



# Red Hat Hardware Certification 2024

## Red Hat Bare Metal 硬件认证 workflow 指南

用于 Red Hat OpenShift Container Platform 4 和 Red Hat OpenStack Platform 17



# Red Hat Hardware Certification 2024 Red Hat Bare Metal 硬件认证 workflow 指南

---

用于 Red Hat OpenShift Container Platform 4 和 Red Hat OpenStack Platform 17

## 法律通告

Copyright © 2024 Red Hat, Inc.

The text of and illustrations in this document are licensed by Red Hat under a Creative Commons Attribution–Share Alike 3.0 Unported license ("CC-BY-SA"). An explanation of CC-BY-SA is available at

<http://creativecommons.org/licenses/by-sa/3.0/>

. In accordance with CC-BY-SA, if you distribute this document or an adaptation of it, you must provide the URL for the original version.

Red Hat, as the licensor of this document, waives the right to enforce, and agrees not to assert, Section 4d of CC-BY-SA to the fullest extent permitted by applicable law.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, the Red Hat logo, JBoss, OpenShift, Fedora, the Infinity logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

Linux<sup>®</sup> is the registered trademark of Linus Torvalds in the United States and other countries.

Java<sup>®</sup> is a registered trademark of Oracle and/or its affiliates.

XFS<sup>®</sup> is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

MySQL<sup>®</sup> is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js<sup>®</sup> is an official trademark of Joyent. Red Hat is not formally related to or endorsed by the official Joyent Node.js open source or commercial project.

The OpenStack<sup>®</sup> Word Mark and OpenStack logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

All other trademarks are the property of their respective owners.

## 摘要

Red Hat Bare Metal 硬件认证 workflow 指南涵盖了实现红帽硬件认证的测试要求。版本 9.0 和 8.80 更新了 2024 年 5 月 28 日。

---

# 目录

使开源包含更多 .....	3
部分 I. RED HAT OPENSTACK PLATFORM 和 OPENSIFT CONTAINER PLATFORM BARE METAL 硬件认证计划简介 .....	4
第 1 章 红帽硬件认证计划概述 .....	5
1.1. 获取支持和提供反馈 .....	5
第 2 章 加入认证合作伙伴 .....	6
2.1. 加入现有认证合作伙伴 .....	6
2.2. 加入新的认证合作伙伴 .....	6
第 3 章 红帽裸机硬件认证计划概述 .....	8
部分 II. RED HAT OPENSTACK PLATFORM BARE METAL 硬件认证 .....	10
第 4 章 设置测试环境 .....	11
4.1. 设置 UNDERCLOUD 节点 .....	11
4.2. 配置裸机 .....	12
4.3. 验证裸机配置 .....	12
第 5 章 使用测试计划置备 UNDERCLOUD 节点 .....	13
第 6 章 运行认证测试 .....	14
第 7 章 提交测试结果文件 .....	15
第 8 章 执行裸机认证 .....	16
8.1. 创建 RHOSP BARE METAL 补充认证 .....	16
部分 III. RED HAT OPENSIFT CONTAINER PLATFORM BARE METAL 硬件认证 .....	17
第 9 章 测试环境概述 .....	18
9.1. 为安装程序置备的基础架构(IPI)准备测试环境 .....	18
9.2. 为支持的安装程序准备测试环境 .....	18
第 10 章 创建裸机补充认证 .....	19
第 11 章 运行 IPI 测试 .....	20
第 12 章 运行支持的安装程序测试 .....	24
部分 IV. 反馈和重新认证 .....	27
第 13 章 查看反馈 .....	28
第 14 章 重新认证 workflow .....	29



## 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。](#)

## 部分 I. RED HAT OPENSTACK PLATFORM 和 OPENSIFT CONTAINER PLATFORM BARE METAL 硬件认证计划简介

使用本指南了解实现 Red Hat OpenStack Platform 和 Red Hat OpenShift Container Platform 裸机硬件认证所需的步骤。



