

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.	Creating Amazon Machine Image (AMI)	21
8.	Create your First EC2 windows instance.....	23
9.	Assigning Elastic IP Addresses to Instance (Static IP Address).....	27
10.	Launching RDS Instance	28
11.	Accessing MySQL Instance Using Workbench	36
12.	AWS S3 Bucket – (Object Storage).....	41
12.1.	AWS S3 Lifecycle Management.....	43
12.2.	S3 Bucket Replication to Cross-Region	46
12.3.	S3 Bucket Policies to control Access	47
13.	VPC – Virtual Private Cloud (isolated Network).....	48
13.1.	Create subnets	51
13.2.	Create Internet gateway and attach to VPC	52
13.3.	Create Virtual Private Gateway and Attach to VPC	52
13.4.	Create route tables and attach to subnets	53
14.	AWS Elastic Load Balancer (ELB).....	56
15.	AWS CloudTrail – Enable Governance and Auditing.....	60
15.1.	How to Create CloudTrail.....	60
16.	Athena Analytics	61
17.	AWS Services and abbreviations.....	67

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.



Networking

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



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.



Virtualization

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



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.



Backup and Recovery

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



Servers

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



Telecommunication

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



Web Applications

Web application development. web designing and web development.

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**

The screenshot shows the 'Create an AWS account' form. It has fields for Email address, Password, Confirm password, and AWS account name. The email field contains 'aravikumar48@gmail.com'. The AWS account name field contains 'Server-Computer'. Below the form is a yellow 'Continue' button. At the bottom left, there's a link to 'Sign in to an existing AWS account'. Small text at the bottom left indicates a copyright notice: '© 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**

AWS – Amazon Web Services Lab Practice Guide <https://www.server-computer.com>

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.

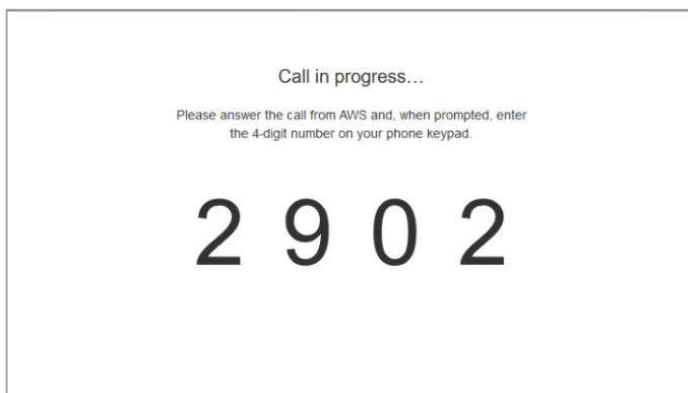
Country/Region code

Phone number Ext

Security Check


© 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**

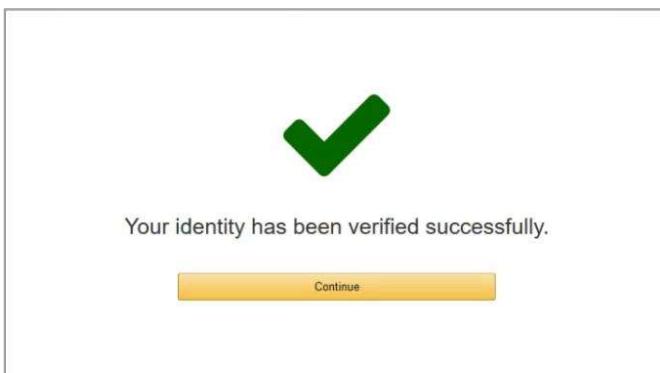


You will receive a call from AWS tele communication and ask you to enter the code displayed on screen.

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

After successful verification

AWS – Amazon Web Services Lab Practice Guide <https://www.server-computer.com>



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
<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• 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.

AWS – Amazon Web Services Lab Practice Guide <https://www.server-computer.com>

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

[AWS Console](#)



The screenshot shows the AWS sign-in page. It features the AWS logo at the top left. Below it is a "Sign in" button with a tooltip. A text input field is labeled "Email address of your AWS account" with a placeholder "Or to sign in as an IAM user, enter your account ID or account alias instead." Below the input field is a "Next" button.



The screenshot shows the "Root user sign in" page. It features the AWS logo at the top left. Below it is a "Root user sign in" button with a tooltip. There are two input fields: "Email:" and "Password". To the right of the password field is a "Forgot password?" link. Below the password field is a "Sign in" button. At the bottom of the page are links for "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, Identity & Compliance → IAM



Click on Users → Add User

AWS – Amazon Web Services Lab Practice Guide <https://www.server-computer.com>

Add user

Set user details

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

User name* * ←

[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

Set permissions

Add user to group Copy permissions from existing user Attach existing policies directly ←

[Create policy](#) ←

Filter policies ← Showing 375 results

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

Set permissions boundary

Cancel Previous ← [Next: Tags](#)

Click [Next: Tags](#)

Add tags whatever required to identify user

AWS – Amazon Web Services Lab Practice Guide <https://www.server-computer.com>

Add user

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	x
Description	Administrator for My ABC Client	x
Add new key		

You can add 48 more tags.

Cancel Previous **Next: Review**

Click **Next: Review**

Add user

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**

AWS – Amazon Web Services Lab Practice Guide <https://www.server-computer.com>

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)

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

Click on Assigned MFA Device – Manage

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

AWS – Amazon Web Services Lab Practice Guide <https://www.server-computer.com>

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

Show QR code www.server-computer.com

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](#)

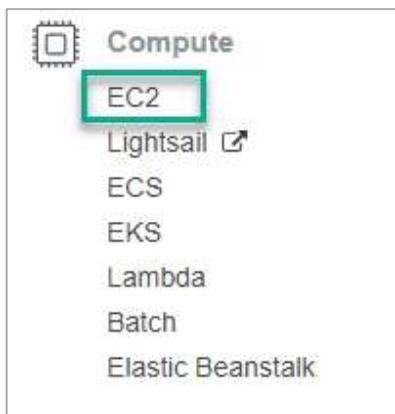
[Close](#)

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

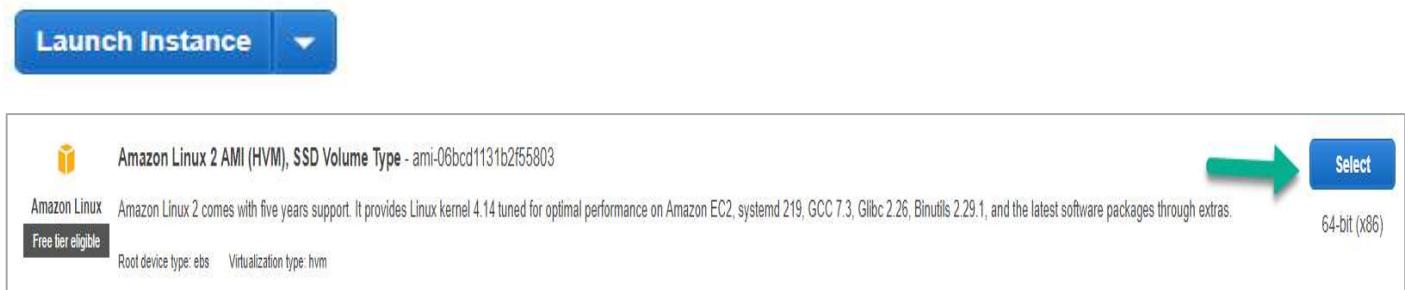
Here after if you want to login, you have to enter credentials and MFA code to Login.

6. Creating First Linux Instance

Login to AWS console, services drop down click on EC2



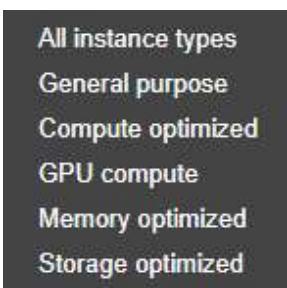
Click on Launch instance



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
<input checked="" type="checkbox"/>	General purpose	t2.micro Free tier eligible	1	1	EBS only	-	Low to Moderate	Yes

We have below types of instances



[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Configure Instance Details](#)

AWS – Amazon Web Services Lab Practice Guide <https://www.server-computer.com>

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

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

Step 4: Add Storage

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

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

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

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

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

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

AWS – Amazon Web Services Lab Practice Guide <https://www.server-computer.com>

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: launch-wizard-1

Description: launch-wizard-1 created 2018-11-22T22:00:20.022+05:30

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

Add Rule

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: server-computer

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

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

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

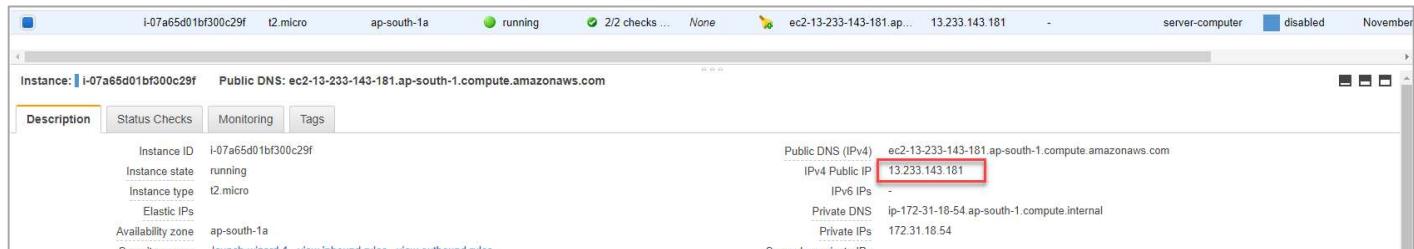
Launch Instances

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
---------------------	----------	-------------	-----------	--------------	------	--------------------------	----------------	---	-----------------	----------	----------

