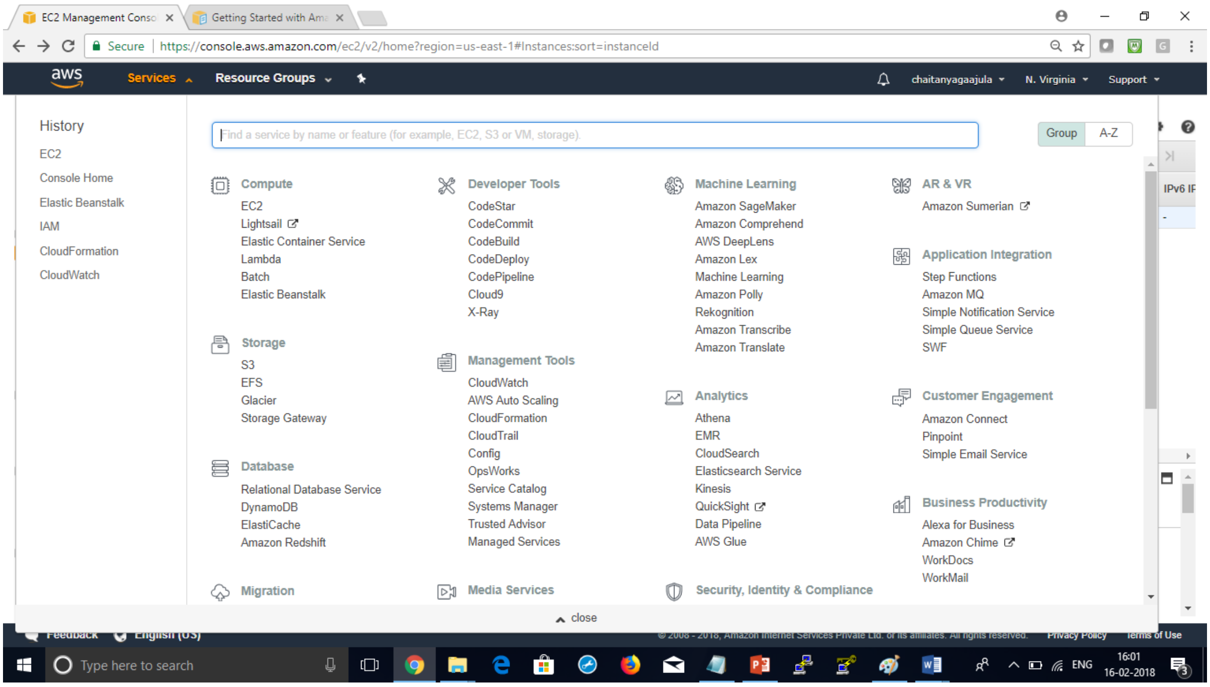
Creating an Amazon EC2 Linux Instance

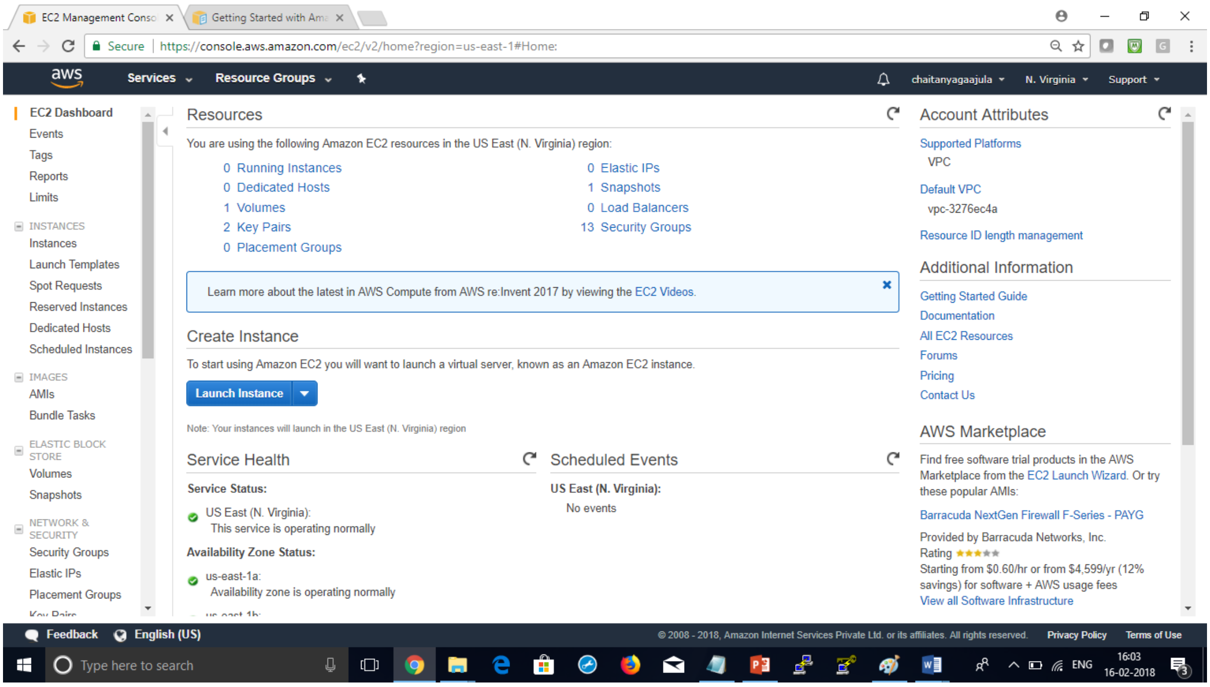
This lab leads you through the steps to launch and configure your first virtual machine in the Amazon cloud. You will learn about using Amazon Machine Images to launch Amazon EC2 instances, creating key pairs for SSH authentication, securing network access to EC2 instances with security groups and automatically configuring EC2 instances with bootstrapping scripts. At the end of this lab you will have deployed a simple web server which includes an informational page to display results of your virtual web server instance.

1. Login to AWS Management Console.



2.Choose Region as N.Virginia

3. Click EC2 under Compute section. This will take you to EC2 dashboard.



Resources

You are using the following Amazon EC2 resources in the US East (N. Virginia) region:

0 Running Instances	0 Elastic IPs
0 Dedicated Hosts	1 Snapshots
1 Volumes	0 Load Balancers
