827876cdd81a
Windows
Free tier eligible
Microsoft Windows 2016 Datacenter edition. [English]
Root device type: ebs Virtualization type: hvm

Select
64-bit (x86)

Select Windows Image

Choose an Instance Type → General Purpose (t2.micro) → Click **Next: Configure Instance Details** →

Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access ma

Number of instances ⓘ

1

Launch into Auto Scaling Group ⓘ

Purchasing option ⓘ

☐ Request Spot instances

Network ⓘ

vpc-2c747344 (default) ▼

Create new VPC

Subnet ⓘ

subnet-750b241d | Default in us-east-2a ▼

Create new subnet

Auto-assign Public IP ⓘ

Enable ▼

Placement group ⓘ

☐ Add instance to placement group.

Capacity Reservation ⓘ

Open ▼

Create new Capacity Reservation

Domain join directory ⓘ

No directory

Create new directory

IAM role ⓘ

None ▼

Create new IAM role

Select VPC, subnet and enable Public IP address.

Click **Next: Add Storage**

Click **Next: Add Tags**

Add Tags to identify instance details Like Name, Purpose, Account and so and so

Click **Next: Configure Security Group**

Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more](#) about Amazon EC2 security groups.

Assign a security group: ☒ Create a new security group
☐ Select an existing security group

Security group name:

WindowsSecurityGroup

Description:

launch-wizard-1 created 2018-12-05T11:39:15.459+05:30

Type ⓘ	Protocol ⓘ	Port Range ⓘ	Source ⓘ
RDP ▼	TCP	3389	Anywhere ▼ 0.0.0.0/0, ::/0

Add Rule

Click **Review and Launch**

Select an existing key pair or create a new key pair

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance. www.Server-computer.com

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about [removing existing key pairs from a public AMI](#).

Create a new key pair

Key pair name
Server-computer-WindowsKey

Download Key Pair

You have to download the **private key file** (*.pem file) before you can continue. Store it in a **secure and accessible location**. You will not be able to download the file again after it's created.

Cancel Launch Instances

Download Key Pair and Launch Instance

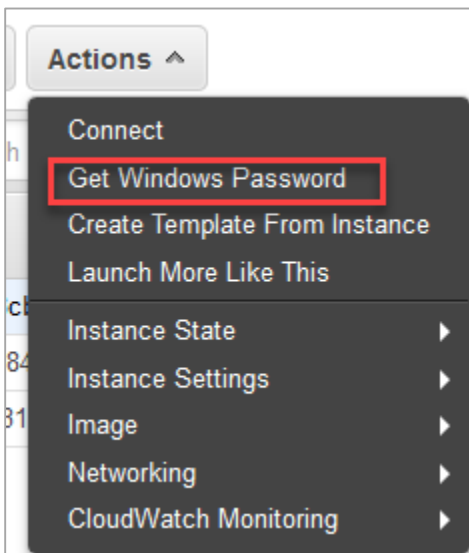
Note: Wait 4 Minutes instance to launch

It should display the following:

- Instance State: running
- Status Checks: 2/2 checks passed

Instance State	Status Checks
● running	✓ 2/2 checks passed

Select instance you have launched → Actions



Retrieve Default Windows Administrator Password

To access this instance remotely (e.g. Remote Desktop Connection), you will need your Windows Administrator password. A default password was created when the instance was launched and is available encrypted in the system log.

To decrypt your password, you will need your key pair for this instance. Browse to your key pair, or copy and paste the contents of your private key file into the text area below, then click Decrypt Password.

The following Key Pair was associated with this instance when it was created.

Key Name Server-computer-WindowsKey

In order to retrieve your password you will need to specify the path of this Key Pair on your local machine:

Key Pair Path Server-computer-WindowsKey.pem

Or you can copy and paste the contents of the Key Pair below:

```
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAjurQSFEoBRrSHhUvr+F0f7fVfALgE8mtzVuq6y0XX0WHgROHwMhz34mRNAdH
...
m4C+pxbyttgKkIipq6ygh/WUKraipKtPXuZ9Ts34b8MxZNYeH/EHjwIDAQABAoIBAGJwGLht+haZ
```

Browse server-computer-WindowsKey.pem file to decrypt and get password

Retrieve Default Windows Administrator Password

Password Decryption Successful

The password for instance i-0b43007700d8cbfe4 was successfully decrypted.

Password change recommended

We recommend that you change your default password. Note: If a default password is changed, it cannot be retrieved through this tool. It's important that you change your password to one that you will remember.

You can connect remotely using this information:

Public DNS `ec2-3-16-76-250.us-east-2.compute.amazonaws.com`

User name Administrator

Password

Now you got password successfully. Click **Close**.

Go to your windows machine Start → Run → mstsc → Ok

Remote Desktop Connection

Remote Desktop Connection

Computer:

User name: None specified

You will be asked for credentials when you connect.

Click **connect** and type user name and password you are connected to your EC2 windows instance.

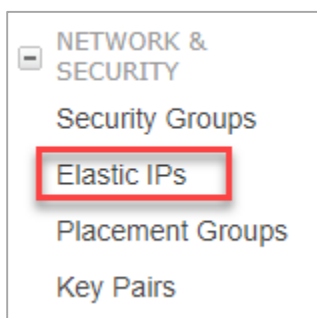
8. Assigning Elastic IP Addresses to Instance (Static IP Address)

Click on instance name and see instance details like Internal and external IP Address, Host name

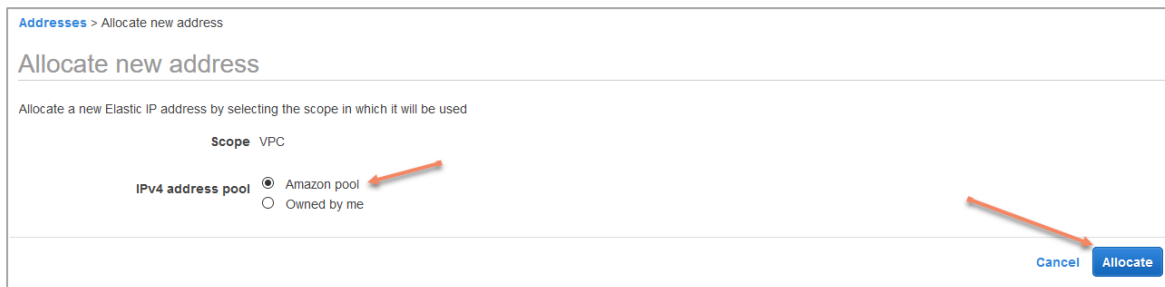
Public DNS (IPv4)	ec2-13-127-65-71.ap-south-1.compute.amazonaws.com
IPv4 Public IP	13.127.65.71
IPv6 IPs	-
Private DNS	ip-172-31-25-150.ap-south-1.compute.internal
Private IPs	172.31.25.150

However, after stop and start of instance assigned public IP address will release to the amazon free pool

If would like to assign an static public address then navigate to Elastic IP's

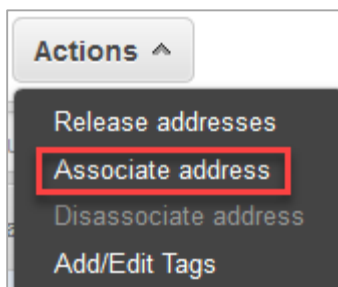


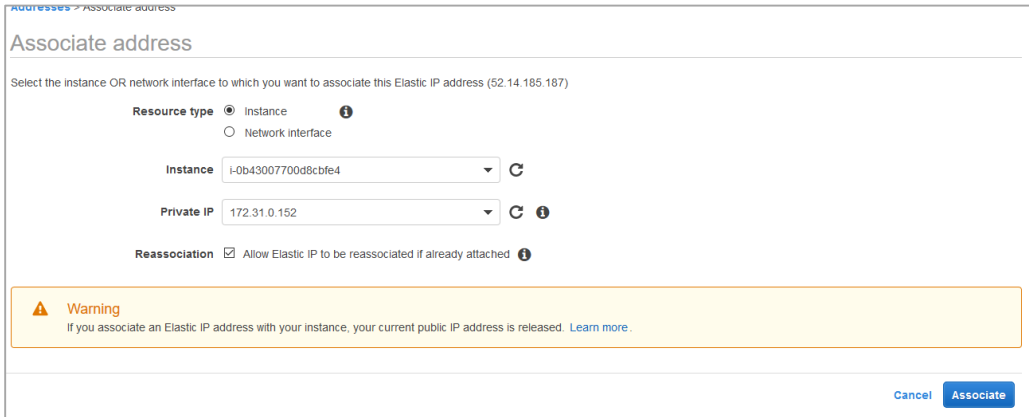
EC2 console right side bar go down → Elastic IPs → Allocate New Address



Click **Allocate**. Amazon allocate you static IP address

Select the IP from Elastic IPs console → Actions → Associate Address





Select Instance ID check Instance ID before allocating. Click **Associate**

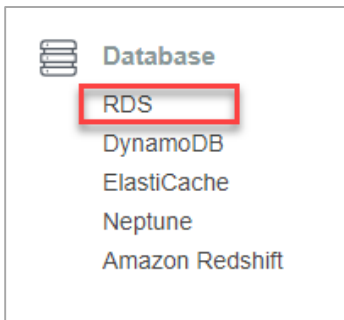
Note: If you have, multiple interfaces to the instance click on Radio button **Network Interface** and select correct NIC card name and Local IP Address.

Now your existing instance has static Public IP address, if you restart your instance also you will get same IP address until you detach from instance.

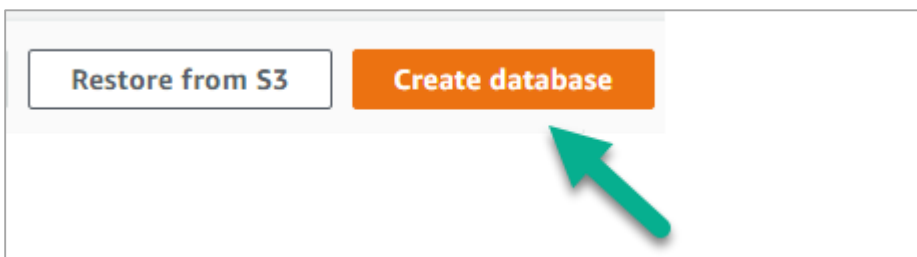
9. Launching RDS Instance

Amazon Relational Database Service (Amazon RDS) is a web service that makes it easier to set up, operate, and scale a relational database in the cloud. It provides cost-efficient, resizable capacity for an industry-standard relational database and manages common database administration tasks.

