Tenable Vulnerability Management and Amazon Web Services Integration Guide

Last Revised: September 11, 2023

Table of Contents

Welcome to AWS for Tenable Vulnerability Management

This document describes how to deploy Tenable Vulnerability Management® for integration with Amazon Web Services.

With more than one million users, Tenable Nessus® is the world's most widely deployed vulnerability, configuration, and compliance assessment product. Tenable 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.

A pre-authorized Tenable Nessus scanner is available in the Amazon Marketplace. The Tenable Nessus scanner links to and is managed by Tenable Vulnerability Management, and allows pre-authorized scanning of AWS EC2 environments and instances. The AWS Connector provides real-time visibility and inventory of EC2 assets in AWS by querying the AWS API. Customers interested in leveraging the pre-authorized Tenable Nessus scanner to secure their AWS environments and instances must have active Tenable Vulnerability Management and Amazon Web Services accounts.

To configure an AWS connector with Frictionless Assessment, see Frictionless Assessment for AWS in the *Tenable Vulnerability Management User Guide*.

To configure an AWS connector without Frictionless Assessment, see AWS Cloud Connector (without Frictionless Assessment) in the *Tenable Vulnerability Management User Guide*,

Note: To manage existing AWS connectors, see Manage Connectors in the *Tenable Vulnerability Management User Guide*.

Tip: For common connector errors, see Connectors in the Tenable Developer Portal.

Integration Requirements

The following are required in order to integrate Tenable Vulnerability Management with AWS:

- **Tenable Vulnerability Management account**

  To purchase a Tenable Vulnerability Management account or set up a free evaluation, visit http://www.tenable.com/products/tenable-io

- **AWS account**

  To create a free account, visit https://aws.amazon.com/start-now

- **Internet connection**

Integration Configuration

To configure AWS for Tenable Vulnerability Management, see the following integration configuration topics:

- AWS Connector
- Pre-Authorized Scanner
  - Obtain Tenable Vulnerability Management Linking Key
  - Create an AWS IAM Role
  - Launch Pre-Authorized Nessus Scanner
  - Create Security Group to Permit Scanning
- Tenable Nessus BYOL Scanner
  - Activate Nessus Professional BYOL Scanner
    - Activate Tenable Nessus BYOL Scanner via the Command Line
  - Obtain Tenable Vulnerability Management Linking Key
  - Activate Tenable Nessus BYOL Scanner Linked to Tenable Vulnerability Management
    - Link Tenable Nessus BYOL Scanner to Tenable Vulnerability Management via the Command Line
  - Optional Configuration
- Create a Scan
  - View Scan Results in Tenable Vulnerability Management
- Create an Agent Scan
- Audit the AWS Environment
  - AWS Audit Troubleshooting

Tenable Nessus BYOL Scanner

The following instructions describe how to configure a Tenable Nessus Bring Your Own License (BYOL) Amazon Web Services (AWS) scanner. Each section includes steps for configuring the scanner via the user interface or via the command line.

> **Note:** For more information on advanced settings for Tenable Nessus (for example, security group configuration), see Advanced Settings in the *Tenable Nessus User Guide*.

Before you begin:

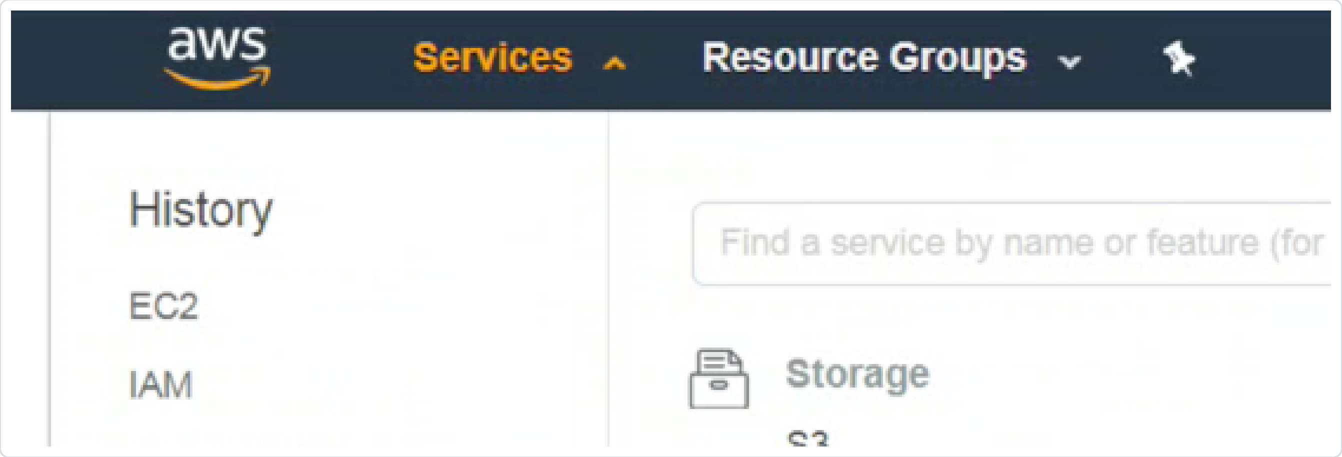
- Ensure that your system meets the hardware requirements described in the *Tenable Nessus User Guide*.

To configure the Nessus BYOL Scanner in AWS:

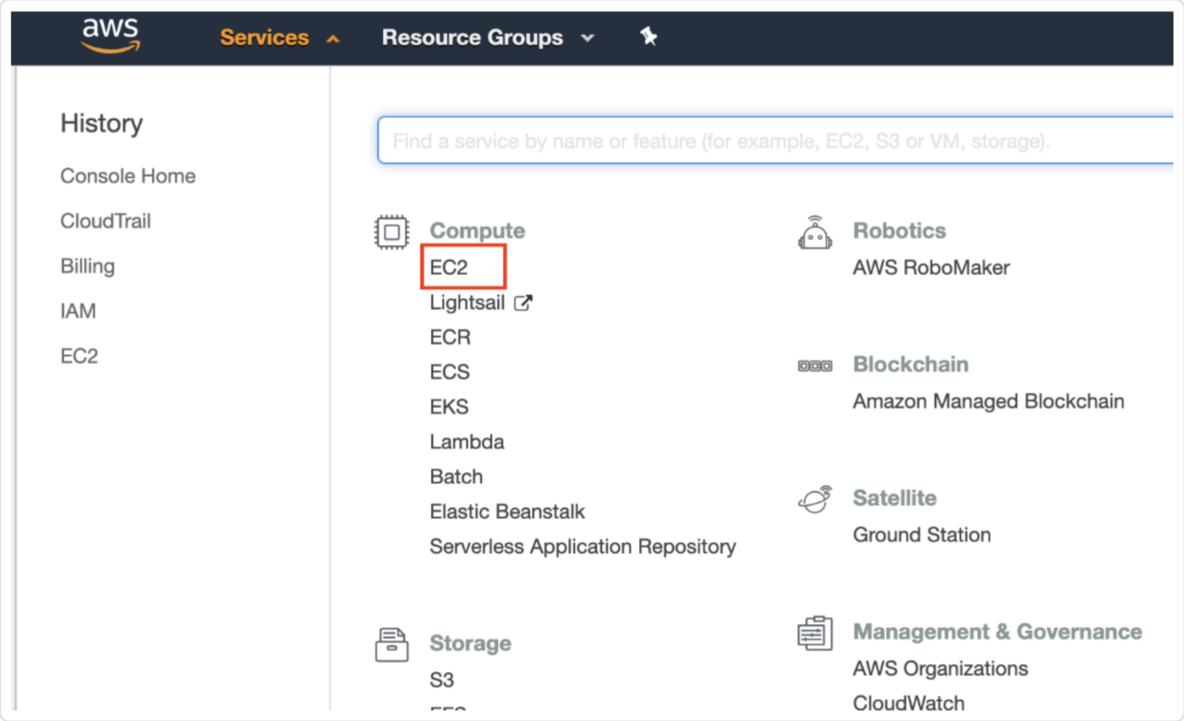
1. Log in to the AWS Management Console.
2. In the top menu bar, click **Services**.

   The **Services** page appears.

   > **Note:** Amazon is continually updating their service, so screenshots may differ from the AWS interface you see.



3. In the **Compute** section, click **EC2**.



The **EC2 Dashboard** appears.

4. In the **Create Instance** section, click **Launch Instance**.

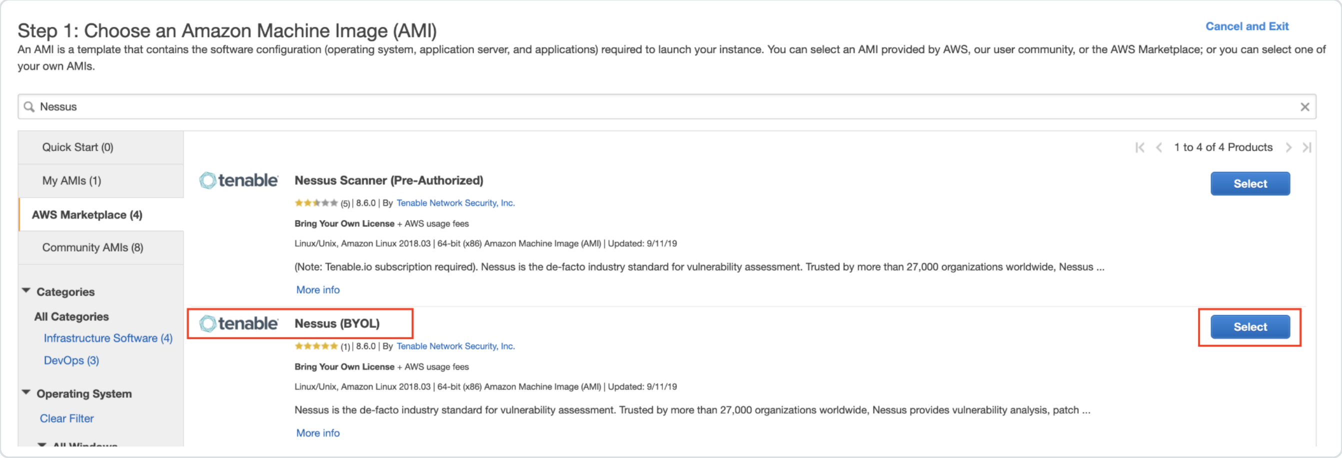
   The **Choose an Amazon Machine Image (AMI)** page appears.

5. In the left panel, click **AWS Marketplace**.

6. In the search box, type **Nessus**.

7. On your keyboard, press **Enter**.

8. In the **Nessus (BYOL)** section, click **Select**.



Step 1: Choose an Amazon Machine Image (AMI)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace; or you can select one of your own AMIs.

Nessus Scanner (Pre-Authorized)

(5) | 8.6.0 | By Tenable Network Security, Inc.

Bring Your Own License + AWS usage fees

Linux/Unix, Amazon Linux 2018.03 | 64-bit (x86) Amazon Machine Image (AMI) | Updated: 9/11/19

(Note: Tenable.io subscription required). Nessus is the de-facto industry standard for vulnerability assessment. Trusted by more than 27,000 organizations worldwide, Nessus ...

Nessus (BYOL)

(1) | 8.6.0 | By Tenable Network Security, Inc.

Bring Your Own License + AWS usage fees

Linux/Unix, Amazon Linux 2018.03 | 64-bit (x86) Amazon Machine Image (AMI) | Updated: 9/11/19

Nessus is the de-facto industry standard for vulnerability assessment. Trusted by more than 27,000 organizations worldwide, Nessus provides vulnerability analysis, patch ...

The **Nessus (BYOL)** review window appears.

9. Review the pricing details and instance type details.

10. Click **Continue**.

    The **Step 2: Choose an Instance Type** page appears.

11. Click **Next: Configure Instance Details**.

    The **Step 3: Configure Instance Details** page appears.

12. Configure the instance details according to your company specific preferences.

    > **Note:** Your system must also:
    >
    > - Meet the hardware requirements described in the *Tenable Nessus User Guide*.
    > - Include an internet connection with which to access Tenable Vulnerability Management.

13. Click **Next: Add Storage**.

    The **Step 4: Add Storage** page appears.

14. Configure the storage details according to your company specific preferences.

15. Click **Next: Add Tags**.

    The **Step 5: Add Tags** page appears.

16. (Optional) Configure tags according to your company specific preferences.

17. Click **Next: Configure Security Group**.

    The **Step 6: Configure Security Group** page appears.

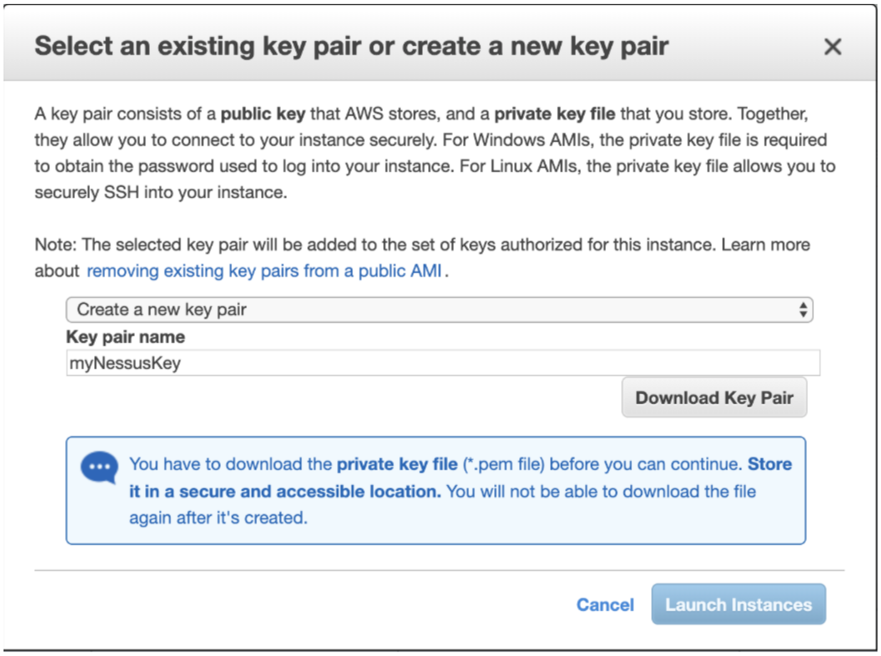
18. (Optional) Configure the security group details according to your company specific preferences.

19. Click **Review and Launch**.

    The **Review Instance** page appears.

20. Click **Launch**.

    A key pair page appears.



Select an existing key pair or create a new key pair

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about removing existing key pairs from a public AMI .

Create a new key pair

Key pair name

myNessusKey

You have to download the **private key file** (*.pem file) before you can continue. **Store it in a secure and accessible location.** You will not be able to download the file again after it's created.

21. Do one of the following:

    - If you have access to an existing key pair, select **Choose an existing key pair**.

        a. In the **Select a key pair** section, select the key pair you want to use.

        b. Select the acknowledge check box.

- If you do not have access to an existing key pair, select **Create a new key pair**.

    a. In the **Key pair name** box, type a name for the key pair.

    b. Click **Download Key Pair**.

> **Tip:** You need this key pair to access the Nessus Professional BYOL scanner from the command line for activation/registration. For more information, see Activate Tenable Nessus BYOL Scanner via the Command Line.

22. Click **Launch Instances**.

    The **Launch Status** page appears. AWS begins a validation process for the new Nessus BYOL EC2 Instance and proceeds to pass health checks.

23. Click **View Instances** to confirm the instance appears successfully.

> **Note:** When the status checks complete, take note of the public IP (if applicable) of the Nessus BYOL instance. Otherwise, you need a Bastion host to access the command line to continue configuration of the Nessus BYOL Scanner.

Activate Nessus Professional BYOL Scanner

Before you begin:

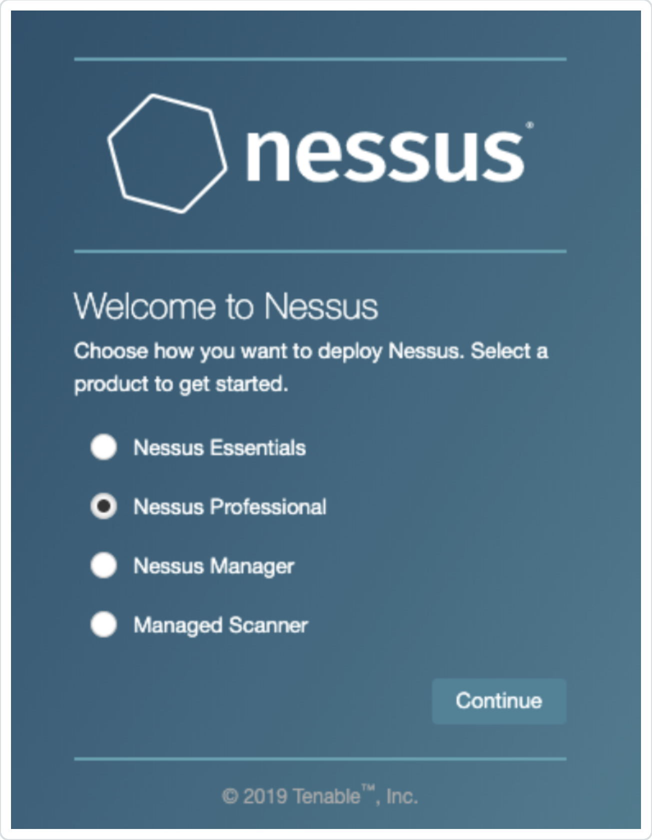
- View the login and instance-type information in Nessus BYOL Scanner.

To activate the Tenable Nessus Professional BYOL Scanner:

1. Navigate to the Tenable Nessus user interface on Port 8834, for example, https://*<NessusBYOL-IP>*:8834, where *<BYOLpublicIP>* is the IP address of your Tenable Nessus Professional instance.

   The **Welcome to Tenable Nessus** page appears.

2. Select **Nessus Professional**.

   Welcome to Nessus

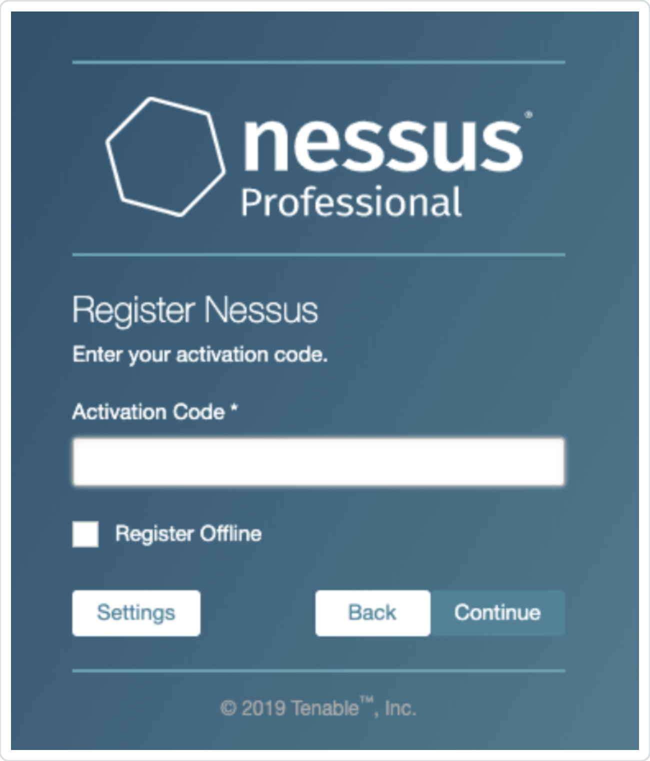
   Choose how you want to deploy Nessus. Select a product to get started.

   ○ Nessus Essentials
   ● Nessus Professional
   ○ Nessus Manager
   ○ Managed Scanner

   © 2019 Tenable™, Inc.

3. Click **Continue**.

   The **Register Tenable Nessus** page appears.



Register Nessus

Enter your activation code.

Activation Code *

□ Register Offline

© 2019 Tenable™, Inc.

4. In the **Activation Code** box, type your Tenable Nessus Professional activation code.

5. Click **Continue**.

   Tenable Nessus Professional activates and plugins begin downloading. For more information, see the Nessus User Guide.

Activate Tenable Nessus BYOL Scanner via the Command Line

To activate the Tenable Nessus Professional BYOL scanner via the command line:

1. Adjust the permissions for your downloaded SSH Key using the following command:

   ```
   chmod 400 myNessusKey.pem
   ```

2. SSH into the Nessus BYOL scanner using the following command:

   ```
   ssh -i myNessusKey.pem ec2-user@<BYOLpublicIP>
   ```

   Where *<BYOLpublicIP>* is the IP address of your Tenable Nessus Professional instance.

3. Elevate privileges using the following command:

   ```
   sudo su
   ```

4. Update the AMI using the following command:

   ```
   yum update -y
   ```

5. Stop Tenable Nessus using the following command:

   ```
   service nessusd stop
   ```

6. Register the scanner with your Tenable Nessus Professional activation code using the following command:

   ```
   /opt/nessus/sbin/nessuscli fetch --register <ACTIVATION CODE>
   ```

   Where *<ACTIVATION CODE>* is the activation code for your instance.

