Red Hat Software Certification 2024

Red Hat Software Certification Workflow Guide

用于 Red Hat Enterprise Linux 和 Red Hat OpenShift

Last Updated: 2024-06-25

Red Hat Software Certification 2024 Red Hat Software Certification Workflow Guide

用于 Red Hat Enterprise Linux 和 Red Hat OpenShift

法律通告

摘要

Red Hat Software Certification Workflow 指南概述了希望在一个共同支持的客户环境中使用 Operator 在 Red Hat OpenShift Platform 上部署自己的应用程序、管理应用程序或软件的红帽合作伙伴认证流程。 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 红帽软件认证计划简介

使用本指南在 Red Hat Enterprise Linux 和 Red Hat OpenShift 平台上认证和分发您的软件应用程序产品。

1.1. RED HAT 认证计划概述

红帽软件认证计划确保了以 Red Hat Enterprise Linux 和 Red Hat OpenShift 作为部署平台为目标的软件应用程序产品的兼容性。

程序有五个主要元素：

- **产品列表** ：潜在客户在使用产品前查找的所有基本产品信息的来源。
- **组件** ：它包含容器、操作员、helm chart 以及附加到产品列表中的各种其他基础架构服务。另外，它还包括跟踪和报告认证请求的进度和状态的在线工作流。
- **测试套件** ：测试作为软件应用程序产品的集成管道实施。
- **出版物** ：
  - **非容器化产品** ：经过认证的传统、非容器化产品在红帽生态系统目录中发布。
  - **容器化应用程序** ：它有以下产品类别：
    - **容器** ：认证容器在红帽生态系统目录中发布。
    - **Operator** ：认证的 Operator 在红帽生态系统目录和嵌入式 OperatorHub 中发布。
    - **Helm Charts** ：认证的 Helm Charts 在红帽生态系统目录中发布。
    - **OpenShift 徽标的功能认证：**
      - **云原生网络功能(CNF)** ：供应商验证和经认证的 CNF 附加到产品列表中，并在红帽生态系统目录中发布。
      - **Container Network Interface (CNI)** 认证的 CNI 在红帽生态系统目录中发布。
      - **容器存储接口(CSI)** ：认证的 CSI 在红帽生态系统目录中发布。
    - **OpenStack 基础架构上的应用：** 非容器化、容器化和 VNF 应用在 OpenStack 基础架构上认证，并在红帽生态系统目录中发布。
- **支持** ：与您与红帽之间的共同支持关系，在部署认证软件应用程序产品时确保客户成功。

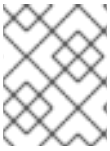
这个表总结了产品列表和组件之间的基本区别：

产品列表	组件 （项目）
包括有关您的产品的详细信息。	您测试、认证并添加到产品列表中的独立容器、操作员、helm chart 和基础架构服务。
产品由一个或多个组件组成。	组件添加到产品列表中。

产品列表	组件（项目）
您可以将组件添加到产品中以继续认证。	通过将组件添加到每个产品列表中，一个组件可用于多个产品。
在没有认证组件的情况下无法发布产品。	认证组件作为产品列表的一部分发布。

1.2. 获取帮助并提供反馈

有关本文档中描述的红帽认证工具集、认证流程或步骤的任何问题，请参阅知识库文章、红帽客户门户网站和 Red Hat Partner Connect。



注意

要接收红帽产品协助，需要具有所需的产品授权或订阅，这些权利或订阅可能与合作伙伴和认证计划成员资格分开。

创建支持问题单

要创建一个支持问题单，请参阅如何提交和管理支持问题单？

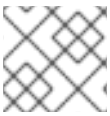
要为任何认证问题创建一个支持问题单，请特别注意以下字段，为合作伙伴加速 Desk 完成支持问题单：

- 在 Issue Category 中，选择 **Product Certification**。
- 在 Product 字段中，选择所需的产品。
- 在 **Product Version** 字段中，选择您的产品或应用程序认证的版本。
- 在 **Problem Statement** 字段中，使用以下格式输入 issue 语句或问题或反馈：

{partner Certification}（问题/咨询或反馈）

- 用认证流程 **或红帽产品或文档的反馈替换（问题/** 反馈或反馈）。

> For example: {Partner Certification} Error occurred while submitting certification test results using the Red Hat Certification application.



注意

红帽建议您在开始认证过程前具有红帽认证工程师或具有同等经验。

其他资源

- 要了解有关软件认证计划和平台的更多信息，请参阅红帽认证软件。
- 有关您所有认证需求的一站解决方案，请参阅 Red Hat Software Certification Quick Start Guide。
- 有关计划要求和策略的更多信息，请参阅 Red Hat OpenShift 软件认证政策指南 和 Red Hat Enterprise Linux 软件认证政策指南。

第 2 章 加入认证合作伙伴

如果您是新合作伙伴，请使用 Red Hat Partner Connect 门户创建新帐户，或者如果您是一个当前合作伙伴用来认证您的产品，请使用您现有的红帽帐户。

2.1. 加入现有认证合作伙伴

作为现有合作伙伴，您可以：

- 对 EPM 团队具有一定程度的一对多 EPM 计划的成员，但认证流程没有任何帮助。
  或者
- 使用分配了管理合作伙伴的专用 EPM 团队成员，以传统方式由 EPM 团队完全管理，包括有关认证请求的问题。

注意

如果您认为您的公司已有红帽帐户，但不确定谁是贵公司的机构管理员，请发送电子邮件 connect@redhat.com 以将您添加到您公司的现有帐户中。

前提条件

您有一个现有的红帽帐户。

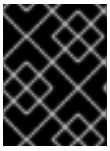
流程

1. 访问 Red Hat Partner Connect 并点 **登录**。
2. 输入您的 Red Hat 登录或电子邮件地址，然后点 **Next**。
   然后，使用以下选项之一：
   a. 使用公司单点登录登录
   b. 使用红帽帐户登录
3. 在标头的菜单栏中，点您的 avatar 查看帐户详情。
   a. 如果帐户号与您的账户相关联，请登录 Red Hat Partner Connect，以继续认证过程。
   b. 如果帐户号没有与您的帐户关联，则首先 联系红帽全局客户服务团队，以引发创建新帐户号码的请求。
   之后，登录到 Red Hat Partner Connect 以完成认证过程。

2.2. 加入新的认证合作伙伴

创建新红帽帐户是加入新认证合作伙伴的第一步。

1. 访问 Red Hat Partner Connect 并点 **登录**。
2. 点 **Register for a Red Hat account**。
3. 输入以下详情来创建新红帽帐户：
   a. **选择红帽 登录和密码**。



重要

如果您的登录 ID 与多个帐户关联，则不要使用您的联系电子邮件作为登录 ID，因为这会导致登录期间出现问题。另外，您在创建后无法更改登录 ID。

c. 输入 **您的个人信息** 和 **公司信息**。

d. 为 **Account Type** 字段选择 **Corporate**。
如果您创建了公司类型帐户并需要帐户号，请联系红帽全球客户服务团队。

注意

确保您创建公司帐户而不是个人帐户。此步骤中创建的帐户也用于在处理认证请求时登录到红帽生态系统目录。

e. 输入您的 **联系信息**。

f. 单击 **Create My Account**。
创建了一个新的红帽帐户。登录到 Red Hat Partner Connect，以继续认证过程。

2.3. 访问合作伙伴登录页面

登录 Red Hat Partner Connect 后，合作伙伴登录页面将打开。本页充当集中的中心，可访问各种合作伙伴服务和功能，以便您开始参与机会。

合作伙伴登录页面提供以下服务：

- 认证技术门户
- 交易注册
- Red Hat Partner training Portal
- 访问我们营销、销售和技术内容的库
- 帮助和支持
- 电子邮件首选项中心
- 合作伙伴订阅
- 用户帐户

作为红帽合作的一部分，合作伙伴可以访问各种红帽系统和服务，使他们能够为我们的共同客户创建与红帽的共享价值。

选择 **认证技术门户** 标题，开始您的产品认证之旅。个性化认证技术合作伙伴仪表板将打开。

部分 I. 认证独立应用程序

第 3 章 非容器化产品认证简介

用于传统、非容器化产品的红帽软件认证计划帮助独立软件供应商(ISV)在共同支持的客户环境中运行、认证和服务器环境中构建、认证并分发其应用程序软件。需要非常了解 RHEL。

第 4 章 非容器化应用的认证工作流

注意

红帽建议您在开始认证过程前具有红帽认证工程师或具有同等经验。

任务摘要

认证工作流包括三个主要阶段 -

1. 第 4.1 节 “认证加入”
2. 第 4.2 节 “认证和测试”
3. 第 4.3 节 “发布认证应用程序”

4.1. 认证加入

执行认证加入概述的步骤：

1. 加入 Red Hat Connect for Technology Program （ Red Hat Connect for Technology Program (Red Hat Connect for Technology Program)
2. 同意计划条款和条件。
3. 选择所需产品类别来创建您的产品列表。您可以从可用产品类别中选择：
   a. 容器化应用程序
   b. 独立应用程序
   c. OpenStack Infrastructure
4. 填写您的公司简介。
5. 将组件添加到产品列表中。
6. 为您的产品列表认证组件。

其他资源

有关创建第一个产品列表的详细信息，请参阅创建产品。

4.2. 认证和测试

按照以下高级别步骤运行认证测试：

- 登录到 红帽认证门户。
- 下载测试计划。
- 配置系统，在 test (SUT)下运行测试。
- 将测试计划下载到我们的 SUT。

- 在您的系统中运行认证测试。
- 查看并上传测试结果到认证门户。

其他资源

有关认证测试的详细信息，请参阅 为非容器化应用程序测试设置测试环境。

4.3. 发布认证应用程序

完成所有认证检查后，您可以向红帽提交测试结果。验证成功后，您可以在 红帽生态系统目录 上发布您的产品。

其他资源

有关发布应用程序的详细信息，请参阅 发布认证应用程序。

第 5 章 创建产品

产品列表提供营销和技术信息，向潜在客户展示您的产品功能和优势。它将为产品添加所有必要组件以进行认证的基础。

先决条件

除了特定认证测试要求外，还验证您的产品在红帽平台上的功能。如果在目标红帽平台上运行您的产品产生了子标准体验，则必须在认证前解决问题。

流程

红帽建议完成列表选项卡中的所有可选字段，以获取全面的产品列表。如需更多信息，可以帮助相互客户做出明智的选择。

在为您的产品列表输入信息时，红帽鼓励与您的产品经理、营销代表或其他产品专家合作。

带有星号 packagemanifests 的字段是必需的。

流程

1. 登录到 Red Hat Partner Connect Portal 。
2. 进入认证技术门户选项卡，**然后单击门户**。
3. 在标题栏中，单击 **产品管理**。
4. 从 **Listing and Certification 选项卡中**，单击 **Manage products**。
5. 在 **My Products** 页面中，单击 **Create Product**。
   此时会打开 **Create New Product** 对话框。
6. 输入 **产品名称**。
7. 从 **您要认证的产品中选择** 所需的产品类别，然后单击 **Create product**。例如，选择 **Standalone Application** 来创建非容器化产品列表。
   此时会打开带有您的 产品名称的新页面。它由以下标签页组成：
   - 第 5.1 节 “概述”
   - 第 5.2 节 “产品信息”
   - 第 5.3 节 “组件”
   - 第 5.4 节 “支持”
     除了以下选项卡外，页面标头还提供 **产品分数** 详细信息。产品分数评估您的产品信息并显示分数。它可以是：
     - 公平
     - 良好
     - 非常好
     - best
       点 **How do improve my score?** 以改进您的产品分数。

8. 提供产品列表详情后，请单击 **Save**，然后移至下一部分。

5.1. 概述

此选项卡由一系列任务组成，您必须完成才能发布您的产品：

- 第 5.1.1 节 “完整的产品列表详情”
- 第 5.1.2 节 “完整的公司配置文件信息”
- 第 5.1.3 节 “至少一个产品组件”
- 第 5.1.4 节 “为您的列表认证组件”

5.1.1. 完整的产品列表详情

1. 要完成您的产品列表详情，请点 **Start**。
   此时会打开 **Product Information** 选项卡。
2. 输入所有基本产品详情并点 **Save**。

5.1.2. 完整的公司配置文件信息

1. 要完成您的公司概况信息，请单击 **Start**。输入所有详情后，单击 **Submit**。
2. 要修改现有的详情，请点 **Review**。此时会打开 **Account Details** 页面。
3. 检查和修改 Company 配置集信息，然后单击 **Submit**。

5.1.3. 至少一个产品组件

1. 点 **Start**。您将被重定向到 **Components** 选项卡。
   要添加新或现有产品组件，请点 **Add component**。
2. 用于添加新组件，
   a. 在 **Component Name** 文本框中，输入组件名称。
   b. **对于您要创建的独立组件，** 请选择您要认证的组件。例如，要认证**非容器化**组件，请选择 **Non-containerized Application**。
   c. 对于 **Red Hat Enterprise Linux 版本**，请选择认证您的组件的主要 RHEL 版本。

   注意

   创建产品列表后，您无法修改版本。

   d. 单击 **Create new component**。
3. 要添加现有组件，请从 **Add 组件** 对话框中选择 **Existing Component**。
   a. 从 **Available components** 列表中，搜索并选择您要认证的组件，然后点转发箭头。所选组件被添加到 Chose **n 组件** 列表中。
   b. 单击 **Attach existing component**。

5.1.4. 为您的列表认证组件

1. 要为您的列表认证组件，请单击 **Start**。如果您有现有的产品组件，您可以查看 **Attached 组件**列表及其详情：
    a. Name
    b. 认证
    c. **安全性**
    d. 类型
    e. Created
    f. 点击**更多**选项**归档**或**删除**组件
2. 选择**用于**认证的组件。

完成上述所有任务后，您将看到与所有选项相对应的绿色勾号标记。

Overview 选项卡还**提供以下信息**：

1. **产品联系人** - 提供产品营销和技术联系信息。
    a. 点 **Add contacts to product** 以提供联系信息
    b. 点 **Edit** 以更新信息。
2. **产品中的组件** - 提供附加到产品的组件列表及其最后的更新信息。
    a. 点 **Add components to product** 将新的或现有组件添加到您的产品中。
    b. 点 **Edit components** 更新现有组件信息。

发布产品列表后，您可以查看您的产品 **就绪情况和 方式，以便在 Overview 选项卡上提高分数**。

5.2. 产品信息

通过此选项卡，您可以提供有关您产品的所有重要信息。产品详情会在红帽生态系统目录中与您的产品一起发布。

常规 标签页：

提供产品的基本详情，包括产品名称和描述。

1. 输入 **产品名称**。
2. 可选：根据 **定义的准则上传产品徽**标。
3. 输入 **Brief 描述** 和长 **描述**。
4. 点击 **Save**。

功能和好处 选项卡：

提供您产品的重要特性。

1. 可选：输入 **Title** 和 **Description**。
2. 可选： 要为您的产品添加额外的功能，请点 **+ Add new feature**。
3. 点击 **Save**。

快速启动和配置标签页 ：

添加指向任何快速入门指南或配置文档的链接，以帮助客户部署并开始使用您的产品。

1. 可选：输入 **Quick start 和 configuration instructions**。
2. 点击 **Save**。
3. 如果您不想显示它们，请选择 **Hide default instructions** 复选框。

链接的资源 标签页：

添加支持文档的链接，以帮助我们的客户使用您的产品。这些信息被映射到，并在产品目录页面中的 Documentation 部分显示。

注意

必须至少添加三个资源。如果可用，红帽建议您添加更多资源。

1. 选择 **Type** 下拉菜单，并输入资源的 **Title** 和 **Description**。
2. 输入 **资源 URL**。
3. 可选： 要为您的产品添加其他资源，请点 **+ Add new Resource**。
4. 点击 **Save**。

常见问题解答 标签页：

添加常见问题以及产品用途、操作、安装或其他属性详情的回答。您可以包括有关您的产品和服务的常见客户查询。

1. 输入问题 **和 answer**。
2. 可选： 要为您的产品添加额外的常见问题，请点 **+ Add new FAQ**。
3. 点击 **Save**。

支持 标签：

此选项卡可让您提供支持团队的联系信息。

1. 输入 **支持 描述、支持网站、支持电话号码 以及支持电子邮件地址**。
2. 点击 **Save**。

Contacts 标签页：

请提供营销和技术团队的联系信息。

1. 输入 **营销联系人电子邮件地址** 及 **技术联系电子邮件地址**。

2. 可选： 要添加其他联系人，请点 **+ Add another**。

3. 点击 **Save**。

法律 选项卡：

提供产品相关的许可证和策略信息。

1. 输入 **产品和隐私策略 URL** 的 **许可证协议 URL**。

2. 点击 **Save**。

SEO 标签页：

使用此选项卡提高我们相互客户的可发现性，提高红帽生态系统目录搜索和互联网搜索引擎中的可见性。提供更多搜索别名（密钥和证书对）会增加产品的可发现性。

1. 选择 **产品类别**。

2. 输入 **Key** 和 **Value** 来设置搜索别名。

3. 点击 **Save**。

4. 可选： 要添加额外的键值对，请点 **+ Add new key-value pair**。

注意

为您的产品至少添加一个搜索别名。如果可用，红帽建议您添加更多别名。

5.3. 组件

使用此选项卡将组件添加到您的产品列表中。通过此选项卡，您还可以查看链接到您的产品列表的附加组件列表。

另外，要将组件附加到产品列表，您可以在 Container、Operator 或 Helm Chart 产品列表的 **Overview** 选项卡中完成 **至少添加一个产品组件** 选项。

1. 要添加新或现有产品组件，请点 **Add component**。

2. 要添加新组件，在 **Component Name** 文本框中输入组件名称。

   a. **对于您要创建的独立组件，** 请选择您要认证的组件。例如，要认证非容器化组件，请选择 **Non-containerized Application**。

   b. 对于 **Red Hat Enterprise Linux 版本**，请选择您在其上认证您的非容器化组件的 RHEL 版本。

   注意

   您无法在创建产品列表后修改 RHEL 版本。

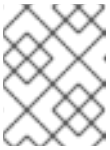
   c. 点击 **Next**。

3. 要添加现有组件，请从 **Add 组件** 对话框中选择 **Existing Component**。

   a. 从 **Available components** 列表中，搜索并选择您要认证的组件，然后点转发箭头。所选组件被添加到 **Chosen 组件** 列表中。

件被添加到 Chosen 组件 列表中。

b. 单击 **Attach existing component**。



注意

您可以将同一组件添加到多个产品列表中。所有附加的组件都必须发布，然后才能发布产品列表。

附加组件后，您可以查看 **Attached 组件** 列表及其详情：

i. Name

ii. 认证

iii. 安全性

iv. 类型

v. Created

vi. 点击更多选项归档或删除附加的组件

或者，要搜索特定组件，请在 **Search by component Name** 文本框中键入组件的名称。

5.4. 支持

红帽合作伙伴加速服务(PAD)是一个产品和技术级别合作伙伴帮助台服务，允许当前和潜在合作伙伴提供与红帽产品、合作伙伴认证、产品认证、服务流程等相关的非技术问题。

您还可以联系红帽合作伙伴加速服务，以了解您可能对认证可能遇到的任何技术问题。技术帮助请求将重定向到认证运营团队。

通过合作伙伴订阅计划，红帽提供免费的、不用于销售的软件订阅，您可用来在目标红帽平台上验证您的产品。要请求访问此计划，请按照 合作伙伴订阅 网站上的说明进行操作。

1. 要请求支持，请点击 Open a support case。请参阅 PAD - 如何打开和管理 PAD 问题单，以创建一个 PAD ticket。

2. 要查看现有支持问题单的列表，请点 **View 支持问题单**。

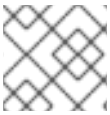
5.5. 删除产品

如果要删除产品列表后，请转到 **Overview** 选项卡，再单击 **Delete**。

先发布的产品必须取消发布，然后才能删除。即使删除该产品后，红帽仍然保留与已删除产品相关的信息。

第 6 章 添加认证组件

创建新产品列表后，为新创建的产品列表添加认证组件。您可以为新添加的组件配置以下选项：



注意

组件配置因不同的产品类别而异。

- 第 6.1 节 “认证”
- 第 6.2 节 “组件详情”
- 第 6.3 节 “联系信息”
- 第 6.4 节 “相关产品”

要配置组件选项，请转至 **Components** 选项卡，然后点任何现有组件。

6.1. 认证

在 Red Hat Enterprise Linux 中验证您的产品的功能

使用认证选项卡验证您的 Red Hat Enterprise Linux 上产品的功能。您可以执行以下功能：

此功能允许您执行以下功能：在本地运行红帽认证工具。下载测试计划。与红帽认证团队共享测试结果。如果需要，与认证团队进行交互。

要验证产品的功能，请执行以下步骤：

1. 如果您是新合作伙伴，请点击 **Request a partner subscription**。批准您的请求后，您将获得添加到您帐户的有效订阅。
2. 当您有有效的合作伙伴订阅后，单击 **开始认证**。
3. 点 **Go to Red Hat Certification 工具**

在 红帽认证门户上创建一个新的认证 案例，您会被重定向到相应的组件门户页面。

认证团队将与您联系以开始认证测试流程，并在出现问题时遵循您的操作。验证成功后，会显示带有 validate complete 消息的绿色勾号。

要查看验证的产品详情，请点 **Review**。

6.2. 组件详情

在以下字段中输入所需的项目详情：

1. **项目名称** - 输入项目名称。此名称没有发布，仅用于内部使用。
2. **Red Hat Enterprise Linux (RHEL)版本** - 指定您要在其上认证非容器化产品组件的 RHEL 版本。

注意

您无法在创建组件后更改 RHEL 版本。

6.3. 联系信息

注意

为这个选项卡提供信息是可选的。

在 **联系人信息** 选项卡中，输入您的产品组件的主要技术联系人详细信息。

1. 可选：在 **技术联系电子邮件地址** 字段中，输入镜像维护人员的电子邮件地址。
2. 可选： 要为您的组件添加额外的联系人，请点 **+ Add new contact**。
3. 点击 **Save**。

6.4. 相关产品

相关产品选项卡提供与您的产品组件关联的产品列表以及以下信息：

- 产品名称
- 类型 - 传统应用程序
- visibility - 发布或未发布
- 最后活动 - 运行测试前的天数

要在组件中添加产品，请执行以下操作：

- 如果要按名称查找产品，请在 **Search by name** 文本框中输入产品名称，然后点击搜索图标。
- 如果您不确定产品名称，请单击 **Find a product**。在 **Add product** 对话框中，从 Available products 列表中选择所需的产品，然后点转发箭头。所选产品被添加到 Chosen 产品列表中。单击 **Update attached products**。添加的产品列在相关的产品列表中。

注意

所有标有星号 * 的字段都是必需的，您必须先完成，然后才能继续认证。

第 7 章 为非容器化应用程序测试设置测试环境

认证您的产品的第一步是设置可运行测试的环境。

测试环境由运行所有认证测试的系统组成。

7.1. 设置在测试下充当系统的系统

安装或配置需要认证的产品的系统称为测试(SUT)下的系统。

先决条件

- SUT 已安装 RHEL 版本 8 或 9。为方便起见，红帽提供了 kickstart 文件来安装 SUT 的操作系统。在启动安装过程前，请按照适合您的系统文件中的说明进行操作。

流程

1. 配置 *红帽认证* 存储库：
   a. 使用您的 RHN 凭证，使用 Red Hat Subscription Management 注册您的系统：

```
$ subscription-manager register
```

   b. 显示您的系统可用订阅列表：

```
$ subscription-manager list --available*
```

   c. 搜索提供红帽认证（适用于 RHEL 服务器）存储库的订阅，并记录订阅及其池 ID。
   d. 将订阅附加到您的系统：

```
$ subscription-manager attach --pool=<pool_ID>
```

   将 pool_ID 替换为订阅的池 ID。

注意

如果您为 Red Hat Subscription Management 启用选项 Simple content access，则不必将订阅附加到您的系统。如需了解更多详细信息，请参阅如何为红帽订阅管理启用简单内容访问？

   e. 订阅红帽认证频道：
      i. 对于 RHEL 8:

```
$ subscription-manager repos --enable=cert-1-for-rhel-8-<HOSTTYPE>-rpms
```

      将 HOSTTYPE 替换为系统架构。要查找系统架构，请运行

```
$ uname -m
```

      Example:

```
$ subscription-manager repos --enable=cert-1-for-rhel-8-x86_64-rpms
```

ii. 在 RHEL 9 中：

```
$ subscription-manager repos --enable=cert-1-for-rhel-9-<HOSTTYPE>-rpms
```

将 HOSTTYPE 替换为系统架构。要查找系统架构，请运行

```
$ uname -m
```

Example:

```
$ subscription-manager repos --enable=cert-1-for-rhel-9-x86_64-rpms
```

f. 安装软件测试套件软件包：

```
$ dnf install redhat-certification-software
```

第 8 章 从红帽客户门户网站下载测试计划

流程

1. 登录到 红帽认证门户。
2. 搜索与您的产品认证相关的问题单号，并复制它。
3. 点 **Cases** → 输入产品问题单号。
4. 可选：点 **Test Plans**。
   测试计划显示测试运行期间将测试的组件列表。
5. 点 **Download Test Plan**。
   - 如果您计划使用 CLI 运行测试，请参阅使用 CLI 运行认证测试并下载结果文件。
   - 否则，如果您计划使用 Cockpit 运行测试，请参见附录。

第 9 章 使用 CLI 运行认证测试并下载结果文件

要使用 CLI 运行认证测试，您必须将测试计划下载到 SUT。运行测试后，下载结果并查看它们。

9.1. 使用 CLI 运行认证测试

流程

1. 运行以下命令:

```
# rhcert-run
```

2. 出现提示时，选择是否通过键入 **yes** 或 **no** 运行每个测试。
   您还可以通过键入 **select**，从列表中选择特定的测试。

注意

测试重启后，**rhcert** 会在后台运行，以验证镜像。使用 **tail -f /*var*/log/rhcert/RedHatCertDaemon.log** 查看当前验证的进度和状态。

9.2. 检查并下载已执行测试计划的结果文件

流程

1. 下载测试结果文件：

```
# rhcert-save
```

2. 使用 **rhcert-save** 命令将结果文件下载到您的本地系统。

其他资源

有关设置和使用 cockpit 运行认证测试的详情，请查看 附录。

第 10 章 将已执行测试计划的结果文件上传到红帽客户门户网站

先决条件

- 您已从 SUT 或 Cockpit 下载了测试结果文件。

流程

1. 登录到 红帽认证门户。
2. 在主页上，在搜索栏中输入产品问题单号。
   从显示的列表中选择问题单号。
3. 在 **Summary** 选项卡中，在 **Files** 部分下点 **Upload**。

红帽将审核提交的测试结果文件并建议后续步骤。

其他资源

如需更多信息，请访问 红帽认证门户。

第 11 章 重新认证

作为现有合作伙伴，您必须重新认证您的应用程序：

- 在 Red Hat Enterprise Linux 的每个主发行版本中
- 在应用程序的每个主版本和次版本中

注意

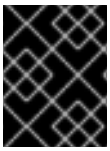
要重新认证您的应用程序，必须创建新的认证请求以进行重新认证。

要重新认证您的申请，请通过 红帽认证工具提交新的认证 请求，或在红帽合作伙伴连接中创建新组件。https://connect.redhat.com/在 SUT 上运行认证测试，并继续执行常规认证工作流，如新的认证。

第 12 章 发布认证应用程序

通过红帽认证门户 提交测试结果后，会针对漏洞扫描您的应用程序。

扫描完成后，产品列表页中将为您的应用程序启用发布按钮。https://connect.redhat.com/manage/products提供所有必要的信息后，单击发布按钮。您的应用程序将在 红帽生态系统目录 上提供。



重要

Red Hat 软件认证不会在其功能或所选平台上执行对合作伙伴的产品进行测试。认证候选产品质量保证的所有方面均保留合作伙伴的职责。

附录 A. 使用 COCKPIT 运行认证测试

注意

使用 cockpit 运行认证测试 **是可选的**。

使用以下步骤使用 cockpit 设置并运行认证测试。

A.1. 使用 COCKPIT 配置系统并运行测试

要使用 Cockpit 运行认证测试，您需要首先将测试计划上传到 SUT。运行测试后，下载结果并查看它们。

注意

虽然这不是强制要求，但红帽建议您配置和使用 Cockpit 进行认证过程。配置 cockpit 有助于您管理和监控 SUT 上的认证流程。

A.1.1. 设置 Cockpit 服务器

Cockpit 是一个 RHEL 工具，可让您更改系统配置，并从用户友好的 Web 界面监控其资源。

注意

- 您必须在 SUT 或新系统上设置 Cockpit。
- 确保 Cockpit 能够访问 SUT。

先决条件

- Cockpit 服务器安装了 RHEL 版本 8 或 9。
- 您已在系统上安装了 Cockpit 插件。
- 您已启用了 Cockpit 服务。

流程

1. 登录到安装 Cockpit 的系统。
2. 安装由红帽认证团队提供的 Cockpit RPM。

```
# dnf install redhat-certification-cockpit
```