2 Key Pairs	13 Security Groups
0 Placement Groups	

Learn more about the latest in AWS Compute from AWS re:Invent 2017 by viewing the EC2 Videos.

Create Instance

To start using Amazon EC2 you will want to launch a virtual server, known as an Amazon EC2 instance.

Note: Your instances will launch in the US East (N. Virginia) region

Service Health

Service Status:

US East (N. Virginia):
This service is operating normally

Availability Zone Status:

us-east-1a:
Availability zone is operating normally

us-east-1b:

Scheduled Events

US East (N. Virginia):
No events

Account Attributes

Supported Platforms
VPC

Default VPC
vpc-3276ec4a

Resource ID length management

Additional Information

Getting Started Guide
Documentation
All EC2 Resources
Forums
Pricing
Contact Us

AWS Marketplace

Find free software trial products in the AWS Marketplace from the EC2 Launch Wizard. Or try these popular AMIs:

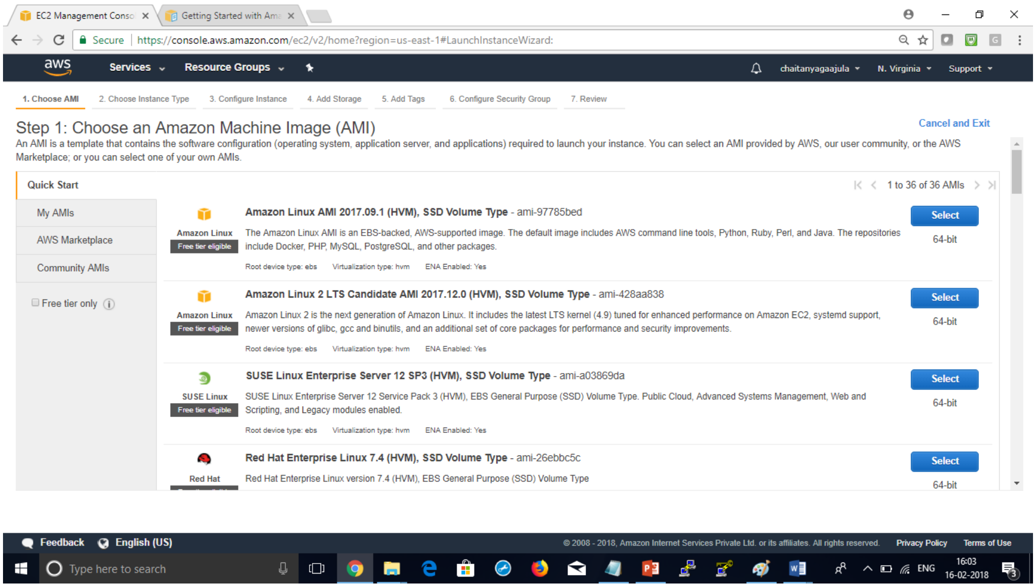
Barracuda NextGen Firewall F-Series - PAYG

