Red Hat Enterprise Linux 8

Verwalten von Systemen mit der RHEL 8 Web-Konsole

Eine Anleitung zur Verwendung der Web-Konsole zur Verwaltung von Systemen in Red Hat Enterprise Linux 8

Last Updated: 2021-03-09

Red Hat Enterprise Linux 8 Verwalten von Systemen mit der RHEL 8 Web-Konsole

Eine Anleitung zur Verwendung der Web-Konsole zur Verwaltung von Systemen in Red Hat Enterprise Linux 8

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

Rechtlicher Hinweis

Zusammenfassung

Dieses Dokument beschreibt, wie Sie physische und virtuelle Linux-basierte Systeme mit der RHEL 8 Web-Konsole verwalten können. Die Anweisungen gehen davon aus, dass der für die Verwaltung verwendete Server unter Red Hat Enterprise Linux 8 läuft.

Inhaltsverzeichnis

OPEN SOURCE INKLUSIVER MACHEN

Red Hat hat sich verpflichtet, problematische Sprache in unserem Code, unserer Dokumentation und unseren Web-Eigenschaften zu ersetzen. Wir beginnen mit diesen vier Begriffen: Master, Slave, Blacklist und Whitelist. Aufgrund des enormen Umfangs dieses Vorhabens werden diese Änderungen schrittweise über mehrere kommende Versionen implementiert. Weitere Details finden Sie in der Nachricht von unserem CTO Chris Wright .

FEEDBACK ZUR RED HAT-DOKUMENTATION GEBEN

Wir freuen uns über Ihre Anregungen zu unserer Dokumentation. Bitte teilen Sie uns mit, wie wir sie noch besser machen können. Um dies zu tun:

- Für einfache Kommentare zu bestimmten Passagen:
  1. Stellen Sie sicher, dass Sie die Dokumentation im Format *Multi-page HTML* anzeigen. Stellen Sie außerdem sicher, dass Sie die Schaltfläche **Feedback** in der oberen rechten Ecke des Dokuments sehen.
  2. Markieren Sie mit dem Mauszeiger den Teil des Textes, den Sie kommentieren möchten.
  3. Klicken Sie auf das Einblendmenü **Add Feedback**, das unter dem markierten Text erscheint.
  4. Folgen Sie den angezeigten Anweisungen.
- Um komplexere Rückmeldungen einzureichen, erstellen Sie ein Bugzilla-Ticket:
  1. Rufen Sie die Bugzilla-Website auf.
  2. Verwenden Sie als Komponente **Documentation**.
  3. Füllen Sie das Feld **Description** mit Ihrem Verbesserungsvorschlag aus. Fügen Sie einen Link zu dem/den relevanten Teil(en) der Dokumentation hinzu.
  4. Klicken Sie auf **Submit Bug**.

KAPITEL 1. ERSTE SCHRITTE MIT DER RHEL WEB-KONSOLE

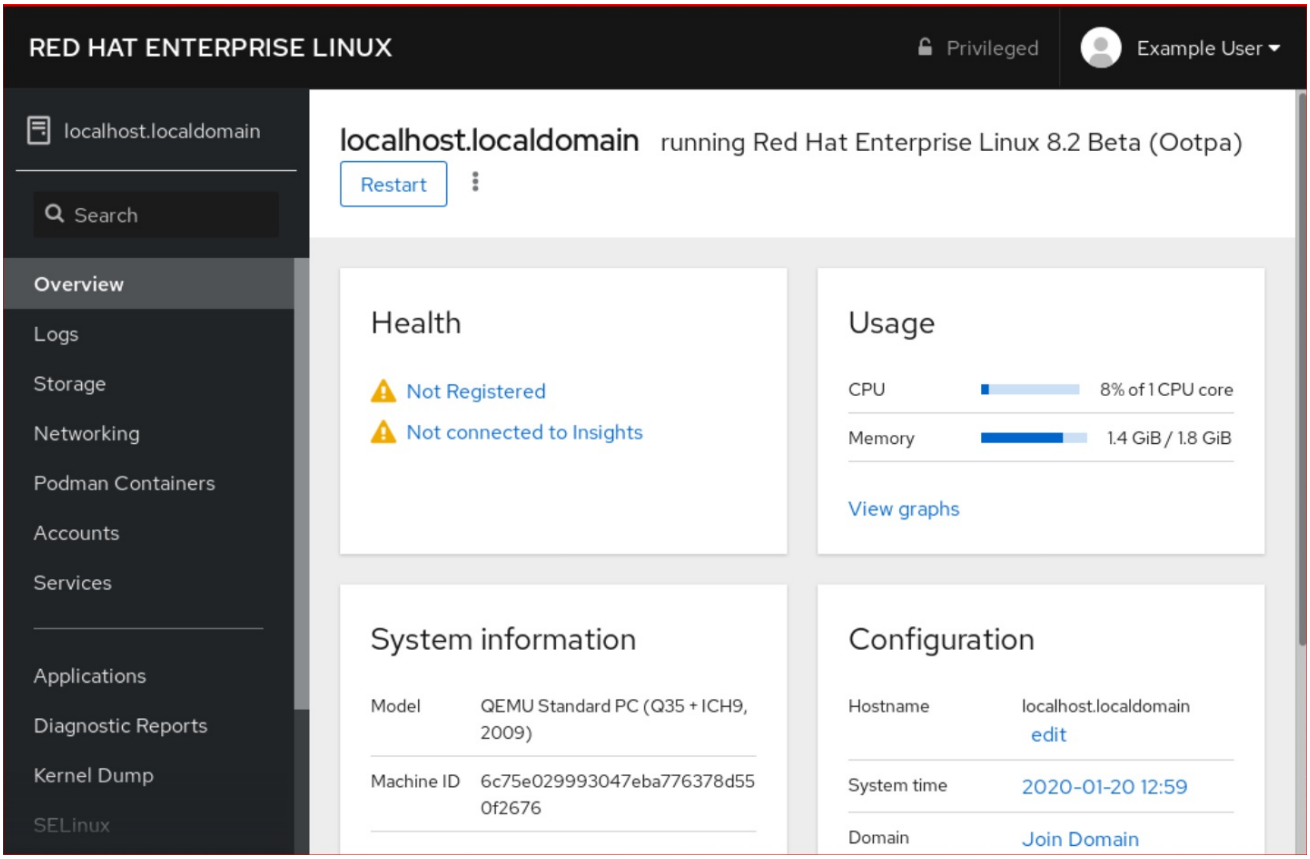
Installieren Sie die Web-Konsole in Red Hat Enterprise Linux 8 und lernen Sie, wie Sie Remote-Hosts hinzufügen und in der RHEL 8 Web-Konsole überwachen können.

Voraussetzungen

- Installieren Sie Red Hat Enterprise Linux 8.
- Aktiviert die Vernetzung.
- Registriertes System mit entsprechendem Abonnement angeschlossen.
  Um ein Abonnement zu erhalten, siehe Verwalten von Abonnements in der Web-Konsole.

1.1. WAS IST DIE RHEL WEB-KONSOLE

Die RHEL-Webkonsole ist eine webbasierte Oberfläche für Red Hat Enterprise Linux 8, die für die Verwaltung und Überwachung Ihres lokalen Systems sowie der Linux-Server in Ihrer Netzwerkumgebung entwickelt wurde.



Die RHEL-Web-Konsole ermöglicht Ihnen eine Vielzahl von Verwaltungsaufgaben, darunter:

- Dienste verwalten
- Verwalten von Benutzerkonten
- Verwaltung und Überwachung von Systemdiensten
- Konfigurieren von Netzwerkschnittstellen und Firewall
- Prüfen von Systemprotokollen

- Virtuelle Maschinen verwalten
- Erstellen von Diagnoseberichten
- Einstellen der Kernel-Dump-Konfiguration
- Konfigurieren von SELinux
- Software aktualisieren
- Verwalten von Systemabonnements

Die RHEL-Webkonsole verwendet dieselben System-APIs wie ein Terminal, und Aktionen, die in einem Terminal ausgeführt werden, werden sofort in der RHEL-Webkonsole wiedergegeben.

Sie können die Protokolle der Systeme in der Netzwerkumgebung sowie deren Leistung überwachen, die als Diagramme angezeigt werden. Darüber hinaus können Sie die Einstellungen direkt in der Web-Konsole oder über das Terminal ändern.

1.2. INSTALLIEREN UND AKTIVIEREN DER WEB-KONSOLE

Um auf die RHEL 8 Web-Konsole zuzugreifen, aktivieren Sie zunächst den Dienst **cockpit.socket**.

Red Hat Enterprise Linux 8 enthält in vielen Installationsvarianten die standardmäßig installierte RHEL 8 Web-Konsole. Wenn dies auf Ihrem System nicht der Fall ist, installieren Sie das Paket **cockpit**, bevor Sie den Dienst **cockpit.socket** aktivieren.

Verfahren

1. Wenn die Web-Konsole auf Ihrer Installationsvariante nicht standardmäßig installiert ist, installieren Sie das Paket **cockpit** manuell:

```
# yum install cockpit
```

2. Aktivieren und starten Sie den Dienst **cockpit.socket**, der einen Webserver betreibt:

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

3. Wenn die Web-Konsole nicht standardmäßig auf Ihrer Installationsvariante installiert wurde und Sie ein benutzerdefiniertes Firewall-Profil verwenden, fügen Sie den Dienst **cockpit** zu **firewalld** hinzu, um Port 9090 in der Firewall zu öffnen:

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

Schritte zur Verifizierung

1. Um die vorherige Installation und Konfiguration zu überprüfen, öffnen Sie die Web-Konsole.

1.3. EINLOGGEN IN DIE WEB-KONSOLE

Verwenden Sie die Schritte in diesem Verfahren für die erste Anmeldung an der RHEL-Webkonsole mit einem Systembenutzernamen und einem Passwort.

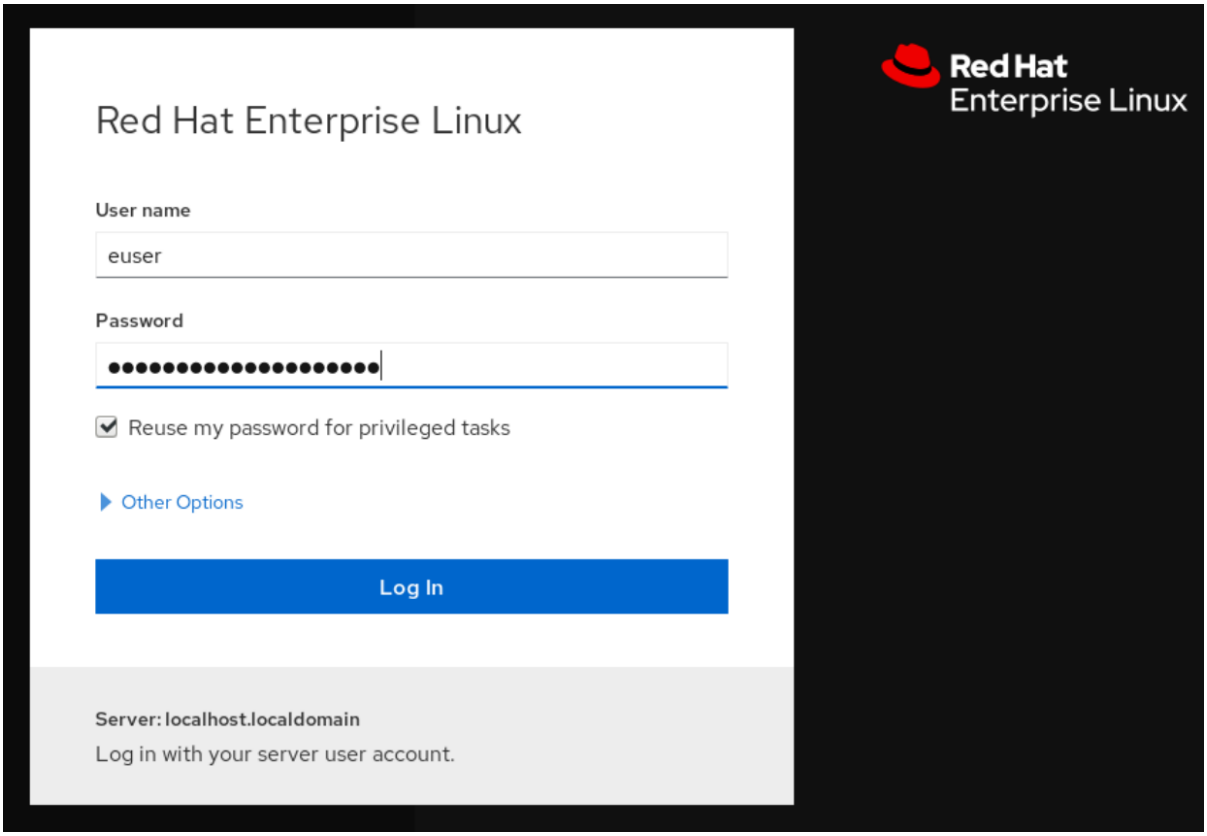
Voraussetzungen

- Verwenden Sie einen der folgenden Browser zum Öffnen der Web-Konsole:
  - Mozilla Firefox 52 und höher
  - Google Chrome 57 und höher
  - Microsoft Edge 16 und höher
- Anmeldeinformationen für das Systembenutzerkonto
  Die RHEL-Webkonsole verwendet einen speziellen PAM-Stack, der sich unter **/etc/pam.d/cockpit** befindet. Die Authentifizierung mit PAM ermöglicht es Ihnen, sich mit dem Benutzernamen und dem Passwort eines beliebigen lokalen Kontos auf dem System anzumelden.

Verfahren

1. Öffnen Sie die Web-Konsole in Ihrem Webbrowser:
   - Örtlich **https://localhost:9090**
   - Aus der Ferne mit dem Hostnamen des Servers **https://example.com:9090**
   - Aus der Ferne mit der IP-Adresse des Servers **https://192.0.2.2:9090**
     Wenn Sie ein selbstsigniertes Zertifikat verwenden, gibt der Browser eine Warnung aus. Prüfen Sie das Zertifikat und akzeptieren Sie die Sicherheitsausnahme, um mit der Anmeldung fortzufahren.

     Die Konsole lädt ein Zertifikat aus dem Verzeichnis **/etc/cockpit/ws-certs.d** und verwendet die letzte Datei mit einer **.cert** -Erweiterung in alphabetischer Reihenfolge. Um keine Sicherheitsausnahmen gewähren zu müssen, installieren Sie ein von einer Zertifizierungsstelle (CA) signiertes Zertifikat.
2. Geben Sie im Anmeldebildschirm Ihren Systembenutzernamen und Ihr Passwort ein.



3. Optional können Sie auf die Option **Reuse my password for privileged tasks**klicken.
   Wenn das Benutzerkonto, mit dem Sie sich anmelden, über sudo-Rechte verfügt, können Sie damit privilegierte Aufgaben in der Web-Konsole durchführen, z. B. die Installation von Software oder die Konfiguration von SELinux.

4. Klicken Sie auf **Log In**.

Nach erfolgreicher Authentifizierung öffnet sich die Oberfläche der RHEL-Webkonsole.

1.4. VERBINDEN MIT DER WEB-KONSOLE VON EINEM ENTFERNTEN RECHNER

Es ist möglich, sich von jedem Client-Betriebssystem und auch von Mobiltelefonen oder Tablets aus mit Ihrer Webkonsolen-Oberfläche zu verbinden.

Voraussetzungen

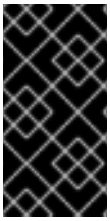
- Gerät mit einem unterstützten Internet-Browser, wie z. B.:
  - Mozilla Firefox 52 und höher
  - Google Chrome 57 und höher
  - Microsoft Edge 16 und höher
- RHEL 8-Server, auf den Sie mit einer installierten und zugänglichen Webkonsole zugreifen möchten. Weitere Informationen zur Installation der Web-Konsole finden Sie unter Installieren der Web-Konsole.

Verfahren

1. Öffnen Sie Ihren Webbrowser.
2. Geben Sie die Adresse des Remote-Servers in einem der folgenden Formate ein:
   a. Mit dem Hostnamen des Servers **server.hostname.example.com:port_number**
   b. Mit der IP-Adresse des Servers **server.IP_address:port_number**
3. Nachdem sich die Anmeldeoberfläche geöffnet hat, melden Sie sich mit den Anmeldedaten Ihres RHEL-Rechners an.

1.5. ANMELDUNG AN DER WEB-KONSOLE MIT EINEM EINMAL-PASSWORT

Wenn Ihr System Teil einer Identity Management (IdM)-Domäne mit aktivierter One-Time-Password (OTP)-Konfiguration ist, können Sie sich mit einem OTP an der RHEL-Webkonsole anmelden.



WICHTIG

Es ist nur dann möglich, sich mit einem Einmalpasswort anzumelden, wenn Ihr System Teil einer Identity Management (IdM)-Domäne mit aktivierter OTP-Konfiguration ist. Weitere Informationen über OTP in IdM finden Sie unter Einmaliges Passwort in Identity Management.

Voraussetzungen

- Die RHEL Web-Konsole wurde installiert.
  Details finden Sie unter Installieren der Web-Konsole.
- Ein Identity Management-Server mit aktivierter OTP-Konfiguration.
  Details finden Sie unter Einmaliges Passwort in der Identitätsverwaltung .
- Ein konfiguriertes Hardware- oder Software-Gerät, das OTP-Tokens erzeugt.

Verfahren

1. Öffnen Sie die RHEL-Webkonsole in Ihrem Browser:
   - Örtlich **https://localhost:PORT_NUMBER**
   - Aus der Ferne mit dem Hostnamen des Servers **https://example.com:PORT_NUMBER**
   - Aus der Ferne mit der IP-Adresse des Servers
     https://EXAMPLE.SERVER.IP.ADDR:PORT_NUMBER
     Wenn Sie ein selbstsigniertes Zertifikat verwenden, gibt der Browser eine Warnung aus. Prüfen Sie das Zertifikat und akzeptieren Sie die Sicherheitsausnahme, um mit der Anmeldung fortzufahren.

     Die Konsole lädt ein Zertifikat aus dem Verzeichnis **/etc/cockpit/ws-certs.d** und verwendet die letzte Datei mit einer **.cert** -Erweiterung in alphabetischer Reihenfolge. Um keine Sicherheitsausnahmen gewähren zu müssen, installieren Sie ein von einer Zertifizierungsstelle (CA) signiertes Zertifikat.
2. Das Fenster Anmeldung öffnet sich. Geben Sie im Login-Fenster Ihren Systembenutzernamen und Ihr Passwort ein.

3. Erzeugen Sie ein Einmal-Passwort auf Ihrem Gerät.
4. Geben Sie das Einmalpasswort in ein neues Feld ein, das in der Oberfläche der Web-Konsole erscheint, nachdem Sie Ihr Passwort bestätigt haben.
5. Klicken Sie auf **Log in**.
6. Nach erfolgreicher Anmeldung gelangen Sie auf die Seite **Overview** der Webkonsolen-Oberfläche.

1.6. NEUSTART DES SYSTEMS ÜBER DIE WEB-KONSOLE

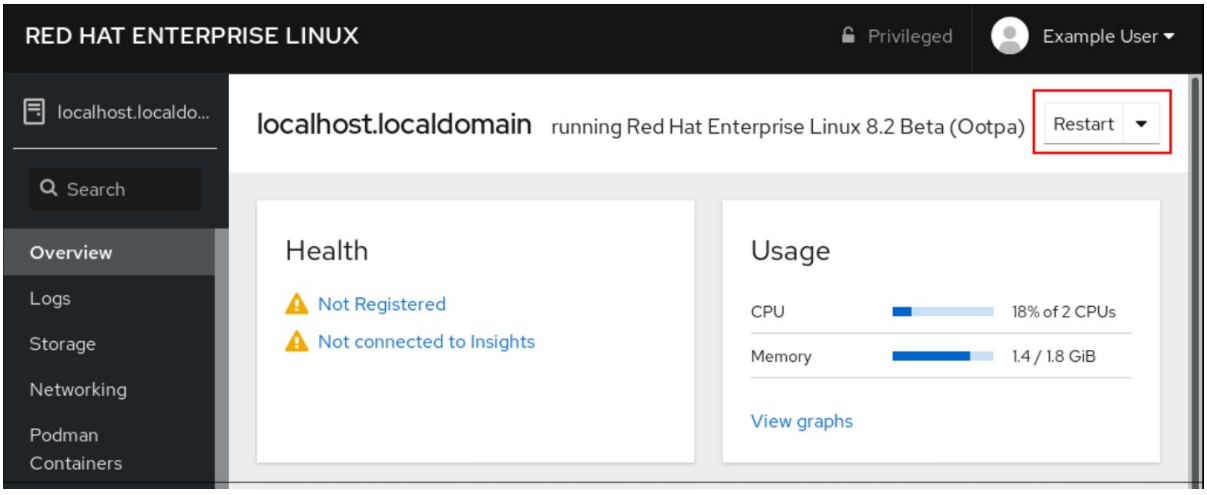
Sie können die Web-Konsole verwenden, um ein RHEL-System neu zu starten, an das die Web-Konsole angeschlossen ist.

Voraussetzungen

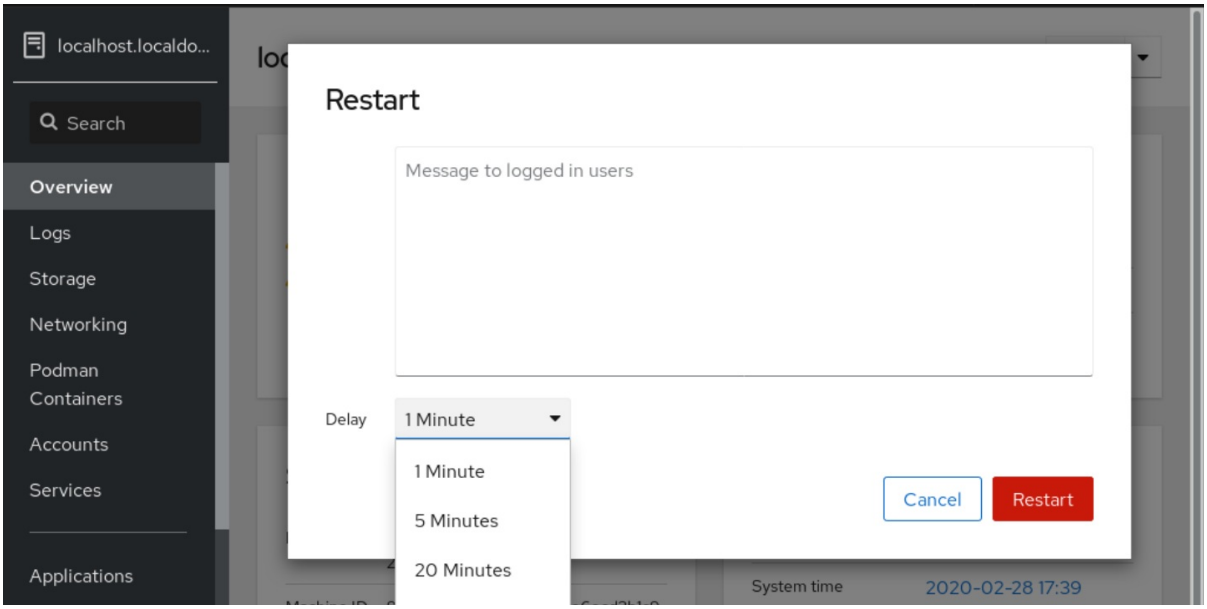
- Die Web-Konsole ist installiert und zugänglich.
  Details finden Sie unter Installieren der Web-Konsole.

Verfahren

1. Melden Sie sich an der RHEL 8 Web-Konsole an.
   Details finden Sie unter Anmeldung an der Web-Konsole.
2. Klicken Sie auf **Overview**.
3. Klicken Sie auf die Schaltfläche **Restart** neu starten.



4. Wenn irgendwelche Benutzer am System angemeldet sind, schreiben Sie einen Grund für den Neustart in das Dialogfeld **Restart**.
5. Optional: Wählen Sie in der Dropdown-Liste **Delay** ein Zeitintervall aus.



6. Klicken Sie auf **Restart**.

1.7. HERUNTERFAHREN DES SYSTEMS ÜBER DIE WEB-KONSOLE

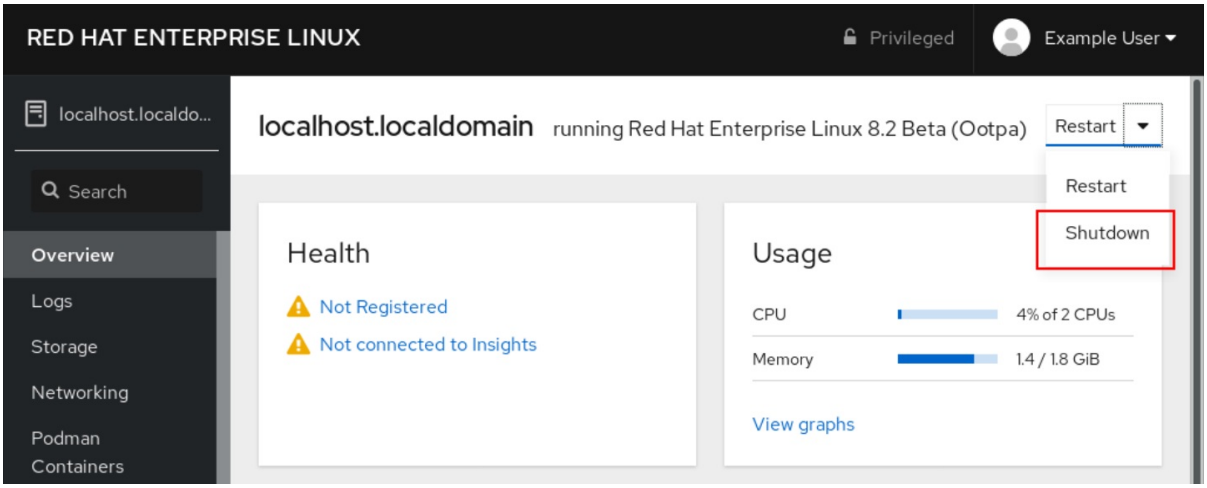
Sie können die Web-Konsole verwenden, um ein RHEL-System herunterzufahren, an das die Web-Konsole angeschlossen ist.

Voraussetzungen

- Die Web-Konsole ist installiert und zugänglich.
  Details finden Sie unter Installieren der Web-Konsole.

Verfahren

1. Melden Sie sich an der RHEL 8 Web-Konsole an.
   Details finden Sie unter Anmeldung an der Web-Konsole.
2. Klicken Sie auf **Overview**.
3. Wählen Sie in der Dropdown-Liste **Restart** die Option **Shut Down**.



4. Wenn irgendwelche Benutzer am System angemeldet sind, schreiben Sie einen Grund für das Herunterfahren in das Dialogfeld **Shut Down**.

5. Optional: Wählen Sie in der Dropdown-Liste **Delay** ein Zeitintervall aus.

6. Klicken Sie auf **Shut Down**.

1.8. KONFIGURIEREN DER ZEITEINSTELLUNGEN ÜBER DIE WEB-KONSOLE

Sie können eine Zeitzone einstellen und die Systemzeit mit einem Network Time Protocol (NTP)-Server synchronisieren.

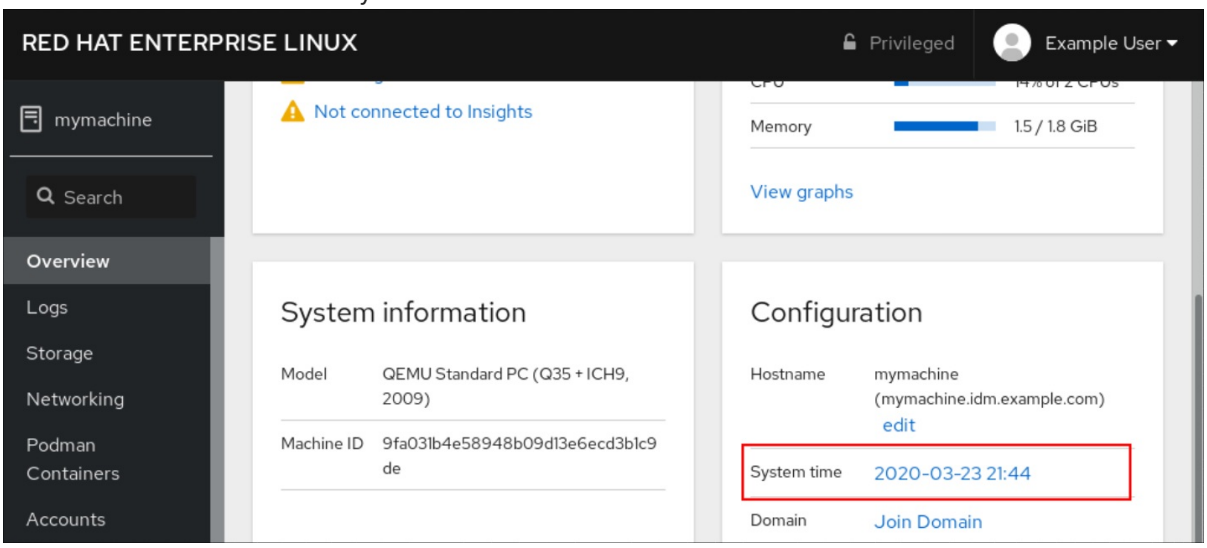
Voraussetzungen

- Die Web-Konsole ist installiert und zugänglich.
  Details finden Sie unter Installieren der Web-Konsole.

Verfahren

1. Melden Sie sich an der RHEL 8 Web-Konsole an.
   Details finden Sie unter Anmeldung an der Web-Konsole.

2. Klicken Sie auf die aktuelle Systemzeit in **Overview**.



3. Ändern Sie im Dialogfeld **Change System Time** die Zeitzone, falls erforderlich.

4. Wählen Sie im Dropdown-Menü **Set Time** eine der folgenden Möglichkeiten:

   Manuell

   Verwenden Sie diese Option, wenn Sie die Zeit manuell einstellen müssen, ohne einen NTP-Server.

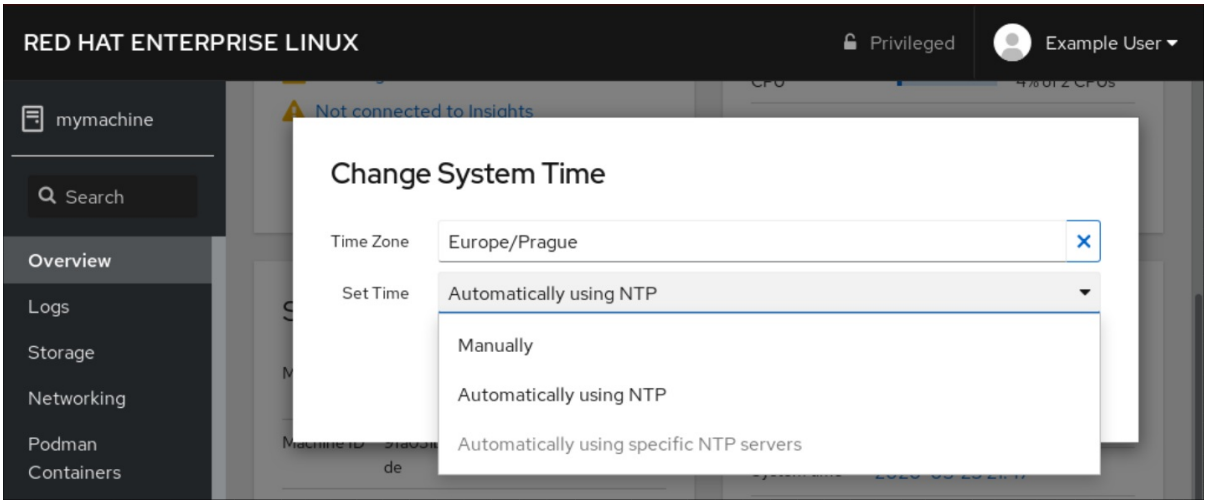
   Automatisch mit NTP-Server

   Dies ist eine Standardoption, die die Zeit automatisch mit den voreingestellten NTP-Servern synchronisiert.

   Automatisch bestimmte NTP-Server verwenden

   Verwenden Sie diese Option nur, wenn Sie das System mit einem bestimmten NTP-Server synchronisieren müssen. Geben Sie den DNS-Namen oder die IP-Adresse des Servers an.

5. Klicken Sie auf **Change**.



Schritte zur Verifizierung

- Überprüfen Sie die Systemzeit, die auf der Registerkarte **System** angezeigt wird.

Zusätzliche Ressourcen

- Verwendung der Chrony-Suite zur Konfiguration von NTP .

1.9. VERBINDEN EINES RHEL 8-SYSTEMS MIT EINER IDM-DOMÄNE ÜBER DIE WEBKONSOLE

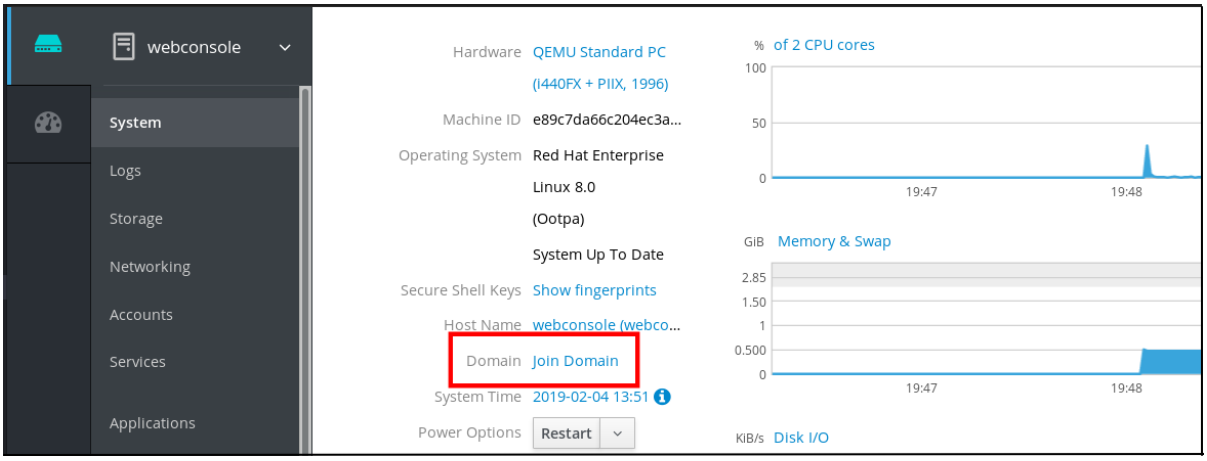
Sie können die Web-Konsole verwenden, um das Red Hat Enterprise Linux 8-System mit der Identity Management (IdM)-Domäne zu verbinden.

Voraussetzungen

- Die IdM-Domäne läuft und ist von dem Client, dem Sie beitreten möchten, erreichbar.
- Sie haben die IdM-Domänenadministrator-Anmeldeinformationen.

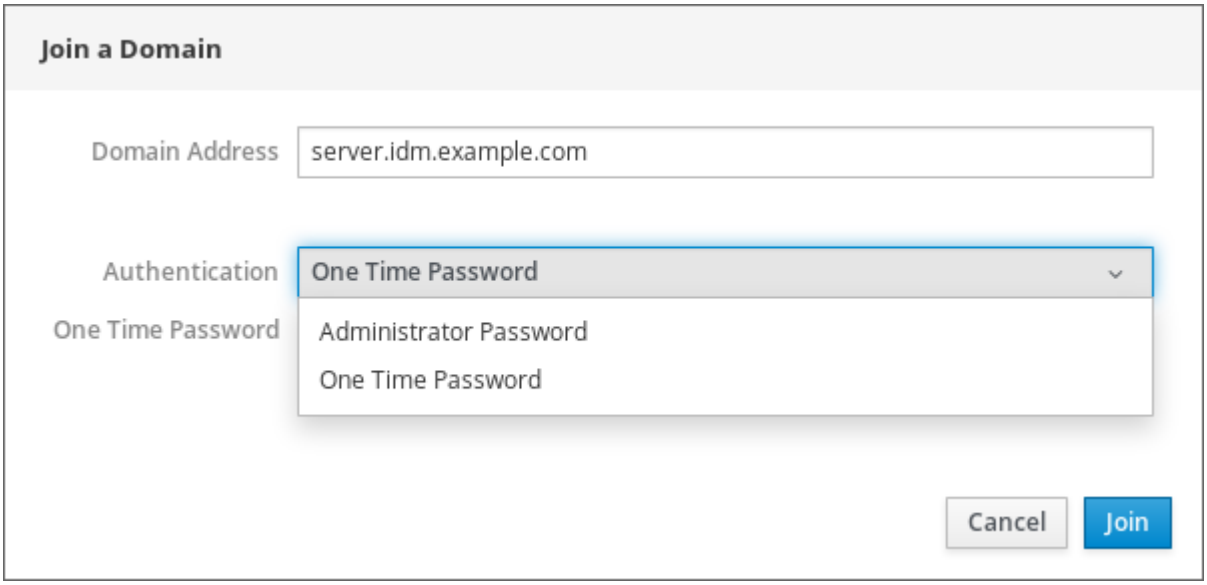
Verfahren

1. Melden Sie sich an der RHEL-Webkonsole an.
   Details finden Sie unter Anmeldung an der Web-Konsole.
2. Öffnen Sie die Registerkarte **System**.
3. Klicken Sie auf **Domäne beitreten**.



4. Geben Sie im Dialogfeld **Join a Domain** den Hostnamen des IdM-Servers in das Feld **Domain Address** ein.

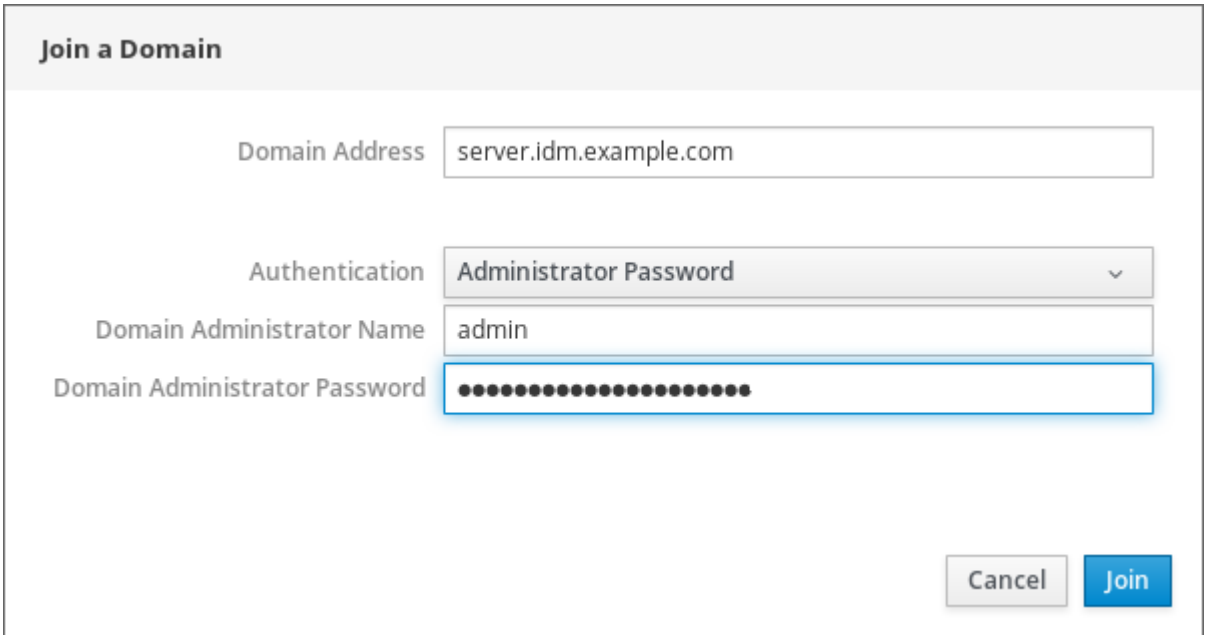
5. Wählen Sie in der Dropdown-Liste **Authentication** aus, ob Sie ein Passwort oder ein Einmalpasswort für die Authentifizierung verwenden möchten.



6. Geben Sie in das Feld **Domain Administrator Name** den Benutzernamen des IdM-Administrationskontos ein.

7. Fügen Sie in das Passwortfeld das Passwort oder Einmalpasswort ein, das Sie zuvor in der Dropdown-Liste **Authentication** ausgewählt haben.

8. Klicken Sie auf **Beitreten**.



Schritte zur Verifizierung

1. Wenn die RHEL 8-Webkonsole keinen Fehler angezeigt hat, wurde das System der IdM-Domäne beigetreten und Sie können den Domänennamen im Bildschirm **System** sehen.

2. Um zu überprüfen, ob der Benutzer ein Mitglied der Domäne ist, klicken Sie auf die Seite Terminal und geben den Befehl **id** ein:

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

Zusätzliche Ressourcen

- Planung der Identitätsverwaltung
- Installieren von Identity Management
- Konfigurieren und Verwalten von Identity Management

1.10. DEAKTIVIEREN VON SMT ZUR VERMEIDUNG VON CPU-SICHERHEITSPROBLEMEN ÜBER DIE WEB-KONSOLE

Deaktivieren Sie Simultaneous Multi Threading (SMT) im Falle von Angriffen, die CPU-SMT missbrauchen. Das Deaktivieren von SMT kann Sicherheitslücken wie L1TF oder MDS abschwächen.

WICHTIG

Das Deaktivieren von SMT kann die Systemleistung verringern.

Voraussetzungen

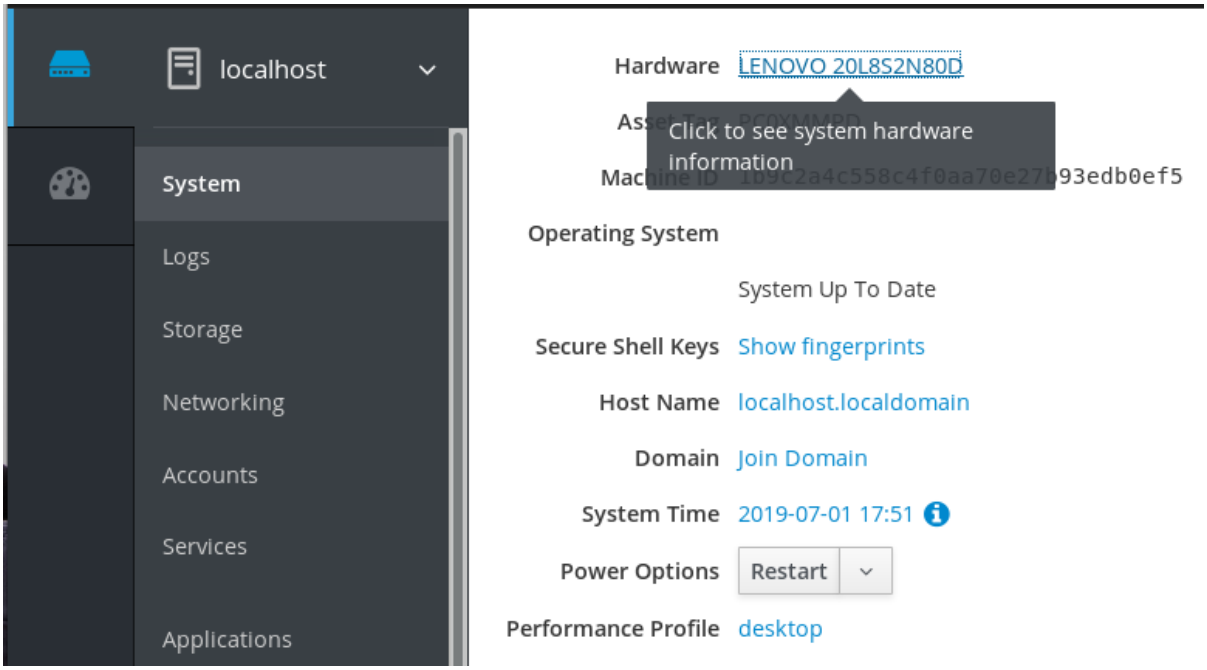
- Die Web-Konsole muss installiert und zugänglich sein.
  Details finden Sie unter Installieren der Web-Konsole.

Verfahren

1. Melden Sie sich an der RHEL 8 Web-Konsole an.
   Details finden Sie unter Anmeldung an der Web-Konsole.

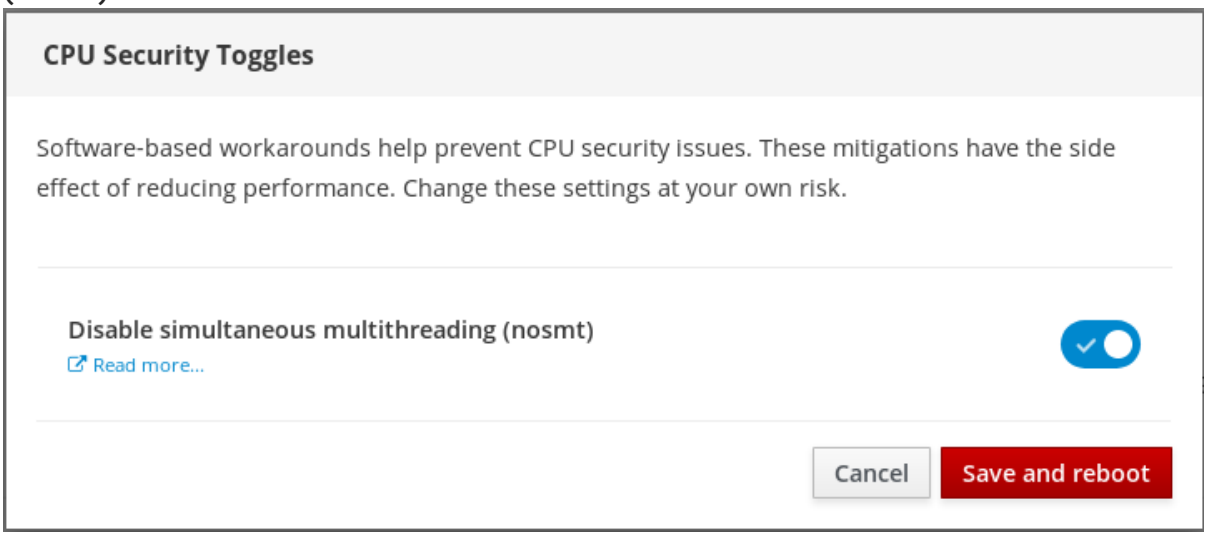
2. Klicken Sie auf **System**.

3. Klicken Sie im Punkt **Hardware** auf die Hardware-Informationen.



4. Klicken Sie im Element **CPU Security** auf **Mitigations**.
   Wenn dieser Link nicht vorhanden ist, bedeutet dies, dass Ihr System SMT nicht unterstützt und daher nicht anfällig ist.

5. Schalten Sie im **CPU Security Toggles** die Option **Disable simultaneous multithreading (nosmt)** ein.



6. Klicken Sie auf die Schaltfläche **Save and reboot**

Nach dem Neustart des Systems verwendet die CPU kein SMT mehr.

Zusätzliche Ressourcen

- L1TF - L1 Terminal Fault Attack - CVE-2018-3620 & CVE-2018-3646

- MDS - Microarchitectural Data Sampling - CVE-2018-12130, CVE-2018-12126, CVE-2018-12127, und CVE-2019-11091

1.11. HINZUFÜGEN EINES BANNERS AUF DER ANMELDESEITE

Unternehmen oder Behörden müssen manchmal eine Warnung anzeigen, dass die Nutzung des Computers für rechtmäßige Zwecke erfolgt, der Benutzer überwacht wird und jeder, der den Computer unbefugt benutzt, strafrechtlich verfolgt wird. Die Warnung muss vor der Anmeldung sichtbar sein. Ähnlich wie bei SSH kann die Web-Konsole optional den Inhalt einer Bannerdatei auf dem Anmeldebildschirm anzeigen. Um Banner in Ihren Webkonsolensitzungen zu aktivieren, müssen Sie die Datei **/etc/cockpit/cockpit.conf** ändern. Beachten Sie, dass die Datei nicht erforderlich ist und Sie sie eventuell manuell erstellen müssen.

Voraussetzungen

- Die Web-Konsole ist installiert und zugänglich. Details finden Sie unter Installieren der Web-Konsole.
- Sie müssen über sudo-Rechte verfügen.

Verfahren

1. Erstellen Sie die Datei **/etc/issue.cockpit** in einem Texteditor Ihrer Wahl, wenn Sie diesen noch nicht haben. Fügen Sie den Inhalt, den Sie als Banner anzeigen möchten, in die Datei ein. Fügen Sie keine Makros in die Datei ein, da keine Umformatierung zwischen dem Dateiinhalt und dem angezeigten Inhalt erfolgt. Verwenden Sie vorgesehene Zeilenumbrüche. Es ist möglich, ASCII-Kunst zu verwenden.
2. Speichern Sie die Datei.
3. Öffnen oder erstellen Sie die Datei **cockpit.conf** im Verzeichnis **/etc/cockpit/** in einem Texteditor Ihrer Wahl.

```
$ sudo vi cockpit.conf
```

4. Fügen Sie den folgenden Text in die Datei ein:

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

5. Speichern Sie die Datei.
6. Starten Sie die Web-Konsole neu, damit die Änderungen wirksam werden.

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

Schritte zur Verifizierung

- Öffnen Sie den Anmeldebildschirm der Web-Konsole erneut, um zu überprüfen, ob das Banner nun sichtbar ist.

Beispiel 1.1. Hinzufügen eines Beispielbanners auf der Anmeldeseite

1. Erstellen Sie mit einem Texteditor eine **/etc/issue.cockpit** Datei mit einem gewünschten Text:

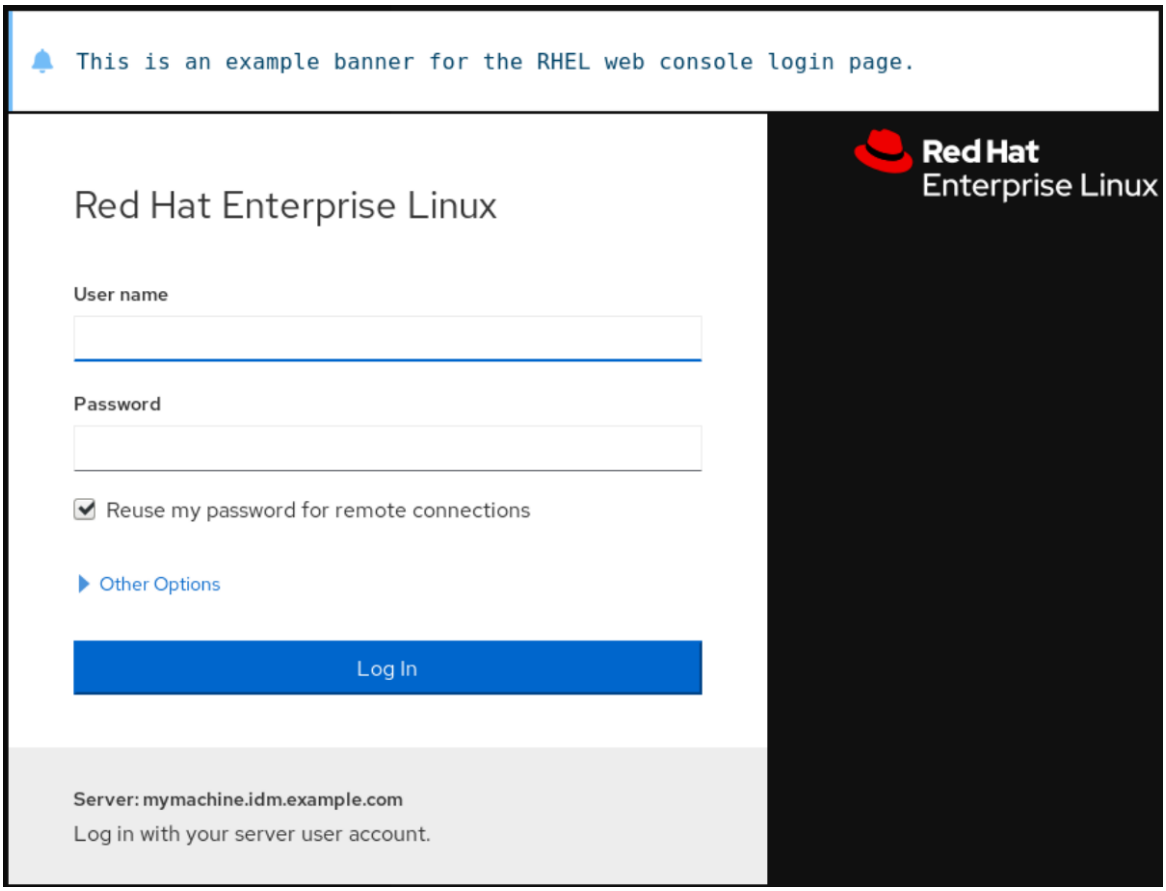
```
Dies ist ein Beispielbanner für die Anmeldeseite der RHEL-Webkonsole.
```

2. Öffnen oder erstellen Sie die Datei **/etc/cockpit/cockpit.conf** und fügen Sie den folgenden Text hinzu:

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

3. Starten Sie die Web-Konsole neu.

4. Öffnen Sie den Anmeldebildschirm der Webkonsole erneut.



1.12. KONFIGURIEREN DER AUTOMATISCHEN LEERLAUFSPERRE IN DER WEB-KONSOLE

Standardmäßig ist in der Webkonsolen-Oberfläche kein Leerlauf-Timeout eingestellt. Wenn Sie ein Leerlauf-Timeout auf Ihrem System aktivieren möchten, können Sie dies durch Ändern der Konfigurationsdatei **/etc/cockpit/cockpit.conf** tun. Beachten Sie, dass die Datei nicht erforderlich ist und Sie sie eventuell manuell erstellen müssen.

Voraussetzungen

- Die Web-Konsole muss installiert und zugänglich sein.
  Details finden Sie unter Installieren der Web-Konsole.

- Sie müssen über sudo-Rechte verfügen.

Verfahren

1. Öffnen oder erstellen Sie die Datei **cockpit.conf** im Verzeichnis **/etc/cockpit/** in einem Texteditor Ihrer Wahl.

```
$ sudo vi cockpit.conf
```

2. Fügen Sie den folgenden Text in die Datei ein:

```
[Session]
IdleTimeout=X
```

   Ersetzen Sie **X** durch eine Zahl für eine Zeitspanne Ihrer Wahl in Minuten.

3. Speichern Sie die Datei.

4. Starten Sie die Web-Konsole neu, damit die Änderungen wirksam werden.

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

Schritte zur Verifizierung

- Prüfen Sie, ob die Sitzung Sie nach einer festgelegten Zeitspanne abmeldet.