默认情况下，Cockpit 在端口 9090 上运行。

其他资源

有关安装和配置 Cockpit 的更多信息，请参阅在 RHEL 8 上使用 RHEL web 控制台入门，使用 RHEL 9 上的 RHEL web 控制台和 Introducing Cockpit。

A.1.2. 将系统添加到 Cockpit 下

将系统添加到 Cockpit 可让它们使用免密码 SSH 进行通信。

先决条件

- 您有 SUT 的 IP 地址或主机名。

流程

1. 在浏览器中输入 **http://<*Cockpit_system_IP*>:9090/** 来启动 Cockpit Web 应用程序。
2. 输入用户名和密码，然后点 **Login**。
3. 点 logged-in cockpit 用户名上的下箭头→**Add new host**。
   此时将显示对话框。
4. 在 **Host** 字段中，输入系统的 IP 地址或主机名。
5. 在 **User name** 字段中输入您要分配给此系统的名称。
6. 可选：选择预定义的颜色，或为添加的主机选择一个新颜色。
7. 点击 **Add**。
8. 点 **Accept key 并连接**，让 Cockpit 通过免密码 SSH 与 SUT 通信。
9. 输入**密码**。
10. 选中 **Authorize SSH Key** 复选框。
11. 点**登录**。

验证

在左侧面板中，点 **Tools →Red Hat Certification**。
验证您刚刚添加的 SUT 显示在右侧的 Hosts 部分下。

A.1.3. 在 Red Hat SSO 网络中获取授权

流程

1. 在 **浏览器的地址栏中输入 http://<Cockpit_system_IP>:9090/** 以启动 Cockpit Web 应用程序。
2. 输入用户名和密码，然后点 **Login**。
3. 在左侧面板中选择 **Tools → Red Hat Certification**。
4. 在 Cockpit 主页上，单击 **Authorize**，以建立与红帽系统的连接。
   显示 **Log in to your Red Hat account**页面。
5. 输入您的凭证并点 **Next**。
   此时会显示 对 **rhcert-cwe** 页面的授予访问权限。
6. 点 **Grant access**。确认消息显示成功设备登录。您现在已连接到 Cockpit Web 应用。

A.1.4. 从红帽客户门户下载 Cockpit 中的测试计划

对于非授权或有限的访问用户：

- 要下载测试计划，请参阅从红帽客户门户网站下载测试计划。

对于授权用户：

流程

1. 在浏览器的地址栏中输入 http://<Cockpit_system_IP>:9090/ 以启动 Cockpit Web 应用程序。
2. 输入用户名和密码，然后点 **Login**。
3. 在左侧面板中选择 **Tools → Red Hat Certification**。
4. 点 **Test Plans** 选项卡。将出现 **Recent Certification Support Cases** 列表。
5. 点 **Download Test Plan**。这时将显示一条消息，确认已成功添加测试计划。
6. 下载的测试计划将在 **Test Plan Files** 的 **File Name** 部分下列出。

A.1.5. 使用测试计划准备系统进行测试

在测试下置备系统(SUT)包括以下操作：

- 设置与 cockpit 的免密码 SSH 通信
- 根据认证类型在您的系统上安装所需的软件包
- 创建运行的最终测试计划，这是从红帽提供的测试计划在发现系统要求时生成的常用测试列表。

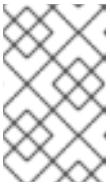
例如，如果测试计划旨在认证软件产品，将安装所需的软件包。

先决条件

- 您已下载红帽提供的测试计划。

流程

1. 在浏览器地址栏中输入 **http:// <*Cockpit_system_IP* > :9090/** 来启动 Cockpit Web 应用。
2. 输入用户名和密码，然后点 **Login**。
3. 在左侧面板中选择 **Tools → Red Hat Certification**。
4. 单击 **Hosts** 选项卡，然后单击测试下要在其上运行测试的主机。
5. 单击 **Provision**。
   此时会出现一个对话框。
   a. 点 **Upload**，然后选择新的 test plan .xml 文件。然后，单击 **Next**。此时会显示成功上传信息。
      另外，如果要重复使用之前上传的测试计划，请再次选择它来重新上传。



注意

在认证过程中，如果您收到持续产品认证的重新设计测试计划，您可以在上一步中上传它。但是，您必须在 Terminal 选项卡中运行 **rhcert-clean all**，然后才能继续。

b. 在 **Role** 字段中，选择 **test** 下的系统，再单击 **Submit**。默认情况下，该文件上传到路径：**/var/rhcert/plans/<testplanfile.xml>**

A.1.6. 使用 Cockpit 运行认证测试

先决条件

- 您已在测试下准备了系统。

流程

1. 在浏览器地址栏中输入 **http://** <*Cockpit_system_IP* > **:9090/** 来启动 Cockpit Web 应用。
2. 输入用户名和密码，然后点 **Login**。
3. 在左侧面板中选择 **Tools → Red Hat Certification**。
4. 单击 **Hosts** 选项卡，再单击要在其上运行测试的主机。
5. 点 **Terminal** 选项卡，然后选择 **Run**。
   此时会显示基于测试计划上传的推荐测试列表。运行的最终测试计划是从红帽提供的测试计划中的常见测试列表，并在发现系统要求时生成的测试。
6. 出现提示时，选择是否通过键入 **yes** 或 **no** 运行每个测试。
   您还可以通过键入 **select**，从列表中选择特定的测试。

A.1.7. 检查并下载已执行测试计划的结果文件

流程

1. 在浏览器地址栏中输入 **http://** <*Cockpit_system_IP* > **:9090/** 来启动 Cockpit Web 应用。
2. 输入用户名和密码，然后点 **Login**。
3. 在左侧面板中选择 **Tools → Red Hat Certification**。
4. 点 **Result Files** 选项卡查看生成的测试结果。
   a. 可选：点 **Preview** 查看每个测试结果。
   b. 点结果文件旁的 **Download**。默认情况下，结果文件保存为 **/var/rhcert/save/hostname-date-time.xml**。

A.1.8. 将测试结果从 Cockpit 提交到红帽客户门户网站

流程

1. 在 浏览器的地址栏中输入 http://<Cockpit_system_IP>:9090/ 以启动 Cockpit Web 应用程序。

2. 输入用户名和密码，然后点 **Login**。
3. 在左侧面板中选择 **Tools → Red Hat Certification**。
4. 点 **Result Files** 选项卡，然后从显示的列表中选择问题单号。
   a. 对于授权用户，请单击 **Submit**。这时将显示一条消息，确认已成功上传测试结果文件。
   b. 对于非授权用户，请参阅将已执行测试计划的结果文件上传到红帽客户门户网站。

已执行的测试计划的测试结果文件将上传到红帽认证门户网站中。

部分 II. 认证容器化应用程序

第 13 章 操作容器

13.1. 容器简介

容器包括库、框架等所有必要组件，这些组件在其自己的可执行文件中 **隔离和自我隔离的** 其他依赖项。红帽容器认证可确保操作系统和应用程序层的可支持性。它通过对红帽组件进行漏洞扫描和健康评分提供增强的安全性，以及更新红帽或合作伙伴组件时的生命周期承诺。

但是，以 **特权模式** 运行或特权容器的容器扩展其边界并与其主机交互，以运行命令或访问主机的资源。例如，对在主机上挂载的文件系统进行读取或写入的容器必须以特权模式运行。

特权容器可能会带来安全风险。被入侵的特权容器也可能破坏其主机以及整个环境的完整性。

此外，特权容器与操作系统接口（如命令、库、ABI 和 API）可能会随时间推移而变化或弃用主机。这可使特权容器以不支持的方式与主机交互的风险。

您必须确保容器可以在客户环境中的任何支持主机上运行。红帽建议您采用持续集成模型，可让您测试使用公共 beta 版或较早版本的红帽产品的容器，以最大化兼容性。

13.2. 容器认证工作流

注意

红帽建议您在开始认证过程前具有红帽认证工程师或具有同等经验。

任务摘要

认证工作流包括三个主要阶段：

1. 第 13.2.1 节 “认证在线”
2. 第 13.2.2 节 “容器化应用程序的认证测试”
3. 第 13.2.3 节 “在红帽生态系统目录中发布认证的产品列表”

13.2.1. 认证在线

执行认证加入概述的步骤：

1. 加入 Red Hat Connect for Technology Program （ Red Hat Connect for Technology Program (Red Hat Connect for Technology Program)
2. 同意计划条款和条件。
3. 选择所需产品类别来创建您的产品列表。您可以从可用产品类别中选择：
    a. 容器化应用程序
    b. 独立应用程序
    c. OpenStack Infrastructure
4. 填写您的公司简介。

5. 将组件添加到产品列表中。
6. 为您的产品列表认证组件。

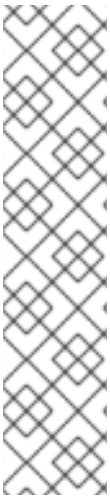
其他资源

有关创建第一个产品列表的详细信息，请参阅创建产品。

13.2.2. 容器化应用程序的认证测试

按照以下高级别步骤运行认证测试：

1. 构建容器镜像。
2. 将容器镜像上传到所选 registry。您可以选择任何您选择的 registry。



注意

您可以使用自定义容器 registry 执行 Red Hat Container 认证。这可让您为用户提供访问令牌，这有助于验证容器镜像的可用性。另外，它还确保容器镜像可以被安全扫描程序进行扫描，并可在红帽生态系统目录中发布。使用各种身份验证方法的自定义 registry，Red Hat Software 认证程序支持以下身份验证方法以及标准 OCI registry API：

- bearer 身份验证
- OAuth2
- 基本身份验证

有关验证方法的详情，请参阅支持的验证方法。

3. 下载 Preflight 认证实用程序。
4. 使用您的容器镜像运行 Preflight。
5. 提交 Red Hat Partner Connect 的结果。

其他资源

有关认证测试的详细信息，请参阅 运行认证测试套件。

13.2.3. 在红帽生态系统目录中发布认证的产品列表

认证的容器镜像通过 Red Hat Connect Image Registry 提供给客户，您可以在受支持的红帽容器平台上运行。您的产品及其镜像使用您提供的列表信息在 Red Hat Container Catalog 上列出。

其他资源

- 有关发布认证容器镜像的更多详细信息，请参阅在红帽生态系统目录上发布认证容器。
- 有关容器的更多信息，请参阅：
  - 容器和 UBI 技术跟踪
  - 选择正确的容器镜像

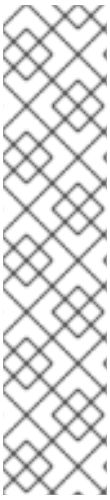
- 您需要了解 Red Hat Universal Base Image 的所有内容

13.3. 使用 PREFLIGHT 测试多架构容器认证

按照以下步骤执行多架构容器认证测试：

流程

1. 构建您的多架构容器镜像。如需更多信息，请参阅使用 Podman 构建和推送多架构容器镜像。
2. 将容器镜像上传到所选 registry。您可以选择任何您选择的 OCI registry。



注意

您可以使用自定义容器 registry 执行 Red Hat Container 认证。这可让您为用户提供访问令牌，这有助于验证容器镜像的可用性。另外，它还确保容器镜像可以被安全扫描程序扫描，并在 红帽生态系统目录 上发布。使用各种身份验证方法的自定义 registry，Red Hat Software 认证程序支持以下身份验证方法以及标准 OCI registry API：

- bearer 身份验证
- OAuth2
- 基本身份验证

有关验证方法的详情，请参阅支持的验证方法。

3. 下载 Preflight 认证实用程序。确保您有最新版本，可从任何更新或改进中受益。
4. 使用多架构容器镜像运行 preflight。如果提供的镜像是清单列表，则 preflight 将自动运行并提交所有架构的结果。
5. 检查并解决 preflight 认证结果。
6. 提交 Red Hat Partner Connect 的结果。

13.3.1. 使用 Podman 构建和推送多架构容器镜像

按照说明使用 Podman 构建和推送多架构镜像：

先决条件

1. podman 安装在您的系统上。
2. 您有一个 Dockerfile，用于定义您要为多个架构构建的镜像。
3. 您有一个 Quay.io 帐户或任何其他容器 registry 帐户。

流程

1. 准备 Dockerfile。
2. 构建和推送多架构容器镜像。有关构建和推送多架构容器镜像的说明，请查看 podman-manifest 文档。

第 14 章 创建产品

产品列表提供营销和技术信息，向潜在客户展示您的产品功能和优势。它将为产品添加所有必要组件以进行认证的基础。

先决条件

除了特定认证测试要求外，还验证您的产品在红帽平台上的功能。如果在目标红帽平台上运行您的产品产生了子标准体验，则必须在认证前解决问题。

您必须构建容器镜像，以便它们符合认证标准和策略。如需了解更多详细信息，请参阅 镜像内容要求。您还可以使用 红帽基础镜像 来构建容器镜像。在将容器镜像与容器主机匹配前，请参阅 Red Hat Enterprise Linux Container Compatibility Matrix。

流程

红帽建议完成列表选项卡中的所有可选字段，以获取全面的产品列表。如需更多信息，可以帮助相互客户做出明智的选择。

在为您的产品列表输入信息时，红帽鼓励与您的产品经理、营销代表或其他产品专家合作。

带有星号 packagemanifests 的字段是必需的。

流程

1. 登录到 Red Hat Partner Connect Portal 。
2. 进入认证技术门户选项卡，**然后单击门户**。
3. 在标题栏中，单击 **产品管理**。
4. 从 **Listing and Certification 选项卡中，** 单击 **Manage products**。
5. 在 **My Products** 页面中，单击 **Create Product**。
   此时会打开 **Create New Product** 对话框。
6. 输入 **产品名称**。
7. 从 **您要认证的产品中选择** 所需的产品类别，然后单击 **Create product**。例如，选择 **Containerized Application** 来创建容器化产品列表。
   此时会打开带有您的 产品名称的新页面。它由以下标签页组成：

   - 第 5.1 节 “概述”
   - 第 5.2 节 “产品信息”
   - 第 5.3 节 “组件”
   - 第 5.4 节 “支持”

   除了以下选项卡外，页面标头还提供 **产品分数** 详细信息。产品分数评估您的产品信息并显示分数。它可以是：

   - 公平
   - 良好

- 非常好
- best

8. 点 **How do improve my score?** 以改进您的产品分数。
9. 提供产品列表详情后，请单击 **Save**，然后移至下一部分。

14.1. 概述

此选项卡由一系列任务组成，您必须完成才能发布您的产品：

- 第 14.1.1 节 “容器化应用程序的完整产品列表详情”
- 第 14.1.2 节 “容器化应用程序的完整公司配置集信息”
- 第 14.1.3 节 “接受容器化应用程序的法律协议”
- 第 14.1.4 节 “为容器化应用程序添加至少一个产品组件”
- 第 14.1.5 节 “为您的容器化应用程序列表认证组件”

14.1.1. 容器化应用程序的完整产品列表详情

1. 要完成您的产品列表详情，请点 **Start**。
   此时会打开 **Product Information** 选项卡。
2. 输入所有基本产品详情并点 **Save**。

14.1.2. 容器化应用程序的完整公司配置集信息

1. 要完成您的公司概况信息，请单击 **Start**。输入所有详情后，单击 **Submit**。
2. 要修改现有的详情，请点 **Review**。此时会打开 **Account Details** 页面。
3. 检查和修改 Company 配置集信息，然后单击 **Submit**。

14.1.3. 接受容器化应用程序的法律协议

要发布您的产品镜像，请同意有关合作伙伴容器镜像的发布条款。

1. 要接受法律协议，请点击 **Start**。
2. 要预览或下载协议，请点 **Review**。

此时会显示 **Red Hat Partner Connect Container 附**录文档。阅读文档，了解与容器镜像分发相关的术语。

14.1.4. 为容器化应用程序添加至少一个产品组件

1. 点 **Start**。您将被重定向到 **Components** 选项卡。
   要添加新或现有产品组件，请点 **Add component**。
2. 用于添加新组件，

a. 在 **Component Name** 文本框中，输入组件名称。

b. **对于您要创建的独立组件，** 请选择您要认证的组件。例如，根据您的要求从以下选项中选择对容器进行认证：

i. 容器镜像

ii. RHEL 的容器化应用程序

iii. OpenStack 的容器化应用程序

c. 点击 **Next**。

d. 对于 **Red Hat Enterprise Linux 版本**，请选择认证您的组件的主要 RHEL 版本。

注意

创建产品列表后，您无法修改版本。

e. 单击 **Create new component**。

3. 要添加现有组件，请从 **Add 组件** 对话框中选择 **Existing Component**。

a. 从 **Available components** 列表中，搜索并选择您要认证的组件，然后点转发箭头。所选组件被添加到 Chose **n 组件** 列表中。

b. 单击 **Attach existing component**。

14.1.5. 为您的容器化应用程序列表认证组件

1. 要为您的列表认证组件，请单击 **Start**。如果您有现有的产品组件，您可以查看 **Attached 组件** 列表及其详情：

a. Name

b. 认证

c. 安全性

d. 类型

e. Created

f. 点击更多选项归档或删除组件

2. 选择用于认证的组件。

完成上述所有任务后，您将看到与所有选项相对应的绿色勾号标记。

Overview 选项卡还提供以下信息：

1. **产品联系人** - 提供产品营销和技术联系信息。

a. 点 **Add contacts to product** 以提供联系信息

b. 点 **Edit** 以更新信息。

2. **产品中的组件** - 提供附加到产品的组件列表及其最后的更新信息。

    a. 点 **Add components to product**将新的或现有组件添加到您的产品中。

    b. 点 **Edit components** 更新现有组件信息。

发布产品列表后，您可以查看您的产品 **就绪情况和 方式，以便在 Overview 选项卡上提高分数**。

14.2. 产品信息

通过此选项卡，您可以提供有关您产品的所有重要信息。产品详情会在红帽生态系统目录中与您的产品一起发布。

常规 标签页：

提供产品的基本详情，包括产品名称和描述。

1. 输入 **产品名称**。
2. 可选：根据 **定义的准则上传产品徽**标。
3. 输入 **Brief 描述** 和长 **描述**。
4. 点击 **Save**。

功能和好处 选项卡：

提供您产品的重要特性。

1. 可选：输入 **Title** 和 **Description**。
2. 可选： 要为您的产品添加额外的功能，请点 **+ Add new feature**。
3. 点击 **Save**。

快速启动和配置标签页 ：

添加指向任何快速入门指南或配置文档的链接，以帮助客户部署并开始使用您的产品。

1. 可选：输入 **Quick start 和 configuration instructions**。
2. 点击 **Save**。
3. 如果您不想显示它们，请选择 **Hide default instructions** 复选框。

链接的资源 标签页：

添加支持文档的链接，以帮助我们的客户使用您的产品。这些信息被映射到，并在产品目录页面中的 Documentation 部分显示。

注意

必须至少添加三个资源。如果可用，红帽建议您添加更多资源。

1. 选择 **Type** 下拉菜单，并输入资源的 **Title** 和 **Description**。

2. 输入 **资源 URL**。
3. 可选： 要为您的产品添加其他资源，请点 **+ Add new Resource**。
4. 点击 **Save**。

常见问题解答 标签页：

添加常见问题以及产品用途、操作、安装或其他属性详情的回答。您可以包括有关您的产品和服务的常见客户查询。

1. 输入问题 **和 answer**。
2. 可选： 要为您的产品添加额外的常见问题，请点 **+ Add new FAQ**。
3. 点击 **Save**。

支持 标签：

此选项卡可让您提供支持团队的联系信息。

1. 输入 **支持 描述、支持网站、支持电话号码 以及支持电子邮件地址**。
2. 点击 **Save**。

Contacts 标签页：

请提供营销和技术团队的联系信息。

1. 输入 **营销联系人电子邮件地址** 及 **技术联系电子邮件地址**。
2. 可选： 要添加其他联系人，请点 **+ Add another**。
3. 点击 **Save**。

法律 选项卡：

提供产品相关的许可证和策略信息。

1. 输入 **产品和隐私策略 URL** 的 **许可证协议 URL**。
2. 点击 **Save**。

SEO 标签页：

使用此选项卡提高我们相互客户的可发现性，提高红帽生态系统目录搜索和互联网搜索引擎中的可见性。提供更多搜索别名（密钥和证书对）会增加产品的可发现性。

1. 选择 **产品类别**。
2. 输入 **Key** 和 **Value** 来设置搜索别名。
3. 点击 **Save**。
4. 可选： 要添加额外的键值对，请点 **+ Add new key-value pair**。

注意

为您的产品至少添加一个搜索别名。如果可用，红帽建议您添加更多别名。

14.3. 容器的 COMPONENTS 标签页

使用此选项卡将组件添加到您的产品列表中。另外，您可以查看链接到您的产品列表的附加组件列表。

从以下选项中选择：

- 第 14.3.1 节 “容器镜像”
- 第 14.3.2 节 “RHEL 的容器化应用程序”
- 第 14.3.3 节 “OpenStack 的容器化应用程序”

另外，要将组件附加到产品列表，您可以在 Container、Operator 或 Helm Chart 产品列表的 **Overview** 选项卡中完成 **至少添加一个产品组件** 选项。

14.3.1. 容器镜像

1. 要添加新或现有产品组件，请点 **Add component**。
2. 若要添加新组件，请执行这些步骤，
   a. 在 **Component Name** 文本框中，输入组件名称。
   b. **对于您要创建的独立组件，** 请选择您要认证的组件。例如，对于认证容器，请选择 **Container Image**。
   c. 点击 **Next**。
   d. 在 **Create and Add**component 页面中，为组件选择首选的 OS Content-Type 和 Distribution Method：
      i. 对于容器 **使用什么基础镜像？**，请选择要用于您的组件的镜像类型：
         A. **Red Hat Universal Base Image**- 您可以通过 Red Hat Container registry 或其他第三方 registry 分发基于 UBI 的容器镜像。
         B. **Red Hat Enterprise Linux**- 您只能通过 Red Hat Container registry 分发基于 RHEL 的容器镜像。
      ii. 对于 **Select your preferred Distribution Method**，请选择用于分发容器镜像的容器 registry。客户将从此位置拉取您的容器镜像，并在您的容器镜像仍托管在您管理的 registry 中的所有方法中。红帽建议 Quay.io 托管您的镜像，但您可以使用任何与 Kubernetes 兼容的 registry。
         A. **Red Hat Container Registry**- 如果您希望红帽通过红帽的容器 registry 分发容器，请选择这个选项。选择 **I need Red Hat 来托管我的 registry**复选框。当您选择这个选项时，带有此分发方法的镜像托管在容器 registry 上，但通过 Red Hat registry 代理地址向客户分发。在不向配置中添加 registry 的情况下，客户可以访问您的容器，但不会了解代理中的特定于客户的下载指标或其他使用数据。
         B. **您自己的容器注册表** - 选择这个选项以在 registry 上发布您的认证容器。在使用您自己的第三方 registry 时，客户需要向 registry 进行身份验证，以拉取您的认证容器，并使用您的产品。在断开连接的环境中，客户必须将 registry 添加到红帽平台中，才

能安装您的认证容器。注意 - 红帽建议在 registry 上自助托管，因为您可以访问整个容器指标并完全控制您的产品访问权限。红帽建议将 Quay.io 用于此目的，但您可以使用任何与 Kubernetes 兼容的 registry。

e. 点 **Add Component**。

3. 要添加现有组件，请从 **Add 组件** 对话框中选择 **Existing Component**。

a. 从 **Available components** 列表中，搜索并选择您要认证的组件，然后点转发箭头。所选组件被添加到 Chose **n 组件** 列表中。

b. 单击 **Attach existing component**。

14.3.2. RHEL 的容器化应用程序

1. 要添加新或现有产品组件，请点 **Add component**。

2. 若要添加新组件，请执行这些步骤，

a. 在 **Component Name** 文本框中，输入组件名称。

b. **对于您要创建的独立组件，** 请选择您要认证的组件。例如，为 RHEL 选择 Containerized application。

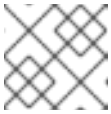
c. 点击 **Next**。

d. 在 **Create and Add component** 页面中，为组件选择首选的 RHEL 版本和分发方法：

i. 对于 **RHEL 的哪个主要版本将对您的镜像进行认证？**，请选择首选的 RHEL 版本：

A. 8

B. 9



注意

您无法在创建产品组件后修改版本。

ii. 对于 **分发方法**，请选择用于分发容器镜像的容器注册表。客户将从此位置拉取您的容器镜像，并在您的容器镜像仍托管在您管理的 registry 中的所有方法中。红帽建议 Quay.io 托管您的镜像，但您可以使用任何与 Kubernetes 兼容的 registry。

A. **Red Hat Container Registry**- 如果您希望红帽通过红帽的容器 registry 分发容器，请选择这个选项。选择 **I need Red Hat 来托管我的 registry** 复选框。当您选择这个选项时，带有此分发方法的镜像托管在容器 registry 上，但通过 Red Hat registry 代理地址分发到客户。在不向配置中添加 registry 的情况下，客户可以访问您的容器，但不会了解代理中的特定于客户的下载指标或其他使用数据。

B. **您自己的容器注册表** - 选择这个选项以在 registry 上发布您的认证容器。在使用您自己的第三方 registry 时，客户需要向 registry 进行身份验证以拉取您的认证容器并使用您的产品。在断开连接的环境中，客户必须将 registry 添加到红帽平台中，才能安装您的认证容器。注意 - 红帽建议在 registry 上自助托管，因为您可以整个容器指标并完全控制您的产品访问权限。红帽建议将 Quay.io 用于此目的，但您可以使用任何与 Kubernetes 兼容的 registry。

e. 点 **Add Component**。

3. 要添加现有组件，请从 **Add 组件** 对话框中选择 **Existing Component**。

   a. 从 **Available components** 列表中，搜索并选择您要认证的组件，然后点转发箭头。所选组件被添加到 Chose **n 组件** 列表中。

   b. 单击 **Attach existing component**。

14.3.3. OpenStack 的容器化应用程序

1. 要添加新或现有产品组件，请点 **Add component**。
2. 要添加新组件，在 **Component Name** 文本框中输入组件名称。

   a. **对于您要创建的独立组件，** 请选择您要认证的组件。例如，为 Red Hat OpenStack 平台认证容器化应用程序，请选择 **OpenStack 的容器化应用程序**。

   b. 对于 **OpenStack 的哪个主要版本，您将为您的镜像进行认证？** 默认情况下，启用版本 17。您无法修改此字段。

   c. 点 **Create new Component**。

3. 要添加现有组件，请从 **Add 组件** 对话框中选择 **Existing Component**。

   a. 从 **Available components** 列表中，搜索并选择您要认证的组件，然后点转发箭头。所选组件被添加到 Chose **n 组件** 列表中。

   b. 单击 **Attach existing component**。

注意

您可以将一个组件添加到多个产品列表中。所有附加的组件都必须发布，然后才能发布产品列表。

附加组件后，您可以查看 **Attached 组件** 列表及其详情：

i. Name

ii. 认证

iii. 安全性

iv. 类型

v. Created

vi. 点击更多选项归档或删除附加的组件

或者，要搜索特定组件，请在 **Search by component Name** 文本框中键入组件的名称。

14.4. 支持

红帽合作伙伴加速服务(PAD)是一个产品和技术级别合作伙伴帮助台服务，允许当前和潜在合作伙伴提供与红帽产品、合作伙伴认证、产品认证、服务流程等相关的非技术问题。

您还可以联系红帽合作伙伴加速服务，以了解您可能对认证可能遇到的任何技术问题。技术帮助请求将重定向到认证运营团队。

通过合作伙伴订阅计划，红帽提供免费的、不用于销售的软件订阅，您可用来在目标红帽平台上验证您的产品。要请求访问此计划，请按照 合作伙伴订阅 网站上的说明进行操作。

1. 要请求支持，请点击 Open a support case。请参阅 PAD - 如何打开和管理 PAD 问题单，以创建一个 PAD ticket。

2. 要查看现有支持问题单的列表，请点 **View 支持问题单**。

14.5. 删除产品

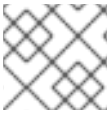
如果要删除产品列表后，请转到 **Overview** 选项卡，再单击 **Delete**。

