**Setting Up Nagios Monitoring Tool**

# **Objectives**

Set up Nagios Server to monitor host (SCP Web Application).

**Sources**:

* <https://support.nagios.com/kb/article/nagios-core-installing-nagios-core-from-source-96.html#CentOS>
* <https://www.tecmint.com/fix-firewall-cmd-command-not-found-error/>
* <https://github.com/NagiosEnterprises/nrpe>
* <https://tecadmin.net/install-nrpe-on-centos-rhel/>
* <https://stackoverflow.com/questions/21981796/cannot-ping-aws-ec2-instance>

**Prerequisites**

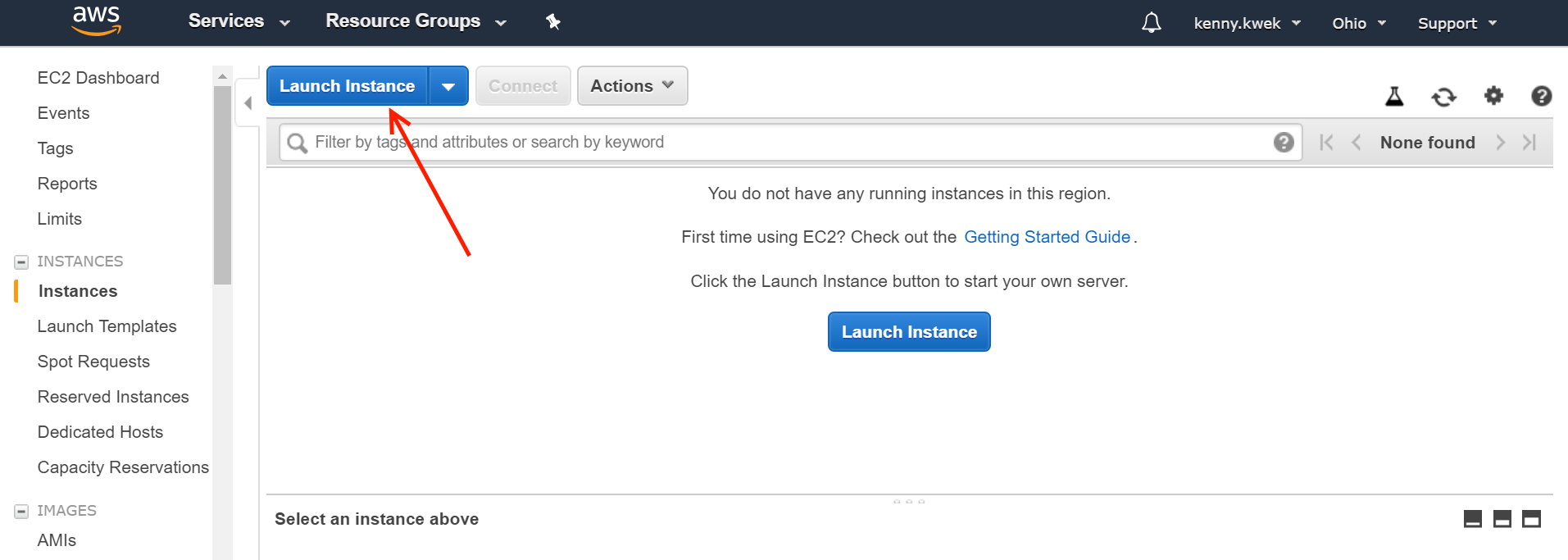
1. Access to your **AWS Console Management** (<https://aws.amazon.com/>)
2. Project (SCP Web Application) Instance deployed and set up

# **Overview**

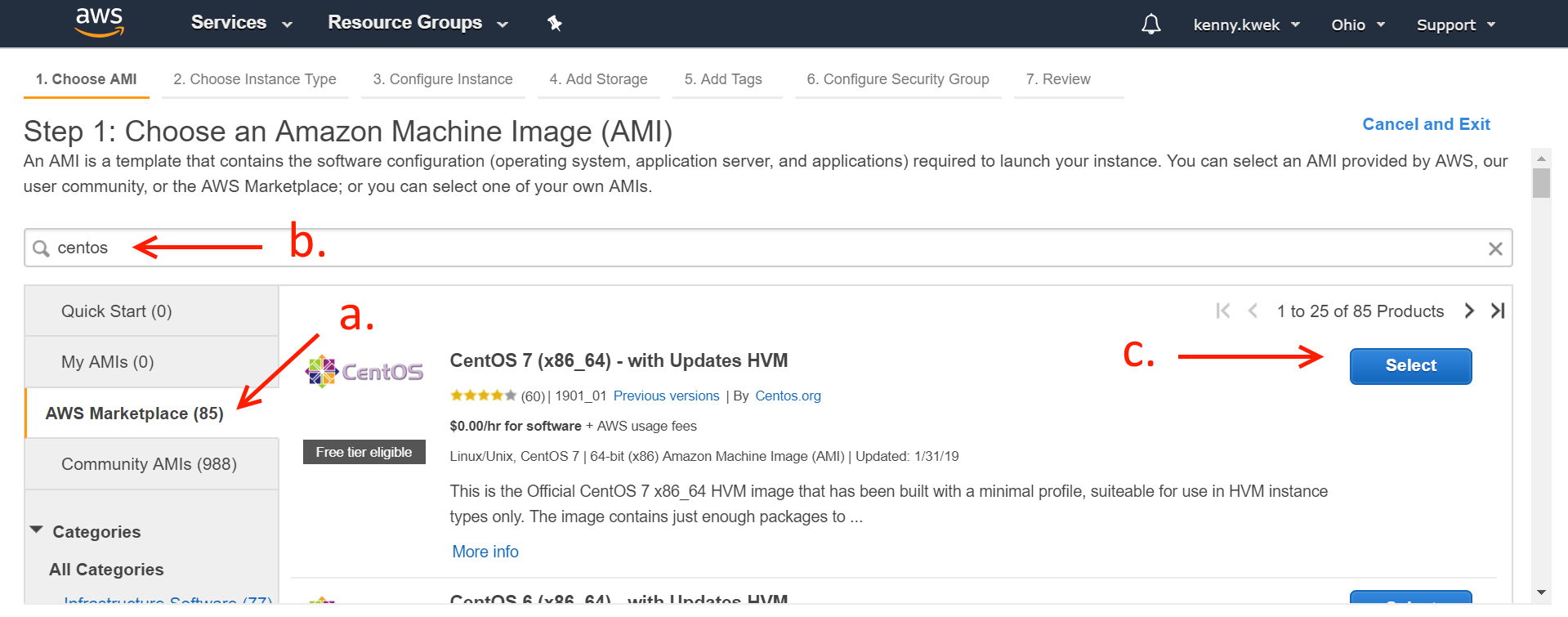
* [Task A: Creating Nagios Server Instance on AWS](#_altoubdqyzu)
* [Task B: Installing Nagios Core on Nagios Server Instance](#_y1anxrx8kag2)
* [Task C: Installing Nagios Plugins on Nagios Server Instance](#_k61r3im0pmzz)
* [Task D: Configuring Nagios Server on Nagios Server Instance](#_wdab9332pmwd)
* [Task E: Downloading and Configuring NRPE on Project Instance](#_ihi0p54zvoeo)
* [Commands to modify Nagios Server and Project](#_jv0bde2slb65)

