hcWTgX

Due to technical issues with AWS, Nessus Enterprise for AWS is currently not available for purchase. To protect your AWS cloud infrastructure, please purchase Nessus Cloud **http://www.tenable.com/products/nessus/nessus-cloud** or Nessus BYOL **https://aws.amazon.com/marketplace/pp/B00G9A5MS0**.

Nessus Enterprise for Amazon Web Services (AWS) Installation and Configuration Guide

July 16, 2014

(Revision 2)

Wiz - EXHIBIT 1123
Wiz, Inc. v. Orca Security Ltd.
IPR2024-00865

Table of Contents

Introduction 3

Requirements 3

Standards and Conventions 3

Nessus Enterprise for AWS Overview 4

Provisioning the Nessus Enterprise for AWS Instances 4
- Adding a Nessus Enterprise for AWS Manager Instance 5

Adding AWS User with Correct Permissions for Nessus Enterprise for AWS API Access 9

Operations 12
- Log in via SSH to Nessus Enterprise for AWS Manager or Scanner 12
- Connect to Nessus UI 12

Configuring the Nessus Enterprise for AWS Manager 13
- Nessus Enterprise for AWS Manager Installation 14
- Nessus Enterprise for AWS Manager Navigation 16
  - Interface Shortcuts 19
- Nessus Enterprise for AWS Manager Settings 20
  - User Profile 20
  - Account Settings 22
- Setting up the Nessus Enterprise for AWS Manager 22
  - Setting up AWS instance authentication 22
  - LDAP Server Settings 23
  - Mail Server Settings 23
  - Multi Scanner Setting 23
  - Scanners Settings 24
  - Advanced Settings 25

Adding a Nessus Enterprise for AWS Scanner Instance 25
- Configuring the Nessus Enterprise for AWS Scanner 26
  - Adding the EC2 User Data to the Nessus Enterprise for AWS Scanner instance 27
  - Creating the Security Group for the Nessus Enterprise for AWS Scanner instance 27
- Adding the EC2 User Data to the Nessus Enterprise for AWS Scanner after instance creation 27

Scanning using Nessus Enterprise for AWS Manager 30
- Policies Overview 30
- Managing Policies 30
- Creating, Launching, and Scheduling a Scan 30

Scanning Reports for Nessus for AWS 36

Adding other Nessus Scanners 37

For Further Information 40

About Tenable Network Security 42

Introduction

This document describes how to use Tenable Network Security's **Nessus Enterprise for AWS (Amazon Web Services)**. Please email any comments and suggestions to support@tenable.com.

AWS is a flexible, scalable, and low-cost cloud computing platform that offers businesses on-demand delivery of IT resources with pay-as-you-go pricing. With AWS, you can develop, launch, and operate software applications without any administrative overhead or worrying about having enough computing, storage, and database resources. However, one big area of concern remains for your software on AWS: security.

As a result, Amazon has teamed with Tenable Network Security to provide you with the industry-leading Nessus application vulnerability scanning solution. Amazon recommends that all new and existing AWS customers scan their AWS instances with Nessus while in development and operations, before publishing to AWS users.

Tenable Network Security offers two products on the AWS environment:

- Nessus for AWS is a Nessus Enterprise instance already available in the AWS Marketplace. Tenable Nessus for AWS provides **pre-authorized scanning** in the AWS cloud via AWS instance ID.
- The Nessus Bring Your Own License (BYOL) is a Nessus scanner installed in AWS that can scan targets outside the AWS infrastructure in a Bring Your Own License model. Customers interested in leveraging Nessus to secure their instance 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 a Nessus instance directly from your AWS account.

Requirements

This document covers Nessus Enterprise for AWS, and makes the assumption that the reader understands the basic concepts and usage in Amazon AWS. This includes:

- EC2 (Amazon Elastic Compute Cloud)
- AMIs (Amazon Machine Images)
- Instances
- IAM (Amazon Identity and Access Management)
- Elastic IP addresses

For more details, see the Amazon AWS User Guide at http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/concepts.html.

Standards and Conventions

Throughout the documentation, filenames, daemons, and executables are indicated with a **`courier bold`** font such as **`gunzip`**, **`httpd`**, and **`/etc/passwd`**.

Command line options and keywords are also indicated with the **`courier bold`** font. Command line examples may or may not include the command line prompt and output text from the results of the command. Command line examples will display the command being run in **`courier bold`** to indicate what the user typed while the sample output generated by the system will be indicated in `courier` (not bold). Following is an example running of the Unix **`pwd`** command:

```
# pwd
/opt/nessus/
```

Important notes and considerations are highlighted with this symbol and grey text boxes.

Tips, examples, and best practices are highlighted with this symbol and white on blue text.

Nessus Enterprise for AWS Overview

Nessus Enterprise for AWS is based on Nessus Enterprise, and is comprised of two components: the Nessus Enterprise for AWS Manager and the Nessus Enterprise for AWS Scanner. The Nessus Enterprise for AWS Manager provides the User Interface (UI) that controls the scanners, configures Nessus, manages user accounts, creates and runs scans, and views reports.

The primary features that denote the differences between Nessus Enterprise for AWS and Nessus Enterprise are:

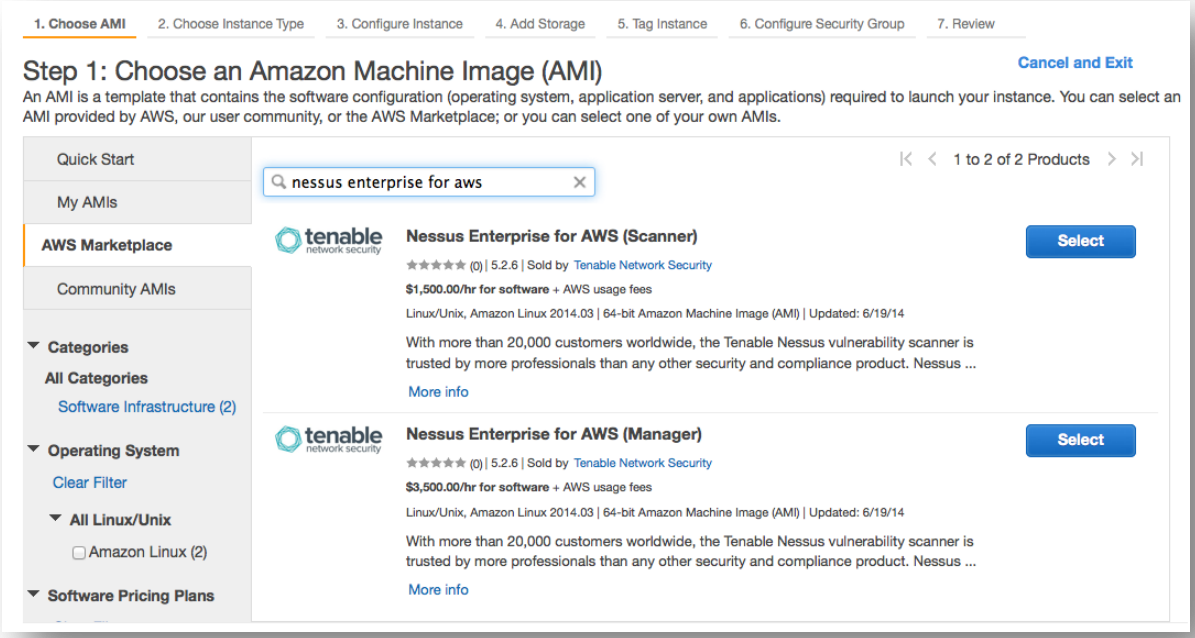
- Nessus Enterprise for AWS Manager WebUI listens on TCP port 443. Other Nessus products use a default TCP port of 8834.
- Nessus Enterprise for AWS runs on Amazon Linux, which is Amazon's own distribution of Linux designed to run on EC2. More details on Amazon Linux are available here: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AmazonLinuxAMIBasics.html.
- Nessus Enterprise for AWS instances will change their IP addresses and hostnames if they are shut down and restarted (not terminated). You will need to keep track of the AWS instance ID so you can correctly reconfigure the Nessus Enterprise for AWS Scanner if the Nessus Enterprise for AWS Manager is restarted.
- Users must have an AWS key pair set up and have a copy of the private key on their local system in order to log in. The AWS key pair is used for SSH user public key access only and will have no effect on the UI functionality.
- Nessus Enterprise for AWS scanners can only scan AWS instances by instance IDs. Nessus Enterprise for AWS can support other Nessus scanners to scan other systems by IP address.

Provisioning the Nessus Enterprise for AWS Instances

To create a Nessus Enterprise for AWS instance, go to the AWS Marketplace. The AWS Marketplace may be reached through the direct URL (https://aws.amazon.com/marketplace/) or via your EC2 dashboard.

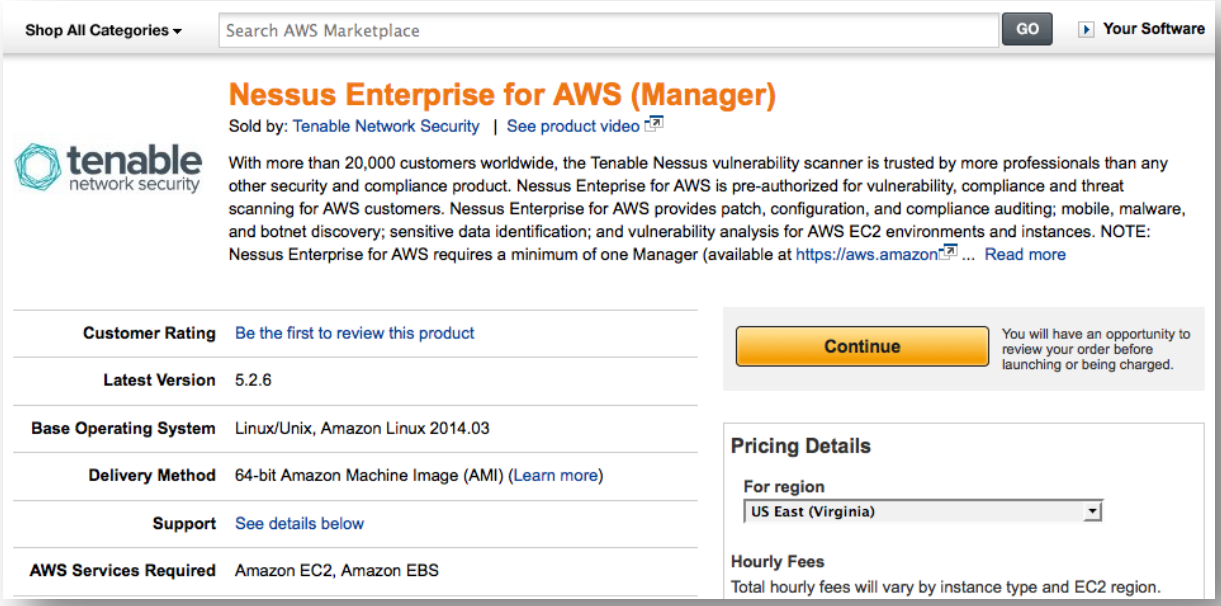
To access the AWS Marketplace through the EC2 dashboard:

1. Log in to the Amazon EC2 Console.
2. Click on "**Launch Instance**".
3. Choose "**AWS Marketplace**".



Adding a Nessus Enterprise for AWS Manager Instance

To add a Nessus Enterprise for AWS Manager instance, go to the AWS Marketplace and select the "**Nessus Enterprise for AWS (Manager)**".



Click "**Continue**" after reviewing the pricing details for the desired region.

Nessus Enterprise for AWS (Manager)

Sold by: Tenable Network Security

With more than 20,000 customers worldwide, the Tenable Nessus vulnerability scanner is trusted by more professionals than any other security and compliance product. Nessus Enteprise for AWS is pre-authorized for vulnerability, compliance and threat scanning for AWS customers. Nessus Enterprise for AWS provides patch, configuration, and compliance auditing; mobile, malware, and botnet discovery; sensitive data identification; and vulnerability analysis for AWS EC2 environments and instances. NOTE: Nessus Enterprise for AWS requires a minimum of one Manager (available at https://aws.amazon ... Read more

Customer Rating	Be the first to review this product
Latest Version	5.2.6
Base Operating System	Linux/Unix, Amazon Linux 2014.03
Delivery Method	64-bit Amazon Machine Image (AMI) (Learn more)
Support	See details below
AWS Services Required	Amazon EC2, Amazon EBS
Highlights	▪ Pre-authorized for vulnerability, compliance and threat scans of AWS environments with the largest collection of network security checks and configuration and compliance audits. ▪ Easy for security, IT, and audit teams to collaborate - sharing scanners, policies, schedules, and reports ▪ Easy configuration and management: policy creation wizards, scan scheduling, and multi-scanner control

Product Description

With more than 20,000 customers worldwide, the Tenable Nessus vulnerability scanner is trusted by more professionals than any other security and compliance product. Nessus Enteprise for AWS is pre-authorized for vulnerability, compliance and threat scanning for AWS customers. Nessus Enterprise for AWS provides patch, configuration, and compliance

Continue

You will have an opportunity to review your order before launching or being charged.

Pricing Details

For region

US East (Virginia)

Hourly Fees

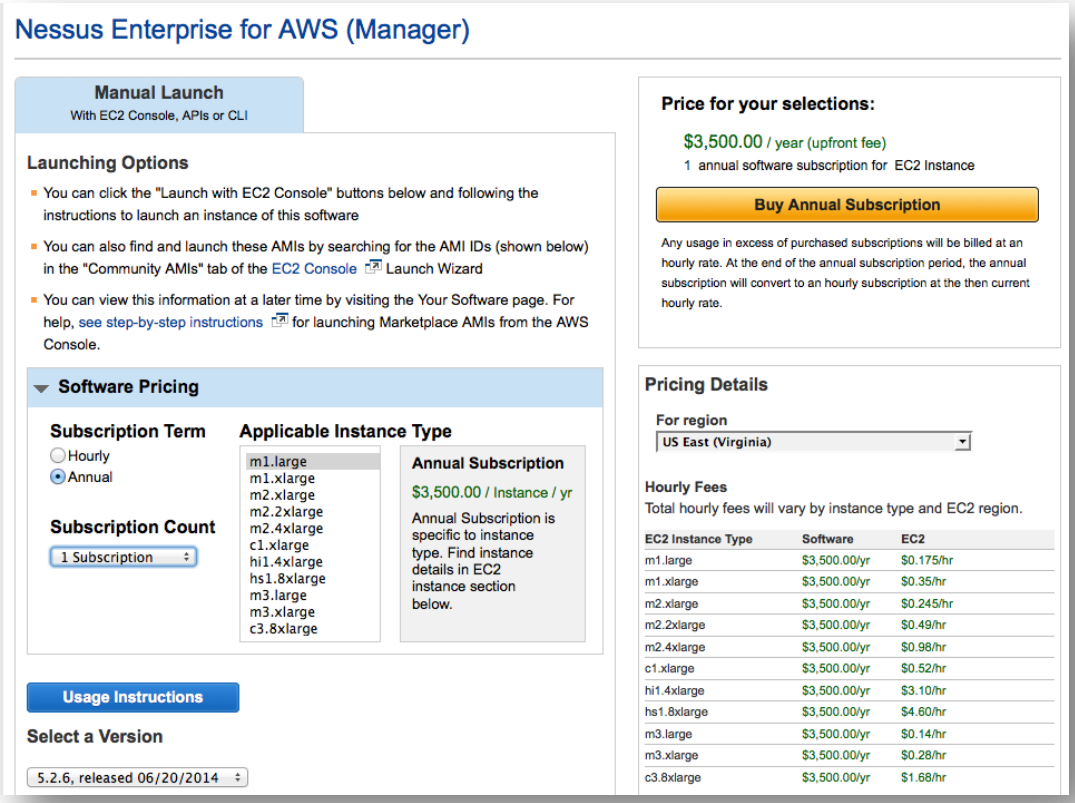
Total hourly fees will vary by instance type and EC2 region.

