



## Red Hat Enterprise Linux 8

# RHEL 8 で Web コンソールを使用したシステムの 管理

グラフィカルな Web ベースのインターフェイスによるサーバー管理



# Red Hat Enterprise Linux 8 RHEL 8 で Web コンソールを使用したシステムの管理

---

グラフィカルな Web ベースのインターフェイスによるサーバー管理

## 法律上の通知

Copyright © 2024 Red Hat, Inc.

The text of and illustrations in this document are licensed by Red Hat under a Creative Commons Attribution–Share Alike 3.0 Unported license ("CC-BY-SA"). An explanation of CC-BY-SA is available at

<http://creativecommons.org/licenses/by-sa/3.0/>

. In accordance with CC-BY-SA, if you distribute this document or an adaptation of it, you must provide the URL for the original version.

Red Hat, as the licensor of this document, waives the right to enforce, and agrees not to assert, Section 4d of CC-BY-SA to the fullest extent permitted by applicable law.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, the Red Hat logo, JBoss, OpenShift, Fedora, the Infinity logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

Linux<sup>®</sup> is the registered trademark of Linus Torvalds in the United States and other countries.

Java<sup>®</sup> is a registered trademark of Oracle and/or its affiliates.

XFS<sup>®</sup> is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

MySQL<sup>®</sup> is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js<sup>®</sup> is an official trademark of Joyent. Red Hat is not formally related to or endorsed by the official Joyent Node.js open source or commercial project.

The OpenStack<sup>®</sup> Word Mark and OpenStack logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

All other trademarks are the property of their respective owners.

## 概要

RHEL Web コンソールは、アップストリームの Cockpit プロジェクトに基づいた Web ベースのグラフィカルインターフェイスです。これを使用すると、systemd サービスの検査と制御、ストレージの管理、ネットワークの設定、ネットワークの問題の分析、ログの検査などのシステム管理タスクを実行できます。

## 目次

|   |           |
|---|-----------|
| 多様性を受け入れるオープンソースの強化 .....                                     | 6         |
| RED HAT ドキュメントへのフィードバック (英語のみ) .....                          | 7         |
| <b>第1章 RHEL WEB コンソールの使用 .....</b>                            | <b>8</b>  |
| 1.1. RHEL WEB コンソールの概要 .....                                  | 8         |
| 1.2. WEB コンソールのインストールおよび有効化 .....                             | 8         |
| 1.3. WEB コンソールへのログイン .....                                    | 9         |
| 1.4. WEB コンソールのデフォルトのスタイル設定の変更 .....                          | 10        |
| 1.5. WEB コンソールでの基本認証の無効化 .....                                | 10        |
| 1.6. リモートマシンから WEB コンソールへの接続 .....                            | 11        |
| 1.7. ワンタイムパスワードを使用した WEB コンソールへのログイン .....                    | 12        |
| 1.8. WEB コンソールを使用したシステムの再起動 .....                             | 13        |
| 1.9. WEB コンソールでのシステムのシャットダウン .....                            | 13        |
| 1.10. WEB コンソールでの時間設定の設定 .....                                | 14        |
| 1.11. WEB コンソールを使用した RHEL 8 システムの IDM ドメインへの参加 .....          | 16        |
| 1.12. WEB コンソールを使用して CPU のセキュリティーの問題を防ぐために SMT を無効化する手順 ..... | 17        |
| 1.13. ログインページへのバナーの追加 .....                                   | 17        |
| 1.14. WEB コンソールでの自動アイドルロックの設定 .....                           | 19        |
| <b>第2章 WEB コンソールでのホスト名の設定 .....</b>                           | <b>21</b> |
| 2.1. ホスト名 .....   | 21        |
| 2.2. WEB コンソールでの PRETTY ホスト名 .....                            | 21        |
| 2.3. WEB コンソールを使用したホスト名の設定 .....                              | 21        |
| <b>第3章 WEB コンソールアドオンのインストールとカスタムページの作成 .....</b>              | <b>24</b> |
| 3.1. RHEL WEB コンソールのアドオン .....                                | 24        |
| 3.2. WEB コンソールでの新しいページの作成 .....                               | 24        |
| <b>第4章 WEB コンソールを使用したシステムパフォーマンスの最適化 .....</b>                | <b>26</b> |
| 4.1. WEB コンソールでのパフォーマンスチューニングオプション .....                      | 26        |
| 4.2. WEB コンソールでのパフォーマンスプロファイルの設定 .....                        | 26        |
| 4.3. WEB コンソールを使用したローカルシステムのパフォーマンスの監視 .....                  | 27        |
| 4.4. WEB コンソールと GRAFANA を使用して複数のシステムのパフォーマンスを監視する .....       | 29        |
| <b>第5章 WEB コンソールでログの確認 .....</b>                              | <b>32</b> |
| 5.1. WEB コンソールでログの確認 .....                                    | 32        |
| 5.2. WEB コンソールでのログのフィルタリング .....                              | 32        |
| 5.3. WEB コンソールでログをフィルターするためのテキスト検索オプション .....                 | 34        |
| 5.4. テキストボックスのボックスを使用した WEB コンソールでのログのフィルター .....             | 35        |
| 5.5. ログフィルタリングのオプション .....                                    | 36        |
| <b>第6章 WEB コンソールでユーザーアカウントの管理 .....</b>                       | <b>38</b> |
| 6.1. WEB コンソールで管理されるシステムユーザーアカウント .....                       | 38        |
| 6.2. WEB コンソールで新規アカウントの追加 .....                               | 38        |
| 6.3. WEB コンソールでパスワード有効期限の強制 .....                             | 39        |
| 6.4. WEB コンソールでユーザーセッションの終了 .....                             | 40        |
| <b>第7章 WEB コンソールでのサービスの管理 .....</b>                           | <b>41</b> |
| 7.1. WEB コンソールでのシステムサービスのアクティブ化または非アクティブ化 .....               | 41        |
| 7.2. WEB コンソールでのシステムサービスの再起動 .....                            | 42        |
| 7.3. WEB コンソールでのマニフェスト設定のオーバーライド .....                        | 43        |
| <b>第8章 WEB コンソールを使用したネットワークボンディングの設定 .....</b>                | <b>45</b> |

|   |           |
|---|-----------|
| 8.1. ボンディングモードに応じたアップストリームのスイッチ設定                       | 45        |
| 8.2. ボンディングモード  | 46        |
| 8.3. RHEL WEB コンソールを使用したネットワークボンディングの設定                 | 46        |
| 8.4. WEB コンソールを使用したボンドへのインターフェイスの追加                     | 50        |
| 8.5. WEB コンソールを使用したボンディングからインターフェイスの削除または無効化            | 50        |
| 8.6. WEB コンソールでのボンディングの削除または無効化                         | 51        |
| <b>第9章 WEB コンソールを使用したネットワークチームの設定</b>                   | <b>52</b> |
| 9.1. RHEL WEB コンソールを使用したネットワークチームの設定                    | 52        |
| 9.2. WEB コンソールを使用したチームへの新規インターフェイスの追加                   | 55        |
| 9.3. WEB コンソールを使用したチームからインターフェイスの削除または無効化               | 56        |
| 9.4. WEB コンソールでのチームの削除または無効化                            | 57        |
| <b>第10章 WEB コンソールでネットワークブリッジの設定</b>                     | <b>58</b> |
| 10.1. RHEL WEB コンソールを使用したネットワークブリッジの設定                  | 58        |
| 10.2. WEB コンソールでブリッジからインターフェイスを削除                       | 60        |
| 10.3. WEB コンソールでブリッジの削除                                 | 61        |
| <b>第11章 WEB コンソールで VLAN の設定</b>                         | <b>62</b> |
| 11.1. RHEL WEB コンソールを使用した VLAN タグ付けの設定                  | 62        |
| <b>第12章 WEB コンソールのリッスンポートの設定</b>                        | <b>65</b> |
| 12.1. アクティブな SELINUX があるシステムで新しいポートを許可                  | 65        |
| 12.2. FIREWALLD を使用したシステムでの新規ポートの許可                     | 65        |
| 12.3. WEB コンソールポートの変更                                   | 66        |
| <b>第13章 WEB コンソールでファイアウォールの管理</b>                       | <b>68</b> |
| 13.1. WEB コンソールを使用したファイアウォールの実行                         | 68        |
| 13.2. WEB コンソールを使用したファイアウォールの停止                         | 68        |
| 13.3. ファイアウォールゾーン                                       | 69        |
| 13.4. WEB コンソールのゾーン                                     | 71        |
| 13.5. WEB コンソールでゾーンの有効化                                 | 71        |
| 13.6. WEB コンソールを使用してファイアウォールでサービスを有効化                   | 73        |
| 13.7. WEB コンソールでカスタムポートの設定                              | 74        |
| 13.8. WEB コンソールを使用したゾーンの無効化                             | 76        |
| <b>第14章 WEB コンソールでシステム全体の暗号化ポリシーを設定する</b>               | <b>78</b> |
| <b>第15章 WEB コンソールで SELINUX 設定の ANSIBLE PLAYBOOK の作成</b> | <b>81</b> |
| <b>第16章 WEB コンソールでパーティションの管理</b>                        | <b>83</b> |
| 16.1. ファイルシステムでフォーマットされたパーティションを WEB コンソールに表示           | 83        |
| 16.2. WEB コンソールでパーティションの作成                              | 84        |
| 16.3. WEB コンソールでパーティションの削除                              | 86        |
| 16.4. WEB コンソールでのファイルシステムのマウントとマウント解除                   | 86        |
| <b>第17章 WEB コンソールで NFS マウントの管理</b>                      | <b>88</b> |
| 17.1. WEB コンソールで NFS マウントの接続                            | 88        |
| 17.2. WEB コンソールで NFS マウントオプションのカスタマイズ                   | 90        |
| <b>第18章 WEB コンソールで RAID の管理</b>                         | <b>91</b> |
| 18.1. WEB コンソールで RAID の作成                               | 91        |
| 18.2. WEB コンソールで RAID のフォーマット                           | 92        |
| 18.3. WEB コンソールを使用した RAID 上のパーティションテーブルの作成              | 94        |
| 18.4. WEB コンソールを使用した RAID 上のパーティションの作成                  | 95        |
| 18.5. WEB コンソールを使用した RAID 上のボリュームグループの作成                | 96        |

|  |            |
|--|------------|
| 18.6. 関連情報   | 97         |
| <b>第19章 WEB コンソールを使用した LVM 論理ボリュームの設定</b>                  | <b>98</b>  |
| 19.1. WEB コンソールの論理ボリュームマネージャー                              | 98         |
| 19.2. WEB コンソールでボリュームグループの作成                               | 99         |
| 19.3. WEB コンソールで論理ボリュームの作成                                 | 100        |
| 19.4. WEB コンソールで論理ボリュームのフォーマット                             | 102        |
| 19.5. WEB コンソールで論理ボリュームのサイズを変更                             | 105        |
| 19.6. 関連情報   | 107        |
| <b>第20章 WEB コンソールを使用したシン論理ボリュームの設定</b>                     | <b>108</b> |
| 20.1. WEB コンソールでシンプロビジョニングボリュームのプールの作成                     | 108        |
| 20.2. WEB コンソールでシンプロビジョニングされた論理ボリュームの作成                    | 109        |
| 20.3. WEB コンソールで論理ボリュームのフォーマット                             | 110        |
| 20.4. WEB コンソールを使用してシンプロビジョニングされたスナップショットボリュームの作成          | 113        |
| <b>第21章 WEB コンソールを使用してボリュームグループ内の物理ドライブを変更する</b>           | <b>116</b> |
| 21.1. WEB コンソールでボリュームグループに物理デバイスを追加                        | 116        |
| 21.2. WEB コンソールでボリュームグループから物理ドライブを削除                       | 116        |
| <b>第22章 WEB コンソールを使用した VIRTUAL DATA OPTIMIZER ボリュームの管理</b> | <b>118</b> |
| 22.1. WEB コンソールでの VDO ボリューム                                | 118        |
| 22.2. WEB コンソールで VDO ボリュームの作成                              | 119        |
| 22.3. WEB コンソールで VDO ボリュームのフォーマット                          | 120        |
| 22.4. WEB コンソールで VDO ボリュームの拡張                              | 122        |
| <b>第23章 RHEL WEB コンソールで LUKS パスワードを使用したデータのロック</b>         | <b>124</b> |
| 23.1. LUKS ディスクの暗号化  | 124        |
| 23.2. WEB コンソールで LUKS パスフレーズの設定                            | 125        |
| 23.3. WEB コンソールで LUKS パスフレーズの変更                            | 126        |
| <b>第24章 WEB コンソールで TANG キーを使用して自動ロック解除を設定する</b>            | <b>128</b> |
| <b>第25章 WEB コンソールでソフトウェア更新の管理</b>                          | <b>132</b> |
| 25.1. WEB コンソールでの手動ソフトウェア更新の管理                             | 132        |
| 25.2. WEB コンソールで自動ソフトウェア更新の管理                              | 132        |
| 25.3. WEB コンソールでソフトウェア更新適用後のオンデマンド再起動の管理                   | 133        |
| 25.4. WEB コンソールでのカーネルライブパッチを使用したパッチ適用                      | 134        |
| <b>第26章 WEB コンソールでサブスクリプションの管理</b>                         | <b>136</b> |
| 26.1. WEB コンソールでサブスクリプションの管理                               | 136        |
| 26.2. WEB コンソールで認証情報を使用してサブスクリプションを登録                      | 136        |
| 26.3. WEB コンソールでアクティベーションキーを使用してサブスクリプションを登録               | 138        |
| <b>第27章 WEB コンソールで KDUMP の設定</b>                           | <b>140</b> |
| 27.1. WEB コンソールで KDUMP メモリーの使用量およびターゲットの場所を設定              | 140        |
| <b>第28章 WEB コンソールでの仮想マシンの管理</b>                            | <b>143</b> |
| 28.1. WEB コンソールを使用した仮想マシンの管理の概要                            | 143        |
| 28.2. 仮想マシンを管理するために WEB コンソールを設定                           | 143        |
| 28.3. WEB コンソールを使用した仮想マシンの名前の変更                            | 144        |
| 28.4. WEB コンソールで利用可能な仮想マシンの管理機能                            | 145        |
| 28.5. 仮想マシンマネージャーと WEB コンソールでの仮想化機能の相違点                    | 146        |
| <b>第29章 WEB コンソールでリモートシステムの管理</b>                          | <b>149</b> |
| 29.1. WEB コンソールのリモートシステムマネージャー                             | 149        |

|  |            |
|--|------------|
| 29.2. WEB コンソールへのリモートシステムの追加   | 150        |
| 29.3. WEB コンソールでリモートホストの削除   | 153        |
| 29.4. 新しいホストの SSH ログインの有効化   | 156        |
| 29.5. アイデンティティ管理における制約付き委任   | 160        |
| 29.6. スマートカードで認証されたユーザーが、再度認証を要求されことなくリモートホストに SSH 接続できるようにするための WEB コンソールの設定            | 161        |
| 29.7. ANSIBLE を使用して WEB コンソールを設定し、スマートカードで認証されたユーザーが再認証を求められることなくリモートホストに SSH 接続できるようにする | 163        |
| <b>第30章 IDM ドメインで RHEL 8 WEB コンソールにシングルサインオンを設定</b>                                      | <b>166</b> |
| 30.1. WEB コンソールを使用した RHEL 8 システムの IDM ドメインへの参加   | 166        |
| 30.2. KERBEROS 認証を使用して WEB コンソールにログイン  | 167        |
| 30.3. 管理者の SUDO で IDM サーバーのドメイン管理者にアクセス可能に   | 168        |
| <b>第31章 集中管理ユーザー向けに WEB コンソールを使用したスマートカード認証の設定</b>                                       | <b>169</b> |
| 31.1. 集中管理ユーザーのスマートカード認証   | 169        |
| 31.2. スマートカードを管理および使用するツールのインストール  | 170        |
| 31.3. スマートカードを準備し、証明書と鍵をスマートカードにアップロードする   | 170        |
| 31.4. WEB コンソールのスマートカード認証の有効化  | 172        |
| 31.5. スマートカードを使用して WEB コンソールへのログイン   | 173        |
| 31.6. DOS 攻撃を防ぐためのユーザーセッションおよびメモリーの制限  | 173        |
| 31.7. 関連情報   | 174        |
| <b>第32章 SATELLITE ホストの管理と監視</b>  | <b>175</b> |
| <b>第33章 RHEL WEB コンソールを使用したコンテナイメージの管理</b>   | <b>176</b> |
| 33.1. WEB コンソールでのコンテナイメージの取得   | 176        |
| 33.2. WEB コンソールでのコンテナイメージのプルーニング   | 176        |
| 33.3. WEB コンソールでのコンテナイメージの削除   | 177        |
| <b>第34章 RHEL WEB コンソールを使用したコンテナの管理</b>   | <b>178</b> |
| 34.1. WEB コンソールでのコンテナの作成   | 178        |
| 34.2. WEB コンソールでのコンテナの検査   | 180        |
| 34.3. WEB コンソールでのコンテナの状態の変更  | 180        |
| 34.4. WEB コンソールでのコンテナのコミット   | 181        |
| 34.5. WEB コンソールでのコンテナチェックポイントの作成   | 182        |
| 34.6. WEB コンソールでのコンテナチェックポイントの復元   | 183        |
| 34.7. WEB コンソールでのコンテナの削除   | 184        |
| 34.8. WEB コンソールでの POD の作成  | 184        |
| 34.9. WEB コンソールの POD 内にコンテナを作成する   | 185        |
| 34.10. WEB コンソールでの POD の状態の変更  | 187        |
| 34.11. WEB コンソールでの POD の削除   | 187        |





## 多様性を受け入れるオープンソースの強化

Red Hat では、コード、ドキュメント、Web プロパティにおける配慮に欠ける用語の置き換えに取り組んでいます。まずは、マスター (master)、スレーブ (slave)、ブラックリスト (blacklist)、ホワイトリスト (whitelist) の 4 つの用語の置き換えから始めます。この取り組みは膨大な作業を要するため、今後の複数のリリースで段階的に用語の置き換えを実施して参ります。詳細は、[Red Hat CTO である Chris Wright のメッセージ](#) をご覧ください。

## RED HAT ドキュメントへのフィードバック (英語のみ)

Red Hat ドキュメントに関するご意見や感想をお寄せください。また、改善点があればお知らせください。

### Jira からのフィードバック送信 (アカウントが必要)

1. [Jira](#) の Web サイトにログインします。
2. 上部のナビゲーションバーで **Create** をクリックします。
3. **Summary** フィールドにわかりやすいタイトルを入力します。
4. **Description** フィールドに、ドキュメントの改善に関するご意見を記入してください。ドキュメントの該当部分へのリンクも追加してください。
5. ダイアログの下部にある **Create** をクリックします。

## 第1章 RHEL WEB コンソールの使用

Red Hat Enterprise Linux 8 Web コンソールのインストール方法、便利なグラフィカルインターフェイスから [リモートホストを追加および管理](#) する方法、Web コンソールによって管理されるシステムを監視する方法を説明します。

### 1.1. RHEL WEB コンソールの概要

RHEL Web コンソールは、ローカルシステム、およびネットワーク環境にある Linux サーバーを管理および監視するために設計された Web ベースのインターフェイスです。

RHEL Web コンソールでは、以下を含むさまざまな管理タスクの実行が可能です。

- サービスの管理
- ユーザーアカウントの管理
- システムサービスの管理および監視
- ネットワークインターフェイスおよびファイアウォールの設定
- システムログの確認
- 仮想マシンの管理
- 診断レポートの作成
- カーネルダンプ設定の設定
- SELinux の設定
- ソフトウェアの更新
- システムサブスクリプションの管理

RHEL Web コンソールは、ターミナルで使用するのと同じシステム API を使用します。ターミナルで実行した操作は、即座に RHEL Web コンソールに反映されます。

ネットワーク環境のシステムのログや、パフォーマンスをグラフで監視できます。さらに、Web コンソールで設定を直接変更したり、ターミナルから設定を変更できます。

### 1.2. WEB コンソールのインストールおよび有効化

RHEL Web コンソールにアクセスするには、最初に **cockpit.socket** サービスを有効にします。

Red Hat Enterprise Linux 9 では、多くのインストール方法で、Web コンソールがデフォルトでインストールされます。ご使用のシステムがこれに該当しない場合は、**cockpit** パッケージをインストールしてから **.socket** サービスを有効にしてください。

#### 手順

1. Web コンソールがインストールバリエーションにデフォルトでインストールされていない場合は、**cockpit** パッケージを手動でインストールします。

```
# yum install cockpit
```

- 必要に応じて、Web サーバーを実行する **cockpit.socket** サービスを有効にして起動します。

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

- Web コンソールがインストールバリエーションにデフォルトでインストールされておらず、カスタムのファイアウォールプロファイルを使用している場合は、**cockpit** サービスを **firewalld** に追加して、ファイアウォールの 9090 番ポートを開きます。

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

## 検証手順

- 以前のインストールと設定を確認するには、[Web コンソールを開きます](#)。

## 1.3. WEB コンソールへのログイン

**cockpit.socket** サービスが実行中で、対応するファイアウォールポートが開いている場合、ブラウザで Web コンソールに初めてログインできます。

### 前提条件

- 次のブラウザのいずれかを使用して Web コンソールを開いている。
  - Mozilla Firefox 52 以降
  - Google Chrome 57 以降
  - Microsoft Edge 16 以降
- システムユーザーアカウントの認証情報  
RHEL Web コンソールは、**/etc/pam.d/cockpit** にある特定のプラグ可能な認証モジュール (PAM) スタックを使用します。デフォルト設定では、システム上の任意のローカルアカウントのユーザー名とパスワードを使用してログインできます。
- ファイアウォールでポート 9090 が開いている。

### 手順

- Web ブラウザーに次のアドレスを入力して Web コンソールにアクセスします。

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



### 注記

これにより、ローカルマシン上で Web コンソールログインが可能になります。リモートシステムの Web コンソールにログインする場合、[「リモートマシンから Web コンソールへの接続」](#) を参照してください。

自己署名証明書を使用する場合は、ブラウザに警告が表示されます。証明書を確認し、セキュリティ例外を許可して、ログインを続行します。

コンソールは `/etc/cockpit/ws-certs.d` ディレクトリーから証明書をロードし、アルファベット順で最後となる `.cert` 拡張子のファイルを使用します。セキュリティーの例外を承認しなくてもすむように、認証局 (CA) が署名した証明書をインストールします。

2. ログイン画面で、システムユーザー名とパスワードを入力します。
3. **Log In** をクリックします。

認証に成功すると、RHEL Web コンソールインターフェイスが開きます。



### 注記

制限付きアクセスと管理アクセスを切り替えるには、Web コンソールページのトップパネルで **Administrative access** または **Limited access** をクリックします。管理者アクセスを取得するには、ユーザーパスワードを入力する必要があります。

## 1.4. WEB コンソールのデフォルトのスタイル設定の変更

デフォルトでは、Web コンソールはブラウザの設定からスタイル設定を採用します。RHEL 8 Web コンソールインターフェイスからデフォルトのスタイル設定をオーバーライドできます。

### 前提条件

- RHEL 8 Web コンソールをインストールし、アクセスできる。詳細は、[Web コンソールのインストール](#) を参照してください。

### 手順

1. RHEL Web コンソールにログインします。詳細は、[Web コンソールへのログイン](#) を参照してください。
2. 右上隅の **Session** ボタンをクリックします。
3. **Style** セクションで、希望の設定を選択します。**デフォルト** 設定は、ブラウザと同じスタイル設定を使用します。

### 検証手順

1. スタイル設定は、設定スタイルに従って変更されました。

## 1.5. WEB コンソールでの基本認証の無効化

`cockpit.conf` ファイルを変更することで、認証方式の動作を変更できます。**none** アクションを使用して認証方式を無効にし、GSSAPI とフォームによる認証のみを許可します。

### 前提条件

- RHEL 8 Web コンソールをインストールし、アクセスできる。詳細は、[Web コンソールのインストール](#) を参照してください。
- **sudo** を使用して管理コマンドを入力するための **root** 権限または権限がある。

### 手順

1. 任意のテキストエディターで、`/etc/cockpit/` ディレクトリーの `cockpit.conf` ファイルを開くか、作成します。次に例を示します。

```
# vi cockpit.conf
```

2. 次のテキストを追加します。

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

3. ファイルを保存します。
4. Web コンソールを再起動して、変更を有効にします。

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

## 1.6. リモートマシンから WEB コンソールへの接続

Web コンソールインターフェイスには、クライアントオペレーティングシステムだけでなく、携帯電話やタブレットからも接続できます。

### 前提条件

- 対応しているインターネットブラウザを備えたデバイス。以下に例を示します。
  - Mozilla Firefox 52 以降
  - Google Chrome 57 以降
  - Microsoft Edge 16 以降
- インストールしてアクセス可能な Web コンソールでアクセスする RHEL 8 サーバー。Web コンソールのインストールの詳細は、[RHEL Web コンソールの使用](#) を参照してください。

### 手順

1. Web ブラウザーを開きます。
2. リモートサーバーのアドレスを次のいずれかの形式で入力します。
  - a. サーバーのホスト名を使用する場合:

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

以下に例を示します。

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

- b. サーバーの IP アドレスを使用する場合:

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

以下に例を示します。

-

https://192.0.2.2:9090

3. ログインインターフェイスが開いたら、RHEL システムの認証情報を使用してログインします。

## 1.7. ワンタイムパスワードを使用した WEB コンソールへのログイン

ワンタイムパスワード (OTP) 設定が有効になっている Identity Management (IdM) ドメインにシステムが含まれている場合には、OTP を使用して RHEL Web コンソールにログインできます。



### 重要

ワンタイムパスワードを使用してログインできるのは、OTP 設定が有効な Identity Management (IdM) ドメインに、お使いのシステムが含まれる場合のみです。IdM の OTP の詳細は、[Identity Management のワンタイムパスワード](#) を参照してください。

### 前提条件

- RHEL Web コンソールがインストールされている。  
詳細は、[Web コンソールのインストールおよび有効化](#) を参照してください。
- Identity Management サーバーで OTP 設定を有効しておく。  
詳細は [Identity Management のワンタイムパスワード](#) を参照してください。
- OTP トークンを生成する設定済みのハードウェアまたはソフトウェアのデバイス

### 手順

1. ブラウザーで RHEL Web コンソールを開きます。
  - ローカルの場合 - **https://localhost:PORT\_NUMBER**
  - リモートでサーバーのホスト名を使用する場合 - **https://example.com:PORT\_NUMBER**
  - リモートでサーバーの IP アドレスを使用する場合 - **https://EXAMPLE.SERVER.IP.ADDR:PORT\_NUMBER**  
自己署名証明書を使用する場合は、ブラウザーに警告が表示されます。証明書を確認し、セキュリティー例外を許可してから、ログインを続行します。  
  
コンソールは `/etc/cockpit/ws-certs.d` ディレクトリーから証明書をロードし、アルファベット順で最後となる `.cert` 拡張子のファイルを使用します。セキュリティーの例外を承認しなくてもすむように、認証局 (CA) が署名した証明書をインストールします。
2. ログイン画面が表示されます。ログイン画面で、システムユーザーの名前とパスワードを入力します。
3. デバイスでワンタイムパスワードを生成します。
4. パスワードを確認してから、Web コンソールインターフェイスに表示される新規フィールドにワンタイムパスワードを入力します。
5. **Log in** をクリックします。
6. ログインに成功すると、Web コンソールインターフェイスの **Overview** ページに移動します。



## 1.8. WEB コンソールを使用したシステムの再起動

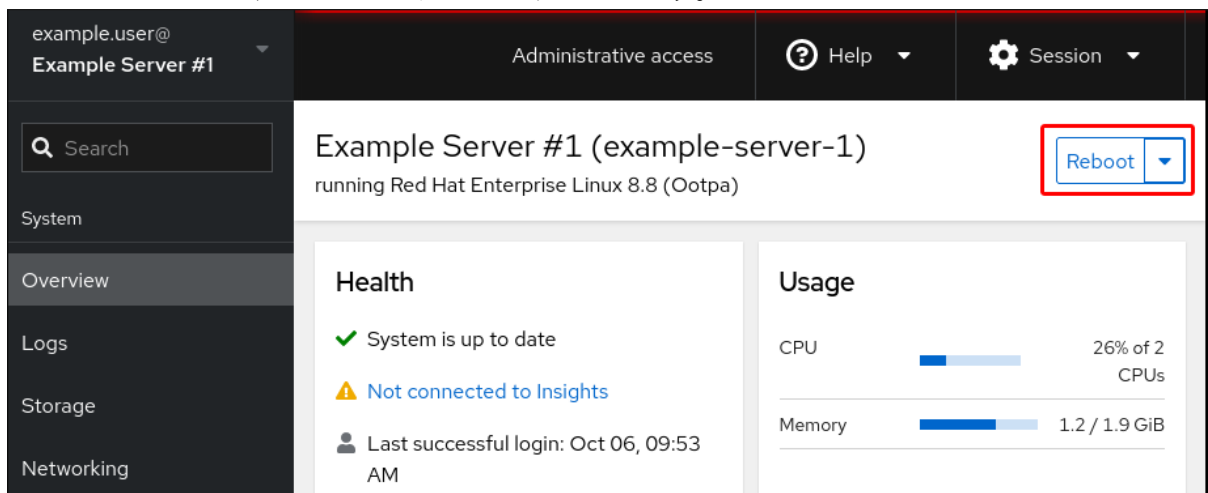
Web コンソールを使用して、Web コンソールの接続先の RHEL システムを再起動します。

### 前提条件

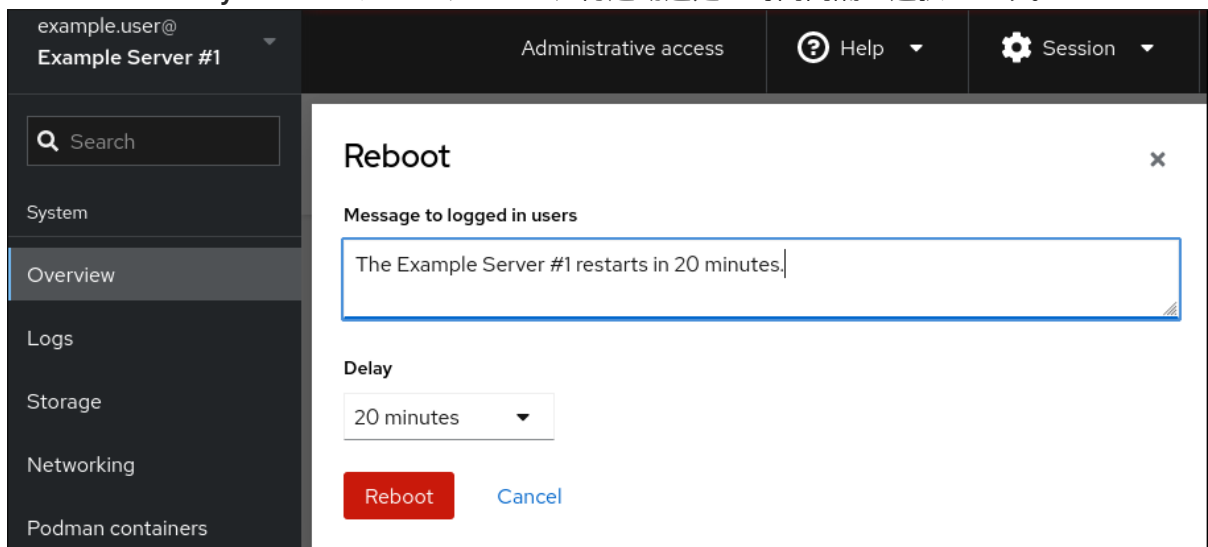
- RHEL 8 Web コンソールをインストールし、アクセスできる。詳細は、[Web コンソールのインストール](#) を参照してください。

### 手順

1. RHEL Web コンソールにログインします。詳細は、[Web コンソールへのログイン](#) を参照してください。
2. **Overview** ページで、**Reboot** ボタンをクリックします。



3. ユーザーがシステムにログインしている場合は、**Reboot** ダイアログボックスに再起動に関するメッセージを書き込むことができます。
4. オプション: **Delay** ドロップダウンリストで、再起動遅延の時間間隔を選択します。



5. **Reboot** をクリックします。

## 1.9. WEB コンソールでのシステムのシャットダウン

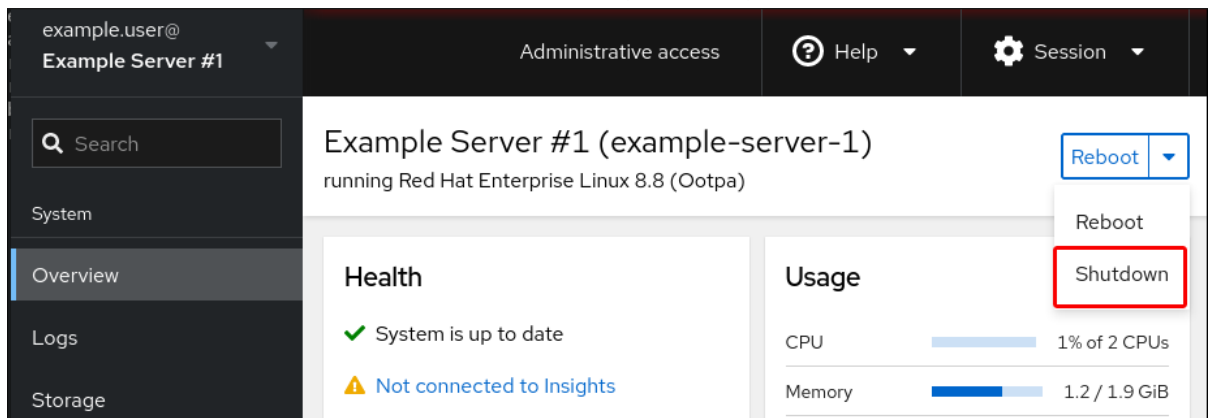
Web コンソールを使用して、Web コンソールが接続している RHEL システムをシャットダウンします。

### 前提条件

- RHEL 8 Web コンソールをインストールし、アクセスできる。  
詳細は、[Web コンソールのインストール](#) を参照してください。

### 手順

1. RHEL Web コンソールにログインします。  
詳細は、[Web コンソールへのログイン](#) を参照してください。
2. **Overview** をクリックします。
3. **Restart** ドロップダウンリストで、**Shut Down** を選択します。



4. システムにログインするユーザーがいる場合は、**シャットダウン** ダイアログボックスに、シャットダウンの理由を入力します。
5. 必要に応じて、**遅延** ドロップダウンリストで、遅延させる時間を選択します。
6. **Shut Down** をクリックします。

## 1.10. WEB コンソールでの時間設定の設定

タイムゾーンを設定して、システム時間を Network Time Protocol (NTP) サーバーと同期できます。

### 前提条件

- RHEL 8 Web コンソールをインストールし、アクセスできる。  
詳細は、[Web コンソールのインストール](#) を参照してください。

### 手順

1. RHEL Web コンソールにログインします。  
詳細は、[Web コンソールへのログイン](#) を参照してください。
2. **概要** で現在のシステム時間をクリックします。

The screenshot shows the RHEL Web Console interface. On the left is a navigation menu with options like System, Overview, Logs, Storage, Networking, Podman containers, Accounts, and Services. The main content area is divided into several sections:

- Administrative access:** Shows 'Not connected to Insights', 'Last successful login: Oct 09, 03:36 PM on tty2', and a link to 'View login history'.
- System information:** A table with the following data:
 

|            |                                     |
|------------|-------------------------------------|
| Model      | QEMU Standard PC (Q35 + ICH9, 2009) |
| Machine ID | 00619f0bf479499a9a2b4bbe342704e5    |
| Uptime     | 11 minutes                          |
- Configuration:** A table with the following data:
 

|                     |   |
|---------------------|---|
| Hostname            | Example Server #1 (example-server-1) <a href="#">edit</a> |
| System time         | Oct 9, 2023, 3:48 PM ⓘ                                    |
| Domain              | <a href="#">Join domain</a>                               |
| Performance profile | virtual-guest   |

3. **System time** をクリックします。
4. 必要に応じて、**システム時間の変更** ダイアログボックスで、タイムゾーンを変更します。
5. **Set Time** ドロップダウンメニューで、以下のいずれかを選択します。

#### 手動

NTP サーバーなしで手動で時間を設定する必要がある場合は、このオプションを使用します。

#### NTP サーバーの自動使用

これはデフォルトのオプションで、既存の NTP サーバーと時間を自動同期します。

#### 特定の NTP サーバーの自動使用

このオプションは、システムを特定の NTP サーバーと同期する必要がある場合に限り使用してください。サーバーの DNS 名または IP アドレスを指定します。

6. **Change** をクリックします。

The screenshot shows the 'Change system time' dialog box. It has a title bar and two main sections:

- Time zone:** A dropdown menu currently set to 'Europe/Prague'.
- Set time:** A dropdown menu with four options:
  - Automatically using NTP (highlighted with a blue line)
  - Manually
  - Automatically using NTP (with a blue checkmark)
  - Automatically using specific NTP servers

## 検証手順

- システム タブに表示されるシステム時間を確認します。

## 関連情報

- [Chrony スイートを使用した NTP の設定](#)

## 1.11. WEB コンソールを使用した RHEL 8 システムの IDM ドメインへの参加

Web コンソールを使用して、Red Hat Enterprise Linux 8 システムを Identity Management (IdM) ドメインに参加させることができます。

### 前提条件

- IdM ドメインが実行中で参加するクライアントから到達可能
- IdM ドメインの管理者認証情報がある。

### 手順

1. RHEL Web コンソールにログインします。  
詳細は、[Web コンソールへのログイン](#) を参照してください。
2. **Overview** タブの **Configuration** フィールドで、**Join Domain** をクリックします。
3. **ドメイン参加** ダイアログボックスの **ドメインアドレス** フィールドに、IdM サーバーのホスト名を入力します。
4. **ドメイン管理者名** フィールドで、IdM 管理アカウントのユーザー名を入力します。
5. **Domain administrator password** にパスワードを追加します。
6. **参加** をクリックします。

### 検証手順

1. システムが IdM ドメインに参加していると、RHEL 8 Web コンソールにエラーが表示されず、**システム** 画面でドメイン名を確認できます。
2. ユーザーがドメインのメンバーであることを確認するには、**Terminal** ページをクリックし、**id** コマンドを実行します。

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

### 関連情報

- [Identity Management の計画](#)
- [Identity Management のインストール](#)
- [IdM ユーザー、グループ、ホスト、およびアクセス制御ルールの管理](#)

## 1.12. WEB コンソールを使用して CPU のセキュリティーの問題を防ぐために SMT を無効化する手順

CPU SMT (Simultaneous Multi Threading) を悪用する攻撃が発生した場合に SMT を無効にします。SMT を無効にすると、L1TF や MDS などのセキュリティー脆弱性を軽減できます。



### 重要

SMT を無効にすると、システムパフォーマンスが低下する可能性があります。

### 前提条件

- Web コンソールがインストールされており、アクセス可能である。詳細は、[Web コンソールのインストール](#) を参照してください。

### 手順

1. RHEL Web コンソールにログインします。詳細は、[Web コンソールへのログイン](#) を参照してください。
2. **Overview** タブで、**System information** フィールドを見つけて、**View hardware details** をクリックします。
3. **CPU Security** 行で、**Mitigations** をクリックします。  
このリンクがない場合は、システムが SMT に対応していないため、攻撃を受けません。
4. **CPU Security Toggles** テーブルで、**Disable simultaneous multithreading (nosmt)** オプションに切り替えます。
5. **Save and reboot** ボタンをクリックします。

システムの再起動後、CPU は SMT を使用しなくなりました。

### 関連情報

- [L1 Terminal Fault \(L1TF\) を使用したカーネルのサイドチャネル攻撃: CVE-2018-3620 & CVE-2018-3646](#)
- [MDS - マイクロアーキテクチャーデータサンプリング - CVE-2018-12130、CVE-2018-12126、CVE-2018-12127、および CVE-2019-11091](#)

## 1.13. ログインページへのバナーの追加

ログイン画面にバナーファイルの内容を表示するように Web コンソールを設定できます。

### 前提条件

- RHEL 8 Web コンソールをインストールし、アクセスできる。  
詳細は、[Web コンソールのインストール](#) を参照してください。
- **sudo** を使用して管理コマンドを入力するための **root** 権限または権限がある。

### 手順

1. 任意のテキストエディターで **/etc/issue.cockpit** ファイルを開きます。

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

2. バナーとして表示するコンテンツをファイルに追加します。次に例を示します。

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

ファイルにマクロを含めることはできませんが、改行と ASCII アートは使用できます。

3. ファイルを保存します。
4. 任意のテキストエディターで、**/etc/cockpit/**ディレクトリーの **cockpit.conf** ファイルを開きます。次に例を示します。

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

5. 以下のテキストをファイルに追加します。

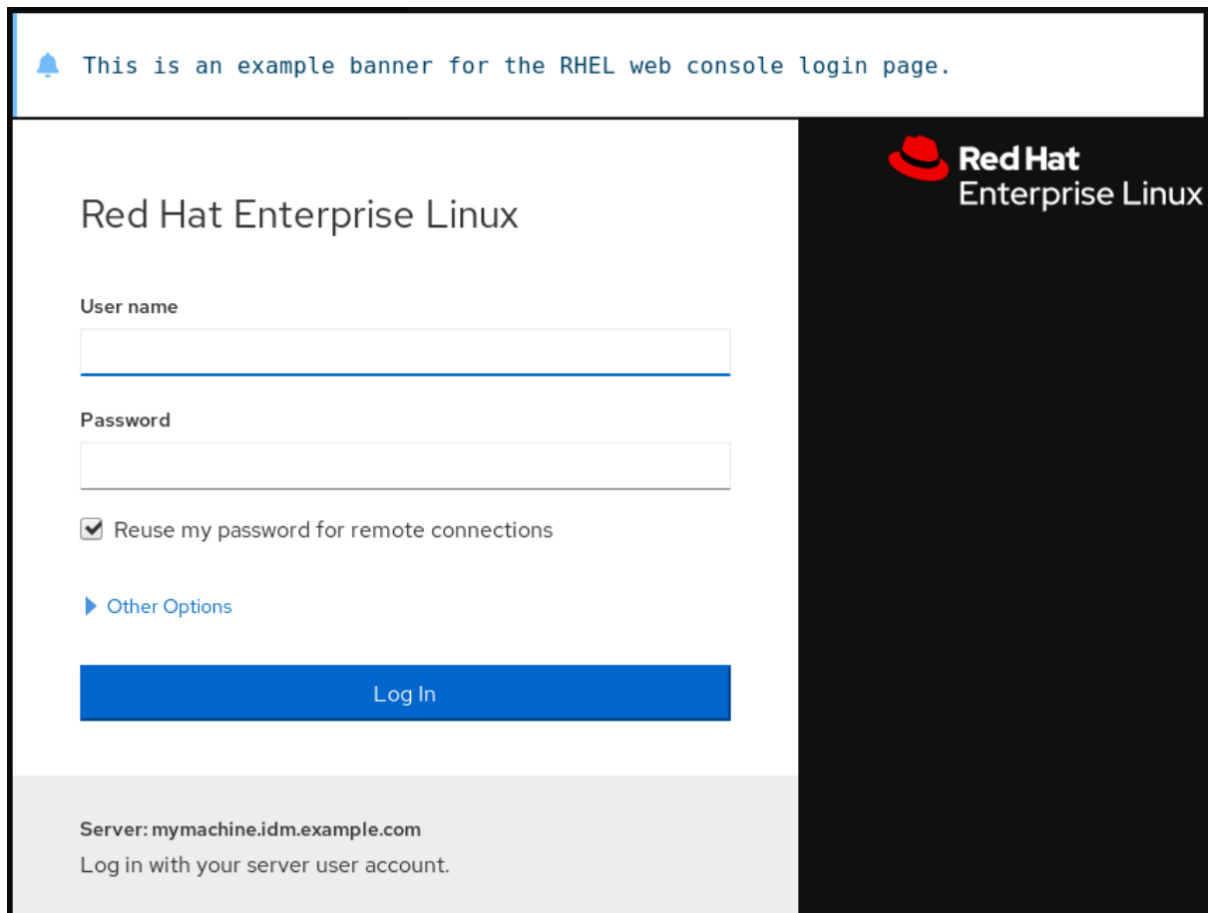
```
[Session]
Banner=/etc/issue.cockpit
```

6. ファイルを保存します。
7. Web コンソールを再起動して、変更を有効にします。

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

## 検証手順

- Web コンソールのログイン画面を再度開き、バナーが表示されていることを確認します。



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

## Red Hat Enterprise Linux

User name

Password

Reuse my password for remote connections

▶ Other Options

Log In

Server: mymachine.idm.example.com  
Log in with your server user account.

