



Red Hat build of MicroShift 4.16

Release notes

Highlights of what is new and what has changed with this MicroShift release

Red Hat build of MicroShift 4.16 Release notes

Highlights of what is new and what has changed with this MicroShift release

Legal Notice

Copyright © 2024 Red Hat, Inc.

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, the Red Hat 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 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

The release notes for MicroShift summarize all new features and enhancements, notable technical changes, major corrections from the previous version, and any known bugs.

Table of Contents

CHAPTER 1. RED HAT BUILD OF MICROSHIFT 4.16 RELEASE NOTES	3
1.1. ABOUT THIS RELEASE	3
1.2. NEW FEATURES AND ENHANCEMENTS	3
1.2.1. Red Hat Enterprise Linux (RHEL)	3
1.2.2. Updating	3
1.2.2.1. Update two minor versions in a single step	3
1.2.3. Configuring	4
1.2.3.1. Customizable certificate authorities for the API server are supported	4
1.2.3.2. Configurable policies for log file rotation and retention	4
1.2.3.3. Support for cleaning up certificates	4
1.2.4. Networking	4
1.2.4.1. Multiple networks capability now available	4
1.2.4.2. Custom configurations for the ingress router are supported	4
1.2.4.3. Configuring the route admission policy now available	4
1.2.5. Running applications	4
1.2.5.1. GitOps with Argo CD now available	4
1.2.6. Support	5
1.2.6.1. Getting a cluster ID	5
1.2.7. Security and compliance	5
1.2.7.1. SSL Medium Strength Cipher Suites now supported	5
1.2.8. Documentation enhancements	5
1.2.8.1. Route configuration now documented	5
1.3. BUG FIXES	5
Networking	5
Support	5
1.4. KNOWN ISSUES	5
1.4.1. Pods crash when writing files that exceed memory limits	5
1.5. ASYNCHRONOUS ERRATA UPDATES	6
1.5.1. RHEA-2024:0043 - MicroShift 4.16.0 bug fix and security update advisory	6

CHAPTER 1. RED HAT BUILD OF MICROSHIFT 4.16 RELEASE NOTES

Red Hat build of MicroShift provides developers and IT organizations with small-form-factor and edge computing delivered as an application that customers can deploy on top of their managed Red Hat Enterprise Linux (RHEL) devices at the edge. Built on OpenShift Container Platform and Kubernetes, MicroShift provides an efficient way to operate single-node clusters in low-resource edge environments.

MicroShift is designed to make control plane restarts economical and be lifecycle-managed as a single unit by the operating system. Updates, roll-backs, and configuration changes consist of simply staging another version in parallel and then - without relying on a network - flipping to and from that version and restarting.

1.1. ABOUT THIS RELEASE

Version 4.16 of Red Hat build of MicroShift includes new features and enhancements. MicroShift was introduced as Generally Available with MicroShift 4.14. Update to the latest version of MicroShift to receive all of the latest features, bug fixes, and security updates. MicroShift is derived from OpenShift Container Platform 4.16 and uses the CRI-O container runtime. New features, changes, and known issues that pertain to MicroShift are included in this topic.

You can deploy MicroShift clusters to on-premise, cloud, disconnected, and offline environments.

MicroShift 4.16 is supported on Red Hat Enterprise Linux (RHEL) or Red Hat Enterprise Linux for Edge (RHEL for Edge) 9.4.

For lifecycle information, see the [Red Hat build of MicroShift Life Cycle Policy](#) .

1.2. NEW FEATURES AND ENHANCEMENTS

This release adds improvements related to the following components and concepts.

1.2.1. Red Hat Enterprise Linux (RHEL)

- MicroShift 4.16 runs on Red Hat Enterprise Linux (RHEL) 9.4.

1.2.2. Updating

Updating two minor versions in a single step is now supported. Updates for both single-version minor releases and patch releases are still supported.

1.2.2.1. Update two minor versions in a single step

See the following list for details:

- You can update from one long-life-cycle version of MicroShift directly to another, without applying the intermediate version. For example, you can update directly to 4.16 from 4.14. Updating 4.14 to 4.15 before updating to 4.16 is no longer required.
- Now, you can focus on developing applications for your devices in remote locations and with limited bandwidth, rather than planning for updates.
- MicroShift offers in-place updates on RHEL for Edge systems with automatic system rollback capabilities and automatic back up and restore functions.

- Updates of the RPMs on a non-OSTree system such as RHEL are also supported.
- See [Update options with Red Hat build of MicroShift and Red Hat Device Edge](#) for details.

1.2.3. Configuring

1.2.3.1. Customizable certificate authorities for the API server are supported

With this release, you can configure a custom server certificate that has been issued by an external certificate authority (CA). The default API server certificate is issued by an internal MicroShift cluster CA. You can now replace this certificate with one that is issued by a CA that clients trust. See [Configuring custom certificate authorities](#).

1.2.3.2. Configurable policies for log file rotation and retention

You can now configure audit logging policies to manage the retention policies for log files, ensuring that edge devices with limited storage capacities are not hampered by accumulated logging data. To configure audit log policies, use settings such as a maximum file size limit and maximum retained files to set a limit on log storage size. You can also choose an audit policy profile to specify the data collected. See [Configuring audit logs](#).

