

SRI LANKA INSTITUTE OF INFORMATION TECHNOLOGY



Enterprise Standards and Best Practices for IT Infrastructure

4th Year 2nd Semester 2016

AWS INSTANCES SUMMARY (Lab02) ASSIGNMENT

Name: H.A.E.Piumali

SLIIT ID: IT13056612

Practical Session: WD Friday

Practical Number: Lab 02

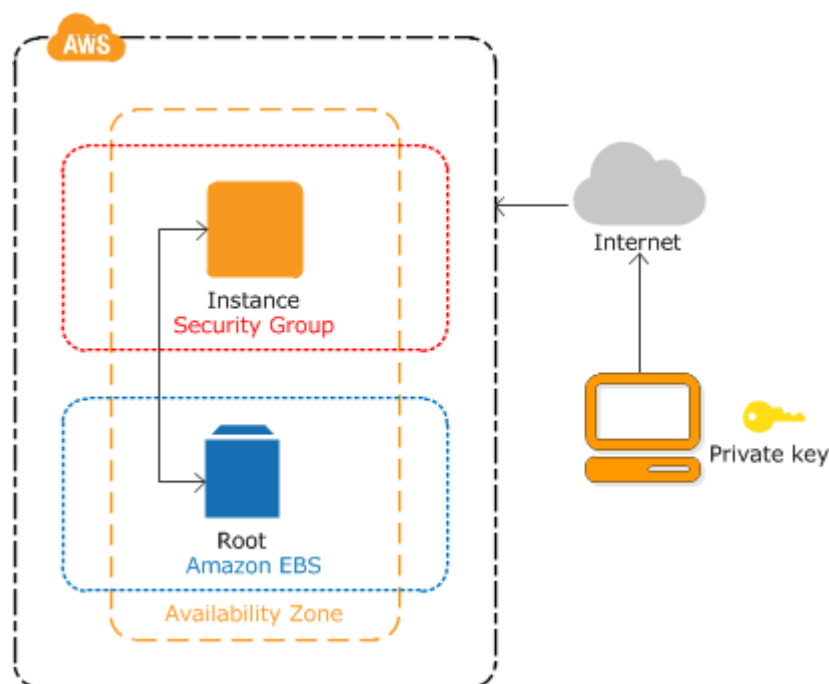
Date of Submission: 31th of July 2016

Getting Started with Amazon EC2 Windows Instances

Tasks

Perform the following tasks:

1. Launch an Instance
2. Connect to Your Instance
3. Clean Up Your Instance



1) Step 1: Launch an Instance

You can launch a Windows instance using the AWS Management Console as described in the following procedure. This tutorial is intended to help you launch your first instance quickly, so it doesn't cover all possible options. For more information about the advanced options, see [Launching an Instance](#).

To launch an instance

1. Open the Amazon EC2 console at <https://console.aws.amazon.com/ec2/>.
2. From the console dashboard, choose Launch Instance.
3. The Choose an Amazon Machine Image (AMI) page displays a list of basic configurations, called Amazon Machine Images (AMIs), that serve as templates for your instance. Select the AMI for Microsoft Windows Server 2012 R2 Base or Microsoft Windows Server 2008 R2 Base. Notice that these AMIs are marked "Free tier eligible."
4. On the Choose an Instance Type page, you can select the hardware configuration of your instance. Select the t2.micro type, which is selected by default. Notice that this instance type is eligible for the free tier.
5. Choose Review and Launch to let the wizard complete the other configuration settings for you.
6. On the Review Instance Launch page, under Security Groups, you'll see that the wizard created and selected a security group for you. You can use this security group, or alternatively you can select the security group that you created when getting set up using the following steps:
 - A) Choose Edit security groups.
 - B) On the Configure Security Group page, ensure that Select an existing security group is selected.
 - C) Select your security group from the list of existing security groups, and then choose Review and Launch.
7. On the Review Instance Launch page, choose Launch.
8. When prompted for a key pair, select Choose an existing key pair, then select the key pair that you created when getting set up.

Alternatively, you can create a new key pair. Select **Create a new key pair**, enter a name for the key pair, and then choose **Download Key Pair**. This is the only chance for you to save the private key file, so be sure to download it. Save the private key file in a safe place. You'll need to provide the name of your key pair when you launch an instance and the corresponding private key each time you connect to the instance.

Caution

- ❖ Don't select the **Proceed without a key pair** option. If you launch your instance without a key pair, then you can't connect to it.

When you are ready, select the acknowledgement check box, and then choose **Launch Instances**.

9. A confirmation page lets you know that your instance is launching. Choose **View Instances** to close the confirmation page and return to the console.
10. On the **Instances** screen, you can view the status of the launch. It takes a short time for an instance to launch. When you launch an instance, its initial state is **pending**. After the instance starts, its state changes to **running** and it receives a public DNS name. (If the **Public DNS** column is hidden, choose the **Show/Hide** icon in the top right corner of the page and then select **Public DNS**.)
11. It can take a few minutes for the instance to be ready so that you can connect to it. Check that your instance has passed its status checks; you can view this information in the **Status Checks** column.

