Metasploit AMI for Amazon EC2

Setting up the Metasploit AMI

Last Updated 3/15/12

RAPID7

TABLE OF CONTENTS

About This Guide

Setting Up the Metasploit AMI

About This Guide

This guide provides instructions for you to set up a Metasploit AMI on Amazon EC2. The following sections describe the audience, organization, and conventions used within this guide.

Target Audience

This guide is for IT and security professionals who use Metasploit Pro as a penetration testing solution.

Organization

This guide includes the following chapters:

- About this Guide
- Setting Up the Metasploit AMI for Amazon EC2

Document Conventions

The following table describes the conventions and formats that this guide uses:

Convention	Description
Command	Indicates buttons, UI controls, and fields. For example, "**Click Projects > New Project**."
Code	Indicates command line, code, or file directories. For example, "Enter the following: `chmod +x Desktop/metasploit-3.7.1-linux-x64-installer`."
Title	Indicates the title of a document or chapter name. For example, "For more information, see the *Metasploit Pro Installation Guide*."
Note	Indicates there is additional information about the topic.

Support

You can visit the Customer Center or e-mail the Rapid7 support team to submit questions and receive support for Metasploit Pro and Metasploit Express. To log in to the Customer Center, use the e-mail and password provided by Rapid7.

The following table describes the methods you can use to contact the Rapid7 support team.

Support Method	Contact Information
Customer Center	http://www.rapid7.com/customers/customer-login.jsp
E-mail	support@rapid7.com

There is not an official support team dedicated to the Metasploit Framework or Metasploit Community. If you are a Metasploit Community or Metasploit Framework user, you can visit the Metasploit Community for support.

Resources

The following resources provide additional information to help you set up a Metasploit AMI:

- Amazon EC2 User Guide
- Amazon EC2 Getting Started Guide
- Amazon EC2 Elastic IP Configuration Guide
- Metasploit Pro Getting Started Guide
- Metasploit Pro User Guide
- Metasploit Community Site

Supported Applications

The Metasploit EC2 image contains the following applications:

- Ubuntu 10.04 LTS Base Install
- Vim
- SSH
- Links
- Lynx
- Metasploit Pro

Setting Up the Metasploit AMI

If you have an Amazon Web Services (AWS) account, you can set up an Amazon Machine Image (AMI) to use Metasploit from the cloud. An AMI is a machine that stores the information that is necessary to launch an instance of Metasploit and uses the Amazon EC2 web service to run from the cloud.

Before You Begin

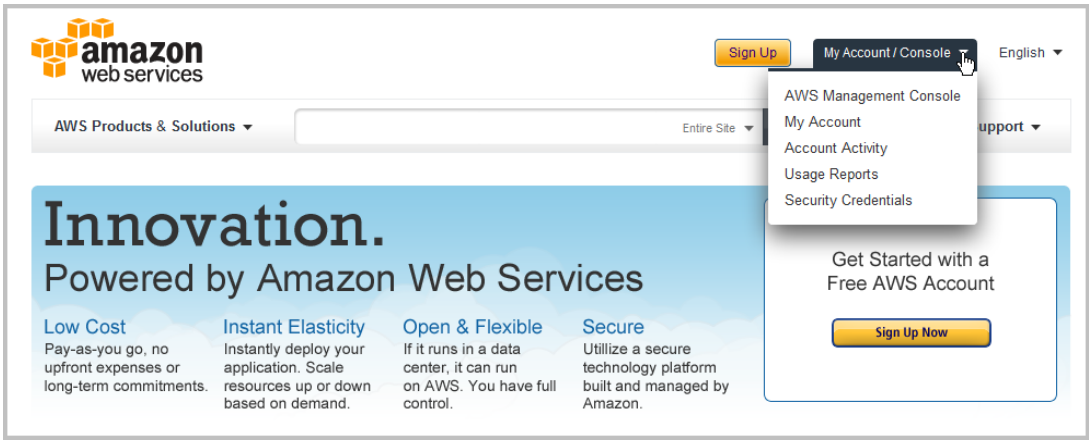
Before you can begin, you must familiarize yourself with Metasploit Pro and the operating systems that the Metasploit AMI contains, such as Snort, Ubuntu, VIM, SSH, Links, and Lynx.

Amazon Web Services Account

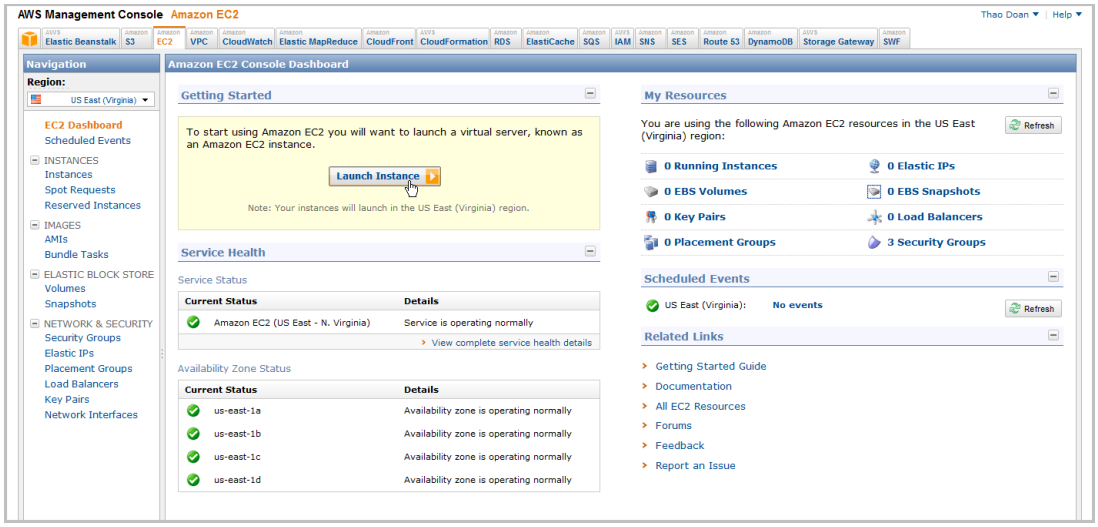
If you do not have an AWS account, you must create one. To create an account, go to http://aws.amazon.com. Find and click the **Sign Up Now** button. When the **Create an AWS Account** window appears, complete the onscreen instructions.