7. Start Tenable Nessus using the following command:

   ```
   service nessusd start
   ```

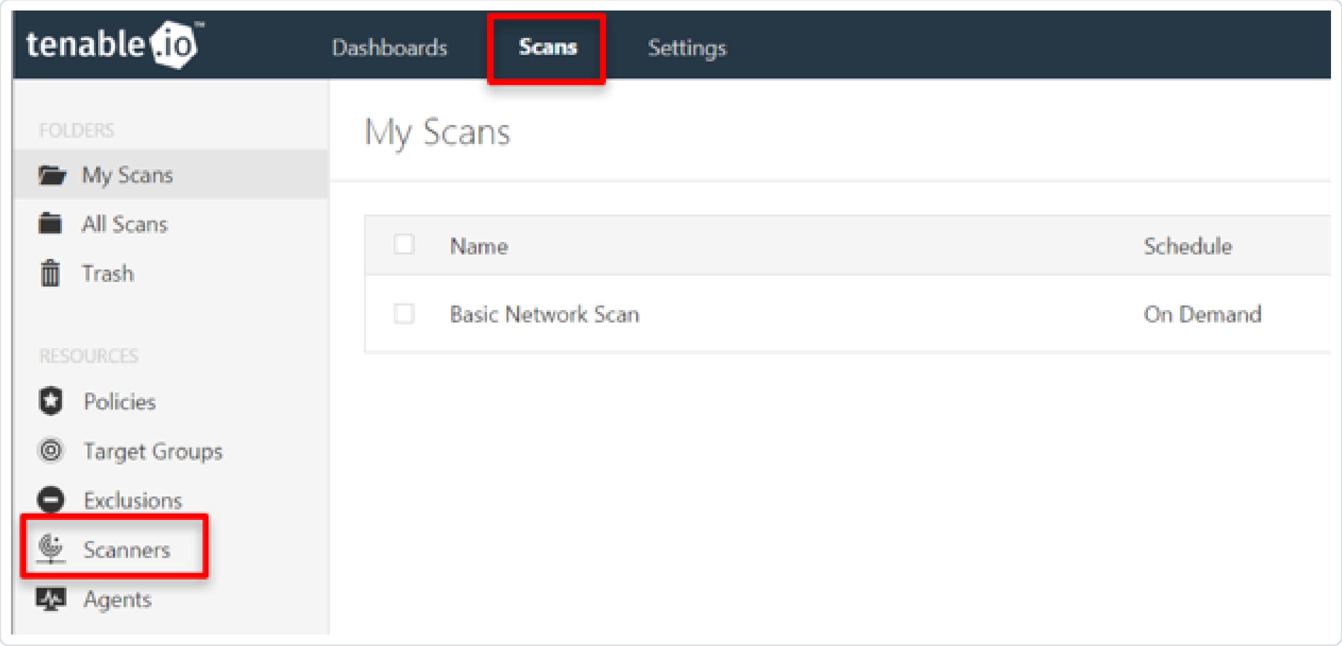
Obtain Tenable Vulnerability Management Linking Key

Note: These steps only apply if registering the Nessus BYOL scanner to be linked to and managed by Tenable Vulnerability Management.

To obtain the Tenable Vulnerability Management linking key:

1. Log in to https://cloud.tenable.com.
2. In the top menu bar, click **Scans**.
3. In the left-hand menu, click **Scanners**.

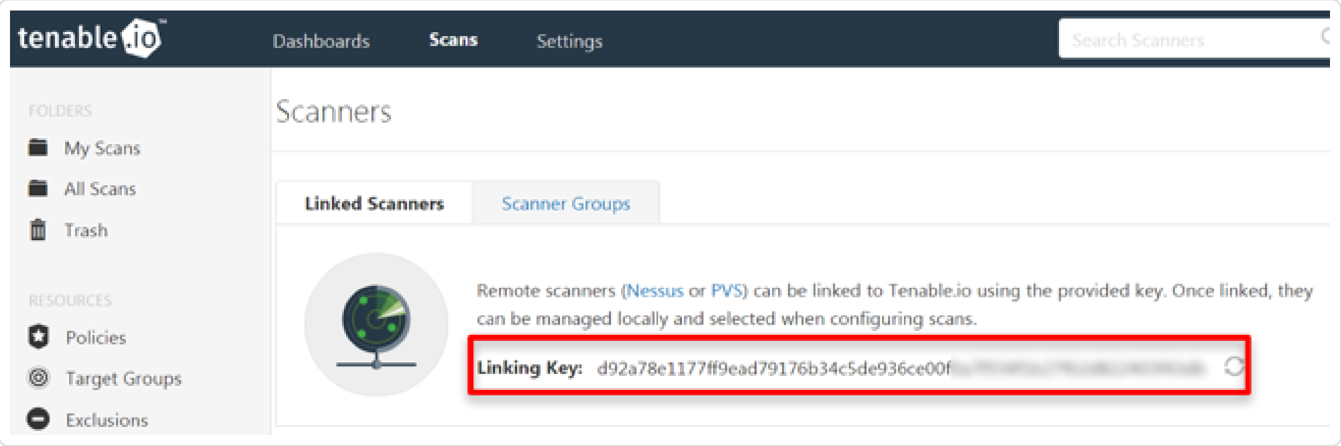
   The **Scanners** page appears.



☐	Name	Schedule
☐	Basic Network Scan	On Demand

4. Click the **Linked Scanners** tab.

5. Copy and save the **Linking Key**.



Remote scanners (Nessus or PVS) can be linked to Tenable.io using the provided key. Once linked, they can be managed locally and selected when configuring scans.

Linking Key: d92a78e1177ff9ead79176b34c5de936ce00f[redacted]

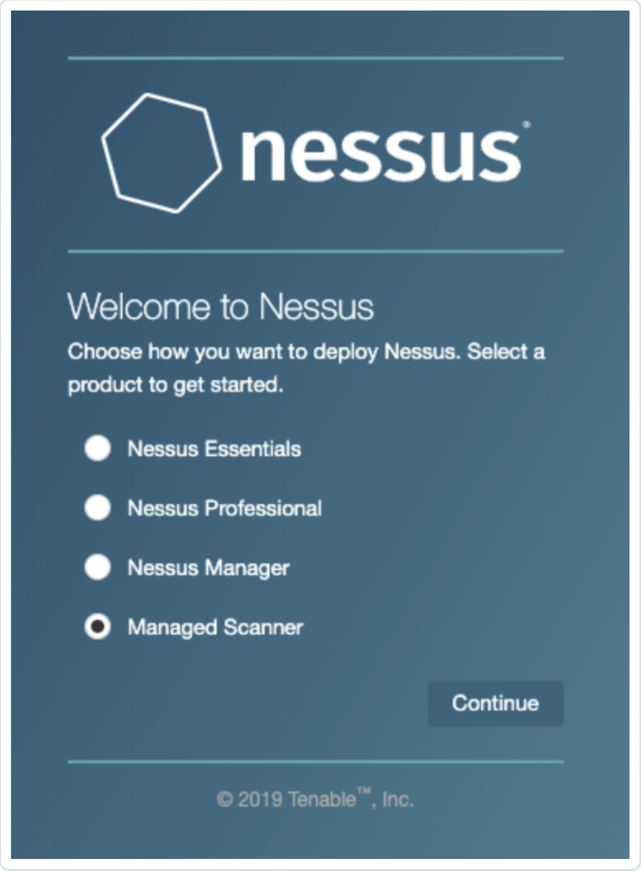
Activate Tenable Nessus BYOL Scanner Linked to Tenable Vulnerability Management

To activate the Tenable Nessus BYOL Scanner linked to and managed by Tenable Vulnerability Management:

1. Navigate to the Tenable Nessus UI on Port 8834, for example, *https://<NessusBYOL-IP>:8834*.

   The **Welcome to Tenable Nessus** page appears.

2. Select **Managed Scanner**.

   Welcome to Nessus

   Choose how you want to deploy Nessus. Select a product to get started.

   ○ Nessus Essentials

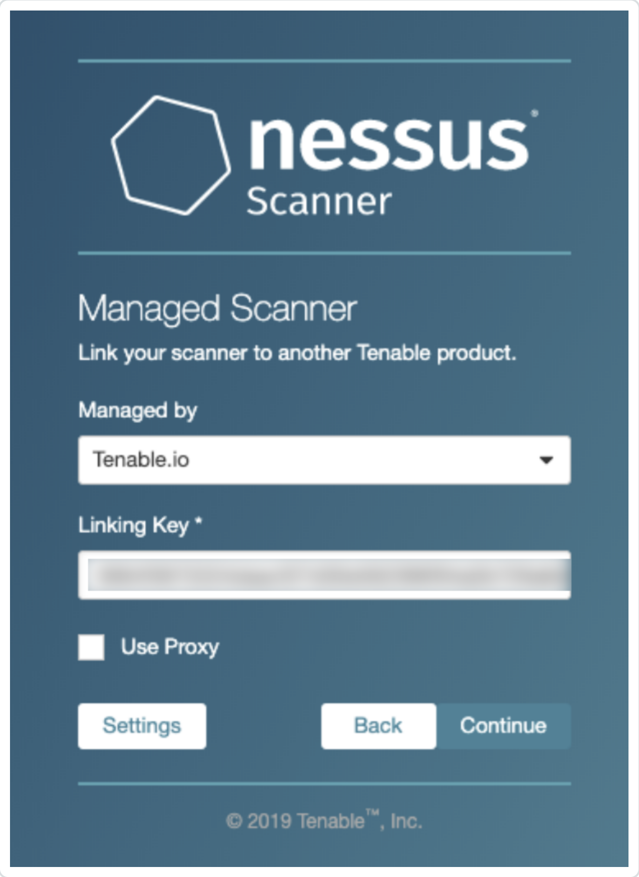
   ○ Nessus Professional

   ○ Nessus Manager

   ● Managed Scanner

3. Click **Continue**.

   The **Managed Scanner** page appears.



Managed Scanner

Link your scanner to another Tenable product.

Managed by: Tenable.io

Linking Key *: [redacted]

□ Use Proxy

4. From the **Managed by** drop-down box, select **Tenable Vulnerability Management**.
5. In the **Linking Key** box, paste the linking key copied in the Obtain Tenable Vulnerability Management Linking Key section.
6. Click **Continue**.

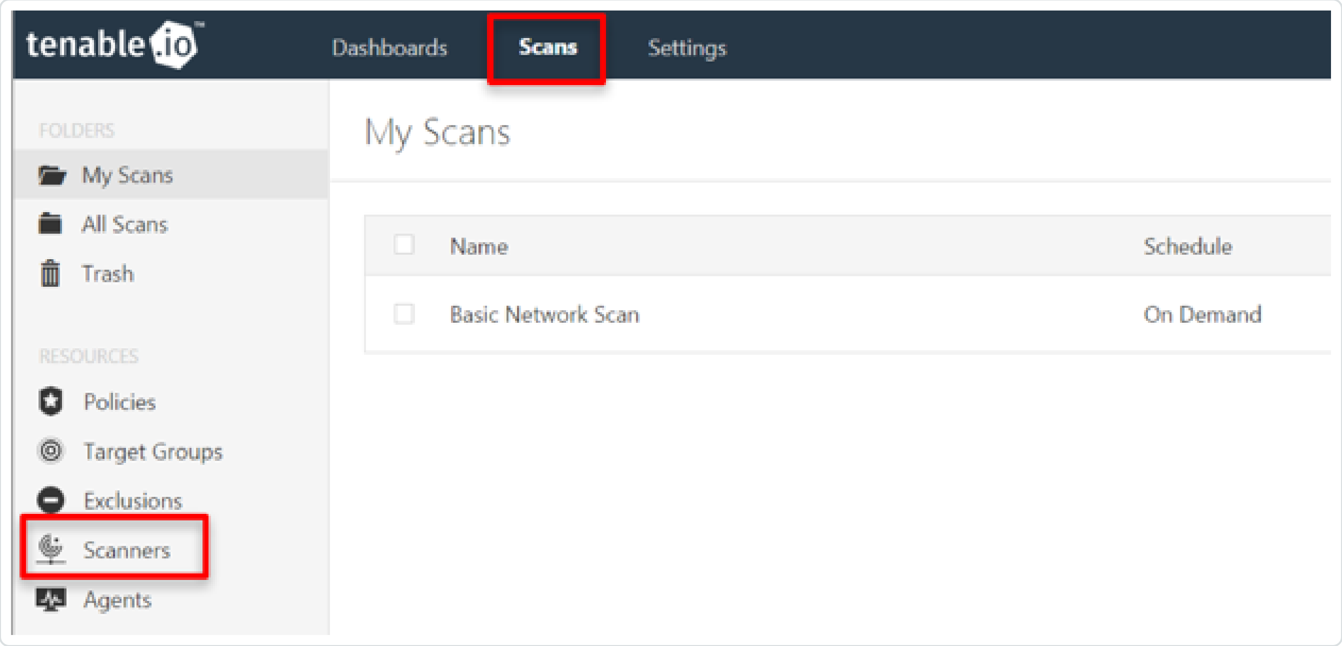
   Tenable Vulnerability Management begins managing Tenable Nessus and plugins begin downloading. For more information, see the Nessus User Guide.

To confirm the Nessus BYOL Scanner in Tenable Vulnerability Management:

1. Log in to Tenable Vulnerability Management.
2. In the top menu bar, click **Scans**.

   The **My Scans** page appears.

3. In the left-hand menu, click **Scanners**.



☐	Name	Schedule
☐	Basic Network Scan	On Demand

The **Scanners** page appears. Confirm the BYOL Scanner appears in the **Linked Scanners** list.

Link Tenable Nessus BYOL Scanner to Tenable Vulnerability Management via the Command Line

To link the Tenable Nessus BYOL scanner to Tenable Vulnerability Management via the command line:

1. Adjust the permissions for your downloaded SSH Key using the following command:

   ```
   chmod 400 myNessusKey.pem
   ```

2. SSH into the Nessus BYOL scanner using the following command:

   ```
   ssh -i myNessusKey.pem ec2-user@<BYOLpublicIP>
   ```

   Where *<BYOLpublicIP>* is the IP address of your Tenable Nessus BYOL instance.

3. Elevate privileges using the following command:

   ```
   sudo su
   ```

4. Update the AMI using the following command:

   ```
   yum update -y
   ```

5. Stop Tenable Nessus using the following command:

   ```
   service nessusd stop
   ```

6. Link the Nessus BYOL scanner to Tenable Vulnerability Management for management using the following command:

   ```
   /opt/nessus/sbin/nessuscli managed link --key=<key> --cloud
   ```

   Where *<key>* is the linking key associated with your Tenable Vulnerability Management instance.

   > **Note:** FedRAMP customers must use the following command:
   >
   > ```
   > /opt/nessus/sbin/nessuscli managed link --key=<key> -host-
   > t=fedcloud.tenable.com --port=443
   > ```

7. Start Tenable Nessus using the following command:

   ```
   service nessusd start
   ```

Link a BYOL Scanner to Tenable Vulnerability Management with Pre-Authorized Scanner Features

You can retain your pre-authorized AMI installation features when linking BYOL scanners to Tenable Vulnerability Management by using the following procedure.

> **Note:** This feature is only available for Nessus versions 10.2.0 and later.

> **Caution:** If you plan to downgrade a 10.2 Nessus scanner that was linked with the AWS scanner flag (see the following steps) to version 10.1.x or earlier, you need to manually unlink and relink the scanner after downgrading. Otherwise, Tenable Vulnerability Management will not recognize the scanner.

Before you begin:

Assign an IAM role to the Tenable Nessus instance you are deploying. For more information, see step 16 of Launch Pre-Authorized Nessus Scanner.

To link a BYOL scanner to Tenable Vulnerability Management with pre-authorized scanner features:

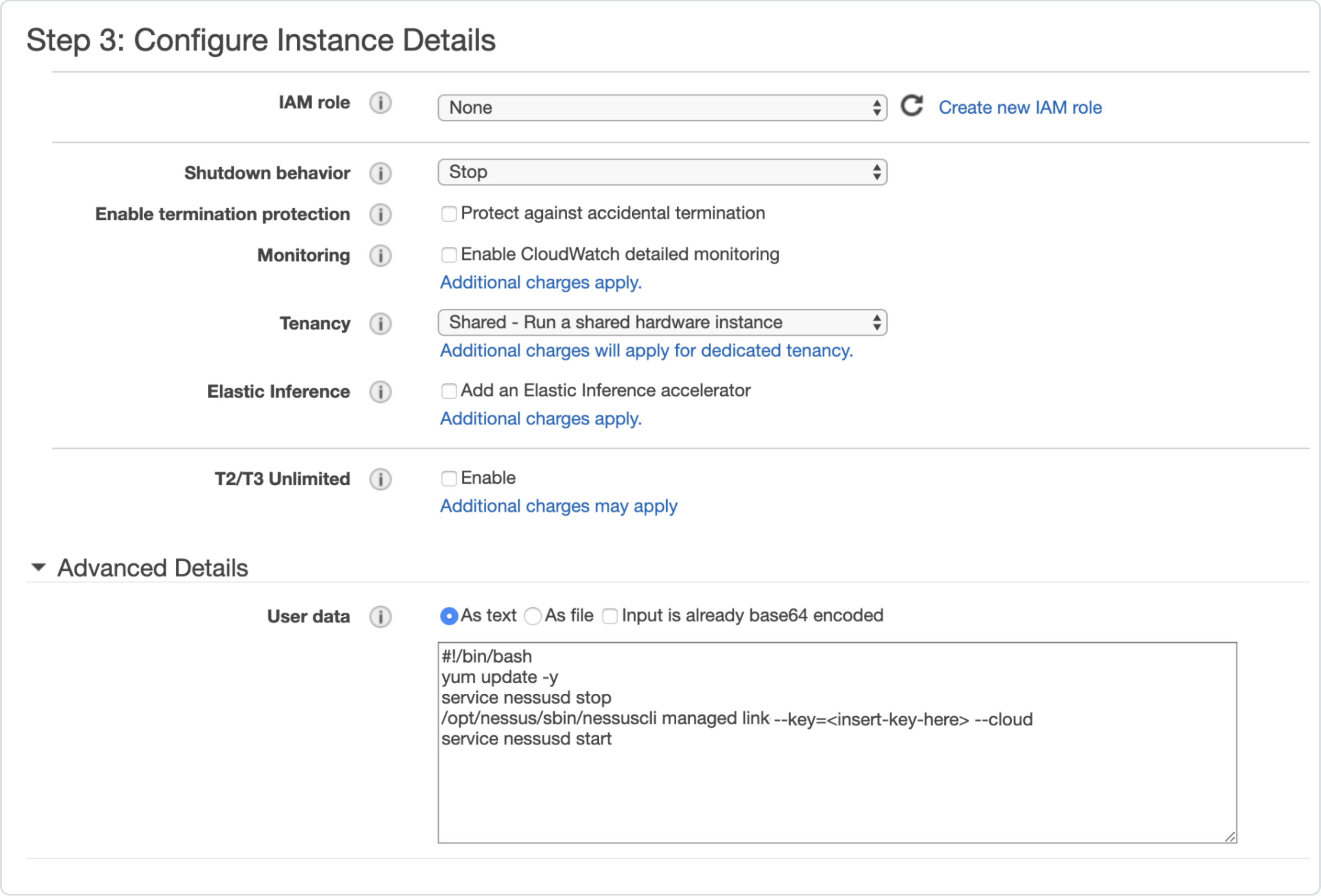
When you link the scanner to Tenable Vulnerability Management using the command line, as described in the Link to Tenable Vulnerability Management topic in the *Tenable Nessus User Guide*, use the optional `--aws-scanner` flag. For example:

```
> nessuscli managed link --key=<LINKING KEY> --cloud --aws-scanner
```

> **Note:** The scanner must already be running on an AWS instance for the flag to take effect.

Optional Configuration

In addition to manual configuration, you can use a bootstrap script to configure the Tenable Nessus BYOL scanner. The following screenshot shows an example of using a bootstrap Script during Nessus BYOL Configuration:



Step 3: Configure Instance Details

IAM role: None

Shutdown behavior: Stop

Enable termination protection: □ Protect against accidental termination

Monitoring: □ Enable CloudWatch detailed monitoring

Additional charges apply.

Tenancy: Shared - Run a shared hardware instance

Additional charges will apply for dedicated tenancy.

Elastic Inference: □ Add an Elastic Inference accelerator

Additional charges apply.

T2/T3 Unlimited: □ Enable

Additional charges may apply

Advanced Details

User data: ● As text ○ As file □ Input is already base64 encoded

```
#!/bin/bash
yum update -y
service nessusd stop
/opt/nessus/sbin/nessuscli managed link --key=<insert-key-here> --cloud
service nessusd start
```

Copy the bootstrap script below:

```
#!/bin/bash
yum update -y
service nessusd stop
/opt/nessus/sbin/nessuscli managed link --key=<insert-key-here> --cloud
service nessusd start
```

AWS Multi-Account Multi-VPC Scanning

You can use your Tenable Nessus BYOL scanner to perform scans across multiple accounts and Virtual Private Clouds (VPCs). The BYOL scanner does not require AWS IAM roles or permissions to scan.

If you want your Tenable Nessus BYOL scanner in AWS to scan across multiple VPCs belonging to different accounts, you must configure your VPCs to allow traffic to flow between them. To do this, you can use VPC peering or Transit Gateway.

VPC peering is the more secure option, but you should decide which approach is best for your VPC configuration. As with on-prem firewalls, if you don't want to facilitate communication between VPCs, you must either install a scan engine in each VPC or embed the agent on all Elastic Compute Cloud (EC2) instances.

AWS Transit Gateway does not support routing between Amazon VPCs with identical classless inter-domain routing (CIDR) IP addresses. If you attach a new Amazon VPC with an identical CIDR address to an already-attached Amazon VPC, AWS Transit Gateway will not propagate the route of the new Amazon VPC into the AWS Transit Gateway route table. See the AWS documentation for more information.

You will only be able to scan by IPs, DNS, or dynamic tags. You will not be able to scan by ID instances.

> **Note:** These steps have been tested with 4 accounts containing 8 VPCs and 16 EC2s.

Before you begin:

- To automate tag-based discovery and scanning, set up the AWS Connector with Tenable Vulnerability Management.

To configure your Tenable Nessus BYOL scanner to scan across multiple accounts and VPCs:

1. In Tenable Vulnerability Management, Deploy the BYOL scanner in one of your VPCs.

   You can use the Tenable Vulnerability Management wizard or CFT using the BYOL scanner Ami Id.

