Red Hat Hardware Certification 2024

Red Hat OpenStack Platform 硬件裸机认证策略指南

用于 Red Hat OpenStack Platform 17

Last Updated: 2024-06-25

Red Hat Hardware Certification 2024 Red Hat OpenStack Platform 硬件裸机认证策略指南

用于 Red Hat OpenStack Platform 17

法律通告

摘要

Red Hat OpenStack Platform Hardware Bare Metal 认证政策指南涵盖了实现红帽硬件认证所需的流程、技术和策略要求。 版本 9.0 和 8.80 更新了 2024 年 5 月 28 日。

目录

使开源包含更多 3

第 1 章 RED HAT OPENSTACK 裸机硬件认证政策简介 4
1.1. 受众 4
1.2. 程序概述 4

第 2 章 认证先决条件 5
2.1. 合作伙伴资格标准 5
2.2. 认证目标 5

第 3 章 裸机认证概述 7
3.1. 目录中的发布 7
3.2. 红帽产品发行版本 7
3.3. 认证持续时间 7
3.4. 重新认证工作流 7

第 4 章 认证和测试 8
4.1. 预要求通过认证测试 8
4.2. 认证工作流 8
4.3. 认证要求 9

第 5 章 利用认证 10

第 6 章 透传认证 11

第 7 章 补充认证 12

第 8 章 IPI 认证测试 13
8.1. 自我检查测试 13
8.2. 可支持的测试 13
8.3. DIRECTOR_UNDERCLOUD TEST 16
8.4. 裸机测试 16

使开源包含更多

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

第 1 章 RED HAT OPENSTACK 裸机硬件认证政策简介

Red Hat OpenStack Platform (RHOSP)裸机硬件认证政策指南适用于希望使用 Red Hat 认证其裸机服务器的硬件供应商。RHOSP 裸机认证测试可确保您可以在无需人工干预的情况下自动编配服务器。

通过此项计划，如果服务器满足您可以对 IPI 组件的服务器进行认证，那么可以在 Red Hat OpenStack Platform 上部署它。

1.1. 受众

本指南适用于提供自己的基础架构硬件（如系统服务器）或管理控制器以便在受支持的客户环境中用于 Red Hat OpenStack Platform 的合作伙伴。

1.2. 程序概述

Red Hat OpenStack Platform (RHOSP)裸机硬件认证给客户带来了价值，因为可以在不需要人工干预的情况下，管理并自动部署并重新部署系统。

通过一系列测试的认证流程验证认证解决方案是否满足企业云要求，并由红帽和您的组织共同支持。

RHOSP 裸机硬件认证程序策略包括多个测试，每个测试都有一系列子测试和检查，记录在文档中。

第 2 章 认证先决条件

注意

需要非常了解 Red Hat Enterprise Linux 和 Red Hat OpenStack。在参与前，最好使用 Red Hat Certified Engineer and a Red Hat OpenStack Platform Certified Engineer 证书。

2.1. 合作伙伴资格标准

在应用红帽裸机硬件认证前，请确保满足以下要求：

- 您是 红帽硬件认证计划的一部分。
- 您正在使用 TSANet 网络或自定义支持协议与红帽的支持关系。

2.2. 认证目标

认证目标提供有关与认证相关的组件和产品的详细信息和要求。

如果适用，会为每个认证组件提供具体信息。

2.2.1. 服务器

- 确保服务器必须具有以下认证：
  - Red Hat Enterprise Linux System
  - Red Hat OpenStack Platform Compute 节点
    每个认证都遵循特定的 Cloud Platform 产品版本及其关联的 ironic 版本。如果您的硬件与该平台的 ironic 驱动程序兼容，您可以为 RHOSP 认证服务器。
- 服务器必须安装有基板管理控制器(BMC)。

2.2.2. Red Hat Cloud Platform 产品

裸机认证

通过此计划，您可以在 Red Hat OpenStack Platform 17.1 上认证 BMC 和裸机服务器。

2.2.3. 基板管理控制器(BMC)

