Red Hat Enterprise Linux 7

虚拟化安全指南

在 RHEL 上的虚拟化环境中保护主机、客户机和共享基础架构

Last Updated: 2023-03-25

Red Hat Enterprise Linux 7 虚拟化安全指南

在 RHEL 上的虚拟化环境中保护主机、客户机和共享基础架构

Enter your first name here. Enter your surname here.
Enter your organisation's name here. Enter your organisational division here.
Enter your email address here.

法律通告

摘要

本指南概述了红帽提供的虚拟化安全技术。它还提供有关在虚拟环境中保护主机、客户机以及共享基础架构和资源的建议。

目录

第 1 章 简介

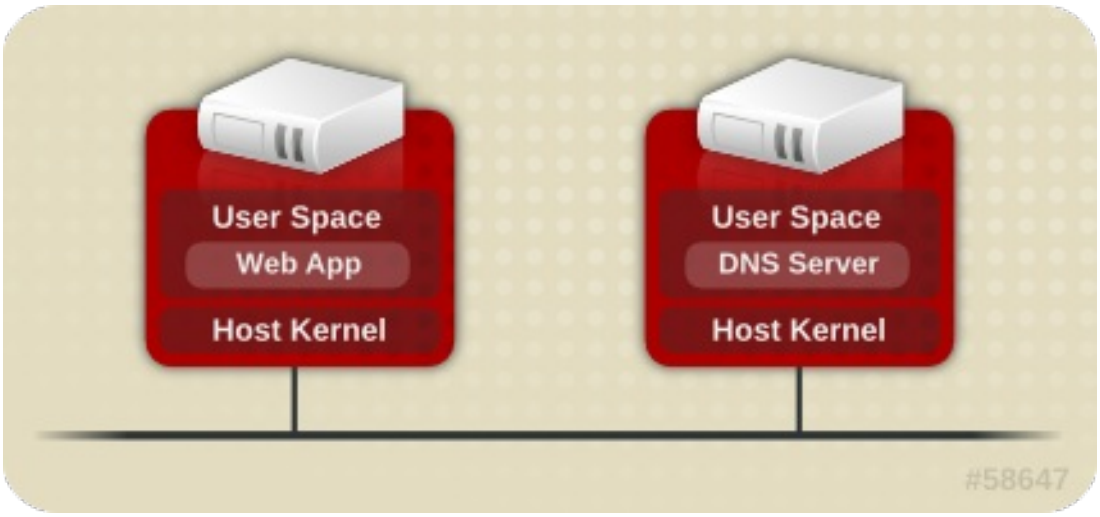
1.1. 虚拟化和非虚拟化环境

虚拟化环境为发现新攻击向量和消除以前可能未为攻击者带来价值的现有漏洞提供了机会。因此，务必要采取措施，确保在创建和维护虚拟机时物理主机和客户机的安全性。

非虚拟化环境

在非虚拟化环境中，主机在物理上相互隔开，每一主机都具有自包含的环境，它由 Web 服务器或 DNS 服务器等服务组成。这些服务直接与自己的用户空间（主机内核和物理主机）通信，为它们的服务直接提供网络。

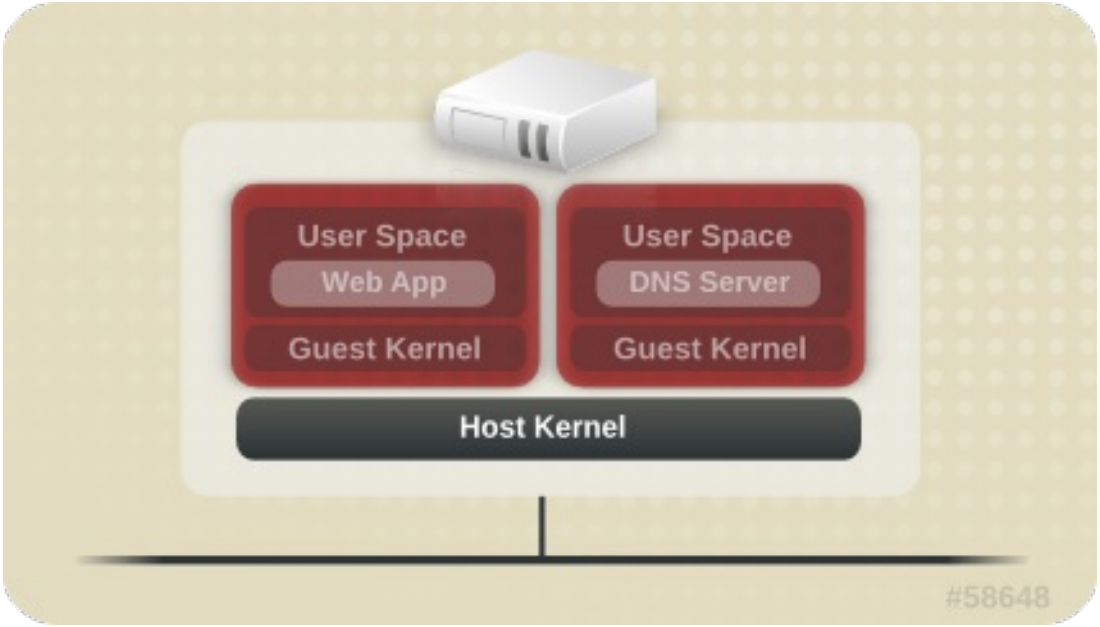
图 1.1. 非虚拟化环境



虚拟化环境

在虚拟化环境中，可以在单一主机内核和物理主机内存放多个操作系统（作为客户机虚拟机）。

图 1.2. 虚拟化环境



如果未虚拟化服务，则物理分隔计算机。因此，除网络攻击外，任何漏洞通常包含在受影响的机器上。当服务分组在虚拟化环境中时，系统中会出现额外的漏洞。如果管理程序中存在可能被客户机实例利用的安全漏洞，此 guest 可能会攻击主机，以及在该主机上运行的其他客户机。

