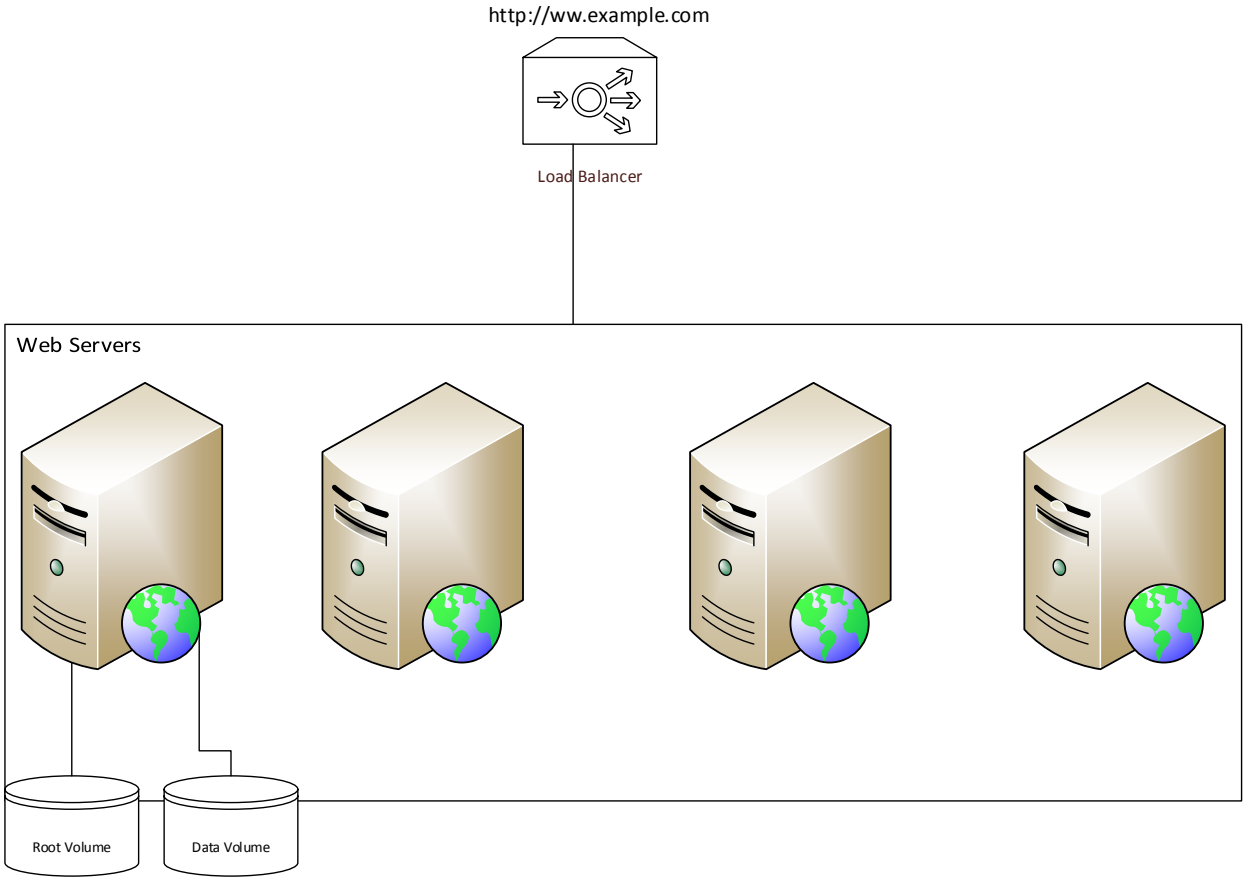
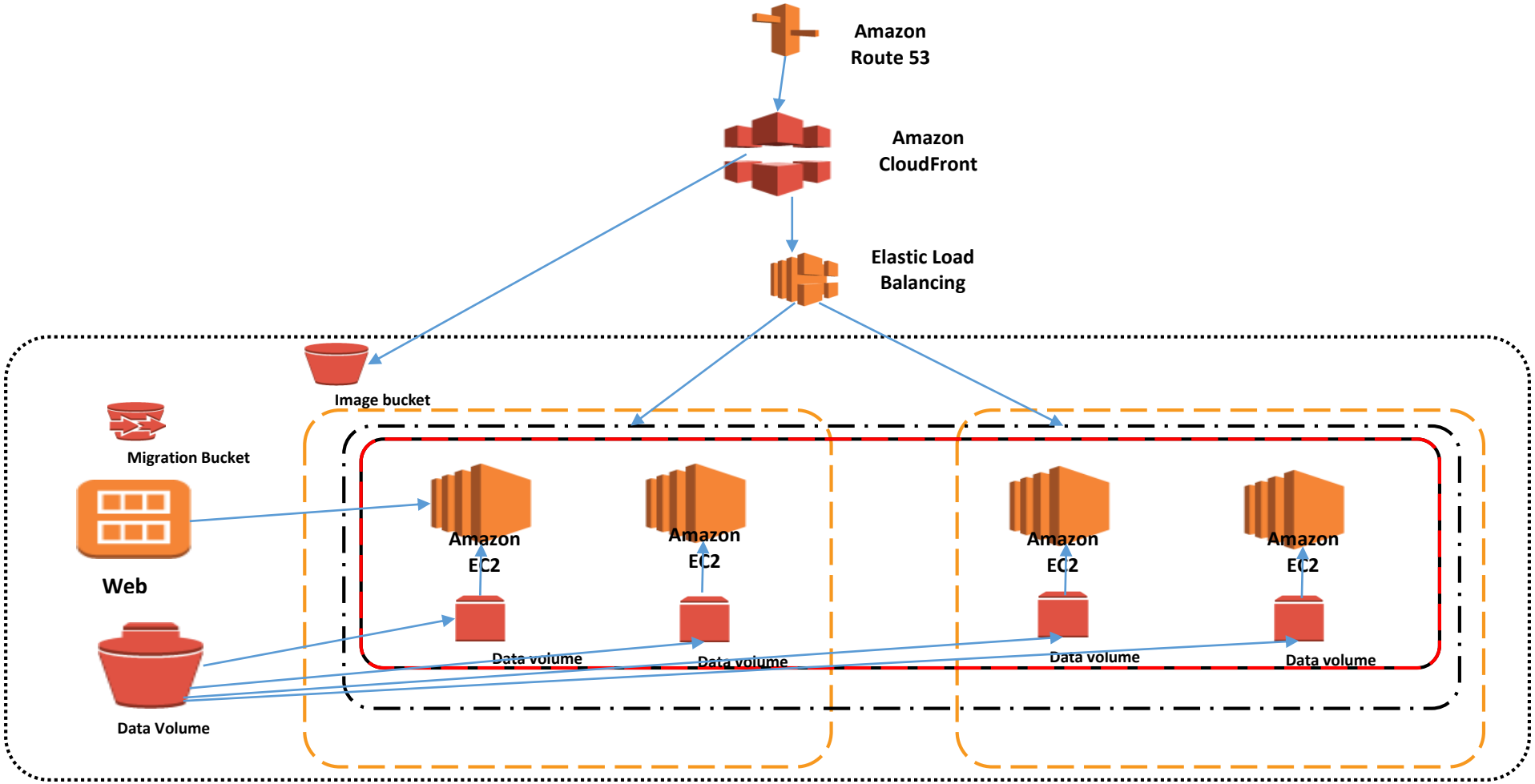
Hands on lab for VM migration

This Lab is to migrate a Web Servers Running on your premises to AWS Cloud

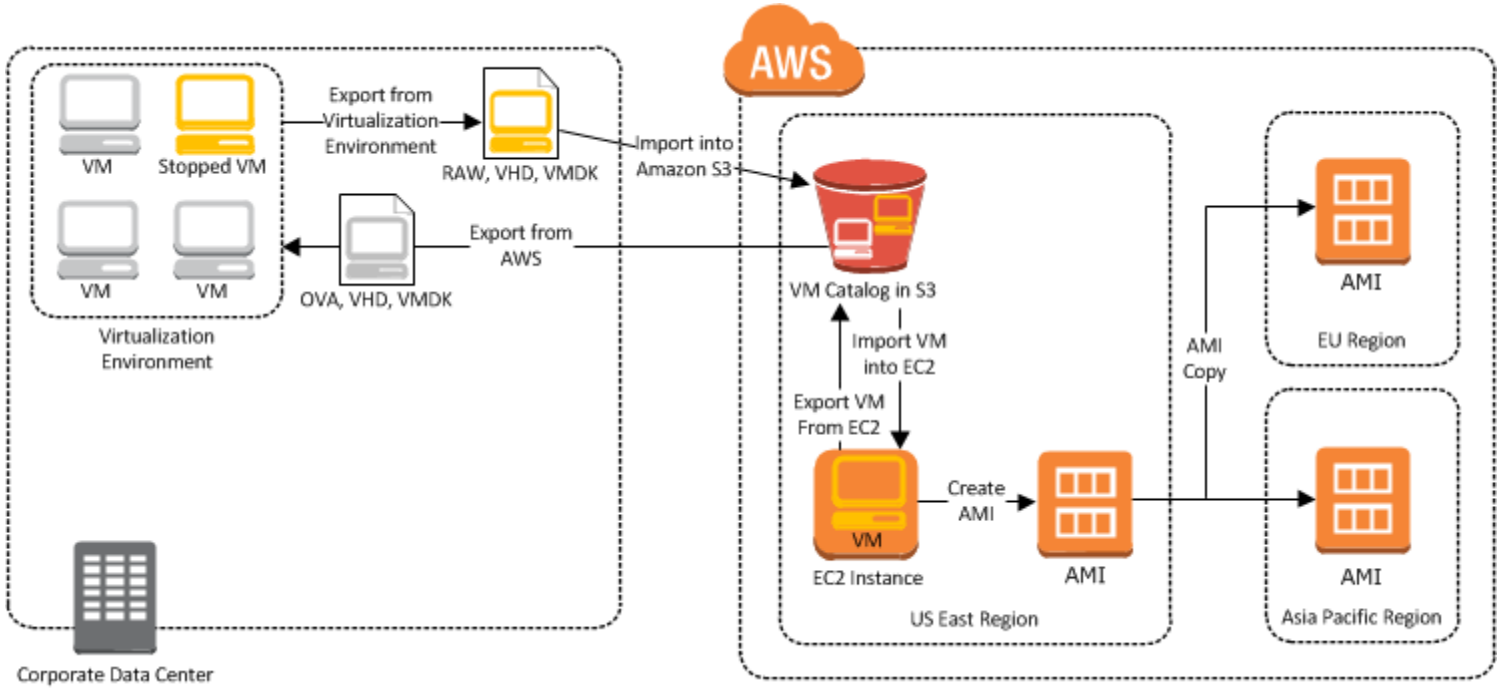
On Premise Architecture



AWS Architecture



Step 1: Import On Premise Image to AWS



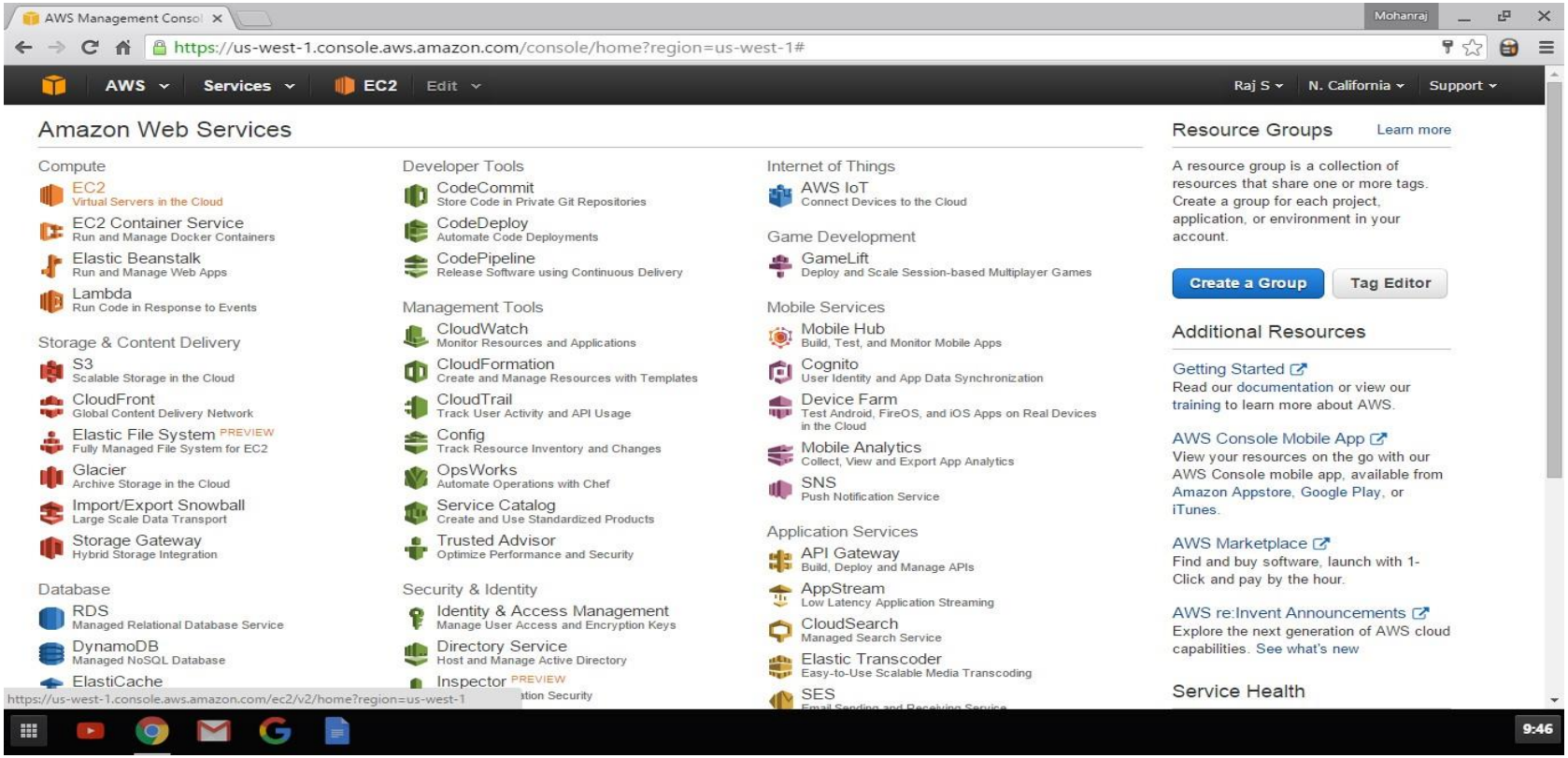
1) Install AWS CLI and EC2 CLI
   Refer the Document Install AWS Command line document to install locally, In this lab we will use AWS build server to do the job which will have AWS cli preinstalled

2) Start a AWS Linux Build Instance in AWS.