## 1.14. WEB コンソールでの自動アイドルロックの設定

Web コンソールインターフェイスを使用して、自動アイドルロックを有効にし、システムのアイドルタイムアウトを設定できます。

### 前提条件

- Web コンソールがインストールされており、アクセス可能である。  
詳細は、[Web コンソールのインストール](#) を参照してください。
- **sudo** を使用して管理コマンドを入力するための **root** 権限または権限がある。

### 手順

1. 任意のテキストエディターで、`/etc/cockpit/` ディレクトリーの `cockpit.conf` ファイルを開きます。次に例を示します。

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

2. 以下のテキストをファイルに追加します。

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

<X> は、任意の期間の数値 (分単位) に置き換えます。

3. ファイルを保存します。

4. Web コンソールを再起動して、変更を有効にします。

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

#### 検証手順

- 設定の期間後にセッションがログアウトされているかどうかを確認します。



## 第2章 WEB コンソールでのホスト名の設定

以下では、Red Hat Enterprise Linux Web コンソールを使用して、Web コンソールの接続先のシステムで、異なる形式のホスト名を設定する方法を説明します。

### 2.1. ホスト名

ホスト名はシステムを識別します。デフォルトでは、ホスト名は **localhost** に設定されていますが、変更できます。

ホスト名は、以下の2つの部分から設定されます。

#### ホスト名

システムを識別する一意の名前です。

#### ドメイン

ネットワーク内でシステムを使用する場合や、IP アドレスではなく名前を使用する場合に、ホスト名の後にドメインを接尾辞として追加します。

ドメイン名が割り当てられたホスト名は、完全修飾ドメイン名 (FQDN) と呼ばれます。たとえば、**mymachine.example.com** です。

ホスト名は **/etc/hostname** ファイルに保存されます。

### 2.2. WEB コンソールでの PRETTY ホスト名

RHEL Web コンソールで Pretty ホスト名を設定することもできます。Pretty ホスト名は、大文字、スペースなどを含むホスト名です。

Pretty ホスト名は Web コンソールに表示されますが、ホスト名に対応させる必要はありません。

#### 例2.1 Web コンソールでのホスト名の形式

Pretty ホスト名

**My machine**

ホスト名

**mymachine**

実際のホスト名 - 完全修飾ドメイン名 (FQDN)

**mymachine.idm.company.com**

### 2.3. WEB コンソールを使用したホスト名の設定

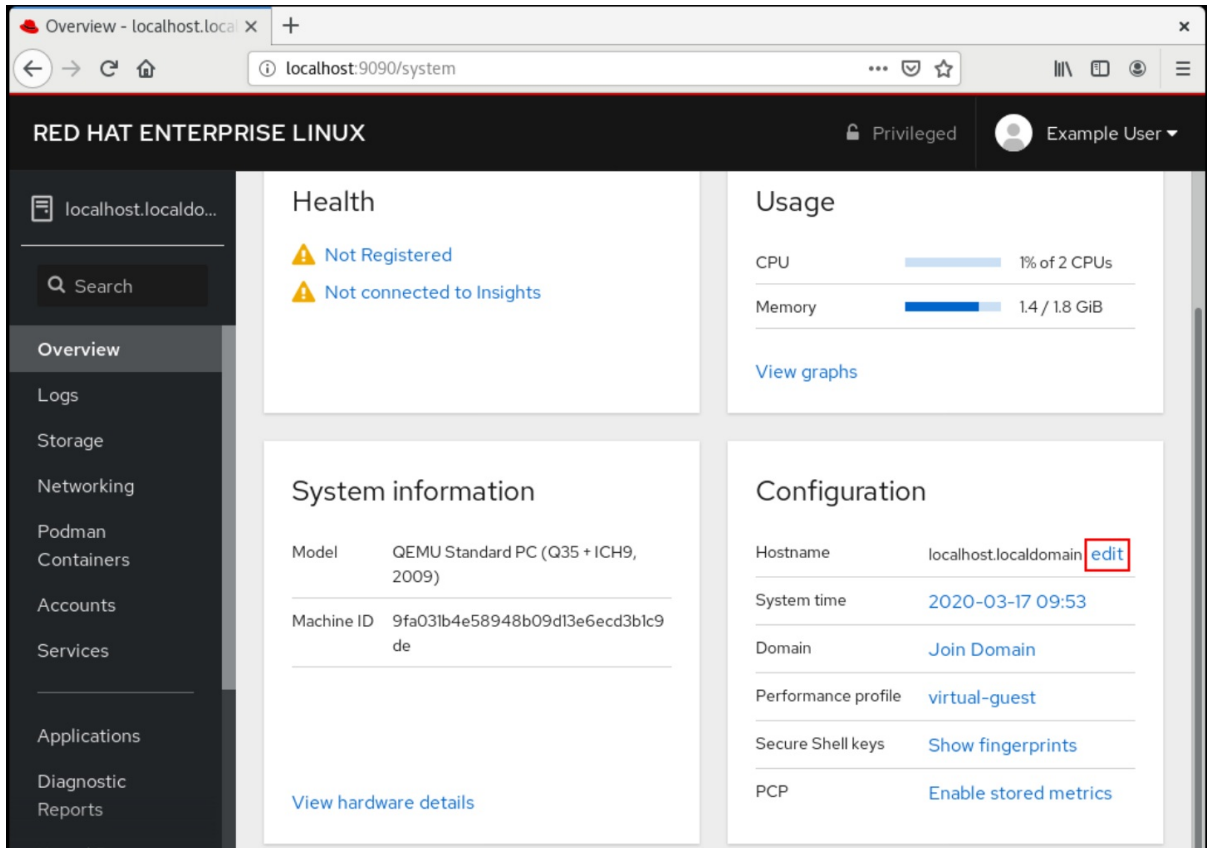
この手順では、Web コンソールで実際のホスト名または Pretty ホスト名を設定します。

#### 前提条件

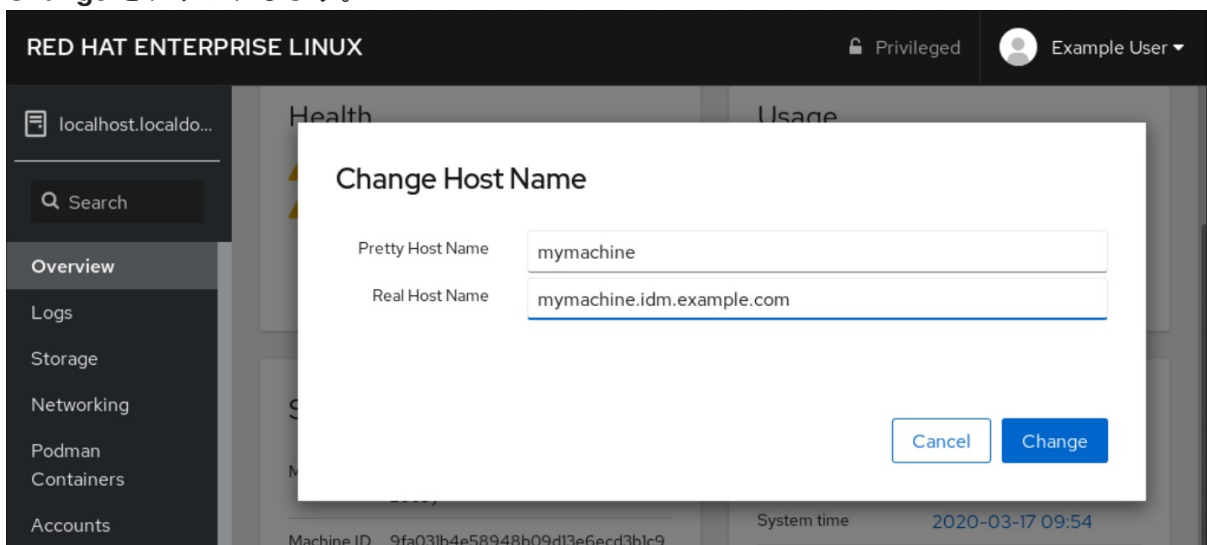
- RHEL 8 Web コンソールをインストールし、アクセスできる。  
詳細は、[Web コンソールのインストール](#) を参照してください。

#### 手順

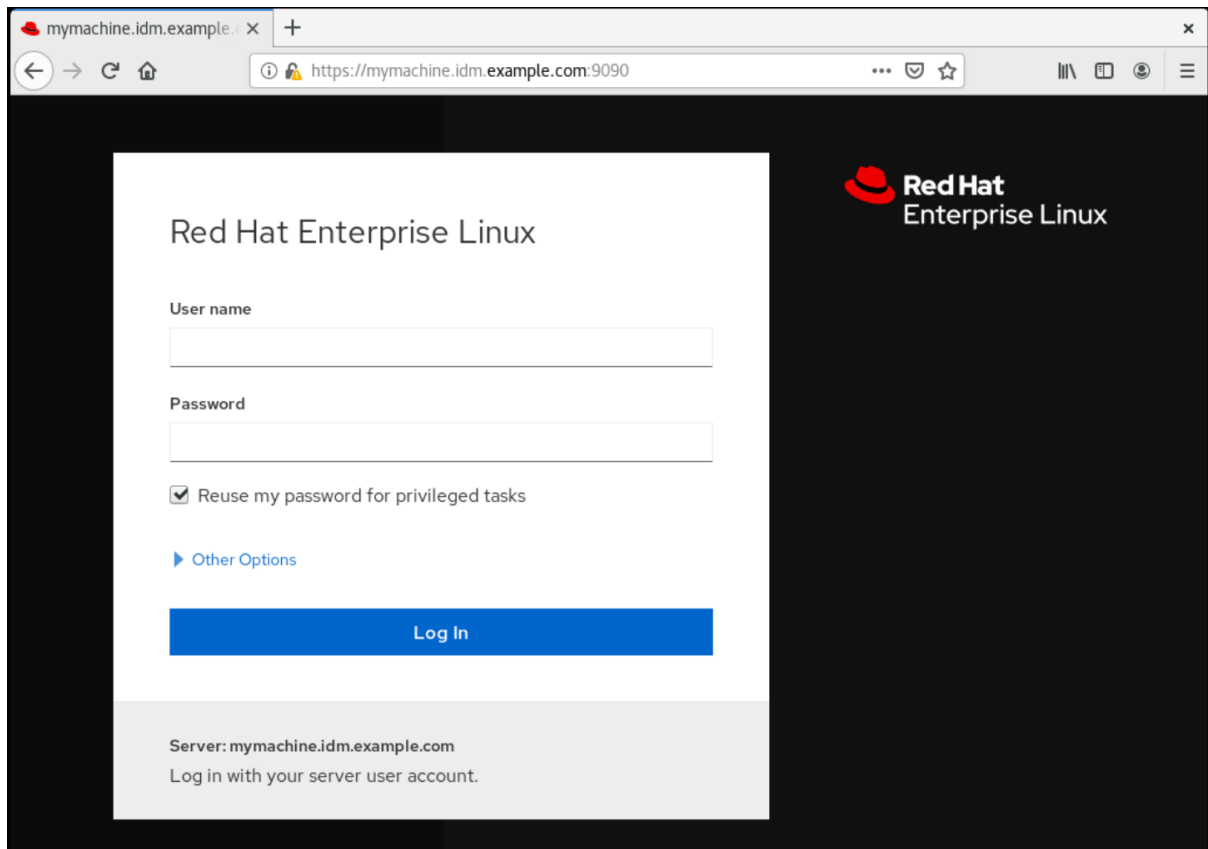
1. Web コンソールへのログイン  
詳細は、[Web コンソールへのログイン](#) を参照してください。
2. **Overview** をクリックします。
3. 現在のホスト名の横にある **edit** をクリックします。



4. **ホスト名の変更** ダイアログボックスの **Pretty ホスト名** フィールドに、ホスト名を入力します。
5. **実際のホスト名フィールド** は、ドメイン名を Pretty 名に割り当てます。  
ホスト名が Pretty ホスト名と一致しない場合は、実際にホスト名を手動で変更できます。
6. **Change** をクリックします。



1. Web コンソールからログアウトします。
2. ブラウザーのアドレスバーに新規ホスト名のアドレスを入力して、Web コンソールを再度開きます。



## 第3章 WEB コンソールアドオンのインストールとカスタムページの作成

Red Hat Enterprise Linux システムの使用方法に応じて、**使用可能** なアプリケーションを Web コンソールに追加したり、ユースケースに基づいてカスタムページを作成したりできます。

### 3.1. RHEL WEB コンソールのアドオン

**cockpit** パッケージはデフォルトで Red Hat Enterprise Linux の一部ですが、次のコマンドを使用してオンデマンドでアドオンアプリケーションをインストールできます。

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

上記コマンドの <add-on> は、RHEL Web コンソールで使用可能なアドオンアプリケーションのリストのパッケージ名に置き換えます。

| 機能名        | パッケージ名                           | 用途  |
|------------|----------------------------------|---|
| Composer   | <b>cockpit-composer</b>          | カスタム OS イメージの構築   |
| マシン        | <b>cockpit-machines</b>          | <b>libvirt</b> 仮想マシンの管理   |
| PackageKit | <b>cockpit-packagekit</b>        | ソフトウェア更新およびアプリケーションインストール (通常はデフォルトでインストールされている)                        |
| PCP        | <b>cockpit-pcp</b>               | 永続的かつ、より詳細なパフォーマンスデータ (UI からオンデマンドでインストール)                              |
| Podman     | <b>cockpit-podman</b>            | <a href="#">コンテナの管理</a> と <a href="#">コンテナイメージの管理</a> (RHEL 8.1 から利用可能) |
| セッションの録画   | <b>cockpit-session-recording</b> | ユーザーセッションの記録および管理   |
| Storage    | <b>cockpit-storaged</b>          | <b>udisk</b> によるストレージの管理  |

### 3.2. WEB コンソールでの新しいページの作成

カスタマイズした関数を Red Hat Enterprise Linux Web コンソールに追加する場合は、必要な関数を実行するページの HTML および JavaScript ファイルを含むパッケージディレクトリを追加する必要があります。

カスタムページの追加の詳細は、[Cockpit Project Web サイトの Creating Plugins for the Cockpit User Interface](#) を参照してください。

## 関連情報

- [Cockpit Project Developer Guide](#) の [Cockpit Packages](#) セクション

## 第4章 WEB コンソールを使用したシステムパフォーマンスの最適化

以下では、RHEL Web コンソールでパフォーマンスプロファイルを設定し、選択したタスクに対してシステムのパフォーマンスを最適化する方法を説明します。

### 4.1. WEB コンソールでのパフォーマンスチューニングオプション

Red Hat Enterprise Linux 8 には、以下のタスクに対してシステムを最適化する複数のパフォーマンスプロファイルが同梱されています。

- デスクトップを使用するシステム
- スループットパフォーマンス
- レイテンシーパフォーマンス
- ネットワークパフォーマンス
- 電力の低消費
- 仮想マシン

**TuneD** サービスは、選択したプロファイルに一致するようにシステムオプションを最適化します。

Web コンソールでは、システムが使用するパフォーマンスプロファイルを設定できます。

#### 関連情報

- [TuneD を使い始める](#)

### 4.2. WEB コンソールでのパフォーマンスプロファイルの設定

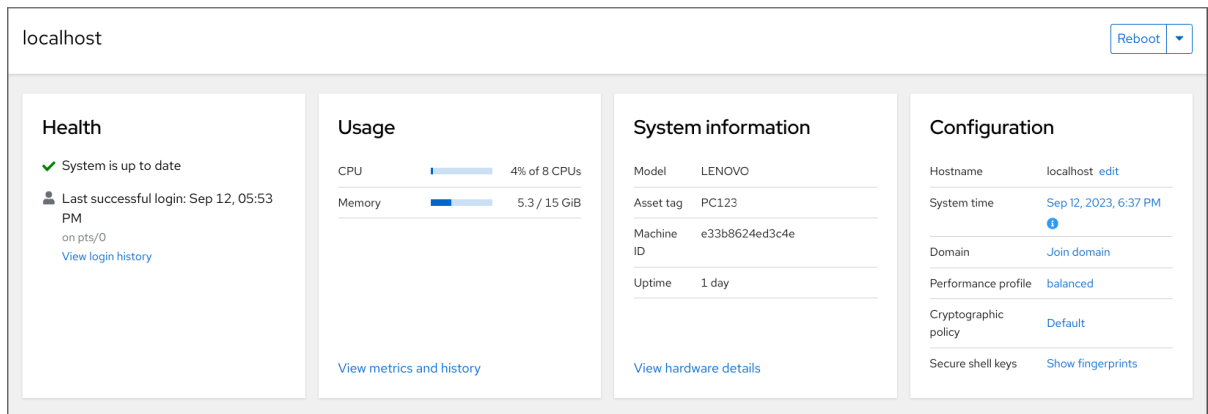
実行するタスクに応じて、Web コンソールを使用して適切なパフォーマンスプロファイルを設定することでシステムパフォーマンスを最適化できます。

#### 前提条件

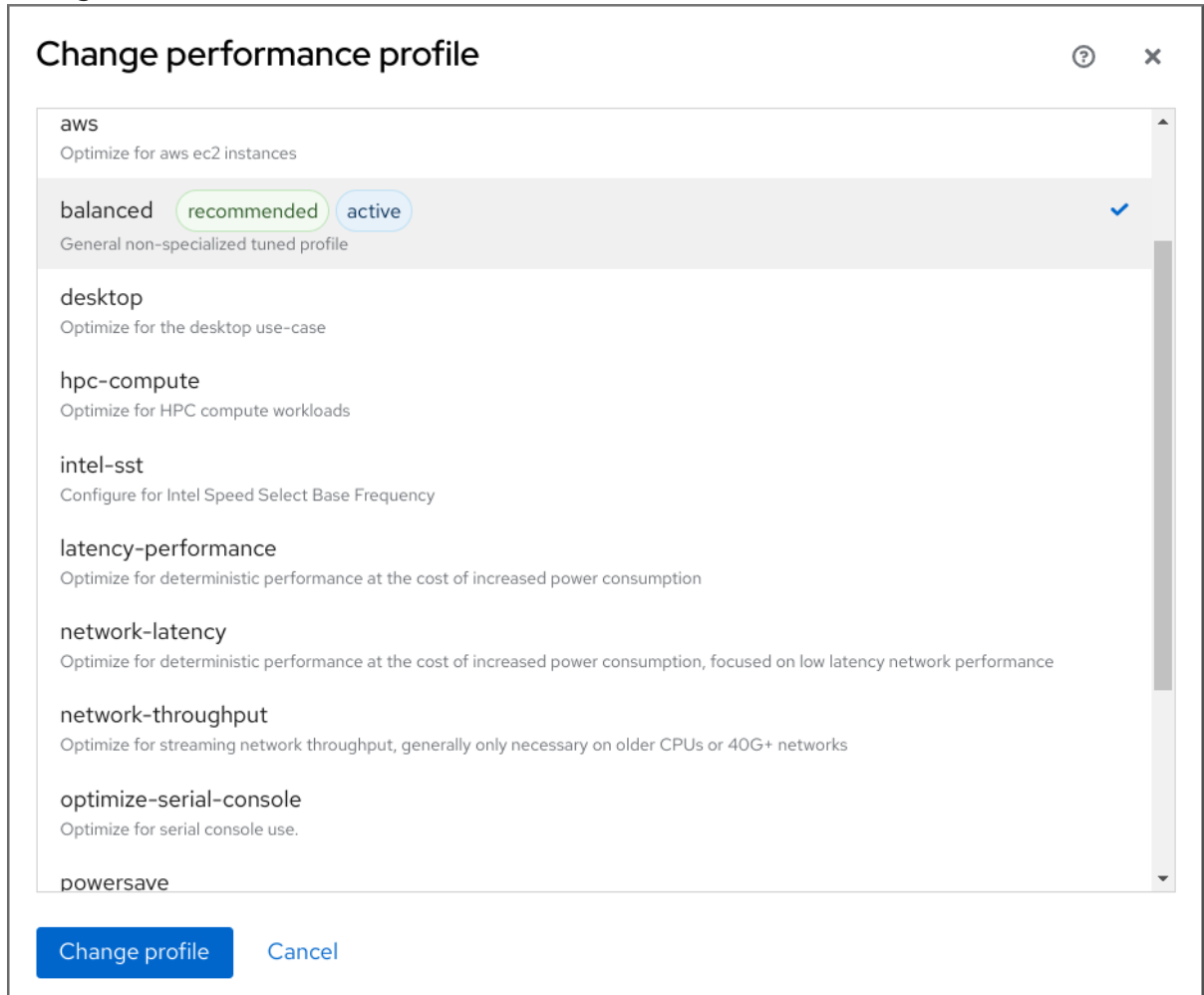
- Web コンソールをインストールし、アクセスできることを確認します。詳細は、[Web コンソールのインストール](#) を参照してください。

#### 手順

1. 8 の Web コンソールにログインします。詳細は、[Web コンソールへのログイン](#) を参照してください。
2. **Overview** をクリックします。
3. **Configuration** セクションで、現在のパフォーマンスプロファイルをクリックします。



4. **Change Performance Profile** ダイアログボックスで、必要なプロファイルを設定します。



5. **Change Profile** をクリックします。

#### 検証手順

- **Overview** タブの **Configuration** セクションに、選択したパフォーマンスプロファイルが表示されます。

### 4.3. WEB コンソールを使用したローカルシステムのパフォーマンスの監視

Red Hat Enterprise Linux の Web コンソールは、トラブルシューティングに Utilization Saturation and Errors (USE) メソッドを使用します。新しいパフォーマンスメトリックページには、データの履歴ビューが時系列に整理されており、最新のデータが上部に表示されます。

**Metrics and history** ページでは、イベント、エラー、リソースの使用率と飽和状態のグラフィカル表示を表示できます。

## 前提条件

- RHEL 8 Web コンソールをインストールし、アクセスできる。詳細は、[Web コンソールのインストール](#) を参照してください。
- パフォーマンスメトリクス収集を可能にする **cockpit-pcp** パッケージがインストールされている。
  - a. Web コンソールインターフェイスからパッケージをインストールするには、以下を行います。
    - i. Web コンソールに管理者権限でログインする。詳細は、[Web コンソールへのログイン](#) を参照してください。
    - ii. **Overview** ページで、**View metrics and history** をクリックします。
    - iii. **cockpit-pcp** の **インストール** ボタンをクリックします。
    - iv. **ソフトウェアのインストール** ダイアログウィンドウで、**Install** をクリックします。
  - b. コマンドラインインターフェイスからパッケージをインストールするには、次を使用します。

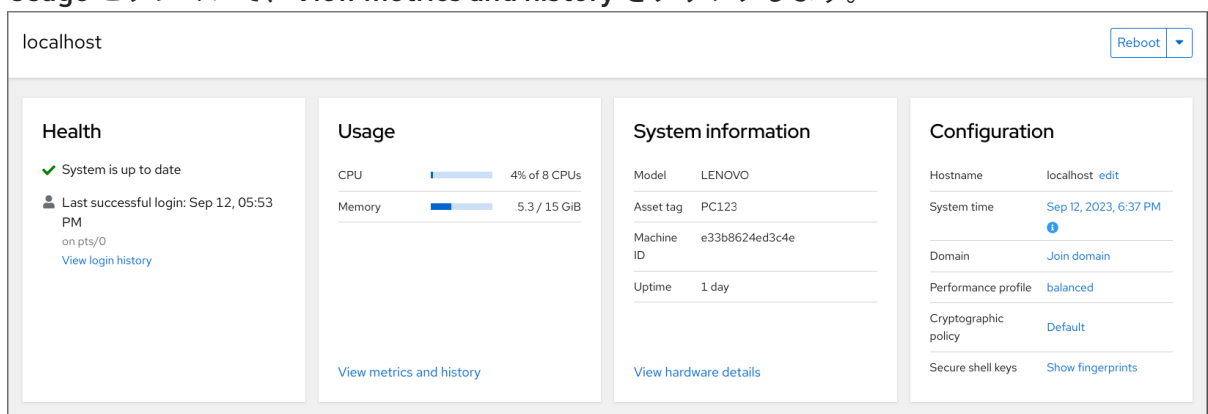
```
# yum install cockpit-pcp
```

- Performance Co-Pilot (PCP) サービスが有効になっている。

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

## 手順

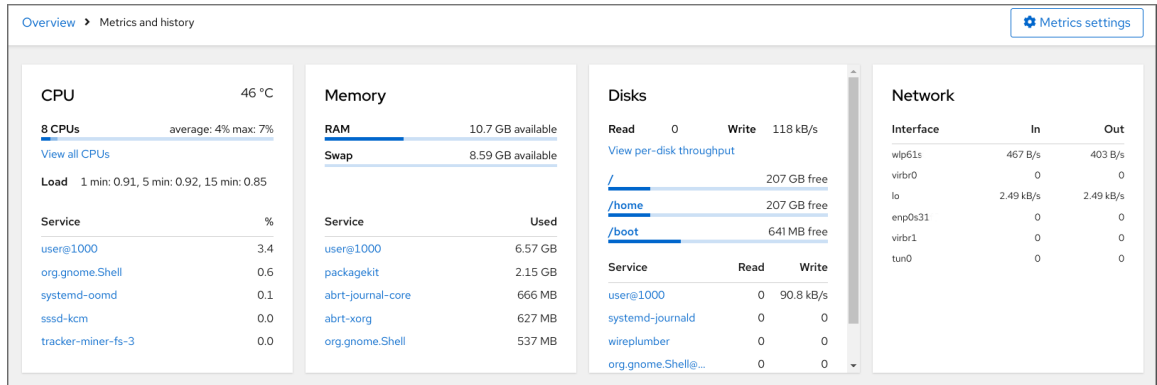
1. 8 の Web コンソールにログインします。詳細は、[Web コンソールへのログイン](#) を参照してください。
2. **Overview** をクリックします。
3. **Usage** セクションで、**View metrics and history** をクリックします。



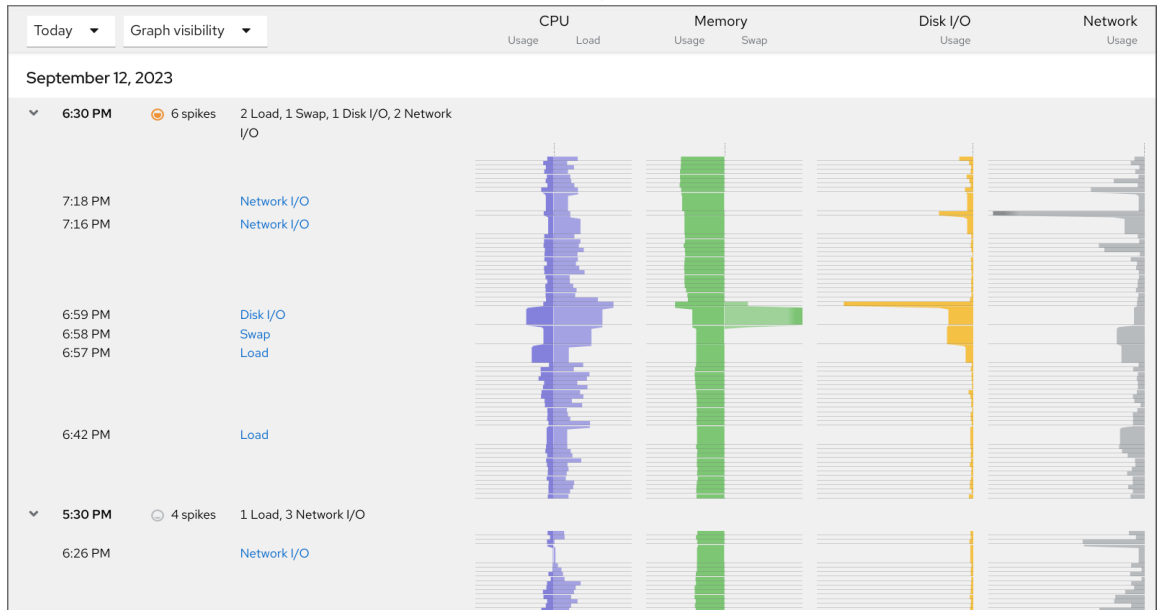
**Metrics and history** セクションが開きます。



- 現在のシステム設定と使用状況:



- ユーザー指定の時間間隔におけるグラフィック形式のパフォーマンスメトリクス:



## 4.4. WEB コンソールと GRAFANA を使用して複数のシステムのパフォーマンスを監視する

Grafana を使用すると、一度に複数のシステムからデータを収集し、収集した Performance Co-Pilot (PCP) メトリックのグラフィカル表現を確認できます。Web コンソールインターフェイスで、複数のシステムのパフォーマンスメトリックの監視およびエクスポートを設定できます。

### 前提条件

- Web コンソールがインストールされており、アクセス可能である。詳細は、[Web コンソールのインストールおよび有効化](#) を参照してください。
- **cockpit-pcp** パッケージをインストールします。
  1. Web コンソールインターフェイスから:
    - a. Web コンソールに管理者権限でログインする。詳細は、[Web コンソールへのログイン](#) を参照してください。
    - b. **概要** ページで、**詳細と履歴を表示** をクリックします。
    - c. **cockpit-pcp** のインストール ボタンをクリックします。
    - d. **ソフトウェアのインストール** ダイアログウィンドウで、**Install** をクリックします。

- e. ログアウトしてから再度ログインして、メトリクスの履歴を表示します。
2. コマンドラインインターフェイスからパッケージをインストールするには、次を使用します。

```
# yum install cockpit-pcp
```

- PCP サービスを有効にします。

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

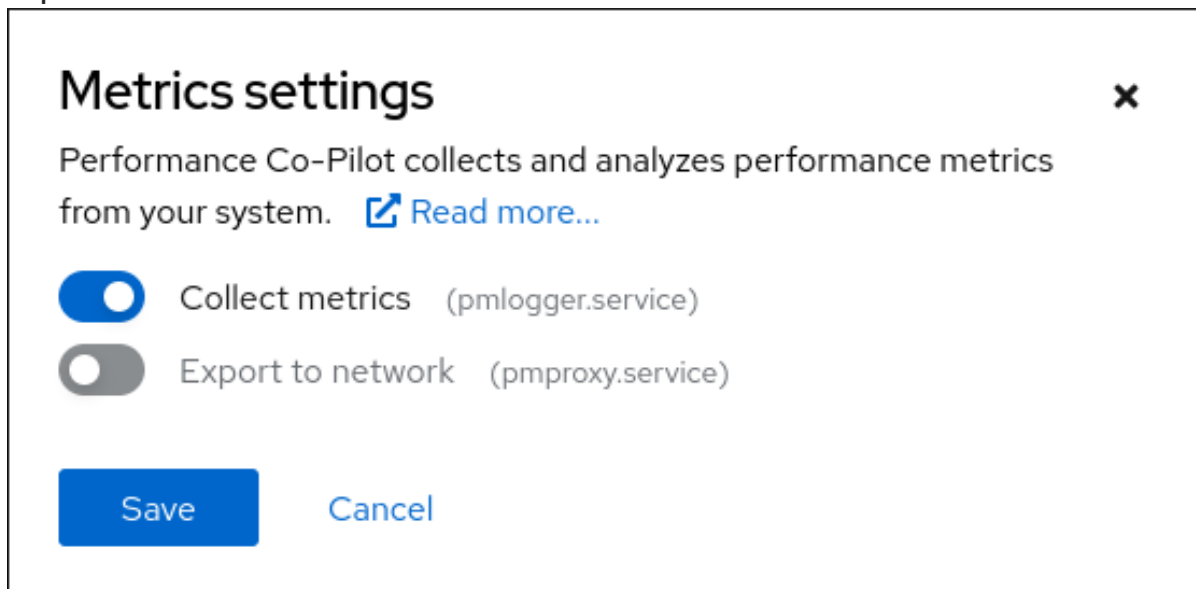
- Grafana ダッシュボードをセットアップします。詳細は、[grafana-server の設定](#) を参照してください。
- **redis** パッケージをインストールします。

```
# yum install redis
```

または、手順の後半で Web コンソールインターフェイスからパッケージをインストールすることもできます。

## 手順

1. **Overview** ページで、**Usage** テーブルの **View metrics and history** をクリックします。
2. **Metrics settings** ボタンをクリックします。
3. **Export to network** スライダーをアクティブな位置に移動します。

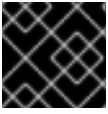


**redis** パッケージがインストールされていない場合は、Web コンソールでインストールするように求められます。

4. **pmproxy** サービスを開くには、ドロップダウンリストからゾーンを選択し、**Add pmproxy** ボタンをクリックします。
5. **Save** をクリックします。

## 検証

1. **Networking** をクリックします。
2. **Firewall** テーブルで、**Edit rules and zones** ボタンをクリックします。
3. 選択したゾーンで **pmproxy** を検索します。



### 重要

監視するすべてのシステムでこの手順を繰り返します。

### 関連情報

- [PCP メトリックのグラフィカル表示の設定](#)

## 第5章 WEB コンソールでログの確認

RHEL 8 Web コンソールでログへのアクセス、確認、およびフィルタリングの方法を説明します。

### 5.1. WEB コンソールでログの確認

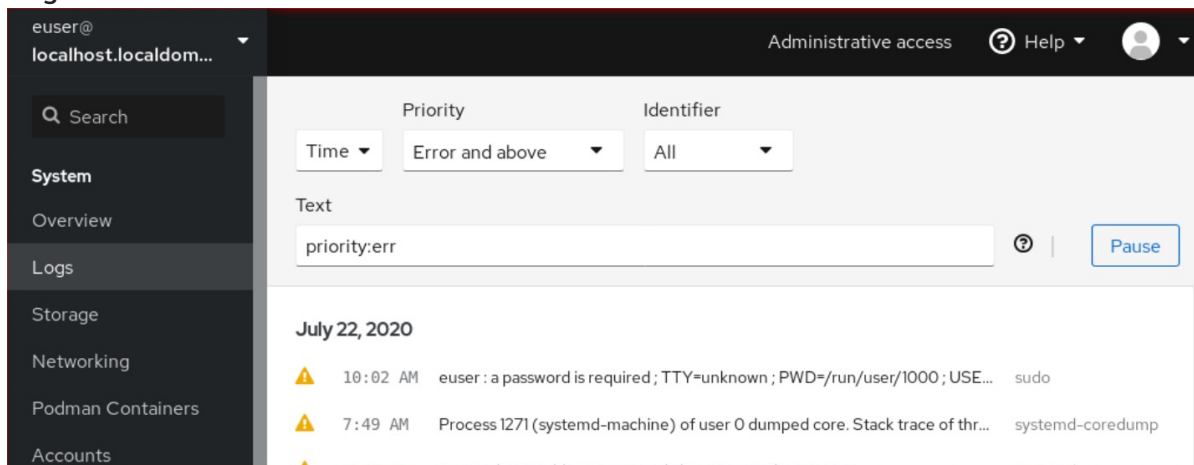
RHEL 8 Web コンソールのログセクションは、**journalctl** ユーティリティーの UI です。Web コンソールインターフェイスで、システムログにアクセスできます。

#### 前提条件

- RHEL 8 Web コンソールがインストールされている。  
詳細は、[Web コンソールのインストールおよび有効化](#) を参照してください。

#### 手順

1. RHEL Web コンソールにログインします。  
詳細は、[Web コンソールへのログイン](#) を参照してください。
2. **Logs** をクリックします。



3. リストからログを確認するログエントリーをクリックして、ログエントリーの詳細を開きます。



#### 注記

**Pause** ボタンを使用すると、新しいログエントリーが表示されないように一時停止できます。新しいログエントリーを再開すると、Web コンソールは、**Pause** ボタンを使用した後に報告されたすべてのログエントリーを読み込みます。

Priority 時間、優先順位、または識別子でログをフィルタリングできます。詳細は、[Web コンソールでのログのフィルタリング](#) を参照してください。

### 5.2. WEB コンソールでのログのフィルタリング

Web コンソールでログエントリーをフィルタリングできます。

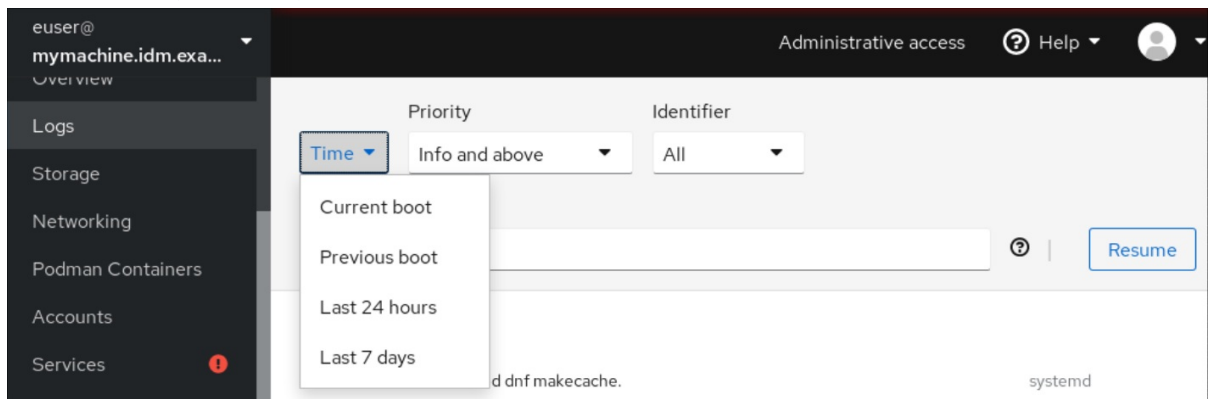
#### 前提条件

- Web コンソールインターフェイスがインストールされており、アクセス可能である。

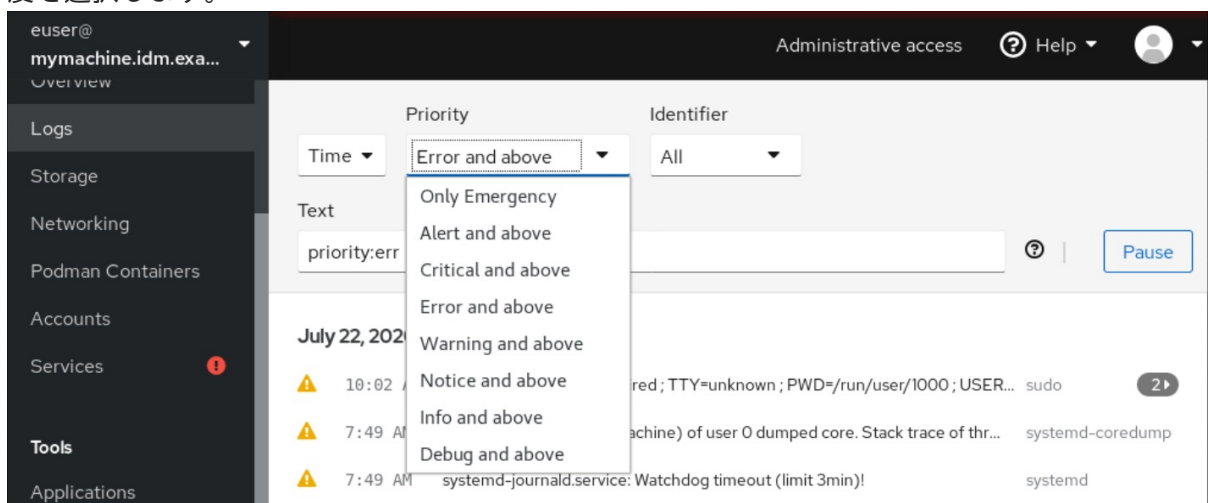
詳細は、[Web コンソールのインストール](#) を参照してください。

## 手順

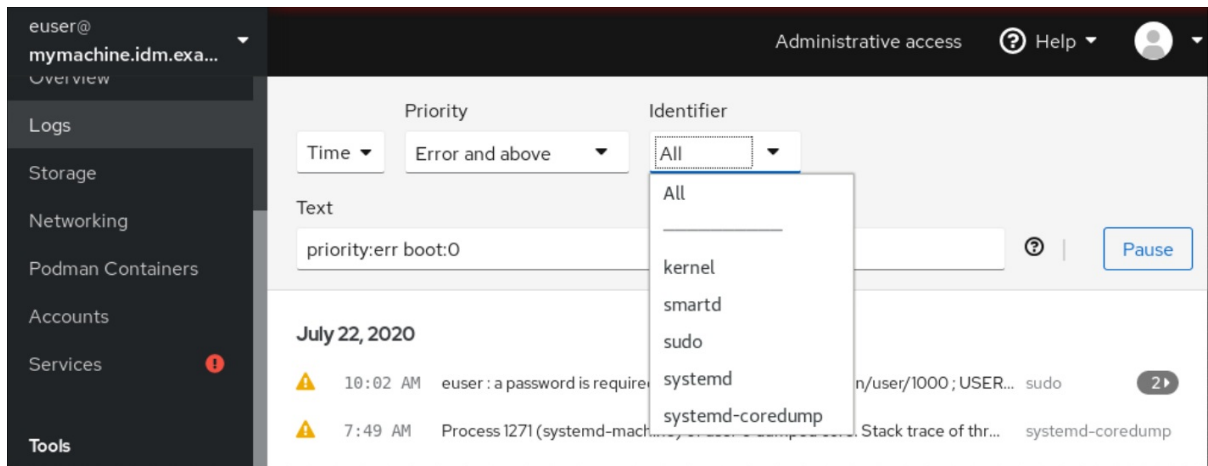
1. RHEL 8 Web コンソールにログインします。  
詳細は、[Web コンソールへのログイン](#) を参照してください。
2. **Logs** をクリックします。
3. コンソールデフォルトでは、Web コンソールには最新のログエントリが表示されます。別の時間範囲でフィルタリングするには、**Time** ドロップダウンメニューをクリックして、希望するオプションを選択します。



4. 重大度ログのリストは、デフォルトで **エラー以上のレベル** が表示されます。優先度のフィルタリングを変更するには、ドロップダウンメニューの **エラー以上のレベル** をクリックして、優先度を選択します。



5. デフォルトでは、Web コンソールにはすべての識別子のログが表示されます。特定のサービスのログをフィルタリングするには、**All** ドロップダウンメニューをクリックして、識別子を選択します。



6. ログエントリーを開くには、選択したログをクリックします。

### 5.3. WEB コンソールでログをフィルターするためのテキスト検索オプション

テキスト検索オプション機能では、ログをフィルタリングするためのさまざまなオプションを利用できます。テキスト検索を使用してログをフィルタリングする場合は、3つのドロップダウンメニューに定義した事前定義オプションを使用するか、自分で検索全体を入力できます。

#### ドロップダウンメニュー

検索のメインパラメーターを指定するのに使用できるドロップダウンメニューには、以下の3つがあります。

- **時間:** このドロップダウンメニューには、検索のさまざまな時間範囲が事前定義されます。
- **優先度:** このドロップダウンメニューでは、さまざまな優先度のオプションを利用できます。**journalctl --priority** オプションに対応します。デフォルトの優先度の値は **Error and above** です。これは、他の優先度を指定しないと毎回設定されます。
- **識別子:** このドロップダウンメニューでは、フィルタリングする ID を選択します。**journalctl --identifier** オプションに対応します。

#### 量記号

検索を指定するのに使用できる量記号は6つあります。これらは、ログテーブルをフィルタリングするための Options で説明されています。

#### ログフィールド

特定のログフィールドを検索する場合は、フィールドとその内容を指定することができます。

#### ログメッセージでの自由形式のテキスト検索

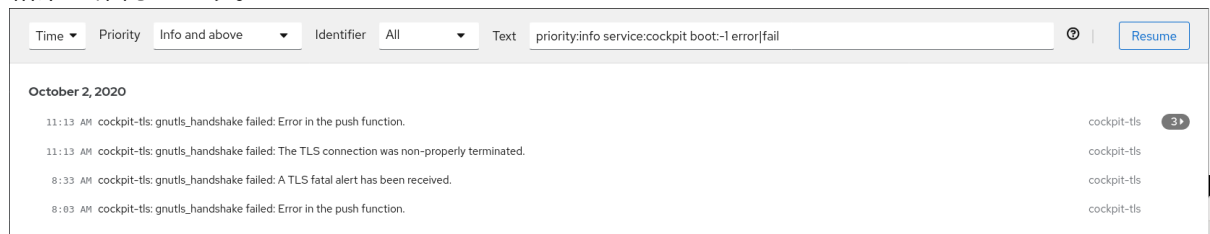
ログメッセージで任意のテキスト文字列をフィルタリングできます。文字列は、正規表現の形式にすることもできます。

#### 高度なログのフィルタリング I

2020年10月22日深夜以降に発生した systemd によって識別されるすべてのログメッセージをフィルターします。ジャーナルフィールド **JOB\_TYPE** は **start** または **restart** のいずれかです。

1. フィールドを検索するには、**identifier:systemd since:2020-10-22 JOB\_TYPE=start,restart** と入力します。

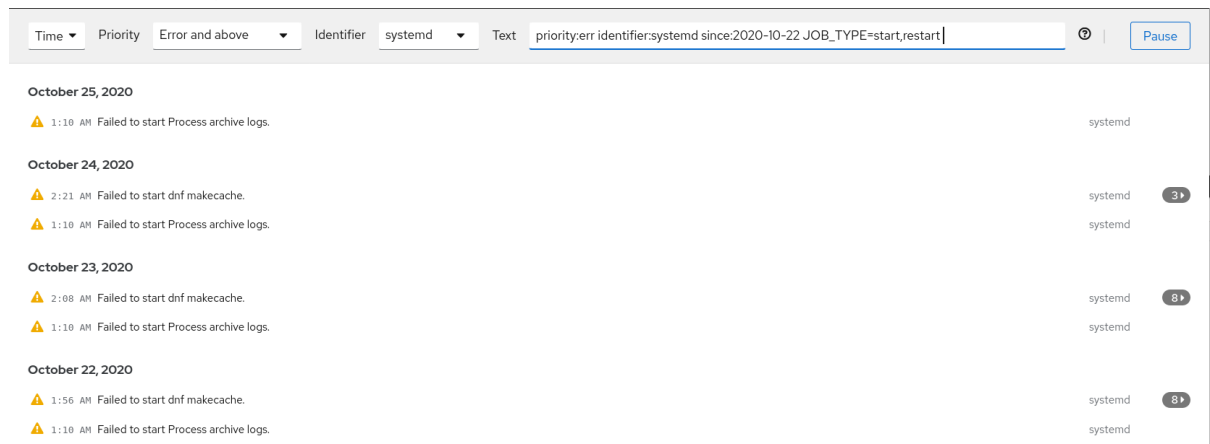
## 2. 結果を確認します。



## 高度なログフィルタリング II

最後の前に起動で cockpit.servicesystemd ユニットから送信されたすべてのログメッセージ、およびメッセージのボディに error または fail が含まれるログメッセージをすべてフィルターします。

1. 検索フィールドに **service:cockpit boot:-1 error|fail** と入力します。
2. 結果を確認します。



## 5.4. テキストボックスのボックスを使用した WEB コンソールでのログのフィルター

テキストの検索ボックスを使用すると、異なるパラメーターに従ってログをフィルターできます。検索は、フィルタリングドロップダウンメニュー、クォーター、ログフィールド、およびフリー形式の文字列検索を組み合わせます。

## 前提条件

- Web コンソールインターフェイスがインストールされており、アクセス可能である。詳細は、[Web コンソールのインストール](#) を参照してください。

## 手順

1. RHEL Web コンソールにログインします。詳細は、[Web コンソールへのログイン](#) を参照してください。
2. **Logs** をクリックします。
3. ドロップダウンメニューを使用して、3つの主要なフィルタリング対象の数量 (時間範囲、優先順位、識別子) (フィルタリングする) を指定します。  
**優先順位** の数量には常に値が必要です。これを指定しない場合、**Error and above** の優先度が自動的にフィルターされます。テキスト検索ボックスに、設定したオプションに注目してください。

4. フィルターするログフィールドを指定します。  
複数のログフィールドを追加できます。
5. 自由形式文字列を使用して他の文字を検索できます。検索ボックスにも正規表現も使用できません。

## 5.5. ログフィルタリングのオプション

複数の `journalctl` オプションがあり、Web コンソールでのログのフィルタリングに使用できます。これは便利な場合があります。これらの一部は、Web コンソールインターフェイスのドロップダウンメニューですすでに扱われています。

表5.1表

| オプション名            | 用途  | 備考   |
|-------------------|---|--|
| <b>priority</b>   | メッセージの優先度による出力をフィルタリングします。単一数値またはテキストログレベルを取ります。ログレベルは、通常の <code>syslog</code> ログレベルです。単一のログレベルが指定されている場合、このログレベルまたは低い (より重要な) ログレベルを持つすべてのメッセージが表示されます。        | <b>優先順位</b> ドロップダウンメニューで説明されます。  |
| <b>identifier</b> | 指定された <code>syslog</code> 識別子 <code>SYSLOG_IDENTIFIER</code> のメッセージを表示します。複数回指定できます。  | <b>識別子</b> ドロップダウンメニューで説明されています。   |
| <b>follow</b>     | 最新のジャーナルエントリーのみを表示し、ジャーナルに追加されるように新しいエントリーを継続的に出力します。   | ドロップダウンで説明しません。  |
| <b>service</b>    | 指定した <code>systemd</code> ユニットのメッセージを表示します。複数回指定できます。   | ドロップダウンで説明されません。 <code>journalctl --unit</code> パラメーターに対応します。                                  |
| <b>boot</b>       | 特定のブートのメッセージを表示します。<br><br>正の整数は、ジャーナルの最初から起動を探し、ゼロ以下の整数は、ジャーナルの最後から起動を探します。このため、1は、時系列順でジャーナルで見つかった最初の起動を意味し、2は次に見つかったものと続きます。また、-0は最後の起動、-1は最後の起動の1つ前などとなります。 | <b>時間</b> ドロップダウンメニューでは、 <b>現在の起動</b> または <b>以前の起動</b> としてのみ説明されています。その他のオプションは手動で書き込む必要があります。 |



| オプション名       | 用途   | 備考              |
|--------------|--|-----------------|
| <b>since</b> | <p>指定の日付以降のエントリーまたは指定の日付以前のエントリーを示します。日付は、2012-10-30 18:17:16 の形式にする必要があります。時間部分を省略すると、00:00:00 が想定されます。2 番目のコンポーネントのみを省略すると、:00 が想定されます。日付コンポーネントを省略すると、現在の日付が想定されます。</p> <p>yesterday、today、tomorrow も利用できます。それぞれ、現在の日付けの前の 00:00:00、現在の日付け、現在の日付けの後の日を参照します。now は、現在時刻を意味します。最後に、相対時間は-または+を前に付けてを指定できます。これは、現在時間の前または後の時間を参照します。</p> | ドロップダウンで説明しません。 |

## 第6章 WEB コンソールでユーザーアカウントの管理

RHEL Web コンソールは、システムユーザーアカウントの追加、編集、および削除を行うインターフェイスを提供します。

本セクションの内容を読むと、以下を理解できます。

- 既存のアカウントが存在する場所
- 新規アカウントの追加方法
- パスワードの有効期限の設定方法
- ユーザーセッションを終了する方法および時期

### 前提条件

- 管理者権限が割り当てられたアカウントで RHEL Web コンソールにログインしている。詳細は [RHEL 8 Web コンソールへのログイン](#) を参照してください。

### 6.1. WEB コンソールで管理されるシステムユーザーアカウント

RHEL Web コンソールに表示されているユーザーアカウントでは、以下が可能になります。

- システムにアクセスする際にユーザーを認証する
- システムへのアクセス権を設定する

RHEL Web コンソールは、システムに存在するすべてのユーザーアカウントを表示します。そのため、最初に Web コンソールにログインした直後は、ユーザーアカウントが少なくとも1つ表示されます。

RHEL Web コンソールにログインしたら、以下の操作を実行できます。

- 新規ユーザーアカウントの作成
- パラメーターの変更
- アカウントのロック
- ユーザーセッションの終了

### 6.2. WEB コンソールで新規アカウントの追加

RHEL Web コンソールを使用して、システムにユーザーアカウントを追加し、アカウントに管理権限を設定できます。

#### 前提条件

- RHEL Web コンソールがインストールされており、アクセス可能である。詳細は、[Web コンソールのインストール](#) を参照してください。

#### 手順

1. RHEL Web コンソールにログインします。

2. **Accounts** をクリックします。
3. **Create New Account** をクリックします。
4. **フルネーム** フィールドにユーザーの氏名を入力します。  
RHEL Web コンソールは、入力した氏名からユーザー名が自動的に作成され、**ユーザー名** フィールドに入力されます。名前の頭文字と、苗字で設定される命名規則を使用しない場合は、入力されたユーザー名を変更します。
5. **パスワード/確認** フィールドにパスワードを入力し、再度パスワードを入力します。  
フィールドの下にあるカラーバーは、入力したパスワードの強度を表し、弱いパスワードは使用できないようにします。
6. **作成** をクリックして設定を保存し、ダイアログボックスを閉じます。
7. 新規作成したアカウントを選択します。
8. **Groups** ドロップダウンメニューで、新しいアカウントに追加するグループを選択します。

The screenshot shows a 'New User' dialog box with the following fields and controls:

- Full name:** Input field containing 'New User'.
- User name:** Input field containing 'nuser'.
- Groups:** Dropdown menu showing 'nuser'.
- Last login:** Input field containing 'Never'.
- Options:** Checkboxes for 'Disallow interactive password' (unchecked), 'Never expire account' (checked), and an 'edit' link.
- Password:** Buttons for 'Set password', 'Force change', and 'Never expire password' with an 'edit' link.
- Buttons for 'Terminate session' and 'Delete' are located in the top right corner.

これで **アカウント** 設定に新規アカウントが表示され、認証情報を使用してシステムに接続できるようになりました。

### 6.3. WEB コンソールでパスワード有効期限の強制

デフォルトでは、ユーザーアカウントのパスワードに期限はありません。定義した日数が経過したら、システムパスワードが期限切れになるように設定できます。パスワードが期限切れになると、次回のログイン時にパスワードの変更が要求されます。

#### 手順

1. RHEL 8 Web コンソールにログインします。
2. **Accounts** をクリックします。
3. パスワードの有効期限を設定するユーザーアカウントを選択します。
4. **Password** 行の **edit** をクリックします。

The screenshot shows a row for password management with the following elements:

- Password:** Label for the row.
- Buttons for 'Set password' and 'Force change'.
- Text: 'Require password change on March 2, 2024'.
- Button: 'edit' (highlighted with a red box).

