

# Guide to the Secure Configuration of Red Hat OpenShift Container Platform 4

with profile CIS Red Hat OpenShift Container Platform 4 Benchmark

— This profile defines a baseline that aligns to the Center for Internet Security® Red Hat OpenShift Container Platform 4 Benchmark™, V1.1.

This profile includes Center for Internet Security® Red Hat OpenShift Container Platform 4 CIS Benchmarks™ content.

Note that this part of the profile is meant to run on the Platform that Red Hat OpenShift Container Platform 4 runs on top of.

This profile is applicable to OpenShift versions 4.6 and greater.

The ComplianceAsCode Project

<https://www.open-scap.org/security-policies/scap-security-guide>

This guide presents a catalog of security-relevant configuration settings for Red Hat OpenShift Container Platform 4. It is a rendering of content structured in the eXtensible Configuration Checklist Description Format (XCCDF) in order to support security automation. The SCAP content is available in the `scap-security-guide` package which is developed at <https://www.open-scap.org/security-policies/scap-security-guide>.

Providing system administrators with such guidance informs them how to securely configure systems under their control in a variety of network roles. Policy makers and baseline creators can use this catalog of settings, with its associated references to higher-level security control catalogs, in order to assist them in security baseline creation. This guide is a *catalog*, *not a checklist*, and satisfaction of every item is not likely to be possible or sensible in many operational scenarios. However, the XCCDF format enables granular selection and adjustment of settings, and their association with OVAL and OCIL content provides an automated checking capability. Transformations of this document, and its associated automated checking content, are capable of providing baselines that meet a diverse set of policy objectives. Some example XCCDF *Profiles*, which are selections of items that form checklists and can be used as baselines, are available with this guide. They can be processed, in an automated fashion, with tools that support the Security Content Automation Protocol (SCAP). The NIST National Checklist Program (NCP), which provides required settings for the United States Government, is one example of a baseline created from this guidance.

Do not attempt to implement any of the settings in this guide without first testing them in a non-operational environment. The creators of this guidance assume no responsibility whatsoever for its use by other parties, and makes no guarantees, expressed or implied, about its quality, reliability, or any other

characteristic.

## Evaluation Characteristics

<b>Evaluation target</b>	ocp4-cis-api-checks-pod
<b>Benchmark URL</b>	#scap_org.open-scap_comp_ssg-ocp4-xccdf-1.2.xml
<b>Benchmark ID</b>	xccdf_org.ssgproject.content_benchmark_OCP-4
<b>Benchmark version</b>	0.1.61
<b>Profile ID</b>	xccdf_org.ssgproject.content_profile_cis
<b>Started at</b>	2022-04-12T08:20:58+00:00
<b>Finished at</b>	2022-04-12T08:21:00+00:00
<b>Performed by</b>	10012100
<b>Test system</b>	cpe:/a:redhat:openscap:1.3.5

## CPE Platforms

- cpe:/a:redhat:openshift\_container\_platform:4.1
- cpe:/a:redhat:openshift\_container\_platform:4.10
- cpe:/a:redhat:openshift\_container\_platform\_on\_aws:4
- cpe:/o:redhat:openshift\_container\_platform\_node:4
- cpe:/a:redhat:openshift\_container\_platform:4.6
- cpe:/a:redhat:openshift\_container\_platform:4.7
- cpe:/a:redhat:openshift\_container\_platform:4.8
- cpe:/a:redhat:openshift\_container\_platform:4.9
- cpe:/a:redhat:openshift\_container\_platform:4.11
- cpe:/a:redhat:openshift\_container\_platform:4.12

- **cpe:/a:redhat:openshift\_container\_platform:4.13**
- **cpe:/a:redhat:openshift\_container\_platform:4.14**
- **cpe:/a:redhat:openshift\_container\_platform:4.15**
- **cpe:/a:redhat:openshift\_container\_platform:4.16**
- **cpe:/a:redhat:openshift\_container\_platform:4.17**
- **cpe:/a:redhat:openshift\_container\_platform:4.18**
- **cpe:/a:redhat:openshift\_container\_platform\_on\_azure:4**
- **cpe:/a:redhat:openshift\_container\_platform\_on\_gcp:4**

