Red Hat Software Certification 2024

Red Hat OpenStack 认证策略指南

用于 Red Hat OpenStack 17

Last Updated: 2024-06-25

Red Hat Software Certification 2024 Red Hat OpenStack 认证策略指南

用于 Red Hat OpenStack 17

法律通告

摘要

Red Hat OpenStack 认证政策指南描述了合作伙伴在受支持的客户环境中提供自己的应用程序或基础架构软件（插件或驱动程序）的可处理、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 4

第 1 章 RED HAT OPENSTACK PLATFORM 认证策略指南 5
1.1. 受众 5
1.2. 为客户创建值 5
1.3. RED HAT OPENSTACK PLATFORM 认证先决条件 5
1.4. RED HAT OPENSTACK PLATFORM 组件发布 6
1.5. 支持的 RHEL 版本和架构 6

第 2 章 RED HAT OPENSTACK PLATFORM 认证目标 7
2.1. 实现 OPENSTACK API 的产品 7
2.2. 使用 OPENSTACK API 的产品 7
2.3. 支持经认证的 OPENSTACK 组件 7

第 3 章 认证生命周期 9
3.1. 产品认证生命周期 9
3.2. 持续测试 9
3.3. 重新认证 9

第 4 章 系统报告测试 10

第 5 章 指定测试 11

第 6 章 测试环境可支持性测试 12
6.1. 内核子测试 12
6.2. 内核模块子测试 13
6.3. 硬件健康子测试 13
6.4. 安装的 RPM 子测试 15
6.5. SELINUX 子测试 15

第 7 章 DIRECTOR 测试 17

第 8 章 CINDER 测试 18
8.1. CINDER_VOLUMES 20
8.2. CINDER_CONSISTENCY_GROUPS 20
8.3. CINDER_BACKUPS 21
8.4. CINDER_MULTI-ATTACH_VOLUME 21

第 9 章 MANILA 测试 23
9.1. MANILA_SHARES (BASE) 23
9.2. MANILA_SHARE_MANAGED 24
9.3. MANILA_SHARE_SHRINK 24
9.4. MANILA_SHARE_EXTEND 24
9.5. MANILA_SNAPSHOT 24
9.6. MANILA_SNAPSHOT_MANAGED 25
9.7. MANILA_SNAPSHOT_SHARE_FROM_SNAPSHOT 25
9.8. MANILA_SNAPSHOT_REVERT_TO_SNAPSHOT 25
9.9. MANILA_SNAPSHOT_MOUNTABLE 26

第 10 章 NEUTRON 测试 27
10.1. NEUTRON_IPV4 (BASE) 27
10.2. NEUTRON_IPV6 (BASE) 27
10.3. NEUTRON_ADDRESS_SCOPE 27
10.4. NEUTRON_AGENTS 28

10.5. NEUTRON_ATTRIBUTE_EXTENSIONS 28
10.6. NEUTRON_AVAILABILITY_ZONES 28
10.7. NEUTRON_DHCP_EXTRA 28
10.8. NEUTRON_FLAVOR 29
10.9. NEUTRON_GATEWAY_EXTRA 29
10.10. NEUTRON_GMAN 29
10.11. NEUTRON_IP_AVAILABILITY 29
10.12. NEUTRON_IPV4 30
10.13. NEUTRON_IPV6 30
10.14. NEUTRON_L2_MULTI_PROVIDER 30
10.15. NEUTRON_L3_EXTRA_ROUTE 30
10.16. NEUTRON_L3_FLAVORS 31
10.17. NEUTRON_L3_HA 31
10.18. OCTAVIA_LOAD_BALANCER 31
10.19. NEUTRON_MTU 32
10.20. NEUTRON_QOS 32
10.21. NEUTRON_RBAC 32
10.22. NEUTRON_SECURITY_GROUPS 33
10.23. NEUTRON_SERVICE_TYPES 33
10.24. NEUTRON_SUBNET_ALLOCATION 33
10.25. NEUTRON_SUBNET_DEFAULT_POOL 33
10.26. NEUTRON_TAGS 33
10.27. NEUTRON_TRUNK 34
10.28. NEUTRON_BORDER_GATEWAY_PROTOCOL_VPN 34

第 11 章 OPENSTACK 配置测试 36
11.1. 其他资源 36

第 12 章 可信容器测试 37

第 13 章 原位升级 38

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 PLATFORM 认证策略指南

Red Hat OpenStack 认证策略指南介绍了通过 Red Hat OpenStack Platform 认证第三方供应商解决方案的策略概述。红帽鼓励合作伙伴通过红帽构建和预发布自己的解决方案测试其插件。

1.1. 受众

本指南描述了技术认证要求，专为希望提供自己的应用程序、管理应用程序或插件/驱动程序软件，以便在共同支持的客户环境中与 Red Hat OpenStack Platform (RHOSP)搭配使用的软件认证合作伙伴实现。