Steps



Figure 1

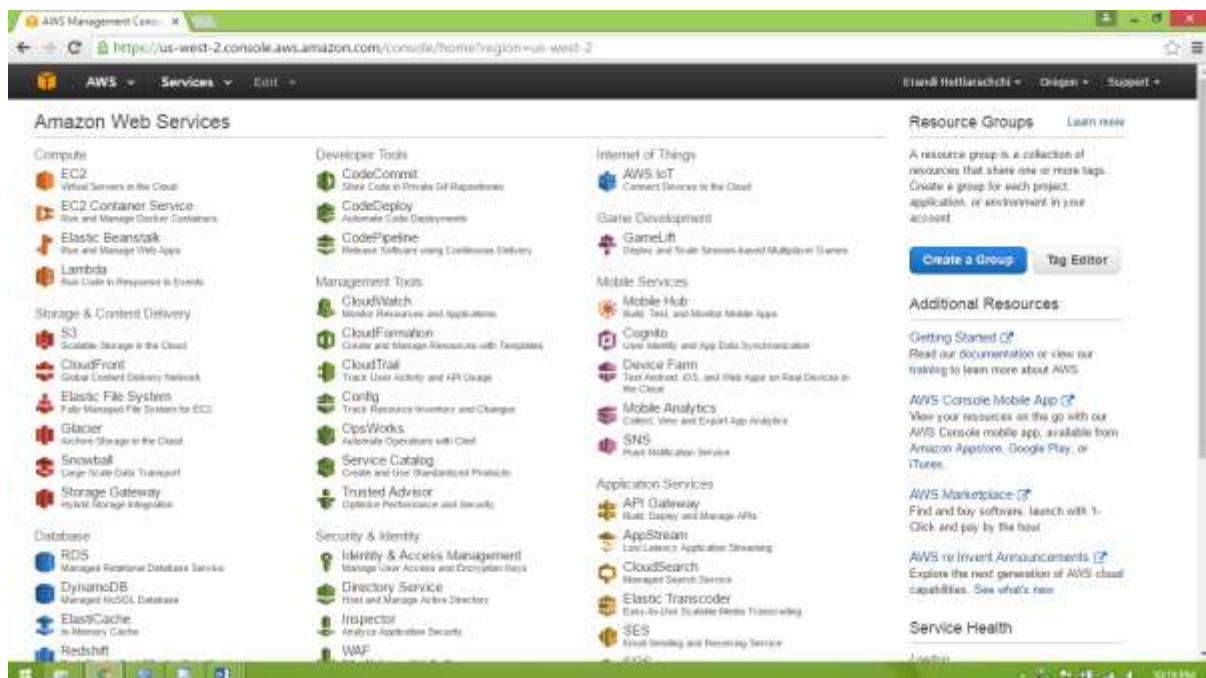


Figure 2

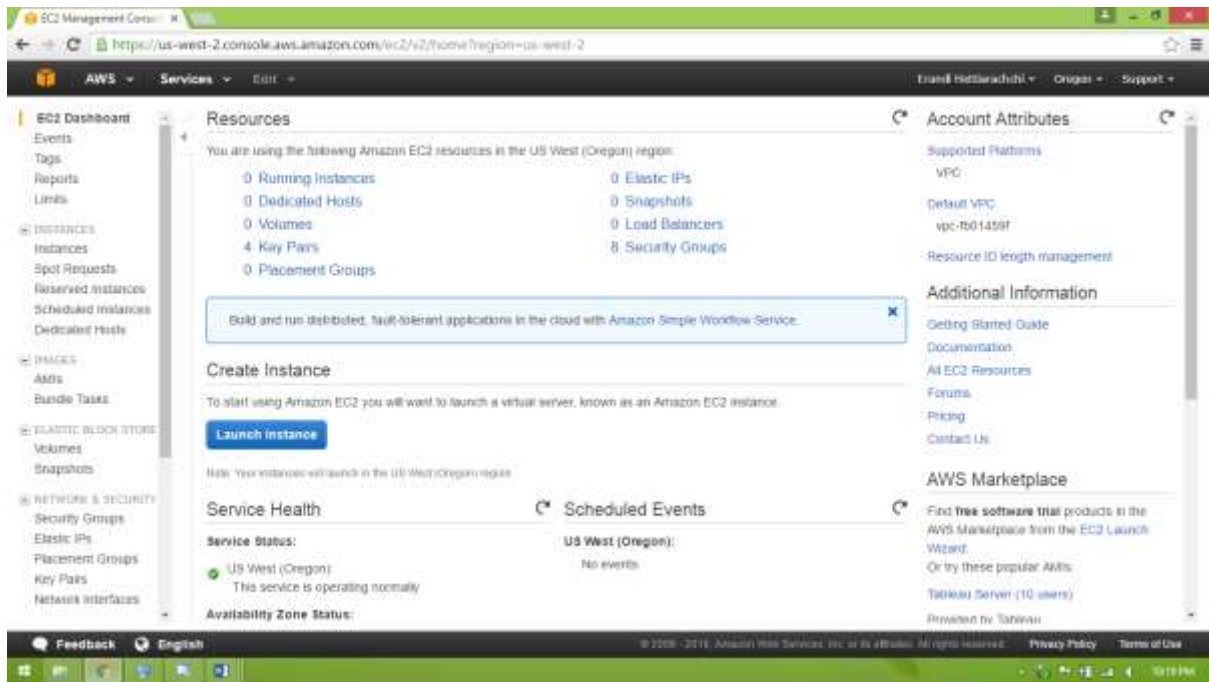


Figure 3

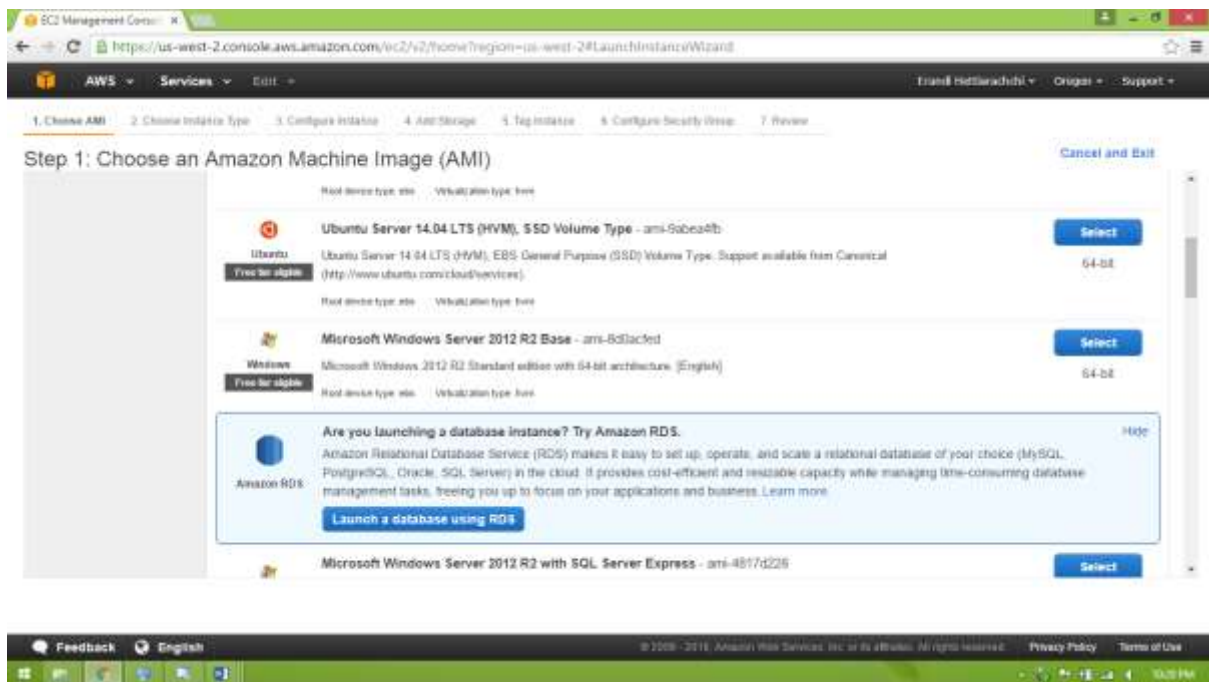


Figure 4

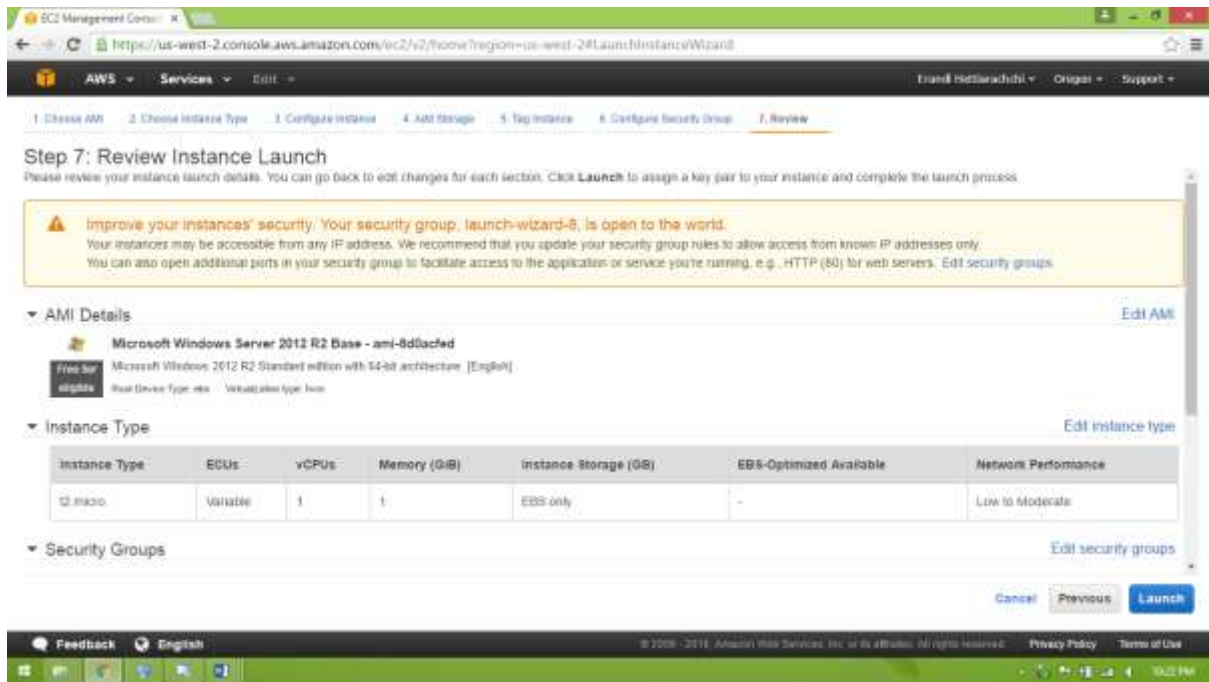


Figure 5

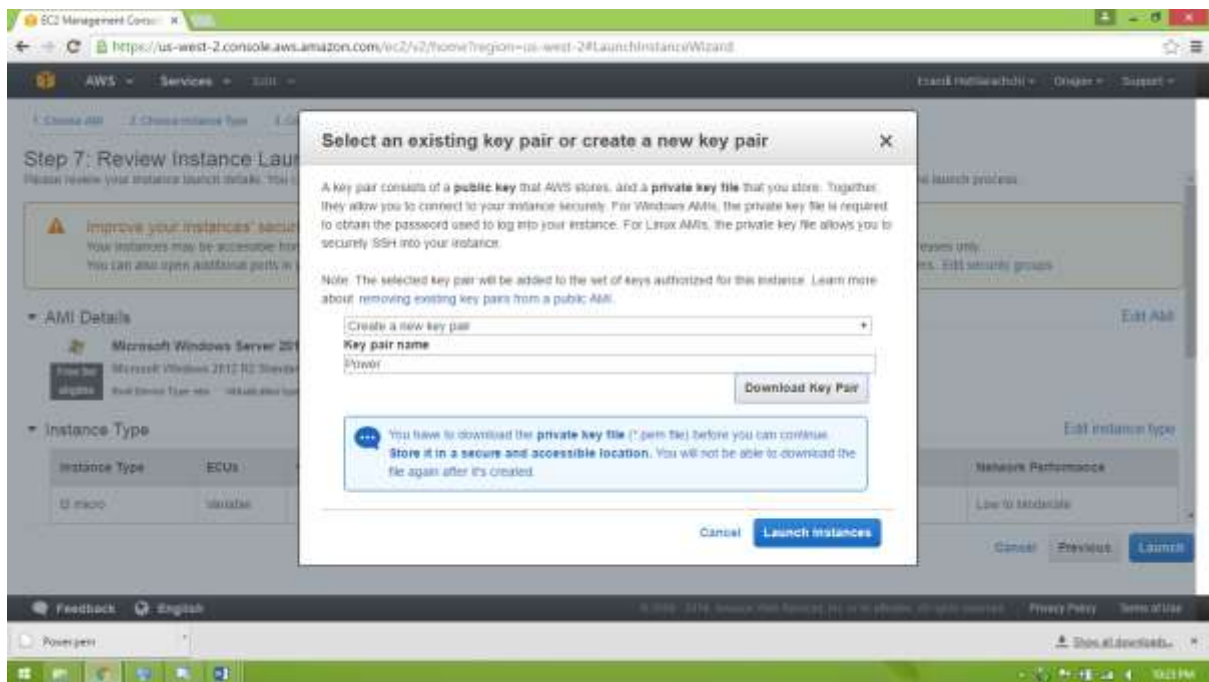


Figure 6

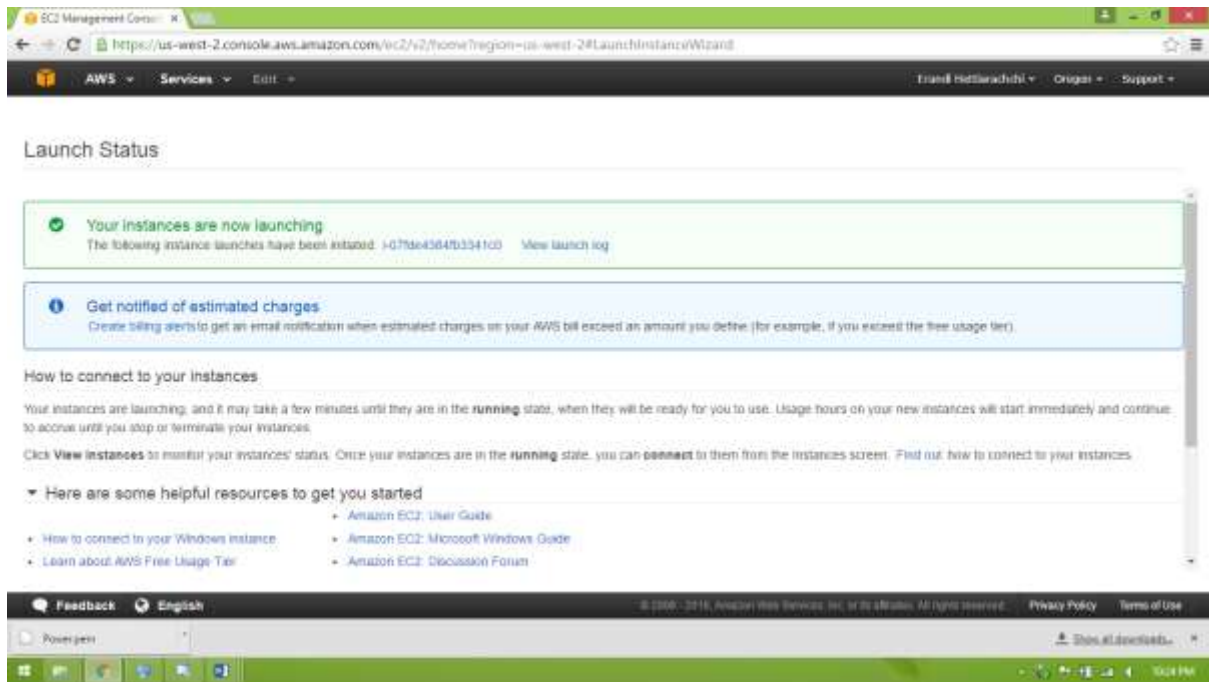


Figure 7

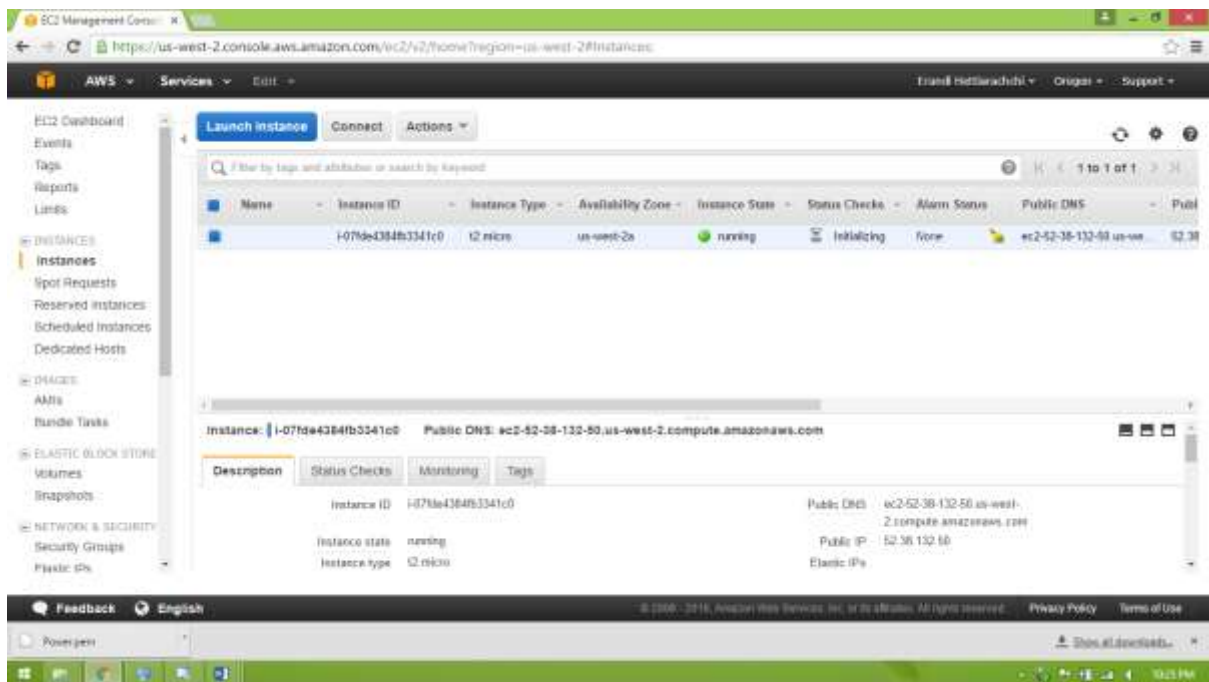


Figure 8

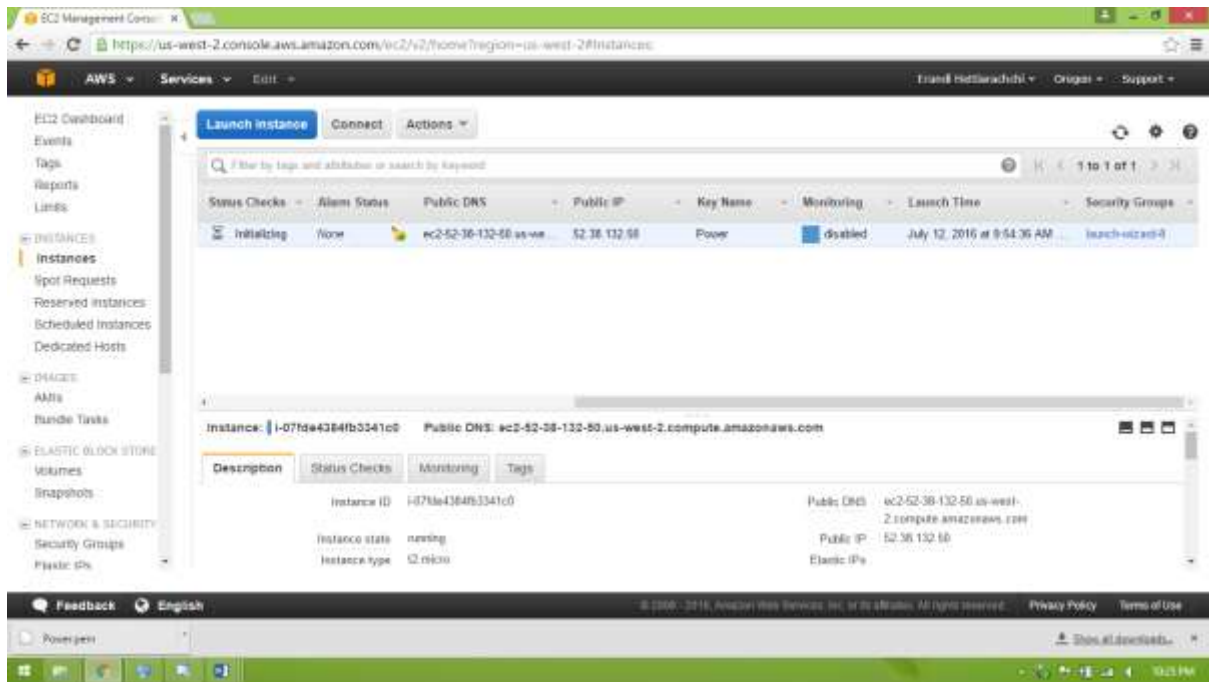


Figure 9

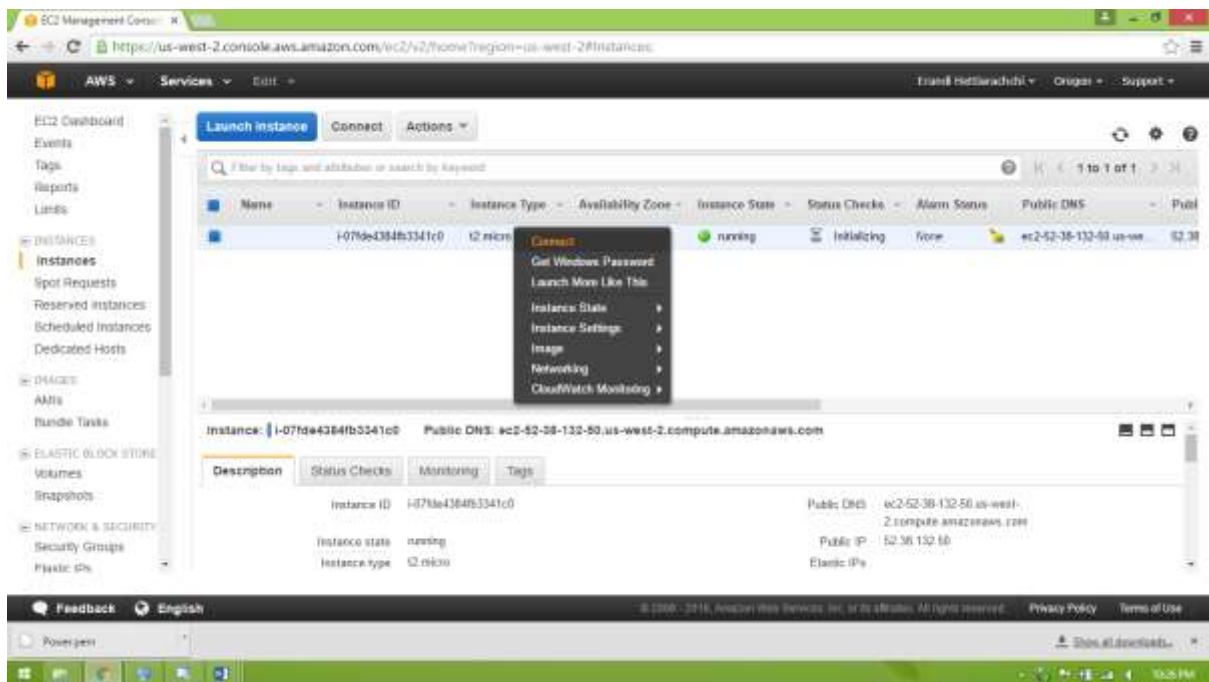


Figure 10

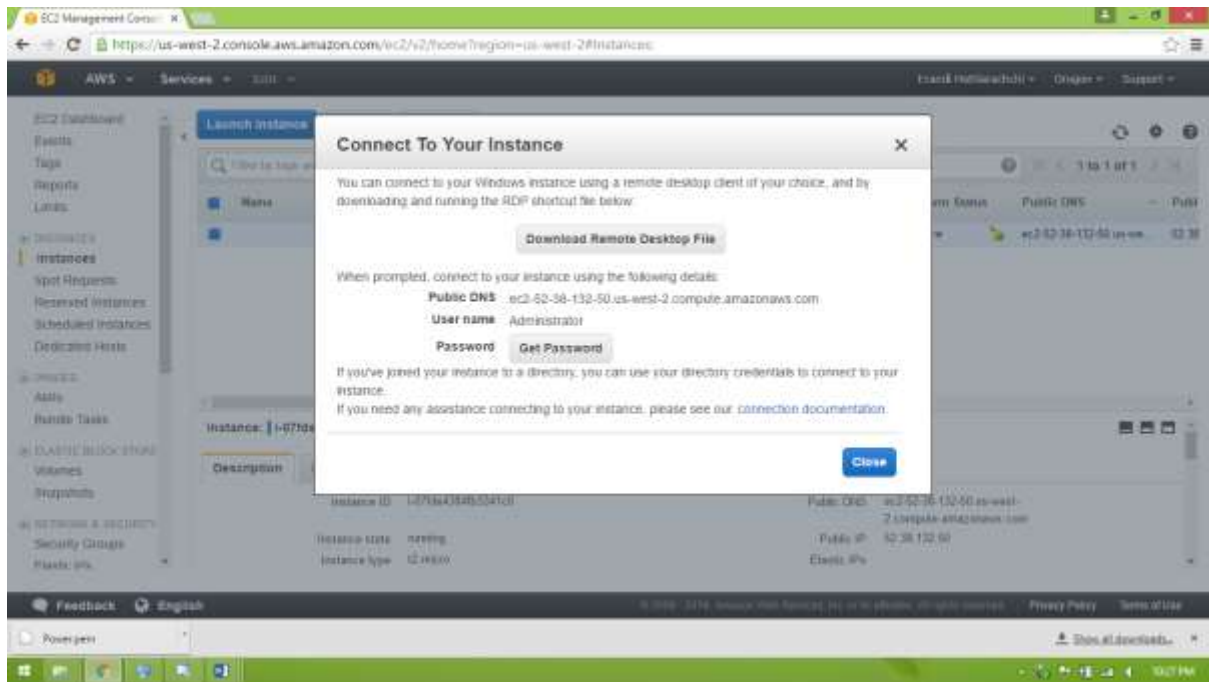


Figure 11

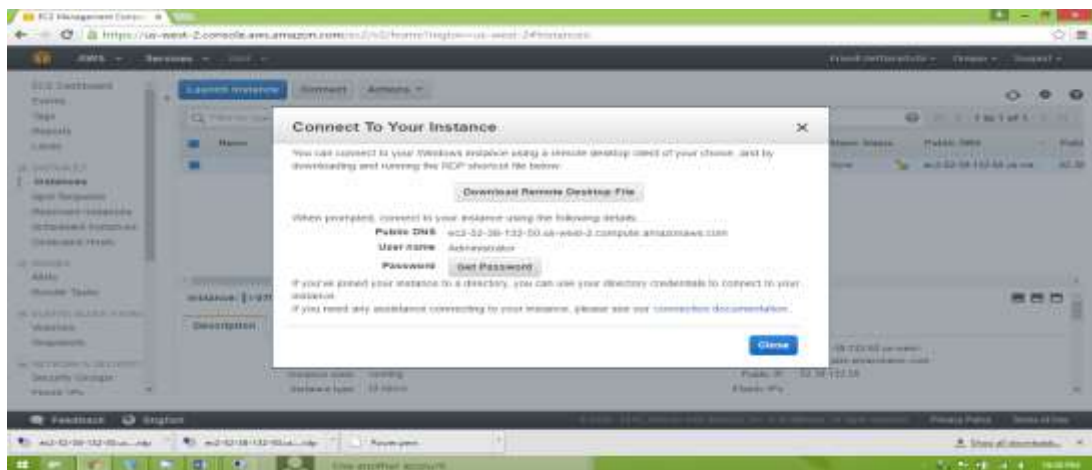


Figure 12

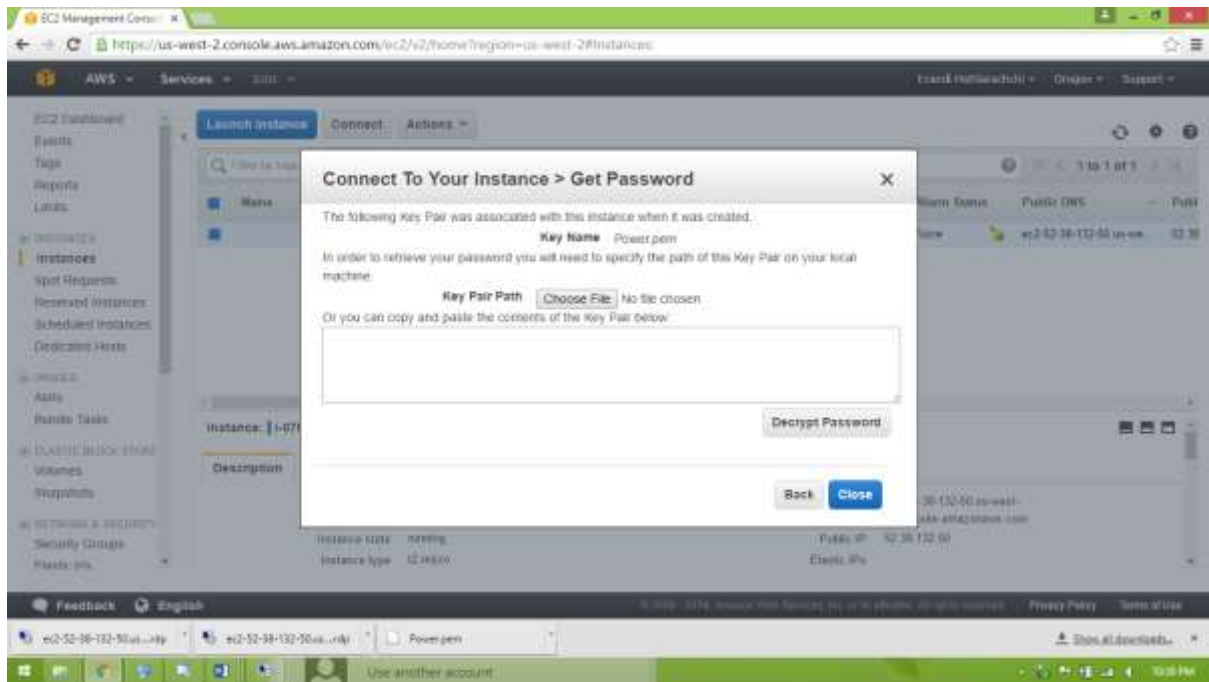


Figure 13

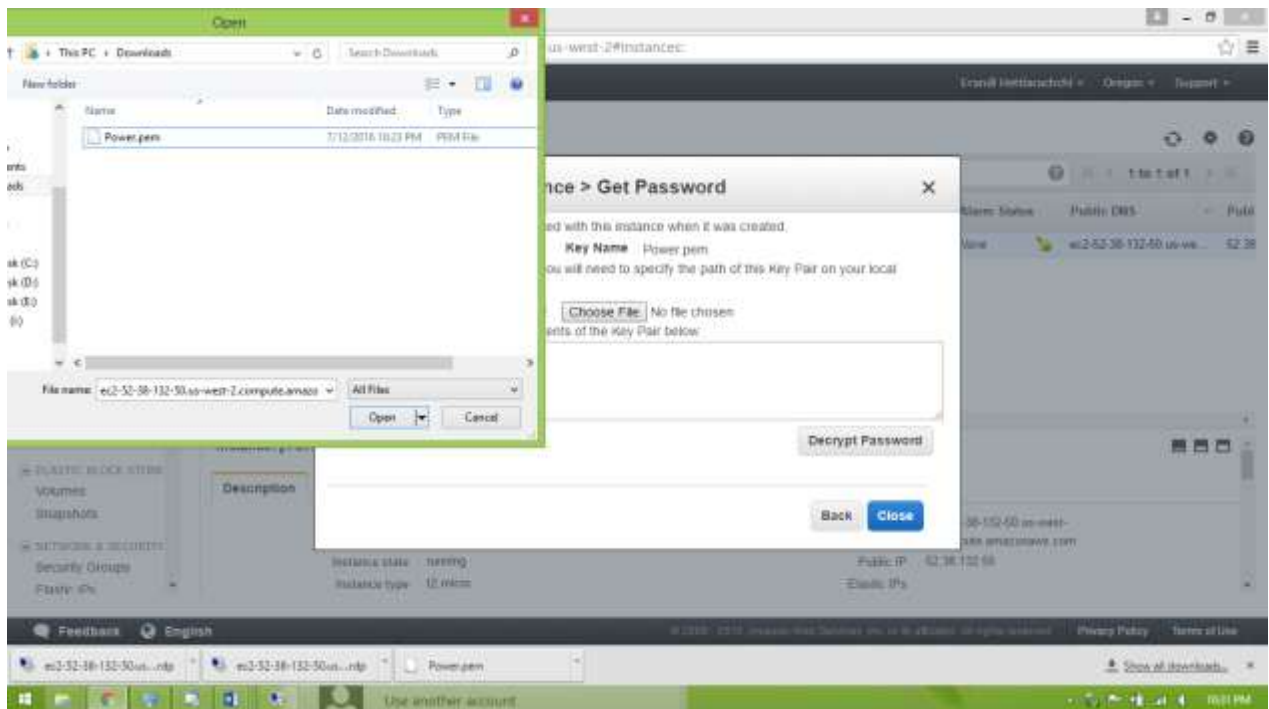


Figure 14

After the Open Power.pem path

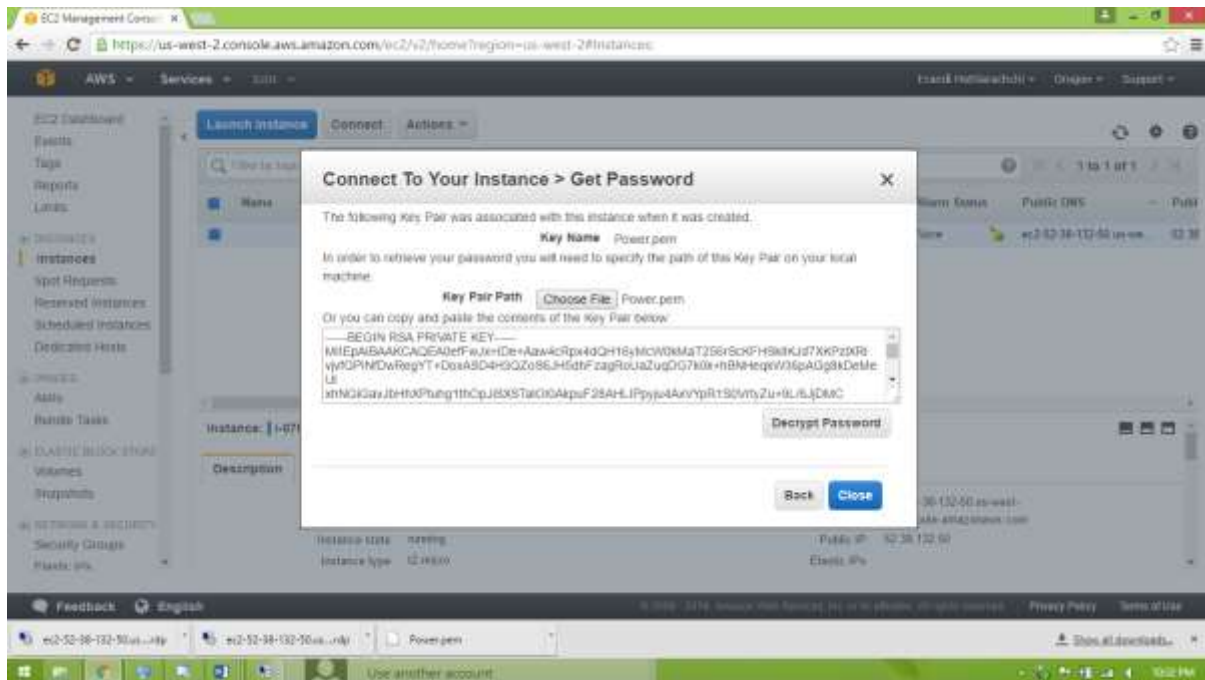


Figure 15

2) Step2: Connect to Your Instance

To connect to a Windows instance, you must retrieve the initial administrator password and then specify this password when you connect to your instance using Remote Desktop.

Note

If you've joined your instance to a domain, you can connect to your instance using domain credentials you've defined in AWS Directory Service. For more information about connecting to an instance in a domain, see [Connecting To Your Instance Using Domain Credentials](#).

The name of the administrator account depends on the language of the operating system. For example, for English, it's Administrator, for French It's Administrator, and for Portuguese it's Administrator. For more information,

see Localized Names for Administrator Account in Windows in the Microsoft TechNet Wiki.

The license for the Windows Server operating system (OS) allows two simultaneous remote connections for administrative purposes. The license for Windows Server is included in the price of your EC2 instance. If you need more than two simultaneous remote connections, you must purchase a Remote Desktop Services (RDS) license. If you attempt a third connection, an error will occur. For more information, see [Configure the Number of Simultaneous Remote Connections Allowed for a Connection](#).

To connect to your Windows instance using an RDP client

1. In the Amazon EC2 console, select the instance, and then choose Connect.
2. In the Connect to Your Instance dialog box, choose Get Password (it will take a few minutes after the instance is launched before the password is available).
3. Choose Browse and navigate to the private key file you created when you launched the instance. Select the file and choose Open to copy the entire contents of the file into contents box.
4. Choose Decrypt Password. The console displays the default administrator password for the instance in the Connect to Your Instance dialog box, replacing the link to Get Password shown previously with the actual password.
5. Record the default administrator password, or copy it to the clipboard. You need this password to connect to the instance.
6. Choose Download Remote Desktop File. Your browser prompts you to either open or save the .rdp file. Either option is fine. When you have finished, you can choose Close to dismiss the Connect to Your Instance dialog box.

- If you opened the .rdp file, you'll see the Remote Desktop Connection dialog box.
 - If you saved the .rdp file, navigate to your downloads directory, and open the .rdp file to display the dialog box.
7. You may get a warning that the publisher of the remote connection is unknown. If you are using Remote Desktop Connection from a Windows PC, choose Connect to connect to your instance. If you are using Microsoft Remote Desktop on a Mac, skip the next step.
 8. When prompted, log in to the instance, using the administrator account for the operating system and the password that you recorded or copied previously. If your Remote Desktop Connection already has an administrator account set up, you might have to choose the Use another account option and enter the user name and password manually.

Note

- ❖ Sometimes copying and pasting content can corrupt data. If you encounter a "Password Failed" error when you log in, try typing in the password manually.
9. Due to the nature of self-signed certificates, you may get a warning that the security certificate could not be authenticated. Use the following steps to verify the identity of the remote computer, or simply choose Yes or Continue to continue if you trust the certificate.
 - a. If you are using Remote Desktop Connection from a Windows PC, choose View certificate. If you are using Microsoft Remote Desktop on a Mac, choose Show Certificate.
 - b. Choose the Details tab, and scroll down to the Thumbprint entry on a Windows PC, or the SHA1 Fingerprints entry on a Mac. This is the unique identifier for the remote computer's security certificate.

- c. In the Amazon EC2 console, select the instance, choose Actions, and then choose Get System Log.
- d. In the system log output, look for an entry labeled RDPCERTIFICATE-THUMBPRINT. If this value matches the thumbprint or fingerprint of the certificate, you have verified the identity of the remote computer.
- e. If you are using Remote Desktop Connection from a Windows PC, return to the Certificate dialog box and choose OK. If you are using Microsoft Remote Desktop on a Mac, return to the Verify Certificate and choose Continue.
- f. If you are using Remote Desktop Connection from a Windows PC, choose Yes in the Remote Desktop Connection window to connect to your instance. If you are using Microsoft Remote Desktop on a Mac, log in to the instance as prompted, using the default Administrator account and the default administrator password that you recorded or copied previously.

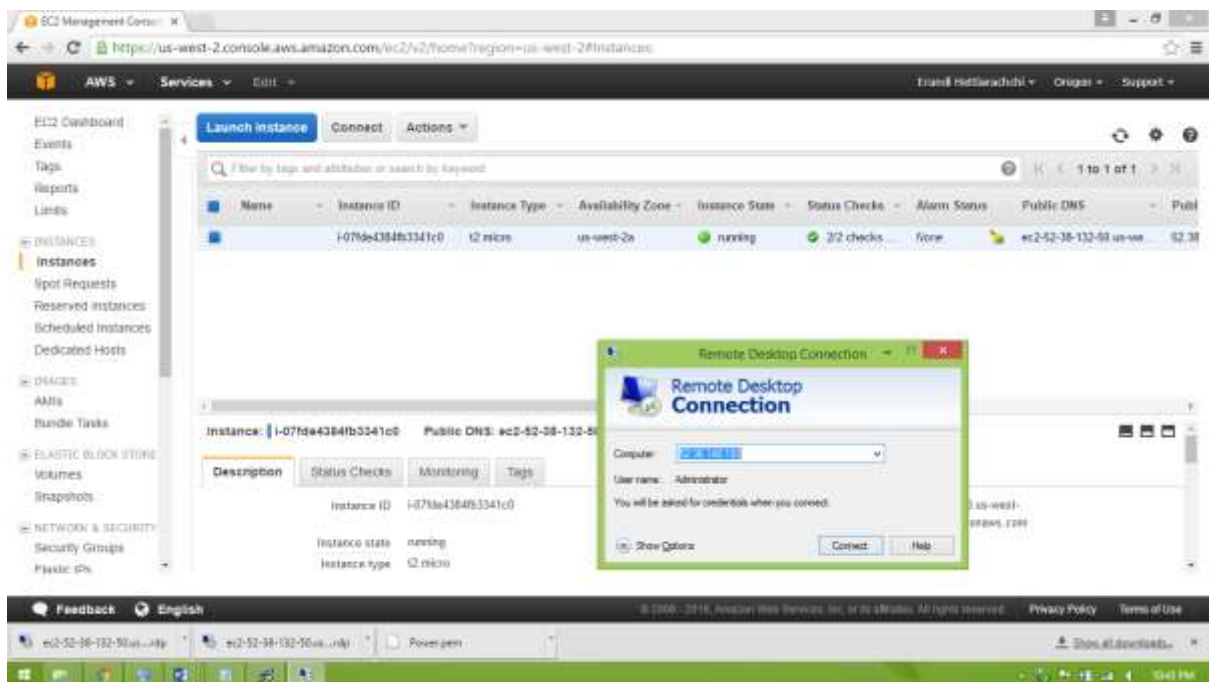


Figure 16

3) Step3: Clean Up Your Instance

After you've finished with the instance that you created for this tutorial, you should clean up by terminating the instance. If you want to do more with this instance before you clean up, see Next Steps.

Important

Terminating an instance effectively deletes it; you can't reconnect to an instance after you've terminated it.

If you launched an instance that is not within the AWS Free Tier, you'll stop incurring charges for that instance as soon as the instance status changes to shutting down or terminated. If you'd like to keep your instance for later, but not incur charges, you can stop the instance now and then start it again later. For more information, see [Stopping Instances](#).

To terminate your instance

1. In the navigation pane, choose Instances. In the list of instances, select the instance.
2. Choose Actions, then Instance State, and then choose Terminate.
3. Choose Yes, Terminate when prompted for confirmation.

Amazon EC2 shuts down and terminates your instance. After your instance is terminated, it remains visible on the console for a short while, and then the entry is deleted.

Next Steps

After you start your instance, you might want to try some of the following exercises:

- Configure a Cloud Watch alarm to notify you if your usage exceeds the Free Tier. For more information, see [Create a Billing Alarm in the AWS Billing and Cost Management User Guide](#).
- Add an EBS volume. For more information, see [Creating an Amazon EBS Volume and Attaching an Amazon EBS Volume to an Instance](#).
- Install the WAMP or WIMP stack. For more information, see [Tutorial: Installing a WAMP Server on an Amazon EC2 Instance Running Windows Server](#) and [Tutorial: Installing a WIMP Server on an Amazon EC2 Instance Running Windows Server](#).



