# Red Hat Software Certification 2024

## Red Hat OpenShift Software Certification Policy Guide

For Use with Red Hat OpenShift

Last Updated: 2024-10-22

# Red Hat Software Certification 2024 Red Hat OpenShift Software Certification Policy Guide

For Use with Red Hat OpenShift

## Legal Notice



## Abstract

The Red Hat OpenShift Certification Policy Guide describes the procedural, technical and policy requirements for achieving a Red Hat certification for a software product. Version 9.3 and 8.83 updated July 31, 2024.

# Table of Contents

# MAKING OPEN SOURCE MORE INCLUSIVE

Red Hat is committed to replacing problematic language in our code and documentation. We are beginning with these four terms: master, slave, blacklist, and whitelist. Due to the enormity of this endeavor, these changes will be gradually implemented over upcoming releases. For more details on making our language more inclusive, see our CTO Chris Wright's message .

# CHAPTER 1. INTRODUCTION TO RED HAT OPENSHIFT CERTIFICATION POLICIES

The Red Hat Openshift certification policy guide covers the technical and operational certification requirements to obtain and maintain Red Hat certification for a software product on Red Hat OpenShift.

To know the test requirements and procedure for achieving this certification, see the Red Hat Software certification workflow guide.

## 1.1. AUDIENCE

Red Hat OpenShift certification is offered to commercial software vendors that deliver cloud-native software products targeting Red Hat OpenShift as the deployment platform.

## 1.2. CREATE VALUE FOR CUSTOMERS

The certification process allows partners to continuously verify if their product meets Red Hat standards of interoperability, security, and life cycle management when deployed on Red Hat OpenShift.

Our customers benefit from a trusted application and infrastructure stack, tested and jointly supported by Red Hat and the Partner.

## 1.3. TARGETED PRODUCTS FOR CERTIFICATION

Certification is available for products that target Red Hat OpenShift as their deployment platform. Red Hat recommends that you manage the product's life cycle by using technology native to Kubernetes, such as Operators or Helm charts, because they deliver a user experience that is closely integrated with Red Hat OpenShift. For these two options, certification covers the packaging format and compatibility with the Red Hat OpenShift tools. If the partner's product uses a different technology for installation and upgrades, certification will be limited to the container images.

Products that deliver infrastructure services for Red Hat OpenShift, storage services provided through a CSI driver or networking services integrated via a CNI plugin require tight integration with the platform's life cycle management. So they must be managed by an Operator and demonstrate compliance with the corresponding Kubernetes APIs.

A specialized certification is also available for cloud-native network functions for the Telecommunications market.

**Additional resources**

- For more information about building Operators that meet the certification criteria, see Certified Operator Guide.

## 1.4. RED HAT OPENSHIFT CERTIFICATION PREREQUISITES

- Join the Red Hat Partner Connect program.
- Accept the standard Partner Agreements along with the terms and conditions specific to containerized software.
- Enter basic information about your company and the products you wish to certify through the Red Hat Partner Connect portal.

- Support OpenShift as a platform for the product being certified and establish a support relationship with Red Hat. You can do this through the multi-vendor support network of TSANet, or through a custom support agreement.

**Additional resources**

- For more information about onboarding and managing your account, see General Program Guide for Partners.

## 1.5. SUPPORTED RED HAT OPENSHIFT VERSIONS

Red Hat OpenShift software certification is available for releases of Red Hat OpenShift v4.x which are in the Full, Maintenance or Extended Update Support (EUS) life cycle phases.

**Additional resources**

- For more information, see Red Hat OpenShift Container Platform Lifecycle Policy .

## 1.6. SUPPORTED ARCHITECTURES

Certification is available for all supported architectures for Red Hat OpenShift Container Platform v4.x releases. At present this includes x86_64, s390x, ppc64, and aarch64.

Certifications are awarded to a single architecture. Apply for multiple certifications if your product supports more than one architecture.

## 1.7. CERTIFICATION LIFECYCLE

Kubernetes innovates at a rapid pace, and it reflects in the fast cadence of OpenShift. It is important to approach OpenShift testing and certification as a continuous process to ensure ongoing interoperability and support for customers as they handle both platform and application updates. Partners are responsible for testing their product with each claimed Red Hat OpenShift Container Platform (RHOCP) v4.x release and each upgrade path that their software supports.