Provided by Barracuda Networks, Inc.
Rating ★★★★★
Starting from $0.60/hr or from $4,599/yr (12% savings) for software + AWS usage fees
View all Software Infrastructure

© 2008 - 2018, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.

4. Click Launch Instance.

5. Because you require a Linux instance, in the row for the basic 64-bit Amazon Linux AMI, which will normally be the first option on the list, click Select.



Step 1: Choose an Amazon Machine Image (AMI)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace; or you can select one of your own AMIs.

□ Free tier only

Amazon Linux AMI 2017.09.1 (HVM), SSD Volume Type - ami-97785bed
The Amazon Linux AMI is an EBS-backed, AWS-supported image. The default image includes AWS command line tools, Python, Ruby, Perl, and Java. The repositories include Docker, PHP, MySQL, PostgreSQL, and other packages.
Root device type: ebs Virtualization type: hvm ENA Enabled: Yes
64-bit

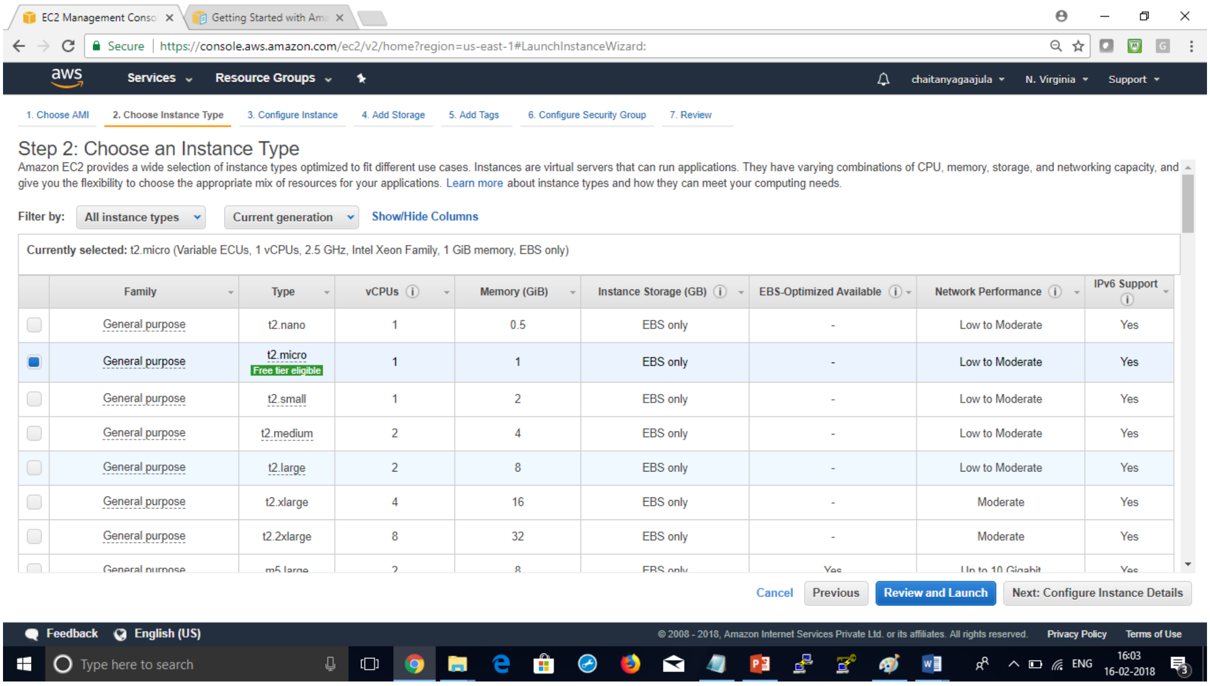
Amazon Linux 2 LTS Candidate AMI 2017.12.0 (HVM), SSD Volume Type - ami-428aa838
Amazon Linux 2 is the next generation of Amazon Linux. It includes the latest LTS kernel (4.9) tuned for enhanced performance on Amazon EC2, systemd support, newer versions of glibc, gcc and binutils, and an additional set of core packages for performance and security improvements.
Root device type: ebs Virtualization type: hvm ENA Enabled: Yes
64-bit

