Tenable.io and Amazon Web Services Integration Guide

Last Revised: March 15, 2022
# Table of Contents

Welcome to AWS for Tenable.io ......................................................... 4  
Integration Requirements ................................................................. 5 
Integration Configuration ................................................................. 6  
Amazon Web Services Connector ....................................................... 7  
Pre-Authorized Scanner ....................................................................... 8  
Obtain Tenable.io Linking Key .............................................................. 9  
Create an AWS IAM Role ................................................................. 11  
Launch Pre-Authorized Nessus Scanner ............................................... 16  
Create Security Group to Permit Scanning ........................................... 27  
Nessus BYOL Scanner ........................................................................... 29  
Activate Nessus Professional BYOL Scanner ....................................... 34  
Activate Nessus BYOL Scanner via the Command Line .......................... 36  
Obtain Tenable.io Linking Key .............................................................. 37  
Activate Nessus BYOL Scanner Linked to Tenable.io ............................. 39  
Link Nessus BYOL Scanner to Tenable.io via the Command Line .......... 42  
Optional Configuration ........................................................................ 43  
AWS Multi-Account Multi-VPC Scanning ............................................ 44  
Create a Scan ...................................................................................... 48  
View Scan Results in Tenable.io .......................................................... 49  
Audit the AWS Environment .............................................................. 50  
Create a Read-Only Group in AWS ..................................................... 51  
Create a Scanning User in AWS ......................................................... 54
Configure AWS Audit Cloud Infrastructure in Tenable.io .......................................................... 57
View Audit Details in the Scan Results ......................................................................................... 60
AWS Audit Troubleshooting ............................................................................................................ 62
Security Hub .................................................................................................................................... 64
Requirements .................................................................................................................................. 65
Installation ......................................................................................................................................... 66
Enable Script in Security Hub .......................................................................................................... 67
Configuration ..................................................................................................................................... 68
Welcome to AWS for Tenable.io

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

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

A pre-authorized Nessus scanner is available in the Amazon Marketplace. The Nessus scanner links to and is managed by Tenable.io, 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 Nessus scanner to secure their AWS environments and instances must have active Tenable.io and Amazon Web Services accounts.
Integration Requirements

The following are required in order to integrate Tenable.io with AWS:

- **Tenable.io account**
  
  To purchase a Tenable.io account or set up a free evaluation, visit [http://www.tenable.com/products/tenable-io](http://www.tenable.com/products/tenable-io)

- **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.io, see the following integration configuration topics:

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

The Amazon Web Services (AWS) Connector provides real-time visibility and inventory of EC2 assets in AWS accounts. To import and analyze information about assets in Amazon Web Services, you must configure AWS to support connectors and/or Frictionless Assessment, and then create an AWS connector in Tenable.io.

With Frictionless Assessment, Tenable.io collects an inventory of data points on your AWS EC2 instances, then assesses the hosts for vulnerabilities in the cloud, rather than running plugins locally on the host. Frictionless Assessment is available when you configure an AWS connector with keyless authentication.

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

To configure an AWS connector without Frictionless Assessment, see AWS Cloud Connector (without Frictionless Assessment) in the Tenable.io User Guide,

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

**Tip:** For common connector errors, see Connectors in the Tenable Developer Portal.
Pre-Authorized Scanner

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

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 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 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.io Linking Key

1. Once you have created a Tenable.io 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.

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:** d92a78e1177f9ead79178b34c5de936ce0f

---

Copyright © 2022 Tenable, Inc. All rights reserved. Tenable, Tenable.io, Tenable Network Security, Nessus, SecurityCenter, SecurityCenter Continuous View and Log Correlation Engine are registered trademarks of Tenable, Inc. Tenable.sc, Tenable.ot, Lumin, Indegy, Assure, and The Cyber Exposure Company are trademarks of Tenable, Inc. All other products or services are trademarks of their respective owners.
Create an AWS IAM Role


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**.
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.

