Amazon Elastic Compute Cloud Elasticfox

Getting Started Guide

Elasticfox Version 1.7-000108

Table of Contents

What's New

The following table describes the important changes since the last release of the Amazon EC2 Elasticfox Getting Started Guide.

Change	Description	Release Date
Initial Release	This is the initial release of the Elasticfox Guide	October 20, 2008
Update 1	Updates to include Multi-Region Support and Elasticfox UX Enhancements	December 09, 2008
Update 2	Updates to include Amazon Virtual Private Cloud (VPC) Support	August 25, 2009

Introduction

Amazon Elastic Compute Cloud (EC2) is a web service that provides resizable compute capacity in the cloud. It is designed to make web-scale computing easier for developers.

Amazon EC2's simple web service interface allows you to obtain and configure capacity with minimal friction. It provides you with complete control of your computing resources and lets you run on Amazon's proven computing environment. Amazon EC2 reduces the time required to obtain and boot new server instances to minutes, allowing you to quickly scale capacity, both up and down, as your computing requirements change. Amazon EC2 changes the economics of computing by allowing you to pay only for capacity that you actually use. Amazon EC2 provides developers the tools to build failure resilient applications and isolate themselves from common failure scenarios.

Amazon Virtual Private Cloud (Amazon VPC) is a secure and seamless bridge between a company's existing IT infrastructure and the AWS cloud.

Amazon VPC enables enterprises to connect their existing infrastructure to a set of isolated AWS compute resources via a Virtual Private Network (VPN) connection, and to extend their existing management capabilities such as security services, firewalls, and intrusion detection systems to include their AWS resources. Amazon VPC integrates today with Amazon EC2, and will integrate with other AWS services in the future.

This Getting Started Guide is designed to teach System Administrators, Software Developers, and other IT professionals how to utilize the Amazon EC2 and Amazon VPC services through several easy tutorials. In this guide, we will demonstrate Elasticfox, a plug-in to the Mozilla Firefox browser that allows you to graphically interact with Amazon EC2 and Amazon VPC. Amazon Web Services (AWS) maintains and distributes this plug-in.

We have organized this Getting Started Guide into five tutorials, ranging from starting a new virtual server (instance) to using our advanced features. Each of these tutorials will provide you with the basics of how to use these components. Users are encouraged to leverage our additional resources (see the Related Resources Section) to learn about more advanced features of our system, like our APIs.

Throughout these tutorials, we highlight areas that have additional considerations if using Amazon VPC. Some features described may only be available if using Amazon VPC, whereas other features may not be available. Look for the VPC icon, as seen to the left on this paragraph, to quickly find these items.

Users with minimal knowledge can interact with Amazon EC2 and Amazon VPC using Elasticfox, but it is recommended to have basic understanding of web services. If you need to get familiar with this concept, please go to the W3 Schools Web Services Tutorial.

Amazon Elastic Compute Cloud is often referred to within this guide as "Amazon EC2" or simply "EC2"; the Amazon Simple Storage Service is often referred to within this guide as "Amazon S3" or simply “S3”; and the Amazon Virtual Private Cloud (VPC) is often referred to within this guide as “Amazon VPC” or simply “VPC”. All copyrights and legal protections still apply.

Setting up Elasticfox

Prerequisite Software

This tutorial exclusively uses Elasticfox for the purposes of this Getting Started Guide. The sections below walk you through how to install Mozilla Firefox, the web browser required to use Elasticfox, and the Elasticfox plug-in.

Installing Mozilla Firefox

The current Elasticfox plug-in requires Mozilla Firefox version 1.5.0 or later. To get Mozilla Firefox, please perform the following steps:

1. In your current web browser, please go to: http://www.mozilla.com.
2. Click on the "Download Firefox – Free" button.
3. Save the file, and follow the installation steps on the acknowledgement page.

Installing the Elasticfox Add On

Once Mozilla Firefox is installed, you can now install the current version of the Elasticfox add on. To do this, please perform the following steps:

1. In your Mozilla Firefox web browser, please go to: http://developer.amazonwebservices.com/connect/entry.jspa?externalID=609&categoryID=88.
2. Click on the download button.
3. After the pop-up box comes up, press the install button.
4. Your Mozilla Firefox browser will prompt you to restart your browser. After you have restarted, you will now have the ability to use Elasticfox.
5. To launch the add on, simply go to the "Tools" menu in Firefox and select "Elasticfox".
6. Please utilize the "Setting up an AWS Account" and "Setting up Elasticfox" sections below to setup Elasticfox with your account and profile.

Setting up an AWS Account

To use Amazon EC2, you must sign up for a AWS Account, sign up for Amazon EC2, and sign up for the Amazon Simple Storage Service (Amazon S3). These are three different actions that must be performed separately. For information on obtaining an AWS Account, go to the Amazon AWS Home Page (http://aws.amazon.com).

Signing up for Amazon EC2

To utilize the Amazon EC2 service, you will need to enable your AWS account for use with Amazon EC2. If you don't already have an AWS account, you will be prompted to create one as part of the sign up process. If you already have an Amazon EC2 account, you can skip this step. To sign-up for Amazon EC2 simply perform the following steps:

1. Go to the Amazon EC2 homepage (http://aws.amazon.com/ec2) in your web browser.
2. Click **Sign Up For Amazon EC2** in the top right of the screen and follow the on-screen instructions.

Signing up for Amazon S3

Amazon EC2 AMIs are stored in and retrieved from Amazon S3. This means you will also need to sign up for Amazon S3. If you already have an Amazon S3 account, you can skip this step.

1. Go to the Amazon S3 homepage (http://aws.amazon.com/s3) in your web browser.
2. Click the **Sign up for Amazon S3** button.

Optional: Signing up for Amazon VPC

To use Amazon VPC in conjunction Amazon EC2, you must also be subscribed to Amazon VPC. To sign-up for Amazon VPC simply perform the following steps:

1. Go to the Amazon VPC homepage (http://aws.amazon.com/vpc) in your web browser.
2. Click the **Sign up for Amazon VPC** button.

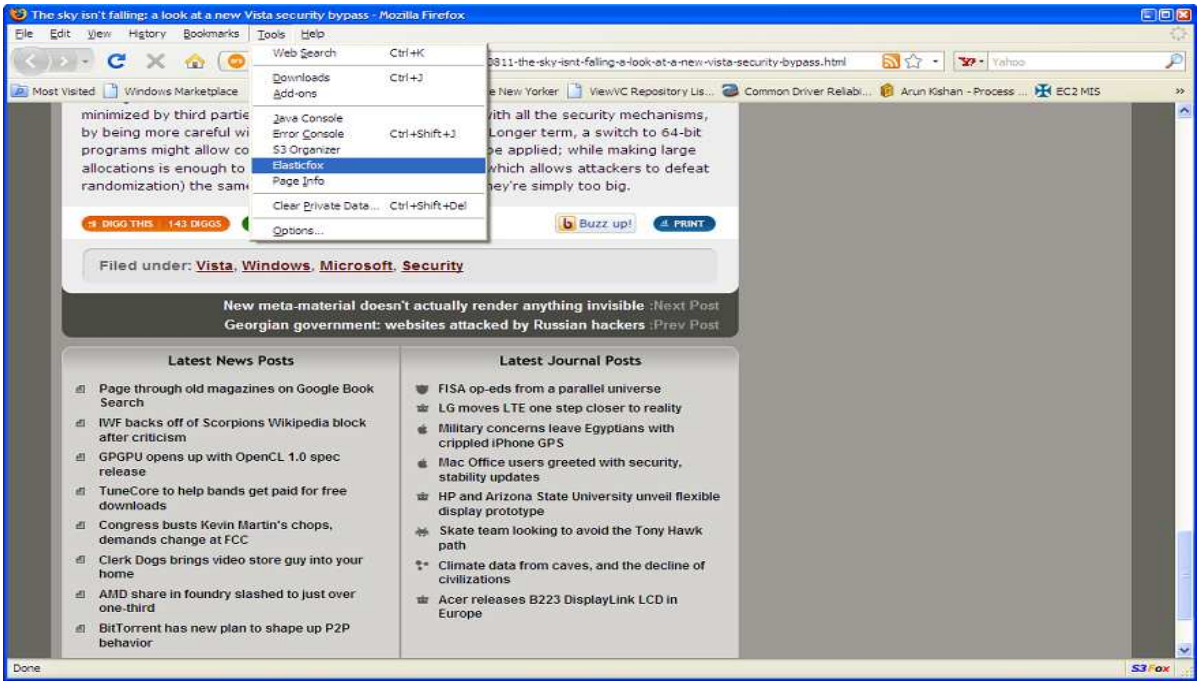
Setting up Elasticfox

The following steps are required to configure Elasticfox with your specific security credentials. These steps only need to be performed once, unless you change your security keys change again. Once you have configured these settings, you will be ready to proceed to the tutorials.

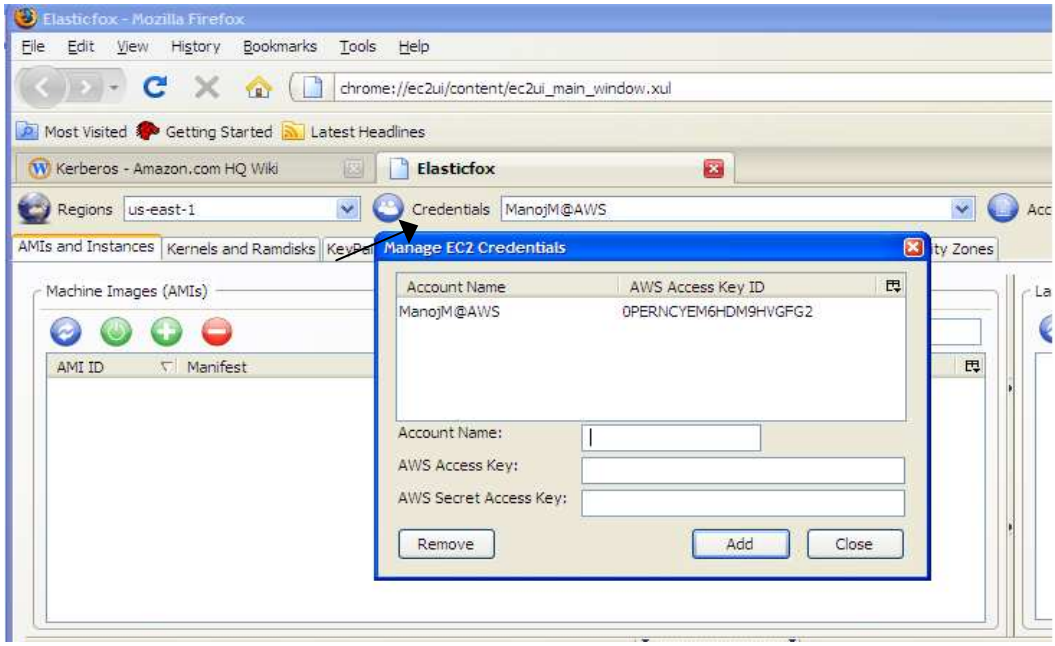
Setting up the Credentials

Elasticfox uses your Access Identifiers to identify you as the sender of a request to an AWS web service. Access identifiers are also used to authenticate requests to AWS. The steps below show how to configure Elasticfox with your credentials, so that it can perform web service requests on your behalf.

