|  |
| --- |
| Datasheethaeder_Overview_word.jpg |
| Astaro Security Gateway  Amazon EC2 Getting Started Guide |

January 2012  
Revision 1.02  
ASG Version 8.300  
Angelo Comazzetto  
Sr. Product Manager

Introduction

Beginning with Astaro Security Gateway V8.300, Amazon Machine Images (AMI’s) are available for Astaro Security Gateway. This brief getting started guide will show you how to create and launch an instance of Astaro Security Gateway running in the Amazon Elastic Computing Cloud (EC2). The Elastic Computing Cloud from AWS provides the ability to run virtual machines from within a scaleable, reliable cloud infrastructure. Astaro Security Gateway instances running in this environment benefit from a level of hardware infrastructure, bandwidth, and resources that most businesses cannot provide themselves.

Partners are using ASG within AWS themselves to offer demos, conduct trainings, perform testing, support customers and many other applications. In production, customers use EC2 ASG’s to connect branch offices via RED, have a robust “central” point for VPN connections, and centrally manage wireless access using Astaro Access Points plugged into deployed RED devices. There are many creative and powerful business applications – share yours on our user forums at www.astaro.org!

Usage Charges

Amazon Web Services is a separate company with their own products and pricing. Any charges you incur as a result of using AWS products are separate from any Astaro purchases and are billed from Amazon directly. All licenses and subscriptions purchased from Astaro do not include any Amazon usage entitlements.

Getting Started

Launching your Astaro Security Gateway inside the Amazon EC2 takes just minutes\*. Amazon Web Services (AWS) has many different and powerful products. To make use of their offerings, you will first need to create a free AWS account at <http://aws.amazon.com> and then sign in. Once at the Amazon Web Services console, follow the steps below to create your ASG machine.

\*This guide is intended to educate you on how to create an Astaro Security Gateway inside the Amazon Elastic Computing Cloud and does not cover how to use ASG, nor does it provide detailed training on Amazon Web Services.

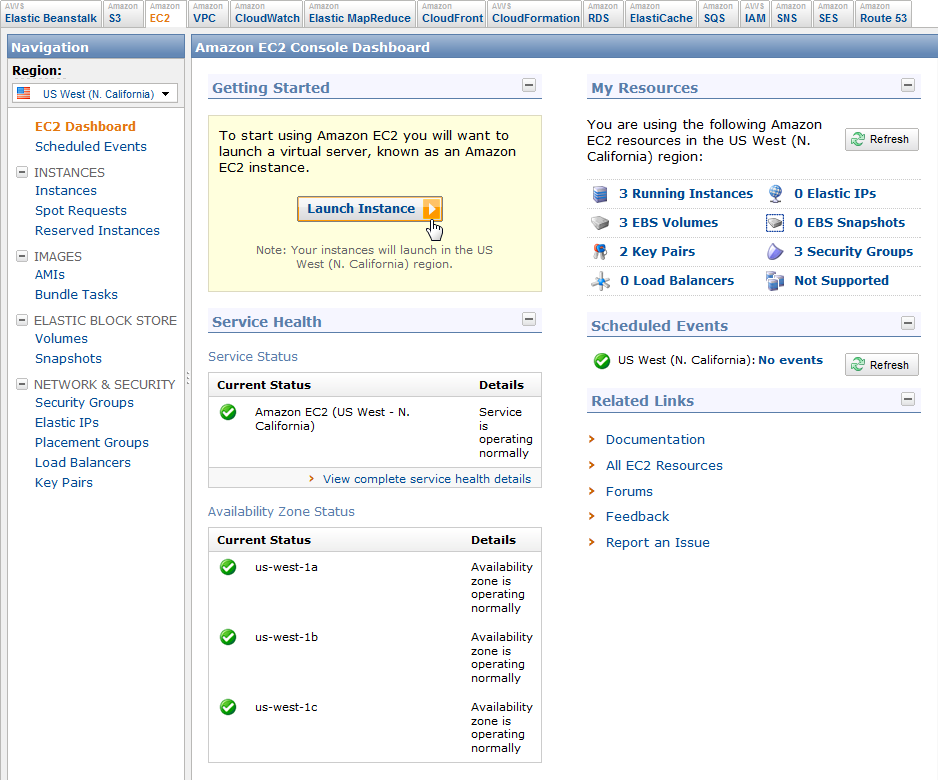
To begin, select the “EC2” tab from the AWS Console and click the “Launch Instance” button (Figure 1) to initiate the wizard.