Software Pricing: Hourly Annual

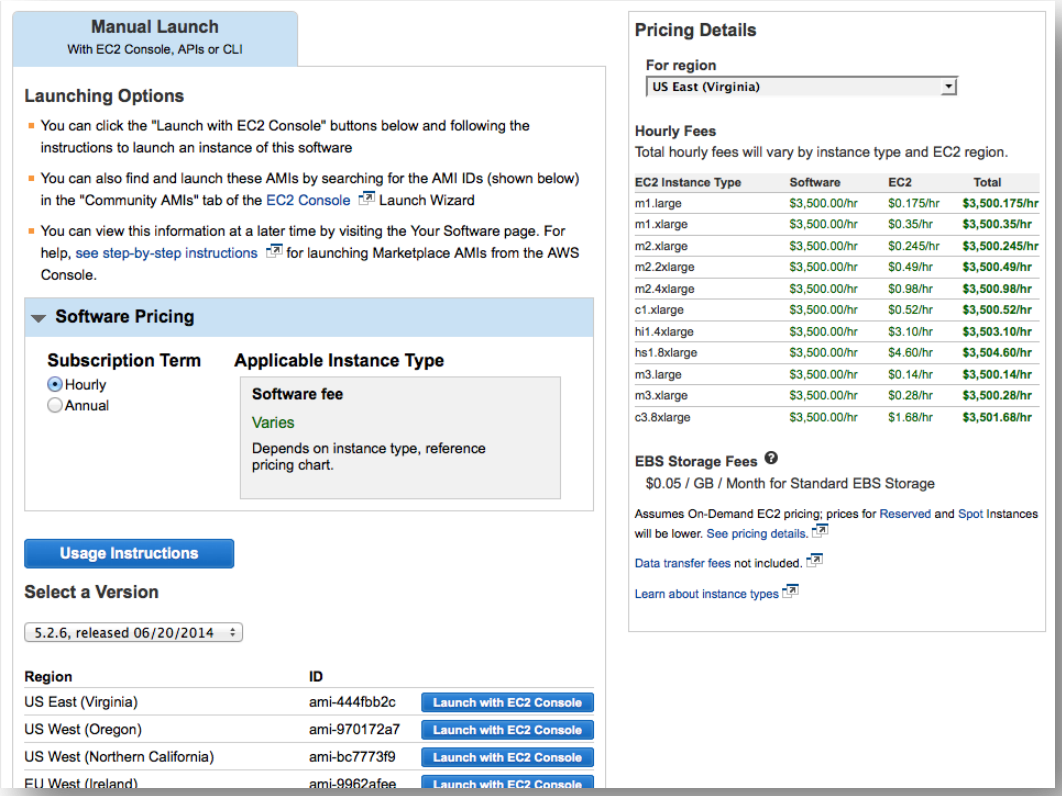
EC2 Infrastructure		Software	
Instance Type	Usage	Price	Savings
m1.large	$0.175/hr	$3,500/yr	100%
m1.xlarge	$0.35/hr	$3,500/yr	100%
m2.xlarge	$0.245/hr	$3,500/yr	100%
m2.2xlarge	$0.49/hr	$3,500/yr	100%
m2.4xlarge	$0.98/hr	$3,500/yr	100%
c1.xlarge	$0.52/hr	$3,500/yr	100%
hi1.4xlarge	$3.10/hr	$3,500/yr	100%
hs1.8xlarge	$4.60/hr	$3,500/yr	100%
m3.large	$0.14/hr	$3,500/yr	100%
m3.xlarge	$0.28/hr	$3,500/yr	100%
c3.8xlarge	$1.68/hr	$3,500/yr	100%

To view the software pricing terms: “**Hourly**” or “**Annual**”. Hourly pricing varies, depending on the type of instance selected. Annual pricing is a fixed cost paid for upfront. Click “**Continue**” after selecting your pricing terms.

Selecting the annual subscription will change the interface and add a “**Buy Annual Subscription**” button to the screen. Note that you will still need to select your instance type and number of subscriptions:



To launch an hourly instance, select the instance region and manually create the instance. Click on "**Launch with EC2 Console**" in the region of your choice. The browser will open a new tab, producing an instance based on the Nessus Enterprise for AWS Manager AMI.



For details on how to configure an instance, see the Amazon AWS EC2 documentation at http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Instances.html.

> AWS will need a new security group that allows inbound HTTPS (TCP port 443) and SSH (TCP port 22) on the Nessus Enterprise for AWS Manager. The scanners and the web UI use TCP port 443 instead of 8834 for communication with the manager.

Tenable requires the following for the Manager instance to work correctly:

- **m3.large** size instance or larger
- Security group allowing inbound TCP ports 443 (HTTPS) and 22 (SSH)
- An AWS keypair for SSH access
- Use an elastic IP address to identify your Manager instance

User management of the Nessus 5 server is conducted through a web interface on Nessus Enterprise for AWS Manager.

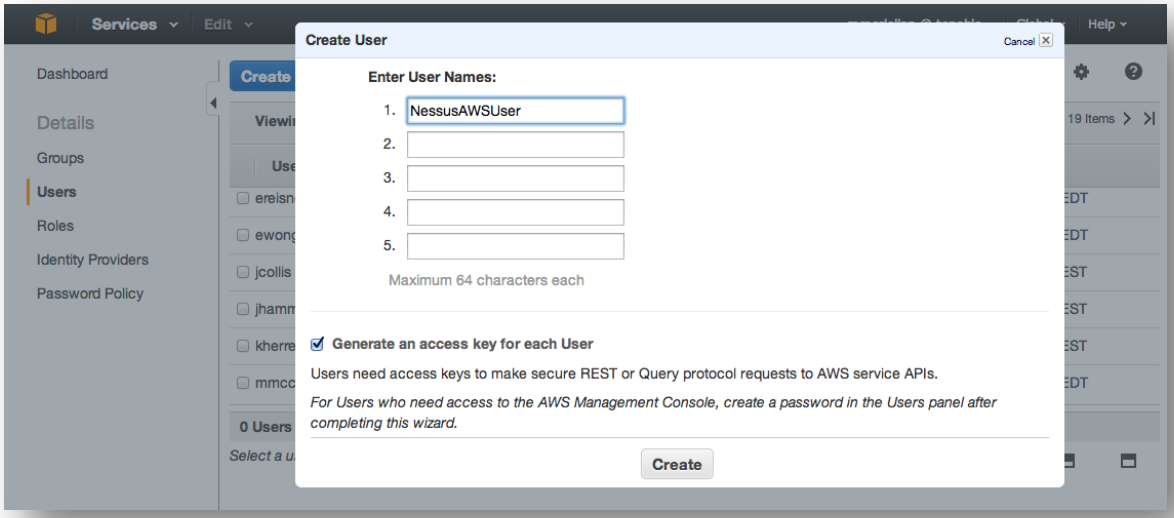
> AWS offers elastic IP addresses for associating a static public IP address to an AWS instance. More information on setting up an elastic IP address is available here http://aws.amazon.com/articles/1346.

Adding AWS User with Correct Permissions for Nessus Enterprise for AWS API Access

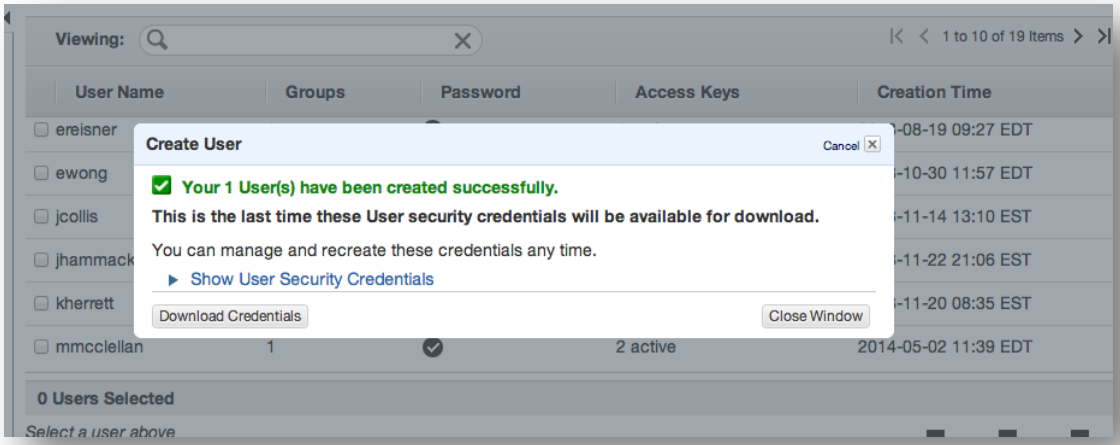
In order to add an EC2 user to your Nessus for AWS Manager instance, the EC2 user needs to be setup with the correct permissions.

To setup the correct permissions:

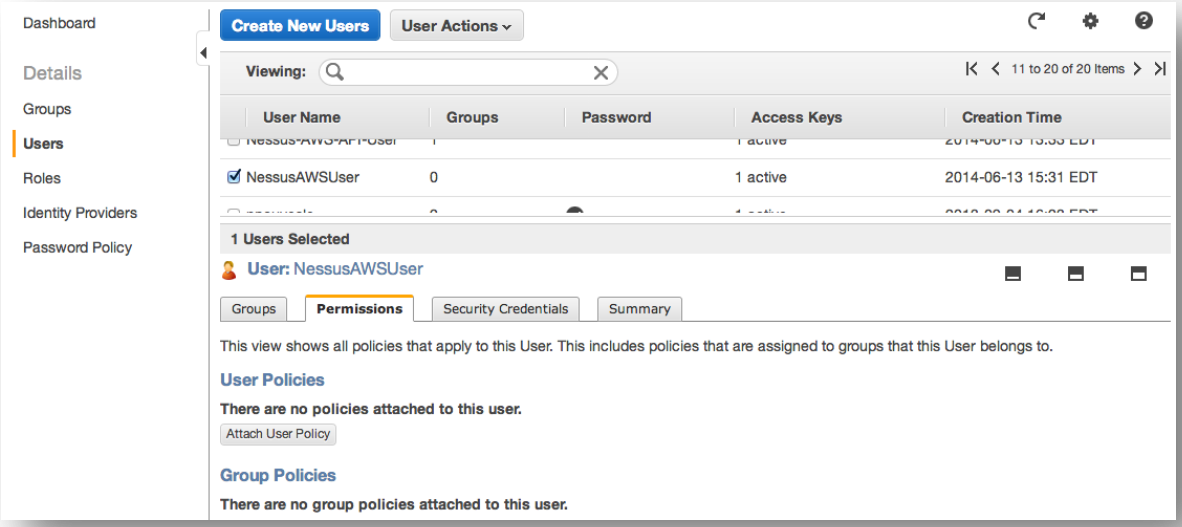
1. Log in to the AWS Console.
2. Select **IAM** (Identify and Access Management). This may be available from the left side of the dashboard or from the **"Edit"** drop down.
3. Click on **Users** on the left hand side.
4. Click on the **Create New Users** button.
5. Enter the user's name. Make sure the **Generate an access key for each User** checkbox is selected; you will need the access key during configuration of Nessus Enterprise for AWS Manager. Click **Create**.



6. In the **Create User** dialog, click on **Download Credentials**. This will download a CSV file with the User's username, AWS Access Key, and AWS Secret Key. Then click **Close Window**.

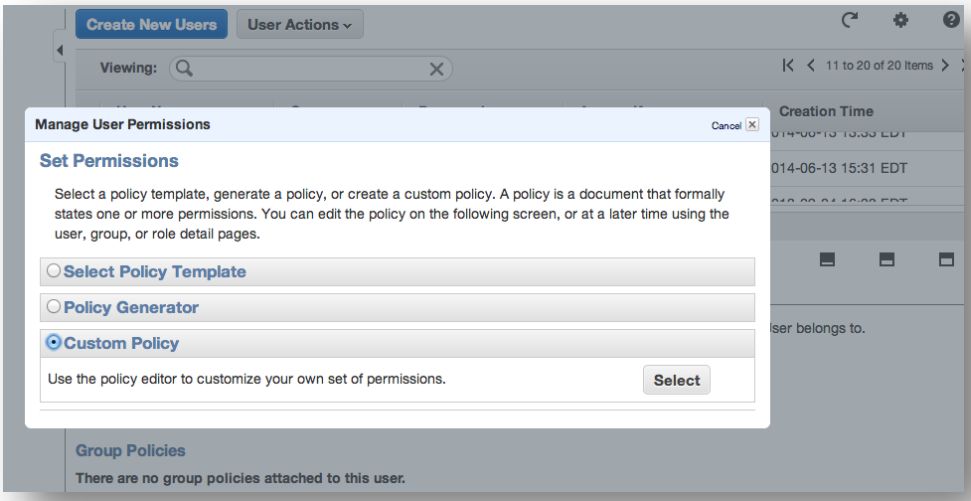


7. Select the newly created user from the list of users, and then click on the **Permissions** tab.



8. Click on "**Attach User Policy**". The **Manage User Permissions** window will display.

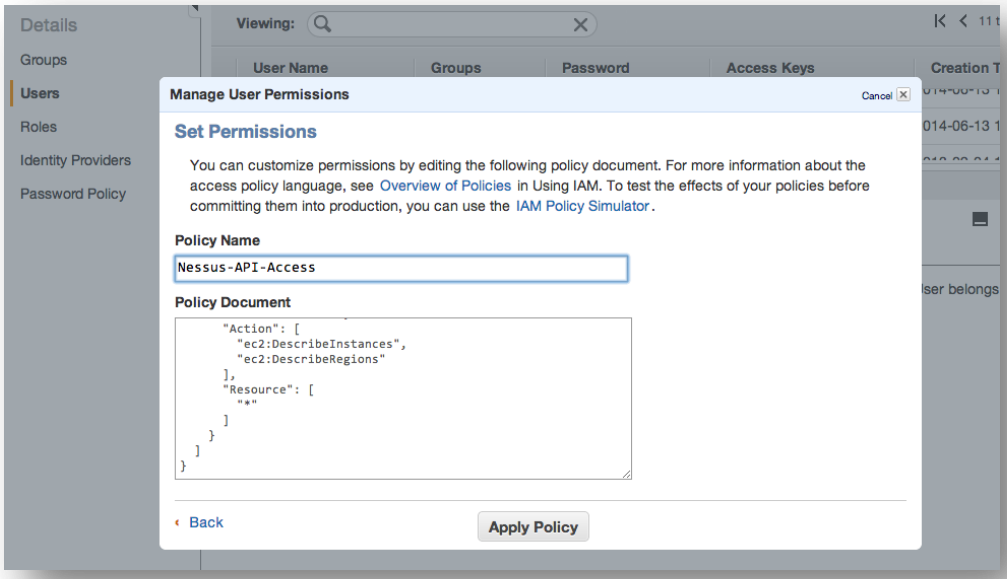
9. Select "**Custom Policy**", then click "**Select**".



