Contents

Lab 2: Elastic Compute Cloud (EC2) 2

Task Breakdown: 2

Task 1: Launch an EC2 instance 2

Task 2: SSH into the EC2 instance 8

Task 3: Create, attach an Elastic Block Store (EBS) volume 14

Task 4: Format and mount the EBS volume. Install Wordpress 17

Task 5: Create Amazon Machine Image(AMI) 19

Task 6: Manage EC2 through CLI 21

Important: Cleanup of all Resources 23

Lab 2: Elastic Compute Cloud (EC2)

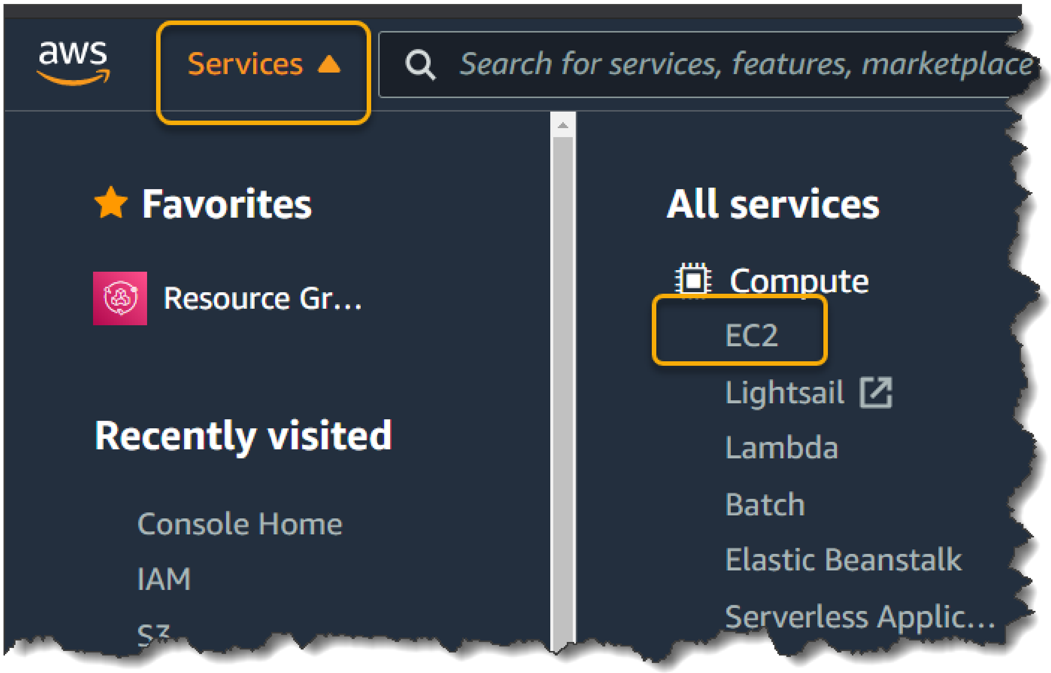
In this lab we are going to launch an EC2 instance, attach and configure storage and deploy an application on it.

Task Breakdown:

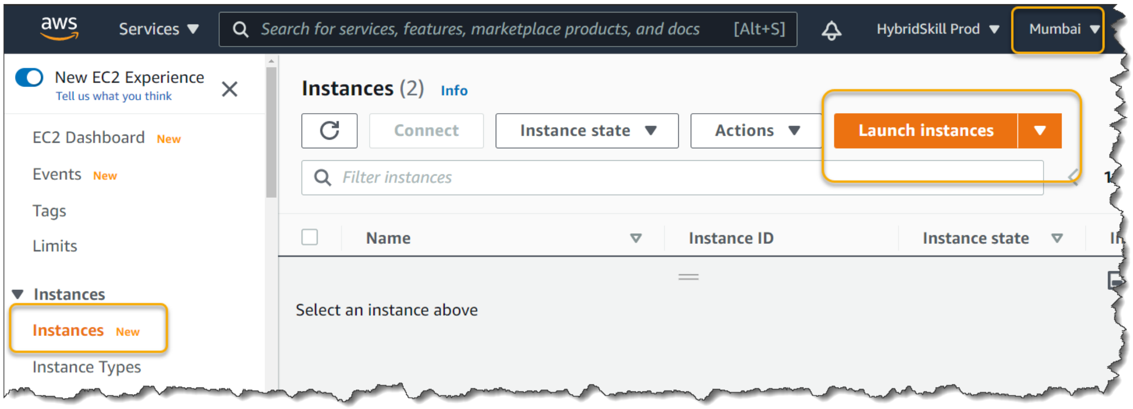
- Launch an EC2 instance
- SSH into the EC2 instance
- Create, attach and format an Elastic Block Store (EBS) volume
- Format, mount the EBS volume. Install Wordpress
- Create Amazon Machine Image(AMI)
- Manage EC2 through CLI

Task 1: Launch an EC2 instance

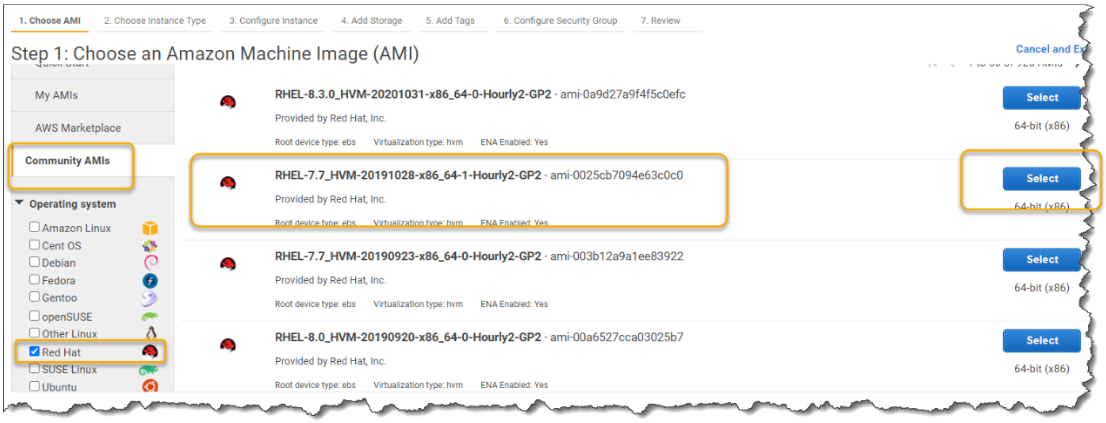
1. Click on **Services** and under **Compute** click on **EC2**



2. Make sure your **Region** is selected, click on **Instances** on the left pane and click on **Launch Instances**. We have selected **Mumbai** as an example.



3. On the left pane click **Community AMIs**, check the **Red Hat** checkbox and Choose **Red Hat Enterprise Linux 7.7(or any RHEL 7.x AMI)** as your **AMI** by clicking the **Select** button.



Step 1: Choose an Amazon Machine Image (AMI)

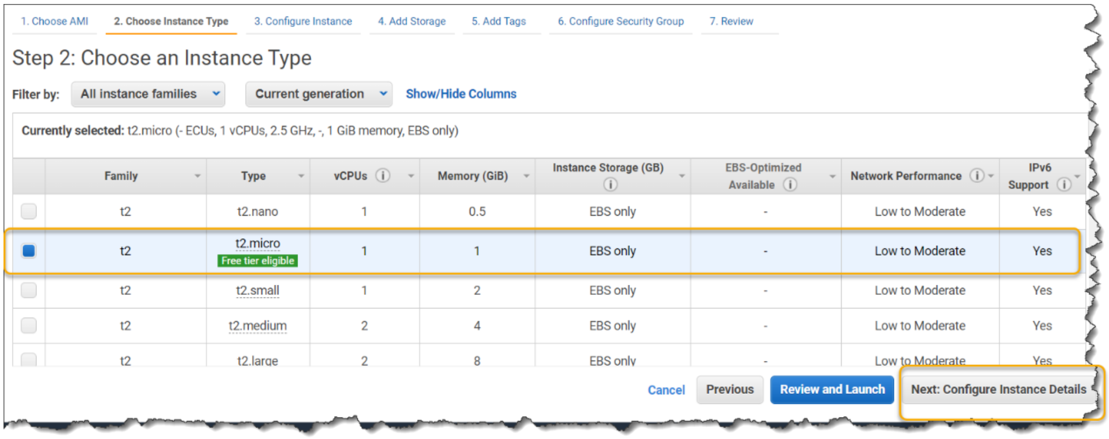
RHEL-8.3.0_HVM-20201031-x86_64-0-Hourly2-GP2 - ami-0a9d27a9f4f5c0efc
Provided by Red Hat, Inc.
Root device type: ebs Virtualization type: hvm ENA Enabled: Yes
64-bit (x86)

RHEL-7.7_HVM-20191028-x86_64-1-Hourly2-GP2 - ami-0025cb7094e63c0c0
Provided by Red Hat, Inc.
Root device type: ebs Virtualization type: hvm ENA Enabled: Yes
64-bit (x86)

RHEL-7.7_HVM-20190923-x86_64-0-Hourly2-GP2 - ami-003b12a9a1ee83922
Provided by Red Hat, Inc.
Root device type: ebs Virtualization type: hvm ENA Enabled: Yes
64-bit (x86)

RHEL-8.0_HVM-20190920-x86_64-0-Hourly2-GP2 - ami-00a6527cca03025b7
Provided by Red Hat, Inc.
Root device type: ebs Virtualization type: hvm ENA Enabled: Yes
64-bit (x86)

4. Select **t2.micro** as your Instance Type and click **Next: Configure Instance Details.**



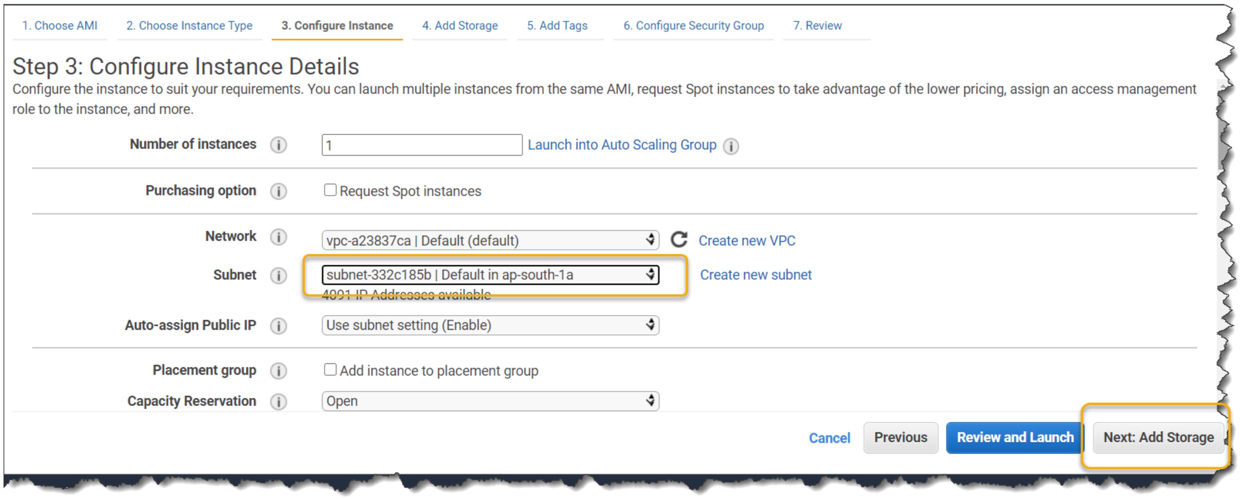
Step 2: Choose an Instance Type

Filter by: All instance families; Current generation

Currently selected: t2.micro (- ECUs, 1 vCPUs, 2.5 GHz, -, 1 GiB memory, EBS only)