Figure 1 - The EC2 Dashboard

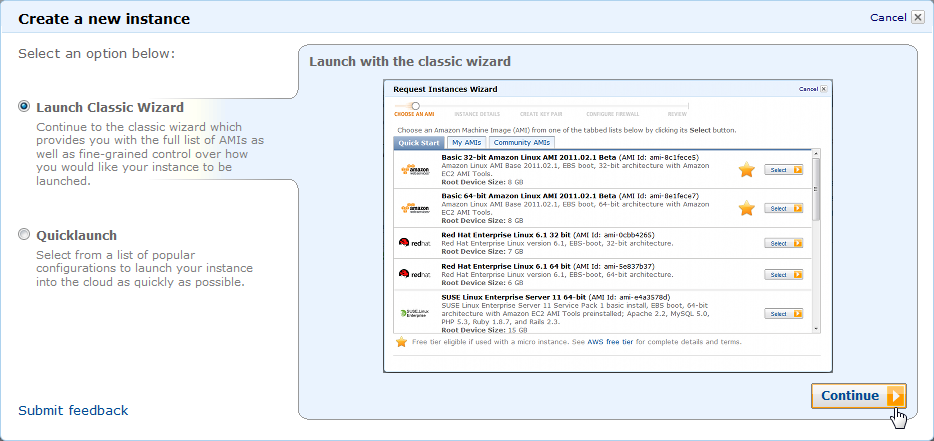
There are two wizards available – choose the “Launch Classic Wizard” option (Figure 2) so you have full control over the various choices and can receive help along the way. When you are more familiar with the process, the “Quicklaunch” option allows you to quickly launch AMI’s in a more advanced fashion.

Figure 2 - Wizard Selection

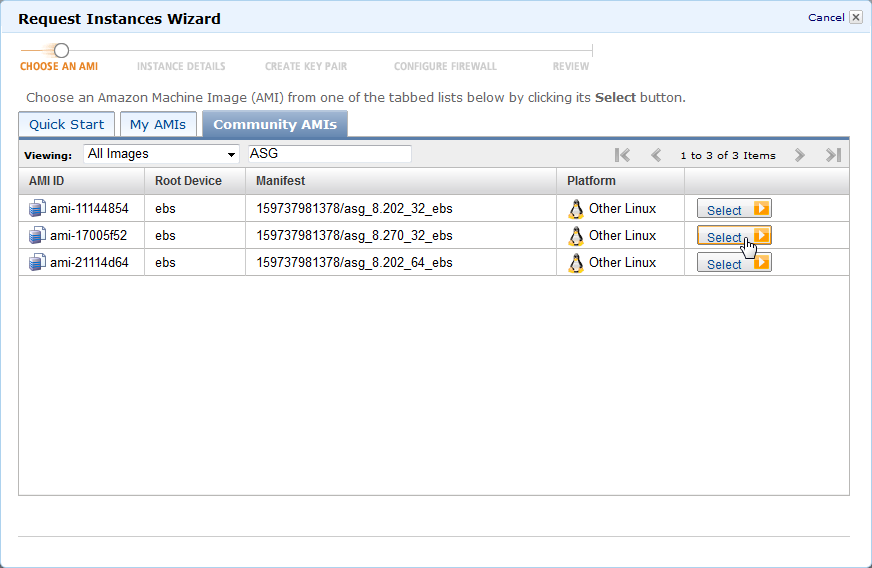
Now that the Wizard has launched, you will notice three tabs from which to pick the Amazon Machine Image you want to launch. AMI’s are specially crafted virtual machines that are designed to run in Amazon’s cloud (you cannot simply launch your own .iso from this interface), and to begin you must select the appropriate ASG AMI which has been created by our developers. To do this, select the “Community AMIs” tab, and then search for “ASG”. Choose the AMI you want to launch and click “Select” (Figure 3). Periodically, we will retire older AMIs as new versions of ASG are released (For this guide, the 8.300 AMI was selected.)