SUSE Linux Enterprise Server 12 SP3 (HVM), SSD Volume Type - ami-a03869da
SUSE Linux Enterprise Server 12 Service Pack 3 (HVM), EBS General Purpose (SSD) Volume Type. Public Cloud, Advanced Systems Management, Web and Scripting, and Legacy modules enabled.
Root device type: ebs Virtualization type: hvm ENA Enabled: Yes
64-bit

Red Hat Enterprise Linux 7.4 (HVM), SSD Volume Type - ami-26ebbc5c
Red Hat Enterprise Linux version 7.4 (HVM), EBS General Purpose (SSD) Volume Type
64-bit

© 2008 - 2018, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.

6. On the Choose an Instance Type page, choose t2.micro, which is free tier eligible.



Step 2: Choose an Instance Type

Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. Learn more about instance types and how they can meet your computing needs.

Filter by: All instance types | Current generation | Show/Hide Columns

Currently selected: t2.micro (Variable ECUs, 1 vCPUs, 2.5 GHz, Intel Xeon Family, 1 GiB memory, EBS only)

	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
□	General purpose	t2.small	1	2	EBS only	-	Low to Moderate	Yes
□	General purpose	t2.medium	2	4	EBS only	-	Low to Moderate	Yes
□	General purpose	t2.large	2	8	EBS only	-	Low to Moderate	Yes
□	General purpose	t2.xlarge	4	16	EBS only	-	Moderate	Yes
□	General purpose	t2.2xlarge	8	32	EBS only	-	Moderate	Yes
□	General purpose	m5.large	2	8	EBS only	Yes	Up to 10 Gigabit	Yes

Cancel
Previous
Review and Launch
Next: Configure Instance Details
Feedback
English (US)
© 2008 - 2018, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
Type here to search
ENG
16:03
16-02-2018

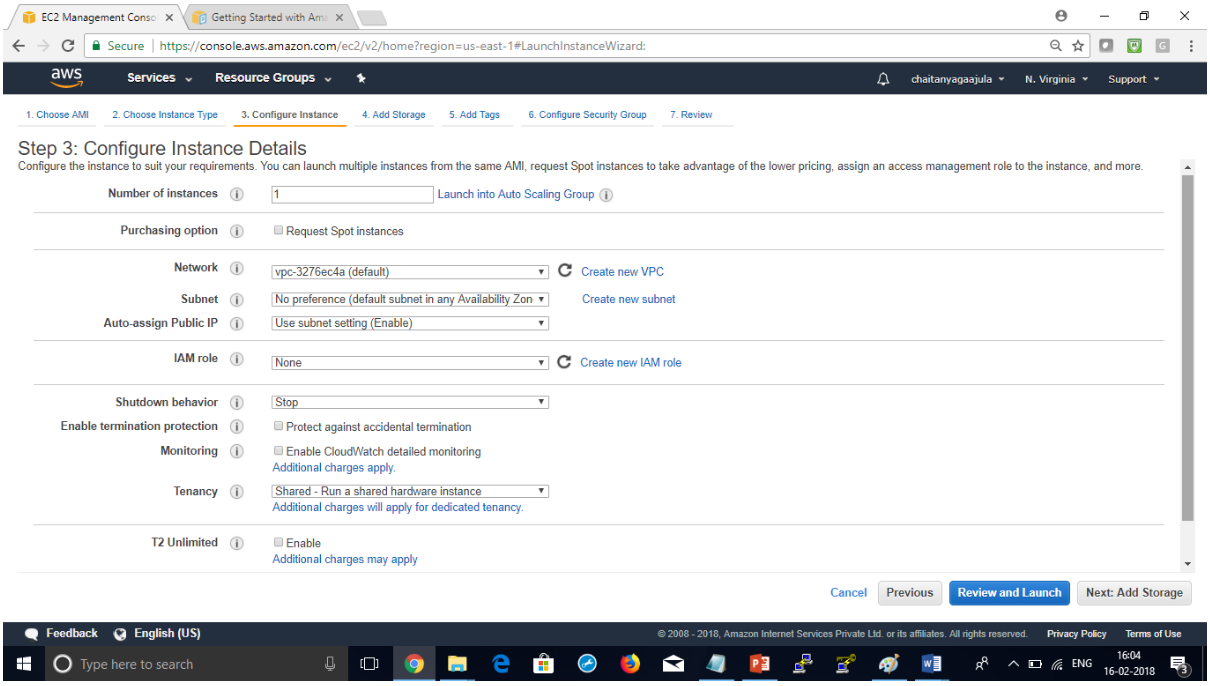
7. Click Next: Configure Instance Details.