1.2. 虚拟化安全性问题的原因

在您的基础架构中部署虚拟化可带来许多好处，但也会带来新的风险。虚拟化资源和服务应该根据以下安全考虑进行部署：

- 主机和管理程序成为主要目标；它们通常是客户机和数据的单一故障点。
- 虚拟机可能会以不必要的方式相互干扰。如果没有访问控制来帮助防止此问题，则一个恶意 guest 可以绕过存在漏洞的管理程序并直接访问主机系统上的其他资源，例如存储其他客户机。
- 资源和服务可能变得难以跟踪和维护；随着虚拟化系统的快速部署越来越需要资源管理，包括足够的补丁、监控和维护。
- 存储等资源可以分散在多台机器上，并依赖于它。这会导致环境过于复杂，管理和维护的系统也较差。
- 虚拟化不会消除环境中存在的任何传统安全风险；必须保护整个解决方案堆栈，而不仅仅是虚拟化层。

本指南旨在通过为红帽企业 Linux 提供多种虚拟化推荐做法来帮助您降低安全风险，从而帮助您保护虚拟化基础架构。

第 2 章 主机安全性

在红帽企业 Linux 系统上部署虚拟化技术时，主机负责管理和控制物理设备、存储和网络以及所有虚拟机的访问权限。如果主机系统泄露，则客户机及其数据也变得易受攻击。

因此，保护红帽企业 Linux 主机系统是确保安全虚拟化平台的第一步。

2.1. 保护主机物理机器

以下任务和提示可帮助您保护红帽企业 Linux 主机的可靠性并确保其性能。

- 确保为安装正确配置了 SELinux，并以 enforcing 模式运行：

  ```
  # setenforce 1
  ```

  除了是一种良好的安全实践外，sVirt 提供的高级虚拟化安全功能还依赖于 SELinux。有关 SELinux 和 sVirt 的详情，请查看 第 4 章 *sVirt*。

- 删除或禁用任何不必要的服务，如 **AutoFS**、**NFS**、**FTP**、**HTTP**、**NIS**、**telnetd** 或 **sendmail**。

- 仅添加服务器上平台管理所需的最少用户帐户数量，并删除不必要的用户帐户。将直接访问系统限制为需要管理系统的用户。考虑禁止共享的 **root** 访问权限，而是使用 **sudo** 等工具来根据管理员的管理角色授予管理员特权访问权限。

- 避免在您的主机上运行任何不必要的应用程序。在主机上运行应用可能会影响虚拟机性能，并影响服务器稳定性。任何可能导致服务器崩溃的应用也将导致服务器中的所有虚拟机发生故障。此外，易受攻击的应用程序可能会成为主机上攻击的向量。

- 将中央位置用于虚拟机安装和映像。虚拟机映像应存储在 **/var/lib/libvirt/images/** 下。如果您的虚拟机镜像使用不同的目录，请确保在 **SELinux** 策略中添加该目录，并在开始安装前重新标记该目录。强烈建议在中央位置使用可共享的网络存储。

- 仅运行支持使用和管理 **guest** 系统所需的服务。如果您需要提供其他服务（如文件或打印服务），请考虑在 **Red Hat Enterprise Linux** 客户机上运行这些服务。

- 确保主机系统上启用了审计，并且 **libvirt** 已配置为生成审计记录。启用审计后，**libvirt** 会生成关于客户机配置更改和启动/停止事件的审计记录，这可帮助您跟踪 **guest** 的状态。此外，也可以使用特殊的 **auvirt** 实用程序查看 **libvirt** 审计事件。如需更多信息，请使用 **man auvirt** 命令。

- 确保系统的任何远程管理都仅通过安全网络通道进行。**SSH** 等实用工具以及 **TLS** 或 **SSL** 等网络协议同时提供身份验证和数据加密，以帮助确保只有经过批准的管理员可以远程管理系统。

- 确保已为您的安装正确配置了防火墙，并在引导时激活了防火墙。应当仅允许使用和管理系统所需的网络端口。

- 不要授予虚拟客户机直接访问整个磁盘或块设备（例如 **/dev/sdb**）；而是使用分区（如 **/dev/sdb1**）或 **LVM** 卷作为 **guest** 存储。

- 当虚拟机无法使用 **SR-IOV** 时，附加 **USB** 设备、物理功能或物理设备可以提供对设备的访问权限，该设备足以覆盖该设备的固件。这会带来一个潜在的安全问题，攻击者可能会因为恶意代码覆盖设备的固件，并在虚拟机或主机引导时移动该设备时出现问题。

  建议您在适用的情况下使用 **SR-IOV** 虚拟功能设备分配。

注意

有关主机系统的更多安全提示和说明，请参阅*Red Hat Enterprise Linux 安全指南*。

2.2. 客户端访问控制

libvirt的客户端访问控制框架允许系统管理员在客户端用户、受管对象和 API 操作之间设置精细的权限规则。这使得客户端连接可以锁定到一组最少的特权。

在默认配置中，**libvirtd** 守护进程有三个级别的访问控制：

1. 所有连接都以未经身份验证的状态开始，其中唯一允许的 API 操作是完成身份验证所需的操作。
2. 身份验证成功后，连接具有对所有 libvirt API 调用的完整、不受限制的访问权限，或者根据客户端连接源自的套接字将其锁定为"只读"操作。
3. 访问控制框架允许经过身份验证的连接具有由管理员定义的细粒度权限规则。

libvirt 中的每个 API 调用都有一组权限，这些权限将针对使用的对象进行验证。如果 API 调用中设置了特定标志，还将检查进一步的权限。除了检查传递给 API 调用的对象外，一些方法还会过滤其结果。

