OpenShift Container Platform 4.20

OpenShift sandboxed containers

OpenShift sandboxed containers guide

Last Updated: 2026-01-20

OpenShift Container Platform 4.20 OpenShift sandboxed containers

OpenShift sandboxed containers guide

Legal Notice

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 OPENSHIFT 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.