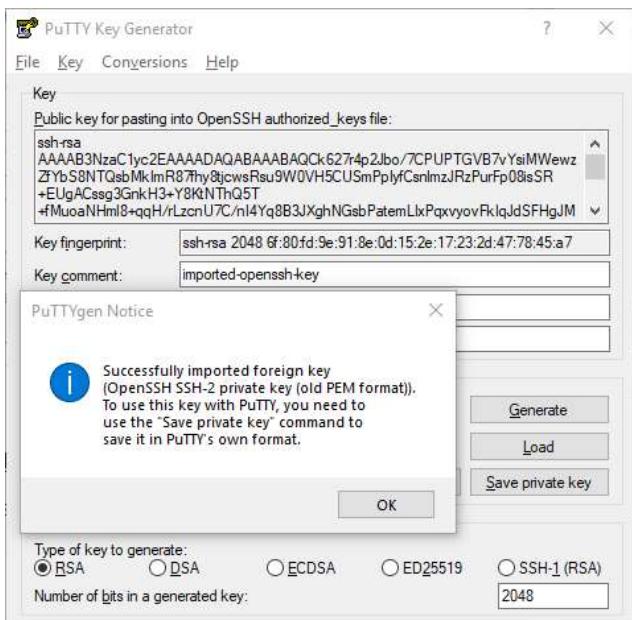
AWS – Amazon Web Services Lab Practice Guide <https://www.server-computer.com>

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

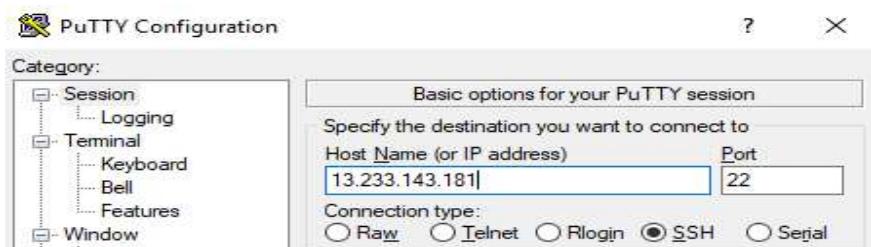


Click Ok.

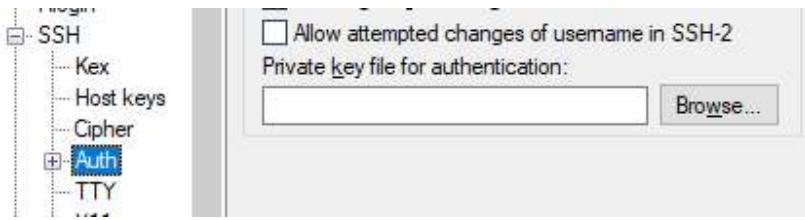
Save Private Key

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

Open putty application and type IP address as shown below



AWS – Amazon Web Services Lab Practice Guide <https://www.server-computer.com>



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

Click on Open

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

You successfully logged into your Amazon Linux instance

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

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

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



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

7. Creating Amazon Machine Image (AMI)

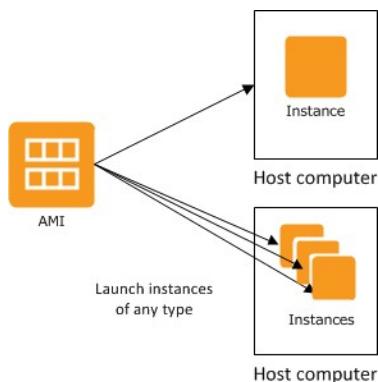
An Amazon Machine Image (AMI) provides the information required to launch an instance, which is a virtual server in the cloud. You must specify a source AMI when you launch an instance. You can launch multiple instances from a single

AWS – Amazon Web Services Lab Practice Guide <https://www.server-computer.com>

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

The screenshot shows the AWS EC2 Instances page. A context menu is open over an instance named 'New Instance' (i-0eb72a6...). The 'Image' option is highlighted with a red box, and its submenu is visible, showing 'Create Image' as the second item. The 'Create Image' dialog box is open below, titled 'Create Image'. It contains the following fields:
- Instance ID: i-0eb72a626687d8baa
- Image name: Server-Computer-AMI
- Image description: This is my Web Server Image
- No reboot:
The 'Instance Volumes' section shows a single volume:
- Volume Type: General Purpose SSD (gp2)
- Device: /dev/sda1
- Snapshot: snap-0474571d378f0fac2
- Size (GiB): 8
- Volume Type: General Purpose SSD (gp2)
- IOPS: 100 / 3000
- Throughput (MB/s): N/A
- Delete on Termination:
- Encrypted:
At the bottom of the dialog, there is a note: 'Total size of EBS Volumes: 8 GiB' and 'When you create an EBS image, an EBS snapshot will also be created for each of the above volumes.' At the very bottom are 'Cancel' and 'Create Image' buttons.

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

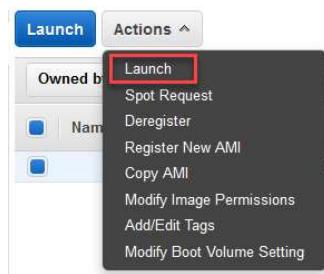
AWS – Amazon Web Services Lab Practice Guide <https://www.server-computer.com>

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

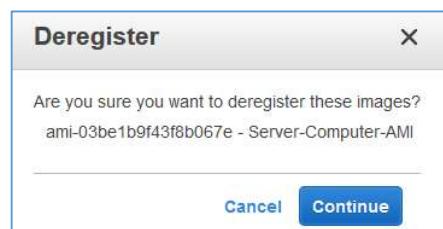
A screenshot of the 'Configure Instance Details' step in the AWS EC2 wizard. It shows network settings: Network (vpc-02c316e5f1be2208a | MyVPC), Subnet (subnet-01f8724bb68578a99 | S3-Public | us-east-2a), and Auto-assign Public IP (Enable). A 'Create new VPC' button is also visible.

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



8. Create your First EC2 windows instance

Expand services EC2 → Launch Instance



Select Windows Image

AWS – Amazon Web Services Lab Practice Guide <https://www.server-computer.com>

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 key, and more.

Number of instances	<input type="text" value="1"/>	Launch into Auto Scaling Group
Purchasing option	<input type="checkbox"/> Request Spot instances	
Network	vpc-2c747344 (default)	<input type="button" value="C Create new VPC"/>
Subnet	subnet-750b241d Default in us-east-2a 4089 IP Addresses available	<input type="button" value="Create new subnet"/>
Auto-assign Public IP	Enable	<input type="button" value="C Create new Capacity Reservation"/>
Placement group	<input type="checkbox"/> Add instance to placement group.	
Capacity Reservation	Open	<input type="button" value="C Create new Capacity Reservation"/>
Domain join directory	No directory	<input type="button" value="C Create new directory"/>
IAM role	None	<input type="button" value="C 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.

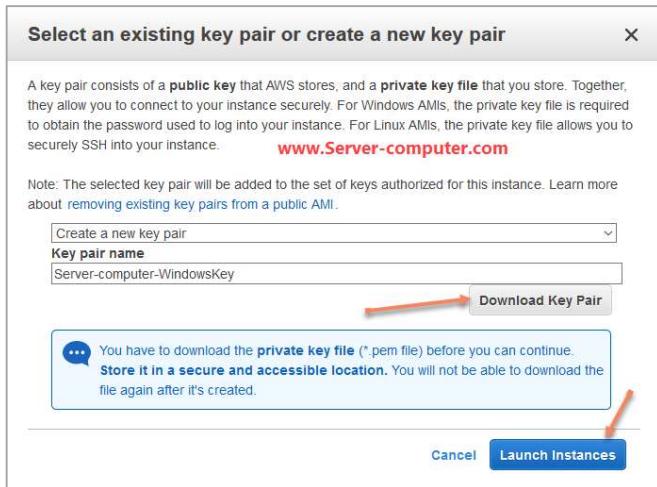
Assign a security group: Create a new security group
 Select an existing security group

Security group name:

Description:

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

Click Review and Launch



Download Key Pair and Launch Instance

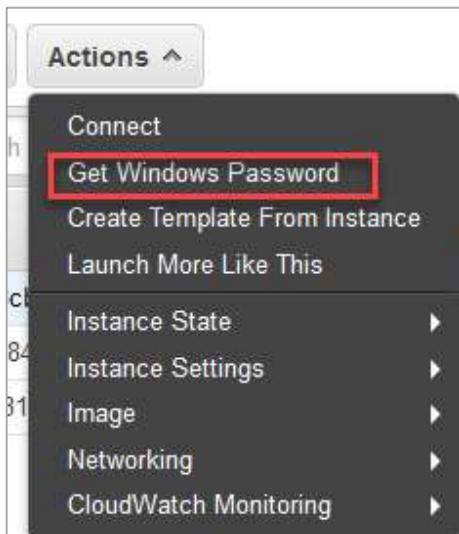
Note: Wait 4 Minutes instance to launch

It should display the following:

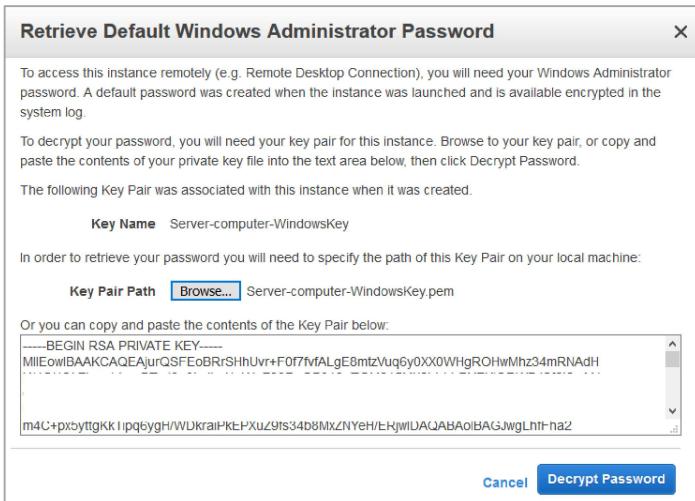
- Instance State: running
- Status Checks: 2/2 checks passed



Select instance you have launched → Actions



AWS – Amazon Web Services Lab Practice Guide <https://www.server-computer.com>



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



Now you got password successfully. Click Close.