Red Hat strongly recommends running the certification tests on the latest Red Hat OpenShift minor version that you support and claim.

Certifications remain valid while the corresponding Red Hat OpenShift Container Platform (RHOCP) v.4 releases are in the Full Support or Maintenance phase of the RHOCP lifecycle. Certifications and the associated products remain published until the certifications are no longer valid or the Red Hat product gets retired from the catalog.

### 1.7.1. Recertification

Recertify your products in the following scenarios:

- Your product supports a different version of RHOCP
- Your product has changed how it is installed or upgraded
- Your product has functionality changes, or includes new functionality

Red Hat expects you to check and verify if the product is compatible with new minor releases of Red Hat OpenShift 4.x as they become available.

For security reasons, update and recertify your product components regularly. For example, recertify your containers regularly, to scan new images for vulnerabilities and mitigate security risks.

Red Hat provides multiple mechanisms to monitor certified containers published to the Red Hat ecosystem for critical vulnerabilities (CVEs) that allow certified containers to be continuously monitored to identify any critical vulnerabilities (CVEs) in the Red Hat content. These mechanisms will help you determine when to rebuild and recertify.

### Additional resources

- For more information about Container scanning and keeping your images up to date, see Container Health Index.
- For more information about implementing a CI/CD process for container builds certification, see Using OpenShift Pipelines CI/CD and Quay for Container Certification.

## 1.8. SOFTWARE DEPENDENCIES

A key benefit of Red Hat Certification is support. Ensure to check if you in coordination with Red Hat, support all the software necessary for customers to deploy and utilize your software on RHOCP.

## 1.9. FUNCTIONAL VERIFICATION

You must ensure that your product, with the same packages and components that you submitted for certification, works with the configurations supported by RHOCP.

Ensure your product does not make any modifications to the RHOCP stack, including the host operating system, other than configuration changes that are covered in the product documentation. Unauthorized changes can impact the support from Red Hat.

Red Hat encourages you to check that your product is capable of running on any node in a OpenShift cluster, regardless of the type of Red Hat OpenShift deployment (bare metal, virtual environment, or cloud service), installation process (IPI or UPI), or cluster size. If there are any limitations due to dependencies on hardware components, public cloud services, or any other cluster configuration requirements, these should be mentioned in the product’s documentation which should be linked to your product catalog listing.

### Additional resources

- To learn more about creating product listings, see Creating a Product Listing.

## 1.10. SECURITY CONTEXTS

To reduce security risks, ensure that your products run in the most restrictive Security Context Constraint (SCC). For example, **restricted-v2** for Red Hat OpenShift 4.12. If the product requires additional privileges, Red Hat recommends using the most restrictive SCC that provides the right capabilities. This configuration information should be included as part of the product documentation, and the certification tests must be conducted using the same security settings that are recommended for end users.

### Additional resources

- For more information, see Security context constraints in Red Hat OpenShift.

## 1.11. PUBLISHING TO RED HAT ECOSYSTEM CATALOG

Upon successful completion of Red Hat OpenShift Software Certification an entry will be published to the Red Hat Ecosystem Catalog . This will include a product entry and relevant information collected as part of the process.

Additionally, products managed by Operators or Helm charts will also be included in the corresponding certified Operator index or the Helm chart repository, to facilitate installation and upgrades. Both are presented to Red Hat OpenShift users through the OpenShift console.

You can opt out of being published in the Red Hat index if it is not compatible with your software distribution model. You are responsible for testing the alternate distribution and update processes, which must be included in your product documentation.

After successful certification your product is published on the Red Hat Ecosystem Catalog. Contact the Red Hat certification team, if you want to remove the certified products or certification from the catalog.

# CHAPTER 2. REQUIREMENTS FOR CONTAINER IMAGES

Certified container images must comply with the following requirements to ensure that:

- The operating system libraries are covered as part of the end-user Red Hat OpenShift support subscription.
- The image is scanned to avoid introducing known security vulnerabilities in customer environments.