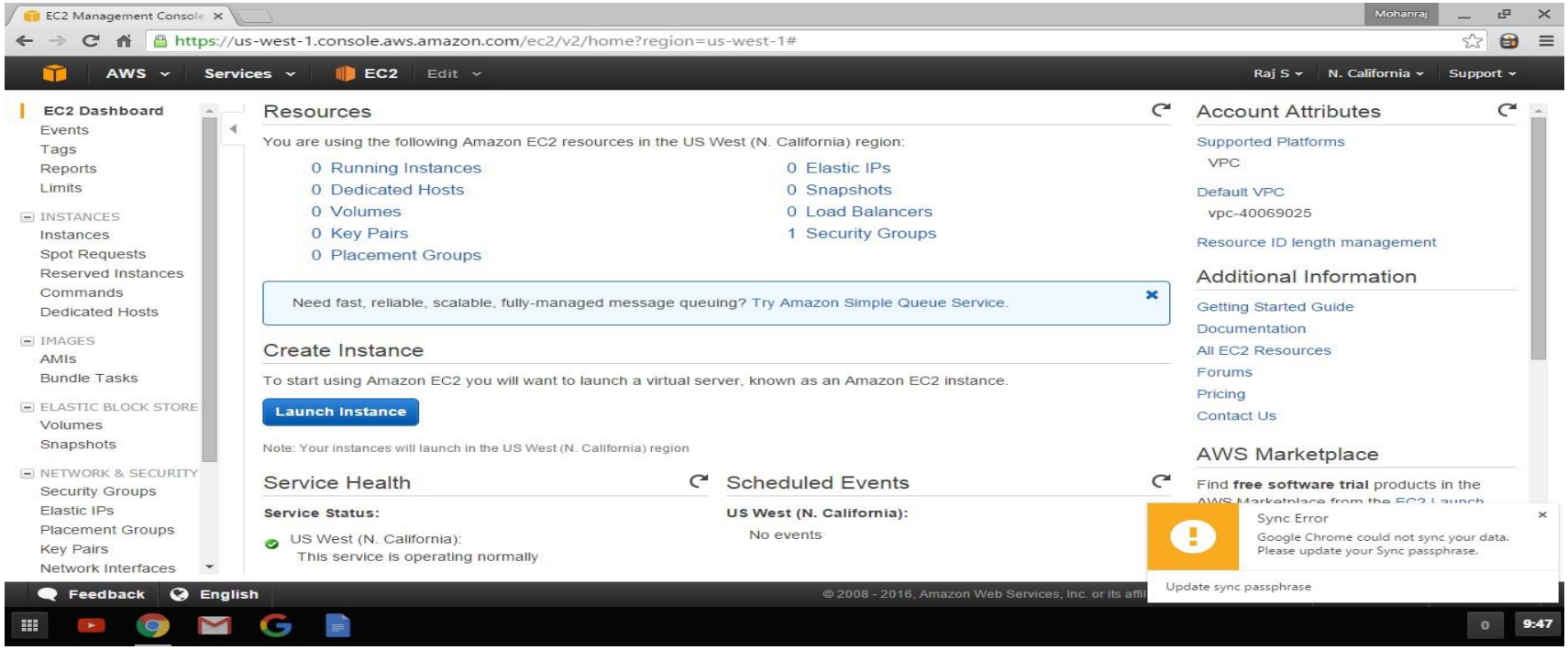
Open Console

https://console.aws.amazon.com/console/home

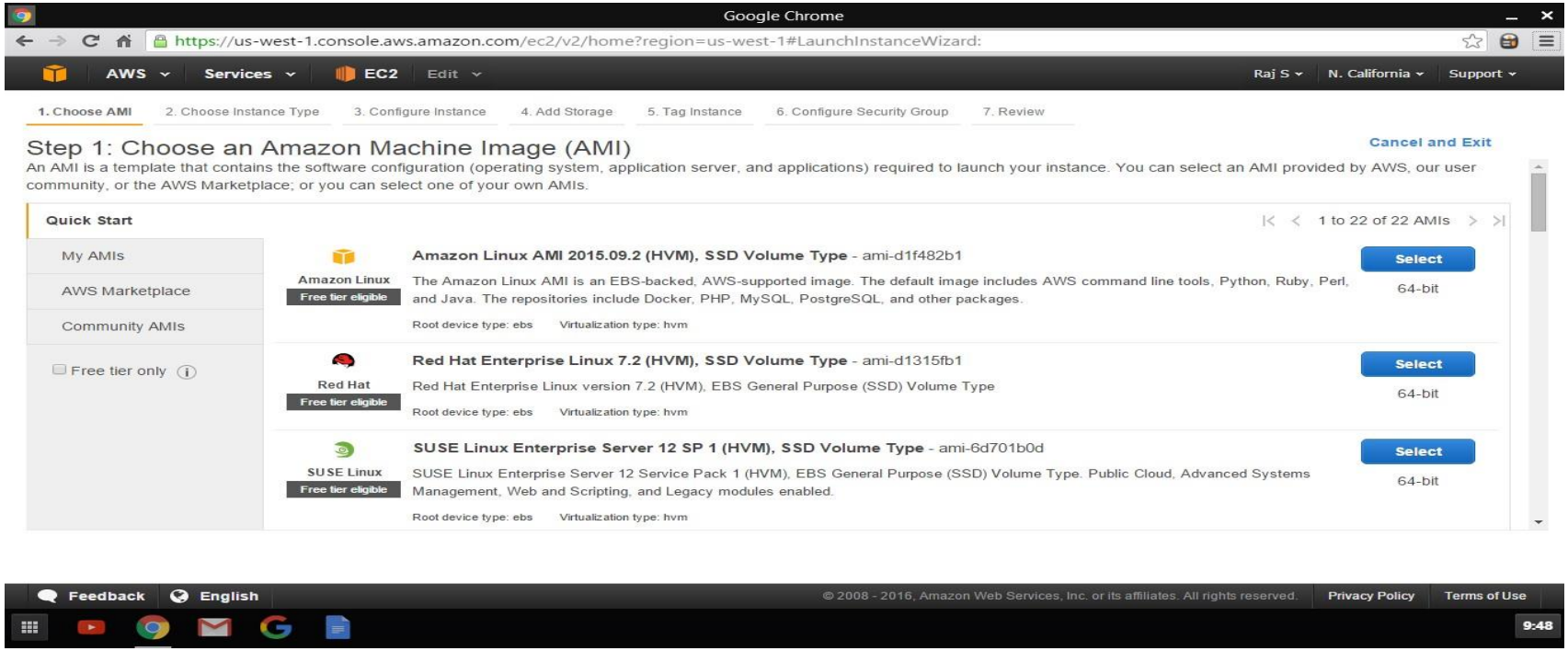
Click EC2 to create Instance or VM



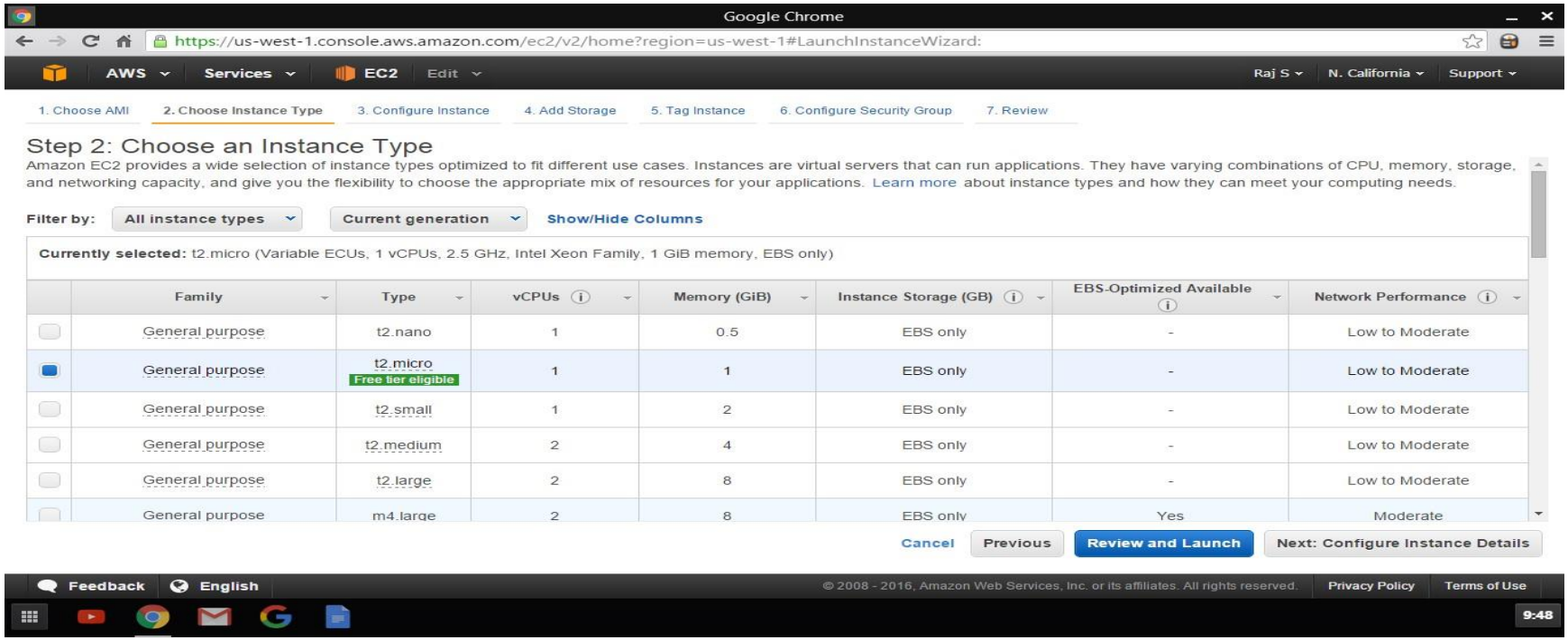
Click Launch Instance



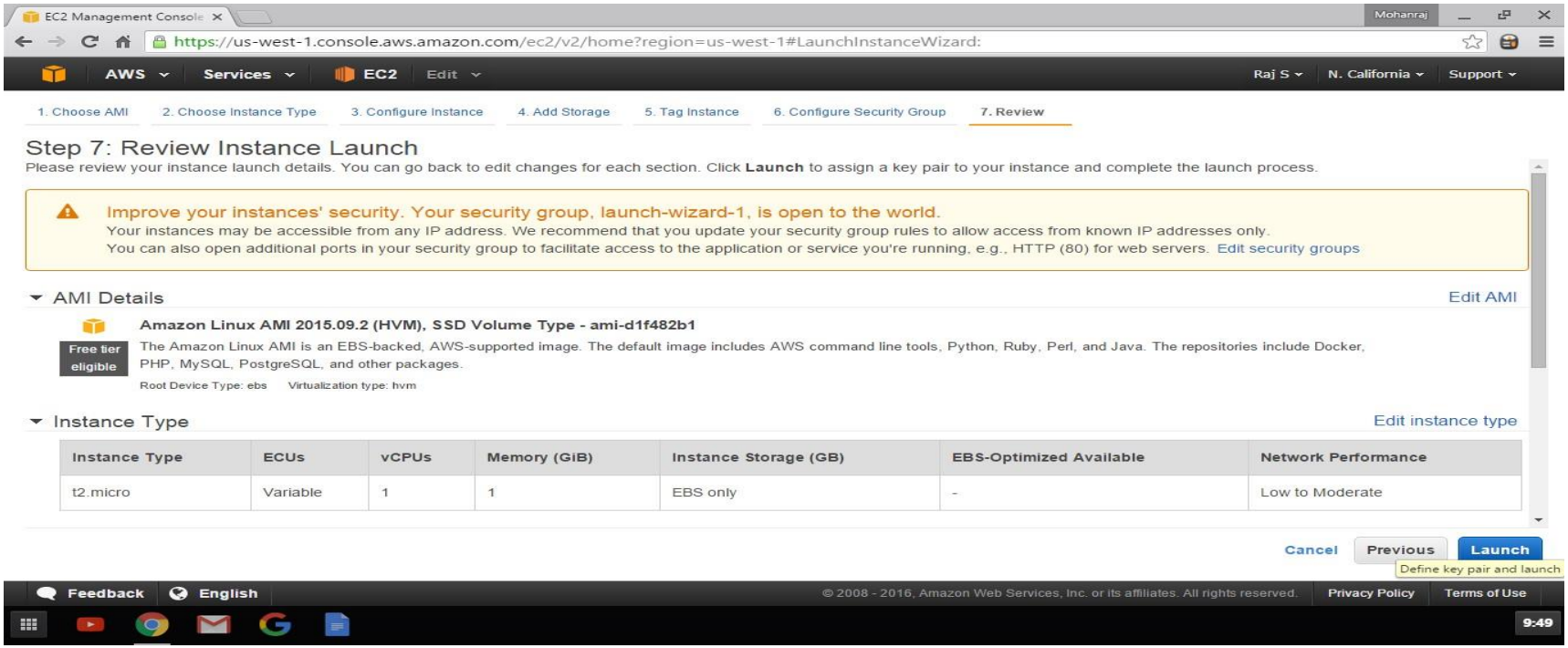
Select Amazon Linux AMI


Google Chrome
https://us-west-1.console.aws.amazon.com/ec2/v2/home?region=us-west-1#LaunchInstanceWizard:
AWS
Services
EC2
Edit
Raj S
N. California
Support
1. Choose AMI
2. Choose Instance Type
3. Configure Instance
4. Add Storage
5. Tag Instance
6. Configure Security Group
7. Review
Step 1: Choose an Amazon Machine Image (AMI)
Cancel and Exit
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.
Quick Start
1 to 22 of 22 AMIs
My AMIs
AWS Marketplace
Community AMIs
Free tier only
Amazon Linux
Free tier eligible
Amazon Linux AMI 2015.09.2 (HVM), SSD Volume Type - ami-d1f482b1
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
Select
64-bit
Red Hat
Free tier eligible
Red Hat Enterprise Linux 7.2 (HVM), SSD Volume Type - ami-d1315fb1
Red Hat Enterprise Linux version 7.2 (HVM), EBS General Purpose (SSD) Volume Type
Root device type: ebs
Virtualization type: hvm
Select
64-bit
SUSE Linux
Free tier eligible
SUSE Linux Enterprise Server 12 SP 1 (HVM), SSD Volume Type - ami-6d701b0d
SUSE Linux Enterprise Server 12 Service Pack 1 (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
Select
64-bit
Feedback
English
© 2008 - 2016, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
9:48

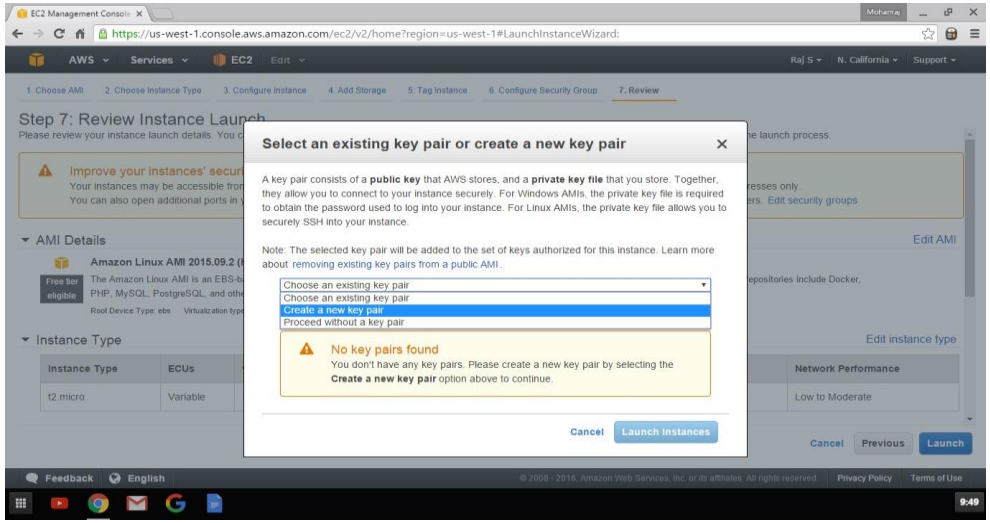
Choose T2.Micro and clock Review and Launch