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



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

9. 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

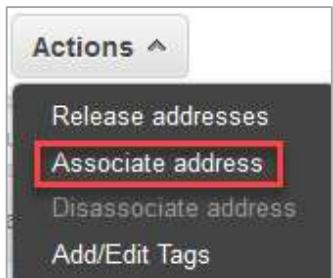


EC2 console right side bar go down → Elastic IPs → Allocate New Address

The screenshot shows the 'Allocate new address' dialog box. It includes fields for 'Scope' (set to 'VPC'), 'IPv4 address pool' (radio button selected for 'Amazon pool'), and 'Allocate' and 'Cancel' buttons. Red arrows point from the text descriptions to the corresponding UI elements.

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

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



AWS – Amazon Web Services Lab Practice Guide <https://www.server-computer.com>

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

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

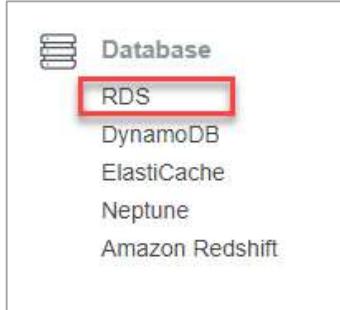
Note: If you have, multiple interfaces to the instance click on Radio button **Network Interface** and select correct NIC card name and Local IP Address.

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.

10.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

AWS – Amazon Web Services Lab Practice Guide <https://www.server-computer.com>

Engine options

Amazon Aurora
Amazon Aurora

MySQL


MariaDB


PostgreSQL


Oracle


Microsoft SQL Server


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

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

Choose use case

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

Use case

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

Production - MySQL
Use Multi-AZ Deployment and Provisioned IOPS Storage as defaults for high availability and fast, consistent performance.

Dev/Test - MySQL
This instance is intended for use outside of production or under the RDS Free Usage Tier.

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

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

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

Specify DB details

www.server-computer.com

Instance specifications

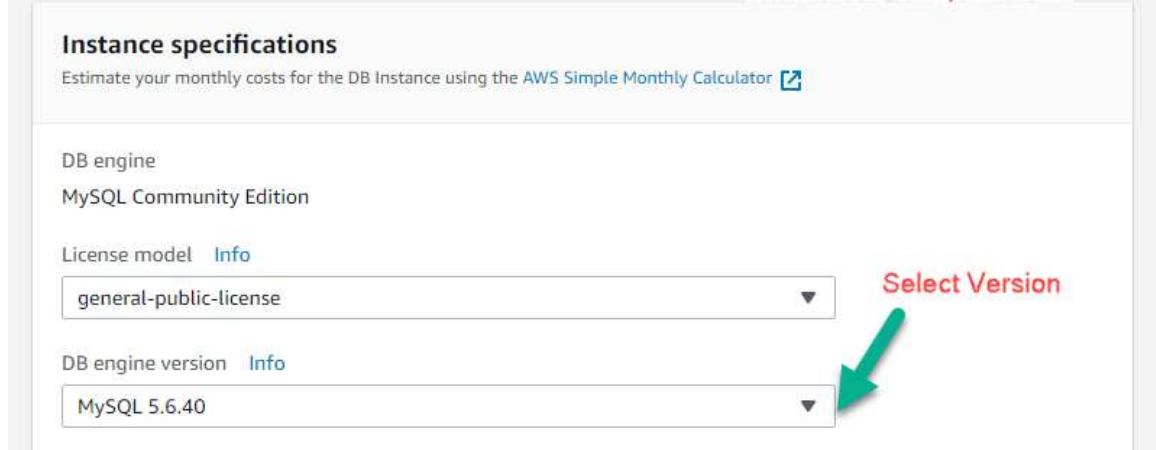
Estimate your monthly costs for the DB Instance using the [AWS Simple Monthly Calculator](#)

DB engine
MySQL Community Edition

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

DB engine version [Info](#)
MySQL 5.6.40

Select Version



In drop down, select appropriate and required MySQL Version.

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

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

Multi-AZ deployment [Info](#)
 Create replica in different zone 2
Creates a replica in a different Availability Zone (AZ) to provide data redundancy, eliminate I/O freezes, and minimize latency spikes during system backups.

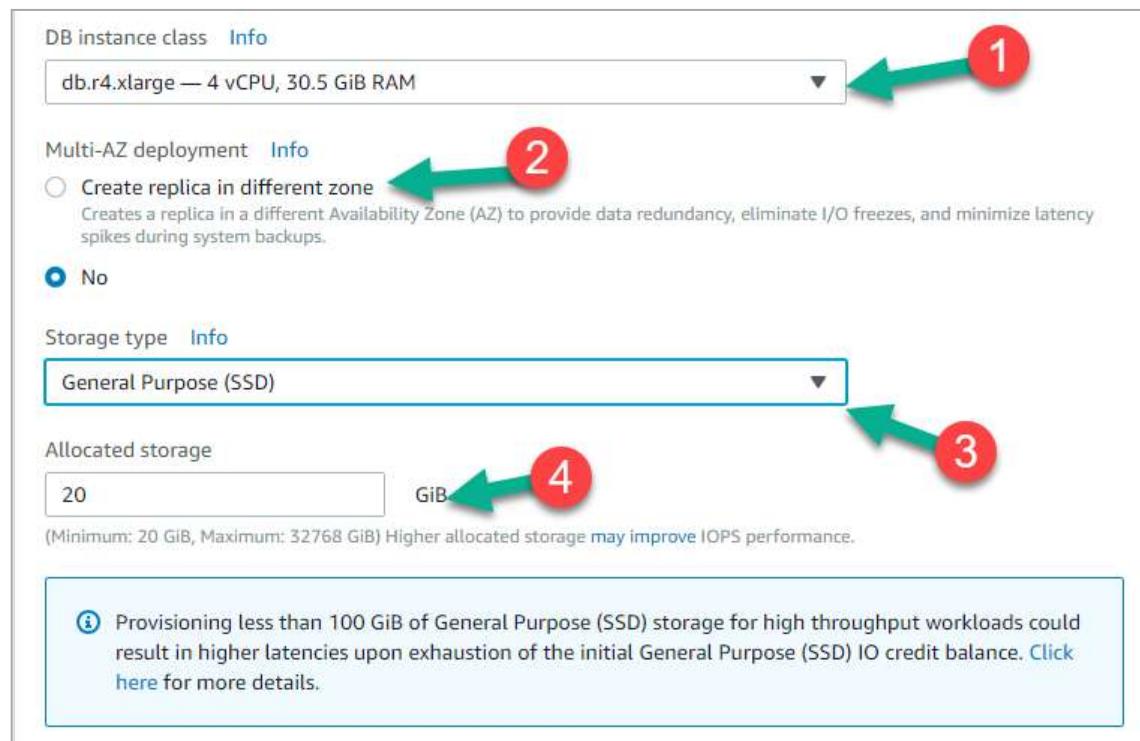
No

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

Allocated storage
20 GiB 4

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

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

AWS – Amazon Web Services Lab Practice Guide <https://www.server-computer.com>

- 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 [Info](#)
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

AWS – Amazon Web Services Lab Practice Guide <https://www.server-computer.com>

Network & Security

Virtual Private Cloud (VPC) [Info](#)
VPC defines the virtual networking environment for this DB instance.

Default VPC (vpc-cbd4f2a3) [C](#)

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 [C](#)

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 [C](#)

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.

AWS – Amazon Web Services Lab Practice Guide <https://www.server-computer.com>

For free tier encryption option is disabled

Backup

A 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

- i** 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.