1. Launch Elasticfox by clicking on "Tools" menu in Mozilla Firefox and selecting "Elasticfox".



2. If this is the first time you are loading Elasticfox, you will be prompted to enter your AWS credentials. You can enter new credentials or modify existing credentials by clicking on the "Credentials" button in the top center of the Elasticfox window.



3. Enter your Account Name. You can set the Account Name to anything you want. It's merely a descriptive name used to organize your credentials. We recommend something meaningful (like the email address you used when you created the account).

4. Enter your Access Key and Secret Key into the "Credentials" dialogue box. These can be found under the "Your Account" menu at http://aws-portal.amazon.com/gp/aws/developer/account/index.html?action=access-key.

5. Click the Add button in the "Credentials" dialogue box to add your access key and secret key to the Elasticfox configuration.

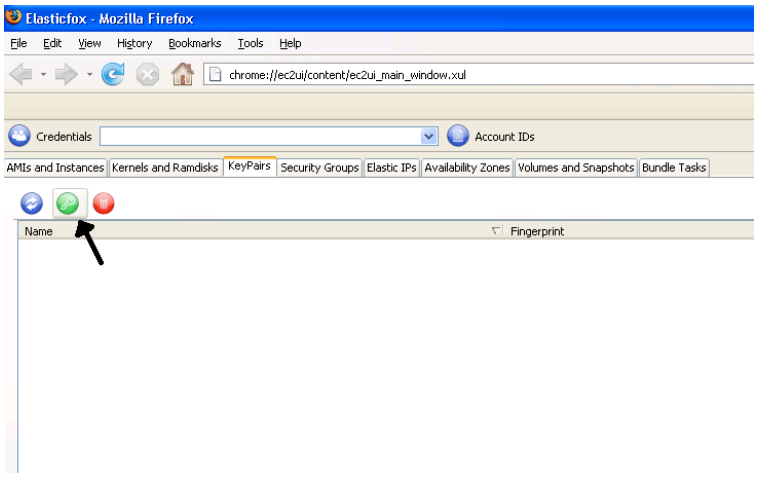
6. Finally, click the "Close" button to complete this configuration.

Creating a KeyPair

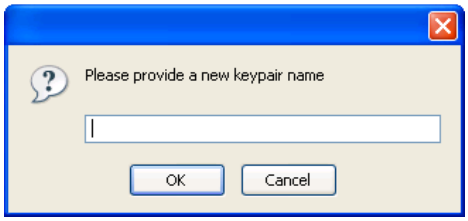
An SSH keypair is used for several purposes including connecting to Linux/OpenSolaris instances and retrieving your Windows Administrator password. To generate a keypair, simply perform the following steps:

1. Click on the "Key Pairs" tab in Elastic Fox.

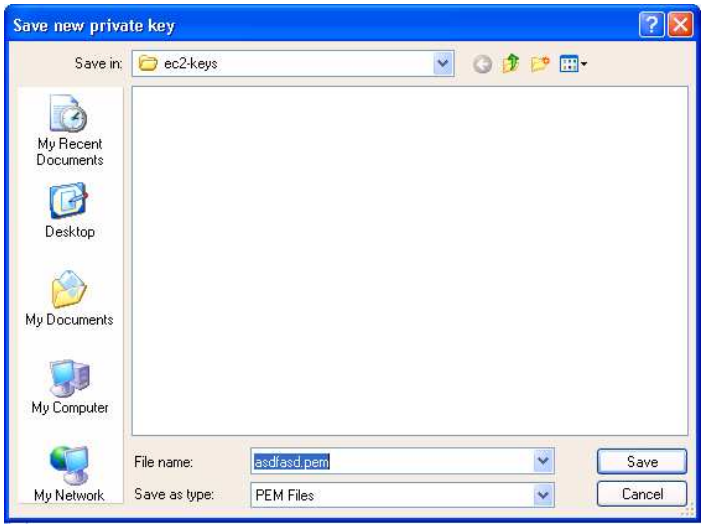
2. Click on the green Key icon at the top of the tab.



3. Type in a name for your KeyPair, and click the "Ok" button.



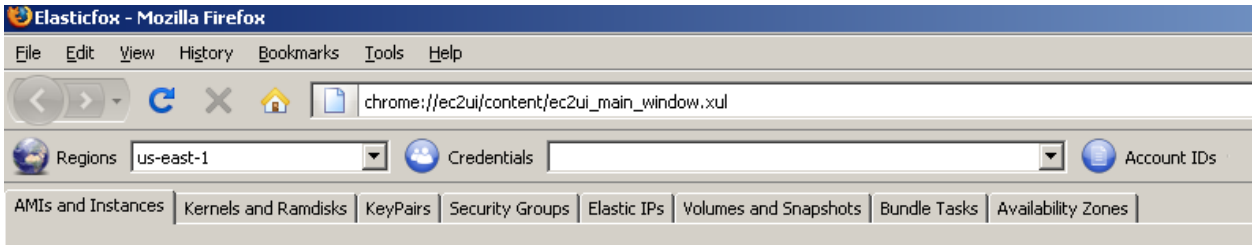
4. You will be prompted for a location to save the .pem file. Select a secure file location, and click "Save".



5. Your KeyPair will now be created; remember this name, because you will use it later.

Choosing your Region

Choose the region of the instances you're going to manage at by selecting it from the drop-down labeled "Regions".



VPC Amazon VPC is currently only available in theus-east-1 region.

Tutorial #1: Running an Instance

Goal

The goal of this tutorial is to launch an Amazon EC2 virtual server, what we call an instance. This tutorial assumes that you have completed the necessary setup as described above.

Core Concepts

The sections below outline the core concepts used in this tutorial.

Amazon Machine Image (AMI)

An Amazon Machine Image (AMI) is an encrypted file stored in Amazon S3. It contains all the information necessary to boot instances of your software. It is somewhat analogous to a snapshot of the boot partition containing the operating system and installed software running on your server.

Amazon EC2 Instance

A running server instantiated from an AMI is referred to as an instance. All instances launched from the same AMI will create a nearly identical running server (except for the IP range or computer name). Note that an instance is ephemeral and that any information on it is lost when it is terminated or if it fails. The Elastic Block Storage feature described in Creating an Elastic Block Store (EBS) Volume of this tutorial can be used to create long term storage for data produced by the instance**.**

Security Group

The security group is analogous to a firewall that can block all incoming (ingress) and outgoing (egress) traffic that does not come in on a specific IP (specified by a CIDR) or port number range. For more information on CIDRs, please visit http://en.wikipedia.org/wiki/CIDR. Each EC2 instance can be a member of up to 100 security groups. Group membership cannot be changed while an instance is running, but the rules within the group can be changed, and will take effect immediately. Multiple security groups can be used to create secure, multi-tiered systems. For example, consider the classic three-tier model consisting of web, application, and database servers. Placing each tier of servers in a distinct security group allows the web server to be accessible externally, with controlled access to the other tiers on an as –needed basis.

Note: Security Groups are not currently available within Amazon VPC. If you are using Amazon VPC, consider using Subnets to group your Amazon EC2 instances. Please see tutorial #5 for more information.

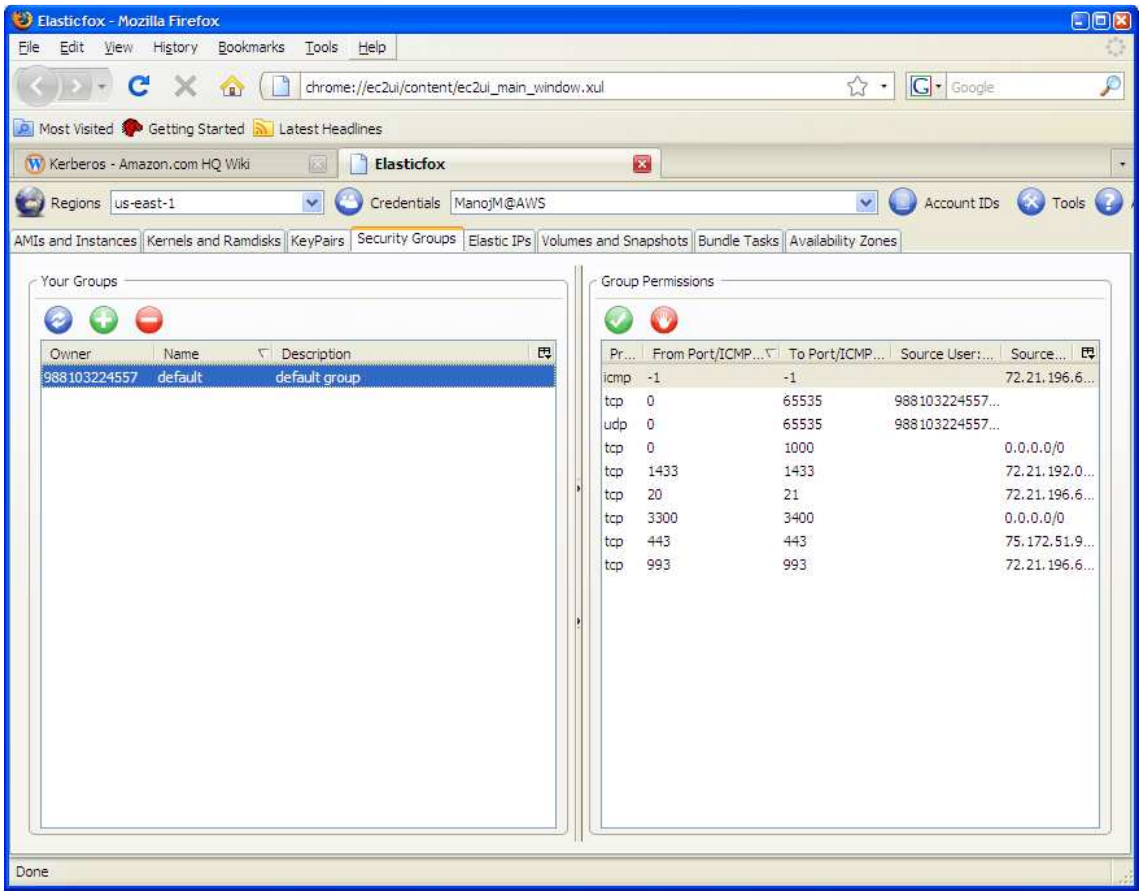
Step 1: Setting up a Security Group

Every launched instance requires that you have a security group defined to specify what network traffic is allowed to reach the instance. By default we do not enable any traffic. If you have already defined a security group to allow network traffic from your address you can skip this step.