10. Enter the "**Policy Name"**, then paste the following text into the "**Policy Document**" window:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1402678666000",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeInstances",
        "ec2:DescribeRegions"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

11. Click on "**Apply Policy**".



Using the EC2 access key from the credentials file is described in the **Setting up AWS instance authentication** later in this document.

Operations

Log in via SSH to Nessus Enterprise for AWS Manager or Scanner

To log in via SSH to your Nessus AWS Manager or Scanner, use the following format:

```
$ ssh -i your-aws-key.pem ec2-user@hostname.amazonaws.com
Last login: Wed Jun  4 22:08:32 2014 from mobile-198-228-213-218.mycingular.net

       __|  __|_  )
       _|  (     /   Amazon Linux AMI
      ___|\___|___|

https://aws.amazon.com/amazon-linux-ami/2014.03-release-notes/
$
```

The AWS key pair is in a supported SSH key format, which most SSH implementations, including OpenSSH, use. To use other SSH implementations such as PuTTY, refer to the AWS documentation on key pairs: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-key-pairs.html.

Connect to Nessus UI

To launch the Nessus Enterprise for AWS Manager UI, perform the following:

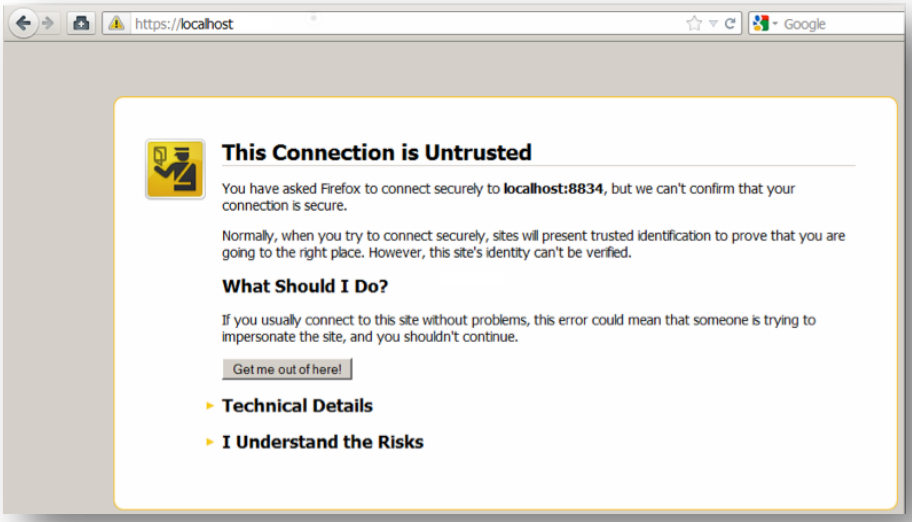
- Open a web browser of your choice.
- Enter `https://[server IP]/` in the navigation bar.

> Be sure to connect to the user interface via HTTPS, as unencrypted HTTP connections are not supported.

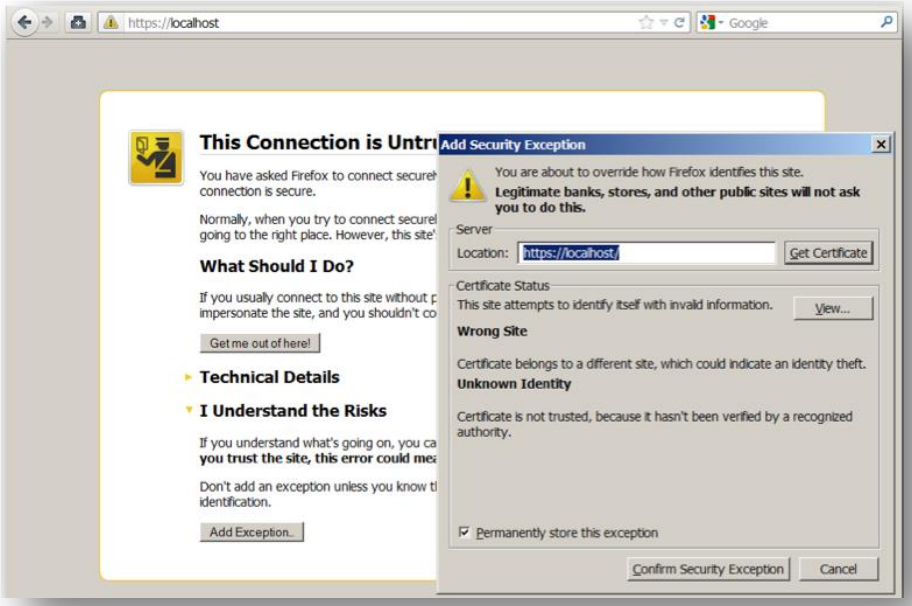
Configuring the Nessus Enterprise for AWS Manager

The first time you connect to the Nessus web server, your browser will display an error indicating the connection is not trusted due to a self-signed SSL certificate. For the first connection, accept the certificate to continue configuration. Instructions for installing a custom certificate are covered in the Nessus 5.2 Installation and Configuration Guide, in the "**Configuring Nessus with Custom SSL Certificate**" section.

> The technical implementation of SSL certificates prevents Nessus from including a certificate that would be trusted by browsers. To avoid this warning, a custom certificate to your organization must be used.

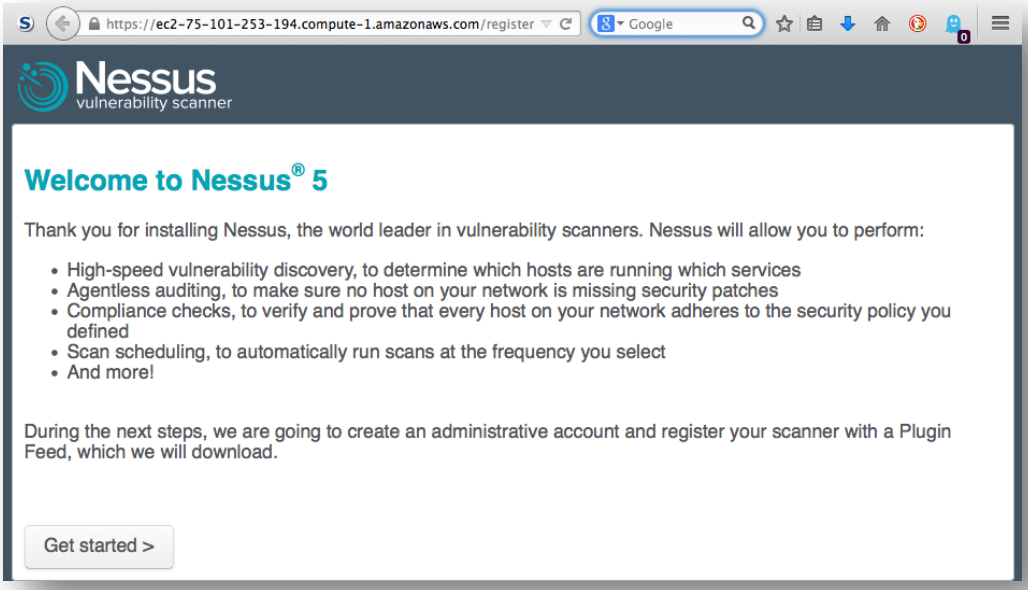


Depending on the browser you use, there may be an additional dialog that provides the ability to accept the certificate:

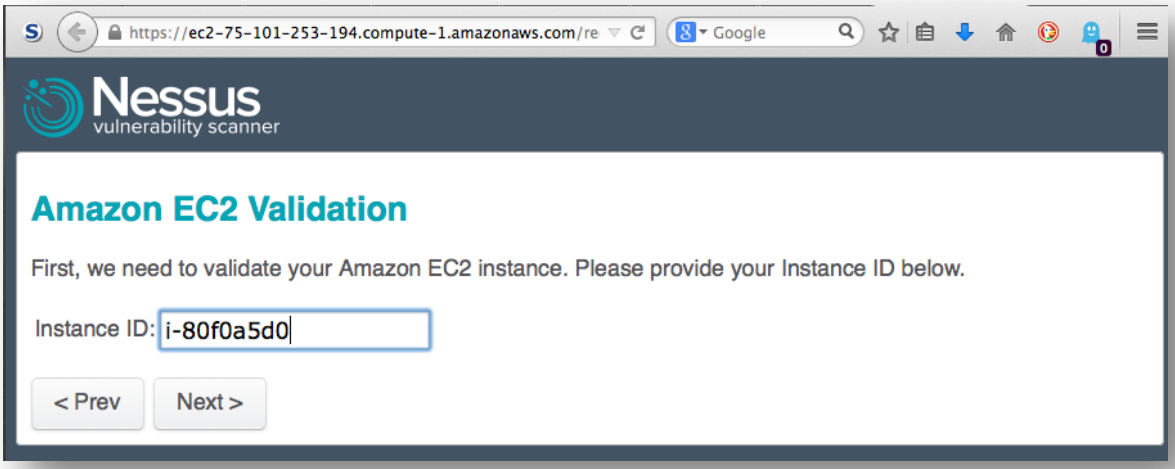


Nessus Enterprise for AWS Manager Installation

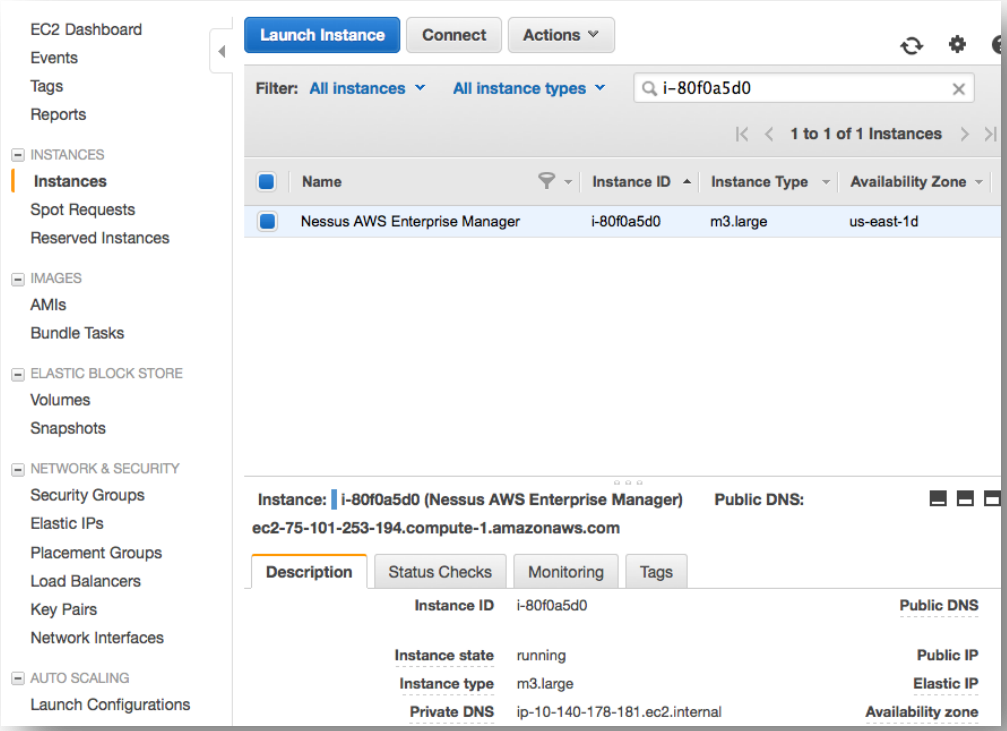
Once the certificate is accepted, you will be redirected to the initial registration screen that begins the installation walk-through:



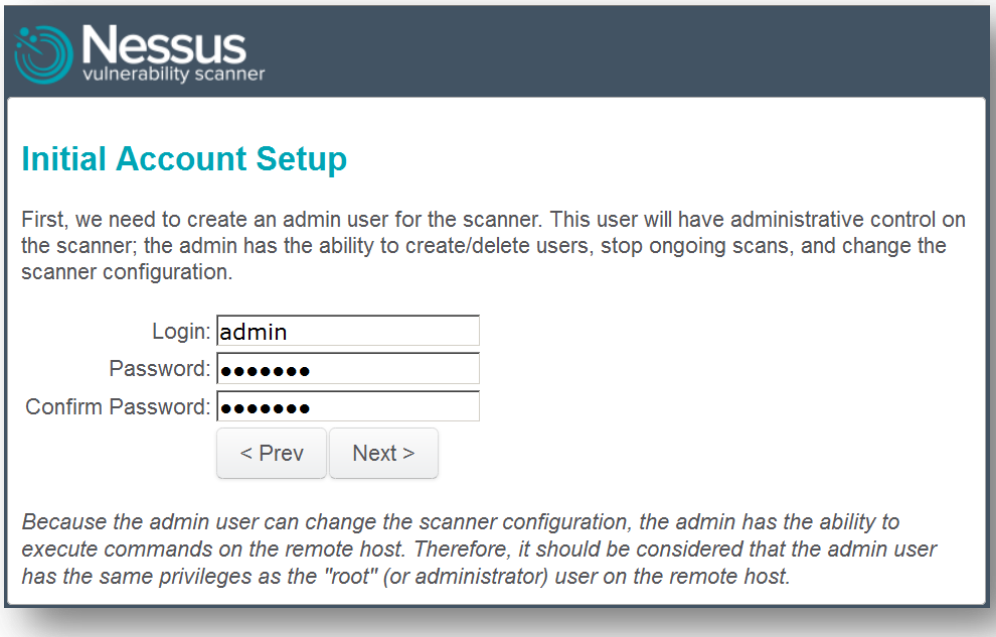
Click the "**Get Started >**" button to go to the next screen:



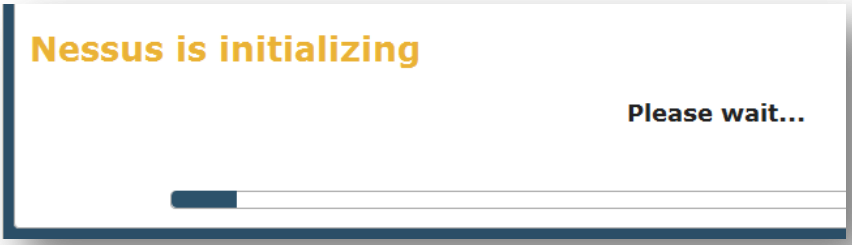
Enter the instance ID of your Nessus Enterprise for AWS Manager. You can find the instance ID in your list of "**Instances**" in the AWS EC2 Console, as shown below:



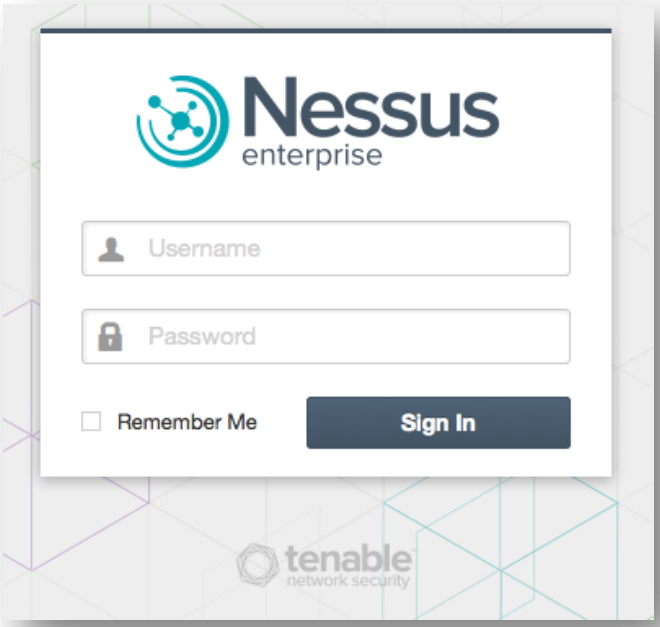
The next step is to create an account for the Nessus Enterprise for AWS Manager. The initial account will have administrative control of the manager and scanner. Note that this account has permission to execute commands as a privileged user on the underlying OS of the Nessus installation:



Once the administrator account is set up, the Nessus GUI will initialize and the Nessus server will start:



After initialization, Nessus is ready for use!