KAPITEL 2. KONFIGURIEREN DES HOST-NAMENS IN DER WEB-KONSOLE

Erfahren Sie, wie Sie mit der RHEL 8 Web-Konsole verschiedene Formen des Host-Namens auf dem System konfigurieren können, an das die Web-Konsole angeschlossen ist.

2.1. HOST-NAME

Der Hostname identifiziert das System. Standardmäßig ist der Hostname auf **localhost** eingestellt, aber Sie können ihn ändern.

Ein Hostname besteht aus zwei Teilen:

Host-Name

Es ist ein eindeutiger Name, der ein System identifiziert.

Domain

Fügen Sie die Domain als Suffix hinter dem Hostnamen hinzu, wenn Sie ein System in einem Netzwerk verwenden und wenn Sie Namen statt nur IP-Adressen verwenden.

Ein Hostname mit angehängtem Domänennamen wird als voll qualifizierter Domänenname (FQDN) bezeichnet. Zum Beispiel: **mymachine.example.com**.

Hostnamen werden in der Datei **/etc/hostname** gespeichert.

2.2. HÜBSCHER HOSTNAME IN DER WEB-KONSOLE

Sie können einen hübschen Hostnamen in der RHEL-Webkonsole konfigurieren. Der Pretty-Host-Name ist ein Host-Name mit Großbuchstaben, Leerzeichen und so weiter.

Der hübsche Hostname wird in der Web-Konsole angezeigt, er muss aber nicht mit dem Hostnamen übereinstimmen.

> **Beispiel 2.1. Hostnamenformate in der Web-Konsole**
>
> **Hübscher Hostname**
>
> **My Machine**
>
> **Host-Name**
>
> **mymachine**
>
> **Echter Hostname - voll qualifizierter Domainname (FQDN)**
>
> **mymachine.idm.company.com**

2.3. EINSTELLEN DES HOST-NAMENS ÜBER DIE WEB-KONSOLE

Diese Prozedur stellt den echten Hostnamen oder den hübschen Hostnamen in der Webkonsole ein.

Voraussetzungen

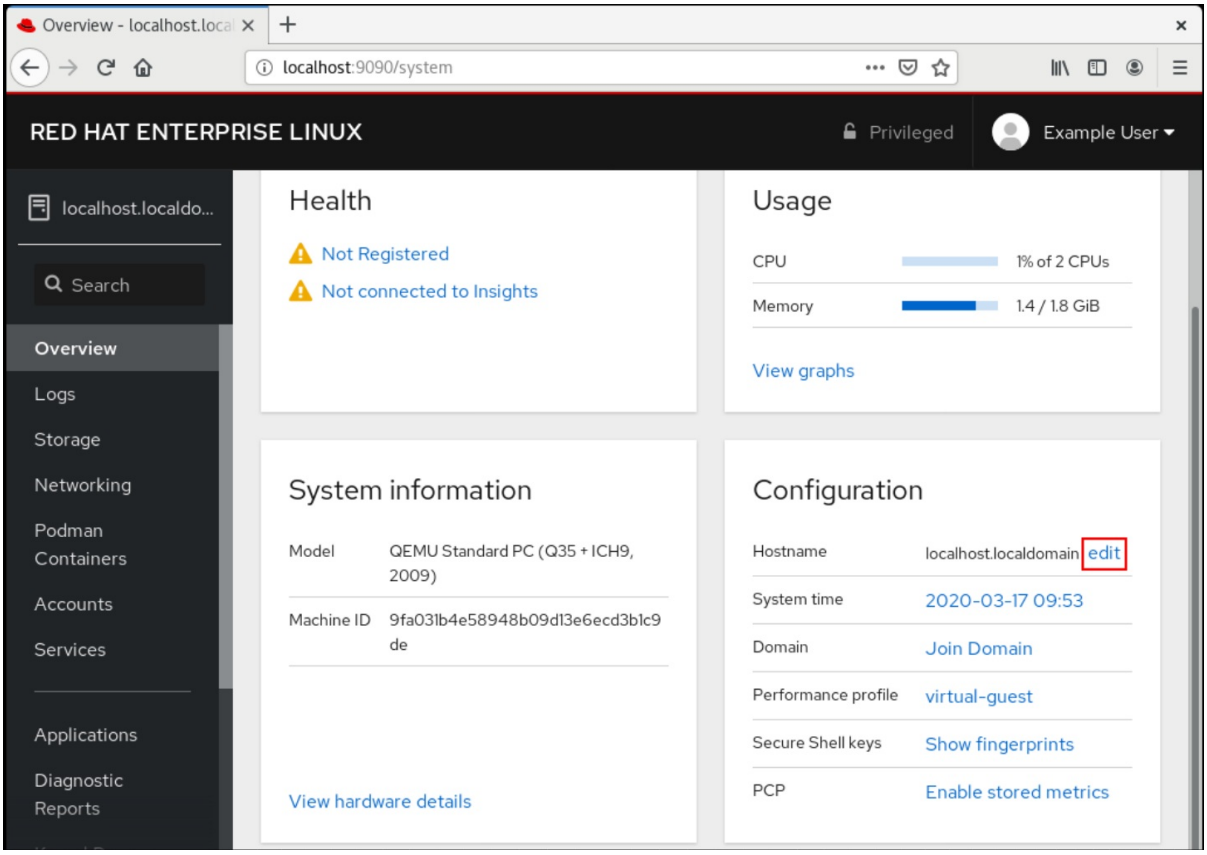
- Die Web-Konsole ist installiert und zugänglich.
  Details finden Sie unter Installieren der Web-Konsole.

Verfahren

1. Melden Sie sich an der RHEL 8 Web-Konsole an.
   Details finden Sie unter Anmeldung an der Web-Konsole.

2. Klicken Sie auf **Übersicht**.

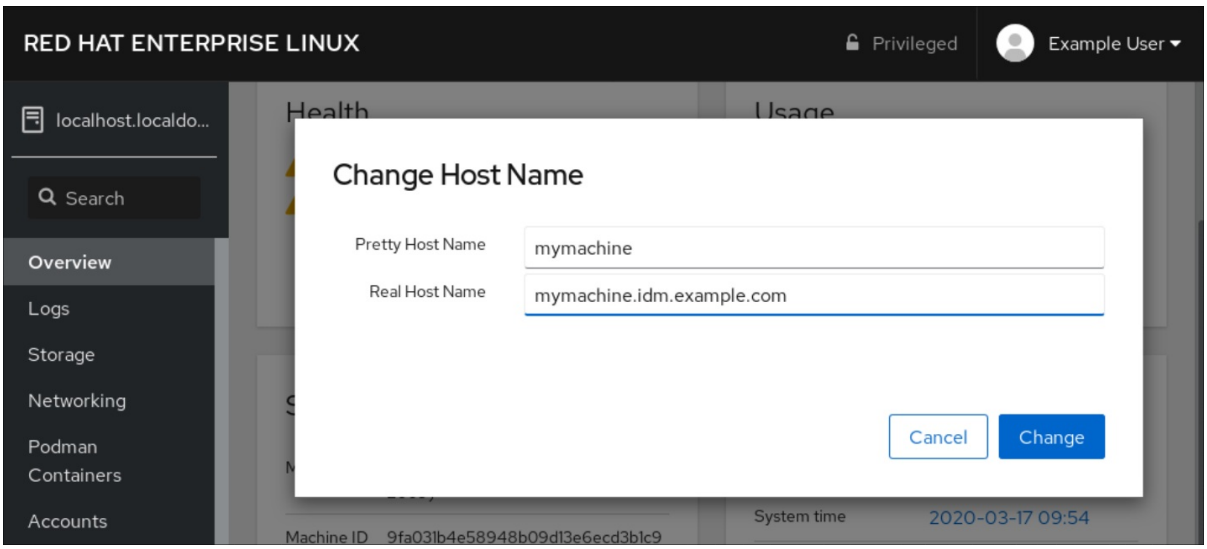
3. Klicken Sie auf **Bearbeiten** neben dem aktuellen Hostnamen.



4. Geben Sie im Dialogfeld **Change Host Name** den Hostnamen in das Feld **Pretty Host Name** ein.

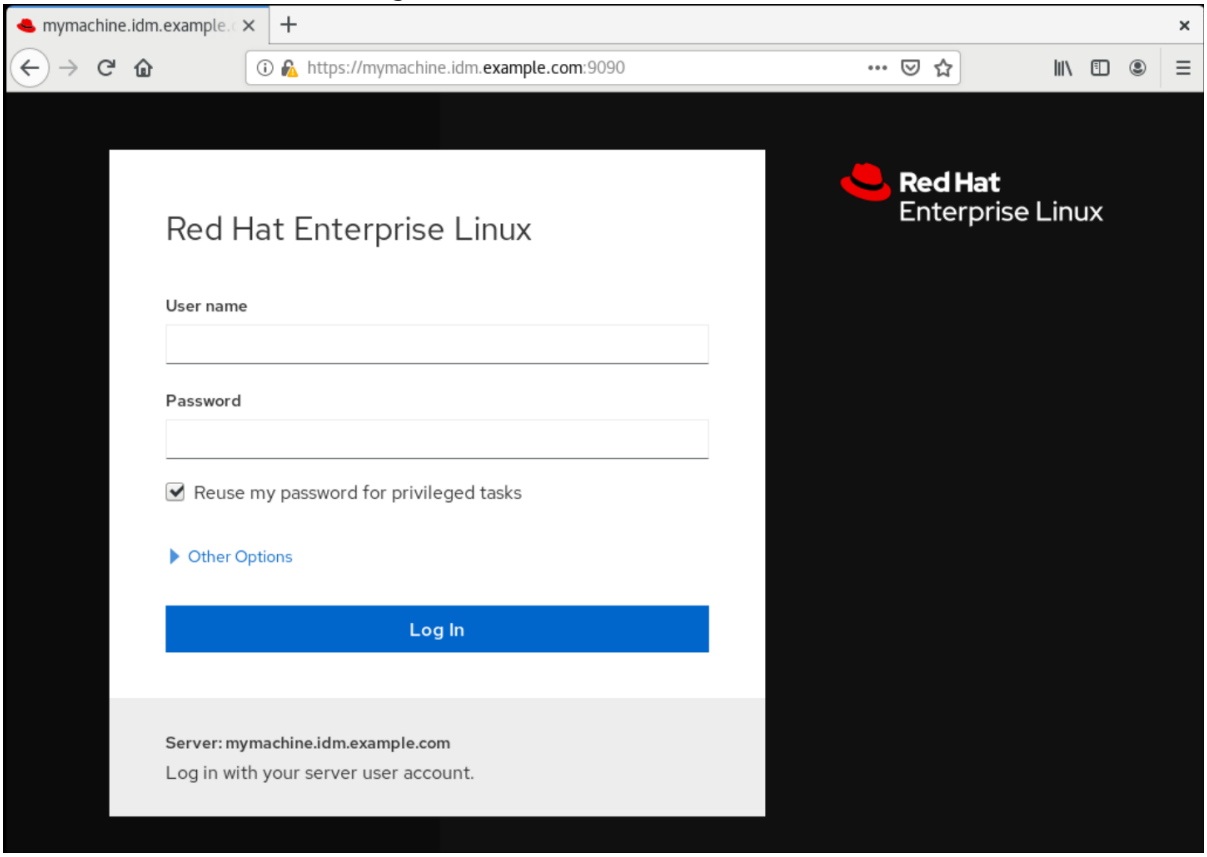
5. Das Feld **Real Host Name** hängt einen Domainnamen an den hübschen Namen.
   Sie können den echten Hostnamen manuell ändern, wenn er nicht mit dem hübschen Hostnamen übereinstimmt.

6. Klicken Sie auf **Ändern**.



Schritte zur Verifizierung

1. Melden Sie sich in der Web-Konsole ab.
2. Öffnen Sie die Web-Konsole erneut, indem Sie eine Adresse mit dem neuen Hostnamen in die Adressleiste Ihres Browsers eingeben.



KAPITEL 3. RED HAT WEB-KONSOLEN-ADD-ONS

Installieren Sie Add-ons in der RHEL 8 Web-Konsole und erfahren Sie, welche Add-on-Anwendungen für Sie verfügbar sind.

3.1. INSTALLIEREN VON ADD-ONS

Das Paket **cockpit** ist standardmäßig Teil von Red Hat Enterprise Linux 8. Um Zusatzanwendungen verwenden zu können, müssen Sie diese separat installieren.

Voraussetzungen

- Installiertes und aktiviertes **cockpit** Paket. Wenn Sie zuerst die Web-Konsole installieren müssen, lesen Sie den Abschnitt über die Installation.

Verfahren

- Installieren Sie ein Add-on.

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

3.2. ADD-ONS FÜR DIE RHEL 8 WEB-KONSOLE

Die folgende Tabelle listet die verfügbaren Zusatzanwendungen für die RHEL 8 Web-Konsole auf.

Feature-Name	Paket-Name	Verwendung
Komponist	cockpit-composer	Erstellen eigener OS-Images
Dashboard	cockpit-dashboard	Verwaltung mehrerer Server in einer Benutzeroberfläche
Maschinen	cockpit-machines	Verwalten von virtuellen Maschinen mit libvirt
PackageKit	cockpit-packagekit	Software-Updates und Anwendungsinstallation (normalerweise standardmäßig installiert)
PCP	cockpit-pcp	Persistente und feinkörnigere Leistungsdaten (bei Bedarf über die Benutzeroberfläche installiert)
podman	cockpit-podman	Verwalten von podman-Containern (verfügbar ab RHEL 8.1)
Session-Aufnahme	cockpit-session-recording	Aufzeichnung und Verwaltung von Benutzersitzungen

KAPITEL 4. OPTIMIEREN DER SYSTEMLEISTUNG ÜBER DIE WEB-KONSOLE

Erfahren Sie, wie Sie in der RHEL 8 Web-Konsole ein Leistungsprofil einstellen, um die Leistung des Systems für eine ausgewählte Aufgabe zu optimieren.

4.1. OPTIONEN FÜR DIE LEISTUNGSOPTIMIERUNG IN DER WEB-KONSOLE

Red Hat Enterprise Linux 8 bietet mehrere Leistungsprofile, die das System für die folgenden Aufgaben optimieren:

- Systeme, die den Desktop verwenden
- Durchsatzleistung
- Latenzleistung
- Netzwerk-Leistung
- Geringe Leistungsaufnahme
- Virtuelle Maschinen

Der Dienst **tuned** optimiert die Systemoptionen entsprechend dem gewählten Profil.

In der Web-Konsole können Sie einstellen, welches Leistungsprofil Ihr System verwendet.

Zusätzliche Ressourcen

- Details zum Dienst **tuned** finden Sie unter Überwachung und Verwaltung von Systemstatus und Leistung.

4.2. EINSTELLEN EINES LEISTUNGSPROFILS IN DER WEB-KONSOLE

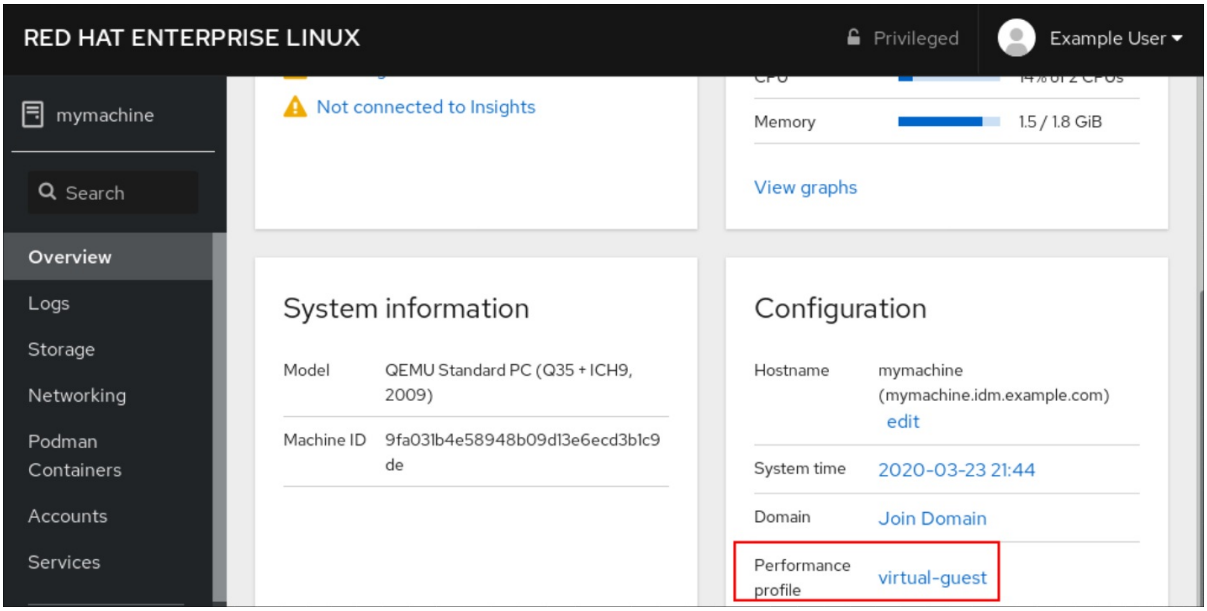
Dieses Verfahren verwendet die Web-Konsole, um die Systemleistung für eine ausgewählte Aufgabe zu optimieren.

Voraussetzungen

- Die Web-Konsole ist installiert und zugänglich.
  Details finden Sie unter Installieren der Web-Konsole.

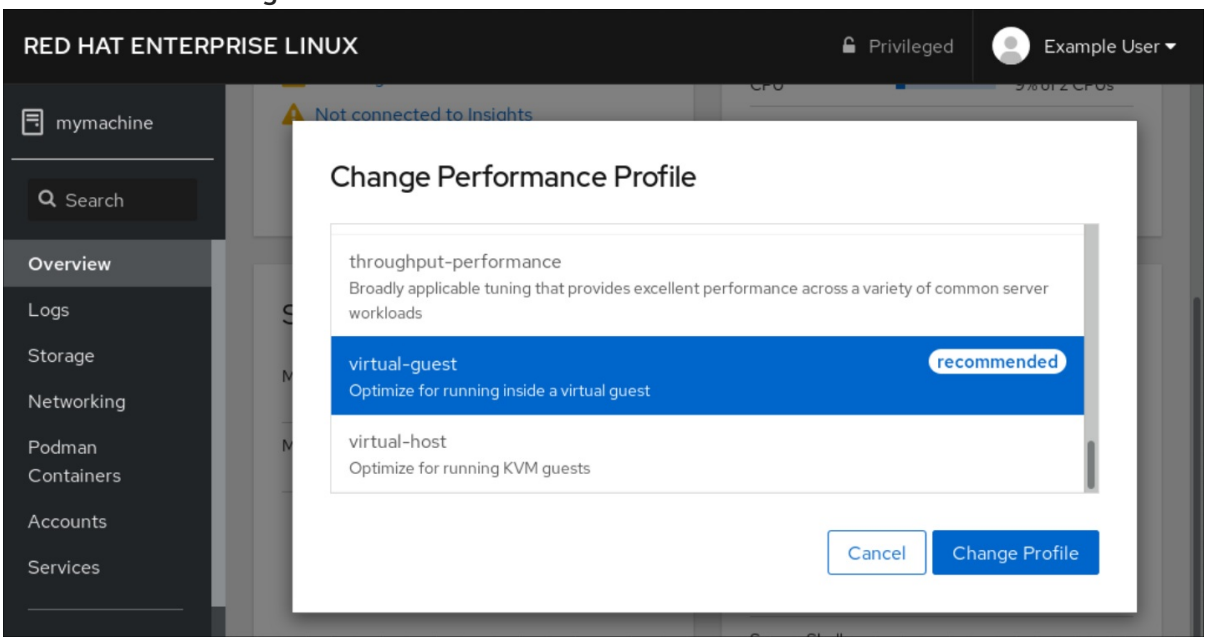
Verfahren

1. Melden Sie sich an der RHEL 8 Web-Konsole an.
   Details finden Sie unter Anmeldung an der Web-Konsole.
2. Klicken Sie auf **Overview**.
3. Klicken Sie im Feld **Performance Profile** auf das aktuelle Leistungsprofil.



4. Ändern Sie im Dialogfeld **Change Performance Profile** das Profil, falls erforderlich.

5. Klicken Sie auf **Change Profile**.



Schritte zur Verifizierung

- Die Registerkarte **Overview** zeigt nun das ausgewählte Leistungsprofil an.

KAPITEL 5. PRÜFEN VON PROTOKOLLEN IN DER WEB-KONSOLE

Erfahren Sie, wie Sie auf Protokolle in der RHEL 8 Web-Konsole zugreifen, diese überprüfen und filtern können.

5.1. PRÜFEN VON PROTOKOLLEN IN DER WEB-KONSOLE

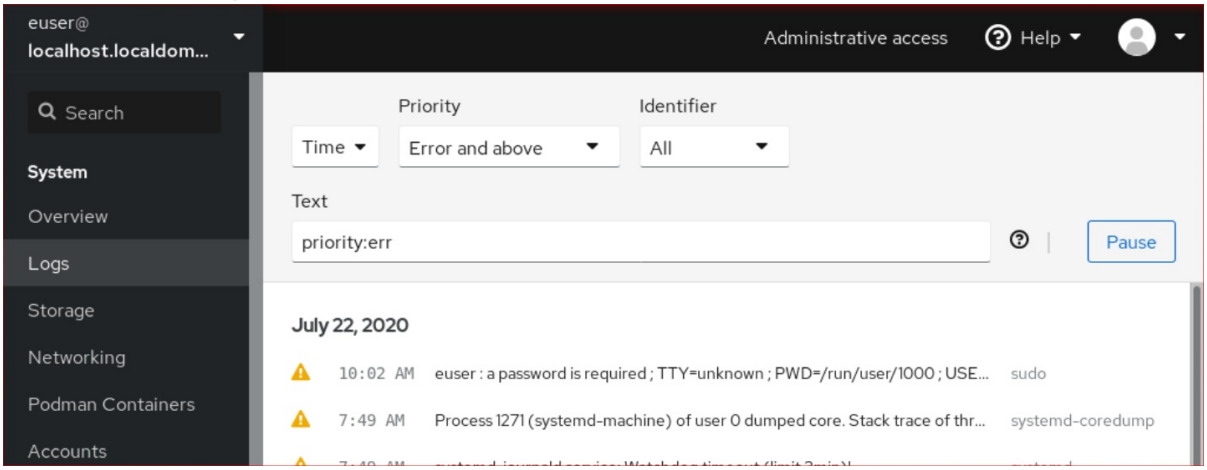
Der Bereich Logs der RHEL 8-Webkonsole ist eine Benutzeroberfläche für das Dienstprogramm **journalctl**. Dieser Abschnitt beschreibt, wie Sie in der Webkonsolen-Oberfläche auf Systemprotokolle zugreifen können.

Voraussetzungen

- Die RHEL 8 Web-Konsole wurde installiert.
  Details finden Sie unter Installieren der Web-Konsole.

Verfahren

1. Melden Sie sich an der RHEL-Webkonsole an.
   Details finden Sie unter Anmeldung an der Web-Konsole.
2. Klicken Sie auf **Logs**.



3. Öffnen Sie die Details des Protokolleintrags, indem Sie in der Liste auf den ausgewählten Protokolleintrag klicken.

ANMERKUNG

Sie können die Schaltfläche **Pause** verwenden, um das Erscheinen neuer Protokolleinträge zu unterbrechen. Sobald Sie neue Protokolleinträge wieder aufnehmen, lädt die Webkonsole alle Protokolleinträge, die gemeldet wurden, nachdem Sie die Schaltfläche **Pause** verwendet haben.

Sie können die Protokolle nach Zeit, Priorität oder Bezeichner filtern. Für weitere Informationen siehe Abschnitt 5.2, »Filtern von Protokollen in der Web-Konsole« .

5.2. FILTERN VON PROTOKOLLEN IN DER WEB-KONSOLE

Dieser Abschnitt zeigt, wie Sie Protokolleinträge in der Web-Konsole filtern können.

Voraussetzungen

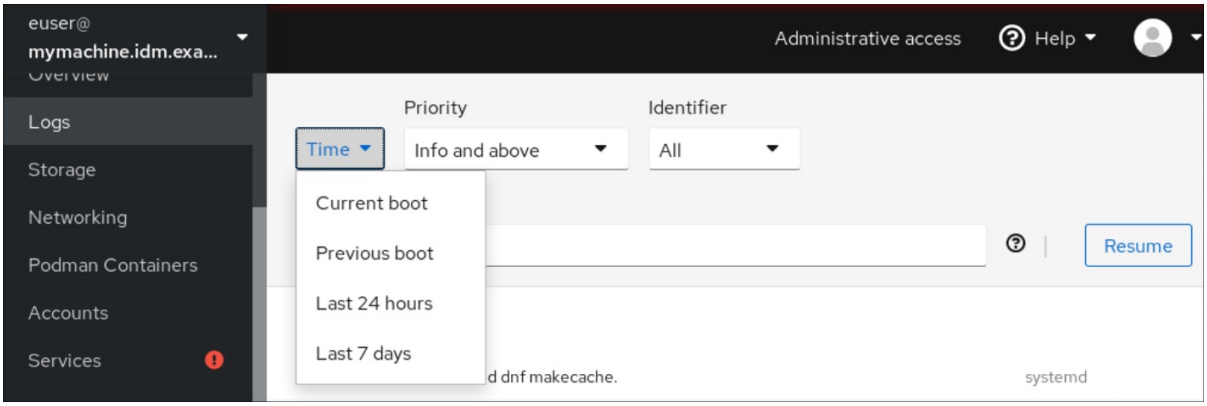
- Die Webkonsolen-Oberfläche muss installiert und zugänglich sein.
  Details finden Sie unter Installieren der Web-Konsole.

Verfahren

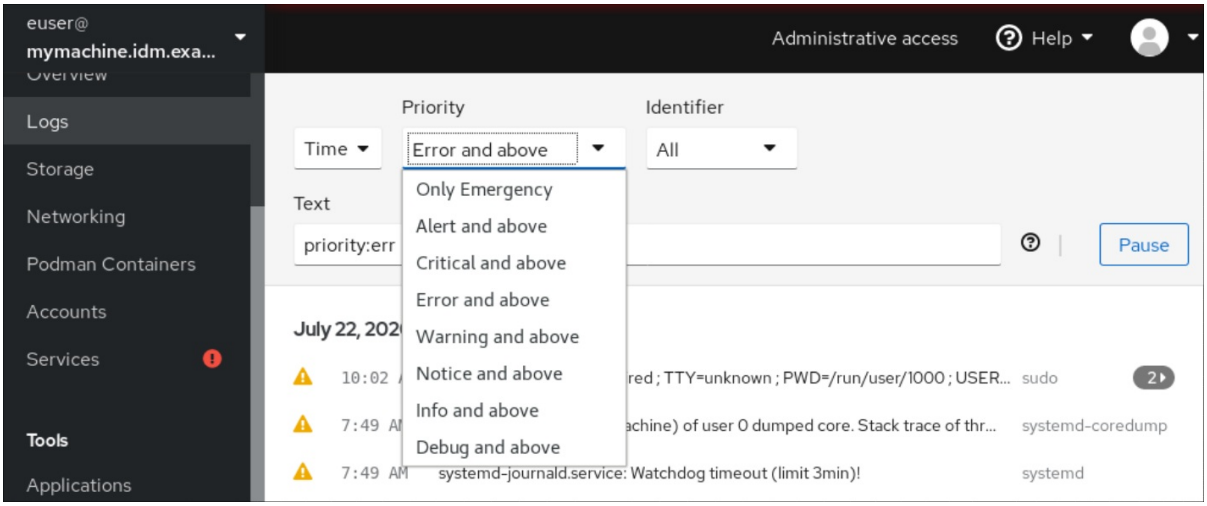
1. Melden Sie sich an der RHEL 8 Web-Konsole an.
   Details finden Sie unter Anmeldung an der Web-Konsole.

2. Klicken Sie auf **Logs**.

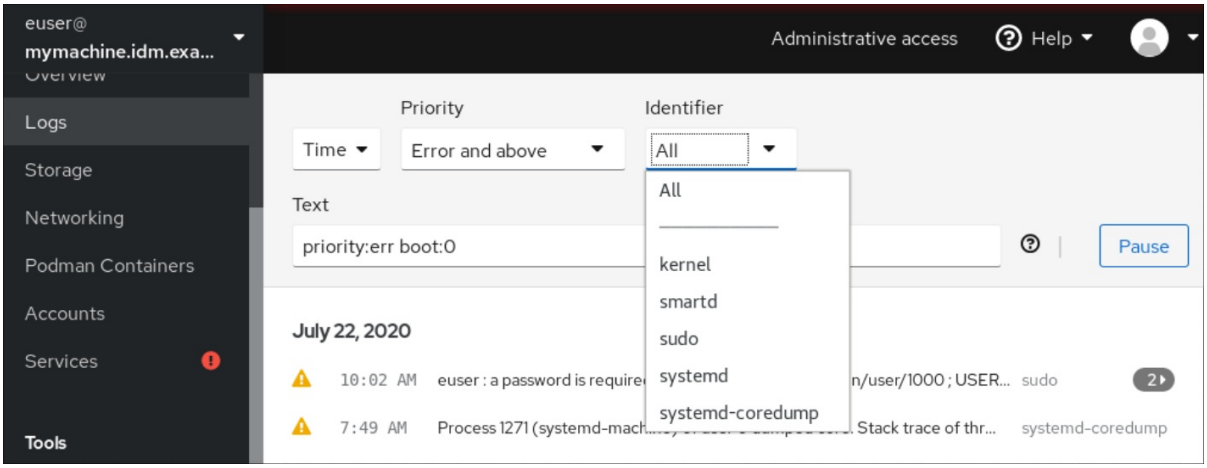
3. Standardmäßig zeigt die Web-Konsole die neuesten Protokolleinträge an. Um nach einem bestimmten Zeitbereich zu filtern, klicken Sie auf das Dropdown-Menü **Time** und wählen eine bevorzugte Option.



4. **Error and above** Liste der Schweregradprotokolle wird standardmäßig angezeigt. Um nach einer anderen Priorität zu filtern, klicken Sie auf das Dropdown-Menü **Error and above** und wählen eine bevorzugte Priorität.



5. Standardmäßig zeigt die Web-Konsole Protokolle für alle Bezeichner an. Um Protokolle für einen bestimmten Bezeichner zu filtern, klicken Sie auf das Dropdown-Menü **All** und wählen einen Bezeichner.



6. Um einen Protokolleintrag zu öffnen, klicken Sie auf ein ausgewähltes Protokoll.

5.3. TEXT-SUCHOPTIONEN ZUM FILTERN VON PROTOKOLLEN IN DER WEB-KONSOLE

Die Funktionalität der Textsuchoption bietet eine große Auswahl an Optionen zum Filtern von Protokollen. Wenn Sie sich entscheiden, Protokolle mit Hilfe der Textsuche zu filtern, können Sie die vordefinierten Optionen verwenden, die in den drei Einblendmenüs definiert sind, oder Sie können die gesamte Suche selbst eingeben.

Dropdown-Menüs

Es gibt drei Einblendmenüs, mit denen Sie die Hauptparameter Ihrer Suche festlegen können:

- **Time**: Dieses Dropdown-Menü enthält vordefinierte Suchen für verschiedene Zeitbereiche Ihrer Suche.
- **Priority**: Dieses Einblendmenü bietet Optionen für verschiedene Prioritätsstufen. Es entspricht der Option **journalctl --priority**. Der Standardwert für die Priorität ist **Error and above**. Er wird immer dann eingestellt, wenn Sie keine andere Priorität angeben.
- **Identifier**: In diesem Einblendmenü können Sie einen Bezeichner auswählen, den Sie filtern möchten. Entspricht der Option **journalctl --identifier**.

Quantoren

Es gibt sechs Quantifizierer, die Sie verwenden können, um Ihre Suche zu spezifizieren. Sie werden in der Tabelle Optionen zum Filtern von Protokollen behandelt.

Log-Felder

Wenn Sie nach einem bestimmten Protokollfeld suchen wollen, können Sie das Feld zusammen mit seinem Inhalt angeben.

Freitextsuche in Protokollnachrichten

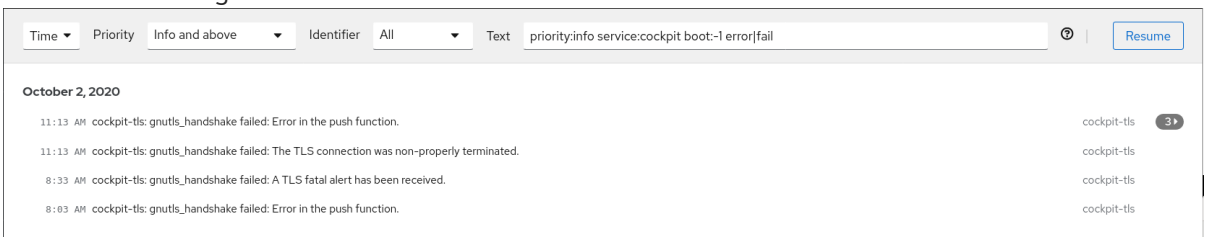
Sie können eine beliebige Textzeichenfolge in den Protokollnachrichten filtern. Die Zeichenfolge kann auch in Form eines regulären Ausdrucks vorliegen.

Erweiterte Filterung von Protokollen I

Filtern Sie alle durch 'systemd' identifizierten Protokollmeldungen, die seit dem 22. Oktober 2020 Mitternacht aufgetreten sind und das Journalfeld 'JOB_TYPE' entweder 'start' oder 'restart' ist.

1. Geben Sie **identifier:systemd since:2020-10-22 JOB_TYPE=start,restart** in das Suchfeld ein.

2. Prüfen Sie die Ergebnisse.

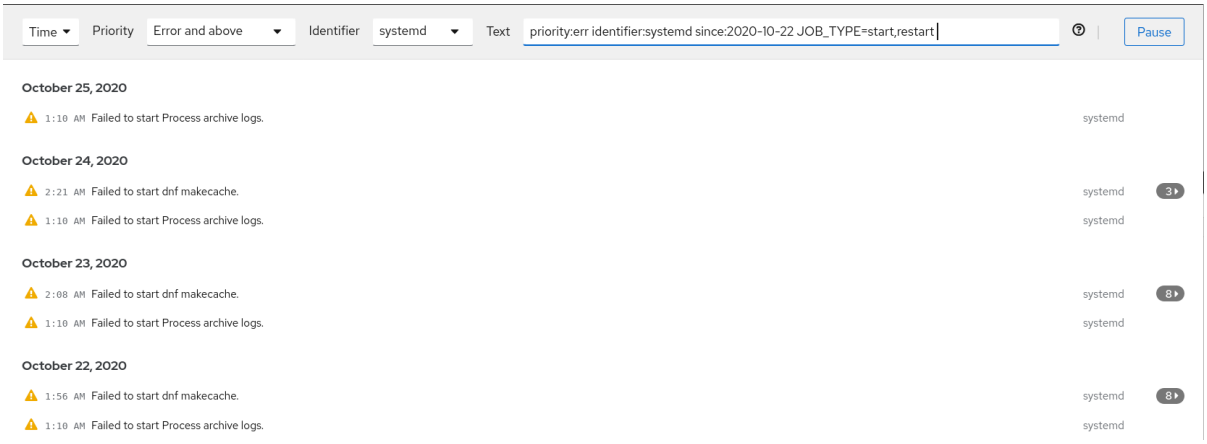


Erweiterte Protokollfilterung II

Filtert alle Protokollmeldungen, die von der systemd-Einheit 'cockpit.service' kommen, die im vorletzten Bootvorgang passiert sind und der Nachrichtentext entweder "error" oder "fail" enthält.

1. Geben Sie **service:cockpit boot:-1 error|fail** in das Suchfeld ein.

2. Prüfen Sie die Ergebnisse.



5.4. VERWENDEN EINES TEXTSUCHFELDS ZUM FILTERN VON PROTOKOLLEN IN DER WEB-KONSOLE

Mit dem Textsuchfeld können Sie Protokolle nach verschiedenen Parametern filtern. Die Suche kombiniert die Verwendung der Filter-Dropdown-Menüs, Quantifizierer, Log-Felder und die Freiform-Stringsuche.

Voraussetzungen

- Die Webkonsolen-Oberfläche muss installiert und zugänglich sein.
  Details finden Sie unter Installieren der Web-Konsole.

Verfahren

1. Melden Sie sich an der RHEL 8 Web-Konsole an.
   Details finden Sie unter Anmeldung an der Web-Konsole.

2. Klicken Sie auf **Logs**.

3. Verwenden Sie die Einblendmenüs, um die drei Hauptquantoren - Zeitbereich, Priorität und Bezeichner - anzugeben, die Sie filtern möchten.

Der Quantifizierer **Priority** muss immer einen Wert haben. Wenn Sie ihn nicht angeben, filtert er automatisch die **Error and above** Priorität. Beachten Sie, dass sich die von Ihnen eingestellten Optionen im Textsuchfeld widerspiegeln.

4. Geben Sie das Protokollfeld an, das Sie filtern möchten.
   Es ist möglich, mehrere Protokollfelder hinzuzufügen.

5. Sie können eine Freiformzeichenkette verwenden, um nach etwas anderem zu suchen. Das Suchfeld akzeptiert auch reguläre Ausdrücke.

5.5. OPTIONEN FÜR DAS FILTERN VON PROTOKOLLEN

Es gibt mehrere **journalctl** Optionen, die Sie zum Filtern von Protokollen in der Web-Konsole verwenden können, die nützlich sein können. Einige davon sind bereits als Teil der Dropdown-Menüs in der Oberfläche der Web-Konsole enthalten.

Tabelle 5.1. Tabelle

Option name	Verwendung	Anmerkungen
priority	Filtert die Ausgabe nach Meldungsprioritäten. Nimmt eine einzelne numerische oder textuelle Protokollstufe an. Die Protokollstufen sind die üblichen Syslog-Protokollstufen. Wenn eine einzelne Protokollebene angegeben wird, werden alle Meldungen mit dieser Protokollebene oder einer niedrigeren (also wichtigeren) Protokollebene angezeigt.	Abgedeckt im Dropdown-Menü **Priority**.
identifier	Zeigt Meldungen für den angegebenen Syslog-Bezeichner SYSLOG_IDENTIFIER an. Kann mehrfach angegeben werden.	Abgedeckt im Dropdown-Menü **Identifier**.
follow	Zeigt nur die neuesten Journaleinträge an und druckt kontinuierlich neue Einträge, sobald sie an das Journal angehängt werden.	Nicht in einer Dropdownliste enthalten.
service	Zeigt Meldungen für das angegebene Gerät **systemd** an. Kann mehrfach angegeben werden.	Wird nicht in einer Dropdownliste abgedeckt. Entspricht dem Parameter **journalctl --unit**.

Option name	Verwendung	Anmerkungen
boot	Meldungen von einem bestimmten Boot anzeigen. Eine positive ganze Zahl sucht die Stiefel vom Anfang des Journals an auf, und eine ganze Zahl gleich oder kleiner als Null sucht die Stiefel vom Ende des Journals an auf. Somit bedeutet 1 den ersten im Journal gefundenen Boot in chronologischer Reihenfolge, 2 den zweiten und so weiter; während -0 der letzte Boot ist, -1 der vorletzte Boot und so weiter.	Wird nur als **Current boot** oder **Previous boot** im Dropdown-Menü **Time** abgedeckt. Andere Optionen müssen manuell geschrieben werden.
since	Starten Sie die Anzeige von Einträgen am oder neuer als das angegebene Datum, bzw. am oder älter als das angegebene Datum. Datumsangaben sollten das Format "2012-10-30 18:17:16" haben. Wenn der Zeitteil weggelassen wird, wird "00:00:00" angenommen. Wenn nur die Sekundenkomponente weggelassen wird, wird ":00" angenommen. Wenn die Datumskomponente weggelassen wird, wird der aktuelle Tag angenommen. Alternativ werden die Zeichenketten "gestern", "heute", "morgen" verstanden, die sich auf 00:00:00 des Tages vor dem aktuellen Tag, des aktuellen Tages bzw. des Tages nach dem aktuellen Tag beziehen. "jetzt" bezieht sich auf die aktuelle Zeit. Schließlich können auch relative Zeiten angegeben werden, die mit dem Präfix "-" oder " " versehen sind und sich auf Zeiten vor bzw. nach der aktuellen Zeit beziehen.	Nicht in einer Dropdownliste enthalten.

KAPITEL 6. VERWALTEN VON BENUTZERKONTEN IN DER WEB-KONSOLE

Die RHEL-Webkonsole bietet eine Oberfläche zum Hinzufügen, Bearbeiten und Entfernen von Systembenutzerkonten.

Nachdem Sie diesen Abschnitt gelesen haben, wissen Sie Bescheid:

- Woher die vorhandenen Konten kommen.
- So fügen Sie neue Konten hinzu.
- So legen Sie den Ablauf des Passworts fest.
- Wie und wann Sie Benutzersitzungen beenden.

Voraussetzungen

- An der RHEL-Webkonsole mit einem Konto angemeldet sein, dem Administratorrechte zugewiesen sind. Details finden Sie unter Anmeldung an der RHEL-Webkonsole.

6.1. IN DER WEB-KONSOLE VERWALTETE SYSTEMBENUTZERKONTEN

Mit Benutzerkonten, die in der RHEL-Webkonsole angezeigt werden, können Sie:

- Authentifizieren Sie Benutzer beim Zugriff auf das System.
- Legen Sie die Zugriffsrechte auf das System fest.

Die RHEL-Webkonsole zeigt alle im System befindlichen Benutzerkonten an. Daher sehen Sie bereits nach der ersten Anmeldung an der Webkonsole mindestens ein Benutzerkonto.

Nach dem Einloggen in die RHEL-Webkonsole können Sie die folgenden Operationen durchführen:

- Erstellen Sie neue Benutzerkonten.
- Ändern Sie ihre Parameter.
- Konten sperren.
- Beenden Sie Benutzersitzungen.

6.2. HINZUFÜGEN NEUER KONTEN ÜBER DIE WEB-KONSOLE

Verwenden Sie die folgenden Schritte zum Hinzufügen von Benutzerkonten zum System und zum Festlegen von Administrationsrechten für die Konten über die RHEL-Webkonsole.

Voraussetzungen

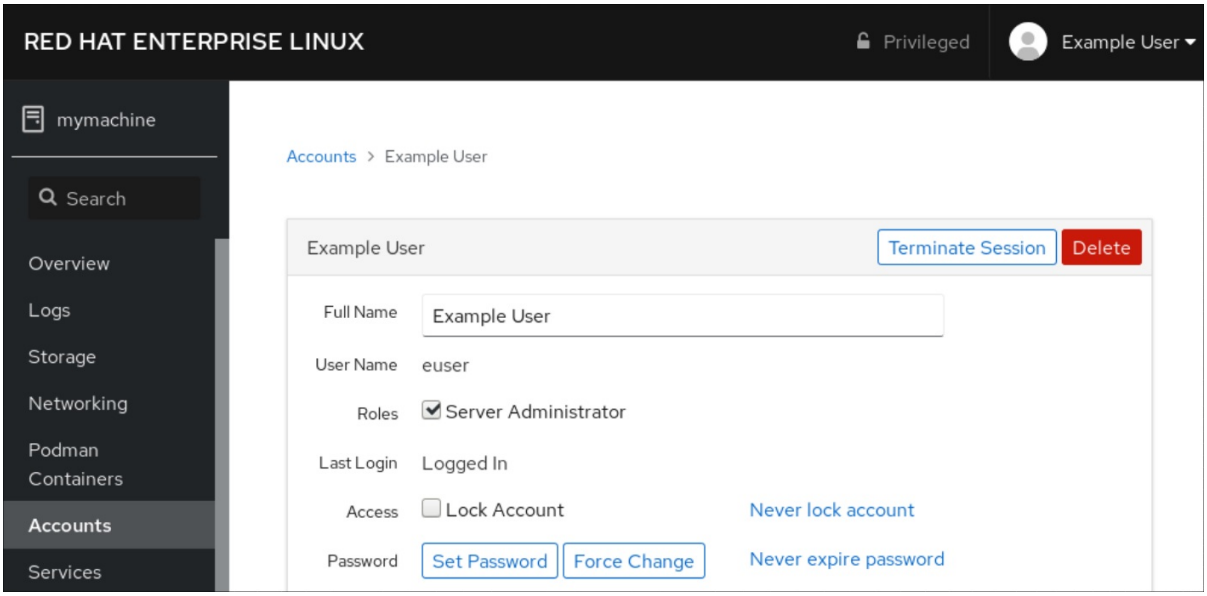
- Die RHEL-Webkonsole muss installiert und zugänglich sein. Details finden Sie unter Installieren der Web-Konsole.

Verfahren

1. Melden Sie sich an der RHEL-Webkonsole an.
2. Klicken Sie auf **Konten**.
3. Klicken Sie auf **Neues Konto erstellen**.

1. Geben Sie in das Feld **Full Name** den vollständigen Namen des Benutzers ein.
   Die RHEL-Webkonsole schlägt automatisch einen Benutzernamen aus dem vollständigen Namen vor und füllt diesen in das Feld **User Name** ein. Wenn Sie nicht die ursprüngliche Namenskonvention, bestehend aus dem ersten Buchstaben des Vornamens und dem ganzen Nachnamen, verwenden wollen, aktualisieren Sie den Vorschlag.
2. Geben Sie in die Felder **Password/Confirm** das Passwort ein und geben Sie es erneut ein, um zu überprüfen, ob Ihr Passwort korrekt ist.
   Der Farbbalken unter den Feldern zeigt Ihnen die Sicherheitsstufe des eingegebenen Passworts an, die es Ihnen nicht erlaubt, einen Benutzer mit einem schwachen Passwort anzulegen.

1. Klicken Sie auf **Erstellen**, um die Einstellungen zu speichern und das Dialogfeld zu schließen.
2. Wählen Sie das neu erstellte Konto aus.
3. Wählen Sie **Server Administrator** im Element **Roles**.



Jetzt sehen Sie das neue Konto in den Einstellungen von **Accounts** und können die Anmeldeinformationen verwenden, um sich mit dem System zu verbinden.

6.3. ERZWINGEN DES ABLAUFS VON PASSWÖRTERN IN DER WEB-KONSOLE

Standardmäßig sind die Passwörter für Benutzerkonten so eingestellt, dass sie nie ablaufen. Sie können Systemkennwörter so einstellen, dass sie nach einer bestimmten Anzahl von Tagen ablaufen. Wenn das Passwort abläuft, wird beim nächsten Anmeldeversuch eine Aufforderung zur Passwortänderung angezeigt.

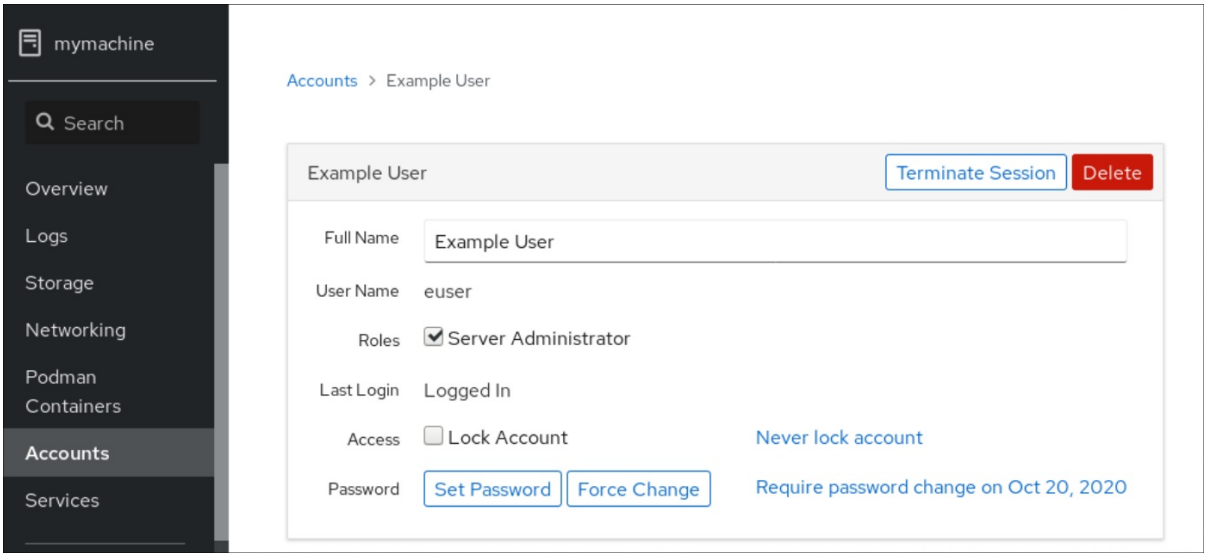
Verfahren

1. Melden Sie sich an der RHEL 8 Web-Konsole an.

2. Klicken Sie auf **Konten**.
3. Wählen Sie das Benutzerkonto, für das der Ablauf des Passworts erzwungen werden soll.
4. Klicken Sie in den Einstellungen des Benutzerkontos auf **Passwort nie ablaufen lassen**.
5. Wählen Sie im Dialogfeld **Password Expiration** die Option **Require password change every ... days** und geben Sie eine positive ganze Zahl ein, die die Anzahl der Tage angibt, nach denen das Passwort abläuft.
1. Klicken Sie auf **Ändern**.

Schritte zur Verifizierung

- Um zu überprüfen, ob der Ablauf des Passworts eingestellt ist, öffnen Sie die Kontoeinstellungen.
  Die RHEL 8 Web-Konsole zeigt einen Link mit dem Ablaufdatum an.



6.4. BEENDEN VON BENUTZERSITZUNGEN IN DER WEB-KONSOLE

Ein Benutzer erstellt Benutzersitzungen, wenn er sich am System anmeldet. Das Beenden von Benutzersitzungen bedeutet, den Benutzer vom System abzumelden. Dies kann hilfreich sein, wenn Sie administrative Aufgaben durchführen müssen, die empfindlich auf Konfigurationsänderungen reagieren, z. B. System-Upgrades.

In jedem Benutzerkonto in der RHEL 8-Webkonsole können Sie alle Sitzungen für das Konto beenden, außer der Webkonsolensitzung, die Sie gerade verwenden. Damit verhindern Sie, dass Sie den Zugriff auf Ihr System verlieren.

Verfahren

1. Melden Sie sich an der RHEL 8 Web-Konsole an.
2. Klicken Sie auf **Konten**.
3. Klicken Sie auf das Benutzerkonto, für das Sie die Sitzung beenden möchten.
4. Klicken Sie auf **Sitzung beenden**.

Wenn die Schaltfläche **Sitzung beenden** inaktiv ist, ist der Benutzer nicht am System angemeldet.

Die RHEL Web-Konsole beendet die Sitzungen.

KAPITEL 7. VERWALTEN VON DIENSTEN IN DER WEB-KONSOLE

Erfahren Sie, wie Sie Systemdienste in der Webkonsolen-Oberfläche von RHEL 8 verwalten können. Sie können Dienste aktivieren oder deaktivieren, sie neu starten oder neu laden oder ihren automatischen Start verwalten.

7.1. AKTIVIEREN ODER DEAKTIVIEREN VON SYSTEMDIENSTEN IN DER WEB-KONSOLE

Mit diesem Verfahren werden Systemdienste über die Webkonsolen-Oberfläche aktiviert oder deaktiviert.

Voraussetzungen

- Die RHEL 8 Web-Konsole wurde installiert.
  Details finden Sie unter Installieren der Web-Konsole.

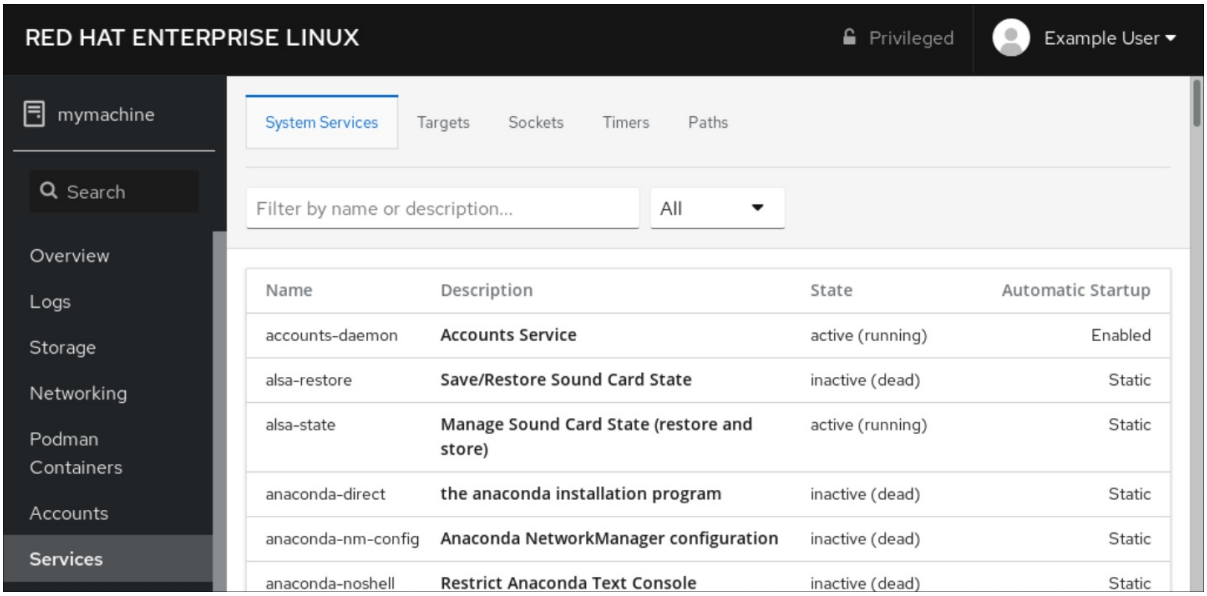
VERFAHREN

Sie können die Dienste nach Name oder Beschreibung und auch nach Aktiviert, Deaktiviert oder Statischer automatischer Start filtern. Die Oberfläche zeigt den aktuellen Status des Dienstes und seine letzten Protokolle an.

1. Melden Sie sich an der RHEL-Webkonsole mit Administratorrechten an.
   Details finden Sie unter Anmeldung an der Web-Konsole.

2. Klicken Sie auf **Services** im Menü der Web-Konsole auf der linken Seite.

3. Die Standard-Registerkarte für **Services** ist **System Services**. Wenn Sie Ziele, Sockets, Timer oder Pfade verwalten wollen, wechseln Sie im Menü oben auf die entsprechende Registerkarte.