For the purposes of this tutorial, we are going to create a new group called “All Incoming”, that will allow any incoming traffic to connect to any launched instances on SSH port (22), HTTP port (80), and RDP port (3389). This will enable us to connect to either a Linux/UNIX or Windows instance. To open these ports for testing purposes, please complete the following steps:

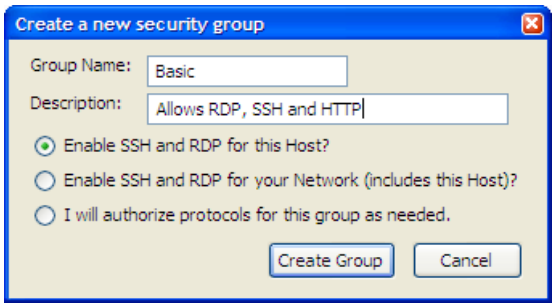
1. Launch Elasticfox by clicking on the “Tools” menu in Firefox, and selecting Elasticfox.

2. Click on the “Security Groups” tab.



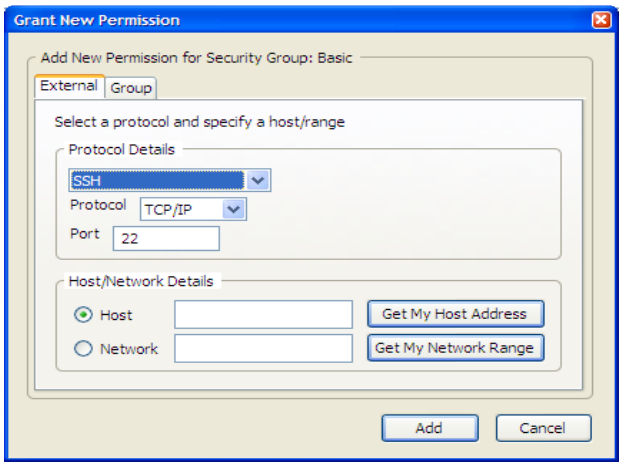
3. Click on the green  icon in the “Your Groups” box.

4. The Group Name and Description fields are used to help you maintain and organize all of your security groups. The default permissions setting for a new group is to enable RDP and SSH for the machine on which Elasticfox is installed. Please select one of the other available options if you would like to fine-tune the permissions for the new Security Group. Clicking “Create Group” will create the new Security Group.



5. Ensure the Security Group is now highlighted and click on the green checkmark in the Group Permissions box. This will allow you to enable specific ports to receive network traffic. Let's open up the HTTP port for access to all hosts on the Internet.

6. Select the HTTP protocol from the protocol dropdown, select "Network" and enter "0.0.0.0/0". If you would like to restrict access to just your local subnet, press "Get My Network Range".



7. Now you will have your security group setup.

Caution

In this example, you enable access to port 80 of the instance for all hosts on the Internet - "0.0.0.0/0". Although this might be acceptable for testing or demo purposes, it is extremely unsafe for production environments. For production systems, you must obtain your public IP address ranges and grant access to those ranges only. For example, if your IP address is 123.123.123.123, you specify "123.123.123.123/32". For more details on controlling network security groups, see the Amazon EC2 Developer Guide.

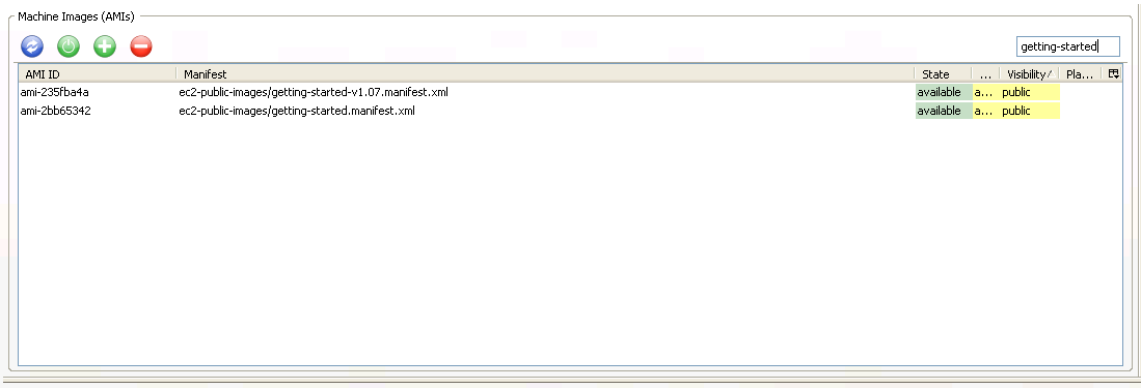
Step 2: Choosing an AMI

Amazon Web Services, software companies, and the community provide many different AMIs to use. You can leverage any of the publicly visible ones to start an instance. A list with more description about many of the paid and public AMIs can be found at: http://developer.amazonwebservices.com/connect/kbcategory.jspa?categoryID=171 and http://developer.amazonwebservices.com/connect/kbcategory.jspa?categoryID=101 respectively. For

the purposes of this tutorial, we will use a pre-configured AMI called “ec2-public-images/getting-started”.

To select this AMI, please perform the following steps:

1. Click on the “Images” tab in Elasticfox.
2. In the text box in the “Images ” section, type in “getting-started” if you want to launch a Linux/UNIX instance or “windows” if you would like a Windows instance. This will search for the image that contains the name “getting-started” or “windows”.

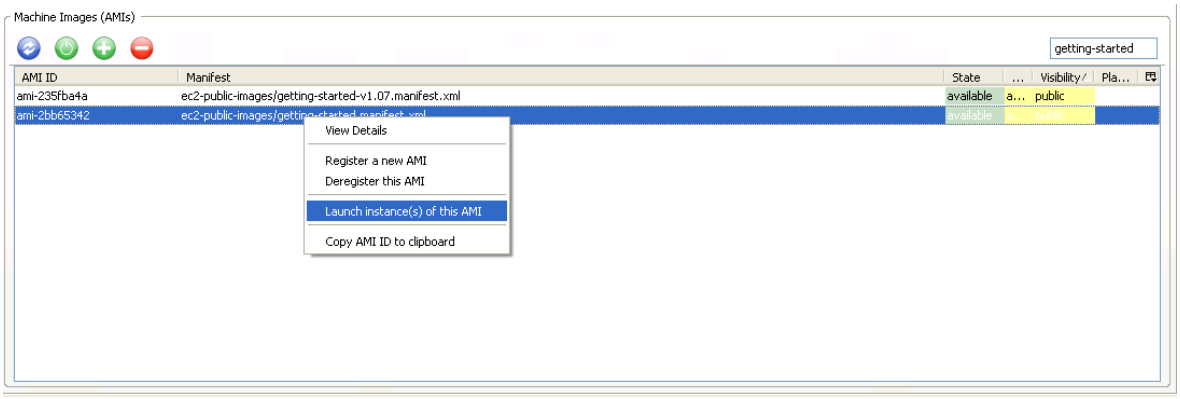


3. Click on the image with the Manifest named “ec2-public-images/getting-started.manifest.xml” for Linux/UNIX or “ec2-public-windows-images/Server2003r2-i386-anon-v1.00.manifest.xml” for Windows.

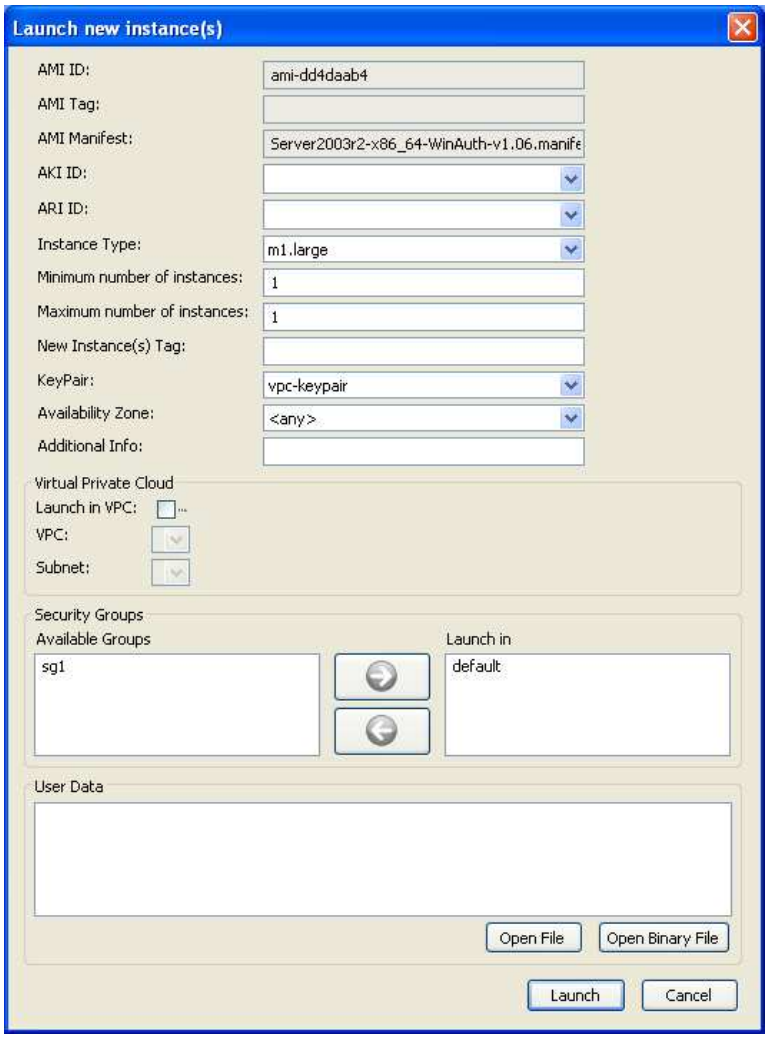
Step 3: Launching an Instance

Once you have the AMI selected, you can easily launch an instance through Elasticfox, by performing the following:

1. Right click on the selected AMI and click on the “Launch Instance(s) of this AMI”.

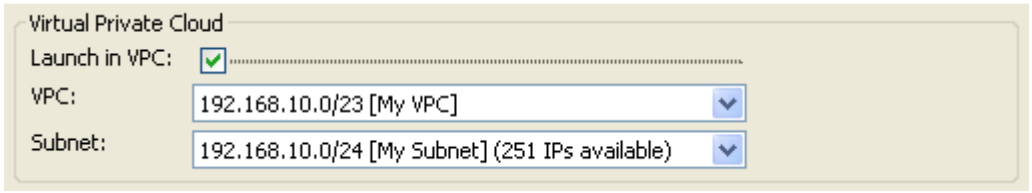


2. In the KeyPair section of the pop-up box, select the KeyPair you created in the setup section. This will associate your security KeyPair with an instance, so that you can connect to it.