Figure 17

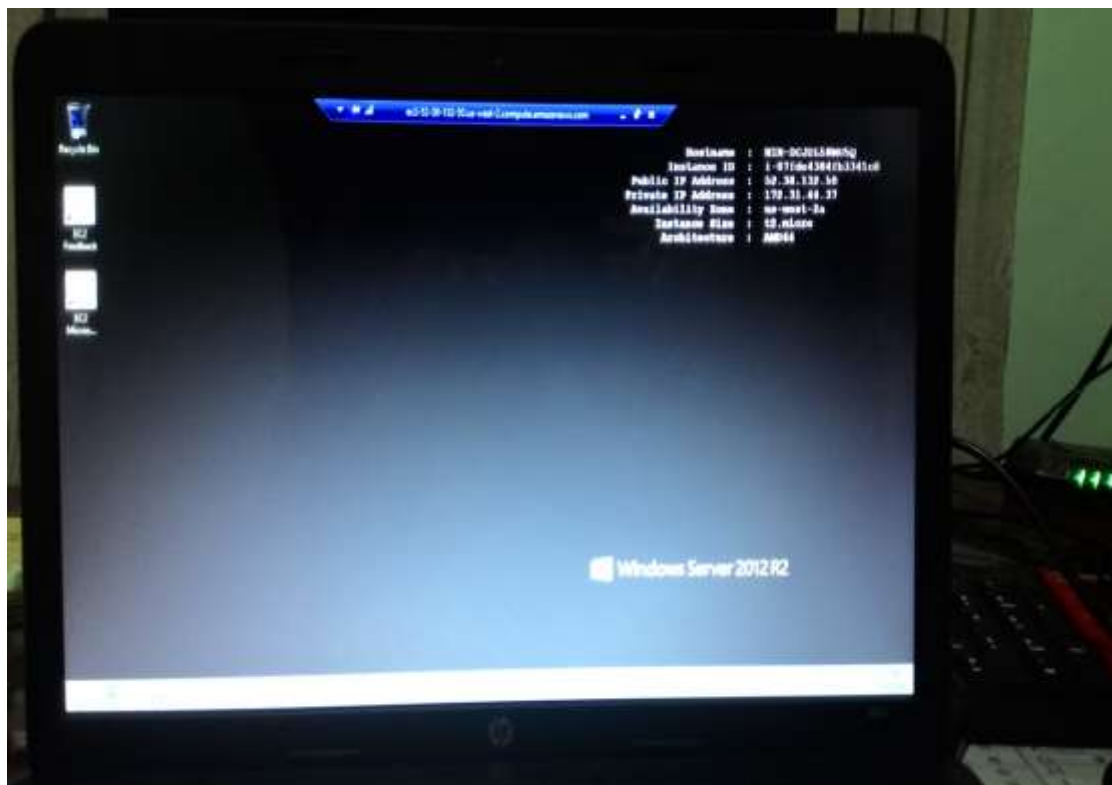


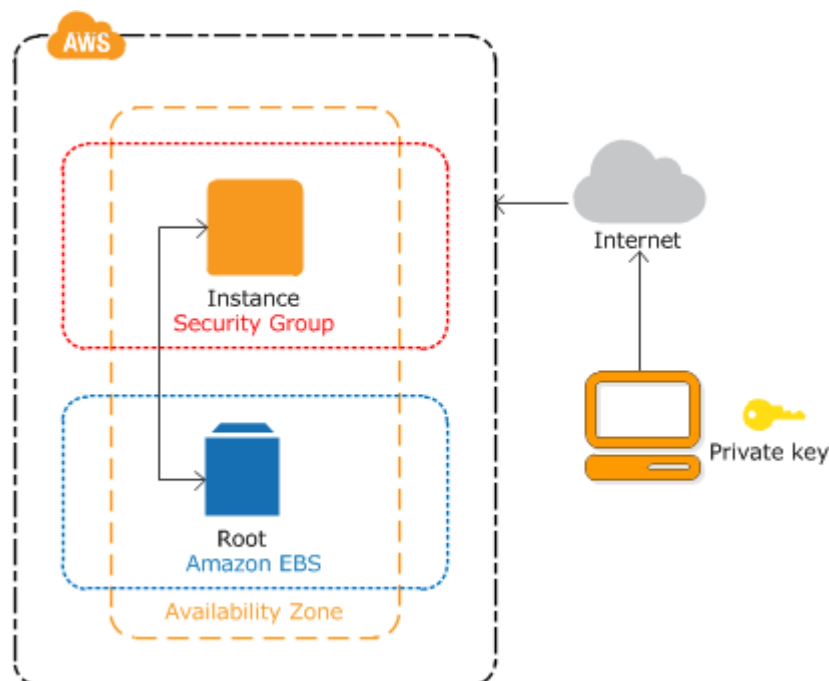
Figure 18

Getting Started with Amazon EC2 Linux Instances

Tasks

Perform the following tasks:

- 1) Launch an Instance
- 2) Connect to Your Instance
- 3) Clean Up Your Instance



1) Step 1: Launch an Instance

You can launch a Linux instance using the AWS Management Console as described in the following procedure. This tutorial is intended to help you launch your first instance quickly, so it doesn't cover all possible options. For more information about the advanced options, see [Launching an Instance](#).

To launch an instance

1. Open the Amazon EC2 console at <https://console.aws.amazon.com/ec2/>.
2. From the console dashboard, choose Launch Instance.
3. The Choose an Amazon Machine Image (AMI) page displays a list of basic configurations, called Amazon Machine Images (AMIs), that serve as templates for your instance. Select the HVM edition of the Amazon Linux AMI. Notice that this AMI is marked "Free tier eligible."
4. On the Choose an Instance Type page, you can select the hardware configuration of your instance. Select the t2.micro type, which is selected by default. Notice that this instance type is eligible for the free tier.
5. Choose Review and Launch to let the wizard complete the other configuration settings for you.
6. On the Review Instance Launch page, under Security Groups, you'll see that the wizard created and selected a security group for you. You can use this security group, or alternatively you can select the security group that you created when getting set up using the following steps:
 - a. Choose Edit security groups.
 - b. On the Configure Security Group page, ensure that Select an existing security group is selected.
 - c. Select your security group from the list of existing security groups, and then choose Review and Launch.
7. On the Review Instance Launch page, choose Launch.
8. When prompted for a key pair, select Choose an existing key pair, then select the key pair that you created when getting set up.

Alternatively, you can create a new key pair. Select Create a new key pair, enter a name for the key pair, and then choose Download Key Pair. This is the only chance for you to save the private key file, so be sure to download it. Save the private key file in a safe place. You'll need to provide the name

of your key pair when you launch an instance and the corresponding private key each time you connect to the instance.

Caution

Don't select the Proceed without a key pair option. If you launch your instance without a key pair, then you can't connect to it.

When you are ready, select the acknowledgement check box, and then choose Launch Instances.

9. A confirmation page lets you know that your instance is launching. Choose View Instances to close the confirmation page and return to the console.
10. On the Instances screen, you can view the status of the launch. It takes a short time for an instance to launch. When you launch an instance, its initial state is pending. After the instance starts, its state changes to running and it receives a public DNS name
11. It can take a few minutes for the instance to be ready so that you can connect to it. Check that your instance has passed its status checks; you can view this information in the Status Checks column.

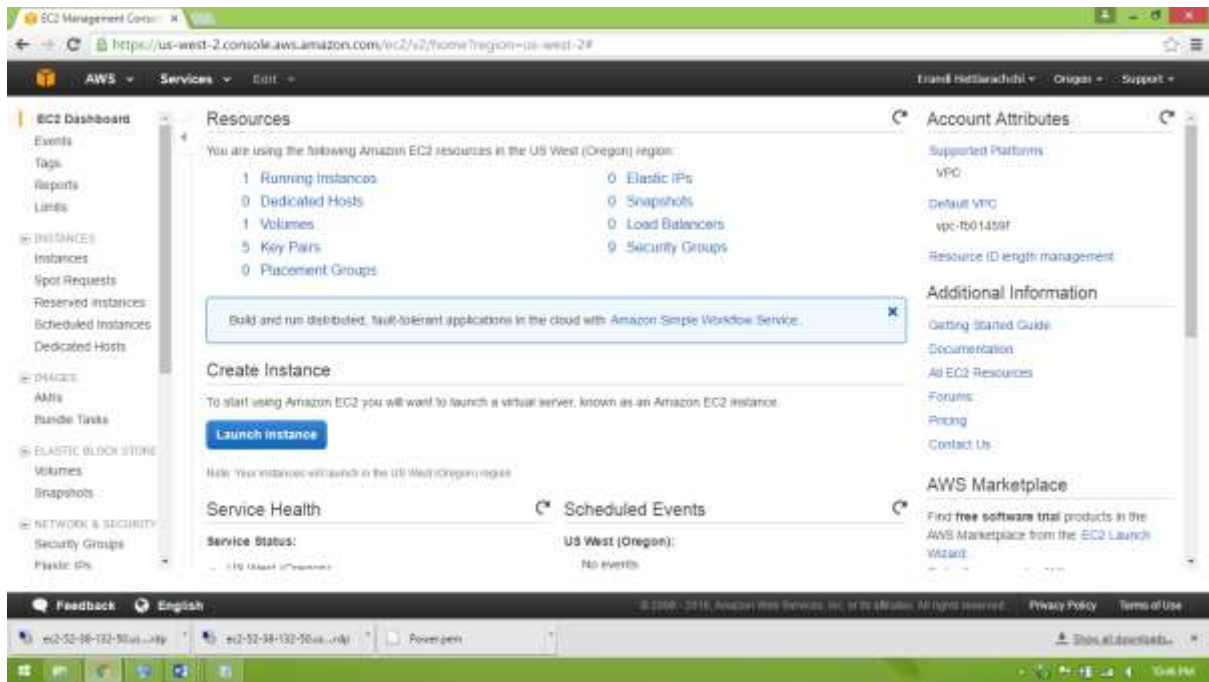


Figure 19

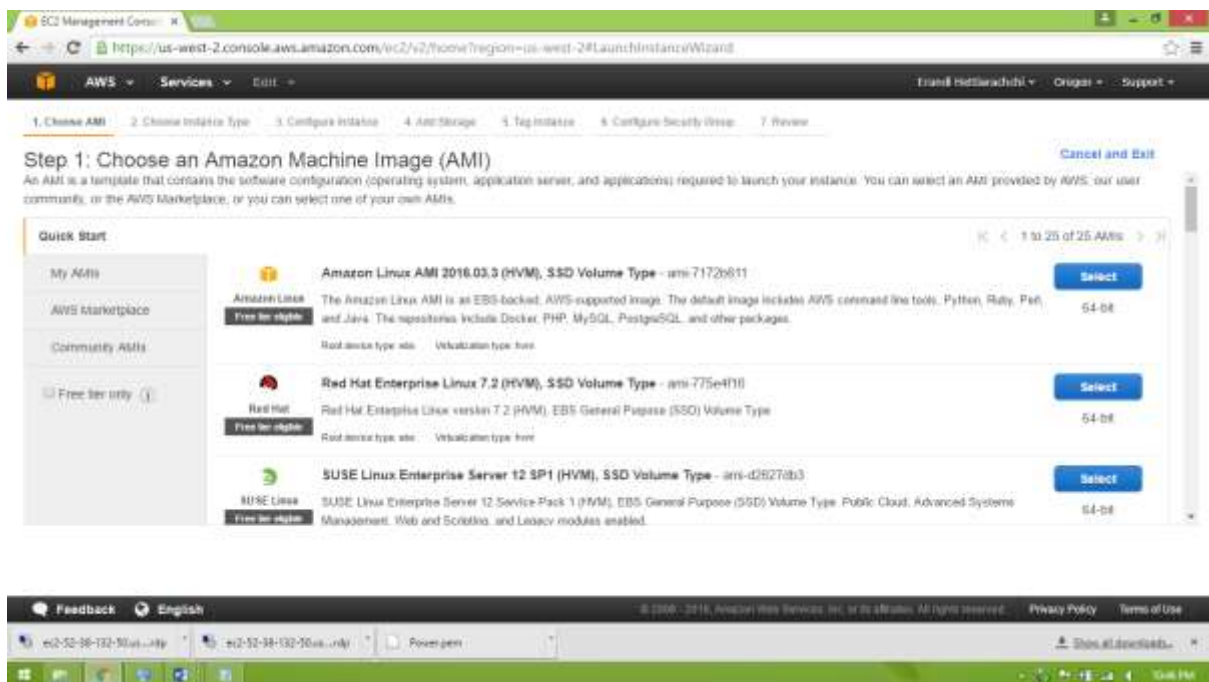


Figure 20

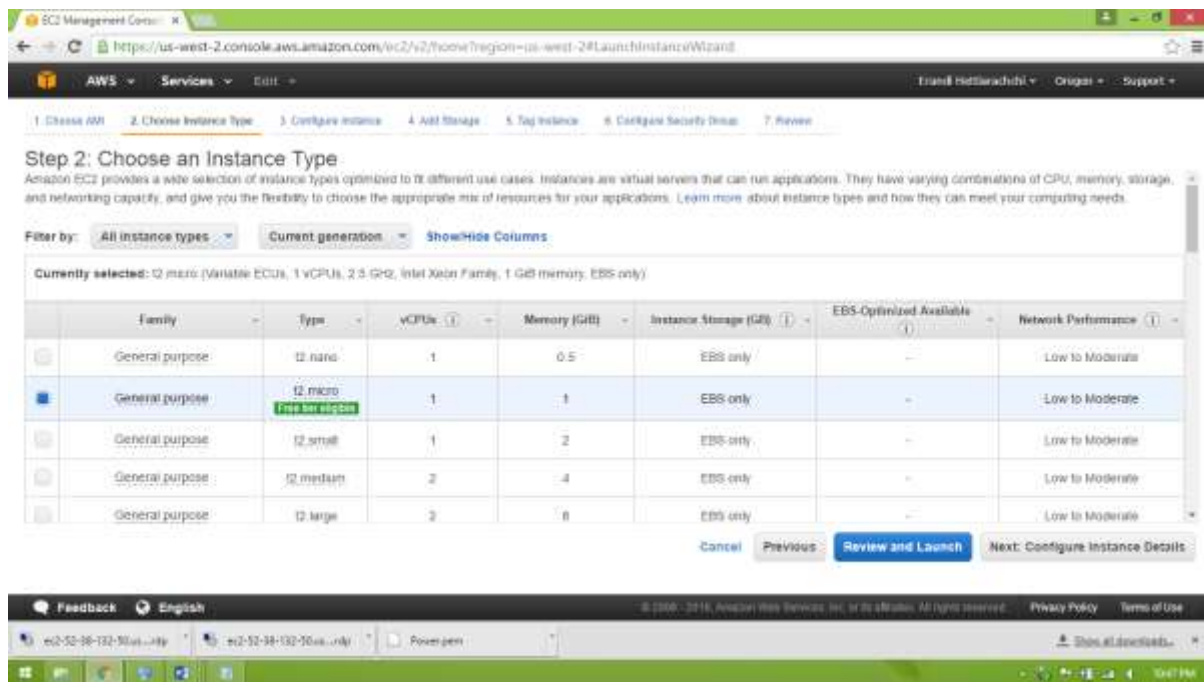


Figure 21

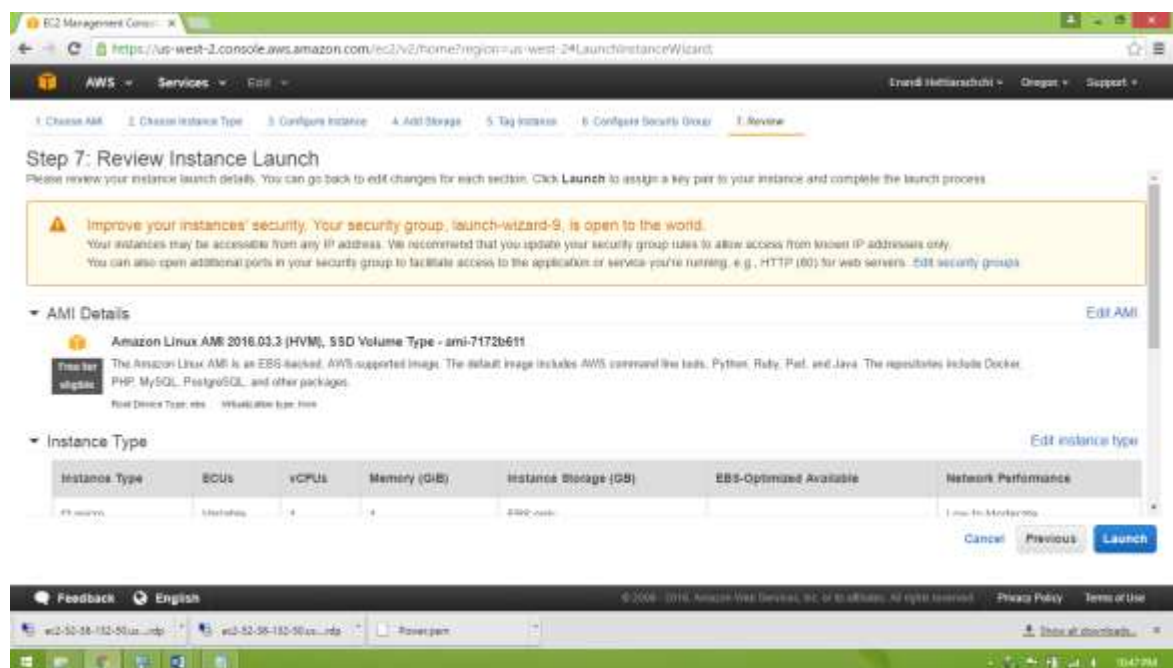


Figure 22

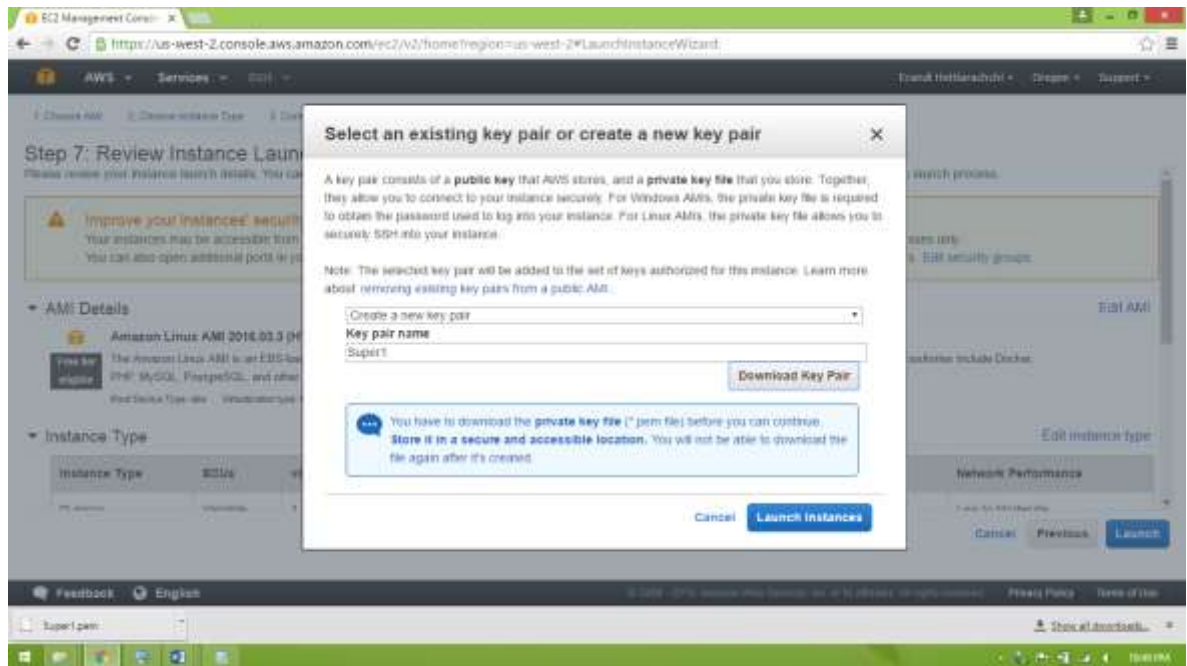


Figure 23

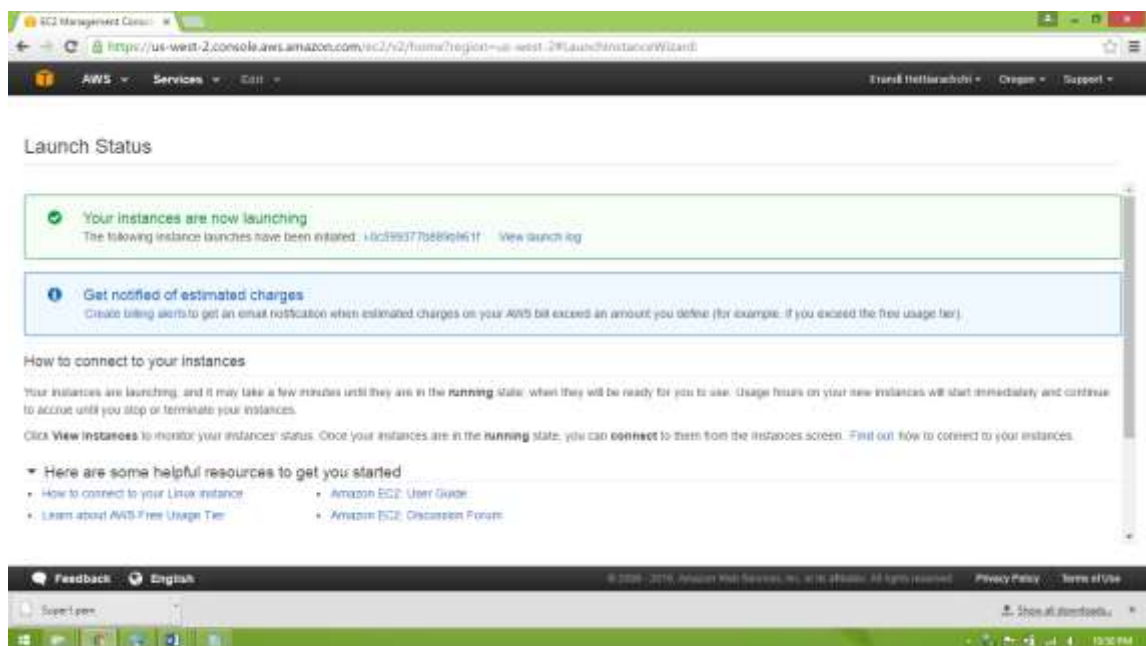


Figure 24

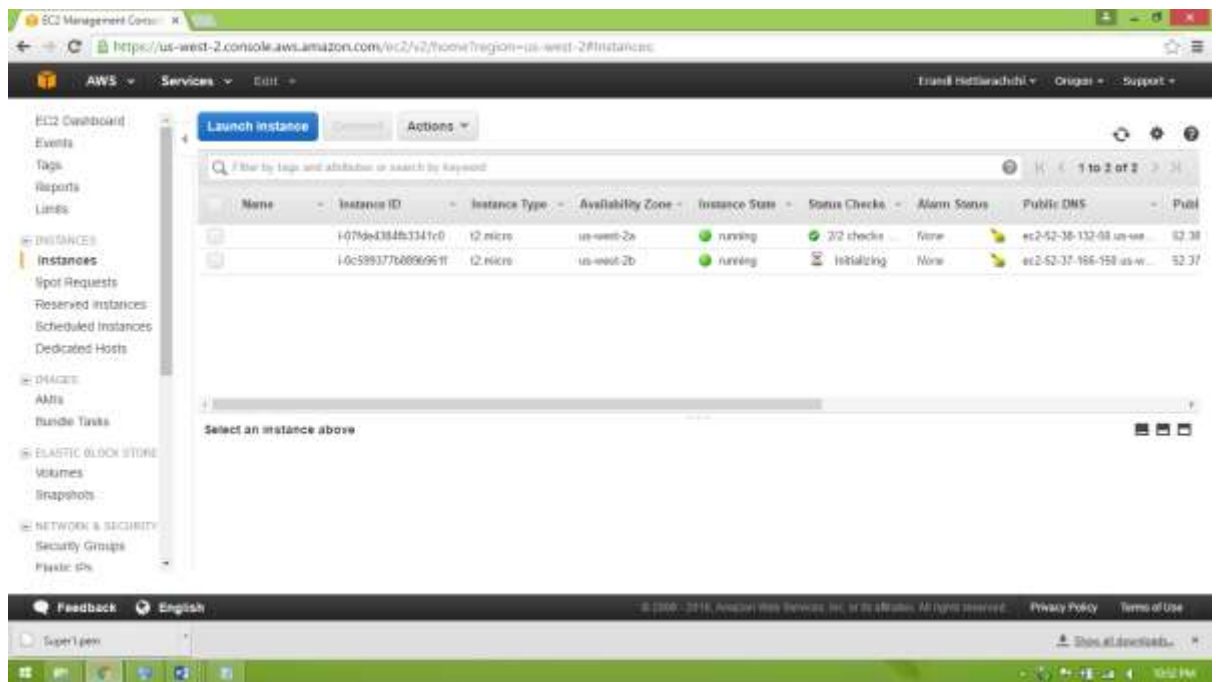


Figure 25

Or

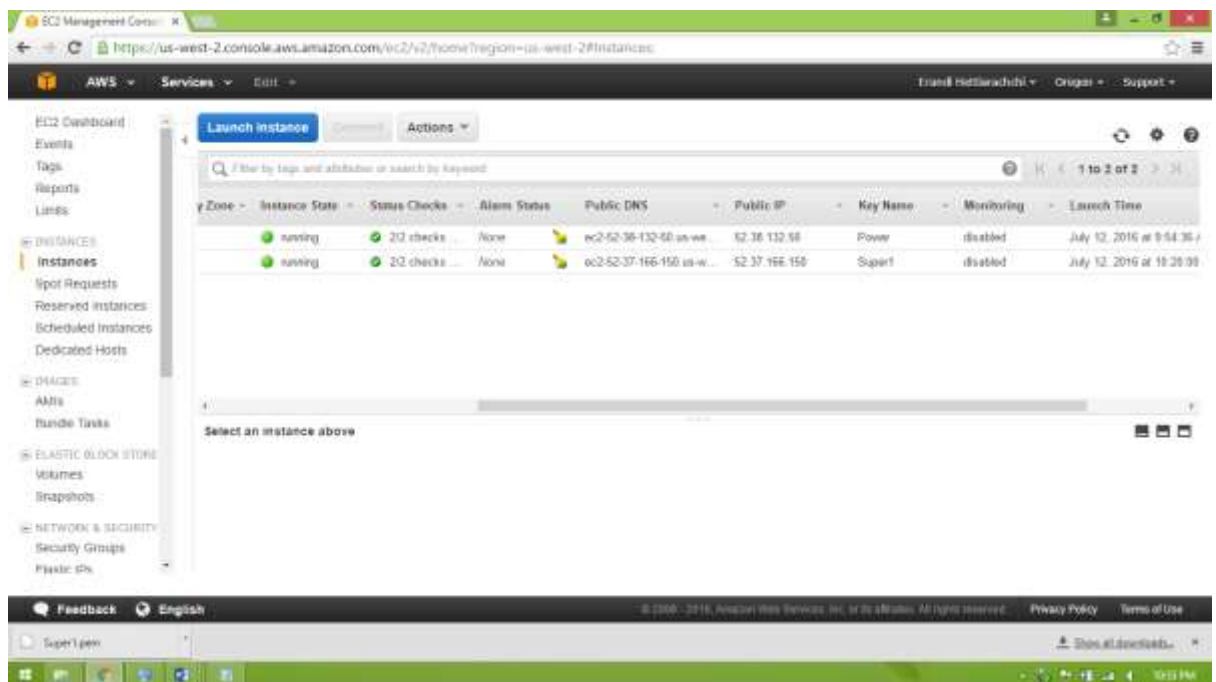


Figure 26

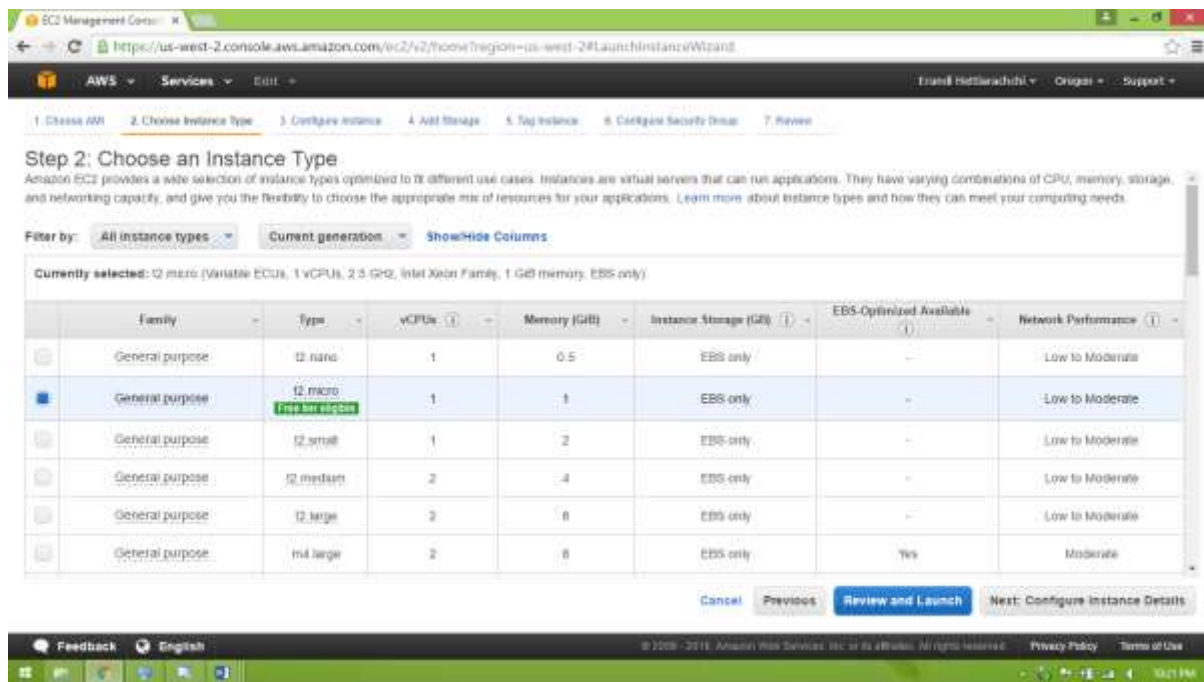


Figure 27

2) Step2: Connect to your Instance

There are several ways to connect to a Linux instance. In this procedure, you'll connect using your browser. Alternatively, you can connect using Putty or an SSH client. It's also assumed that you followed the steps earlier and launched an instance from an Amazon Linux AMI, which has a specific user name. Other Linux distributions may use a different user name. For more information, see [Connecting to Your Linux Instance from Windows Using Putty or Connecting](#).