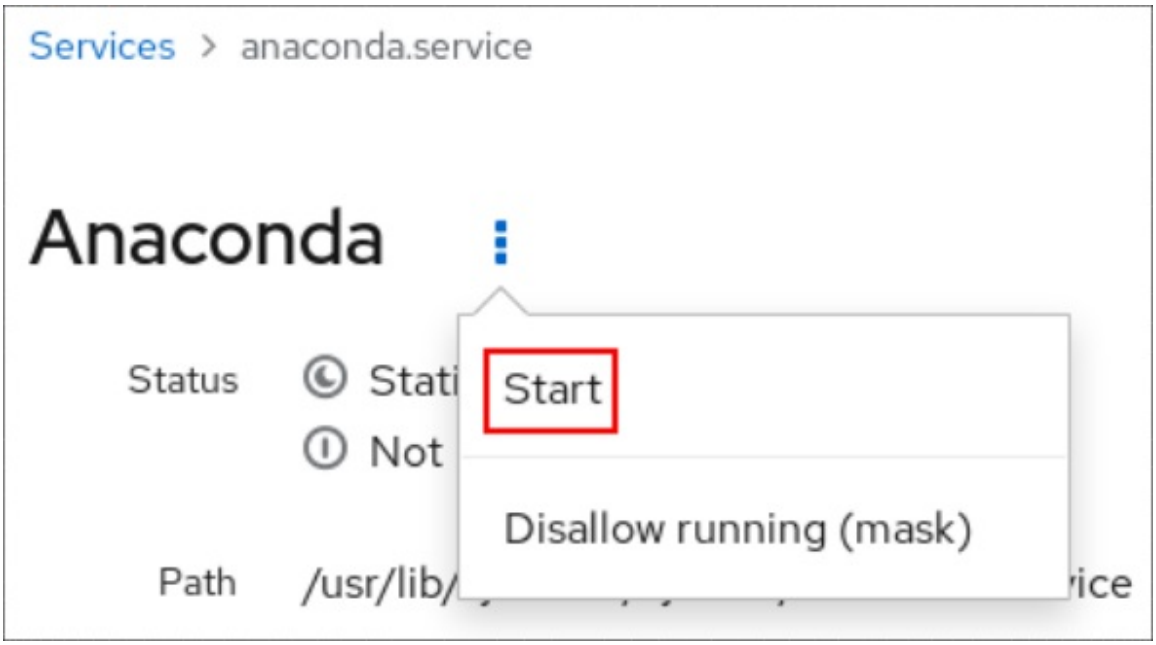


4. Um die Diensteinstellungen zu öffnen, klicken Sie auf einen ausgewählten Dienst in der Liste. Sie können erkennen, welche Dienste aktiv oder inaktiv sind, indem Sie die Spalte **State** überprüfen.

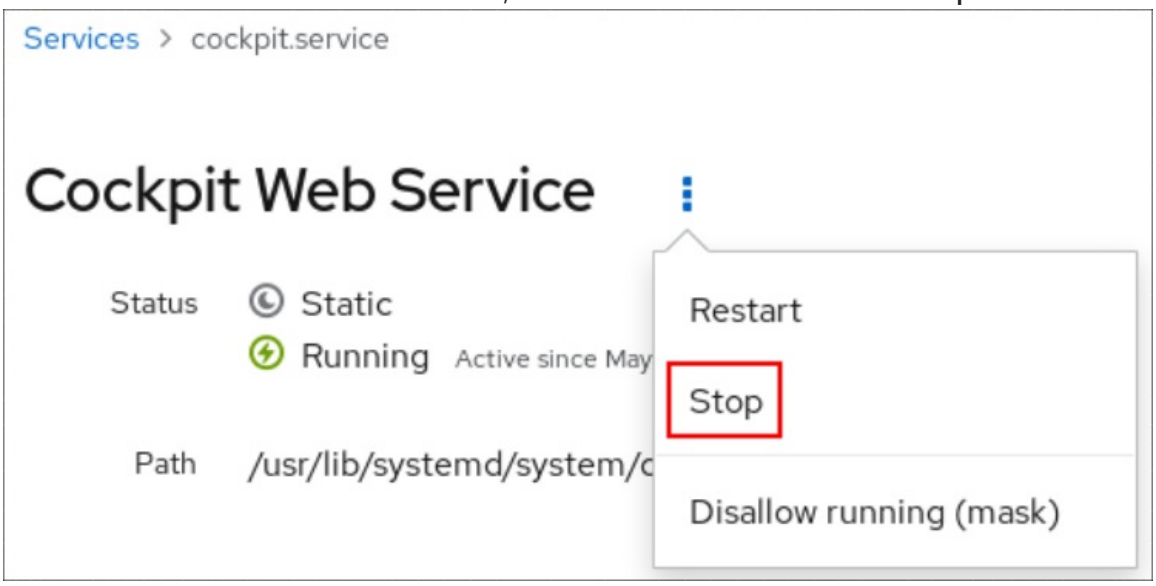
5. Aktivieren oder deaktivieren Sie einen Dienst:

   - Um einen inaktiven Dienst zu aktivieren, klicken Sie auf die Schaltfläche **Start**

- Um einen inaktiven Dienst zu aktivieren, klicken Sie auf die Schaltfläche **Start**.



- Um einen aktiven Dienst zu deaktivieren, klicken Sie auf die Schaltfläche **Stop**.

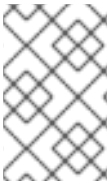


7.2. NEUSTART DER SYSTEMDIENSTE IN DER WEB-KONSOLE

Dieser Vorgang startet die Systemdienste über die Web-Konsolen-Oberfläche neu.

Voraussetzungen

- Die RHEL 8 Web-Konsole wurde installiert.
  Details finden Sie unter Installieren der Web-Konsole.



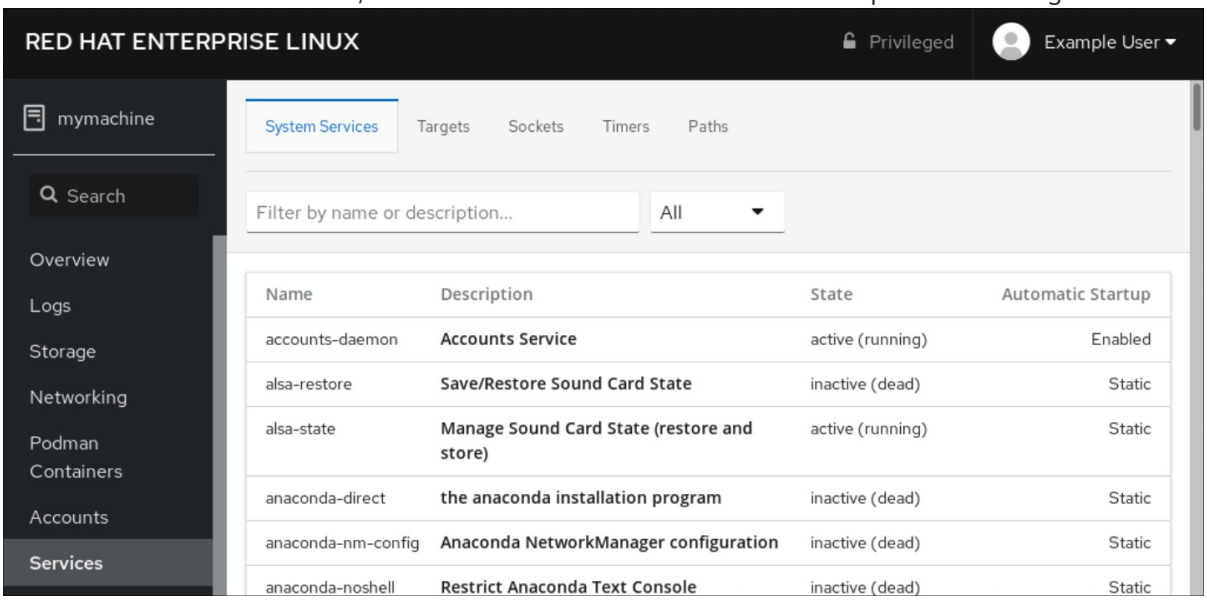
VERFAHREN

Sie können die Dienste nach Name oder Beschreibung und auch nach Aktiviert, Deaktiviert oder Statischer automatischer Start filtern. Die Oberfläche zeigt den aktuellen Status des Dienstes und seine letzten Protokolle an.

1. Melden Sie sich an der RHEL-Webkonsole mit Administratorrechten an.
   Details finden Sie unter Anmeldung an der Web-Konsole.

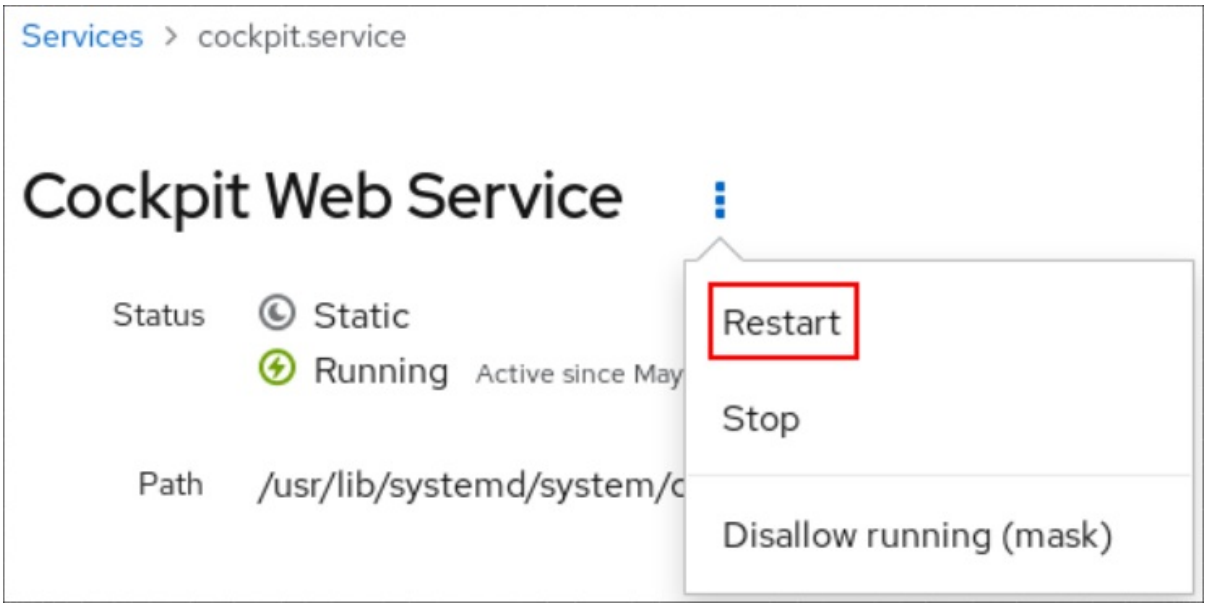
2. Klicken Sie auf **Services** im Menü der Web-Konsole auf der linken Seite.

3. Die Standard-Registerkarte für **Services** ist **System Services**. Wenn Sie Ziele, Sockets, Timer oder Pfade verwalten wollen, wechseln Sie im Menü oben auf die entsprechende Registerkarte.



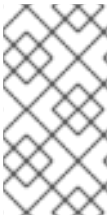
4. Um die Diensteinstellungen zu öffnen, klicken Sie auf einen ausgewählten Dienst in der Liste.

5. Um einen Dienst neu zu starten, klicken Sie auf die Schaltfläche **Restart**.



KAPITEL 8. KONFIGURIEREN VON NETZWERKVERBINDUNGEN ÜBER DIE WEB-KONSOLE

Erfahren Sie, wie Netzwerk-Bonding funktioniert und konfigurieren Sie Netzwerk-Bonds in der RHEL 8 Web-Konsole.



ANMERKUNG

Die RHEL 8 Web-Konsole ist auf dem NetworkManager-Dienst aufgebaut.

Details finden Sie unter Erste Schritte mit NetworkManager zur Verwaltung von Netzwerken.

Voraussetzungen

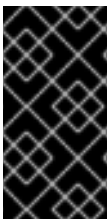
- Die RHEL 8 Web-Konsole ist installiert und aktiviert.
  Details finden Sie unter Installieren der Web-Konsole.

8.1. VERSTEHEN VON NETZWERK-BONDING

Netzwerk-Bonding ist eine Methode zur Kombination oder Aggregation von Netzwerkschnittstellen, um eine logische Schnittstelle mit höherem Durchsatz oder Redundanz bereitzustellen.

Die Modi **active-backup**, **balance-tlb** und **balance-alb** erfordern keine spezielle Konfiguration des Netzwerk-Switches. Andere Bonding-Modi erfordern jedoch eine Konfiguration des Switches zur Aggregation der Links. Cisco-Switches benötigen z. B. **EtherChannel** für die Modi 0, 2 und 3, aber für Modus 4 sind das Link Aggregation Control Protocol (LACP) und **EtherChannel** erforderlich.

Weitere Details finden Sie in der Dokumentation zu Ihrem Switch und im Linux Ethernet Bonding Driver HOWTO.



WICHTIG

Bestimmte Netzwerk-Bonding-Funktionen, wie z. B. der Fail-Over-Mechanismus, unterstützen keine direkten Kabelverbindungen ohne einen Netzwerk-Switch. Weitere Details finden Sie im Abschnitt Wird Bonding bei direkter Verbindung über Crossover-Kabel unterstützt? KCS-Lösung.

8.2. BOND-MODI

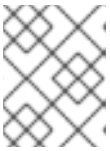
In RHEL 8 gibt es mehrere Modus-Optionen. Jede Modusoption zeichnet sich durch spezifische Lastverteilung und Fehlertoleranz aus. Das Verhalten der gebündelten Schnittstellen hängt vom Modus ab. Die Bonding-Modi bieten Fehlertoleranz, Lastausgleich oder beides.

Lastausgleichsmodi

- **Round Robin**: Sequentielle Übertragung von Paketen von der ersten verfügbaren Schnittstelle zur letzten.

Fehlertoleranz-Modi

- **Active Backup**: Nur wenn die primäre Schnittstelle ausfällt, wird sie durch eine der Backup-Schnittstellen ersetzt. Nur eine von der aktiven Schnittstelle verwendete MAC-Adresse ist sichtbar.
- **Broadcast**: Alle Übertragungen werden an alle Schnittstellen gesendet.



ANMERKUNG

Das Broadcasting erhöht den Netzwerkverkehr auf allen gebundenen Schnittstellen erheblich.

Modi für Fehlertoleranz und Lastausgleich

- **XOR**: Die Ziel-MAC-Adressen werden mit einem Modulo-Hash gleichmäßig auf die Schnittstellen verteilt. Jede Schnittstelle bedient dann die gleiche Gruppe von MAC-Adressen.
- **802.3ad**: Legt eine dynamische IEEE 802.3ad Link-Aggregationsrichtlinie fest. Erzeugt Aggregationsgruppen, die dieselben Geschwindigkeits- und Duplex-Einstellungen verwenden. Sendet und empfängt auf allen Schnittstellen im aktiven Aggregator.

ANMERKUNG

Dieser Modus erfordert einen Switch, der 802.3ad-kompatibel ist.

- **Adaptive transmit load balancing**: Der ausgehende Verkehr wird entsprechend der aktuellen Last auf jeder Schnittstelle verteilt. Eingehender Verkehr wird von der aktuellen Schnittstelle empfangen. Wenn die empfangende Schnittstelle ausfällt, übernimmt eine andere Schnittstelle die MAC-Adresse der ausgefallenen Schnittstelle.
- **Adaptive load balancing**: Umfasst den Sende- und Empfangslastausgleich für IPv4-Verkehr. Der Empfangslastausgleich wird durch die Aushandlung des Address Resolution Protocol (ARP) erreicht, daher ist es notwendig, in der Konfiguration des Bonds **Link Monitoring** auf **ARP** zu setzen.

8.3. HINZUFÜGEN EINER NEUEN BINDUNG ÜBER DIE WEB-KONSOLE

Konfigurieren Sie einen Active-Backup-Verbund auf zwei oder mehr Netzwerkschnittstellen mit der Web-Konsole.

Andere Netzwerk-Bond-Modi können auf ähnliche Weise konfiguriert werden.

Voraussetzungen

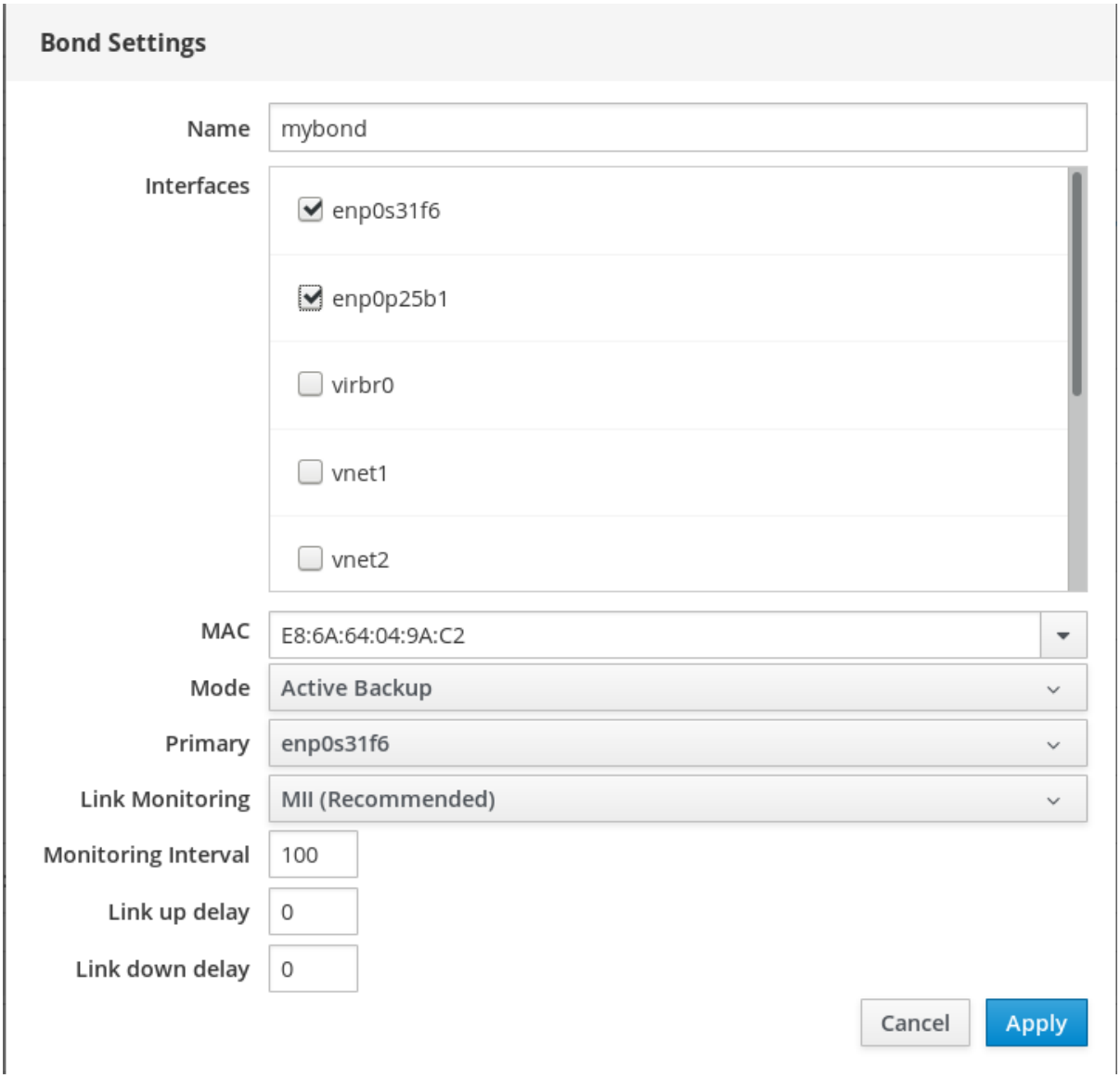
- Im Server sind zwei oder mehr Netzwerkkarten installiert.
- Die Netzwerkkarten sind mit einem Switch verbunden.

Verfahren

1. Melden Sie sich an der Web-Konsole an.
   Details finden Sie unter Anmeldung an der Web-Konsole.
2. Öffnen Sie **Networking**.

3. Klicken Sie auf die Schaltfläche **Add Bond**.
4. Geben Sie im Dialogfeld **Bond Settings** einen Namen für die neue Anleihe ein.
5. Wählen Sie im Feld **Members** Schnittstellen aus, die Mitglied des Verbunds sein sollen.
6. [Optional] Wählen Sie in der Dropdown-Liste **MAC** eine MAC-Adresse, die für diese Schnittstelle verwendet werden soll.
   Wenn Sie das Feld **MAC** leer lassen, erhält die Anleihe eine der Adressen, die in der Dropdown-Liste aufgeführt sind.
7. Wählen Sie in der Dropdown-Liste **Mode** den Modus aus.
   Für Details siehe Netzwerk-Bond-Modi
8. Wenn Sie **Active Backup** wählen, wählen Sie die primäre Schnittstelle.

9. Lassen Sie im Dropdown-Menü **Link Monitoring** die Option **MII** stehen.
   Nur für den adaptiven Lastausgleichsmodus muss diese Option auf **ARP** umgestellt werden.
10. Die Felder **Monitoring Interval**, **Link up delay** und **Link down delay**, die Werte in Millisekunden enthalten, lassen Sie so, wie sie sind. Ändern Sie sie nur zur Fehlersuche.
11. Klicken Sie auf **Apply**.



Um zu überprüfen, ob die Verbindung korrekt funktioniert, gehen Sie in den Bereich **Networking** und prüfen Sie, ob die Spalten **Sending** und **Receiving** in der Tabelle **Interfaces** eine Netzwerkaktivität anzeigen.

8.4. HINZUFÜGEN VON SCHNITTSTELLEN ZUM BOND ÜBER DIE WEB-KONSOLE

Netzwerkverbindungen können mehrere Schnittstellen umfassen und Sie können jederzeit eine davon hinzufügen oder entfernen.

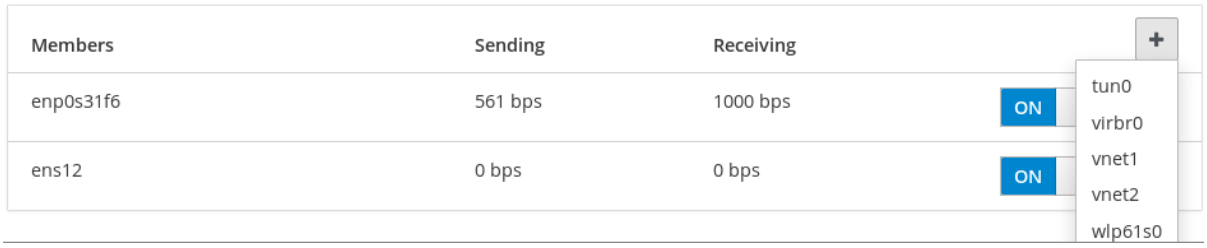
Erfahren Sie, wie Sie eine Netzwerkschnittstelle zu einer bestehenden Verbindung hinzufügen.

Voraussetzungen

- Wenn Sie eine Verbindung mit mehreren Schnittstellen haben, die wie in Abschnitt 8.3, »Hinzufügen einer neuen Bindung über die Web-Konsole« beschrieben konfiguriert sind.

Verfahren

1. Melden Sie sich an der Web-Konsole an.
   Details finden Sie unter Anmeldung an der Web-Konsole.
2. Öffnen Sie **Networking**.
3. Klicken Sie in der Tabelle **Interfaces** auf die Bindung, die Sie konfigurieren möchten.
4. Blättern Sie im Bildschirm mit den Bindungseinstellungen nach unten zur Tabelle der Mitglieder (Schnittstellen).
5. Klicken Sie auf das Symbol .
6. Wählen Sie die Schnittstelle in der Dropdown-Liste aus und klicken Sie darauf.



Die RHEL 8 Web-Konsole fügt die Schnittstelle zum Bond hinzu.

8.5. ENTFERNEN ODER DEAKTIVIEREN EINER SCHNITTSTELLE AUS DEM BOND ÜBER DIE WEB-KONSOLE

Netzwerkbonds können mehrere Schnittstellen umfassen. Wenn Sie ein Gerät wechseln müssen, können Sie bestimmte Schnittstellen aus der Bindung entfernen oder deaktivieren, was mit den restlichen aktiven Schnittstellen funktioniert.

Um die Verwendung einer in einer Anleihe enthaltenen Schnittstelle zu beenden, können Sie:

- Entfernen Sie die Schnittstelle aus dem Verbund.
- Deaktivieren Sie die Schnittstelle vorübergehend. Die Schnittstelle bleibt Teil des Verbunds, aber der Verbund verwendet sie nicht, bis Sie sie wieder aktivieren.

Voraussetzungen

- Wenn Sie eine Verbindung mit mehreren Schnittstellen haben, die wie in Abschnitt 8.3, »Hinzufügen einer neuen Bindung über die Web-Konsole« beschrieben konfiguriert sind.

Verfahren

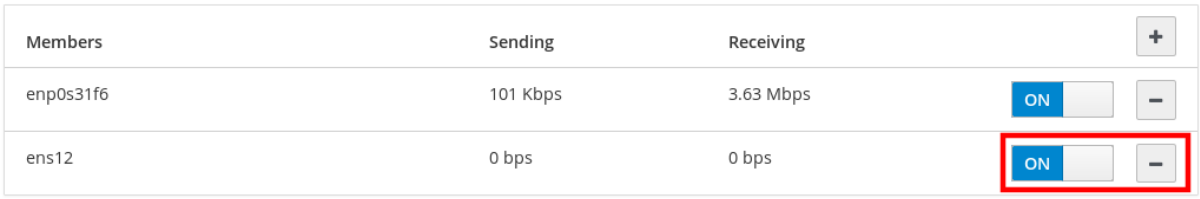
1. Melden Sie sich an der RHEL-Webkonsole an.
   Details finden Sie unter Anmeldung an der Web-Konsole.
2. Öffnen Sie **Networking**.

3. Klicken Sie auf die Bindung, die Sie konfigurieren möchten.

4. Blättern Sie im Bildschirm mit den Bindungseinstellungen nach unten zur Tabelle der Ports (Schnittstellen).

5. Wählen Sie die Schnittstelle und und entfernen oder deaktivieren Sie sie:

   - Klicken Sie auf das Symbol **-**, um die Schnittstelle zu entfernen.
   - Schalten Sie die Taste **ON/OFF** auf Aus.



Basierend auf Ihrer Wahl entfernt oder deaktiviert die Web-Konsole die Schnittstelle aus dem Verbund und Sie können sie wieder im Bereich **Networking** als eigenständige Schnittstelle sehen.

8.6. ENTFERNEN ODER DEAKTIVIEREN EINER BINDUNG ÜBER DIE WEB-KONSOLE

Entfernen oder deaktivieren Sie einen Netzwerk-Bond über die Web-Konsole. Wenn Sie den Bond deaktivieren, bleiben die Schnittstellen im Bond, aber der Bond wird nicht für den Netzwerkverkehr verwendet.

Voraussetzungen

- Es gibt eine bestehende Verbindung in der Web-Konsole.

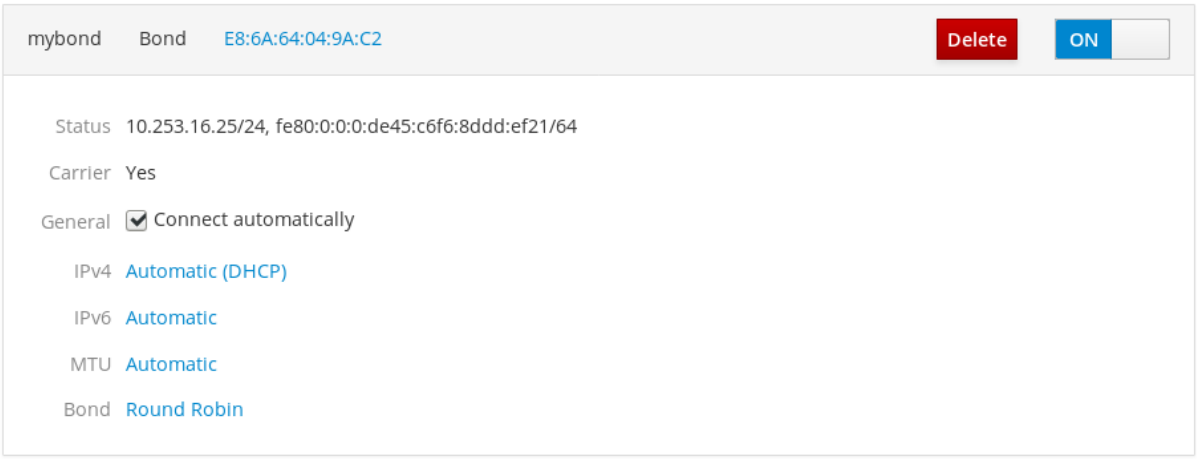
Verfahren

1. Melden Sie sich an der Web-Konsole an.
   Details finden Sie unter Anmeldung an der Web-Konsole.

2. Öffnen Sie **Networking**.

3. Klicken Sie auf die Bindung, die Sie entfernen möchten.

4. Im Bildschirm für die Bindungseinstellungen können Sie die Bindung mit der Schaltfläche **ON/OFF** deaktivieren oder auf die Schaltfläche **Delete** klicken, um die Bindung dauerhaft zu entfernen.



Sie können zurück zu **Networking** gehen und überprüfen, dass alle Schnittstellen aus dem Verbund nun eigenständige Schnittstellen sind.

KAPITEL 9. KONFIGURIEREN VON NETZWERKTEAMS ÜBER DIE WEB-KONSOLE

Erfahren Sie, wie Netzwerk-Bonding funktioniert, was die Unterschiede zwischen Netzwerk-Teams und Netzwerk-Bonds sind und welche Möglichkeiten der Konfiguration in der Web-Konsole bestehen.

Zusätzlich finden Sie Richtlinien für:

- Hinzufügen eines neuen Netzwerkteams
- Hinzufügen neuer Schnittstellen zu einem bestehenden Netzwerkteam
- Entfernen von Schnittstellen aus einem bestehenden Netzwerkteam
- Entfernen eines Netzwerkteams

Voraussetzungen

- Die RHEL 8 Web-Konsole ist installiert und aktiviert.
  Details finden Sie unter Installieren der Web-Konsole.

9.1. VERSTEHEN VON NETZWERK-TEAMING

Netzwerk-Teaming ist eine Funktion, die Netzwerkschnittstellen kombiniert oder aggregiert, um eine logische Schnittstelle mit höherem Durchsatz oder Redundanz bereitzustellen.

Netzwerk-Teaming verwendet einen Kernel-Treiber, um die schnelle Verarbeitung von Paketflüssen zu implementieren, sowie User-Space-Bibliotheken und Dienste für andere Aufgaben. Auf diese Weise ist Netzwerk-Teaming eine leicht erweiterbare und skalierbare Lösung für Lastausgleichs- und Redundanzanforderungen.

WICHTIG

Bestimmte Netzwerk-Teaming-Funktionen, wie z. B. der Fail-Over-Mechanismus, unterstützen keine direkten Kabelverbindungen ohne einen Netzwerk-Switch. Weitere Details finden Sie unter Wird Bonding bei direkter Verbindung über Crossover-Kabel unterstützt?

9.2. VERGLEICH VON NETZWERK-TEAMING- UND BONDING-FUNKTIONEN

Erfahren Sie mehr über die Funktionen, die in Netzwerkteams und Netzwerkverbindungen unterstützt werden:

Funktion	Netzwerkverbindung	Netzwerk-Team
Broadcast Tx-Richtlinie	Ja	Ja
Round-Robin Tx-Politik	Ja	Ja
Aktiv-Backup Tx-Richtlinie	Ja	Ja

Funktion	Netzwerkverbindung	Netzwerk-Team
LACP (802.3ad) Unterstützung	Ja (nur aktiv)	Ja
Hash-basierte Tx-Richtlinie	Ja	Ja
Benutzer kann Hash-Funktion einstellen	Nein	Ja
Unterstützung des Tx-Lastausgleichs (TLB)	Ja	Ja
LACP-Hash-Port auswählen	Ja	Ja
Load-Balancing für LACP-Unterstützung	Nein	Ja
Ethtool Link-Überwachung	Ja	Ja
ARP-Link-Überwachung	Ja	Ja
NS/NA (IPv6) Link-Überwachung	Nein	Ja
Ports auf/ab Verzögerungen	Ja	Ja
Port-Prioritäten und Stickiness ("primäre" Optionserweiterung)	Nein	Ja
Separate Einrichtung der Link-Überwachung pro Port	Nein	Ja
Einrichtung der Überwachung mehrerer Verbindungen	Begrenzt	Ja
Sperrfreier Tx/Rx-Pfad	Nein (rwlock)	Ja (RCU)
VLAN-Unterstützung	Ja	Ja
Benutzerraum-Laufzeitsteuerung	Begrenzt	Ja
Logik im Anwenderbereich	Nein	Ja
Erweiterbarkeit	Hart	Einfach
Modularer Aufbau	Nein	Ja
Performance-Overhead	Niedrig	Sehr niedrig

Funktion	Netzwerkverbindung	Netzwerk-Team
D-Bus-Schnittstelle	Nein	Ja
Stapeln mehrerer Geräte	Ja	Ja
Nullkonfiguration mit LLDP	Nein	(in Planung)
NetworkManager-Unterstützung	Ja	Ja

9.3. HINZUFÜGEN EINES NEUEN TEAMS ÜBER DIE WEB-KONSOLE

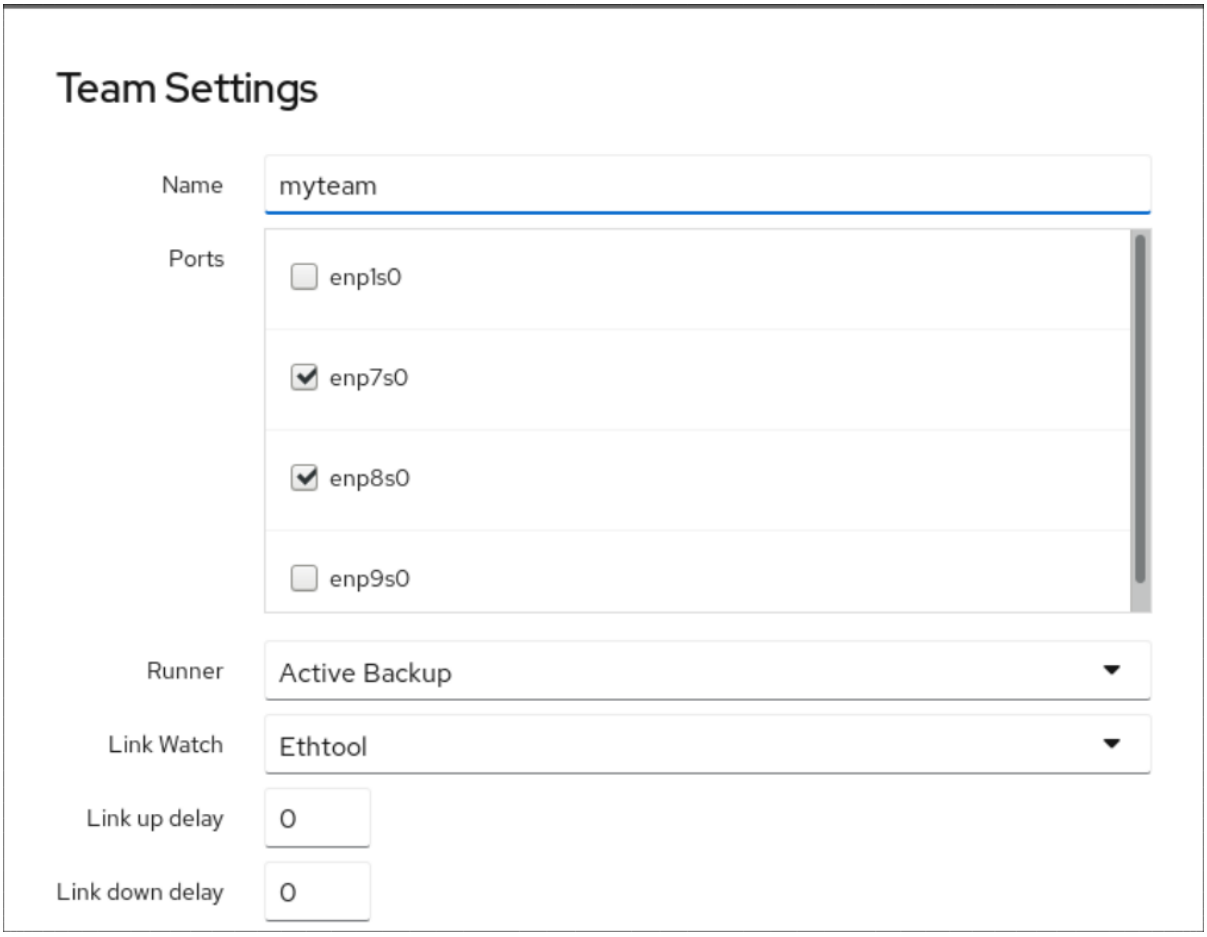
Konfigurieren Sie über die Web-Konsole ein neues aktives Backup-Netzwerkteam auf zwei oder mehr Netzwerkschnittstellen.

Voraussetzungen

- Zwei oder mehr Netzwerkkarten auf dem Server installiert.
- Die Netzwerkkarten sind mit einem Switch verbunden.

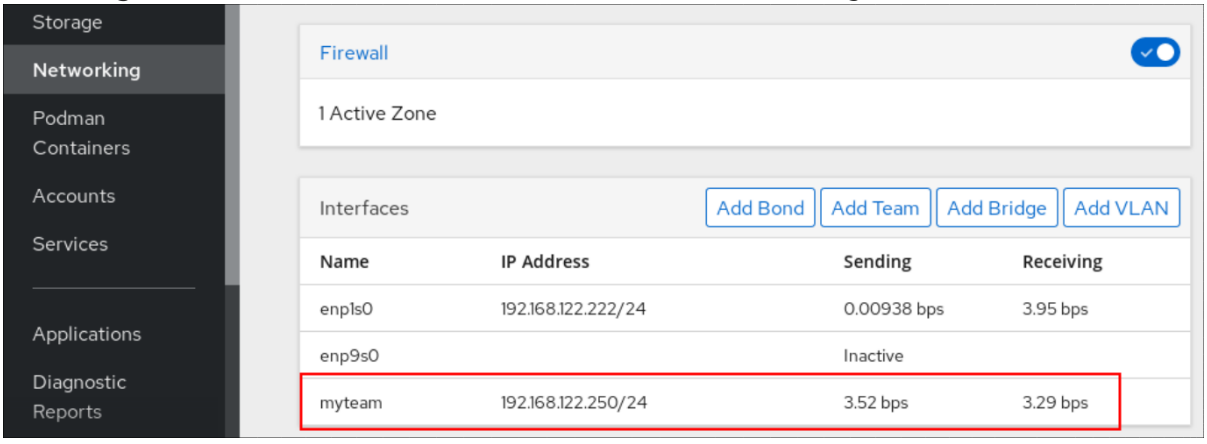
Verfahren

1. Melden Sie sich an der Web-Konsole an.
   Details finden Sie unter Anmelden an der Web-Konsole
2. Wechseln Sie zur Registerkarte **Networking**.
3. Klicken Sie auf die Schaltfläche **Add Team**.
4. Im Bereich **Team Settings** konfigurieren Sie Parameter für das neue Team:
   a. Fügen Sie einen Namen für Ihr Team-Gerät in das Feld **Name** ein.
   b. Wählen Sie im Feld **Ports** alle Netzwerkschnittstellen aus, die Sie dem Team hinzufügen möchten.
   c. Wählen Sie im Dropdown-Menü **Runner** den Läufer aus.
   d. Wählen Sie im Dropdown-Menü **Link Watch** einen Link Watcher aus.
      i. Wenn Sie **Ethtool** wählen, stellen Sie zusätzlich eine Verzögerung für den Verbindungsaufbau und eine Verzögerung für den Verbindungsabbau ein.
      ii. Wenn Sie **ARP Ping** oder **NSNA Ping** wählen, legen Sie zusätzlich ein Ping-Intervall und ein Ping-Ziel fest.
5. Klicken Sie auf **Apply**



Schritte zur Verifizierung

1. Wechseln Sie zur Registerkarte **Networking** und prüfen Sie, ob die Spalten **Sending** und **Receiving** in der Tabelle Schnittstellen eine Netzwerkaktivität anzeigen.



Zusätzliche Ressourcen

- Netzwerk-Team-Läufer

9.4. HINZUFÜGEN NEUER SCHNITTSTELLEN ZUM TEAM ÜBER DIE WEB-KONSOLE

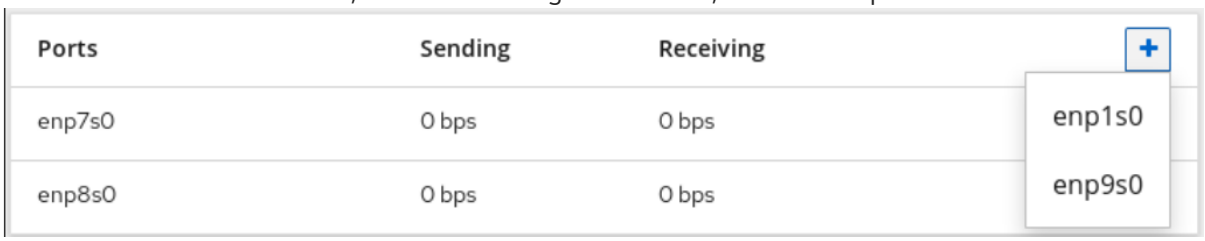
Netzwerkteams können mehrere Schnittstellen umfassen, und es ist jederzeit möglich, eine beliebige Schnittstelle hinzuzufügen oder zu entfernen. Der folgende Abschnitt beschreibt, wie Sie eine neue Netzwerkschnittstelle zu einem bestehenden Team hinzufügen.

Voraussetzungen

- Ein Netzwerkteam mit ist konfiguriert.

Verfahren

1. Melden Sie sich an der Web-Konsole an.
   Details finden Sie unter Anmeldung an der Web-Konsole.
2. Wechseln Sie auf die Registerkarte **Networking**.
3. Klicken Sie in der Tabelle **Interfaces** auf das Team, das Sie konfigurieren möchten.
4. Blättern Sie im Fenster "Teameinstellungen" nach unten zur Tabelle **Ports**.
5. Klicken Sie auf das Symbol .
6. Wählen Sie die Schnittstelle, die Sie hinzufügen möchten, aus der Dropdown-Liste aus.



Die Web-Konsole von RHEL 8 fügt die Schnittstelle zum Team hinzu.

9.5. ENTFERNEN ODER DEAKTIVIEREN EINER SCHNITTSTELLE AUS DEM TEAM ÜBER DIE WEB-KONSOLE

Netzwerkteams können mehrere Schnittstellen enthalten. Wenn Sie ein Gerät ändern müssen, können Sie bestimmte Schnittstellen aus dem Netzwerkteam entfernen oder deaktivieren, die dann mit dem Rest der aktiven Schnittstellen zusammenarbeiten.

Es gibt zwei Möglichkeiten, wie Sie die Verwendung einer in einem Team enthaltenen Schnittstelle beenden können:

- Entfernen der Schnittstelle aus dem Team
- Vorübergehendes Deaktivieren der Schnittstelle. Die Schnittstelle bleibt dann ein Teil des Teams, aber das Team wird sie nicht verwenden, bis Sie sie wieder aktivieren.

Voraussetzungen

- Auf dem Host ist ein Netzwerkteam mit mehreren Schnittstellen vorhanden.

Verfahren

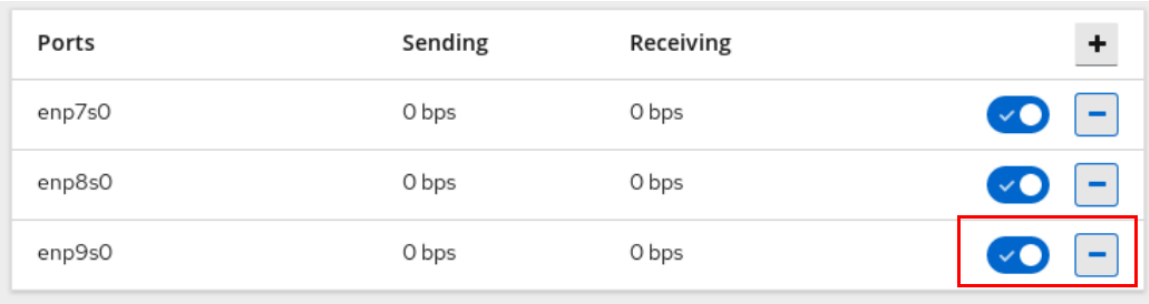
1. Melden Sie sich an der RHEL-Webkonsole an.
   Details finden Sie unter Anmeldung an der Web-Konsole.
2. Wechseln Sie auf die Registerkarte **Networking**.
3. Klicken Sie auf das Team, das Sie konfigurieren möchten.

4. Blättern Sie im Fenster der Teameinstellungen nach unten zur Tabelle der Ports (Schnittstellen).

5. Wählen Sie eine Schnittstelle und entfernen oder deaktivieren Sie sie.

   a. Schalten Sie die Taste **ON/OFF** auf Off, um die Schnittstelle zu deaktivieren.

   b. Klicken Sie auf das Symbol **-**, um die Schnittstelle zu entfernen.



Basierend auf Ihrer Wahl, entfernt oder deaktiviert die Web-Konsole die Schnittstelle. Wenn Sie die Schnittstelle entfernen, ist sie in **Networking** als eigenständige Schnittstelle verfügbar.

9.6. ENTFERNEN ODER DEAKTIVIEREN EINES TEAMS ÜBER DIE WEB-KONSOLE

Entfernen oder deaktivieren Sie ein Netzwerkteam über die Webkonsole. Wenn Sie das Team nur deaktivieren, bleiben die Schnittstellen im Team, aber das Team wird nicht für den Netzwerkverkehr verwendet.

Voraussetzungen

- Auf dem Host ist ein Netzwerkteam konfiguriert.

Verfahren

1. Melden Sie sich an der Web-Konsole an.
   Details finden Sie unter Anmeldung an der Web-Konsole.

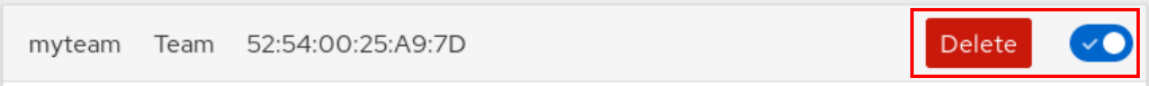
2. Wechseln Sie auf die Registerkarte **Networking**.

3. Klicken Sie auf das Team, das Sie entfernen oder deaktivieren möchten.

4. Entfernen oder deaktivieren Sie das ausgewählte Team.

   a. Sie können das Team entfernen, indem Sie auf die Schaltfläche **Löschen** klicken.

   b. Sie können das Team deaktivieren, indem Sie den **ON/OFF-Schalter** in eine deaktivierte Position bringen.



Schritte zur Verifizierung

- Wenn Sie das Team entfernt haben, gehen Sie zu **Networking** und überprüfen Sie, ob alle Schnittstellen aus Ihrem Team jetzt als eigenständige Schnittstellen aufgelistet sind.

KAPITEL 10. KONFIGURIEREN VON NETZWERKBRÜCKEN IN DER WEB-KONSOLE

Netzwerk-Bridges werden verwendet, um mehrere Schnittstellen mit dem gleichen Bereich von IP-Adressen an ein Subnetz anzuschließen.

Voraussetzungen

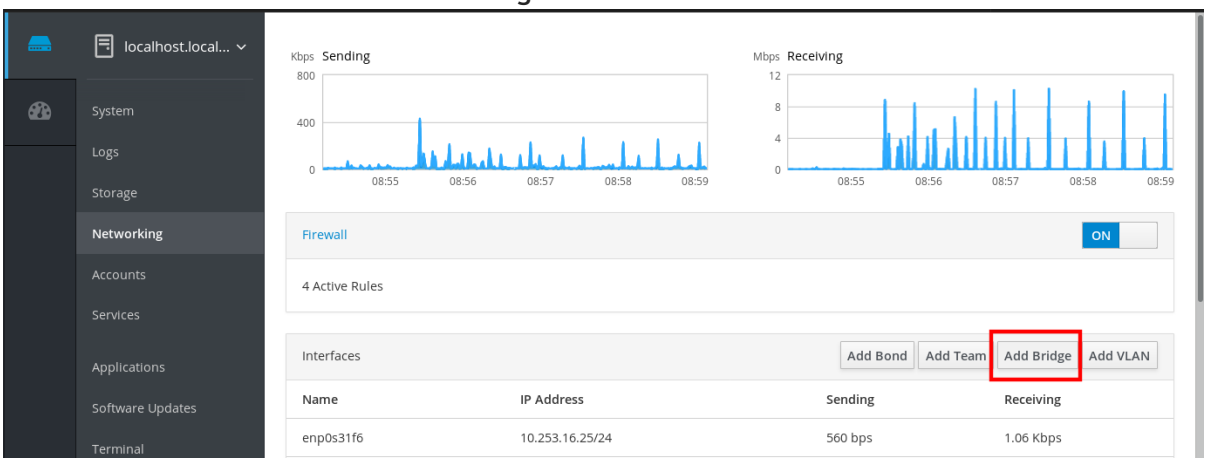
- Die RHEL 8 Web-Konsole ist installiert und aktiviert.
  Details finden Sie unter Installieren der Web-Konsole.

10.1. HINZUFÜGEN VON BRÜCKEN IN DER WEB-KONSOLE

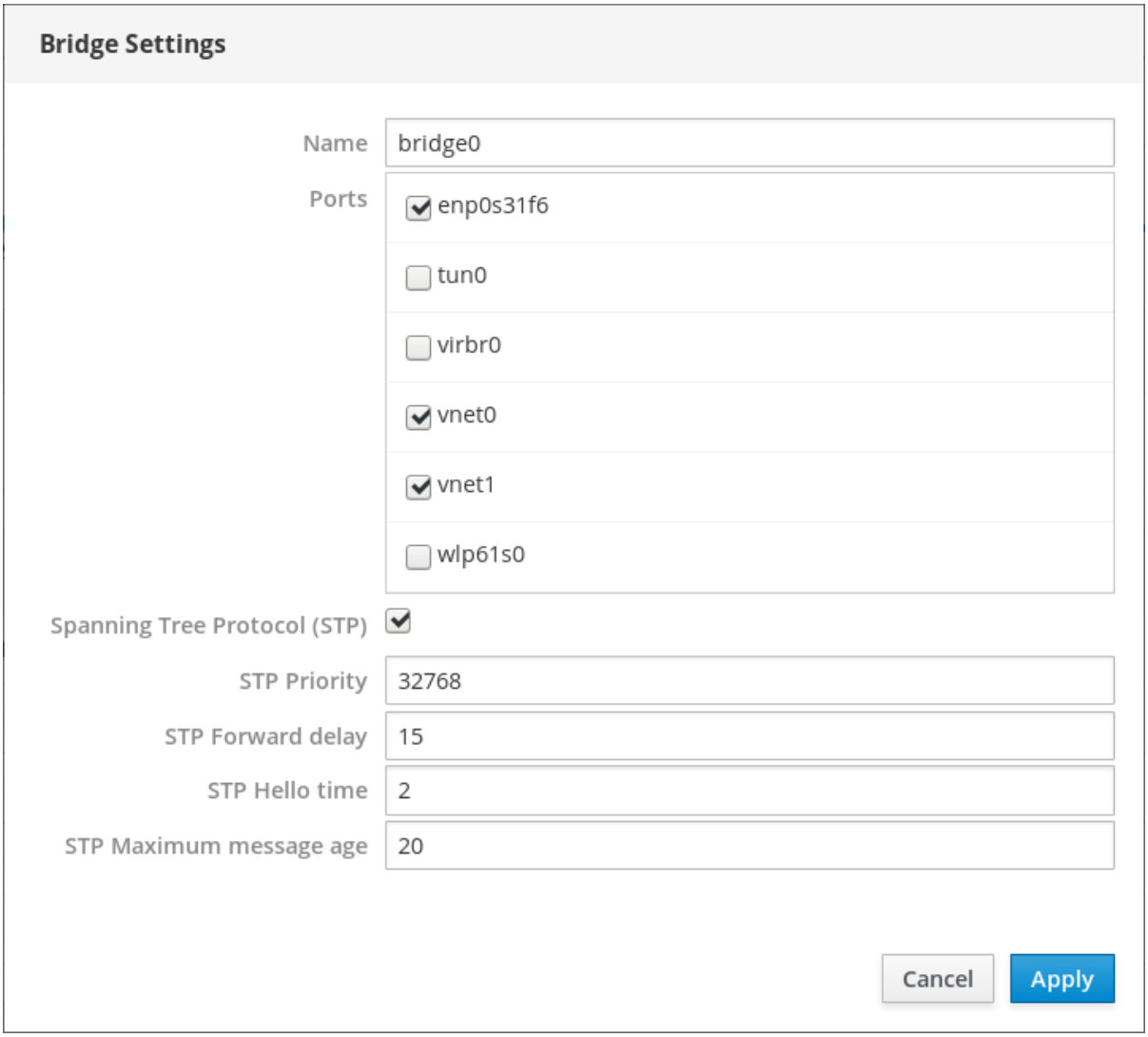
Erstellen Sie über die Web-Konsole eine Software-Bridge auf mehreren Netzwerkschnittstellen.

Verfahren

1. Melden Sie sich an der RHEL-Webkonsole an.
   Details finden Sie unter Anmeldung an der Web-Konsole.
2. Öffnen Sie **Networking**.
3. Klicken Sie auf die Schaltfläche **Add Bridge**.



4. Geben Sie im Dialogfeld **Bridge Settings** einen Namen für die neue Brücke ein.
5. Wählen Sie im Feld **Port** die Schnittstellen aus, die Sie in das eine Subnetz legen wollen.
6. Optional können Sie die **Spanning Tree protocol (STP)** auswählen, um Brückenschleifen und Rundfunkabstrahlung zu vermeiden.
   Wenn Sie keine starke Präferenz haben, lassen Sie die vordefinierten Werte so, wie sie sind.



7. Klicken Sie auf **Create**.

Wenn die Bridge erfolgreich erstellt wurde, zeigt die Web-Konsole die neue Bridge im Bereich **Networking** an. Überprüfen Sie die Werte in den Spalten **Sending** und **Receiving** in der Zeile der neuen Bridge.

Wenn Sie sehen können, dass null Bytes über die Bridge gesendet und empfangen werden, funktioniert die Verbindung nicht richtig und Sie müssen die Netzwerkeinstellungen anpassen.