5. **Password expiration** ダイアログボックスで、**Require password change every ... days**を選択し、パスワードの期限が切れるまでの日数 (正の整数) を入力します。
6. **Change** をクリックします。  
Web コンソールの **Password** 行に、将来のパスワード変更リクエストの日付がすぐに表示されます。

## 6.4. WEB コンソールでユーザーセッションの終了

ユーザーがシステムにログインすると、ユーザーセッションが作成されます。ユーザーセッションを終了すると、ユーザーはシステムからログアウトされます。これは、システムのアップグレードなどの、設定変更の影響を受ける管理タスクを実行する必要がある場合に便利です。

RHEL 8 Web コンソールの各ユーザーアカウントで、現在使用している Web コンソールセッション以外のセッションすべてを終了できます。これにより、システムへの不正アクセスを阻止できます。

### 手順

1. RHEL 8 Web コンソールにログインします。
2. **Accounts** をクリックします。
3. セッションを終了するユーザーアカウントをクリックします。
4. **Terminate Session** をクリックします。  
**Terminate Session** ボタンが無効になっている場合は、ユーザーがシステムにログインしていません。

RHEL Web コンソールはセッションを終了します。

## 第7章 WEB コンソールでのサービスの管理

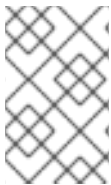
RHEL Web コンソールインターフェイスでシステムサービスを管理する方法を説明します。サービスをアクティブまたは非アクティブにしたり、サービスを再起動または再読み込みしたり、自動起動を管理したりできます。

### 7.1. WEB コンソールでのシステムサービスのアクティブ化または非アクティブ化

この手順では、Web コンソールインターフェイスを使用して、システムサービスをアクティブまたは非アクティブにします。

#### 前提条件

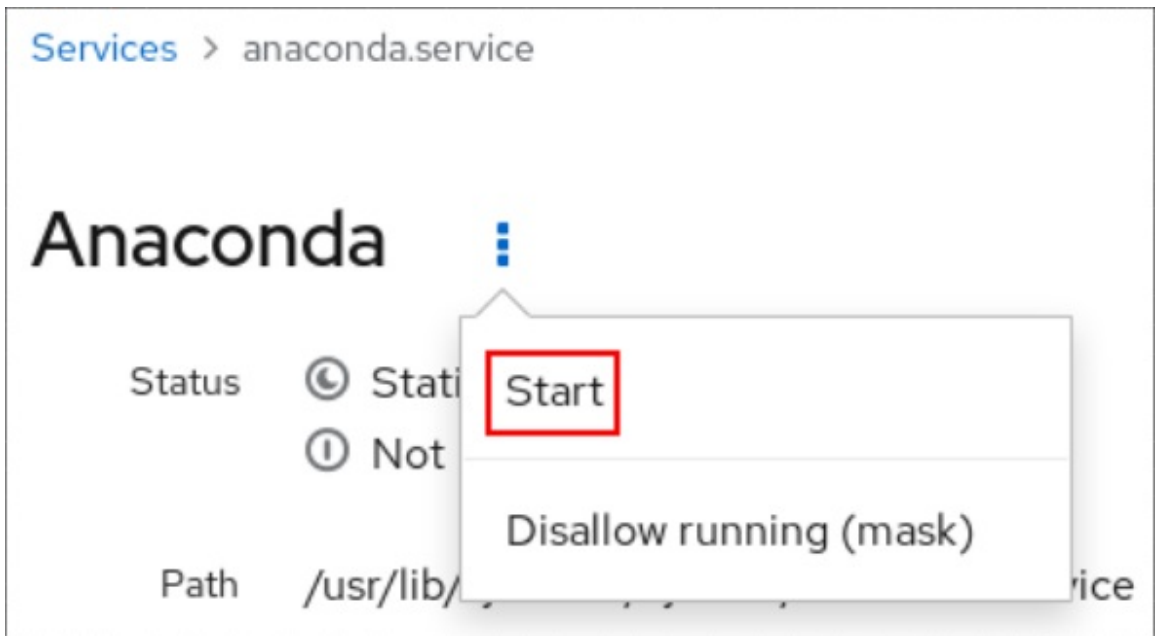
- RHEL 8 Web コンソールがインストールされている。  
詳細は、[Web コンソールのインストールおよび有効化](#) を参照してください。



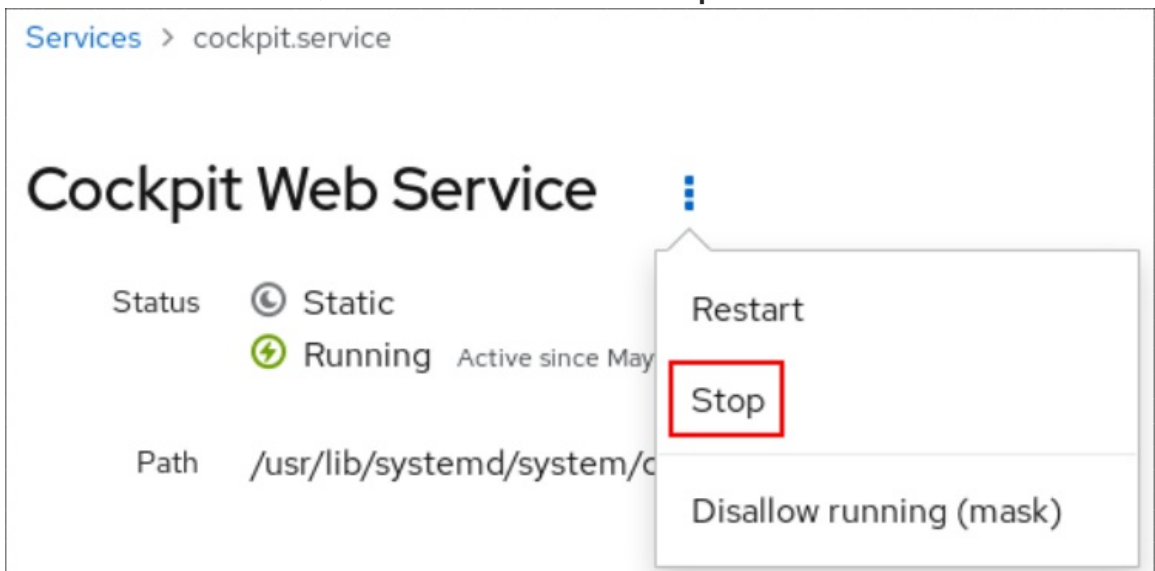
#### 手順

名前または説明でサービスをフィルタリングできます。また、サービスの自動起動を有効、無効、または静的なものでフィルタリングできます。インターフェイスには、サービスの現在の状態と最近のログが表示されます。

1. 管理者権限で RHEL Web コンソールにログインしている。  
詳細は、[Web コンソールへのログイン](#) を参照してください。
2. 左側の Web コンソールメニューで **Services** をクリックします。
3. **サービス** のデフォルトタブは **システムサービス** です。ターゲット、ソケット、タイマー、またはパスを管理する場合は、上部のメニューのそれぞれのタブに切り替えます。
4. サービス設定を開くには、リストから選択したサービスをクリックします。**状態** 列を選択すると、アクティブまたは非アクティブのサービスを確認できます。
5. サービスをアクティブ化または非アクティブ化します。
  - 非アクティブなサービスをアクティブにするには、**Start** ボタンをクリックします。



- アクティブなサービスを非アクティブにするには、**Stop** ボタンをクリックします。



## 7.2. WEB コンソールでのシステムサービスの再起動

この手順では、Web コンソールインターフェイスを使用してシステムサービスを再起動します。

### 前提条件

- RHEL 8 Web コンソールがインストールされている。  
詳細は、[Web コンソールのインストールおよび有効化](#) を参照してください。



### 手順

名前または説明でサービスをフィルタリングできます。また、サービスの自動起動を有効、無効、または静的なものでフィルタリングできます。インターフェイスには、サービスの現在の状態と最近のログが表示されます。

1. 管理者権限で RHEL Web コンソールにログインしている。  
詳細は、[Web コンソールへのログイン](#) を参照してください。

2. 左側の Web コンソールメニューで **Services** をクリックします。
3. サービスのデフォルトタブは **システムサービス** です。ターゲット、ソケット、タイマー、またはパスを管理する場合は、上部のメニューのそれぞれのタブに切り替えます。
4. サービス設定を開くには、リストから選択したサービスをクリックします。
5. サービスを再起動するには、**Restart** ボタンをクリックします。

### 7.3. WEB コンソールでのマニフェスト設定のオーバーライド

システムの特定のユーザーおよび全ユーザーの Web コンソールのメニューを変更できます。**cockpit** プロジェクトでは、パッケージ名はディレクトリー名です。パッケージには、**manifest.json** ファイルと他のファイルが含まれています。デフォルト設定は、**manifest.json** ファイルに存在します。指定したユーザーの特定の場所に **<package-name>.override.json** ファイルを作成することで、デフォルトの **cockpit** メニュー設定をオーバーライドできます。

#### 前提条件

- RHEL 8 Web コンソールがインストールされている。  
詳細は、[Web コンソールのインストールおよび有効化](#) を参照してください。

#### 手順

1. 任意のテキストエディターで **<systemd>.override.json** ファイルのマニフェスト設定をオーバーライドします。次に例を示します。
  - a. すべてのユーザーの設定を編集するには、次のように入力します。

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

- b. 単一ユーザーの設定を編集するには、次のように入力します。

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

2. 次の詳細を含む必要なファイルを編集します。

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

- **null** 値を指定すると、**services** タブが非表示になります。
  - **-1** 値を指定すると、**logs** タブが一番目に移動します。
3. **cockpit** サービスを再起動します。

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

## 関連情報

- **cockpit(1)** man ページ
- [Manifest overrides](#)



## 第8章 WEB コンソールを使用したネットワークボンディングの設定

RHEL 8 Web コンソールでネットワークボンディングがどのように機能し、ネットワークボンディングの設定方法を確認します。



### 注記

RHEL 8 Web コンソールは、ネットワーク関連の操作に NetworkManager サービスを使用します。

### 前提条件

- RHEL 8 Web コンソールがインストールされ、有効になっている。詳細は、[Web コンソールのインストール](#) を参照してください。

## 8.1. ボンディングモードに応じたアップストリームのスイッチ設定

使用するボンディングモードに応じて、スイッチでポートを設定する必要があります。

| ボンディングモード                | スイッチの設定  |
|--------------------------|--|
| <b>0 - balance-rr</b>    | Link Aggregation Control Protocol (LACP) がネゴシエートされたものではなく、静的 EtherChannel を有効にする必要があります。 |
| <b>1 - active-backup</b> | このスイッチで必要な設定は必要ありません。  |
| <b>2 - balance-xor</b>   | (LACP がネゴシエートされたものではなく) 静的な Etherchannel を有効にする必要があります。                                  |
| <b>3 - broadcast</b>     | (LACP がネゴシエートされたものではなく) 静的な Etherchannel を有効にする必要があります。                                  |
| <b>4 - 802.3ad</b>       | LACP がネゴシエートされた Etherchannel が有効になっている必要があります。   |
| <b>5 - balance-tlb</b>   | このスイッチで必要な設定は必要ありません。  |
| <b>6 - balance-alb</b>   | このスイッチで必要な設定は必要ありません。  |

スイッチの設定方法の詳細は、スイッチのドキュメントを参照してください。



### 重要

特定のネットワークボンディング機能 (例: fail-over メカニズム) は、ネットワークスイッチなしでのダイレクトケーブル接続に対応していません。詳細は、[ボンディングは、クロスオーバーケーブルを使用したダイレクトコレクションをサポートしますか?](#) を参照してください。を参照してください。

## 8.2. ボンディングモード

RHEL 8 では、複数のモードオプションがあります。各モードオプションは、特定の負荷分散とフォールトトレランスを特徴としています。ボンディングインターフェイスの動作は、モードによって異なります。ボンディングモードは、フォールトトレランス、負荷分散、またはその両方を提供します。

### ロードバランスモード

- **ラウンドロビン** - 最初に利用可能なインターフェイスから最後のインターフェイスへ、パケットを送信します。

### フォールトトレランスモード

- **アクティブバックアップ** - プライマリーインターフェイスが失敗した場合にのみ、いずれかのバックアップインターフェイスがそれを置き換えます。アクティブインターフェイスが使用する MAC アドレスだけが表示されます。
- **ブロードキャスト** - すべての送信は、すべてのインターフェイスで行われます。



#### 注記

ブロードキャストは、ボンディングされたすべてのインターフェイスのネットワークトラフィックを大幅に増やします。

### フォールトトレランスおよび負荷分散モード

- **XOR** - 宛先 MAC アドレスは、モジュロハッシュを持つインターフェイス間で均等に分散されます。そして、各インターフェイスは、同じ MAC アドレスのグループを提供します。
- **802.3ad** - IEEE 802.3ad 動的リンクアグリゲーションのポリシーを設定します。同一の速度とデュプレックス設定を共有するアグリゲーショングループを作成します。アクティブなアグリゲーターのすべてのインターフェイスで送受信を行います。



#### 注記

このモードには、802.3ad コンプライアントのスイッチが必要です。

- **適応送信の負荷分散** - 発信トラフィックは、各インターフェイスの現在の負荷に従って分散されます。受信トラフィックは、現在のインターフェイスにより受信されます。受信しているインターフェイスが失敗すると、別のインターフェイスが、失敗したインターフェイスの MAC アドレスを引き継ぎます。
- **適応負荷分散** - IPv4 トラフィック用の送受信負荷分散が含まれます。受信ロードバランスは、アドレス解決プロトコル (ARP) ネゴシエーションにより行われるため、ボンディングの設定で **リンク監視** を **ARP** に設定する必要があります。

## 8.3. RHEL WEB コンソールを使用したネットワークボンディングの設定

Web ブラウザーベースのインターフェイスを使用してネットワーク設定を管理する場合は、RHEL Web コンソールを使用してネットワークボンディングを設定します。

### 前提条件

- RHEL Web コンソールにログインしています。

- サーバーに、2つ以上の物理ネットワークデバイスまたは仮想ネットワークデバイスがインストールされている。
- ボンディングのメンバーとしてイーサネットデバイスを使用するには、物理または仮想のイーサネットデバイスがサーバーにインストールされている。
- チーム、ブリッジ、または VLAN デバイスを結合のメンバーとして使用するには、次の説明に従って事前に作成します。
  - [RHEL Web コンソールを使用したネットワークチームの設定](#)
  - [RHEL Web コンソールを使用したネットワークブリッジの設定](#)
  - [RHEL Web コンソールを使用した VLAN タグ付けの設定](#)

## 手順

1. 画面左側のナビゲーションで **Networking** タブを選択します。
2. **Interfaces** セクションで **Add bond** をクリックします。
3. 作成するボンドデバイスの名前を入力します。
4. 結合のメンバーにするインターフェイスを選択します。
5. 結合のモードを選択します。  
**Active backup** を選択すると、Web コンソールに追加フィールド **Primary** が表示され、優先するアクティブデバイスを選択できます。
6. リンクモニタリング監視モードを設定します。たとえば、**Adaptive load balancing** モードを使用する場合は、**ARP** に設定します。
7. オプション: モニター間隔、リンクアップ遅延、およびリンクダウン遅延の設定を調整します。通常、トラブルシューティングの目的でのみデフォルトを変更します。

## Bond settings

Name

Interfaces  enp7s0  
 enp8s0

MAC

Mode

Primary

Link monitoring

Monitoring interval

Link up delay

Link down delay

8. **Apply** をクリックします。
9. デフォルトでは、ボンドは動的 IP アドレスを使用します。静的 IP アドレスを設定する場合:
  - a. **Interfaces** セクションでボンドの名前をクリックします。
  - b. 設定するプロトコルの横にある **Edit** をクリックします。
  - c. **Addresses** の横にある **Manual** を選択し、IP アドレス、接頭辞、およびデフォルトゲートウェイを入力します。
  - d. **DNS** セクションで **+** ボタンをクリックし、DNS サーバーの IP アドレスを入力します。複数の DNS サーバーを設定するには、この手順を繰り返します。

- e. **DNS search domains** セクションで、**+** ボタンをクリックし、検索ドメインを入力します。
- f. インターフェイスにスタティックルートが必要な場合は、**Routes** セクションで設定します。

### IPv4 settings ×

Addresses Manual ▼ +

| Address                                | Prefix length or netmask        | Gateway                                  |   |
|--|---------------------------------|--|---|
| <input type="text" value="192.0.2.1"/> | <input type="text" value="24"/> | <input type="text" value="192.0.2.254"/> | - |

---

DNS  Automatic +

Server -

---

DNS search domains  Automatic +

Search domain -

---

Routes  Automatic +

Apply Cancel

- g. **Apply** をクリックします。

## 検証

- 画面左側のナビゲーションで **Networking** タブを選択し、インターフェイスに着信および発信トラフィックがあるかどうかを確認します。

| Interfaces <span style="float: right;"> <span style="border: 1px solid #ccc; padding: 2px 5px; margin-right: 5px;">Add bond</span> <span style="border: 1px solid #ccc; padding: 2px 5px; margin-right: 5px;">Add team</span> <span style="border: 1px solid #ccc; padding: 2px 5px; margin-right: 5px;">Add bridge</span> <span style="border: 1px solid #ccc; padding: 2px 5px;">Add VLAN</span> </span> |              |           |           |
|--|--------------|-----------|-----------|
| Name   | IP address   | Sending   | Receiving |
| <b>bond0</b>   | 192.0.2.1/24 | 1.11 Mbps | 61.2 Mbps |

- ホストからネットワークケーブルを一時的に削除します。  
ソフトウェアユーティリティーを使用して、リンク障害イベントを適切にテストする方法がないことに注意してください。Web コンソールなどの接続を非アクティブ化するツールは、実際のリンク障害イベントではなく、メンバー設定の変更を処理するボンディングドライバーの機能のみを示します。
- ボンドのステータスを表示します。

■

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

## 8.4. WEB コンソールを使用したボンドへのインターフェイスの追加

ネットワークボンディングには複数のインターフェイスを含めることができ、いつでも追加/削除することができます。

既存のボンディングにネットワークインターフェイスを追加する方法を説明します。

### 前提条件

- [Web コンソールを使用したネットワークボンドの設定](#) で説明したように、複数のインターフェイスを持つボンドが設定されている

### 手順

1. Web コンソールにログインします。  
詳細は、[Web コンソールへのログイン](#) を参照してください。
2. **ネットワーキング** を開きます。
3. **インターフェース** テーブルで、設定するボンディングをクリックします。
4. ボンディング設定画面で、メンバー (インターフェイス) の表をスクロールします。
5. **Add member** のドロップダウンアイコンをクリックします。
6. ドロップダウンメニューからインターフェイスを選択し、クリックします。

### 検証手順

- ボンディング設定画面の **インターフェイスメンバー** テーブルに、選択したインターフェイスが表示されていることを確認します。

## 8.5. WEB コンソールを使用したボンディングからインターフェイスの削除または無効化

ネットワークボンディングには複数のインターフェイスを追加できます。デバイスを変更する必要がある場合は、ボンディングから特定のインターフェイスを削除または無効にできます。これにより、残りのアクティブなインターフェイスと動作するようになります。

ボンディングに含まれるインターフェイスの使用を停止するには、以下を行います。

- ボンディングからインターフェイスを削除します。
- インターフェイスを一時的に無効にします。インターフェイスはボンディングの一部のままになりますが、ボンディングは再び有効にするまで使用されません。

### 前提条件

- [Web コンソールを使用したネットワークボンドの設定](#) で説明したように、複数のインターフェイスを持つボンドが設定されている

### 手順

1. RHEL Web コンソールにログインします。詳細は、[Web コンソールへのログイン](#) を参照してください。
2. **ネットワーキング** を開きます。
3. 設定するボンディングをクリックします。
4. ボンディング設定画面で、ポート (インターフェイス) の表をスクロールします。
5. インターフェイスを選択し、削除または無効化します。
  - インターフェイスを削除する場合は、**-** ボタンをクリックします。
  - インターフェイスを無効または有効にするには、選択したインターフェイスの横にあるスイッチを切り替えます。

選択に基づいて、Web コンソールはボンディングからインターフェイスを削除または無効化し、スタンドアロンインターフェイスとして **Networking** セクションに戻ることができます。

## 8.6. WEB コンソールでのボンディングの削除または無効化

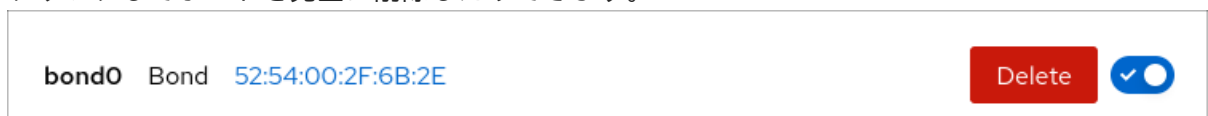
Web コンソールを使用してネットワークボンディングを削除または無効化します。ボンディングを無効にすると、インターフェイスはボンディングに残りますが、ボンディングはネットワークトラフィックに使用されません。

### 前提条件

- Web コンソールには既存のボンディングがあります。

### 手順

1. Web コンソールにログインします。  
詳細は、[Web コンソールへのログイン](#) を参照してください。
2. **ネットワーキング** を開きます。
3. 削除するボンディングをクリックします。
4. ボンドの設定画面では、スイッチを切り替えてボンドを無効/有効にしたり、**Delete** ボタンをクリックしてボンドを完全に削除したりできます。



### 検証手順

- **Networking** に戻り、ボンディングのすべてのインターフェイスがスタンドアロンインターフェイスであることを確認します。

## 第9章 WEB コンソールを使用したネットワークチームの設定

ネットワークボンディングの仕組み、ネットワークチームとネットワークボンディングの違い、および Web コンソールの設定の可能性を学びます。

さらに、以下に関するガイドラインを見つけることができます。

- 新規ネットワークチームの追加
- 既存のネットワークチームへの新規インターフェイスの追加
- 既存のネットワークチームからのインターフェイスの削除
- ネットワークチームの削除



### 重要

Red Hat Enterprise Linux 9 では、ネットワークチーミングが非推奨になりました。サーバーを将来バージョンの RHEL にアップグレードする予定がある場合は、代替手段としてカーネルボンディングドライバーの使用を検討してください。詳細は、[Configuring network bonding](#) を参照してください。

### 前提条件

- RHEL Web コンソールがインストールされ、有効になっている。  
詳細は、[Web コンソールのインストール](#) を参照してください。

## 9.1. RHEL WEB コンソールを使用したネットワークチームの設定

Web ブラウザーベースのインターフェイスを使用してネットワーク設定を管理する場合は、RHEL Web コンソールを使用してネットワークチームを設定します。



### 重要

Red Hat Enterprise Linux 9 では、ネットワークチーミングが非推奨になりました。サーバーを将来バージョンの RHEL にアップグレードする予定がある場合は、代替手段としてカーネルボンディングドライバーの使用を検討してください。詳細は、[Configuring network bonding](#) を参照してください。

### 前提条件

- **teamd** および **NetworkManager-team** パッケージがインストールされている。
- サーバーに、2 つ以上の物理ネットワークデバイスまたは仮想ネットワークデバイスがインストールされている。
- チームのポートとしてイーサネットデバイスを使用するには、物理または仮想のイーサネットデバイスがサーバーにインストールされ、スイッチに接続されている必要があります。
- ボンド、ブリッジ、または VLAN デバイスをチームのポートとして使用するには、次の説明に従って事前に作成します。
  - [RHEL Web コンソールを使用したネットワークボンディングの設定](#)
  - [RHEL Web コンソールを使用したネットワークブリッジの設定](#)



- RHEL Web コンソールを使用した VLAN タグ付けの設定

## 手順

1. 画面左側のナビゲーションで **Networking** タブを選択します。
2. **Interfaces** セクションで **Add team** をクリックします。
3. 作成するチームデバイスの名前を入力します。
4. チームのポートにするインターフェイスを選択します。
5. チームのランナーを選択します。  
**Load balancing** または **802.3ad LACP** を選択すると、Web コンソールに追加のフィールド **Balancer** が表示されます。
6. リンクウォッチャーを設定します。
  - **Ethtool** を選択した場合は、さらに、リンクアップおよびリンクダウンの遅延を設定します。
  - **ARP ping** または **NSNA ping** を選択し、さらに ping の間隔と ping ターゲットを設定します。

### Team settings ×

**Name**

**Ports**

- enp7s0
- enp8s0

**Runner**

**Link watch**

**Link up delay**

**Link down delay**

7. **Apply** をクリックします。
8. デフォルトでは、チームは動的 IP アドレスを使用します。静的 IP アドレスを設定する場合:
  - a. **Interfaces** セクションでチームの名前をクリックします。
  - b. 設定するプロトコルの横にある **Edit** をクリックします。
  - c. **Addresses** の横にある **Manual** を選択し、IP アドレス、接頭辞、およびデフォルトゲートウェイを入力します。
  - d. **DNS** セクションで **+** ボタンをクリックし、DNS サーバーの IP アドレスを入力します。複数の DNS サーバーを設定するには、この手順を繰り返します。
  - e. **DNS search domains** セクションで、**+** ボタンをクリックし、検索ドメインを入力します。
  - f. インターフェイスにスタティックルートが必要な場合は、**Routes** セクションで設定します。

**IPv4 settings** ×

Addresses Manual ▾ **+**

| Address   | Prefix length or netmask | Gateway     |   |
|-----------|--------------------------|-------------|---|
| 192.0.2.1 | 24                       | 192.0.2.254 | − |

DNS  Automatic **+**

Server 192.0.2.253 −

DNS search domains  Automatic **+**

Search domain example.com −

Routes  Automatic **+**

**Apply** Cancel

- g. **Apply** をクリックします。

## 検証

1. 画面左側のナビゲーションで **Networking** タブを選択し、インターフェイスに着信および発信トラフィックがあるかどうかを確認します。

| Interfaces            |              |           |           |
|-----------------------|--------------|-----------|-----------|
| Name                  | IP address   | Sending   | Receiving |
| <a href="#">team0</a> | 192.0.2.1/24 | 1.11 Mbps | 61.2 Mbps |

2. チームのステータスを表示します。

```
# 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
```

この例では、両方のポートが起動しています。

## 関連情報

- [ネットワークチームランナー](#)

## 9.2. WEB コンソールを使用したチームへの新規インターフェイスの追加

ネットワークチームには複数のインターフェイスを含めることができ、いつでもインターフェイスを追加または削除できます。次のセクションでは、既存のチームに新しいネットワークインターフェイスを追加する方法を説明します。

### 前提条件

- ネットワークチームが設定されている。

### 手順

1. Web コンソールにログインします。  
詳細は、[Web コンソールへのログイン](#) を参照してください。
2. ネットワーク タブに切り替えます。
3. インターフェイス テーブルで、設定するチームをクリックします。

4. チーム設定画面で、**ポート** テーブルまでスクロールします。
5. **+** ボタンをクリックします
6. ドロップダウンリストから追加するインターフェイスを選択します。

| Ports  | Sending | Receiving |  |
|--------|---------|-----------|--|
| enp7s0 | 0 bps   | 0 bps     | <div style="border: 1px solid #ccc; padding: 5px;"> <div style="text-align: right; border-bottom: 1px solid #ccc; padding-bottom: 5px;">+</div> <p>enp1s0</p> <p>enp9s0</p> </div> |
| enp8s0 | 0 bps   | 0 bps     |  |

RHEL Web コンソールは、インターフェイスをチームに追加します。

### 9.3. WEB コンソールを使用したチームからインターフェイスの削除または無効化

ネットワークチームには複数のインターフェイスを追加できます。デバイスを変更する必要がある場合は、ネットワークチームから特定のインターフェイスを削除または無効にできます。これにより、残りのアクティブなインターフェイスと動作するようになります。

チームに含まれるインターフェイスの使用を停止する場合は、以下のいずれかの方法で行います。

- チームからのインターフェイスの削除
- インターフェイスを一時的に無効その後、インターフェイスはチームの一部として残りますが、再度有効にするまでチームは使用しません。

#### 前提条件

- 複数のインターフェイスを持つネットワークチームがホストに存在する。

#### 手順

1. RHEL Web コンソールにログインします。  
詳細は、[Web コンソールへのログイン](#) を参照してください。
2. **ネットワーク** タブに切り替えます。
3. 設定するチームをクリックします。
4. チーム設定ウィンドウで、**ポート** (インターフェイス) の表をスクロールします。
5. インターフェイスを選択し、削除または無効化します。
  - a. **ON/OFF** ボタンを Off に切り替えてインターフェイスを無効にします。
  - b. **-** ボタンをクリックしてインターフェイスを削除します。

| Ports  | Sending | Receiving |                                     | + |
|--------|---------|-----------|-------------------------------------|---|
| enp7s0 | 0 bps   | 0 bps     | <input checked="" type="checkbox"/> | - |
| enp8s0 | 0 bps   | 0 bps     | <input checked="" type="checkbox"/> | - |
| enp9s0 | 0 bps   | 0 bps     | <input checked="" type="checkbox"/> | - |

選択に応じて、Web コンソールはインターフェイスを削除または無効にします。インターフェイスを削除すると、ネットワークでスタンドアロンインターフェイスとして利用できます。

## 9.4. WEB コンソールでのチームの削除または無効化

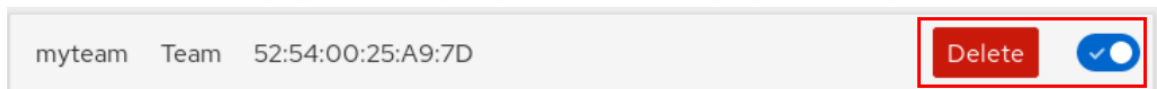
Web コンソールを使用してネットワークチームを削除または無効化します。チームのみを無効にする場合、チーム内のインターフェイスはそのまま残りますが、ネットワークトラフィックには使用されません。

### 前提条件

- ネットワークチームがホストに設定されている。

### 手順

1. Web コンソールにログインします。  
詳細は、[Web コンソールへのログイン](#) を参照してください。
2. ネットワーク タブに切り替えます。
3. 削除または無効にするチームをクリックします。
4. 選択したチームを削除または無効にします。
  - a. **削除** ボタンをクリックすると、チームを削除できます。
  - b. **ON/OFF** スイッチを無効な位置に移動すると、チームを無効にできます。



### 検証手順

- チームを削除した場合には、ネットワークに移動して、チームからのすべてのインターフェイスがスタンドアロンインターフェイスとしてリスト表示されていることを確認します。

## 第10章 WEB コンソールでネットワークブリッジの設定

ネットワークブリッジは、同じ範囲の IP アドレスを持つ1つのサブネットに、複数のインタフェースを接続するのに使用します。

### 前提条件

- RHEL 8 Web コンソールがインストールされ、有効になっている。  
詳細は、[Web コンソールのインストール](#) を参照してください。

### 10.1. RHEL WEB コンソールを使用したネットワークブリッジの設定

Web ブラウザーベースのインターフェイスを使用してネットワーク設定を管理する場合は、RHEL Web コンソールを使用してネットワークブリッジを設定します。

### 前提条件

- サーバーに、2つ以上の物理ネットワークデバイスまたは仮想ネットワークデバイスがインストールされている。
- ブリッジのポートとしてイーサネットデバイスを使用するには、物理または仮想のイーサネットデバイスをサーバーにインストールする必要があります。
- ブリッジのポートにチーム、ボンディング、または VLAN デバイスを使用するには、ブリッジの作成時にこれらのデバイスを作成するか、次の説明に従って事前にデバイスを作成することができます。
  - [RHEL Web コンソールを使用したネットワークチームの設定](#)
  - [RHEL Web コンソールを使用したネットワークボンディングの設定](#)
  - [RHEL Web コンソールを使用した VLAN タグ付けの設定](#)

### 手順

1. 画面左側のナビゲーションで **Networking** タブを選択します。
2. **Interfaces** セクションで **Add bridge** をクリックします。
3. 作成するブリッジデバイスの名前を入力します。
4. ブリッジのポートにするインターフェイスを選択します。
5. オプション: **Spanning tree protocol (STP)** 機能を有効にして、ブリッジループとブロードキャスト放射を回避します。

## Bridge settings ×

**Name**

**Ports**

- enp7s0
- enp8s0

**Options**

- Spanning tree protocol (STP)

6. **Apply** をクリックします。
7. デフォルトでは、ブリッジは動的 IP アドレスを使用します。静的 IP アドレスを設定する場合:
  - a. **Interfaces** セクションでブリッジの名前をクリックします。
  - b. 設定するプロトコルの横にある **Edit** をクリックします。
  - c. **Addresses** の横にある **Manual** を選択し、IP アドレス、接頭辞、およびデフォルトゲートウェイを入力します。
  - d. **DNS** セクションで **+** ボタンをクリックし、DNS サーバーの IP アドレスを入力します。複数の DNS サーバーを設定するには、この手順を繰り返します。
  - e. **DNS search domains** セクションで、**+** ボタンをクリックし、検索ドメインを入力します。
  - f. インターフェイスにスタティックルートが必要な場合は、**Routes** セクションで設定します。

### IPv4 settings ×

Addresses Manual ▾ +

| Address                                | Prefix length or netmask        | Gateway                                  | -  |
|--|---------------------------------|--|--|
| <input type="text" value="192.0.2.1"/> | <input type="text" value="24"/> | <input type="text" value="192.0.2.254"/> | <span style="border: 1px solid gray; padding: 2px 5px;">-</span> |

---

DNS  Automatic +

Server -

---

DNS search domains  Automatic +

Search domain -

---

Routes  Automatic +

Apply Cancel

g. **Apply** をクリックします。

## 検証

- 画面左側のナビゲーションで **Networking** タブを選択し、インターフェイスに着信および発信トラフィックがあるかどうかを確認します。

| Interfaces <span style="float: right;"> <span style="border: 1px solid gray; padding: 2px 5px; margin-right: 5px;">Add bond</span> <span style="border: 1px solid gray; padding: 2px 5px; margin-right: 5px;">Add team</span> <span style="border: 1px solid gray; padding: 2px 5px; margin-right: 5px;">Add bridge</span> <span style="border: 1px solid gray; padding: 2px 5px;">Add VLAN</span> </span> |              |           |           |
|--|--------------|-----------|-----------|
| Name   | IP address   | Sending   | Receiving |
| <span style="color: #0070c0;">bridge0</span>   | 192.0.2.1/24 | 1.11 Mbps | 61.2 Mbps |

## 10.2. WEB コンソールでブリッジからインターフェイスを削除

ネットワークブリッジには複数のインターフェイスを追加できます。インターフェイスは、ブリッジから削除できます。削除した各インターフェイスは、自動的にスタンドアロンインターフェイスに変更します。

RHEL 8 システムで作成したソフトウェアブリッジからネットワークインターフェイスを削除する方法を説明します。

### 前提条件



- システムで複数のインターフェイスを持つブリッジがある。

### 手順

1. RHEL Web コンソールにログインします。詳細は、[Web コンソールへのログイン](#) を参照してください。
2. **ネットワーキング** を開きます。
3. 設定するブリッジを選択します。
4. ブリッジ設定画面で、ポート (インターフェイス) の表をスクロールします。
5. インターフェイスを選択し、**-** ボタンをクリックします。

### 検証手順

- **Networking** に移動して、**Interface members** テーブルにスタンドアロンインターフェイスとして表示されていることを確認します。

## 10.3. WEB コンソールでブリッジの削除

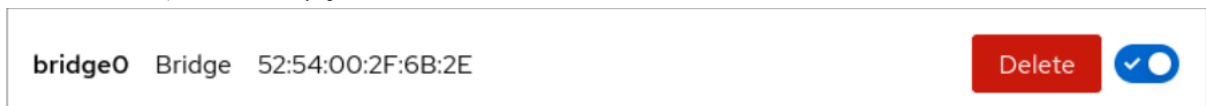
RHEL Web コンソールで、ソフトウェアのネットワークブリッジを削除できます。ブリッジに含まれるすべてのネットワークインターフェイスが、自動的にスタンドアロンインターフェイスに変更されます。

### 前提条件

- システムにブリッジがある。

### 手順

1. RHEL Web コンソールにログインします。  
詳細は、[Web コンソールへのログイン](#) を参照してください。
2. **ネットワーキング** セクションを開きます。
3. 設定するブリッジを選択します。
4. **Delete** をクリックします。



### 検証手順

- **ネットワーク** に戻り、すべてのネットワークインターフェイスが **インターフェイスメンバー** テーブル に表示されていることを確認します。

以前はブリッジの一部であったインターフェイスが無効になることもあります。必要に応じて、アクティベーションを行い、ネットワークパラメーターを手動で設定してください。

## 第11章 WEB コンソールで VLAN の設定

本セクションでは、仮想ローカルエリアネットワーク (VLAN) を設定する方法を説明します。VLAN は、物理ネットワーク内の論理ネットワークです。VLAN インターフェイスは、インターフェイスを通過する際に VLAN ID でパケットをタグ付けし、返信パケットのタグを削除します。

### 11.1. RHEL WEB コンソールを使用した VLAN タグ付けの設定

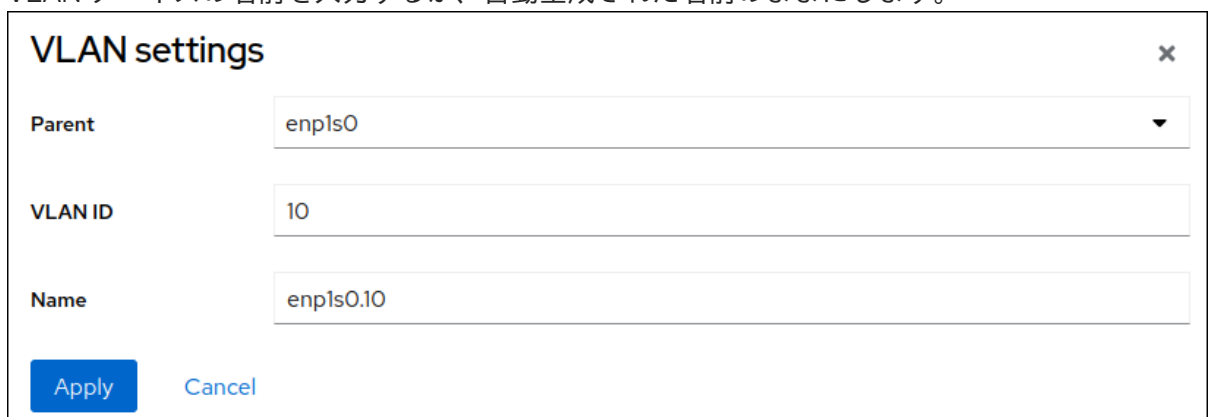
Web ブラウザーベースのインターフェイスを使用してネットワーク設定を管理する場合は、RHEL Web コンソールを使用して VLAN タグ付けを設定します。

#### 前提条件

- 仮想 VLAN インターフェイスに対する親として使用するインターフェイスが VLAN タグに対応している。
- ボンドインターフェイスに VLAN を設定する場合は、以下のようになります。
  - ボンディングのポートが起動している。
  - ボンドが、**fail\_over\_mac=follow** オプションで設定されていない。VLAN 仮想デバイスは、親の新規 MAC アドレスに一致する MAC アドレスを変更できません。このような場合、トラフィックは間違ったソースの MAC アドレスで送信されます。
  - ボンドは通常、DHCP サーバーまたは IPv6 自動設定から IP アドレスを取得することは想定されていません。結合を作成する IPv4 および IPv6 プロトコルを無効にして、これを確認します。そうしないと、DHCP または IPv6 の自動設定がしばらくして失敗した場合に、インターフェイスがダウンする可能性があります。
- ホストが接続するスイッチは、VLAN タグに対応するように設定されています。詳細は、スイッチのドキュメントを参照してください。

#### 手順

1. 画面左側のナビゲーションで **Networking** タブを選択します。
2. **Interfaces** セクションで **Add VLAN** をクリックします。
3. 親デバイスを選択します。
4. VLAN ID を入力します。
5. VLAN デバイスの名前を入力するか、自動生成された名前のままにします。



**VLAN settings** ✕

Parent

VLAN ID

Name

6. **Apply** をクリックします。
7. デフォルトでは、VLAN デバイスは動的 IP アドレスを使用します。静的 IP アドレスを設定する場合:
  - a. **Interfaces** セクションで VLAN デバイスの名前をクリックします。
  - b. 設定するプロトコルの横にある **Edit** をクリックします。
  - c. **Addresses** の横にある **Manual** を選択し、IP アドレス、接頭辞、およびデフォルトゲートウェイを入力します。
  - d. **DNS** セクションで **+** ボタンをクリックし、DNS サーバーの IP アドレスを入力します。複数の DNS サーバーを設定するには、この手順を繰り返します。
  - e. **DNS search domains** セクションで、**+** ボタンをクリックし、検索ドメインを入力します。
  - f. インターフェイスにスタティックルートが必要な場合は、**Routes** セクションで設定します。

### IPv4 settings ×

Addresses Manual ▾ +

| Address                                | Prefix length or netmask        | Gateway                                  |  |
|--|---------------------------------|--|--|
| <input type="text" value="192.0.2.1"/> | <input type="text" value="24"/> | <input type="text" value="192.0.2.254"/> | <span style="border: 1px solid #ccc; padding: 2px 5px;">-</span> |

---

DNS  Automatic +

Server  -

---

DNS search domains  Automatic +

Search domain  -

---

Routes  Automatic +

Apply Cancel

- g. **Apply** をクリックします。

## 検証

- 画面左側のナビゲーションで **Networking** タブを選択し、インターフェイスに着信および発信トラフィックがあるかどうかを確認します。

| Interfaces                |              |           |           |
|---------------------------|--------------|-----------|-----------|
| Name                      | IP address   | Sending   | Receiving |
| <a href="#">enp1s0.10</a> | 192.0.2.1/24 | 1.11 Mbps | 61.2 Mbps |

## 第12章 WEB コンソールのリッスンポートの設定

RHEL 8 Web コンソールを使用して新しいポートを許可するか、既存のポートを変更する方法を説明します。

### 12.1. アクティブな SELINUX があるシステムで新しいポートを許可

選択したポートで Web コンソールがリッスンできるようにします。

#### 前提条件

- Web コンソールがインストールされており、アクセス可能である。詳細は、[Web コンソールのインストール](#) を参照してください。

#### 手順

- SELinux の他の部分で定義されていないポートの場合は、次のコマンドを実行します。

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

- SELinux の他の部分ですでに定義されているポートの場合は、次のコマンドを実行します。

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

変更はすぐに有効になります。

### 12.2. FIREWALLD を使用したシステムでの新規ポートの許可

Web コンソールが新規ポートで接続を受信するようにします。

#### 前提条件

- Web コンソールがインストールされており、アクセス可能である。詳細は、[Web コンソールのインストール](#) を参照してください。
- **firewalld** サービスが実行している。

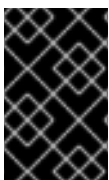
#### 手順

1. 新しいポート番号を追加するには、次のコマンドを実行します。

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

2. **cockpit** サービスから古いポート番号を削除するには、次のコマンドを実行します。

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



#### 重要

**--permanent** オプションなしで **firewall-cmd --service cockpit --add-port=PORT\_NUMBER/tcp** を実行するだけで、次回の **firewalld** の再読み込みまたはシステムの再起動で変更が取り消されます。

## 12.3. WEB コンソールポートの変更

ポート 9090 でデフォルトの転送制御プロトコル (TCP) を別のポートに変更します。

### 前提条件

- Web コンソールがインストールされており、アクセス可能である。詳細は、[Web コンソールのインストール](#) を参照してください。
- SELinux を有効にして、Web コンソールが新しいポートでリッスンできるようにポリシーを変更します。詳細は [アクティブな SELinux があるシステムで新しいポートを許可](#) を参照してください。
- デフォルト設定の **firewalld** サービスでは、Web コンソールの新しいポートを開く必要があります。詳細は、[firewalld を使用してシステムで新しいポートを許可する](#) を参照してください。

### 手順

1. 以下のいずれかの方法でリッスンポートを変更します。

- a. **systemctl edit cockpit.socket** コマンドの使用

- i. 以下のコマンドを入力します。

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

これにより、**/etc/systemd/system/cockpit.socket.d/override.conf** ファイルが開きます。

- ii. **override.conf** の内容を変更して、次の設定を含めます。

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

**ListenStream** オプションは、目的のアドレスと TCP ポートを指定します。



### 注記

最初の行に空の値が含まれているのは意図的なものです。**systemd** では、1つのソケットユニットで複数の **ListenStream** ディレクティブを宣言できます。ドロップインファイルの空の値は一覧をリセットし、元のユニットからのデフォルトのポート 9090 を無効にします。

- b. または、以前のソケット設定を **/etc/systemd/system/cockpit.socket.d/listen.conf** ファイルに追加します。

**cockpit.socket.d.** ディレクトリーがない場合は、**listen.conf** ファイルを作成します。

2. 変更を有効にするには、次のコマンドを実行します。

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

前の手順で **systemctl edit cockpit.socket** を使用していた場合は、**systemctl daemon-reload** を実行する必要はありません。

## 検証手順

- 変更が成功したことを確認するには、新しいポートで Web コンソールへの接続を試行します。

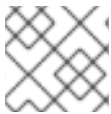
## 第13章 WEB コンソールでファイアウォールの管理

ファイアウォールは、外部からの不要なトラフィックからマシンを保護する方法です。ファイアウォールルールセットを定義することで、ホストマシンに着信ネットワークトラフィックを制御できます。このようなルールは、着信トラフィックを分類して、拒否または許可するために使用されます。RHEL では、**nftables** バックエンドを備えた **firewalld** サービスがデフォルトのファイアウォールとして機能します。RHEL Web コンソールを通じて、**firewalld** を設定できます。

**firewalld** サービスの詳細は [firewalld の使用](#) を参照してください。

### 13.1. WEB コンソールを使用したファイアウォールの実行

次の手順では、Web コンソールのどこでどのように RHEL 9 システムファイアウォールを実行するかを説明します。

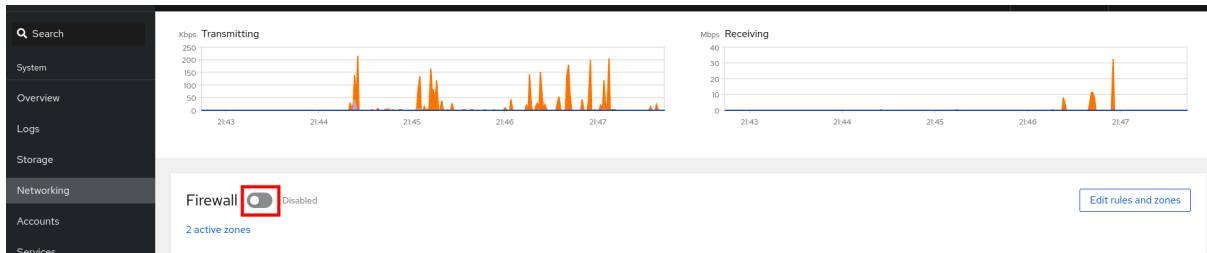


#### 注記

RHEL 8 Web コンソールは、**firewalld** サービスを設定します。

#### 手順

1. RHEL 8 Web コンソールにログインします。詳細は、[Web コンソールへのログイン](#) を参照してください。
2. ネットワーキング セクションを開きます。
3. **ファイアウォール** の項目で、ファイアウォールを実行するスライダーをクリックします。



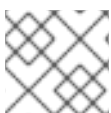
Firewall のスライダーが表示されない場合は、Web コンソールに管理者権限でログインしてください。

この時点で、ファイアウォールは実行しています。

ファイアウォールのルールを設定するには、[Enabling services on the firewall using the web console](#) を参照してください。

### 13.2. WEB コンソールを使用したファイアウォールの停止

次の手順では、Web コンソールのどこでどのように RHEL 9 システムファイアウォールを停止するかを説明します。



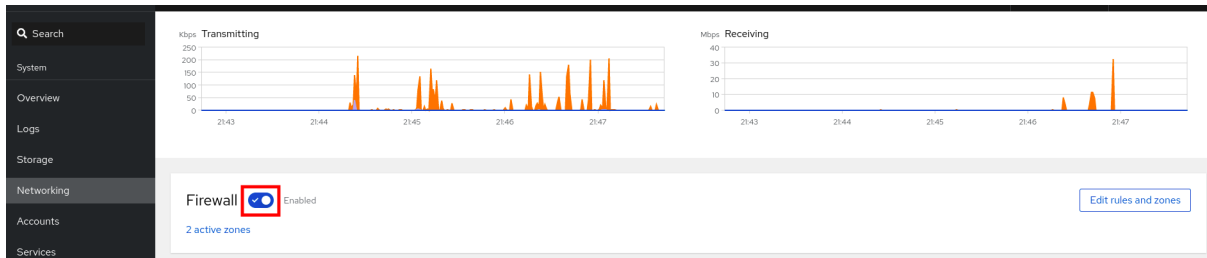
#### 注記

RHEL 8 Web コンソールは、**firewalld** サービスを設定します。

#### 手順



1. RHEL 8 Web コンソールにログインします。詳細は、[Web コンソールへのログイン](#) を参照してください。
2. ネットワーキング セクションを開きます。
3. ファイアウォールの項目で、スライダーをクリックするとファイアウォールが停止します。



Firewall のスライダーが表示されない場合は、Web コンソールに管理者権限でログインしてください。

この段階では、ファイアウォールは停止しており、システムは保護されていません。

### 13.3. ファイアウォールゾーン

**firewalld** ユーティリティを使用すると、ネットワーク内のインターフェイスおよびトラフィックに対する信頼レベルに応じて、ネットワークをさまざまなゾーンに分離できます。接続は1つのゾーンにしか指定できませんが、そのゾーンは多くのネットワーク接続に使用できます。

**firewalld** はゾーンに関して厳格な原則に従います。

1. トラフィックは1つのゾーンのみに入ります。
2. トラフィックは1つのゾーンのみから流出します。
3. ゾーンは信頼のレベルを定義します。
4. ゾーン内トラフィック (同じゾーン内) はデフォルトで許可されます。
5. ゾーン間トラフィック (ゾーンからゾーン) はデフォルトで拒否されます。

原則 4 と 5 は原則 3 の結果です。

原則 4 は、ゾーンオプション **--remove-forward** を使用して設定できます。原則 5 は、新しいポリシーを追加することで設定できます。

**NetworkManager** は、**firewalld** にインターフェイスのゾーンを通知します。次のユーティリティを使用して、ゾーンをインターフェイスに割り当てることができます。

- **NetworkManager**
- **firewall-config** ユーティリティ
- **firewall-cmd** ユーティリティ
- RHEL Web コンソール

RHEL Web コンソール、**firewall-config**、および **firewall-cmd** は、適切な **NetworkManager** 設定ファイルのみを編集できます。Web コンソール、**firewall-cmd** または **firewall-config** を使用してインターフェイスのゾーンを変更する場合、リクエストは **NetworkManager** に転送され、**firewalld** では処理さ

れません。

`/usr/lib/firewalld/zones/` ディレクトリーには事前定義されたゾーンが保存されており、利用可能なネットワークインターフェイスに即座に適用できます。このファイルは、修正しないと `/etc/firewalld/zones/` ディレクトリーにコピーされません。事前定義したゾーンのデフォルト設定は以下のようになります。

### block

- IPv4 の場合は **icmp-host-prohibited** メッセージ、IPv6 の場合は `icmp6-adm-prohibited` メッセージで、すべての着信ネットワーク接続が拒否されます。
- システム内から開始したネットワーク接続のみ。

### dmz

- パブリックにアクセス可能で、内部ネットワークへのアクセスが制限されている DMZ 内のコンピューター。
- Accept: 選択された着信接続のみ。

### drop

適切：着信ネットワークパケットは通知なしでドロップされます。

- 受け入れる: 送信ネットワーク接続のみ。

### external

- マスカレードが有効にされている外部ネットワーク（特にルーター）に適しています。ネットワーク上の他のコンピューターを信頼できない状況。
- Accept: 選択された着信接続のみ。

### home

- ネットワーク上の他のコンピューターをほぼ信頼できる自宅の環境。
- Accept: 選択された着信接続のみ。

### internal

- ネットワーク上の他のコンピューターをほぼ信頼できる内部ネットワーク。
- Accept: 選択された着信接続のみ。

### public

- 適合：ネットワーク上の他のコンピューターを信頼しないパブリックエリア。
- Accept: 選択された着信接続のみ。

### trusted

- Accept: すべてのネットワーク接続を許可します。

### work

ネットワーク上の他のコンピューターをほぼ信頼できる職場の環境。

- Accept: 選択された着信接続のみ。

このゾーンのいずれかを **デフォルトゾーン** に設定できます。インターフェイス接続を **NetworkManager** に追加すると、デフォルトゾーンに割り当てられます。インストール時は、**firewalld** のデフォルトゾーンは **public** ゾーンです。デフォルトゾーンは変更できます。



#### 注記

ユーザーがすぐに理解できるように、ネットワークゾーン名は分かりやすい名前にしてください。

セキュリティ問題を回避するために、ニーズおよびリスク評価に合わせて、デフォルトゾーンの見直しを行ったり、不要なサービスを無効にしてください。

#### 関連情報

- man ページの **firewalld.zone(5)**

## 13.4. WEB コンソールのゾーン

Red Hat Enterprise Linux Web コンソールは、firewalld サービスの主な機能を実装し、以下を可能にします。

- 事前定義したファイアウォールゾーンを特定のインターフェイスまたは IP アドレスの範囲に追加します。
- サービスを選択して、有効なサービスのリストにゾーンを設定できます。
- 有効なサービスのリストからサービスを削除して、サービスを無効にすることもできます。
- インターフェイスからゾーンの削除

## 13.5. WEB コンソールでゾーンの有効化

RHEL Web コンソールを使用して、事前定義された既存のファイアウォールゾーンを特定のインターフェイスまたは IP アドレスの範囲に適用できます。

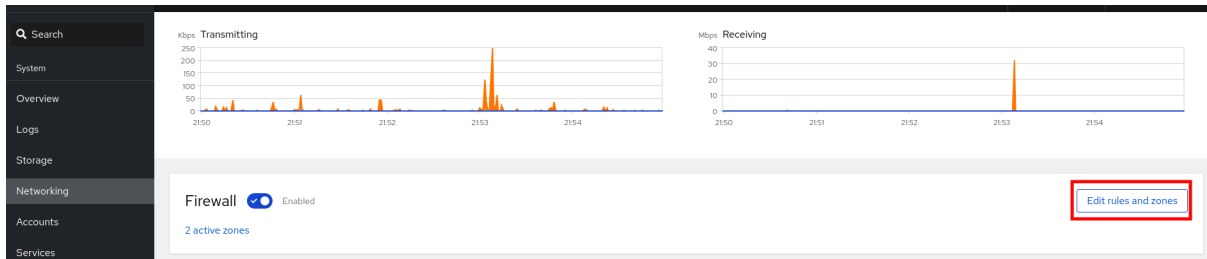
#### 前提条件

- RHEL 8 Web コンソールがインストールされている。詳細は、[Web コンソールのインストールおよび有効化](#) を参照してください。
- ファイアウォールが有効になっている。詳細は [Web コンソールでファイアウォールの実行](#) を参照してください。

#### 手順

1. 管理者権限で Web コンソールにログインします。詳細は、[Web コンソールへのログイン](#) を参照してください。
2. **Networking** をクリックします。

## 3. ルールとゾーンの編集 ボタンをクリックします。



ルールとゾーンの編集 ボタンが表示されない場合は、管理者権限で Web コンソールにログインしてください。

## 4. Firewall セクションの Add new zone をクリックします。

5. ゾーンの追加 ダイアログボックスで、信頼レベル オプションからゾーンを選択します。Web コンソールには、**firewalld** サービスで事前定義されたすべてのゾーンが表示されます。

6. インターフェイス で、選択したゾーンが適用されるインターフェイスを選択します。

7. 許可されたサービス で、ゾーンを適用するかどうかを選択できます。

- サブネット全体
- または、以下の形式の IP アドレスの範囲
  - 192.168.1.0
  - 192.168.1.0/24
  - 192.168.1.0/24,192.168.1.0

## 8. Add zone ボタンをクリックします。

## Add zone ×

**Trust level** Sorted from least to most trusted Custom zones

Public  FedoraServer  
 External  
 Dmz  
 Work  
 Home  
 Internal

**Description** For use in home areas. You mostly trust the other computers on networks to not harm your computer. Only selected incoming connections are accepted.

