Nessus (BYOL) on Amazon Web Services Quick Start Guide

Introduction

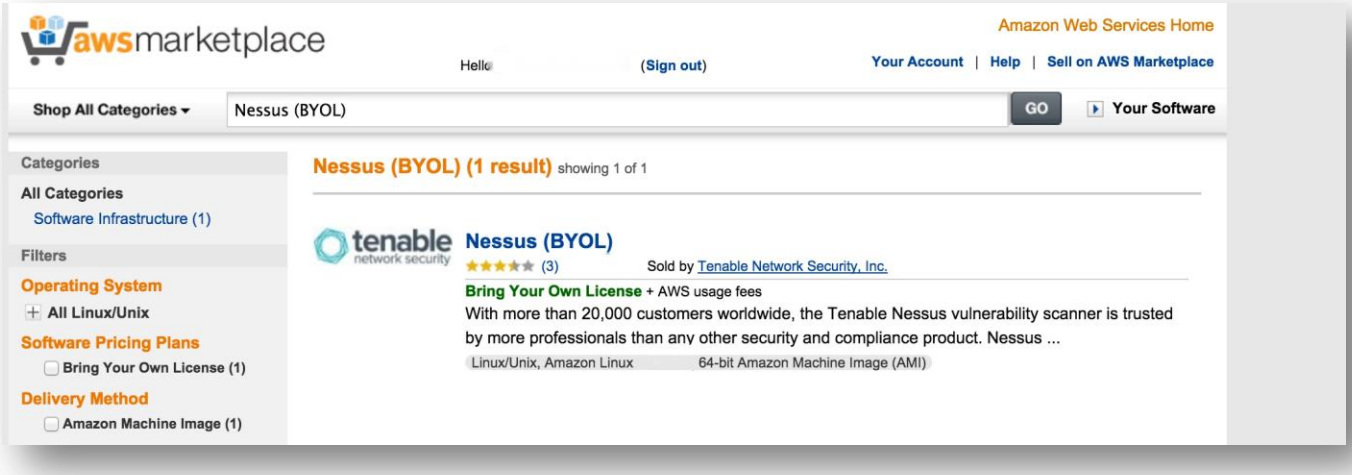
This document describes how to deploy Tenable Network Security's **Nessus BYOL (Bring Your Own License) for AWS (Amazon Web Services)**. Please email any comments and suggestions to support@tenable.com.

With more than one million users, Nessus is the world's most widely-deployed vulnerability, configuration, and compliance assessment product. Nessus prevents attacks by identifying the vulnerabilities, configuration issues, and malware that hackers could use to penetrate your network. It is as important to run these assessments in AWS as it is in any other IT environment. Amazon recommends that all new and existing AWS customers scan their AWS instances while in development and operations and before publishing to AWS users.

The Nessus BYOL is an instance of Nessus installed in AWS that allows scanning of AWS EC2 environments and instances. Customers interested in leveraging Nessus to secure their environments and instances must first purchase a Nessus license either directly from Tenable's e-Commerce store or from an authorized reseller. The license will provide an Activation Code to apply when provisioning Nessus from your AWS account.

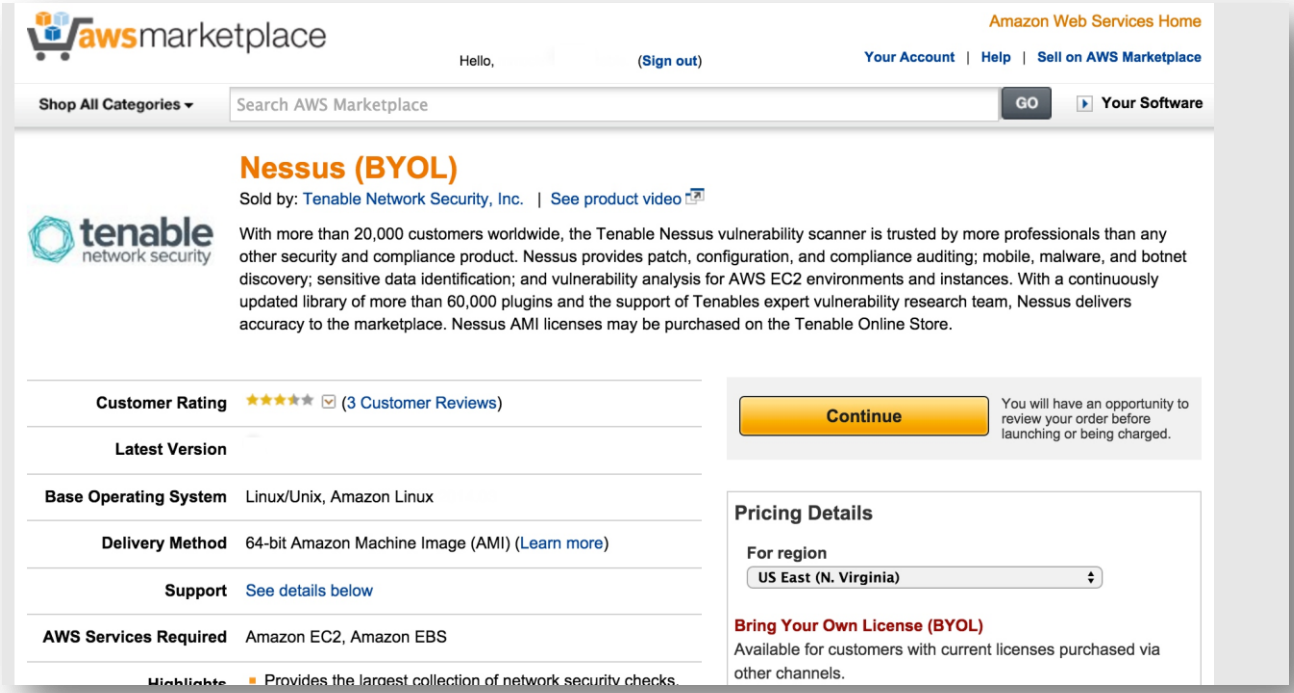
Provisioning Nessus from the AWS Marketplace