## 2.1. IMAGE CONTENT REQUIREMENTS

| Requirement | Justification |
|---|---|
| Container images must declare a non-root user unless their functionality requires privileged access.<br><br>To certify container images requiring *root* access, you must:<br><br>• Include the requirement in the product documentation.<br>• Indicate that the container requires privileged host-level access in the certification project settings. This setting is subject to Red Hat review.<br><br>Test name: *RunAsNonRoot* | Ensures that containers do not run as the root user unless required. Images running as the root user can pose a security risk. |
| Container images must use a Universal Base Image (UBI) provided by Red Hat.<br><br>You can add additional RHEL packages to the UBI images, except for kernel packages.<br><br>Test name: *BasedOnUbi* | Ensures that application runtime dependencies, such as operating system components and libraries, are covered under the customer’s subscription. |
| Container images must not change content provided by Red Hat packages or layers except for files that both you or the customers can change, such as configuration files.<br><br>Test name: *HasModifiedFiles* | Ensures that Red Hat does not deny support on the basis of unauthorized changes to Red Hat components. |
| Container images must contain a “licenses” directory. Use this directory to add files containing software terms and conditions for your product and any open source software included in the image.<br><br>Test name: *HasLicense* | Ensures that customers are aware of the terms and conditions applicable to the software included in the image. |

| Requirement | Justification |
|---|---|
| Uncompressed container images must have less than 40 layers.<br><br>Test name: *LayerCountAcceptable* | Ensures that images run appropriately on containers. Too many layers could degrade the performance. |
| Container images must not include RHEL kernel packages.<br><br>Test name: *HasNoProhibitedPackages* | Ensures compliance with RHEL redistribution rules for partners. |
| Container images must not contain Red hat components with identified important or critical vulnerabilities.<br><br>Test name: *N/A*. The Red Hat Certification Service conducts this scan. | Ensures that customers are not exposed to known vulnerabilities. |

### Additional resources

- Red Hat Container Support Policy
- UBI FAQ's and licensing information
- UBI images, repositories, and package details

## 2.2. IMAGE METADATA REQUIREMENTS

| Requirement | Justification |
|---|---|
| Container images must include the following labels:<br><br>• **name**: Image Name<br>• **vendor**: Company name<br>• **version**: Version of the image<br>• **release**: A number used to identify the specific build for this image<br>• **summary**: A short overview of the application or component in this image<br>• **description**: A long description of the application or component in this image<br><br>Test name: *HasRequiredLabel* | Ensures that customers can obtain information about the image provider and the content of the images in a consistent way. |

| Requirement | Justification |
| --- | --- |
| Container images must include a unique tag that is descriptive of the certified image.<br><br>Red Hat recommends appending the image version and its build date or released date to the unique tag.<br><br>Floating tags, such as **latest** although not adequate for certification, can be added to the image in addition to the descriptive tag.<br><br>Test name: *HasUniqueTag* | Ensures that images can be uniquely identified. |

#### Additional resources

- For more information about container images and Red Hat support, see Red Hat Container Support Policy.
- For more information about Red Hat base images, see Red Hat Enterprise Linux documentation .

## 2.3. IMAGE MAINTENANCE REQUIREMENTS

Partners are responsible for monitoring the health status of their certified containers. When an image rebuild is required because of new functionality or a security update, submit the updated container image for recertification and publication.

Partners must keep the application components up-to-date and rebuild their container images periodically.

## 2.4. ADDITIONAL RESOURCES

- Red Hat Container Support Policy
- UBI FAQ's and licensing information
- UBI images, repositories, and package details

# CHAPTER 3. PRODUCTS MANAGED BY AN OPERATOR

Operators must be capable of deploying your software product on Red Hat OpenShift, using Operator Lifecycle Manager (OLM) from the targeted Red Hat OpenShift releases.

> **WARNING**
>
> If any specific hardware requirements are essential to run your certified operator, Red Hat recommends informing your customers by listing all the requirements on your product's system requirement page and linking it to your product page on the Red Hat Ecosystem catalog .