8. On the Configure Instance Details page, scroll down and expand Advanced Details section.

9. For User Data, select As Text.

10. Copy and paste following script into the User Data box.

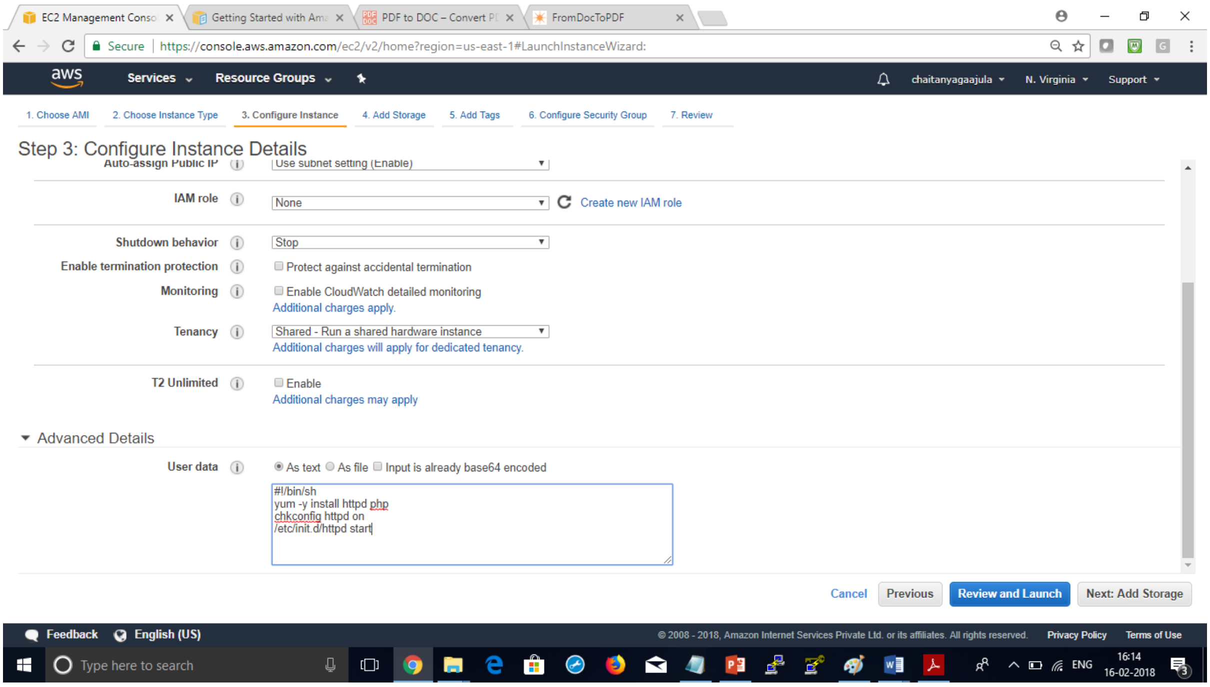
```
#!/bin/sh
yum -y install httpd php
chkconfig httpd on
/etc/init.d/httpd start
```



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-3276ec4a (default) Create new VPC
Subnet	No preference (default subnet in any Availability Zon Create new subnet
Auto-assign Public IP	Use subnet setting (Enable)
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



Step 3: Configure Instance Details

Auto-assign Public IP	Use subnet setting (Enable)
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

