Red Hat Enterprise Linux 9

使用 RHEL 9 web 控制台管理系统

具有基于 Web 的图形界面服务器管理

Last Updated: 2024-06-26

Red Hat Enterprise Linux 9 使用 RHEL 9 web 控制台管理系统

具有基于 Web 的图形界面服务器管理

法律通告

摘要

RHEL web 控制台是一个基于 Web 的图形界面，它基于上游 Cockpit 项目。通过使用它，您可以执行系统管理任务，如检查和控制 systemd 服务、管理存储、配置网络、分析网络问题以及检查日志。

目录

对红帽文档提供反馈

我们感谢您对我们文档的反馈。让我们了解如何改进它。

通过 Jira 提交反馈（需要帐户）

1. 登录到 Jira 网站。
2. 点顶部导航栏中的 **Create**
3. 在 **Summary** 字段中输入描述性标题。
4. 在 **Description** 字段中输入您对改进的建议。包括文档相关部分的链接。
5. 点对话框底部的 **Create**。

第 1 章 使用 RHEL WEB 控制台入门

了解如何安装 Red Hat Enterprise Linux 9 web 控制台、如何通过其方便的图形界面 添加和管理远程主机，以及如何监控 web 控制台管理的系统。

1.1. 什么是 RHEL WEB 控制台

RHEL web 控制台是一个基于 web 的界面，用于管理和监控您的本地系统，以及您网络环境中的 Linux 服务器。

RHEL web 控制台允许您执行广泛的管理任务，包括：

- 管理服务
- 管理用户帐户
- 管理及监控系统服务
- 配置网络接口和防火墙
- 检查系统日志
- 管理虚拟机
- 创建诊断报告
- 设置内核转储配置
- 配置 SELinux
- 更新软件
- 管理系统订阅

RHEL web 控制台使用与在终端中使用的同样的系统 API，终端中执行的操作会立即反映在 RHEL web 控制台中。

您可以监控网络环境中的系统日志及其性能，以图形的形式显示。另外，您可以在 web 控制台中直接或通过终端更改设置。

1.2. 安装并启用 WEB 控制台

要访问 RHEL web 控制台，请首先启用 **cockpit.socket** 服务。

在许多安装变体中，Red Hat Enterprise Linux 9 默认包括 web 控制台。如果您的系统每以包括，请在启用 **cockpit.socket** 服务前安装 **cockpit** 软件包。

流程

1. 如果在安装变体中没有默认安装 Web 控制台，请手动安装 **cockpit** 软件包：

```
# dnf install cockpit
```

2. 启用并启动 **cockpit.socket** 服务，该服务运行一个 Web 服务器：

```
# systemctl enable --now cockpit.socket
```

3. 如果在安装变体中没有默认安装 Web 控制台，且您使用自定义防火墙配置集，请将 **cockpit** 服务添加到 **firewalld** 中，以在防火墙中打开端口 9090：

```
# firewall-cmd --add-service=cockpit --permanent
# firewall-cmd --reload
```

验证步骤

- 要验证之前的安装和配置，请打开 web 控制台。

1.3. 登录到 WEB 控制台

当 **cockpit.socket** 服务正在运行并且相应的防火墙端口打开时，您可以在浏览器中第一次登录到 Web 控制台。

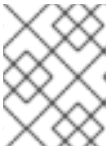
先决条件

- 使用以下浏览器之一打开 Web 控制台：
  - Mozilla Firefox 52 及更新的版本
  - Google Chrome 57 及更新的版本
  - Microsoft Edge 16 及更新的版本
- 系统用户帐户凭证
  RHEL web 控制台使用位于 **/etc/pam.d/cockpit** 的特定可插拔验证模块(PAM)堆栈。默认配置允许使用系统上任何本地帐户的用户名和密码登录。
- 在防火墙中端口 9090 已打开。

流程

1. 在网页浏览器中输入以下地址来访问 Web 控制台：

```
https://localhost:9090
```



注意

这为您提供了本地计算机上的 web 控制台登录。如果要登录到远程系统的 Web 控制台，请参阅 第 1.6 节 “从远程机器连接至 web 控制台”

如果您使用自签名证书，浏览器会显示一个警告。检查证书，并接受安全例外以进行登录。

控制台从 **/etc/cockpit/ws-certs.d** 目录中加载证书，并使用带有 **.cert** 扩展名的最后一个文件（按字母排序）。要避免接受安全例外的操作，安装由证书颁发机构（CA）签名的证书。

2. 在登录屏幕中输入您的系统用户名和密码。
3. 点 **Log In**。

成功验证后，会打开 RHEL web 控制台界面。

注意

要在有限和管理访问权限间进行切换，请在 web 控制台页面的顶部面板中点 **Administrative access** 或 **Limited access**。您必须提供用户密码以获取管理访问权限。

1.4. 更改 WEB 控制台的默认风格设置

默认情况下，Web 控制台采用浏览器设置中的风格设置。您可以从 RHEL 9 web 控制台界面覆盖默认的风格设置。

先决条件

- Web 控制台已安装并可以访问。详情请参阅安装 Web 控制台。

流程

1. 登录到 RHEL web 控制台。详情请参阅 Web 控制台的日志记录。
2. 在右上角，点 **Session** 按钮。
3. 在 **Style** 部分中，选择首选的设置。**Default** 设置使用与浏览器相同的样式设置。

验证步骤

1. 样式设置已根据设置风格进行了更改。

1.5. 在 WEB 控制台中禁用基本身份验证

您可以通过修改 **cockpit.conf** 文件来修改身份验证方案的行为。使用 **none** 操作来禁用身份验证方案，只允许通过 GSSAPI 和表单进行身份验证。

先决条件

- Web 控制台已安装并可以访问。详情请参阅安装 Web 控制台。
- 您有 **root** 特权或权限来使用 **sudo** 输入管理命令的命令。

流程

1. 在您首选的文本编辑器中，在 **/etc/cockpit/** 目录中打开或创建 **cockpit.conf** 文件，例如：

```
# vi cockpit.conf
```

2. 添加以下文本：

```
[basic]
action = none
```

3. 保存这个文件。
4. 重启 Web 控制台以使更改生效。

```
# systemctl try-restart cockpit
```

1.6. 从远程机器连接至 WEB 控制台

您可以从任何客户端操作系统以及手机或平板电脑连接到 Web 控制台界面。

先决条件

- 具有支持的互联网浏览器的设备，例如：
  - Mozilla Firefox 52 及更新的版本
  - Google Chrome 57 及更新的版本
  - Microsoft Edge 16 及更新的版本
- 您需要安装的并可访问 web 控制台的 RHEL 9 服务器。

流程

1. 打开浏览器。
2. 使用以下格式输入远程服务器地址：
   a. 使用服务器主机名：

   ```
   https://<server.hostname.example.com>:<port-number>
   ```

   例如：

   ```
   https://example.com:9090
   ```

   b. 使用服务器 IP 地址：

   ```
   https://<server.IP_address>:<port-number>
   ```

   例如：

   ```
   https://192.0.2.2:9090
   ```

3. 登录界面打开后，使用 RHEL 系统凭证登录。

1.7. 以 ROOT 用户身份从远程机器连接到 WEB 控制台

在 RHEL 9.2 或更高版本的新安装中，出于安全原因，RHEL web 控制台默认不允许 root 帐户登录。您可以在 **/etc/cockpit/disallowed-users** 文件中允许 **root** 登录。

先决条件

- RHEL 9 web 控制台已安装并启用。详情请参阅安装和启用 Web 控制台。

流程

1. 在您首选的文本编辑器中打开 **/etc/cockpit/** 目录中的 **disallowed-users** 文件，例如：

```
# vi /etc/cockpit/disallowed-users
```

2. 编辑文件并删除 **root** 用户的行：

```
# List of users which are not allowed to login to Cockpit root
```

3. 保存更改并退出编辑器。

验证

- 以 **root** 用户身份登录到 Web 控制台。详情请参阅 Web 控制台的日志记录。

1.8. 使用一次性密码登录到 WEB 控制台

如果您的系统是启用了一次性密码（OTP）配置的 Identity Management（IdM）域的一部分，您可以使用 OTP 登录到 RHEL web 控制台。

重要

只有在系统是启用了 OTP 配置的 Identity Management（IdM）域的一部分时，才可以使用一次性密码登录。

先决条件

- 已安装 RHEL web 控制台。
- 带有启用 OTP 配置的 Identity Management 服务器。
- 配置的硬件或软件设备生成 OTP 令牌。

流程

1. 在浏览器中打开 RHEL web 控制台：
   - 本地：**https://localhost:PORT_NUMBER**
   - 远程使用服务器主机名： **https://example.com:PORT_NUMBER**
   - 远程使用服务器 IP 地址： **https://EXAMPLE.SERVER.IP.ADDR:PORT_NUMBER**
     如果您使用自签名证书，浏览器会发出警告。检查证书并接受安全例外以进行登录。

     控制台从 **/etc/cockpit/ws-certs.d** 目录中加载证书，并使用带有 **.cert** 扩展名的最后一个文件（按字母排序）。要避免接受安全例外的操作，安装由证书颁发机构（CA）签名的证书。
2. 登录窗口将打开。在登录窗口中输入您的系统用户名和密码。
3. 在您的设备中生成一次性密码。
4. 在确认您的密码后，在 web 控制台界面中出现的新字段输入一次性密码。
5. 点**登录**。

6. 成功登录会进入 web 控制台界面的 **Overview** 页面。

1.9. 使用 WEB 控制台重启系统

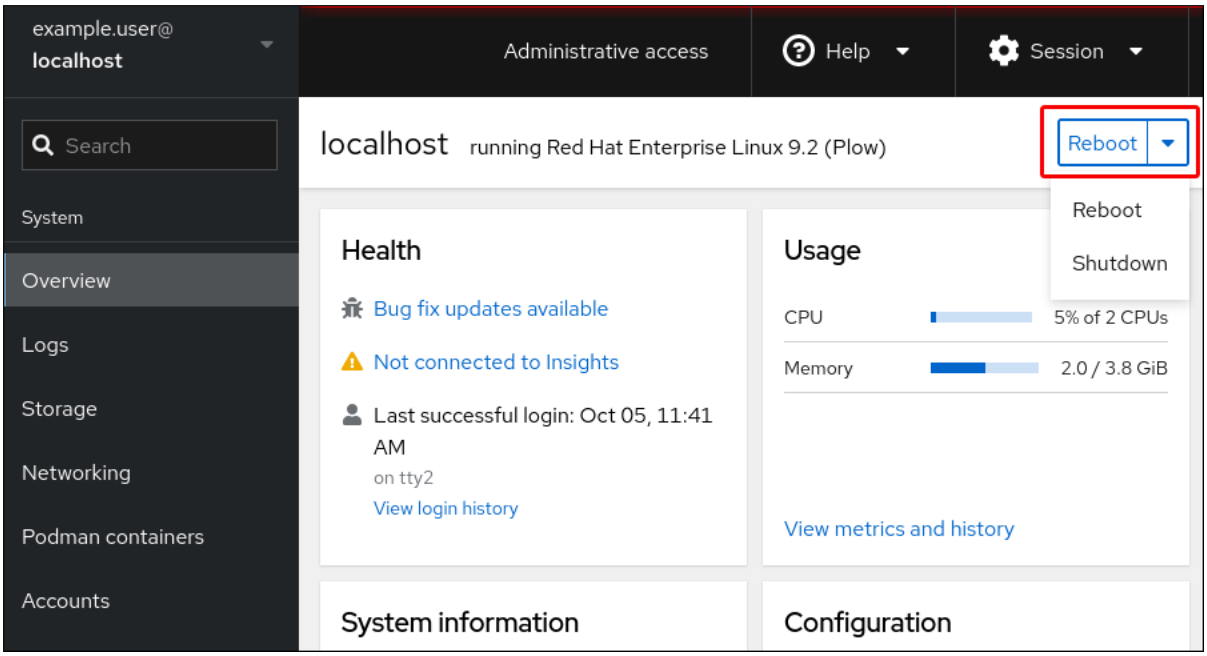
您可以使用 Web 控制台重启附加到 web 控制台的 RHEL 系统。

先决条件

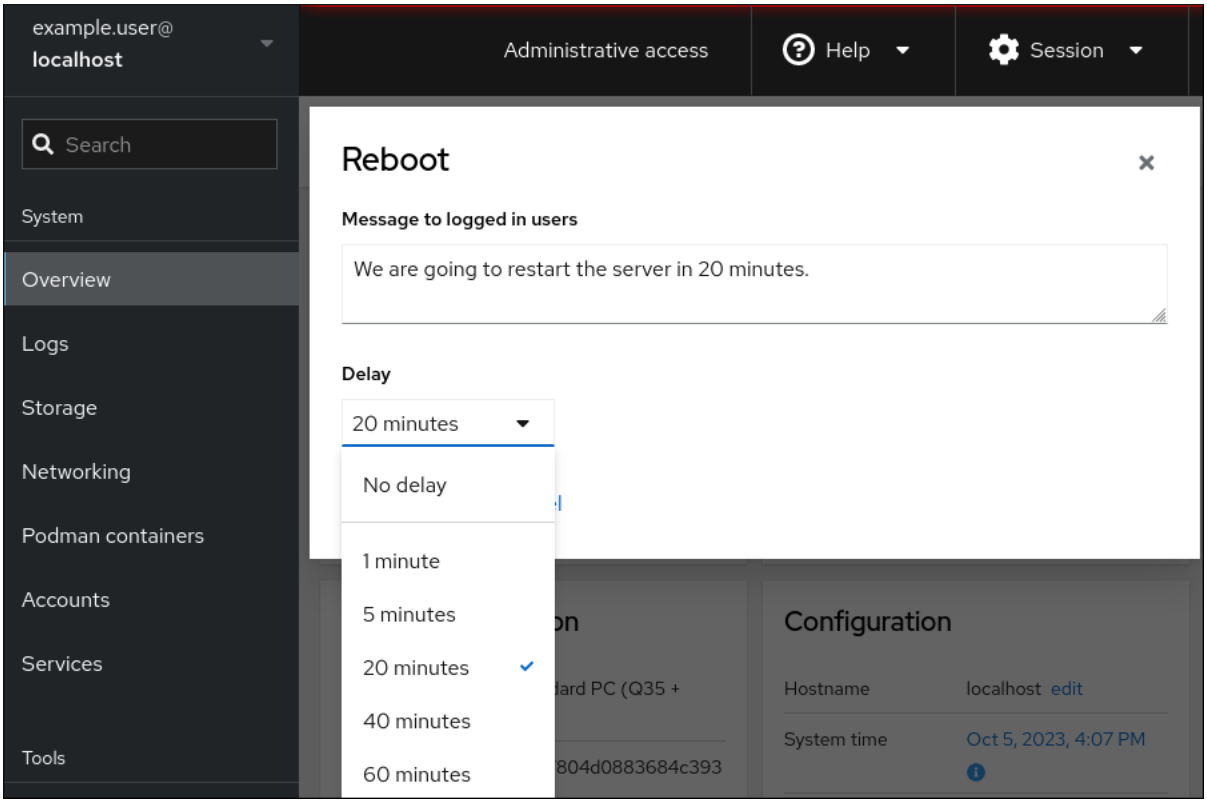
- Web 控制台已安装并可以访问。详情请参阅安装 Web 控制台。

流程

1. 登录到 RHEL web 控制台。详情请参阅 Web 控制台的日志记录。
2. 在 **Overview** 页面中，点 **Reboot** 按钮。



3. 如果有任何用户登录到系统，您可以在**重启**对话框中写入有关重启的消息。
4. 可选：在 **Delay** 下拉列表中，为重启延迟选择一个时间间隔。



5. 点**Reboot**。

1.10. 使用 WEB 控制台关闭系统

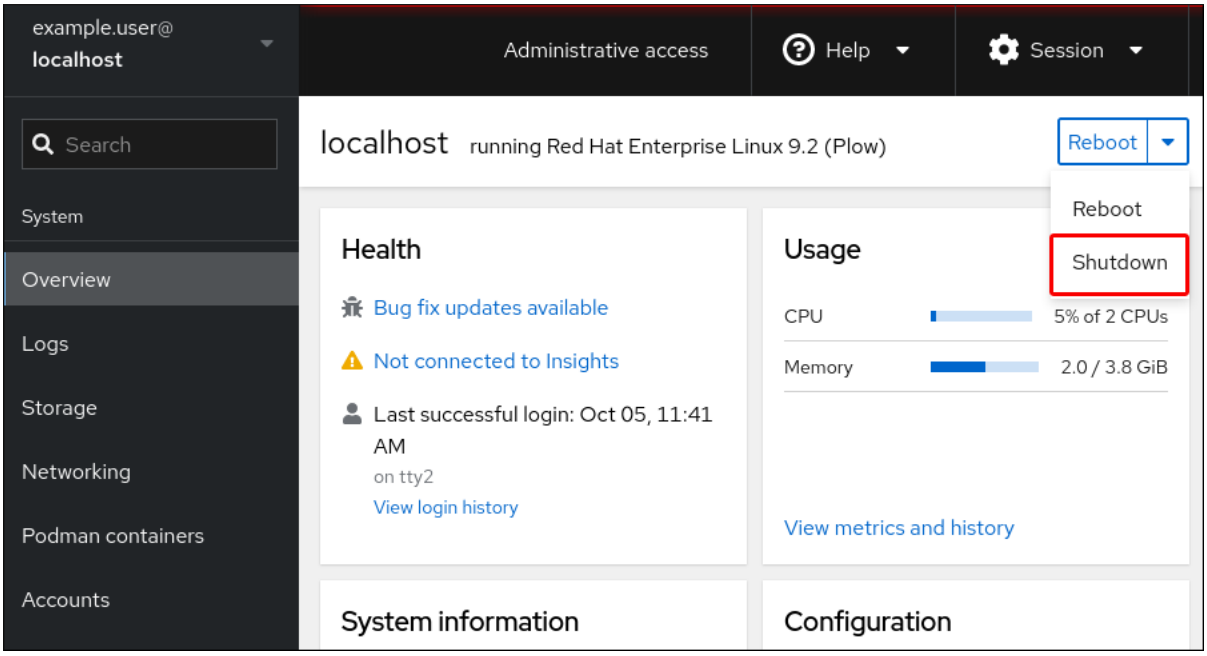
您可以使用 Web 控制台关闭附加到 web 控制台的 RHEL 系统。

先决条件

- Web 控制台已安装并可以访问。
  详情请参阅安装 Web 控制台。

流程

1. 登录到 RHEL web 控制台。
   详情请参阅 Web 控制台的日志记录。
2. 点 **Overview**。
3. 在 **Restart** 下拉列表中，选择 **Shut Down**。



4. 如果有用户登录到该系统，在 **Shut Down** 对话框中写入关闭的原因。
5. 可选：在 **Delay** 下拉列表中选择一个时间间隔。
6. 点 **Shut Down**。

1.11. 使用 WEB 控制台配置时间设置

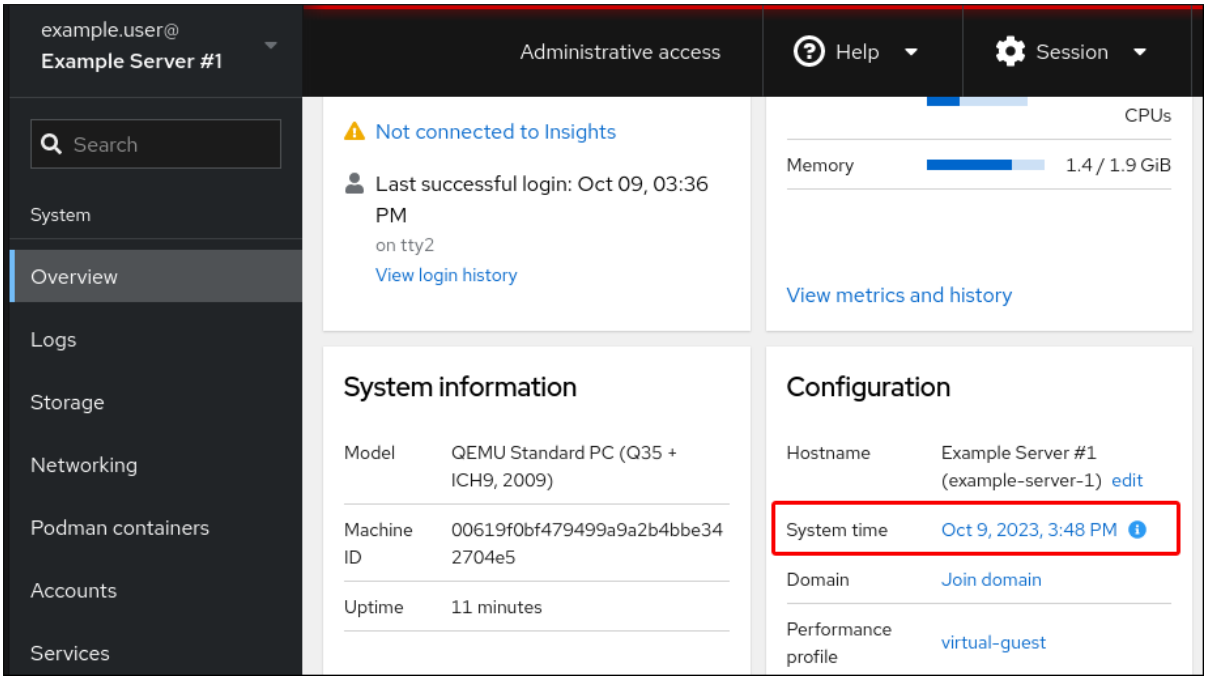
您可以设置时区并将系统时间与网络时间协议（NTP）服务器同步。

先决条件

- Web 控制台已安装并可以访问。
  详情请参阅安装 Web 控制台。

流程

1. 登录到 RHEL web 控制台。
   详情请参阅 Web 控制台的日志记录。
2. 点**概述**中的当前系统时间。



3. 点 **System time**。
4. 在 **更改系统时间** 对话框中，根据需要更改时区。
5. 在 **Set Time** 下拉菜单中选择以下之一：

   手动

   如果您需要手动设定时间，而不使用 NTP 服务器，则使用这个选项。

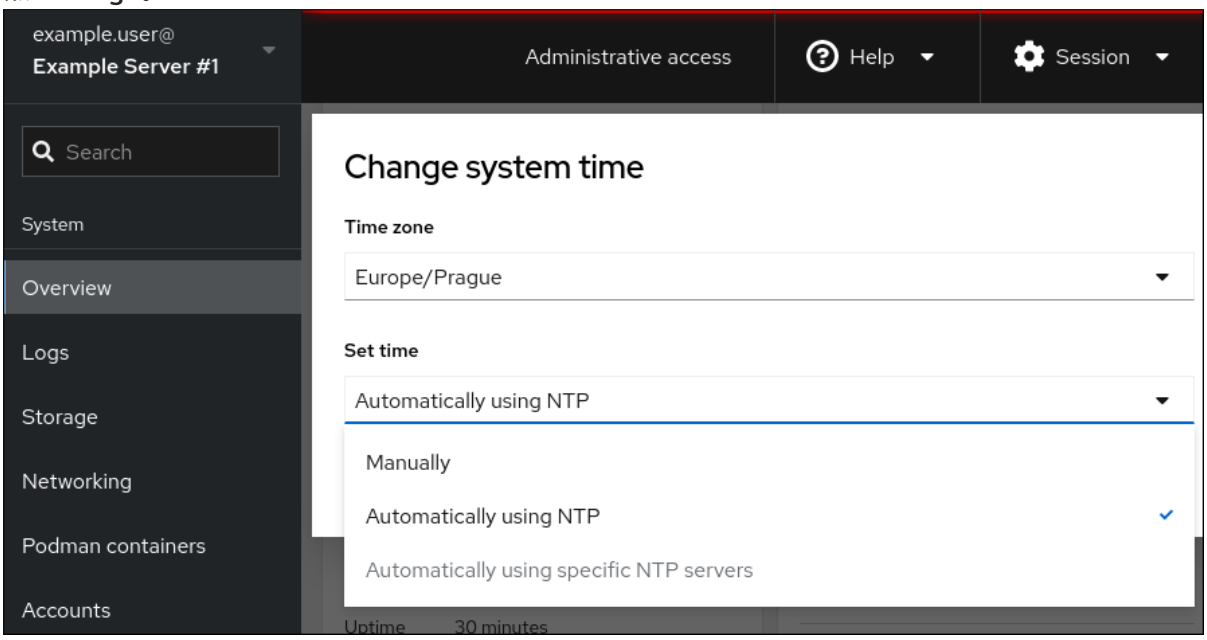
   自动使用 NTP 服务器

   这是一个默认选项，它会自动与预设置的 NTP 服务器同步。

   自动使用特定的 NTP 服务器

   只有在您需要将系统与特定 NTP 服务器同步时使用这个选项。指定服务器的 DNS 名称或 IP 地址。

6. 点 **Change**。



验证步骤

- 检查在 **System** 标签页中显示的系统时间。

其它资源

- 使用 Chrony 套件配置 NTP。

1.12. 使用 WEB 控制台禁用 SMT 以防止 CPU 安全问题

在出现滥用 CPU SMT 的攻击时禁用 Simultaneous Multi Threading（SMT）。禁用 SMT 可缓解安全漏洞（如 L1TF 或 MDS）对系统的影响。

重要

禁用 SMT 可能会降低系统性能。

先决条件

- 必须安装并可以访问 Web 控制台。详情请参阅安装 Web 控制台。

流程

1. 登录到 RHEL web 控制台。详情请参阅 Web 控制台的日志记录。
2. 在 **Overview** 选项卡中，找到 **系统信息** 字段并点查**看硬件详细信息**。
3. 在 **CPU Security** 行上，点 **Mitigations**。
   如果这个链接不存在，这意味着您的系统不支持 SMT，因此不会受到这个安全漏洞的影响。
4. 在 **CPU Security Toggles** 表中，打开 **Disable simultaneous multithreading (nosmt)** 选项。
5. 点**保存并重启**按钮。

系统重启后，CPU 不再使用 SMT。

其它资源

- L1TF - L1 Terminal Fault Attack - CVE-2018-3620 & CVE-2018-3646
- MDS - Microarchitectural Data Sampling - CVE-2018-12130, CVE-2018-12126, CVE-2018-12127, and CVE-2019-11091

1.13. 在登录页面中添加标题

您可以将 Web 控制台设置为在登录屏幕上显示横幅文件的内容。

先决条件

- Web 控制台已安装并可以访问。
  详情请参阅安装 Web 控制台。
- 您有 **root** 特权或权限来使用 **sudo** 输入管理命令的命令。

流程

1. 在您首选的文本编辑器中打开 **/etc/issue.cockpit** 文件：

```
# vi /etc/issue.cockpit
```

2. 将您要显示的内容作为横幅添加到文件中，例如：

```
This is an example banner for the RHEL web console login page.
```

   您不能在文件中包含任何宏，但您可以使用换行符和 ASCII 工件。

3. 保存这个文件。

4. 在您首选的文本编辑器中打开 **/etc/cockpit/** 目录中的 **cockpit.conf** 文件，例如：

```
# vi /etc/cockpit/cockpit.conf
```

5. 在文件中添加以下文本：

```
[Session]
Banner=/etc/issue.cockpit
```

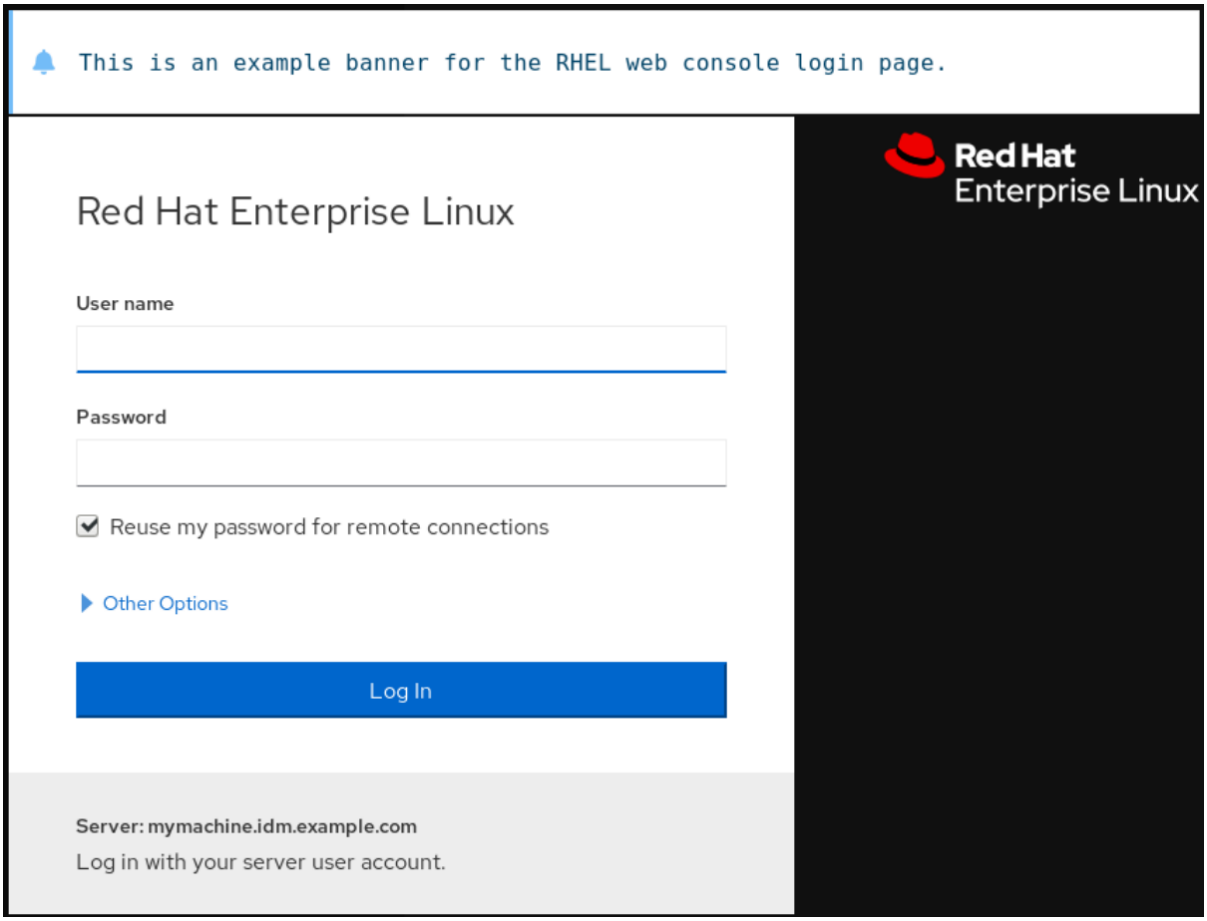
6. 保存这个文件。

7. 重启 Web 控制台以使更改生效。

```
# systemctl try-restart cockpit
```

验证步骤

- 再次打开 Web 控制台登录屏幕，以验证横幅现在是否可见：



1.14. 在 WEB 控制台中配置自动闲置锁定

您可以通过 web 控制台界面启用自动空闲锁定，并为您的系统设置空闲超时。

先决条件

- 必须安装并可以访问 Web 控制台。
  详情请参阅安装 Web 控制台。
- 您有 **root** 特权或权限来使用 **sudo** 输入管理命令的命令。

流程

1. 在您首选的文本编辑器中打开 **/etc/cockpit/** 目录中的 **cockpit.conf** 文件，例如：

   ```
   # vi /etc/cockpit/cockpit.conf
   ```

2. 在文件中添加以下文本：

   ```
   [Session]
   IdleTimeout=<X>
   ```

   将 *<X>* 替换为您选择的时间段数（以分钟为单位）。

3. 保存该文件。

4. 重启 Web 控制台以使更改生效。

```
# systemctl try-restart cockpit
```

验证步骤

- 检查在设定的时间后，用户是否会退出系统。

第 2 章 在 WEB 控制台中配置主机名

了解如何使用 Red Hat Enterprise Linux web 控制台在附加到 web 控制台的系统中配置不同类型的主机名。

2.1. 主机名

用于识别该系统的主机名。默认情况下，主机名设定为 **localhost**，您可以修改它。

主机名由两个部分组成：

主机名

它是识别系统的唯一名称。

域

当在网络中使用系统以及使用名称而非 IP 地址时，将域作为主机名后面的后缀添加。

附加域名的主机名称为完全限定域名（FQDN）。例如： **mymachine.example.com**。

主机名保存在 **/etc/hostname** 文件中。

2.2. WEB 控制台中的用户友善的主机名

您可以在 RHEL web 控制台中配置用户友善的主机名。用户友善的主机名是一个带有大写字母、空格等的主机名。

在 web 控制台中会显示用户友善的主机名，但不一定与主机名对应。

> **例 2.1. Web 控制台中的主机名格式**
>
> **用户友善主机名**
>
> **My Machine**
>
> **主机名**
>
> **mymachine**
>
> **真实主机名 - 完全限定域名（FQDN）**
>
> **mymachine.idm.company.com**

2.3. 使用 WEB 控制台设置主机名

此流程设置 web 控制台中的真实主机名或用户友善的主机名。

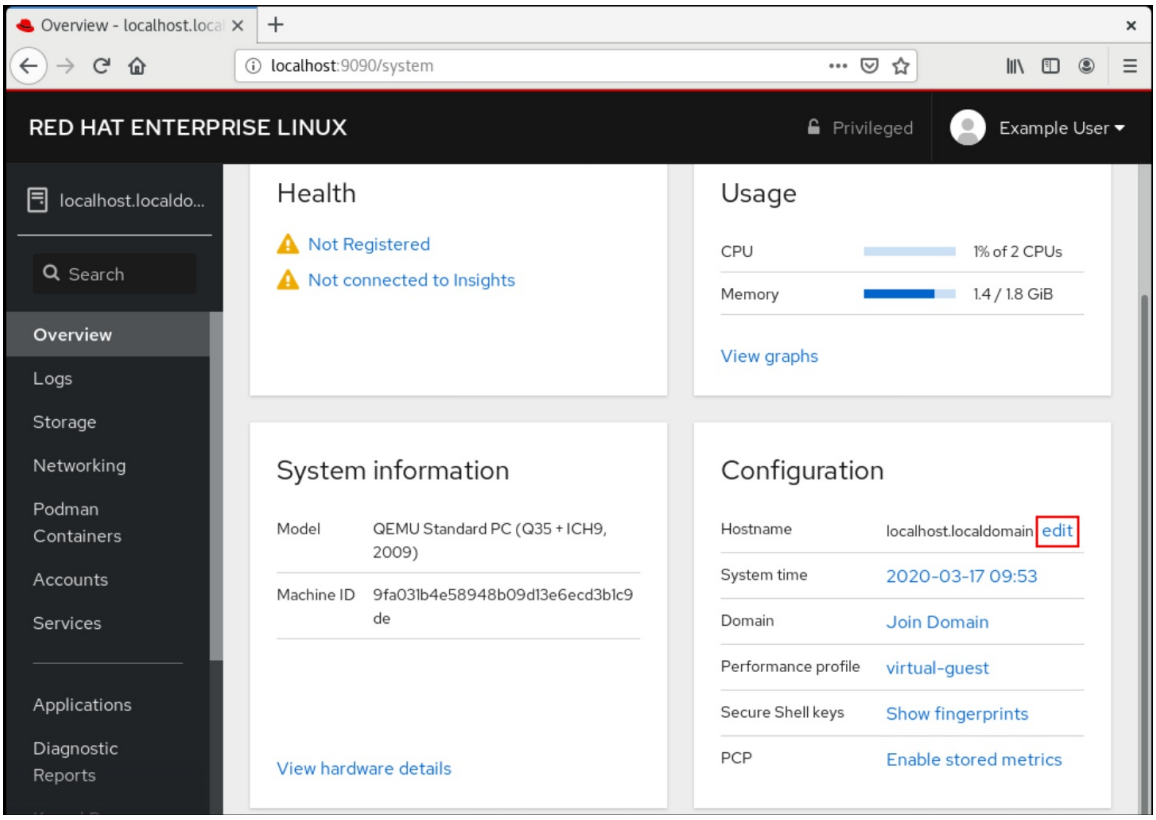
先决条件

- Web 控制台已安装并可以访问。

流程

1. 登录到 Web 控制台。
2. 点 **Overview**。

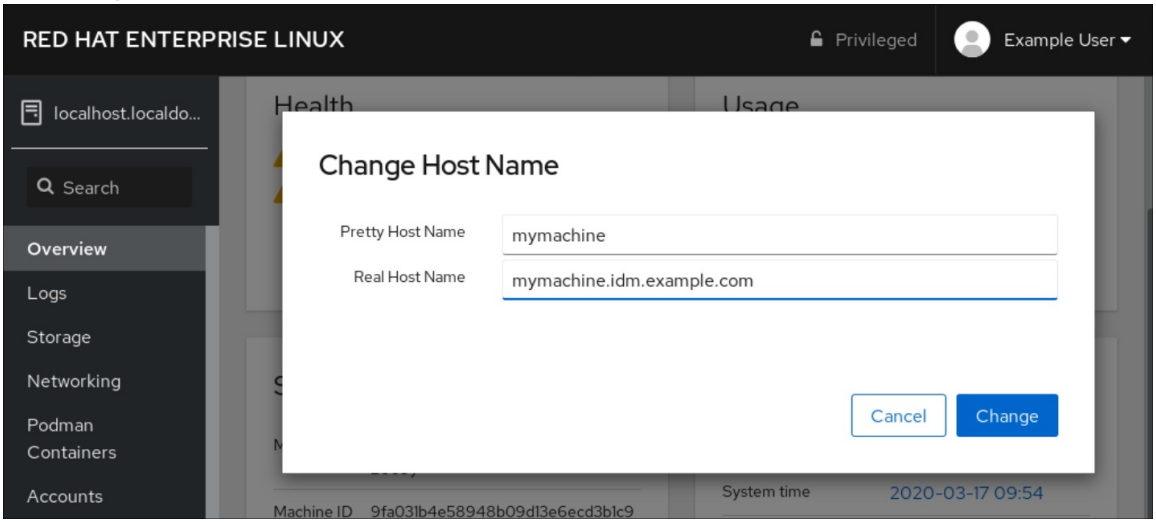
3. 点击当前主机名旁的 **编辑**。



4. 在 **更改主机名**对话框中，在 **Pretty Host Name**字段中输入主机名。

5. **Real Host Name** 字段把域名附加到用户友善名。
如果它不与用户友善主机名，可以手动更改真实主机名。

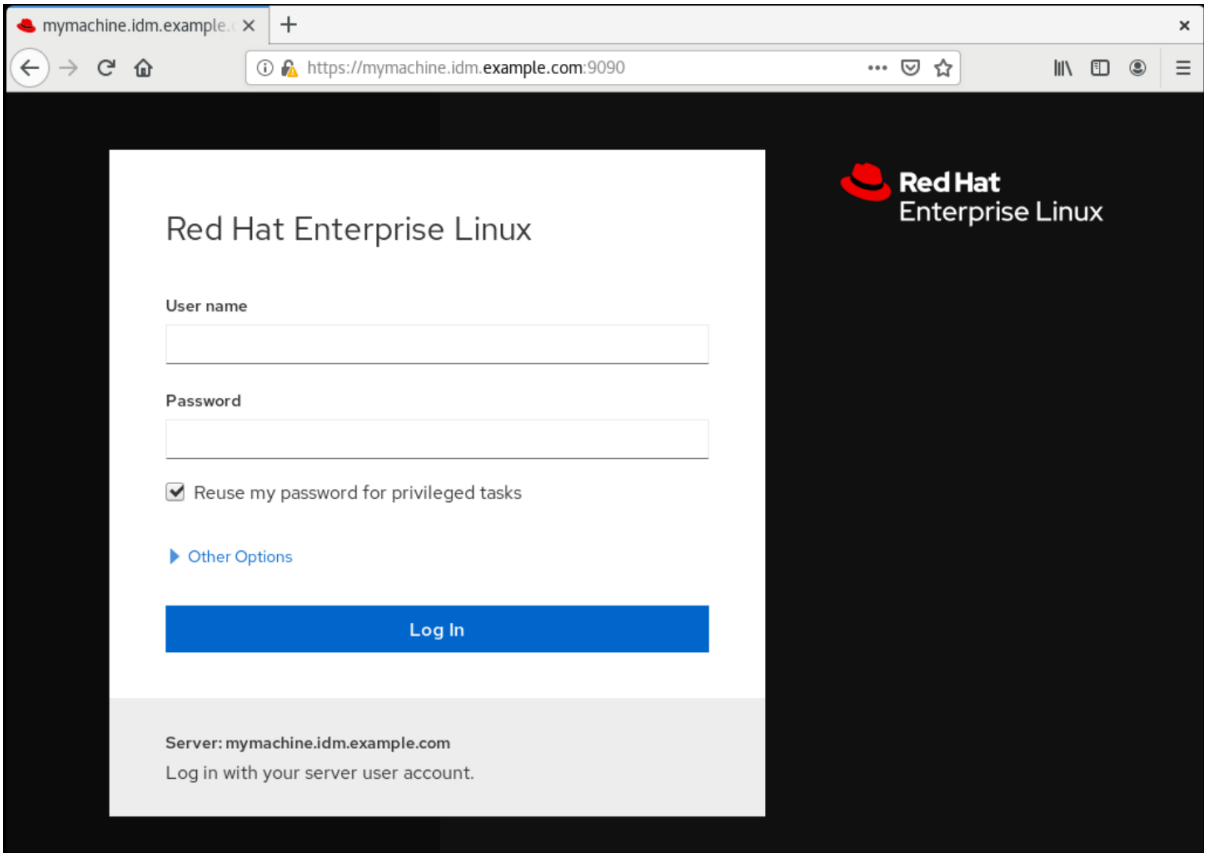
6. 点 **Change**。



验证步骤

1. 从 Web 控制台登出。

2. 通过在浏览器地址栏中输入新主机名重新打开 web 控制台。


mymachine.idm.example.
https://mymachine.idm.example.com:9090
Red Hat Enterprise Linux
Red Hat
Enterprise Linux
User name
Password
Reuse my password for privileged tasks
Other Options
Log In
Server: mymachine.idm.example.com
Log in with your server user account.

第 3 章 安装 WEB 控制台附加组件，并创建自定义页面

根据您要如何使用 Red Hat Enterprise Linux 系统，您可以向 web 控制台中添加额外的 **可用** 应用程序，或根据您的用例创建自定义页面。

3.1. RHEL WEB 控制台的附加组件

虽然 **cockpit** 软件包默认是 Red Hat Enterprise Linux 的一部分，但您可以使用以下命令根据需要安装附加应用程序：

```
# dnf install <add-on>
```

在上面的命令中，将 *<add-on>* 替换为 RHEL web 控制台的可用附加组件应用程序列表中的软件包名称。

功能名称	软件包名称	使用
Composer	**cockpit-composer**	构建自定义操作系统镜像
Machines	**cockpit-machines**	管理 **libvirt** 虚拟机
PackageKit	**cockpit-packagekit**	软件更新和应用程序安装（通常会被默认安装）
PCP	**cockpit-pcp**	具有持久性和更精细的性能数据（根据 UI 的要求安装）
Podman	**cockpit-podman**	管理容器 和 管理容器镜像
Session Recording	**cockpit-session-recording**	记录和管理用户会话
存储	**cockpit-storaged**	通过 **udisks**管理存储

3.2. 在 WEB 控制台中创建新页面

如果要向 Red Hat Enterprise Linux web 控制台中添加自定义功能，您必须为运行所需功能的页面添加包含 HTML 和 JavaScript 文件的软件包目录。

有关添加自定义页面的详细信息，请参阅 Cockpit Project 网站上的 为 Cockpit 用户界面创建插件。

其它资源

- Cockpit 项目开发人员指南 中的 Cockpit 软件包部分

第 4 章 使用 WEB 控制台优化系统性能

了解如何在 RHEL web 控制台中设置性能配置集，以便为所选任务优化系统性能。

4.1. WEB 控制台中的性能调优选项

Red Hat Enterprise Linux 9 提供几个根据以下任务优化系统的性能配置集：

- 使用桌面的系统
- 吞吐性能
- 延迟性能
- 网络性能
- 低电源消耗
- 虚拟机

TuneD 服务优化系统选项以匹配所选配置集。

在 Web 控制台中，您可以设置系统使用的哪个性能配置集。

其它资源

- TuneD 入门

4.2. 在 WEB 控制台中设置性能配置集

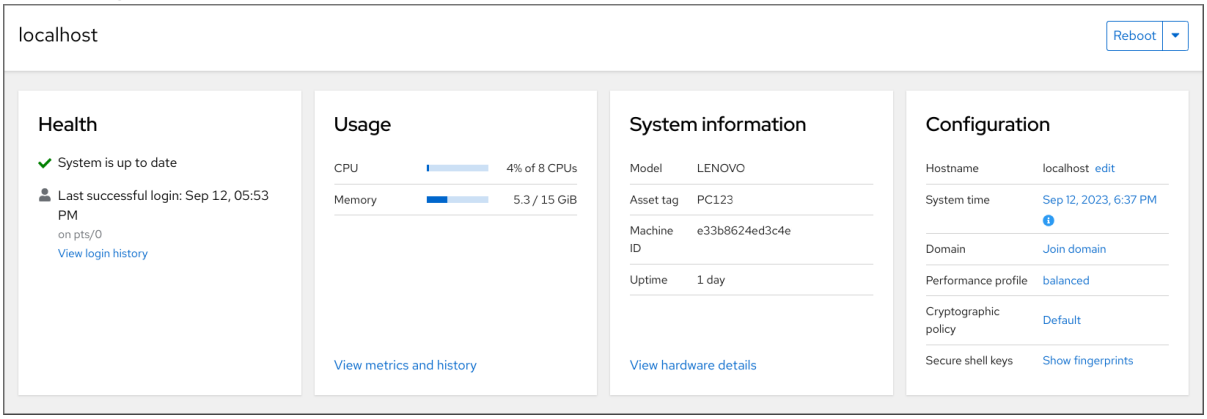
根据您要执行的任务，您可以使用 Web 控制台通过设置合适的性能配置文件来优化系统性能。

先决条件

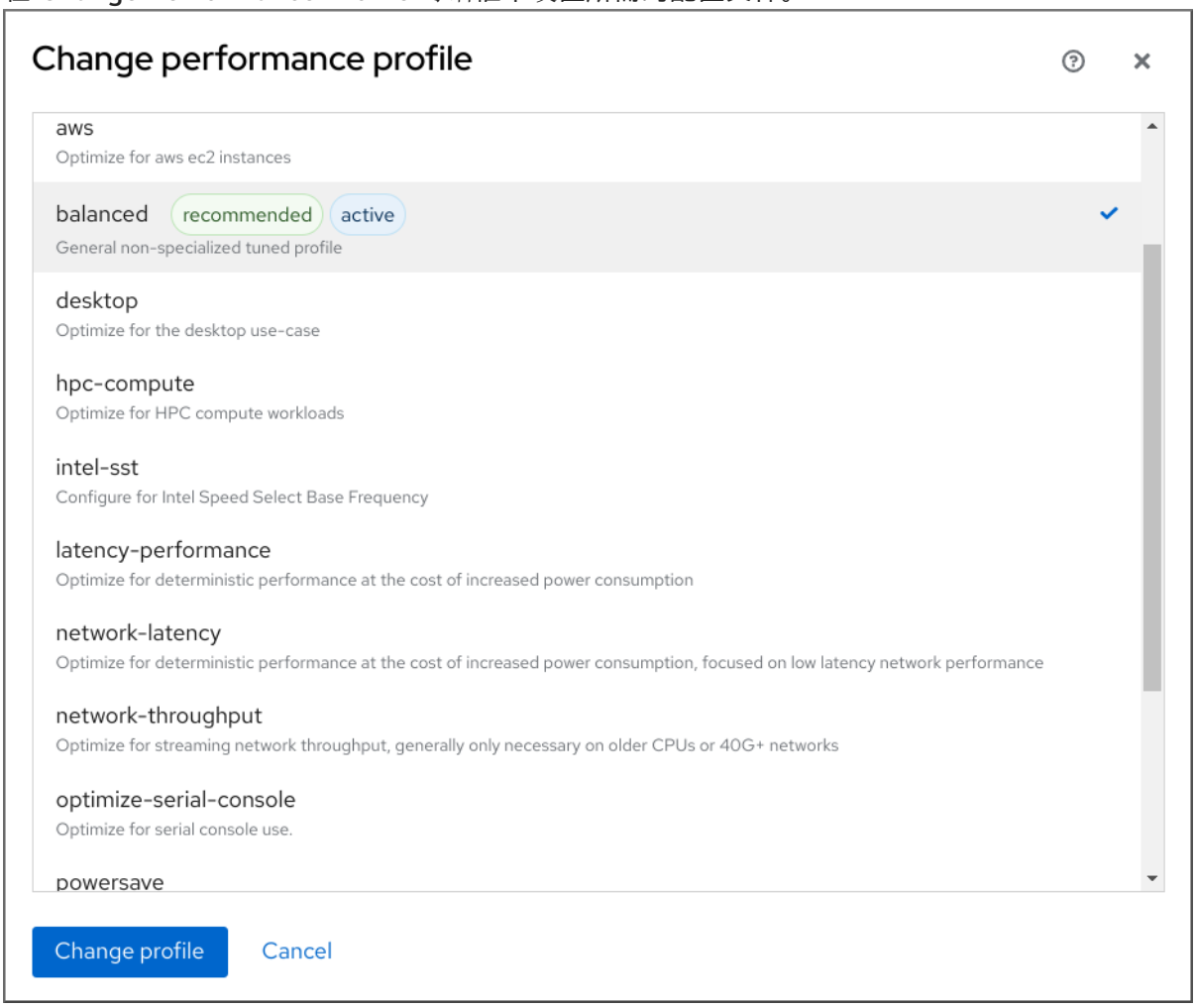
- 确保 Web 控制台已安装并可以访问。详情请参阅安装 Web 控制台。

流程

1. 登录到 web 控制台。详情请参阅 登录到 web 控制台。
2. 点 **Overview**。
3. 在 **Configuration** 部分中，点当前的性能配置文件。



4. 在 **Change Performance Profile** 对话框中设置所需的配置文件。



5. 点 **Change Profile**。

验证步骤

- **Overview** 选项卡现在在 **Configuration** 部分中显示所选的性能配置文件。

4.3. 使用 WEB 控制台监控本地系统的性能

Red Hat Enterprise Linux Web 控制台使用 Utilization Saturation and Errors (USE) 方法进行故障排除。新的性能指标页面带有最新数据，您可以对数据进行组织化的历史视图。

在 **Metrics and history** 页面中，您可以查看事件、错误以及资源利用率和饱和度的图形表示。

先决条件

- Web 控制台已安装并可以访问。详情请参阅安装 Web 控制台。
- **cockpit-pcp** 软件包（启用收集性能指标）已安装：
  a. 从 Web 控制台界面安装软件包：
    i. 使用管理权限登录到 web 控制台。详情请参阅 登录到 web 控制台。
    ii. 在 **Overview** 页面中，单击 **View metrics and history**。
    iii. 点 **Install cockpit-pcp** 按钮。

iv. 在**安装软件**对话框窗口中，点**安装**。

b. 要从命令行界面安装软件包，请使用：

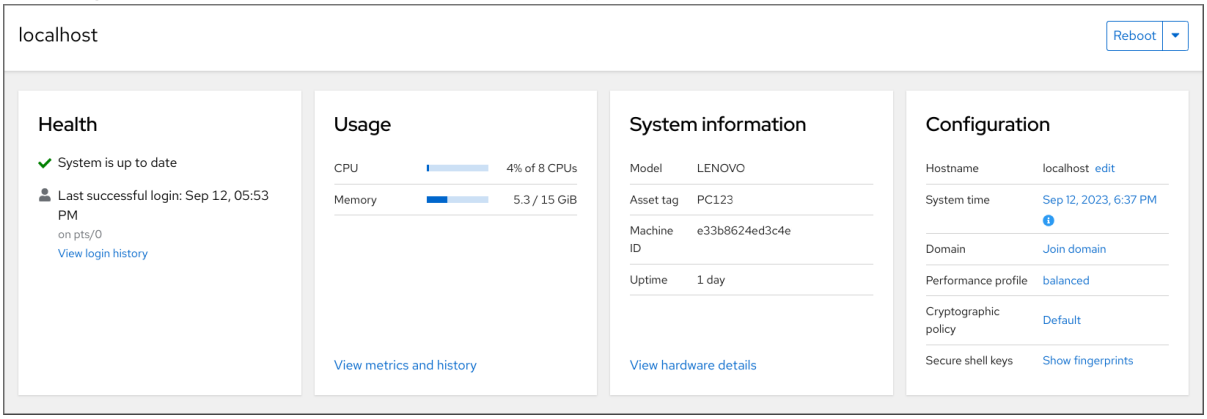
```
# dnf install cockpit-pcp
```

- 启用 Performance Co-Pilot (PCP)服务：

```
# systemctl enable --now pmlogger.service pmproxy.service
```

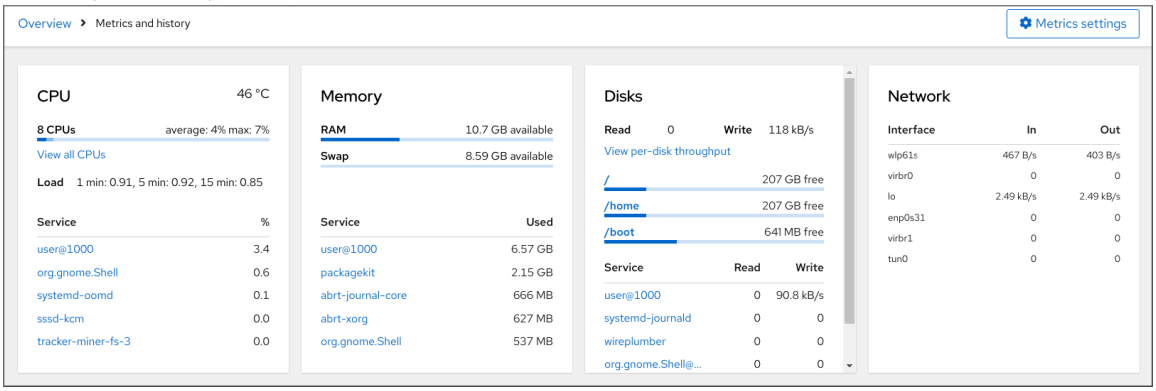
流程

1. 登录到 web 控制台。详情请参阅 登录到 web 控制台。
2. 点 **Overview**。
3. 在 **Usage** 部分中，点 **View metrics and history**。

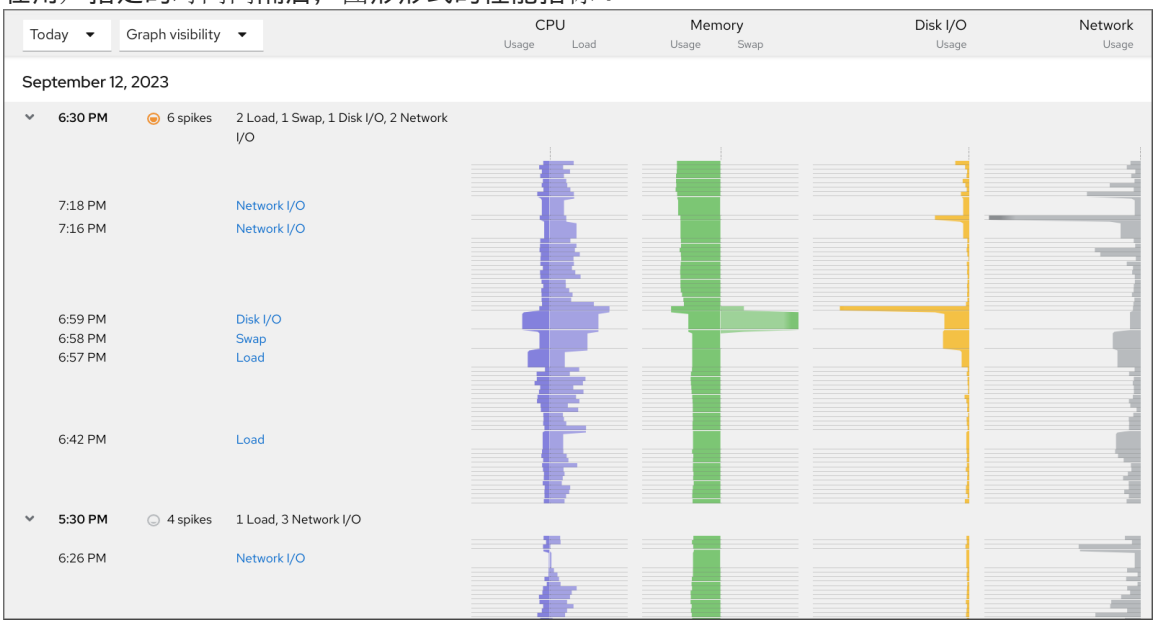


MMetrics and history 部分打开：

- 当前系统配置和使用情况：



- 在用户指定的时间间隔后，图形形式的性能指标：



4.4. 使用 WEB 控制台和 GRAFANA 监控多个系统的性能

Grafana 允许您一次从多个系统收集数据，并查看其收集的 Performance Co-Pilot (PCP)指标的图形表示。您可以在 web 控制台界面中的多个系统设置性能指标监控和导出。

先决条件

- 必须安装并可以访问 Web 控制台。详情请参阅链接：安装 Web 控制台。
- 安装 **cockpit-pcp** 软件包。
  1. 在 Web 控制台界面中：
     a. 使用管理权限登录到 web 控制台。详情请参阅 登录到 web 控制台。
     b. 在 **Overview** 页面中，点 **View details 和 history**。
     c. 点 **Install cockpit-pcp** 按钮。
     d. 在**安装软件**对话框窗口中，点**安装**。
     e. 注销并再次登录以查看指标历史记录。
  2. 要从命令行界面安装软件包，请使用：

```
# dnf install cockpit-pcp
```

- 启用 PCP 服务：

```
# systemctl enable --now pmlogger.service pmproxy.service
```

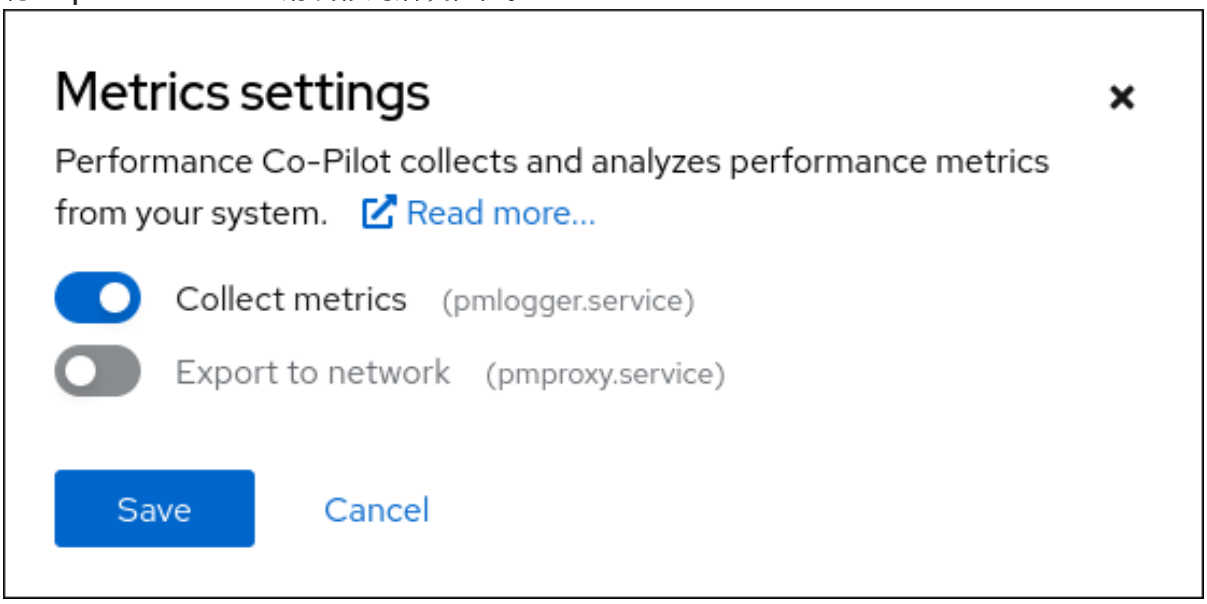
- 设置 Grafana 仪表板。如需更多信息，请参阅设置 grafana-server。
- 安装 **redis** 软件包。

```
# dnf install redis
```

另外，您可以稍后从 Web 控制台界面安装软件包。

流程

1. 在 **Overview** 页面中，点 **Usage** 表中的 **View metrics and history**。
2. 点 **Metrics 设置** 按钮。
3. 将 **Export to network** 滑块移到活跃位置。



如果您没有安装 **redis** 软件包，Web 控制台会提示您安装它。

4. 要打开 **pmproxy** 服务，请从下拉列表中选择一个区域，然后点 **Add pmproxy** 按钮。
5. 点 **Save**。

验证

1. 点 **Networking**。
2. 在 **Firewall** 表中，点 **Edit rules and zones** 按钮。
3. 在您选择的区域中搜索 **pmproxy**。

重要

在您要监视的所有系统中重复此步骤。

其它资源

- 设置 PCP 指标的图形表示

第 5 章 查看 WEB 控制台中的日志

了解如何在 RHEL web 控制台中访问、查看和过滤日志。

5.1. 查看 WEB 控制台中的日志

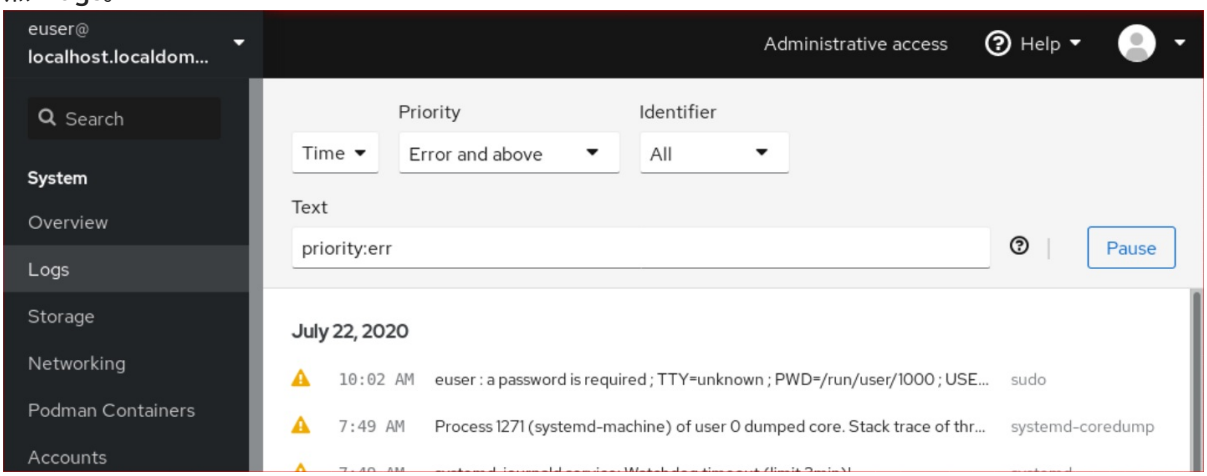
RHEL 9 web 控制台日志部分是 **journalctl** 实用程序的 UI。您可以在 web 控制台界面中访问系统日志。

先决条件

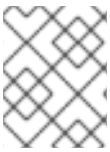
- 已安装 RHEL 9 web 控制台。
  详情请参阅安装 Web 控制台。

流程

1. 登录到 RHEL web 控制台。
   详情请参阅 登录到 web 控制台。
2. 点 **Logs**。



3. 点击列表中的选定日志条目条目，打开日志条目详情。



注意

您可以使用 **暂停** 按钮在显示时暂停新日志条目。恢复新日志条目后，Web 控制台将加载您使用 **Pause** 按钮后报告的所有日志条目。

您可以根据时间、优先级或标识符过滤日志。如需更多信息，请参阅 web 控制台中的过滤日志

5.2. 在 WEB 控制台中过滤日志

您可以在 web 控制台中过滤日志条目。

先决条件

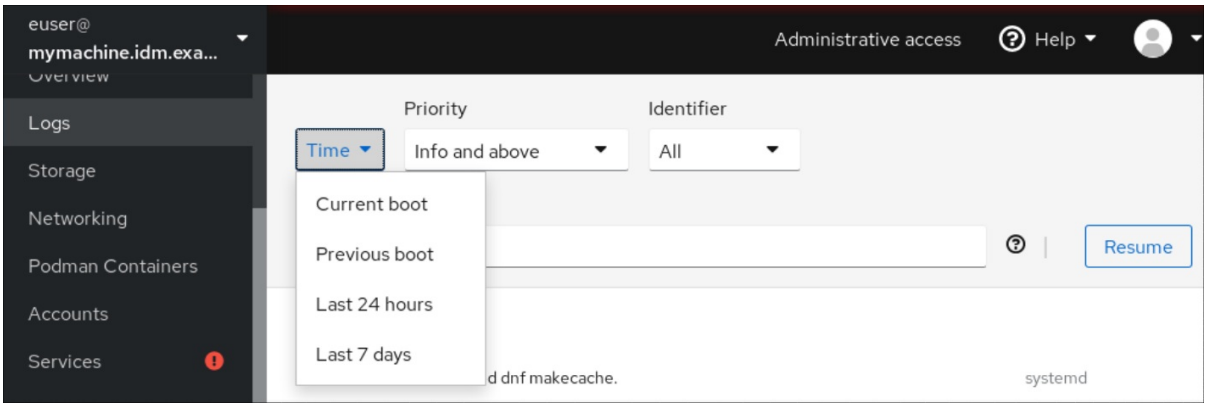
- 必须安装并可以访问 Web 控制台界面。
  详情请参阅安装 Web 控制台。