### 重要

红帽硬件认证计划假定硬件和红帽产品知识与技能的高级水平。红帽硬件认证计划中不提供红帽产品支持，但可单独购买。

# 第 1 章 红帽硬件认证计划概述

红帽硬件认证计划确保了 [OpenStack 平台上的硬件、软件和云产品的兼容性](#)。程序有三个主要元素：

- **测试套件**：完成硬件或软件测试。
- **红帽认证生态系统**：帮助探索和查找认证产品，包括硬件、软件、云和服务提供商。
- **支持**：与您与红帽之间的共同支持关系。

## 1.1. 获取支持和提供反馈

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](#)。

您还可以创建一个支持问题单以获取支持或提交反馈。

要创建一个支持问题单，请参阅[如何提交和管理客户门户网站中的支持问题单？](#)

### 认证过程中的问题

如果您对特定认证有任何问题或响应，请在认证条目的 **Dialog Tab** 的评论部分中记录它们。



#### 警告

可以阻止认证并可能需要解决问题的问题必须通过工程合作伙伴经理或其他工程参与来解决。

### 其他资源

- 如需有关 Red Hat OpenStack 裸机硬件和 Red Hat OpenShift Container Platform 裸机硬件认证的要求和策略的更多信息，请参阅 [Red Hat OpenStack Hardware Bare Metal 认证策略指南](#)。

## 第 2 章 加入认证合作伙伴

如果您是一个新合作伙伴，请使用红帽客户门户网站创建一个新帐户，或者如果您是一个当前合作伙伴用来认证您的产品，请使用您的现有红帽帐户。

### 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 OpenStack 认证没有任何帮助。  
或者
- 使用分配了管理合作伙伴的专用 EPM 团队，以传统方式由 EPM 团队完全管理的成员，包括有关 OpenStack 认证请求的问题。

#### 先决条件

您有一个现有的红帽帐户。

#### 流程

1. 访问[红帽客户门户](#)，再单击 **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. 如果帐户号与您的帐户关联，请联系认证团队以继续认证流程。<mailto:connect@redhat.com>
  - 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。  
获得帐户号后，请联系认证团队进行认证过程。<mailto:connect@redhat.com>

### 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 [红帽客户门户网站](#) 并点 **Register**。
2. 输入以下详情来创建新红帽帐户：
  - a. 在 **Account Type** 字段中选择 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。

- b. 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. 单击 **Create My Account**，创建了一个新的红帽帐户。
3. 如果可用，请联系您的生态系统合作伙伴管理(EPM)代表。否则，请联系 [认证团队](#) 以继续认证过程。

### 第 3 章 红帽裸机硬件认证计划概述

Red Hat OpenStack Platform 和 Red Hat OpenShift Container Platform 裸机硬件认证为客户带来了价值，因为服务器可以自动部署和重新部署 Red Hat OpenStack Platform 和 Red Hat OpenShift Container Platform，而无需人工干预。认证流程通过一系列测试验证，验证认证解决方案是否满足企业云的要求，并由红帽和您的组织共同支持。