Important

You can't connect to your instance unless you launched it with a key pair for which you have the .pem file and you launched it with a security group that allows SSH access. If you can't connect to your instance, see [Troubleshooting Connecting to Your Instance](#) for assistance.

To connect to your Linux instance using a web browser

1. You must have Java installed and enabled in the browser. If you don't have Java already, you can contact your system administrator to get it installed, or follow the steps outlined in the following pages: [Install Java and Enable Java in your web browser](#).
2. From the Amazon EC2 console, choose Instances in the navigation pane.
3. Select the instance, and then choose Connect.
4. Choose A Java SSH client directly from my browser (Java required).
5. Amazon EC2 automatically detects the public DNS name of your instance and populates Public DNS for you. It also detects the key pair that you specified when you launched the instance. Complete the following, and then choose Launch SSH Client.
 - a. In User name, enter ec2-user.
 - b. In Private key path, enter the fully qualified path to your private key (.pem) file, including the key pair name.
 - c. (Optional) Choose Store in browser cache to store the location of the private key in your browser cache. This enables Amazon EC2 to detect the location of the private key in subsequent browser sessions, until you clear your browser's cache.
6. If necessary, choose Yes to trust the certificate, and choose Run to run the Mind Term client.
7. If this is your first time running Mind Term, a series of dialog boxes asks you to accept the license agreement, confirm setup for your home directory, and confirm setup of the known hosts directory. Confirm these settings.
8. A dialog prompts you to add the host to your set of known hosts. If you do not want to store the host key information on your local computer, choose No.
9. A window opens and you are connected to your instance.

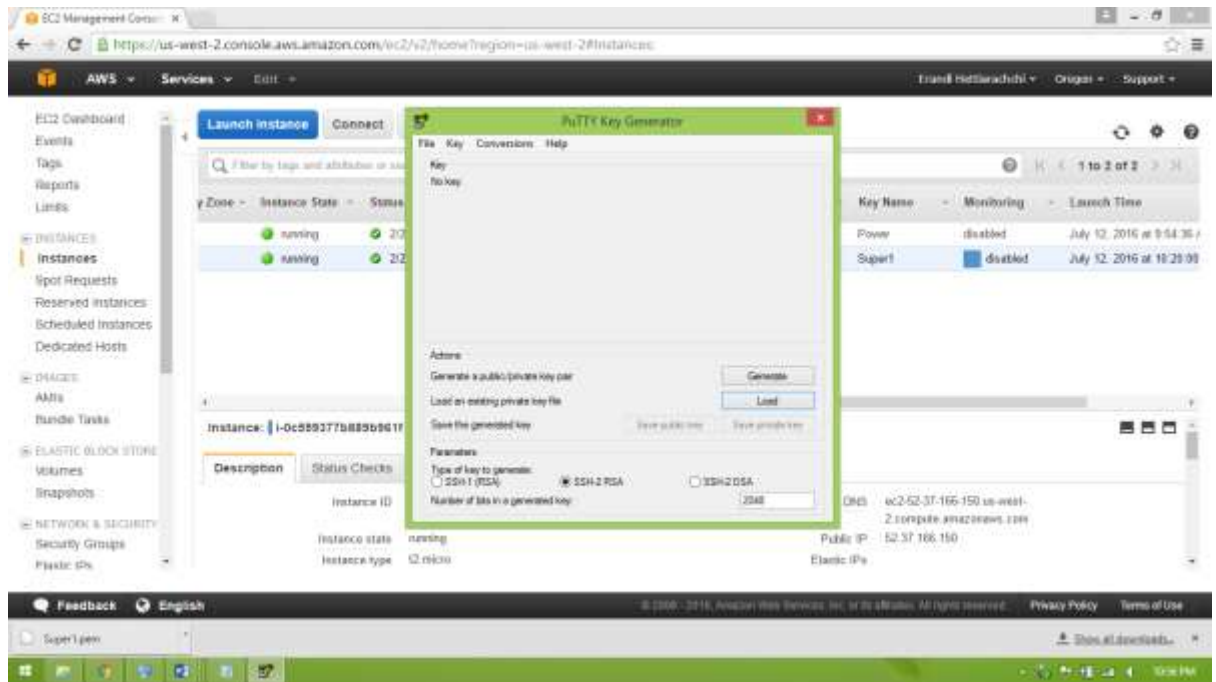


Figure 28

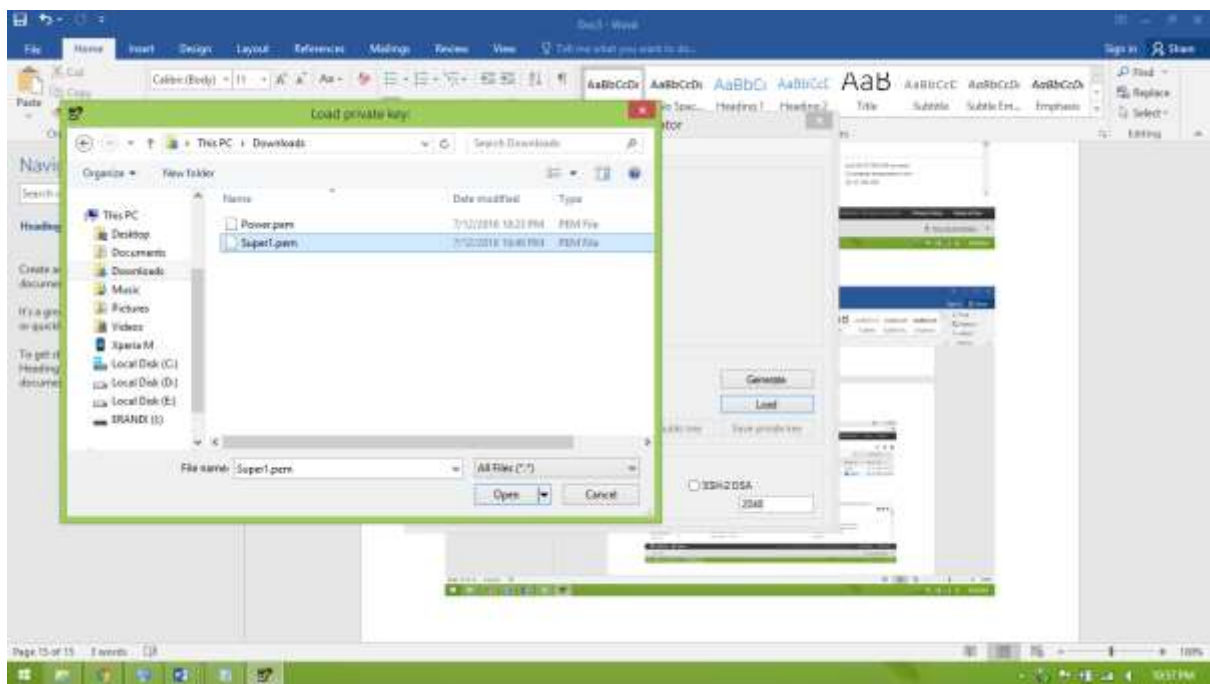


Figure 29

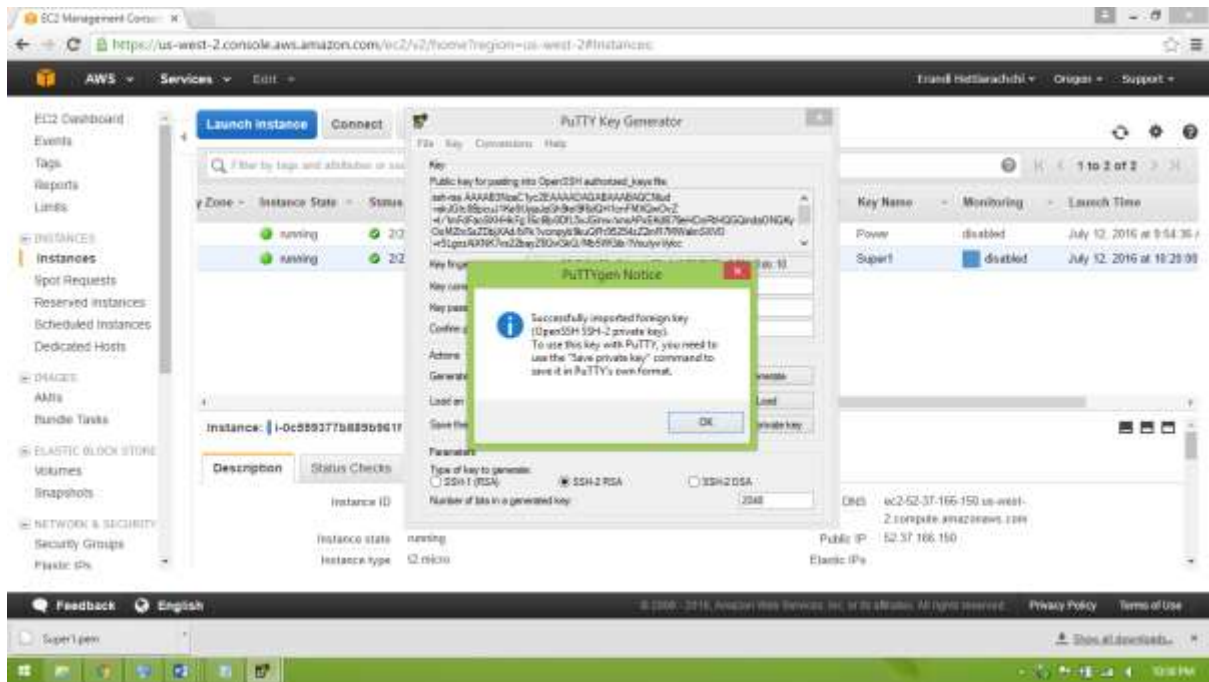


Figure 30

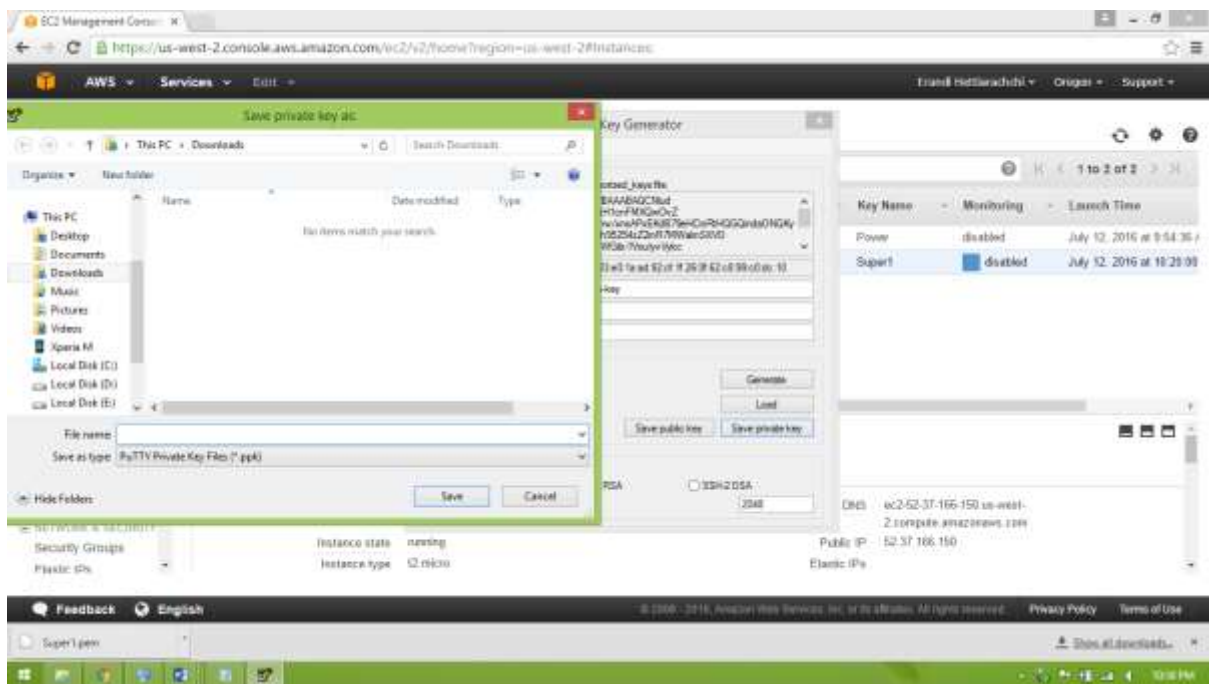


Figure 31

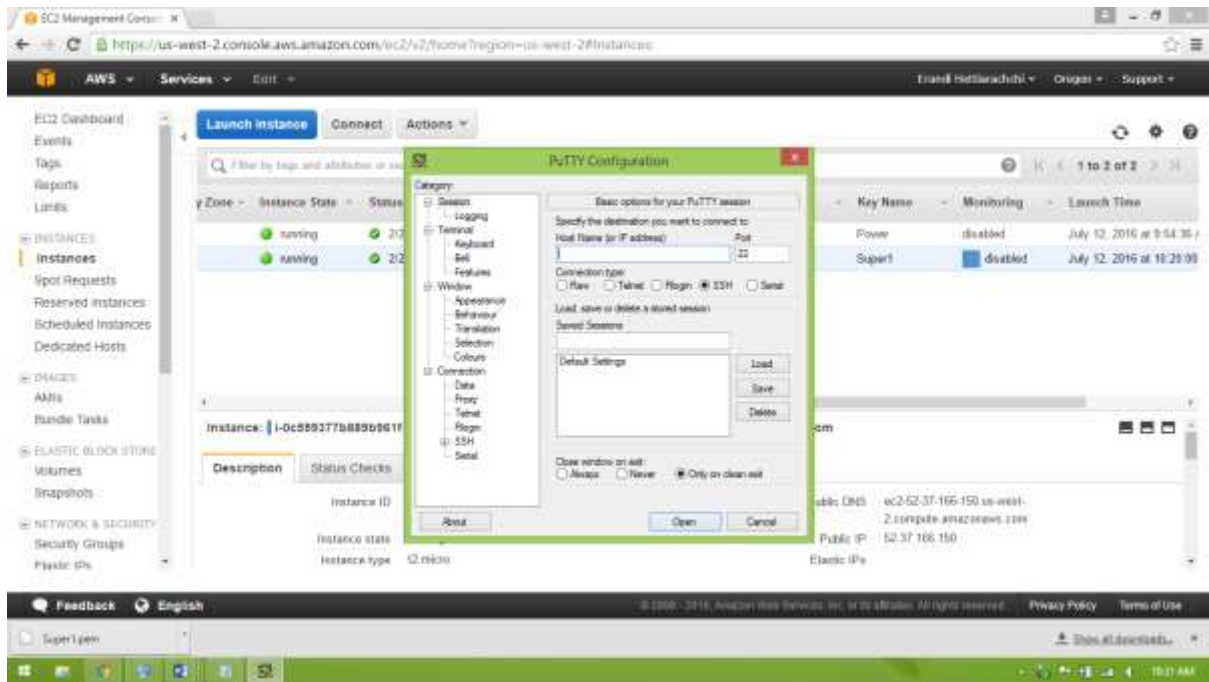


Figure 32

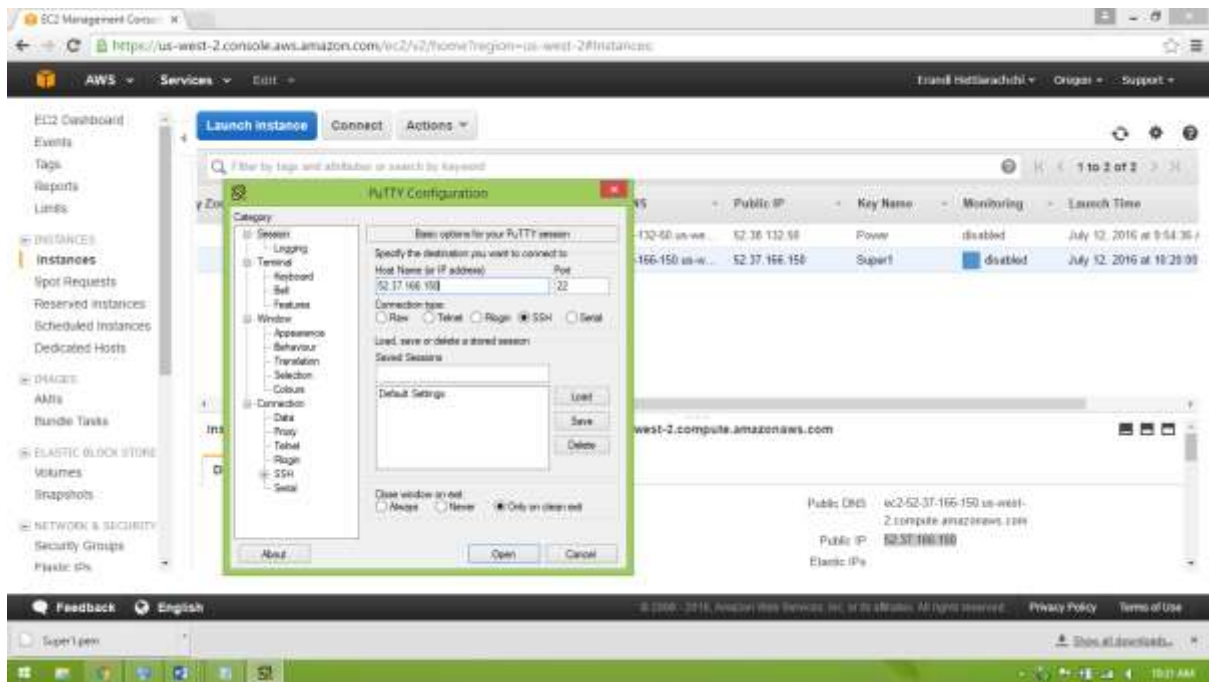


Figure 33

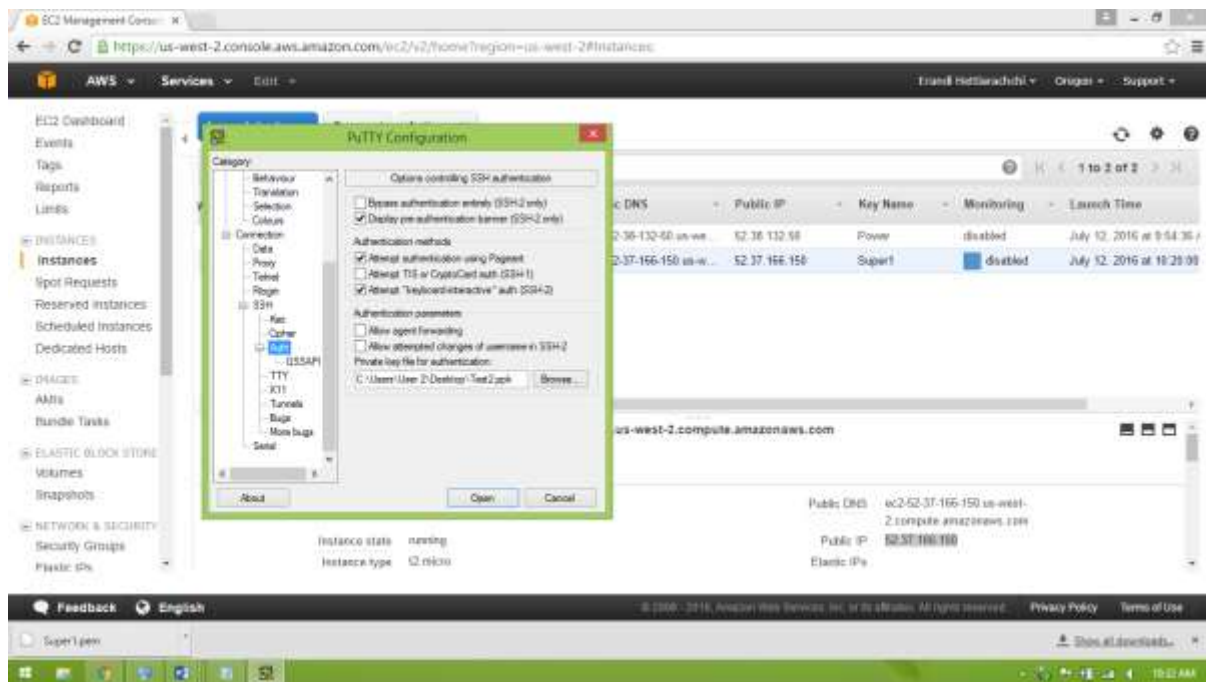


Figure 34

3) Step3: Clean Up Your Instance

After you've finished with the instance that you created for this tutorial, you should clean up by terminating the instance. If you want to do more with this instance before you clean up, see Next Steps.

Important

Terminating an instance effectively deletes it; you can't reconnect to an instance after you've terminated it.

If you launched an instance that is not within the AWS Free Tier, you'll stop incurring charges for that instance as soon as the instance status changes to shutting down or terminated. If you'd like to keep your instance for later, but not incur charges, you can stop the instance now and then start it again later. For more information, see Stopping Instances.

To terminate your instance

1. In the navigation pane, choose Instances. In the list of instances, select the instance.
2. Choose Actions, then Instance State, and then choose Terminate.
3. Choose Yes, Terminate when prompted for confirmation.

Amazon EC2 shuts down and terminates your instance. After your instance is terminated, it remains visible on the console for a short while, and then the entry is deleted.

Next Steps

After you start your instance, you might want to try some of the following exercises:

- Configure a Cloud Watch alarm to notify you if your usage exceeds the Free Tier. For more information, see [Create a Billing Alarm](#) in the AWS Billing and Cost Management User Guide.
- Add an EBS volume. For more information, see [Creating an Amazon EBS Volume and Attaching](#).
- Install the LAMP stack. For more information, see [Tutorial: Installing a LAMP Web Server on Amazon Linux](#).