	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance	IPv6 Support
☐	t2	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
■	t2	t2.micro Free tier eligible	1	1	EBS only	-	Low to Moderate	Yes
☐	t2	t2.small	1	2	EBS only	-	Low to Moderate	Yes
☐	t2	t2.medium	2	4	EBS only	-	Low to Moderate	Yes
☐	t2	t2.large	2	8	EBS only	-	Low to Moderate	Yes

5. Go to **Subnet** and Select **subnet-xxxxx(ap-south-1a)** from the dropdown as your availability zone. Leave all other options as **default** and finally click **Next: Add Storage**



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-a23837ca | Default (default) — Create new VPC

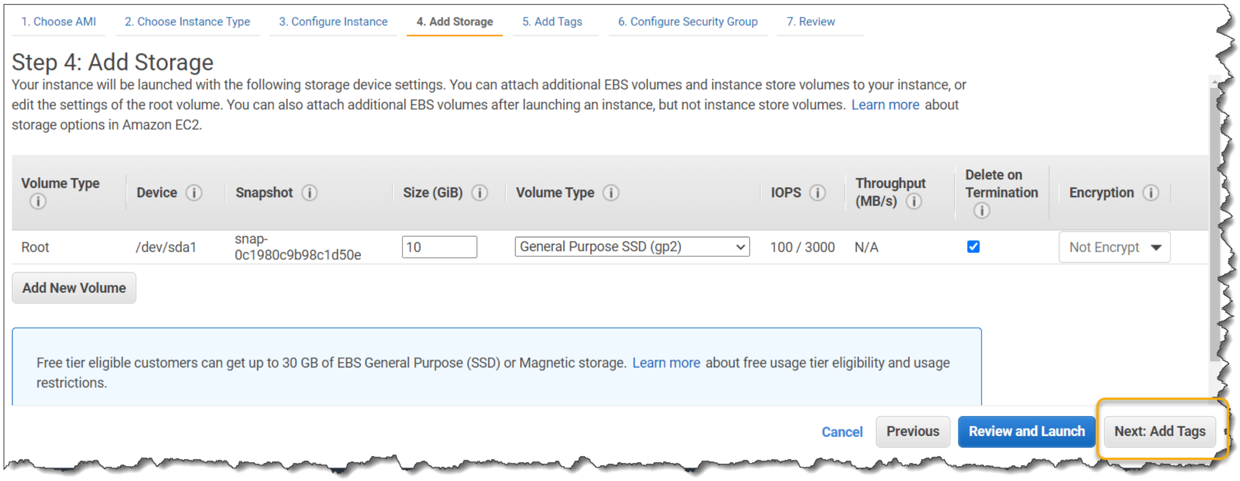
Subnet: subnet-332c185b | Default in ap-south-1a — Create new subnet
4091 IP Addresses available

Auto-assign Public IP: Use subnet setting (Enable)

Placement group: □ Add instance to placement group

Capacity Reservation: Open

6. Leave all the options as default and click on **Next: Add Tags**



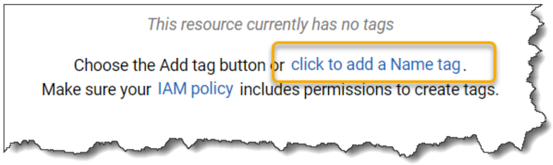
Step 4: Add Storage

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	Encryption
Root	/dev/sda1	snap-0c1980c9b98c1d50e	10	General Purpose SSD (gp2)	100 / 3000	N/A	☑	Not Encrypt

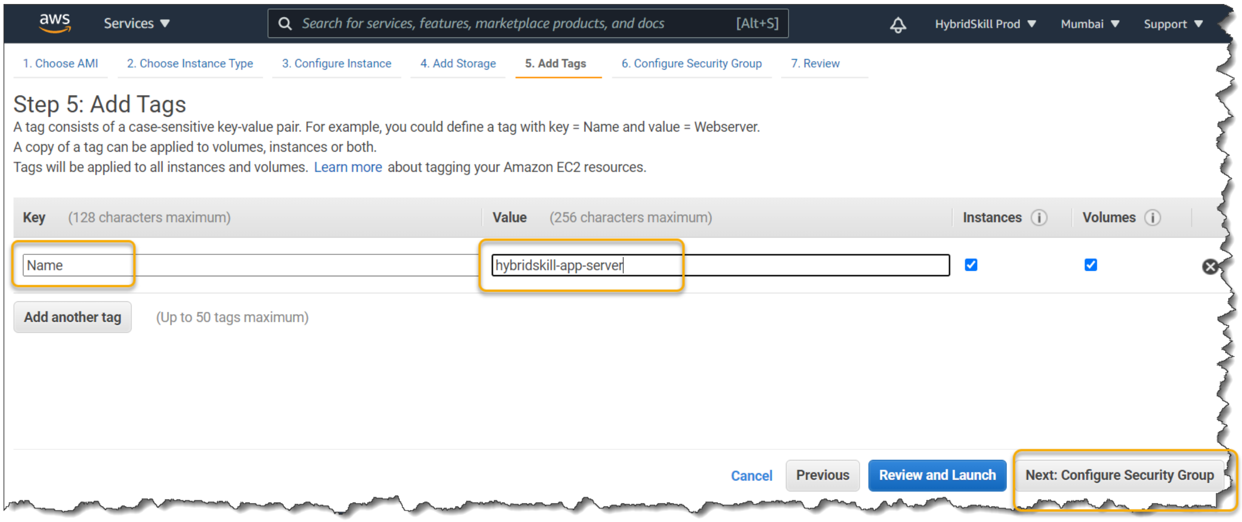
Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. Learn more about free usage tier eligibility and usage restrictions.

7. Click **Create** name tag and enter **hybridskill-app-server** as the name of your EC2 instance click **Next: Configure Security Group**



This resource currently has no tags

Choose the Add tag button or click to add a Name tag.
Make sure your IAM policy includes permissions to create tags.

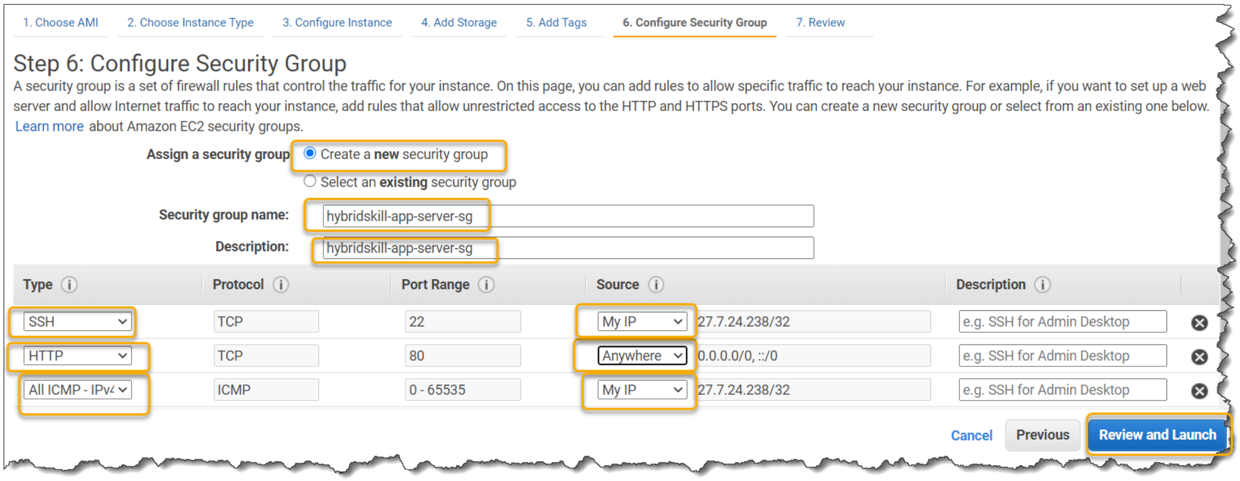


Step 5: Add Tags

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver.
A copy of a tag can be applied to volumes, instances or both.
Tags will be applied to all instances and volumes. Learn more about tagging your Amazon EC2 resources.

Key (128 characters maximum)	Value (256 characters maximum)	Instances	Volumes
Name	hybridskill-app-server	☑	☑

8. Enter **hybridskill-app-server-sg** as Security group name, enter a description. Click on add rule and from the dropdown add **HTTP, ICMP-IPv4** and **SSH** as rules. For **SSH** select the source as **My IP** from the dropdown. For **HTTP** leave the source as **Anywhere** and for **ICMP-IPv4** select the source as **My IP**. Finally click on **Review and Launch**.



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.

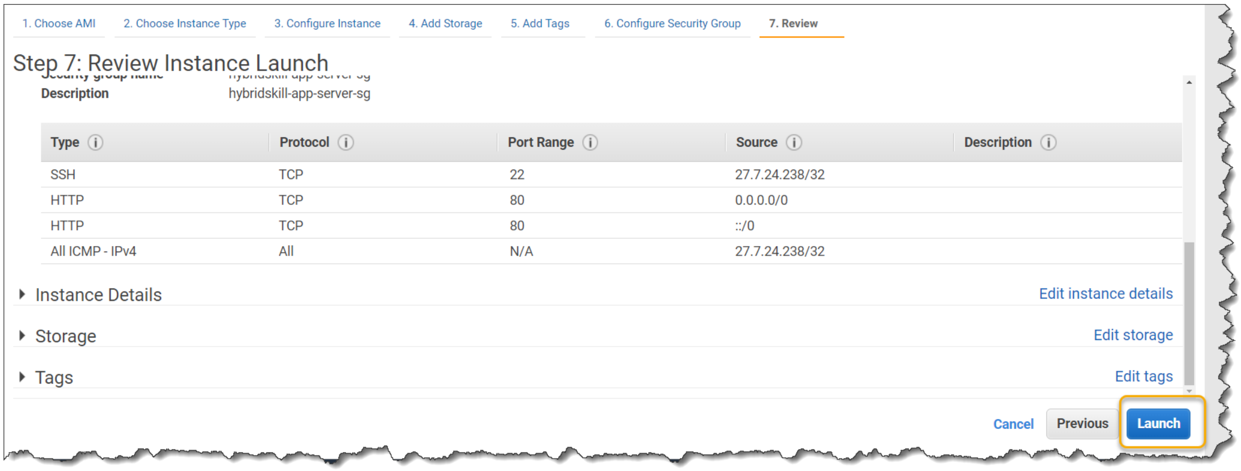
Assign a security group: ● Create a **new** security group
○ Select an **existing** security group