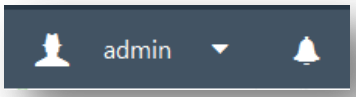


Using the administrative credentials created during the installation, log in to the Nessus interface to verify access.

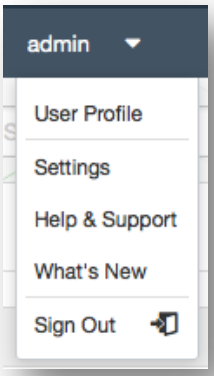
Authenticate using the administrative account and password previously created during the installation process. When logging in, you can optionally instruct your browser to remember the username on that computer. Only use this option if the computer is always in a secured location! After successful authentication, the UI will present menus to browse reports, conduct scans, and manage policies. Administrative users will also see options for user management and configuration options for the Nessus scanner.

Nessus Enterprise for AWS Manager Navigation

The bar displayed on the upper right hand side of the screen and shown in the screenshot below denotes the account currently logged in (in this example, the “admin” account), a drop-down menu, and a bell for quick access to important notifications related to Nessus operation.

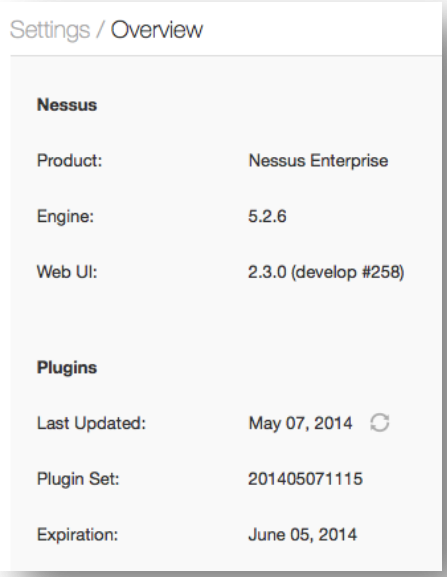


Clicking on the down arrow provides a menu containing options to access your user profile, general Nessus settings, information about the installation, help & support options, what's new in this release, as well as an option to sign out.

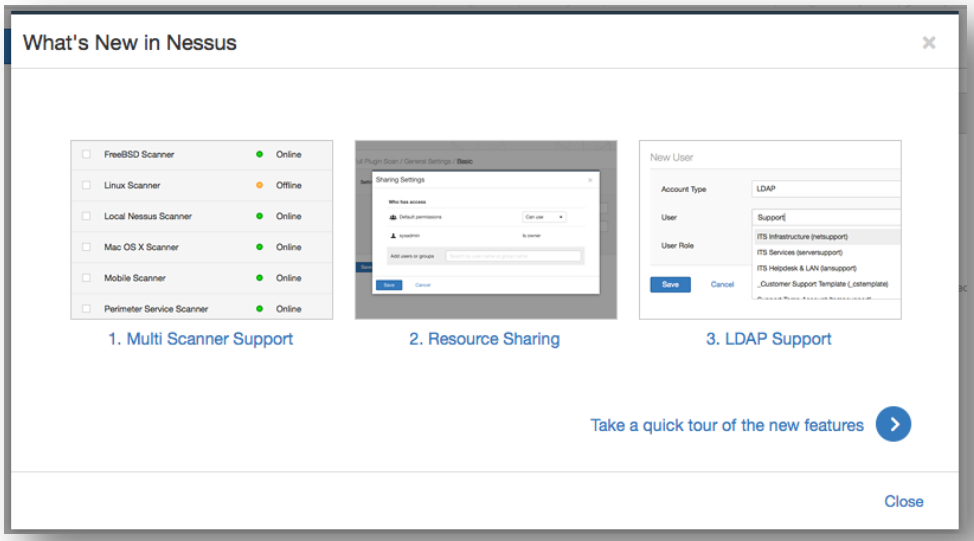


The "**User Profile**" option displays a menu with several pages of options related to the user account including the password change facility, folder management, and plugin rules page. For more information about these options, please refer to the Nessus 5.2 Enterprise User Guide under "**User Profile**".

The "**Settings**" option provides access to the "**Overview**" page, mail server configuration options (if administrator), plugin feed (if administrator), and advanced scanner options (if administrator). More information about these options can be found below.

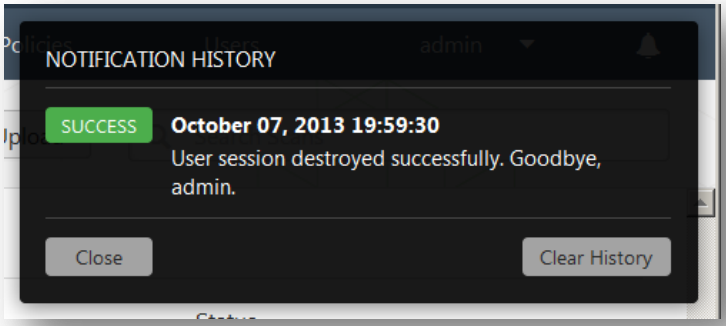


The “**What’s New**” link provides a quick tour of new features with this Nessus release. More information about each option can be found below the image. In this example, we see new features of a Nessus Enterprise for AWS release:

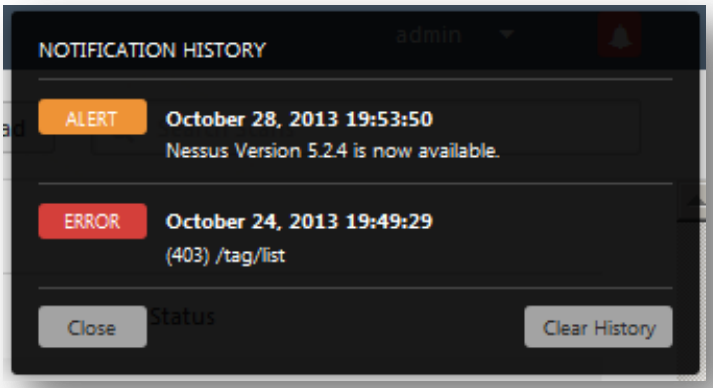


The “**Help & Support**” link loads the Tenable support page in a new tab or window. “**Sign Out**” terminates your current session with Nessus.

Clicking on the bell icon on the upper right side shows any messages related to Nessus operations including errors, notification of new Nessus releases, session events, and more:



This will also serve as a place to provide any additional alerts or errors via popups that will fade shortly after and stay in the notification history until cleared:



Interface Shortcuts

The HTML5 interface has several hotkeys that allow quick keyboard-navigation to the major sections of the interface, as well as performing common activities. These can be used at any time, from anywhere within the interface:

Main Interface	
R	Scans
N	Scans -> New Scan
S	Schedules
P	Policies
U	Users
G	Groups
C	Settings
M	User Profile
Creation	
Shift + R	New Scan
Shift + S	New Schedule
Shift + F	New Folder (Scan view only)
Schedules View	
N	New Schedule

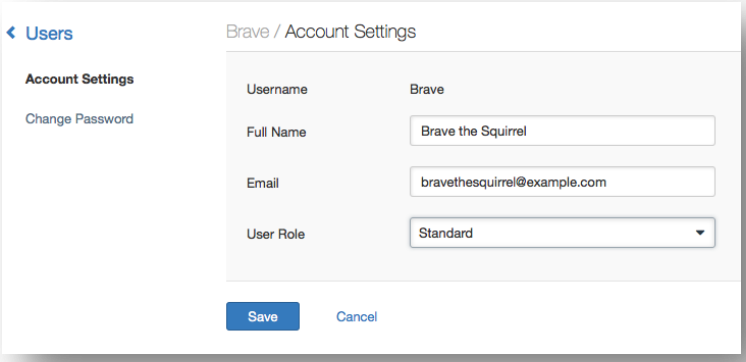
Scan View	
N	New Scan
Policy View	
N	New Policy
Users View	
N	New User
Schedules View	
N	New Schedule
Groups View	
N	New Group
Advanced Settings View	
N	New Setting

Nessus Enterprise for AWS Manager Settings

The Nessus Enterprise for AWS Manager settings controls users, groups, policies, and scanner control.

User Profile

The user profile options allow you to manipulate options related to your account.



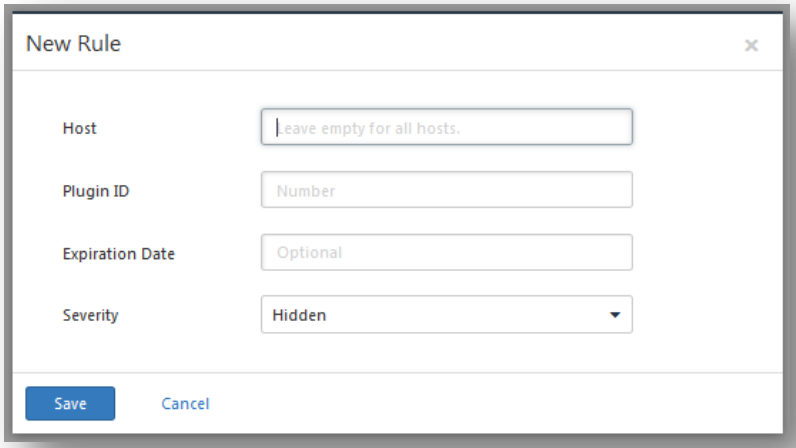
Click on the user account to change the options related to the account.

The "**Account Settings**" field shows the current authenticated user as well as the user role: **Read Only**, **Standard**, **Administrator**, or **System Administrator**. The default "**admin**" account has the user role **System Administrator**.

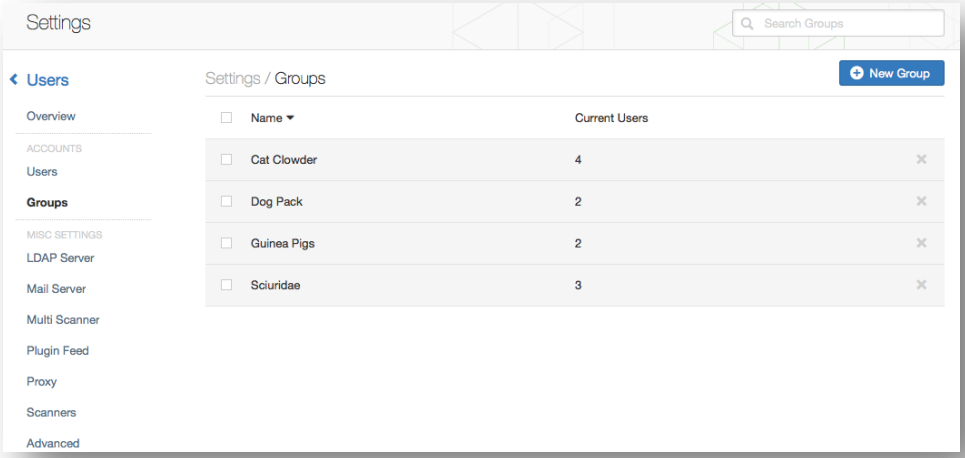
User Role	Description
Read Only	Users with the Read Only user role can only read scan results.
Standard	Users with the Standard user role can create scans, policies, schedules, and reports. They cannot change any user, user groups, scanner, or system configurations.
Administrator	Users with the administrator role have the same privileges as the standard user but can also manage users, user groups, and scanners.
System Administrator	Users with the system administrator role have the same privileges as the administrator and can also configure the system.

The "**Change Password**" option allows you to change the password, which should be done in accordance with your organization's security policy.

The "**Plugin Rules**" option provides a facility to create a set of rules that dictate the behavior of certain plugins related to any scan performed. A rule can be based on the Host (or all hosts), Plugin ID, an optional Expiration Date, and manipulation of Severity. The same rules can be set from the scan results page. This allows you to reprioritize the severity of plugin results to better account for your organization's security posture and response plan.



Users can be placed into groups, depending on their function or classification (e.g., Windows Administrators, Auditors, Firewall Administrators, or Security Analysts).



Account Settings

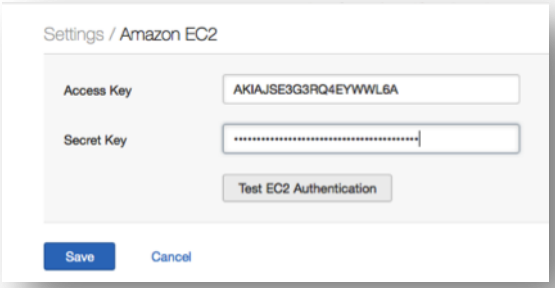
To configure account settings, including Users and Groups, please refer to the Nessus Installation and Configuration Guide under "**Configuration**".

Setting up the Nessus Enterprise for AWS Manager

Setting up AWS instance authentication

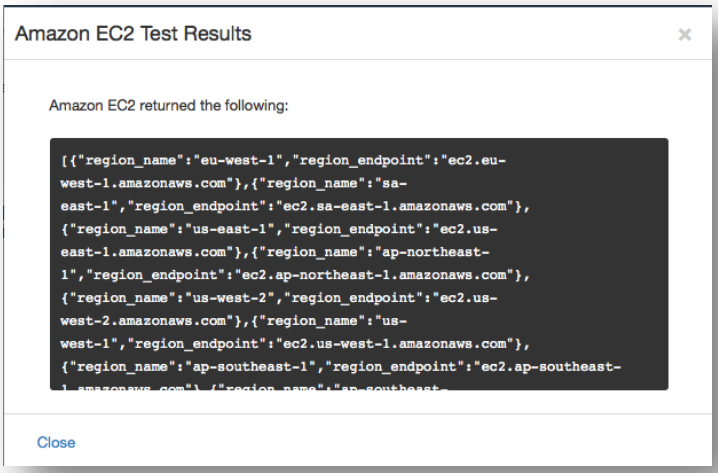
To scan your AWS instances, you need to authenticate the Nessus Enterprise for AWS Manager with your EC2 environment. The EC2 credentials are used by the Nessus Enterprise for AWS Manager to enumerate the user's instances via an AWS API call in order to build a list of possible scan targets.