## Addresses

- **IPv4** 127.0.0.1
- **IPv4** 10.128.0.17
- **IPv6** 0:0:0:0:0:0:1
- **IPv6** fe80:0:0:0:543f:eff:fe31:720c
- **MAC** 00:00:00:00:00:00
- **MAC** 0A:58:0A:80:00:11

# Compliance and Scoring

**The target system did not satisfy the conditions of 1 rules!** Please review rule results and consider applying remediation.

## Rule results

67 passed

1 failed

26 other

## Severity of failed rules

0 other

0 low

1 medium

0 high

## Score

Scoring system	Score	Maximum	Percent
urn:xccdf:scoring:default	99.816849	100.000000	99.82%

## Rule Overview

Title	Severity	Result
<b>Guide to the Secure Configuration of Red Hat OpenShift Container Platform 4</b> 1x fail 26x notchecked		
<b>OpenShift Settings</b> 1x fail 26x notchecked		
<b>OpenShift - Account and Access Control</b> 2x notchecked		
Restrict Automounting of Service Account Tokens	medium	<b>notchecked</b>
Ensure Usage of Unique Service Accounts	medium	<b>notchecked</b>
<b>OpenShift Kube API Server</b> 1x fail 2x notchecked		
Disable the AlwaysAdmit Admission Control Plugin	medium	<b>pass</b>
Ensure that the Admission Control Plugin AlwaysPullImages is not set	high	<b>pass</b>
Enable the NamespaceLifecycle Admission Control Plugin	medium	<b>pass</b>
Enable the NodeRestriction Admission Control Plugin	medium	<b>pass</b>
Enable the SecurityContextConstraint Admission Control Plugin	medium	<b>pass</b>
Ensure that the admission control plugin SecurityContextDeny is set if PodSecurityPolicy is not used	medium	<b>pass</b>
Enable the ServiceAccount Admission Control Plugin	medium	<b>pass</b>

<b>Title</b>	<b>Severity</b>	<b>Result</b>
Ensure that anonymous requests to the API Server are authorized	medium	<b>pass</b>
Ensure catch-all FlowSchema object for API Priority and Fairness Exists	medium	<b>pass</b>
Enable the APIPriorityAndFairness feature gate	medium	<b>pass</b>
Ensure catch-all FlowSchema object for API Priority and Fairness Exists (v1alpha1)	medium	<b>notapplicable</b>
Configure the Kubernetes API Server Maximum Retained Audit Logs	low	<b>pass</b>
Configure Kubernetes API Server Maximum Audit Log Size	medium	<b>pass</b>
Configure the Audit Log Path	high	<b>pass</b>
The authorization-mode cannot be AlwaysAllow	medium	<b>pass</b>
Ensure authorization-mode Node is configured	medium	<b>pass</b>
Ensure authorization-mode RBAC is configured	medium	<b>pass</b>
Disable basic-auth-file for the API Server	medium	<b>pass</b>
Ensure that the bindAddress is set to a relevant secure port	low	<b>pass</b>
Configure the Client Certificate Authority for the API Server	medium	<b>pass</b>
Configure the Encryption Provider Cipher	medium	<b>pass</b>
Configure the Encryption Provider	medium	<b>pass</b>
Configure the etcd Certificate Authority for the API Server	medium	<b>pass</b>
Configure the etcd Certificate for the API Server	medium	<b>pass</b>
Configure the etcd Certificate Key for the API Server	medium	<b>pass</b>