# **Task A: Creating Nagios Server Instance on AWS**

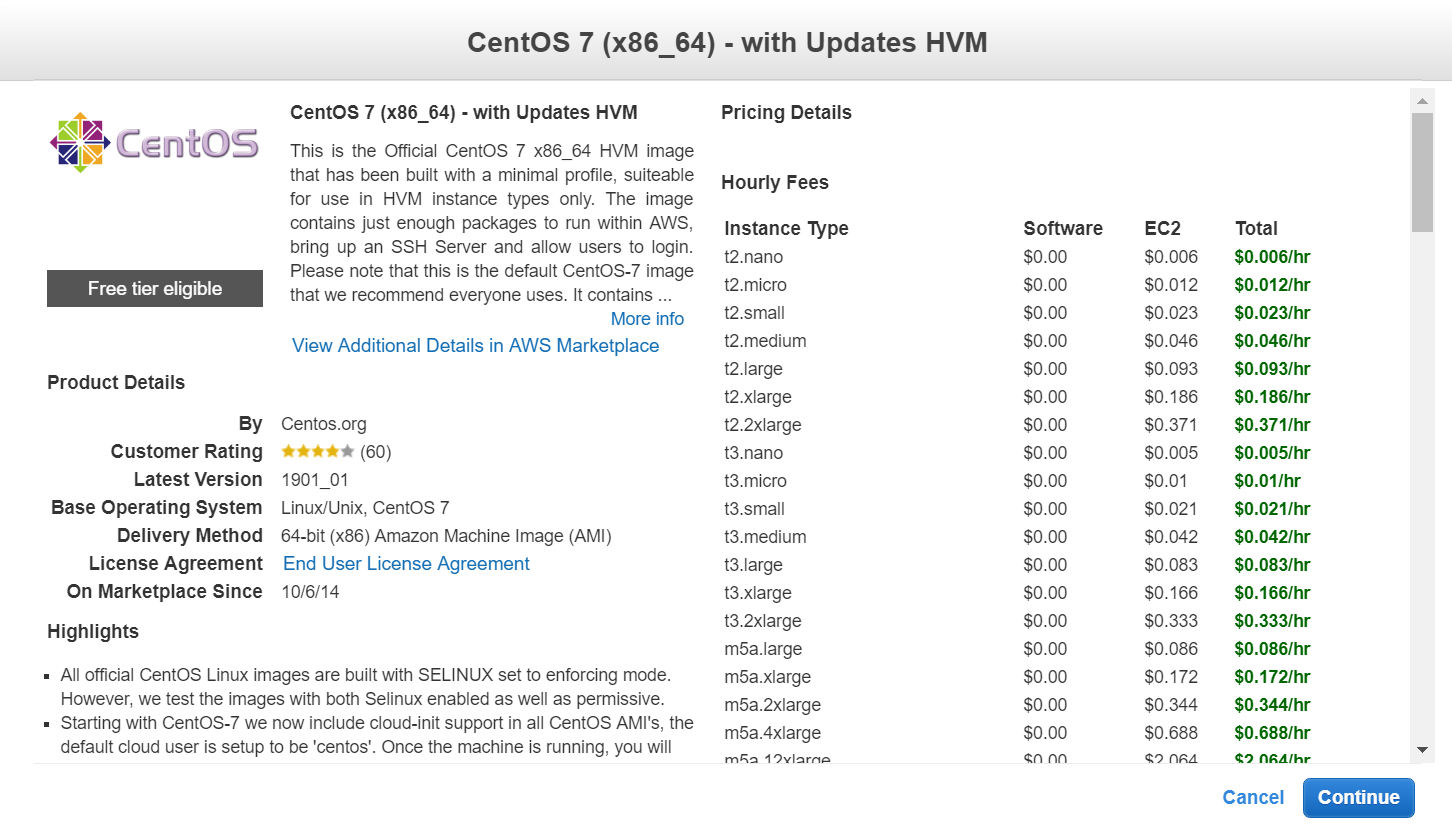
1. Create a new AWS account solely for Nagios Server to avoid exceeding free tier limit of 750 hours.
2. Go to Instances dashboard and click on “Launch Instance”



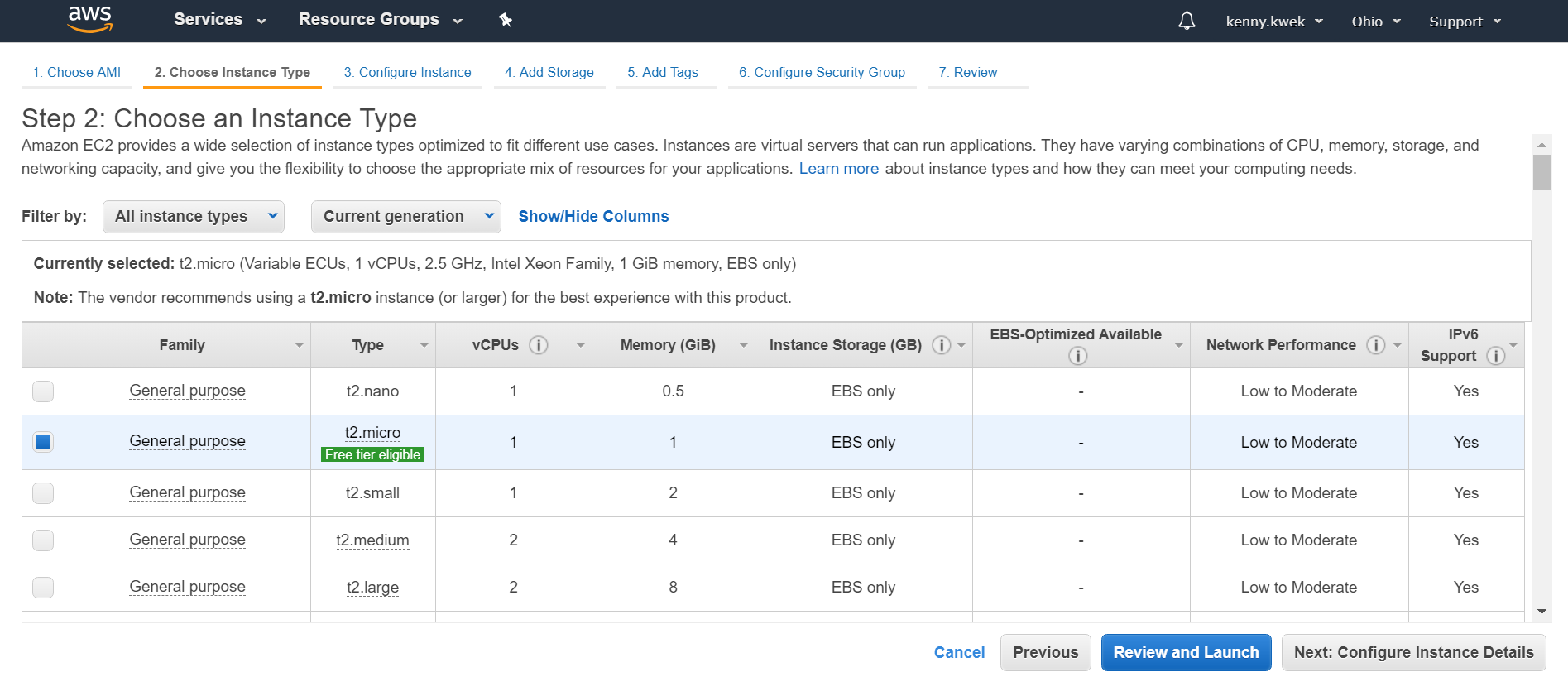
1. Get the CentOS 7 Amazon Machine Image (Free Tier eligible)
   1. Click on “AWS Marketplace”
   2. Search for “centos”
   3. Select “CentOS 7 (x84 64) - with Updates HVM“