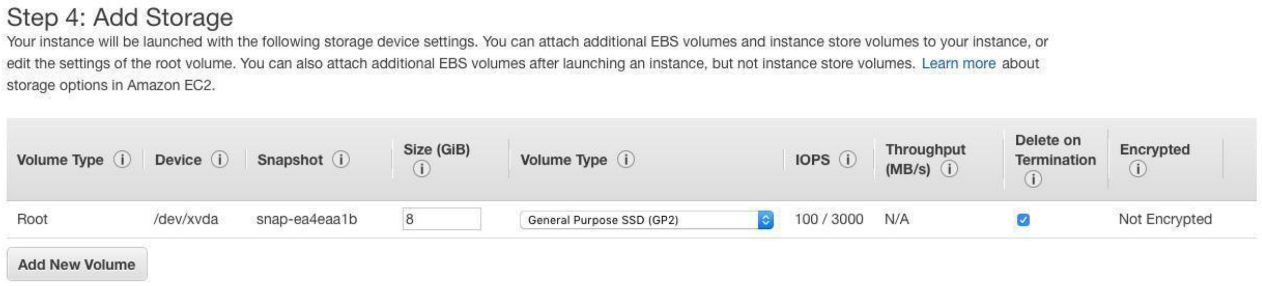
Advanced Details

User data ● As text ○ As file □ Input is already base64 encoded

```
#!/bin/sh
yum -y install httpd php
chkconfig httpd on
/etc/init.d/httpd start
```

11. Click Next: Add Storage.

→ This page displays which EBS volumes are attached to your image. When you launch an EC2 instance, the root volume contains the image used to boot the instance. Instances that use EBS for root device automatically have an EBS volume attached. When an EBS-backed instance is launched, an EBS volume is created for each EBS snapshot referenced by the AMI. You must have at least one snapshot that denotes the root device; the others are optional and denote additional volumes to be created from other snapshots.



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-ea4eaa1b	8	General Purpose SSD (GP2)	100 / 3000	N/A	☑	Not Encrypted

12. Click Next: Tag Instance to accept the default storage device configuration

13. On the Tag Instance page, type a name for your instance in the Value box. This name, more correctly known as tag, will appear in the console when the instance launches. It makes it easy to keep track of running machines in a complex environment. Use a name that you can easily recognize and remember.

14. Click Next: Configure Security Group.

    For each security group, you add rules that govern the allowed inbound traffic to instances in the group. All other inbound traffic is discarded. You can modify rules for a security group at any time. The new rules are automatically enforced for all existing and future instances in the group.

15. For Assign a security group, click Create a new Security group.

16. In the Security group name box, type a name that you would like to assign to this security group.

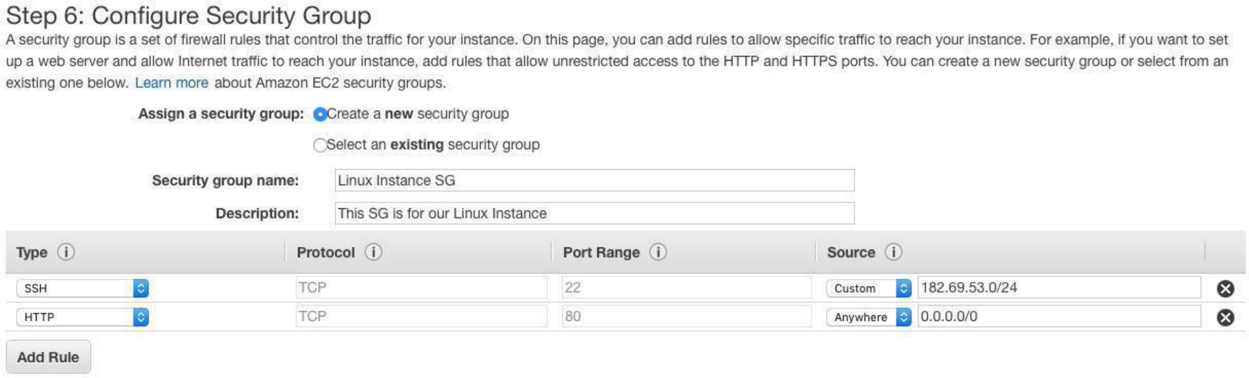
17. (Optional) type a description for your security group.

By default, AWS creates a rule that allows Secure Shell (SSH) access from any IP address. It is highly recommended that you restrict terminal access to the ranges of IP addresses (e.g., IPs assigned to machines within your company) that have a legitimate business need to administer to your EC2 instance.

18. Click Add Rule to open a new port.

19. In the Type drop-down list, click HTTP.

→ This will add a default handler for HTTP that will allow requests from anywhere on the internet. Since you want this web server to be accessible to the general public, you can leave this rule as is without any further configuration.



