Purpose

This document describes how to launch a new pre-installed Nagios Log Server server in the Amazon EC2 cloud in order to quickly run a trial of Nagios Log Server without using physical hardware, migrate existing physical installations to a cloud infrastructure, and/or scale an existing Log Server environment.

Target Audience

This document is intended for use by Nagios Log Server Administrators who would like to bring up new Nagios Log Server instances in the Amazon Elastic Compute Cloud (EC2).

Prerequisites

Before you begin, this document assumes the user has an Amazon AWS account, if not one can be obtained at http://aws.amazon.com. **Note:** The end user is responsible for all billing that results from using the Amazon Web Services.

Creating The Virtual Machine

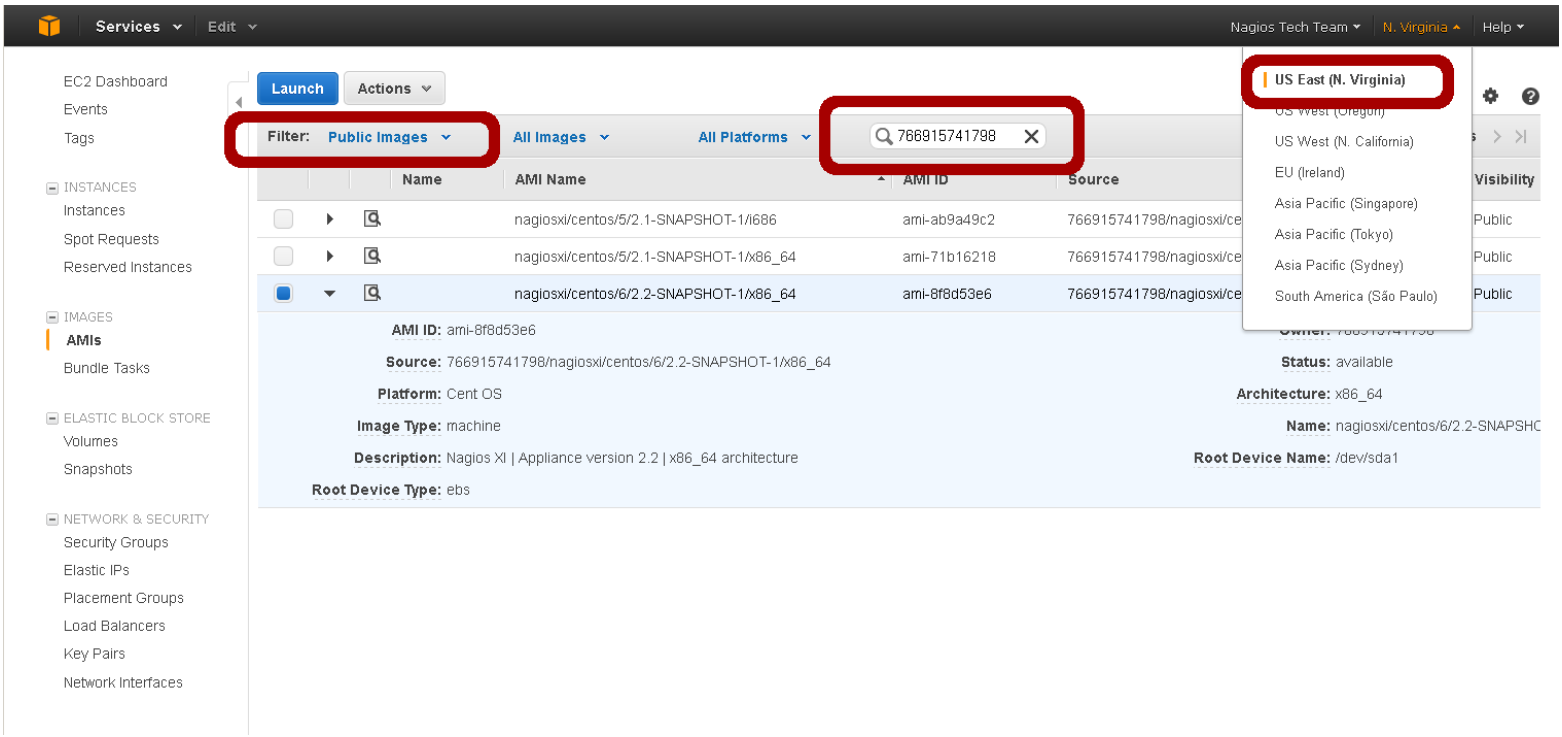
To be sure you are getting the Official Nagios Log Server public Amazon Machine Images (AMIs) it is recommended that you login to the Amazon Web Services (AWS) management console at https://console.aws.amazon.com/ec2/home?region=us-east-1#s=Images.