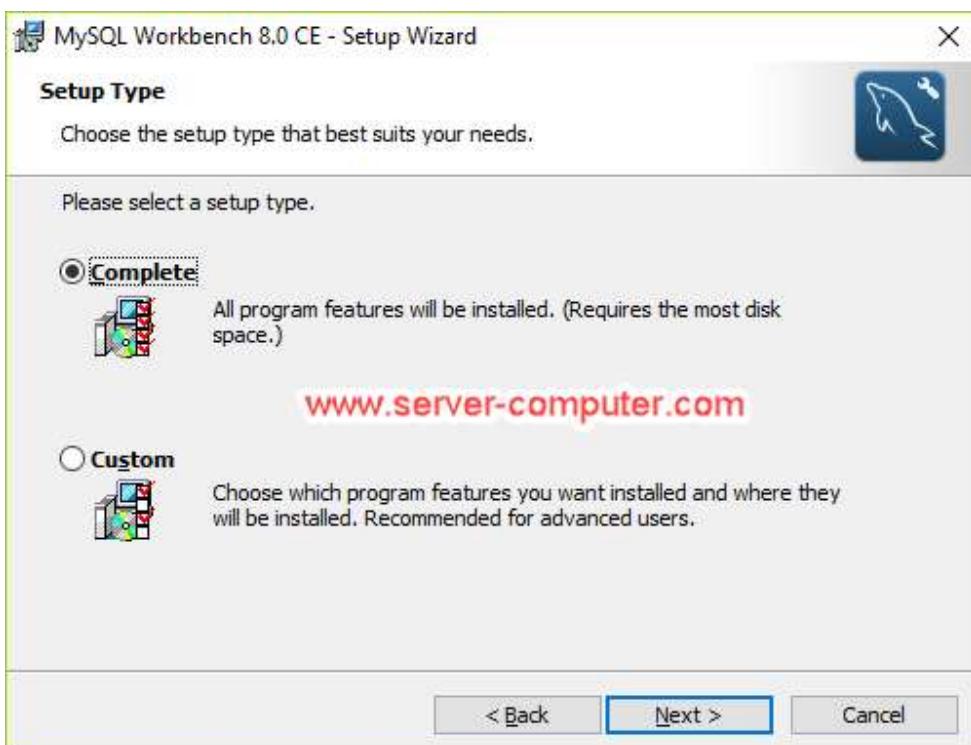
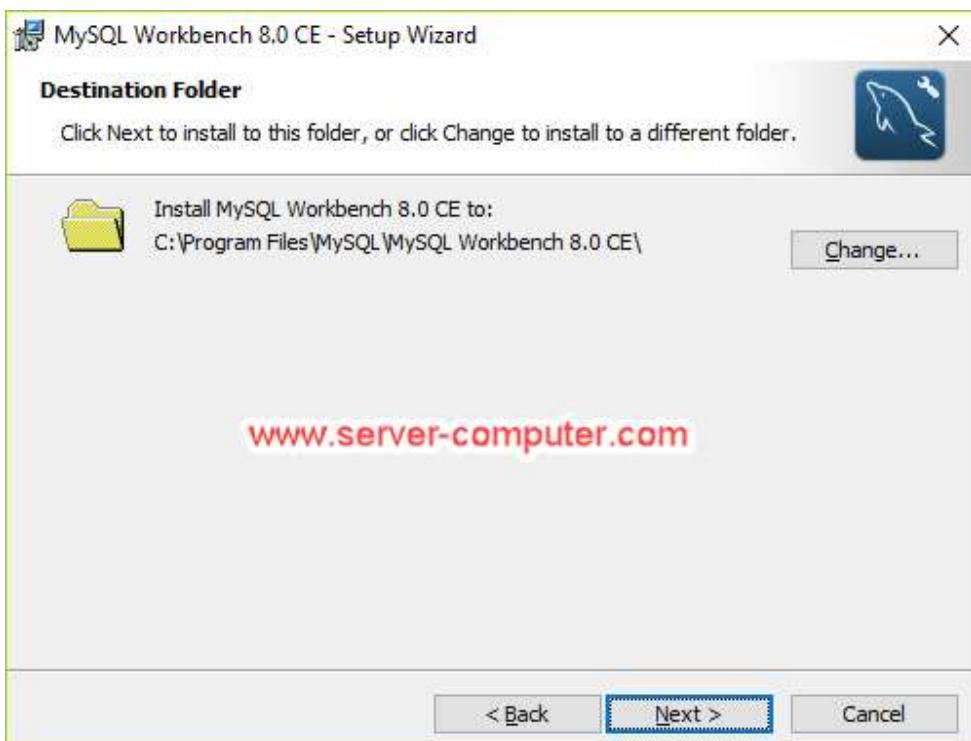
11. Accessing MySQL Instance Using Workbench

Download MySQL Workbench to access MySQL instance remotely

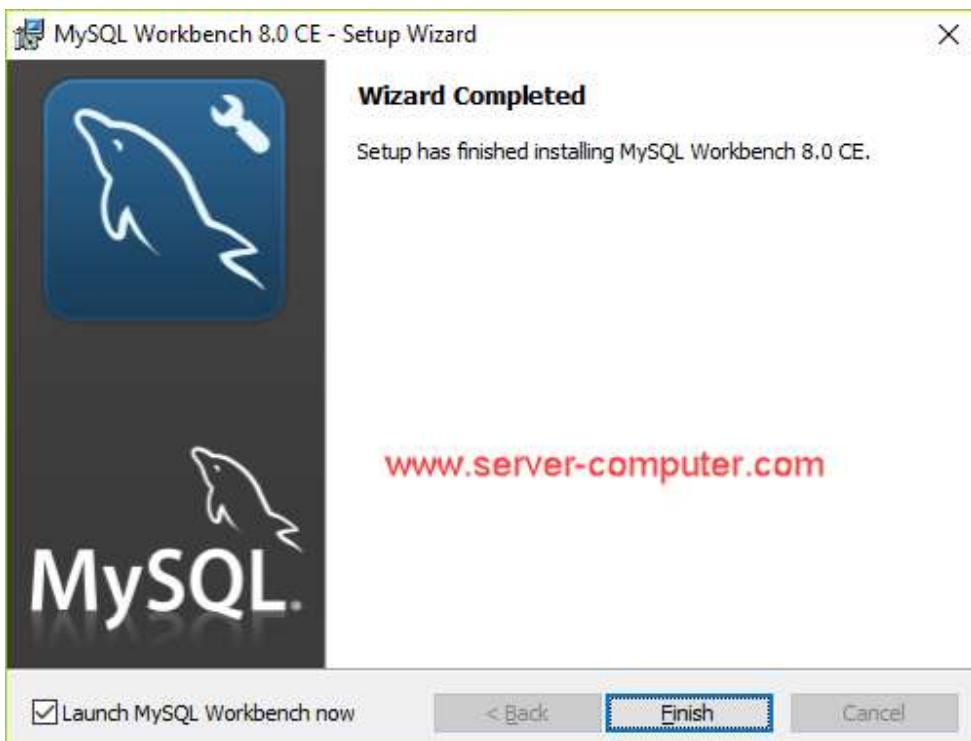
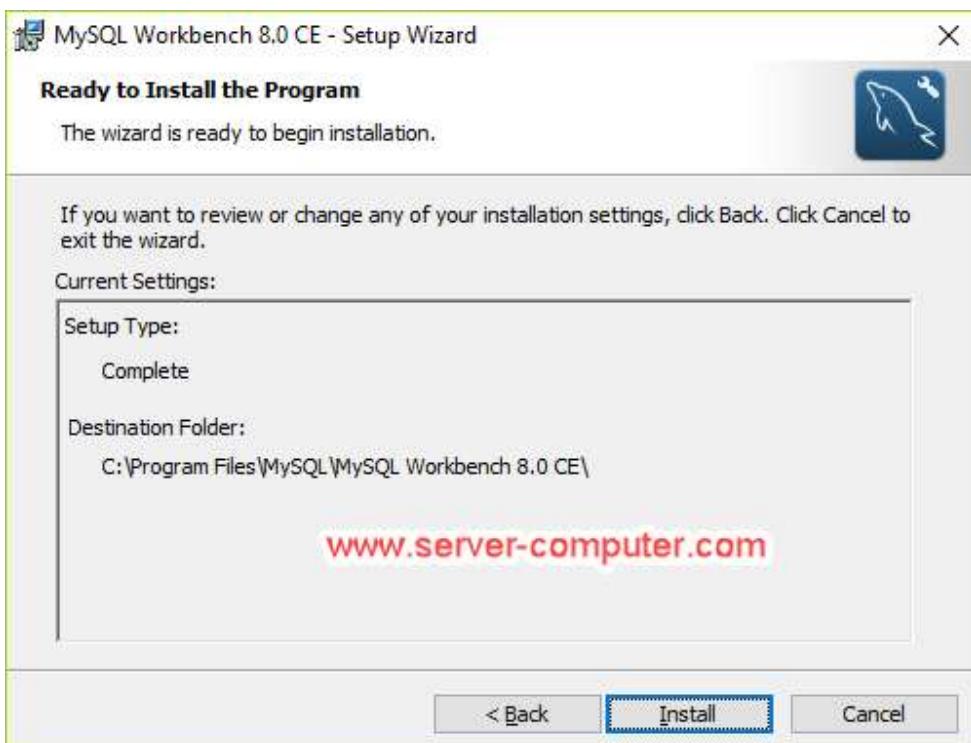
<https://dev.mysql.com/downloads/workbench/>



AWS – Amazon Web Services Lab Practice Guide <https://www.server-computer.com>



AWS – Amazon Web Services Lab Practice Guide <https://www.server-computer.com>



After successful creation you see like below

AWS – Amazon Web Services Lab Practice Guide <https://www.server-computer.com>

DB instance	▲ Engine	Status	CPU	Current activity	Maintenance	Class	VPC	Multi-AZ	Replicat
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

The dialog box for creating a new MySQL connection:

Connection Name: server-computer Type a name for the connection

Connection Method: Standard (TCP/IP) Method to use to connect to the RDBMS

Parameters SSL Advanced

Hostname: techarkitdatabase.c0lcaa1avaiz.ap-south Port: 3306 Name or IP address of the server host - and TCP/IP port.

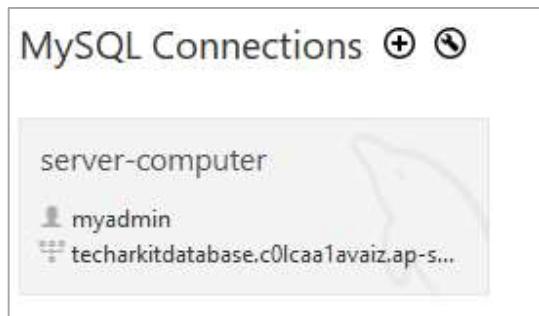
Username: myadmin Name of the user to connect with.

Password: Store in Vault ... Clear 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.

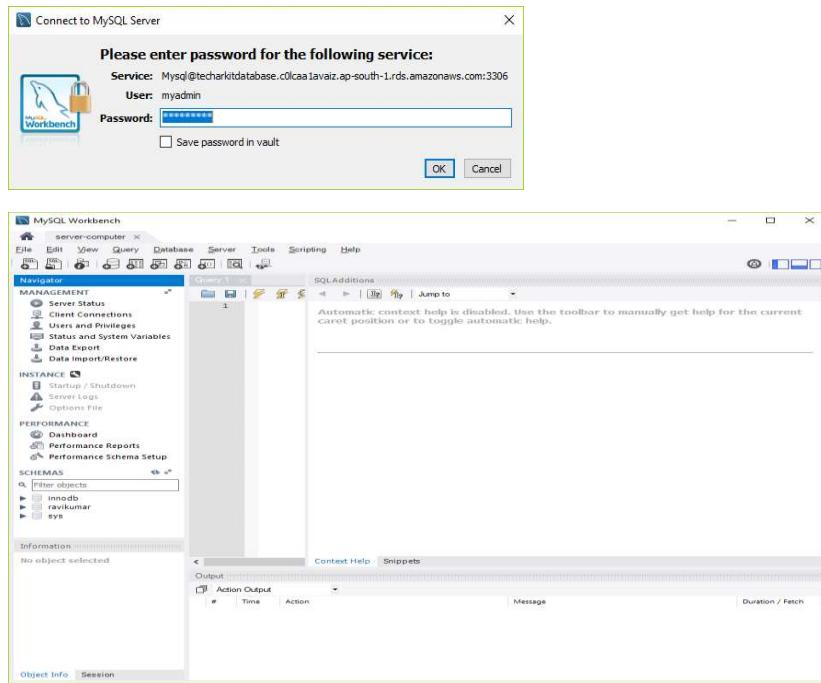
Buttons at the bottom: Configure Server Management..., Test Connection, Cancel, OK

Click **OK**



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

AWS – Amazon Web Services Lab Practice Guide <https://www.server-computer.com>



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.