2.2.1. 访问控制驱动程序

访问控制框架设计为可插拔系统，以便将来与任意访问控制技术集成。默认情况下使用 **none** 驱动程序，它根本不执行访问控制检查。目前，libvirt 支持将 polkit 用作真正的访问控制驱动程序。要了解如何使用 polkit 访问驱动程序，请参阅配置文档。

访问驱动程序在 **/etc/libvirt/libvirtd.conf** 配置文件中使用 ***access_drivers*** 参数进行配置。此参数接受一组访问控制驱动程序名称。如果请求多个访问驱动程序，则所有访问驱动程序都必须成功才能授予访问权限。要启用 **'polkit'** 作为驱动程序，请使用 **augtool** 命令：

```
# augtool -s set '/files/etc/libvirt/libvirtd.conf/access_drivers[1]' polkit
```

要将驱动程序设置为默认（没有访问控制），请输入以下命令：

```
# augtool -s rm /files/etc/libvirt/libvirtd.conf/access_drivers
```

若要使 **libvirtd.conf** 所做的更改生效，请重新启动 **libvirtd** 服务。

```
# systemctl restart libvirtd.service
```

2.2.2. 对象和权限

libvirt 将访问控制应用到其 API 中的所有主要对象类型。每一对象类型依次定义了一组权限。要确定为特定 API 调用检查哪些权限，请参阅相关 API 参考手册文档。有关对象和权限的完整列表，请参阅 libvirt.org。

2.2.3. 将块设备添加到客户机时的安全问题

- 主机物理计算机不应使用文件系统标签来识别**fstab** 文件、**initrd** 文件或内核命令行中的文件系统。如果客户机虚拟机对整个分区或 LVM 卷具有写入访问权限，那么执行此操作会带来安全风险，因为客户机虚拟机可能会将属于主机物理计算机的文件系统标签写入其自己的块设备存储。重新引导主机物理计算机时，主机物理计算机随后可能会错误地将 guest 虚拟机的磁盘用作系统磁盘，这会破坏主机物理计算机系统。

最好使用设备的 UUID 在 **/etc/fstab** 文件中、/ **dev/initrd** 文件或在内核命令行上识别它。

- 客户机虚拟机不应被授予对整个磁盘或块设备的写入访问权限（例如 **/dev/sdb**）。可访问整个块设备的客户机虚拟机可以修改卷标签，这些标签可用于破坏主机物理计算机系统。使用分区（例如 **/dev/sdb1**或 **LVM** 卷）以防止此问题。有关 **LVM** 管理和配置示例的详情，请参阅使用 **CLI** 命令或 **LVM** 配置示例进行 **LVM** 管理。

  如果您使用对分区的原始访问，如 **/dev/sdb1** 或原始磁盘，如 **/dev/sdb**，您应该将 **LVM** 配置为仅扫描安全的磁盘，使用 **global_filter** 设置。有关使用 **global_filter** 命令的 **LVM** 配置脚本示例，请参阅逻辑卷管理器管理指南。

2.3. 公共云 OPERATOR 的特殊注意事项

公共云服务提供商会暴露在传统虚拟化用户之外的一系列安全风险。由于恶意客户机威胁以及整个虚拟化基础架构中对客户数据保密性和完整性的要求，虚拟客户机隔离在主机和客户机之间以及客户机之间至关重要。

除了之前列出的 **Red Hat Enterprise Linux** 虚拟化推荐做法外，公共云操作员还应考虑以下项目：

- 不允许从客户机直接访问硬件。**PCI**、**USB**、**FireWire**、**Thunderbolt**、**eSATA** 和其他设备直通机制使得管理困难，通常依赖于底层硬件来强制区分客户机。

- 将云操作员的私有管理网络与客户虚拟客户机网络和客户网络相互隔离，以便：

  - 虚拟机无法通过网络访问主机系统。

  - 个客户无法直接通过云提供商的内部网络访问其他客户的客户机系统。

第 3 章 虚拟机安全性

3.1. 客户机安全性关系原因

虽然主机系统的安全性对于确保主机上运行的客户机的安全性至关重要，但它并未免除正确保护各个客户机计算机的需求。当系统作为虚拟 **guest** 运行时，与传统非虚拟化系统相关的所有安全风险仍然存在。如果客户机系统出现故障，客户机系统可访问的任何资源（如关键业务数据或敏感客户信息）均可能变得易受攻击。

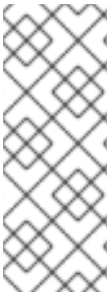
3.2. 虚拟机安全推荐做法

红帽企业 **Linux** *安全指南中记录的保护红帽企业* **Linux** 系统的所有推荐做法均适用于传统非虚拟化系统和作为虚拟客户机安装的系统。但是，在虚拟环境中运行客户机时，有几个安全实践至关重要：

- 由于 **guest** 的所有管理可能远程发生，请确保仅通过安全网络通道进行系统管理。**SSH** 等工具以及 **TLS** 或 **SSL** 等网络协议提供身份验证和数据加密，以确保只有经过批准的管理员可以远程管理系统。

- 某些虚拟化技术使用特殊的客户机代理或驱动程序来启用某些特定的虚拟化功能。确保使用标准红帽企业 **Linux** 安全功能（如 **SELinux**）保护这些代理和应用程序。

- 在虚拟化环境中，访问敏感数据的风险更大，超过客户机系统保护边界。使用 **dm-crypt** 和 **GnuPG** 等加密工具保护存储的敏感数据；虽然需要特别注意确保加密密钥的机密性。