## 3.1. OPERATOR REQUIREMENTS

| Requirement | Justification |
| --- | --- |
| The Operator bundle must successfully pass the Operator SDK bundle validation.<br><br>Red Hat recommends the usage of the SDK to create the Operator, to ensure that the format is correct. | To ensure correct format and compatibility with Operator Lifecycle Manager (OLM). |
| The Operator must update the status field of each custom resource (CR). | To ensure that users can determine the running state of the CR and identify potential failures. |
| The cluster service version (CSV) in the Operator bundle must include all the fields indicated in Required CSV fields as well as the following required fields under **metadata.annotations**:<br><br>**categories**<br>Comma-separated string of the community-operators/categories list that applies to this product.<br>**description**<br>Short description of the Operator.<br>**containerImage**<br>The full location (registry, repository, name, and tag) of the Operator image.<br>**createdAt**<br>A rough (to the day) timestamp of the creation of the Operator image.<br>**support**<br>Name of your company, as the vendor supporting this product.<br>**operators.openshift.io/valid-subscription**<br>Information about subscriptions or licenses that are required to use the product, as free form text.<br>**features.operators.openshift.io/disconnected** | Provides detailed information about the product managed by this Operator to users and support organizations. |

| Requirement | Justification |
| --- | --- |
| Specify whether an Operator leverages the **spec.relatedImages** CSV field and can run without an internet connection by referring to any related image by its digest. Valid values are **"true"** or **"false"**.<br><br>**features.operators.openshift.io/fips-compliant**<br>Specify whether an Operator accepts the Federal Information Processing Standards (FIPS) configuration of the underlying platform and works on nodes that are booted into FIPS mode. In this mode, the Operator and any workloads it manages (operands) are solely calling the Red Hat Enterprise Linux (RHEL) cryptographic library submitted for FIPS-140 validation. Valid values are **"true"** or **"false"**.<br><br>**features.operators.openshift.io/proxy-aware**<br>Specify whether an Operator supports running on a cluster behind a proxy by accepting the standard **HTTP_PROXY** and **HTTPS_PROXY** proxy environment variables. If applicable, the Operator passes this information to the workload it manages (operands). Valid values are **"true"** or **"false"**.<br><br>**features.operators.openshift.io/tls-profiles**<br>Specify whether an Operator implements well-known tunables to modify the TLS cipher suite used by the Operator and, if applicable, any of the workloads it manages (operands). Valid values are **"true"** or **"false"**.<br><br>**features.operators.openshift.io/token-auth-aws**<br>Specify whether an Operator supports configuration for tokenzied authentication with AWS APIs via AWS Secure Token Service (STS) by using the Cloud Credential Operator (CCO). Valid values are **"true"** or **"false"**.<br><br>**features.operators.openshift.io/token-auth-azure**<br>Specify whether an Operator supports configuration for tokenzied authentication with Microsoft Azure APIs via Azure Managed Identity by using the Cloud Credential Operator (CCO). Valid values are **"true"** or **"false"**.<br><br>**features.operators.openshift.io/token-auth-gcp**<br>Specify whether an Operator supports configuration for tokenzied authentication with Google Cloud APIs via Google Cloud Platform (GCP) Workload Identity Foundation (WIF) by using the Cloud Credential Operator (CCO). Valid values are **"true"** or **"false"**.<br><br>Other optional annotations can be defined as well, such as for the following Kubernetes plugins:<br><br>**features.operators.openshift.io/cnf**<br>Specify whether an Operator provides a Cloud-Native Network Function (CNF) Kubernetes plugin.<br><br>**features.operators.openshift.io/cni**<br>Specify whether an Operator provides a Container Network Interface (CNI) Kubernetes plugin.<br><br>**features.operators.openshift.io/csi**<br>Specify whether an Operator provides a Container Storage Interface (CSI) Kubernetes plugin.<br><br>For more information about required annotations, optional annotations, and example usage in CSVs, see Operator metadata annotations. | |

