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

with profile PCI-DSS v3.2.1 Control Baseline for Red Hat OpenShift Container Platform 4
— Ensures PCI-DSS v3.2.1 security configuration settings are applied.

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 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

Evaluation target	ocp4-pci-dss-api-checks-pod

Benchmark URL	#scap_org.open-scap_comp_ssg-ocp4-xccdf-1.2.xml
Benchmark ID	xccdf_org.ssgproject.content_benchmark_OCP-4
Benchmark version	0.1.61
Profile ID	xccdf_org.ssgproject.content_profile_pci-dss
Started at	2022-04-12T08:20:52+00:00
Finished at	2022-04-12T08:20:55+00:00
Performed by	10012100
Test system	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** 10.128.0.15
- **IPv6** 0:0:0:0:0:0:0:1
- **IPv6** fe80:0:0:0:60ba:61ff:fe3f:bc3b
- **MAC** 00:00:00:00:00:00
- **MAC** 0A:58:0A:80:00:0F

Compliance and Scoring

The target system did not satisfy the conditions of 4 rules! Please review rule results and consider applying remediation.

Rule results

75 passed

4 failed

26 other

Severity of failed rules

0 other

0 low

4 medium

0 high

Score

Scoring system	Score	Maximum	Percent
urn:xccdf:scoring:default	90.952377	100.000000	90.95%

Rule Overview

Title	Severity	Result
Guide to the Secure Configuration of Red Hat OpenShift Container Platform 4 **4x fail** **26x notchecked**		
OpenShift Settings **4x fail** **26x notchecked**		
System and Software Integrity **1x fail**		
System Cryptographic Policies		
Ensure that File Integrity Operator is scanning the cluster	medium	**fail**
OpenShift - Account and Access Control **2x notchecked**		
Restrict Automounting of Service Account Tokens	medium	**notchecked**
Ensure Usage of Unique Service Accounts	medium	**notchecked**
OpenShift Kube API Server **1x fail** **2x notchecked**		
Disable the AlwaysAdmit Admission Control Plugin	medium	**pass**
Ensure that the Admission Control Plugin AlwaysPullImages is not set	high	**pass**
Enable the NamespaceLifecycle Admission Control Plugin	medium	**pass**
Enable the NodeRestriction Admission Control Plugin	medium	**pass**
Enable the SecurityContextConstraint Admission Control Plugin	medium	**pass**
Ensure that the admission control plugin SecurityContextDeny is set if PodSecurityPolicy is not used	medium	**pass**
Enable the ServiceAccount Admission Control Plugin	medium	**pass**
Ensure that anonymous requests to the API Server are authorized	medium	**pass**

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

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

Title	Severity	Result
Configure OpenShift API Server Maximum Audit Log Size	medium	**pass**
Authentication		
OpenShift Controller Settings		
OpenShift etcd Settings		
OpenShift - General Security Practices **1x fail** **5x notchecked**		
Ensure the notification is enabled for file integrity operator	medium	**fail**
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**
Ensure TLS v1.2 is minimum for Openshift APIServer	medium	**pass**
Kubernetes Kubelet Settings		
OpenShift - Logging Settings		
Network Configuration and Firewalls **1x fail** **1x notchecked**		
Ensure that the CNI in use supports Network Policies	high	**notchecked**
Ensure that application Namespaces have Network Policies defined.	high	**pass**

Title	Severity	Result
Ensure that all OpenShift Routes prefer TLS	medium	**fail**
OpenShift API Server		
Role-based Acess Control **4x notchecked**		
Ensure cluster roles are defined in the cluster	medium	**pass**
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**
Ensure roles are defined in the cluster	medium	**pass**
Minimize Wildcard Usage in Cluster and Local Roles	medium	**notchecked**
OpenShift - Risk Assessment Settings		
Security Context Constraints (SCC) **8x notchecked**		
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**

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

Generated using OpenSCAP 1.3.4