AWS – Amazon Web Services Lab Practice Guide <https://www.server-computer.com>

12. 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

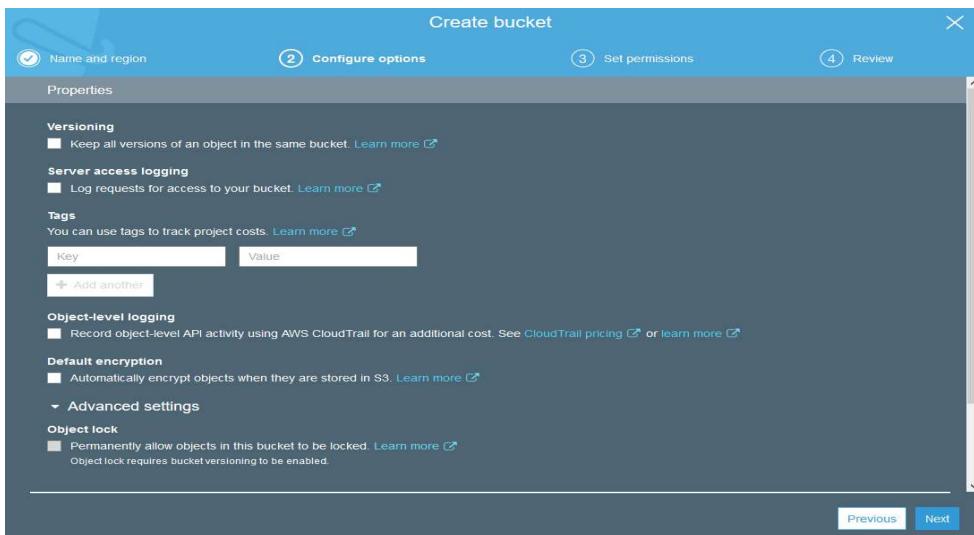
Click on

The screenshot shows the "Create bucket" wizard. Step 1: Name and region. The "Bucket name" field contains "server-computer-bucket". The "Region" dropdown is set to "Asia Pacific (Mumbai)". Below these fields is a "Copy settings from an existing bucket" section with a dropdown menu showing "Select bucket (optional) 1 Buckets". At the bottom are "Create" and "Next" buttons.

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

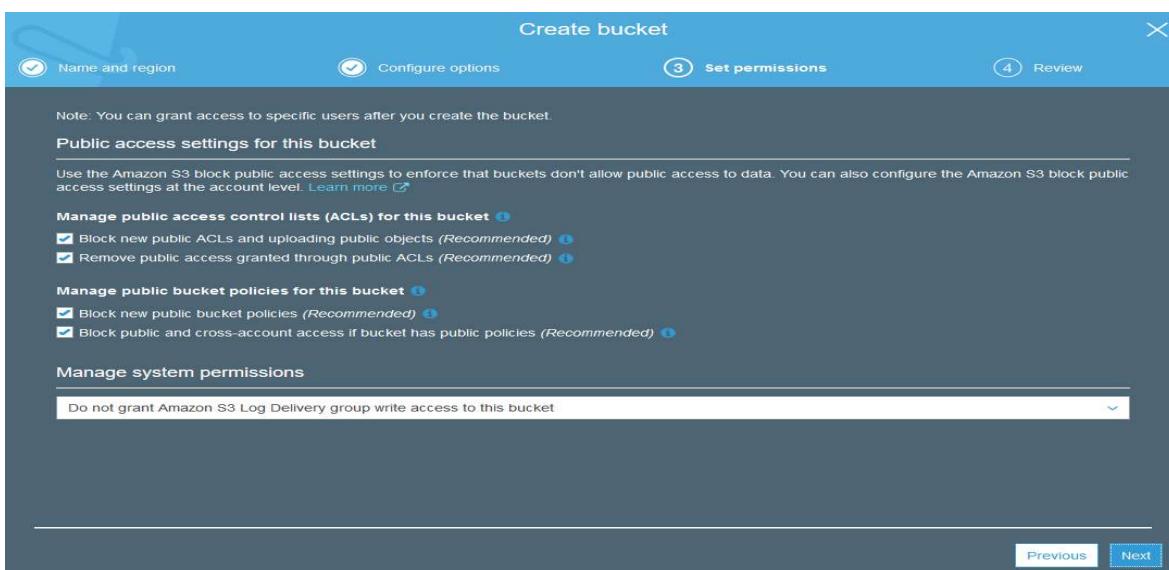
Click **Next**

AWS – Amazon Web Services Lab Practice Guide <https://www.server-computer.com>



- ⊕ **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](#)

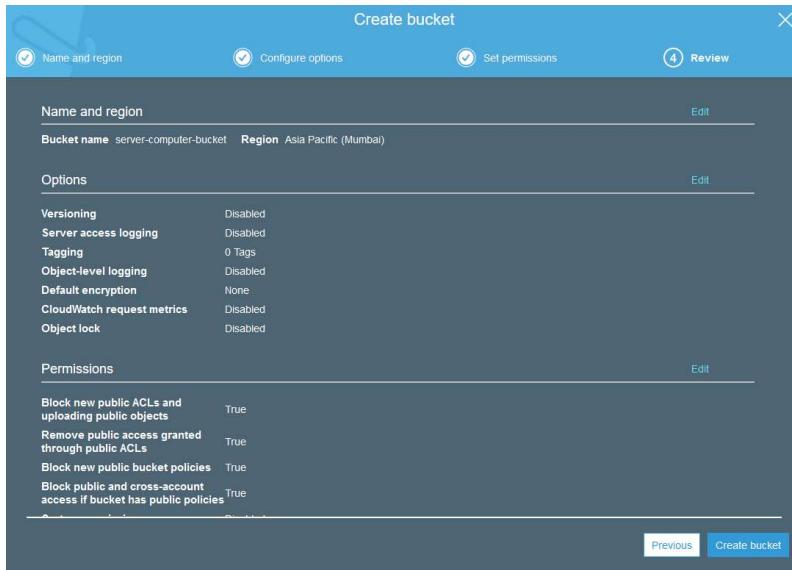


AWS recent update is to block public access by default, if you want to enable public access to your S3 bucket un-check all above tick marks.

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

AWS – Amazon Web Services Lab Practice Guide <https://www.server-computer.com>

Click **Next**



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

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

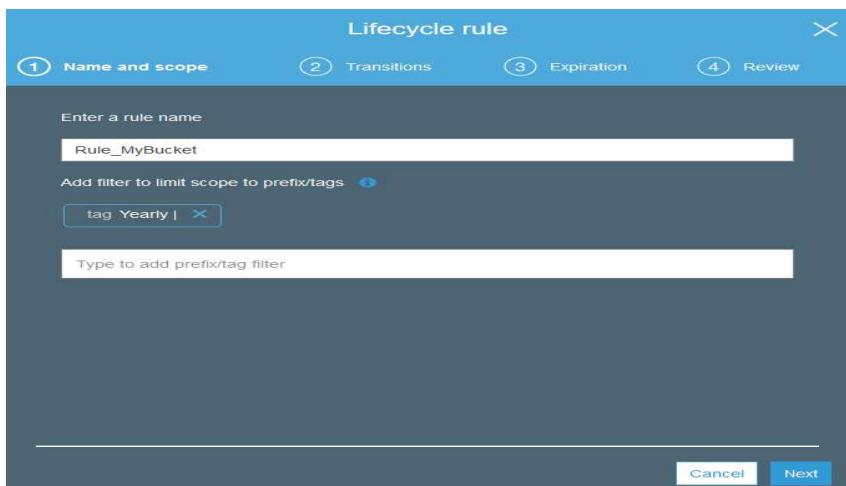
<https://s3.ap-south-1.amazonaws.com/server-computer-bucket>

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

12.1. AWS S3 Lifecycle Management

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

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



Enter Rule Name

Amazon Web Services Lab Practice Guide Prepared by www.server-computer.com – AWS Sysops Associate course • 43

AWS – Amazon Web Services Lab Practice Guide <https://www.server-computer.com>

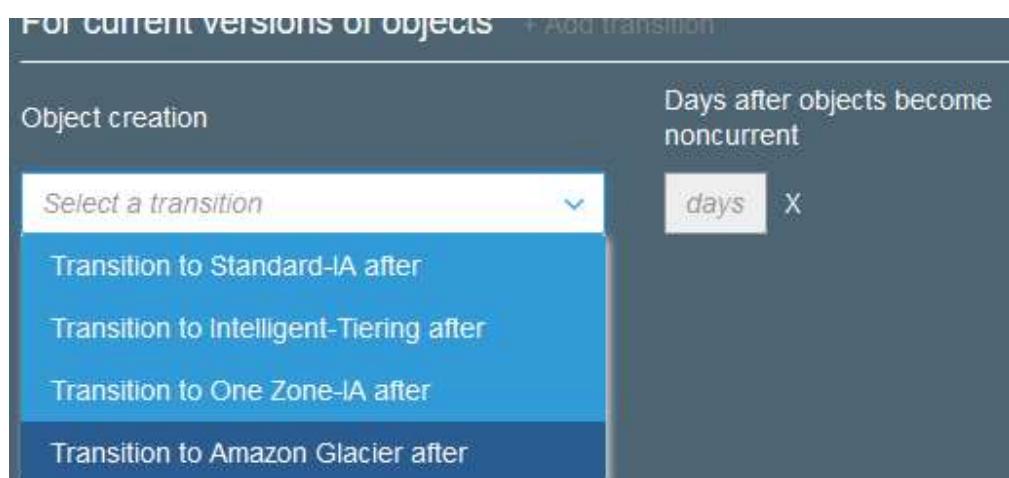
Tag Name if you do not want leave it blank