下图显示了 OpenShift 和 OpenStack 的裸机认证 workflow：

图 3.1. Red Hat OpenStack Platform Bare Metal 硬件认证过程

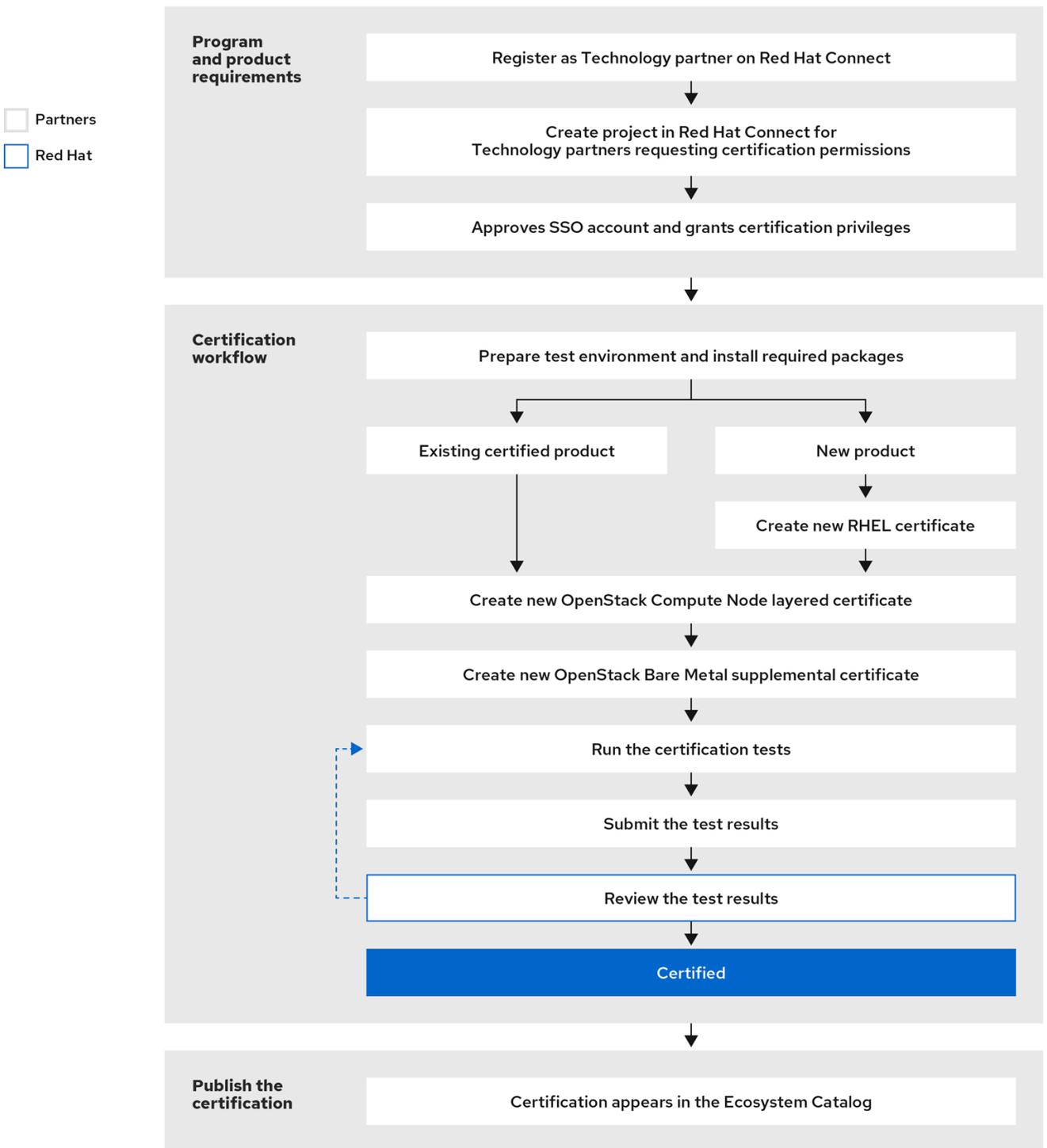
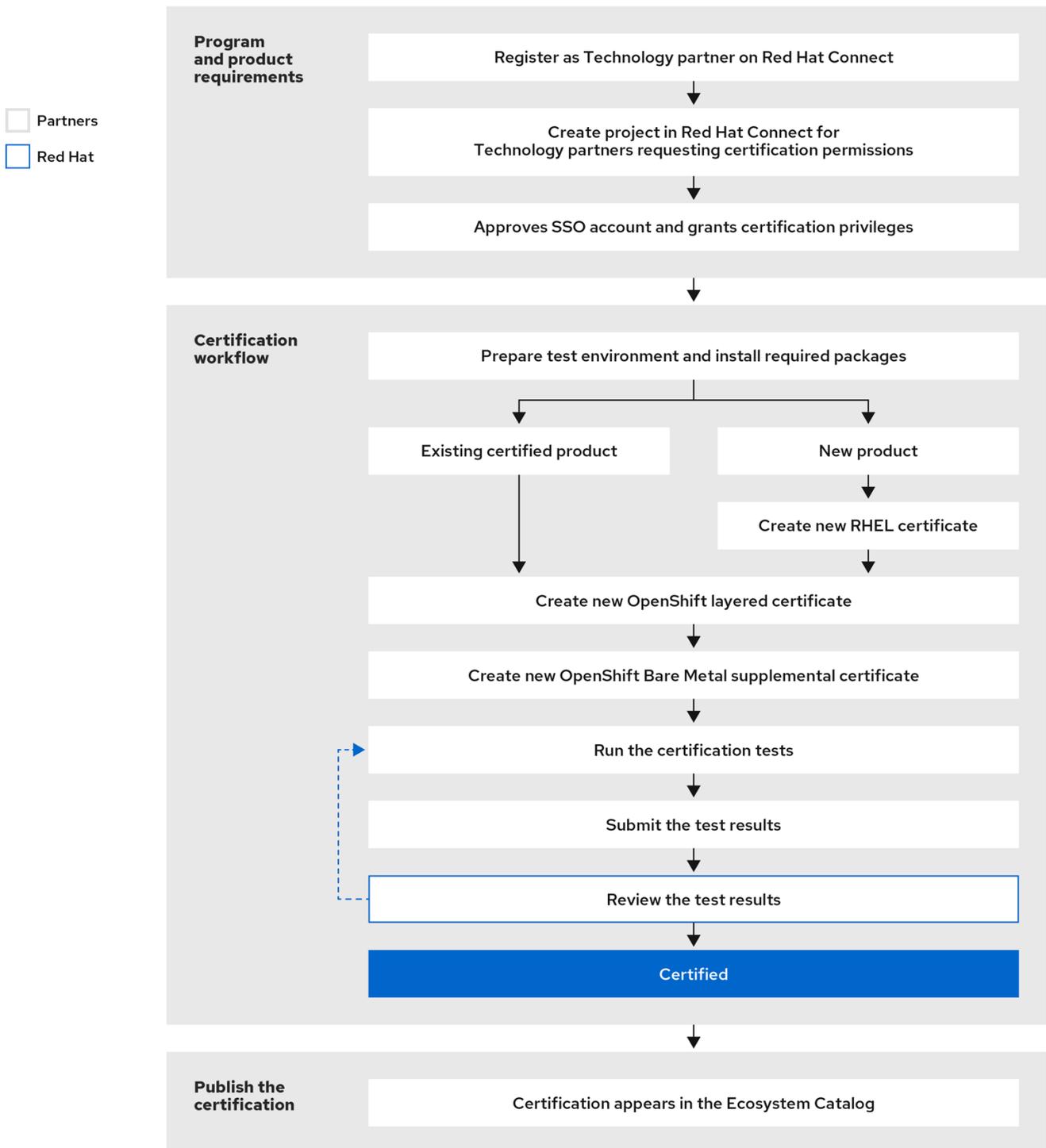