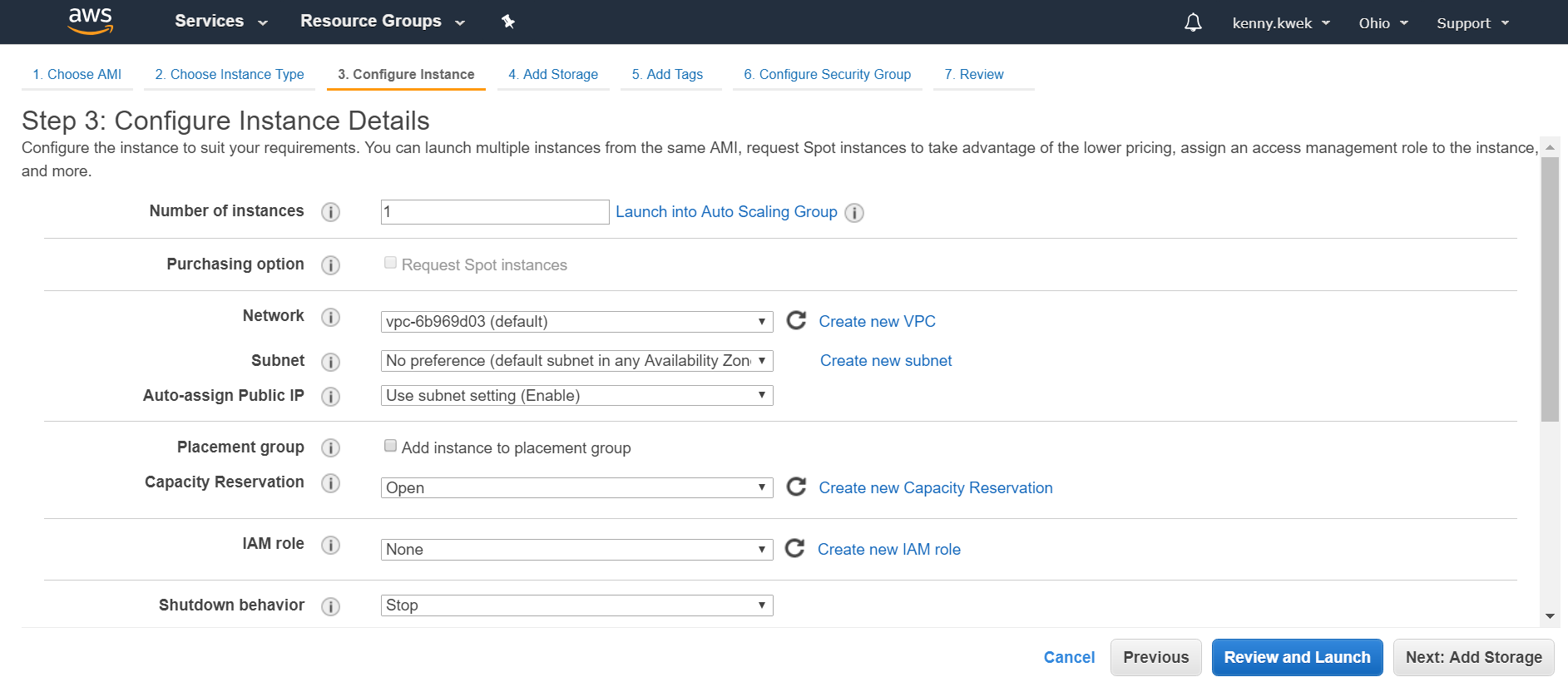
1. Click continue



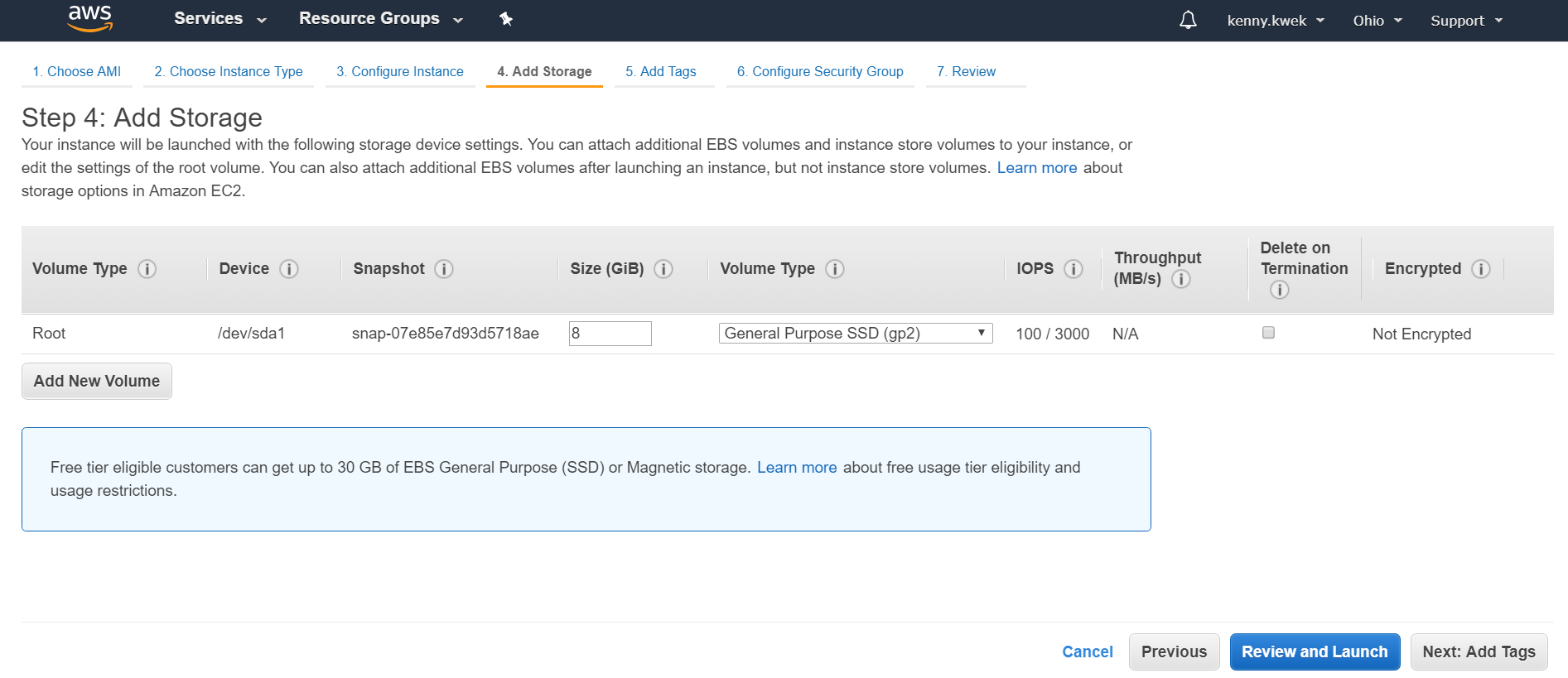
1. Select “t2.micro” and “Next Configuration Instance Details”



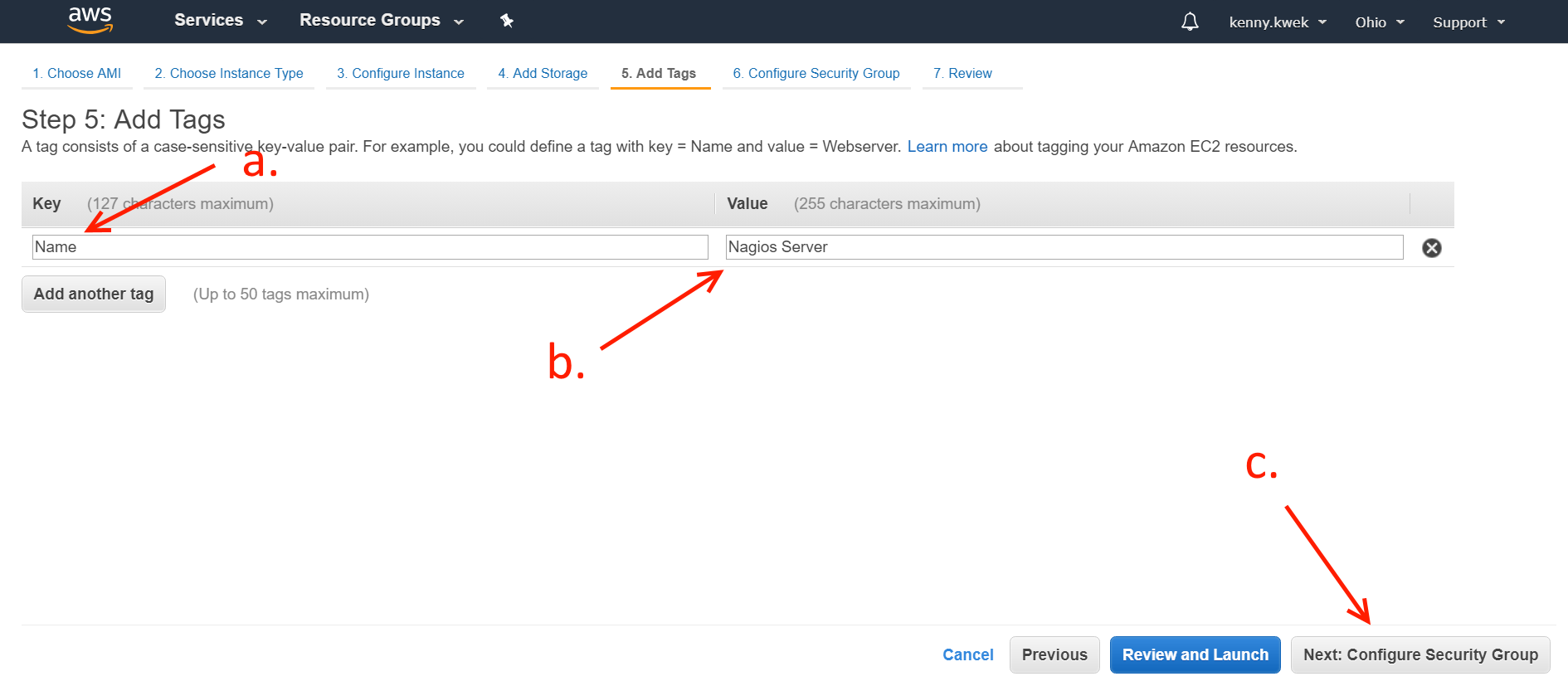
1. Click “Next: Add Storage”