Login to **AWS Console** and Click on **services** to list all services. Navigate to **Database → RDS**





Now we are going to create a new Database instance with empty database





Amazon will support below 5 types of Relational database engines as managed services


Engine options


☐ Amazon Aurora


☒ MySQL


☐ MariaDB


☐ PostgreSQL


☐ Oracle


☐ Microsoft SQL Server


Select any one of the database engine, which you want to launch and Click **Next**

Note: Careful if you are using free tier account. MSSQL and Oracle are charged.

Choose use case

Use case
Do you plan to use this database for production purposes?
www.server-computer.com

Use case

☐ **Production - Amazon Aurora** Recommended
MySQL-compatible, enterprise-class database at 1/10th the cost of commercial databases.

☐ **Production - MySQL**
Use [Multi-AZ Deployment](#) and [Provisioned IOPS Storage](#) as defaults for high availability and fast, consistent performance.

☒ **Dev/Test - MySQL**
This instance is intended for use outside of production or under the [RDS Free Usage Tier](#).

Billing is based on [RDS pricing](#).

Cancel

Previous

Next

Choose appropriate usage of your instance. In this scenario, I am using Dev/Test instance Click **Next**

Specify DB details

www.server-computer.com

Instance specifications

Estimate your monthly costs for the DB Instance using the [AWS Simple Monthly Calculator](#)

DB engine
MySQL Community Edition

License model [Info](#)
general-public-license

DB engine version [Info](#)
MySQL 5.6.40

Select Version

In drop down, select appropriate and required MySQL Version.

Note: If you select Free Tier. Selected version and options will overwritten free options.

DB instance class [Info](#)
db.r4.xlarge — 4 vCPU, 30.5 GiB RAM

Multi-AZ deployment [Info](#)
☐ Create replica in different zone
Creates a replica in a different Availability Zone (AZ) to provide data redundancy, eliminate I/O freezes, and minimize latency spikes during system backups.
☒ No

Storage type [Info](#)
General Purpose (SSD)

Allocated storage
20 GiB

(Minimum: 20 GiB, Maximum: 32768 GiB) Higher allocated storage may improve IOPS performance.

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

29

30

31

32

33

34

35

36

37

38

39

40

41

42

43

44

45

46

47

48

49

50

51

52

53

54

55

56

57

58

59

60

61

62

63

64

65

66

67

68

69

70

71

72

73

74

75

76

77

78

79

80

81

82

83

84

85

86

87

88

89

90

91

92

93

94

95

96

97

98

99

100

101

102

103

104

105

106

107

108

109

110

111

112

113

114

115

116

117

118

119

120

121

122

123

124

125

126

127

128

129

130

131

132

133

134

135

136

137

138

139

140

141

142

143

144

145

146

147

148

149

150

151

152

153

154

155

156

157

158

159

160

161

162

163

164

165

166

167

168

169

170

171

172

173

174

175

176

177

178

179

180

181

182

183

184

185

186

187

188

189

190

191

192

193

194

195

196

197

198

199

200

201

202

203

204

205

206

207

208

209

210

211

212

213

214

215

216

217

218

219

220

221

222

223

224

225

226

227

228

229

230

231

232

233

234

235

236

237

238

239

240

241

242

243

244

245

246

247

248

249

250

251

252

253

254

255

256

257

258

259

260

261

262

263

264

265

266

267

268

269

270

271

272

273

274

275

276

277

278

279

280

281

282

283

284

285

286

287

288

289

290

291

292

293

294

295

296

297

298

299

300

301

302

303

304

305

306

307

308

309

310

311

312

313

314

315

316

317

318

319

320

321

322

323

324

325

326

327

328

329

330

331

332

333

334

335

336

337

338

339

340

341

342

343

344

345

346

347

348

349

350

351

352

353

354

355

356

357

358

359

360

361

362

363

364

365

366

367

368

369

370

371

372

373

374

375

376

377

378

379

380

381

382

383

384

385

386

387

388

389

390

391

392

393

394

395

396

397

398

399

400

401

402

403

404

405

406

407

408

409

410

411

412

413

414

415

416

417

418

419

420

421

422

423

424

425

426

427

428

429

430

431

432

433

434

435

436

437

438

439

440

441

442

443

444

445

446

447

448

449

450

451

452

453

454

455

456

457

458

459

460

461

462

463

464

465

466

467

468

469

470

471

472

473

474

475

476

477

478

479

480

481

482

483

484

485

486

487

488

489

490

491

492

493

494

495

496

497

498

499

500

501

502

503

504

505

506

507

508

509

510

511

512

513

514

515

516

517

518

519

520

521

522

523

524

525

526

527

528

529

530

531

532

533

534

535

536

537

538

539

540

541

542

543

544

545

546

547

548

549

550

551

552

553

554

555

556

557

558

559

560

561

562

563

564

565

566

567

568

569

570

571

572

573

574

575

576

577

578

579

580

581

582

583

584

585

586

587

588

589

590

591

592

593

594

595

596

597

598

599

600

601

602

603

604

605

606

607

608

609

610

611

612

613

614

615

616

617

618

619

620

621

622

623

624

625

626

627

628

629

630

631

632

633

634

635

636

637

638

639

640

641

642

643

644

645

646

647

648

649

650

651

652

653

654

655

656

657

658

659

660

661

662

663

664

665

666

667

668

669

670

671

672

673

674

675

676

677

678

679

680

681

682

683

684

685

686

687

688

689

690

691

692

693

694

695

696

697

698

699

700

701

702

703

704

705

706

707

708

709

710

711

712

713

714

715

716

717

718

719

720

721

722

723

724

725

726

727

728

729

730

731

732

733

734

735

736

737

738

739

740

741

742

743

744

745

746

747

748

749

750

751

752

753

754

755

756

757

758

759

760

761

762

763

764

765

766

767

768

769

770

771

772

773

774

775

776

777

778

779

780

781

782

783

784

785

786

787

788

789

790

791

792

793

794

795

796

797

798

799

800

801

802

803

804

805

806

807

808

809

810

811

812

813

814

815

816

817

818

819

820

821

822

823

824

825

826

827

828

829

830

831

832

833

834

835

836

837

838

839

840

841

842

843

844

845

846

847

848

849

850

851

852

853

854

855

856

857

858

859

860

861

862

863

864

865

866

867

868

869

870

871

872

873

874

875

876

877

878

879

880

881

882

883

884

885

886

887

888

889

890

891

892

893

894

895

896

897

898

899

900

901

902

903

904

905

906

907

908

909

910

911

912

913

914

915

916

917

918

919

920

921

922

923

924

925

926

927

928

929

930

931

932

933

934

935

936

937

938

939

940

941

942

943

944

945

946

947

948

949

950

951

952

953

954

955

956

957

958

959

960

961

962

963

964

965

966

967

968

969

970

971

972

973

974

975

976

977

978

979

980

981

982

983

984

985

986

987

988

989

990

991

992

993

994

995

996

997

998</

- b. Provisioned IOPS is for most read/write operations
- 4. Size of the storage

Settings

DB instance identifier [Info](#)
Specify a name that is unique for all DB instances owned by your AWS account in the current region.

DB instance identifier is case insensitive, but stored as all lower-case, as in "mydbinstance". Must contain from 1 to 63 alphanumeric characters or hyphens (1 to 15 for SQL Server). First character must be a letter. Cannot end with a hyphen or contain two consecutive hyphens.

Master username [Info](#)
Specify an alphanumeric string that defines the login ID for the master user.

Master Username must start with a letter. Must contain 1 to 16 alphanumeric characters.


Master password [Info](#) **Confirm password** [Info](#)

Master Password must be at least eight characters long, as in "mypassword". Can be any printable ASCII character except "/", "", or "@".

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

Provide

- Instance name should be unique
- Master username anything you can give without special characters
- Provide master password and remember

 **Free tier**

The Amazon RDS Free Tier provides a single db.t2.micro instance as well as up to 20 GiB of storage, allowing new AWS customers to gain hands-on experience with Amazon RDS. Learn more about the RDS Free Tier and the instance restrictions [here](#).

☒ Only enable options eligible for RDS Free Usage Tier [Info](#)

DO NOT FORGOT TO SELECT IF YOU'RE USING FREE TIER OTHERWISE YOU WILL BE CHARGED

Network & Security

Virtual Private Cloud (VPC) [Info](#)

VPC defines the virtual networking environment for this DB instance.

Default VPC (vpc-cbd4f2a3)

Only VPCs with a corresponding DB subnet group are listed.

Subnet group [Info](#)

DB subnet group that defines which subnets and IP ranges the DB instance can use in the VPC you selected.

default

Public accessibility [Info](#)

☒ Yes

EC2 instances and devices outside of the VPC hosting the DB instance will connect to the DB instances. You must also select one or more VPC security groups that specify which EC2 instances and devices can connect to the DB instance.

☐ No

DB instance will not have a public IP address assigned. No EC2 instance or devices outside of the VPC will be able to connect.

Availability zone [Info](#)

ap-south-1a

VPC security groups

Security groups have rules authorizing connections from all the EC2 instances and devices that need to access the DB instance.

☒ Create new VPC security group

☐ Choose existing VPC security groups

Select appropriate VPC and Subnet group (If any)

If you want access database from remote machine put “Public Accessibility” **Yes**

Choose existing VPC security groups if you have already or it will create new security group for this instance access.

Database options

Database name [Info](#)

mydatabase

Note: if no database name is specified then no initial MySQL database will be created on the DB Instance.

Port [Info](#)

TCP/IP port the DB instance will use for application connections.

3306

DB parameter group [Info](#)

default.mysql5.6

Option group [Info](#)

default:mysql-5-6

IAM DB authentication [Info](#)

☐ Enable IAM DB authentication

Manage your database user credentials through AWS IAM users and roles.

☒ Disable


Encryption

Encryption

☒ Enable encryption [Learn more](#)

Select to encrypt the given instance. Master key ids and aliases appear in the list after they have been created using the Key Management Service(KMS) console.

☐ Disable encryption


 The selected engine or DB instance class does not support storage encryption.

Provide database name, default port number is 3306 you can even customize the port number if you want.

Enabling IAM DB Authentication. IAM Users also can access your instance based on IAM policies.

For free tier encryption option is disabled

Backup

 Please note that automated backups are currently supported for InnoDB storage engine only. If you are using MyISAM, refer to detail [here](#). [↗](#)

Backup retention period [Info](#)

Select the number of days that Amazon RDS should retain automatic backups of this DB instance.

7 days ▼

Backup window [Info](#)

☐ Select window

☒ No preference

☒ Copy tags to snapshots

If you want database backups select, the retention max is **35 Days**

If you have particular backup window for database select it otherwise leave it default.