注意

使用页面重复数据删除技术（如 **Kernel Same-page Merging(KSM)**）可能会引入可能会用于跨客户机泄漏信息的侧信道。在存在问题的情况下，可以全局或逐个客户禁用 **KSM**。有关 **KSM** 的详情请参考 **Red Hat Enterprise Linux 7 Virtualization** 调整和优化指南。

3.3. 内核地址空间随机化

红帽企业 **Linux 7.5** 及更高版本包括 **KVM** 虚拟机的内核地址空间随机化**(KASLR)**功能。**KASLR** 启用随机化内核映像压缩的物理和虚拟地址，从而防止客户机根据内核对象的位置被利用。

KASLR 默认激活，但可以通过在客户机的内核命令行中添加 **nokaslr** 字符串来取消激活。要编辑客户机引导选项，请使用以下命令，其中 ***guestname*** 是您的客户端的名称：

```
# virt-edit -d guestname /etc/default/grub
```

之后修改 **GRUB_CMDLINE_LINUX** 行，例如：

```
GRUB_CMDLINE_LINUX="rd.lvm.lv=rhel/root rd.lvm.lv=rhel/swap rhgb quiet nokaslr"
```

重要

从已激活 **KASLR** 的客户机转储创建的虚拟机转储文件无法被崩溃实用程序读取。要修复这个问题，请在客户机的 **XML** 配置文件的 **<features>** 部分添加 **<vmcoreinfo/>** 元素。

但请注意，如果目标主机使用不支持 **<vmcoreinfo/>** 的操作系统，则迁移带有 **<vmcoreinfo/>** 的客户机会失败。其中包括红帽企业 **Linux 7.4** 和更早版本，以及红帽企业 **Linux 6.9** 及更早版本。

3.4. 使用 VIRT-MANAGER 创建安全红帽企业 LINUX 7 虚拟机

此流程涵盖使用本地存储的安装 **DVD** 或者 **DVD** 镜像创建 **SecureBoot Red Hat Enterprise Linux 7 guest** 虚拟机。**Red Hat Enterprise Linux 7 DVD** 镜像包括在红帽客户门户网站中。

SecureBoot 功能可确保虚拟机正在运行加密签名的操作系统。如果一个虚拟机的客户机操作系统已被恶意软件更改，**SecureBoot** 会阻止虚拟机启动，从而停止恶意软件到您的主机计算机的潜在传播。

过程 **3.1.** 使用本地安装介质使用 **virt-manager** 创建 **SecureBoot Red Hat Enterprise Linux 7** 客户机虚拟机

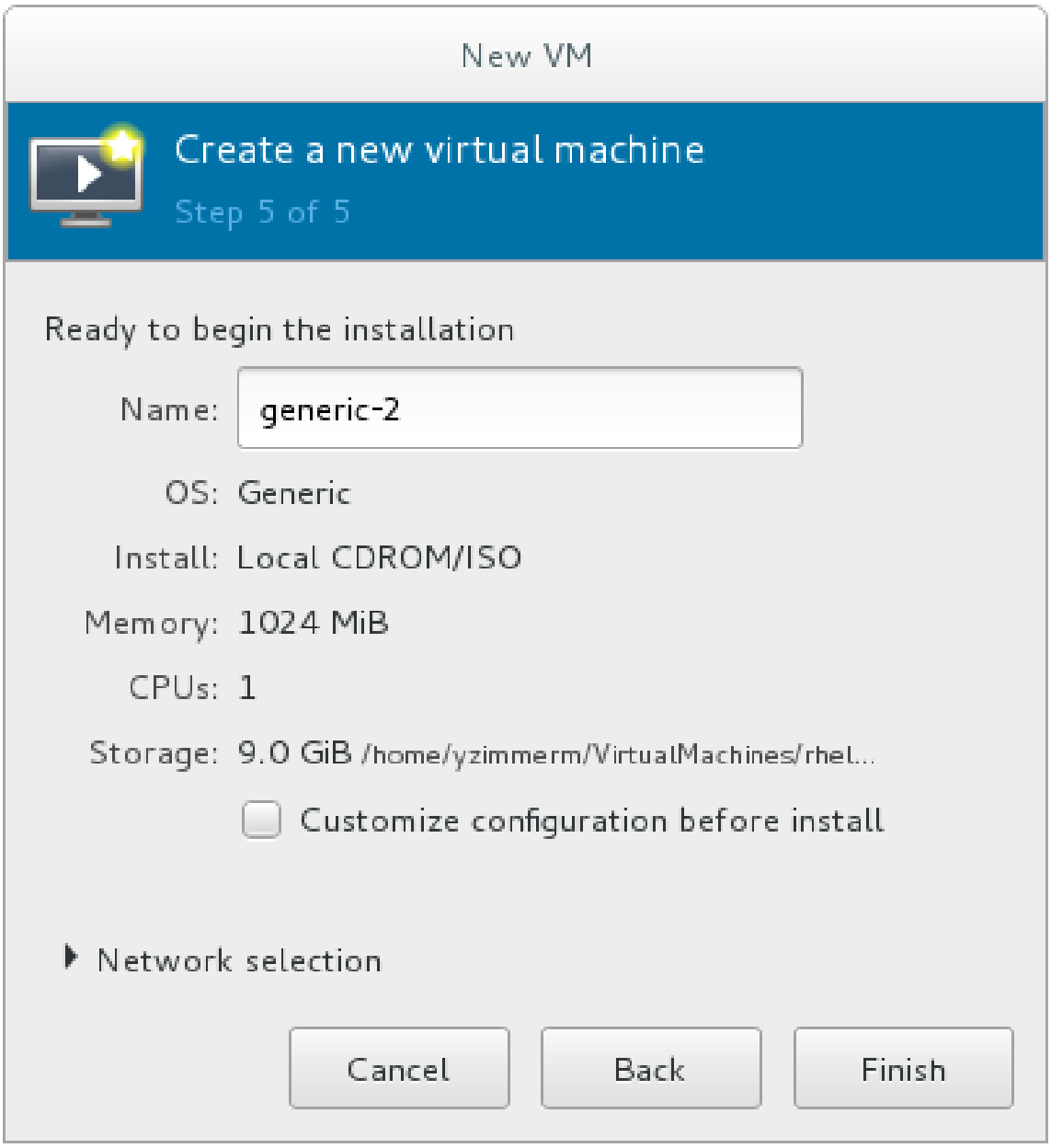
1. 执行使用 **virt-manager** 创建红帽企业 **Linux 7** 虚拟机的步骤 **1** 到 **6**。