To configure your EC2 credentials, navigate to "**Settings > Amazon EC2**". Enter your "**Access Key**" and "**Secret Key**" in their respective fields:

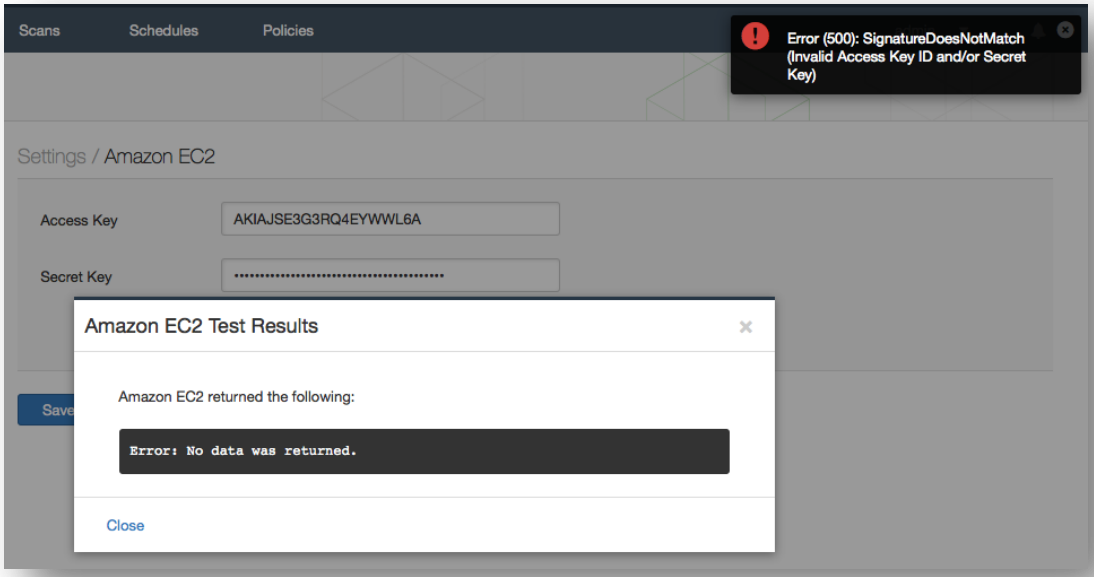


For more information on obtaining your AWS access and secret keys, please refer to "Managing Access Keys for your AWS Account" available here: http://docs.aws.amazon.com/general/latest/gr/managing-aws-access-keys.html.

Once the access and secret keys are entered correctly, you will see a message similar to this containing the JSON output indicating success:



If you entered your credentials incorrectly, you will see an error message similar to this:



LDAP Server Settings

To configure an LDAP server so users can authenticate to the Nessus server using LDAP domain credentials, please refer to the Nessus 5.2 Installation and Configuration Guide under "**Configuration**".

Mail Server Settings

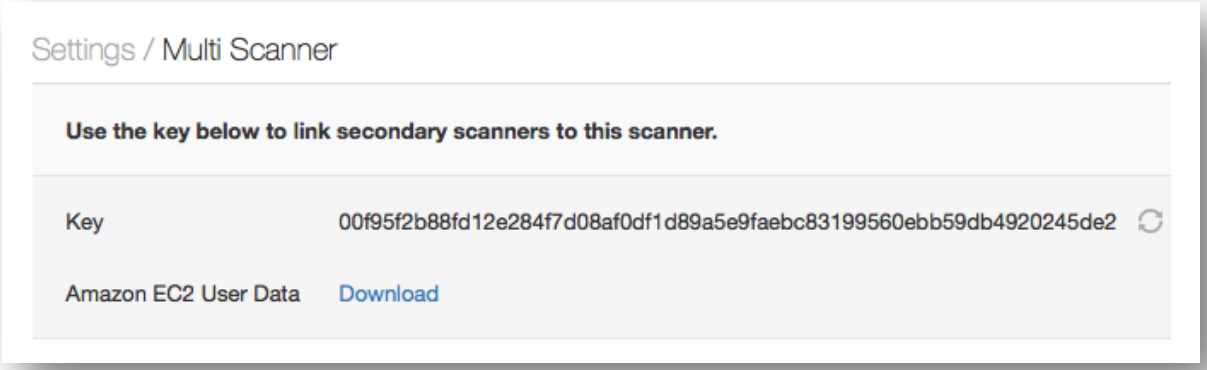
To configure an SMTP server to allow completed scans to automatically email the results, please refer to the Nessus 5.2 Installation and Configuration Guide under "**Configuration**".

Multi Scanner Setting

The Multi Scanner setting provides the key and EC2 user data for connecting scanners. To configure the scanner to connect to the manager, download the Amazon EC2 User Data text file, and upload it to the Nessus Enterprise for AWS

Scanners that are to be managed. This key is automatically generated and is only used for the initial linking of two scanners. Subsequent communication is performed via a separate set of credentials.

If there is concern over the shared secret becoming compromised, you can regenerate the key at any time by clicking the arrows to the right of the key. Regenerating the key will not disable any scanners that are already registered.



The contents of this file are in the following format:

```
{"key" : "00a42f2b88ff12e284f7d08af0df1d89a5e9fcabc93188560ebb59db4920245cf2",
"primary_hostname" : "10.1.1.100" }
```

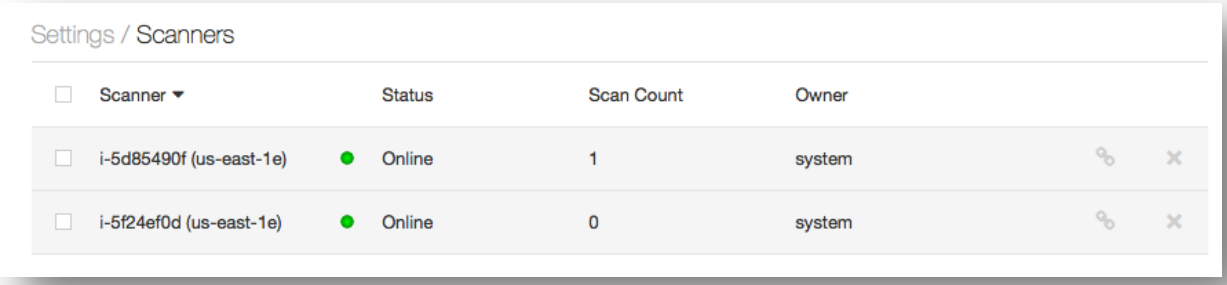
If you are using an Elastic IP for the Manager instance **and** the EIP was associated with the Manager after the instance had started, the EC2 user data file may need to be updated so that the **`primary_hostname`** field contains the EIP.

Scanners Settings

The "**Scanners**" tab shows available scanners, as defined by the "**Multi Scanner**" feature. If no scanners are configured, no scanners will be displayed on the AWS Nessus Manager.

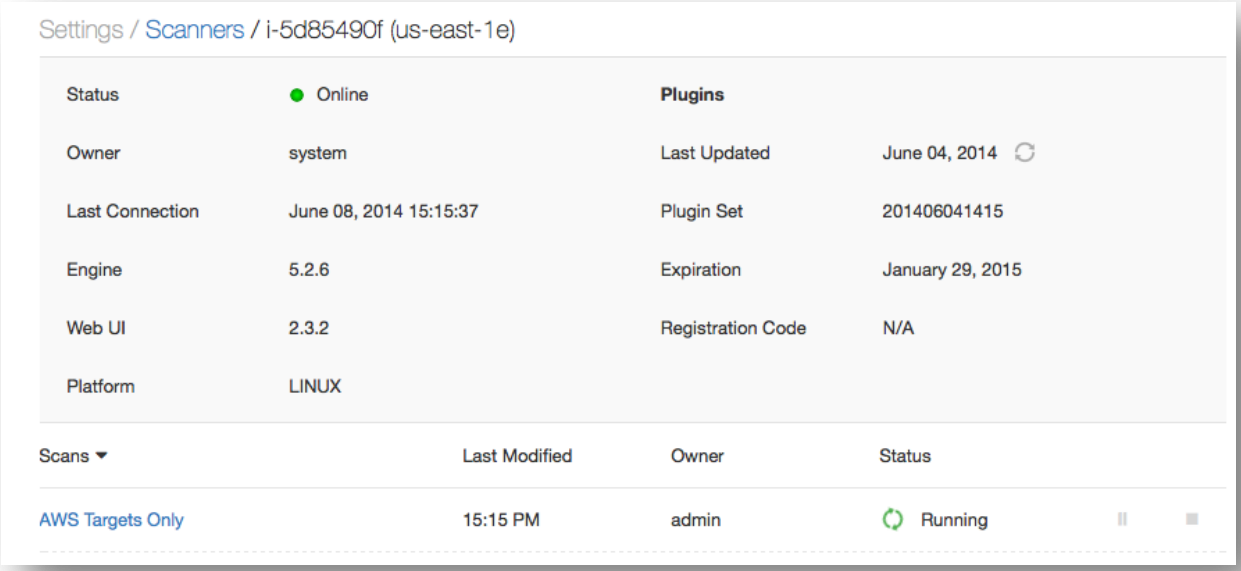
This setting allows Nessus scanners to work together to outsource and aggregate scanning activity. This administrator feature is explained in greater detail in the "Nessus 5.2 Enterprise User Guide" under the "**Multi Scanner**" section. At any time, you can unlink a scanner with the "**Unlink Scanner**" button.

Note the difference between Nessus Enterprise and Nessus Enterprise for AWS Manager is that the latter identifies scanners by instance ID and AWS region instead of by a user designated name:



Only Nessus Enterprise for AWS Scanners are identified with this type of designation.

Click on any individual scanner to see its settings and the status of any scans running on that system:

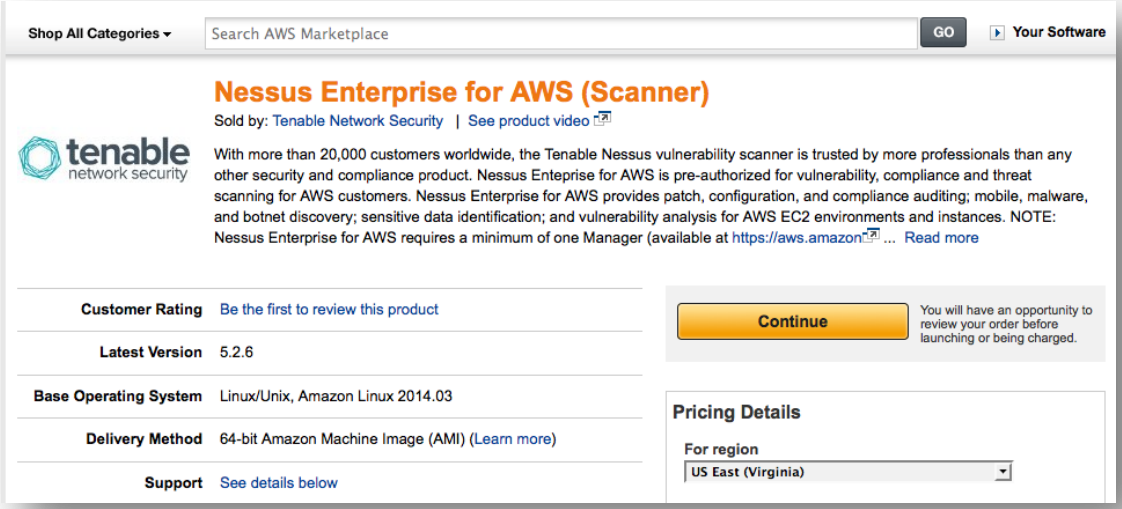


Advanced Settings

Nessus uses a wide variety of configuration options to offer more granular control of how the scanner operates. An administrative user can manipulate these settings from the "**Advanced**" tab via the drop-down on the top left. For more information on the Advanced Settings, please refer to the Nessus 5.2 Installation and Configuration Guide under "**Configuration**".

Adding a Nessus Enterprise for AWS Scanner Instance

To add a Nessus Enterprise for AWS Scanner instance, go to the AWS Marketplace and select the "**Nessus Enterprise for AWS (Scanner)**".



Click "**Continue**" after reviewing the pricing details for the desired region.

Click on "**Launch with EC2 Console**" in the region of your choice. The browser will open a new tab, producing an instance based on the Nessus for AWS Scanner AMI.

Tenable requires for the scanner instance to work correctly:

- **m3.medium** size instance or larger
- Security group allowing port 22 (SSH)
- An AWS keypair for SSH access

> Note that you will need to add both a Manager instance and a Scanner instance to successfully scan using Nessus Enterprise for AWS.

Configuring the Nessus Enterprise for AWS Scanner

Nessus Enterprise for AWS Scanners are only managed by the Nessus Enterprise for AWS Manager. They need to be configured in order to run scans.

Once the manager is configured and the EC2 User Data is downloaded, you will need to configure one or more scanners. There are two ways to configure scanners:

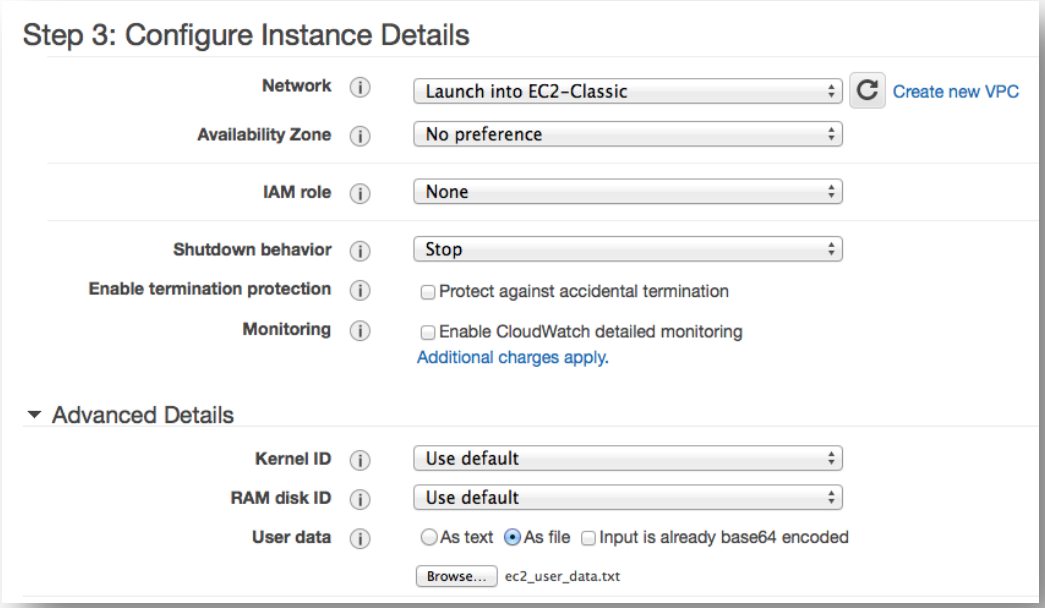
1. Add the EC2 User Data during the scanner instance creation.