图 3.2. Red Hat OpenShift Container Platform Bare Metal 硬件认证过程



305\_OpenStack\_0523

大多数认证子测试都提供了一个即时的返回状态(Pass/Fail)；有些子测试可能需要由红帽进行详细检查，以确认成功或失败。这类测试在红帽认证应用程序中被标记为 **REVIEW** 状态。有些测试可能会识别潜在的问题并返回 **WARN** 状态。此状态表示可能还没有遵循最佳实践。标有 **WARN** 状态的测试保证注意或操作，但不会阻止认证发布。您应该查看此类测试的输出，并根据警告中包含的信息执行适当的操作。

有关认证先决条件的详情，请查看 [策略指南](#)。

## 部分 II. RED HAT OPENSTACK PLATFORM BARE METAL 硬件认证



### 注意

本章仅适用于 Red Hat OpenStack Platform 裸机硬件认证。

## 第 4 章 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。测试环境仅包含 Undercloud 节点。

所有强制测试，验证裸机认证所需的系统配置在 Undercloud 节点上运行。



### 重要

如果您希望使用 Cockpit 而不是命令行进行裸机测试，您必须首先设置 Cockpit。具体步骤请参阅 [使用 Cockpit 配置系统并运行测试](#)。

### 4.1. 设置 UNDERCLOUD 节点

#### 先决条件

- 您已在基于支持的 RHEL 版本的系统中安装了 RHOSP，如适用。确保使用 RHOSP Director 进行安装，因为它是在生产环境中安装和管理 RHOSP 支持的工具集。

对应的支持版本如下：

RHOSP 版本	支持的 RHEL 版本
RHEL 16.0	8.1
RHEL 16.1	8.2
RHEL 16.2	8.4
RHEL 17.0	9.0
RHEL 17.1	9.2 和 9.4

