Red Hat Software Certification 2024

Red Hat OpenShift 软件认证政策指南

用于 Red Hat OpenShift

Last Updated: 2024-06-25

Red Hat Software Certification 2024 Red Hat OpenShift 软件认证政策指南

用于 Red Hat OpenShift

法律通告

摘要

Red Hat OpenShift 认证策略指南描述了实现红帽产品认证所需的流程、技术和策略要求。 版本 9.0 和 8.80 更新了 2024 年 5 月 28 日。

目录

使开源包含更多

红帽承诺替换我们的代码和文档中存在问题的语言。我们从这四个术语开始：master、slave、黑名单和白名单。由于这一努力的精力，这些更改将在即将发布的版本中逐渐实施。有关让我们的语言更加包含的更多详情，请参阅我们的CTO Chris Wright 信息。

第 1 章 RED HAT OPENSHIFT 认证政策简介

Red Hat Openshift 认证策略指南涵盖了在 Red Hat OpenShift 上获取和维护红帽产品的红帽产品的技术和操作要求。

要了解实现此认证的测试要求和程序，请参阅 Red Hat Software 认证工作流指南 。

1.1. 受众

Red Hat OpenShift 认证提供给提供以 Red Hat OpenShift 作为部署平台为目标的云原生软件产品的商业软件供应商。

1.2. 为客户创建值

认证流程允许合作伙伴在 Red Hat OpenShift 上部署时，不断验证其产品是否符合红帽互操作性、安全性和生命周期管理标准。

我们的客户受益于受信任的应用程序和基础架构堆栈，由红帽及合作伙伴测试并共同支持。

1.3. 用于认证的目标产品

认证适用于将 Red Hat OpenShift 作为其部署平台的产品。红帽建议您使用 Kubernetes 原生技术（如 Operator 或 Helm chart）来管理产品生命周期，因为它们提供与 Red Hat OpenShift 紧密集成的用户体验。对于这两个选项，认证涵盖了与 Red Hat OpenShift 工具的打包格式和兼容性。如果合作伙伴的产品使用不同的技术来安装和升级，则认证将仅限于容器镜像。

通过 CNI 插件集成通过 CSI 驱动程序或网络服务为 Red Hat OpenShift 提供基础架构服务的产品需要与平台生命周期管理紧密集成。因此，它们必须由 Operator 管理，并演示与对应的 Kubernetes API 合规性。

专门认证还可用于电信市场的云原生网络功能。

其他资源

- 如需有关构建符合认证条件的 Operator 的更多信息，请参阅 认证的 Operator 指南。

1.4. RED HAT OPENSHIFT 认证先决条件

- 加入 Red Hat Partner Connect 计划。
- 接受标准合作伙伴协议以及特定于容器化软件的条款和条件。
- 输入有关您的公司的基本信息以及您希望通过 Red Hat Partner Connect 门户认证的产品。
- 支持 OpenShift 作为经过认证的产品平台，并与红帽建立支持关系。您可以通过 TSANet 的多供应商支持网络或通过自定义支持协议完成此操作。

其他资源

- 有关加入和管理您的帐户的更多信息，请参阅合作伙伴的常规计划指南。

1.5. 支持的 RED HAT OPENSHIFT 版本

Red Hat OpenShift 软件认证适用于处于完全支持阶段、维护或延长更新支持(EUS)生命周期阶段的 Red Hat OpenShift v4.x 版本。

其他资源

- 如需更多信息，请参阅 Red Hat OpenShift Container Platform 生命周期政策 。

1.6. 支持的构架

认证适用于 Red Hat OpenShift Container Platform v4.x 版本的所有支持架构。目前，这包括 x86_64、s390x、ppc64 和 aarch64。

认证被授予单个架构。如果您的产品支持多个架构，则适用于多个认证。

1.7. 认证生命周期

Kubernetes 以快速节奏进行创新，它代表了 OpenShift 的快速节奏。OpenShift 测试和认证作为持续流程，确保在客户处理平台和应用程序更新时持续互操作性和支持，这一点非常重要。合作伙伴负责测试其产品及每个声明的 Red Hat OpenShift Container Platform (RHOCP) v4.x 版本及其软件支持的升级路径。