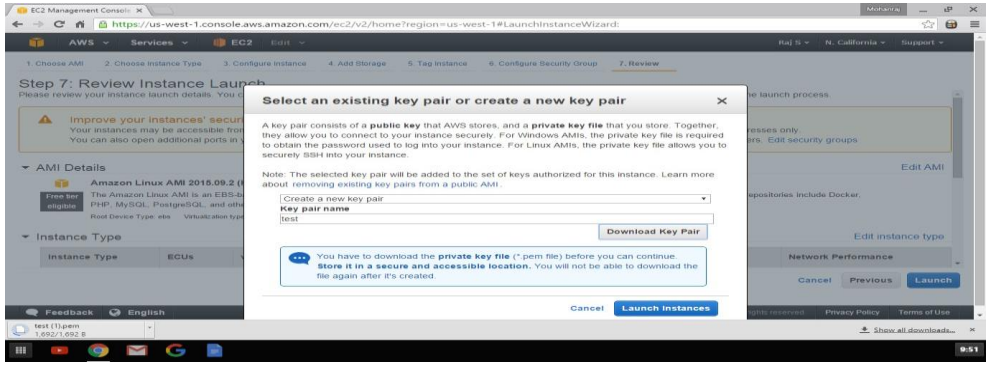


Click Launch in Review Screen

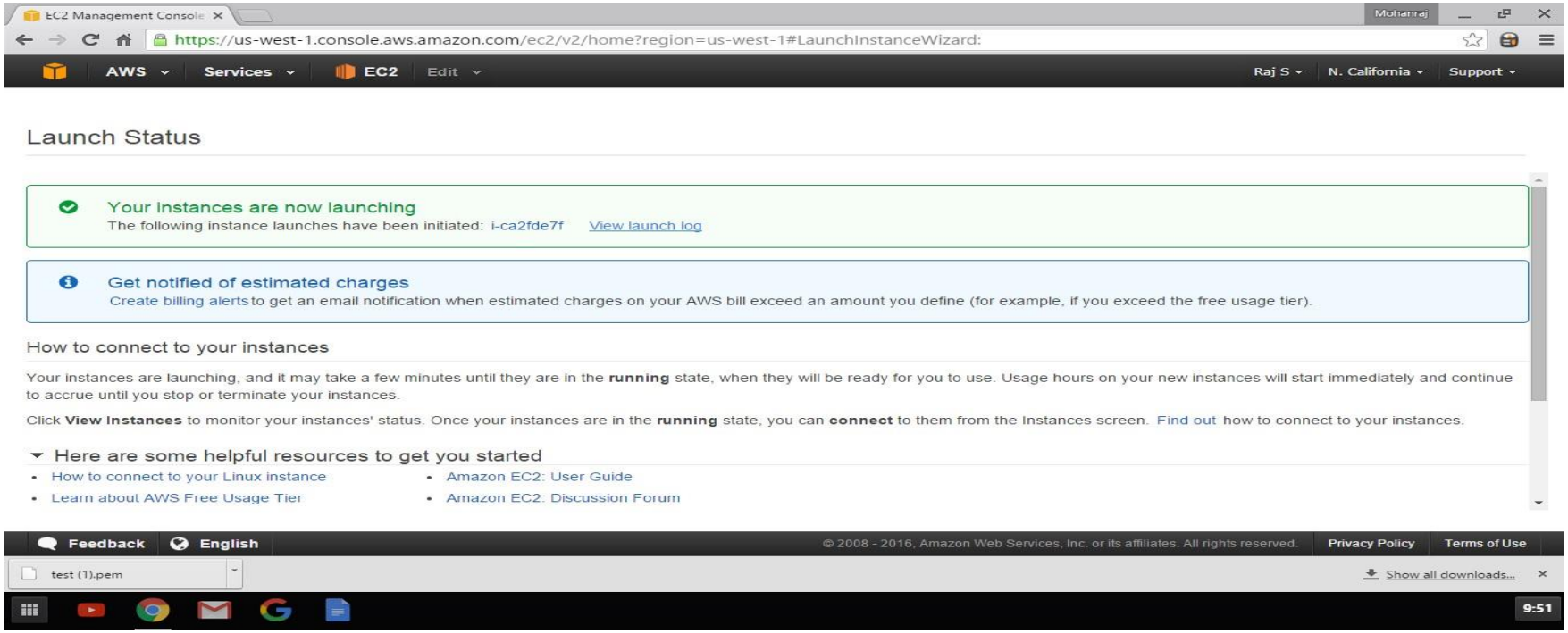


Choose Create New Key Pair and provide Name and Download Key

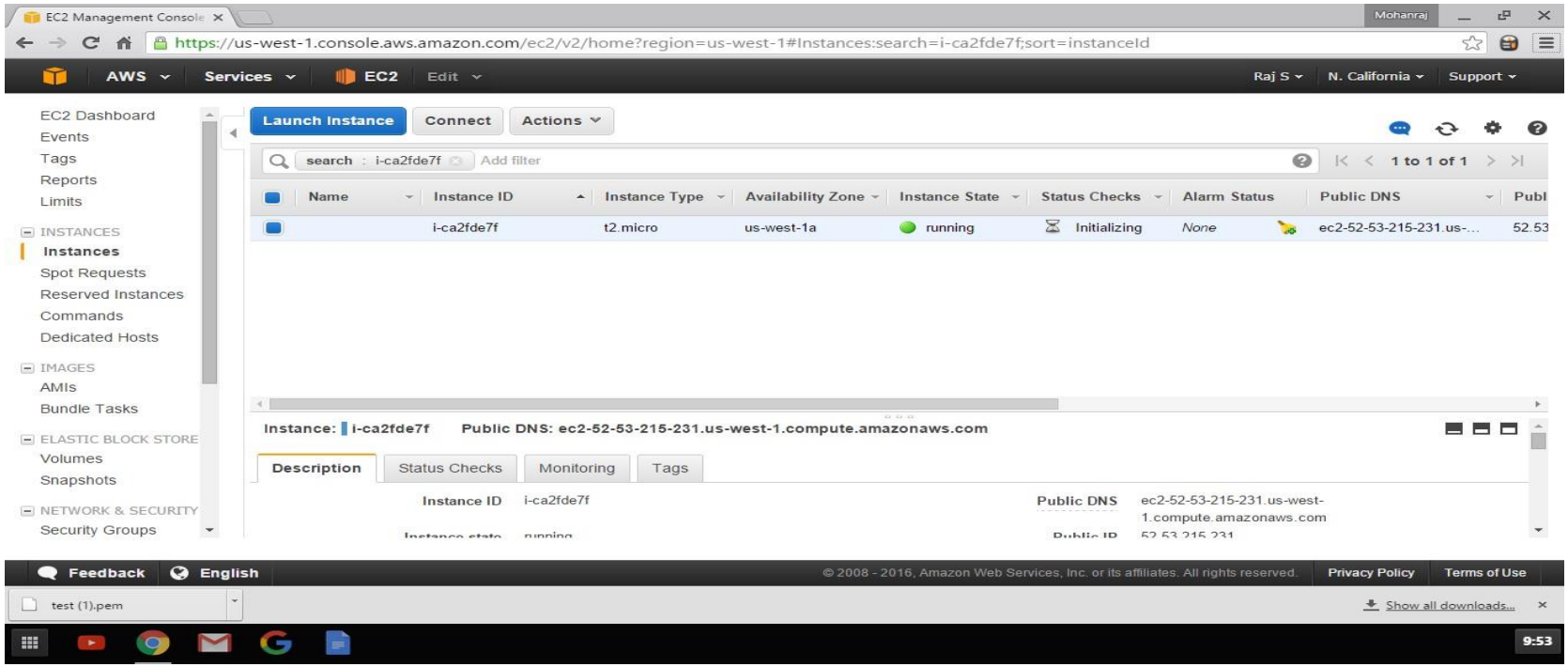


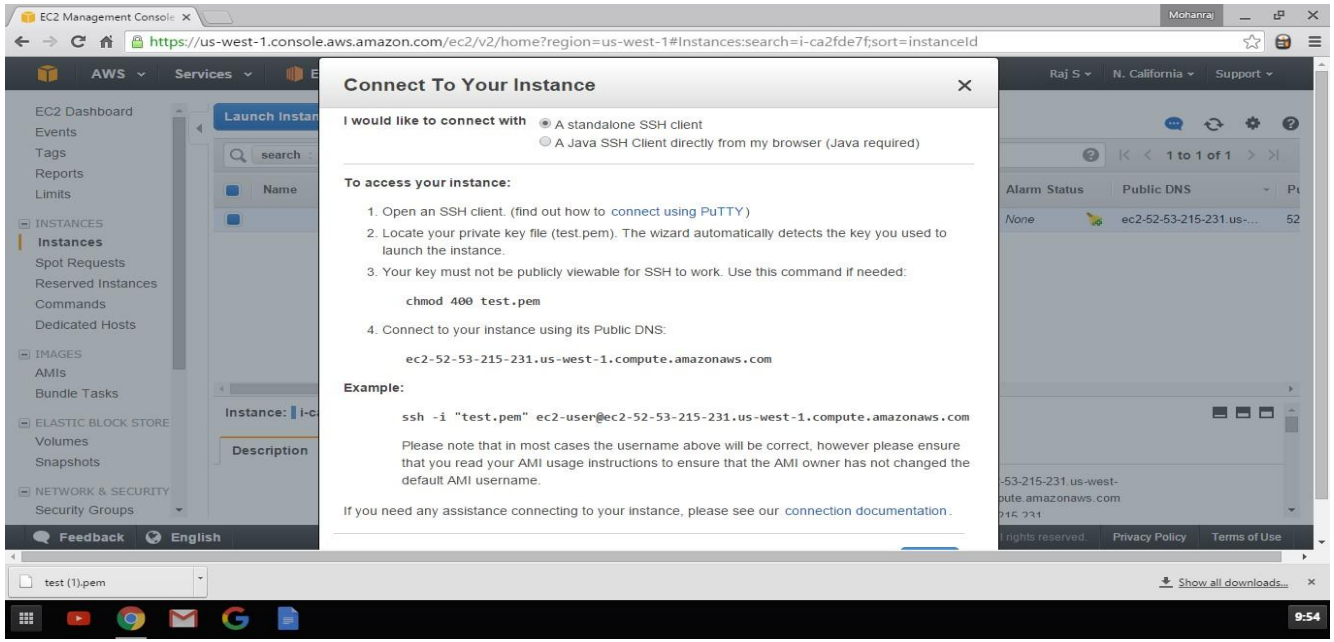


Click view instance Id i-xxxxxxx to take you EC2 Console



Click Connect tab to find the Options to connect




EC2 Management Console
Mohanraj
https://us-west-1.console.aws.amazon.com/ec2/v2/home?region=us-west-1#Instances:search=i-ca2fde7f;sort=instanceId
AWS
Services
Raj S
N. California
Support
EC2 Dashboard
Events
Tags
Reports
Limits
INSTANCES
Instances
Spot Requests
Reserved Instances
Commands
Dedicated Hosts
IMAGES
AMIs
Bundle Tasks
ELASTIC BLOCK STORE
Volumes
Snapshots
NETWORK & SECURITY
Security Groups
Launch Instan
search
Name
Instance: i-c
Description
1 to 1 of 1
Alarm Status
Public DNS
None
ec2-52-53-215-231.us-...
Connect To Your Instance
I would like to connect with
A standalone SSH client
A Java SSH Client directly from my browser (Java required)
To access your instance:
1. Open an SSH client. (find out how to connect using PuTTY)
2. Locate your private key file (test.pem). The wizard automatically detects the key you used to launch the instance.
3. Your key must not be publicly viewable for SSH to work. Use this command if needed:
chmod 400 test.pem
4. Connect to your instance using its Public DNS:
ec2-52-53-215-231.us-west-1.compute.amazonaws.com
Example:
ssh -i "test.pem" ec2-user@ec2-52-53-215-231.us-west-1.compute.amazonaws.com
Please note that in most cases the username above will be correct, however please ensure that you read your AMI usage instructions to ensure that the AMI owner has not changed the default AMI username.
If you need any assistance connecting to your instance, please see our connection documentation.
Feedback
English
Privacy Policy
Terms of Use
test (1).pem
Show all downloads...
9:54

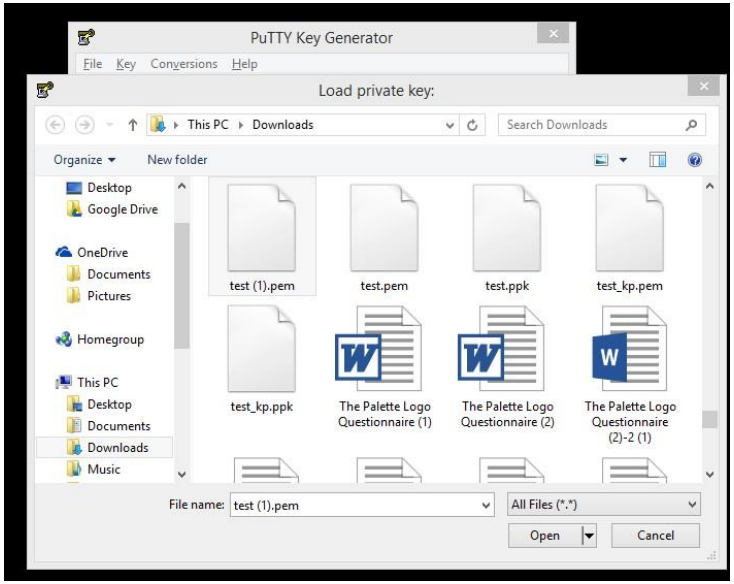
Connecting using Putty

Download Putty and PuttyGen from the below URL http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