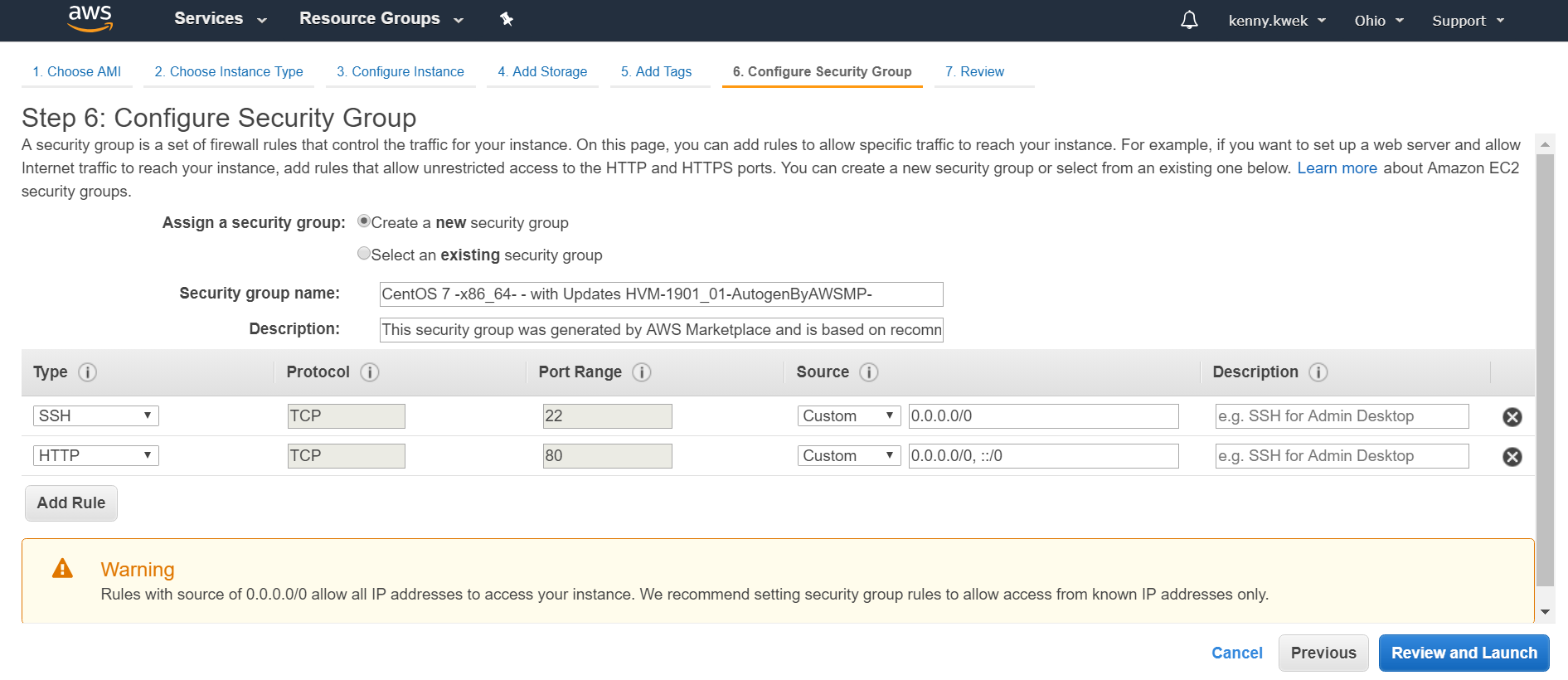
1. Click “Next: Add Tags”



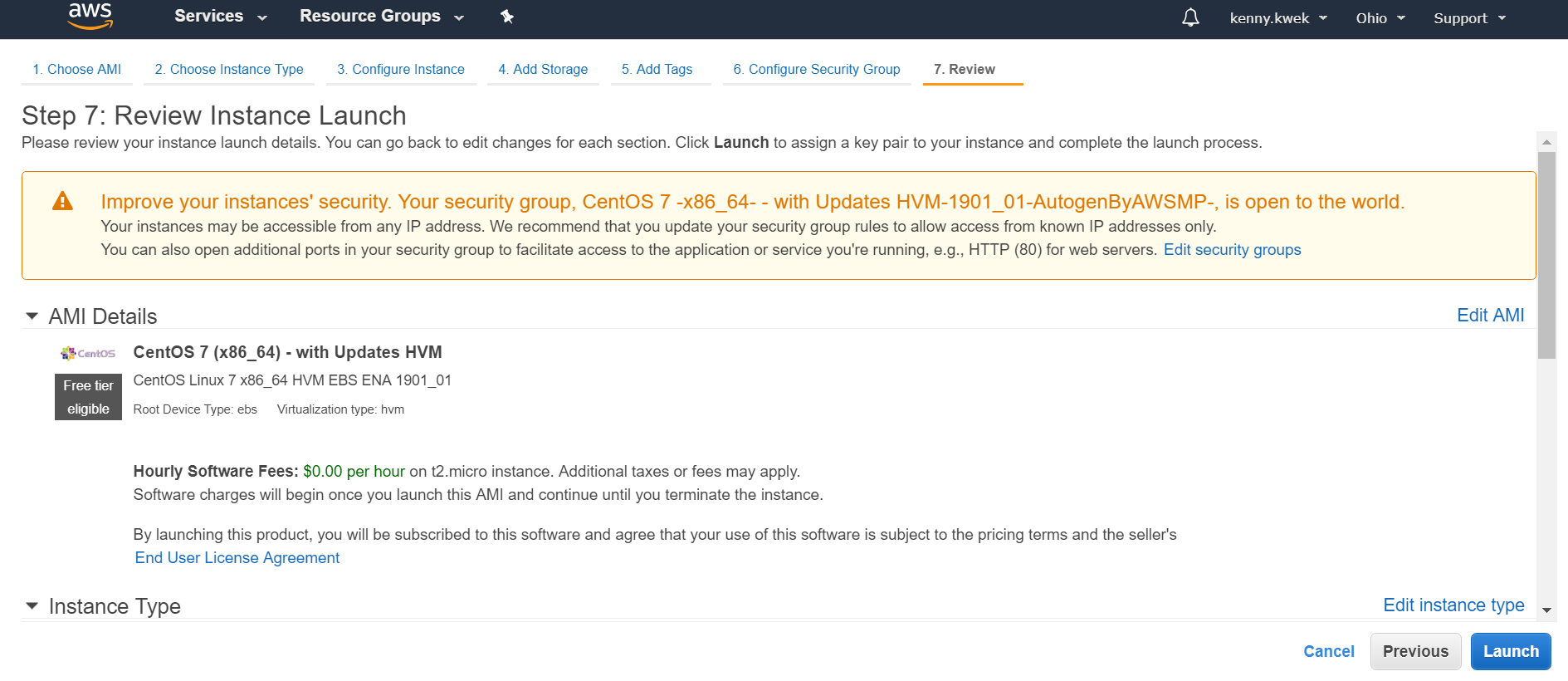
1. Add Tags
   1. Enter “Name” under Key
   2. Enter “Nagios Server” or any name to identify instance under Value
   3. Click “Next: Configure Security Group”