Security group name: hybridskill-app-server-sg

Description: hybridskill-app-server-sg

Type	Protocol	Port Range	Source		Description
SSH	TCP	22	My IP	27.7.24.238/32	e.g. SSH for Admin Desktop
HTTP	TCP	80	Anywhere	0.0.0.0/0, ::/0	e.g. SSH for Admin Desktop
All ICMP - IPv4	ICMP	0 - 65535	My IP	27.7.24.238/32	e.g. SSH for Admin Desktop

9. Review your settings and click **Launch**



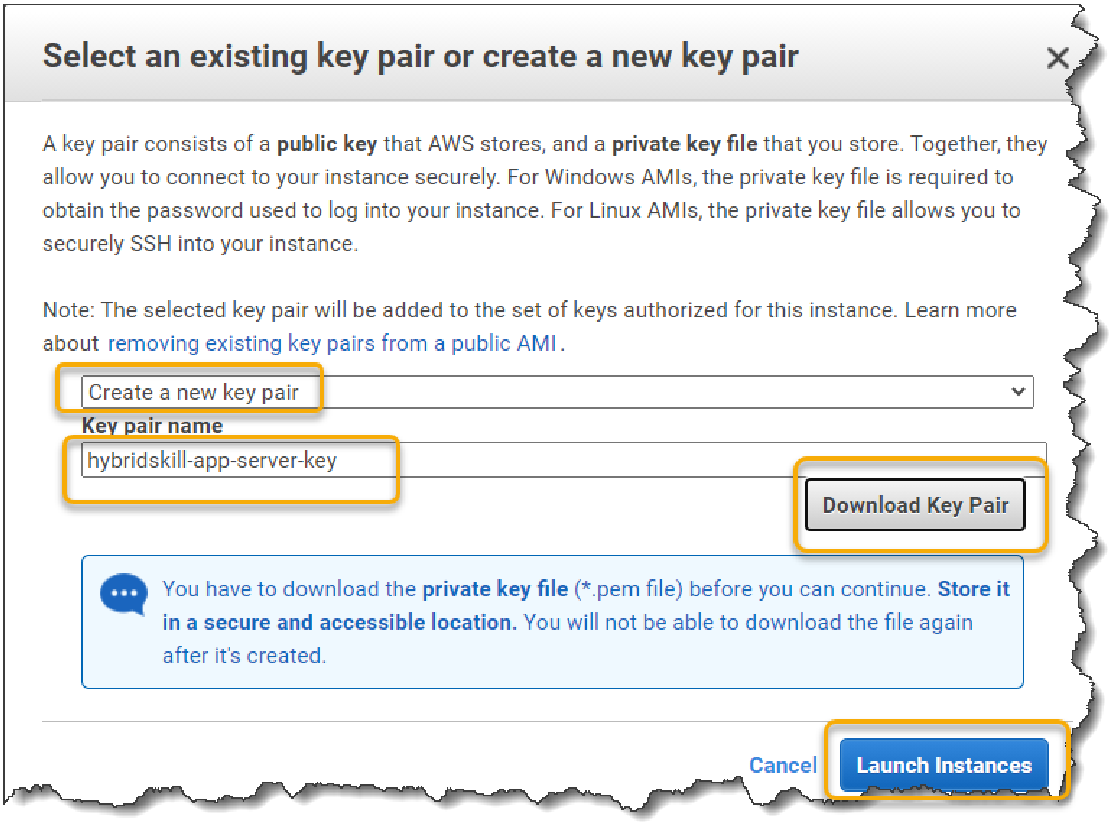
Step 7: Review Instance Launch

Security group name hybridskill-app-server-sg

Description hybridskill-app-server-sg

Type	Protocol	Port Range	Source	Description
SSH	TCP	22	27.7.24.238/32	
HTTP	TCP	80	0.0.0.0/0	
HTTP	TCP	80	::/0	
All ICMP - IPv4	All	N/A	27.7.24.238/32	

10. Select **Create a new key pair** from the dropdown, enter **hybridskill-app-server-key** as the **Key pair name** and click **Download Key Pair.**



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.

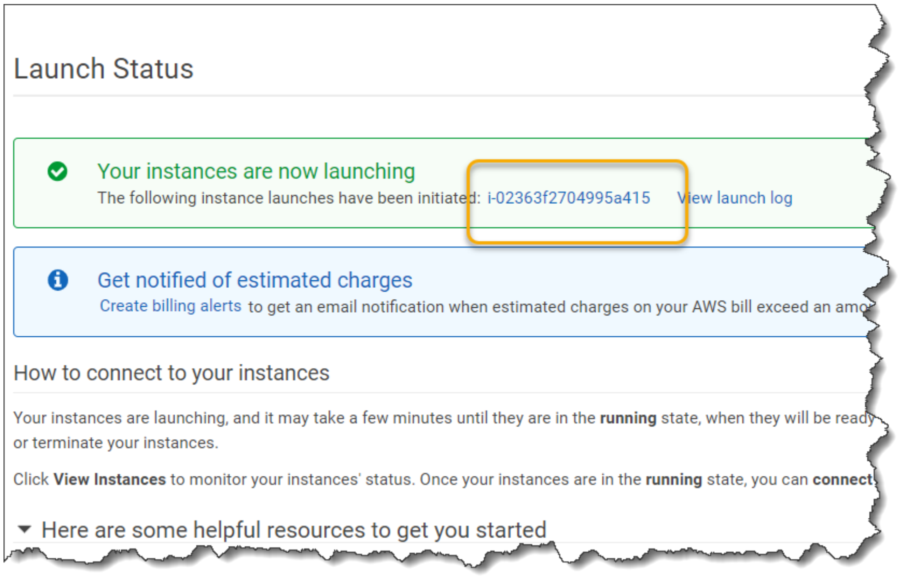
Create a new key pair

Key pair name

hybridskill-app-server-key

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.

11. Your Instance should be launching now. Click on the **Instance id.**



Launch Status

Your instances are now launching

The following instance launches have been initiated: i-02363f2704995a415 View launch log

Get notified of estimated charges

Create billing alerts to get an email notification when estimated charges on your AWS bill exceed an amo

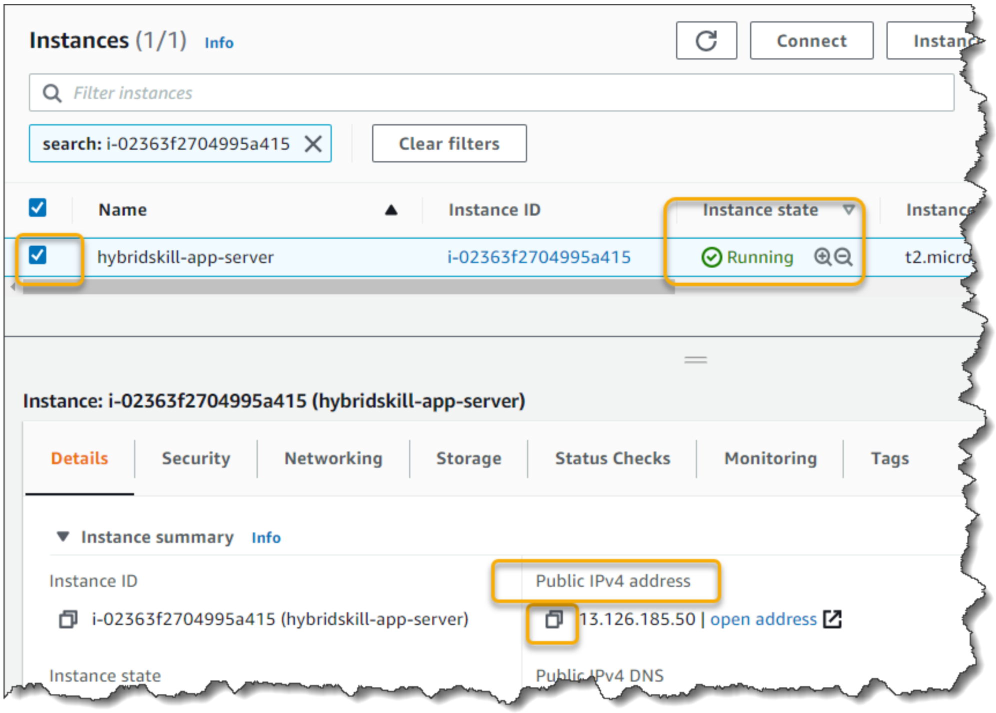
How to connect to your instances

Your instances are launching, and it may take a few minutes until they are in the **running** state, when they will be ready or terminate your instances.

Click **View Instances** to monitor your instances' status. Once your instances are in the **running** state, you can **connect**

Here are some helpful resources to get you started

12. You should see information about your EC2 instance. On the lower pane click **Description** and note down the **IPv4 Public IP**. We will use this later for connecting to the machine.



search: i-02363f2704995a415

☑	Name	Instance ID	Instance state	Instanc
☑	hybridskill-app-server	i-02363f2704995a415	✓ Running	t2.micro

Instance: i-02363f2704995a415 (hybridskill-app-server)

Instance ID

i-02363f2704995a415 (hybridskill-app-server)

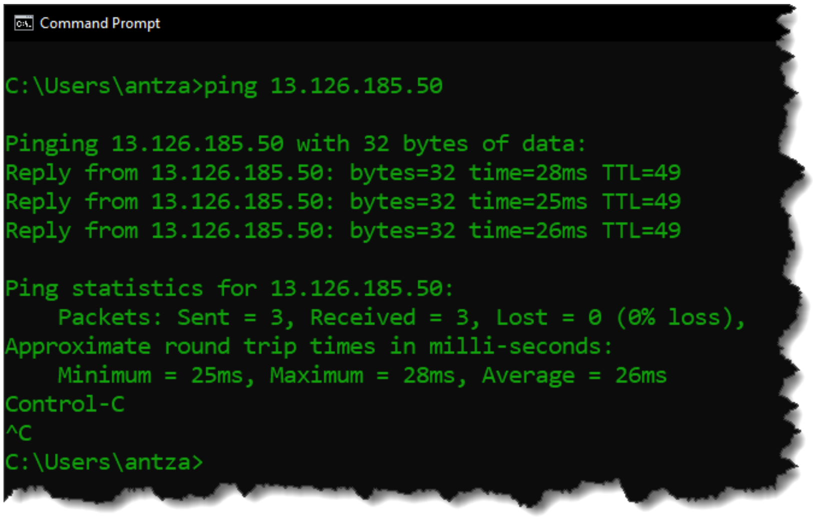
Public IPv4 address

13.126.185.50 | open address

Instance state

Public IPv4 DNS

13. Open a command prompt and type in **Ping <Instance IPv4 PUBLIC IP>.** You should be able to reach your instance**.** If your instance is unreachable, then review your security group and make sure **ICMP IPv4** is whitelisted.