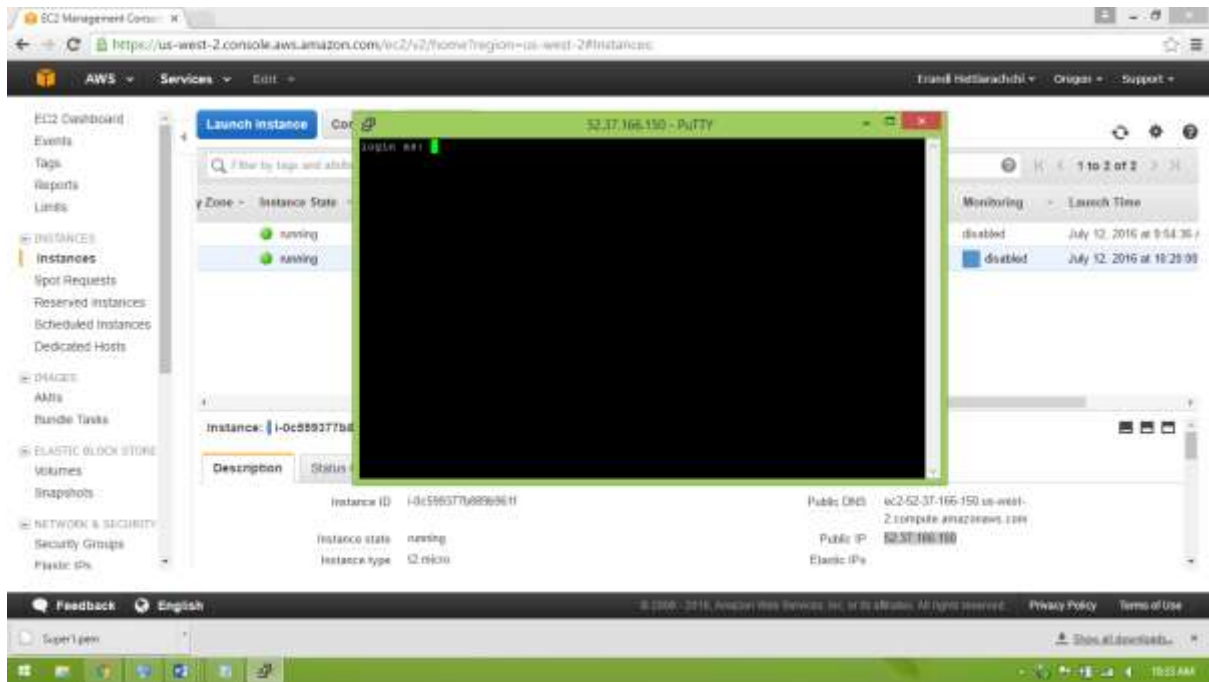


Figure 35

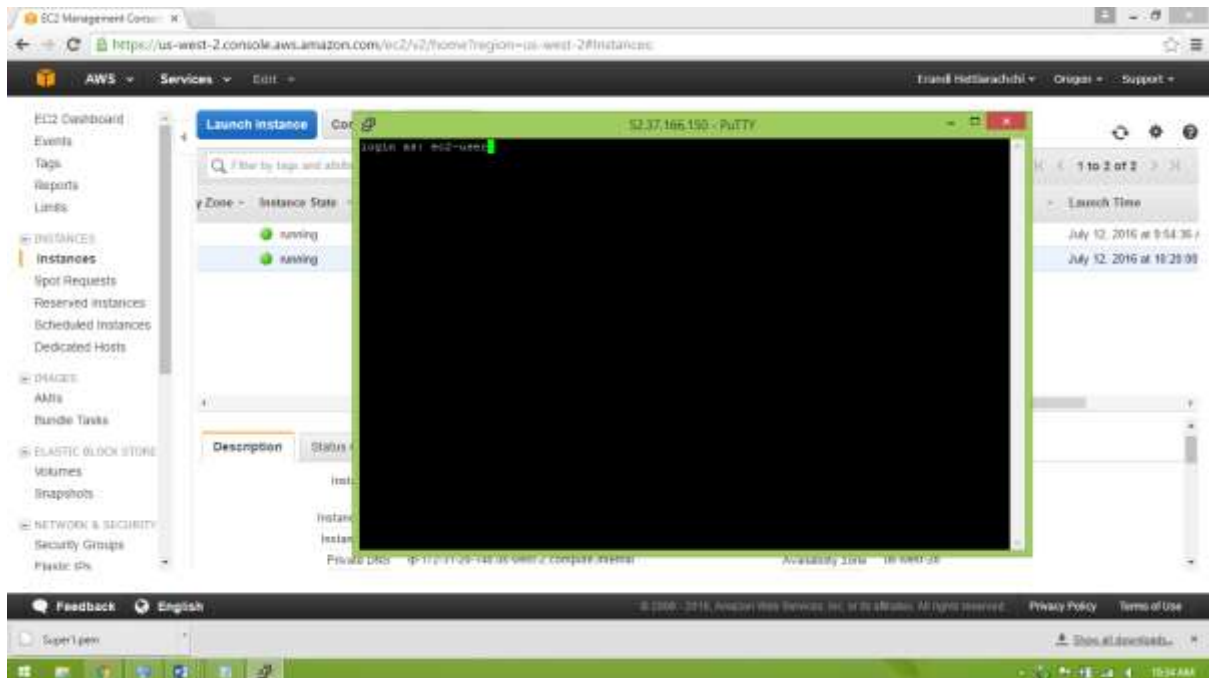


Figure 36

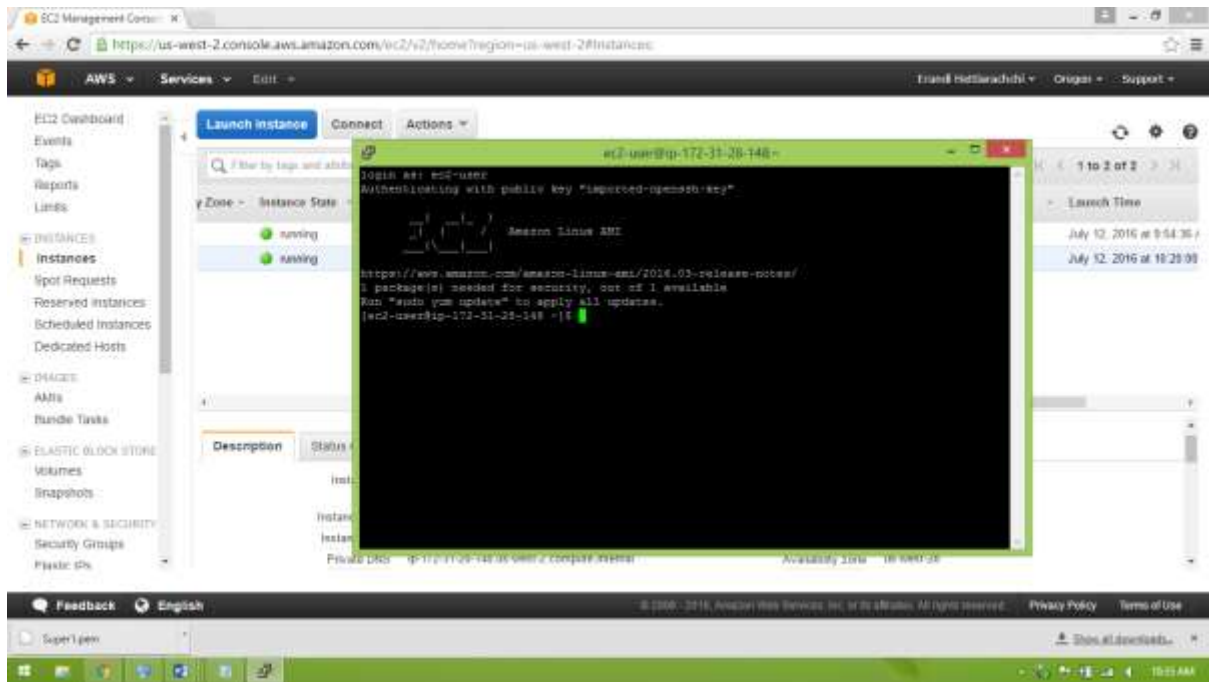


Figure 37

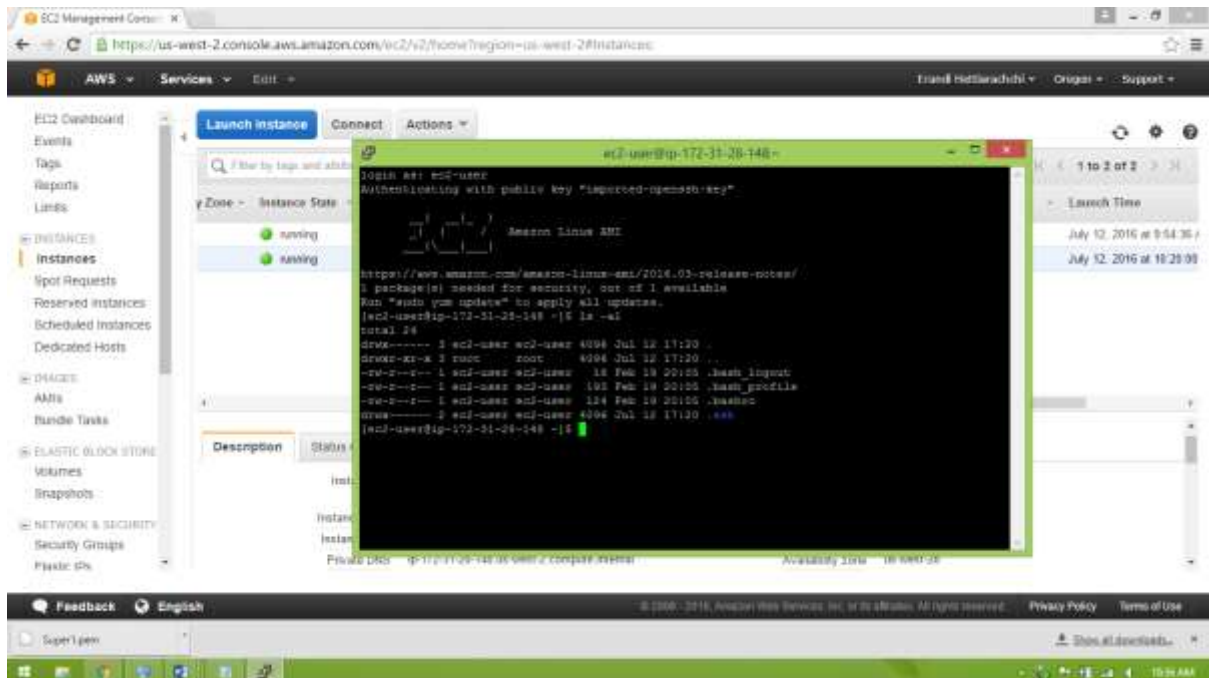


Figure 38

```
ec2-user@ip-172-31-28-148:~$ login as: ec2-user
Authenticating with public key "imported-openssh-key"

      _   _
     | | | |
    | |_| |
    |  __/
    | |  | |
    |_| |_|
    |_|_|_|

Amazon Linux AMI

https://aws.amazon.com/amazon-linux-ami/2016.03-release-notes/
1 package(s) needed for security, out of 1 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-172-31-28-148 ~]$ ls -al
total 36
drwxr-xr-x 2 ec2-user ec2-user 4096 Jul 13 17:20 .
drwxr-xr-x 2 root root 4096 Jul 13 17:20 ..
-rw-r--r-- 1 ec2-user ec2-user 18 Feb 18 20:05 .bash_logout
-rw-r--r-- 1 ec2-user ec2-user 140 Feb 18 20:05 .bash_profile
-rw-r--r-- 1 ec2-user ec2-user 124 Feb 19 20:05 .bashrc
-rw-r--r-- 2 ec2-user ec2-user 4096 Jul 12 17:20 .ssh
[ec2-user@ip-172-31-28-148 ~]$
```

Figure 39

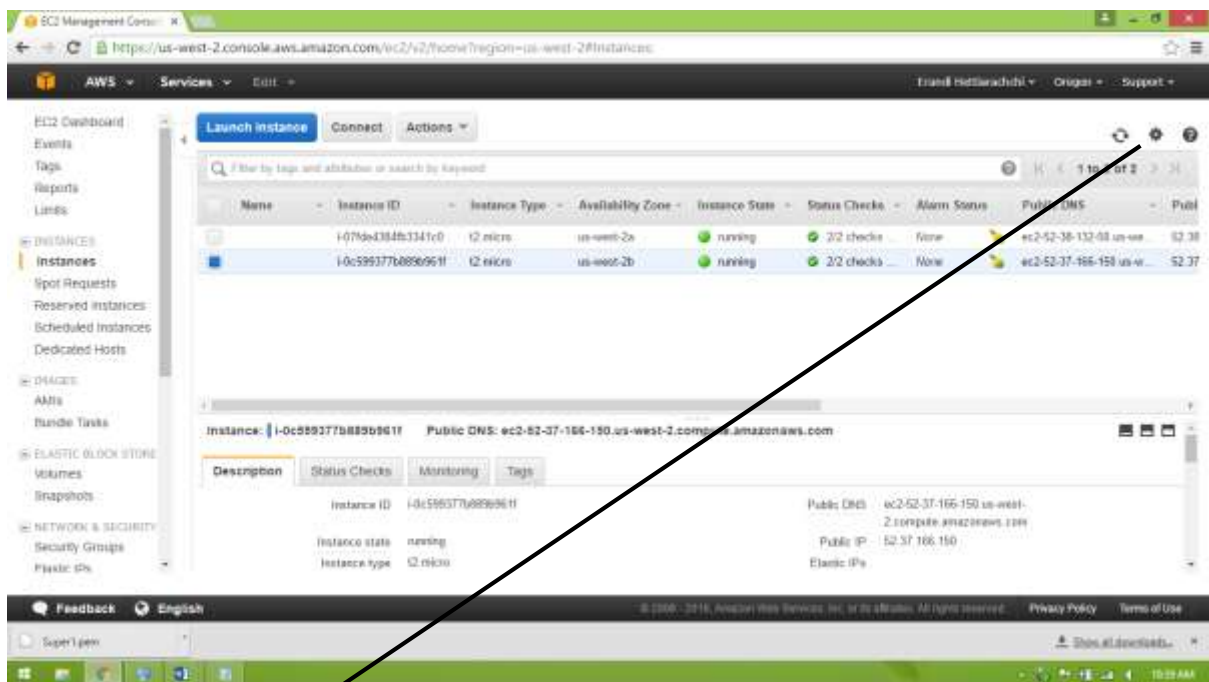


Figure 40

Sign out



Figure 41

Creating a MySQL DB Instance and Connecting to a Database on a MySQL DB Instance

The easiest way to create a DB instance is to use the AWS Management Console. Once you have created the DB instance, you can use standard MySQL utilities such as MySQL Workbench to connect to a database on the DB instance.

Important

You must complete the tasks in the Setting Up for Amazon RDS section before you can create or connect to a DB instance.

Tasks

- Creating a MySQL DB Instance
- Connecting to a Database on a DB Instance Running the MySQL Database Engine
- Deleting a DB Instance

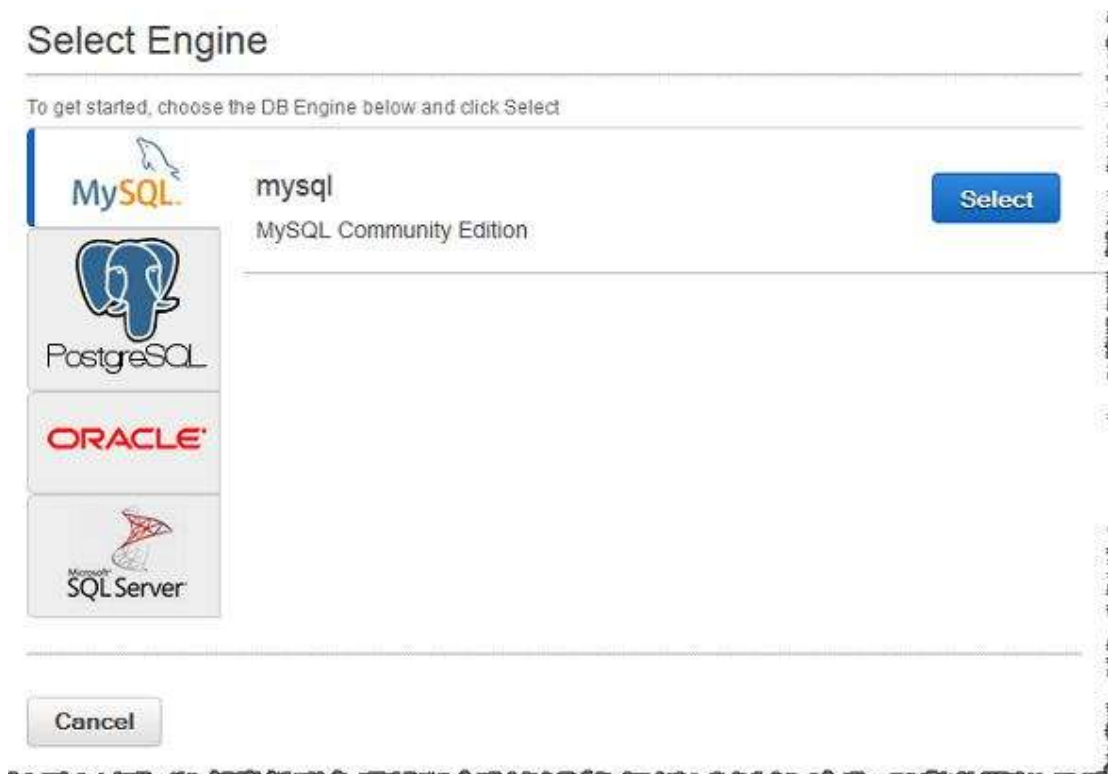
Creating a MySQL DB Instance

The basic building block of Amazon RDS is the DB instance. This is the environment in which you will run your MySQL databases.

In this example, you create a DB instance running the MySQL database engine called west2-mysql-instance1, with a db.m1.small DB instance class, 5 GB of storage, and automated backups enabled with a retention period of one day.

To create a MySQL DB instance

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the top right corner of the Amazon RDS console, choose the region in which you want to create the DB instance.
3. In the navigation pane, choose Instances.
4. Choose Launch DB Instance. The Launch DB Instance Wizard opens on the Select Engine page.



5. On the Select Engine page, choose the MySQL icon and then choose Select for the MySQL DB engine.
6. On the Specify DB Details page, specify your DB instance information. The following table shows settings for an example DB instance. When the settings are as you want them, choose Next.

For This Parameter	Do This
License Model	Choose the default, general-public-license, to use the general license agreement for MySQL. MySQL has only one license model.
DB Engine Version	Choose the default version of MySQL. Note that Amazon RDS supports multiple versions of MySQL in some regions.
DB Instance Class	Choose db.m1.small for a configuration that equates to 1.7 GB memory, 1 ECU (1 virtual core with 1 ECU), 64-bit platform, and moderate I/O capacity.

For This Parameter	Do This
Multi-AZ Deployment	<p>Choose Yes to have a standby replica of your DB instance created in another Availability Zone for failover support. We recommend Multi-AZ for production workloads to maintain high availability. For development and testing, you can choose No.</p> <p>For more information, see High Availability (Multi-AZ).</p>
Allocated Storage	<p>Type 5 to allocate 5 GB of storage for your database. In some cases, allocating a higher amount of storage for your DB instance than the size of your database can improve I/O performance. For more information about storage allocation, see Amazon Relational Database Service Features.</p>
Storage Type	<p>Choose the storage type Magnetic. For more information about storage, see Storage for Amazon RDS.</p>
DB Instance Identifier	<p>Type a name for the DB instance that is unique for your account in the region you chose. You can add some intelligence to the name, such as including the region and DB engine you chose, for example west2-mysql-instance1.</p>
Master Username	<p>Type a name using alphanumeric characters that you will use as the master user name to log on to your DB instance. This will be the user name you use to log on to your database on the DB instance for the first time.</p>
Master Password and Confirm Password	<p>Type a password that contains from 8 to 41 printable ASCII characters (excluding /, ", and @) for your master user password. This will be the password you will use when you use the user name to log on to your database. Then type the password again in the Confirm Password box.</p>


Specify DB Details

Instance Specifications

DB Engine

License Model

DB Engine Version


 Review the [Known Issues/Limitations](#) to learn about potential compatibility issues with specific database versions.

DB Instance Class

Multi-AZ Deployment

Storage Type

Allocated Storage* GB

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

Settings

DB Instance Identifier*

Master Username*

Master Password*

Confirm Password*

* Required

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

- 7.
8. On the Configure Advanced Settings page, provide additional information that RDS needs to launch the MySQL DB instance. The table shows settings for an example DB instance. Specify your DB instance information, then choose Launch DB Instance.

For Parameter	This Do This
VPC	Choose the name of the Virtual Private Cloud (VPC) that will host your MySQL DB instance. If your DB instance will not be hosted

For This Parameter	Do This
	in a VPC, choose Not in VPC. For more information about VPC, see Amazon RDS and Amazon Virtual Private Cloud (VPC) .
Availability Zone	Determine if you want to specify a particular Availability Zone. If you chose Yes for the Multi-AZ Deployment parameter on the previous page, you will not have any options here. For more information about Availability Zones, see Regions and Availability Zones .
DB Security Groups	Choose the security group you want to use with this DB instance. For more information about security groups, see Working with DB Security Groups .
Database Name	Type a database name that is 1 to 64 alpha-numeric characters. If you do not provide a name, Amazon RDS will not automatically create a database on the DB instance you are creating.
Database Port	Leave the default value of 3306 unless you have a specific port you want to access the database through. MySQL installations default to port 3306.
DB Parameter Group	Leave the default value unless you created your own DB parameter group. For more information about parameter groups, see Working with DB Parameter Groups .
Option Group	Choose the default value because this option group is used with the MySQL version you chose on the previous page.
Copy Tags To Snapshots	Choose this option to have any DB instance tags copied to a DB snapshot when you create a snapshot. For more information, see Tagging Amazon RDS Resources .
Enable Encryption	Choose Yes to enable encryption at rest for this DB instance. For more information, see Encrypting Amazon RDS Resources .

For This Parameter	Do This
Backup Retention Period	Set the number of days you want automatic backups of your database to be retained. For testing purposes, you can set this value to 1.
Backup Window	Unless you have a specific time that you want to have your database backup, use the default of No Preference.
Enable Enhanced Monitoring	Unless you want to enable gathering metrics in real time for the operating system that your DB instance runs on, use the default of No.
Auto Minor Version Upgrade	Choose Yes to enable your DB instance to receive minor DB engine version upgrades automatically when they become available.
Maintenance Window	Choose the 30 minute window in which pending modifications to your DB instance are applied. If you the time period doesn't matter, choose No Preference.

Configure Advanced Settings

Network & Security

This instance will be created with the new Certificate Authority rds-ca-2015. If you are using SSL to connect to this instance, you should use the [new certificate bundle](#). Learn more [here](#).

VPC:

Subnet Group:

Publicly Accessible:

Availability Zone:

VPC Security Group(s):

Database Options

Database Name:

Note: If no database name is specified then no initial MySQL database will be created on the DB instance.

Database Port:

DB Parameter Group:

Option Group:

Copy logs to Snapshots: ☐

Enable Encryption:

Backup

Please note that automated backups are currently supported for InnoDB storage engine only. If you are using MyISAM, refer to detail [here](#).

Backup Retention Period: days

Backup Window:

Monitoring

Enable Enhanced Monitoring:

Maintenance

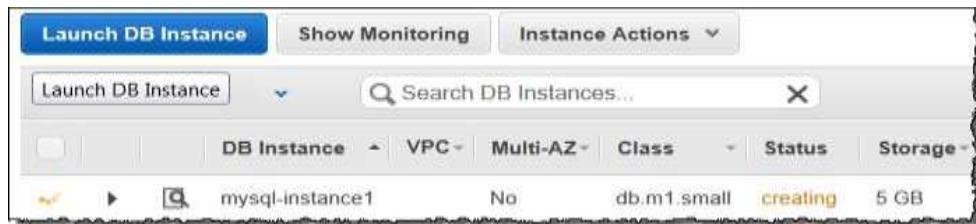
Auto Minor Version Upgrade:

Maintenance Window:

* Required

[Cancel](#) [Previous](#) [Launch DB Instance](#)

- 9.
10. On the RDS console, the new DB instance appears in the list of DB instances. The DB instance will have a status of creating until the DB instance is created and ready for use. When the state changes to available, you can connect to a database on the DB instance. Depending on the DB instance class and store allocated, it could take several minutes for the new DB instance to become available.



Connecting to a Database on a DB Instance Running the MySQL Database Engine

Once Amazon RDS provisions your DB instance, you can use any standard SQL client application to connect to a database on the DB instance. In this example, you connect to a database on a MySQL DB instance using MySQL monitor commands. One GUI-based application you can use to connect is MySQL Workbench; for more information, go to the [Download MySQL Workbench](#) page. For more information on using MySQL, go to the [MySQL documentation](#).

To connect to a database on a DB instance using MySQL monitor

- Type the following command at a command prompt on a client computer to connect to a database on a MySQL DB instance using the MySQL monitor. Substitute the DNS name for your DB instance for <endpoint>, the master user name you used for <mymasteruser>, and the master password you used for <password>.

```
PROMPT> mysql -h <endpoint> -P 3306 -u <mymasteruser> -p
```

You will see output similar to the following.

```
Welcome to the MySQL monitor.  Commands end with ; or \g.
```

```
Your MySQL connection id is 350
```

```
Server version: 5.1.32-log MySQL Community Server (GPL)
```

```
Type 'help;' or '\h' for help. Type '\c' to clear the buffer.
```

```
mysql>
```

Deleting a DB Instance

Once you have connected to the sample DB instance that you created, you should delete the DB instance so you are no longer charged for it.

To delete a DB instance with no final DB snapshot

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the Instances list, choose the DB instance you wish to delete.
3. Choose Instance Actions, and then choose Delete from the dropdown menu.
4. Choose No in the Create Final Snapshot? drop-down list box.
5. Choose Yes, Delete.