流程

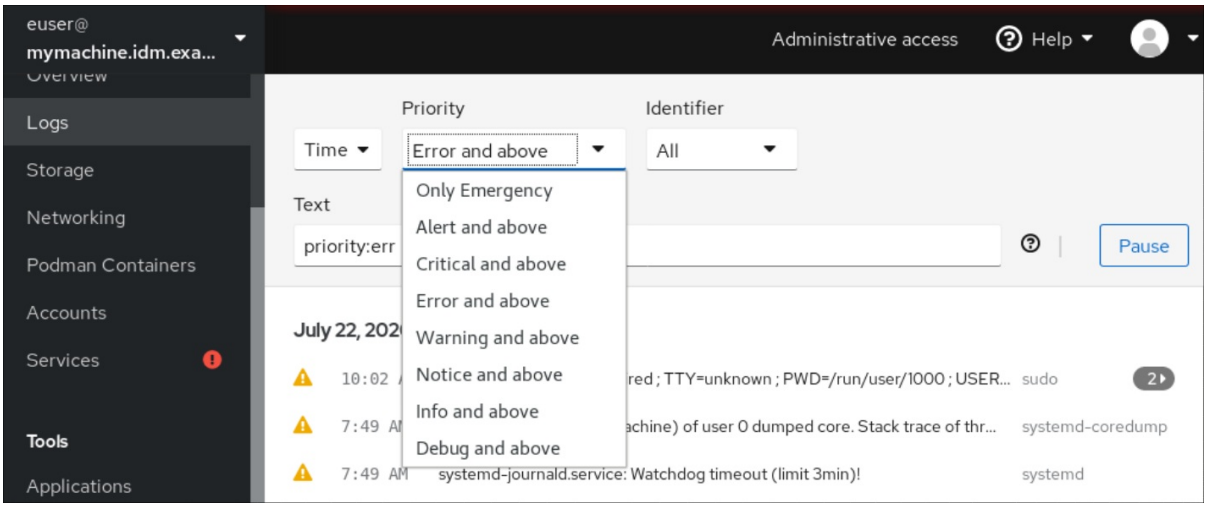
1. 登录到 RHEL 9 web 控制台。
   详情请参阅 登录到 web 控制台。

2. 点 **Logs**。

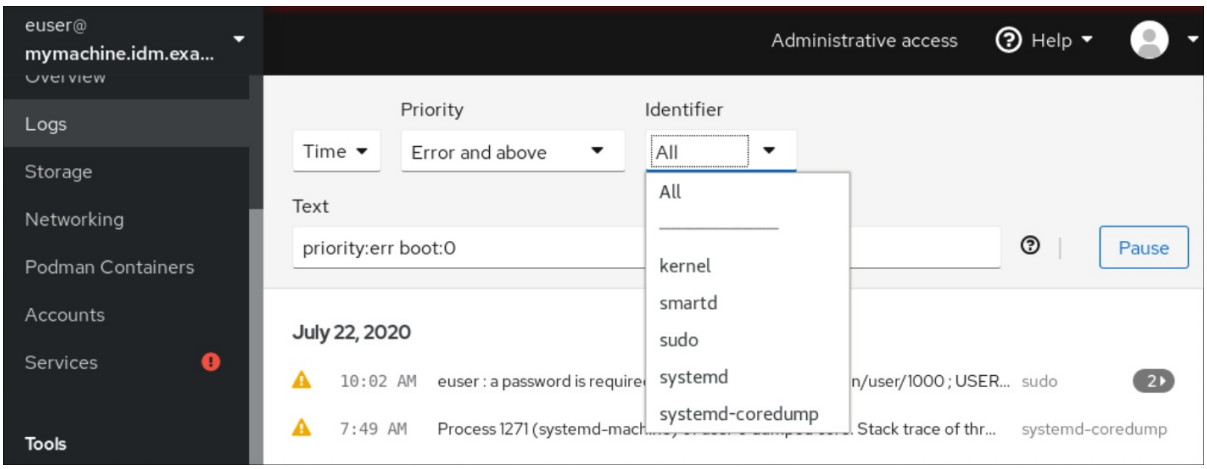
3. 默认情况下，Web 控制台显示最新的日志条目。要根据具体时间范围过滤，请点 **Time** 下拉菜单并选择一个首选的选项。



4. 默认情况下会显示 **Error 及更高级别**的日志列表。要根据不同的优先级过滤，请点击 **Error 及更高**下拉菜单并选择一个首选的优先级。



5. 默认情况下，Web 控制台会显示所有标识符的日志。要过滤特定标识符的日志，请点 **All** 下拉菜单并选择标识符。



6. 要打开日志条目，请点所选日志。

5.3. 在 WEB 控制台中过滤日志的文本搜索选项

文本搜索选项功能为过滤日志提供了大量选项。如果您决定使用文本搜索过滤日志，您可以使用三个下拉菜单中定义的预定义选项，或者您可以自己键入整个搜索。

下拉菜单

您可以使用三个下拉菜单来指定搜索的主参数：

- **Time**:此下拉菜单包含搜索的不同时间范围的预定义搜索。
- **Priority**:此下拉菜单提供了不同优先级级别的选项。它对应于 **journalctl --priority** 选项。默认优先级值为 **Error 及以上**。每次在不指定其它优先级时，会设置它。
- **Identifier**:在这个下拉菜单中，您可以选择要过滤的标识符。对应于 **journalctl --identifier** 选项。

限定符

您可以使用六个限定符来指定搜索。它们包含在用于过滤日志表的 Options 中。

日志字段

如果要搜索特定日志字段，可以用其内容指定字段。

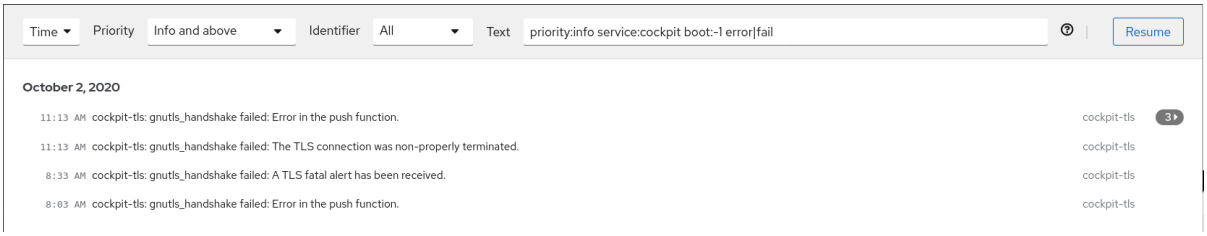
在日志信息中进行自由文本搜索

您可以在日志消息中过滤您选择的任何文本字符串。字符串也可以采用正则表达式的形式。

高级日志过滤 I

过滤 2020 年 10 月 22 日之后带有 'systemd' 识别的、日志字段 'JOB_TYPE' 是 'start' 或 'restart 的所有日志信息。

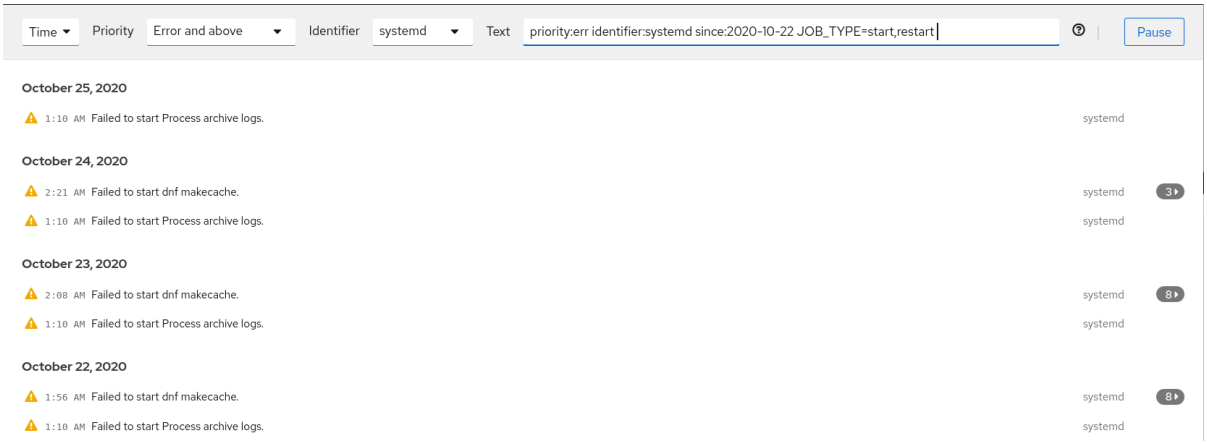
1. 在搜索字段中输入 **identifier:systemd since:2020-10-22 JOB_TYPE=start,restart**。
2. 检查结果。



高级日志过滤 II

过滤上一次启动前出现的所有来自"cockpit.service' systemd 单元且邮件正文包含"error"或"fail"的所有日志消息。

1. 在搜索字段中输入 **service:cockpit boot:-1 error|fail**。
2. 检查结果。



5.4. 使用文本搜索框过滤 WEB 控制台中的日志

通过使用文本搜索框，您可以根据不同的参数过滤日志。搜索合并了过滤下拉菜单、限定符、日志字段和自由格式字符串搜索的使用。

先决条件

- 必须安装并可以访问 Web 控制台界面。
  详情请参阅安装 Web 控制台。

流程

1. 登录到 RHEL web 控制台。
   详情请参阅 登录到 web 控制台。
2. 点 **Logs**。
3. 使用下拉菜单指定您想要过滤的三个主要的限定符 - 时间范围、优先级和标识符。
   优先级（Priority） 限定符总需要有一个值。如果没有指定，它会自动过滤 **Error 及以上** 优先级。请注意，您设置的选项反映了在文本搜索框中。
4. 指定您要过滤的 log 字段。
   可以添加几个日志字段。
5. 您可以使用自由格式的字符串搜索任何其他内容。搜索框也接受正则表达式。

5.5. 日志过滤选项

有几个 **journalctl** 选项可用于在 web 控制台中过滤日志，这或许非常有用。其中一些已作为 web 控制台界面的下拉菜单的一部分进行介绍。

表 5.1. 表

选项名称	使用	备注

选项名称	使用	备注
priority	按消息优先级过滤输出。取单个数字或文本日志级别。日志级别是常见的 syslog 日志级别。如果指定了单一日志级别，则会显示具有此日志级别的所有消息或低（更重要）日志级别。	包括在**优先级**下拉菜单中。
identifier	显示被 syslog 标识为 SYSLOG_IDENTIFIER 的信息。可多次指定。	包括在 **标识符** 下拉菜单中。
follow	仅显示最新的日志条目，并在新条目附加到日志中时持续打印新条目。	没有包含在下拉菜单中。
service	显示指定 **systemd** 单元的消息。可多次指定。	没有包含在下拉菜单中。对应于 **journalctl --unit** 参数。
boot	显示来自特定启动的消息。 正整数代表从日志开始查找启动，等于或小于零的整数代表将从日志末尾查找启动。因此, 1 表示日志中的第一个引导（按时间顺序排列）， 2 为第 2 个，以此类推 ; -0 是最后一次引导，-1 是最后一次引导的前一个，以此类推。	在**时间**下拉菜单中作为 **Current boot** 或 **Previous boot**。其他选项需要手动编写。
since	开始显示指定日期更新或分别位于指定日期或比指定日期旧的条目。日期规格应为 "2012-10-30 18:17:16"。如果省略了时间部分，使用 "00:00:00"。如果只省略了秒的组件，使用 ":00"。如果省略了日期的部分，使用当前日期。另外，还可以使用 "yesterday"、"today"、"tomorrow"（分别代表前一天、当天和明天的 00:00:00），以及 "now"（代表当前时间）。最后，可以指定相对时间，前缀为 "-" 或 "+"，分别引用当前时间前或之后的时间。	没有包含在下拉菜单中。

第 6 章 在 WEB 控制台中管理用户帐户

RHEL web 控制台提供了一个添加、编辑和删除系统用户帐户的界面。

在阅读这个部分后，您将了解：

- 现有帐户来自哪里。
- 如何添加新帐户。
- 如何设置密码过期。
- 如何和何时终止用户会话。

先决条件

- 使用分配了管理员权限的帐户登录到 RHEL web 控制台。详情请参阅 Web 控制台的日志记录

6.1. WEB 控制台中管理的系统用户帐户

您可在 RHEL web 控制台中显示用户帐户：

- 在访问系统时验证用户。
- 设置系统的访问权限。

RHEL web 控制台显示系统中的所有用户帐户。因此，在首次登录 web 控制台后，至少可以看到一个可用的用户帐户。

登录到 RHEL web 控制台后，您可以执行以下操作：

- 创建新用户帐户。
- 更改其参数。
- 锁定帐户。
- 终止用户会话。

6.2. 使用 WEB 控制台添加新帐户

您可以将用户帐户添加到系统，并通过 RHEL web 控制台向帐户设置管理权限。

先决条件

- 必须安装并可以访问 RHEL web 控制台。详情请参阅安装 Web 控制台。

流程

1. 登录到 RHEL web 控制台。
2. 点 **Account**。
3. 点 **Create New Account**。

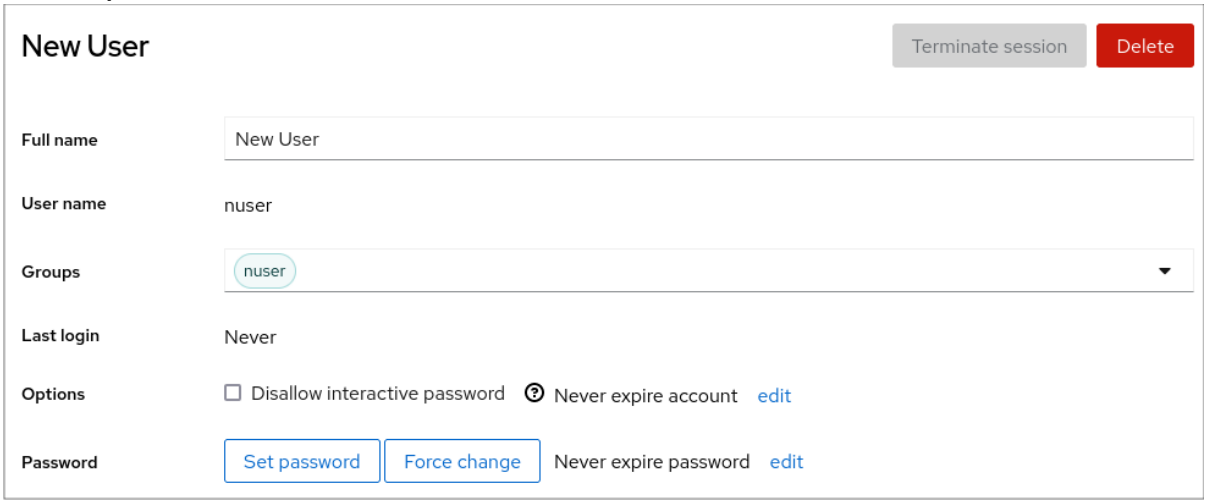
4. 在 **Full Name** 字段中输入用户全名。
   RHEL web 控制台会自动在全名中推荐用户名并在 **User Name** 字段中填充该用户名。如果您不想使用原始命名规则（由名的第一个字母和完整的姓组成），对它进行更新。

5. 在 **Password/Confirm** 字段中输入密码并重新输入该密码以便验证您的密码是否正确。
   下面的颜色栏显示您输入密码的安全等级，这不允许您创建带弱密码的用户。

6. 点 **Create** 保存设置并关闭对话框。

7. 选择新创建的帐户。

8. 在 **Groups** 下拉菜单中选择您要添加到新帐户的组。



现在您可以在 **Accounts** 设置中看到新帐户，您可以使用凭证连接到该系统。

6.3. 在 WEB 控制台中强制密码过期

默认情况下，用户帐户将密码设定为永远不会过期。您可以设置系统密码在指定的天数后过期。当密码过期时，下次登录尝试会提示密码更改。

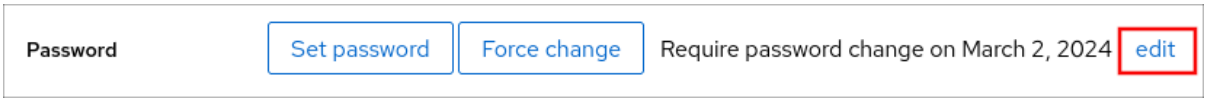
流程

1. 登录到 RHEL 9 web 控制台。

2. 点 **Account**。

3. 选择您要强制密码过期的用户帐户。

4. 点 **Password** 行上的 **edit**。



5. 在 **Password expiration** 对话框中，选择 **Require password change every ... days**并输入一个正数，代表密码过期的天数。

6. 点 **Change**。
   Web 控制台会立即在 **Password** 行上显示将来的密码更改请求的日期。

6.4. 在 WEB 控制台中终止用户会话

用户在登录系统时创建用户会话。终止用户会话意味着从系统中注销用户。如果您需要执行对配置更改敏感的管理任务，比如升级系统，这非常有用。

在 RHEL 9 web 控制台中的每个用户帐户中，您可以终止该帐户的所有会话，但您当前使用的 web 控制台会话除外。这可防止您丢失对您的系统的访问。

流程

1. 登录到 RHEL 9 web 控制台。
2. 点 **Account**。
3. 点击要终止会话的用户帐户。
4. 点 **Terminate Session**。
   如果 **Terminate Session** 按钮不可用，这个用户就不能登录到系统。

   RHEL web 控制台会终止会话。

第 7 章 在 WEB 控制台中管理服务

了解如何在 RHEL web 控制台界面中管理系统服务。您可以激活或停用服务、重新启动或重新加载服务，或者管理它们的自动启动。

7.1. 在 WEB 控制台中激活或取消激活系统服务

此流程使用 Web 控制台界面激活或取消激活系统服务。

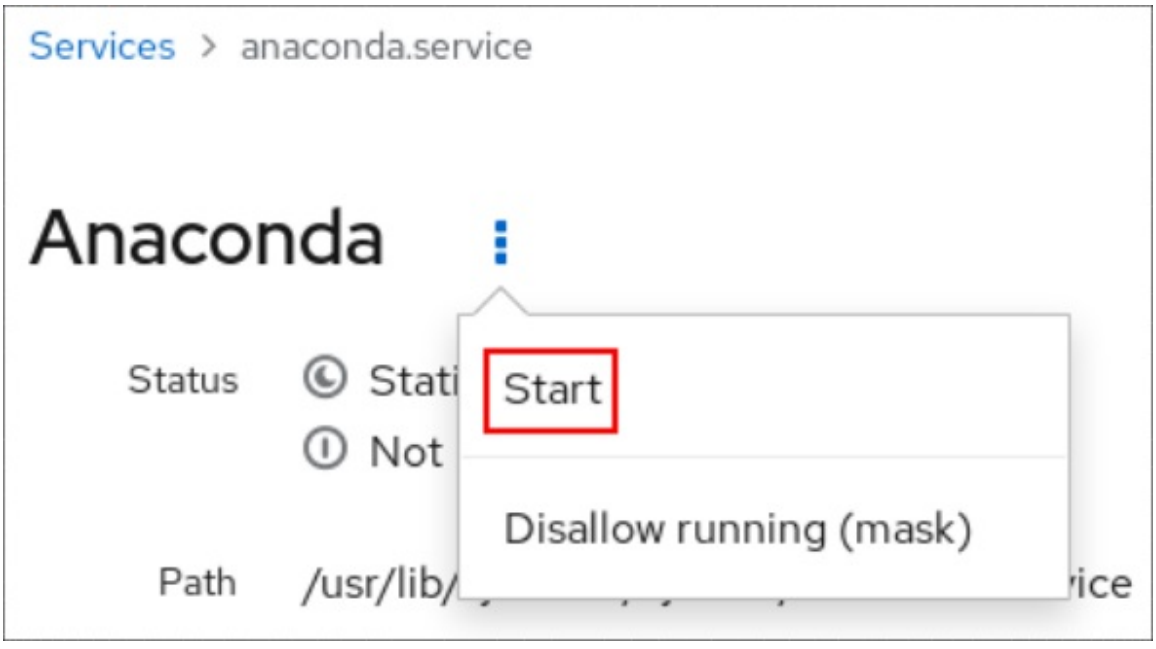
先决条件

- 已安装 RHEL 9 web 控制台。
  详情请参阅安装 Web 控制台。

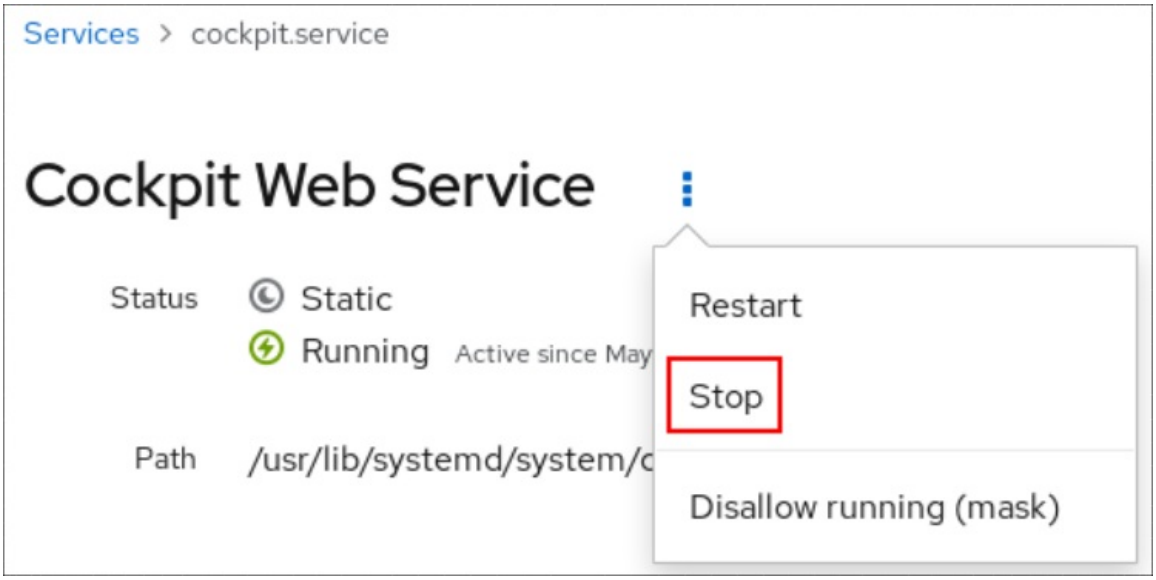
流程

您可以根据名称或描述过滤服务，也可以通过 Enabled、Disabled 或 Static 自动启动过滤服务。接口显示服务的当前状态及其最近日志。

1. 使用管理员权限登录到 RHEL web 控制台。
   详情请参阅 登录到 web 控制台。
2. 点左侧的 web 控制台菜单中的 **Services**。
3. **服**务的默认标签页是 **System Services**。如果要管理目标、套接字、计时器或路径，请切换到顶部菜单中的相应选项卡。
4. 要打开服务设置，请点击列表中的所选服务。您可以选择 **State** 列来告诉哪些服务处于活跃状态或不活跃。
5. 激活或取消激活服务：
   - 要激活不活跃的服务，点**开始**按钮。



   - 要取消激活一个活跃的服务，点**停止**按钮。



7.2. 在 WEB 控制台中重启系统服务

此流程使用 Web 控制台界面重启系统服务。

先决条件

- 已安装 RHEL 9 web 控制台。
  详情请参阅安装 Web 控制台。

流程

您可以根据名称或描述过滤服务，也可以通过 Enabled、Disabled 或 Static 自动启动过滤服务。接口显示服务的当前状态及其最近日志。

1. 使用管理员权限登录到 RHEL web 控制台。
   详情请参阅 登录到 web 控制台。
2. 点左侧的 web 控制台菜单中的 **Services**。
3. **服务的默认标签页是 System Services。如果要管理目标、套接字、计时器或路径，请切换到顶部菜单中的相应选项卡。**
4. 要打开服务设置，请点击列表中的所选服务。
5. 要重启某个服务，点**重启**按钮。

7.3. 在 WEB 控制台中覆盖清单设置

您可以为系统的特定用户和所有用户修改 Web 控制台的菜单。在 **cockpit** 项目中，软件包名称是一个目录名称。软件包包含 **manifest.json** 文件以及其他文件。默认设置存在于 **manifest.json** 文件中。您可以通过在特定位置为指定的用户创建一个 ***<package-name>*.override.json** 文件来覆盖默认的 **cockpit** 菜单设置。

先决条件

- 已安装 RHEL 9 web 控制台。
  详情请参阅安装 Web 控制台。

流程

1. 在您选择的文本编辑器中覆盖**<*systemd*>.override.json** 文件中的清单设置，例如：
   a. 要为所有用户编辑，请输入：

```
# vi /etc/cockpit/<systemd>.override.json
```

   b. 要为单个用户编辑，请输入：

```
# vi ~/.config/cockpit/<systemd>.override.json
```

2. 使用以下详情编辑所需的文件：

```
{
  "menu": {
  "services": null,
  "logs": {
      "order": -1
  }
 }
}
```

   - **null** 值隐藏了 **services** 选项卡
   - **-1** 值将 **logs** 选项卡移到第一个位置。

3. 重启 **cockpit** 服务：

```
# systemctl restart cockpit.service
```

其它资源

- **cockpit (1)** 手册页
- 清单覆盖

第 8 章 使用 WEB 控制台配置网络绑定

了解网络绑定的工作原理并在 RHEL 9 web 控制台中配置网络绑定。

注意

RHEL 9 web 控制台使用 NetworkManager 服务进行网络相关的操作。

先决条件

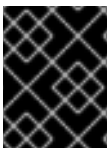
- 已安装并启用 RHEL 9 web 控制台。详情请参阅安装 Web 控制台。

8.1. 上游交换机配置依赖绑定模式

根据您要使用的绑定模式，您必须在交换机上配置端口：

绑定模式	交换机上的配置
0 - balance-rr	需要启用静态 EtherChannel，而不是链路聚合控制协议(LACP)协商。
1 - active-backup	交换机上不需要配置。
2 - balance-xor	需要启用静态 EtherChannel，而不是 LACP 协商。
3 - broadcast	需要启用静态 EtherChannel，而不是 LACP 协商。
4 - 802.3ad	需要启用 LACP 协商的 EtherChannel。
5 - balance-tlb	交换机上不需要配置。
6 - balance-alb	交换机上不需要配置。

有关如何配置交换机的详情，请查看交换机的文档。



重要

某些网络绑定的功能，比如故障切换机制，不支持不通过网络交换机的直接电缆连接。详情请查看是否支持直接连接的绑定？KCS 解决方案。

8.2. 绑定模式

RHEL 9 中有几个模式选项。每个模式选项都用特定的负载平衡和容错来定性。绑定接口的行为取决于模式。绑定模式提供容错、负载平衡或两者。

负载均衡模式

- **Round Robin**:按顺序传输从第一个可用接口到最后一个接口的数据包。

容错模式

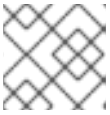
- **Active Backup**:只有主接口失败时，其中一个备份接口会替换它。只有活动接口使用的 MAC 地址是可见的。
- **Broadcast**:所有传输都将在所有接口上发送。

注意

广播可显著增加所有绑定接口上的网络流量。

容错和负载均衡模式

- **XOR**:目标 MAC 地址在具有 modulo 哈希的接口之间平均分配。然后，每个接口都提供相同的 MAC 地址组。
- **802.3ad**:设置 IEEE 802.3ad 动态链路聚合策略。创建共享相同速度和双工设置的聚合组。在活跃聚合器中的所有接口上传输并接收接收。



注意

此模式需要兼容 802.3ad 的交换机。

- **自适应传输负载平衡** ：传出流量会根据每个接口上的当前负载进行分发。传入流量由当前接口接收。如果接收接口失败，另一个接口会接管失败的 MAC 地址。
- **自适应负载平衡** ：包括 IPv4 流量的传输和接收负载平衡。
  接收负载平衡是通过地址解析协议(ARP)协商来实现的，因此需要在绑定配置中将 **Link Monitoring** 设置为 **ARP**。

8.3. 使用 RHEL WEB 控制台配置网络绑定

如果您希望使用基于 Web 浏览器的界面管理网络设置，请使用 RHEL web 控制台配置网络绑定。

先决条件

- 已登陆到 RHEL web 控制台。
- 在服务器中安装两个或者两个以上物理或者虚拟网络设备。
- 要将以太网设备用作绑定的成员，必须在服务器中安装物理或者虚拟以太网设备。
- 要将 team、bridge 或 VLAN 设备用作绑定成员，请预先创建它们，如：
  - 使用 RHEL web 控制台配置网络团队
  - 使用 RHEL web 控制台配置网桥
  - 使用 RHEL web 控制台配置 VLAN 标记

流程

1. 在屏幕左侧的导航中选择 **Networking** 选项卡。
2. 在 **Interfaces** 部分点 **Add bond**。

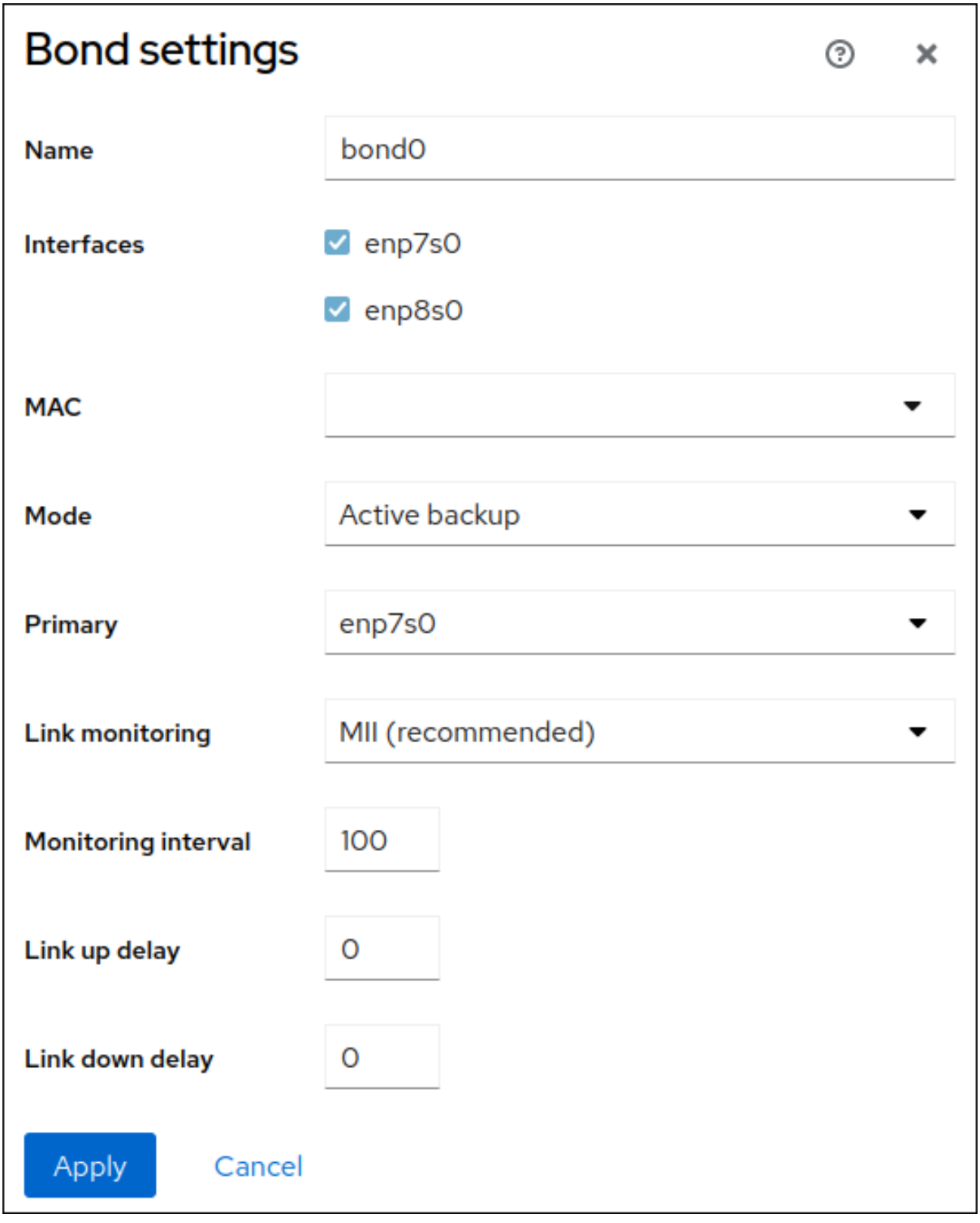
3. 输入您要创建的绑定设备名称。

4. 选择应该是绑定成员的接口。

5. 选择绑定模式。
   如果您选择 **Active backup**，Web 控制台会显示额外的 **Primary** 字段，您可以在其中选择首选的活动设备。

6. 设置链路监控模式。例如，当您使用 **Adaptive 负载均衡** 模式时，将它设置为 **ARP**。

7. 可选：调整监控间隔、连接延迟和链路延迟设置。通常，您只需要更改默认值以进行故障排除。



8. 点**应用**。

9. 默认情况下，绑定使用动态 IP 地址。如果要设置静态 IP 地址：

a. 在 **Interfaces** 部分点绑定的名称。

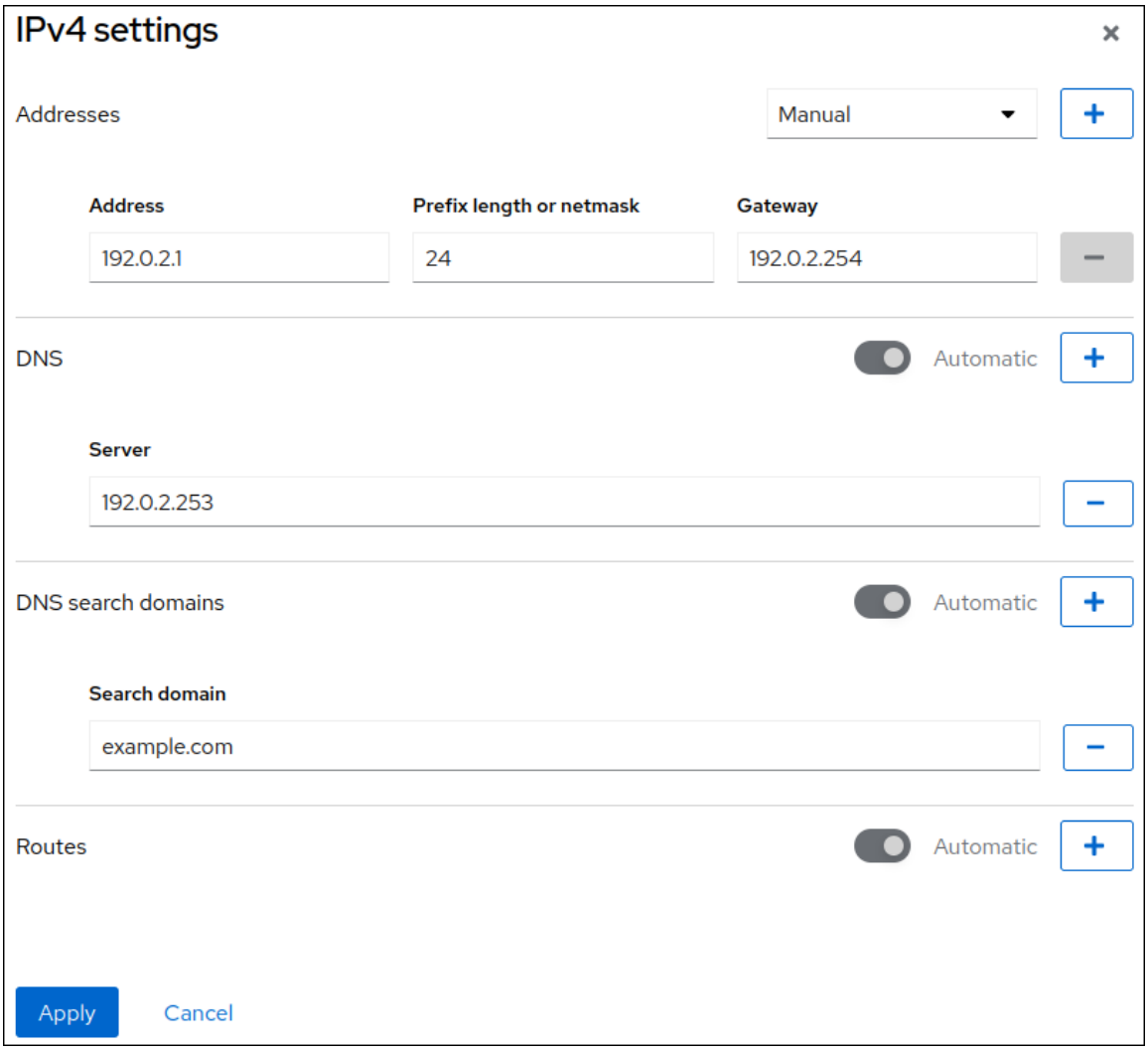
b. 点您要配置的协议旁的 **Edit**。

c. 选择 **Addresses** 旁的 **Manual**，并输入 IP 地址、前缀和默认网关。

d. 在 **DNS** 部分，点 **+** 按钮，并输入 DNS 服务器的 IP 地址。重复此步骤来设置多个 DNS 服务器。

e. 在 **DNS search domains** 部分中，点 **+** 按钮并输入搜索域。

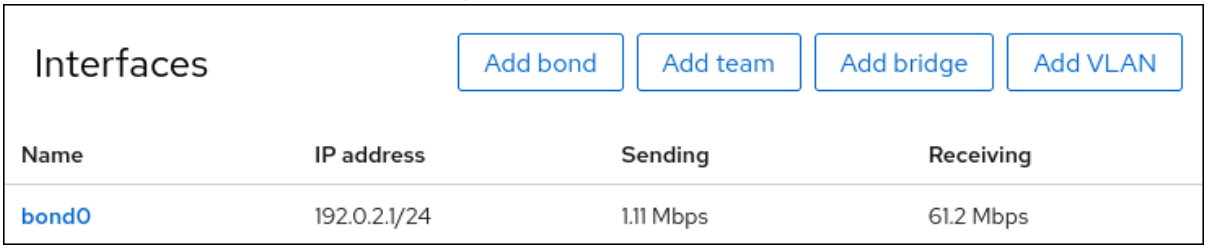
f. 如果接口需要静态路由，请在 **Routes** 部分配置它们。



g. 点 **应用**

验证

1. 在屏幕左侧的导航中选择 **Networking** 选项卡，并检查接口上是否有传入和传出流量：



2. 从其中一个网络设备中临时删除网络电缆，并检查绑定中是否有其他设备处理流量。

请注意，无法使用软件工具正确测试链路失败事件。取消激活连接的工具（如 Web 控制台）只显示处理成员配置更改且没有实际链路失败事件的能力。

3. 显示绑定状态：

```
# cat /proc/net/bonding/bond0
```

8.4. 使用 WEB 控制台向绑定添加接口

网络绑定可以包含多个接口，您可以随时添加或删除任何接口。

了解如何在现有绑定中添加网络接口。

先决条件

- 使用配置了多个接口的绑定，如使用 Web 控制台配置网络绑定所述

流程

1. 登录到 web 控制台。
   详情请参阅 登录到 web 控制台。
2. 打开 **网络**。
3. 在 **接口** 表中，点您要配置的绑定。
4. 在绑定设置屏幕中，滚动到成员表（接口）。
5. 点 **Add member** 下拉菜单图标。
6. 从下拉菜单中选择接口，并点击它。

验证步骤

- 检查所选接口是否出现在绑定设置屏幕中的**接口成员**表中。

8.5. 使用 WEB 控制台从绑定中删除或禁用接口

网络绑定可以包含多个接口。如果您需要更改设备，您可以从绑定中删除或者禁用特定接口，这样可处理剩余的活跃接口。

要使用绑定中包含的接口停止，您可以：

- 从绑定中删除接口。
- 暂时禁用接口。这个接口会保持绑定的一部分，但绑定不会使用它，除非您再次启用它。

先决条件

- 使用配置了多个接口的绑定，如使用 Web 控制台配置网络绑定所述

流程

1. 登录到 RHEL web 控制台。详情请参阅 登录到 web 控制台。

2. 打开 **网络**。
3. 点击您要配置的绑定。
4. 在绑定设置屏幕中，滚动到端口表（接口）。
5. 选择接口并删除或禁用它：
   - 要删除接口，请点击 **-** 按钮。
   - 要禁用或启用接口，在所选接口旁切换切换。

根据您的选择，Web 控制台可以从绑定中删除或禁用接口，您可以在 **Networking** 部分作为独立接口重新看到它。

8.6. 使用 WEB 控制台删除或禁用绑定

使用 Web 控制台删除或禁用网络绑定。如果您禁用绑定，接口保留在绑定中，但绑定不会用于网络流量。

先决条件

- web 控制台中有一个现有绑定。

流程

1. 登录到 web 控制台。
   详情请参阅 登录到 web 控制台。
2. 打开 **网络**。
3. 点击您要删除的绑定。
4. 在绑定设置屏幕中，您可以通过切换切换程序或点 **Delete** 按钮来永久删除绑定来禁用或启用绑定。

验证步骤

- 返回到 **网络**，并验证绑定中的所有接口现在都是独立接口。

第 9 章 使用 WEB 控制台配置网络团队（NETWORK TEAM）

了解网络绑定如何工作，网络团队和网络绑定之间的区别，以及 web 控制台中配置的可能性。

另外，您还可以参阅以下指南：

- 添加新网络 team
- 在现有网络 team 中添加新接口
- 从现有网络 team 中删除接口
- 删除网络 team

重要

网络 teaming 在 Red Hat Enterprise Linux 9 中已弃用。如果您计划将服务器升级到将来的 RHEL 版本，请考虑使用内核绑定驱动程序作为替代方案。详情请参阅 配置网络绑定。

先决条件

- 已安装并启用 RHEL web 控制台。
  详情请参阅安装 Web 控制台。

9.1. 使用 RHEL WEB 控制台配置网络团队

如果您希望使用基于 Web 浏览器的界面管理网络设置，请使用 RHEL web 控制台来配置网络团队。

重要

网络 teaming 在 Red Hat Enterprise Linux 9 中已弃用。考虑使用网络绑定驱动程序作为替代方案。详情请参阅 配置网络绑定。

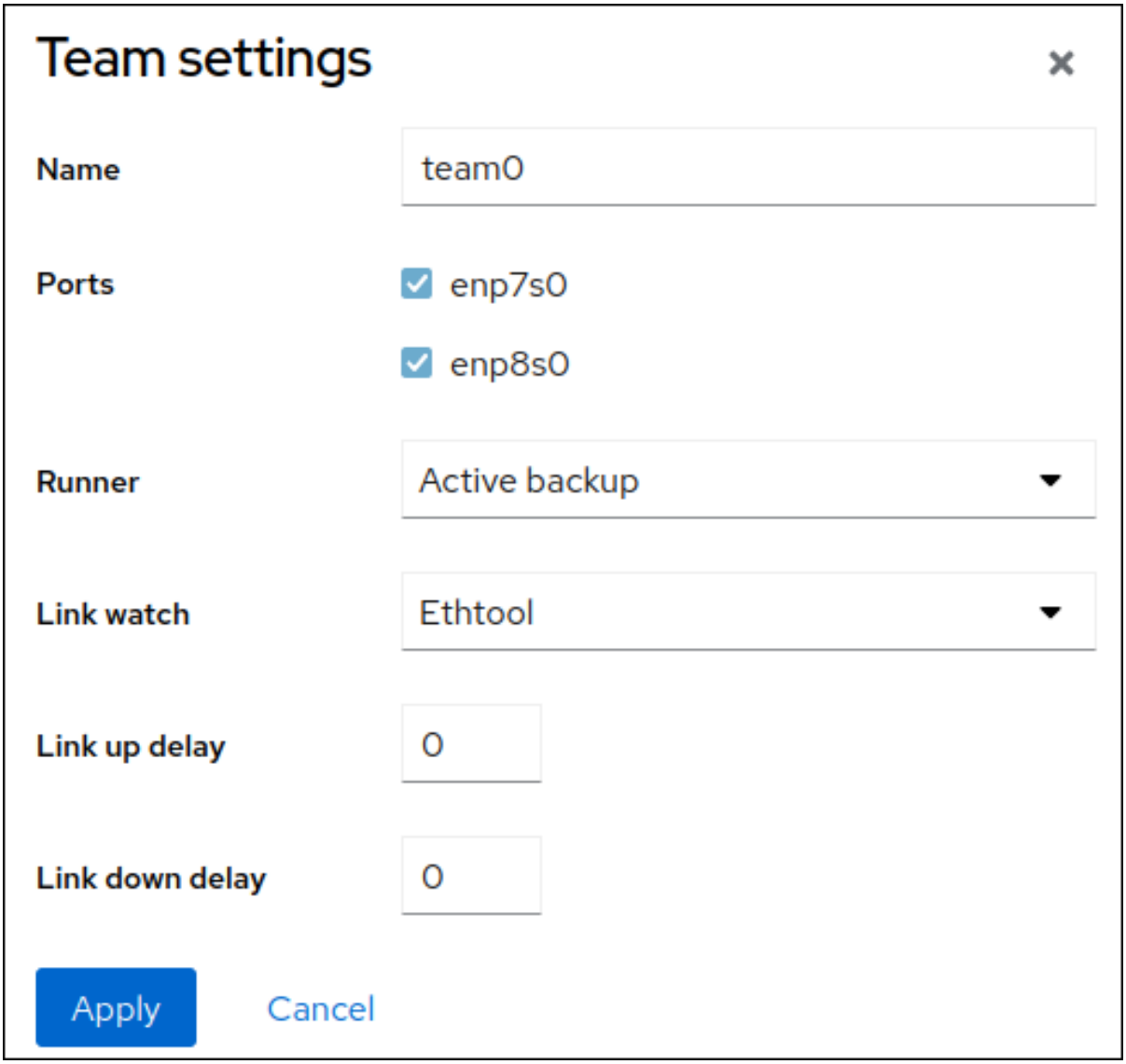
先决条件

- 已安装 **teamd** 和 **NetworkManager-team** 软件包。
- 在服务器中安装两个或者两个以上物理或者虚拟网络设备。
- 要将以太网设备用作组的端口，必须在服务器中安装物理或者虚拟以太网设备并连接到交换机。
- 要将 bond、bridge 或 VLAN 设备用作团队的端口，请预先创建它们，如下所述：
  - 使用 RHEL web 控制台配置网络绑定
  - 使用 RHEL web 控制台配置网桥
  - 使用 RHEL web 控制台配置 VLAN 标记

流程

1. 在屏幕左侧的导航中选择 **Networking** 选项卡。
2. 在 **Interfaces** 部分点 **Add team**。

3. 输入您要创建的团队设备名称。
4. 选择应该是团队端口的接口。
5. 选择团队的运行程序。
   如果您选择 **Load balancing** 或 **802.3ad LACP**，Web 控制台会显示额外的 **Balancer** 字段。
6. 设置链接监视器：
   - 如果您选择 **Ethtool**，请设置链接并关闭延迟。
   - 如果您设置了 **ARP ping** 或 **NSNA ping**，还要设置 ping 间隔并 ping 目标。

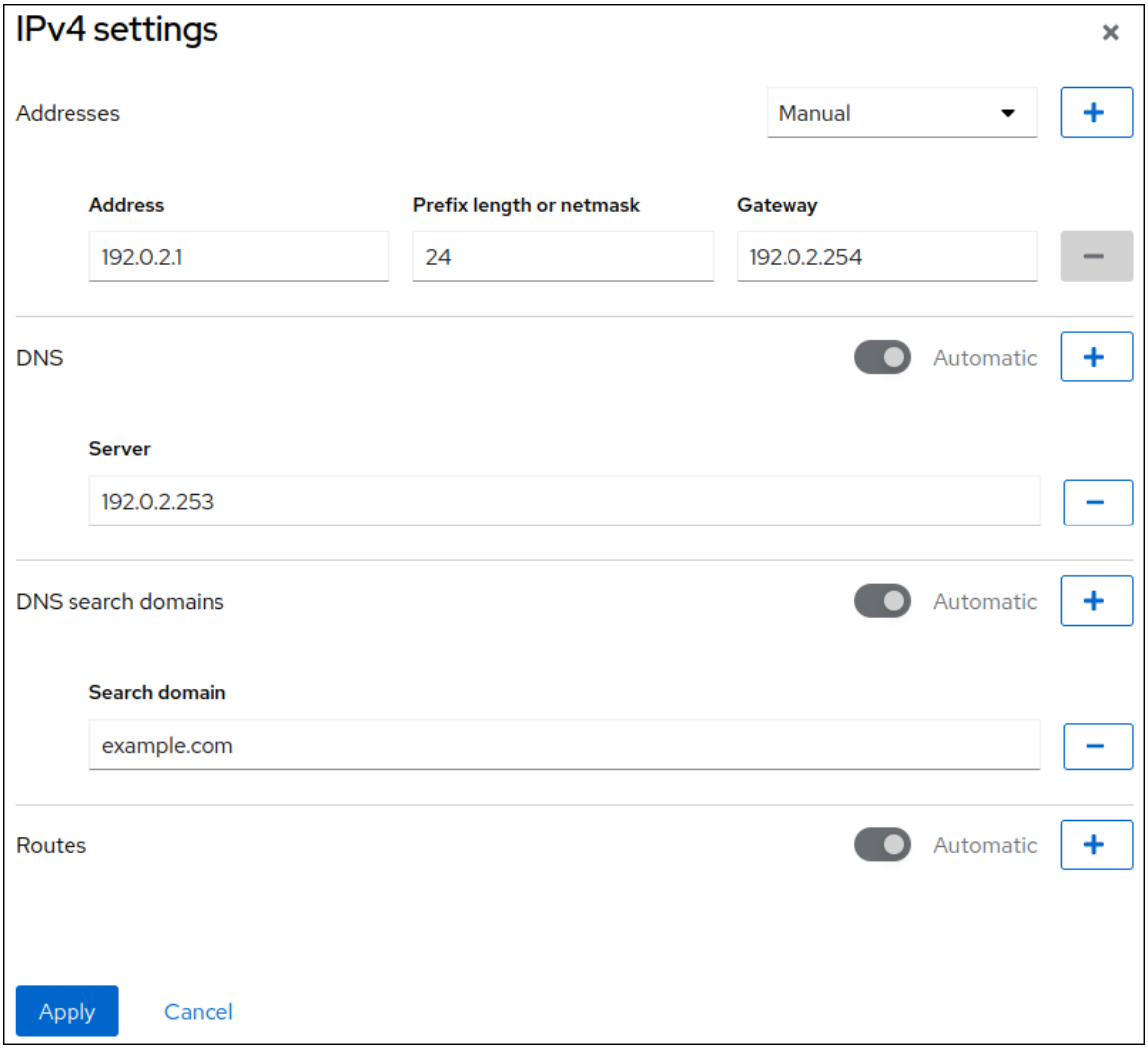


7. 点**应用**。
8. 默认情况下，团队使用动态 IP 地址。如果要设置静态 IP 地址：
   a. 在 **Interfaces** 部分点团队的名称。
   b. 点您要配置的协议旁的 **Edit**。
   c. 选择 **Addresses** 旁的 **Manual**，并输入 IP 地址、前缀和默认网关。

d. 在 **DNS** 部分，点 **+** 按钮，并输入 DNS 服务器的 IP 地址。重复此步骤来设置多个 DNS 服务器。

e. 在 **DNS search domains** 部分中，点 **+** 按钮并输入搜索域。

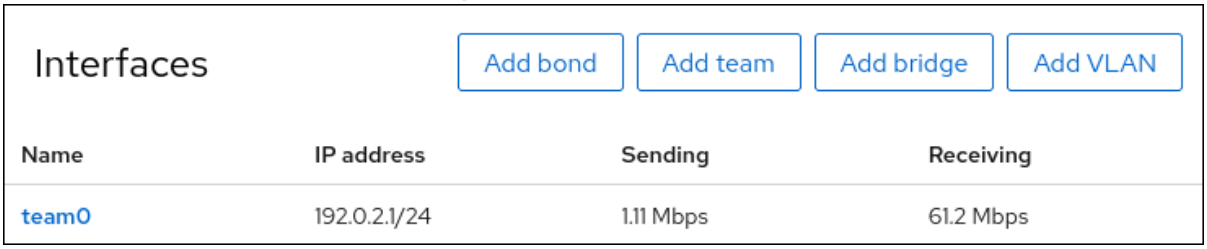
f. 如果接口需要静态路由，请在 **Routes** 部分配置它们。



g. 点 **应用**

验证

1. 在屏幕左侧的导航中选择 **Networking** 选项卡，并检查接口上是否有传入和传出流量。



2. 显示团队状态：

```
# teamdctl team0 state
setup:
  runner: activebackup
ports:
  enp7s0
```

```
    link watches:
      link summary: up
      instance[link_watch_0]:
        name: ethtool
        link: up
        down count: 0
  enp8s0
    link watches:
      link summary: up
      instance[link_watch_0]:
        name: ethtool
        link: up
        down count: 0
runner:
  active port: enp7s0
```

在这个示例中，两个端口都是上线的。

其它资源

- 网络团队运行程序

9.2. 使用 WEB 控制台向团队添加新接口

网络团队可以包含多个接口，可以随时添加或删除任何接口。下面的部分论述了如何为现有团队添加新网络接口。

先决条件

- 配置了网络团队。

流程

1. 登录到 web 控制台。
   详情请参阅 登录到 web 控制台。
2. 切换到 **Networking** 选项卡。
3. 在 **Interfaces** 表中，点您要配置的团队。
4. 在团队设置窗口中，向下滚动到 **Ports** 表。
5. 点 **+** 按钮。
6. 从下拉列表中选择您要添加的接口。

RHEL web 控制台为团队添加接口。

9.3. 使用 WEB 控制台从团队中删除或禁用接口

网络团队可以包含多个接口。如果您需要更改设备，可以从网络团队中删除或者禁用特定的接口，这些接口可与其它活跃接口一同工作。

可以使用两个选项停止一个团队中的一个接口：

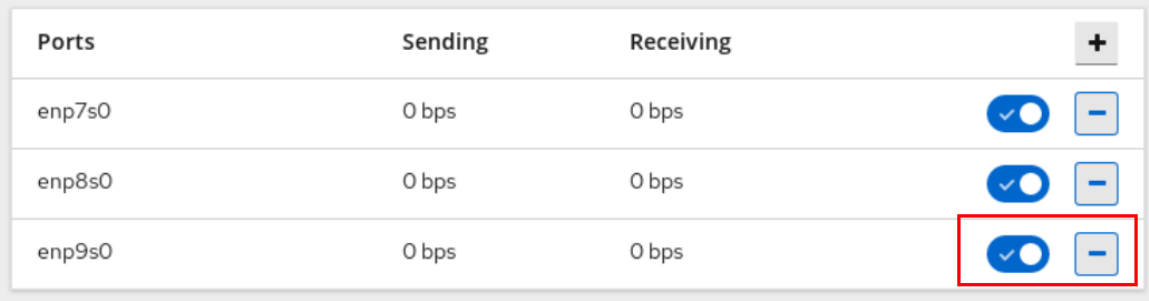
- 从团队中删除接口
- 临时禁用该接口。这个接口会作为团队的一部分被保留，当在重新启用它之前不会被使用。

先决条件

- 主机上存在具有多个接口的网络组。

流程

1. 登录到 RHEL web 控制台。
   详情请参阅 登录到 web 控制台。
2. 切换到 **Networking** 选项卡。
3. 点您要配置的团队。
4. 在团队设置窗口中，向下滚动到端口表（接口）。
5. 选择一个接口并删除或禁用它。
   a. 将 **ON/OFF** 按钮切换为 Off 以禁用接口。
   b. 点 **-** 按钮删除接口。



根据您的选择，Web 控制台会删除或禁用接口。如果删除该接口，它将作为独立接口在网络中可用。

9.4. 使用 WEB 控制台删除或禁用团队

使用 Web 控制台删除或禁用网络团队。如果您只禁用该团队，则团队中的接口将保留在其中，但团队不会用于网络流量。

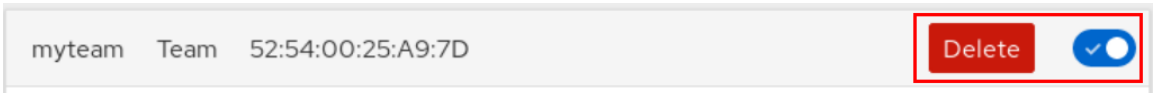
先决条件

- 主机上配置了网络组。

流程

1. 登录到 web 控制台。
   详情请参阅 登录到 web 控制台。

2. 切换到 **Networking** 选项卡。
3. 点您要删除或禁用的 team。
4. 删除或禁用所选团队。
   a. 您可以点击 **Delete** 按钮删除团队。
   b. 您可以通过将 **ON/OFF** 开关切换到禁用的位置来禁用团队。



验证步骤

- 如果您删除了该团队，请访问 **Networking**，并验证您的团队中的所有接口现在都列为独立接口。

第 10 章 在 WEB 控制台中配置网络桥接

网络桥接用于将多个接口连接到一个具有相同 IP 地址范围的子网。

先决条件

- 已安装并启用 RHEL 9 web 控制台。
  详情请参阅安装 Web 控制台。

10.1. 使用 RHEL WEB 控制台配置网桥

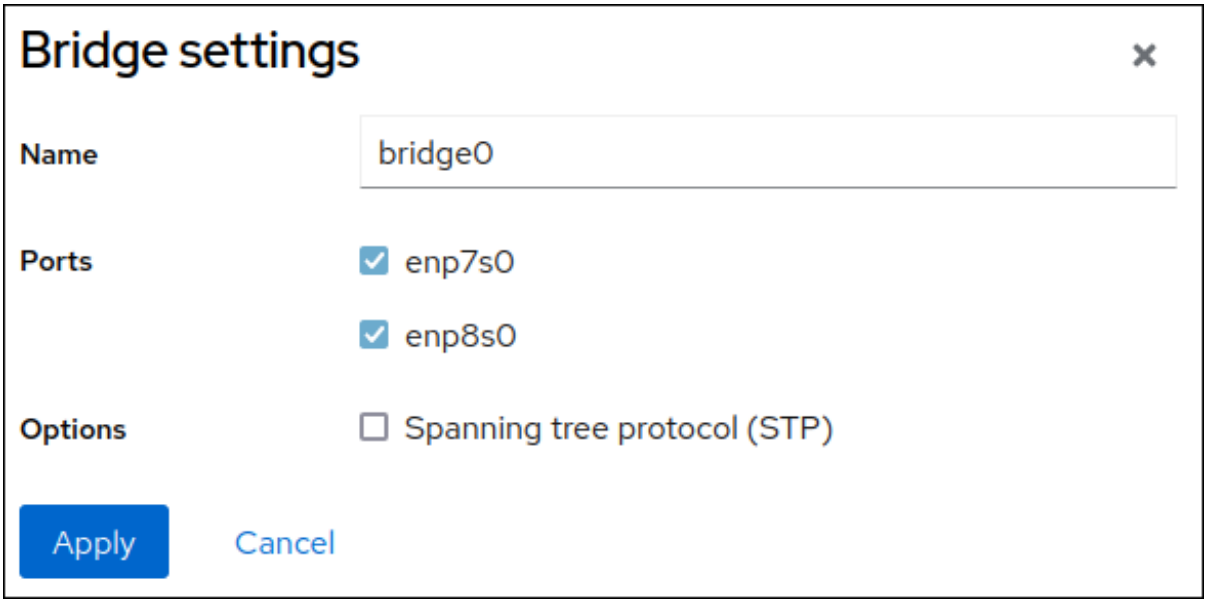
如果您希望通过基于 Web 浏览器的界面管理网络设置，请使用 RHEL web 控制台来配置网桥。

先决条件

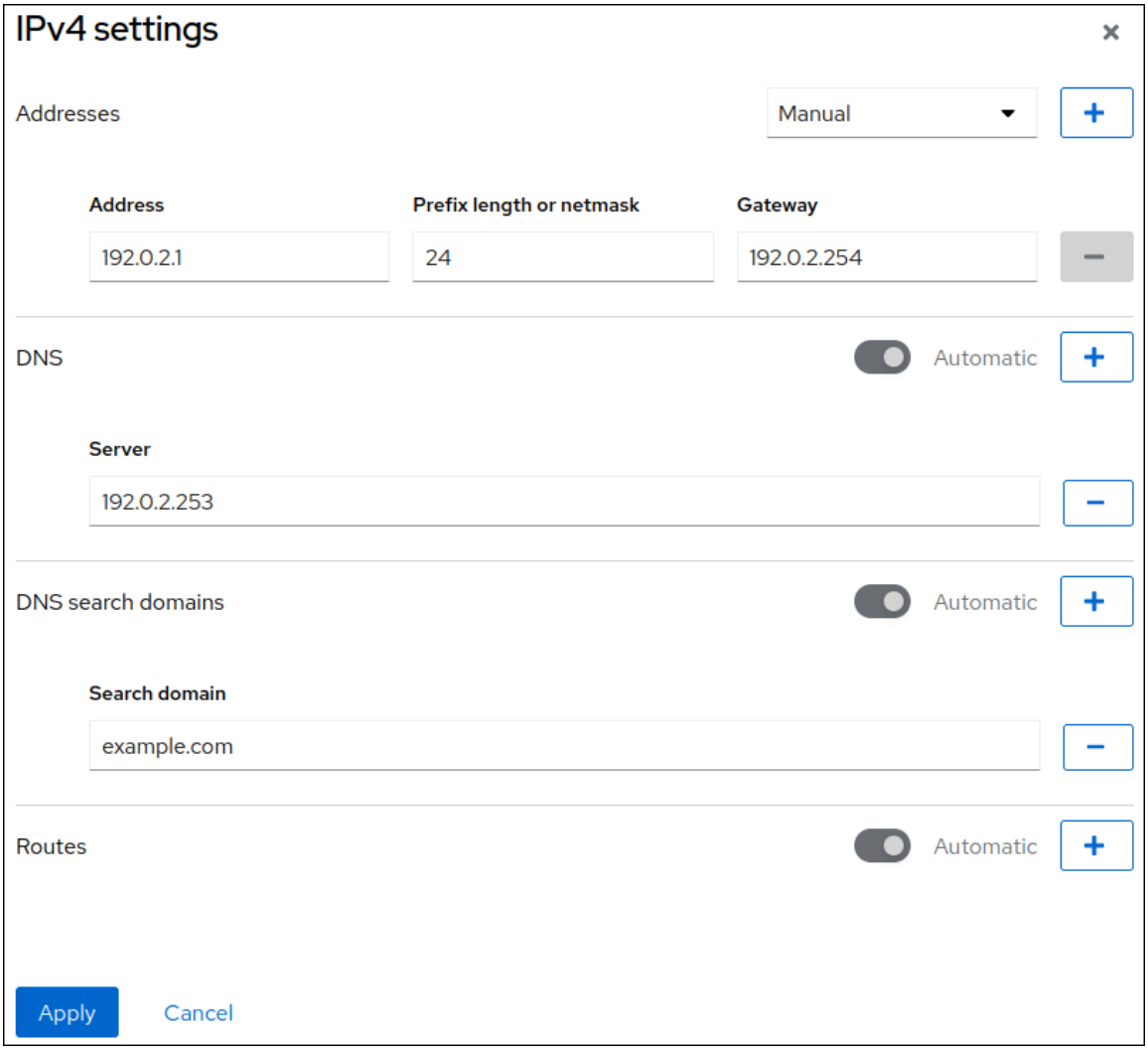
- 在服务器中安装两个或者两个以上物理或者虚拟网络设备。
- 要将以太网设备用作网桥的端口，必须在服务器中安装物理或者虚拟以太网设备。
- 要使用 team、bond 或 VLAN 设备作为网桥的端口，您可以在创建桥接时创建这些设备，或者预先创建它们，如：
  - 使用 RHEL web 控制台配置网络团队
  - 使用 RHEL web 控制台配置网络绑定
  - 使用 RHEL web 控制台配置 VLAN 标记

流程

1. 在屏幕左侧的导航中选择 **Networking** 选项卡。
2. 在 **Interfaces** 部分点 **Add bridge**。
3. 输入您要创建的网桥设备名称。
4. 选择应该是网桥端口的接口。
5. 可选：可选：启用 **生成树协议(STP)** 功能，以避免桥接循环和广播。



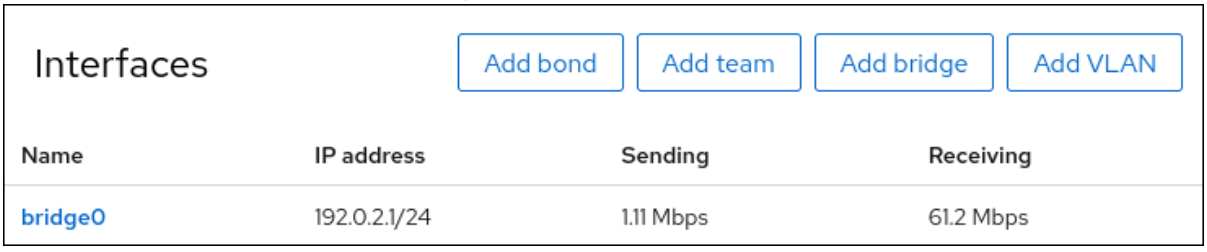
6. 点**应用**。
7. 默认情况下，网桥使用动态 IP 地址。如果要设置静态 IP 地址：
   a. 在 **Interfaces** 部分，点网桥的名称。
   b. 点您要配置的协议旁的 **Edit**。
   c. 选择 **Addresses** 旁的 **Manual**，并输入 IP 地址、前缀和默认网关。
   d. 在 **DNS** 部分，点 **+** 按钮，并输入 DNS 服务器的 IP 地址。重复此步骤来设置多个 DNS 服务器。
   e. 在 **DNS search domains** 部分中，点 **+** 按钮并输入搜索域。
   f. 如果接口需要静态路由，请在 **Routes** 部分配置它们。



g. 点 应用

验证

1. 在屏幕左侧的导航中选择 **Networking** 选项卡，并检查接口上是否有传入和传出流量：



10.2. 使用 WEB 控制台从网桥中删除接口

网络桥接可以包含多个接口。您可以从网桥中删除它们。每个删除的接口将自动改为独立接口。

了解如何从 RHEL 9 系统中创建的软件桥接中删除网络接口。

先决条件

- 在系统中使用带有多个接口的网桥。

流程

1. 登录到 RHEL web 控制台。详情请参阅 登录到 web 控制台。
2. 打开 **网络**。
3. 点击您要配置的网桥。
4. 在网桥设置屏幕中，滚动到端口表（接口）。
5. 选择一个接口并点 **-** 按钮。