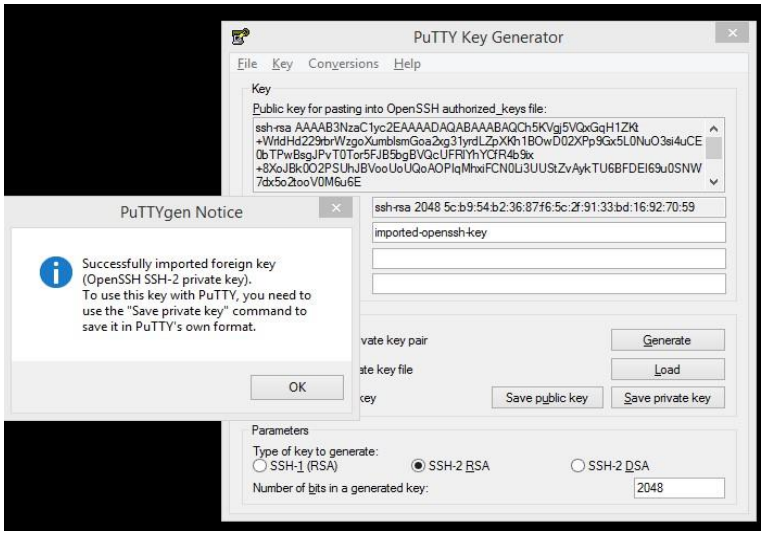
Open PuttyGen

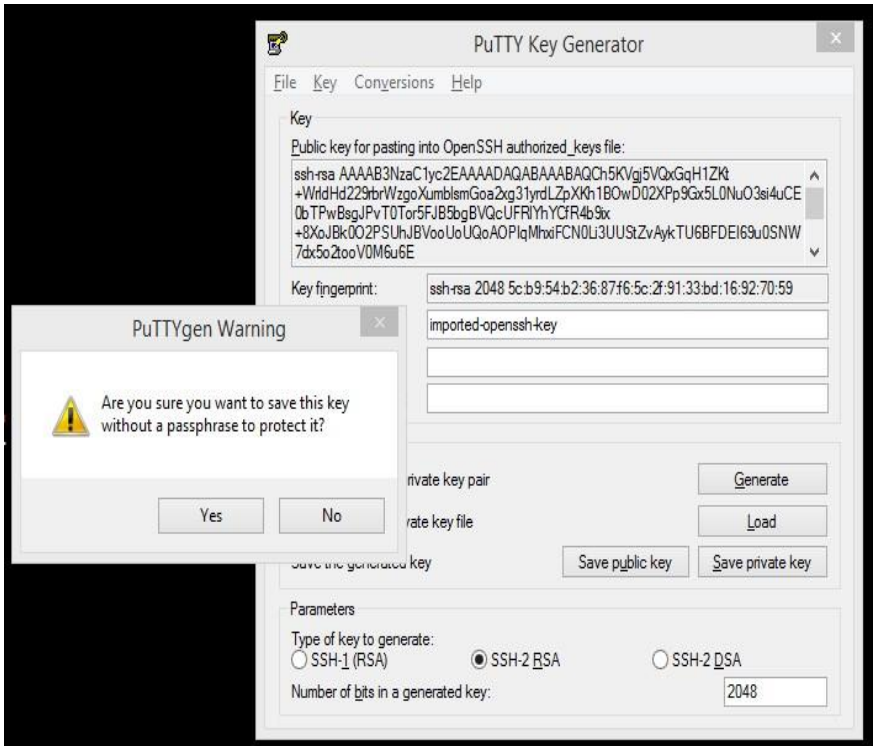
Open Putty Key Generator

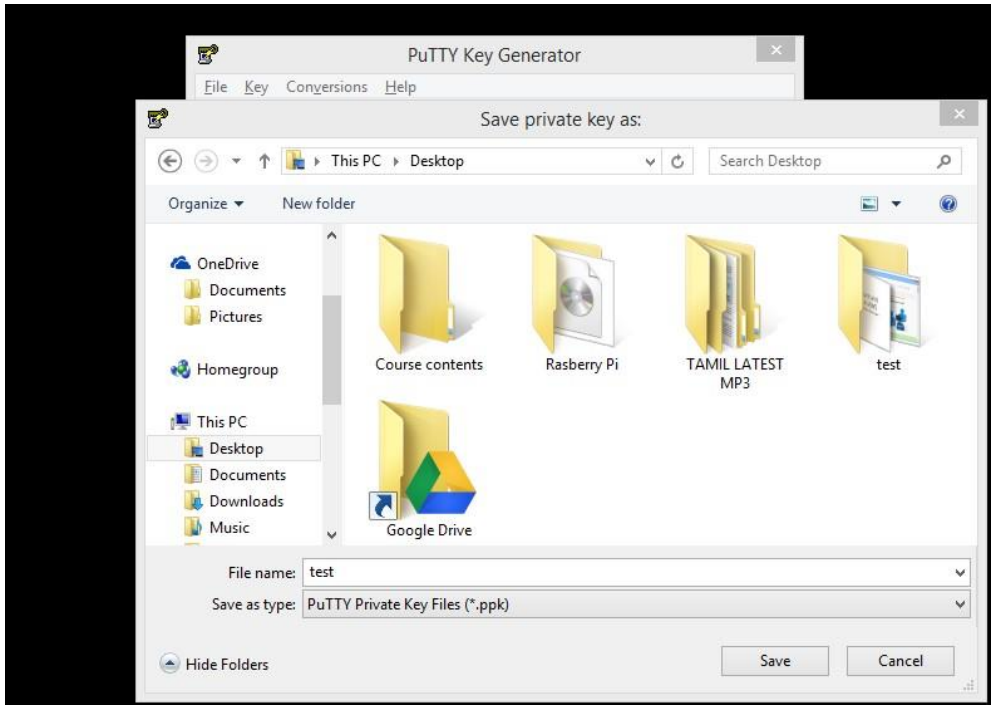
Click Load and lead the PEM File downloaded while creating the Instance
Select All Files to show the .pem files


PuTTY Key Generator
File Key Conversions Help
Load private key:
This PC ▸ Downloads
Search Downloads
Organize
New folder
Desktop
Google Drive
OneDrive
Documents
Pictures
Homegroup
This PC
Desktop
Documents
Downloads
Music
test (1).pem
test.pem
test.ppk
test_kp.pem
test_kp.ppk
The Palette Logo Questionnaire (1)
The Palette Logo Questionnaire (2)
The Palette Logo Questionnaire (2)-2 (1)
File name: test (1).pem
All Files (*.*)
Open
Cancel

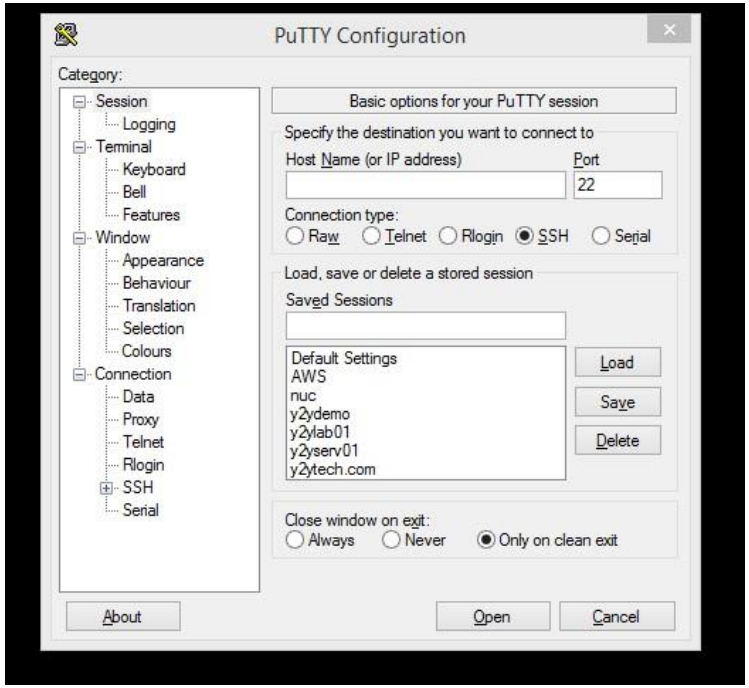
Use Save private key to Save it in PPK Format which Putty Understands



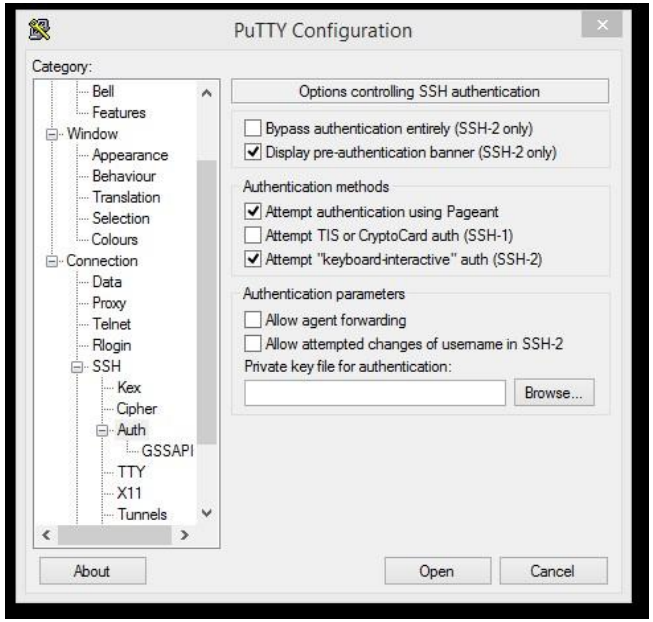

PuTTY Key Generator
File Key Conversions Help
Key
Public key for pasting into OpenSSH authorized_keys file:
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCh5KVgj5VQxGqH1ZKt
+WrldHd229rbrWzgoXumblsmGoa2xg31yrdLZpXKh1BOwD02XPp9Gx5L0NuO3si4uCE
0bTPwBsgJPvT0Tor5FJB5bgBVQcUFRlYhYCfR4b9ix
+8XoJBk0O2PSUhJBVooUoUQoAOPIqMhxiFCN0Li3UUStZvAykTU6BFDEI69u0SNW
7dx5o2tooV0M6u6E
Key fingerprint:
ssh-rsa 2048 5c:b9:54:b2:36:87:f6:5c:2f:91:33:bd:16:92:70:59
imported-openssh-key
Generate
Load
Save public key
Save private key
Parameters
Type of key to generate:
SSH-1 (RSA)
SSH-2 RSA
SSH-2 DSA
Number of bits in a generated key:
2048
PuTTYgen Warning
Are you sure you want to save this key
without a passphrase to protect it?
Yes
No

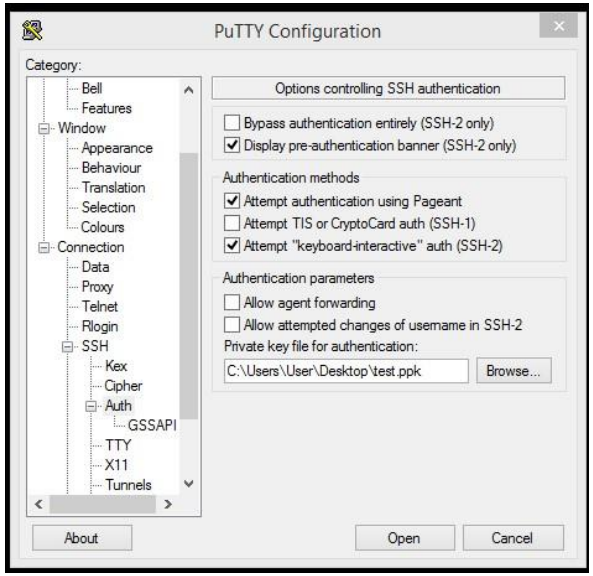

PuTTY Key Generator
File Key Conversions Help
Save private key as:
This PC ▸ Desktop
Search Desktop
Organize
New folder
OneDrive
Documents
Pictures
Homegroup
This PC
Desktop
Documents
Downloads
Music
Course contents
Rasberry Pi
TAMIL LATEST MP3
test
Google Drive
File name: test
Save as type: PuTTY Private Key Files (*.ppk)
Hide Folders
Save
Cancel

Open Putty

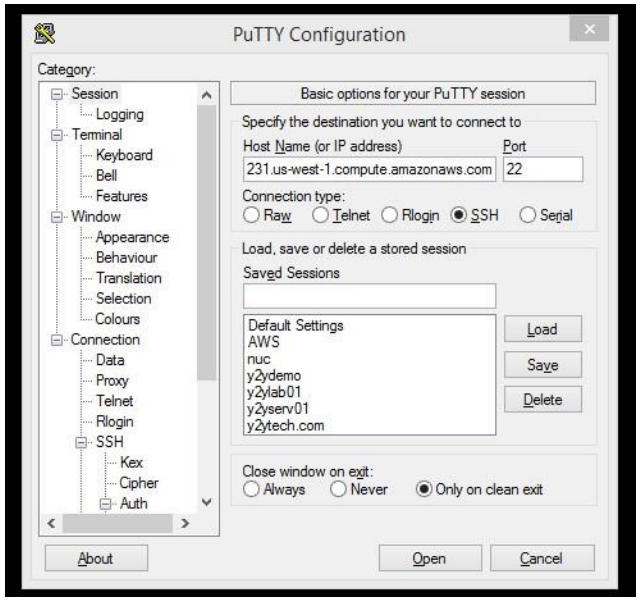


Click SSH-> Auth -> Choose the private key saved


PuTTY Configuration
Category:
Bell
Features
Window
Appearance
Behaviour
Translation
Selection
Colours
Connection
Data
Proxy
Telnet
Rlogin
SSH
Kex
Cipher
Auth
GSSAPI
TTY
X11
Tunnels
Options controlling SSH authentication
Bypass authentication entirely (SSH-2 only)
Display pre-authentication banner (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:
Browse...
About
Open
Cancel



Go to session and Put the DNS name show in Connect Tab of AWS console



Enter ec2-user as User name


ec2-52-53-215-231.us-west-1.compute.amazonaws.com - PuTTY
login as:

Step 3: Migrate your On Premise VM root disk to AWS AMI

Before Migrating the VM, We need to prepare the VM

Prepare Your VM

Use the following guidelines to configure your VM before exporting it from the virtualization environment.

- Review the prerequisites.
- Disable any antivirus or intrusion detection, software on your VM. These services can be re-enabled after the import process is complete.
- Uninstall the VMware Tools from your VMware VM.
- Disconnect any CD-ROM drives (virtual or physical).
- Set your network to DHCP instead of a static IP address. If you want to assign a static private IP address, be sure to use a non-reserved private IP address in your VPC subnet. Amazon Virtual Private Cloud (Amazon VPC) reserves the first four private IP addresses in a VPC subnet.
- Shut down your VM before exporting it from your virtualization environment.
- Amazon EC2 automatically assigns a private DHCP IP address to your instance. The DNS name and IP address are available through the `ec2-describe-instances`command when the instance starts running.
- Your instance will have only one Ethernet network interface.
- We recommend that your Windows instances contain strong passwords for all user accounts. We recommend that your Linux instances use public keys for SSH.
- For Windows instances, we recommend that you install the latest version of theAmazon Windows EC2Config Service after you import your virtual machine into Amazon EC2.

Windows

- Enable Remote Desktop (RDP) for remote access.
- Make sure that your host firewall (Windows firewall or similar), if configured, allows access to RDP. Otherwise, you will not be able to access your instance after the import is complete.
- Make sure that the administrator account and all other user accounts use secure passwords. All accounts must have passwords or the importation might fail.
- Make sure that your Windows VM has .NET Framework 3.5 or later installed, as required by Amazon Windows EC2Config Service.
- You can run System Preparation (Sysprep) on your Windows Server 2008 or Windows Server 2012 VM images before or after they are imported. If you run Sysprep before importing your VM, the importation process adds an answer file (unattend.xml) to the VM that automatically accepts the End User License Agreement (EULA) and sets the locale to EN-US. If you choose to run Sysprep after importation, we recommend that you use the Amazon EC2 Config service to run Sysprep.

  To include your own answer file instead of the default (unattend.xml):

  1. Copy the sample unattend.xml file below and set the **processorArchitecture**parameter to **x86** or **amd64**, depending on your OS architecture:

```
<?xml version='1.0' encoding='UTF-8'?>
<unattend xmlns:wcm='http://schemas.microsoft.com/WMIConfig/2002/State' xmlns='urn:schemas-microsoft-
com:unattend'>
 <settings pass='oobeSystem'>
  <component versionScope='nonSxS' processorArchitecture='x86 or amd64' name='Microsoft-Windows-
International-Core' publicKeyToken='31bf3856ad364e35' language='neutral'>
   <InputLocale>en-US</InputLocale>
   <SystemLocale>en-US</SystemLocale>
   <UILanguage>en-US</UILanguage>
   <UserLocale>en-US</UserLocale>
  </component>
  <component versionScope='nonSxS' processorArchitecture='x86 or amd64' name='Microsoft-Windows-Shell-
Setup' publicKeyToken='31bf3856ad364e35' language='neutral'>
   <OOBE>
    <HideEULAPage>true</HideEULAPage>
```

```
    <SkipMachineOOBE>true</SkipMachineOOBE>
    <SkipUserOOBE>true</SkipUserOOBE>
   </OOBE>
  </component>
 </settings>
</unattend>
```

2. Save the file in the **C:\Windows\Panther** directory with the name **unattend.xml**.
3. Run Sysprep with the **/oobe** and **/generalize** options.

   Note

   The **/oobe** and **/generalize** options strip all unique system information from the Microsoft Windows installation and will prompt you to reset the administrator password.
4. Shutdown the VM and export it from your virtualization environment.

- Disable Autologon on your Windows VM.
- Open **Control Panel** > **System and Security** > **Windows Update**. In the left pane, choose **Change settings**. Choose the desired setting. Be aware that if you choose**Download updates but let me choose whether to install them** (the default value) the update check can temporarily consume between 50% and 99% of CPU resources on the instance. The check usually occurs several minutes after the instance starts. Make sure that there are no pending Microsoft updates, and that the computer is not set to install software when it reboots.
- Apply the following hotfixes:
  - You cannot change system time if RealTimeIsUniversal registry entry is enabled in Windows
  - High CPU usage during DST changeover in Windows Server 2008, Windows 7, or Windows Server 2008 R2
- Enable the RealTimeIsUniversal registry.

