

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	5
2. Services we provide to our customers.....	6
3. Cloud Computing Models.....	7
3.1. Infrastructure as a Service (IaaS):	7
3.2. Platform as a Service (PaaS):.....	7
3.3. Software as a Service (SaaS):	7
4. Amazon Free Tier Account Creation	8
5. Enabling Multi-Factor Authentication to Secure Your Access	12
6. Creating First Linux Instance	16
7. Adding New EBS Volume to Linux Instance	22
8. Creating Amazon Machine Image (AMI)	25
9. Create your First EC2 windows instance.....	27
10. Assigning Elastic IP Addresses to Instance (Static IP Address).....	31
11. Amazon Elastic File System	32
12. Launching RDS Instance	34
13. Accessing MySQL Instance Using Workbench	43
14. AWS S3 Bucket – (Object Storage).....	48
14.1. AWS S3 Lifecycle Management.....	50
14.2. S3 Bucket Replication to Cross-Region	53
14.3. S3 Bucket Policies to control Access	54
15. VPC – Virtual Private Cloud (isolated Network).....	55
15.1. Create subnets	58
15.2. Create Internet gateway and attach to VPC	59
15.3. Create Virtual Private Gateway and Attach to VPC	59
15.4. Create route tables and attach to subnets	60
16. AWS Elastic Load Balancer (ELB)	63
17. AWS CloudTrail – Enable Governance and Auditing.....	67
17.1. How to Create CloudTrail.....	67
18. Athena Analytics	68
19. Auto Scaling.....	70
19.1. Launch configuration	70

19.2.	Auto Scaling Groups	71
20.	CloudFormation	74
21.	Amazon FSx	75
22.	SQS – Simple Queue Service	77
23.	SNS – Simple Notification Service	79
24.	Few AWS Articles	85
25.	AWS Services and abbreviations	85

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
.....

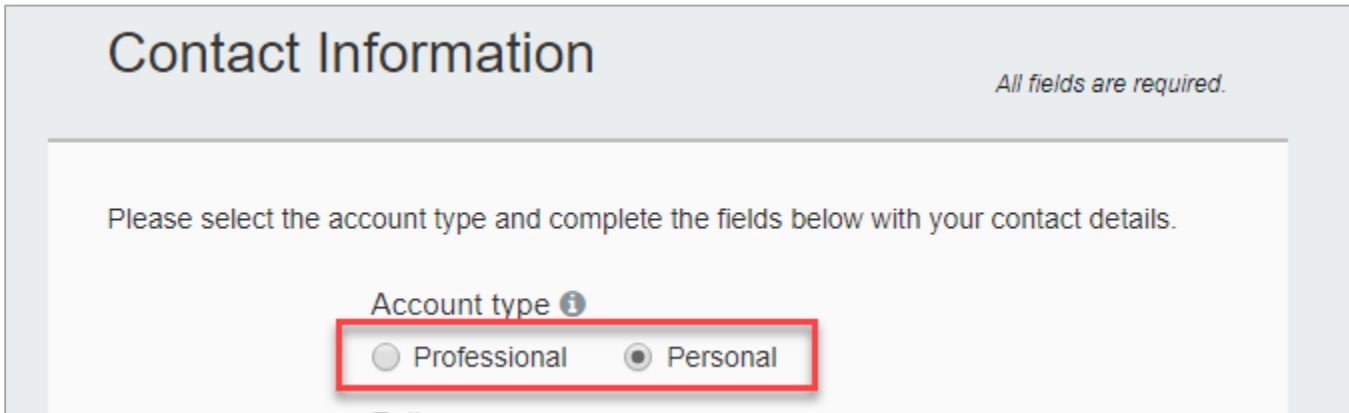
AWS account name ⓘ
Server-Computer

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**



Contact Information *All fields are required.*

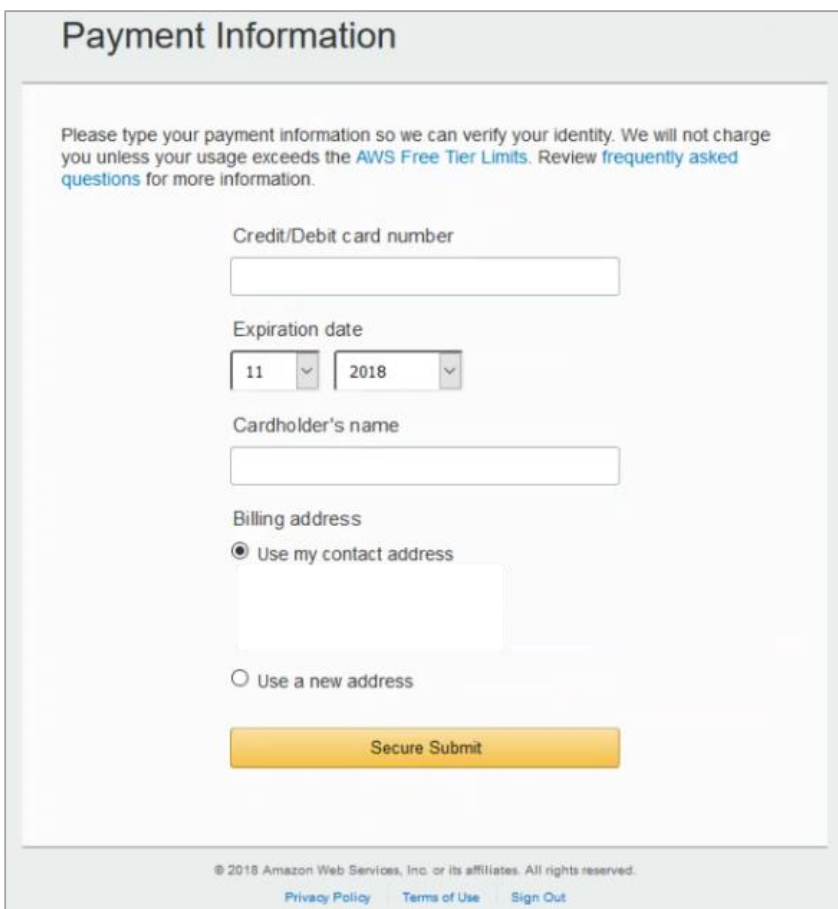
Please select the account type and complete the fields below with your contact details.

Account type ⓘ

☐ Professional ☒ Personal

Click on radio button

- Professional is for company
- Personal is for single person



Payment Information

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.

Credit/Debit card number

Expiration date

11 2018

Cardholder's name

Billing address

☒ Use my contact address

☐ Use a new address

Secure Submit

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

[Privacy Policy](#) [Terms of Use](#) [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...

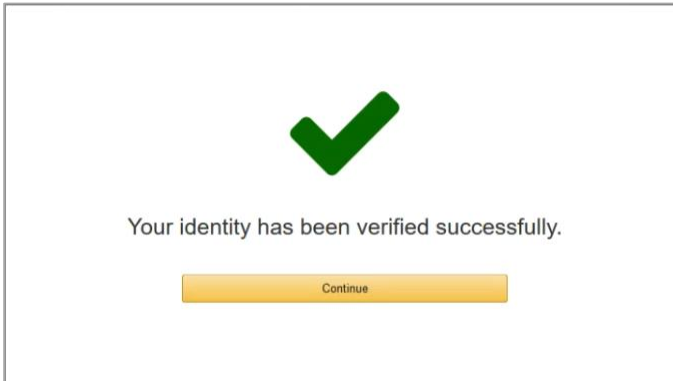
Please answer the call from AWS and, when prompted, enter the 4-digit number on your phone keypad.

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 a Support Plan

AWS offers a selection of support plans to meet your needs. Choose the support plan that best aligns with your AWS usage. [Learn more](#)

Basic Plan	Developer Plan	Business Plan
Free	From \$29/month	From \$100/month
• Included with all accounts • 24/7 self-service access to forums and resources • Best practice checks to help improve security and performance • Access to health status and notifications	• For early adoption, testing and development • Email access to AWS Support during business hours • 1 primary contact can open an unlimited number of support cases • 12-hour response time for nonproduction systems	• For production workloads & business-critical dependencies • 24/7 chat, phone, and email access to AWS Support • Unlimited contacts can open an unlimited number of support cases • 1-hour response time for production systems

Need Enterprise level support?
Contact your account manager for additional information on running business and mission critical-workloads on AWS (starting at \$15,000/month). [Learn more](#)

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

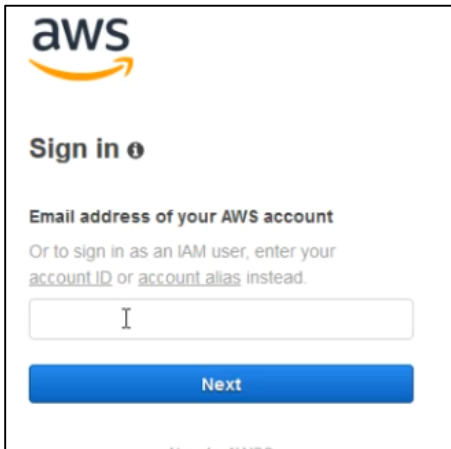
Select Support plan in this case select **Free**

Welcome to Amazon Web Services

Thank you for creating an Amazon Web Services Account. We are activating your account, which should only take a few minutes. You will receive an email when this is complete.

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. The main heading is "Email address of your AWS account". Below this is a subtext: "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.

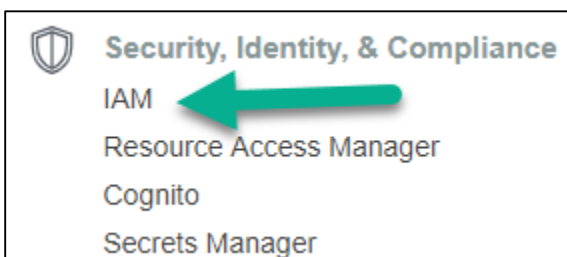


The image shows the AWS Root user sign in page. At the top is the AWS logo. Below it is the text "Root user sign in" with a help icon. The main heading is "Email:". Below this is a text input field. Below the email field is the text "Password" and a link "Forgot password?". There is a password input field. Below the password field 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](#) [Refresh](#)

Filter policies **Showing 375 results**

	Policy name	Type	Used as	Description
☒	AdministratorAccess	Job function	Permissions policy (1)	Provides full access to AWS services and...
☐	AlexaForBusinessD...	AWS managed	None	Provide device setup access to AlexaFor...
☐	AlexaForBusinessF...	AWS managed	None	Grants full access to AlexaForBusiness r...
☐	AlexaForBusinessG...	AWS managed	None	Provide gateway execution access to Ale...
☐	AlexaForBusinessR...	AWS managed	None	Provide read only access to AlexaForBus...
☐	AmazonAPIGatewa...	AWS managed	None	Provides full access to create/edit/delete ...
☐	AmazonAPIGatewa...	AWS managed	None	Provides full access to invoke APIs in Am...
☐	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

12345

[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

12345

[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

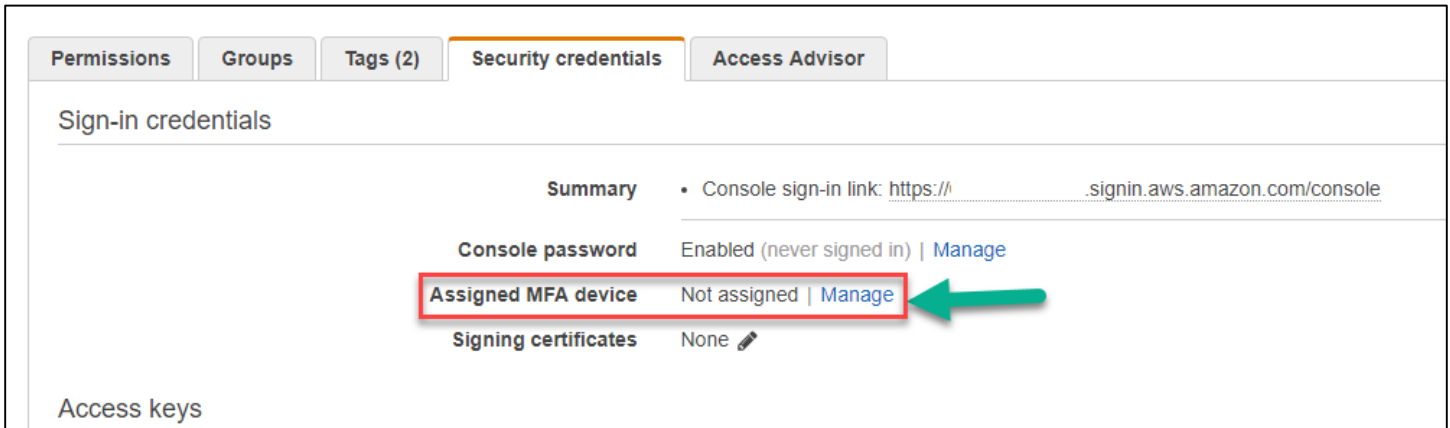
Key	Value
Created Date:	25th Oct 2018
Description	Administrator for My ABC Client

[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)

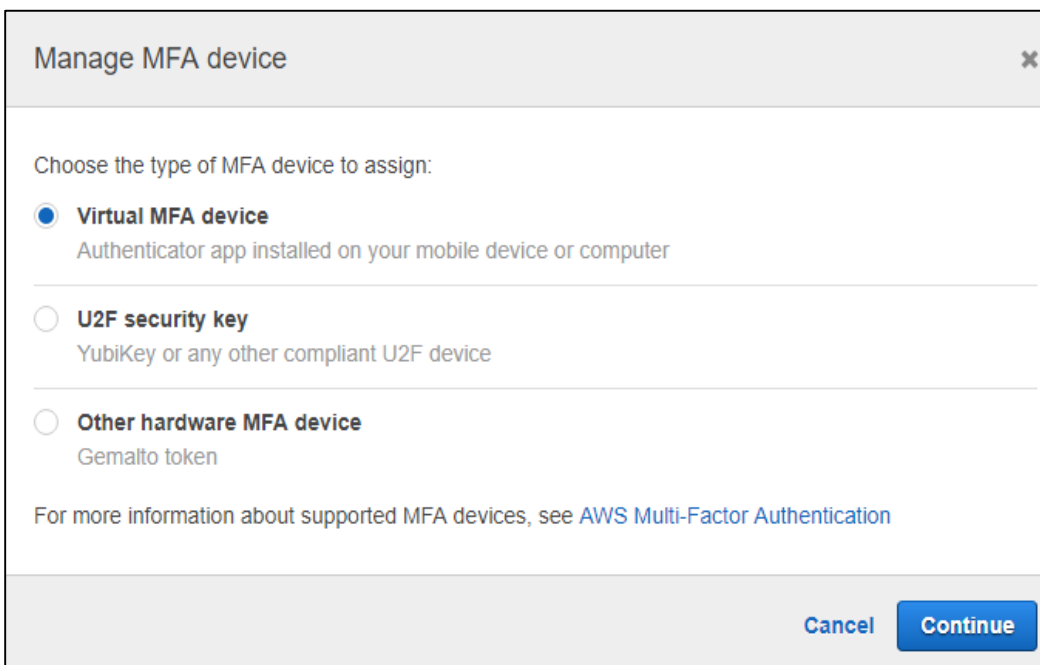


The screenshot shows the 'Security credentials' tab in the AWS IAM console. It displays the 'Sign-in credentials' section with a summary of the user's security settings. The 'Assigned MFA device' row is highlighted with a red box, and a green arrow points to the 'Manage' link next to it.