Setting up the Metasploit AMI

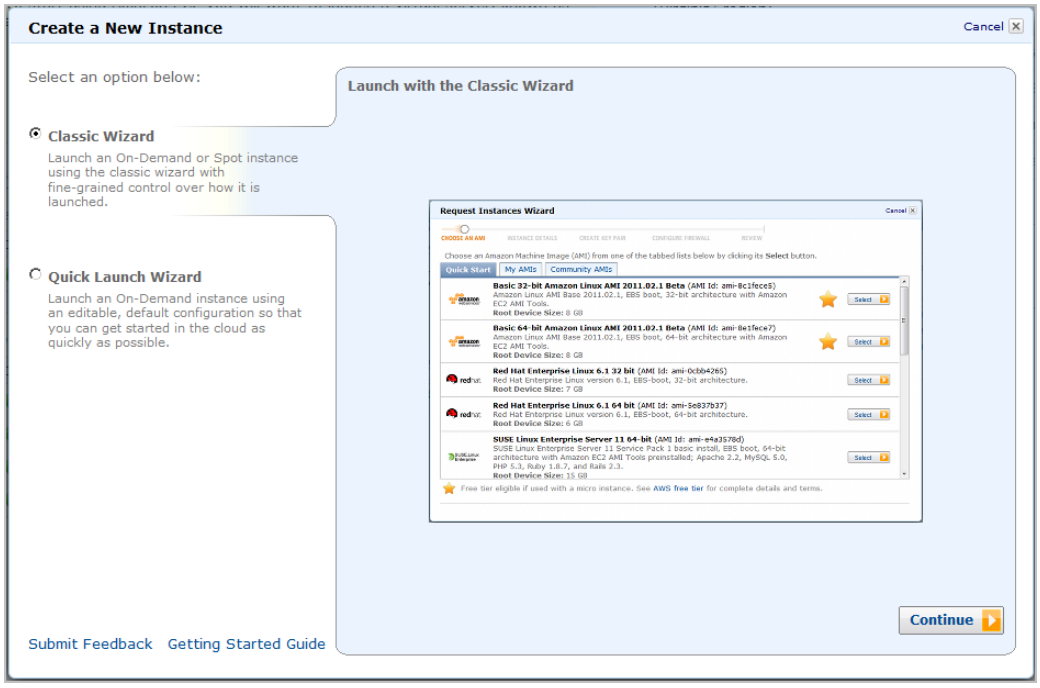
1. Log in to the Amazon Web Services at http://aws.amazon.com.
2. Select **My Account/Console > AWS Management Console**.



3. Click the **Amazon EC2** tab and click **Launch Instance**.

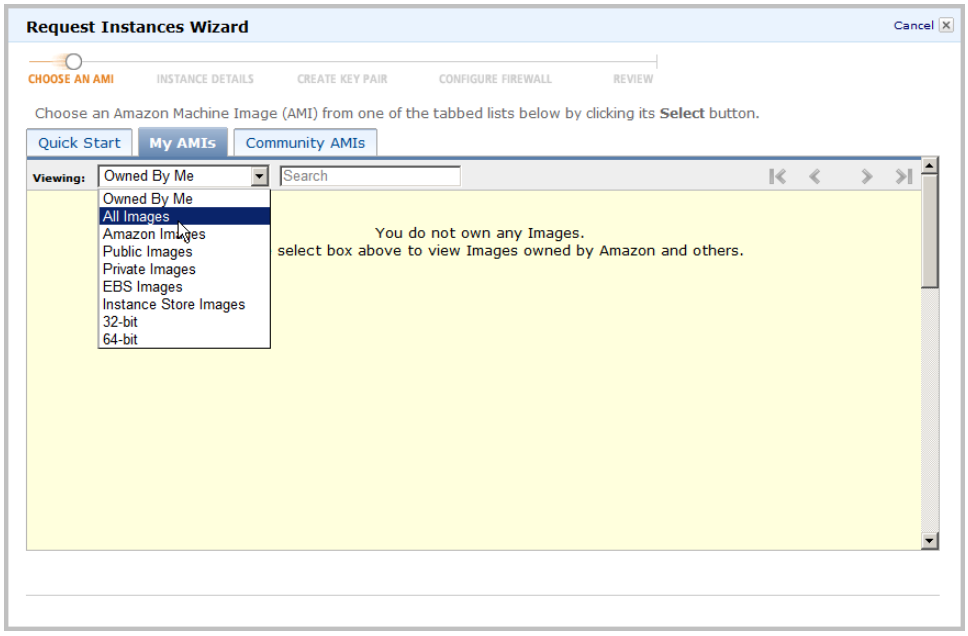


4. When the **Create a New Instance** window appears, choose **Launch Classic Wizard** and click **Continue**.



5. Click the **My AMIs** tab. The wizard displays a list of AMIs that you own.

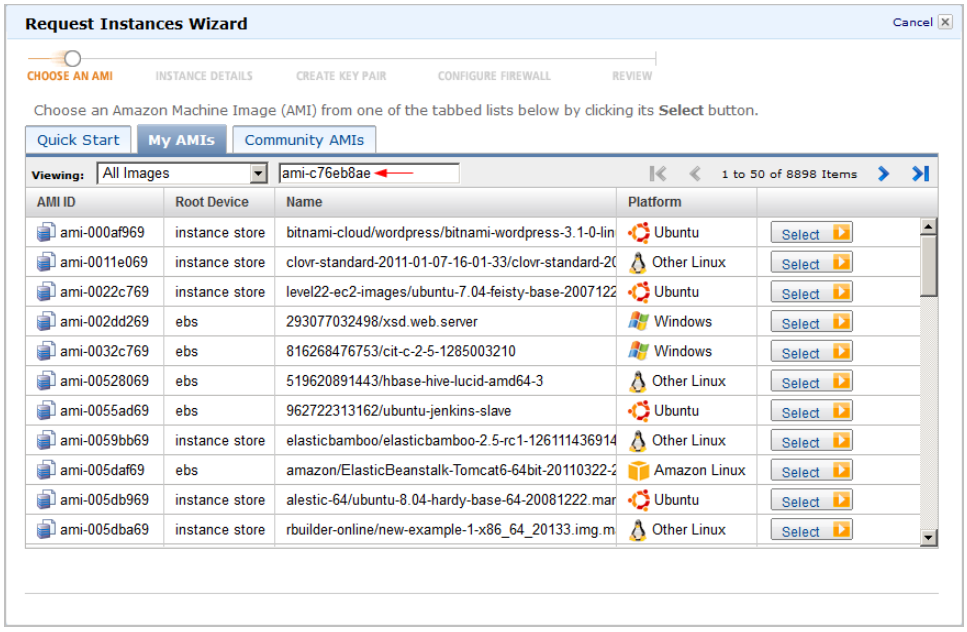
6. Click the **Viewing** list and choose **All Images**.