2. 名称和最终配置

   将虚拟机命名为。虚拟机名称可以包含字母、数字和以下字符：下划线(_)、句点(.)和连字符(-)。虚拟机名称对于迁移而言必须是唯一的，且不能只包含数字。

   默认情况下，将为名为"default"的网络使用网络地址转换(NAT)创建虚拟机。若要更改网络选择，可单击网络选择，再选择主机设备和源模式。

图 **3.1.** 验证配置



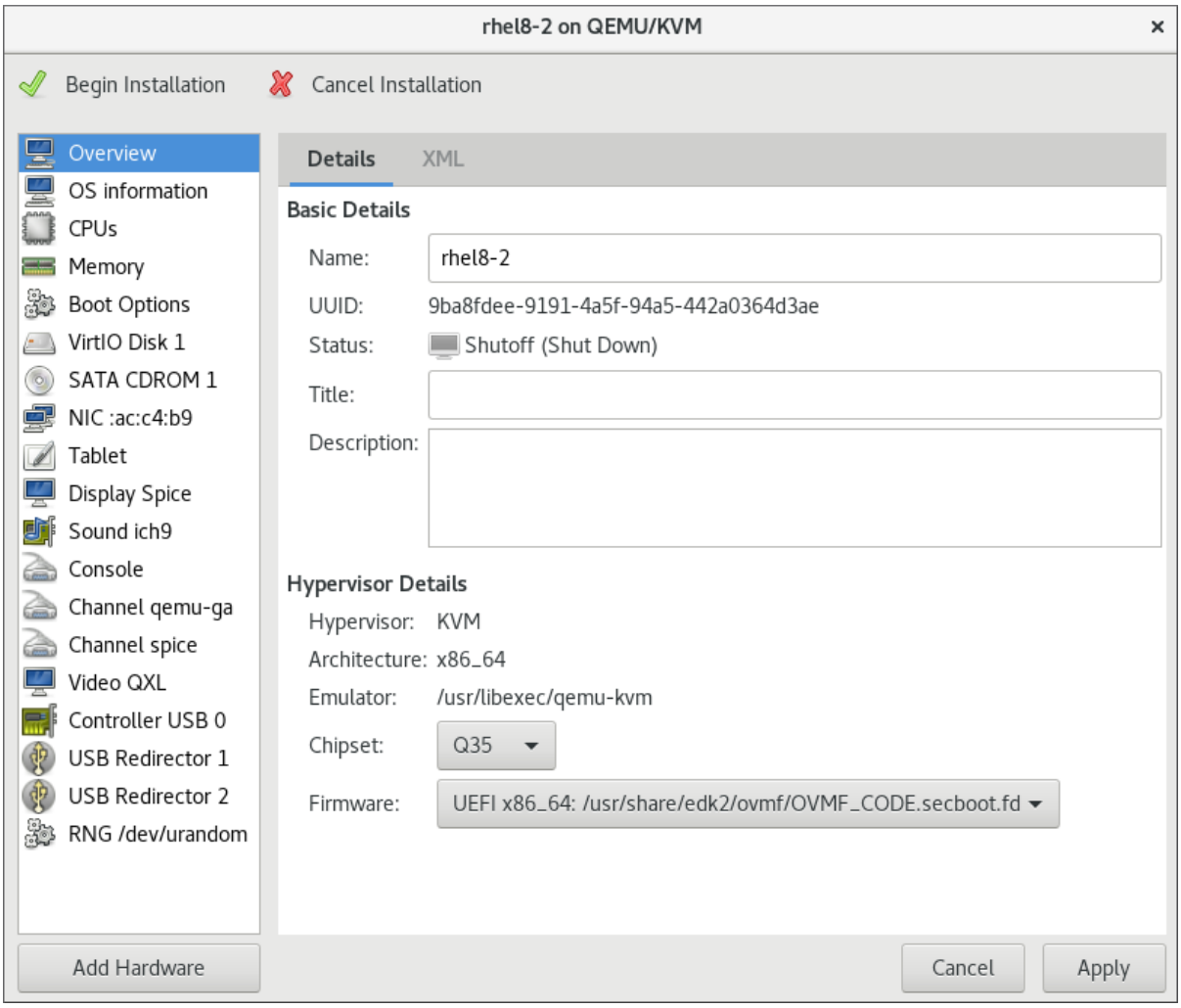
要进一步配置虚拟机的硬件，请在安装前选中自定义配置以更改 **guest** 的存储或网络设备，以使用半虚拟化**(virtio)**驱动程序或添加其他设备。验证虚拟机的设置，并在您满意时单击**"**完成**"**。这将为 **futher** 配置虚拟机打开一个新向导。