| Requirement | Justification |
|---|---|
| The Operator bundle must indicate the minor versions of OpenShift that the target product supports by setting the **com.redhat.openshift.versions** annotation. For details on the syntax, see Controlling Operator compatibility with OpenShift Container Platform versions.<br><br>The version range must include one or more actively supported RHOCP versions, that are in the Full Suport or Maintenance Support life cycle phases.<br><br>Any Red Hat OpenShift releases that are included in the range but are no longer supported are not considered certification targets. Publication of the Operator for those releases will be handled on a best-effort-basis.<br><br>The version range can include a future release version of RHOCP. In that case, the Operator will be listed as certified after that version becomes generally available. | Informs users about the Red Hat OpenShift versions supported by the partner for this Operator, while ensuring that customers can deploy it in an OpenShift environment that can be supported by Red Hat.<br><br>The version details are used to determine which version-specific Operator catalog indexes must be updated. |
| The Operator must not use any APIs that are not present in all versions of Red Hat OpenShift included in this range. | Ensures that any APIs used are available in the targeted versions. |
| The CSV in the Operator bundle must indicate all the CRDs Owned by the Operator. | To ensure adequate tracking and management of CRD lifecycle. |
| The CSV in the Operator bundle must indicate all the container images needed to perform its function, using the **spec.relatedImages** field. | To correctly identify all the dependencies. |
| The Operator name must be different from any other Operator name already published in the Community, Certified, and Red Hat catalogs. | To avoid name conflicts. |

### Additional resources

- OpenShift Container Platform documentation: Developing Operators

## 3.2. OPERAND REQUIREMENTS

Each container managed by the Operator (Operands) must be certified by Red Hat and must fulfill the requirements listed in the Requirements for container images section.

# CHAPTER 4. PRODUCTS MANAGED BY HELM CHARTS

The Helm chart must be capable of deploying your product on Red Hat OpenShift, using the Helm utilities provided by this platform. For more information about using Helm charts on Red Hat OpenShift, see Working with Helm charts.

To be certified, the Helm chart must meet the following requirements.

| Requirement | Justification |
|---|---|
| All containers used by the Helm chart must be Red Hat certified containers. | Operating system libraries in the certified container images are covered by the Red Hat OpenShift support, and continuously monitored for security vulnerabilities. For more information on container certification requirements, see Requirements for container images. For more information about the steps to certify your containers, see Working with containers. |
| The chart's apiVersion field must be v2.0. | Chart must be compatible with Helm 3 (for example, apiVersion v2), the Helm version supported in OpenShift. |
| Chart must contain a README.md file. | Provide basic information about the chart in a human-readable format. |
| Chart must set the kubeVersion field to indicate the minimum Kubernetes version supported. | To determine chart compatibility with specific versions of OpenShift. For information on Kubernetes versions used in OpenShift, see What version of the Kubernetes API is included with each OpenShift 4.x release? article. |
| Chart must include one or more tests located in the templates directory. | To verify successful chart installation. |
| Chart must include a **values.yaml** file and a **values.schema.json** file. | Identify chart inputs and provide proper validation. |
| Chart must not contain any Custom Resource Definitions (CRDs). | Lifecycle of Custom Resource Definitions (CRDs) needs to be managed properly. Red Hat recommends an Operator for performing this task. For more information about Operators, see Working with Operators. |
| Chart must pass the helm lint command. | Ensuring correct chart format. |
| Chart must include the **charts.openshift.io/name** annotation with a human-readable name. | Provide a name that can be used when displaying the chart on the OpenShift console. |

# CHAPTER 5. FUNCTIONAL CERTIFICATION FOR OPENSHIFT BADGES

Certification badges extend the Red Hat OpenShift certification into specific functional areas or infrastructure services. A badge indicates that a certified product delivers capabilities that have been verified by Red Hat, such as conformance with Kubernetes Container Storage Interface (CSI) or Container Networking Interface (CNI) APIs.

If your product delivers any of the capabilities described in this section, Red Hat encourages you to conduct additional tests. This helps you to identify your product accordingly on the Red Hat Ecosystem Catalog.

## 5.1. CONTAINER NETWORK INTERFACE (CNI)

The CNI badge is a specialization within Red Hat OpenShift certification. It is available for networking products that integrate with OpenShift using a CNI plug-in.

### 5.1.1. Plug-in requirements

The plug-in must conform to the CNI specification version 0.3.1 or later.

You must manage the CNI plug-in through an Operator that meets the Operator certification requirements described in this document. To manage the updates to the CNI plug-in, the Operator must have the *Seamless Upgrades* capability and reflects this in the CSV.