先发布的产品必须取消发布，然后才能删除。即使删除该产品后，红帽仍然保留与已删除产品相关的信息。

第 15 章 添加认证组件

创建新产品列表后，为新创建的产品列表添加认证组件。

您可以为新添加的组件配置以下选项：



注意

组件配置因不同的产品类别而异。

- 第 15.1 节 “镜像”
- 第 15.2 节 “容器认证”
- 第 15.3 节 “安全性”
- 第 15.4 节 “仓库信息”
- 第 15.5 节 “组件详情”
- 第 6.3 节 “联系信息”
- 第 15.7 节 “容器的相关产品”

要配置选项，请转至 **Components** 选项卡，然后点任何现有组件。

15.1. 镜像

Images 选项卡提供您使用 preflight 工具提交的容器镜像的测试结果。您必须配置 preflight 并推送容器镜像来查看测试结果。

- 要推送容器镜像，请点击 **Set up Preflight**。
- 有关认证测试的详细信息，请参阅 运行认证测试套件。

测试完成后，您可以看到两类镜像：

- **清单 Digests** - 表示可用于多个架构的容器镜像。
- **独立容器镜像** - 表示仅适用于单一架构的容器镜像。

本页提供以下容器镜像详情：

- 特定镜像 ID 或 SHA ID
- 镜像标签
- 认证 - 认证或未认证，根据执行的检查通过或失败状态。单击它以获取更多详细信息。
- 架构 - 镜像的特定架构（如果适用）。
- 安全 - 检查任何漏洞（如果有）。
- Health Index - Container Health Index 是容器镜像可用的最旧、最严重安全更新的测量结果。'a' 比 'F' 更最新。如需了解更多详细信息，请参阅 Red Hat Container Catalog 内部使用的容器健康状态索引等级。

- created - 您提交认证的日期。
- 点击 Actions 菜单执行以下任务：
  - Delete Image - 在镜像未发布时点此选项删除您的容器镜像。
  - 同步标签 - 当您更改镜像标签时，请使用此选项同步 Red Hat Partner Connect 和 Red Hat Container Catalog 上可用的容器镜像信息。
  - Catalog 中的查看 - 当您的容器镜像发布后，点此选项查看 红帽生态系统 容器目录上发布的容器镜像。
- 单击 **Publish**，以发布您的认证容器镜像。

15.2. 容器认证

15.2.1. 对于容器镜像

认证选项卡提供有关出口控制问题、为附加容器镜像执行的所有认证测试的详细信息，以及用于提交容器镜像以进行认证的方法。

- 出口控制问题
  出口控制问卷 包含一系列问题，红帽法律团队会评估第三方供应商的导出合规性。合作伙伴的法律代表必须审查并回答问题。红帽需要大约五个工作日来评估响应，并根据红帽批准合作伙伴或延迟决策或请求更多信息。

  1. 点 **Start questionnaire**，以输入有关您的产品的所有法律信息。
  2. 点 **Review** 修改现有的详情。

注意

如果您使用 通用基础镜像(UBI)的版本 来构建容器镜像，您可以在私有存储库中托管您的镜像。这可让您跳过 Export Compliance questionnaire。只有在 Red Hat Container Catalog 上托管您的镜像时，才需要此表单。

- 认证测试
  它提供为附加容器镜像执行的 **Manifest Digests** 认证测试或独立认证测试的状态，其中包括以下详情：
  - **results - 与结果一起运行的测试总数。单击它以获取更多详细信息。**
  - **Image - 特定镜像 ID 或 SHA ID**
  - **最后活动 - 运行测试前的天数**
- **提交您的容器镜像进行验证**
  - **在容器镜像上运行认证套件。请参阅 运行认证测试套件。**
  - **上传测试结果。之后您可以在 Images 标签页中看到测试结果。**
  - **在红帽目录中发布容器镜像认证。请参阅在红帽生态系统目录上发布认证容器。**

注意

此步骤仅认证您的容器。使用 Certifications 选项卡认证功能。

15.2.2. 对于 RHEL 上的容器化应用程序

- **出口控制问题**
  出口控制问卷 包含一系列问题，红帽法律团队会评估第三方供应商的导出合规性。合作伙伴的法律代表必须审查并回答问题。红帽需要大约五个工作日来评估响应，并根据红帽批准合作伙伴或延迟决策或请求更多信息。

  1. 点 Start questionnaire，以输入有关您的产品的所有法律信息。
  2. 点 Review 修改现有的详情。

注意

如果您使用 通用基础镜像(UBI)的版本 来构建容器镜像，您可以在私有存储库中托管您的镜像。这可让您跳过 Export Compliance questionnaire。只有在 Red Hat Container Catalog 上托管您的镜像时，才需要此表单。

- **在 Red Hat Enterprise Linux 中验证您的产品的功能**
  使用认证选项卡验证您的 Red Hat Enterprise Linux 上产品的功能。您可以执行以下功能：
  - 在本地运行红帽认证工具
  - 下载测试计划
  - 与红帽认证团队分享测试结果。
  - 如果需要，与认证团队进行交互。
    要验证产品的功能，请执行以下步骤：
    - 如果您是新合作伙伴，请点击 Request a partner subscription。批准您的请求后，您将获得添加到您帐户的有效订阅。
    - 当您有有效的合作伙伴订阅后，单击 Start Certification，然后单击 Go to Red Hat Certification 工具。
      在 红帽认证门户上创建一个新的认证 案例，您会被重定向到相应的认证门户页面。

      认证团队将与您联系以开始认证测试流程，并在出现问题时遵循您的操作。验证成功后，会显示带有 validate complete 消息的绿色勾号。

      要查看验证的产品详情，请点 Review。
- **提交您的容器镜像进行验证**
  - 在容器镜像上运行认证套件。请参阅 运行认证测试套件。
  - 上传测试结果。
    之后您可以在 Images 标签页中看到测试结果。
  - 在红帽目录中发布容器镜像认证。请参阅在红帽生态系统目录上发布认证容器。

注意

此步骤仅认证您的容器。使用 Certifications 选项卡认证功能。

15.2.3. 用于 OpenStack 的容器化应用程序

认证选项卡提供有关出口控制问题以及提交容器镜像以进行认证的方法的详细信息。

- 出口控制问题
  出口控制问卷 包含一系列问题，红帽法律团队会评估第三方供应商的导出合规性。合作伙伴的法律代表必须审查并回答问题。红帽需要大约五个工作日来评估响应，并根据红帽批准合作伙伴或延迟决策或请求更多信息。

  1. 点 Start questionnaire，以输入有关您的产品的所有法律信息。
  2. 点 Review 修改现有的详情。

注意

如果您使用 通用基础镜像(UBI)的版本 来构建容器镜像，您可以在私有存储库中托管您的镜像。这可让您跳过 Export Compliance questionnaire。只有在 Red Hat Container Catalog 上托管您的镜像时，才需要此表单。

- 提交您的容器镜像进行验证
  - 在容器镜像上运行认证套件。请参阅 运行认证测试套件。
  - 上传测试结果。之后您可以在 Images 标签页中看到测试结果。
  - 在红帽目录中发布容器镜像认证。请参阅在红帽生态系统目录上发布认证容器。

注意

此步骤仅认证您的容器。使用 Certifications 选项卡认证功能。

15.3. 安全性

security 选项卡提供附加产品组件的健康状况。红帽使用 Health Index 来识别红帽通过 红帽生态系统目录 提供的组件的安全风险。

Health Index 是一个对容器镜像可用的最旧、最严重安全更新的测量。等级为 'A' 的镜像比一个等级为 'F。如需了解更多信息，请参阅 Red Hat Container Catalog 内部使用的 Container Health Index grades。

此选项卡提供镜像的健康状况索引，其中包括以下详情：

- 镜像 ID
- 健康索引

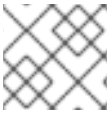
15.4. 仓库信息

您可以使用 Repository information 选项卡配置 registry 和存储库详情。

在以下字段中输入所需详情：

字段名称	描述
容器 registry 命名空间	创建容器时设置的 registry 名称。当容器发布时，此字段变得不可编辑。
出站存储库名称	您选择的存储库名称，或者从托管您的镜像的私有 registry 获取的名称，如 ubi-minimal。
仓库概述	从容器镜像中获取的存储库摘要。
仓库描述	从容器镜像中获取的存储库描述。
用户在 Red Hat Container Catalog 上获取您公司镜像的说明	提供您希望用户在获取容器镜像时遵循的具体说明。此字段仅适用于容器镜像。

配置所有必需字段后，单击 **Save。**



注意

所有标有星号 * 的字段都是必需的，您必须先完成，然后才能继续容器认证。

15.5. 组件详情

使用此选项卡配置产品组件详情。

在以下字段中输入所需详情：

字段名称	描述
镜像类型	为您的产品组件选择对应的镜像类型。 • **Operator 镜像** - 如果要部署管理其他镜像的 Operator，请选择此类型。 • **独立镜像** - 如果您希望镜像由您的产品或用户部署，请选择此类型。 • **组件镜像** - 如果您希望镜像由您的产品部署，而不是由用户部署，请选择此类型。
应用程序类别	选择您的软件产品相应的应用程序类型。

字段名称	描述
主机级别访问	在两个选项之间进行选择： • **unprivileged** - 如果您的容器与主机分离。 或者 • **privileged** - 如果您的容器需要特殊的主机级别特权。  **注意** 如果您的产品功能需要 root 访问权限，则必须在运行 preflight 工具前选择 **privileged** 选项。这个设置可能由红帽审核。
发行版本类别	在两个选项之间进行选择： • **正式发布** - 当您选择这个选项时，应用程序已正式发布并被支持。 或者 • **beta** - 当您选择这个选项时，应用程序会作为预发布候选版本提供。
项目名称	用于内部目的的项目名称。
自动发布	当您启用这个选项时，容器镜像会在通过所有认证测试后会在 Red Hat Container Catalog 上自动发布。
Red Hat Enterprise Linux 版本	它表示您要在其上认证容器化应用程序的 RHEL 版本。  **注意** 此字段不可编辑，仅适用于 RHEL 上的容器化应用程序。
Red Hat OpenStack platform	它表示您要在其上认证容器化应用程序的 OpenStack 平台版本。  **注意** 此字段不可编辑，仅适用于 Red Hat OpenStack 平台上的容器化应用程序。

15.6. 联系信息

注意

为这个选项卡提供信息是可选的。

在 联系人信息 选项卡中，输入您的产品组件的主要技术联系人详细信息。

1. 可选：在 技术联系电子邮件地址 字段中，输入镜像维护人员的电子邮件地址。
2. 可选： 要为您的组件添加额外的联系人，请点 + Add new contact。
3. 点击 Save。

15.7. 容器的相关产品

相关产品选项卡提供与您的产品组件关联的产品列表以及以下信息：

- 产品名称
- 类型
- visibility - 发布或未发布
- 最后活动 - 运行测试前的天数

要在组件中添加产品，请执行以下操作：

- 如果要按名称查找产品，请在 Search by name 文本框中输入产品名称，然后点击搜索图标。
- 如果您不确定产品名称，请单击 Find a product。在 Add product 对话框中，从 Available products 列表中选择所需的产品，然后点转发箭头。所选产品被添加到 Chosen 产品列表中。单击 Update attached products。添加的产品列在相关的产品列表中。

注意

所有标有星号 * 的字段都是必需的，您必须先完成，然后才能继续认证。

第 16 章 运行认证测试套件

按照说明运行认证测试套件：

先决条件

- 您有一个 Red Hat Enterprise Linux (RHEL)系统。
- 您可以使用 Podman 登录您的镜像 registry。例如：

```
$ podman login --username <your_username> --password <your_password> --authfile
./temp-authfile.json <registry>
```

在以下步骤中，需要使用 --authfile ./temp-authfile.json 选项生成的身份验证文件。当您使用 Preflight 工具提交测试结果时，--docker-config 选项会使用这个身份验证文件。

- 您已在 Red Hat Partner Connect 门户上设置容器。产品列表必须至少正在进行中。
- 您有一个 pyxis API 密钥。

流程

1. 使用 Podman 构建容器镜像。

注意

使用 Podman 构建容器镜像是可选的。

2. 将容器上传到您选择的任何私有或公共 registry。
3. 下载最新的 Preflight 认证实用程序。
4. 执行以下步骤验证正在认证的容器的功能：
   a. 运行 Preflight 认证工具：

```
$ preflight check container \
registry.example.org/<namespace>/<image_name>:<image_tag>
```

   b. 检查日志信息并根据需要更改容器。如需更多信息，请参阅故障排除信息页面。如果发现任何问题，可以 提交支持问题单 或运行以下命令：

```
$ preflight support
```

红帽欢迎社区贡献。如果您遇到与 Preflight 或 Red Hat Partner Connect Portal 相关的错误，或者对功能改进或贡献有建议，请报告问题。在报告问题前，请确保查看打开的问题以避免重复。

   c. 运行容器认证实用程序并进行更改，直到所有测试都通过。
5. 运行以下命令来提交认证测试结果：

```
$ preflight check container \
registry.example.org/<namespace>/<image_name>:<image_tag> \
--submit \
```

```
--pyxis-api-token=<api_token> \
--certification-project-id=<project_id> \
--docker-config=./temp-authfile.json
```

将测试结果提交至红帽合作伙伴连接门户后，红帽将扫描容器的层以了解软件包漏洞。

6. 通过进入到 Red Hat Partner Connect 门户中的*Images* 选项卡，查看认证组件 UI 中的认证和漏洞测试结果。

其他资源

如果您要认证 RHEL 应用程序，请按照 非容器认证工作流 验证产品的功能。

您还可以使用红帽认证的工具（具有内置 pre-flight 工具）认证 RHEL 应用程序容器，从而可让您验证容器。

流程

按照以下步骤使用内置的 preflight 工具：

1. 安装 preflight 软件包：
   # dnf install redhat-certification-preflight

2. 运行 rhcert 并按照说明进行操作：
   # rhcert-run

3. 查看并保存测试结果：
   # rhcert-save

第 17 章 在红帽生态系统目录中发布经过认证的容器

在 合作伙伴连接门户上 从 preflight 工具提交测试结果后，会针对漏洞扫描您的容器镜像。扫描成功完成后，将为您的镜像启用发布按钮。点击发布按钮后，您的镜像将在 红帽生态系统目录 上提供。

重要

Red Hat 软件认证不会在其功能或所选平台上执行对合作伙伴的产品进行测试。认证候选产品质量保证的所有方面均保留合作伙伴的职责。

部分 III. OPERATOR 认证

第 18 章 使用 OPERATOR

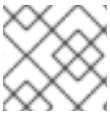
注意

在进行 Red Hat Operator 认证前，将您的 Operator 镜像或必要的容器镜像作为组件认证。在开始认证 Operator 捆绑包前，Operator Bundle 中引用的所有容器都必须经过红帽生态系统目录中认证并发布。

18.1. OPERATOR 简介

Kubernetes 操作器是打包、部署和管理 Kubernetes 应用程序的方法。我们的 Operator 认证计划确保合作伙伴的 Operator Operator 由 OpenShift 平台上的 Operator Lifecycle Manager (OLM)可部署，并使用红帽认证的容器镜像正确格式化。

18.2. OPERATOR 的认证工作流



注意

红帽建议您在开始认证过程前具有红帽认证工程师或具有同等经验。

任务摘要

认证工作流包括三个主要步骤：

1. 第 18.2.1 节 “Operator 板认证”
2. 第 18.2.2 节 “Operator 的认证测试”
3. 第 18.2.3 节 “在红帽生态系统目录中发布经过认证的 Operator”

18.2.1. Operator 板认证

执行认证加入概述的步骤：

1. 加入 Red Hat Connect for Technology Program （ Red Hat Connect for Technology Program (Red Hat Connect for Technology Program)
2. 同意计划条款和条件。
3. 选择所需产品类别来创建您的产品列表。您可以从可用产品类别中选择：
   a. 容器化应用程序
   b. 独立应用程序
   c. OpenStack Infrastructure
4. 填写您的公司简介。
5. 将组件添加到产品列表中。
6. 为您的产品列表认证组件。

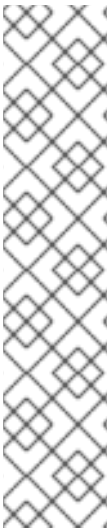
其他资源

有关创建第一个产品列表的详细信息，请参阅创建产品。

18.2.2. Operator 的认证测试

要运行认证测试：

1. 派生红帽上游存储库。
2. 在测试环境中安装并运行红帽认证管道。
3. 检查测试结果并进行故障排除（若有问题）。
4. 通过拉取请求向红帽提交认证结果。
5. 如果您希望红帽运行所有测试，请创建一个拉取请求。这会触发认证托管管道，以便在红帽基础架构上运行所有认证检查。



注意

有些 Operator 版本可能会从目录中消失，当图形被自动修剪时会出现这种情况，从而导致一些 Operator 版本不包括在更新图中。因此，当 Operator 捆绑包生成少于之前发行版本的频道时，您将被阻止发布 Operator 捆绑包。

如果要有意修剪图形，您可以使用拉取请求中的以下命令跳过测试并重启管道：

/test skip <test_case_name>	将跳过 test_case_name test。请注意，只能跳过测试的子集。
/pipeline restart certified-hosted-pipeline	托管的管道将重新触发。

其他资源

有关认证测试的详细信息，请参阅 运行认证测试套件。

18.2.3. 在红帽生态系统目录中发布经过认证的 Operator

完成所有认证检查后，您可以向红帽提交测试结果。您可以根据您的个人目标打开或关闭此结果提交步骤。提交测试结果后，它会触发红帽基础架构来自动合并拉取请求并发布您的 Operator。

其他资源

如需有关 Operator 的更多详细信息，请参阅：

- Operator
- Operator Framework
- Operator 能力级别
- 使用 Kubernetes Operator 打包应用程序和服务

第 19 章 创建产品

产品列表提供营销和技术信息，向潜在客户展示您的产品功能和优势。它将为产品添加所有必要组件以进行认证的基础。

先决条件

除了特定认证测试要求外，还验证您的产品在红帽平台上的功能。如果在目标红帽平台上运行您的产品产生了子标准体验，则必须在认证前解决问题。

在创建 operator 捆绑包前，将您的 Operator 镜像或必要的容器镜像作为容器应用程序组件认证。

流程

红帽建议完成列表选项卡中的所有可选字段，以获取全面的产品列表。如需更多信息，可以帮助相互客户做出明智的选择。

在为您的产品列表输入信息时，红帽鼓励与您的产品经理、营销代表或其他产品专家合作。

带有星号 packagemanifests 的字段是必需的。

流程

1. 登录到 Red Hat Partner Connect Portal。
2. 进入认证技术门户选项卡，然后单击门户。
3. 在标题栏中，单击 产品管理。
4. 从 Listing and Certification 选项卡中，单击 Manage products。
5. 在 My Products 页面中，单击 Create Product。
   此时会打开 Create New Product 对话框。
6. 输入 产品名称。
7. 从 您要认证的产品中选择 所需的产品类别，然后单击 Create product。例如，选择 Containerized Application 来创建容器化产品列表。
   此时会打开带有您的 产品名称的新页面。它由以下标签页组成：

   - 第 5.1 节 “概述”
   - 第 5.2 节 “产品信息”
   - 第 5.3 节 “组件”
   - 第 5.4 节 “支持”

   除了以下选项卡外，页面标头还提供 产品分数 详细信息。产品分数评估您的产品信息并显示分数。它可以是：

   - 公平
   - 良好
   - 非常好

- best

8. 点 How do improve my score?以改进您的产品分数。
9. 提供产品列表详情后，请单击 Save，然后移至下一部分。

19.1. 概述

此选项卡由一系列任务组成，您必须完成才能发布您的产品：

- 第 19.1.1 节 “Operator 的完整产品列表详情”
- 第 19.1.2 节 “Operator 的完整公司配置集信息”
- 第 19.1.3 节 “接受 Operator 的法律协议”
- 第 19.1.4 节 “为 Operator 添加至少一个产品组件”
- 第 19.1.5 节 “为您的 Operator 列表认证组件”

19.1.1. Operator 的完整产品列表详情

1. 要完成您的产品列表详情，请点 Start。
   此时会打开 Product Information 选项卡。
2. 输入所有基本产品详情并点 Save。

19.1.2. Operator 的完整公司配置集信息

1. 要完成您的公司概况信息，请单击 Start。输入所有详情后，单击 Submit。
2. 要修改现有的详情，请点 Review。此时会打开 Account Details 页面。
3. 检查和修改 Company 配置集信息，然后单击 Submit。

19.1.3. 接受 Operator 的法律协议

要发布您的产品镜像，请同意有关合作伙伴容器镜像的发布条款。

1. 要接受法律协议，请点击 Start。
2. 要预览或下载协议，请点 Review。

此时会显示 Red Hat Partner Connect Container 附录文档。阅读文档，了解与容器镜像分发相关的术语。

19.1.4. 为 Operator 添加至少一个产品组件

1. 点 Start。您将被重定向到 Components 选项卡。
   要添加新或现有产品组件，请点 Add component。
2. 用于添加新组件，
   a. 在 Component Name 文本框中，输入组件名称。

b. 对于您要创建的 OpenShift 组件，请选择您要认证的组件。例如，对于认证您的 Operator，请选择 Operator Bundle。

c. 点击 Next。

d. 专业认证 - 此功能允许您认证专门的 operator。

i. 如果要认证一个专用的 operator. ...Select the required operator，选择 My operator 是一个 CNI 或 CSI 复选框：

A. Container Network Interface (CNI)

B. 云存储接口(CSI)

e. 发行选项 - 为发布 Operator 选择以下选项之一：

i. 仅限 Web 目录(catalog.redhat.com) - Operator 发布到 Red Hat Container Catalog，在 Red Hat OpenShift OperatorHub 中不可见。当您创建新的操作器组件时，此选项适用于不想在 OpenShift 中可公开安装其操作员但需要验证认证的合作伙伴。只有在您有一个未满足 OpenShift In-product Catalog （认证）选项中的发布、权利或其他业务要求时，才选择此选项。

ii. OpenShift In-product Catalog (Certified) - Operator 在 Red Hat Container Catalog 上列出，并发布到 OpenShift OperatorHub 中的认证 operator 索引。

f. 单击 Add component。

3. 要添加现有组件，请从 Add 组件 对话框中选择 Existing Component。

a. 从 Available components 列表中，搜索并选择您要认证的组件，然后点转发箭头。所选组件被添加到 Chose n 组件 列表中。

b. 单击 Attach existing component。

19.1.5. 为您的 Operator 列表认证组件

1. 要为您的列表认证组件，请单击 Start。如果您有现有的产品组件，您可以查看 Attached 组件 列表及其详情：

a. Name

b. 认证

c. 安全性

d. 类型

e. Created

f. 点击更多选项归档或删除组件

2. 选择用于认证的组件。

完成上述所有任务后，您将看到与所有选项相对应的绿色勾号标记。

Overview 选项卡还提供以下信息：

1. 产品联系人 - 提供产品营销和技术联系信息。

a. 点 Add contacts to product以提供联系信息

b. 点 Edit 以更新信息。

2. 产品中的组件 - 提供附加到产品的组件列表及其最后的更新信息。

a. 点 Add components to product将新的或现有组件添加到您的产品中。

b. 点 Edit components 更新现有组件信息。

发布产品列表后，您可以查看您的产品 就绪情况和 方式，以便在 Overview 选项卡上提高分数。

19.2. 产品信息

通过此选项卡，您可以提供有关您产品的所有重要信息。产品详情会在红帽生态系统目录中与您的产品一起发布。

常规 标签页：

提供产品的基本详情，包括产品名称和描述。

1. 输入 产品名称。
2. 可选：根据 定义的准则上传产品徽标。
3. 输入 Brief 描述 和长 描述。
4. 点击 Save。

功能和好处 选项卡：

提供您产品的重要特性。

1. 可选：输入 Title 和 Description。
2. 可选： 要为您的产品添加额外的功能，请点 + Add new feature。
3. 点击 Save。

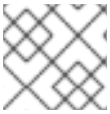
快速启动和配置标签页 ：

添加指向任何快速入门指南或配置文档的链接，以帮助客户部署并开始使用您的产品。

1. 可选：输入 Quick start 和 configuration instructions。
2. 点击 Save。
3. 如果您不想显示它们，请选择 Hide default instructions复选框。

链接的资源 标签页：

添加支持文档的链接，以帮助我们的客户使用您的产品。这些信息被映射到，并在产品目录页面中的 Documentation 部分显示。



注意

必须至少添加三个资源。如果可用，红帽建议您添加更多资源。

1. 选择 Type 下拉菜单，并输入资源的 Title 和 Description。
2. 输入 资源 URL。
3. 可选： 要为您的产品添加其他资源，请点 + Add new Resource。
4. 点击 Save。

常见问题解答 标签页：

添加常见问题以及产品用途、操作、安装或其他属性详情的回答。您可以包括有关您的产品和服务的常见客户查询。

1. 输入问题 和 answer。
2. 可选： 要为您的产品添加额外的常见问题，请点 + Add new FAQ。
3. 点击 Save。

支持 标签：

此选项卡可让您提供支持团队的联系信息。

1. 输入 支持 描述、支持网站、支持电话号码 以及支持电子邮件地址。
2. 点击 Save。

Contacts 标签页：

请提供营销和技术团队的联系信息。

1. 输入 营销联系人电子邮件地址 及 技术联系电子邮件地址。
2. 可选： 要添加其他联系人，请点 + Add another。
3. 点击 Save。

法律 选项卡：

提供产品相关的许可证和策略信息。

1. 输入 产品和隐私策略 URL 的 许可证协议 URL。
2. 点击 Save。

SEO 标签页：

使用此选项卡提高我们相互客户的可发现性，提高红帽生态系统目录搜索和互联网搜索引擎中的可见性。提供更多搜索别名（密钥和证书对）会增加产品的可发现性。

1. 选择 产品类别。
2. 输入 Key 和 Value 来设置搜索别名。
3. 点击 Save。
4. 可选： 要添加额外的键值对，请点 + Add new key-value pair。

注意

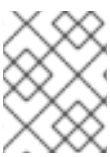
为您的产品至少添加一个搜索别名。如果可用，红帽建议您添加更多别名。

19.3. 组件

使用此选项卡将组件添加到您的产品列表中。通过此选项卡，您还可以查看链接到您的产品列表的附加组件列表。

另外，要将组件附加到产品列表，您可以完成 Container、Operator 或 Helm Chart 产品列表的 Overview 选项卡中提供的 Add least one product component选项。

1. 要添加新或现有产品组件，请点 Add component。
2. 用于添加新组件，
   a. 在 Component Name 文本框中，输入组件名称。
   b. 对于您要创建的 OpenShift 组件，请选择您要认证的组件。例如，要认证您的 Operator，请选择 Operator Bundle。
   c. 点击 Next。
   d. 专业认证 - 此功能允许您认证专门的 operator。
      i. 如果要认证专用操作器，选择 My operator 是一个 CNI 或 CSI复选框。
      ii. 选择所需的 Operator：
         A. Container Network Interface (CNI)
         B. 云存储接口(CSI)
   e. 发行选项 - 为发布 Operator 选择以下选项之一：
      A. 仅限 Web 目录(catalog.redhat.com)- Operator 已发布到 Red Hat Container Catalog，但无法在 Red Hat OpenShift OperatorHub 上可见。当您创建新 Operator 捆绑包组件时，这是默认选项。
      B. OpenShift In-product Catalog (Certified) - Operator 在Red Hat Container Catalog 上列出，并发布到 OpenShift OperatorHub 中的认证 operator 索引。这个选项可让客户在 OpenShift UI 中直接从 OperatorHub 安装 Operator。
   f. 点 Add Component。
3. 要添加现有组件，请从 Add 组件 对话框中选择 Existing Component。
   a. 从 Available components 列表中，搜索并选择要添加的组件，然后点转发箭头。所选组件被添加到 Chose n 组件 列表中。
   b. 单击 Attach existing component。



注意

您可以将同一组件添加到多个产品列表中。所有附加的组件都必须发布，然后才能发布产品列表。

附加组件后，您可以查看 Attached 组件 列表及其详情：

i. Name

ii. 认证

iii. 安全性

iv. 类型

v. Created

vi. 点击更多选项归档或删除附加的组件

或者，要搜索特定组件，请在 Search by component Name 文本框中键入组件的名称。

19.4. 支持

红帽合作伙伴加速服务(PAD)是一个产品和技术级别合作伙伴帮助台服务，允许当前和潜在合作伙伴提供与红帽产品、合作伙伴认证、产品认证、服务流程等相关的非技术问题。

您还可以联系红帽合作伙伴加速服务，以了解您可能对认证可能遇到的任何技术问题。技术帮助请求将重定向到认证运营团队。

通过合作伙伴订阅计划，红帽提供免费的、不用于销售的软件订阅，您可用来在目标红帽平台上验证您的产品。要请求访问此计划，请按照 合作伙伴订阅 网站上的说明进行操作。

1. 要请求支持，请点击 Open a support case。请参阅 PAD - 如何打开和管理 PAD 问题单，以创建一个 PAD ticket。

2. 要查看现有支持问题单的列表，请点 View 支持问题单。

19.5. 删除产品

如果要删除产品列表后，请转到 Overview 选项卡，再单击 Delete。

先发布的产品必须取消发布，然后才能删除。即使删除该产品后，红帽仍然保留与已删除产品相关的信息。

第 20 章 添加认证组件

创建新产品列表后，为新创建的产品列表添加认证组件。

您可以为新添加的组件配置以下选项：

注意

组件配置因不同的产品类别而异。

- 第 20.1 节 “Operator 的认证”
- 第 20.2 节 “Operator 的可选资格”
- 第 20.3 节 “Operator 的存储库信息”
- 第 20.4 节 “Operator 的组件详情”
- 第 20.5 节 “Operator 的联系信息”
- 第 20.6 节 “Operator 的相关产品”
- 第 20.7 节 “更新 Graph”