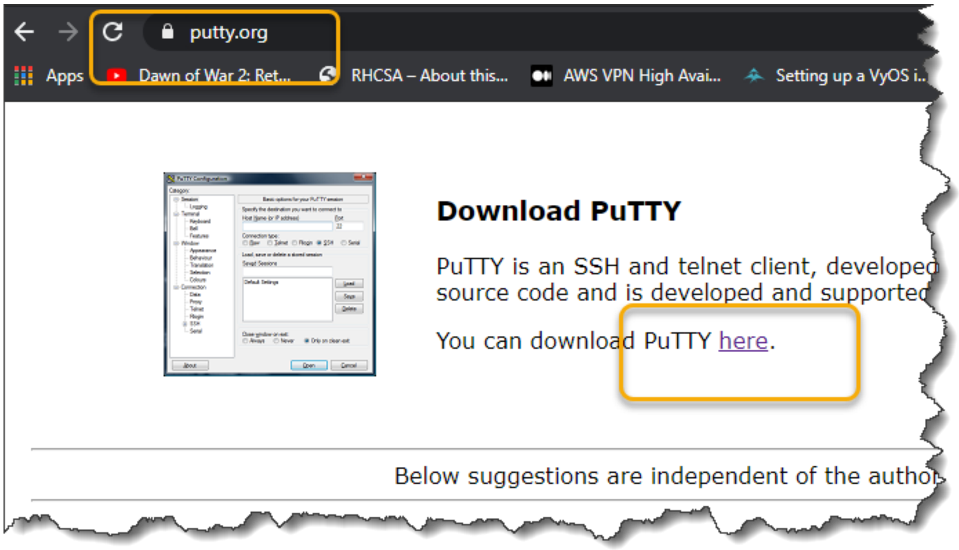
```
C:\Users\antza>ping 13.126.185.50

Pinging 13.126.185.50 with 32 bytes of data:
Reply from 13.126.185.50: bytes=32 time=28ms TTL=49
Reply from 13.126.185.50: bytes=32 time=25ms TTL=49
Reply from 13.126.185.50: bytes=32 time=26ms TTL=49

Ping statistics for 13.126.185.50:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 25ms, Maximum = 28ms, Average = 26ms
Control-C
^C
C:\Users\antza>
```

Task 2: SSH into the EC2 instance

1. We are now going to log into our instance. For Mac and Linux users run the following command to connect your instances. Make sure to use your public **IPv4** and your **Key pair** in the command.

```
chmod 500 hybridskill-app-server-key.pem
ssh -i hybridskill-app-server-key.pem ec2-user@13.126.115.88
```

3. For Windows users we are going to use a SSH client called Putty. Visit www.putty.org and click on download Putty **here.**



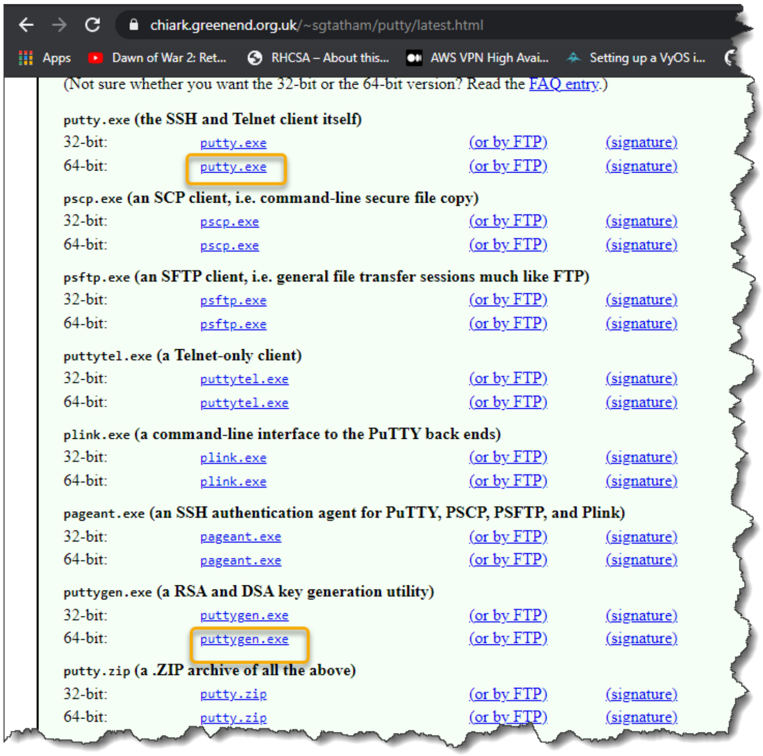
Download PuTTY

PuTTY is an SSH and telnet client, developed
source code and is developed and supported

You can download PuTTY here.

Below suggestions are independent of the author

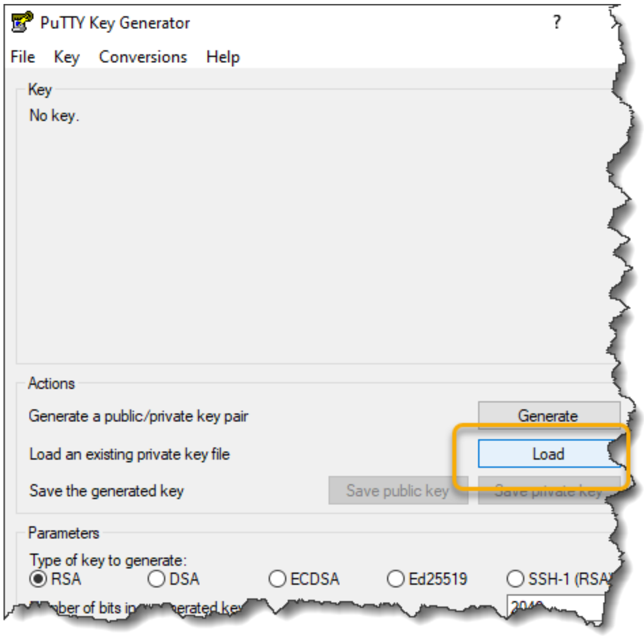
4. Download **putty.exe** and **puttygen.exe.**



(Not sure whether you want the 32-bit or the 64-bit version? Read the FAQ entry.)

putty.exe (the SSH and Telnet client itself)			
32-bit:	putty.exe	(or by FTP)	(signature)
64-bit:	putty.exe	(or by FTP)	(signature)
pscp.exe (an SCP client, i.e. command-line secure file copy)			
32-bit:	pscp.exe	(or by FTP)	(signature)
64-bit:	pscp.exe	(or by FTP)	(signature)
psftp.exe (an SFTP client, i.e. general file transfer sessions much like FTP)			
32-bit:	psftp.exe	(or by FTP)	(signature)
64-bit:	psftp.exe	(or by FTP)	(signature)
puttytel.exe (a Telnet-only client)			
32-bit:	puttytel.exe	(or by FTP)	(signature)
64-bit:	puttytel.exe	(or by FTP)	(signature)
plink.exe (a command-line interface to the PuTTY back ends)			
32-bit:	plink.exe	(or by FTP)	(signature)
64-bit:	plink.exe	(or by FTP)	(signature)
pageant.exe (an SSH authentication agent for PuTTY, PSCP, PSFTP, and Plink)			
32-bit:	pageant.exe	(or by FTP)	(signature)
64-bit:	pageant.exe	(or by FTP)	(signature)
puttygen.exe (a RSA and DSA key generation utility)			
32-bit:	puttygen.exe	(or by FTP)	(signature)
64-bit:	puttygen.exe	(or by FTP)	(signature)
putty.zip (a .ZIP archive of all the above)			
32-bit:	putty.zip	(or by FTP)	(signature)
64-bit:	putty.zip	(or by FTP)	(signature)

5. First open puttygen.exe. Click on **Generate**.



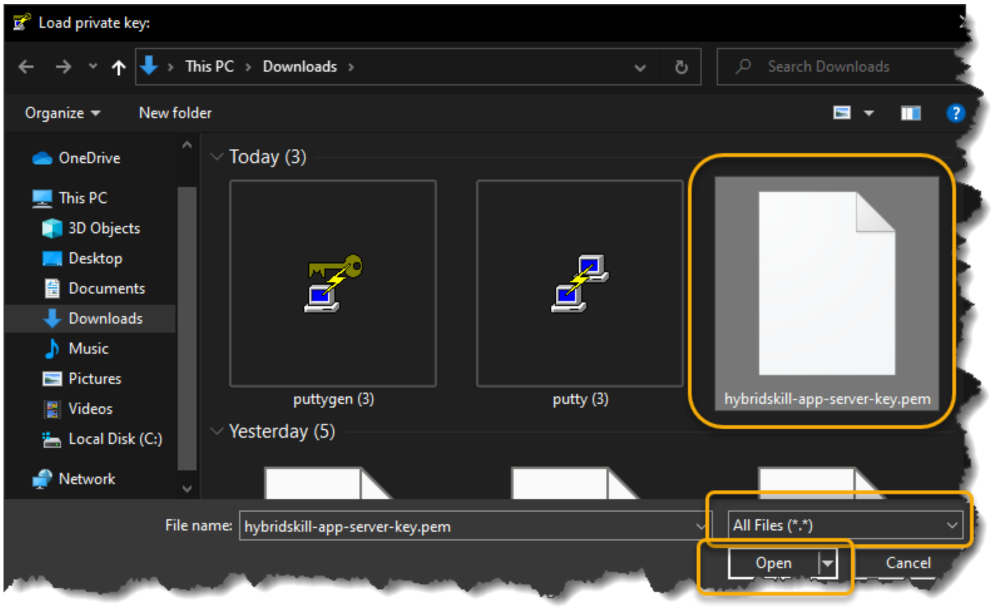
Key
No key.

Generate a public/private key pair
Load an existing private key file
Save the generated key

Type of key to generate:
● RSA ○ DSA ○ ECDSA ○ Ed25519 ○ SSH-1 (RSA

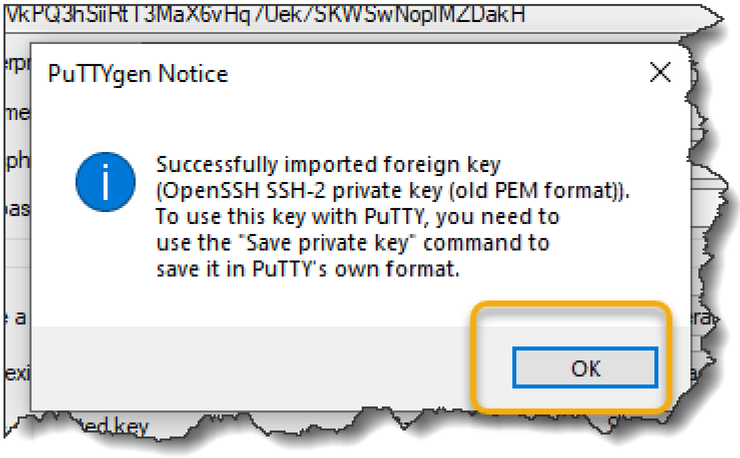
Number of bits in a generated key 2048

6. Select **All files** and then find and select your key you downloaded earlier. Click **Open**.



File name: hybridskill-app-server-key.pem
All Files (*.*)

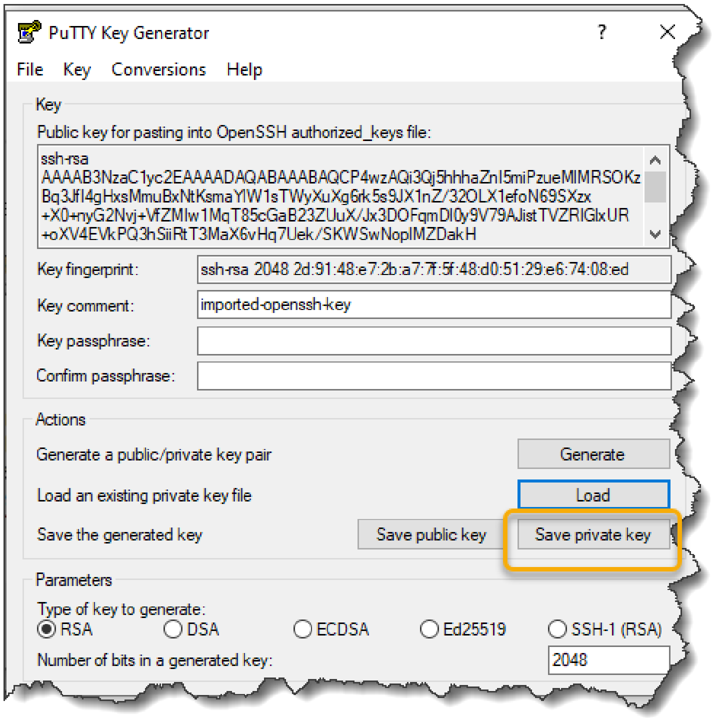
7. Your key should be successfully imported. Click **Ok**



PuTTYgen Notice

Successfully imported foreign key
(OpenSSH SSH-2 private key (old PEM format)).
To use this key with PuTTY, you need to
use the "Save private key" command to
save it in PuTTY's own format.