Linux

- Enable Secure Shell (SSH) for remote access.
- Make sure that your host firewall (such as Linux iptables) allows access to SSH. Otherwise, you will not be able to access your instance after the import is complete.
- Make sure that you have configured a non-root user to use public key-based SSH to access your instance after it is imported. The use of password-based SSH and root login over SSH are both possible, but not recommended. The use of public keys and a non-root user is recommended because it is more secure. VM Import will not configure an *ec2-user* account as part of the import process.
- Make sure that your Linux VM uses GRUB (GRUB legacy) or GRUB 2 as its bootloader.
- Make sure that your Linux VM uses a root filesystem is one of the following: EXT2, EXT3, EXT4, Btrfs, JFS, or XFS.

Export Your VM from Its Virtual Environment

After you have prepared your VM for export, you can export it from your virtualization environment.

Citrix: Export to OVF

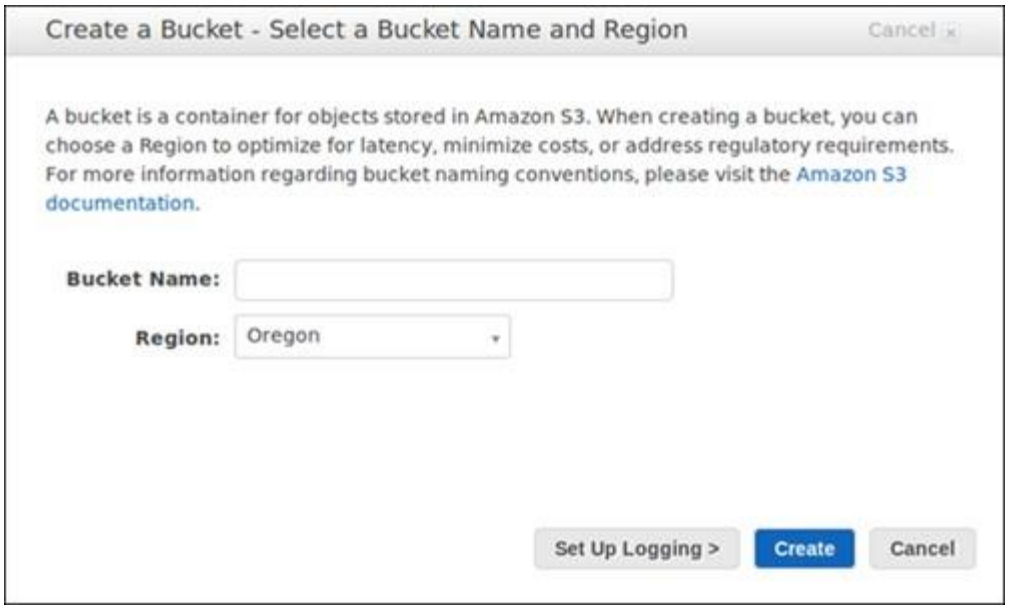
Microsoft Hyper-V: Export to VHD

VMWare: Export to OVF

KVM: Convert to Raw Disk

Create a Migration bucket

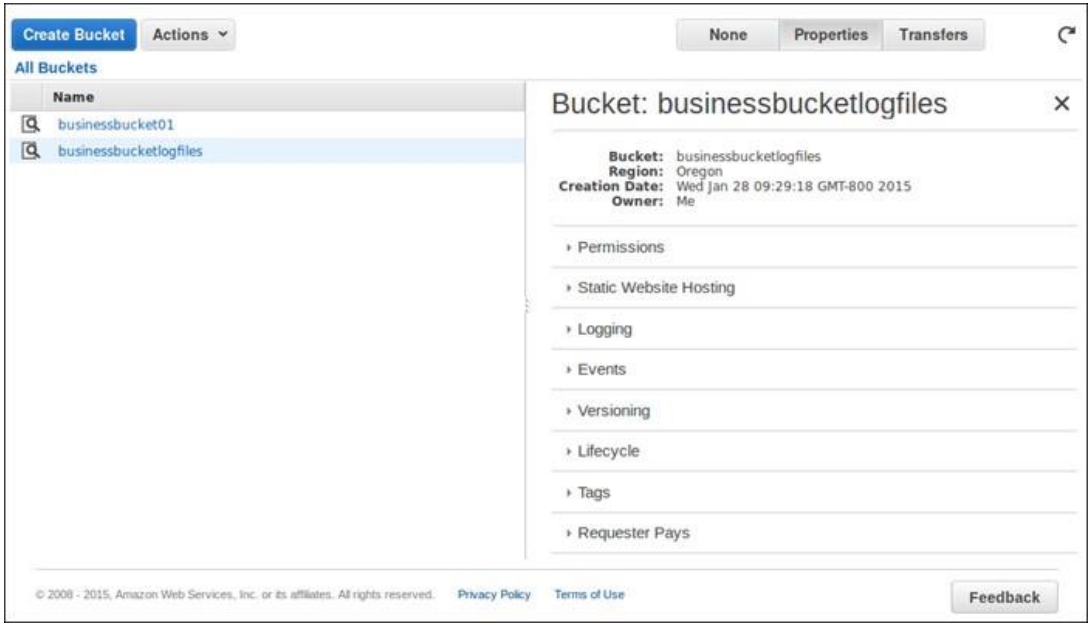
1. Sign into the AWS Management Console and open the Amazon S3 console athttps://console.aws.amazon.com/s3.
2. Click **Create Bucket**.



3. In the **Create a Bucket** dialog box, in the **Bucket Name** box, enter a bucket name and enter Virginia as a Region

4. In the **Region** box, select a region. For this exercise, select **Oregon** from the drop-down list.
5. Click **Create**.

When Amazon S3 successfully creates your bucket, the console displays your empty bucket in the **Buckets** panel.


Create Bucket
Actions
None
Properties
Transfers
All Buckets
Name
businessbucket01
businessbucketlogfiles
Bucket: businessbucketlogfiles
Bucket: businessbucketlogfiles
Region: Oregon
Creation Date: Wed Jan 28 09:29:18 GMT-800 2015
Owner: Me
Permissions
Static Website Hosting
Logging
Events
Versioning
Lifecycle
Tags
Requester Pays
© 2008 - 2015, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
Feedback

Create a vmimport role

To create the role using AWS CLI, Login in to build server

- Create a file named trust-policy.json as:

#vi trust-policy.json

```
{

   "Version":"2012-10-17",

   "Statement":[

      {

         "Sid":"",

         "Effect":"Allow",

         "Principal":{

            "Service":"vmie.amazonaws.com"
         },
         "Action":"sts:AssumeRole",
         "Condition":{
            "StringEquals":{
               "sts:ExternalId":"vmimport"
```

```
            }
         }
      }
   ]
}
```

Use AWS CLI, run the **aws iam create-role** command to create the role

```
aws iam create-role --role-name vmimport --assume-role-policy-document file://trust-policy.json
```

Create a Policy with name vmimport and attach a role called vmimport

#vi policy.json

```
"Version":"2012-10-17",

   "Statement":[

      {

         "Effect":"Allow",

         "Action":[

            "s3:ListBucket",
```

```
            "s3:GetBucketLocation"

        ],

        "Resource":[

            "arn:aws:s3:::<disk-image-file-bucket>"

        ]

    },

    {

        "Effect":"Allow",

        "Action":[

            "s3:GetObject"

        ],

        "Resource":[

            "arn:aws:s3:::<disk-image-file-bucket>/*"
```

```
        ]

    },

    {

        "Effect":"Allow",

        "Action":[

            "ec2:ModifySnapshotAttribute",

            "ec2:CopySnapshot",

            "ec2:RegisterImage",

            "ec2:Describe*"

        ],

        "Resource":"*"

    }

]
```

```
}
```

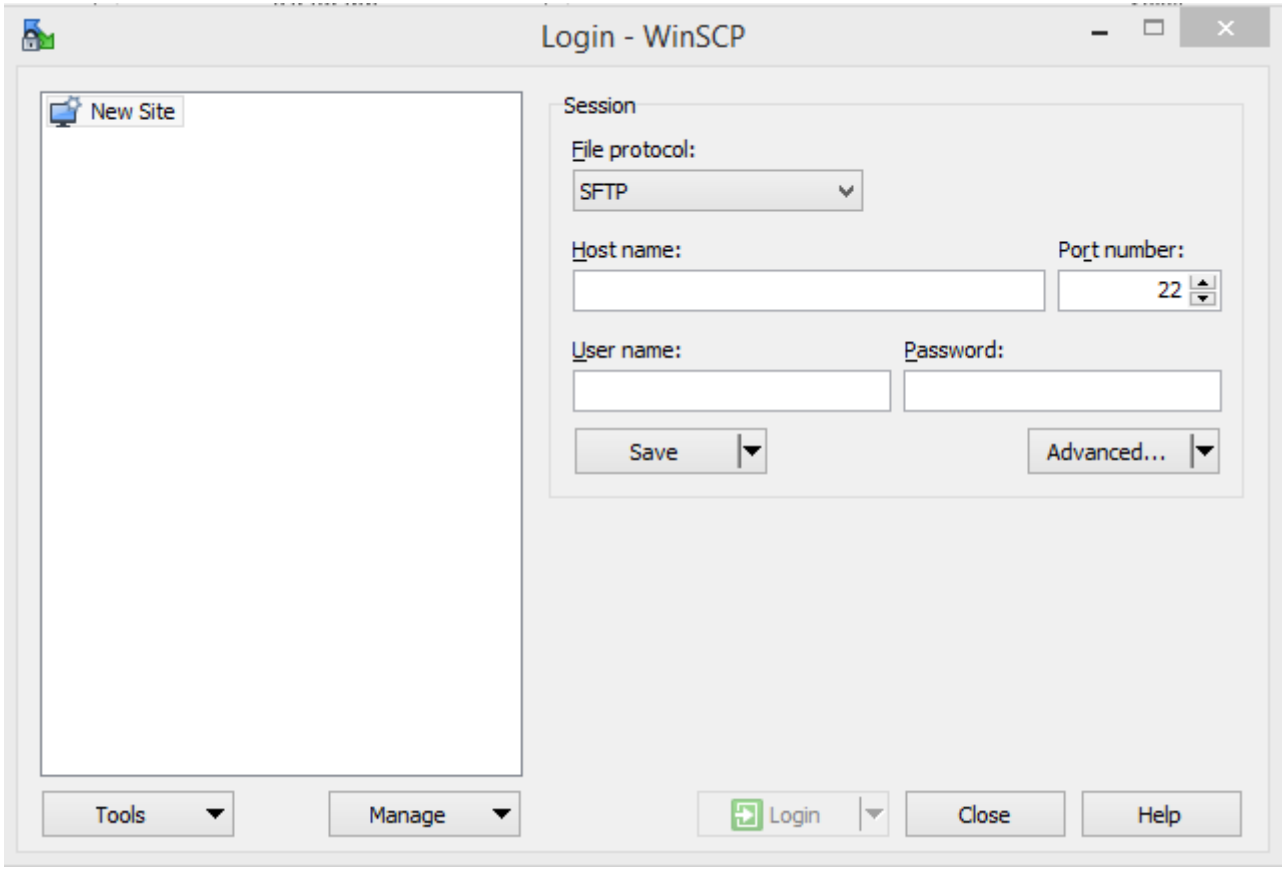
Use AWS CLI, run the **aws iam put-role-policy** command to attach the policy to the role created:

```
aws iam put-role-policy --role-name vmimport --policy-name vmimport --policy-document file://role-policy.json
```

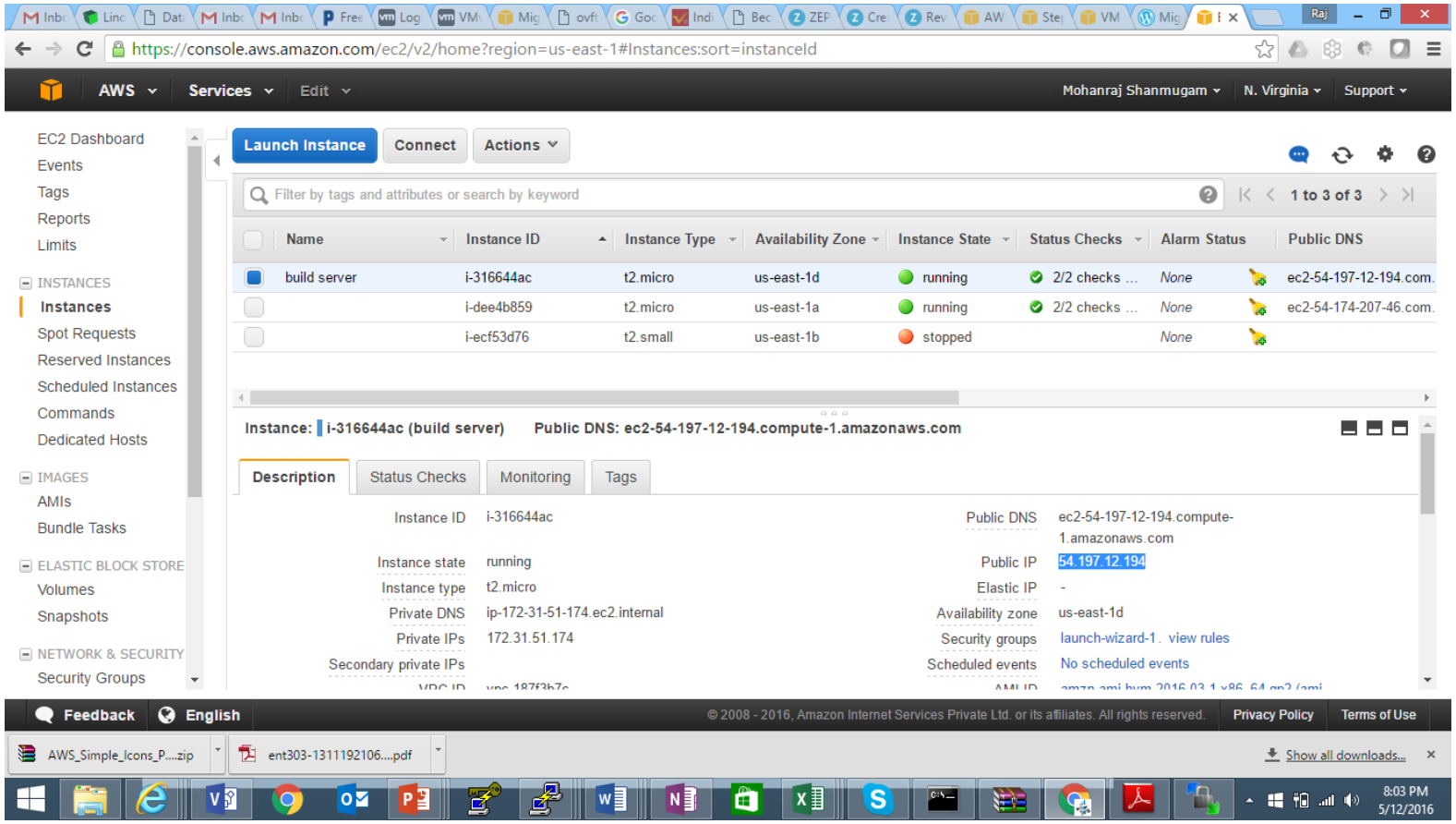
SCP the root volume and Data volume to Build server