- 确保 RSA 私钥文件采用 PEM 格式。如需更多信息，请参阅 [RHOSP 17.1 配置参考文档](#)。

#### 流程

- 使用您的 RHN 凭证，使用 Red Hat Subscription Management 注册您的系统：

```
# subscription-manager register
```

- 显示您的系统可用订阅列表：

```
# subscription-manager list --available*
```

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。

- 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。

#### 4. 订阅红帽认证频道：

- 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
```

- 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
```

#### 5. 安装认证 RPM。

- 仅在 RHEL 9 中

```
# yum install redhat-certification
```

#### 6. 安装 OpenStack 测试套件软件包：

```
yum install redhat-certification-baremetal
```

## 4.2. 配置裸机

有关在 Red Hat OpenStack Platform 环境的 `undercloud` 中安装、配置和使用裸机服务，请参阅 [裸机置备服务\(ironic\)功能](#)。

## 4.3. 验证裸机配置

### 流程

在开始认证过程前，您必须验证裸机是否正常工作。要查看注册的节点及其状态，请按照 [使用 director 安装和管理 Red Hat OpenStack Platform 指南中的故障排除节点置备](#) 章节。

## 第 5 章 使用测试计划置备 UNDERCLOUD 节点

### 流程

1. 运行 provision 命令。

```
# rhcert-provision <path_to_test_plan_document>
```

将 <path\_to\_test\_plan\_document> 替换为在测试主机上保存的测试计划文件。

## 第 6 章 运行认证测试

rhcert CLI 是支持的运行测试的方法。

### 流程

1. 运行测试

```
# rhcert run
```

非交互式标签是一个 RHCert 标志，用于运行所有与认证相关的强制测试。

2. 保存测试结果文件

```
# rhcert-save
```

默认情况下，结果文件保存为 `/var/rhcert/save/rhcert-results-<host-name>-<timestamp>.xml`。

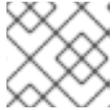
## 第 7 章 提交测试结果文件

您可以使用 RHCert CLI 或红帽 [认证工具](#)向红帽提交 测试结果文件。

使用 RHCert CLI 工具：

### 流程

1. 登录以验证您的设备。



#### 注意

要提交测试结果文件，需要登录。

```
# rhcert-cli login
```

- a. 在新浏览器窗口或标签页中打开生成的 URL。
  - b. 输入登录名和密码，并单击 **Log in**。
  - c. 点 **Grant access**。  
显示设备日志成功信息。
  - d. 返回到终端，然后在 **您授予访问权限后**输入 **yes** 给 **Please confirm**。
2. 提交结果文件。

```
# rhcert-submit
```

出现提示时，输入您的认证 ID。

### 使用红帽认证工具

#### 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**。

#### 后续步骤

红帽将审核您提交的结果文件，并提出下一步以授予认证。如需更多信息，请访问红帽客户门户。<https://rhcert.connect.redhat.com/#/home>

认证后，该产品将在 [红帽生态系统目录](#) 上列出。

## 第 8 章 执行裸机认证

Red Hat OpenStack Platform Bare Metal 认证验证您的系统可作为 OpenStack 环境的一部分编配。

### 8.1. 创建 RHOSP BARE METAL 补充认证

Red Hat OpenStack Platform Bare Metal 认证可能已作为 Red Hat Enterprise Linux 系统认证的一部分为您创建。

如果没有为您自动创建，或者需要在以后应用认证，请执行以下步骤：

#### 先决条件

- 您的服务器必须已经获得以下认证：
  - Red Hat Enterprise Linux System
  - Red Hat OpenStack Platform Compute 节点

如果您需要创建 Red Hat OpenStack Platform Compute 节点分层认证的信息，请参阅 [认证分层产品](#)。

#### 流程

1. 登录到 [Red Hat Partner Connect](#) 门户。
2. 点与您要打开的裸机认证相关的 Red Hat Enterprise Linux 系统认证。
3. 进入 **相关认证** 选项卡。
4. 点与您要打开的裸机认证相关的 Red Hat OpenStack Platform Compute 节点认证。
5. 进入 **相关认证** 选项卡。
6. 在认证表的顶部，单击 **Add Related Certification**。  
此时会出现 **Create Related Certification** 窗口。
7. 选择 **Supplemental** 并点 **Next**。
8. 查看认证信息并点 **Open**。  
创建补充认证，红帽认证团队会将 **裸机管理组件** 添加到测试计划中。
9. 在获得新的测试计划后，开始测试。