**Included services** ssh, mdns, samba-client, dhcpv6-client  
The cockpit service is automatically included

**Interfaces** 
 enp0s20f0u4u1u2  enp0s31f6  p2p-dev-wlp61s0  tap0  tun0

**Allowed addresses** 
 Entire subnet  Range

[Cancel](#)

## 検証

- Firewall セクションの設定を確認します。

Network > Firewall

Firewall  Enabled Incoming requests are blocked by default. Outgoing requests are not blocked. [Add new zone](#)

| Service       | TCP  | UDP     |
|---------------|------|---------|
| ssh           | 22   |         |
| mdns          |      | 5353    |
| samba-client  |      | 137,138 |
| dhcpv6-client |      | 546     |
| cockpit       | 9090 |         |

## 13.6. WEB コンソールを使用してファイアウォールでサービスを有効化

デフォルトでは、サービスはデフォルトのファイアウォールゾーンに追加されます。他のネットワークインターフェイスで別のファイアウォールゾーンも使用する場合は、最初にゾーンを選択してから、そのサービスをポートとともに追加する必要があります。

RHEL 8 Web コンソールには、事前定義の **firewalld** サービスが表示され、それらをアクティブなファイアウォールゾーンに追加することができます。



### 重要

RHEL 8 Web コンソールは、**firewalld** サービスを設定します。

また、Web コンソールは、Web コンソールに追加されていない一般的な **firewalld** ルールを許可しません。

### 前提条件

- RHEL 8 Web コンソールがインストールされている。詳細は、[Web コンソールのインストールおよび有効化](#) を参照してください。
- ファイアウォールが有効になっている。詳細は[Web コンソールでファイアウォールの実行](#)を参照してください。

### 手順

1. 管理者権限で RHEL Web コンソールにログインしている。詳細は、[Web コンソールへのログイン](#) を参照してください。
2. **Networking** をクリックします。
3. **ルールとゾーンの編集** ボタンをクリックします。

Search

System

Overview

Logs

Storage

Networking

Accounts

Services

Kbps Transmitting

Mbps Receiving

Firewall  Enabled

2 active zones

[Edit rules and zones](#)

**ルールとゾーンの編集** ボタンが表示されない場合は、管理者権限で Web コンソールにログインしてください。

4. **Firewall** セクションで、サービスを追加するゾーンを選択し、**Add Services** をクリックします。



5. **サービスの追加** ダイアログボックスで、ファイアウォールで有効にするサービスを見つけます。
6. シナリオに応じてサービスを有効にします。

### Add services to home zone

Services  Custom ports

Filter services

- freeipa-4  
TCP: 80, 443, 88, 464, 389, 636 UDP: 88, 464
- freeipa-ldap  
TCP: 80, 443, 88, 464, 389 UDP: 88, 464, 123
- freeipa-ldaps  
TCP: 80, 443, 88, 464, 636 UDP: 88, 464, 123
- freeipa-replication

Add services

Cancel

7. **Add Services** をクリックします。

この時点で、RHEL 8 Web コンソールは、ゾーンの **Services** リストにサービスを表示します。

## 13.7. WEB コンソールでカスタムポートの設定

Web コンソールでは、以下を追加できます。

- 標準ポートでリッスンするサービス: [Web コンソールを使用してファイアウォールでサービスを有効にする](#)
- カスタムポートでリッスンするサービス。

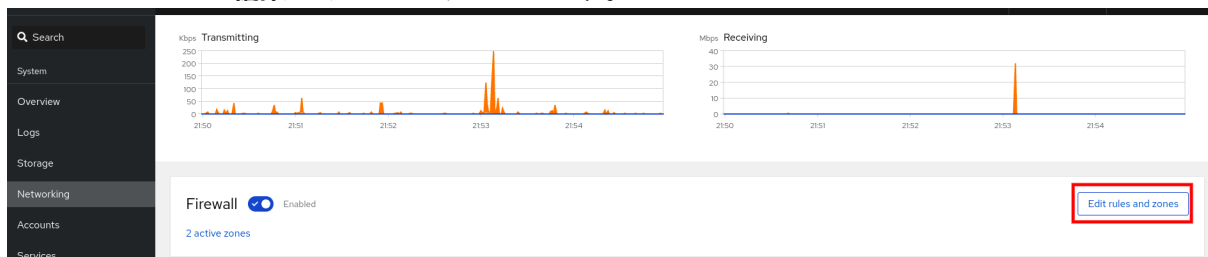
説明に従ってカスタムポートを設定することで、サービスを追加できます。

## 前提条件

- RHEL 8 Web コンソールがインストールされている。詳細は、[Web コンソールのインストールおよび有効化](#) を参照してください。
- ファイアウォールが有効になっている。詳細は[Web コンソールでファイアウォールの実行](#)を参照してください。

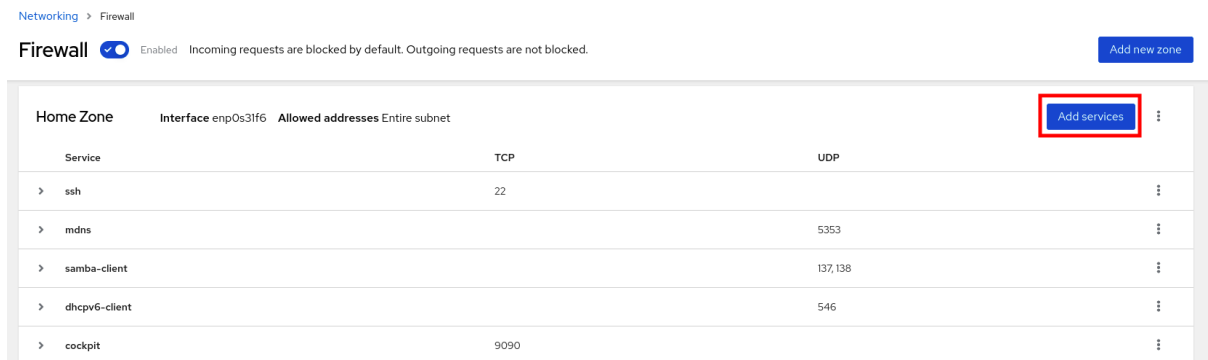
## 手順

1. 管理者権限で RHEL Web コンソールにログインしている。詳細は、[Web コンソールへのログイン](#) を参照してください。
2. **Networking** をクリックします。
3. **ルールとゾーンの編集** ボタンをクリックします。



**ルールとゾーンの編集** ボタンが表示されない場合は、Web コンソールに管理者権限でログインしてください。

4. **ファイアウォール** セクションで、カスタムポートを設定するゾーンを選択し、**サービスの追加** をクリックします。



5. **サービスの追加** ダイアログボックスで、**カスタムポート** ラジオボタンをクリックします。
6. TCP フィールドおよび UDP フィールドに、例に従ってポートを追加します。以下の形式でポートを追加できます。
  - ポート番号 (22 など)
  - ポート番号の範囲 (5900-5910 など)
  - エイリアス (nfs、rsync など)



### 注記

各フィールドには、複数の値を追加できます。値はコンマで区切り、スペースは使用しないでください (例:8080,8081,http)。

7. **TCP** filed、**UDP** filed、またはその両方にポート番号を追加した後、**Name** フィールドでサービス名を確認します。  
名前 フィールドには、このポートを予約しているサービスの名前が表示されます。このポートが無料で、サーバーがこのポートで通信する必要がない場合は、名前を書き換えることができます。
8. **名前** フィールドに、定義されたポートを含むサービスの名前を追加します。
9. **Add Ports** ボタンをクリックします。

## Add ports to home zone ×

Services  Custom ports

**TCP**   
Comma-separated ports, ranges, and services are accepted

**UDP**   
Comma-separated ports, ranges, and services are accepted

**ID**   
If left empty, ID will be generated based on associated port services and port numbers

**Description**

**⚠ Adding custom ports will reload firewalld. A reload will result in the loss of any runtime-only configuration!**

Add ports

Cancel

設定を確認するには、**ファイアウォール** ページに移動し、ゾーンの **サービス** リストでサービスを見つけます。

Networking > Firewall

**Firewall**  Enabled Incoming requests are blocked by default. Outgoing requests are not blocked.

Add new zone

| Service         | TCP  | UDP     |   |
|-----------------|------|---------|---|
| > ssh           | 22   |         | ⋮ |
| > mdns          |      | 5353    | ⋮ |
| > samba-client  |      | 137,138 | ⋮ |
| > dhcpv6-client |      | 546     | ⋮ |
| > cockpit       | 9090 |         | ⋮ |

## 13.8. WEB コンソールを使用したゾーンの無効化

Web コンソールを使用して、ファイアウォール設定のファイアウォールゾーンを無効にできます。

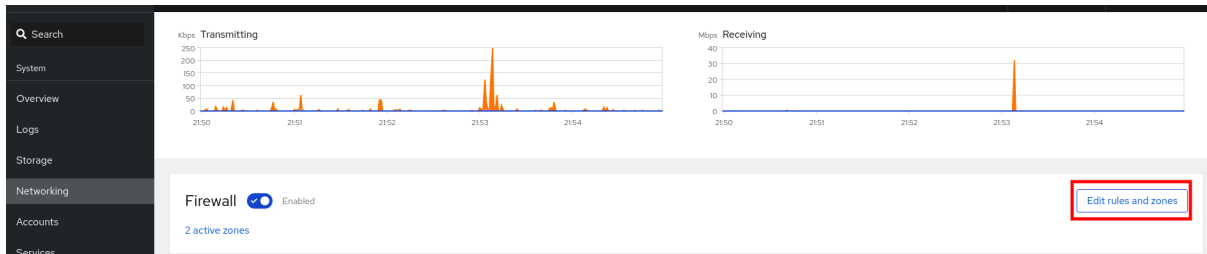
### 前提条件

- RHEL 8 Web コンソールがインストールされている。詳細は、[Web コンソールのインストールおよび有効化](#) を参照してください。



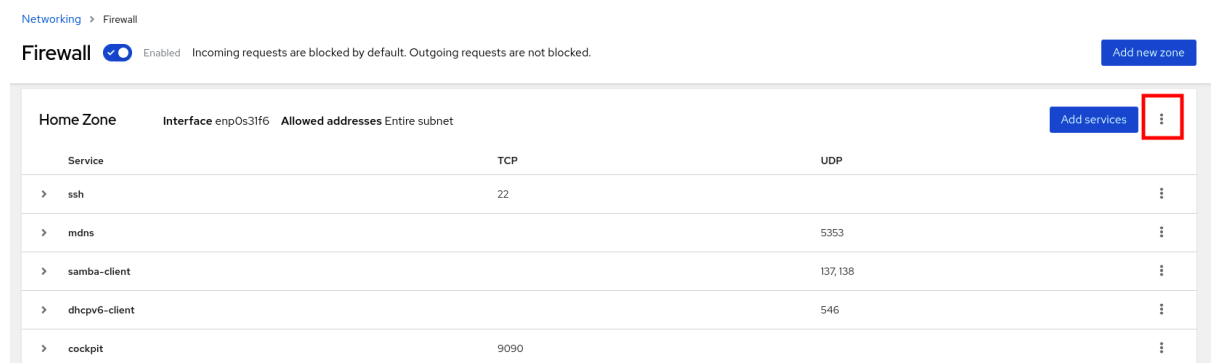
## 手順

1. 管理者権限で RHEL Web コンソールにログインしている。詳細は、[Web コンソールへのログイン](#) を参照してください。
2. **Networking** をクリックします。
3. **ルールとゾーンの編集** ボタンをクリックします。



**ルールとゾーンの編集** ボタンが表示されない場合は、管理者権限で Web コンソールにログインしてください。

4. 削除するゾーンの **オプションアイコン** をクリックします。



5. **Delete** をクリックします。

これでゾーンが無効になり、そのゾーンに設定されたオープンなサービスおよびポートがインターフェイスに含まれなくなります。

## 第14章 WEB コンソールでシステム全体の暗号化ポリシーを設定する

RHEL Web コンソールインターフェイスで、システム全体の暗号化ポリシーとサブポリシーのいずれかを直接設定できます。4つの事前定義されたシステム全体の暗号化ポリシーに加え、グラフィカルインターフェイスを介して、次のポリシーとサブポリシーの組み合わせを適用することもできます。

### DEFAULT:SHA1

**SHA-1** アルゴリズムが有効になっている **DEFAULT** ポリシー。

### LEGACY:AD-SUPPORT

Active Directory サービスの相互運用性を向上させる、セキュリティの低い設定を含む **LEGACY** ポリシー。

### FIPS:OSPP

Common Criteria for Information Technology Security Evaluation 標準によって要求される追加の制限を含む **FIPS** ポリシー。



#### 警告

システム全体のサブポリシー **FIPS:OSPP** には、Common Criteria (CC) 認定に必要な暗号化アルゴリズムに関する追加の制限が含まれています。そのため、このサブポリシーを設定すると、システムの相互運用性が低下します。たとえば、3072 ビットより短い RSA 鍵と DH 鍵、追加の SSH アルゴリズム、および複数の TLS グループを使用できません。また、**FIPS:OSPP** を設定すると、Red Hat コンテンツ配信ネットワーク (CDN) 構造への接続が防止されます。さらに、**FIPS:OSPP** を使用する IdM デプロイメントには Active Directory (AD) を統合できません。**FIPS:OSPP** を使用する RHEL ホストと AD ドメイン間の通信が機能しないか、一部の AD アカウントが認証できない可能性があります。

**FIPS:OSPP** 暗号化サブポリシーを設定すると、システムが **CC 非準拠** になることに注意してください。RHEL システムを CC 標準に準拠させる唯一の正しい方法は、**cc-config** パッケージをインストールすることです。認定済みの RHEL バージョン、検証レポート、および [National Information Assurance Partnership \(NIAP\)](#) で提供されている CC ガイドへのリンクのリストについては、ナレッジベース記事「[Compliance Activities and Government Standards](#)」の [Common Criteria](#) セクションを参照してください。

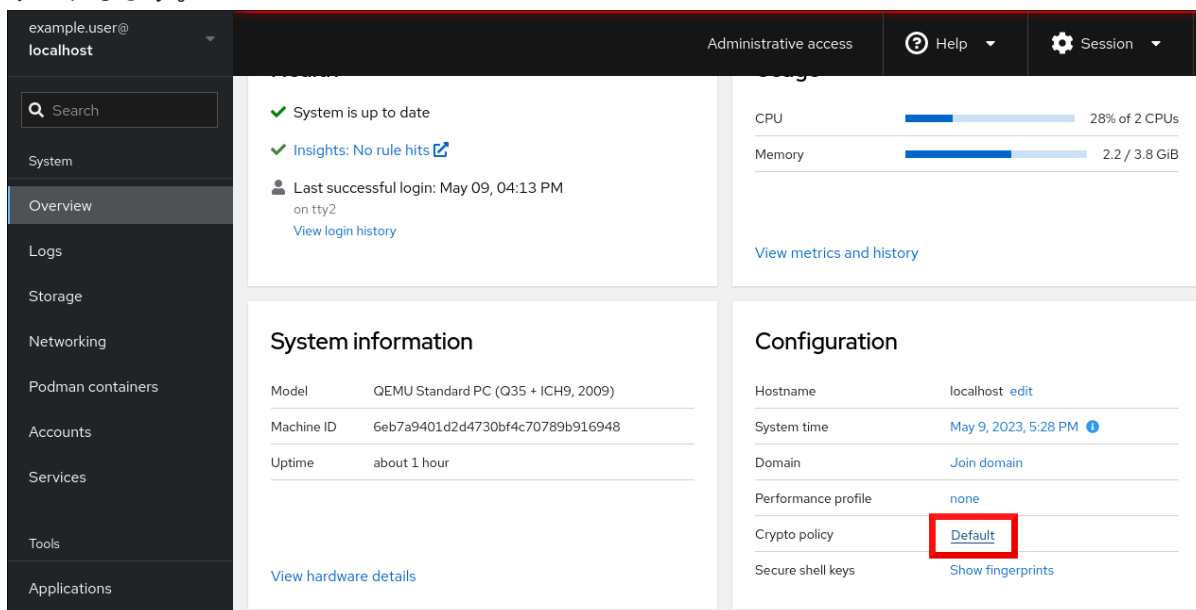
### 前提条件

- RHEL 8 Web コンソールがインストールされている。詳細は、[Web コンソールのインストールおよび有効化](#) を参照してください。
- **sudo** を使用して管理コマンドを入力するための **root** 権限または権限がある。

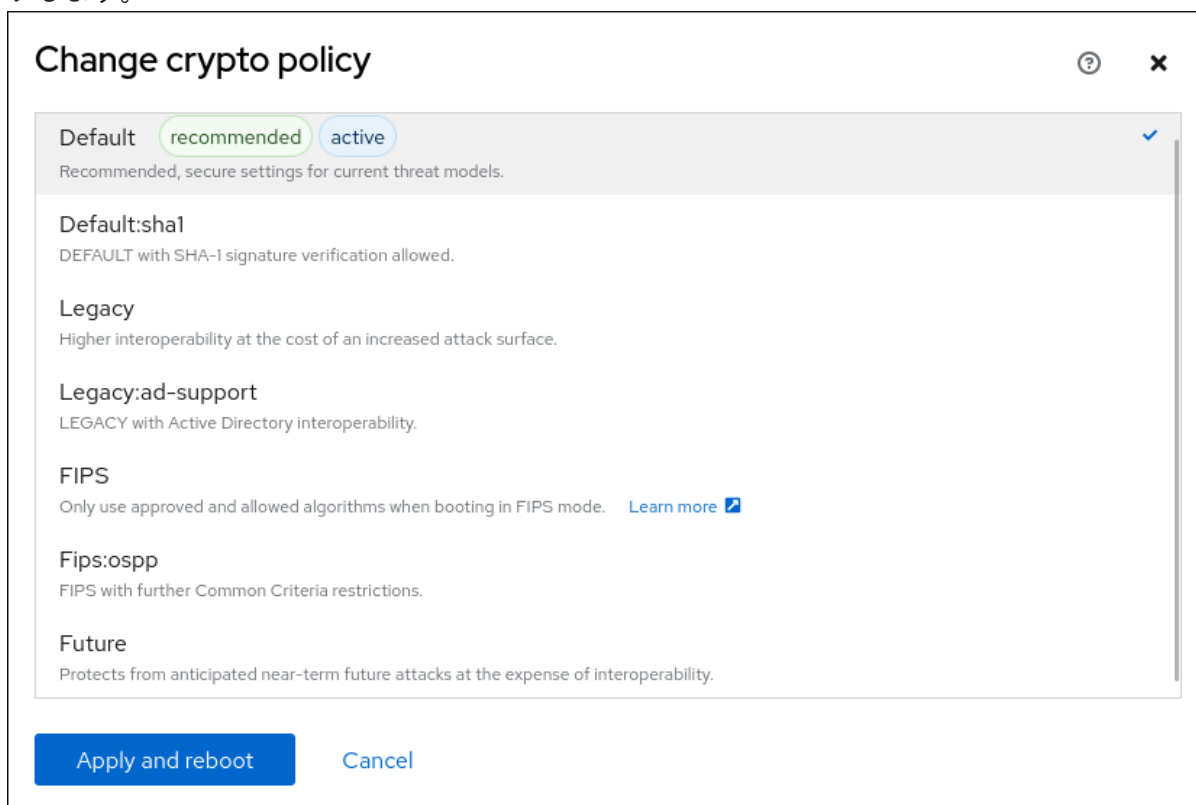
### 手順

1. Web コンソールにログインします。詳細は、[Web コンソールへのログイン](#) を参照してください。

2. Overview ページの Configuration カードで、Crypto policy の横にある現在のポリシー値をクリックします。



3. Change crypto policy ダイアログウィンドウで、システムで使用を開始するポリシーをクリックします。



4. Apply and reboot ボタンをクリックします。

## 検証

- 再起動後、Web コンソールに再度ログインし、暗号化ポリシー の値が選択したものと一致していることを確認します。あるいは、`update-crypto-policies --show` コマンドを入力して、現在のシステム全体の暗号化ポリシーをターミナルに表示することもできます。

## 関連情報

- 各暗号化ポリシーの詳細は、セキュリティー強化ドキュメントの [システム全体の暗号化ポリシー](#) セクションを参照してください。

## 第15章 WEB コンソールで SELINUX 設定の ANSIBLE PLAYBOOK の作成

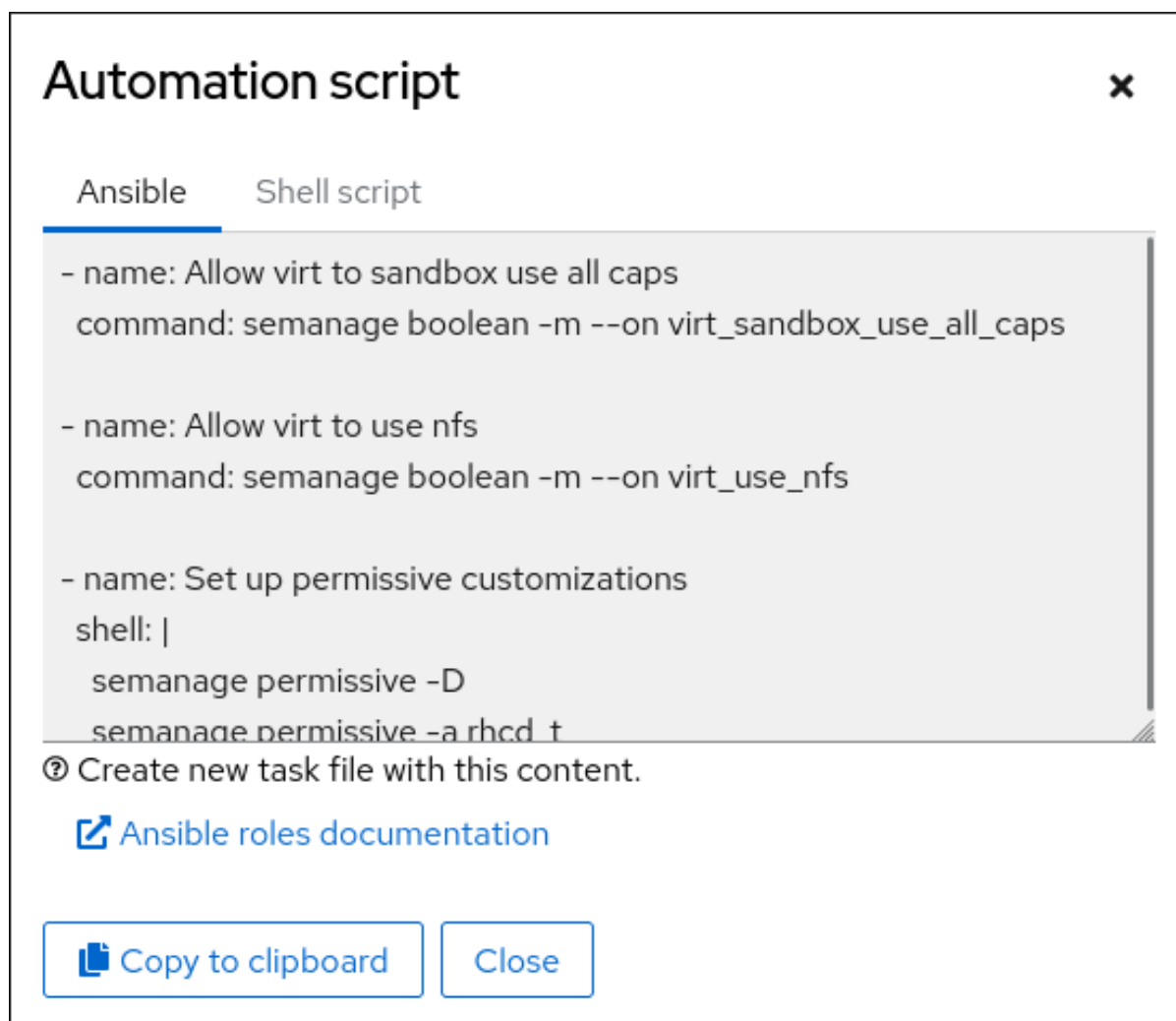
Web コンソールでは、SELinux 設定のシェルスクリプトまたは Ansible Playbook を生成できます。Ansible Playbook の場合、複数のシステムに設定を簡単に適用できます。

### 前提条件

- Web コンソールがインストールされており、アクセス可能である。  
詳細は、[Web コンソールのインストール](#) を参照してください。

### 手順

1. SELinux をクリックします。
2. **View the automation script** をクリックします。  
生成されたスクリプトを含むウィンドウが開きます。シェルスクリプトと Ansible Playbook の生成オプションタブ間を移動できます。



3. **Copy to clipboard** ボタンをクリックし、スクリプトまたは Playbook を選択して適用します。

これにより、他のマシンに適用できる自動スクリプトがあります。

### 関連情報

- [SELinux 関連の問題のトラブルシューティング](#)
- [複数のシステムへの同じ SELinux 設定のデプロイメント](#)
- **ansible-playbook(1)** の man ページ

## 第16章 WEB コンソールでパーティションの管理

Web コンソールを使用して、RHEL 8 でファイルシステムを管理する方法を説明します。

利用可能なファイルシステムの詳細は、[利用可能なファイルシステムの概要](#) を参照してください。

### 16.1. ファイルシステムでフォーマットされたパーティションを WEB コンソールに表示

Web コンソールの **ストレージ** セクションには、**ファイルシステム** テーブルで使用可能なファイルシステムがすべて表示されます。

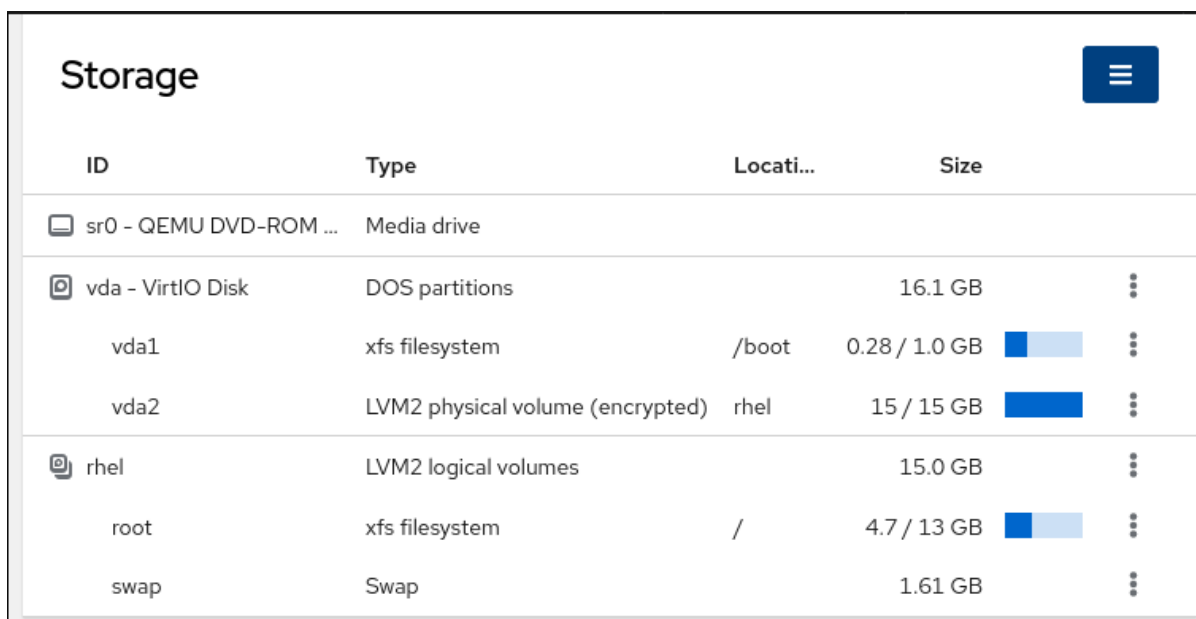
ファイルシステムでフォーマットされたパーティションのリストに加えて、新しいストレージを作成するためのページも使用できます。

#### 前提条件

- **cockpit-storaged** パッケージがシステムにインストールされている。
- Web コンソールがインストールされており、アクセス可能である。詳細は、[Web コンソールのインストール](#) を参照してください。

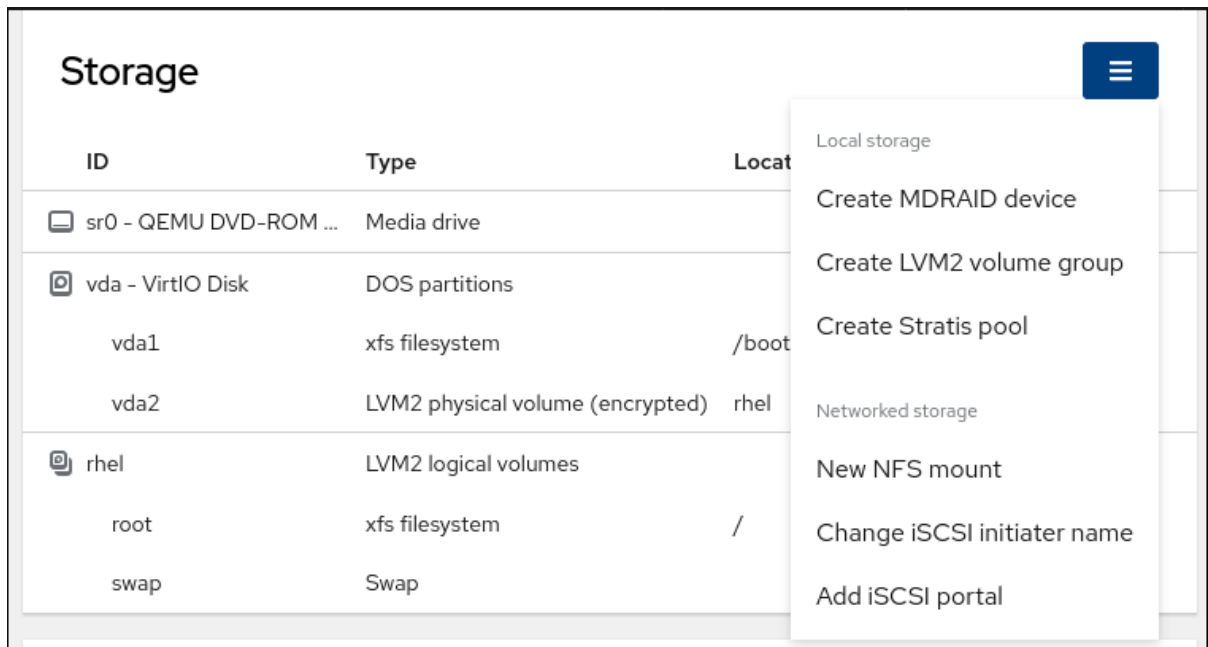
#### 手順

1. RHEL 8 Web コンソールにログインします。詳細は、[Web コンソールへのログイン](#) を参照してください。
2. **Storage** タブをクリックします。  
**ストレージ** テーブルでは、ファイルシステムでフォーマットされたすべての使用可能なパーティション、それらの ID、タイプ、場所、サイズ、および各パーティションで使用可能な容量を確認できます。



| ID                     | Type                             | Locati... | Size          |
|------------------------|----------------------------------|-----------|---------------|
| sr0 - QEMU DVD-ROM ... | Media drive                      |           |               |
| vda - VirtIO Disk      | DOS partitions                   |           | 16.1 GB       |
| vda1                   | xfs filesystem                   | /boot     | 0.28 / 1.0 GB |
| vda2                   | LVM2 physical volume (encrypted) | rhel      | 15 / 15 GB    |
| rhel                   | LVM2 logical volumes             |           | 15.0 GB       |
| root                   | xfs filesystem                   | /         | 4.7 / 13 GB   |
| swap                   | Swap                             |           | 1.61 GB       |

右上隅のドロップダウンメニューを使用して、新しいローカルストレージまたはネットワークストレージを作成することもできます。



## 16.2. WEB コンソールでパーティションの作成

新しいパーティションを作成するには、以下を行います。

- 既存のパーティションテーブルを使用する
- パーティションを作成する

### 前提条件

- **cockpit-storaged** パッケージがシステムにインストールされている。
- Web コンソールがインストールされており、アクセス可能である。詳細は、[Web コンソールのインストール](#) を参照してください。
- システムに接続されたフォーマットされていないボリュームは、**Storage** タブの **Storage** テーブルに表示されます。

### 手順

1. RHEL Web コンソールにログインします。詳細は、[Web コンソールへのログイン](#) を参照してください。
2. **Storage** タブをクリックします。
3. **Storage** テーブルで、パーティションを分割するデバイスをクリックして、そのデバイスのページとオプションを開きます。
4. デバイスページで、メニューボタン **⋮** をクリックし、**Create partition table** を選択します。
5. **Initialize disk** ダイアログボックスで、以下を選択します。
  - a. **パーティション設定:**
    - すべてのシステムおよびデバイスと互換性あり (MBR)
    - 最新のシステムおよび 2TB (GPT) 以上のハードディスクと互換性あり



- パーティションなし

b. オーバーライト:

- RHEL Web コンソールでディスク全体をゼロで書き換える場合は、**Overwrite existing data with zeros** チェックボックスをオンにします。このプログラムはディスク全体を調べるため、このオプションを使用すると遅くなりますが、安全性は高まります。ディスクにデータが含まれていて、上書きする必要がある場合は、このオプションを使用します。

**Overwrite existing data with zeros** チェックボックスを選択しない場合、RHEL Web コンソールはディスクヘッダーのみを書き換えます。これにより、フォーマットの速度が向上します。

6. **Initialize** をクリックします。
7. 作成したパーティションテーブルの横にあるメニューボタン **⋮** をクリックします。デフォルトでは **Free space** という名前が付けられます。
8. **Create Partition** をクリックします。
9. **Create partition** ダイアログボックスで、ファイルシステムの **Name** を入力します。
10. **Mount point** を追加します。
11. **Type** ドロップダウンメニューで、ファイルシステムを選択します。
  - **XFS** ファイルシステムは大規模な論理ボリュームをサポートし、オンラインの物理ドライブを停止せずに、既存のファイルシステムの拡大および縮小を行うことができます。別のストレージの使用を希望しない場合は、このファイルシステムを選択したままにしてください。
  - **ext4** ファイルシステムは以下に対応します。
    - 論理ボリューム
    - オンラインの物理ドライブを停止せずに切り替え
    - ファイルシステムの拡張
    - ファイルシステムの縮小

追加オプションは、LUKS (Linux Unified Key Setup) によって行われるパーティションの暗号化を有効にすることです。これにより、パスワードでボリュームを暗号化できます。

12. 作成するボリュームの **Size** を入力します。
13. RHEL Web コンソールでディスク全体をゼロで書き換える場合は、**Overwrite existing data with zeros** チェックボックスをオンにします。このプログラムはディスク全体を調べるため、このオプションを使用すると遅くなりますが、安全性は高まります。ディスクにデータが含まれていて、上書きする必要がある場合は、このオプションを使用します。

**Overwrite existing data with zeros** チェックボックスを選択しない場合、RHEL Web コンソールはディスクヘッダーのみを書き換えます。これにより、フォーマットの速度が向上します。
14. ボリュームを暗号化する場合は、**Encryption** ドロップダウンメニューで暗号化の種類を選択します。

ボリュームを暗号化しない場合は、**No encryption** を選択します。
15. **At boot** ドロップダウンメニューで、ボリュームをマウントするタイミングを選択します。

## 16. Mount options セクションで:

- a. ボリュームを読み取り専用論理ボリュームとしてマウントする場合は、**Mount read only** チェックボックスをオンにします。
- b. デフォルトのマウントオプションを変更する場合は、**Custom mount options** チェックボックスをオンにしてマウントオプションを追加します。

## 17. パーティションを作成します。

- パーティションを作成してマウントする場合は、**Create and mount** ボタンをクリックします。
- パーティションのみを作成する場合は、**Create only** ボタンをクリックします。ボリュームのサイズや、選択するオプションによって、フォーマットに数分かかることがあります。

### 検証手順

- パーティションが正常に追加されたことを確認するには、**Storage** タブに切り替えて **Storage** テーブルを確認し、新しいパーティションがリストされているかどうかを確認します。

## 16.3. WEB コンソールでパーティションの削除

Web コンソールインターフェイスでパーティションを削除できます。

### 前提条件

- **cockpit-storaged** パッケージがシステムにインストールされている。
- Web コンソールがインストールされており、アクセス可能である。詳細は、[Web コンソールのインストール](#) を参照してください。

### 手順

1. RHEL Web コンソールにログインします。詳細は、[Web コンソールへのログイン](#) を参照してください。
2. **Storage** タブをクリックします。
3. パーティションを削除するデバイスをクリックします。
4. デバイスページの **GPT partitions** セクションで、削除するパーティションの横にあるメニューボタン **⋮** をクリックします。
5. ドロップダウンメニューから **Delete** を選択します。  
RHEL Web コンソールは、パーティションを削除する前に、現在パーティションを使用しているすべてのプロセスを終了し、パーティションをアンマウントします。

### 検証手順

- パーティションが正常に削除されたことを確認するには、**ストレージ** タブに切り替えて、**コンテンツ** テーブルを確認します。

## 16.4. WEB コンソールでのファイルシステムのマウントとマウント解除

RHEL システムでパーティションを使用できるようにするには、パーティションにファイルシステムをデバイスとしてマウントする必要があります。



### 注記

ファイルシステムのマウントを解除することもできます。アンマウントすると RHEL システムはその使用を停止します。ファイルシステムのマウントを解除すると、デバイスを削除 (delete または remove) または再読み込みできるようになります。

### 前提条件

- **cockpit-storaged** パッケージがシステムにインストールされている。
- Web コンソールがインストールされており、アクセス可能である。詳細は、[Web コンソールのインストール](#) を参照してください。
- ファイルシステムのマウントを解除する場合は、システムがパーティションに保存されているファイル、サービス、またはアプリケーションを使用しないようにする。

### 手順

1. RHEL Web コンソールにログインします。詳細は、[Web コンソールへのログイン](#) を参照してください。
2. **Storage** タブをクリックします。
3. **Storage** テーブルで、パーティションを削除するボリュームを選択します。
4. **GPT partitions** セクションで、ファイルシステムをマウントまたはマウント解除するパーティションの横にあるメニューボタン **⋮** をクリックします。
5. **Mount** または **Unmount** をクリックします。

## 第17章 WEB コンソールで NFS マウントの管理

RHEL 8 Web コンソールを使用すると、ネットワークファイルシステム (NFS) プロトコルを使用して、リモートディレクトリーをマウントできます。

NFS を使用すると、ネットワークに置かれたリモートディレクトリーに到達してマウントし、ディレクトリーが物理ドライブに置かれているかのようにファイルを操作できます。

### 前提条件

- RHEL 8 Web コンソールがインストールされている。  
詳細は、[Web コンソールのインストールおよび有効化](#) を参照してください。
- **cockpit-storaged** パッケージがシステムにインストールされている。
- NFS サーバー名または IP アドレス
- リモートサーバーのディレクトリーのパス

### 17.1. WEB コンソールで NFS マウントの接続

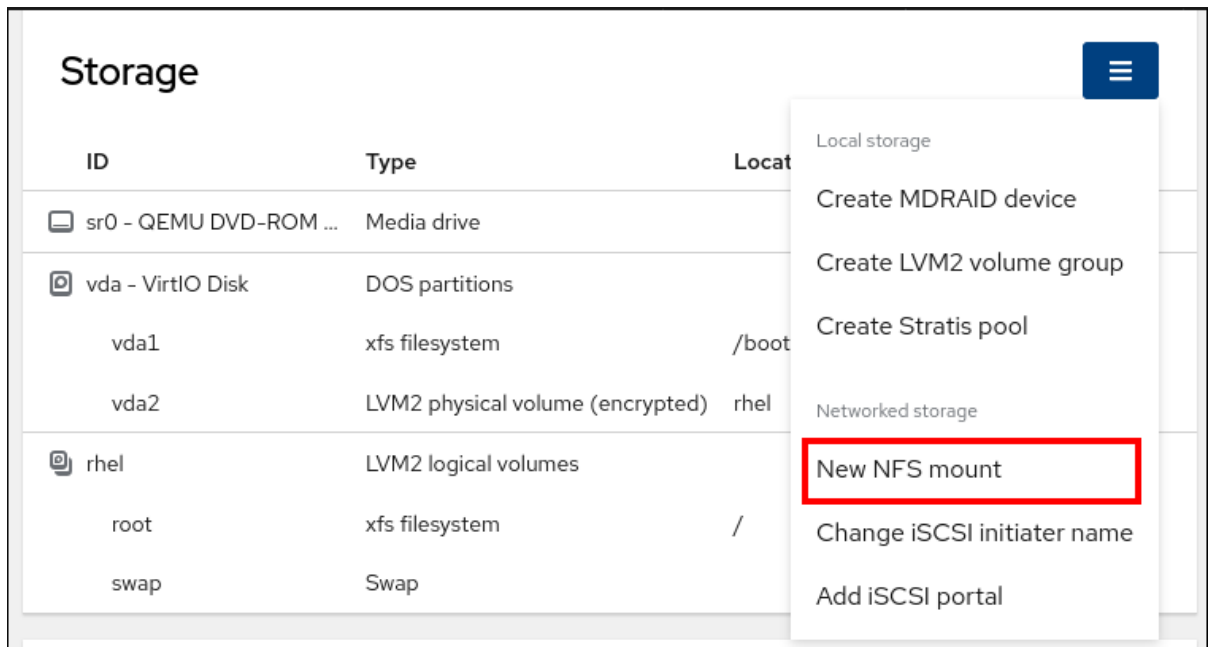
NFS を使用して、リモートディレクトリーをファイルシステムに接続します。

#### 前提条件

- NFS サーバー名または IP アドレス。
- リモートサーバーのディレクトリーのパス

#### 手順

1. RHEL 8 Web コンソールにログインします。詳細は、[Web コンソールへのログイン](#) を参照してください。
2. **Storage** をクリックします。
3. **Storage** テーブルで、メニューボタンをクリックします。
4. ドロップダウンメニューから、**New NFS mount** を選択します。



5. **NFSの新規マウント** ダイアログボックスに、リモートサーバーのサーバー名または IP アドレスを入力します。
6. **サーバーのパス** フィールドに、マウントするディレクトリーのパスを入力します。
7. **Local Mount Point** フィールドに、NFS をマウントするローカルシステム上のディレクトリーへのパスを入力します。
8. **Mount options** チェックボックスリストで、NFS をマウントする方法を選択します。要件に応じて複数のオプションを選択できます。
  - ローカルシステムを再起動した後もディレクトリーにアクセスできるようにするには、**Mount at boot** をオンにします。
  - NFS の内容を変更したくない場合は、**Mount read only** ボックスをオンにします。
  - デフォルトのマウントオプションを変更する場合は、**Custom mount options** ボックスをオンにしてマウントオプションを追加します。詳細は、[Web コンソールでの NFS マウントオプションのカスタマイズ](#) を参照してください。

### New NFS mount

**Server address**

**Path on server**

**Local mount point**

**Mount options**

- Mount at boot
- Mount read only
- Custom mount options

9. **Add** をクリックします。

- マウントしたディレクトリーを開き、コンテンツがアクセスできることを確認します。

## 17.2. WEB コンソールで NFS マウントオプションのカスタマイズ

既存の NFS マウントを編集し、カスタムのマウントオプションを追加します。

カスタムのマウントオプションは、タイムアウトの制限を変更したり、認証を設定するなどの NFS マウントの接続をトラブルシュートしてパラメーターを変更するのに役に立ちます。

### 前提条件

- NFS マウントがシステムに追加されている。

### 手順

1. RHEL 8 Web コンソールにログインします。詳細は、[Web コンソールへのログイン](#) を参照してください。
2. **Storage** をクリックします。
3. **Storage** テーブルで、調整する NFS マウントをクリックします。
4. リモートディレクトリーをマウントしている場合は、**アンマウント** をクリックします。カスタムマウントオプションの設定中にディレクトリーをアンマウントする必要があります。そうしないと、Web コンソールは設定を保存せず、エラーが発生します。
5. **Edit** をクリックします。
6. **NFS マウント** ダイアログボックスで、**カスタムのマウントオプション** を選択します。
7. マウントオプションを、コンマで区切って入力します。以下に例を示します。
  - **nfsvers=4** - NFS プロトコルのバージョン番号
  - NFS 要求のタイムアウト後に復元する種類
  - **sec=krb5** - NFS サーバーのファイルが、Kerberos 認証により保護されます。NFS のクライアントとサーバーの両方で Kerberos 認証に対応する必要があります。

NFS マウントオプションのリストは、コマンドラインで **man nfs** を実行します。

8. **Apply** をクリックします。
9. **Mount** をクリックします。

### 検証手順

- マウントしたディレクトリーを開き、コンテンツがアクセスできることを確認します。

## 第18章 WEB コンソールで RAID の管理

RAID (Redundant Arrays of Independent Disks) は、パフォーマンスと冗長性を目的として、複数のディスクを1つのストレージに配置する方法を表します。

RAID は、次のデータ配信ストラテジーを使用します。

- ミラーリング - データは、2つの異なる場所にコピーします。片方のディスクに障害が発生しても、コピーがあるため、データが失われることはありません。
- ストライピング - データが均等に分散されています。

保護レベルは、RAID レベルにより異なります。

RHEL Web コンソールは、次の RAID レベルに対応します。

- RAID 0 (ストライプ)
- RAID 1 (ミラー)
- RAID 4 (専用パリティ)
- RAID 5 (分散パリティ)
- RAID 6 (ダブル分散パリティ)
- RAID 10 (ミラーのストライプ)

RAID でディスクを使用する前に、次の操作を行う必要があります。

- RAID を作成します。
- ファイルシステムでフォーマットします。
- RAID をシステムにマウントします。

### 前提条件

- RHEL 8 Web コンソールをインストールし、アクセスできる。詳細は、[Web コンソールのインストールおよび有効化](#) を参照してください。
- **cockpit-storaged** パッケージがシステムにインストールされている。

## 18.1. WEB コンソールで RAID の作成

RHEL 8 Web コンソールで RAID を設定します。

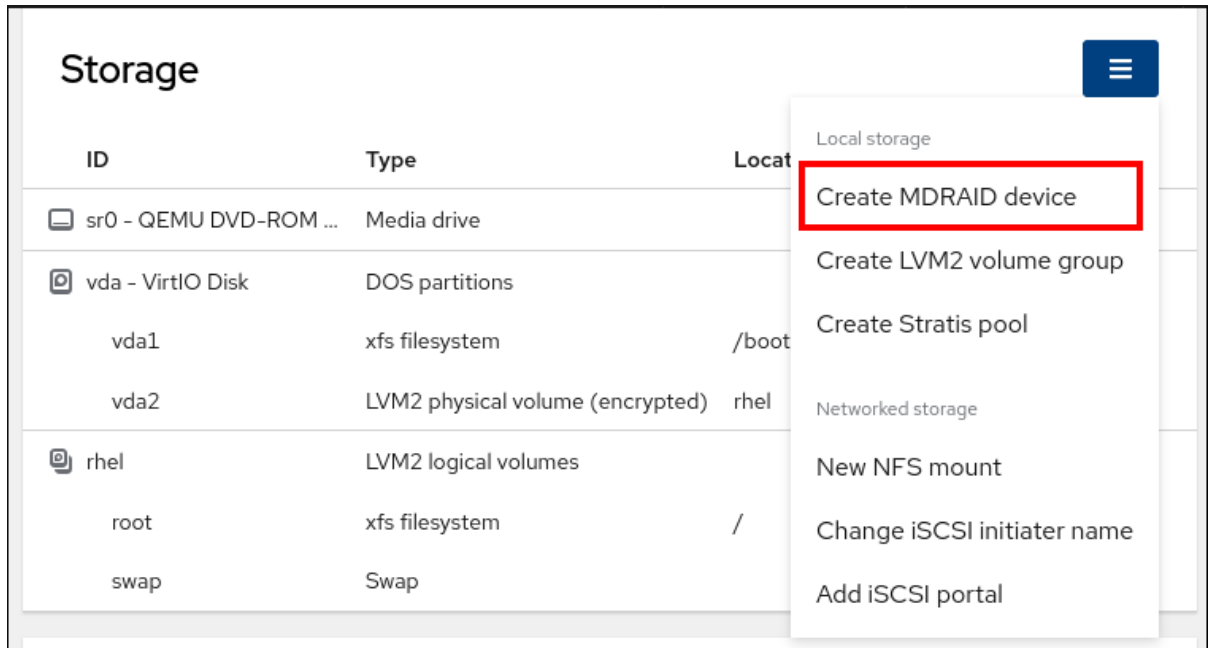
### 前提条件

- システムに接続している物理ディスク。各 RAID レベルに必要なディスク容量は異なります。

### 手順

1. RHEL 8 Web コンソールを開きます。
2. **Storage** をクリックします。

3. **Storage** テーブルで、メニューボタンをクリックします。
4. ドロップダウンメニューから、**Create MDRAID device** を選択します。



5. **RAID デバイスの作成** ダイアログボックスで、新しい RAID の名前を入力します。
6. **RAID レベル** ドロップダウンリストで、使用する RAID レベルを選択します。
7. **Chunk Size** ドロップダウンリストから、使用可能なオプションのリストからサイズを選択します。  
**Chunk Size** の値は、データ書き込み用の各ブロックの大きさを指定します。たとえば、チャンクサイズが 512 KiB の場合、システムは最初の 512 KiB を最初のディスクに書き込み、次の 512 KiB を次のディスクに書き込み、その次の 512 KiB をその次のディスクに書き込みます。RAID に 3 つのディスクがある場合は、4 つ目の 512 KiB が最初のディスクに再度書き込まれます。
8. RAID に使用するディスクを選択します。
9. **Create** をクリックします。

### 検証手順

- **ストレージ** セクションに移動し、**RAID デバイス** ボックスに新しい RAID が表示されることを確認します。  
Web コンソールで新しい RAID をフォーマットしてマウントするには、次のオプションがあります。
  - [RAID のフォーマット](#)
  - [パーティションテーブルへのパーティションの作成](#)
  - [RAID へのボリュームグループの作成](#)

