Red Hat Certified Cloud and Service Provider Certification 2024

Red Hat Certified Cloud 和 Service Provider Certification 政策指南

用于红帽认证的云和服务供应商 1.0

Last Updated: 2024-06-25

Red Hat Certified Cloud and Service Provider Certification 2024 Red Hat Certified Cloud 和 Service Provider Certification 政策指南

用于红帽认证的云和服务供应商 1.0

法律通告

摘要

本文档论述了 CCSP 合作伙伴希望根据 Red Hat Enterprise Linux 提供基础架构即服务(IaaS)的技术和操作认证要求。 版本 9.0 和 8.80 更新了 2024 年 5 月 28 日。

目录

使开源包含更多

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

第 1 章 红帽认证云和服务提供商认证政策简介

1.1. 受众

使用本指南了解为 CCSP 合作伙伴实施的技术和操作认证要求，他们希望提供基于 Red Hat Enterprise Linux 的基础设施即服务(PaaS)、平台即服务(PaaS)或托管服务。认证工具和方法为在 Red Hat Enterprise Linux 上构建的云应用程序镜像提供帮助。

1.2. 为我们的共同客户创建值

作为认证的云和服务提供程序(CCSP)，您需要认证您在目录中发布的镜像。认证流程包括一系列测试，为您的红帽客户保证在云提供商之间具有一致的体验，客户体验具有最高级别的支持，以及为客户提供良好的安全实践。

云认证测试套件(redhat-certification-cloud)包括三个测试（可支持、配置、安全性），每个测试都有一系列子测试和检查，如下所述。需要向红帽提交包含所有三个云测试以及测试套件自我检查测试(rhcert/selfcheck)的运行日志，以进行新的认证和重新ation。

大多数云认证子测试都提供即时的返回状态(Pass/Fail)；但是，一些子测试可能需要红帽详细审查才能确认成功。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。此状态表示尚未遵循最佳实践。带有 WARN 状态的测试保证注意或操作，但不会阻止认证成功。建议合作伙伴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 CCSP 认证工作流指南。

1.3. 测试套件版本

您必须安装最新版本的认证工具，并使用最新的工作流进行认证。发布新版本的认证工具后，红帽会在 90 天后支持之前的工具和工作流。

在 90 天 周期结束时，使用之前的版本生成的测试日志/结果会自动被拒绝，您应该使用最新的工具和工作流重新生成测试日志/结果。

通过红帽订阅管理提供最新版本的 认证工具和工作流，并记录在 CCSP 认证工作流指南中。

1.4. 支持的 RHEL 版本和架构

认证在以下 RHEL 版本和构架上被支持。

RHEL 版本	架构

RHEL 版本	架构
RHEL 9	• 64 位 AMD 和 Intel • 64-bit IBM Z • 64-bit ARM • little endian IBM Power 系统
RHEL 8	• 64 位 AMD 和 Intel • 64-bit IBM Z • 64-bit ARM • little endian IBM Power 系统
RHEL 7	• 64 位 AMD 和 Intel • little endian IBM Power 系统

有关 hypervisor 支持的详情，请查看 Red Hat OpenStack Platform、Red Hat Virtualization 和 OpenShift Virtualization 中的认证客户机操作系统。

1.5. 了解 PASSTHROUGH 认证

当提供与现有云认证的副本相同的镜像时，使用 passthrough 认证，并在不同的镜像名称下列出。

您可以从最初认证的常规或金级 RHEL 镜像创建 passthrough 常规或金级 RHEL 镜像。

提交 passthrough 镜像认证请求的策略需要您：

- 确保镜像是原始认证镜像的副本，但名称可能不同。
- 与原始镜像认证一样，给定运行的镜像以实例类型依赖的配置数据的形式包括原始静态 on-disk 镜像文件中的特定偏移。