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: Linux Instance SG

Description: This SG is for our Linux Instance

Type	Protocol	Port Range	Source	
SSH	TCP	22	Custom	182.69.53.0/24
HTTP	TCP	80	Anywhere	0.0.0.0/0

20. Click Review and Launch.

21. Review your choices, and then click Launch.

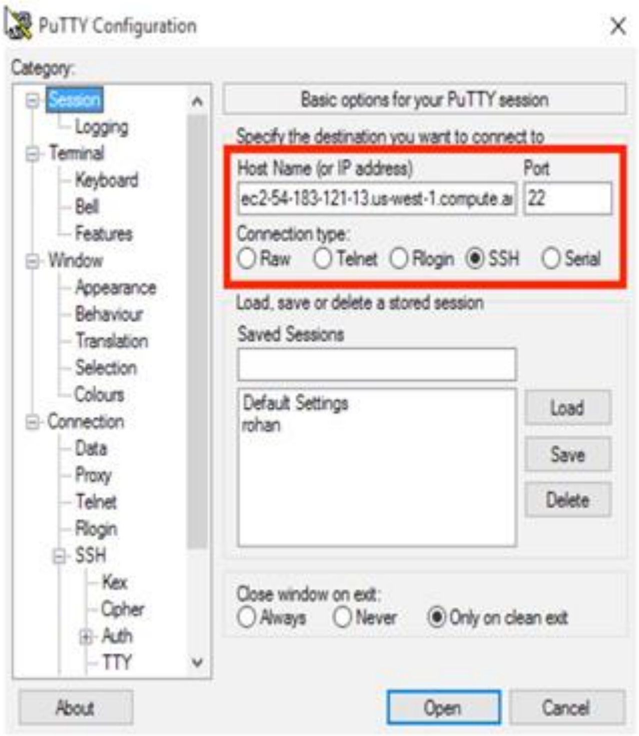
22. Create a new key pair and select the acknowledgement check box

Instructions for Windows Users: Connecting to EC2 instance via SSH

→ In this section, you will use the PuTTY Secure Shell (SSH) client and your server's public DNS address to connect to your server.

→ All EC2 instances are assigned two IP addresses at launch: a private IP address (RFC 1918) and a public IP address that are directly mapped to each other through Network Address Translation (NAT). Private IP addresses are only reachable form within Amazon EC2 network. Public IP addresses are reachable from the internet.

→ EC2 also provides an internal DNS name and public DNS name that map to the private and public IP addresses, respectively. The internal DNS name can only be resolved within Amazon EC2. The public DNS name resolves to the public IP address outside the EC2 network, and to the private IP address within the EC2 network.



Specify the destination you want to connect to

Host Name (or IP address): ec2-54-183-121-13.us-west-1.compute.ar

Port: 22

Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

Load, save or delete a stored session

Saved Sessions

Default Settings
rohan

Close window on exit: ○ Always ○ Never ● Only on clean exit

40. Open the Terminal application.

Connect to EC2 instance using OpenSSH CLI client

41. Enter the following commands.

```
chmod 400 <private key file>

ssh –i <private key file> ec2-user@<public IP address>
```

The AMI has already been customized with the installation of Apache and PHP from the script you entered as user data when the instance was launched. Modify the web server by adding an index.php file.

42. Copy the following commands into PuTTY. This will create an index.php file at the root of your HTTP web server's HTML document directory.

```
cd /var/www/html sudo nano index.php
```

43. Copy the following code and paste to Nano /vi editor

```
<?php

$url = "http://169.254.169.254/latest/meta-data/instance-id"; $instance_id = file_get_contents($url);


echo "Instance ID: <b>" . $instance_id . "</b><br/>";

$url = "http://169.254.169.254/latest/meta-data/placement/availability-zone";
$zone = file_get_contents($url);


echo "Zone: <b>" . $zone . "</b><br/>";

?>
```

View Your Website

In this section, you will navigate to your new website and see the content of the page that you just created.

44. Return to AWS Management Console.

45. In your list of running EC2 instances, select the instance to display the instance details.

46. Copy and paste either the Public IP or Public DNS name in your browser. Your instance ID and Availability Zone should be displayed in the browser.

Congratulations! You have now successfully:

- Learned about basic concepts and terminology of the Amazon Elastic Compute Cloud (EC2) service.
- Created your own EC2 server instance running Linux in the AWS cloud.
- Modified it to run a web server with a page that displays machine-specific information.