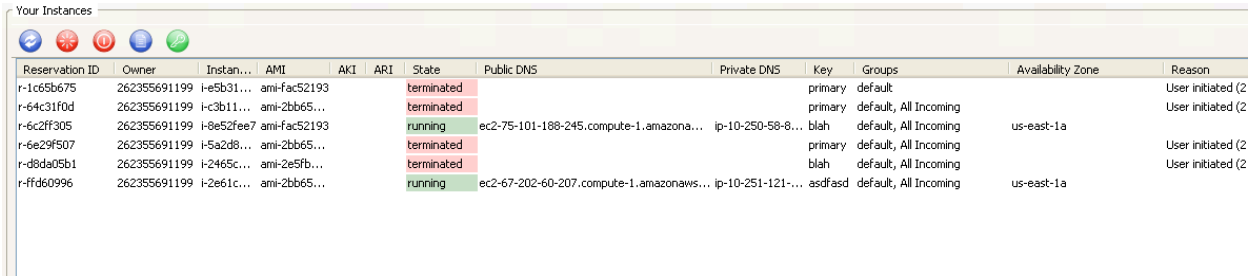
3. In the Security Groups section, select the appropriate group and click on the right arrow to move it into the Launch in box.

Note: You cannot assign a security group to an instance if the VPC checkbox is selected. Instead, select the VPC and Subnet that you would like the launch the instance in. You will not be able to launch an instance within VPC until you have created a VPC and at least one Subnet. If you want to launch an instance within a VPC, please skip to tutorial 5 and then return here.

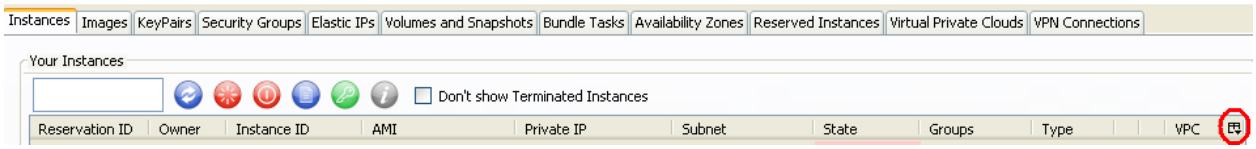


4. Click the “Launch” button.

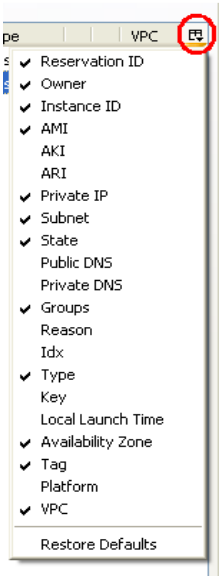
5. The instance will show up in the “Your Instances” section of the “AMIs and Instances” tab in the “pending” state. Click the refresh button in the “Your Instances” section after about a minute or two to ensure it reaches the “running” state. If you are running a Linux/UNIX instance, it will be ready to use. If you are using Windows, please right click on the instance, and select “Show Console Output”. When the text “Windows is ready to use” appears, your instance is ready to use!



Note: There are additional options available when launching an instance. These additional options are covered in the Advanced Features section below.



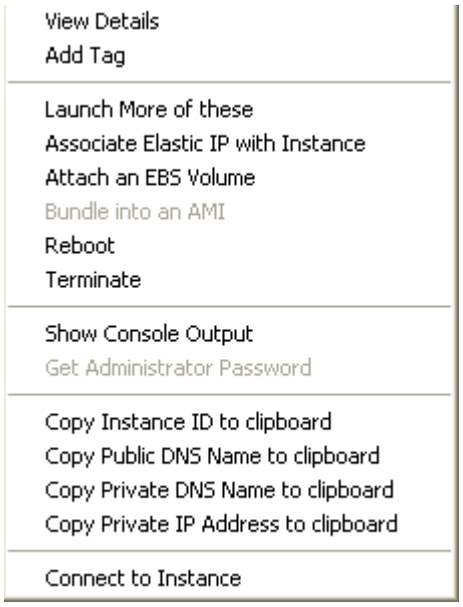
Note: When viewing instances on the Instances tab, you can change the columns that Elasticfox displays. To display these fields, click on button circled in red above. You can also change the order of the columns to better suite your needs by dragging a column to your desired location or order.



Step 4: Connecting to the Instance

To connect to an instance, simply perform the following steps:

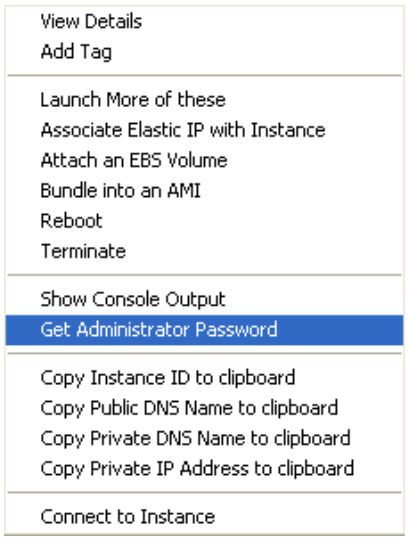
1. Right click on the instance you want to connect to, and select the “Connect to Instance”.



2. If it is a Linux/UNIX instance, an ssh connection will be established with the instance. Since you provided the ssh key, it will automatically log you in as root.

   If this is Windows, then it will launch a Remote Desktop (RDP) session. To login, you may need to type “Administrator” as the username and provide the automatically generated Windows password. The Windows password can be retrieved by right clicking on the instance in Firefox and clicking “Get Administrator Password”.

Note: If your security group doesn’t allow access to the RDP or SSH port, Elasticfox will prompt you to open the port for the host you are connecting from.



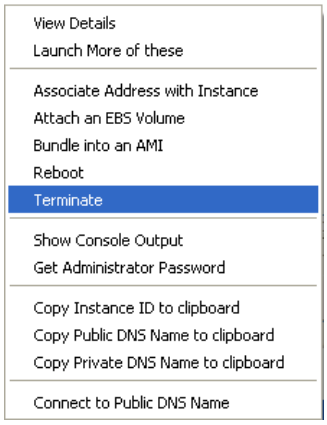
VPC **Note:** Elasticfox will automatically use the private IP address rather than the public DNS name of your instance to connect via SSH or RDP if your instance has a subnet assigned. The computer that you are running Elasticfox on must have IP connectivity via a VPN connection to your VPC to be able to connect to the instance.

3. At this point, you have now successfully gained access to your new instance!

Cleaning Up: Terminating your Instance

When you are done with your instance, you can simply terminate it by:

1. On the "AMIs and Instances" tab, right click on the instance you want to terminate in "Your Instances" section and select "Terminate".



2. Press the refresh button  in the "Your Instances" box to ensure that the state changes to "Terminated".

Advanced Topics

It is possible to launch an instance with additional options, enabling you to better control the type of server instance you are launching or where the instance will launch. Recall that to launch an instance, we had a particular AMI selected in Elasticfox, and then right clicked on the selected AMI choosing the "Launch Instance(s) of this AMI" option from the menu that appeared. Previously, when you launched your instance you utilized the security group and KeyPair functionality. There are several optional fields that you can use to customize our instance launch, including:

Instance Type

The instance types described different configurations of CPU, memory, and ephemeral storage capacity. An example instance type is the small, which has 1.7 GB of RAM, 160 GB of storage, and roughly 1 EC2 Compute Unit (1 virtual core with 1 EC2 Compute Unit). For more detail about the available instances types, please see: http://aws.amazon.com/ec2.

Availability Zone

Amazon EC2 provides the ability to place instances in multiple locations. Amazon EC2 locations are composed of availability zones and regions. Availability zones are distinct locations that are engineered to be insulated from failures in other availability zones and provide inexpensive, low latency network connectivity to other availability zones in the same region. Regions consist of one or more availability zones. By launching instances in separate availability zones, you can protect your applications from the failure of a single location.

Minimum/Maximum Number of Instances

This functionality provides you with a way asking Amazon EC2 for a specific range of instances. Amazon EC2 will try to provide you with the maximum number of instances possible within your range. If you cannot get the minimum number of instances, then you will not launch any instances.

Tutorial #2: Bundling an Instance into an AMI

Goal

The goal of this tutorial is to bundle an instance into an AMI. This is helpful so that you can customize an instance with any software or changes you may need to make. Then, at a later point you can launch one or more copies of the AMI.

Core Concepts

The sections below outline the core concepts used in this tutorial.

S3 Bucket

S3 is a persistent data store that enables you to store objects, like an AMI. The bucket is similar to a folder on a file system so that you can keep your objects organized. The bucket name though is unique across all S3 users.

Bundling

Bundling is a method of taking a snapshot of the file system, so you can later boot from it. You can make a new AMI by modifying and extending an existing image (such as the one you just booted and logged onto in Tutorial #1), and then bundling it to use later.

Windows Operating Systems

Step 1: Make any Modifications

The first step in creating any AMI is to make any modifications to your running instance. To create a running instance, please follow the steps provided in the tutorial #1. For the purposes of this tutorial, please just add a file named test.txt to your "c:\" directory. Once you have added this file, please proceed to the next step.

We also suggest that you perform the following steps to reduce your startup time, by clearing up any temporary files on your instance, defragmenting your system, and explicitly "zeroing" out your free space using the 'sdelete' command. Your startup time is proportional to the size of your AMI.

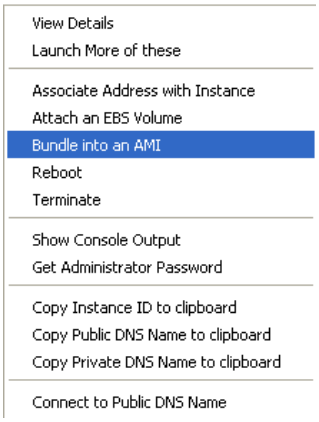
- We recommend using the Disk Cleanup tool to remove unneeded temporary files from your instance, since it provides easy-to-use wizards that remove the files for you. To access the Disk Cleanup tool, click Start, click Run, and then type "Cleanmgr.exe".
- To defragment your machine, we recommend the Disk Defragmenter utility included with Microsoft Windows. To access that tool you can click Start, click All Programs, click Accessories, click System Tools, click Disk Defragmenter.

To "zero" out your free space, you can simply use the "sdelete –c C:\" command. For full details on how to use the sdelete command, please see http://technet.microsoft.com/en-us/sysinternals/bb897443.aspx.

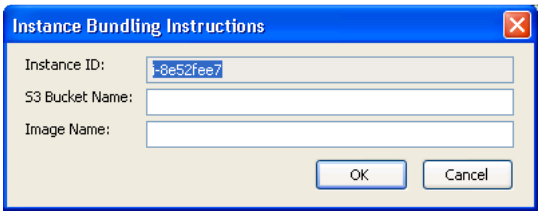
Step 2: Bundle the Image

Once your modifications have been made to a running instance, you can bundle your instance into an AMI. This will automatically shut down your instance, take a snapshot, and restart it for you. To take the snapshot:

1. Launch Elasticfox by clicking on the "Tools" menu in Firefox, and selecting Elasticfox.
2. Click on the "AMIs and Instances" tab.
3. Refresh the "Your Instances" box by clicking on the  button. This will ensure you have the most up to date list of instances shown on your screen.
4. Right click on the instance to bundle, and select "Bundle into an AMI".