Monitoring

Enhanced monitoring

☐ Enable enhanced monitoring

Enhanced monitoring metrics are useful when you want to see how different processes or threads use the CPU.

☒ Disable enhanced monitoring

Enhanced monitoring will charged

Log exports



Select the log types to publish to Amazon CloudWatch Logs

- ☐ Audit log
- ☐ Error log
- ☐ General log
- ☐ Slow query log

IAM role

The following service-linked role is used for publishing logs to CloudWatch Logs.

RDS Service Linked Role

 Ensure that General, Slow Query, and Audit Logs are turned on. Error logs are enabled by default.
[Learn more](#) 

Maintenance

Auto minor version upgrade [Info](#)

- ☒ **Enable auto minor version upgrade**
Enables automatic upgrades to new minor versions as they are released. The automatic upgrades occur during the maintenance window for the DB instance.
- ☐ Disable auto minor version upgrade

Maintenance window [Info](#)

Select the period in which you want pending modifications or patches applied to the DB instance by Amazon RDS.

- ☐ Select window
- ☒ No preference

Select the options you required

Deletion protection

☐ **Enable deletion protection**
Protects the database from being deleted accidentally. While this option is enabled, you can't delete the database.

Cancel Previous Create database

Enabling database protection, you cannot delete database

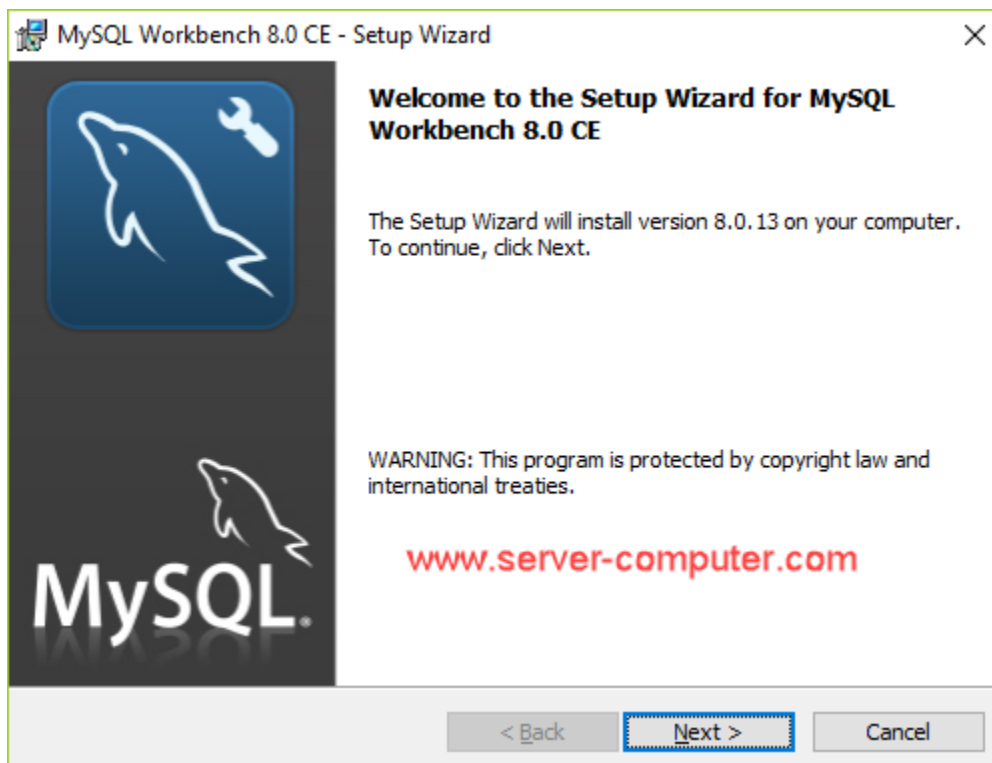
Click **Create Database**

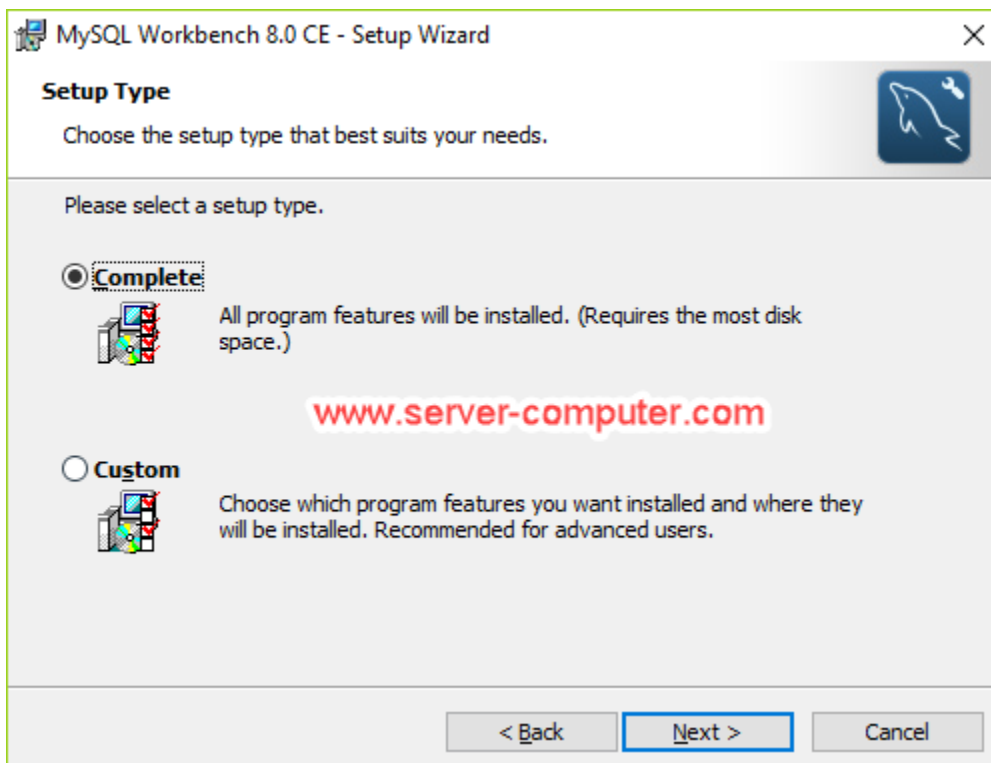
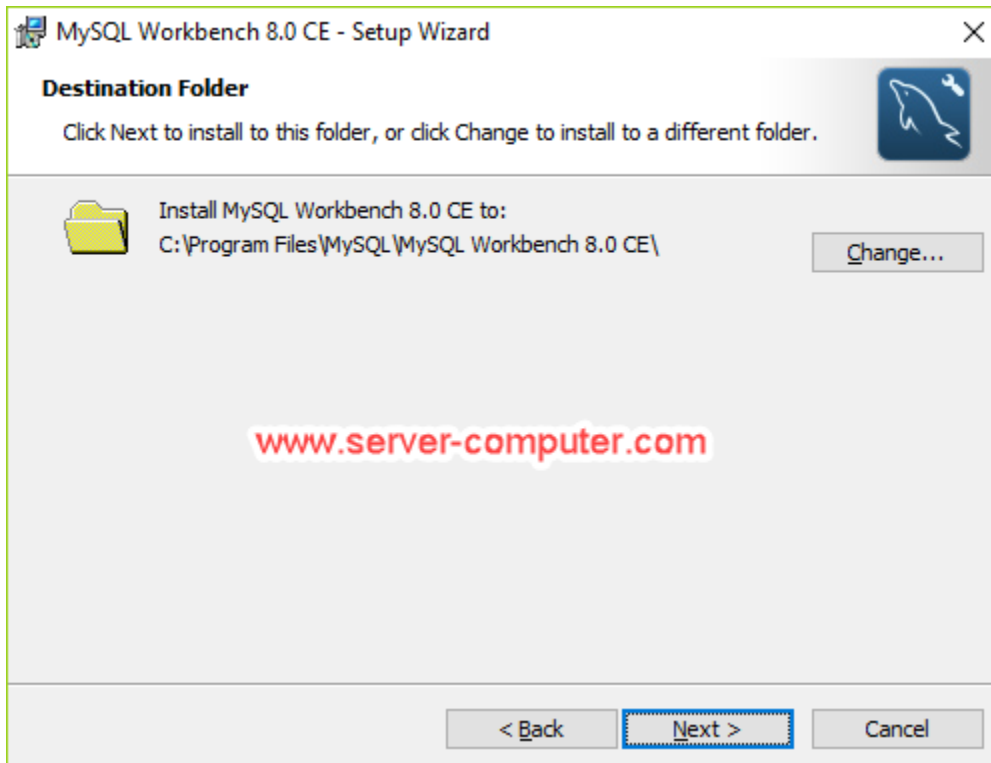
Note: Database instance creation will take at least 10minutes.