## 部分 III. RED HAT OPENSIFT CONTAINER PLATFORM BARE METAL 硬件认证



### 注意

本章仅适用于 Red Hat OpenShift Container Platform 裸机硬件认证。

Red Hat OpenShift Platform 裸机硬件认证验证您的裸机服务器已准备好在 OpenStack 环境中远程编配和部署。

认证有两个组件：

- installer-provisioner 基础架构(IPI)
- 支持的安装程序

您可以为任何组件或两者都认证裸机服务器。

以下部分将在适用时为您提供每个部分的详细说明。

## 第 9 章 测试环境概述

### 9.1. 为安装程序置备的基础架构(IPI)准备测试环境

认证的环境包括以下组件：

- 安装需要认证的 IPI 集群的裸机服务器称为测试下的主机(HUT)。
- 在裸机系统上成功进行安装程序置备的安装。请参阅[在裸机上部署 IPI 集群](#)。

### 9.2. 为支持的安装程序准备测试环境



#### 重要

如果您希望使用 Cockpit 而不是命令行进行辅助安装程序认证测试，您必须首先设置 Cockpit。具体步骤请参阅[使用 Cockpit 配置系统并运行测试](#)。

认证的环境包括以下组件：

- 充当 Host Under Test (HUT)的裸机服务器。这是您要认证的服务器。服务器必须具有互联网连接。  
测试 仅验证单节点集群。如果要认证多个裸机服务器，您必须将每个服务器作为单节点集群安装。  
  
裸机恢复服务器必须符合 control plane 节点的硬件要求和网络要求，如[OpenShift Container Platform 支持的安装程序](#)所述。
- 可以登录到 [Red Hat Hybrid Cloud Console](#) 的 Red Hat 账户，以使用支持的安装程序安装 HUT。您可以使用 UI 或 API 来执行安装。
- 使用支持的安装程序安装单节点集群后，您可以使用可访问单节点集群的 RHEL 8 或 RHEL 9 客户端继续运行 assisted\_installer 测试。

## 第 10 章 创建裸机补充认证

Red Hat OpenShift Bare Metal 认证是一个补充认证。它可能已经为您创建，作为 Red Hat Enterprise Linux 系统认证的一部分。

如果没有为您自动创建，或者需要在以后应用认证，请执行以下步骤：

### 先决条件

- 您的服务器必须已经获得以下认证：
  - Red Hat Enterprise Linux System
  - Red Hat OpenShift Container Platform

您必须为每个类型、IPI 或 AI 创建单独的补充认证。但是，如果您打算同时认证 IPI 和 AI，请创建一个附加认证请求。

有关创建 Red Hat OpenShift Container Platform 分层认证的更多信息，请参阅 [认证分层产品](#)。

### 流程

1. 登录到 [Red Hat Partner Connect](#) 门户。
2. 点与您要打开的辅助安装程序认证相关的 Red Hat Enterprise Linux 系统认证。
3. 点表左上角的 **相关认证** 选项卡。
4. 点与您要打开的辅助安装程序认证相关的 Red Hat OpenShift Container Platform 认证。
5. 点表左上角的 **相关认证** 选项卡。
6. 在认证表的顶部，单击 **Add Related Certification**。此时会出现 **Create Related Certification** 窗口。
7. 选择 **Supplemental** 并点 **Next**。
8. 查看认证信息并点 **Open**。已创建补充认证。
9. 对红帽认证团队提出评论，以指定您希望或两个组件添加到测试计划中：
  - 裸机管理
  - 支持的安装程序
10. 在获得新的测试计划后，开始测试。