2. Add the EC2 User Data after the scanner instance creation.

> Nessus Enterprise for AWS Scanner communicates with Nessus Enterprise for AWS Manager over TCP port 443; Nessus scanners typically communicate over TCP port 8834

Adding the EC2 User Data to the Nessus Enterprise for AWS Scanner instance

At the step "**Configure Instance Details**", select "**Advanced Details**". Click the radio button "**As file**".



Upload the "**ec2-user-data.txt**" file.

This is the credentials file "`ec2-user-data.txt`" downloaded from the "**Settings > Multi Scanner**" instructions in this document.

Creating the Security Group for the Nessus Enterprise for AWS Scanner instance

The security group for the Nessus Enterprise for AWS scanner will need SSH access using the default port 22.

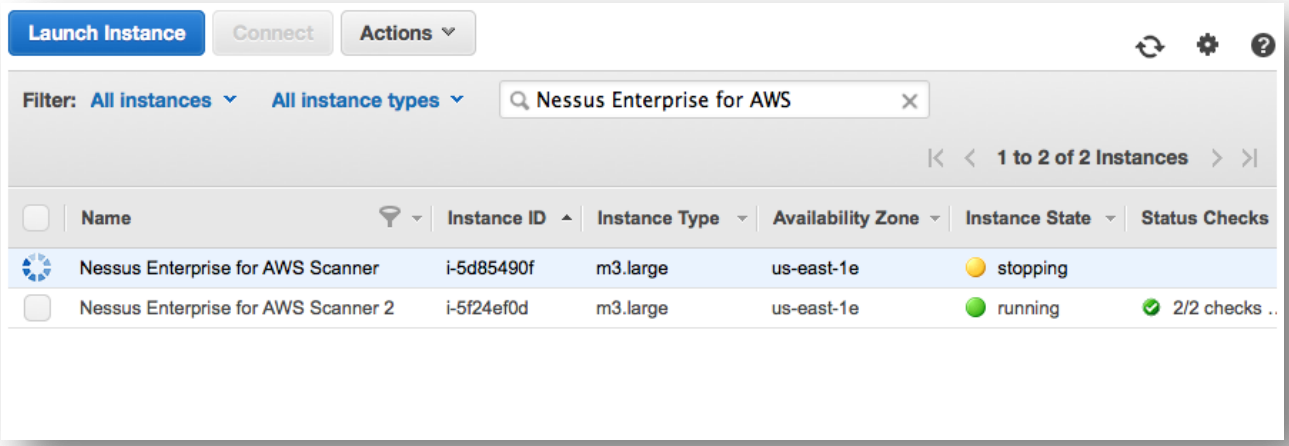
The scanner communicates with the manager internally on the AWS network. Therefore, no security group needs to be defined for the scanner to communicate with the manager.

> For more details on how to configure an instance, see the Amazon AWS EC2 documentation at http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Instances.html

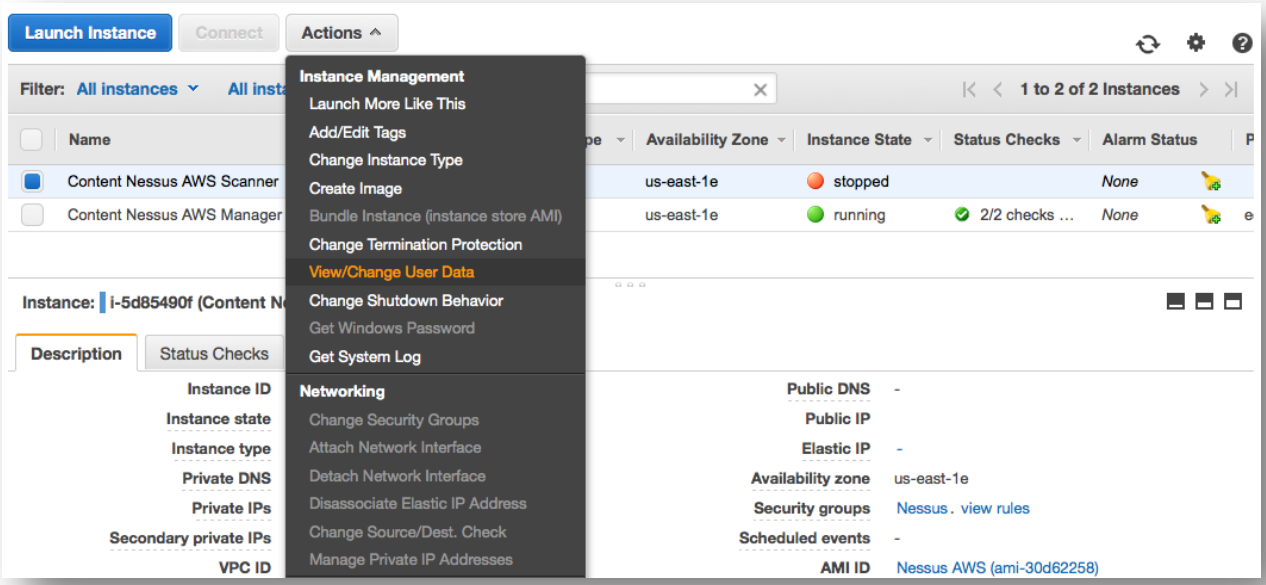
Adding the EC2 User Data to the Nessus Enterprise for AWS Scanner after instance creation

If the scanner instance exists and needs to be attached to a new Manager, you will need to perform the following to join the scanner to your Nessus Enterprise for AWS Manager:

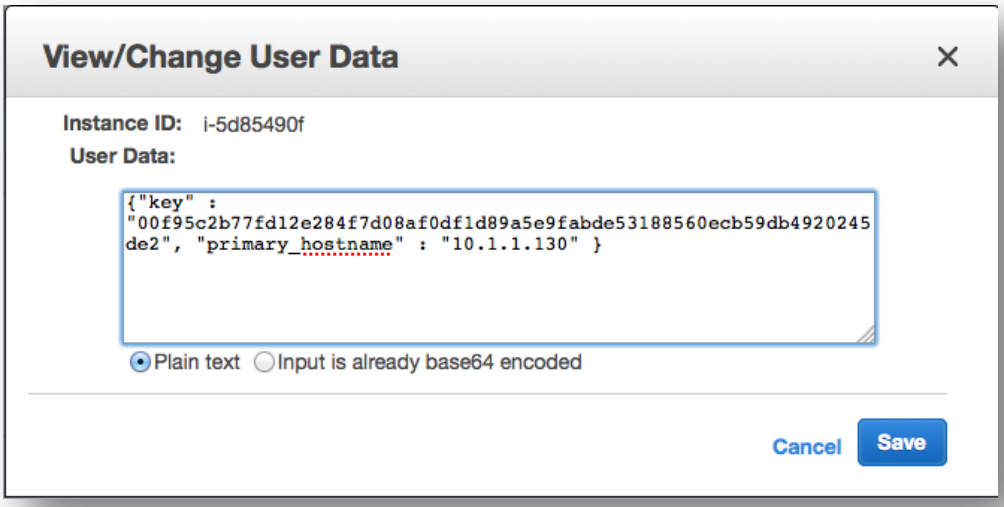
Select the desired scanner instance and stop it in the AWS EC2 environment:



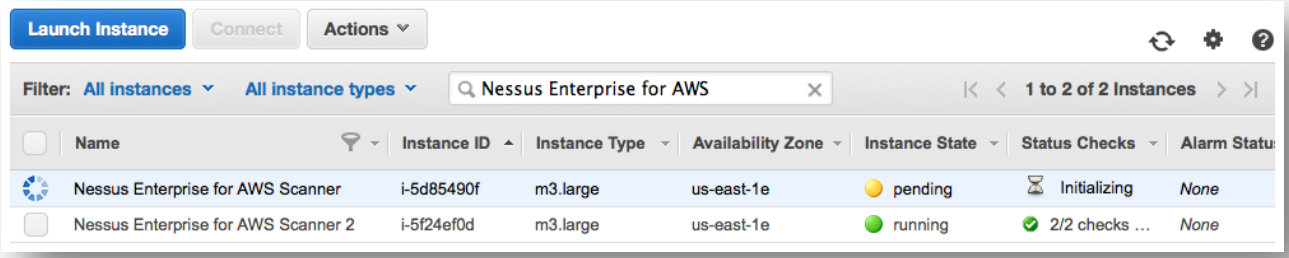
Once the instance has stopped, select the "**View/Change User Data**" in the "**Actions**" menu:



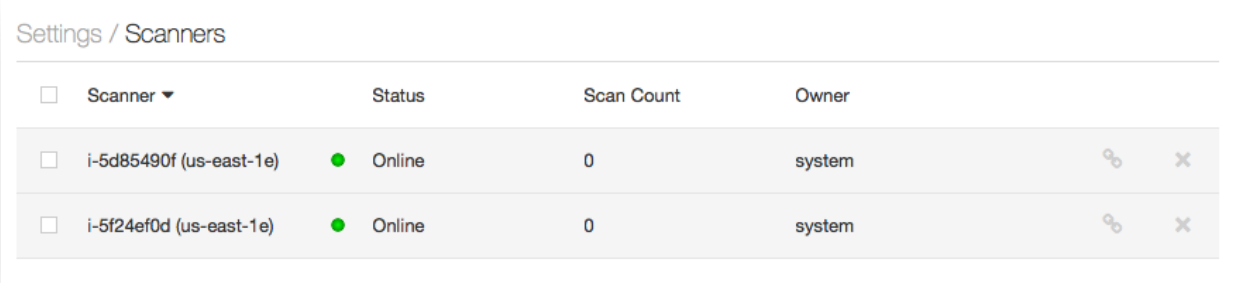
Cut and paste the contents of the `ec2_user_data.txt` in the text field, and click "**Save**":



Restart the scanner instance.



After the scanner is fully running, it will automatically connect with the Nessus Enterprise for AWS Manager. You will see the instance ID will match the one listed in the AWS EC2 console under **Settings > Scanners**:



Scanning using Nessus Enterprise for AWS Manager

Policies Overview

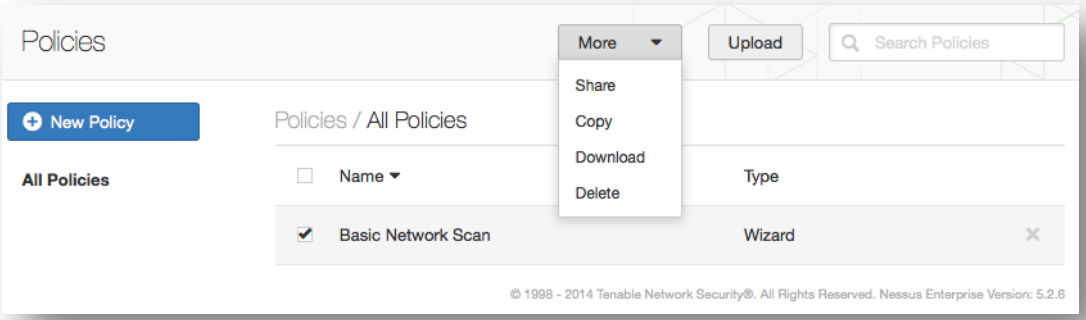
A Nessus policy consists of configuration options related to performing a vulnerability scan. These options include, but are not limited to:

- Parameters that control technical aspects of the scan such as timeouts, number of hosts, type of port scanner, and more.
- Credentials for local scans (e.g., Windows, SSH), authenticated Oracle database scans, HTTP, FTP, POP, IMAP, or Kerberos-based authentication.
- Granular family or plugin based scan specifications.
- Database compliance policy checks, report verbosity, service detection scan settings, Unix compliance checks, and more.

Once you have connected to Nessus Enterprise for AWS, you can create a custom policy by clicking on the "**Policies**" option on the bar at the top and then "**+ New Policy**" button toward the left. For more details on Nessus Enterprise policies, please refer to the Nessus 5.2 Enterprise User Guide under "**Creating a New Policy**".

Managing Policies

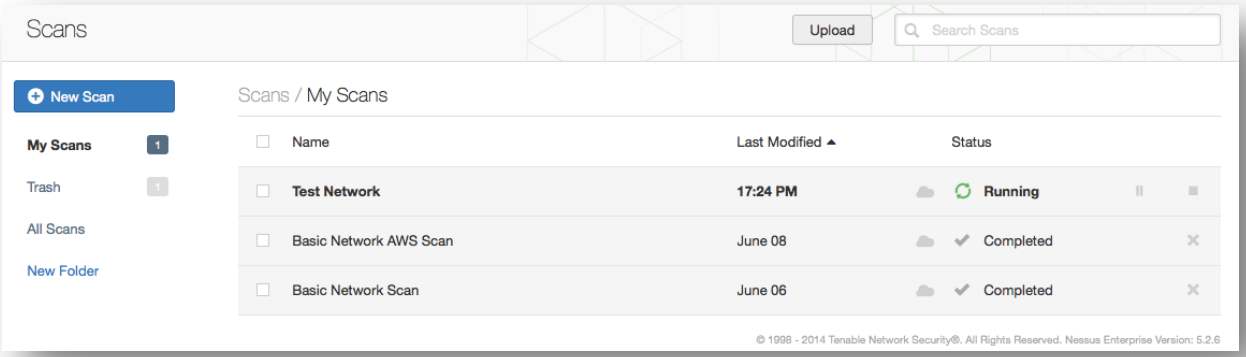
The "**Upload**" button on the Policies menu bar allows you to upload previously created policies to the scanner. For more information on managing policies, please refer to the Nessus 5.2 Enterprise User Guide under "**Sharing, Importing, Exporting, and Copying Policies**".



Creating, Launching, and Scheduling a Scan

Users can create their own report by chapters: Host Summary (Executive), Vulnerabilities by Host, Compliance Check (Executive), Suggested Remediations, Vulnerabilities by Plugin, or Compliance Checks. The HTML format is supported by default; however, it is also possible to export reports in PDF, CSV, or the Nessus DB formats. By using the report filters and export features, users can create dynamic reports of their own choosing instead of selecting from a specific list.

> Nessus DB format is an encrypted proprietary format. Note that the Nessus DB format contains all the possible data about a scan, including but not limited to the results, the audit trails and attachments.