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

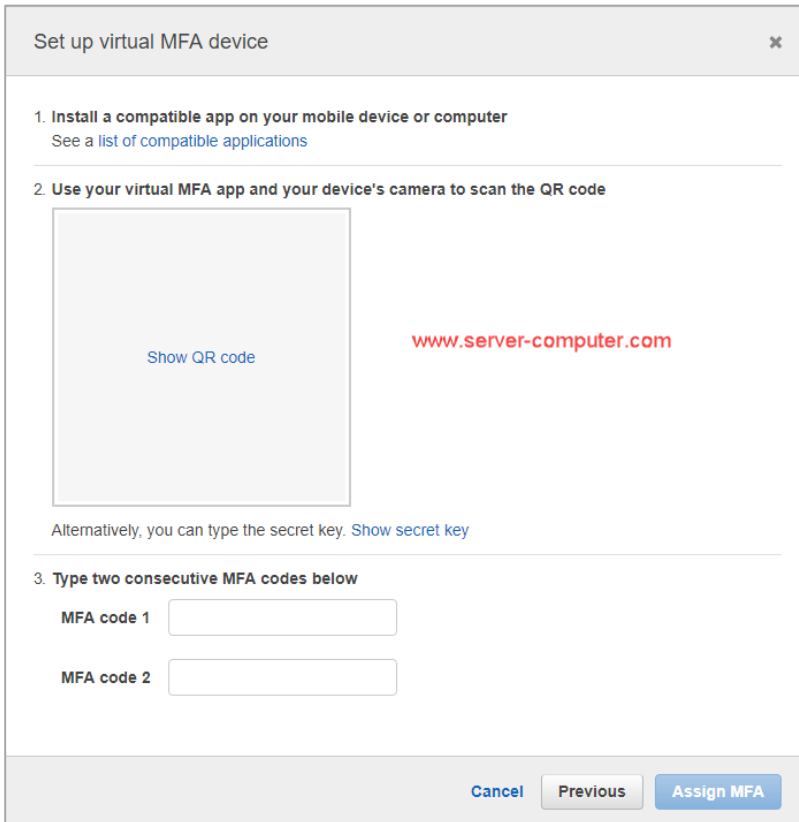
For more information about supported MFA devices, see [AWS Multi-Factor Authentication](#)

[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

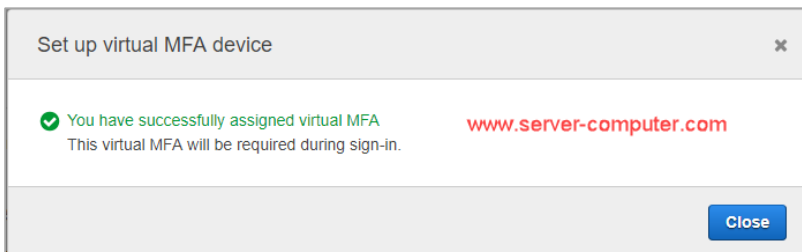
www.server-computer.com

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

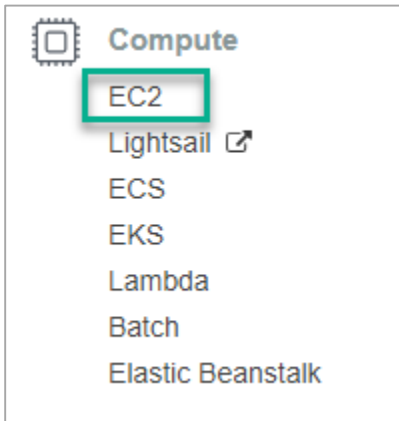
Close

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

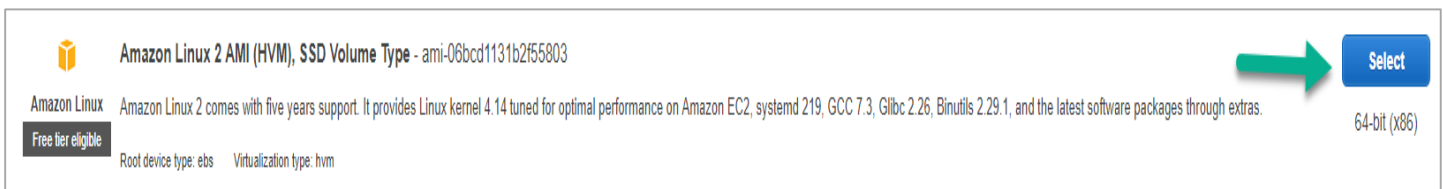
Here after if you want to login, you have to enter credentials and MFA code to Login.

6. Creating First Linux Instance

Login to AWS console, services drop down click on EC2



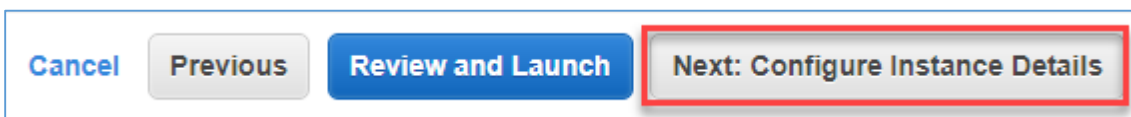
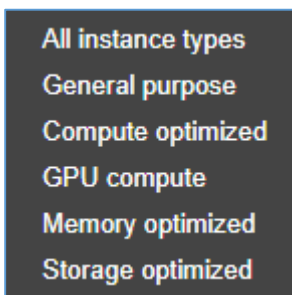
Click on **Launch instance**



I am selecting Free Tier instance Amazon Linux

	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance	IPv6 Support
☐	General purpose	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
☒	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 AMI, 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	☐ 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	☐ 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	☐ Protect against accidental termination	
Monitoring	☐ Enable CloudWatch detailed monitoring Additional charges apply.	
Tenancy	Shared - Run a shared hardware instance Additional charges will apply for dedicated tenancy.	
T2 Unlimited	☐ 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	☒	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**

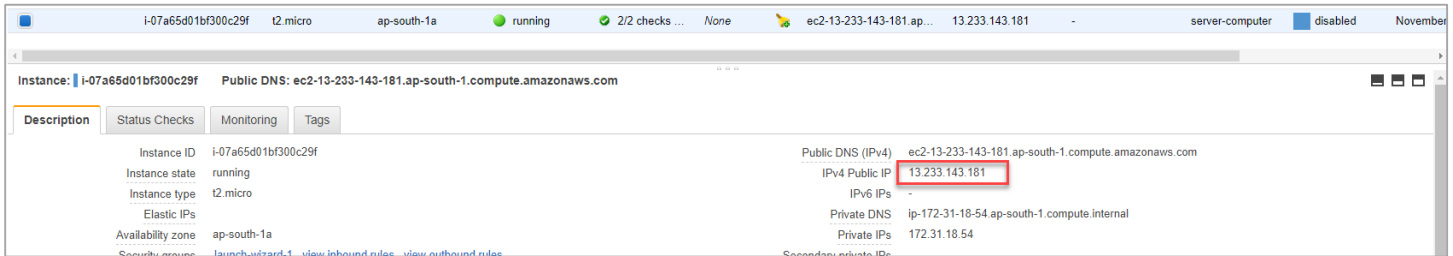
Server-computer.pem file will downloaded, **keep it safe**

Launch Instances

Go to EC2 → See the instances

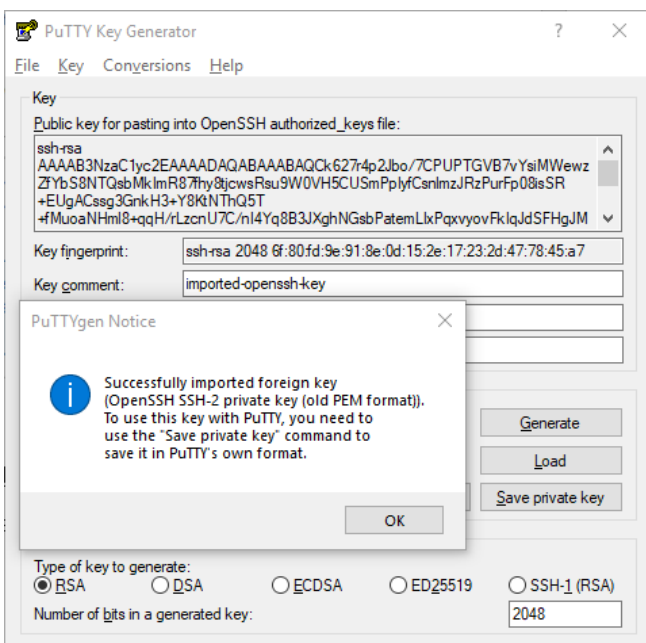
☐	i-07a65d01bf300c29f	t2.micro	ap-south-1a	running	Initializing	None	ec2-13-233-143-181.ap...	13.233.143.181	-	server-computer	disabled	November
--------------------------	---------------------	----------	-------------	---------	--------------	------	--------------------------	----------------	---	-----------------	----------	----------

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

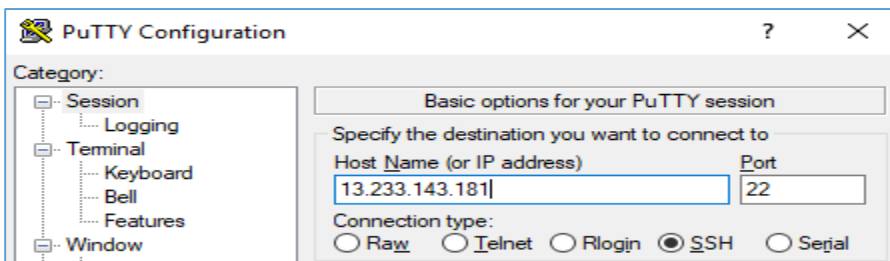


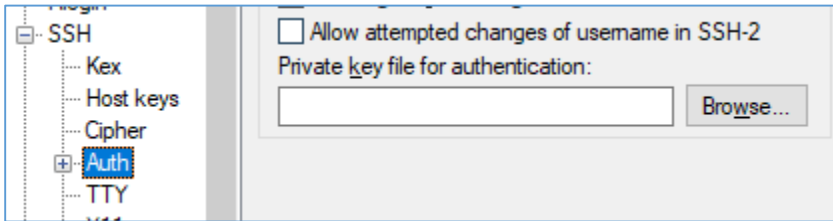
Click Ok.

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

<https://github.com/techtutorials/aws-lab-guide/blob/aws/webserver.sh>

You can also use above shell script to automatically build webserver for you

```
sudo yum update -y;  
sudo yum install httpd -y;  
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. Adding New EBS Volume to Linux Instance

Amazon Elastic Block Store (Amazon EBS) provides persistent block storage volumes for use with Amazon EC2 instances in the AWS Cloud. Each Amazon EBS volume is automatically replicated within its Availability Zone to protect you from component failure, offering high availability and durability. Amazon EBS volumes offer the consistent and low-latency performance needed to run your workloads. With Amazon EBS, you can scale your usage up or down within minutes – all while paying a low price for only what you provision. EBS is designed for application workloads that benefit from fine tuning for performance, cost and capacity.

EC2 Console Left side → Elastic Block Store → Volumes

Create Volume

Select required type of EBS Volume from below types

- General Purpose SSD(gp2)
- Provisioned IOPD SSD (io1)
- Cold HDD(sc1)
- Throughput Optimized HDD (st1)
- Magnetic (standard)

Volumes > Create Volume

Create Volume

Volume Type General Purpose SSD (gp2) ⓘ

Size (GiB) 8 (Min: 1 GiB, Max: 16384 GiB) ⓘ

IOPS 100 / 3000 (Baseline of 3 IOPS per GiB with a minimum of 100 IOPS, burstable to 3000 IOPS) ⓘ

Availability Zone* ap-south-1a ⓘ

Throughput (MB/s) Not applicable ⓘ

Snapshot ID Select a snapshot ⓘ

Encryption ☐ Encrypt this volume ⓘ

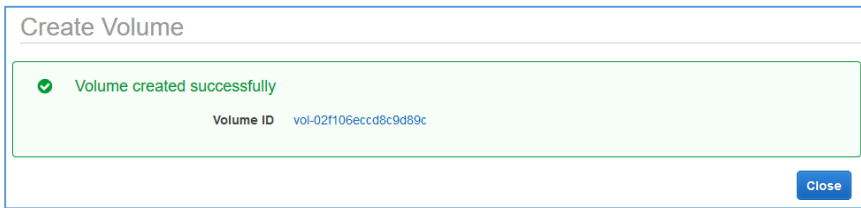
Key	Value
Purpose	External Disk For Data

Add Tag 49 remaining (Up to 50 tags maximum)

Cancel Create Volume

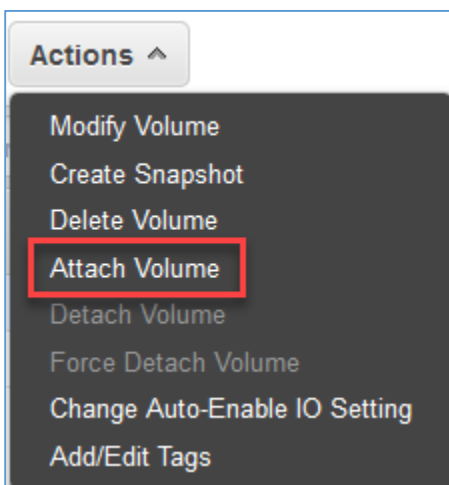
Remember maximum size of EBS volume is 16TB, Select appropriate AZ, if you want to create a volume using existing snapshot select from snapshot ID drop down list. Tick mark Encryption to encrypt data inside volume automatically.

Add tags for easy identification later point of time and click **Create Volume**



Select created EBS volume to attach to the EC2 instance → Click Actions → Attach Volume

☐	Name	Volume ID	Size	Volume Type	IOPS	Snapshot	Created	Availability Zone	State
☐		vol-02f106eccd8c9d89c	8 GiB	gp2	100		December 18, 2018 ...	ap-south-1a	available



Select instance from drop down list and click attach

Attach Volume

Volume ⓘ

vol-02f106eccd8c9d89c in ap-south-1a

Instance ⓘ

in ap-south-1a

Device ⓘ

Linux Devices: /dev/sdf through /dev/sdp

Note: Newer Linux kernels may rename your devices to /dev/xvdf through /dev/xvdp internally, even when the device name entered here (and shown in the details) is /dev/sdf through /dev/sdp.

Cancel

Attach

Login to instance and see the disk using `fdisk -l` command

```
Disk /dev/xvdf: 8 GiB, 8589934592 bytes, 16777216 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
```

In order to format and create new partition use below commands (shown in screenshot)

```
[root@ip-172-31-28-41 ~]# fdisk /dev/xvdf

Welcome to fdisk (util-linux 2.30.2).
Changes will remain in memory only, until you decide to write them.
Be careful before using the write command.

Device does not contain a recognized partition table.
Created a new DOS disklabel with disk identifier 0x3dd167db.

Command (m for help): n
Partition type
   p   primary (0 primary, 0 extended, 4 free)
   e   extended (container for logical partitions)
Select (default p):
Using default response p.
Partition number (1-4, default 1):
First sector (2048-16777215, default 2048):
Last sector, +sectors or +size{K,M,G,T,P} (2048-16777215, default 16777215):

Created a new partition 1 of type 'Linux' and of size 8 GiB.

Command (m for help): wq
The partition table has been altered.
Calling ioctl() to re-read partition table.
Syncing disks.

[root@ip-172-31-28-41 ~]# partprobe /dev/xvdf
[root@ip-172-31-28-41 ~]# mkfs.ext4 /dev/xvdf1
mke2fs 1.42.9 (28-Dec-2013)
Filesystem label=
OS type: Linux
Block size=4096 (log=2)
Fragment size=4096 (log=2)
Stride=0 blocks, Stripe width=0 blocks
524288 inodes, 2096896 blocks
104844 blocks (5.00%) reserved for the super user
First data block=0
Maximum filesystem blocks=2147483648
64 block groups
32768 blocks per group, 32768 fragments per group
8192 inodes per group
Superblock backups stored on blocks:
    32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632

Allocating group tables: done
Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting information: done
```

```
[root@ip-172-31-28-41 ~]# mkdir /newpart
[root@ip-172-31-28-41 ~]# mount /dev/xvdf1 /newpart
[root@ip-172-31-28-41 ~]# df -h
```

Filesystem	Size	Used	Avail	Use%	Mounted on
devtmpfs	476M	0	476M	0%	/dev
tmpfs	493M	0	493M	0%	/dev/shm
tmpfs	493M	392K	493M	1%	/run
tmpfs	493M	0	493M	0%	/sys/fs/cgroup
/dev/xvda1	8.0G	1.2G	6.9G	15%	/
tmpfs	99M	0	99M	0%	/run/user/1000
/dev/xvdf1	7.8G	36M	7.3G	1%	/newpart

Successfully created EBS Volume and attached to Linux Ec2 instance.

