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™, V0.3, currently unreleased.
>
> 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 (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 is available in the `scap-security-guide` package which is developed at https://www.open-scap.org/security-policies/scap-security-guide (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

Evaluation target	ocp4-cis-api-checks-pod

Benchmark URL	/content/ssg-ocp4-ds.xml
Benchmark ID	xccdf_org.ssgproject.content_benchmark_OCP-4
Profile ID	xccdf_org.ssgproject.content_profile_cis
Started at	2021-06-22T03:43:48+00:00
Finished at	2021-06-22T03:43:49+00:00
Performed by	

CPE Platforms

- **cpe:/a:redhat:openshift_container_platform:4.1**
- **cpe:/a:redhat:openshift_container_platform:4.7**
- **cpe:/o:redhat:openshift_container_platform_node:4**
- **cpe:/a:redhat:openshift_container_platform:4.6**
- **cpe:/a:redhat:openshift_container_platform:4.8**
- **cpe:/a:redhat:openshift_container_platform:4.9**
- **cpe:/a:redhat:openshift_container_platform:4.10**

Addresses

IPv4	127.0.0.1
IPv4	10.130.0.27
IPv6	0:0:0:0:0:0:0:1
IPv6	fe80:0:0:0:68b8:31ff:fe67:1878
MAC	00:00:00:00:00:00
MAC	0A:58:0A:82:00:1B

Compliance and Scoring

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

Rule results

64 passed 1 28 other

Severity of failed rules

0 1 medium

Score

Scoring system	Score	Maximum	Percent
urn:xccdf:scoring:default	99.761902	100.000000	99.76%

Rule Overview

Title	Severity	Result
Guide to the Secure Configuration of Red Hat OpenShift Container Platform 4 **1x fail** **28x notchecked**		
OpenShift Settings **1x fail** **28x notchecked**		
OpenShift - Account and Access Control **2x notchecked**		
Restrict Automounting of Service Account Tokens	medium	notchecked
Ensure Usage of Unique Service Accounts	medium	notchecked
OpenShift Secrets Management **2x notchecked**		
Consider external secret storage	medium	notchecked
Do Not Use Environment Variables with Secrets	medium	notchecked
Authentication		
OpenShift - Logging Settings		
OpenShift Kube API Server **1x fail** **2x notchecked**		
Configure the Encryption Provider Cipher	medium	pass
Ensure the openshift-oauth-apiserver service uses TLS	medium	notchecked
Enable the ServiceAccount Admission Control Plugin	medium	pass
Disable basic-auth-file for the API Server	medium	pass
Enable the APIPriorityAndFairness feature gate	medium	pass
Configure the Encryption Provider	medium	pass
Ensure authorization-mode RBAC is configured	medium	pass
Configure the OpenShift API Server Maximum Retained Audit Logs	low	pass
Ensure that the Admission Control Plugin AlwaysPullImages is not set	high	pass
Configure the API Server Minimum Request Timeout	medium	pass
Configure the etcd Certificate Key for the API Server	medium	pass
Configure the etcd Certificate Authority for the API Server	medium	pass

Title	Severity	Result
Configure the Service Account Public Key for the API Server	medium	pass
Configure the etcd Certificate for the API Server	medium	pass
Configure the Client Certificate Authority for the API Server	medium	pass
Ensure that the service-account-lookup argument is set to true	medium	pass
Configure the kubelet Certificate Key for the API Server	high	pass
Ensure catch-all FlowSchema object for API Priority and Fairness Exists (v1alpha1)	medium	pass
Prevent Insecure Port Access	medium	pass
Ensure the openshift-oauth-apiserver service uses TLS	medium	notchecked
Profiling is protected by RBAC	medium	pass
Disable Token-based Authentication	high	pass
Enable the NamespaceLifecycle Admission Control Plugin	medium	pass
Configure the kubelet Certificate File for the API Server	high	pass
Disable Use of the Insecure Bind Address	medium	pass
Enable the NodeRestriction Admission Control Plugin	medium	pass
Ensure that the --kubelet-https argument is set to true	medium	pass
Configure the Kubernetes API Server Maximum Retained Audit Logs	low	pass
Disable the AlwaysAdmit Admission Control Plugin	medium	pass
Enable the SecurityContextConstraint Admission Control Plugin	medium	pass
Ensure catch-all FlowSchema object for API Priority and Fairness Exists	medium	notapplicable
Configure Kubernetes API Server Maximum Audit Log Size	medium	pass
The authorization-mode cannot be AlwaysAllow	medium	pass
Ensure that anonymous requests to the API Server are authorized	medium	pass

Title	Severity	Result
Ensure all admission control plugins are enabled	medium	pass
Configure the Certificate Key for the API Server	medium	pass
Ensure that Audit Log Forwarding Is Enabled	medium	fail
Configure the Audit Log Path	high	pass
Ensure that the admission control plugin SecurityContextDeny is set if PodSecurityPolicy is not used	medium	pass
Use Strong Cryptographic Ciphers on the API Server	medium	pass
Ensure that the bindAddress is set to a relevant secure port	low	pass
Configure OpenShift API Server Maximum Audit Log Size	medium	pass
Configure the kubelet Certificate Authority for the API Server	high	pass
Ensure authorization-mode Node is configured	medium	pass
Configure the Certificate for the API Server	medium	pass
OpenShift Controller Settings		
OpenShift - General Security Practices **5x notchecked**		
Ensure Seccomp Profile Pod Definitions	medium	notchecked
Manage Image Provenance Using ImagePolicyWebhook	medium	notchecked
The default namespace should not be used	medium	notchecked
Create administrative boundaries between resources using namespaces	medium	notchecked
Apply Security Context to Your Pods and Containers	medium	notchecked
OpenShift API Server		
Configure the Audit Log Path	high	pass
Role-based Acess Control **4x notchecked**		
Limit Access to Kubernetes Secrets	medium	notchecked
Minimize Wildcard Usage in Cluster and Local Roles	medium	notchecked
Ensure that the cluster-admin role is only used where required	medium	notchecked

Title	Severity	Result
Minimize Access to Pod Creation	medium	**notchecked**
Profiling is protected by RBAC	medium	**pass**
Security Context Constraints (SCC) **9x notchecked**		
Limit Access to the Host IPC Namespace	medium	**notchecked**
Limit Container Running As Root User	medium	**notchecked**
Limit Access to the Host Process ID Namespace	medium	**notchecked**
Limit Use of the CAP_NET_RAW	medium	**notchecked**
Drop Container Capabilities	medium	**notchecked**
Limit Containers Ability to Escalate Privileges	medium	**notchecked**
Limit Privileged Container Use	medium	**notchecked**
Limit Access to the Host Network Namespace	medium	**notchecked**
Limit Container Capabilities	medium	**notchecked**
OpenShift etcd Settings		
Network Configuration and Firewalls **2x notchecked**		
Ensure that application Namespaces have Network Policies defined.	high	**notchecked**
Ensure that the CNI in use supports Network Policies	high	**notchecked**
OpenShift - Kubernetes - Scheduler Settings		
Kubernetes Kubelet Settings		
OpenShift - Master Node Settings **2x notchecked**		
Verify User Who Owns The Worker Proxy Kubeconfig File	medium	**notchecked**
Verify Group Who Owns The Worker Proxy Kubeconfig File	medium	**notchecked**
Verify Permissions on the Worker Proxy Kubeconfig File	medium	**pass**

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.