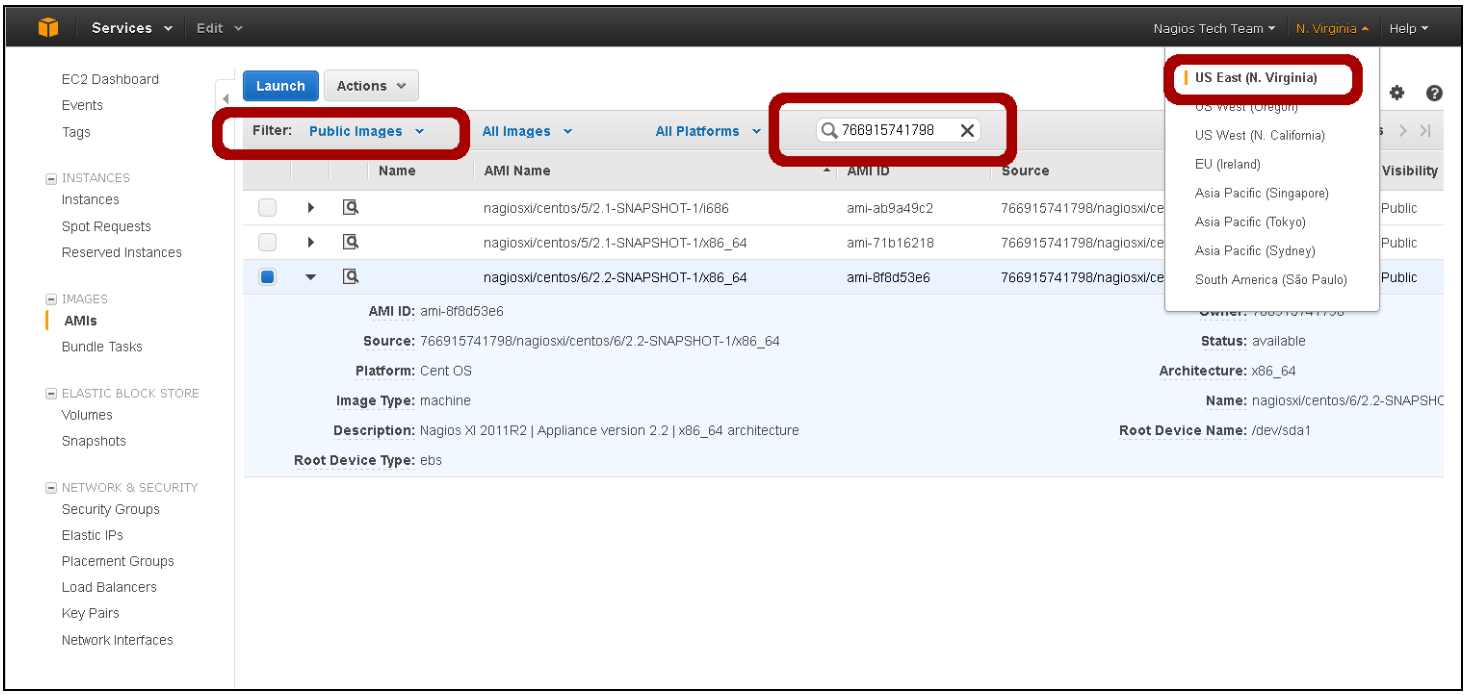
Creating an NNA instance in Amazon EC2 with Nagios Network Analyzer 2024

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 Network Analyzer 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#ss=Images