红帽强烈建议在您支持和声明的最新 Red Hat OpenShift 次版本中运行认证测试。

当相应的 Red Hat OpenShift Container Platform (RHOCP) v.4 版本处于 RHOCP 生命周期的全面支持或维护阶段时，认证仍有效。认证和相关产品会一直发布，直到认证不再有效或红帽产品从目录中停用为止。

1.7.1. 重新认证

在以下情况下更新您的产品：

- 您的产品支持不同版本的 RHOCP
- 您的产品已改变如何安装或升级它
- 您的产品具有功能更改，或者包含新功能

红帽期望您检查并验证产品是否与 Red Hat OpenShift 4.x 的新次版本兼容。

为安全起见，请定期更新并重新认证您的产品组件。例如，定期更新您的容器，以扫描新镜像中的漏洞并降低安全风险。

红帽提供了多种 机制 来监控红帽生态系统中发布的、关键漏洞(CVE)的认证容器，允许持续监控认证容器以识别红帽内容中的任何关键漏洞(CVE)。这些机制可帮助您确定何时重新构建和重新认证。

其他资源

- 有关容器扫描并保持镜像最新的更多信息，请参阅 Container Health Index。
- 有关为容器构建认证实施 CI/CD 进程的更多信息，请参阅使用 OpenShift Pipelines CI/CD 和 Quay 进行容器认证。

1.8. 软件依赖项

红帽认证的主要优点是支持。确保检查您是否与红帽的协调，支持客户在 RHOCP 上部署和使用您的软件所需的所有软件。

1.9. 功能验证

您必须确保您的产品与您提交的软件包和组件相同的软件包和组件与 RHOCP 支持的配置一起工作。

确保您的产品不会对 RHOCP 堆栈进行任何修改，包括主机操作系统，除了产品文档中涵盖的配置更改外。未授权的更改可能会影响红帽支持。

红帽建议您检查您的产品是否可以在 OpenShift 集群的任意节点上运行，无论 Red Hat OpenShift 部署的类型（裸机、虚拟环境或云服务）、安装过程(IPI 或 UPI)或集群大小。如果硬件组件、公共云服务或任何其他集群配置要求存在任何限制，则应在产品文档中提到这些限制，它们应该与您的产品 目录列表 相关联。

其他资源

- 要了解有关创建产品列表的更多信息，请参阅创建产品列表。

1.10. 安全上下文

要降低安全风险，请确保您的产品以限制性最严格的安全性上下文约束(SCC)运行。例如，Red Hat OpenShift 4.12 的 **restricted-v2**。如果产品需要额外的特权，红帽建议使用提供正确功能的最严格的 SCC。此配置信息应包括在产品文档中，必须使用为最终用户推荐的相同安全设置来执行认证测试。

其他资源

- 如需更多信息，请参阅 Red Hat OpenShift 中的安全性上下文约束。

1.11. 发布到红帽生态系统目录

在成功完成 Red Hat OpenShift Software 认证后，会在 Red Hat Ecosystem Catalog 中发布一个条目。这将包括产品条目以及作为进程的一部分收集的相关信息。

另外，由 Operator 或 Helm chart 管理的产品也会包含在相应的认证的 Operator 索引或 Helm Chart 仓库中，以便于安装和升级。它们都通过 OpenShift 控制台提供给 Red Hat OpenShift 用户。