BMC 是服务器主板上的专用微控制器，用于管理系统管理软件和物理硬件之间的接口。Red Hat Platform 中的裸机服务通过使用 BMC 控制电源、网络引导和自动化节点部署和终止来在集群中置备系统。

BMC 可以被认证为一个组件，用于在多个服务器系统中 利用 组件。与红帽硬件认证计划类似，红帽利用合作伙伴的内部质量测试来简化认证流程，而无需给客户环境带来风险。

红帽建议合作伙伴使用裸机硬件认证中的组件来利用特定的服务器系统、BMC 和 Red Hat 云平台产品进行测试以验证每个组合。但是，您不需要向红帽提交个人认证结果。

2.2.4. 裸机驱动程序

IPI 组件认证

BMC 必须使用相应 Red Hat Cloud Platform 产品中提供的支持的 Red Hat OpenStack Platform Bare Metal Driver。您不能认证需要没有包含在红帽产品中的 ironic 驱动程序的 BMC。

第 3 章 裸机认证概述

裸机认证概述提供了在目录、产品发布、认证持续时间和重新认证中有关产品发布的详细信息。

3.1. 目录中的发布

当您为 Red Hat OpenStack Platform 上的裸机硬件认证服务器时，会在红帽生态系统目录中作为 **裸机** 目录发布。裸机管理功能也作为服务器的已认证组件显示。

3.2. 红帽产品发行版本

您有权访问，并鼓励使用预先发布的红帽软件进行测试。在红帽软件正式发布(GA)之前，您可以开始与红帽认证团队合作，以加快您的产品认证流程。但是，仅在 Red Hat OpenShift Container Platform 裸机硬件的 GA 版本中进行官方认证测试。

3.3. 认证持续时间

从 Red Hat OpenStack Platform 软件的特定主版本和次要发行本开始，认证在红帽生态系统目录中经过测试并列出。它们仍然通过主版本的最后一个次版本有效。这样，客户可以在产品的生命周期结束前考虑其列出的认证。