3. 自定义虚拟机硬件

在向导的 **Overview** 部分中，在 **Chipset** 下拉菜单中选择 **Q35**。

在 **Firmware** 下拉菜单中选择 **UEFI x86_64**。

图 **3.2.** 配置硬件窗口



验证虚拟机的设置，然后在您满意时单击 **Apply**。

单击 **Begin Installation**，创建具有指定网络设置、虚拟化类型和架构的虚拟机。

SecureBoot Red Hat Enterprise Linux 7 客户机虚拟机现在从 **ISO** 安装磁盘镜像创建。

第 4 章 SVIRT

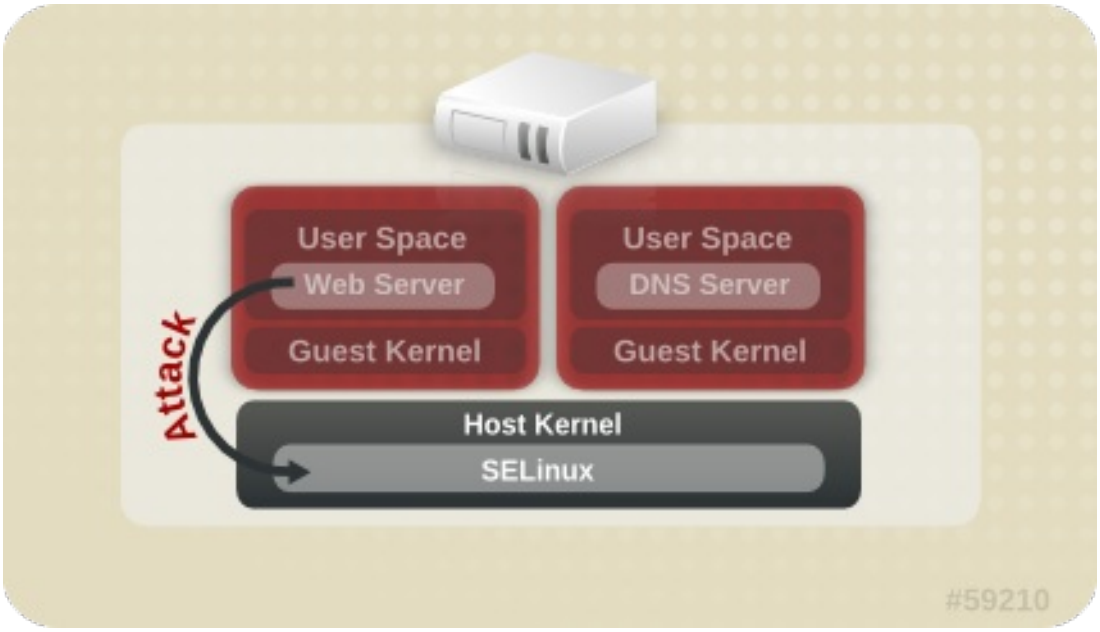
4.1. 简介

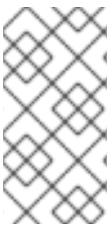
由于 **KVM** 下的虚拟机是作为 **Linux** 进程实施的，**KVM** 使用标准 **Linux** 安全模型来提供隔离和资源控制。**Linux** 内核包含 **Security-Enhanced Linux(SELinux)**，通过灵活、可自定义的安全策略添加强制访问控制**(MAC)**、多级安全**(MLS)**和多类别安全**(MCS)**。**SELinux** 为 **Linux** 内核（包括虚拟机进程）上运行的进程提供严格的资源隔离和限制。**sVirt** 项目基于 **SELinux** 构建，以进一步启用虚拟机隔离和受控共享。例如，细粒度权限可应用于将虚拟机分组到一起以共享资源。

从安全角度而言，管理程序很可能是攻击者的目标，因为被破坏的虚拟机监控程序可能导致主机系统上运行的所有虚拟机。将 **SELinux** 集成到虚拟化技术有助于提高管理程序安全性，防御试图访问主机系统或其他虚拟机的恶意虚拟机。

下图代表 **SELinux** 隔离客户机，这限制了被入侵的虚拟机监控程序（或客户机）启动进一步攻击的能力，或者扩展到另一个实例：

图 **4.1. SELinux** 隔离的攻击路径





注意

有关 **SELinux** 的更多信息，请参阅 **Red Hat Enterprise Linux SELinux** 用户和管理员指南。

4.2. SELINUX 和强制访问控制(MAC)

Security-Enhanced Linux(SELinux)是在 **Linux** 内核中实现 **MAC**，在检查标准自主访问控制**(DAC)**

后检查允许的操作。**SELinux** 可以针对正在运行的进程及其操作实施用户可定制的安全策略，包括尝试访问文件系统对象。在 **Red Hat Enterprise Linux** 中默认启用，**SELinux** 限制了利用应用程序和系统服务（如虚拟机监控程序）中漏洞可能导致的潜在损坏范围。

sVirt 与虚拟化管理抽象层 **libvirt** 集成，为虚拟机提供 **MAC** 框架。此架构允许 **libvirt** 支持的所有虚拟化平台以及 **sVirt** 支持的所有 **MAC** 实施互操作。

4.3. SVIRT 配置

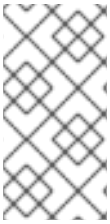
SELinux 布尔值是可打开或关闭、快速启用或禁用功能或其他特殊条件的变量。通过运行 **setsebool *boolean_name* {on|off}** 或 **setsebool -P *boolean_name* {on|off}** 可以切换布尔值，使更改在重新引导后保留。

下表显示了在 **libvirt** 启动时影响 **KVM** 的 **SELinux** 布尔值。通过运行 **getsebool -a|grep virt** 命令可以找到这些布尔值（ **on** 或 **off**）的当前状态。