10.2. KONFIGURIEREN EINER STATISCHEN IP-ADRESSE IN DER WEB-KONSOLE

Die IP-Adresse für Ihr System kann automatisch vom DHCP-Server aus dem Pool zugewiesen werden oder Sie können die IP-Adresse manuell konfigurieren. Die IP-Adresse wird nicht von den Einstellungen des DHCP-Servers beeinflusst.

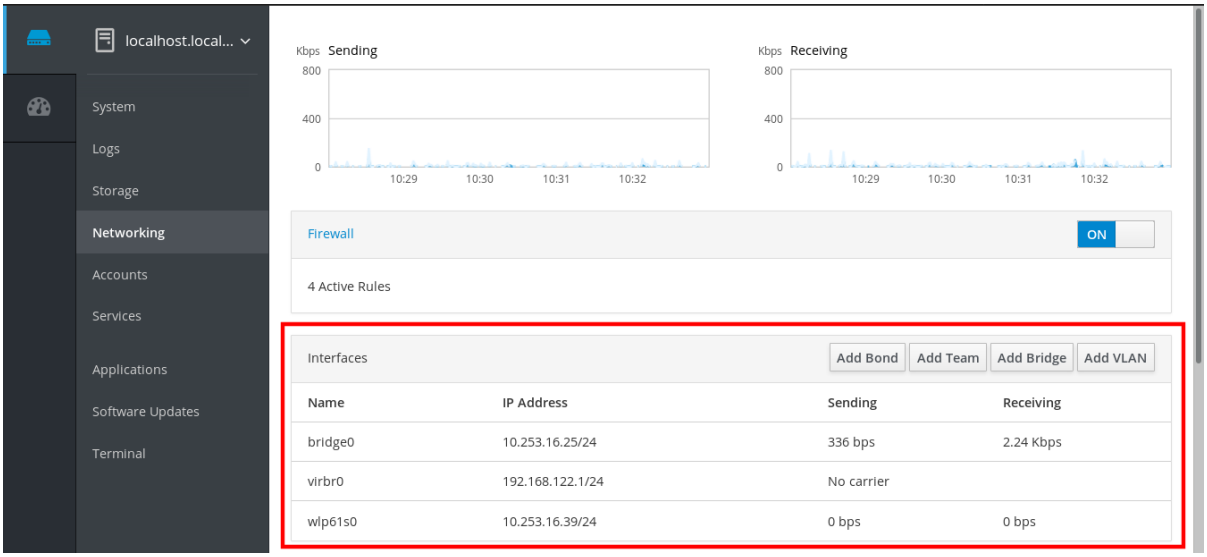
Erfahren Sie, wie Sie statische IPv4-Adressen einer Netzwerk-Bridge über die RHEL-Webkonsole konfigurieren.

Verfahren

1. Melden Sie sich an der RHEL-Webkonsole an.
   Details finden Sie unter Anmeldung an der Web-Konsole.

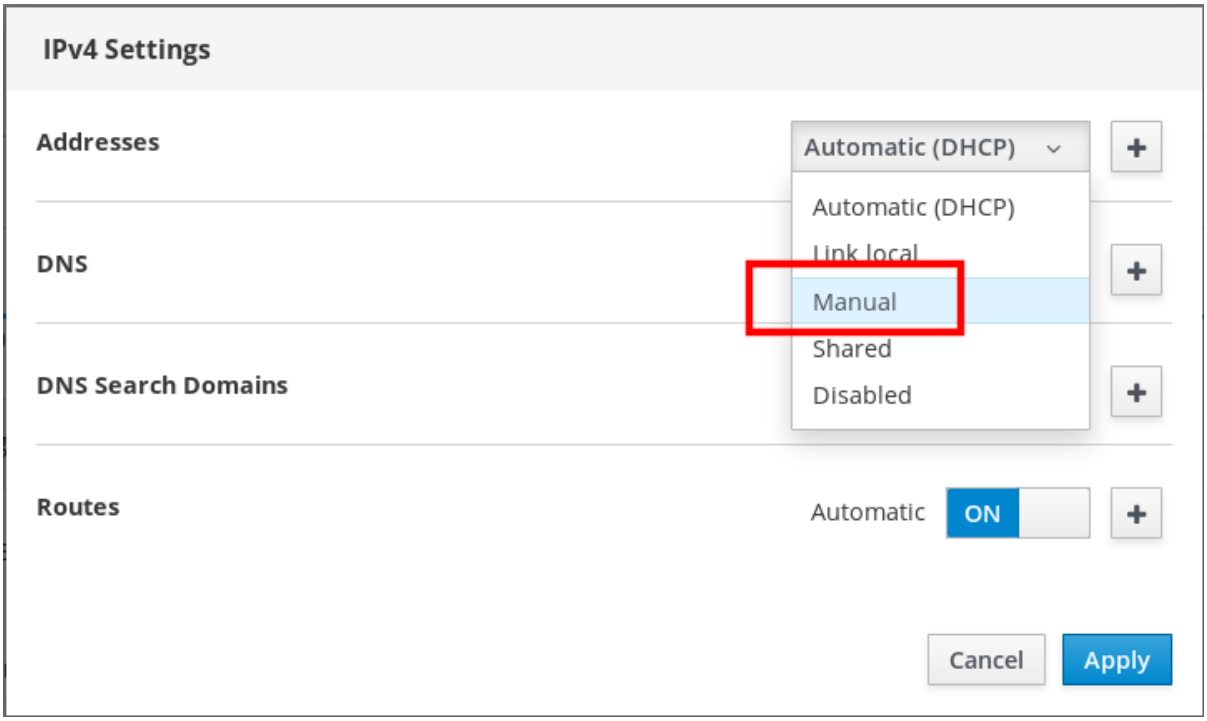
2. Öffnen Sie den Bereich **Networking**.

3. Klicken Sie auf die Schnittstelle, an der Sie die statische IP-Adresse einstellen möchten.

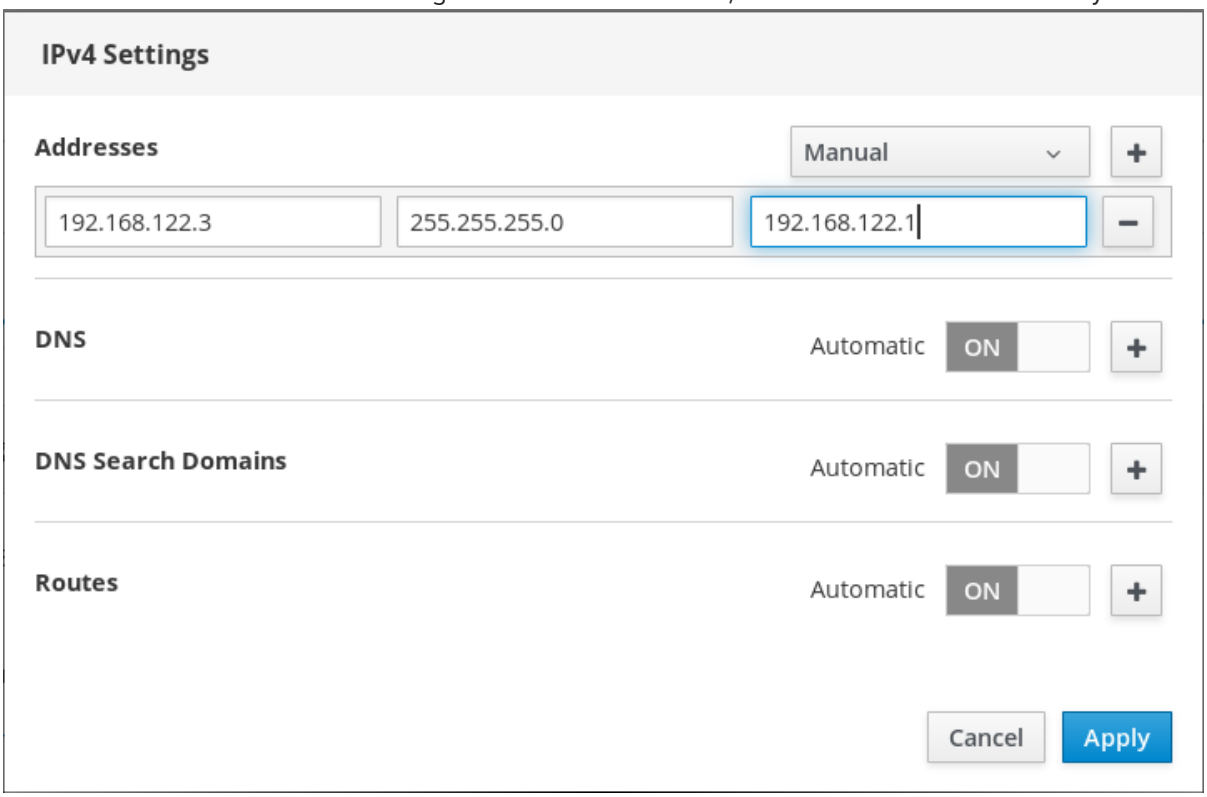


4. Klicken Sie im Bildschirm mit den Schnittstellendetails auf die Konfiguration **IPv4**.

5. Wählen Sie im Dialogfeld **IPv4 Settings** die Option **Manual** in der Dropdown-Liste **Addresses**.



6. Klicken Sie auf **Apply**.
7. Geben Sie im Feld **Addresses** die gewünschte IP-Adresse, Netzmaske und das Gateway ein.



8. Klicken Sie auf **Apply**.

Zu diesem Zeitpunkt ist die IP-Adresse konfiguriert und die Schnittstelle verwendet die neue statische IP-Adresse.

10.3. ENTFERNEN VON SCHNITTSTELLEN AUS DER BRIDGE ÜBER DIE WEB-KONSOLE

Netzwerk-Bridges können mehrere Schnittstellen enthalten. Sie können diese aus der Bridge entfernen. Jede entfernte Schnittstelle wird automatisch in die eigenständige Schnittstelle geändert.

Erfahren Sie, wie Sie eine Netzwerkschnittstelle aus einer im RHEL 8-System erstellten Software-Bridge entfernen.

Voraussetzungen

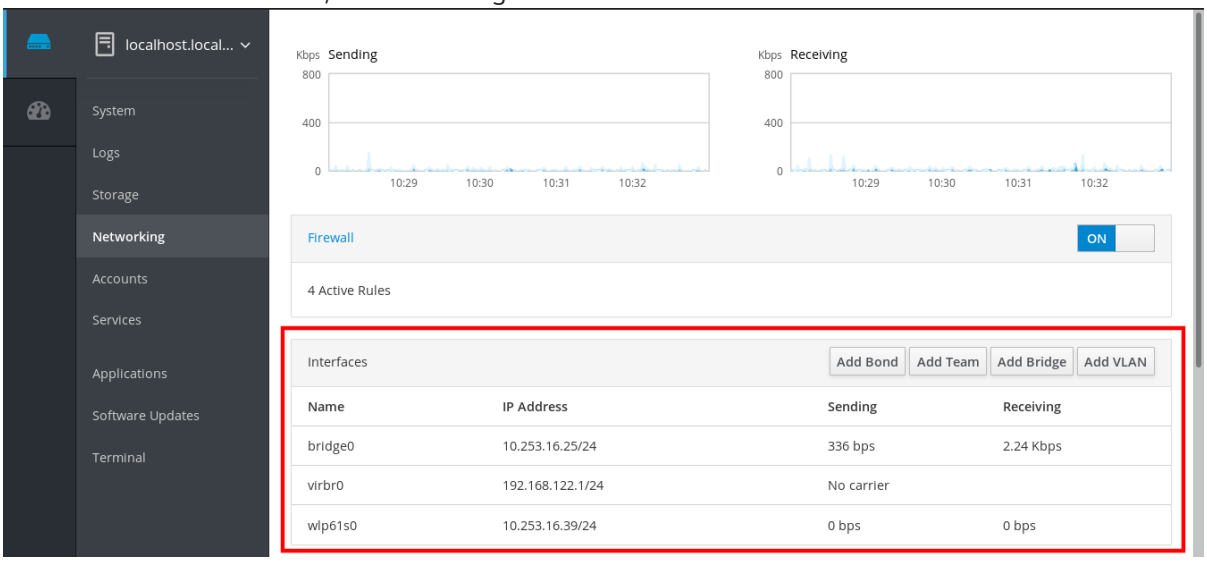
- Eine Bridge mit mehreren Schnittstellen in Ihrem System zu haben.

Verfahren

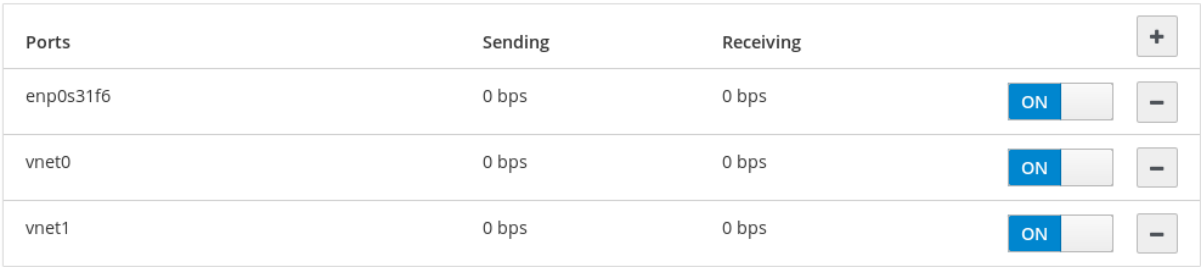
1. Melden Sie sich an der RHEL-Webkonsole an.
   Details finden Sie unter Anmeldung an der Web-Konsole.

2. Öffnen Sie **Networking**.

3. Klicken Sie auf die Brücke, die Sie konfigurieren möchten.



4. Blättern Sie im Bildschirm mit den Bridge-Einstellungen nach unten zur Tabelle der Ports (Schnittstellen).



5. Wählen Sie die Schnittstelle und klicken Sie auf das Symbol **-**.

Die RHEL 8-Webkonsole entfernt die Schnittstelle aus der Bridge und Sie können sie wieder im Bereich **Networking** als eigenständige Schnittstelle sehen.

10.4. LÖSCHEN VON BRÜCKEN IN DER WEB-KONSOLE

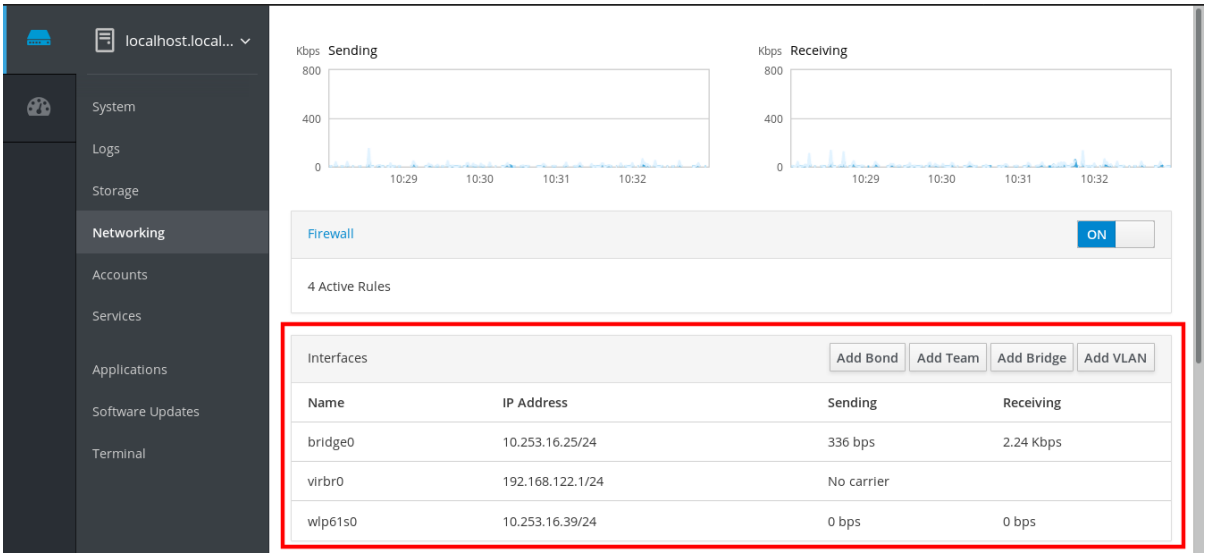
Sie können eine Software-Netzwerk-Bridge in der RHEL-Webkonsole löschen. Alle Netzwerkschnittstellen, die in der Bridge enthalten sind, werden automatisch zu eigenständigen Schnittstellen geändert.

Voraussetzungen

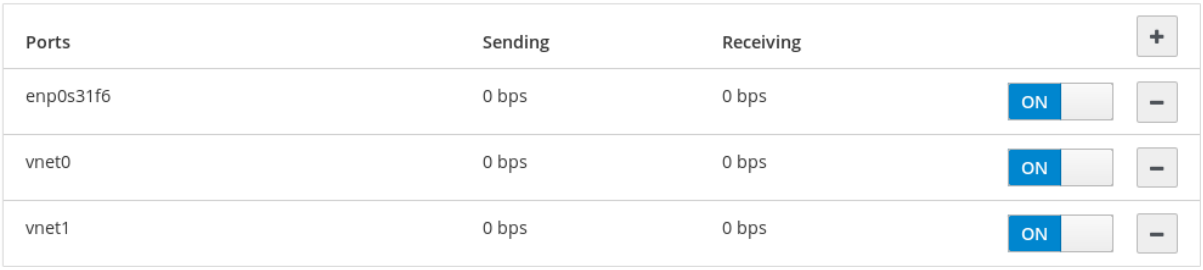
- Sie haben eine Brücke in Ihrem System.

Verfahren

1. Melden Sie sich an der RHEL-Webkonsole an.
   Details finden Sie unter Anmeldung an der Web-Konsole.
2. Öffnen Sie den Bereich **Networking**.
3. Klicken Sie auf die Brücke, die Sie konfigurieren möchten.

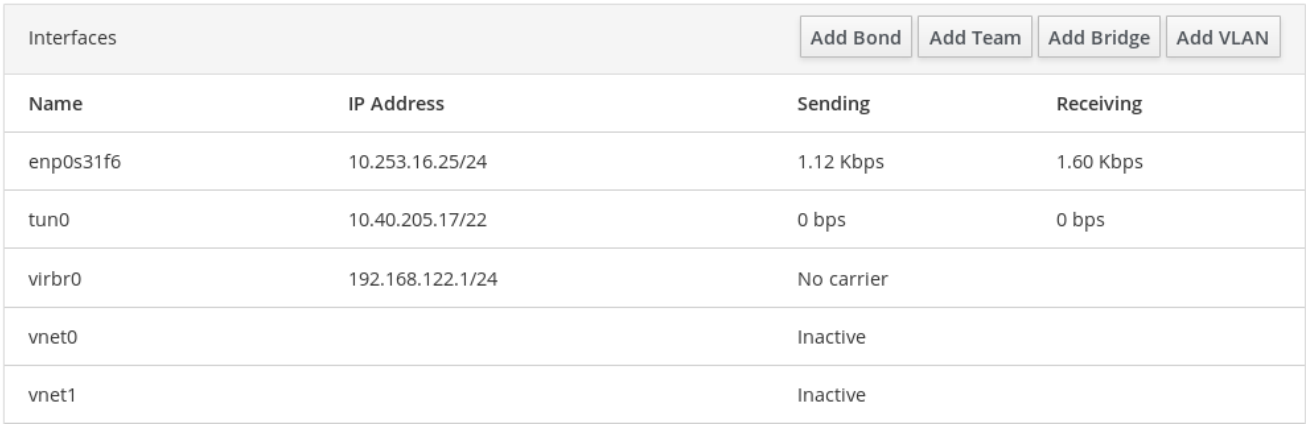


4. Blättern Sie im Bildschirm mit den Bridge-Einstellungen nach unten zur Tabelle der Ports.



5. Klicken Sie auf **Delete**.

Gehen Sie in diesem Stadium zurück zu **Networking** und überprüfen Sie, ob alle Netzwerkschnittstellen auf der Registerkarte **Interfaces** angezeigt werden. Schnittstellen, die Teil der Bridge waren, können jetzt inaktiv sein. Daher müssen Sie sie eventuell aktivieren und die Netzwerkparameter manuell einstellen.



KAPITEL 11. KONFIGURIEREN VON VLANS IN DER WEB-KONSOLE

VLANs (Virtual LANs) sind virtuelle Netzwerke, die auf einer einzelnen physikalischen Ethernet-Schnittstelle erstellt werden. Jedes VLAN wird durch eine ID definiert, die eine eindeutige positive Ganzzahl darstellt und als eigenständige Schnittstelle arbeitet.

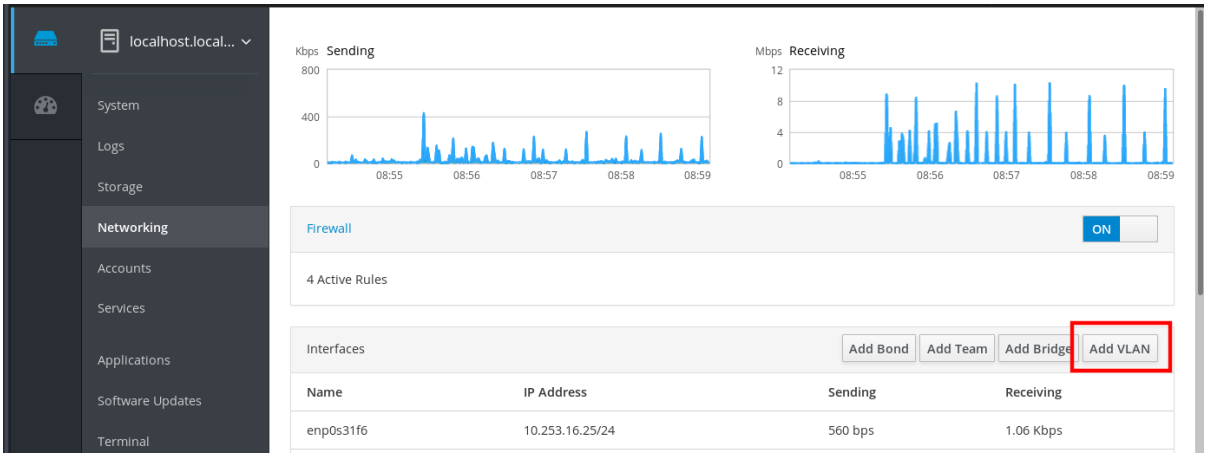
Erfahren Sie, wie Sie VLANs in der RHEL-Webkonsole erstellen.

Voraussetzungen

- Die RHEL 8 Web-Konsole ist installiert und aktiviert.
  Details finden Sie unter Installieren der Web-Konsole.
- Sie haben eine Netzwerkschnittstelle in Ihrem System.

Verfahren

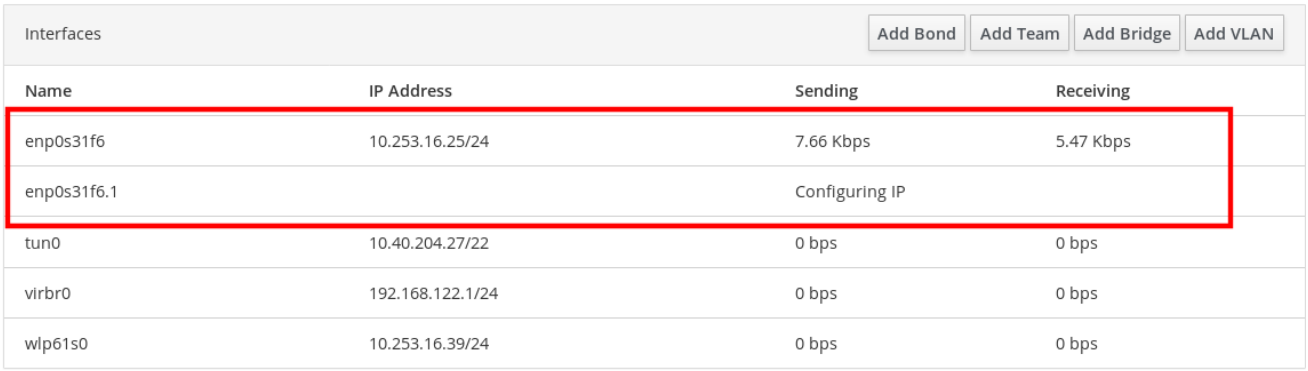
1. Melden Sie sich an der RHEL-Webkonsole an.
   Details finden Sie unter Anmeldung an der Web-Konsole.
2. Öffnen Sie **Networking**.
3. Klicken Sie auf die Schaltfläche **Add VLAN**.



4. Wählen Sie im Dialogfeld **VLAN Settings** die physikalische Schnittstelle aus, für die Sie ein VLAN erstellen möchten.
5. Geben Sie die VLAN-ID ein oder verwenden Sie einfach die vordefinierte Nummer.
6. Im Feld **Name** sehen Sie einen vordefinierten Namen, der aus der übergeordneten Schnittstelle und der VLAN-ID besteht. Wenn es nicht notwendig ist, lassen Sie den Namen so, wie er ist.

7. Klicken Sie auf **Apply**.

Das neue VLAN wurde erstellt und Sie müssen auf das VLAN klicken und die Netzwerkeinstellungen konfigurieren.



KAPITEL 12. KONFIGURIEREN DES ABHÖRPORTS DER WEB-KONSOLE

Erfahren Sie, wie Sie mit der RHEL-Webkonsole neue Ports zulassen oder die vorhandenen Ports ändern können.

Voraussetzungen

- Die RHEL 8 Web-Konsole ist installiert und aktiviert.
  Details finden Sie unter Installieren der Web-Konsole.

12.1. ZULASSEN EINES NEUEN PORTS AUF EINEM SYSTEM MIT AKTIVEM SELINUX

Aktivieren Sie die Web-Konsole, um auf einem ausgewählten Port zu lauschen.

Voraussetzungen

- Die Web-Konsole muss installiert und zugänglich sein. Details finden Sie unter Installieren der Web-Konsole.

Verfahren

- Für Ports, die nicht durch einen anderen Teil von SELinux definiert sind, führen Sie aus:

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

- Für Ports, die bereits durch einen anderen Teil von SELinux definiert sind, führen Sie aus:

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

Die Änderungen sollten sofort wirksam werden.

12.2. ERLAUBEN EINES NEUEN PORTS AUF EINEM SYSTEM MIT FIREWALLD

Aktivieren Sie die Web-Konsole, um Verbindungen auf einem neuen Port zu empfangen.

Voraussetzungen

- Die Web-Konsole muss installiert und zugänglich sein. Details finden Sie unter Installieren der Web-Konsole.
- Der Dienst **firewalld** muss ausgeführt werden.

Verfahren

1. Um eine neue Portnummer hinzuzufügen, führen Sie den folgenden Befehl aus:

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

2. Um die alte Portnummer aus dem Dienst **cockpit** zu entfernen, führen Sie aus:

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

WICHTIG

Wenn Sie nur die **firewall-cmd --service cockpit --add-port=PORT_NUMBER/tcp** ohne die Option **--permanent** ausführen, wird Ihre Änderung mit dem nächsten Neuladen von **firewalld** oder einem Systemneustart rückgängig gemacht.

12.3. ÄNDERN DES PORTS DER WEB-KONSOLE

Ändern Sie das Standard-Übertragungssteuerungsprotokoll (TCP) auf Port **9090** in ein anderes.

Voraussetzungen

- Die Web-Konsole muss installiert und zugänglich sein. Details finden Sie unter Installieren der Web-Konsole.
- Wenn Sie Ihr System mit SELinux schützen, müssen Sie es so einstellen, dass Cockpit auf einem neuen Port lauschen darf. Weitere Informationen finden Sie unter Zulassen eines neuen Ports auf einem System mit aktivem SELinux.
- Wenn Sie **firewalld** als Firewall konfiguriert haben, müssen Sie diese so einstellen, dass Cockpit Verbindungen auf einem neuen Port empfangen kann. Weitere Informationen finden Sie unter Zulassen eines neuen Ports auf einem System mit **firewalld**.

Verfahren

1. Ändern Sie den Listening-Port mit einer der folgenden Methoden:
   a. Verwenden Sie den Befehl **systemctl edit cockpit.socket**:
      i. Führen Sie den folgenden Befehl aus:

```
$ sudo systemctl edit cockpit.socket
```

      Dadurch wird die Datei **/etc/systemd/system/cockpit.socket.d/override.conf** geöffnet.

      ii. Ändern Sie den Inhalt von **override.conf** oder fügen Sie einen neuen Inhalt in folgendem Format hinzu:

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

   b. Alternativ fügen Sie den oben genannten Inhalt in die Datei **/etc/systemd/system/cockpit.socket.d/listen.conf** ein.
   Erstellen Sie das Verzeichnis **cockpit.socket.d.** und die Datei **listen.conf**, wenn sie noch nicht existieren.

2. Führen Sie die folgenden Befehle aus, damit die Änderungen wirksam werden:

```
$ sudo systemctl daemon-reload
$ sudo systemctl restart cockpit.socket
```

Wenn Sie im vorherigen Schritt **systemctl edit cockpit.socket** verwendet haben, ist die Ausführung von **systemctl daemon-reload** nicht erforderlich.

Schritte zur Verifizierung

- Um zu überprüfen, ob die Änderung erfolgreich war, versuchen Sie, eine Verbindung zur Web-Konsole mit dem neuen Port herzustellen.

KAPITEL 13. VERWALTEN DER FIREWALL ÜBER DIE WEB-KONSOLE

Eine Firewall ist eine Möglichkeit, Rechner vor unerwünschtem Datenverkehr von außen zu schützen. Sie ermöglicht es Benutzern, den eingehenden Netzwerkverkehr auf Host-Rechnern zu kontrollieren, indem sie einen Satz von Firewall-Regeln definieren. Diese Regeln werden verwendet, um den eingehenden Datenverkehr zu sortieren und ihn entweder zu blockieren oder durchzulassen.

Voraussetzungen

- Die RHEL 8 Web-Konsole konfiguriert den Dienst **firewalld**.
  Einzelheiten über den Dienst **firewalld** finden Sie unter Erste Schritte mit firewalld.

13.1. AUSFÜHREN DER FIREWALL ÜBER DIE WEB-KONSOLE

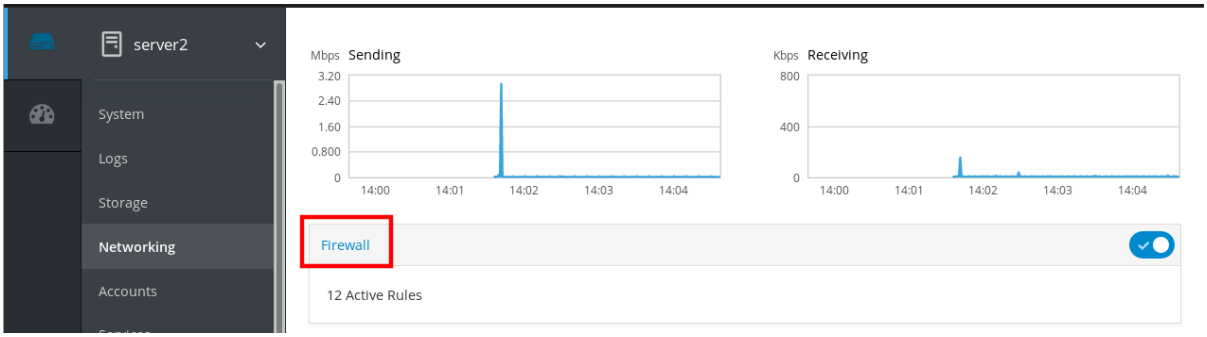
Dieser Abschnitt beschreibt, wo und wie Sie die RHEL 8-Systemfirewall in der Web-Konsole ausführen.

ANMERKUNG

Die RHEL 8 Web-Konsole konfiguriert den Dienst **firewalld**.

Verfahren

1. Melden Sie sich an der RHEL 8 Web-Konsole an.
   Details finden Sie unter Anmeldung an der Web-Konsole.
2. Öffnen Sie den Bereich **Networking**.
3. Klicken Sie im Bereich **Firewall** auf **ON**, um die Firewall auszuführen.



   Wenn Sie das Feld **Firewall** nicht sehen, melden Sie sich an der Webkonsole mit den Administrationsrechten an.

In diesem Stadium ist Ihre Firewall in Betrieb.

Um Firewall-Regeln zu konfigurieren, siehe Abschnitt 13.7, »Aktivieren von Diensten auf der Firewall über die Web-Konsole«.

13.2. ANHALTEN DER FIREWALL ÜBER DIE WEB-KONSOLE

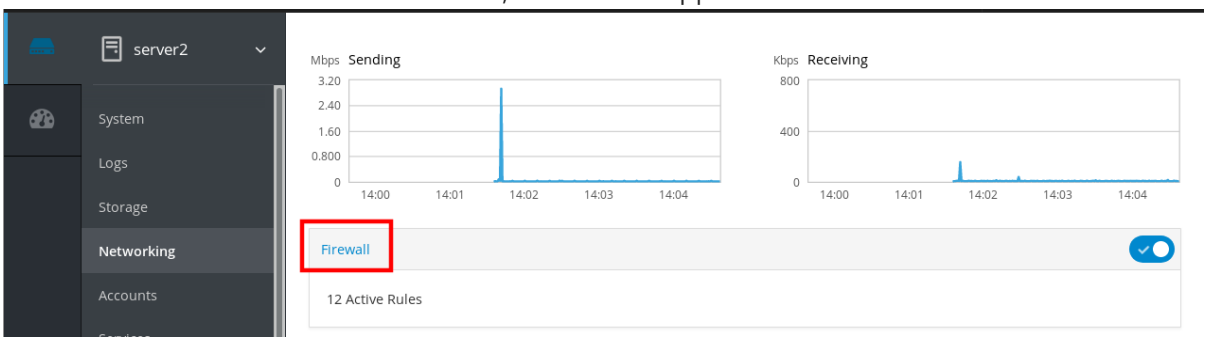
Dieser Abschnitt beschreibt, wo und wie Sie die RHEL 8-Systemfirewall in der Web-Konsole anhalten können.

ANMERKUNG

Die RHEL 8 Web-Konsole konfiguriert den Dienst **firewalld**.

Verfahren

1. Melden Sie sich an der RHEL 8 Web-Konsole an.
   Details finden Sie unter Anmeldung an der Web-Konsole.
2. Öffnen Sie den Bereich **Networking**.
3. Klicken Sie im Bereich **Firewall** auf **OFF**, um ihn zu stoppen.



   Wenn Sie das Feld **Firewall** nicht sehen, melden Sie sich an der Webkonsole mit den Administrationsrechten an.

In diesem Stadium ist die Firewall gestoppt und sichert Ihr System nicht.

13.3. FIREWALLD

firewalld ist ein Firewall-Dienst-Daemon, der eine dynamische, anpassbare Host-basierte Firewall mit einer **D-Bus** Oberfläche bietet. Da er dynamisch ist, ermöglicht er das Erstellen, Ändern und Löschen der Regeln, ohne dass der Firewall-Daemon jedes Mal neu gestartet werden muss, wenn die Regeln geändert werden.

firewalld verwendet die Konzepte von *zones* und *services*, die die Verkehrsverwaltung vereinfachen. Zonen sind vordefinierte Sätze von Regeln. Netzwerkschnittstellen und Quellen können einer Zone zugewiesen werden. Der erlaubte Datenverkehr hängt von dem Netzwerk ab, mit dem Ihr Computer verbunden ist, und von der Sicherheitsstufe, die diesem Netzwerk zugewiesen ist. Firewall-Dienste sind vordefinierte Regeln, die alle notwendigen Einstellungen umfassen, um eingehenden Datenverkehr für einen bestimmten Dienst zuzulassen, und sie gelten innerhalb einer Zone.

Dienste verwenden einen oder mehrere *ports* oder *addresses* für die Netzwerkkommunikation. Firewalls filtern die Kommunikation auf der Basis von Ports. Um den Netzwerkverkehr für einen Dienst zuzulassen, müssen seine Ports *open* sein. **firewalld** blockiert den gesamten Verkehr auf Ports, die nicht explizit als offen eingestellt sind. Einige Zonen, wie z. B. *trusted*, erlauben standardmäßig den gesamten Datenverkehr.

Zusätzliche Ressourcen

- **firewalld(1)** man-Seite

13.4. ZONEN

firewalld kann verwendet werden, um Netzwerke in verschiedene Zonen zu unterteilen, je nach dem Grad des Vertrauens, den der Benutzer für die Schnittstellen und den Datenverkehr innerhalb dieses

Netzwerks festgelegt hat. Eine Verbindung kann nur Teil einer Zone sein, aber eine Zone kann für viele Netzwerkverbindungen verwendet werden.

NetworkManager benachrichtigt **firewalld** über die Zone einer Schnittstelle. Sie können den Schnittstellen Zonen zuweisen mit:

- **NetworkManager**
- **firewall-config** tool
- **firewall-cmd** Befehlszeilen-Tool
- Die RHEL Web-Konsole

Die letzteren drei können nur die entsprechenden **NetworkManager** Konfigurationsdateien bearbeiten. Wenn Sie die Zone der Schnittstelle über die Webkonsole, **firewall-cmd** oder **firewall-config** ändern, wird die Anfrage an **NetworkManager** weitergeleitet und nicht von **firewalld** bearbeitet.

Die vordefinierten Zonen werden im Verzeichnis /**usr**/**lib**/**firewalld**/**zones**/ gespeichert und können sofort auf jede verfügbare Netzwerkschnittstelle angewendet werden. Diese Dateien werden nur dann in das Verzeichnis /**etc**/**firewalld**/**zones**/ kopiert, wenn sie geändert werden. Die Standardeinstellungen der vordefinierten Zonen sind wie folgt:

block

Alle eingehenden Netzwerkverbindungen werden mit einer icmp-host-prohibited-Meldung für **IPv4** und icmp6-adm-prohibited für **IPv6** zurückgewiesen. Es sind nur Netzwerkverbindungen möglich, die von innerhalb des Systems initiiert werden.

dmz

Für Computer in Ihrer demilitarisierten Zone, die öffentlich zugänglich sind und nur begrenzten Zugriff auf Ihr internes Netzwerk haben. Es werden nur ausgewählte eingehende Verbindungen akzeptiert.

drop

Alle eingehenden Netzwerkpakete werden ohne Benachrichtigung verworfen. Nur ausgehende Netzwerkverbindungen sind möglich.

external

Zur Verwendung in externen Netzwerken mit aktiviertem Masquerading, insbesondere für Router. Sie vertrauen den anderen Computern im Netzwerk nicht, dass sie Ihren Computer nicht beschädigen. Es werden nur ausgewählte eingehende Verbindungen akzeptiert.

home

Für die Verwendung zu Hause, wenn Sie den anderen Computern im Netzwerk weitgehend vertrauen. Es werden nur ausgewählte eingehende Verbindungen akzeptiert.

internal

Zur Verwendung in internen Netzwerken, wenn Sie den anderen Computern im Netzwerk weitgehend vertrauen. Es werden nur ausgewählte eingehende Verbindungen akzeptiert.

public

Zur Verwendung in öffentlichen Bereichen, in denen Sie anderen Computern im Netzwerk nicht vertrauen. Es werden nur ausgewählte eingehende Verbindungen akzeptiert.

trusted

Alle Netzwerkverbindungen werden akzeptiert.

work

Für die Verwendung am Arbeitsplatz, wo Sie den anderen Computern im Netzwerk meist vertrauen. Nur ausgewählte eingehende Verbindungen werden akzeptiert.

Eine dieser Zonen wird als Zone *default* festgelegt. Wenn Schnittstellenverbindungen zu **NetworkManager** hinzugefügt werden, werden sie der Standardzone zugewiesen. Bei der Installation ist die Standardzone in **firewalld** auf die Zone **public** eingestellt. Die Standardzone kann geändert werden.

ANMERKUNG

Die Netzwerkzonennamen sollten selbsterklärend sein und dem Benutzer eine schnelle, sinnvolle Entscheidung ermöglichen. Um Sicherheitsprobleme zu vermeiden, überprüfen Sie die Standardzonenkonfiguration und deaktivieren Sie alle unnötigen Dienste entsprechend Ihren Bedürfnissen und Risikobewertungen.

Zusätzliche Ressourcen

- **firewalld.zone(5)** man-Seite

13.5. ZONEN IN DER WEB-KONSOLE

WICHTIG

Firewall-Zonen sind neu in der RHEL 8.1.0 Beta.

Die Red Hat Enterprise Linux Web-Konsole implementiert wichtige Funktionen des Firewalld-Dienstes und ermöglicht es Ihnen,:

- Hinzufügen vordefinierter Firewall-Zonen zu einer bestimmten Schnittstelle oder einem Bereich von IP-Adressen
- Konfigurieren Sie Zonen mit der Auswahl von Diensten in der Liste der aktivierten Dienste
- Deaktivieren Sie einen Dienst, indem Sie diesen Dienst aus der Liste der aktivierten Dienste entfernen
- Entfernen einer Zone von einer Schnittstelle

13.6. AKTIVIEREN VON ZONEN ÜBER DIE WEB-KONSOLE

Die Web-Konsole ermöglicht es Ihnen, vordefinierte und vorhandene Firewall-Zonen auf eine bestimmte Schnittstelle oder einen Bereich von IP-Adressen anzuwenden. Dieser Abschnitt beschreibt, wie Sie eine Zone auf einer Schnittstelle aktivieren.

Voraussetzungen

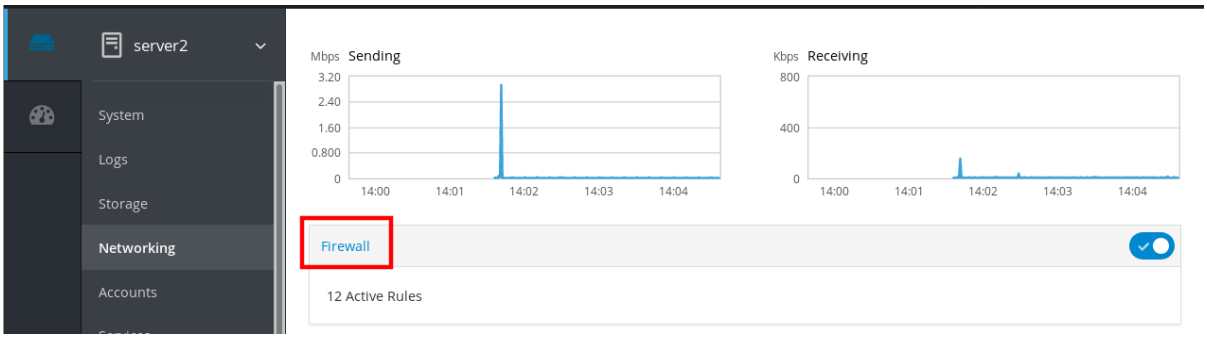
- Die RHEL 8 Web-Konsole wurde installiert.
  Details finden Sie unter Installieren der Web-Konsole.
- Die Firewall muss aktiviert sein.
  Für Details siehe Abschnitt 13.1, »Ausführen der Firewall über die Web-Konsole«.

Verfahren

1. Melden Sie sich an der RHEL-Webkonsole mit Administrationsrechten an.
   Details finden Sie unter Anmeldung an der Web-Konsole.

2. Klicken Sie auf **Networking**.

3. Klicken Sie auf den Titel der Box **Firewall**.



   Wenn Sie das Feld **Firewall** nicht sehen, melden Sie sich an der Webkonsole mit den Administratorrechten an.

4. Klicken Sie im Bereich **Firewall** auf **Add Services**.

5. Klicken Sie auf die Schaltfläche **Add Zone**.

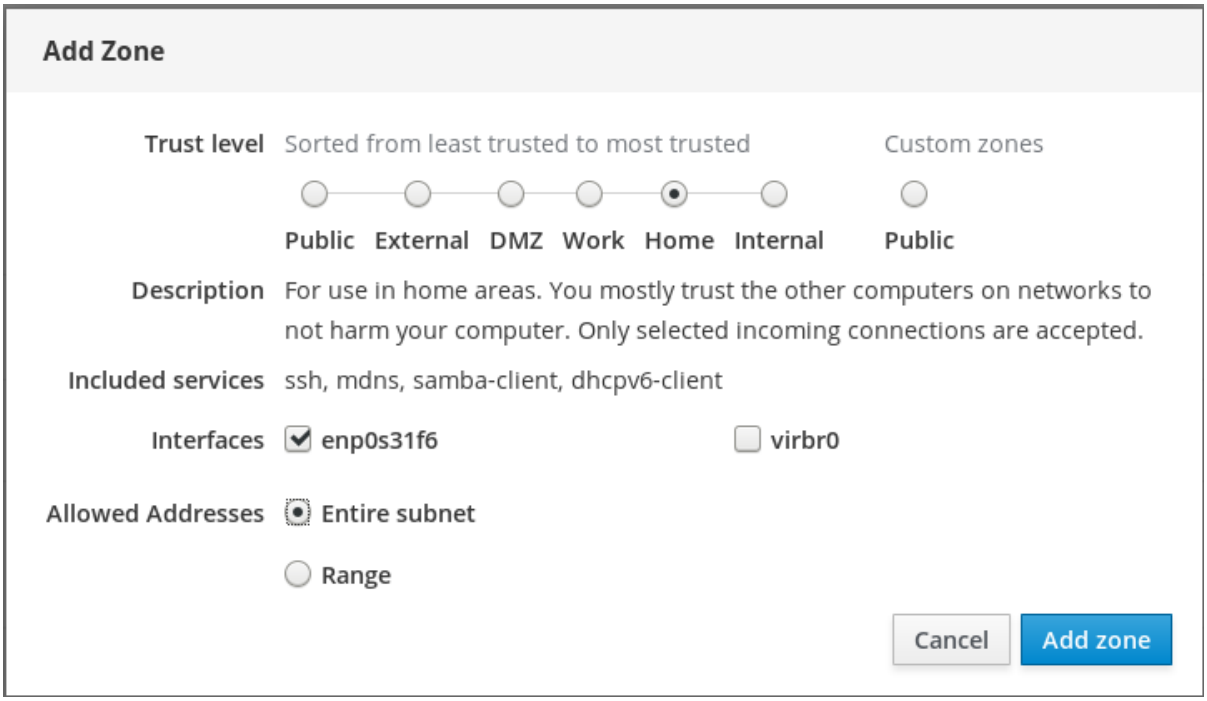
6. Wählen Sie im Dialogfeld **Add Zone** eine Zone aus der Skala **Trust level** aus.
   Sie können hier alle im Dienst **firewalld** vordefinierten Zonen sehen.

7. Wählen Sie im Teil **Interfaces** eine oder mehrere Schnittstellen, auf die die ausgewählte Zone angewendet wird.

8. Im Teil **Allowed Addresses** können Sie wählen, ob die Zone eingeschaltet werden soll:

   - das gesamte Subnetz
   - oder einen Bereich von IP-Adressen im folgenden Format:
     - 192.168.1.0
     - 192.168.1.0/24
     - 192.168.1.0/24, 192.168.1.0

9. Klicken Sie auf die Schaltfläche **Add zone**.

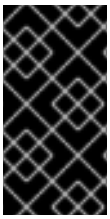


Überprüfen Sie die Konfiguration in **Active zones**.

13.7. AKTIVIEREN VON DIENSTEN AUF DER FIREWALL ÜBER DIE WEB-KONSOLE

Standardmäßig werden Dienste der Standard-Firewall-Zone hinzugefügt. Wenn Sie weitere Firewall-Zonen auf weiteren Netzwerkschnittstellen verwenden, müssen Sie zuerst eine Zone auswählen und dann den Dienst mit Port hinzufügen.

Die RHEL 8 Web-Konsole zeigt vordefinierte **firewalld** Dienste an und Sie können diese zu aktiven Firewall-Zonen hinzufügen.



WICHTIG

Die RHEL 8 Web-Konsole konfiguriert den Dienst **firewalld**.

Die Web-Konsole erlaubt keine generischen **firewalld** Regeln, die nicht in der Web-Konsole aufgeführt sind.

Voraussetzungen

- Die RHEL 8 Web-Konsole wurde installiert.
  Details finden Sie unter Installieren der Web-Konsole.

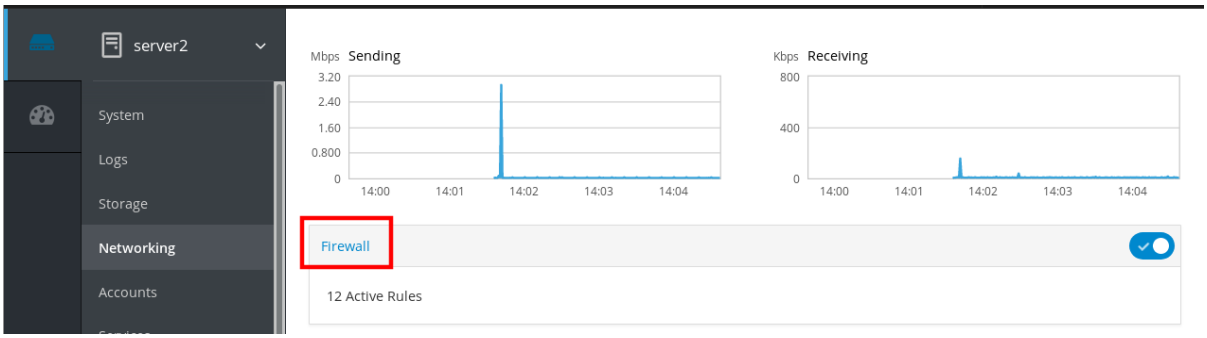
- Die Firewall muss aktiviert sein.
  Für Details siehe Abschnitt 13.1, »Ausführen der Firewall über die Web-Konsole«.

Verfahren

1. Melden Sie sich an der RHEL-Webkonsole mit Administratorrechten an.
   Details finden Sie unter Anmeldung an der Web-Konsole.

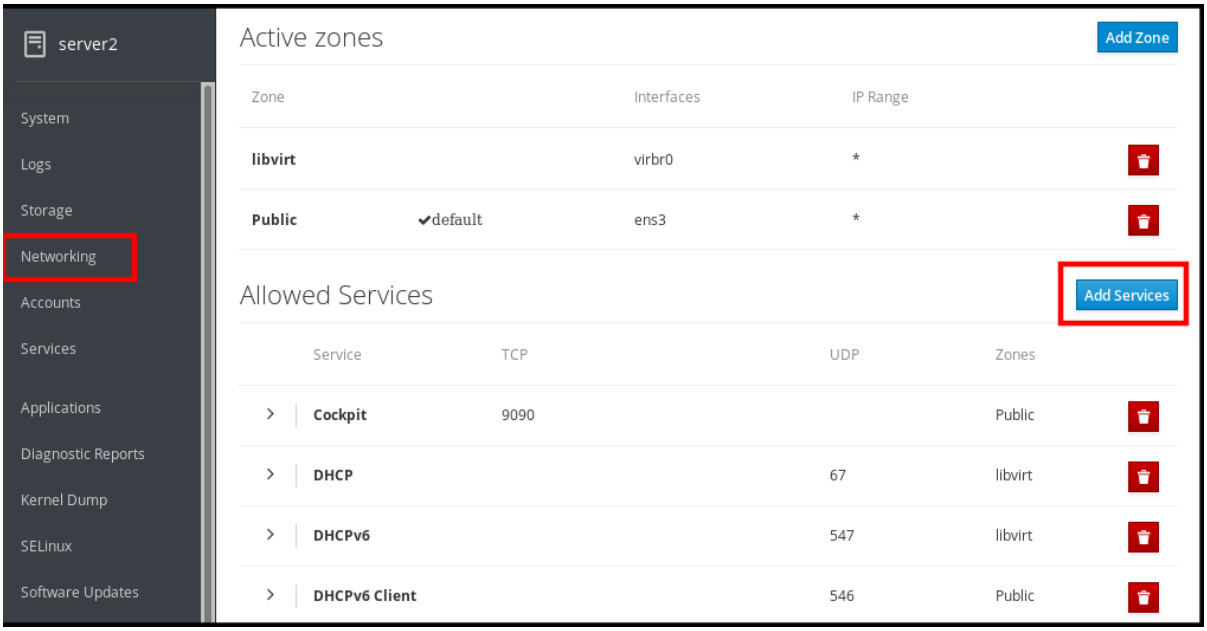
2. Klicken Sie auf **Networking**.

3. Klicken Sie auf den Titel der Box **Firewall**.



   Wenn Sie das Feld **Firewall** nicht sehen, melden Sie sich an der Webkonsole mit den Administratorrechten an.

4. Klicken Sie im Bereich **Firewall** auf **Add Services**.

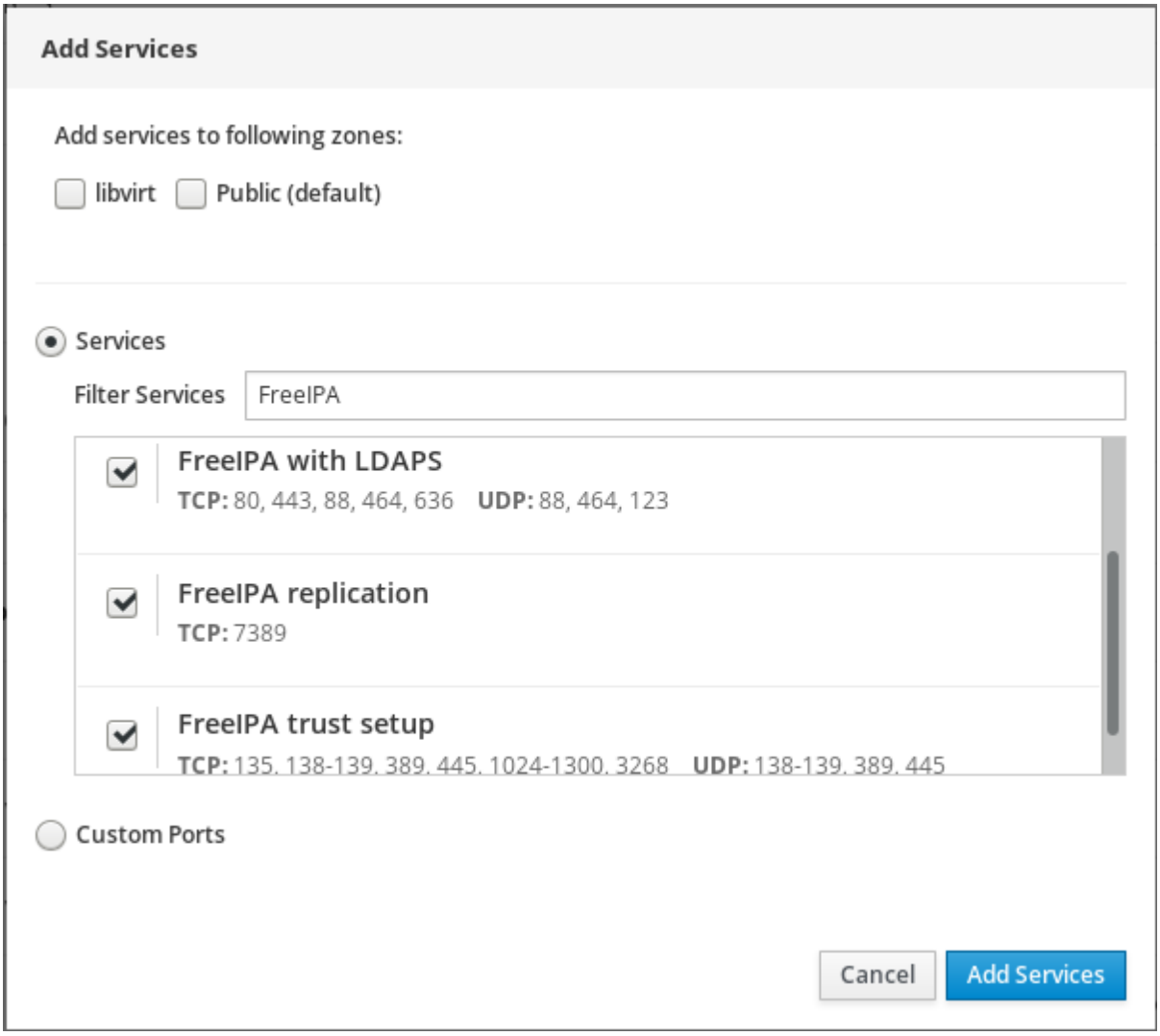


5. Wählen Sie im Dialogfeld **Add Services** eine Zone aus, für die Sie den Dienst hinzufügen möchten.
   Das Dialogfeld **Add Services** enthält nur dann eine Liste der aktiven Firewall-Zonen, wenn das System mehrere aktive Zonen enthält.