   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.

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

**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).
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)**.

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: Configure Instance Details**.

    The **Step 3: Configure Instance Details** 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** 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 accidentally being terminated, 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 the **EBS-optimized instance** check box is selected.

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.io, and the previously created IAM role in JSON format:

```json
{
    "name": "AWS_Scanner",
    "key":"d92a78e1177ff9ead79176b34c5de936ce00f0a7f......",
    "iam_role": "TenableIO",
    "proxy": "10.11.12.13",
}
```
"proxy_port": "8080"
}

**Note:** The **Linking Key** and IAM role are both required entries in the **User Data** field. Other acceptable entries include:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Name of the scanner shown in the Nessus UI (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 scanner with Tenable.io. 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**

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

<table>
<thead>
<tr>
<th>Volume Type</th>
<th>Device</th>
<th>Snapshot</th>
<th>Size (GiB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Root</td>
<td>/dev/xvd0</td>
<td>snap-001</td>
<td>30</td>
</tr>
</tbody>
</table>

**Add New Volume**
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**.

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

**Note:** There is no way to directly access the AMI, 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**.

![Launch screen](image)

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 **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

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**.

3. In the **Security group name** field, enter a name for the 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.
Nessus BYOL Scanner

The following instructions describe how to configure a 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.

Before you begin:

- Ensure that your system meets the [hardware requirements](#) described in the *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**.

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 Nessus User Guide.
```

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.

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 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

To activate the Nessus Professional BYOL Scanner:

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

   The Welcome to Nessus page appears.

2. Select Nessus Professional.

![Welcome to Nessus page](image)

3. Click Continue.

   The Register Nessus page appears.
4. In the **Activation Code** box, type your Nessus Professional activation code.

5. Click **Continue**.

   Nessus Professional activates and plugins begin downloading. For more information, see the **Nessus User Guide**.
Activate Nessus BYOL Scanner via the Command Line

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

1. Adjust the permissions for your downloaded SSH Key using the following command:
   
   ```bash
   chmod 400 myNessusKey.pem
   ```

2. SSH into the Nessus BYOL scanner using the following command:
   
   ```bash
   ssh -i myNessusKey.pem ec2-user@<BYOLpublicIP>
   ```
   
   Where `<BYOLpublicIP>` is the IP address of your Nessus Professional instance.

3. Elevate privileges using the following command:
   
   ```bash
   sudo su
   ```

4. Update the AMI using the following command:
   
   ```bash
   yum update -y
   ```

5. Stop Nessus using the following command:
   
   ```bash
   service nessusd stop
   ```

6. Register the scanner with your Nessus Professional activation code using the following command:
   
   ```bash
   /opt/nessus/sbin/nessuscli fetch --register <ACTIVATION_CODE>
   ```
   
   Where `<ACTIVATION_CODE>` is the activation code for your instance.

7. Start Nessus using the following command:
   
   ```bash
   service nessusd start
   ```
Obtain Tenable.io Linking Key

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

To obtain the Tenable.io 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 Nessus BYOL Scanner Linked to Tenable.io

To activate the Nessus BYOL Scanner linked to and managed by Tenable.io:

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

   The Welcome to 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.io.

5. In the Linking Key box, paste the linking key copied in the Obtain Tenable.io Linking Key section.

6. Click Continue.

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

To confirm the Nessus BYOL Scanner in Tenable.io:

1. Log in to Tenable.io.

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 Nessus BYOL Scanner to Tenable.io via the Command Line

To link the Nessus BYOL scanner to Tenable.io via the command line:

1. Adjust the permissions for your downloaded SSH Key using the following command:
   
   ```bash
   chmod 400 myNessusKey.pem
   ```

2. SSH into the Nessus BYOL scanner using the following command:
   
   ```bash
   ssh -i myNessusKey.pem ec2-user@<BYOLpublicIP>
   ```
   Where `<BYOLpublicIP>` is the IP address of your Nessus BYOL instance.

3. Elevate privileges using the following command:
   
   ```bash
   sudo su
   ```

4. Update the AMI using the following command:
   
   ```bash
   yum update -y
   ```

5. Stop Nessus using the following command:
   
   ```bash
   service nessusd stop
   ```

6. Link the Nessus BYOL scanner to Tenable.io for management using the following command:
   
   ```bash
   /opt/nessus/sbin/nessuscli managed link --key=<key> --cloud
   ```
   Where `<key>` is the linking key associated with your Tenable.io instance.

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

7. Start Nessus using the following command:
   
   ```bash
   service nessusd start
   ```
Optional Configuration

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

Step 3: Configure Instance Details

<table>
<thead>
<tr>
<th>IAM role</th>
<th>None</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shutdown behavior</td>
<td>Stop</td>
</tr>
<tr>
<td>Enable termination protection</td>
<td>Protect against accidental termination</td>
</tr>
<tr>
<td>Monitoring</td>
<td>Enable CloudWatch detailed monitoring</td>
</tr>
<tr>
<td>Tenancy</td>
<td>Shared - Run a shared hardware instance</td>
</tr>
<tr>
<td>Elastic Inference</td>
<td>Add an Elastic Inference accelerator</td>
</tr>
<tr>
<td>T2/T3 Unlimited</td>
<td>Enable</td>
</tr>
</tbody>
</table>

Advanced Details

User data