要配置选项，请转至 Components 选项卡，然后点任何现有组件。

20.1. OPERATOR 的认证

- 验证 Red Hat OpenShift 中 CNI 或 CSI 的功能

  注意

  此功能仅适用于 CNI 和 CSI operator。

  此功能允许您在本地运行认证测试，并使用红帽认证团队共享测试结果。

  验证专用 CNI 或 CSI Operator 的功能：

  1. 点 Go to Red Hat Certification 工具，在红帽认证门户上创建一个新的认证案例，之后您会被重定向到相应的门户页面。
  2. 在 Summary 选项卡中，进入 Files 部分并点击 Upload， 以上传您的测试结果。
  3. 在 Discussions 部分添加所有相关注释，然后点 添加注释。
     红帽将检查您提交的结果文件并验证您的专用 CNI 或 CSI operator。验证成功后，您的 Operator 将被批准并发布。

     其他资源

     如需更多信息，请参阅 CNI 和 CSI 工作流。

- Operator 认证
  要运行 Operator 认证套件，请转至测试选项。它显示两个标签页，以确定如何测试和验证您的 Operator。

- 使用 OpenShift 本地测试，使用您选择的 OpenShift 集群进行测试和认证。这个选项允许您将提供的管道集成到您自己的工作流中，以便持续验证和访问全面的日志，以加快反馈循环。这是推荐的方法。如需更多信息，请参阅 在本地运行认证测试套件。
- 使用红帽托管的管道进行测试，此方法与 OpenShift 软件测试与认证分开。在您要认证的 OpenShift 版本中测试了 Operator 后，如果您不希望全面日志，或者没有准备好将其包含在您自己的工作流中，您可以使用这个方法。如需更多信息，请参阅使用红帽托管管道运行认证套件。
  比较认证测试选项

  长期以来，红帽建议使用"本地测试"选项（也称为 CI Pipeline）来测试 Operator。此方法允许您将测试合并到 CI/CD 工作流和开发过程中，从而确保您的产品在 OpenShift 平台上正常工作，并简化 Operator 的未来更新和重新认证。

  虽然最初了解方法和调试错误可能需要一些时间，但它是一个高级方法，并提供最佳和最快速的反馈。另一方面，红帽建议使用托管管道，在 Red Hat infrastructure 选项上运行用于多个用例，例如在紧急期限工作时，或者在没有足够的资源和时间来学习和使用工具。

  您可以将托管管道与 CI/local 管道同时一起使用，因为您学习了长期本地工具。
- 最新测试运行选项卡 提供最新的测试结果（若有）。
  认证表提供以下信息：
  - Operator 版本
  - Pull request
  - 测试于
  - 测试结果 - Pass 或 Fail
  - Created
- 单击 View all tests 以了解有关所有测试的详细信息。它有两个标签页：
  - 测试结果 - 显示所有认证测试摘要及其结果。
  - test Artifacts - 显示日志文件。

20.2. OPERATOR 的可选资格

注意

此选项卡仅适用于 Operator 和 Helm Chart 认证。

可选资格 选项卡提供了验证您的产品是否遵循红帽推荐的准则，以及在 Red Hat OpenShift 上部署工作负载的最佳实践。当您选择此选项卡时，会创建一个功能认证，您可以在其中提交红帽审核结果。在成功验证工作负载产品后，红帽生态系统目录中的 Meets 最佳实践 徽标将列为已认证。

其他资源

如需更多信息，请参阅 最佳实践。

20.3. OPERATOR 的存储库信息

您可以使用 Repository information选项卡配置 registry 和存储库详情。

在以下字段中输入所需详情：

字段名称	描述
容器 registry 命名空间	创建容器时设置的 registry 名称。当容器发布时，此字段变得不可编辑。
出站存储库名称	您选择的存储库名称，或者从托管您的镜像的私有 registry 获取的名称，如 *ubi-minimal*。
授权 GitHub 用户帐户	它表示允许代表您公司提交 operator 的 GitHub 用户。
OpenShift Object YAML	如果使用私有容器 registry，则使用此选项添加 docker *config.json secret*。
仓库概述	从容器镜像中获取的存储库摘要。
仓库描述	从容器镜像中获取的存储库描述。

配置所有必需字段后， 单击 **Save。**

注意

所有标有星号 * 的字段都是必需的，您必须先完成，然后才能继续容器认证。

20.4. OPERATOR 的组件详情

使用此选项卡配置产品组件详情。

在以下字段中输入所需详情：

字段名称	描述
镜像类型	默认选择 Operator 捆绑包。
应用程序类别	选择您的软件产品相应的应用程序类型。
项目名称	用于内部目的的项目名称。

配置所有必需字段后， 单击 **Save。**

20.5. OPERATOR 的联系信息

注意

为这个选项卡提供信息是可选的。

在 联系人信息 选项卡中，输入您的产品组件的主要技术联系人详细信息。

1. 可选：在 技术联系电子邮件地址 字段中，输入镜像维护人员的电子邮件地址。
2. 可选： 要为您的组件添加额外的联系人，请点 + Add new contact。
3. 点击 Save。

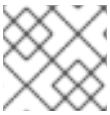
20.6. OPERATOR 的相关产品

相关产品选项卡提供与您的产品组件关联的产品列表以及以下信息：

- 产品名称
- 类型
- visibility - 发布或未发布
- 最后活动 - 运行测试前的天数

要在组件中添加产品，请执行以下操作：

- 如果要按名称查找产品，请在 Search by name 文本框中输入产品名称，然后点击搜索图标。
- 如果您不确定产品名称，请单击 Find a product。在 Add product 对话框中，从 Available products 列表中选择所需的产品，然后点转发箭头。所选产品被添加到 Chosen 产品列表中。单击 Update attached products。添加的产品列在相关的产品列表中。



注意

所有标有星号 * 的字段都是必需的，您必须先完成，然后才能继续认证。

20.7. 更新 GRAPH

通过此标签页为您的组件选择 OpenShift 产品版本和频道详情。

- 从 OpenShift Version 列表框中选择所需的版本。
- 从 Channel 列表中选择所需的频道。

Update graph 表提供以下信息：

- Version
- 更新路径
- 其他可用频道

有关升级的更多信息，请参阅标题下的 Operator 更新文档。

注意

所有标记为**星号 * 的字段都必**须**完成，然后才能**继续 Operator 捆绑包认证。

第 21 章 本地运行认证测试套件

通过选择此选项，您可以在您自己的 OpenShift 集群上运行认证工具。

注意

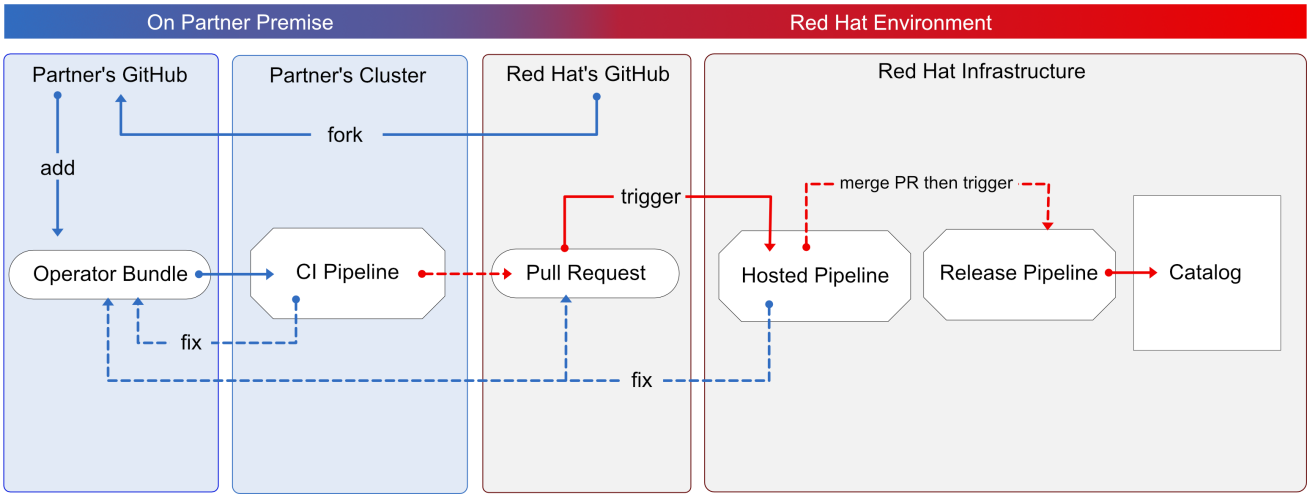
红帽建议您遵循此方法认证您的 Operator。

这个选项是合作伙伴的高级方法：

- 有兴趣将工具集成到自己的开发人员工作流中，以进行持续验证。
- 想要访问全面的日志以获得更快速的反馈循环，
- 或具有在默认 OpenShift 安装中没有的依赖项。

以下是该过程的概述：

图 21.1. 本地运行认证测试套件的概述



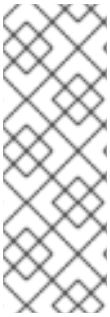
您可以使用基于 Tekton 的 OpenShift 管道来运行认证测试，从而实时查看全面的日志和调试信息。当您准备好认证并发布 Operator 捆绑包后，管道会代表您向 GitHub 提交拉取请求(PR)。如果一切都成功通过，您的 Operator 会自动合并并发布在 Red Hat Container Catalog 和 OpenShift 中的嵌入式 operatorHub 中。

按照说明在本地运行认证测试套件：

先决条件

要在 Red Hat OpenShift 测试环境中认证您的软件产品，请确保：

- 已安装 OpenShift 集群版本 4.8 或更高版本。



注意

OpenShift Operator Pipeline 为 5GB 卷创建一个持久性卷声明。如果您 在裸机上运行 OpenShift 集群，请确保配置了 动态卷置备。如果您没有配置动态卷置备，请考虑设置 本地卷。要防止 **Permission Denied** 错误，请使用以下命令修改本地卷存储路径以使用 **container_file_t** SELinux 标签：

```
chcon -Rv -t container_file_t "storage_path(/.*)?"
```

- 您有具有集群管理员特权的 admin 用户的 kubeconfig 文件。
- 您有一个有效的 operator 捆绑包。
- 已安装 OpenShift CLI 工具(oc)版本 4.7.13 或更高版本。
- 已安装 Git CLI 工具(git)版本 2.32.0 或更高版本。
- 已安装 Tekton CLI 工具(tkn)版本 0.19.1 或更高版本。

其他资源

有关计划先决条件，请参阅 Red Hat Openshift 认证先决条件。

21.1. 添加 OPERATOR 捆绑包

在 fork 的 operators 目录中，有一系列子目录。

21.1.1. 如果您在之前已认证了这个 operator -

在 operators 目录中为您的 Operator 找到对应的文件夹。将 Operator Bundle 的内容放在这个目录中。

注意

确保您的软件包名称与 Operator 的现有文件夹名称一致。

21.1.2. 如果您新认证这个 operator -

如果新认证 Operator 没有 Operator 的父目录下的子目录，则必须创建一个子目录。

在 operators 下创建新目录。这个目录的名称应与 Operator 的软件包名称匹配。例如，**my-operator**。

- 在这个 operator 目录中，使用 Operator 名称创建一个新子目录，如 < **my-operator>**，并为 < **V1.0** > 创建一个版本目录，并放置您的捆绑包。这些目录对于之前已通过认证的 operator 预加载。

```
├── operators
    └── my-operator
        └── v1.0
```

- 在 version 目录下，添加一个 **manifests** 文件夹，其中包含所有 OpenShift 清单，包括 **clusterserviceversion.yaml** 文件。

推荐的目录结构

以下示例演示了推荐的目录结构。

```
├── config.yaml
├── operators
│   └── my-operator
│       ├── v1.4.8
│       │   ├── manifests
│       │   │   ├── cache.example.com_my-operators.yaml
│       │   │   ├── my-operator-controller-manager-metrics-service_v1_service.yaml
│       │   │   ├── my-operator-manager-config_v1_configmap.yaml
│       │   │   ├── my-operator-metrics-reader_rbac.authorization.k8s.io_v1_clusterrole.yaml
│       │   │   └── my-operator.clusterserviceversion.yaml
│       │   └── metadata
│       │       └── annotations.yaml
│       └── ci.yaml
```

配置文件	描述
config.yaml	在这个文件中，包含 Operator 的组织。它可以是 **certified-operators**。例如，**机构： certified-operators**
ci.yaml	在此文件中，包括您的 Red Hat 技术合作伙伴项目 ID 和此 operator 的组织目标。 例如，**cert_project_id: <your partner project id>**。此文件存储成功认证流程所需的所有元数据。

配置文件	描述
annotations.yaml	在此文件中，包含 OpenShift 版本的注解，它引用 OpenShift 版本的范围。例如，**v4.8-v4.10** 表示 4.8 到 4.10 版本。将其添加到任何现有内容。 例如，NTT **：OpenShift 注解 com.redhat.openshift.versions: v4.8-v4.10。com.redhat.openshift.versions** 字段（作为 operator 捆绑包中的元数据的一部分）用于确定 Operator 是否包含在给定 OpenShift 版本的认证目录中。您必须使用它来指定 Operator 支持的一个或多个 OpenShift 版本。 请注意，在版本之前必须使用字母 'v'，且不允许使用空格。语法如下： ● 单一版本表示该 Operator 在 OpenShift 或更高版本上被支持。Operator 会自动添加到后续 OpenShift 版本的已认证目录中。 ● 前面带有 '=' 的单个版本表示 Operator 只在该特定版本的 OpenShift 上被支持。例如，使用 **=v4.8** 会将 Operator 添加到 OpenShift 4.8 认证的目录中，但不用于后续 OpenShift 版本。 ● 范围可用于指示仅支持该范围内的 OpenShift 版本。例如，使用 **v4.8-v4.10** 会将 Operator 添加到 OpenShift 4.8 到 4.10 的认证目录中，但不适用于 OpenShift 4.11 或 4.12。

其他资源

- **如需了解更多详细信息，请参阅管理 OpenShift 版本。**
- **如需 operator 捆绑包的示例，请参阅 此处。**

21.2. 分叉软件仓库

1. **登录 GitHub，再分叉红帽OpenShift 操作器上游存储库。**
2. **根据您要分发的 Catalogs，从下表派生适当的软件仓库：**

目录	上游存储库
认证目录	https://github.com/redhat-openshift-ecosystem/certified-operators

3. **克隆 fork 的 certified-operators 存储库。**
4. **将 Operator 捆绑包的内容添加到已分叉仓库中的 operators 目录中。**

如果要在多个目录中发布 Operator 捆绑包，您可以分叉每个目录并为每个分叉完成一次认证。

其他资源

有关在 GitHub 中创建分叉的更多信息，请参阅 Fork 仓库。

21.3. 安装 OPENSHIFT OPERATOR PIPELINE

先决条件

OpenShift 集群上的管理员特权。

流程

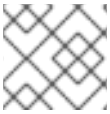
您可以通过两种方法安装 OpenShift Operator Pipeline：

- 自动化流程 （红帽推荐的流程）
- 手动过程

21.3.1. 自动化过程

红帽建议使用自动过程来安装 OpenShift Operator Pipeline。自动化过程可确保在执行 CI Pipeline 前正确配置了集群。此流程将 Operator 安装到集群中，可帮助您自动更新所有 CI Pipeline 任务，而无需手动干预。这个过程还支持多租户场景，您可以在其中在同一集群中迭代测试多个 operator。

按照以下步骤通过 Operator 安装 OpenShift Operator Pipeline：



注意

在安装 Operator Pipeline 前，保留 Operator 捆绑包的源文件。

21.3.1.1. 先决条件

在安装 OpenShift Operator Pipeline 之前，在终端窗口中运行以下命令配置所有先决条件：

注意

Operator 会监视所有命名空间。因此，如果其他命名空间中已存在 **secret/configs/etc**，您可以使用现有命名空间来安装 Operator Pipeline。

1. 新建命名空间：

```
oc new-project oco
```

2. 设置 **kubeconfig** 环境变量：

```
export KUBECONFIG=/path/to/your/cluster/kubeconfig
```

注意

此 **kubeconfig** 变量用于在测试并运行认证检查下部署 Operator。

```
oc create secret generic kubeconfig --from-file=kubeconfig=$KUBECONFIG
```

3. 执行以下命令提交认证结果：

   - 将 github API 令牌添加到创建拉取请求的存储库：

     ```
     oc create secret generic github-api-token --from-literal GITHUB_TOKEN=<github token>
     ```

   - 添加红帽容器 API 访问密钥：

     ```
     oc create secret generic pyxis-api-secret --from-literal pyxis_api_key=< API KEY >
     ```

     此 API 访问密钥与您的 Red Hat Partner Connect门户上的唯一合作伙伴帐户特别相关。

4. 在裸机上运行 OpenShift 集群的先决条件：

   a. 如果您在裸机上运行 OpenShift 集群，Operator 管道需要运行 5Gi 的持久性卷。以下 yaml 模板可帮助您使用本地存储创建 5Gi 的持久性卷。
   例如：

   ```
   apiVersion: v1
   kind: PersistentVolume
   metadata:
     name: my-local-pv
   spec:
     capacity:
       storage: 5Gi
     volumeMode: Filesystem
     accessModes:
       - ReadWriteOnce
     persistentVoumeReclaimPolicy: Delete
     local:
       path: /dev/vda4  ← use a path from your cluster
     nodeAffinity:
       required:
         nodeSelectorTerms:
           - matchExpressions:
             - key: kubernetes.io/hostname
               operator: In
               values:
                 - crc-8k6jw-master-0  ← use the name of one of your cluster's node
   ```

   b. CI 管道自动构建 Operator 捆绑包镜像和捆绑包镜像索引，以进行测试和验证。默认情况下，管道在集群的 OpenShift 容器注册表中创建镜像。
   要在裸机上使用此 registry，请在运行管道前设置内部镜像 registry。有关设置内部镜像 registry 的详细信息，请参阅镜像 registry 存储配置。

   如果要使用外部私有 registry，请通过添加 secret 来提供集群的访问凭证。具体步骤请参阅使用私有容器 registry。

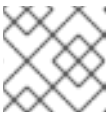
其他资源

- 有关获取 API 密钥的步骤，请参阅 获取 API 密钥。
- 如需额外的存储库配置，请参阅配置存储库以提交认证结果。

21.3.1.2. 通过 Operator 安装管道

按照以下步骤将 Operator 添加到集群中：

1. 安装 Operator 认证 Operator。
   - 登录您的 OpenShift 集群控制台。
   - 在主菜单中导航到 Operators → OperatorHub。
   - 在 All Items - Filter by keyword filter/search 框中键入 Operator Certification Operator。
   - 当显示时，选择 Operator Certification Operator 标题。此时会显示 Operator Certification Operator 页面。
   - 点 Install。此时会显示 Install Operator 网页。
   - 向下滚动并单击 Install。
   - 点 View Operator 来验证安装。
2. 为新安装的 Operator Pipeline 应用自定义资源。
   - 登录您的 OpenShift 集群控制台。
   - 在 Projects 下拉菜单中选择您要应用自定义资源的项目。
   - 展开 Operator Pipeline，然后点 Create instance。
     Create Operator Pipeline 屏幕会使用默认值自动填充。

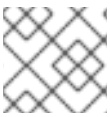
     注意

     如果您根据 先决条件 创建了所有资源名称，则不需要更改任何默认值。
   - 点 Create。

   自定义资源已创建，Operator 开始协调。

验证步骤

1. 检查自定义资源的条件。
   - 登录您的 OpenShift 集群控制台。
   - 进入到您新创建的 Operator Pipeline 自定义资源的项目，并点击 Custom Resource。
   - 向下滚动到 Conditions 部分，再检查所有 Status 值是否都设为 True。



注意

如果资源无法协调，请检查 Message 部分以识别后续步骤来修复错误。

2. 检查 Operator 日志。
   - 在终端窗口中运行以下命令：

```
oc get pods -n openshift-marketplace
```

- 记录 **certification-operator-controller-manager** pod 的完整 podman 名称并运行以下命令：

```
oc get logs -f -n openshift-marketplace <pod name> manager
```

- 检查 Operator 的协调是否发生。

其他资源

1. 卸载 Operator Pipeline 自定义资源：
   - 登录您的 OpenShift 集群控制台。
   - 进入到 Operator Certification Operator 主页，再点击您要卸载的 Operator Pipeline。
   - 点击 Custom Resource overflow 菜单并选择 Uninstall。
2. 卸载 Operator：
   - 登录您的 OpenShift 集群控制台。
   - 进入到 Operators → Installed Operators，再搜索您要卸载的 Operator。
   - 点相应 Operator 的 overflow 菜单并点 Uninstall Operator。

21.3.1.3. 执行管道

要执行管道，请确保在目录中的 templates 文件夹中有 **workspace-template.yml** 文件，从中要运行 **tkn** 命令。

要创建 **workspace-template.yml** 文件，在终端窗口中运行以下命令：

```
cat <<EOF> workspace-template.yml
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 5Gi
EOF
```

您可以通过 不同的方法 运行管道。

21.3.2. 手动过程

按照以下步骤手动安装 OpenShift Operator Pipeline：

21.3.2.1. 安装 OpenShift Pipeline Operator

1. 登录您的 OpenShift 集群控制台。
2. 在主菜单中导航到 Operators >OperatorHub。

3. 在 All Items - Filter by keyword filter/search 框中键入 OpenShift Pipelines。
4. 显示 Red Hat OpenShift Pipelines 标题时选择它。显示 Red Hat OpenShift Pipelines 页面。
5. 点 Install。此时会显示 Install Operator 网页。
6. 向下滚动并单击 Install。

21.3.2.2. 配置 OpenShift (oc) CLI 工具

用于配置对集群的访问的文件称为 kubeconfig 文件。这是引用配置文件的通用方法。使用 kubeconfig 文件组织集群、用户、命名空间和身份验证机制的信息。

kubectl 命令行工具使用 kubeconfig 文件来查找它选择集群所需的信息，并与集群的 API 服务器通信。

1. 在终端窗口中设置 KUBECONFIG 环境变量：

```
export KUBECONFIG=/path/to/your/cluster/kubeconfig
```

kubeconfig 文件将 Operator 部署到测试并运行认证检查。

其他资源

有关 kubeconfig 文件的更多信息，请参阅使用 kubeconfig 文件组织集群访问。

21.3.2.3. 创建 OpenShift 项目

创建一个新命名空间，以在管道中启动工作。

要创建命名空间，在终端窗口中运行以下命令：

```
oc adm new-project <my-project-name> # create the project
oc project <my-project-name> # switch into the project
```

重要

不要在 default 项目或命名空间中运行管道。红帽建议为管道创建一个新项目。

21.3.2.4. 添加 kubeconfig secret

创建包含 kubeconfig 的 kubernetes secret，以便向运行认证管道的集群进行身份验证。认证管道需要在 OpenShift 集群上执行 Operator 测试部署。

要添加 kubeconfig secret，在终端窗口中运行以下命令：

```
oc create secret generic kubeconfig --from-file=kubeconfig=$KUBECONFIG
```

其他资源

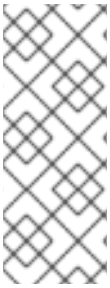
如需有关 kubeconfig secret 的更多信息，请参阅 Secret。

21.3.2.5. 从 Red Hat Catalog 导入 Operator

从红帽目录 导入 Operator。

在终端窗口中运行以下命令：

```
oc import-image certified-operator-index \
  --from=registry.redhat.io/redhat/certified-operator-index \
  --reference-policy local \
  --scheduled \
  --confirm \
  --all
```



注意

如果您在 IBM Power 集群中将 OpenShift 用于 ppc64le 架构，请运行以下命令以避免权限问题：

oc adm policy add-scc-to-user anyuid -z pipeline

此命令将 anyuid 安全性上下文约束(SCC)赋予默认的管道服务帐户。

21.3.2.6. 安装认证管道依赖项

在终端窗口中，使用以下命令在集群中安装认证管道依赖项：

```
$git clone https://github.com/redhat-openshift-ecosystem/operator-pipelines
$cd operator-pipelines
$oc apply -R -f ansible/roles/operator-pipeline/templates/openshift/pipelines
$oc apply -R -f ansible/roles/operator-pipeline/templates/openshift/tasks
```

21.3.2.7. 配置提交认证结果的存储库

在终端窗口中，运行以下命令来配置存储库以提交认证结果：

21.3.2.7.1. 添加 GitHub API 令牌

执行所有配置后，管道可以自动打开拉取请求，以将 Operator 提交到红帽。

要启用此功能，请添加 GitHub API Token，在运行管道时使用 **--param submit=true** ：

```
oc create secret generic github-api-token --from-literal GITHUB_TOKEN=<github token>
```

21.3.2.7.2. 添加 Red Hat Container API 访问密钥

添加您从红帽接收的特定容器 API 访问密钥：

```
oc create secret generic pyxis-api-secret --from-literal pyxis_api_key=< API KEY >
```

21.3.2.7.3. 启用摘要固定

注意

此步骤对于向红帽提交认证结果是必需的。

OpenShift Operator 管道可以自动将捆绑包中的所有镜像标签替换为镜像 Digest SHA。这允许管道确保是否使用所有镜像的固定版本。管道将捆绑包的固定版本作为新分支提交到 GitHub 存储库。

要启用此功能，请添加一个能够作为 secret 访问 GitHub 的私钥。

1. 使用 Base64 对可访问包含捆绑包的 GitHub 存储库的私钥进行编码。

```
base64 /path/to/private/key
```

2. 创建包含 base64 编码的私钥的 secret。

```
cat << EOF > ssh-secret.yml
kind: Secret
apiVersion: v1
metadata:
  name: github-ssh-credentials
data:
  id_rsa: |
    <base64 encoded private key>
EOF
```

3. 在集群中添加 secret。

```
oc create -f ssh-secret.yml
```

21.3.2.7.4. 使用私有容器 registry

管道会自动构建 Operator 捆绑包镜像和捆绑包镜像索引，以进行测试和验证。默认情况下，管道在集群的 OpenShift Container Registry 中创建镜像。如果要使用外部私有 registry，则必须通过在集群中添加 secret 来提供凭证。

```
oc create secret docker-registry registry-dockerconfig-secret \
    --docker-server=quay.io \
    --docker-username=<registry username> \
    --docker-password=<registry password> \
    --docker-email=<registry email>
```

21.4. 执行 OPENSHIFT OPERATOR 管道

您可以使用以下方法运行 OpenShift Operator 管道。

提示

在以下示例中，根据您的要求删除或添加参数和工作区。

如果您使用 Red Hat OpenShift Local，以前称为 Red Hat CodeReady Containers (CRC)或 Red Hat OpenShift on IBM Power for ppc64le 架构，请将以下 tekton CLI 参数传递给每个 ci pipeline 命令以避免权限问题：

--pod-template templates/crc-pod-template.yml

故障排除

如果您的 OpenShift Pipelines operator 1.9 或更高版本无法正常工作，请按照以下步骤修复它：

先决条件

在创建自定义安全性上下文约束(SCC)前，请确保您具有集群的管理员特权。

流程

要使 OpenShift Pipelines operator 1.9 或更高版本正常工作，并在需要特权升级的 ci-pipeline 中执行一部分任务，创建一个自定义安全性上下文约束(SCC)，并使用下列命令将它链接到 pipeline 服务帐户：

1. **创建新 SCC：**

```
oc apply -f ansible/roles/operator-pipeline/templates/openshift/openshift-pipelines-custom-scc.yml
```

2. **将新 SCC 添加到 ci-pipeline 服务帐户：**

```
oc adm policy add-scc-to-user pipelines-custom-scc -z pipeline
```