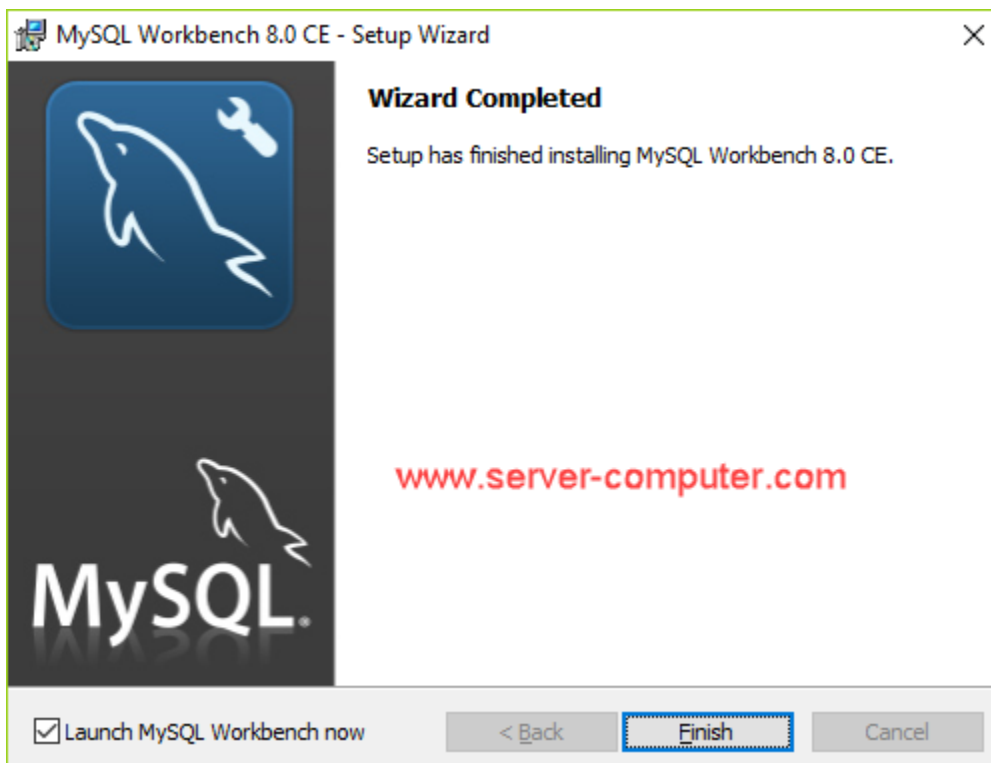
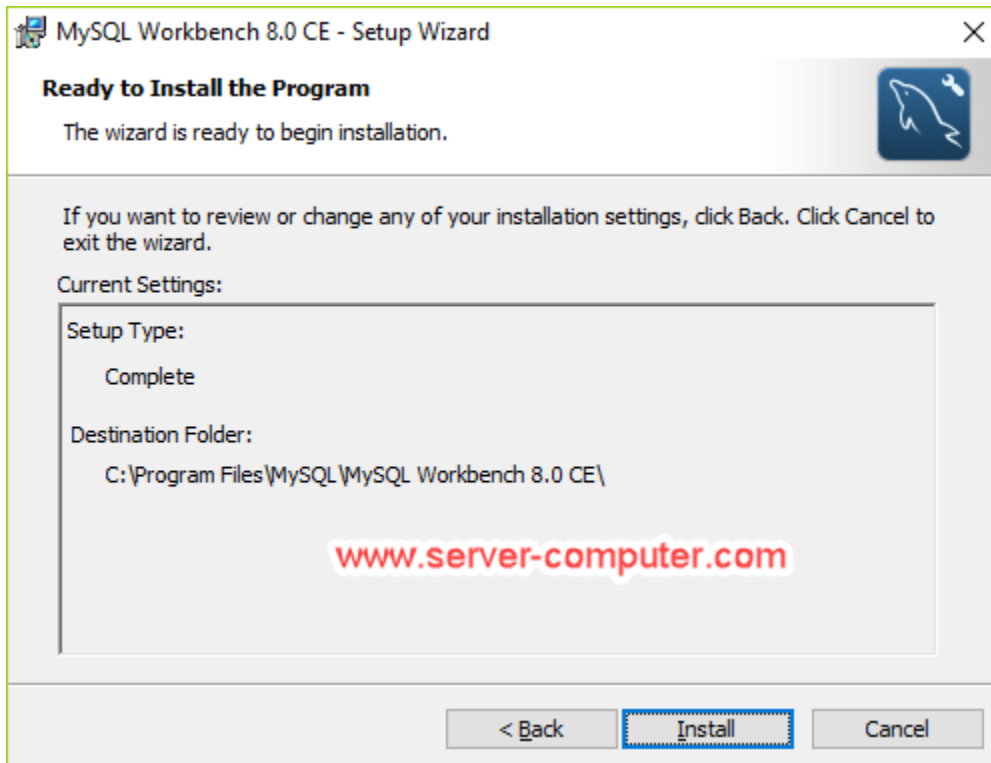
10.Accessing MySQL Instance Using Workbench

Download MySQL Workbench to access MySQL instance remotely

<https://dev.mysql.com/downloads/workbench/>







After successful creation you see like below

DB instance	Engine	Status	CPU	Current activity	Maintenance	Class	VPC	Multi-AZ	Replica
techarkitdatabase	MySQL	available	1.00%	0 Connections	none	db.t2.micro	vpc-cbd4f2a3	No	

Click on Database name and come down copy the **Endpoint URL**

Open your MySQL workbench and create connection



Click on Plus (+) sign to create a New MySQL Connection

Connection Name: Type a name for the connection

Connection Method: Method to use to connect to the RDBMS

Parameters SSL Advanced

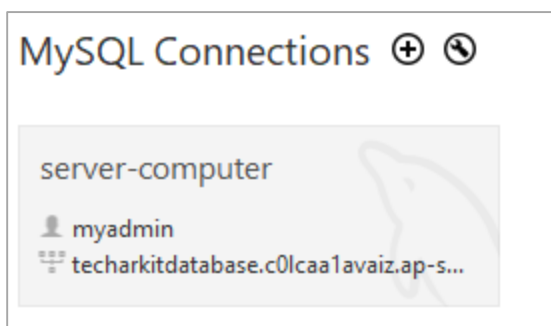
Hostname: Port: Name or IP address of the server host - and TCP/IP port.

Username: Name of the user to connect with.

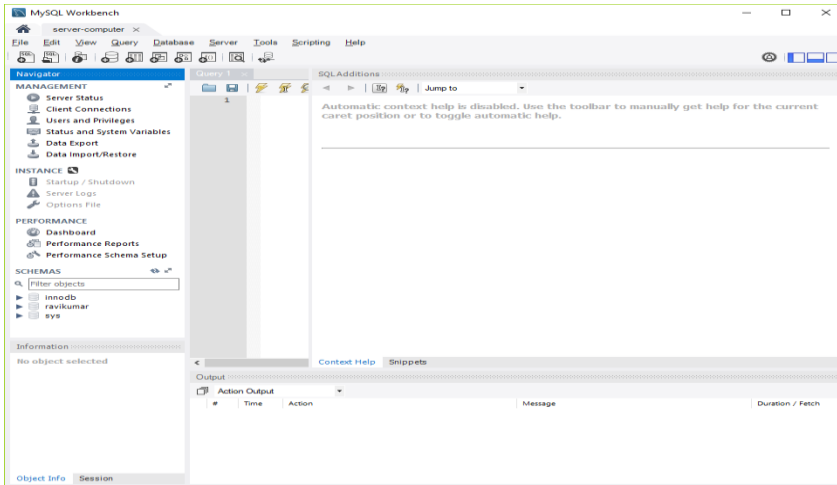
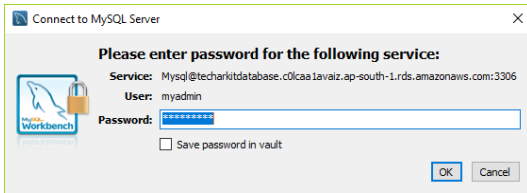
Password: The user's password. Will be requested later if it's not set.

Default Schema: The schema to use as default schema. Leave blank to select it later.

Click **OK**



After successful creation, Click on Connection it will ask you for the password



Successfully launched MySQL RDS Instance and accessed via MySQL Work bench.

Run below queries to create database and some tables on it.

```
create database 'DBNAME';  
use DBNAME;
```

Create Table using below query

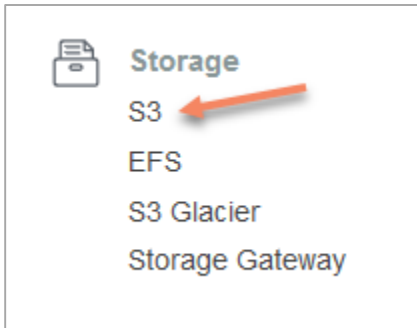
```
create table students(  
    student_id INT NOT NULL AUTO_INCREMENT,  
    student_title VARCHAR(100) NOT NULL,  
    student_author VARCHAR(40) NOT NULL,  
    submission_date DATE,  
    PRIMARY KEY ( student_id )  
);  
show databases;  
use DBNAME;  
show tables;
```

If you know much more database queries like select, insert and delete statement try doing more. Good Luck.

11. AWS S3 Bucket – (Object Storage)

Amazon Simple Storage Service (Amazon S3) is storage for the Internet. You can use Amazon S3 to store and retrieve any amount of data at any time, from anywhere on the web. You can accomplish these tasks using the AWS Management Console, which is a simple and intuitive web interface.

Login to AWS Console and navigate to **Storage → S3**



Click on

A screenshot of the 'Create bucket' wizard in the AWS Management Console. The wizard has four steps: 1. Name and region, 2. Configure options, 3. Set permissions, and 4. Review. The first step is active. It contains a 'Bucket name' field with the value 'server-computer-bucket', a 'Region' dropdown menu set to 'Asia Pacific (Mumbai)', and a 'Copy settings from an existing bucket' dropdown menu set to 'Select bucket (optional)'. At the bottom, there are 'Create', 'Cancel', and 'Next' buttons.

Provide bucket name, it should be a unique name. To Access your S3 bucket over internet it will create DNS entry.

Click **Next**

The screenshot shows the 'Create bucket' wizard in the AWS Management Console, specifically the 'Configure options' step. The progress bar at the top indicates four steps: 1. Name and region (completed), 2. Configure options (current), 3. Set permissions, and 4. Review. The 'Properties' section on the left lists several options: 'Versioning' (Keep all versions), 'Server access logging' (Log requests), 'Tags' (Add another), 'Object-level logging' (Record object-level API activity), 'Default encryption' (Automatically encrypt objects), and 'Advanced settings' (Object lock). The 'Next' button is visible at the bottom right.

- ✚ **Keep All Version of object** means it will not delete any files if you upload same file multiple times. It will keep all the files as multiple versions
- ✚ **Log Requests for access to your bucket** option will log all the actions users did on this particular S3 bucket
- ✚ **Object-level Logging** used to monitor all the object level modifications. Additional cost.
- ✚ **Encryption** You can encrypt S3 bucket data or Encrypt and upload the data either way your data is encrypted.
- ✚ **Object Lock**
- ✚ **Cloudwatch request metrics** for monitoring purpose

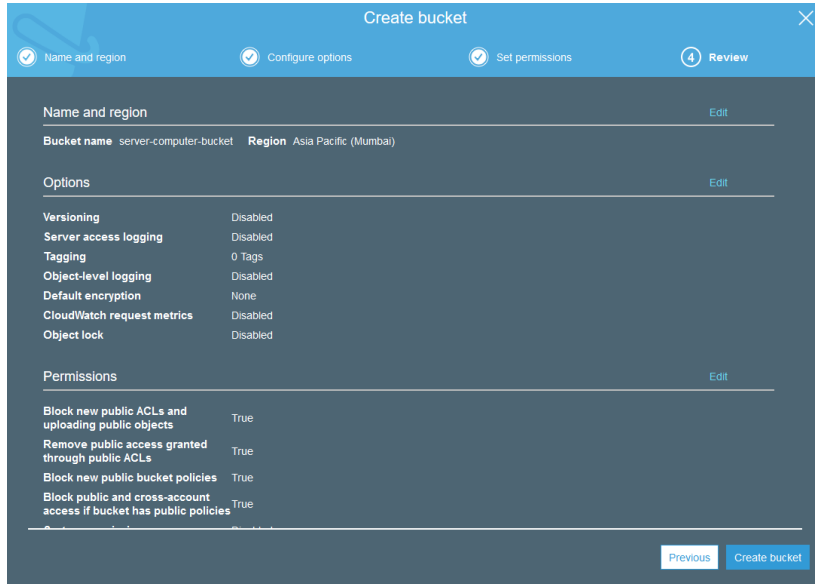
Click **Next**

The screenshot shows the 'Set permissions' step of the 'Create bucket' wizard. A note at the top states: 'Note: You can grant access to specific users after you create the bucket.' The 'Public access settings for this bucket' section includes a warning about public access and two recommended checkboxes: 'Block new public ACLs and uploading public objects' and 'Remove public access granted through public ACLs'. Below this, the 'Manage public bucket policies for this bucket' section has two recommended checkboxes: 'Block new public bucket policies' and 'Block public and cross-account access if bucket has public policies'. The 'Manage system permissions' section has a dropdown menu set to 'Do not grant Amazon S3 Log Delivery group write access to this bucket'. The 'Next' button is highlighted at the bottom right.