Images are currently available in the following zones:

- US East (N. Virginia & Ohio), US West (N. California & Oregon)
- Canada (Central)
- EU (Frankfurt, Ireland, London)
- Asia Pacific (Mumbai, Seoul, Singapore, Sydney, Tokyo)
- S. America (Sao Paulo)

Making sure you are using the appropriate region and have the filter set to: Public Images.

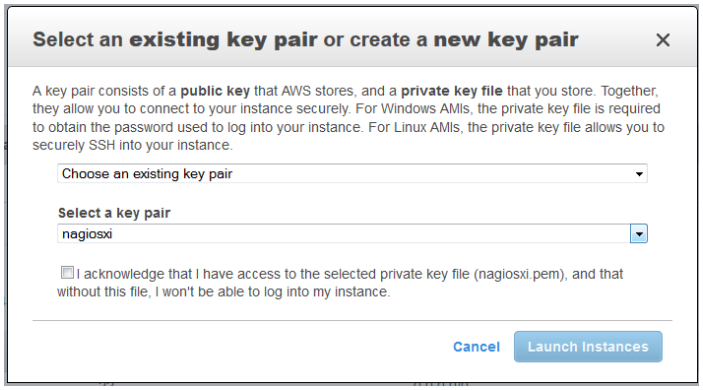
In the search bar, enter: **766915741798**, this is the Nagios Tech Team official ID. From here you can select the image that meets your needs and click **Launch**.



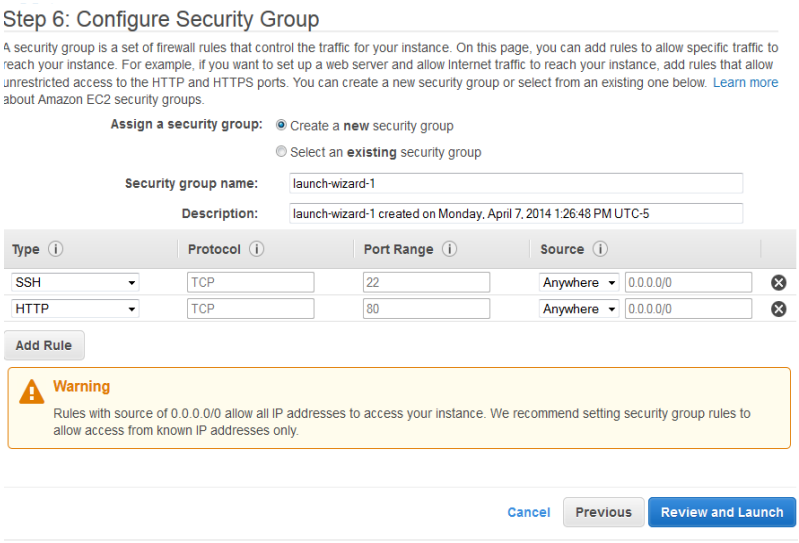
Next, the Request Instance Wizard will begin. Within the wizard you will be able to select your instance type and customize the allocated resource settings and naming information. For Nagios Log Server, the minimum specifications we recommend are 2 cores and 4GB RAM.

