**Table of Contents**

**Welcome to AWS for Tenable Vulnerability Management** ........................................ 4

**Integration Requirements** ......................................................................................... 5

**Integration Configuration** ......................................................................................... 6

Tenable Nessus BYOL Scanner .......................................................................................... 7

  Activate the Nessus BYOL Scanner ........................................................................ 12

  Activate Tenable Nessus BYOL Scanner via the Command Line ............................. 13

Obtain Tenable Vulnerability Management Linking Key ........................................... 14

Activate Tenable Nessus BYOL Scanner Linked to Tenable Vulnerability Management ........................................ 16

  Link Tenable Nessus BYOL Scanner to Tenable Vulnerability Management via the Command Line ........................................................................................................ 19

Link a BYOL Scanner to Tenable Vulnerability Management with Pre-Authorized Scanner Features .......................................................... 20

Optional Configuration ................................................................................................. 21

AWS Multi-Account Multi-VPC Scanning ..................................................................... 22

Pre-Authorized Scanner ............................................................................................... 26

Obtain Tenable Vulnerability Management Linking Key ........................................... 27

Create an AWS IAM Role .............................................................................................. 28

Launch Pre-Authorized Nessus Scanner ..................................................................... 34

Create Security Group to Permit Scanning ................................................................. 45

Create a Scan .................................................................................................................. 47

  View Scan Results in Tenable Vulnerability Management ...................................... 48

Audit the AWS Environment ......................................................................................... 49

Create a Read-Only Group in AWS ............................................................................. 50
Create a Scanning User in AWS .......................................................... 53
Configure AWS Audit Cloud Infrastructure in Tenable Vulnerability Management ............ 56
View Audit Details in the Scan Results ........................................................................ 58
AWS Audit Troubleshooting ....................................................................................... 60

Security Hub ................................................................................................. 62
Requirements ............................................................................................ 63
Installation .................................................................................................. 64
Enable Script in Security Hub .......................................................................... 65
Configuration ............................................................................................... 66
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**
  

- **AWS account**
  
  To create a free account, visit [https://aws.amazon.com/start-now](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 the Nessus 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**.

![EC2 Dashboard](image)

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**.

![Nessus (BYOL) selection](image)

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](image)

    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*
    - **Download Key Pair**

    **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.**

    **Cancel** 
    **Launch Instances**

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 checkbox.
• 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 are 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 the Nessus BYOL Scanner

Before you begin:

- View the login and instance-type information in the [Nessus BYOL Scanner](#) documentation.

To activate the Tenable Nessus BYOL Scanner (Tenable Nessus Expert or Tenable Nessus Professional):

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 Expert or Tenable Nessus Professional instance.

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

2. Select Tenable Nessus Expert or Tenable Nessus Professional.

3. Click **Continue**.

   The **Register Tenable Nessus** page appears.

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

5. Click **Continue**.

   Activation begins and plugins download. 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](https://cloud.tenable.com).
2. In the top menu bar, click **Scans**.
3. In the left-hand menu, click **Scanners**.

The Scanners page appears.

4. Click the **Linked Scanners** tab.
5. Copy and save the **Linking Key**.
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 user interface on Port 8834, for example, https://<NessusBYOL-IP>:8834.

   The Welcome to Tenable Nessus page appears.

2. Select Managed Scanner.

3. Click Continue.

   The Managed Scanner page appears.
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**.

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=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 does 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:

Copy the following bootstrap script:

```bash
#!/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-premises 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 does not propagate the route of the new Amazon VPC into the AWS Transit Gateway route table. See the AWS documentation for more information.

You can only scan by IPs, DNS, or dynamic tags. You cannot 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.
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:
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.
6. Create a scan, and select the tag you created in Step 5 in the Basic settings.

7. Launch the scan.

   The scan displays 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 instances as seen in the Launch Nessus Scanner Instance section. 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 VPCs 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 returns 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 into [https://cloud.tenable.com](https://cloud.tenable.com).

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

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

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

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

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


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]

- 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**.
5. Click **Create Role**.

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

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

9. Click **Next: Permissions**.

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

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

The newly created IAM role appears in the role list.
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. For more information, see the AWS Documentation.

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

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

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

6. On your keyboard, press **Enter**.
7. Select **Nessus Scanner (Pre-Authorized)**.

![Image of Nessus Scanner selection](image)

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.
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** checkbox 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** checkbox.

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

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** checkbox.

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**.

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:

```json
{
    "name": "AWS_Scanner",
    "key": "d92a78e1177f9ead79176b34c5de936ce00f0a7fE.......",
    "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.

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

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](image)

**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** checkbox.

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.
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.

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.

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.
38. Check the **Acknowledgement** checkbox.

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 Tenable Nessus scanner. The Tenable Nessus scanner can scan any EC2 instance that this security group is applied to.

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

![Security Groups screenshot](image-url)
3. In the **Security group name** field, enter a name for the security group.

![Create Security Group](image)

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 Tenable 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 allowlisting 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 **Vulnerabilities** tab.

- 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**.

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.
8. Click **Next Step**.

   The **Attach Policy** screen appears.

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

![Attach Policy screen]

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** checkbox.

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.

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.
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 upper-left corner, click the button.
   The left navigation plane appears.
3. In the left navigation plane, in the Vulnerability Management section, click Scans.
   The Scans page appears.
4. In the upper-right corner of the page, click Create a Scan.
   The Select a Scan Template page appears.
5. Click Audit Cloud Infrastructure.
   The New Scan page appears.
6. On the Settings tab, type a name for the scan.
7. Set Scanner Type to Tenable Cloud Sensor.
8. Click the Compliance tab.
   The Compliance options appear.
9. Click AMAZON AWS.
10. Select the appropriate audit files for the scan.
    When you select an audit file, Tenable Vulnerability Management adds the file to the list.
11. Click the Credentials tab.
    The Credentials options appear.
12. In the ADD CREDENTIALS section, select Amazon AWS.
13. In the AWS Access Key ID text box, type the key you copied in the Create a Scanning User in AWS section.
14. In the **AWS Secret Key** text box, type the key you copied in the Create a Scanning User in **AWS** section.

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

16. 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.

5. Click an audit in the table to view audit details, including the **Description**, **Reference**
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
```
a2s iam update-account-password-policy --password-reuse-prevention 24
```

Note: All commands starting with 'a2s iam update-account-password-policy' can be combined into a single command.
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 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 checkbox.
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**.

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:

```bash
./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:

```bash
./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:

```bash
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
```