Go to the AWS Marketplace (https://aws.amazon.com/marketplace) and log in.

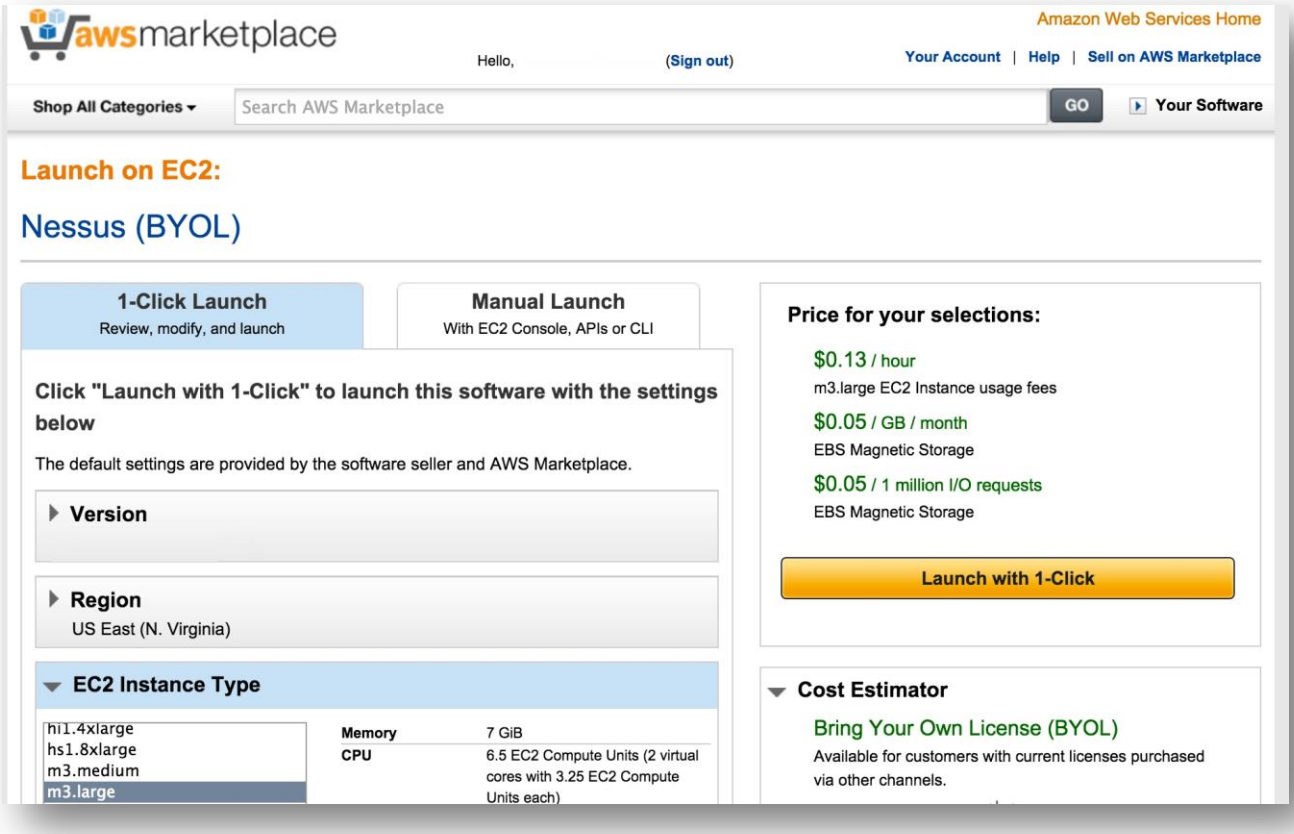


Search for "**Nessus (BYOL)**".