如果红帽索引中与您的软件分发模型不兼容，您可以选择不发布。您负责测试替代的发行版和更新流程，这些流程必须包含在您的产品文档中。

在成功认证您的产品后，红帽生态系统目录上发布您的产品。如果要从目录中删除认证产品或认证，请联系红帽认证团队。

第 2 章 容器镜像的要求

认证的容器镜像必须符合以下要求，以确保：

- 操作系统库作为最终用户 Red Hat OpenShift 支持订阅的一部分进行介绍。
- 镜像会被扫描，以避免在客户环境中引入已知的安全漏洞。

2.1. 镜像内容要求

要求	原因
容器镜像必须声明一个非 root 用户，除非其功能需要特权访问权限。 要认证需要 *root* 访问权限的容器镜像，您必须： - 在产品文档中包含要求。 - 指明容器在认证项目设置中需要特权的主机级别访问权限。这个设置可能由红帽审核。 测试名称：*RunAsNonRoot*	确保容器不会以 root 用户身份运行，除非需要。以 root 用户身份运行的镜像可能会造成安全风险。
容器镜像必须使用红帽提供的 通用基础镜像(UBI)。 您可以在 UBI 镜像中添加额外的 RHEL 软件包，但内核软件包除外。 测试名称：*BasedOnUbi*	确保客户订阅涵盖应用程序运行时依赖项，如操作系统组件和库。
除您或客户可能更改的文件（如配置文件）之外，容器镜像不得更改红帽软件包或层提供的内容。 test name: *HasModifiedFiles*	确保红帽不会因为未经授权更改红帽组件而拒绝支持。
容器镜像必须包含"许可证"目录。使用此目录添加包含您产品的软件条款和条件的文件，以及镜像中包含的任何开源软件。 测试名称：*HasLicense*	确保客户了解适用于镜像中包含的软件的条款和条件。
不压缩的容器镜像必须小于 40 层。 测试名称：*LayerCountAcceptable*	确保镜像在容器中正确运行。太多的层可能会降低性能。
容器镜像不得包含 RHEL 内核软件包。 测试名称：*HasNoProhibitedPackages*	确保符合 RHEL 为合作伙伴重新发布规则。
容器镜像不得包含具有确定 重要或关键漏洞的红帽 组件。 测试名称：*N/A*.红帽认证服务进行此扫描。	确保客户不会暴露于已知的漏洞。

要求	原因

其他资源

- Red Hat Container 支持政策
- UBI FAQ 和许可证信息
- UBI 镜像、存储库和软件包详情

2.2. 镜像元数据要求

要求	原因
容器镜像必须包括以下标签： • **名称** ：镜像名称 • **供应商** ：公司名称 • **版本** ：镜像的版本 • **release** : 用于标识此镜像的特定构建的号码 • **summary**：此镜像中应用程序或组件的简短概述 • **描述** ：此镜像中应用程序或组件的长描述 test name: *HasRequiredLabel*	确保客户可以通过一致的方式获取有关镜像供应商和镜像内容的信息。
容器镜像必须包含一个唯一标签，该标签是已认证镜像的描述。 红帽建议将镜像版本及其构建日期附加到唯一标签中。 除了描述性标签外，还可以向镜像添加 浮动标签，如 **latest**，但无法进行认证。 测试名称： *HasUniqueTag*	确保可以唯一标识镜像。

其他资源

- 有关容器镜像和红帽支持的更多信息，请参阅 Red Hat Container 支持政策 。
- 有关红帽基础镜像的更多信息，请参阅 Red Hat Enterprise Linux 文档 。

2.3. 镜像维护要求

合作伙伴负责监控其认证容器的健康状况。当因为新功能或安全更新而需要重建镜像时，提交更新的容器镜像以进行重新认证和发布。

合作伙伴必须保持应用程序组件最新状态，并定期重新构建其容器镜像。

2.4. 其他资源

- Red Hat Container 支持政策
- UBI FAQ 和许可证信息
- UBI 镜像、存储库和软件包详情

第 3 章 由 OPERATOR 管理的产品

Operator 必须能够使用目标 Red Hat OpenShift 版本的 Operator Lifecycle Manager (OLM)在 Red Hat OpenShift 上部署您的软件产品。

警告

如果任何特定的硬件要求对于运行您的认证 operator 至关重要，红帽建议通过列出产品系统要求页面中的所有要求，并将其链接到 红帽生态系统目录上的产品页面来通知 您的客户。