Figure 3 - AMI Search & Selection

Now you must pick the size of the instance you want to operate. AWS offers a “free” micro instance which has only ~600MB of RAM and a small CPU. It is great for testing and getting familiar with ASG in the Amazon Cloud, but the limited specifications of the instance make it a poor choice for production ASG’s. Further, the “free” nature of this instance type is limited to new customers for the first 12-months following the creation of an AWS account, and there are several usage limits to prevent abuse. You can find out more about Free Micro Instances at <http://aws.amazon.com/free/>.

For this guide, a “small” instance with 1.7GB of Memory was selected (Figure 4). Billing is never a surprise from Amazon; you can determine (in great detail if desired) the exact usage and associated costs of your AMIs from the “Account Activity”section of the AWS Dashboard.

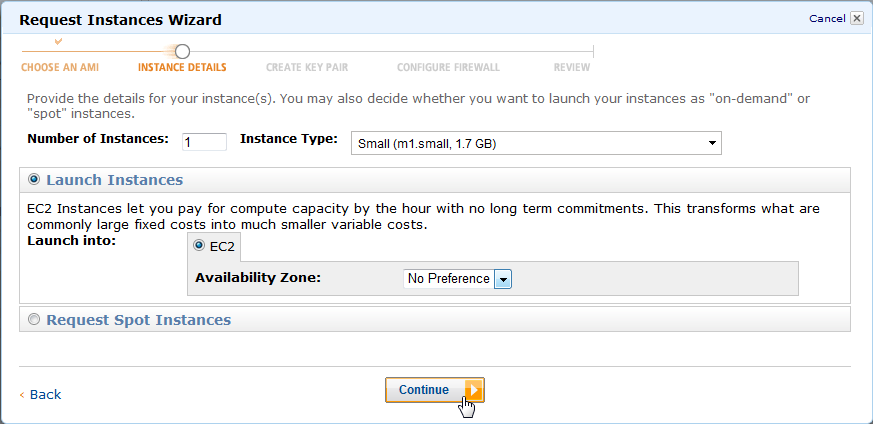
For basic users, there is no need to choose the Availablity zone during this step. When you are ready, click “Continue” to move on to the rest of the instance options.

Figure 4 - Instance Selection

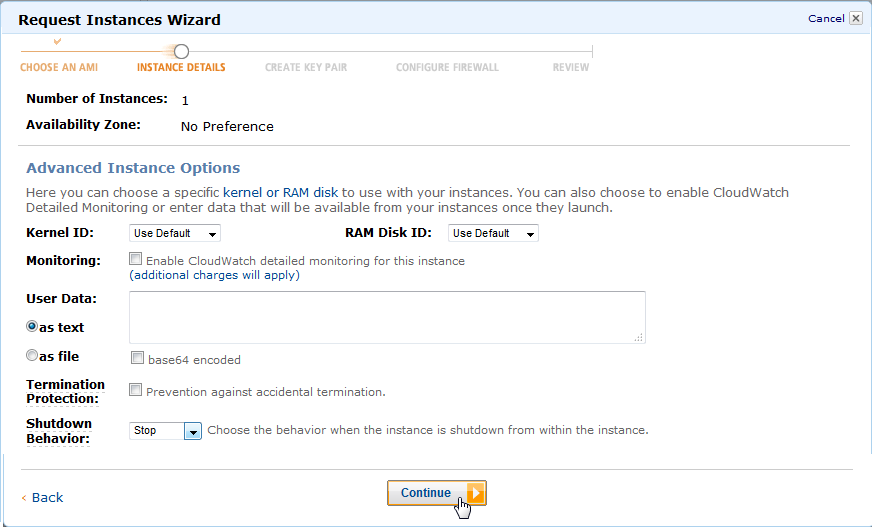
This next screen contains advanced instance options. From here you can choose how the machine should shut down, advanced Kernel and RAM Disk ID’s, and other options. For launching your ASG AMI, you do not need to adjust anything here from the defaults; simply click “Continue” (Figure 5).