   Wenn das System nur eine (die Standard-)Zone verwendet, enthält der Dialog keine Zoneneinstellungen.

6. Suchen Sie im Dialogfeld **Add Services** den Dienst, den Sie auf der Firewall aktivieren möchten.

7. Aktivieren Sie die gewünschten Dienste.



8. Klicken Sie auf **Add Services**.

An diesem Punkt zeigt die RHEL 8 Web-Konsole den Dienst in der Liste von **Allowed Services** an.

13.8. KONFIGURIEREN VON BENUTZERDEFINIERTEN PORTS ÜBER DIE WEB-KONSOLE

In der Web-Konsole können Sie hinzufügen:

- Dienste, die auf Standard-Ports hören Abschnitt 13.7, »Aktivieren von Diensten auf der Firewall über die Web-Konsole«
- Dienste, die auf benutzerdefinierten Ports lauschen.

Dieser Abschnitt beschreibt, wie Sie Dienste mit konfigurierten benutzerdefinierten Ports hinzufügen.

Voraussetzungen

- Die RHEL 8 Web-Konsole wurde installiert.
  Details finden Sie unter Installieren der Web-Konsole.
- Die Firewall muss aktiviert sein.
  Für Details siehe Abschnitt 13.1, »Ausführen der Firewall über die Web-Konsole«.

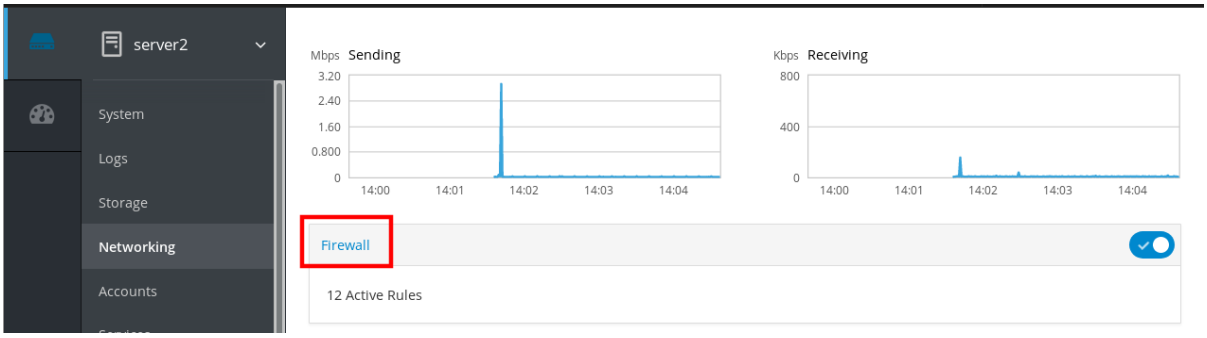
Verfahren

Verfahren

1. Melden Sie sich an der RHEL-Webkonsole mit Administratorrechten an.
   Details finden Sie unter Anmeldung an der Web-Konsole.

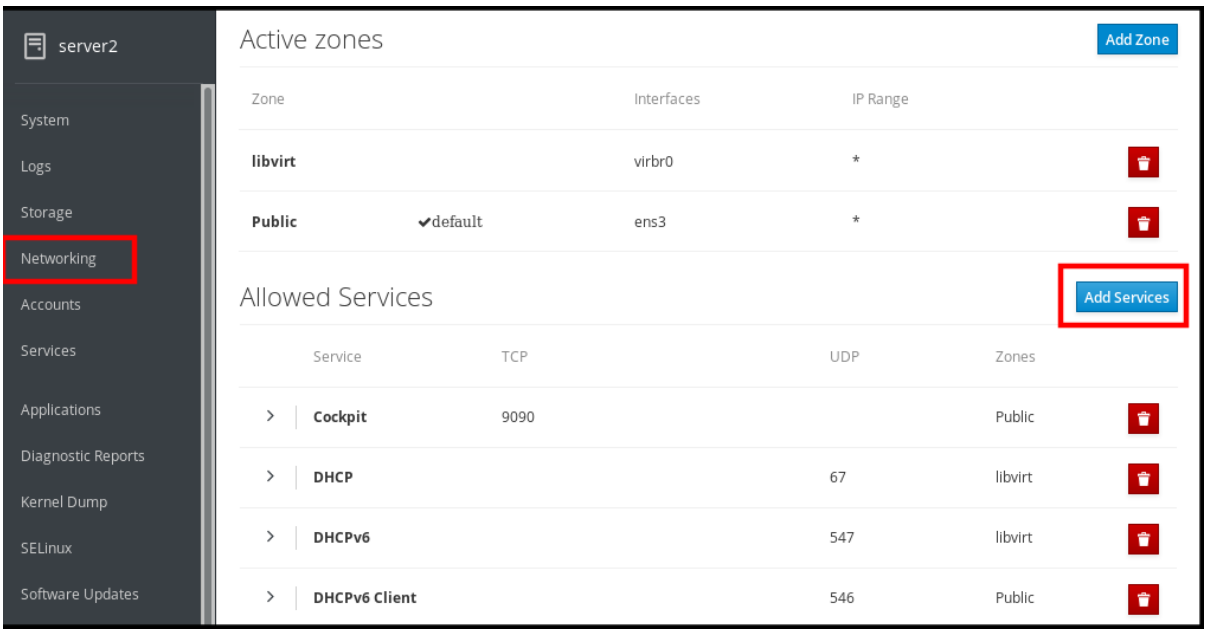
2. Klicken Sie auf **Networking**.

3. Klicken Sie auf den Titel der Box **Firewall**.



   Wenn Sie das Feld **Firewall** nicht sehen, melden Sie sich an der Webkonsole mit den Administrationsrechten an.

4. Klicken Sie im Bereich **Firewall** auf **Add Services**.



5. Wählen Sie im Dialogfeld **Add Services** eine Zone aus, für die Sie den Dienst hinzufügen möchten.
   Das Dialogfeld **Add Services** enthält nur dann eine Liste der aktiven Firewall-Zonen, wenn das System mehrere aktive Zonen enthält.

   Wenn das System nur eine (die Standard-)Zone verwendet, enthält der Dialog keine Zoneneinstellungen.

6. Klicken Sie im Dialogfeld **Add Ports** auf das Optionsfeld **Custom Ports**.

7. Fügen Sie in den Feldern TCP und UDP Ports entsprechend den Beispielen hinzu. Sie können Ports in den folgenden Formaten hinzufügen:

   - Port-Nummern wie z. B. 22

   - Bereich von Port-Nummern wie z. B. 5900-5910

- Aliasnamen wie nfs, rsync

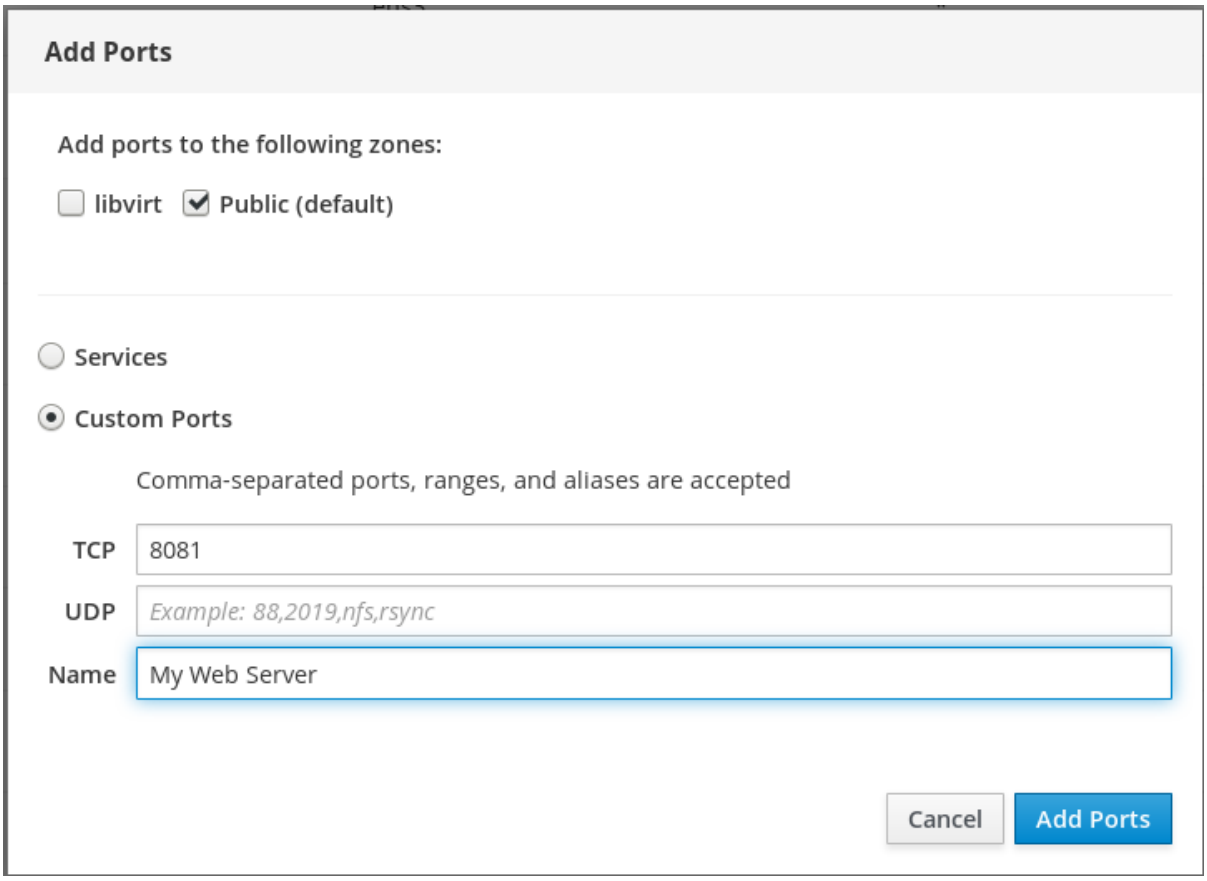
ANMERKUNG

Sie können mehrere Werte in jedes Feld eingeben. Die Werte müssen mit dem Komma und ohne Leerzeichen getrennt werden, zum Beispiel: 8080,8081,http

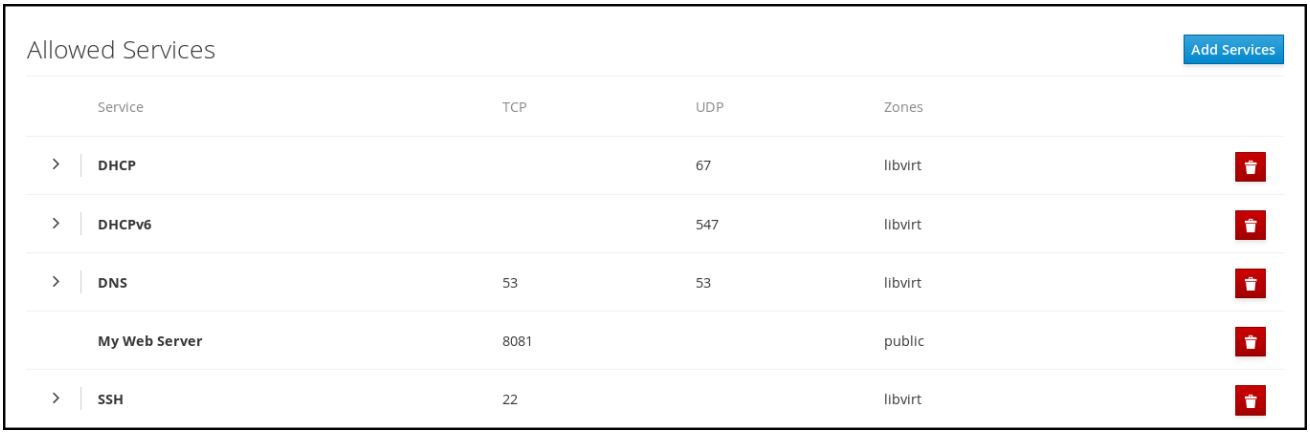
8. Nachdem Sie die Portnummer in den Feldern **TCP** und/oder **UDP** eingegeben haben, überprüfen Sie den Dienstnamen im Feld **Name**.
   Im Feld **Name** wird der Name des Dienstes angezeigt, für den dieser Port reserviert ist. Sie können den Namen umschreiben, wenn Sie sicher sind, dass dieser Port frei ist und kein Server über diesen Port kommunizieren muss.

9. Fügen Sie im Feld **Name** einen Namen für den Dienst einschließlich definierter Ports hinzu.

10. Klicken Sie auf die Schaltfläche **Add Ports**.



Um die Einstellungen zu überprüfen, gehen Sie auf die Seite **Firewall** und suchen Sie den Dienst in der Liste von **Allowed Services**.



13.9. DEAKTIVIEREN VON ZONEN ÜBER DIE WEB-KONSOLE

Dieser Abschnitt beschreibt, wie Sie eine Firewall-Zone in Ihrer Firewall-Konfiguration über die Web-Konsole deaktivieren.

Voraussetzungen

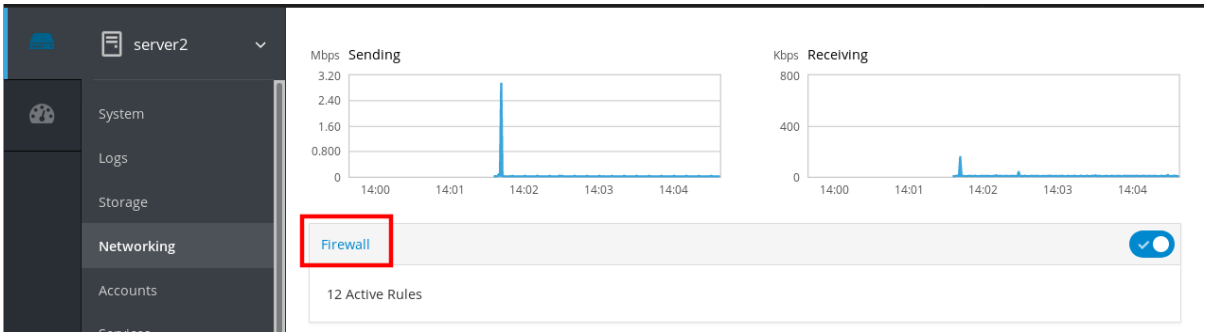
- Die RHEL 8 Web-Konsole wurde installiert.
  Details finden Sie unter Installieren der Web-Konsole.

Verfahren

1. Melden Sie sich an der RHEL-Webkonsole mit Administratorrechten an.
   Details finden Sie unter Anmeldung an der Web-Konsole.

2. Klicken Sie auf **Networking**.

3. Klicken Sie auf den Titel der Box **Firewall**.



   Wenn Sie das Feld **Firewall** nicht sehen, melden Sie sich an der Webkonsole mit den Administratorrechten an.

4. Klicken Sie in der Tabelle **Active zones** auf das Symbol **Delete** bei der Zone, die Sie entfernen möchten.

Die Zone ist nun deaktiviert und die Schnittstelle enthält keine geöffneten Dienste und Ports, die in der Zone konfiguriert wurden.

KAPITEL 14. ANWENDEN EINES GENERIERTEN ANSIBLE-PLAYBOOKS

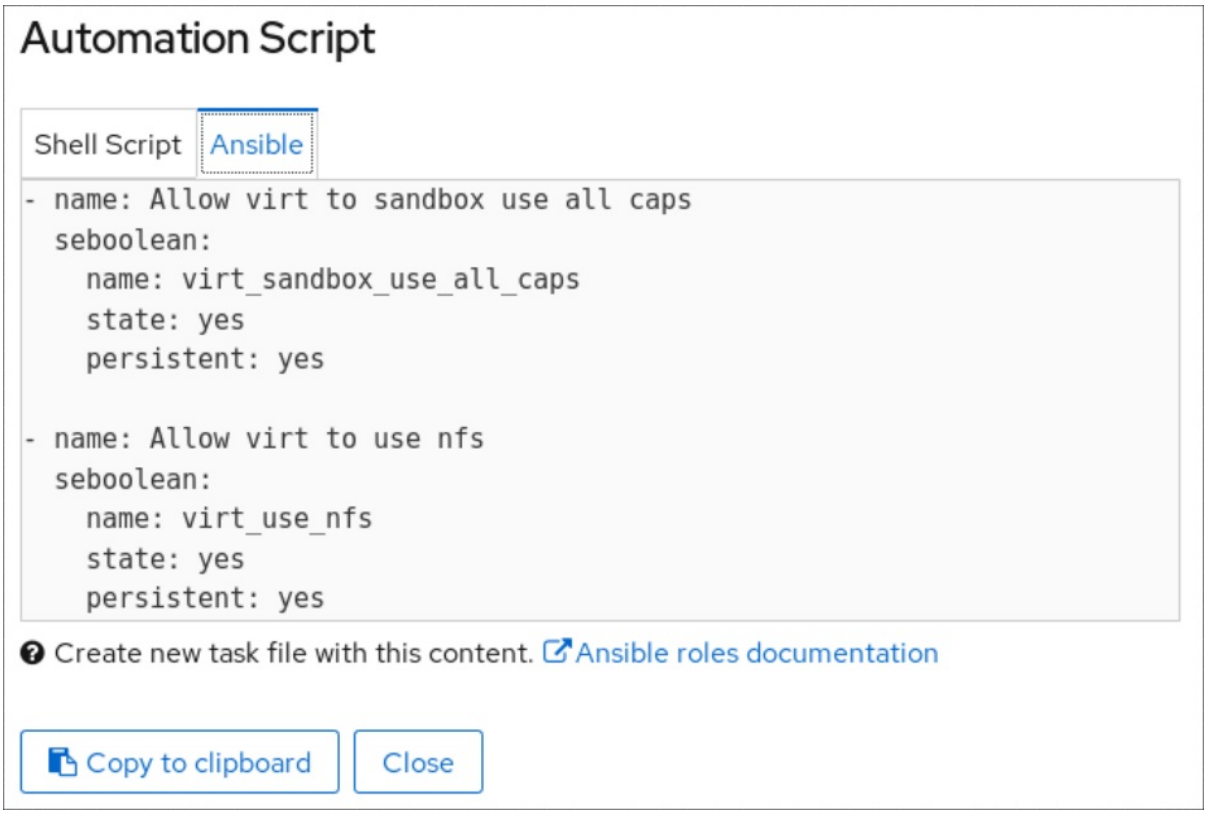
Bei der Fehlerbehebung von Problemen mit SELinux kann die Web-Konsole ein Shell-Skript oder ein Ansible-Playbook erzeugen, das Sie dann exportieren und auf weitere Rechner anwenden können.

Voraussetzungen

- Die Oberfläche der Web-Konsole muss installiert und zugänglich sein.
  Details finden Sie unter Installieren der Web-Konsole.

Verfahren

1. Klicken Sie auf **SELinux**.
2. Klicken Sie auf "Automatisierungsskript anzeigen" auf der oberen rechten Seite.
   Es öffnet sich ein Fenster mit dem generierten Skript. Sie können zwischen einem Shell-Skript und einer Registerkarte mit Optionen für die Ansible-Playbook-Generierung navigieren.



3. Klicken Sie auf die Schaltfläche **In die Zwischenablage kopieren**, um das Skript oder Playbook auszuwählen und es anzuwenden.

Als Ergebnis haben Sie ein Automatisierungsskript, das Sie auf weitere Maschinen anwenden können.

Zusätzliche Ressourcen

- Fehlerbehebung bei Problemen im Zusammenhang mit SELinux
- Bereitstellen der gleichen SELinux-Konfiguration auf mehreren Systemen
- Details zum Befehl **ansible-playbook** finden Sie in der Man Page **ansible-playbook(1)**.

KAPITEL 15. VERWALTEN VON PARTITIONEN ÜBER DIE WEB-KONSOLE

Lernen Sie, wie Sie Dateisysteme unter RHEL 8 mit der Web-Konsole verwalten.

Details zu den verfügbaren Dateisystemen finden Sie in der Übersicht der verfügbaren Dateisysteme.

15.1. ANZEIGE VON MIT DATEISYSTEMEN FORMATIERTEN PARTITIONEN IN DER WEB-KONSOLE

Der Bereich **Storage** in der Web-Konsole zeigt alle verfügbaren Dateisysteme in der Tabelle **Filesystems** an.

Dieser Abschnitt navigiert Sie zu der Liste der Partitionen, die mit den in der Web-Konsole angezeigten Dateisystemen formatiert sind.

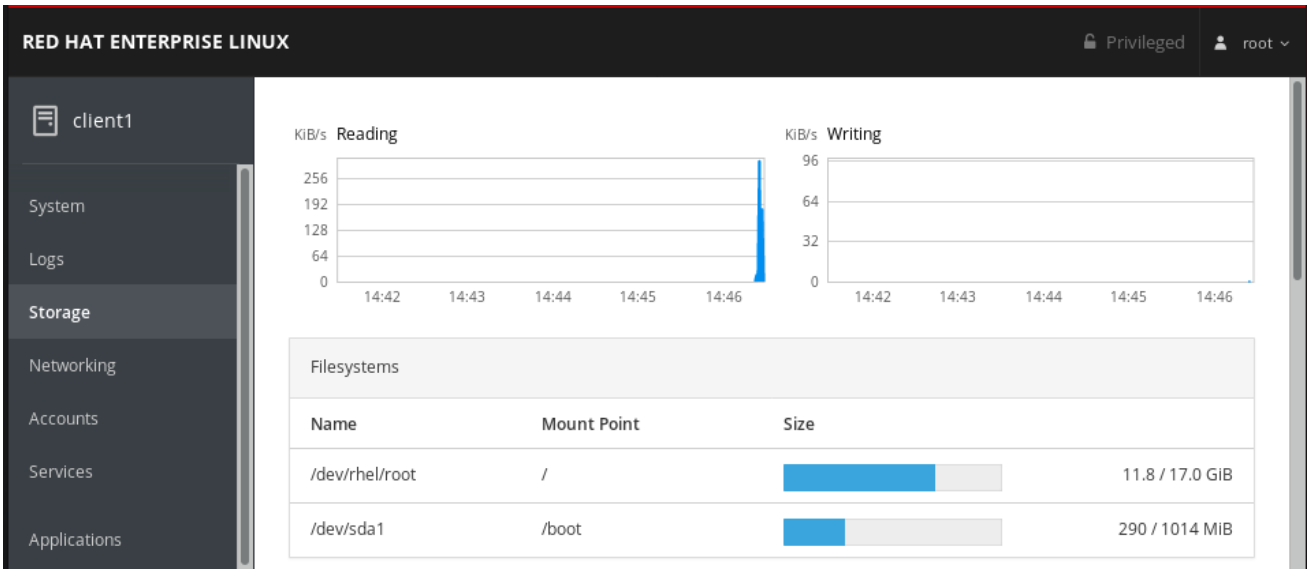
Voraussetzungen

- Das Paket **cockpit-storaged** ist auf Ihrem System installiert.
- Die Web-Konsole muss installiert und zugänglich sein.
  Details finden Sie unter Installieren der Web-Konsole.

Verfahren

1. Melden Sie sich an der RHEL-Webkonsole an.
   Details finden Sie unter Anmeldung an der Web-Konsole.
2. Klicken Sie auf die Registerkarte **Storage**.

In der Tabelle **Filesystems** sehen Sie alle verfügbaren Partitionen, die mit Dateisystemen formatiert sind, deren Namen, Größe und wie viel Speicherplatz auf jeder Partition verfügbar ist.



15.2. ERSTELLEN VON PARTITIONEN IN DER WEB-KONSOLE

So erstellen Sie eine neue Partition:

- Verwenden einer vorhandenen Partitionstabelle
- Erstellen Sie eine Partition

Voraussetzungen

- Das Paket **cockpit-storaged** ist auf Ihrem System installiert.
- Die Web-Konsole muss installiert und zugänglich sein.
  Details finden Sie unter Installieren der Web-Konsole.
- Ein mit dem System verbundenes unformatiertes Volume, das in der Tabelle **Other Devices** auf der Registerkarte **Storage** sichtbar ist.

Verfahren

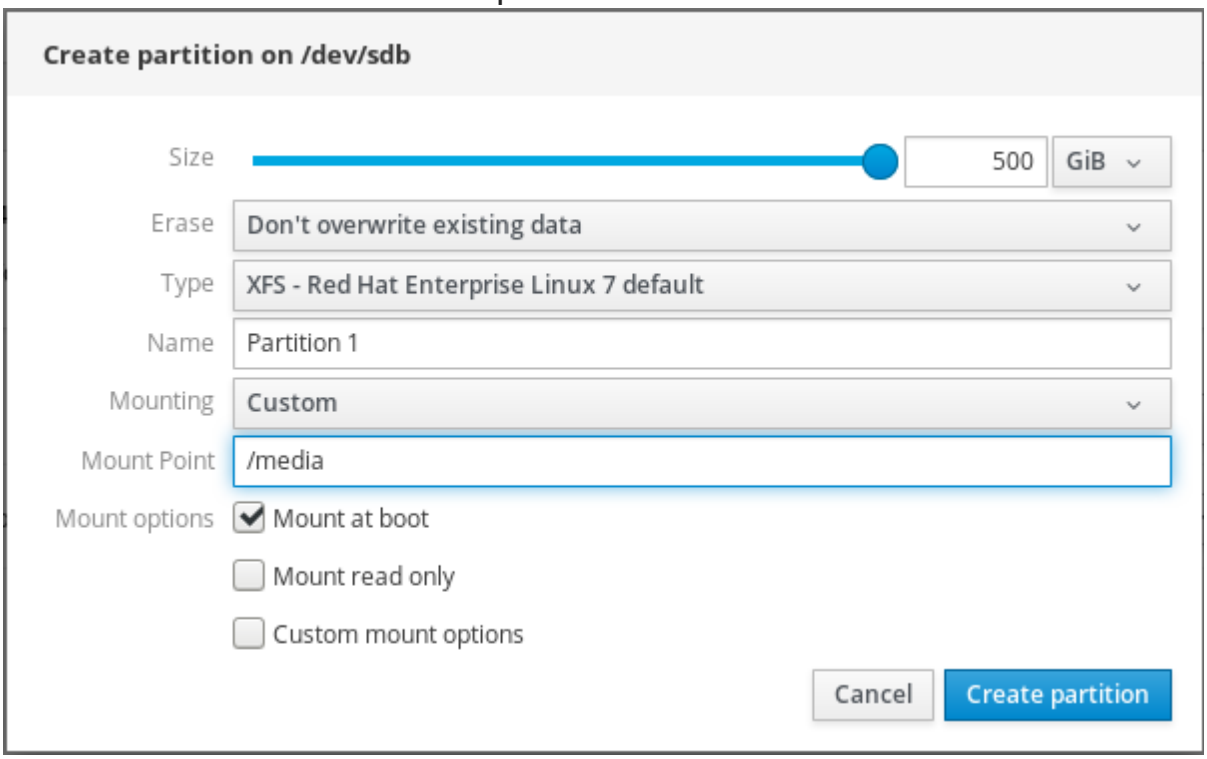
1. Melden Sie sich an der RHEL-Webkonsole an.
   Details finden Sie unter Anmeldung an der Web-Konsole.
2. Klicken Sie auf die Registerkarte **Storage**.
3. Klicken Sie in der Tabelle **Other Devices** auf ein Volume, in dem Sie die Partition erstellen möchten.
4. Klicken Sie im Bereich **Content** auf die Schaltfläche **Create Partition**.
5. Wählen Sie im Dialogfeld **Create partition** die Größe der neuen Partition.
6. Wählen Sie im Dropdown-Menü **Erase**:
   - **Don't overwrite existing data** – die RHEL-Webkonsole schreibt nur den Festplatten-Header neu. Der Vorteil dieser Option ist die Geschwindigkeit der Formatierung.
   - **Overwrite existing data with zeros** – die RHEL-Webkonsole schreibt die gesamte Festplatte mit Nullen neu. Diese Option ist langsamer, weil das Programm die gesamte Festplatte durchgehen muss, aber sie ist sicherer. Verwenden Sie diese Option, wenn der Datenträger Daten enthält und Sie diese überschreiben müssen.
7. Wählen Sie im Dropdown-Menü **Type** ein Dateisystem aus:
   - **XFS** Dateisystem unterstützt große logische Volumes, das Umschalten physischer Laufwerke online ohne Ausfall und das Erweitern eines vorhandenen Dateisystems. Lassen

Sie dieses Dateisystem ausgewählt, wenn Sie keine andere starke Präferenz haben.

- **ext4** Dateisystem unterstützt:
  - Logische Datenträger
  - Physikalische Laufwerke online schalten ohne Ausfall
  - Wachsen eines Dateisystems
  - Verkleinern eines Dateisystems

Als zusätzliche Option können Sie die Verschlüsselung der Partition durch LUKS (Linux Unified Key Setup) aktivieren, die es Ihnen erlaubt, das Volume mit einer Passphrase zu verschlüsseln.

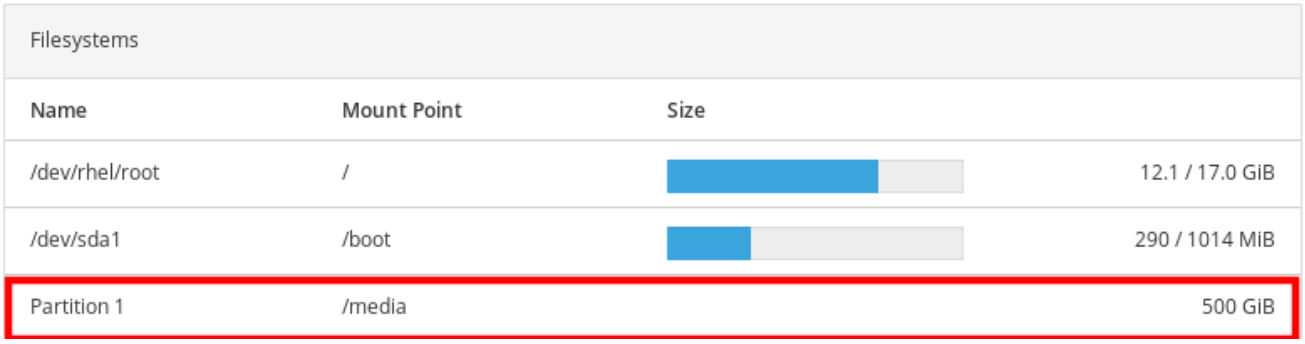
8. Geben Sie in das Feld **Name** den Namen des logischen Volumes ein.
9. Wählen Sie im Dropdown-Menü **Mounting** die Option **Custom**.
   Die Option **Default** stellt nicht sicher, dass das Dateisystem beim nächsten Booten eingehängt wird.
10. Fügen Sie im Feld **Mount Point** den Einhängepfad hinzu.
11. Wählen Sie **Mount at boot**.
12. Klicken Sie auf die Schaltfläche **Create partition**.



Die Formatierung kann einige Minuten dauern, je nachdem, wie groß das Volume ist und welche Formatierungsoptionen gewählt wurden.

Nachdem die Formatierung erfolgreich abgeschlossen wurde, können Sie die Details des formatierten logischen Volumes auf der Registerkarte **Filesystem** sehen.

Um zu überprüfen, ob die Partition erfolgreich hinzugefügt wurde, wechseln Sie auf die Registerkarte **Storage** und prüfen Sie die Tabelle **Filesystems**.



15.3. LÖSCHEN VON PARTITIONEN IN DER WEB-KONSOLE

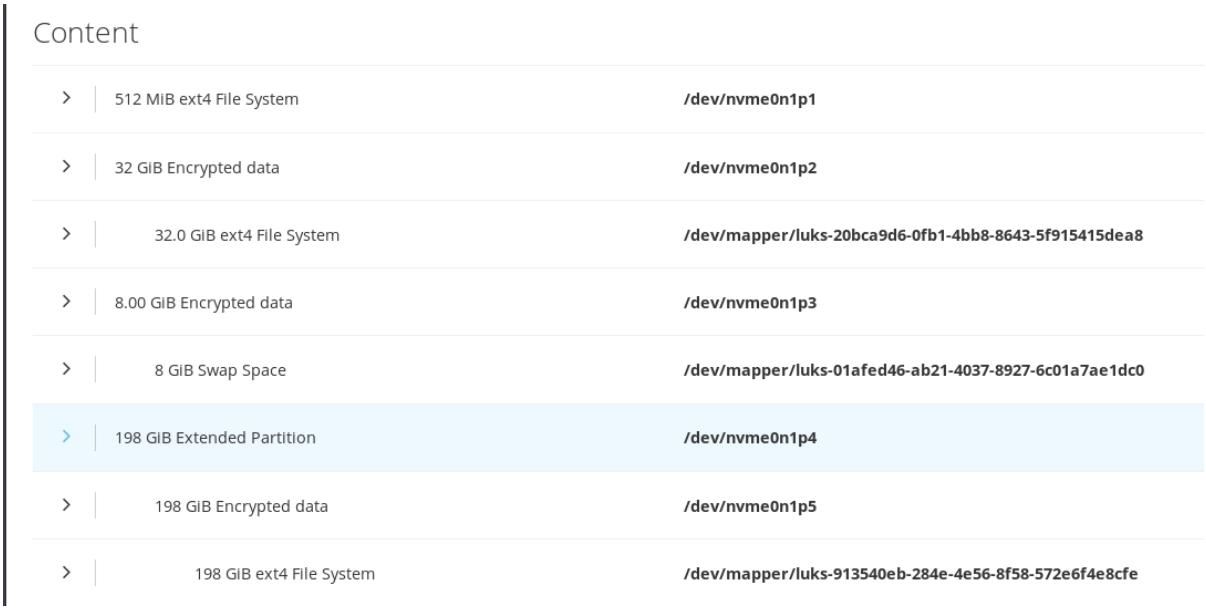
Dieser Absatz ist die Einleitung des Verfahrensmoduls: eine kurze Beschreibung des Verfahrens.

Voraussetzungen

- Das Paket **cockpit-storaged** ist auf Ihrem System installiert.
- Die Web-Konsole muss installiert und zugänglich sein.
  Details finden Sie unter Installieren der Web-Konsole.
- Hängen Sie das Dateisystem der Partition aus.
  Details zum Einhängen und Aushängen von Partitionen finden Sie unter Abschnitt 15.4, »Einhängen und Aushängen von Dateisystemen in der Web-Konsole«.

Verfahren

1. Melden Sie sich an der RHEL-Webkonsole an.
   Details finden Sie unter Anmeldung an der Web-Konsole.
2. Klicken Sie auf die Registerkarte **Storage**.
3. Wählen Sie in der Tabelle **Filesystems** ein Volume aus, in dem Sie die Partition löschen möchten.
4. Klicken Sie im Bereich **Content** auf die Partition, die Sie löschen möchten.



5. Die Partition rollt herunter und Sie können auf die Schaltfläche **Delete** klicken.

Die Partition darf nicht eingehängt und verwendet werden.

Um zu überprüfen, ob die Partition erfolgreich entfernt wurde, wechseln Sie auf die Registerkarte **Storage** und prüfen Sie die Tabelle **Content**.

15.4. EINHÄNGEN UND AUSHÄNGEN VON DATEISYSTEMEN IN DER WEB-KONSOLE

Um Partitionen auf RHEL-Systemen verwenden zu können, müssen Sie ein Dateisystem auf der Partition als Gerät einhängen.

ANMERKUNG

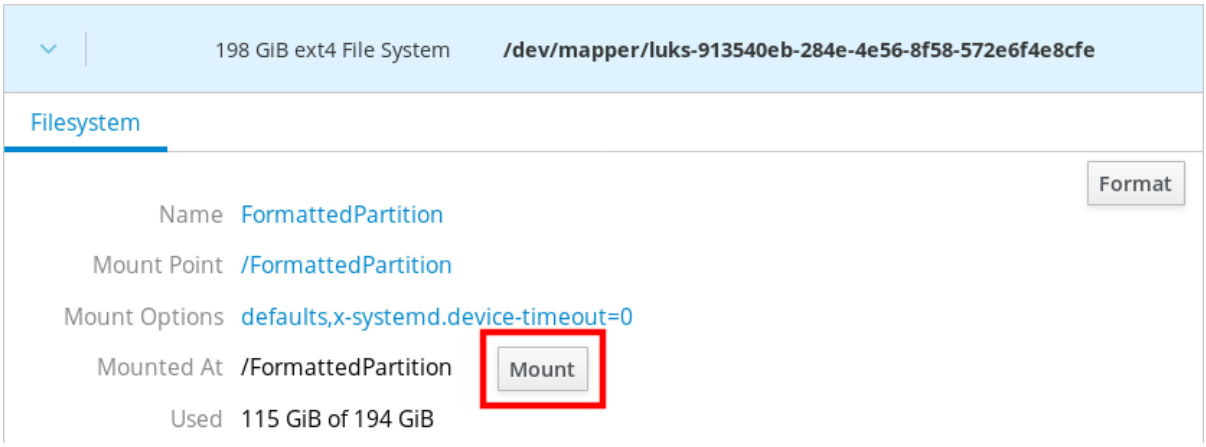
Sie können ein Dateisystem auch aushängen und das RHEL-System wird es nicht mehr verwenden. Durch das Aushängen des Dateisystems können Sie Geräte löschen, entfernen oder neu formatieren.

Voraussetzungen

- Das Paket **cockpit-storaged** ist auf Ihrem System installiert.
- Die Web-Konsole muss installiert und zugänglich sein.
  Details finden Sie unter Installieren der Web-Konsole.
- Wenn Sie ein Dateisystem aushängen möchten, stellen Sie sicher, dass das System keine in der Partition gespeicherten Dateien, Dienste oder Anwendungen verwendet.

Verfahren

1. Melden Sie sich an der RHEL-Webkonsole an.
   Details finden Sie unter Anmeldung an der Web-Konsole.
2. Klicken Sie auf die Registerkarte **Storage**.
3. Wählen Sie in der Tabelle **Filesystems** ein Volume aus, in dem Sie die Partition löschen möchten.
4. Klicken Sie im Bereich **Content** auf die Partition, deren Dateisystem Sie ein- oder aushängen möchten.
5. Klicken Sie auf die Schaltfläche **Mount** oder **Unmount**.



Zu diesem Zeitpunkt ist das Dateisystem entsprechend Ihrer Aktion ein- oder ausgehängt worden.

KAPITEL 16. VERWALTEN VON NFS-EINHÄNGUNGEN IN DER WEB-KONSOLE

Die RHEL 8 Web-Konsole ermöglicht es Ihnen, entfernte Verzeichnisse über das Network File System (NFS)-Protokoll einzuhängen.

NFS ermöglicht es, entfernte Verzeichnisse, die sich im Netzwerk befinden, zu erreichen und einzuhängen und mit den Dateien zu arbeiten, als ob sich das Verzeichnis auf Ihrem physischen Laufwerk befände.

Voraussetzungen

- Die RHEL 8 Web-Konsole wurde installiert.
  Details finden Sie unter Installieren der Web-Konsole.
- Das Paket **cockpit-storaged** ist auf Ihrem System installiert.
- Name oder IP-Adresse des NFS-Servers.
- Pfad zu dem Verzeichnis auf dem Remote-Server.

16.1. VERBINDEN VON NFS-EINHÄNGUNGEN IN DER WEB-KONSOLE

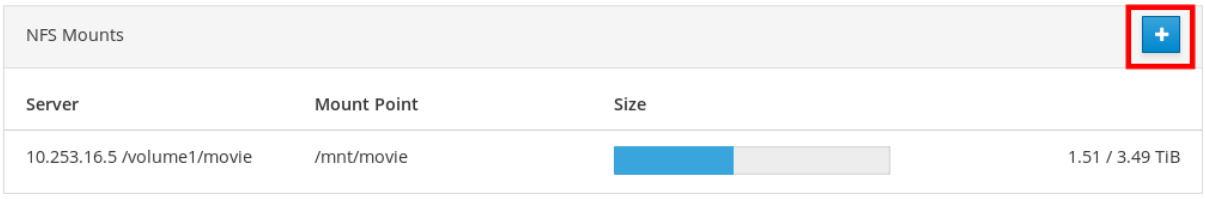
Verbinden Sie ein entferntes Verzeichnis über NFS mit Ihrem Dateisystem.

Voraussetzungen

- Name oder IP-Adresse des NFS-Servers.
- Pfad zu dem Verzeichnis auf dem Remote-Server.

Verfahren

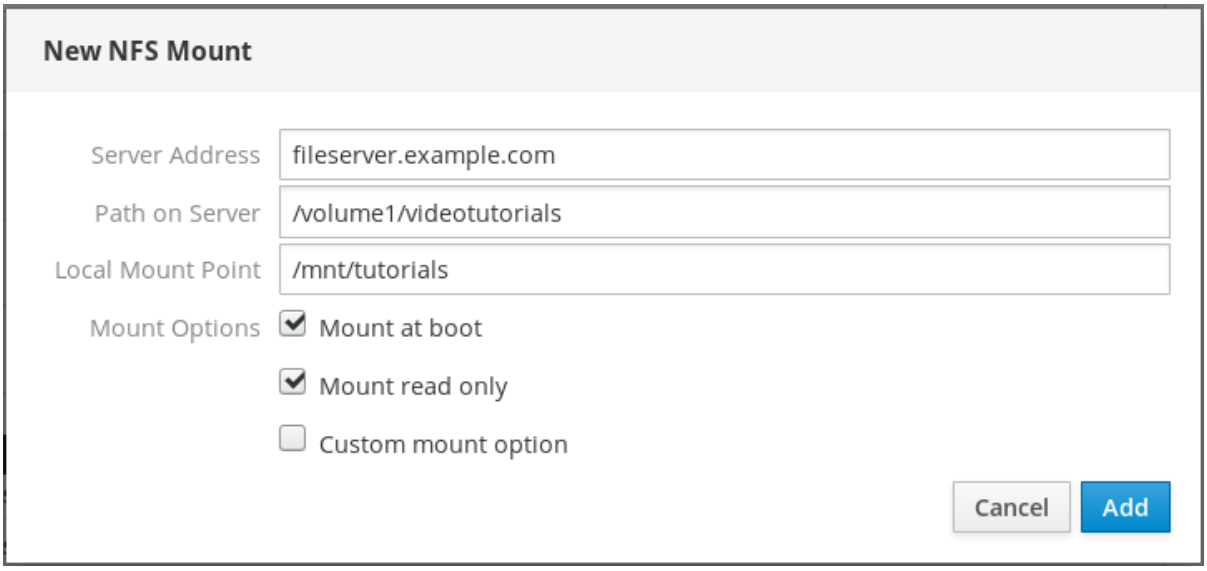
1. Melden Sie sich an der RHEL 8 Web-Konsole an.
   Details finden Sie unter Anmeldung an der Web-Konsole.
2. Klicken Sie auf **Storage**.
3. Klicken Sie auf im Bereich **NFS mounts**.



4. Geben Sie im Dialogfeld **New NFS Mount** den Server oder die IP-Adresse des Remote-Servers ein.
5. Geben Sie in das Feld **Path on Server** den Pfad zu dem Verzeichnis ein, das Sie mounten möchten.
6. Geben Sie in das Feld **Local Mount Point** den Pfad ein, unter dem Sie das Verzeichnis in Ihrem lokalen System finden möchten.

7. Wählen Sie **Mount at boot**. Dadurch wird sichergestellt, dass das Verzeichnis auch nach dem Neustart des lokalen Systems erreichbar ist.

8. Wählen Sie optional **Mount read only**, wenn Sie den Inhalt nicht ändern möchten.



9. Klicken Sie auf **Add**.

An diesem Punkt können Sie das gemountete Verzeichnis öffnen und überprüfen, ob der Inhalt zugänglich ist.

Zur Fehlersuche können Sie die Verbindung mit den Benutzerdefinierten Montageoptionen anpassen.

16.2. ANPASSEN DER NFS-EINHÄNGEOPTIONEN IN DER WEB-KONSOLE

Bearbeiten Sie eine vorhandene NFS-Einhängung und fügen Sie benutzerdefinierte Einhängeoptionen hinzu.

Benutzerdefinierte Einhängeoptionen können Ihnen bei der Fehlersuche in der Verbindung oder beim Ändern von Parametern der NFS-Einhängung helfen, z. B. beim Ändern von Timeout-Grenzen oder beim Konfigurieren der Authentifizierung.

Voraussetzungen

- NFS-Mount hinzugefügt.

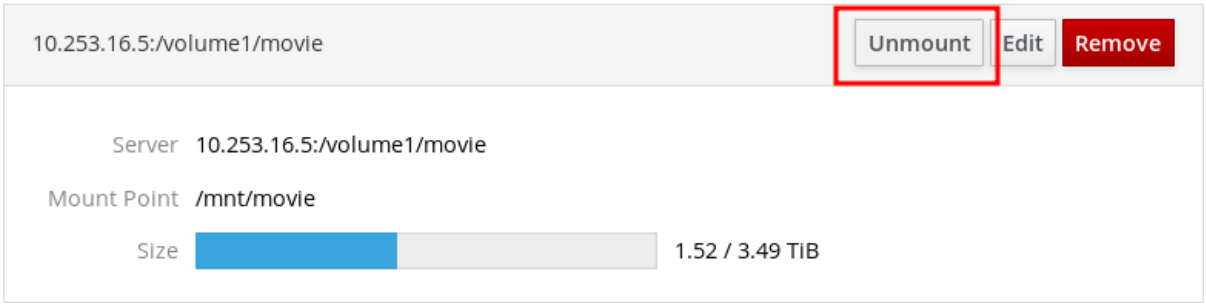
Verfahren

1. Melden Sie sich an der RHEL 8 Web-Konsole an.
   Details finden Sie unter Anmeldung an der Web-Konsole.

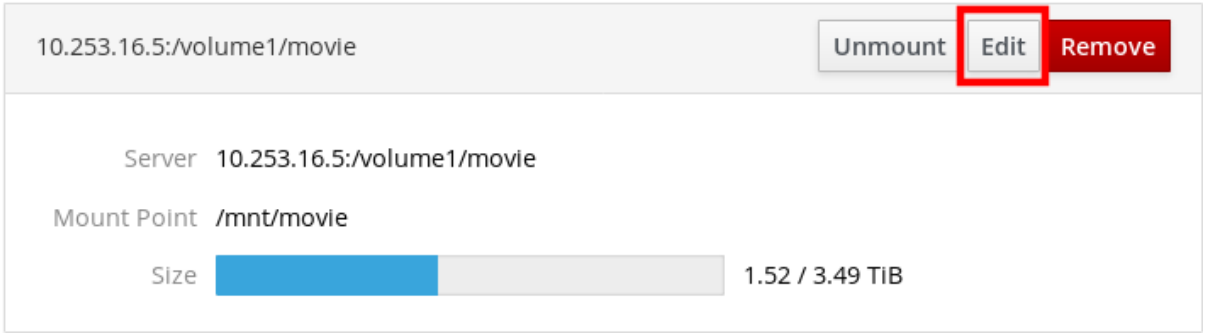
2. Klicken Sie auf **Storage**.

3. Klicken Sie auf die NFS-Einhängung, die Sie anpassen möchten.

4. Wenn das Remote-Verzeichnis eingehängt ist, klicken Sie auf **Unmount**.
   Das Verzeichnis darf während der Konfiguration der benutzerdefinierten Einhängeoptionen nicht eingehängt werden. Andernfalls speichert die Web-Konsole die Konfiguration nicht und dies führt zu einem Fehler.



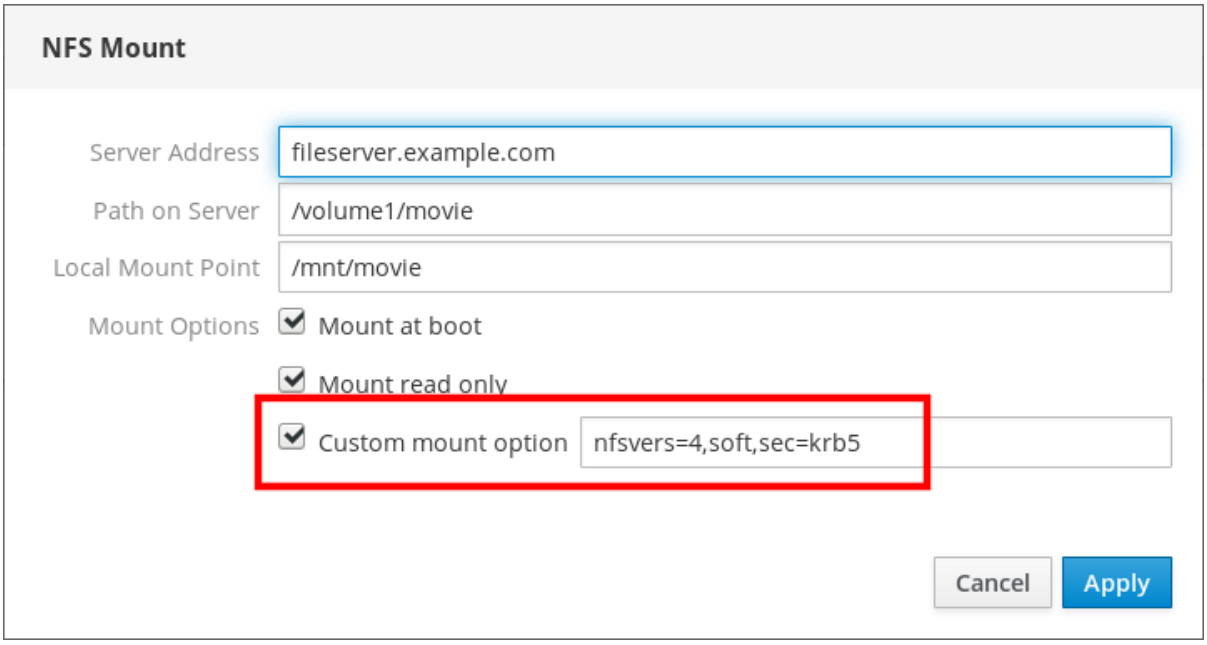
5. Klicken Sie auf **Edit**.



6. Wählen Sie im Dialogfeld **NFS Mount** die Option **Custom mount option**.

7. Geben Sie Einhängeoptionen durch ein Komma getrennt ein. Zum Beispiel:

   - **nfsvers=4**- die Versionsnummer des NFS-Protokolls
   - **soft**- Art der Wiederherstellung nach Zeitüberschreitung einer NFS-Anfrage
   - **sec=krb5**- Dateien auf dem NFS-Server können durch Kerberos-Authentifizierung gesichert werden. Sowohl der NFS-Client als auch der Server müssen die Kerberos-Authentifizierung unterstützen.



Eine vollständige Liste der NFS-Einhängeoptionen erhalten Sie, wenn Sie in der Befehlszeile **man nfs** eingeben.

8. Klicken Sie auf **Apply**.

9. Klicken Sie auf **Mount**.

Jetzt können Sie das gemountete Verzeichnis öffnen und überprüfen, ob der Inhalt zugänglich ist.

KAPITEL 17. REDUNDANTE ARRAYS UNABHÄNGIGER FESTPLATTEN IN DER WEB-KONSOLE VERWALTEN

Redundant Arrays of Independent Disks (RAID) stellt eine Möglichkeit dar, wie mehrere Festplatten in einem Speicher angeordnet werden können. RAID schützt die auf den Festplatten gespeicherten Daten vor Festplattenausfällen.

RAID verwendet die folgenden Datenverteilungsstrategien:

- Mirroring - Daten werden an zwei verschiedene Orte kopiert. Wenn eine Festplatte ausfällt, haben Sie eine Kopie und Ihre Daten sind nicht verloren.
- Striping - Daten werden gleichmäßig auf die Festplatten verteilt.

Der Grad des Schutzes hängt vom RAID-Level ab.

Die RHEL Web-Konsole unterstützt die folgenden RAID-Level:

- RAID 0 (Stripe)
- RAID 1 (Spiegelung)
- RAID 4 (Dedizierte Parität)
- RAID 5 (Verteilte Parität)
- RAID 6 (Doppelte verteilte Parität)
- RAID 10 (Stripe of Mirrors)

Bevor Sie Festplatten im RAID verwenden können, müssen Sie Folgendes tun:

- Erstellen Sie ein RAID.
- Formatieren Sie es mit dem Dateisystem.
- Montieren Sie das RAID auf dem Server.

Voraussetzungen

- Die RHEL 8 Web-Konsole wurde installiert.
  Details finden Sie unter Installieren der Web-Konsole.
- Das Paket **cockpit-storaged** ist auf Ihrem System installiert.
- Die RHEL 8 Web-Konsole läuft und ist zugänglich.
  Details finden Sie unter Installieren der Web-Konsole.

17.1. RAID IN DER WEB-KONSOLE ERSTELLEN

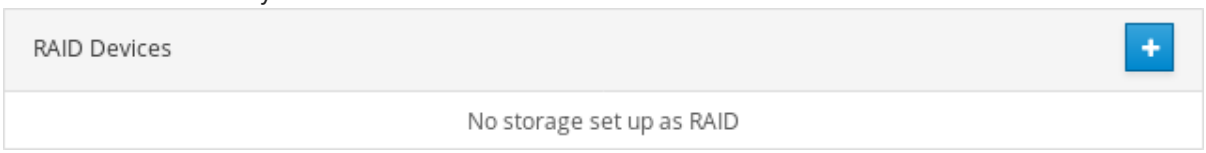
Konfigurieren Sie RAID in der RHEL 8 Web-Konsole.