Steps

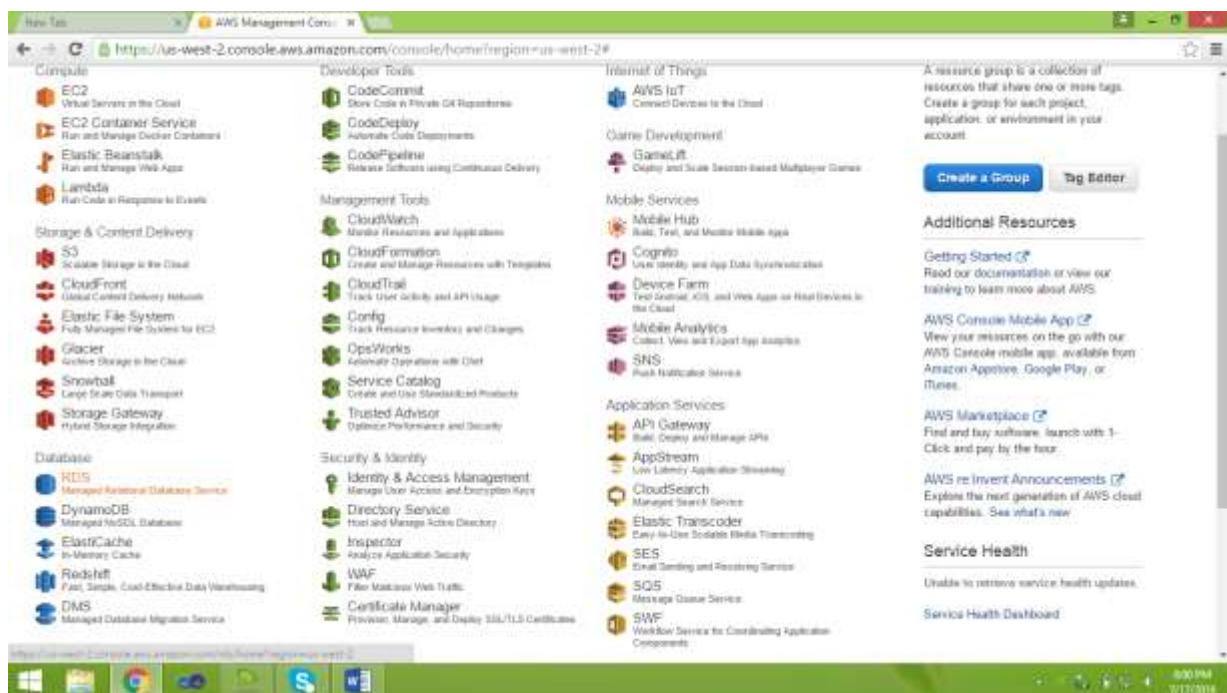


Figure 42

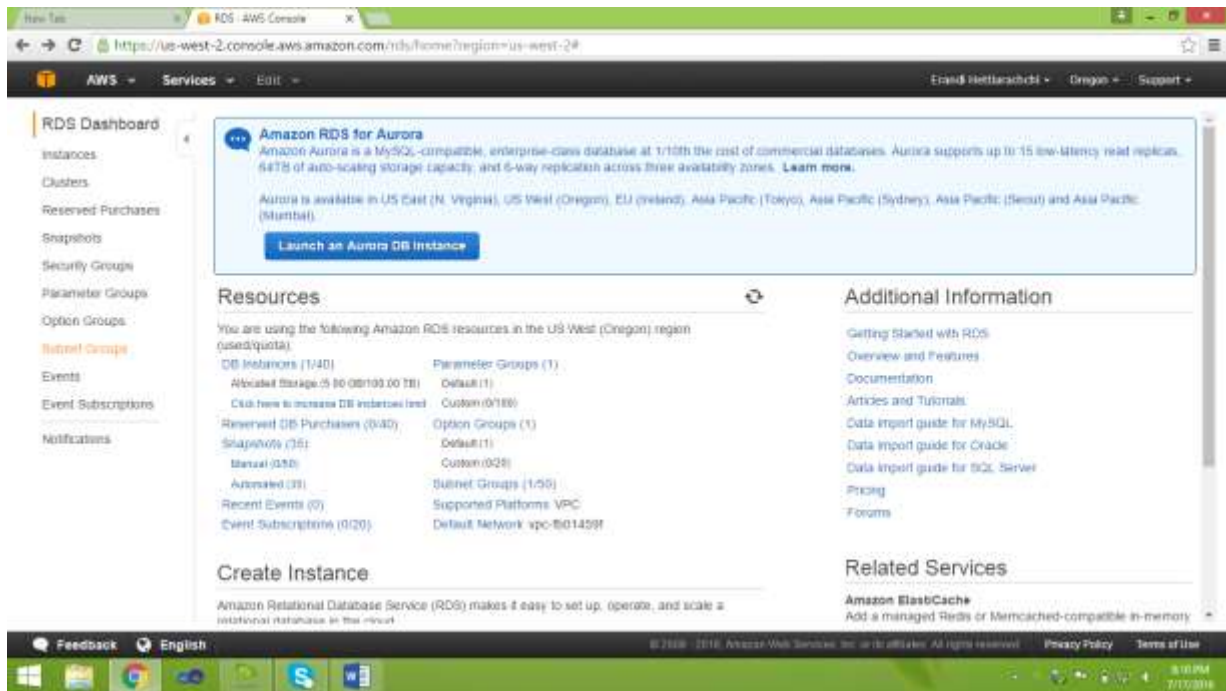


Figure 43

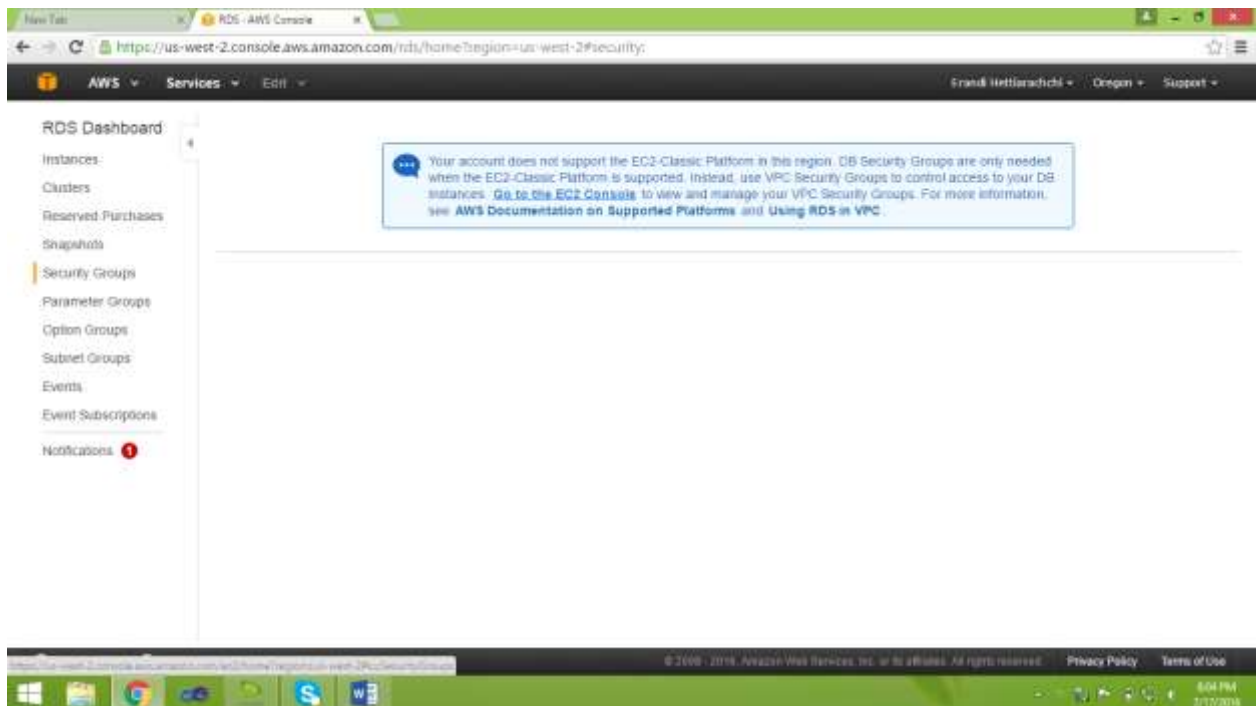


Figure 44

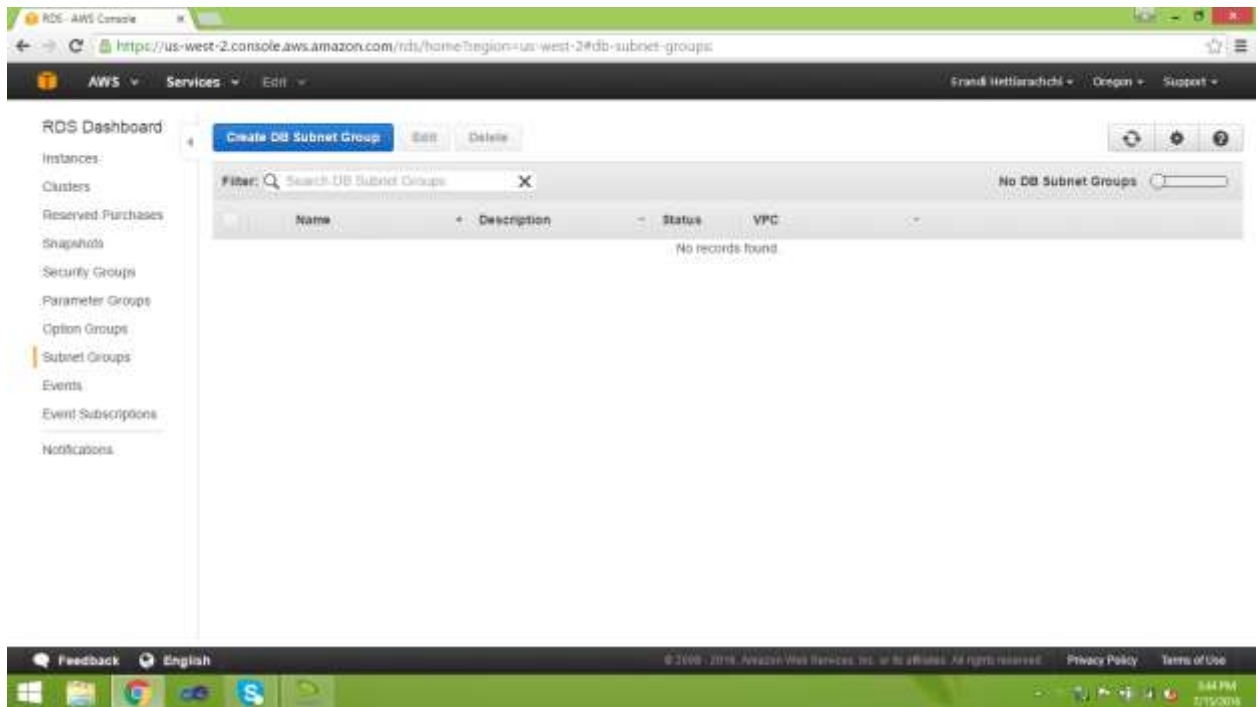


Figure 45

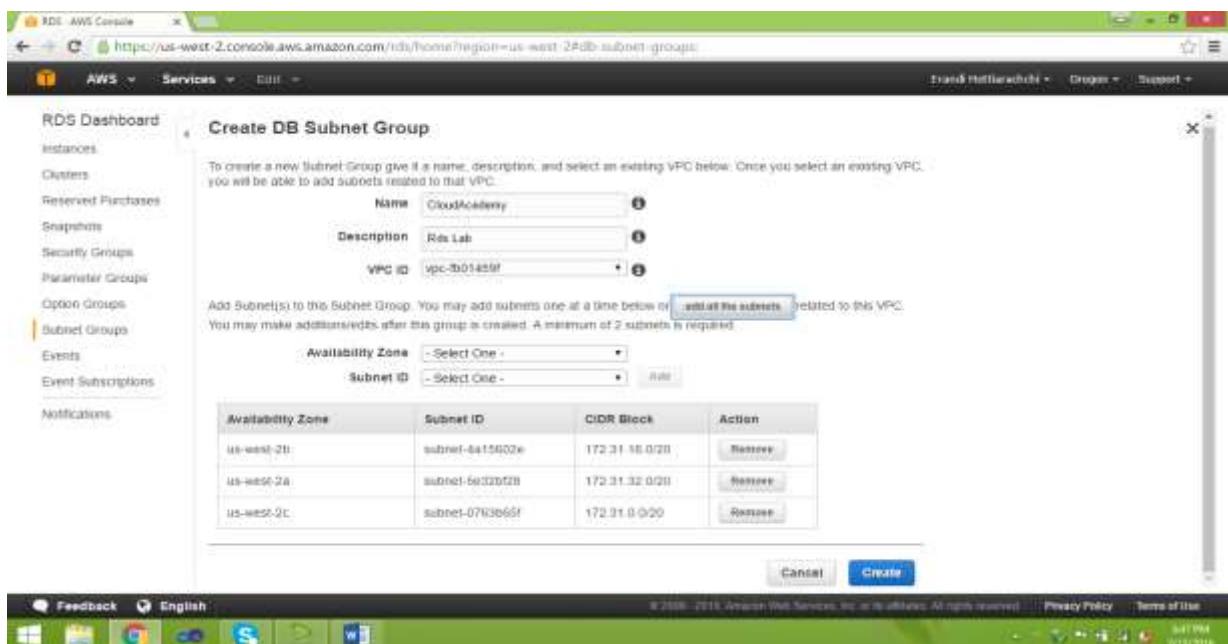


Figure 46

- Remove one Availability Zone. So, it should consist of two Availability Zone.