1.2.3.3. Support for cleaning up certificates

With this release, you can clean up custom certificates. For more information, see [Cleaning up and recreating the custom certificates](#).

1.2.4. Networking

1.2.4.1. Multiple networks capability now available

With this release, using multiple networks is supported with the MicroShift Multus plugin. If you have advanced networking requirements, you can attach additional networks to a pod for high-performance network configurations. After installing the MicroShift Multus RPM package, you can use the Bridge, MACVLAN, or IPVLAN plugins to create additional networks. See [Additional networks in MicroShift](#).

1.2.4.2. Custom configurations for the ingress router are supported

You can now configure ingress routes to create access to multiple services inside your MicroShift cluster. You can use a variety of combinations to customize the endpoint configuration for your use case. See [About configuring the router](#).

1.2.4.3. Configuring the route admission policy now available

You can now configure the route admission policy to allow routes to claim different paths of the same hostname across namespaces. See [Configuring the route admission policy](#).

1.2.5. Running applications

1.2.5.1. GitOps with Argo CD now available

With this release, you can use the GitOps with Argo CD agent derived from GitOps 1.12 with MicroShift. Using GitOps means you can update a single Git repository and automate the deployment of new

applications or updates to existing ones. You can also use your Git repository as an audit trail of changes so that you can create processes such as review and approval for merging pull requests that implement configuration changes. See [Automating application management with the GitOps controller](#).

1.2.6. Support

1.2.6.1. Getting a cluster ID

With this release, you can get the ID of a MicroShift cluster. When opening a support case, you can provide the cluster ID to Red Hat Support to help in identifying issues with your cluster. See [Getting your cluster ID](#).

1.2.7. Security and compliance

1.2.7.1. SSL Medium Strength Cipher Suites now supported

During an SSL handshake between a client and a server, the cipher to use is negotiated between them. With this release, SSL Medium Strength Cipher Suites are now supported for the kube-controller-manager daemon, kube-scheduler control-plane process, and kubelet "node agent." This enhancement to the internal communication between kubernetes components improves control plane communications security. ([OCPBUGS-29037](#))

1.2.8. Documentation enhancements

1.2.8.1. Route configuration now documented

With this release, specific details for creating and managing supported route configurations are documented, see [Configuring routes](#).

1.3. BUG FIXES

Networking

Previously, the MicroShift load balancer controller tried to update the IP addresses of every **LoadBalancer** service in the cluster. Some of these services, such as those with a defined **loadBalancerClass**, have their own update procedures for external IPs. This conflicted with the MicroShift controller. Now, services that have a **loadBalancerClass** are filtered and IP addresses owned by other load balancer services are ignored by MicroShift. ([OCPBUGS-30833](#))

Support

Previously, when **microshift-etcd** unexpectedly exited, MicroShift tried to restart so that **microshift-etcd** could restart, but there was a lingering unit fragment. Every attempt to restart **microshift-etcd** failed, making the system unusable. The **--collect** flag was added to the **systemd-run** invocation used to start **microshift-etcd**. The additional flag results in systemd cleaning up the unit fragment even if the unit failed. The system now recovers and restarts. ([OCPBUGS-33588](#))

1.4. KNOWN ISSUES

1.4.1. Pods crash when writing files that exceed memory limits

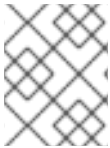
Because of an issue with RHEL, when a pod tries to write files that are larger than configured memory limits to a persistent volume claim, the pod might crash with an out-of-memory error. The pod status shows **OOMKilled** when this occurs. Use the following workarounds to avoid this issue: [Pods writing files](#)

[larger than memory limit to PVCs tend to OOM frequently running on MicroShift](#)(Red Hat Knowledgebase).

1.5. ASYNCHRONOUS ERRATA UPDATES

Security, bug fix, and enhancement updates for MicroShift 4.16 are released as asynchronous errata through the Red Hat Network. All MicroShift 4.16 errata are [available on the Red Hat Customer Portal](#) . For more information about asynchronous errata, read the [MicroShift Life Cycle](#).

Red Hat Customer Portal users can enable errata notifications in the account settings for Red Hat Subscription Management (RHSM). When errata notifications are enabled, you are notified through email whenever new errata relevant to your registered systems are released.



NOTE

Red Hat Customer Portal user accounts must have systems registered and consuming MicroShift entitlements for MicroShift errata notification emails to generate.

This section is updated over time to provide notes on enhancements and bug fixes for future asynchronous errata releases of MicroShift 4.16. Versioned asynchronous releases, for example with the form MicroShift 4.16.z, are detailed in the following subsections.

1.5.1. RHEA-2024:0043 - MicroShift 4.16.0 bug fix and security update advisory

Issued: 2024-06-27

Red Hat build of MicroShift release 4.16.0 is now available. The list of bug fixes that are included in the update is documented in the [RHSA-2024:0043](#) advisory. The images that are included in the update are provided by the [RHSA-2024:0041](#) advisory.

For the latest images included with MicroShift, view the contents of the **microshift-release-info** RPM. See [Embedding MicroShift containers for offline deployments](#).