验证步骤

- 前往 **Networking** 以检查您可以作为接口 **成员** 表中的独立接口。

10.3. 删除 WEB 控制台中的网桥

您可以删除 RHEL web 控制台中的软件网络桥接。网桥中包括的所有网络接口将自动改为独立接口。

先决条件

- 在您的系统中有一个桥接。

流程

1. 登录到 RHEL web 控制台。
   详情请参阅 登录到 web 控制台。
2. 打开 **Networking** 部分。
3. 点击您要配置的网桥。
4. 点击 **Delete**。

验证步骤

- 返回到 **Networking**，并验证所有网络接口都显示在接口 **成员** 表中。

之前作为网桥的一部分的一些接口可能会变得不活跃。如有必要，激活它们并手动设置网络参数。

第 11 章 在 WEB 控制台中配置 VLAN

这部分论述了如何配置虚拟本地区域网络（VLAN）。VLAN 是物理网络中的一个逻辑网络。当 VLAN 接口通过接口时，VLAN 接口标签带有 VLAN ID 的数据包，并删除返回的数据包的标签。

11.1. 使用 RHEL WEB 控制台配置 VLAN 标记

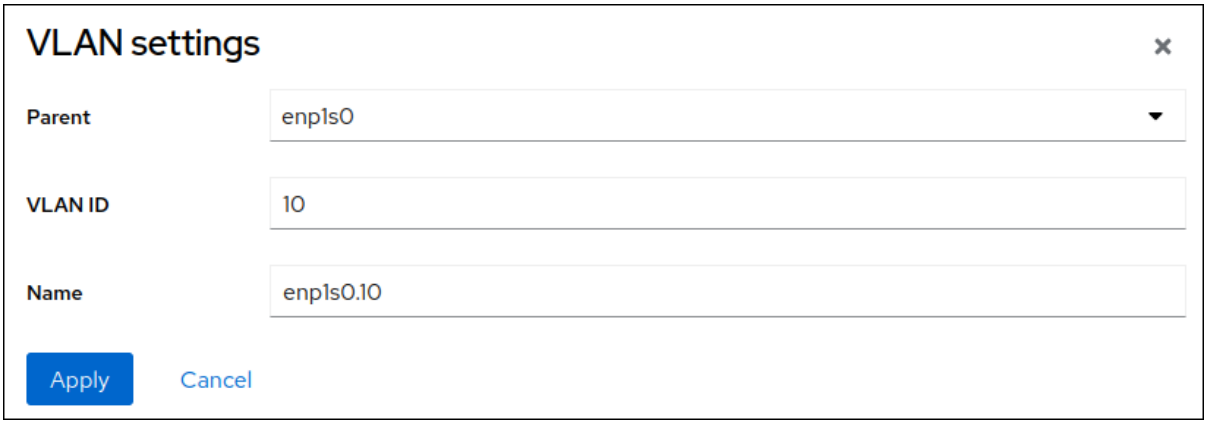
如果您希望使用基于 Web 浏览器的界面管理网络设置，请使用 RHEL web 控制台配置 VLAN 标记。

先决条件

- 您计划用作虚拟 VLAN 接口的父接口支持 VLAN 标签。
- 如果您在绑定接口之上配置 VLAN：
  - 绑定的端口是上线的。
  - 这个绑定没有使用 **fail_over_mac=follow** 选项进行配置。VLAN 虚拟设备无法更改其 MAC 地址以匹配父设备的新 MAC 地址。在这种情况下，流量仍会与不正确的源 MAC 地址一同发送。
  - 这个绑定通常不会预期从 DHCP 服务器或 IPv6 自动配置获取 IP 地址。禁用 IPv4 和 IPv6 协议创建绑定以确保它。否则，如果 DHCP 或 IPv6 自动配置在一段时间后失败，接口可能会关闭。
- 主机连接到的交换机被配置为支持 VLAN 标签。详情请查看您的交换机文档。

流程

1. 在屏幕左侧的导航中选择 **Networking** 选项卡。
2. 在 **Interfaces** 部分点 **Add VLAN**。
3. 选择父设备。
4. 输入 VLAN ID。
5. 输入 VLAN 设备的名称，或保留自动生成的名称。



6. 点应用。
7. 默认情况下，VLAN 设备使用动态 IP 地址。如果要设置静态 IP 地址：
   a. 点 **Interfaces** 部分中的 VLAN 设备名称。

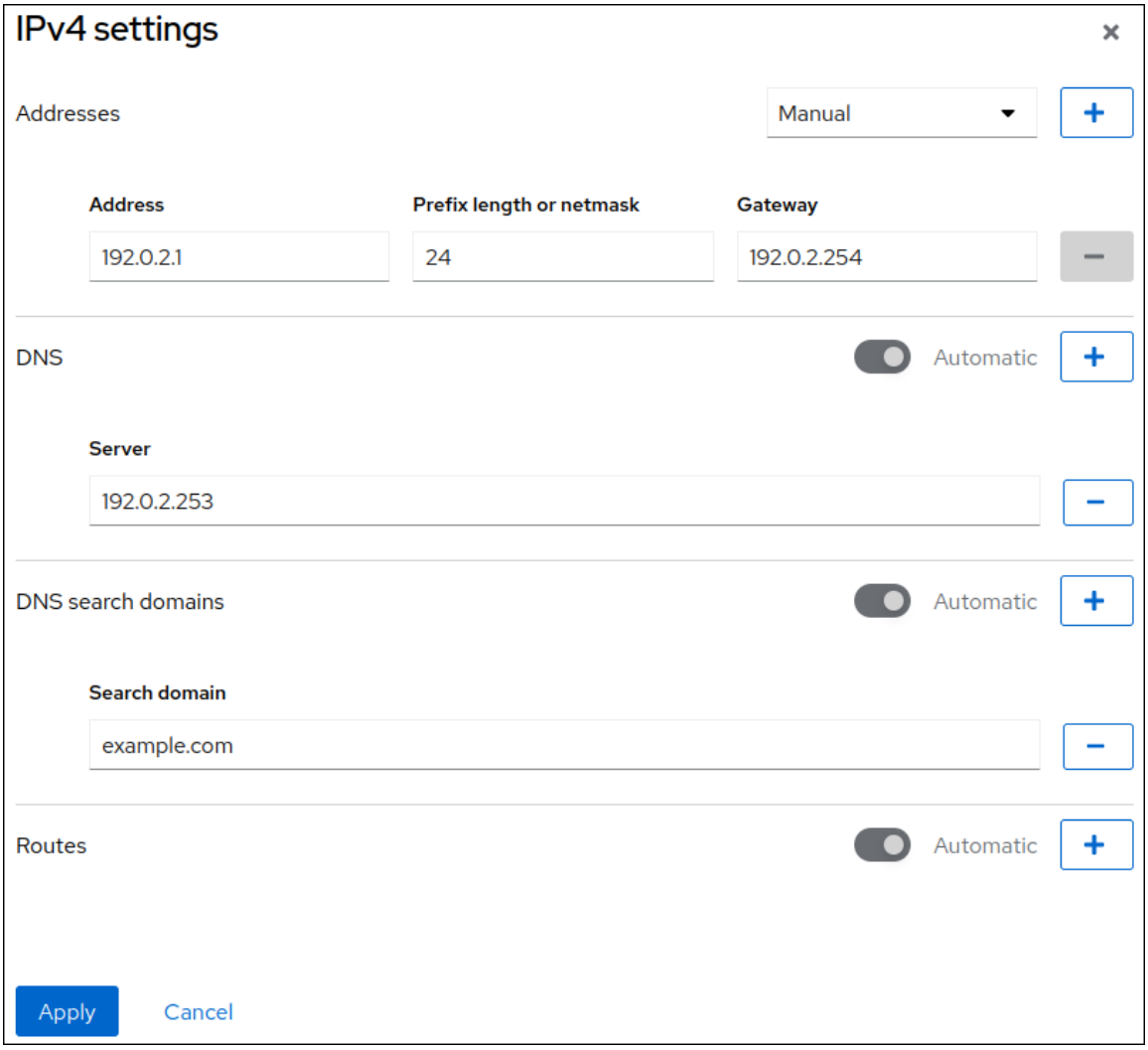
b. 点您要配置的协议旁的 **Edit**。

c. 选择 **Addresses** 旁的 **Manual**，并输入 IP 地址、前缀和默认网关。

d. 在 **DNS** 部分，点 **+** 按钮，并输入 DNS 服务器的 IP 地址。重复此步骤来设置多个 DNS 服务器。

e. 在 **DNS search domains** 部分中，点 **+** 按钮并输入搜索域。

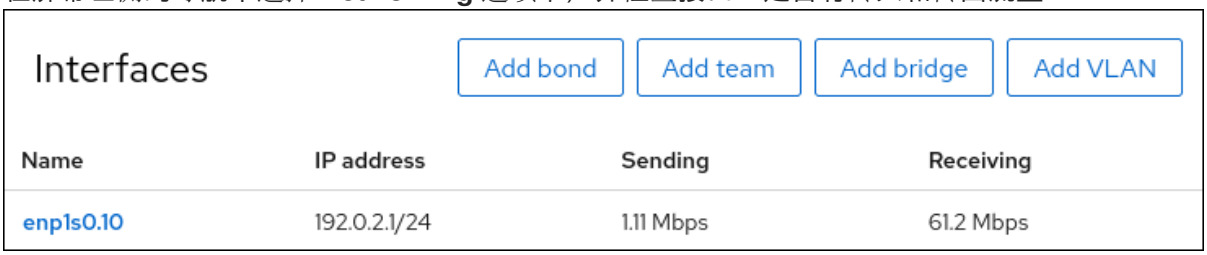
f. 如果接口需要静态路由，请在 **Routes** 部分配置它们。



g. 点 **应用**

验证

- 在屏幕左侧的导航中选择 **Networking** 选项卡，并检查接口上是否有传入和传出流量：



第 12 章 使用 RHEL WEB 控制台设置 WIREGUARD VPN

WireGuard 是一个在 Linux 内核中运行的高性能 VPN 解决方案。它使用现代加密机制，并且比许多其他 VPN 解决方案更容易配置。另外，WireGuard 的小代码库降低了安全攻击的攻击面，因此提高安全性。对于身份验证和加密，WireGuard 使用类似于 SSH 的键。

重要

WireGuard 只作为技术预览提供。红帽产品服务级别协议（SLA）不支持技术预览功能，且其功能可能并不完善，因此红帽不建议在生产环境中使用它们。这些预览可让用户早期访问将来的产品功能，让用户在开发过程中测试并提供反馈意见。

如需有关 技术预览功能支持范围 的信息，请参阅红帽客户门户网站中的技术预览功能支持范围。

请注意，参与 WireGuard VPN 的所有主机都是同级的。本文档使用术语 **客户端** 来描述建立连接的主机，使用 **服务器** 来描述固定主机名或客户端连接的 IP 地址的主机，并可选通过这个服务器路由所有流量。

WireGuard 在网络层（层 3）上运行。因此，您无法使用 DHCP，且必须为服务器和客户端上的隧道设备分配静态 IP 地址或 IPv6 本地链接地址。

重要

只有在禁用 RHEL 中的 Federal Information Processing Standard(FIPS)模式时，才能使用 WireGuard。

12.1. WIREGUARD 使用的协议和原语

WireGuard 使用以下协议和原语：

- ChaCha20 用于通过 Poly1305 进行身份验证，使用带有关联数据(AEAD)的 Authenticated Encryption，如 RFC7539 所述
- Curve25519 用于 Elliptic-curve Diffie-Hellman(ECDH)密钥交换
- 用于哈希和密钥哈希的 BLAKE2s，如 RFC7693所述
- 用于哈希表键的 SipHash24
- 用于密钥派生的 HKDF，如 RFC5869所述

12.2. WIREGUARD 如何使用隧道 IP 地址、公钥和远程端点

当 WireGuard 将网络数据包发送到对等点时：

1. WireGuard 从数据包读取目标 IP，并将其与本地配置中允许的 IP 地址列表进行比较。如果未找到 peer，WireGuard 会丢弃数据包。
2. 如果 peer 有效，WireGuard 使用对等的公钥对数据包进行加密。
3. 发送主机查找主机的最新互联网 IP 地址，并将加密数据包发送到此地址。

当 WireGuard 接收数据包时：

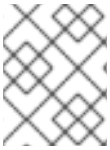
1. WireGuard 使用远程主机的私钥解密数据包。
2. WireGuard 从数据包读取内部源地址，并在本地主机上对等点的设置中查询 IP 地址是否配置。如果源 IP 位于允许列表中，WireGuard 会接受数据包。如果 IP 地址不在列表中，WireGuard 会丢弃数据包。

公钥和允许的 IP 地址的关联称为 **加密密钥路由表**。这意味着，当发送数据包时，IP 地址列表的行为与路由表相似，在接收数据包时作为一种访问控制列表。

12.3. 使用 NAT 和防火墙后面的 WIREGUARD 客户端

WireGuard 使用 UDP 协议，只有在对等点发送数据包时才会传输数据。路由器上的有状态防火墙和网络地址转换(NAT)可跟踪连接，以启用 NAT 或防火墙接收数据包的对等点。

为了保持连接处于活动状态，WireGuard 支持 **持久性 keepalives**。这意味着您可以设置一个间隔，其中 WireGuard 发送 keepalive 数据包。默认情况下，禁用持久的 keep-alive 功能来减少网络流量。如果您在带有 NAT 的网络中使用客户端，或者防火墙在一定时间不活动状态后关闭连接，在客户端上启用此功能。



注意

请注意，您无法使用 RHEL web 控制台在 WireGuard 连接中配置 keepalive 数据包。要配置此功能，请使用 **nmcli** 工具编辑连接配置文件。

12.4. 使用 RHEL WEB 控制台配置 WIREGUARD 服务器

您可以使用基于浏览器的 RHEL web 控制台配置 WireGuard 服务器。使用此方法让 NetworkManager 管理 WireGuard 连接。

先决条件

- 已登陆到 RHEL web 控制台。
- 您知道以下信息：
  - 服务器和客户端的静态隧道 IP 地址和子网掩码
  - 客户端的公钥

流程

1. 在屏幕左侧的导航中选择 **Networking** 选项卡。
2. 在 **Interfaces** 部分中点 **Add VPN**。
3. 如果还没有安装 **wireguard-tools** 和 **systemd-resolved** 软件包，Web 控制台会显示一条相应的通知。点 **Install** 安装这些软件包。
4. 输入您要创建的 WireGuard 设备的名称。
5. 配置此主机的密钥对：
   - 如果要使用 web 控制台创建的密钥：
     i. 在 **Private key** 区域中保持预先选择的 **Generated** 选项。

ii. 请注意 **Public key** 值。配置客户端时需要此信息。

- 如果要使用现有的私钥：

  i. 在 **Private key** 区域中选择 **Paste existing key**。

  ii. 将私钥粘贴到文本字段中。Web 控制台自动计算相应的公钥。

6. 为传入的 WireGuard 连接设置一个侦听端口号，如 **51820**。
   在主机上始终设置固定端口号，接收传入的 WireGuard 连接。如果您没有设置端口，WireGuard 会在每次激活接口时都使用一个随机的空闲端口。

7. 设置服务器的隧道 IPv4 地址和子网掩码。
   要也设置 IPv6 地址，您必须在创建连接后编辑它。

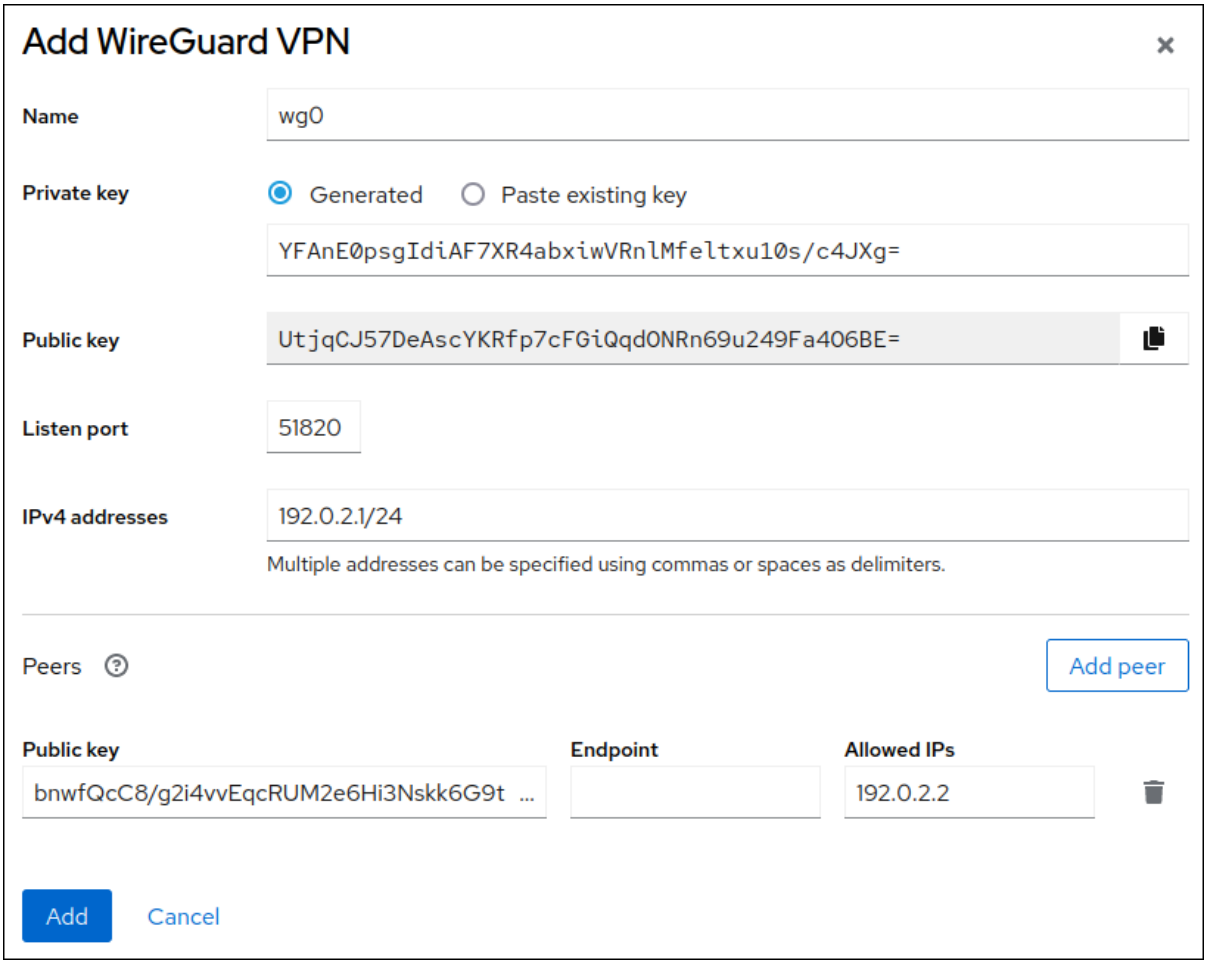
8. 为您要允许与此服务器进行通信的每个客户端添加对等配置：

   a. 单击 **Add peer**。

   b. 输入客户端的公钥。

   c. **Endpoint** 字段留空。

   d. 将 **Allowed IP** 字段设置为允许向这个服务器发送数据的客户端的隧道 IP 地址。



9. 点 **Add** 创建 WireGuard 连接。

10. 如果您还想设置隧道 IPv6 地址：

    a. 在 **Interfaces** 部分点 WireGuard 连接的名称。

b. 点 **IPv6** 旁的 **edit**。

c. 将 **Addresses** 字段设置为 **Manual**，并输入服务器的隧道 IPv6 地址和前缀。

d. 点 **Save**。

后续步骤

- 在 WireGuard 服务器上配置 firewalld 服务。

验证

1. 显示 **wg0** 设备的接口配置：

```
# wg show wg0
interface: wg0
  public key: UtjqCJ57DeAscYKRfp7cFGiQqdONRn69u249Fa4O6BE=
  private key: (hidden)
  listening port: 51820

peer: bnwfQcC8/g2i4vvEqcRUM2e6Hi3Nskk6G9t4r26nFVM=
  allowed ips: 192.0.2.2/32, 2001:db8:1::2/128
```

要在输出中显示私钥，请使用 **WG_HIDE_KEYS=never wg show *wg0*** 命令。

2. 显示 **wg0** 设备的 IP 配置：

```
# ip address show wg0
20: wg0: <POINTOPOINT,NOARP,UP,LOWER_UP> mtu 1420 qdisc noqueue state
UNKNOWN group default qlen 1000
    link/none
    inet 192.0.2.1/24 brd 192.0.2.255 scope global noprefixroute wg0
       valid_lft forever preferred_lft forever
    inet6 2001:db8:1::1/32 scope global noprefixroute
       valid_lft forever preferred_lft forever
    inet6 fe80::3ef:8863:1ce2:844/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

12.5. 使用 RHEL WEB 控制台在 WIREGUARD 服务器上配置 FIREWALLD

您必须在 WireGuard 服务器上配置 **firewalld** 服务，以允许来自客户端的传入的连接。另外，如果客户端能够使用 WireGuard 服务器作为默认网关，并通过隧道路由所有流量，则必须启用伪装。

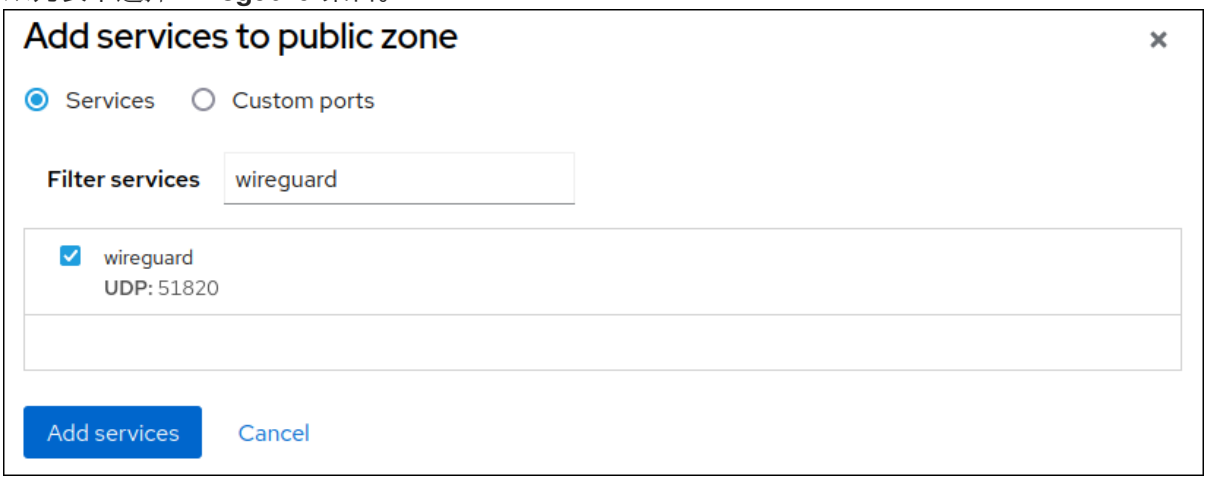
先决条件

- 已登陆到 RHEL web 控制台。

流程

1. 在屏幕左侧的导航中选择 **Networking** 选项卡。
2. 点 **Firewall** 部分中的 **Edit rules and zones**。
3. 在 **Filter services** 字段中输入 **wireguard**。

4. 从列表中选择 **wireguard** 条目。



5. 点 **Add services**。

6. 如果客户端应该使用 WireGuard 服务器作为默认网关来通过隧道路由所有流量，请为 **public** 区域启用伪装：

```
# firewall-cmd --permanent --zone=public --add-masquerade
# firewall-cmd --reload
```

请注意，您无法在 web 控制台的 **firewalld** 区域中启用伪装。

验证

1. 在屏幕左侧的导航中选择 **Networking** 选项卡。
2. 点 **Firewall** 部分中的 **Edit rules and zones**。
3. 列表包含一个 **wireguard** 服务的条目，并显示您在 WireGuard 连接配置文件中配置的 UDP 端口。
4. 要验证在 **firewalld public** 区域中是否启用了伪装，请输入：

```
# firewall-cmd --list-all --zone=public
public (active)
  ...
  ports: 51820/udp
  masquerade: yes
  ...
```

12.6. 使用 RHEL WEB 控制台配置 WIREGUARD 客户端

您可以使用基于浏览器的 RHEL web 控制台配置 WireGuard 客户端。使用此方法让 NetworkManager 管理 WireGuard 连接。

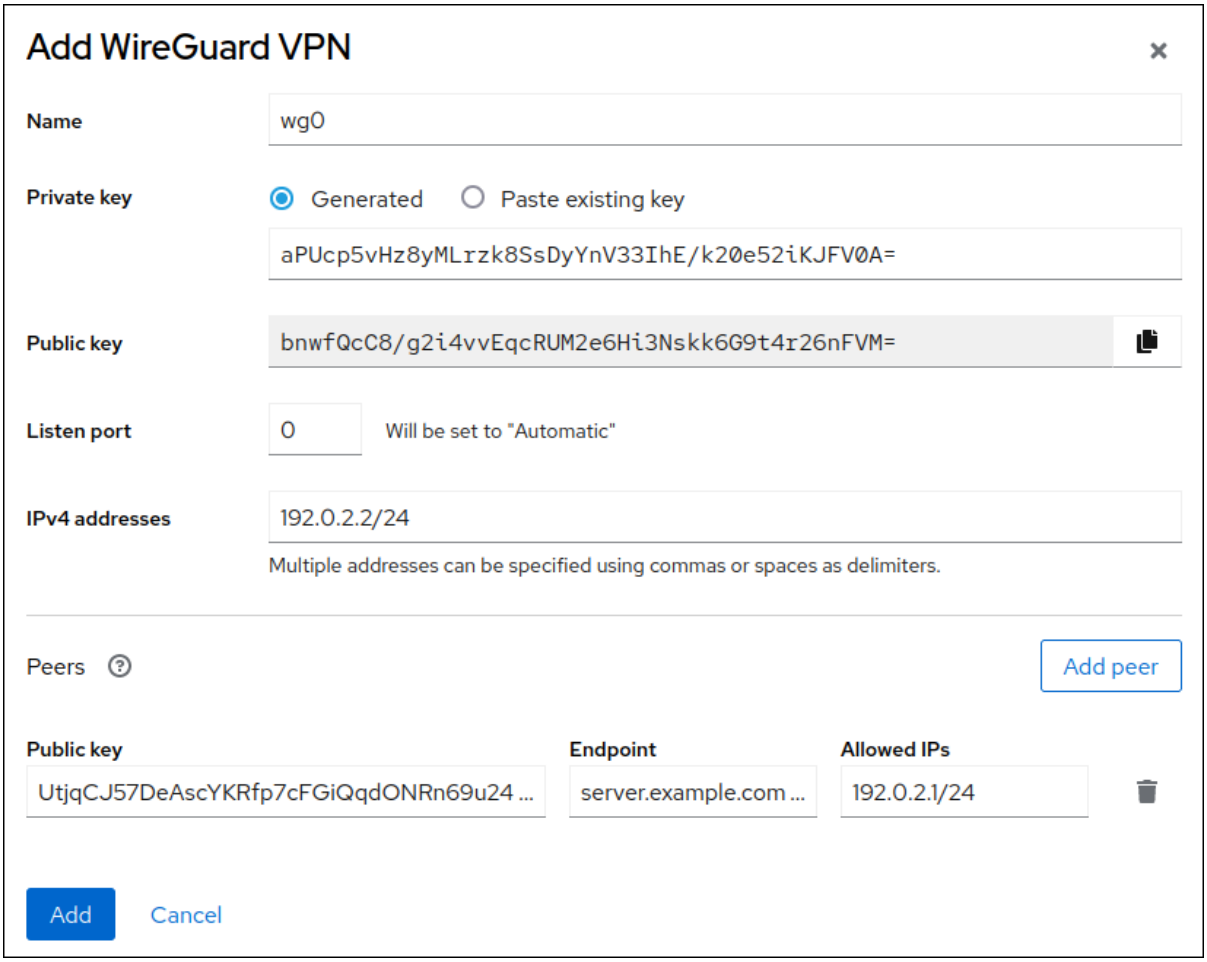
先决条件

- 已登陆到 RHEL web 控制台。
- 您知道以下信息：
  - 服务器和客户端的静态隧道 IP 地址和子网掩码

- 服务器的公钥

流程

1. 在屏幕左侧的导航中选择 **Networking** 选项卡。
2. 在 **Interfaces** 部分中点 **Add VPN**。
3. 如果还没有安装 **wireguard-tools** 和 **systemd-resolved** 软件包，Web 控制台会显示一条相应的通知。点 **Install** 安装这些软件包。
4. 输入您要创建的 WireGuard 设备的名称。
5. 配置此主机的密钥对：
   - 如果要使用 web 控制台创建的密钥：
     i. 在 **Private key** 区域中保持预先选择的 **Generated** 选项。
     ii. 请注意 **Public key** 值。配置客户端时需要此信息。
   - 如果要使用现有的私钥：
     i. 在 **Private key** 区域中选择 **Paste existing key** 。
     ii. 将私钥粘贴到文本字段中。Web 控制台自动计算相应的公钥。
6. 在 **Listen port** 字段中保留 **0** 值。
7. 设置客户端的隧道 IPv4 地址和子网掩码。
   要也设置 IPv6 地址，您必须在创建连接后编辑它。
8. 为您要允许与此客户端进行通信的服务器添加对等配置：
   a. 单击 **Add peer**。
   b. 输入服务器的公钥。
   c. 将 **Endpoint** 字段设置为主机名或 IP 地址，以及服务器的端口，如 **server.example.com:51820**。客户端使用此信息来建立连接。
   d. 将 **Allowed IP** 字段设置为允许向这个服务器发送数据的客户端的隧道 IP 地址。例如，将字段设置为以下之一：
      - 服务器隧道 IP 地址，以仅允许服务器与此客户端通信。下面屏幕截图中的值配置这种场景。
      - **0.0.0.0/0** 允许任何远程 IPv4 地址与此客户端进行通信。使用此设置通过隧道路由所有流量，并使用 WireGuard 服务器作为默认网关。



9. 点 **Add** 创建 WireGuard 连接。
10. 如果您还想设置隧道 IPv6 地址：
    a. 在 **Interfaces** 部分点 WireGuard 连接的名称。
    b. 点 **IPv6** 旁的 **edit**。
    c. 将 **Addresses** 字段设置为 **Manual**，并输入客户端的隧道 IPv6 地址和前缀。
    d. 点 **Save**。

验证

1. Ping 服务器的 IP 地址：

```
# ping 192.0.2.1
```

当您尝试通过隧道发送流量时，WireGuard 会建立连接。

2. 显示 **wg0** 设备的接口配置：

```
# wg show wg0
interface: wg0
  public key: bnwfQcC8/g2i4vvEqcRUM2e6Hi3Nskk6G9t4r26nFVM=
  private key: (hidden)
  listening port: 45513
```

```
peer: UtjqCJ57DeAscYKRfp7cFGiQqdONRn69u249Fa4O6BE=
  endpoint: server.example.com:51820
  allowed ips: 192.0.2.1/32, 2001:db8:1::1/128
  latest handshake: 1 minute, 41 seconds ago
  transfer: 824 B received, 1.01 KiB sent
  persistent keepalive: every 20 seconds
```

要在输出中显示私钥，请使用 **WG_HIDE_KEYS=never wg show *wg0*** 命令。

请注意，如果您已经通过 VPN 隧道发送流量，则输出只有 **latest handshake** 和**transfer** 条目。

3. 显示 **wg0** 设备的 IP 配置：

```
# ip address show wg0
10: wg0: <POINTOPOINT,NOARP,UP,LOWER_UP> mtu 1420 qdisc noqueue state
UNKNOWN group default qlen 1000
    link/none
    inet 192.0.2.2/24 brd 192.0.2.255 scope global noprefixroute wg0
       valid_lft forever preferred_lft forever
    inet6 2001:db8:1::2/32 scope global noprefixroute
       valid_lft forever preferred_lft forever
    inet6 fe80::73d9:6f51:ea6f:863e/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

第 13 章 配置 WEB 控制台侦听端口

了解如何使用 RHEL 9 web 控制台允许新端口或更改现有端口。

13.1. 在带有活跃 SELINUX 的系统中允许一个新端口

启用 Web 控制台以侦听所选端口。

先决条件

- 必须安装并可以访问 Web 控制台。详情请参阅安装 Web 控制台。

流程

- 对于未由 SELinux 其它部分定义的端口，请运行：

```
$ sudo semanage port -a -t websm_port_t -p tcp PORT_NUMBER
```

- 对于已经由 SELinux 其它部分定义的端口，请运行：

```
$ sudo semanage port -m -t websm_port_t -p tcp PORT_NUMBER
```

更改应该会立即生效。

13.2. 使用 FIREWALLD 在系统中允许新端口

启用 Web 控制台在新端口上接收连接。

先决条件

- 必须安装并可以访问 Web 控制台。详情请参阅安装 Web 控制台。
- **firewalld** 服务必须正在运行。

流程

1. 要添加新端口号，请运行以下命令：

```
$ sudo firewall-cmd --permanent --service cockpit --add-port=PORT_NUMBER/tcp
```

2. 要从 **cockpit** 服务中删除旧的端口号，请运行：

```
$ sudo firewall-cmd --permanent --service cockpit --remove-port=OLD_PORT_NUMBER/tcp
```

重要

如果您在没有使用 **--permanent** 选项的情况下运行 **firewall-cmd --service cockpit --add-port=PORT_NUMBER/tcp**，则更改将在下次重新加载 **firewalld** 或系统重启时消失。

13.3. 更改 WEB 控制台端口

将端口 9090 上的默认传输控制协议(TCP)更改为不同的端口。

先决条件

- 必须安装并可以访问 Web 控制台。详情请参阅安装 Web 控制台。
- 启用 SELinux 后，修改策略以允许 Web 控制台侦听新端口。如需更多信息，请参阅在带有活跃 SELinux 的系统上允许一个新端口。
- 使用默认配置中的 **firewalld** 服务，您必须为 Web 控制台打开新端口。如需更多信息，请参阅 在具有 **firewalld** 的系统商允许一个新端口。

流程

1. 使用以下方法之一更改侦听端口：
   a. 使用 **systemctl edit cockpit.socket** 命令：
      i. 输入以下命令：

      ```
      # systemctl edit cockpit.socket
      ```

      这会打开 **/etc/systemd/system/cockpit.socket.d/override.conf** 文件。
      ii. 修改 **override.conf** 的内容，以包含以下配置：

      ```
      [Socket]
      ListenStream=
      ListenStream=PORT_NUMBER
      ```

      ListenStream 选项指定所需的地址和 TCP 端口。

      注意

      具有空值的第一行是有意设计的。**systemd** 允许在单个套接字单元中声明多个 **ListenStream** 指令。置入文件中的空值重置列表，并从原始单元禁用默认端口 9090。

   b. 或者，将前面的套接字配置添加到 **/etc/systemd/system/cockpit.socket.d/listen.conf** 文件中。
   创建 **cockpit.socket.d.** 目录和 **listen.conf** 文件（如果它们尚不存在）。
2. 输入以下命令以使更改生效：

   ```
   # systemctl daemon-reload
   # systemctl restart cockpit.socket
   ```

   如果您在上一步中使用了 **systemctl edit cockpit.socket**，则不需要运行 **systemctl daemon-reload**。

验证步骤

- 要验证更改是否成功，请使用新端口连接 Web 控制台。

第 14 章 使用 WEB 控制台管理防火墙

防火墙是保护机器不受来自外部的、不需要的网络数据影响的一种方式。它允许用户通过定义一组防火墙规则来控制主机上的入站网络流量。这些规则用于对传入流量进行排序，并阻止它或允许它通过。在 RHEL 中，将具有 **nftables** 后端功能的 **firewalld** 服务作为默认防火墙。通过 RHEL web 控制台，您可以配置 **firewalld**。

有关 **firewalld** 服务的详情，请参阅开始使用 firewalld。

14.1. 使用 WEB 控制台运行防火墙

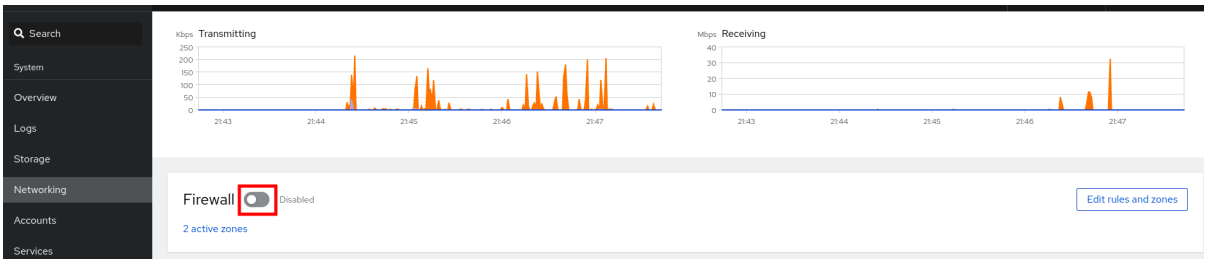
以下步骤演示了在 web 控制台中运行 RHEL 9 系统防火墙的位置和方式。

注意

RHEL 9 web 控制台配置 **firewalld** 服务。

流程

1. 登录到 RHEL 9 web 控制台。详情请参阅 登录到 web 控制台。
2. 打开 **Networking** 部分。
3. 在 **Firewall** 部分，点滑块运行防火墙。



如果没有看到 **Firewall** slider，使用管理权限登录到 web 控制台。

在此阶段，您的防火墙正在运行。

要配置防火墙规则，请参阅使用 Web 控制台在防火墙中启用服务

14.2. 使用 WEB 控制台停止防火墙

以下步骤演示了在 web 控制台中停止 RHEL 9 系统防火墙的位置和方式。

注意

RHEL 9 web 控制台配置 **firewalld** 服务。

流程

1. 登录到 RHEL 9 web 控制台。详情请参阅 登录到 web 控制台。
2. 打开 **Networking** 部分。
3. 在 **Firewall** 部分，点滑块停止防火墙。

如果没有看到 **Firewall** slider，使用管理权限登录到 web 控制台。

在这个阶段，防火墙已经停止，且不会保护您的系统的安全。

14.3. 防火墙区域

您可以使用 **firewalld** 工具根据您与该网络中接口和流量的信任级别将网络划分为不同的区域。连接只能是一个区域的一部分，但您可以对许多网络连接使用这个区域。

firewalld 在区域方面遵循严格的原则：

1. 流量只进入一个区域。
2. 流量只离开一个区域。
3. 一个区域定义一个信任级别。
4. 默认情况下，允许区域内流量（在同一区域中）。
5. 默认情况下，拒绝区域间流量（从区域到区域）。

原则 4 和 5 是原则 3 的结果。

原则 4 可以通过区域选项 **--remove-forward** 进行配置。原则 5 可以通过添加新策略来进行配置。

NetworkManager 通知接口区的 **firewalld**。您可以使用以下工具为接口分配区域：

- **NetworkManager**
- **firewall-config** 工具
- **firewall-cmd** 工具
- RHEL web 控制台

RHEL web 控制台、**firewall-config** 和 **firewall-cmd** 只能编辑合适的 **NetworkManager** 配置文件。如果您使用 web 控制台、**firewall-cmd** 或 **firewall-config** 更改接口的区域，则请求将被转发到 **NetworkManager**，且不会由 **firewalld** 进行处理。

/usr/lib/firewalld/zones/ 目录存储预定义的区域，您可以立即将它们应用到任何可用的网络接口。只有在修改后，这些文件才会被拷贝到 **/etc/firewalld/zones/** 目录中。预定义区的默认设置如下：

block

- 适用于：任何传入的网络连接都会被拒绝，并报 **IPv4** 的 icmp-host-prohibited 消息和 **IPv6** 的 icmp6-adm-prohibited 消息 。
- 接受：只从系统内启动的网络连接。

dmz

- 适用于：DMZ 中的计算机可以公开访问，但对您的内部网络有有限的访问权限。
- 接受：仅所选的传入连接。

drop

适用于：所有传入的网络数据包都会丢失，没有任何通知。

- 接受：仅传出的网络连接。

external

- 适用于：启用了伪装的外部网络，特别是路由器。不信任网络上其他计算机的情况。
- 接受：仅所选的传入连接。

home

- 适用于：您主要信任网络上其他计算机的家庭环境。
- 接受：仅所选的传入连接。

internal

- 适用于：您主要信任网络上其他计算机的内部网络。
- 接受：仅所选的传入连接。

public

- 适用于：您不信任网络上其他计算机的公共区域。
- 接受：仅所选的传入连接。

trusted

- 接受：所有网络连接。

work

适用于：您主要信任网络上其他计算机的工作环境。

- 接受：仅所选的传入连接。

这些区中的一个被设置为 *default* 区。当接口连接被添加到 **NetworkManager** 中时，它们会被分配到默认区。安装时，**firewalld** 中的默认区域是 **public** 区域。您可以更改默认区域。

注意

使网络区域名称自我解释，以帮助用户快速理解它们。

要避免安全问题，请查看默认区配置并根据您的需要和风险禁用任何不必要的服务。

其它资源

- **firewalld.zone(5)** 手册页

14.4. WEB 控制台中的区

Red Hat Enterprise Linux Web 控制台实现 firewalld 服务的主要功能，并可让您：

- 将预定义的防火墙区添加到特定接口或 IP 地址范围
- 在启用的服务列表中配置选择服务的区域
- 通过从已启用的服务列表中删除此服务来禁用服务
- 从接口中删除区

14.5. 使用 WEB 控制台启用区

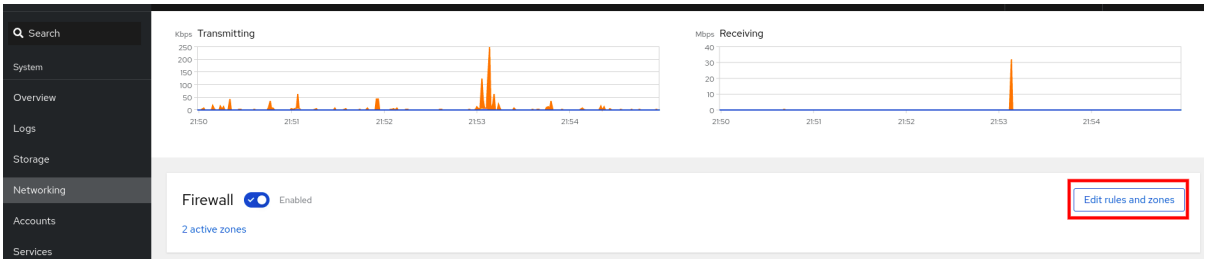
您可以通过 RHEL web 控制台在特定接口或一系列 IP 地址上应用预定义的和现有的防火墙区域。

先决条件

- 已安装 RHEL 9 web 控制台。详情请参阅安装 Web 控制台。
- 必须启用防火墙。详情请参阅使用 Web 控制台运行防火墙。

流程

1. 使用管理权限登录到 RHEL web 控制台。详情请参阅 登录到 web 控制台。
2. 点 **Networking**。
3. 点**编辑规则和区域**按钮。

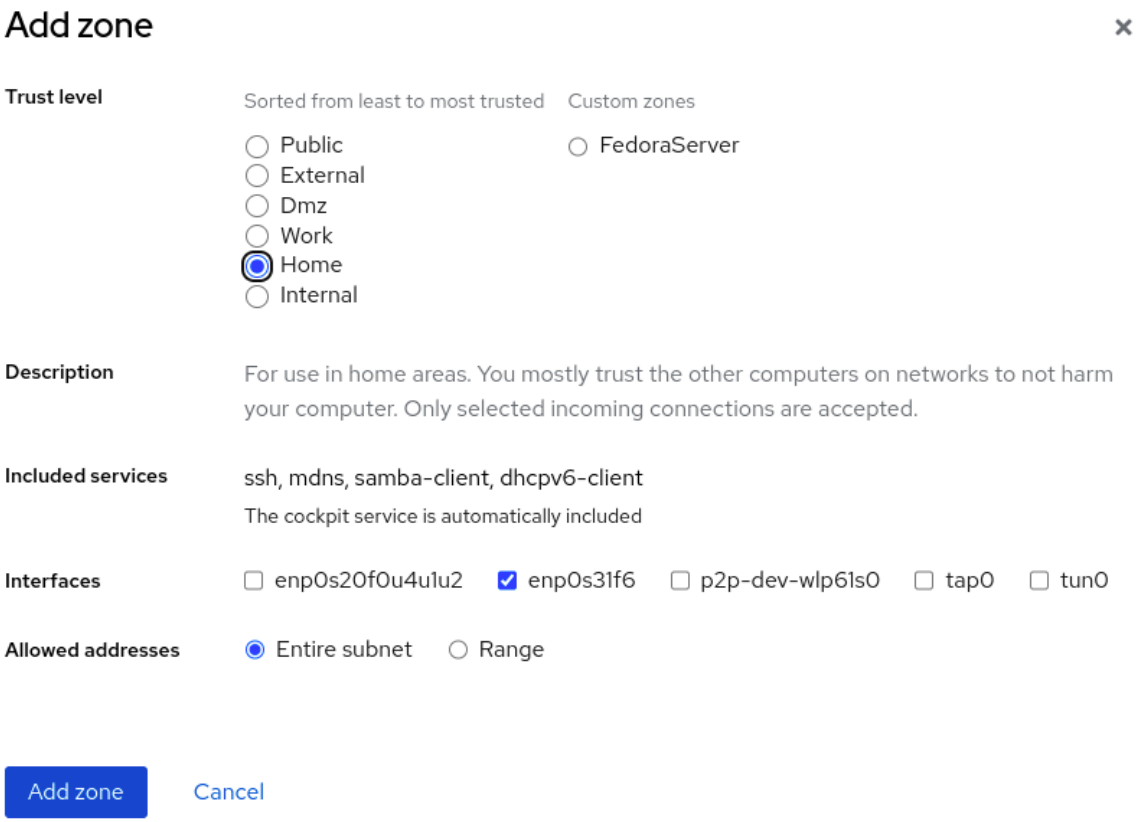


如果没有看到 **Edit rules and zones** 按钮，使用管理员权限登录到 web 控制台。

4. 在 **Firewall** 部分，点 **Add new zone**。
5. 在 **Add zone** 对话框中，从**信任级别**选项选择一个区。
Web 控制台显示 **firewalld** 服务中预定义的所有区域。
6. 在**接口**部分，选择一个应用所选区的接口或接口。
7. 在 **Allowed Addresses** 部分中，您可以选择是否应用该区：
   - 整个子网
   - 或者以以下格式表示的 IP 地址范围：
     - 192.168.1.0

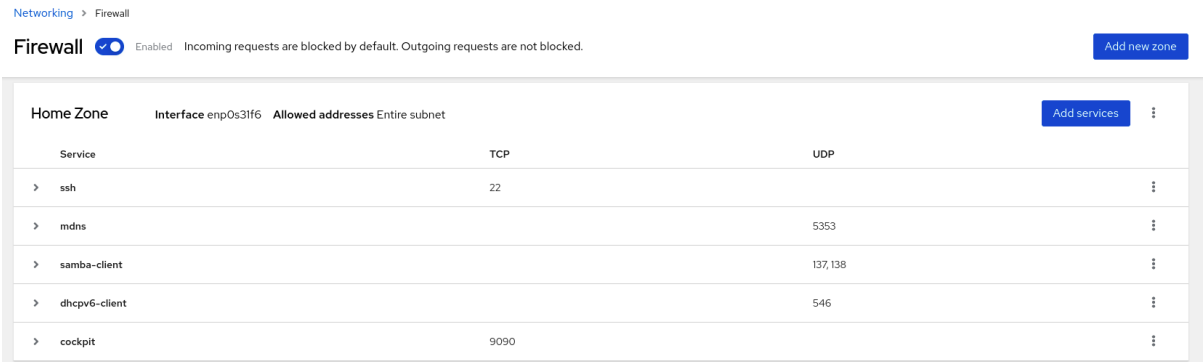
- 192.168.1.0/24
- 192.168.1.0/24, 192.168.1.0

8. 点 **Add zone** 按钮。



验证

- 检查 **Firewall** 部分中的配置：



14.6. 使用 WEB 控制台在防火墙中启用服务

默认情况下，服务添加到默认防火墙区。如果在更多网络接口中使用更多防火墙区，您必须首先选择一个区域，然后添加带有端口的服务。

RHEL 9 web 控制台显示预定义的 **firewalld** 服务，您可以将其添加到活跃的防火墙区。

重要

RHEL 9 web 控制台配置 **firewalld** 服务。

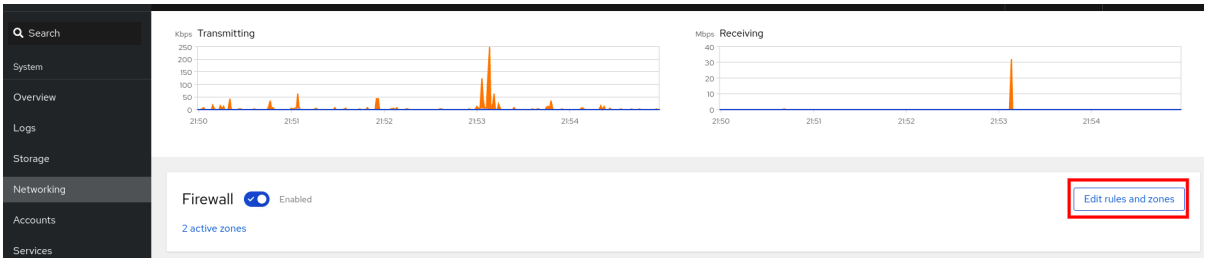
Web 控制台不允许没有在 web 控制台中列出的通用 **firewalld** 规则。

先决条件

- 已安装 RHEL 9 web 控制台。详情请参阅安装 Web 控制台。
- 必须启用防火墙。详情请参阅使用 Web 控制台运行防火墙。

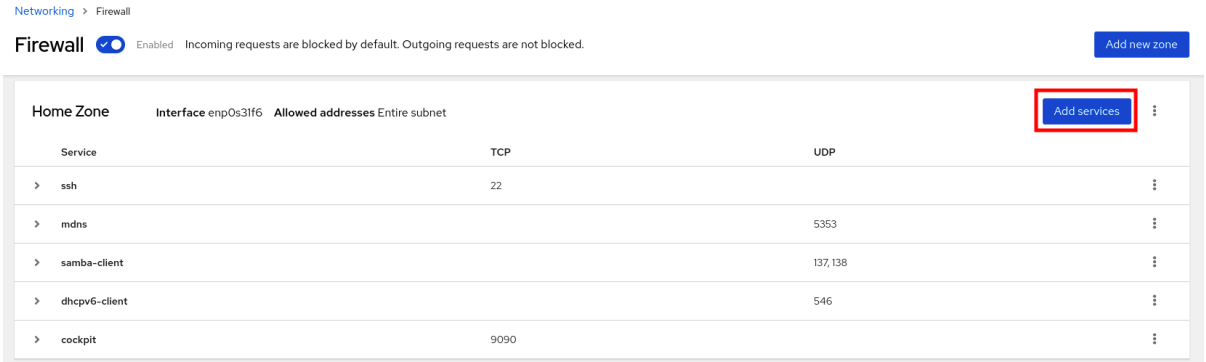
流程

1. 使用管理员权限登录到 RHEL web 控制台。详情请参阅 登录到 web 控制台。
2. 点 **Networking**。
3. 点**编辑规则和区域**按钮。

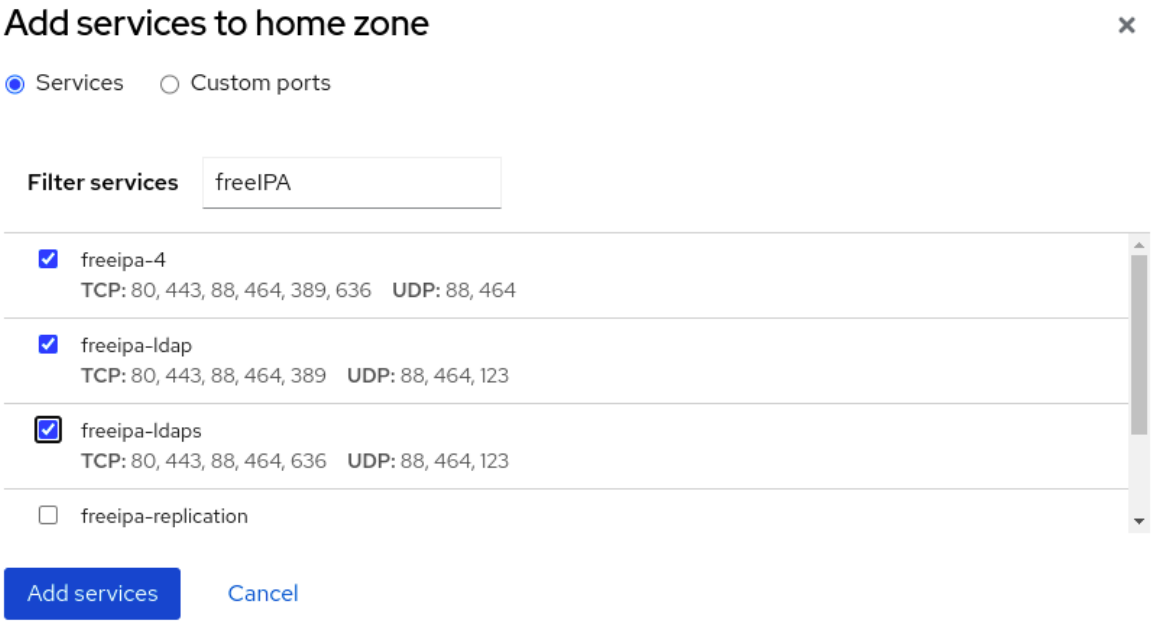


如果没有看到 **Edit rules and zones** 按钮，使用管理员权限登录到 web 控制台。

4. 在 **Firewall** 部分，选择要添加该服务的区，然后点击 **Add Services**。



5. 在 **Add Services** 对话框中，找到您要在防火墙中启用的服务。
6. 根据您的场景启用服务：



7. 点 **Add Services**。

此时，RHEL 9 web 控制台在区域的**服务**列表中显示该服务。

14.7. 使用 WEB 控制台配置自定义端口

Web 控制台允许您添加：

- 服务侦听标准端口：使用 Web 控制台在防火墙中启用服务
- 服务侦听自定义端口。

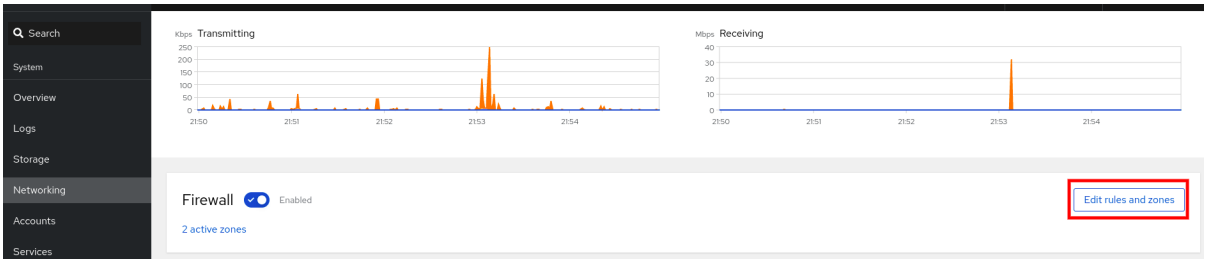
您可以通过配置自定义端口来添加服务，如下所述。

先决条件

- 已安装 RHEL 9 web 控制台。详情请参阅安装 Web 控制台。
- 必须启用防火墙。详情请参阅使用 Web 控制台运行防火墙。

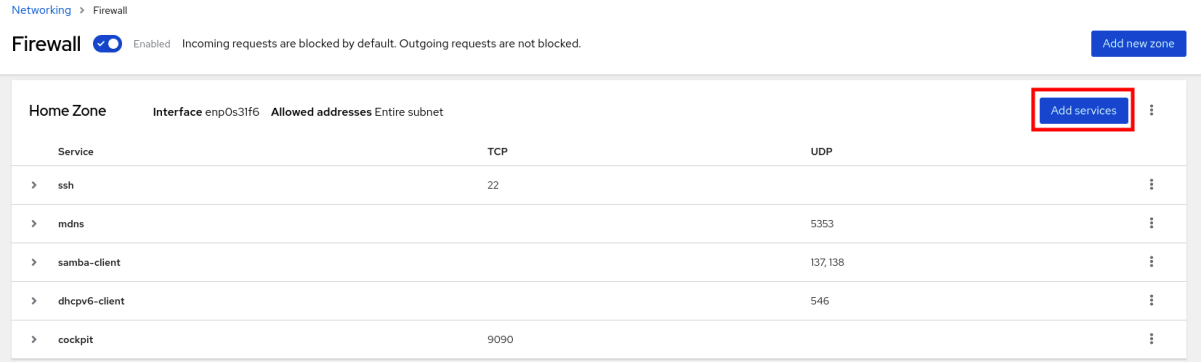
流程

1. 使用管理员权限登录到 RHEL web 控制台。详情请参阅 登录到 web 控制台。
2. 点 **Networking**。
3. 点**编辑规则和区域**按钮。



如果没有看到 **Edit rules and zones** 按钮，使用管理员权限登录到 web 控制台。

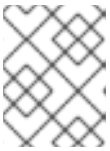
4. 在 **Firewall** 部分，选择要配置自定义端口的区域，并点 **Add Services**。



5. 在 **Add services** 对话框中，点 **Custom Ports** 单选按钮。

6. 在 TCP 和 UDP 字段中，根据示例添加端口。您可以使用以下格式添加端口：

   - 端口号，如 22
   - 端口号范围，如 5900-5910
   - 别名，比如 nfs, rsync



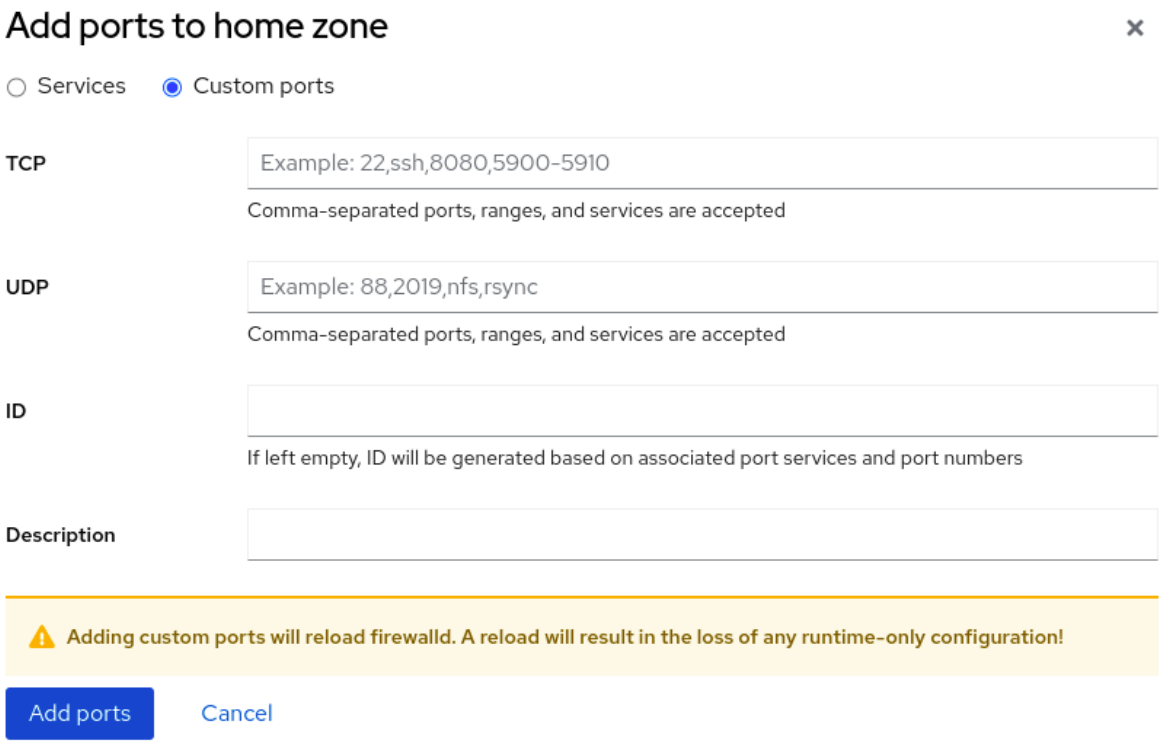
注意

您可以在每个字段中添加多个值。值必须用逗号分开，且没有空格，例如：8080,8081,http

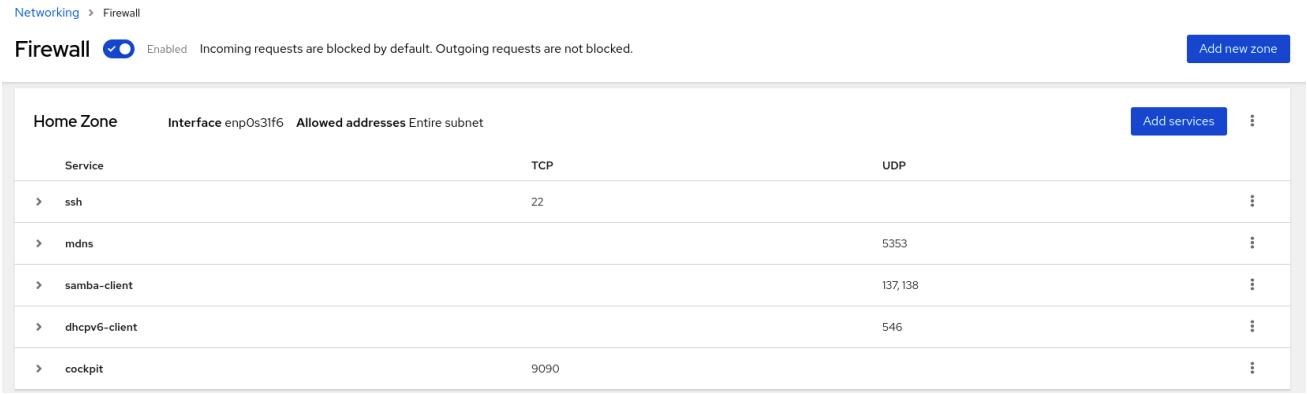
7. 在 **TCP** 文件、**UDP** 文件或两者中添加端口号后，在 **Name** 字段中验证服务名称。**Name** 字段显示保留此端口的服务名称。如果您确定这个端口可用，且不需要在该端口上通信，则可以重写名称。

8. 在 **Name** 字段中，为服务添加一个名称，包括定义的端口。

9. 点**添加端口**按钮。



要验证设置，请进入**防火墙**页面，并在区域的**服务**列表中找到该服务。



14.8. 使用 WEB 控制台禁用区

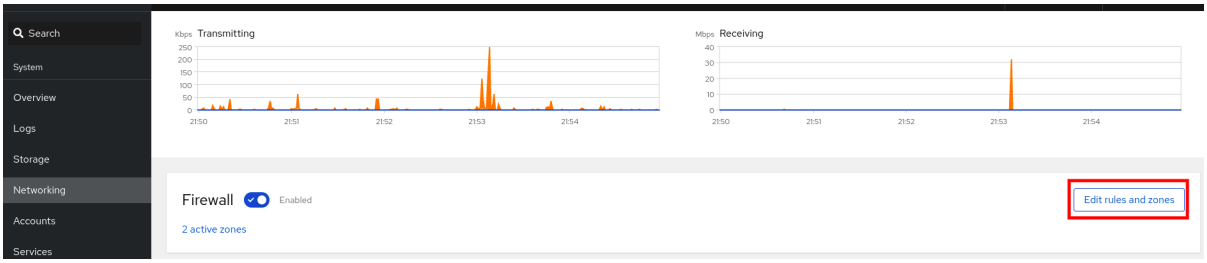
您可以使用 Web 控制台在防火墙配置中禁用防火墙区域。

先决条件

- 已安装 RHEL 9 web 控制台。详情请参阅安装 Web 控制台。

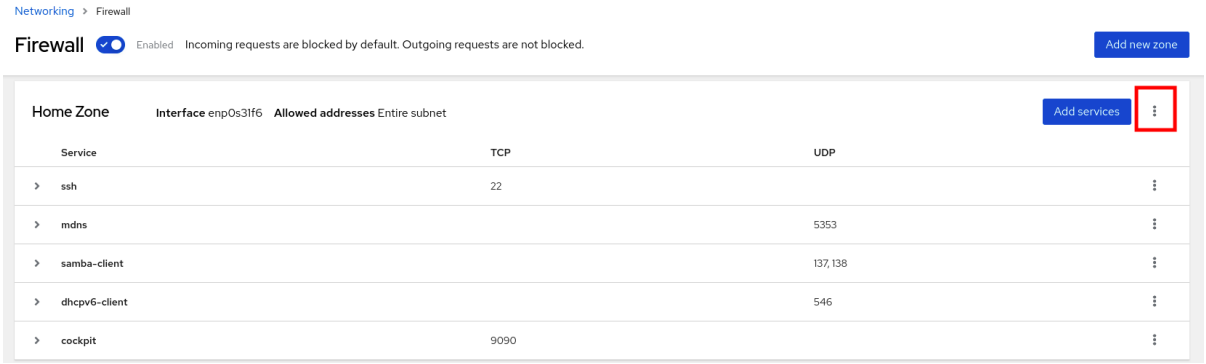
流程

1. 使用管理员权限登录到 RHEL web 控制台。详情请参阅 登录到 web 控制台。
2. 点 **Networking**。
3. 点**编辑规则和区域**按钮。