8. Next click Save Private key



PuTTY Key Generator

Key

Public key for pasting into OpenSSH authorized_keys file:

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQCP4wzAQi3Qj5hhhaZnI5miPzueMIMRSOKz
Bq3Jfl4gHxsMmuBxNtKsmaYlW1sTWyXuXg6rk5s9JX1nZ/32OLX1efoN69SXzx
+X0+nyG2Nvj+VfZMIw1MqT85cGaB23ZUuX/Jx3DOFqmDl0y9V79AJistTVZRIGlxUR
+oXV4EVkPQ3hSiiRtT3MaX6vHq7Uek/SKWSwNopIMZDakH
```

Key fingerprint: ssh-rsa 2048 2d:91:48:e7:2b:a7:7f:5f:48:d0:51:29:e6:74:08:ed

Key comment: imported-openssh-key

Key passphrase:

Confirm passphrase:

Actions

Generate a public/private key pair — Generate

Load an existing private key file — Load

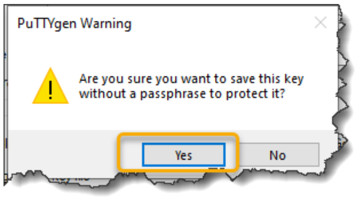
Save the generated key — Save public key — Save private key

Parameters

Type of key to generate:
● RSA ○ DSA ○ ECDSA ○ Ed25519 ○ SSH-1 (RSA)

Number of bits in a generated key: 2048

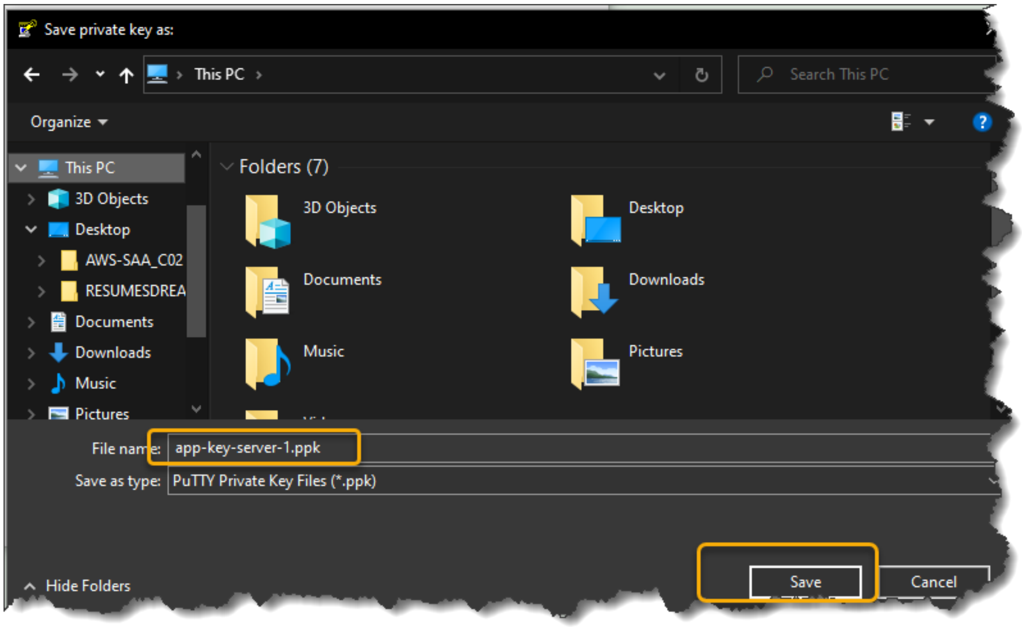
Click Yes to Save without a passphrase.



PuTTYgen Warning

Are you sure you want to save this key
without a passphrase to protect it?

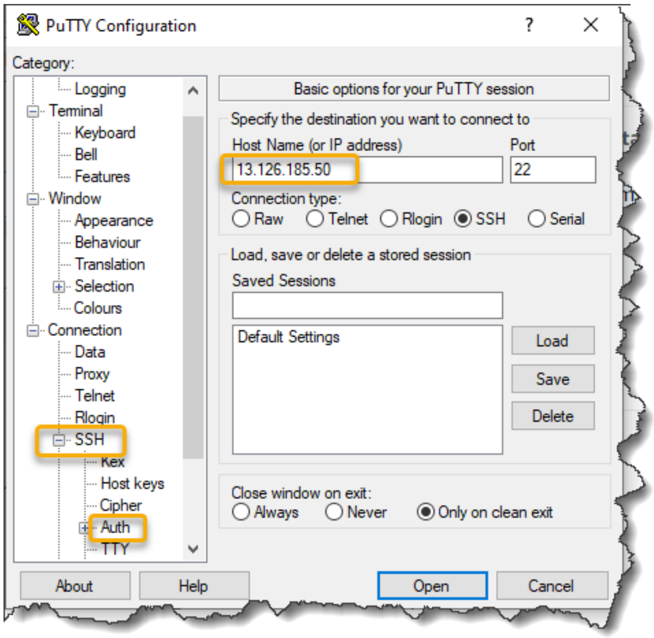
9. **Save** the key with a **.ppk** extension.



File name: app-key-server-1.ppk

Save as type: PuTTY Private Key Files (*.ppk)

10. Next Open putty.exe. Paste the **Public IP** of your instance(you copied earlier) in the **Host Name** field. Next expand **SSH** and click on **Auth.**



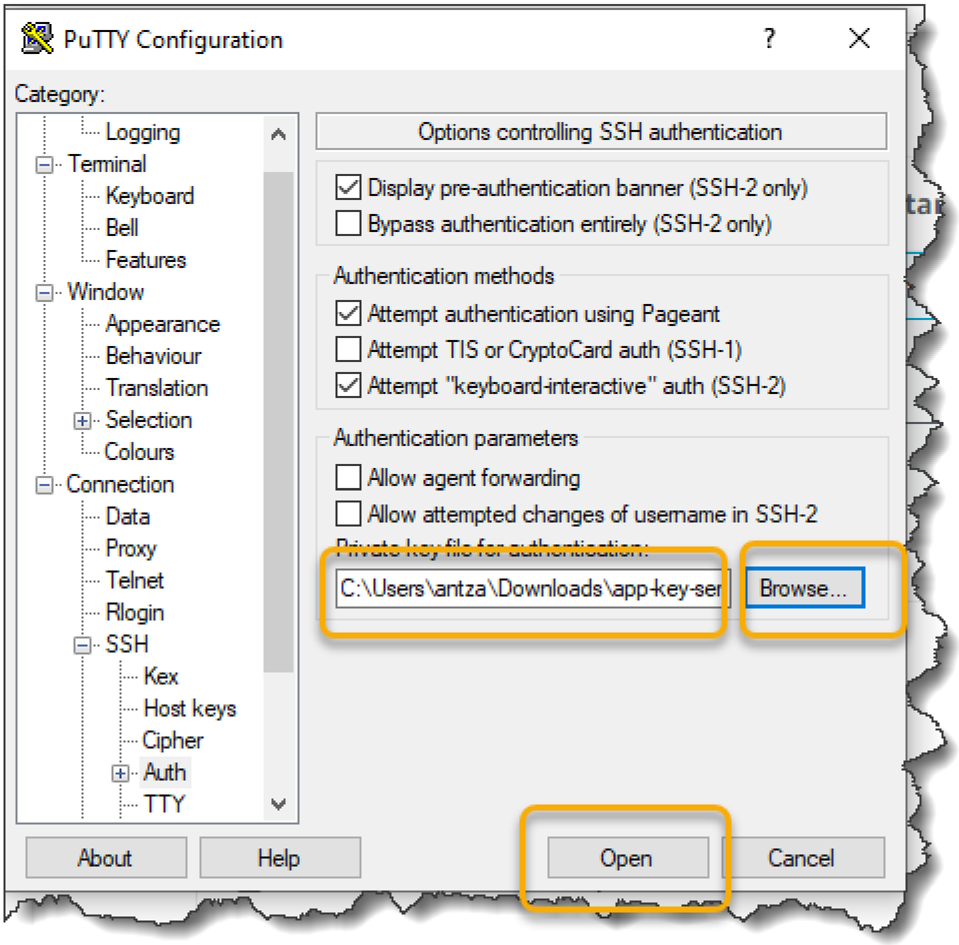
Host Name (or IP address): 13.126.185.50

Port: 22

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

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

11. Browse and select your **ppk** file you created earlier from **puttygen** and click **Open.**



PuTTY Configuration

Options controlling SSH authentication

☑ Display pre-authentication banner (SSH-2 only)
□ Bypass authentication entirely (SSH-2 only)

Authentication methods

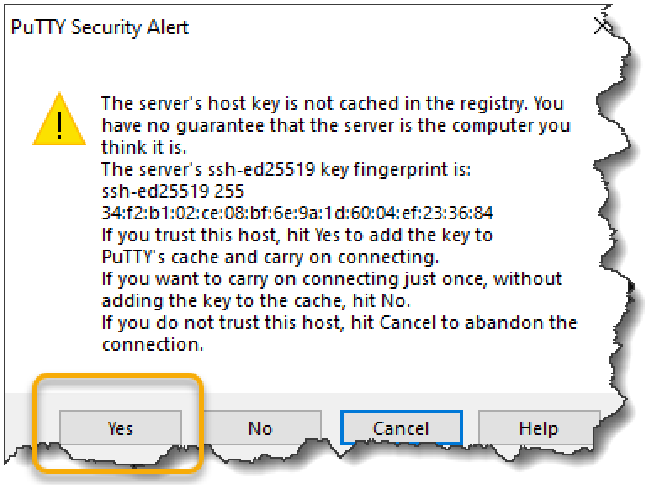
☑ Attempt authentication using Pageant
□ Attempt TIS or CryptoCard auth (SSH-1)
☑ Attempt "keyboard-interactive" auth (SSH-2)

Authentication parameters

□ Allow agent forwarding
□ Allow attempted changes of username in SSH-2

Private key file for authentication:
C:\Users\antza\Downloads\app-key-ser

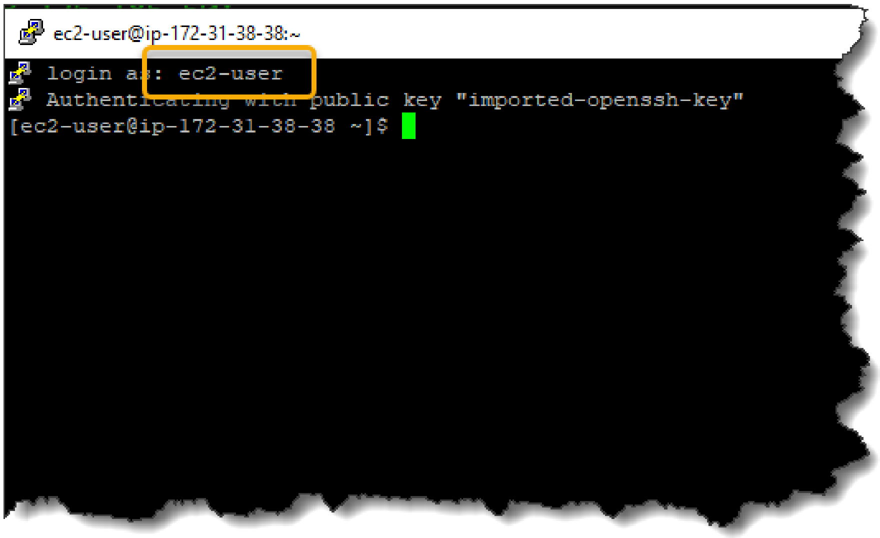
Click **Yes** to add the key to **Puttys** cache



PuTTY Security Alert

The server's host key is not cached in the registry. You have no guarantee that the server is the computer you think it is.
The server's ssh-ed25519 key fingerprint is:
ssh-ed25519 255
34:f2:b1:02:ce:08:bf:6e:9a:1d:60:04:ef:23:36:84
If you trust this host, hit Yes to add the key to PuTTY's cache and carry on connecting.
If you want to carry on connecting just once, without adding the key to the cache, hit No.
If you do not trust this host, hit Cancel to abandon the connection.

Enter the username as **ec2-user**

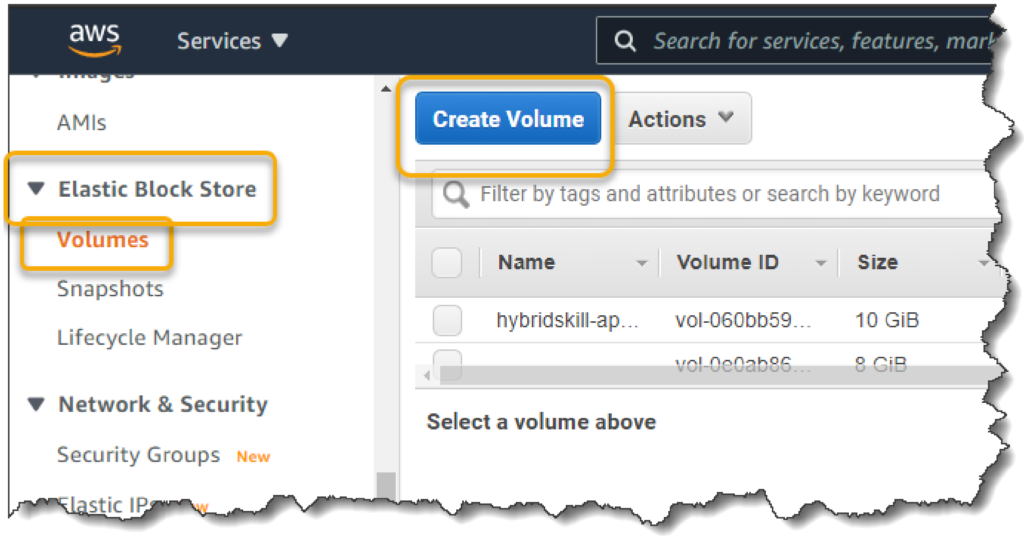