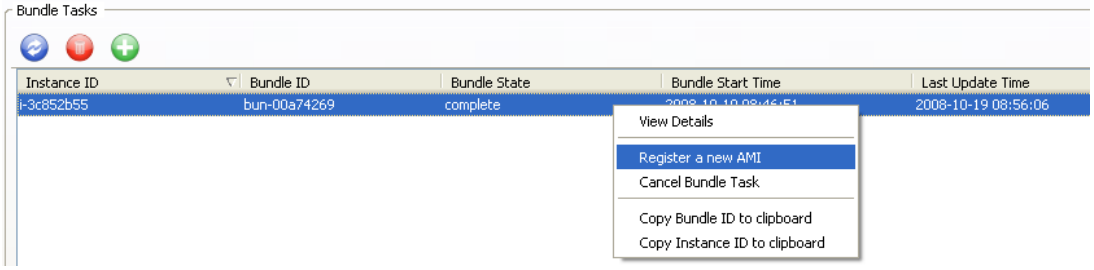
5. Enter in a S3 bucket name to store the AMI in and a name for the image, then click "OK". Please ensure that the bucket name has no upper-case characters in it. Assuming you have entered a valid bucket and image name, this will cause you to be switched to the "Bundle Tasks" tab where it will show you the status of the bundling process.



Step 3: Register the Image

Once the image has reached the "completed" state in the "Bundle Tasks" tab, you just need to register the AMI to make it available for you to use. To do this:

1. Ensure you are on the "Bundle Tasks" tab, by clicking on the "Bundle Tasks" tab.
2. Right click on the bundle to register, and select "Register a new AMI". If successful, this will take you back to the "AMIs and Instances" page and select the newly created AMI. Now you can launch that instance if you need.



Linux/UNIX Instance

Bundling a Linux/UNIX instance requires the use of the AMI tools, and differs from Windows in that the bundling is performed from within the running EC2 instance. (As described above, you need to bundle Windows from outside the actual EC2 instance). Since this Getting Started Guide is focused on Elasticfox, it is outside the scope of the tutorial. For more detail on how to perform these steps, please see the Amazon EC2 API Tools Getting Started Guide at http://docs.amazonwebservices.com/AWSEC2/2008-05-05/GettingStartedGuide.

Tutorial #3: Creating an Elastic Block Store (EBS) Volume

Goal

The goal of this tutorial is to create a new EBS volume and attach it to your running EC2 instance.

Core Concepts

Amazon Elastic Block Store (EBS)

Amazon Elastic Block Store (EBS) provides block level storage volumes for use with Amazon EC2 instances. It provides highly available, highly reliable storage volumes that can be attached to a running Amazon EC2 instance and exposed as a device within the instance.

Amazon EBS Volume

Amazon EBS volumes are off-instance storage that persists independently from the life of an instance. You can create storage volumes from 1 GB to 1 TB that can be mounted as devices by Amazon EC2 instances. Multiple volumes can be mounted to the same instance. Amazon EBS volumes are placed in a specific Availability Zone, and can then be attached to instances also in that same Availability Zone. Each storage volume is automatically replicated within the same Availability Zone. This prevents data loss due to failure of any single hardware component.

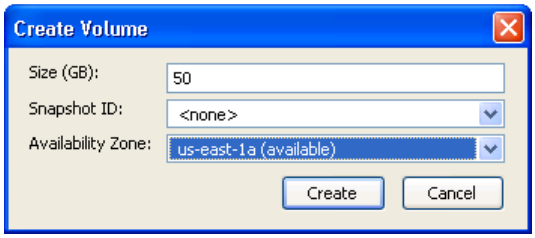
Amazon EBS Snapshot

Amazon EBS also provides the ability to create point-in-time snapshots of volumes, which are persisted to Amazon S3. These snapshots can be used as the starting point for new Amazon EBS volumes, and protect data for long-term durability. The same snapshot can be used to instantiate as many volumes as you wish.

Step 1: Create a New Amazon EBS Volume

To create a new Amazon EBS Volume, please perform the following steps:

1. Click on the “Volumes and Snapshots” tab in Elasticfox.
2. Press the green  symbol in the “Volumes” box.
3. Type in the size in gigabytes (GB) of the volume you would like between 1 and 1000. For the purposes of this demo, please use “50” to specify a 50 GB drive.



Note: A volume must be in the same availability zone as an instance. You can optionally specify an Availability Zone if desired or the snapshot id to create a volume from. If you accidentally create a volume in the wrong zone, you can either create a new blank volume in the proper zone, or create a new volume based on a snapshot of a volume in another zone.

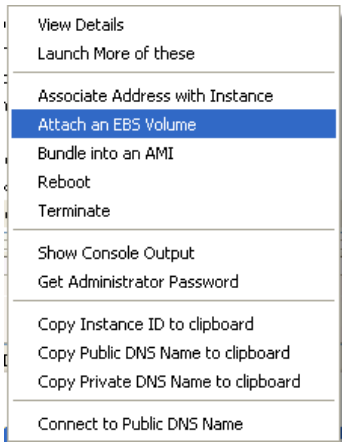
4. Click the OK button, and your Amazon EBS volume will be created. Take note of the volume id of the Amazon EBS volume you just created, because we will use it later.

Step 2: Attach the Amazon EBS Volume with an Instance

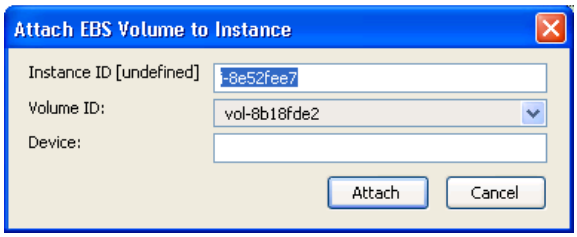
If you do not have an instance running, please start one as defined in Tutorial #1. Once you have created the EBS volume, you can attach it to one of the instances by performing the following steps:

1. Click on the "AMIs and Instances" tab.

2. Right click on the instance you want to associate the EBS volume with, and select the "Attach an EBS volume". A dialog box will appear.



3. Select the Amazon EBS volume that you created earlier from the drop down box.



4. In the "device" box, you will need to input the device you would like to attach to the volume.

   The device must be in the format of "/dev/sdh" for Linux/UNIX. The device is automatically selected for Windows (in most cases, the Device field is disabled and displays the text "windows_device"). Linux/UNIX instances currently support devices "sdf" to "sdh". Any device

that is not reserved can be attached to an Amazon EBS volume. For a list of devices that are reserved by the instance stores, see Instance Storage in the developer guide.

5. Click OK when completed. This will attach the new Amazon EBS volume to your specified instance.

Step 3: Formatting an Amazon EBS Volume

Windows

To format a volume for Amazon EC2 running Windows, please perform the following steps.

1. Log in to your instance using Remote Desktop.
2. Select Start and click Run.
3. Type diskmgmt.msc and click OK. The Disk Management utility opens.
4. Right-click the Amazon EBS volume, select Initialize, and follow the on-screen prompts.

Linux/UNIX

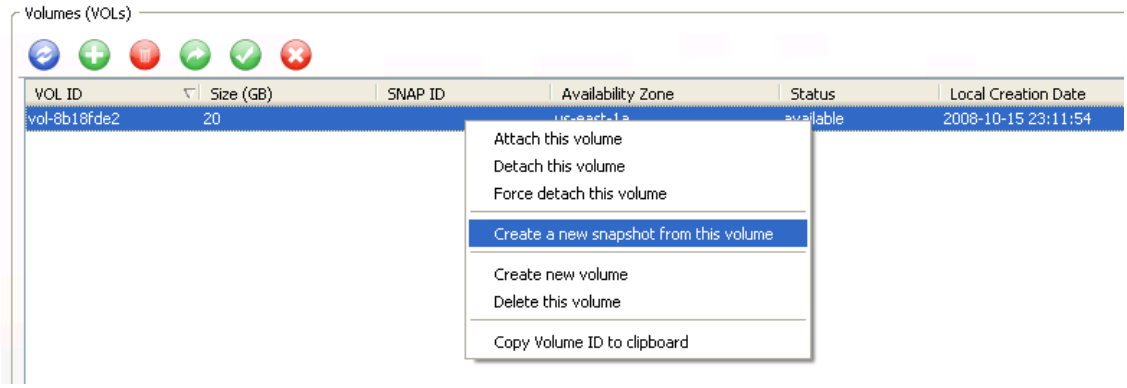
To format your volume for Amazon EC2 running Linux/UNIX, please perform the following steps.

1. Log into your instance using ssh.
2. Use the mk2fs tool to format the EBS volume.

Step 4: Taking a Amazon EBS Volume Snapshot

Once you have formatted a volume and made any necessary changes, you can take a snapshot of the volume so that you have a point in time record of the block storage. The snapshot occurs asynchronously and the volume's status indicates "pending" until it completes. To complete this snapshot, please perform the following steps:

1. Click on the “AMIs and Instances” tab.
2. Determine the instance that you would like to take a snapshot of, and record the instance id.
3. Click on the “Volumes and Snapshots” tab.
4. Right click on the EBS volume that corresponds to the device and instance id you recorded, and select “Create a new snapshot from this volume”. This will kick off a snapshot task, which will go to “completed” status when done. You may need to click the refresh button to get an updated status.



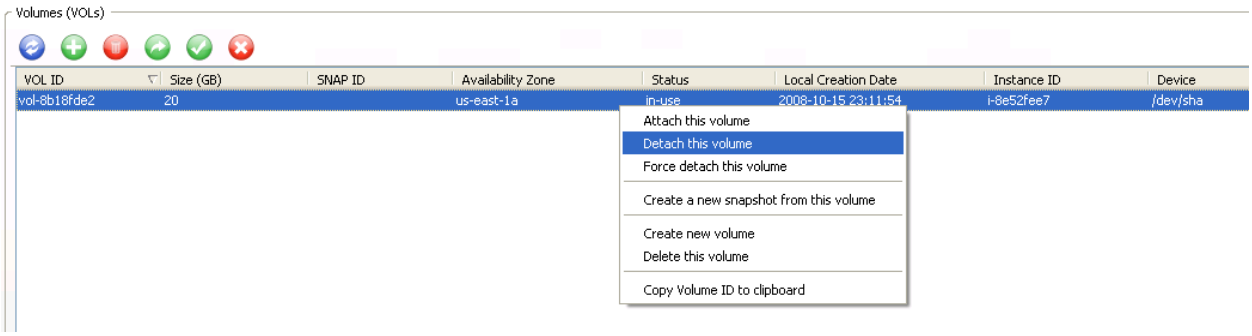
Clean-up

To ensure that you remove any components created from this tutorial, please shutdown any instances as defined in Tutorial #1 and perform the following two steps.