Click Next

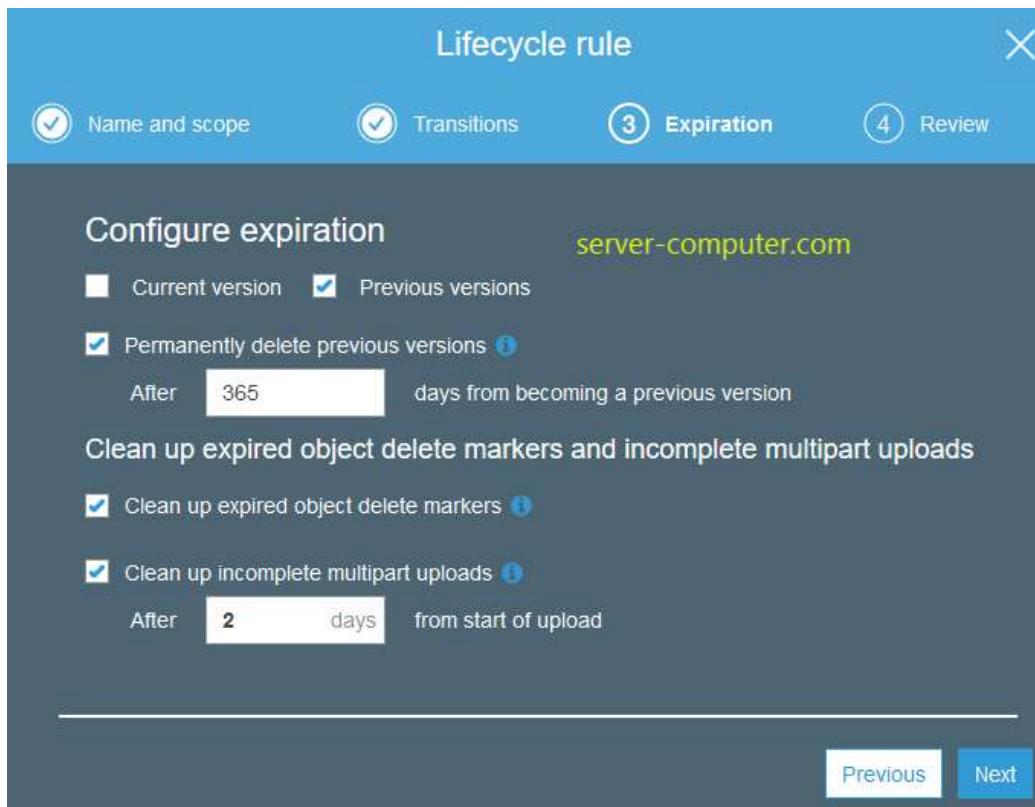


- Current Versions
- Previous Versions

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



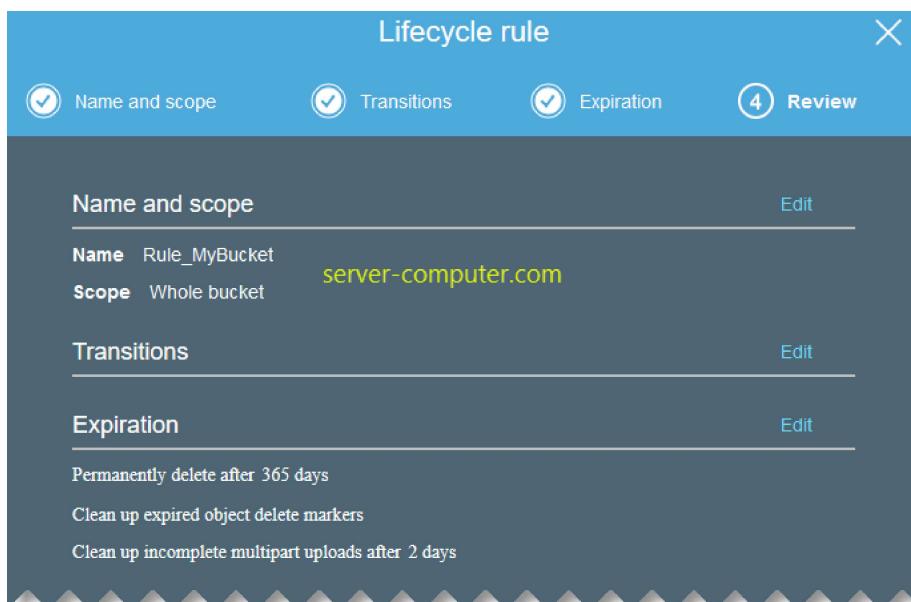
Click Next



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

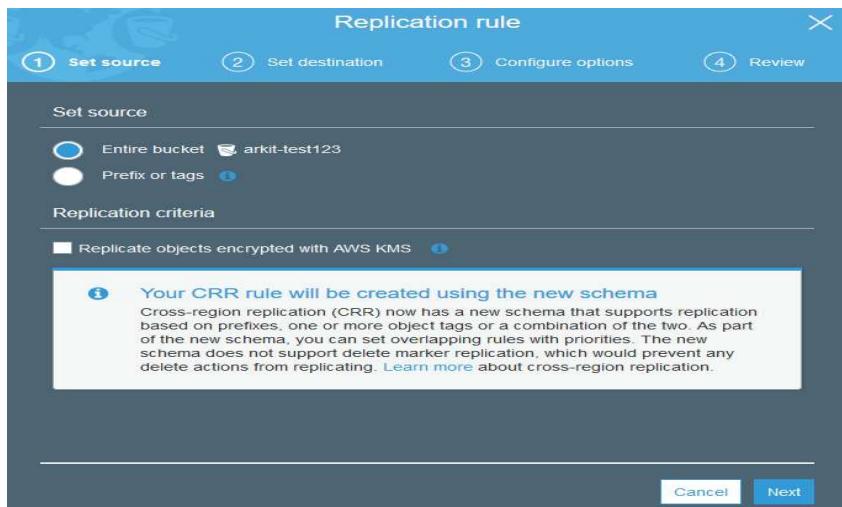


Click Save.

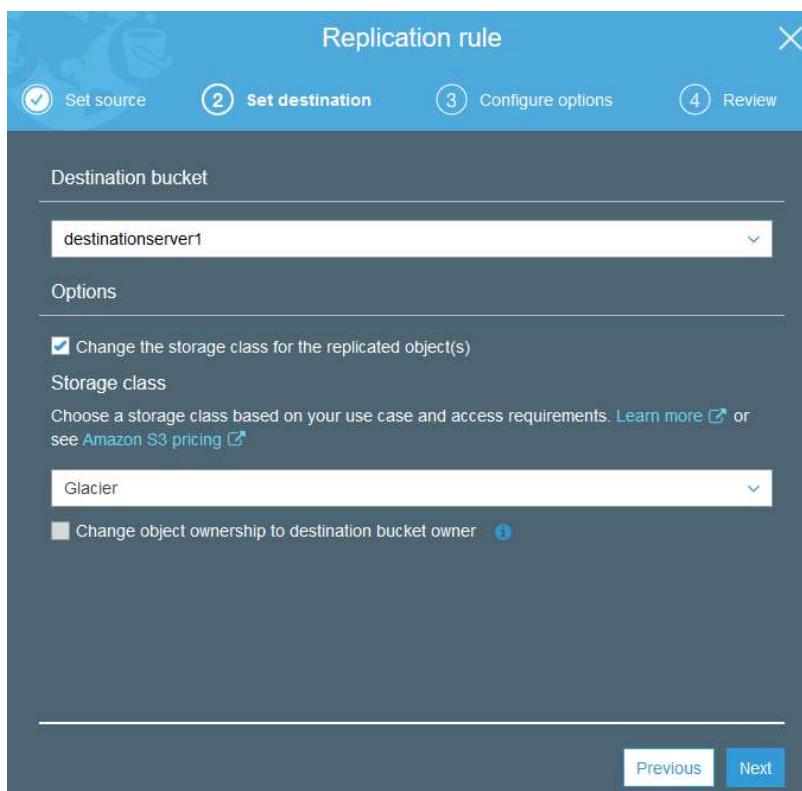
12.2. S3 Bucket Replication to Cross-Region

S3 bucket **Name → Management → Replication**

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



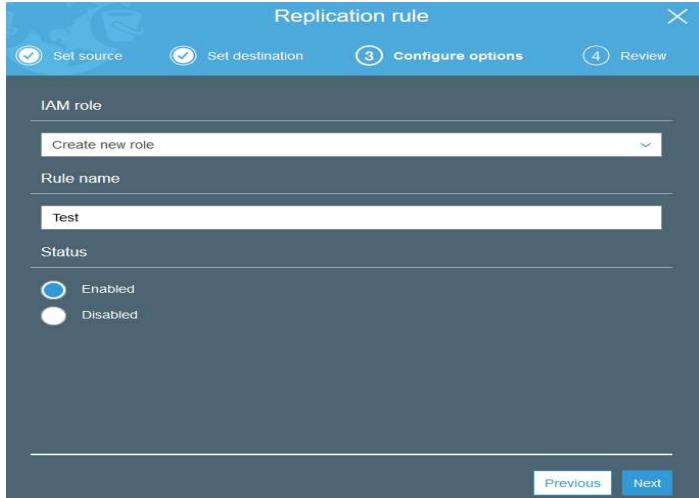
Click [Next](#)



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**

12.3. 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

AWS – Amazon Web Services Lab Practice Guide <https://www.server-computer.com>

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

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
Use a comma to separate multiple values.