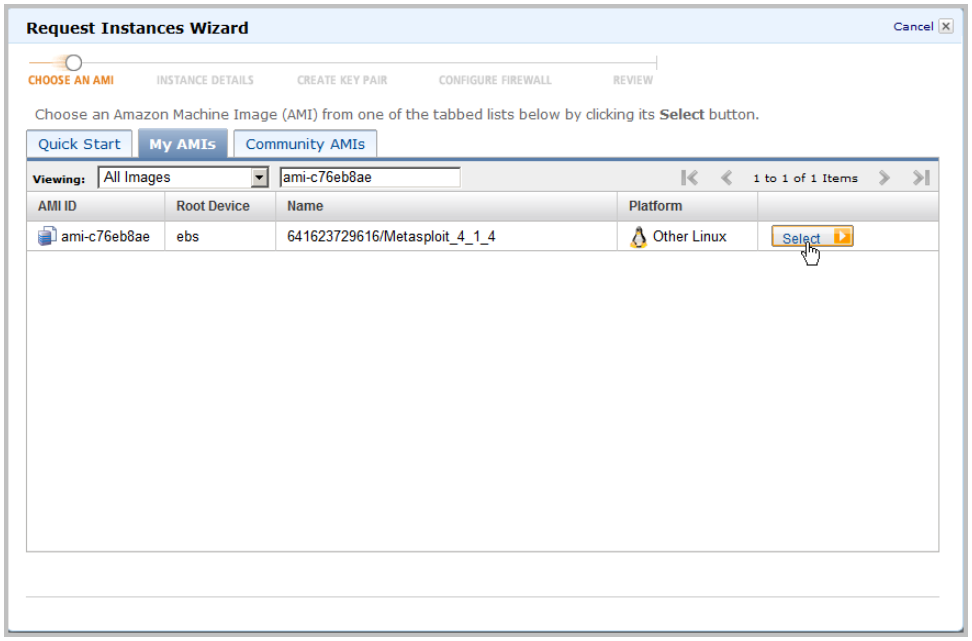
7. Enter the AMI ID for the Metasploit EC2 image in the search field. The latest Metasploit AMI ID is **ami-9a07dbf3** and press enter to perform the search.

   Note: The Metasploit AMI ID differs for each version. If you want to view additional images that are available, you can search for “Metasploit” instead of the AMI ID. However, Rapid7 can only ensure the validity of images that use the AMI

IDs that Rapid7 specifies.

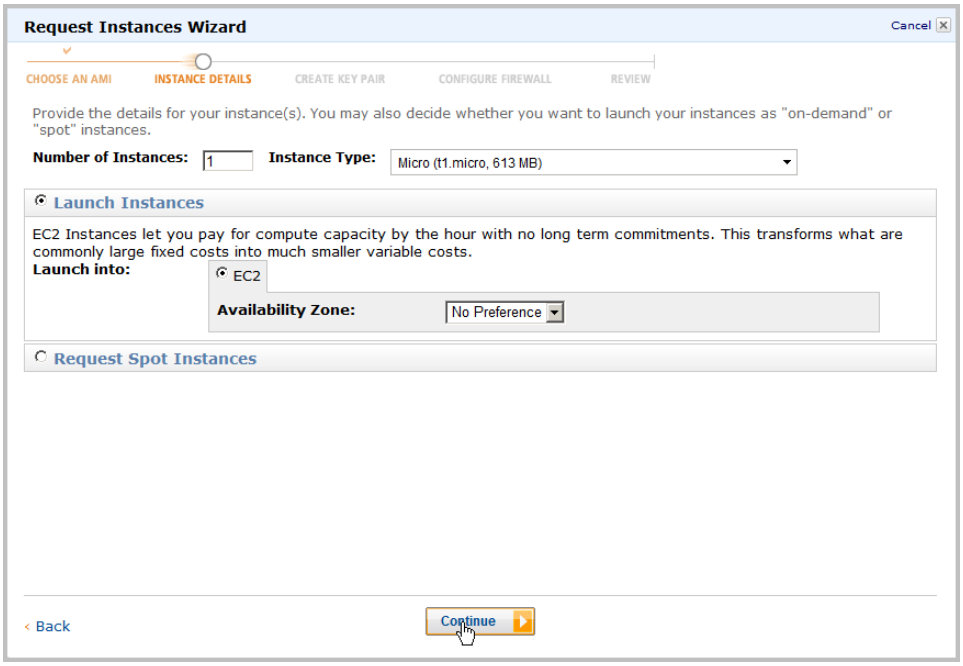


8. Select the AMI that you want to create.

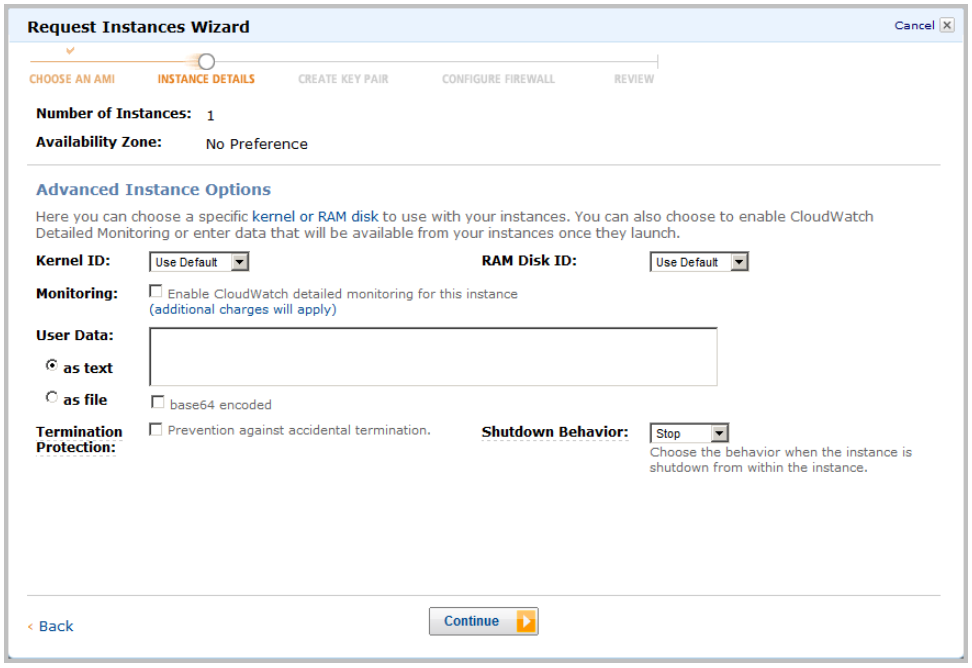


9. Define the instance details, which determine the number of instances and type of instances you want to create.The large instance type, **m.large**, is recommended.

Click **Continue**.