第 2 章 RED HAT CERTIFICATION SELF CHECK

2.1. 红帽认证自我检查(RHCERT/SELFCHECK)测试

红帽认证自我检查测试也称为 **rhcert/selfcheck**，确认认证过程中所需的所有软件包都已安装，且尚未更改。这样可确保测试环境已准备好获得认证流程，并且所有认证软件包都支持。

注意

对于认证测试或任何其他目的，不得修改证书软件包。

成功标准

测试环境包括认证过程中所需的所有软件包，并且没有修改软件包。

2.2. 系统报告

系统报告(sosreport)测试（也称为 **cloud/sosreport** ）捕获基本的 sosreport。

红帽使用一个名为 sos 的工具从 RHEL 系统收集配置和诊断信息，并协助客户对系统进行故障排除并遵循推荐做法。系统报告子测试可确保 sos 工具在 image/system 中按预期功能，并捕获基本的 sosreport。

成功标准

镜像上可以捕获基本的 sosreport。

其他资源

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

第 3 章 支持性

可支持性测试（也称为 **云/支持** ）检查镜像是否在红帽可支持的环境中运行，并至少包括 RHEL 的最小安装。

另外，测试会检查镜像是否由红帽内核和用户空间软件组成，并支持红帽更新和修复。

测试包括以下子测试。

3.1. 日志版本子测试

日志版本 subtest 检查它是否可以找到主机上安装的 RHEL 版本和在测试下安装的内核版本。

成功标准

- 测试可以成功同时检测到 RHEL 版本和内核版本。

3.2. 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？

3.3. 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？

3.4. 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。

- 检查测试下的系统是否满足最低硬件要求。

  - **RHEL 8 和 9** ：每个 CPU 逻辑内核数的最小系统 RAM 应该为 1.5GB。

  - **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 。

3.5. HYPERVISOR/分区子测试

Hypervisor/Partitioning 子测试确认 RHEL 镜像中显示的主机架构受 RHEL、CCSP 程序和内核的支持。目前，CCSP 镜像认证支持以下现有和即将发布的 RHEL 版本和相应的架构：

- **RHEL 8 和 9**: x86_64, ppc64le, IBM Z

- **RHEL 7**: x86_64, ppc, ppc64, ppc64le

成功标准

- RHEL 8 和 9 的 PASS 场景在 RHEL KVM、Nutanix、VMware 和 HyperV 上是 x86_64。它还在 BareMetal、PowerVM 和 RHV for Power 上包括 ppc64le。
- RHEL 7 的 PASS 场景在 RHEL KVM、Nutanix、VMware 和 HyperV 上是 x86_64。它还包括 PowerVM 上的 ppc 和 ppc64le，在 BareMetal、PowerVM 和 RHV for Power 上包括 ppc 和 ppc64le。

3.6. 文件系统布局子测试

Filesystem Layout 确认镜像的类型和最小大小遵循每个 RHEL 版本的准则。这样可确保镜像具有有效操作、运行应用程序和安装升级所需空间，供客户使用。

成功标准

- **RHEL 8 和 9** ： root 文件系统大小为 10 GB 或更大。引导文件系统是一个 1GB xfs 分区。
- **RHEL 7** ：根文件系统是一个 10 GB ext4 或 xfs 分区，或更大。

3.7. 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

3.8. 软件存储库子测试

软件存储库确认配置了相关的红帽存储库，并且已在镜像上导入了 GPG 密钥，以避免从不支持的内容中潜在的显著风险。

红帽在 Red Hat 官方软件存储库（附带附加订阅）中提供核心软件包/内容，这些存储库使用 GPG 密钥签名，以确保分布式文件的真实性。作为这些软件仓库的一部分提供的软件，客户生产环境完全支持且可靠。

如果需要启用云环境，可以配置由红帽发布但不受红帽支持的软件仓库，如 EPEL 或 RHEL Supplementary 和 Optional，也可以配置非红帽软件仓库。但是，必须正确描述并批准此类存储库。