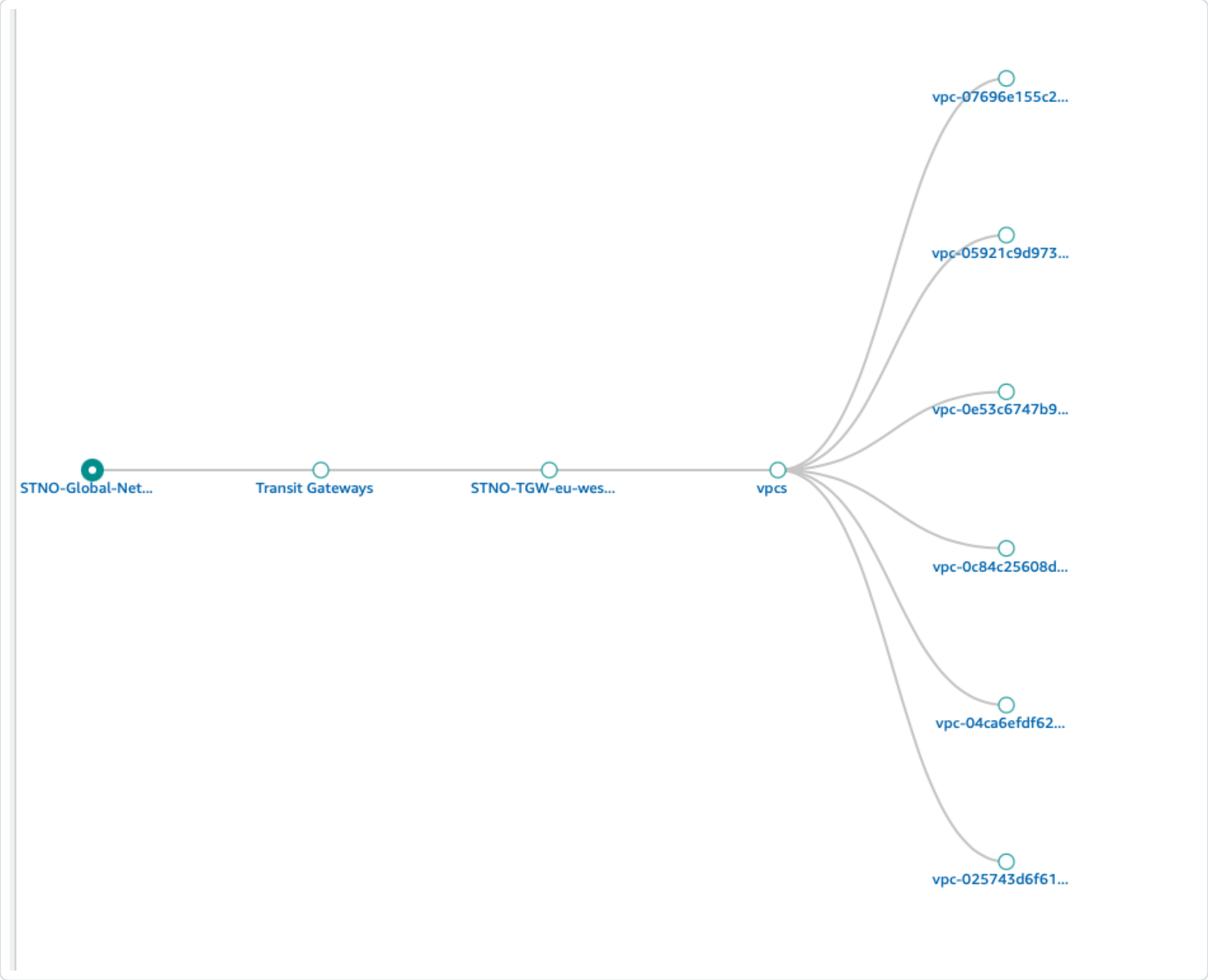
Tip: You can find the Ami Id here, after you select a region for the scanner.

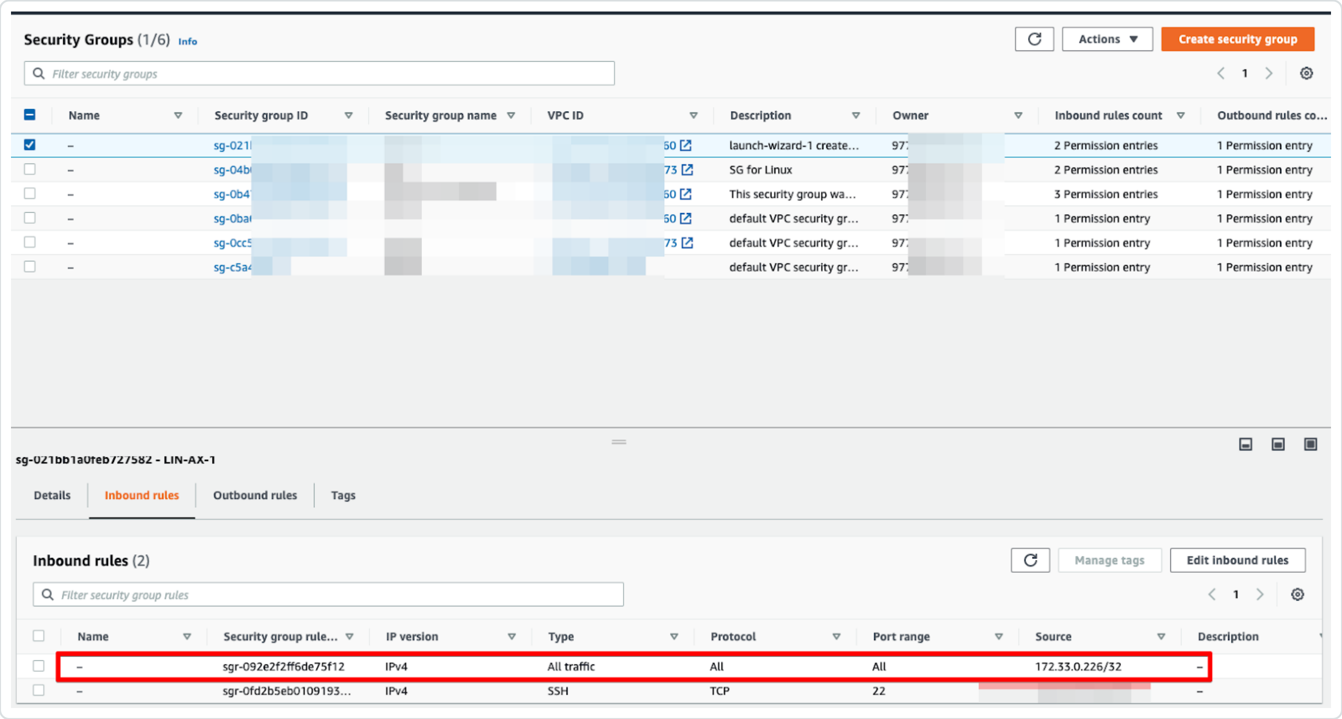
2. Link the Tenable Nessus BYOL scanner to Tenable Vulnerability Management in one of two ways:

   - Link the Tenable Nessus BYOL scanner in Tenable Vulnerability Management.
   - Use a bootstrap script to configure the Tenable Nessus BYOL scanner.

3. Perform the VPC peering or Transit Gateway configurations and allow the scanner to access all ports in the security groups.

   The following is an example transit gateway and the scanner authorization in the inbound rules of the security groups:





Security Groups (1/6) Info

☐	Name	Security group ID	Security group name	VPC ID	Description	Owner	Inbound rules count	Outbound rules co...
☑	–	sg-021[redacted]	[redacted]	[redacted]60	launch-wizard-1 create...	97[redacted]	2 Permission entries	1 Permission entry
☐	–	sg-04b[redacted]	[redacted]	[redacted]73	SG for Linux	97[redacted]	2 Permission entries	1 Permission entry
☐	–	sg-0b4[redacted]	[redacted]	[redacted]60	This security group wa...	97[redacted]	3 Permission entries	1 Permission entry
☐	–	sg-0ba[redacted]	[redacted]	[redacted]60	default VPC security gr...	97[redacted]	1 Permission entry	1 Permission entry
☐	–	sg-0cc5[redacted]	[redacted]	[redacted]73	default VPC security gr...	97[redacted]	1 Permission entry	1 Permission entry
☐	–	sg-c5a[redacted]	[redacted]	[redacted]	default VPC security gr...	97[redacted]	1 Permission entry	1 Permission entry

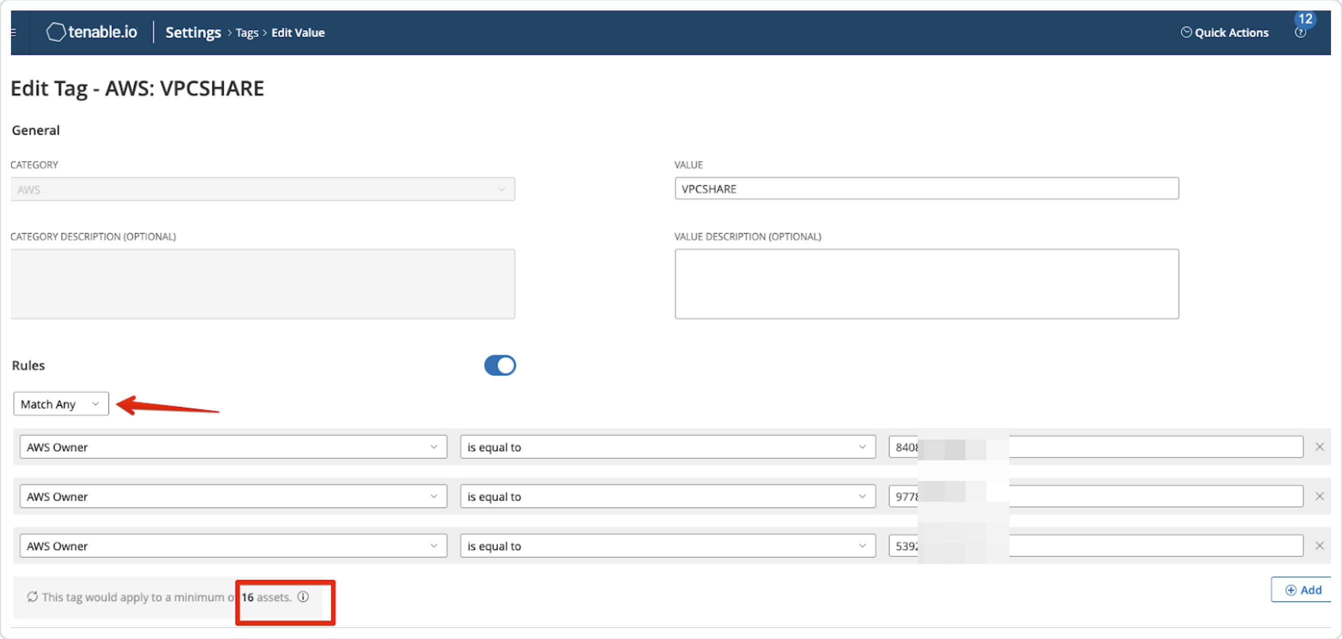
sg-021bb1a0feb727582 - LIN-AX-1

Inbound rules (2)

☐	Name	Security group rule...	IP version	Type	Protocol	Port range	Source	Description
☐	–	sgr-092e2f2ff6de75f12	IPv4	All traffic	All	All	172.33.0.226/32	–
☐	–	sgr-0fd2b5eb0109193...	IPv4	SSH	TCP	22	[redacted]	–

4. After the communication at your transit gateway is verified, in Tenable Vulnerability Management, select the assets you want to scan.

5. Create a tag for the assets. You can create this tag based on the account IDs, VPCs, instance types, or the AWS discovery source.



Edit Tag - AWS: VPCSHARE

General

CATEGORY: AWS

VALUE: VPCSHARE

CATEGORY DESCRIPTION (OPTIONAL)

VALUE DESCRIPTION (OPTIONAL)

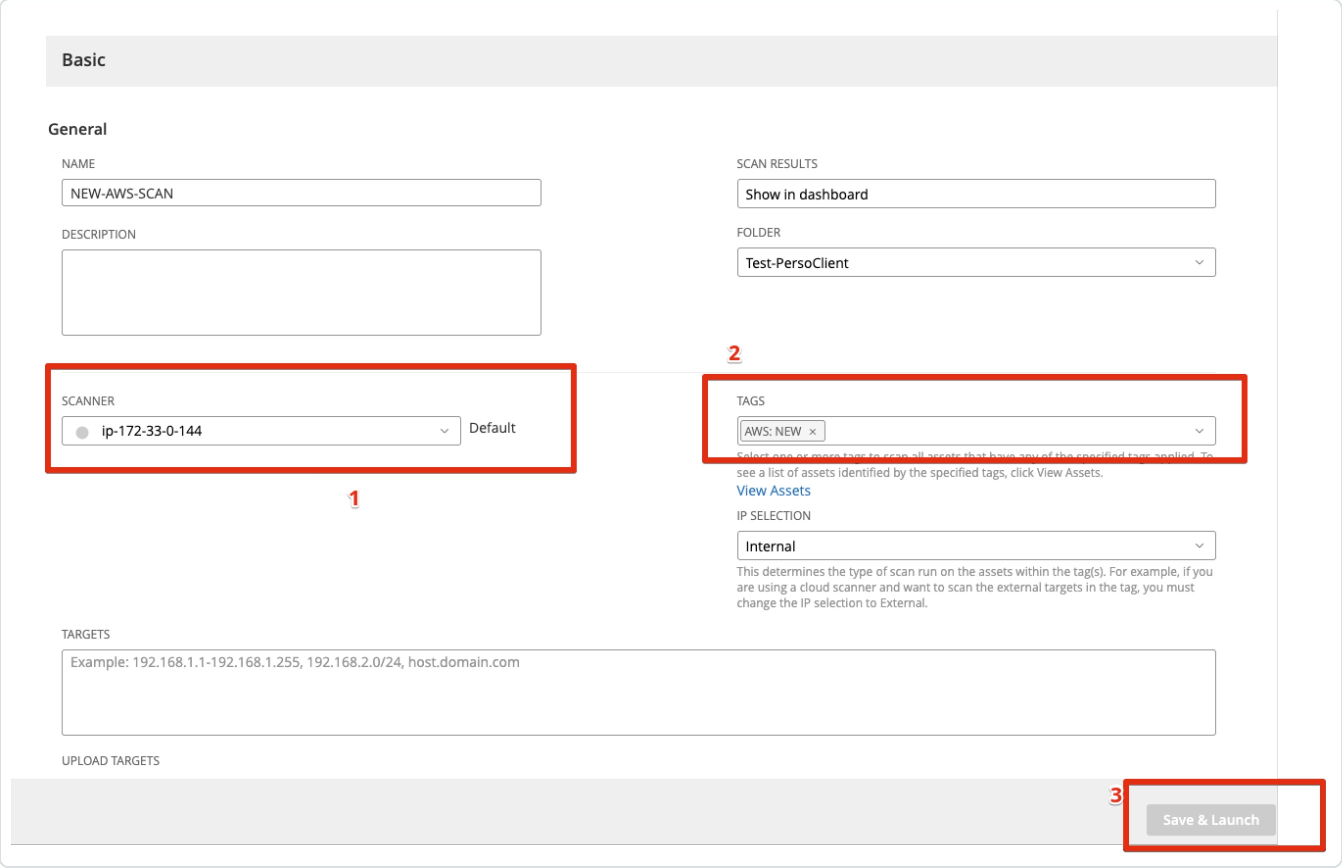
Rules

Match Any

AWS Owner	is equal to	840[redacted]
AWS Owner	is equal to	977[redacted]
AWS Owner	is equal to	539[redacted]

This tag would apply to a minimum of 16 assets.

6. Create a scan, and select the tag you created in Step 5 in the **Basic** settings.



Basic

General

NAME: NEW-AWS-SCAN

DESCRIPTION:

SCANNER: ip-172-33-0-144 Default

SCAN RESULTS: Show in dashboard

FOLDER: Test-PersoClient

TAGS: AWS: NEW ×

Select one or more tags to scan all assets that have any of the specified tags applied. To see a list of assets identified by the specified tags, click View Assets.

View Assets

IP SELECTION: Internal

This determines the type of scan run on the assets within the tag(s). For example, if you are using a cloud scanner and want to scan the external targets in the tag, you must change the IP selection to External.

TARGETS: Example: 192.168.1.1-192.168.1.255, 192.168.2.0/24, host.domain.com

UPLOAD TARGETS

7. Launch the scan.

   The scan will display results from across all the scanned VPCs.

Pre-Authorized Scanner

The following feature is not supported in Tenable Vulnerability Management Federal Risk and Authorization Management Program (FedRAMP) environments. For more information, see the FedRAMP Product Offering.

Caution: This version of the AWS pre-authorized scanner has been removed and is no longer available to new customers.

To begin the Pre-Authorized Scanner AWS configuration, you must first create an Identity and Access Management (IAM) role. This role eliminates the need to store AWS access keys by providing the scanner instance with temporary AWS credentials. Once created, the IAM role is assigned to the Tenable Nessus instance(s) as seen in the *Launch Nessus Scanner Instance* section below. Additionally, this role must also have the Describe VPC Peering Connections role. The VPC peering relationship must be from the VPC containing the pre-authorized Tenable Nessus scanner (requestor) to the VPC(s) you want to scan.

Note: Pre-Authorized Scanner scans by instance ID and cannot be used in scans to target hosts by IP address. Configuring Pre-Authorized Scanner scans to target hosts by IP address will return an error.

Obtain Tenable Vulnerability Management Linking Key

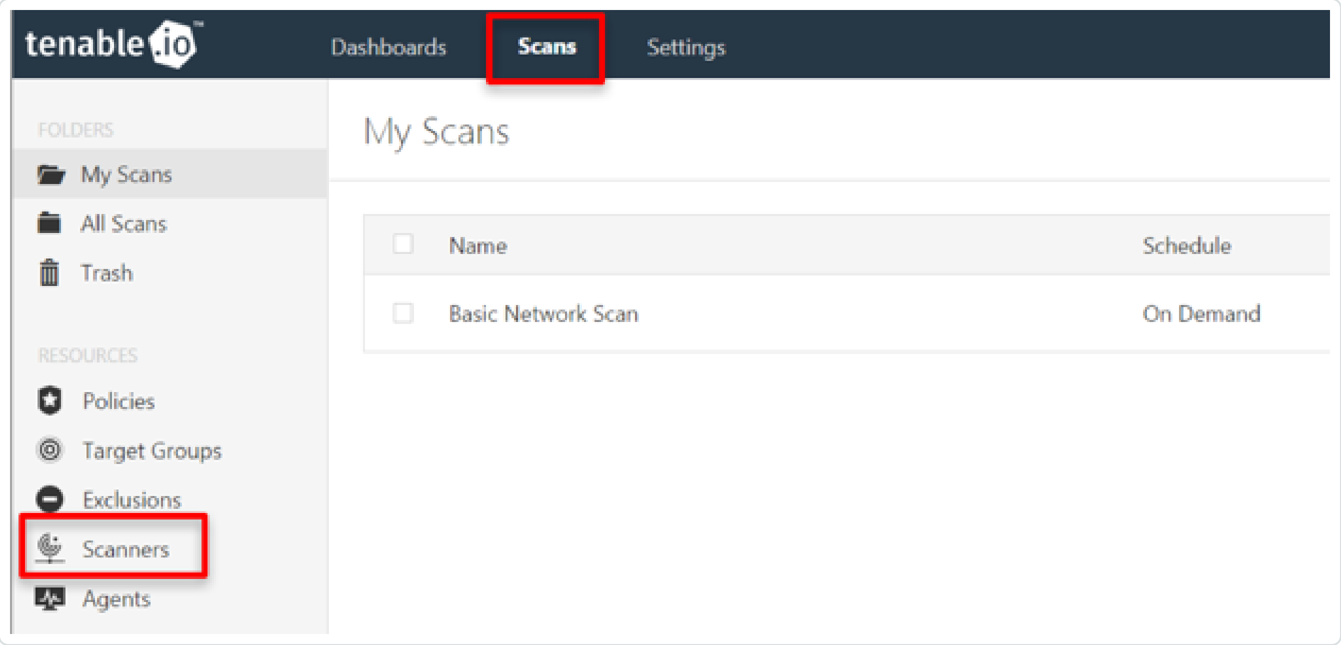
Caution: This version of the AWS pre-authorized scanner has been removed and is no longer available to new customers.

1. Once you have created a Tenable Vulnerability Management account, log in to https://cloud.tenable.com.

2. In the top menu bar, click **Scans**.

3. In the left-hand menu, click **Scanners**.

   The **Scanners** page appears.

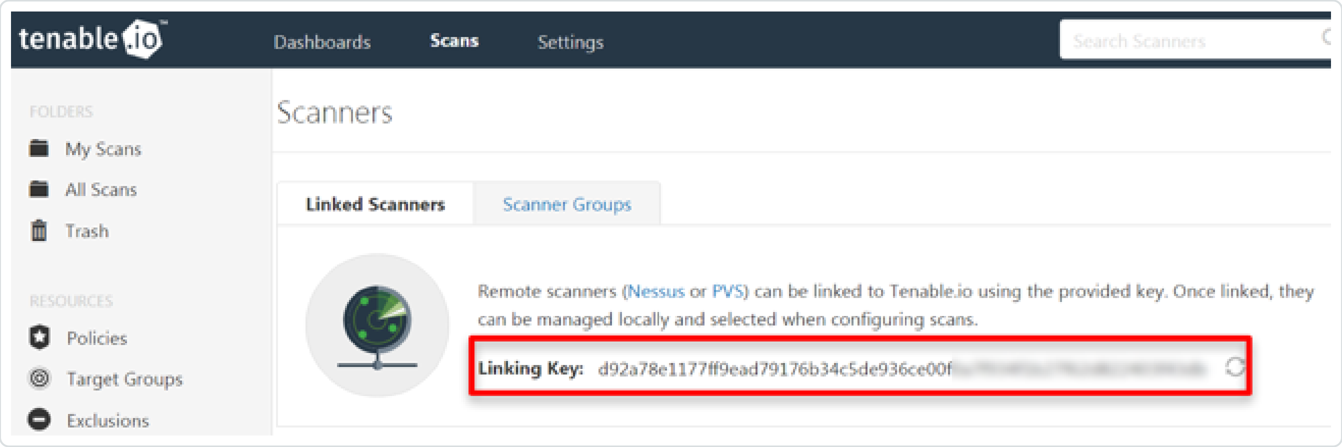


☐	Name	Schedule
☐	Basic Network Scan	On Demand

4. Click the **Linked Scanners** tab.

5. Copy and save the **Linking Key**.

   Tip: This key is needed during the AWS configuration steps.



Remote scanners (Nessus or PVS) can be linked to Tenable.io using the provided key. Once linked, they can be managed locally and selected when configuring scans.