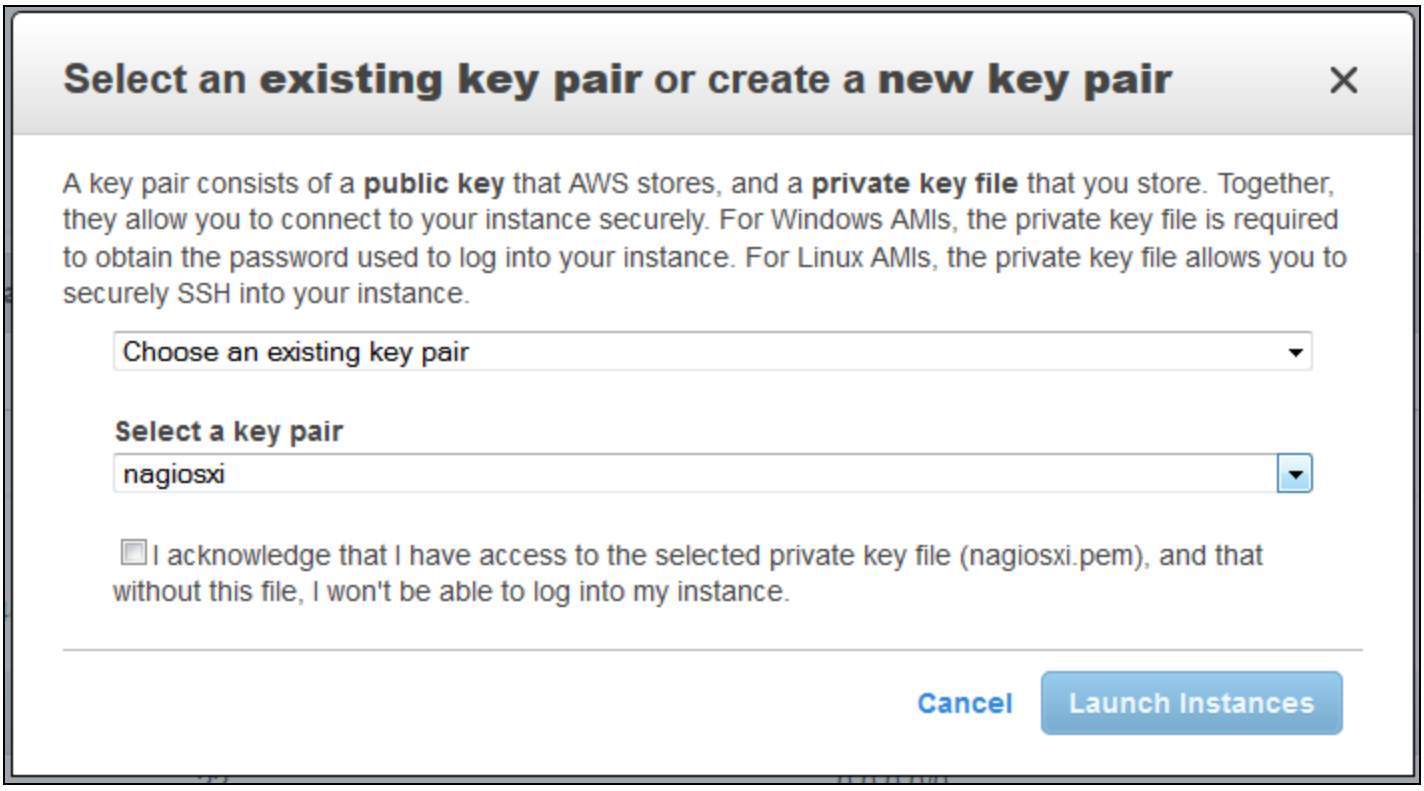
Images are currently available in the following zones:

- 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.

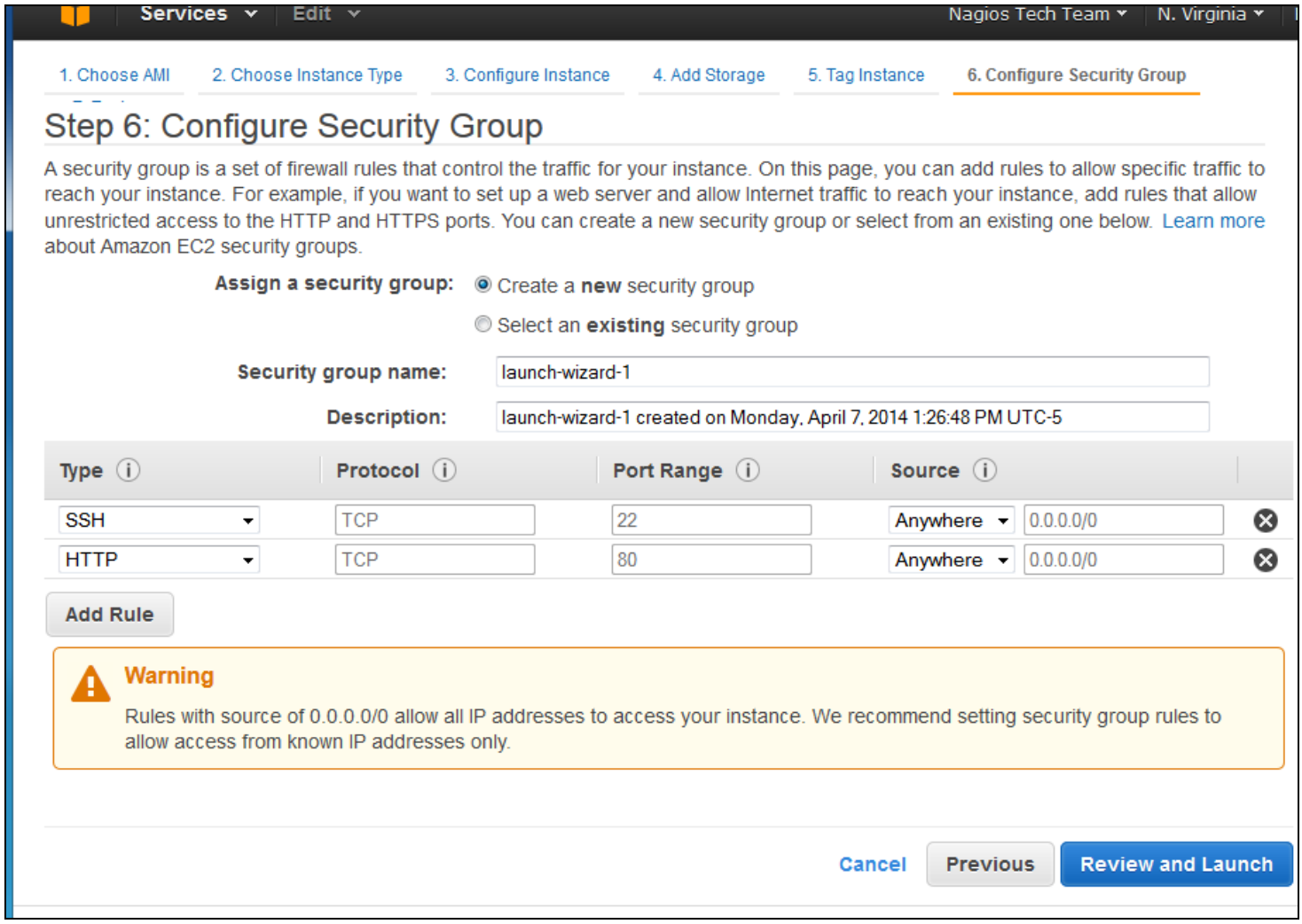
In the search bar enter: 766915741798. This is the Nagios Tech Team official ID. From here you can select the image that meets your needs and click Launch.