成功标准

- 配置了受支持的红帽软件仓库。
- 红帽存储库的 GPG 密钥已在镜像中导入。
- 有效的软件仓库是 Red Hat Update Infrastructure 和 Red Hat Satellite。
- 必须启用 RHEL 8 和 AppStream 存储库。
- 镜像上配置的红帽软件仓库与镜像内容匹配。
- 在需要时，非红帽软件仓库才能正确配置和描述云的操作。

注意

要验证红帽存储库，合作伙伴必须通过以下关键字之一配置其基础 URL：*satellite*、*redhat.com* 或 *rhui* 之一。

其他资源

- 如需更多信息，请参阅产品支持覆盖范围。

3.9. 容器

RHEL 支持打算在混合云中使用容器的客户。

software/container 测试会验证：

- 如果安装了 Red Hat 容器工具。如果没有安装它们，且不是最小 RHEL 安装的一部分，测试将确认可以从 RHEL registry 安装该工具，并可下载和执行容器。
- 如果 RHEL 云镜像上的容器是由红帽提供的，或者是红帽认证合作伙伴容器。如果需要将任何其他容器用于云操作，则必须在您的文档中提到它们。

成功标准

- 所有已安装的容器都可以由红帽提供或认证。
- **podman** 工具已安装，也可以在测试运行期间安装。RHEL 8 和 9 镜像支持安装。
- **podman** 工具可以下载并运行示例红帽容器。
- **registry.redhat.io** registry 在 RHEL 镜像上安装 podman 后已启用或已启用。

3.10. INSIGHTS 子测试

Insights 子测试会在 RHEL 8 和 9 上验证 **insights-client** rpm。

成功标准

- **insights-client** rpm 安装在 RHEL 8 和 RHEL 9 上。

3.11. 软件模块测试

RHEL 模块功能是系统上可用的软件包集合。软件模块测试验证 RHEL 8 或 RHEL 9 系统中可用的模块。

成功标准

如果存在非红帽软件模块，则测试会失败。

第 4 章 镜像配置概述

镜像配置测试（也称为 **云/配置** ）确认镜像已根据红帽标准进行配置，以便客户在集成环境中的多个云供应商和镜像中具有统一和一致的体验。

cloud/configuration 测试包括以下子测试：

4.1. 默认系统日志

确认默认系统日志服务(syslog)被配置为将日志存储在镜像的 **/var/log/** 目录中，以便在需要时快速解决问题。

成功标准

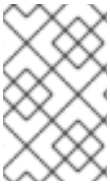
基本系统日志存储在镜像的 **/var/log/** 目录中。

4.2. 网络配置测试

网络配置确认默认防火墙服务(iptables)正在运行，运行 SSHD 的端口 22 将打开，端口 80 和 443 已打开或关闭，所有其他端口都已关闭。这样可确保镜像默认不受未授权访问的影响，并具有已知的访问配置。

这也可确保客户有 SSH 访问镜像，并且能够在没有额外配置的情况下快速部署 HTTP 应用程序。如果需要其他端口才能正确操作云基础架构，但必须记录此类端口。

只有在镜像上打开端口 22、80 （可选）、443 （可选）时，此测试才会在运行时显示状态(Pass)。如果其他端口处于打开状态，这个测试会要求在红帽上查看开放端口的描述，以确认成功或失败。



注意

作为认证过程的一部分，红帽认证应用程序默认在端口 8009 上运行。红帽认证应用程序也可以在认证测试期间在另一个开放端口上运行，但建议仅在测试期间打开此端口，而不是在镜像配置中作为默认值打开。

成功标准

- 根据 RHEL 版本，确保启用并运行以下服务：

RHEL 版本	服务
RHEL 9	**firewalld** 或 **nftables**
RHEL 8.3 及更新的版本	**firewalld** 或 **nftables**
RHEL 8 到 8.2	**firewalld** 和 **nftables** 或 **firewalld** 和 **iptables**
RHEL 7	**firewalld**