1.2. 为客户创建值

认证流程包括一系列测试，为红帽客户提供保证，保证认证解决方案满足企业云的所有要求。认证流程由红帽和合作伙伴的组织共同支持。

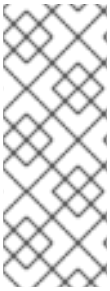
Red Hat OpenStack 认证工作流指南 包括多个测试，每个测试都有一系列子测试和检查，本指南中介绍了这些测试。每个认证都不需要所有测试。

必须使用所有强制测试以及测试套件自我检查测试(rhcert/selfcheck)的单个运行日志必须向红帽提交给红帽进行新的认证和重新认证。文章中记录的认证工具和工作流将在 90 天内支持当前正在进行的认证。

您必须使用 Red Hat OpenStack 认证 策略 和工作流指南中的最新认证工具和工作流文档完成所有新认证。https://access.redhat.com/documentation/zh-cn/red_hat_software_certification/2024/html-single/red_hat_openstack_certification_workflow_guide

红帽建议您在认证过程中安装和使用最新版本的认证工具和工作流。在新的认证工具发行版本时，为以前的工具和工作流提供 90 天宽限期。这样，可以在不中断的情况下完成进度认证。在宽限期结束时，将不再接受使用早期版本的工具生成的测试结果。

最新版本的认证工具和工作流可以通过红帽订阅管理获得，并记录在 Red Hat OpenStack Certification WorkFlow 指南中。



注意

大多数认证子测试都提供了一个即时的返回状态(Pass/Fail)，但有些子测试可能需要由红帽进行详细检查来确认成功。这些测试在红帽认证应用程序中被标记为 **Review** 状态。

有些测试也可以识别潜在的问题并返回 **Warn** 状态。此状态表示尚未遵循最佳实践。标有 **Warn** 状态的测试保证注意或操作，但不会阻止认证成功。建议您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。

其他资源

- 有关运行测试的更多信息，请参阅 Red Hat OpenStack 认证工作流指南 。

1.3. RED HAT OPENSTACK PLATFORM 认证先决条件

在应用 OpenStack 认证之前，您必须满足以下要求。

- 公司必须是 Red Hat Connect for Technology Partners (Red Hat Connect for Technology Partners)中的合作伙伴。此计划为商业 OpenStack 部署提供生态系统，并包含许多技术公司。
- 您必须与红帽有支持关系。这可以通过以下方法之一来实现：

    - 自定义支持协议
    - TSANet

- 您必须对 RHOSP 有很好的了解，包括安装和配置产品
- 您必须为认证 OpenStack 插件提供安装指南的链接。此安装指南必须指示使用 Red Hat Director 进行 OpenStack 部署。

其它资源

- 有关产品的更多信息，请参阅红帽客户门户网站的详细产品文档
- 参与有关 红帽培训页面的产品培训或认证。
- 有关 TSANet 的更多信息，请参阅 TSANet 网页。

1.4. RED HAT OPENSTACK PLATFORM 组件发布

作为 Red Hat OpenStack Platform (RHOSP)的一部分，红帽分发了提交 在上游 OpenStack 项目 版本（如 Kilo、Infitt 等）中所提交的组件。这些组件称为 **树形** 组件。您仍负责认证，以及用于分发不属于上游 OpenStack 项目的所有依赖项。

没有在上游 OpenStack 项目中提交的产品或组件的分发是合作伙伴的责任。这些组件也称为 **Out of tree** 组件。

1.5. 支持的 RHEL 版本和架构

RHOSP 认证在以下 RHEL 版本和构架上被支持。

RHOSP 版本	RHEL 版本	架构
16.0	RHEL 8.1	• x86_64 • ppc64le
16.1	RHEL 8.2	• x86_64 • ppc64le
16.2	RHEL 8.4	• x86_64 • ppc64le
17.0	RHEL 9.0	• x86_64

第 2 章 RED HAT OPENSTACK PLATFORM 认证目标

您应该实现以下目标实现认证：

2.1. 实现 OPENSTACK API 的产品

此类别包括提供 OpenStack 服务/功能的产品，如启动服务器实例、添加新路由器、创建镜像、创建存储容器和对象、创建用户配置文件等。通过实施 API 和/或网络、块存储或文件共享服务的 API 扩展等。

对于实施 OpenStack API 的产品，除了 OpenStack Director 测试(**openstack/director**)和 OpenStack 支持性测试(**openstack/supportable**)外，还需要成功完成 API 组的相关认证测试。

为确保红帽支持底层平台，请在多个 overcloud 节点上运行 OpenStack Director、支持和 sosreport 测试。测试结果应该来自控制器，以及实施/耗时的 Openstack API （厂商插件控制）的计算或存储节点。