Click on "**Nessus (BYOL)**" and review the product page.



Click "**Continue**".



Select the appropriate region, instance type, security group, and key pair. Tenable recommends configuring the security group to prevent access from IP addresses not associated with your organization.

If you are deploying the instance into a VPC, you must ensure you can reach TCP port 8834 on an IP address associated with the instance. This will be needed to complete the configuration process, as well as for the use of the product.

Configure the instance and/or VPC so that Nessus can communicate with Tenable servers; this is required for registration and plugin updates. If for some reason this is not possible, please refer to the Nessus documentation regarding off-line updates.

Click "**Launch with 1-Click**" to deploy the instance.

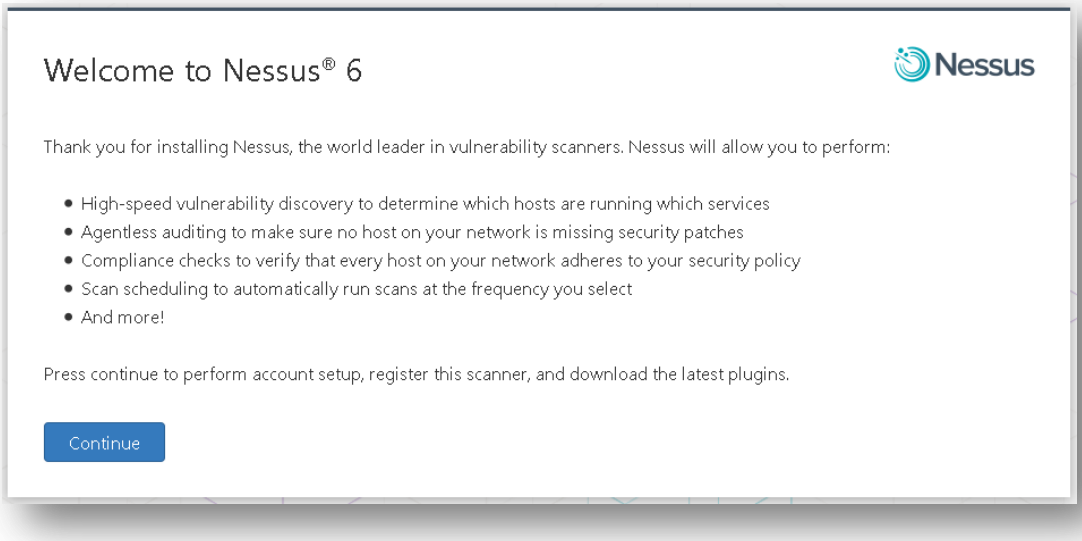
You will be presented with a window summarizing the details of the instance. Close the window and log in to the AWS EC2 Console to check on the progress of the deployment.

After the instance has initialized, open a browser and connect to the instance to complete the configuration; for example:

https://<IP address or hostname>:8834

Generally, you will connect to the public IP address (or external hostname) associated with an instance. If you are connecting to Nessus over a VPN to a VPC, it may be the private IP address. The IP addresses associated with the instance can be found by clicking on the instance in the EC2 console.

The following welcome screen will be displayed:



To complete the configuration, please refer to the Nessus documentation.

Prior to scanning, you must request permission to conduct vulnerability and penetration testing on instances in the AWS cloud by completing the following form:

AWS Vulnerability / Penetration Testing Request Form (form needed for BYOL usage model):
https://portal.aws.amazon.com/gp/aws/html-forms-controller/contactus/AWSSecurityPenTestRequest

About Tenable Network Security

Tenable Network Security transforms security technology for the business needs of tomorrow through comprehensive solutions that provide continuous visibility and critical context, enabling decisive actions to protect your organization. Tenable eliminates blind spots, prioritizes threats, and reduces exposure and loss. With more than one million users and more than 20,000 enterprise customers worldwide, organizations trust Tenable for proven security innovation. Tenable's customers range from Fortune Global 500 companies, to the U.S. Department of Defense, to mid-sized and small businesses in all sectors, including finance, government, healthcare, higher education, retail, and energy. Transform security with Tenable, the creators of Nessus and leaders in continuous monitoring. For more information, visit tenable.com.