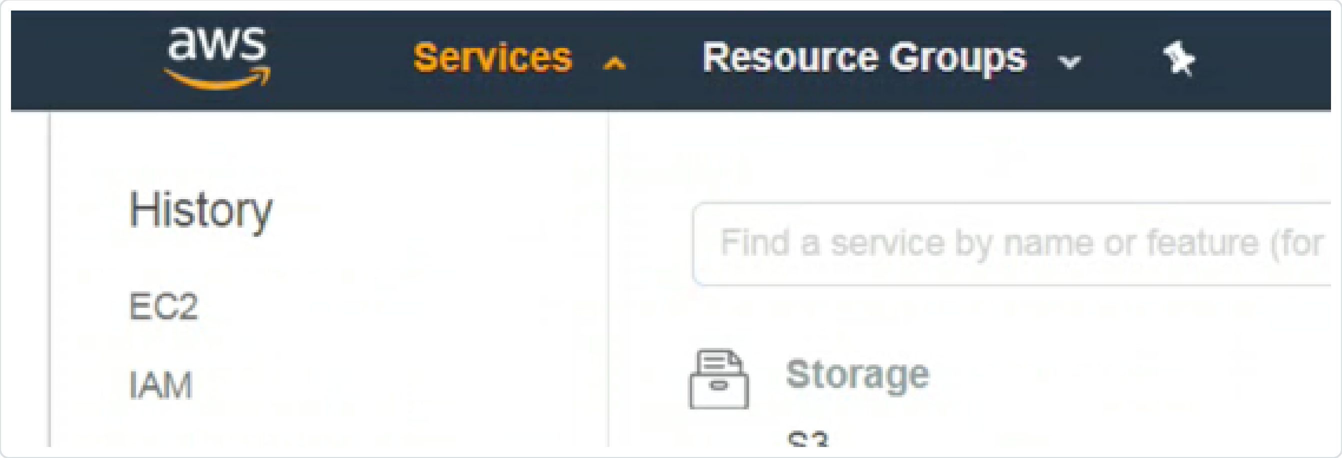
Linking Key: d92a78e1177ff9ead79176b34c5de936ce00f[redacted]

Create an AWS IAM Role

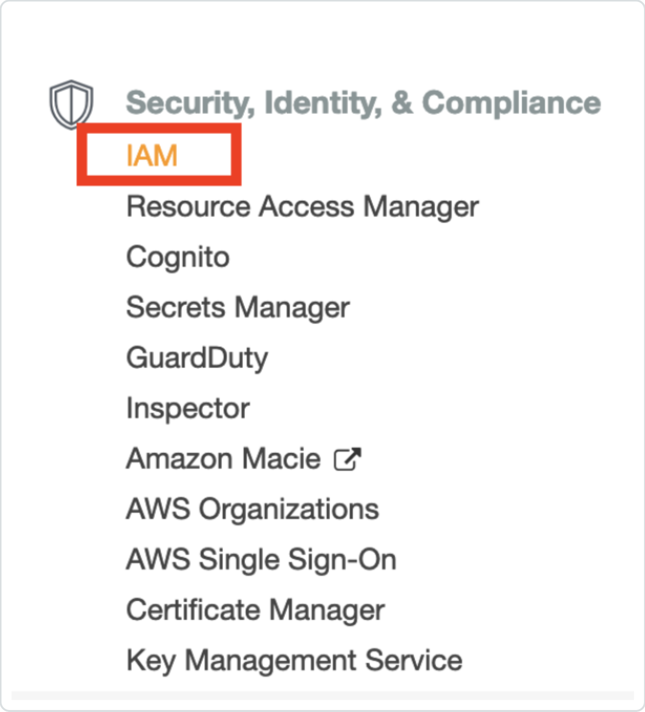
Caution: This version of the AWS pre-authorized scanner has been removed and is no longer available to new customers.

1. Navigate to https://aws.amazon.com and log in.
2. In the top menu bar, click **Services**.

   Note: Amazon is continually updating their service, so screenshots may differ from the AWS interface you see.



3. In the **Security, Identity, and Compliance** section, click **IAM**.



Security, Identity, & Compliance

IAM

Resource Access Manager

Cognito

Secrets Manager

GuardDuty

Inspector

Amazon Macie

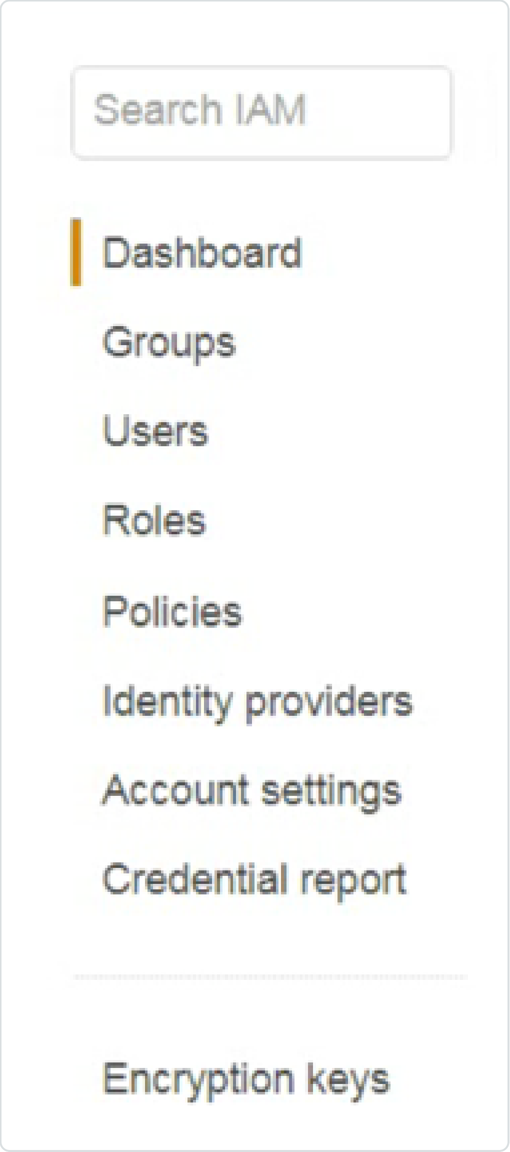
AWS Organizations

AWS Single Sign-On

Certificate Manager

Key Management Service

4. In the left-hand menu, click **Roles**.



Search IAM

Dashboard

Groups

Users

Roles

Policies

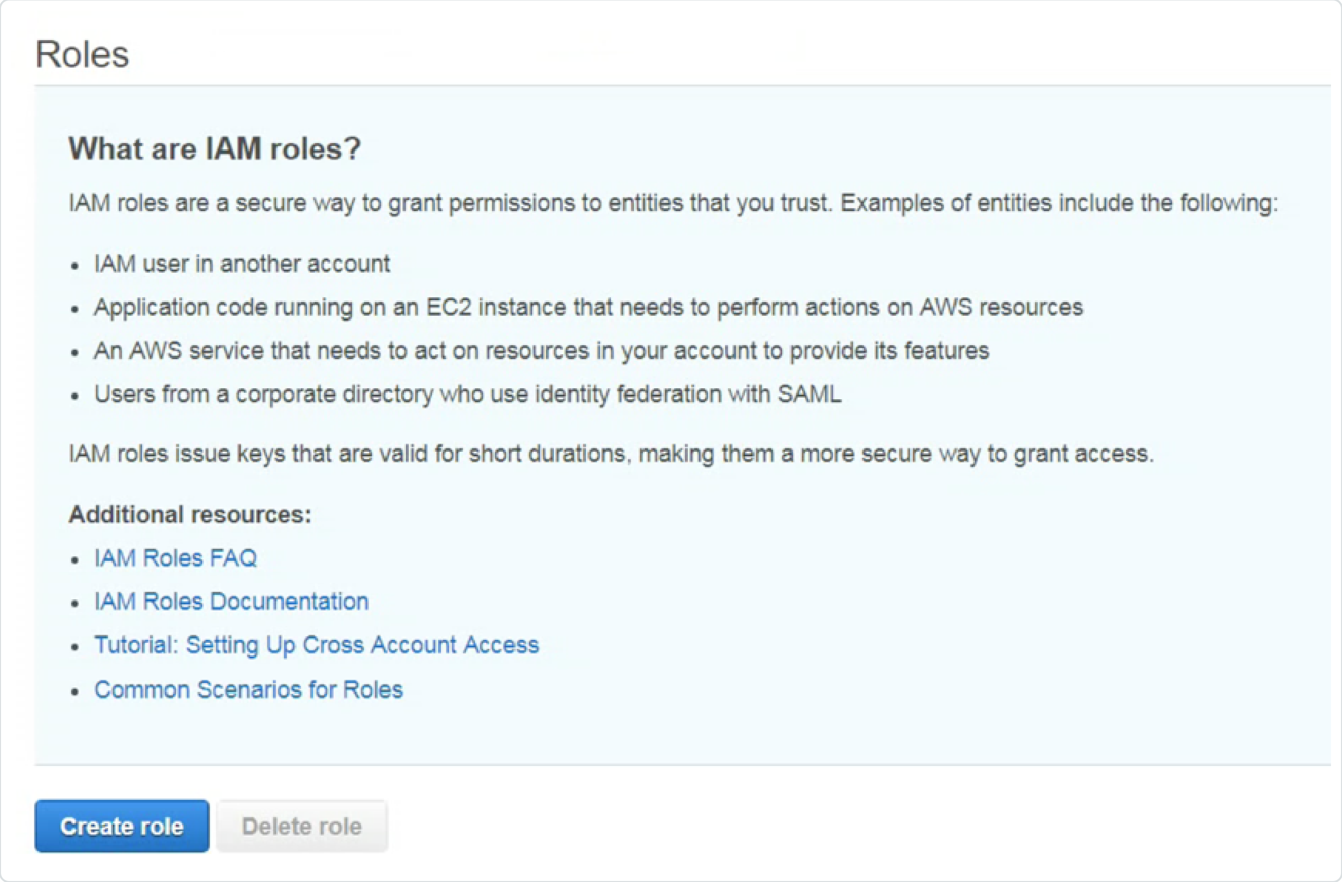
Identity providers

Account settings

Credential report

Encryption keys

5. Click **Create Role**.



Roles

What are IAM roles?

IAM roles are a secure way to grant permissions to entities that you trust. Examples of entities include the following:

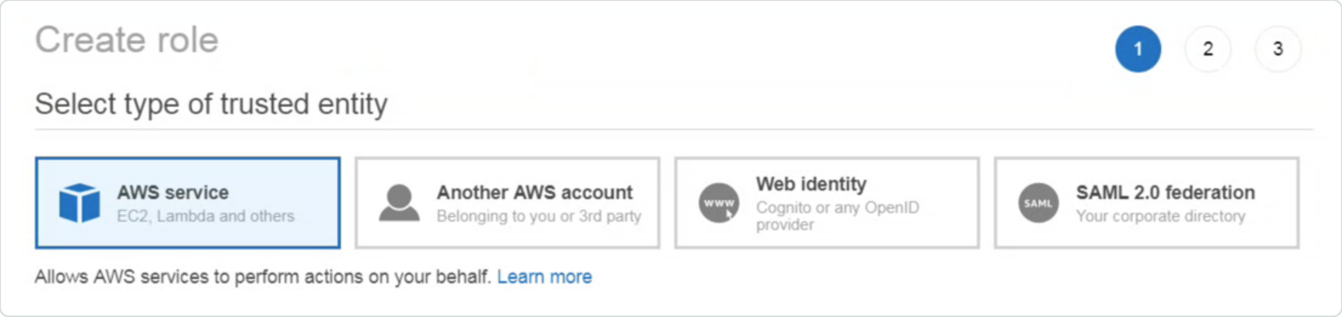
- IAM user in another account
- Application code running on an EC2 instance that needs to perform actions on AWS resources
- An AWS service that needs to act on resources in your account to provide its features
- Users from a corporate directory who use identity federation with SAML

IAM roles issue keys that are valid for short durations, making them a more secure way to grant access.

Additional resources:

- IAM Roles FAQ
- IAM Roles Documentation
- Tutorial: Setting Up Cross Account Access
- Common Scenarios for Roles

6. In the **Select Type of Trusted Entity** section, select **AWS Service**.



Create role

Select type of trusted entity

Allows AWS services to perform actions on your behalf. Learn more

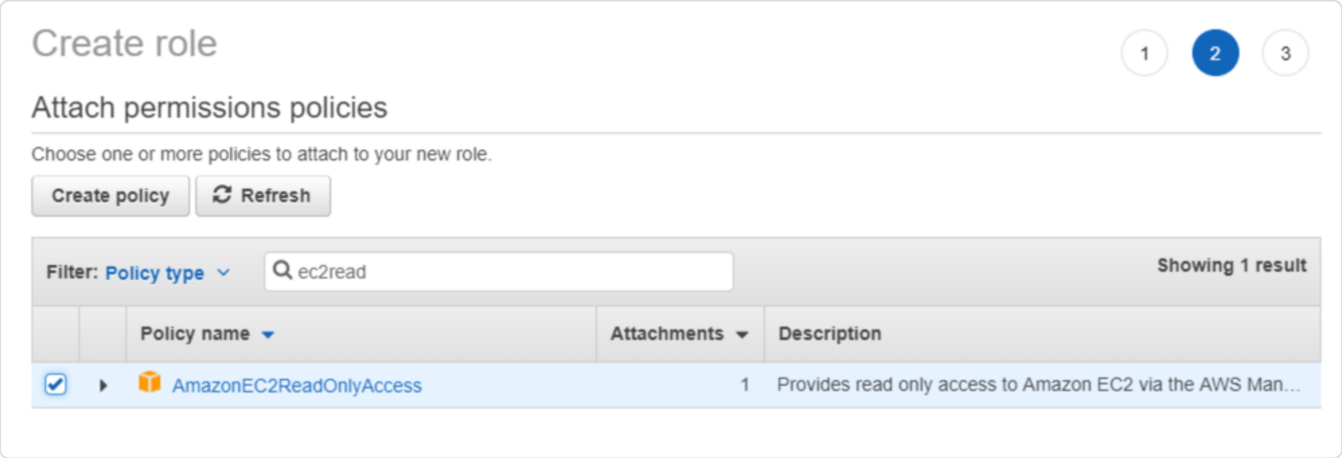
7. In the **Choose the service that will use this role** section, click **EC2**.

> **Note:** EC2 assets must be activated for your AWS license in order to scan them. If you are going to use the Pre-authorized scanner in AWS, you are required to activate your assets.
>
> The AWS acceptable scanning policy prevents scanning the m1.small, t1.micro or t2.nano instances.

8. In the **Select your use case section**, click **EC2**.

9. Click **Next: Permissions**.

10. Select the **AmazonEC2ReadOnlyAccess** check box.



Create role

Attach permissions policies

Choose one or more policies to attach to your new role.

Filter: Policy type ⌄ ec2read

Showing 1 result

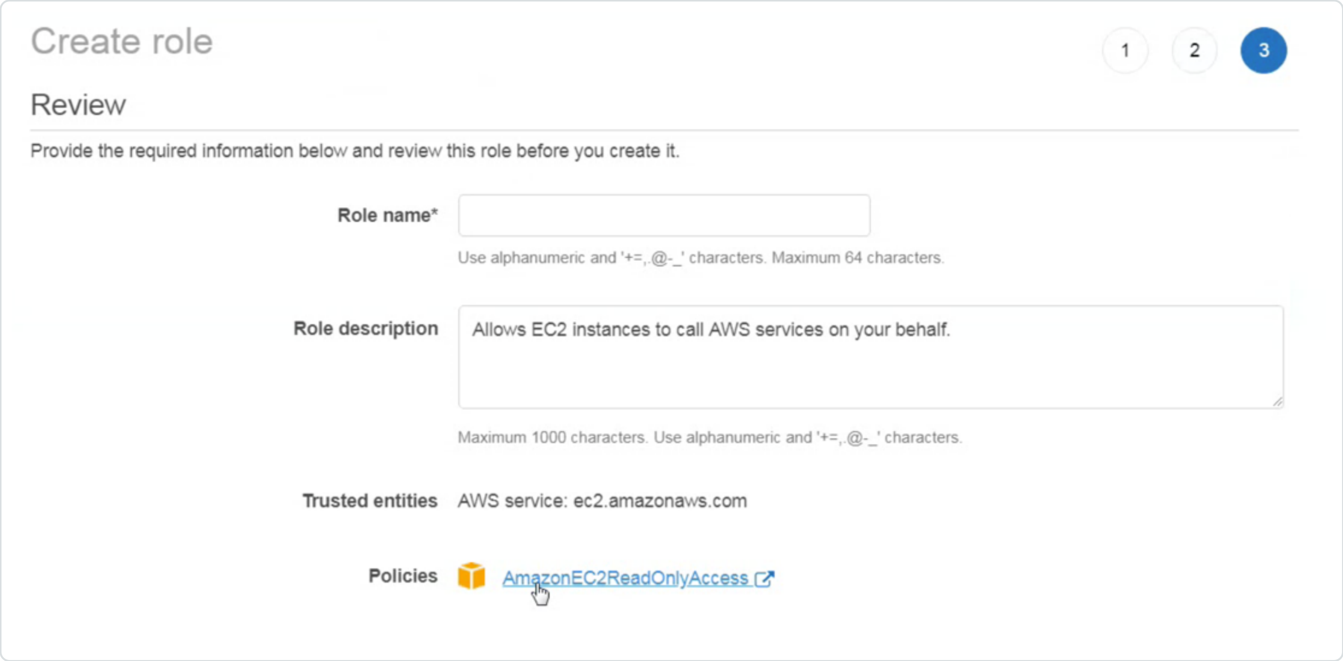
		Policy name ▾	Attachments ▾	Description
☑	▸	AmazonEC2ReadOnlyAccess	1	Provides read only access to Amazon EC2 via the AWS Man...

11. In the **Set Permissions Boundary** section, ensure the **Create role without a permissions boundary** radio button is selected.

12. Click **Next: Review**.

13. In the **Role Name** field, enter a descriptive name for the role.

> **Note:** The role name cannot be edited once it is created.



Review

Provide the required information below and review this role before you create it.

Role name*

Use alphanumeric and '+=,.@-_' characters. Maximum 64 characters.

Role description: Allows EC2 instances to call AWS services on your behalf.

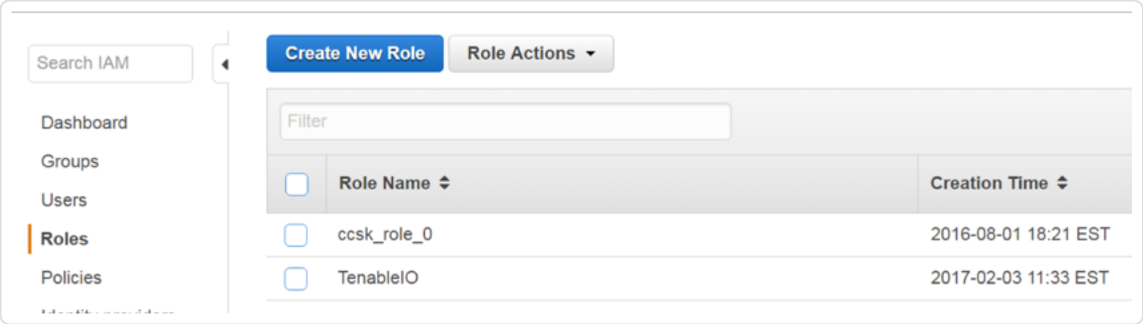
Maximum 1000 characters. Use alphanumeric and '+=,.@-_' characters.

Trusted entities: AWS service: ec2.amazonaws.com

Policies: AmazonEC2ReadOnlyAccess

14. Once you have reviewed the the IAM information, click **Create Role**.

    The newly created IAM role appears in the role list.



	Role Name	Creation Time
□	ccsk_role_0	2016-08-01 18:21 EST
□	TenableIO	2017-02-03 11:33 EST

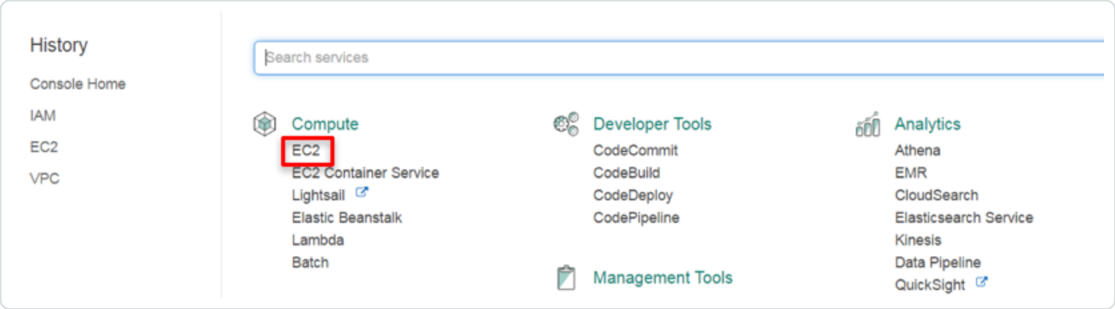
Launch Pre-Authorized Nessus Scanner

Caution: This version of the AWS pre-authorized scanner has been removed and is no longer available to new customers.

Note: You do not need SSH access or a key pair to launch the instance.

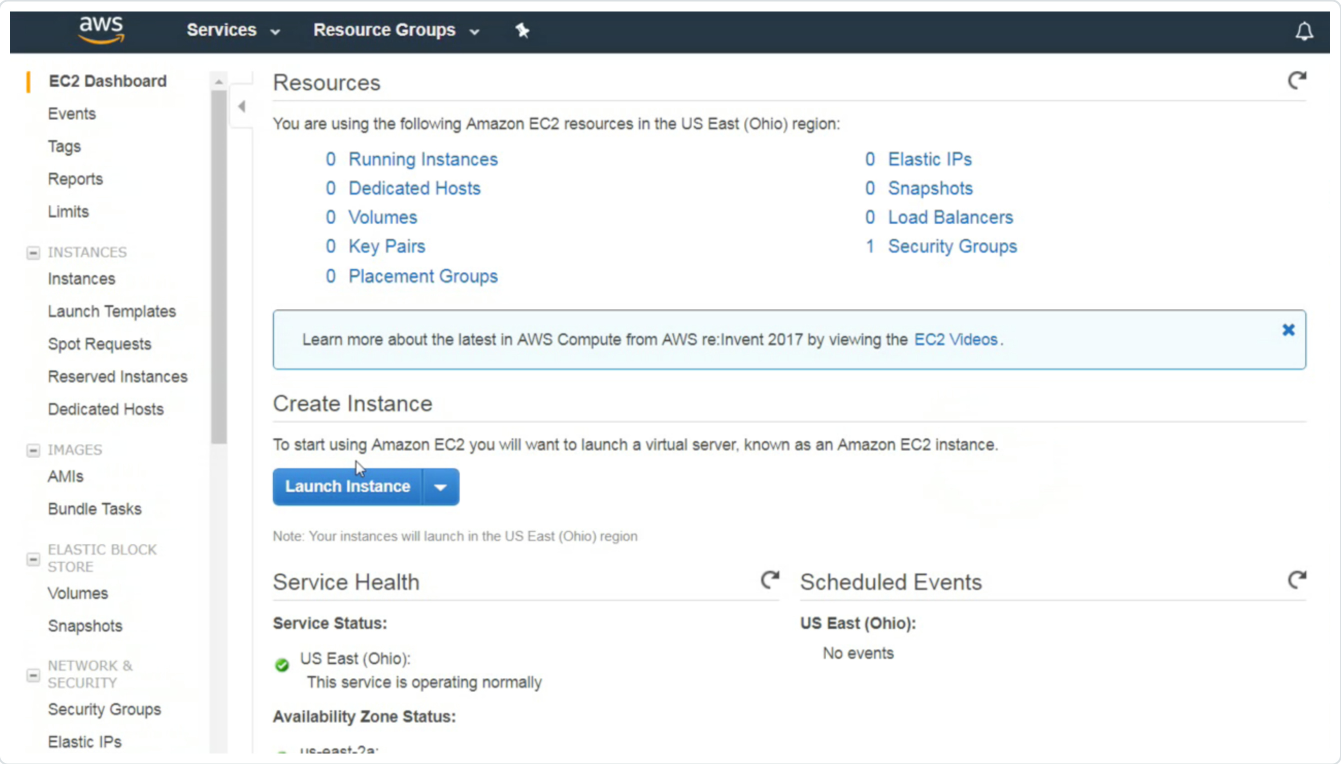
Note: You must use an Elastic IP address for the scanner to work properly.