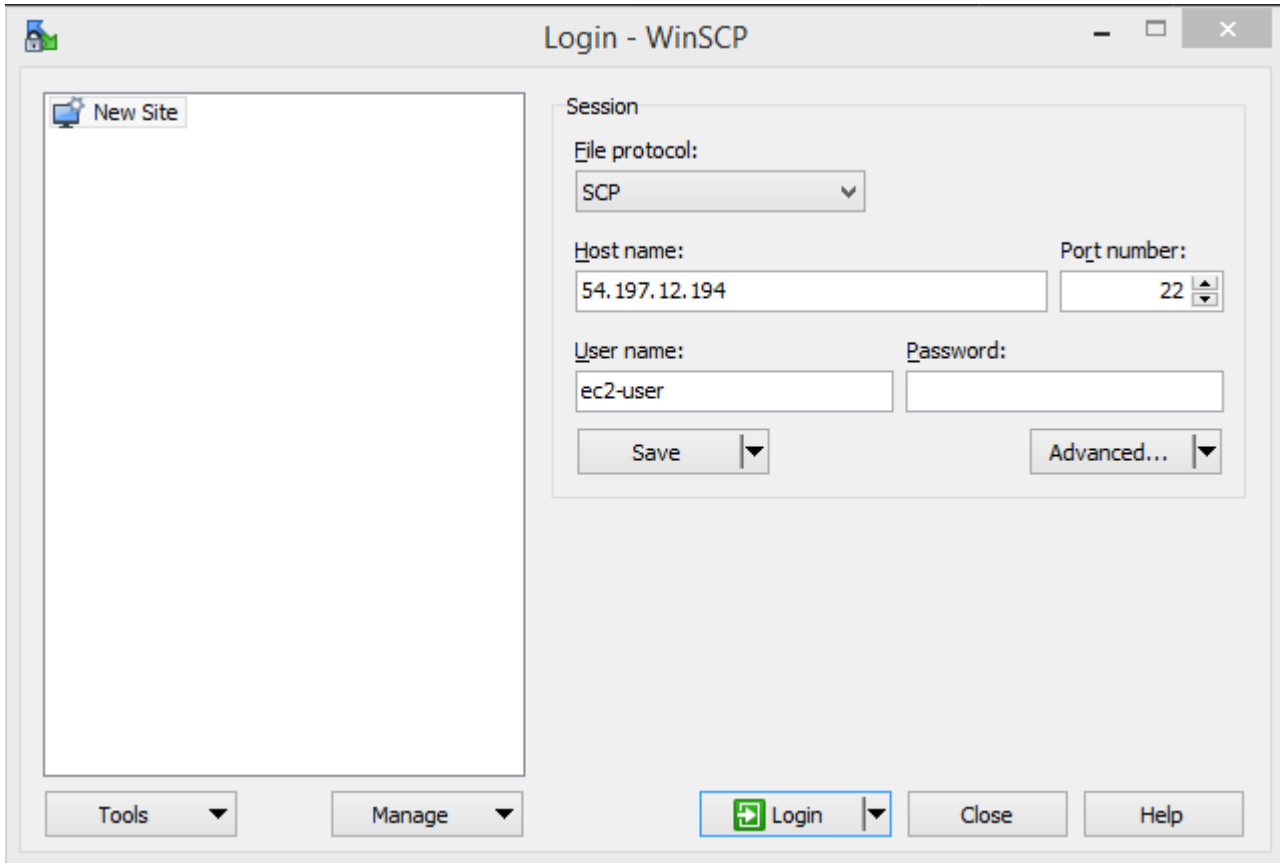
This is one approach I found good in slow internet, In Faster Enterprise environment you can use all the commands in build server in your local enterpeise server/

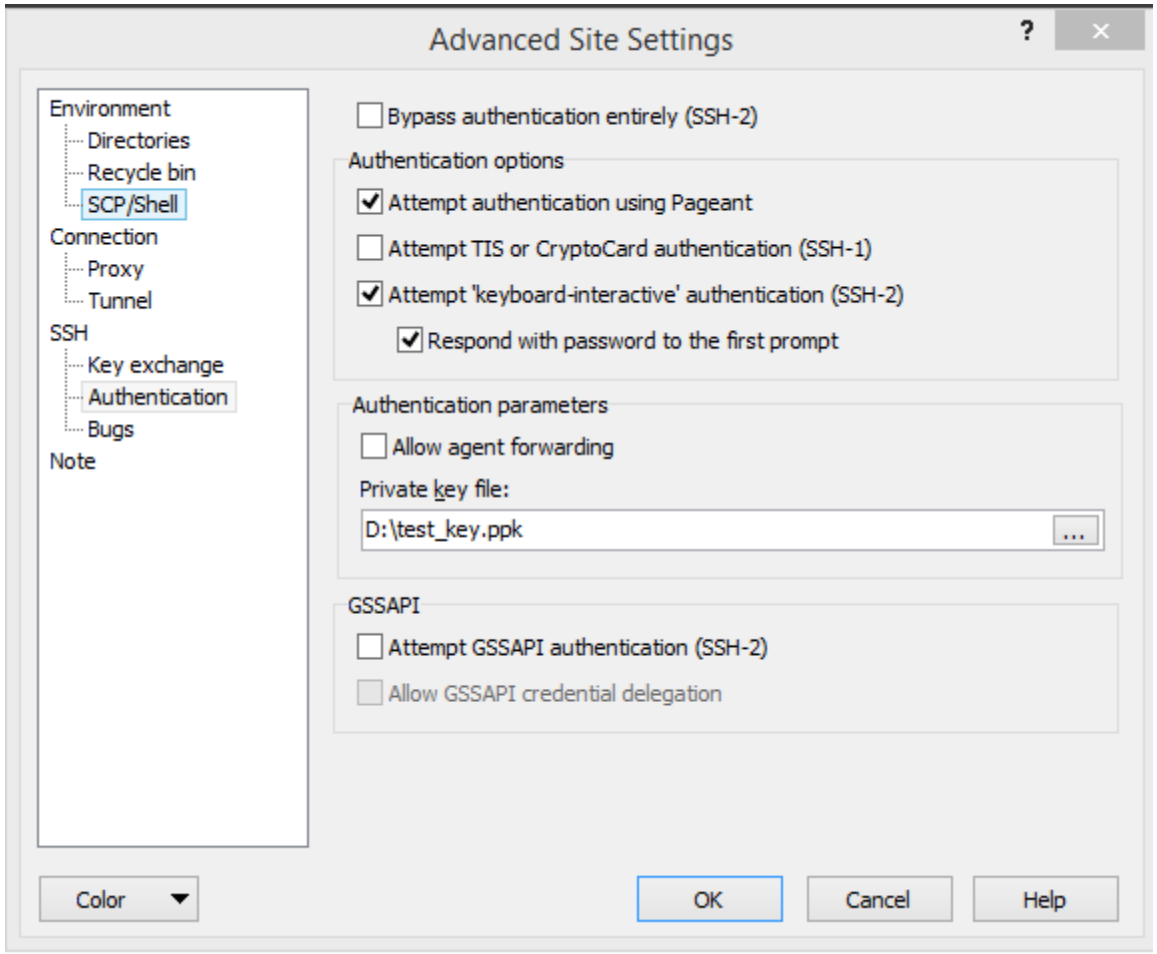
Open Winscp

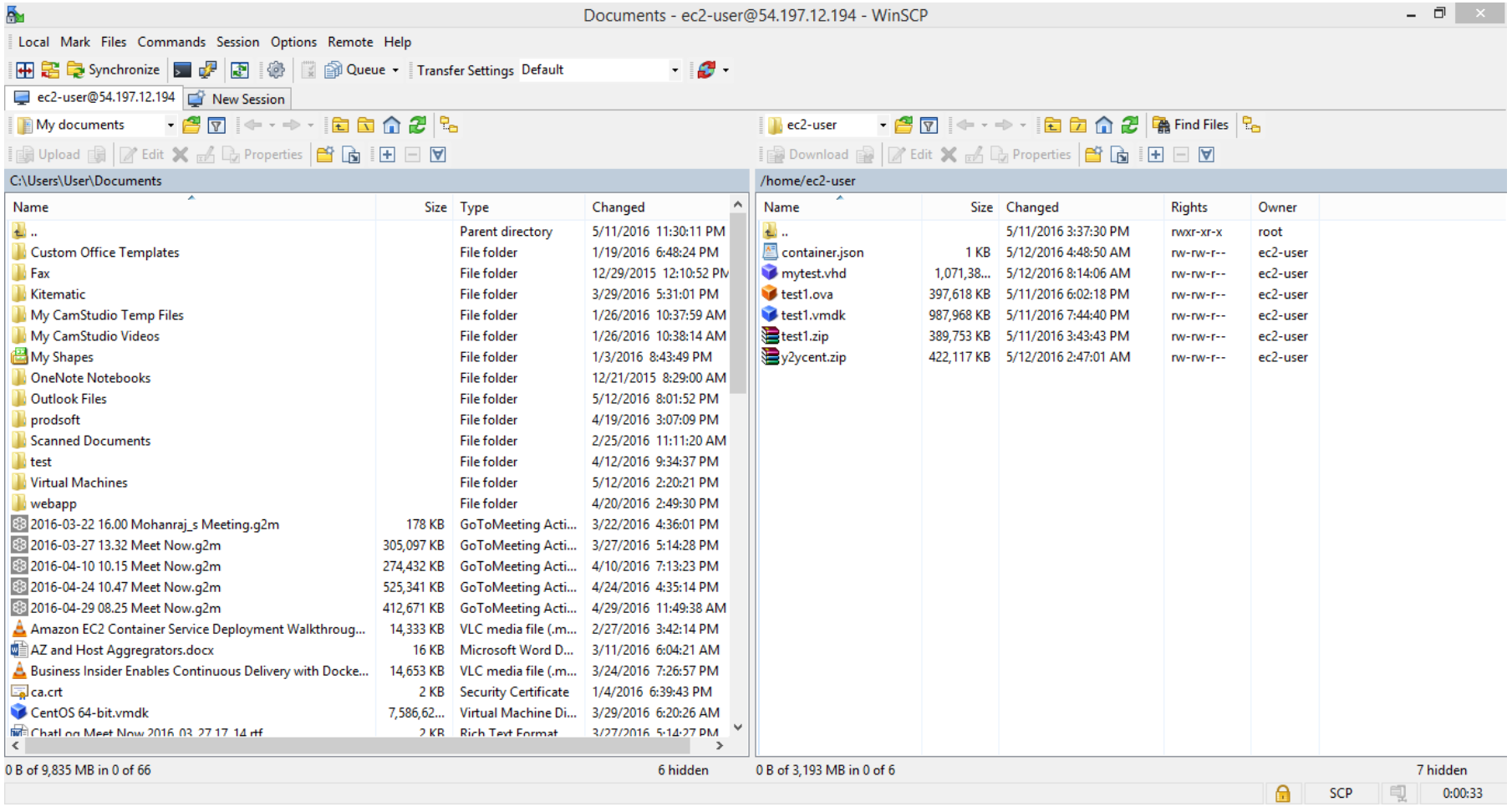


Get the IP of Build Server




Login - WinSCP
New Site
Session
File protocol:
SCP
Host name:
54.197.12.194
Port number:
22
User name:
ec2-user
Password:
Save
Advanced...
Tools
Manage
Login
Close
Help


Advanced Site Settings
Environment
Directories
Recycle bin
SCP/Shell
Connection
Proxy
Tunnel
SSH
Key exchange
Authentication
Bugs
Note
Bypass authentication entirely (SSH-2)
Authentication options
Attempt authentication using Pageant
Attempt TIS or CryptoCard authentication (SSH-1)
Attempt 'keyboard-interactive' authentication (SSH-2)
Respond with password to the first prompt
Authentication parameters
Allow agent forwarding
Private key file:
D:\test_key.ppk
...
GSSAPI
Attempt GSSAPI authentication (SSH-2)
Allow GSSAPI credential delegation
Color
OK
Cancel
Help


Documents - ec2-user@54.197.12.194 - WinSCP
Local Mark Files Commands Session Options Remote Help
Synchronize Queue Transfer Settings Default
ec2-user@54.197.12.194 New Session
My documents
Upload Edit Properties
C:\Users\User\Documents
Name Size Type Changed
.. Parent directory 5/11/2016 11:30:11 PM
Custom Office Templates File folder 1/19/2016 6:48:24 PM
Fax File folder 12/29/2015 12:10:52 PM
Kitematic File folder 3/29/2016 5:31:01 PM
My CamStudio Temp Files File folder 1/26/2016 10:37:59 AM
My CamStudio Videos File folder 1/26/2016 10:38:14 AM
My Shapes File folder 1/3/2016 8:43:49 PM
OneNote Notebooks File folder 12/21/2015 8:29:00 AM
Outlook Files File folder 5/12/2016 8:01:52 PM
prodsoft File folder 4/19/2016 3:07:09 PM
Scanned Documents File folder 2/25/2016 11:11:20 AM
test File folder 4/12/2016 9:34:37 PM
Virtual Machines File folder 5/12/2016 2:20:21 PM
webapp File folder 4/20/2016 2:49:30 PM
2016-03-22 16.00 Mohanraj_s Meeting.g2m 178 KB GoToMeeting Acti... 3/22/2016 4:36:01 PM
2016-03-27 13.32 Meet Now.g2m 305,097 KB GoToMeeting Acti... 3/27/2016 5:14:28 PM
2016-04-10 10.15 Meet Now.g2m 274,432 KB GoToMeeting Acti... 4/10/2016 7:13:23 PM
2016-04-24 10.47 Meet Now.g2m 525,341 KB GoToMeeting Acti... 4/24/2016 4:35:14 PM
2016-04-29 08.25 Meet Now.g2m 412,671 KB GoToMeeting Acti... 4/29/2016 11:49:38 AM
Amazon EC2 Container Service Deployment Walkthroug... 14,333 KB VLC media file (.m... 2/27/2016 3:42:14 PM
AZ and Host Aggregators.docx 16 KB Microsoft Word D... 3/11/2016 6:04:21 AM
Business Insider Enables Continuous Delivery with Docke... 14,653 KB VLC media file (.m... 3/24/2016 7:26:57 PM
ca.crt 2 KB Security Certificate 1/4/2016 6:39:43 PM
CentOS 64-bit.vmdk 7,586,62... Virtual Machine Di... 3/29/2016 6:20:26 AM
0 B of 9,835 MB in 0 of 66
6 hidden
ec2-user
Find Files
Download Edit Properties
/home/ec2-user
Name Size Changed Rights Owner
.. 5/11/2016 3:37:30 PM rwxr-xr-x root
container.json 1 KB 5/12/2016 4:48:50 AM rw-rw-r-- ec2-user
mytest.vhd 1,071,38... 5/12/2016 8:14:06 AM rw-rw-r-- ec2-user
test1.ova 397,618 KB 5/11/2016 6:02:18 PM rw-rw-r-- ec2-user
test1.vmdk 987,968 KB 5/11/2016 7:44:40 PM rw-rw-r-- ec2-user
test1.zip 389,753 KB 5/11/2016 3:43:43 PM rw-rw-r-- ec2-user
y2ycent.zip 422,117 KB 5/12/2016 2:47:01 AM rw-rw-r-- ec2-user
0 B of 3,193 MB in 0 of 6
7 hidden
SCP
0:00:33

Copy the Volume from AWS Build Server to Build S3 Bucket

Copy both Root volume and Data volume

$ aws s3 cp <filename.vhd> s3://<bucket name>/<file name.vhd>

Importing Your VM into Amazon EC2

#vi containers.json

```
[{
    "Description": "First CLI task",
    "Format": "ova",
    "UserBucket": {
        "S3Bucket": "my-import-bucket",
        "S3Key": "my-windows-2008-vm.ova"
    }
}]
```

Import the Root disk as AMI

```
$ aws ec2 import-image --description "example_com_web_Server" --disk-containers file://containers.json
```

Output " Note the Import Task ID"

```
<ImportImageResponse xmlns="http://ec2.amazonaws.com/doc/2015-03-01/">
    <progress>2</progress>
    <importTaskId>import-ami-fgxn195v</importTaskId>
```

```
    <status>active</status>
    <description>Windows 2008 OVA</description>
    <snapshotTaskDetailSet>
        <item>
            <diskImageSize>0.0</diskImageSize>
            <userBucket>
                <s3Bucket>my-import-bucket</s3Bucket>
                <s3Key>my-windows-2008-vm.ova</s3Key>
            </userBucket>
        </item>
    </snapshotTaskDetailSet>
    <licenseType>AWS</licenseType>
    <statusMessage>pending</statusMessage>
    <requestId>1571e127-d6d8-4984-b4f1-3a21e9dbdcb5</requestId>
</ImportImageResponse>
```