重要

确保这些测试在正确的节点上运行。可以请求其他运行来满足这些要求。

在这种情况下，认证过程会根据平台规格验证服务是否提供 API，以及底层 OpenStack 环境是否正确配置。

2.2. 使用 OPENSTACK API 的产品

此类别涵盖所有依赖 OpenStack 服务（如网络、块存储、文件共享等）的产品/应用。

此类产品通常有助于 OpenStack 部署或利用其他功能（如配置、扩展和管理）补充云基础架构。

例子

- OpenStack 管理和编排应用，如网络功能虚拟化管理和编排(NFV MANO)
- OpenStack 监控应用程序
- 其他启用了 OpenStack 的应用程序，如虚拟网络功能(VNF)

对于此类应用程序，您需要成功完成 OpenStack Director 测试(**openstack/director**)和 OpenStack 支持性测试(**openstack/supportable**)。

2.3. 支持经认证的 OPENSTACK 组件

对经过认证的 Openstack 组件（如插件/驱动程序和客户协助）的支持来自提供该组件的供应商。

- 如果红帽认证并作为 RHOSP 的一部分提供第三方组件，且该组件有问题或问题，则客户将联系红帽以获得帮助。
- 如果第三方附带一个 RHOSP 认证组件，且组件存在问题或问题，第三方将完全负责协助客户并提供对该组件的支持。

但是，红帽认证合作伙伴和红帽，维护任何方都可利用的活跃工程关系来确保对客户问题做出快速进展。

其它资源

- 有关 RHOSP 认证组件支持性的更多信息，请参 文章。

第 3 章 认证生命周期

3.1. 产品认证生命周期

从 Red Hat OpenStack Platform (RHOSP) 16 开始，认证会根据特定的主版本和次版本授予 RHOSP。例如，RHOSP 16.0 是主版本 16，0 是次版本。

虽然认证在主版本的生命周期内有效，但在我们的 RHOSP 16 示例中，有些情况下需要重新认证。这些实例在 重新认证 中进行了描述。

3.2. 持续测试

您负责在产品的生命周期和他们认证的 Red Hat OpenStack Platform 主要版本中自行进行内部持续测试。建议您使用 DCI 等 CI 系统，其中包括使用认证测试进行测试。不需要向 CI 系统评估认证测试结果，但应该由合作伙伴监控以获得回归和意外行为，并指示是否需要重新认证。

您可能有权访问预先发布的 Red Hat OpenStack Platform 的软件构建，并鼓励在 Red Hat OpenStack Platform 版本正式发布前开始其初始和 CI 测试，并参与 Red Hat OpenStack Platform。最终的测试和容器构建必须在该主版本的正式发布(GA)发布的容器上执行。

3.3. 重新认证

红帽会在以下情况下通知您，并要求您重新认证您的产品：

- Red Hat OpenStack Platform 的新主版本。
- 一个 Red Hat OpenStack Platform 的新小版本，它添加了之前未包含在早期认证中的额外功能或功能，合作伙伴希望将其添加到其认证中。
- 一个 Red Hat OpenStack Platform 的新次发行版本，它更新内核和合作伙伴产品依赖于内核模块。

您将在以下情况下通知红帽，您需要重新认证其产品：

- 合作伙伴产品的新主要更新，使原始测试无效。
- 合作伙伴产品的新的小更新，更改认证的原始测试计划。

应为每个情况提交一个新的认证。在可能的情况下，在红帽和合作伙伴产品的次要发行本更新中，认证工作和测试计划将侧重于尚未在之前的认证中测试的新特性和功能，因为应该通过所需的持续测试来维护所建立的功能。

当作为 OpenStack 认证的一部分提供自定义容器镜像时，每次为特定的 Major-Minor 版本发布 Red Hat OpenStack Platform z-stream 时，都必须重新构建此自定义容器镜像。这将确保您的镜像利用最新的程序错误修复和 CVE。

注意

对于 RHOSP 容器重新认证，如果没有修改，则不需要重新验证您的产品功能。

第 4 章 系统报告测试

红帽系统报告测试，也称为 **openstack/sosreport**，并捕获基本系统报告。

系统报告测试可确保 SOS 工具捕获基本报告，并在镜像或系统上按预期执行操作。

sosreport 命令是从 RHEL 系统收集配置详情、系统和诊断信息的工具，并帮助您对系统进行故障排除。

成功标准

- 可以从测试下的系统捕获基本 sosreport。
- 如果启用了有效的 rpm 版本捕获并收集 openstack 插件(manila、cinder、neutron)，则测试状态将为 PASS。