1. In the top-menu bar, click **Services**.
2. In the **Compute** section, click **EC2** to begin launching the pre-authorized scanner instance.



The **EC2 Dashboard** appears.

3. Click **Launch Instance** to create an Amazon EC2 instance (virtual server).



Resources

You are using the following Amazon EC2 resources in the US East (Ohio) region:

0 Running Instances	0 Elastic IPs
0 Dedicated Hosts	0 Snapshots
0 Volumes	0 Load Balancers
0 Key Pairs	1 Security Groups
0 Placement Groups	

Learn more about the latest in AWS Compute from AWS re:Invent 2017 by viewing the EC2 Videos.

Create Instance

To start using Amazon EC2 you will want to launch a virtual server, known as an Amazon EC2 instance.

Note: Your instances will launch in the US East (Ohio) region

Service Health

Service Status:

US East (Ohio):
This service is operating normally

Availability Zone Status:

us-east-2a:

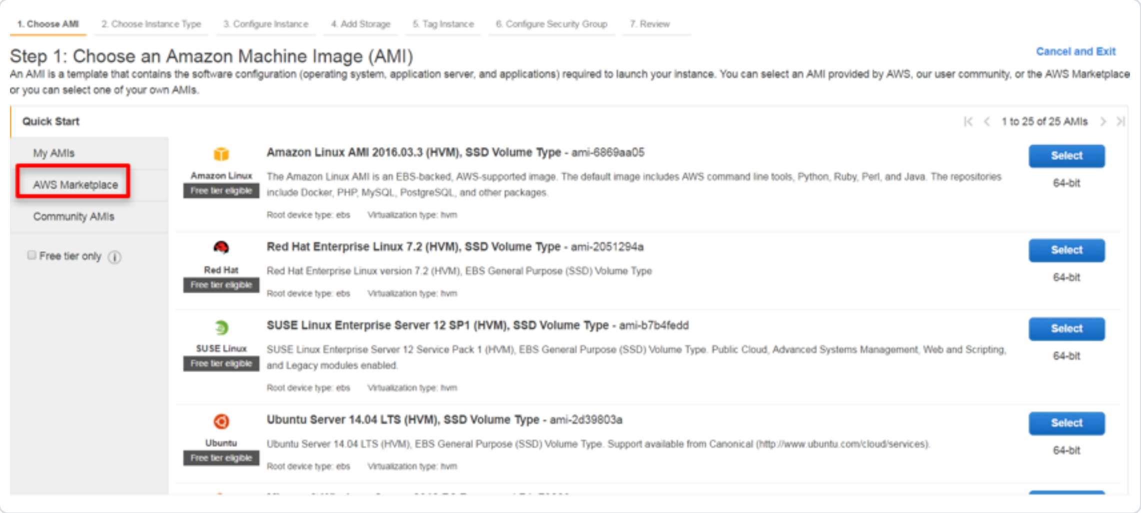
Scheduled Events

US East (Ohio):

No events

The **Choose an Amazon Machine Image (AMI)** page appears.

4. In the left panel, click **AWS Marketplace**.



Step 1: Choose an Amazon Machine Image (AMI)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace or you can select one of your own AMIs.

Amazon Linux AMI 2016.03.3 (HVM), SSD Volume Type - ami-6869aa05
The Amazon Linux AMI is an EBS-backed, AWS-supported image. The default image includes AWS command line tools, Python, Ruby, Perl, and Java. The repositories include Docker, PHP, MySQL, PostgreSQL, and other packages.
Root device type: ebs Virtualization type: hvm
64-bit

Red Hat Enterprise Linux 7.2 (HVM), SSD Volume Type - ami-2051294a
Red Hat Enterprise Linux version 7.2 (HVM), EBS General Purpose (SSD) Volume Type
Root device type: ebs Virtualization type: hvm
64-bit

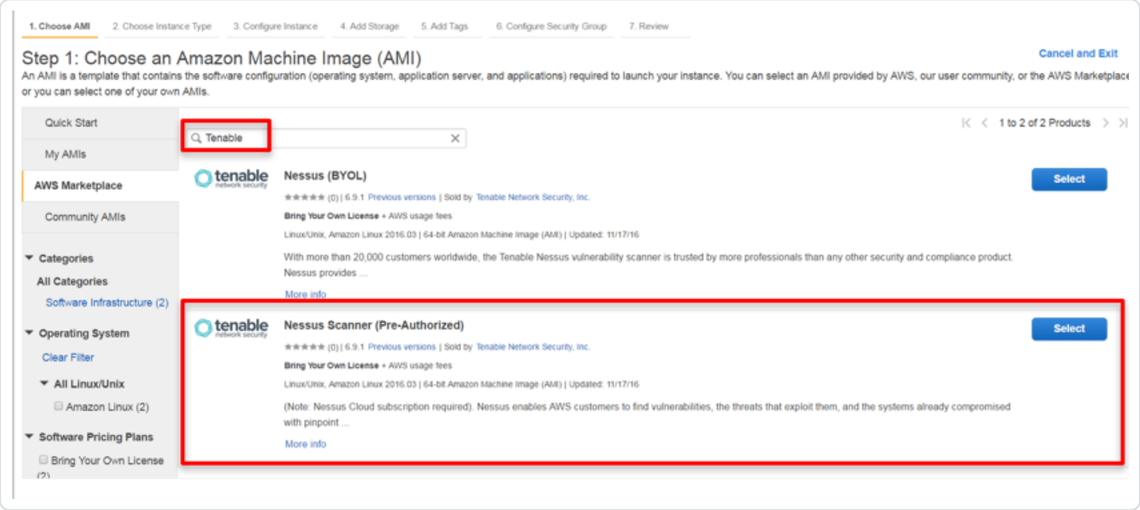
SUSE Linux Enterprise Server 12 SP1 (HVM), SSD Volume Type - ami-b7b4fedd
SUSE Linux Enterprise Server 12 Service Pack 1 (HVM), EBS General Purpose (SSD) Volume Type. Public Cloud, Advanced Systems Management, Web and Scripting, and Legacy modules enabled.
Root device type: ebs Virtualization type: hvm
64-bit

Ubuntu Server 14.04 LTS (HVM), SSD Volume Type - ami-2d39803a
Ubuntu Server 14.04 LTS (HVM), EBS General Purpose (SSD) Volume Type. Support available from Canonical (http://www.ubuntu.com/cloud/services).
Root device type: ebs Virtualization type: hvm
64-bit

5. In the **Search** box, type **Tenable**.

6. On your keyboard, press **Enter**.

7. Select **Nessus Scanner (Pre-Authorized)**.



Step 1: Choose an Amazon Machine Image (AMI)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace or you can select one of your own AMIs.

Nessus (BYOL)

★★★★★ (0) | 6.9.1 Previous versions | Sold by Tenable Network Security, Inc.

Bring Your Own License + AWS usage fees

Linux/Unix, Amazon Linux 2016.03 | 64-bit Amazon Machine Image (AMI) | Updated: 11/17/16

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 provides ...

More info

Nessus Scanner (Pre-Authorized)

★★★★★ (0) | 6.9.1 Previous versions | Sold by Tenable Network Security, Inc.

Bring Your Own License + AWS usage fees

Linux/Unix, Amazon Linux 2016.03 | 64-bit Amazon Machine Image (AMI) | Updated: 11/17/16

(Note: Nessus Cloud subscription required). Nessus enables AWS customers to find vulnerabilities, the threats that exploit them, and the systems already compromised with pinpoint ...

More info

8. Click **Continue**.

   The **Step 2: Choose an Instance Type** page appears.

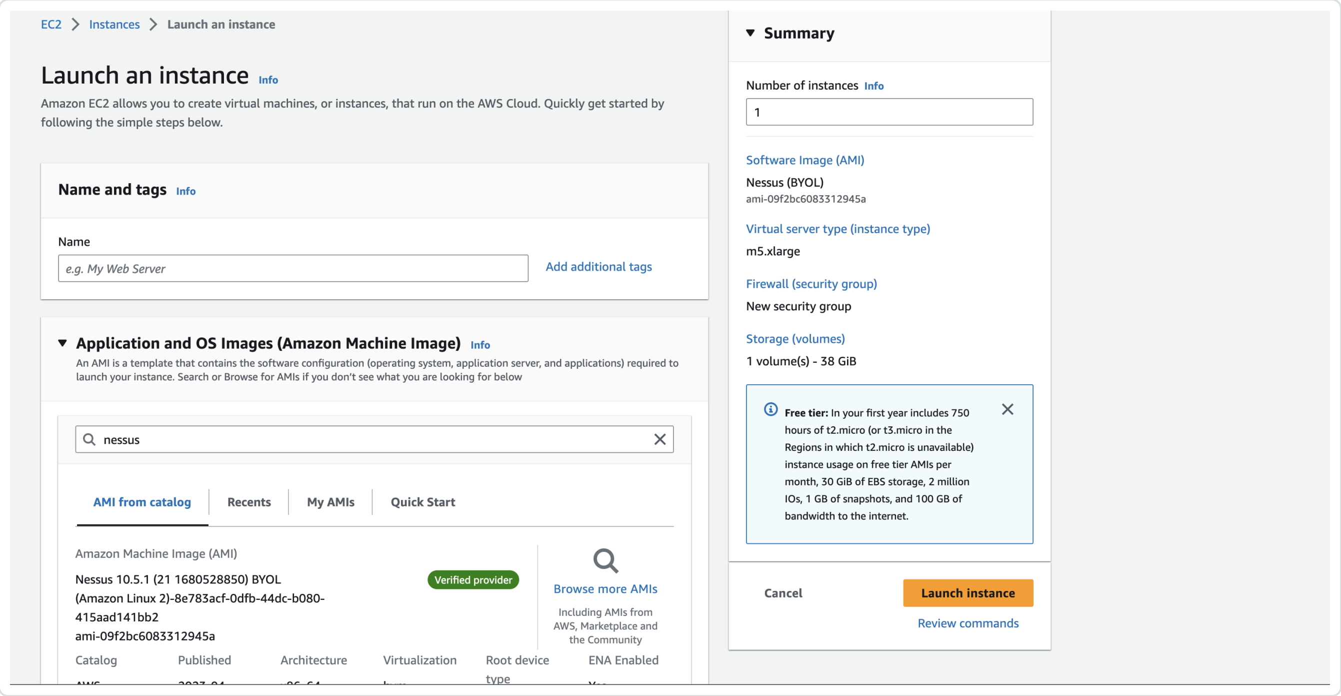
9. Select the instance type for the scanner.

   > **Note**: The available instances meet the minimum product requirements, however, Tenable recommends selecting the instance that best suits your customer-specific needs. For more information, see Nessus General Requirements.

   > **Tip:** The instances offer various combinations of CPU, memory, storage, and network performance. Refer to Amazon EC2 Pricing for more details on Amazon's pricing structure.

10. Click **Next: Launch an instance**.

    The **Launch an instance** page appears.



EC2 > Instances > Launch an instance

Launch an instance Info

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags Info

Name

e.g. My Web Server

Add additional tags

▼ Application and OS Images (Amazon Machine Image) Info

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

nessus

Amazon Machine Image (AMI)

Nessus 10.5.1 (21 1680528850) BYOL (Amazon Linux 2)-8e783acf-0dfb-44dc-b080-415aad141bb2
ami-09f2bc6083312945a

Verified provider

Browse more AMIs

Including AMIs from AWS, Marketplace and the Community

Catalog Published Architecture Virtualization Root device type ENA Enabled

▼ Summary

Number of instances Info

1

Software Image (AMI)
Nessus (BYOL)
ami-09f2bc6083312945a

Virtual server type (instance type)
m5.xlarge

Firewall (security group)
New security group

Storage (volumes)
1 volume(s) - 38 GiB

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 30 GiB of EBS storage, 2 million IOs, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

11. In the **Number of Instances** field, type the number of AMI instances to deploy.

12. In the **Purchasing Option** section, select the **Request Spot Instances** check box to launch an instance at spot prices rather than on-demand prices. Refer to Spot Instances for details.

> **Note:** By default, this option is disabled.

13. From the **Network** drop-down box, select the Amazon VPC in which to launch the instance.

> **Tip:** To create a new VPC, click **Create new VPC**.

14. From the **Subnet** drop-down box, select the subnet within the previously chosen VPC.

> **Tip:** To create a new subnet, click **Create new subnet**.

15. Choose an IP address/subnet that permits the scanner to access https://cloud.tenable.com and AWS APIs.

> **Note:** (Optional) To request a public IP address from Amazon's public pool, enable the **Auto-assign Public IP** option.

16. From the IAM Role drop-down box, select the required IAM role.

    > **Tip:** To create a new role, click the **Create new IAM role** and follow the Create AWS IAM Role instructions in this document. For more information on IAM roles, refer to IAM Roles for Amazon EC2.

17. From the **Shutdown Behavior** drop-down box, select either **Stop** or **Terminate** to determine the instance behavior when an OS-level shutdown is performed.

18. (Optional) To prevent an instance from accidental termination, select the **Enable termination protection** check box.

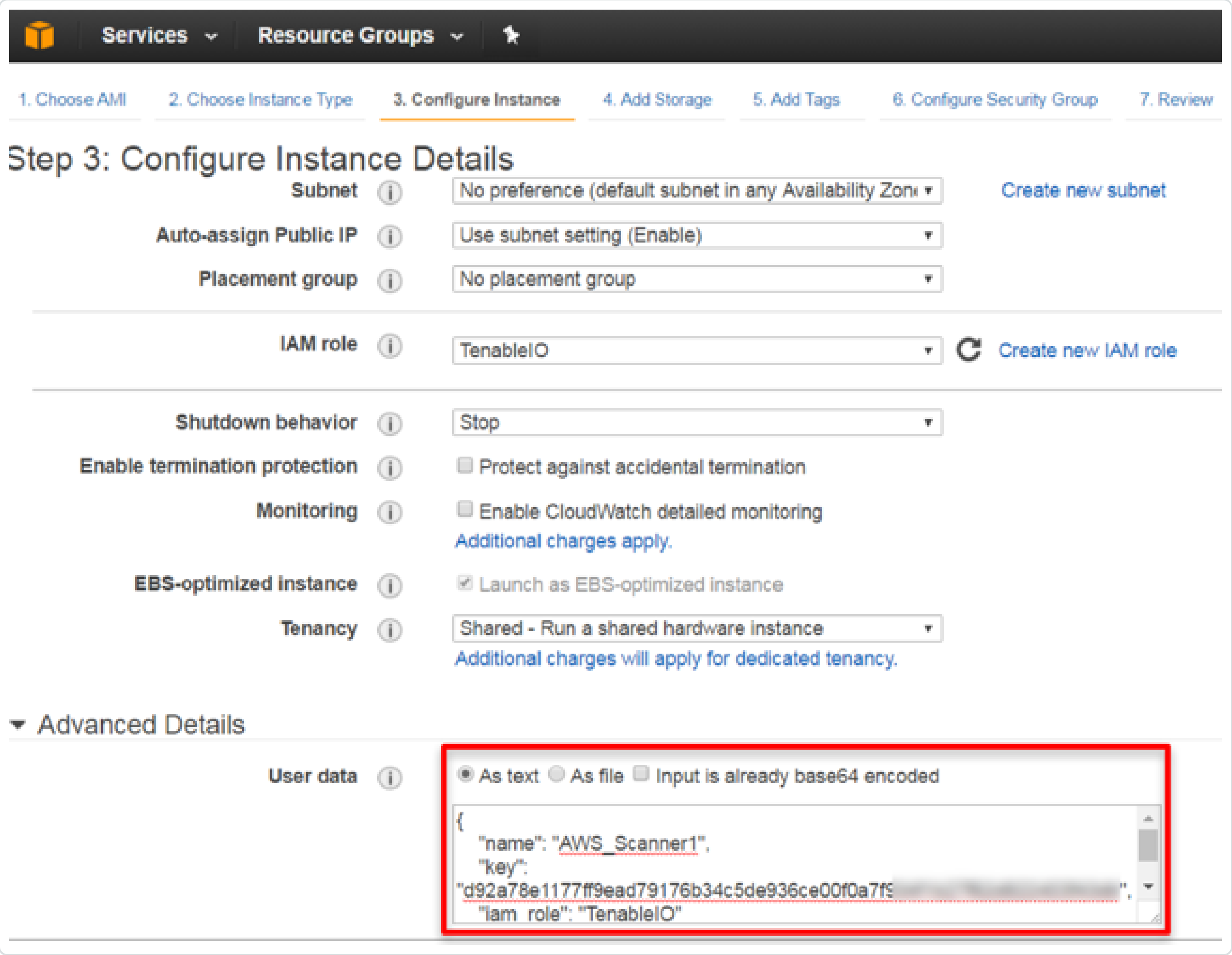
19. (Optional) To monitor, collect, and analyze metrics about the instances, select the **Monitoring** check box.

20. (Optional) To allow for improved performance for Amazon EBS volumes through the use of dedicated throughput between Amazon EC2 and Amazon EBS, ensure you select the **EBS-optimized instance** check box.

21. From the **Tenancy** drop-down box, select whether you want the instance to run on a dedicated or shared host. For more information on dedicated hosts, refer to Amazon EC2 Dedicated Hosts.

    > **Note:** By default, the **Shared** option is selected.

22. Click **Advanced Details**.



Step 3: Configure Instance Details

Subnet: No preference (default subnet in any Availability Zone

Auto-assign Public IP: Use subnet setting (Enable)

Placement group: No placement group

IAM role: TenableIO

Shutdown behavior: Stop

Enable termination protection: □ Protect against accidental termination

Monitoring: □ Enable CloudWatch detailed monitoring
Additional charges apply.

EBS-optimized instance: ☑ Launch as EBS-optimized instance

Tenancy: Shared - Run a shared hardware instance
Additional charges will apply for dedicated tenancy.

▾ Advanced Details

User data: ● As text ○ As file □ Input is already base64 encoded

```
{
  "name": "AWS_Scanner1",
  "key":
"d92a78e1177ff9ead79176b34c5de936ce00f0a7f9[redacted]",
  "iam_role": "TenableIO"
```

23. In the **User Data** section, select the **As Text** radio button.

24. In the text field, enter the scanner name, the **Linking Key** previously copied from Tenable Vulnerability Management, and the previously created IAM role in JSON format:

```
{
"name": "AWS_Scanner",
"key":"d92a78e1177ff9ead79176b34c5de936ce00f0a7.......",
"aws_scanner": true,
"iam_role": "TenableIO",
"proxy": "10.11.12.13",
"proxy_port": "8080"
}
```

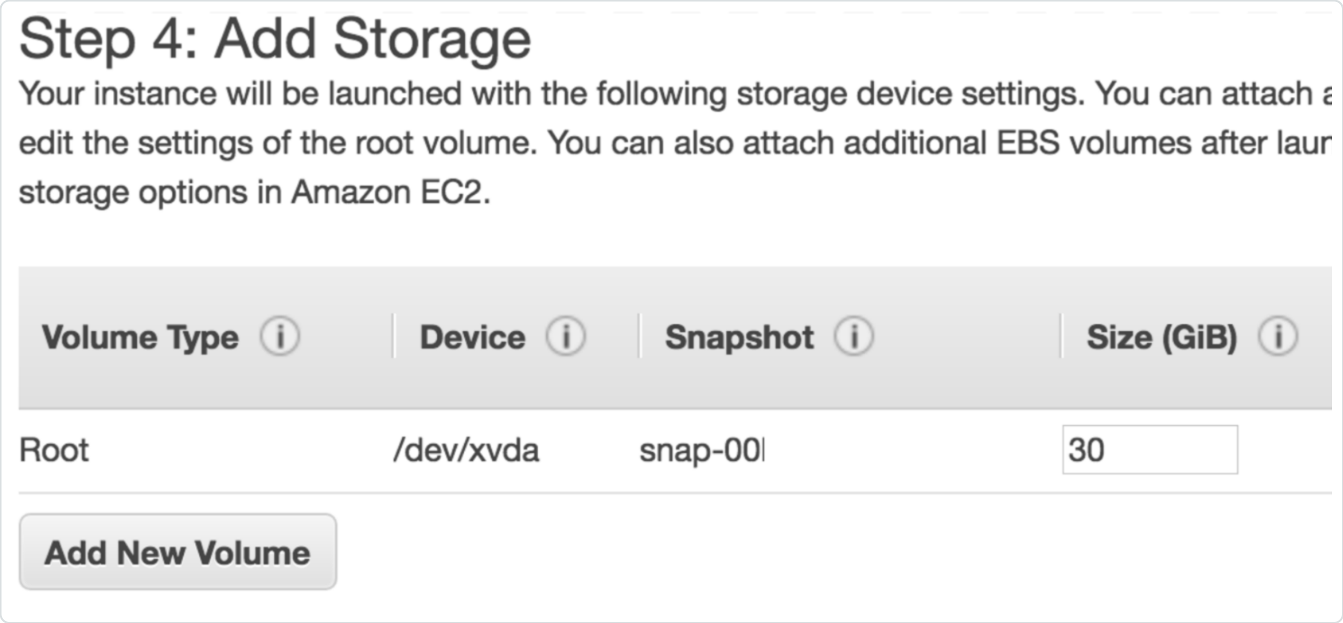
Note: The **key** and **aws_scanner** are both required entries in the **User Data** field. The following table lists acceptable entries.

Parameter	Description
aws_scanner	Configure the scanner in the pre-auth/AWS scanner mode.
name	Name of the scanner shown in the Nessus user interface (recommended). If a name is not specified, it defaults to the instance ID.
key	Linking key used to register scanner with Tenable Vulnerability Management. Only used during initial registration (required).
iam_role	Name of the IAM role assigned to the scanner instance (required).
proxy	FQDN/IP address of proxy, if required.
proxy_port	Port used to connect to proxy, if required.

25. Click **Next: Add Storage**.

    The **Step 4: Add Storage** page appears.