3.1. OPERATOR 要求

要求	原因
Operator 捆绑包必须成功通过 Operator SDK 捆绑包验证。 红帽建议使用 SDK 来创建 Operator，以确保格式正确。	确保与 Operator Lifecycle Manager (OLM)正确格式和兼容性。
Operator 必须更新每个自定义资源(CR)的 status 字段。	确保用户可以确定 CR 的运行状态并确定潜在的故障。
Operator 捆绑包中的集群服务版本(CSV)必须包含 Required CSV 字段中指示的所有字段，以及 **metadata.annotations** 下的以下必填字段： **类别** 应用于此产品的 community-operators/categories 列表的逗号分隔列表字符串。 **description** Operator 的简短描述。 **containerImage** Operator 镜像的完整位置(registry、存储库、名称和标签)。 **createdAt** 创建 Operator 镜像的大约（到天）的时间戳。 **支持** 作为支持此产品的供应商，您公司的名称。 **operators.openshift.io/valid-subscription** 有关使用该产品所需的订阅或许可证的信息，作为自由表文本。 **features.operators.openshift.io/disconnected** 指定 Operator 是否利用 **spec.relatedImages** CSV 字段，并通过引用其摘要中的任何相关镜像在没有互联网连接的情况下运行。有效值为 **"true"** 或 **"false** "。 **features.operators.openshift.io/fips-compliant** 指定 Operator 是否接受底层平台的联邦信息处理标准(FIPS)配置，并可用于引导到 FIPS 模式的节点。在这个模式中，Operator 及其管理（操作）的任何工作负载都只调用为 FIPS-140 验证提交的 Red Hat Enterprise Linux (RHEL)加密库。有效值为 **"true"** 或 **"false** "。	向用户和支持机构提供有关此 Operator 管理的产品的详细信息。

要求	原因
features.operators.openshift.io/proxy-aware 通过接受标准 **HTTP_PROXY** 和 **HTTPS_PROXY** 代理环境变量来指定 Operator 支持在代理后面的集群中运行。如果适用，Operator 会将此信息传递给它管理的工作负载（操作）。有效值为 **"true"** 或 **"false** "。 **features.operators.openshift.io/tls-profiles** 指定 Operator 是否实现已知的可调项，以修改 Operator 使用的 TLS 密码套件；如果适用，它管理的任何工作负载（操作）。有效值为 **"true"** 或 **"false** "。 **features.operators.openshift.io/token-auth-aws** 使用 Cloud Credential Operator (CCO) 指定 Operator 支持通过 AWS Secure Token Service (STS)使用 AWS API 进行 tokenzied 身份验证配置。有效值为 **"true"** 或 **"false** "。 **features.operators.openshift.io/token-auth-azure** 指定 Operator 支持使用 Cloud Credential Operator (CCO)通过 Azure Managed Identity 通过 Azure Managed Identity 进行 tokenzied 身份验证配置。有效值为 **"true"** 或 **"false** "。 **features.operators.openshift.io/token-auth-gcp** 指定 Operator 是否支持通过 Google Cloud Platform (GCP) Workload Identity Foundation (WIF)使用 Cloud Credential Operator (CCO)通过 Google Cloud API 进行 tokenzied 身份验证的配置。有效值为 **"true"** 或 **"false** "。 也可以定义其他可选注解，如以下 Kubernetes 插件： **features.operators.openshift.io/cnf** 指定 Operator 是否提供 Cloud-Native Network Function (CNF) Kubernetes 插件。 **features.operators.openshift.io/cni** 指定 Operator 是否提供 Container Network Interface (CNI) Kubernetes 插件。 **features.operators.openshift.io/csi** 指定 Operator 是否提供 Container Storage Interface (CSI) Kubernetes 插件。 如需有关 CSV 中所需注解、可选注解和示例用法的更多信息，请参阅 Operator 元数据注解。	
Operator 捆绑包必须通过设置 **com.redhat.openshift.versions** 注解来指示目标产品支持的 OpenShift 的次要版本。有关语法的详情，请参阅控制与 OpenShift Container Platform 版本的 Operator 兼容性。 版本范围必须包含一个或多个主动支持的 RHOCP 版本，它们处于 完全支持阶段或维护支持阶段。 所有包含在范围中的 Red Hat OpenShift 版本，但不再被支持。对这些版本的 Operator 发布将处理在 best-effort-basis 上。 版本范围可以包括 RHOCP 的未来发行版本。在这种情况下，Operator 会在该版本正式发布后被列为已认证。	告知用户此 Operator 支持的 Red Hat OpenShift 版本，同时确保客户可以在红帽支持的 OpenShift 环境中进行部署。 版本详情用于决定必须更新特定于版本的 Operator 目录索引。
Operator 不能使用在此范围内所有 Red Hat OpenShift 版本中不存在的任何 API。	确保目标版本中提供了使用的任何 API。
Operator 捆绑包中的 CSV 必须指示 Operator 拥有的所有 CRD。	确保正确跟踪和管理 CRD 生命周期。