Figure 5 - Advanced Instance Options

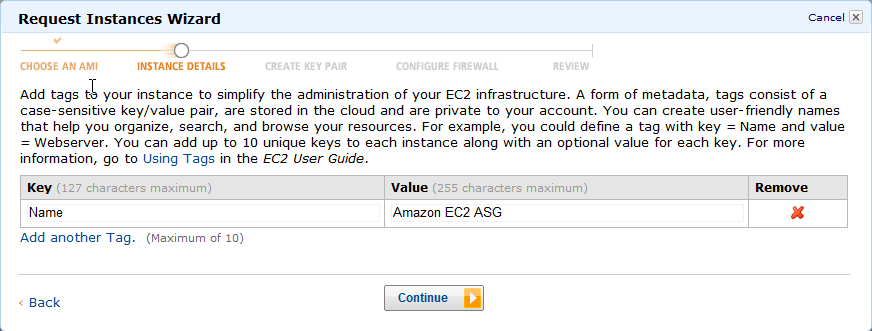
At this point you will be presented with the option to add keyword tags to your instance. These are useful when you have many AMIs for searching, filtering, and otherwise locating AMI’s in a large list. You can also customize your dashboard to include various Key columns in the overall display. For now just enter a name like “Amazon EC2 ASG” (Figure 6) and click “Continue” (you can always go back and add more Keys and their Values later).

Figure 6 - Instance Keyword Tags

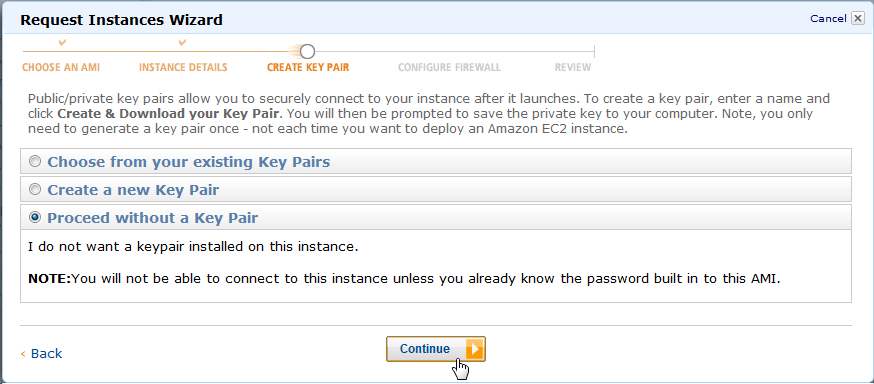
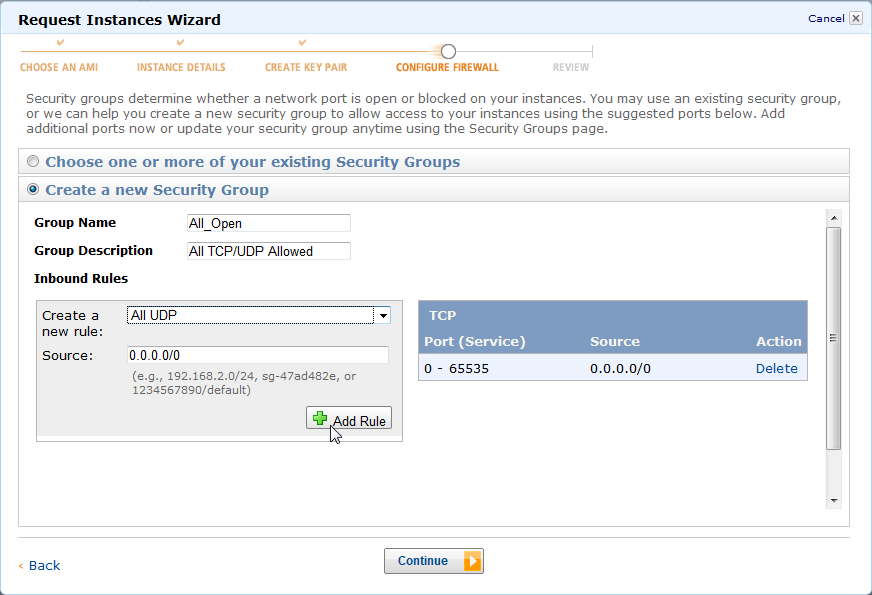
The next step involves the creation of public/private key pairs. Most often used with pure Linux AMI’s for secure command-line access, you do not need to issue and save key pairs for your ASG AMI. All configuration is done via WebAdmin, and should you need command line access at some point, you enable it from the GUI and connect via SSH using a process managed by your Astaro configuration. For this step, choose the “Proceed without a Key Pair” option (Figure 7).