26. In the **Size** field, enter a value of 30 or higher.



Step 4: Add Storage

Your instance will be launched with the following storage device settings. You can attach a edit the settings of the root volume. You can also attach additional EBS volumes after laur storage options in Amazon EC2.

Volume Type	Device	Snapshot	Size (GiB)
Root	/dev/xvda	snap-00	30

> **Note:** Tenable Nessus Network Monitor requires the pre-authorized Nessus scanners to have a minimum of 30GB of storage.

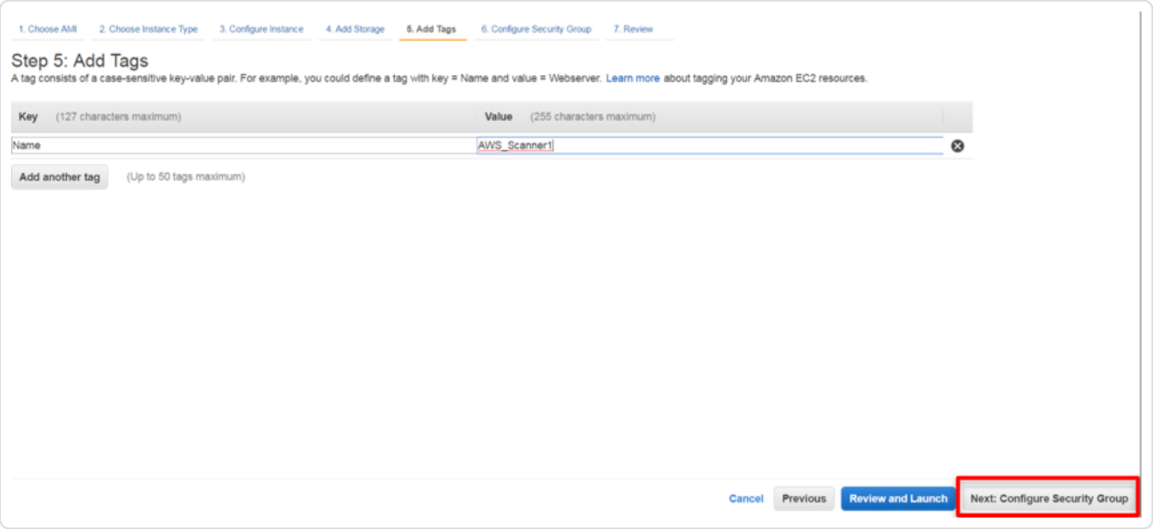
27. Select the **Delete on Termination** check box.

28. Click **Next: Add Tags**.

    The **Step 5: Add Tags** page appears.

29. Click **Add another tag** for as many tags as you want to create to help manage and categorize your AWS EC2 resources.

> **Note:** Each tag requires both a **Key** and a **Value**, and each resource can have a maximum of 10 tags. For more information on tags, refer to Tagging Your Amazon EC2 Resources.



Step 5: Add Tags

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver. Learn more about tagging your Amazon EC2 resources.

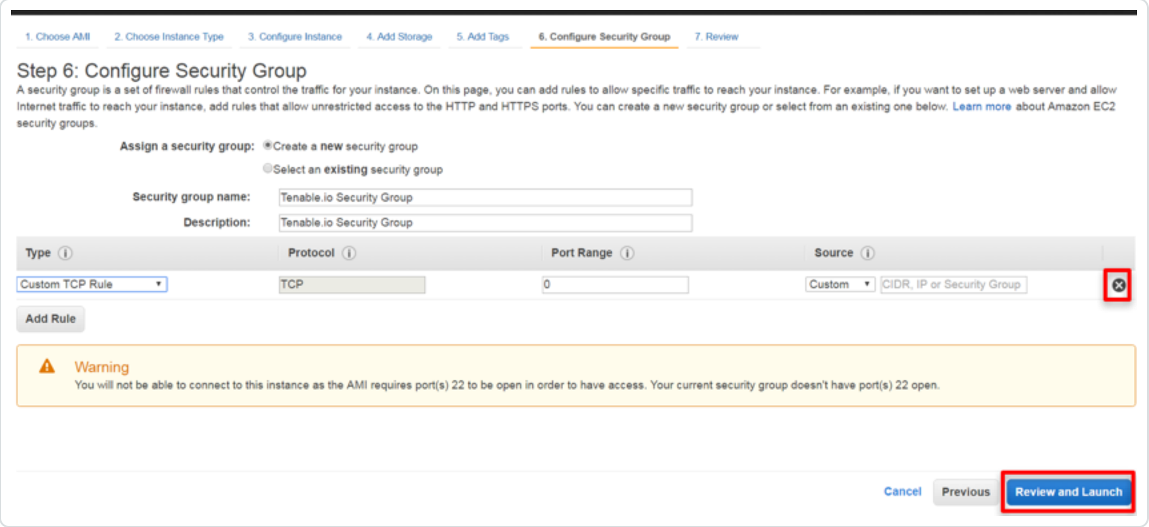
Key (127 characters maximum)	Value (255 characters maximum)
Name	AWS_Scanner1

30. Click **Next: Configure Security Group**.

    The **Step 6: Configure Security Group** page appears.

    > **Tip:** Here, you are creating a security group to which only the Nessus Scanner belongs. You create this to assign it as the source to scan target security groups.

31. In the **Assign a security group** section, select the **Create a new security group** radio button.



Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. Learn more about Amazon EC2 security groups.

Assign a security group: ● Create a **new** security group
○ Select an **existing** security group

Security group name: Tenable.io Security Group

Description: Tenable.io Security Group

Type	Protocol	Port Range	Source
Custom TCP Rule	TCP	0	Custom CIDR, IP or Security Group

Warning
You will not be able to connect to this instance as the AMI requires port(s) 22 to be open in order to have access. Your current security group doesn't have port(s) 22 open.

32. In the **Security group name** field, enter a descriptive name for the security group.

33. In the **Description** field, enter a description of the security group.

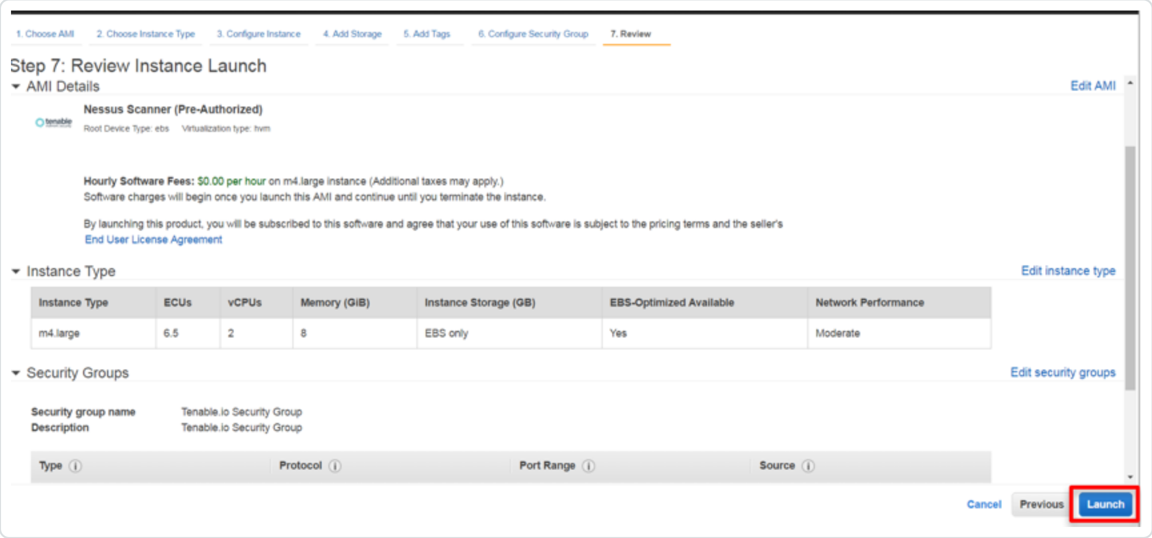
34. In the following **Rules** section, click the **X** to the right of the **Security Group** rule to delete it.

> **Note:** There is no way to access the AMI directly, so removing this rule prevents any inbound traffic and is essentially a deny-all firewall rule.

35. Click **Review and Launch**.

    The **Step 7: Review Instance Launch** page appears.

36. Once you have reviewed the instance, click **Launch**.



Step 7: Review Instance Launch

AMI Details

Nessus Scanner (Pre-Authorized)

Root Device Type: ebs   Virtualization type: hvm

Hourly Software Fees: $0.00 per hour on m4.large instance (Additional taxes may apply.)
Software charges will begin once you launch this AMI and continue until you terminate the instance.

By launching this product, you will be subscribed to this software and agree that your use of this software is subject to the pricing terms and the seller's End User License Agreement

Instance Type

Instance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
m4.large	6.5	2	8	EBS only	Yes	Moderate

Security Groups

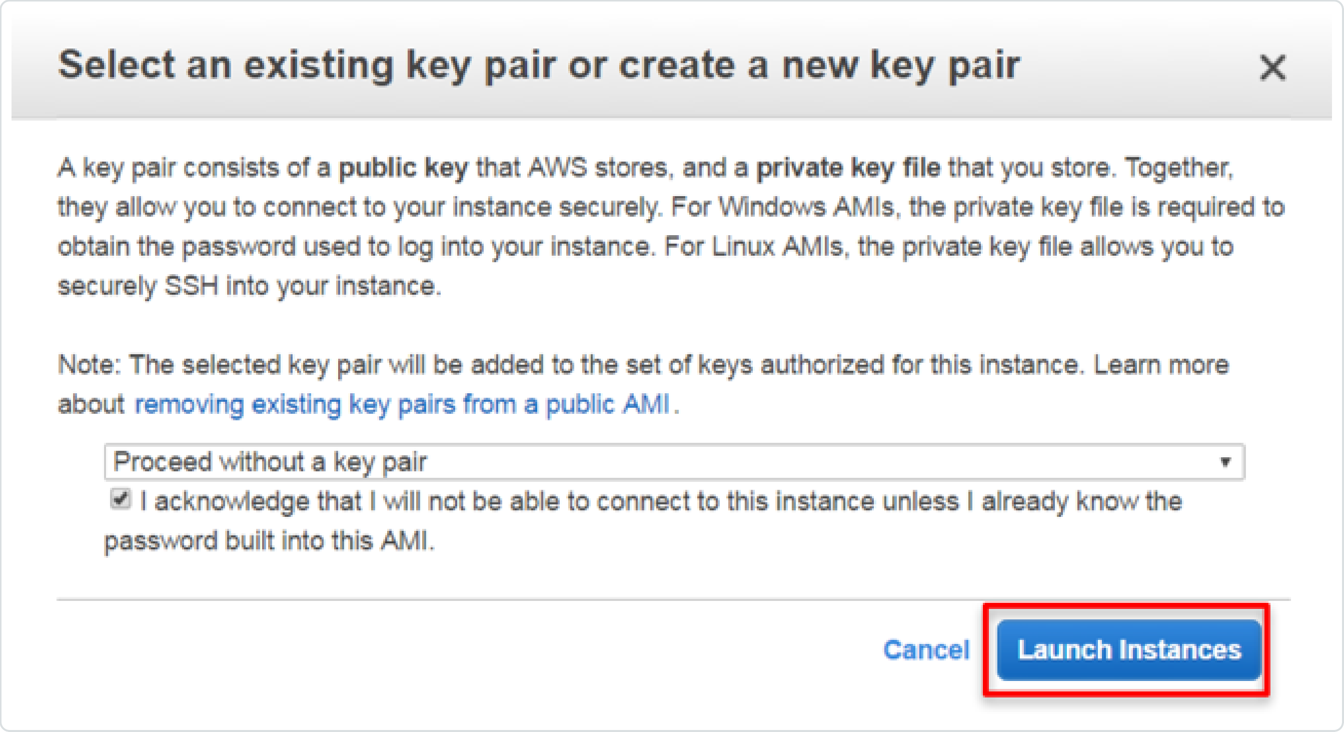
Security group name   Tenable.io Security Group
Description   Tenable.io Security Group

Type	Protocol	Port Range	Source

A key pair page appears.

37. In the **Select an existing key pair or create a new pair** dialog box, from the drop-down box, select **Proceed without a key pair**.

> **Tip:** No key pair is needed since the instance is not listening on any ports and there are no available connections to it.



Select an existing key pair or create a new key pair

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about removing existing key pairs from a public AMI.

Proceed without a key pair

☑ I acknowledge that I will not be able to connect to this instance unless I already know the password built into this AMI.

38. Check the **Acknowledge** check box.

39. Click **Launch Instances**. The new instance displays in your instance list. Once the newly created instance finishes initializing, the **Instance State** appears as **running**.

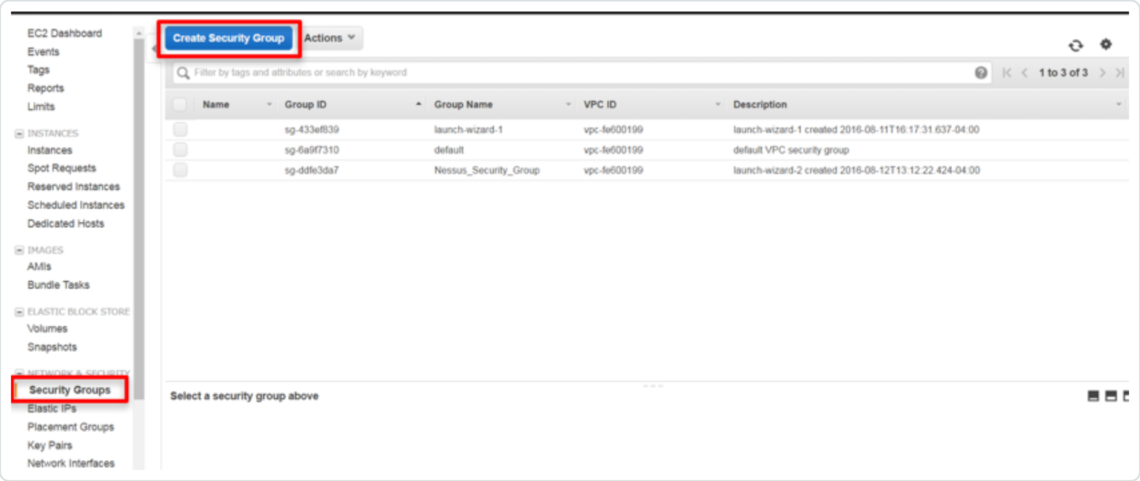
> **Note:** If any configuration information is incorrect, the scanner does not link. Stop the launch, edit the configuration information, and restart the launch.

Create Security Group to Permit Scanning

Caution: This version of the AWS pre-authorized scanner has been removed and is no longer available to new customers.

The following steps describe how to create a security group that allows all inbound access from the Nessus scanner. Any EC2 instance that this security group is applied to can be scanned by Nessus scanner.

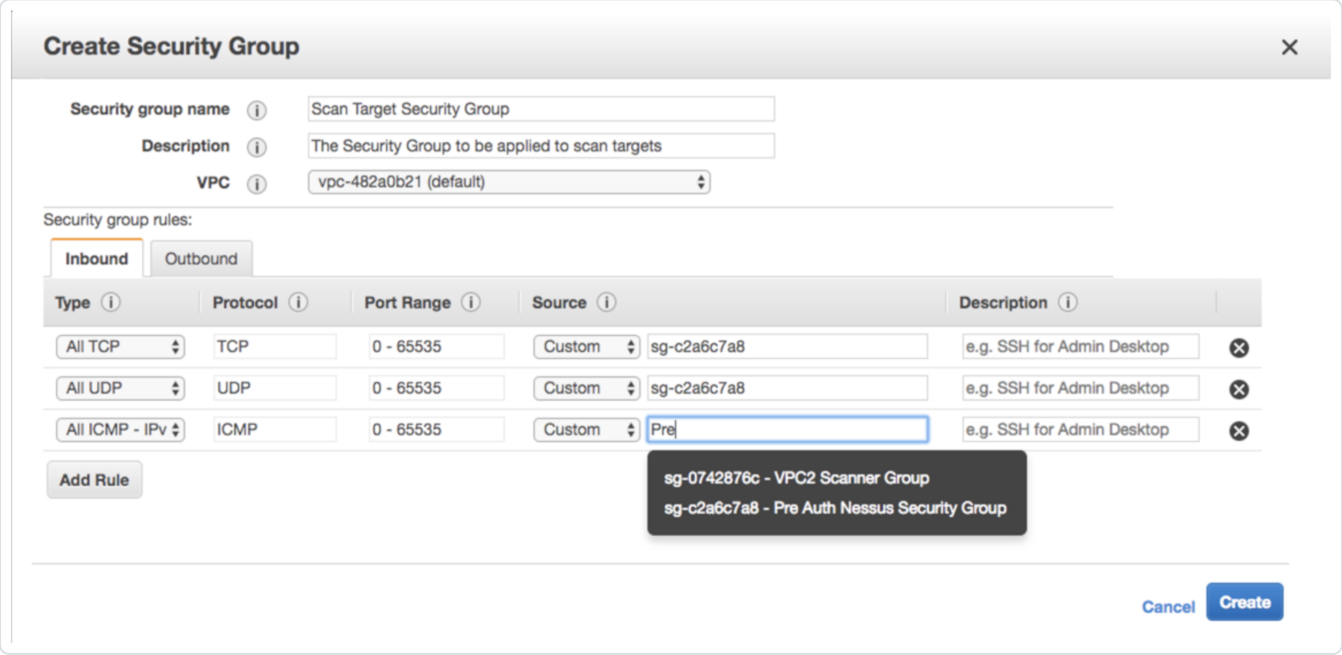
1. In the left-hand menu, click **Security Groups**.
2. Click **Create Security Group**.



Name	Group ID	Group Name	VPC ID	Description
	sg-433ef839	launch-wizard-1	vpc-fe600199	launch-wizard-1 created 2016-08-11T16:17:31.637-04:00
	sg-6a9f7310	default	vpc-fe600199	default VPC security group
	sg-ddfe3da7	Nessus_Security_Group	vpc-fe600199	launch-wizard-2 created 2016-08-12T13:12:22.424-04:00

Select a security group above

3. In the **Security group name** field, enter a name for the security group.



Create Security Group

Security group name	Scan Target Security Group
Description	The Security Group to be applied to scan targets
VPC	vpc-482a0b21 (default)

Security group rules:

Inbound | Outbound

Type	Protocol	Port Range	Source		Description
All TCP	TCP	0 - 65535	Custom	sg-c2a6c7a8	e.g. SSH for Admin Desktop
All UDP	UDP	0 - 65535	Custom	sg-c2a6c7a8	e.g. SSH for Admin Desktop
All ICMP - IPv	ICMP	0 - 65535	Custom	Pre	e.g. SSH for Admin Desktop

sg-0742876c - VPC2 Scanner Group

sg-c2a6c7a8 - Pre Auth Nessus Security Group

4. In the **Description** field, enter a description for the security group.

5. From the **VPC** drop-down box, select the appropriate network for the security group.

6. Click **Add Rule** to create an inbound security group.

7. From the **Type** drop-down box, select **All TCP**.

8. In the **CIDR, IP or Security Group** box, enter the name of the previously created security group.

9. Repeat steps 6-8 for **All UDP** and **All ICMP** types.

> **Tip:** The rules give the Nessus scanner's security group full access to the scan targets (any EC2 instances assigned to this security group).

10. Click **Create**.

> **Note:** If your organization requires whitelisting of outbound traffic for the Pre Authorized Scanner, you can specify the required API IP address ranges for Tenable and AWS in the **Security Group** section under **EC2**. Click the Pre-Authorized Security Group and edit the outbound rules. See the Tenable API IPs and AWS API IPs documentation for more information.

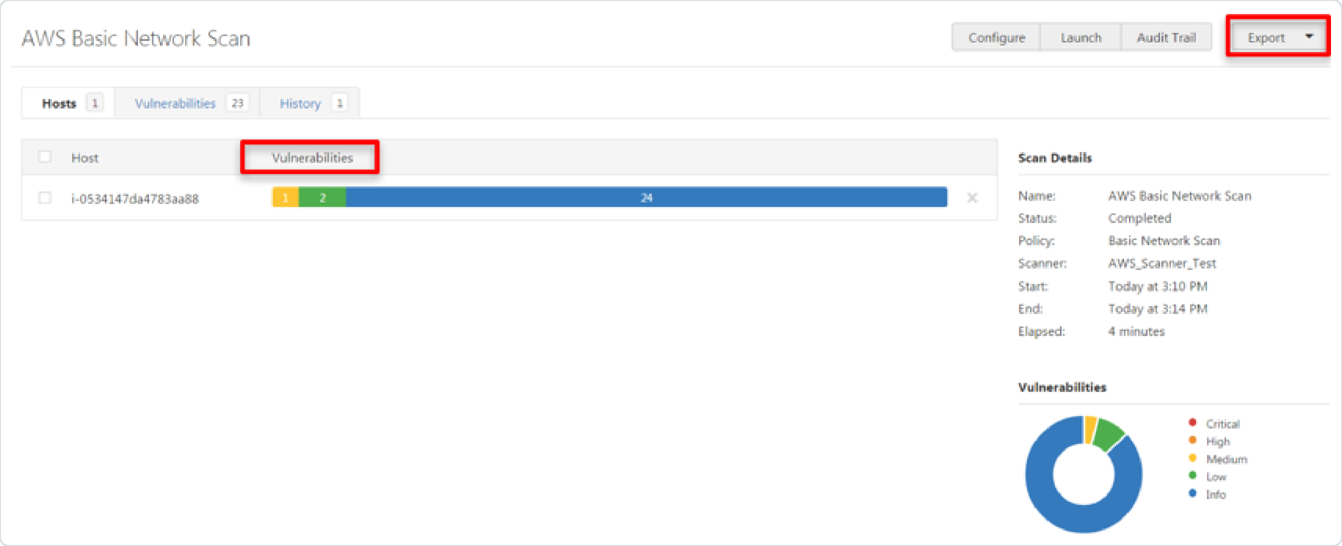
Create a Scan

Follow the Create a Scan steps in the Tenable Vulnerability Management User Guide.

View Scan Results in Tenable Vulnerability Management

Do one of the following:

- To view scan results, click on the completed scan.
- To view more details about the scan results, click the **Vulnerabilites** tab.



□	Host	Vulnerabilities
□	i-0534147da4783aa88	1 2 24

Scan Details

Name:	AWS Basic Network Scan
Status:	Completed
Policy:	Basic Network Scan
Scanner:	AWS_Scanner_Test
Start:	Today at 3:10 PM
End:	Today at 3:14 PM
Elapsed:	4 minutes

Vulnerabilities

- To export the results in Nessus, PDF, HTML, CSV or Nessus DB formats, click the **Export** button in the top right corner.