其他资源

如需有关 SCC 的更多信息，请参阅关于安全性上下文约束。

21.4.1. 运行 Minimal 管道

流程

在终端窗口中运行以下命令：

```
GIT_REPO_URL=<Git URL to your certified-operators fork >
BUNDLE_PATH=<path to the bundle in the Git Repo> (For example - operators/my-operator/1.2.8)

tkn pipeline start operator-ci-pipeline \
  --param git_repo_url=$GIT_REPO_URL \
  --param git_branch=main \
  --param bundle_path=$BUNDLE_PATH \
  --param env=prod \
  --workspace name=pipeline,volumeClaimTemplateFile=templates/workspace-template.yml \
  --showlog
```

运行命令后，管道会提示您提供额外的参数。接受所有默认值以完成管道执行。

以下被设置为 default，不需要显式包含，但如果 kubeconfig secret 在不同名称下创建，则可以被覆盖。

```
--param kubeconfig_secret_name=kubeconfig \
--param kubeconfig_secret_key=kubeconfig
```

如果您在 ppc64le 和 s390x 架构上运行 ci 管道，请从默认值 quay.io/redhat-isv/operator-pipelines-images:released 改为 quay.io/redhat-isv/operator-pipelines-images:multi-arch。

故障排除

如果您在使用 SSH URL 时收到 Permission Denied 错误，请尝试 GITHUB HTTPS URL。

21.4.2. 使用镜像摘要固定运行管道

先决条件

执行 启用摘要固定的指令。

流程

在终端窗口中运行以下命令：

```
GIT_REPO_URL=<Git URL to your certified-operators fork >
BUNDLE_PATH=<path to the bundle in the Git Repo> (ie: operators/my-operator/1.2.8)
GIT_USERNAME=<your github username>
GIT_EMAIL=<your github email address>

tkn pipeline start operator-ci-pipeline \
  --param git_repo_url=$GIT_REPO_URL \
  --param git_branch=main \
  --param bundle_path=$BUNDLE_PATH \
  --param env=prod \
  --param pin_digests=true \
  --param git_username=$GIT_USERNAME \
  --param git_email=$GIT_EMAIL \
  --workspace name=pipeline,volumeClaimTemplateFile=templates/workspace-template.yml \
  --workspace name=ssh-dir,secret=github-ssh-credentials \
  --showlog
```

故障排除

当您收到错误 - 无法读取 https://github.com的 Username 时，请提供 --param git_repo_url 的 SSH github URL。

21.4.3. 使用私有容器 registry 运行管道

先决条件

使用私有容器 registry 执行包含在 下的指令。

流程

在终端窗口中运行以下命令：

```
GIT_REPO_URL=<Git URL to your certified-operators fork >
BUNDLE_PATH=<path to the bundle in the Git Repo> (ie: operators/my-operator/1.2.8)
GIT_USERNAME=<your github username>
GIT_EMAIL=<your github email address>
REGISTRY=<your image registry.  ie: quay.io>
IMAGE_NAMESPACE=<namespace in the container registry>

tkn pipeline start operator-ci-pipeline \
  --param git_repo_url=$GIT_REPO_URL \
  --param git_branch=main \
  --param bundle_path=$BUNDLE_PATH \
  --param env=prod \
  --param pin_digests=true \
  --param git_username=$GIT_USERNAME \
  --param git_email=$GIT_EMAIL \
  --param registry=$REGISTRY \
  --param image_namespace=$IMAGE_NAMESPACE \
  --workspace name=pipeline,volumeClaimTemplateFile=templates/workspace-template.yml \
  --workspace name=ssh-dir,secret=github-ssh-credentials \
  --workspace name=registry-credentials,secret=registry-docker config-secret \
  --showlog \
```

21.5. 提交认证结果

以下流程可帮助您向红帽提交认证测试结果。

先决条件

1. 执行 配置存储库以提交认证结果 的说明。

2. 将以下参数添加到您要从中提交红帽认证拉取请求的 GitHub 上游存储库。默认情况下，它是红帽认证存储库，但您可以使用自己的存储库进行测试。

```
-param upstream_repo_name=$UPSTREAM_REPO_NAME #Repo where Pull Request (PR) will be opened

--param submit=true
```

以下内容被设置为 default，不需要显式包含，但如果在其他名称下创建了您的 Pyxis secret，则可以被覆盖。

```
--param pyxis_api_key_secret_name=pyxis-api-secret \
--param pyxis_api_key_secret_key=pyxis_api_key
```

流程

您可以为四个不同的场景提交红帽认证测试结果：

21.5.1. 从最小管道提交测试结果

流程

在终端窗口中执行以下命令：

```
GIT_REPO_URL=<Git URL to your certified-operators fork >
BUNDLE_PATH=<path to the bundle in the Git Repo> (ie: operators/my-operator/1.2.8)

tkn pipeline start operator-ci-pipeline \
  --param git_repo_url=$GIT_REPO_URL \
  --param git_branch=main \
  --param bundle_path=$BUNDLE_PATH \
  --param upstream_repo_name=redhat-openshift-ecosystem/certified-operators \
  --param submit=true \
  --param env=prod \
  --workspace name=pipeline,volumeClaimTemplateFile=templates/workspace-template.yml \
  --showlog
```

21.5.2. 使用镜像摘要固定提交测试结果

在终端窗口中执行以下命令：

先决条件

执行包括以下内容的说明：

- 配置提交认证结果的存储库。
- 启用摘要固定.

流程

```
GIT_REPO_URL=<Git URL to your certified-operators fork >
BUNDLE_PATH=<path to the bundle in the Git Repo> (ie: operators/my-operator/1.2.8)
GIT_USERNAME=<your github username>
GIT_EMAIL=<your github email address>

tkn pipeline start operator-ci-pipeline \
  --param git_repo_url=$GIT_REPO_URL \
  --param git_branch=main \
  --param bundle_path=$BUNDLE_PATH \
  --param env=prod \
  --param pin_digests=true \
  --param git_username=$GIT_USERNAME \
  --param git_email=$GIT_EMAIL \
  --param upstream_repo_name=red-hat-openshift-ecosystem/certified-operators \
  --param submit=true \
  --workspace name=pipeline,volumeClaimTemplateFile=templates/workspace-template.yml \
  --workspace name=ssh-dir,secret=github-ssh-credentials \
  --showlog
```

故障排除

当您收到错误 - 无法读取 https://github.com的 Username 时，请提供 --param git_repo_url 的 SSH github URL。

21.5.3. 从私有容器 registry 提交测试结果

在终端窗口中执行以下命令：

先决条件

执行包括以下内容的说明：

- 配置提交认证结果的存储库。
- 通过使用私有容器注册表。

流程

```
GIT_REPO_URL=<Git URL to your certified-operators fork >
BUNDLE_PATH=<path to the bundle in the Git Repo> (ie: operators/my-operator/1.2.8)
GIT_USERNAME=<your github username>
GIT_EMAIL=<your github email address>
REGISTRY=<your image registry.  ie: quay.io>
IMAGE_NAMESPACE=<namespace in the container registry>

tkn pipeline start operator-ci-pipeline \
  --param git_repo_url=$GIT_REPO_URL \
  --param git_branch=main \
  --param bundle_path=$BUNDLE_PATH \
  --param env=prod \
  --param pin_digests=true \
  --param git_username=$GIT_USERNAME \
  --param git_email=$GIT_EMAIL \
  --param registry=$REGISTRY \
  --param image_namespace=$IMAGE_NAMESPACE \
  --param upstream_repo_name=red hat-openshift-ecosystem/certified-operators \
  --param submit=true \
  --workspace name=pipeline,volumeClaimTemplateFile=templates/workspace-template.yml \
  --workspace name=ssh-dir,secret=github-ssh-credentials \
  --workspace name=registry-credentials,secret=registry-docker config-secret \
  --showlog
```

21.5.4. 使用镜像摘要固定和从私有容器 registry 提交测试结果

在终端窗口中执行以下命令：

先决条件

执行包括以下内容的说明：

- 配置提交认证结果的存储库。
- 启用摘要固定.
- 通过使用私有容器注册表。

流程

```
GIT_REPO_URL=<Git URL to your certified-operators fork >
BUNDLE_PATH=<path to the bundle in the Git Repo> (ie: operators/my-operator/1.2.8)
GIT_USERNAME=<your github username>
GIT_EMAIL=<your github email address>
REGISTRY=<your image registry.  ie: quay.io>
IMAGE_NAMESPACE=<namespace in the container registry>

tkn pipeline start operator-ci-pipeline \
  --param git_repo_url=$GIT_REPO_URL \
  --param git_branch=main \
  --param bundle_path=$BUNDLE_PATH \
  --param env=prod \
  --param pin_digests=true \
  --param git_username=$GIT_USERNAME \
  --param git_email=$GIT_EMAIL \
  --param upstream_repo_name=red-hat-openshift-ecosystem/certified-operators \
  --param registry=$REGISTRY \
  --param image_namespace=$IMAGE_NAMESPACE \
  --param submit=true \
  --workspace name=pipeline,volumeClaimTemplateFile=templates/workspace-template.yml \
  --workspace name=ssh-dir,secret=github-ssh-credentials \
  --workspace name=registry-credentials,secret=registry-docker config-secret \
  --showlog
```

认证成功后，认证产品将在 红帽生态系统目录 上列出。

客户通过嵌入式 OpenShift operatorHub 列出并消耗认证的 Operator，使他们能够轻松部署和运行解决方案。此外，您的产品和操作器镜像还将在 红帽生态系统目录 上列出。

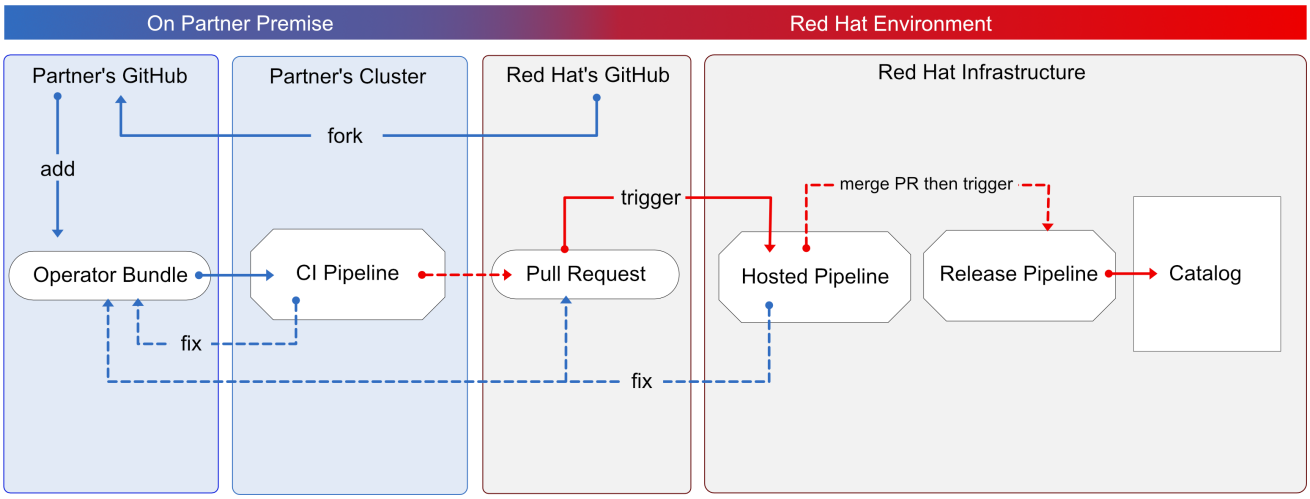
第 22 章 使用红帽托管管道运行认证套件

如果要使用 Red Hat Hosted Pipeline 认证您的 Operator，则必须为红帽认证存储库创建拉取请求。

如果您不有兴趣接收全面的日志，或者未准备好将工具包含在您自己的 CI/CD 工作流中，请选择此路径。

以下是该过程的概述：

图 22.1. 红帽托管管道概述



此过程首先通过 GitHub 拉取请求提交 Operator 捆绑包。然后，红帽使用内部 OpenShift 集群运行认证测试。此路径与以前的 Operator 捆绑包认证类似。您可以在拉取请求和 Red Hat Partner Connect Operator 捆绑包中看到认证测试结果。如果所有认证测试都成功，您的 Operator 将自动合并并发布到 Red Hat Container Catalog 和 OpenShift 中的嵌入式 OperatorHub。

按照说明，通过红帽托管管道认证您的 Operator：

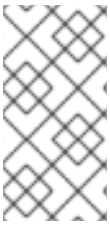
先决条件

- 完成 Red Hat Partner Connect 网站中提供的 *产品列表*。
- 在 Red Hat Partner Connect 网站，转至 组件 选项卡。
  - 在 Authorized GitHub user accounts 字段中，输入您的 GitHub 用户名到授权

GitHub 用户列表。

- 如果使用私有容器 registry，在 OpenShift Object YAML 字段中点 Add 来添加 docker config.json secret，然后点 Save。

流程



注意

只有在您希望在 Red Hat 托管管道上运行 Red Hat OpenShift Operator 认证时，才按照以下步骤操作。

22.1. 分叉软件仓库

1. 登录 GitHub，再分叉红帽OpenShift 操作器上游存储库。
2. 根据您要分发的 Catalogs，从下表派生适当的软件仓库：

目录	上游存储库
认证目录	https://github.com/redhat-openshift-ecosystem/certified-operators

3. 克隆 fork 的 certified-operators 存储库。
4. 将 Operator 捆绑包的内容添加到已分叉仓库中的 operators 目录中。

如果要在多个目录中发布 Operator 捆绑包，您可以分叉每个目录并为每个分叉完成一次认证。

其他资源

有关在 GitHub 中创建分叉的更多信息，请参阅 Fork 仓库。

22.2. 添加 OPERATOR 捆绑包

在 fork 的 operators 目录中，有一系列子目录。

22.2.1. 如果您在之前已认证了这个 operator -

在 operators 目录中为您的 Operator 找到对应的文件夹。将 Operator Bundle 的内容放在这个目录中。

注意

确保您的软件包名称与 Operator 的现有文件夹名称一致。

22.2.2. 如果您新认证这个 operator -

如果新认证 Operator 没有 Operator 的父目录下的子目录，则必须创建一个子目录。

在 operators 下创建新目录。这个目录的名称应与 Operator 的软件包名称匹配。例如， my-operator。

- 在这个 operator 目录中，使用 Operator 名称创建一个新子目录，如 < my-operator>，并为 < V1.0 > 创建一个版本目录，并放置您的捆绑包。这些目录对于之前已通过认证的 operator 预加载。

```
├── operators
    └── my-operator
        └── v1.0
```

- 在 version 目录下，添加一个 manifests 文件夹，其中包含所有 OpenShift 清单，包括 clusterserviceversion.yaml 文件。

推荐的目录结构

以下示例演示了推荐的目录结构。

```
├── config.yaml
```

```
├── operators
│   └── my-operator
│       ├── v1.4.8
│       │   ├── manifests
│       │   │   ├── cache.example.com_my-operators.yaml
│       │   │   ├── my-operator-controller-manager-metrics-service_v1_service.yaml
│       │   │   ├── my-operator-manager-config_v1_configmap.yaml
│       │   │   ├── my-operator-metrics-reader_rbac.authorization.k8s.io_v1_clusterrole.yaml
│       │   │   └── my-operator.clusterserviceversion.yaml
│       │   └── metadata
│       │       └── annotations.yaml
│       └── ci.yaml
```

配置文件	描述
config.yaml	在这个文件中，包含 Operator 的组织。它可以是 **certified-operators**。例如，**机构： certified-operators**
ci.yaml	在此文件中，包括您的 Red Hat 技术合作伙伴项目 ID 和此 operator 的组织目标。 例如，**cert_project_id: <your partner project id>**。此文件存储成功认证流程所需的所有元数据。
annotations.yaml	在此文件中，包含 OpenShift 版本的注解，它引用 OpenShift 版本的范围。例如，**v4.8-v4.10** 表示 4.8 到 4.10 版本。将其添加到任何现有内容。 例如，NTT **: OpenShift 注解 com.redhat.openshift.versions: v4.8-v4.10**。**com.redhat.openshift.versions** 字段（作为 operator 捆绑包中的元数据的一部分）用于确定 Operator 是否包含在给定 OpenShift 版本的认证目录中。您必须使用它来指定 Operator 支持的一个或多个 OpenShift 版本。 请注意，在版本之前必须使用字母 'v'，且不允许使用空格。语法如下： ● 单一版本表示该 Operator 在 OpenShift 或更高版本上被支持。Operator 会自动添加到后续 OpenShift 版本的已认证目录中。 ● 前面带有 '=' 的单个版本表示 Operator 只在该特定版本的 OpenShift 上被支持。例如，使用 **=v4.8** 会将 Operator 添加到 OpenShift 4.8 认证的目录中，但不用于后续 OpenShift 版本。 ● 范围可用于指示仅支持该范围内的 OpenShift 版本。例如，使用 **v4.8-v4.10** 会将 Operator 添加到 OpenShift 4.8 到 4.10 的认证目录中，但不适用于 OpenShift 4.11 或 4.12。

其他资源

- 如需了解更多详细信息，请参阅管理 OpenShift 版本。
- 如需 operator 捆绑包的示例，请参阅 此处。

22.3. 创建拉取请求

最后一步是为目标上游存储库创建拉取请求。

目录	上游存储库
认证目录	https://github.com/redhat-openshift-ecosystem/certified-operators

如果要在多个目录中发布 Operator 捆绑包，您可以为每个目标目录创建一个拉取请求。

如果您不熟悉在 GitHub 中创建拉取请求，您可以在此中找到说明。https://docs.github.com/en/pull-requests/collaborating-with-pull-requests/proposing-changes-to-your-work-with-pull-requests/creating-a-pull-request-from-a-fork

注意

拉取请求的标题必须符合以下格式：operator my-operator (v1.4.8)它应该以单词 operator 开头，后跟您的 Operator 软件包名称，后面跟在括号中的版本号。
当您创建拉取请求时，它会触发红帽托管管道，并在失败或完成时通过拉取请求注释提供更新。

22.3.1. 要遵循的指南

- 您可以通过关闭并重新打开拉取请求来重新触发红帽托管管道。
- 对于给定的 Operator 版本，一次只能有一个打开的拉取请求。
- 拉取请求成功合并后，它就无法更改。您必须检查 Operator 的版本并打开新的拉取请求。

- 您必须使用 Operator 的软件包名称作为您在 Operator 下创建的目录名称。这个软件包名称应与 annotations.yaml 文件中的 package 注解匹配。这个软件包名称还应与 clusterserviceversion.yaml 文件名的前缀匹配。

- 您的拉取请求应该只修改单个 Operator 版本目录中的文件。不要尝试将更新合并到多个 Operator 间的多个版本或更新。

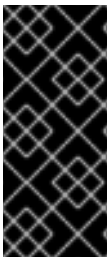
- 用于命名您的版本目录的版本指示符应与拉取请求的标题中使用的版本指示符匹配。

- 运行认证测试不接受镜像标签，只使用 SHA 摘要。将对 镜像标签的所有引用替换为 对应的 SHA 摘要。

第 23 章 发布经认证的 OPERATOR

认证被视为完成，您的 Operator 将出现在 Red Hat Container Catalog 中，并在所有测试都成功后在 OpenShift 中嵌入的 OperatorHub，并启用了认证管道向红帽提交结果。

此外，该条目将出现在 红帽认证生态系统上。



重要

Red Hat OpenShift 软件认证不会对合作伙伴的产品进行测试，在 Operator 构建之外或执行其对安装和执行的红帽平台的影响。认证候选产品质量保证的所有方面均保留合作伙伴的职责。

第 24 章 故障排除指南

有关故障排除提示和临时解决方案，请参阅 对 Operator Cert Pipeline 进行故障排除。

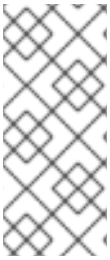
附录 B. HELM 和 ANSIBLE OPERATOR

- 有关构建 Helm Operator 的详情，请参考 构建 Helm Operator。

- 有关构建 Ansible 操作器的详情，请参考 构建 Ansible Operator。

部分 IV. HELM CHART 认证

第 25 章 使用 HELM CHART



注意

在继续 Red Hat Helm Chart 认证前，请认证您的容器应用程序组件。在认证 Helm Chart 组件前，Helm Chart 组件中引用的所有容器都必须已通过红帽生态系统目录认证并发布。

25.1. HELM CHART 简介

Helm 是一个 Kubernetes 原生自动化技术和软件包管理器，简化了应用程序和服务的部署。Helm 使用名为 chart 的打包格式。chart 是描述一组相关 Kubernetes 资源的文件集合。集群中 chart 的特定版本的运行实例被称为 release。当每次一个 chart 在集群中安装时，一个新的 release 会被创建。在每次安装 chart，或一个版本被升级或回滚时，都会创建增量修订版本。图表通过自动化的 Red Hat OpenShift 认证工作流，确保安全合规以及与平台的最佳集成和体验。

25.2. HELM CHART 的认证工作流

注意

红帽建议您在开始认证过程前具有红帽认证工程师或具有同等经验。

任务摘要

认证工作流包括三个主要步骤：

1. 第 25.2.1 节 “Helm chart 板认证”
2. 第 25.2.2 节 “Helm chart 的认证测试”
3. 第 25.2.3 节 “在红帽生态系统目录中发布经认证的 Helm chart”

25.2.1. Helm chart 板认证

执行认证加入概述的步骤：

1. 加入 Red Hat Connect for Technology Program （ Red Hat Connect for Technology Program (Red Hat Connect for Technology Program)
2. 同意计划条款和条件。
3. 选择所需产品类别来创建您的产品列表。您可以从可用产品类别中选择：
   a. 容器化应用程序
   b. 独立应用程序
   c. OpenStack Infrastructure
4. 填写您的公司简介。
5. 将组件添加到产品列表中。
6. 为您的产品列表认证组件。

其他资源

有关创建第一个产品列表的详细信息，请参阅创建产品。

25.2.2. Helm chart 的认证测试

按照以下高级别步骤运行认证测试：

1. 派生 红帽上游存储库。

2. 在测试环境中安装并运行 chart verifier 工具。

3. 检查测试结果并进行故障排除（若有问题）。

4. 通过拉取请求向红帽提交认证结果。

其他资源

有关认证测试的详细信息，请参阅验证 Helm chart 以获得认证。

25.2.3. 在红帽生态系统目录中发布经认证的 Helm chart

认证的 helm chart 在 红帽合作伙伴连接 门户的 产品列表 页面中发布，然后您可以在受支持的红帽容器平台上运行。您的产品及其 Helm Chart 会使用您提供的列表信息在 Red Hat Container Catalog 上列出。

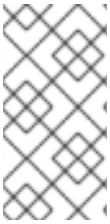
其他资源

- 有关发布认证 Helm Chart 的更多信息，请参阅 发布经认证的 Helm Chart。
- 如需有关 Helm chart 的更多信息，请参阅：
  - 什么是 Helm？
  - Helm chart
  - 技术研讨会：OpenShift Helm Chart 认证

第 26 章 验证 HELM CHART 以进行认证

您可以使用 chart-verifier CLI 工具验证 Helm chart。Chart-verifier 是一个基于 CLI 的开源工具，它运行一个可配置的检查列表，以验证 Helm chart 是否有满足红帽认证的标准所需的所有相关元数据和格式。它验证 Helm chart 是否在 Red Hat OpenShift Container Platform 上无缝分布，并可作为认证的 Helm Chart 条目提交给 Red Hat OpenShift Helm Chart 仓库。

该工具还会验证 Helm Chart URL，并以 YAML 格式提供报告，以及每个检查都有正或负结果的人类可读描述。检查的负结果表示图表中需要更正的问题。您还可以自定义您要在验证过程中执行的检查。



注意

红帽强烈建议您使用最新版本的 chart-verifier 工具来验证本地测试环境中的 Helm chart。这可让您在 Chart 开发周期内自行检查结果，从而防止每次都向红帽提交结果。

其他资源

有关 chart-verifier CLI 工具的更多信息，请参阅 chart-verifier。

26.1. 准备测试环境

认证您的产品的第一步是设置可运行测试的环境。要运行完整的 chart-verifier 测试，您需要访问 Red Hat OpenShift 集群环境。您可以安装 chart-verifier 工具，并在此环境中执行所有与 chart 相关的测试。您可以使用几个可配置的命令行选项禁用这些测试，但为了获得红帽批准的认证，必须运行测试。

注意

作为授权的红帽合作伙伴，您可以免费访问 Red Hat OpenShift Container Platform，您可以使用 Red Hat 合作伙伴订阅(RHPS)计划在您自己的测试环境中安装集群。要了解有关在 Red Hat Partner Connect 计划中软件访问的好处的更多信息，请参阅计划指南。

流程

- 使用基于 x86-64 的 Red Hat Enterprise Linux 系统(oc)、Helm 和 Podman 或安装了 chart-verifier 工具来设置测试服务器。

- 使用 Red Hat Managed Services Openshift 集群安装 完全受管集群。这是一个试用选项，仅在 60 天内有效。

- 或者，在您的云环境、数据中心或计算机上安装自我管理的集群。通过使用此选项，您可以将合作伙伴订阅（也称为 NFR）用于永久部署。

其他资源

- 有关设置您的环境的更多信息，请参阅 Try Red Hat OpenShift。

- 要了解更多有关安装集群和配置 helm chart 的信息，请参阅：

  - OpenShift Container Platform

  - OpenShift 集群 CLI 管理

  - 集群中的 Helm Chart 管理

26.2. 运行 HELM CHART-VERIFIER 工具

执行 chart-verifier 工具的建议目录结构如下：

```
.
└── src
    ├── Chart.yaml
    ├── README.md
    ├── templates
    │   ├── deployment.yaml
    │   ├── _helpers.tpl
    │   ├── hpa.yaml
    │   ├── ingress.yaml
    │   ├── NOTES.txt
    │   ├── serviceaccount.yaml
    │   ├── service.yaml
    │   └── tests
    │       └── test-connection.yaml
    ├── values.schema.json
    └── values.yaml
```

先决条件

- 安装了 Podman 或 Docker CLI 的容器引擎。
- 互联网连接，检查镜像是否已通过红帽认证。
- GitHub 配置集，将 chart 提交到 OpenShift Helm Charts 仓库。
- Red Hat OpenShift Container Platform 集群。
- 在运行 chart-verifier 工具前，使用以下命令打包 Helm chart：

```
$ helm package <helmchart folder>
```

此命令将归档 Helm Chart，并将其转换为 .tgz 文件格式。

流程

您可以使用两种方法运行完整的 chart-verifier 工具集：

- 使用 Podman 或 Docker
- 通过使用二进制文件（仅限 Linux）

26.2.1. 使用 Podman 或 Docker

1. 使用通用资源标识符(uri)远程运行所有可用检查，假设 kube 配置文件位于位置 ${HOME}/.kube ：

```
$ podman run --rm -i                          \
      -e KUBECONFIG=/.kube/config             \
      -v "${HOME}/.kube":/.kube               \
```

```
        "quay.io/redhat-certification/chart-verifier" \
        verify                                        \
        <chart-uri>
```

在这个命令中，chart-uri 是 https uri 上提供的 chart 存档的位置。确保存档必须采用 .tgz 格式。

2. **运行系统上本地可用的 chart 的所有可用检查，假设 chart 位于当前目录中，kube 配置文件位于位置 ${HOME}/.kube:**

```
$ podman run --rm                                 \
      -e KUBECONFIG=/.kube/config                 \
      -v "${HOME}/.kube":/.kube                   \
      -v $(pwd):/charts                           \
      "quay.io/redhat-certification/chart-verifier" \
      verify                                      \
      /charts/<chart>
```

在这个命令中，chart-uri 是本地目录中提供的 Chart 存档的位置。确保存档必须采用 .tgz 格式。

3. **运行以下 verify 命令以获取与该命令关联的可用选项列表及其用法：**

```
$ podman run -it --rm quay.io/redhat-certification/chart-verifier verify --help
```