Voraussetzungen

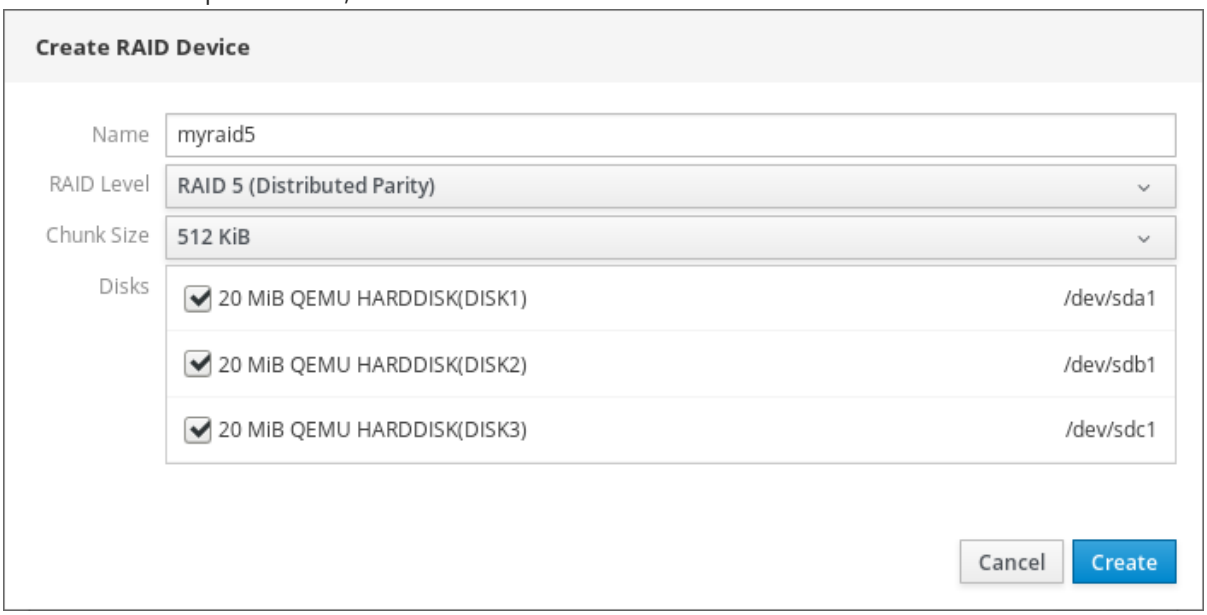
- Physikalische Festplatten, die an das System angeschlossen sind. Jeder RAID-Level erfordert eine unterschiedliche Anzahl von Festplatten.

Verfahren

1. Öffnen Sie die RHEL 8 Web-Konsole.
2. Klicken Sie auf **Storage**.
3. Klicken Sie auf das Symbol im Feld **RAID Devices**.

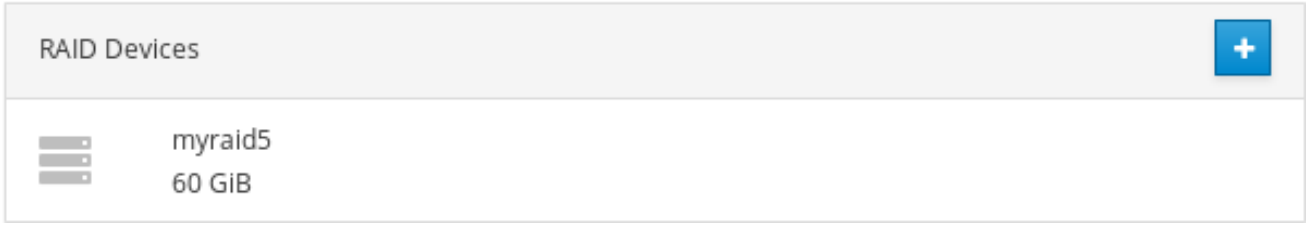


4. Geben Sie im Dialogfeld **Create RAID Device** einen Namen für ein neues RAID ein.
5. Wählen Sie in der Dropdown-Liste **RAID Level** einen RAID-Level aus, den Sie verwenden möchten.
6. Lassen Sie in der Dropdown-Liste **Chunk Size** den vordefinierten Wert stehen.
   Der Wert **Chunk Size** gibt an, wie groß jeder Block für das Schreiben von Daten ist. Wenn die Chunk-Größe 512 KiB beträgt, schreibt das System die ersten 512 KiB auf die erste Platte, die zweiten 512 KiB werden auf die zweite Platte geschrieben, und der dritte Chunk wird auf die dritte Platte geschrieben. Wenn Sie drei Festplatten in Ihrem RAID haben, wird das vierte 512 KiB wieder auf die erste Platte geschrieben.
7. Wählen Sie Festplatten aus, die Sie für RAID verwenden möchten.



8. Klicken Sie auf **Create**.

Im Bereich **Storage** können Sie das neue RAID im Feld **RAID devices** sehen und es formatieren.



Nun haben Sie folgende Möglichkeiten, wie Sie das neue RAID in der Web-Konsole formatieren und einbinden können:

- RAID formatieren
- Erstellen von Partitionen in der Partitionstabelle
- Erstellen einer Volume-Gruppe auf einem RAID

17.2. RAID IN DER WEB-KONSOLE FORMATIEREN

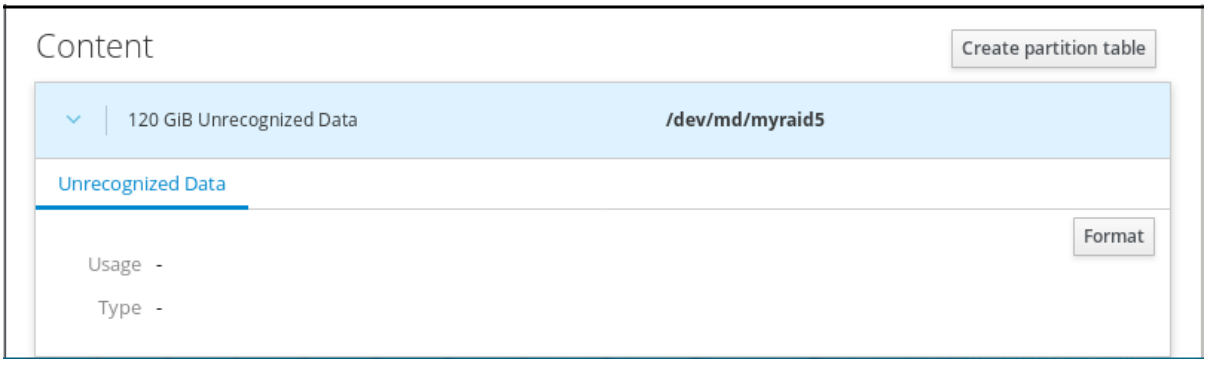
Formatieren Sie das neu angelegte Software-RAID-Gerät in der RHEL 8-Web-Oberfläche.

Voraussetzungen

- Physikalische Festplatten sind angeschlossen und von RHEL 8 sichtbar.
- RAID wird erstellt.
- Berücksichtigen Sie das Dateisystem, das für das RAID verwendet werden soll.
- Erwägen Sie das Anlegen einer Partitionierungstabelle.

Verfahren

1. Öffnen Sie die RHEL 8 Web-Konsole.
2. Klicken Sie auf **Storage**.
3. Wählen Sie im Feld **RAID devices** das RAID, das Sie formatieren möchten, indem Sie darauf klicken.
4. Scrollen Sie im Bildschirm RAID-Details nach unten zum Teil **Content**.
5. Klicken Sie auf das neu erstellte RAID.



6. Klicken Sie auf die Schaltfläche **Format**.
7. Wählen Sie in der Dropdown-Liste **Erase**:
   - **Don't overwrite existing data** – die RHEL-Webkonsole schreibt nur den Festplatten-Header neu. Der Vorteil dieser Option ist die Geschwindigkeit der Formatierung.
   - **Overwrite existing data with zeros** – die RHEL-Webkonsole schreibt die gesamte Festplatte mit Nullen neu. Diese Option ist langsamer, da das Programm die gesamte Platte durchgehen muss. Verwenden Sie diese Option, wenn das RAID irgendwelche Daten enthält

und Sie diese neu schreiben müssen.

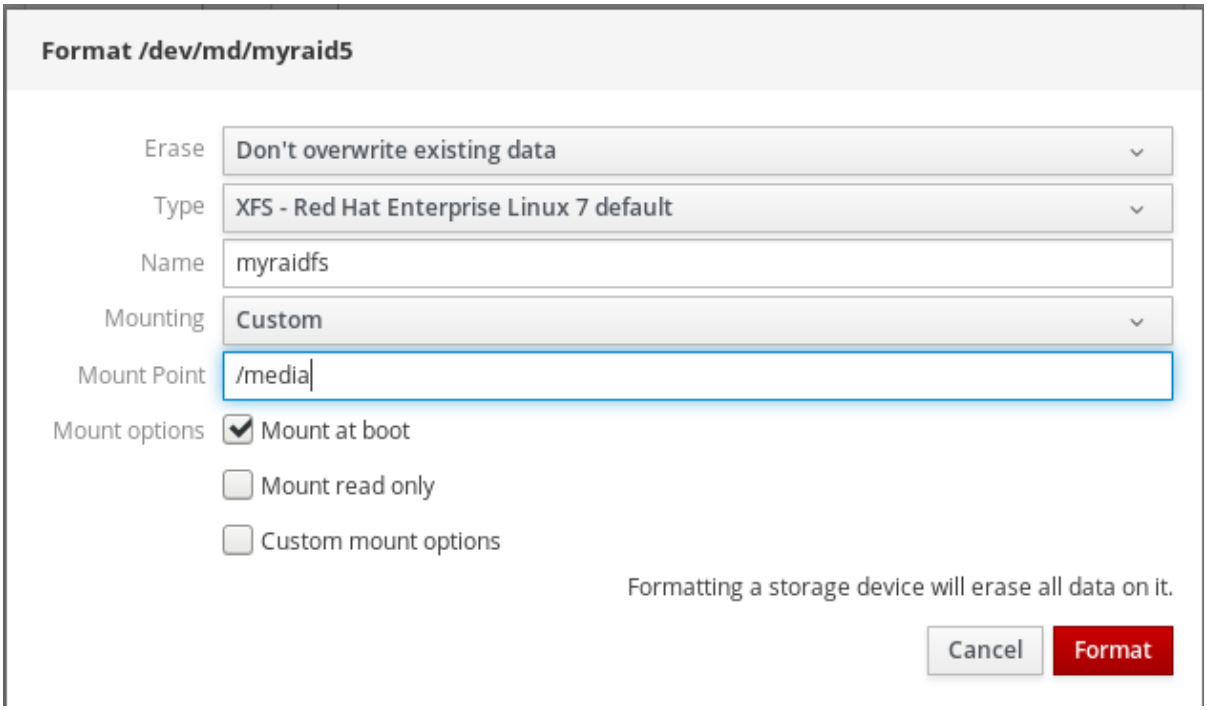
8. Wählen Sie in der Dropdown-Liste **Type** ein XFS-Dateisystem, wenn Sie keine andere starke Präferenz haben.

9. Geben Sie einen Namen für das Dateisystem ein.

10. Wählen Sie in der Dropdown-Liste **Mounting** die Option **Custom**.
Die Option **Default** stellt nicht sicher, dass das Dateisystem beim nächsten Booten eingehängt wird.

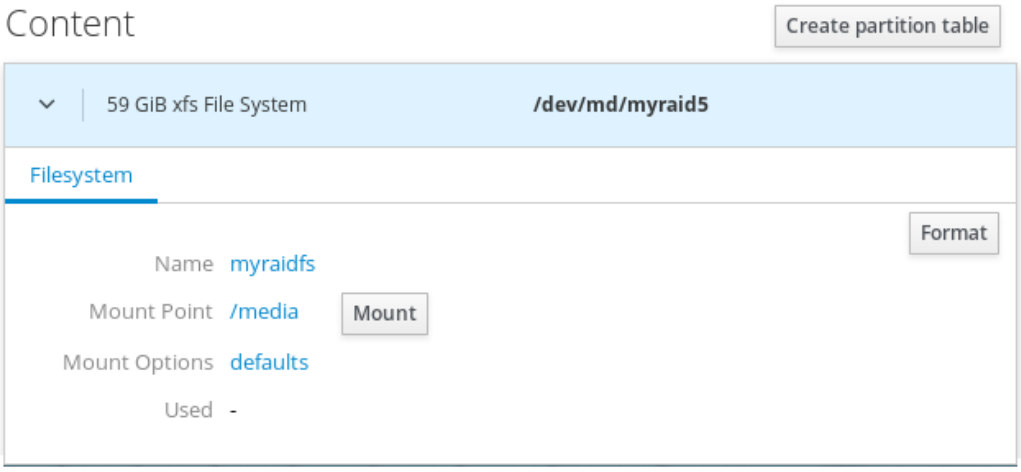
11. Fügen Sie im Feld **Mount Point** den Einhängepfad hinzu.

12. Wählen Sie **Mount at boot**



13. Klicken Sie auf die Schaltfläche **Format**.
Die Formatierung kann einige Minuten dauern, je nach den verwendeten Formatierungsoptionen und der Größe des RAID.

Nach erfolgreichem Abschluss können Sie die Details des formatierten RAIDs auf der Registerkarte **Filesystem** sehen.



14. Um das RAID zu verwenden, klicken Sie auf **Mount**.

An diesem Punkt verwendet das System ein montiertes und formatiertes RAID.

17.3. VERWENDEN DER WEB-KONSOLE ZUM ERSTELLEN EINER PARTITIONSTABELLE AUF RAID

Formatieren Sie RAID mit der Partitionstabelle auf dem neuen Software-RAID-Gerät, das in der RHEL 8-Web-Oberfläche erstellt wurde.

RAID erfordert eine Formatierung wie jedes andere Speichergerät. Sie haben zwei Möglichkeiten:

- Formatieren Sie das RAID-Gerät ohne Partitionen
- Erstellen einer Partitionstabelle mit Partitionen

Voraussetzungen

- Physikalische Festplatten sind angeschlossen und von RHEL 8 sichtbar.
- RAID wird erstellt.
- Betrachten Sie das für das RAID verwendete Dateisystem.
- Erwägen Sie das Erstellen einer Partitionierungstabelle.

Verfahren

1. Öffnen Sie die RHEL 8 Web-Konsole.
2. Klicken Sie auf **Storage**.
3. Wählen Sie im Feld **RAID devices** das RAID, das Sie bearbeiten möchten.
4. Scrollen Sie im Bildschirm RAID-Details nach unten zum Teil **Content**.
5. Klicken Sie auf das neu erstellte RAID.

6. Klicken Sie auf die Schaltfläche **Create partition table**.

7. Wählen Sie in der Dropdown-Liste **Erase**:

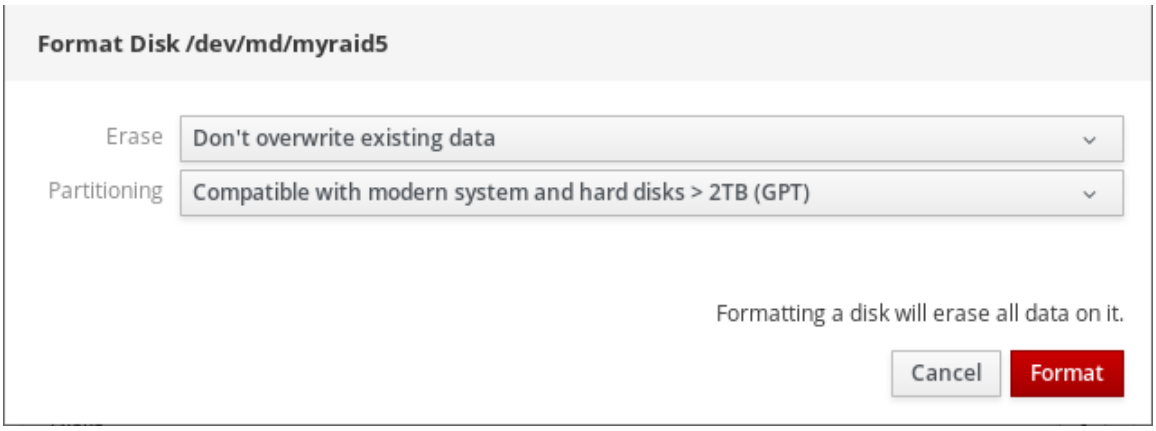
   - **Don't overwrite existing data** - die RHEL-Webkonsole schreibt nur den Festplatten-Header neu. Der Vorteil dieser Option ist die Geschwindigkeit der Formatierung.

   - **Overwrite existing data with zeros** - die RHEL-Webkonsole schreibt das gesamte RAID mit Nullen neu. Diese Option ist langsamer, weil das Programm das gesamte RAID durchlaufen muss. Verwenden Sie diese Option, wenn das RAID irgendwelche Daten enthält und Sie es neu schreiben müssen.

8. Wählen Sie in der Dropdown-Liste **Partitioning**:

   - Kompatibel mit modernen System und Festplatten > 2TB (GPT) - GUID Partition Table ist ein modernes empfohlenes Partitionierungssystem für große RAIDs mit mehr als vier Partitionen.

   - Kompatibel mit allen Systemen und Geräten (MBR) - Master Boot Record funktioniert mit Festplatten bis zu einer Größe von 2 TB. MBR unterstützt außerdem maximal vier primäre Partitionen.



9. Klicken Sie auf **Format**.

Zu diesem Zeitpunkt ist die Partitionierungstabelle erstellt worden und Sie können Partitionen erstellen.

Zum Erstellen von Partitionen siehe Verwenden der Web-Konsole zum Erstellen von Partitionen auf RAID.

17.4. VERWENDEN DER WEB-KONSOLE ZUM ERSTELLEN VON PARTITIONEN AUF RAID

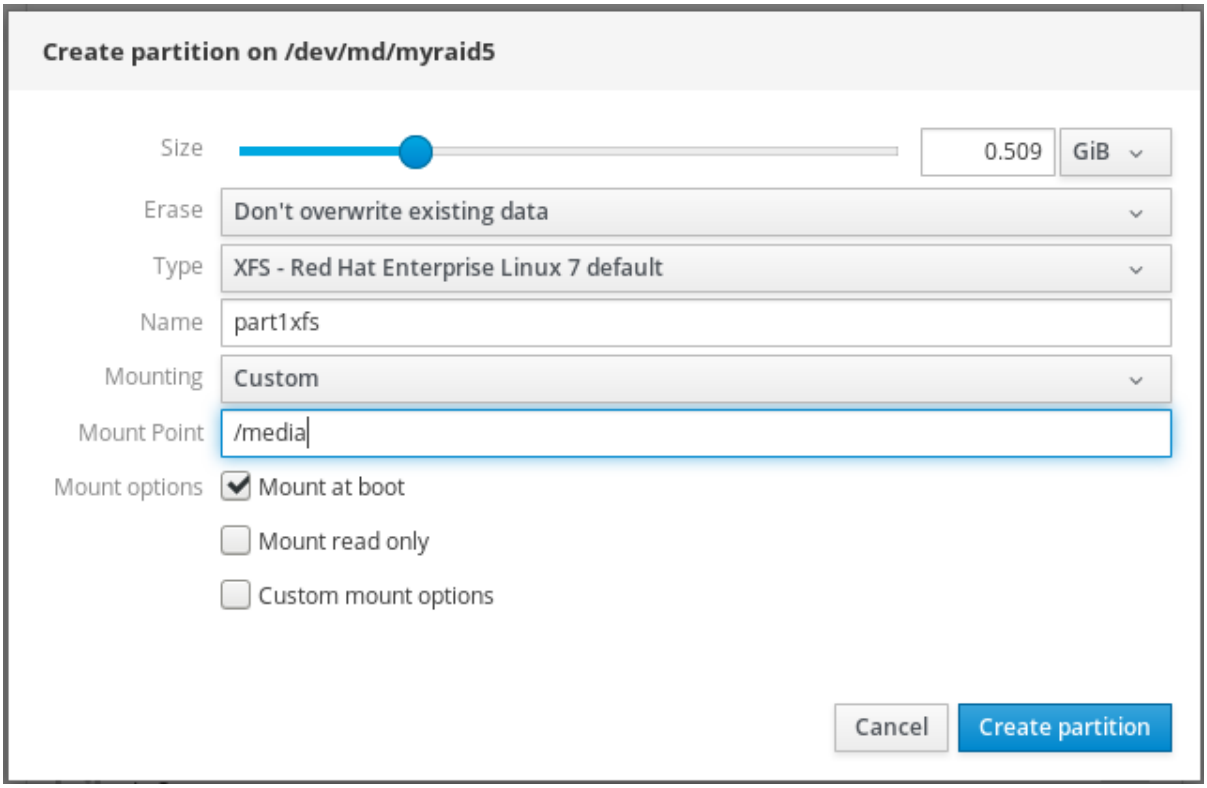
Erstellen Sie eine Partition in der vorhandenen Partitionstabelle.

Voraussetzungen

- Die Partitionstabelle wird erstellt.
  Für Details, siehe Abschnitt 17.3, »Verwenden der Web-Konsole zum Erstellen einer Partitionstabelle auf RAID«

Verfahren

1. Öffnen Sie die RHEL 8 Web-Konsole.
2. Klicken Sie auf **Storage**.
3. Klicken Sie im Feld **RAID devices** auf das RAID, das Sie bearbeiten möchten.
4. Scrollen Sie im Bildschirm RAID-Details nach unten zum Teil **Content**.
5. Klicken Sie auf das neu erstellte RAID.
6. Klicken Sie auf **Create Partition**.
7. Legen Sie im Dialogfeld **Create partition** die Größe der ersten Partition fest.
8. Wählen Sie in der Dropdown-Liste **Erase**:
   - **Don't overwrite existing data** – die RHEL-Webkonsole schreibt nur den Festplatten-Header neu. Der Vorteil dieser Option ist die Geschwindigkeit der Formatierung.
   - **Overwrite existing data with zeros** – die RHEL-Webkonsole schreibt das gesamte RAID mit Nullen neu. Diese Option ist langsamer, da das Programm das gesamte RAID durchlaufen muss. Verwenden Sie diese Option, wenn das RAID Daten enthält und Sie es neu schreiben müssen.
9. Wählen Sie in der Dropdown-Liste **Type** ein XFS-Dateisystem, wenn Sie keine andere starke Präferenz haben.
10. Geben Sie einen beliebigen Namen für das Dateisystem ein. Verwenden Sie keine Leerzeichen im Namen.
11. Wählen Sie in der Dropdown-Liste **Mounting** die Option **Custom**.
    Die Option **Default** stellt nicht sicher, dass das Dateisystem beim nächsten Booten eingehängt wird.
12. Fügen Sie im Feld **Mount Point** den Einhängepfad hinzu.
13. Wählen Sie **Mount at boot**.
14. Klicken Sie auf **Create partition**.



Die Formatierung kann einige Minuten dauern, je nach verwendeten Formatierungsoptionen und Größe des RAID.

Nach erfolgreichem Abschluss können Sie mit dem Anlegen weiterer Partitionen fortfahren.

An diesem Punkt verwendet das System ein montiertes und formatiertes RAID.

17.5. VERWENDEN DER WEB-KONSOLE ZUM ERSTELLEN EINER VOLUME-GRUPPE AUF EINEM RAID

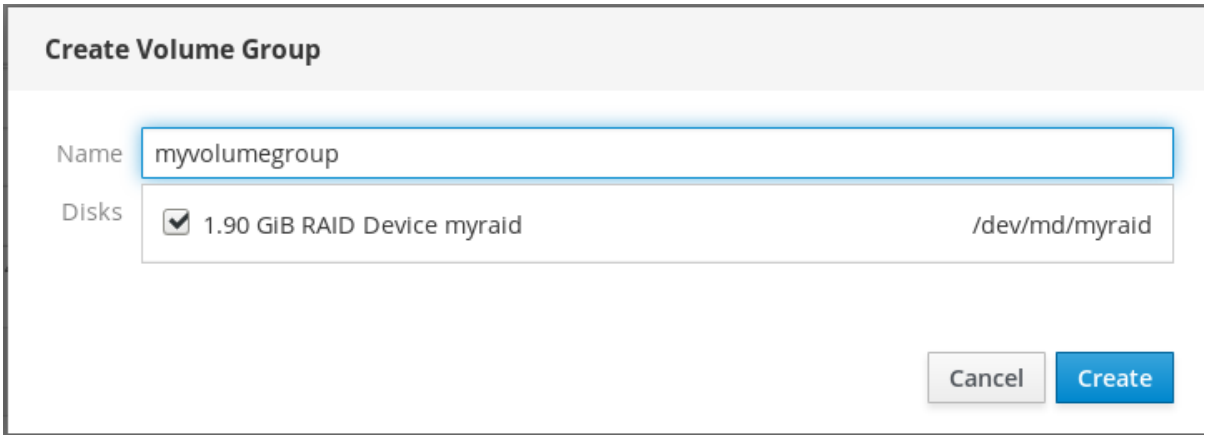
Erstellen Sie eine Volume-Gruppe aus Software-RAID.

Voraussetzungen

- RAID-Gerät, das nicht formatiert und eingehängt ist.

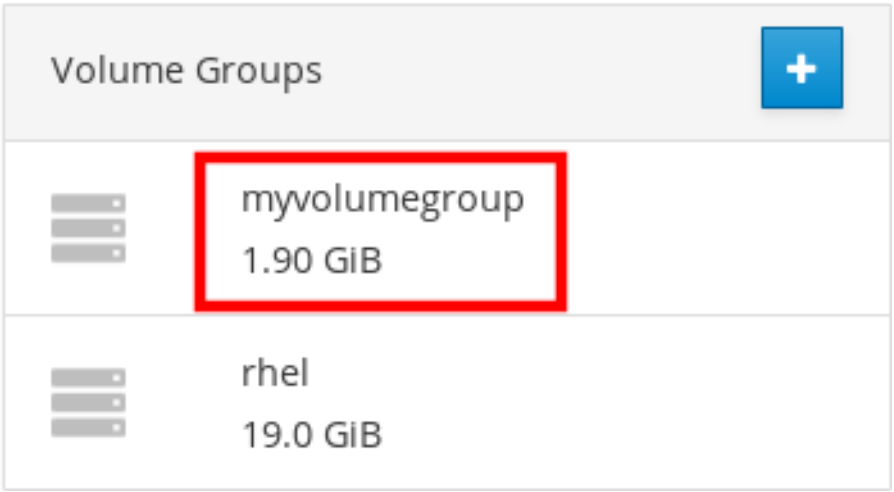
Verfahren

1. Öffnen Sie die RHEL 8 Web-Konsole.
2. Klicken Sie auf **Storage**.
3. Klicken Sie auf das Symbol im Feld **Volume Groups**.
4. Geben Sie im Dialogfeld **Create Volume Group** einen Namen für die neue Volume-Gruppe ein.
5. Wählen Sie in der Liste **Disks** ein RAID-Gerät aus.
   Wenn Sie das RAID nicht in der Liste sehen, hängen Sie das RAID vom System aus. Das RAID-Gerät darf nicht vom RHEL 8-System verwendet werden.



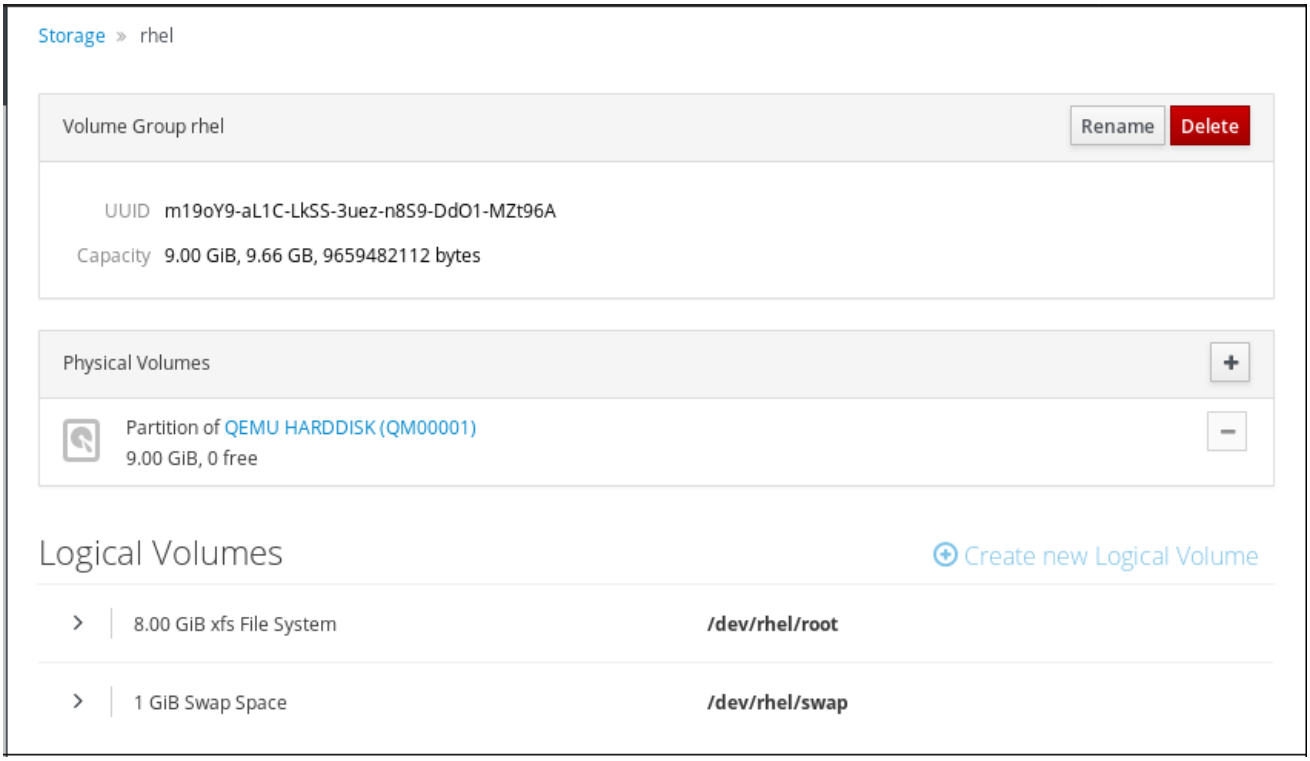
6. Klicken Sie auf **Create**.

Die neue Volume-Gruppe wurde erstellt und Sie können mit dem Erstellen eines logischen Volumes fortfahren.



KAPITEL 18. VERWENDEN DER WEB-KONSOLE ZUM KONFIGURIEREN VON LVM-LOGICAL-VOLUMES

Red Hat Enterprise Linux 8 unterstützt den LVM Logical Volume Manager. Wenn Sie ein Red Hat Enterprise Linux 8 installieren, wird es auf LVM installiert, das während der Installation automatisch erstellt wird.



Der Screenshot zeigt Ihnen eine saubere Installation des RHEL 8-Systems mit zwei logischen Volumes in der RHEL 8-Webkonsole, die während der Installation automatisch erstellt wurden.

Um mehr über logische Volumes zu erfahren, folgen Sie den Abschnitten, die beschreiben:

- Was ist der Logical Volume Manager und wann sollte man ihn verwenden.
- Was sind Volume-Gruppen und wie erstellt man sie.
- Was sind logische Volumes und wie erstellt man sie.
- Wie Sie logische Volumes formatieren.
- So ändern Sie die Größe von logischen Volumes.

Voraussetzungen

- Die RHEL 8 Web-Konsole wurde installiert.
  Details finden Sie unter Installieren der Web-Konsole.
- Das Paket **cockpit-storaged** ist auf Ihrem System installiert.
- Physikalische Laufwerke, RAID-Geräte oder jede andere Art von Blockgerät, von dem Sie das logische Volume erstellen können.

18.1. LOGICAL VOLUME MANAGER IN DER WEB-KONSOLE

Die RHEL 8 Web-Konsole bietet eine grafische Oberfläche zum Erstellen von LVM-Volume-Gruppen und logischen Volumes.

Volume-Gruppen bilden eine Ebene zwischen physischen und logischen Volumes. Sie ermöglichen es, physische Volumes hinzuzufügen oder zu entfernen, ohne das logische Volume selbst zu beeinflussen. Volume-Gruppen erscheinen als ein Laufwerk mit einer Kapazität, die aus den Kapazitäten aller in der Gruppe enthaltenen physischen Laufwerke besteht.

Sie können physische Laufwerke in der Web-Konsole zu Volume-Gruppen zusammenfassen.

Logische Volumes verhalten sich wie ein einzelnes physisches Laufwerk und es wird auf einer Volume-Gruppe in Ihrem System aufgebaut.

Die wichtigsten Vorteile von logischen Volumes sind:

- Bessere Flexibilität als das auf Ihrem physischen Laufwerk verwendete Partitionierungssystem.
- Möglichkeit, mehrere physische Laufwerke zu einem Volume zu verbinden.
- Möglichkeit, die Kapazität des Volumens online zu erweitern (wachsen) oder zu reduzieren (schrumpfen), ohne Neustart.
- Fähigkeit, Schnappschüsse zu erstellen.

Zusätzliche Ressourcen

- Details finden Sie unter Konfigurieren und Verwalten von logischen Volumes .

18.2. ERSTELLEN VON VOLUME-GRUPPEN IN DER WEB-KONSOLE

Erstellen Sie Volume-Gruppen aus einem oder mehreren physischen Laufwerken oder anderen Speichergeräten.

Logische Volumes werden aus Volume-Gruppen erstellt. Jede Volume-Gruppe kann mehrere logische Volumes enthalten.

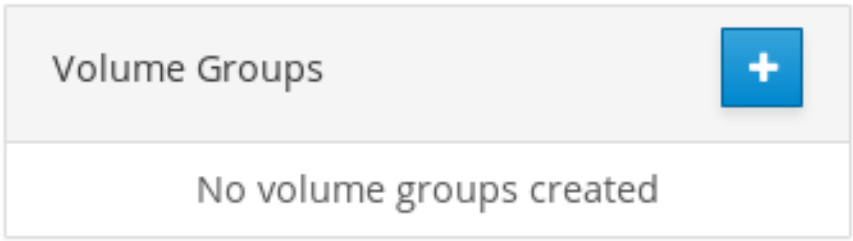
Details finden Sie unter Volume-Gruppen.

Voraussetzungen

- Physische Laufwerke oder andere Arten von Speichergeräten, von denen Sie Volume-Gruppen erstellen möchten.

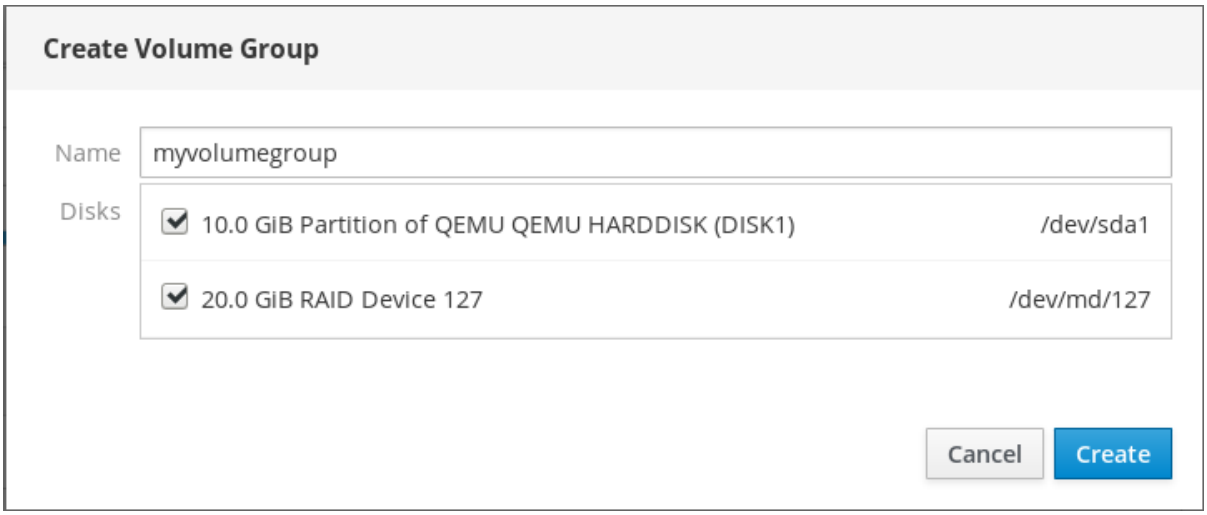
Verfahren

1. Melden Sie sich an der RHEL 8 Web-Konsole an.
2. Klicken Sie auf **Storage**.
3. Klicken Sie auf das Symbol im Feld **Volume Groups**.



4. Geben Sie im Feld **Name** einen Namen einer Gruppe ohne Leerzeichen ein.

5. Wählen Sie die Laufwerke aus, die Sie kombinieren möchten, um die Volume-Gruppe zu erstellen.

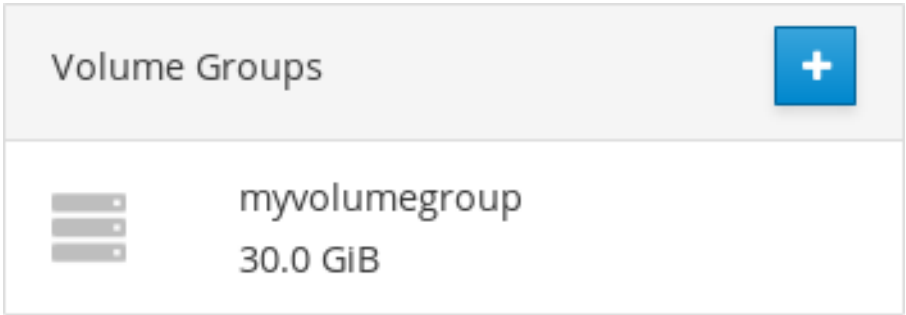


   Es kann vorkommen, dass Sie Geräte nicht wie erwartet sehen können. Die RHEL-Webkonsole zeigt nur unbenutzte Blockgeräte an. Benutzte Geräte bedeutet z. B.:

   - Geräte, die mit einem Dateisystem formatiert sind
   - Physische Volumes in einer anderen Volume-Gruppe
   - Physische Volumes, die Mitglied eines anderen Software-RAID-Geräts sind
     Wenn Sie das Gerät nicht sehen, formatieren Sie es so, dass es leer und unbenutzt ist.

6. Klicken Sie auf **Create**.

Die Web-Konsole fügt die Volume-Gruppe im Bereich **Volume Groups** hinzu. Nachdem Sie auf die Gruppe geklickt haben, können Sie logische Volumes erstellen, die von dieser Volume-Gruppe zugewiesen werden.



18.3. ERSTELLEN VON LOGISCHEN VOLUMES IN DER WEB-KONSOLE

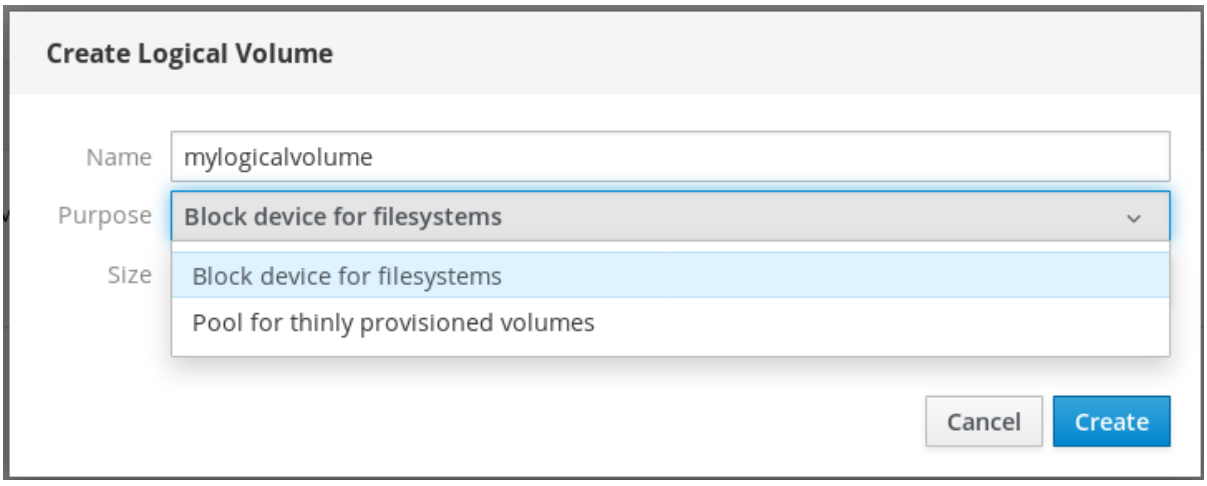
Erstellen Sie logische LVM-Volumes.

Voraussetzungen

- Das Paket **cockpit-storaged** ist auf Ihrem System installiert.
- Volume-Gruppe erstellt. Details finden Sie unter Erstellen von Volume-Gruppen in der Web-Konsole.

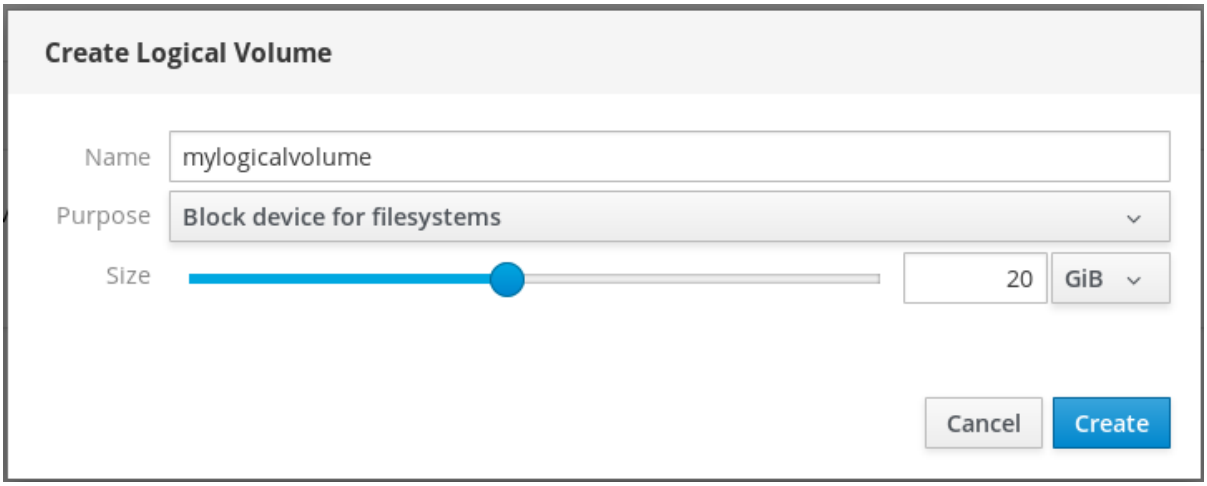
Verfahren

1. Melden Sie sich an der RHEL 8 Web-Konsole an.
2. Klicken Sie auf **Storage**.
3. Klicken Sie auf die Volume-Gruppe, in der Sie logische Volumes erstellen möchten.
4. Klicken Sie auf **Create new Logical Volume**
5. Geben Sie in das Feld **Name** einen Namen für das neue logische Volume ohne Leerzeichen ein.
6. Wählen Sie im Dropdown-Menü **Purpose** die Option **Block device for filesystems**.
   Mit dieser Konfiguration können Sie ein logisches Volume mit der maximalen Volume-Größe erstellen, die der Summe der Kapazitäten aller in der Volume-Gruppe enthaltenen Laufwerke entspricht.



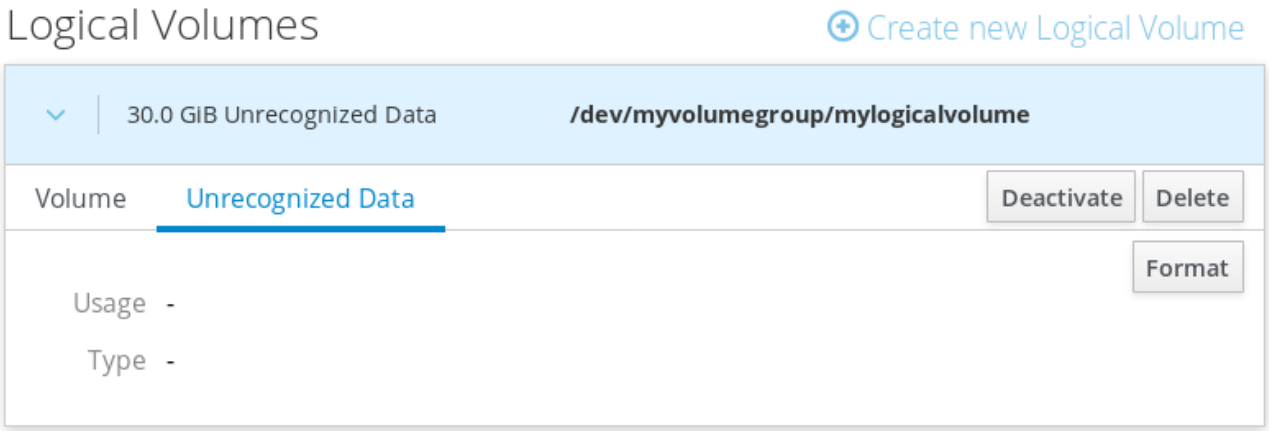
7. Definieren Sie die Größe des logischen Volumes. Berücksichtigen Sie:
   - Wie viel Platz das System, das dieses logische Volume verwendet, benötigt.
   - Wie viele logische Volumes Sie erstellen möchten.

   Sie müssen nicht den gesamten Platz nutzen. Falls nötig, können Sie das logische Volume später vergrößern.



8. Klicken Sie auf **Create**.

Um die Einstellungen zu überprüfen, klicken Sie auf Ihr logisches Volume und prüfen Sie die Details.



In diesem Stadium ist das logische Volume erstellt worden und Sie müssen ein Dateisystem mit dem Formatierungsprozess erstellen und einbinden.

18.4. FORMATIEREN VON LOGISCHEN VOLUMES IN DER WEB-KONSOLE

Logische Volumes verhalten sich wie physische Laufwerke. Um sie zu verwenden, müssen Sie sie mit einem Dateisystem formatieren.

WARNUNG

Beim Formatieren von logischen Volumes werden alle Daten auf dem Volume gelöscht.

Das von Ihnen gewählte Dateisystem bestimmt die Konfigurationsparameter, die Sie für logische Volumes verwenden können. Das XFS-Dateisystem unterstützt z. B. das Verkleinern von Volumes nicht. Details finden Sie unter Größenänderung von logischen Volumes in der Web-Konsole .

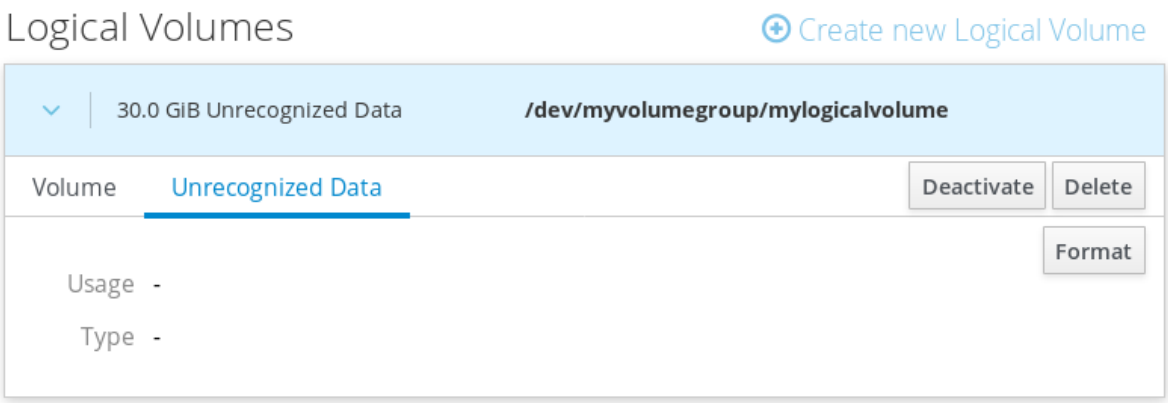
Die folgenden Schritte beschreiben die Vorgehensweise zum Formatieren von logischen Volumes.

Voraussetzungen

- Das Paket **cockpit-storaged** ist auf Ihrem System installiert.
- Logisches Volume erstellt. Details finden Sie unter Erstellen von Volume-Gruppen in der Web-Konsole.

Verfahren

1. Melden Sie sich an der RHEL-Webkonsole an.
2. Klicken Sie auf **Storage**.
3. Klicken Sie auf die Volume-Gruppe, in der sich das logische Volume befindet.
4. Klicken Sie auf das logische Volume.
5. Klicken Sie auf die Registerkarte **Unrecognized Data**.



6. Klicken Sie auf **Format**.
7. Wählen Sie im Dropdown-Menü **Erase**:
   - **Don't overwrite existing data** – die RHEL-Webkonsole schreibt nur den Festplatten-Header neu. Der Vorteil dieser Option ist die Geschwindigkeit der Formatierung.
   - **Overwrite existing data with zeros** – die RHEL-Webkonsole schreibt die gesamte Festplatte mit Nullen neu. Diese Option ist langsamer, weil das Programm die gesamte Festplatte durchgehen muss. Verwenden Sie diese Option, wenn die Festplatte Daten enthält und Sie diese überschreiben müssen.
8. Wählen Sie im Dropdown-Menü **Type** ein Dateisystem aus:
   - **XFS** Dateisystem unterstützt große logische Volumes, das Umschalten physischer Laufwerke online ohne Ausfall und das Erweitern eines vorhandenen Dateisystems. Lassen Sie dieses Dateisystem ausgewählt, wenn Sie keine andere starke Präferenz haben. XFS unterstützt nicht die Verkleinerung eines Volumes, das mit einem XFS-Dateisystem formatiert ist
   - **ext4** Dateisystem unterstützt:
     - Logische Datenträger

- Physikalische Laufwerke online schalten ohne Ausfall
- Wachsen eines Dateisystems
- Verkleinern eines Dateisystems

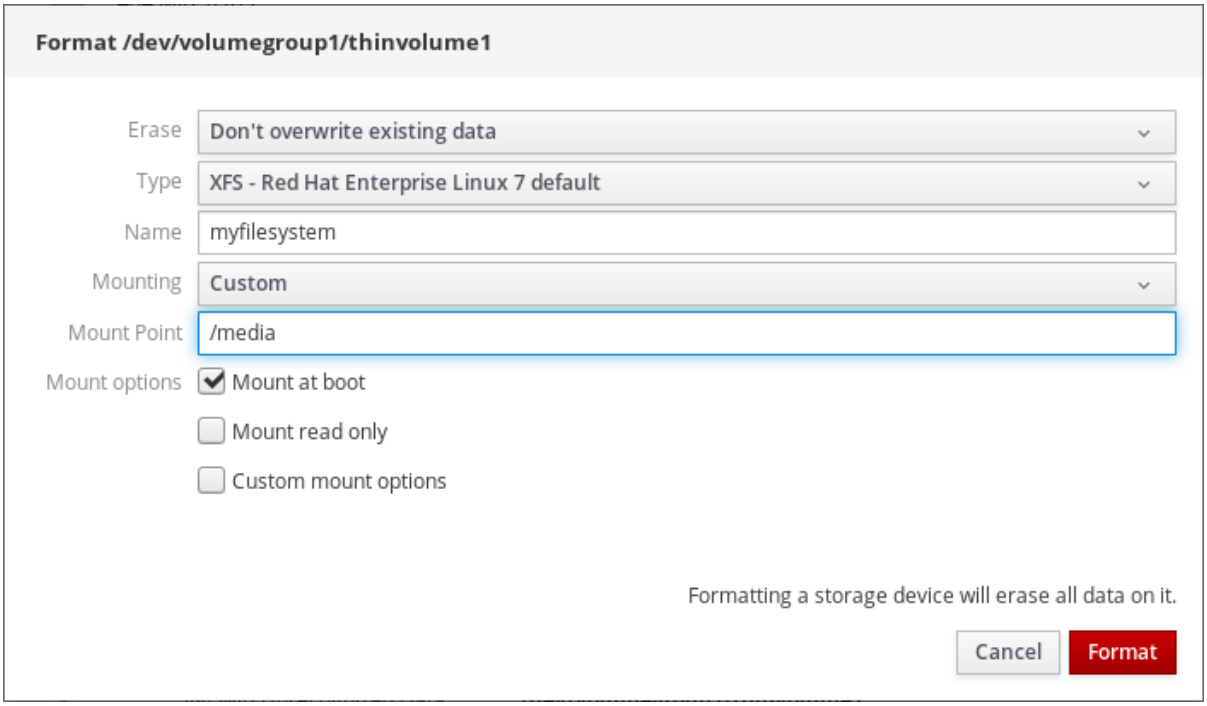
Sie können auch eine Version mit der LUKS-Verschlüsselung (Linux Unified Key Setup) wählen, die es Ihnen erlaubt, das Volume mit einer Passphrase zu verschlüsseln.

9. Geben Sie in das Feld **Name** den Namen des logischen Volumes ein.

10. Wählen Sie im Dropdown-Menü **Mounting** die Option **Custom**.
Die Option **Default** stellt nicht sicher, dass das Dateisystem beim nächsten Booten eingehängt wird.

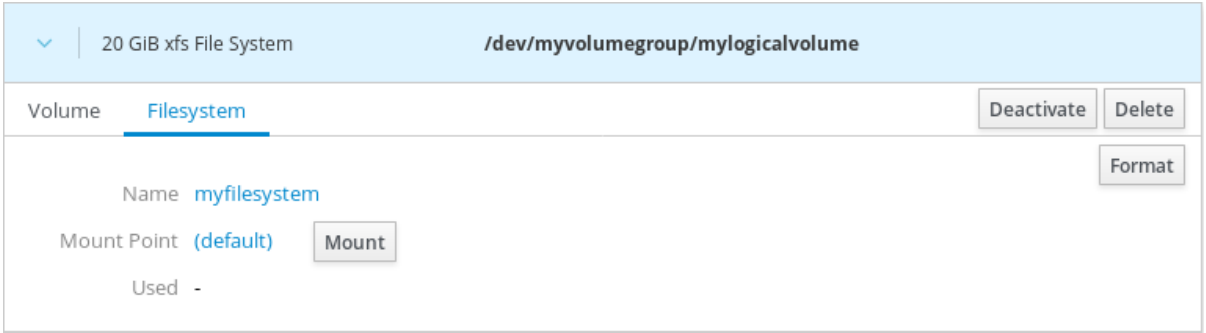
11. Fügen Sie im Feld **Mount Point** den Einhängepfad hinzu.