## 18.2. WEB コンソールで RAID のフォーマット

RHEL 9 Web コンソールでソフトウェア RAID デバイスをフォーマットおよびマウントできます。

### 前提条件



- 物理ディスクが接続され、RHEL 8 から確認できる。
- RAID が追加されている。
- RAID に使用するファイルシステムを検討します。
- パーティションテーブルの作成を検討する。

## 手順

1. RHEL 8 Web コンソールを開きます。
2. **Storage** をクリックします。
3. **ストレージ** テーブルで、フォーマットする RAID デバイスの横にあるメニューボタン **⋮** をクリックします。
4. ドロップダウンメニューから **Format** を選択します。
5. **Format** ダイアログボックスに名前を入力します。
6. **マウントポイント** フィールドに、マウントパスを追加します。
7. **Type** ドロップダウンリストから、ファイルシステムのタイプを選択します。
8. RHEL Web コンソールでディスク全体をゼロで書き換える場合は、**Overwrite existing data with zeros** チェックボックスをオンにします。このプログラムはディスク全体を調べるため、このオプションを使用すると遅くなりますが、安全性は高まります。ディスクにデータが含まれていて、上書きする必要がある場合は、このオプションを使用します。  
**Overwrite existing data with zeros** チェックボックスを選択しない場合、RHEL Web コンソールはディスクヘッダーのみを書き換えます。これにより、フォーマットの速度が向上します。
9. ボリュームを暗号化する場合は、**Encryption** ドロップダウンメニューから暗号化の種類を選択します。  
ボリュームを暗号化しない場合は、**No encryption** を選択します。
10. **At boot** ドロップダウンメニューで、ボリュームをマウントするタイミングを選択します。
11. **Mount options** セクションで:
  - a. ボリュームを読み取り専用論理ボリュームとしてマウントする場合は、**Mount read only** チェックボックスをオンにします。
  - b. デフォルトのマウントオプションを変更する場合は、**Custom mount options** チェックボックスをオンにしてマウントオプションを追加します。詳細は、[Web コンソールでの NFS マウントオプションのカスタマイズ](#) を参照してください。
12. RAID パーティションをフォーマットします。
  - パーティションをフォーマットしてマウントする場合は、**Format and mount** ボタンをクリックします。
  - パーティションのみをフォーマットする場合は、**Format only** ボタンをクリックします。ボリュームのサイズや、選択するオプションによって、フォーマットに数分かかることがあります。

## 検証

- フォーマットが正常に完了すると、**Storage** ページの **Storage** テーブルでフォーマットされた論理ボリュームの詳細を確認できます。

### 18.3. WEB コンソールを使用した RAID 上のパーティションテーブルの作成

RHEL 8 インターフェイスに作成した新しいソフトウェア RAID デバイスで、パーティションテーブルを有する RAID をフォーマットします。

RAID は、その他のストレージデバイスとしてフォーマットする必要があります。2つのオプションがあります。

- パーティションを使用せずに RAID デバイスをフォーマットする
- パーティションを有するパーティションテーブルを作成する

#### 前提条件

- 物理ディスクが接続され、確認できる。
- RAID が追加されている。
- RAID に使用するファイルシステムを検討する。
- パーティションテーブルの作成を検討する。

#### 手順

1. RHEL 8 のコンソールを開きます。
2. **Storage** をクリックします。
3. **Storage** テーブルで、パーティションテーブルを作成する RAID デバイスをクリックします。
4. **MDRAID device** セクションのメニューボタン **⋮** をクリックします。
5. ドロップダウンメニューから、**Create partition table** を選択します。
6. **Initialize disk** ダイアログボックスで、以下を選択します。
  - a. **パーティション設定:**
    - すべてのシステムおよびデバイスと互換性あり (MBR)
    - 最新のシステムおよび 2TB (GPT) 以上のハードディスクと互換性あり
    - パーティションなし
  - b. **オーバーライト:**
    - RHEL Web コンソールでディスク全体をゼロで書き換える場合は、**Overwrite existing data with zeros** チェックボックスをオンにします。このプログラムはディスク全体を調べるため、このオプションを使用すると遅くなりますが、安全性は高まります。ディスクにデータが含まれていて、上書きする場合は、このオプションを使用します。**Overwrite existing data with zeros** チェックボックスを選択しない場合、RHEL Web コンソールはディスクヘッダーのみを書き換えます。これにより、フォーマットの速度が向上します。

#### 7. **Initialize** をクリックします。

パーティションテーブルが作成され、そのテーブル上にパーティションを作成できるようになりました。詳細は、[Web コンソールを使用した RAID 上のパーティションの作成](#) を参照してください。

## 18.4. WEB コンソールを使用した RAID 上のパーティションの作成

既存のパーティションテーブルにパーティションを作成します。

### 前提条件

- パーティションテーブルが作成されている。詳細については、[Web コンソールを使用した RAID 上のパーティションテーブルの作成](#) を参照してください。

### 手順

1. RHEL 8 Web コンソールを開きます。
2. **Storage** をクリックします。
3. **Storage** テーブルで、パーティションを作成する RAID デバイスをクリックします。
4. RAID デバイスページで、**GPT partitions** セクションまでスクロールし、作成したパーティションテーブルの横にあるメニューボタン **⋮** をクリックします。デフォルトでは **Free space** という名前が付けられます。
5. **Create Partition** をクリックします。
6. **Create partition** ダイアログボックスで、ファイルシステムの名前を入力します。名前にスペースは使用しないでください。
7. **マウントポイント** フィールドに、マウントパスを追加します。
8. **Type** ドロップダウンリストで、ファイルシステムのタイプを選択します。
9. **Size** フィールドで、パーティションのサイズを設定します。
10. RHEL Web コンソールでディスク全体をゼロで書き換える場合は、**Overwrite existing data with zeros** チェックボックスをオンにします。このプログラムはディスク全体を調べるため、このオプションを使用すると遅くなりますが、安全性は高まります。ディスクにデータが含まれていて、上書きする場合は、このオプションを使用します。  
**Overwrite existing data with zeros** チェックボックスを選択しない場合、RHEL Web コンソールはディスクヘッダーのみを書き換えます。これにより、フォーマットの速度が向上します。
11. ボリュームを暗号化する場合は、**Encryption** ドロップダウンメニューで暗号化の種類を選択します。  
ボリュームを暗号化しない場合は、**No encryption** を選択します。
12. **At boot** ドロップダウンメニューで、ボリュームをマウントするタイミングを選択します。
13. **Mount options** セクションで:
  - a. ボリュームを読み取り専用論理ボリュームとしてマウントする場合は、**Mount read only** チェックボックスをオンにします。

- b. デフォルトのマウントオプションを変更する場合は、**Custom mount options** チェックボックスをオンにしてマウントオプションを追加します。

14. パーティションを作成します。

- パーティションを作成してマウントする場合は、**Create and mount** ボタンをクリックします。
- パーティションのみを作成する場合は、**Create only** ボタンをクリックします。  
ボリュームのサイズや、選択するオプションによって、フォーマットに数分かかることがあります。

パーティションを作成した後、さらにパーティションを作成できます。

この時点で、システムが、マウントされてフォーマットされた RAID を使用します。

#### 検証

- フォーマットされた論理ボリュームの詳細は、メインストレージページの **Storage** テーブルで確認できます。

## 18.5. WEB コンソールを使用した RAID 上のボリュームグループの作成

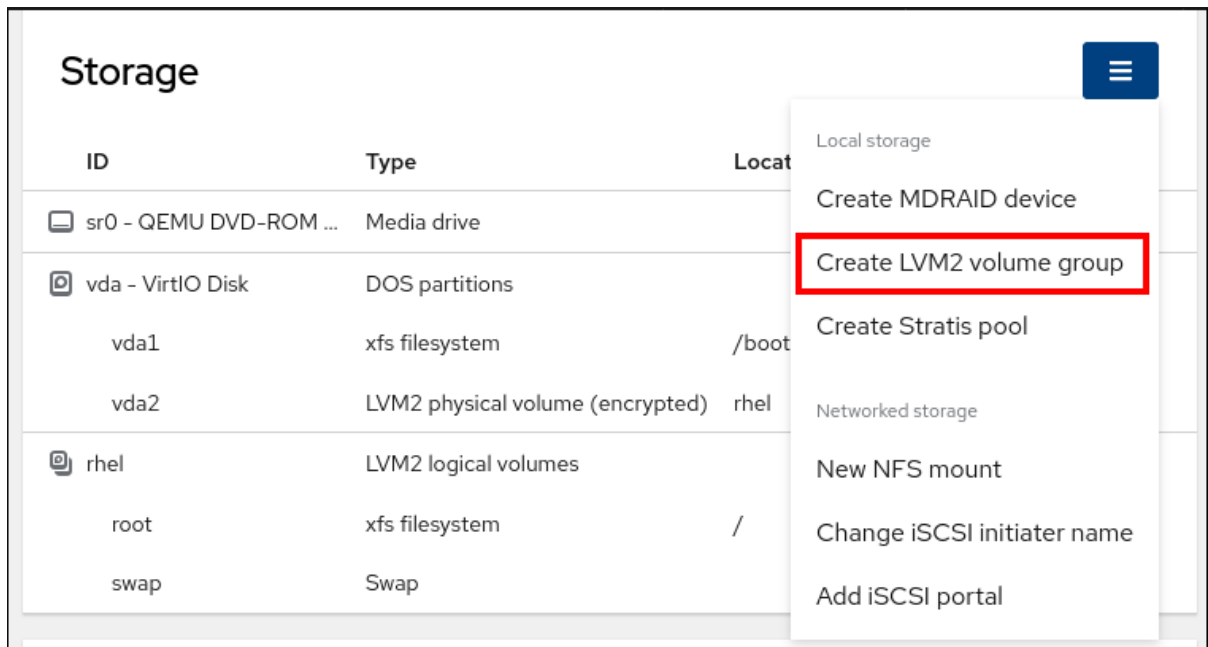
ソフトウェア RAID からボリュームグループを構築

#### 前提条件

- フォーマットされておらず、マウントされていない RAID デバイス。

#### 手順

1. RHEL 8 Web コンソールを開きます。
2. **Storage** をクリックします。
3. **Storage** テーブルで、メニューボタンをクリックします。
4. ドロップダウンメニューから、**Create LVM2 volume group** を選択します。



5. **Create LVM2 volume group** ダイアログボックスで、新しいボリュームグループの名前を入力します。
6. **Disks** リストで、RAID デバイスを選択します。  
リストに RAID が表示されない場合は、システムから RAID のマウントを解除します。RAID デバイスは RHEL 9 システムで使用されていない必要があります。
7. **Create** をクリックします。

## 18.6. 関連情報

- ソフト破損と、RAID LV の設定時にデータを保護する方法の詳細は、[DM 整合性を使用した RAID LV の作成](#) を参照してください。

## 第19章 WEB コンソールを使用した LVM 論理ボリュームの設定

Red Hat Enterprise Linux 9 は論理ボリューム管理 (LVM) をサポートしています。RHEL 9 インストーラーは、インストールプロセス中に LVM2 ボリュームグループを自動的に作成し、その上にシステムをインストールします。

次の LVM2 グループの例のページに示すように、RHEL Web コンソールを使用して LVM2 ボリュームグループとボリュームを管理できます。

The screenshot displays the 'LVM2 volume group' interface. At the top, there is a title 'LVM2 volume group' and a button 'Add physical volume'. Below this, the group's details are listed: Name 'rhel' with an 'edit' link, UUID 'qlbGga-4x8l-ggOi-n3jy-SfFa-uWeV-dD5MAr', and Capacity '15.0 GB, 14.0 GiB, 15011414016 bytes'. Under the 'Physical volumes' section, a single volume 'vda2' is shown as a 'Partition (encrypted) - VirtIO Disk' with a capacity of '15 / 15 GB' and a progress bar. Below this is the 'LVM2 logical volumes' section with a 'Create new logical volume' button. A table lists the logical volumes:

| ID   | Type           | Location | Size        |
|------|----------------|----------|-------------|
| root | xfv filesystem | /        | 4.7 / 13 GB |
| swap | Swap           |          | 1.61 GB     |

### 前提条件

- RHEL 8 Web コンソールがインストールされている。  
手順は、[Installing and enabling the web console](#) を参照してください。
- **cockpit-storaged** パッケージがシステムにインストールされている。
- 物理ドライブ、RAID デバイス、または論理ボリュームを作成できるその他のブロックデバイスの種類。

### 19.1. WEB コンソールの論理ボリュームマネージャー

RHEL 8 Web コンソールは、LVM ボリュームグループおよび論理ボリュームを作成するグラフィカルインターフェイスを提供します。

ボリュームグループは、物理ボリュームと論理ボリュームとの間に層を作成します。このレイヤーでは、論理ボリューム自体に影響を与えずに物理ボリュームの追加または削除が可能になります。ボリュームグループは、そのグループに含まれるすべての物理ドライブの容量を、1つのドライブの容量として表示します。Web コンソールのボリュームグループに物理ドライブを参加させることができます。

論理ボリュームの主な利点は以下ようになります。

- 物理ドライブに使用されるパーティションシステムよりも優れた柔軟性
- 複数の物理ドライブを1つのボリュームに接続する機能
- 再起動せずに、オンラインボリュームの容量を拡張 (拡大) または減少 (縮小) する可能性
- スナップショットを作成する機能

## 関連情報

- [論理ボリュームの設定および管理](#)

## 19.2. WEB コンソールでボリュームグループの作成

1つ以上の物理ドライブまたは他のストレージデバイスからボリュームグループを作成します。

論理ボリュームは、ボリュームグループから作成されます。各ボリュームグループに、複数の論理ボリュームを追加できます。

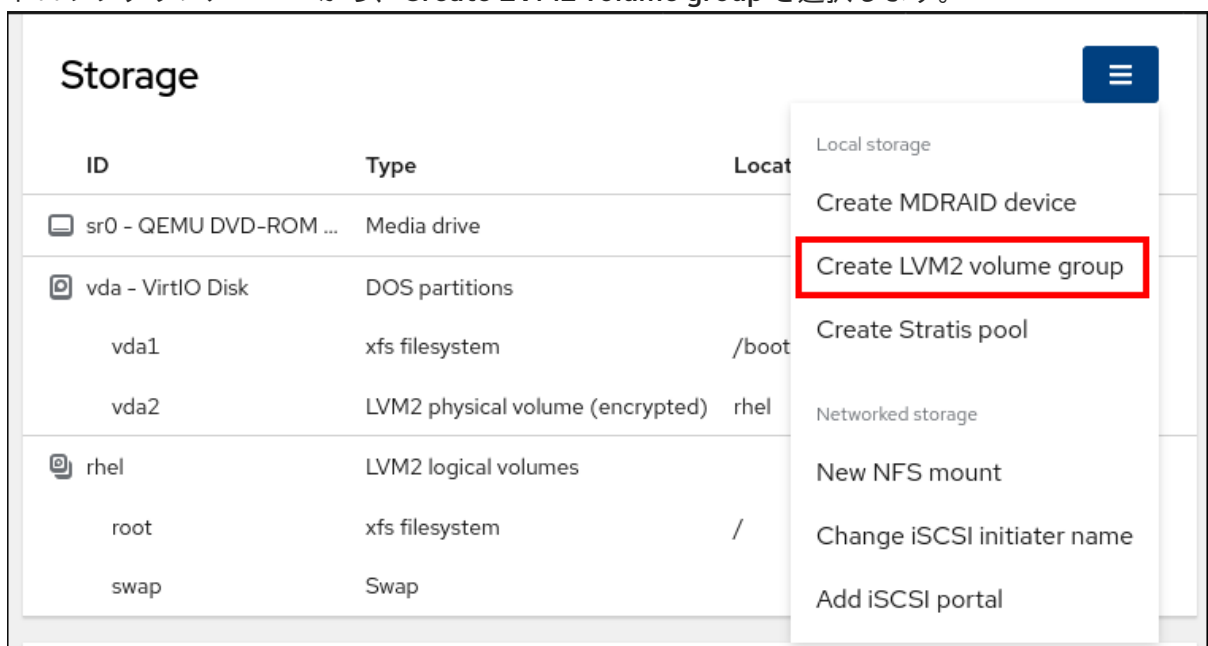
詳細は、[LVM ボリュームグループの管理](#) を参照してください。

## 前提条件

- ボリュームグループを作成する物理ドライブ、またはその他の種類のストレージデバイス。

## 手順

1. RHEL 8 Web コンソールにログインします。
2. **Storage** をクリックします。
3. **Storage** テーブルで、メニューボタンをクリックします。
4. ドロップダウンメニューから、**Create LVM2 volume group** を選択します。



5. **Name** フィールドにボリュームグループの名前を入力します。名前にスペースを含めることはできません。
6. ボリュームグループを作成するために組み合わせるドライブを選択します。

### Create volume group

**Name**

---

**Disks**

|                                     |                                 |                     |
|-------------------------------------|---------------------------------|---------------------|
| <input checked="" type="checkbox"/> | 16.0 GB RAID device raid-device | /dev/md/raid-device |
| <input checked="" type="checkbox"/> | 16.0 GB VirtIO Disk             | /dev/vdb            |

RHEL Web コンソールは、未使用のブロックデバイスのみを表示します。リストにデバイスが表示されない場合は、そのデバイスがシステムで使用されていないことを確認するか、デバイスを空で未使用の状態にフォーマットしてください。使用されるデバイスには、たとえば次のようなものがあります。

- ファイルシステムでフォーマットしたデバイス
  - 別のボリュームグループの物理ボリューム
  - 別のソフトウェアの RAID デバイスのメンバーになる物理ボリューム
7. **Create** をクリックします。  
ボリュームグループが作成されます。

#### 検証

- **Storage** ページで、新しいボリュームグループが **Storage** テーブルにリストされているかどうかを確認します。

### 19.3. WEB コンソールで論理ボリュームの作成

論理ボリュームは物理ドライブとして動作します。RHEL 8 Web コンソールを使用して、ボリュームグループに LVM 論理ボリュームを作成できます。

#### 前提条件

- **cockpit-storaged** パッケージがシステムにインストールされている。
- ボリュームグループが作成されている。詳細については、[Web コンソールでのボリュームグループの作成](#) を参照してください。

#### 手順

1. RHEL 8 Web コンソールにログインします。
2. **Storage** をクリックします。
3. **Storage** テーブルで、論理ボリュームを作成するボリュームグループをクリックします。



4. **Logical volume group** ページで、**LVM2 logical volumes** セクションまでスクロールし、**Create new logical volume** をクリックします。
5. **Name** フィールドに、新しい論理ボリュームの名前を入力します。名前にスペースを含めないでください。
6. **Purpose** ドロップダウンメニューで、**Block device for filesystems** を選択します。この設定では、ボリュームグループに含まれるすべてのドライブの容量の合計に等しい最大ボリュームサイズを持つ論理ボリュームを作成できます。

7. 論理ボリュームのサイズを定義します。以下を検討してください。
  - この論理ボリュームを使用するシステムにどのぐらいの容量が必要か
  - 作成する論理ボリュームの数

領域をすべて使用する必要はありません。必要な場合は、後で論理ボリュームを大きくすることができます。

8. **Create** をクリックします。論理ボリュームが作成されます。論理ボリュームを使用するには、ボリュームをフォーマットしてマウントする必要があります。

## 検証

- **Logical volume** ページで、**LVM2 logical volumes** セクションまでスクロールし、新しい論理ボリュームがリストされているかどうかを確認します。

The screenshot displays the LVM2 management interface. At the top, the 'LVM2 volume group' 'Test-VolGrp-0' is shown with its UUID and capacity. Below this, the 'Physical volumes' section lists 'sda' as a Kingston DT 101 II drive. The 'LVM2 logical volumes' section shows 'Test-Vol-0' as an unformatted data volume. A context menu is open over the logical volume, offering actions like 'Format', 'Shrink', 'Grow', 'Deactivate', and 'Delete'.

## 19.4. WEB コンソールで論理ボリュームのフォーマット

論理ボリュームは物理ドライブとして動作します。これらを使用するには、ファイルシステムでフォーマットする必要があります。



### 警告

論理ボリュームをフォーマットすると、ボリューム上のすべてのデータが消去されます。

選択するファイルシステムにより、論理ボリュームに使用できる設定パラメーターが決まります。たとえば、XFS ファイルシステムはボリュームの縮小をサポートしていません。詳細については、[Web コンソールでの論理ボリュームのサイズ変更](#) を参照してください。

### 前提条件

- **cockpit-storaged** パッケージがシステムにインストールされている。
- 論理ボリュームが作成されている。詳細については、[Web コンソールでの論理ボリュームの作成](#) を参照してください。
- システムに対する root アクセス権を持っている。

### 手順

1. RHEL 8 Web コンソールにログインします。

2. **Storage** をクリックします。
3. **Storage** テーブルで、論理ボリュームが作成されたボリュームグループをクリックします。
4. **Logical volume group** ページで、**LVM2 logical volumes** セクションまでスクロールします。
5. フォーマットするボリュームグループの横にあるメニューボタン **⋮** をクリックします。
6. ドロップダウンメニューから **Format** を選択します。

**LVM2 volume group** Add physical volume **⋮**

**Name** Test-VolGrp-0 [edit](#)

**UUID** pYf9eO-7nwg-ms96-LbmM-AYBf-puBq-jpjetg

**Capacity** 8.01 GB, 7.46 GiB, 8011120640 bytes

**Physical volumes**

|     |   |           |
|-----|---|-----------|
| sda | Kingston DT 101 II (001372997BD5F941C63402DA) | 3.7 / 8.0 |
|-----|---|-----------|

**LVM2 logical volumes** Create new

| ID         | Type             | Location |          |
|------------|------------------|----------|----------|
| Test-Vol-0 | Unformatted data | 3.70 GB  | <b>⋮</b> |

- Unformatted data
- Format**
- LVM2 logical volume
- Shrink
- Grow
- Deactivate
- Delete**

7. **Name** フィールドに、ファイルシステムの名前を入力します。
8. **マウントポイント** フィールドに、マウントパスを追加します。

**⚠ Format /dev/rhel-volume-group/rhel-logical-volume**

Name

Mount point

Type

Overwrite  Overwrite existing data with zeros (slower)

Encryption

At boot

Mounts in parallel with services  
 Boot still succeeds when filesystem does not mount

Mount options  Mount read only  
 Custom mount options

Formatting erases all data on a storage device.

9. **Type** ドロップダウンメニューで、ファイルシステムを選択します。

- **XFS** ファイルシステムは大規模な論理ボリュームをサポートし、オンラインの物理ドライブを停止せずに、既存のファイルシステムの拡大および縮小を行うことができます。別のストレージの使用を希望しない場合は、このファイルシステムを選択したままにしてください。

XFS は、XFS ファイルシステムでフォーマットしたボリュームサイズを縮小することには対応していません。

- **ext4** ファイルシステムは以下に対応します。
  - 論理ボリューム
  - オンラインの物理ドライブを停止せずに切り替え
  - ファイルシステムの拡張
  - ファイルシステムの縮小

10. RHEL Web コンソールでディスク全体をゼロで書き換える場合は、**Overwrite existing data with zeros** チェックボックスをオンにします。このプログラムはディスク全体を調べるため、このオプションを使用すると遅くなりますが、安全性は高まります。ディスクにデータが含まれていて、上書きする必要がある場合は、このオプションを使用します。

**Overwrite existing data with zeros** チェックボックスを選択しない場合、RHEL Web コンソールはディスクヘッダーのみを書き換えます。これにより、フォーマットの速度が向上します。

11. 論理ボリュームで暗号化を有効にする場合は、**Encryption** ドロップダウンメニューで暗号化のタイプを選択します。

LUKS1 (Linux Unified Key Setup) または LUKS2 暗号化を使用したバージョンを選択できます。これを使用すると、パスフレーズを使用してボリュームを暗号化できます。

12. **At boot** ドロップダウンメニューで、システムの起動後に論理ボリュームをいつマウントするかを選択します。
13. 必要な **Mount options** を選択します。
14. 論理ボリュームをフォーマットします。
  - ボリュームをフォーマットしてすぐにマウントする場合は、**Format and mount** をクリックします。
  - ボリュームをマウントせずにフォーマットする場合は、**Format only** をクリックします。ボリュームのサイズや、選択するオプションによって、フォーマットに数分かかることがあります。

## 検証

1. **Logical volume group** ページで、**LVM2 logical volumes** セクションまでスクロールし、論理ボリュームをクリックして詳細と追加オプションを確認します。

The screenshot displays the web console interface for managing LVM2 logical volumes. It is divided into two main sections: 'LVM2 volume group' and 'LVM2 logical volumes'.

**LVM2 volume group section:**

- Name:** Test-VolGrp-0 (with an edit link)
- UUID:** pYf9eO-7nwg-ms96-LbmM-AYBf-puBq-jpjetg
- Capacity:** 8.01 GB, 7.46 GiB, 8011120640 bytes
- Physical volumes:** A table showing the physical volume 'sda' (Kingston DT 101 II) with a capacity of 3.7 / 8.0 GB.

**LVM2 logical volumes section:**

| ID         | Type           | Location      | Size    |
|------------|----------------|---------------|---------|
| Test-Vol-0 | xfs filesystem | (not mounted) | 3.70 GB |

2. **Format only** オプションを選択した場合は、論理ボリュームの行末にあるメニューボタンをクリックし、**Mount** を選択して論理ボリュームを使用します。

## 19.5. WEB コンソールで論理ボリュームのサイズを変更

RHEL 8 Web コンソールで論理ボリュームを拡張または縮小する方法を説明します。

論理ボリュームのサイズを変更できるかどうかは、使用しているファイルシステムの種類に依存します。ほとんどのファイルシステムは、ボリュームをオンライン (停止) せずに拡張 (拡大) できます。

論理ボリュームに、縮小に対応するファイルシステムが含まれる場合は、論理ボリュームのサイズを縮小することもできます。これは、たとえば、ext3 または ext4 のファイルシステムでも利用できます。



## 警告

GFS2 または XFS のファイルシステムを含むボリュームを減らすことはできません。

## 前提条件

- 論理ボリュームのサイズ変更に対応するファイルシステムを含む既存の論理ボリューム。

## 手順

次の手順は、ボリュームをオフラインにすることなく、論理ボリュームを大きくする手順を説明します。

- RHEL Web コンソールにログインします。
- Storage** をクリックします。
- Storage** テーブルで、論理ボリュームが作成されたボリュームグループをクリックします。
- Logical volume group** ページで、**LVM2 logical volumes** セクションまでスクロールし、サイズを変更するボリュームグループの横にあるメニューボタン **⋮** をクリックします。
- メニューから **Grow** または **Shrink** を選択してボリュームのサイズを変更します。
  - ボリュームの増加:
    - ボリュームのサイズを増やすには、**Grow** を選択します。

The screenshot shows the 'LVM2 volume group' configuration page. At the top, there is a title 'LVM2 volume group' and a button 'Add physical volume'. Below this, the group details are listed: Name (Test-VolGrp-0), UUID (pYf9eO-7nwg-ms96-LbmM-AYBf-puBq-jpjetg), and Capacity (8.01 GB, 7.46 GiB, 8011120640 bytes). Under 'Physical volumes', there is a table with one entry: sda (Kingston DT 101 II (001372997BD5F941C63402DA)) with a size of 3.7 / 8.0 GB. Below this is the 'LVM2 logical volumes' section with a 'Create new' button and a table. The table has columns for ID, Type, and Location. One row is visible: Test-Vol-0 (Unformatted data, 3.70 GB). A context menu is open over the 'Test-Vol-0' row, showing options: Unformatted data, Format, LVM2 logical volume, Shrink, Grow, Deactivate, and Delete.

- Grow logical volume** ダイアログボックスで、論理ボリュームのサイズを調整します。

**Grow logical volume**

Size  GB

- c. **Grow** をクリックします。  
LVM はシステム停止を引き起こすことなく論理ボリュームを拡張します。
- ボリュームの縮小:
    - a. ボリュームのサイズを縮小するには、**Shrink** を選択します。

**LVM2 volume group**

Name Test-VolGrp-0 [edit](#)

UUID pYf9eO-7nwg-ms96-LbmM-AYBf-puBq-jpjetg

Capacity 8.01 GB, 7.46 GiB, 8011120640 bytes

**Physical volumes**

|     |   |           |
|-----|---|-----------|
| sda | Kingston DT 101 II (001372997BD5F941C63402DA) | 3.7 / 8.0 |
|-----|---|-----------|

**LVM2 logical volumes**

| ID         | Type             | Location | Size    |
|------------|------------------|----------|---------|
| Test-Vol-0 | Unformatted data |          | 3.70 GB |

Context menu options: Unformatted data, **Format**, LVM2 logical volume, **Shrink**, Grow, Deactivate, **Delete**

- b. **Shrink logical volume** ダイアログボックスで、論理ボリュームのサイズを調整します。

**Shrink logical volume**

Size  GB

- c. **Shrink** をクリックします。  
LVM はシステム停止を引き起こすことなく論理ボリュームを縮小します。

## 19.6. 関連情報

- [論理ボリュームの設定および管理](#)

## 第20章 WEB コンソールを使用したシン論理ボリュームの設定

シンプロビジョニングされた論理ボリュームを使用すると、実際に利用可能な物理ストレージよりも多くの領域を、指定したアプリケーションまたはサーバーに割り当てることができます。

詳細については、[シンプロビジョニングされたスナップショットボリュームの作成](#) を参照してください。

### 前提条件

- RHEL 8 Web コンソールがインストールされている。  
詳細は、[Web コンソールのインストールおよび有効化](#) を参照してください。
- **cockpit-storaged** パッケージがシステムにインストールされている。
- ボリュームグループの作成に使用する物理ドライブまたは他のタイプのストレージデバイスがシステムに接続されている。

### 20.1. WEB コンソールでシンプロビジョニングボリュームのプールの作成

シンプロビジョニングされたボリューム用のプールを作成します。

#### 前提条件

- [ボリュームグループが作成されました](#)。

#### 手順

1. RHEL 8 Web コンソールにログインします。
2. **Storage** をクリックします。
3. **Storage** テーブルで、シンボリュームを作成するボリュームグループをクリックします。
4. **Logical volume group** ページで、**LVM2 logical volumes** セクションまでスクロールし、**Create new logical volume** をクリックします。
5. **Name** フィールドに、新しい論理ボリュームの名前を入力します。名前にスペースを含めないでください。
6. **Purpose** ドロップダウンメニューで、**Pool for thinly provisioned volumes** を選択します。この設定では、ボリュームグループに含まれるすべてのドライブの容量の合計に等しい最大ボリュームサイズを持つ論理ボリュームを作成できます。



7. 論理ボリュームのサイズを定義します。以下を検討してください。

- この論理ボリュームを使用するシステムに必要なスペースの量。
- 作成する論理ボリュームの数

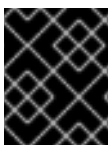
領域をすべて使用する必要はありません。必要な場合は、後で論理ボリュームを大きくすることができます。

8. **Create** をクリックします。

シンボリュームのプールが作成され、プールにシンボリュームを追加できるようになりました。

## 20.2. WEB コンソールでシンプロビジョニングされた論理ボリュームの作成

Web コンソールを使用して、プール内にシンプロビジョニングされた論理ボリュームを作成できます。複数のシンボリュームを追加でき、各シンボリュームは、シンボリュームのプールと同じ大きさにできます。



### 重要

シンボリュームを使用する場合は、論理ボリュームの物理的な空き容量を定期的に確認する必要があります。

## 前提条件

- シンボリックボリュームのプールを作成している。  
詳細は、[Web コンソールでシンボリックボリュームにプールを作成](#) を参照してください。

## 手順

1. RHEL 8 Web コンソールにログインします。
2. **Storage** をクリックします。
3. **Storage** テーブルで、シンボリックボリュームを作成するボリュームグループのメニューボタンをクリックします。
4. **Logical volume group** ページで、**LVM2 logical volumes** セクションまでスクロールし、シンボリックボリュームを作成するプールをクリックします。
5. **Pool for thinly provisioned LVM2 logical volumes** ページで、**Thinly provisioned LVM2 logical volumes** セクションまでスクロールし、**Create new thinly provisioned logical volume** をクリックします。
6. **Create thin volume** ダイアログボックスで、シンボリックボリュームの名前を入力します。名前にスペースは使用しないでください。
7. シンボリックボリュームのサイズを定義します。
8. **Create** をクリックします。  
シンボリックボリュームが作成されます。ボリュームを使用する前にフォーマットする必要があります。

## 20.3. WEB コンソールで論理ボリュームのフォーマット

論理ボリュームは物理ドライブとして動作します。これらを使用するには、ファイルシステムでフォーマットする必要があります。



### 警告

論理ボリュームをフォーマットすると、ボリューム上のすべてのデータが消去されます。

選択するファイルシステムにより、論理ボリュームに使用できる設定パラメーターが決まります。たとえば、XFS ファイルシステムはボリュームの縮小をサポートしていません。詳細については、[Web コンソールでの論理ボリュームのサイズ変更](#) を参照してください。

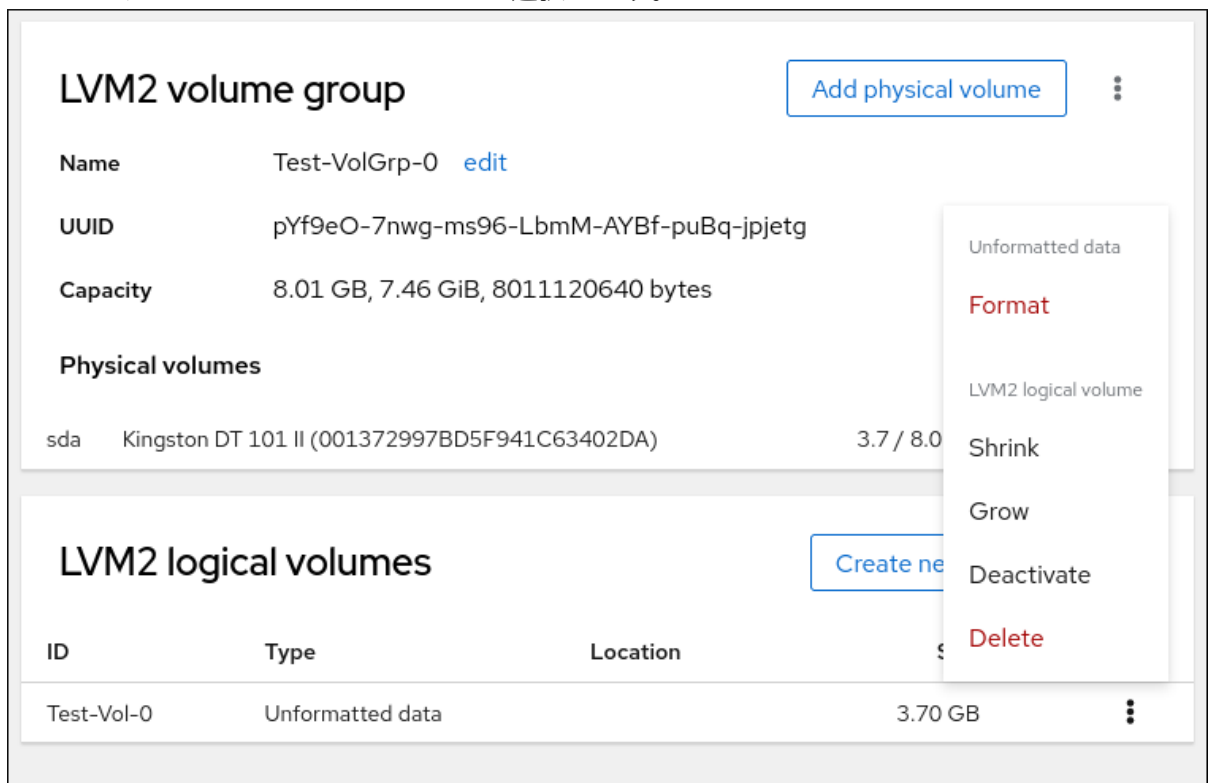
## 前提条件

- **cockpit-storaged** パッケージがシステムにインストールされている。
- 論理ボリュームが作成されている。詳細については、[Web コンソールでの論理ボリュームの作成](#) を参照してください。

- システムに対する root アクセス権を持っている。

## 手順

1. RHEL 8 Web コンソールにログインします。
2. **Storage** をクリックします。
3. **Storage** テーブルで、論理ボリュームが作成されたボリュームグループをクリックします。
4. **Logical volume group** ページで、**LVM2 logical volumes** セクションまでスクロールします。
5. フォーマットするボリュームグループの横にあるメニューボタン **⋮** をクリックします。
6. ドロップダウンメニューから **Format** を選択します。



7. **Name** フィールドに、ファイルシステムの名前を入力します。
8. **マウントポイント** フィールドに、マウントパスを追加します。

**⚠ Format /dev/rhel-volume-group/rhel-logical-volume**

Name

Mount point

Type

Overwrite  Overwrite existing data with zeros (slower)

Encryption

At boot

Mounts in parallel with services  
 Boot still succeeds when filesystem does not mount

Mount options  Mount read only  
 Custom mount options

Formatting erases all data on a storage device.

9. **Type** ドロップダウンメニューで、ファイルシステムを選択します。

- **XFS** ファイルシステムは大規模な論理ボリュームをサポートし、オンラインの物理ドライブを停止せずに、既存のファイルシステムの拡大および縮小を行うことができます。別のストレージの使用を希望しない場合は、このファイルシステムを選択したままにしてください。

XFS は、XFS ファイルシステムでフォーマットしたボリュームサイズを縮小することには対応していません。

- **ext4** ファイルシステムは以下に対応します。
  - 論理ボリューム
  - オンラインの物理ドライブを停止せずに切り替え
  - ファイルシステムの拡張
  - ファイルシステムの縮小

10. RHEL Web コンソールでディスク全体をゼロで書き換える場合は、**Overwrite existing data with zeros** チェックボックスをオンにします。このプログラムはディスク全体を調べるため、このオプションを使用すると遅くなりますが、安全性は高まります。ディスクにデータが含まれていて、上書きする必要がある場合は、このオプションを使用します。

**Overwrite existing data with zeros** チェックボックスを選択しない場合、RHEL Web コンソールはディスクヘッダーのみを書き換えます。これにより、フォーマットの速度が向上します。

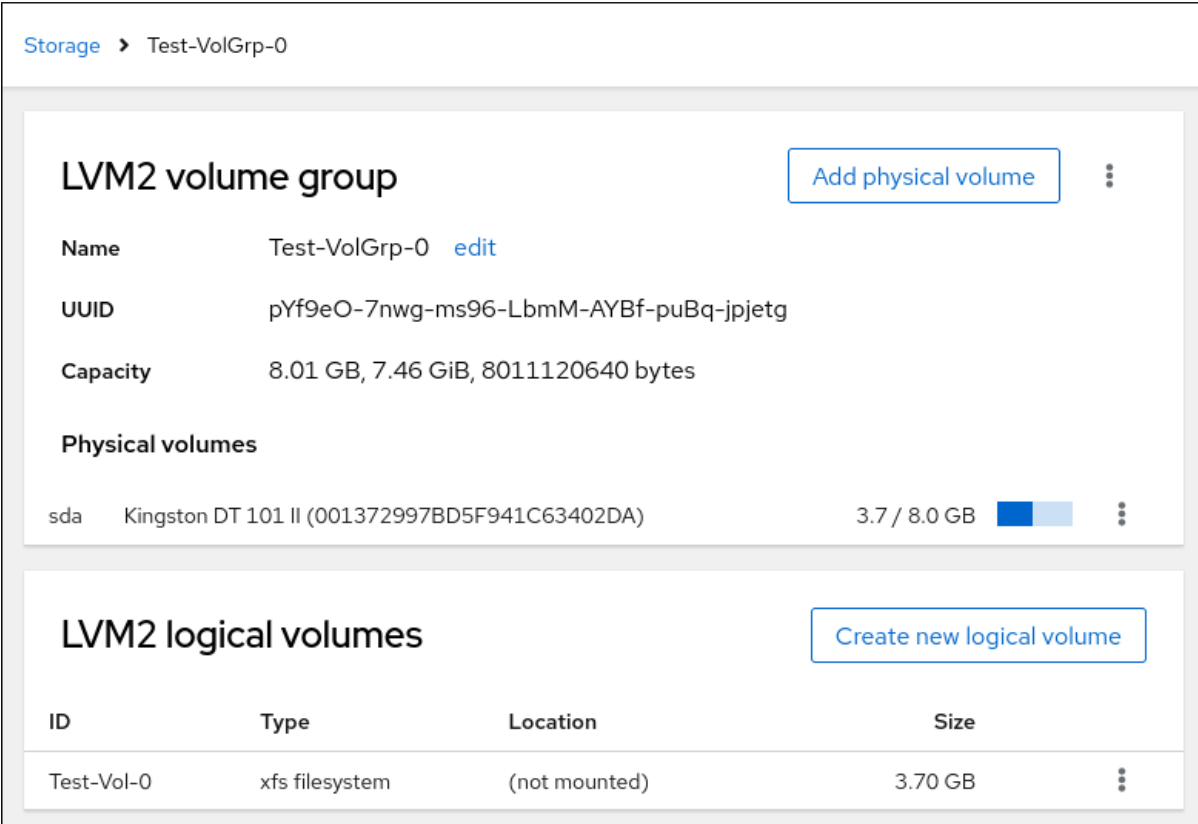
11. 論理ボリュームで暗号化を有効にする場合は、**Encryption** ドロップダウンメニューで暗号化のタイプを選択します。

LUKS1 (Linux Unified Key Setup) または LUKS2 暗号化を使用したバージョンを選択できます。これを使用すると、パスフレーズを使用してボリュームを暗号化できます。

12. **At boot** ドロップダウンメニューで、システムの起動後に論理ボリュームをいつマウントするかを選択します。
13. 必要な **Mount options** を選択します。
14. 論理ボリュームをフォーマットします。
  - ボリュームをフォーマットしてすぐにマウントする場合は、**Format and mount** をクリックします。
  - ボリュームをマウントせずにフォーマットする場合は、**Format only** をクリックします。ボリュームのサイズや、選択するオプションによって、フォーマットに数分かかることがあります。

## 検証

1. **Logical volume group** ページで、**LVM2 logical volumes** セクションまでスクロールし、論理ボリュームをクリックして詳細と追加オプションを確認します。



The screenshot displays the configuration for the LVM2 volume group 'Test-VolGrp-0'. It includes a table for physical volumes and a table for logical volumes.

| Physical volumes |  |
|------------------|--|
| sda              | Kingston DT 101 II (001372997BD5F941C63402DA) 3.7 / 8.0 GB |

| LVM2 logical volumes |                |               |         |
|----------------------|----------------|---------------|---------|
| ID                   | Type           | Location      | Size    |
| Test-Vol-0           | xfv filesystem | (not mounted) | 3.70 GB |

2. **Format only** オプションを選択した場合は、論理ボリュームの行末にあるメニューボタンをクリックし、**Mount** を選択して論理ボリュームを使用します。

## 20.4. WEB コンソールを使用してシンプロビジョニングされたスナップショットボリュームの作成

RHEL Web コンソールでシン論理ボリュームのスナップショットを作成し、前回のスナップショット以降ディスクに記録された変更をバックアップできます。

### 前提条件

- RHEL 8 Web コンソールをインストールし、アクセスできる。詳細は、[Web コンソールのインストールと有効化](#) を参照してください。

- **cockpit-storaged** パッケージがシステムにインストールされている。
- シンプロビジョニングボリュームが作成されている。詳細は、[Web コンソールを使用したシン論理ボリュームの設定](#) を参照してください。

## 手順

1. RHEL 8 Web コンソールにログインします。
2. **Storage** をクリックします。
3. **Storage** テーブルで、シンボリュームを作成するボリュームグループをクリックします。
4. **Logical volume group** ページで、**LVM2 logical volumes** セクションまでスクロールし、シン論理ボリュームを作成するプールをクリックします。
5. **Pool for thinly provisioned LVM2 logical volumes** ページで、**Thinly provisioned LVM2 logical volumes** セクションまでスクロールし、論理ボリュームの横にあるメニューボタン **:** をクリックします。
6. ドロップダウンメニューから、**Create snapshot** を選択します。

Storage > Test-VolGrp-0 > test-vpool-thin

**Pool for thinly provisioned LVM2 logical volumes** Grow **:**

|               |                 |                      |
|---------------|-----------------|----------------------|
| Name          | test-vpool-thin | <a href="#">edit</a> |
| Size          | 3.18 GB         |                      |
| Data used     | 0%              |                      |
| Metadata used | 11%             |                      |

**Thinly provisioned LVM2 logical volumes** Create new thinly provisioned

| ID         | Type             | Location |
|------------|------------------|----------|
| test-tvol0 | Unformatted data | 1.05 GB  |
| test-tvol1 | Unformatted data | 1.05 GB  |

Unformatted data  
**Format**  
 LVM2 logical volume  
 Shrink  
 Grow  
 Deactivate  
 Create snapshot  
**Delete**

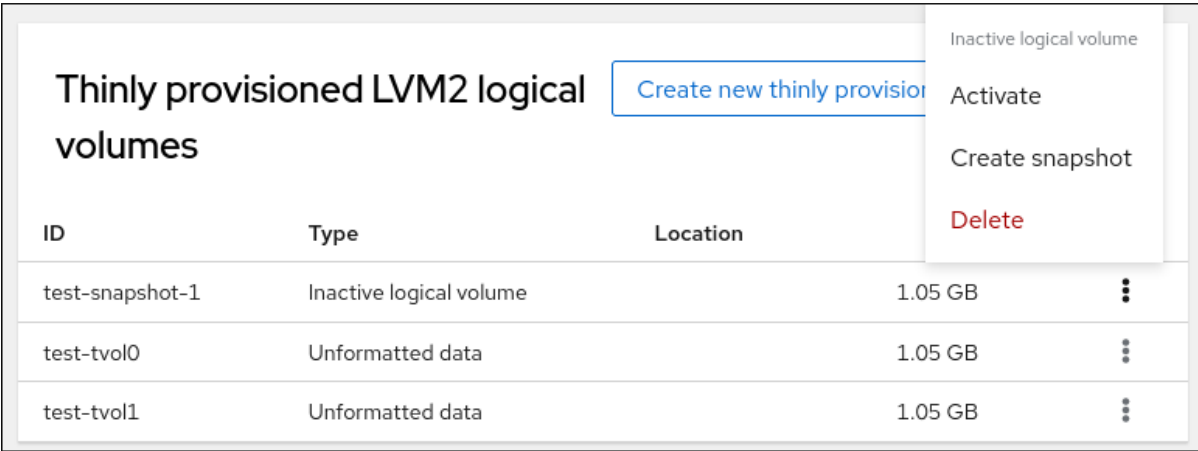
7. **Name** フィールドにスナップショット名を入力します。

**Create snapshot**

Name

Create Cancel

8. **Create** をクリックします。
9. **Pool for thinly provisioned LVM2 logical volumes** ページで、**Thinly provisioned LVM2 logical volumes** セクションまでスクロールし、新しく作成されたスナップショットの横にあるメニューボタン **⋮** をクリックします。
10. ドロップダウンメニューから **Activate** を選択してボリュームをアクティブ化します。



The screenshot shows the 'Thinly provisioned LVM2 logical volumes' page. A table lists three volumes: 'test-snapshot-1' (Inactive logical volume, 1.05 GB), 'test-tvol0' (Unformatted data, 1.05 GB), and 'test-tvol1' (Unformatted data, 1.05 GB). A context menu is open over the 'test-snapshot-1' row, showing options: 'Inactive logical volume', 'Activate', 'Create snapshot', and 'Delete'. A blue box highlights the 'Create new thinly provisioned LVM2 logical volume' button in the top right corner.

| ID              | Type                    | Location |   |
|-----------------|-------------------------|----------|---|
| test-snapshot-1 | Inactive logical volume | 1.05 GB  | ⋮ |
| test-tvol0      | Unformatted data        | 1.05 GB  | ⋮ |
| test-tvol1      | Unformatted data        | 1.05 GB  | ⋮ |

## 第21章 WEB コンソールを使用してボリュームグループ内の物理ドライブを変更する

RHEL 8 Web コンソールを使用して、ボリュームグループのドライブを変更します。

物理ドライブを変更するには、次の手順に従ってください。

- [Web コンソールでボリュームグループに物理デバイスを追加](#)
- [Web コンソールでボリュームグループから物理ドライブを削除](#)

### 前提条件

- RHEL 8 Web コンソールがインストールされている。  
詳細は、[Web コンソールのインストールおよび有効化](#) を参照してください。
- **cockpit-storaged** パッケージがシステムにインストールされている。
- 古いまたは不具合がある物理ドライブを交換するための新しい物理ドライブ。
- この設定には、物理ドライブがボリュームグループに編成されていることが必要になります。

### 21.1. WEB コンソールでボリュームグループに物理デバイスを追加

RHEL 8 Web コンソールを使用すると、既存の論理ボリュームに新しい物理ドライブ、またはその他のタイプのボリュームを追加できます。

#### 前提条件

- ボリュームグループが作成されている。
- マシンに新しいドライブが接続されている。

#### 手順

1. RHEL 8 Web コンソールにログインします。
2. **Storage** をクリックします。
3. **Storage** テーブルで、物理ドライブを追加するボリュームグループをクリックします。
4. **LVM2 volume group** ページで、**Add physical volume** をクリックします。
5. **Add Disks** ダイアログボックスでドライブを選択し、**Add** をクリックします。

#### 検証手順

- **LVM2 volume group** ページで、**Physical volumes** セクションをチェックして、新しい物理ドライブがボリュームグループで使用可能かどうかを確認します。

### 21.2. WEB コンソールでボリュームグループから物理ドライブを削除

論理ボリュームに複数の物理ドライブが含まれている場合は、オンラインの物理ドライブのいずれかを削除できます。



システムは、削除時に、削除するドライブから全てのデータを自動的に別のデバイスに移動します。これには少し時間がかかる場合があります。

Web コンソールは、物理ドライブを削除するための十分な容量があるかどうかを検証します。

### 前提条件

- 複数の物理ドライブが接続するボリュームグループ

### 手順

1. RHEL 8 Web コンソールにログインします。
2. **Storage** をクリックします。
3. **Storage** テーブルで、物理ドライブを追加するボリュームグループをクリックします。
4. **LVM2 volume group** ページで、**Physical volumes** セクションまでスクロールします。
5. 削除する物理ボリュームの横にあるメニューボタン **⋮** をクリックします。
6. ドロップダウンメニューから **Remove** を選択します。  
ディスクを削除するための十分な容量が論理ボリュームにあるかどうかを RHEL 9 Web コンソールが検証します。データを転送するための空き領域がない場合は、ディスクを削除することはできず、最初に別のディスクを追加してボリュームグループの容量を増やす必要があります。詳細については、[Web コンソールで物理ドライブを論理ボリュームに追加する](#) を参照してください。

## 第22章 WEB コンソールを使用した VIRTUAL DATA OPTIMIZER ボリュームの管理

RHEL 8 Web コンソールを使用して、VDO (Virtual Data Optimizer) を設定します。

以下の方法について説明します。

- VDO ボリュームの作成
- VDO ボリュームのフォーマット
- VDO ボリュームの拡張

### 前提条件

- RHEL 8 Web コンソールをインストールし、アクセスできる。詳細は、[Web コンソールのインストールおよび有効化](#) を参照してください。
- **cockpit-storaged** パッケージがシステムにインストールされている。