其他资源

- 有关 sosreport 的详情，请查看 sosreport 是什么以及如何在 Red Hat Enterprise Linux 中创建？

第 5 章 指定测试

指定 测试使用 Tempest 框架 来验证 Designate DNS 服务是否与您要认证的 Neutron 插件正常工作。

测试执行以下操作：

- 确保以下对象成功 CRUD 操作：
  - Records
  - Domains
  - 服务器
  - blacklists
  - 池
  - 配额
  - 记录集
  - 顶级域
  - 事务签名
- 确保只有管理用户才能对黑名单、配额、池和事务签名执行操作。
- 检查记录集是否不符合 DNS RFC 规格。例如，包含尾部空格或无效字符的记录集将被拒绝。
- 检查包含通配符字符(1)的记录集是否与不存在的域的请求匹配。
- **确保可能跨 DNS 服务器的区域传送。**
- **确保区域创建和区删除在 DNS 服务器间传播。**

成功标准

所有操作和验证都成功。

第 6 章 测试环境可支持性测试

可支持性测试（也称为 openstack/supportable）确保测试环境符合红帽的支持政策。所有 OpenStack 软件认证都需要此测试。该测试确认测试节点（一个 OpenStack deployment-under-test）仅由红帽支持的组件(Red Hat OpenStack Platform、Red Hat Enterprise Linux)或合作伙伴支持。OpenStack deployment-under-test 指的是安装 plugin/application-under-test 的节点，以及 Undercloud Director 节点。

openstack/supportable 测试包括以下子测试。

6.1. 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？

6.2. 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？

6.3. 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。

6.4. 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

6.5. SELINUX 子测试

此子测试确认 Security-Enhanced Linux (SELinux)在 OpenStack deployment-under 测试的 enforcing 模式下运行。

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，在系统范围内强制执行，用户不会在用户自由裁量减少权限升级攻击的漏洞，有助于限制配置错误造成的破坏。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

SELinux 在 OpenStack deployment-under-test 上配置并在 enforcing 模式下运行。

其它资源

其它资源

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

第 7 章 DIRECTOR 测试

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

Red Hat OpenStack Platform (RHOSP) Director 是在生产环境中安装和管理 RHOSP 环境支持的工具集。它有助于轻松安装精益、强大的 OpenStack 云，面向更新、升级和基础架构控制的企业云环境，对底层 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 RHOSP Director 的更多信息，请参阅 Director 安装和使用指南。

第 8 章 CINDER 测试

cinder 测试 仅适用于为 OpenStack 块存储服务实施功能的 OpenStack 产品或组件。测试使用 Tempest Framework 与 Red Hat OpenStack Platform (RHOSP)集成来测试可操作和功能的功能。

cinder 测试通过运行所选功能测试验证相应 cinder 驱动程序的功能。目前支持以下功能：

- cinder_volumes
- cinder_consistency_groups
- cinder_backups
- cinder_multi-attach_volume

先决条件

1. 在部署 overcloud 时，请确保：
   a. 您已提供了您要认证的后端的两个实例。

注意

不需要多个硬件存储；支持将两个 cinder 后端配置为使用同一硬件阵列。

   b. 您已启用了 *cinder-backup* 服务。为此，请在 overcloud 部署命令中添加 cinder-backup 环境文件。

```
-e /usr/share/openstack-tripleo-heat-templates/environments/cinder-backup.yaml
```

如需更多信息，请参阅使用环境文件配置 overcloud。

c.

您已禁用了 cinder 的 LVM/iSCSI 后端，并将 Glance 配置为使用 Cinder 作为其后端。要做到这一点，创建一个新的自定义环境文件，如 *rhcert-overrides.yaml* 并添加以下行：

```
parameter_defaults:
  CinderEnableIscsiBackend: false
  GlanceBackend: cinder
```

然后，将 *rhcert-overrides.yaml* 文件添加到 overcloud 部署命令中。

-e /home/stack/rhcert-overrides.yaml

2.

在执行 tempest_config 测试前，请确保：

a.

您已在 *tempest.conf* 文件中对应的部分标头中启用了以下标记。

注意

如果您的插件支持 *一致性组和 多附加卷* 功能，请确保在 *tempest.conf* 文件中启用对应的标志。

例如，*tempest.conf* 文件中的 *consistency_group* 和 *volume_multiattach* 标志被启用。

```
[volume-feature-enabled]
consistency_group = True
extend_attached_encrypted_volume = True
extend_attached_volume = True
manage_snapshot = True
manage_volume = True
volume_revert = True

[image-feature-enabled]
import_image = True

[compute-feature-enabled]
volume_multiattach = True
```

b.