如果没有看到 **Edit rules and zones** 按钮，使用管理员权限登录到 web 控制台。

4. 点您要删除的区的 **Options** 图标。



5. 点击 **Delete**。

区域现在被禁用，接口不包括在区域中配置的打开的服务和端口。

第 15 章 在 WEB 控制台中设置系统范围的加密策略

您可以在 RHEL web 控制台界面中直接设置系统范围的加密策略和子策略。除了四个预定义的系统范围的加密策略外，您现在还可以通过图形界面应用以下策略和子策略的组合：

DEFAULT:SHA1

启用了 **SHA-1** 算法的 **DEFAULT** 策略。

LEGACY:AD-SUPPORT

带有不太安全设置的 **LEGACY** 策略，提高了活动目录服务的互操作性。

FIPS:OSPP

信息安全评估标准的通用标准所需的具有进一步限制的 **FIPS** 策略。

警告

因为 **FIPS:OSPP** 系统范围的子策略包含对通用标准(CC)认证所需的加密算法的进一步限制，因此设置后系统的互操作性较差。例如，您无法使用少于 3072 位的 RSA 和 DH 密钥、其它 SSH 算法和几个 TLS 组。设置 **FIPS:OSPP** 也会阻止连接到 Red Hat Content Delivery Network (CDN)结构。另外，您无法将活动目录(AD)集成到使用 **FIPS:OSPP**的 IdM 部署中，使用 **FIPS:OSPP** 的 RHEL 主机和 AD 域之间的通信可能无法工作，或者某些 AD 帐户可能无法进行身份验证。

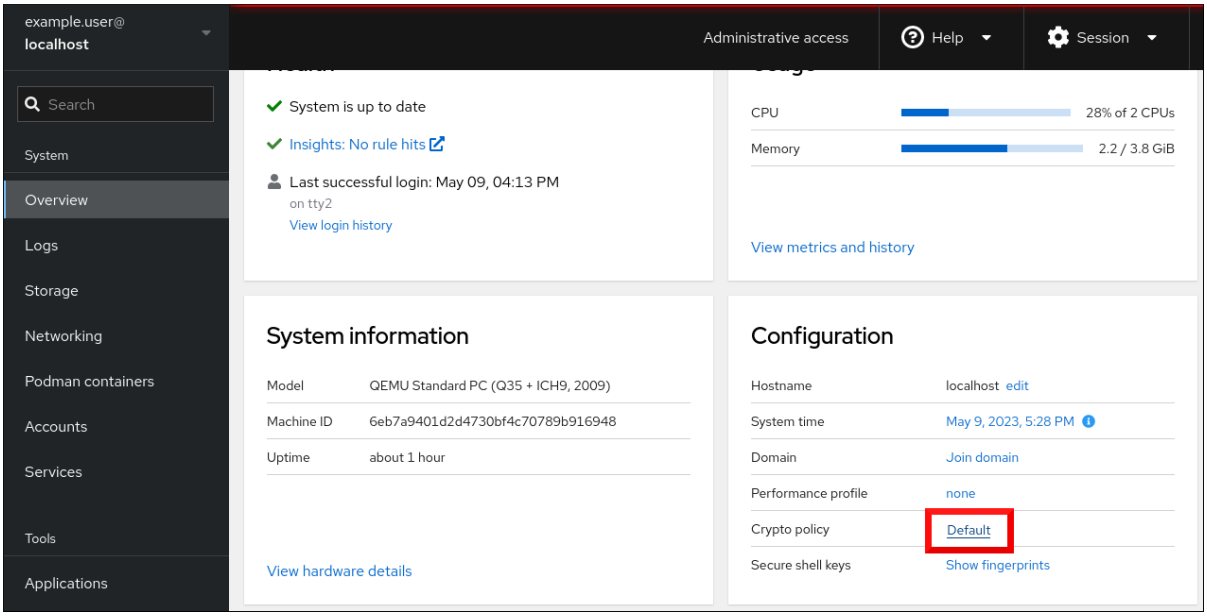
请注意，在设置了 **FIPS:OSPP** 加密子策略后，您的 **系统不符合 CC**。使 RHEL 系统符合 CC 标准的唯一正确方法是安装 **cc-config** 软件包。有关认证的 RHEL 版本的列表、验证报告以及 CC 指南的链接，请参阅 国家信息保障合作伙伴(NIAP) 网站上托管的合规性活动和政府标准知识库文章里的 通用标准 部分。

先决条件

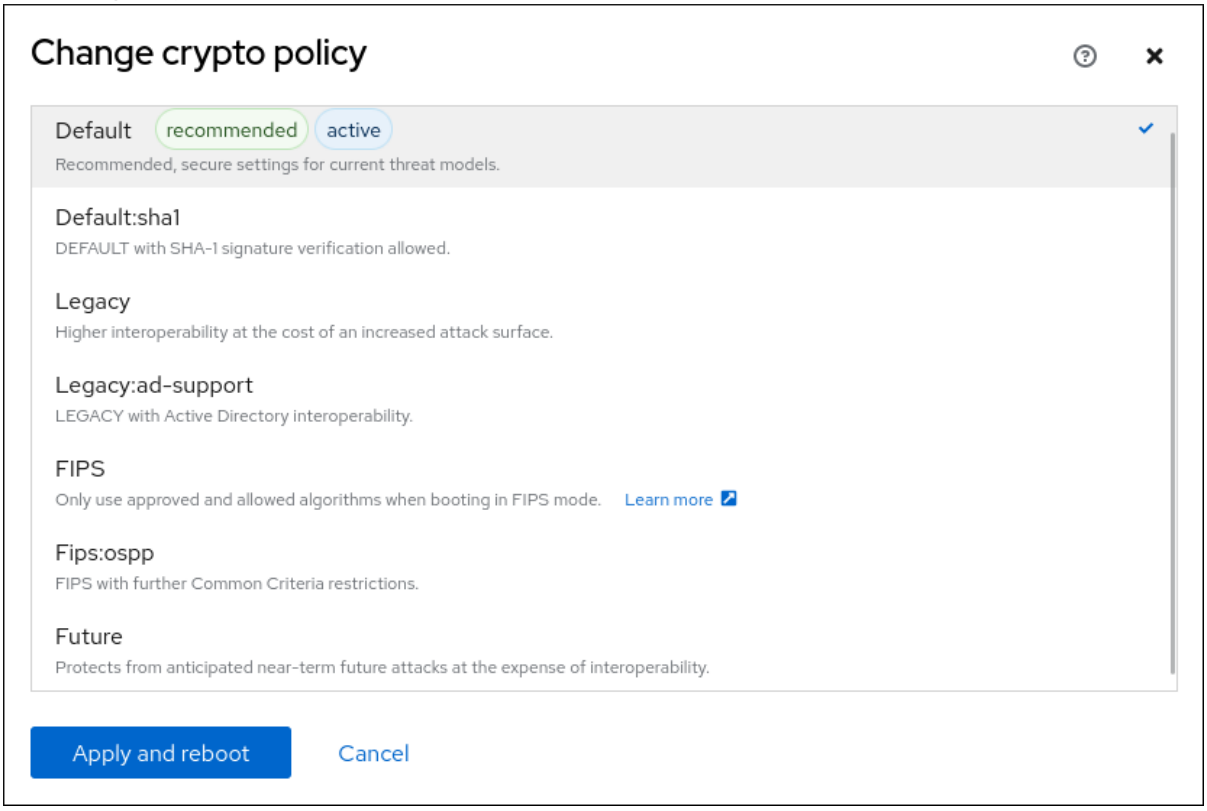
- 已安装 RHEL 9 web 控制台。详情请参阅安装和启用 Web 控制台。
- 您有 **root** 特权或权限来使用 **sudo** 输入管理命令的命令。

流程

1. 登录到 web 控制台。如需更多信息，请参阅 Web 控制台的日志记录。
2. 在 **Overview** 页面的 **Configuration** 卡中，点 **Crypto 策略**旁的当前策略值。



3. 在 **Change crypto policy** 对话框窗口中，点您要在系统上开始使用的策略。



4. 点应**用并重新引**导按钮。

验证

- 重启后，重新登录到 web 控制台，并检查 **Crypto policy** 值是否与您选择的策略值对应。或者，您可以输入 **update-crypto-policies --show** 命令来在终端中显示当前系统范围的加密策略。

其它资源

- 有关每个加密策略的详情，请参考安全强化文档中的 系统范围的加密策略 部分。

第 16 章 在 WEB 控制台中创建一个 SELINUX 配置 ANSIBLE PLAYBOOK

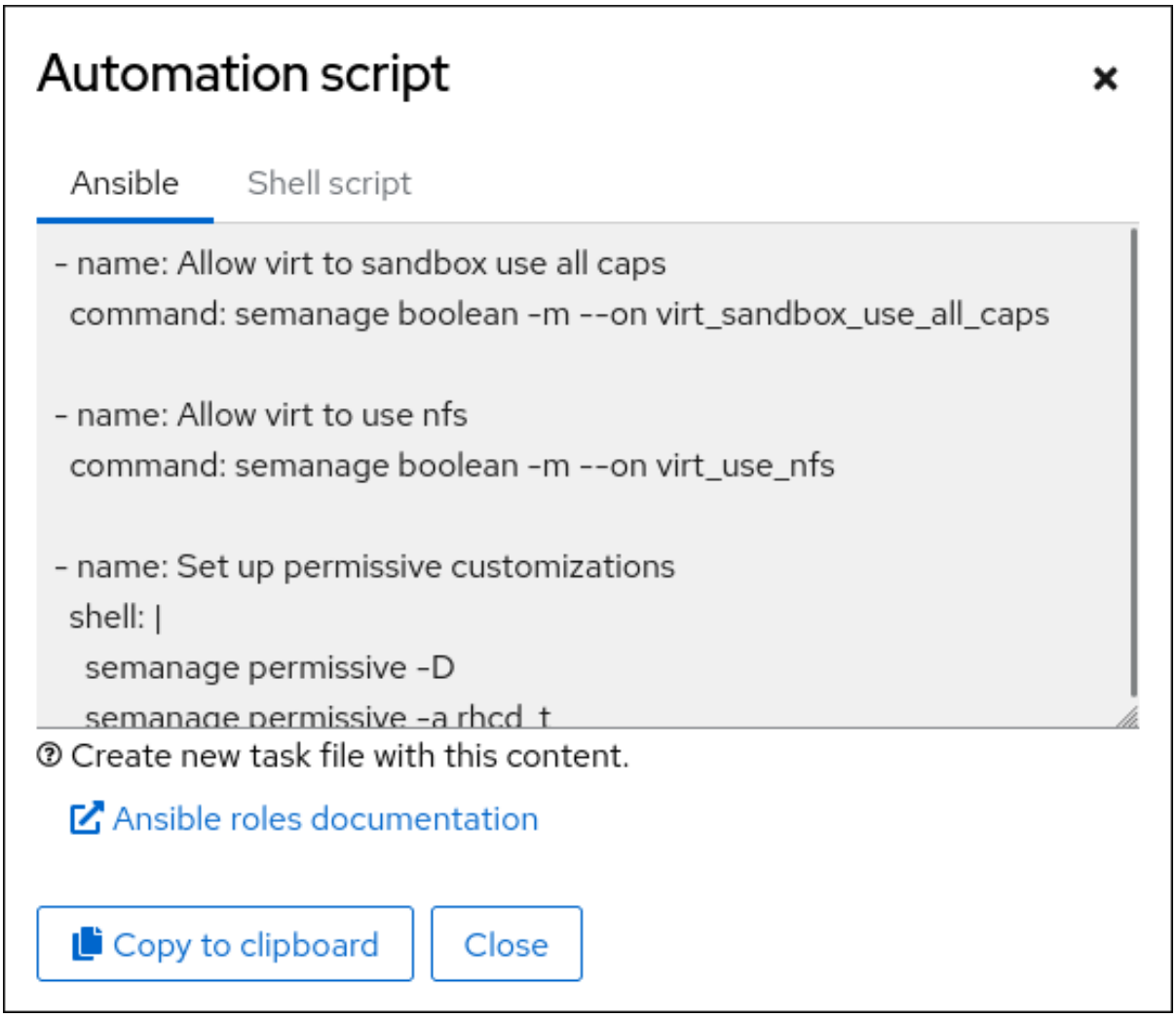
在 Web 控制台中，您可以生成一个 shell 脚本或一个 SELinux 配置的 Ansible playbook。如果是 Ansible playbook，您可以在多个系统上方便地应用配置。

先决条件

- 必须安装并可以访问 Web 控制台。
  详情请参阅安装 Web 控制台。

流程

1. 点 **SELinux**。
2. 点 **View the automation script**。
   此时会打开一个带有生成的脚本的窗口。您可以在 shell 脚本页和 Ansible playbook 生成选项页之间转换。



3. 点 **Copy to clipboard** 按钮选择脚本或 playbook 并应用它。

因此，您有一个可应用到更多机器的自动脚本。

其它资源

- 故障排除与 SELinux 相关的问题
- 在多个系统中部署相同的 SELinux 配置
- **ansible-playbook(1)** 手册页

第 17 章 使用 WEB 控制台管理分区

了解如何使用 web 控制台管理 RHEL 9 上的文件系统。

有关可用文件系统的详情，请查看可用文件系统概述。

17.1. 在 WEB 控制台中显示使用文件系统格式化的分区

Web 控制台中的 **Storage** 部分会在 **Filesystems** 表中显示所有可用文件系统。

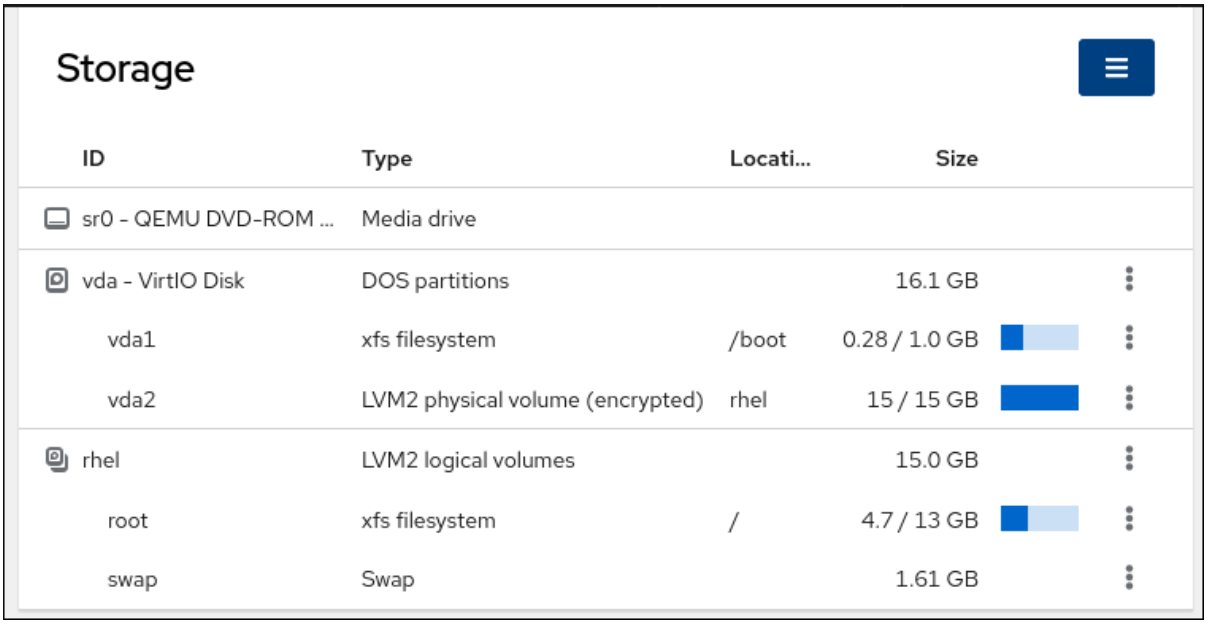
除了使用文件系统格式化的分区的列表外，您还可以使用页来创建新存储。

先决条件

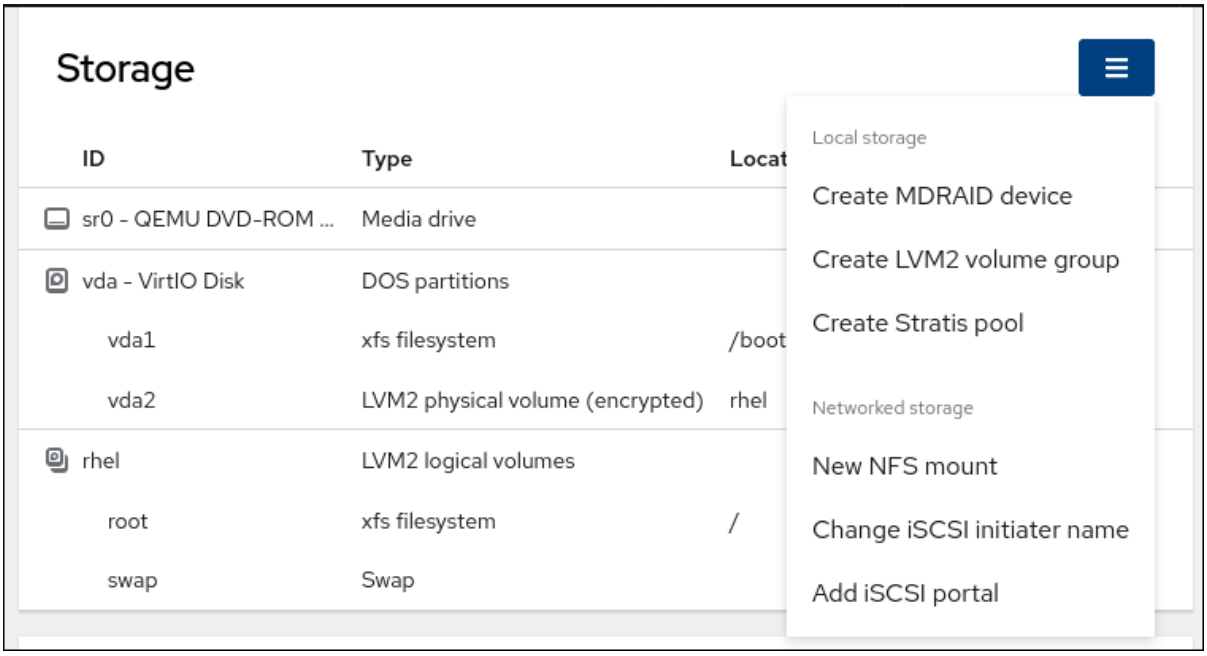
- **cockpit-storaged** 软件包已安装在您的系统上。
- 必须安装并可以访问 Web 控制台。详情请参阅安装 Web 控制台。

流程

1. 登录到 RHEL 9 web 控制台。详情请参阅 登录到 web 控制台。
2. 点 **Storage** 选项卡。
   在 **Storage** 表中，您可以看到使用文件系统格式化的所有可用分区、其 ID、类型、位置、大小以及每个分区中有多少可用空间。



   您还可以使用右上角的下拉菜单来创建新的本地或网络存储。



17.2. 在 WEB 控制台中创建分区

创建新分区：

- 使用现有的分区表
- 创建分区

先决条件

- **cockpit-storaged** 软件包已安装在您的系统上。
- 必须安装并可以访问 Web 控制台。详情请参阅安装 Web 控制台。
- 在 **Storage** 选项卡的 **Storage** 表中可以看到一个连接到系统的未格式化的卷。

流程

1. 登录到 RHEL web 控制台。详情请参阅 登录到 web 控制台。
2. 点 **Storage** 选项卡。
3. 在 **Storage** 表中，点您要进行分区的设备，以打开用于该设备的页和选项。
4. 在设备页面中，点菜单按钮 ⋮，然后选择 **Create partition table**。
5. 在 **Initialize disk** 对话框中选择以下内容：
   a. **Partitioning** ：
      - 与所有系统和设备兼容(MBR)
      - 与现代系统和硬盘 > 2TB 兼容(GPT)
      - 没有分区
   b. **Overwrite** ：

- 如果您希望 RHEL web 控制台使用零重写整个磁盘，请选择 **Overwrite existing data with zeros** 复选框。使用这个选项较慢，因为程序必须经过整个磁盘，但它更为安全。如果磁盘包含任何数据且需要覆盖数据，则使用这个选项。
  如果您没有选择 **Overwrite existing data with zeros** 复选框，RHEL web 控制台只重写磁盘头。这提高了格式化速度。

6. 单击 **Initialize**。
7. 点您创建的分区表旁边的菜单按钮 ⋮。默认情况下，它被命名为 **Free space**。
8. 点 **Create partition**。
9. 在 **Create partition** 对话框中输入文件系统 **名称**。
10. 添加 **Mount point**。
11. 在 **Type** 下拉菜单中选择一个文件系统：
    - **XFS** 文件系统支持大的逻辑卷，在不停止工作的情况下在线切换物理驱动器，并可以增大现有的文件系统。如果您没有不同的首选项，请保留这个文件系统。
    - **ext4** 文件系统支持：
      - 逻辑卷
      - 在不停止工作的情况下在线切换物理驱动器
      - 增大文件系统
      - 缩小文件系统

    额外的选项是启用 LUKS（Linux 统一密钥设置）完成的分区加密，该加密可让您使用密码短语加密卷。
12. 输入您要创建的卷的 **大小**。
13. 如果您希望 RHEL web 控制台使用零重写整个磁盘，请选择 **Overwrite existing data with zeros** 复选框。使用这个选项较慢，因为程序必须经过整个磁盘，但它更为安全。如果磁盘包含任何数据且需要覆盖数据，则使用这个选项。
    如果您没有选择 **Overwrite existing data with zeros** 复选框，RHEL web 控制台只重写磁盘头。这提高了格式化速度。
14. 如果要加密卷，请在 **Encryption** 下拉菜单中选择加密类型。
    如果您不想加密卷，请选择 **No encryption**。
15. 在 **At boot** 下拉菜单中选择您要何时挂载卷。
16. 在 **Mount options** 部分中：
    a. 如果您希望将卷挂载为只读逻辑卷，请选择 **Mount read only** 复选框。
    b. 选择 **Custom mount options** 复选框，如果您要更改默认挂载选项，请添加挂载选项。
17. 创建分区：
    - 如果要创建并挂载分区，请点 **Create and mount** 按钮。
    - 如果您只想创建分区，点 **Create only** 按钮。

根据卷大小以及选择格式化选项，格式化可能需要几分钟。

验证步骤

- 要验证分区是否已成功添加，请切换到 **Storage** 选项卡，并检查 **Storage** 表，并验证是否列出了新分区。

17.3. 在 WEB 控制台中删除分区

您可以在 web 控制台界面中删除分区。

先决条件

- **cockpit-storaged** 软件包已安装在您的系统上。
- 必须安装并可以访问 Web 控制台。详情请参阅安装 Web 控制台。

步骤

1. 登录到 RHEL web 控制台。详情请参阅 登录到 web 控制台。
2. 点 **Storage** 选项卡。
3. 点击您要从中删除分区的设备。
4. 在设备页和 **GPT partitions** 部分中，点您要删除的分区旁的菜单按钮 ⋮。
5. 从下拉菜单中选择 **Delete**。
   RHEL web 控制台终止所有当前使用分区的进程，并在删除分区前卸载分区。

验证步骤

- 要验证分区是否已成功删除，请切换到 **Storage** 选项卡，并检查 **Storage** 表。

17.4. 在 WEB 控制台中挂载和卸载文件系统

为了能够在 RHEL 系统中使用分区，您需要在分区中作为一个设备挂载文件系统。

注意

您还可以卸载文件系统，RHEL 系统将会停止使用它。卸载文件系统可让您删除、删除或重新格式化设备。

先决条件

- **cockpit-storaged** 软件包已安装在您的系统上。
- 必须安装并可以访问 Web 控制台。详情请参阅安装 Web 控制台。
- 如果要卸载文件系统，请确保系统没有使用存储在分区中的任何文件、服务或应用程序。

步骤

1. 登录到 RHEL web 控制台。详情请参阅 登录到 web 控制台。

2. 点 **Storage** 选项卡。
3. 在 **Storage** 表中，选择您要从中删除分区的卷。
4. 在 **GPT partitions** 部分中，点击您要挂载或卸载其文件系统的分区旁边的菜单按钮 ⋮。
5. 点 **Mount** 或 **Unmount**。

第 18 章 在 WEB 控制台中管理 NFS 挂载

RHEL 9 web 控制台允许您使用网络文件系统(NFS)协议挂载远程目录。

NFS 使可以访问并挂载位于网络上的远程目录，并像位于物理驱动器上一样处理文件。

先决条件

- 已安装 RHEL 9 web 控制台。
  详情请参阅安装 Web 控制台。
- **cockpit-storaged** 软件包已安装在您的系统上。
- NFS 服务器名称或 IP 地址。
- 到远程服务器中的目录的路径。

18.1. 在 WEB 控制台中连接 NFS 挂载

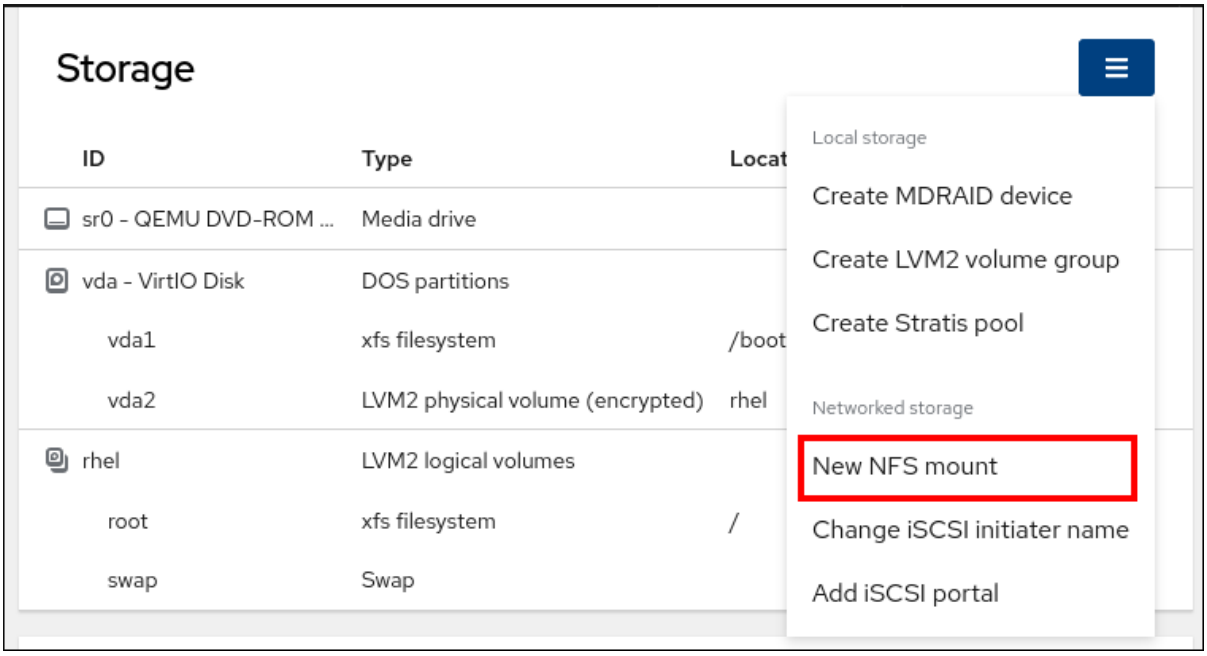
使用 NFS 将远程目录连接到文件系统。

先决条件

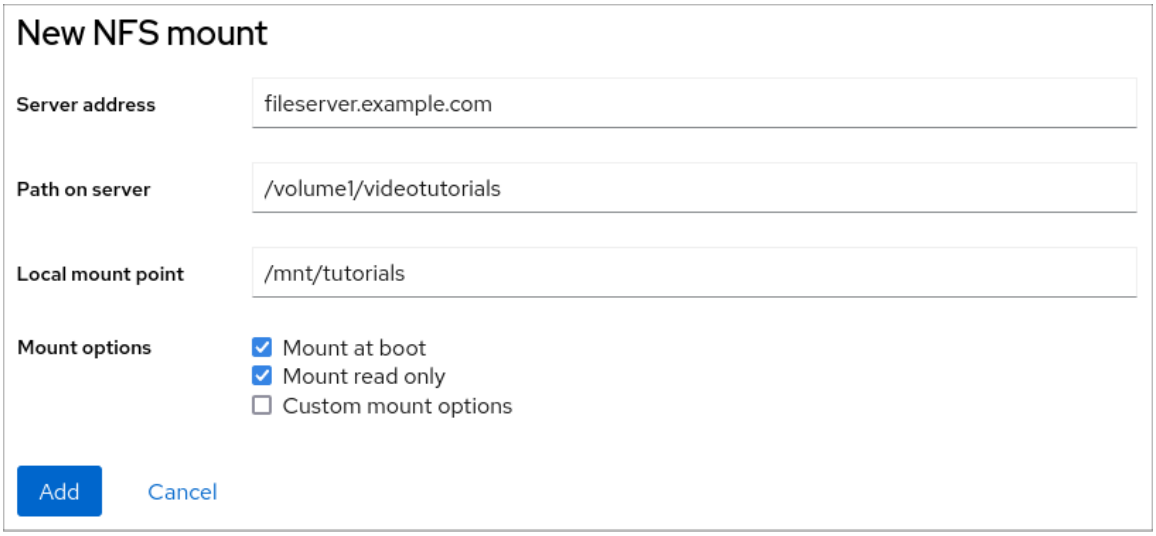
- NFS 服务器名称或 IP 地址。
- 到远程服务器中的目录的路径。

流程

1. 登录到 RHEL 9 web 控制台。详情请参阅 登录到 web 控制台。
2. 点击 **Storage**。
3. 在 **Storage** 表中，点菜单按钮。
4. 从下拉菜单中选择 **New NFS mount**。



5. 在**新建 NFS Mount**对话框中输入远程服务器的服务器或者 IP 地址。
6. 在 **Path on Server**字段中，输入您要挂载的目录的路径。
7. 在 **Local Mount Point** 字段中输入您要在本地系统上挂载 NFS 的目录的路径。
8. 在 **Mount options** 复选框列表中，选择如何挂载 NFS。您可以根据要求选择多个选项。
   - 如果您希望在重启本地系统后仍然可以访问目录，请选中 **Mount at boot** 框。
   - 如果您不想更改 NFS 的内容，请选中 **Mount read only** 框。
   - 选中 **Custom mount options** 框，如果您要更改默认挂载选项，请添加挂载选项。如需更多信息，请参阅 在 web 控制台中自定义 NFS 挂载选项。



9. 点击 **Add**。

验证步骤

- 打开挂载的目录，并验证内容可以访问。

18.2. 在 WEB 控制台中自定义 NFS 挂载选项

编辑现有 NFS 挂载并添加自定义挂载选项。

自定义挂载选项可帮助您排除 NFS 挂载的连接或更改参数，如更改超时限制或配置验证。

先决条件

- NFS 挂载被添加到您的系统上。

流程

1. 登录到 RHEL 9 web 控制台。详情请参阅 登录到 web 控制台。
2. 点击 **Storage**。
3. 在 **Storage** 表中，点您要调整的 NFS 挂载。
4. 如果挂载了远程目录，点 **Unmount**。

您必须在自定义挂载选项配置过程中卸载目录。否则，Web 控制台不会保存配置，这会导致错误。

5. 点 **Edit**。
6. 在 **NFS Mount** 对话框中，选择**自定义挂载选项**。
7. 输入用逗号分开的挂载选项。例如：
   - **nfsvers=4**:NFS 协议版本号
   - **soft** ：NFS 请求超时后恢复的类型
   - **sec=krb5**:NFS 服务器上的文件可以通过 Kerberos 身份验证进行保护。NFS 客户端和服务器都必须支持 Kerberos 验证。

   如需 NFS 挂载选项的完整列表，请在命令行中输入 **man nfs**。
8. 点**应用**。
9. 点 **Mount**。

验证步骤

- 打开挂载的目录，并验证内容可以访问。

第 19 章 在 WEB 控制台中管理 RAID

Redundant Arrays of Independent Disks (RAID) 表示一种如何将多个磁盘安排到一个存储中，以实现性能和冗余目标的方法。

RAID 使用以下数据发布策略：

- 镜像 - 数据被复制到两个不同的位置。如果一个磁盘失败，因为您有一个副本，就不会丢失数据。
- 条带 - 数据在磁盘间平均分布。

保护级别取决于 RAID 级别。

RHEL web 控制台支持以下 RAID 级别：

- RAID 0（条带）
- RAID 1（镜像）
- RAID 4（专用奇偶校验）
- RAID 5（分布奇偶校验）
- RAID 6（双倍分布奇偶校验）
- RAID 10（镜像的条带）

在使用 RAID 中的磁盘前，您必须：

- 创建 RAID。
- 使用文件系统格式化它。
- 将 RAID 挂载到系统。

先决条件

- RHEL 9 web 控制台已安装并可以访问。详情请参阅安装 Web 控制台。
- **cockpit-storaged** 软件包已安装在您的系统上。

19.1. 在 WEB 控制台中创建 RAID

在 RHEL 9 web 控制台中配置 RAID。

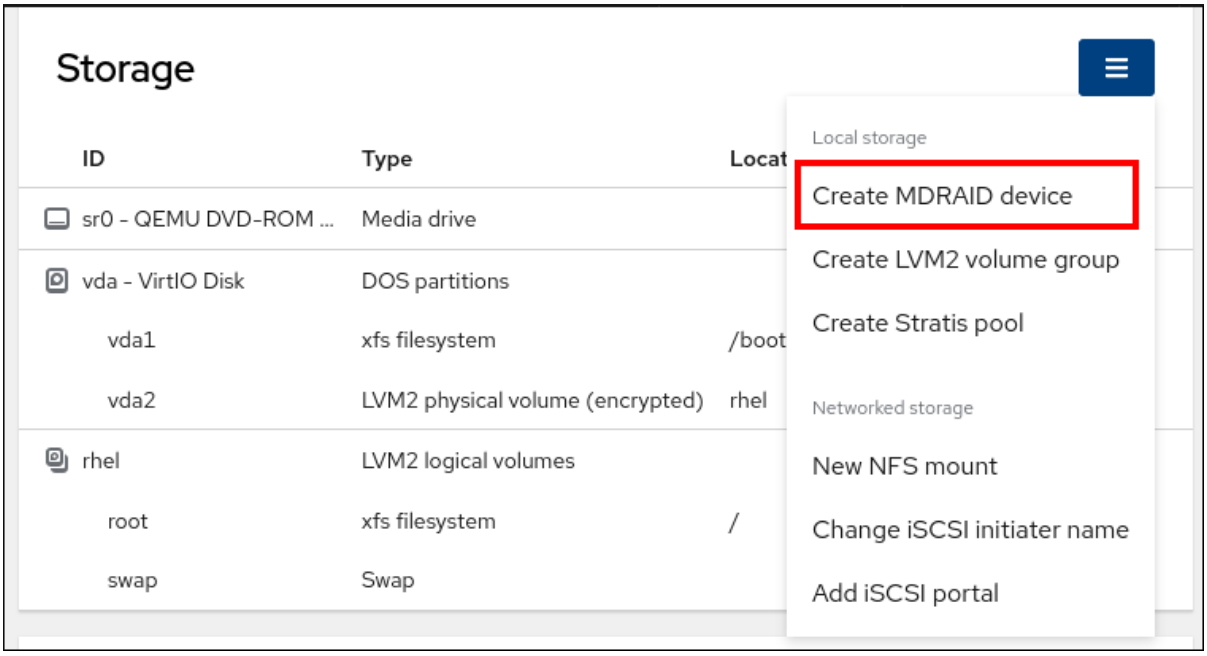
先决条件

- 连接到该系统的物理磁盘。每个 RAID 级别都需要不同的磁盘。

流程

1. 打开 RHEL 9 web 控制台。
2. 点击 **Storage**。

3. 在 **Storage** 表中，点菜单按钮。
4. 从下拉菜单中选择 **Create MDRAID device**。



5. 在 **Create RAID Device** 对话框中，为新 RAID 输入一个名称。
6. 在 **RAID 级别**下拉列表中，选择您要使用的 RAID 级别。
7. 在 **Chunk Size** 下拉列表中，从可用选项列表中选择大小。
   Chunk Size 值指定用于写数据的每个块有多大。例如，如果块大小为 512 KiB，系统将把第一个 512 KiB 写入第一个磁盘中，第二个 512 KiB 将被写入第二个磁盘中，第三个块将被写入第三个磁盘中。如果您的 RAID 中有三个磁盘，则第四个 512 KiB 被再次写入第一个磁盘中。
8. 选择您要用于 RAID 的磁盘。
9. 点击 **Create**。

验证步骤

- 进到 **Storage** 部分，并在 **RAID devices** 框中选中您可以看到的新 RAID。
  您在 web 控制台中有以下格式化和挂载新 RAID 的选项：
  - Formatting RAID
  - Creating partitions on the partition table
  - Creating a volume group on top of the RAID

19.2. 在 WEB 控制台中格式化 RAID

您可以在 RHEL 9 web 控制台中格式化和挂载软件 RAID 设备。

先决条件

- RHEL 9 已连接并看到物理磁盘。
- 创建 RAID。

- 考虑用于 RAID 的文件系统。
- 考虑创建一个分区表。

流程

1. 打开 RHEL 9 web 控制台。
2. 点击 **Storage**。
3. 在 **Storage** 表中，点击您要格式化的 RAID 设备旁边的菜单按钮 ⋮。
4. 从下拉菜单中选择 **Format**。
5. 在 **Format** 对话框中输入名称。
6. 在 **Mount Point** 字段中添加挂载路径。
7. 从 **Type** 下拉列表中选择文件系统的类型。
8. 如果您希望 RHEL web 控制台使用零重写整个磁盘，请选择 **Overwrite existing data with zeros** 复选框。使用这个选项较慢，因为程序必须经过整个磁盘，但它更为安全。如果磁盘包含任何数据且需要覆盖数据，则使用这个选项。
   如果您没有选择 **Overwrite existing data with zeros** 复选框，RHEL web 控制台只重写磁盘头。这提高了格式化速度。
9. 如果要加密卷，请从 **Encryption** 下拉菜单中选择加密的类型。
   如果您不想加密卷，请选择 **No encryption**。
10. 在 **At boot** 下拉菜单中选择您要何时挂载卷。
11. 在 **Mount options** 部分中：
    a. 如果您希望将卷挂载为只读逻辑卷，请选择 **Mount read only** 复选框。
    b. 选择 **Custom mount options** 复选框，如果您要更改默认挂载选项，请添加挂载选项。如需更多信息，请参阅 在 web 控制台中自定义 NFS 挂载选项。
12. 格式化 RAID 分区：
    - 如果要格式化并挂载分区，请点 **Format and mount** 按钮。
    - 如果您只想格式化分区，请点 **Format only** 按钮。
      根据卷大小以及选择格式化选项，格式化可能需要几分钟。

验证

- 格式化成功完成后，您可以在 **Storage** 页的 **Storage** 表中看到格式化逻辑卷的详情。

19.3. 使用 WEB 控制台在 RAID 上创建分区表

在 RHEL 9 接口中创建的新软件 RAID 设备中使用分区表格式化 RAID。

与任何其他存储设备一样，RAID 也需要格式化。您有两个选项：

- 格式化没有分区的 RAID 设备

- 创建带有分区的分区表

先决条件

- 物理磁盘已连接并可见。
- 创建 RAID。
- 考虑用于 RAID 的文件系统。
- 考虑创建一个分区表。

流程

1. 打开 RHEL 9 控制台。
2. 点击 **Storage**。
3. 在 **Storage** 表中，点您要在其上创建分区表的 RAID 设备。
4. 点 **MDRAID device** 部分中的菜单按钮 ⋮。
5. 从下拉菜单中选择 **Create partition table**。
6. 在 **Initialize disk** 对话框中选择以下内容：
   a. **Partitioning** ：
      - 与所有系统和设备兼容(MBR)
      - 与现代系统和硬盘 > 2TB 兼容(GPT)
      - 没有分区
   b. **Overwrite** ：
      - 如果您希望 RHEL web 控制台使用零重写整个磁盘，请选择 **Overwrite existing data with zeros** 复选框。使用这个选项较慢，因为程序必须经过整个磁盘，但它更为安全。如果磁盘包含任何数据且您要覆盖数据，请使用这个选项。
        如果您没有选择 **Overwrite existing data with zeros** 复选框，RHEL web 控制台只重写磁盘头。这提高了格式化速度。
7. 单击 **Initialize**。
   分区表已创建，现在可以在该表上创建分区。如需了解更多详细信息，请参阅 使用 Web 控制台在 RAID 上创建分区。

19.4. 使用 WEB 控制台在 RAID 上创建分区

在现有分区表中创建一个分区。

先决条件

- 已创建分区表。详情请参阅 使用 Web 控制台在 RAID 上创建分区表

流程

1. 打开 RHEL 9 web 控制台。
2. 点击 **Storage**。
3. 在 **Storage** 表中，点您要在其上创建分区的 RAID 设备。
4. 在 RAID 设备页面中，滚动到 **GPT partitions** 部分，然后点击您创建的分区表旁的菜单按钮 ⋮。
   默认情况下，它被命名为 **Free space**。
5. 点 **Create partition**。
6. 在 **Create partition** 对话框中输入文件系统的名称。不要在名称中使用空格。
7. 在 **Mount Point** 字段中添加挂载路径。
8. 在 **Type** 下拉列表中选择文件系统的类型。
9. 在 **Size** 字段中，设置分区的大小。
10. 如果您希望 RHEL web 控制台使用零重写整个磁盘，请选择 **Overwrite existing data with zeros** 复选框。使用这个选项较慢，因为程序必须经过整个磁盘，但它更为安全。如果磁盘包含任何数据且您要覆盖数据，请使用这个选项。
    如果您没有选择 **Overwrite existing data with zeros** 复选框，RHEL web 控制台只重写磁盘头。这提高了格式化速度。
11. 如果要加密卷，请在 **Encryption** 下拉菜单中选择加密类型。
    如果您不想加密卷，请选择 **No encryption**。
12. 在 **At boot** 下拉菜单中选择您要何时挂载卷。
13. 在 **Mount options** 部分中：
    a. 如果您希望将卷挂载为只读逻辑卷，请选择 **Mount read only** 复选框。
    b. 选择 **Custom mount options** 复选框，如果您要更改默认挂载选项，请添加挂载选项。
14. 创建分区：
    - 如果要创建并挂载分区，请点 **Create and mount** 按钮。
    - 如果您只想创建分区，点 **Create only** 按钮。
      根据卷大小以及选择格式化选项，格式化可能需要几分钟。

      您可以在创建分区后创建更多的分区。

      此时，系统使用挂载的和格式化的 RAID。

验证

- 您可以在主存储页的 **Storage** 表中看到格式化的逻辑卷的详情。

19.5. 使用 WEB 控制台在 RAID 上创建卷组

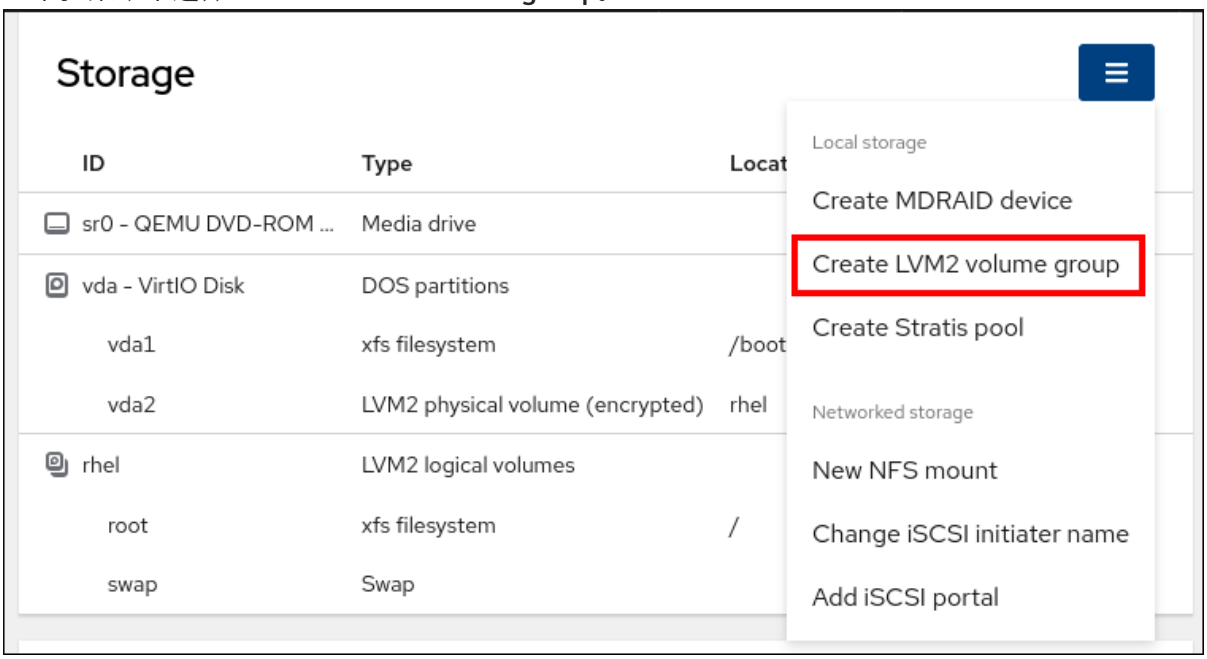
从软件 RAID 构建卷组。

先决条件

- 未格式化且未挂载的 RAID 设备。

流程

1. 打开 RHEL 9 web 控制台。
2. 点击 **Storage**。
3. 在 **Storage** 表中，点菜单按钮。
4. 从下拉菜单中选择 **Create LVM2 volume group**。



5. 在 **Create LVM2 volume group** 对话框中，输入新卷组的名称。
6. 在 **Disks** 列表中选择一个 RAID 设备。
   如果您在列表中没有看到 RAID，从系统中卸载 RAID。RAID 设备必须不能被 RHEL 9 系统使用。
7. 点 **Create**。

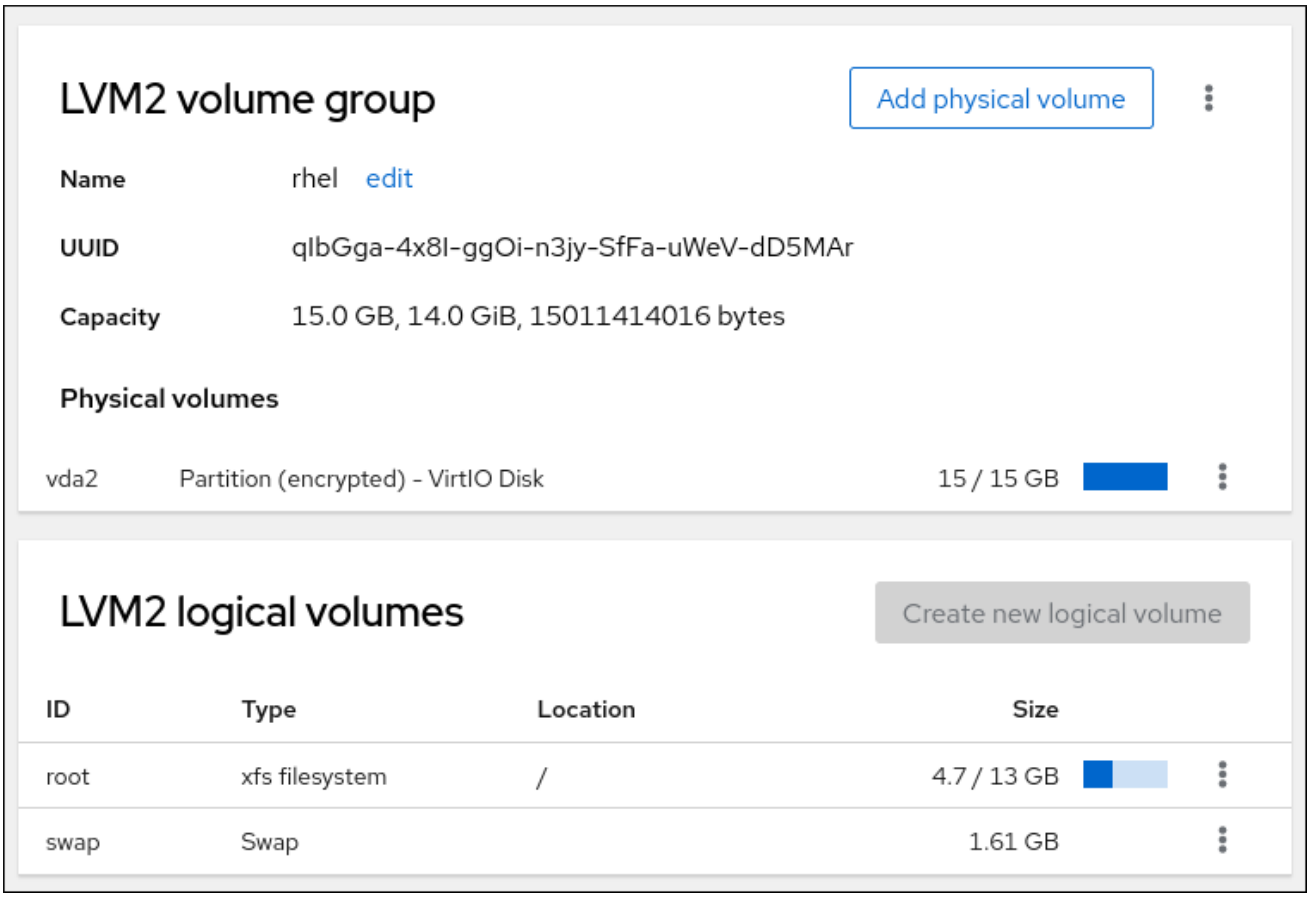
19.6. 其它资源

- 要了解更多有关软崩溃以及在配置 RAID LV 时如何保护数据的信息，请参阅 创建带有 DM 完整性的 RAID LV。

第 20 章 使用 WEB 控制台配置 LVM 逻辑卷

Red Hat Enterprise Linux 9 支持逻辑卷管理(LVM)。RHEL 9 安装程序自动创建一个 LVM2 卷组，并在安装过程中在其上安装系统。

您可以使用 RHEL web 控制台管理 LVM2 卷组和逻辑卷，如下面的 LVM2 组的示例页面中所示：



先决条件

- 已安装 RHEL 9 web 控制台。
  具体步骤请参阅安装并启用 Web 控制台。
- **cockpit-storaged** 软件包已安装在您的系统上。
- 您可以创建逻辑卷的物理驱动器、RAID 设备或其他类型的块设备。

20.1. WEB 控制台中的逻辑卷管理器

RHEL 9 web 控制台提供了一个图形界面，来创建 LVM 卷组和逻辑卷。

卷组在物理卷和逻辑卷之间创建一个层。此层允许添加或删除物理卷，而不影响逻辑卷本身。卷组显示为一个驱动器，其容量由组中包含的所有物理驱动器的容量组成。您可以在 web 控制台中将物理驱动器加入到卷组中。

逻辑卷的主要优点是：

- 比您的物理驱动器中使用的分区系统具有更大的灵活性。
- 能够将更多物理驱动器连接到一个卷中。

- 在不重启的情况下，可以在线扩展（增加）或缩减（减少）卷的容量。
- 能够创建快照。

其它资源

- 配置和管理逻辑卷

20.2. 在 WEB 控制台中创建卷组

从一个或多个物理驱动器或者其它存储设备创建卷组。

从卷组创建逻辑卷。每个卷组都可以包括多个逻辑卷。

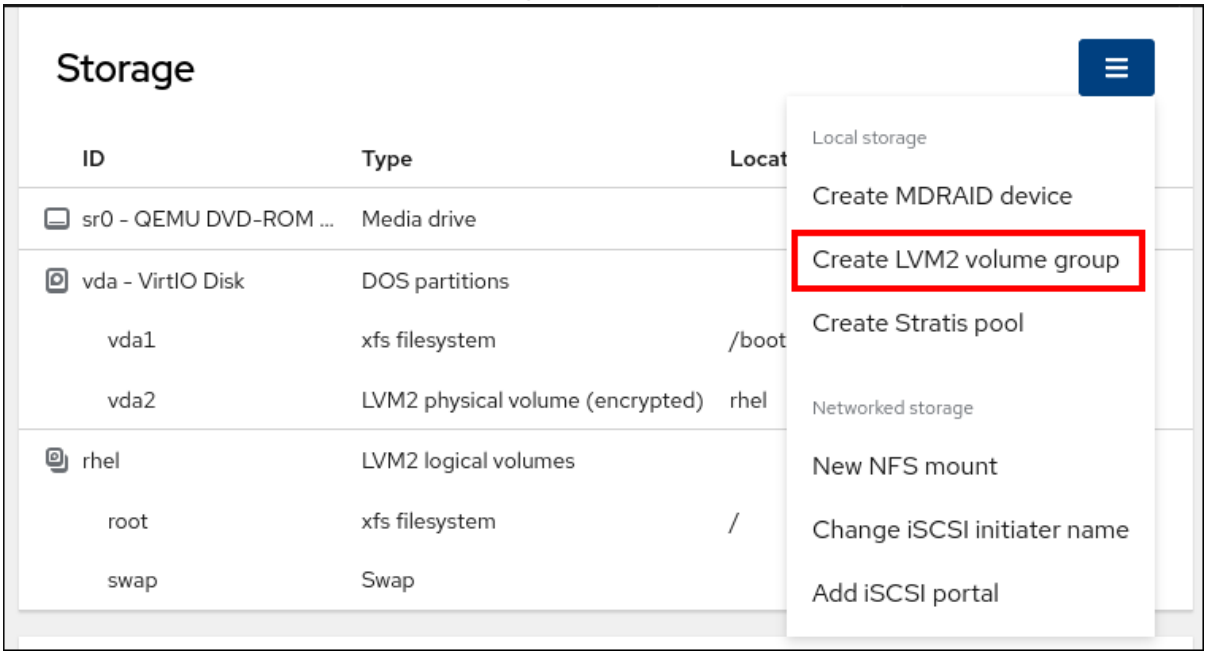
详情请查看管理 LVM 卷组。

先决条件

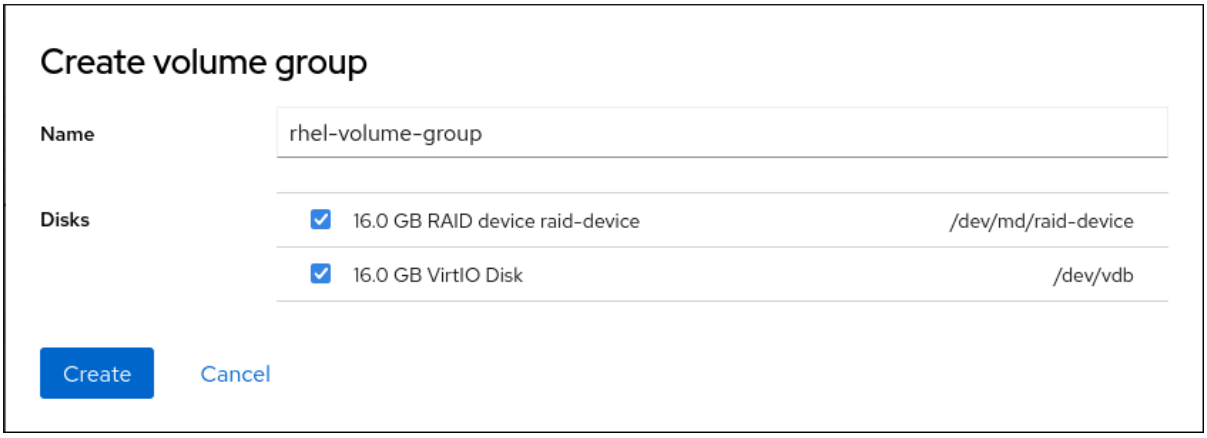
- 要创建卷组的物理驱动器或其他类型的存储设备。

流程

1. 登录到 RHEL 9 web 控制台。
2. 点 **Storage**。
3. 在 **Storage** 表中，点菜单按钮。
4. 从下拉菜单中选择 **Create LVM2 volume group**。



5. 在 **Name** 字段中输入卷组的名称。名称不得包含空格。
6. 选择您要组合的驱动器来创建卷组。



RHEL web 控制台仅显示未使用的块设备。如果您没有在列表中看到设备，请确保它没有被系统使用，或者将其格式化为空且未使用。使用的设备包括，例如：

- 使用文件系统格式化的设备
- 另一个卷组中的物理卷
- 物理卷是另一个软件 RAID 设备的成员

7. 点击 **Create**。
已创建卷组。

验证

- 在 **Storage** 页面中，检查新卷组是否列在 **Storage** 表中。

20.3. 在 WEB 控制台中创建逻辑卷

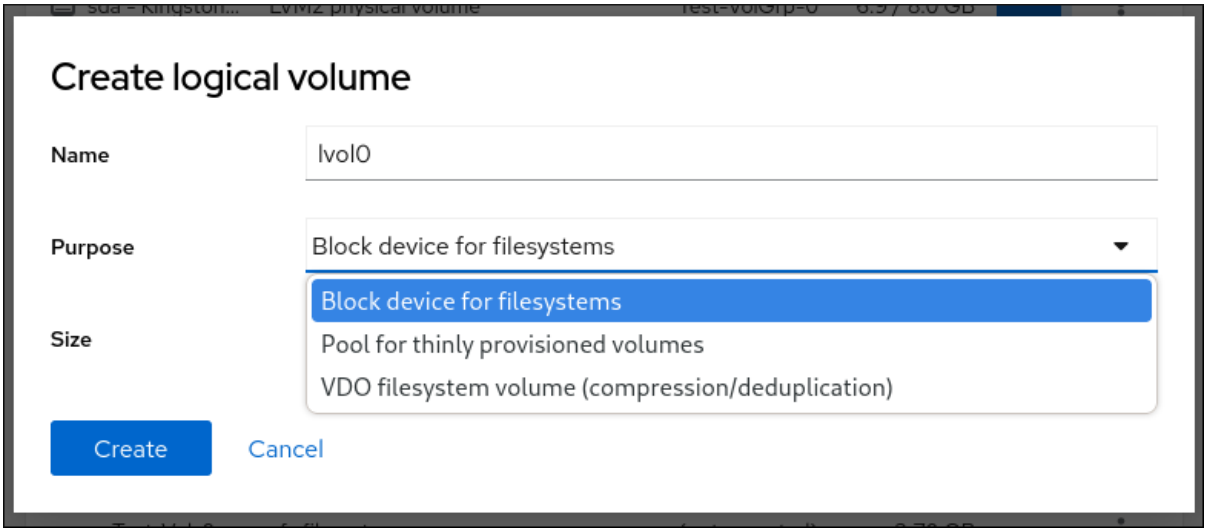
逻辑卷作为物理驱动器使用。您可以使用 RHEL 9 web 控制台在卷组中创建 LVM 逻辑卷。

先决条件

- **cockpit-storaged** 软件包已安装在您的系统上。
- 已创建的卷组。详情请参阅 在 web 控制台中创建卷组。

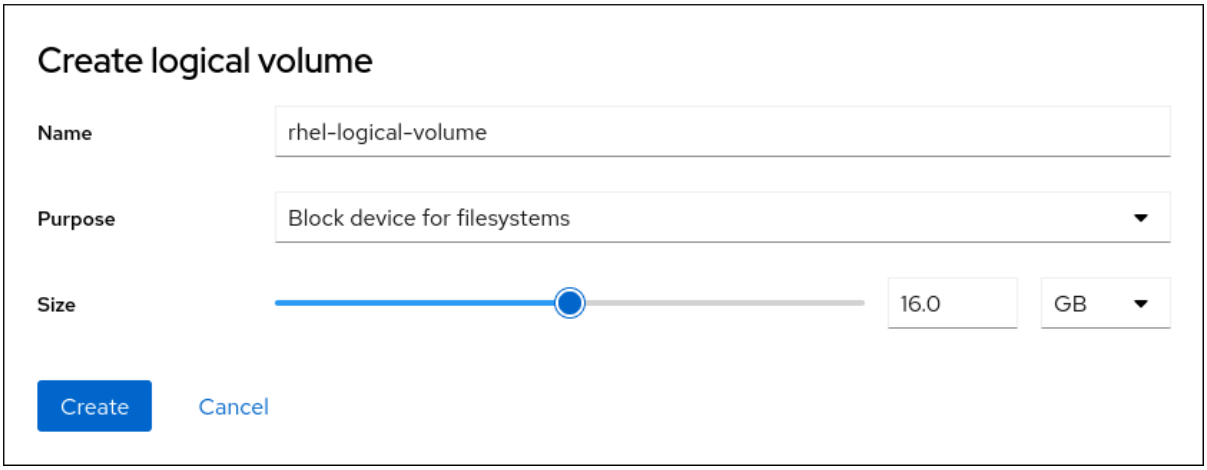
流程

1. 登录到 RHEL 9 web 控制台。
2. 点击 **Storage**。
3. 在 **Storage** 表中，点您要在其中创建逻辑卷的卷组。
4. 在 **Logical volume group** 页面中，滚动到 **LVM2 logical volumes** 部分，然后点击 **Create new logical volume**。
5. 在 **Name** 字段中输入新逻辑卷的名称。不要在名称中包含空格。
6. 在 **Purpose** 下拉菜单中，选择 **Block device for filesystems**。
此配置允许您创建一个逻辑卷，其最大卷大小等于卷组中所含所有驱动器的总和。



7. 定义逻辑卷的大小。考虑：
   - 使用这个逻辑卷的系统所需的空间。
   - 您要创建的逻辑卷数量。

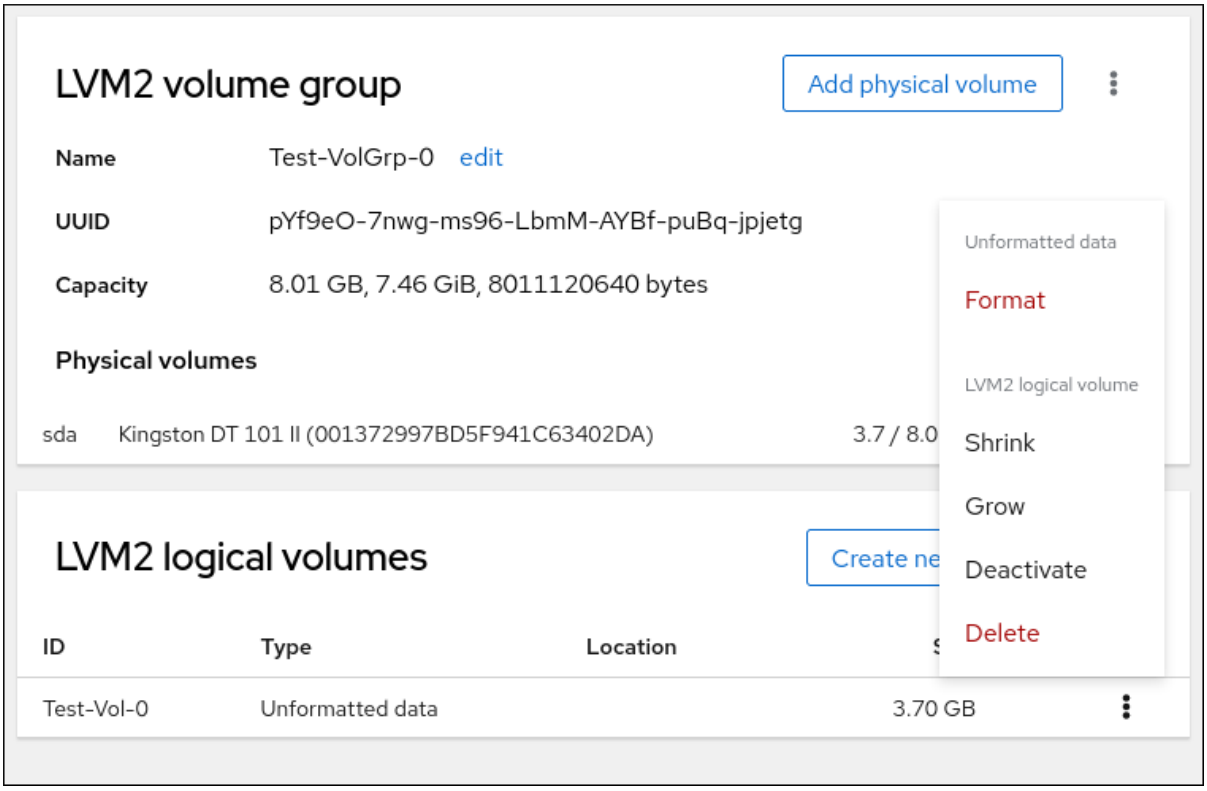
   您可以选择不使用整个空间。如果需要，您可以稍后增大逻辑卷。



8. 点 **Create**。
   逻辑卷被创建。要使用逻辑卷，您必须格式化并挂载卷。

验证

- 在 **Logical volume** 页面中，滚动到 **LVM2 logical volumes** 部分，并验证是否列出了新逻辑卷。



20.4. 在 WEB 控制台中格式化逻辑卷

逻辑卷作为物理驱动器使用。要使用它们，您必须使用文件系统对其进行格式化。

警告

格式化逻辑卷会删除卷上的所有数据。

您选择的文件系统决定了可用于逻辑卷的配置参数。例如，XFS 文件系统不支持缩小卷。详情请参阅 在 web 控制台中调整逻辑卷大小。

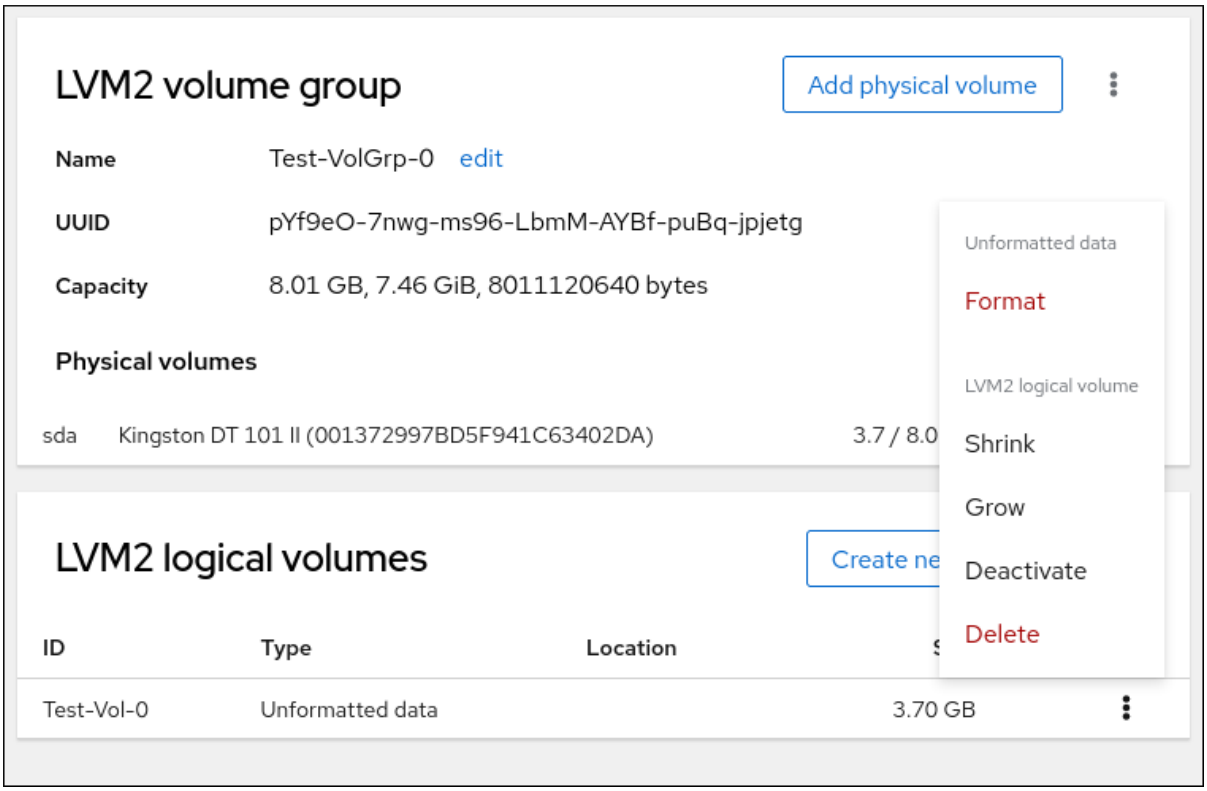
先决条件

- **cockpit-storaged** 软件包已安装在您的系统上。
- 已创建逻辑卷。详情请参阅 在 web 控制台中创建逻辑卷。
- 您有对系统的 root 访问权限。