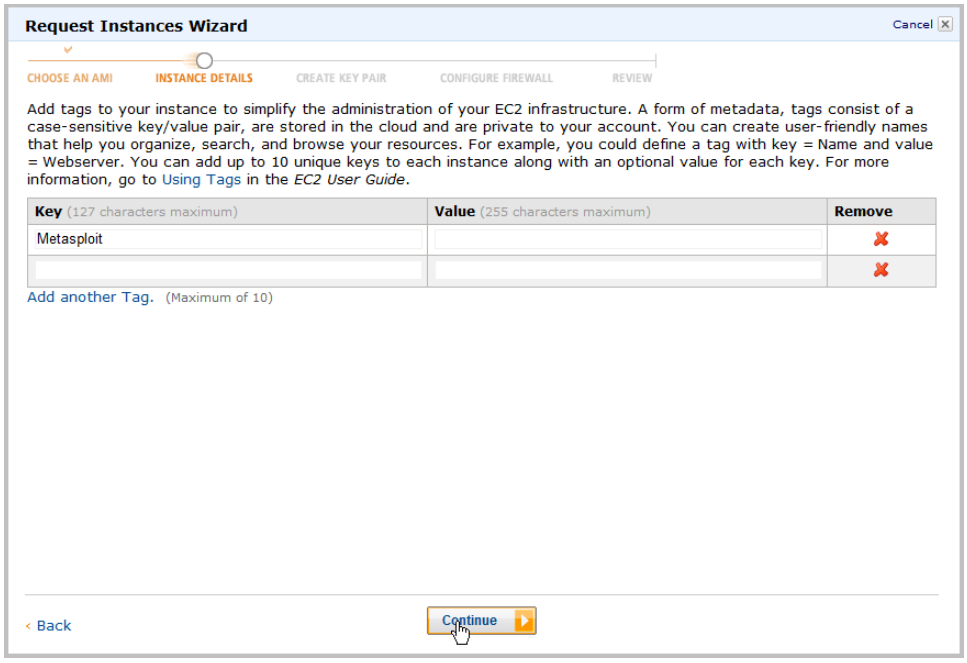


10. Define the advanced details for the instance, which determine the amount of kernel or RAM disk that you want the instance to use. The default values are recommended. Click **Continue**.



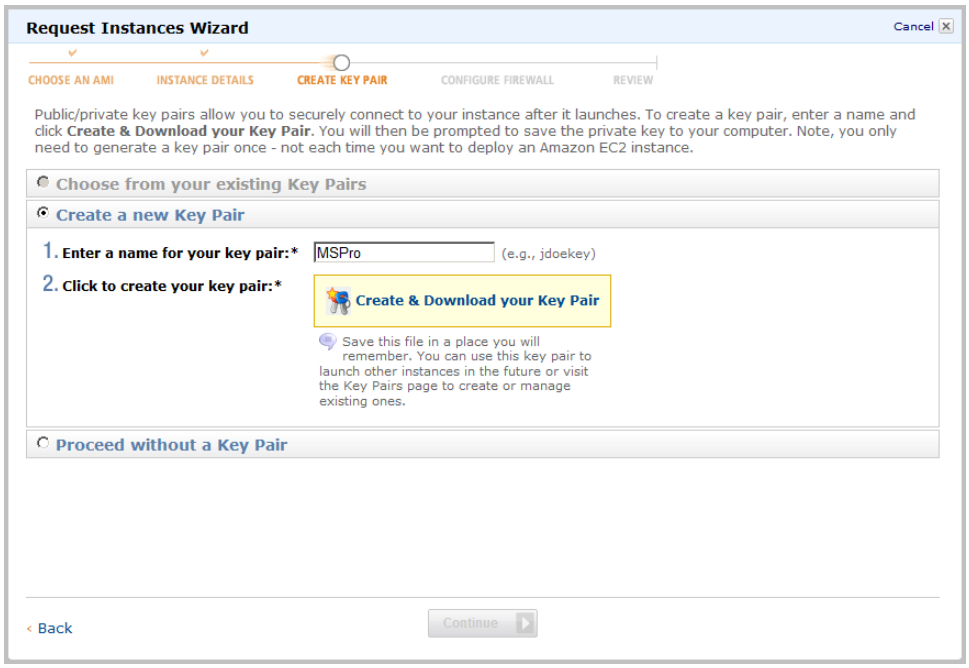
11. Add tag to the instance to help you organize and search for resources. Then, click

Continue.



12. Create a key pair. To create a key pair, enter a name for the key pair and then click the **Create and Download your Key Pair** link. Your local system prompts you to save the key pair. Remember where you save the key pair because you need to access this information again.

    After you create the key pair, click **Continue**.

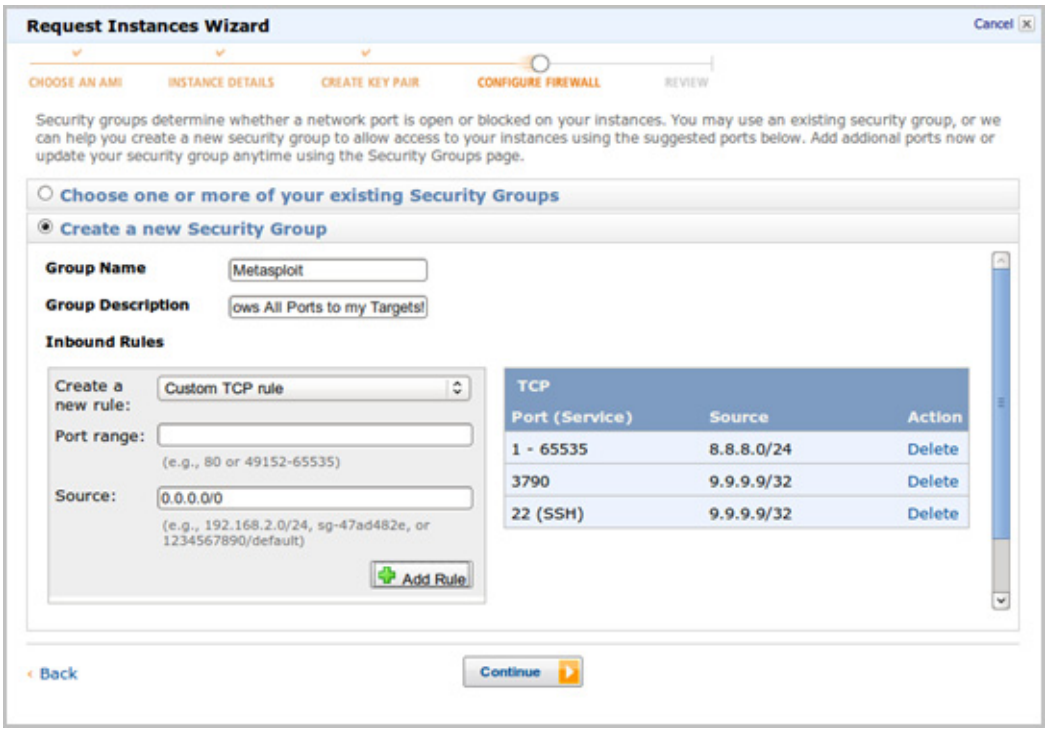


13. Create a security group. To create a security group, you must define the group name, group description, and inbound rules. You must create an inbound rule that defines the TCP and UDP ports that are open to your target range.

