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.
### Table of Contents

**PART I. MAKING OPEN SOURCE MORE INCLUSIVE** .................................................. 3

**CHAPTER 1. INTRODUCTION TO RED HAT OPENSHIFT CERTIFICATION POLICIES** .................. 4
1.1. AUDIENCE  ........................................... 4
1.2. CREATE VALUE FOR CUSTOMERS  ........................................... 4
1.3. RED HAT OPENSHIFT CERTIFICATION PREREQUISITES  ........................................... 4
1.4. SUPPORTED OPENSHIFT VERSIONS  ........................................... 4
1.5. CERTIFICATION LIFECYCLE  ........................................... 4
1.6. TARGETED PRODUCTS FOR CERTIFICATION  ........................................... 5
1.7. FUNCTIONAL VERIFICATION AND OPENSHIFT ENVIRONMENT  ........................................... 5

**CHAPTER 2. REQUIREMENTS FOR CONTAINER IMAGES** ........................................... 6
2.1. IMAGE CONTENT REQUIREMENTS  ........................................... 6
2.2. IMAGE METADATA REQUIREMENTS  ........................................... 7
2.3. IMAGE MAINTENANCE REQUIREMENTS  ........................................... 7
2.4. ADDITIONAL RESOURCES  ........................................... 7

**CHAPTER 3. PRODUCTS MANAGED BY AN OPERATOR** ........................................... 9
3.1. OPERATOR REQUIREMENTS  ........................................... 9
3.2. OPERAND REQUIREMENTS  ........................................... 10

**CHAPTER 4. SPECIALIZED CERTIFICATION FOR OPENSHIFT BADGES**  ........................................... 11
4.1. CONTAINER NETWORK INTERFACE (CNI)  ........................................... 11
   4.1. Plug-in requirements  ........................................... 11
   4.1.2. OpenShift interoperability requirements  ........................................... 11
   4.1.3. Lifecycle management requirements  ........................................... 11
   4.1.4. CNI test compliance  ........................................... 12
4.2. CONTAINER STORAGE INTERFACE (CSI)  ........................................... 12
   4.2.1. Driver requirements  ........................................... 12
   4.2.2. Operator and sidecar requirements  ........................................... 12
   4.2.3. OpenShift interoperability requirements  ........................................... 12
   4.2.4. CSI test compliance  ........................................... 13

**CHAPTER 5. PARTNER DOCUMENTATION REQUIREMENTS** ........................................... 14
PART I. 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 OPENSSHIFT 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 Red Hat certification for a software product on Red Hat OpenShift, see the Red Hat OpenShift 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 utilizing Kubernetes Operators.

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.

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

1.3. RED HAT OPENSHEET 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.

1.4. SUPPORTED OPENSHEET VERSIONS

Certification is available for OpenShift Container Platform v4. This provides a modern release-driven, phased life cycle, specifically for minor OpenShift versions under maintenance or extended support.

Additional resources

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

1.5. CERTIFICATION LIFECYCLE
Kubernetes innovates at a fast 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.

Verify if your product is compatible with new minor releases (4.x) of OpenShift and check if it is working after a platform upgrade. The Operator packaging format captures the compatibility information as a part of the metadata, so users can know the supported versions of OpenShift and set upgrade policies accordingly. For more details on encoding this information, see metadata requirements for Operators.

Recertify your Operator for major releases of your product or on the addition of new functionality that warrants repeating the verification tests.

Verify the content of individual components (containers) continuously to mitigate security risks. Red Hat provides this as a service for all certified containers, constantly monitoring to identify any critical vulnerabilities (CVEs) for all the Red Hat packages.

Additional resources

- For more information about OpenShift Lifecycle and release cadence, see the corresponding Lifecycle Policy.
- For more information about Container scanning and keeping your images up to date, see Maintain image grades.

1.6. TARGETED PRODUCTS FOR CERTIFICATION

The products targeted for OpenShift certification must be installed and managed by a Kubernetes Operator, and its components must be packaged as containers.

Additional resources

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

1.7. FUNCTIONAL VERIFICATION AND OPENSHIFT ENVIRONMENT

Verify if your product is working with the supported configuration on the Red Hat OpenShift Container Platform, using the same components and packaging that you submitted for certification. Install your product using the corresponding Operator.

Determine the specifics of the functional testing solely at your own discretion based on your criteria for correct application behavior.

Ensure your product does not make any modifications to the OpenShift 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.

Check if your product is capable of running on any OpenShift cluster node, regardless of the type of 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, a specific type of configuration, or cluster size, mention them in the product documentation.
CHAPTER 2. REQUIREMENTS FOR CONTAINER IMAGES

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

- Covered as part of the end-user OpenShift support subscription.
- Scanned to avoid introducing known security vulnerabilities in customer environments.