```
ec2-user@ip-172-31-38-38:~
login as: ec2-user
Authenticating with public key "imported-openssh-key"
[ec2-user@ip-172-31-38-38 ~]$
```

You should be logged into your machine.

Task 3: Create, attach an Elastic Block Store (EBS) volume

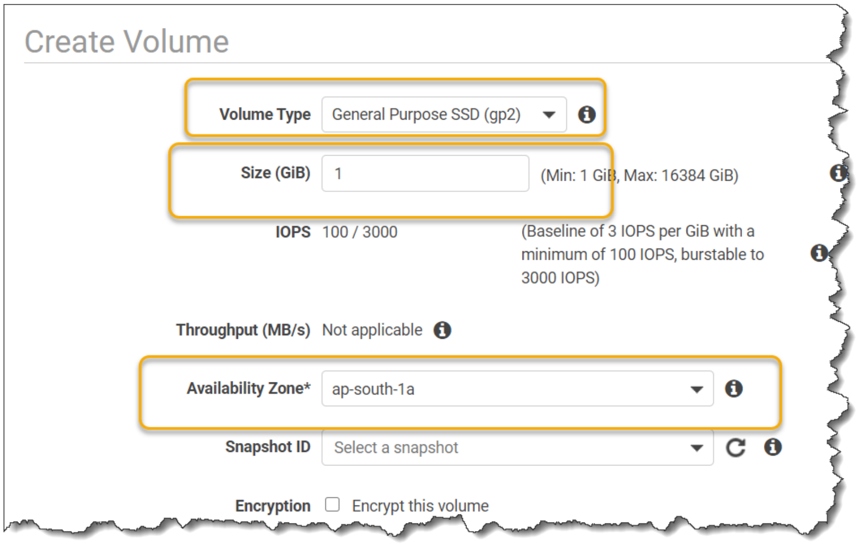
1. On the EC2 dashboard on the left hand side under **Elastic Block Store** click **Volumes** and then select **Create Volume**.



□	Name	Volume ID	Size
□	hybridskill-ap...	vol-060bb59...	10 GiB
□		vol-0e0ab86...	8 GiB

Select a volume above

2. Select the **Volume Type** as **General Purpose SSD (GP2)**, change the volume size as **1 GB,** select the zone **as ap-south-1a** *(This should be the same zone as your EC2 instance).*



Create Volume

Volume Type: General Purpose SSD (gp2)

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

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

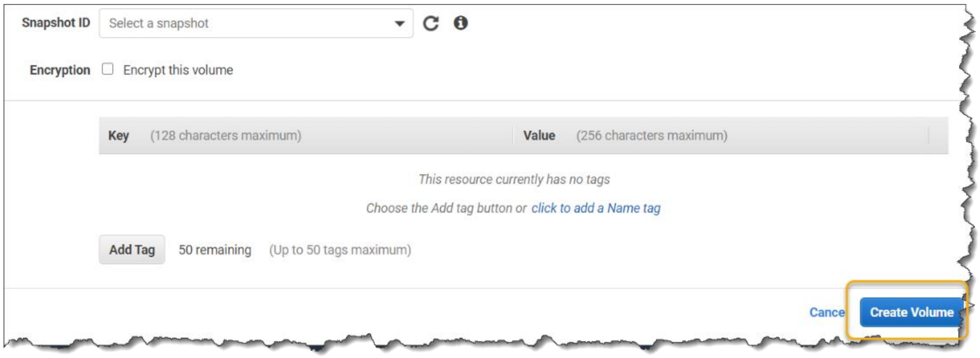
Throughput (MB/s): Not applicable

Availability Zone*: ap-south-1a

Snapshot ID: Select a snapshot

Encryption: □ Encrypt this volume

Leave other options as default and click **Create Volume**



Snapshot ID: Select a snapshot

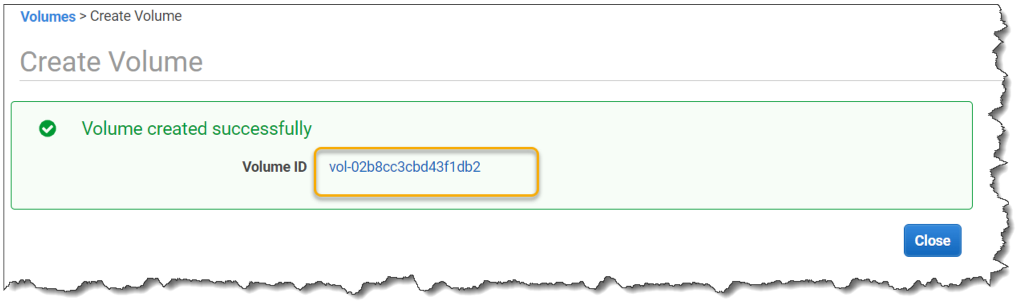
Encryption: □ Encrypt this volume

Key (128 characters maximum)	Value (256 characters maximum)

This resource currently has no tags

Choose the Add tag button or click to add a Name tag

3. Your volume should be created now. Click on the **Volume ID** to view your volume.



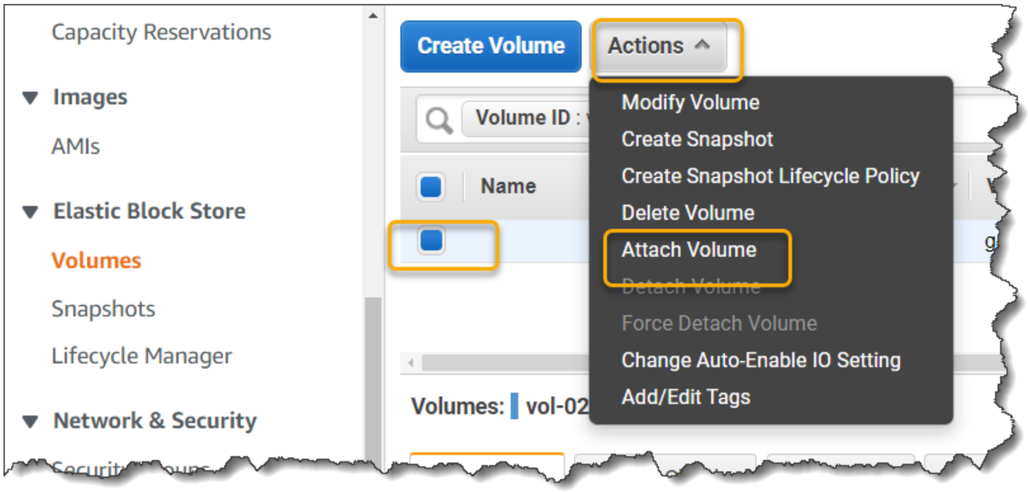
Volumes > Create Volume

Create Volume

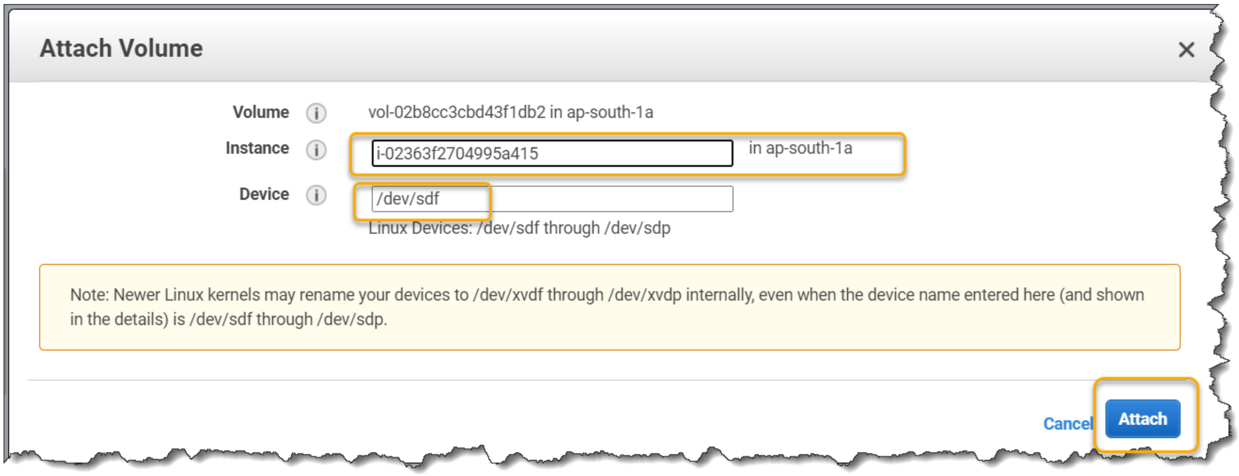
Volume created successfully

Volume ID: vol-02b8cc3cbd43f1db2

4. With your Volume selected, click **Actions** and click **Attach Volume.**



5. Select your **EC2 instance *(hybridskill app server)*** from the dropdown, leave the **Device** as **/dev/sdf** and click **Attach**.


Attach Volume

Volume: vol-02b8cc3cbd43f1db2 in ap-south-1a

Instance: i-02363f2704995a415 in ap-south-1a

Device: /dev/sdf

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

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

6. Login into your EC2 instance and run the following commands.

