



OpenShift Container Platform 4.20

OpenShift sandboxed containers

OpenShift sandboxed containers guide

OpenShift Container Platform 4.20 OpenShift sandboxed containers

OpenShift sandboxed containers guide

Legal Notice

Copyright © Red Hat.

The text of and illustrations in this document are licensed by Red Hat under a Creative Commons Attribution–Share Alike 3.0 Unported license ("CC-BY-SA"). An explanation of CC-BY-SA is available at

<http://creativecommons.org/licenses/by-sa/3.0/>

. In accordance with CC-BY-SA, if you distribute this document or an adaptation of it, you must provide the URL for the original version.

Red Hat, as the licensor of this document, waives the right to enforce, and agrees not to assert, Section 4d of CC-BY-SA to the fullest extent permitted by applicable law.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, JBoss, OpenShift, Fedora, the Infinity logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

Linux[®] is the registered trademark of Linus Torvalds in the United States and other countries.

Java[®] is a registered trademark of Oracle and/or its affiliates.

XFS[®] is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

MySQL[®] is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js[®] is an official trademark of Joyent. Red Hat Software Collections is not formally related to or endorsed by the official Joyent Node.js open source or commercial project.

The OpenStack[®] Word Mark and OpenStack logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

All other trademarks are the property of their respective owners.

Abstract

OpenShift sandboxed containers support for OpenShift Container Platform provides users with built-in support for running Kata Containers as an additional optional runtime.

Table of Contents

CHAPTER 1. ABOUT OPENSIFT SANDBOXED CONTAINERS	3
--	---

CHAPTER 1. ABOUT OPENSIFT SANDBOXED CONTAINERS

OpenShift sandboxed containers provide security by running containerized applications in lightweight virtual machines. This architecture isolates your workloads from other workloads on the cluster and does not require significant changes to your existing workflows.

Confidential Containers extend OpenShift sandboxed containers and provide an additional layer of security. They ensure that your workloads are isolated from hypervisors and cloud providers. Confidential Containers protect data in use by leveraging hardware-based Trusted Execution Environments, which are verified by the Trustee attestation service.



NOTE

Because OpenShift sandboxed containers releases on a different cadence from OpenShift Container Platform, its documentation is now available as a separate documentation set at [Red Hat OpenShift sandboxed containers](#).