Tenable and OpenShift Integration Guide

Last Revised: August 07, 2023

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 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 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 Vulnerability Management or Tenable Nessus, you can detect misconfigurations in the environment.

For more information on OpenShift, see the Red Hat OpenShift documentation.

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

For information on Nessus Manager functions or launching Nessus, see 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 Vulnerability Management or Tenable Nessus:
    - Audit RedHat OpenShift Container Platform in Tenable 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, and configure access:

1. Create a service account:

   ```
   $ oc create sa <service-account-name>

   serviceaccount "audit" created
   ```

2. Describe the service account to list the tokens:

   ```
   $ oc describe sa <service-account-name>

   Name: audit

   Tokens: audit-token-f4khf
           audit-token-z8h44
   ```

3. Retrieve the token for API authentication. The token value is used as the **Token** in the **OpenShift Container Platform** Nessus credential.

   ```
   $ oc describe secret <service-account-name>-token-z8h44

   Name: robot-token-uzkbh

   Labels: <none>

   Annotations:

   kubernetes.io/service-account.name=audit,kubernetes.io/service-accoun-
   t.uid=49f19e2e-16c6-11e5-afdc-3c970e4b7ffe

   Type: kubernetes.io/service-account-token

   Data token: eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9...
   ```

4. Grant the service account appropriate permissions by logging in to your OpenShift cluster console: https://console-openshift-console.apps.openshift.<your-domain>

5. Grant the service account GET access to the following API endpoints:

   ```
   * getAuthentications: /apis/config.openshift.io/v1/authentications
   ```

* getClusterOperators: /apis/config.openshift.io/v1/clusteroperators

* getClusterRoleBindings:

/apis/rbac.authorization.k8s.io/v1/clusterrolebindings

* getClusterRoles: /apis/rbac.authorization.k8s.io/v1/clusterroles

* getClusterVersions: /apis/config.openshift.io/v1/clusterversions

* getConfigMaps_openshift-apiserver:

/api/v1/namespaces/openshift-apiserver/configmaps

* getConfigMaps_openshift-authentication:

/api/v1/namespaces/openshift-authentication/configmaps

* getConfigMaps_openshift-kube-apiserver:

/api/v1/namespaces/openshift-kube-apiserver/configmaps

* getConfigMaps_openshift-kube-controller-manager:

/api/v1/namespaces/openshift-kube-controller-manager/configmaps

* getEndpoints: /api/v1/endpoints

* getIdentities: /apis/user.openshift.io/v1/identities

* getIngressControllers_openshift-ingress-operator:

/apis/operator.openshift.io/v1/namespaces/openshift-ingress-oper-
ator/ingresscontrollers

* getKubeApiServers: /apis/operator.openshift.io/v1/kubeapiservers

* getMachineConfigPools:

/apis/machineconfiguration.openshift.io/v1/machineconfigpools

* getMachineConfigs:

/apis/machineconfiguration.openshift.io/v1/machineconfigs

* getNamespaces: /api/v1/namespaces

* getNetworkPolicies: /apis/networking.k8s.io/v1/networkpolicies

* getNodeLogs_kube-apiserver:

/api/v1/nodes/openshift/proxy/logs/kube-apiserver/

* getNodeLogs_openshift-apiserver:

/api/v1/nodes/openshift/proxy/logs/openshift-apiserver/

* getOpenShiftApiServers: /ap-
is/operator.openshift.io/v1/openshiftapiservers

* getPods: /api/v1/pods

* getPods_openshift-kube-apiserver:

/api/v1/namespaces/openshift-kube-apiserver/pods

* getRoleBindings:

/apis/rbac.authorization.k8s.io/v1/namespaces/default/rolebindings

* getRoles: /apis/rbac.authorization.k8s.io/v1/roles

* getSecrets_kubeadmin_kube-system:

/api/v1/namespaces/kube-system/secrets/kubeadmin

* getSecrets_serving-cert_openshift-apiserver:

/api/v1/namespaces/openshift-apiserver/secrets/serving-cert

* getSecurityContextConstraints:

/apis/security.openshift.io/v1/securitycontextconstraints

* getServiceAccounts: /api/v1/serviceaccounts

Audit the OpenShift Container Platform in Tenable Vulnerability Management

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