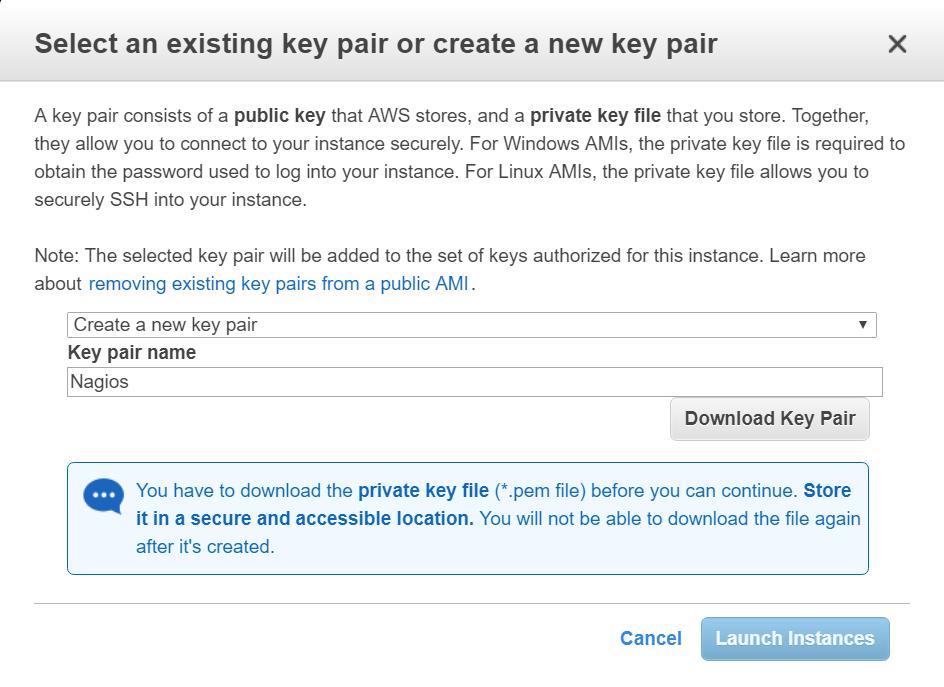
1. Configure Security Group to the following settings and click “Review and Launch”



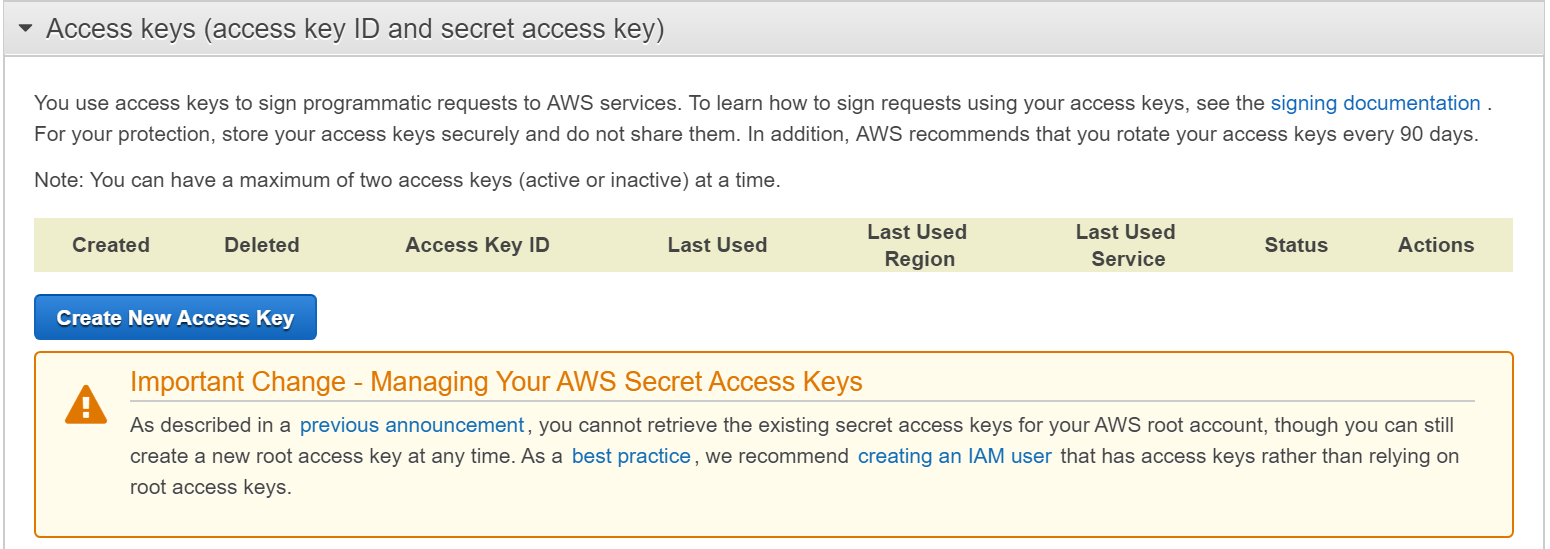
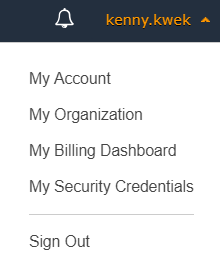
1. Review Instance settings and click “Launch”



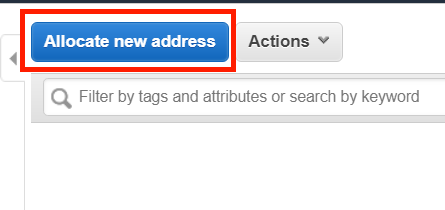
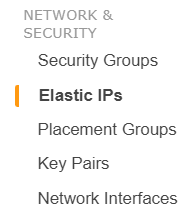
1. Create a new key pair and Download Key Pair to get .pem file, then click “Launch Instances”



1. Get Security Credentials
   1. At AWS Management Console, click “My Security Credentials”
   2. Choose “Access Keys” and “Create New Access Key”

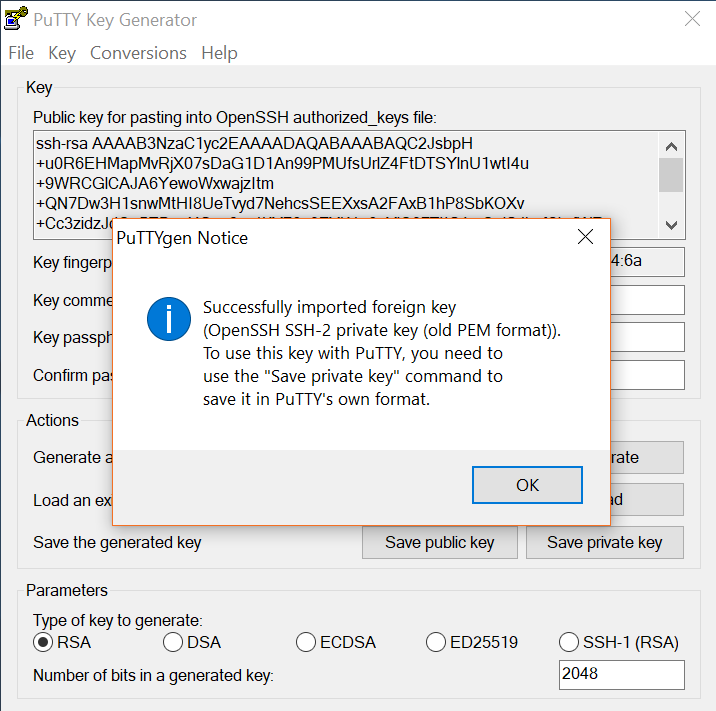


1. Assign Elastic IP address
   1. At the EC2 dashboard console, at the Network and Security category, choose the Elastic IPs option
   2. Click “Allocate new address”, click “Allocate”, and click “close”
   3. Click “Actions” tab and “Associate address”
   4. Select the instance to associate to and Private IP address