Finally

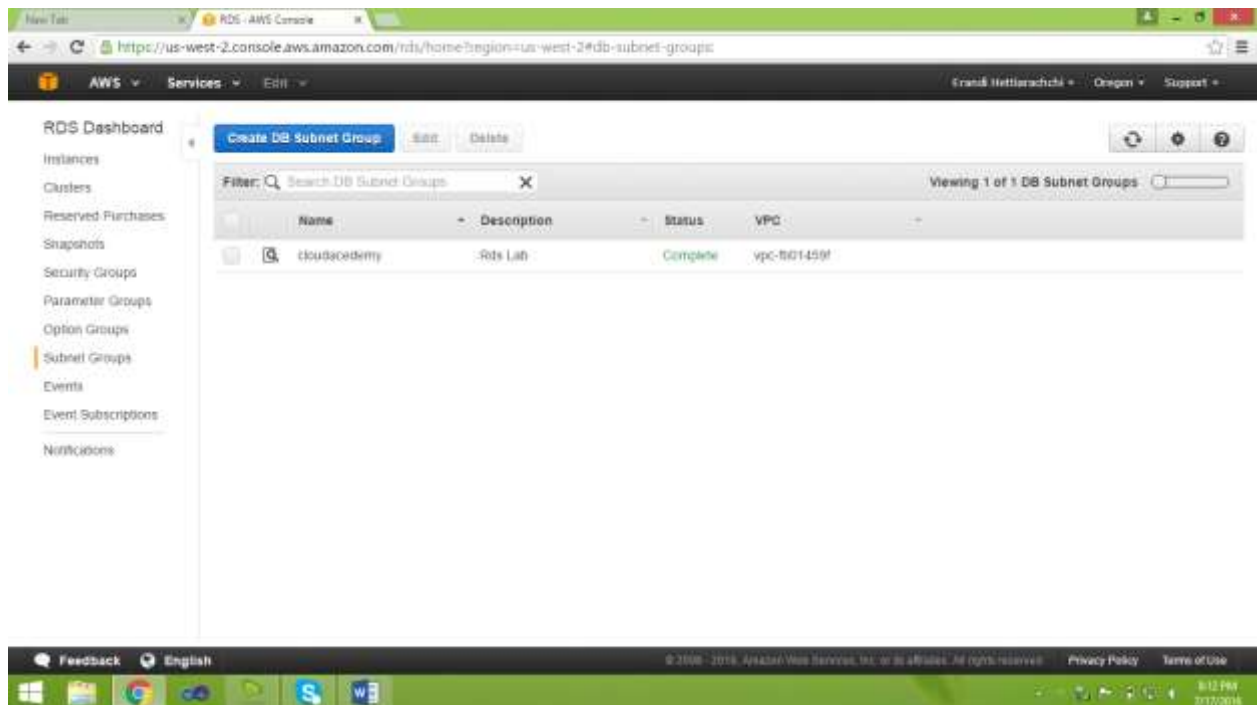


Figure 47

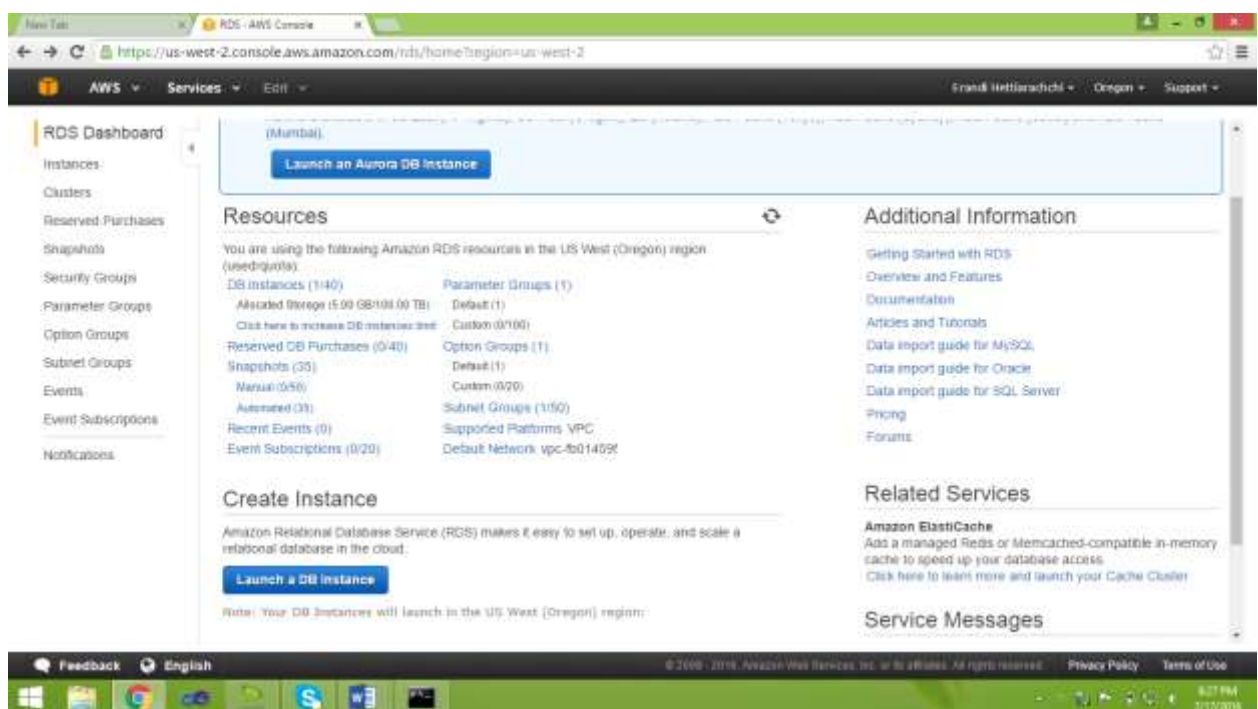


Figure 48

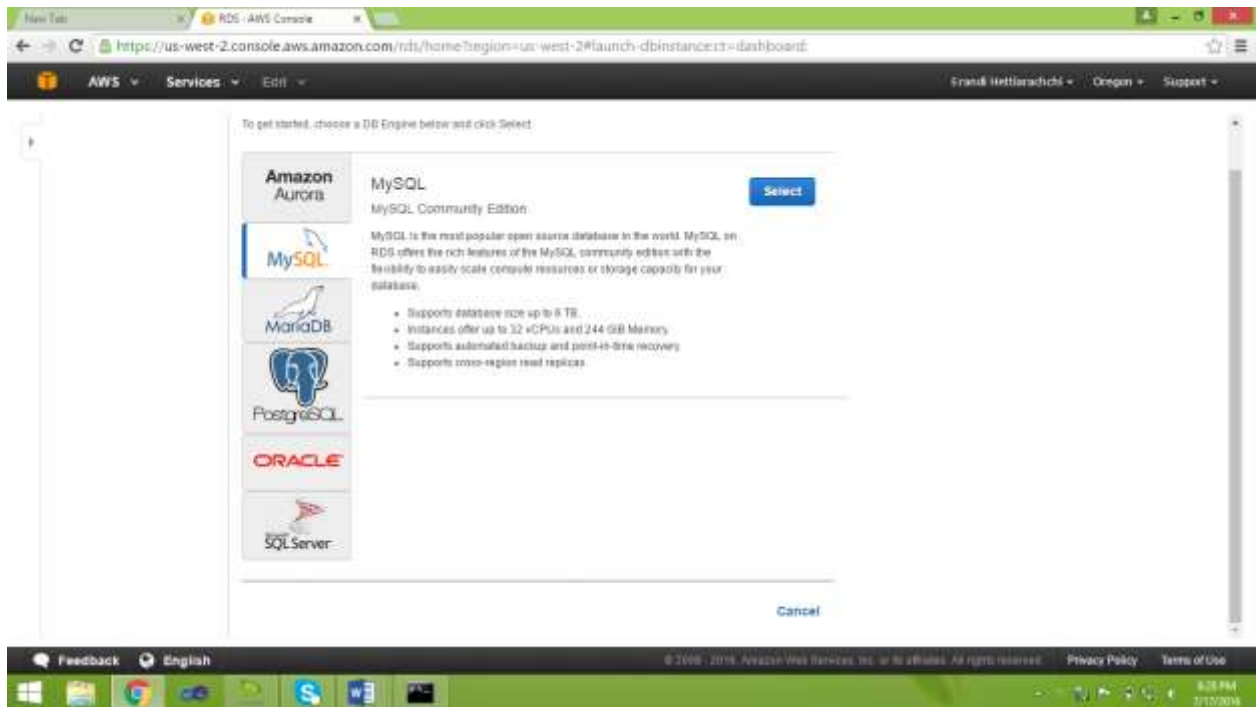


Figure 49

Select the Mysql

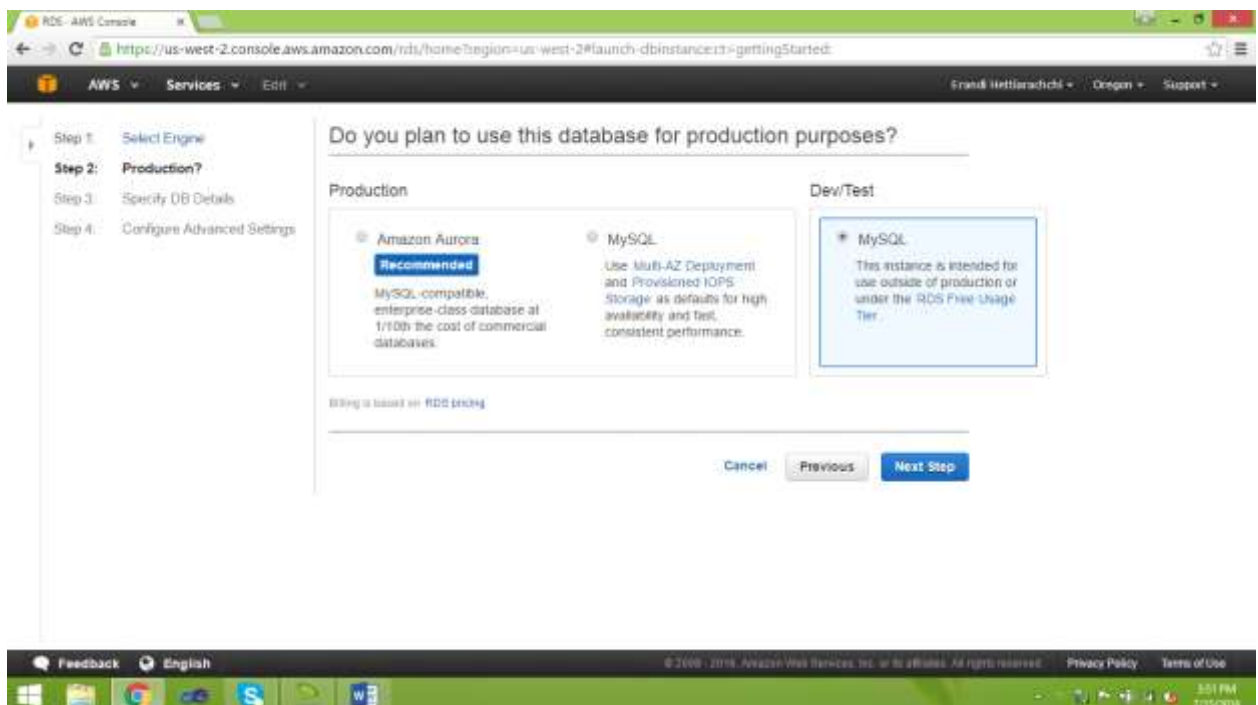


Figure 50

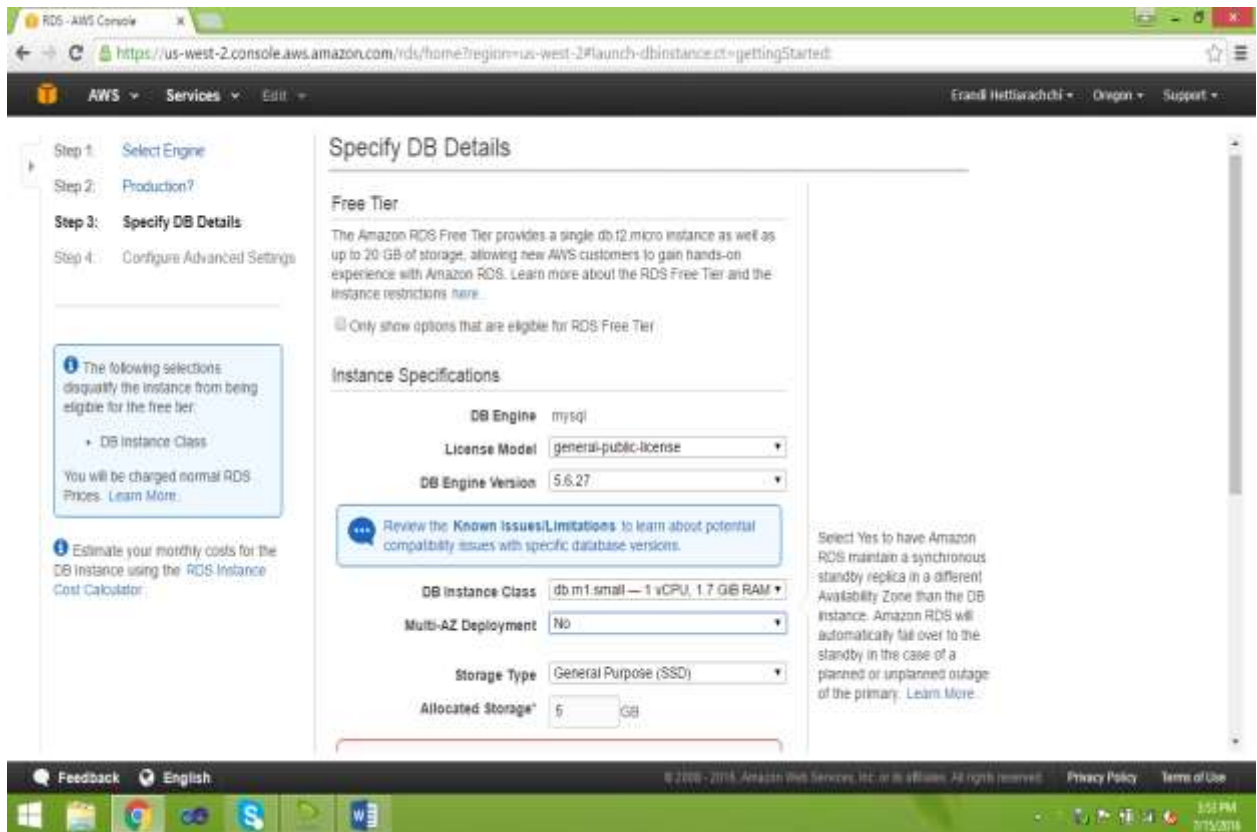


Figure 51

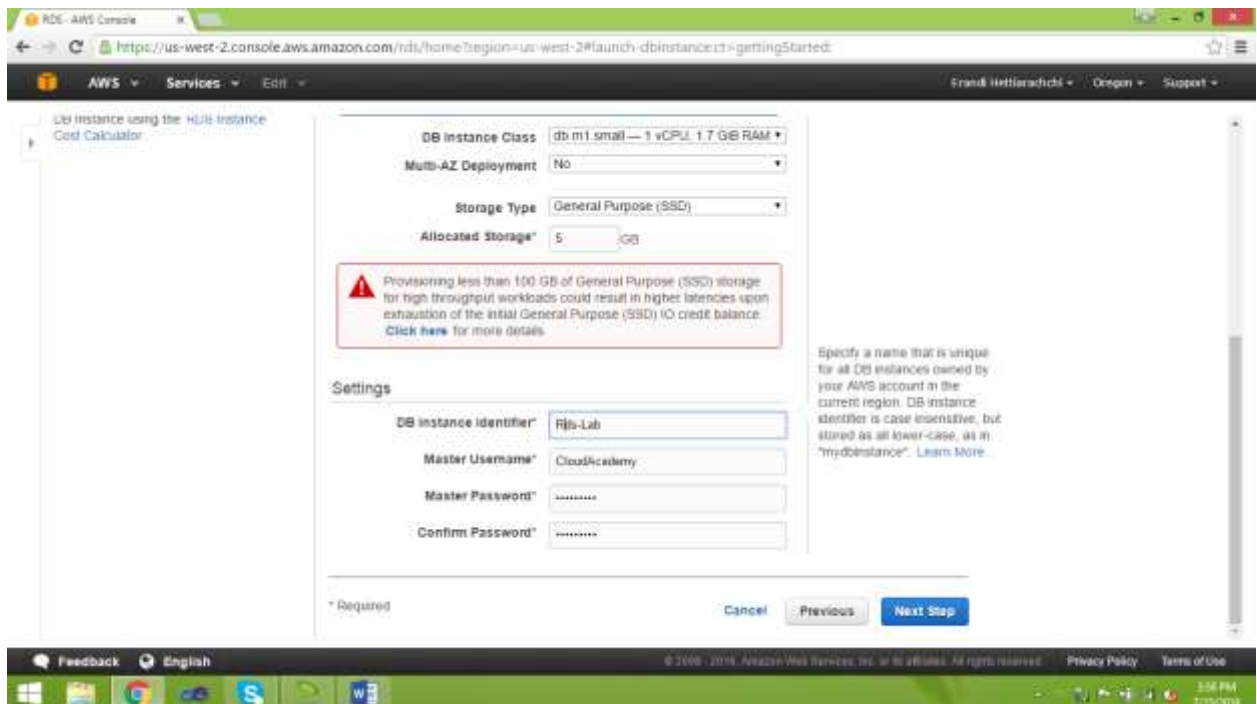


Figure 52

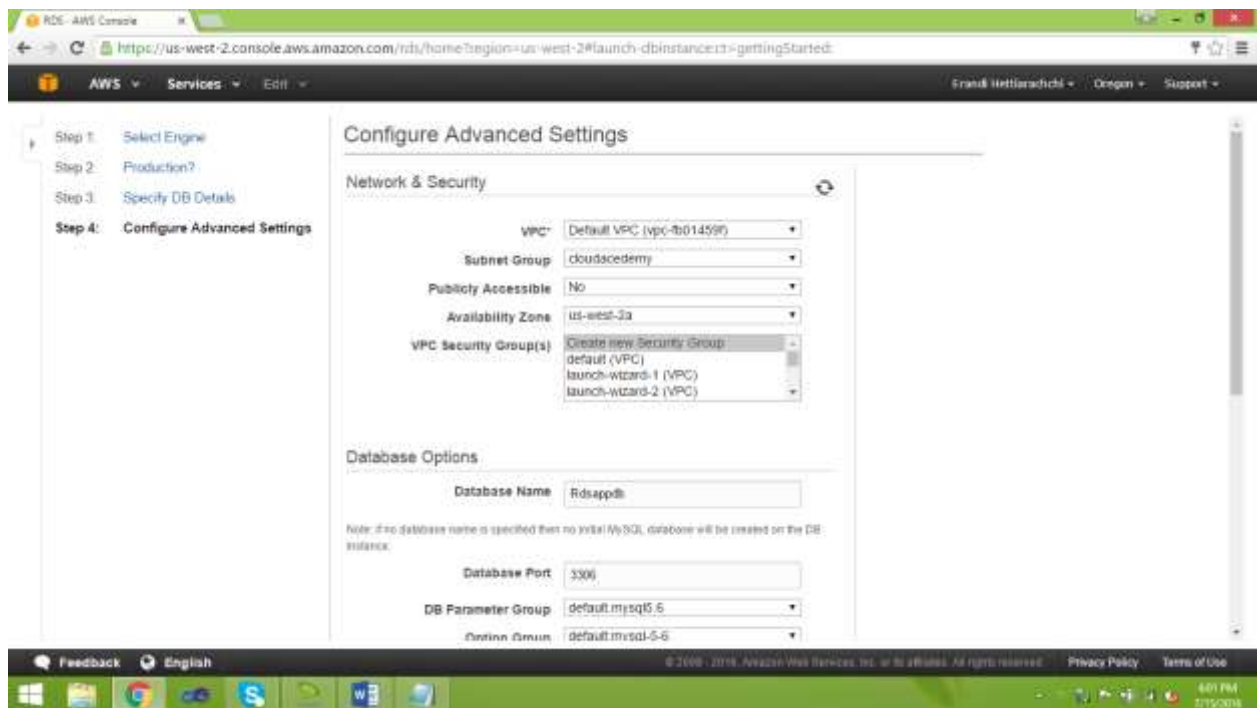


Figure 53

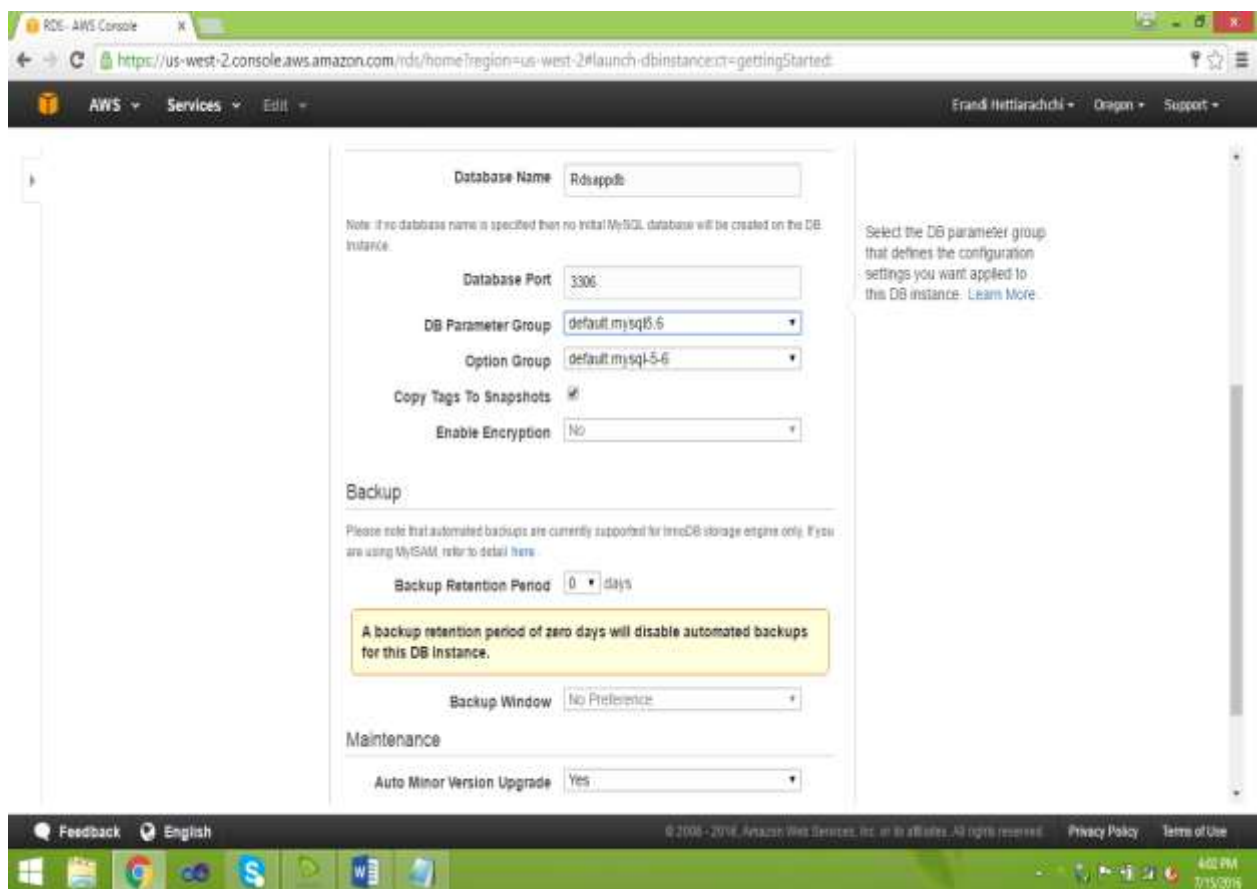


Figure 54

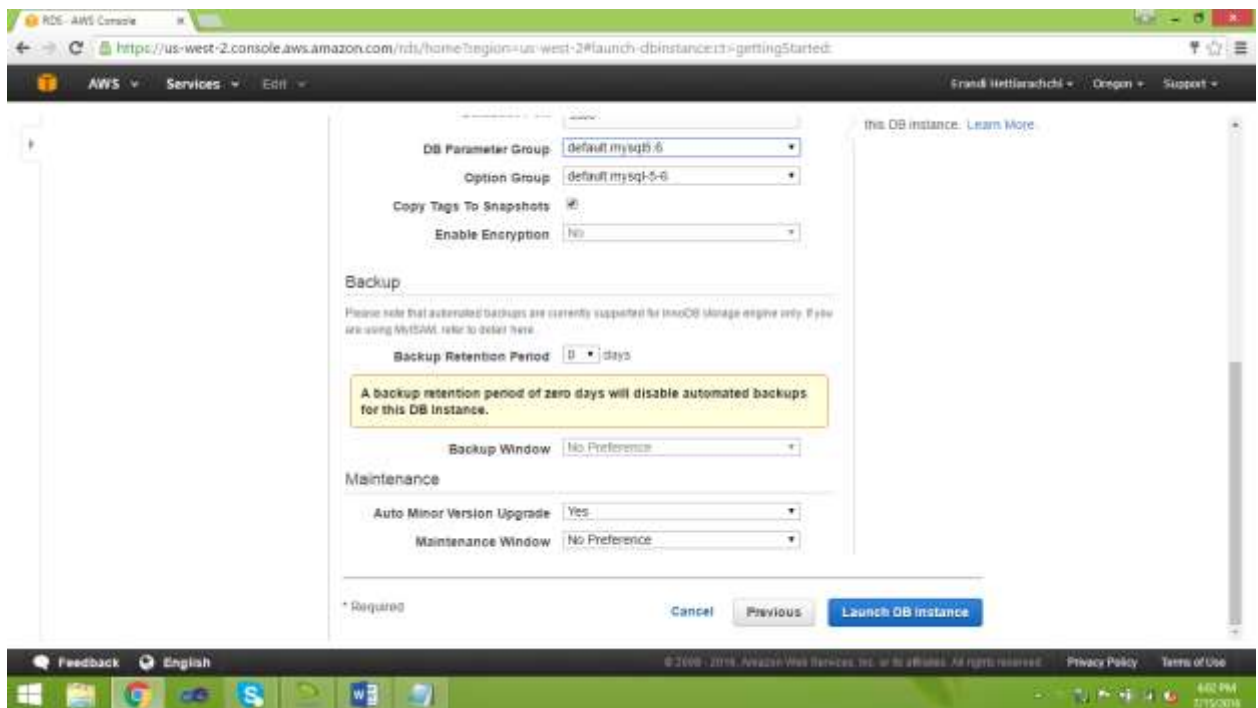


Figure 55

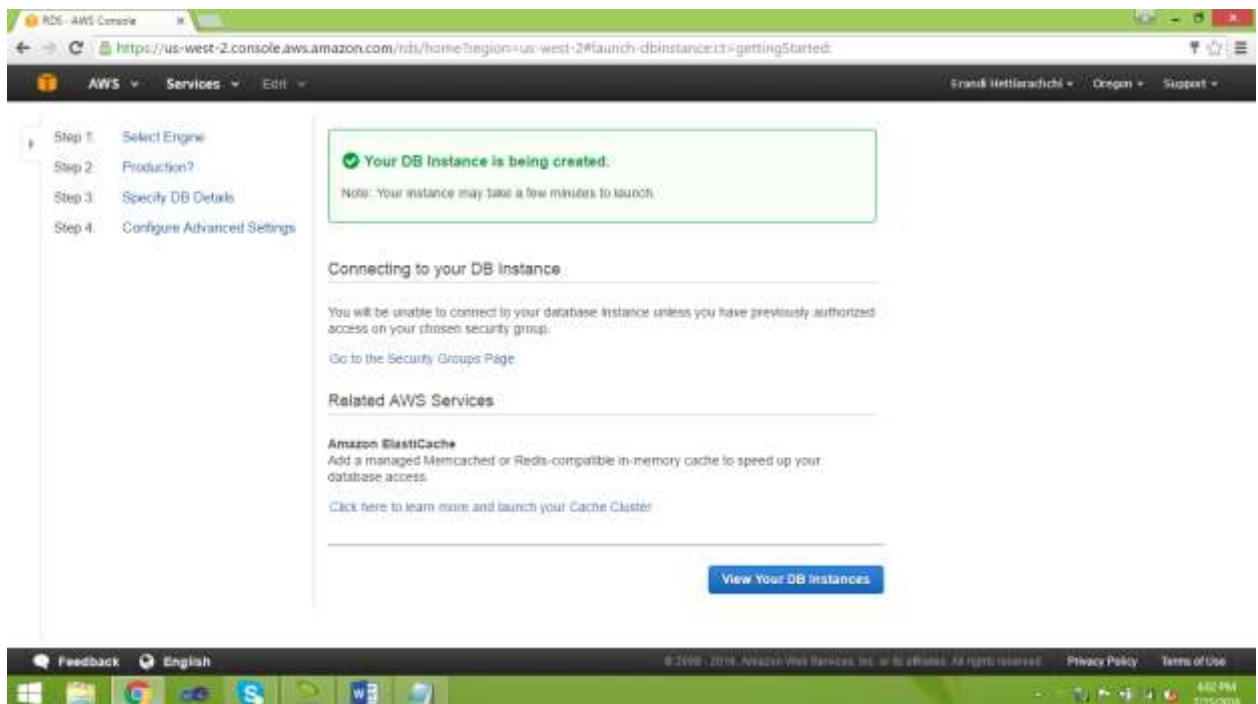


Figure 56

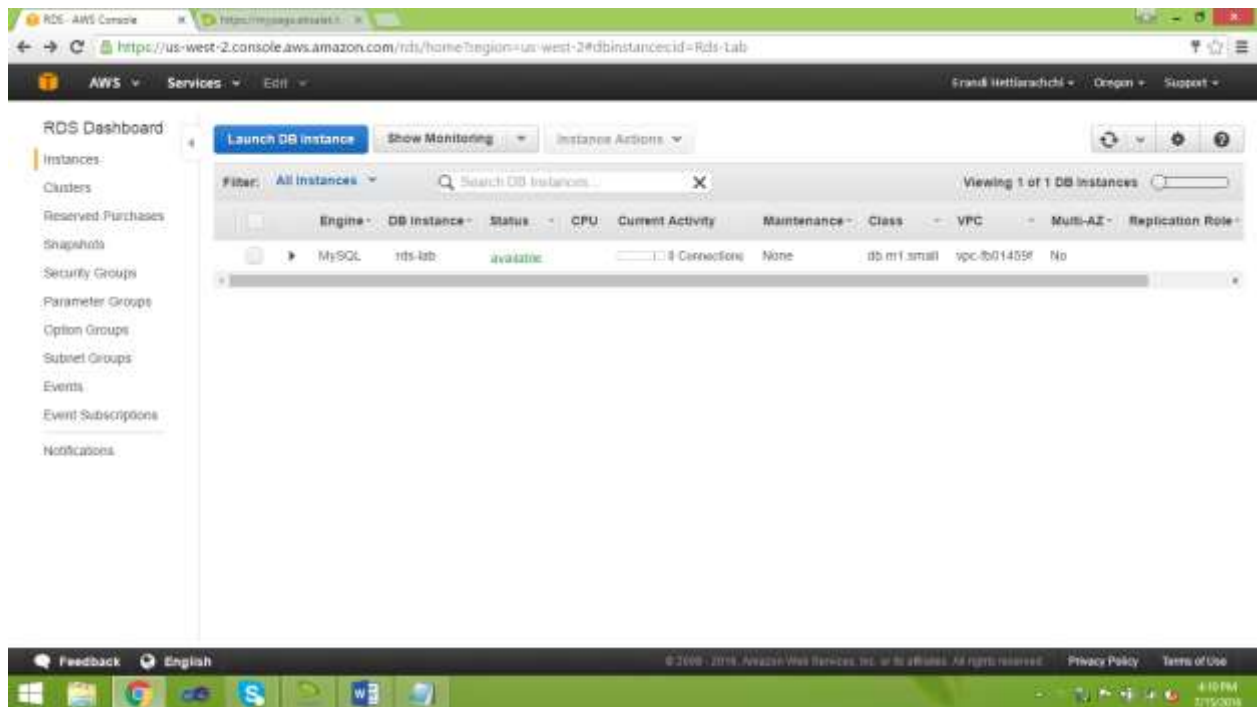


Figure 57

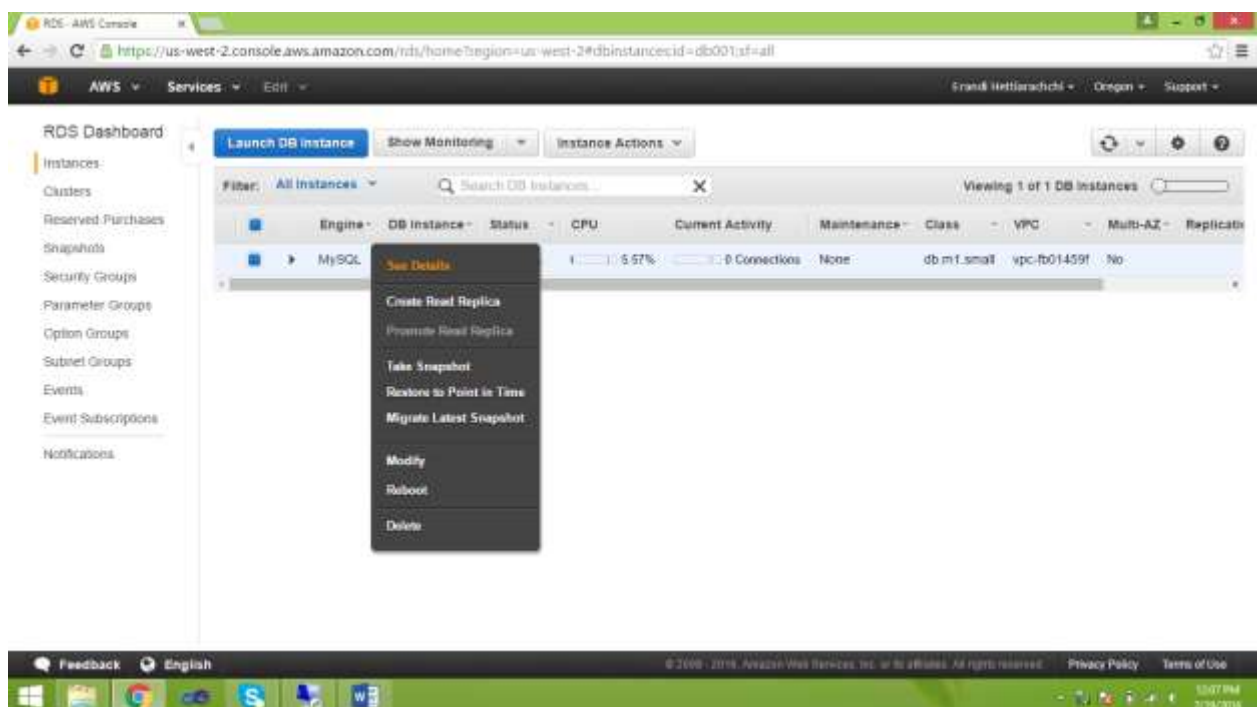


Figure 58