12. Wählen Sie **Mount at boot**.



13. Klicken Sie auf **Format**.
Die Formatierung kann einige Minuten dauern, je nachdem, wie groß das Volume ist und welche Formatierungsoptionen gewählt wurden.

Nachdem die Formatierung erfolgreich abgeschlossen wurde, können Sie die Details des formatierten logischen Volumes auf der Registerkarte **Filesystem** sehen.



14. Um das logische Volume zu verwenden, klicken Sie auf **Mount**.

Zu diesem Zeitpunkt kann das System ein montiertes und formatiertes logisches Volume verwenden.

18.5. GRÖSSENÄNDERUNG VON LOGISCHEN VOLUMES IN DER WEB-KONSOLE

Erfahren Sie, wie Sie logische Volumes in der RHEL 8 Web-Konsole erweitern oder reduzieren können.

Ob Sie die Größe eines logischen Volumes ändern können, hängt davon ab, welches Dateisystem Sie verwenden. Die meisten Dateisysteme ermöglichen es Ihnen, das Volume online (ohne Ausfall) zu erweitern (zu wachsen).

Sie können auch die Größe von logischen Volumes reduzieren (schrumpfen), wenn das logische Volume ein Dateisystem enthält, das das Schrumpfen unterstützt. Dies sollte z. B. bei den Dateisystemen ext3/ext4 vorhanden sein.

WARNUNG

Sie können keine Volumes reduzieren, die ein GFS2- oder XFS-Dateisystem enthalten.

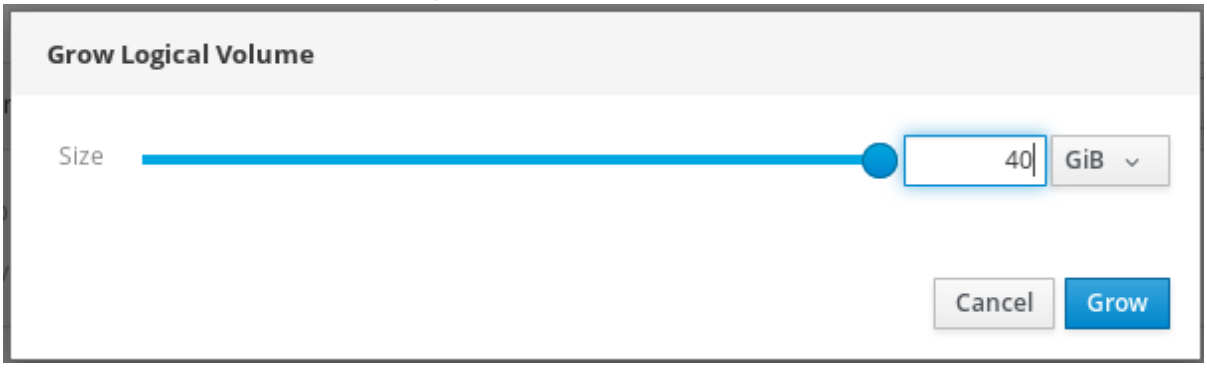
Voraussetzungen

- Vorhandenes logisches Volume, das ein Dateisystem enthält, das die Größenänderung logischer Volumes unterstützt.

Verfahren

Die folgenden Schritte beschreiben die Vorgehensweise zum Erweitern eines logischen Volumes, ohne das Volume offline zu nehmen:

1. Melden Sie sich an der RHEL-Webkonsole an.
2. Klicken Sie auf **Storage**.
3. Klicken Sie auf die Volume-Gruppe, in der sich das logische Volume befindet.
4. Klicken Sie auf das logische Volume.
5. Klicken Sie auf der Registerkarte **Volume** auf **Grow**.
6. Stellen Sie im Dialogfeld **Grow Logical Volume** den Lautstärkeabstand ein.



7. Klicken Sie auf **Grow**.

LVM vergrößert das logische Volume ohne Systemausfälle.

18.6. ZUSÄTZLICHE RESSOURCEN

- Weitere Details zum Erstellen von logischen Volumes finden Sie unter Konfigurieren und Verwalten von logischen Volumes.

KAPITEL 19. VERWENDEN DER WEB-KONSOLE ZUM KONFIGURIEREN VON THIN LOGICAL VOLUMES

Thinly-Provisioned Logical Volumes ermöglichen es Ihnen, mehr Speicherplatz für bestimmte Anwendungen oder Server zuzuweisen, als tatsächlich in den Logical Volumes vorhanden ist.

Details finden Sie unter Thinly-provisionierte logische Volumes (Thin-Volumes).

Die folgenden Abschnitte beschreiben:

- Erstellen von Pools für die Thinly Provisioned Logical Volumes.
- Erstellen von dünnen logischen Volumes.
- Formatieren von dünnen logischen Volumes.

Voraussetzungen

- Die RHEL 8 Web-Konsole wurde installiert.
  Details finden Sie unter Installieren der Web-Konsole.
- Das Paket **cockpit-storaged** ist auf Ihrem System installiert.
- Physische Laufwerke oder andere Arten von Speichergeräten, von denen Sie Volume-Gruppen erstellen möchten.

19.1. ERSTELLEN VON POOLS FÜR DÜNNE LOGISCHE VOLUMES IN DER WEB-KONSOLE

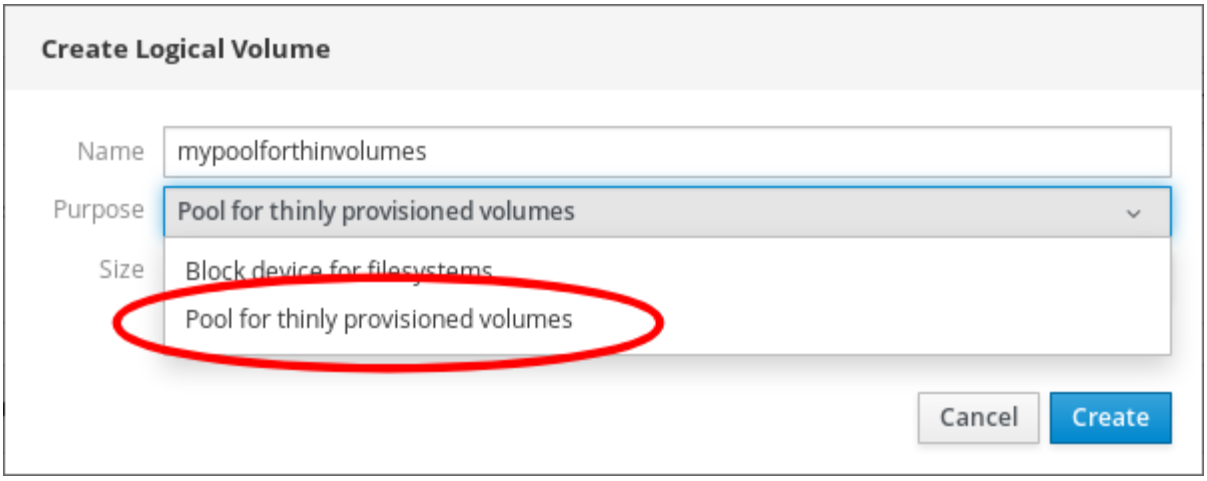
Erstellen Sie einen Pool für Thinly-Provisioned-Volumes.

Voraussetzungen

- Volume-Gruppe erstellt.

Verfahren

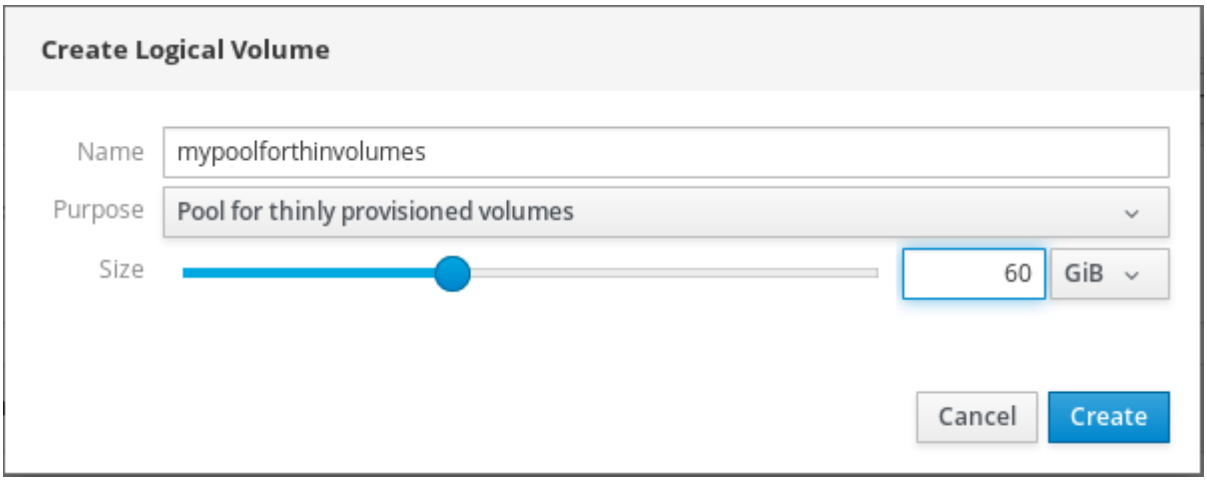
1. Melden Sie sich an der RHEL 8 Web-Konsole an.
2. Klicken Sie auf **Storage**.
3. Klicken Sie auf die Volume-Gruppe, in der Sie Thin-Volumes erstellen möchten.
4. Klicken Sie auf **Create new Logical Volume**
5. Geben Sie in das Feld **Name** einen Namen für den neuen Pool von Thin-Volumes ohne Leerzeichen ein.
6. Wählen Sie im Dropdown-Menü **Purpose** die Option **Pool for thinly provisioned volumes** Mit dieser Konfiguration können Sie das Thin-Volume erstellen.



7. Definieren Sie die Größe des Pools von Thin-Volumes. Berücksichtigen Sie:

   - Wie viele Thin-Volumes werden Sie in diesem Pool benötigen?
   - Was ist die erwartete Größe der einzelnen Thin-Volumes?

   Sie müssen nicht den gesamten Platz nutzen. Wenn nötig, können Sie den Pool später vergrößern.



8. Klicken Sie auf **Create**.
   Der Pool für Thin-Volumes wurde erstellt und Sie können Thin-Volumes hinzufügen.

19.2. ERSTELLEN VON THIN LOGICAL VOLUMES IN DER WEB-KONSOLE

Erstellen Sie ein logisches Thin-Volume im Pool. Der Pool kann mehrere Thin-Volumes enthalten und jedes Thin-Volume kann so groß sein wie der Pool für Thin-Volumes selbst.

WICHTIG

Die Verwendung von Thin-Volumes erfordert eine regelmäßige Überprüfung des tatsächlich freien physischen Speicherplatzes des logischen Volumes.

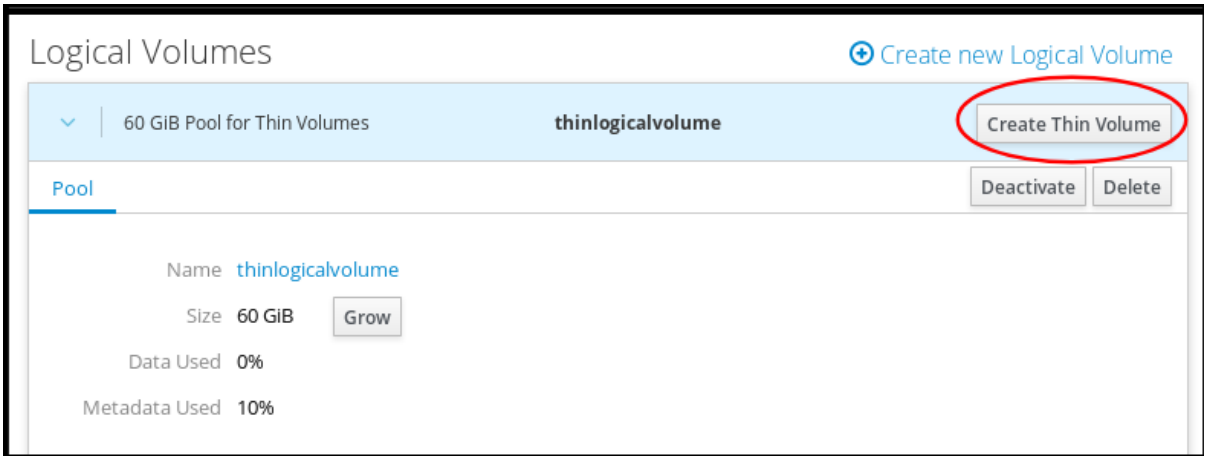
Voraussetzungen

- Pool für Thin-Volumes erstellt.

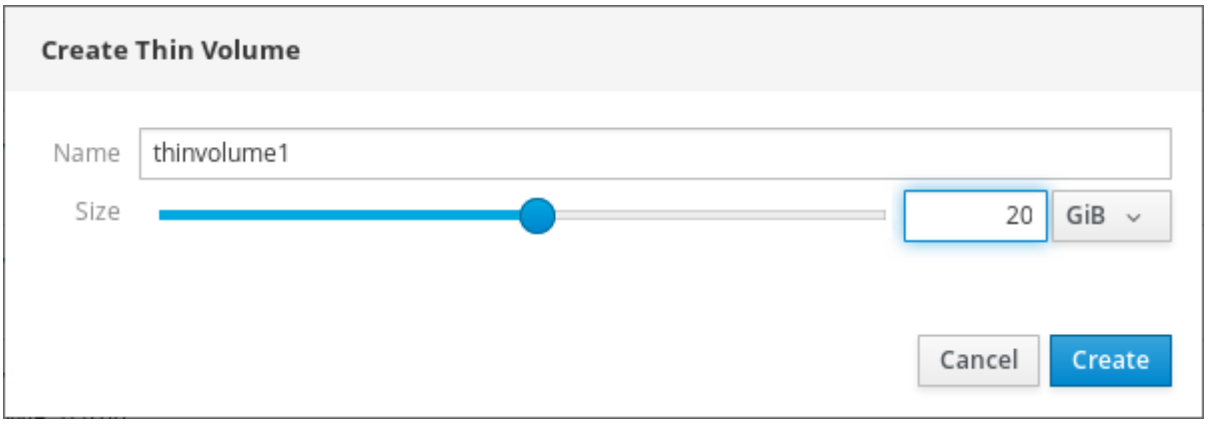
Für Details siehe Abschnitt 19.1, »Erstellen von Pools für dünne logische Volumes in der Web-Konsole«.

Verfahren

1. Melden Sie sich an der RHEL 8 Web-Konsole an.
2. Klicken Sie auf **Storage**.
3. Klicken Sie auf die Volume-Gruppe, in der Sie Thin-Volumes erstellen möchten.
4. Klicken Sie auf den gewünschten Pool.
5. Klicken Sie auf **Create Thin Volume**.



6. Geben Sie im Dialogfeld **Create Thin Volume** einen Namen für das Thin-Volume ohne Leerzeichen ein.
7. Definieren Sie die Größe des dünnen Volumens.



8. Klicken Sie auf **Create**.

In diesem Stadium ist das logische Thin-Volume erstellt worden und Sie müssen es formatieren.

19.3. FORMATIEREN VON LOGISCHEN VOLUMES IN DER WEB-KONSOLE

Logische Volumes verhalten sich wie physische Laufwerke. Um sie zu verwenden, müssen Sie sie mit einem Dateisystem formatieren.

WARNUNG

Beim Formatieren von logischen Volumes werden alle Daten auf dem Volume gelöscht.

Das von Ihnen gewählte Dateisystem bestimmt die Konfigurationsparameter, die Sie für logische Volumes verwenden können. Das XFS-Dateisystem unterstützt z. B. das Verkleinern von Volumes nicht. Details finden Sie unter Größenänderung von logischen Volumes in der Web-Konsole .

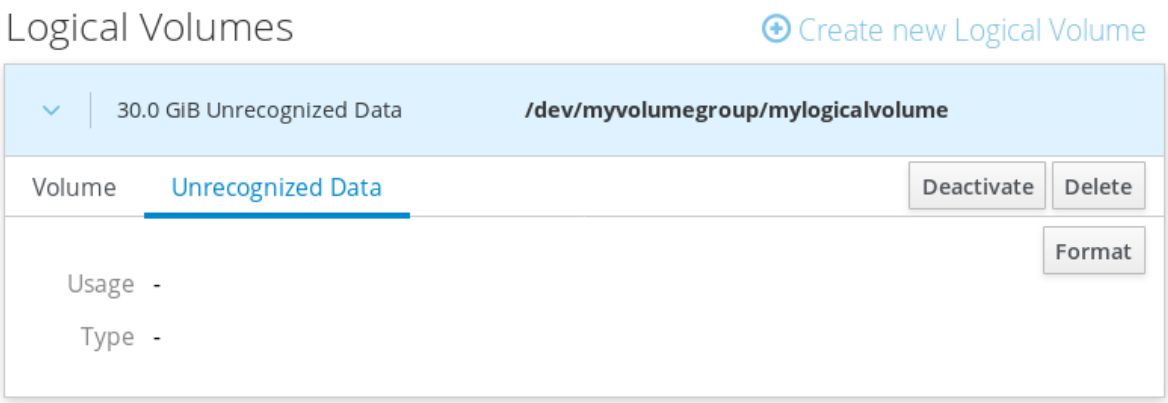
Die folgenden Schritte beschreiben die Vorgehensweise zum Formatieren von logischen Volumes.

Voraussetzungen

- Das Paket **cockpit-storaged** ist auf Ihrem System installiert.
- Logisches Volume erstellt. Details finden Sie unter Erstellen von Volume-Gruppen in der Web-Konsole.

Verfahren

1. Melden Sie sich an der RHEL-Webkonsole an.
2. Klicken Sie auf **Storage**.
3. Klicken Sie auf die Volume-Gruppe, in der sich das logische Volume befindet.
4. Klicken Sie auf das logische Volume.
5. Klicken Sie auf die Registerkarte **Unrecognized Data**.



6. Klicken Sie auf **Format**.
7. Wählen Sie im Dropdown-Menü **Erase**:
   - **Don't overwrite existing data**- die RHEL-Webkonsole schreibt nur den Festplatten-Header neu. Der Vorteil dieser Option ist die Geschwindigkeit der Formatierung.
   - **Overwrite existing data with zeros**- die RHEL-Webkonsole schreibt die gesamte Festplatte mit Nullen neu. Diese Option ist langsamer, weil das Programm die gesamte

Festplatte durchgehen muss. Verwenden Sie diese Option, wenn die Festplatte Daten enthält und Sie diese überschreiben müssen.

8. Wählen Sie im Dropdown-Menü **Type** ein Dateisystem aus:

   - **XFS** Dateisystem unterstützt große logische Volumes, das Umschalten physischer Laufwerke online ohne Ausfall und das Erweitern eines vorhandenen Dateisystems. Lassen Sie dieses Dateisystem ausgewählt, wenn Sie keine andere starke Präferenz haben.
     XFS unterstützt nicht die Verkleinerung eines Volumes, das mit einem XFS-Dateisystem formatiert ist

   - **ext4** Dateisystem unterstützt:

     - Logische Datenträger
     - Physikalische Laufwerke online schalten ohne Ausfall
     - Wachsen eines Dateisystems
     - Verkleinern eines Dateisystems

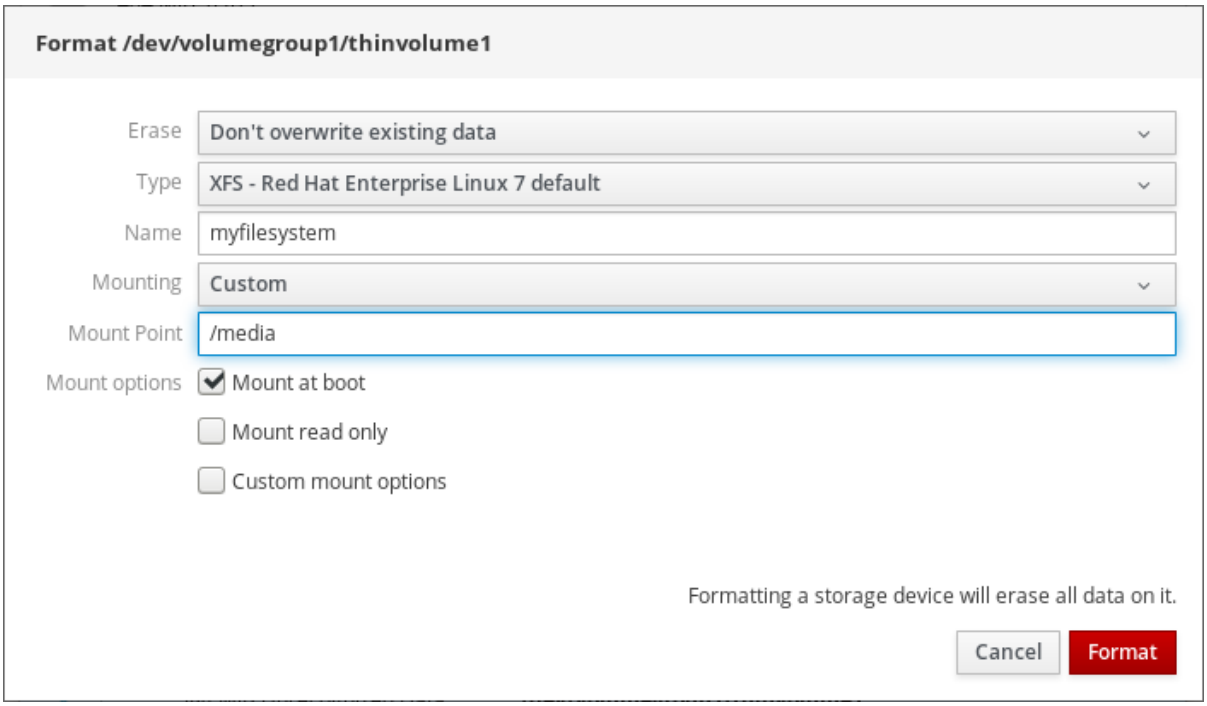
   Sie können auch eine Version mit der LUKS-Verschlüsselung (Linux Unified Key Setup) wählen, die es Ihnen erlaubt, das Volume mit einer Passphrase zu verschlüsseln.

9. Geben Sie in das Feld **Name** den Namen des logischen Volumes ein.

10. Wählen Sie im Dropdown-Menü **Mounting** die Option **Custom**.
    Die Option **Default** stellt nicht sicher, dass das Dateisystem beim nächsten Booten eingehängt wird.

11. Fügen Sie im Feld **Mount Point** den Einhängepfad hinzu.

12. Wählen Sie **Mount at boot**.



13. Klicken Sie auf **Format**.
    Die Formatierung kann einige Minuten dauern, je nachdem, wie groß das Volume ist und welche Formatierungsoptionen gewählt wurden.

Nachdem die Formatierung erfolgreich abgeschlossen wurde, können Sie die Details des formatierten logischen Volumes auf der Registerkarte **Filesystem** sehen.

14. Um das logische Volume zu verwenden, klicken Sie auf **Mount**.

Zu diesem Zeitpunkt kann das System ein montiertes und formatiertes logisches Volume verwenden.

KAPITEL 20. VERWENDEN DER WEB-KONSOLE ZUM ÄNDERN PHYSISCHER LAUFWERKE IN VOLUME-GRUPPEN

Ändern Sie das Laufwerk in einer Volume-Gruppe mit der RHEL 8-Webkonsole.

Der Wechsel der physikalischen Laufwerke besteht aus den folgenden Vorgängen:

- Hinzufügen von physischen Laufwerken aus logischen Volumes.
- Entfernen von physischen Laufwerken aus logischen Volumes.

Voraussetzungen

- Die RHEL 8 Web-Konsole wurde installiert.
  Details finden Sie unter Installieren der Web-Konsole.
- Das Paket **cockpit-storaged** ist auf Ihrem System installiert.
- Ein neues physisches Laufwerk zum Ersetzen des alten oder defekten Laufwerks.
- Die Konfiguration erwartet, dass physische Laufwerke in einer Volume-Gruppe organisiert sind.

20.1. HINZUFÜGEN VON PHYSISCHEN LAUFWERKEN ZU VOLUME-GRUPPEN IN DER WEB-KONSOLE

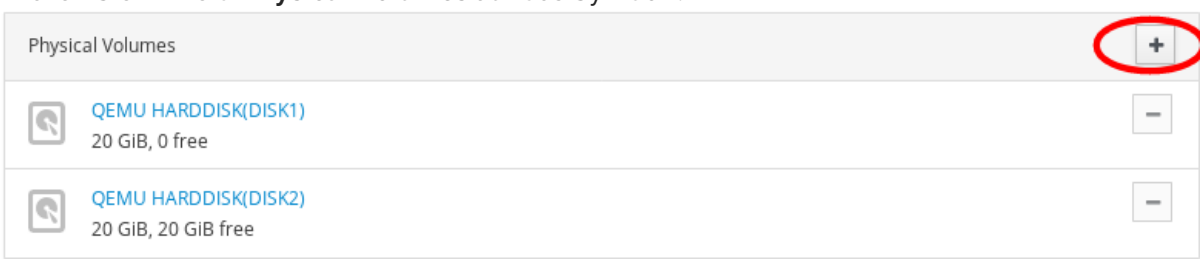
Die RHEL 8 Web-Konsole ermöglicht es Ihnen, ein neues physisches Laufwerk oder einen anderen Volume-Typ zu einem bestehenden logischen Volume hinzuzufügen.

Voraussetzungen

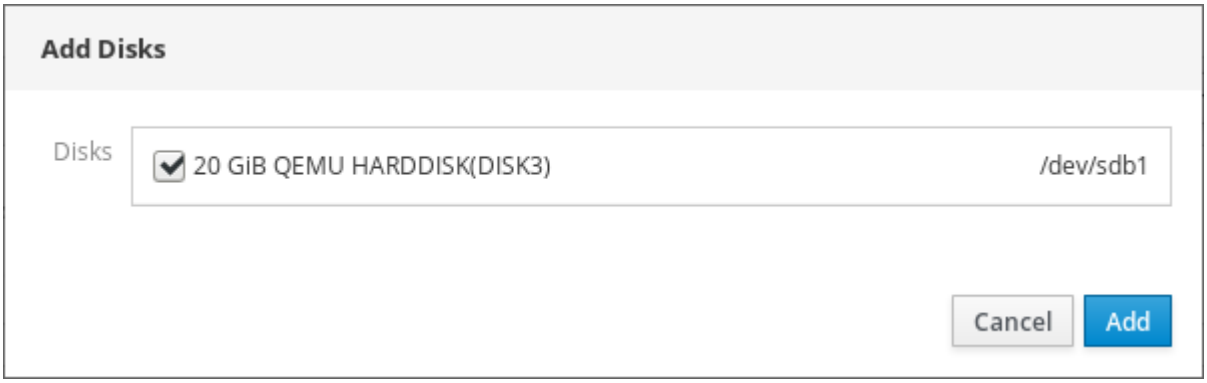
- Es muss eine Volume-Gruppe erstellt werden.
- Ein neues Laufwerk ist an das Gerät angeschlossen.

Verfahren

1. Melden Sie sich an der RHEL 8 Web-Konsole an.
2. Klicken Sie auf **Storage**.
3. Klicken Sie im Feld **Volume Groups** auf die Volume-Gruppe, in der Sie ein physisches Volume hinzufügen möchten.
4. Klicken Sie im Feld **Physical Volumes** auf das Symbol .



5. Wählen Sie im Dialogfeld **Add Disks** das gewünschte Laufwerk und klicken Sie auf **Add**.



Als Ergebnis fügt die RHEL 8-Webkonsole das physische Volume hinzu. Sie können es im Abschnitt **Physical Volumes** sehen, und das logische Volume kann sofort beginnen, auf das Laufwerk zu schreiben.

20.2. ENTFERNEN VON PHYSISCHEN LAUFWERKEN AUS VOLUME-GRUPPEN IN DER WEB-KONSOLE

Wenn ein logisches Volume mehrere physische Laufwerke enthält, können Sie eines der physischen Laufwerke online entfernen.

Das System verschiebt während des Entfernungsvorgangs automatisch alle Daten von dem zu entfernenden Laufwerk auf andere Laufwerke. Beachten Sie, dass dies einige Zeit dauern kann.

Die Web-Konsole prüft auch, ob genügend Platz zum Entfernen des physischen Laufwerks vorhanden ist.

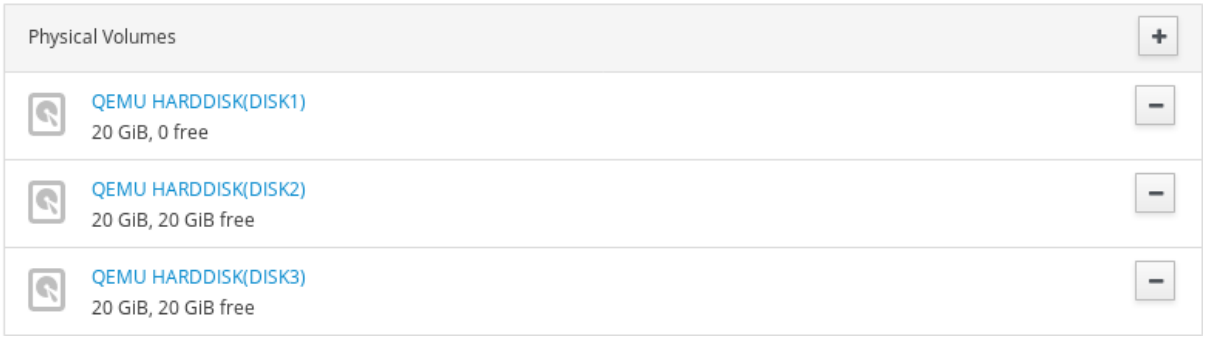
Voraussetzungen

- Eine Volume-Gruppe mit mehr als einem angeschlossenen physischen Laufwerk.

Verfahren

Die folgenden Schritte beschreiben, wie Sie ein Laufwerk aus der Volume-Gruppe entfernen, ohne einen Ausfall in der RHEL-Webkonsole zu verursachen.

1. Melden Sie sich an der RHEL 8 Web-Konsole an.
2. Klicken Sie auf **Storage**.
3. Klicken Sie auf die Volume-Gruppe, in der Sie das logische Volume haben.
4. Suchen Sie im Bereich **Physical Volumes** das gewünschte Volume.
5. Klicken Sie auf das Symbol **-**.
   Die RHEL 8 Web-Konsole prüft, ob das logische Volume genügend freien Platz zum Entfernen der Platte hat. Wenn nicht, können Sie das Laufwerk nicht entfernen und es ist notwendig, zuerst ein anderes Laufwerk hinzuzufügen. Details finden Sie unter Hinzufügen von physischen Laufwerken zu logischen Volumes in der Webkonsole.



Als Ergebnis entfernt die RHEL 8 Web-Konsole das physische Volume aus dem erstellten logischen Volume, ohne einen Ausfall zu verursachen.

KAPITEL 21. VERWENDEN DER WEB-KONSOLE ZUR VERWALTUNG VON VIRTUAL DATA OPTIMIZER-VOLUMES

Konfigurieren Sie den Virtual Data Optimizer (VDO) über die RHEL 8-Webkonsole.

Sie werden lernen, wie man:

- VDO-Volumes erstellen
- VDO-Volumen formatieren
- VDO-Volumen verlängern

Voraussetzungen

- Die RHEL 8 Web-Konsole ist installiert und zugänglich.
  Details finden Sie unter Installieren der Web-Konsole.
- Das Paket **cockpit-storaged** ist auf Ihrem System installiert.

21.1. VDO-VOLUMES IN DER WEB-KONSOLE

Red Hat Enterprise Linux 8 unterstützt Virtual Data Optimizer (VDO).

VDO ist eine Blockvirtualisierungstechnologie, die kombiniert:

Komprimierung
Details finden Sie unter Aktivieren oder Deaktivieren der Komprimierung in VDO .

Deduplizierung
Details finden Sie unter Aktivieren oder Deaktivieren der Deduplizierung in VDO .

Thin Provisioning
Details finden Sie unter Thinly-provisionierte logische Volumes (Thin-Volumes).

Mit diesen Technologien kann VDO:

- Spart Speicherplatz in der Leitung
- Komprimiert Dateien
- Eliminiert Duplikate
- Ermöglicht es Ihnen, mehr virtuellen Speicherplatz zuzuweisen, als der physische oder logische Speicher zur Verfügung stellt
- Ermöglicht es Ihnen, den virtuellen Speicher zu erweitern, indem Sie den

VDO kann auf vielen Speichertypen erstellt werden. In der Web-Konsole von RHEL 8 können Sie VDO auf einem Speicher konfigurieren:

- LVM

ANMERKUNG

Es ist nicht möglich, VDO auf einem Thin-Provisioned-Volume zu konfigurieren.

- Physikalisches Volumen
- Software-RAID

Details zur Platzierung von VDO im Speicherstapel finden Sie unter Systemanforderungen.

Zusätzliche Ressourcen

- Details zu VDO finden Sie unter Deduplizieren und Komprimieren von Speicher .

21.2. ERSTELLEN VON VDO-VOLUMES IN DER WEB-KONSOLE

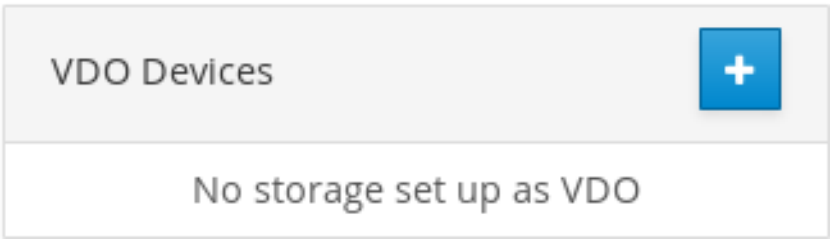
Erstellen Sie ein VDO-Volume in der RHEL-Webkonsole.

Voraussetzungen

- Physikalische Laufwerke, LVMs oder RAID, von denen Sie VDO erstellen möchten.

Verfahren

1. Melden Sie sich an der RHEL 8 Web-Konsole an.
   Details finden Sie unter Anmeldung an der Web-Konsole.
2. Klicken Sie auf **Storage**.
3. Klicken Sie auf das Symbol im Feld **VDO Devices**.



4. Geben Sie im Feld **Name** einen Namen eines VDO-Volumes ohne Leerzeichen ein.
5. Wählen Sie das Laufwerk, das Sie verwenden möchten.
6. Stellen Sie in der Leiste **Logical Size** die Größe des VDO-Volumes ein. Sie können es um mehr als das Zehnfache erweitern, aber überlegen Sie, für welchen Zweck Sie das VDO-Volume erstellen:
   - Verwenden Sie für aktive VMs oder Container-Speicher eine logische Größe, die dem Zehnfachen der physischen Größe des Volumes entspricht.
   - Verwenden Sie für Objektspeicher eine logische Größe, die dem Dreifachen der physischen Größe des Volumes entspricht.

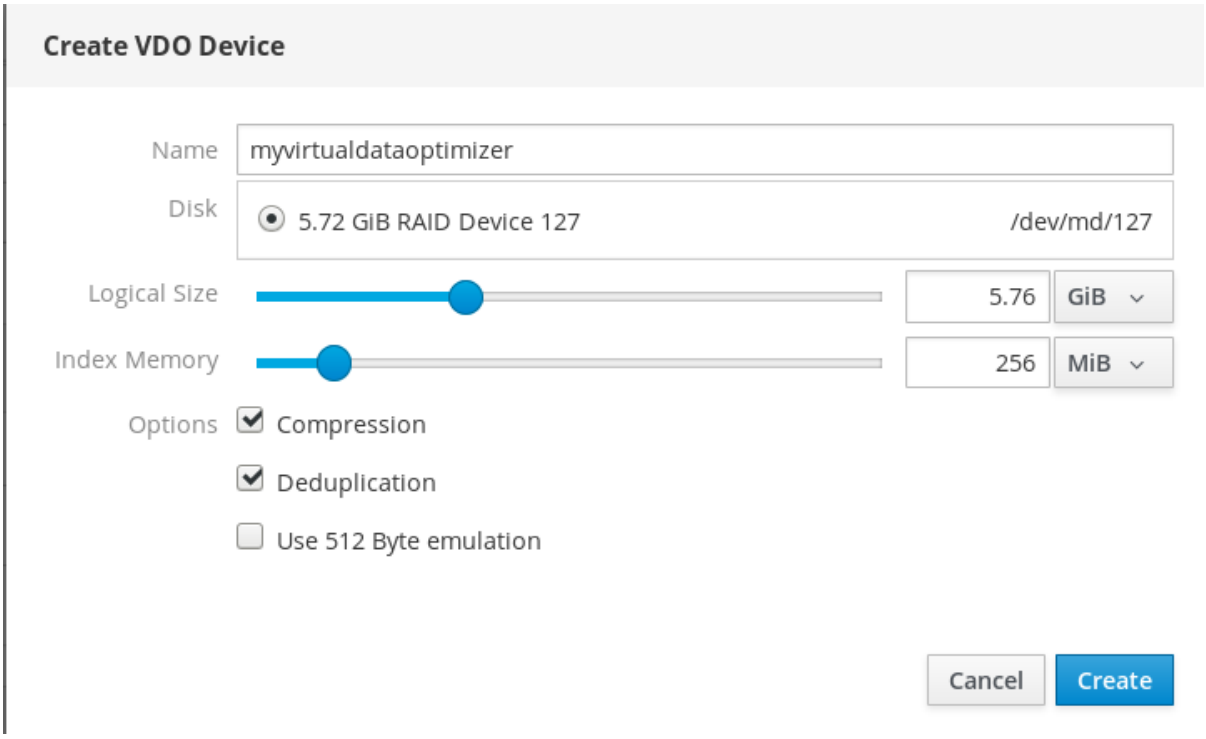
   Details finden Sie unter Einsetzen von VDO.
7. Weisen Sie in der Leiste **Index Memory** Speicherplatz für das VDO-Volumen zu.
   Details zu den VDO Systemanforderungen finden Sie unter Systemanforderungen.

8. Wählen Sie die Option **Compression**. Diese Option kann verschiedene Dateiformate effizient reduzieren.
   Details finden Sie unter Aktivieren oder Deaktivieren der Komprimierung in VDO .

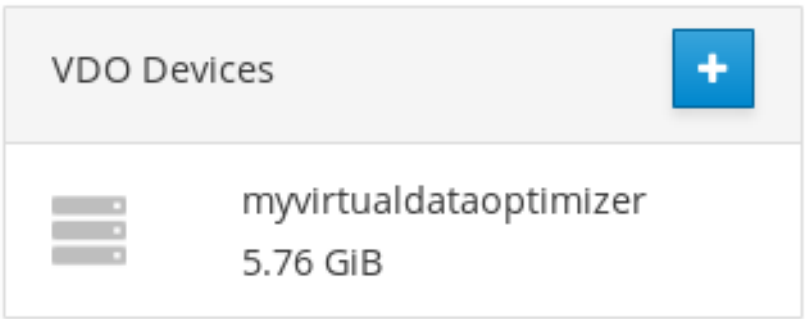
9. Wählen Sie die Option **Deduplication**.
   Diese Option reduziert den Verbrauch von Speicherressourcen, indem mehrere Kopien von doppelten Blöcken eliminiert werden. Details finden Sie unter Aktivieren oder Deaktivieren der Deduplizierung in VDO.

10. [Optional] Wenn Sie das VDO-Volume mit Anwendungen verwenden wollen, die eine Blockgröße von 512 Byte benötigen, wählen Sie **Use 512 Byte emulation**. Dies reduziert die Leistung des VDO-Volumes, sollte aber nur sehr selten benötigt werden. Lassen Sie es im Zweifelsfall aus.

11. Klicken Sie auf **Create**.



Wenn der Prozess der Erstellung des VDO-Volumes erfolgreich war, können Sie das neue VDO-Volume im Bereich **Storage** sehen und mit einem Dateisystem formatieren.



21.3. FORMATIEREN VON VDO-VOLUMES IN DER WEB-KONSOLE

VDO-Volumes verhalten sich wie physische Laufwerke. Um sie zu verwenden, müssen Sie sie mit einem Dateisystem formatieren.

WARNUNG

Beim Formatieren von VDO werden alle Daten auf dem Datenträger gelöscht.

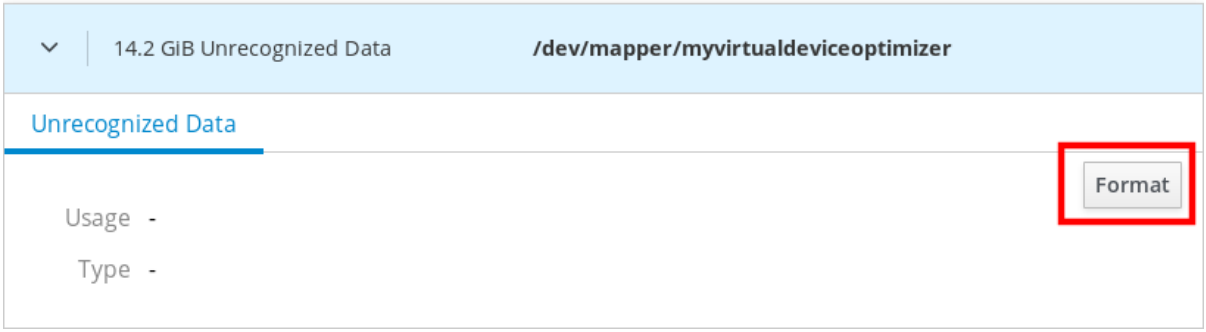
Die folgenden Schritte beschreiben die Vorgehensweise zum Formatieren von VDO-Volumes.

Voraussetzungen

- Ein VDO-Volume wird erstellt. Für Details siehe Abschnitt 21.2, »Erstellen von VDO-Volumes in der Web-Konsole«.

Verfahren

1. Melden Sie sich an der RHEL 8 Web-Konsole an.
   Details finden Sie unter Anmeldung an der Web-Konsole.
2. Klicken Sie auf **Storage**.
3. Klicken Sie auf das VDO-Volumen.
4. Klicken Sie auf die Registerkarte **Unrecognized Data**.
5. Klicken Sie auf **Format**.



6. Wählen Sie im Dropdown-Menü **Erase**:

   Don't overwrite existing data

   Die RHEL-Webkonsole schreibt nur den Festplatten-Header neu. Der Vorteil dieser Option ist die Geschwindigkeit der Formatierung.

   Overwrite existing data with zeros

   Die RHEL-Webkonsole schreibt die gesamte Festplatte mit Nullen neu. Diese Option ist langsamer, weil das Programm die gesamte Festplatte durchgehen muss. Verwenden Sie diese Option, wenn der Datenträger Daten enthält und Sie diese neu schreiben müssen.

7. Wählen Sie im Dropdown-Menü **Type** ein Dateisystem aus:

   - Das Dateisystem **XFS** unterstützt große logische Volumes, das Umschalten physischer Laufwerke online ohne Ausfall und Wachstum. Lassen Sie dieses Dateisystem ausgewählt, wenn Sie keine andere starke Präferenz haben.
     XFS unterstützt das Verkleinern von Volumes nicht. Daher können Sie mit XFS formatierte Volumes nicht verkleinern.

- Das Dateisystem **ext4** unterstützt logische Volumes, das Umschalten von physischen Laufwerken online ohne Ausfall, Wachsen und Schrumpfen.

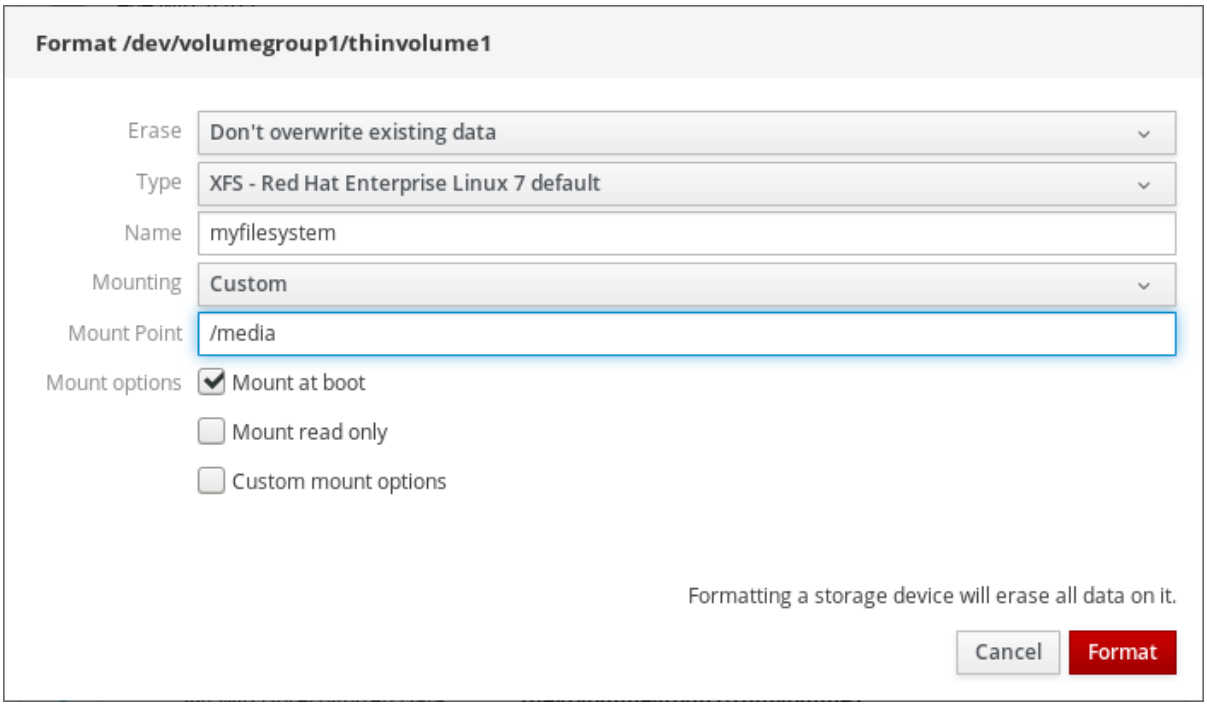
Sie können auch eine Version mit der LUKS-Verschlüsselung (Linux Unified Key Setup) wählen, die es Ihnen erlaubt, das Volume mit einer Passphrase zu verschlüsseln.

8. Geben Sie in das Feld **Name** den Namen des logischen Volumes ein.

9. Wählen Sie im Dropdown-Menü **Mounting** die Option **Custom**.
Die Option **Default** stellt nicht sicher, dass das Dateisystem beim nächsten Booten eingehängt wird.

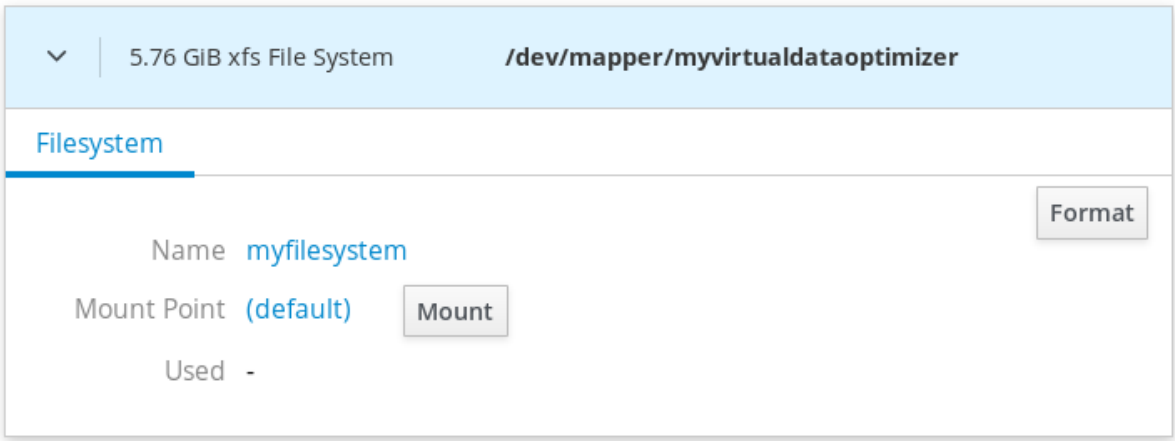
10. Fügen Sie im Feld **Mount Point** den Einhängepfad hinzu.

11. Wählen Sie **Mount at boot**.



12. Klicken Sie auf **Format**.
Die Formatierung kann je nach den verwendeten Formatierungsoptionen und der Volume-Größe mehrere Minuten dauern.

Nach erfolgreichem Abschluss können Sie die Details des formatierten VDO-Volumes auf der Registerkarte **Filesystem** sehen.



13. Um das VDO-Volumen zu verwenden, klicken Sie auf **Mount**.

An diesem Punkt verwendet das System das eingelegte und formatierte VDO-Volume.

21.4. ERWEITERN VON VDO-VOLUMES IN DER WEB-KONSOLE

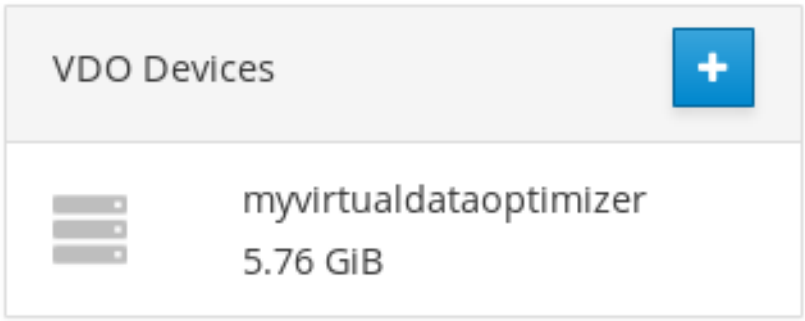
Erweitern Sie VDO-Volumes in der RHEL 8 Web-Konsole.

Voraussetzungen

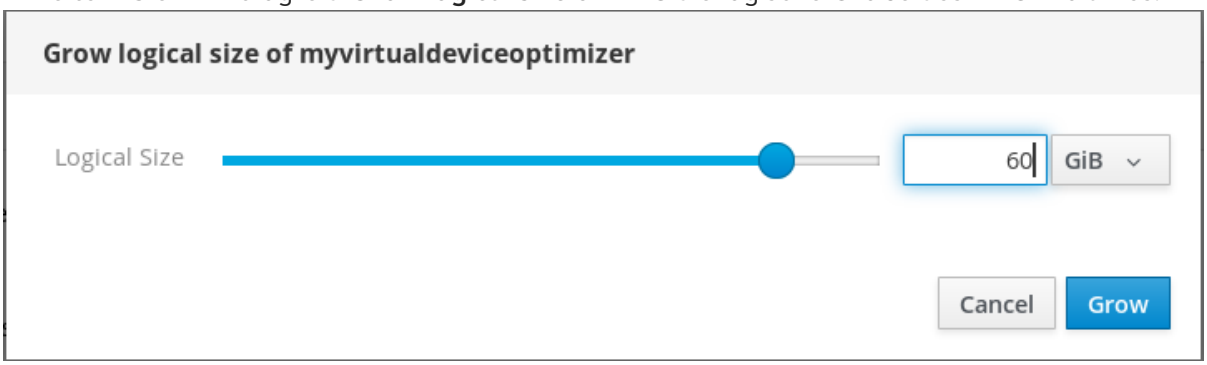
- Das Paket **cockpit-storaged** ist auf Ihrem System installiert.
- Das erstellte VDO-Volumen.

Verfahren

1. Melden Sie sich an der RHEL 8 Web-Konsole an.
   Details finden Sie unter Anmeldung an der Web-Konsole.
2. Klicken Sie auf **Storage**.
3. Klicken Sie im Feld **VDO Devices** auf Ihr VDO-Volumen.



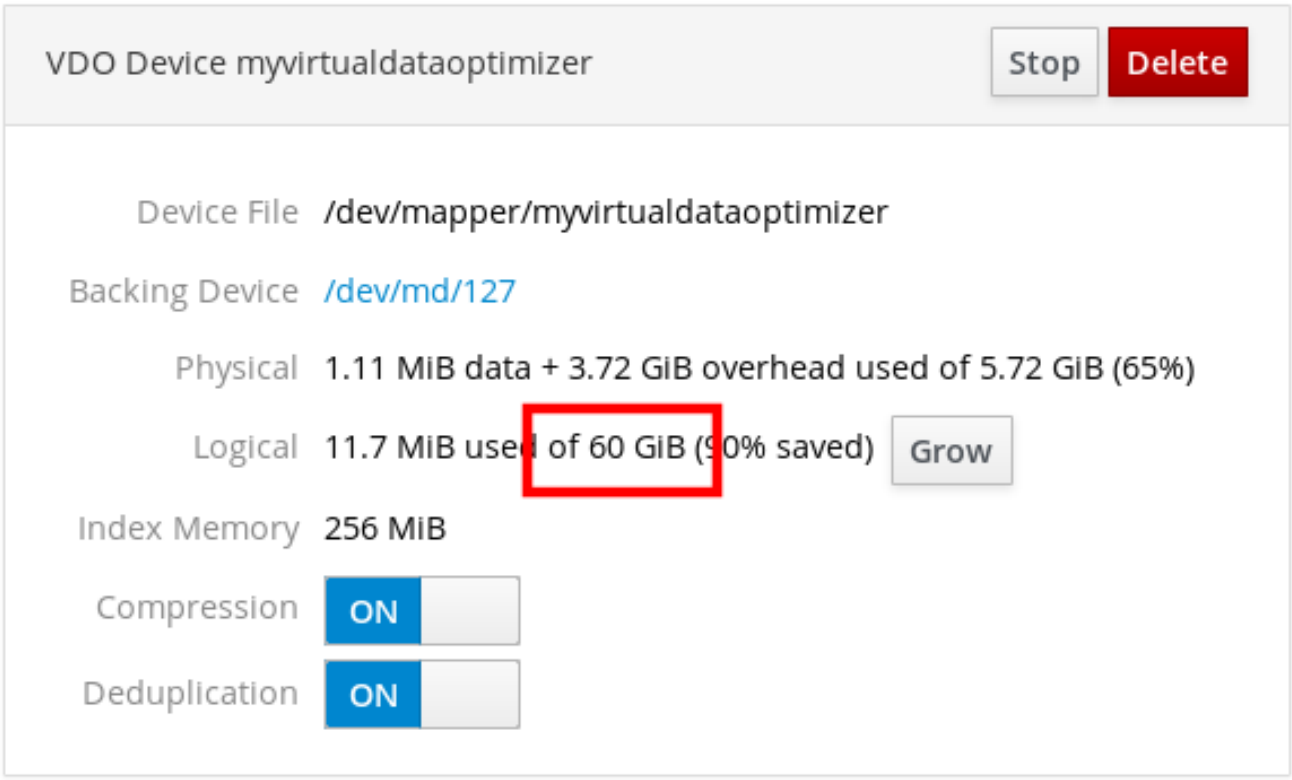
4. Klicken Sie in den VDO-Volumendetails auf die Schaltfläche **Grow**.
5. Erweitern Sie im Dialogfeld **Grow logical size of VDO** die logische Größe des VDO-Volumes.