AWS Service All Services ("*")
Use multiple statements to add permissions for more than one service.

Actions All Actions ("*")

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

Add Conditions (Optional)

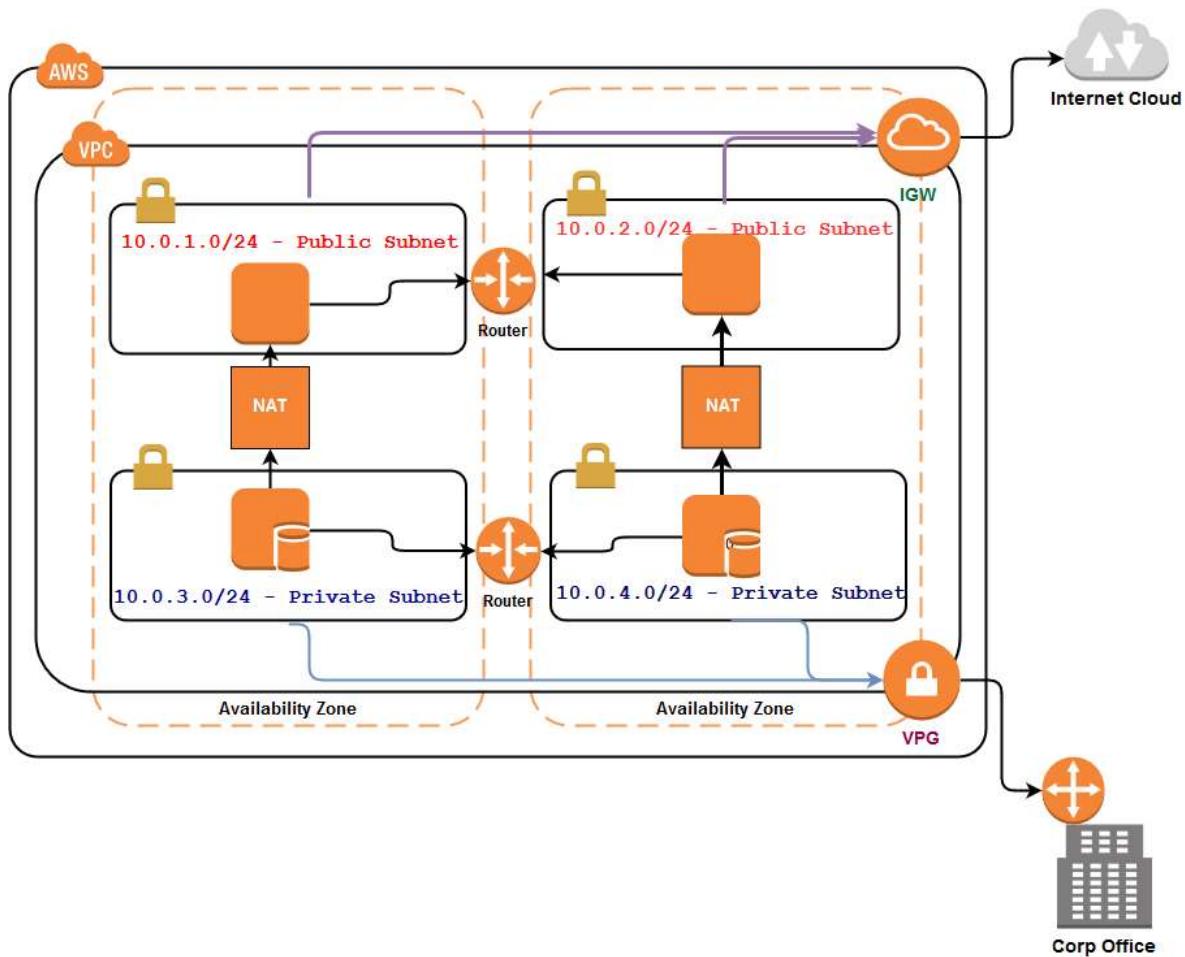
Add Statement and click on **Generate Policy**

```
{
  "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**

13. 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

AWS – Amazon Web Services Lab Practice Guide <https://www.server-computer.com>

- 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

VPCs > Create VPC

Create VPC

A VPC is an isolated portion of the AWS cloud populated by AWS objects, such as Amazon EC2 instances. You must specify an IPv4 address range for your VPC. Specify the IPv4 address range as a Classless Inter-Domain Routing (CIDR) block, for example, 10.0.0.0/16. You cannot specify an IPv4 CIDR block larger than /16. You can optionally associate an Amazon-provided IPv6 CIDR block with the VPC.

Name tag: MyVPC

IPv4 CIDR block*: 10.0.0.0/16

IPv6 CIDR block: No IPv6 CIDR Block Amazon provided IPv6 CIDR block

Tenancy: Default

Required

Cancel **Create**

- **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

AWS – Amazon Web Services Lab Practice Guide <https://www.server-computer.com>

Create VPC

The following VPC was created:

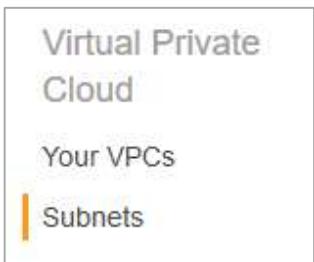
VPC ID vpc-02c316e5f1be2208a

[Close](#)

Your VPC created successfully.

13.1. 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 /29 netmask, and can be the same size as your VPC. An IPv6 CIDR block must be a /64 CIDR block.

Name tag	S1-Private	Required	
VPC*	vpc-02c316e5f1be2208a	Required	
VPC CIDRs	CIDR	Status	Status Reason
10.0.0.0/16		associated	
Availability Zone	us-east-2a	Required	
IPv4 CIDR block*	10.0.1.0/24	Required	

* 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

13.2. 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.

Internet gateways > Create internet gateway www.server-computer.com

Create internet gateway

An internet gateway is a virtual router that connects a VPC to the internet. To create a new internet gateway specify the name for the gateway below.

Name tag i

* Required Cancel **Create**

Create internet gateway

✓ The following internet gateway was created:

Internet gateway ID `igw-0b5da69f9e34ec455`

Close

Actions ▾

- [Delete internet gateway](#)
- [Attach to VPC](#)
- [Detach from VPC](#)
- [Add/Edit Tags](#)

Now attach Internet Gateway to VPC

Internet gateways > Attach to VPC www.server-computer.com

Attach to VPC

Attach an internet gateway to a VPC to enable communication with the internet. Specify the VPC you would like to attach below.

VPC* i

▶ AWS Command Line Interface command

* Required Cancel **Attach**

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

13.3. 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.

AWS – Amazon Web Services Lab Practice Guide <https://www.server-computer.com>

Create Virtual Private Gateway

Virtual Private Gateways > Create Virtual Private Gateway
Create Virtual Private Gateway
www.server-computer.com

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

Name tag i

ASN Amazon default ASN i
 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
Associate Detach

Attach VGW to MyVPC

Attach to VPC

Select the VPC to attach to the virtual private gateway.

Virtual Private Gateway Id vgw-0649463556a8290fe

VPC* C

Cancel Yes, Attach

13.4. 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

AWS – Amazon Web Services Lab Practice Guide <https://www.server-computer.com>

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: R1-IGW i

VPC*: vpc-02c316e5f1be2208a C i

* 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: R2-VGW i

VPC*: vpc-02c316e5f1be2208a C i

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 X

Add route 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 X

Add route 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)

AWS – Amazon Web Services Lab Practice Guide <https://www.server-computer.com>

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

Subnet: subnet-09d6c82e020a61325

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

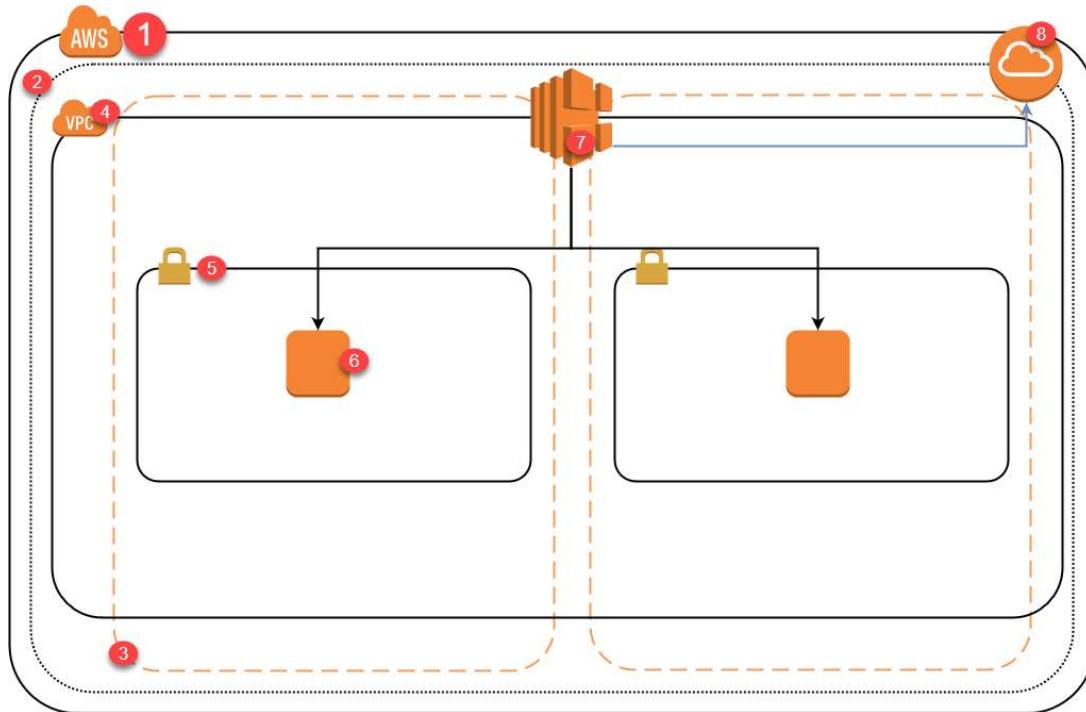
Edit route table association

Route Table: rtb-08aa6cb351595eac2 | R1-IGW

< < 1 to 2 of 2 > >

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

14. 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

AWS – Amazon Web Services Lab Practice Guide <https://www.server-computer.com>

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

Types of ELB

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

ELB Practical

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

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

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

▼ Advanced Details

User data  As text As file Input is already base64 encoded

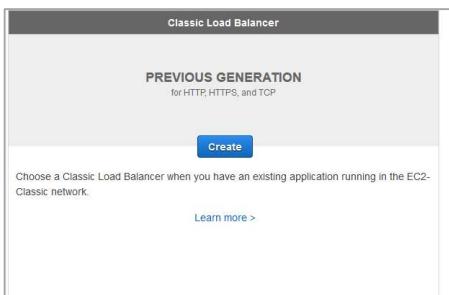
```
#!/bin/bash
sudo yum update -y
sudo yum install httpd* -y
sudo service httpd start
sudo chkconfig httpd on
echo '<html><h1>Hello, Welcome to Server1</h1></html>' > /var/www/html/index.html
sudo service httpd restart
```

Note: while launching second instance change echo statement to server2

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

Creating Classic Elastic Load Balancer

AWS – Amazon Web Services Lab Practice Guide <https://www.server-computer.com>



Step 1: Define Load Balancer

Basic Configuration

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

Load Balancer name: Create LB Inside:

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

Enable advanced VPC configuration:

Listener Configuration:

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

Add

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-0415a767640ae4ef9	10.0.2.0/24	S2-Private

Selected subnets				
Actions	Availability Zone	Subnet ID	Subnet CIDR	Name
- -	us-east-2a	subnet-01f8724bb68578a99	10.0.3.0/24	S3-Public
- -	us-east-2b	subnet-09d6c82e020a61325	10.0.4.0/24	S4-Public

Cancel **Next: Assign Security Groups**

Click Next: Assign Security Groups

Assign a security group: Create a **new** security group
 Select an **existing** security group

Security group name:

Description: 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

AWS – Amazon Web Services Lab Practice Guide <https://www.server-computer.com>

Step 4: Configure Health Check

Your load balancer will automatically perform health checks on your

Ping Protocol	HTTP
Ping Port	80
Ping Path	/index.html

Advanced Details

Response Timeout	5	seconds
Interval	30	seconds
Unhealthy threshold	2	
Healthy threshold	10	

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 300 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...	running	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

AWS – Amazon Web Services Lab Practice Guide <https://www.server-computer.com>

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.

15. 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.

15.1. 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 you wish in this case **server-computer-trail**

AWS – Amazon Web Services Lab Practice Guide <https://www.server-computer.com>

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

The screenshot shows the 'Management events' section of the CloudTrail configuration. It includes a description of management events, a radio button group for 'Read/Write events' (with 'All' selected), and a help icon.

The screenshot shows the 'S3' tab of the CloudTrail configuration. It displays a table with one resource, 'arkit-test123', and its details: Prefix '/CloudTrail', Read and Write permissions checked. A note about recording S3 API activity is present.

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.

The screenshot shows the 'Storage location' section. It has a radio button for 'Create a new S3 bucket' (selected 'No') and a dropdown for 'S3 bucket' containing 'arkit-test123'. An 'Advanced' link is also visible.

Click **Create**

The screenshot shows the 'Trails' section of the CloudTrail configuration. It lists a single trail named 'server-computer-trail' with 'Region' set to 'US East (Ohio)' and 'Organization trail' set to 'No'.

CloudTrail has been created successfully.

16. 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