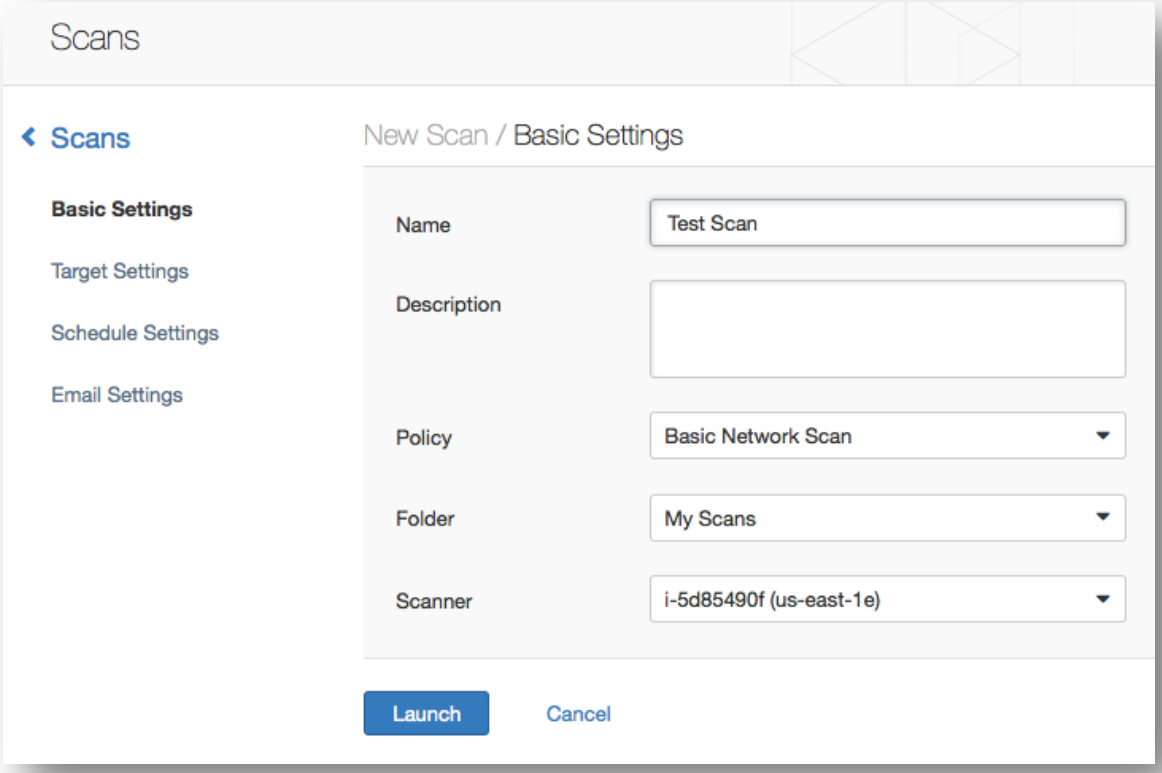


The following scan statuses are available in the scan list table:

Scan Status	Description
Completed	The scan is fully finished.
Running	The scan is currently in progress.
Canceled	The user stopped the scan before the end.
Aborted	The scan has been aborted due to an invalid target list or a server error (e.g., reboot, crash).
Imported	The scan has been imported using the upload functionality.

These statuses only apply to new scans. Old scans are all considered “Completed”. Scans with the same status can be listed through the virtual folders on the left navigation panel.

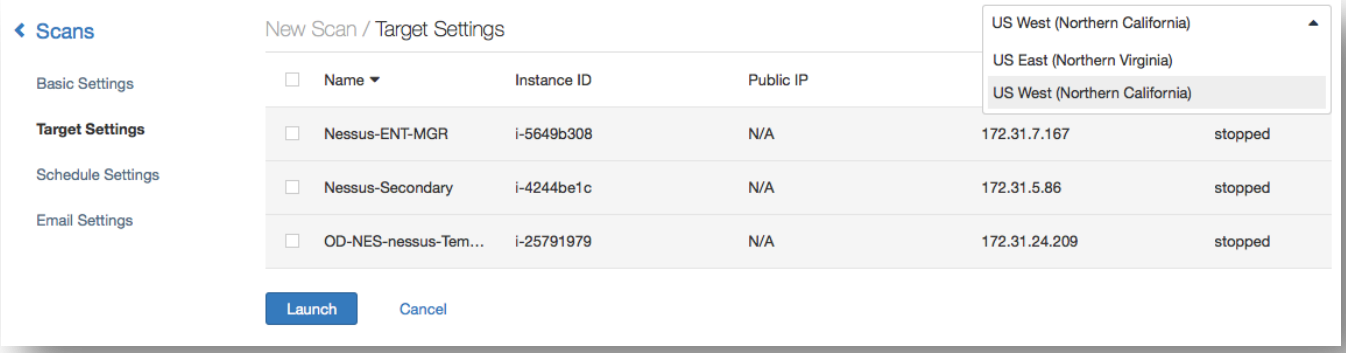
After creating or selecting a policy, you can create a new scan by clicking on the "**Scans**" option on the menu bar at the top and then click on the "**+ New Scan**" button on the left. The "**New Scan**" screen will be displayed as follows:



Under the "**Basic Settings**" tab, there are five fields to enter the scan target:

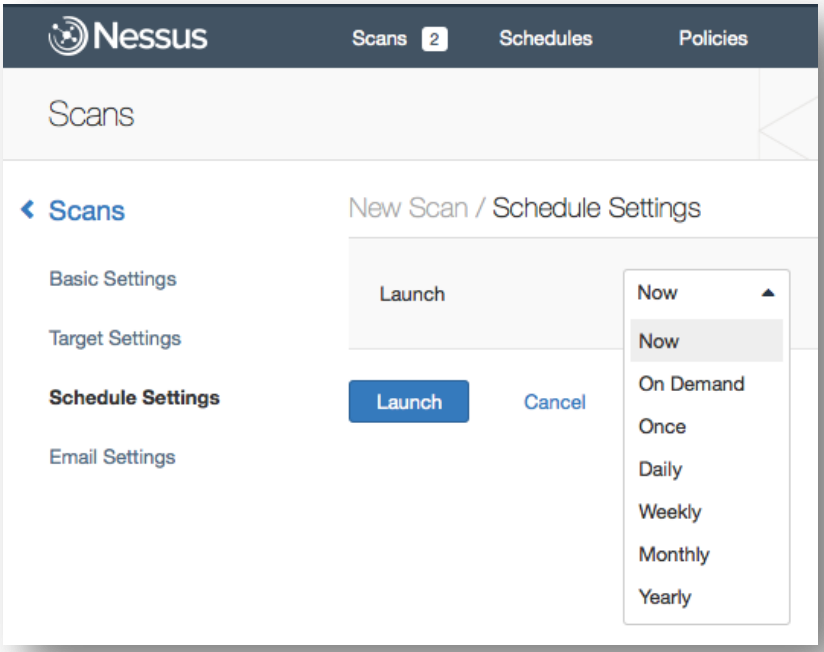
- **Name** – Sets the name that will be displayed in the Nessus UI to identify the scan.
- **Description** – Optional field for a more detailed description of the scan.
- **Policy** – Select a previously created policy that the scan will use to set parameters controlling Nessus server scanning behavior.
- **Folder** – The Nessus UI folder to store the scan results.
- **Scanner** – Which Nessus scanner to perform the scan. This will provide multiple options if you have configured additional Nessus scanners to be secondary to this one. Note that these Nessus Enterprise for AWS Scanners will be identified by their instance ID.

Under the "**Targets Settings**" tab, there is a series of checkboxes that allow you to select your targets. Selecting the first checkbox will select all instances in specified region:



The only targets you will be allowed to scan are other recognized Amazon instances. "Micro" and "small" instances will not be listed; Amazon forbids scanning these.

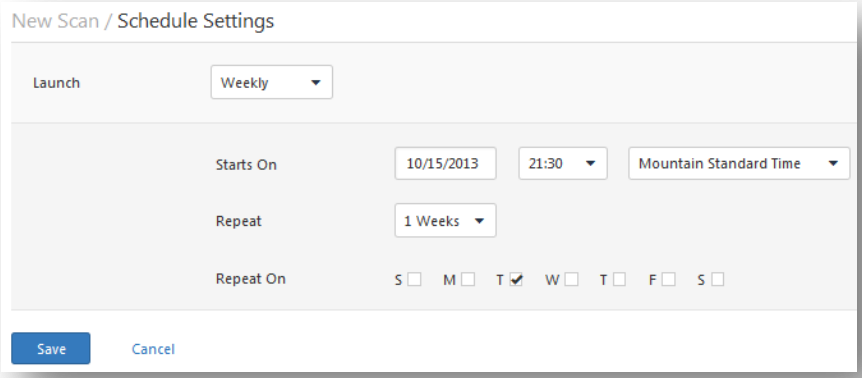
Under the "**Schedule Settings**" tab, there is a drop-down menu that controls when the scan will be launched:



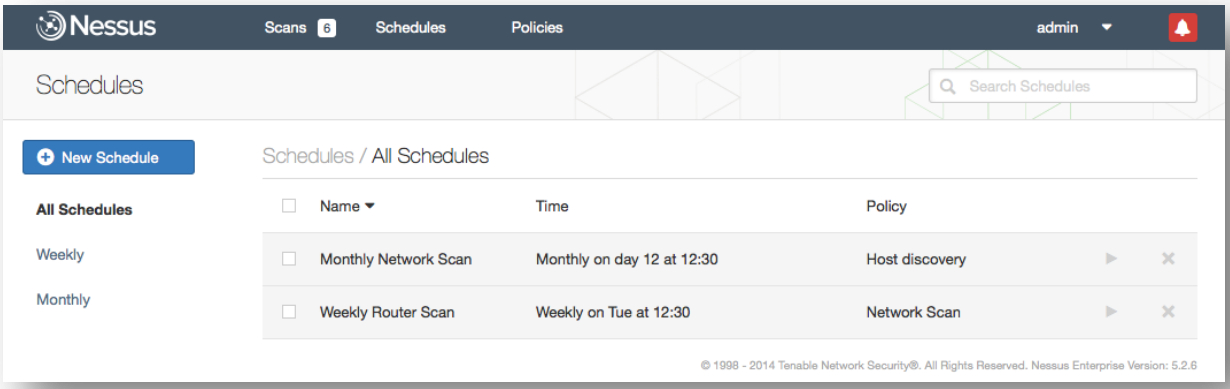
The launch options are as follows:

- **Now** – Start the scan immediately.
- **On Demand** – Create the scan as a template so that it can be manually launched at any time (this feature was formerly handled under the "Scan Template" option).
- **Once** – Schedule the scan at a specific time.
- **Daily** – Schedule the scan to occur on a daily basis, at a specific time, or interval up to 20 days.
- **Weekly** – Schedule the scan to occur on a recurring basis, by time and day of week, for up to 20 weeks.
- **Monthly** – Schedule the scan to occur every month, by time and day or week of month, for up to 20 months.
- **Yearly** – Schedule the scan to occur every year, by time and day, for up to 20 years.

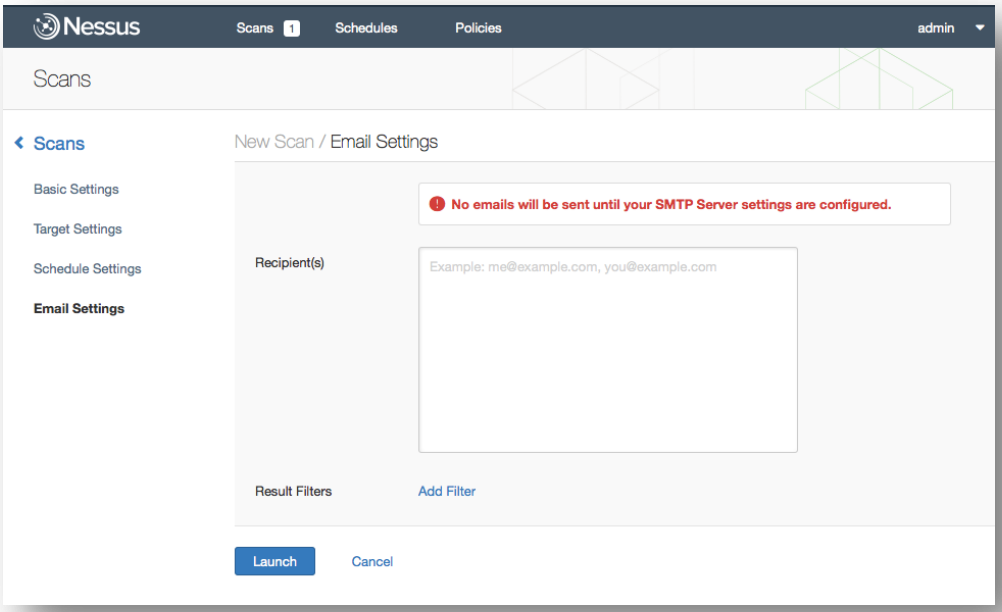
An example of a scheduled scan is below:



Once a scheduled scan is created, it can be accessed via the "**Schedules**" menu at the top. This page allows you manage scheduled scans and update them as required:

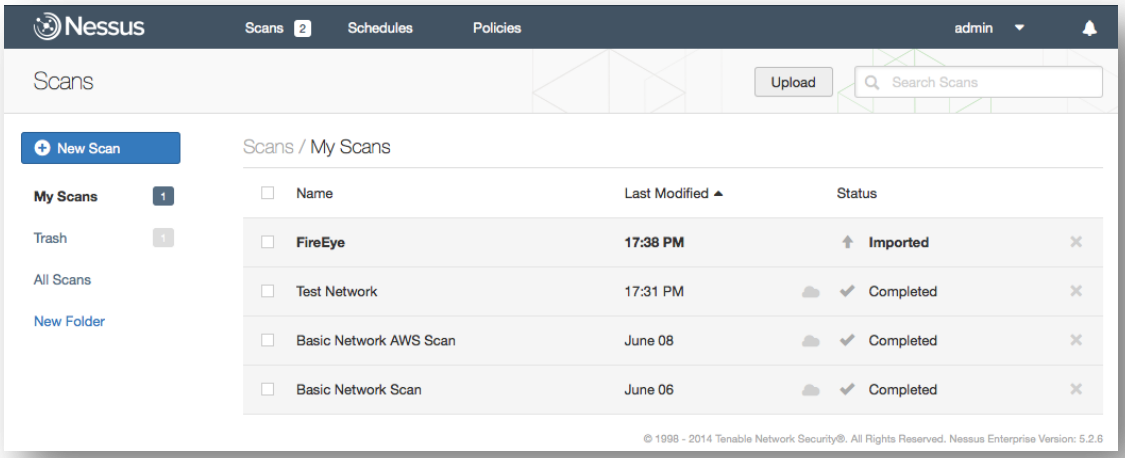


Under the "**Email Settings**" tab, you can optionally configure email addresses to which the scan results will be mailed upon scan completion.

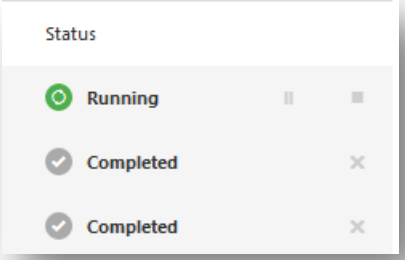


The "**Email Scan Results**" functionality requires that a Nessus administrator configure the SMTP settings. For more information on configuring SMTP settings, consult the Nessus 5.2 Installation and Configuration Guide. If you have not configured these settings, Nessus will warn you that they must be set for the functionality to work.

After you have entered the scan information, click "**Save**". After submitting, the scan will begin immediately (if "**Now**" was selected) before the display is returned to the general "**Scans**" page. The top menu bar will also update the number overlaying the "**Scans**" button to indicate how many total scans are present.