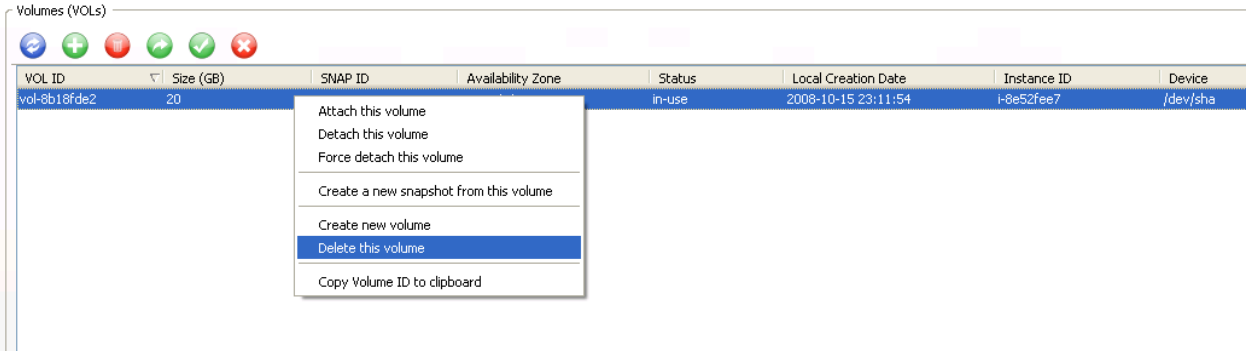
Step 1: Detaching and Deleting the EBS Volume

Once you have completed the tutorial you will want to detach and your volume from your EC2 instance. To accomplish this, please perform the following steps:

1. Click on the "Volumes and Snapshots" tab.
2. Right click on the Amazon EBS volume that you want to detach, and select the "Detach this volume" option. This will disassociate the Amazon EBS volume from the instance.



3. Click OK on the dialog box that will emerge to confirm that the instance is to be detached.
4. Right click on the Amazon EBS volume that you want to delete, and select the "Delete this volume" option. This will delete the Amazon EBS volume.



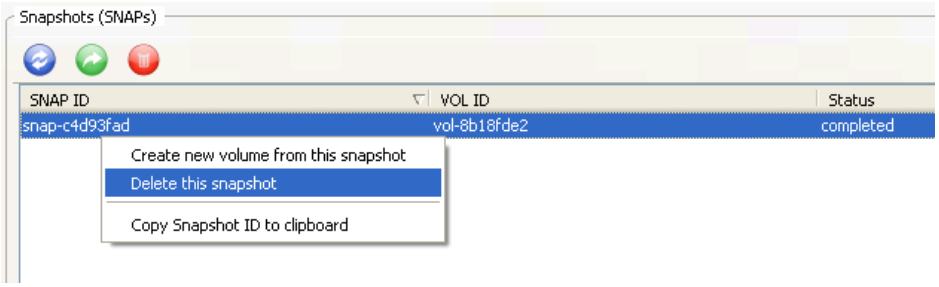
5. Click OK on the dialog box that will emerge to confirm the destruction of the Amazon EBS volume. This will stop the billing for the Amazon EBS volume.

Step 2: Deleting any EBS Snapshots

To delete the Amazon EBS snapshot, please perform the following steps:

1. Click on the "Volumes and Snapshots" tab.

2. Right click on the snapshot you would like to delete, and select "Delete this snapshot".



3. Click the OK in the confirmation box, and this will delete your Amazon EBS snapshot.

Tutorial #4: Associating an Elastic IP (EIP) with an instance

Goal

The goal of this tutorial is to create a new elastic IP (EIP) and map it to an instance. Elastic IPs are important to provide a static IP associated with an EC2 instance.

Core Concepts

Elastic IP (EIP)

Elastic IP addresses are static IP addresses designed for dynamic cloud computing. Elastic IP addresses are associated with your account, not specific instances. Any elastic IP addresses that you associate with your account remain associated with your account until you explicitly release them. Unlike traditional static IP addresses, however, elastic IP addresses allow you to mask instance or availability zone failures by rapidly remapping your public IP addresses to any instance in your account. You can only associate one elastic IP address with one instance at a time.

Step 1: Creating a new EIP

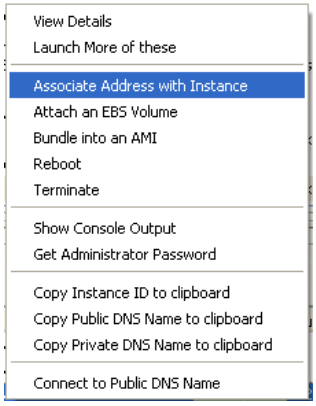
To create an EIP, simply perform the following steps:

1. Click on the "Elastic IPs" tab.
2. Press the refresh button  to update the page with the latest EIPs.
3. Click on the green  icon. This will add a new Elastic IP. Take note of this Elastic IP, because you will use it later.

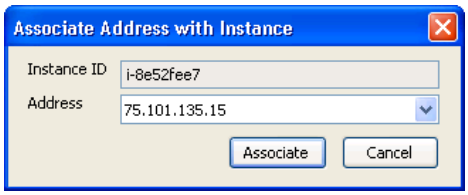
Step 2: Associating the EIP with a new instance

If you do not have an instance running, please start one as outlined in Tutorial #1. Once you have created an EIP, you will want to associate the IP with an instance. To accomplish this, please perform the following steps:

1. Click on the "AMIs and Instances" tab.
2. Right click on the instance you want to associate the EIP with, and select "Associate Address with Instance".



3. Choose the EIP address from the drop down list and click “Associate”. This will associate the EIP with the instance.

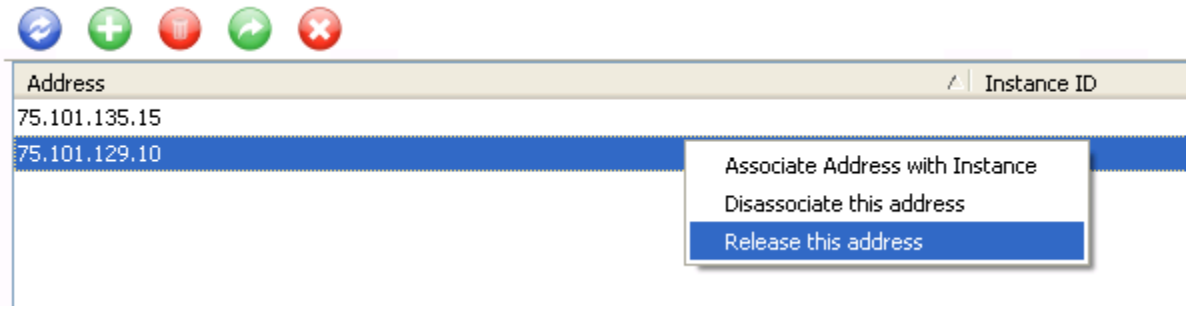


VPC Note: You cannot currently use Elastic IP addresses with Amazon VPC

Clean-up

To ensure that you remove any components created from this tutorial, please shutdown any instances as defined in Tutorial #1 and perform the following steps:

1. Right click on the “Elastic IPs” tab, and select “Release this address”.



2. Click OK in the dialog box to confirm the release of the EIP. This will relinquish your IP address, so that it can be reclaimed by any other customer.

Tutorial #5: Amazon Virtual Private Cloud (Amazon VPC)

About Amazon VPC

Amazon Virtual Private Cloud (Amazon VPC) enables a secure and seamless bridge between a company's existing IT infrastructure and the AWS cloud. Amazon VPC enables enterprises to connect their existing infrastructure to a set of logically isolated AWS compute resources via a Virtual Private Network (VPN) connection, and to extend their existing management capabilities such as security services, firewalls, and intrusion detection systems to include their AWS resources.

Core Concepts

Amazon VPC is comprised of a variety of familiar objects:

- **A Virtual Private Cloud (VPC)**: a logically isolated portion of the AWS cloud. You define a VPC's IP address space from a range you select.
- **Subnet**: a segment of a VPC's IP address where you can place groups of logically isolated resources.
- **VPN Connection**: a connection between your VPC and datacenter, home network, or co-location facility.
- **VPN Gateway**: the VPC side of a VPN Connection.
- **Customer Gateway**: Your side of a VPN Connection.
- **Router**: routers interconnect subnets, and direct traffic between VPN Gateways and Subnets.

You are encouraged to review our technical documentation (see Additional References) to learn more about our system, including the APIs and VPN configuration details.

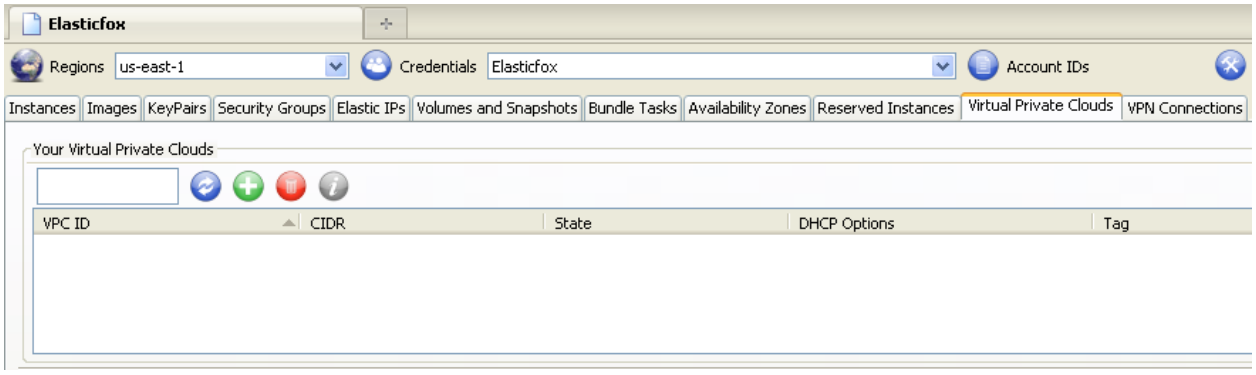
Goal

The goal of this tutorial is to:

1. Create a VPC, Subnet, VPN Gateway, Customer Gateway, and a VPN Connection.
2. Save the automatically generated VPN Connection configuration to a file.
3. Attach the VPN Gateway to your VPC
4. Configure advanced options: DHCP Option Set

Step 1: Creating a VPC

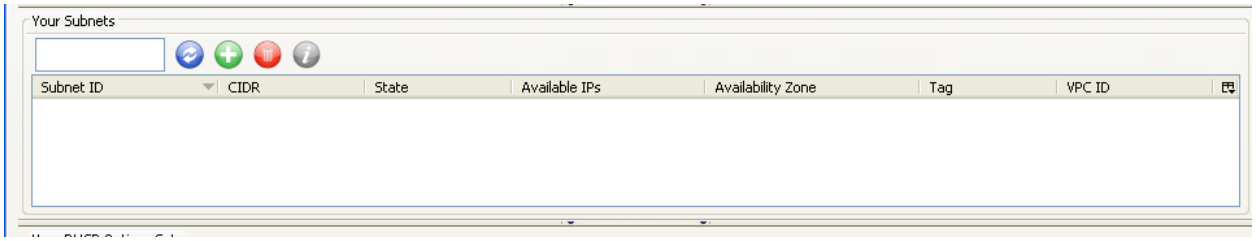
1. Click on the “Virtual Private Clouds” tab.
2. Navigate to the “Your Virtual Private Clouds” section.