3.4. 重新认证工作流

如果您没有对产品进行任何更改，则不需要在 RHOSP 的新主版本或次版本后进行重新认证。但是，您负责再次认证您的产品。

红帽建议您定期在产品上运行认证测试，以确保其使用支持的 RHOSP 版本质量、功能和性能。

要重新认证您的产品，请打开附加认证。

第 4 章 认证和测试

认证测试简介，有关测试的先决条件、了解认证流程及其要求。

4.1. 预要求通过认证测试

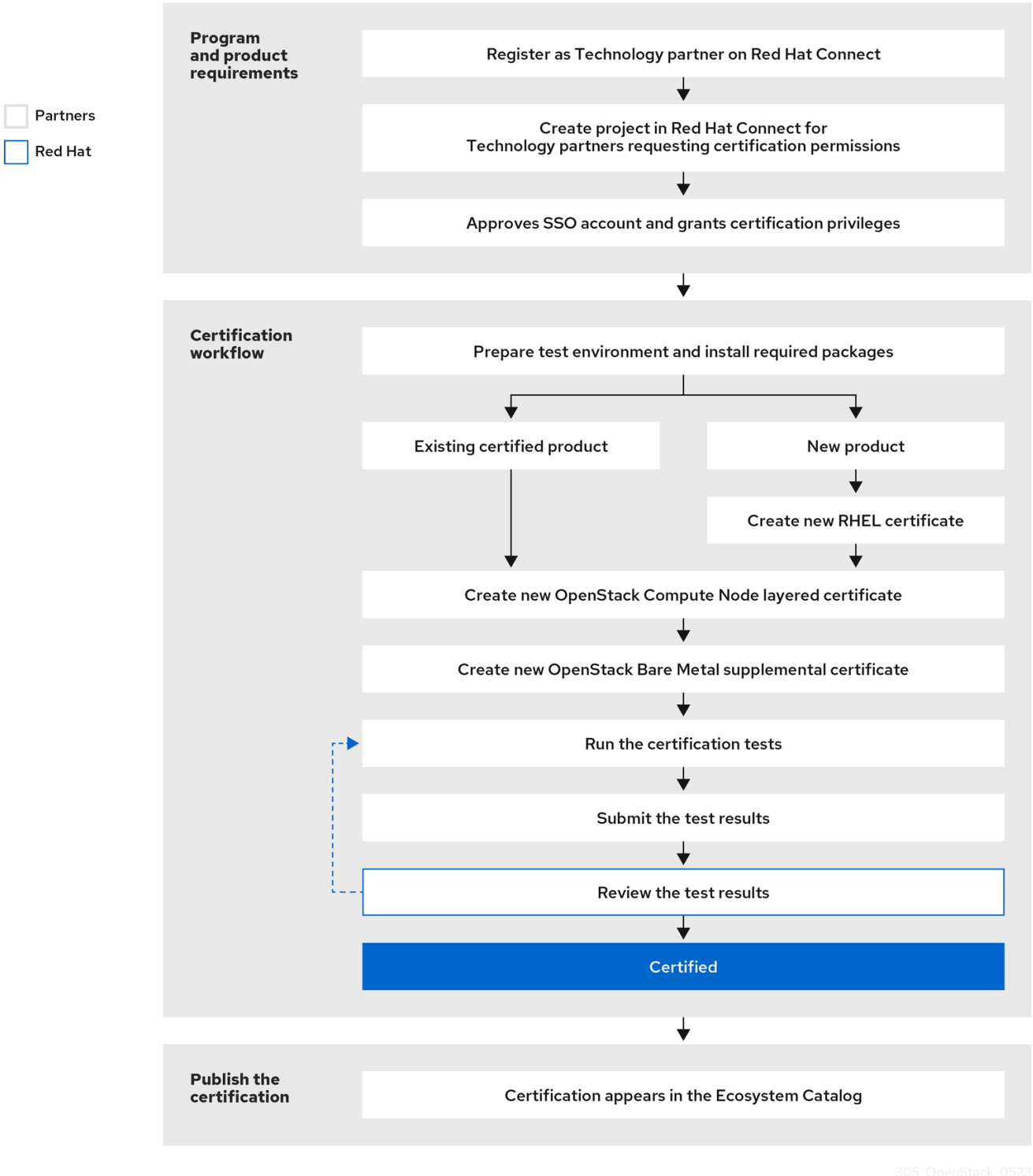
裸机认证

- 对应的 RHEL 服务器认证成功完成并发布。
- 对应的 Red Hat OpenStack Platform Compute 节点认证成功完成并发布。
- 对应的裸机驱动程序位于相应 Red Hat OpenStack Platform 发行版本支持 的驱动程序 列表中。

4.2. 认证工作流

Red Hat Bare Metal 硬件认证过程包括以下要求和步骤：

图 4.1. Red Hat OpenStack Platform Bare Metal 硬件认证流程



4.3. 认证要求

确保您遵循 Red Hat OpenStack 裸机硬件指南。认证要求的更多详情包括：

- Host Under Test (HUT)必须已经是 RHEL 认证。此外，测试必须在之前认证的服务器上运行，测试计划中规定的所有测试都必须在单一运行中执行。
- 如果您有失败的测试，请采取纠正措施，**并在单个运行 中执行所有测试**。如果需要，创建一个支持问题单。

第 5 章 利用认证

通过利用，您可以在一系列服务器系统中使用类似或显著类似的 BMC 时，您可以请求获得以前的成功测试。它基于您在每个系统中特定 BMC 的内部资格测试，确认任何变化并非材料，且解决方案与之前认证的解决方案匹配。