AWS recent update is to block public access by default, if you want to enable public access to your S3 bucket un-check all above tick marks.

Still you can provide access to other users on bucket level and object level.

Click **Next**



Final Step is to review selected options and Click **Create bucket**

Your S3 bucket created successfully. Click bucket name you will see all the options

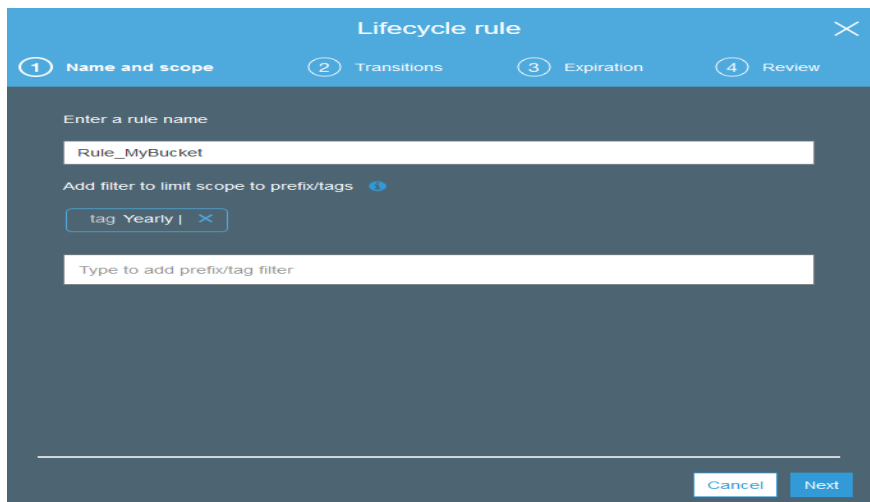
<https://s3.ap-south-1.amazonaws.com/server-computer-bucket>

Above is the example URL to access your S3 bucket over internet

11.1. AWS S3 Lifecycle Management

Click on **S3 Bucket → Management → Lifecycle**

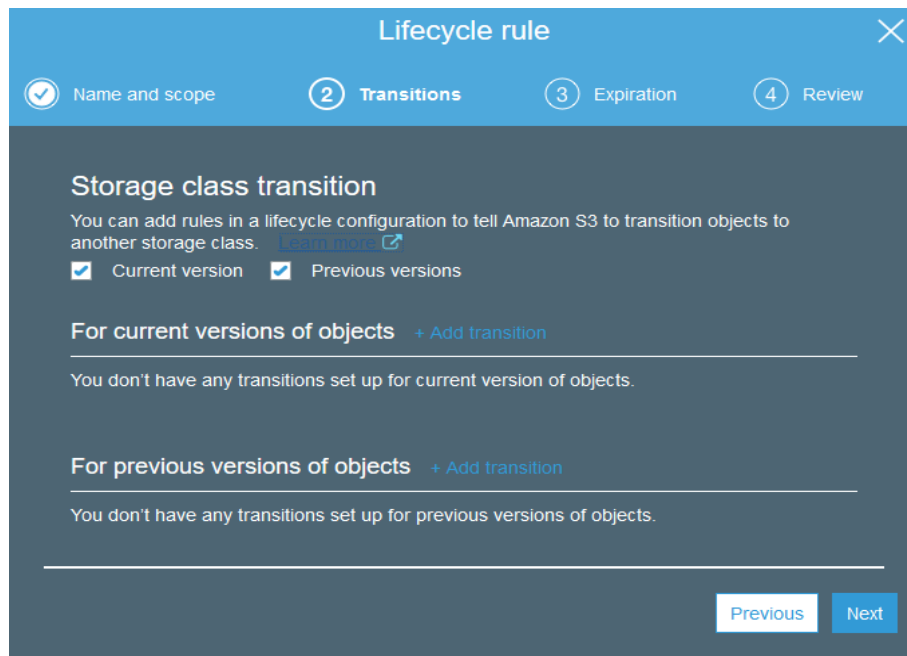
You can manage an objects lifecycle using this feature/rule, which defines



Enter Rule Name

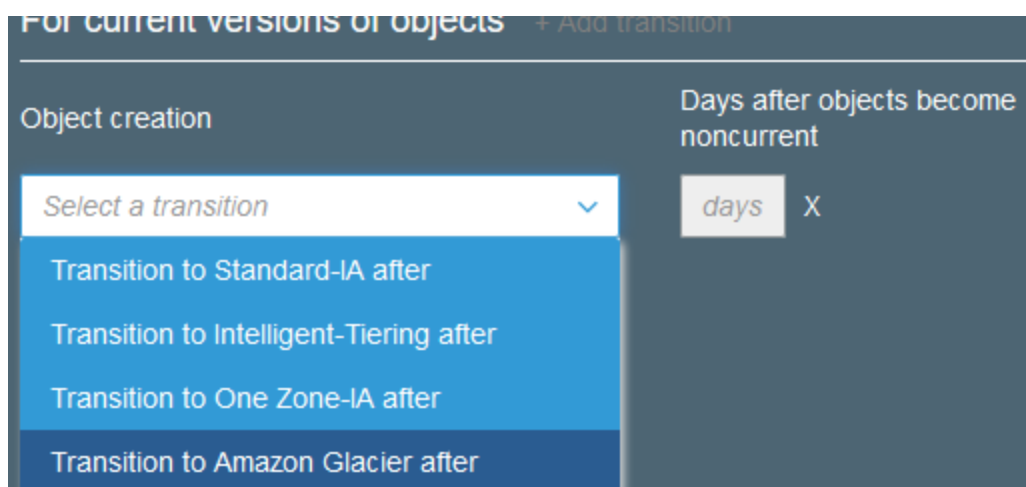
Tag Name if you do not want leave it blank

Click **Next**



- ☒ Current Versions
- ☒ Previous Versions

Based on selected versions action will be performed example if you want to keep current versions in A1 or maybe previous versions on Glacier as per your requirement



Click **Next**

The screenshot shows the 'Lifecycle rule' configuration window with the 'Expiration' step selected. The progress bar at the top indicates the following steps: 1. Name and scope (checked), 2. Transitions (checked), 3. Expiration (active), and 4. Review. The main content area is titled 'Configure expiration' and includes the following options:

- ☐ Current version
- ☒ Previous versions
- ☒ Permanently delete previous versions ⓘ
- After days from becoming a previous version
- Clean up expired object delete markers and incomplete multipart uploads**
- ☒ Clean up expired object delete markers ⓘ
- ☒ Clean up incomplete multipart uploads ⓘ
- After days from start of upload

At the bottom right, there are 'Previous' and 'Next' buttons.

Explanation: Previous versions of files after 365 days means one year permanently delete from S3 bucket.

Clean up expired and incomplete uploads after 2 days.

Click **Next**

The screenshot shows the 'Lifecycle rule' configuration window with the 'Review' step selected. The progress bar at the top indicates the following steps: 1. Name and scope (checked), 2. Transitions (checked), 3. Expiration (checked), and 4. Review (active). The main content area displays a summary of the rule configuration:

- Name and scope** ⓘ
 - Name** Rule_MyBucket
 - Scope** Whole bucket
- Transitions** ⓘ
- Expiration** ⓘ
 - Permanently delete after 365 days
 - Clean up expired object delete markers
 - Clean up incomplete multipart uploads after 2 days

Click **Save**.

11.2. S3 Bucket Replication to Cross-Region

S3 bucket **Name** → **Management** → **Replication**

Note: In order to enable Replication for S3 bucket **Versioning** should be enabled.

The screenshot shows the 'Replication rule' configuration window in the AWS console, specifically the 'Set source' step. The progress bar at the top indicates four steps: 1. Set source (active), 2. Set destination, 3. Configure options, and 4. Review. Under 'Set source', the 'Entire bucket' option is selected for the bucket 'arkit-test123'. The 'Replication criteria' section has a checkbox for 'Replicate objects encrypted with AWS KMS' which is currently unchecked. A blue information box contains a message about the new CRR schema. At the bottom right, there are 'Cancel' and 'Next' buttons.

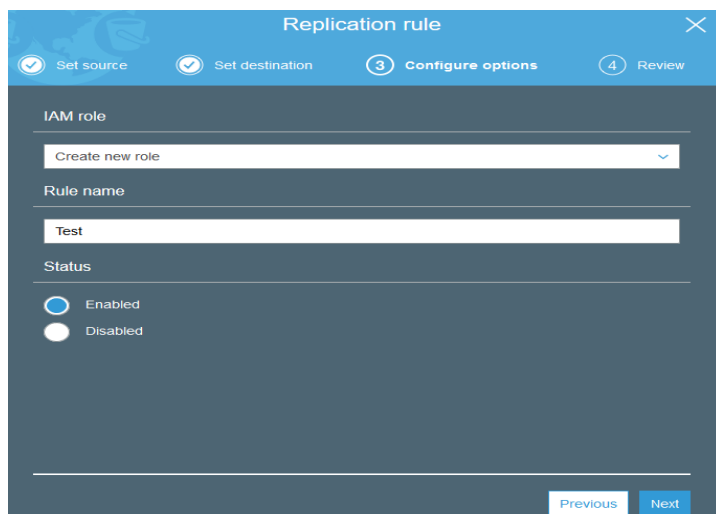
Click **Next**

The screenshot shows the 'Replication rule' configuration window in the AWS console, specifically the 'Set destination' step. The progress bar at the top indicates four steps: 1. Set source, 2. Set destination (active), 3. Configure options, and 4. Review. Under 'Destination bucket', a dropdown menu shows 'destinationserver1'. The 'Options' section has a checked checkbox for 'Change the storage class for the replicated object(s)'. Below this, the 'Storage class' dropdown menu shows 'Glacier'. There is also an unchecked checkbox for 'Change object ownership to destination bucket owner'. At the bottom right, there are 'Previous' and 'Next' buttons.