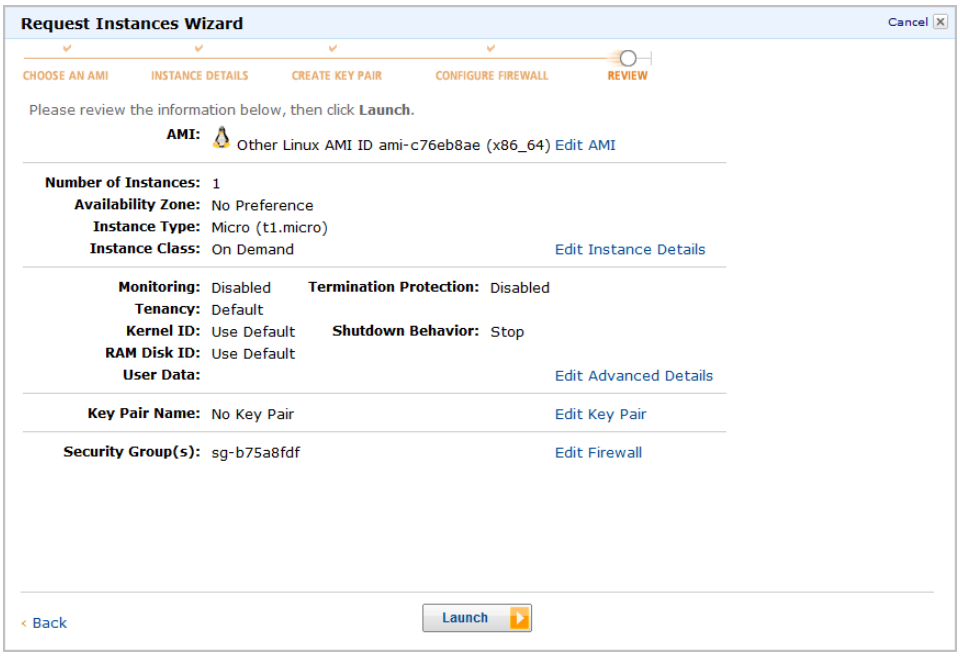
Ports 22/TCP and 3790/TCP must be available on your system. The following image shows the inbound rules that you can create for the instance.

For example, the first rule defines 8.8.8.0/24 as the range that you want to test. The second and third rules define 9.9.9.9/32 as the IP address for the attacking machine and the ports that are open to the instance.

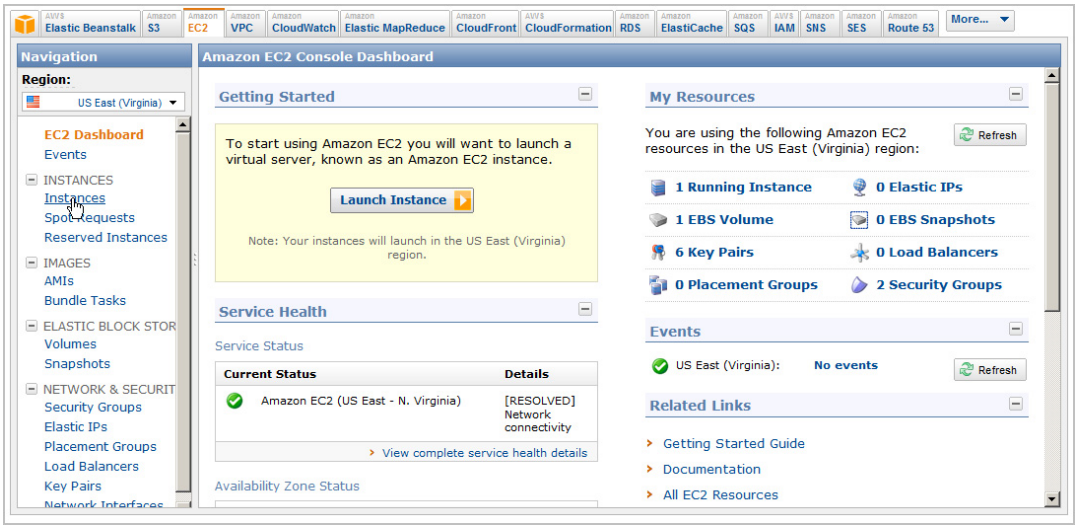
Click **Continue** after you define the inbound rules.



14. The next window displays the details for the instance. Verify that the settings for the instance are correct and launch the instance.



15. After you launch the instance, a window displays and alerts you that your instance is launching. Click the link provided from the window to view a list of your instances.

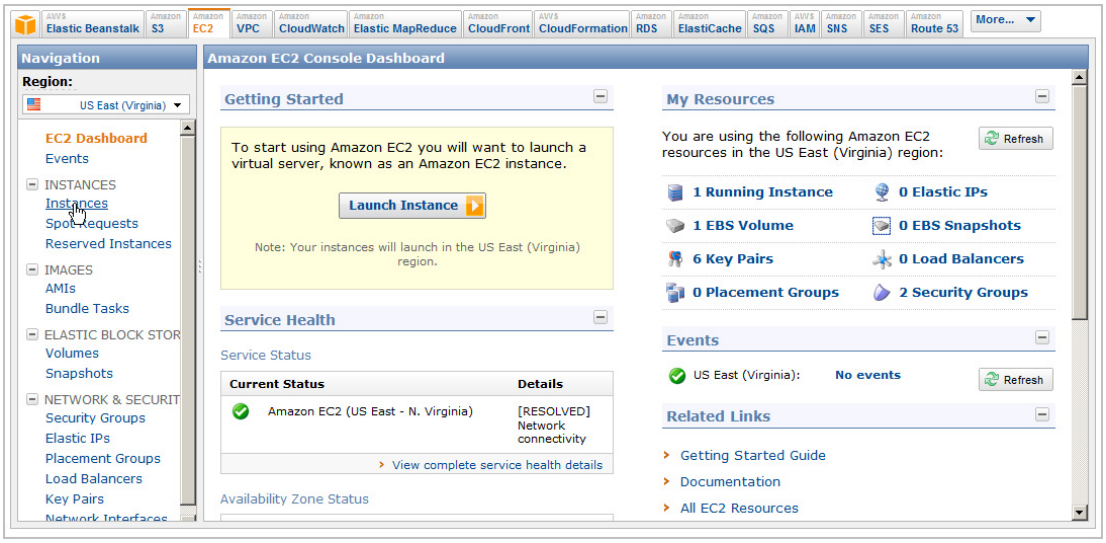


Connecting to the Metasploit AMI from a Linux Machine

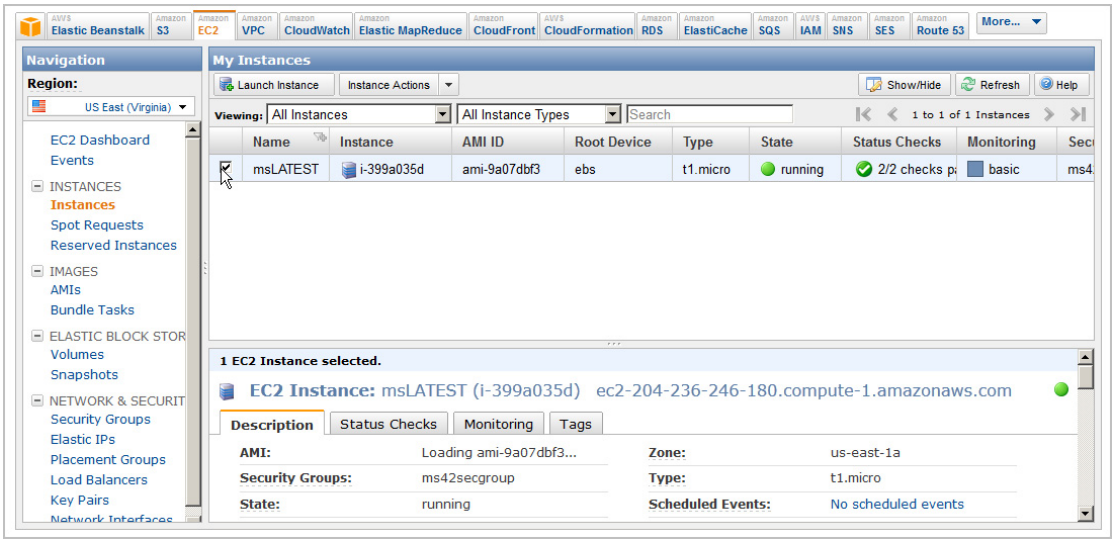
1. Open a command line terminal.
2. Use the `chmod` command to change the permissions for the SSH key pair to 600 For example, you can enter the following command:

```
chmod 600 [your keypair.pem]
```