表 **4.1. KVM SELinux** 布尔值

SELinux 布尔值	描述
staff_use_svirt	使员工用户能够创建和转换到 sVirt 域。
unprivuser_use_svirt	使非特权用户能够创建和转换到 sVirt 域。
virt_sandbox_use_audit	启用沙盒容器来发送审核信息。
virt_sandbox_use_netlink	启用沙盒容器使用 netlink 系统调用。
virt_sandbox_use_sys_admin	启用沙盒容器使用 sys_admin 系统调用，如 mount。
virt_transition_userdomain	启用虚拟进程作为用户域运行。
virt_use_comm	启用 virt 使用串行/并行通信端口。
virt_use_execmem	支持受限虚拟客户机使用可执行内存和可执行堆栈.
virt_use_fusefs	启用 virt 读取 FUSE 挂载的文件。
virt_use_nfs	启用 virt 管理 NFS 挂载的文件。
virt_use_rawip	启用 virt 与 rawip 套接字交互。
virt_use_samba	启用 virt 管理 CIFS 挂载的文件。

SELinux 布尔值	描述
virt_use_sanlock	启用受限制的虚拟客户机与 sanlock 交互。
virt_use_usb	启用 virt 使用 USB 设备。
virt_use_xserver	启用虚拟机与 X 窗口系统交互。



注意

有关 **SELinux** 布尔值的更多信息，请参阅 **Red Hat Enterprise Linux SELinux** 用户和管理员指南。

4.4. SVIRT 标记

与受 **SELinux** 保护的其他服务一样，**sVirt** 使用基于流程的机制、标签和限制，为虚拟客户机实例提供额外的安全性和控制。标签基于当前运行的虚拟机（动态）自动应用到系统上的资源，但也可以由管理员（静态）手动指定，以满足可能存在的任何特定要求。

要编辑客户机的 **sVirt** 标签，使用 **virsh edit *guest_name*** 命令并添加或编辑 **<seclabel>** 元素，如下一节所述。**<seclabel>** 可用作整个客户机的根元素，也可以指定为 **<source>** 元素的子元素，用于选择给定设备的特定 **sVirt** 标签。

有关 **<seclabel>** 元素的综合信息，请参阅 **libvirt** 上游文档。

4.4.1. sVirt Labels 类型

下表概述了可以分配给虚拟机进程、镜像文件和共享内容等资源的不同 **sVirt** 标签：

表 4.2. sVirt Labels

类型	SELinux 上下文	description/Effect
虚拟机进程	system_u:system_r:svirt_t:*MCS1*	*MCS1* 是一个随机选择的字段。目前支持约 500,000 个标签。
虚拟机镜像	system_u:object_r:svirt_image_t:*MCS1*	*只有具有相同MCS1* 字段的 *svirt_t* 进程才能读取/写入这些镜像文件和设备。

类型	SELinux 上下文	description/Effect
虚拟机共享读取/写入内容	system_u:object_r:svirt_image_t:s0	所有 *svirt_t* 进程都可写入到 *svirt_image_t:s0* 文件和设备。
虚拟机共享只读内容	system_u:object_r:svirt_content_t:s0	所有 *svirt_t* 进程都可以读取具有此标签的文件/设备。
虚拟机镜像	system_u:object_r:virt_content_t:s0	镜像退出时使用的系统默认标签.不允许 *svirt_t* 虚拟进程读取使用该标签的文件/设备。

4.4.2. 动态配置

在 **SELinux** 中使用 **sVirt** 时，动态标签配置是默认的标记选项。请参阅以下示例来演示动态标记：

```
# ps -eZ | grep qemu-kvm

system_u:system_r:svirt_t:s0:c87,c520 27950 ？ 00:00:17 qemu-kvm
```

在本例中，**qemu-kvm** 进程的基础标签为 **system_u:system_r:svirt_t:s0**。**libvirt** 系统已为此进程生成了一个唯一的 **MCS** 标签 **c87,c520**。基本标签和 **MCS** 标签组合形成进程的完整安全标签。同样，**libvirt** 采用相同的 **MCS** 标签和基础标签来构成镜像标签。然后，此镜像标签会自动应用到虚拟机需要访问的所有主机文件，如磁盘映像、磁盘设备、**PCI** 设备、**USB** 设备以及内核/**initrd** 文件。每个进程都与具有不同标签的其他虚拟机隔离。

以下示例显示了虚拟机的唯一安全标签（本例中带有对应的 **MCS** 标签 **c87,c520** ），它们应用到 **/var/lib/libvirt/images** 中的客户机磁盘镜像文件：

```
# ls -lZ /var/lib/libvirt/images/*

  system_u:object_r:svirt_image_t:s0:c87,c520   image1
```

以下示例显示了客户机 **XML** 配置中的动态标记：

```
<seclabel type='dynamic' model='selinux' relabel='yes'>
  <label>system_u:system_r:svirt_t:s0:c87,c520</label>
  <imagelabel>system_u:object_r:svirt_image_t:s0:c87,c520</imagelabel>
</seclabel>
```

4.4.3. 使用基本标记进行动态配置

要在动态模式中覆盖默认基本安全标签，可在 **XML** 客户机配置中手动配置 **<baselabel>** 选项，如下例所示：

```
<seclabel type='dynamic' model='selinux' relabel='yes'>
  <baselabel>system_u:system_r:svirt_custom_t:s0</baselabel>
  <label>system_u:system_r:svirt_custom_t:s0:c87,c520</label>
  <imagelabel>system_u:object_r:svirt_image_t:s0:c87,c520</imagelabel>
</seclabel>
```

4.4.4. 使用动态资源标记进行静态配置

有些应用需要完全控制安全标签的生成，但仍需要 **libvirt** 来处理资源标签。以下客户机 **XML** 配置演示了带有动态资源标签的静态配置示例：

```
<seclabel type='static' model='selinux' relabel='yes'>
  <label>system_u:system_r:svirt_custom_t:s0:c87,c520</label>
</seclabel>
```