Select Destination bucket within same account or another account

Options to Change Storage class and permissions in destination

Click **Next**



Select existing IAM Role or Create new for replication. In this case, I am creating new role for replication called Test

Click **Next**

Review final and Click **Save**

11.3. S3 Bucket Policies to control Access

Click on bucket Name → Permissions → bucket policy

<https://awspolicygen.s3.amazonaws.com/policygen.html>

Go to this above URL and generate policy if you do not know how to write a S3 bucket policy

Step 1: Select Policy Type

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

Select Type of Policy S3 Bucket Policy

Step 2: Add Statement(s)

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

Effect ☒ Allow ☐ Deny

Principal Test

Use a comma to separate multiple values.

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

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

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

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

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

[Add Conditions \(Optional\)](#)

Add Statement

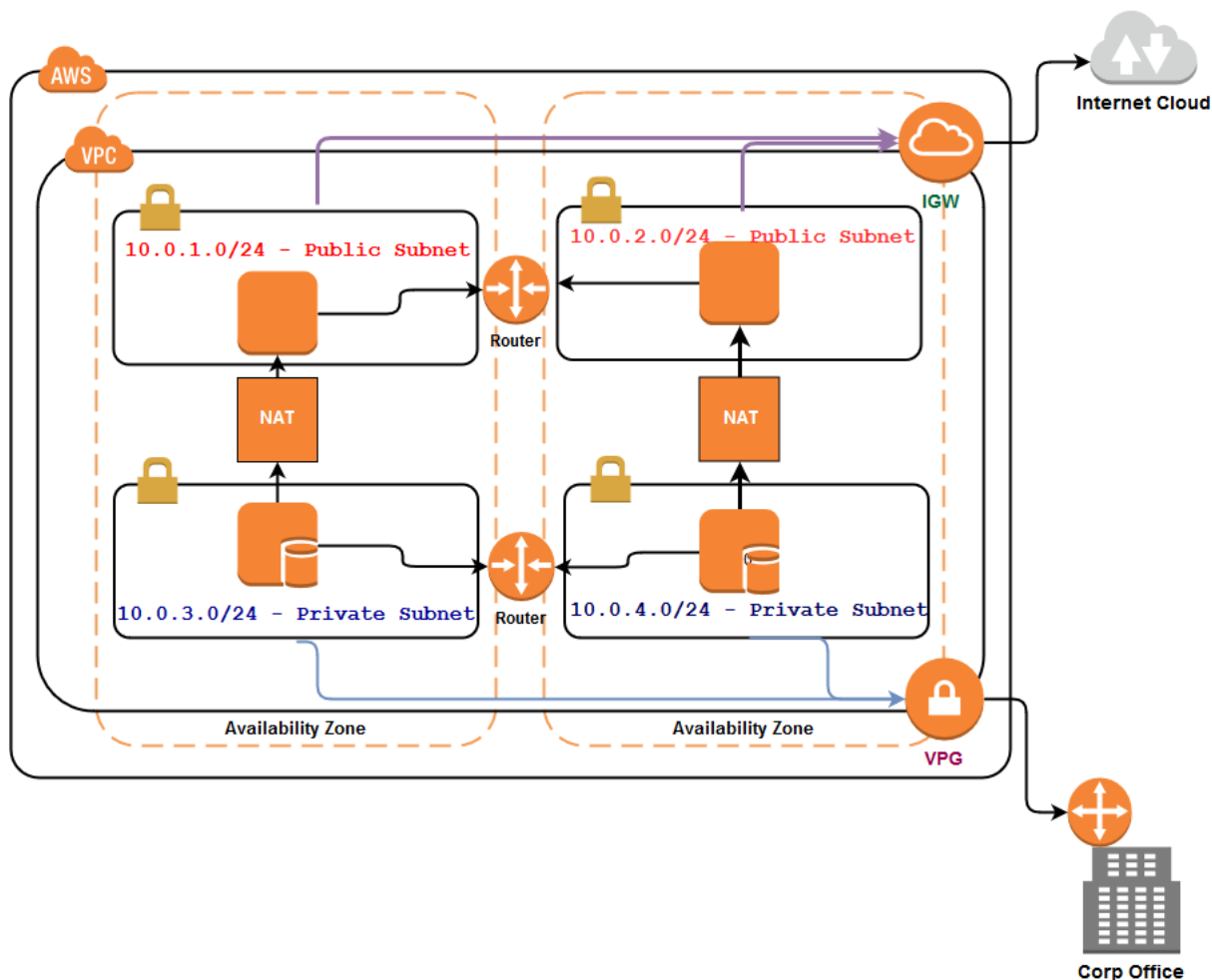
Add Statement and click on **Generate Policy**

```
{
  "Id": "Policy1543401188367",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1543401184049",
      "Action": [
        "s3:ListBucket",
        "s3:ListBucketByTags",
        "s3:ListBucketVersions"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::arkit-prog",
      "Principal": {
        "AWS": [
          "test"
        ]
      }
    }
  ]
}
```








Same policy copy and paste it in policy editor and **save**

12. VPC – Virtual Private Cloud (isolated Network)

A **virtual private cloud** (VPC) is a virtual network dedicated to your AWS account. It is logically isolated from other virtual networks in the AWS Cloud. You can launch your AWS resources, such as Amazon EC2 instances, into your VPC.



Picture: 1.1 Typical VPC Example

-  EC2 Instance
-  Virtual Private Gateway
-  Router
-  Customer Gateway
-  Internet Gateway
-  Availability Zone
-  VPC subnet

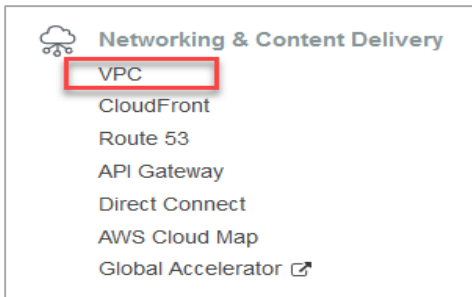
Architecture Explanation:

- AWS in single region
- Two Availability zones
- One Virtual Private Cloud

- Four Subnets Two Are Public and Two Are Private subnets
- Four instances Two App Servers, Two Database Servers
- One Internet Gateway to access internet
- One Virtual Private Gateway to Connect Corporate Office
- Two routers one is connected to private subnets, another is connected to public subnets

We would like to host web application with two web app servers and two Database servers. Two Tier architecture. Web app servers will serve to public, from public facing subnets. Database servers are in private network and only have access to app servers and corporate network (VPG).

When Database servers want to download any kind of files/patches from internet it routes through NAT Gateway and get the internet data from web app servers.



AWS Console → Services → Networking & Content Delivery → VPC → Your VPCs

A screenshot of the 'Create VPC' form in the AWS Console. The form includes fields for 'Name tag' (MyVPC), 'IPv4 CIDR block' (10.0.0.0/16), and 'IPv6 CIDR block' (No IPv6 CIDR Block). The 'Tenancy' is set to 'Default'. There are 'Cancel' and 'Create' buttons at the bottom right.

- **VPC Name:** MyVPC
- **IPv4 CIDR Block:** 10.0.0.0/16 (Use this [CIDR Calculator](#))

Click **Create**

Result	
CIDR Range	10.0.0.0/16
Netmask	255.255.0.0
Wildcard Bits	0.0.255.255
First IP	10.0.0.0
Last IP	10.0.255.255
Total Host	65536
CIDR	10.0.0.0/16

Create VPC

✓ The following VPC was created:

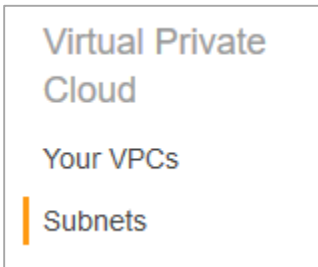
VPC ID vpc-02c316e5f1be2208a

Close

Your VPC created successfully.

12.1. Create subnets

Inside VPC to divide smaller blocks and separation



Subnets > Create subnet

Create subnet

Specify your subnet's IP address block in CIDR format. For example, 10.0.0.0/24. IPv4 block sizes must be between a /16 netmask and /28 netmask, and can be the same size as your VPC. An IPv6 CIDR block must be a /64 CIDR block.

Name tag: S1-Private

VPC: vpc-02c316e5f1be2208a

VPC CIDR	CIDR	Status	Status Reason
	10.0.0.0/16	associated	

Availability Zone: us-east-2a

IPv4 CIDR block: 10.0.1.0/24

* Required

Cancel Create

Create subnet

✓ The following Subnet was created:

Subnet ID subnet-01b0a1e5be742dde0

Close

In Similar way, create all four subnets

Subnet Name	Availability Zone	CIDR Block	Private/Public
S1-Private	Us-east-2a	10.0.1.0/24	Private
S2-Private	Us-east-2b	10.0.2.0/24	Private
S3-Public	Us-east-2a	10.0.3.0/24	Public
S4-Public	Us-east-2b	10.0.4.0/24	Public

<input type="checkbox"/>	Name	Subnet ID	State	VPC	IPv4 CIDR	Available IPv4	IPv6 CIDR	Availability Zone	Availability Zone ID
<input type="checkbox"/>	S1-Private	subnet-01b0a1e5be742dde0	available	vpc-02c316e5f1be2208a MyVPC	10.0.1.0/24	251	-	us-east-2a	use2-az1
<input type="checkbox"/>	S2-Private	subnet-0415e767640ae4ef9	available	vpc-02c316e5f1be2208a MyVPC	10.0.2.0/24	251	-	us-east-2b	use2-az2
<input type="checkbox"/>	S3-Public	subnet-01f8724bb68578a99	available	vpc-02c316e5f1be2208a MyVPC	10.0.3.0/24	251	-	us-east-2a	use2-az1
<input type="checkbox"/>	S4-Public	subnet-09d6c82e020a61325	available	vpc-02c316e5f1be2208a MyVPC	10.0.4.0/24	251	-	us-east-2b	use2-az2

12.2. Create Internet gateway and attach to VPC

Internet Gateways. An internet gateway is a horizontally scaled, redundant, and highly available VPC component that allows communication between instances in your VPC and the internet. It therefore imposes no availability risks or bandwidth constraints on your network traffic.

Attach to S3 and S4, after attach S3 and S4 become public subnets.