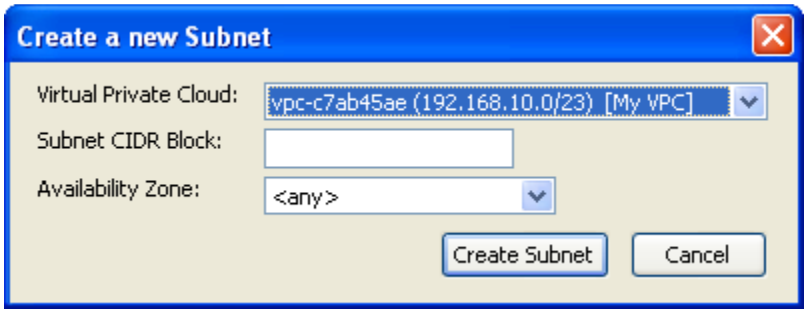
3. Click on the green  icon.
4. Specify the Classless Internet Domain Routing (CIDR) block for the VPC that you would like to create. For example, “192.168.10.0/23”
5. Click the “Create VPC” button.
6. Press the refresh button  to update the page.

Step 2: Creating a Subnet

1. Click on the “Virtual Private Clouds” tab.
2. Navigate to the “Your Subnets” section.



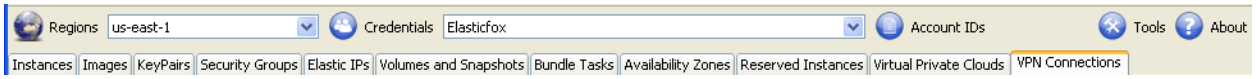
3. Click on the green  icon.

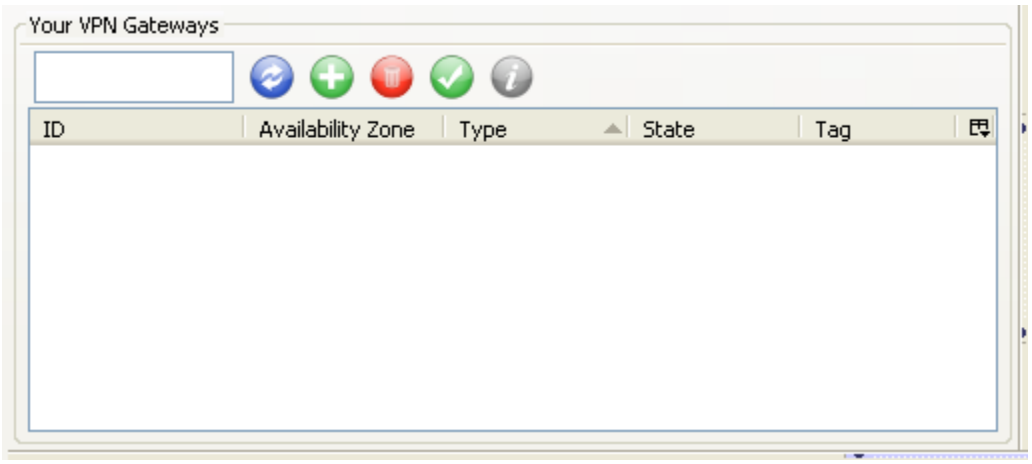


4. Using the pull-down menu, select which VPC you would like to create the Subnet in.
5. Specify the Classless Internet Domain Routing (CIDR) block for the Subnet that you would like to create. For example, “192.168.10.0/24”.
6. Specify the Availability Zone (AZ) for the Subnet that you would like to create. If you leave this option set to <any>, the system will pick an Availability Zone for you.
7. Click the “Create Subnet” button.
8. Press the refresh button  to update the page.

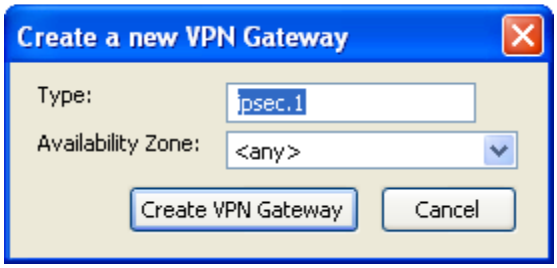
Step 3: Creating a VPN Gateway

1. Click on the “VPN Connections” tab.
2. Navigate to the “Your VPN Gateways” section.





3. Click on the green  icon.

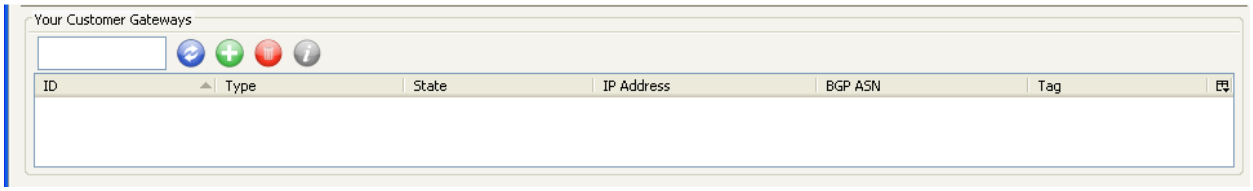


4. Specify the type of VPN Gateway you wish to create. For now the only valid option is “ipsec.1”.
5. Specify the Availability Zone (AZ) for the Subnet that you would like to create. If you leave this option set to <any>, the system will pick an Availability Zone for you.
6. Click the “Create VPN Gateway” button.
7. Press the refresh button  to update the page.

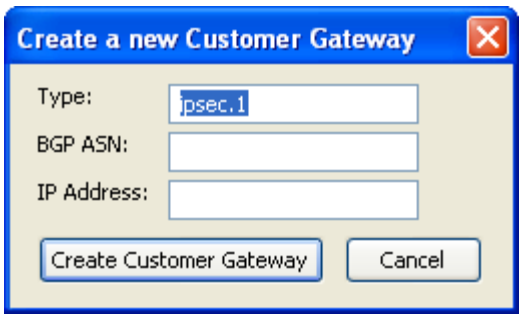
Step 4: Creating a Customer Gateway

1. Click on the “VPN Connections” tab.

2. Navigate to the “Your Customer Gateways” section.



3. Click on the green  icon.



4. Specify the type of Customer Gateway you wish to create. For now the only valid option is “ipsec.1”.

5. Specify the BGP ASN that you would like to use. For most deployments, using one of the private ASNs from the range 64512 through 65534 will be acceptable. Please see the Network Administrators Guide (linked from Additional References) for more information.

6. Specify the IP address of your Customer Gateway. This is the Internet routable IP address of the device you are using as your Customer Gateway. It must be static and cannot be behind a Network Address Translation (NAT) device. Please see the Network Administrators Guide (linked from Additional References) for more information.

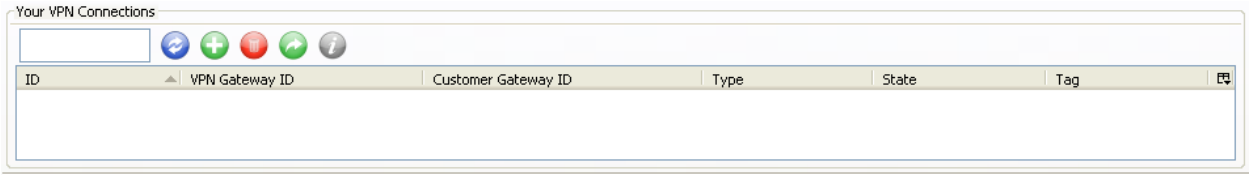
7. Click the “Create Customer Gateway” button.

8. Press the refresh button  to update the page.

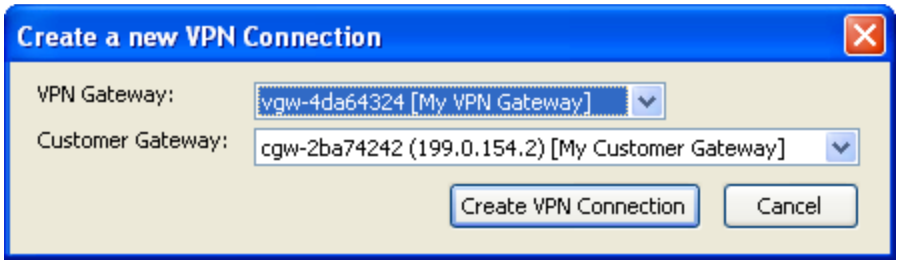
Step 5: Creating a VPN Connection

1. Click on the “VPN Connections” tab.

2. Navigate to the “Your VPN Connections” section.



3. Click on the green  icon.



4. Using the pull-down menu, select which VPN Gateway you would like to use.

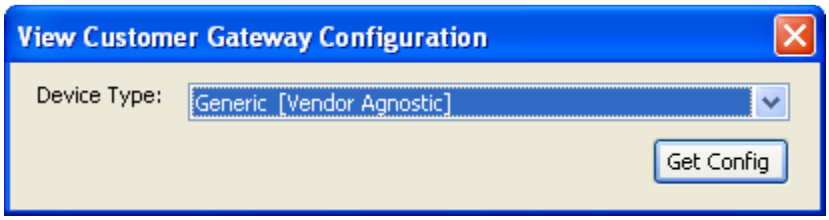
5. Using the pull-down menu, select which Customer Gateway you would like to use.

6. Click the “Create VPN Connection” button.

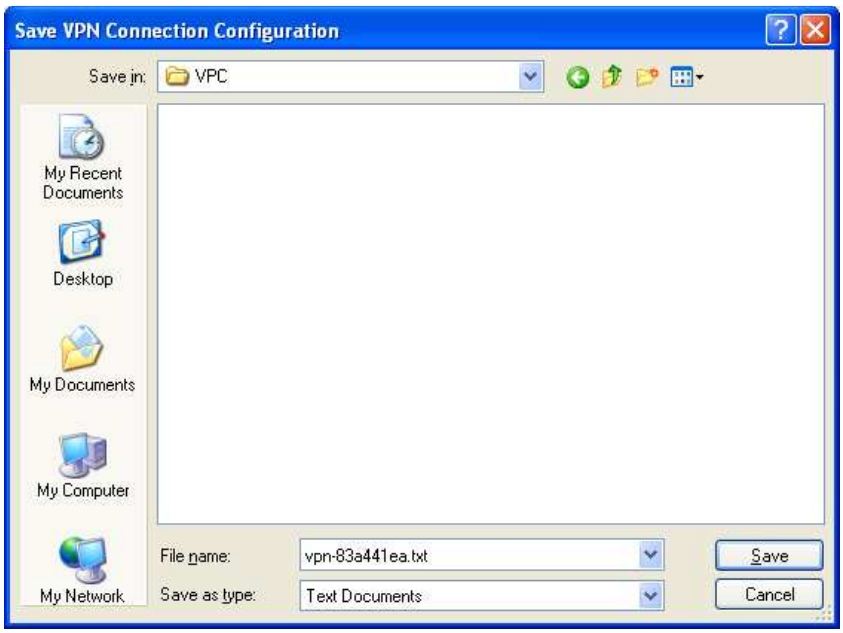
7. Press the refresh button  to update the page.

