Tenable and OpenShift Integration Guide

Last Revised: August 26, 2026

Copyright © 2026 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Table of Contents

Welcome to Tenable for Red Hat OpenShift 3

Audit the OpenShift Container Platform 4

Configure the OpenShift Container Platform 5

Audit the OpenShift Container Platform in Tenable One Vulnerability Management 8

Audit the OpenShift Container Platform in Nessus 10

Welcome to Tenable for Red Hat OpenShift

The following guide provides information and steps for integrating Tenable One Vulnerability Management or Tenable Nessus Manager with RedHat OpenShift.

Red Hat® OpenShift® is a unified platform to build, modernize, and deploy applications at scale. Work smarter and faster with a complete set of services for bringing apps to market on your choice of infrastructure. By integrating OpenShift Container Platform with Tenable One Vulnerability Management or Tenable Nessus, you can detect misconfigurations in the environment.

For more information on OpenShift, refer to the Red Hat OpenShift documentation.

For information on Tenable One Vulnerability Management functions or installing and/or launching Tenable One Vulnerability Management, refer to the Tenable One Vulnerability Management User Guide.

For information on Tenable Nessus Manager functions or launching Tenable Nessus, refer to the Nessus User Guide.

Audit the OpenShift Container Platform

To audit the OpenShift Container Platform, do the following:

1. Configure the OpenShift Container Platform for use with a compliance audit, as described in Configure RedHat OpenShift Container Platform (Compliance Audit).
2. Create an audit scan with Tenable One Vulnerability Management or Tenable Nessus:
    - Audit RedHat OpenShift Container Platform in Tenable One Vulnerability Management
    - Audit RedHat OpenShift Container Platform in Nessus

Configure the OpenShift Container Platform

The Tenable integration for the Red Hat OpenShift Container Platform requires a service account configured with appropriate permissions.

Complete the following steps to create the service account, update `<service-account-name>`, and configure access:

1. Create a `yaml` file with the following (defines service account, token, cluster role, and cluster role mapping):

```
apiVersion: v1
kind: ServiceAccount
metadata:
  name: <service-account-name>
  namespace: default
---
apiVersion: v1
kind: Secret
type: kubernetes.io/service-account-token
metadata:
  name: <service-account-name>-token
  namespace: default
  annotations:
    kubernetes.io/service-account.name: <service-account-name>
---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: <service-account-name>-viewonly
rules:
  - apiGroups:
      - '*'
    resources:
      - '*'
    verbs:
      - get
      - watch
```

```
      - list
      - view
---
kind: ClusterRoleBinding
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: <service-account-name>-readonly
subjects:
  - kind: ServiceAccount
    name: <service-account-name>
    namespace: default
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: <service-account-name>-viewonly
```

2. To apply the file in the previous step, run the following command:

```
$ oc apply -f <file.yml>
serviceaccount/<service-account-name> created
secret/<service-account-name>-token created
clusterrole.rbac.authorization.k8s.io/<service-account-name>-viewonly created
clusterrolebinding.rbac.authorization.k8s.io/<service-account-name>-readonly created
```

3. To retrieve the token for API authentication, run the following command:

> **Note:** The token value is used as the **Token** in the **OpenShift Container Platform** Nessus credential.

```
$ oc describe secret <service-account-name>-token
Name:         <service-account-name>-token
Namespace:    default
Labels:       kubernetes.io/legacy-token-last-used=2025-11-04
Annotations:  kubernetes.io/service-account.name: <service-account-name>
              kubernetes.io/service-account.uid: e25ef2a6-93bf-4ff3-83d3-5328b6c82877
Type:  kubernetes.io/service-account-token
```

```
Data
====
ca.crt:          7262 bytes
namespace:       7 bytes
service-ca.crt:  8475 bytes
token:           eyJhbGciOiJSUzI1NiI…
```

Audit the OpenShift Container Platform in Tenable One Vulnerability Management

Tenable offers the ability to audit the Red Hat OpenShift Container Platform environment to detect misconfigurations in the environment using Tenable One Vulnerability Management. Complete the following steps to audit the OpenShift Container Platform in Tenable One Vulnerability Management:

Before you begin:

- Configure the OpenShift Container Platform as described in Configure Red Hat OpenShift Container Platform for a Compliance Audit.

To audit the OpenShift Container Platform in Tenable One Vulnerability Management:

1. Log in to your Tenable user interface.
2. In the upper-left corner, click the ☰ button.

   The left navigation plane appears.
3. In the upper-right corner of the page, click **Create a Scan**.

   The **Select a Scan Template** page appears.
4. Select the **Policy Compliance Auditing** template.

   The **Policy Compliance Auditing** page appears.
5. In the **Name** box, type a name for the scan.
6. (Optional) In the **Description** box, enter information to describe your scan.
7. In the **Targets** box, provide the hostname for the RedHat OpenShift Container Platform API.
8. Click **Compliance**.

9. Click **OpenShift**.

   Tenable offers pre-configured compliance checks and provides the ability to upload a custom OpenShift audit file.

10. Click each compliance check you want to add to the scan.

11. If you choose to add a custom audit file, click **Add File** and select the file to upload.

12. Click **Credentials**.

13. Click **OpenShift Container Platform**.

14. In the **Token** box, add the service account token.

15. Do one of the following:

    - Click **Save**.
    - Click the drop-down arrow next to **Save** and select **Launch** to initiate the scan.

Audit the OpenShift Container Platform in Nessus

Tenable offers the ability to audit the Red Hat OpenShift Container Platform environment to detect misconfigurations in the environment using Tenable Nessus. Complete the following steps to audit the OpenShift Container Platform in Tenable Nessus:

Before you begin:

- Configure the OpenShift Container Platform as described in Configure RedHat OpenShift Container Platform for a Compliance Audit.

To audit the OpenShift Container Platform in Tenable Nessus:

1. Log in to Tenable Nessus.
2. In the top navigation plane, click **Scans**.

   The **Scans** page appears.
3. In the upper-right corner of the page, click **New Scan**.

   The **Select a Scan Template** page appears.
4. Select the **Policy Compliance Auditing** template.

   The **Policy Compliance Auditing** page appears.
5. In the **Name** box, type a name for the scan.
6. (Optional) In the **Description** box, enter information to describe your scan.
7. In the **Targets** box, provide the hostname for the RedHat OpenShift Container Platform API.
8. Click **Compliance**.

9. Click **OpenShift** from the **Categories** drop-down.

   Tenable offers pre-configured compliance checks and provides the ability to upload a custom OpenShift audit file.

10. Click each compliance check you want to add to the scan.

11. If you choose to add a custom audit file, click **Add File** and select the file to upload.

12. Click **Credentials**.

13. Click **OpenShift Container Platform**.

14. In the **Token** box, add the service account token.

15. Do one of the following:

    - Click **Save**.
    - Click the drop-down arrow next to **Save** and select **Launch** to initiate the scan.