要求	原因
Operator 捆绑包中的 CSV 必须使用 **spec.relatedImages** 字段指示执行其功能所需的所有容器镜像。	正确识别所有依赖项。
Operator 名称必须与社区、认证和红帽目录中已经发布的任何其他 Operator 名称不同。	为避免名称冲突。

其他资源

- OpenShift Container Platform 文档：开发 Operator

3.2. 操作对象要求

由 Operator 管理的每个容器(Operands)都必须由红帽认证，且必须满足 容器镜像要求 部分中列出的要求。

第 4 章 由 HELM CHART 管理的产品

Helm Chart 必须能够使用此平台提供的 Helm 实用程序在 Red Hat OpenShift 上部署您的产品。有关在 Red Hat OpenShift 中使用 Helm chart 的更多信息，请参阅使用 Helm chart。

要认证，Helm Chart 必须满足以下要求。

要求	原因
Helm Chart 使用的所有容器都必须是红帽认证的容器。	认证容器镜像中的操作系统库由 Red Hat OpenShift 支持涵盖，并持续监控安全漏洞。如需有关容器认证要求的更多信息，请参阅 容器镜像的要求。有关认证容器的步骤的更多信息，请参阅使用容器。
chart 的 apiVersion 字段必须是 v2.0。	Chart 必须与 Helm 3 （如 apiVersion v2）兼容，OpenShift 支持的 Helm 版本。
chart 必须包含 README.md 文件。	以人类可读格式提供有关 chart 的基本信息。
chart 必须设置 kubeVersion 字段来指示支持的最小 Kubernetes 版本。	要确定与特定版本的 OpenShift 的 Chart 兼容性。如需有关 OpenShift 中使用的 Kubernetes 版本的信息，请参阅 每个 OpenShift 4.x 版本中包括的 Kubernetes API 版本是什么？ 文章。
chart 必须在 templates 目录中包含一个或多个 测试。	验证 chart 安装是否成功。
chart 必须包含 **values.yaml** 文件和 **values.schema.json** 文件。	识别 chart 输入并提供正确的验证。
chart 不得包含任何自定义资源定义(CRD)。	需要正确管理自定义资源定义(CRD)的生命周期。红帽建议 Operator 执行此任务。如需有关 Operator 的更多信息，请参阅使用 Operator。
Chart 必须传递 helm lint 命令。	确保正确图表格式。
chart 必须包含 **chart.openshift.io/name** 注解，并带有人类可读名称。	提供在 OpenShift 控制台中显示 chart 时可以使用的名称。

第 5 章 OPENSHIFT BADGES 的功能认证

认证徽标将 Red Hat OpenShift 认证扩展到特定的功能区域或基础架构服务。徽标表示经过认证的产品提供由红帽验证的功能，如与 Kubernetes Container Storage Interface (CSI)或 Container Network Interface (CNI) API 保持一致。

如果您的产品提供了本节中描述的任何功能，红帽建议您进行其他测试。这有助于您在 红帽生态系统目录 上相应地识别您的产品。

5.1. CONTAINER NETWORK INTERFACE (CNI)

CNI 徽标是 Red Hat OpenShift 认证中的分类。它可用于使用 CNI 插件与 OpenShift 集成的网络产品。

5.1.1. 插件要求

插件必须符合 CNI 规格版本 0.3.1 或更高版本。

您必须通过满足本文档中描述的 Operator 认证要求的 Operator 管理 CNI 插件。要管理 CNI 插件的更新，Operator 必须具有 *Seamless Upgrades* 功能，并在 CSV 中反映这一点。

5.1.2. OpenShift 互操作性要求

除了 功能验证 的默认要求外，用来验证 CNI 功能的 OpenShift 集群必须在所有测试过程中都启用了 Multus CNI 插件。在主机上安装的所有组件都必须在 Red Hat Enterprise Linux 和 Red Hat Enterprise Linux CoreOS 版本中经过测试和支持。