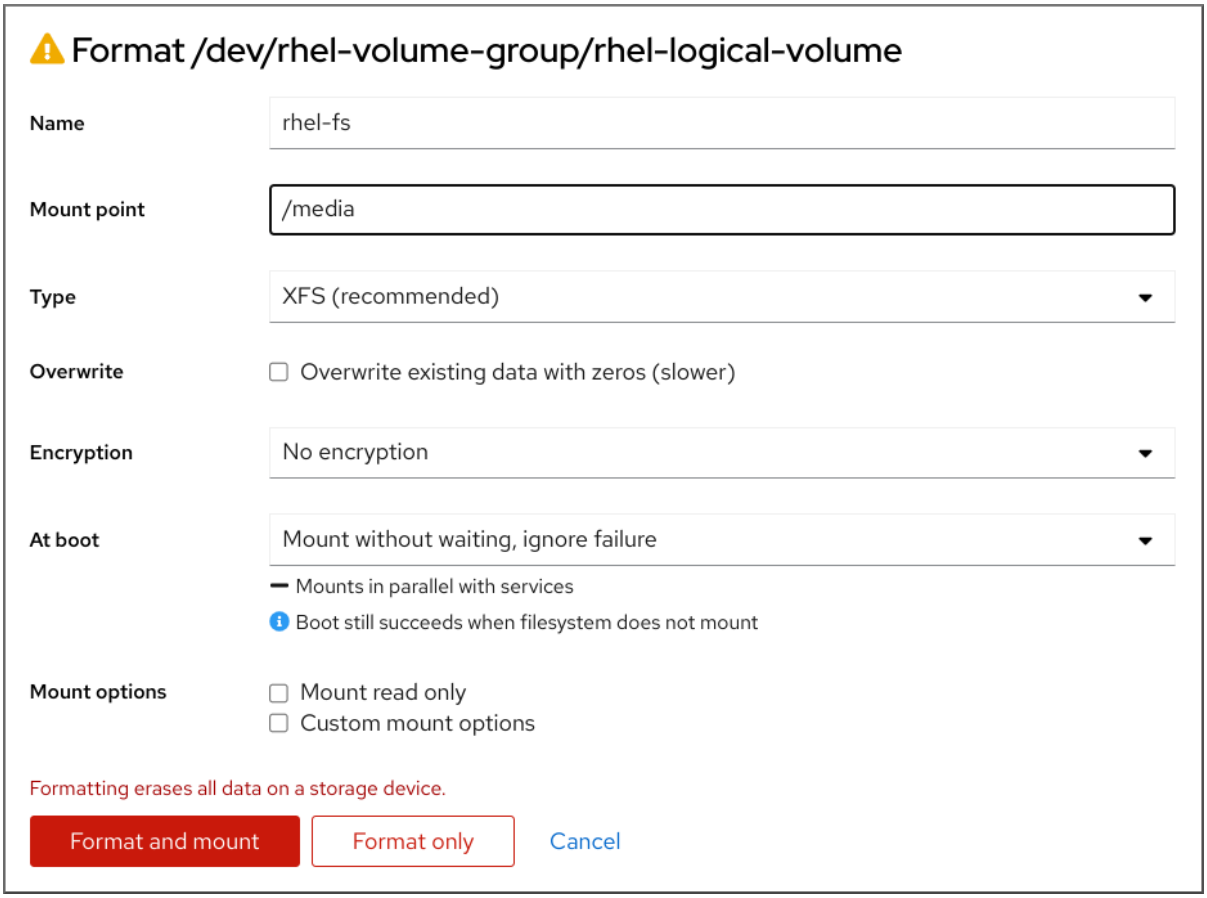
流程

1. 登录到 RHEL 9 web 控制台。
2. 点 **Storage**。
3. 在 **Storage** 表中，点创建了逻辑卷的卷组。

4. 在 **Logical volume group** 页面中，滚动到 **LVM2 logical volumes** 部分。
5. 点击您要格式的卷组旁的菜单按钮 ⋮。
6. 从下拉菜单中选择 **Format**。



7. 在 **Name** 字段中输入文件系统的名称。
8. 在 **Mount Point** 字段中添加挂载路径。



9. 在 **Type** 下拉菜单中选择一个文件系统：

   - **XFS** 文件系统支持大的逻辑卷，在不停止工作的情况下在线切换物理驱动器，并可以增大现有的文件系统。如果您没有不同的首选项，请保留这个文件系统。
     XFS 不支持缩小使用 XFS 文件系统格式的卷大小

   - **ext4** 文件系统支持：

     - 逻辑卷
     - 在不中断的情况下在线切换物理驱动器
     - 增大文件系统
     - 缩小文件系统

10. 如果您希望 RHEL web 控制台使用零重写整个磁盘，请选择 **Overwrite existing data with zeros** 复选框。使用这个选项较慢，因为程序必须经过整个磁盘，但它更为安全。如果磁盘包含任何数据且需要覆盖数据，则使用这个选项。
    如果您没有选择 **Overwrite existing data with zeros** 复选框，RHEL web 控制台只重写磁盘头。这提高了格式化速度。

11. 如果要在逻辑卷上启用它，请在 **Encryption** 下拉菜单中选择加密的类型。
    您可以选择 LUKS1 (Linux Unified Key Setup)或 LUKS2 加密的版本，这允许您使用密码短语来加密卷。

12. 在 **At boot** 下拉菜单中，选择系统引导后您希望逻辑卷何时挂载。

13. 选择所需的 **Mount options**。

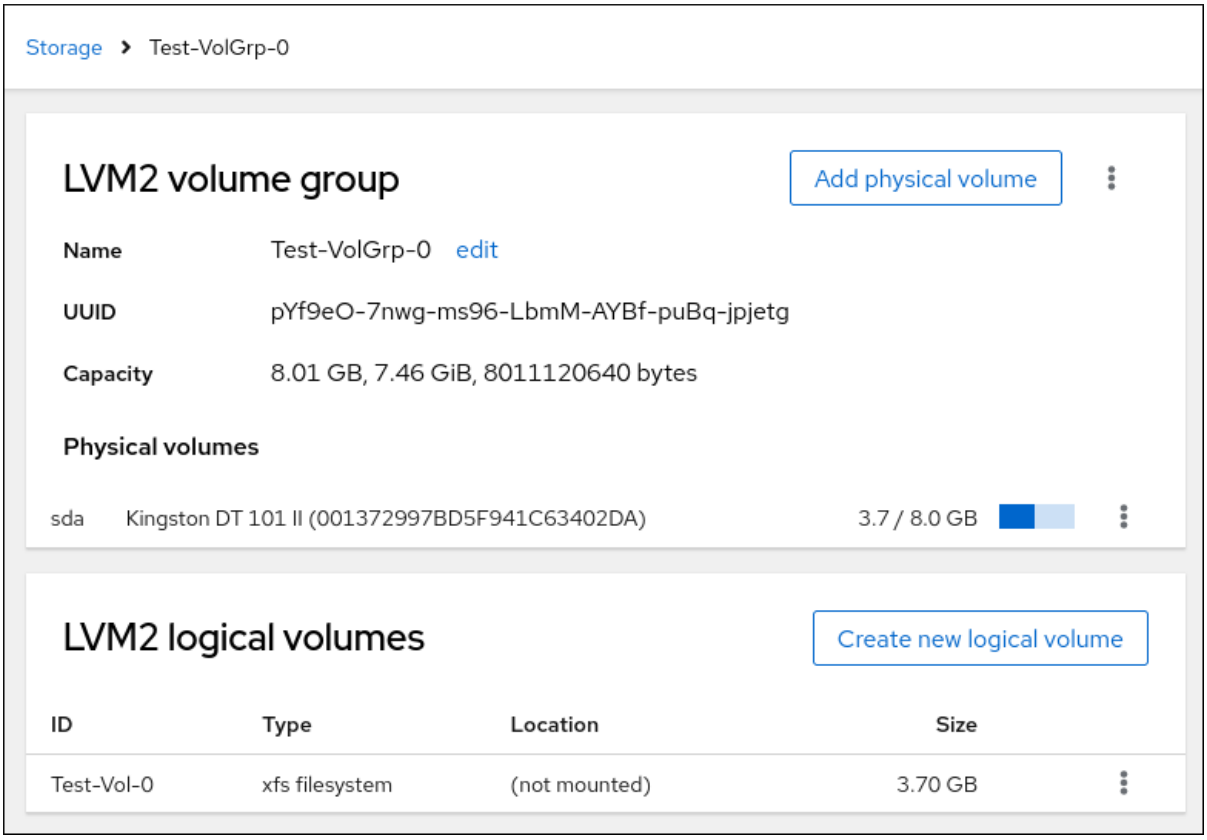
14. 格式化逻辑卷：

    - 如果要格式化卷并立即挂载它，请单击 **Format and mount**。

    - 如果要格式化卷而不挂载它，请单击 **Format only**。
      根据卷大小以及选择格式化选项，格式化可能需要几分钟。

验证

1. 在 **Logical volume group** 页面中，滚动到 **LVM2 logical volumes** 部分，然后点逻辑卷，来检查详情和其它选项。



2. 如果您选择了 **Format only** 选项，点逻辑卷行末尾的菜单按钮，然后选择 **Mount** 来使用逻辑卷。

20.5. 在 WEB 控制台中重新定义逻辑卷大小

了解如何在 RHEL 9 web 控制台中扩展或缩减逻辑卷。

您能否重新定义逻辑卷大小取决于您使用的文件系统。大多数文件系统允许您在在线扩展（不停机的情况）卷。

如果逻辑卷包含支持缩小的文件系统，您也可以减小（缩小）逻辑卷的大小。它应该在例如 ext3/ext4 的文件系统中可用。

警告

您不能减少包含 GFS2 或者 XFS 文件系统的卷。

先决条件

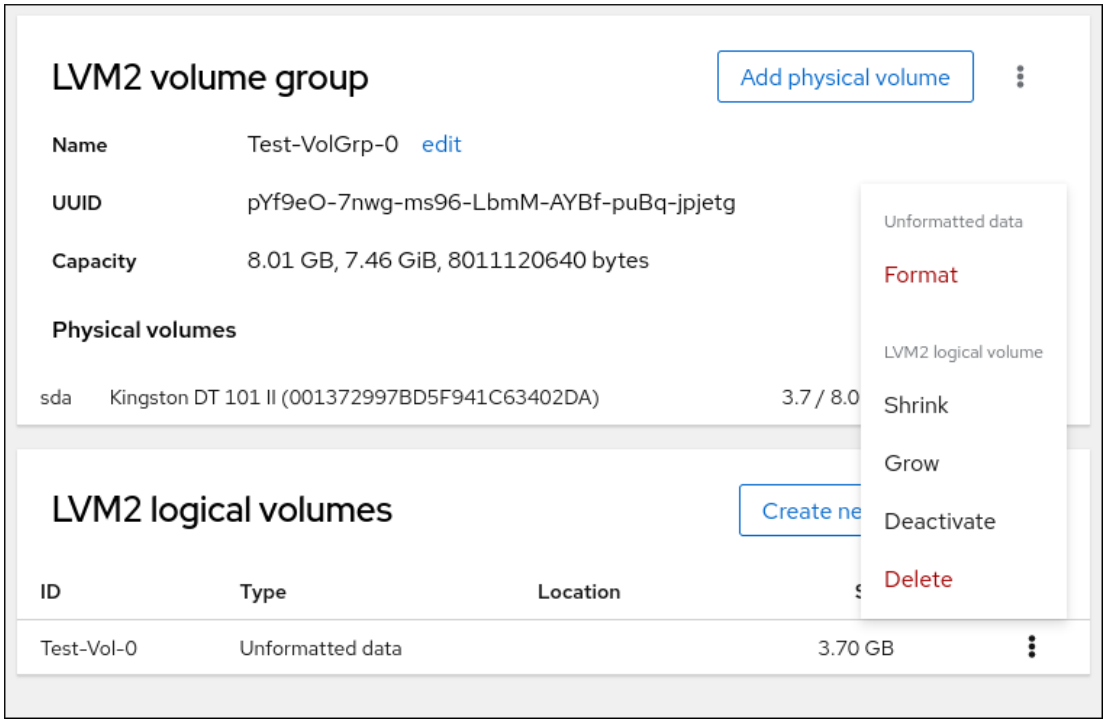
- 现有逻辑卷包含支持重新定义逻辑卷大小的文件系统。

流程

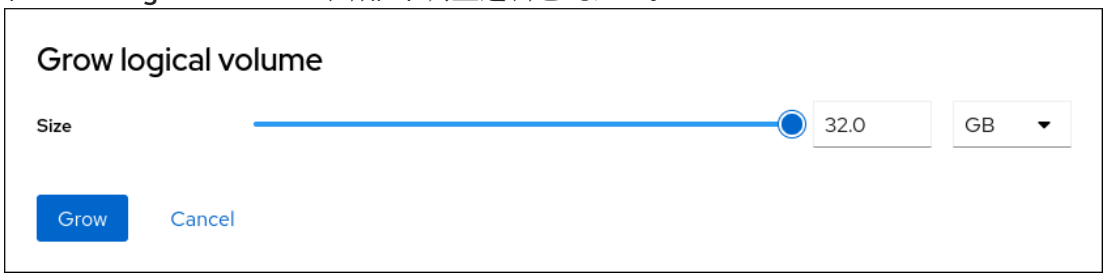
以下步骤提供了在不使卷离线的情况下增大逻辑卷的步骤：

1. 登录到 RHEL web 控制台。

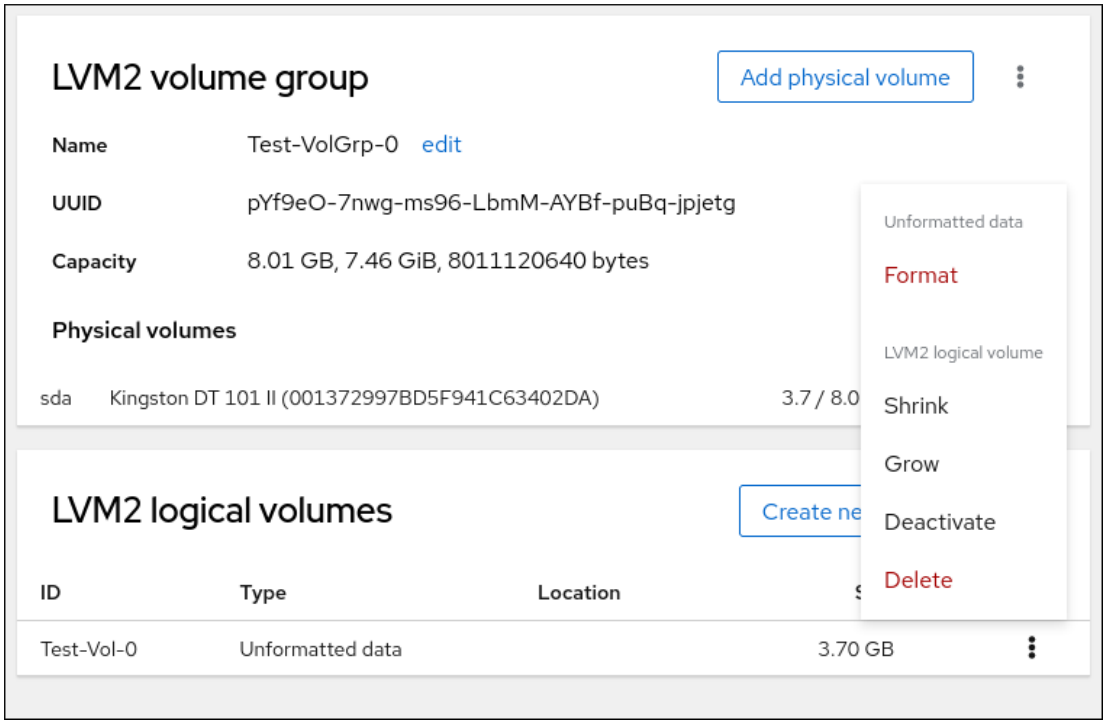
2. 点 **Storage**。
3. 在 **Storage** 表中，点创建了逻辑卷的卷组。
4. 在 **Logical Volume group** 页面中，滚动到 **LVM2 logical volumes** 部分，然后点击您要调整其大小的卷组旁的菜单按钮 ⋮。
5. 在菜单中，选择 **Grow** 或 **Shrink** 来调整卷的大小：
   - 增大卷：
     a. 选择 **Grow** 来增加卷的大小。



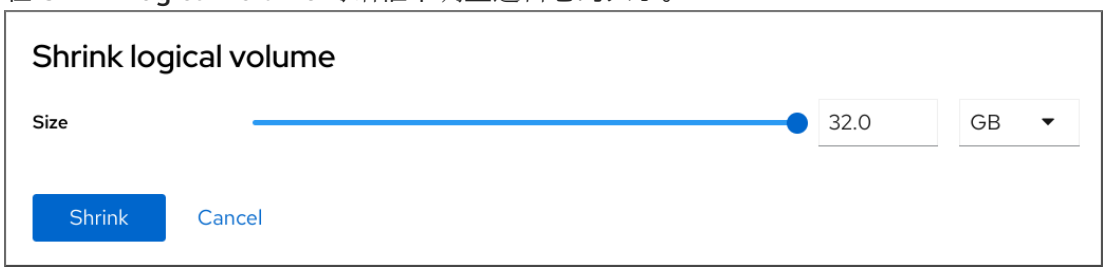
     b. 在 **Grow logical volume** 对话框中调整逻辑卷的大小。



     c. 点 **Grow**。
     LVM 增大逻辑卷，而不会导致系统中断。
   - 缩小卷：
     a. 选择 **Shrink** 以减少卷的大小。



b. 在 **Shrink logical volume** 对话框中调整逻辑卷的大小。



c. 点 **Shrink**。
LVM 缩小逻辑卷，而不会导致系统中断。

20.6. 其它资源

- 配置和管理逻辑卷

第 21 章 使用 WEB 控制台配置精简逻辑卷

您可以使用精简配置的逻辑卷为指定的应用程序或服务器分配比实际可用物理存储更多的空间。

详情请参阅 创建精简配置的快照卷。

先决条件

- 已安装 RHEL 9 web 控制台。
  详情请参阅安装 Web 控制台。
- **cockpit-storaged** 软件包已安装在您的系统上。
- 您要用来创建卷组的物理驱动器或者其他类型的存储设备被附加到您的系统上。

21.1. 在 WEB 控制台中为精简置备的卷创建池

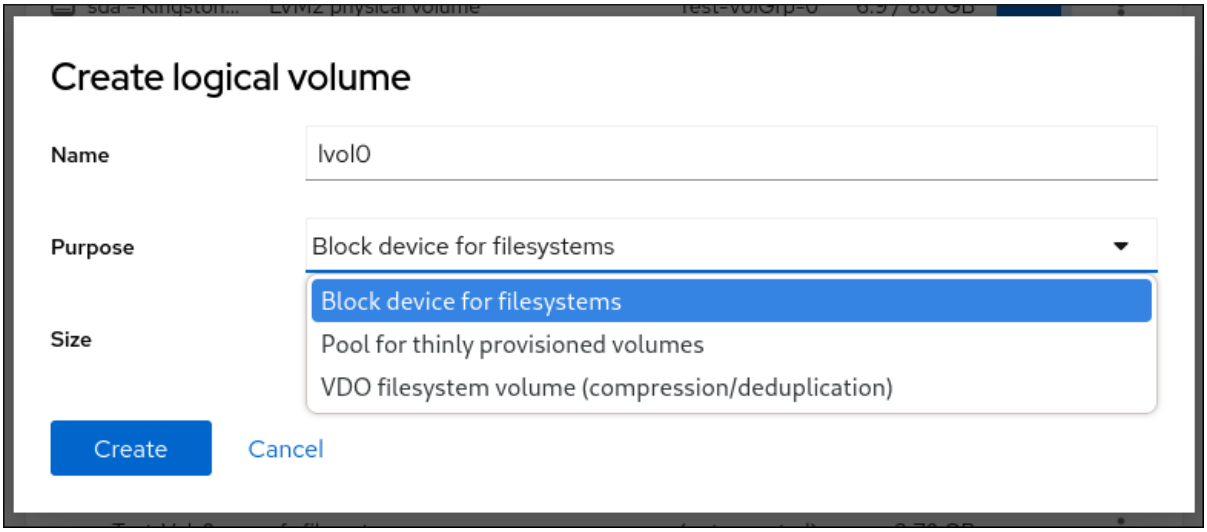
为精简配置的卷创建一个池。

先决条件

- 卷组已创建。

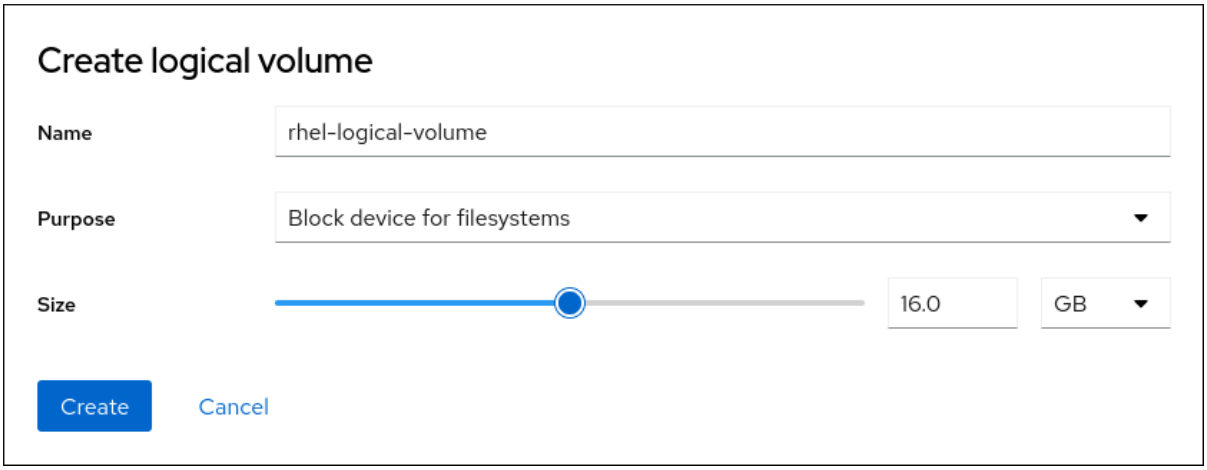
流程

1. 登录到 RHEL 9 web 控制台。
2. 点击 **Storage**。
3. 在 **Storage** 表中，点您要在其中创建精简卷的卷组。
4. 在 **Logical volume group** 页面中，滚动到 **LVM2 logical volumes** 部分，然后点击 **Create new logical volume**。
5. 在 **Name** 字段中输入新逻辑卷的名称。不要在名称中包含空格。
6. 在 **Purpose** 下拉菜单中，选择 **Pool for thinly provisioned volumes**。
   此配置允许您创建一个逻辑卷，其最大卷大小等于卷组中所含所有驱动器的总和。



7. 定义逻辑卷的大小。考虑：
   - 使用这个逻辑卷的系统需要多少空间。
   - 您要创建的逻辑卷数量。

   您可以选择不使用整个空间。如果需要，您可以稍后增大逻辑卷。



8. 点 **Create**。
   精简卷的池创建了，您现在可以向池中添加精简卷。

21.2. 在 WEB 控制台中创建精简配置的逻辑卷

您可以使用 Web 控制台在池中创建精简配置的逻辑卷。该池可以包含多个精简卷，每个精简卷可以变大，作为精简卷本身的池。

重要

使用精简卷需要定期检查逻辑卷的实际可用物理空间。

先决条件

- 用于精简卷的池已创建。
  详情请参阅在 web 控制台中为精简逻辑卷创建池。

流程

1. 登录到 RHEL 9 web 控制台。
2. 点击 **Storage**。
3. 在 **Storage** 表中，点您要在其中创建精简卷的卷组的菜单按钮。
4. 在 **Logical volume group** 页面中，滚动到 **LVM2 logical volumes** 部分，然后点击您要在其中创建精简逻辑卷的池。
5. 在 **Pool for thinly provisioned LVM2 logical volumes**页面中，滚动到 **Thinly provisioned LVM2 logical volumes** 部分，然后点 **Create new thinly provisioned logical volume**。
6. 在 **Create thin volume** 对话框中输入精简卷的名称。不要在名称中使用空格。

7. 定义精简卷的大小。

8. 点 **Create**。
精简逻辑卷被创建。您必须先格式化卷，然后才能使用它。

21.3. 在 WEB 控制台中格式化逻辑卷

逻辑卷作为物理驱动器使用。要使用它们，您必须使用文件系统对其进行格式化。

警告

格式化逻辑卷会删除卷上的所有数据。

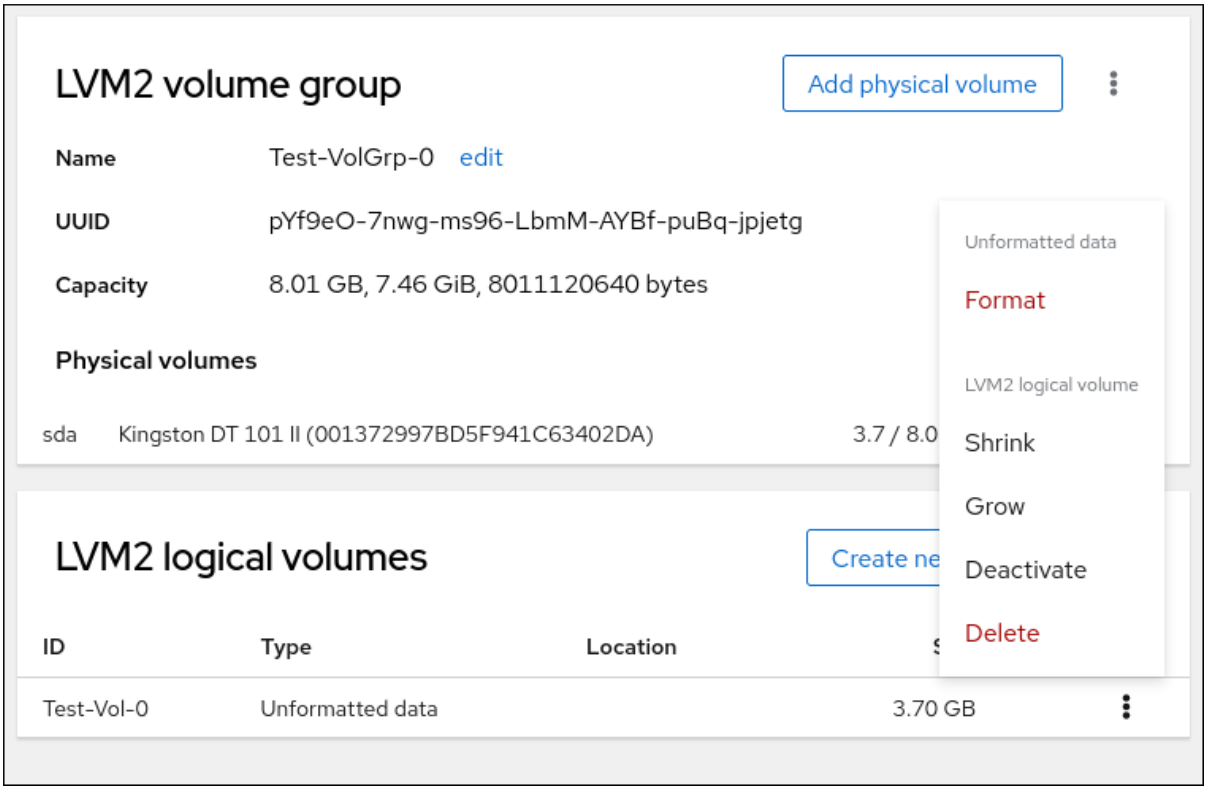
您选择的文件系统决定了可用于逻辑卷的配置参数。例如，XFS 文件系统不支持缩小卷。详情请参阅 在 web 控制台中调整逻辑卷大小。

先决条件

- **cockpit-storaged** 软件包已安装在您的系统上。
- 已创建逻辑卷。详情请参阅 在 web 控制台中创建逻辑卷。
- 您有对系统的 root 访问权限。

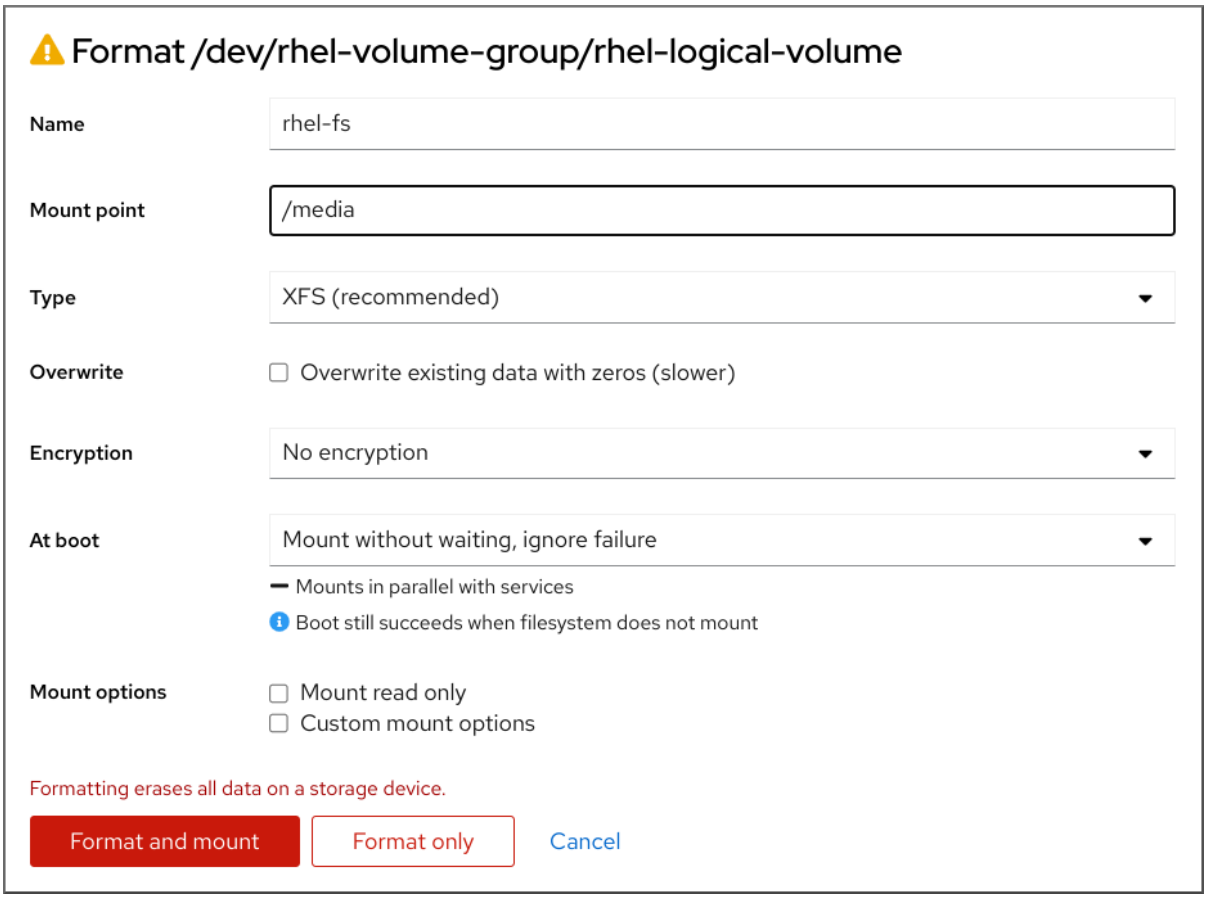
流程

1. 登录到 RHEL 9 web 控制台。
2. 点 **Storage**。
3. 在 **Storage** 表中，点创建了逻辑卷的卷组。
4. 在 **Logical volume group** 页面中，滚动到 **LVM2 logical volumes** 部分。
5. 点击您要格式的卷组旁的菜单按钮 ⋮。
6. 从下拉菜单中选择 **Format**。



7. 在 **Name** 字段中输入文件系统的名称。

8. 在 **Mount Point** 字段中添加挂载路径。



9. 在 **Type** 下拉菜单中选择一个文件系统：

   - **XFS** 文件系统支持大的逻辑卷，在不停止工作的情况下在线切换物理驱动器，并可以增大现有的文件系统。如果您没有不同的首选项，请保留这个文件系统。

XFS 不支持缩小使用 XFS 文件系统格式的卷大小

- ext4 文件系统支持：
  - 逻辑卷
  - 在不中断的情况下在线切换物理驱动器
  - 增大文件系统
  - 缩小文件系统

10. 如果您希望 RHEL web 控制台使用零重写整个磁盘，请选择 **Overwrite existing data with zeros** 复选框。使用这个选项较慢，因为程序必须经过整个磁盘，但它更为安全。如果磁盘包含任何数据且需要覆盖数据，则使用这个选项。
    如果您没有选择 **Overwrite existing data with zeros** 复选框，RHEL web 控制台只重写磁盘头。这提高了格式化速度。

11. 如果要在逻辑卷上启用它，请在 **Encryption** 下拉菜单中选择加密的类型。
    您可以选择 LUKS1 (Linux Unified Key Setup)或 LUKS2 加密的版本，这允许您使用密码短语来加密卷。

12. 在 **At boot** 下拉菜单中，选择系统引导后您希望逻辑卷何时挂载。

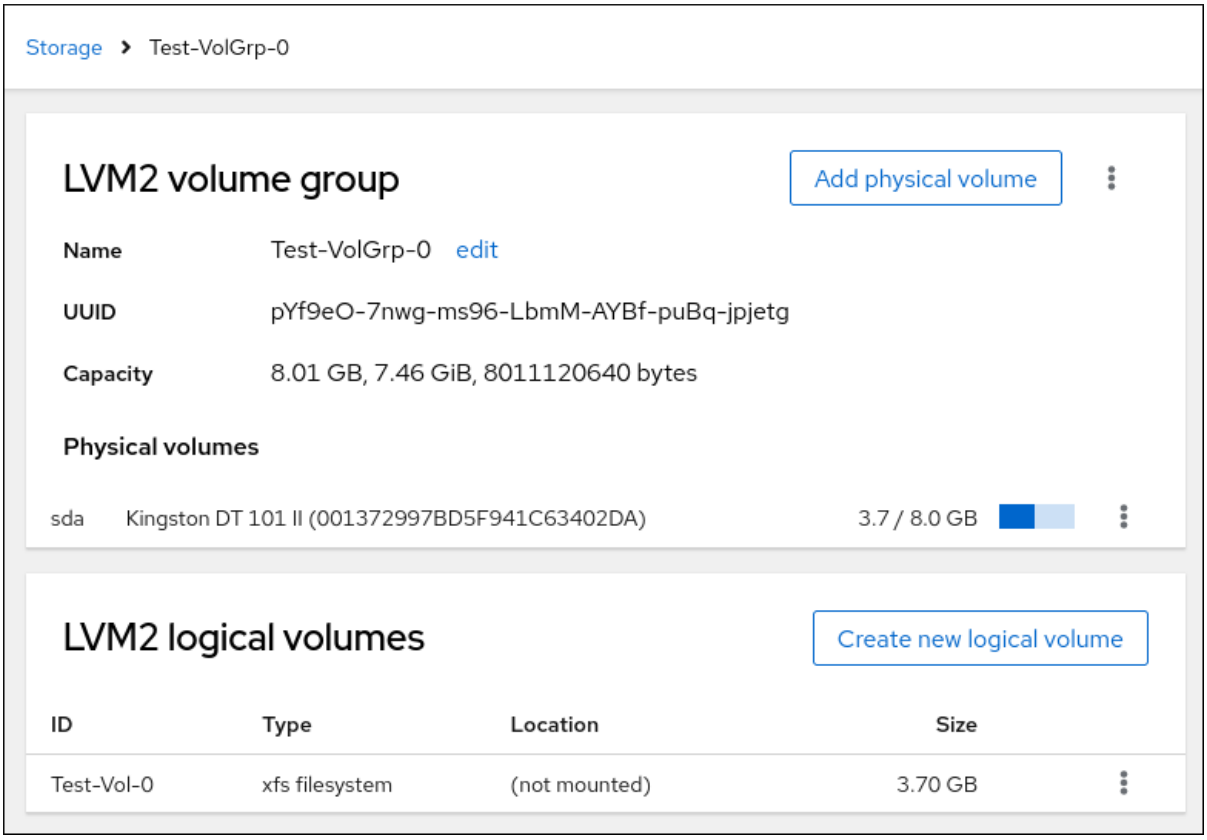
13. 选择所需的 **Mount options**。

14. 格式化逻辑卷：

    - 如果要格式化卷并立即挂载它，请单击 **Format and mount**。
    - 如果要格式化卷而不挂载它，请单击 **Format only**。
      根据卷大小以及选择格式化选项，格式化可能需要几分钟。

验证

1. 在 **Logical volume group** 页面中，滚动到 **LVM2 logical volumes** 部分，然后点逻辑卷，来检查详情和其它选项。



2. 如果您选择了 **Format only** 选项，点逻辑卷行末尾的菜单按钮，然后选择 **Mount** 来使用逻辑卷。

21.4. 使用 WEB 控制台创建精简配置的快照卷

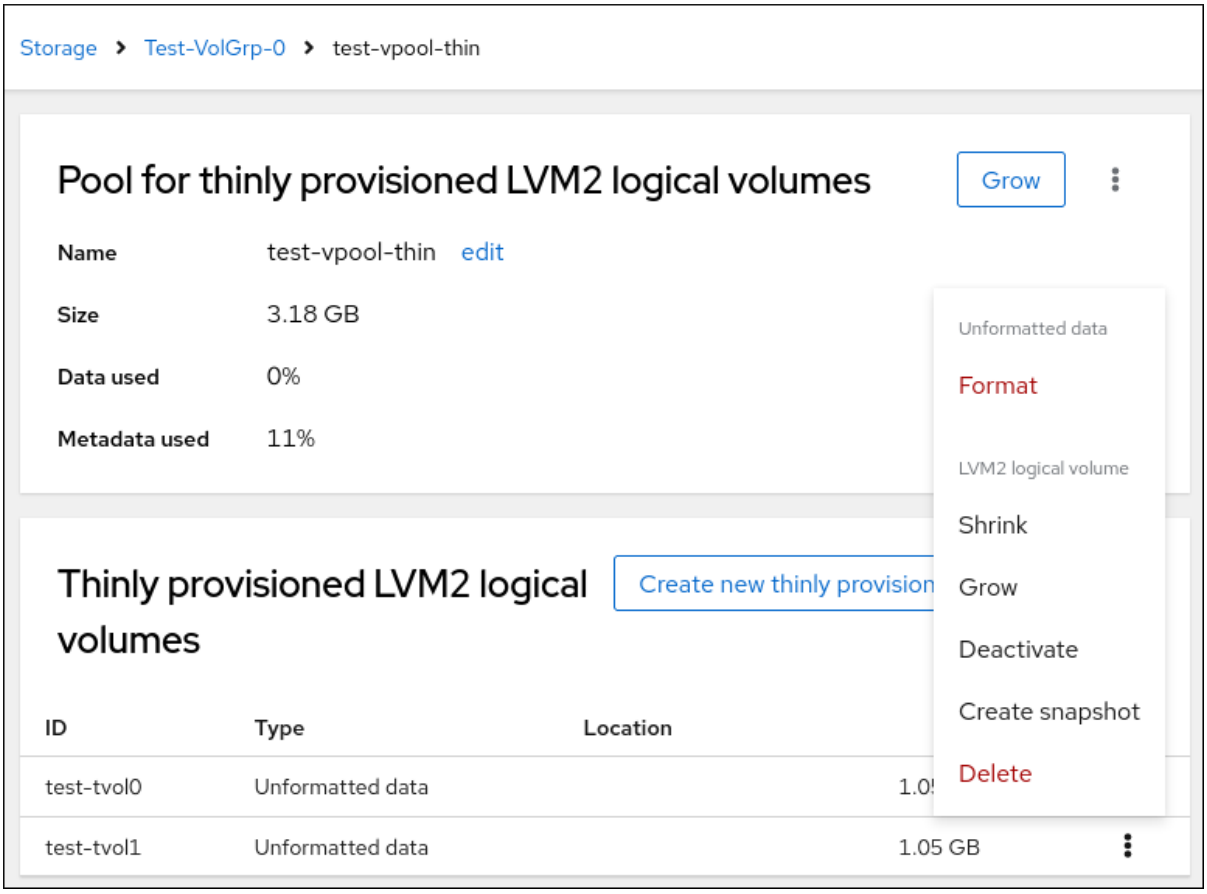
您可以在 RHEL web 控制台中创建精简逻辑卷的快照，来从最后一个快照备份磁盘上记录的更改。

先决条件

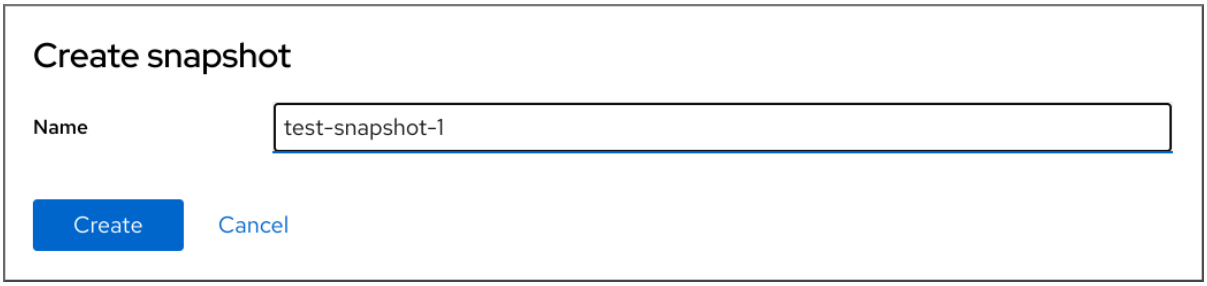
- Web 控制台已安装并可以访问。如需更多信息，请参阅 安装并启用 Web 控制台。
- **cockpit-storaged** 软件包已安装在您的系统上。
- 一个精简配置的卷已创建。如需更多信息，请参阅 使用 Web 控制台配置精简逻辑卷。

流程

1. 登录到 RHEL 9 web 控制台。
2. 点击 **Storage**。
3. 在 **Storage** 表中，点您要在其中创建精简卷的卷组。
4. 在 **Logical volume group** 页面中，滚动到 **LVM2 logical volumes** 部分，然后点击您要在其中创建精简逻辑卷的池。
5. 在 **Pool for thinly provisioned LVM2 logical volumes**页面中，滚动到 **Thinly provisioned LVM2 logical volumes** 部分，然后点击逻辑卷旁边的菜单按钮 ⋮。
6. 从下拉菜单中选择 **Create snapshot**。



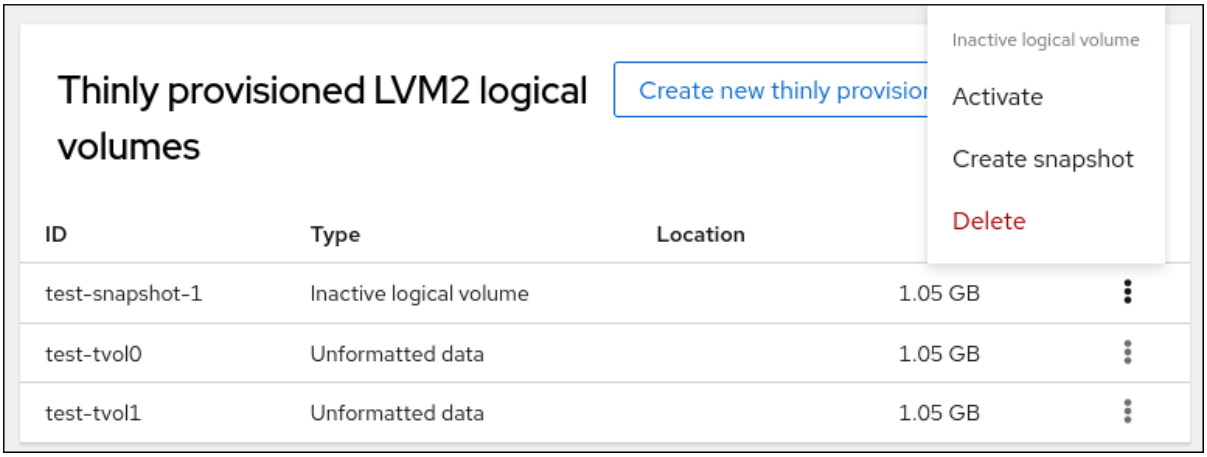
7. 在 Name 字段中输入快照名称。



8. 点 **Create**。

9. 在 **Pool for thinly provisioned LVM2 logical volumes**页面中，滚动到 **Thinly provisioned LVM2 logical volumes** 部分，然后点击新创建的快照旁的菜单按钮 ⋮。

10. 从下拉菜单中选择 **Activate** 来激活卷。



第 22 章 使用 WEB 控制台更改卷组中的物理驱动器

使用 RHEL 9 web 控制台更改卷组中的驱动器。

物理驱动器的更改由以下过程组成：

- 在逻辑卷中添加物理驱动器。
- 从逻辑卷中删除物理驱动器。

先决条件

- 已安装 RHEL 9 web 控制台。
  详情请参阅安装 Web 控制台。
- **cockpit-storaged** 软件包已安装在您的系统上。
- 用于替换旧的或有问题的驱动器的新物理驱动器。
- 该配置期望物理驱动器在一个卷组中进行组织。

22.1. 在 WEB 控制台中的卷组中添加物理驱动器

RHEL 9 web 控制台允许您在现有逻辑卷中添加新的物理驱动器或者其他类型的卷。

先决条件

- 必须创建一个卷组。
- 连接到机器的新驱动器。

流程

1. 登录到 RHEL 9 web 控制台。
2. 点击 **Storage**。
3. 在 **Storage** 表中，点您要向其添加物理驱动器的卷组。
4. 在 **LVM2 volume group** 页面中，单击 **Add physical volume**。
5. 在 **Add Disks** 对话框中，选择首选的驱动器并点 **Add**。

验证步骤

- 在 **LVM2 volume group** 页面中，检查 **Physical volumes** 部分，以验证卷组中的新物理驱动器是否可用。

22.2. 在 WEB 控制台中，从卷组中删除物理驱动器

如果逻辑卷包含多个物理驱动器，您可以在线删除其中一个物理驱动器。

系统会在删除过程中自动将驱动器中的所有数据移至其他驱动器。请注意，这可能需要一些时间。

web 控制台也会验证删除物理驱动器是否会有足够的空间。

先决条件

- 一个连接了多个物理驱动器的卷组。

流程

1. 登录到 RHEL 9 web 控制台。
2. 点击 **Storage**。
3. 在 **Storage** 表中，点您要向其添加物理驱动器的卷组。
4. 在 **LVM2 volume group** 页面中，滚动到 **Physical volumes** 部分。
5. 点您要删除的物理卷旁边的菜单按钮 ⋮。
6. 从下拉菜单中选择 **Remove**。
   RHEL 9 web 控制台验证逻辑卷是否有足够的可用空间来删除磁盘。如果没有可用空间来传输数据，则无法删除磁盘，您必须首先添加一个磁盘来增加卷组的容量。详情请参阅 在 web 控制台中向逻辑卷添加物理驱动器。

第 23 章 使用 WEB 控制台管理 VIRTUAL DATA OPTIMIZER 卷

使用 RHEL 9 web 控制台配置 Virtual Data Optimizer(VDO)。

您将学习如何：

- 创建 VDO 卷
- 格式化 VDO 卷
- 扩展 VDO 卷

先决条件

- RHEL 9 web 控制台已安装并可以访问。详情请参阅安装 Web 控制台。
- **cockpit-storaged** 软件包已安装在您的系统上。

23.1. WEB 控制台中的 VDO 卷

Red Hat Enterprise Linux 9 支持 Virtual Data Optimizer(VDO)。

VDO 是一个组合了以下功能的虚拟化技术：

压缩
详情请参阅在VDO 中启用或禁用压缩。

重复数据删除（Deduplication）
详情请参阅在VDO 中启用或禁用压缩。

精简置备
详情请参阅创建和管理精简置备卷（精简卷）。

使用这些技术，VDO：

- 保存存储空间内联
- 压缩文件
- 消除重复
- 可让您分配超过物理或者逻辑存储量的虚拟空间
- 允许您通过增大虚拟存储来扩展虚拟存储

VDO 可以在很多类型的存储之上创建。在 RHEL 9 web 控制台中，您可以在以下之上配置 VDO：

- LVM

注意

不可能在精简置备的卷之上配置 VDO。

- 物理卷
- 软件 RAID

有关在 Storage Stack 中放置 VDO 的详情，请参阅系统要求。

其它资源

- 有关 VDO 的详情，请参阅 重复数据删除和压缩存储。

23.2. 在 WEB 控制台中创建 VDO 卷

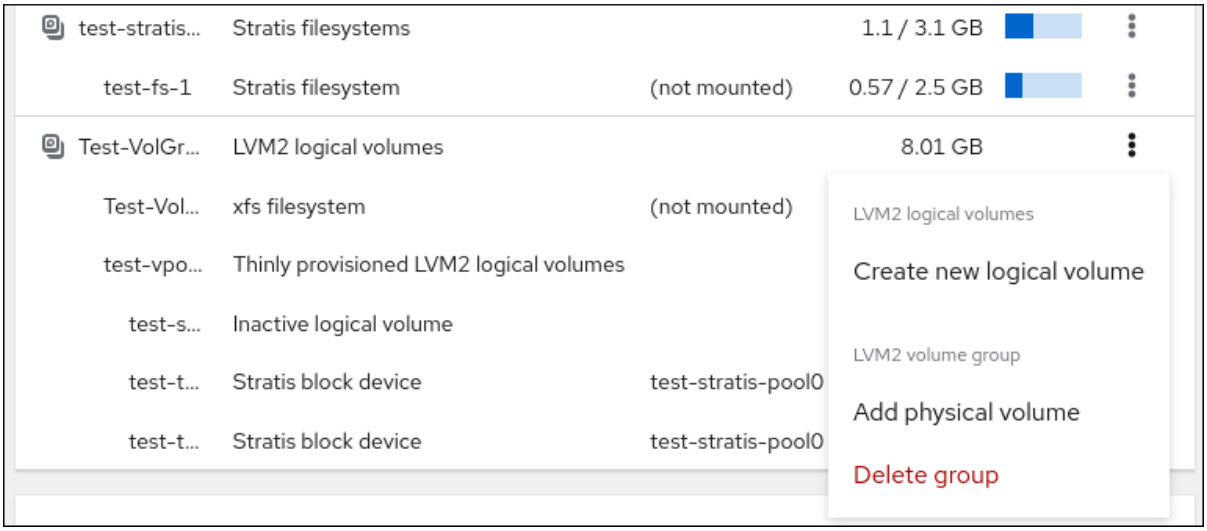
在 RHEL web 控制台中创建 VDO 卷。

先决条件

- 要从其创建 VDO 的 LVM2 组。

流程

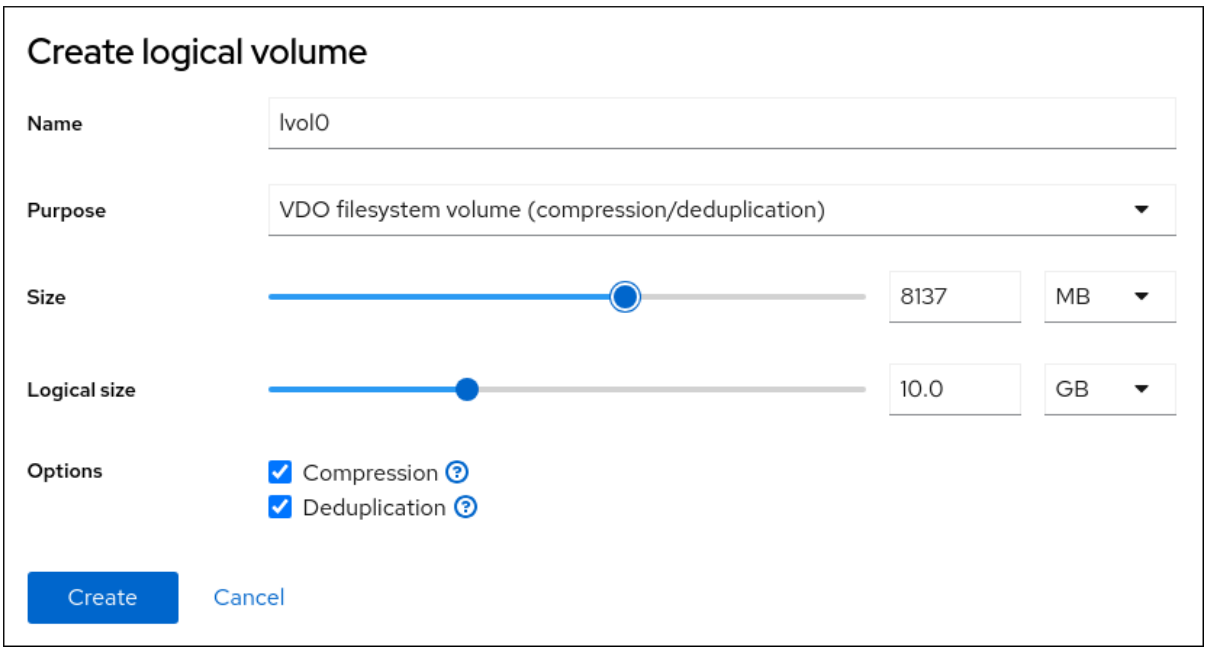
1. 登录到 RHEL 9 web 控制台。
   详情请参阅 登录到 web 控制台。
2. 点击 **Storage**。
3. 点击您要在其中创建 VDO 卷的 LVM2 组旁边的菜单按钮 ⋮。



4. 在 **Purpose** 字段旁边的下拉菜单中选择 **VDO filesystem volume**。
5. 在 **Name** 字段中输入 VDO 卷的名称，没有空格。
6. 在 **Logical Size** 条中，设置 VDO 卷的大小。您可以扩展超过十倍，但请考虑创建 VDO 卷的目的是：
   - 对于活跃的虚拟机或容器存储，逻辑大小为物理大小的十倍。
   - 对于对象存储，逻辑大小为物理大小的三倍。

   详情请参阅 Deploying VDO。
7. 选择 **Compression** 选项。这个选项可以有效地减少各种文件格式。
   详情请参阅在VDO 中启用或禁用压缩。
8. 选择 **Deduplication** 选项。

这个选项通过删除重复块的多个副本来减少存储资源的消耗。详情请参阅在VDO 中启用或禁用压缩。



验证步骤

- 检查您是否可在 **Storage** 部分看到新的 VDO 卷。然后，您可以使用文件系统对其进行格式化。

23.3. 在 WEB 控制台中格式化 VDO 卷

VDO 卷作为物理驱动器使用。要使用它们，您必须使用文件系统对其进行格式化。

警告

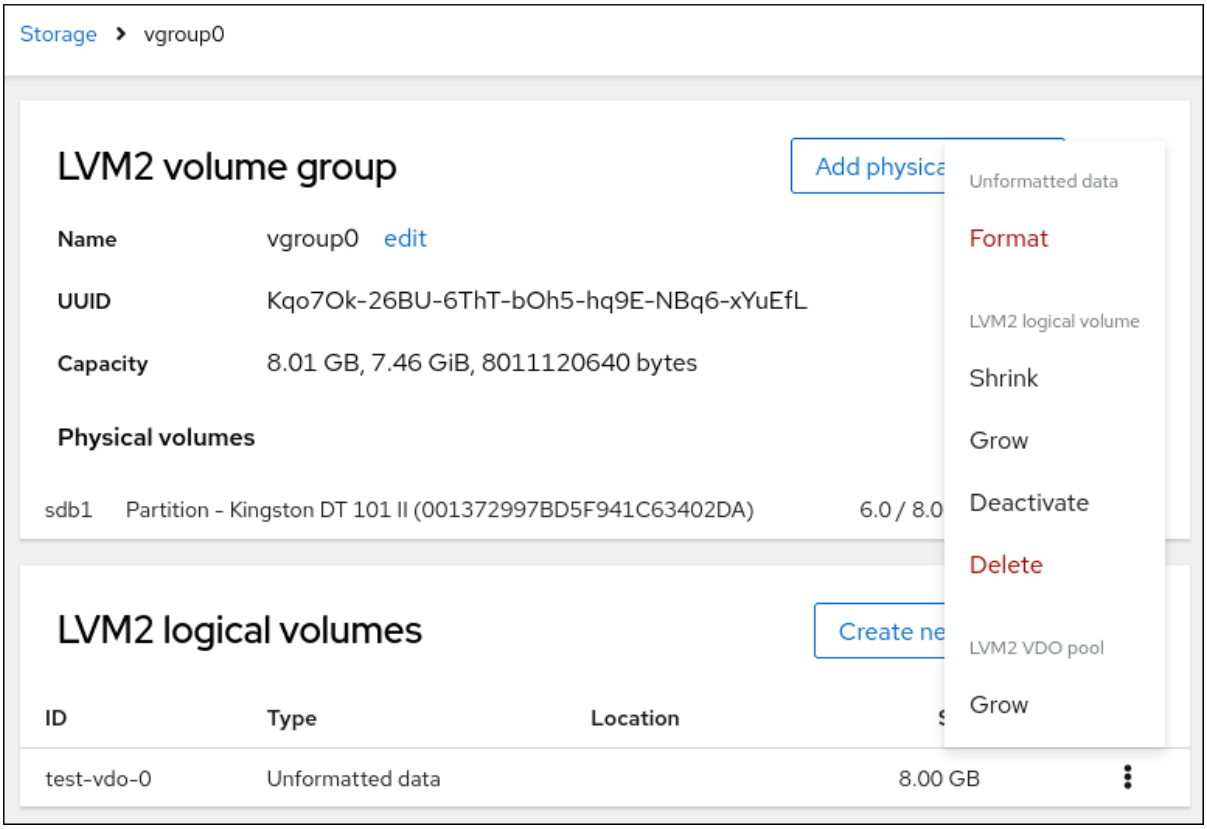
格式化会清除卷上的所有数据。

先决条件

- 已创建一个 VDO 卷。详情请参阅在 web 控制台中创建 VDO 卷。

流程

1. 登录到 RHEL 9 web 控制台。详情请参阅 登录到 web 控制台。
2. 点击 **Storage**。
3. 点击包含您要格式化的 VDO 卷的 LVM2 卷组。
4. 点击您要格式化的 VDO 卷所在行末尾的菜单按钮 ⋮。
5. 点 **Format**。



6. 在 **Name** 字段输入逻辑卷名称。

7. 在 **Mount Point** 字段中添加挂载路径。

8. 默认情况下，在完成此对话框后，web 控制台只重写磁盘头。这个选项的优点是格式化速度快。如果您选中了 **Overwrite existing data with zeros**选项，Web 控制台会使用零重写整个磁盘。这个选项较慢，因为程序必须经过整个磁盘。如果磁盘包含任何敏感数据，且您想要重写它们，则使用这个选项。

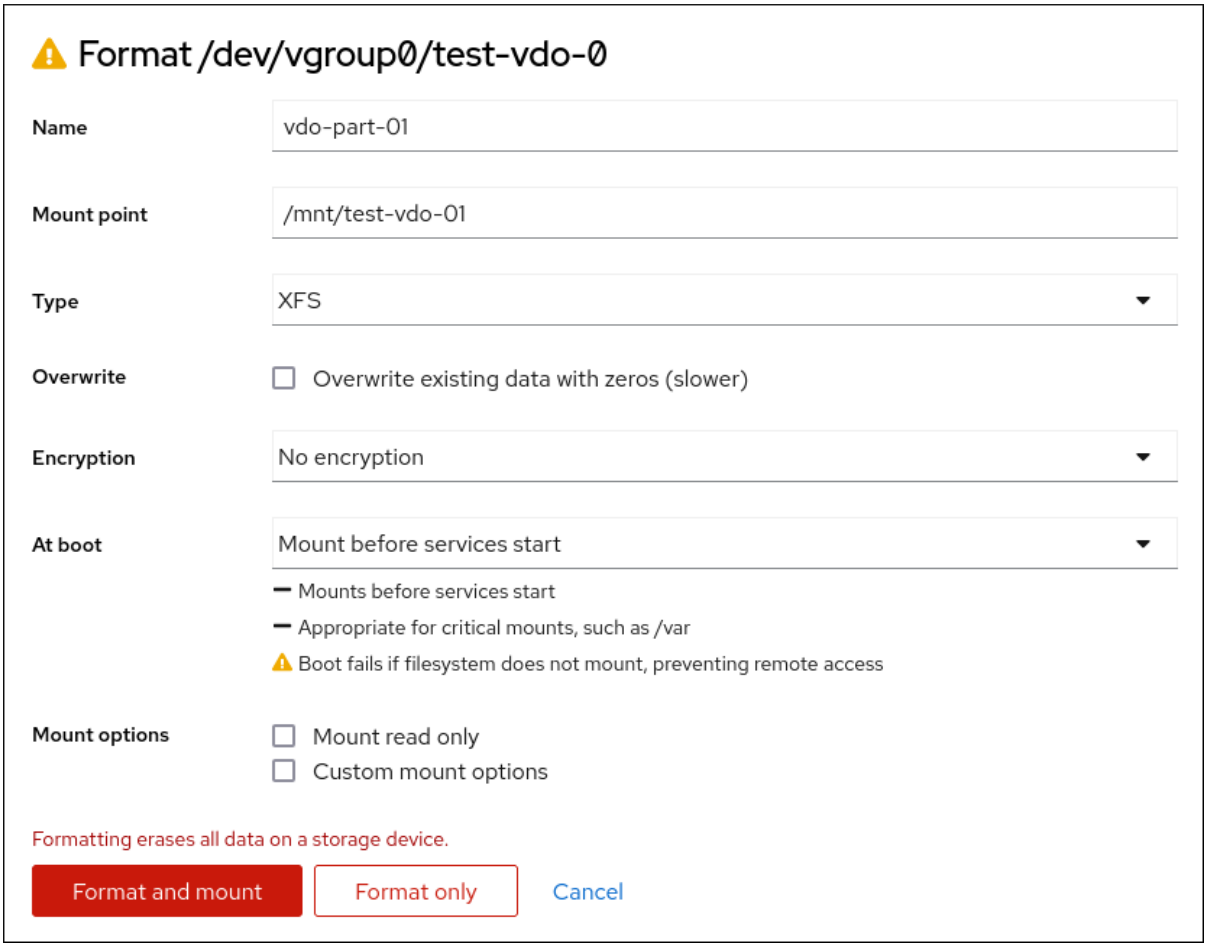
9. 在 **Type** 下拉菜单中选择一个文件系统：

   - 默认选项 **XFS** 文件系统支持大型逻辑卷，在不中断的情况下在线切换物理驱动器，并增大。XFS 不支持缩小卷。因此，您无法缩小使用 XFS 格式的卷的大小。
   - **ext4** 文件系统支持逻辑卷，在不停止工作的情况下在线切换物理驱动器，并缩减。