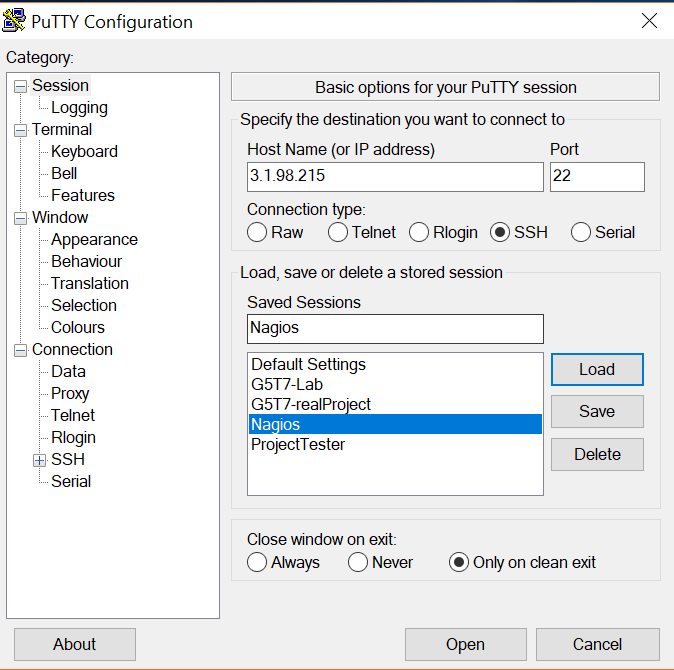


# **Task B: Installing Nagios Core on Nagios Server Instance**

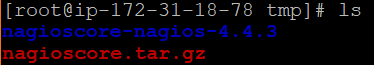
1. Convert .pem key to .ppk format
   1. Open PuTTY Key Generator
   2. Click “Load” and select .pem key
   3. Click “Save private key” and save .ppk key



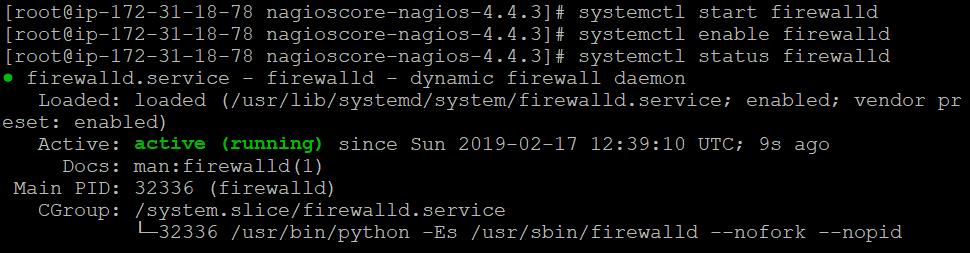
1. Connect to Instance SSH using PuTTY
   1. Open PuTTY
   2. Enter:
      1. Host Name/IP Address (Assigned Nagios Elastic IP): [3.1.98.215](https://ap-southeast-1.console.aws.amazon.com/ec2/v2/home?region=ap-southeast-1#Addresses:search=3.1.98.215;sort=publicIp)
      2. SSH > Data > auto-login username: **centos**
      3. SSH > Auth > private key file for authentication : **<.ppk file>**
   3. Click “Open”



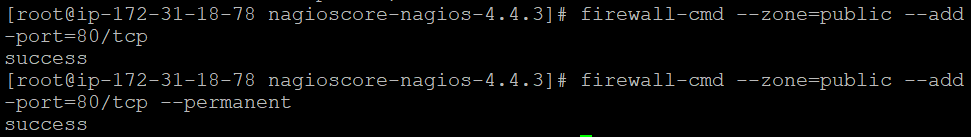
1. Run the command “sudo su” to run subsequent commands as root user
2. Security-Enhanced Linux - SELinux being disabled or in permissive mode
   1. sed -i 's/SELINUX=.\*/SELINUX=disabled/g' /etc/selinux/config
   2. setenforce 0
3. Prerequisites - Perform these steps to install the prerequisite packages.
   1. yum install -y gcc glibc glibc-common wget unzip httpd php gd gd-devel perl postfix
      1. **Yum** - package manager
      2. **Install** - to install
      3. **-y** - automatically says yes to all prompts
      4. **gcc** - GNU Compiler Collection (GCC) is a compiler system produced by the GNU Project, it is the standard compiler for most Unix-like operating systems
      5. **glibc** - provides the user land interface to the services provided by kernel so that user application can use a system call just like a ordinary function. The glibc package contains standard libraries which are used by multiple programs on the system.
      6. **glibc-common** - package includes common binaries for the GNU libc libraries, as well as national language (locale) support.
      7. **wget** - stands for "web get". It is a command-line utility which downloads files over a network
      8. **unzip** - unzip files
      9. **httpd** - Apache Hypertext Transfer Protocol daemon or Apache web server
      10. **php** - PHP: Hypertext Preprocessor
      11. **gd**  - The GD Graphics Library for dynamically manipulating images. You will need to compile PHP with the GD library of image functions for this to work
      12. **gd-devel** - package contains the development libraries and header files for gd
      13. **perl** - perl programming language
      14. **postfix** - free and open-source mail transfer agent that routes and delivers electronic mail
4. Downloading the Source
   1. cd /tmp
   2. wget -O nagioscore.tar.gz https://github.com/NagiosEnterprises/nagioscore/archive/nagios-4.4.3.tar.gz
   3. tar xzf nagioscore.tar.gz



1. Compile
   1. cd /tmp/nagioscore-nagios-4.4.3/
   2. ./configure
   3. make all
2. Create User And Group - This creates the nagios user and group. The apache user is also added to the nagios group.
   1. make install-groups-users
   2. usermod -a -G nagios apache
3. Install Binaries - This step installs the binary files, CGIs, and HTML files.
   1. make install
4. Install Service / Daemon
   1. make install-daemoninit
   2. systemctl enable httpd.service
5. Install Command Mode - This installs and configures the external command file.
   1. make install-commandmode
6. Install Configuration Files - This installs the \*SAMPLE\* configuration files. These are required as Nagios needs some configuration files to allow it to start.
   1. make install-config
7. Install Apache Config Files - This installs the Apache web server configuration files. Also configure Apache settings if required.
   1. make install-webconf
8. Install Firewall
   1. yum install firewalld
9. Start firewalld and enable it to auto-start at system boot, then check its status
   1. systemctl start firewalld
   2. systemctl enable firewalld
   3. systemctl status firewalld

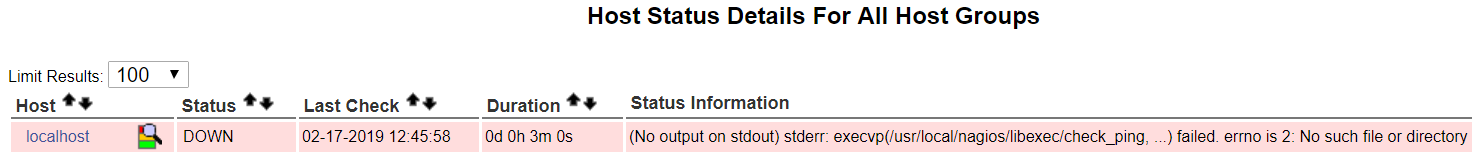


1. Configure Firewall - You need to allow port 80 inbound traffic on the local firewall so you can reach the Nagios Core web interface.
   1. firewall-cmd --zone=public --add-port=80/tcp
   2. firewall-cmd --zone=public --add-port=80/tcp --permanent