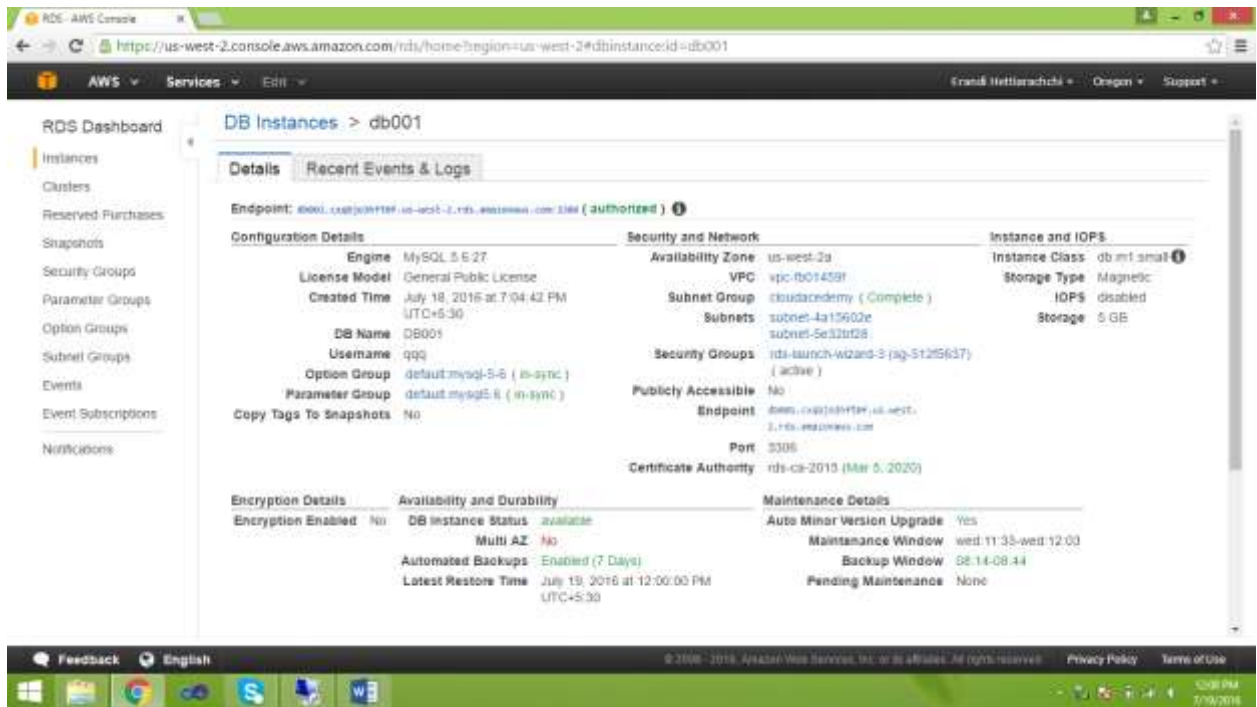


Figure 59

➤ Download MySQL Workbench and Setup the Connection

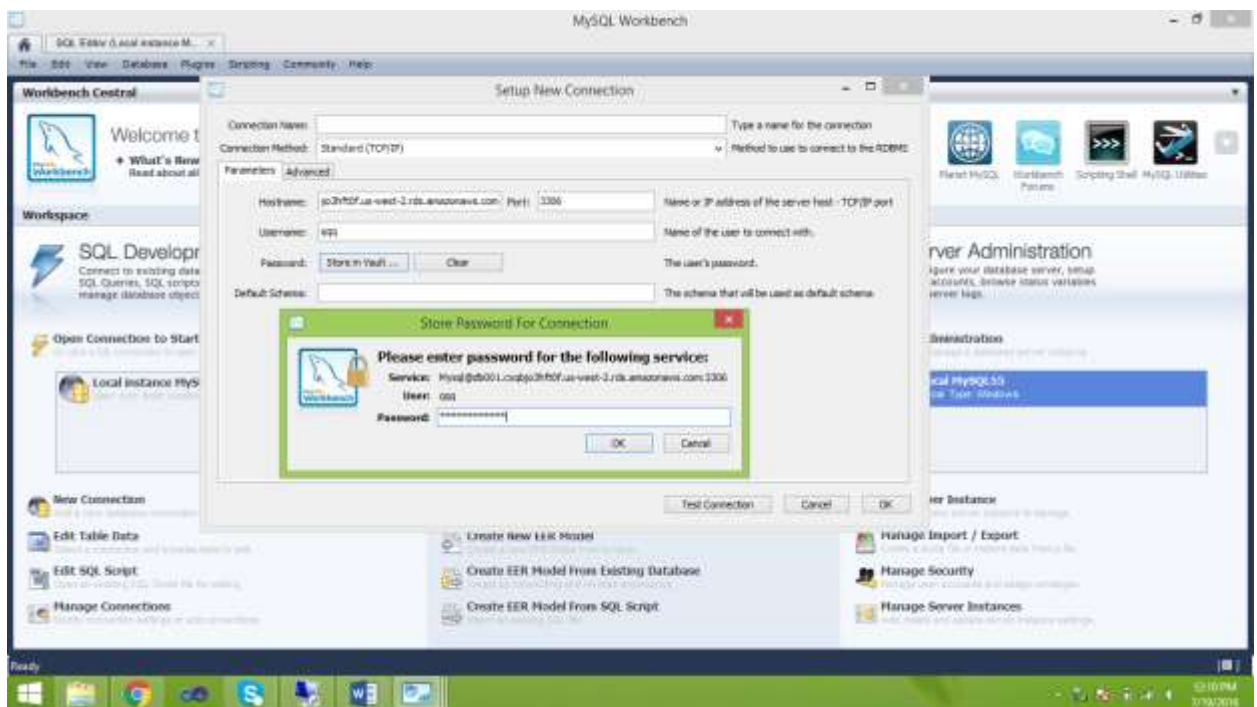


Figure 60

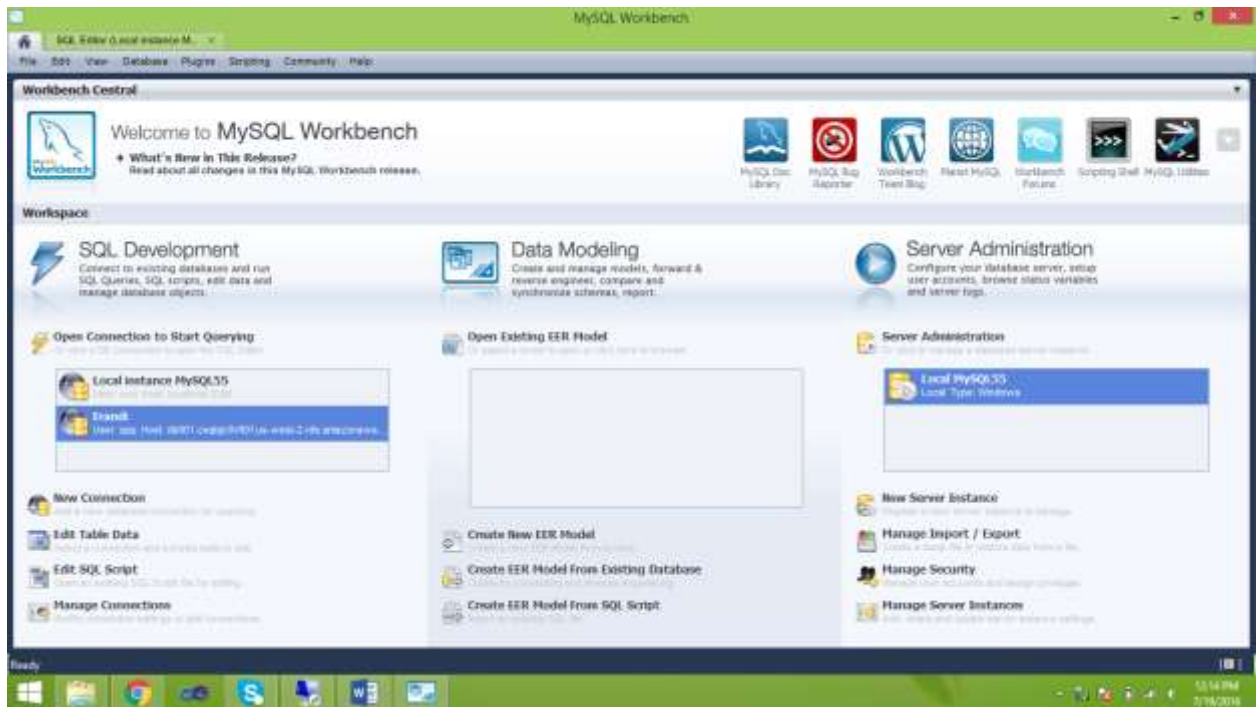


Figure 61

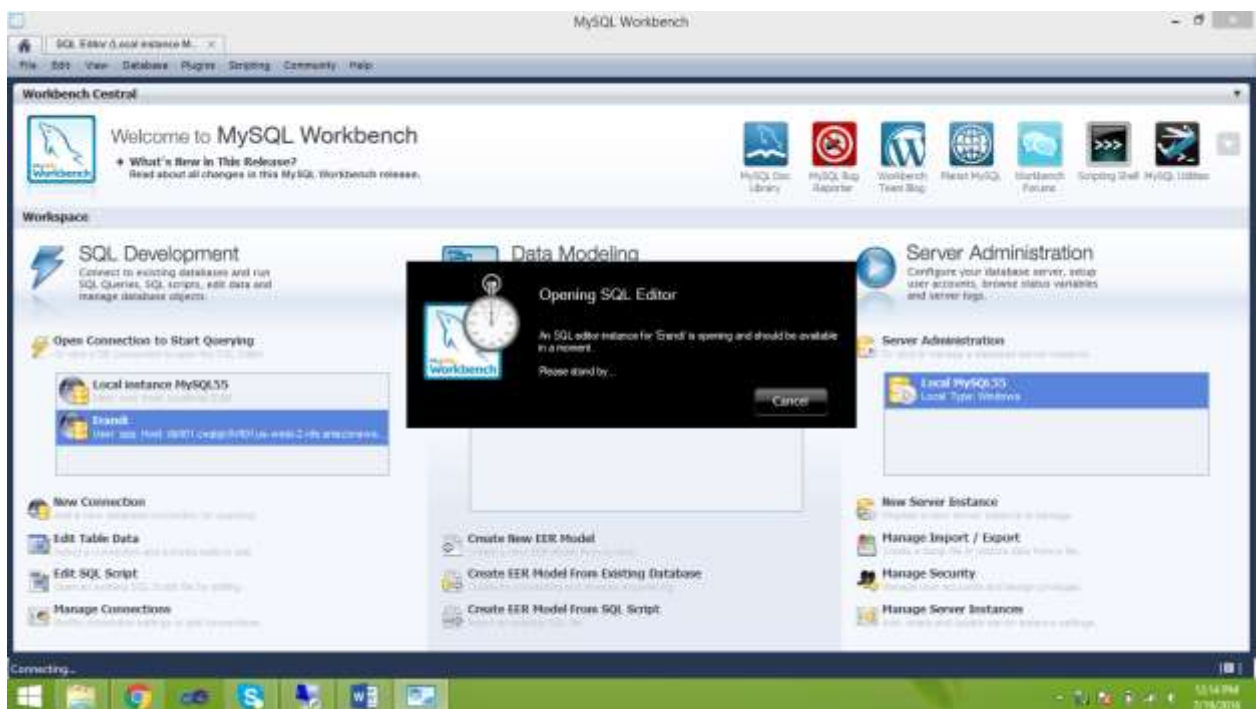


Figure 62

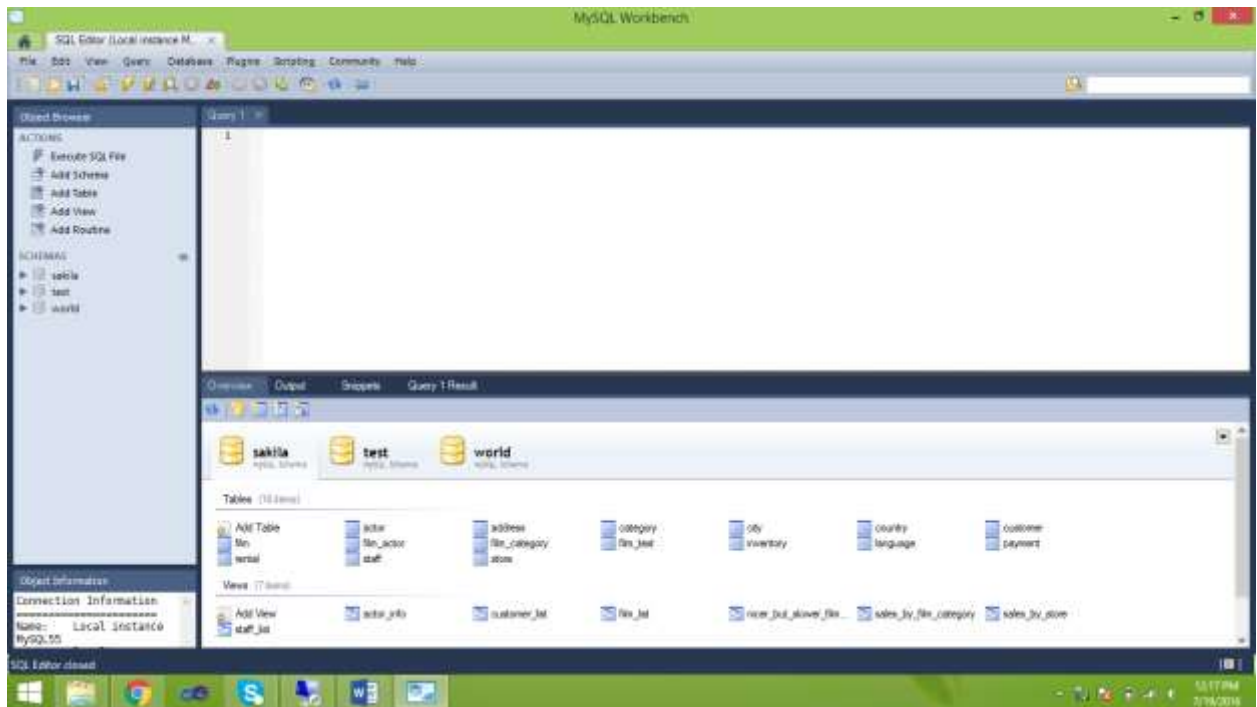


Figure 63

Create A Security Group

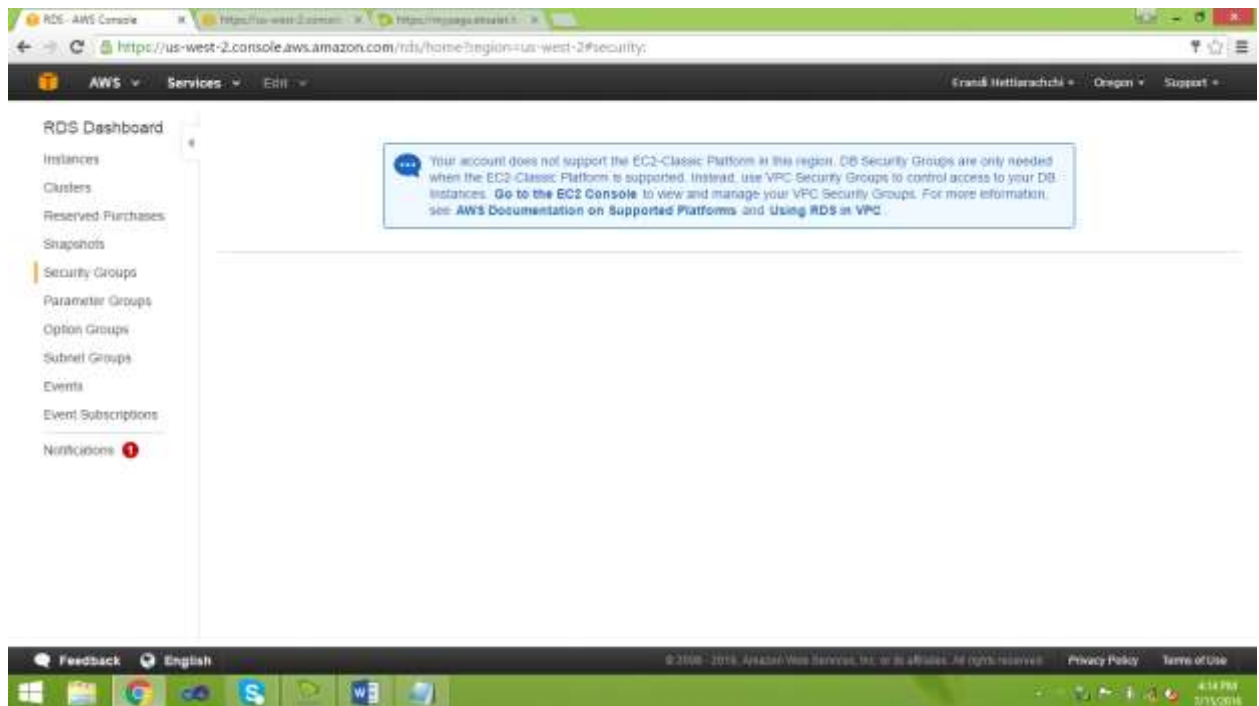


Figure 64

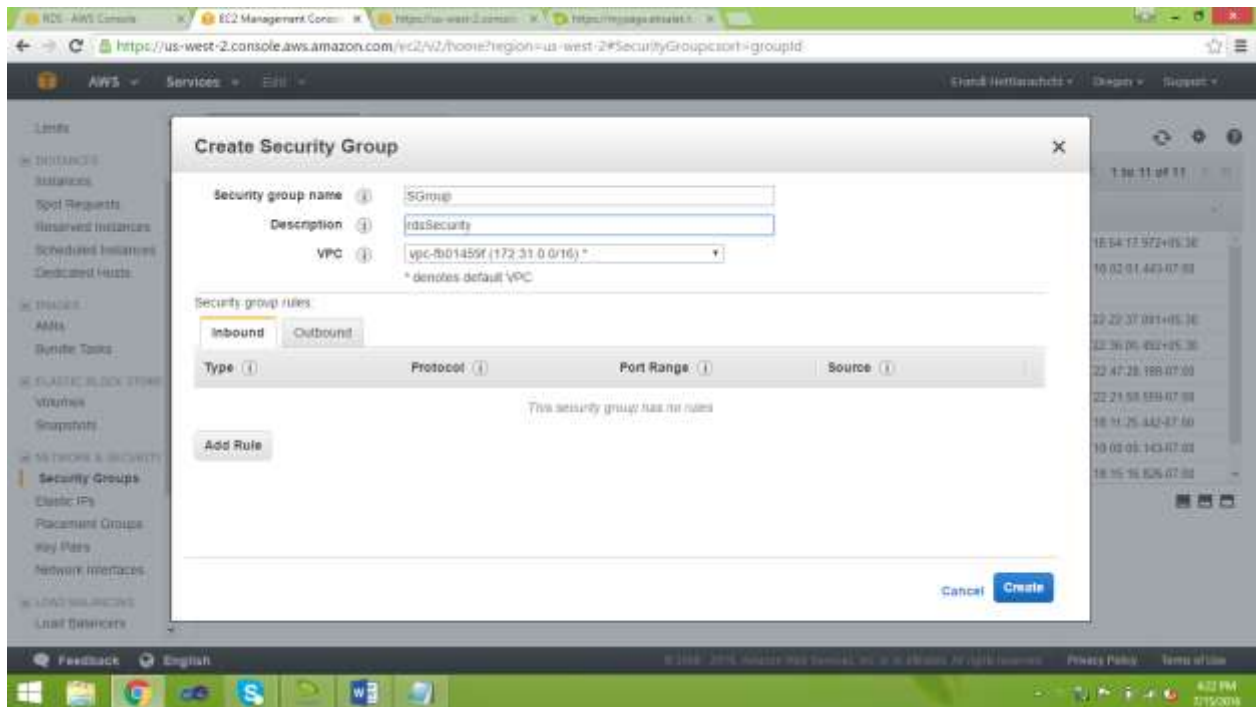


Figure 65

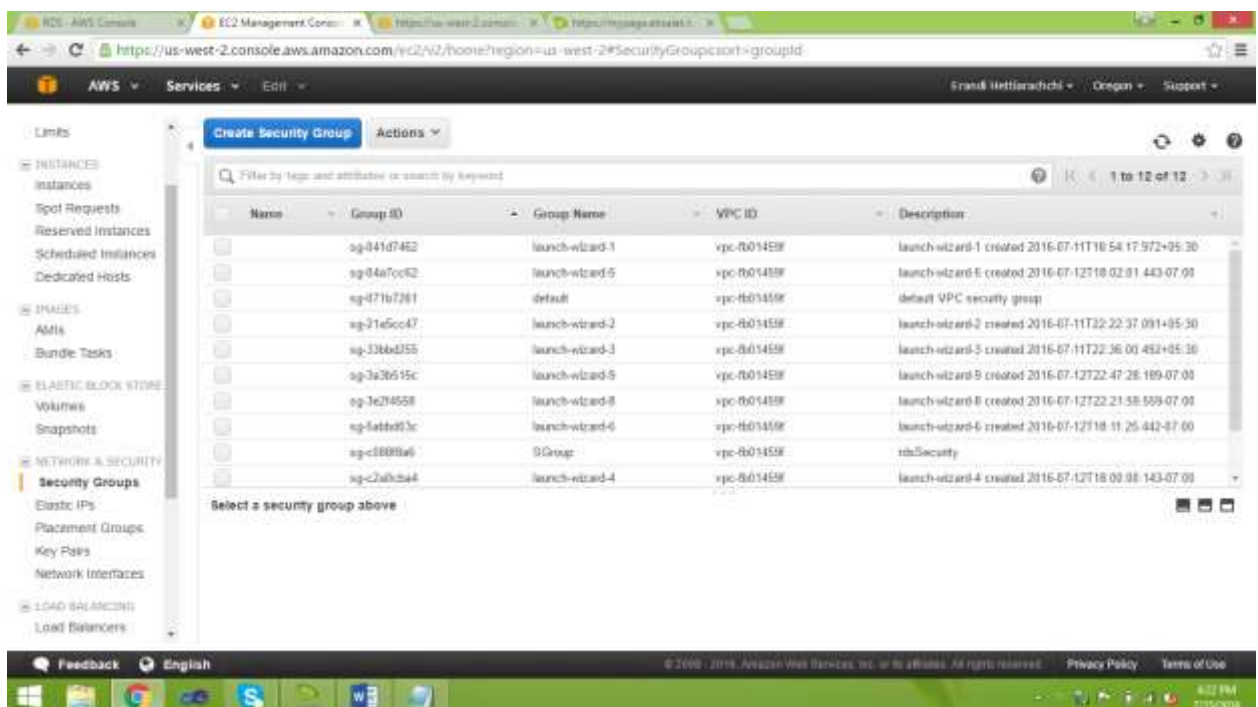


Figure 66

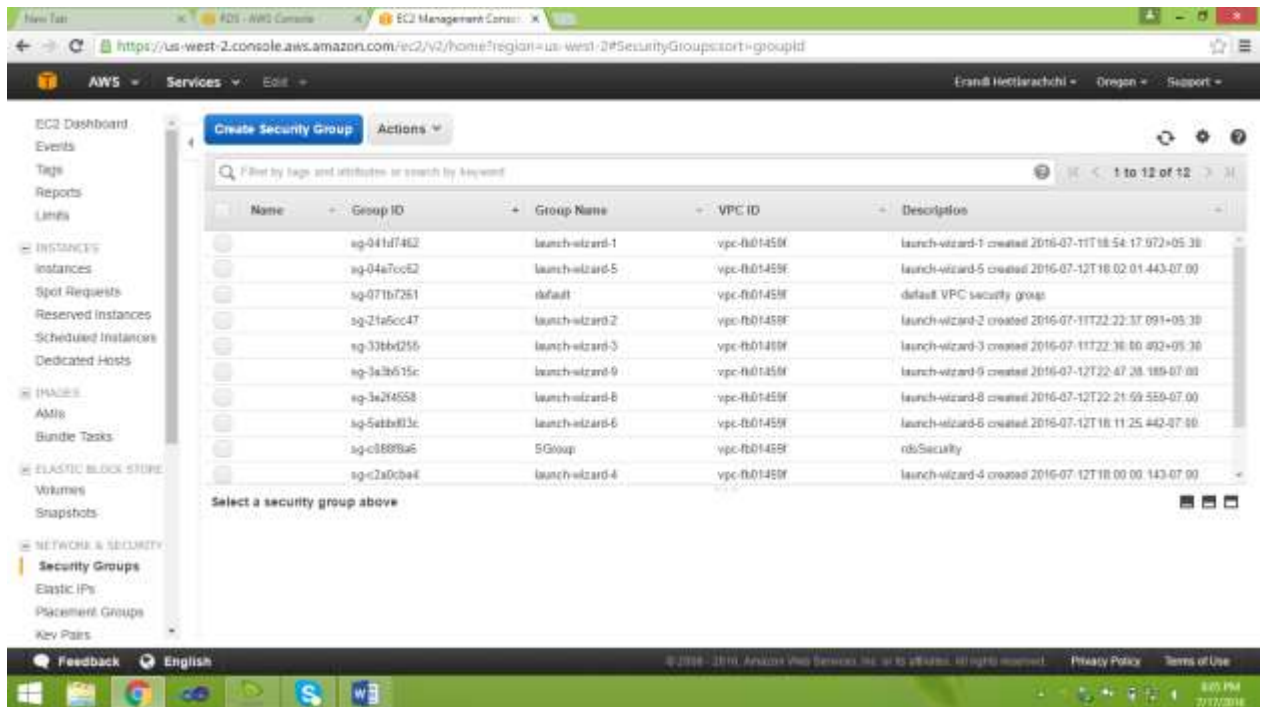


Figure 67

To connect to a database on a DB instance using MySQL monitor

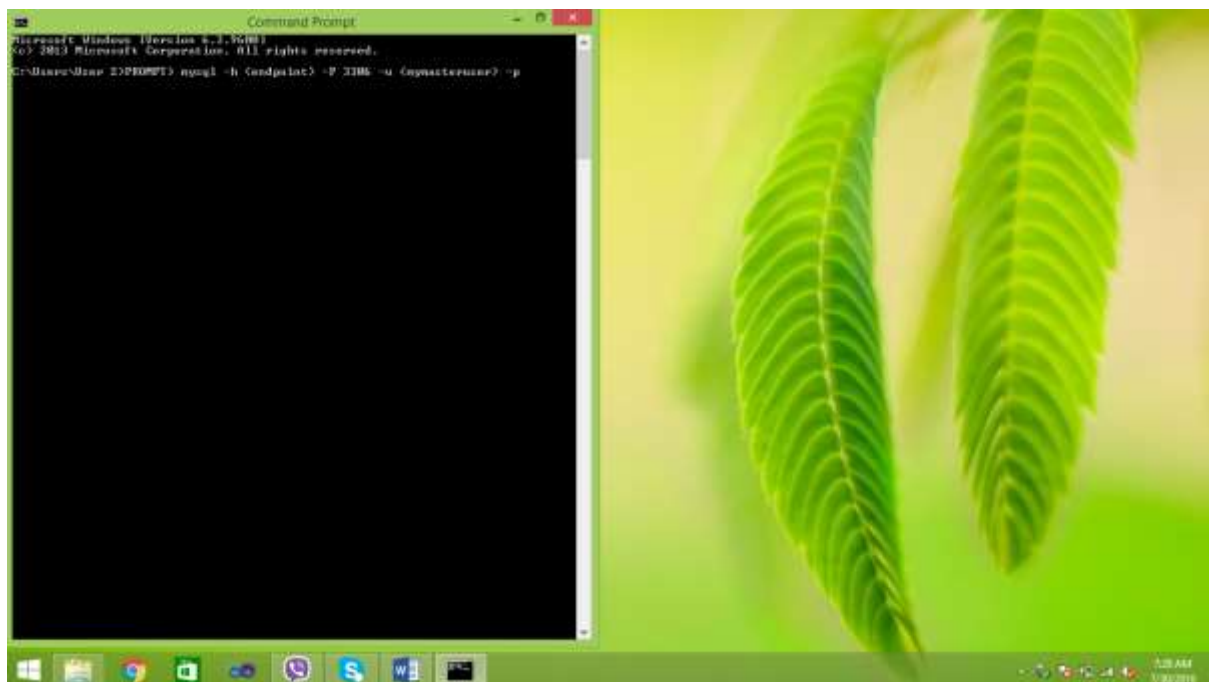


Figure 68