```
[root@ip-172-31-28-41 ~]# umount /newpart
[root@ip-172-31-28-41 ~]# fdisk /dev/xvdf
```

Welcome to fdisk (util-linux 2.30.2).
Changes will remain in memory only, until you decide to write them.
Be careful before using the write command.

Command (m for help): p
Disk /dev/xvdf: 8 GiB, 8589934592 bytes, 16777216 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x3dd167db

Device	Boot	Start	End	Sectors	Size	Id	Type
/dev/xvdf1		2048	16777215	16775168	8G	83	Linux

Command (m for help): d
Selected partition 1
Partition 1 has been deleted.

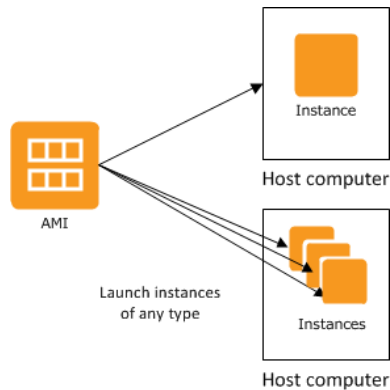
Command (m for help): wq
The partition table has been altered.
Calling ioctl() to re-read partition table.
Syncing disks.

8. Creating Amazon Machine Image (AMI)

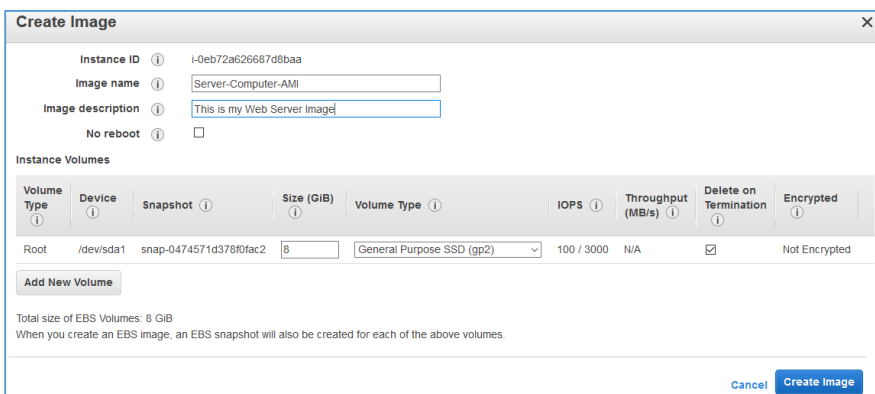
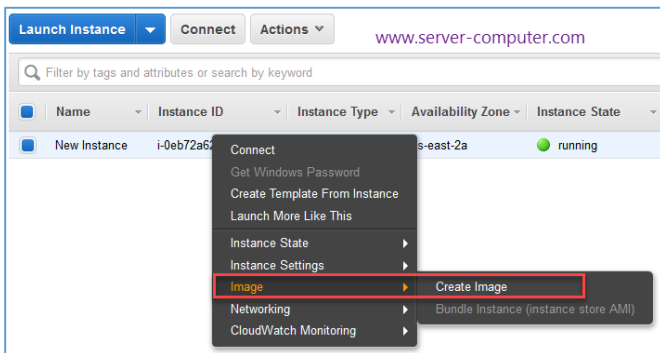
An Amazon Machine Image (AMI) provides the information required to launch an instance, which is a virtual server in the cloud. You must specify a source AMI when you launch an instance. You can launch multiple instances from a single AMI when you need multiple instances with the same configuration. You can use different AMIs to launch instances when you need instances with different configurations.

An AMI includes the following:

- A template for the root volume for the instance (for example, an operating system, an application server, and applications)
- Launch permissions that control which AWS accounts can use the AMI to launch instances
- A block device mapping that specifies the volumes to attach to the instance when it's launched



First, follow above steps to create EC2 instance, modify all the required settings, and install required applications. Right click on instance **Image** → **Create Image**



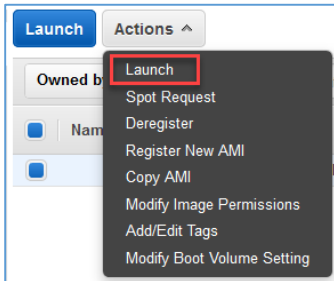
Provide Image name (Easy to Identify), Image Description and Click **Create Image**

It will take few minutes depends on your EC2 instance size.

Go to → EC2 → AMIs

	Name	AMI Name	AMI ID	Source	Owner	Visibility	Status
		Server-Computer-AMI	ami-03be1b9f43f8b067e	685992403869/S...	685992403869	Private	available

Select AMI → Actions → Launch



Choose Instance Type → Click Next: Configure Instance Details

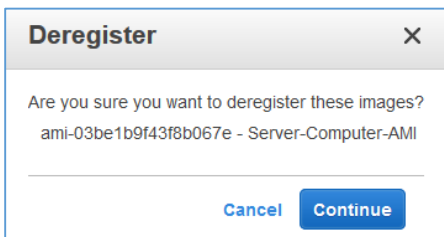
Network	vpc-02c316e5f1be2208a MyVPC	Create new VPC
No default VPC found. Create a new default VPC .		
Subnet	subnet-01f8724bb68578a99 S3-Public us-east-2	Create new subnet
250 IP Addresses available		
Auto-assign Public IP	Enable	

Select appropriate details Click **Next: Add Storage** → **Next: Add Tags** → **Next: Configure Security Group** → **Review and Launch** → **Launch**

That is it your application is ready to use.

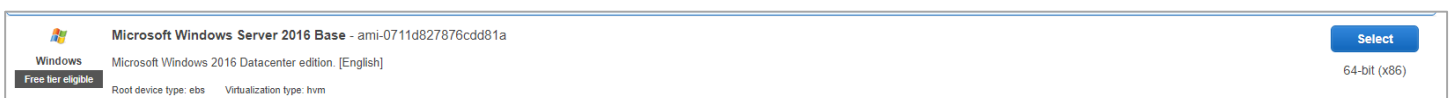
Note: Storing AMI will be charged based on your EC2 instance size.

To delete the AMI select AMI → Actions → Deregister



9. Create your First EC2 windows instance

Expand services EC2 → Launch Instance



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 4089 IP Addresses available	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:

Description:

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

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

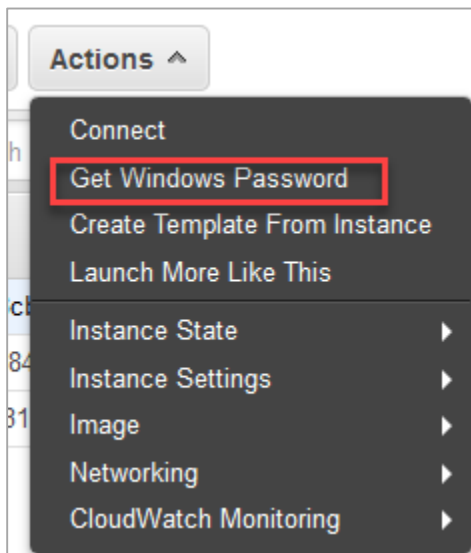
Note: Wait 4 Minutes instance to launch

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/EHjWlDAQABAOIBAGJwGLht+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.

10. 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

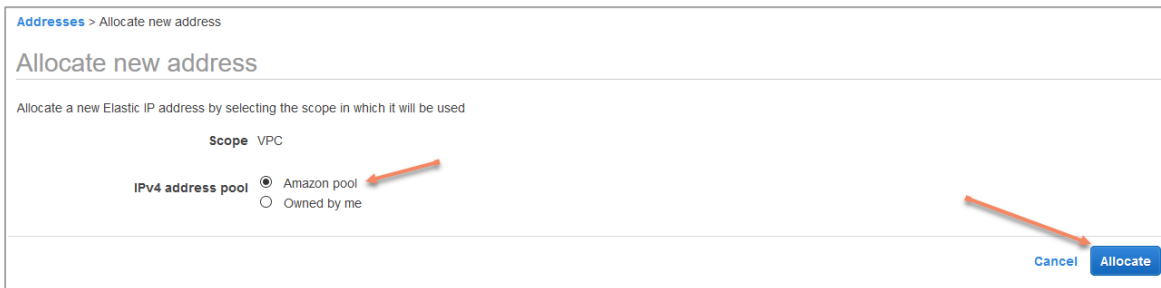
Public DNS (IPv4)	ec2-13-127-65-71.ap-south-1.compute.amazonaws.com
IPv4 Public IP	13.127.65.71
IPv6 IPs	-
Private DNS	ip-172-31-25-150.ap-south-1.compute.internal
Private IPs	172.31.25.150

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

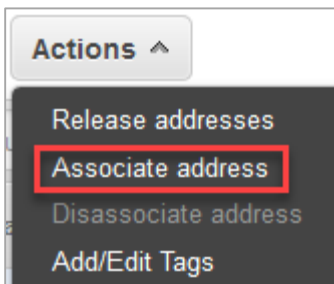


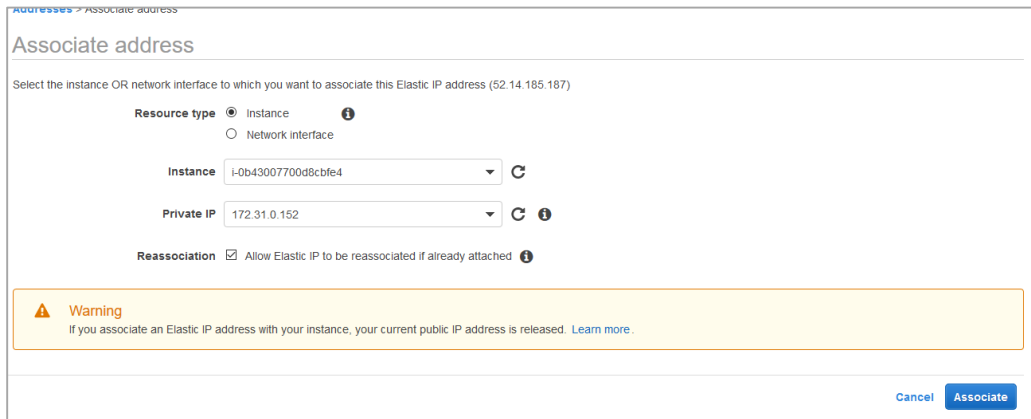
EC2 console right side bar go down → Elastic IPs → Allocate New Address



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.

11. Amazon Elastic File System

Amazon Elastic File System (Amazon EFS) provides simple, scalable file storage for use with Amazon EC2. With Amazon EFS, storage capacity is elastic, growing and shrinking automatically as you add and remove files, so your applications have the storage they need, when they need it. Amazon EFS has a simple web services interface that allows you to create and configure file systems quickly and easily. The service manages all the file storage infrastructure for you, meaning that you can avoid the complexity of deploying, patching, and maintaining complex file system configurations.

Amazon EFS supports the Network File System version 4 (NFSv4.1 and NFSv4.0) protocol, so the applications and tools that you use today work seamlessly with Amazon EFS. Multiple Amazon EC2 instances can access an Amazon EFS file system at the same time, providing a common data source for workloads and applications running on more than one instance or server.

Services → EFS



Configure file system access

An Amazon EFS file system is accessed by EC2 instances running inside one of your VPCs. Instances connect to a file system by using a network interface called a mount target. Each mount target has an IP address, which we assign automatically or you can specify.

VPC vpc-b03915d7 (default) ⓘ

Create mount targets

Instances connect to a file system by using mount targets you create. We recommend creating a mount target in each of your VPC's Availability Zones so that EC2 instances across your VPC can access the file system.

	Availability Zone	Subnet	IP address	Security groups
☒	ap-southeast-1a	subnet-e0c5c4a9 (default)	Automatic ⓘ	sg-d02a96ab - default ×
☒	ap-southeast-1b	subnet-f79f8e90 (default)	Automatic ⓘ	sg-d02a96ab - default ×
☒	ap-southeast-1c	subnet-121bd74b (default)	Automatic ⓘ	sg-d02a96ab - default ×