您已在 *tempest.conf* 文件中设置 *tempest_roles* ：

```
[auth]
tempest_roles = member,swiftoperator
```

3. 如果您的驱动程序支持多附件卷功能，请在执行 cinder 的 multi-attach 卷测试 前执行以下步骤：

   a. 按照创建多附加卷类型中所述的步骤 创建一个多附件卷类型。不要将 cinder 的默认卷类型配置为 multi-attach 卷类型。

   b. 在 *tempest.conf* 文件中添加对 multi-attach 卷类型的引用，如下所示：

```
[volume]
volume_type_multiattach = <multiattach volume type>
```

其他资源

如需更多信息，请参阅 运行 tempest_config 测试。

8.1. CINDER_VOLUMES

cinder_volume 测试检查 cinder 的驱动程序功能和基础功能，如卷操作、快照、引导、卷迁移、加密和克隆是否正常工作。此测试是必须的。

8.2. CINDER_CONSISTENCY_GROUPS

cinder_consistency_groups 测试通过同时执行一致性组的多个卷快照来检查灾难恢复和以下操作：

- 创建和删除一致性组
- 创建和删除一致性组快照
- 从现有一致性组快照创建一个新的一致性组

如果您的驱动程序需要实现一致性组功能，则此测试是必须的。

8.3. CINDER_BACKUPS

cinder_backups 测试通过测试以下内容来验证驱动程序的备份/恢复功能：

- 从现有卷创建和恢复备份
- 测试增量备份
- 备份卷快照

8.4. CINDER_MULTI-ATTACH_VOLUME

cinder_multi-attach_volume 测试检查是否可以通过运行以下测试从多个主机或服务器附加并访问单个块存储卷：

- 从多附件卷引导虚拟机
- 使用 multi-attach 卷重新定义服务器大小
- 列出多附件卷的卷附加
- 来自支持的多附件卷的快照
- 从 shelved 或 卸载服务器附加和分离多附件卷
- 删除附加的多附件卷
- 将 multi-attach 卷附加到相同或不同的服务器。

如果您的驱动程序实现了 multi-attach 功能，则此测试是必须的。

其他资源

- 有关 cinder 测试的更多信息，请参阅 实施 OpenStack API 的产品。

第 9 章 MANILA 测试

根据合作伙伴提供的解决方案，红帽将在 RH-cert Web UI 中定义测试计划，以及合作伙伴需要执行的测试计划。manila 测试执行所选文件共享组件功能测试，并在测试运行时检查用户所选择的插件/驱动程序功能。Manila 测试必须包含在测试计划中定义的测试，该测试将包括强制基础测试和任何实施的额外功能，每个支持的文件系统后端和 DHSS true 或 false 模式的支持如下：

9.1. MANILA_SHARES (BASE)

manila_shares 测试将使用 NFS 或 CIFS 协议来检查基础文件操作。此测试还包括启用了"驱动程序处理共享服务器" (DHSS)功能的基本操作。当插件支持多个协议以及被启用和禁用的 DHSS 时，可能需要在后续运行中重复此测试。

在 manila.conf 文件中，如果 DHSS=true，则网络插件应该是 NeutronNetworkPlugin 或 NeutronBindNetworkPlugin。

成功标准

- 如果 Manila 使用 NeutronNetworkPlugin，且 tempest 启用了多租户，则 dhss 测试状态将为 PASS
- 如果 Manila 使用独立网络 dhss 测试状态，则测试状态为 FAIL

Manila_shares 具有一些功能，如可用区、一致性组、扩展、限制、元数据、微型、版本、配额、规则、安全服务、共享网络、共享操作和共享实例。

作为 Manila_shares 测试的一部分测试的插件/驱动程序功能有：

- create
- delete
- list

- snapshot
- 修改

如果厂商插件实现 manila_shares 及其功能，它们也应该为 manila_shares 执行以下子测试：

9.2. MANILA_SHARE_MANAGED

此测试检查驱动程序功能，以保持共享处于 managed/unmanaged 状态。

9.3. MANILA_SHARE_SHRINK

此测试会检查驱动程序的缩小 manila 共享的能力。

9.4. MANILA_SHARE_EXTEND

此测试检查驱动程序扩展 manila 共享的能力。

9.5. MANILA_SNAPSHOT

快照允许客户从他们希望的特定时间恢复数据。只能为具有快照的数据创建新共享。作为 manila_snapshot 测试的一部分测试的插件/驱动程序功能有：

- 重置快照
- 强制删除快照
- 共享快照实例
- 删除现有快照的共享

- 创建具有较小的大小快照的共享
- 使用不同共享网络从快照创建共享
- 删除带有错误的 id 的快照
- 创建带有错误的 id 的快照
- 创建快照的访问规则
- 按快照 ID 列出共享
- 列出和重命名快照
- 共享快照实例
- 快照规则

9.6. MANILA_SNAPSHOT_MANAGED

此测试检查驱动程序的能力使快照保存在受管或非受管状态中。

9.7. MANILA_SNAPSHOT_SHARE_FROM_SNAPSHOT

当不提供共享网络时，此测试会从快照创建快照。

9.8. MANILA_SNAPSHOT_REVERT_TO_SNAPSHOT

此测试检查驱动程序将共享恢复到快照的能力。

9.9. MANILA_SNAPSHOT_MOUNTABLE

此测试检查驱动程序的创建可挂载快照的能力，而不是从快照创建整个共享，然后删除共享。

成功标准

以下是 Manila 测试和子测试的独立成功标准：

- Manila 测试必须使用 NeutronNetworkPlugin，tempest 必须启用多租户
- manila_share_managed 驱动程序可用于管理 manila 共享状态
- manila_share_shrink 驱动程序执行 manila 共享的缩小操作
- manila_share_extend 是功能性的
- manila_snapshot 使用其所有功能
- 所有 manila_snapshot 子功能测试都成功执行