### 5.1.2. OpenShift interoperability requirements

In addition to the default requirements for functional verification, the OpenShift cluster that you use to verify the CNI functionality must have the Multus CNI plug-in enabled during all tests. All the components that are installed on the host must be tested and supported on the versions of Red Hat Enterprise Linux and Red Hat Enterprise Linux CoreOS.

The CNI plug-in must support OpenShift Virtualization. Any unsupported or degraded features of the plug-in or OpenShift Virtualization when used in combination, must be indicated in your product documentation.

As part of the CNI certification badge, the CNI plugin can be verified for compatibility with Red Hat OpenShift Service Mesh.

### 5.1.3. Lifecycle management requirements

The plug-in must ensure minimal impact on upgrades for either major or minor plug-in releases. The plug-in upgrades should not require a full node reboot (whether major or minor) and must preserve existing connections during cluster upgrades.

The plug-in must allow new connections during upgrades. If new or existing connection preservation is not possible, this must be documented along with detailed upgrade steps. For example, if a full cluster drain or node cordoning/drain is required.

The plug-in documentation must show any difference in upgrade procedure between minor releases, bug fixes, or major updates.

Certifications are specific to the OpenShift minor release tested. Partners are required to recertify their product on new minor OpenShift releases.

### 5.1.4. CNI test compliance

The plug-in must pass the network tests of the OpenShift End-to-End Tests, based on the Kubernetes End-to-End Tests.These tests exercise the basic functions of the plug-in and show conformance to Kubernetes networking expectations.

It is mandatory to complete the corresponding virtualization tests to validate the interoperability between the CNI plug-in and Red Hat OpenShift Virtualization.

If you want to check the interoperability between the CNI plug-in and Red Hat OpenShift Service Mesh, complete the corresponding service mesh tests as part of the certification. Running the service mesh tests is optional.

#### Additional resources

- For more information about performing the certification, see Workflow Guide.
- For more information about the capability level of Operators, with Seamless Upgrades, see Operator Framework documentation.

## 5.2. CONTAINER STORAGE INTERFACE (CSI)

The CSI badge is a specialization within Red Hat OpenShift Certification. It is available to the storage products that integrate with OpenShift using a CSI driver.

### 5.2.1. Driver requirements

The CSI driver must implement version 1.0 or later of the CSI specification. The CSI driver must implement the Create and Delete volume capabilities. All other capabilities are optional but, if implemented and supported, they must be declared via a manifest file see (example manifest file ) so they can be tested.

#### Additional resources

- For more information about the CSI versions supported by a specific OpenShift version, see specific release documents.

### 5.2.2. Operator and sidecar requirements

The CSI driver must be deployed and managed through an Operator that meets the Operator certification requirements described in this document. The requirements to use certified operands (containers) also apply to the driver’s sidecar images. You should build and maintain their sidecar images so they can meet this criterion. You can select a sidecar image published and maintained by Red Hat, available as a part of OpenShift. If you do so, verify the interoperability of your CSI driver with the sidecars, as well as test and incorporate sidecar updates when available.

### 5.2.3. OpenShift interoperability requirements

All components installed on the host must be tested and supported on the versions of Red Hat Enterprise Linux and Red Hat CoreOS, used by the OpenShift release targeted for certification.

The CSI driver should support the storage features listed in the OpenShift Virtualization storage feature matrix, so users can take full advantage of platform services for virtual machines. The CSI product documentation must indicate if any of these features are not supported by the driver.

### 5.2.4. CSI test compliance

The plugin must complete the CSI tests of the OpenShift End-to-End Tests, based on the Kubernetes End-to-End Tests.

Execute the tests for each of the storage protocols supported (such as iSCSI, NFS, FC) and must match the declared capabilities.

#### Additional resources

For more information about performing the certification, see Workflow Guide.

# CHAPTER 6. PARTNER DOCUMENTATION REQUIREMENTS

The product documentation that partners provide to their customers must:

- Include instructions on how to install and update your product on OpenShift using the certified Operator or Helm chart as applicable.
- List OpenShift as a supported platform.

Add links to your product documentation in the Product Listing information, provided as a part of the certification process.