The screenshot shows the AWS Management Console interface for creating and attaching an Internet Gateway. The top section, titled 'Create internet gateway', includes a breadcrumb 'Internet gateways > Create internet gateway' and a URL 'www.server-computer.com'. It explains that an internet gateway is a virtual router connecting a VPC to the internet. A 'Name tag' field contains 'My-IGW'. At the bottom are 'Cancel' and 'Create' buttons. The middle section, titled 'Create internet gateway', shows a success message: 'The following internet gateway was created:' with the 'Internet gateway ID' 'igw-0b5da69f9e34ec455' and a 'Close' button. The bottom section, titled 'Actions', shows a dropdown menu with options: 'Delete internet gateway', 'Attach to VPC' (highlighted in orange), 'Detach from VPC', and 'Add/Edit Tags'.

Now attach Internet Gateway to VPC

The screenshot shows the 'Attach to VPC' step in the AWS Management Console. It includes a breadcrumb 'Internet gateways > Attach to VPC' and the URL 'www.server-computer.com'. It instructs the user to attach an internet gateway to a VPC to enable communication with the internet. A 'VPC*' dropdown menu is set to 'vpc-02c316e5f1be2208a'. Below this is an 'AWS Command Line Interface command' section. At the bottom are 'Cancel' and 'Attach' buttons.

Select MyVPC in drop down menu Click **Attach**

12.3. Create Virtual Private Gateway and Attach to VPC

It can be a physical or software appliance. The anchor on the AWS side of the VPN connection is called a virtual private gateway. The following diagram shows your network, the customer gateway, the VPN connection that goes to the virtual private gateway, and the VPC.

Create Virtual Private Gateway

Virtual Private Gateways > Create Virtual Private Gateway

Create Virtual Private Gateway

A virtual private gateway is the router on the Amazon side of the VPN tunnel.

Name tag

ASN ☒ Amazon default ASN ☐ Custom ASN

Cancel Create Virtual Private Gateway

Virtual Private Gateways > Create Virtual Private Gateway

Create Virtual Private Gateway

Create Virtual Private Gateway succeeded

Virtual Private Gateway ID vgw-0649463556a8290fe

Close

Actions

Delete Virtual Private
Attach to VPC
Detach from VPC
Add/Edit Tags

Attach VGW to MyVPC

Attach to VPC

Select the VPC to attach to the virtual private gateway.

Virtual Private Gateway ID vgw-0649463556a8290fe

VPC

Cancel Yes, Attach

12.4. Create route tables and attach to subnets

Route Tables. A route table contains a set of rules, called routes that are used to determine where network traffic is directed. Each subnet in your VPC must be associated with a route table; the table controls the routing for the subnet.

One route for Internet gateway, another for Virtual private gateway (R1-IGW and R2-VGW)

- Route - 0.0.0.0/0 to IGW
- Route - 192.168.0.0/16 to VGW

Create route table

Route Tables > Create route table

Create route table

A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.

Name tag ⓘ

VPC* ↕ ⓘ

* Required

Cancel Create

Route Tables > Create route table

Create route table

✓ The following Route Table was created:

Route Table ID [rtb-08aa6cb351595eac2](#)

Close

Name tag ⓘ

VPC* ↕ ⓘ

Now edit R1-IGW and add routing rule as mentioned below

Route Tables > Edit routes

Edit routes

Destination	Target	Status	Propagated
10.0.0.0/16	local	active	No
<input type="text" value="0.0.0.0/0"/>	<input type="text" value="igw-0b5da69f9e34ec455"/>		No ⓘ

Add route

* Required

Cancel Save routes

Route Tables > Edit routes

Edit routes

Destination	Target	Status	Propagated
10.0.0.0/16	local	active	No
<input type="text" value="192.168.0.0/16"/>	<input type="text" value="vgw-0649463556a8290fe"/>		No ⓘ

Add route

* Required

Cancel Save routes

Attach routing tables to subnets. R1-IGW to S3-Public and S4-Public, public network required to have internet access. Attach R2-VGW to S1-Private and S2-Private (No internet become a private subnets)

<input type="checkbox"/>	Name	Subnet ID	State	VPC
<input checked="" type="checkbox"/>	S1-Private	subnet-01b0a1e5be742dde0	available	vpc-02c316e5f1be2208a ...
<input type="checkbox"/>	S3-Public	subnet-01f8724bb68578a99	available	vpc-02c316e5f1be2208a ...

Subnet: subnet-01b0a1e5be742dde0

Description Flow Logs **Route Table** Network ACL Tags

[Edit route table association](#) www.server-computer.com

Route Table: rtb-0bd197f39222e69ea | R2-VGW

< < 1 to 2 of 2 > >

Destination	Target
192.168.0.0/16	vgw-0649463556a8290fe
10.0.0.0/16	local

<input type="checkbox"/>	Name	Subnet ID	State	VPC
<input checked="" type="checkbox"/>	S4-Public	subnet-09d6c82e020a61325	available	vpc-02c316e5f1be2208a ...

Subnet: subnet-09d6c82e020a61325

Description Flow Logs **Route Table** Network ACL Tags

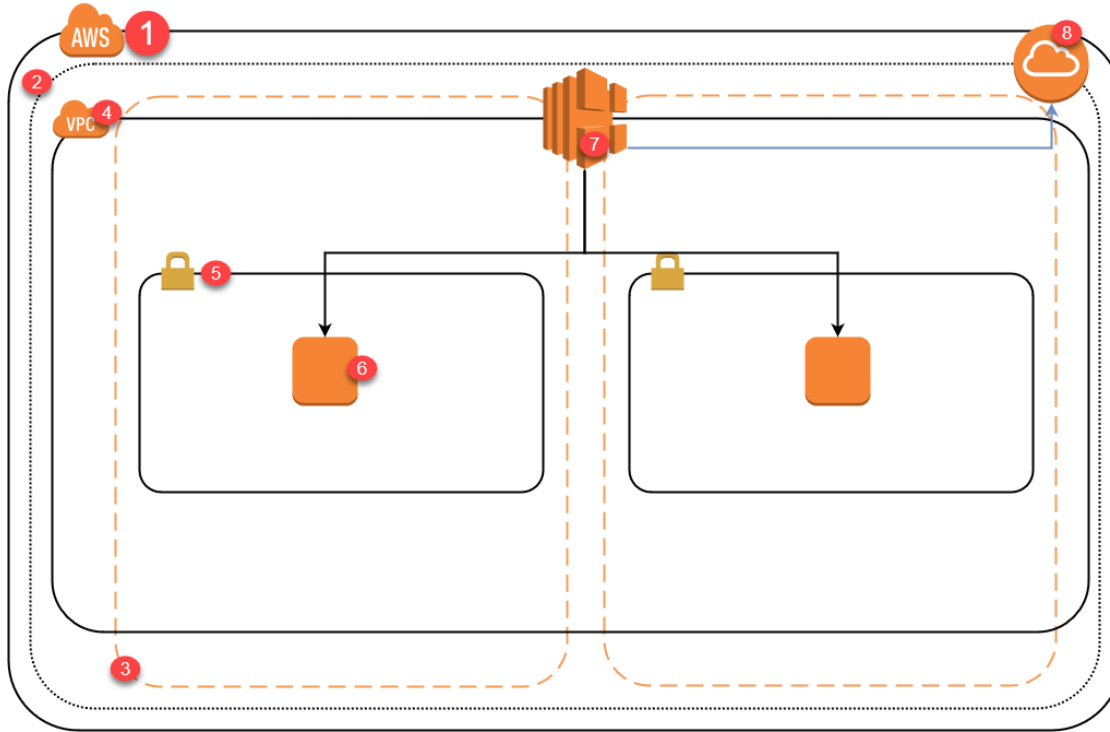
[Edit route table association](#)

Route Table: rtb-08aa6cb351595eac2 | R1-IGW

< < 1 to 2 of 2 > >

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	igw-0b5da69f9e34ec455

13. AWS Elastic Load Balancer (ELB)



2.1 Elastic Load Balancer Typical Architecture

1. AWS Cloud
2. Region
3. Availability Zone
4. VPC – Virtual Private Cloud
5. VPC Subnet
6. EC2 Instance Running Webserver
7. Elastic Load Balancer
8. Internet Gateway

Elastic Load Balancing (ELB) is a load-balancing service for Amazon Web Services (AWS) deployments. ELB automatically distributes incoming application traffic and scales resources to meet traffic demands.

A Managed Load Balancing service

- Distributes load incoming application traffic across multiple targets, such as amazon EC2 instances, containers, and IP Addresses
- Recognizes and responds to unhealthy instances
- Can be public or internal-facing
- Uses HTTP, HTTPS, TCP, and SSL Protocols
- Each Load Balancer is given a public DNS name
 - Internet-facing load balancers have DNS names which publicly resolve to the public IP Addresses of the load balancer of the load balancers nodes

- Internal load balancers have DNS names, which publicly resolve to the private IP Addresses of the load balancers nodes.

Types of ELB

1. Application Load Balancer
2. Network Load Balancer
3. Classic Load Balancer

ELB Practical

- Launch two EC2 instances in different AZs
- Enable Web services
- Launch Load Balancer
- Add both instances under load balancer now check traffic

Follow **EC2 Linux instance launch steps** however in step two (configure Instance) go to down to the bottom in advanced section add below script will create auto webserver

```
#!/bin/bash
sudo yum update -y
sudo yum install httpd* -y
sudo service httpd start
sudo chkconfig httpd on
echo '<html><h1>Hello, Welcome to Server1</h1></html>' > /var/www/html/index.html
sudo service httpd restart
```

▼ Advanced Details

User data ⓘ

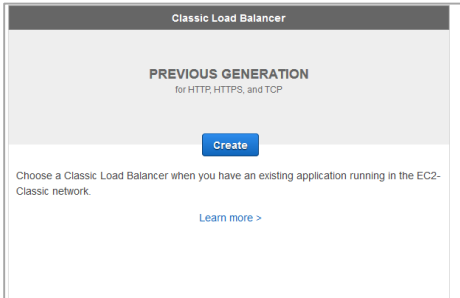
☒ As text ☐ As file ☐ Input is already base64 encoded

```
#!/bin/bash
sudo yum update -y
sudo yum install httpd* -y
sudo service httpd start
sudo chkconfig httpd on
echo '<html><h1>Hello, Welcome to Server1</h1></html>' > /var/www/html/index.html
sudo service httpd restart
```

Note: while launching second instance change echo statement to server2

```
echo '<html><h1>Hello, Welcome to Server2</h1></html>' > /var/www/html/index.html
```

Creating Classic Elastic Load Balancer



Step 1: Define Load Balancer

Basic Configuration

This wizard will walk you through setting up a new load balancer. Begin by giving your new load balancer a unique name so that you can identify it from other load balancers you might create. You will also need to configure ports and protocols for your load balancer. Traffic from your clients can be routed from any load balancer port to any port on your EC2 instances. By default, we've configured your load balancer with a standard web server on port 80.