```
#!/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 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 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.io.

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

1. In Tenable.io, [Deploy the BYOL scanner](https://tenable.io) in one of your VPCs.
   
   You can use the Tenable.io 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 Nessus BYOL scanner to Tenable.io in one of two ways:
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.io, 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 will display results from across all the scanned VPCs.
Create a Scan

Follow the Create a Scan steps in the Tenable.io User Guide.
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.io to audit the Amazon Web Services environment to detect misconfigurations in your cloud environment and account settings using Tenable.io. Complete the following steps to configure AWS for successful Audit Cloud Infrastructure assessments with Tenable.io.

**Note:** Tenable recommends that you create a new read-only access AWS account just for Tenable.io. 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.io](#)
- [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.

![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.

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](image)
   
   **Set user details**
   
   You can add multiple users at once with the same access type and permissions. Learn more
   
   **User name**
   
   ![User name field](image)
   
   ![Add another user](image)
   
   **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](image)
   
   **Access type**
   
   ![Programmatic access](image)
   
   ![AWS Management Console access](image)

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 to group](image)

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.io.
Configure AWS Audit Cloud Infrastructure in Tenable.io

To configure AWS Audit Cloud Infrastructure in Tenable.io:

1. Log in to Tenable.io.
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**.
   The **New Scan** page appears.
5. On the **Settings** tab, type a name for the scan.
6. Click the **Compliance** tab.

   The **Compliance** options appear.

7. Click **AMAZON AWS**.

8. Select the appropriate audit files for the scan.

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

9. Click the **Credentials** tab.

   The **Credentials** options appear.

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

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

12. In the **AWS Secret Key** text box, type the key you copied in the Create a Scanning User in **AWS** section.
13. From the **Regions to Access** drop-down box, select the region to which you want to apply the scan.

14. 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.io scans, please refer to the [Tenable.io User Guide](#).
View Audit Details in the Scan Results

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

To view audit details in the scan results:

1. Log in to Tenable.io.
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 Information**, **Family**, and **Count**.
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 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.
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.io 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**.

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.io to AWS Security Hub Transformer, Tenable.io can send vulnerabilities to AWS Security Hub. This tool consumes Tenable.io 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.io account
- Tenable.io AWS connector enabled and configured
- AWS Security Hub
- Tenable.io 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:

```markdown
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_]
                        [--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,
--since OBSERVED_SINCE         The unix timestamp of the age threshold
--run-every RUN_EVERY          
```
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
```