```
New query 1 +
1 SELECT * FROM "default"."cloudtrail_logs_server-computer-test123" limit 10;
```

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

17. 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.

17.1. 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	<input type="text" value="MyFirstLaunchConfiguration"/>
Purchasing option	<input type="checkbox"/> Request Spot Instances
IAM role	<input type="text" value="None"/>
Monitoring	<input type="checkbox"/> Enable CloudWatch detailed monitoring Learn more

>> Click Advanced Details

IP Address Type	<input type="radio"/> Only assign a public IP address to instances launched in the default VPC and subnet. (default) <input checked="" type="radio"/> Assign a public IP address to every instance. <input type="radio"/> 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

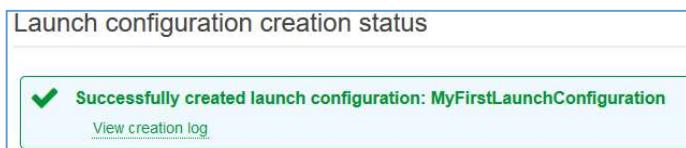
AWS – Amazon Web Services Lab Practice Guide <https://www.server-computer.com>

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

Click Review

Click Create Launch Configuration

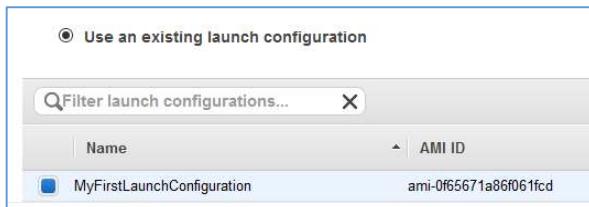
Select the Key Pair or create key pair



Launch configuration created successfully. Click Close

17.2. Auto Scaling Groups

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



Click Next Step

This form step includes the following fields:

- Group name:** Server-Computer-Group
- Launch Configuration:** MyFirstLaunchConfiguration
- Group size:** Start with 1 instances
- Network:** vpc-02c316e5f1be2208a (10.0.0.0/16) | MyVPC
- Subnet:** subnet-01f8724bb68578a99(10.0.3.0/24) | S3-Public | us-east-2a
subnet-09d6c82e020a61325(10.0.4.0/24) | S4-Public | us-east-2b
- Load Balancing:** Receive traffic from one or more load balancers
- Classic Load Balancers:** (empty input field)
- Target Groups:** (empty input field)
- Health Check Type:** ELB EC2
- Health Check Grace Period:** 300 seconds
- Monitoring:** Amazon EC2 Detailed Monitoring metrics, which are provided at 1 minute frequency, are not enabled for the launch configuration MyFirstLaunchConfiguration. Instances launched from it will use Basic Monitoring metrics, provided at 5 minute frequency.
- Instance Protection:** (empty input field)
- Service-Linked Role:** AWSServiceRoleForAutoScaling

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

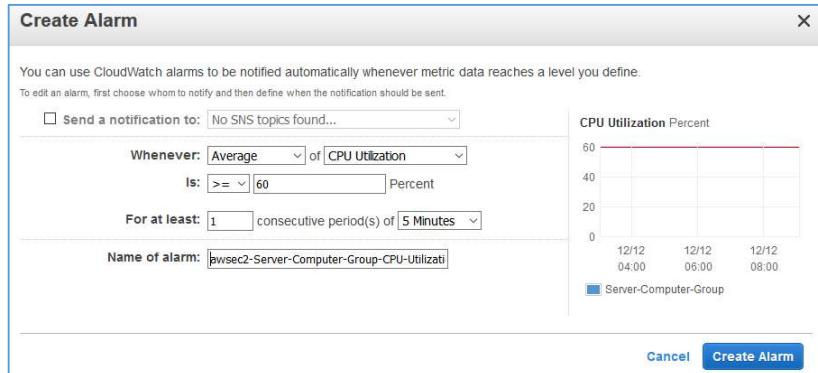
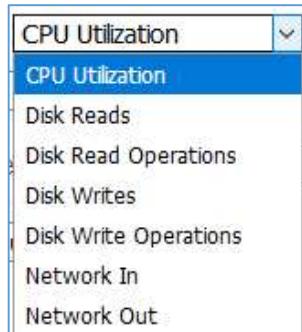
AWS – Amazon Web Services Lab Practice Guide <https://www.server-computer.com>

Click **Next: Configure Scaling Policies**

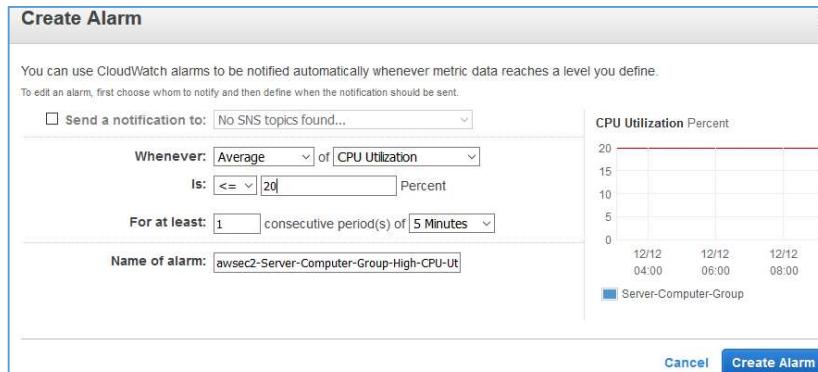
Keep this group at its initial size
 Use scaling policies to adjust the capacity of this group

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



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

AWS – Amazon Web Services Lab Practice Guide <https://www.server-computer.com>

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: instances <= 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: instances >= 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

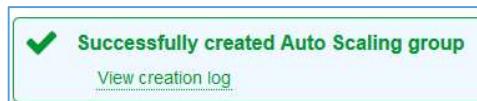
[Add notification](#)

Click **Next: Configure Tags**

Add tags for recognizing auto scale instances

Click **review**

Click **Create Auto Scaling Group**



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.

18. 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](#)

19. AWS Services and abbreviations

- S3 – Simple Storage
- EC2 – Elastic Compute Cloud
- EBS – Elastic Block Storage
- EFS – Elastic File System
- ECS – Elastic Container Service

AWS – Amazon Web Services Lab Practice Guide <https://www.server-computer.com>

- 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