### 22.1. WEB コンソールでの VDO ボリューム

Red Hat Enterprise Linux 8 では、Virtual Data Optimizer (VDO) がサポートされます。

VDO は、以下を組み合わせたブロック仮想化テクノロジーです。

#### 圧縮

詳細は、[Enabling or disabling compression in VDO](#) を参照してください。

#### 重複排除

詳細は、[Enabling or disabling compression in VDO](#) を参照してください。

#### シンプロビジョニング

詳細は、[シンプロビジョニングボリューム \(シンボリューム\) の作成と管理](#) を参照してください。

このような技術を使用して、VDO は、以下を行います。

- ストレージ領域をインラインに保存します。
- ファイルを圧縮します。
- 重複を排除します。
- 物理ストレージまたは論理ストレージが提供するサイズよりも多くの仮想領域を割り当てることができます。
- 拡大して仮想ストレージを拡張できます。

VDO は、さまざまなタイプのストレージに作成できます。RHEL 8 Web コンソールでは、以下に VDO を設定できます。

- LVM



## 注記

シンプロビジョニングされたボリュームに VDO を設定することはできません。

- 物理ボリューム
- ソフトウェア RAID

ストレージスタックにおける VDO の配置の詳細は、[System Requirements](#) を参照してください。

## 関連情報

- VDO の詳細は、[Deduplicating and compressing storage](#) を参照してください。

## 22.2. WEB コンソールで VDO ボリュームの作成

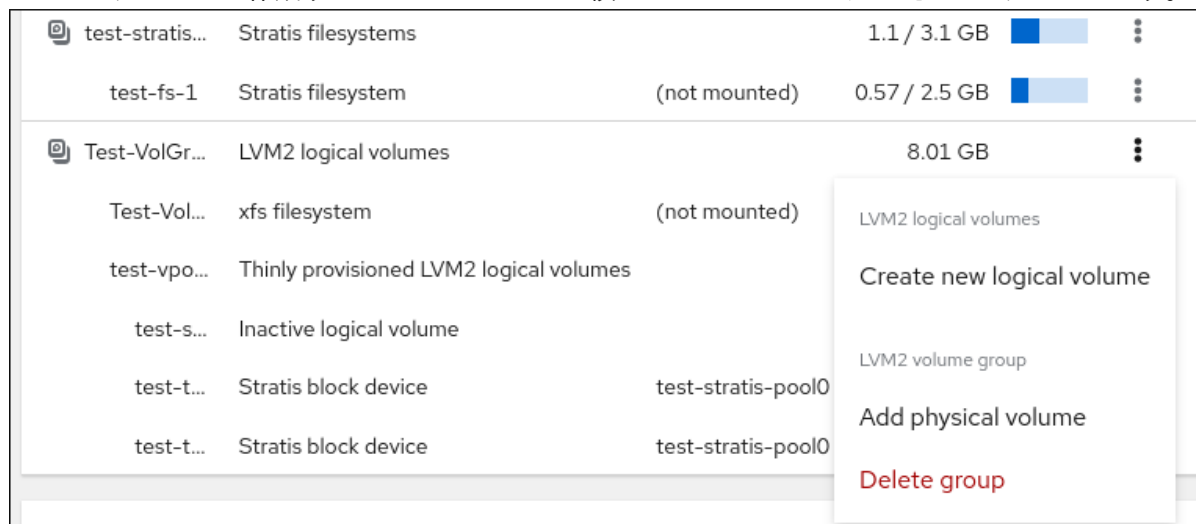
RHEL Web コンソールで VDO ボリュームを作成します。

### 前提条件

- VDO を作成する LVM2 グループ。

### 手順

1. RHEL 8 Web コンソールにログインします。  
詳細は、[Web コンソールへのログイン](#) を参照してください。
2. **Storage** をクリックします。
3. VDO ボリュームを作成する LVM2 グループの横にあるメニューボタン **⋮** をクリックします。



4. **Purpose** フィールドの横にあるドロップダウンメニューで **VDO filesystem volume** を選択します。
5. **Name** フィールドに、VDO ボリュームの名前 (スペースなし) を入力します。
6. **論理サイズ** バーに、VDO ボリュームのサイズを設定します。10 回以上拡張できますが、VDO ボリュームを作成する目的を検討してください。

- アクティブな仮想マシンまたはコンテナストレージの場合は、使用する論理のサイズを、ボリュームの物理サイズの10倍にするようにします。
- オブジェクトストレージの場合は、使用する論理のサイズを、ボリュームの物理サイズの3倍にするようにします。

詳細は、[Deploying VDO](#) を参照してください。

7. **圧縮** オプションを選択します。このオプションを使用すると、さまざまなファイル形式を効率的に減らすことができます。

詳細は、[Enabling or disabling compression in VDO](#) を参照してください。

8. **重複排除** オプションを選択します。

このオプションは、重複ブロックのコピーを削除して、ストレージリソースが使用されなくなるようにします。詳細は、[Enabling or disabling compression in VDO](#) を参照してください。

### Create logical volume

Name

Purpose

Size  8137 MB

Logical size  10.0 GB

Options

Compression [?](#)

Deduplication [?](#)

#### 検証手順

- ストレージセクションに新しいVDOボリュームが表示されることを確認します。そして、ファイルシステムでフォーマットすることができます。

## 22.3. WEB コンソールで VDO ボリュームのフォーマット

VDO ボリュームは物理ドライブとして動作します。これらを使用するには、ファイルシステムでフォーマットする必要があります。



#### 警告

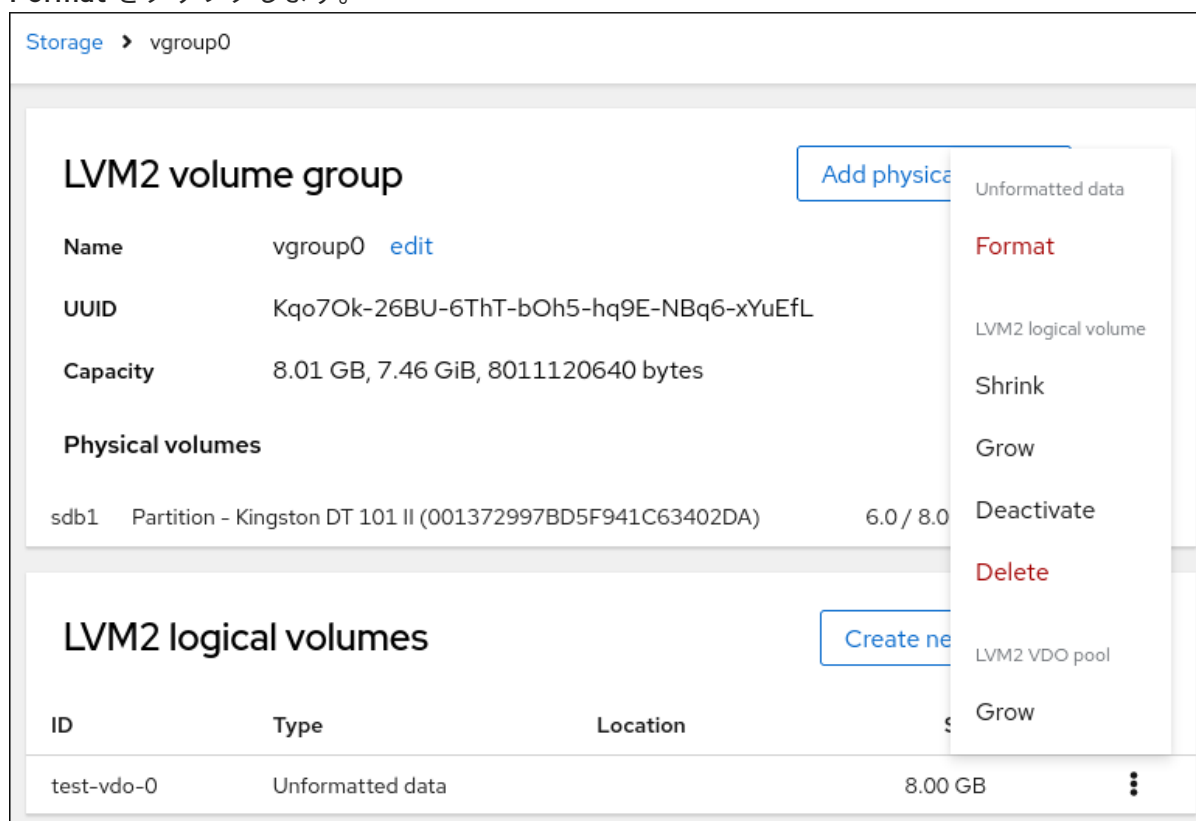
フォーマットするとボリューム上のすべてのデータが消去されます。

#### 前提条件

- VDO ボリュームが作成されている。詳細については、[Web コンソールでの VDO ボリュームの作成](#) を参照してください。

## 手順

1. RHEL 8 Web コンソールにログインします。詳細は、[Web コンソールへのログイン](#) を参照してください。
2. **Storage** をクリックします。
3. フォーマットする VDO ボリュームを含む LVM2 ボリュームグループをクリックします。
4. フォーマットする VDO ボリュームの行末にあるメニューボタン **⋮** をクリックします。
5. **Format** をクリックします。



6. **名前** フィールドに、論理ボリューム名を入力します。
7. **マウントポイント** フィールドに、マウントパスを追加します。
8. デフォルトでは、このダイアログを完了すると、Web コンソールはディスクヘッダーのみを書き換えます。このオプションの利点は、フォーマットの速度です。**Overwrite existing data with zeros** オプションをオンにすると、Web コンソールはディスク全体をゼロで書き換えます。このプログラムはディスク全体を調べるため、このオプションを使用すると遅くなります。ディスクに機密データが含まれており、それを書き換えたい場合は、このオプションを使用します。
9. **Type** ドロップダウンメニューで、ファイルシステムを選択します。
  - デフォルトオプションの **XFS** ファイルシステムは、大規模な論理ボリュームをサポートし、物理ドライブを停止せずにオンラインで切り替え、拡張することができます。XFS は、ボリュームの縮小に対応していません。したがって、XFS でフォーマットされたボリュームのサイズを縮小することはできません。

- **ext4** ファイルシステムは論理ボリュームをサポートし、オンラインの物理ドライブを停止せずに、既存のファイルシステムの拡大および縮小を行うことができます。

LUKS (Linux Unified Key Setup) 暗号を使用したバージョンも選択できます。パスフレーズを使用してボリュームの暗号化を行えます。

10. **At boot** ドロップダウンメニューで、ボリュームをマウントするタイミングを選択します。
11. **Format and mount** または **Format only** をクリックします。  
フォーマットに使用されるオプションや、ボリュームのサイズによって、フォーマットに数分かかることがあります。

**⚠ Format /dev/vgroup0/test-vdo-0**

**Name**

**Mount point**

**Type**

**Overwrite**  Overwrite existing data with zeros (slower)

**Encryption**

**At boot**

- Mounts before services start
- Appropriate for critical mounts, such as /var
- ⚠ Boot fails if filesystem does not mount, preventing remote access

**Mount options**  Mount read only  
 Custom mount options

Formatting erases all data on a storage device.

## 検証

- 正常に完了すると、フォーマットされた VDO ボリュームの詳細が **Storage** タブと LVM2 ボリュームグループタブに表示されます。

## 22.4. WEB コンソールで VDO ボリュームの拡張

RHEL 8 Web コンソールで VDO ボリュームを拡張します。

### 前提条件

- **cockpit-storaged** パッケージがシステムにインストールされている。
- VDO ボリュームが作成されている。

### 手順

1. RHEL 8 Web コンソールにログインします。  
詳細は、[Web コンソールへのログイン](#) を参照してください。
2. **Storage** をクリックします。
3. **VDO デバイス** で、VDO ボリュームをクリックします。
4. VDO ボリュームの詳細で、**Grow** ボタンをクリックします。
5. **VDO の論理サイズを増加** ダイアログボックスで、VDO ボリュームの論理サイズを増やします。
  1. **Grow** をクリックします。

#### 検証手順

- 新しいサイズの VDO ボリュームの詳細を確認し、変更が正常に行われたことを確認します。

## 第23章 RHEL WEB コンソールで LUKS パスワードを使用したデータのロック

Web コンソールのストレージタブでは、作成、ロック、ロック解除、サイズ変更、または LUKS (Linux Unified Key Setup) バージョン 2 形式を使用した暗号化デバイスを設定できます。

この新しいバージョンの LUKS は、以下を提供します。

- より柔軟なロック解除ポリシー
- より強力な暗号化
- 今後の変更との互換性の高さ

### 前提条件

- RHEL 8 Web コンソールがインストールされている。詳細は、[Web コンソールのインストールおよび有効化](#) を参照してください。
- **cockpit-storaged** パッケージがシステムにインストールされている。

### 23.1. LUKS ディスクの暗号化

Linux Unified Key Setup-on-disk-format (LUKS) は、暗号化されたデバイスの管理を簡素化するツールセットを提供します。LUKS を使用すると、ブロックデバイスを暗号化し、複数のユーザーキーでマスターキーを復号化できるようになります。パーティションの一括暗号化には、このマスターキーを使用します。

Red Hat Enterprise Linux は、LUKS を使用してブロックデバイスの暗号化を実行します。デフォルトではインストール時に、ブロックデバイスを暗号化するオプションが指定されていません。ディスクを暗号化するオプションを選択すると、コンピューターを起動するたびにパスワードの入力が求められます。このパスワードは、パーティションを復号化するバルク暗号鍵のロックを解除します。デフォルトのパーティションテーブルを変更する場合は、暗号化するパーティションを選択できます。この設定は、パーティションテーブル設定で行われます。

### Ciphers

LUKS に使用されるデフォルトの暗号は **aes-xts-plain64** です。LUKS のデフォルトの鍵サイズは 512 ビットです。**Anaconda** XTS モードを使用した LUKS のデフォルトの鍵サイズは 512 ビットです。使用可能な暗号は次のとおりです。

- 高度暗号化標準 (Advanced Encryption Standard, AES)
- Twofish
- Serpent

### LUKS によって実行される操作

- LUKS は、ブロックデバイス全体を暗号化するため、脱着可能なストレージメディアやノート PC のディスクドライブといった、モバイルデバイスのコンテンツを保護するのに適しています。



- 暗号化されたブロックデバイスの基本的な内容は任意であり、スワップデバイスの暗号化に役立ちます。また、とりわけデータストレージ用にフォーマットしたブロックデバイスを使用する特定のデータベースに関する情報でも有用です。
- LUKS は、既存のデバスマッパーのカーネルサブシステムを使用します。
- LUKS はパスフレーズのセキュリティーを強化し、辞書攻撃から保護します。
- LUKS デバイスには複数のキースロットが含まれているため、バックアップキーやパスフレーズを追加できます。



### 重要

LUKS は次のシナリオには推奨されません。

- LUKS などのディスク暗号化ソリューションは、システムの停止時にしかデータを保護しません。システムの電源がオンになり、LUKS がディスクを復号化すると、そのディスクのファイルは、そのファイルにアクセスできるすべてのユーザーが使用できます。
- 同じデバイスに対する個別のアクセスキーを複数のユーザーが持つ必要があるシナリオ。LUKS1 形式はキースロットを 8 個提供し、LUKS2 形式はキースロットを最大 32 個提供します。
- ファイルレベルの暗号化を必要とするアプリケーション。

### 関連情報

- [LUKS プロジェクトのホームページ](#)
- [LUKS オンディスクフォーマットの仕様](#)
- [FIPS 197: Advanced Encryption Standard \(AES\)](#)

## 23.2. WEB コンソールで LUKS パスフレーズの設定

システムの既存の論理ボリュームに暗号化を追加する場合は、ボリュームをフォーマットすることでは実行できません。

### 前提条件

- Web コンソールがインストールされており、アクセス可能である。詳細は、[Web コンソールのインストール](#) を参照してください。
- **cockpit-storaged** パッケージがシステムにインストールされている。
- 暗号化なしで、既存の論理ボリュームを利用できます。

### 手順

1. RHEL 8 Web コンソールにログインします。  
詳細は、[Web コンソールへのログイン](#) を参照してください。
2. **Storage** をクリックします。

3. **Storage** テーブルで、暗号化するストレージデバイスの横にあるメニューボタン **⋮** をクリックします。
4. ドロップダウンメニューから **Format** を選択します。
5. **Encryption field** で、暗号化仕様 **LUKS1** または **LUKS2** を選択します。
6. 新しいパスフレーズを設定し、確認します。
7. (必要に応じて) さらなる暗号化オプションを変更します。
8. フォーマット設定の最終処理
9. **Format** をクリックします。

### 23.3. WEB コンソールで LUKS パスフレーズの変更

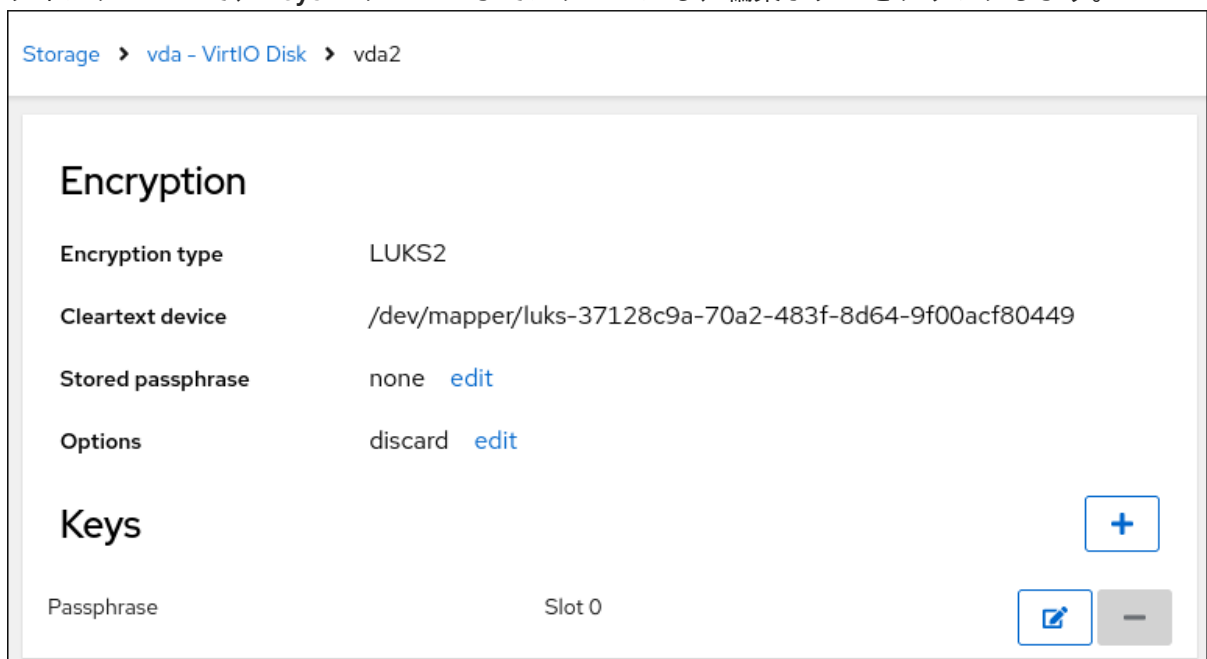
Web コンソールで、暗号化されたディスクまたはパーティションで LUKS パスフレーズを変更します。

#### 前提条件

- Web コンソールがインストールされており、アクセス可能である。詳細は、[Web コンソールのインストール](#) を参照してください。
- **cockpit-storaged** パッケージがシステムにインストールされている。

#### 手順

1. Web コンソールにログインします。詳細は、[Web コンソールへのログイン](#) を参照してください。
2. **Storage** をクリックします。
3. **Storage** テーブルで、暗号化されたデータを含むディスクを選択します。
4. ディスクページで、**Keys** セクションまでスクロールし、**編集ボタン** をクリックします。



5. **パスフレーズの変更** ダイアログウィンドウで、以下を行います。
  - a. 現在のパスフレーズを入力します。
  - b. 新しいパスフレーズを入力します。
  - c. 新しいパスフレーズを確認します。

### Change passphrase

Old passphrase  

New passphrase  

Repeat passphrase  

6. **Save** をクリックします。

## 第24章 WEB コンソールで TANG キーを使用して自動ロック解除を設定する

Tang サーバーが提供する鍵を使用して、LUKS で暗号化したストレージデバイスの自動ロック解除を設定できます。

### 前提条件

- RHEL 8 Web コンソールがインストールされている。詳細は、[Web コンソールのインストール](#)を参照してください。
- **cockpit-storaged** と **clevis-luks** パッケージがシステムにインストールされている。
- **cockpit.socket** サービスがポート 9090 で実行されている。
- Tang サーバーを利用できる。詳細は、[Deploying a Tang server with SELinux in enforcing mode](#) 参照してください。

### 手順

1. Web ブラウザーに以下のアドレスを入力して、RHEL Web コンソールを開きます。

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

リモートシステムに接続する場合は、<localhost> の部分をリモートサーバーのホスト名または IP アドレスに置き換えます。

2. 認証情報を入力して、**Storage** をクリックします。**Storage** テーブルで、自動的にロックを解除するために追加する予定の暗号化ボリュームが含まれるディスクをクリックします。
3. 次のページに選択したディスクの詳細が表示されたら、**Keys** セクションの **+** をクリックして Tang 鍵を追加します。

Storage > vda - VirtIO Disk > vda2

|      |  |
|------|--|
| Name | -  |
| UUID | 44d29c6b-02                                |
| Type | Linux filesystem data <a href="#">edit</a> |
| Size | 15.0 GB                                    |

### Encryption

|                   |   |
|-------------------|---|
| Encryption type   | LUKS2   |
| Cleartext device  | /dev/mapper/luks-37128c9a-70a2-483f-8d64-9f00acf80449 |
| Stored passphrase | none <a href="#">edit</a>                             |
| Options           | discard <a href="#">edit</a>                          |

### Keys

Passphrase Slot 0 [+](#) [-](#)

4. **Key source** として **Tang keyserver** を選択し、Tang サーバーのアドレスと、LUKS で暗号化されたデバイスのロックを解除するパスワードを入力します。**Add** をクリックして確定します。

### Add key

Key source  Passphrase  Tang keyserver

Keyserver address

Disk passphrase  [eye](#)

Saving a new passphrase requires unlocking the disk. Please provide a current disk passphrase.

[Add](#) [Cancel](#)

以下のダイアログウィンドウは、鍵ハッシュが一致することを確認するコマンドを提供します。

5. Tang サーバーのターミナルで、**tang-show-keys** コマンドを使用して、比較のためにキーハッシュを表示します。この例では、Tang サーバーはポート 7500 で実行されています。

```
# tang-show-keys 7500
x100_1k6GPiDOaMIL3WbpCjHOy9ul1bSfdhI3M08wO0
```

6. Web コンソールと前述のコマンドの出力のキーハッシュが同じ場合は、**Trust key** をクリックします。

### Verify key

Check the key hash with the Tang server.

[Copy to clipboard](#)

#### How to check

In a terminal, run: `ssh tang1.████████████████████.com tang-show-keys`

Check that the SHA-256 or SHA-1 hash from the command matches this dialog.

**SHA-256**

```
x100_1k6GPiDOaMIL3WbpCjHOy9ul1bSfdhI3M08wO0
```

**SHA-1**

```
hmINhleYB000ddFszgICjqJizFI
```

Trust key
Cancel

7. RHEL 8.8 以降では、暗号化されたルートファイルシステムと Tang サーバーを選択した後、カーネルコマンドラインへの **rd.neednet=1** パラメーターの追加、**clevis-dracut** パッケージのインストール、および初期 RAM ディスク (**initrd**) の再生成をスキップできます。非ルートファイルシステムの場合、Web コンソールは、**remote-cryptsetup.target** および **clevis-luks-akspass.path systemd** ユニットを有効にし、**clevis-systemd** パッケージをインストールし、**\_netdev** パラメーターを **fstab** および **crypttab** 設定ファイルに追加するようになりました。

## 検証

1. 新規に追加された Tang キーが **Keyserver** タイプの **Keys** セクションにリスト表示されていることを確認します。

### Encryption

|                   |   |
|-------------------|---|
| Encryption type   | LUKS2   |
| Cleartext device  | /dev/mapper/luks-37128c9a-70a2-483f-8d64-9f00acf80449 |
| Stored passphrase | none <a href="#">edit</a>                             |
| Options           | discard <a href="#">edit</a>                          |

### Keys

+

|            |  |        |  |
|------------|--|--------|--|
| Passphrase | Slot 0                                 |        |  |
| Keyserver  | http://tang1.████████████████████.com/ | Slot 1 |  |

2. バインディングが初期ブートで使用できることを確認します。次に例を示します。

```
# 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  
...
```

#### 関連情報

- [ポリシーベースの複号を使用して暗号化ボリュームの自動アンロックの設定](#)

## 第25章 WEB コンソールでソフトウェア更新の管理

RHEL 9 Web コンソールでソフトウェア更新を管理する方法と、それらを自動化する方法について説明します。

Web コンソールのソフトウェア更新モジュールは、**yum** ユーティリティーに基づいています。**yum** を使用したソフトウェアの更新の詳細は、[Updating software packages](#) セクションを参照してください。

### 25.1. WEB コンソールでの手動ソフトウェア更新の管理

Web コンソールを使用してソフトウェアを手動で更新できます。

#### 前提条件

- Web コンソールがインストールされており、アクセス可能である。詳細は、[Web コンソールのインストール](#) を参照してください。

#### 手順

1. RHEL 8 Web コンソールにログインします。  
詳細は、[Web コンソールへのログイン](#) を参照してください。
2. **ソフトウェアの更新** をクリックします。  
最後のチェックが行われてから 24 時間以上経っている場合は、利用可能な更新のリストが自動的に更新されます。更新を発生させるには、**Check for Updates** ボタンをクリックします。
3. 更新を適用します。更新の実行中に更新ログを見ることができます。
  - a. 利用可能な更新をすべてインストールするには、**Install all updates** ボタンをクリックします。
  - b. セキュリティー更新プログラムがある場合は、**Install Security Updates** ボタンをクリックすると個別にインストールできます。
  - c. 利用可能な kpatch 更新がある場合は、**Install kpatch updates** ボタンをクリックして、それらを個別にインストールできます。
4. オプション: システムを自動的に再起動するために、**Reboot after completion** スイッチをオンにすることができます。  
この手順を実行する場合は、この手順の残りの手順をスキップできます。
5. システムが更新を適用すると、システムを再起動するように勧められます。  
個別には再起動しない新しいカーネルまたはシステムサービスが更新に含まれている場合は、特に推奨されます。
6. **無視** をクリックして再起動をキャンセルするか、**今すぐ再起動** をクリックしてシステムの再起動を続行します。  
システムの再起動後、Web コンソールにログインし、**ソフトウェアの更新** ページに移動して、更新が成功したことを確認します。

### 25.2. WEB コンソールで自動ソフトウェア更新の管理

Web コンソールでは、すべての更新またはセキュリティ更新の適用を選択し、自動更新の周期とタイミングを管理することもできます。



## 前提条件

- Web コンソールがインストールされており、アクセス可能である。詳細は、[Web コンソールのインストール](#) を参照してください。

## 手順

1. RHEL 8 Web コンソールにログインします。詳細は、[Web コンソールへのログイン](#) を参照してください。
2. **ソフトウェアの更新** をクリックします。
3. **設定** 表で、**編集** ボタンをクリックします。
4. 自動更新の種類を一つ選びます。**セキュリティ更新プログラムのみ**、または **すべての更新プログラム** から選択することができます。
5. 自動更新の日付を変更するには、ドロップダウンメニューの **毎日** をクリックして、特定の日付を選択します。
6. 自動更新の時刻を変更するには、**6:00** のフィールドをクリックして、特定の時刻を選択するか、入力します。
7. ソフトウェアの自動更新を無効にする場合は、**更新なし** を選択してください。

## 25.3. WEB コンソールでソフトウェア更新適用後のオンデマンド再起動の管理

インテリジェント再起動機能は、ソフトウェア更新後にシステム全体を再起動する必要があるのか、それとも特定のサービスだけを再起動すればよいのかをユーザーに通知する機能です。

## 前提条件

- Web コンソールがインストールされており、アクセス可能である。詳細は、[Web コンソールのインストール](#) を参照してください。

## 手順

1. RHEL 8 Web コンソールにログインします。詳細は、[Web コンソールへのログイン](#) を参照してください。
2. **ソフトウェアの更新** をクリックします。
3. システムの更新を適用します。
4. 更新が成功したら、**Reboot system...**、**Restart services...**、または **Ignore** をクリックします。
5. 無視することにした場合には、次のいずれかの方法で再起動またはリブートメニューに戻ることができます。
  - a. リブート:
    - i. **Software Updates** ページの **Status** フィールドにある **Reboot system** ボタンをクリックします。
    - ii. (オプション) ログインしているユーザーへのメッセージを書きます。

- iii. **Delay** ドロップダウンメニューから、**delay** を選択します。
  - iv. **Reboot** をクリックします。
- b. サービスの再起動:
- i. **Software Updates** ページの **Status** フィールドにある **Restart services...** ボタンをクリックします。  
再起動が必要なすべてのサービスのリストが表示されます。
  - ii. **サービスの再起動** をクリックします。  
選択した内容に応じて、システムを再起動するか、サービスを再起動します。

## 25.4. WEB コンソールでのカーネルライブパッチを使用したパッチ適用

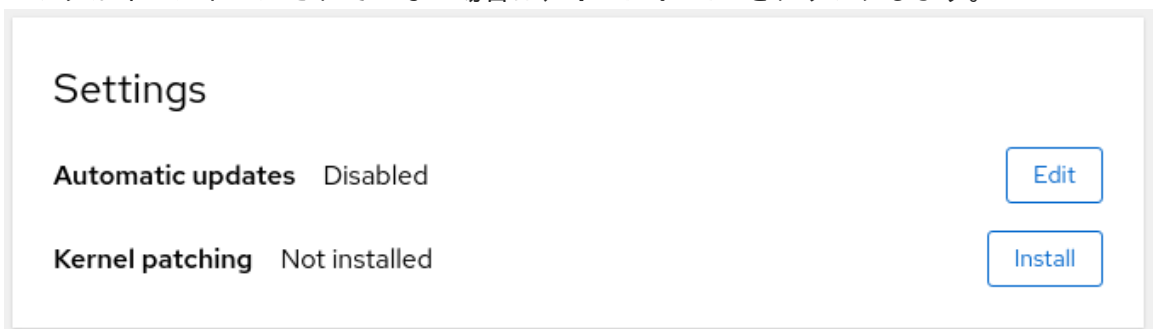
この Web コンソールでは、**kpatch** フレームワークを使用して再起動を強制せずに、カーネルセキュリティパッチを適用できます。以下の手順で、任意のパッチを設定する方法を説明します。

### 前提条件

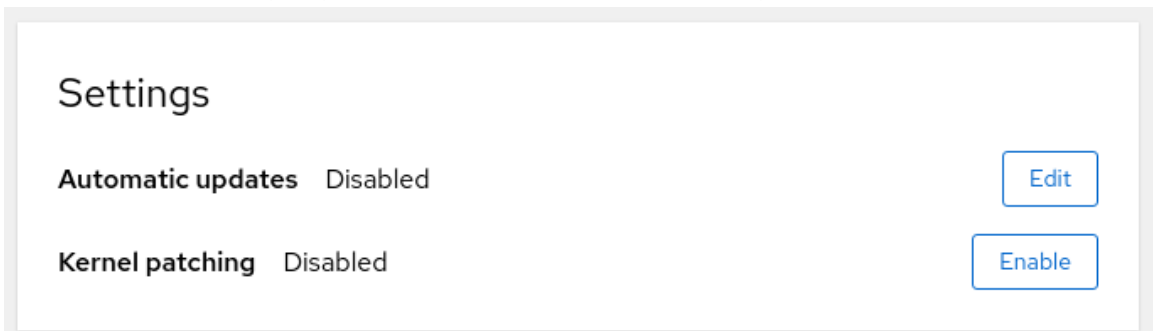
- Web コンソールがインストールされており、アクセス可能である。詳細は、[Web コンソールのインストール](#) を参照してください。

### 手順

1. Web コンソールに管理者権限でログインする。詳細は、[Web コンソールへのログイン](#) を参照してください。
2. **ソフトウェアの更新** をクリックします。
3. カーネルパッチの設定状況を確認します。
  - a. パッチがインストールされていない場合は、**インストール** をクリックします。

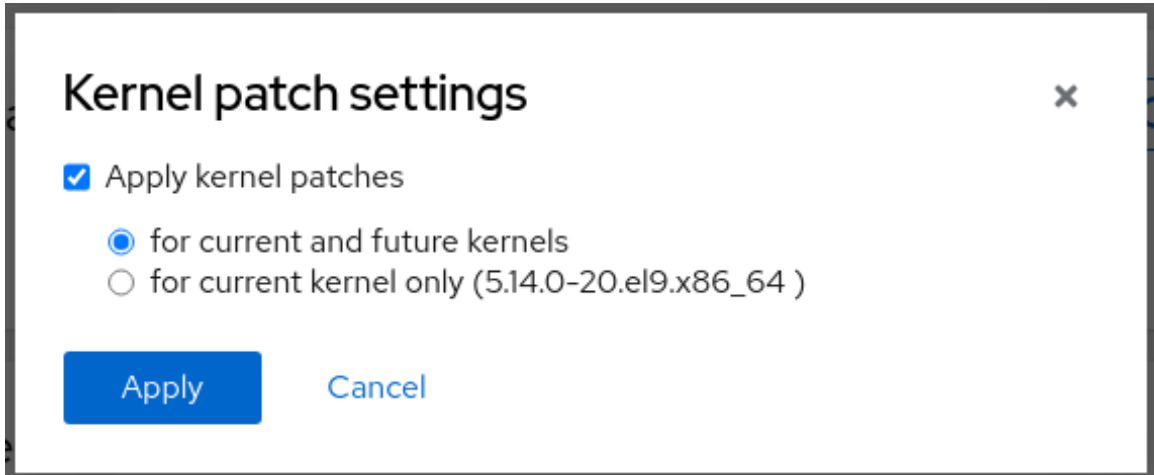


- b. カーネルパッチを有効にするには、**Enable** をクリックします。



- c. カーネルパッチを適用する場合はチェックを入れます。

- d. 現在および今後のカーネルにパッチを適用するか、現在のカーネルにのみ適用するかを選択します。今後のカーネルに対するパッチの適用を選択した場合に、システムは今後リリースされるカーネルに対してもパッチを適用します。

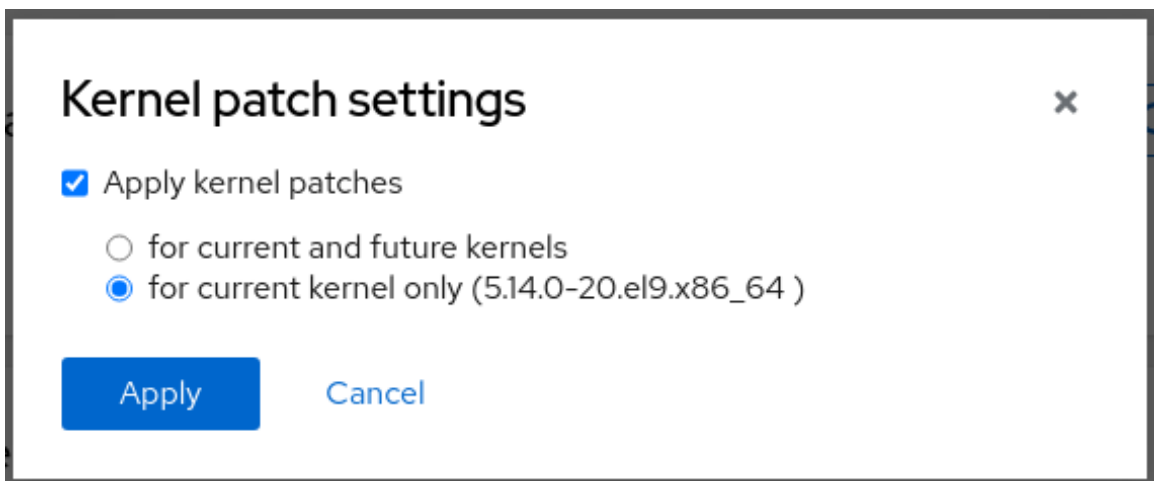


**Kernel patch settings** ×

Apply kernel patches

for current and future kernels  
 for current kernel only (5.14.0-20.el9.x86\_64)

**Apply** Cancel



**Kernel patch settings** ×

Apply kernel patches

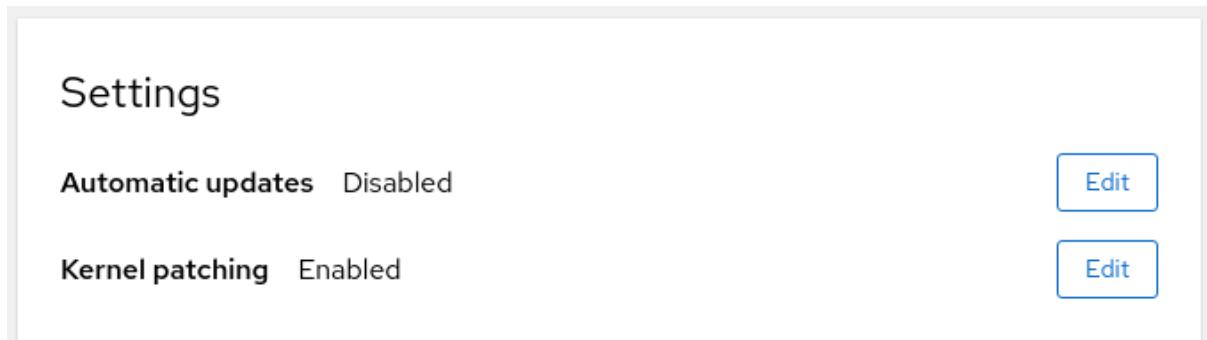
for current and future kernels  
 for current kernel only (5.14.0-20.el9.x86\_64)

**Apply** Cancel

- e. **Apply** をクリックします。

#### 検証

- ソフトウェア更新の 設定 の表で、カーネルパッチが **有効** になっていることを確認します。



**Settings**

**Automatic updates** Disabled Edit

**Kernel patching** Enabled Edit

#### 関連情報

- カーネルライブパッチでパッチの適用

## 第26章 WEB コンソールでサブスクリプションの管理

Web コンソールから Red Hat Enterprise Linux 8 のサブスクリプションを管理します。

Red Hat Enterprise Linux のサブスクリプションを取得するには、[Red Hat カスタマーポータル](#) または アクティベーションキーが必要です。

本章の内容は次のとおりです。

- RHEL 8 Web コンソールを使用したサブスクリプション管理
- Red Hat ユーザー名およびパスワードを使用して、Web コンソールでシステムのサブスクリプション登録
- アクティベーションキーを使用してサブスクリプションを登録

### 前提条件

- サブスクリプションを購入している。
- サブスクリプションの対象となっているシステムが、インターネットに接続している (Web コンソールは Red Hat カスタマーポータルと通信する必要があるため)。

### 26.1. WEB コンソールでサブスクリプションの管理

RHEL 8 Web コンソールは、ローカルシステムにインストールされている Red Hat Subscription Manager を使用するインターフェイスを提供します。

Subscription Manager は Red Hat カスタマーポータルに接続し、利用可能な次のものをすべて確認します。

- アクティブなサブスクリプション
- 期限が切れたサブスクリプション
- 更新されたサブスクリプション

Red Hat カスタマーポータルでサブスクリプションを更新したり、別のサブスクリプションを入手したい場合に、Subscription Manager のデータを手動で更新する必要はありません。サブスクリプションマネージャーは、Red Hat カスタマーポータルと自動的に同期します。

### 26.2. WEB コンソールで認証情報を使用してサブスクリプションを登録

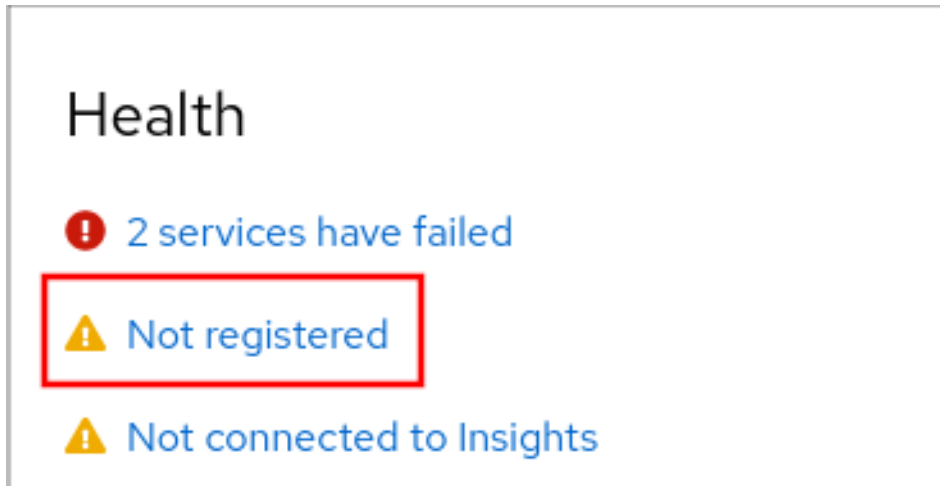
RHEL Web コンソールを使用して、新しくインストールされた Red Hat Enterprise Linux をアカウント認証情報で登録するには、次の手順を使用します。

#### 前提条件

- Red Hat カスタマーポータルに有効なユーザーアカウントがある。  
[Red Hat アカウントの作成](#) ページを参照してください。
- RHEL システムに使用するアクティブなサブスクリプションがある。

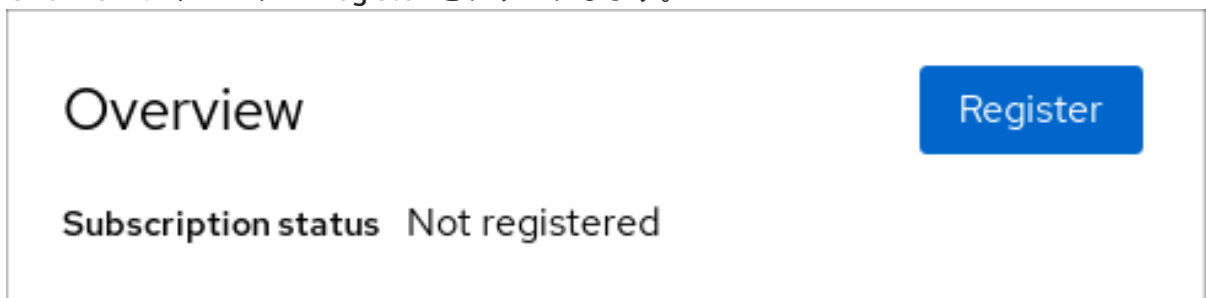
#### 手順

1. RHEL Web コンソールにログインします。詳細は、[Web コンソールへのログイン](#) を参照してください。
2. 概要 ページのヘルス ファイル内の **未登録** の警告をクリックするか、メインメニューの **サブスクリプション** をクリックして、サブスクリプション情報のあるページに移動します。



をクリックします。

3. Overview フィールドの **Register** をクリックします。



4. システムの登録 ダイアログボックスで、アカウント情報での登録を選択します。

5. ユーザー名を入力します。
6. パスワードを入力します。
7. オプションで、組織名または ID を入力します。  
アカウントが Red Hat カスタマーポータルで複数の組織に所属している場合には、組織名または組織 ID を追加する必要があります。組織 ID は、Red Hat の連絡先に問い合わせてください。
  - Red Hat Insights にシステムを接続しない場合は、**Insights** チェックボックスのチェックを外してください。
8. **登録** ボタンをクリックします。

この時点で、Red Hat Enterprise Linux システムが正常に登録されました。

### 26.3. WEB コンソールでアクティベーションキーを使用してサブスクリプションを登録

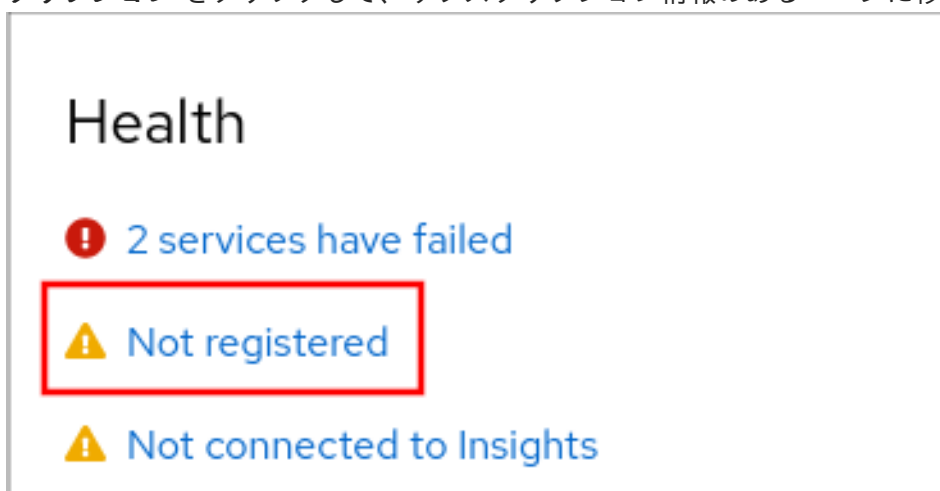
RHEL Web コンソールを使用して、新しくインストールされた Red Hat Enterprise Linux をアクティベーションキーで登録するには、次の手順を使用します。

#### 前提条件

- ポータルにユーザーアカウントがない場合は、ベンダーからアクティベーションキーが提供されます。

#### 手順

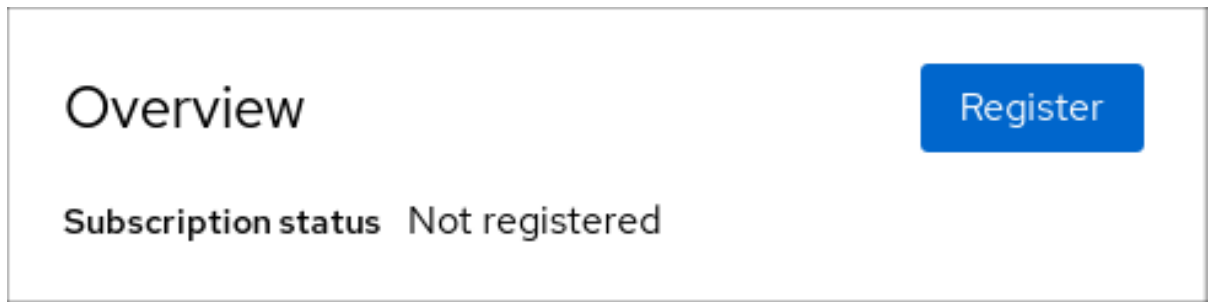
1. RHEL Web コンソールにログインします。詳細は、[Web コンソールへのログイン](#) を参照してください。
2. **概要** ページの **ヘルス** ファイル内の **未登録** の警告をクリックするか、メインメニューの **サブスクリプション** をクリックして、サブスクリプション情報のあるページに移動します。



す。

をクリックしま

3. **Overview** フィールドの **Register** をクリックします。



4. システムの登録 ダイアログボックスで、アクティベーションキーを使用した登録を選択します。

The "Register System" dialog box contains the following fields and options:

- URL:** A dropdown menu with "Default" selected.
- Use proxy server
- Method:** Radio buttons for "Account" and "Activation key". The "Activation key" option is selected and highlighted with a red box.
- Activation Key:** A text input field containing "key\_one,key\_two".
- Organization:** An empty text input field.
- Subscriptions:**  Attach automatically
- Insights:**  Connect this system to [Red Hat Insights](#)

At the bottom of the dialog are two buttons: "Register" (blue) and "Cancel" (grey).