   您还可以使用 LUKS(Linux Unified Key Setup)加密选择版本，该加密允许您使用密码短语加密卷。

10. 在 **At boot** 下拉菜单中选择您要何时挂载卷。

11. 点 **Format and mount** 或 **Format only**。
    根据使用的格式化选项和卷大小，格式化的过程可能需要几分钟。



验证

- 成功完成后，您可以在 **Storage** 选项卡和 LVM2 volume group 选项卡中看到格式化的 VDO 卷的详情。

23.4. 在 WEB 控制台中扩展 VDO 卷

在 RHEL 9 web 控制台中扩展 VDO 卷。

先决条件

- **cockpit-storaged** 软件包已安装在您的系统上。
- 已创建的 VDO 卷。

流程

1. 登录到 RHEL 9 web 控制台。
   详情请参阅 登录到 web 控制台。
2. 点击 **Storage**。
3. 在 **VDO Devices** 框中点您的 VDO 卷。
4. 在 VDO 卷详情中点 **Grow** 按钮。
5. 在 **Grow logical size of VDO** 对话框中，扩展 VDO 卷的逻辑大小。

1. 点 **Grow**。

验证步骤

- 检查 VDO 卷详情中的新大小，以验证您的更改是否成功。

第 24 章 使用 WEB 控制台建立 STRATIS 文件系统

Stratis 作为服务运行，来管理物理存储设备池，简化本地存储管理，易于使用，同时帮助您设置和管理复杂的存储配置。

24.1. 使用 WEB 控制台创建一个未加密的 STRATIS 池

您可以使用 Web 控制台从一个或多个块设备创建一个未加密的 Stratis 池。

先决条件

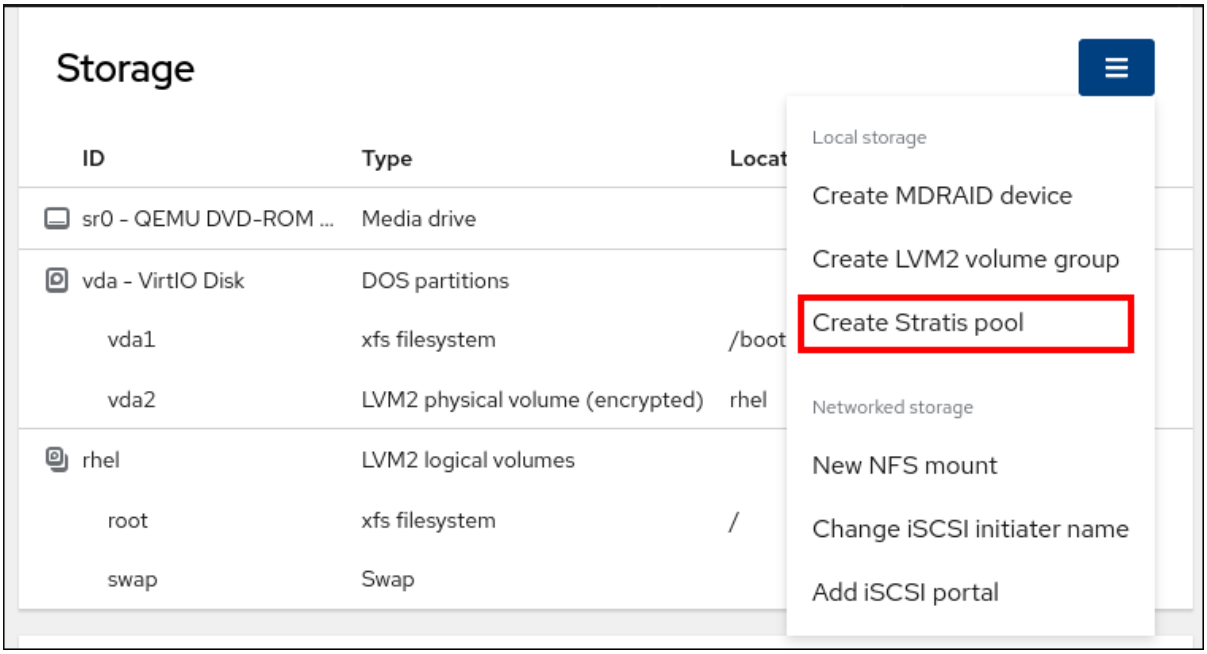
- RHEL 9 web 控制台已安装并启用。详情请参阅安装 Web 控制台。
- Stratis 已安装。
  默认情况下，web 控制台会检测并安装 Stratis。但是，要手动安装 Stratis，请参阅 安装 Stratis。
- **stratisd** 服务在运行。
- 创建 Stratis 池的块设备没有被使用，且没有被挂载。
- 要在其上创建 Stratis 池的每个块设备至少为 1 GB。

注意

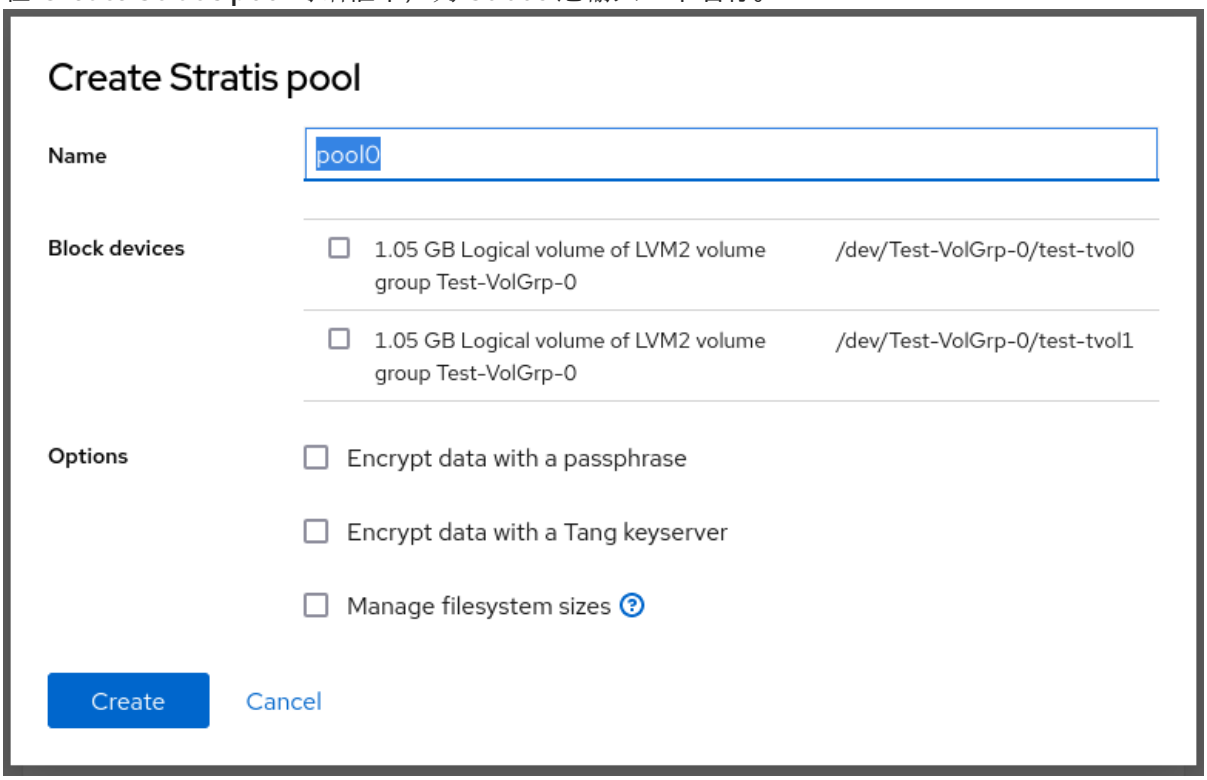
您不能在其创建后加密一个未加密的 Stratis 池。

流程

1. 登录到 RHEL 9 web 控制台。
2. 点 **Storage**。
3. 在 **Storage** 表中，点菜单按钮。
4. 从下拉菜单中选择 **Create Stratis pool**。



5. 在 **Create Stratis pool**对话框中，为 Stratis 池输入一个名称。



6. 选择您要从中创建 Stratis 池的**Block devices**。
7. **可选：**如果要为池中创建的每个文件系统指定最大大小，请选择 **Manage filesystem sizes**。
8. 点 **Create**。

验证

- 进到 **Storage** 部分，并确认您可以在 **Devices** 表中看到新的 Stratis 池。

24.2. 使用 WEB 控制台创建一个加密的 STRATIS 池

要保护您的数据，您可以使用 Web 控制台从一个或多个块设备创建一个加密的 Stratis 池。

当从一个或多个块设备创建加密的 Stratis 池时，请注意以下几点：

- 每个块设备都使用 cryptsetup 库进行加密，并实施 LUKS2 格式。
- 每个 Stratis 池都可以有一个唯一的密钥，或者与其他池共享相同的密钥。这些密钥保存在内核密钥环中。
- 组成 Stratis 池的块设备必须全部加密或者全部未加密。不可能同时在同一个 Stratis 池中加密和未加密块设备。
- 添加到加密 Stratis 池的数据层中的块设备会自动加密。

先决条件

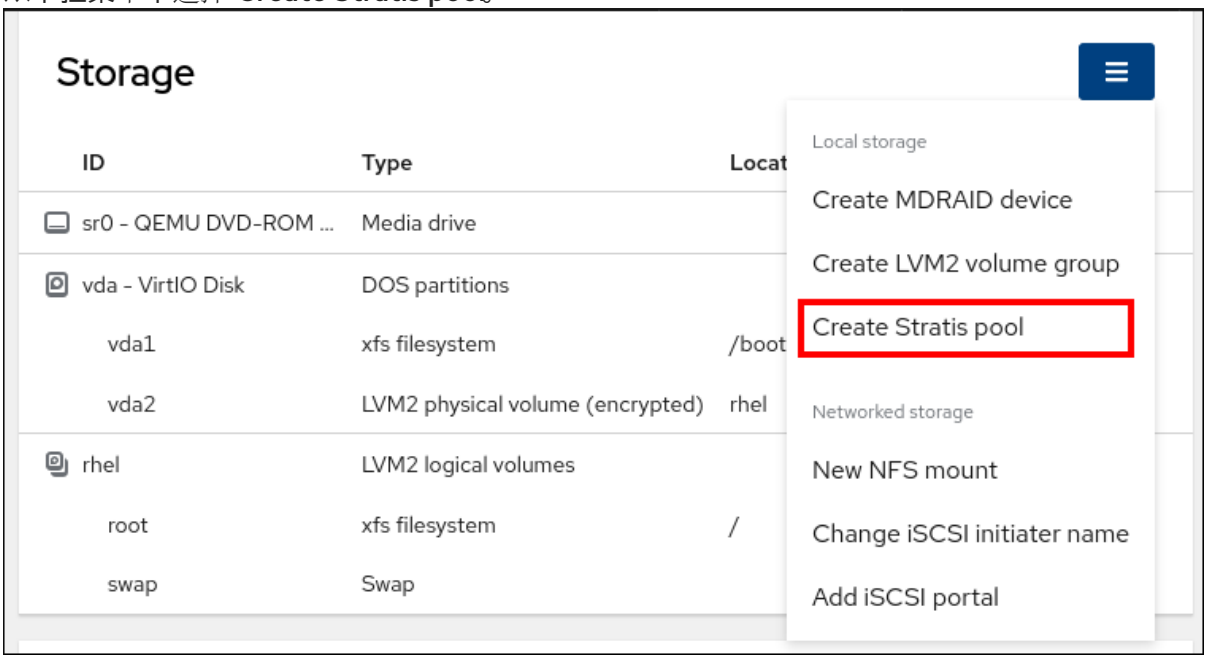
- RHEL 9 web 控制台已安装并启用。详情请参阅安装 Web 控制台。
- Stratis v2.1.0 或更高版本已安装。

默认情况下，web 控制台会检测并安装 Stratis。但是，要手动安装 Stratis，请参阅 安装 Stratis。

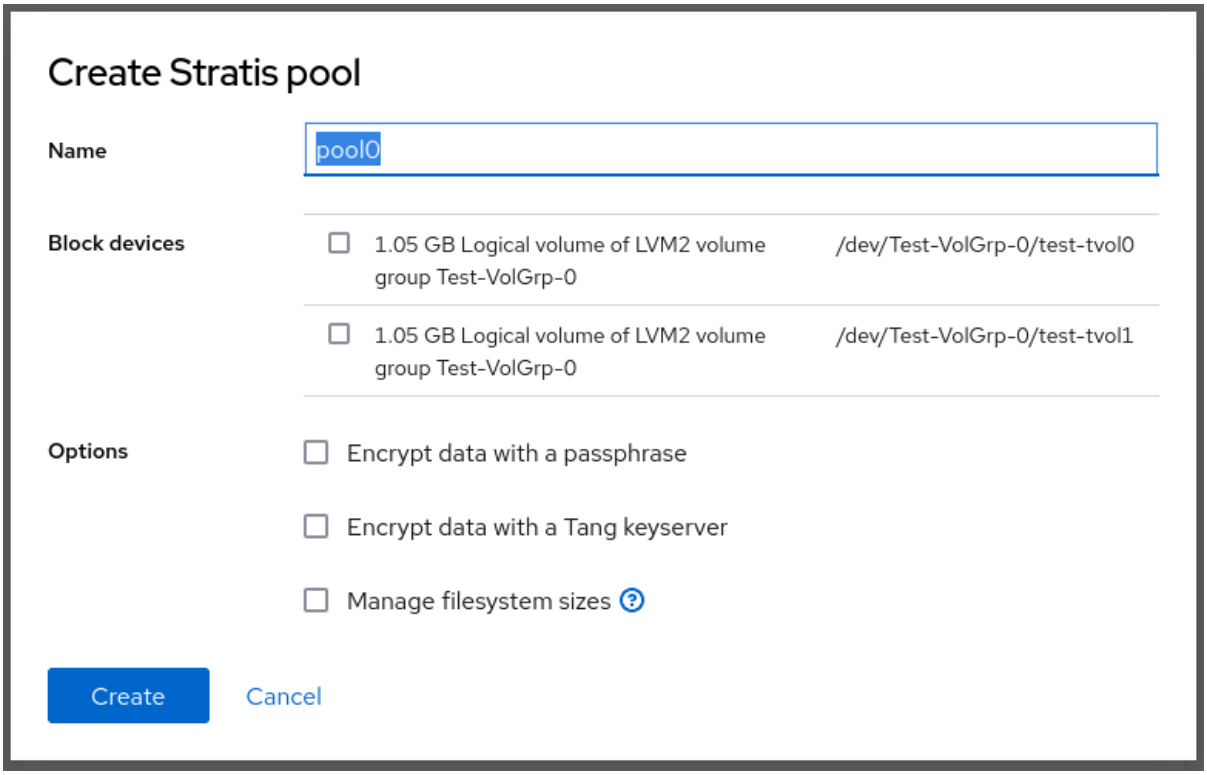
- **stratisd** 服务在运行。
- 创建 Stratis 池的块设备没有被使用，且没有被挂载。
- 要在其上创建 Stratis 池的每个块设备至少为 1 GB。

流程

1. 登录到 RHEL 9 web 控制台。
2. 点 **Storage**。
3. 在 **Storage** 表中，点菜单按钮。
4. 从下拉菜单中选择 **Create Stratis pool**。



5. 在 **Create Stratis pool**对话框中，为 Stratis 池输入一个名称。



6. 选择您要从中创建 Stratis 池的**Block devices**。
7. 选择加密类型，您可以使用密码短语、Tang keyserver 或两者：
   - passphrase:
     i. 输入密码短语。
     ii. 确认密码短语
   - Tang keyserver ：
     i. 输入 keyserver 地址。如需更多信息，请参阅 部署 SELinux 为 enforcing 模式的 Tang 服务器。
8. **可选：**如果要为池中创建的每个文件系统指定最大大小，请选择 **Manage filesystem sizes**。
9. 点 **Create**。

验证

- 进到 **Storage** 部分，并确认您可以在 **Devices** 表中看到新的 Stratis 池。

24.3. 使用 WEB 控制台查看 STRATIS 池

您可以使用 Web 控制台查看现有的 Stratis 池，以及其包含的文件系统。

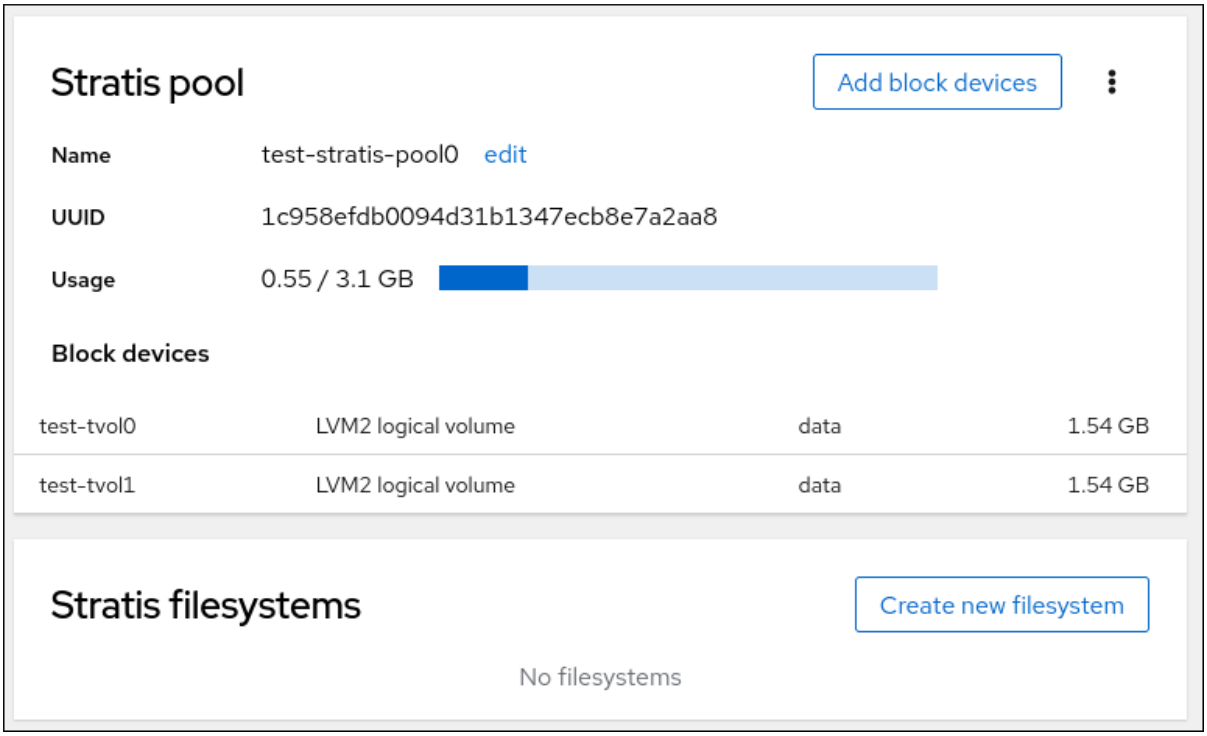
先决条件

- RHEL 9 web 控制台已安装并启用。详情请参阅安装 Web 控制台。
- Stratis 已安装。
  默认情况下，web 控制台会检测并安装 Stratis。但是，要手动安装 Stratis，请参阅 安装 Stratis。

- **stratisd** 服务在运行。
- 您有一个现有的 Stratis 池。请参阅创建未加密的 Stratis 池或创建加密的 Stratis 池。

流程

1. 登录到 RHEL 9 web 控制台。
2. 点 **Storage**。
3. 在 **Storage** 表中，点您要查看的 Stratis 池。
   Stratis 池页面显示有关池以及您在池中创建的文件系统的所有信息。



24.4. 使用 WEB 控制台在 STRATIS 池上创建一个文件系统

您可以使用 Web 控制台在现有 Stratis 池中创建一个文件系统。

先决条件

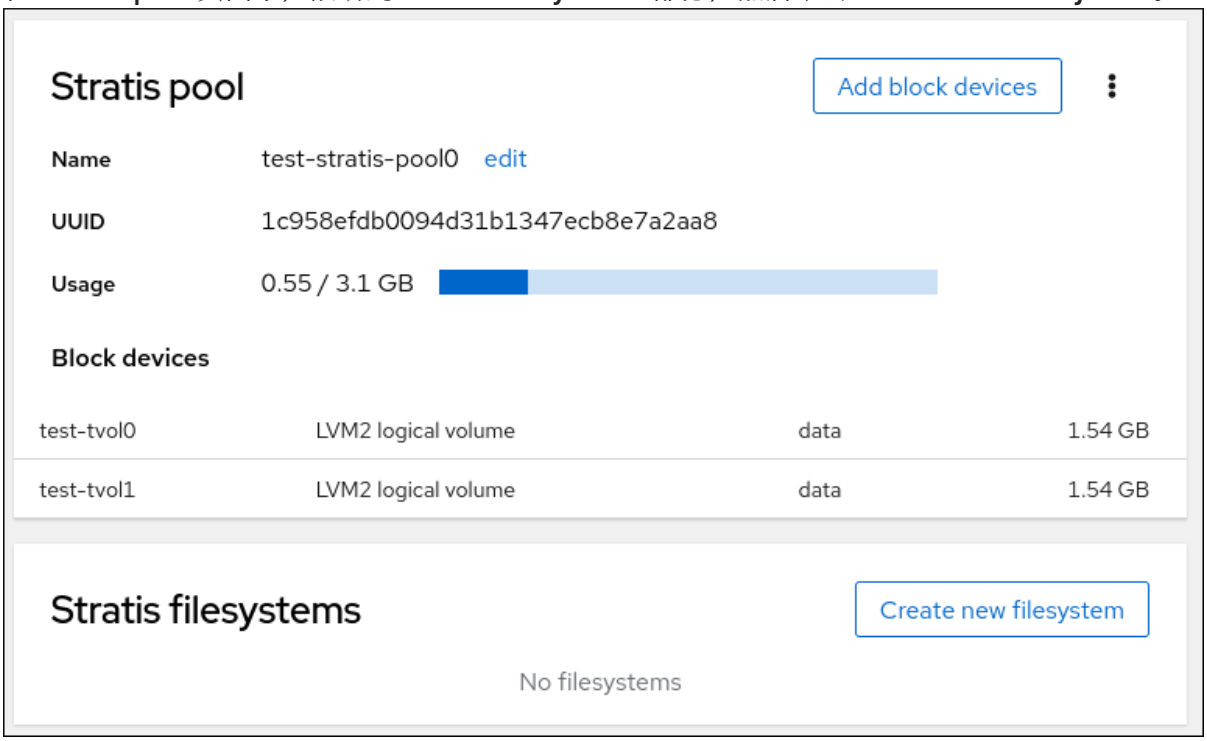
- RHEL 9 web 控制台已安装并启用。详情请参阅安装 Web 控制台。
- Stratis 已安装。
  默认情况下，web 控制台会检测并安装 Stratis。但是，要手动安装 Stratis，请参阅 安装 Stratis。
- **stratisd** 服务在运行。
- 一个 Stratis 池已创建。请参阅创建未加密的 Stratis 池或创建加密的 Stratis 池。

流程

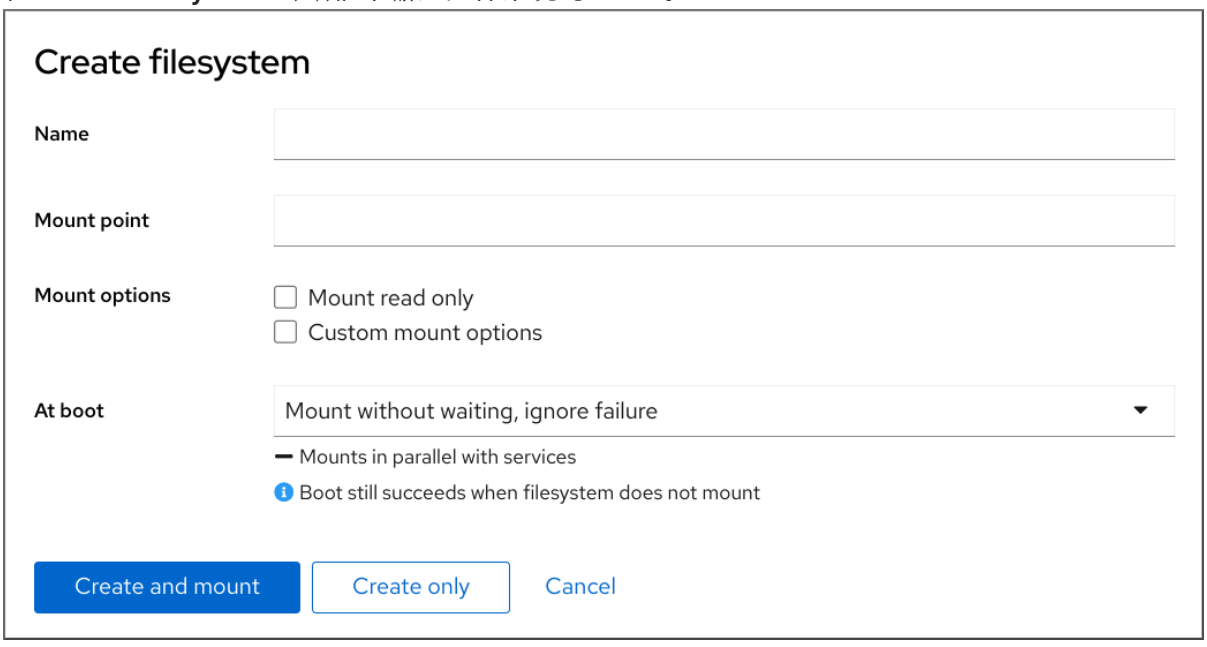
1. 登录到 RHEL 9 web 控制台。
2. 点 **Storage**。

3. 点击您要在其上创建文件系统的 Stratis 池。

4. 在 **Stratis pool** 页面中，滚动到 **Stratis filesystems** 部分，然后单击 **Create new filesystem**。



5. 在 **Create filesystem** 对话框中输入文件系统的**Name**。



6. 输入文件系统的**Mount point**。

7. 选择 **Mount option**。

8. 在 **At boot** 下拉菜单中选择您要何时挂载文件系统。

9. 创建文件系统：

   - 如果要创建并挂载文件系统，点 **Create and mount**。
   - 如果您只想创建文件系统，请单击 **Create only**。

验证

- 新文件系统在 **Stratis filesystems** 选项卡下的 **Stratis pool** 页面中可见。

24.5. 使用 WEB 控制台从 STRATIS 池中删除一个文件系统

您可以使用 Web 控制台从现有 Stratis 池中删除一个文件系统。

注意

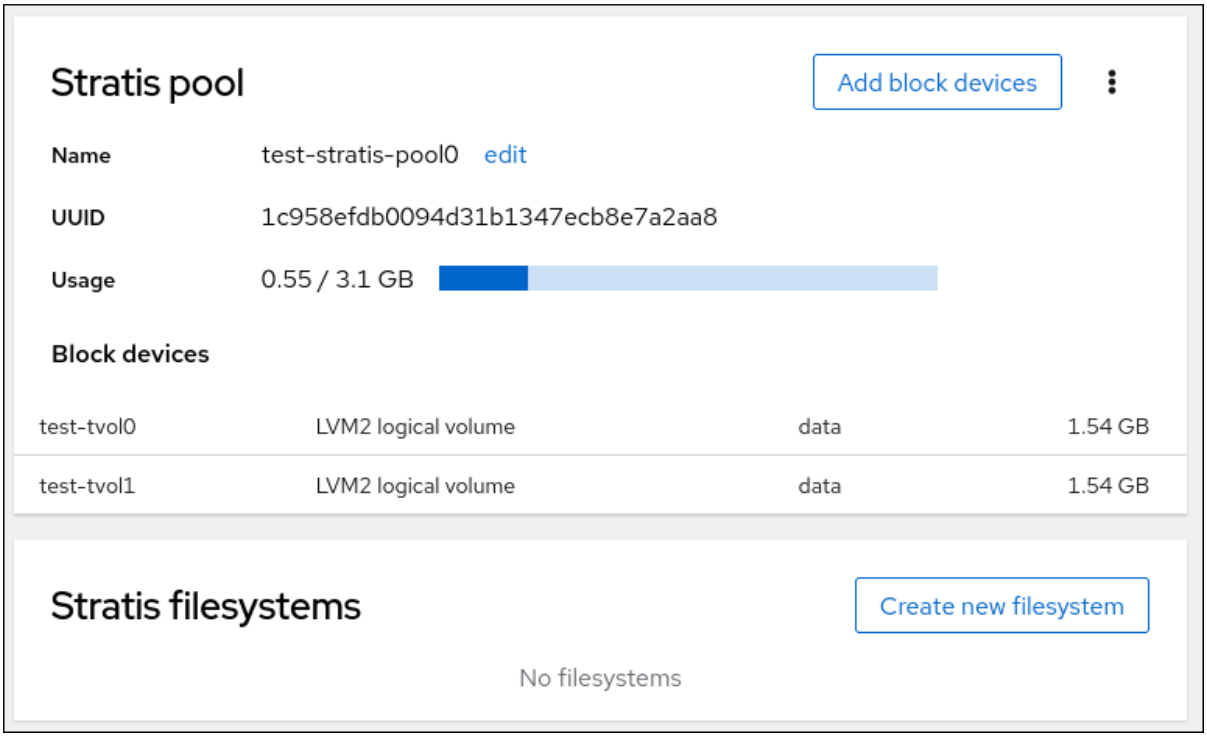
删除 Stratis 池文件系统会删除其包含的所有数据。

先决条件

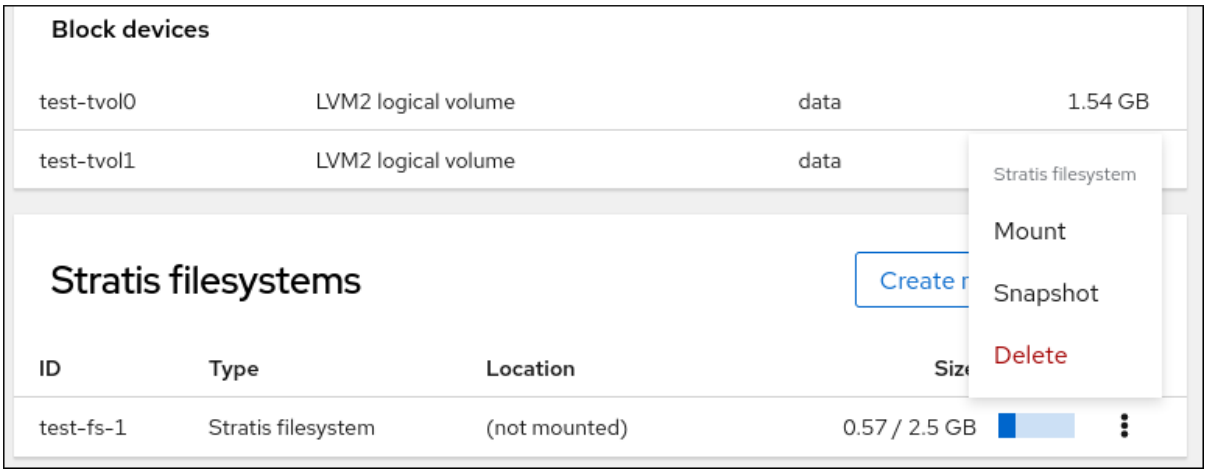
- RHEL 9 web 控制台已安装并启用。详情请参阅安装 Web 控制台。
- Stratis 已安装。
  默认情况下，web 控制台会检测并安装 Stratis。但是，要手动安装 Stratis，请参阅 安装 Stratis。
- **stratisd** 服务在运行。
- 您有一个现有的 Stratis 池。请参阅创建未加密的 Stratis 池或创建加密的 Stratis 池。
- 您已在 Stratis 池上创建了一个文件系统。请参阅 在 Stratis 池上创建一个文件系统。

流程

1. 登录到 RHEL 9 web 控制台。
2. 点 **Storage**。
3. 在 **Storage** 表中，点击您要从中删除文件系统的 Stratis 池。
4. 在 **Stratis pool** 页面中，滚动到 **Stratis filesystems** 部分，然后点击您要删除的文件系统旁的菜单按钮 ⋮。



5. 从下拉菜单中选择 **delete**。



6. 在 **Confirm deletion** 对话框中，单击 **Delete**。

24.6. 使用 WEB 控制台重命名 STRATIS 池

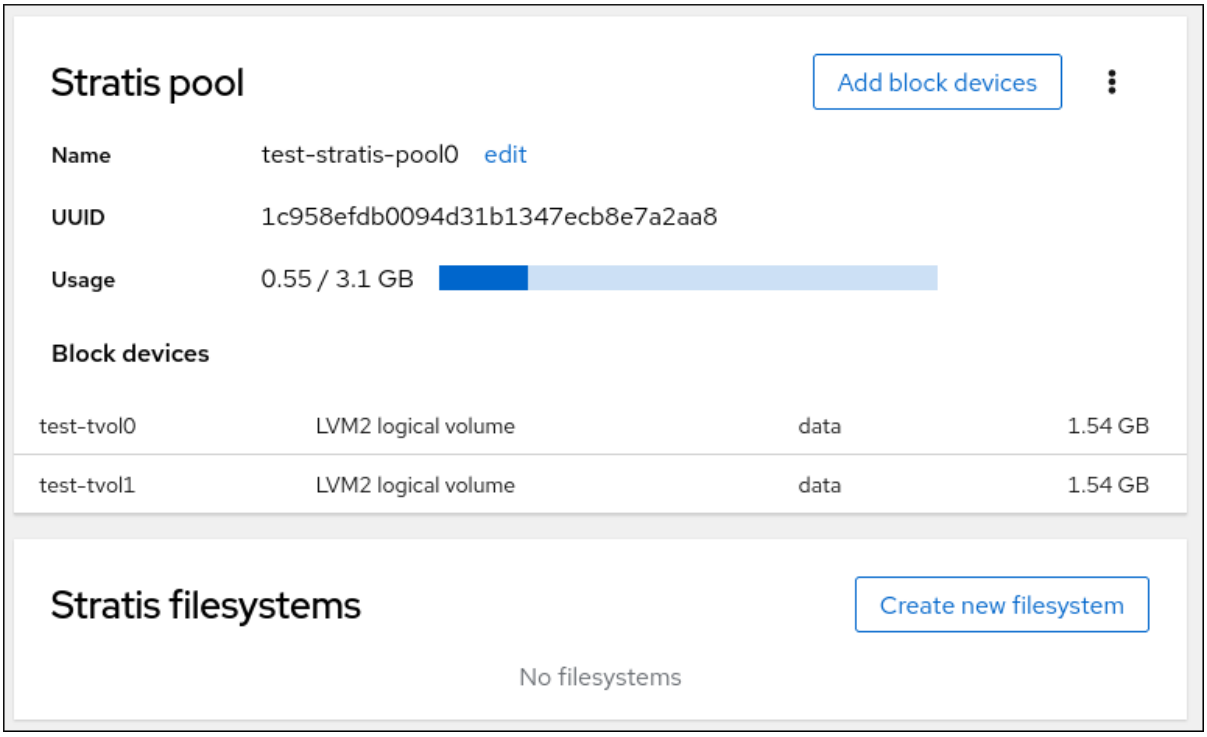
您可以使用 Web 控制台重命名现有的 Stratis 池。

先决条件

- RHEL 9 web 控制台已安装并启用。详情请参阅安装 Web 控制台。
- Stratis 已安装。
  默认情况下，web 控制台会检测并安装 Stratis。但是，要手动安装 Stratis，请参阅 安装 Stratis。
- **stratisd** 服务在运行。
- 一个 Stratis 池已创建。请参阅创建未加密的 Stratis 池或创建加密的 Stratis 池。

流程

1. 登录到 RHEL 9 web 控制台。
2. 点 **Storage**。
3. 在 **Storage** 表中，点您要重命名的 Stratis 池。
4. 在 **Stratis pool** 页面中，点 **Name** 字段旁边的 **edit**。



5. 在 **Rename Stratis pool** 对话框中输入新名称。
6. 点 **Rename**。

24.7. 使用 WEB 控制台向 STRATIS 池中添加块设备

您可以使用 Web 控制台向现有 Stratis 池中添加块设备。您还可以将缓存添加为块设备。

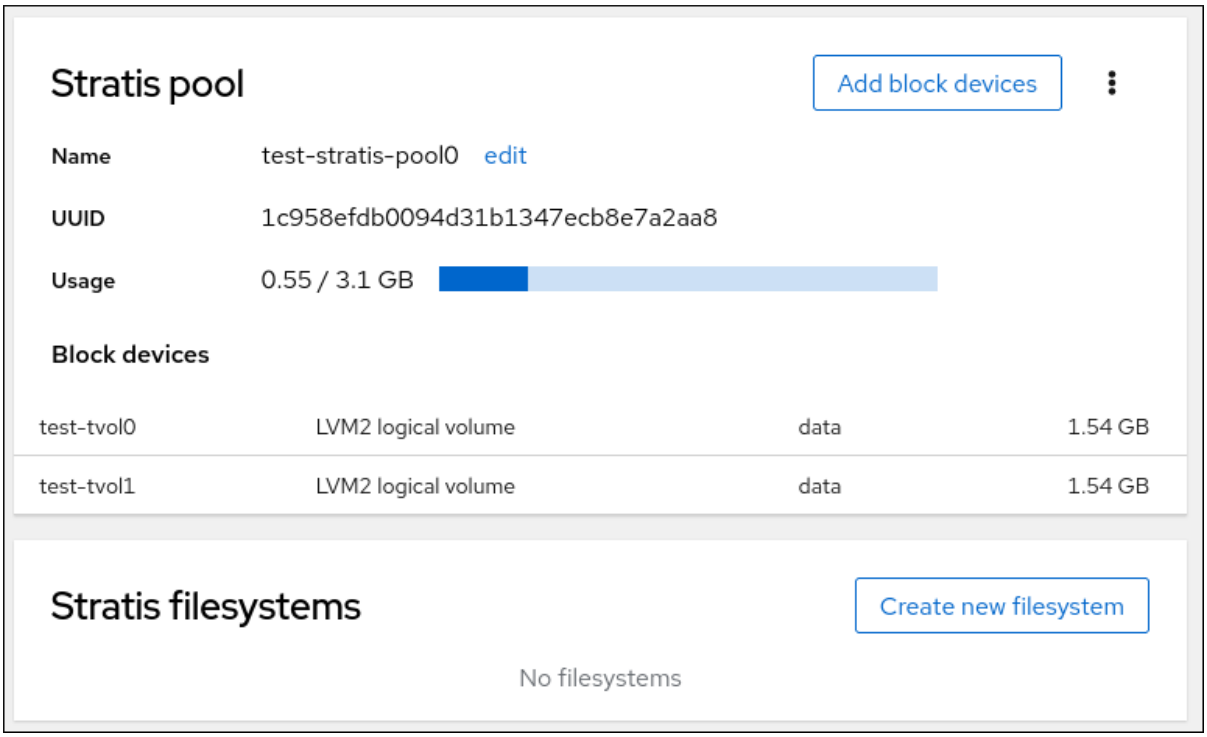
先决条件

- RHEL 9 web 控制台已安装并启用。详情请参阅安装 Web 控制台。
- Stratis 已安装。
  默认情况下，web 控制台会检测并安装 Stratis。但是，要手动安装 Stratis，请参阅 安装 Stratis。
- **stratisd** 服务在运行。
- 一个 Stratis 池已创建。请参阅创建未加密的 Stratis 池或创建加密的 Stratis 池。
- 创建 Stratis 池的块设备没有被使用，且没有被挂载。
- 要在其上创建 Stratis 池的每个块设备至少为 1 GB。

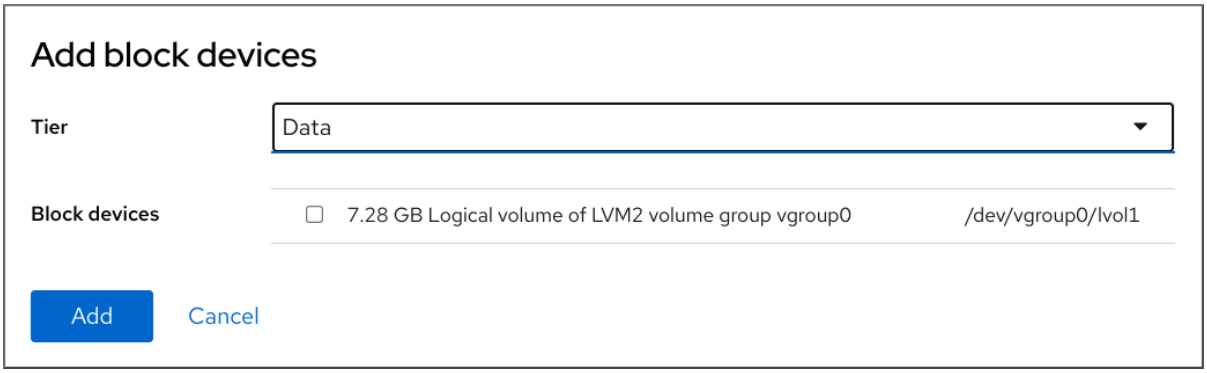
流程

1. 登录到 RHEL 9 web 控制台。

2. 点 **Storage**。
3. 在 **Storage** 表中，点您要向其添加块设备的 Stratis 池。
4. 在 **Stratis 池** 页面中，单击 **Add block devices**。



5. 在 **Add block devices** 对话框中，选择 **Tier**，无论您要将块设备添加为数据还是缓存。



6. **可选：**如果您要将块设备添加到使用密码短语加密的 Stratis 池中，则必须输入密码短语。
7. 在 **Block devices** 下，选择要添加到池中的设备。
8. 点击 **Add**。

24.8. 使用 WEB 控制台删除 STRATIS 池

您可以使用 Web 控制台删除现有的 Stratis 池。

注意

删除 Stratis 池会删除其包含的所有数据。

先决条件

- RHEL 9 web 控制台已安装并启用。详情请参阅安装 Web 控制台。
- Stratis 已安装。
  默认情况下，web 控制台会检测并安装 Stratis。但是，要手动安装 Stratis，请参阅 安装 Stratis。
- **stratisd** 服务在运行。
- 您有一个现有的 Stratis 池。请参阅创建未加密的 Stratis 池或创建加密的 Stratis 池。

流程

1. 登录到 RHEL 9 web 控制台。
2. 点 **Storage**。
3. 在 **Storage** 表中，点您要删除的 Stratis 池旁边的菜单按钮 ⋮。
4. 从下拉菜单中选择 **Delete pool**。
5. 在 **Permanently delete pool** 对话框中，单击 **Delete**。

第 25 章 在 RHEL WEB 控制台中使用 LUKS 密码锁定数据

在 Web 控制台的 **Storage** 选项卡中，您现在可以使用 LUKS(Linux Unified Key Setup)版本 2 格式创建、锁定、解锁、调整大小和其他配置加密设备。

这个 LUKS 的新版本提供：

- 更灵活的解锁策略
- 更强大的加密
- 更好地与将来的更改兼容

先决条件

- 已安装 RHEL 9 web 控制台。详情请参阅安装 Web 控制台。
- **cockpit-storaged** 软件包已安装在您的系统上。

25.1. LUKS 磁盘加密

Linux Unified Key Setup-on-disk-format (LUKS)提供了一组简化管理加密设备的工具。使用 LUKS，您可以加密块设备，并使多个用户密钥能够解密主密钥。要批量加密分区，请使用这个主密钥。

Red Hat Enterprise Linux 使用 LUKS 执行块设备加密。默认情况下，在安装过程中不选中加密块设备的选项。如果您选择加密磁盘的选项，则系统会在每次引导计算机时都提示您输入密码短语。这个密码短语解锁了解密分区的批量加密密钥。如果要修改默认分区表，您可以选择要加密的分区。这是在分区表设置中设定的。

加密系统

LUKS 使用的默认密码是 **aes-xts-plain64**。LUKS 的默认密钥大小为 512 字节。 **Anaconda** XTS 模式的 LUKS 的默认密钥大小为 512 位。以下是可用密码：

- 高级加密标准(AES)
- Twofish
- Serpent

LUKS 执行的操作

- LUKS 对整个块设备进行加密，因此非常适合保护移动设备的内容，如可移动存储介质或笔记本电脑磁盘驱动器。
- 加密块设备的底层内容是任意的，这有助于加密交换设备。对于将特殊格式化块设备用于数据存储的某些数据库，这也很有用。
- LUKS 使用现有的设备映射器内核子系统。
- LUKS 增强了密码短语，防止字典攻击。
- LUKS 设备包含多个密钥插槽，这意味着您可以添加备份密钥或密码短语。

重要

以下情况不建议使用 LUKS：

- LUKS 等磁盘加密解决方案仅在您的系统关闭时保护数据。在系统启动并且 LUKS 解密磁盘后，该磁盘上的文件对有权访问它们的用户可用。
- 需要多个用户对同一设备具有不同的访问密钥的情况。LUKS1 格式提供八个密钥插槽，LUKS2 提供最多 32 个密钥插槽。
- 需要文件级加密的应用程序。

其它资源

- LUKS 项目主页
- LUKS 磁盘格式规范
- FIPS 197:高级加密标准(AES)

25.2. 在 WEB 控制台中配置 LUKS 密码短语

如果要在系统中的现有逻辑卷中添加加密，则只能通过格式化卷进行。

先决条件

- 必须安装并可以访问 Web 控制台。详情请参阅安装 Web 控制台。
- **cockpit-storaged** 软件包已安装在您的系统上。
- 在没有加密的情况下可用的现有逻辑卷.

流程

1. 登录到 RHEL 9 web 控制台。
   详情请参阅 登录到 web 控制台。
2. 点击 **Storage**。
3. 在 **Storage** 表中，单击您要加密的存储设备旁边的菜单按钮 ⋮。
4. 从下拉菜单中选择 **Format**。
5. 在 **Encryption field** 中，选择加密规格 **LUKS1** 或 **LUKS2**。
6. 设置并确认您的新密码短语。
7. [可选] 修改进一步加密选项。
8. 完成格式化设置。
9. 点 **Format**。

25.3. 在 WEB 控制台中更改 LUKS 密码短语

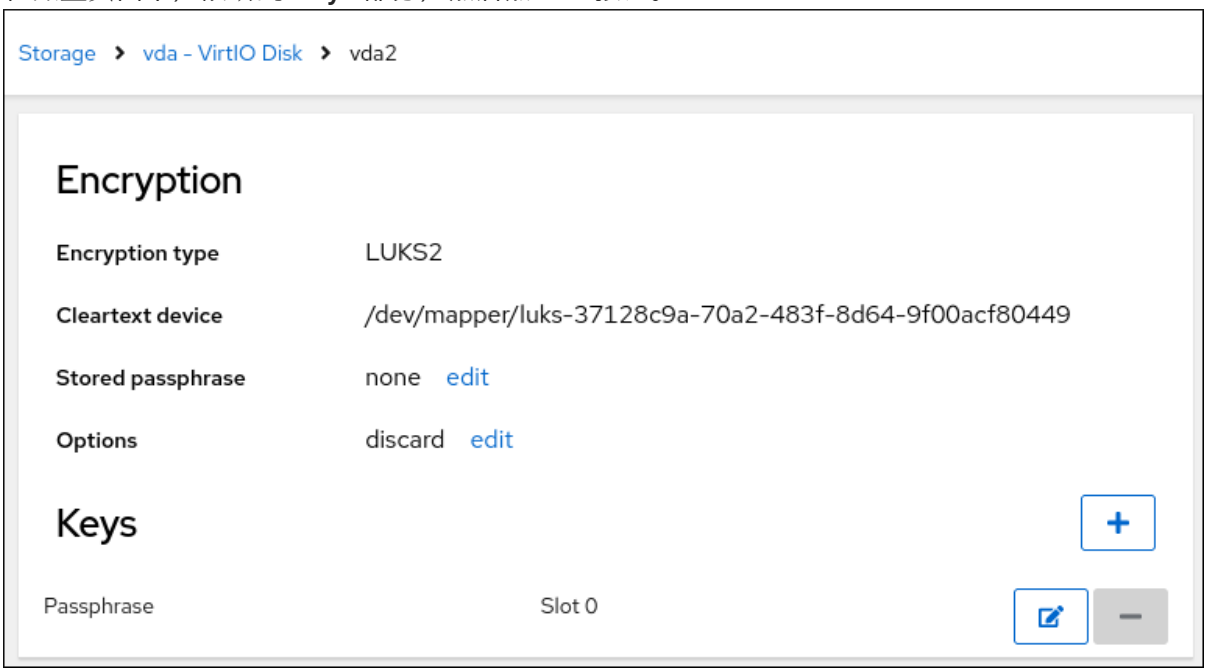
在 web 控制台中的加密磁盘或分区上更改 LUKS 密码短语。

先决条件

- 必须安装并可以访问 Web 控制台。详情请参阅安装 Web 控制台。
- **cockpit-storaged** 软件包已安装在您的系统上。

流程

1. 登录到 web 控制台。详情请参阅 登录到 web 控制台。
2. 点 **Storage**
3. 在 **Storage** 表中，选择带有加密数据的磁盘。
4. 在磁盘页面中，滚动到 **Keys** 部分，然后点 edit 按钮。



5. 在**更改密码短语**对话框中：
   a. 输入您当前的密码短语。
   b. 输入您的新密码短语。
   c. 确认您的新密码短语。

6. 点 **Save**

第 26 章 在 WEB 控制台中使用 TANG 密钥配置自动解锁

您可以使用 Tang 服务器提供的密钥配置 LUKS 加密存储设备的自动解锁。

先决条件

- 已安装 RHEL 9 web 控制台。详情请参阅 安装 web 控制台。
- **cockpit-storaged** 和 **clevis-luks** 软件包已安装在您的系统上。
- **cockpit.socket**服务运行在9090端口。
- Tang 服务器可用。详情请参阅 部署 SELinux 处于 enforcing 模式的 Tang 服务器 。

流程

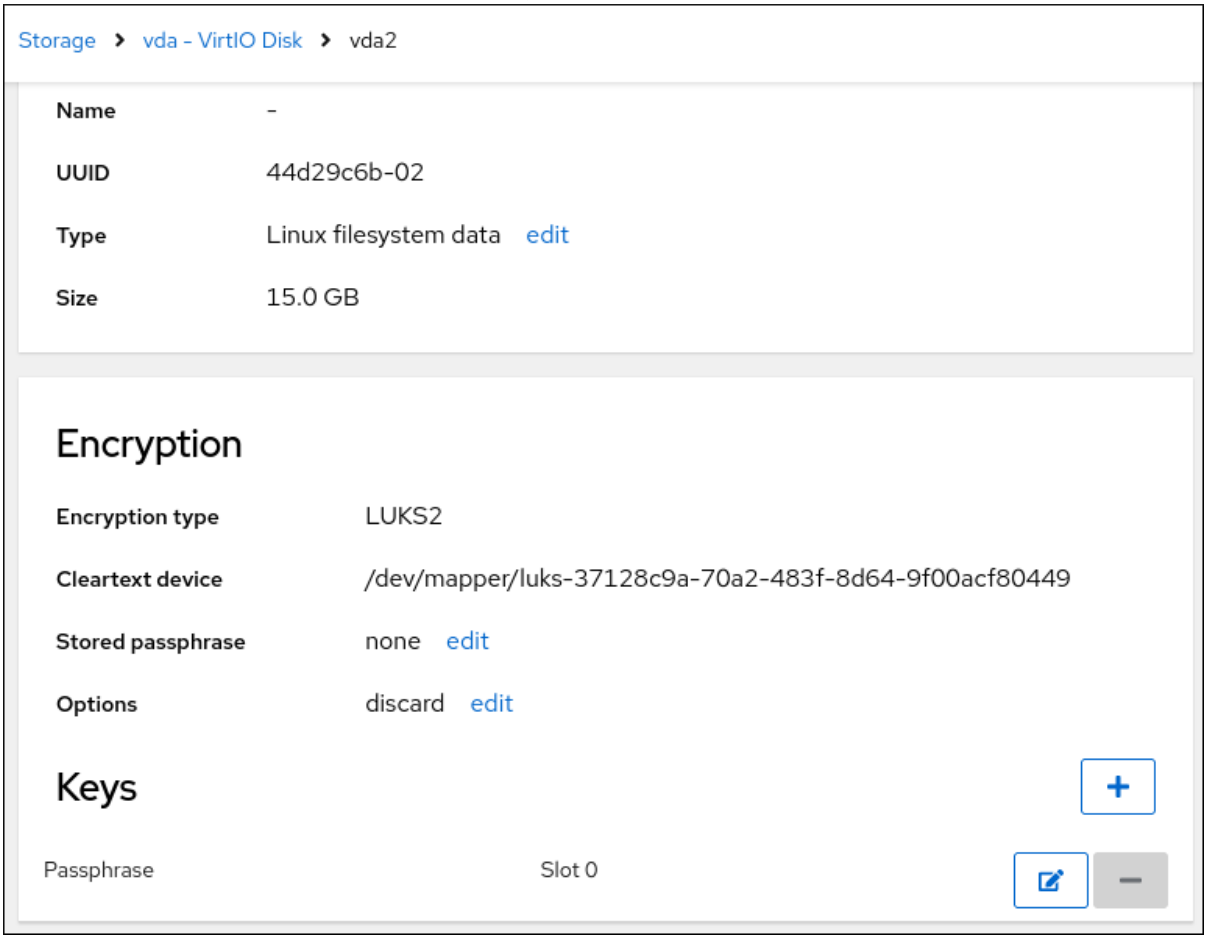
1. 在 web 浏览器中输入以下地址来打开 RHEL web 控制台：

   ```
   https://<localhost>:9090
   ```

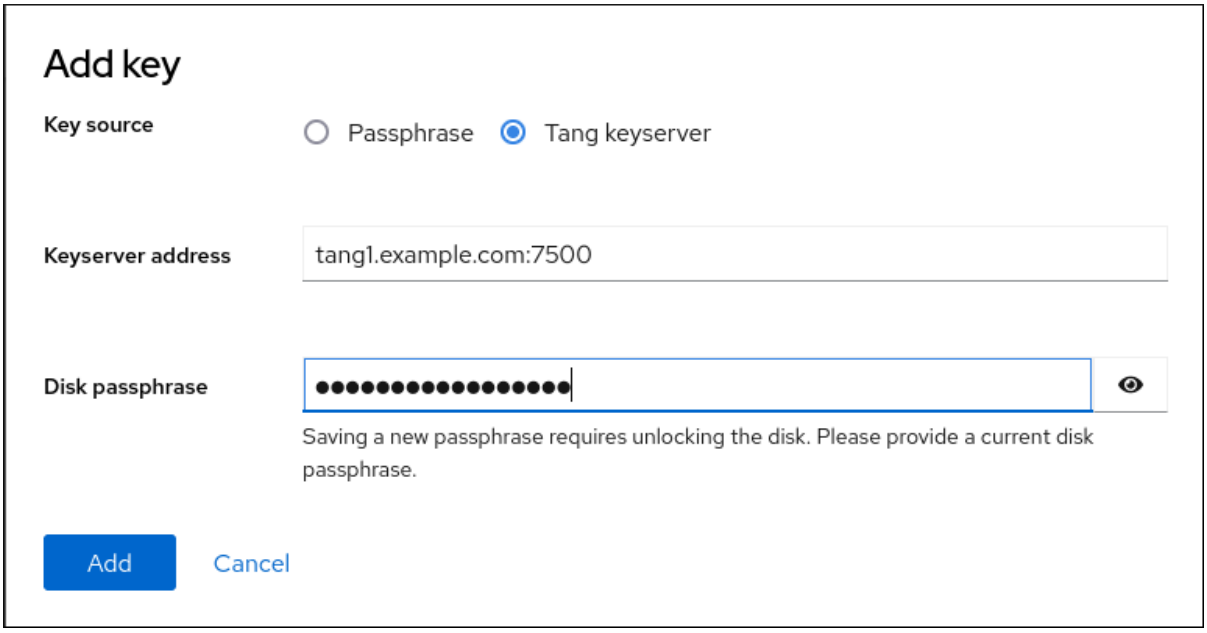
   连接到远程系统时，将 *<localhost>* 部分替换为远程服务器的主机名或 IP 地址。

2. 提供您的凭证并点击 **Storage**。在 **Storage** 表中，点包含您计划添加的加密卷的磁盘，来自动解锁。

3. 在以下带有所选磁盘详情的页面中，点 **Keys** 部分中的 **+** 来添加 Tang 密钥：



4. 选择 **Tang keyserver** 作为 **Key source**，提供 Tang 服务器的地址，以及解锁 LUKS 加密设备的密码。点击 **Add** 确认：



以下对话框窗口提供了一个命令来验证密钥哈希是否匹配。

5. 在 Tang 服务器上的终端中，使用 **tang-show-keys** 命令来显示密钥哈希以进行比较。在本例中，Tang 服务器运行在端口 *7500* 上：

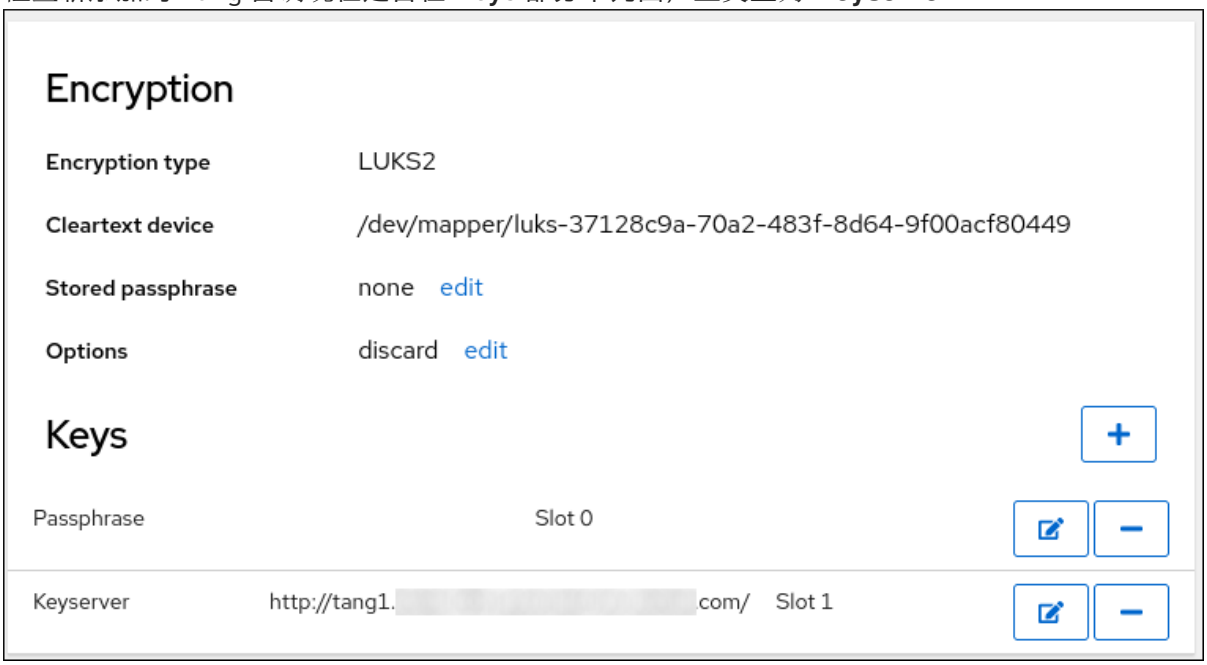
```
# tang-show-keys 7500
x100_1k6GPiDOaMlL3WbpCjHOy9ul1bSfdhI3M08wO0
```

6. 当 web 控制台中的密钥哈希与之前列出的命令的输出中的密钥哈希相同时，请点击 **Trust key**：

7. 在 RHEL 9.2 及更高版本中，选择了加密的根文件系统和 Tang 服务器后，您可以跳过向内核命令行中添加 **rd.neednet=1** 参数，安装 **clevis-dracut** 软件包，并重新生成一个初始 RAM 磁盘 (**initrd**)。对于非 root 文件系统，web 控制台现在启用 **remote-cryptsetup.target** 和 **clevis-luks-akspass.path systemd** 单元，安装 **clevis-systemd** 软件包，并将 **_netdev** 参数添加到 **fstab** 和 **crypttab** 配置文件中。

验证

1. 检查新添加的 Tang 密钥现在是否在 **Keys** 部分中列出，且类型为 **Keyserver** ：



2. 验证绑定是否在早期引导时可用，例如：

```
# lsinitrd | grep clevis-luks
lrwxrwxrwx   1 root     root          48 Jan  4 02:56
etc/systemd/system/cryptsetup.target.wants/clevis-luks-askpass.path ->
/usr/lib/systemd/system/clevis-luks-askpass.path
…
```

其它资源

- 使用基于策略的解密配置加密卷的自动解锁

第 27 章 在 WEB 控制台中管理软件更新

了解如何在 RHEL 9 web 控制台中管理软件更新，以及如何自动化它们的方法。

web 控制台中的软件更新模块基于 **dnf** 工具。有关使用 **dnf** 更新软件的更多信息，请参阅更新软件包部分。

27.1. 在 WEB 控制台中管理手动软件更新

您可以使用 Web 控制台手动更新软件。

先决条件

- 必须安装并可以访问 Web 控制台。详情请参阅安装 Web 控制台。

流程

1. 登录到 RHEL 9 web 控制台。
   详情请参阅 登录到 web 控制台。
2. 点**软件更新**。
   如果最后一次检查发生时间超过 24 小时，可用更新列表会自动刷新。要触发刷新，请点 **Check for Updates** 按钮。
3. 应用更新。您可以在更新运行时监控更新日志。
   a. 要安装所有可用更新，请点**安装所有更新**按钮。
   b. 如果您有可用的安全更新，请点击**安装安全更新**按钮单独安装它们。
   c. 如果您有 kpatch 更新可用，请点 **Install kpatch 更新**按钮单独安装它们。
4. 可选：您可以选择 **Reboot after completion** 来自动重启您的系统。
   如果执行此步骤，您可以跳过这个过程的剩余步骤。
5. 在系统应用更新后，您会看到重启系统的建议。
   特别是，当更新中包含一个您不想单独重启的新内核或系统服务时，我们尤其建议这样做。
6. 点 **Ignore** 以取消重启，或选择 **Restart Now** 重启系统。
   系统重启后，登录 web 控制台并进入 **Software Updates** 页面以验证更新是否成功。

27.2. 在 WEB 控制台中管理自动更新

在 web 控制台中，您可以选择应用所有更新，或者安全更新，以及管理自动更新的定期和时间。

先决条件

- 必须安装并可以访问 Web 控制台。详情请参阅安装 Web 控制台。

流程

1. 登录到 RHEL 9 web 控制台。详情请参阅 登录到 web 控制台。
2. 点**软件更新**。

3. 在 Settings 表中，点 **Edit** 按钮。
4. 挑选一种自动更新类型。您可以选择 **Security updates only** 或 **All updates**。
5. 要修改自动更新的日期，在下拉菜单中点 **every day** 并选择特定日期。
6. 要修改自动更新的时间，请点击 **6:00** 字段并选择或输入特定时间。
7. 如果要禁用自动软件更新，请选择 **No update** 类型。

27.3. 在 WEB 控制台中应用软件更新后管理按需重启

智能重启功能会通知用户是否在应用软件更新后重新引导整个系统，或者是否足以重新启动某些服务。

先决条件

- 必须安装并可以访问 Web 控制台。详情请参阅安装 Web 控制台。

流程

1. 登录到 RHEL 9 web 控制台。详情请参阅 登录到 web 控制台。
2. 点**软件更新**。
3. 对您的系统应用更新。
4. 成功更新后，点 **Reboot system...**, **restart services...**或 **Ignore**
5. 如果您决定忽略，您可以通过执行以下操作之一来返回到重启或重启菜单：
   a. 重新引导：
      i. 点 **Software Updates** 页面的 **Status** 字段中的 **Reboot system** 按钮。
      ii. （可选）将消息写入登录的用户。
      iii. 从 **Delay** 下拉菜单中选择一个延迟。
      iv. 点**Reboot**。
   b. 重启服务：
      i. 点 **Restart services...** 按钮（在 **Software Updates** 页面的 **Status** 字段中）。
      您将看到需要重启的所有服务的列表。
      ii. 点 **重启服务**。
      根据您的选择，系统将重新启动，或者您的服务将重启。

27.4. 在 WEB 控制台中使用内核实时补丁应用补丁

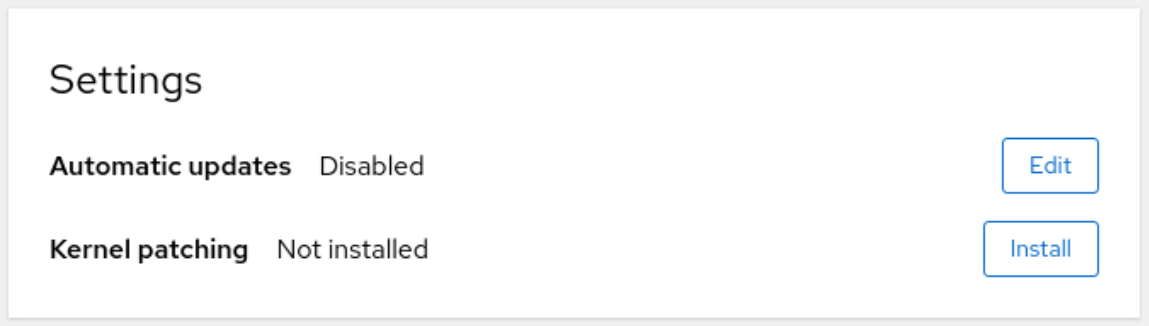
Web 控制台允许用户在不强制使用 **kpatch** 框架强制重启的情况下应用内核安全补丁。以下流程演示了如何设置首选补丁类型。