Cancel Next Step

Configure optional settings

Add tags

You can add tags to describe your file system. A tag consists of a case-sensitive key-value pair. (For example, you can define a tag with key-value pair with key = Corporate Department and value = Sales and Marketing.) At a minimum, we recommend a tag with key = Name.

Key	Value	Remove
Name	NFS Share	×
Purpose	Data Store for Users	×
Add New Key		

Choose performance mode

We recommend **General Purpose** performance mode for most file systems. **Max I/O** performance mode is optimized for applications where tens, hundreds, or thousands of EC2 instances are accessing the file system — it scales to higher levels of aggregate throughput and operations per second with a tradeoff of slightly higher latencies for file operations.

☒ **General Purpose**
☐ **Max I/O**

Choose throughput mode

We recommend **Bursting** throughput mode for most file systems. Use **Provisioned** throughput mode for applications that require more throughput than allowed by **Bursting** throughput. [Learn more](#)

☒ **Bursting**
☐ **Provisioned**

Enable encryption

If you enable encryption for your file system, all data on your file system will be encrypted at rest. You can select a KMS key from your account to protect your file system, or you can provide the ARN of a key from a different account. Encryption of data at rest can only be enabled during file system creation. Encryption of data in transit is configured when mounting your file system. [Learn more](#)

☐ **Enable encryption of data at rest**

Cancel Previous Next Step

Review and create

Review the configuration below before proceeding to create your file system.

File system access

VPC	Availability Zone	Subnet	IP address	Security groups
vpc-b03915d7 (default)	ap-southeast-1a	subnet-e0c5c4a9 (default)	Automatic	sg-d02a96ab - default
	ap-southeast-1b	subnet-f79f8e90 (default)	Automatic	sg-d02a96ab - default
	ap-southeast-1c	subnet-121bd74b (default)	Automatic	sg-d02a96ab - default

Optional settings

Tags

Name: NFS Share

Purpose: Data Store for Users

Performance mode

General Purpose

Throughput mode

Bursting

Encrypted

No

Cancel

Previous

Create File System

	Name	File system ID	Metered size	Number of mount targets	Creation date
● ▼	NFS Share	fs-8ede0bcf	6.0 KiB	3	12/18/2018, 16:56:28 UTC

VPC	Availability Zone	Subnet	IP address	Mount target ID	Network interface ID	Security groups	Mount target state
vpc-b03915d7 (default)	ap-southeast-1a	subnet-e0c5c4a9 (default)	172.31.44.200	fsmt-2cd3276d	eni-0b6eff4261e7bd82e	sg-d02a96ab - default	Available
	ap-southeast-1c	subnet-121bd74b (default)	172.31.0.90	fsmt-2fd3276e	eni-08fdd5d4a457eaa7b	sg-d02a96ab - default	Available
	ap-southeast-1b	subnet-f79f8e90 (default)	172.31.30.4	fsmt-31d32770	eni-058f7e4b529f27eee	sg-d02a96ab - default	Available

Login to EC2 Linux instance and mount EFS using below commands

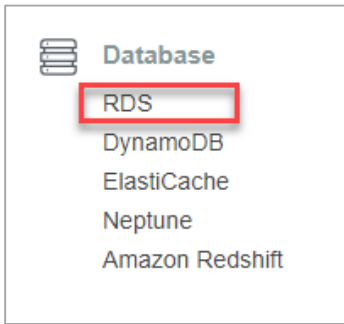
```
# sudo yum -y install nfs-utils*
# sudo mount -t nfs4 IP_ADDRESS_OF_EFS:/ MOUNTPOINT
```

That's it about EFS.

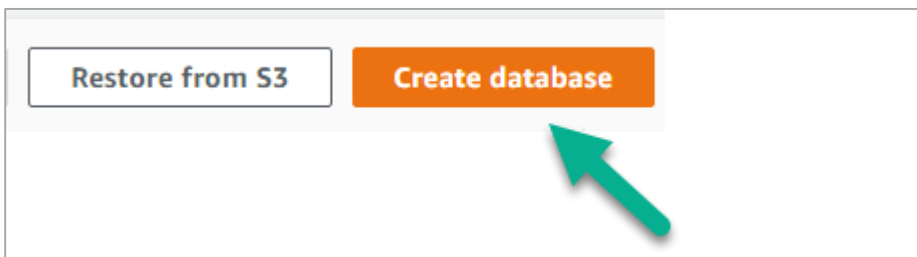
12.Launching RDS Instance

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.

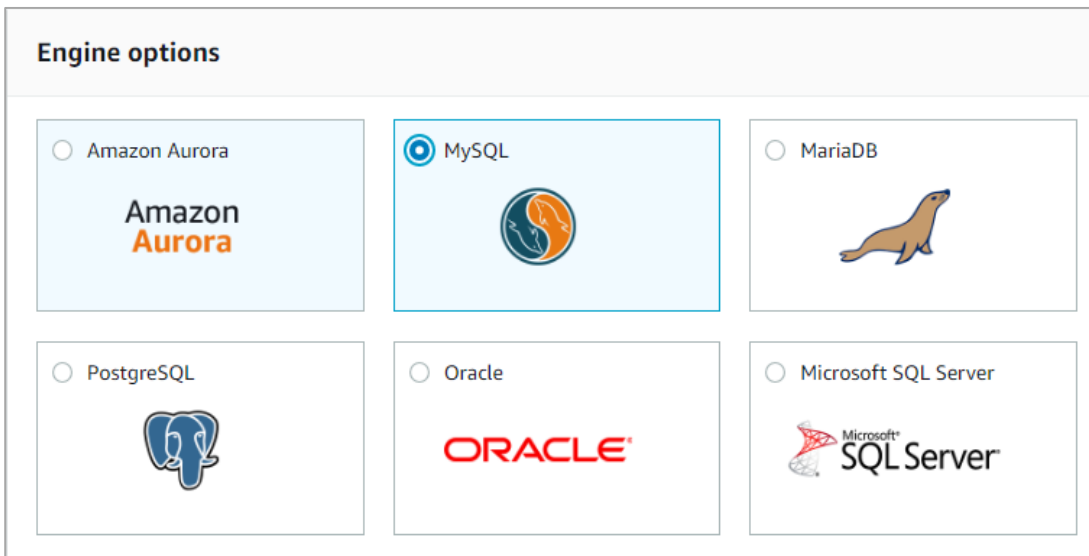
Login to **AWS Console** and Click on **services** to list all services. Navigate to **Database → RDS**



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



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.

The screenshot shows the AWS RDS instance configuration page. It includes a dropdown for 'DB instance class' (db.r4.xlarge), a radio button for 'Multi-AZ deployment' (No), a dropdown for 'Storage type' (General Purpose (SSD)), and a text input for 'Allocated storage' (20 GiB). Red circles with numbers 1-4 and green arrows point to these specific fields. A blue information box at the bottom provides a warning about provisioning less than 100 GiB of General Purpose (SSD) storage.

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.

i Provisioning less than 100 GiB of General Purpose (SSD) storage for high throughput workloads could result in higher latencies upon exhaustion of the initial General Purpose (SSD) IO credit balance. [Click here](#) for more details.

1. Select DB Instance class like required CPU Cores and RAM.
2. Create Replica in Different Zone. (Which means database will be replicated to another available zone for redundant(data protection))
3. General purpose (SSD) or provisioned IOPS (SSD)
 - a. General purpose is for low through put applications
 - 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](#)

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.

DB parameter group [Info](#)

Option group [Info](#)

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

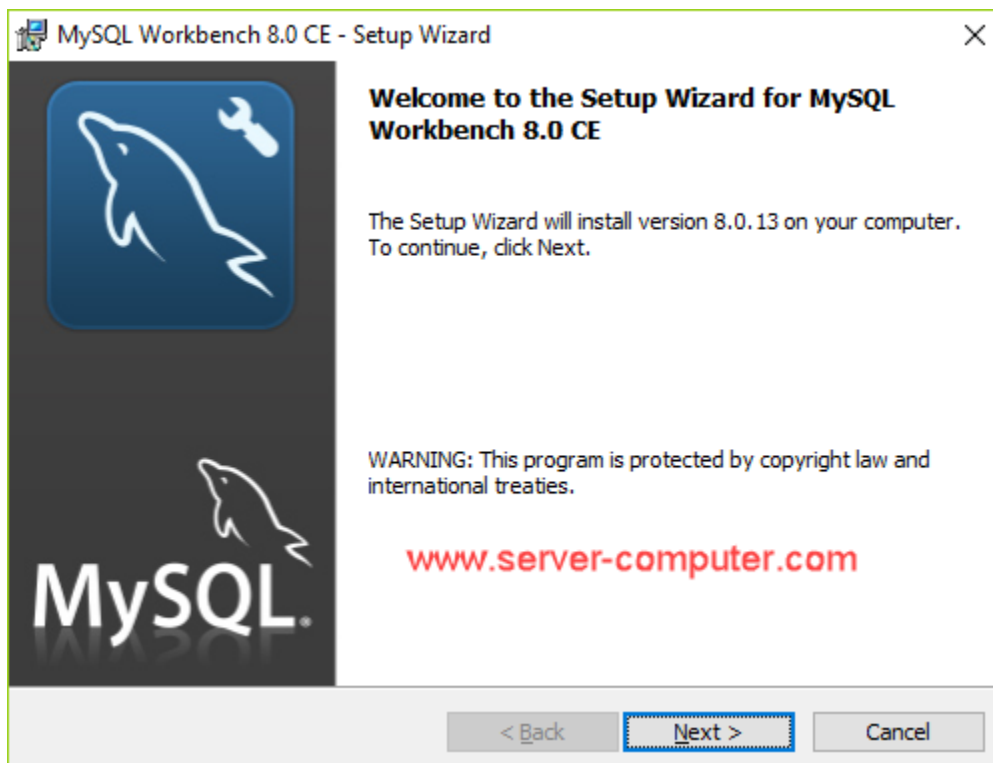
Click **Create Database**

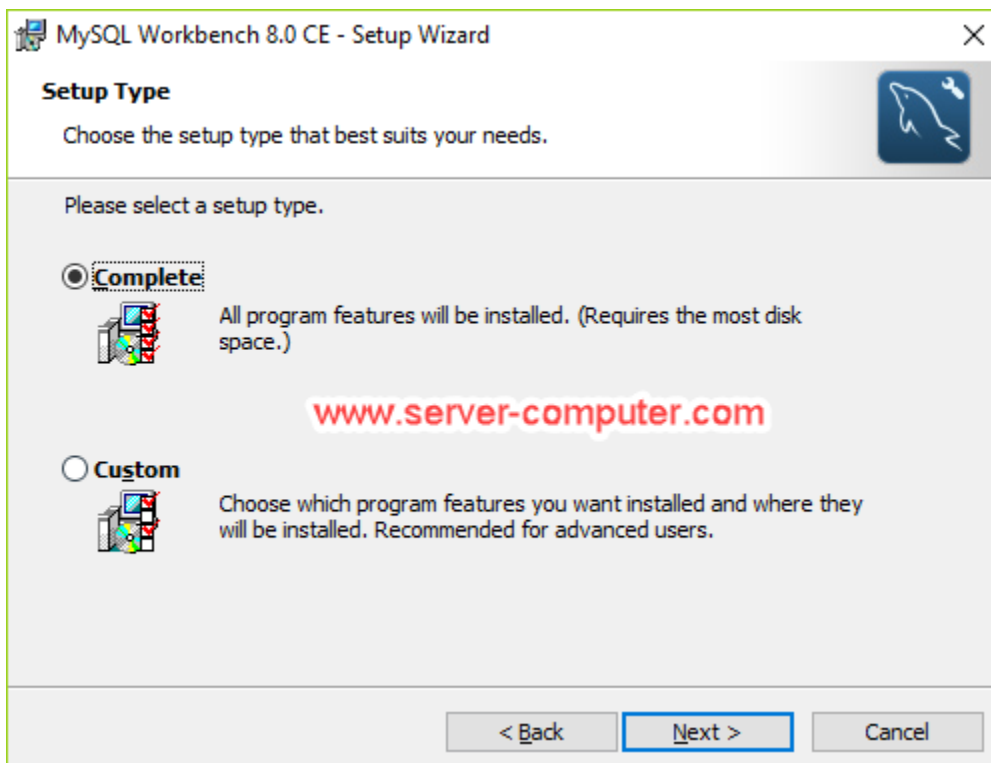
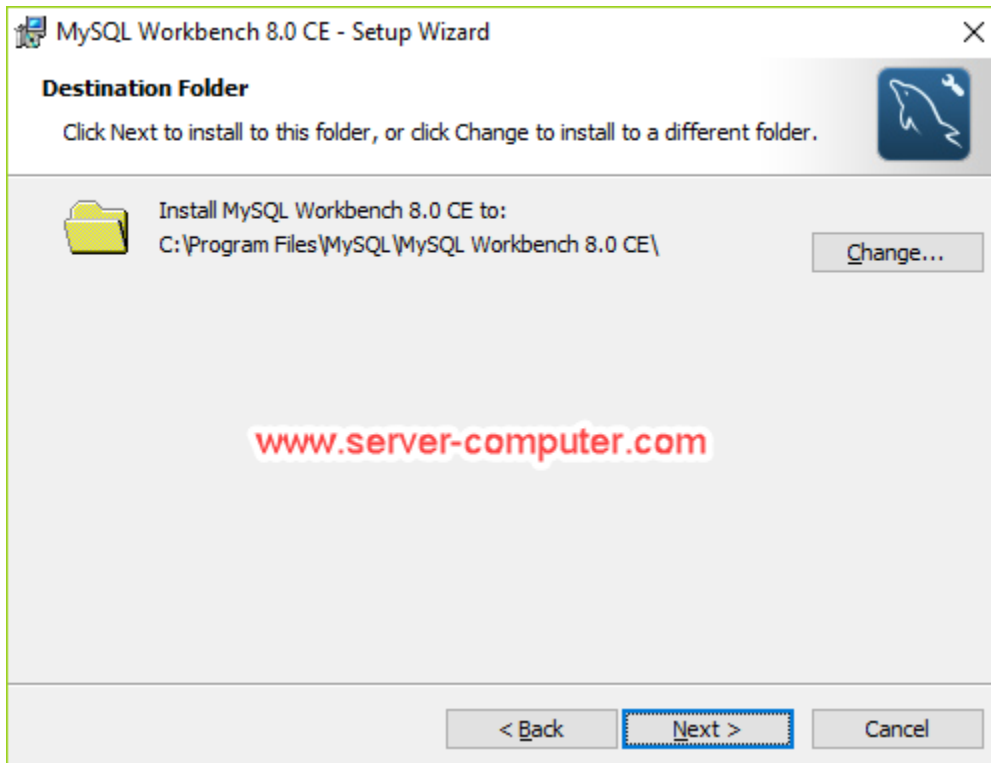
Note: Database instance creation will take at least 10minutes.

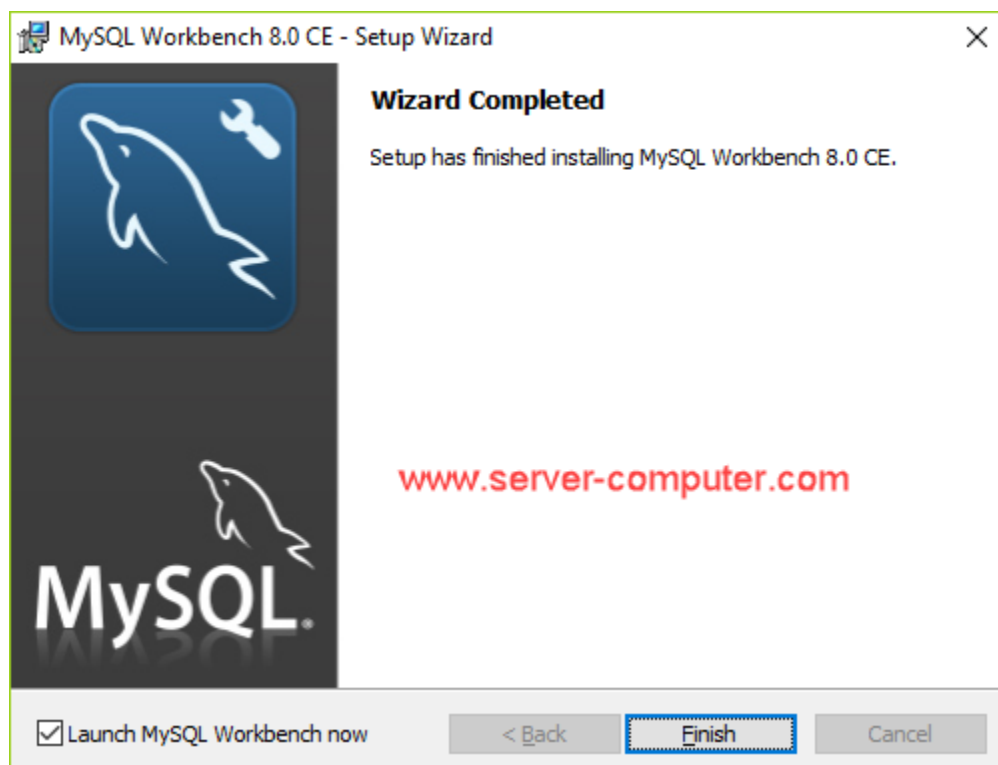
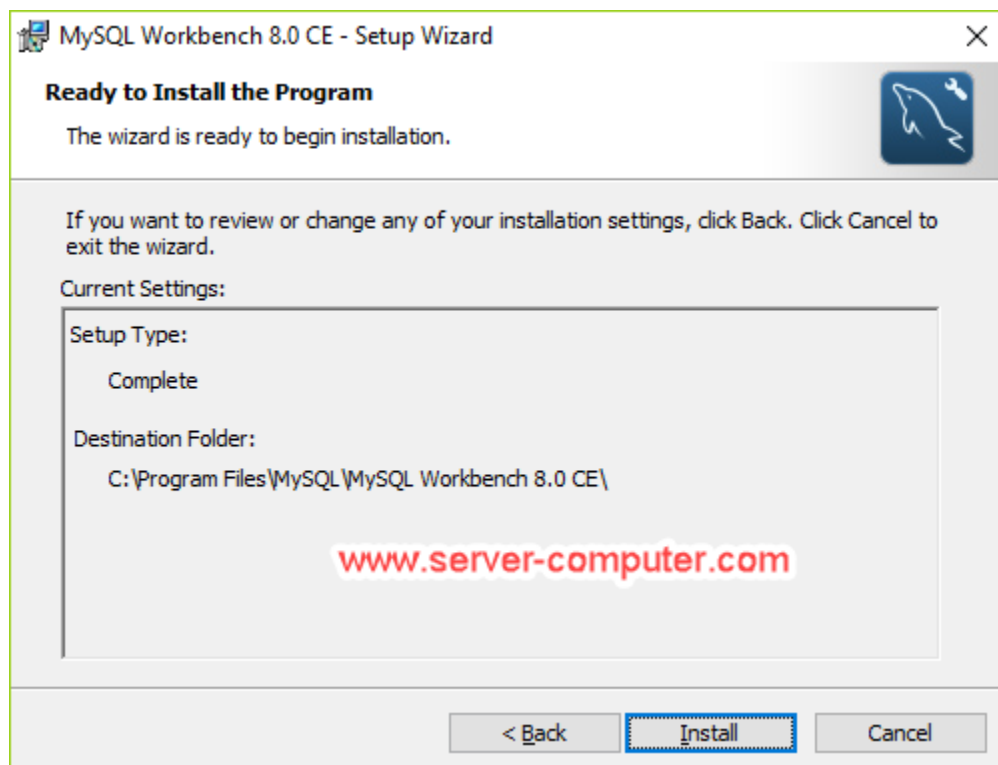
13.Accessing MySQL Instance Using Workbench

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

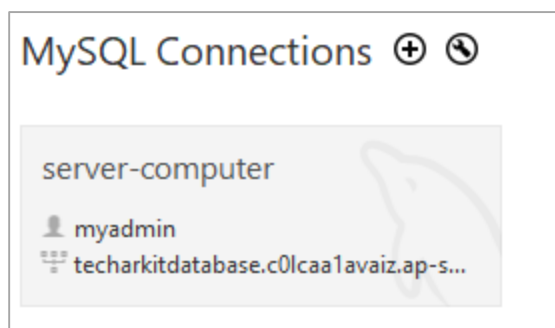
Hostname: Port: Name or IP address of the server host - and TCP/IP port.

Username: Name of the user to connect with.

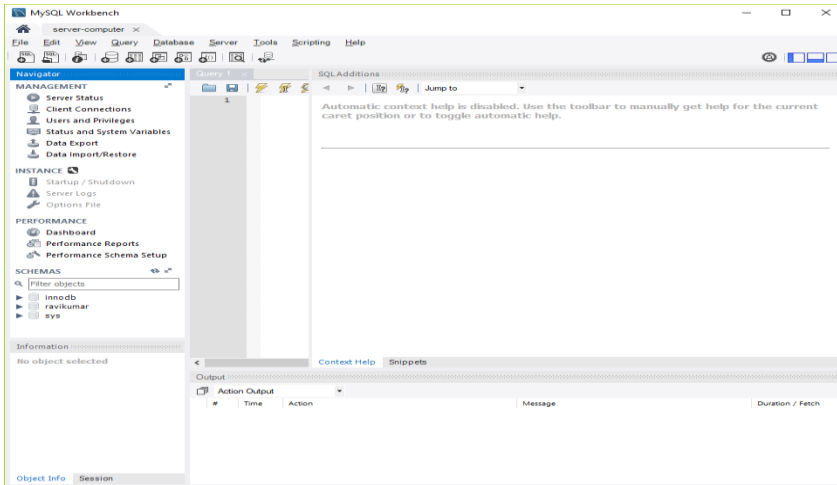
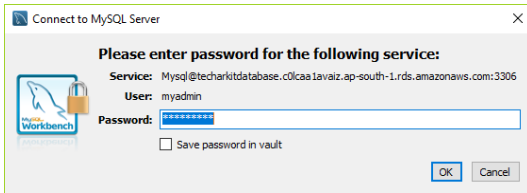
Password: The user's password. Will be requested later if it's not set.

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

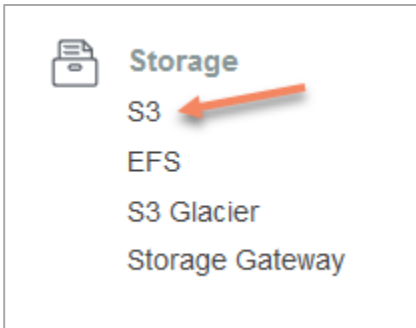
```
create table students(  
    student_id INT NOT NULL AUTO_INCREMENT,  
    student_title VARCHAR(100) NOT NULL,  
    student_author VARCHAR(40) NOT NULL,  
    submission_date DATE,  
    PRIMARY KEY ( student_id )  
);  
  