CNI 插件必须支持 OpenShift Virtualization。在组合使用时，插件或 OpenShift Virtualization 的不受支持的或降级功能都必须在产品文档中指明。

作为 CNI 认证徽标的一部分，可以验证 CNI 插件以便与 Red Hat OpenShift Service Mesh 的兼容性。

5.1.3. 生命周期管理要求

该插件必须确保对主版本或次版本的升级的影响最小。插件升级不需要完全节点重新引导（无论是主节点还是次要），且必须在集群升级过程中保留现有连接。

该插件必须在升级过程中允许新的连接。如果无法进行新的或现有连接保留，则必须记录详细的升级步骤。例如，如果需要完整集群排空或节点 cordoning/drain。

插件文档必须在次发行版本、错误修复或主要更新之间显示升级流程的区别。

认证特定于已测试的 OpenShift 次版本。合作伙伴需要在新的次版本中重新认证其产品。

5.1.4. CNI 测试合规性

该插件必须根据 Kubernetes End-to-End Tests 传递 OpenShift End-to-End Tests 的网络测试。这些测试会操作插件的基本功能，并显示符合 Kubernetes 网络预期。

该插件必须完成对应的虚拟化测试，以验证 CNI 插件和 OpenShift Virtualization 之间的互操作性。如果 CNI 插件和 Red Hat OpenShift Service Mesh 之间的互操作性被视为认证的一部分，则插件必须完成对应的服务网格测试。

其他资源

- 有关执行认证的更多信息，请参阅 工作流指南。
- 如需有关 Operator 功能级别的更多信息，使用 Seamless Upgrades，请参阅 Operator Framework 文档。

5.2. 容器存储接口(CSI)

CSI 徽标是 Red Hat OpenShift 认证中的分类。它可供使用 CSI 驱动程序与 OpenShift 集成的存储产品使用。

5.2.1. 驱动程序要求

CSI 驱动程序必须实现 CSI 规范的 版本 1.0 或更高版本。CSI 驱动程序必须实现创建和删除卷功能。所有其他功能都是可选的，但如果实施和支持，它们必须通过清单文件查看(示例清单文件)进行声明，以便可以测试它们。

其他资源

- 有关特定 OpenShift 版本支持的 CSI 版本的更多信息，请参阅特定 的发行 文档。

5.2.2. Operator 和 sidecar 要求

CSI 驱动程序必须通过满足本文档中描述的 Operator 认证要求的 Operator 来部署和管理。使用认证操作对象（容器）的要求也适用于驱动程序的 sidecar 镜像。您应该构建和维护其 sidecar 镜像，以便它们可以满足此条件。您可以选择由红帽发布和维护的 sidecar 镜像，作为 OpenShift 的一部分。如果您这样做，请验证 CSI 驱动程序与 sidecar 的互操作性，并在可用时测试并纳入 sidecar 更新。

5.2.3. OpenShift 互操作性要求

在主机上安装的所有组件都必须在 Red Hat Enterprise Linux 和 Red Hat CoreOS 版本中进行测试和支持，供 OpenShift 发行版本用于认证。

CSI 驱动程序应支持 OpenShift Virtualization 存储功能 中列出的存储功能，因此用户可以充分利用虚拟机的平台服务。CSI 产品文档必须指示驱动程序是否支持这些功能。

5.2.4. CSI 测试合规性

该插件必须根据 Kubernetes 端到端测试，完成 OpenShift 端到端测试的 CSI 测试 。

对支持的每个存储协议（如 iSCSI、NFS、FC）执行测试，并且必须与声明的功能匹配。

其他资源

有关执行认证的更多信息，请参阅 工作流指南。

第 6 章 合作伙伴文档要求

合作伙伴为客户提供的产品文档必须：

- 包括有关如何使用认证的 Operator 或 Helm chart 在 OpenShift 上安装和更新您的产品的说明。
- 将 OpenShift 列为受支持的平台。

在产品列表信息中添加您的产品文档链接，作为认证过程的一部分。