```
sudo mkfs -t ext4 /dev/xvdf
sudo mkdir /mnt/vol
sudo mount /dev/xvdf /mnt/vol
```

Task 4: Format and mount the EBS volume. Install Wordpress

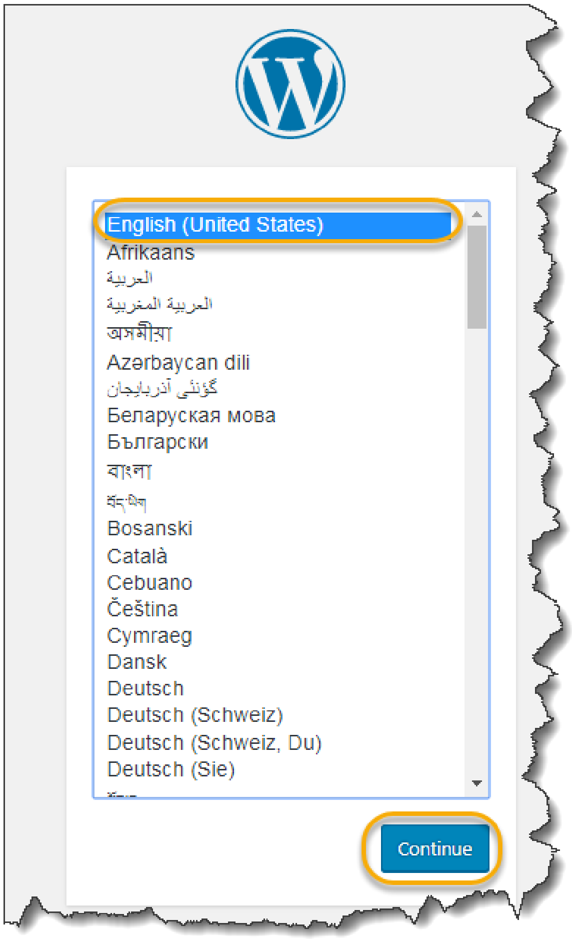
1. We are going to install an application called wordpress on the instance. For this we have to download a script

```
sudo yum install wget -y
sudo wget https://hybridskill-training.s3.amazonaws.com/wordpress.sh
```

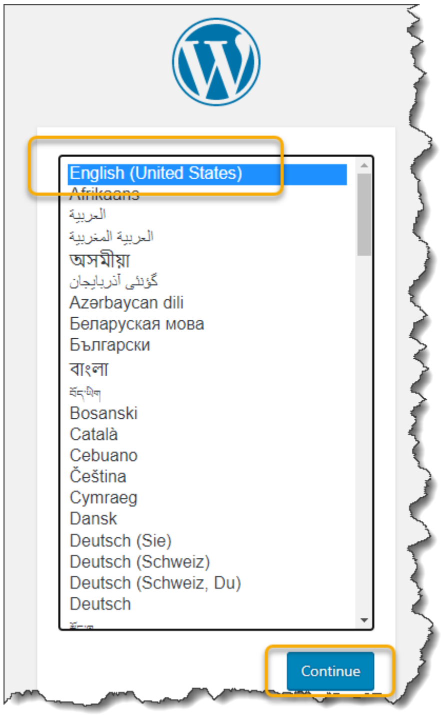
2. We are going to run the script.

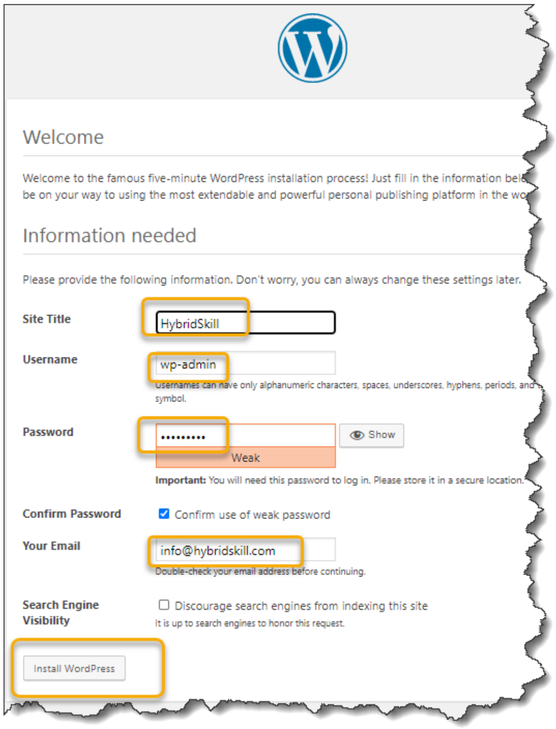
```
sudo chmod +x wordpress.sh
sudo bash wordpress.sh
```

3. Open the public IP of the instance on a browser. The wordpress installation wizard should begin Select the language as English and continue



4. Enter a name for your blog. Set a **Username** and the **Password.** Enter **Email address** and click **Install Wordpress.**





Welcome

Welcome to the famous five-minute WordPress installation process! Just fill in the information bel
be on your way to using the most extendable and powerful personal publishing platform in the wo

Information needed

Please provide the following information. Don't worry, you can always change these settings later.

Site Title: HybridSkill

Username: wp-admin

Usernames can have only alphanumeric characters, spaces, underscores, hyphens, periods, and
symbol.

Password: •••••••••• Show

Weak

Important: You will need this password to log in. Please store it in a secure location.

Confirm Password: ☑ Confirm use of weak password

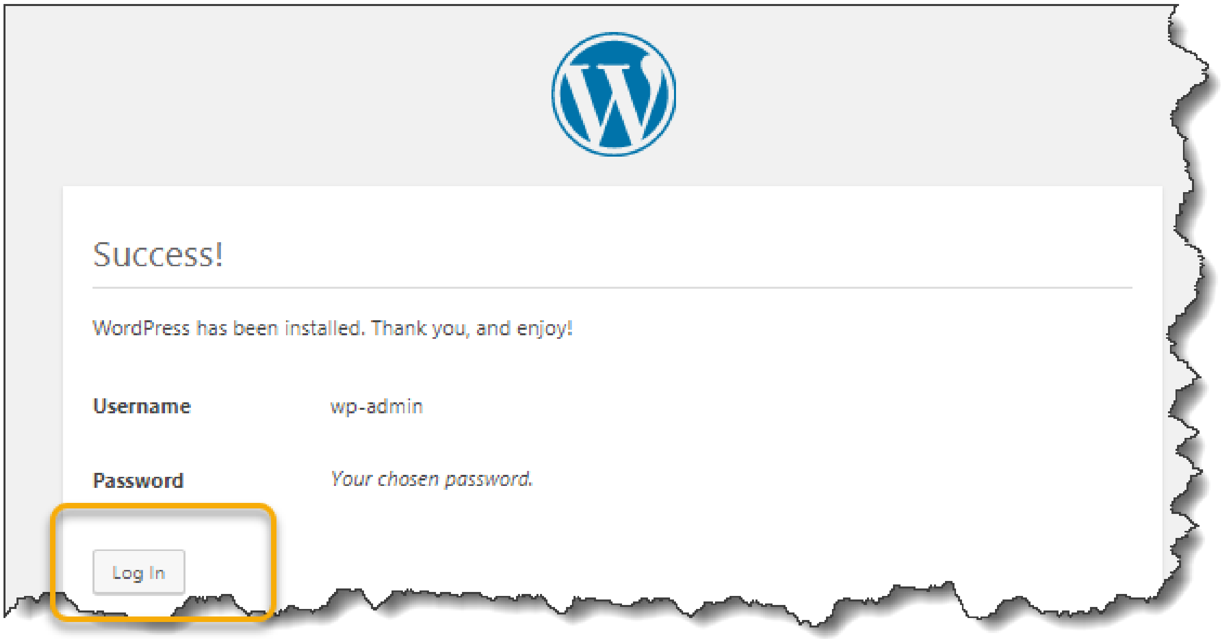
Your Email: info@hybridskill.com

Double-check your email address before continuing.

Search Engine Visibility: ☐ Discourage search engines from indexing this site

It is up to search engines to honor this request.

Install WordPress



Success!

WordPress has been installed. Thank you, and enjoy!

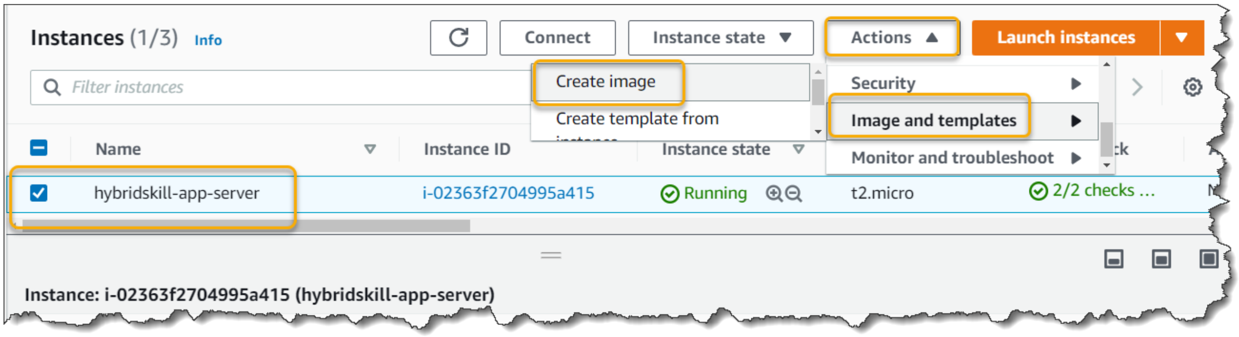
Username wp-admin

Password *Your chosen password.*

Task 5: Create Amazon Machine Image(AMI)

After successful installation, let's take an Image of your EC2 instance.

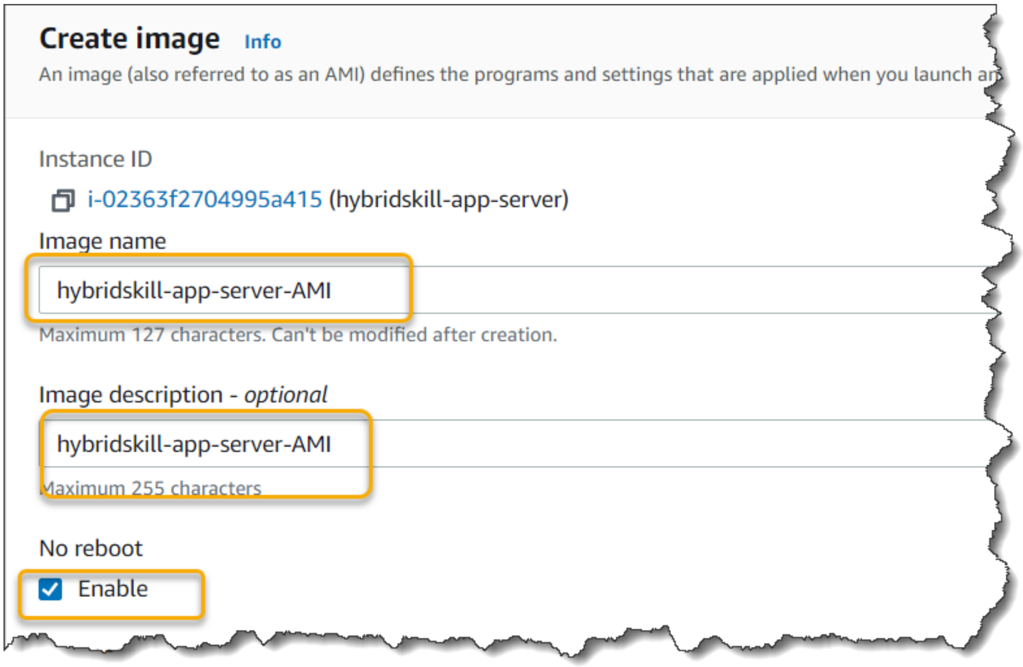
1. Select your instace. Click **Actions** and select **Image and tempaltes and click on Create Image.**



Name	Instance ID	Instance state	Instance type	Status check
☑ hybridskill-app-server	i-02363f2704995a415	Running	t2.micro	2/2 checks ...

Instance: i-02363f2704995a415 (hybridskill-app-server)

2. Enter **hybridskill-app-server-AMI** as the image name, enter a description, select **No reboot.**



Create image

An image (also referred to as an AMI) defines the programs and settings that are applied when you launch ar

Instance ID

i-02363f2704995a415 (hybridskill-app-server)

Image name

hybridskill-app-server-AMI

Maximum 127 characters. Can't be modified after creation.

Image description - *optional*

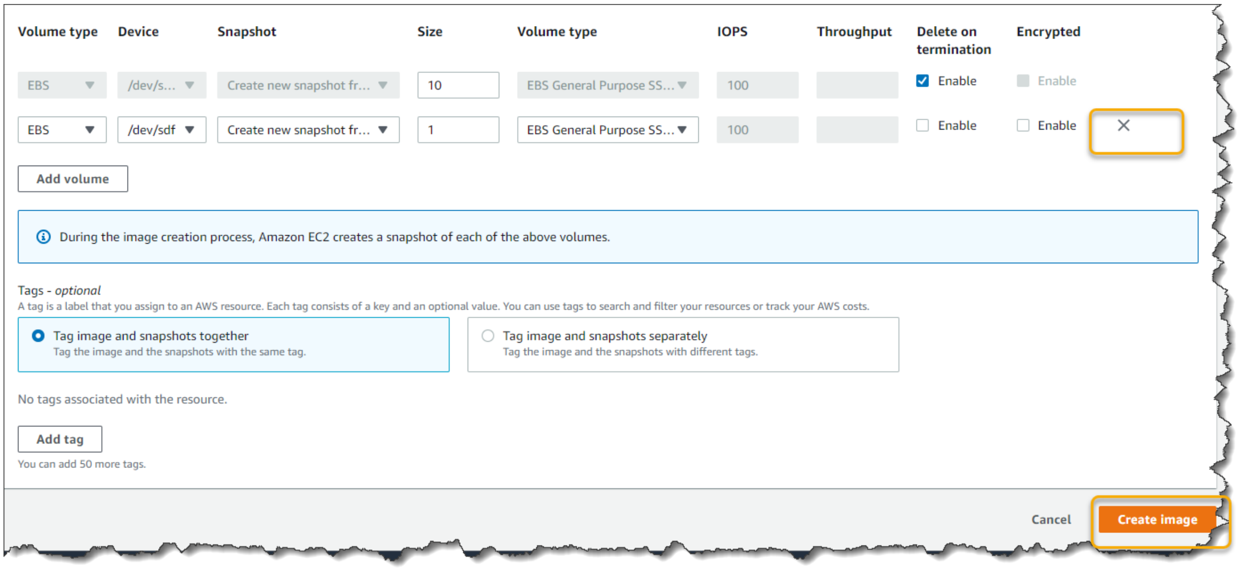
hybridskill-app-server-AMI

Maximum 255 characters

No reboot

☑ Enable

Delete the **1 GB** volume snapshot and click **Create Image.**



Volume type	Device	Snapshot	Size	Volume type	IOPS	Throughput	Delete on termination	Encrypted	
EBS ▼	/dev/s... ▼	Create new snapshot fr... ▼	10	EBS General Purpose SS... ▼	100		☑ Enable	□ Enable	
EBS ▼	/dev/sdf ▼	Create new snapshot fr... ▼	1	EBS General Purpose SS... ▼	100		□ Enable	□ Enable	✕

ⓘ During the image creation process, Amazon EC2 creates a snapshot of each of the above volumes.

Tags - *optional*

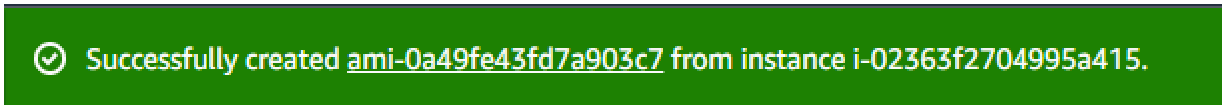
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

● Tag image and snapshots together
Tag the image and the snapshots with the same tag.

○ Tag image and snapshots separately
Tag the image and the snapshots with different tags.

No tags associated with the resource.

You can add 50 more tags.



Successfully created ami-0a49fe43fd7a903c7 from instance i-02363f2704995a415.

Task 6: Manage EC2 through CLI

Now that we have explored EC2 through the console, let’s do the same through the CLI. Run the following commands on the command line interface, you had setup earlier.

1. Create Security group (by default SG will be created into default VPC)