Step 6: Save the automatically generated VPN Connection configuration to a file

1. Click on the “VPN Connections” tab.
2. Navigate to the “Your VPN Connections” section.
3. Select the VPN Connection that you would like to generate the configuration for.
4. Click on the green  button.



5. Using the pull-down menu, select the device type that you are using for your Customer Gateway device. If your device is not listed, select Generic. This will result in a human-readable file that contains all the information necessary to configure any compatible device. Please check the Additional References section for more information.
6. Click the “Get Config” button.



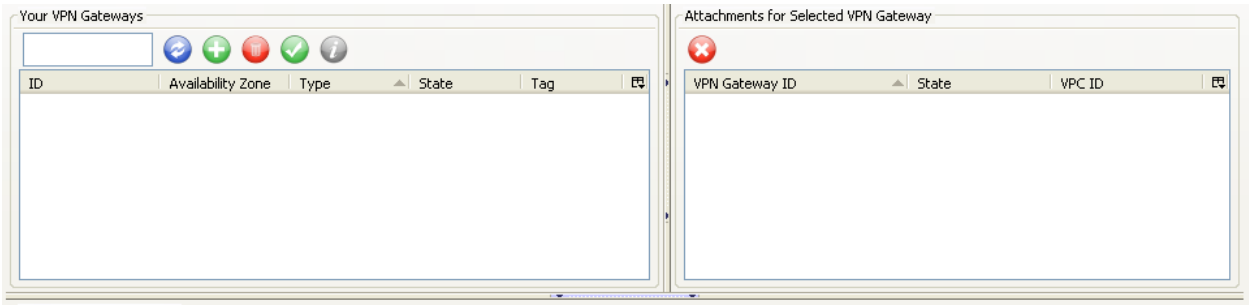
7. In the “Save VPN Connection Configuration” dialog, indicate where you would like to save the file, and the file name. By default, the file name is the ID of your VPN Connection with a .txt suffix.

8. Click “Save”.

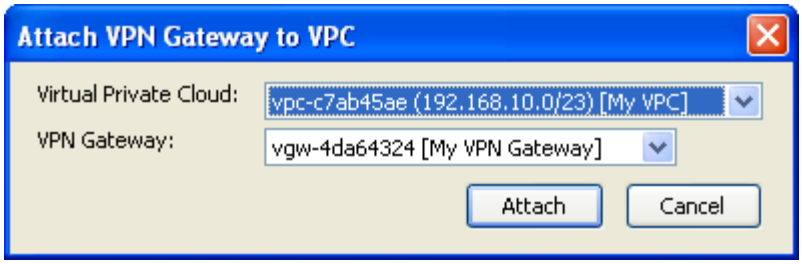
9. Review the resulting configuration file, and consult the Network Administrators Guide for more details about configuring your network device using this file.

Step 7: Attaching a VPN Gateway to a VPC

1. Click on the “VPN Connections” tab.
2. Navigate to the “Your VPN Gateways” section.



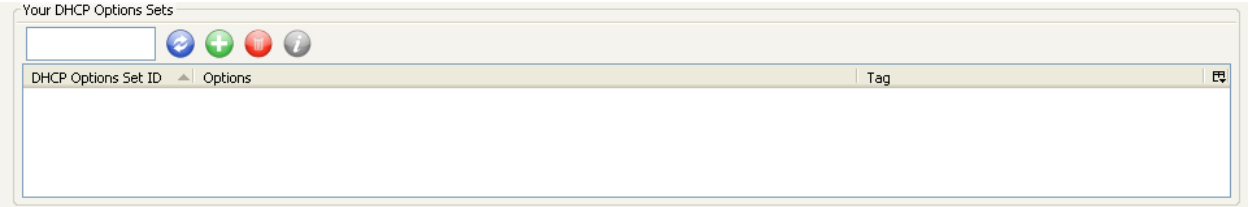
3. Click on the green  button.



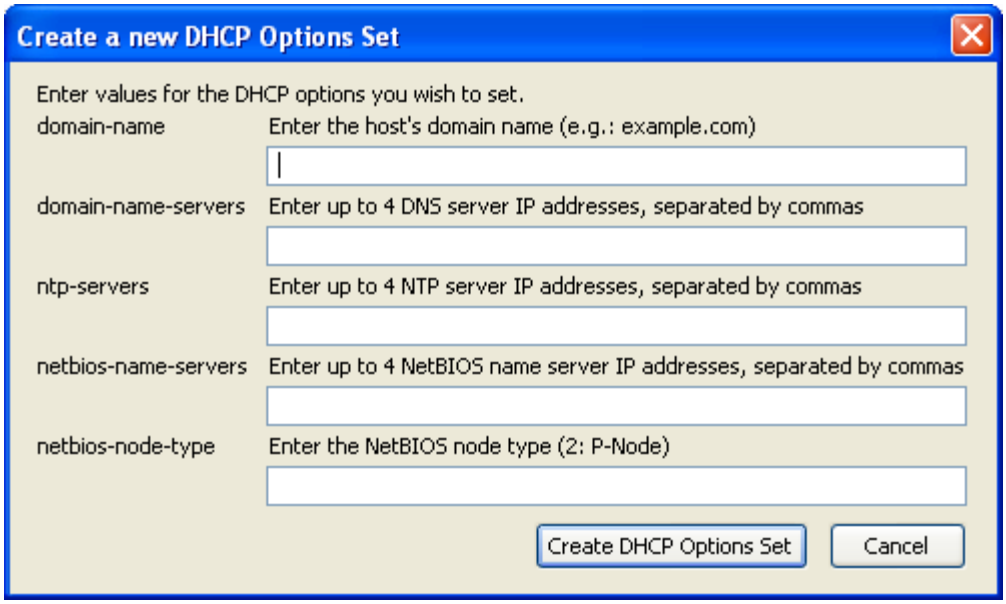
4. Using the pull-down menu, select which Virtual Private Cloudyou would like to use.
5. Using the pull-down menu, select which VPN Gateway you would like to use.
6. Click the “Attach” button.
7. Press the refresh button  to update the page.

Step 8: Advanced Options: Configure a DHCP Option Set

1. Click on the “Virtual Private Clouds” tab.
2. Navigate to the “Your DHCP Option Sets” section.



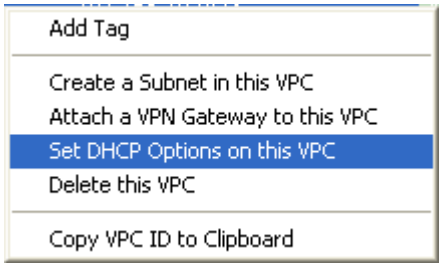
3. Click on the green  icon.



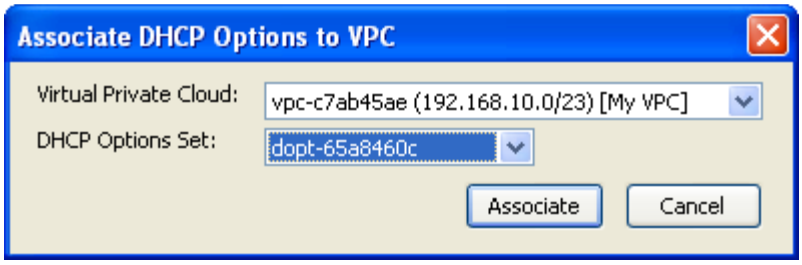
4. In the dialog box, configure one or more options. Multiple IP addresses should be separated with commas.
5. Click the “Create DHCP Option Set” button.

Step 9: Advanced Options: Associate DHCP Option Set to a VPC

1. Click on the “Virtual Private Clouds” tab.
2. Navigate to the “Your Virtual Private Clouds” section.
3. Right-Click on the VPC ID of the VPC you wish to associate a DHCP Option Set



4. Select “Set DHCP Options on this VPC.



5. Using the pull-down menu, select which DHCP Option Set you wish to use.
6. Click the “Associate” button.

Clean-up

When you are finished with this tutorial, you must terminate or delete the components that you created if you no longer wish to incur service charges. Some components have dependencies and the order in which you delete components does matter. Specifically:

- Deleting Subnets requires that you terminate all instances in that Subnet.
- Deleting VPN Gateways requires that you terminate all VPN Connections and Attachments to that VPN Gateway.
- Deleting VPCs requires that you delete all Subnets and VPN Gateway Attachments to that VPC.

In some cases, you may need to use the refresh button  to see when these components have been successfully deleted.

Additional References

The following table lists related resources that you'll find useful as you work with Amazon EC2 and Amazon VPC. These resources and more can be found at http://aws.amazon.com/resources/.

Resource	Description
Amazon EC2 Developer Guide	A comprehensive look at all of the features associated with Amazon EC2.
Amazon EC2 Getting Started Guide	A quick tutorial on how to use the command line tools for Amazon EC2. This guide also includes how to bundle an AMI on Linux/UNIX.
Amazon EC2 Feature Guide	Detailed information about each of the new features released by Amazon EC2.
Amazon EC2 Release Notes	The Release Notes give a high-level overview of the current release. They specifically note any new features, corrections, and known issues.
Amazon VPC Developer Guide	A comprehensive look at all of the features associated with Amazon VPC
Amazon VPC Getting Started Guide	A quick tutorial on how to use the command line tools for Amazon VPC.
Amazon VPC Network Administrators Guide	Detailed information written for Network Engineers or someone who is very familiar with networking concepts that concentrates on the VPN components of Amazon VPC.
Amazon VPC Release Notes	The Release Notes give a high-level overview of the current release. They specifically note any new features, corrections, and known issues.
AWS Developer Resource Center	A central starting point to find documentation, code samples, release notes, and other information to help you build innovative applications with AWS.
Discussion Forums	A community-based forum for developers to discuss technical questions related to Amazon Web Services.
AWS Support Center	The home page for AWS Technical Support, including access to our Developer Forums, Technical FAQs, Service Status page, and AWS Premium Support (if you are subscribed to this program).
AWS Premium Support Information	The primary web page for information about AWS Premium Support, a one-on-one, fast-response support channel to help you build and run applications on AWS Infrastructure Services.
E-mail address for questions related to your AWS account: <webservices@amazon.com>	This e-mail address is *only* for account questions. For technical questions, use the Discussion Forums.