Audit the AWS Environment

You can use Tenable Vulnerability Management to audit the Amazon Web Services environment to detect misconfigurations in your cloud environment and account settings using Tenable Vulnerability Management. Complete the following steps to configure AWS for successful Audit Cloud Infrastructure assessments with Tenable Vulnerability Management.

> **Note:** Tenable recommends that you create a new read-only access AWS account just for Tenable Vulnerability Management. If you experience issues, see AWS Audit Troubleshooting.

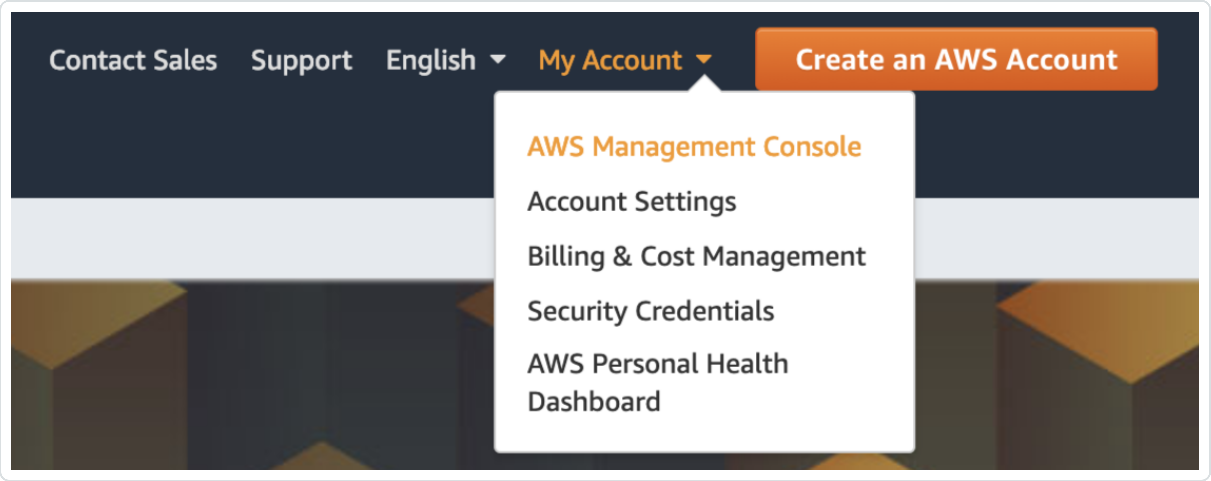
To audit the AWS environment, you must complete the following tasks:

- Create a Read-Only Group in AWS
- Create a Scanning User in AWS
- Configure AWS Audit Cloud Infrastructure in Tenable Vulnerability Management
- View Audit Details in the Scan Results

Create a Read-Only Group in AWS

To create a read-only group in AWS:

1. Log in to your AWS account.
2. Click **My Account** > **AWS Management Console**.

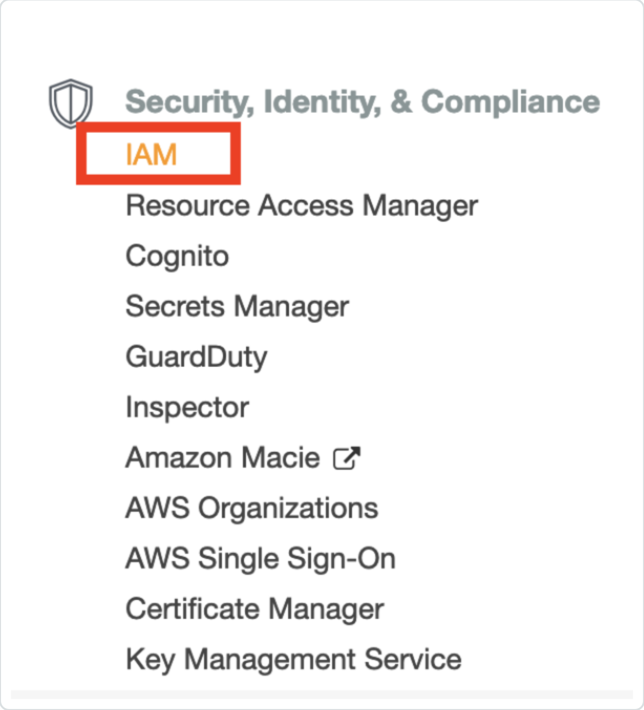
   

   The **AWS Management Console** appears.

3. Click **Services**.

   The **Services** page appears.

4. In the **Security, Identity, and Compliance** section, click **IAM**.



Security, Identity, & Compliance

IAM

Resource Access Manager

Cognito

Secrets Manager

GuardDuty

Inspector

Amazon Macie

AWS Organizations

AWS Single Sign-On

Certificate Manager

Key Management Service

The **IAM** control panel appears.

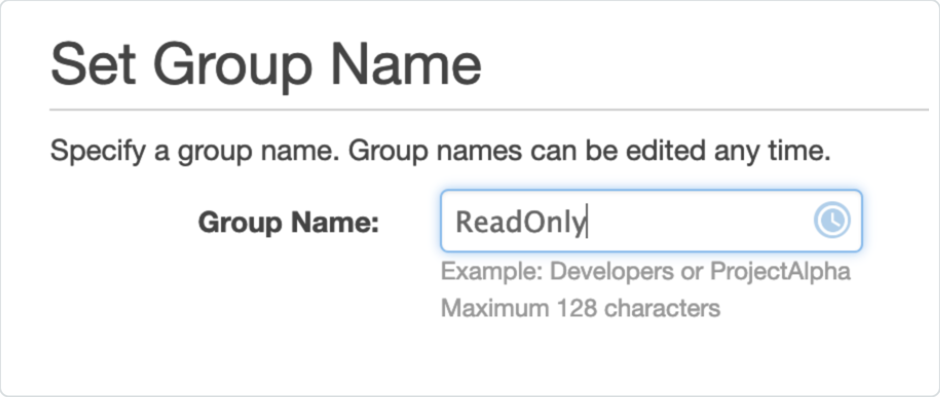
5. In the left panel, click **Groups**.

The **Groups** page appears.

6. Click **Create New Group**.

The **Create New Group Wizard** appears.

7. In the **Group Name** box, type a name for the read-only group.



Set Group Name

Specify a group name. Group names can be edited any time.

Group Name: ReadOnly

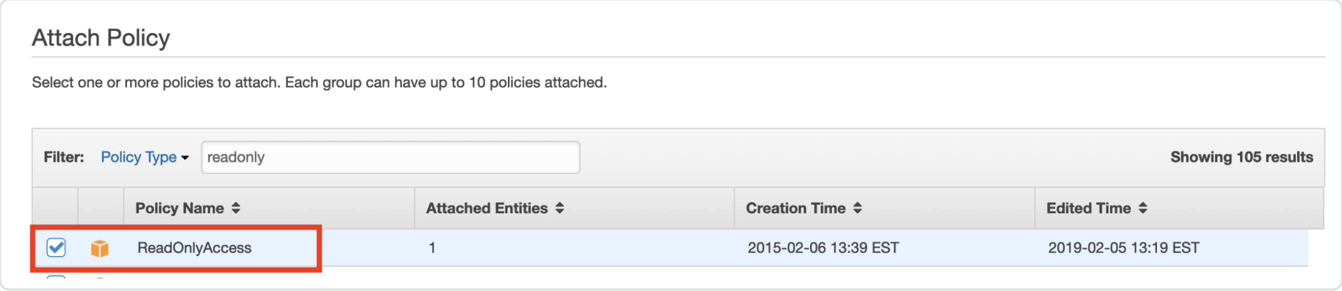
Example: Developers or ProjectAlpha

Maximum 128 characters

8. Click **Next Step**.

   The **Attach Policy** screen appears.

9. Select the **ReadOnlyAccess** AWS-managed policy.



Attach Policy

Select one or more policies to attach. Each group can have up to 10 policies attached.

Filter: Policy Type ▾ readonly　　Showing 105 results

		Policy Name ⬍	Attached Entities ⬍	Creation Time ⬍	Edited Time ⬍
☑		ReadOnlyAccess	1	2015-02-06 13:39 EST	2019-02-05 13:19 EST

10. (Optional) On the **Attach Policy** screen, select the **SecurityAudit** AWS-managed policy.

11. Click **Next Step**.

    The **Review** page appears.

12. Review the group information.

13. Click **Create Group**.

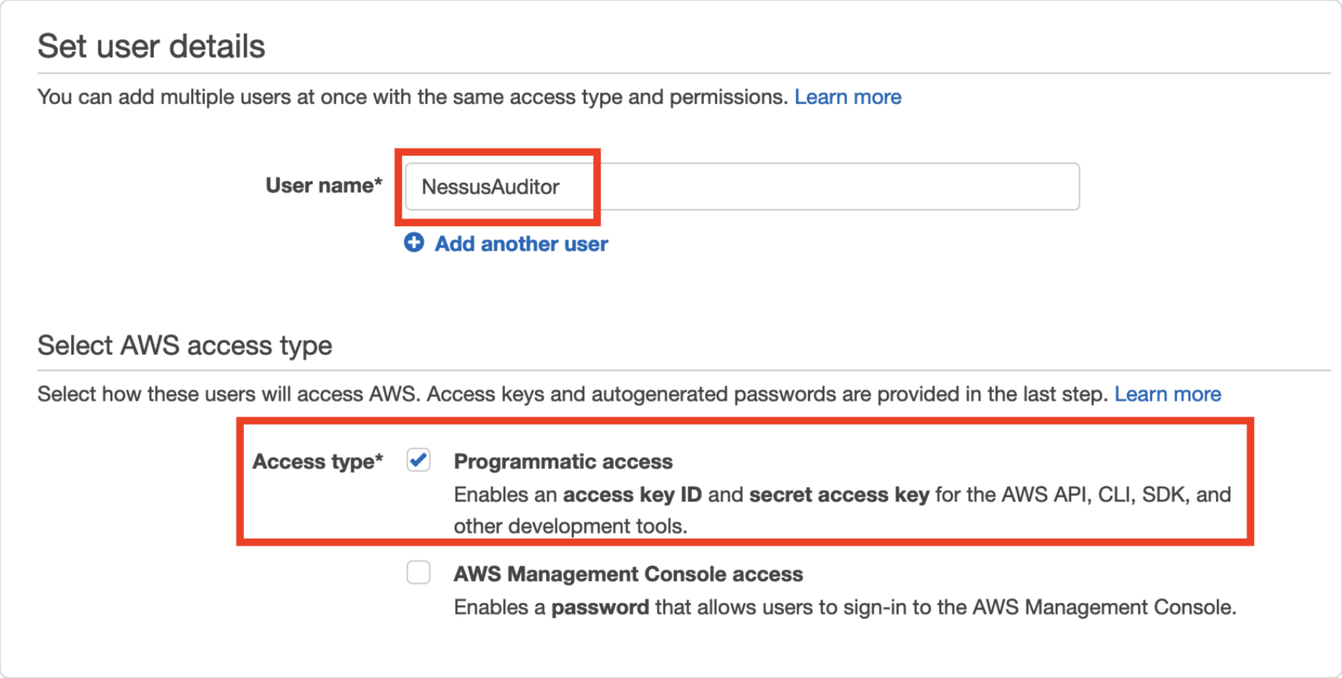
    AWS creates the read-only group.

Create a Scanning User in AWS

To create a scanning user in AWS:

1. Log in to your AWS account.
2. Click **Users** > **Add Users**.

   The **Add User** page appears.
3. In the **Set user details** section, in the **User name** text box, type a name for the user.
4. In the **Select AWS access type** section, select the **Programmatic access** check box.



Set user details

You can add multiple users at once with the same access type and permissions. Learn more

User name* NessusAuditor

Select AWS access type

Select how these users will access AWS. Access keys and autogenerated passwords are provided in the last step. Learn more

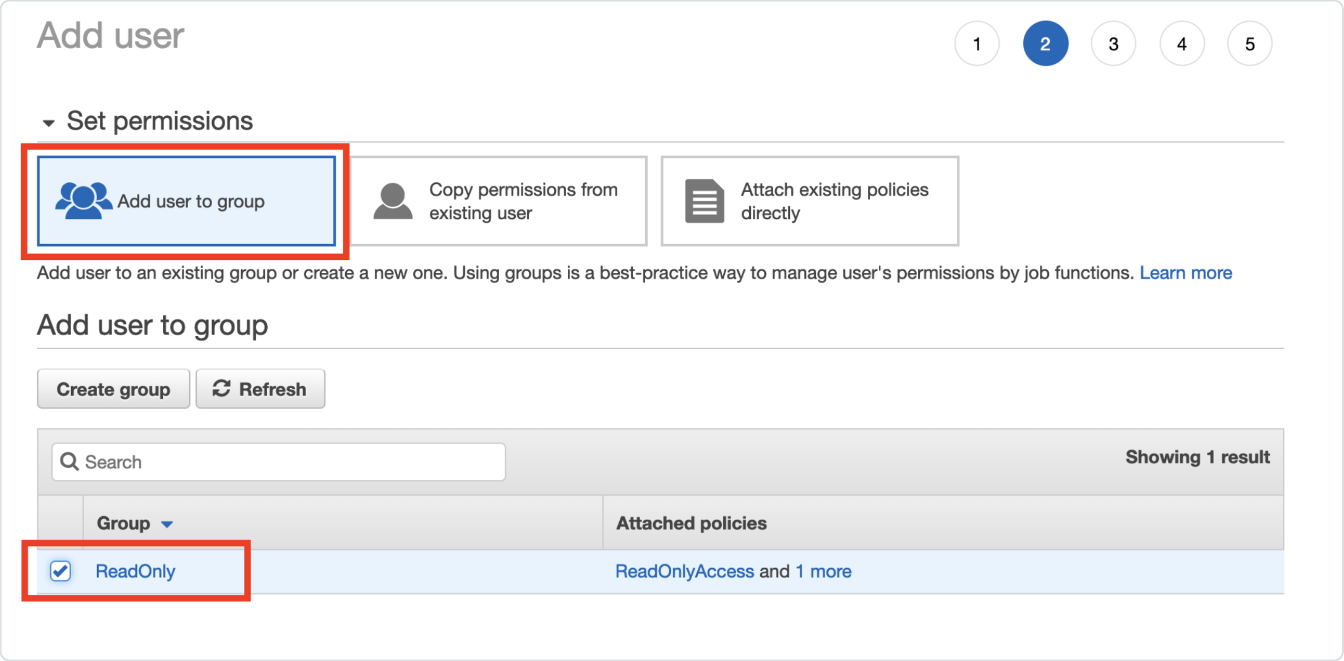
Access type* ☑ **Programmatic access**
Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.

□ **AWS Management Console access**
Enables a **password** that allows users to sign-in to the AWS Management Console.

5. Click **Next: Permissions**.

   The **Set permissions** page appears.
6. Click **Add user to group**.

7. In the **Add user to group** section, select the read-only group you previously created.



Add user

1 2 3 4 5

Set permissions

Add user to group | Copy permissions from existing user | Attach existing policies directly

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. Learn more

Add user to group

Create group | Refresh

Search

Showing 1 result

	Group	Attached policies
☑	ReadOnly	ReadOnlyAccess and 1 more

8. Click **Next: Tags**.

   The **Tags** page appears.

9. (Optional) Configure any tags you want to add to the user profile.

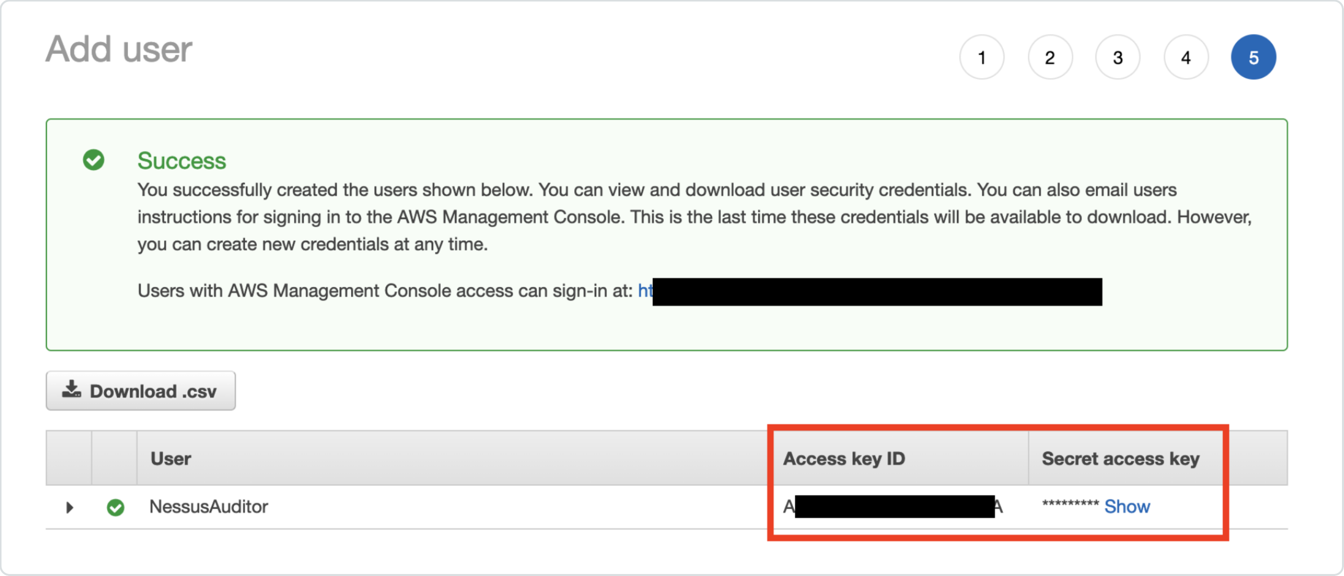
10. Click **Next: Review**.

    The **Review** page appears.

11. Review the user profile.

12. Click **Create User**.

    An **Access key ID** and **Secret access key** appear.



Success

You successfully created the users shown below. You can view and download user security credentials. You can also email users instructions for signing in to the AWS Management Console. This is the last time these credentials will be available to download. However, you can create new credentials at any time.

Users with AWS Management Console access can sign-in at: ht[redacted]

		User	Access key ID	Secret access key
▸	✓	NessusAuditor	A[redacted]A	********* Show

13. Copy the **Access key ID** and **Secret access key** to use to configure the Audit Cloud Infrastructure in Tenable Vulnerability Management.

Configure AWS Audit Cloud Infrastructure in Tenable Vulnerability Management

To configure AWS Audit Cloud Infrastructure in Tenable Vulnerability Management:

1. Log in to Tenable Vulnerability Management.

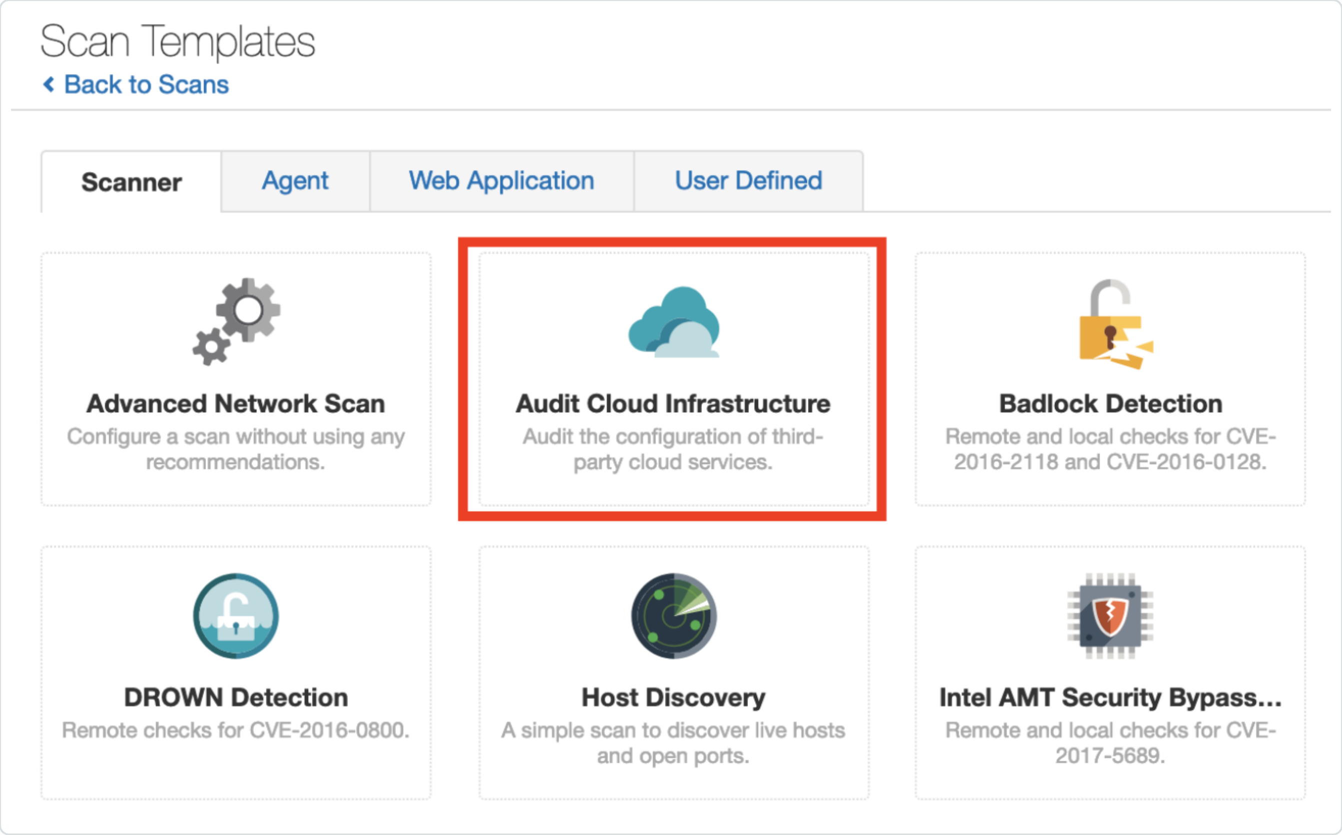
2. In the top navigation bar, click **Scans**.

   The **My Scans** page appears.

3. In the upper-right corner, click the **New Scan** button.

   The **Scan Templates** page appears.