Figure 7 - Key Pair Selection

Amazon Web Services offers a security firewall for your hosted AMIs. However, since ASG is itself a Network Security device, you do not need to place a “firewall in front of a firewall”. It is easy to get confused and make errors when having to consult two different sets of firewall rules. To avoid this, create a New Security Group (Figure 8) that opens all TCP and UDP ports on the Amazon firewall and places the security burden on your ASG AMI instead. This will let you then connect to WebAdmin and otherwise operate your ASG without first needing to accommodate your task in the Amazon firewall. To do this, give your new group a name, a quick description, and add rules for “All TCP” and “All UDP”, then click Continue.

Note: The Amazon firewall only controls inbound traffic – all outgoing traffic from your ASG will be permitted.

Figure 8 - Creating Open Security Group on the Amazon Firewall

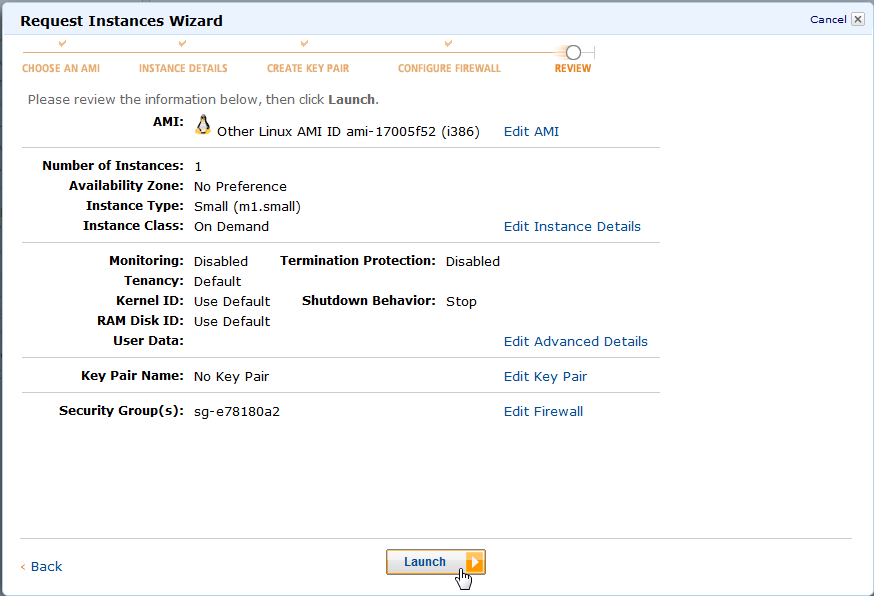
You have now progressed through the Wizard. A summary page will display the options and choices you have made so far, and give you the chance to edit things before launching your ASG AMI. The settings here can also be changed after launching the instance (Figure 9); however you will need to shut off your ASG in order to change most things. When you are ready, click “Launch” to start your cloud ASG!