其他资源

- 有关 manila 测试的更多信息，请参阅 实施 OpenStack API 的产品。

第 10 章 NEUTRON 测试

openstack/neutron 测试仅适用于为 OpenStack 网络服务实施 OpenStack 功能的 OpenStack 产品/组件。这些测试涵盖了 OpenStack networking-component 功能测试，它包括使用 RHOSP 中集成的 Tempest Framework 的基本和操作功能测试。Neutron 包括网络、IP 地址管理(IPAM)和路由器支持，以启用内部和外部网络之间的路由。

根据您提供的解决方案，红帽将在 RH-cert Web UI 中定义测试计划，以及您需要执行的测试计划。neutron 测试执行所选 networking-component 功能测试，并在测试期间检查用户所选择的插件/驱动程序功能。Neutron 必须包含测试计划中定义的测试，该测试将包括强制基础测试以及实施的任何额外功能，每个支持基础协议都会运行一个测试，如下所示：

10.1. NEUTRON_IPV4 (BASE)

此测试会检查所有基于 neutron 的插件/驱动程序，如网络、端口、路由器、配额、子网池、allowed_address_pair、external_networks 和 address_scope （与 ipv4 地址方案相关）。

成功标准

已成功执行所有基于 neutron 的插件/驱动程序 ipv4 功能。

10.2. NEUTRON_IPV6 (BASE)

此测试会检查所有基于 neutron 的插件/驱动程序，如网络、端口、路由器、配额、子网池、allowed_address_pair、external_networks 和 address_scope （与 ipv6 地址方案相关）。

成功标准

已成功执行所有基于 neutron 的插件/驱动程序 ipv6 功能。

10.3. NEUTRON_ADDRESS_SCOPE

此测试检查是否可以通过供应商驱动程序来执行可用于地址范围的所有操作。操作包括：

- 创建

- 删除
- updation
- 地址范围

成功标准

所有 address_scope 操作都可以正常工作。

10.4. NEUTRON_AGENTS

此测试检查 DHCP 和 L3 代理操作是否已成功执行。

成功标准

DHCP 和 L3 代理可正常运行。

10.5. NEUTRON_ATTRIBUTE_EXTENSIONS

此测试检查时间戳是否与标准 api 扩展关联。

成功标准

Neutron_attribute_extensions 测试状态为 Pass，并可成功关联时间戳。

10.6. NEUTRON_AVAILABILITY_ZONES

此测试会检查可应用到可用区的所有标准 API 操作。

成功标准

Neutron_availability_zones 可以将 API 操作应用到可用性区域。

10.7. NEUTRON_DHCP_EXTRA

DHCP 选项扩展允许添加与 Neutron 端口关联的 DHCP 选项。您可以在定义或更新端口时指定 DHCP 选项，方法是指定 extra_dhcp_opts 标签，并将其选项作为名称值对提供。所有与 extra_dhcp_opts 相关的操作都已测试，以检查是否可以应用新选项。

成功标准

新的 dhcp 选项可以成功应用。

10.8. NEUTRON_FLAVOR

Flavor Framework 的目的是提供一个 API，允许用户通过一组公告的服务功能（而非提供程序类型）选择服务类型。此测试将检查是否可以通过第三方插件/驱动程序帮助来完成所有标准类别操作。

成功标准

所有标准操作都可通过第三方插件/驱动程序成功执行。

10.9. NEUTRON_GATEWAY_EXTRA

此测试检查是否可以使用插件/驱动程序来应用与网关相关的额外选项。

成功标准

额外的网关选项可以成功应用。

10.10. NEUTRON_GMAN

在使用 Neutron 的一些云部署中，每个租户都需要配置资源，如网络、子网和路由器，然后才能引导虚拟机。此测试将检查是否作为租户驱动程序，您可以删除或获取分配的拓扑结构。

成功标准

租户驱动程序删除并成功分配拓扑。

10.11. NEUTRON_IP_AVAILABILITY

它允许用户或进程来确定在网络及其子网的分配池之间消耗的 IP 地址数量。在对相关资源执行操作后，测试会检查网络 admin 和 network ip 的可用性，如子网和端口添加和删除。

成功标准

网络 IP 和网络 admin 可用。

10.12. NEUTRON_IPV4

此测试会检查所有基于 neutron 的插件/驱动程序，如网络、端口、路由器、配额、子网池、allowed_address_pair、external_networks 和 address_scope （与 ipv4 地址方案相关）。