4. Click **Audit Cloud Infrastructure**.

   
   Scan Templates
   ‹ Back to Scans
   Scanner
   Agent
   Web Application
   User Defined
   Advanced Network Scan
   Configure a scan without using any recommendations.
   Audit Cloud Infrastructure
   Audit the configuration of third-party cloud services.
   Badlock Detection
   Remote and local checks for CVE-2016-2118 and CVE-2016-0128.
   DROWN Detection
   Remote checks for CVE-2016-0800.
   Host Discovery
   A simple scan to discover live hosts and open ports.
   Intel AMT Security Bypass...
   Remote and local checks for CVE-2017-5689.

   The **New Scan** page appears.

5. On the **Settings** tab, type a name for the scan.

6. Set **Scanner Type** to **Tenable Cloud Sensor**.

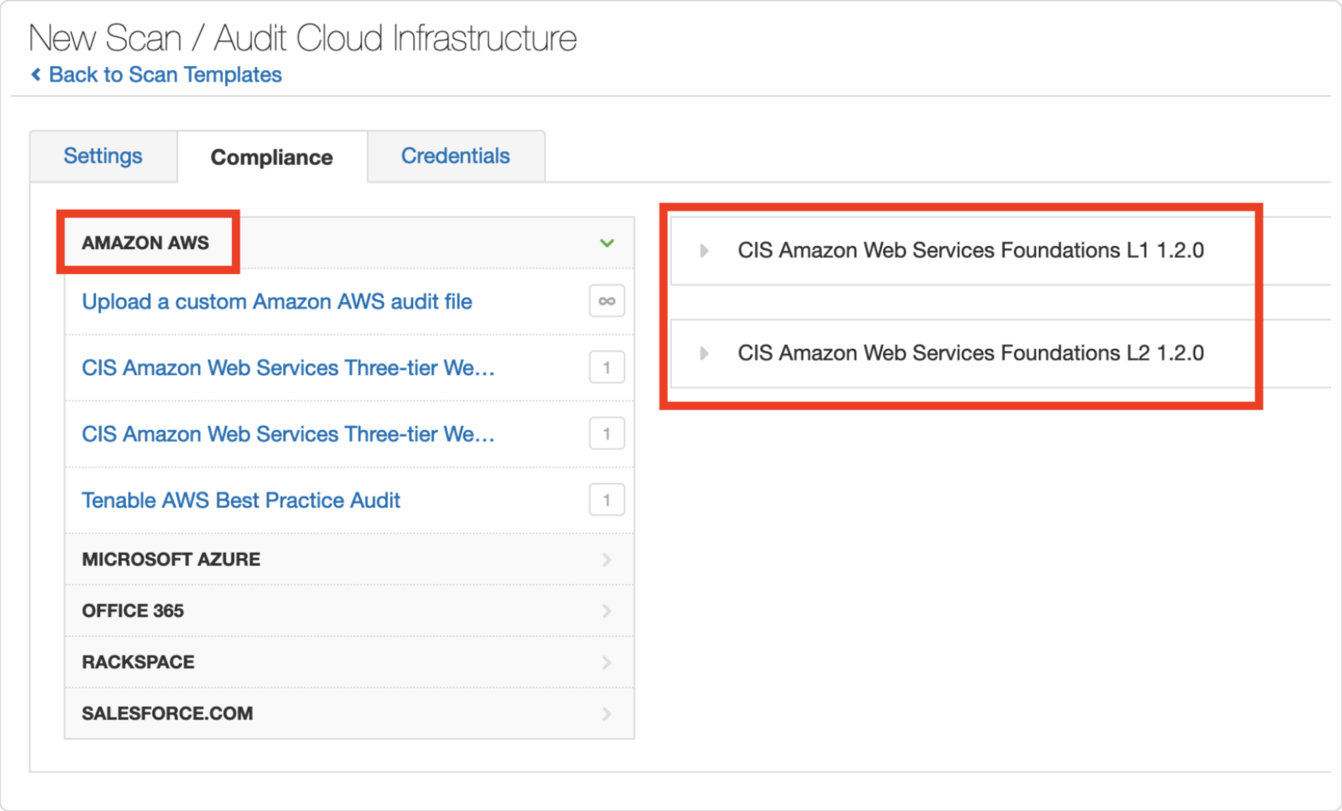
7. Click the **Compliance** tab.

   The **Compliance** options appear.

8. Click **AMAZON AWS**.

9. Select the appropriate audit files for the scan.

   When you select an audit file, Tenable Vulnerability Management adds the file to the list in the right pane.



New Scan / Audit Cloud Infrastructure

‹ Back to Scan Templates

Settings | **Compliance** | Credentials

AMAZON AWS

Upload a custom Amazon AWS audit file

CIS Amazon Web Services Three-tier We… 1

CIS Amazon Web Services Three-tier We… 1

Tenable AWS Best Practice Audit 1

MICROSOFT AZURE

OFFICE 365

RACKSPACE

SALESFORCE.COM

CIS Amazon Web Services Foundations L1 1.2.0

CIS Amazon Web Services Foundations L2 1.2.0

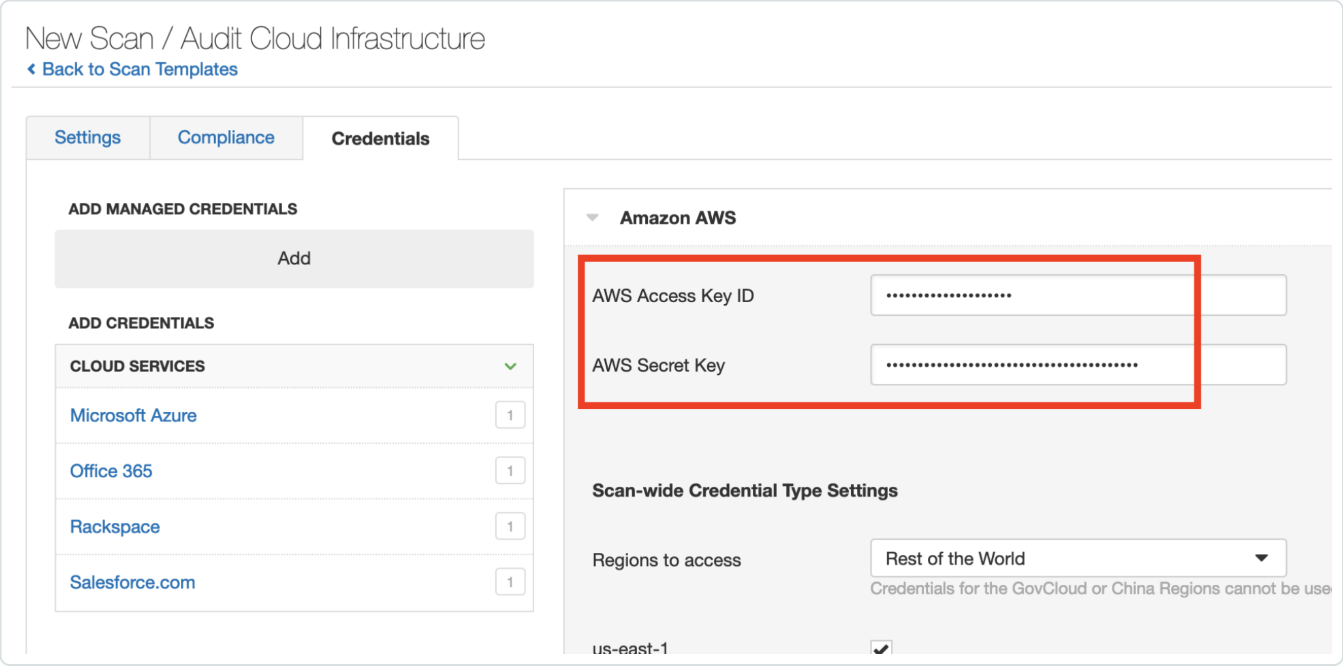
10. Click the **Credentials** tab.

    The **Credentials** options appear.

11. In the **ADD CREDENTIALS** section, select **Amazon AWS**.

12. In the **AWS Access Key ID** text box, type the key you copied in the Create a Scanning User in AWS section.

13. In the **AWS Secret Key** text box, type the key you copied in the Create a Scanning User in AWS section.



New Scan / Audit Cloud Infrastructure

‹ Back to Scan Templates

AWS Access Key ID: ••••••••••••••••••••

AWS Secret Key: ••

Scan-wide Credential Type Settings

Regions to access: Rest of the World

Credentials for the GovCloud or China Regions cannot be use

us-east-1 ☑

14. From the **Regions to Access** drop-down box, select the region to which you want to apply the scan.

15. Do one of the following:

    - To save without launching the scan click **Save**.

    - To save and launch the scan immediately, click the drop-down arrow next to **Save** and select **Launch**.

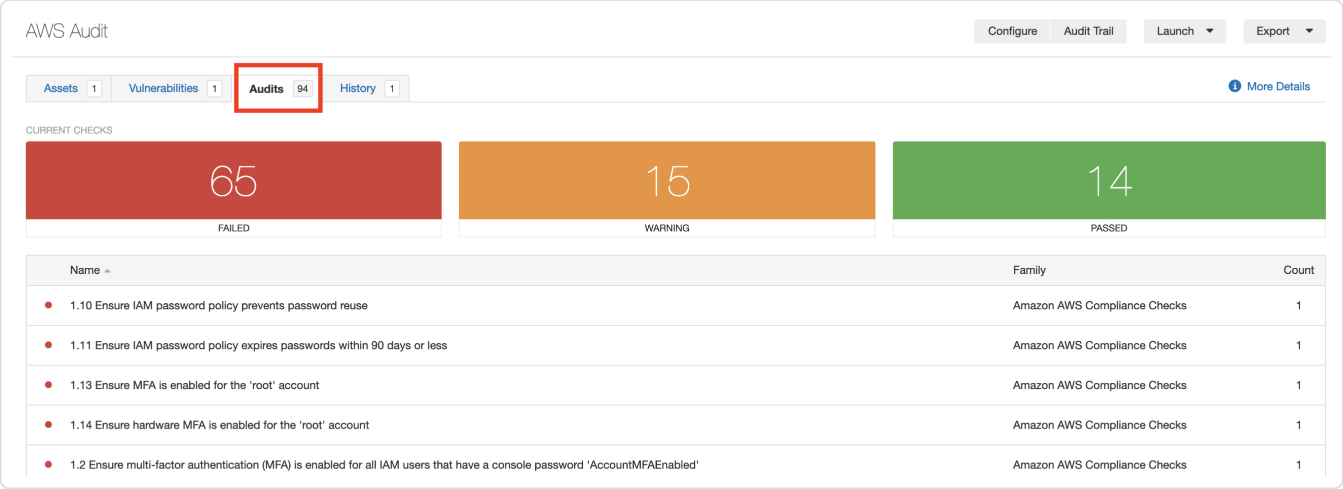
Tip: If you experience aborted scans or are unable to find a matching scanner route, you may need to specify a dedicated scanner, and re-scan. For troubleshooting help, see AWS Audit Troubleshooting. For more information on Tenable Vulnerability Management scans, refer to the Tenable Vulnerability Management User Guide.

View Audit Details in the Scan Results

After the scan completes, you can analyze the results in Tenable Vulnerability Management.

To view audit details in the scan results:

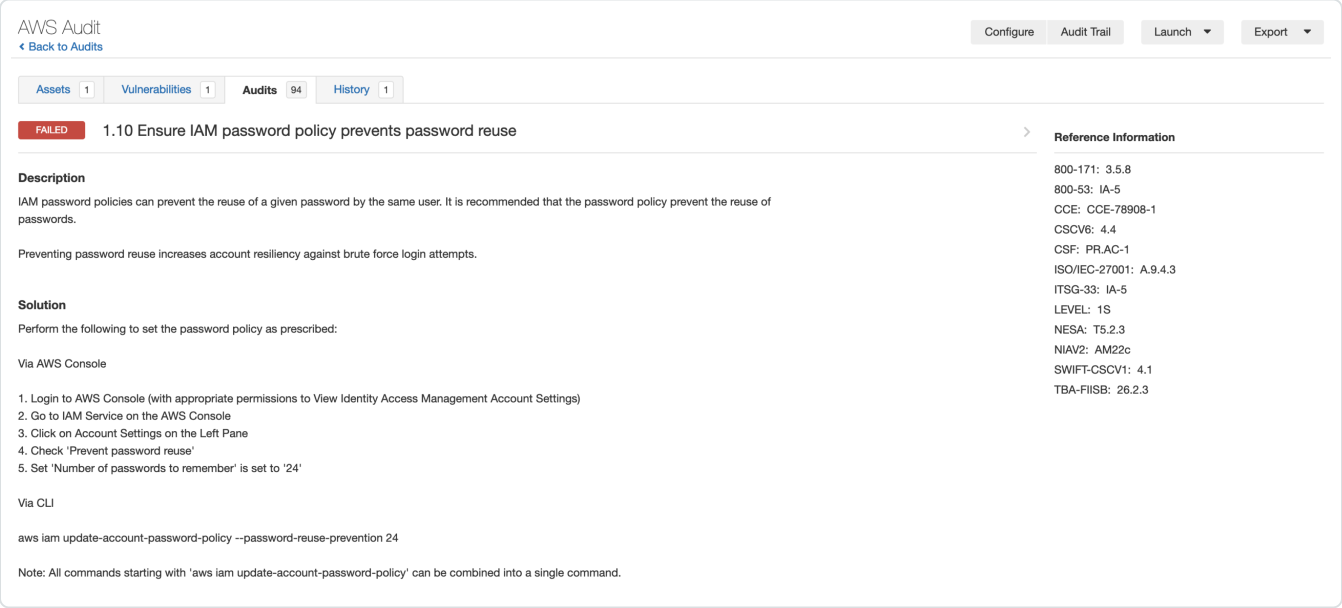
1. Log in to Tenable Vulnerability Management.
2. In the top navigation bar, click **Scans**.
3. Click the AWS Cloud Infrastructure scan you previously created.
4. Click the **Audits** tab.



	Name	Family	Count
●	1.10 Ensure IAM password policy prevents password reuse	Amazon AWS Compliance Checks	1
●	1.11 Ensure IAM password policy expires passwords within 90 days or less	Amazon AWS Compliance Checks	1
●	1.13 Ensure MFA is enabled for the 'root' account	Amazon AWS Compliance Checks	1
●	1.14 Ensure hardware MFA is enabled for the 'root' account	Amazon AWS Compliance Checks	1
●	1.2 Ensure multi-factor authentication (MFA) is enabled for all IAM users that have a console password 'AccountMFAEnabled'	Amazon AWS Compliance Checks	1

5. Click an audit in the table to view audit details, including the **Description**, **Reference Inform-**

ation, and **Solution**.



1.10 Ensure IAM password policy prevents password reuse

Description

IAM password policies can prevent the reuse of a given password by the same user. It is recommended that the password policy prevent the reuse of passwords.

Preventing password reuse increases account resiliency against brute force login attempts.

Solution

Perform the following to set the password policy as prescribed:

Via AWS Console

1. Login to AWS Console (with appropriate permissions to View Identity Access Management Account Settings)
2. Go to IAM Service on the AWS Console
3. Click on Account Settings on the Left Pane
4. Check 'Prevent password reuse'
5. Set 'Number of passwords to remember' is set to '24'

Via CLI

```
aws iam update-account-password-policy --password-reuse-prevention 24
```

Note: All commands starting with 'aws iam update-account-password-policy' can be combined into a single command.

Reference Information

800-171:	3.5.8
800-53:	IA-5
CCE:	CCE-78908-1
CSCV6:	4.4
CSF:	PR.AC-1
ISO/IEC-27001:	A.9.4.3
ITSG-33:	IA-5
LEVEL:	1S
NESA:	T5.2.3
NIAV2:	AM22c
SWIFT-CSCV1:	4.1
TBA-FIISB:	26.2.3

AWS Audit Troubleshooting

If you encounter issues while running the Audit Cloud Infrastructure scan, first, check the following:

- User configuration or permissions issues with the AWS account.
- AWS networking mechanisms that potentially block Tenable Vulnerability Management scan attempts.

If necessary, enable debug logging and contact Tenable Support (use the variable for Tenable Support) for troubleshooting assistance.

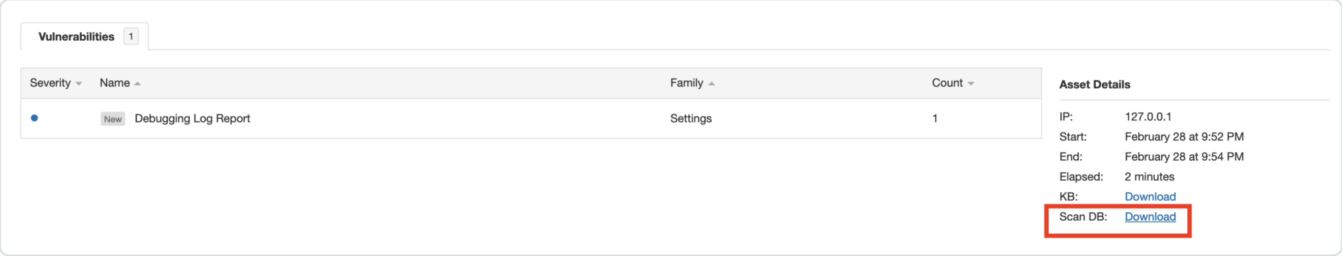
To enable debug logging for the Audit Cloud Infrastructure scan:

1. Navigate to the **Audit Cloud Infrastructure** scan you created in Audit the AWS Environment.
2. On the **Settings** tab, click **Advanced**.
3. In the **Debug Settings** section, select the **Enable plugin debugging** check box.
4. Do one of the following:
   - To save without launching the scan click **Save**.
   - To save and launch the scan immediately, click the drop-down arrow next to **Save** and select **Launch**.
5. In the top navigation bar, click **Scans**.
6. Click the row for the Audit Cloud Infrastructure scan you created.
7. Click the **Assets** tab.

   The **Assets** information appears.
8. Click the AWS Account asset.

   > **Note:** This asset always has a loopback address of 127.0.0.1.

9. In the **Asset Details** section, next to **Scan DB**, click **Download**.



Vulnerabilities 1

Severity	Name	Family	Count
●	New Debugging Log Report	Settings	1

Asset Details

IP: 127.0.0.1
Start: February 28 at 9:52 PM
End: February 28 at 9:54 PM
Elapsed: 2 minutes
KB: Download
Scan DB: Download

The **Export** window appears.

10. In the **Password** box, type the password you want to use to encrypt the **Scan DB** file.

11. Contact Tenable Support and provide the .db log file and the encryption password.

Security Hub

Through the use and configuration of the Tenable Vulnerability Management to AWS Security Hub Transformer, Tenable Vulnerability Management can send vulnerabilities to AWS Security Hub. This tool consumes Tenable Vulnerability Management asset and vulnerability data, transforms that data into the AWS Security Hub Finding format, and then uploads the resulting data into AWS Security Hub.

Note: The script does not need to be run in AWS.

The tool can be run either as a one-shot docker container or as a command-line tool:

- To run as a docker image, you must build the image and then pass the necessary secrets on to the container.
- To run as a command-line tool, you must install the required python modules and then run the tool using either environment variables or by passing the required parameters as run-time parameters.

Requirements

- Tenable Vulnerability Management account
- Tenable Vulnerability Management AWS connector enabled and configured
- AWS Security Hub
- Tenable Vulnerability Management Provider enabled and configured in Security Hub

Installation

To build the Docker image, run the following script:

```
docker build -t tio2sechub:latest .
```

To install python requirements, run the following script:

```
pip install -r requirements.txt
```

Enable Script in Security Hub

To enable the script in Security Hub:

1. Log in to Security Hub.
2. If you have not yet enabled Security Hub, click **Enable Security Hub**.
3. Navigate to **Settings** > **Providers.**
4. In the **Search** box, type *Tenable*.
5. Click **Configure**.

   Your account subscribes to accept events from the script.

Configuration

The following lists the command-line arguments as well as the equivalent environment variables:

```
usage: sechubingest.py [-h] [--tio-access-key TIO_ACCESS_KEY]
                                            [--tio-secret-key TIO_SECRET_KEY]
                                            [--batch-size BATCH_SIZE] [--aws-region
AWS_REGION]
                                            [--aws-account-id AWS_ACCOUNT_ID]
                                            [--aws-access-id AWS_ACCESS_ID]
                                            [--aws-secret-key AWS_SECRET_KEY]
                                            [--log-level LOG_LEVEL] [--since OBSERVED_
SINCE]
                                            [--run-every RUN_EVERY]

optional arguments:
-h, --help            show this help message and exit
--tio-access-key TIO_ACCESS_KEY
                                            Tenable.io Access Key
--tio-secret-key TIO_SECRET_KEY
                                            Tenable.io Secret Key
--batch-size BATCH_SIZE
                                            Size of the batches to populate into
Security Hub
--aws-region AWS_REGION
                                            AWS region for Security Hub
--aws-account-id AWS_ACCOUNT_ID
                                            AWS Account ID
--aws-access-id AWS_ACCESS_ID
                                            AWS Access ID
--aws-secret-key AWS_SECRET_KEY
                                            AWS Secret Key
--log-level LOG_LEVEL
                                            Log level: available levels are debug,
info, warn,
                                            error, crit
--since OBSERVED_SINCE
                                            The unix timestamp of the age threshold
--run-every RUN_EVERY
                                            How many hours between recurring imports
```

To run the import once, run the following script:

```
./sechubingest.py                   \
--tio-access-key {TIO_ACCESS_KEY}   \
--tio-secret-key {TIO_SECRET_KEY}   \
--aws-region us-east-1              \
--aws-account-id {AWS_ACCOUNT_ID}   \
--aws-access-id {AWS_ACCESS_ID}     \
--aws-secret-key {AWS_SECRET_KEY}   \
```

To run the import once an hour, run the following script:

```
./sechubingest.py                   \
--tio-access-key {TIO_ACCESS_KEY}   \
--tio-secret-key {TIO_SECRET_KEY}   \
--aws-region us-east-1              \
--aws-account-id {AWS_ACCOUNT_ID}   \
--aws-access-id {AWS_ACCESS_ID}     \
--aws-secret-key {AWS_SECRET_KEY}   \
--run-every 1
```

To run the same import using environment vars, run the following script:

```
export TIO_ACCESS_KEY="{TIO_ACCESS_KEY}"
export TIO_SECRET_KEY="{TIO_SECRET_KEY}"
export AWS_REGION="us-east-1"
export AWS_ACCOUNT_ID="{AWS_ACCOUNT_ID}"
export AWS_ACCESS_ID="{AWS_ACCESS_ID}"
export AWS_SECRET_KEY="{AWS_SECRET_KEY}"
export RUN_EVERY=1
./sechubingest.py
```