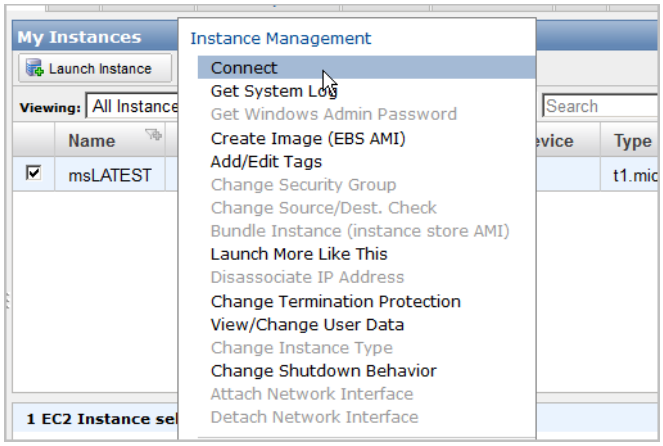
3. From the Amazon Management Console, open the Amazon EC2 Console.
4. From the Navigation pane, click **Instances**. A list of your instances displays.



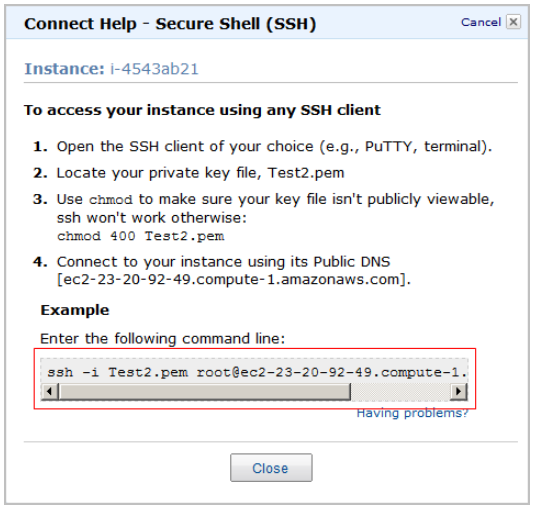
5. Make sure that the Metasploit instance has a **Running** status, and then select the instance.



6. Click the **Instance Actions** list and choose **Connect**.



7. The **Connect Help** window appears. Copy the command line example provided to you in the **Connect Help** window.



8. Run the SSH command that you copied from the Connect Help window.

```
ssh -i [your keypair.pem] ubuntu@ec2-50-17-112-163.compute-
1.amazonaws.com.
```

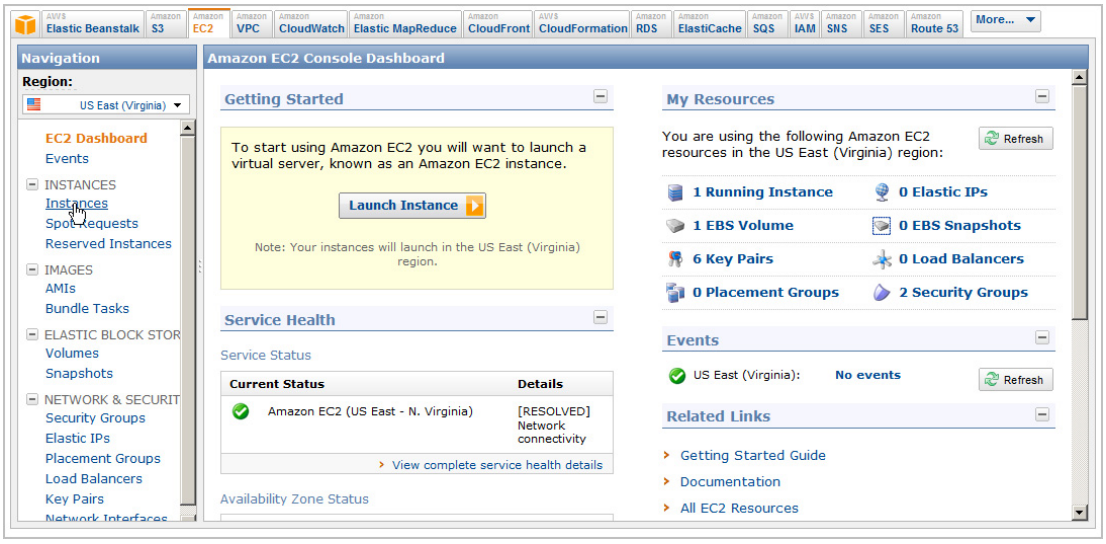
After the login appears, the Metasploit Pro installer runs the set up script and creates an account for you. Copy the account information that the system provides. The configuration is complete.

```
[*] Running Metasploit Pro setup script.
[*] Starting unattended Metasploit Pro installer.
[*] Please stand by, this will take a few minutes.
[*] Generating initial Postgres database.
[*] Generating SSL certificate and initial API key.
[*] Creating a Metasploit Pro user named admin.
[*] Please wait while the environment is loaded.
[*] Creating user 'admin' with password '[password]' ...
[*] User admin has been created, please change your password on
login.
[+] Metasploit user created!
[+] This Metasploit Pro instance can be accessed at: https://
[hostname]:3790
[*] Make sure your security group is configured to allow ALL
PORTS OPEN to your targets.
[+] The current API key is: cP3AyY8aQ28j6L0emei6mEJGQJkYQiER
[+] Installation Finished.
[+] The latest Metasploit Pro documentation can be found at:
[+] https://community.rapid7.com/community/
metasploit?view=documents
```