成功标准

已成功执行所有基于 neutron 的插件/驱动程序 ipv4 功能。

10.13. NEUTRON_IPV6

此测试会检查所有基于 neutron 的插件/驱动程序，如网络、端口、路由器、配额、子网池、allowed_address_pair、external_networks 和 address_scope （与 ipv6 地址方案相关）。

成功标准

已成功执行所有基于 neutron 的插件/驱动程序 ipv6 功能。

10.14. NEUTRON_L2_MULTI_PROVIDER

ml2 插件数据库模式和驱动程序 API，支持由多个片段组成的虚拟 L2 网络。测试会区分支持的操作。

成功标准

支持的操作会成功执行。

10.15. NEUTRON_L3_EXTRA_ROUTE

此测试会检查诸如 updation 和删除额外路由等操作，以及插件是否提供 l3 功能。

成功标准

能够成功执行 updation 和 deletion 操作。

10.16. NEUTRON_L3_FLAVORS

类别允许在同一部署中运行多个 L3 驱动程序。此测试将检查通过类别创建和删除路由器。

成功标准

能够成功执行创建和删除操作。

10.17. NEUTRON_L3_HA

高可用性功能作为扩展和驱动程序实现。此测试将检查是否可以将高可用性应用到路由器。

成功标准

高可用性可以成功应用到路由器。

10.18. OCTAVIA_LOAD_BALANCER

LBaaS v2 支持 Octavia 插件。如果合作伙伴驱动程序或插件支持此功能，认证测试将包括 octavia_load_balancer 测试的结果。此测试是在基于 Red Hat OpenStack Director 的安装中实现的。

Octavia 测试使用以下功能检查负载均衡器创建流：

- 健康管理器
- housekeeping Manager
- LoadBalancer
- Amphora

- listener
- pool
- 成员

成功标准

测试对 Octavia 负载均衡器功能执行 create、read、update 和 delete 操作。成功 PASS 操作表示所有 Octavia 相关功能都可用于合作伙伴插件。

10.19. NEUTRON_MTU

此测试检查 MTU 大小的变化是否反映在 api 中。

成功标准

MTU 大小已反映。

10.20. NEUTRON_QOS

QoS 被定义为保证某些网络要求（如带宽、延迟、jitter 和可靠性）能够满足应用程序供应商和最终用户之间的服务级别协议(SLA)。此测试会检查与 QoS 相关的所有规则和策略都可以正确应用到 neutron 资源。

成功标准

与 QoS 相关的规则和策略成功应用到 neutron 资源。

10.21. NEUTRON_RBAC

此测试检查是否可在不同的 neutron 资源上执行所有 RBAC 操作。

成功标准

RBAC 操作可以在不同的 neutron 资源上成功完成。

10.22. NEUTRON_SECURITY_GROUPS

通过安全组和安全组规则，管理员和租户能够指定允许通过端口的流量和方向(ingress/egress)的类型。安全组是安全组规则的容器。此测试会检查在驱动程序/插件实现该功能时可以完成的所有安全组相关操作。

成功标准

安全组相关的操作成功执行。

10.23. NEUTRON_SERVICE_TYPES

使用此功能，您可以确保端口总是使用不同的子网，如实例和路由器接口。此测试将检查是否可以正确完成子网服务类型的所有基本操作。

成功标准

子网服务相关操作成功执行。

10.24. NEUTRON_SUBNET_ALLOCATION

它涉及为子网自动分配地址，而不是在创建时请求子网详情。此测试检查 neutron 的子网池功能的测试。

成功标准

neutron 已成功执行的子网池操作。

10.25. NEUTRON_SUBNET_DEFAULT_POOL

此测试会检查默认子网池的操作。

成功标准

默认子网池操作成功

10.26. NEUTRON_TAGS

各种虚拟网络资源支持标签供外部系统或网络服务 API 的任何其他客户端使用。此测试将检查是否可执行所有标签相关的操作。

成功标准

标签相关的操作成功执行。

10.27. NEUTRON_TRUNK

网络中继服务允许多个网络使用单一虚拟 NIC (vNIC)连接到实例。通过将多个网络连接到一个端口，可以将多个网络提供给实例。此测试检查是否可以执行所有中继相关操作。

成功标准

中继相关操作成功执行。

10.28. NEUTRON_BORDER_GATEWAY_PROTOCOL_VPN

这是 RHOSP16 中引入的新测试，对应于新的功能 Border Gateway Protocol Virtual Private Network (BGP VPN)。

BGP VPN 支持 L3VPN 和 Neutron 资源间的连接，如网络、路由器和端口。要在多个站点之间提供隔离连接，基于 BGP 的 VPN 允许网络操作员为其客户提供 VPN 服务。