利用 可以减少认证所需的官方测试量。当解决方案包含之前认证的 BMC 时，您可以请求利用相同的固件分支和等号或更少功能。

注意

您负责验证 BMC-to-server 交互的差异不会影响认证。

第 6 章 透传认证

传递认证指的是第三方系统或组件能够获得之前由原始硬件制造商认证的硬件认证的能力。透传可以减少执行并向红帽提交的完整测试数量，以便为第三方硬件获得认证。

系统制造商可将授权给自己的系统的认证扩展到其他供应商的系统：

- 有来自第三方的权限，
- 具有确保第三方不更改硬件的机制时，它不再被视为由红帽认证的原始模型的子集，
- 将支持和代表硬件的职责扩展到涉及第三方硬件的情况。

然后，第三方无法将其传递认证扩展到另一个供应商。

虽然这两个供应商都需要成为红帽硬件认证计划的成员，但只有原始供应商才能请求通过认证。供应商还可能使用 Pass-Through 进程，其中同一供应商对于同一硬件有多个名称。

第 7 章 补充认证

在以下情况下打开补充认证：

首次认证

可以在不同的认证过程中自动创建裸机补充认证，例如，当您为 Red Hat Enterprise Linux 系统认证应用时。
如果没有自动创建，或者需要在以后应用认证，请在 Red Hat OpenStack Compute 节点认证之上打开一个新的附件认证。

重新认证

打开附加认证以更新现有的 RHOSP 裸机认证。
例如，您可能希望更新您的产品，以便在红帽平台的不同版本上认证相同的系统，或者因为您的产品收到了重大更新。

您负责启动这些认证，并通知红帽对您的产品的任何材料更改。

第 8 章 IPI 认证测试

认证包括 *自我检查*、*可支持*、*director_undercloud* 和*裸机* 测试。

8.1. 自我检查测试

自我检查 测试确认是否已安装并取消认证所需的所有软件包，确保测试环境已准备好进行认证。不得修改认证软件包以进行测试或任何其他目的。

成功标准

测试环境包括所有必要的认证软件包，并且没有修改软件包。

8.2. 可支持的测试

可支持的测试（也称为 **baremetal/supportable** ）可确保测试环境与红帽的支持政策兼容。此测试确认测试节点（测试中的 OpenStack 部署）仅由红帽支持的组件(Red Hat OpenStack Platform、Red Hat Enterprise Linux)组成。

测试下的 OpenStack 部署指的是安装插件或应用程序测试中的节点。

支持性测试必须在控制节点和计算节点上运行。

所有 OpenStack 软件认证都需要此测试。

Compute 节点注意事项：

- 如果您的内核没有更新，请确保您更新了内核 test 部分，以验证计算是否使用 GA 内核以防止查看退出。审核将需要考虑 RHEL 认证的状态。
- 驱动程序更新程序(DUP)在计算节点上可以接受，但将导致测试退出检查。检查需要确认与相应 RHEL 认证中使用的 DUP 保持一致。

baremetal/supportable 测试包括以下子测试：

8.2.1. 内核子测试

内核 子测试检查在测试环境中运行的内核模块。内核版本可以是原始正式发行(GA)版本，也可以是为 RHEL 主版本和次版本发布的任何后续内核更新。

内核子测试还确保内核在环境中运行时没有污点。

成功标准

- 正在运行的内核是一个 Red Hat 内核。
- 正在运行的内核由红帽发布，用于 RHEL 版本。
- 运行的内核没有污点。
- 正在运行的内核尚未修改。

其他资源

- Red Hat Enterprise Linux 生命周期

- Red Hat Enterprise Linux Release Dates
- 为什么内核"包含"以及污点值如何解译？

8.2.2. 内核模块子测试

内核模块 子测试会验证载入的内核模块是否被红帽发布，也可以作为内核软件包的一部分或通过 Red Hat 驱动程序更新添加。内核模块子测试还确保内核模块没有被视为技术预览。