5. キーを入力します。
6. 組織名または ID を入力します。  
組織 ID の取得は、Red Hat にお問い合わせください。
  - Red Hat Insights にシステムを接続しない場合は、**Insights** チェックボックスのチェックを外してください。
7. **登録** ボタンをクリックします。

この時点で、Red Hat Enterprise Linux システムが正常に登録されました。

## 第27章 WEB コンソールで KDUMP の設定

RHEL 9 Web コンソールを使用して、**kdump** 設定をセットアップおよびテストできます。Web コンソールでは、起動時に **kdump** サービスを有効にすることができます。さらに、Web コンソールを使用すると、**kdump** 用に予約されたメモリーを設定し、**vmcore** の保存場所を非圧縮形式または圧縮形式で選択できます。

### 27.1. WEB コンソールで KDUMP メモリーの使用量およびターゲットの場所を設定

RHEL Web コンソールインターフェイスを使用して、**kdump** カーネルのメモリー予約を設定し、**vmcore** ダンプファイルをキャプチャーするターゲットの場所を指定することもできます。

#### 前提条件

- Web コンソールがインストールされており、アクセス可能である。  
詳細は、[Web コンソールのインストール](#) を参照してください。

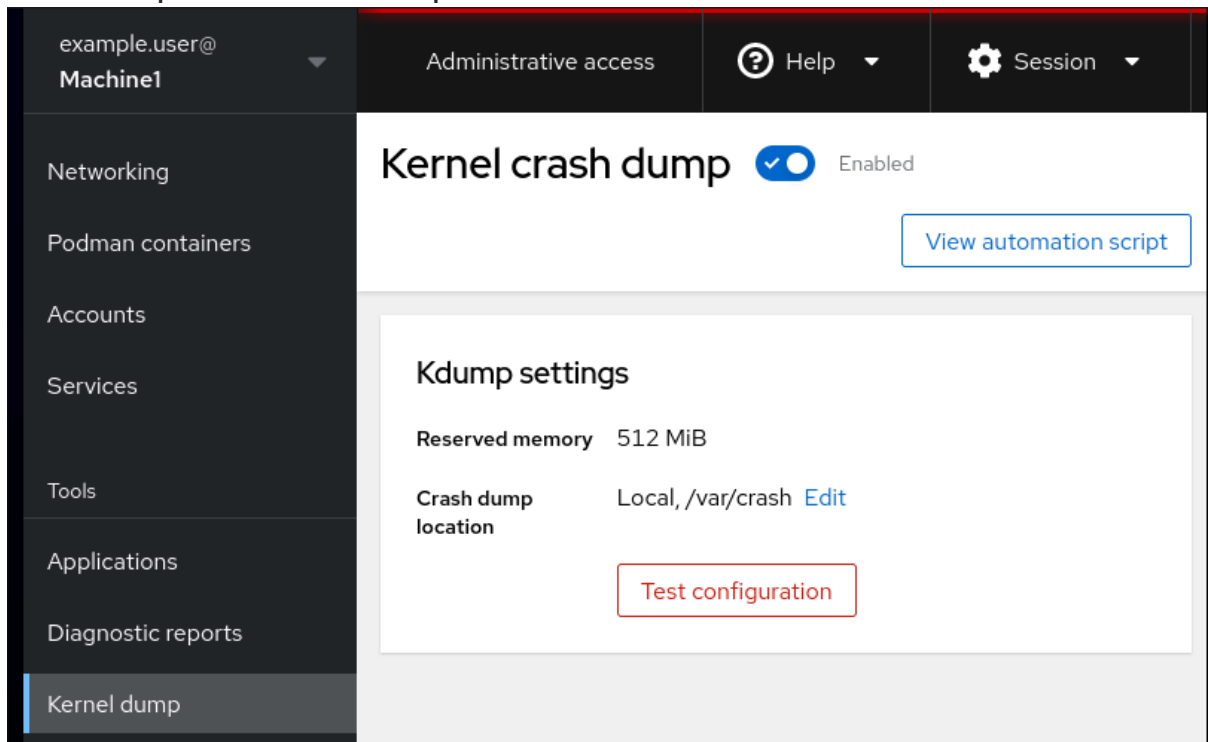
#### 手順

1. Web コンソールで、**Kernel dump** タブを開き、**Kernel crash dump** スイッチをオンに設定して **kdump** サービスを起動します。
2. ターミナルで **kdump** のメモリー使用量を設定します。以下に例を示します。

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

変更を適用するにはシステムを再起動します。

3. **Kernel dump** タブで、**Crash dump location** フィールドの末尾にある **Edit** をクリックします。



4. **vmcore** ダンプファイルを保存するターゲットディレクトリーを指定します。

- ローカルファイルシステムの場合は、ドロップダウンメニューから **Local Filesystem** を選



択します。

### Crash dump location

Location ▼  
Local filesystem

Directory  
/var/crash

Compression  Compress crash dumps to save space

Apply
Cancel

- SSH プロトコルを使用したリモートシステムの場合は、ドロップダウンメニューから **Remote over SSH** を選択し、次のフィールドを指定します。
  - Server フィールドに、リモートサーバーのアドレスを入力します。
  - SSH key フィールドに、SSH キーの場所を入力します。
  - Directory フィールドに、ターゲットディレクトリーを入力します。
- NFS プロトコルを使用したリモートシステムの場合は、ドロップダウンメニューから **Remote over NFS** を選択し、次のフィールドを指定します。
  - Server フィールドに、リモートサーバーのアドレスを入力します。
  - Export フィールドに、NFS サーバーの共有フォルダーの場所を入力します。
  - Directory フィールドに、ターゲットディレクトリーを入力します。



#### 注記

**Compression** チェックボックスをオンにすると、**vmcore** ファイルのサイズを削減できます。

5. **View automation script** をクリックして自動化スクリプトを表示します。  
生成されたスクリプトを含むウィンドウが開きます。シェルスクリプトと Ansible Playbook の生成オプションタブ間を移動できます。
6. オプション: **[クリップボードにコピー]** をクリックしてスクリプトをコピーします。  
このスクリプトを使用すると、複数のマシンに同じ設定を適用できます。

#### 検証

1. **Test configuration** をクリックします。

## Kdump settings

Reserved memory 512 MiB

Crash dump location Local, /var/crash [Edit](#)

[Test configuration](#)

2. Test kdump settings の下にある **Crash system** をクリックします。



### 警告

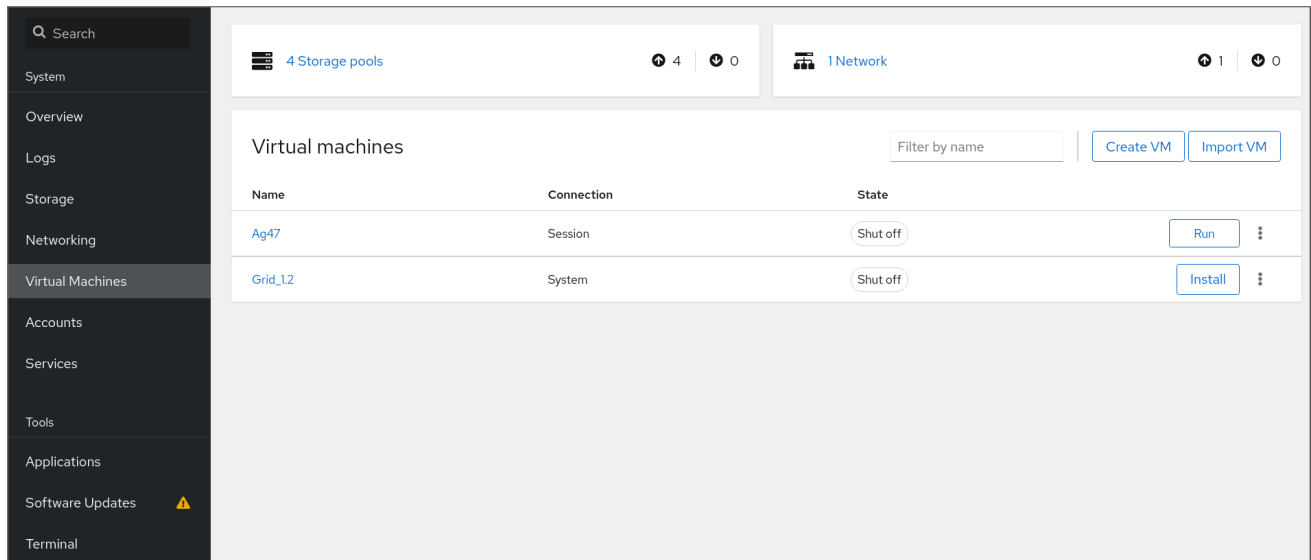
システムクラッシュを開始すると、カーネルの動作が停止し、システムがクラッシュしてデータが失われます。

### 関連情報

- [サポートしている kdump のダンプ出力先](#)

## 第28章 WEB コンソールでの仮想マシンの管理

RHEL 8 ホストのグラフィカルインターフェイスで仮想マシンを管理する場合は、RHEL 8 Web コンソールの **Virtual Machines** ペインを使用できます。



### 28.1. WEB コンソールを使用した仮想マシンの管理の概要

RHEL 8 Web コンソールは、Web ベースのシステム管理インターフェイスです。Web コンソールは、その機能の1つとして、ホストシステムで仮想マシンをグラフィカルに表示してその仮想マシンの作成、アクセス、および設定を可能にします。

Web コンソールを使用して RHEL 8 で仮想マシンを管理するには、最初に、仮想化用の [Web コンソールプラグイン](#) をインストールする必要があります。

#### 次のステップ

- Web コンソールで仮想マシンの管理を有効にする手順は、[Setting up the web console to manage virtual machines](#) を参照してください。
- Web コンソールで利用できる仮想マシン管理アクションの包括的な一覧は、[Web コンソールで利用可能な仮想マシンの管理機能](#) を参照してください。
- Web コンソールでは使用できず、`virt-manager` アプリケーションで利用できる機能のリストは、[Differences between virtualization features in Virtual Machine Manager and the web console](#) を参照してください。

### 28.2. 仮想マシンを管理するために WEB コンソールを設定

Web コンソールの仮想マシン (VM) プラグインをインストールして、RHEL 8 Web コンソールを使用してホストで仮想マシンを管理できるようにしてある。

#### 前提条件

- Web コンソールがマシンにインストールされ、有効化されている。

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

[...]

このコマンドが、**Unit cockpit.socket could not be found** を返す場合は、[Web コンソールのインストールおよび有効化](#) のドキュメントに従って Web コンソール を有効にします。

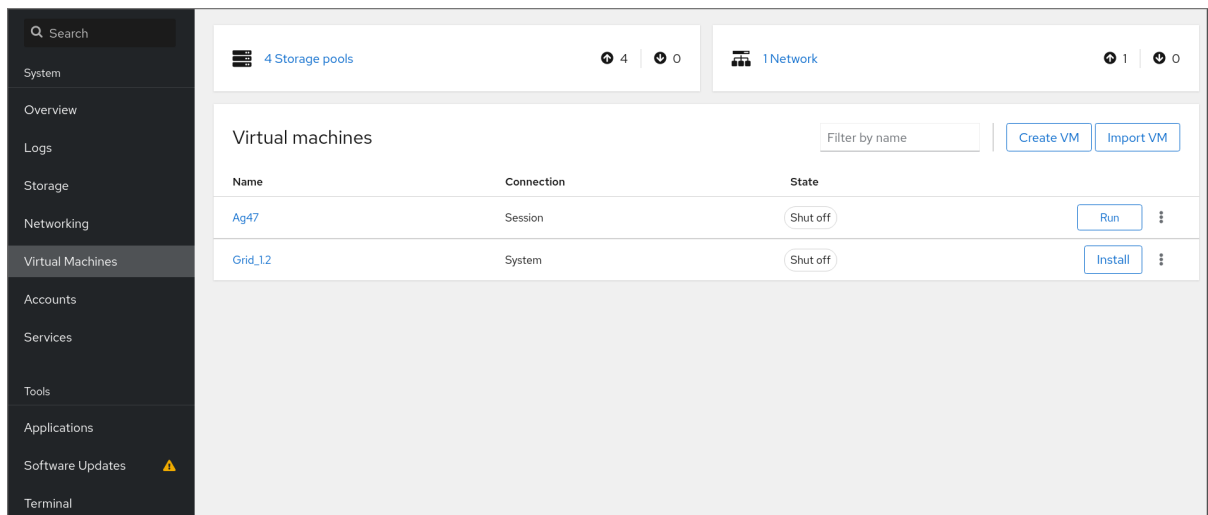
## 手順

- **cockpit-machines** プラグインをインストールします。

```
# yum install cockpit-machines
```

## 検証

1. ブラウザーに **https://localhost:9090** のアドレスを入力するなどして、Web コンソールにアクセスします。
2. ログインします。
3. インストールに成功すると、**仮想マシン** が Web コンソールのサイドメニューに表示されません。



## 関連情報

- [RHEL 9 Web コンソールを使用したシステムの管理](#)

## 28.3. WEB コンソールを使用した仮想マシンの名前の変更

名前の競合を避けるために、またはユースケースに基づいて新しい一意の名前を割り当てるために、既存の仮想マシンの名前を変更することが必要な場合があります。RHEL Web コンソールを使用して仮想マシンの名前を変更できます。

### 前提条件

- Web コンソールの VM プラグインが **システムにインストールされている**。
- 仮想マシンがシャットダウンされている。

## 手順

1. **Virtual Machines** インターフェイスで、名前を変更する仮想マシンのメニューボタン **⋮** をクリックします。  
仮想マシン操作を制御するためのドロップダウンメニューが表示されます。
2. **Rename** をクリックします。  
**Rename a VM** ダイアログが表示されます。

3. **New name** フィールドに、仮想マシンの名前を入力します。
4. **Rename** をクリックします。

#### 検証

- 新しい仮想マシン名が **Virtual Machines** インターフェイスに表示されていることを確認します。

## 28.4. WEB コンソールで利用可能な仮想マシンの管理機能

RHEL 9 Web コンソールを使用すると、システム上の仮想マシンを管理する以下のアクションを実行できます。

表28.1 RHEL 8 Web コンソールで実行できる仮想マシンタスク

| タスク                                | 詳細は、次を参照してください。   |
|------------------------------------|---|
| 仮想マシンの作成およびゲストオペレーティングシステムでのインストール | <a href="#">Web コンソールを使用した仮想マシンの作成、およびゲストのオペレーティングシステムのインストール</a>         |
| 仮想マシンを削除します。                       | <a href="#">Web コンソールを使用した仮想マシンの削除</a>                                    |
| 仮想マシンを起動、シャットダウンし、再起動              | <a href="#">Web コンソールを使用した仮想マシンの起動と Web コンソールを使用した仮想マシンのシャットダウンおよび再起動</a> |
| さまざまなコンソールを使用した仮想マシンへの接続および操作      | <a href="#">Web コンソールを使用した仮想マシンとの相互作用</a>                                 |
| 仮想マシンに関するさまざまな情報の表示                | <a href="#">Web コンソールを使用した仮想マシン情報の表示</a>                                  |

| タスク   | 詳細は、次を参照してください。                     |
|---|-------------------------------------|
| 仮想マシンに割り当てられたホストメモリーの調整                     | Web コンソールを使用した仮想マシンのメモリーの追加および削除    |
| 仮想マシンのネットワーク接続管理                            | Web コンソールで仮想マシンのネットワークインターフェイスの管理   |
| ホストでの利用可能な仮想マシンストレージ管理および仮想ディスクを仮想マシンへの割り当て | 仮想マシン用のストレージの管理                     |
| 仮想マシンの仮想 CPU 設定                             | Web コンソールを使用した仮想 CPU の管理            |
| 仮想マシンのライブマイグレーション                           | Web コンソールを使用した仮想マシンのライブ移行           |
| 仮想マシンの名前変更                                  | Web コンソールを使用した仮想マシンの名前の変更           |
| ホストと VM の間でファイルを共有する                        | ホストとその仮想マシン間でのファイルの共有               |
| ホストデバイスの管理                                  | Web コンソールを使用した仮想デバイスの管理             |
| 仮想光学ドライブを管理する                               | 仮想光学ドライブの管理                         |
| ウォッチドッグデバイスを接続する                            | Web コンソールを使用した仮想マシンへのウォッチドッグデバイスの接続 |

## 28.5. 仮想マシンマネージャーと WEB コンソールでの仮想化機能の相違点

仮想マシンマネージャー (`virt-manager`) は、RHEL 8 で対応していますが、非推奨になっています。後続の主要なリリースでは、Web コンソールがその代替となる予定です。したがって、GUI で仮想化を管理する場合は、Web コンソールを使用することが推奨されます。

ただし、RHEL 8 では、`virt-manager` またはコマンドラインでのみ実行可能な仮想マシン管理タスクがあります。次の表は、`virt-manager` で使用でき、RHEL 8.0 Web コンソールでは使用できない機能を示しています。

この機能は、RHEL 8 の後続のマイナーバージョンで利用可能な場合は、Web コンソールのサポートの列に、最小バージョンの RHEL 8 が表示されます。

表28.2 RHEL 8.0 の Web コンソールを使用して実行できない仮想マシンの管理タスク

| タスク                  | Web コンソールでのサポートが導入されました。 | CLI を使用した代替方法                |
|----------------------|--------------------------|------------------------------|
| ホストの起動時に起動する仮想マシンを設定 | RHEL 8.1                 | <code>virsh autostart</code> |
| 仮想マシンの一時停止           | RHEL 8.1                 | <code>virsh suspend</code>   |

| タスク                                 | Web コンソールでのサポートが導入されました。 | CLI を使用した代替方法                                       |
|-------------------------------------|--------------------------|---|
| 中断している仮想マシンの再開                      | RHEL 8.1                 | <b>virsh resume</b>                                 |
| ファイルシステムディレクトリーストレージプールの作成          | RHEL 8.1                 | <b>virsh pool-define-as</b>                         |
| NFS ストレージプールの作成                     | RHEL 8.1                 | <b>virsh pool-define-as</b>                         |
| 物理ディスクデバイスのストレージプールの作成              | RHEL 8.1                 | <b>virsh pool-define-as</b>                         |
| LVM ボリュームグループストレージプールの作成            | RHEL 8.1                 | <b>virsh pool-define-as</b>                         |
| パーティションベースのストレージプールの作成              | 現在利用不可                   | <b>virsh pool-define-as</b>                         |
| GlusterFS ベースのストレージプールの作成           | 現在利用不可                   | <b>virsh pool-define-as</b>                         |
| SCSI デバイスを使用した vHBA ベースのストレージプールの作成 | 現在利用不可                   | <b>virsh pool-define-as</b>                         |
| マルチパスベースのストレージプールの作成                | 現在利用不可                   | <b>virsh pool-define-as</b>                         |
| RBD ベースのストレージプールの作成                 | 現在利用不可                   | <b>virsh pool-define-as</b>                         |
| ストレージボリュームの新規作成                     | RHEL 8.1                 | <b>virsh vol-create</b>                             |
| 新しい仮想ネットワークの追加                      | RHEL 8.1                 | <b>virsh net-create</b> または <b>virsh net-define</b> |
| 仮想ネットワークの削除                         | RHEL 8.1                 | <b>virsh net-undefine</b>                           |
| ホストマシンのインターフェイスから仮想マシンへのブリッジを作成     | 現在利用不可                   | <b>virsh iface-bridge</b>                           |
| スナップショットの作成                         | 現在利用不可                   | <b>virsh snapshot-create-as</b>                     |
| スナップショットへの復帰                        | 現在利用不可                   | <b>virsh snapshot-revert</b>                        |
| スナップショットの削除                         | 現在利用不可                   | <b>virsh snapshot-delete</b>                        |

| タスク                 | Web コンソールでのサポートが導入されました。 | CLI を使用した代替方法                   |
|---------------------|--------------------------|---------------------------------|
| 仮想マシンのクローン作成        | RHEL 8.4                 | <b>virt-clone</b>               |
| 仮想マシンの別のホストマシンへの移行  | RHEL 8.5                 | <b>virsh migrate</b>            |
| ホストデバイスの仮想マシンへの割り当て | RHEL 8.5                 | <b>virt-xml --add-device</b>    |
| 仮想マシンからのホストデバイスの削除  | RHEL 8.5                 | <b>virt-xml --remove-device</b> |

### 関連情報

- [RHEL 7 で Virtual Machine Manager を使い始める \( RHEL 8 以降では非推奨\)](#)



## 第29章 WEB コンソールでリモートシステムの管理

リモートシステムに接続し、RHEL 8 Web コンソールで管理します。

次の章で以下を説明します。

- 接続したシステムで最適なトポロジー
- リモートシステムを追加および削除する方法
- リモートシステム認証に SSH 鍵を使用する時、理由、および方法
- スマートカードで認証されたユーザーがリモートホストに **SSH** 接続してサービスにアクセスできるように Web コンソールクライアントを設定する方法。

### 前提条件

- リモートシステムで、SSH サービスが開いている。

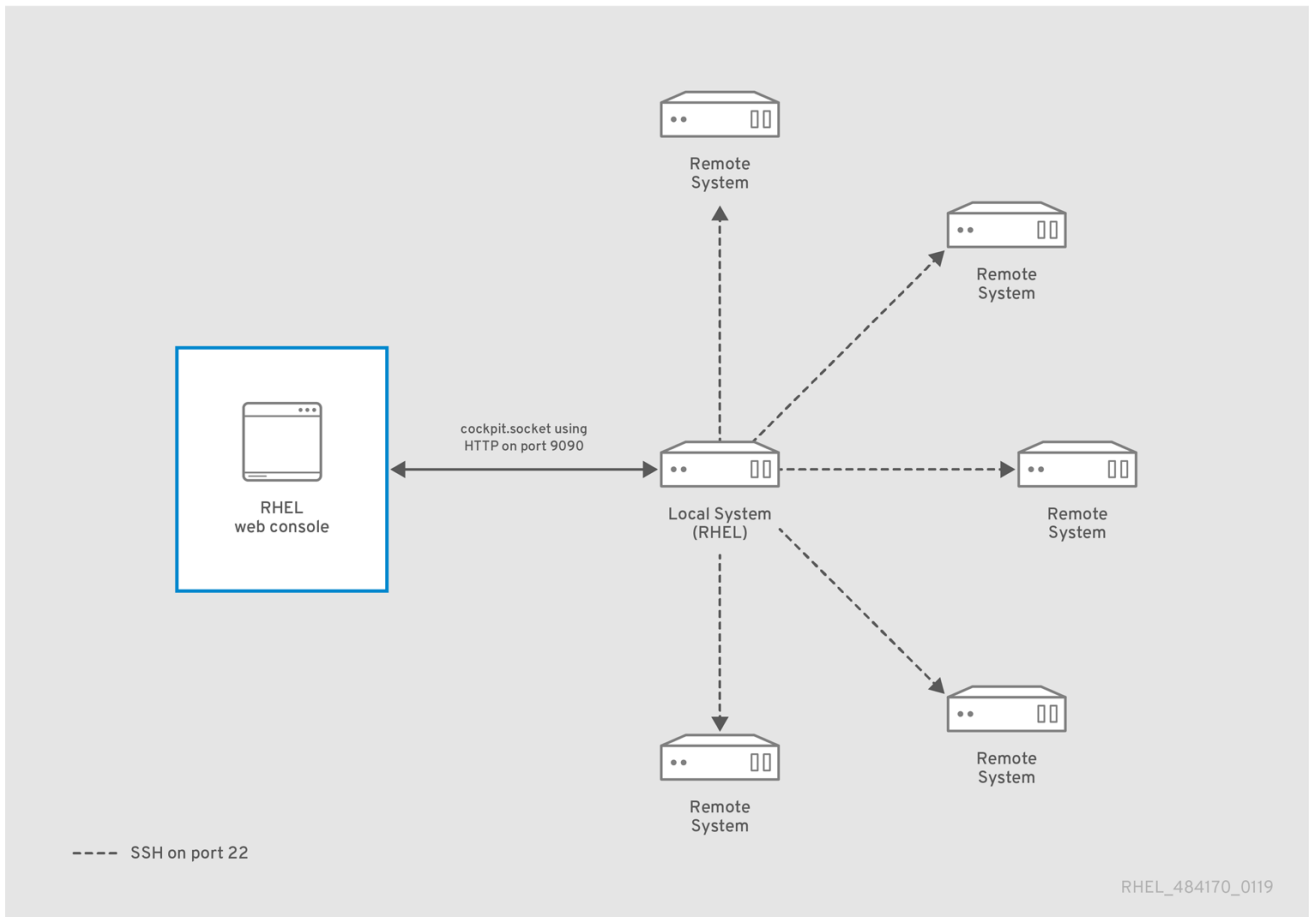
### 29.1. WEB コンソールのリモートシステムマネージャー

ネットワークでリモートシステムを管理する RHEL 8 Web コンソールを使用する場合は、接続したサーバーのトポロジーを考慮する必要があります。

最適なセキュリティーを確保するには、次の接続設定を使用します。

- Web コンソールを使用して、システム1台を要塞ホストとして使用します。要塞ホストは、開いている HTTPS ポートを使用するシステムです。
- その他のすべてのシステムは SSH を介して通信します。

要塞ホストで Web インターフェイスを使用して、デフォルト設定でポート 22 を使用して、SSH プロトコルを介して他のすべてのシステムに到達できます。



## 29.2. WEB コンソールへのリモートシステムの追加

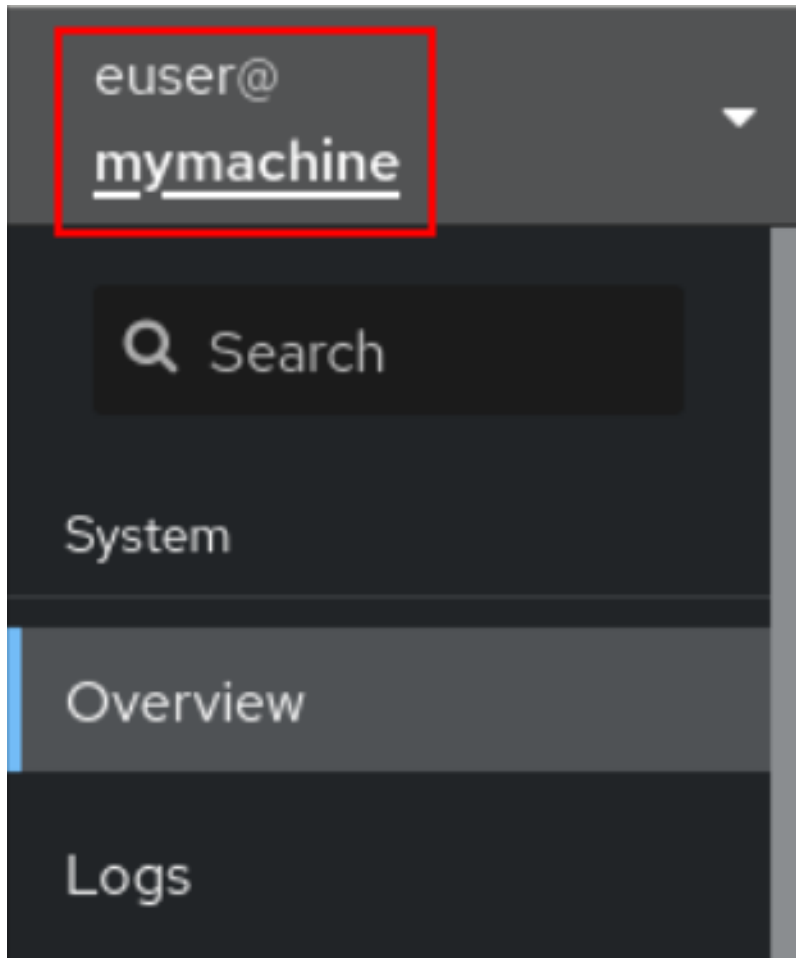
ユーザー名とパスワードを使用して他のシステムに接続できます。

### 前提条件

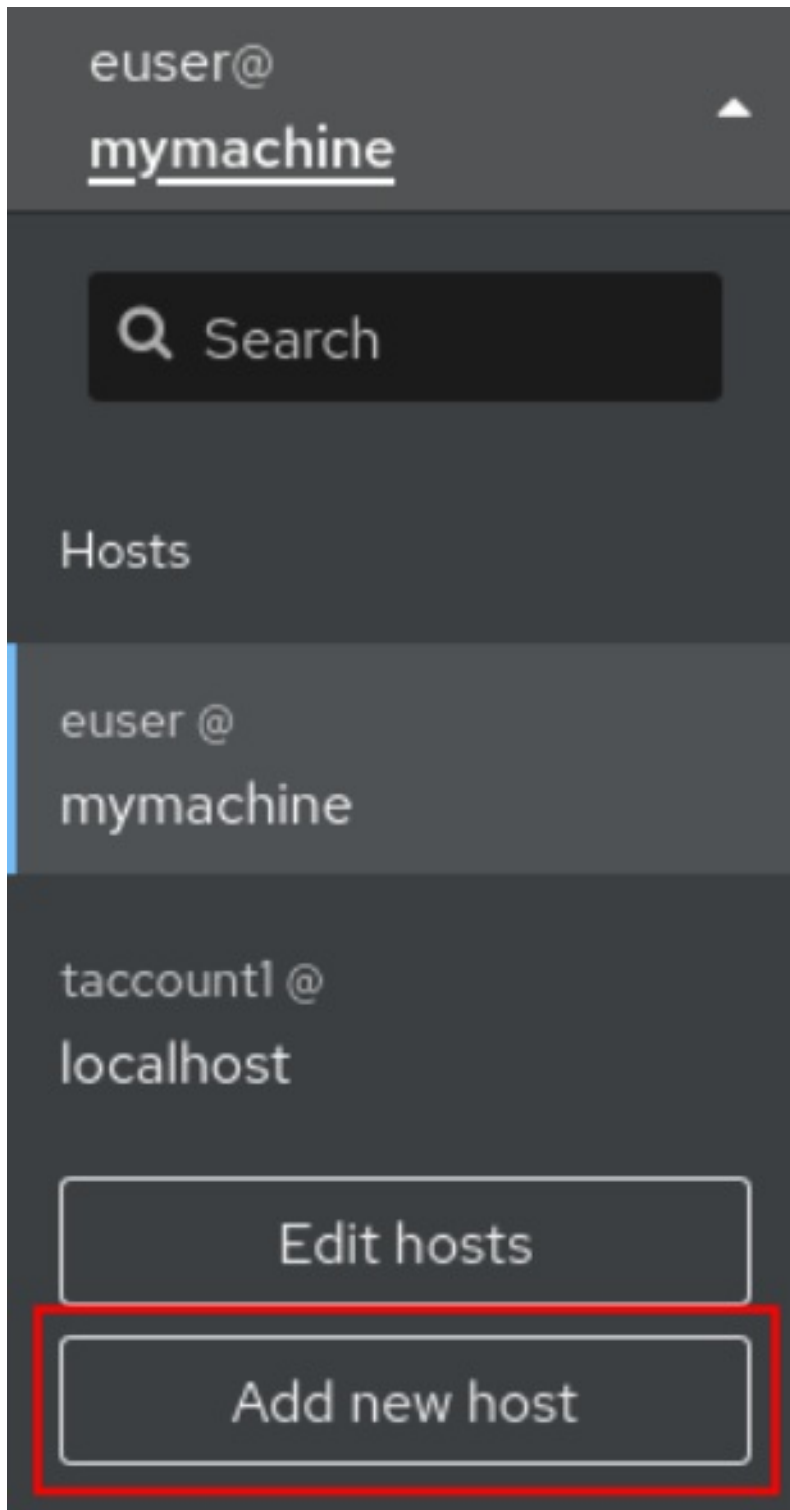
- 管理者権限で Web コンソールにログインしている。詳細は、[Web コンソールへのログイン](#) を参照してください。

### 手順

1. RHEL 8 の Web コンソールで、**Overview** ページの左上にある **username@hostname** をクリックします。



2. ドロップダウンメニューから、**Add new host** ボタンを選択します。

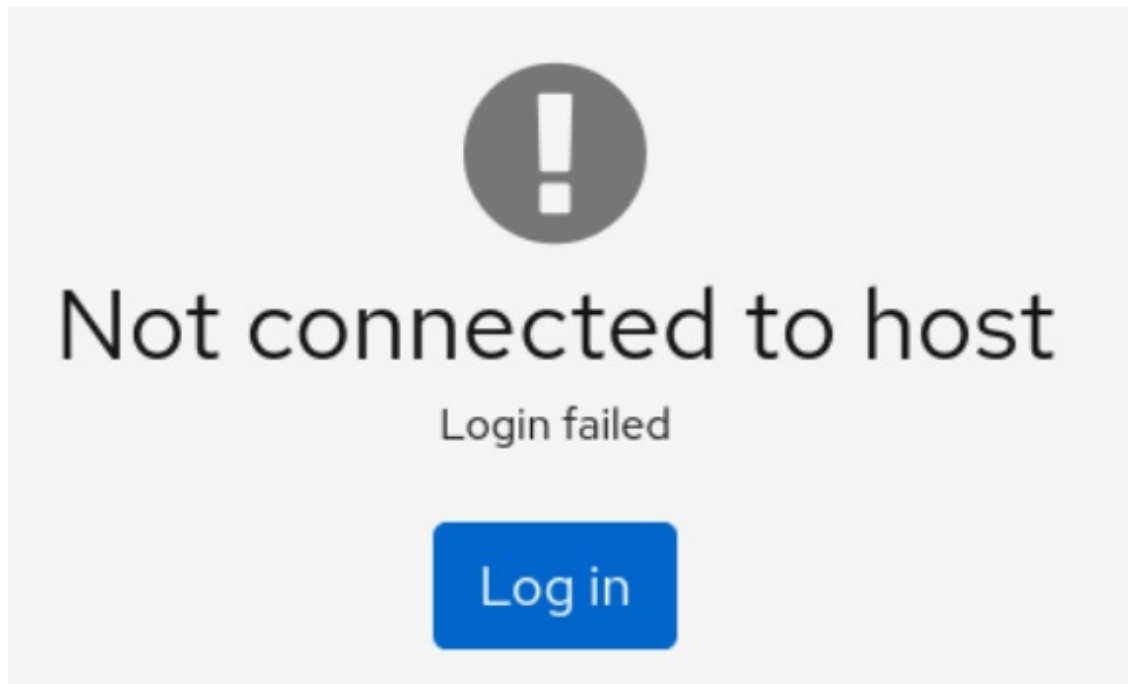


3. **新規ホストの追加** ダイアログボックスで、追加するホストを指定します。
4. (オプション) 接続するアカウントのユーザー名を追加します。  
リモートシステムのユーザーアカウントを使用できます。ただし、管理者権限を持たないユーザーアカウントの認証情報を使用している場合は、管理タスクを実行できません。  
  
ローカルシステムと同じ認証情報を使用する場合は、ログインするたびに、Web コンソールがリモートシステムを自動的に認証します。したがって、複数のマシンで同じ認証情報を使用すると、潜在的なセキュリティーリスクになります。
5. 必要に応じて、色 フィールドをクリックして、システムの色を変更します。
6. Add をクリックします。

新しいホストは、**username@hostname** ドロップダウンメニューのホストリストに表示されます。

### 注記

Web コンソールは、リモートシステムのログインに使用するパスワードを保存しないため、システムが再起動するたびに再度ログインする必要があります。次回のログイン時には、切断されたリモートシステムのメイン画面に配置された **ログイン** ボタンをクリックして、ログインダイアログを開きます。



## 29.3. WEB コンソールでリモートホストの削除

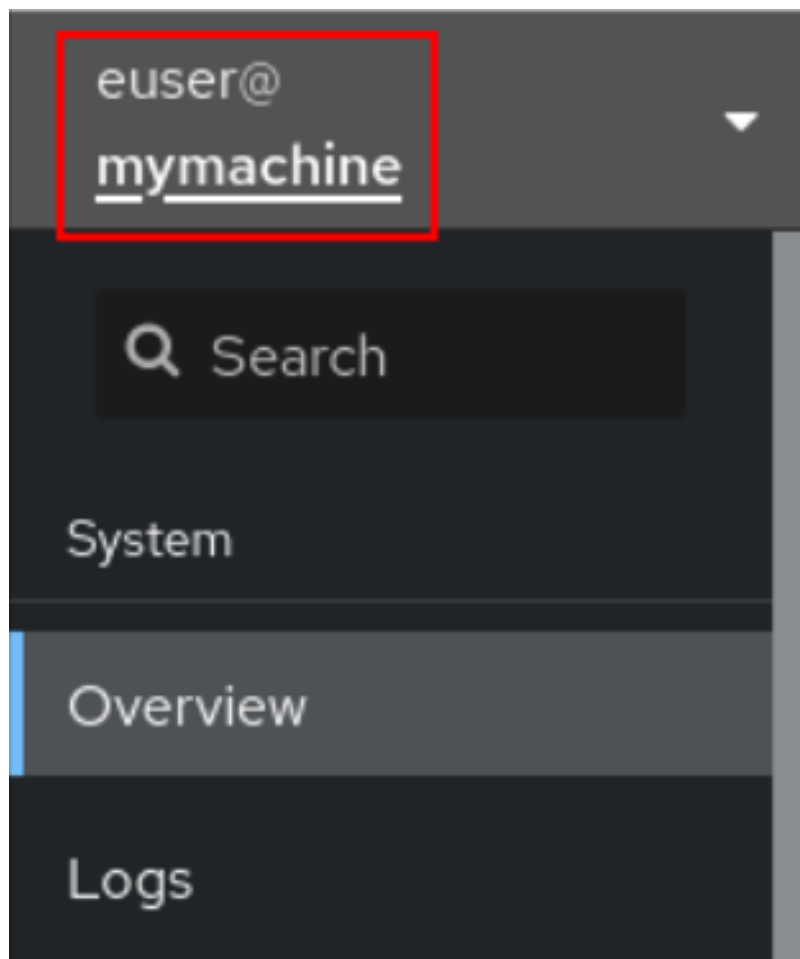
Web コンソールから他のシステムを削除できます。

### 前提条件

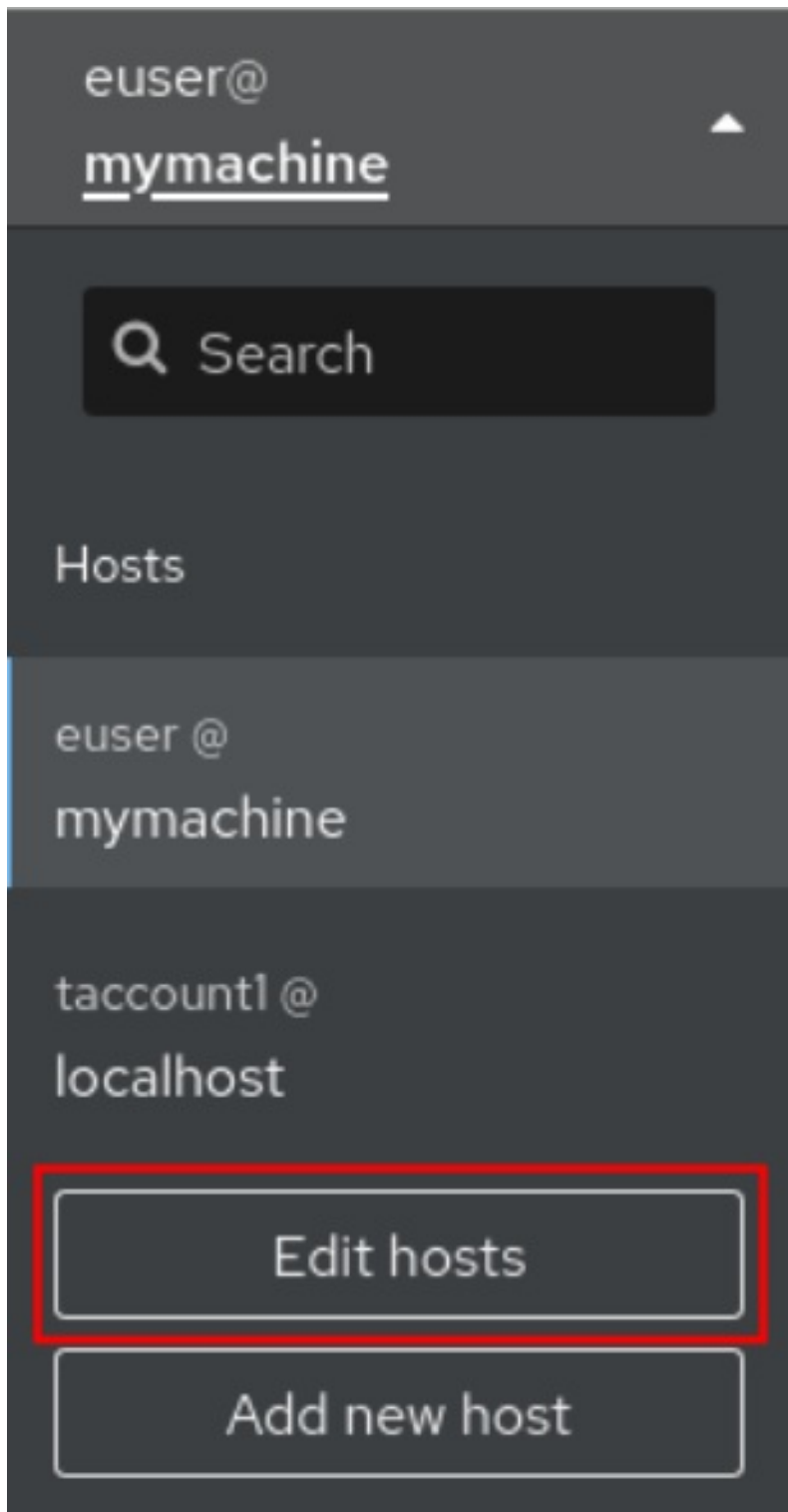
- リモートシステムが追加されている。  
詳細は、「[Web コンソールへのリモートシステムの追加](#)」を参照してください。
- 管理者権限で Web コンソールにログインしている。  
詳細は、「[Web コンソールへのログイン](#)」を参照してください。

### 手順

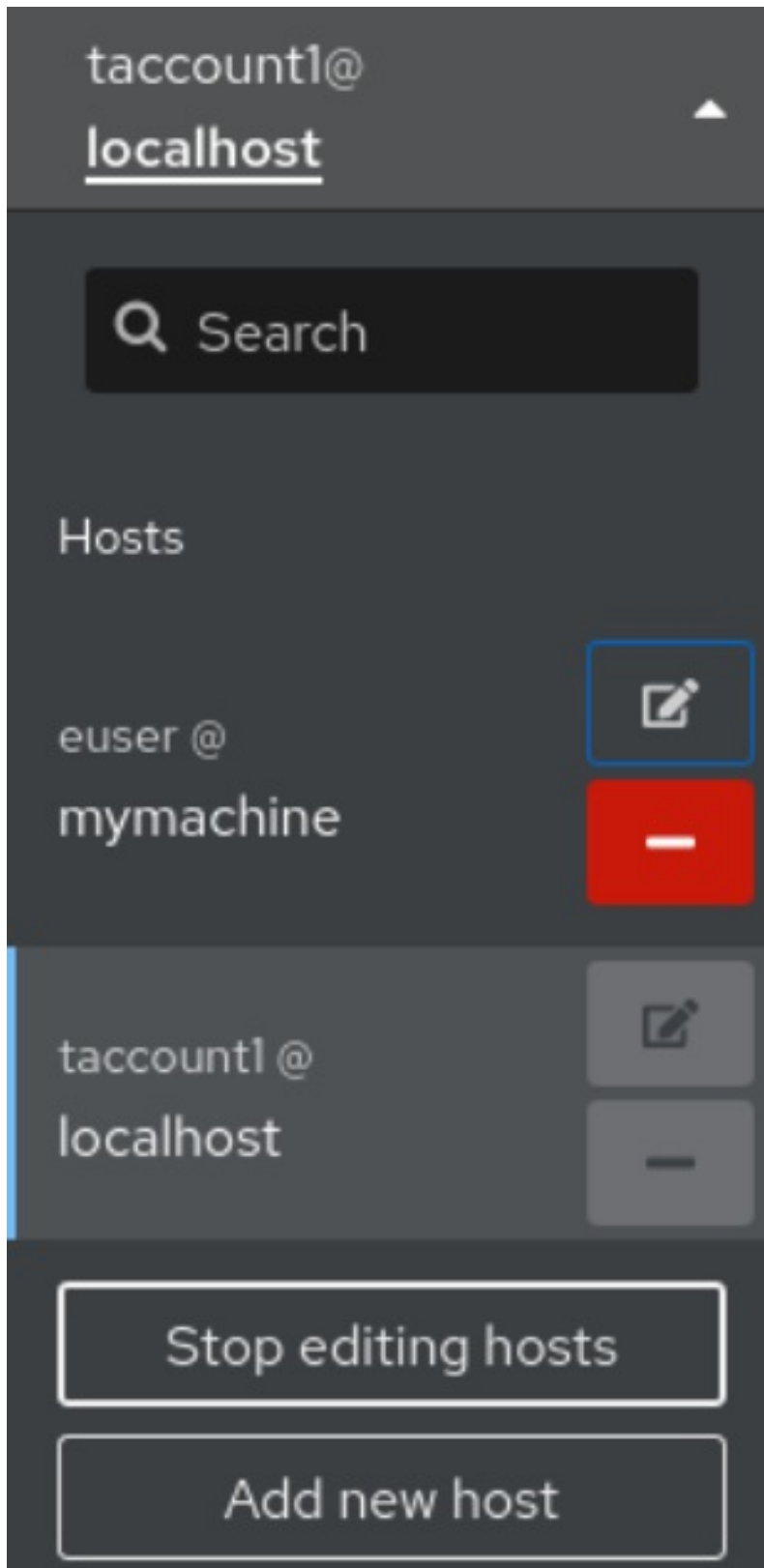
1. RHEL 8 Web コンソールにログインします。
2. **概要** ページの左上にある **username@hostname** をクリックします。



3. **Edit hosts** アイコンをクリックします。



4. Web コンソールからホストを削除するには、対象のホスト名の横にある赤いマイナス記号 - のボタンをクリックします。なお、現在接続中のホストは削除できません。



これにより、そのサーバーはお客様の Web コンソールから削除されます。

#### 29.4. 新しいホストの SSH ログインの有効化

新しいホストを追加するときに、SSH キーを使用してホストにログインすることもできます。システム上にすでに SSH キーがある場合は、Web コンソールは既存のものを使用します。そうでない場合は、Web コンソールはキーを作成できます。

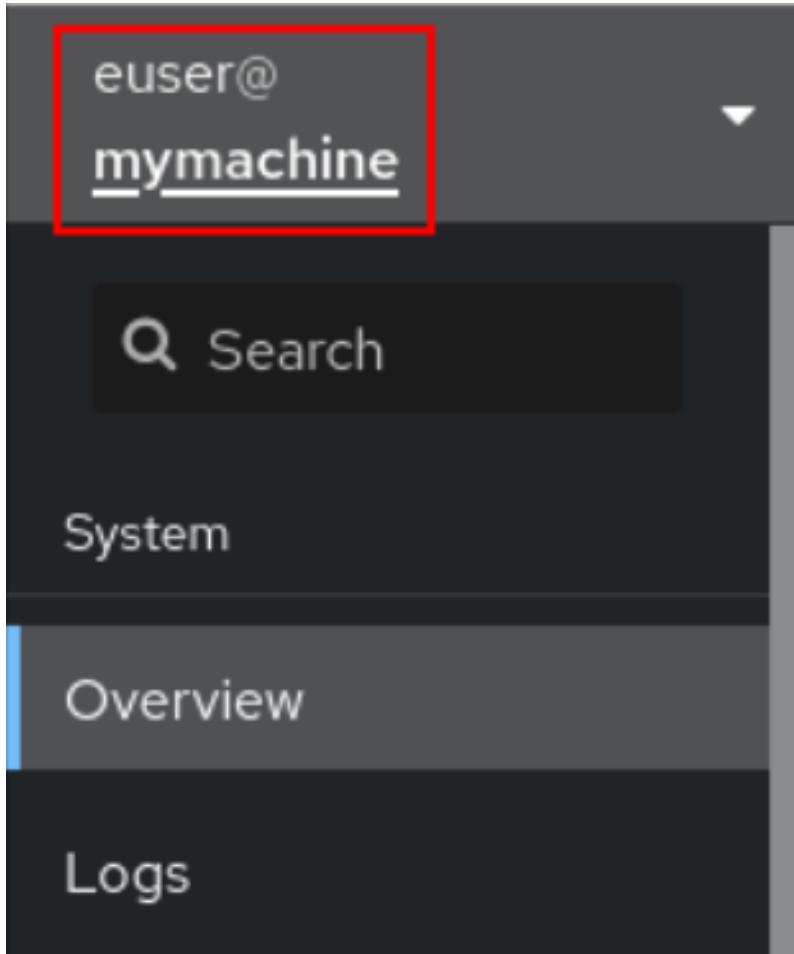
前提条件



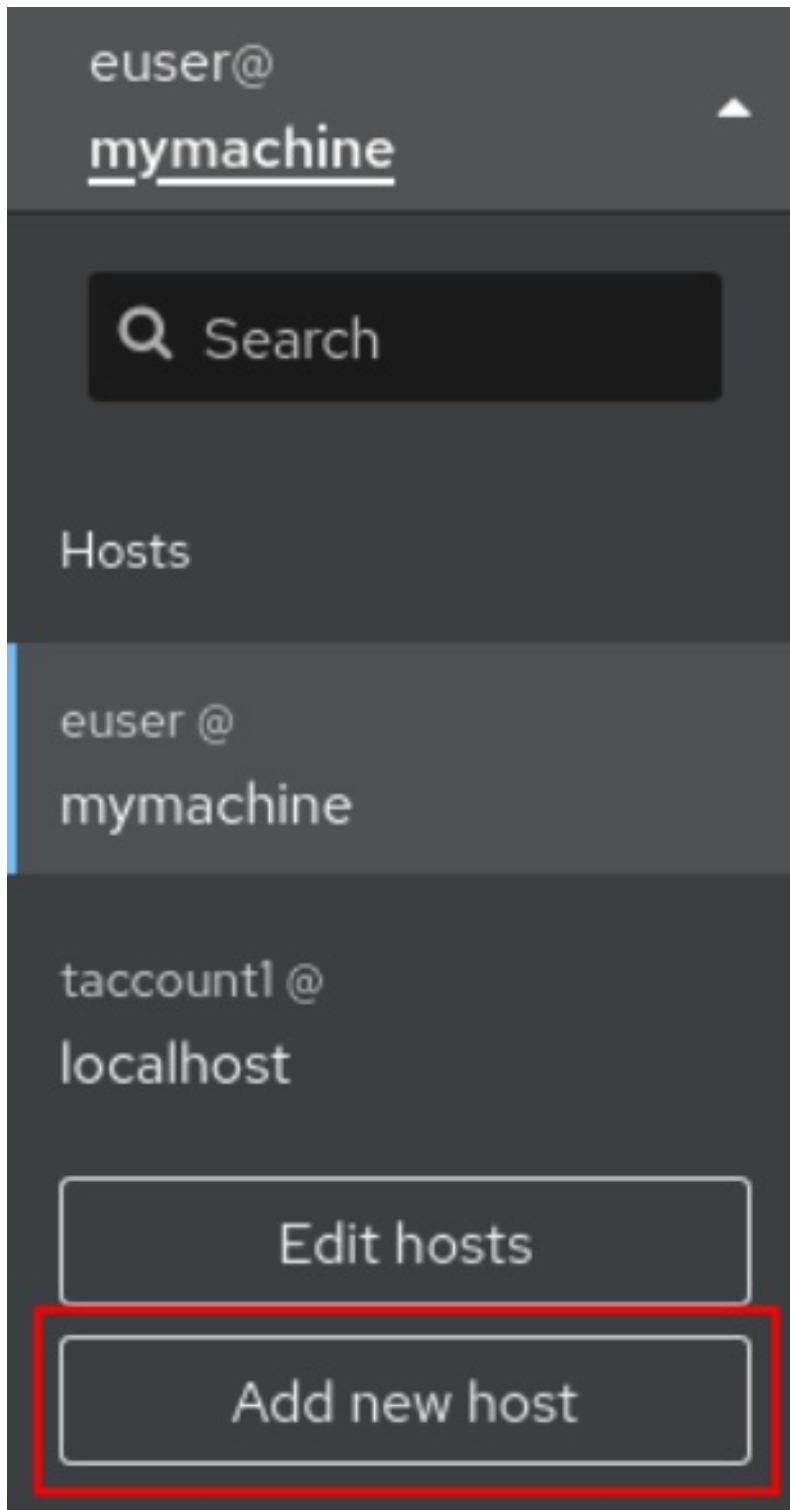
- 管理者権限で Web コンソールにログインしている。  
詳細は、[Web コンソールへのログイン](#) を参照してください。

## 手順

1. RHEL 8 の Web コンソールで、**Overview** ページの左上にある **username@hostname** をクリックします。



2. ドロップダウンメニューから、**Add new host** ボタンを選択します。



3. **新規ホストの追加** ダイアログボックスで、追加するホストを指定します。
4. 接続するアカウントのユーザー名を追加します。  
リモートシステムのユーザーアカウントを使用できます。ただし、管理者権限を持たないユーザーアカウントの認証情報を使用している場合は、管理タスクを実行できません。
5. 必要に応じて、色 フィールドをクリックして、システムの色を変更します。
6. **Add** をクリックします。  
新しいダイアログウィンドウが表示され、パスワードの入力が求められます。
7. ユーザーアカウントのパスワードを入力します。

8. すでに SSH 鍵がある場合は、**Authorize ssh key** にチェックを入れてください。

### Log in to mymachine

Unable to log in to **euser@mymachine** using SSH key authentication. Please provide the password. You may want to set up your SSH keys for automatic login.

Password

Automatic login  Authorize SSH key.

The SSH key `/home/euser/.ssh/id_rsa` of **euser** on **localhost** will be added to the `~/.ssh/authorized_keys` file of **euser** on **mymachine**.

This will allow you to log in without password in the future.

9. SSH 鍵がない場合は、**Create new SSH key and authorize it** にチェックを入れてください。Web コンソールで作成します。

### Log in to mymachine

Unable to log in to **euser@mymachine** using SSH key authentication. Please provide the password. You may want to set up your SSH keys for automatic login.

Password

Automatic login  Create a new SSH key and authorize it.

A new SSH key at `/home/euser/.ssh/id_rsa` will be created for **euser** on **localhost** and it will be added to the `~/.ssh/authorized_keys` file of **euser** on **mymachine**.