Once a scan has launched, the "**Scans**" list will display a list of all scans currently running or paused, along with basic information about the scan. While a scan is running, a pause and stop button are available on the left to change the status:

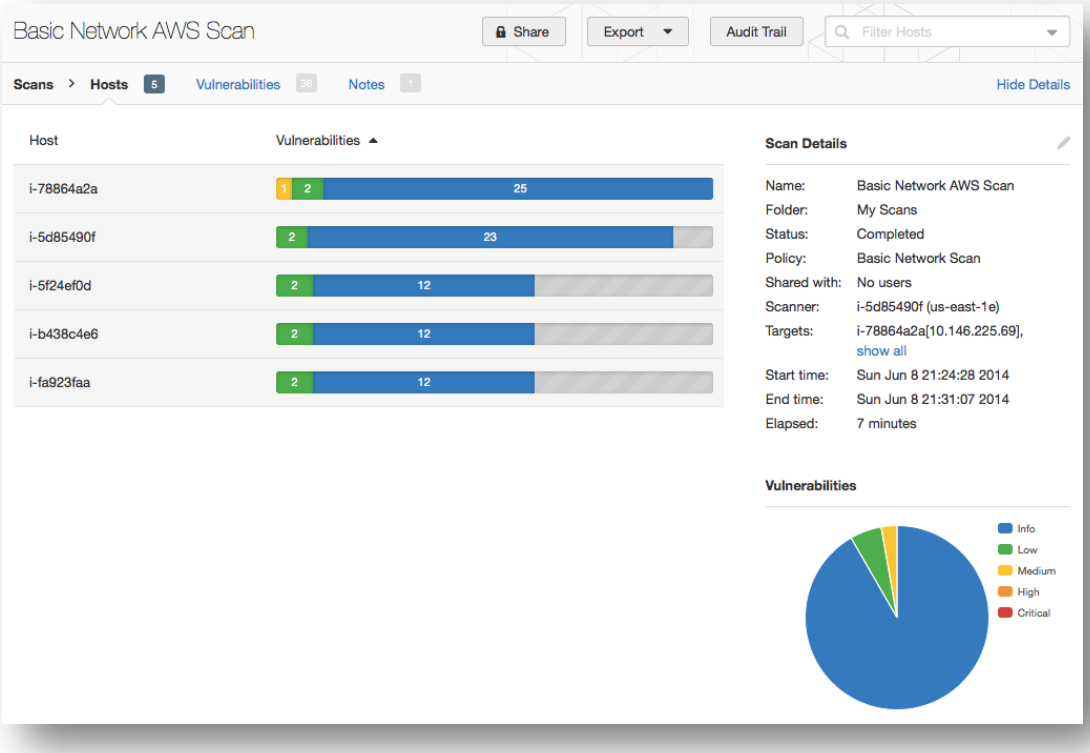


After selecting a particular scan on the list via the checkbox on the left, the "**More**" and "**Move To**" buttons on the top right will allow you to perform further actions including the ability to rename, manipulate scan status, mark as read, or move it to a different folder.

For more details on managing folders, please refer to the Nessus 5.2 Enterprise User Guide under "**Creating and Managing Scan Folders**".

Scanning Reports for Nessus for AWS

To browse the results of a scan, click on a report from the list. This allows you to view results by navigating through the results by vulnerabilities or hosts, displaying ports, and specific vulnerability information. The default view/tab is by host summary, which shows a list of hosts with a color-coded vulnerability summary per host:

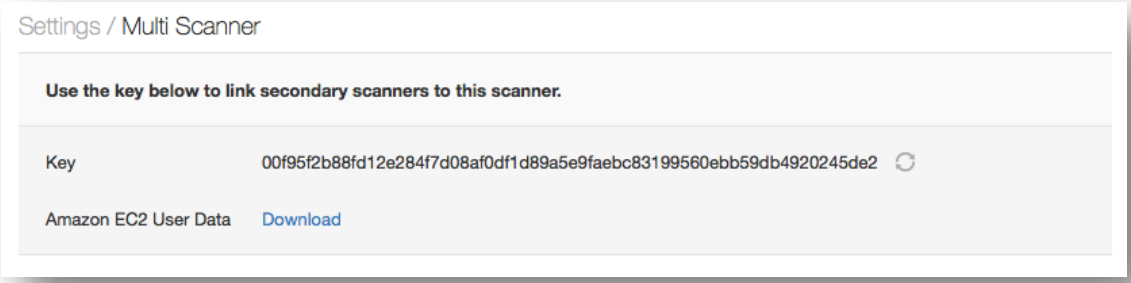


Note that targets are identified by their instance ID instead of their IP address or hostname.

For more details on managing folders, please refer to the Nessus 5.2 Enterprise User Guide under "**Browse Scan Results**".

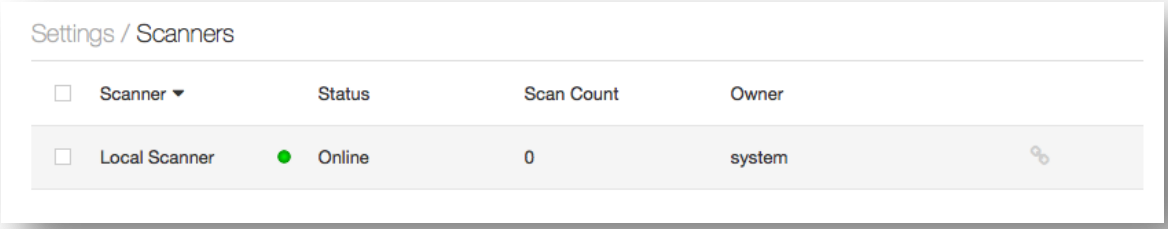
Adding other Nessus Scanners

The Nessus Enterprise for AWS Manager can connect other Nessus scanners, such as Nessus or Nessus Enterprise. In order to connect the scanner, use the key under "**Settings > Multi Scanner**":



Do not download the Amazon EC2 User Data at this time. It will not be needed for these scanners.

This key is only used for the initial linking of two scanners. Subsequent communication is done via a separate set of credentials. At any time, you can disable this functionality by clicking the "**Disable Scanner**" button. If there is ever concern over the shared secret becoming compromised, you can regenerate the key at any time by clicking the arrows to the right of the key. Regenerating the key will not disable any scanners that are already registered. Once a scanner has been configured to controlled by the Nessus Enterprise for AWS Manager, it will display this on its interface:



On the Nessus Enterprise for AWS Manager, you can unlink a scanner via the icon on the left. Unlinking the scanner will make it unavailable for scheduled scans until re-linked.

Settings / Scanners

Scanner	Status	Scan Count	Owner
i-5d85490f (us…	Online	0	system
i-5f24ef0d (us-…	Online	0	system
non AWS Sca…	Online	0	system

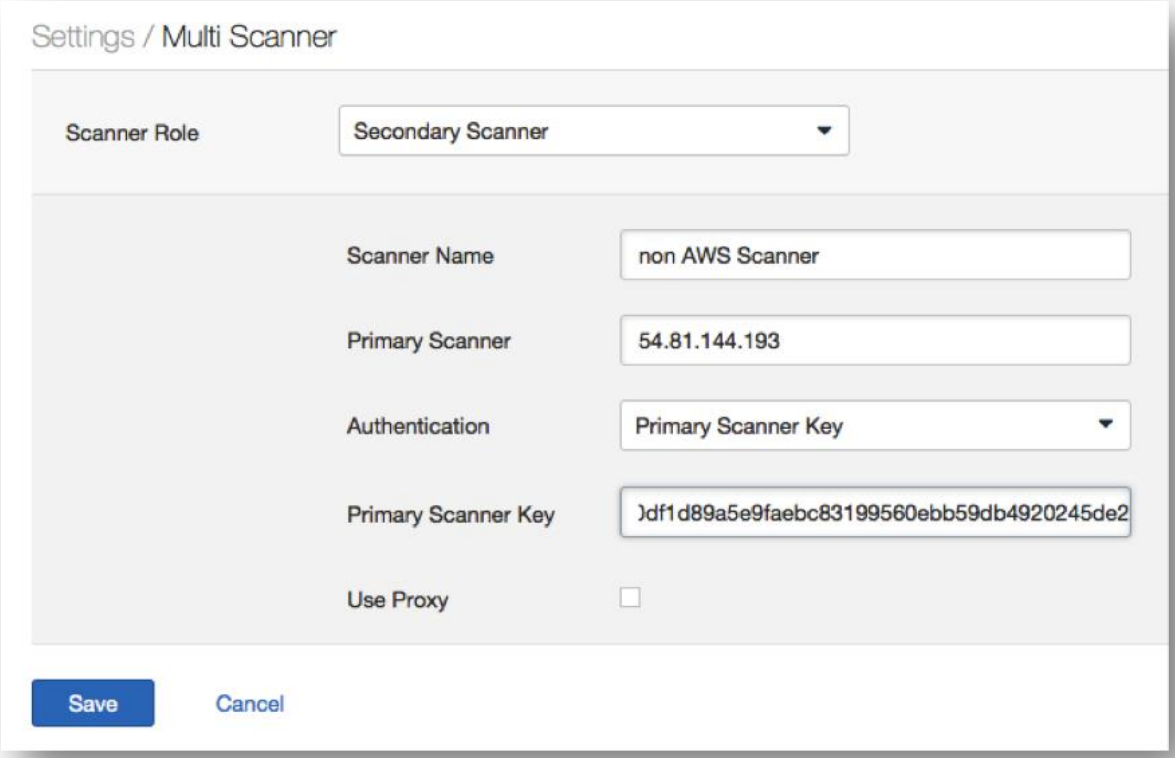
To completely remove a scanner, click the “X”. To retrieve information about the scanner, click on the scanner name:

Settings / Scanners / non AWS Scanner

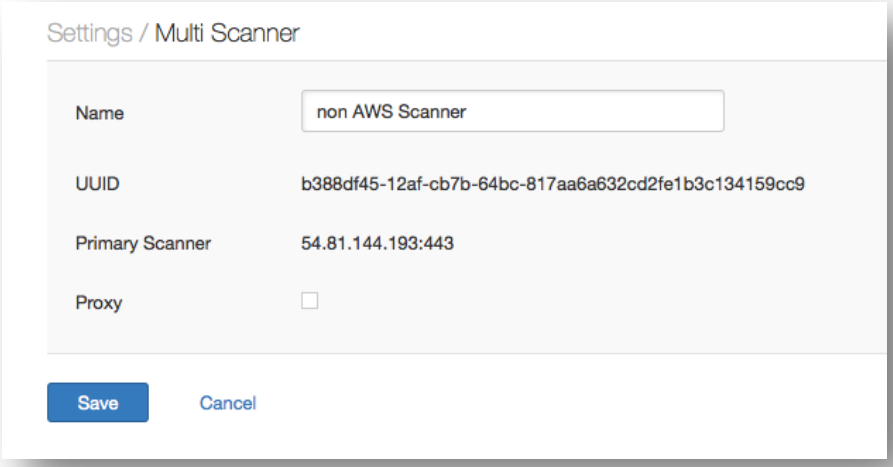
Status	Online	**Plugins**	
Owner	system	Last Updated	June 11, 2014
Last Connection	N/A	Plugin Set	201406111615
Engine	5.2.6	Expiration	May 12, 2017
Web UI	2.3.2	Registration Code	N/A
Platform	LINUX		

No data is available for this scanner.

To configure your scanner to be a secondary scanner, select that option:



Assign the scanner a unique name for easy identification, along with the key generated from the primary scanner, the primary scanner IP address, and primary scanner port. If communication must be directed through a proxy, select this option. Once selected, the scanner will use the proxy configured under `Settings` > `Proxy`. Once configured, Nessus will ensure that the scanner can reach and access the primary scanner and assign it a UUID for identification:



For Further Information

Tenable has produced a variety of other documents detailing Nessus' installation, deployment, configuration, user operation, and overall testing. These are listed here:

- **Nessus 5.2 Installation and Configuration Guide** – step by step walk through of installation and configuration on Nessus and Nessus Enterprise
- **Nessus 5.2 User Guide**– walk through the Nessus UI functionality
- **Nessus 5.2 Enterprise User Guide** – how to configure and operate the Nessus User Interface for Nessus Enterprise
- **Nessus Enterprise Cloud User Guide** – describes use of Nessus Enterprise Cloud and includes subscription and activation, vulnerability scanning, compliance reporting, and Nessus Enterprise Cloud support
- **Nessus Credential Checks for Unix and Windows –** information on how to perform authenticated network scans with the Nessus vulnerability scanner
- **Nessus Compliance Checks** – high-level guide to understanding and running compliance checks using Nessus and SecurityCenter
- **Nessus Compliance Checks Reference** – comprehensive guide to Nessus Compliance Check syntax
- **Nessus v2 File Format** – describes the structure for the `.nessus` file format, which was introduced with Nessus 3.2 and NessusClient 3.2
- **Nessus 5.0 REST Protocol Specification** – describes the REST protocol and interface in Nessus
- **Nessus 5 and Antivirus** – outlines how several popular security software packages interact with Nessus, and provides tips or workarounds to allow the software to better co-exist without compromising your security or hindering your vulnerability scanning efforts
- **Nessus 5 and Mobile Device Scanning** – describes how Nessus integrates with Microsoft Active Directory and mobile device management servers to identify mobile devices in use on the network
- **Nessus 5.0 and Scanning Virtual Machines** – describes how Tenable Network Security's Nessus vulnerability scanner can be used to audit the configuration of virtual platforms as well as the software that is running on them
- **Strategic Anti-malware Monitoring with Nessus, PVS, and LCE** – describes how Tenable's USM platform can detect a variety of malicious software and identify and determine the extent of malware infections
- **Patch Management Integration** – document describes how Nessus and SecurityCenter can leverage credentials on the IBM TEM, Microsoft WSUS and SCCM, VMware Go, and Red Hat Network Satellite patch management systems to perform patch auditing on systems for which credentials may not be available to the Nessus scanner
- **Real-Time Compliance Monitoring** – outlines how Tenable's solutions can be used to assist in meeting many different types of government and financial regulations
- **Tenable Products Plugin Families** – provides a description and summary of the plugin families for Nessus, Log Correlation Engine, and the Passive Vulnerability Scanner
- **SecurityCenter Administration Guide**

Other online resources are listed below:

- Nessus Discussions Forum: https://discussions.nessus.org/
- Tenable Blog: http://www.tenable.com/blog
- Tenable Podcast: http://www.tenable.com/podcast
- Example Use Videos: http://www.youtube.com/user/tenablesecurity
- Tenable Twitter Feed: http://twitter.com/tenablesecurity

Please feel free to contact Tenable at support@tenable.com, sales@tenable.com, or visit our website at http://www.tenable.com/.

About Tenable Network Security

Tenable Network Security provides continuous network monitoring to identify vulnerabilities, reduce risk, and ensure compliance. Our family of products includes SecurityCenter Continuous View™, which provides the most comprehensive and integrated view of network health, and Nessus®, the global standard in detecting and assessing network data. Tenable is relied upon by more than 20,000 organizations, including the entire U.S. Department of Defense and many of the world's largest companies and governments. For more information, please visit www.tenable.com.

GLOBAL HEADQUARTERS

Tenable Network Security
7021 Columbia Gateway Drive
Suite 500
Columbia, MD 21046
410.872.0555
www.tenable.com

Copyright © 2014. Tenable Network Security, Inc. All rights reserved. Tenable Network Security and Nessus are registered trademarks of Tenable Network Security, Inc.