Load Balancer name:

Create LB inside:

Create an internal load balancer: ☐ (what's this?)

Enable advanced VPC configuration: ☒

Listener Configuration:

Load Balancer Protocol	Load Balancer Port	Instance Protocol	Instance Port
HTTP	80	HTTP	80

Select Subnets

You will need to select a Subnet for each Availability Zone where you wish traffic to be routed by your load balancer. If you have instances in only one Availability Zone, please select at least two Subnets in different Availability Zones to provide higher availability for your load balancer.

VPC vpc-02c316e5f1be2208a (10.0.0.0/16) | MyVPC

Available subnets

Actions	Availability Zone	Subnet ID	Subnet CIDR	Name
	us-east-2a	subnet-01b0a1e5be742dde0	10.0.1.0/24	S1-Private
	us-east-2b	subnet-0415e767640ae4ef9	10.0.2.0/24	S2-Private

Selected subnets

Actions	Availability Zone	Subnet ID	Subnet CIDR	Name
	us-east-2a	subnet-01b724bb68578a99	10.0.3.0/24	S3-Public
	us-east-2b	subnet-09d5c82e020a61325	10.0.4.0/24	S4-Public

[Cancel](#) [Next: Assign Security Groups](#)

Click **Next: Assign Security Groups**

Assign a security group: ☒ Create a new security group
☐ Select an existing security group

Security group name:

Description:

Type	Protocol	Port Range
Custom TCP F	TCP	80

[Add Rule](#)

Click **Next: Security Settings**

Click **Next: Configure Health Checks**

Step 4: Configure Health Check

Your load balancer will automatically perform health checks on your

Ping Protocol

Ping Port

Ping Path

Advanced Details

Response Timeout seconds

Interval seconds

Unhealthy threshold

Healthy threshold

Specify your default web file in this example I am using /index.html

Click **Next: Add EC2 Instances**

Step 5: Add EC2 Instances

The table below lists all your running EC2 Instances. Check the boxes in the Select column to add those instances to this load balancer.

VPC vpc-02c316e5f1be2208a (10.0.0.0/16) | MyVPC

Instance	Name	State	Security groups
<input checked="" type="checkbox"/>	i-0e831d986cac3f5f6	running	WebServer-Loadbalancer
<input checked="" type="checkbox"/>	i-0e02d814b0ce068bd	running	WebServer-Loadbalancer

www.server-computer.com

Availability Zone Distribution

2 instances in us-east-2a

☒ Enable Cross-Zone Load Balancing

☒ Enable Connection Draining seconds

Click **Next: Add Tags**

Click **Review and Create**

Click **Create**

Name	DNS name	State	VPC ID	Availability Zones	Type	Created At
server-computer	server-computer-921437411....		vpc-02c316e5f1be2208a	us-east-2a, us-east-2b	classic	December 5, 2018 at 6:01:1...

Load balancer: server-computer

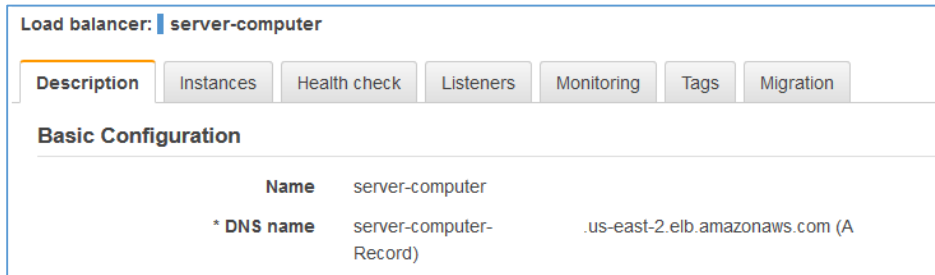
Description Instances Health check Listeners Monitoring Tags Migration

Connection Draining: Enabled, 300 seconds (Edit)

Edit Instances

Instance ID	Name	Availability Zone	Status	Actions
i-0e831d986cac3f5f6		us-east-2a	InService	Remove from Load Balancer

Check instances status should be InService



Load balancer: **server-computer**

Description Instances Health check Listeners Monitoring Tags Migration

Basic Configuration

Name	server-computer		
* DNS name	server-computer-	.us-east-2.elb.amazonaws.com (A	Record)

Load Balancer DNS Name copy it and paste in web browser now fresh twice you will see response is coming from Server1 and Server2



Which concludes load balancer is working fine.

14. AWS CloudTrail – Enable Governance and Auditing

AWS CloudTrail is an AWS service that helps you enable governance, compliance, and operational and risk auditing of your AWS account. Actions taken by a user, role, or an AWS services are recorded as events in CloudTrail. Events include actions taken in the AWS Management Console, AWS Command Line Interface, and AWS SDKs and APIs.

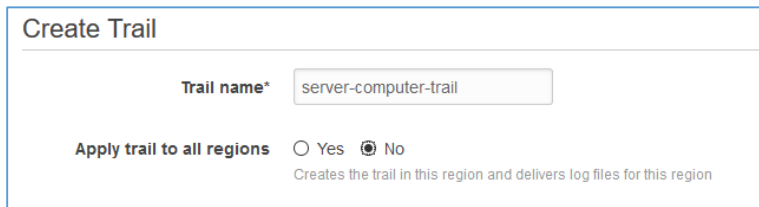
CloudTrail is enabled on your AWS account when you create it. When activity occurs in your AWS account, that activity is recorded in a CloudTrail event. You can easily view recent events in the CloudTrail console by going to Event history.

Visibility into your AWS account activity is a key aspect of security and operational best practices. You can use CloudTrail to view, search, download, archive, analyze, and respond to account activity across your AWS infrastructure. You can identify whom or what took which action, what resources were acted upon, when the event occurred, and other details to help you analyze and respond to activity in your AWS account.

14.1. How to Create CloudTrail

Login to AWS Console → Services → Management & Governance → CloudTrail

Click on **Create Trail**



Create Trail

Trail name*

Apply trail to all regions ☐ Yes ☒ No
Creates the trail in this region and delivers log files for this region

Provide trail name as your wish in this case **server-computer-trail**

Note: If you want to audit all regions by default select “Yes” radio, button otherwise select “No”

Management events

Management events provide insights into the management operations that are performed on

Read/Write events ☒ All ☐ Read-only ☐ Write-only ☐ None ⓘ

S3 **Lambda**

You can record S3 object-level API activity (for example, GetObject and PutObject) for individual buckets, or for all current and future buckets in your AWS account. Additional [charges](#) apply. [Learn more](#) www.server-computer.com

Showing 1 of 1 resources

Bucket name	Prefix	Read	Write
<input type="checkbox"/> Select all S3 buckets in your account ⓘ		<input checked="" type="checkbox"/> Read	<input checked="" type="checkbox"/> Write
arkit-test123	/ CloudTrail	<input checked="" type="checkbox"/> Read	<input checked="" type="checkbox"/> Write ⓘ

Select S3 bucket where you want to store CloudTrail Logs. CloudTrail logs uses S3 bucket for storing audit logs.

If you did not have S3 bucket created, provide bucket name in storage location section by selecting “Yes” radio button, it will create it for you. Select no if you have existing S3 bucket.

Storage location

Create a new S3 bucket ☐ Yes ☒ No

S3 bucket* ⓘ

[Advanced](#)

Click **Create**

Name	Region	Organization trail
server-computer-trail	US East (Ohio)	No

CloudTrail has been created successfully.

15. Athena Analytics

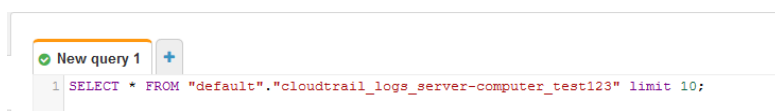
If you would like to create a table in hive using existing logs, you can create by clicking on **Athena table creation**.

```
CREATE EXTERNAL TABLE cloudtrail_logs_server-computer_test123 (  
  eventVersion STRING,  
  userIdentity STRUCT<  
    type: STRING,  
    principalId: STRING,  
    arn: STRING,
```

```
    accountId: STRING,
    invokedBy: STRING,
    accessKeyId: STRING,
    userName: STRING,
    sessionContext: STRUCT<
      attributes: STRUCT<
        mfaAuthenticated: STRING,
        creationDate: STRING>,
      sessionIssuer: STRUCT<
        type: STRING,
        principalId: STRING,
        arn: STRING,
        accountId: STRING,
        userName: STRING>>>,
    eventTime STRING,
    eventSource STRING,
    eventName STRING,
    awsRegion STRING,
    sourceIpAddress STRING,
    userAgent STRING,
    errorCode STRING,
    errorMessage STRING,
    requestParameters STRING,
    responseElements STRING,
    additionalEventData STRING,
    requestId STRING,
    eventId STRING,
    resources ARRAY<STRUCT<
      arn: STRING,
      accountId: STRING,
      type: STRING>>,
    eventType STRING,
    apiVersion STRING,
    readOnly STRING,
    recipientAccountId STRING,
    serviceEventDetails STRING,
    sharedEventID STRING,
    vpcEndpointId STRING
  )
COMMENT 'CloudTrail table for server-computer-test123 bucket'
ROW FORMAT SERDE 'com.amazon.emr.hive.serde.CloudTrailSerde'
STORED AS INPUTFORMAT 'com.amazon.emr.cloudtrail.CloudTrailInputFormat'
OUTPUTFORMAT 'org.apache.hadoop.hive ql.io.HiveIgnoreKeyTextOutputFormat'
LOCATION 's3://server-computer-test123/AWSLogs/687993403879/CloudTrail/'
TBLPROPERTIES ('classification'='cloudtrail');
```

Create table and query using athena interface

Analytics → Athena



You can see the data in tabular format

```
DROP TABLE cloudtrail_logs_server-computer_test123;
```

Delete Athena table using above like query (replace table name).

Otherwise, for RAW log go to your S3 bucket and click on bucket name → **AWSLogs** → **Account Number** → You can see all the CloudTrail logs over there.

Download the json.gz file and analyze the activities

16. AWS Services and abbreviations

- S3 – Simple Storage
- EC2 – Elastic Compute Cloud
- EBS – Elastic Block Storage
- EFS – Elastic File System
- ECS – Elastic Container Service
- EKS – Elastic Container Service for Kubernetes
- RDS – Amazon Relational Database Service

- IAM – Identity, Access Management
- VPC – Virtual Private Cloud (isolated Network)
- ELB – Elastic Load Balancer
- EMR – Elastic MapReduce
- MSK – Managed Streaming for Kafka