Figure 9 - AMI Summary

You will be returned to the EC2 dashboard, and your Astaro Security Gateway instance will now power up. It will take a few minutes to fully start, however while you wait you can prepare to connect to the ASG WebAdmin. Select the checkbox next to your ASG instance (Figure 10) and then in the details pane note the “Public DNS” hostname assigned; this is what you will use to connect to your ASG. This hostname is static, you might consider creating a CNAME record in your company DNS for this hostname (e.g. cloudasg.mycompany.com) so that you have something easier to remember when connecting to WebAdmin.

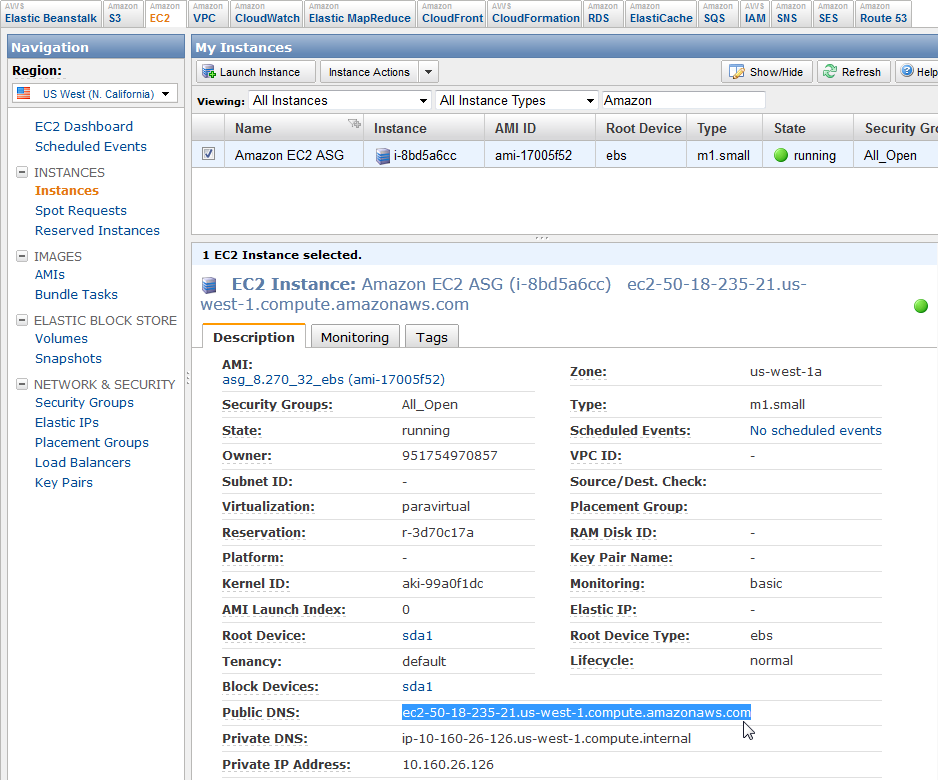


Figure 10 - ASG Instance Details

When your ASG has fully started, you will be able to connect to WebAdmin in the normal way via HTTPS in your browser on port 4444 (Figure 11). Now you can setup your ASG as you normally would by running through the setup wizard and using the default 30-day evaluation, entering a key for the free Astaro Essential Firewall, or using a purchased license. Now you can create VPN’s to other Astaro appliances, add Astaro RED devices (and Wireless Access Points connected to those!), and many other powerful things with your cloud-based ASG. Enjoy!