show databases;  
  
use DBNAME;  
  
show tables;
```

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

14. AWS S3 Bucket – (Object Storage)

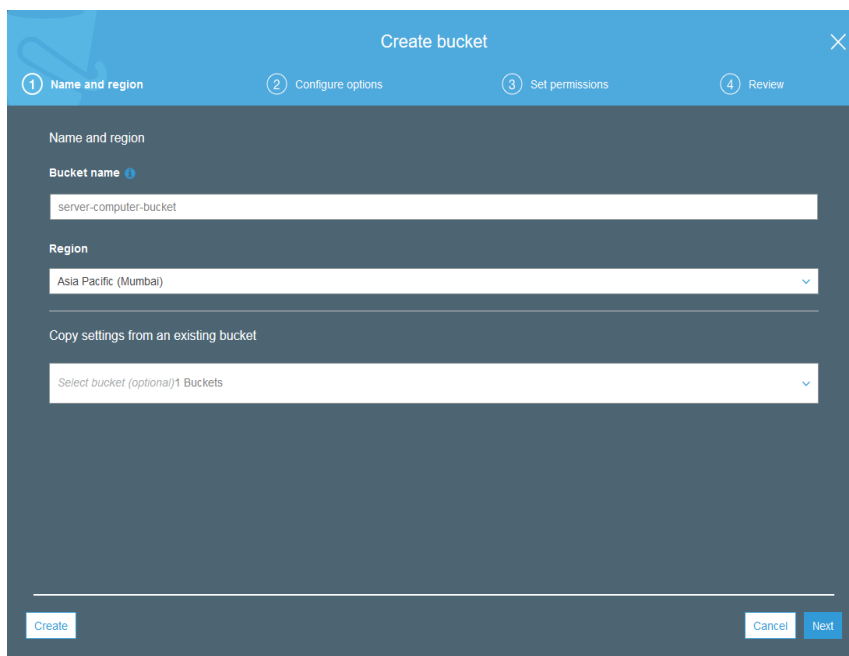
Amazon Simple Storage Service (Amazon S3) is storage for the Internet. You can use Amazon S3 to store and retrieve any amount of data at any time, from anywhere on the web. You can accomplish these tasks using the AWS Management Console, which is a simple and intuitive web interface.

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



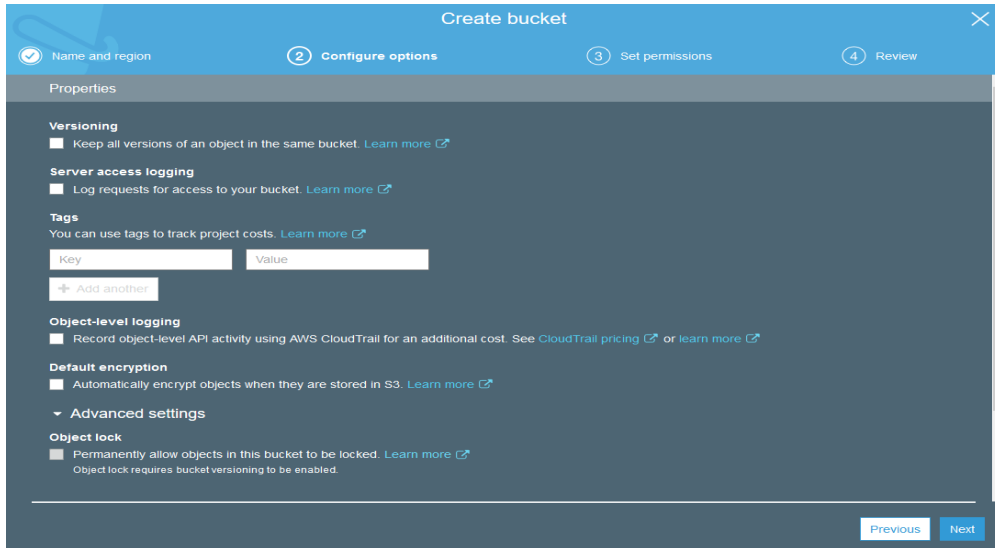
+ Create bucket

Click on

A screenshot of the 'Create bucket' wizard in the AWS Management Console. The wizard has a blue header with the title 'Create bucket' and a close button. Below the header is a progress bar with four steps: 1. Name and region, 2. Configure options, 3. Set permissions, and 4. Review. The first step, 'Name and region', is active. It contains three input fields: 'Bucket name' with the value 'server-computer-bucket', 'Region' with a dropdown menu showing 'Asia Pacific (Mumbai)', and 'Copy settings from an existing bucket' with a dropdown menu showing 'Select bucket (optional) 1 Buckets'. At the bottom of the form are three buttons: 'Create', 'Cancel', and 'Next'.

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

Click **Next**



Create bucket

1 Name and region 2 **Configure options** 3 Set permissions 4 Review

Properties

Versioning
☐ Keep all versions of an object in the same bucket. [Learn more](#)

Server access logging
☐ Log requests for access to your bucket. [Learn more](#)

Tags
You can use tags to track project costs. [Learn more](#)

Key Value
[Add another](#)

Object-level logging
☐ Record object-level API activity using AWS CloudTrail for an additional cost. See [CloudTrail pricing](#) or [learn more](#)

Default encryption
☐ Automatically encrypt objects when they are stored in S3. [Learn more](#)

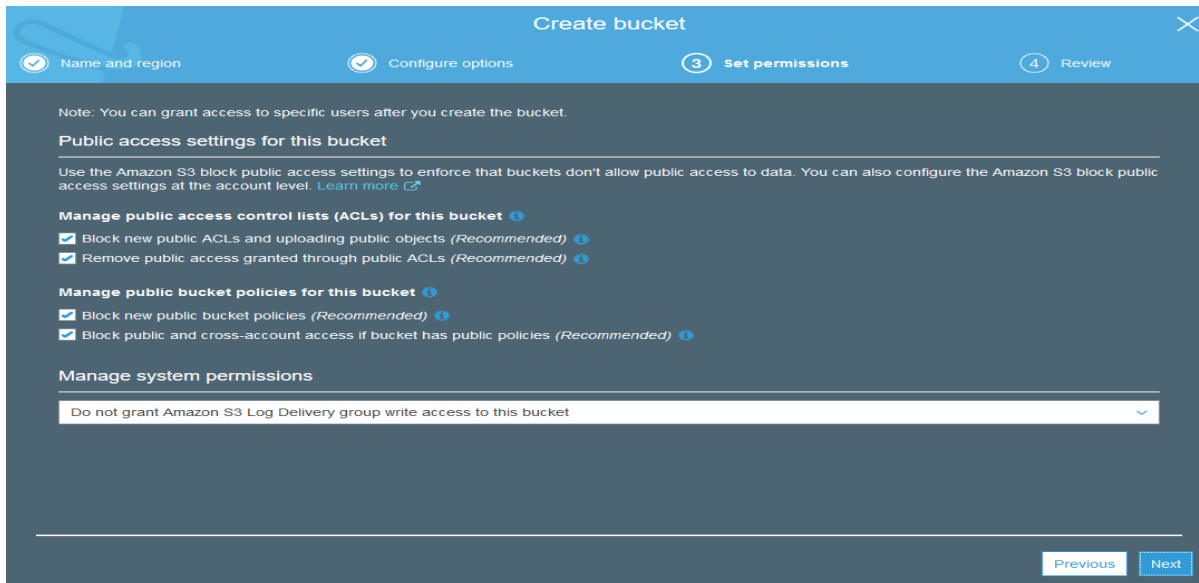
Advanced settings

Object lock
☐ Permanently allow objects in this bucket to be locked. [Learn more](#)
Object lock requires bucket versioning to be enabled.

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

- ✚ **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**



Create bucket

1 Name and region 2 Configure options 3 **Set permissions** 4 Review

Note: You can grant access to specific users after you create the bucket.

Public access settings for this bucket

Use the Amazon S3 block public access settings to enforce that buckets don't allow public access to data. You can also configure the Amazon S3 block public access settings at the account level. [Learn more](#)

Manage public access control lists (ACLs) for this bucket

☒ Block new public ACLs and uploading public objects (*Recommended*)

☒ Remove public access granted through public ACLs (*Recommended*)

Manage public bucket policies for this bucket

☒ Block new public bucket policies (*Recommended*)

☒ Block public and cross-account access if bucket has public policies (*Recommended*)

Manage system permissions

Do not grant Amazon S3 Log Delivery group write access to this bucket

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

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**

The screenshot shows the 'Create bucket' wizard in the AWS Management Console, specifically the 'Review' step. The progress bar at the top indicates that 'Name and region', 'Configure options', and 'Set permissions' are completed, while 'Review' is the current step. The 'Name and region' section shows the bucket name 'server-computer-bucket' and the region 'Asia Pacific (Mumbai)'. The 'Options' section lists various settings: Versioning (Disabled), Server access logging (Disabled), Tagging (0 Tags), Object-level logging (Disabled), Default encryption (None), CloudWatch request metrics (Disabled), and Object lock (Disabled). The 'Permissions' section shows four settings, all set to 'True': Block new public ACLs and uploading public objects, Remove public access granted through public ACLs, Block new public bucket policies, and Block public and cross-account access if bucket has public policies. At the bottom right, there are 'Previous' and 'Create bucket' buttons.

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

14.1. AWS S3 Lifecycle Management

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

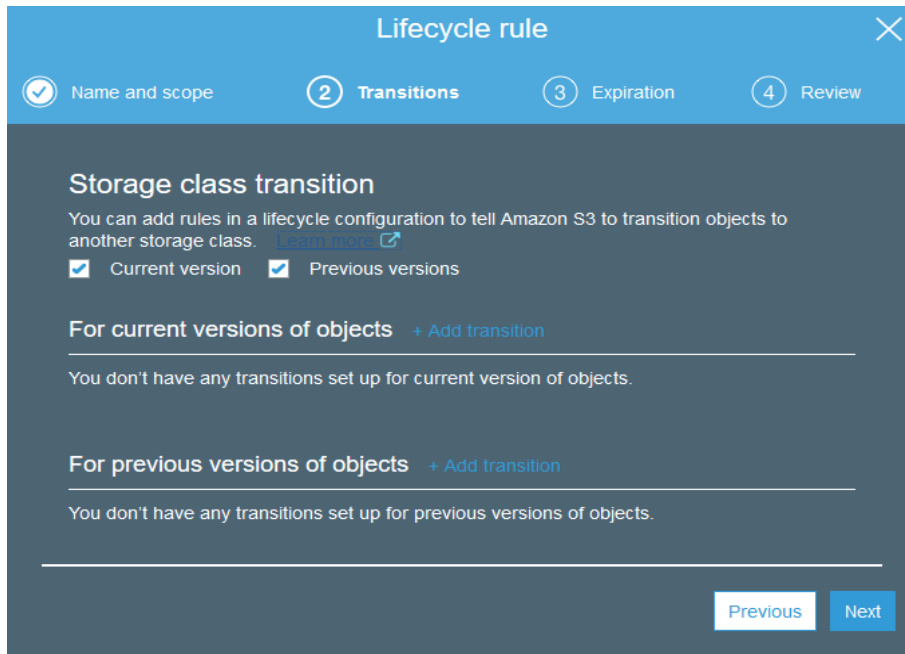
You can manage an objects lifecycle using this feature/rule, which defines

The screenshot shows the 'Lifecycle rule' wizard in the AWS Management Console, specifically the 'Name and scope' step. The progress bar at the top indicates that 'Name and scope' is the current step, followed by 'Transitions', 'Expiration', and 'Review'. The 'Enter a rule name' section has a text input field containing 'Rule_MyBucket'. The 'Add filter to limit scope to prefix/tags' section has a button labeled 'tag Yearly | X'. Below this is a text input field labeled 'Type to add prefix/tag filter'. At the bottom right, there are 'Cancel' and 'Next' buttons.

Enter Rule Name

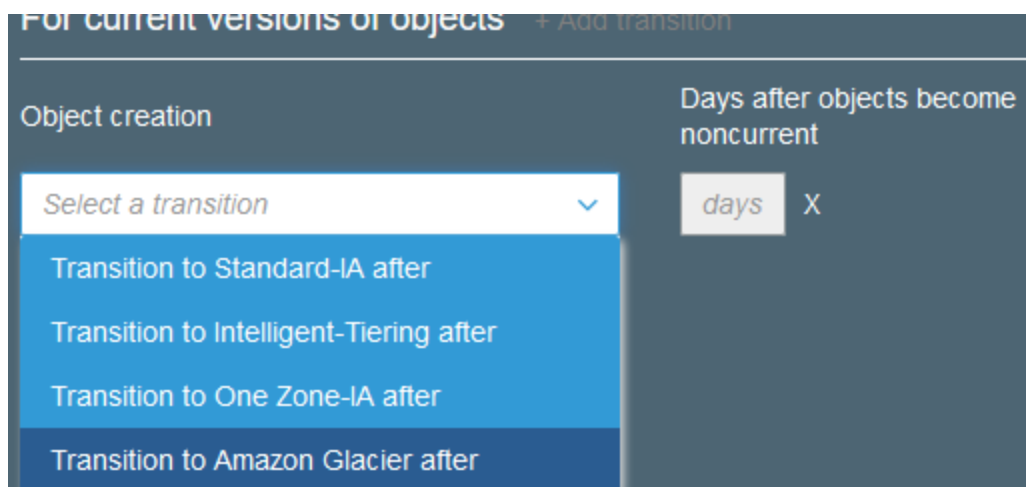
Tag Name if you do not want leave it blank

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 shows four steps: 1. Name and scope, 2. Transitions, 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 shows four steps: 1. Name and scope, 2. Transitions, 3. Expiration, 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**.

14.2. 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' radio button is selected, and the bucket name 'arkit-test123' is displayed. The 'Prefix or tags' option is also visible. Under 'Replication criteria', the checkbox 'Replicate objects encrypted with AWS KMS' is unchecked. A blue information box contains a message about the new CRR schema. At the bottom right, there are 'Cancel' and 'Next' buttons.

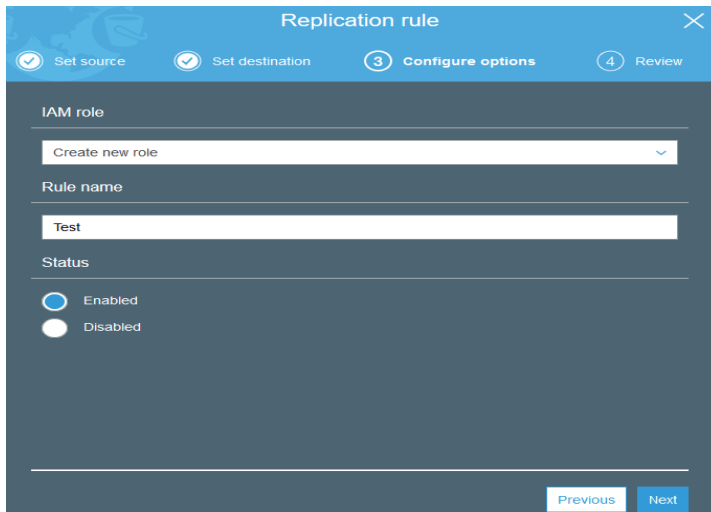
Click **Next**

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'. Under 'Options', the checkbox 'Change the storage class for the replicated object(s)' is checked. Below this, the 'Storage class' is set to 'Glacier'. A note suggests choosing a storage class based on use case and access requirements, with links to 'Learn more' and 'Amazon S3 pricing'. At the bottom, there is an unchecked checkbox '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**

14.3. 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 ("*")

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

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

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

Add Statement

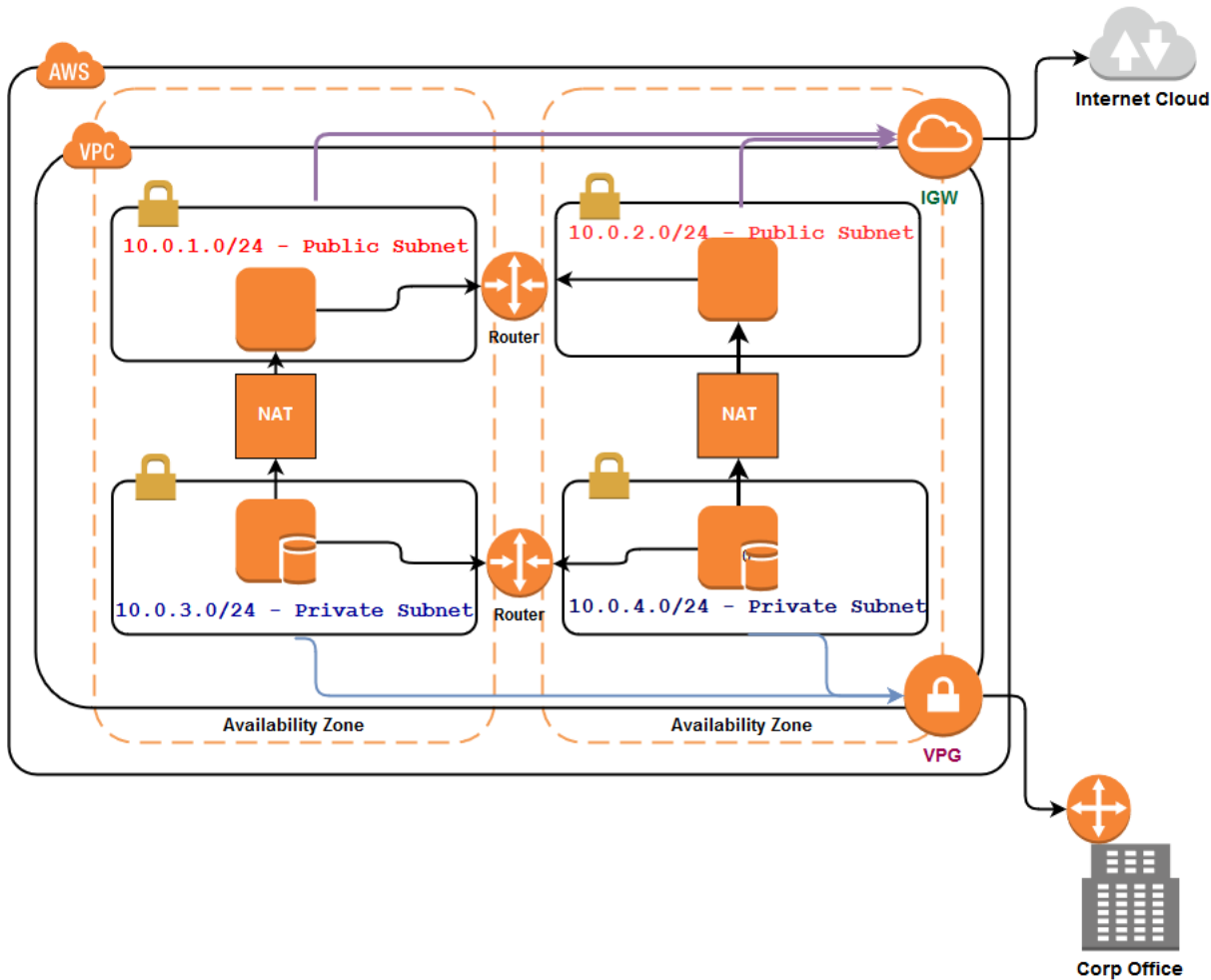
Add Statement and click on **Generate Policy**