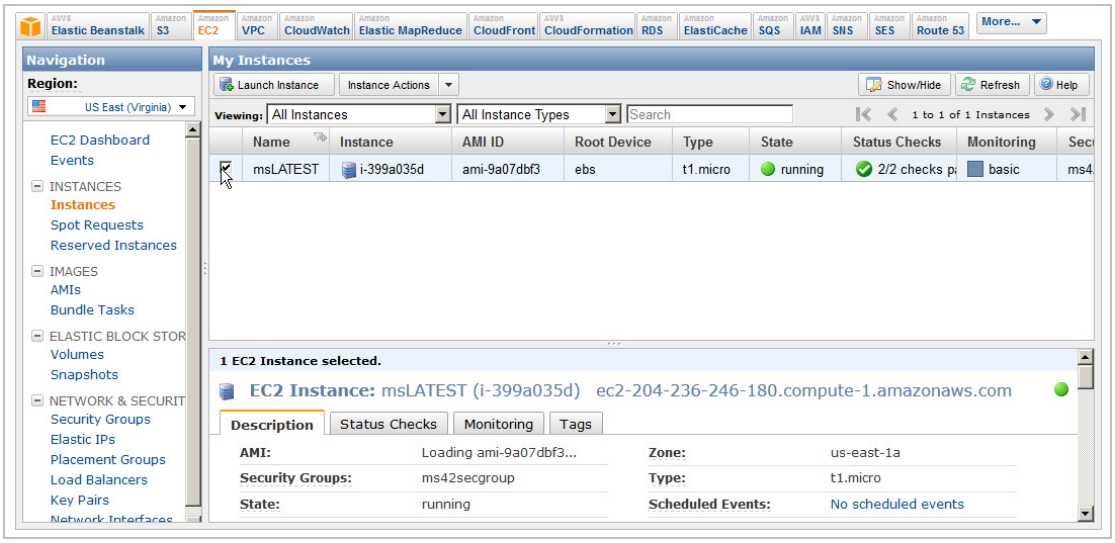
Connecting to the Metasploit AMI from a Windows Machine

1. Start PuTTYgen to convert the key pair pem file to a PuTTY private key file.
2. Click **Load** and browse to the location of the private key pair that you saved earlier. You may need to change the file extensions from **PuTTY Private Key Files** (.ppk) to **All Files** to view the pem file.
3. Select the pem key and click **Open**.
4. Click **OK** when the PuTTYgen notice appears.
5. Click **Save private key**.
6. Click **Yes** when PuTTYgen warns you about saving the key without a passphrase.
7. Close PuTTYgen.
8. From the Amazon Management Console, open the Amazon EC2 Console.

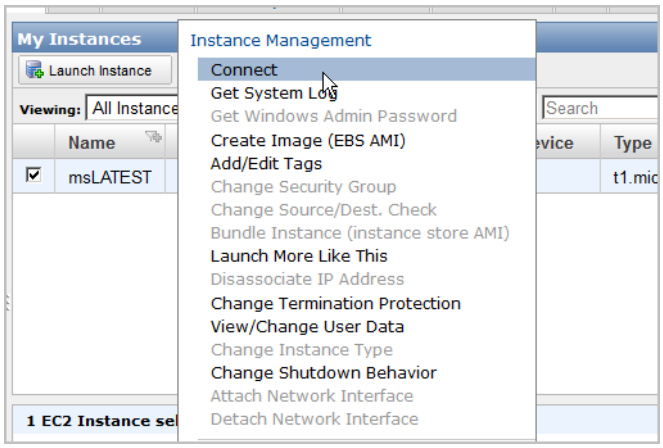
9. From the Navigation pane, click **Instances**. A list of your instances displays.



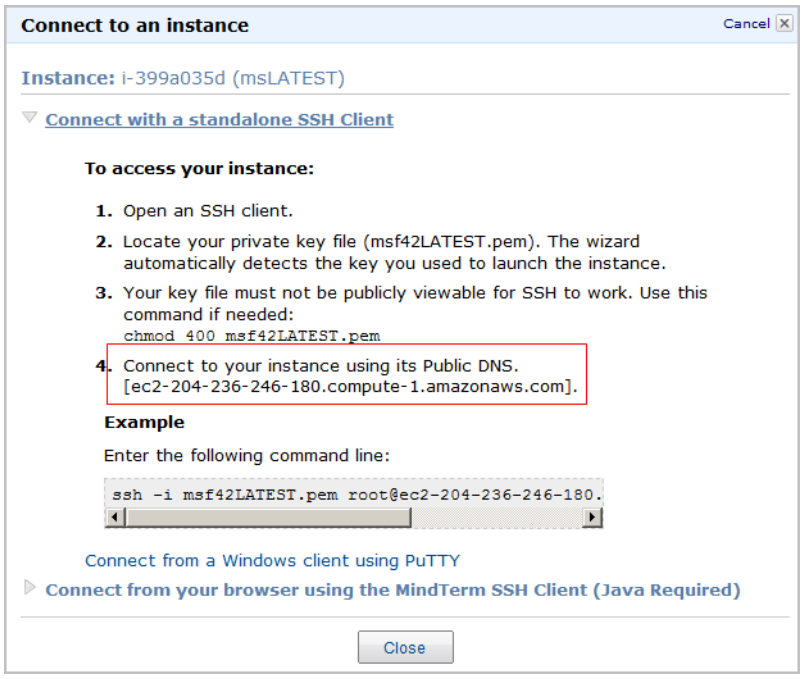
10. Make sure that the Metasploit instance has a **Running** status, and then select the instance.



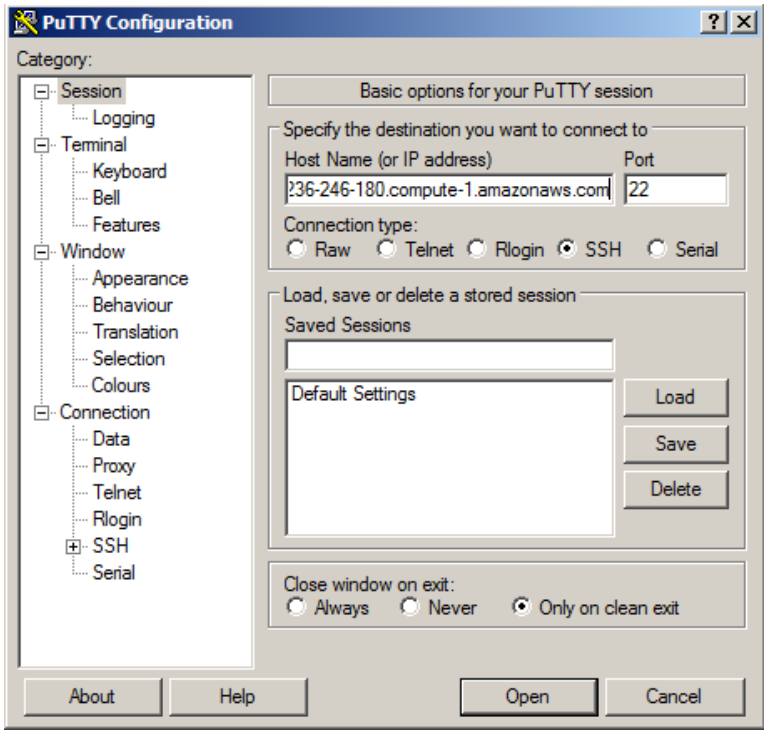
11. Click the **Instance Actions** list and choose **Connect**.