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 Network Analyzer, the minimum specifications we recommend are 1 core and 2GB 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.

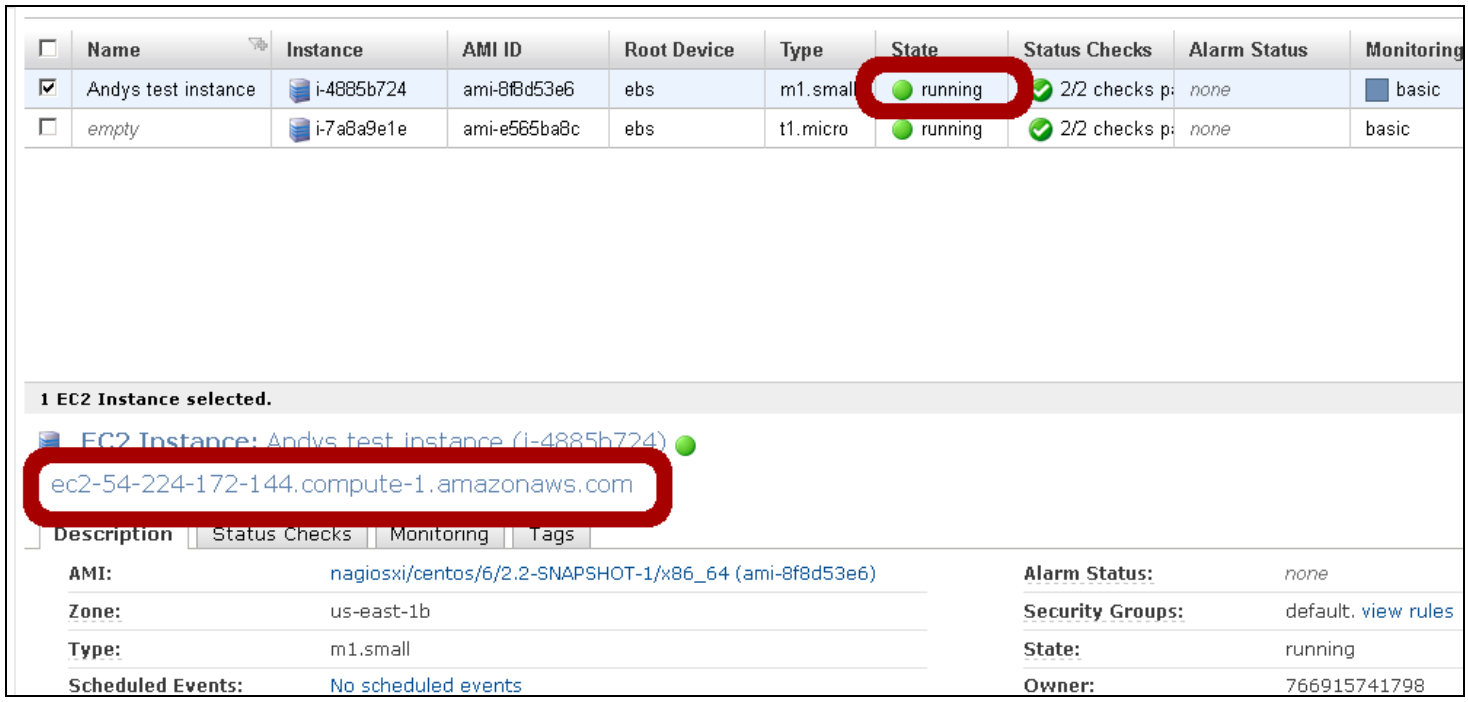
Root password login is disabled.



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 network flow data to.

When you first start your instance, the latest version of Nagios Network Analyzer 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 Network Analyzer



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

http://<ipaddress>/nagiosna

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

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 Network Analyzer. 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.

```
ssh -i .ssh/mykey.pem centos@[AWS_public_DNS]
```

Notes About System Credentials And Security

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

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.