```
{
  "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**

15. 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

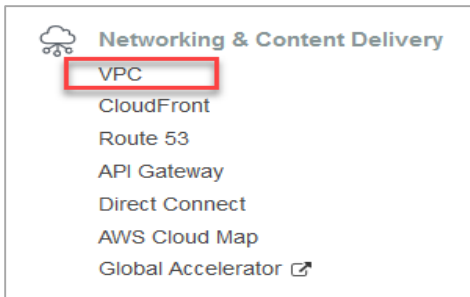
Architecture Explanation:

- 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 selected). 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:

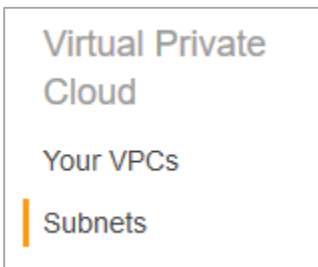
VPC ID vpc-02c316e5f1be2208a

Close

Your VPC created successfully.

15.1. 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 CIDRs	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

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

15.2. 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 the 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. Below this, a green notification box states 'The following internet gateway was created:' with the 'Internet gateway ID' 'igw-0b5da69f9e34ec455' and a 'Close' button. An 'Actions' dropdown menu is open, showing 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. The breadcrumb is 'Internet gateways > Attach to VPC' and the URL is '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 is an 'AWS Command Line Interface command' section. At the bottom are 'Cancel' and 'Attach' buttons.

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

15.3. 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

15.4. 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
0.0.0.0/0	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
192.168.0.0/16	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)

☐	Name	Subnet ID	State	VPC
☒	S1-Private	subnet-01b0a1e5be742dde0	available	vpc-02c316e5f1be2208a ...
☐	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

☐	Name	Subnet ID	State	VPC
☒	S4-Public	subnet-09d6c82e020a61325	available	vpc-02c316e5f1be2208a ...

Subnet: subnet-09d6c82e020a61325

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

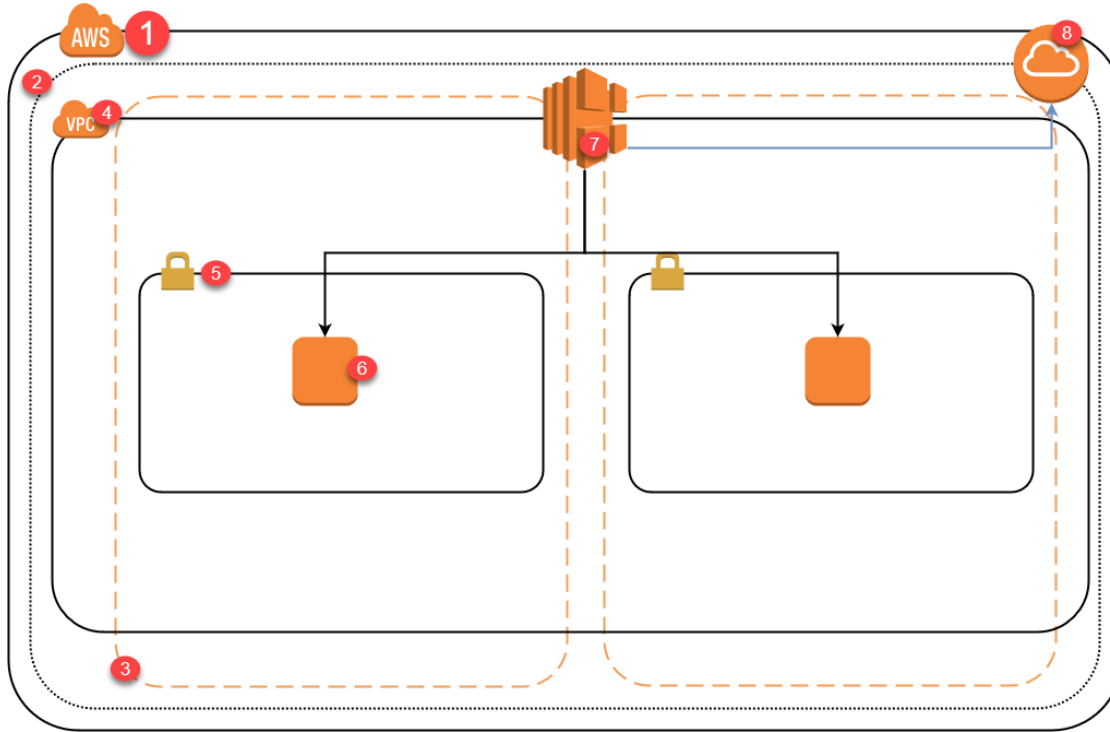
[Edit route table association](#)

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

16. 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

<https://github.com/techtutorials/aws-lab-guide/blob/aws/webserver.sh>

```
#!/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 ⓘ

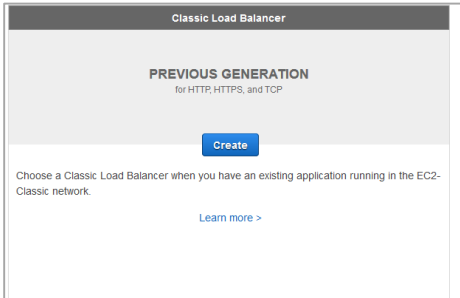
☒ As text ☐ As file ☐ Input is already base64 encoded

```
#!/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: server-computer

Create LB inside: vpc-02c316e5f1be2208a (10.0.0.0/16) | MyVPC

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: LoadBalancer-Sec

Description: quick-create-1 created on Wednesday, December 5, 2018 at 5:55:45 F

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
☒	i-0e831d986cac3f5f6	running	WebServer-Loadbalancer
☒	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

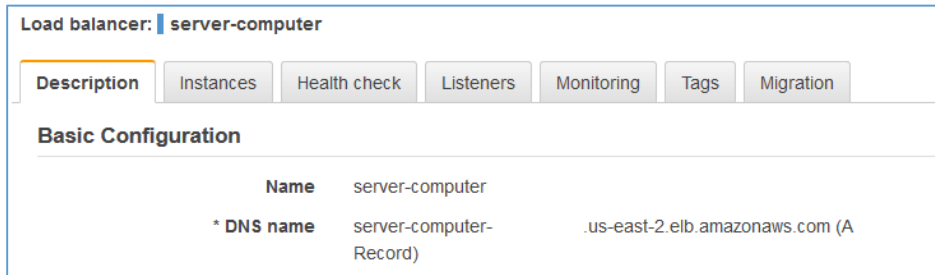
Description Instances Health check Listeners Monitoring Tags Migration

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.

17. 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.

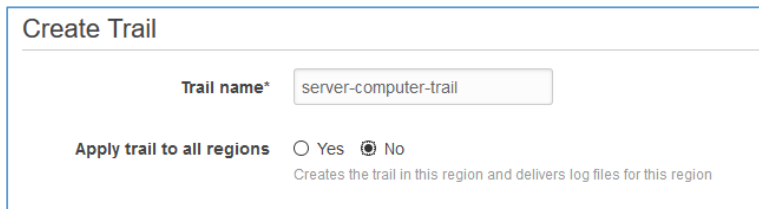
CloudTrail is enabled on your AWS account when you create it. When activity occurs in your AWS account, that activity is recorded in a CloudTrail event. You can easily view recent events in the CloudTrail console by going to Event history.

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.

17.1. 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
☐ Select all S3 buckets in your account ⓘ		☒ Read	☒ Write
arkit-test123	/ CloudTrail	☒ Read	☒ 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.