命令的输出类似以下示例：

```
Verifies a Helm chart by checking some of its characteristics

Usage:
  chart-verifier verify <chart-uri> [flags]

Flags:
  -S, --chart-set strings           set values for the chart (can specify multiple or separate values
with commas: key1=val1,key2=val2)
  -G, --chart-set-file strings      set values from respective files specified via the command line
(can specify multiple or separate values with commas: key1=path1,key2=path2)
  -X, --chart-set-string strings    set STRING values for the chart (can specify multiple or
separate values with commas: key1=val1,key2=val2)
  -F, --chart-values strings        specify values in a YAML file or a URL (can specify multiple)
      --debug                       enable verbose output
  -x, --disable strings             all checks will be enabled except the informed ones
  -e, --enable strings              only the informed checks will be enabled
      --helm-install-timeout duration   helm install timeout (default 5m0s)
  -h, --help                        help for verify
```

```
      --kube-apiserver string       the address and the port for the Kubernetes API server
      --kube-as-group stringArray   group to impersonate for the operation, this flag can be
repeated to specify multiple groups.
      --kube-as-user string         username to impersonate for the operation
      --kube-ca-file string         the certificate authority file for the Kubernetes API server
connection
      --kube-context string         name of the kubeconfig context to use
      --kube-token string           bearer token used for authentication
      --kubeconfig string           path to the kubeconfig file
  -n, --namespace string            namespace scope for this request
  -V, --openshift-version string    set the value of certifiedOpenShiftVersions in the report
  -o, --output string               the output format: default, json or yaml
  -k, --pgp-public-key string       file containing gpg public key of the key used to sign the chart
  -W, --web-catalog-only            set this to indicate that the distribution method is web catalog
only (default: true)
      --registry-config string      path to the registry config file (default
"/home/baiju/.config/helm/registry.json")
      --repository-cache string     path to the file containing cached repository indexes (default
"/home/baiju/.cache/helm/repository")
      --repository-config string    path to the file containing repository names and URLs (default
"/home/baiju/.config/helm/repositories.yaml")
  -s, --set strings                 overrides a configuration, e.g: dummy.ok=false
  -f, --set-values strings          specify application and check configuration values in a YAML
file or a URL (can specify multiple)
  -E, --suppress-error-log          suppress the error log (default: written to
./chartverifier/verifier-<timestamp>.log)
      --timeout duration            time to wait for completion of chart install and test (default
30m0s)
  -w, --write-to-file               write report to ./chartverifier/report.yaml (default: stdout)
Global Flags:
      --config string   config file (default is $HOME/.chart-verifier.yaml)
```

4. **运行检查的子集：**

```
$ podman run --rm -i                            \
      -e KUBECONFIG=/.kube/config               \
      -v "${HOME}/.kube":/.kube                 \
      "quay.io/redhat-certification/chart-verifier" \
      verify -enable images-are-certified,helm-lint     \
      <chart-uri>
```

5. **运行除子集之外的所有检查：**

```
$ podman run --rm -i                            \
      -e KUBECONFIG=/.kube/config               \
      -v "${HOME}/.kube":/.kube                 \
      "quay.io/redhat-certification/chart-verifier" \
      verify -disable images-are-certified,helm-lint     \
      <chart-uri>
```

注意

运行检查子集旨在减少开发的反馈循环。要认证您的图表，您必须运行所有必需的检查。

6. 提供 **chart-override** 值：

```
$ podman run --rm -i                              \
      -e KUBECONFIG=/.kube/config                 \
      -v "${HOME}/.kube":/.kube                   \
      "quay.io/redhat-certification/chart-verifier" \
      verify –chart-set default.port=8080         \
      <chart-uri>
```

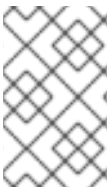
7. 从当前目录中的文件提供 **chart-override** 值：

```
$ podman run --rm -i                              \
      -e KUBECONFIG=/.kube/config                 \
      -v "${HOME}/.kube":/.kube                   \
      -v $(pwd):/values                           \
      "quay.io/redhat-certification/chart-verifier" \
      verify –chart-values /values/overrides.yaml \
      <chart-uri>
```

26.2.1.1. 配置 timeout 选项

如果 chart-testing 进程延迟，则增加超时值。默认情况下，chart-testing 过程需要大约 30 分钟才能完成。

```
$ podman run --rm -i                              \
      -e KUBECONFIG=/.kube/config                 \
      -v "${HOME}/.kube":/.kube                   \
      -v $(pwd):/values                           \
      "quay.io/redhat-certification/chart-verifier" \
      verify --timeout 40m                        \
      <chart-uri>
```



注意

如果您在测试过程中观察了延迟，红帽建议您向红帽认证团队提交报告进行验证。

26.2.1.2. 保存报告

当 chart-testing 过程完成后，默认会显示报告信息。您可以通过将报告重定向到文件来保存报告。

例如：

```
$ podman run --rm -i                              \
      -e KUBECONFIG=/.kube/config                 \
      -v "${HOME}/.kube":/.kube                   \
      "quay.io/redhat-certification/chart-verifier" \
      verify –enable images-are-certified,helm-lint      \
      <chart-uri> > report.yaml
```

除了此命令外，使用 -w 选项可将报告直接写入文件 ./chartverifier/report.yaml。要获取此文件，您必须将文件挂载到 /app/chartverifer。

例如：

```
$ podman run --rm -i                              \
      -e KUBECONFIG=/.kube/config                 \
      -v "${HOME}/.kube":/.kube                   \
      -v $(pwd)/chartverifier:/app/chartverifier    \
      -w                                          \
      "quay.io/redhat-certification/chart-verifier" \
      verify –enable images-are-certified,helm-lint      \
      <chart-uri>
```

如果文件已存在，新报告将覆盖该文件。

26.2.1.3. 配置错误日志

默认情况下，生成错误日志并保存到文件 ./chartverifier/verify-<timestamp>.yaml 中。它包括错误消息、每个检查的结果以及有关 chart 测试的附加信息。要获得错误日志的副本，您必须将文件挂载到 /app/chartverifer。

例如：

```
$ podman run --rm -i                              \
      -e KUBECONFIG=/.kube/config                 \
      -v "${HOME}/.kube":/.kube                   \
      -v $(pwd)/chartverifier:/app/chartverifier    \
```

```
"quay.io/redhat-certification/chart-verifier" \
verify –enable images-are-certified,helm-lint      \
<chart-uri> > report.yaml
```

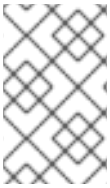
如果要将多个日志保存到同一目录中，您可以一次存储最多 10 个日志文件。当达到最大文件限制时，旧的日志文件将自动替换为较新的日志文件。

使用 -E 或 -suppress-error-log 选项阻止错误日志输出。

注意

错误和警告消息是标准错误消息，通过使用 -E 或 - suppress-error-log 选项不会 被禁止。

26.2.2. 使用二进制文件



注意

这个方法仅适用于 Linux 系统。

1. 从 发行版本 页面下载并安装最新的 chart-verifier 二进制文件。

2. 使用以下命令解压 tarball 二进制文件：

```
$ tar zxvf <tarball>
```

3. 在 unzipped 目录中运行以下命令执行所有 Helm Chart 检查：

```
$ ./chart-verifier verify <chart-uri>
```

在这个命令中，chart-uri 是服务器上可用的 Chart 存档的位置。确保存档必须采用 .tgz 格式。默认情况下，chart-verifier 工具假定 kube 配置文件位于默认位置 $HOME/.kube。如果文件在默认位置上不可用，请将环境变量设置为 KUBECONFIG。

chart-verifier 的输出包括执行的测试详情以及每个测试的结果状态。它还指示每个测试是强制的，还是建议用于红帽认证。如需更多信息，请参阅 Helm Chart 检查的类型。

其他资源

- **要了解更多有关 chart-verifier 工具的信息，请参阅 Helm Chart 检查 Red Hat OpenShift 认证。**

第 27 章 创建产品

产品列表提供营销和技术信息，向潜在客户展示您的产品功能和优势。它将为产品添加所有必要组件以进行认证的基础。

先决条件

除了特定认证测试要求外，还验证您的产品在红帽平台上的功能。如果在目标红帽平台上运行您的产品产生了子标准体验，则必须在认证前解决问题。

在创建 Helm Chart 组件前，将您的 chart 的容器镜像认证为容器应用程序。

流程

红帽建议完成列表选项卡中的所有可选字段，以获取全面的产品列表。如需更多信息，可以帮助相互客户做出明智的选择。

在为您的产品列表输入信息时，红帽鼓励与您的产品经理、营销代表或其他产品专家合作。

带有星号 packagemanifests 的字段是必需的。

流程

1. 登录到 Red Hat Partner Connect Portal。
2. 进入认证技术门户选项卡，然后单击门户。
3. 在标题栏中，单击 产品管理。
4. 从 Listing and Certification 选项卡中，单击 Manage products。

5. 在 My Products 页面中，单击 Create Product。

   此时会打开 Create New Product 对话框。

6. 输入 产品名称。

7. 从 您要认证的产品中选择 所需的产品类别，然后单击 Create product。例如，选择 Containerized Application 来创建容器化产品列表。

   此时会打开带有您的 产品名称的新页面。它由以下标签页组成：

   - 第 27.1 节 “Helm chart 概述”
   - 第 27.2 节 “Helm chart 的产品信息”
   - 第 27.3 节 “Helm chart 的组件”
   - 第 27.4 节 “对 Helm chart 的支持”

   除了以下选项卡外，页面标头还提供 产品分数 详细信息。产品分数评估您的产品信息并显示分数。它可以是：

   - 公平
   - 良好
   - 非常好
   - best

8. 点 How do improve my score? 以改进您的产品分数。

9. 提供产品列表详情后，请单击 Save，然后移至下一部分。

27.1. HELM CHART 概述

此选项卡由一系列任务组成，您必须完成才能发布您的产品：

- 第 27.1.1 节 “Helm chart 的完整产品列表详情”
- 第 27.1.2 节 “Helm chart 的完整公司配置集信息”
- 第 27.1.3 节 “接受 Helm chart 的法律协议”
- 第 27.1.4 节 “为 Helm chart 添加至少一个产品组件”
- 第 27.1.5 节 “为您的 Helm chart 列表认证组件”

27.1.1. Helm chart 的完整产品列表详情

1. 要完成您的产品列表详情，请点 Start。

   此时会打开 Product Information 选项卡。

2. 输入所有基本产品详情并点 Save。

27.1.2. Helm chart 的完整公司配置集信息

1. 要完成您的公司概况信息，请单击 Start。输入所有详情后，单击 Submit。

2. 要修改现有的详情，请点 Review。此时会打开 Account Details 页面。

3. 检查和修改 Company 配置集信息，然后单击 Submit。

27.1.3. 接受 Helm chart 的法律协议

要发布您的产品镜像，请同意有关合作伙伴容器镜像的发布条款。

1. 要接受法律协议，请点击 Start。

2. 要预览或下载协议，请点 Review。

此时会显示 Red Hat Partner Connect Container 附录 文档。阅读文档，了解与容器镜像分发相关的术语。

27.1.4. 为 Helm chart 添加至少一个产品组件

1. 点 Start。您将被重定向到 Components 选项卡。

   要添加新或现有产品组件，请点 Add component。

2. 用于添加新组件，

   a. 在 Component Name 文本框中，输入组件名称。

   b. 对于您要创建的独立组件， 请选择您要认证的组件。例如，要认证 Helm Charts，请选择 Helm Chart。

   c. 点击 Next。

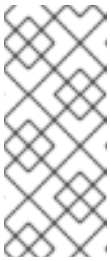
   d. 在 Chart Name 文本框中，为您的 Chart 输入一个唯一名称。

e.

Release Method - 为发布 **Helm Chart** 选择以下选项之一：

i.

Helm Chart 仓库 **chart.openshift.io - Helm chart** 发布到 **Red Hat Helm Chart** 仓库 **charts.openshift.io**，用户可以从此仓库中提取 **chart**。



注意

当您选择复选框 **The certified helm chart** 将从我的公司的存储库分发时，您的 **chart** 位置的条目将添加到 **Red Hat Helm Chart** 仓库 **charts.openshift.io** 的 索引中。

ii.

仅限 **Web** 目录**(catalog.redhat.com) - Helm chart** 没有发布到 **Red Hat Helm Chart** 仓库 **charts.openshift.io**，且不在 **Red Hat OpenShift OperatorHub** 中可见。当您创建新组件时，这个选项是默认选项，这个选项适用于不希望其 **Helm Chart** 在 **OpenShift** 中公开安装但需要验证认证的合作伙伴。只有在您有一个未满足 **OpenShift In-product Catalog** （认证）选项中的发布、权利或其他业务要求时，才选择此选项。

f.

单击 **Add component**。

3.

要添加现有组件，请从 **Add** 组件 对话框中选择 **Existing Component**。

a.

从 **Available components** 列表中，搜索并选择您要认证的组件，然后点转发箭头。所选组件被添加到 **Chose n** 组件 列表中。

b.

单击 **Attach existing component**。

27.1.5. 为您的 Helm chart 列表认证组件

1.

要为您的列表认证组件，请单击 **Start**。如果您有现有的产品组件，您可以查看 **Attached** 组件 列表及其详情：

a.

Name

b.

认证

c. **安全性**

d. **类型**

e. **Created**

f. **点击更多选项归档或删除组件**

2. **选择用于认证的组件。**

完成上述所有任务后，您将看到与所有选项相对应的绿色勾号标记。

Overview 选项卡还提供以下信息：

1. **产品联系人 - 提供产品营销和技术联系信息。**

a. **点 Add contacts to product 以提供联系信息**

b. **点 Edit 以更新信息。**

2. **产品中的组件 - 提供附加到产品的组件列表及其最后的更新信息。**

a. **点 Add components to product 将新的或现有组件添加到您的产品中。**

b. **点 Edit components 更新现有组件信息。**

发布产品列表后，您可以查看您的产品 就绪情况和 方式，以便在 Overview 选项卡上提高分数。

其他资源

有关分发方法的更多信息，请参阅 Helm Chart 分发方法。

27.2. HELM CHART 的产品信息

通过此选项卡，您可以提供有关您产品的所有重要信息。产品详情会在红帽生态系统目录中与您的产品一起发布。

常规 标签页：

提供产品的基本详情，包括产品名称和描述。

1. 输入 产品名称。
2. 可选：根据 定义的准则上传产品徽标。
3. 输入 Brief 描述 和长 描述。
4. 点击 Save。

功能和好处 选项卡：

提供您产品的重要特性。

1. 可选：输入 Title 和 Description。
2. 可选： 要为您的产品添加额外的功能，请点 + Add new feature。
3. 点击 Save。

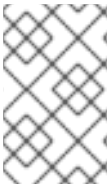
快速启动和配置标签页 ：

添加指向任何快速入门指南或配置文档的链接，以帮助客户部署并开始使用您的产品。

1. **可选：输入 Quick start 和 configuration instructions。**
2. **点击 Save。**
3. **如果您不想显示它们，请选择 Hide default instructions 复选框。**

链接的资源 标签页：

添加支持文档的链接，以帮助我们的客户使用您的产品。这些信息被映射到，并在产品目录页面中的 Documentation 部分显示。



注意

必须至少添加三个资源。如果可用，红帽建议您添加更多资源。

1. **选择 Type 下拉菜单，并输入资源的 Title 和 Description。**
2. **输入 资源 URL。**
3. **可选： 要为您的产品添加其他资源，请点 + Add new Resource。**
4. **点击 Save。**

常见问题解答 标签页：

添加常见问题以及产品用途、操作、安装或其他属性详情的回答。您可以包括有关您的产品和服务的常见客户查询。

1. 输入问题 和 answer。
2. 可选： 要为您的产品添加额外的常见问题，请点 + Add new FAQ。
3. 点击 Save。

支持 标签：

此选项卡可让您提供支持团队的联系信息。

1. 输入 支持 描述、支持网站、支持电话号码 以及支持电子邮件地址。
2. 点击 Save。

Contacts 标签页：

请提供营销和技术团队的联系信息。

1. 输入 营销联系人电子邮件地址 及 技术联系电子邮件地址。
2. 可选： 要添加其他联系人，请点 + Add another。
3. 点击 Save。

法律 选项卡：

提供产品相关的许可证和策略信息。

1. 输入 产品和隐私策略 URL 的 许可证协议 URL。
2. 点击 Save。

SEO 标签页：

使用此选项卡提高我们相互客户的可发现性，提高红帽生态系统目录搜索和互联网搜索引擎中的可见性。提供更多搜索别名（密钥和证书对）会增加产品的可发现性。

1. 选择 产品类别。
2. 输入 Key 和 Value 来设置搜索别名。
3. 点击 Save。
4. 可选： 要添加额外的键值对，请点 + Add new key-value pair。

注意

为您的产品至少添加一个搜索别名。如果可用，红帽建议您添加更多别名。

27.3. HELM CHART 的组件

使用此选项卡将组件添加到您的产品列表中。通过此选项卡，您还可以查看链接到您的产品列表的附加组件列表。

另外，要将组件附加到产品列表，您可以完成 Container、Operator 或 Helm Chart 产品列表的 Overview 选项卡中提供的 Add least one product component 选项。

1. 要添加新或现有产品组件，请点 **Add component**。

2. 用于添加新组件，

   a. 在 **Component Name** 文本框中，输入组件名称。

   b. 对于您要创建的 **OpenShift** 组件，请选择您要认证的组件。例如，要认证 **Helm Charts**，请选择 **Helm Chart**。

   c. 点击 **Next**。

   d. 在 **Chart Name** 文本框中，为您的 **Chart** 输入一个唯一名称。

   e. **Release Method -** 为发布 **Helm Chart** 选择以下选项之一：

      i. **Helm Chart** 仓库 **chart.openshift.io - Helm chart** 发布到 **Red Hat Helm Chart** 仓库 **charts.openshift.io**，用户可以从此仓库中提取 **chart**。

      注意

      当您选择复选框 **The certified helm chart** 将从我的公司的存储库分发时，您的 **chart** 位置的条目将添加到 **Red Hat Helm Chart** 仓库 **charts.openshift.io** 的 索引中。

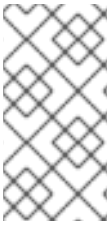
      ii. 仅限 **Web** 目录**(catalog.redhat.com) - Helm chart** 没有发布到 **Red Hat Helm Chart** 仓库 **charts.openshift.io**，且不在 **Red Hat OpenShift OperatorHub** 中可见。当您创建新组件时，这个选项是默认选项，这个选项适用于不希望其 **Helm Chart** 在 **OpenShift** 中公开安装但需要验证认证的合作伙伴。只有在您有一个未满足 **OpenShift In-product Catalog** （认证）选项中的发布、权利或其他业务要求时，才选择此选项。

   f. 单击 **Add component**。

3. 要添加现有组件，请从 **Add** 组件 对话框中选择 **Existing Component**。

   a. 从 **Available components** 列表中，搜索并选择您要认证的组件，然后点转发箭头。所选组件被添加到 **Chose n** 组件 列表中。

   b. 单击 **Attach existing component**。



注意

您可以将同一组件添加到多个产品列表中。所有附加的组件都必须发布，然后才能发布产品列表。

附加组件后，您可以查看 **Attached** 组件 列表及其详情：

i. **Name**

ii. 认证

iii. **安全性**

iv. 类型

v. **Created**

vi. 点击更多选项归档或删除附加的组件

或者，要搜索特定组件，请在 **Search by component Name** 文本框中键入组件的名称。

27.4. 对 HELM CHART 的支持

红帽合作伙伴加速服务(PAD)是一个产品和技术级别合作伙伴帮助台服务，允许当前和潜在合作伙伴提供与红帽产品、合作伙伴认证、产品认证、服务流程等相关的非技术问题。

您还可以联系红帽合作伙伴加速服务，以了解您可能对认证可能遇到的任何技术问题。技术帮助请求将重定向到认证运营团队。

通过合作伙伴订阅计划，红帽提供免费的、不用于销售的软件订阅，您可用来在目标红帽平台上验证您的产品。要请求访问此计划，请按照 合作伙伴订阅 网站上的说明进行操作。

1. 要请求支持，请点击 Open a support case。请参阅 PAD - 如何打开和管理 PAD 问题单，以创建一个 PAD ticket。

2. 要查看现有支持问题单的列表，请点 View 支持问题单。

27.5. 删除产品

如果要删除产品列表后，请转到 Overview 选项卡，再单击 Delete。

先发布的产品必须取消发布，然后才能删除。即使删除该产品后，红帽仍然保留与已删除产品相关的信息。

第 28 章 添加认证组件

创建新产品列表后，为新创建的产品列表添加认证组件。

您可以为新添加的组件配置以下选项：

注意

组件配置因不同的产品类别而异。

- 第 28.1 节 “Helm chart 认证”
- 第 28.2 节 “Helm chart 的可选资格”
- 第 28.3 节 “Helm chart 的存储库信息”
- 第 28.4 节 “Helm chart 的组件详情”
- 第 28.5 节 “Helm chart 的联系信息”
- 第 28.6 节 “Helm chart 的相关产品”

要配置选项，请转至 Components 选项卡，然后点任何现有组件。

28.1. HELM CHART 认证

GitHub 验证

在红帽合作伙伴连接上创建 Helm Chart 组件后，提交 Helm Chart 进行验证。

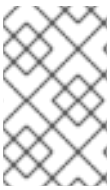
1. 从 Certification 选项卡中，前往 GitHub 验证。
2. 单击 Go to GitHub。您将被重定向到 OpenShift Helm Charts 仓库。
3. 提交拉取请求。

拉取请求由红帽认证团队审核。验证成功后，您的 Helm Chart 会在 红帽生态系统目录上发布。

其他资源

有关提交拉取请求的更多信息，请参阅 提交您的 Helm chart 以进行认证。

28.2. HELM CHART 的可选资格



注意

此选项卡仅适用于 Operator 和 Helm Chart 认证。

使用 可选资格 选项卡验证您的产品是否遵循红帽推荐的准则，以及在 Red Hat OpenShift 上部署工作负载的最佳实践。当您选择此选项卡时，会创建一个功能认证，您可以在其中提交红帽审核结果。验证成功后，您的工作负载产品将与红帽生态系统目录上的 Meets 最佳实践 徽标认证。

其他资源

如需更多信息，请参阅 最佳实践。

28.3. HELM CHART 的存储库信息

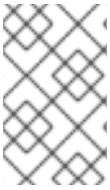
通过外部 Helm Chart 仓库发布

当您验证 Helm chart 时，会在红帽生态系统目录中发布以及以下详情。

在以下字段中输入所需详情：

字段名称	描述
Chart 名称	Helm Chart 的唯一名称
容器 registry 命名空间	创建容器时设置的 registry 名称。当容器发布时，此字段变得不可编辑。
Helm Chart 仓库	它表示 Helm Chart 仓库的位置。
用户访问 Helm chart 的任何其他说明	此信息将在红帽生态系统目录中发布。
公共 PGP 密钥	它是可选字段。如果要签署您的认证测试结果，请输入密钥。
授权 GitHub 用户帐户	它表示允许代表您公司提交 Helm chart 进行认证的 GitHub 用户。
简短和长存储库描述	在 Red Hat Ecosystem Catalog 上列出 Helm chart 时，将使用此信息。

配置所有必需字段后，单击 **Save。**



注意

所有标有星号 * 的字段都是必需的，您必须先完成，然后才能继续 Helm Chart 认证。

28.4. HELM CHART 的组件详情

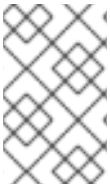
使用此选项卡配置产品组件详情。

在以下字段中输入所需详情：

字段名称	描述
应用程序类别	选择您的软件产品相应的应用程序类型。
项目名称	用于内部目的的项目名称。

配置所有必需字段后，单击 **Save**。

28.5. HELM CHART 的联系信息



注意

为这个选项卡提供信息是可选的。

在 联系人信息 选项卡中，输入您的产品组件的主要技术联系人详细信息。

1. 可选：在 技术联系电子邮件地址 字段中，输入镜像维护人员的电子邮件地址。
2. 可选： 要为您的组件添加额外的联系人，请点 + Add new contact。
3. 点击 **Save**。

28.6. HELM CHART 的相关产品

相关产品选项卡提供与您的产品组件关联的产品列表以及以下信息：

- 产品名称
- 类型 - 传统应用程序
- visibility - 发布或未发布
- 最后活动 - 运行测试前的天数

要在组件中添加产品，请执行以下操作：

- 如果要按名称查找产品，请在 **Search by name** 文本框中输入产品名称，然后点击搜索图标。

- 如果您不确定产品名称，请单击 **Find a product**。在 **Add product** 对话框中，从 **Available products** 列表中选择所需的产品，然后点转发箭头。所选产品被添加到 **Chosen** 产品列表中。单击 **Update attached products**。添加的产品列在相关的产品列表中。

注意

所有标有星号 * 的字段都是必需的，您必须先完成，然后才能继续认证。

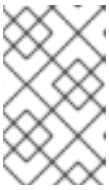
第 29 章 提交 HELM CHART 以进行认证

在 Red Hat Partner Connect 上配置和设置 Helm chart 组件后，通过创建一个红帽 OpenShift Helm Chart 仓库的拉取请求来提交您的 Helm chart 以进行认证。在拉取请求中，您可以包含 chart 或 chart-verifier 工具 生成的报告。根据拉取请求的内容，chart 将会被认证，如果未提供报告，则 chart-verifier 将运行。

先决条件

在创建拉取请求前，请确保满足以下先决条件：

1. 对 红帽的 OpenShift Helm Chart 仓库进行分叉，并将其克隆到本地系统。在这里，您可以在合作伙伴的 目录下看到为您的公司创建的目录。



注意

目录名称与您在认证容器时设置的容器 registry 命名空间相同。

在您的公司目录中，您在上一步中创建的每个 Chart 认证组件都会有一个子目录。要验证是否正确设置了此设置，请查看 OWNERS 文件。OWNERS 文件会在您的机构目录中的 chart 目录中自动创建。它包含有关组件的信息，包括授权代表您公司认证 Helm chart 的 GitHub 用户。您可以在位置 chart/ Partners/acme/awesome/OWNERS 中找到该文件。如果要编辑 GitHub 用户详情，请导航至 Settings 页面。

例如，如果您的组织名称是 acme，并且 Chart 名称是非常繁琐的。OWNERS 文件的内容如下：

```
chart:
  name: awesome
  shortDescription: A Helm chart for Awesomeness
publicPgpKey: null
providerDelivery: False
users:
  - githubUsername: <username-one>
  - githubUsername: <username-two>
vendor:
  label: acme
  name: ACME Inc.
```

您提交的 chart 的名称必须与 OWNERS 文件中的值匹配。

2. 在提交 Helm Chart 源或 Helm Chart 验证报告前，请使用其版本号创建一个目录。例如，如果您要发布 awesome chart 的 0.1.0 版本，请按如下所示创建一个目录：

```
charts/partners/acme/awesome/0.1.0/
```

注意

对于代表红帽支持的产品的图表，请使用位于 chart 的 OWNERS 文件(chart)提交对主分支的拉取请求，您的机构目录中可用的 redhat 目录。例如，对于名为 awesome 的红帽图表，请将拉取请求提交到位于 chart/redhat/awesome/OWNERS 的主分支。请注意，对于红帽支持的组件，您的机构名称是 redhat。

流程

您可以使用三种方法提交 Helm chart 以进行认证：

1. 提交没有 chart 验证报告的 Helm chart
2. 提交没有 Helm chart 的 chart 验证报告
3. 提交 chart 验证报告以及 Helm chart

29.1. 提交没有 CHART 验证报告的 HELM CHART

您可以以两种不同的格式提交您的 Helm chart 以进行认证，而无需 chart 验证报告：

29.1.1. 作为 tarball 进行图表

如果要将 Helm chart 提交为 tarball，您可以使用 Helm package 命令创建 Helm chart 的 tarball，并将其直接放在 0.1.0 目录中。

例如，如果您的 Helm Chart 对于 一个机构 acme来说非常困难

```
charts/partners/acme/awesome/0.1.0/awesome-0.1.0.tgz
charts/partners/acme/awesome/0.1.0/awesome-0.1.0.tgz.prov
```

29.1.2. 目录中的 chart

如果要在目录中提交 Helm chart，请将 Helm chart 放在带有 chart 源的目录中。

如果您签署了 chart，请将 providence 文件放在同一目录中。您可以在 OWNERS 文件中包括 chart 的 base64 编码公钥。当 base64 编码的公钥存在时，当使用 chart-verifier 为 chart 创建报告时，密钥将被解码并指定。

如果公钥与 chart 不匹配，verifier 报告将包含检查失败，拉取请求将以错误结尾。

如果公钥与 chart 匹配且没有其他故障，则会创建一个发行版本，该发行版本将包括 tarball、提供文件、公钥文件和生成的报告。

例如，

```
awesome-0.1.0.tgz
awesome-0.1.0.tgz.prov
awesome-0.1.0.tgz.key
report.yaml
```

如果 OWNERS 文件不包含公钥，则会跳过 chart verifier 检查，不会影响拉取请求的结果。此外，该公钥文件将不会包含在发行版中。

如果 chart 是 chart 源的目录，请创建一个 src 目录来放置 chart 源。

例如，

路径 可以是 chart/partners/acme/awesome/0.1.0/src/

文件结构可以是

```
.
└── src
    ├── Chart.yaml
    ├── README.md
    ├── templates
    │   ├── deployment.yaml
    │   ├── _helpers.tpl
    │   ├── hpa.yaml
    │   ├── ingress.yaml
    │   ├── NOTES.txt
    │   ├── serviceaccount.yaml
    │   ├── service.yaml
    │   └── tests
    │       └── test-connection.yaml
    ├── values.schema.json
    └── values.yaml
```