```
:~$ aws ec2 create-security-group --group-name hybridskill-sg-test --description
"created via awscli"
{
    "GroupId": "sg-59d67832"
}
```

2. Add an ingress rule for port 22

```
:~$ aws ec2 authorize-security-group-ingress --group-name  hybridskill-sg-test   --
protocol tcp --port 22 --cidr 106.206.52.76/32
```

3. Describe SG:

```
:~$ aws ec2 describe-security-groups --group-name hybridskill-sg-test
{   "SecurityGroups": [
        {
            "IpPermissionsEgress": [
                {   "IpProtocol": "-1",
                    "IpRanges": [
                        {
                            "CidrIp": "0.0.0.0/0"
                        }
                    ],
                    "UserIdGroupPairs": [],
                    "PrefixListIds": []
                }
            ],
            "Description": "created via awscli",
            "IpPermissions": [
                {
                    "PrefixListIds": [],
                    "FromPort": 22,
                    "IpRanges": [
                        {
                            "CidrIp": "106.206.52.76/32"
                        }
                    ],
                    "ToPort": 22,
                    "IpProtocol": "tcp",
                    "UserIdGroupPairs": []
                }
            ],
            "GroupName": "hybridskill-sg-test",
            "VpcId": "vpc-d6a00fbe",
            "OwnerId": "123456789123",
            "GroupId": "sg-59d67832"
        }
    ]
}
```

4. Create Key-pair:

```
:~$  aws ec2 create-key-pair --key-name hybridskill-test --query 'KeyMaterial' --
output text > hybridskill-test.pem
```

5. Launch EC2 instance. Create a file for user data, this user data script will run at bootup time.

```
:~$ cat wordpress.sh
#!/bin/bash
yum update -y
yum -y install httpd wget php php-pear php-mysql php-gd mysql wget
yum -y install mariadb-server mariadb
yum install bash-completion -y
systemctl enable httpd.service
systemctl start httpd.service
systemctl enable mariadb
systemctl start mariadb.service
mysql -u root -e "create database wordpressdb";
mysql -u root -e "GRANT ALL PRIVILEGES ON wordpressdb.* TO 'root'@'localhost'
  IDENTIFIED BY 'hybridskill@123'";
mysql -u root -phybridskill@123 -e "FLUSH PRIVILEGES;"
wget -c http://wordpress.org/latest.tar.gz
wget https://s3.ap-south-1.amazonaws.com/hybridskill/wp-config.php
tar -xzvf latest.tar.gz
rsync -av wordpress/* /var/www/html/
mv wp-config.php /var/www/html
sed -i 's/^\(SELINUX\s*=\s*\).*$/\1disabled/' /etc/selinux/config
rm -rf latest.tar.gz wordpress
find /var/www/html -type f -exec chmod 0664 {} \;
find /var/www/html -type d -exec chmod 2775 {} \;
chown -R apache:apache /var/www/html
echo "Rebooting..........!!!!!!!!!!!!!!!!"
reboot
```

6. Launch box with extra EBS volume and note down instance ID.

```
aws ec2 run-instances --image-id ami-e60e5a89 --count 1 --instance-type t2.micro --
key-name hybridskill-test --security-groups hybridskill-sg-test --block-device-
mappings
"[{\"DeviceName\":\"/dev/sdf\",\"Ebs\":{\"VolumeSize\":20,\"DeleteOnTermination\":fals
e}}]" --user-data file://./wordpress.sh
```

7. You can mount EBS via user data also. Run following commands to mount on EC2 instance:

```
sudo mkfs -t ext4 /dev/xvdf
sudo mkdir /mnt/vol
sudo mount /dev/xvdf /mnt/vol
```

8. Open the public IP of the instance on a browser and setup the wordpress.
9. Create AMI of box

```
aws ec2 create-image --instance-id i-0a457c3c8696213ad --name "wordpress_AMI" --
description "An AMI for my wp server"  --no-reboot
 {
  "ImageId": "ami-0e356a61"
}
```

Important: Cleanup of all Resources

Next let’s follow this checklist make sure all resources are cleaned up. to prevent billing to your account.

- **EC2 instances**
- **EBS volumes**
- **Elastic Ips**

Keep the AMI we will use it in the next lab