1. Create nagiosadmin User Account - You'll need to create an Apache user account to be able to log into Nagios. The following command will create a user account called nagiosadmin and you will be prompted to provide a password for the account.
   1. htpasswd -c /usr/local/nagios/etc/htpasswd.users nagiosadmin
2. Start Apache Web Server
   1. systemctl start httpd.service
3. Start Service / Daemon - This command starts Nagios Core.
   1. systemctl start nagios.service
4. Test Nagios - Nagios is now running, to confirm this you need to log into the Nagios Web Interface.
   1. Go to [3.1.98.215/nagios](https://ap-southeast-1.console.aws.amazon.com/ec2/v2/home?region=ap-southeast-1#Addresses:search=3.1.98.215;sort=publicIp)
   2. Login with
      1. Username: **nagiosadmin**
      2. Password (Password set earlier): **apple**

Currently you have only installed the Nagios Core engine. You'll notice some errors under the hosts and services along the lines of:



These errors will be resolved once you install the Nagios Plugins

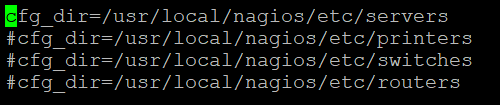
# **Task C: Installing Nagios Plugins on Nagios Server Instance**

1. Prerequisites
   1. yum install -y gcc glibc glibc-common make gettext automake autoconf wget openssl-devel net-snmp net-snmp-utils epel-release
   2. yum install -y perl-Net-SNMP
   3. Install nano text editor for CentOS
      1. yum install nano
2. Downloading The Source
   1. cd /tmp
   2. wget --no-check-certificate -O nagios-plugins.tar.gz https://github.com/nagios-plugins/nagios-plugins/archive/release-2.2.1.tar.gz
   3. tar zxf nagios-plugins.tar.gz
3. Compile + Install
   1. cd /tmp/nagios-plugins-release-2.2.1/
   2. ./tools/setup
   3. ./configure
   4. make
   5. make install
4. Test Plugins: [3.1.98.215/nagios](https://ap-southeast-1.console.aws.amazon.com/ec2/v2/home?region=ap-southeast-1#Addresses:search=3.1.98.215;sort=publicIp)
5. Restart nagios
   1. Service / Daemon Commands
      1. systemctl start nagios.service
      2. systemctl stop nagios.service
      3. systemctl restart nagios.service
      4. systemctl status nagios.service

# **Task D: Configuring Nagios Server on Nagios Server Instance**

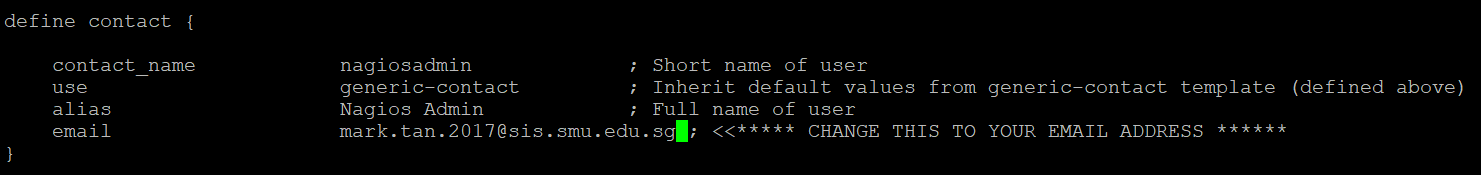
1. Enable Servers
   1. Go to: nano /usr/local/nagios/etc/nagios.cfg
   2. Scroll down and uncomment

#cfg\_dir=/usr/local/nagios/etc/servers



* 1. **Ctrl X** to exit, **Y** to save modified file, **Enter** to override current file name

1. Add email
   1. Go to: nano /usr/local/nagios/etc/objects/contacts.cfg
   2. Enter your email



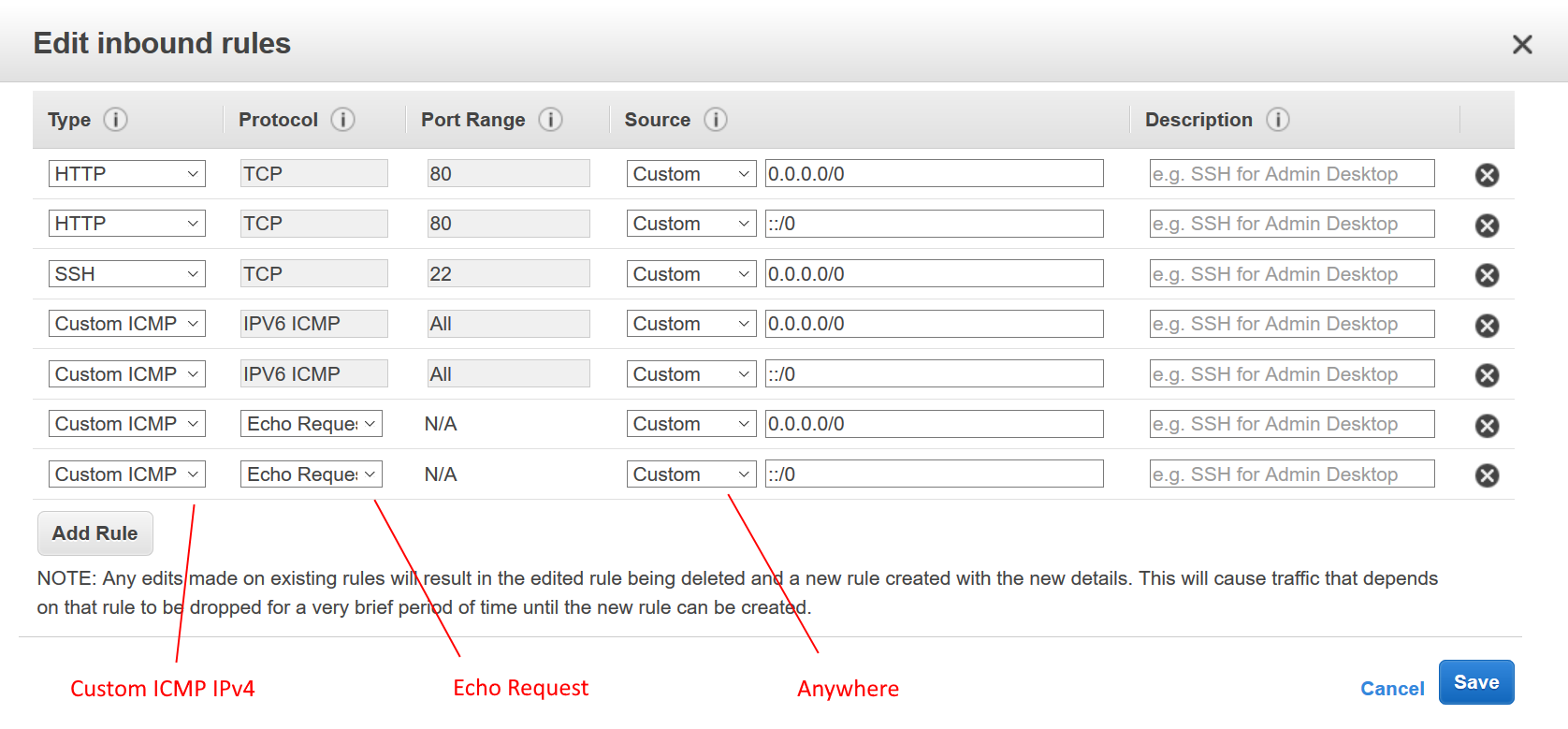
* 1. **Ctrl X** to exit, **Y** to save modified file, **Enter** to override current file