- sshd 已启用并在端口 22 上运行，并可访问
- 需要打开任何其他端口才能正确操作云基础架构，并记录

- 红帽认证应用程序在端口 8009 上运行（或其他配置的端口）
- 所有其他端口都关闭

注意

允许 httpd 服务，但不需要在端口 80 和/或端口 443 上运行。

4.3. 默认操作系统运行级别

确认当前系统运行级别为 3、4 或 5。此子测试可确保镜像以所需的模式/状态运行，且所有所需的系统服务（如网络）正在运行。

成功标准

当前运行级别为 3、4 或 5。

其他资源

有关运行级别的更多信息，请参阅：

- **RHEL 9** ：使用 systemd 目标.
- **RHEL 8** ：使用 systemd 目标.
- **RHEL 7** ：使用 systemd 目标.

4.4. 系统服务

系统服务确认 root 用户可以启动和停止系统上的服务。这样可确保拥有系统管理特权的客户可以访问/处理系统上的应用程序和服务，并执行需要以无缝方式管理访问的所有任务。系统服务还确保配置与已安装系统服务的实际状态之间没有差距。

成功标准

- root 用户可以启动和停止红帽产品提供的系统服务。
- 对于所有安装的系统服务，实际状态应与其配置的状态匹配。例如，如果服务已启用，则它应处于 running 状态。

其他资源

有关获取所需权限的更多信息，请参阅：

- **RHEL 9** ：管理 sudo 访问.
- **RHEL 8** ：管理 sudo 访问.
- **RHEL 7** ：获得权限.

4.5. 订阅服务

确认配置了所需的红帽订阅，可用并处理镜像，并且更新机制是 Red Hat Satellite 或 RHUI。这样可保证客户能够获取对通过标准红帽软件包更新或交付机制支持其应用程序所需的软件包和更新。

成功标准

镜像已配置，并且能够从 Red Hat Satellite 或 RHUI 订阅管理服务下载、安装和升级软件包。

第 5 章 安全实践概述

安全实践测试也称为 **云/安全性**，确认镜像是否遵循一组最低标准安全实践。它们还确认（但目前不需要）安装了最新的红帽安全更新。

cloud/security 测试包括以下子测试：

5.1. 密码配置测试

密码配置 测试检查 HUT 上是否启用了登录身份验证服务，并且服务正在使用 SHA512 加密算法。测试可确保镜像使用标准 SHA512 加密和解密算法来获得最佳性能。

对于 RHEL 7，配置集使用 **authconfig** 工具。对于 RHEL 8 和 9，它使用 **authselect** 工具。

成功标准

- 为系统验证启用 SHA-512 加密算法。
- 如果没有配置 NIS、SSSD 或 winbind 服务，则 RHEL 8 和 RHEL 9 的测试会失败，因为这些服务支持 SHA-512 算法。

5.2. RPM 最新

确认已安装针对镜像中包含的红帽软件包发布的所有重要和关键安全勘误。红帽建议您在发布勘误时更新并重新认证其镜像。此测试在运行时显示状态(REVIEW)，因为它需要在红帽审核来确认成功或失败。

成功标准

为已安装的红帽软件包发布的所有重要和关键安全勘误均有效。

其他资源

- 有关红帽安全评级的更多信息，请参阅 了解红帽安全评级。

5.3. SELINUX ENFORCING SUBTEST

Security-Enhanced Linux (SELinux)强制子测试确认 SELinux 已启用并在镜像上运行。

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，在系统范围内强制使用，用户不会自行设置。它减少了权限升级攻击的漏洞，并限制配置过程中出现的损坏。如果进程被破坏，攻击者只能访问该进程的正常功能，以及已配置进程可访问的文件。

成功标准

在镜像上配置并在 enforcing 模式下运行 SELinux。

其他资源

有关 SELinux 的详情，请参考：

- **RHEL 9** ：使用 SElinux.
- **RHEL 8** ：使用 SElinux.

- **RHEL 7** ：SELinux 用户和管理员指南.