## 第 11 章 运行 IPI 测试

安装程序置备的基础架构(IPI)测试验证您的支持 BMC 的裸机节点是否可以在已建立的 RHOCP 环境中访问、部署和重启。

该测试使用 RHOCP 环境中已在运行的 Ironic 服务调配裸机节点正在进行认证。

### 先决条件

- 您已准备了安装程序置备的集群。
- 您已将 [裸机节点添加到 RHOCP 集群](#)。此节点必须：
  - 没有安装操作系统。
  - 尚未置备。
  - 如果 RHOCP 环境中两者都可用，则具有 [裸机和 调配网络](#) 的访问权限。如果您只配置了 **baremetal 网络**，则必须连接到该服务器。

### 重要

测试必须验证服务器是否可以远程打开和关闭。为裸机节点创建 **bmh.yaml** 文件时，将 **online** 字段设置为 **false**。例如：

```
apiVersion: metal3.io/v1alpha1
kind: BareMetalHost
metadata:
  name: openshift-worker-<num>
spec:
  online: false
```

无法正确设置此字段将导致测试失败。

### 流程

1. 识别运行 **Ironic** 服务的节点的 **IP 地址**。例如：

```
# oc -n openshift-machine-api get pods -o wide | egrep -v 'image|controller|operator'
```

NAME	READY	STATUS	RESTARTS	AGE	IP	NODE
metal3-78b556db65-1gkrp	7/7	Running	0	12d	172.22.0.111	worker-0

**metal3 pod** 运行测试用来安装裸机节点的 **Ironic** 服务。记录其 **IP 地址**；这是您将在稍后的步骤中使用的 **Ironic API 端点**。

2. 获取 **Ironic** 服务的凭据，并记录它们。您将在后续步骤中使用它们。

```
# oc -n openshift-machine-api get secret/metal3-ironic-password -o template --template
'{{.data.username}}' | base64 -d

# oc -n openshift-machine-api get secret/metal3-ironic-password -o template --template
'{{.data.password}}' | base64 -d
```

3. 登录到任何集群节点。例如：

```
# oc debug host/master-0
```

4. 准备节点以运行认证测试：

- a. 如果还没有安装，安装 **podman**。
- b. 创建 **/tmp/results** 目录。测试会将结果存储在这个目录中



#### 注意

如果 **RHOCP** 环境中两者都可用，则节点必须有权访问 **baremetal** 和 **provisioning** 网络。如果您只配置了 **baremetal** 网络，则必须连接到该节点。

- c. 登录到红帽认证的镜像 **registry**：

```
# podman login registry.redhat.io
Username: <registry_service_account_username>
Password: <registry_service_account_password>
Login Succeeded!
```

- d. 从红帽目录下载 **redhat-certification-baremetal** 镜像：

```
# podman pull registry.redhat.io/rhcertification/redhat-certification-baremetal
```

5. 运行 **IPI** 测试：

```
# podman run -it --net host -v /tmp/results:/var/rhcert_results:Z redhat-certification-baremetal
```

表 11.1. IPI test 参数描述

参数	描述
<b>-it</b>	启动交互式会话。
<b>--net host</b>	Podman 将主机的网络堆栈用于容器。容器的网络配置与主机的相同。容器共享可供主机使用的同一服务端口。
<b>-v tmp/results:/var/rhcert_results</b>	允许将主机文件夹 <b>/tmp/results</b> 的内容挂载到 <b>/var/rhcert_results</b> 。
<b>:Z</b>	确保挂载点具有读写权限。

6. 输入您之前获取的 Ironic 服务的用户名、密码和 URL。URL 必须采用 [https://<Ironic\\_IP\\_address>:6385](#) 格式。

7. 选择您要在其上运行测试的裸机节点。

这时将显示所选节点的 UUID、Name、Power State 和 Provision State。测试将在选择节点后启动。

8. 在提示时确认裸机节点是否开机。确认这一点后，测试会重启裸机节点。

测试结果文件在 **/tmp/results** 生成。

9. 在红帽认证网站中，将结果提交到您服务器的补充 RHOCP 认证。

#### 其他资源

- 有关 IPI 测试的更多信息，请参阅 [Red Hat OpenStack Platform 硬件裸机认证策略指南](#)。
- [安装 Red Hat OpenShift Container Platform](#)



