



# OpenShift Container Platform 4.19

## Release notes

Highlights of what is new and what has changed with this OpenShift Container Platform release

## Table of Contents

<b>CHAPTER 1. OPENSIFT CONTAINER PLATFORM 4.19 RELEASE NOTES .....</b>	<b>6</b>
1.1. ABOUT THIS RELEASE	6
1.2. OPENSIFT CONTAINER PLATFORM LAYERED AND DEPENDENT COMPONENT SUPPORT AND COMPATIBILITY	6
1.3. NEW FEATURES AND ENHANCEMENTS	7
1.3.1. Authentication and authorization	7
1.3.1.1. Enabling direct authentication with an external OIDC identity provider (Technology Preview)	7
1.3.1.2. Enable ServiceAccountTokenNodeBinding Kubernetes feature by default	7
1.3.2. Documentation	7
1.3.2.1. Consolidated etcd documentation	7
1.3.2.2. Tutorials guide	7
1.3.3. Edge computing	7
1.3.3.1. Using RHACM PolicyGenerator resources to manage GitOps ZTP cluster policies (General Availability)	7
1.3.3.2. Configuring a local arbiter node	8
1.3.3.3. Coordinating reboots for configuration changes	8
1.3.4. Extensions (OLM v1)	8
1.3.4.1. Preflight permissions check for cluster extensions (Technology Preview)	8
1.3.4.2. Deploying a cluster extension in a specific namespace (Technology Preview)	8
1.3.5. Hosted control planes	9
1.3.5.1. Hosted control planes on Red Hat OpenStack Platform (RHOSP) 17.1 (Technology Preview)	9
1.3.6. IBM Power	9
1.3.7. IBM Z and IBM LinuxONE	9
IBM Power, IBM Z, and IBM LinuxONE support matrix	9
1.3.8. Insights Operator	13
1.3.8.1. Insights Runtime Extractor is generally available	13
1.3.9. Installation and update	14
1.3.9.1. Cluster API replaces Terraform on IBM Cloud installations	14
1.3.9.2. Installing a cluster on AWS in the Malaysia and Thailand regions	14
1.3.9.3. Cluster API replaces Terraform on Microsoft Azure Stack Hub installations	14
1.3.9.4. Support added for additional Microsoft Azure instance types	14
1.3.9.5. Outbound access for VMs in Microsoft Azure will be retired	14
1.3.9.6. Additional Confidential Computing platforms for GCP	15
1.3.9.7. Installing a cluster on Google Cloud Platform (GCP) with a user-provisioned DNS (Technology Preview)	15
1.3.9.8. Installing a cluster on VMware vSphere with multiple disks (Technology Preview)	15
1.3.9.9. Enabling boot diagnostics collection during installation on Microsoft Azure	15
1.3.9.10. Required administrator acknowledgment when updating from OpenShift Container Platform 4.18 to 4.19	16
1.3.9.11. OpenShift zones support for vSphere host groups (Technology Preview)	16
1.3.9.12. Nutanix support for the Agent-based Installer	16
1.3.10. Machine Config Operator	16
1.3.10.1. New naming for features	16
1.3.10.2. Image mode for OpenShift is now generally available	16
1.3.10.3. Boot image management is now default for Google Cloud Platform (GCP) and Amazon Web Services (AWS)	17
1.3.10.4. Changes to the Machine Config Operator certificates	17
1.3.11. Machine management	18
1.3.11.1. Migrating resources between the Cluster API and the Machine API (Technology Preview)	18
1.3.11.2. Custom prefixes for control plane machine names	18
1.3.11.3. Configuring Capacity Reservations on Amazon Web Services clusters	18

# CHAPTER 1. OPENSIFT CONTAINER PLATFORM 4.19 RELEASE NOTES

Red Hat OpenShift Container Platform provides developers and IT organizations with a hybrid cloud application platform for deploying both new and existing applications on secure, scalable resources with minimal configuration and management. OpenShift Container Platform supports a wide selection of programming languages and frameworks, such as Java, JavaScript, Python, Ruby, and PHP.