To check the status of your import task

```
aws ec2 describe-import-image-tasks --cli-input-json "{ \"ImportTaskIds\": [\"import-ami-fgxn195v\"],
\"NextToken\": \"abc\", \"MaxResults\": 10 } "
```

Output

```
<DescribeImportImageTasksResponse xmlns="http://ec2.amazonaws.com/doc/2015-03-01/">
    <importImageTaskSet>
        <item>
            <platform>Windows</platform>
            <importTaskId>import-ami-fgs8im0c</importTaskId>
            <imageId>ami-4a6c2722</imageId>
            <status>completed</status>
            <description>Linux OVA</description>
            <architecture>x86_64</architecture>
            <snapshotTaskDetailSet>
```

```
                <item>
                    <diskImageSize>3.115815424E9</diskImageSize>
                    <deviceName>/dev/sda1</deviceName>
                    <description>First CLI task</description>
                    <format>VMDK</format>
                    <url>https://mys3bucket/vms/my-linux-
vm.ova?AWSAccessKeyId=myAccessKeyId&Expires=expirationDate&Signature=mySignature</url>
                </item>
            </snapshotTaskDetailSet>
            <licenseType>AWS</licenseType>
        </item>
    </importImageTaskSet>
    <requestId>377ec1ca-6a47-42f5-8b84-aa07ff87f7b0</requestId>
</DescribeImportImageTasksResponse>
```

Import Data VM disk to a Snapshot

#vi containers.json

```
[{
    "DryRun": false,
    "Description": "First CLI snap",
    "DiskContainer": {
        "Description": "web data snapshot",
        "Format": "vhd",
                "Url": "https://mys3bucket/data_disk.vhd"
        }
}]
```

Create snapshot

```
aws ec2 import-snapshot --description "Data Disk" --disk-container file://containers.json
```

Output

```
<ImportSnapshotResponse xmlns="http://ec2.amazonaws.com/doc/2015-03-01/">
    <snapshotTaskDetail>
        <diskImageSize>0.0</diskImageSize>
        <progress>3</progress>
        <status>active</status>
        <description>Windows 2008 VMDK</description>
        <url>https://mys3bucket/vms/Win_2008_Server_Enterprise_R2_64-
bit.vmdk?AWSAccessKeyId=myaccesskey&Expires=expirationdate&Signature=signature\</url>
        <statusMessage>pending</statusMessage>
    </snapshotTaskDetail>
    <importTaskId>import-snap-ffy5pvea</importTaskId>
    <description>Windows 2008 VMDK</description>
    <requestId>2ef5652d-6816-4c20-89b2-a4bbb0560190</requestId>
</ImportSnapshotResponse>
```

Verify the completion " Replace the import Task id"

```
aws ec2 describe-import-snapshot-tasks --cli-input-json "{ \"ImportTaskIds\": [\"import-snap-fgr1mmg7\"],
\"NextToken\": \"abc\", \"MaxResults\": 10 } "
```

Create a auto scaling group

To create a launch configuration and Auto Scaling group from the launch wizard

1. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
2. From the dashboard, choose **Launch Instance**.
3. Choose an AMI created through migration, then choose an instance type on the next page, and then choose **Next: Configure Instance Details**.
4. In **Number of instances**, enter the number of instances that you want to launch, and then choose **Launch into Auto Scaling Group**. You do not need to enter any other configuration details on the page.
5. In the confirmation dialog box, choose **Create Launch Configuration**.
6. You are switched to step 3 of the launch configuration wizard. The AMI and instance type are already selected based on the selection you made in the Amazon EC2 launch wizard. Enter a name for the launch configuration, configure any other settings as required, and then choose **Next: Add Storage**.
7. Add Data volume and create from the snapshot created from Data snapshot
8. Configure any additional volumes, and then choose **Next: Configure Security Group**.

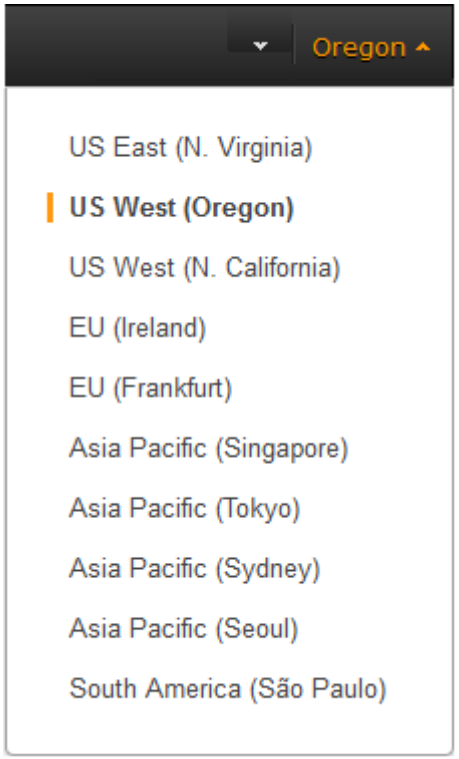
   Enable port 80 in security group

9. Create a new security group, or choose an existing group, and then choose **Review**.
10. Review the details of the launch configuration, and then choose **Create launch configuration** to choose a key pair and create the launch configuration.
11. in the **Configure Auto Scaling group details** page, the launch configuration you created is already selected for you, and the number of instances you specified in the Amazon EC2 launch wizard is populated for **Group size**. Enter a name for the group, specify a VPC and subnet (if required), and then choose **Next: Configure scaling policies**.

12. In the **Configure scaling policies** page, choose one of the following options, and then choose **Review**:
    - To automatically adjust the size of the Auto Scaling group based on criteria that you specify, choose **Use scaling policies to adjust the capacity of this group** and follow the directions
13. On the **Review** page, you can optionally add tags or notifications, and edit other configuration details. When you are done, choose **Create Auto Scaling group**.

To access Elastic Load Balancing using the Amazon EC2 console

1. Sign in to the AWS Management Console and open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
2. From the navigation bar, select a region. Each load balancer is tied to the region in which you create it. You can select any region that's available to you, regardless of your location.



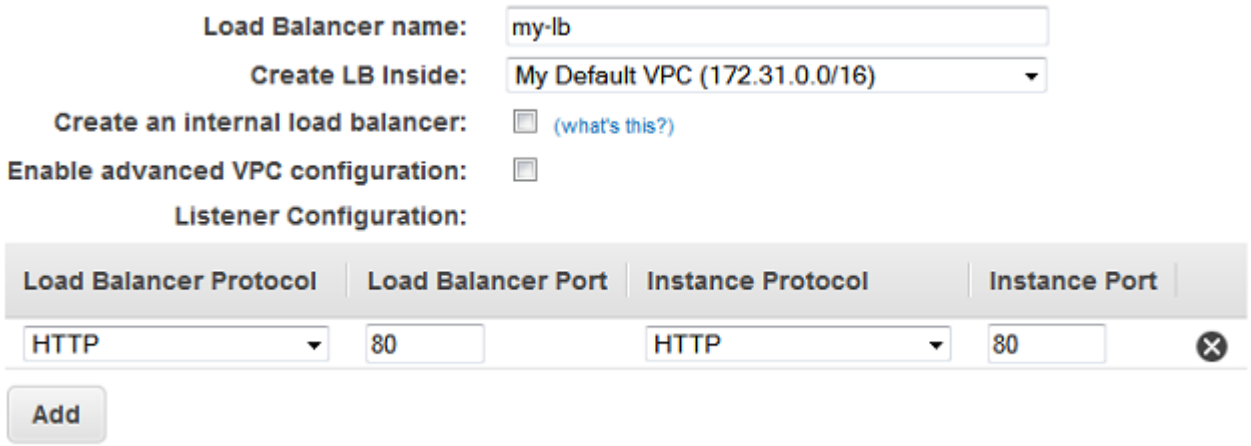
3. In the navigation pane, under **LOAD BALANCING**, click **Load Balancers**.

To define your load balancer

1. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
2. From the navigation bar, select a region for your load balancers. Be sure to select the same region that you selected for your EC2 instances.
3. In the navigation pane, under **LOAD BALANCING**, click **Load Balancers**.
4. Click **Create Load Balancer**.
5. In **Load Balancer name**, enter a name for your load balancer.

   The name of your load balancer must be unique within your set of load balancers for the region, can have a maximum of 32 characters, and can contain only alphanumeric characters and hyphens.

6. From **Create LB inside**, select the same network that you selected for your instances: EC2-Classic or a specific VPC.
7. [Default VPC] If you selected a default VPC and would like to choose the subnets for your load balancer, select **Enable advanced VPC configuration**.
8. Leave the default listener configuration.



9. [EC2-VPC] Under **Select Subnets**, select at least one available public subnet. To improve the availability of your load balancer, select more than one public subnet.

   Note

   If you selected EC2-Classic as your network, or you have a default VPC but did not select **Enable advanced VPC configuration**, you do not see **Select Subnets**.

   The available subnets for the VPC for your load balancer are displayed under **Available Subnets**. Select public subnets that are in the same Availability Zones as your instances. Click the icon in the **Action** column for each subnet to attach. These subnets are moved under **Selected Subnets**. You can select at most one subnet per Availability Zone. If you select a subnet from an Availability Zone where there is already a selected subnet, this subnet replaces the currently selected subnet for the Availability Zone.

Available Subnets

Actions	Availability Zone	Subnet ID	Subnet CIDR	Name
⊕	us-west-2c	subnet-cb663da2	10.0.1.0/24	
⊕	us-west-2c	subnet-c9663da0	10.0.0.0/24	

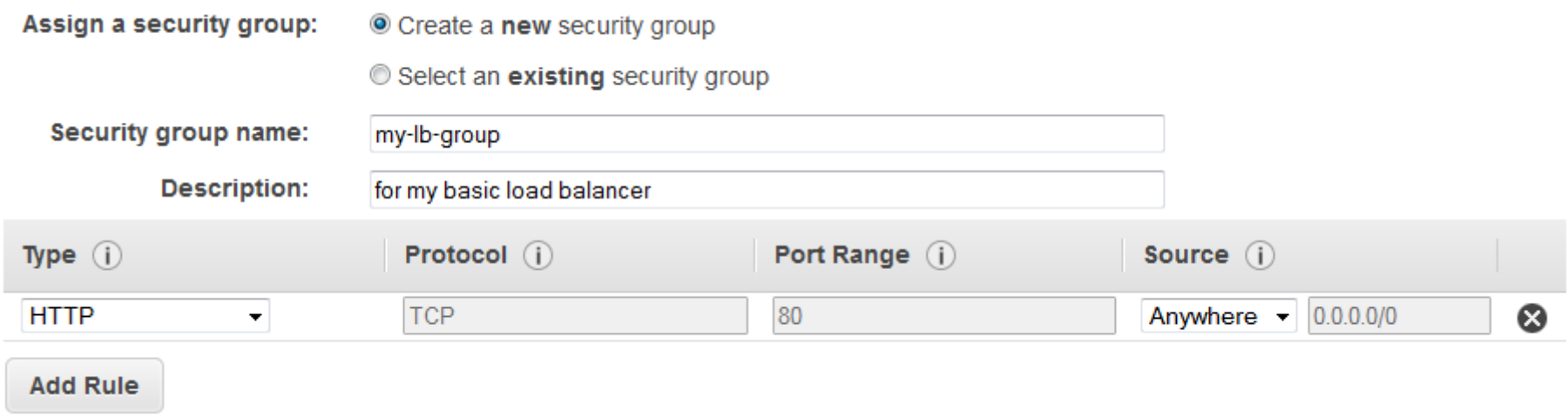
Selected Subnets

Actions	Availability Zone	Subnet ID	Subnet CIDR	Name
⊖	us-west-2a	subnet-e4f33493	10.0.2.0/24	
⊖	us-west-2b	subnet-5264e837	10.0.3.0/24	

10. Click **Next: Assign Security Groups**.

To assign security group to your load balancer

1. On the **Assign Security Groups** page, select **Create a new security group**.
2. Enter a name and description for your security group, or leave the default name and description. This new security group contains a rule that allows traffic to the port that you configured your load balancer to use.



3. Click **Next: Configure Security Settings**.

To configure health checks for your instances

1. On the **Configure Health Check** page, do the following:
    a. Leave **Ping Protocol** set to its default value, `HTTP`.
    b. Leave **Ping Port** set to its default value, `80`.

c. In the **Ping Path** field, replace the default value with a single forward slash ("/"). This tells Elastic Load Balancing to send health check queries to the default home page for your web server, such as `index.html` or `default.html`.

d. Leave the other fields set to their default values.

Add a Load Balancer to auto scaling group Using the Console

Use the following procedure to attach a load balancer to your Auto Scaling group.

To attach a load balancer to a group

1. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
2. In the navigation pane, under **Auto Scaling**, click **Auto Scaling Groups**.
3. Select your group.

4. In the bottom pane, on the **Details** tab, click **Edit**.
5. In **Load Balancers**, select the load balancer.
6. Click **Save**.

Copy website images to Image Bucket and edit the code

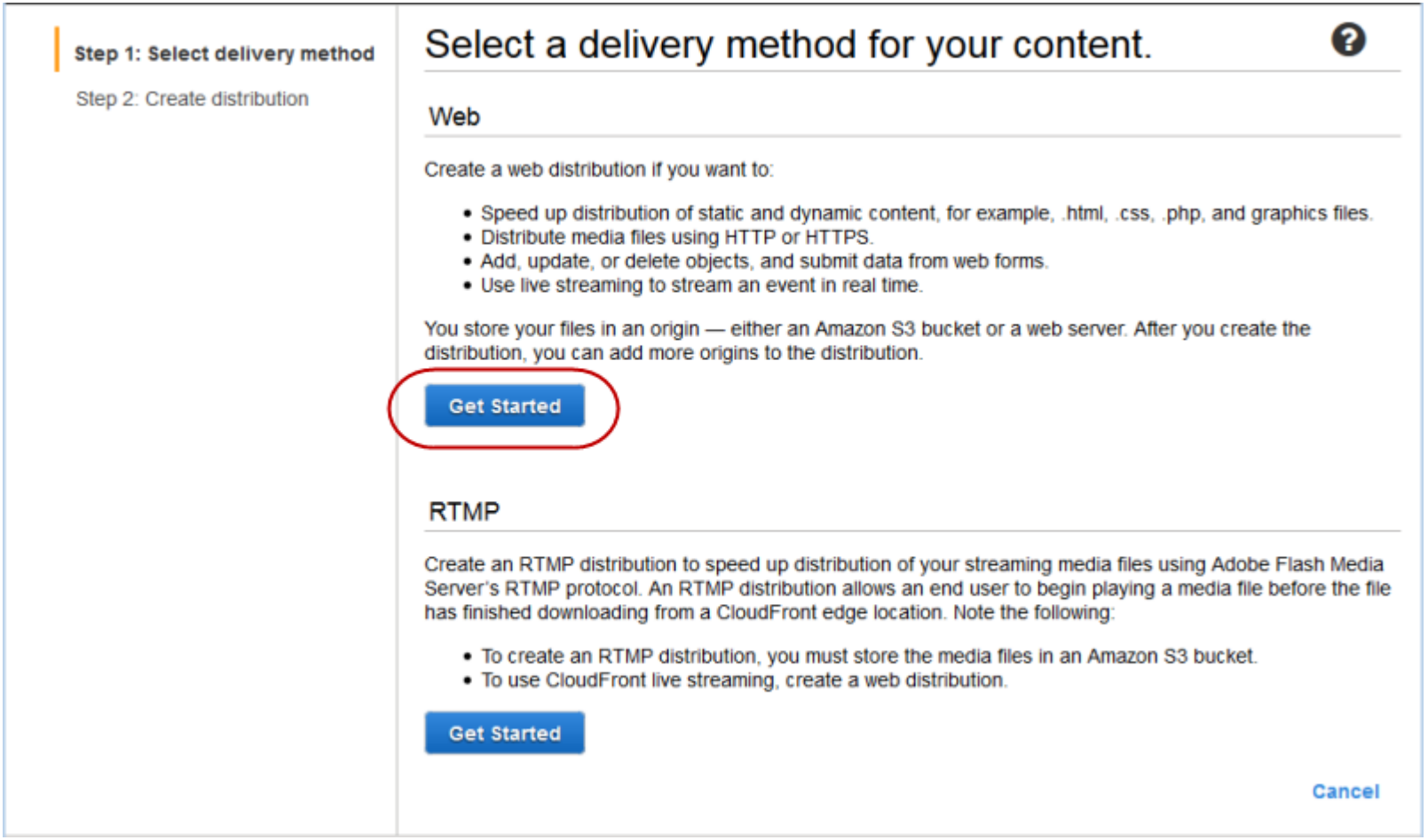
1) Click Create Bucket.
2) In the Create a Bucket dialog box, in the Bucket Name box, enter a bucket name. The bucket name you choose must be unique across all existing bucket names in Amazon S3. ...