准备裸机节点

## 第 12 章 运行支持的安装程序测试

支持的安装程序测试验证您的裸机服务器是否可以使用 **OpenShift Container Platform** 的辅助安装程序安装。

测试仅用于裸机服务器。不支持虚拟机。



### 重要

如果您希望使用 **Cockpit** 而不是命令行进行辅助安装程序认证测试，您必须首先设置 **Cockpit**。具体步骤请参阅 [使用 Cockpit 配置系统并运行测试](#)。

### 先决条件

- 您已使用 **Red Hat OpenShift Container Platform** 支持的安装程序将 **HUT** 安装为单节点 **OpenShift** 集群。
- 您已按照 **Red Hat OpenShift Container Platform** 支持的安装程序 所述配置了 **kubeconfig** 文件。
- 您可以使用以下方法之一运行 **rhcert-provision** 命令：
  - 在运行 **rhcert-provision** 命令时按照以下步骤操作，它会直接从 [连接门户](#) 下载测试计划，以便进行身份验证。
  - 使用从 [连接门户](#) 下载的测试计划，如 [创建裸机补充认证](#) 文档中所述。

### 流程

1. 登录到单节点集群。
2. 安装以下 **redhat-certification** 软件包：

- 红帽认证
- **redhat-certification-openshift**

例如：

```
# dnf install redhat-certification redhat-certification-openshift
```

3. 在 [Red Hat Hybrid Cloud Console](#) 中，生成 OpenShift Manager API 令牌。

4. 将令牌添加到 **OFFLINE\_TOKEN** 变量中，并导出它。

例如，

```
# export OFFLINE_TOKEN=<value_of_your_token>
```

5. 使用以下命令确认集群是否可访问：

```
# oc status
```

6. 根据测试计划运行测试：

```
# rhcert-run
```

类似的测试显示，如下所示：

```
The following test run is recommended:
self_check                               pre-run
assisted_installer                       runnable
sosreport                                 runnable
Would you like to run all the tests, or select them? [all|select|quit]: all
```

或者，您可以使用 **rhcert-cli** 运行测试，如下所示：

```
# rhcert-cli plan
```

```
# rhcert-cli run --test assisted_installer
```

保存测试结果：

```
# rhcert-cli save
```

7.

在 [红帽认证网站](#) 将这两个测试结果提交到您服务器的补充 **RHOCP** 认证。

## 部分 IV. 反馈和重新认证

此模块可帮助您了解反馈和重新认证信息。

## 第 13 章 查看反馈

提交结果后，红帽认证团队将分析内容并授予每个通过测试计划一部分的测试分数。当它们验证每个通过测试时，团队会将每个测试计划项目设置为 **Confirmed**，您可以在目录的 **Results** 选项卡下看到。

图 13.1. 认证和测试计划

Test	Host Device	Save Assignment	Results
baremetal/director_undercloud		DIRECTOR_UNDERCLOUD: DIRECTOR_UNDERCLOUD	<p>&gt; <b>PASS</b></p> <p>Attachments:</p> <ul style="list-style-type: none"> <li>os_collect_config.json</li> <li>undercloud_nova_list.log</li> </ul>
rhcert/self_check		SELF_CHECK: SELF_CHECK	<p>&gt; <b>PASS</b></p> <p>Verify Test Suite: PASS Combined: PASS</p>
baremetal/baremetal		BAREMETAL: BAREMETAL	<p>&gt; <b>FAIL</b></p> <p>Attachments:</p> <ul style="list-style-type: none"> <li>instackerv.json</li> </ul>
baremetal/supportable		SUPPORTABLE: SUPPORTABLE	<p>&gt; <b>FAIL</b></p>
baremetal/sosreport		SOSREPORT: SOSREPORT	<p>&gt; <b>PASS</b></p> <p>Attachments:</p> <ul style="list-style-type: none"> <li>sosreport-undercloud-0.redhat.local-2...</li> </ul>

如果发现任何问题，红帽认证团队将更新认证请求，该请求将自动发送给提交证书的人员。您还可以尝试在测试页面中调试结果。

**注意**

您可以在认证中讨论来自 **Dialog** 选项卡的结果或问题。

## 第 14 章 重新认证 workflow

增量产品或功能可能也可能不需要重新认证。该要求最终由红帽合作伙伴认证团队提供。但是，红帽鼓励您始终自行重新测试这些更改，而不考虑正式要求，以确保产品正常工作。