Title	Severity	Result
Ensure that the --kubelet-https argument is set to true	medium	<b>pass</b>
Disable Use of the Insecure Bind Address	medium	<b>pass</b>
Prevent Insecure Port Access	medium	<b>pass</b>
Configure the kubelet Certificate Authority for the API Server	high	<b>pass</b>
Configure the kubelet Certificate File for the API Server	high	<b>pass</b>
Configure the kubelet Certificate Key for the API Server	high	<b>pass</b>
Ensure all admission control plugins are enabled	medium	<b>pass</b>
Ensure the openshift-oauth-apiserver service uses TLS	medium	<b>notchecked</b>
Ensure the openshift-oauth-apiserver service uses TLS	medium	<b>notchecked</b>
Profiling is protected by RBAC	medium	<b>pass</b>
Configure the API Server Minimum Request Timeout	medium	<b>pass</b>
Ensure that the service-account-lookup argument is set to true	medium	<b>pass</b>
Configure the Service Account Public Key for the API Server	medium	<b>pass</b>
Configure the Certificate for the API Server	medium	<b>pass</b>
Use Strong Cryptographic Ciphers on the API Server	medium	<b>pass</b>
Configure the Certificate Key for the API Server	medium	<b>pass</b>
Disable Token-based Authentication	high	<b>pass</b>
Ensure that Audit Log Forwarding Is Enabled	medium	<b>fail</b>

Title	Severity	Result
Configure the OpenShift API Server Maximum Retained Audit Logs	low	pass
Configure OpenShift API Server Maximum Audit Log Size	medium	pass
Authentication		
OpenShift Controller Settings		
OpenShift etcd Settings		
<b>OpenShift - General Security Practices 5x notchecked</b>		
Apply Security Context to Your Pods and Containers	medium	notchecked
Manage Image Provenance Using ImagePolicyWebhook	medium	notchecked
The default namespace should not be used	medium	notchecked
Ensure Seccomp Profile Pod Definitions	medium	notchecked
Create administrative boundaries between resources using namespaces	medium	notchecked
Ensure that the kubeadmin secret has been removed	medium	pass
Kubernetes Kubelet Settings		
OpenShift - Logging Settings		
<b>Network Configuration and Firewalls 1x notchecked</b>		
Ensure that the CNI in use supports Network Policies	high	notchecked
Ensure that application Namespaces have Network Policies defined.	high	pass
OpenShift API Server		

Title	Severity	Result
<b>Role-based Access Control 4x notchecked</b>		
Profiling is protected by RBAC	medium	pass
Ensure that the cluster-admin role is only used where required	medium	notchecked
Limit Access to Kubernetes Secrets	medium	notchecked
Minimize Access to Pod Creation	medium	notchecked
Minimize Wildcard Usage in Cluster and Local Roles	medium	notchecked
<b>Security Context Constraints (SCC) 8x notchecked</b>		
Drop Container Capabilities	medium	notchecked
Limit Container Capabilities	medium	pass
Limit Access to the Host IPC Namespace	medium	notchecked
Limit Use of the CAP_NET_RAW	medium	notchecked
Limit Access to the Host Network Namespace	medium	notchecked
Limit Containers Ability to Escalate Privileges	medium	notchecked
Limit Privileged Container Use	medium	notchecked
Limit Access to the Host Process ID Namespace	medium	notchecked
Limit Container Running As Root User	medium	notchecked
OpenShift - Kubernetes - Scheduler Settings		
<b>OpenShift Secrets Management 2x notchecked</b>		



Title	Severity	Result
Consider external secret storage	medium	<b>notchecked</b>
Do Not Use Environment Variables with Secrets	medium	<b>notchecked</b>
<b>OpenShift - Worker Node Settings 2x notchecked</b>		
Verify Group Who Owns The Worker Proxy Kubeconfig File	medium	<b>notchecked</b>
Verify User Who Owns The Worker Proxy Kubeconfig File	medium	<b>notchecked</b>
Verify Permissions on the Worker Proxy Kubeconfig File	medium	<b>pass</b>

Red Hat and Red Hat Enterprise Linux are either registered trademarks or trademarks of Red Hat, Inc. in the United States and other countries. All other names are registered trademarks or trademarks of their respective companies.

Generated using OpenSCAP 1.3.4