BGP VPN 允许您的实例连接到现有的第 3 层 VPN 服务。创建 BGP VPN 网络后，您可以将其与项目关联，允许项目的用户连接到 BGP VPN 网络。

neutron_border_gateaway_protocol_vpn 测试认证以下 tempest 测试操作：

- create
- delete
- list

- 显示
- update

成功标准

所有 BGP VPN 相关操作都成功执行。

其他资源

有关 neutron 测试的更多信息，请参阅 实施 OpenStack API 的产品。

第 11 章 OPENSTACK 配置测试

从 Red Hat OpenStack Platform (RHOSP) 15 开始，OpenStack 配置测试将是合作伙伴提供新的测试。此测试适用于 Manila 和 Neutron 插件认证测试计划，只计划用于控制器节点。OpenStack 配置测试包括并支持 Open Virtual Network 子测试。

- 打开虚拟网络子测试

Open Virtual Network (OVN)是基于 Open vSwitch 的软件定义型网络(SDN)解决方案，为实例提供网络服务。OVN 应该已配置且可操作。此子测试验证 OVN 的状态。

成功标准

测试的状态取决于 OVN，如下所示：

- 如果 OVN 为 ON，则测试状态为 PASS。
- 如果 OVN 是 OFF，则测试状态为 FAIL。
- 如果 OVN 未知，则测试状态为 REVIEW。

11.1. 其他资源

有关 OVN 的更多信息，请参阅 OVN 架构。

第 12 章 可信容器测试

Trusted Container 测试检查红帽是否识别 Red Hat OpenStack Platform (RHOSP)插件/驱动程序容器。该测试还会验证容器是否是由红帽提供的，还是您。认证的容器镜像减少了客户必须用于部署的源数量，它还确保解决方案堆栈中包含的所有组件都来自可信源。

RHOSP 认证测试工作

在 RHOSP 认证测试过程中，受信任的容器测试会捕获有关已安装和运行容器的信息。在捕获了信息后，测试会查询红帽认证服务来确定容器是否可被识别和认证。

合作伙伴的要求

如果您的驱动程序作为 RHOSP (In Tree)的一部分提供，则应该只运行受信任的容器测试，因为容器镜像已经认证。但是，如果您提供自己的容器镜像（树外），作为前提条件，合作伙伴必须使用 Red Hat Connect 认证容器镜像。有关容器镜像认证的更多信息，请参阅 合作伙伴集成指南。

在 Red Hat 中，当合作伙伴为 RHOSP 13 创建新产品请求时，他们只能选择 Release Category as Tech-Preview。您可以在 Red Hat Connect 上认证容器镜像后执行受信任的容器测试。成功完成受信任的容器测试后，合作伙伴可以选择正式发行(GA)选项。

成功标准

您已收到了一个容器报告，其中显示了在 overcloud 控制器节点上运行和非运行的容器。该报告显示，RHOSP 服务（如 cinder、manila 和 neutron ）已安装并运行。根据 RHOSP 认证测试，正在运行的容器可以是 RHOSP 认证或红帽认证的容器。

第 13 章 原位升级

从 Red Hat OpenStack Platform (RHOSP) 16.1.1 开始，在新的 In-place Upgrades 测试中使用了升级(FFU)的框架。此测试可在 RHOSP 插件认证过程中提供。它验证插件的功能，以便在 RHOSP 的长生命版本之间进行自动升级期间和之后按预期执行。成功完成此测试后，会将相应的功能添加到生态系统目录条目中以进行认证。

示例

"In-place upgrade from RHOSP 13 (Queens) " 功能会在 RHOSP 16.1.x (Train)认证中显示为一行项目。

in_place_upgrades 测试可用于认证的所有插件类型。它将出现在认证测试计划中，且仅在 Controller 节点上计划和执行。此功能因此测试要求通过 RHOSP Director 工具集安装、管理和升级插件。它在控制器节点上执行后运行，并将内省升级环境中的各种日志文件，以验证是否已执行升级。

原位升级测试包括以下子测试：

- in_place_upgrades

  此测试验证 RHOSP 云已使用 RHOSP Framework for Upgrades 机制从一个 RHOSP 长生命版本升级到下一个 RHOSP 长生命周期版本。然后提示您确认这一点。

  成功标准

  - PASS：如果系统成功升级，则代表您使用相同的升级。
  - FAIL：如果系统没有升级，或者您没有认证相同的。

- director 插件验证

  添加了一个自声明提示，供您声明插件安装是通过 director 完成的。

  成功标准

  - PASS：如果您认证插件安装是通过 director 完成的。

- FAIL：如果您认证插件安装没有通过 director 来完成。

成功标准

原位升级测试的状态取决于：

- PASS：如果 subtests、in_place_upgrades 和 Director 插件验证通过。
- FAIL ：如果 或 subtest，in_place_upgrades 和 Director 插件验证失败。