18. Athena Analytics

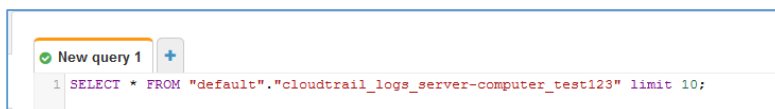
If you would like to create a table in hive using existing logs, you can create by clicking on **Athena table creation**.

```
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

19. Auto Scaling

Amazon EC2 Auto Scaling helps you ensure that you have the correct number of Amazon EC2 instances available to handle the load for your application. You create collections of EC2 instances, called Auto Scaling groups. You can specify the minimum number of instances in each Auto Scaling group, and Amazon EC2 Auto Scaling ensures that your group never goes below this size. You can specify the maximum number of instances in each Auto Scaling group, and Amazon EC2 Auto Scaling ensures that your group never goes above this size. If you specify the desired capacity, either when you create the group or at any time thereafter, Amazon EC2 Auto Scaling ensures that your group has this many instances. If you specify scaling policies, then Amazon EC2 Auto Scaling can launch or terminate instances as demand on your application increases or decreases.

19.1. Launch configuration

Login to **AWS Console** → **EC2** → (Under Auto Scaling) Click on **Launch Configurations**

Create launch configuration

- **Choose AMI** (I select Ubuntu 18.04 LTS)
- **Choose Instance Type** (t2.micro) Click Next: Configure Details

Create Launch Configuration

Name ⓘ	MyFirstLaunchConfiguration
Purchasing option ⓘ	☐ Request Spot Instances
IAM role ⓘ	None
Monitoring ⓘ	☐ Enable CloudWatch detailed monitoring Learn more

>> Click **Advanced Details**

IP Address Type ⓘ

- ☐ Only assign a public IP address to instances launched in the default VPC and subnet. (default)
- ☒ Assign a public IP address to every instance.
- ☐ Do not assign a public IP address to any instances.

Note: this option only affects instances launched into an Amazon VPC

Note: In case there is no default VPC available in selected zone (In my case I deleted default VPC).

Click **Next: Add Storage**

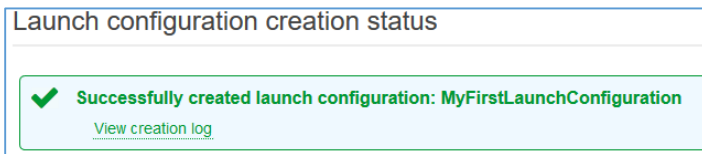
Click **Next: Configure Security Group**

Select existing Security group or create new security group, as you are wish, (Selecting existing would be good)

Click **Review**

Click Create Launch Configuration

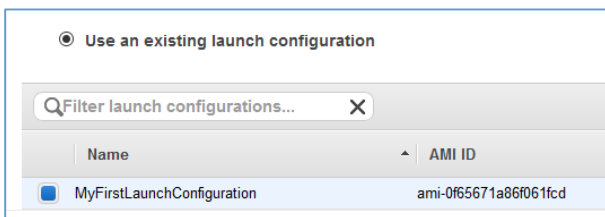
Select the Key Pair or create key pair



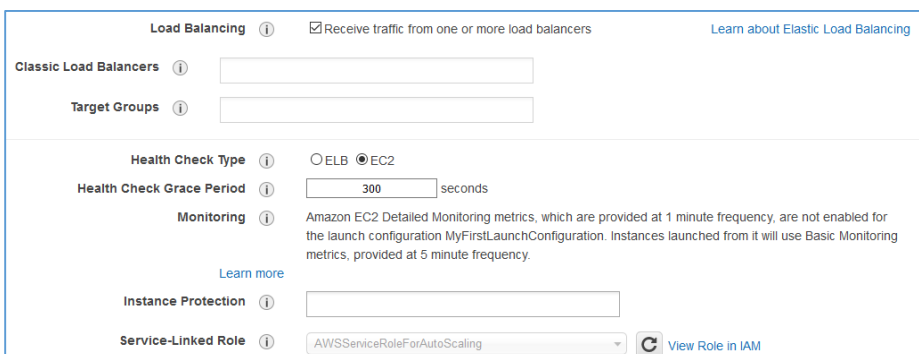
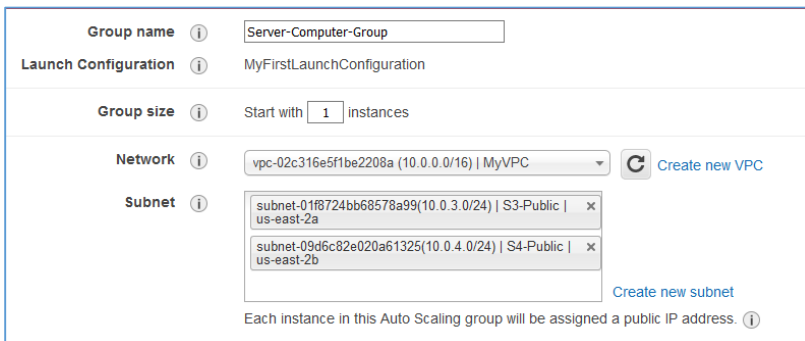
Launch configuration created successfully. Click **Close**

19.2. Auto Scaling Groups

Select Auto Scaling Groups → Create Auto Scaling Group → Select Launch Configuration



Click **Next Step**



If you are auto-scaling group, want load balancer you can add ELB to auto scaling group

Click **Next: Configure Scaling Policies**

☐ Keep this group at its initial size

☒ Use scaling policies to adjust the capacity of this group

If you do not want to create scaling policy, select first radio button otherwise select use scaling policies button

Below are the conditions you can use for auto scaling EC2 instances

CPU Utilization

CPU Utilization

Disk Reads

Disk Read Operations

Disk Writes

Disk Write Operations

Network In

Network Out

Create Alarm

You can use CloudWatch alarms to be notified automatically whenever metric data reaches a level you define.
To edit an alarm, first choose whom to notify and then define when the notification should be sent.

☐ Send a notification to: No SNS topics found...

Whenever: Average of CPU Utilization

Is: >= 60 Percent

For at least: 1 consecutive period(s) of 5 Minutes

Name of alarm: awssec2-Server-Computer-Group-CPU-Utilizati

CPU Utilization Percent

60

40

20

0

12/12 04:00 12/12 06:00 12/12 08:00

Server-Computer-Group

Cancel Create Alarm

Created Auto increase group IF CPU Utilization is Greater than or equal to 60 for 5minutes add new EC2 instance to auto scaling group

Create Alarm

You can use CloudWatch alarms to be notified automatically whenever metric data reaches a level you define.
To edit an alarm, first choose whom to notify and then define when the notification should be sent.

☐ Send a notification to: No SNS topics found...

Whenever: Average of CPU Utilization

Is: <= 20 Percent

For at least: 1 consecutive period(s) of 5 Minutes

Name of alarm: awssec2-Server-Computer-Group-High-CPU-UT

CPU Utilization Percent

20

15

10

5

0

12/12 04:00 12/12 06:00 12/12 08:00

Server-Computer-Group

Cancel Create Alarm

Create auto decrease group IF CPU Utilization is less than or equal to 20 for 5 minutes remove on EC2 instance from scaling group

Increase Group Size

Name:

Execute policy when: [awsec2-Server-Computer-Group-CPU-Utilization](#) [Edit](#) [Remove](#)
breaches the alarm threshold: CPUUtilization >= 60 for 300 seconds
for the metric dimensions AutoScalingGroupName = Server-Computer-Group

Take the action: when <= CPUUtilization < +infinity
[Add step](#) [i](#)

Instances need: seconds to warm up after each step

[Create a simple scaling policy](#) [i](#)

Decrease Group Size

Name:

Execute policy when: [awsec2-Server-Computer-Group-High-CPU-Utilization](#) [Edit](#) [Remove](#)
breaches the alarm threshold: CPUUtilization <= 20 for 300 seconds
for the metric dimensions AutoScalingGroupName = Server-Computer-Group

Take the action: when >= CPUUtilization > -infinity
[Add step](#) [i](#)

Click **Next: Configure Notifications**

If you want notifications when auto scale triggers create notification

Send a notification to: [use existing topic](#)

With these recipients:

Whenever instances:

- ☒ launch
- ☒ terminate
- ☒ fail to launch
- ☒ fail to terminate

Click **Next: Configure Tags**

Add tags for recognizing auto scale instances

Click **review**

Click **Create Auto Scaling Group**

✓ **Successfully created Auto Scaling group**

[View creation log](#)

Now go back to instances you would see EC2 instances launched by auto scaling group configuration.

In order to create a CPU load to test auto scaling use below scripts

```
while true; do true; done &  
dd if=/dev/zero of=/dev/null &
```

Execute above scripts multiple times in your EC2 instances, to create CPU Load is more than 60 percent for 5 minutes it will automatically launch another EC2 instance.

Wait for 5 Minutes and see

To scale down identify the background running jobs and kill them

```
jobs  
fg <Job Number>  
CTRL + C
```

OR

```
ps -aux |grep dd |awk '{print $2}' | xargs kill -9  
ps -aux |grep bash |awk '{print $2}' | xargs kill -9
```

OR