4.4.5. 没有资源标记的静态配置

主要用于多级安全**(MLS)**和其他严格控制的环境中，可以在不重新标记资源的静态配置。静态标签允许管理员为虚拟机选择特定的标签，包括 **MCS/MLS** 字段。运行静态标记虚拟机的管理员负责在镜像文件上设置正确的标签。虚拟机将始终使用该标签启动，**sVirt** 系统永远不会修改静态标记的虚拟机内容的标签。以下客户机 **XML** 配置演示了这种情况的示例：

```
<seclabel type='static' model='selinux' relabel='no'>
  <label>system_u:system_r:svirt_custom_t:s0:c87,c520</label>
</seclabel>
```

4.4.6. sVirt 标记和 NFS

要在 **NFSv4.1** 或者 **NFSv4.2** 文件系统中使用 **sVirt** 标签，需要为您要为客户端共享导出的 **NFS** 目录根目录将 **SELinux** 上下文改为 **virt_var_lib_t**。例如，如果您导出 **/exports/nfs/** 目录，使用以下命令：

```
# semanage fcontext -a -t virt_var_lib_t '/exports/nfs/'
# restorecon -Rv /exports/nfs/
```

此外，当 **libvirt** 动态为 **NFS** 卷中的虚拟客户机生成 **sVirt** 标签时，它只保证单一主机中的标签唯一性。这意味着，如果跨多个主机的大量客户机共享一个 **NFS** 卷，则可能会出现重复的标签，从而导致潜在的漏洞。

要避免这种情况，请执行以下操作之一：

- 为每个虚拟化主机使用不同的 **NFS** 卷。此外，在执行客户机迁移时，使用 **--migrate-disks** 和 **--copy-storage-all** 选项复制客户机存储。

- 使用 **virt-install** 命令创建新客户机时，请使用以下命令为客户机设置静态标签：

  - 使用 **--security** 选项：例如：

```
# virt-install --name guest1-rhel7 --memory 2048 --vcpus 2 --disk size=8 --cdrom
/home/username/Downloads/rhel-workstation-7.4-x86_64-dvd.iso --os-variant rhel7 --
security model=selinux,label='system_u:object_r:svirt_image_t:s0:c100,c200'
```

    这会为客户机上的所有磁盘设置安全标签。

  - 将 **--disk** 选项与 ***seclabel*** 参数搭配使用。例如：

```
# virt-install --name guest1-rhel7 --memory 2048 --vcpus 2 --disk
/path/to/disk.img,seclabel.model=selinux,seclabel.label='system_u:object_r:svirt_image_t:s0
c100,c200' --cdrom /home/username/Downloads/rhel-workstation-7.4-x86_64-dvd.iso --
os-variant rhel7
```

    这只在指定的磁盘上设置安全标签。

第 5 章 虚拟化环境中的网络安全性

5.1. 网络安全概述

在几乎所有情形中，网络是访问系统、应用和管理接口的唯一方式。由于网络在虚拟化系统的管理及其托管应用程序的可用性中起到至关重要的作用，因此确保进出虚拟化系统的网络通道安全非常重要。

保护网络可让管理员控制访问，保护敏感数据免受信息泄漏和篡改。

5.2. 网络安全建议做法

网络安全性是安全虚拟化基础架构的重要组成部分。请参见以下保护网络的建议做法：

- 确保系统的远程管理仅通过安全网络通道进行。**SSH** 等工具以及 **TLS** 或 **SSL** 等网络协议提供身份验证和数据加密，以帮助安全且受控的系统访问。
- 确保客户机应用程序通过安全的网络通道传输敏感数据。如果 **TLS** 或 **SSL** 等协议不可用，请考虑使用 **IPsec** 等协议。
- 配置防火墙并确保在引导时激活了防火墙。应当仅允许使用和管理系统所需的网络端口。定期测试和查看防火墙规则。

5.2.1. 保护到 SPICE 的连接性

SPICE 远程桌面协议支持 **SSL/TLS**，为所有 **SPICE** 通信渠道（主、显示、输入、光标、回放、记录）启用。

5.2.2. 保护到存储的连接

您可以通过许多不同的方式将虚拟化系统连接到网络化存储。每种方法都存在不同的安全优势和顾虑，但相同的安全原则适用于每种方法：在使用前验证远程存储池，并保护数据在传输期间的机密性和完整性。

数据在存储时也必须保持安全性。红帽建议在存储或存储数据前加密或进行数字签名。

注意

*有关联网存储的更多信息，请参阅《红帽企业 **Linux** 虚拟化部署和管理指南*》中的"存储池"一章。

附录 A. 更多信息

A.1. SELINUX 和 SVIRT

有关 **SELinux** 和 **sVirt** 的更多信息：

- 主 **SELinux** 网站：
- **SELinux** 文档：
- 主要 **sVirt** 网站：
- **Dan Walsh** 博客：

A.2. 虚拟化安全性

有关虚拟化安全的更多信息：

- **NIST**（国家标准与技术学院）完全虚拟化安全准则：

附录 B. 修订历史记录

修订 1.0-22 7.7 Beta 版发布的版本	Thu May 23 2019	Jiri Herrmann
修订 1.0-21 7.6 GA 发行的版本	Thu Oct 25 2018	Jiri Herrmann
修订 1.0-21 7.6 Beta 版发布的版本	Thu Aug 14 2018	Jiri Herrmann
修订 1.0-20 7.5 GA 发行的版本	Thu Apr 5 2018	Jiri Herrmann
修订 1.0-18 7.4 GA 发行的版本	Thu Jul 27 2017	Jiri Herrmann
修订 1.0-15 7.3 GA 发布的版本	Mon Oct 17 2016	Jiri Herrmann
修订 1.0-9 清理修订历史记录	Thu Oct 08 2015	Jiri Herrmann
修订 1.0-8 7.1 GA 版本.	Wed Feb 18 2015	Scott Radvan