成功标准

- 内核模块由红帽发布并被支持。

其他资源

- "技术预览（Technology Preview）"功能是什么？

8.2.3. 硬件健康子测试

Hardware Health 子测试通过测试硬件是否被支持、满足要求并具有任何已知的硬件漏洞来检查系统的健康状况。子测试执行以下操作：

- 检查 Red Hat Enterprise Linux (RHEL)内核没有识别不支持的硬件。当内核识别不支持的硬件时，它会在系统日志中显示不受支持的硬件信息，并/或触发不支持的内核污点。此子测试可防止客户在不受支持的配置和环境中运行红帽产品时可能出现的生产风险。
  在 hypervisor 中，分区、云实例和其他虚拟机情况，内核可能会根据虚拟机(VM)提供的硬件数据触发不受支持的硬件消息或污点。
- 检查 Host Under Test (HUT)是否满足最低硬件要求。
  - RHEL 8 和 9：最小系统 RAM 应该为 1.5GB，每个 CPU 逻辑内核数。
  - RHEL 7：最小系统 RAM 每个 CPU 逻辑内核数应当为 1GB。
- 检查内核是否报告了任何已知的硬件漏洞，以及这些漏洞是否已解决这个漏洞。许多缓解方案都是自动的，以确保客户不需要采取主动步骤来解决漏洞。在某些情况下，大多数剩余的情况都需要更改系统 BIOS/固件，因此客户可能根本无法修改。
- 确认系统没有任何离线 CPU。
- 确认系统中是否有 Simultaneous Multithreading (SMT)可用、启用并激活。

如果这些测试失败，将导致测试套件中的 WARN 信息，并且合作伙伴应由合作伙伴验证具有正确的和预期的行为。

成功标准

- 内核没有设置 UNSUPPORTEDHARDWARE 污点位。
- 内核不会报告不支持的硬件系统信息。
- 内核不应报告任何带有这个安全漏洞的缓解方案的漏洞。
- 内核不会报告逻辑内核与安装的内存比率超出范围。
- 内核不会报告处于离线状态的 CPU。

其他资源

- 最低内存要求
- 在 RHEL 8 中支持但从 RHEL 9 中删除的硬件支持 。
- 在 RHEL 7 中支持当从 RHEL 8 中删除的硬件支持 。
- 在 RHEL 6 中支持当从 RHEL 7 中删除的硬件支持 。

8.2.4. 安装的 RPM 子测试

安装的 RPM 子测试会验证系统上安装的 RPM 软件包是否是由红帽发布的且未修改。修改的软件包可能会带来风险并影响客户环境的可支持性。如果需要，您可以安装非红帽软件包，但必须将它们添加到产品的文档中，且不得修改或与任何红帽软件包冲突。

如果您安装了非红帽软件包，红帽将审核此测试的输出。

成功标准

- 安装的红帽 RPM 没有被修改。
- 安装的非红帽 RPM 需要并记录。
- 安装的非红帽 RPM 不与红帽 RPM 或软件冲突。

其他资源

- 产品支持覆盖范围

8.2.5. 系统报告子测试

红帽使用名为 **sos** 的工具从 RHEL 系统收集配置和诊断信息。 **sos** 工具可帮助客户对 RHEL 系统进行故障排除并遵循推荐的实践。

系统报告子测试可确保 sos 工具在镜像或系统上按预期运行，并捕获基本的 sosreport。

成功标准

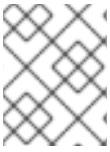
RHCERT 工具在测试下捕获 OpenStack 部署的基本 sosreport。

其他资源

- 有关 sosreport 的更多信息，请参阅 sosreport 是什么以及如何在 Red Hat Enterprise Linux 中创建？

8.2.6. SELinux 子测试

确认 SELinux 在 OpenStack deployment-under 测试上以 **enforcing 模式运行**。



注意

Security-Enhanced Linux (SELinux)为 Linux 内核添加了强制访问控制(MAC)，并在 Red Hat Enterprise Linux 中默认启用。

SELinux 策略由系统管理员进行定义，在系统范围内实施，用户自由裁量未自行设置，从而降低特权升级攻击漏洞，有助于限制配置错误的破坏。如果进程被破坏，攻击者只能访问该进程的正常功能，以及进程已配置为的文件。