1. Make Servers Directory
   1. mkdir /usr/local/nagios/etc/servers
2. Define host
   1. Create new file: nano /usr/local/nagios/etc/servers/clientSCP.cfg
   2. Copy and paste this into configuration file or customise, and change IP address:

define host **{**  
 use linux-server  
 host\_name clientSCP  
 alias clientSCP  
 address 3.1.118.42  
 register 1  
**}**  
  
define service **{**  
 host\_name clientSCP  
 service\_description PING  
 check\_command check\_ping!100.0,20%!500.0,60%  
 max\_check\_attempts 2  
 check\_interval 2  
 retry\_interval 2  
 check\_period 24x7  
 check\_freshness 1  
 contact\_groups admins  
 notification\_interval 2  
 notification\_period 24x7  
 notifications\_enabled 1  
 register 1  
**}**  
  
define service **{**  
 host\_name clientSCP  
 service\_description Disk Usage  
 check\_command check\_local\_disk!20%!10%!/  
 max\_check\_attempts 2  
 check\_interval 2  
 retry\_interval 2  
 check\_period 24x7  
 check\_freshness 1  
 contact\_groups admins  
 notification\_interval 2  
 notification\_period 24x7  
 notifications\_enabled 1  
 register 1  
**}**  
  
define service **{**  
 host\_name clientSCP  
 service\_description SSH Service  
 check\_command check\_ssh  
 max\_check\_attempts 2  
 check\_interval 2  
 retry\_interval 2  
 check\_period 24x7  
 check\_freshness 1  
 contact\_groups admins  
 notification\_interval 2  
 notification\_period 24x7  
 notifications\_enabled 1  
 register 1  
**}**

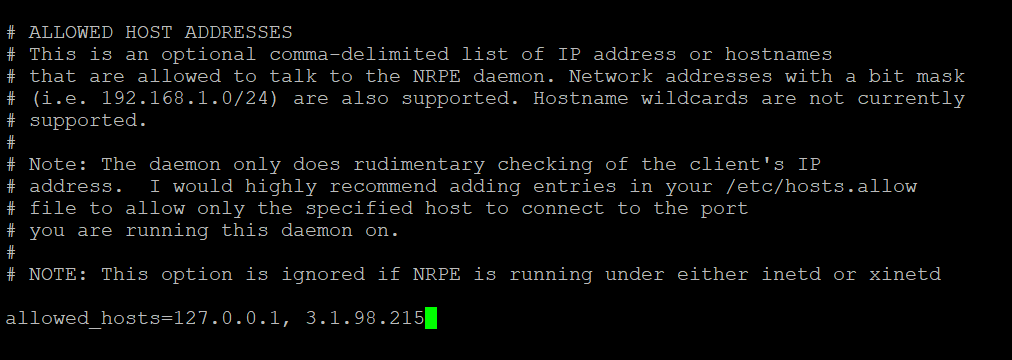
* 1. **Ctrl X** to exit, **Y** to save modified file, **Enter** to override current file
  2. Restart Nagios: systemctl restart nagios

1. In AWS Console Management, add new inbound rule
   1. Go to Network & Security > Security Groups
   2. Select the security group associated with Nagios Server (eg. CentOS7)
   3. Edit inbound rules > Add Rule
      1. Type: **Custom ICMP Rule - IPv4**
      2. Protocol: **Echo Request**
      3. Source: **Anywhere**
   4. Save

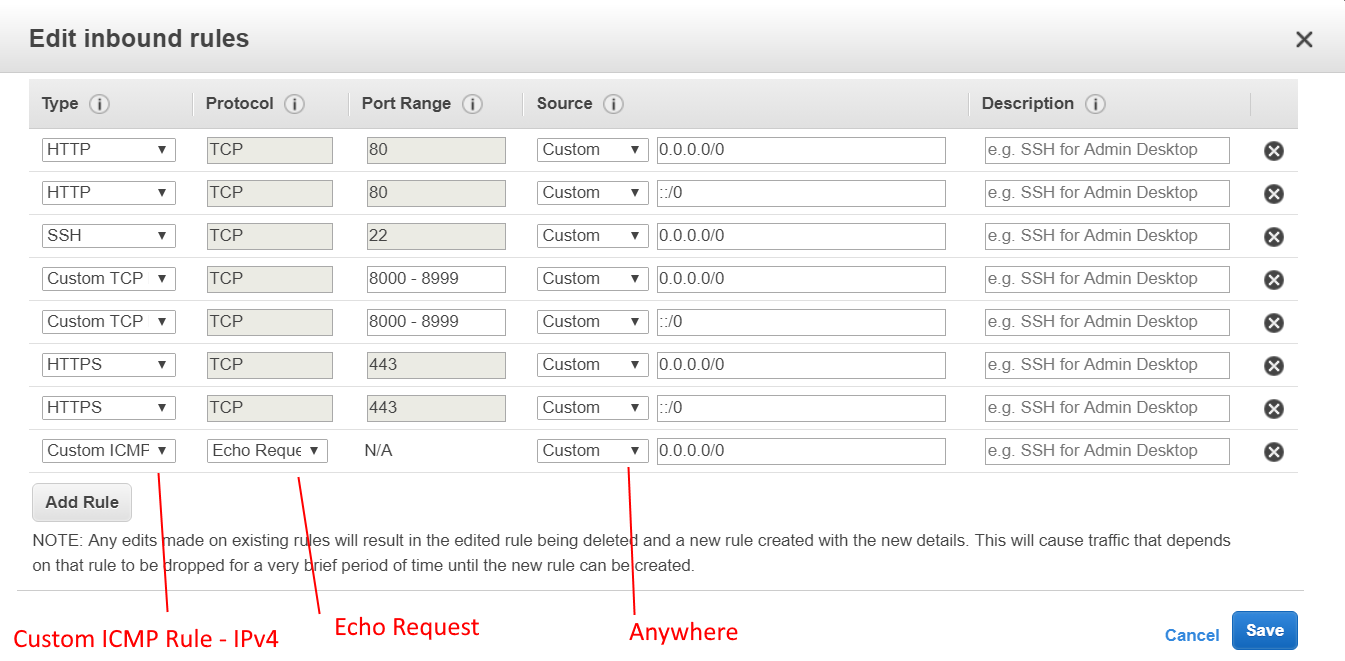


# **Task E: Downloading and Configuring NRPE on Project Instance**

1. Prerequisites
   1. yum install -y gcc glibc glibc-common make gettext automake autoconf wget openssl-devel net-snmp net-snmp-utils epel-release
   2. yum install -y perl-Net-SNMP
2. Downloading Nagios Plugin
   1. cd /tmp
   2. wget --no-check-certificate -O nagios-plugins.tar.gz https://github.com/nagios-plugins/nagios-plugins/archive/release-2.2.1.tar.gz
   3. tar zxf nagios-plugins.tar.gz
3. Compile + Install
   1. cd /tmp/nagios-plugins-release-2.2.1/
   2. ./tools/setup
   3. ./configure
   4. make
   5. make install
4. Install NRPE
   1. yum --enablerepo=epel -y install nrpe nagios-plugins
5. Include Nagios host address
   1. nano /etc/nagios/nrpe.cfg
   2. Add Nagios Server IP Address after 127.0.0.1
   3. Save



1. Restart NRPE
   1. service nrpe stop
   2. service nrpe start
2. In AWS Console Management, add new inbound rule
   1. Go to Network & Security > Security Groups
   2. Select the security group associated with Project Instance (eg. launch-wizard)
   3. Edit inbound rules > Add Rule
      1. Type: **Custom ICMP Rule - IPv4**
      2. Protocol: **Echo Request**
      3. Source: **Anywhere**
   4. Save



# **Commands to modify Nagios Server and Project**

**In Project Instance:**

To edit NRPE settings: sudo nano /etc/nagios/nrpe.cfg

To restart NRPE service: service nrpe restart

To stop NRPE service: service nrpe stop

To start NRPE service: service nrpe start

**In Nagios Server Instance:**

To go to server directory: cd /usr/local/nagios/etc/servers

To edit host settings in server directory: nano /usr/local/nagios/etc/servers/clientSCP.cfg

(where clientSCP.cfg is the host file name)

To reload Nagios: systemctl reload nagios