2.1. IMAGE CONTENT REQUIREMENTS

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Justification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Container images must declare a non-root user unless their functionality requires privileged access.</td>
<td>Ensures that containers do not run as the root user unless required. Images running as the root user can pose a security risk.</td>
</tr>
<tr>
<td>To certify container images requiring root access, the partner must:</td>
<td></td>
</tr>
<tr>
<td>- Include the requirement in the product documentation.</td>
<td></td>
</tr>
<tr>
<td>- Indicate that the container requires privileged host-level access in the certification project settings. This setting is subject to Red Hat review.</td>
<td></td>
</tr>
<tr>
<td>Test name: RunAsNonRoot</td>
<td></td>
</tr>
<tr>
<td>Container images must use a Universal Base Image (UBI) provided by Red Hat.</td>
<td>Ensures that images support application runtime dependencies, such as operating system components and libraries.</td>
</tr>
<tr>
<td>You can add additional RHEL packages to the UBI images, except for kernel packages.</td>
<td></td>
</tr>
<tr>
<td>Test name: BasedOnUbi</td>
<td></td>
</tr>
<tr>
<td>Container images must not change content provided by Red Hat packages or layers except for files that users can change, such as configuration files.</td>
<td>Ensures that Red Hat does not deny support on the basis of unauthorized changes to Red Hat components.</td>
</tr>
<tr>
<td>Test name: HasModifiedFiles</td>
<td></td>
</tr>
<tr>
<td>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.</td>
<td>Ensures that customers are aware of the terms and conditions applicable to the software included in the image.</td>
</tr>
<tr>
<td>Test name: HasLicense</td>
<td></td>
</tr>
<tr>
<td>Uncompressed container images must have less than 40 layers.</td>
<td>Ensures that images run appropriately on containers. Too many layers might also degrade container performance.</td>
</tr>
<tr>
<td>Test name: LayerCountAcceptable</td>
<td></td>
</tr>
</tbody>
</table>
2.2. IMAGE METADATA REQUIREMENTS

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

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Justification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Container images must include a tag other than &quot;latest&quot;.</td>
<td>Ensures that images can be uniquely identified.</td>
</tr>
<tr>
<td>Test name: HasUniqueTag</td>
<td></td>
</tr>
</tbody>
</table>

2.3. IMAGE MAINTENANCE REQUIREMENTS

Partners are responsible for monitoring the health status of their certified containers and, when a rebuild is required, submit an updated container image for certification 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
Operators must be capable of deploying your software product on Red Hat OpenShift, using the Operator Lifecycle Manager from the targeted Red Hat OpenShift releases.

### 3.1. OPERATOR REQUIREMENTS

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Justification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operator bundle must successfully pass the <a href="https://example.com">Operator SDK bundle validation</a>.</td>
<td>To ensure correct format and compatibility with the Operator Lifecycle Manager (OLM).</td>
</tr>
<tr>
<td>Red Hat recommends the usage of the SDK to create the Operator, to ensure that the format is correct.</td>
<td></td>
</tr>
<tr>
<td>The Operator must update the status field of each Custom Resource (CR).</td>
<td>To ensure that users can determine the running state of the CR and identify potential failures.</td>
</tr>
<tr>
<td>The Cluster Service Version (CSV) in the Operator bundle must include all the fields indicated as required in the <a href="https://example.com">CSV fields</a> and the following fields as metadata.</td>
<td>Provides detailed information about the product managed by this Operator to users and support organizations.</td>
</tr>
<tr>
<td>categories: Comma-separated string of the <a href="https://example.com">community-operators/categories</a> list that applies to this product.</td>
<td></td>
</tr>
<tr>
<td>description: Short description of the Operator.</td>
<td></td>
</tr>
<tr>
<td>container Image: The full location (registry, repository, name, and tag) of the Operator image.</td>
<td></td>
</tr>
<tr>
<td>created at: A rough (to the day) timestamp of the creation of the Operator image.</td>
<td></td>
</tr>
<tr>
<td>support: Name of your company, as the vendor supporting this product.</td>
<td></td>
</tr>
<tr>
<td>operators.openshift.io/valid-subscription: Information about subscriptions or licenses that are required to use the product (as free form text, for examples, see Operator metadata annotations).</td>
<td></td>
</tr>
<tr>
<td>Requirement</td>
<td>Justification</td>
</tr>
<tr>
<td>-------------</td>
<td>---------------</td>
</tr>
<tr>
<td>The Operator bundle must indicate in its metadata the minor versions of OpenShift supported for the target product by setting the com.redhat.openshift.versions through a label. For details on the syntax, see the Managing OpenShift Versions. The version range must include an actively supported OpenShift version. The Operator must not make use of APIs that have been removed in a version of OpenShift included in this range.</td>
<td>Declare OpenShift versions supported by the Operator.</td>
</tr>
<tr>
<td>CSV in Operator bundle must indicate all the CRDs Owned by the Operator.</td>
<td>To ensure adequate tracking and management of CRD lifecycle.</td>
</tr>
<tr>
<td>The Operator name must be different from any other Operator name already published in the Community, Certified, and Red Hat catalogs.</td>
<td>To avoid name conflicts.</td>
</tr>
</tbody>
</table>

**Additional resources**

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

**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. SPECIALIZED CERTIFICATION FOR OPENSHIFT BADGES

Certification badges extend the Red Hat OpenShift certification into specific functional areas or infrastructure services. These badges are the key for our customers helping them perform cloud-native deployments. 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.

4.1. 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.

4.1.1. Plug-in requirements

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

You can deploy and manage the CNI plug-in through an Operator and it must meet the requirements described in this document. Do the initial setup of the networking product before deploying OpenShift, and manage the updates to the CNI plug-in through its Operator. This implies, the Operator must have the Seamless Upgrades capability and reflects this in the CSV.

4.1.2. 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 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 the documentation of the CNI product.

4.1.3. 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 cordon/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.
4.1.4. 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.

The plug-in must complete the corresponding virtualization tests to validate the interoperability between the CNI plug-in and OpenShift Virtualization.

Additional resources

- For more information about the specific test suite components and commands, see Workflow Guide.
- For more information about the capability level of Operators, with Seamless Upgrades, see Operator Framework documentation.

4.2. 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.

to the storage products that integrate with OpenShift using a CSI driver.

4.2.1. 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.

4.2.2. Operator and sidecar requirements

You can deploy and manage the CSI driver on Red Hat OpenShift through an Operator and it must meet the 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.

4.2.3. 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 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.
4.2.4. 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.
CHAPTER 5. 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.

- 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.