29.2. 提交没有 HELM CHART 的 CHART 验证报告

使用 chart-verifier 工具生成报告，并将它以文件名 report.yaml 保存到 0.1.0 目录中。您可以提交两种类型的报告：

29.2.1. 提交已签名报告

在提交报告以进行认证前，您可以在 chart 验证报告中添加 PGP 公钥。添加 PGP 公钥 是可选的。当将其添加到报告中时，您可以在您的机构目录中的 chart 目录下的 OWNERS 文件中找到您的公钥。PGP 公钥位于 publicPgpKey 属性中。此属性的值必须遵循 ASCII armor 格式。

在提交 chart 验证报告时，您可以在没有 chart 的情况下为报告签名，并以 ASCII armor 格式 签名。

例如，

```
gpg --sign --armor --detach-sign --output report.yaml.asc report.yaml
```

注意

如果签名验证失败，您可以在控制台中看到警告信息。

29.2.2. 为签名 chart 提交报告

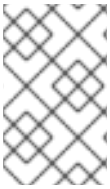
对于为签名 chart 提交 chart 验证报告，当您在生成报告时向 Chart verifier 工具提供 PGP 公钥时，它包含密钥摘要以及报告。

另外，当您将 base64 编码的 PGP 公钥添加到 OWNERS 文件时，将进行检查来确认 OWNERS 文件中解码的密钥摘要是否与报告中的密钥摘要匹配。

当不匹配时，拉取请求会失败。但是，如果密钥摘要与报告匹配，且处理拉取请求时没有其他错误，则会生成包含公钥和报告的版本。

例如，

```
awesome-0.1.0.tgz.key
report.yaml
```



注意

如果您启用了供应商控制交付，则不会生成发行版本。

29.3. 提交 CHART 验证报告以及 HELM CHART

您还可以提交图表以及报告。按照 Submitting a Chart without Chart Verification Report 步骤，将源或 tarball 放在版本号目录中。同样，请按照 在没有 Chart 的情况下提交 Chart 验证报告 中的步骤，并将 report.yaml 文件放在相同的版本号目录中。

29.3.1. 提交已签名报告

您可以签署报告并提交进行验证。如果签名验证失败，您可以在控制台中看到警告信息。如需更多信息，请参阅"提交签名报告"部分，在没有 Chart 的情况下提交 Chart 验证报告。

29.3.2. 提交签名的 Helm chart

对于签名的图表，除了报告文件外，还必须包括一个 tarball 和一个 providesnce 文件。如需更多信息，请参阅" 在没有 Chart 的情况下提交 Chart 验证报告中的"提交 签名 chart"部分。

29.4. 认证提交选项概述

根据您要访问 chart 以及检查 chart 在本地环境中是否有一些依赖项，请按照表总结了提交 Helm chart 的情况。

目标	包含 Helm chart	包括 chart 验证报告	红帽认证结果	发布您的认证 Helm chart 的方法
如果要执行以下操作： • 在 **charts.openshift.io** 中保存您的认证图表。 • 充分利用 Red Hat CI 进行持续图表测试	是	否	chart-verifier 工具在红帽 CI 环境中执行，以确保合规性。	您的客户可以从 chart. **openshift.io** 下载经过认证的 **Helm chart**。
如果要执行以下操作： • 在 **charts.openshift.io** 中保存您的认证图表。 • 旨在测试您自己的环境中的图表，因为它有一些外部依赖项。	是	是	红帽认证团队会审查结果以确保合规性。	您的客户可以从 chart. **openshift.io** 下载经过认证的 **Helm chart**。
如果您不想在 **charts.openshift.io** 中保存您的认证图表。	否	是	红帽认证团队会审查结果以确保合规性。	您的客户可以从您指定的 Helm Chart 仓库下载认证的 Helm chart。在 **charts.openshift.io** 的 **index.yaml** 文件中添加了一个对应的条目。

29.5. 验证步骤

提交拉取请求后，需要几分钟才能运行所有检查，并自动合并拉取请求。提交拉取请求后执行以下步

骤：

1. 检查新拉取请求中的任何消息。

2. 如果您看到错误消息，请参阅 故障排除 Pull Request Failures。使用必要的更改相应地更新拉取请求，以更正问题。

3. 如果您看到成功消息，这表示 Chart 存储库索引已被成功更新。您可以通过检查 gh-pages 分支中的最新提交来验证它。提交消息采用以下格式：

   > <partner-label>-<chart-name>-<version-number> index.yaml (#<PR-number>) (e.g, acme-psql-service-0.1.1 index.yaml (#7)).

   您可以在 index.yaml 文件中看到与 chart 相关的更改。

4. 如果您提交了一个 chart 源，则 GitHub 发行页中提供了带有 chart 和对应报告的 GitHub 发行版本。release 标签采用以下格式： < partner-label>-<chart-name>-<version-number>（例如 acme-psql-service-0.1.1）。

5. 您可以在 红帽官方 Helm Chart 仓库中找到经过认证的 Helm chart。按照以下列出的说明，在 OpenShift 集群上安装经过认证的 Helm chart。

第 30 章 发布认证的 HELM CHART

当您通过拉取请求提交 Helm chart 进行验证时，红帽认证团队会检查并验证您的组件是否有认证。验证成功后，您的 Helm Chart 通过 GitHub 认证。

按照以下步骤发布您的认证 Helm chart：

1. 访问 合作伙伴连接 网页。My Products 网页显示 产品列表。
2. 导航到 Product Listings 选项卡，再搜索所需的产品列表。
3. 单击您要发布的新创建的产品列表。检查您的产品列表的所有详细信息。
4. 转至 Components 选项卡。
5. 点 Add component 并进入 Existing component 选项卡，将您的认证的 Helm chart 附加到此列表中。另外，添加 Helm Chart 使用的认证容器。这两个组件都必须处于 Published 状态。

   当您指定产品列表的所有所需信息以及附加的组件时，会启用 Publish 按钮。
6. 单击 Publish。

您的经认证的 Helm Chart 现在可在 红帽生态系统目录 上公开访问。

部分 V. OPENSHIFT 徽标的功能认证：最佳实践、CNF、CNI、CSI

Red Hat OpenShift 认证徽标扩展 Red Hat OpenShift Operator 认证。认证徽标基于容器和操作员认证的基础而构建。

通过获得 Red Hat OpenShift 认证 Badge，合作伙伴可以确认其解决方案已启用 Kubernetes，满足 Kubernetes 最佳实践，并利用特定的 Kubernetes API 来解决相应的用例。

可用的当前 OpenShift 认证徽标如下：

- 满足最佳实践- 满足 Red Hat OpenShift 上部署的云原生软件产品的红帽最佳实践检查点。
- Cloud-Native Network Function (CNF)- 作为容器部署的电信功能实施。
- Container Network Interface (CNI)- 通过可插拔框架提供网络服务。
- Container Storage Interface (CSI) - 用于为 Red Hat OpenShift 提供和支持块或文件持久性存储后端。

第 31 章 满足最佳实践

31.1. 在云原生软件认证中满足最佳实践

Meet s 最佳实践 徽标是 Red Hat OpenShift 工作负载认证中的一个可选分类，它表示您的产品遵循 Red Hat OpenShift 软件认证的容器化应用程序的最佳实践。

这些最佳实践包括一系列检查，用来验证您提交给认证的 helm chart 和 operator，满足在 Red Hat OpenShift 上部署的标准准则。在成功验证认证产品后，会在 红帽生态系统目录 中使用 Meet s 最佳实践 徽标列出。

注意

红帽建议您在开始认证过程前具有红帽认证工程师或具有同等经验。

认证工作流包括以下阶段：

- 认证加入
- 创建产品
- 添加组件
- 认证和测试
- 在红帽生态系统目录中发布产品列表

31.2. 认证加入

1. 加入 Red Hat Partner Connect for Technology Partner Program。
2. 同意 计划条款和条件。

3. 填写 您的公司简介。

有关详细信息，请参阅 概述。

31.3. 创建产品

有关创建产品列表的详细信息，请参阅创建产品列表。

31.4. 添加组件

1. 对于 Operator，请参阅为 Operator 添加认证组件。

2. 对于 Helm chart，请参阅为 Helm chart 添加认证组件。

31.5. 认证和测试

流程

1. 进入 Components 选项卡 > Optional Qualifications

2. 单击 Start Testing。

3. 点 Go to Red Hat Certification 工具。创建了一个新的功能认证，之后，您将在红帽 合作伙伴认证 (rhcert)门户上重定向到您的组件页面。

4. 在您的 测试环境中使用您的产品，运行适用于 Kubernetes 的红帽最佳实践 测试套件。它由一系列从我们的合作伙伴建立的最佳实践派生出的一系列测试案例组成。测试套件将评估您的产品是否遵循这些原则并满足红帽标准。

5. 在 Red Hat Partner Certification (rhcert)门户的产品组件页面中执行以下步骤：

   a. 进入 Summary 选项卡：

i. 从 Files 部分，单击 Upload，以提交您的产品认证结果。选择 claim .json 和 tnf_config.yml 文件。然后，单击 Next。此时会显示成功上传信息。

ii. 可选：在 讨论 文本框中添加与认证相关的查询（若有），然后点 Add Comment。红帽认证团队将为您的查询提供说明。

b. 进入 Properties 选项卡：

i. 点 Platform 列表菜单选择要在其上认证您的组件的平台。例如，x86_64

ii. 点 Product Version 列表菜单选择您要在其上认证您的组件的红帽产品版本。例如，Red Hat OpenShift Platform

iii. 单击 Update Values。所选值已更新。

31.6. 在红帽生态系统目录中发布产品列表

当您通过红帽认证门户提交您的产品进行验证时，红帽认证团队将检查并验证您的产品进行验证。验证成功后，您的认证产品会通过 Meet s 最佳实践 标签在红帽生态系统目录中发布。

流程

1. 访问 合作伙伴连接 网页。My Products 网页显示 产品列表。
2. 搜索您要发布的新创建的产品列表，单击并查看其详细信息。
3. 进入 Components 选项卡，点 Add component 将认证 operator 或 Helm chart 附加到此列表。另外，添加由您的产品组件使用的额外认证容器。所有组件都必须处于 Published 状态。当您完成产品列表的所有所需信息以及附加的产品组件时，会启用 Publish 按钮。
4. 单击 Publish。

您的已认证产品现在可在 红帽生态系统目录 上公开访问。认证的产品也会在 OpenShift 的 Web 控制台的 OperatorHub 中列出。合作伙伴将收到 最佳实践徽标，以便在 Red Hat OpenShift 平台上推广其经过认证的产品。

注意

Red Hat OpenShift 软件认证测试不会在 Operator 和 Helm Chart 构造外对产品进行功能测试。另外，它不会测试您的产品对安装和执行它的红帽平台的影响。认证候选产品质量保证的所有方面均保留合作伙伴的职责。

第 32 章 CNF 认证和供应商验证

32.1. 使用 CLOUD-NATIVE NETWORK FUNCTION (CNF)认证

32.1.1. Cloud-native 网络功能简介

云原生网络功能虚拟化(CNF)是经典物理或虚拟网络功能(VNF)的容器化实例，它们被放入支持弹性、生命周期管理、安全性、日志记录和其他功能的微服务中。

CNF 徽标是 Red Hat OpenShift 认证中的分类。它可供使用 Red Hat OpenShift 作为部署平台以容器格式提供的网络功能的产品使用。红帽提供两级 CNF 认证：

- Vendor Validation - 如果您的容器基础镜像不是 RHEL 和 UBI，请选择这类 CNF 认证。对于这类认证，供应商通过在红帽生态系统目录中将其作为厂商验证的 CNF 产品发布之前，在内部测试您的 CNF 产品。
- 认证的 CNF - 如果您的容器基础镜像是 RHEL 或 UBI，请选择这类 CNF 认证。对于这类认证，Vendor 验证您的 CNF 产品，在您的工作负载上运行认证测试，然后提交以进行验证。在成功验证 CNF 产品后，红帽生态系统目录中将 CNF 产品列为认证的 CNF 产品。

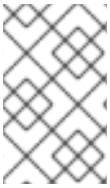
满足要求并完成红帽生态系统目录上列出的认证工作流的产品，并与 CNF 徽标来标识。合作伙伴将收到徽标以推广其产品认证。

其他资源

- 有关 CNF 的更多信息，请参阅：
  - CNF 和 VNF 认证
  - 关于云原生网络功能
  - 使用 OpenShift Pipelines 构建 CNF 应用程序
- 要了解有关 Vendor Validated CNF 和经认证的 CNF 的优点的更多信息，请参阅 云原生网络功能(CNF)。

- 要了解获得 CNF 认证的要求，请参阅 CNF 的要求。
- 要了解有关 OLM 和 SDK 项目的最佳实践和常见建议的更多信息，请参阅 Operator 最佳实践。

32.1.2. CNF 的认证工作流



注意

红帽建议您在开始认证过程前具有红帽认证工程师或具有同等经验。

任务摘要

认证工作流包括以下三个主要阶段：

1. 第 32.1.2.1 节 “cnf 的认证加入”
2. 第 32.1.2.2 节 “完成 cnf 的产品列表”
3. 第 31.6 节 “在红帽生态系统目录中发布产品列表”

32.1.2.1. cnf 的认证加入

执行认证加入概述的步骤：

1. 加入 Red Hat Connect for Technology Program （ Red Hat Connect for Technology Program (Red Hat Connect for Technology Program)
2. 同意计划条款和条件。

3. 选择所需产品类别来创建您的产品列表。您可以从可用产品类别中选择：

   a. 容器化应用程序

   b. 独立应用程序

   c. OpenStack Infrastructure

4. 填写您的公司简介。

注意

为每个合作伙伴产品版本及其相应的红帽基础版本创建单独的 CNF 组件。如果要认证 CNF 组件，请为每个附加的 CNF 组件（如容器镜像和 Operator 捆绑包或 Helm Chart）创建单独的 CNF 组件。

其他资源

有关创建 CNF 产品的详细信息，请参阅创建产品列表。

32.1.2.2. 完成 cnf 的产品列表

执行完成清单概述的步骤：

1. 为您的验证提供详情。

2. 验证 Red Hat OpenShift 上 CNF 的功能进行供应商验证。

3. 完成产品列表详情，以认证您的 CNF 组件。

4. 将组件添加到产品列表中。

5. 为您的产品列表认证组件。

其他资源

有关完成产品列表的详情，请参阅 添加认证组件。

32.1.2.3. 在红帽生态系统目录中发布产品列表

认证或 供应商验证的 CNF 组件必须添加到 Red Hat Partner Connect 门户的产品列表页面中。发布后，您的产品列表将在 红帽生态系统目录 上显示，使用您提供的产品信息。您可以使用相应的标签在 红帽生态系统目录 中发布 Vendor Validated 和 Certified CNF 产品。

其他资源

- 有关发布 CNF 组件的详情，请参阅在红帽生态系统目录上发布产品列表。

32.2. 创建产品

产品列表提供营销和技术信息，向潜在客户展示您的产品功能和优势。它将为产品添加所有必要组件以进行认证的基础。

先决条件

在继续认证过程前，请确保您的产品满足以下要求：

- 您的产品通常可用于公共访问
- 您的产品已在 Red Hat OpenShift 中经过测试并部署
- 您的产品在 Red Hat OpenShift 中受到商业支持

除了特定认证测试要求外，还验证您的产品在红帽平台上的功能。如果在目标红帽平台上运行您的产品产生了子标准体验，则必须在认证前解决问题。

流程

红帽建议完成列表选项卡中的所有可选字段，以获取全面的产品列表。如需更多信息，可以帮助相互客户做出明智的选择。

在为您的产品列表输入信息时，红帽鼓励与您的产品经理、营销代表或其他产品专家合作。

带有星号 packagemanifests 的字段是必需的。

流程

1. 登录到 Red Hat Partner Connect Portal。
2. 进入认证技术门户选项卡，然后单击门户。
3. 在标题栏中，单击 产品管理。
4. 从 Listing and Certification 选项卡中，单击 Manage products。
5. 在 My Products 页面中，单击 Create Product。

   此时会打开 Create New Product 对话框。
6. 输入 产品名称。
7. 从 您要认证的产品中选择 所需的产品类别，然后单击 Create product。例如，选择 Containerized Application 来创建容器化产品列表。

   此时会打开带有您的 产品名称的新页面。它由以下标签页组成：

- 第 32.2.1 节 “CNF 概述”
- 第 32.2.2 节 “CNF 的产品信息”
- 第 32.2.3 节 “CNF 的组件”
- 第 32.2.4 节 “支持 CNF”

除了以下选项卡外，页面标头还提供 产品分数 详细信息。产品分数评估您的产品信息并显示分数。它可以是：

- 公平
- 良好
- 非常好
- best

8. 点 How do improve my score? 以改进您的产品分数。

9. 提供产品列表详情后，请单击 Save，然后移至下一部分。

32.2.1. CNF 概述

此选项卡由一系列任务组成，您必须完成才能发布您的产品：

- 第 32.2.1.1 节 “CNF 的完整产品列表详情”

- 第 32.2.1.2 节 “CNF 的完整公司配置文件信息”
- 第 32.2.1.3 节 “接受 CNF 的法律协议”
- 第 32.2.1.4 节 “为 CNF 添加至少一个产品组件”
- 第 32.2.1.5 节 “为您的 CNF 列表认证组件”

32.2.1.1. CNF 的完整产品列表详情

1. 要完成您的产品列表详情，请点 Start。

   此时会打开 Product Information 选项卡。

2. 输入所有基本产品详情并点 Save。

32.2.1.2. CNF 的完整公司配置文件信息

1. 要完成您的公司概况信息，请单击 Start。输入所有详情后，单击 Submit。
2. 要修改现有的详情，请点 Review。此时会打开 Account Details 页面。
3. 检查和修改 Company 配置集信息，然后单击 Submit。

32.2.1.3. 接受 CNF 的法律协议

要发布您的产品镜像，请同意有关合作伙伴容器镜像的发布条款。

1. 要接受法律协议，请点击 Start。
2. 要预览或下载协议，请点 Review。

此时会显示 Red Hat Partner Connect Container 附录 文档。阅读文档，了解与容器镜像分发相关的术语。

32.2.1.4. 为 CNF 添加至少一个产品组件

1. 点 Start。您将被重定向到 Components 选项卡。

   要添加新或现有产品组件，请点 Add component。

2. 用于添加新组件，

   a. 在 Component Name 文本框中，输入组件名称。此名称没有发布，仅用于内部使用。

   注意

   红帽建议在组件名称中包含产品版本，以方便地识别新创建的 CNF 组件。例如，&lt ;CompanyName ProductName> 1.2 - OCP 4.12.2）

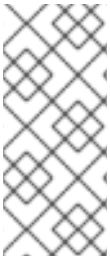
   b. 对于您要创建的 OpenShift 组件，请选择您要认证的组件。例如，要认证您的 CNF，请选择 Cloud Native Function (CNF)。

   c. 单击 Create new component。

3. 要添加现有组件，请从 Add 组件 对话框中选择 Existing Component。

   a. 从 Available components 列表中，搜索并选择您要认证的组件，然后点转发箭头。所选组件被添加到 Chose n 组件 列表中。

   b. 单击 Attach existing component。



注意

为每个合作伙伴产品版本及其相应的红帽基础版本创建单独的 CNF 组件。另外，还创建并附加认证组件，如容器镜像和操作器捆绑包或 Helm chart，它们是认证所需的。您可以为产品创建多个 CNF 组件。

32.2.1.5. 为您的 CNF 列表认证组件

1. 要为您的列表认证组件，请单击 **Start**。如果您有现有的产品组件，您可以查看 **Attached** 组件 列表及其详情：

   a. **Name**

   b. 认证

   c. **安全性**

   d. 类型

   e. **Created**

   f. 点击更多选项归档或删除组件

2. 选择用于认证的组件。

完成上述所有任务后，您将看到与所有选项相对应的绿色勾号标记。

Overview 选项卡还提供以下信息：

1. 产品联系人 - 提供产品营销和技术联系信息。

   a. 点 **Add contacts to product** 以提供联系信息

b. 点 Edit 以更新信息。

2. 产品中的组件 - 提供附加到产品的组件列表及其最后的更新信息。

a. 点 Add components to product 将新的或现有组件添加到您的产品中。

b. 点 Edit components 更新现有组件信息。

发布产品列表后，您可以查看您的产品 就绪情况和 方式，以便在 Overview 选项卡上提高分数。

32.2.2. CNF 的产品信息

通过此选项卡，您可以提供有关您产品的所有重要信息。产品详情会在红帽生态系统目录中与您的产品一起发布。

常规 标签页：

提供产品的基本详情，包括产品名称和描述。

1. 输入 产品名称。

2. 可选：根据 定义的准则上传产品徽标。

3. 输入 Brief 描述 和长 描述。

4. 点击 Save。

功能和好处 选项卡：

提供您产品的重要特性。

1. 可选：输入 Title 和 Description。

2. 可选： 要为您的产品添加额外的功能，请点 + Add new feature。

3. 点击 Save。

快速启动和配置标签页 ：

添加指向任何快速入门指南或配置文档的链接，以帮助客户部署并开始使用您的产品。

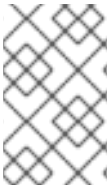
1. 可选：输入 Quick start 和 configuration instructions。

2. 点击 Save。

3. 如果您不想显示它们，请选择 Hide default instructions 复选框。

链接的资源 标签页：

添加支持文档的链接，以帮助我们的客户使用您的产品。这些信息被映射到，并在产品目录页面中的 Documentation 部分显示。



注意

必须至少添加三个资源。如果可用，红帽建议您添加更多资源。

1. 选择 Type 下拉菜单，并输入资源的 Title 和 Description。

2. 输入 资源 URL。

3. 可选： 要为您的产品添加其他资源，请点 + Add new Resource。

4. 点击 Save。

常见问题解答 标签页：

添加常见问题以及产品用途、操作、安装或其他属性详情的回答。您可以包括有关您的产品和服务的常见客户查询。

1. 输入问题 和 answer。

2. 可选： 要为您的产品添加额外的常见问题，请点 + Add new FAQ。

3. 点击 Save。

支持 标签：

此选项卡可让您提供支持团队的联系信息。

1. 输入 支持 描述、支持网站、支持电话号码 以及支持电子邮件地址。

2. 点击 Save。

Contacts 标签页：

请提供营销和技术团队的联系信息。

1. 输入 营销联系人电子邮件地址 及 技术联系电子邮件地址。

2. 可选： 要添加其他联系人，请点 + Add another。

3. 点击 Save。

法律 选项卡：

提供产品相关的许可证和策略信息。

1. 输入 产品和隐私策略 URL 的 许可证协议 URL。

2. 点击 Save。

SEO 标签页：

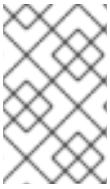
使用此选项卡提高我们相互客户的可发现性，提高红帽生态系统目录搜索和互联网搜索引擎中的可见性。提供更多搜索别名（密钥和证书对）会增加产品的可发现性。

1. 选择 产品类别。

2. 输入 Key 和 Value 来设置搜索别名。

3. 点击 Save。

4. 可选： 要添加额外的键值对，请点 + Add new key-value pair。



注意

为您的产品至少添加一个搜索别名。如果可用，红帽建议您添加更多别名。

32.2.3. CNF 的组件

使用此选项卡将组件添加到您的产品列表中。通过此选项卡，您还可以查看链接到您的产品列表的附加组件列表。

另外，要将组件附加到产品列表，您可以完成 Container、Operator 或 Helm Chart 产品列表的 Overview 选项卡中提供的 Add least one product component 选项。

1. 要添加新或现有产品组件，请点 Add component。
2. 用于添加新组件，
   a. 在 Component Name 文本框中，输入组件名称。
   b. 在 Component Name 文本框中，输入组件名称。此名称没有发布，仅用于内部使用。

注意

红帽建议在组件名称中包含产品版本，以方便地识别新创建的 CNF 组件。例如，&lt ;CompanyName ProductName> 1.2 - OCP 4.12.2）

   c. 对于您要创建的 OpenShift 组件，请选择您要认证的组件。例如，要认证您的 CNF，请选择 Cloud Native Function (CNF)。
   d. 单击 Create new component。
3. 要添加现有组件，请从 Add 组件 对话框中选择 Existing Component。
   a. 从 Available components 列表中，搜索并选择您要认证的组件，然后点转发箭头。所

选组件被添加到 Chose n 组件 列表中。

b. 单击 **Attach existing component**。

注意

您可以将一个组件添加到多个产品列表中。所有附加的组件都必须发布，然后才能发布产品列表。

附加组件后，您可以查看 Attached 组件 列表及其详情：

i. **Name**

ii. 认证

iii. **安全性**

iv. 类型

v. **Created**

vi. 点击更多选项归档或删除附加的组件

或者，要搜索特定组件，请在 Search by component Name 文本框中键入组件的名称。

32.2.3.1. 为您的列表认证组件

1. 要为您的列表认证组件，请单击 **Start**。如果您有现有的产品组件，您可以查看 **Attached** 组件 列表及其详情：

a. **Name**

b. 认证

c. **安全性**

d. 类型

e. **Created**

f. 点击更多选项归档或删除组件

2. 选择用于认证的组件。

32.2.4. 支持 CNF

红帽合作伙伴加速服务(PAD)是一个产品和技术级别合作伙伴帮助台服务，允许当前和潜在合作伙伴提供与红帽产品、合作伙伴认证、产品认证、服务流程等相关的非技术问题。

您还可以联系红帽合作伙伴加速服务，以了解您可能对认证可能遇到的任何技术问题。技术帮助请求将重定向到认证运营团队。

通过合作伙伴订阅计划，红帽提供免费的、不用于销售的软件订阅，您可用来在目标红帽平台上验证您的产品。要请求访问此计划，请按照 合作伙伴订阅 网站上的说明进行操作。

1. 要请求支持，请点击 Open a support case。请参阅 PAD - 如何打开和管理 PAD 问题单，以创建一个 PAD ticket。

2. 要查看现有支持问题单的列表，请点 View 支持问题单。

32.2.5. 删除产品

如果要删除产品列表后，请转到 Overview 选项卡，再单击 Delete。

先发布的产品必须取消发布，然后才能删除。即使删除该产品后，红帽仍然保留与已删除产品相关的信息。

32.3. 添加认证组件

创建新产品列表后，为新创建的产品列表添加认证组件。

您可以为新添加的组件配置以下选项：

注意

组件配置因不同的产品类别而异。

- 第 32.3.1 节 “CNF 认证”
- 第 32.3.2 节 “CNF 的组件详情”
- 第 32.3.3 节 “CNF 的联系信息”
- 第 32.3.4 节 “CNF 的关联产品”

32.3.1. CNF 认证

使用 Certification 选项卡验证并认证 Red Hat OpenShift 中 CNF 的功能。

32.3.1.1. 在 Red Hat OpenShift 中验证 CNF 的功能

通过使用此功能，Red Hat CNF 认证团队会检查您的产品是否满足供应商验证的所有标准。

要验证 CNF 组件的功能，请执行以下操作：

1. 选择这个选项并点 Start questionnaire。显示 CNF questionnaire 页面。

2. 输入您的所有产品和公司信息。

3. 填写所有详细信息后，单击 Submit。

4. 要修改现有的详情，请点 Review。显示 CNF questionnaire 页面，供您查看和修改输入的信息。

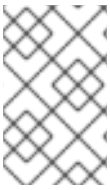
单击 Submit 后，将创建一个新的功能认证请求。红帽 CNF 认证团队将审核并验证所输入的 CNF 问题详情。成功审核和验证后，您的功能认证请求将获得批准，产品列表中的 认证级别 字段将设置为 Vendor Validated。

完成每个步骤后，每个标题旁边会显示一个绿色勾号，表示特定的配置项目已完成。当所有项目在清单中完成时，预公开清单 左侧的披露将被关闭。

其他资源

有关验证过程的详细信息，请参阅 CNF 工作流。

32.3.1.2. 在 Red Hat OpenShift 上认证 CNF 的功能



注意

只有在您要认证厂商验证的 CNF 组件时，才选择这个选项。

这是一个可选功能，允许您使用 Red Hat 认证工具认证您的 Vendor Validated 组件。对于每个供应商验证的组件，将在红帽合作伙伴认证门户上创建一个新的功能认证请求。当您请求认证时，您的功能认证请求将由 CNF 团队处理，以进行认证。

如果您认证了 Vendor Validated CNF 组件，它将在 红帽生态系统目录 中显示，并带有 认证 标签。

先决条件

1. 在继续认证前，完成产品列表。

2. 在提交 CNF 组件以进行认证前，请认证附加的容器镜像、operator 捆绑包或 helm chart。

流程

要认证您的厂商验证的 CNF 组件，请执行以下步骤：

1. 进入 Certification 选项卡，并从 Certify Red Hat OpenShift 标题的 CNF 的功能，点 Start。创建了一个新的功能认证请求，并将在红帽 合作伙伴认证 (rhcert)门户上重定向到您的组件。