Key password

Confirm key password

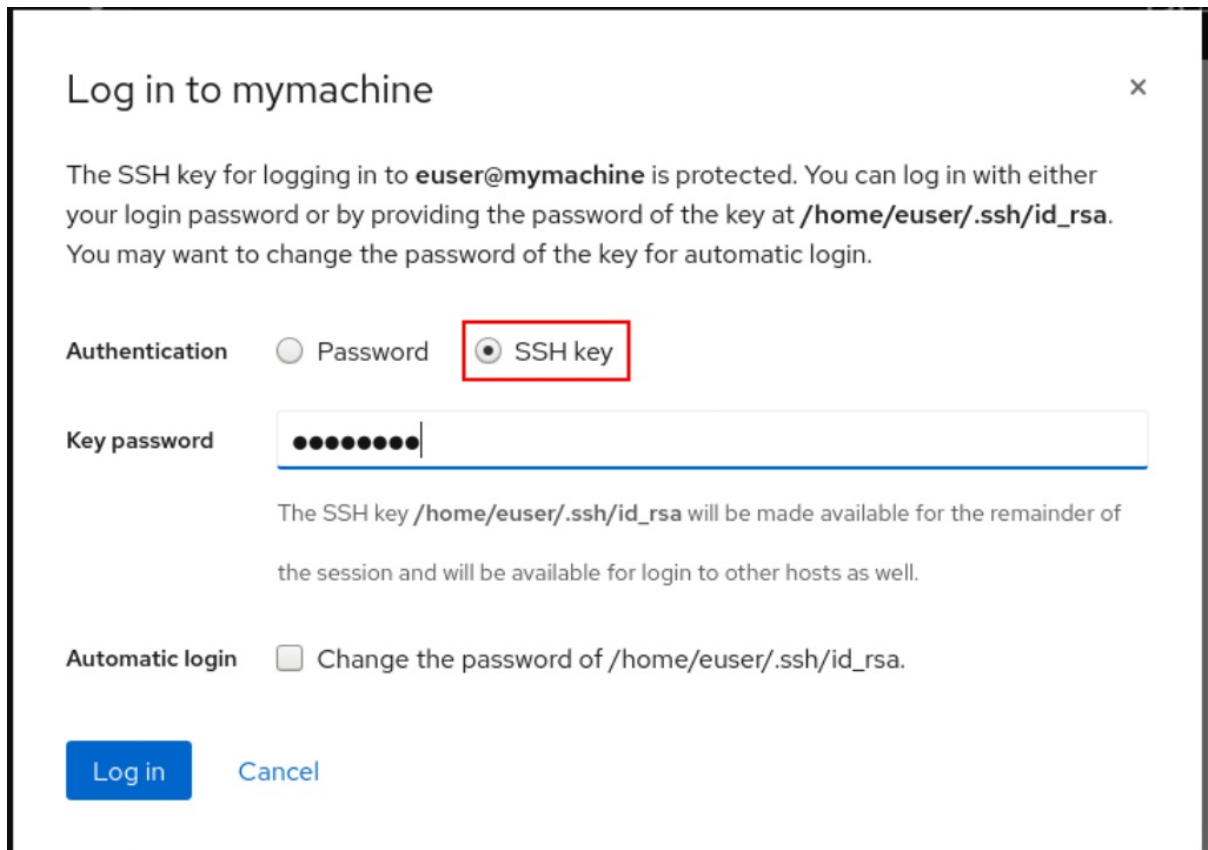
In order to allow log in to **mymachine** as **euser** without password in the future, use the login password of **euser** on **localhost** as the key password, or leave the key password blank.

- a. SSH 鍵のパスワードを追加します。

- b. パスワードを確認します。
10. **Log In** をクリックします。  
新しいホストは、**username@hostname** ドロップダウンメニューのホストリストに表示されます。

#### 検証手順

1. ログアウトします。
2. ログインし直してください。
3. **Not connected to host** 画面の **Log in** をクリックします。
4. 認証オプションとして、**SSH 鍵** を選択します。



Log in to mymachine

The SSH key for logging in to **euser@mymachine** is protected. You can log in with either your login password or by providing the password of the key at `/home/euser/.ssh/id_rsa`. You may want to change the password of the key for automatic login.

Authentication  Password  SSH key

Key password

The SSH key `/home/euser/.ssh/id_rsa` will be made available for the remainder of the session and will be available for login to other hosts as well.

Automatic login  Change the password of `/home/euser/.ssh/id_rsa`.

Log in Cancel

5. 鍵のパスワードを入力します。
6. **Log in** をクリックします。

#### 関連情報

- [2 台のシステム間で OpenSSH を使用した安全な通信の使用](#)

## 29.5. アイデンティティ管理における制約付き委任

Service for User to Proxy (**S4U2proxy**) 拡張機能は、ユーザーに代わって他のサービスに対するサービスチケットを取得するサービスを提供します。この機能は、**制約付き委任**と呼ばれています。2 番目のサービスは通常、ユーザーの承認コンテキストの下で、最初のサービスに代わって何らかの作業を実行するプロキシです。制約付き委任を使用することで、ユーザーが Ticket Granting Ticket (TGT) を完全に委任する必要がなくなります。

Identity Management (IdM) は従来、Kerberos **S4U2proxy** 機能を使用して、Web サーバーフレームワークがユーザーの代わりに LDAP サービスチケットを取得することを可能にするものです。また、IdM-AD の信頼システムも、**cifs** プリンシパルを取得するために制約付き委任を使用しています。

**S4U2proxy** 機能を使用して Web コンソールクライアントを設定し、スマートカードで認証された IdM ユーザーが以下を達成できるようにすることができます。

- Web コンソールサービスが実行されている RHEL ホストで、再度認証を求められることなく、スーパーユーザー権限でコマンドを実行します。
- **SSH** を使用してリモートホストにアクセスし、再度認証を求められることなくホスト上のサービスにアクセスします。

## 関連情報

- [Ansible を使用して Web コンソールを設定し、スマートカードで認証されたユーザーが再認証を求められることなくリモートホストに SSH 接続できるようにする](#)
- [Ansible を使用して Web コンソールを設定し、スマートカードで認証されたユーザーが再認証を求められることなく sudo を実行できるようにする](#)
- [S4U2proxy](#)
- [サービスの制約付き委任](#)

## 29.6. スマートカードで認証されたユーザーが、再度認証を要求されることなくリモートホストに SSH 接続できるようにするための WEB コンソールの設定

RHEL の Web コンソールでユーザーアカウントにログインした後、Identity Management (IdM) システム管理者として、**SSH** プロトコルを使用してリモートマシンに接続する必要がある場合があります。[制約付き委任](#) 機能を使用すると、再度認証を求められることなく **SSH** を使用することができます。

制約付き委任を使用するように Web コンソールを設定するには、次の手順に従います。以下の例では、Web コンソールセッションは `myhost.idm.example.com` ホストで実行され、認証されたユーザーの代わりに **SSH** を使用して `remote.idm.example.com` ホストにアクセスするように設定されています。

### 前提条件

- IdM **admin** Ticket-Granting Ticket (TGT) を取得している
- `remote.idm.example.com` への **root** アクセス権がある
- Web コンソールサービスが IdM に存在する
- `remote.idm.example.com` ホストが IdM に存在する
- Web コンソールは、ユーザーセッションに **S4U2Proxy** Kerberos チケットを作成している。これを確認するために、IdM ユーザーで Web コンソールにログインし、**Terminal** ページを開き、以下を入力します。

```
$ 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
```

## 手順

1. 委任ルールでアクセス可能な対象ホストのリストを作成します。

- a. サービス委任ターゲットを作成します。

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

- b. 委任対象に対象ホストを追加します。

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

2. サービス委任ルールを作成し、**HTTP** サービスの Kerberos プリンシパルを追加することで、**cockpit** セッションが対象ホストのリストにアクセスできるようにします。

- a. サービス委任ルールを作成します。

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

- b. Web コンソールクライアントを委任ルールに追加します。

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

- c. 委任対象を委任ルールに追加します。

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

3. `remote.idm.example.com` ホストで Kerberos 認証を有効にします。

- a. **root** として `remote.idm.example.com` に **SSH** 接続します。

- b. `/etc/ssh/sshd_config` ファイルを開いて編集します。

- c. **GSSAPIAuthentication no** 行のコメントを外し、**GSSAPIAuthentication yes** に置き換えて、**GSSAPIAuthentication** を有効にします。

4. 上記の変更がすぐに有効になるように、`remote.idm.example.com` の **SSH** サービスを再起動します。

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

## 関連情報

- スマートカードを使用して Web コンソールへのログイン
- アイデンティティ管理における制約付き委任

## 29.7. ANSIBLE を使用して WEB コンソールを設定し、スマートカードで認証されたユーザーが再認証を求められことなくリモートホストに SSH 接続できるようにする

RHEL の Web コンソールでユーザーアカウントにログインした後、Identity Management (IdM) システム管理者として、SSH プロトコルを使用してリモートマシンに接続する必要がある場合があります。制約付き委任機能を使用すると、再度認証を求められことなく SSH を使用することができます。

`servicedelegationrule` および `servicedelegationtarget ansible-freeipa` モジュールを使用して、制約付き委任を使用するように Web コンソールを設定するには、この手順に従います。以下の例では、Web コンソールセッションは `myhost.idm.example.com` ホストで実行され、認証されたユーザーの代わりに SSH を使用して `remote.idm.example.com` ホストにアクセスするように設定されています。

### 前提条件

- IdM `admin` パスワードがある
- `remote.idm.example.com` への `root` アクセスがある
- Web コンソールサービスが IdM に存在する
- `remote.idm.example.com` ホストが IdM に存在する
- Web コンソールは、ユーザーセッションに `S4U2Proxy` Kerberos チケットを作成している。これを確認するために、IdM ユーザーで Web コンソールにログインし、`Terminal` ページを開き、以下を入力します。

```
$ 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
```

- 次の要件を満たすように Ansible コントロールノードを設定している。
  - Ansible バージョン 2.14 以降を使用している。
  - Ansible コントローラーに `ansible-freeipa` パッケージがインストールされている。
  - この例では、`~/MyPlaybooks/` ディレクトリーに、IdM サーバーの完全修飾ドメイン名 (FQDN) を使用して `Ansible インベントリーファイル` を作成したことを前提としている。
  - この例では、`secret.yml` Ansible vault に `ipadmin_password` が保存されていることを前提としています。

- ターゲットノード (**ansible-freeipa** モジュールが実行されるノード) が、IdM クライアント、サーバー、またはレプリカとして IdM ドメインに含まれている。

## 手順

1. ~/MyPlaybooks/ ディレクトリーに移動します。

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

2. 以下の内容で **web-console-smart-card-ssh.yml** Playbook を作成します。
  - a. 委任対象の存在を確認するタスクを作成します。

```
---
- 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:
      ipadmin_password: "{{ ipadmin_password }}"
      name: web-console-delegation-target
```

- b. 対象ホストを委任ターゲットに追加するタスクを追加します。

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

- c. 委任ルールの存在を確認するタスクを追加します。

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

- d. Web コンソールクライアントサービスの Kerberos プリンシパルが制約付き委任ルールのメンバーであることを確認するタスクを追加します。

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



- e. 制約付き委任ルールが web-console-delegation-target 委任対象と関連付けられることを確認するタスクを追加します。

```
- 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. ファイルを保存します。
4. Ansible Playbook を実行します。Playbook ファイル、**secret.yml** ファイルを保護するパスワードを格納するファイル、およびインベントリーファイルを指定します。

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

5. **remote.idm.example.com** で Kerberos 認証を有効にします。
  - a. **root** として **remote.idm.example.com** に **SSH** 接続します。
  - b. **/etc/ssh/sshd\_config** ファイルを開いて編集します。
  - c. **GSSAPIAuthentication no** 行のコメントを外し、**GSSAPIAuthentication yes** に置き換えて、**GSSAPIAuthentication** を有効にします。

## 関連情報

- [スマートカードを使用して Web コンソールへのログイン](#)
- [アイデンティティ管理における制約付き委任](#)
- **/usr/share/doc/ansible-freeipa/** ディレクトリーの **README-servicedelegationrule.md** および **README-servicedelegationtarget.md**
- **/usr/share/doc/ansible-freeipa/playbooks/servicedelegationtarget** および **/usr/share/doc/ansible-freeipa/playbooks/servicedelegationrule** ディレクトリーのサンプル Playbook

## 第30章 IDM ドメインで RHEL 8 WEB コンソールにシングルサインオンを設定

RHEL 8 Web コンソールでの Identity Management (IdM) が提供する SSO (シングルサインオン) 認証を使用する方法を学びます。

利点:

- IdM ドメインの管理者は、RHEL 8 Web コンソールを使用して、ローカルマシンを管理できます。
- IdM ドメインで Kerberos チケットを使用すると、Web コンソールにアクセスする際にログイン認証情報を指定する必要がなくなりました。
- IdM ドメインが認識しているすべてのホストは、RHEL 8 Web コンソールのローカルインスタンスから SSH 経由でアクセスできます。
- 証明書設定は必須ではありません。コンソールの Web サーバーでは、IdM 認証局が発行した証明書に自動的に切り替わり、ブラウザーに許可されます。

本章は、RHEL Web コンソールにログインするために SSO を設定する手順を説明します。

1. RHEL 8 Web コンソールを使用して IdM ドメインにマシンを追加します。  
詳細は、[Joining a RHEL 8 system to an IdM domain using the web console](#) を参照してください。
2. 認証に Kerberos を使用する場合は、マシンで Kerberos チケットを取得する必要があります。  
詳細は、[Kerberos 認証を使用した Web コンソールへのログイン](#) を参照してください。
3. IdM サーバーの管理者が、任意のホストで任意のコマンドを実行できます。  
詳細は、[Enabling admin sudo access to domain administrators on the IdM server](#) を参照してください。

### 前提条件

- RHEL Web コンソールが RHEL 8 システムにインストールされている。  
詳細は、[Web コンソールのインストールおよび有効化](#) を参照してください。
- RHEL Web コンソールを使用して IdM クライアントがシステムにインストールされている。  
詳細は [IdM クライアントのインストール](#) を参照してください。

### 30.1. WEB コンソールを使用した RHEL 8 システムの IDM ドメインへの参加

Web コンソールを使用して、Red Hat Enterprise Linux 8 システムを Identity Management (IdM) ドメインに参加させることができます。

#### 前提条件

- IdM ドメインが実行中で参加するクライアントから到達可能
- IdM ドメインの管理者認証情報がある。

#### 手順

1. RHEL Web コンソールにログインします。  
詳細は、[Web コンソールへのログイン](#) を参照してください。
2. **Overview** タブの **Configuration** フィールドで、**Join Domain** をクリックします。
3. **ドメイン参加** ダイアログボックスの **ドメインアドレス** フィールドに、IdM サーバーのホスト名を入力します。
4. **ドメイン管理者名** フィールドで、IdM 管理アカウントのユーザー名を入力します。
5. **Domain administrator password** にパスワードを追加します。
6. **参加** をクリックします。

### 検証手順

1. システムが IdM ドメインに参加していると、RHEL 8 Web コンソールにエラーが表示されず、**システム** 画面でドメイン名を確認できます。
2. ユーザーがドメインのメンバーであることを確認するには、**Terminal** ページをクリックし、**id** コマンドを実行します。

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

### 関連情報

- [Identity Management の計画](#)
- [Identity Management のインストール](#)
- [IdM ユーザー、グループ、ホスト、およびアクセス制御ルールの管理](#)

## 30.2. KERBEROS 認証を使用して WEB コンソールにログイン

次の手順は、Kerberos 認証を使用するように RHEL 8 システムを設定する方法を説明します。



### 重要

SSO を使用した場合は、通常、Web コンソールに管理者権限がありません。これは、パスワードがない `sudo` を設定した場合に限り機能します。Web コンソールは、対話的に `sudo` パスワードを要求しません。

### 前提条件

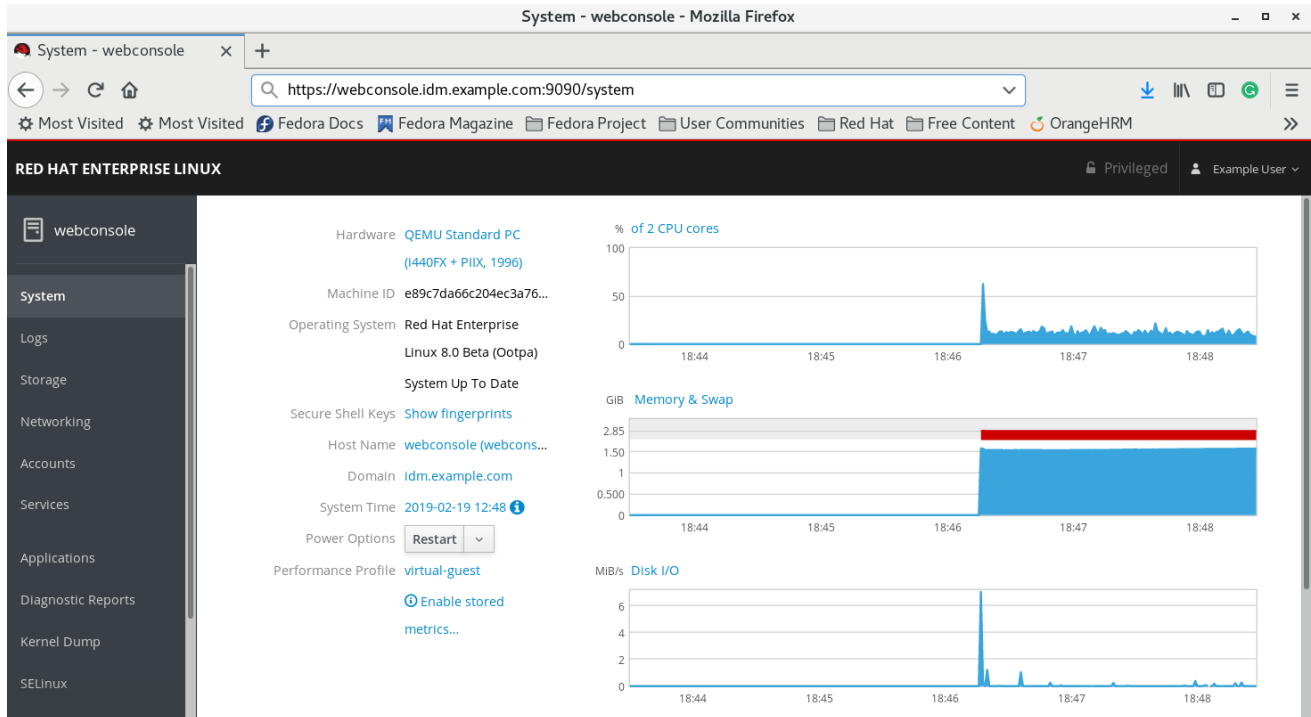
- 稼働中で、会社の環境で到達可能な IdM ドメイン  
詳細は、[Joining a RHEL 8 system to an IdM domain using the web console](#) を参照してください。
- リモートシステムで、RHEL Web コンソールで接続して管理する **cockpit.socket** サービスを有効にしている。  
詳細は、[Web コンソールのインストール](#) を参照してください。

- システムが、SSSD クライアントが管理する Kerberos チケットを使用しない場合は、**kinit** ユーティリティを使用して手動でチケットを要求してみる。

## 手順

[https://dns\\_name:9090](https://dns_name:9090) から、RHEL Web コンソールにログインします。

この時点で、RHEL Web コンソールへの接続に成功しており、設定を開始できます。



## 30.3. 管理者の SUDO で IDM サーバーのドメイン管理者にアクセス可能に

RHEL Web コンソールを使用すると、ドメイン管理者が Identity Management (IdM) ドメイン内の任意のホストで任意のコマンドを使用できるようにすることができます。

これを可能にするために、IdM サーバーのインストール時に自動的に作成された **admins** ユーザーグループに **sudo** がアクセスできるようにします。グループで **ipa-advise** スクリプトを実行すると、**admins** グループに追加されたすべてのユーザーに **sudo** アクセス権が付与されます。

### 前提条件

- サーバーが、IdM 4.7.1 以降を実行している。

### 手順

- IdM サーバーに接続します。
- `ipa-advise` スクリプトを実行します。

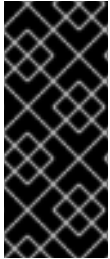
```
$ ipa-advise enable-admins-sudo | sh -ex
```

コンソールにエラーが表示されない場合、**admins** グループには IdM ドメイン内のすべてのマシンに対する **sudo** 権限があります。

## 第31章 集中管理ユーザー向けに WEB コンソールを使用したスマートカード認証の設定

RHEL Web コンソールでスマートカード認証を集中管理しているユーザーに設定します。

- Identity Management
- Identity Management を使用してフォレスト間の信頼に接続する Active Directory



### 重要

Smart card authentication does not elevate administrative privileges yet and the web console opens in the web browser in the read-only mode.

You can run administrative commands in the built-in terminal with ``sudo``.

### 前提条件

- スマートカード認証を使用するシステムは、Active Directory または Identity Management ドメインのメンバーである必要があります。  
Web コンソールを使用して RHEL 8 システムをドメインに参加させる方法は [Web コンソールで RHEL 8 システムを IdM ドメインに参加](#) を参照してください。
- スマートカード認証に使用される証明書は、Identity Management または Active Directory の特定のユーザーに関連付けられている必要があります。  
Identity Management のユーザーと証明書の関連付けの詳細は、[Adding a certificate to a user entry in the IdM Web UI](#) または [Adding a certificate to a user entry in the IdM CLI](#) を参照してください。

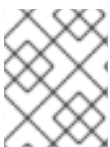
### 31.1. 集中管理ユーザーのスマートカード認証

スマートカードは、カードに保存されている証明書を使用して個人認証を提供できる物理デバイスです。個人認証とは、ユーザーパスワードと同じ方法でスマートカードを使用できることを意味します。

秘密鍵と証明書の形式で、スマートカードにユーザーの認証情報を保存できます。特別なソフトウェアおよびハードウェアを使用して、そのソフトウェアにアクセスします。スマートカードをリーダーまたは USB ソケットに挿入して、パスワードを入力する代わりに、スマートカードの PIN コードを入力します。

Identity Management (IdM) では、以下によるスマートカード認証に対応しています。

- IdM 認証局が発行するユーザー証明書。詳細は、[スマートカード認証用の Identity Management の設定](#) を参照してください。
- Active Directory Certificate Service (ADCS) 認証局が発行するユーザー証明書。詳細は [IdM でスマートカード認証用に ADCS が発行した証明書の設定](#) を参照してください。



### 注記

スマートカード認証の使用を開始する場合は、ハードウェア要件 [Smart Card support in RHEL8+](#) を参照してください。

## 31.2. スマートカードを管理および使用するツールのインストール

### 前提条件

- **gnutls-utils** パッケージがインストールされている。
- **opensc** パッケージがインストールされている。
- **pcscd** サービスを実行している。

スマートカードを設定する前に、対応するツール (証明書を生成して **pcscd** サービスを起動できるもの) をインストールする必要があります。

### 手順

1. **opensc** パッケージおよび **gnutls-utils** パッケージをインストールします。

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

2. **pcscd** サービスを開始します。

```
# systemctl start pcscd
```

### 検証手順

- **pcscd** サービスが稼働していることを確認します。

```
# systemctl status pcscd
```

## 31.3. スマートカードを準備し、証明書と鍵をスマートカードにアップロードする

**pkcs15-init** ツールを使用してスマートカードを設定するには、この手順に従います。このツールは、以下を設定するのに役立ちます。

- スマートカードの消去
- 新しい PIN および任意の PIN ブロック解除キー (PUK) の設定
- スマートカードでの新規スロットの作成
- スロットへの証明書、秘密鍵、および公開鍵の保存
- 必要に応じて、特定のスマートカードではこのタイプのファイナライズが必要なため、スマートカードの設定をロックします。



### 注記

**pkcs15-init** ツールは、すべてのスマートカードで機能するとは限りません。使用しているスマートカードで動作するツールを使用する必要があります。

### 前提条件

- **pkcs15-init** ツールを含む **opensc** パッケージがインストールされている。  
詳細は [スマートカードを管理および使用するツールのインストール](#) を参照してください。
- カードがリーダーに挿入され、コンピューターに接続されている。
- スマートカードに保存する秘密鍵、公開鍵、および証明書がある。この手順の **testuser.key**、**testuserpublic.key**、および **testuser.crt** は、秘密鍵、公開鍵、および証明書に使用される名前です。
- 現在のスマートカードユーザー PIN およびセキュリティーオフィス PIN (SO-PIN)

## 手順

1. スマートカードを消去して PIN で自身を認証します。

```
$ 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]:
```

カードが削除されました。

2. スマートカードを初期化し、ユーザーの PIN と PUK を設定します。また、セキュリティー担当者の PIN と PUK を設定します。

```
$ 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
```

**pkcs15-init** ツールは、スマートカードに新しいスロットを作成します。

3. スロットのラベルと認証 ID を設定します。

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

ラベルは人間が判読できる値に設定されます (この場合は **testuser**)。 **auth-id** は 16 進数の値である必要があります。この場合、**01** に設定されます。

4. スマートカードの新しいスロットに秘密鍵を保存し、ラベルを付けます。

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



## 注記

--id に指定する値は、秘密鍵を保存するときと、次の手順で証明書を保存するときと同じである必要があります。--id に独自の値を指定することを推奨します。そうしないと、より複雑な値がツールによって計算されます。

5. スマートカードの新しいスロットに証明書を保存し、ラベル付けします。

```
$ 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. オプション: スマートカードの新しいスロットに公開鍵を保存し、ラベルを付けます。

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



### 注記

公開鍵が秘密鍵または証明書に対応する場合は、秘密鍵または証明書の ID と同じ ID を指定します。

7. オプション: スマートカードの中には、設定をロックしてカードをファイナライズする必要があるものもあります。

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

この段階では、スマートカードには、新たに作成されたスロットに証明書、秘密鍵、および公開鍵が含まれます。ユーザーの PIN と PUK、およびセキュリティー担当者の PIN と PUK も作成しました。

## 31.4. WEB コンソールのスマートカード認証の有効化

Web コンソールでスマートカード認証を使用できるようにするには、**cockpit.conf** ファイルでスマートカード認証を有効にします。

また、同じファイルでパスワード認証を無効にすることもできます。

### 前提条件

- RHEL Web コンソールがインストールされている。  
詳細については、[Web コンソールのインストール](#) を参照してください。

### 手順

1. 管理者権限で RHEL Web コンソールにログインしている。  
詳細は、[Web コンソールへのログイン](#) を参照してください。
2. **Terminal** をクリックします。
3. **/etc/cockpit/cockpit.conf** で **ClientCertAuthentication** を **yes** に設定します。

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

4. 必要に応じて、以下のようにして **cockpit.conf** でパスワードベースの認証を無効にします。

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



この設定ではパスワード認証が無効になり、常にスマートカードを使用する必要があります。

5. Web コンソールを再起動して、**cockpit.service** が変更を受け入れることを確認します。

```
# systemctl restart cockpit
```

## 31.5. スマートカードを使用して WEB コンソールへのログイン

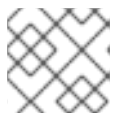
スマートカードを使用して、Web コンソールにログインできます。

### 前提条件

- 有効な証明書が、Active Directory または Identity Management ドメインで作成されたユーザーアカウントに関連付けられているスマートカードに保存されている。
- スマートカードのロックを解除するピン。
- スマートカードがリーダーに追加されている。

### 手順

1. Web ブラウザーを開き、アドレスバーに Web コンソールのアドレスを追加します。  
ブラウザーは、スマートカードに保存されている証明書を PIN で保護するよう要求します。
2. **Password Required** ダイアログボックスで PIN を入力し、**OK** をクリックします。
3. **User Identification Request** ダイアログボックスで、スマートカードに保存されている証明書を選択します。
4. **Remember this decision** を選択します。  
次回、このウィンドウが開きません。



### 注記

この手順は、Google Chrome ユーザーには適用されません。

5. **OK** をクリックします。

これで接続され、Web コンソールがそのコンテンツを表示します。

## 31.6. DOS 攻撃を防ぐためのユーザーセッションおよびメモリーの制限

証明書認証は、別のユーザーの権限を借用しようとする攻撃者に対して Web サーバー **cockpit-ws** のインスタンスを分離して孤立させることで保護されます。ただし、これによりサービス拒否攻撃 (DoS) 攻撃が発生する可能性があります。リモートの攻撃者は大量の証明書を作成し、異なる証明書を使用してそれぞれ cockpit-ws に多数の HTTPS 要求を送信することができます。

この DoS を防ぐために、これらの Web サーバーインスタンスの共同リソースは制限されます。デフォルトでは、接続数に制限され、メモリー使用量の制限は 200 スレッドと、75% (ソフト) または 90% (ハード) のメモリーに設定されます。

以下の手順では、接続およびメモリーの数を制限することで、リソースの保護を説明します。

## 手順

1. 端末で **system-cockpithttps.slice** 設定ファイルを開きます。

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

2. **TasksMax** を 100 に、**CPUQuota** を 30% に制限します。

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

3. 変更を適用するには、システムを再起動します。

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

これで、新しいメモリーとユーザーセッションの制限により、Web サーバー **cockpit-ws** が DoS 攻撃から保護されるようになりました。

## 31.7. 関連情報

- [Configuring Identity Management for smart card authentication .](#)
- [Configuring certificates issued by ADCS for smart card authentication in IdM .](#)
- [ローカル証明書のスマートカードへの設定およびインポート](#)

## 第32章 SATELLITE ホストの管理と監視

Red Hat Satellite は、物理、仮想、クラウド環境にわたってシステムを導入、設定、保守するためのシステム管理ソリューションです。Satellite は、集中化されたツールを使用して、複数の Red Hat Enterprise Linux デプロイメントのプロビジョニング、リモート管理、および監視を提供します。

デフォルトでは、Red Hat Satellite では RHEL Web コンソールの統合は無効になっています。Red Hat Satellite 内からホストの Red Hat Web コンソール機能にアクセスするには、まず Red Hat Satellite Server で RHEL Web コンソールの統合を有効にする必要があります。

### ウェブコンソールで多数のホストを大規模に管理するための Satellite ドキュメント

- RHEL Web コンソールと Satellite の統合の詳細は、[Satellite での RHEL Web コンソールの有効化](#) を参照してください。
- Web コンソールを使用したホストの管理と監視の詳細は、[RHEL Web コンソールを使用したホストの管理と監視](#) を参照してください。

## 第33章 RHEL WEB コンソールを使用したコンテナイメージの管理

RHEL Web コンソールの Web ベースのインターフェイスを使用して、コンテナイメージをプル、プルーニング、または削除できます。

### 33.1. WEB コンソールでのコンテナイメージの取得

コンテナイメージをローカルシステムにダウンロードし、それを使用してコンテナを作成できます。

#### 前提条件

- RHEL 8 Web コンソールをインストールし、アクセスできる。詳細は、[Web コンソールのインストール](#) および [Web コンソールへのログイン](#) を参照してください。
- **cockpit-podman** アドオンをインストールしている。

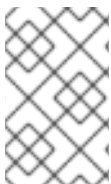
```
# yum install cockpit-podman
```

#### 手順

1. メインメニューで **Podman containers** をクリックします。
2. **Images** テーブルで、右上隅にあるオーバーフローメニューをクリックし、**Download new image** を選択します。
3. **Search for an image** ダイアログボックスが表示されます。
4. **Search for** フィールドに、イメージの名前を入力するか、その説明を指定します。
5. **in** ドロップダウンリストで、イメージを取得するレジストリーを選択します。
6. オプション: **Tag** フィールドに、イメージのタグを入力します。
7. **Download** をクリックします。

#### 検証

- メインメニューで **Podman containers** をクリックします。新しくダウンロードしたイメージは、**Images** テーブルで確認できます。



#### 注記

**Images** テーブルで **Create container** をクリックすると、ダウンロードしたイメージからコンテナを作成できます。コンテナを作成するには、[Web コンソールでのコンテナの作成](#) の手順 3 - 8 に従います。

### 33.2. WEB コンソールでのコンテナイメージのプルーニング

コンテナを持たない未使用のイメージをすべて削除できます。

#### 前提条件

- 少なくとも1つのコンテナイメージがプルされます。
- RHEL 8 Web コンソールをインストールし、アクセスできる。詳細は、[Web コンソールのインストール](#) および [Web コンソールへのログイン](#) を参照してください。
- **cockpit-podman** アドオンをインストールしている。

```
# yum install cockpit-podman
```

#### 手順

1. メインメニューで **Podman containers** をクリックします。
2. **Images** テーブルで、右上隅のオーバーフローメニューをクリックし、**Prune unused images** を選択します。
3. イメージのリストを含むポップアップウィンドウが表示されます。**Prune** をクリックして選択を確定します。

#### 検証

- メインメニューで **Podman containers** をクリックします。削除されたイメージは、**Images** テーブルにリストされません。

### 33.3. WEB コンソールでのコンテナイメージの削除

Web コンソールを使用して、以前にプルしたコンテナイメージを削除できます。

#### 前提条件

- 少なくとも1つのコンテナイメージがプルされます。
- RHEL 8 Web コンソールをインストールし、アクセスできる。詳細は、[Web コンソールのインストール](#) および [Web コンソールへのログイン](#) を参照してください。
- **cockpit-podman** アドオンをインストールしている。

```
# yum install cockpit-podman
```

#### 手順

1. メインメニューで **Podman containers** をクリックします。
2. **Images** テーブルで、削除するイメージを選択し、オーバーフローメニューをクリックして **Delete** を選択します。
3. ウィンドウが表示されます。**Delete tagged images** をクリックして選択を確認します。

#### 検証

- メインメニューで **Podman containers** をクリックします。削除されたコンテナは、**Images** テーブルにリストされません。

## 第34章 RHEL WEB コンソールを使用したコンテナの管理

Red Hat Enterprise Linux Web コンソールを使用して、コンテナと Pod を管理できます。Web コンソールを使用すると、非 root または root ユーザーとしてコンテナを作成できます。

- root ユーザーとして、追加の権限とオプションを備えたシステムコンテナを作成できます。
- 非 root ユーザーには 2 つのオプションがあります。
  - ユーザーコンテナのみを作成するには、Web コンソールをデフォルトモード (**Limited access**) で使用できます。
  - ユーザーコンテナとシステムコンテナの両方を作成するには、Web コンソールページの上部パネルで **Administrative access** をクリックします。

ルートコンテナとルートレスコンテナの違いの詳細については、[ルートレスコンテナに関する特別な考慮事項](#) を参照してください。

### 34.1. WEB コンソールでのコンテナの作成

コンテナを作成し、ポートマッピング、ボリューム、環境変数、ヘルスチェックなどを追加できます。

#### 前提条件

- RHEL 8 Web コンソールをインストールし、アクセスできる。詳細は、[Web コンソールのインストール](#) および [Web コンソールへのログイン](#) を参照してください。
- **cockpit-podman** アドオンをインストールしている。

```
# yum install cockpit-podman
```

#### 手順

1. メインメニューで **Podman containers** をクリックします。
2. **Create container** をクリックします。
3. **Name** フィールドに、コンテナの名前を入力します。
4. **Details** タブに必要な情報を入力します。
  - **管理アクセスでのみ使用可能**: コンテナの所有者: システムまたはユーザーを選択します。
  - **Image** ドロップダウンリストで、選択したレジストリー内のコンテナイメージを選択または検索します。
    - オプション: 最新のコンテナイメージをプルするには、**Pull latest image** チェックボックスをオンにします。
  - **Command** フィールドはコマンドを指定します。必要に応じて、デフォルトのコマンドを変更できます。
    - オプション: ターミナルを使用してコンテナを実行するには、**With terminal** チェックボックスをオンにします。

- **Memory limit** フィールドでは、コンテナのメモリー制限を指定します。デフォルトのメモリー制限を変更するには、チェックボックスをオンにして制限を指定します。
- **システムコンテナでのみ使用可能: CPU シェア** フィールドで、相対的な CPU 時間量を指定します。デフォルト値は 1024 です。デフォルト値を変更するには、チェックボックスをオンにします。
- **システムコンテナでのみ使用可能: Restart policy** ドロップダウンメニューで、次のオプションのいずれかを選択します。
  - いいえ (デフォルト値): アクションはありません。
  - 失敗時: 失敗時にコンテナを再起動します。
  - コンテナの終了時、またはシステムの再起動後にコンテナを再起動します。

#### 5. Integration タブに必要な情報を入力します。

- **Add port mapping** をクリックして、コンテナとホストシステムの間ポートマッピングを追加します。
  - IP アドレス、ホストポート、コンテナポート、および **プロトコル** を入力します。
- **Add volume** をクリックしてボリュームを追加します。
  - **ホストパス**、**コンテナパス** を入力します。**Writable** オプションのチェックボックスをオンにして、書き込み可能なボリュームを作成できます。SELinux ドロップダウンリストで、次のオプションのいずれかを選択します: No Label、Shared、または Private。
- **Add variable** をクリックして環境変数を追加します。
  - **Key** と **Value** を入力します。

#### 6. Health check タブに必要な情報を入力します。

- **Command** フィールドに、'healthcheck' コマンドを入力します。
- ヘルスチェックオプションを指定します。
  - **Interval** (デフォルトは 30 秒)
  - **Timeout** (デフォルトは 30 秒)
  - **Start period**
  - **Retries** (デフォルトは 3)
  - **When unhealthy**: 次のいずれかのオプションを選択します。
    - **No action** (デフォルト): アクションは実行しません。
    - **Restart**: コンテナを再起動します。
    - **Stop**: コンテナを停止します。
    - **Force stop**: コンテナを強制的に停止します。コンテナが終了するのを待ちません。

7. **Create and run** をクリックして、コンテナを作成して実行します。



#### 注記

**Create** をクリックすると、コンテナのみを作成できます。

#### 検証

- メインメニューで **Podman containers** をクリックします。新しく作成されたコンテナは **Containers** テーブルで確認できます。

## 34.2. WEB コンソールでのコンテナの検査

Web コンソールでコンテナの詳細情報を表示できます。

#### 前提条件

- コンテナが作成されている。
- RHEL 8 Web コンソールをインストールし、アクセスできる。詳細は、[Web コンソールのインストール](#) および [Web コンソールへのログイン](#) を参照してください。
- **cockpit-podman** アドオンをインストールしている。

```
# yum install cockpit-podman
```

#### 手順

1. メインメニューで **Podman containers** をクリックします。
2. > 矢印アイコンをクリックすると、コンテナの詳細が表示されます。
  - **Details** タブでは、コンテナ ID、イメージ、コマンド、作成済み (コンテナ作成時のタイムスタンプ)、およびその状態を確認できます。
    - システムコンテナでのみ利用可能: IP アドレス、MAC アドレス、およびゲートウェイアドレスも表示されます。
  - **Integration** タブでは、環境変数、ポートマッピング、およびボリュームを確認できます。
  - **Log** タブでは、コンテナのログを確認できます。
  - **Console** タブでは、コマンドラインを使用してコンテナを操作できます。

## 34.3. WEB コンソールでのコンテナの状態の変更

Red Hat Enterprise Linux Web コンソールでは、システム上のコンテナの起動、停止、再起動、一時停止、および名前変更が可能です。

#### 前提条件

- コンテナが作成されている。



- RHEL 8 Web コンソールをインストールし、アクセスできる。詳細は、[Web コンソールのインストール](#) および [Web コンソールへのログイン](#) を参照してください。
- **cockpit-podman** アドオンをインストールしている。

```
# yum install cockpit-podman
```

## 手順

1. メインメニューで **Podman containers** をクリックします。
2. **Containers** テーブルで、変更するコンテナを選択し、オーバーフローメニューをクリックして、実行するアクションを選択します。
  - Start
  - Stop
  - Force stop
  - Restart
  - Force restart
  - Pause
  - Rename

## 34.4. WEB コンソールでのコンテナのコミット

コンテナの現在の状態に基づいて新しいイメージを作成できます。

### 前提条件

- コンテナが作成されている。
- RHEL 8 Web コンソールをインストールし、アクセスできる。詳細は、[Web コンソールのインストール](#) および [Web コンソールへのログイン](#) を参照してください。
- **cockpit-podman** アドオンをインストールしている。

```
# yum install cockpit-podman
```

## 手順

1. メインメニューで **Podman containers** をクリックします。
2. **Containers** テーブルで、変更するコンテナを選択し、オーバーフローメニューをクリックして **Commit** を選択します。
3. **Commit container** フォームに、次の詳細を追加します。
  - **New image name** フィールドにイメージ名を入力します。
  - オプション: **Tag** フィールドにタグを入力します。

- オプション: **Author** フィールドに名前を入力します。
- オプション: 必要に応じて、**Command** フィールドでコマンドを変更します。
- オプション: 必要なオプションを確認します。
  - イメージ作成時にコンテナを一時停止する: イメージがコミットされている間、コンテナとそのプロセスは一時停止されます。
  - 従来の Docker 形式を使用する: Docker イメージ形式を使用しない場合は、OCI 形式が使用されます。

4. **Commit** をクリックします。

## 検証

- メインメニューで **Podman containers** をクリックします。新しく作成されたイメージは **Images** テーブルで確認できます。

## 34.5. WEB コンソールでのコンテナチェックポイントの作成

Web コンソールを使用すると、実行中のコンテナまたは個々のアプリケーションにチェックポイントを設定し、その状態をディスクに保存できます。



### 注記

チェックポイントの作成は、システムコンテナでのみ使用できます。

## 前提条件

- コンテナが実行されている。
- RHEL 8 Web コンソールをインストールし、アクセスできる。詳細は、[Web コンソールのインストール](#) および [Web コンソールへのログイン](#) を参照してください。
- **cockpit-podman** アドオンをインストールしている。

```
# yum install cockpit-podman
```

## 手順

1. メインメニューで **Podman containers** をクリックします。
2. **Containers** テーブルで、変更するコンテナを選択し、オーバーフローアイコンメニューをクリックして **Containers** を選択します。
3. オプション: **Checkpoint container** フォームで、必要なオプションをチェックします。
  - すべての一時チェックポイントファイルを保持する: チェックポイント作成中に CRIU によって作成されたすべての一時ログおよび統計ファイルを保持します。さらなるデバッグのためのチェックポイント設定が失敗した場合でも、これらのファイルは削除されません。
  - チェックポイントをディスクに書き込んだ後も実行したままにする: チェックポイントを作成した後もコンテナを停止するのではなく、実行したままにします。

- 確立された TCP 接続の維持のサポート

4. **Checkpoint** をクリックします。

### 検証

- メインメニューで **Podman containers** をクリックします。チェックポイントを設定したコンテナを選択し、オーバーフローメニューアイコンをクリックして、**Restore** オプションがあることを確認します。

## 34.6. WEB コンソールでのコンテナチェックポイントの復元

保存したデータを使用して、再起動後に、チェックポイントの時点にコンテナを復元できます。



### 注記

チェックポイントの作成は、システムコンテナでのみ使用できます。

### 前提条件

- コンテナにチェックポイントが設定されている。
- RHEL 8 Web コンソールをインストールし、アクセスできる。詳細は、[Web コンソールのインストール](#) および [Web コンソールへのログイン](#) を参照してください。
- **cockpit-podman** アドオンをインストールしている。

```
# yum install cockpit-podman
```

### 手順

1. メインメニューで **Podman containers** をクリックします。
2. **Containers** テーブルで、変更するコンテナを選択し、オーバーフローメニューをクリックして **Restore** を選択します。
3. オプション: **Restore container** フォームで、必要なオプションを確認します。
  - すべての一時チェックポイントファイルを保持する: チェックポイント作成中に CRIU によって作成されたすべての一時ログおよび統計ファイルを保持します。さらなるデバッグのためのチェックポイント設定が失敗した場合でも、これらのファイルは削除されません。
  - **Restore with established TCP connections**
  - 静的に設定されている場合は IP アドレスを無視する: コンテナが IP アドレスで開始された場合、復元されたコンテナもその IP アドレスを使用しようとし、その IP アドレスがすでに使用されている場合は復元は失敗します。このオプションは、コンテナの作成時に Integration タブでポートマッピングを追加した場合に適用されます。
  - 静的に設定されている場合は MAC アドレスを無視する: コンテナが MAC アドレスで開始された場合、復元されたコンテナもその MAC アドレスを使用しようとし、その MAC アドレスがすでに使用されている場合は復元が失敗します。
4. **Restore** をクリックします。

## 検証

- メインメニューで **Podman containers** クリックします。Containers テーブルで復元されたコンテナが実行されていることがわかります。

## 34.7. WEB コンソールでのコンテナの削除

Web コンソールを使用して既存のコンテナを削除できます。

### 前提条件

- コンテナがシステムに存在する。
- RHEL 8 Web コンソールをインストールし、アクセスできる。詳細は、[Web コンソールのインストール](#) および [Web コンソールへのログイン](#) を参照してください。
- **cockpit-podman** アドオンをインストールしている。

```
# yum install cockpit-podman
```

### 手順

1. メインメニューで **Podman containers** をクリックします。
2. Containers テーブルで、削除するコンテナを選択し、オーバーフローメニューをクリックして **Delete** を選択します。
3. ポップアップウィンドウが表示されます。Delete をクリックして選択を確定します。

## 検証

- メインメニューで **Podman containers** クリックします。削除されたコンテナは、Containers テーブルにリストされません。

## 34.8. WEB コンソールでの POD の作成

RHEL Web コンソールインターフェイスで Pod を作成できます。

### 前提条件

- RHEL 8 Web コンソールをインストールし、アクセスできる。詳細は、[Web コンソールのインストール](#) および [Web コンソールへのログイン](#) を参照してください。
- **cockpit-podman** アドオンをインストールしている。

```
# yum install cockpit-podman
```

### 手順

1. メインメニューで **Podman containers** をクリックします。
2. **Create pod** をクリックします。
3. Create pod フォームに必要な情報を入力します。

- **管理アクセスでのみ使用可能:** コンテナの所有者: システムまたはユーザーを選択します。
  - **Name** フィールドに、コンテナの名前を入力します。
  - **Add port mapping** をクリックして、コンテナとホストシステムの間ポートマッピングを追加します。
    - IP アドレス、ホストポート、コンテナポート、プロトコルを入力します。
  - **Add volume** をクリックしてボリュームを追加します。
    - ホストパス、コンテナパスを入力します。書き込み可能チェックボックスをオンにして、書き込み可能なボリュームを作成できます。SELinux ドロップダウンリストで、次のオプションのいずれかを選択します: No Label、Shared、または Private。
4. **Create** をクリックします。

### 検証

- メインメニューで **Podman containers** をクリックします。新しく作成された Pod は **Containers** テーブルで確認できます。

## 34.9. WEB コンソールの POD 内にコンテナを作成する

Pod 内にコンテナを作成できます。

### 前提条件

- RHEL 8 Web コンソールをインストールし、アクセスできる。詳細は、[Web コンソールのインストール](#) および [Web コンソールへのログイン](#) を参照してください。
- **cockpit-podman** アドオンをインストールしている。

```
# yum install cockpit-podman
```

### 手順

1. メインメニューで **Podman containers** をクリックします。
2. **Create container in pod** をクリックします。
3. **Name** フィールドに、コンテナの名前を入力します。
4. **Details** タブに必要な情報を入力します。
  - **管理アクセスでのみ使用可能:** コンテナの所有者: システムまたはユーザーを選択します。
  - **Image** ドロップダウンリストで、選択したレジストリー内のコンテナイメージを選択または検索します。
    - オプション: 最新のコンテナイメージをプルするには、**Pull latest image** チェックボックスをオンにします。

- **Command** フィールドはコマンドを指定します。必要に応じて、デフォルトのコマンドを変更できます。
  - オプション: ターミナルを使用してコンテナを実行するには、**With terminal** チェックボックスをオンにします。
- **Memory limit** フィールドでは、コンテナのメモリー制限を指定します。デフォルトのメモリー制限を変更するには、チェックボックスをオンにして制限を指定します。
- **システムコンテナでのみ使用可能: CPU シェア** フィールドで、相対的な CPU 時間量を指定します。デフォルト値は 1024 です。デフォルト値を変更するには、チェックボックスをオンにします。
- **システムコンテナでのみ使用可能: Restart policy** ドロップダウンメニューで、次のオプションのいずれかを選択します。
  - いいえ (デフォルト値): アクションはありません。
  - 失敗時: 失敗時にコンテナを再起動します。
  - 常に: コンテナの終了時またはシステム起動後にコンテナを再起動します。

#### 5. Integration タブに必要な情報を入力します。

- **Add port mapping** をクリックして、コンテナとホストシステムの間ポートマッピングを追加します。
  - IP アドレス、ホストポート、コンテナポート、および **プロトコル** を入力します。
- **Add volume** をクリックしてボリュームを追加します。
  - ホストパス、コンテナパス を入力します。 **Writable** オプションのチェックボックスをオンにして、書き込み可能なボリュームを作成できます。SELinux ドロップダウンリストで、次のオプションのいずれかを選択します: No Label、Shared、または Private。
- **Add variable** をクリックして環境変数を追加します。
  - **Key** と **Value** を入力します。

#### 6. Health check タブに必要な情報を入力します。

- **Command** フィールドに、ヘルスチェックコマンドを入力します。
- ヘルスチェックオプションを指定します。
  - **Interval** (デフォルトは 30 秒)
  - **Timeout** (デフォルトは 30 秒)
  - **Start period**
  - **Retries** (デフォルトは 3)
  - **When unhealthy**: 次のいずれかのオプションを選択します。
    - **No action** (デフォルト): アクションは実行しません。
    - **Restart**: コンテナを再起動します。

- Stop: コンテナを停止します。
- Force stop: コンテナを強制的に停止します。コンテナが終了するのを待ちません。



#### 注記

コンテナの所有者は Pod の所有者と同じです。



#### 注記

Pod では、コンテナの検査、コンテナのステータスの変更、コンテナのコミット、またはコンテナの削除を行うことができます。

#### 検証

- メインメニューで **Podman containers** をクリックします。Pod 内の **Containers** テーブルの下に、新しく作成されたコンテナが表示されます。

## 34.10. WEB コンソールでの POD の状態の変更

Pod のステータスを変更できます。

#### 前提条件

- Pod が作成済みである。
- RHEL 8 Web コンソールをインストールし、アクセスできる。詳細は、[Web コンソールのインストール](#) および [Web コンソールへのログイン](#) を参照してください。
- **cockpit-podman** アドオンをインストールしている。

```
# yum install cockpit-podman
```

#### 手順

1. メインメニューで **Podman containers** をクリックします。
2. **Containers** テーブルで、変更する Pod を選択し、オーバーフローメニューをクリックして、実行するアクションを選択します。
  - Start
  - Stop
  - Force stop
  - Restart
  - Force restart
  - Pause

## 34.11. WEB コンソールでの POD の削除

Web コンソールを使用して既存の Pod を削除できます。

### 前提条件

- Pod がシステムに存在する。
- RHEL 8 Web コンソールをインストールし、アクセスできる。詳細は、[Web コンソールのインストール](#) および [Web コンソールへのログイン](#) を参照してください。
- **cockpit-podman** アドオンをインストールしている。

```
# yum install cockpit-podman
```

### 手順

1. メインメニューで **Podman containers** をクリックします。
2. **Containers** テーブルで、削除する Pod を選択し、オーバーフローメニューをクリックして **Delete** を選択します。
3. 次のポップアップウィンドウで、**Delete** をクリックして選択を確定します。



#### 警告

Pod 内のすべてのコンテナが削除されます。

### 検証

- メインメニューで **Podman containers** をクリックします。削除された Pod は、**Containers** テーブルにリストされません。