先决条件

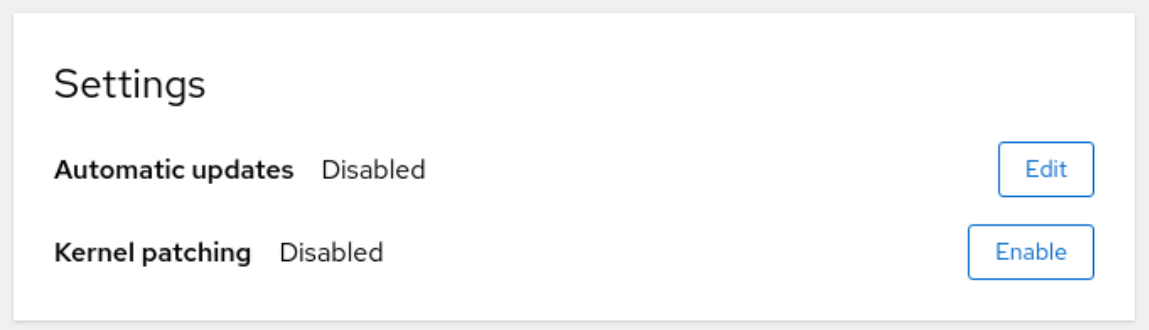
- 必须安装并可以访问 Web 控制台。详情请参阅安装 Web 控制台。

流程

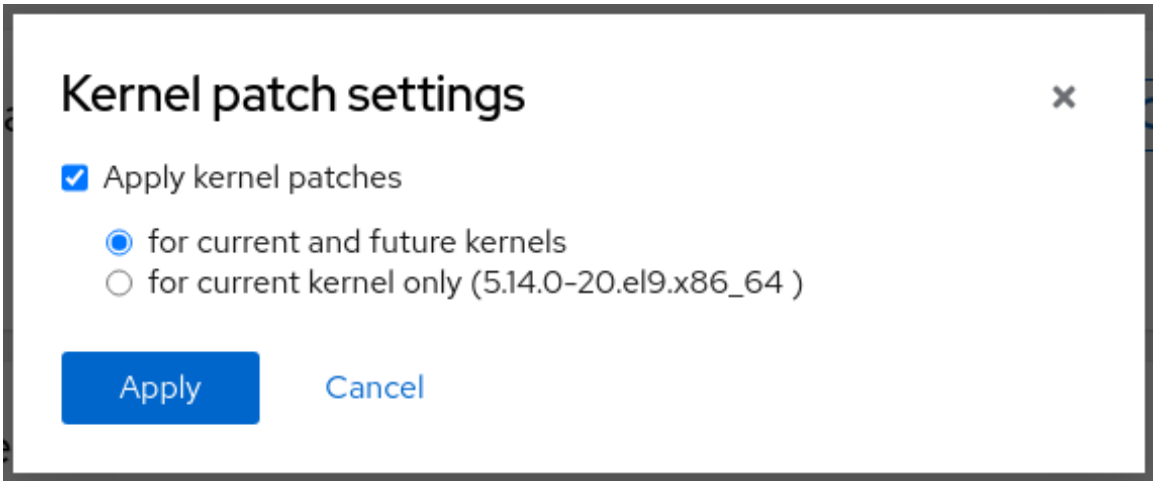
1. 使用管理权限登录到 web 控制台。详情请参阅 登录到 web 控制台。
2. 点**软件更新**。
3. 检查内核补丁设置的状态。
   a. 如果没有安装补丁，点 **Install**。

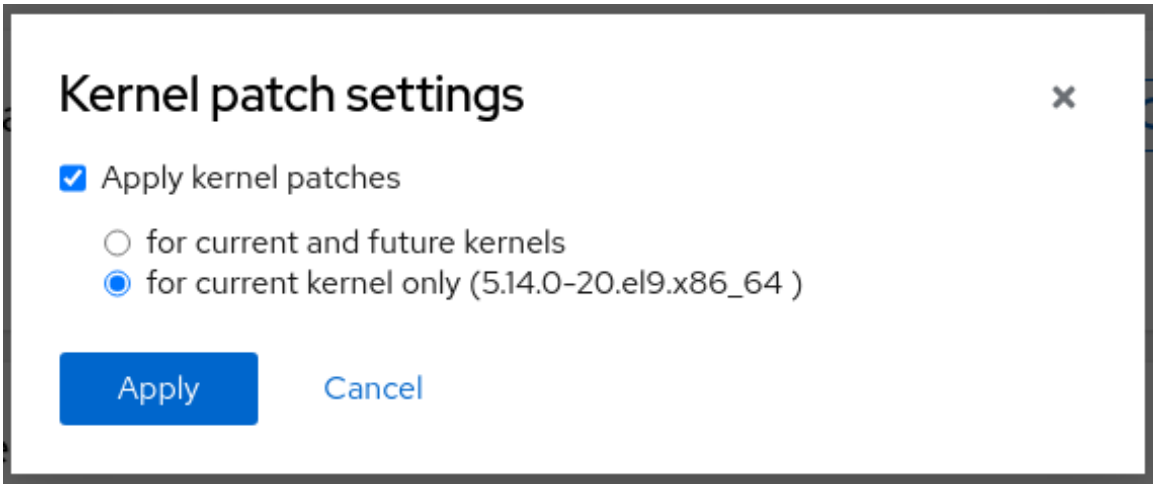


   b. 要启用内核补丁，请点击 **启用**。



   c. 选中应用内核补丁的复选框。
   d. 选择您要为当前和将来的内核应用补丁，还是只针对当前内核应用补丁。如果您选择为将来的内核应用补丁，系统将为后续的内核版本应用补丁。

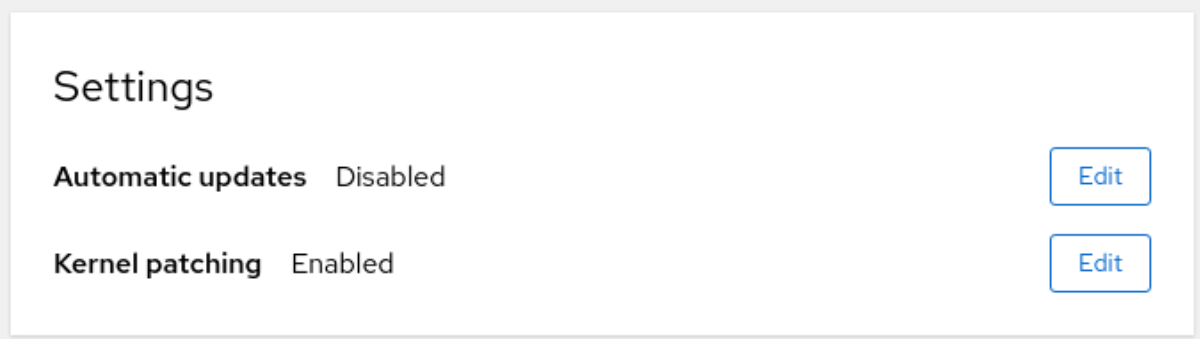




e. 点**应用**。

验证

- 检查内核补丁在 **Software updates** 项的 **Settings** 表中为 **Enabled**。



其它资源

- 使用内核实时修补程序应用补丁

第 28 章 在 WEB 控制台中管理订阅

通过 web 控制台管理 Red Hat Enterprise Linux 9 的订阅。

要获得 Red Hat Enterprise Linux 订阅，您需要在 红帽客户门户网站中有一个帐户或一个激活码。

本章论述了：

- RHEL 9 web 控制台中的订阅管理。
- 在 web 控制台中使用红帽用户名和密码为您的系统注册订阅。
- 使用激活码注册订阅。

先决条件

- 购买了订阅。
- 受订阅限制的系统必须连接到互联网，因为 Web 控制台需要与红帽客户门户网站通信。

28.1. WEB 控制台中的订阅管理

RHEL 9 web 控制台为使用在本地系统中安装的红帽订阅管理器提供了一个界面。

Subscription Manager 连接到红帽客户门户网站，并验证所有可用信息：

- 活跃订阅
- 过期的订阅
- 续订的订阅

如果要续订订阅或在红帽客户门户网站中获取不同的订阅，则不需要手动更新订阅管理器数据。Subscription Manager 会自动将数据与红帽客户门户网站同步。

28.2. 在 WEB 控制台中使用凭证注册订阅

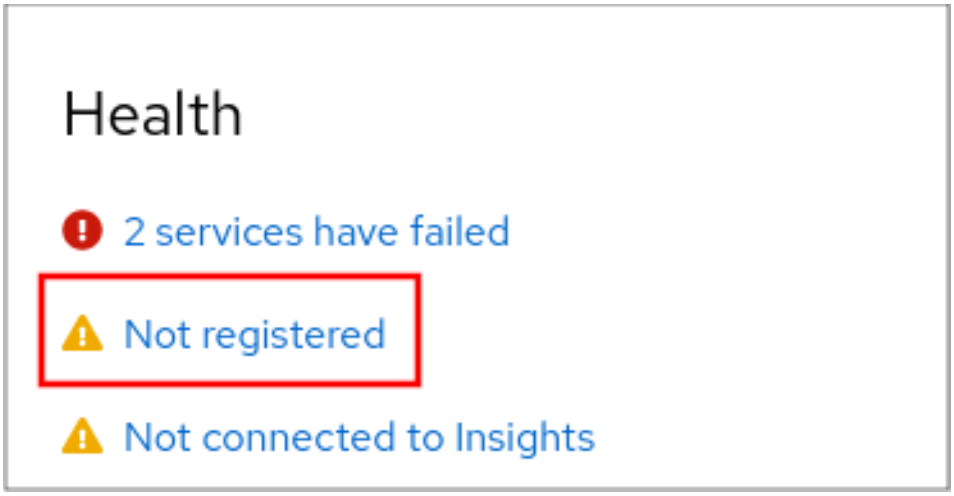
使用以下步骤通过 RHEL web 控制台使用帐户凭证注册新安装的 Red Hat Enterprise Linux。

先决条件

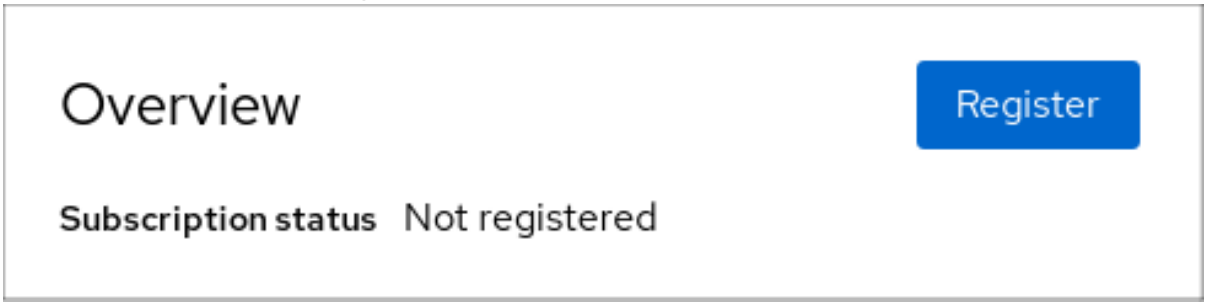
- 红帽客户门户网站中的有效用户帐户。
  请参阅 创建红帽登录 页面。
- RHEL 系统的有效订阅。

流程

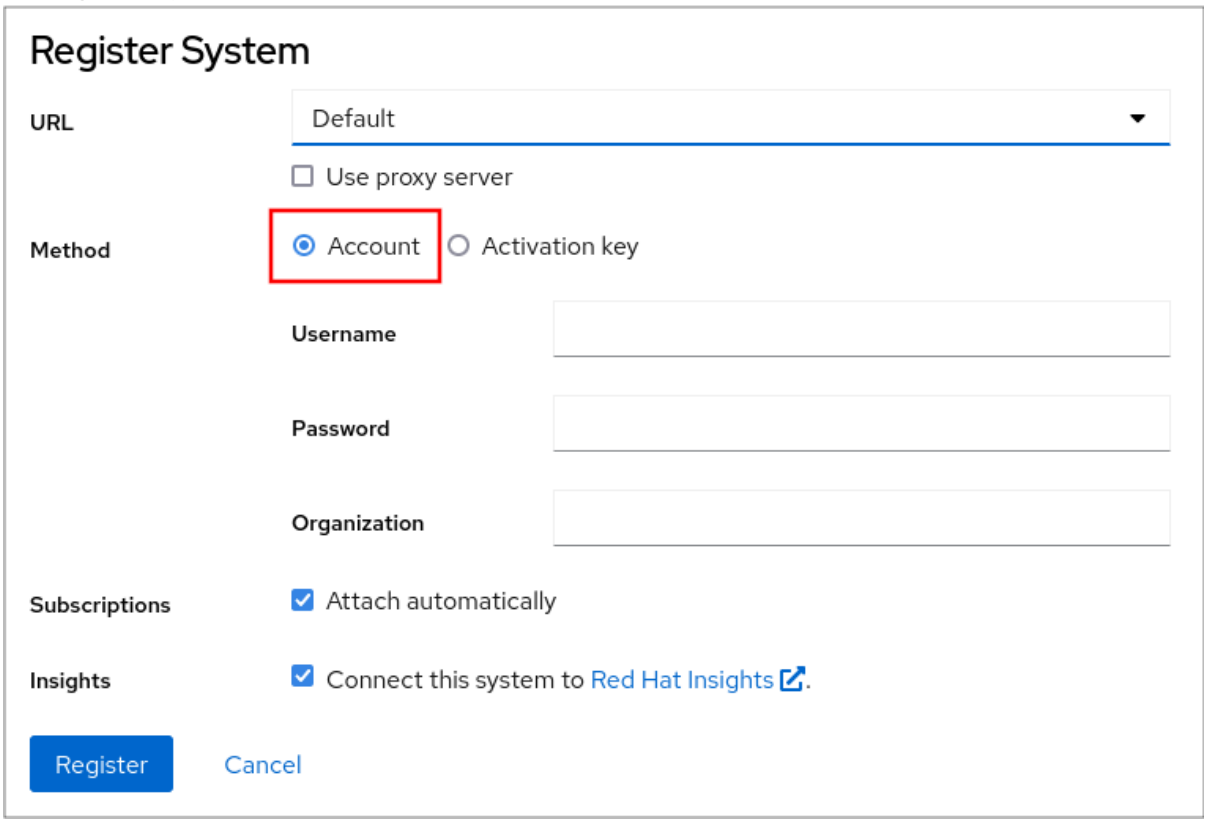
1. 登录到 RHEL web 控制台。详情请参阅 登录到 web 控制台。
2. 在 **Overview** 页面中的 **Health** 文件中，点 **Not registered** 警告，或者点击主菜单中的 **Subscriptions** 来进入页面。



3. 在 **Overview** 文件中，点 **Register**。



4. 在 **Register system** 对话框中，选择您要使用您的帐户凭证进行注册。



5. 输入您的用户名。
6. 输入您的密码。
7. （可选）输入您的机构名称或 ID。

如果您的帐户属于红帽客户门户网站中的多个机构，您必须添加机构名称或机构 ID。要获得机构 ID，请联系您的红帽相关人员。

- 如果您不想将您的系统连接到 Red Hat Insights，请取消选中 **Insights** 复选框。

8. 点 **Register** 按钮。

此时您的 Red Hat Enterprise Linux Enterprise Linux 系统已被成功注册。

28.3. 在 WEB 控制台中使用激活码注册订阅

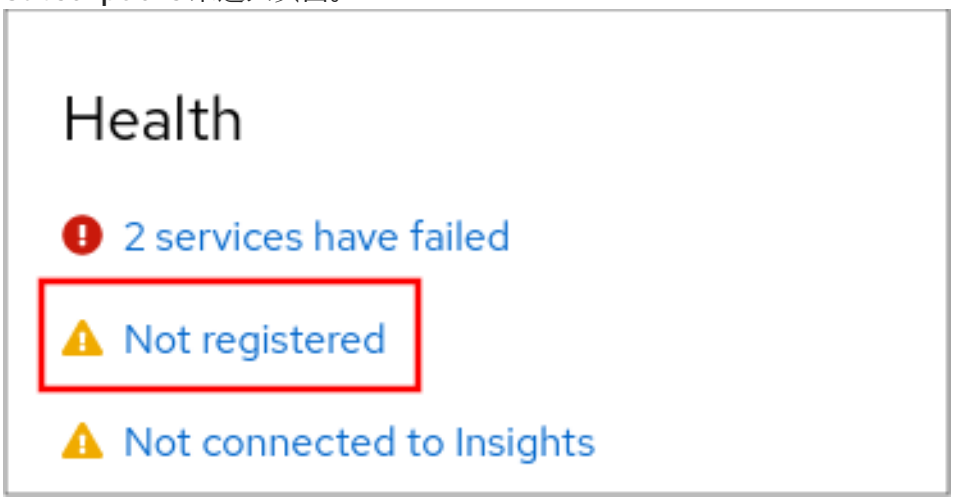
按照以下步骤，通过 RHEL web 控制台使用激活码注册新安装的 Red Hat Enterprise Linux。

先决条件

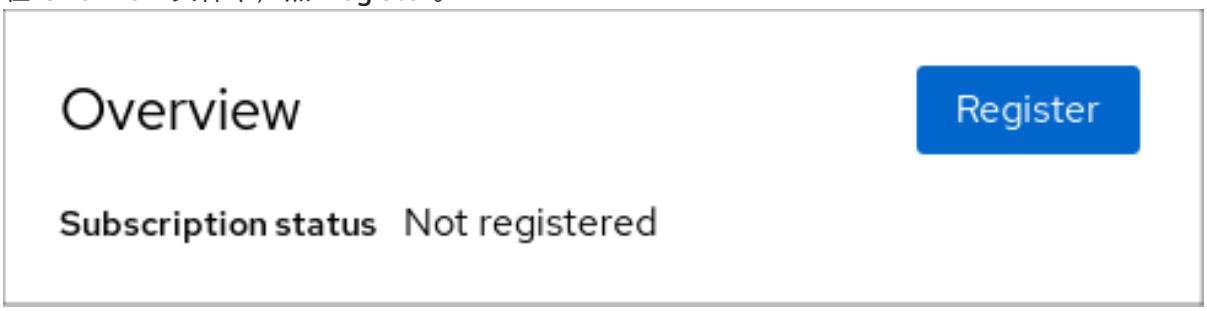
- 如果您在该门户中没有用户帐户，您的厂商会为您提供激活码。

流程

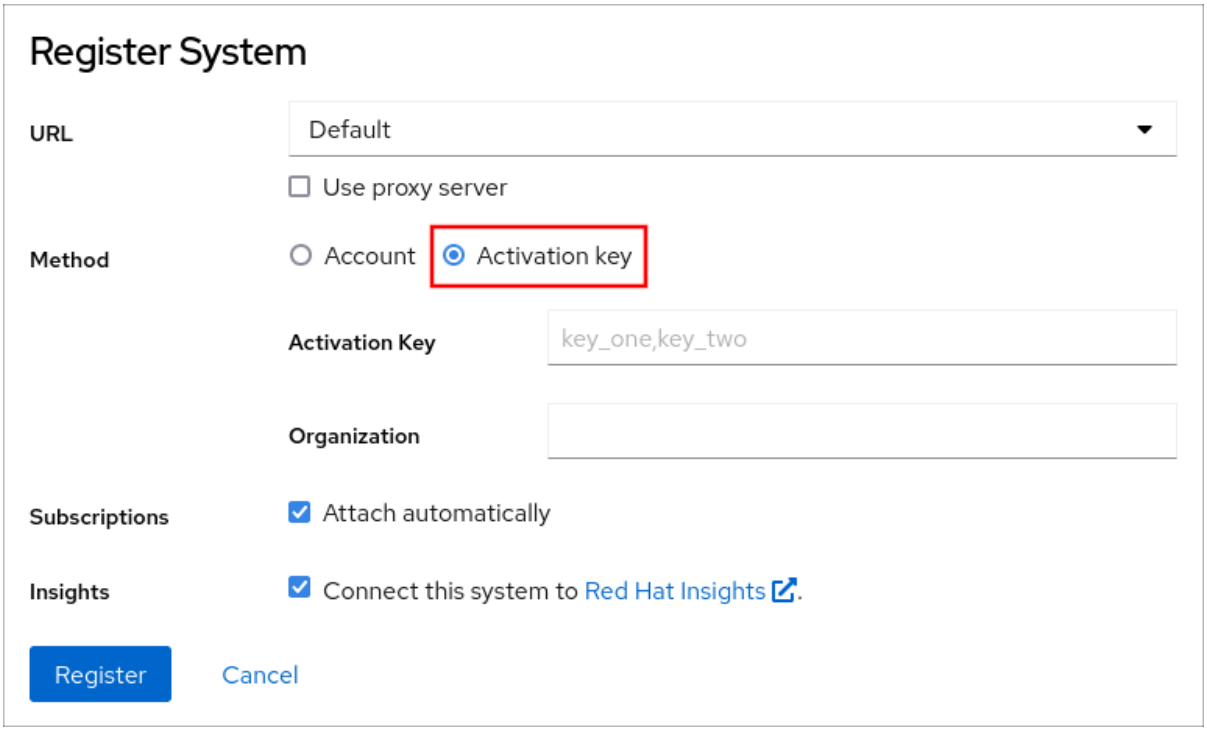
1. 登录到 RHEL web 控制台。详情请参阅 登录到 web 控制台。
2. 在 **Overview** 页面中的 **Health** 文件中，点 **Not registered** 警告，或者点击主菜单中的 **Subscriptions** 来进入页面。



3. 在 **Overview** 文件中，点 **Register**。



4. 在**注册系统**对话框中，选择您要使用激活码进行注册。



5. 输入您的密钥或密钥。
6. 输入您的机构名称或 ID。
   要获得机构 ID，请联系您的红帽联系点。
   - 如果您不想将您的系统连接到 Red Hat Insights，请取消选中 **Insights** 复选框。
7. 点 **Register** 按钮。

此时您的 Red Hat Enterprise Linux 系统已被成功注册。

第 29 章 在 WEB 控制台中配置 KDUMP

您可以使用 RHEL 9 web 控制台设置并测试 **kdump** 配置。Web 控制台可以在引导时启用 **kdump** 服务。另外，web 控制台允许您为 **kdump** 配置保留的内存，并选择未压缩或压缩格式的 **vmcore** 的保存位置。

29.1. 在 WEB 控制台中配置 KDUMP 内存用量和目标位置

您可以为 **kdump** 内核配置内存保留，并指定目标位置，来使用 RHEL web 控制台界面捕获 **vmcore** 转储文件。

先决条件

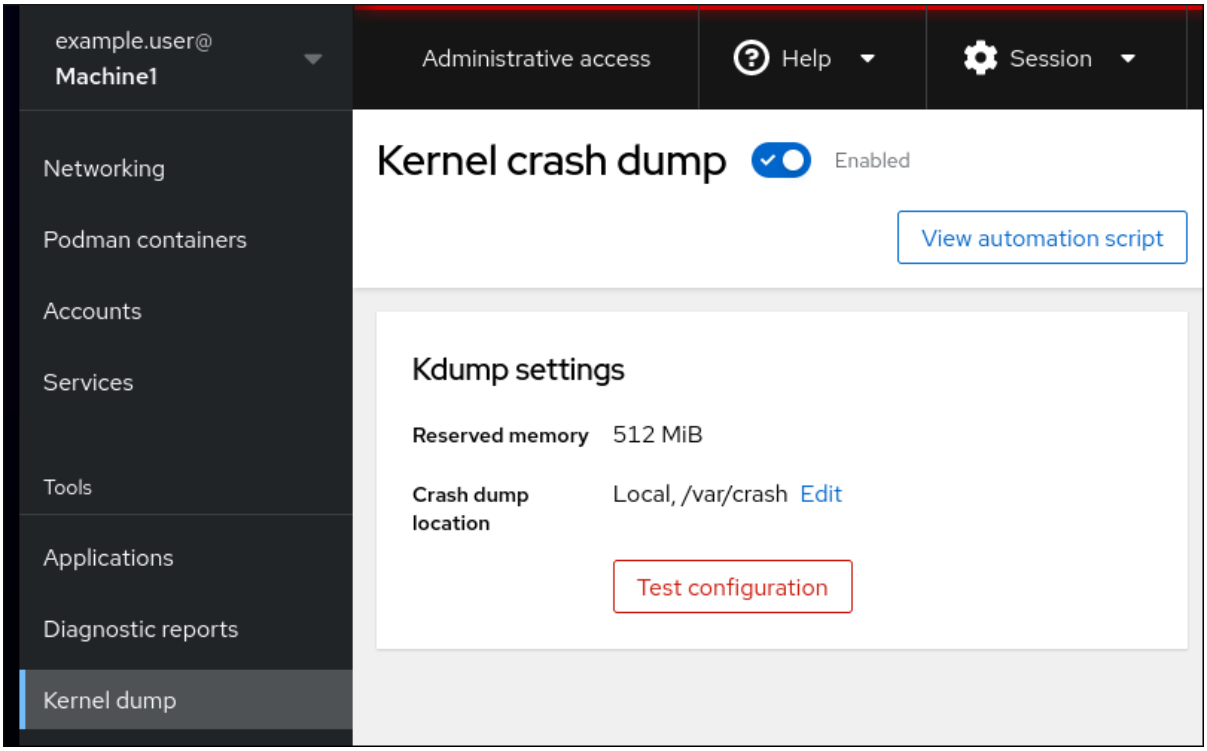
- 必须安装并可以访问 Web 控制台。
  详情请参阅安装 Web 控制台。

流程

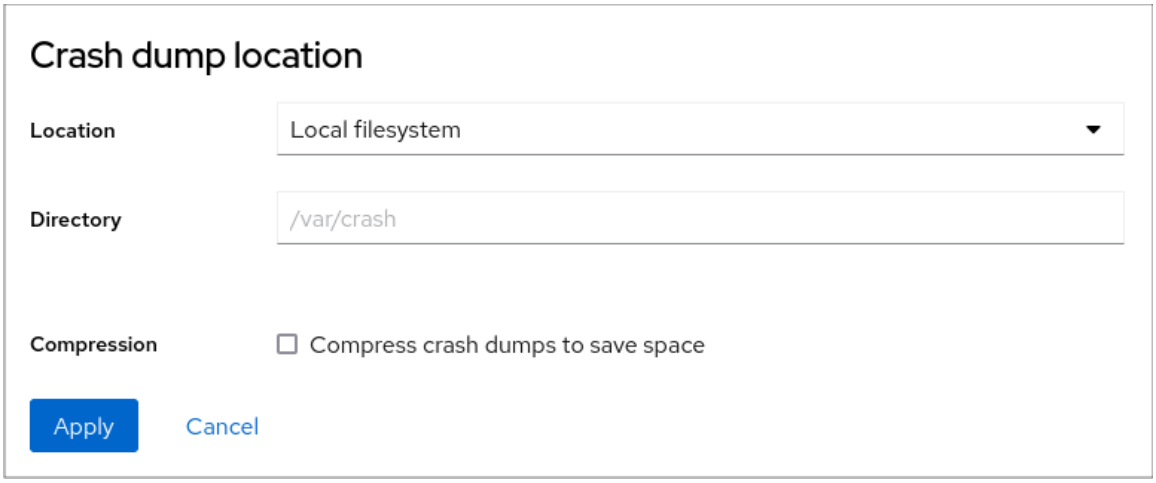
1. 在 web 控制台中，打开 **Kernel dump** 选项卡，并通过将 **Kernel crash dump** 开关设置为 on 来启动 **kdump** 服务。
2. 在终端中配置 **kdump** 内存使用情况，例如：

   ```
   $ sudo grubby --update-kernel ALL --args crashkernel=512M
   ```

   重启系统以应用更改。
3. 在 **Kernel dump** 选项卡中，点 **Crash dump location** 字段末尾的 **Edit**。



4. 指定保存 **vmcore** 转储文件的目标目录：
   - 对于本地文件系统，从下拉菜单中选择 **Local Filesystem**。



- 对于使用 SSH 协议的远程系统，从下拉菜单中选择 **Remote over SSH**，并指定以下字段：
  - 在 **Server** 字段中，输入远程服务器地址。
  - 在 **SSH key** 字段中，输入 SSH 密钥位置。
  - 在 **Directory** 字段中，输入目标目录。
- 对于使用 NFS 协议的远程系统，从下拉菜单中选择 **Remote over NFS**，并指定以下字段：
  - 在 **Server** 字段中，输入远程服务器地址。
  - 在 **Export** 字段中，输入 NFS 服务器的共享文件夹的位置。
  - 在 **Directory** 字段中，输入目标目录。

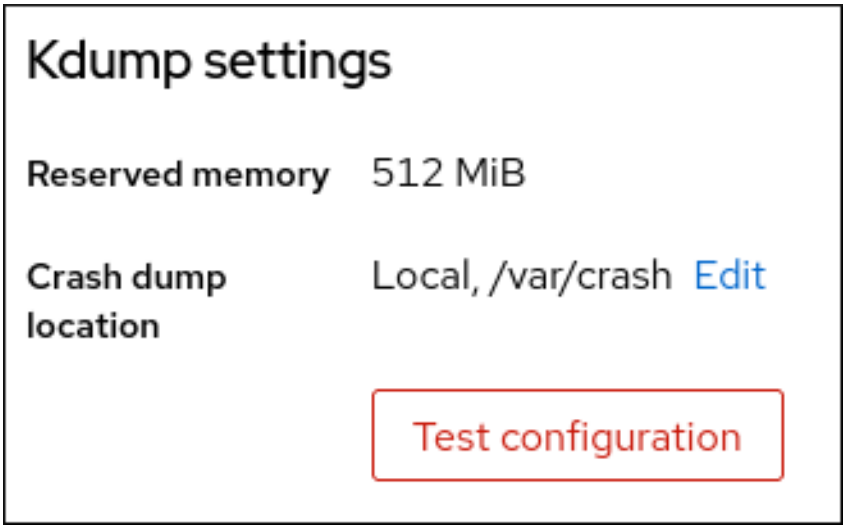
注意

您可以通过选择 **Compression** 复选框来减小 **vmcore** 文件的大小。

5. 可选：点 **View automation script** 来显示自动化脚本。
   此时会打开一个带有生成的脚本的窗口。您可以在 shell 脚本页和 Ansible playbook 生成选项页之间转换。
6. 可选：点 **Copy to clipboard** 来复制脚本。
   您可以使用此脚本在多台机器上应用相同的配置。

验证

1. 单击 **Test configuration**。



2. 在 **Test kdump settings** 下点 **Crash system**。

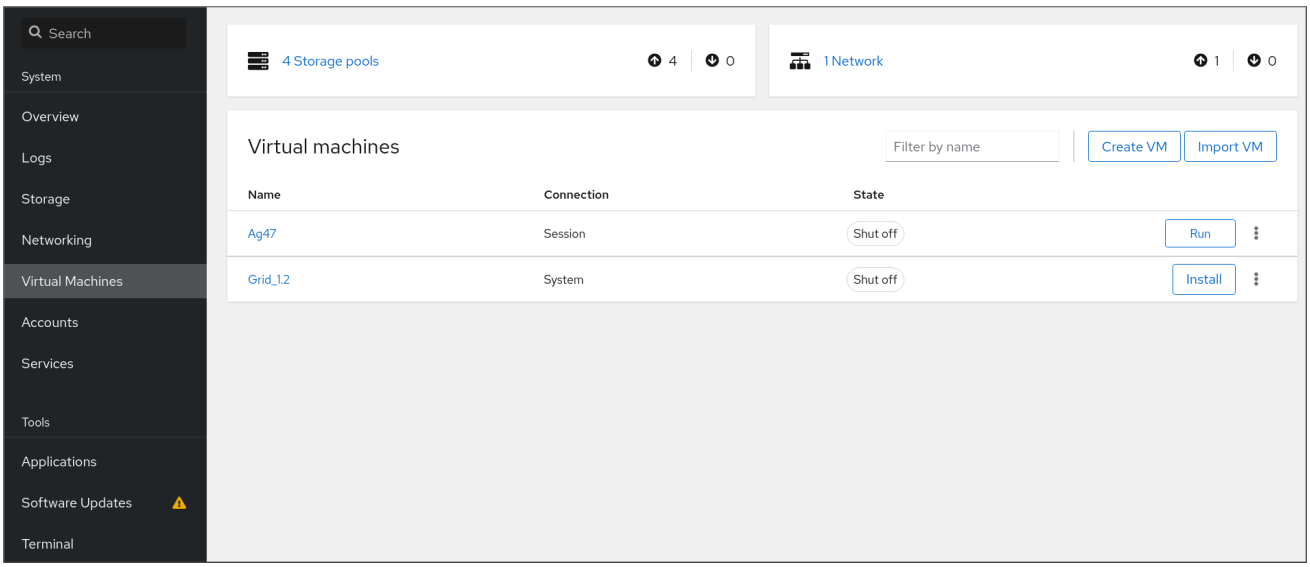
> **警告**
>
> 当您发起系统崩溃时，内核操作停止，并导致系统崩溃，且数据丢失。

其它资源

- 支持的 kdump 目标

第 30 章 在 WEB 控制台中管理虚拟机

要在 RHEL 9 主机上的图形界面管理虚拟机，您可以在 RHEL 9 web 控制台中使用 **Virtual Machines** 窗格。



30.1. 使用 WEB 控制台管理虚拟机的概述

RHEL 9 web 控制台是一个用于系统管理的基于 web 的界面。作为其功能之一，Web 控制台提供主机系统中虚拟机（VM）的图形视图，并可创建、访问和配置这些虚拟机。

请注意，要使用 Web 控制台在 RHEL 9 上管理虚拟机，您必须首先为虚拟化安装 web 控制台插件。

后续步骤

- 有关在 web 控制台中启用虚拟机管理的说明，请参阅 设置 web 控制台来管理虚拟机。
- 有关 web 控制台提供的虚拟机管理操作的完整列表，请参阅 web 控制台中提供的虚拟机管理功能。

30.2. 设置 WEB 控制台以管理虚拟机

在使用 RHEL 9 web 控制台管理虚拟机 (VM) 之前，您必须在主机上安装 web 控制台虚拟机插件。

先决条件

- 确保机器上安装并启用了 Web 控制台。

```
# systemctl status cockpit.socket
cockpit.socket - Cockpit Web Service Socket
Loaded: loaded (/usr/lib/systemd/system/cockpit.socket
[...]
```

如果此命令返回 **Unit cockpit.socket could not be found**，请按照 安装 Web 控制台 文档来启用 Web 控制台。

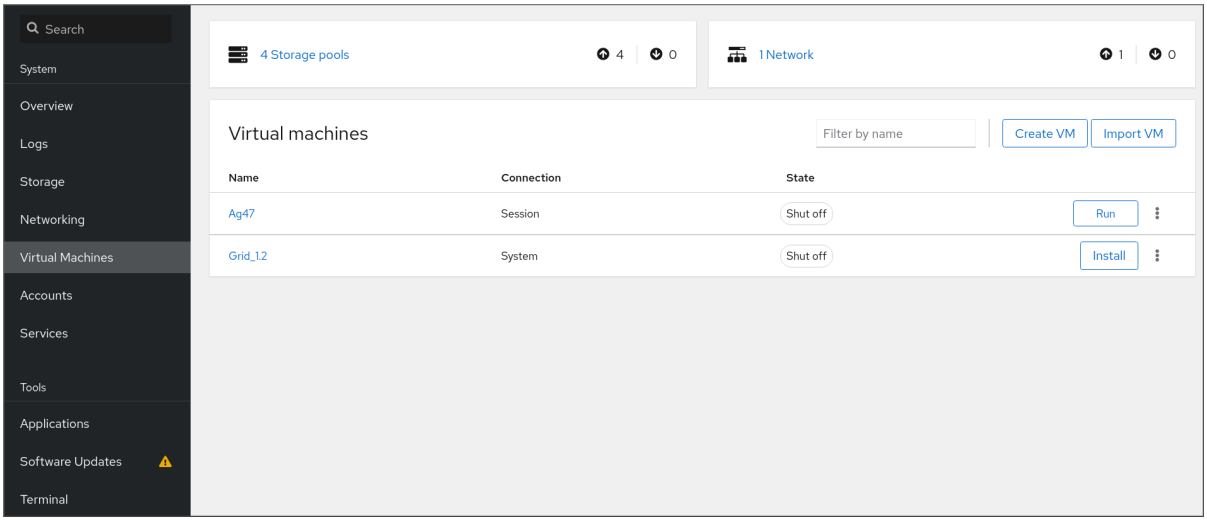
流程

- 安装 **cockpit-machines** 插件。

```
# dnf install cockpit-machines
```

验证

1. 访问 Web 控制台，例如在浏览器中输入 **https://localhost:9090** 地址。
2. 登录。
3. 如果安装成功，**Virtual Machines** 会出现在 web 控制台侧菜单中。



其它资源

- 使用 RHEL 9 web 控制台管理系统

30.3. 使用 WEB 控制台重命名虚拟机

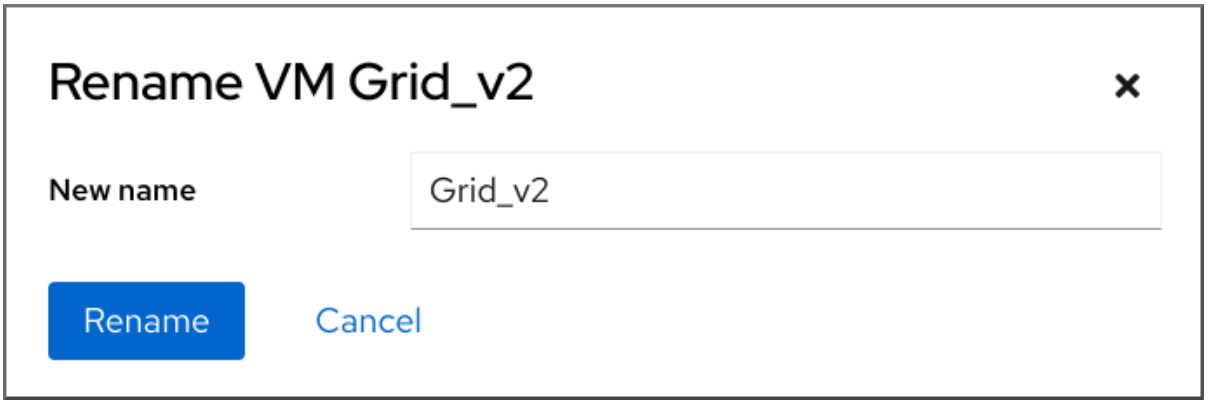
您可能需要重命名现有虚拟机(VM)，以避免命名冲突，或者根据您的用例分配一个新的唯一名称。要重命名虚拟机，您可以使用 RHEL web 控制台。

先决条件

- Web 控制台 VM 插件 已安装在您的系统上。
- 虚拟机已关闭。

流程

1. 在 **Virtual Machines** 界面中，点击您要重命名的虚拟机的菜单按钮 ⋮。
   此时会出现一个控制各种虚拟机操作的下拉菜单。
2. 点 **Rename**。
   此时会出现**Rename a VM**对话框。



3. 在 **New name** 字段中输入虚拟机的名称。
4. 点 **Rename**。

验证

- 检查新虚拟机名称是否已出现在 **Virtual Machines** 界面中。

30.4. WEB 控制台中提供的虚拟机管理功能

通过使用 RHEL 9 web 控制台，您可以执行以下操作，来管理系统上的虚拟机(VM)。

表 30.1. RHEL 9 web 控制台中执行的虚拟机任务

任务	详情请查看：
创建虚拟机并将其安装到客户端操作系统	使用 web 控制台创建虚拟机并安装客户机操作系统
删除虚拟机。	使用 web 控制台删除虚拟机。
启动、关闭和重启虚拟机	使用 web 控制台启动虚拟机，并 使用 web 控制台关闭和重启虚拟机
使用各种控制台连接到虚拟机并与虚拟机交互	使用 web 控制台与虚拟机进行交互
查看有关虚拟机的各种信息	使用 web 控制台查看虚拟机信息
调整分配给虚拟机的主机内存	使用 web 控制台添加和删除虚拟机内存
管理虚拟机的网络连接	使用 web 控制台管理虚拟机网络接口
管理主机上可用的虚拟机存储，并将虚拟磁盘附加到虚拟机	为虚拟机管理存储
配置虚拟机的虚拟 CPU 设置	使用 Web 控制台管理虚拟 CPU
实时迁移虚拟机	使用 web 控制台实时迁移虚拟机
重命名虚拟机	使用 web 控制台重命名虚拟机

任务	详情请查看：
在主机和虚拟机间共享文件	在主机及其虚拟机间共享文件
管理主机设备	使用 web 控制台管理虚拟设备
管理虚拟光驱	管理虚拟光驱
附加 watchdog 设备	使用 web 控制台将 watchdog 设备附加到虚拟机

第 31 章 在 WEB 控制台中管理远程系统

连接到远程系统，并在 RHEL 9 web 控制台中管理它们。

下面的章节描述：

- 连接系统的最佳拓扑。
- 如何添加和删除远程系统。
- 何时，以及如何使用 SSH 密钥进行远程系统身份验证。
- 如何配置 Web 控制台客户端，以允许使用智能卡通过 **SSH** 访问远程主机并访问服务的用户。

先决条件

- 在远程系统中打开 SSH 服务。

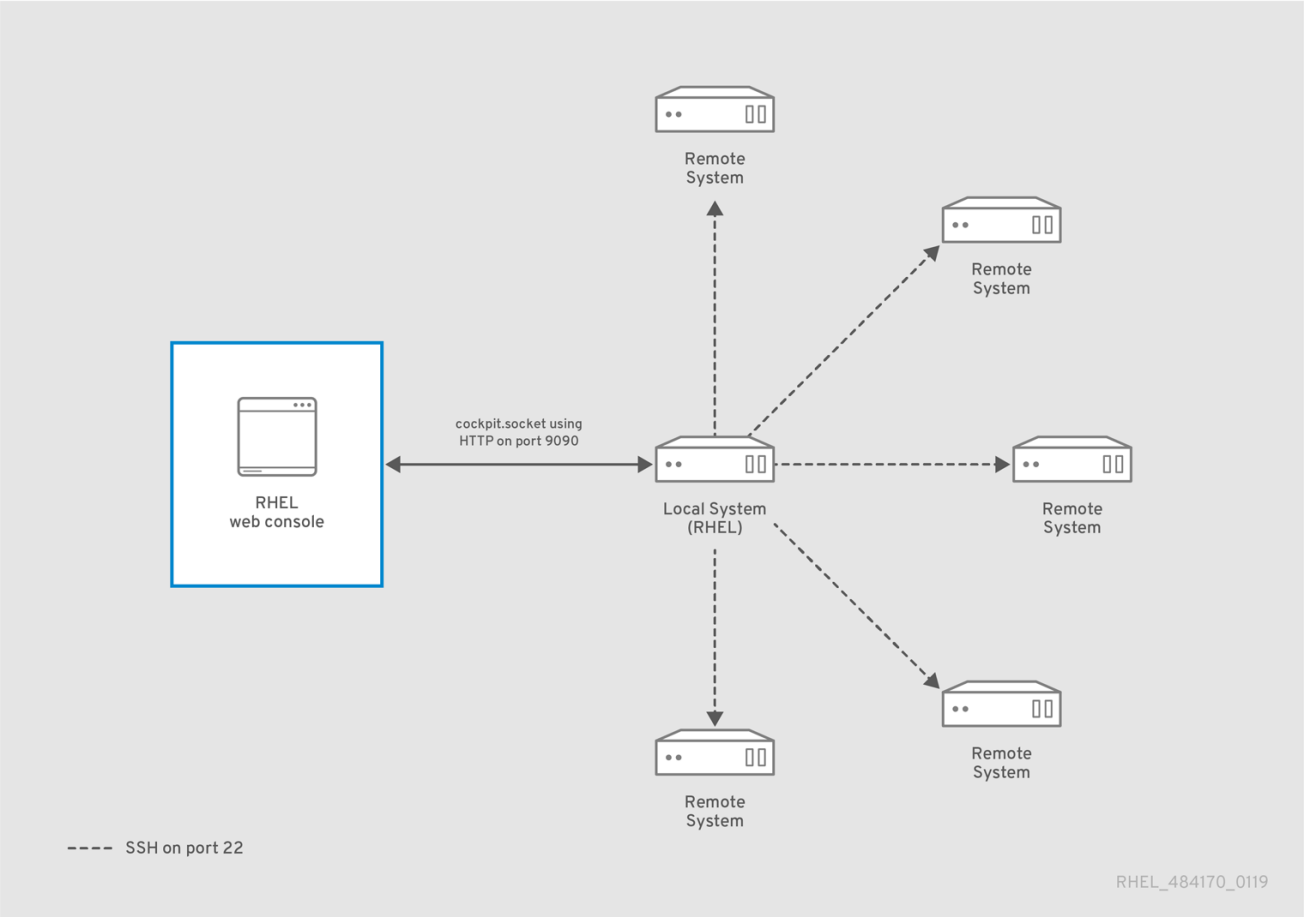
31.1. WEB 控制台中的远程系统管理器

使用 RHEL 9 Web 控制台管理网络中的远程系统需要考虑连接的服务器拓扑。

要实现最佳安全性，请使用以下连接设置：

- 使用 Web 控制台将系统配置为堡垒主机。堡垒主机是带有打开 HTTPS 端口的系统。
- 所有其他系统通过 SSH 进行通信。

通过在堡垒主机上运行的 Web 接口，您可以使用默认配置中的端口 22 通过 SSH 协议访问所有其他系统。



31.2. 在 WEB 控制台中添加远程主机

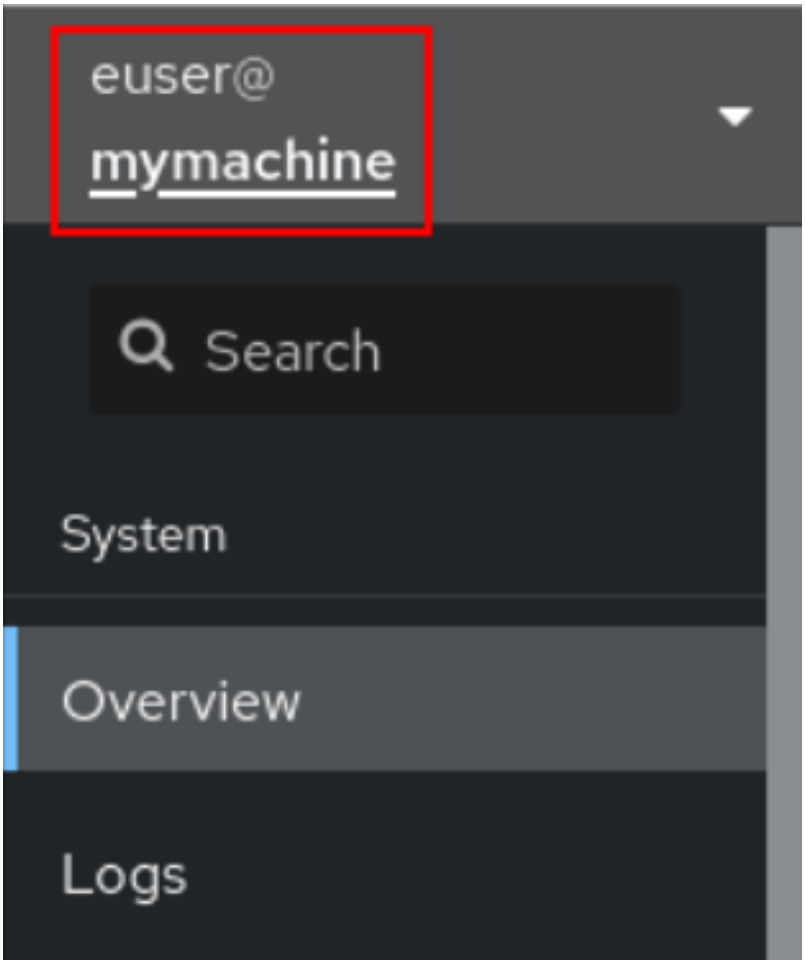
您可以使用用户名和密码连接其他系统。

先决条件

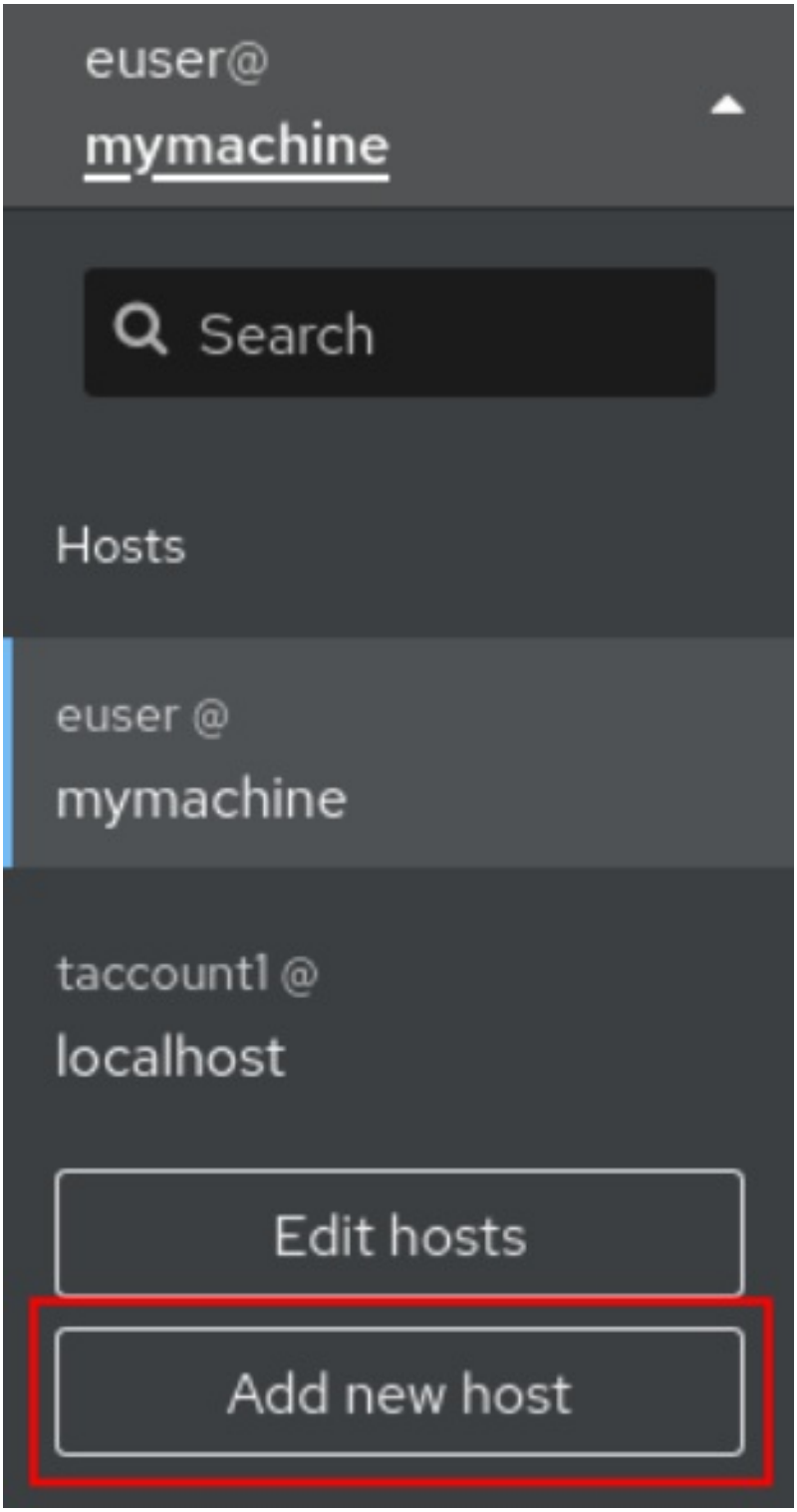
- 您需要使用管理权限登录到 web 控制台。详情请参阅 登录到 web 控制台。

流程

1. 在 RHEL 9 web 控制台中，点 **Overview** 页面左上角的 **username@hostname**。



2. 从下拉菜单中选择 **Add new host** 按钮。



3. 在 **Add new host** 对话框中，指定要添加的主机。

4. （可选）为您要连接的帐户添加用户名。
   您可以使用远程系统的任意用户帐户。但是，如果您使用一个没有管理特权的用户凭证时，将无法执行管理任务。

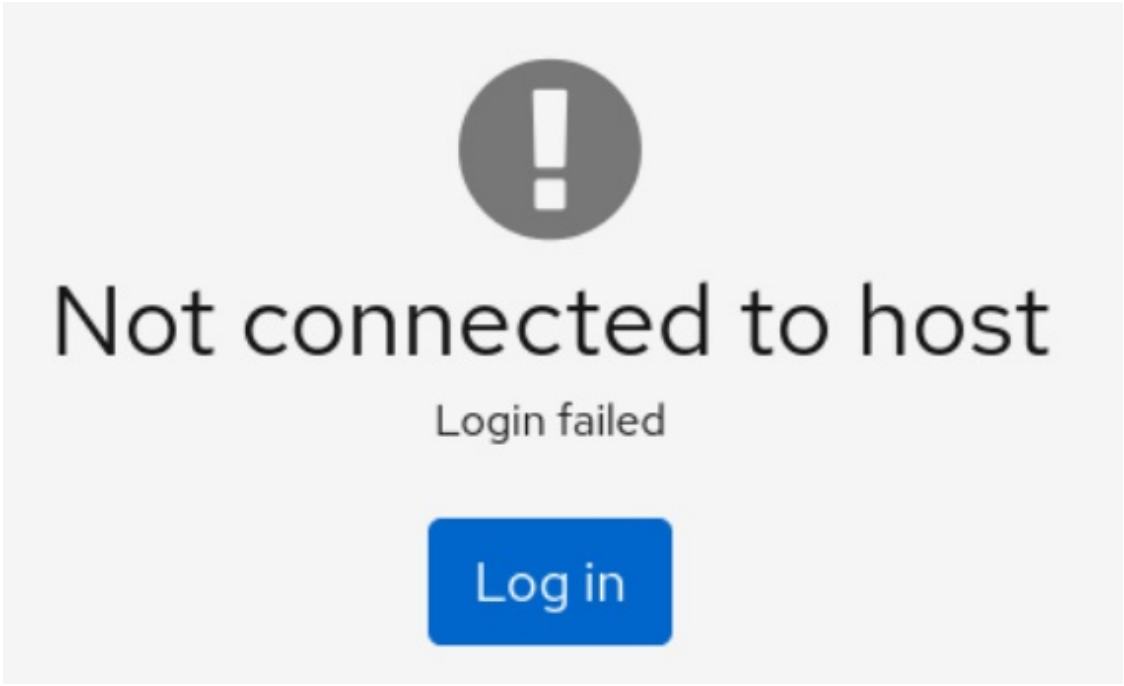
   如果您与本地系统使用相同的凭证，Web 控制台会在您登录时自动验证远程系统。但是，对更多机器使用相同的凭证可能会带来潜在的安全风险。

5. （可选）点 **Color** 字段更改系统颜色。

6. 点击 **Add**。
   新主机将显示在 **username@hostname** 下拉菜单中的主机列表中。

注意

Web 控制台不会保存用于登录到远程系统的密码，这意味着您必须在每次系统重启后再次登录。下次登录时，点**登录** 按钮放置在断开连接的远程系统的主屏幕中，以打开登录对话框。



31.3. 从 WEB 控制台删除远程主机

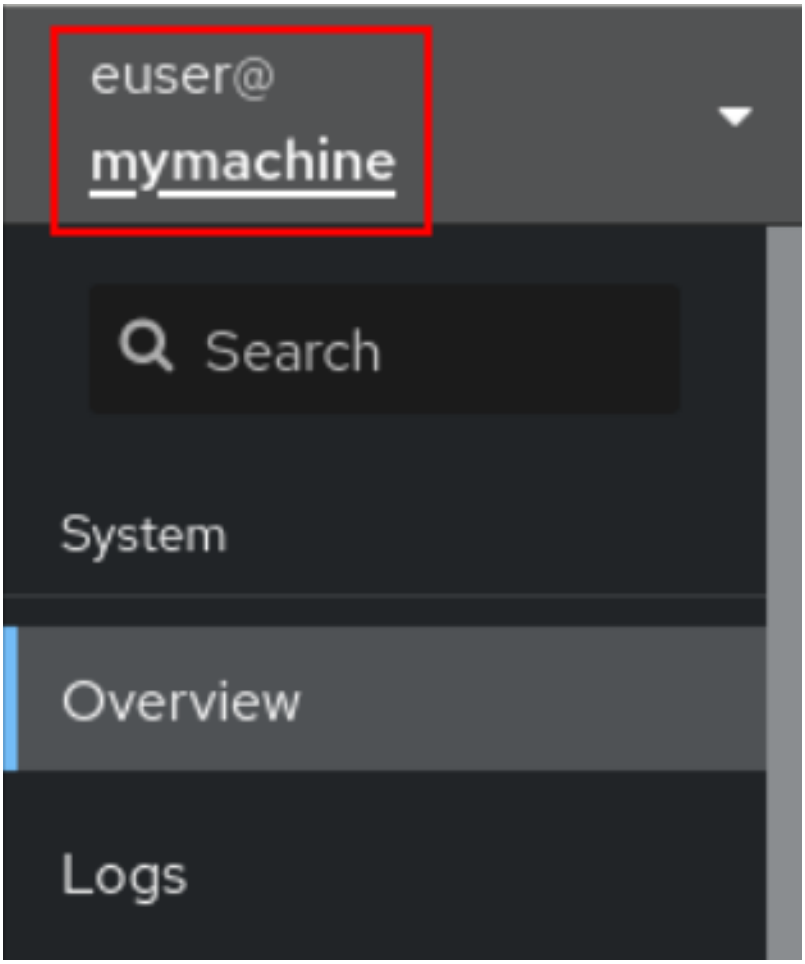
您可从 web 控制台删除其他系统。

先决条件

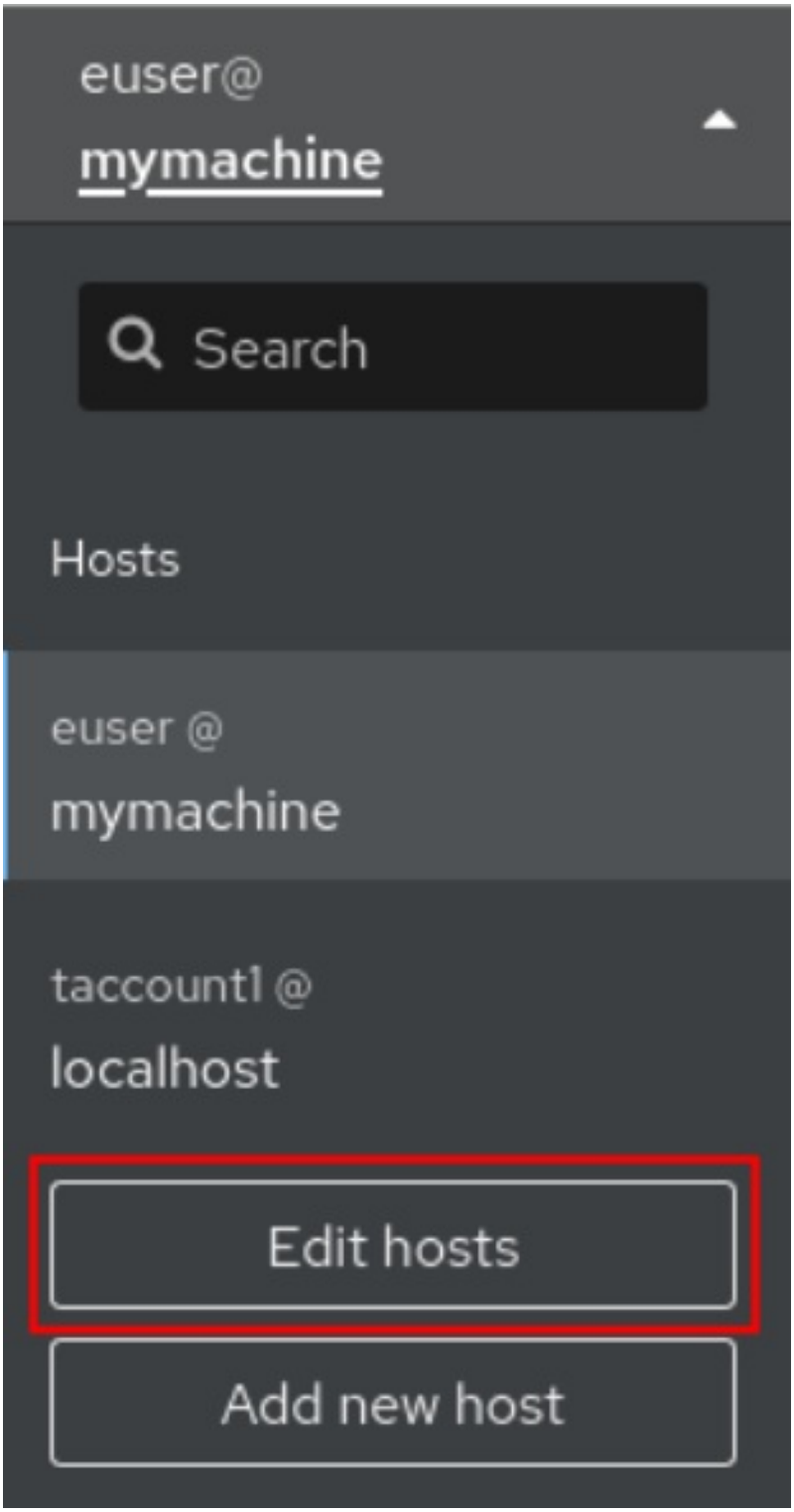
- 添加了远程系统。
  详情请参阅在 web 控制台中添加远程主机。
- 您必须使用管理员权限登录到 web 控制台。
  详情请参阅 登录到 web 控制台。

流程

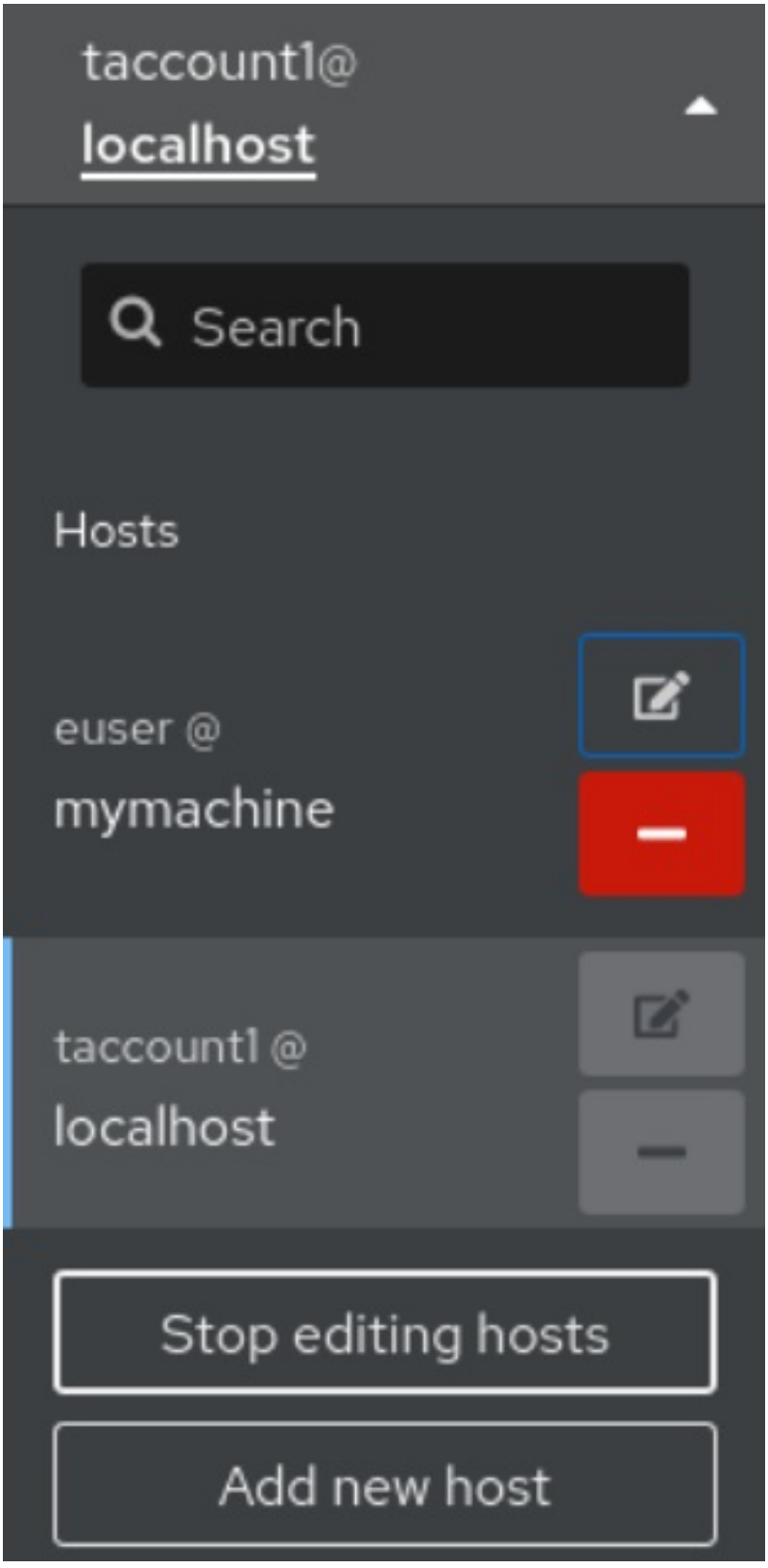
1. 登录到 RHEL 9 web 控制台。
2. 点 **Overview** 页面左上角的 **username@hostname**。