2. 为 Kubernetes 运行红帽最佳实践测试套件，或使用 DCI OpenShift App Agent。它由一系列来自最佳实践的测试案例组成，以评估您的产品是否遵循这些原则并满足红帽认证标准。

3. 要认证您的 CNF 组件，请在 Red Hat Partner Certification (rhcert)门户的 CNF 组件页面中执行以下步骤：

   a. 进入 Summary 选项卡，

      i. 要提交您的产品认证测试结果，请从 Files 部分单击 Upload。选择 claim .json 和 tnf_config.yml 文件。然后，单击 Next。您可以看到成功上传消息。

      ii. 在讨论文本框中添加与认证相关的查询 (如果有)。

      iii. 点 Add Comment。通过使用这个选项，您可以将您的问题与红帽 CNF 认证团队沟通。红帽 CNF 认证团队将为您的查询提供说明。

   b. 在 Summary 选项卡中，

      .

i. 导航到 合作伙伴产品类别。

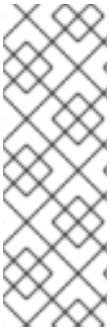
ii. 单击 合作伙伴 产品版本选项下面的编辑图标，以输入您的产品版本，然后单击复选标记按钮。您的产品版本被更新。

c. 导航到 Properties 选项卡，

i. 点 Platform 列表菜单选择要在其上认证 CNF 组件的平台。例如 - x86_64

ii. 点 Product Version 列表菜单选择您要在其上认证 CNF 组件的红帽产品版本。例如 - Red Hat OpenShift Platform

iii. 单击 Update Values。所选值已更新。



注意

所有版本的合作伙伴产品都未经过认证，可与每个版本的红帽产品一起使用。您需要使用所选的红帽基础版本认证您的产品的每个版本。例如，如果您使用 Red Hat OpenShift Container Platform 版本 4.13 认证您的产品版本 5.11，则只能使用 5.11 版本，而不是更新的版本。因此，使用最新版本的红帽基本产品单独认证您的产品的每个版本。

Red Hat CNF 认证团队将检查并验证 CNF 组件的详情。当红帽 CNF 认证团队通过 CNF 在推荐的最佳实践中识别问题或违反情况时，联合讨论将意味着找到补救选项和时间表。如果承诺解决已确定的发行目标或时间表的问题，该团队也会考虑临时异常。所有例外都会记录在 KIE 基础文章中，在 CNF 在红帽生态系统目录中列出所有不合规的项目，但技术详情将保持私有。

注意

在开始按规定的顺序认证 CNF 组件前，必须重新认证 CNF 产品中引用的所有容器、Operator 或 Helm chart。

在经过红帽 CNF 认证团队验证成功后，您的 Vendor Validated CNF 组件将获得认证，并将在 红帽生态系统目录 中带有 认证 标签自动发布。

其他资源

1. 有关 Kubernetes 的红帽最佳实践测试套件的更多信息，请参阅 概述 和测试 目录。

2. 有关安装和配置 DCI OpenShift App Agent 的更多信息，请参阅 DCI OpenShift App Agent。

32.3.2. CNF 的组件详情

使用此选项卡配置产品组件详情。

在以下字段中输入所需详情：

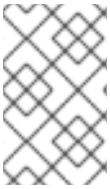
- 项目名称 - 输入项目名称。此名称没有发布，仅用于内部使用。

注意

红帽建议将产品版本包含在组件版本中，以方便地识别新创建的 CNF 组件。例如，&lt ;CompanyName ProductName> 1.2 - OCP 4.12.2）

- 点击 Save。

32.3.3. CNF 的联系信息



注意

为这个选项卡提供信息是可选的。

在 联系人信息 选项卡中，输入您的产品组件的主要技术联系人详细信息。

1. 可选：在 技术联系电子邮件地址 字段中，输入镜像维护人员的电子邮件地址。

2. 可选： 要为您的组件添加额外的联系人，请点 + Add new contact。

3. 点击 Save。

32.3.4. CNF 的关联产品

相关产品选项卡提供与您的产品组件关联的产品列表以及以下信息：

- 产品名称
- 类型 - 传统应用程序
- visibility - 发布或未发布
- 最后活动 - 运行测试前的天数

要在组件中添加产品，请执行以下操作：

- 如果要按名称查找产品，请在 Search by name 文本框中输入产品名称，然后点击搜索图标。
- 如果您不确定产品名称，请单击 Find a product。在 Add product 对话框中，从 Available products 列表中选择所需的产品，然后点转发箭头。所选产品被添加到 Chosen 产品列表中。单击 Update attached products。添加的产品列在相关的产品列表中。

注意

所有标有星号 * 的字段都是必需的，您必须先完成，然后才能继续认证。

32.4. 在红帽生态系统目录中发布产品列表

当您提交 CNF 组件进行验证时，红帽 CNF 认证团队将检查并验证输入的 CNF questionsnaire 的详

细信息。如果要认证您的 Vendor Validated CNF 组件，请完成认证详情。

红帽认证团队将审核提交的测试结果。验证成功后，若要在 红帽生态系统目录 上发布您的产品，请转至 Product Listings 页面，以附加 Vendor Validated 或 认证的 CNF 组件。

按照以下步骤发布您的产品列表：

1. 访问 Red Hat Partner connect 网页。My Product 网页显示 Product Listings。
2. 导航到 Product Listings 选项卡，再搜索所需的产品列表。
3. 单击您要发布的新创建的产品列表。检查您的产品列表的所有详细信息。
4. 转至 Components 选项卡。
5. 点 Add Component 将新组件添加到您的产品列表中。

注意

在发布您的产品版本和产品认证前，您必须发布所有附加的组件。

6. 点 Attach Component 将 Vendor Validated 或 Certified CNF 组件附加到此列表中。在附加认证的 CNF 组件时，必须添加经过认证的容器镜像以及 CNF 组件使用的 operator 捆绑包或 Helm chart。

注意

所有附加的组件都必须处于 Published 状态。

对于 Vendor Validated 组件，不需要这一步。当您指定产品列表的所有所需信息时，会启用 Publish 按钮，包括附加的组件。

7. 单击 **Publish**。

现在，通过 红帽生态系统目录 上的相应 厂商 验证或 经认证的 CNF 标签，提供了新的 CNF 产品列表。产品列表页面中的 认证 表显示以下详情：

- 产品 - 例如 Red Hat OpenShift Container Platform
- 版本 - 选择了红帽基本产品版本。例如，4.12 - 4.x
- 架构 - 例如，x86_64
- 合作伙伴产品版本 - 例如 5.11
- 认证类型 - 例如 RHOCP 4 CNF
- level - 例如，Vendor Validated 或 Certified

您需要使用所选的红帽基础版本认证您的产品的每个版本。因此，认证 表可以有同一红帽基础版本的多个版本的产品。例如，

产品	Version	架构	合作伙伴产品版本	认证类型	认证级别
Red Hat OpenShift Container Platform	4.12	x86_64	5.11	RHOCP 4 CNF	vendor Validated
Red Hat OpenShift Container Platform	4.12	x86_64	5.12	RHOCP 4 CNF	已认证

产品	Version	架构	合作伙伴产品版本	认证类型	认证级别
Red Hat OpenShift Container Platform	4.12	x86_64	5.13	RHOCP 4 CNF	已认证
Red Hat OpenShift Container Platform	4.12	x86_64	5.14	RHOCP 4 CNF	vendor Validated

32.5. 重新认证 CNF 软件包

重新认证工作流 与常规 CNF 认证工作流 类似。红帽建议在以下情况下更新您的应用程序：

- **在 Red Hat OpenShift Container Platform 的每个主发行版本中。**
- **在应用程序的每个主发行版本中。**

注意

要重新认证您的应用程序，必须创建新的认证请求以进行重新认证。

流程

1. **在 Red Hat Partner Connect 上创建一个新的 CNF 组件。**
2. **在 Project name 字段中，输入产品名称及其版本。例如 - &lt ;CompanyName ProductName> 1.2 - OCP 4.12.2**
3. **在 概述 选项卡中完成所有任务，但 CNF questionsnaire 除外，然后继续执行 常规 CNF 认证工作流，就像新的认证一样。**

4. 通过红帽 合作伙伴认证(rhcert)门户提交新的认证 请求。

注意

重新认证整个 CNF 软件包，并单独将每个 CNF 组件认证为独立的 CNF 组件。例如，如果您使用单独的 helm chart 或 Operator 部署了 CNF 应用程序，则必须单独对每个 CNF 进行重新认证。另外，如果您在同一个红帽产品版本中更新 CNF 产品的新版本，则不需要更新未验证的 CNF 镜像容器。

在经过红帽 CNF 认证团队验证成功后，您的 CNF 软件包的新版本会被重新认证，并将在红帽生态系统目录中带有 认证 标签自动发布。

第 33 章 CNI 认证

33.1. 使用 CONTAINER NETWORK INTERFACE (CNI)认证

注意

要认证 CNI 插件，必须将其配置为使用 Operator 部署和管理。在继续执行 Red Hat CNI 认证前，Operator 以及 CNI operator 捆绑包引用的所有容器（包括插件）必须在认证 CNI 插件前已在 红帽生态系统目录 中认证并发布。

33.1.1. 容器网络接口简介

Container Network Interface (CNI)是在 Linux 容器中配置网络接口的规格。它由一个规范和库组成，用于编写插件以在 Linux 容器中配置网络接口，以及多个支持的插件。CNI 主要用于将容器添加到网络、连接、删除和断开容器。

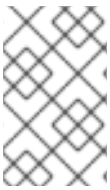
CNI 徽标是 Red Hat OpenShift 认证中的分类。它可供使用 Red Hat OpenShift 作为部署 平台的 CNI 插件实现 容器格式提供的网络功能的产品。

满足要求并完成认证工作流的产品可以在 Red Hat OpenShift Container Platform 上称为已认证 CNI。批准认证后，认证的 CNI 产品将在 红帽生态系统目录以及 Red Hat OpenShift Web 控制台中的 OperatorHub 上列出。认证的 CNI Operator 使用 CNI 徽标标识。合作伙伴将收到徽标以推广其产品认证。

其他资源

- 如需有关 CNI 的更多信息，请参阅：
  - 认证的 OpenShift CNI 插件
  - CNI 规格
  - Kubernetes 中 Container Network Interface (CNI)的简短概述
  - Kubernetes CNI

33.1.2. CNI 认证工作流



注意

红帽建议您在开始认证过程前具有红帽认证工程师或具有同等经验。

任务摘要

认证工作流包括三个主要步骤：

1. 第 33.1.2.1 节 “CNI 认证”
2. 第 33.1.2.2 节 “CNI 认证测试”
3. 第 31.6 节 “在红帽生态系统目录中发布产品列表”

33.1.2.1. CNI 认证

执行认证加入概述的步骤：

1. 加入 Red Hat Connect for Technology Program （ Red Hat Connect for Technology Program (Red Hat Connect for Technology Program)
2. 同意计划条款和条件。
3. 选择所需产品类别来创建您的产品列表。您可以从可用产品类别中选择：
   a. 容器化应用程序
   b. 独立应用程序

c. **OpenStack Infrastructure**

4. **填写您的公司简介。**

5. **将组件添加到产品列表中。**

6. **为您的产品列表认证组件。**

其他资源

有关创建产品列表的详细信息，请参阅创建产品列表。

33.1.2.2. CNI 认证测试

按照以下高级别步骤运行认证测试：

1. **派生红帽上游存储库。**

2. **在测试环境中安装并运行红帽认证管道。**

3. **查看测试结果并进行故障排除（如果遇到任何问题）。**

4. **通过拉取请求向红帽提交认证结果。**

其他资源

有关附加产品组件并验证 Red Hat OpenShift 中 CNI Operator 功能的详细信息，请参阅 添加认证组件。

33.1.2.3. 在红帽生态系统目录中发布产品列表

完成所有认证检查后，您可以向红帽提交测试结果。您可以根据您的个人目标打开或关闭此结果提交步骤。提交测试结果后，它会触发红帽基础架构来自动合并拉取请求并发布您的 Operator。

其他资源

有关在红帽生态系统目录上发布产品列表的详细信息，请参阅在红帽生态系统目录上发布产品列表。

33.2. 创建产品

有关创建产品列表的详细信息，请参阅创建产品列表。

33.3. 添加认证组件

有关附加产品组件并验证 Red Hat OpenShift 中 CNI Operator 功能的详细信息，请参阅 添加认证组件。

33.4. 使用 OPENSHIFT OPERATOR PIPELINE

在继续 CNI 认证前，按照步骤认证您的 Operator：

1. 添加 Operator 捆绑包
2. 分叉软件仓库
3. 安装 OpenShift Operator Pipeline
4. 执行 Openshift Operator 管道
5. 提交认证结果

客户通过嵌入式 OpenShift operatorHub 列出并消耗认证的 Operator，使他们能够轻松部署和运行解决方案。此外，您的产品和操作器镜像还将在 红帽生态系统目录 上列出。

33.5. 配置测试环境以运行 CNI 测试

在运行 CNI 测试前，请验证您用于运行 CNI 测试的 Red Hat OpenShift 环境是否满足以下条件：

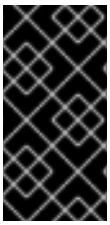
1. 在生命周期的完全支持阶段使用 Red Hat OpenShift 版本。红帽建议使用最新支持的版本。如需有关 OpenShift 发行版本的更多信息，请参阅 Red Hat OpenShift Container Platform 生命周期政策。

2. 仅使用记录的安装过程部署网络产品。

3. 安装 Red Hat OpenShift Virtualization。

4. 如果要测试 Service Mesh，请安装 Red Hat Service Mesh operator 和 Service Mesh Control Plane (SMCP)。

5. 配置可访问 OpenShift 集群的主机，以用作运行 CNI 认证测试的测试客户端。此环境必须包含 gcc,git, go, make, openssl 和 sonobuoy 等工具。



重要

在同一个配置上运行您自己的产品验证测试，以确保您的产品功能在 Red Hat OpenShift 环境中按预期工作。

Red Hat Partner Connect 提供对软件的免费访问，作为计划的好处。要了解如何获取 Red Hat OpenShift 环境订阅，请参阅 Red Hat 合作伙伴连接计划指南。

33.6. 运行 CNI 测试

1. 要运行 Red Hat OpenShift 网络一致性测试套件，请将 kubeconfig.yaml 文件放在当前工作目录中，并运行以下命令：

```
$ podman run -v `pwd`:/data:z --rm -it registry.redhat.io/openshift4/ose-tests sh -c
"KUBECONFIG=/data/kubeconfig.yaml /usr/bin/openshift-tests run openshift/network/third-
party -o /data/results.txt"
```

命令使用与 Red Hat OpenShift 当前次要版本对应的测试套件，例如 4.x。如果要为以前的次版本运行测试，请使用镜像标签来指示所需的版本。例如，当为 OpenShift 4.6 运行测试时，

将版本号添加到上述命令，如 ose-tests:v4.6。有关可用标签的信息，请参阅 ose-tests 存储库页面。

2. 按照以下步骤运行 Red Hat OpenShift Virtualization 一致性测试套件：

a. 使用以下命令下载特定于环境的一致性测试：

```
$ curl -L https://github.com/kubevirt/kubevirt/releases/download/v<KubeVirt
version>/conformance.yaml -o kubevirt-conformance.yaml
```

在这个命令中，& lt;KubeVirt version > 对应于您使用的 OpenShift Virtualization 版本。如需了解更多详细信息，请参阅 Version 映射表。

b. 使用以下命令执行测试：

```
$ sonobuoy run --skip-preflight --plugin kubevirt-conformance.yaml
```

在这个命令中，& lt;KubeVirt version > 表示 kubevirt 的版本。

c. 使用以下命令监控测试的状态：

```
$ sonobuoy status
```

d. 当测试运行时，使用以下命令获取结果：

```
$ sonobuoy retrieve
```

它生成一个压缩的 tar 文件。

验证步骤

使用以下命令验证测试是否已成功完成：

```
$ sonobuoy results <tarball>
```

输出应类似于如下：

```
Plugin: kubevirt-conformance
Status: passed
Total: 637
Passed: 9
Failed: 0
Skipped: 628
```

3. 按照以下步骤运行 Red Hat OpenShift Service Mesh 测试套件：

   a. 克隆 Maistra Test 工具 GitHub 存储库。

   b. 根据仓库中的 README.md 文件中提供 的说明，运行测试。请注意，这些测试可能需要大约 3 小时才能完成。

   如果您遇到导致套件失败的问题，请使用以下命令检查受影响的 pod，以检查 ImagePullBackOff 错误：

   ```
   $ describe
   ```

   c. 测试成功完成后，会生成 results.xml 和 test.log 文件。将文件与 CNI 一致性测试结果提交到红帽认证团队进行验证。

33.7. 提交 CNI OPERATOR 以进行认证

捕获端到端 CNI 测试的输出、OpenShift Virtualization 测试和 Service Mesh 测试（如果适用），并通过红帽客户门户网站提交结果。

1. 登录到 红帽认证门户。
2. 在主页上，在搜索栏中输入产品问题单号。从显示的列表中选择问题单号。
3. 在 Summary 选项卡中，在 Files 部分下点 Upload。

在上传结果前，请确保所有 CNI 测试都成功完成。如果特定测试不适用于认证产品，请附上说明以及结果提交。

33.8. 在红帽生态系统目录中发布产品列表

当您通过红帽客户门户网站提交 CNI 组件进行验证时，红帽认证团队将检查并验证您的组件进行验证。验证成功后，您的认证产品将在红帽生态系统目录中发布。

按照以下步骤发布您的认证 CNI operator：

1. 访问 合作伙伴连接 网页。My Products 网页显示 产品列表。
2. 搜索所需的产品列表。
3. 单击您要发布的新创建的产品列表。检查您的产品列表的所有详细信息。
4. 转至 Components 选项卡。
5. 点 Add Component 将您的认证 CNI operator 附加到此列表中。另外，添加 CNI 组件使用的认证容器。所有组件都必须处于 Published 状态。

   当您指定产品列表的所有所需信息以及附加的组件时，会启用 Publish 按钮。
6. 单击 Publish。

您的经认证的 CNI Operator 现在可在 红帽生态系统目录 上公开访问。认证的 CNI Operator 也会在 OpenShift 的 Web 控制台的 OperatorHub 中列出。合作伙伴将收到徽标，以便在 Red Hat OpenShift 平台上推广其认证产品。

注意

Red Hat OpenShift 软件认证不会在 Operator 结构之外对合作伙伴产品的功能或性能测试，它对安装和执行它的红帽平台的影响。认证候选产品质量保证的所有方面均保持合作伙伴的责任。

第 34 章 CSI 认证

34.1. 使用容器存储接口(CSI)认证

注意

要认证 CSI 插件，必须将其配置为使用 Operator 部署和管理。在继续 Red Hat CSI 认证前，Operator 以及 CSI operator 捆绑包引用的所有容器（包括插件）必须在认证 CSI 驱动程序前已通过 红帽生态系统目录 中认证并发布。

34.1.1. 容器存储接口简介

容器存储接口(CSI)允许 OpenShift Container Platform 上的产品消耗从支持 CSI 接口的存储后端提供 的持久性存储。CSI 驱动程序通常由容器镜像提供。CSI 徽标是 Red Hat OpenShift 认证中的分类。它可供使用 CSI 驱动程序 与 Red Hat OpenShift 作为部署平台集成的存储产品。

满足要求并完成认证工作流的产品可以引用并推广 Red Hat OpenShift Container Platform 上的认证 CSI 产品。批准认证后，认证的 CSI 产品将在 红帽生态系统目录以及 Red Hat OpenShift 的 Web 控制台中的 OperatorHub 上列出。认证的 CSI Operator 使用 CSI 徽标标识。合作伙伴将收到徽标以推广其产品认证。

其他资源

- 有关 CSI 的更多信息，请参阅：
  - CSI 规格
  - 使用 CSI
  - Kubernetes CSI 开发人员文档

34.1.2. CSI 认证工作流

注意

红帽建议您在开始认证过程前具有红帽认证工程师或具有同等经验。

任务摘要

认证工作流包括三个主要步骤：

1. 第 34.1.2.1 节 “CSI 认证”
2. 第 34.1.2.2 节 “CSI 认证测试”
3. 第 31.6 节 “在红帽生态系统目录中发布产品列表”

34.1.2.1. CSI 认证

执行认证加入概述的步骤：

1. **加入 Red Hat Connect for Technology Program （ Red Hat Connect for Technology Program (Red Hat Connect for Technology Program)**
2. **同意计划条款和条件。**
3. **选择所需产品类别来创建您的产品列表。您可以从可用产品类别中选择：**
   a. **容器化应用程序**
   b. **独立应用程序**
   c. **OpenStack Infrastructure**
4. **填写您的公司简介。**

-

5. 将组件添加到产品列表中。

6. 为您的产品列表认证组件。

其他资源

有关创建产品列表的详细信息，请参阅创建产品列表。

34.1.2.2. CSI 认证测试

要运行认证测试，

1. 派生红帽上游存储库。

2. 在测试环境中安装并运行红帽认证管道。

3. 检查测试结果并进行故障排除（若有问题）。

4. 通过拉取请求向红帽提交认证结果。

其他资源

有关附加产品组件并验证 Red Hat OpenShift 中 CNI Operator 功能的详细信息，请参阅 添加认证组件。

34.1.2.3. 在红帽生态系统目录中发布产品列表

完成所有认证检查后，您可以向红帽提交测试结果。您可以根据您的个人目标打开或关闭此结果提交步骤。提交测试结果后，它会触发红帽基础架构来自动合并拉取请求并发布您的 Operator。

其他资源

有关在红帽生态系统目录上发布产品列表的详细信息，请参阅在红帽生态系统目录上发布产品列表。

34.2. 创建产品

有关创建产品列表的详细信息，请参阅创建产品列表。

34.3. 添加认证组件

有关附加产品组件并验证 Red Hat OpenShift 中 CNI Operator 功能的详细信息，请参阅 添加认证组件。

34.4. 使用 OPENSHIFT OPERATOR PIPELINE

在继续 CSI 认证前，按照步骤认证您的 Operator：

1. 添加 Operator 捆绑包
2. 分叉软件仓库
3. 安装 OpenShift Operator Pipeline
4. 执行 Openshift Operator 管道
5. 提交认证结果

客户通过嵌入式 OpenShift operatorHub 列出并消耗认证的 Operator，使他们能够轻松部署和运行解决方案。此外，您的产品和操作器镜像还将在 红帽生态系统目录 上列出。

34.5. 配置测试环境以运行 CSI 测试

在运行 CSI 测试前，请验证您用于运行 CSI 测试的 Red Hat OpenShift 环境是否满足以下条件：

1. 在生命周期的完全支持阶段使用 Red Hat OpenShift 版本。红帽建议使用最新支持的版本。如需有关 OpenShift 发行版本的更多信息，请参阅 Red Hat OpenShift Container Platform 生

命周期政策。

2. 使用其 Operator 安装 CSI 驱动程序。

3. 安装 Red Hat OpenShift Virtualization。

4. 配置可访问 OpenShift 集群的 RHEL 主机，以用作运行 CSI 认证测试的测试客户端。

重要

在同一个配置上运行您自己的产品验证测试，以确保您的产品功能在 Red Hat OpenShift 环境中按预期工作。

Red Hat Partner Connect 提供对软件的免费访问，作为计划的好处。要了解如何获取 Red Hat OpenShift 环境订阅，请参阅 Red Hat 合作伙伴连接计划指南。

34.6. 访问 CSI 认证测试

CSI 认证测试被打包到一个容器中，并包含在 OpenShift End-to-End 存储库中。要检索测试的当前版本，请导航至 红帽生态系统目录，并按照 Get this image 选项卡中提供的说明进行操作。

在访问 OpenShift 端到端测试容器时，请确保拉取用于产品认证的 OpenShift 版本的对应标签。

34.7. 设置 CSI 测试参数

CSI 认证测试需要在客户端主机上存在以下文件：

- 包含凭证的 kubeconfig.yaml 文件，用于访问 test 下的 OpenShift 集群。此文件会在 OpenShift 安装过程中自动创建，但您可以使用以下命令重新创建副本：

```
$ oc config view --raw > kubeconfig.yaml
```

- 描述驱动程序功能的 manifest.yaml 文件。此文件用于确定必须执行的测试。如需更多信息，请参阅 示例文件。

34.8. 运行 CSI 测试

在测试客户端中，将 kubeconfig.yaml 和 manifest.yaml 文件放在当前工作目录中，并运行以下命令：

```
$ podman run -v `pwd`:/data:z --rm -it registry.redhat.io/openshift4/ose-tests sh -c
"KUBECONFIG=/data/kubeconfig.yaml TEST_CSI_DRIVER_FILES=/data/manifest.yaml
/usr/bin/openshift-tests run openshift/csi --junit-dir /data/results"
```

如果您在最新的 OpenShift 版本上执行测试，请确保将正确的标签添加到容器镜像名称：registry.redhat.io/openshift4/ose-tests:<tag>。如需可用标签列表，请参阅 OpenShift End-to-End Tests 存储库 页面。

验证步骤

1. 命令的输出包括有关 CSI 功能的测试以及 OpenShift 中的容器原生虚拟化(CNV)的测试概述。以下是输出示例：

```
Storage Capabilities (guaranteed only on full CSI test suite with 0 fails)
============================================================
Driver short name: ceph-test
Driver name: test.rbd.csi.ceph.com
Storage class: ceph-rbd-sc.yaml
Supported OpenShift / CSI features:
Persistent volumes: true
Raw block mode: true
FSGroup: true
Executable files on a volume: true
Volume snapshots: true
Volume cloning: true
Use volume from multiple pods on a node:true
ReadWriteMany access mode: true
Volume expansion for controller: true
Volume expansion for node: true
Volume limits: true
Volume can run on single node: true
Topology: true
Supported CNV features:
Raw block VM disks: true
Live migration: true
VM snapshots: true
Storage-assisted cloning: true
```

详细结果将放置在 结果 子目录中。

2. 如果要查看为 CSI 认证运行的测试列表，请运行以下命令：

```
podman run -v `pwd`:/data:z --rm -it registry.redhat.io/openshift4/ose-tests sh -c
"KUBECONFIG=/data/kubeconfig.yaml TEST_CSI_DRIVER_FILES=/data/manifest.yaml
/usr/bin/openshift-tests run --dry-run openshift/csi
```

注意

为每个支持的存储协议执行单独的测试。

34.9. 提交 CSI 测试结果

在提交测试结果前，请确保以下就绪：

- results 目录中的内容
- manifest.yaml 文件
- 以下命令的输出：

```
$ oc get clusterversion -o yaml
```

和

```
$ podman image list registry.redhat.io/openshift4/ose-tests
```

按照以下步骤通过红帽客户门户网站提交结果文件：

1. 登录到 红帽认证门户。
2. 在主页上，在搜索栏中输入产品问题单号。从显示的列表中选择问题单号。

3. 在 Summary 选项卡中，在 Files 部分下点 Upload。

在上传结果前，请确保所有 CSI 测试都成功完成。如果特定测试不适用于认证产品，请附上说明以及结果提交。

34.10. 在红帽生态系统目录中发布产品列表

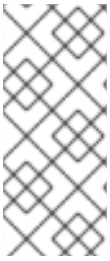
当您通过红帽认证门户提交 CSI 组件进行验证时，红帽认证团队将检查并验证您的组件进行验证。验证成功后，您的认证产品将在红帽生态系统目录中发布。

按照以下步骤发布您的认证 CSI operator：

1. 访问 合作伙伴连接 网页。My Products 网页显示 产品列表。
2. 搜索所需的产品列表。
3. 单击您要发布的新创建的产品列表。检查您的产品列表的所有详细信息。
4. 转至 Components 选项卡。
5. 点 Add Component 将认证 CSI operator 附加到此列表中。另外，添加 CSI 组件使用的额外认证容器。所有组件都必须处于 Published 状态。

   当您指定产品列表的所有所需信息以及附加的组件时，会启用 Publish 按钮。
6. 单击 Publish。

您的经认证的 CSI operator 现在可在 红帽生态系统目录 上公开访问。认证的 CSI Operator 也会在 OpenShift 的 Web 控制台的 OperatorHub 中列出。合作伙伴将收到徽标，以便在 Red Hat OpenShift 平台上推广其认证产品。



注意

Red Hat OpenShift 软件认证不会在 Operator 结构之外对合作伙伴产品的功能或性能测试，它对安装和执行它的红帽平台的影响。认证候选产品质量保证的所有方面均保持合作伙伴的责任。