Built on Red Hat Enterprise Linux (RHEL) and Kubernetes, OpenShift Container Platform provides a more secure and scalable multitenant operating system for today's enterprise-class applications, while delivering integrated application runtimes and libraries. OpenShift Container Platform enables organizations to meet security, privacy, compliance, and governance requirements.

## 1.1. ABOUT THIS RELEASE

OpenShift Container Platform ([RHSA-2024:11038](#)) is now available. This release uses [Kubernetes 1.32](#) with CRI-O runtime. New features, changes, and known issues that pertain to OpenShift Container Platform 4.19 are included in this topic.

OpenShift Container Platform 4.19 clusters are available at <https://console.redhat.com/openshift>. From the Red Hat Hybrid Cloud Console, you can deploy OpenShift Container Platform clusters to either on-premises or cloud environments.

You must use RHCOS machines for the control plane and for the compute machines.

The support lifecycle for odd-numbered releases, such as OpenShift Container Platform 4.19, on all supported architectures, including **x86\_64**, 64-bit ARM (**aarch64**), IBM Power® (**ppc64le**), and IBM Z® (**s390x**) architectures is 18 months. For more information about support for all versions, see the [Red Hat OpenShift Container Platform Life Cycle Policy](#).

Commencing with the OpenShift Container Platform 4.14 release, Red Hat is simplifying the administration and management of Red Hat shipped cluster Operators with the introduction of three new life cycle classifications; Platform Aligned, Platform Agnostic, and Rolling Stream. These life cycle classifications provide additional ease and transparency for cluster administrators to understand the life cycle policies of each Operator and form cluster maintenance and upgrade plans with predictable support boundaries. For more information, see [OpenShift Operator Life Cycles](#).

OpenShift Container Platform is designed for FIPS. When running Red Hat Enterprise Linux (RHEL) or Red Hat Enterprise Linux CoreOS (RHCOS) booted in FIPS mode, OpenShift Container Platform core components use the RHEL cryptographic libraries that have been submitted to NIST for FIPS 140-2/140-3 Validation on only the **x86\_64**, **ppc64le**, and **s390x** architectures.

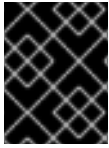
For more information about the NIST validation program, see [Cryptographic Module Validation Program](#). For the latest NIST status for the individual versions of RHEL cryptographic libraries that have been submitted for validation, see [Compliance Activities and Government Standards](#).

## 1.2. OPENSIFT CONTAINER PLATFORM LAYERED AND DEPENDENT COMPONENT SUPPORT AND COMPATIBILITY

The scope of support for layered and dependent components of OpenShift Container Platform changes independently of the OpenShift Container Platform version. To determine the current support status and compatibility for an add-on, refer to its release notes. For more information, see the [Red Hat OpenShift Container Platform Life Cycle Policy](#).

## CHAPTER 2. ADDITIONAL RELEASE NOTES

Release notes for additional related components and products not included in the core [OpenShift Container Platform 4.19 release notes](#) are available in the following documentation.



### IMPORTANT

The following release notes are for downstream Red Hat products only; upstream or community release notes for related products are not included.

#### A

[AWS Load Balancer Operator](#)

#### B

[Builds for Red Hat OpenShift](#)

#### C

[cert-manager Operator for Red Hat OpenShift](#)

[Cluster Observability Operator \(COO\)](#)

[Compliance Operator](#)

[Custom Metrics Autoscaler Operator](#)

#### D

[Red Hat Developer Hub Operator](#)

#### E

[External DNS Operator](#)

#### F

[File Integrity Operator](#)

#### K

[Kube Descheduler Operator](#)

#### M

[Migration Toolkit for Containers \(MTC\)](#)

#### N

[Network Observability Operator](#)

[Network-bound Disk Encryption \(NBDE\) Tang Server Operator](#)

#### O

[OpenShift API for Data Protection \(OADP\)](#)

[Red Hat OpenShift Dev Spaces](#)

[Red Hat OpenShift Distributed Tracing Platform](#)

[Red Hat OpenShift GitOps](#)

[Red Hat OpenShift Local \(Upstream CRC documentation\)](#)

[Red Hat OpenShift Pipelines](#)