3) In the Region box, select a region. For this exercise, select Virginia from the drop-down list. ...
4) Click Create.
5) Copy website images to the bucket
6) Do the code changes to the website code to point to S3 URLs for the images

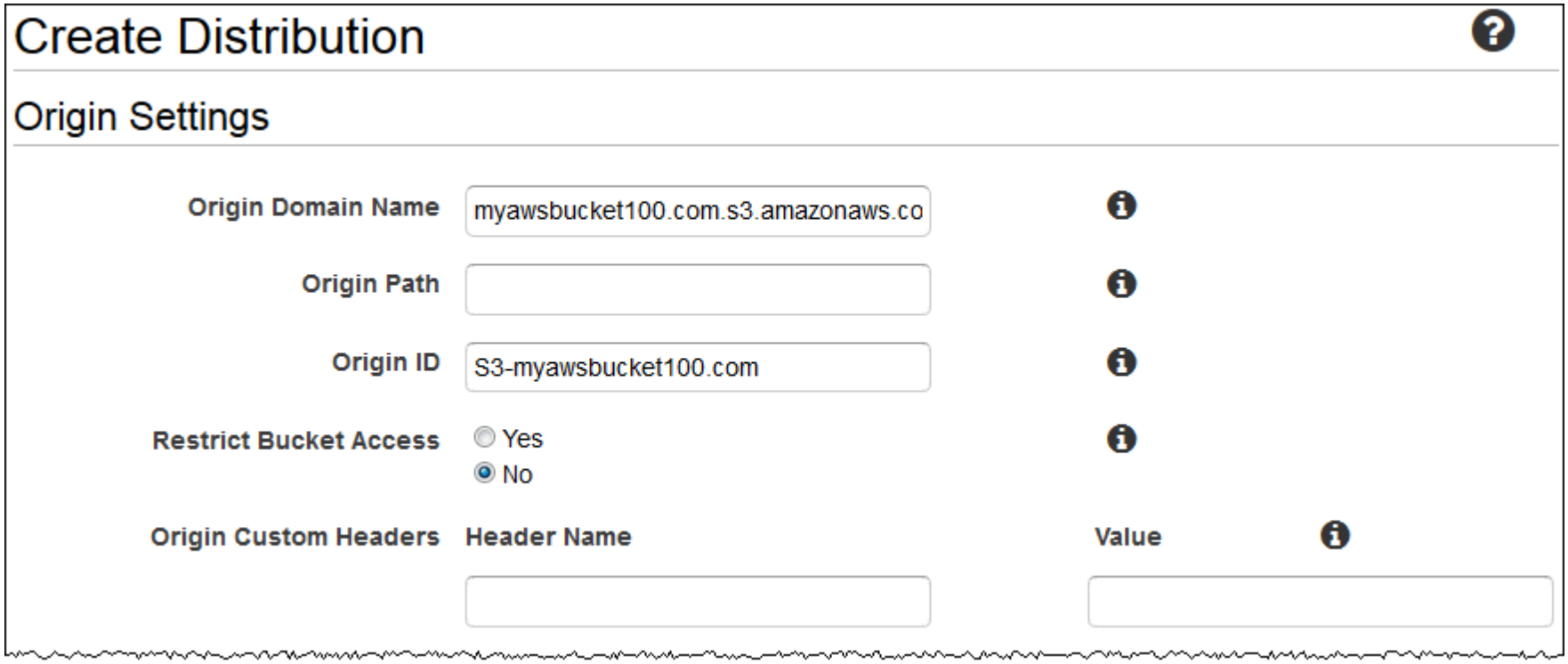
Create the Cloud Front distribution

To create a CloudFront web distribution

1. Open the CloudFront console at https://console.aws.amazon.com/cloudfront/.
2. Choose **Create Distribution**.
3. On the **Select a delivery method for your content** page, in the **Web** section, choose **Get Started**.



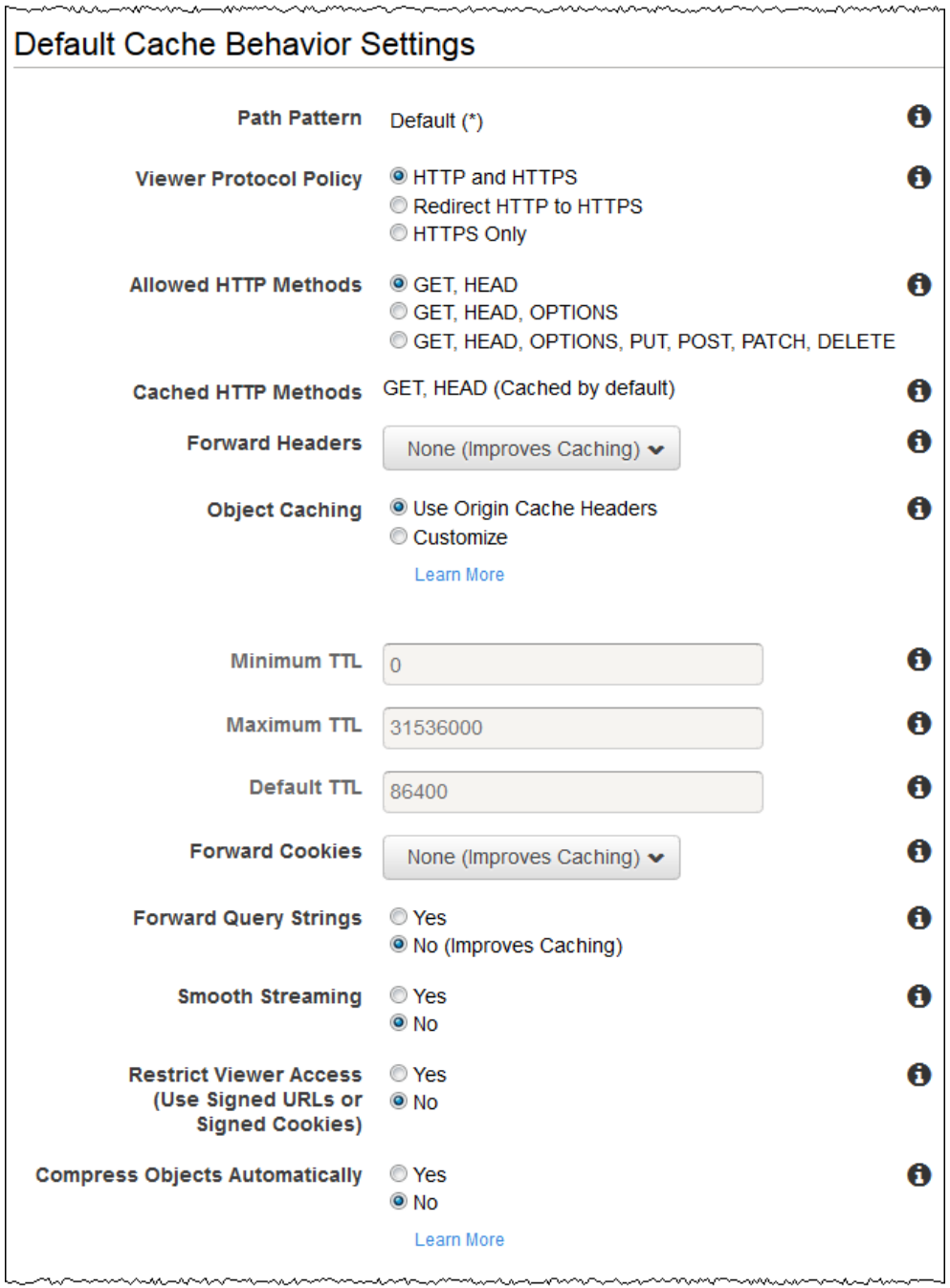
4. On the **Create Distribution** page, under **Origin Settings**, choose the Amazon S3 bucket that you created earlier. For **Origin ID**, **Origin Path**, **Restrict Bucket Access**, and **Origin Custom Headers**, accept the default values.



5. Under **Default Cache Behavior Settings**, accept the default values, and CloudFront will:
   - Forward all requests that use the CloudFront URL for your distribution (for example, `http://d111111abcdef8.cloudfront.net/image.jpg`) to the Amazon S3 bucket that you specified in Step 4.
   - Allow end users to use either HTTP or HTTPS to access your objects.
   - Respond to requests for your objects.
   - Cache your objects at CloudFront edge locations for 24 hours.
   - Forward only the default request headers to your origin and not cache your objects based on the values in the headers.

- Exclude cookies and query string parameters, if any, when forwarding requests for objects to your origin. (Amazon S3 doesn't process cookies and processes only a limited set of query string parameters.)
- Not be configured to distribute media files in the Microsoft Smooth Streaming format.
- Allow everyone to view your content.
- Not automatically compress your content.

For more information about cache behavior options, see Cache Behavior Settings.



Default Cache Behavior Settings

Path Pattern Default (*)

Viewer Protocol Policy
- (•) HTTP and HTTPS
- ( ) Redirect HTTP to HTTPS
- ( ) HTTPS Only

Allowed HTTP Methods
- (•) GET, HEAD
- ( ) GET, HEAD, OPTIONS
- ( ) GET, HEAD, OPTIONS, PUT, POST, PATCH, DELETE

Cached HTTP Methods GET, HEAD (Cached by default)

Forward Headers None (Improves Caching)

Object Caching
- (•) Use Origin Cache Headers
- ( ) Customize

Learn More

Minimum TTL 0

Maximum TTL 31536000

Default TTL 86400

Forward Cookies None (Improves Caching)

Forward Query Strings
- ( ) Yes
- (•) No (Improves Caching)

Smooth Streaming
- ( ) Yes
- (•) No

Restrict Viewer Access (Use Signed URLs or Signed Cookies)
- ( ) Yes
- (•) No

Compress Objects Automatically
- ( ) Yes
- (•) No

Learn More

6. Under **Distribution Settings**, enter the applicable values:

   Price Class

   Select the price class that corresponds with the maximum price that you want to pay for CloudFront service. By default, CloudFront serves your objects from edge locations in all CloudFront regions.

   For more information about price classes and about how your choice of price class affects CloudFront performance for your distribution, go to Choosing the Price Class for a CloudFront Distribution. For information about CloudFront pricing, including how price classes map to CloudFront regions, go to Amazon CloudFront Pricing.

   AWS WAF Web ACL

   If you want to use AWS WAF to allow or block HTTP and HTTPS requests based on criteria that you specify, choose the web ACL to associate with this distribution. For more information about AWS WAF, see the AWS WAF Developer Guide.

   Alternate Domain Names (CNAMEs) (Optional)

   Specify one or more domain names that you want to use for URLs for your objects instead of the domain name that CloudFront assigns when you create your distribution. For example, if you want the URL for the object:

   ```
   /images/image.jpg
   ```

   to look like this:

   ```
   http://www.example.com/images/image.jpg
   ```

   instead of like this:

`http://d111111abcdef8.cloudfront.net/images/image.jpg`

you would create a CNAME for `www.example.com`.

> **Important**
>
> If you add a CNAME for `www.example.com` to your distribution, you also need to create (or update) a CNAME record with your DNS service to route queries for `www.example.com` to `d111111abcdef8.cloudfront.net`. You must have permission to create a CNAME record with the DNS service provider for the domain. Typically, this means that you own the domain, but you may also be developing an application for the domain owner. For more information about CNAMEs, see Using Alternate Domain Names (CNAMEs).

For the current limit on the number of alternate domain names that you can add to a distribution, see Amazon CloudFront Limits in the *Amazon Web Services General Reference*. To request a higher limit, go to https://console.aws.amazon.com/support/home#/case/create?issueType=service-limit-increase&limitType=service-code-cloudfront-distributions.

SSL Certificate

Accept the default value, **Default CloudFront Certificate**.

Default Root Object (Optional)

The object that you want CloudFront to request from your origin (for example, `index.html`) when a viewer requests the root URL of your distribution (`http://www.example.com/`) instead of an object in your distribution (`http://www.example.com/product-description.html`). Specifying a default root object avoids exposing the contents of your distribution.

Logging (Optional)

If you want CloudFront to log information about each request for an object and store the log files in an Amazon S3 bucket, select **On**, and specify the bucket and an optional prefix for the names of the log files. There is no extra charge to enable logging, but you accrue the usual Amazon S3 charges for storing and accessing the files. CloudFront doesn't delete the logs automatically, but you can delete them at any time.

Cookie Logging

In this example, we're using Amazon S3 as the origin for your objects, and Amazon S3 doesn't process cookies, so we recommend that you select **Off** for the value of **Cookie Logging**.

Comment (Optional)

Enter any comments that you want to save with the distribution.

Distribution State

Select **Enabled** if you want CloudFront to begin processing requests as soon as the distribution is created, or select **Disabled** if you do not want CloudFront to begin processing requests after the distribution is created.

Distribution Settings

Price Class Use All Edge Locations (Best Performance)

AWS WAF Web ACL None

Alternate Domain Names (CNAMEs)

SSL Certificate

- Default CloudFront Certificate (*.cloudfront.net)

  Choose this option if you want your users to use HTTPS or HTTP to access your content with the CloudFront domain name (such as https://d111111abcdef8.cloudfront.net/logo.jpg).
  Important: If you choose this option, CloudFront requires that browsers or devices support TLSv1 or later to access your content.

- Custom SSL Certificate (stored in AWS IAM): No certificates available

  Choose this option if you want your users to use HTTPS to access your content with an alternate domain name (such as https://www.example.com/logo.jpg) using either dedicated CloudFront IP addresses or SNI.
  To choose this option, you first need to upload your certificate to the AWS IAM certificate store (the -path parameter must start with /cloudfront/).
  Learn More

Default Root Object

Logging

- On
- Off

Bucket for Logs

Log Prefix

7. Choose **Create Distribution**.
8. After CloudFront has created your distribution, the value of the **Status** column for your distribution will change from **InProgress** to **Deployed**. If you chose to enable the distribution, it will then be ready to process requests. This should take less than 15 minutes.

   The domain name that CloudFront assigns to your distribution appears in the list of distributions. (It also appears on the **General** tab for a selected distribution.)

If you wanted to move your domain or subdomain to Route53, Create a Route 53 Publicly hosted zone (This is done only in active domain in amazon or for a subdomain)

To create a hosted zone using the Amazon Route 53 console

1. Sign in to the AWS Management Console and open the Amazon Route 53 console at https://console.aws.amazon.com/route53/.
2. If you already have a hosted zone for your domain, skip to step 4. If you don't, perform the following steps:
    a. Click **Create Hosted Zone**.
    b. For **Domain Name**, enter the name of your domain.
    c. *Optional:* For **Comment**, enter a comment about the hosted zone.
    d. Click **Create**.
3. On the **Hosted Zones** page, choose the name of the hosted zone in which you want to create resource record sets.
4. Click **Create Record Set**.