成功标准

在测试的 OpenStack 部署过程中，SELinux 配置并以 enforcing 模式运行。

其他资源

- 有关 RHEL 中 SELinux 的更多信息，请参阅 SELinux 用户和管理员指南。

8.3. DIRECTOR_UNDERCLOUD TEST

Director_undercloud 测试（也称为 **openstack/director** ）确保最初使用 Red Hat OpenStack Platform Director 安装 **deployment-under-test**。所有 OpenStack 软件认证都需要此测试。

Red Hat OpenStack Platform Director 是在生产环境中安装和管理 Red Hat OpenStack Platform 环境支持的工具集。它有助于轻松安装精益、强大的 OpenStack 云。它特别针对于企业云环境，更新、升级和基础架构控制对于底层 OpenStack 操作至关重要。

成功标准

测试下的部署最初使用 Red Hat OpenStack Platform Director 安装。

其他资源

- 有关安装 Red Hat OpenStack Platform Director 的更多信息，请参阅 Director 安装和使用指南。

8.4. 裸机测试

以下子测试由裸机测试组成。测试执行注册、检查和部署以验证裸机节点。

8.4.1. 裸机 InstackStackrc 验证

验证 **instackenv.json** 和 **stackrc** 文件。

成功标准

- 检查 **instackenv.json** 和 **stackrc** 文件是否存在于指定位置，并验证 **instackenv.json** 文件的内容，以及
- 需要验证检查文件是否为有效的 json 文件，并且可以访问指定的 BMC IP。

8.4.2. 裸机驱动程序验证

将 HUT 上配置的驱动程序与红帽支持的驱动程序进行比较。如果出现驱动程序不匹配，则子测试会生成 *Review* 状态并退出。红帽支持的驱动程序是测试套件的一部分

成功标准

- 指定的驱动程序应与 **instackenv.json** 文件中的驱动程序匹配，以及

- 如果驱动程序与测试不匹配，则会以 *Review* 状态退出。在这种情况下，红帽认证团队将手动检查 **instackenv.json** 文件以及指定的驱动程序，以验证驱动程序是否支持驱动程序。

8.4.3. 裸机 undercloud 验证

检查测试是否从 undercloud 节点运行。如果测试没有在此节点上运行，测试会失败，您需要重新运行测试。

成功标准

测试 undercloud 工件，以检查测试是否从 undercloud 节点运行。

注意

undercloud 节点是有效的节点。

8.4.4. 裸机注册测试

检查裸机驱动程序是否成功可以使用 BMC IP 注册硬件节点。注册过程需要驱动程序与 BMC IP 正确通信。BMC 将注册节点的 **Power state** 和 **Provisioning state** 改为 **off** 和 **available**。

该测试还会检查堆栈 overcloud 是否存在，以及节点是否已添加。如果堆栈和节点存在，它会删除它们，然后尝试根据 **instackenv.json** 文件注册节点。如果任何阶段失败，则测试会失败。

成功标准

注册的节点应该处于 **Power** 和 **Provisioning** 状态。

8.4.5. 裸机检查测试

当 Operator 设置所需的 **driver_info** 字段后，BareMetalInspectingTest 允许 **Bare Metal** 服务发现所需的节点属性。

成功标准

节点属性应正确填充，以便 BMC 可以根据驱动程序提供的说明收集硬件详情。

8.4.6. 裸机部署测试

检查成功完成后，裸机部署测试将尝试通过创建和分配自定义类别到节点来尝试 **nova 引导** 两台虚拟机。这有助于检查 BMC 是否可以为实例提供所需的引导镜像，然后尝试引导实例。

成功标准

虚拟机启动，并附加了 **Active** 状态。

8.4.7. 裸机重新部署测试

尝试重新部署 nova 实例。

成功标准

前面涵盖的所有阶段也应传递重新部署。测试注册并检查硬件实例，根据注册和检查阶段部署实例。