12. The **Connect Help** window appears. Copy the public DNS from the **Connect Help** window.



13. Start PuTTY to connect to the Metasploit instance.
14. Enter the public DNS in the **Host Name** field.



15. Choose **Connection > SSH > Auth**. The options for controlling SSH authentication appears.
16. From the **Authentication Parameters** area, click **Browse** to navigate to the

PuTTY private key file that you generated earlier.

17. Click **Open**.
18. An SSH session window opens. Click **Yes** when the security alert appears.

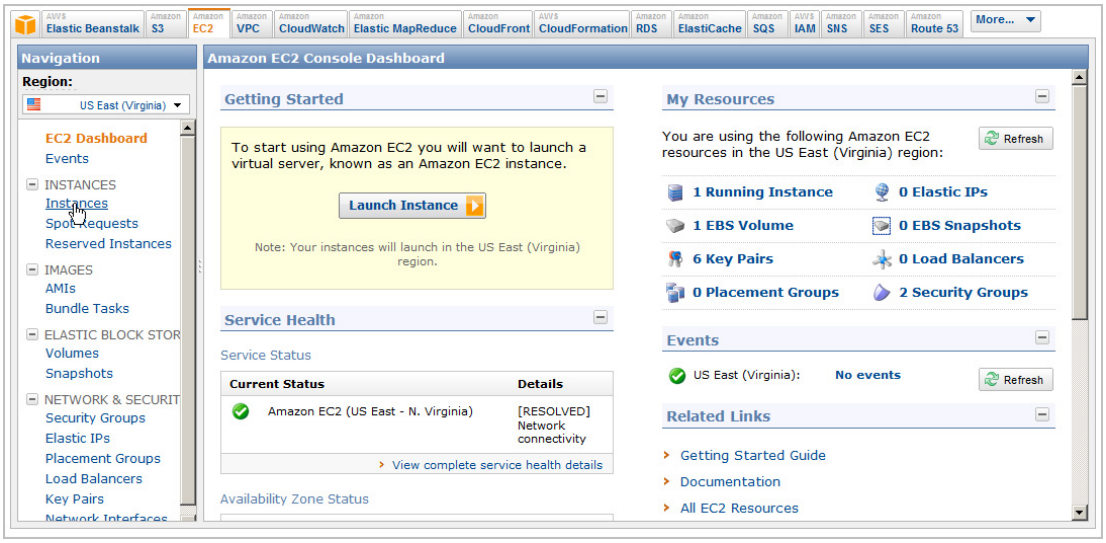
After the login appears, the Metasploit Pro installer runs the set up script and creates an account for you. Copy the account information that the system provides. The configuration is complete.

```
[*] Running Metasploit Pro setup script.
[*] Starting unattended Metasploit Pro installer.
[*] Please stand by, this will take a few minutes.
[*] Generating initial Postgres database.
[*] Generating SSL certificate and initial API key.
[*] Creating a Metasploit Pro user named admin.
[*] Please wait while the environment is loaded.
[*] Creating user 'admin' with password '[password]' ...
[*] User admin has been created, please change your password on
login.
[+] Metasploit user created!
[+] This Metasploit Pro instance can be accessed at: https://
[hostname]:3790
[*] Make sure your security group is configured to allow ALL
PORTS OPEN to your targets.
[+] The current API key is: cP3AyY8aQ28j6L0emei6mEJGQJkYQiER
[+] Installation Finished.
[+] The latest Metasploit Pro documentation can be found at:
[+] https://community.rapid7.com/community/
metasploit?view=documents
```

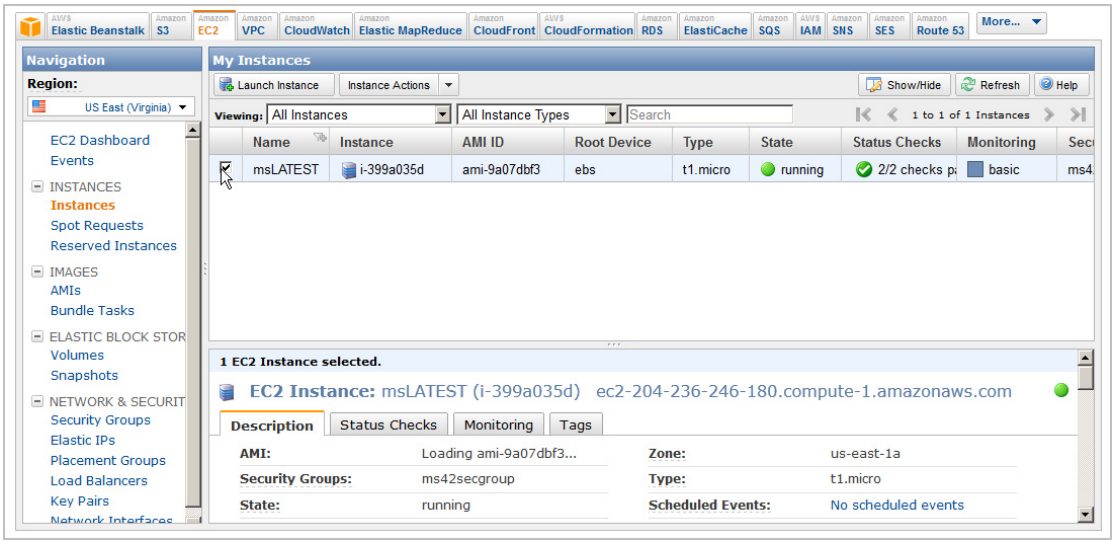
Terminating the Instance

Amazon bills you when your instance begins to boot up and continues to bill you until you terminate the instance. Therefore, it is very important that you terminate the instance when you are done.

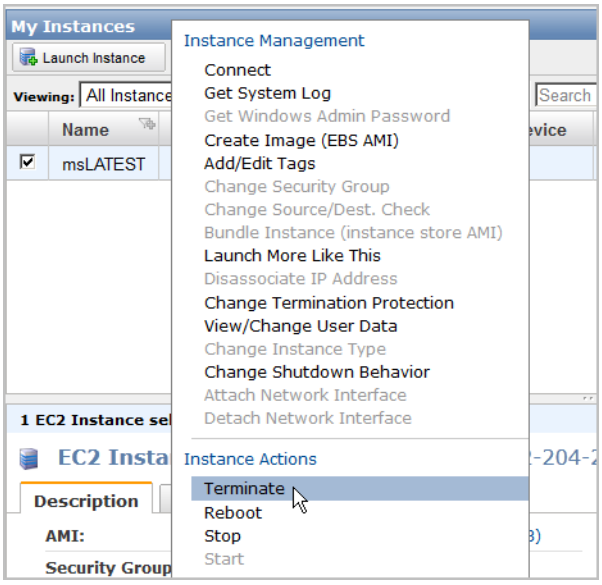
1. From the Amazon Management Console, open the Amazon EC2 Console.
2. From the Navigation pane, click **Instances**. A list of your instances displays.



3. Select the instance that you want to terminate.



4. Select Instance **Actions > Terminate**.



5. Click **Yes, Terminate** to confirm that you want to terminate the instance.