3. 点 **Edit hosts** 图标。



4. 要从 web 控制台删除主机，请点其主机名旁的红色减号 - 按钮。请注意，您无法删除当前连接的主机。



因此，服务器会从 web 控制台中删除。

31.4. 为新主机启用 SSH 登录

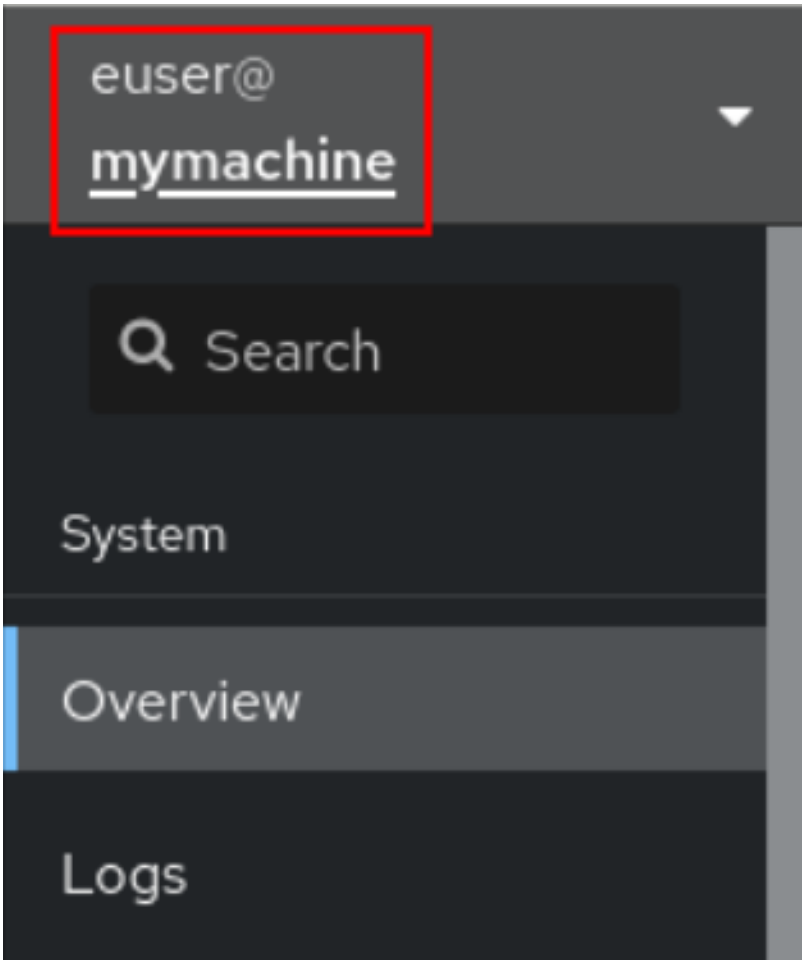
当您添加新主机时，您也可以使用 SSH 密钥登录到主机。如果您的系统上已有一个 SSH 密钥，则 web 控制台将使用现有的密钥；否则，Web 控制台可以创建一个密钥。

先决条件

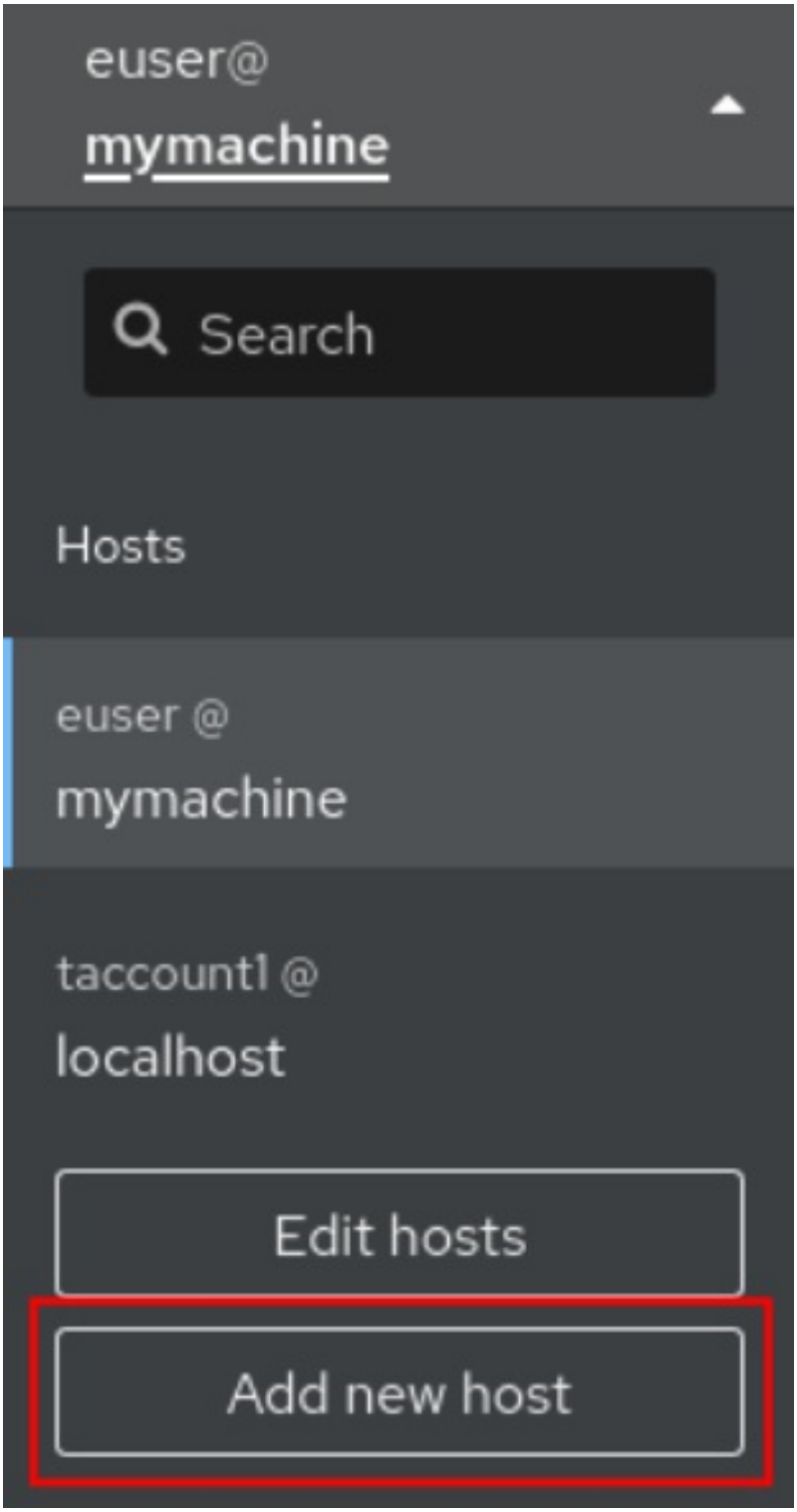
- 您已使用管理权限登录到 web 控制台。
  详情请参阅 登录到 web 控制台。

流程

1. 在 RHEL 9 web 控制台中，点 **Overview** 页面左上角的 **username@hostname**。



2. 从下拉菜单中选择 **Add new host** 按钮。



3. 在 **Add new host** 对话框中，指定要添加的主机。

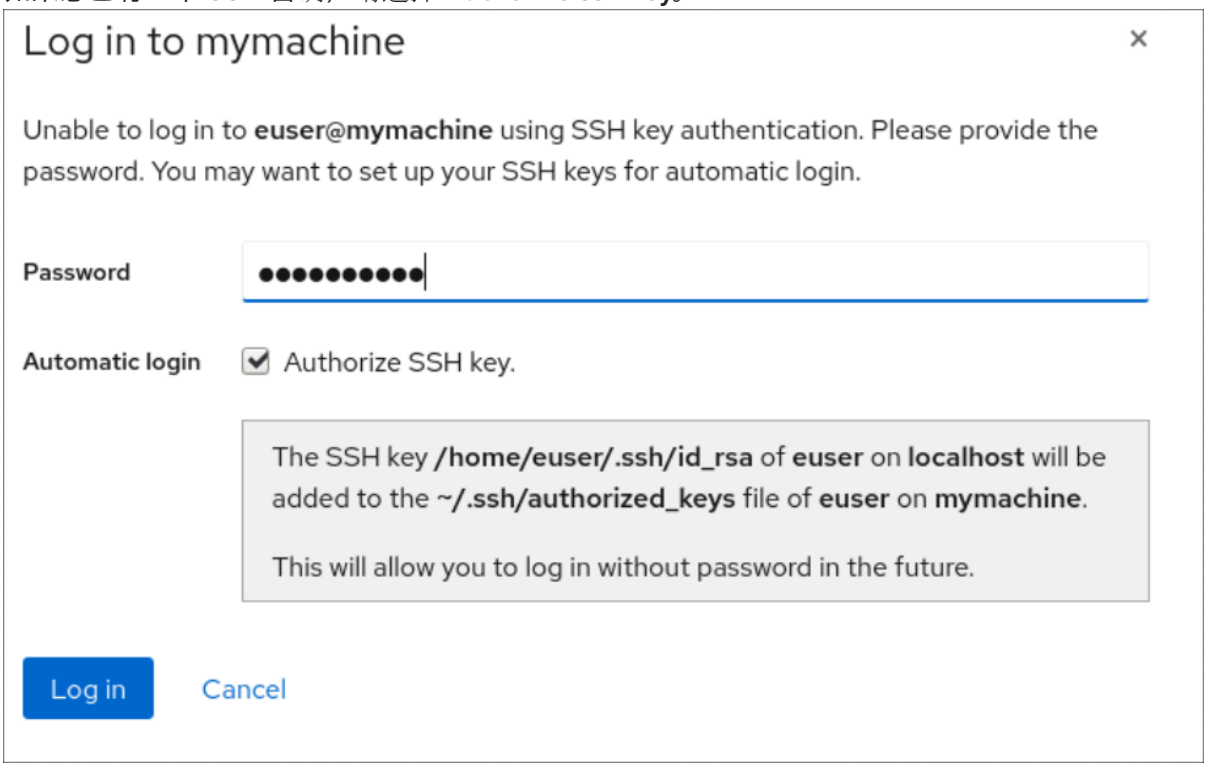
4. 为要连接的帐户添加用户名。
   您可以使用远程系统的任意用户帐户。但是，如果您使用一个没有管理特权的用户凭证时，将无法执行管理任务。

5. （可选）点 **Color** 字段更改系统颜色。

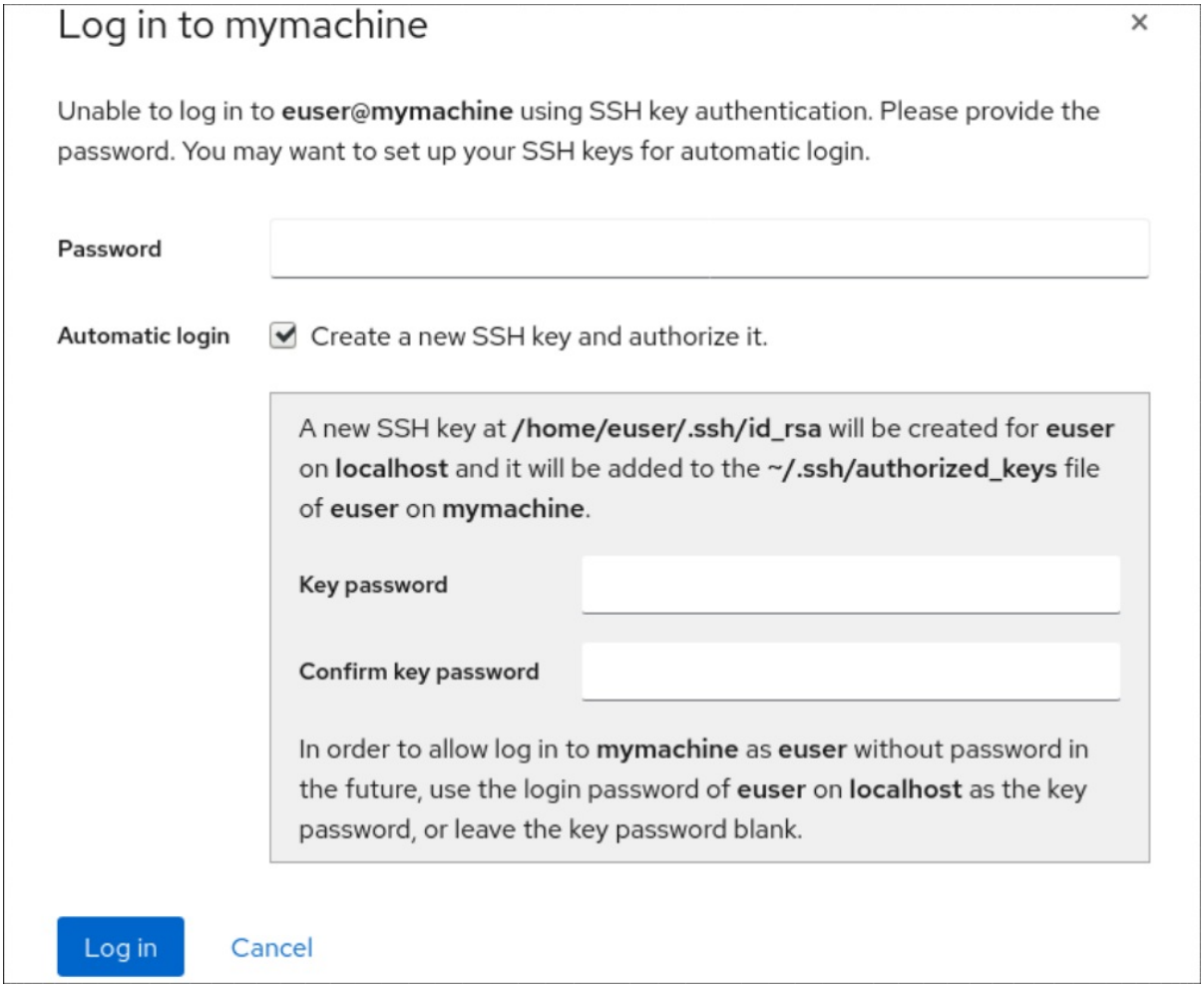
6. 点击 **Add**。
   系统将显示一个新对话框窗口，要求输入密码。

7. 输入用户帐户密码。

8. 如果您已有一个 SSH 密钥，请选择 **Authorize ssh key**。



9. 如果您没有 SSH 密钥，选择 **Create a new SSH key and authorize it**。Web 控制台会为您创建它。



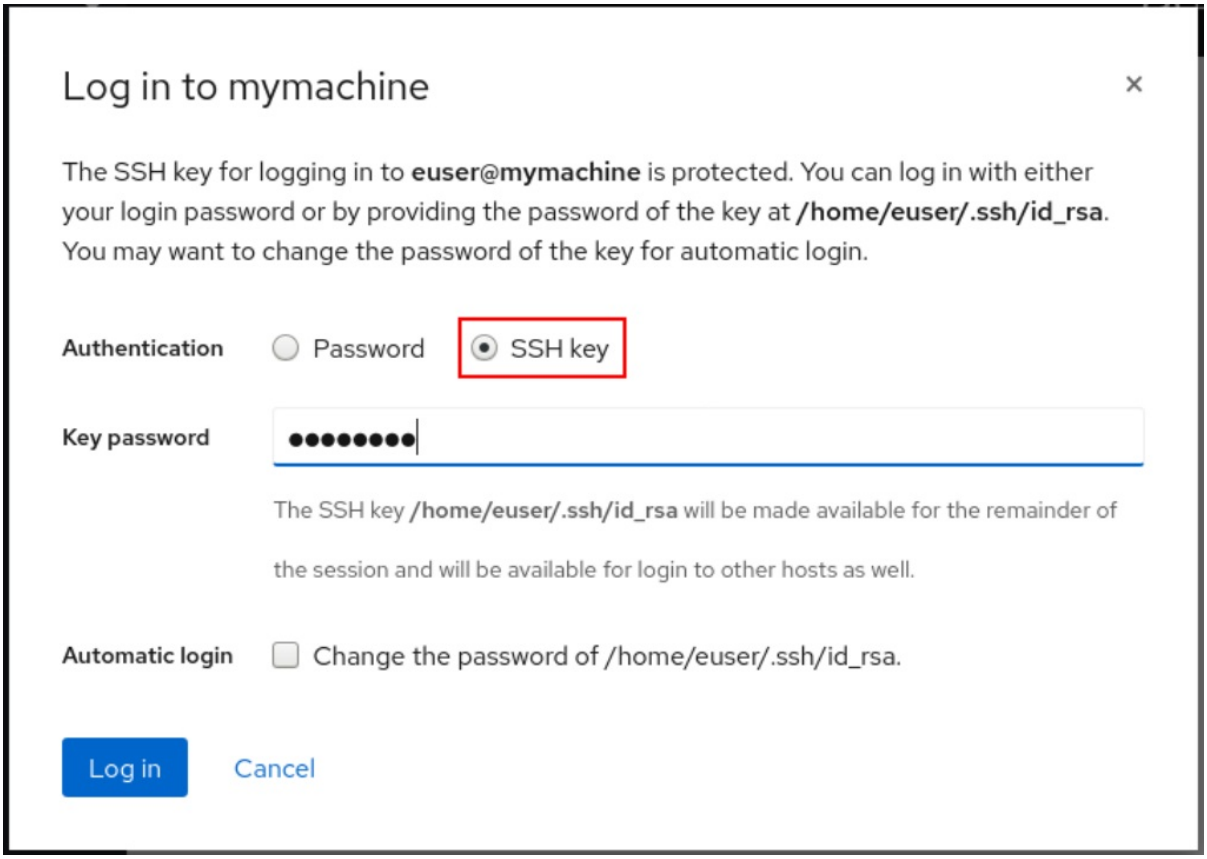
a. 为 SSH 密钥添加密码。

b. 确认密码。

10. 点 **Log in**
新主机将显示在 **username@hostname** 下拉菜单中的主机列表中。

验证步骤

1. 注销。
2. 重新登录。
3. 在 **Not connected to host** 屏幕中点 **Log in**。
4. 选择 **SSH 密钥** 作为您的身份验证选项。



5. 输入您的密钥密码。
6. 点**登录**。

其它资源

- 使用 OpenSSH 的两个系统间使用安全通讯

31.5. 身份管理中的受限委托

用户到代理 (**S4U2proxy**) 扩展的服务为代表用户的另一服务获取服务票据。此功能称为**受限委托**。第二个服务通常是在用户的授权上下文下代表第一个服务执行某些工作的代理。使用受限委托无需用户委派其完整票据授予票 (TGT)。

身份管理 (IdM) 通常使用 Kerberos **S4U2proxy** 功能来允许 Web 服务器框架代表用户获取 LDAP 服务票据。IdM-AD 信任系统也使用受限委托来获取 **cifs** 主体。

您可以使用 **S4U2proxy** 功能配置 Web 控制台客户端，以允许使用智能卡进行身份验证的 IdM 用户来实现以下内容：

- 在运行 web 控制台服务的 RHEL 主机上以超级用户权限运行命令，而无需再次进行身份验证。
- 使用 **SSH** 访问远程主机并访问主机上的服务，而无需再次进行身份验证。

其它资源

- S4U2proxy
- 服务受限委托

31.6. 将 WEB 控制台配置为允许使用智能卡通过 SSH 验证到远程主机的用户，而无需再次进行身份验证

登录到 RHEL web 控制台中的用户帐户后，作为身份管理 (IdM) 系统管理员，您可能需要使用 **SSH** 协议连接到远程机器。您可以使用受限委托 功能来使用 **SSH**，而无需再次进行身份验证。

按照以下流程，将 Web 控制台配置为使用受限委托。在以下示例中，web 控制台会话在 **myhost.idm.example.com** 主机上运行，它被配置为代表经过身份验证的用户使用 **SSH** 访问 **remote.idm.example.com** 主机。

先决条件

- 您已获得 IdM **admin** 票据授予票(TGT)。
- 您有访问 **remote.idm.example.com** 的 **root** 权限。
- Web 控制台服务存在于 IdM 中。
- **remote.idm.example.com** 主机存在于 IdM 中。
- Web 控制台在用户会话中创建了一个 **S4U2Proxy** Kerberos ticket。要验证是否是这种情况，请以 IdM 用户身份登录 Web 控制台，打开 **Terminal** 页面，并输入：

```
$ klist
Ticket cache: FILE:/run/user/1894000001/cockpit-session-3692.ccache
Default principal: user@IDM.EXAMPLE.COM

Valid starting     Expires            Service principal
07/30/21 09:19:06 07/31/21 09:19:06
HTTP/myhost.idm.example.com@IDM.EXAMPLE.COM
07/30/21 09:19:06  07/31/21 09:19:06  krbtgt/IDM.EXAMPLE.COM@IDM.EXAMPLE.COM
        for client HTTP/myhost.idm.example.com@IDM.EXAMPLE.COM
```

流程

1. 创建可以通过委派规则访问的目标主机列表：
   a. 创建服务委托目标：

```
$ ipa servicedelegationtarget-add cockpit-target
```

b. 将目标主机添加到委派目标：

```
$ ipa servicedelegationtarget-add-member cockpit-target \ --
principals=host/remote.idm.example.com@IDM.EXAMPLE.COM
```

2. 通过创建服务委派规则并将 **HTTP** 服务 Kerberos 主体添加到其中，允许 **cockpit** 会话访问目标主机列表：

a. 创建服务委派规则：

```
$ ipa servicedelegationrule-add cockpit-delegation
```

b. 将 Web 控制台客户端添加到委派规则中：

```
$ ipa servicedelegationrule-add-member cockpit-delegation \ --
principals=HTTP/myhost.idm.example.com@IDM.EXAMPLE.COM
```

c. 将委派目标添加到委派规则中：

```
$ ipa servicedelegationrule-add-target cockpit-delegation \ --
servicedelegationtargets=cockpit-target
```

3. 在 **remote.idm.example.com** 主机上启用 Kerberos 身份验证：

a. 以 **root** 身份通过 **SSH** 连接到 **remote.idm.example.com**。

b. 打开 **/etc/ssh/sshd_config** 文件进行编辑。

c. 通过取消注释 **GSSAPIAuthentication no** 行，并将它替换为 **GSSAPIAuthentication yes** 来启用 **GSSAPIAuthentication**。

4. 在 **remote.idm.example.com** 上重启 **SSH** 服务，以便上述更改会立即生效：

```
$ systemctl try-restart sshd.service
```

其它资源

- 使用智能卡登录到 web 控制台
- 身份管理中的受限委托

31.7. 使用 ANSIBLE 配置 WEB 控制台，允许用户使用智能卡通过 SSH 向远程主机进行身份验证，而无需再次进行身份验证

登录到 RHEL web 控制台中的用户帐户后，作为身份管理 (IdM) 系统管理员，您可能需要使用 **SSH** 协议连接到远程机器。您可以使用受限委托 功能来使用 **SSH**，而无需再次进行身份验证。

按照以下流程，使用 **servicedelegationrule** 和 **servicedelegationtarget ansible-freeipa** 模块将 Web 控制台配置为使用受限委托。在以下示例中，web 控制台会话在 **myhost.idm.example.com** 主机上运行，它被配置为代表经过身份验证的用户使用 **SSH** 访问 **remote.idm.example.com** 主机。

先决条件

- IdM **admin** 密码。
- 对 **remote.idm.example.com** 的 **root** 访问权限。
- Web 控制台服务存在于 IdM 中。
- **remote.idm.example.com** 主机存在于 IdM 中。
- Web 控制台在用户会话中创建了一个 **S4U2Proxy** Kerberos ticket。要验证是否是这种情况，请以 IdM 用户身份登录 Web 控制台，打开 **Terminal** 页面，并输入：

```
$ klist
Ticket cache: FILE:/run/user/1894000001/cockpit-session-3692.ccache
Default principal: user@IDM.EXAMPLE.COM

Valid starting     Expires            Service principal
07/30/21 09:19:06 07/31/21 09:19:06
HTTP/myhost.idm.example.com@IDM.EXAMPLE.COM
07/30/21 09:19:06  07/31/21 09:19:06  krbtgt/IDM.EXAMPLE.COM@IDM.EXAMPLE.COM
        for client HTTP/myhost.idm.example.com@IDM.EXAMPLE.COM
```

- 您已配置了 Ansible 控制节点以满足以下要求：
  - 您使用 Ansible 版本 2.14 或更高版本。
  - 您已在 Ansible 控制器上安装了 **ansible-freeipa** 软件包。
  - 示例假定在 ***~/MyPlaybooks/*** 目录中，您已创建了一个带有 IdM 服务器的完全限定域名 (FQDN)的 Ansible 清单文件。
  - 示例假定 **secret.yml** Ansible vault 存储了 **ipaadmin_password**。
- 目标节点（这是执行 **ansible-freeipa** 模块的节点）是 IdM 域的一部分，来作为 IdM 客户端、服务器或副本。

流程

1. 进入您的 ***~/MyPlaybooks/*** 目录：

```
$ cd ~/MyPlaybooks/
```

2. 创建包含以下内容的 **web-console-smart-card-ssh.yml** playbook：
   a. 创建确保存在委派目标的任务：

```
---
- name: Playbook to create a constrained delegation target
  hosts: ipaserver

  vars_files:
  - /home/user_name/MyPlaybooks/secret.yml
  tasks:
  - name: Ensure servicedelegationtarget web-console-delegation-target is present
    ipaservicedelegationtarget:
      ipaadmin_password: "{{ ipaadmin_password }}"
      name: web-console-delegation-target
```

b. 添加将目标主机添加到委派目标的任务：

```
  - name: Ensure servicedelegationtarget web-console-delegation-target member
principal host/remote.idm.example.com@IDM.EXAMPLE.COM is present
    ipaservicedelegationtarget:
      ipaadmin_password: "{{ ipaadmin_password }}"
      name: web-console-delegation-target
      principal: host/remote.idm.example.com@IDM.EXAMPLE.COM
      action: member
```

c. 添加一个任务来确保存在委派规则：

```
  - name: Ensure servicedelegationrule delegation-rule is present
    ipaservicedelegationrule:
      ipaadmin_password: "{{ ipaadmin_password }}"
      name: web-console-delegation-rule
```

d. 添加一项任务，该任务确保 Web 控制台客户端服务的 Kerberos 主体是受限委派规则的成员：

```
  - name: Ensure the Kerberos principal of the web console client service is added to the
servicedelegationrule web-console-delegation-rule
    ipaservicedelegationrule:
      ipaadmin_password: "{{ ipaadmin_password }}"
      name: web-console-delegation-rule
      principal: HTTP/myhost.idm.example.com
      action: member
```

e. 添加一个任务，以确保 delegation 规则与 web-console-delegation-target 委派目标关联：

```
  - name: Ensure a constrained delegation rule is associated with a specific delegation
target
    ipaservicedelegationrule:
      ipaadmin_password: "{{ ipaadmin_password }}"
      name: web-console-delegation-rule
      target: web-console-delegation-target
      action: member
```

3. 保存该文件。

4. 运行 Ansible playbook。指定 playbook 文件、存储保护 **secret.yml** 文件的密码，以及清单文件：

```
$ ansible-playbook --vault-password-file=password_file -v -i inventory web-console-
smart-card-ssh.yml
```

5. 在 **remote.idm.example.com** 上启用 Kerberos 身份验证：

a. 以 **root** 身份通过 **SSH** 连接到 **remote.idm.example.com**。

b. 打开 **/etc/ssh/sshd_config** 文件进行编辑。

c. 通过取消注释 **GSSAPIAuthentication no** 行，并将它替换为 **GSSAPIAuthentication yes** 来启用 **GSSAPIAuthentication**。

其它资源

- 使用智能卡登录到 web 控制台
- 身份管理中的受限委托
- **/usr/share/doc/ansible-freeipa/** 目录中的 **README-servicedelegationrule.md** 和 **README-servicedelegationtarget.md**
- **/usr/share/doc/ansible-freeipa/playbooks/servicedelegationtarget** 和 **/usr/share/doc/ansible-freeipa/playbooks/servicedelegationrule** 目录中的 playbook 示例

第 32 章 为 IDM 域中的 RHEL 9 WEB 控制台配置单点登录

了解如何使用 RHEL 9 web 控制台中的 Identity Management(IdM)提供的单点登录(SSO)身份验证。

优点：

- IdM 域管理员可以使用 RHEL 9 web 控制台来管理本地机器。
- IdM 域中具有 Kerberos 票据的用户不需要提供登录凭据来访问 Web 控制台。
- IdM 域已知的所有主机均可通过 RHEL 9 web 控制台本地实例的 SSH 访问。
- 不需要证书配置。控制台的 Web 服务器会自动切换到 IdM 证书颁发机构发布的证书，并被浏览器接受。

本章论述了配置用于登录到 RHEL web 控制台的 SSO 的步骤：

1. 使用 RHEL 9 web 控制台将机器添加到 IdM 域中。
   详情请参阅使用 Web 控制台将 RHEL 9 系统添加到 IdM 域中 。
2. 如果要使用 Kerberos 进行身份验证，则需要在机器上获得 Kerberos ticket。
   详情请参阅使用 Kerberos 身份验证登录到 web 控制台。
3. 允许 IdM 服务器上的管理员在任何主机上运行任何命令。
   详情请参阅为 IdM 服务器上的域管理员启用管理员的 admin sudo 访问权限

先决条件

- 在 RHEL 9 系统上安装的 RHEL web 控制台。
  详情请参阅安装 Web 控制台。
- 在使用 RHEL web 控制台的系统中安装 IdM 客户端。
  详情请查看 IdM 客户端安装。

32.1. 使用 WEB 控制台将 RHEL 9 系统添加到 IDM 域中

您可以使用 Web 控制台将 Red Hat Enterprise Linux 9 系统添加到 Identity Management(IdM)域中。

先决条件

- IdM 域正在运行，并可访问您想要加入的客户端。
- 您有 IdM 域管理员凭证。

流程

1. 登录到 RHEL web 控制台。
   详情请参阅 登录到 web 控制台。
2. 在 **Overview** 选项卡的 **Configuration** 字段中点 **Join Domain**。
3. 在 **Join a Domain** 对话框的 **Domain Address** 字段中输入 IdM 服务器的主机名。
4. 在 **Domain administrator name** 字段中输入 IdM 管理帐户的用户名。

5. 在域 **管理员密码** 中，添加密码。
6. 点 **Join**。

验证步骤

1. 如果 RHEL 9 web 控制台没有显示错误，系统已加入到 IdM 域，您可以在 **System** 屏幕中看到域名。
2. 要验证该用户是否为域的成员，点 Terminal 页面并输入 **id** 命令：

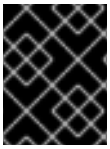
```
$ id
euid=548800004(example_user) gid=548800004(example_user)
groups=548800004(example_user) context=unconfined_u:unconfined_r:unconfined_t:s0-
s0:c0.c1023
```

其它资源

- 规划身份管理
- 安装身份管理
- 管理 IdM 用户、组、主机和访问控制规则

32.2. 使用 KERBEROS 身份验证登录到 WEB 控制台

以下流程描述了如何设置 RHEL 9 系统以使用 Kerberos 验证的步骤。



重要

使用 SSO 时，通常在 Web 控制台中拥有任何管理特权。这只有在您配置了免密码 sudo 时有效。Web 控制台不以交互方式询问 sudo 密码。

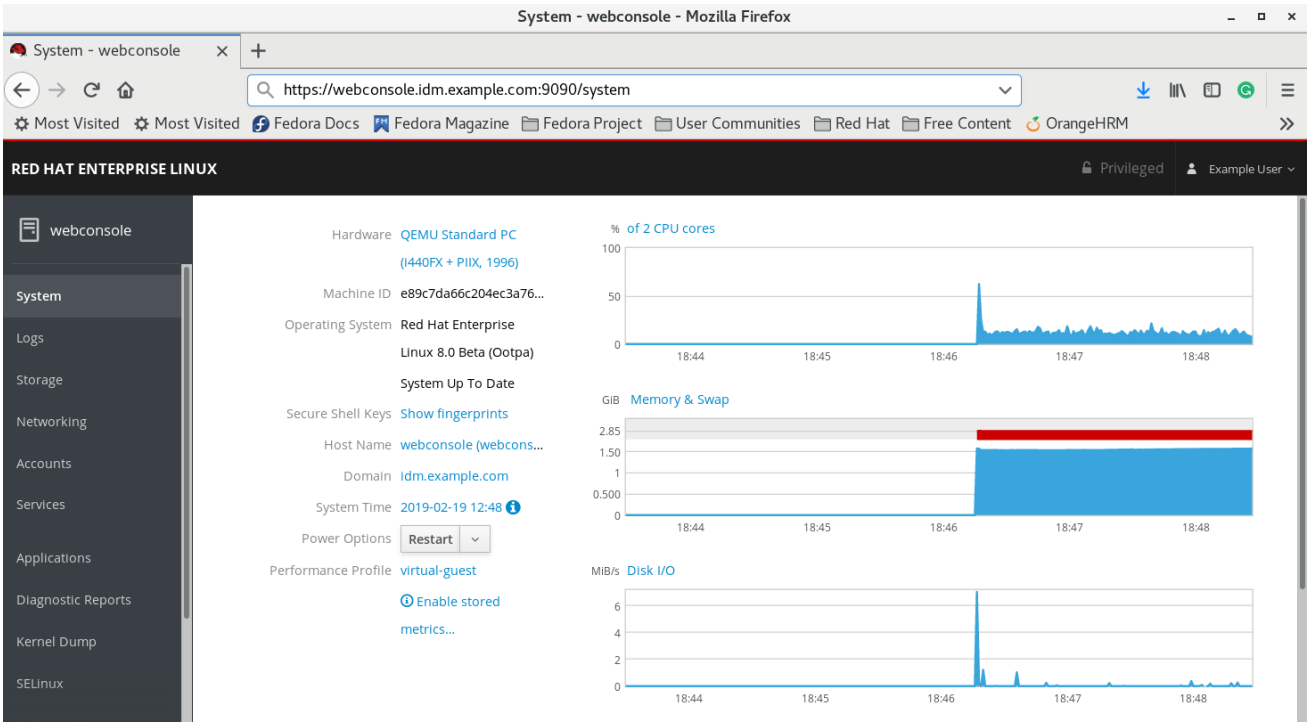
先决条件

- IdM 域在您的公司环境中运行并可访问。
  详情请参阅使用 Web 控制台将 RHEL 9 系统添加到 IdM 域中 。
- 在您要通过 RHEL web 控制台连接和管理的远程系统中启用 **cockpit.socket** 服务。
  详情请参阅安装 Web 控制台。
- 如果系统没有使用 SSSD 客户端管理的 Kerberos ticket，请尝试使用 **kinit** 程序手动请求 ticket。

流程

使用以下地址登录到 RHEL web 控制台：**https://dns_name:9090**

此时，您已成功连接到 RHEL web 控制台，您可以使用配置启动。



32.3. 为 IDM 服务器上的域管理员启用管理员 SUDO 访问权限

您可以使用 RHEL web 控制台，允许域管理员在身份管理(IdM)域中的任何主机上使用任何命令。

要实现这一目的，请启用对 IdM 服务器安装过程中自动创建的 **admins** 用户组的 sudo 访问权限。如果您对组运行 **ipa-advise** 脚本，则添加到 **admins** 组的所有用户都会获得 sudo 权限。

先决条件

- 服务器运行 IdM 4.7.1 或更高版本。

流程

1. 连接到 IdM 服务器。
2. 运行 ipa-advise 脚本：

```
$ ipa-advise enable-admins-sudo | sh -ex
```

如果控制台没有显示错误，则 **admins** 组对 IdM 域中的所有机器有 sudo 权限。

第 33 章 使用 WEB 控制台为集中管理的用户配置智能卡验证

在 RHEL web 控制台中为集中管理的用户配置智能卡验证：

- 身份管理
- Active Directory，它在 Identity Management 的跨林信任中连接

先决条件

- 您要使用智能卡验证的系统必须是 Active Directory 或 Identity Management 域的成员。
- 用于智能卡验证的证书必须与身份管理或 Active Directory 中的特定用户关联。
  有关在 Identity Management 中将证书与用户关联的详情，请参阅在 IdM Web UI 中的用户条目中添加证书，或将证书添加到 IdM CLI 中的用户条目中。

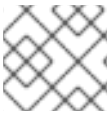
33.1. 实现中央管理用户的智能卡验证

智能卡是一个物理设备，可以使用保存在卡中的证书提供个人验证。个人验证意味着，您可以象使用用户密码一样使用智能卡。

您可以使用私钥和证书的形式在智能卡中保存用户凭证。特殊的软件和硬件可用于访问它们。您可以将智能卡插入到读取器或者 USB 套接字中，并为智能卡提供 PIN 代码，而不是提供密码。

身份管理(IdM)支持使用如下方式的智能卡身份验证：

- IdM 证书颁发机构发布的用户证书。
- Active Directory 证书服务(ADCS)证书颁发机构发布的用户证书。



注意

如果要使用智能卡验证，请参阅硬件要求：RHEL8+ 中的智能卡支持。

33.2. 安装用来管理和使用智能卡的工具

先决条件

- **gnutls-utils** 软件包已安装。
- **opensc** 软件包已安装。
- **pcscd** 服务正在运行。

在配置智能卡前，您必须安装相应的工具，该工具可以生成证书，并启动 **pscd** 服务。

流程

1. 安装 **opensc** 和 **gnutls-utils** 软件包：

```
# dnf -y install opensc gnutls-utils
```

2. 启动 **pcscd** 服务。

```
# systemctl start pcscd
```

验证步骤

- 验证 **pcscd** 服务是否已启动并运行

```
# systemctl status pcscd
```

33.3. 准备智能卡并将证书和密钥上传到智能卡

按照以下流程，使用 **pkcs15-init** 工具配置智能卡，该工具可帮助您配置：

- 擦除智能卡
- 设置新的 PIN 和可选的 PIN Unblocking Keys（PUKs）
- 在智能卡上创建新插槽
- 在插槽存储证书、私钥和公钥
- 如果需要，请锁定智能卡设置，因为某些智能卡需要这个类型的最终化

注意

pkcs15-init 工具可能无法使用所有智能卡。您必须使用您使用智能卡的工具。

先决条件

- 已安装 **opensc** 软件包，其中包括 **pkcs15-init** 工具。
  如需了解更多详细信息，请参阅 安装用于管理和使用智能卡的工具。
- 该卡插入读卡器并连接到计算机。
- 您有一个要存储在智能卡上的私钥、公钥和证书。在此流程中，**testuser.key**、**testuserpublic.key** 和 **testuser.crt** 是用于私钥、公钥和证书的名称。
- 您有当前的智能卡用户 PIN 和 Security Officer PIN (SO-PIN)。

流程

1. 擦除智能卡并使用您的 PIN 验证自己：

```
$ pkcs15-init --erase-card --use-default-transport-keys
Using reader with a card: Reader name
PIN [Security Officer PIN] required.
Please enter PIN [Security Officer PIN]:
```

   这个卡已经被清除。

2. 初始化智能卡，设置您的用户 PIN 和 PUK，以及您的安全响应 PIN 和 PUK：

```
$ pkcs15-init --create-pkcs15 --use-default-transport-keys \ --pin 963214 --puk 321478 --so-pin 65498714 --so-puk 784123
Using reader with a card: Reader name
```

pcks15-init 工具在智能卡上创建一个新插槽。

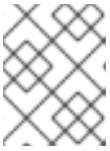
3. 为插槽设置标签和验证 ID：

```
$ pkcs15-init --store-pin --label testuser \ --auth-id 01 --so-pin 65498714 --pin 963214 --puk
321478
Using reader with a card: Reader name
```

标签设置为人类可读的值，在本例中为 **testuser**。**auth-id** 必须是两个十六进制值，在本例中设为 **01**。

4. 在智能卡的新插槽中存储并标记私钥：

```
$ pkcs15-init --store-private-key testuser.key --label testuser_key \ --auth-id 01 --id 01 --pin
963214
Using reader with a card: Reader name
```



注意

在存储您的私钥并将证书存储在下一步中时，您为 **--id** 指定的值必须相同。建议为 **--id** 指定自己的值，否则它们将更复杂的值由工具计算。

5. 在智能卡上的新插槽中存储并标记该证书：

```
$ pkcs15-init --store-certificate testuser.crt --label testuser_crt \ --auth-id 01 --id 01 --format
pem --pin 963214
Using reader with a card: Reader name
```

6. 可选：在智能卡上的新插槽中保存并标记公钥：

```
$ pkcs15-init --store-public-key testuserpublic.key --label testuserpublic_key --auth-id 01 --id
01 --pin 963214
Using reader with a card: Reader name
```

注意

如果公钥与私钥或证书对应，请指定与私钥或证书的 ID 相同的 ID。

7. 可选：某些智能卡要求您通过锁定设置来完成卡：

```
$ pkcs15-init -F
```

此时您的智能卡在新创建的插槽中包含证书、私钥和公钥。您还创建了您的用户 PIN 和 PUK，以及安全响应 PIN 和 PUK。

33.4. 为 WEB 控制台启用智能卡验证

要在 web 控制台中使用智能卡验证，请在 **cockpit.conf** 文件中启用智能卡验证。

另外，您还可以在同一文件中禁用密码验证。

先决条件

- 已安装 RHEL web 控制台。

流程

1. 使用管理员权限登录到 RHEL web 控制台。
2. 点 **Terminal**。
3. 在 **/etc/cockpit/cockpit.conf** 中，将 **ClientCertAuthentication** 设置为 **yes** ：

```
[WebService]
ClientCertAuthentication = yes
```

4. 可选：在 **cockpit.conf** 中禁用基于密码的身份验证：

```
[Basic]
action = none
```

这个配置禁用了密码验证，且必须总是使用智能卡。

5. 重启 Web 控制台，以确保 **cockpit.service** 接受更改：

```
# systemctl restart cockpit
```

33.5. 使用智能卡登录到 WEB 控制台

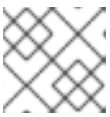
您可以使用智能卡登录到 web 控制台。

先决条件

- 保存在智能卡中的有效证书，该证书与 Active Directory 或 Identity Management 域中的用户帐户关联。
- PIN 用于解锁智能卡。
- 已经将智能卡放入读卡器。

流程

1. 打开 Web 浏览器，并在地址栏中添加 Web 控制台的地址。
浏览器要求您添加 PIN 保护保存在智能卡中的证书。
2. 在 **Password Required** 对话框中，输入 PIN 并点 **OK**。
3. 在 **User Identification Request** 对话框中，选择保存在智能卡中的证书。
4. 选择 **Remember this decision**。
系统下次打开这个窗口。



注意

此步骤不适用于 Google Chrome 用户。

5. 点击 **确定**。

您现在已连接，Web 控制台会显示其内容。

33.6. 为智能卡用户启用无密码的 SUDO 验证

您可以使用 Web 控制台为智能卡用户配置 **sudo** 和其他服务的无密码身份验证。

另一种选择是，如果您使用红帽身份管理，您可以将初始 Web 控制台证书身份验证声明为可信，以向 **sudo**、SSH 或其他服务进行身份验证。为此，Web 控制台会在用户会话中自动创建 S4U2Proxy Kerberos ticket。

先决条件

- 身份管理已安装。
- 跨林信任中与身份管理连接的活动目录。
- 设置为登录到 web 控制台的智能卡。如需更多信息，请参阅使用 Web 控制台配置智能卡验证。

流程

1. 设置约束委派规则，以列出托管票据可以访问哪些主机。

例 33.1. 设置约束委派规则

Web 控制台会话运行主机 **host.example.com**，并应受信任，以通过 **sudo** 访问自己的主机。此外，我们还添加了第二个可信主机 - **remote.example.com**。

- 创建以下委派：
  - 运行以下命令添加特定规则可以访问的目标机器列表：

```
# ipa servicedelegationtarget-add cockpit-target
# ipa servicedelegationtarget-add-member cockpit-target \ --
principals=host/host.example.com@EXAMPLE.COM \ --
principals=host/remote.example.com@EXAMPLE.COM
```

  - 要允许 Web 控制台会话(HTTP/principal)访问该主机列表，请使用以下命令：

```
# ipa servicedelegationrule-add cockpit-delegation
# ipa servicedelegationrule-add-member cockpit-delegation \ --
principals=HTTP/host.example.com@EXAMPLE.COM
# ipa servicedelegationrule-add-target cockpit-delegation \ --
servicedelegationtargets=cockpit-target
```

2. 在对应服务中启用 GSS 身份验证：

   a. 对于 sudo，在 **/etc/sssd/sssd.conf** 文件中启用 **pam_sss_gss** 模块：

      i. 以 root 用户身份，将域的条目添加到 **/etc/sssd/sssd.conf** 配置文件。

```
[domain/example.com]
pam_gssapi_services = sudo, sudo-i
```

ii. 在第一行启用 **/etc/pam.d/sudo** 文件中的模块。

```
auth sufficient pam_sss_gss.so
```

b. 对于 SSH，将 **/etc/ssh/sshd_config** 文件中的 **GSSAPIAuthentication** 选项更新为 **yes**。

警告

从 Web 控制台连接到远程 SSH 主机时，委派的 S4U 票据不会被转发到远程 SSH 主机。使用您的票据在远程主机上向 sudo 进行身份验证将无法正常工作。

验证

1. 使用智能卡登录到 web 控制台。
2. 点 **Limited access** 按钮。
3. 使用您的智能卡进行验证。

或者：

- 尝试使用 SSH 连接到其他主机。

33.7. 限制用户会话和内存以防止 DOS 攻击

证书验证被分离和隔离 **cockpit-ws** Web 服务器的实例保护，使其免受要模拟其他用户的攻击者的攻击。但是，这会引入了一个潜在的拒绝服务(DoS)攻击：远程攻击者可以创建大量证书，并将大量 HTTPS 请求发送到 **cockpit-ws** 各自使用不同的证书。

为防止这一 DoS，这些 Web 服务器实例的收集资源受到限制。默认情况下，对连接数量和内存用量限制为 200 个线程，且具有 75%（软）/ 90%（硬）内存限值。

以下流程描述了通过限制连接和内存量的资源保护。

流程

1. 在终端中，打开 **system-cockpithttps.slice** 配置文件：

```
# systemctl edit system-cockpithttps.slice
```

2. 将 **TasksMax** 限制为 *100*，将 **CPUQuota** 限制为 *30%* ：

```
[Slice]
# change existing value
TasksMax=100
# add new restriction
CPUQuota=30%
```

3. 要应用这些更改，请重启系统：

-

```
# systemctl daemon-reload
# systemctl stop cockpit
```

现在，新的内存和用户会话限制了 **cockpit-ws** Web 服务器不受 DoS 攻击。

第 34 章 SATELLITE 主机管理和监控

Red Hat Satellite 是一个系统管理解决方案，可在物理、虚拟和云环境中部署、配置和维护您的系统。Satellite 使用集中工具提供对多个 Red Hat Enterprise Linux 部署的配置、远程管理和监控。

默认情况下，RHEL web 控制台集成在 Red Hat Satellite 中被禁用。要从 Red Hat Satellite 内部访问主机的 Red Hat Web 控制台功能，您必须首先在 Red Hat Satellite 服务器上启用 RHEL web 控制台集成。

在 web 控制台中大规模管理许多主机的 Satellite 文档

- 有关集成 RHEL web 控制台和 Satellite 的详情，请参阅在 Satellite 中启用 RHEL web 控制台 。
- 有关使用 Web 控制台管理和监控主机的更多信息，请参阅使用 RHEL web 控制台管理和监控主机。

第 35 章 使用 RHEL WEB 控制台管理容器镜像

您可以使用 RHEL web 控制台基于 Web 的界面来拉取、修剪或删除您的容器镜像。

35.1. 在 WEB 控制台中拉取容器镜像

您可以将容器镜像下载到本地系统，并使用它们创建容器。

先决条件

- Web 控制台已安装并可以访问。如需更多信息，请参阅 安装 Web 控制台 和 登录到 Web 控制台。
- **cockpit-podman** 附加组件已安装：

```
# dnf install cockpit-podman
```

流程

1. 点主菜单中的 **Podman containers**。
2. 在 **Images** 表中，单击右上角的溢出菜单，然后选择 **Download new image**。
3. 此时会出现 **Search for an image**对话框。
4. 在 **Search for** 字段中输入镜像的名称或指定其描述。
5. 在 **in** 下拉列表中，选择要从中拉取镜像的注册中心。
6. 可选：在 **Tag** 字段中输入镜像标签。
7. 点 **Download**。

验证

- 点主菜单中的 **Podman containers**。您可以在 **Images** 表中看到新下载的镜像。

注意

您可以通过点 **Images** 表中的 **Create container**，从下载的镜像创建容器。要创建容器，请按照 在 web 控制台中创建容器 中的步骤 3-8。

35.2. 在 WEB 控制台中修剪容器镜像

您可以删除所有未使用的，没有任何容器基于它的镜像。

先决条件

- 至少一个容器镜像会被拉取。
- Web 控制台已安装并可以访问。如需更多信息，请参阅 安装 Web 控制台 和 登录到 Web 控制台。
- **cockpit-podman** 附加组件已安装：

```
# dnf install cockpit-podman
```

流程

1. 点主菜单中的 **Podman containers**。
2. 在 **Images** 表中，单击右上角的溢出菜单，然后选择 **Prune unused images**。
3. 此时会显示镜像列表的弹出窗口。点 **Prune** 确认您的选择。

验证

- 点主菜单中的 **Podman containers**。删除的镜像不应列在 **Images** 表中。

35.3. 在 WEB 控制台中删除容器镜像

您可以使用 Web 控制台删除之前拉取的容器镜像。

先决条件

- 至少一个容器镜像会被拉取。
- Web 控制台已安装并可以访问。如需更多信息，请参阅 安装 Web 控制台 和 登录到 Web 控制台。
- **cockpit-podman** 附加组件已安装：

```
# dnf install cockpit-podman
```

流程

1. 点主菜单中的 **Podman containers**。
2. 在 **Images** 表中，选择您要删除的镜像，然后点溢出菜单并选择 **Delete**。
3. 此时会出现一个窗口。点 **Delete tagged images** 确认您的选择。

验证

- 点主菜单中的 **Podman containers**。删除的容器不应列在 **Images** 表中。

第 36 章 使用 RHEL WEB 控制台管理容器

您可以使用 Red Hat Enterprise Linux Web 控制台管理容器和 pod。使用 Web 控制台，您可以以非 root 或 root 用户身份创建容器。

- 作为 *root* 用户，您可以使用额外的特权和选项创建系统容器。
- 作为 *非 root* 用户，您有两个选项：
  - 要仅创建用户容器，您可以在其默认模式 - **Limited access** 中使用 Web 控制台。
  - 要创建用户和系统容器，请单击 Web 控制台页面顶部面板中的 **Administrative access**。

有关根和无根容器之间的区别的详情，请参阅 无根容器的特殊注意事项。

36.1. 在 WEB 控制台中创建容器

您可以创建容器并添加端口映射、卷、环境变量、健康检查等。

先决条件

- Web 控制台已安装并可以访问。如需更多信息，请参阅 安装 Web 控制台 和 登录到 Web 控制台。
- **cockpit-podman** 附加组件已安装：

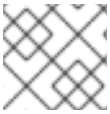
```
# dnf install cockpit-podman
```

流程

1. 点主菜单中的 **Podman containers**。
2. 点 **Create container**。
3. 在 **Name** 字段中输入容器的名称。
4. 在 **Details** 选项卡中提供所需信息。
   - *仅适用于管理访问权限*：选择容器的所有者：系统或用户。
   - 在 **Image** 下拉列表中，选择或搜索所选注册中心中的容器镜像。
     - 可选：选中 **Pull latest image** 复选框，以拉取最新的容器镜像。
   - **Command** 字段指定命令。如果需要，您可以更改默认命令。
     - 可选：选中 **With terminal** 复选框，以使用终端运行容器。
   - **Memory limit** 字段指定容器的内存限制。要更改默认内存限制，请选中复选框并指定限制。
   - *仅适用于系统容器*：在 **CPU shares 字段**中，指定 CPU 时间的相对量。默认值为 1024。选中复选框以修改默认值。
   - *仅适用于系统容器*：在 **Restart policy** 下拉菜单中，选择以下选项之一：
     - **No**（默认值）：无操作。

- On Failure ：在失败时重启容器。
- Always ：在退出或重启系统后重启容器。

5. 在 Integration 选项卡中提供所需的信息。
   - 点 **Add port mapping**，来在容器和主机系统之间添加端口映射。
     - 输入 *IP 地址*、*Host port*、*Container port* 和 *Protocol*。
   - 点 **Add volume** 添加卷。
     - 输入 *host path*、*Container path*。您可以选择 **Writable** 选项复选框来创建一个可写卷。在 SELinux 下拉列表中选择以下选项之一：**No Label**、**Shared** 或 **Private**。
   - 单击 **Add variable** 以添加环境变量。
     - 输入 *Key* 和 *Value*。
6. 在 Health check 选项卡中提供所需的信息。
   - 在 **Command** 字段中，输入 'healthcheck' 命令。
   - 指定 healthcheck 选项：
     - **Interval**（默认为 30 秒）
     - **Timeout**（默认为 30 秒）
     - **Start period**
     - **Retries** （默认为 3）
     - 当不健康时：选择以下选项之一：
       - **No action**（默认）：不执行任何操作。
       - **Restart** ：重启容器。
       - **Stop** ：停止容器。
       - **Force stop** ：强制停止容器，它不等待容器退出。
7. 点 **Create and run** 创建并运行容器。



注意

您可以点击 **Create** 来只创建容器。

验证

- 点主菜单中的 **Podman containers**。您可以在 **Containers** 表中看到新创建的容器。

36.2. 在 WEB 控制台中检查容器

您可以在 web 控制台中显示容器的详细信息。

先决条件

- 容器已创建。
- Web 控制台已安装并可以访问。如需更多信息，请参阅 安装 Web 控制台 和 登录到 Web 控制台。
- **cockpit-podman** 附加组件已安装：

```
# dnf install cockpit-podman
```

流程

1. 点主菜单中的 **Podman containers**。
2. 点 **>** 箭头图标查看容器的详情。
   - 在 **Details** 选项卡中，您可以看到容器 ID、镜像、命令、创建时间（创建容器时的时间戳）及其状态。
     - *仅适用于系统容器*：您还可以查看 IP 地址、MAC 地址和网关地址。
   - 在 **Integration** 选项卡中，您可以看到环境变量、端口映射和卷。
   - 在 **Log** 选项卡中，您可以看到容器日志。
   - 在 **Console** 选项卡中，您可以使用命令行与容器进行交互。

36.3. 在 WEB 控制台中更改容器状态

在 Red Hat Enterprise Linux web 控制台中，您可以启动、停止、重启、暂停和重命名系统上的容器。

先决条件

- 容器已创建。
- Web 控制台已安装并可以访问。如需更多信息，请参阅 安装 Web 控制台 和 登录到 Web 控制台。
- **cockpit-podman** 附加组件已安装：

```
# dnf install cockpit-podman
```

流程

1. 点主菜单中的 **Podman containers**。
2. 在 **Containers** 表中，选择您要修改的容器，点击溢出菜单并选择您要执行的操作：
   - **Start**
   - **Stop**
   - **Force stop**
   - **Restart**

- Force restart
- Pause
- Rename

36.4. 在 WEB 控制台中提交容器

您可以根据容器的当前状态创建新镜像。

先决条件

- 容器已创建。
- Web 控制台已安装并可以访问。如需更多信息，请参阅 安装 Web 控制台 和 登录到 Web 控制台。
- **cockpit-podman** 附加组件已安装：

```
# dnf install cockpit-podman
```

流程

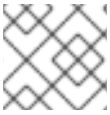
1. 点主菜单中的 **Podman containers**。
2. 在 **Containers** 表中，选择您要修改的容器，点击溢出菜单并选择 **Commit**。
3. 在 **Commit container** 表单中，添加以下详情：
   - 在 **New image name** 字段中输入镜像名称。
   - 可选：在 **Tag** 字段中输入标签。
   - 可选：在 **Author** 字段中输入您的名称。
   - 可选：在 **Command** 字段中，如果需要更改命令。
   - 可选：检查您需要的 **Options** ：
     - 在创建镜像时暂停容器：容器及其进程在提交镜像时暂停。
     - 使用传统的 Docker 格式：如果您不使用 Docker 镜像格式，请使用 OCI 格式。
4. 点 **Commit**。

验证

- 点主菜单中的 **Podman containers**。您可以在 **Images** 表中看到新创建的镜像。

36.5. 在 WEB 控制台中创建容器检查点

使用 Web 控制台，您可以在正在运行的容器或单个应用程序上设置检查点，并将其状态存储到磁盘中。



注意

创建检查点仅适用于系统容器。

先决条件

- 容器正在运行。
- Web 控制台已安装并可以访问。如需更多信息，请参阅 安装 Web 控制台 和 登录到 Web 控制台。
- **cockpit-podman** 附加组件已安装：

```
# dnf install cockpit-podman
```

流程

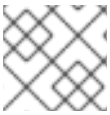
1. 点主菜单中的 **Podman containers**。
2. 在 **Containers** 表中，选择您要修改的容器，点击溢出图标菜单并选择 **Checkpoint**。
3. 可选：在 **Checkpoint container** 表单中，检查您需要的选项：
   - 保留所有临时检查点文件：在检查点过程中保留 CRIU 创建的所有临时日志和统计数据文件。如果检查点失败，则这些文件不会被删除，用于进一步调试。
   - 将检查点写入磁盘后让其继续运行：让容器在检查点后继续运行，而不是停止它。
   - 支持保留建立的 TCP 连接
4. 点 **Checkpoint**。

验证

- 点主菜单中的 **Podman containers**。选择您做了检查点的容器，点溢出菜单图标，并验证是否有 **Restore** 选项。

36.6. 在 WEB 控制台中恢复容器检查点

您可以在重启时同时使用保存的数据来恢复容器。



注意

创建检查点仅适用于系统容器。

先决条件

- 已对容器执行了检查点。
- Web 控制台已安装并可以访问。如需更多信息，请参阅 安装 Web 控制台 和 登录到 Web 控制台。
- **cockpit-podman** 附加组件已安装：

```
# dnf install cockpit-podman
```

-

流程

1. 点主菜单中的 **Podman containers**。
2. 在 **Containers** 表中，选择您要修改的容器，点击溢出菜单，并选择 **Restore**。
3. 可选：在 **Restore container** 表单中，检查您需要的选项：
   - **保留所有临时检查点文件** ：保留检查点过程中 CRIU 创建的所有临时日志和统计数据文件。如果检查点失败，则这些文件不会被删除，用于进一步调试。
   - **恢复建立的 TCP 连接**
   - **如果设置为静态，则忽略 IP 地址** ：如果容器使用 IP 地址启动，恢复的容器也会尝试使用该 IP 地址，如果该 IP 地址已在使用，则恢复会失败。如果您在创建容器时在 Integration 选项卡中添加了端口映射，则此选项适用。
   - **如果设置为静态，则忽略 MAC 地址** ：如果容器使用 MAC 地址启动，恢复的容器也会尝试使用该 MAC 地址，如果该 MAC 地址已在使用，则恢复会失败。
4. 单击 **Restore**。

验证

- 点主菜单中的 **Podman containers**。您可以在 **Containers** 表中看到恢复的容器正在运行。

36.7. 在 WEB 控制台中删除容器

您可以使用 Web 控制台删除现有容器。

先决条件

- 容器在系统上存在。
- Web 控制台已安装并可以访问。如需更多信息，请参阅 安装 Web 控制台 和 登录到 Web 控制台。
- **cockpit-podman** 附加组件已安装：

```
# dnf install cockpit-podman
```

流程

1. 点主菜单中的 **Podman containers**。
2. 在 **Containers** 表中，选择您要删除的容器，点击溢出菜单，并选择 **Delete**。
3. 此时会出现弹出窗口。点 **Delete** 确认您的选择。

验证

- 点主菜单中的 **Podman containers**。删除的容器不应列在 **Containers** 表中。

36.8. 在 WEB 控制台中创建 POD

您可以在 RHEL web 控制台界面中创建 pod。

先决条件

- Web 控制台已安装并可以访问。如需更多信息，请参阅 安装 Web 控制台 和 登录到 Web 控制台。
- **cockpit-podman** 附加组件已安装：

```
# dnf install cockpit-podman
```

流程

1. 点主菜单中的 **Podman containers**。
2. 点 **Create pod**。
3. 在 **Create pod** 表单中提供所需信息：
   - *仅适用于管理访问权限*：选择容器的所有者：系统或用户。
   - 在 **Name** 字段中输入容器的名称。
   - 点 **Add port mapping** 在容器和主机系统之间添加端口映射。
     - 输入 IP 地址、主机端口、容器端口和协议。
   - 点 **Add volume** 添加卷。
     - 输入主机路径，容器路径。您可以选择 Writable 复选框来创建可写卷。在 SELinux 下拉列表中选择以下选项之一：No Label, Shared or Private。
4. 点 **Create**。

验证

- 点主菜单中的 **Podman containers**。您可以在 **Containers** 表中看到新创建的 pod。

36.9. 在 WEB 控制台中的 POD 中创建容器

您可以在 pod 中创建容器。

先决条件

- Web 控制台已安装并可以访问。如需更多信息，请参阅 安装 Web 控制台 和 登录到 Web 控制台。
- **cockpit-podman** 附加组件已安装：

```
# dnf install cockpit-podman
```

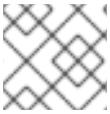
流程

1. 点主菜单中的 **Podman containers**。
2. 点 **Create container in pod**。
3. 在 **Name** 字段中输入容器的名称。
4. 在 **Details** 选项卡中提供所需的信息。
   - *仅适用于管理访问权限* ：选择容器的所有者：系统或用户。
   - 在 **Image** 下拉列表中，选择或搜索所选注册中心中的容器镜像。
     - 可选：选中 **Pull latest image**复选框，以拉取最新的容器镜像。
   - **Command** 字段指定命令。如果需要，您可以更改默认命令。
     - 可选：选中 **With terminal**复选框，以使用终端运行容器。
   - **Memory limit**字段指定容器的内存限制。要更改默认内存限制，请选中复选框并指定限制。
   - *仅适用于系统容器* ：在 **CPU shares 字段**中，指定 CPU 时间的相对量。默认值为 1024。选中复选框以修改默认值。
   - *仅适用于系统容器* ：在 **Restart policy** 下拉菜单中，选择以下选项之一：
     - **No**（默认值）：无操作。
     - **On Failure** ：在失败时重启容器。
     - **Always** ：在退出或系统引导时重启容器。
5. 在 **Integration** 选项卡中提供所需的信息。
   - 点 **Add port mapping**，来在容器和主机系统之间添加端口映射。
     - 输入 *IP 地址*、*Host port*、*Container port* 和 *Protocol*。
   - 点 **Add volume** 添加卷。
     - 输入 *host path*、*Container path*。您可以选择 **Writable** 选项复选框来创建一个可写卷。在 SELinux 下拉列表中选择以下选项之一：**No Label**、**Shared** 或 **Private**。
   - 单击 **Add variable** 以添加环境变量。
     - 输入 *Key* 和 *Value*。
6. 在 **Health check** 选项卡中提供所需的信息。
   - 在 **Command** 字段中输入 healthcheck 命令。
   - 指定 healthcheck 选项：
     - **Interval**（默认为 30 秒）
     - **Timeout**（默认为 30 秒）
     - **Start period**
     - **Retries** （默认为 3）

- 当不健康时：选择以下选项之一：
  - **No action**（默认）：不执行任何操作。
  - **Restart**：重启容器。
  - **Stop**：停止容器。
  - **Force stop**：强制停止容器，它不等待容器退出。

注意

容器的所有者与 pod 的所有者相同。



注意

在 pod 中，您可以检查容器，更改容器的状态、提交容器或删除容器。

验证

- 点主菜单中的 **Podman containers**。您可以在 **Containers** 表下的 pod 中看到新创建的容器。

36.10. 在 WEB 控制台中更改 POD 的状态

您可以更改 pod 的状态。

先决条件

- pod 已创建。
- Web 控制台已安装并可以访问。如需更多信息，请参阅 安装 Web 控制台 和 登录到 Web 控制台。
- **cockpit-podman** 附加组件已安装：

```
# dnf install cockpit-podman
```

流程

1. 点主菜单中的 **Podman containers**。
2. 在 **Containers** 表中，选择要修改的 pod，点击溢出菜单，并选择您要执行的操作：
   - **Start**
   - **Stop**
   - **Force stop**
   - **Restart**
   - **Force restart**
   - **Pause**

36.11. 在 WEB 控制台中删除 POD

您可以使用 Web 控制台删除现有 pod。

先决条件

- pod 在系统上存在。
- Web 控制台已安装并可以访问。如需更多信息，请参阅 安装 Web 控制台 和 登录到 Web 控制台。
- **cockpit-podman** 附加组件已安装：

```
# dnf install cockpit-podman
```

流程

1. 点主菜单中的 **Podman containers**。
2. 在 **Containers** 表中，选择您要删除的 pod，点击溢出菜单，并选择 **Delete**。
3. 在以下弹出窗口中点击 **Delete** 以确认您的选择。

警告

您可以删除 pod 中的所有容器。

验证

- 点主菜单中的 **Podman containers**。已删除的 pod 不应列在 **Containers** 表中。