The wizard will have you choose, or create a key pair. If you are creating a key pair for the first time, you will be asked to download the key before continuing. The private key will be required to SSH into your machine.

Note: root password login is disabled.



Additionally you will be asked to select or configure a Security Group. The Security Group should allow public access on port `22` and port `80`. This may be fine for some installations, however keep in mind that you will also require the use of additional ports that you will be sending your log data to. These by default are `2056`, `2057`, `3515`, `5544`.



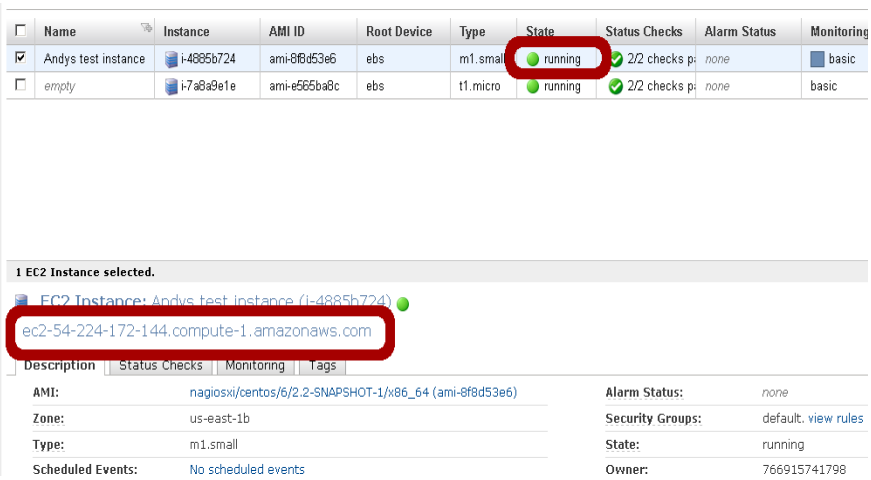
Note: When you first start your instance, the latest version of Nagios Log Server is installed and compiled at boot. This will take at least 15 minutes before the instance will become available. The amount of time will depend on the instance size you create.

Connecting To Nagios Log Server

Once the instance is running, you can complete the installation of Nagios Log Server through the web interface. To access Log Server, type in the following URL:

`http://<ipaddress>/nagioslogserver`

(where `<ipaddress>` is the IP address of the virtual machine)



Note: You can find the Public DNS address by selecting the instance and viewing the details.

Once you access the login screen, you can log in as the Admin to begin using Log Server. The credentials are listed below.

Username: `nagiosadmin`
Password: *`random`* (this gets initialized during setup)

You may also need to occasionally make an SSH connection to your machine. This connection must use the private key you downloaded earlier. When connecting you must use the username **`centos`**, NOT `root`. This user has full sudo access. Here is an example of how to establish an SSH session using this key from a terminal session in Linux:

```
ssh -i .ssh/mykey.pem centos@<ipaddress>
```

If you are using an SSH client like PuTTY, you may need to use the PuTTYgen app that allows you to convert the key to be used with PuTTY.

Note About System Credentials

You are strongly advised to change these initial passwords immediately as they are not secure and are shipped as the default passwords as other Log Server virtual machines. If you forget these passwords, we can't help recover them, so keep track of the new credentials you choose.

Troubleshooting Tip

If you are having trouble with the configuration, make sure that your security group in Amazon EC2 includes information regarding Email. Outbound email may not work if the AMI doesn't have a valid DNS name, or your firewall rules don't allow outbound SMTP except through a proxy.

Finishing Up

This completes the documentation on how to create a Nagios Log Server instance in the Amazon EC2 Cloud Environment.

If you have additional questions or other support related questions, please visit us at our Nagios Support Forums:

https://support.nagios.com/forum

The Nagios Support Knowledgebase is also a great support resource:

https://support.nagios.com/kb