```
kill -9 <PID>
```

Wait for 5 minutes EC2 instances will be terminated automatically which are launched using auto scale option.

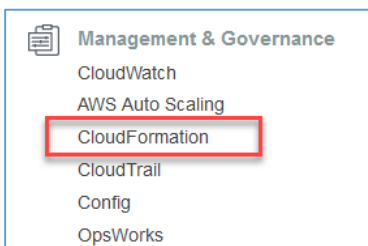
20. ClodFormation

AWS CloudFormation provides a common language for you to describe and provision all the infrastructure resources in your cloud environment. CloudFormation allows you to use a simple text file to model and provision, in an automated and secure manner, all the resources needed for your applications across all regions and accounts. This file serves as the single source of truth for your cloud environment.

AWS CloudFormation is available at no additional charge, and you pay only for the AWS resources needed to run your applications.

“Cloud Infrastructure as Code”

Login to **AWS Web console** → **Services**



Create Stack

Specify Details

Specify a stack name and parameter values. You can use or change the default parameter values, which are defined in the AWS CloudFormation template. [Learn more.](#)

Stack name www.server-computer.com

Parameters

InstanceType WebServer EC2 instance type

KeyName Name of an existing EC2 KeyPair to enable SSH access to the instances

SSHLocation The IP address range that can be used to SSH to the EC2 instances

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

<https://github.com/techtutorials/aws-lab-guide/blob/aws/LaunchEC2WebServer.template>

Download and upload the template file Click **Next**

Tags

You can specify tags (key-value pairs) for resources in your stack. You can add up to 50 unique key-value pairs for each stack. [Learn more.](#)

	Key (127 characters maximum)	Value (255 characters maximum)
1	Purpose	WebServer
2	ENV	Dev/Test

Add Tags

Termination Protection ☐ Enabled ☒ Disabled

Timeout Minutes

Rollback on failure ☒ Yes ☐ No

Stack policy ☐ Enter policy
☒ Upload policy file
 No file selected. [Learn more](#)

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

Click **Next**

Click on **Create**

It will create S3 bucket for CF template store and keeps your ClouFormation templates in it

If you delete ClouFormation, it will automatically delete associate stack/resources

21. Amazon FSx

Amazon FSx provides fully managed third-party file systems. Amazon FSx provides you with the native compatibility of third-party file systems with feature sets for workloads such as Windows-based storage, high-performance computing

(HPC), machine learning, and electronic design automation (EDA). You don't have to worry about managing file servers and storage, as Amazon FSx automates the time-consuming administration tasks such as hardware provisioning, software configuration, patching, and backups. Amazon FSx integrates the file systems with cloud-native AWS services, making them even more useful for a broader set of workloads.

Services → Storage → FSx → Create File system

File system options www.server-computer.com

☒ Amazon FSx for Windows File Server

Amazon FSx
for Windows File Server

☐ Amazon FSx for Lustre

Amazon FSx
for Lustre

Note: If you're looking for HPC High Performance computer then select FSX for Lustre

Click **Next**

File System name

Minimum 300GB and Max 65536GB

Default throughput 8MB/s you can also select different values of throughput

Select Network & Security

- ✓ VPC
- ✓ AZ
- ✓ Subnet
- ✓ Security Group

Windows Authentication

Note: Must be active directory or create new active directory in AWS

Encryption

Maintenance preferences

Select backup window time

Click **Next**

22. SQS – Simple Queue Service

Amazon SQS provides several advantages over building your own software for managing message queues or using commercial or open-source message queuing systems that require significant up-front time for development and configuration.

These alternatives require ongoing hardware maintenance and system administration resources. The complexity of configuring and managing these systems is compounded by the need for redundant storage of messages that ensures messages are not lost if hardware fails.

What can be used to communicate between components?

- ✓ Amazon Simple Queue Service (SQS)

Standard Queue

- At-Least-Once Delivery
- Best-Effort-Ordering

FIFO Queue

- Exactly-Once Processing
 - Duplicates are not introduced
- Limited Throughput
 - Up to 300 send, receive, delete per second

Services → Application Integration → Simple Queue Service



Application Integration

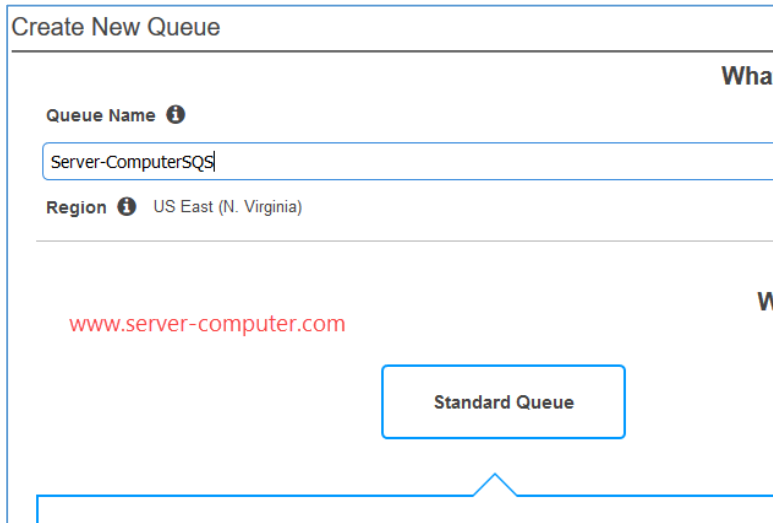
Step Functions

Amazon MQ

Simple Notification Service

Simple Queue Service

SWF



Create New Queue

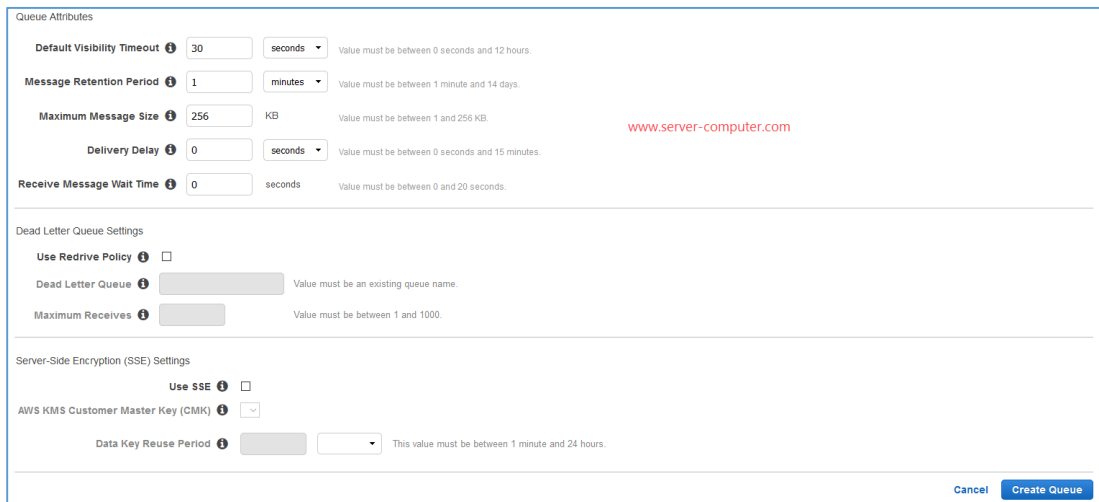
Queue Name ⓘ Server-ComputerSQS

Region ⓘ US East (N. Virginia)

www.server-computer.com

Standard Queue

Provide queue name and Click **Configure Queue**



Queue Attributes

Default Visibility Timeout ⓘ 30 seconds Value must be between 0 seconds and 12 hours.

Message Retention Period ⓘ 1 minutes Value must be between 1 minute and 14 days.

Maximum Message Size ⓘ 256 KB Value must be between 1 and 256 KB.

Delivery Delay ⓘ 0 seconds Value must be between 0 seconds and 15 minutes.

Receive Message Wait Time ⓘ 0 seconds Value must be between 0 and 20 seconds.

Dead Letter Queue Settings

Use Redrive Policy ⓘ ☐

Dead Letter Queue ⓘ Value must be an existing queue name.

Maximum Receives ⓘ Value must be between 1 and 1000.

Server-Side Encryption (SSE) Settings

Use SSE ⓘ ☐

AWS KMS Customer Master Key (CMK) ⓘ

Data Key Reuse Period ⓘ This value must be between 1 minute and 24 hours.

Cancel Create Queue

Click **Create Queue**

New queue created successfully. Now send message and poll to see the message queue

Select newly created queue name and Actions → send message

Write the message in message box example is shown in below screenshot Click **Send Message**

Send a Message to Server-ComputerSQS

Message Body Message Attributes

Enter the text of a message you want to send.

Hi Testing Message from SQS server-computer.com

☐ Delay delivery of this message by 0 seconds (up to 15 minutes).

Cancel Send Message

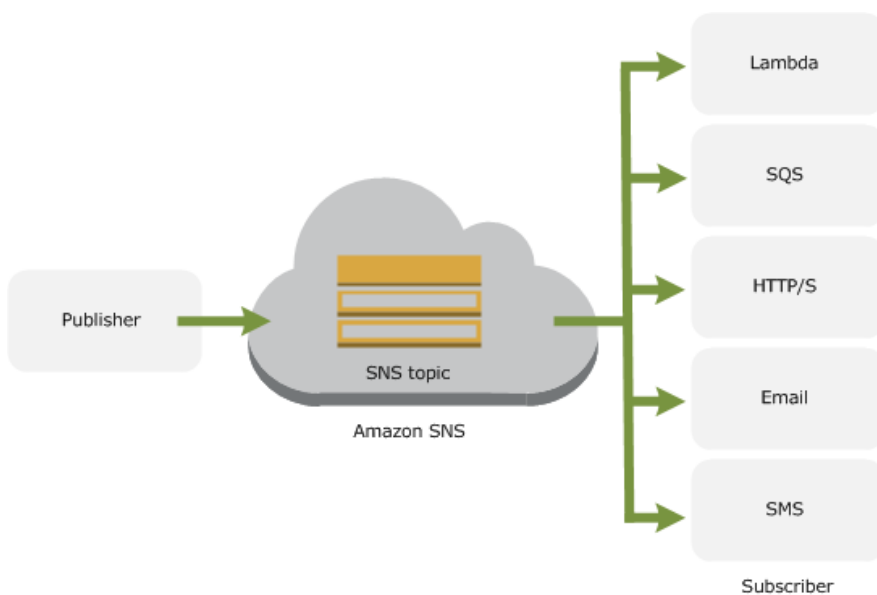
Close the popup window, select queue name **Actions** → **View/Delete messages** → **start polling for messages**

Delete	Body	Size	Sent	Receive Count	
☐	Hi Testing message from SQS server-computer.com	47 bytes	2018-12-19 14:28:06 GMT+05:30	1	More Details

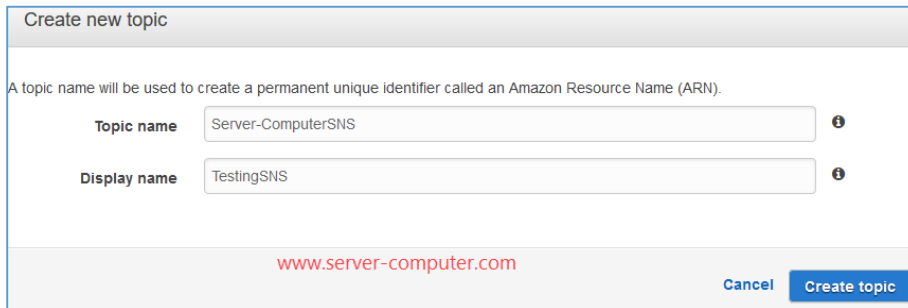
This scenario is only for testing SQS or practicing SQS. If you know use case or project, where you can integrate SQS try

23. SNS – Simple Notification Service

Amazon Simple Notification Service (Amazon SNS) is a web service that coordinates and manages the delivery or sending of messages to subscribing endpoints or clients. In Amazon SNS, there are two types of clients—publishers and subscribers—also referred to as producers and consumers. Publishers communicate asynchronously with subscribers by producing and sending a message to a topic, which is a logical access point and communication channel. Subscribers (i.e., web servers, email addresses, Amazon SQS queues, AWS Lambda functions) consume or receive the message or notification over one of the supported protocols (i.e., Amazon SQS, HTTP/S, email, SMS, Lambda) when they are subscribed to the topic.



Services → Simple Notification Service → Create topic



Create new topic

A topic name will be used to create a permanent unique identifier called an Amazon Resource Name (ARN).

Topic name

Display name

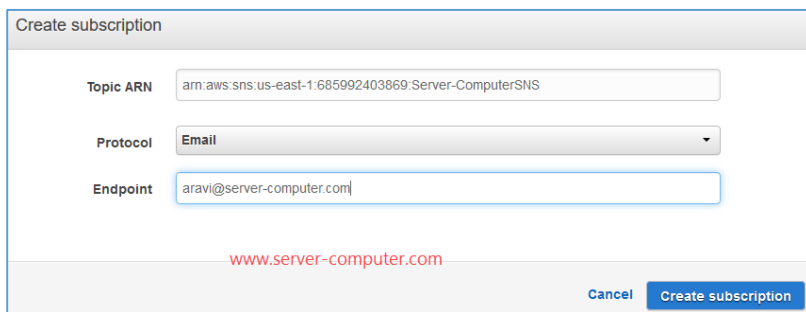
www.server-computer.com

[Cancel](#) [Create topic](#)

Click **Create Topic**

Topic created successfully. Click on topic

Create subscription



Create subscription

Topic ARN

Protocol

Endpoint

www.server-computer.com

[Cancel](#) [Create subscription](#)

Subscription will send an email for verification after verification you will see subscription ID

Click **Publish to Topic**

Write Subject and Message body click publish

All the subscribers will receive email immediately

Will do Flow as **SNS → SQS → Lambda function**

Go to SQS and provide permissions to SNS to send notifications using ARN value

Select SQS Queue and add permissions

Add a Permission to Server-ComputerSQS

Permissions enable you to control which operations a user can perform on a queue. [Click here](#) to learn more about access control concepts.

Effect ☒ Allow www.server-computer.com
☐ Deny

Principal ☒ Everybody (*)

Use commas between multiple values.

Actions --- 1 Specific Action --- ☐ All SQS Actions (SQS:*)

- ☐ AddPermission
- ☐ ChangeMessageVisibility
- ☐ DeleteMessage
- ☐ DeleteQueue
- ☐ GetQueueAttributes
- ☐ GetQueueUrl
- ☐ ListDeadLetterSourceQueues
- ☐ PurgeQueue
- ☒ ReceiveMessage
- ☐ RemovePermission
- ☐ SendMessage
- ☐ SetQueueAttributes

Cancel Add Permission

Copy the ARN value from Details tab on SQS

arn:aws:sqs:us-east-1:585692493869:Server-ComputerSQS

Change back to SNS and create Subscription under topic

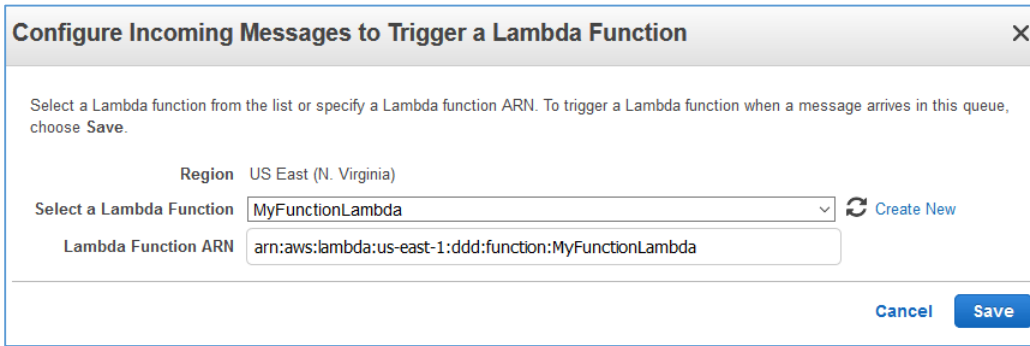
- ✓ Topic ARN : Autofil
- ✓ Protocol: Amazon SQS
- ✓ EndPoint: ARN Value copied from SQS

Send topic

Go back to SQS and View/Delete Messages → Start polling messages you can see the message from SNS

Similar to this create Lambda function, get ARN value from Lambda, and add to SQS for further triggers

Queue Actions → configure Trigger for Lambda Function



Configure Incoming Messages to Trigger a Lambda Function [X]

Select a Lambda function from the list or specify a Lambda function ARN. To trigger a Lambda function when a message arrives in this queue, choose **Save**.

Region: US East (N. Virginia)

Select a Lambda Function: [Create New](#)

Lambda Function ARN:

Cancel **Save**

Go back to SNS and publish to topic

As soon as SNS trigs SQS will send message after words lambda will execute the defined function.

24. AWS CLI

The AWS Command Line Interface (CLI) is a unified tool to manage your AWS services. With just one tool to download and configure, you can control multiple AWS services from the command line and automate them through scripts. The AWS CLI introduces a new set of simple file commands for efficient file transfers to and from Amazon S3.

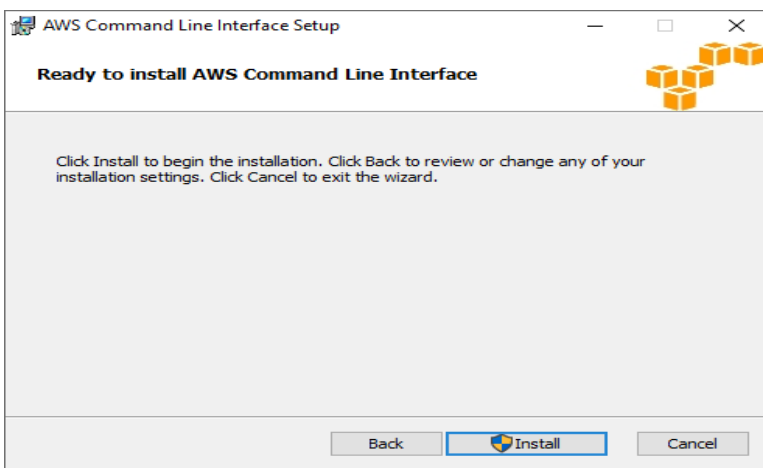
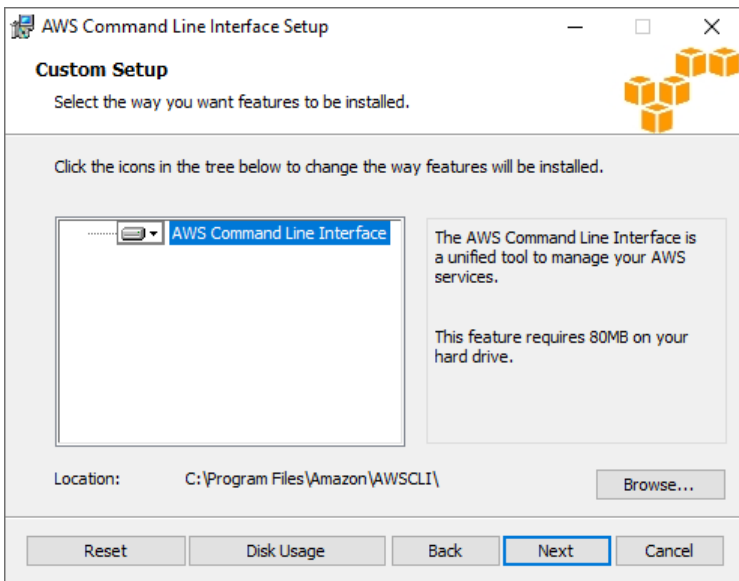
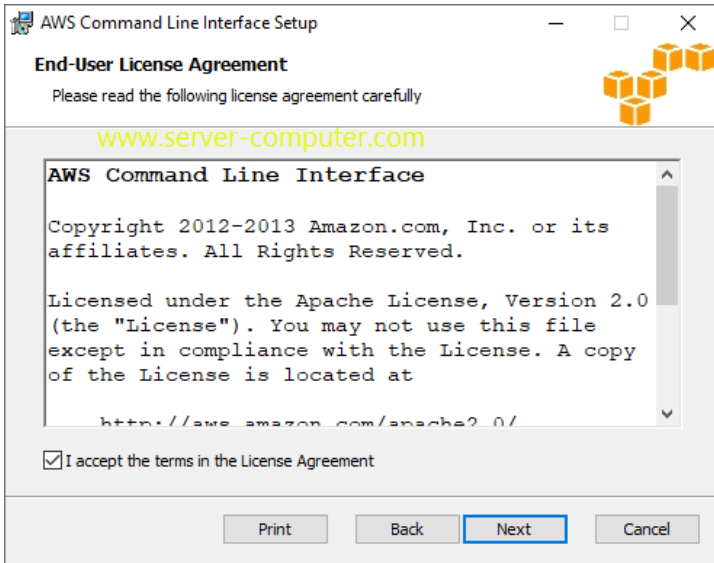
[Aws cli configuration for Linux](#)

[Download AWS CLI for Windows 64 Bit](#)

You should require administrator privileges to install this package in windows machine

Double click on .msi file





Click **Install**

Click **Finish**

Login back to AWS Management console and create user with programmatic access **Refer Topic 5 download** ACCESS Key and secret key

Start Menu → Run → cmd

cd C:\Program Files\Amazon\AWSCLI\bin

Change your directory path to above mentioned

>aws configure

```
C:\Program Files\Amazon\AWSCLI\bin>aws configure
AWS Access Key ID [*****ULVQ]:
AWS Secret Access Key [*****XhN2]:
Default region name [ap-south-1]:
Default output format [None]:
```

Now successfully installed and configure aws cli, run few aws cli commands to manage AWS infrastructure

```
C:\Program Files\Amazon\AWSCLI\bin>aws s3 mb s3://servercomputerbucket
make_bucket: servercomputerbucket

C:\Program Files\Amazon\AWSCLI\bin>aws s3 ls
2018-12-18 08:31:47 arkit-test123
2018-12-20 16:57:01 servercomputerbucket

C:\Program Files\Amazon\AWSCLI\bin>aws s3 cp D:\Red_Hat_Enterprise_Linux-7-System_Administrators_Guide-en-US.pdf s3://servercomputerbucket
upload: D:\Red_Hat_Enterprise_Linux-7-System_Administrators_Guide-en-US.pdf to s3://servercomputerbucket/Red_Hat_Enterprise_Linux-7-System_Administrators_Guide-en-US.pdf

C:\Program Files\Amazon\AWSCLI\bin>aws s3 ls s3://servercomputerbucket
2018-12-20 16:58:39 25173965 Red_Hat_Enterprise_Linux-7-System_Administrators_Guide-en-US.pdf

C:\Program Files\Amazon\AWSCLI\bin>aws s3api delete-object --bucket servercomputerbucket --key Red_Hat_Enterprise_Linux-7-System_Administrators_Guide-en-US.pdf

C:\Program Files\Amazon\AWSCLI\bin>aws s3 ls s3://servercomputerbucket

C:\Program Files\Amazon\AWSCLI\bin>aws s3api delete-bucket --bucket servercomputerbucket --region ap-south-1

C:\Program Files\Amazon\AWSCLI\bin>aws s3 ls
2018-12-18 08:31:47 arkit-test123
```

Create S3 Bucket

```
Bin> aws s3 mb s3://servercomputerbucket
```

make_bucket: servercomputerbucket

List S3 buckets

```
Bin> aws s3 ls
```

2018-12-18 08:31:47 arkit-test123

2018-12-20 16:57:01 servercomputerbucket

Upload Object to S3 Bucket

```
Bin> aws s3 cp D:\Red_Hat_Enterprise_Linux-7-System_Administrators_Guide-en-US.pdf
s3://servercomputerbucket
```

upload: D:\Red_Hat_Enterprise_Linux-7-System_Administrators_Guide-en-US.pdf to
s3://servercomputerbucket/Red_Hat_Enterprise_Linux-7-System_Administrators_Guide-en-US.pdf

List Objects in S3 Bucket

```
Bin> aws s3 ls s3://servercomputerbucket
```

```
2018-12-20 16:58:39 25173965 Red_Hat_Enterprise_Linux-7-System_Administrators_Guide-en-US.pdf
```

Delete Object from S3 bucket

```
Bin> aws s3api delete-object --bucket servercomputerbucket --key  
Red_Hat_Enterprise_Linux-7-System_Administrators_Guide-en-US.pdf
```

```
Bin> aws s3 ls s3://servercomputerbucket
```

Delete S3 bucket

```
Bin> aws s3api delete-bucket --bucket servercomputerbucket --region ap-south-1
```

25. Creating EC2 Instance using AWS CLI

Before creating an EC2 instance using AWS CLI collect few details

- AMI ID
- Instance Type
- Key Name (If there is no Key Pair create one)
- Security Group ID
- Subnet ID

```
Bin> aws ec2 run-instances --image-id ami-06bcd1131b2f55803 --count 1 --instance-  
type t2.micro --key-name KEYNAME --security-group-ids sg-857f92e9 --subnet-id  
subnet-51e5592c
```

26. Few AWS Articles

- ➔ [Mount S3 Bucket in Linux using S3FS](#)
- ➔ [Use S3 Bucket as Windows Local Drive](#)
- ➔ [AWS Basic Interview Questions and Answers](#)
- ➔ [AWS Certification course Content](#)
- ➔ [List all AWS Instances from All Regions](#)
- ➔ [How To create your First Free Tier AWS Account](#)
- ➔ [AWS Add New User Accounts with SSH Access Linux Instance](#)
- ➔

27. 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
- SQS – Amazon Simple Queue Service
- SNS – Amazon Simple Notification Service
- SES – Amazon Simple Email Service
- ECR – Amazon Elastic Container Registry
- SWF – Amazon Simple Workflow Service