   Die ursprüngliche Größe des logischen Volumes aus dem Screenshot war 6 GB. Wie Sie sehen, können Sie das Volume über die RHEL-Webkonsole auf mehr als die zehnfache Größe vergrößern und es funktioniert aufgrund der Komprimierung und Deduplizierung korrekt.

6. Klicken Sie auf **Grow**.

Wenn der Prozess des Vergrößerns von VDO erfolgreich war, können Sie die neue Größe in den VDO-Datenträgerdetails sehen.


VDO Device myvirtualdataoptimizer
Stop
Delete
Device File
/dev/mapper/myvirtualdataoptimizer
Backing Device
/dev/md/127
Physical
1.11 MiB data + 3.72 GiB overhead used of 5.72 GiB (65%)
Logical
11.7 MiB used of 60 GiB (80% saved)
Grow
Index Memory
256 MiB
Compression
ON
Deduplication
ON

KAPITEL 22. SPERREN VON DATEN MIT LUKS-PASSWORT IN DER RHEL-WEBKONSOLE

Auf der Registerkarte **Storage** der Web-Konsole können Sie jetzt verschlüsselte Geräte mit dem LUKS-Format (Linux Unified Key Setup) Version 2 erstellen, sperren, entsperren, die Größe ändern und anderweitig konfigurieren.

Diese neue Version von LUKS bietet:

- Flexiblere Entsperrungsrichtlinien
- Stärkere Kryptographie
- Bessere Kompatibilität mit zukünftigen Änderungen

Voraussetzungen

- Die RHEL 8 Web-Konsole wurde installiert.
  Details finden Sie unter Installieren der Web-Konsole.
- Das Paket **cockpit-storaged** ist auf Ihrem System installiert.

22.1. LUKS-FESTPLATTENVERSCHLÜSSELUNG

Das Linux Unified Key Setup-on-disk-format (LUKS) ermöglicht die Verschlüsselung von Blockgeräten und bietet eine Reihe von Tools, die die Verwaltung der verschlüsselten Geräte vereinfachen. LUKS ermöglicht es, dass mehrere Benutzerschlüssel einen Master-Schlüssel entschlüsseln, der für die Massenverschlüsselung der Partition verwendet wird.

RHEL verwendet LUKS, um die Verschlüsselung von Blockgeräten durchzuführen. Standardmäßig ist die Option zum Verschlüsseln des Blockgeräts während der Installation nicht aktiviert. Wenn Sie die Option zum Verschlüsseln des Datenträgers wählen, fordert das System Sie bei jedem Start des Computers zur Eingabe einer Passphrase auf. Diese Passphrase »schaltet« den Massenverschlüsselungsschlüssel »frei«, der Ihre Partition entschlüsselt. Wenn Sie sich entscheiden, die Standard-Partitionstabelle zu ändern, können Sie wählen, welche Partitionen Sie verschlüsseln wollen. Dies wird in den Einstellungen der Partitionstabelle festgelegt.

Was LUKS macht

- LUKS verschlüsselt ganze Blöcke und eignet sich daher gut zum Schutz von Inhalten mobiler Geräte wie z.B. Wechseldatenträgern oder Laptop-Laufwerken.
- Der zugrundeliegende Inhalt des verschlüsselten Blockgeräts ist willkürlich, was es für die Verschlüsselung von Swap-Geräten nützlich macht. Dies kann auch bei bestimmten Datenbanken nützlich sein, die speziell formatierte Blockgeräte zur Datenspeicherung verwenden.
- LUKS verwendet das bestehende Device-Mapper-Kernel-Subsystem.
- LUKS bietet eine Passphrasenverstärkung, die vor Wörterbuchangriffen schützt.
- LUKS-Geräte enthalten mehrere Schlüsselsteckplätze, die es dem Benutzer ermöglichen, Backup-Schlüssel oder Passphrasen hinzuzufügen.

Was macht LUKS*not*

- Festplatten-Verschlüsselungslösungen wie LUKS schützen die Daten nur, wenn Ihr System ausgeschaltet ist. Sobald das System eingeschaltet ist und LUKS den Datenträger entschlüsselt hat, sind die Dateien auf diesem Datenträger für jeden verfügbar, der normalerweise Zugriff auf sie hätte.
- LUKS ist nicht gut geeignet für Szenarien, in denen viele Benutzer unterschiedliche Zugriffsschlüssel für dasselbe Gerät benötigen. Das LUKS1-Format bietet acht Schlüssel-Slots, LUKS2 bis zu 32 Schlüssel-Slots.
- LUKS ist nicht gut geeignet für Anwendungen, die eine Verschlüsselung auf Dateiebene erfordern.

Chiffren

Die für LUKS verwendete Standard-Chiffre ist **aes-xts-plain64**. Die Standard-Schlüsselgröße für LUKS ist 512 Bit. Die Standard-Schlüsselgröße für LUKS mit **Anaconda** (XTS-Modus) ist 512 Bit. Verfügbare Chiffren sind:

- AES - Advanced Encryption Standard - FIPS PUB 197
- Twofish (eine 128-Bit-Blockchiffre)
- Schlange

Zusätzliche Ressourcen

- LUKS-Projekt-Startseite
- LUKS On-Disk-Format-Spezifikation

22.2. KONFIGURIEREN DER LUKS-PASSPHRASE IN DER WEB-KONSOLE

Wenn Sie ein vorhandenes logisches Volume auf Ihrem System verschlüsseln wollen, können Sie dies nur durch Formatieren des Volumes erreichen.

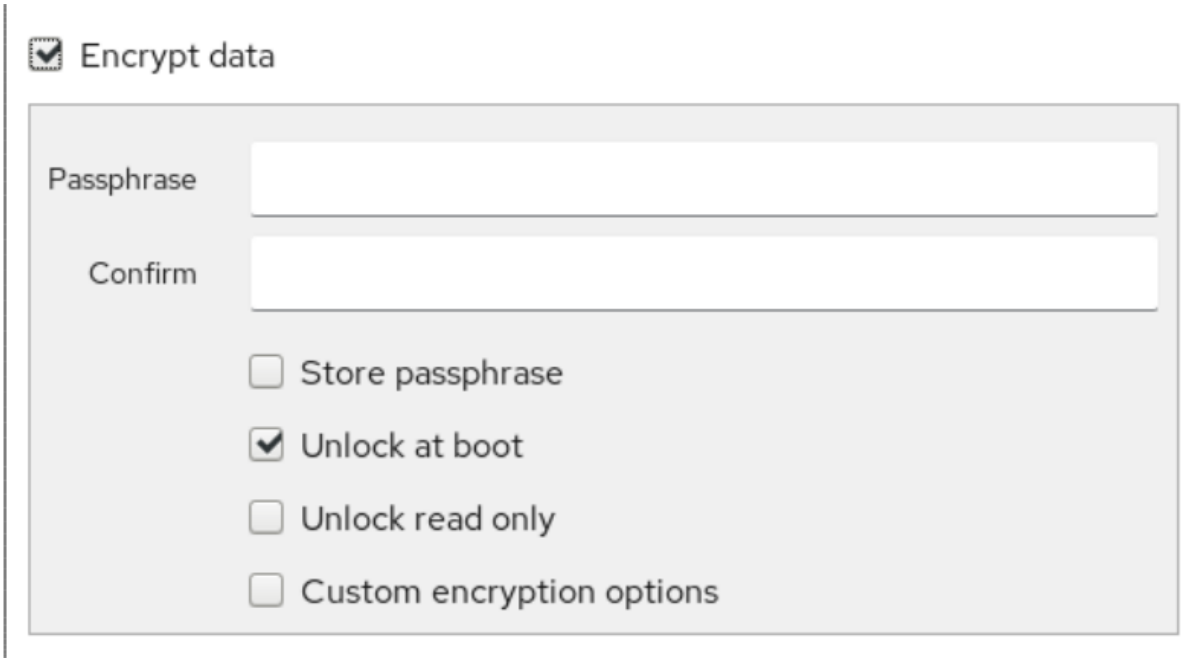
Voraussetzungen

- Die Web-Konsole muss installiert und zugänglich sein.
  Details finden Sie unter Installieren der Web-Konsole.
- Das Paket **cockpit-storaged** ist auf Ihrem System installiert.
- Verfügbares vorhandenes logisches Volume ohne Verschlüsselung.

Verfahren

1. Melden Sie sich an der RHEL 8 Web-Konsole an.
   Details finden Sie unter Anmeldung an der Web-Konsole.
2. Klicken Sie auf **Storage**.
3. Wählen Sie das Speichergerät, das Sie formatieren möchten.

4. Klicken Sie auf das Menüsymbol und wählen Sie die Option **Format**.
5. Aktivieren Sie das Feld **Encrypt data**, um die Verschlüsselung auf Ihrem Speichergerät zu aktivieren.



6. Stellen Sie Ihre neue Passphrase ein und bestätigen Sie sie.
7. [Optional] Ändern Sie weitere Verschlüsselungsoptionen.
8. Schließen Sie die Formatierungseinstellungen ab.
9. Klicken Sie auf **Format**.

22.3. ÄNDERN DER LUKS-PASSPHRASE IN DER WEB-KONSOLE

Ändern Sie eine LUKS-Passphrase auf einer verschlüsselten Festplatte oder Partition in der Web-Konsole.

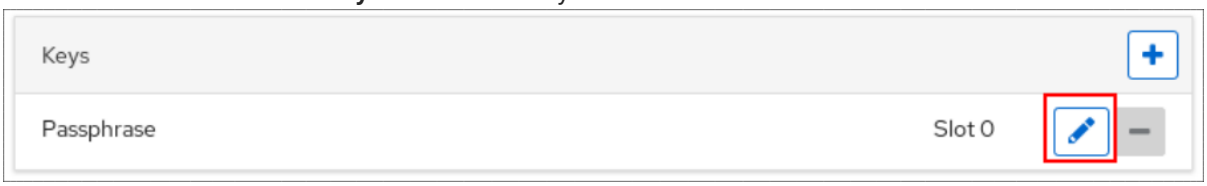
Voraussetzungen

- Die Web-Konsole muss installiert und zugänglich sein.
  Details finden Sie unter Installieren der Web-Konsole.
- Das Paket **cockpit-storaged** ist auf Ihrem System installiert.

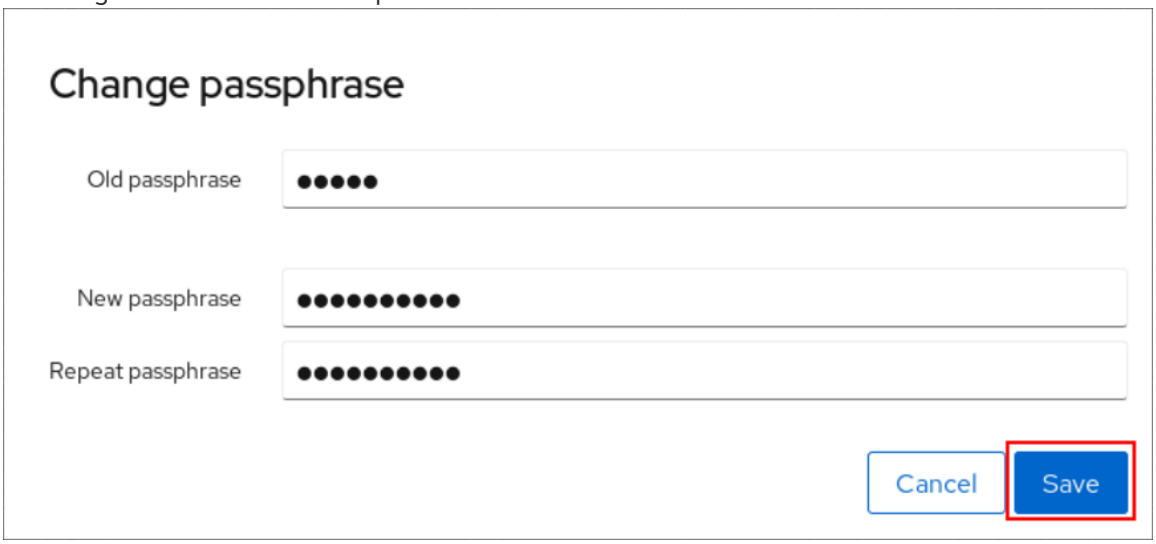
Verfahren

1. Melden Sie sich an der Web-Konsole an.
   Details finden Sie unter Anmeldung an der Web-Konsole.
2. Klicken Sie auf **Storage**
3. Wählen Sie in der Tabelle Laufwerke den Datenträger mit den verschlüsselten Daten aus.
4. Wählen Sie unter **Content** die verschlüsselte Partition aus.
5. Klicken Sie auf **Encryption**.

6. Klicken Sie in der Tabelle **Keys** auf das Stiftsymbol.



7. Im Dialogfenster **Change passphrase**:
   a. Geben Sie Ihre aktuelle Passphrase ein.
   b. Geben Sie Ihre neue Passphrase ein.
   c. Bestätigen Sie Ihre neue Passphrase.



8. Klicken Sie auf **Save**

KAPITEL 23. KONFIGURIEREN DES AUTOMATISCHEN ENTSPERRENS MIT EINEM TANG-SCHLÜSSEL IN DER WEB-KONSOLE

Konfigurieren Sie die automatische Entsperrung eines LUKS-verschlüsselten Speichergeräts mit einem von einem Tang-Server bereitgestellten Schlüssel.

Voraussetzungen

- Die RHEL 8 Web-Konsole wurde installiert.
  Details finden Sie unter Installieren der Web-Konsole.
- Das Paket **cockpit-storaged** ist auf Ihrem System installiert.
- Der Dienst **cockpit.socket** läuft auf Port 9090.
- Die Pakete **clevis**, **tang**, und **clevis-dracut** sind installiert.
- Es läuft ein Tang-Server.

Verfahren

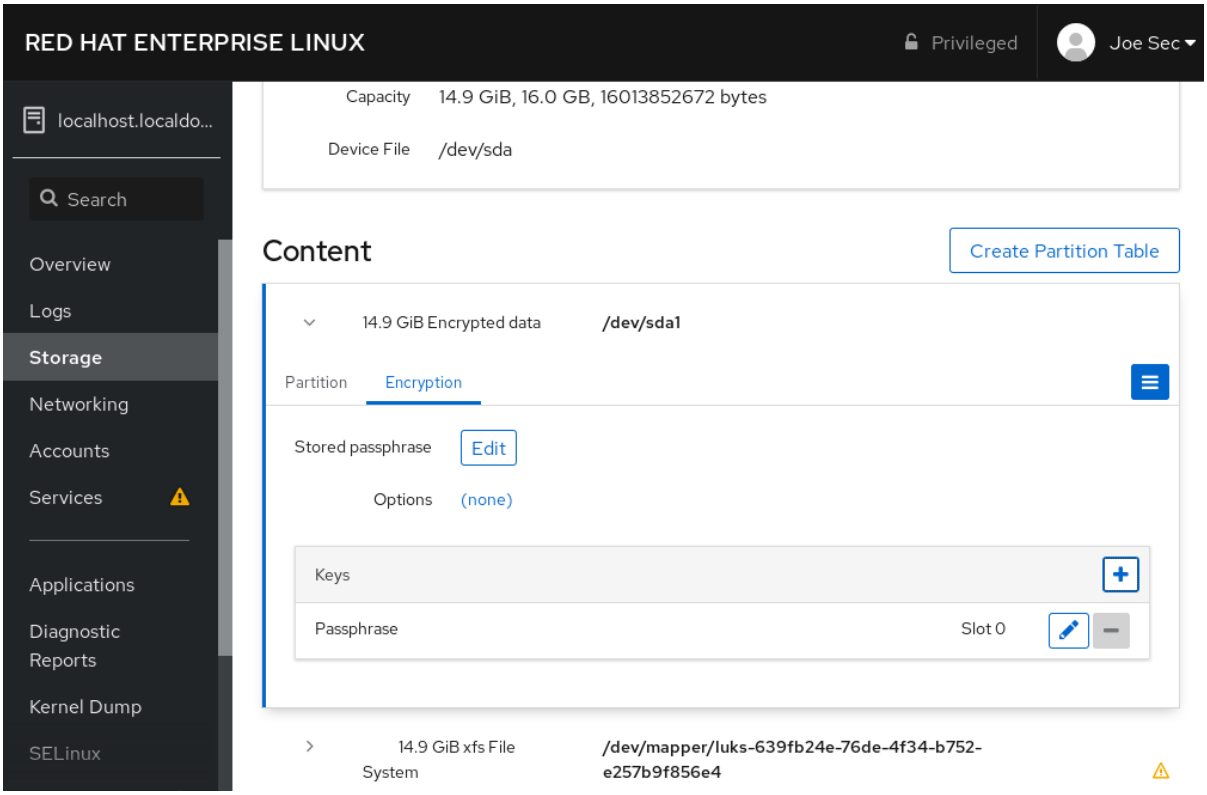
1. Öffnen Sie die RHEL-Webkonsole, indem Sie die folgende Adresse in einen Webbrowser eingeben:

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

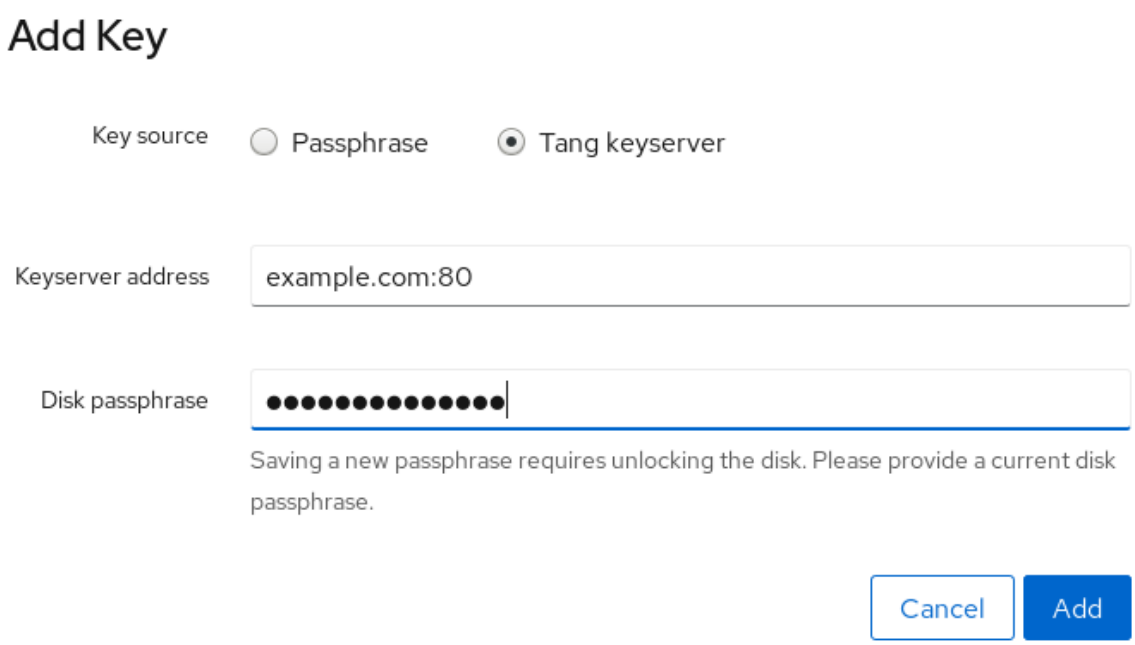
   Ersetzen Sie den Teil *localhost* durch den Hostnamen oder die IP-Adresse des Remote-Servers, wenn Sie eine Verbindung zu einem Remote-System herstellen.

2. Geben Sie Ihre Anmeldedaten ein und klicken Sie auf **Speicher**. Wählen Sie ein verschlüsseltes Gerät und klicken Sie im Teil **Content** auf **Verschlüsselung**:

3. Klicken Sie auf im Bereich **Keys**, um einen Tang-Schlüssel hinzuzufügen:



4. Geben Sie die Adresse Ihres Tang-Servers und ein Passwort an, das das LUKS-verschlüsselte Gerät entsperrt. Klicken Sie zum Bestätigen auf **Hinzufügen**:



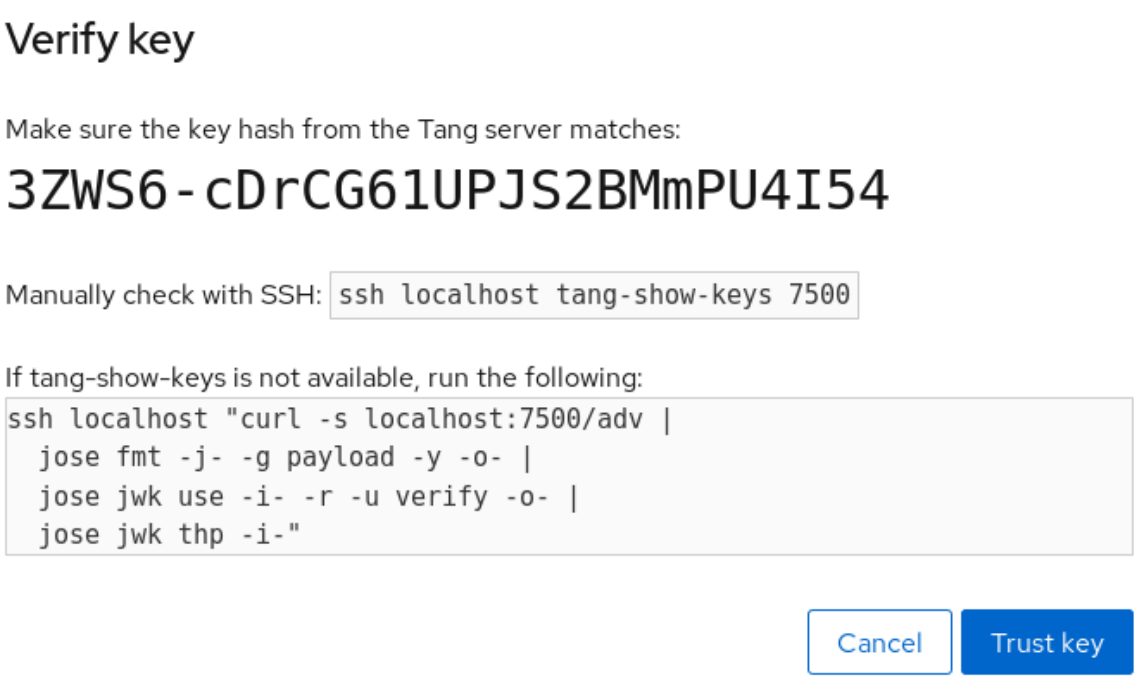
5. Das folgende Dialogfenster bietet einen Befehl, um zu überprüfen, ob der Schlüssel-Hash übereinstimmt. Mit RHEL 8.2 wurde das Skript **tang-show-keys** eingeführt, und Sie können den Schlüssel-Hash mit dem folgenden Befehl auf dem Tang-Server abrufen, der auf dem Port *7500* läuft:

```
# tang-show-keys 7500
3ZWS6-cDrCG61UPJS2BMmPU4I54
```

Unter RHEL 8.1 und früher erhalten Sie den Schlüssel-Hash mit dem folgenden Befehl:

```
# curl -s localhost:7500/adv | jose fmt -j- -g payload -y -o- | jose jwk use -i- -r -u verify -o- |
jose jwk thp -i-
3ZWS6-cDrCG61UPJS2BMmPU4I54
```

6. Klicken Sie auf **Schlüssel vertrauen**, wenn die Schlüssel-Hashes in der Web-Konsole und in der Ausgabe der zuvor aufgeführten Befehle übereinstimmen:

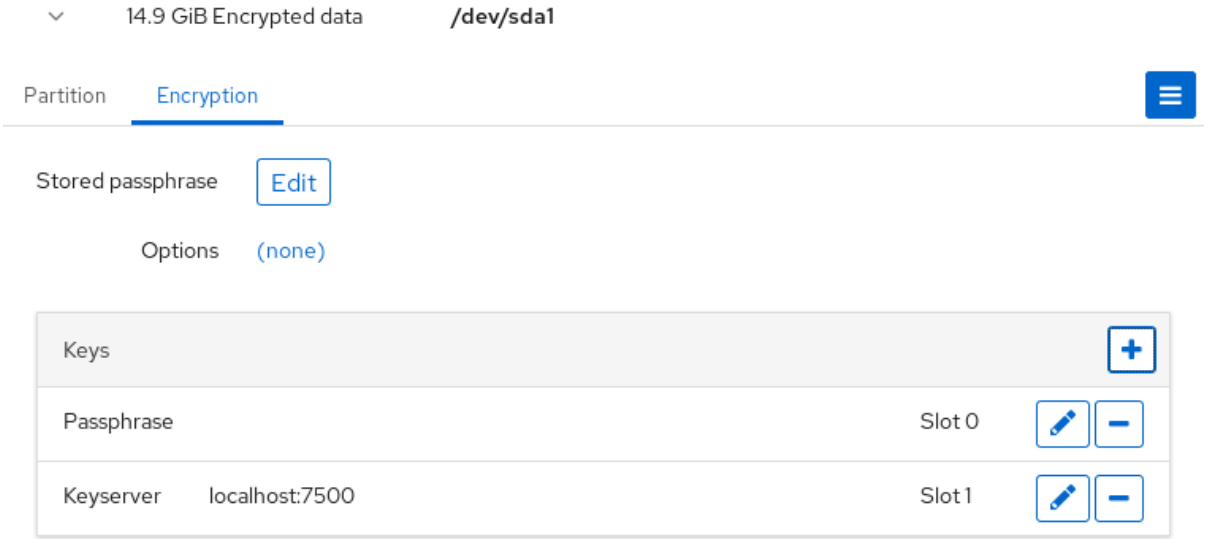


7. Um das Frühstartsystem zu aktivieren, damit es die Festplattenbindung verarbeitet, klicken Sie unten in der linken Navigationsleiste auf **Terminal** und geben Sie die folgenden Befehle ein:

```
# yum install clevis-dracut
# dracut -fv --regenerate-all
```

Schritte zur Verifizierung

1. Prüfen Sie, ob der neu hinzugefügte Tang-Schlüssel nun im Bereich **Keys** mit dem Typ **Keyserver** aufgeführt ist:



2. Vergewissern Sie sich, dass die Bindungen z. B. für den frühen Start verfügbar sind:

```
# lsinitrd | grep clevis
clevis
clevis-pin-sss
clevis-pin-tang
clevis-pin-tpm2
-rwxr-xr-x   1 root     root        1600 Feb 11 16:30 usr/bin/clevis
-rwxr-xr-x   1 root     root        1654 Feb 11 16:30 usr/bin/clevis-decrypt
...
-rwxr-xr-x   2 root     root          45 Feb 11 16:30 usr/lib/dracut/hooks/initqueue/settled/60-
clevis-hook.sh
-rwxr-xr-x   1 root     root        2257 Feb 11 16:30 usr/libexec/clevis-luks-askpass
```

Zusätzliche Ressourcen

- Weitere Details zum automatischen Entsperren von LUKS-verschlüsselten Volumes mit Clevis und Tang finden Sie im Kapitel Konfigurieren des automatischen Entsperrens von verschlüsselten Volumes mit richtlinienbasierter Entschlüsselung.

KAPITEL 24. VERWALTEN VON SOFTWARE-UPDATES IN DER WEB-KONSOLE

Lernen Sie, wie Sie Software-Updates in der RHEL 8 Web-Konsole verwalten und wie Sie diese automatisieren können.

Das Modul Software-Updates in der Web-Konsole basiert auf dem Dienstprogramm **yum**. Weitere Informationen zum Aktualisieren von Software mit **yum** finden Sie im Abschnitt Prüfen auf Updates und Aktualisieren von Paketen.

24.1. VERWALTEN VON MANUELLEN SOFTWARE-UPDATES IN DER WEB-KONSOLE

Dieser Abschnitt beschreibt, wie Sie Ihre Software manuell über die Web-Konsole aktualisieren können.

Voraussetzungen

- Die Web-Konsole muss installiert und zugänglich sein.
  Details finden Sie unter Installieren der Web-Konsole.

Verfahren

1. Melden Sie sich an der RHEL 8 Web-Konsole an.
   Details finden Sie unter Anmeldung an der Web-Konsole.

2. Klicken Sie auf **Software Updates**.
   Die Liste der verfügbaren Updates wird automatisch aktualisiert, wenn die letzte Prüfung mehr als 24 Stunden zurückliegt. Um eine Aktualisierung auszulösen, klicken Sie auf die Schaltfläche **Check for Updates**.

3. Aktualisierungen anwenden.

   a. Um alle verfügbaren Updates zu installieren, klicken Sie auf die Schaltfläche **Install all updates**.

   b. Wenn Sie über Sicherheitsupdates verfügen, können Sie diese separat installieren, indem Sie auf die Schaltfläche **Install Security Updates** klicken.

   Sie können das Update-Protokoll beobachten, während das Update läuft.

4. Nachdem das System Updates angewendet hat, erhalten Sie die Empfehlung, Ihr System neu zu starten.
   Wir empfehlen dies insbesondere dann, wenn das Update einen neuen Kernel oder Systemdienste enthielt, die Sie nicht einzeln neu starten möchten.

5. Klicken Sie auf **Ignore**, um den Neustart abzubrechen, oder auf **Restart Now**, um mit dem Neustart Ihres Systems fortzufahren.

Melden Sie sich nach dem Neustart des Systems an der Webkonsole an und gehen Sie auf die Seite **Software Updates**, um zu überprüfen, ob das Update erfolgreich war.

24.2. VERWALTEN VON AUTOMATISCHEN SOFTWARE-UPDATES IN DER WEB-KONSOLE

In der Web-Konsole können Sie wählen, ob Sie alle Updates oder Sicherheitsupdates anwenden möchten und auch die Periodizität und den Zeitpunkt Ihrer automatischen Updates verwalten.

Voraussetzungen

- Die Web-Konsole muss installiert und zugänglich sein. Details finden Sie unter Installieren der Web-Konsole.

Verfahren

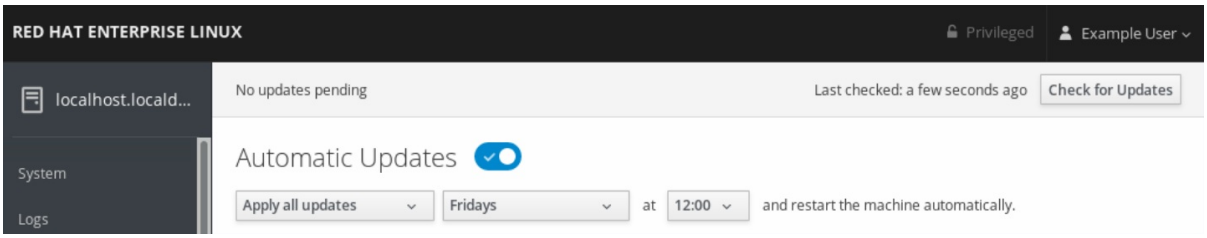
1. Melden Sie sich an der RHEL 8 Web-Konsole an.
   Details finden Sie unter Anmeldung an der Web-Konsole.

2. Klicken Sie auf **Software Updates**.

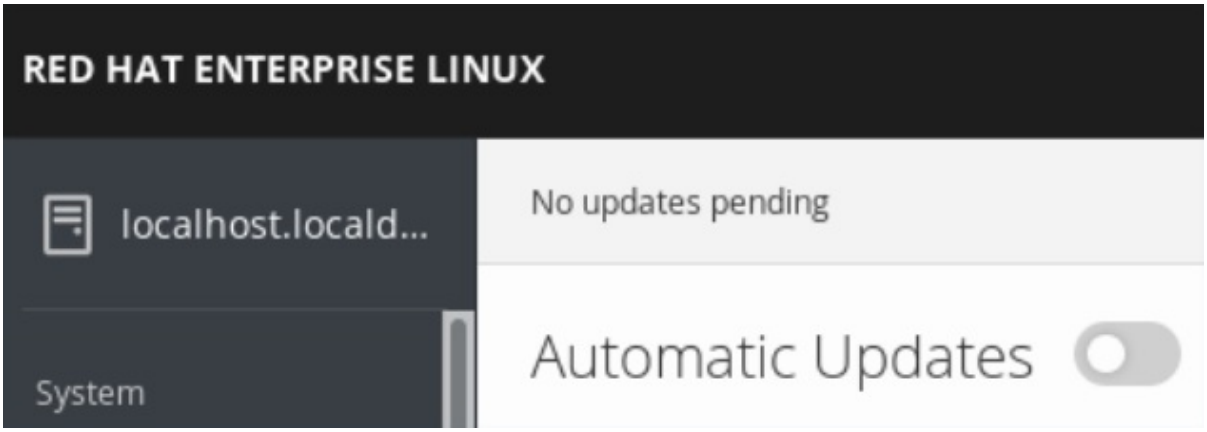
3. Wenn Sie nur Sicherheitsupdates automatisch anwenden möchten, klicken Sie auf das Dropdown-Menü **Apply all updates** und wählen Sie **Apply security updates**.

4. Um den Tag der automatischen Aktualisierung zu ändern, klicken Sie auf das Dropdown-Menü **every day** und wählen einen bestimmten Tag aus.

5. Um die Zeit der automatischen Aktualisierung zu ändern, klicken Sie auf das Dropdown-Menü **6:00** und wählen Sie eine bestimmte Zeit.



6. Wenn Sie automatische Software-Updates deaktivieren möchten, klicken Sie auf den Schalter neben **Automatic Updates**, um ihn in die Position "Deaktiviert" zu bringen.



KAPITEL 25. VERWALTEN VON ABONNEMENTS IN DER WEB-KONSOLE

Verwalten Sie Ihr Abonnement für Red Hat Enterprise Linux 8 über die Webkonsole.

Um ein Abonnement für Ihr Red Hat Enterprise Linux zu erhalten, benötigen Sie ein Konto im Red Hat-Kundenportal oder einen Aktivierungsschlüssel.

Dieses Kapitel behandelt:

- Abonnementverwaltung in der RHEL 8 Web-Konsole.
- Registrierung von Abonnements für Ihr System in der Web-Konsole mit dem Red Hat-Benutzernamen und -Passwort.
- Registrierung von Abonnements mit dem Aktivierungsschlüssel.

Voraussetzungen

- Gekaufte Abonnements.
- Das System, das einem Abonnement unterliegt, muss mit dem Internet verbunden sein, da die Webkonsole mit dem Red Hat-Kundenportal kommunizieren muss.

25.1. ABONNEMENT-VERWALTUNG IN DER WEB-KONSOLE

Die RHEL 8 Web-Konsole bietet eine Schnittstelle für die Verwendung von Red Hat Subscription Manager, der auf Ihrem lokalen System installiert ist.

Der Subscription Manager verbindet sich mit dem Red Hat-Kundenportal und überprüft alle verfügbaren:

- Aktive Abonnements
- Abgelaufene Abonnements
- Verlängerte Abonnements

Wenn Sie das Abonnement verlängern oder ein anderes im Red Hat Customer Portal erhalten möchten, müssen Sie die Daten im Subscription Manager nicht manuell aktualisieren. Der Subscription Manager synchronisiert die Daten automatisch mit dem Red Hat-Kundenportal.

25.2. REGISTRIERUNG VON ABONNEMENTS MIT ANMELDEINFORMATIONEN IN DER WEB-KONSOLE

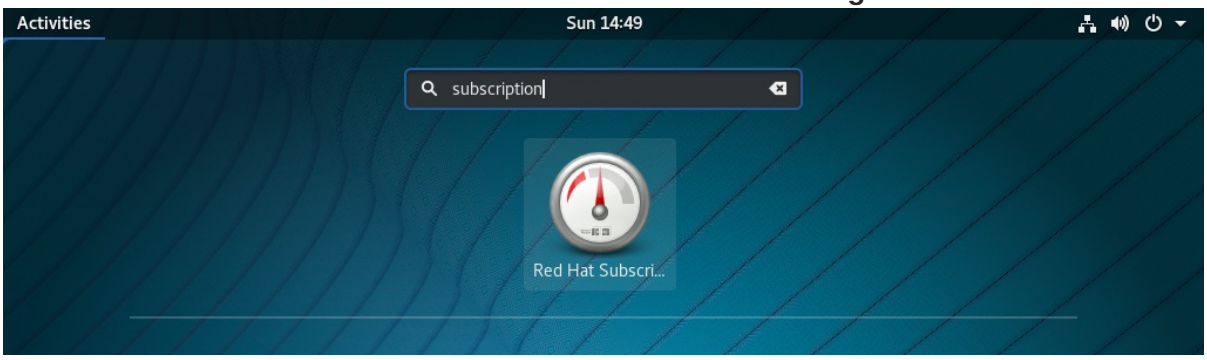
Verwenden Sie die folgenden Schritte, um ein neu installiertes Red Hat Enterprise Linux mit der RHEL 8 Web-Konsole zu registrieren.

Voraussetzungen

- Ein gültiges Benutzerkonto auf dem Red Hat-Kundenportal.
  Siehe die Seite Erstellen einer Red Hat-Anmeldung .
- Aktives Abonnement für Ihr RHEL-System.

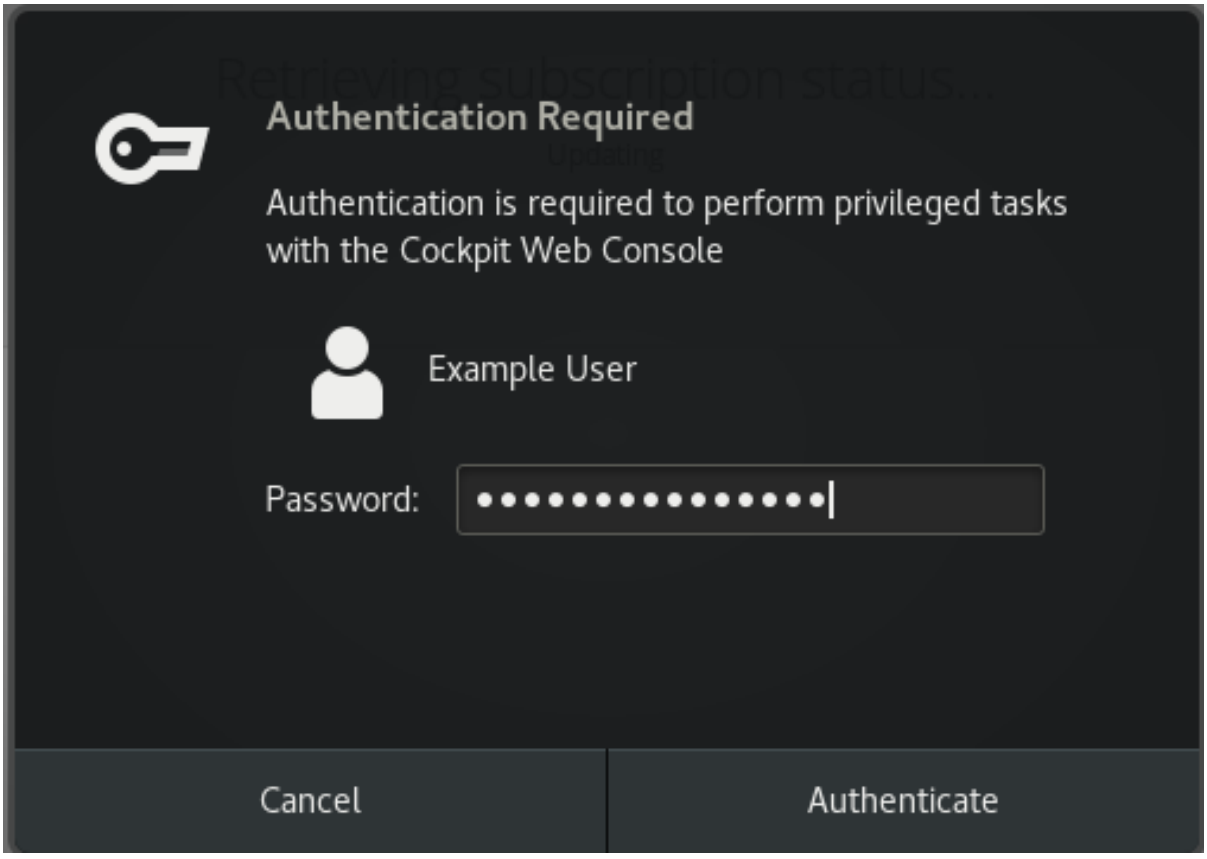
Verfahren

1. Geben Sie Abonnement in das Suchfeld ein und drücken Sie die **Eingabetaste**.



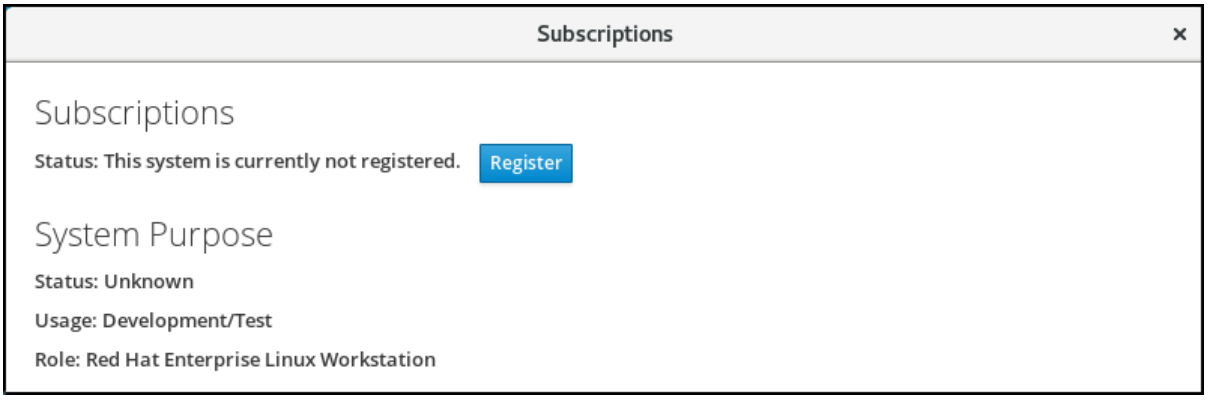
   Alternativ können Sie sich an der RHEL 8-Webkonsole anmelden. Details finden Sie unter Anmeldung an der Web-Konsole.

2. Fügen Sie im Authentifizierungsdialog **polkit** für privilegierte Tasks das Passwort hinzu, das zu dem im Dialog angezeigten Benutzernamen gehört.

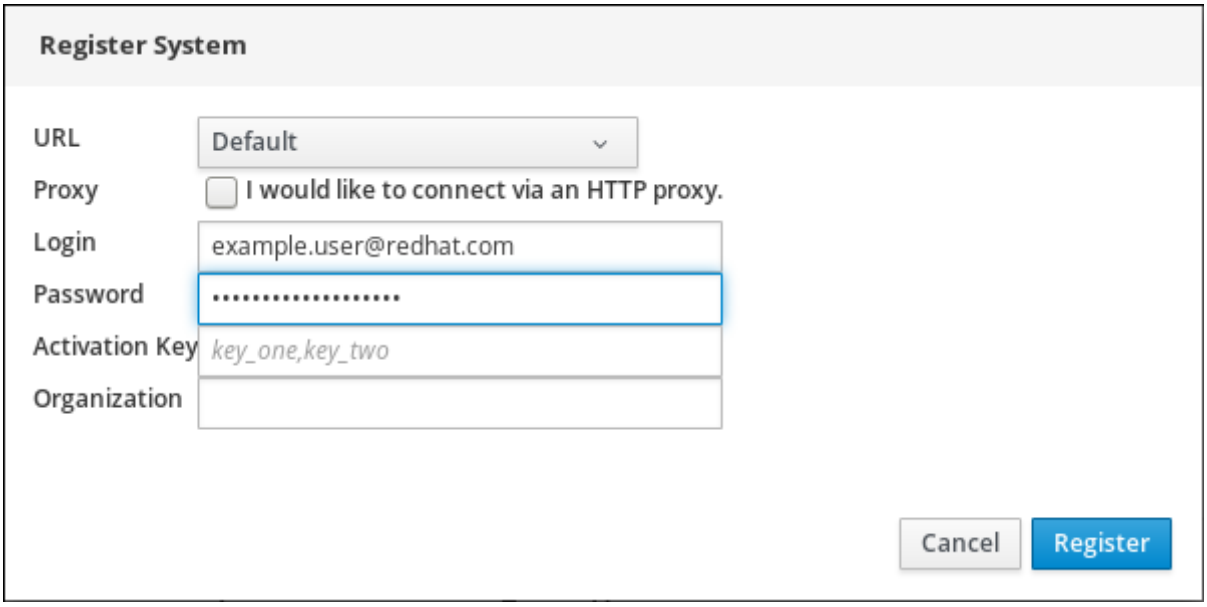


3. Klicken Sie auf **Authentifizieren**.

4. Klicken Sie im Dialogfeld **Subscriptions** auf **Registrieren**.



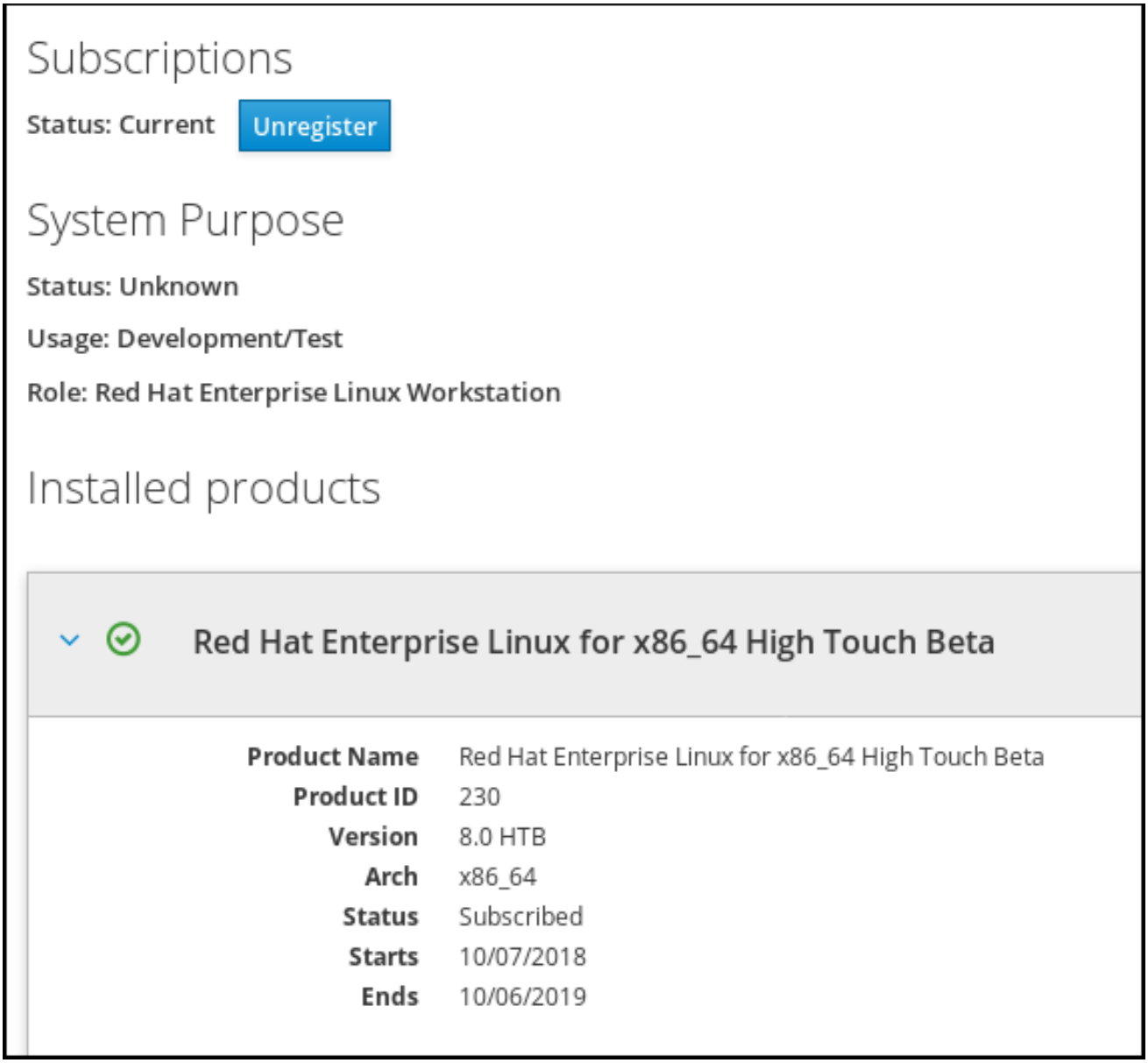
5. Geben Sie Ihre Anmeldedaten für das Kundenportal ein.



6. Geben Sie den Namen Ihrer Organisation ein.
   Wenn Sie mehr als ein Konto im Red Hat-Kundenportal haben, müssen Sie den Organisationsnamen oder die Organisations-ID hinzufügen. Um die Org-ID zu erhalten, gehen Sie zu Ihrer Red Hat-Kontaktstelle.

7. Klicken Sie auf die Schaltfläche **Registrieren**.

An diesem Punkt wurde Ihr Red Hat Enterprise Linux 8-System erfolgreich registriert.



25.3. REGISTRIERUNG VON ABONNEMENTS MIT AKTIVIERUNGSSCHLÜSSELN IN DER WEB-KONSOLE

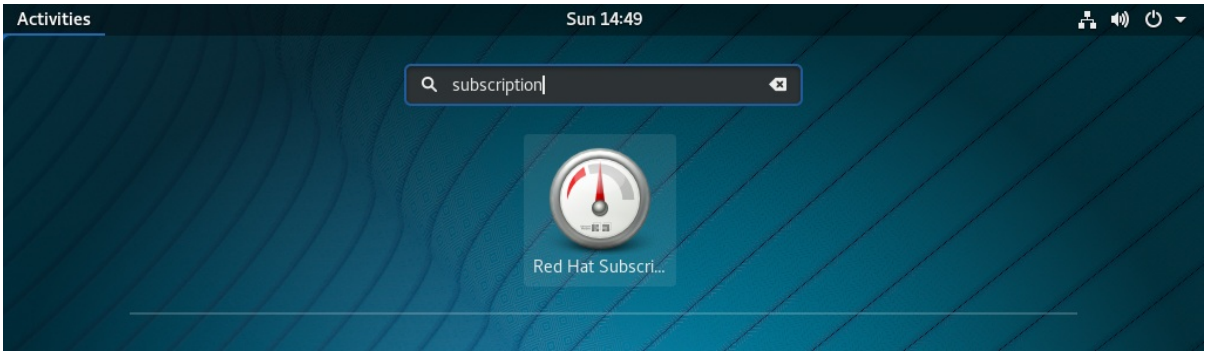
So registrieren Sie ein Abonnement für Red Hat Enterprise Linux,

Voraussetzungen

- Wenn Sie noch kein Benutzerkonto im Portal haben, erhalten Sie den Aktivierungsschlüssel von Ihrem Lieferanten.

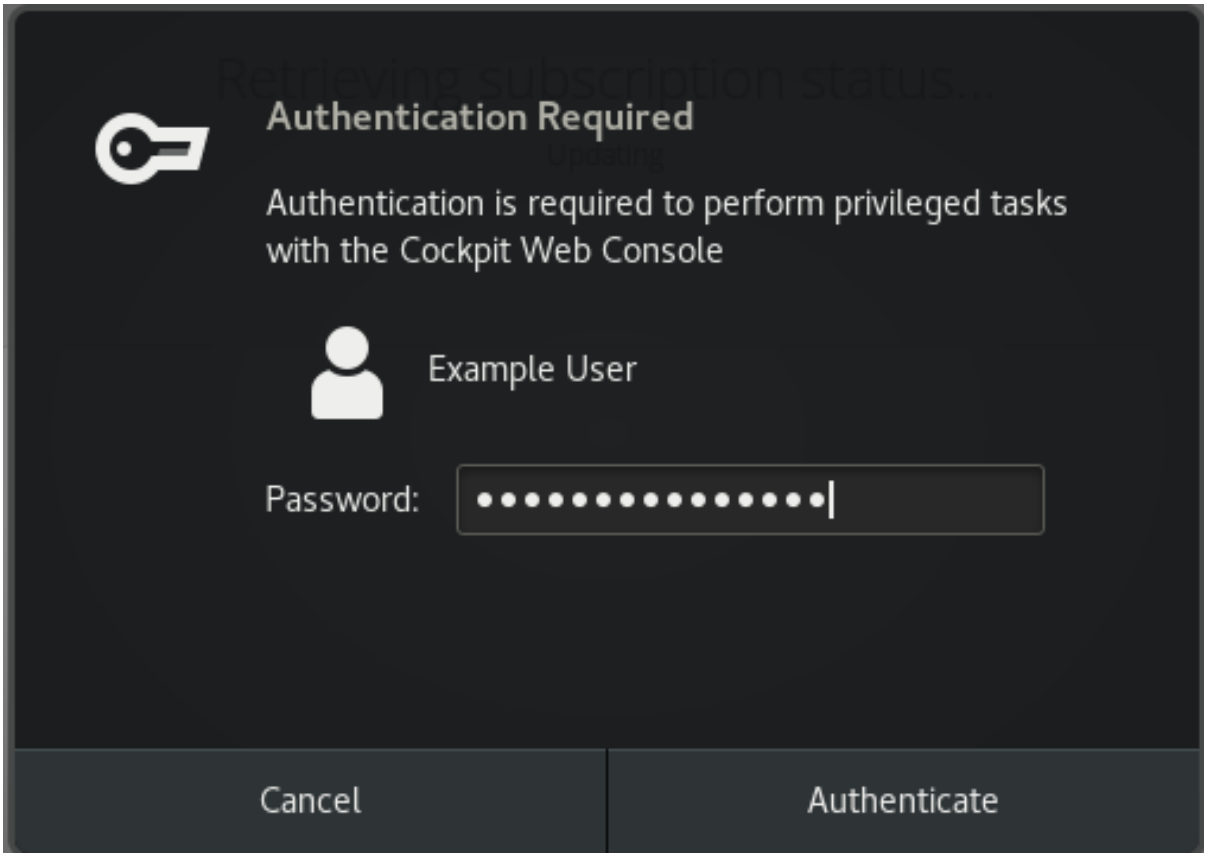
Verfahren

1. Geben Sie Abonnement in das Suchfeld ein und drücken Sie die Taste **Enter**.



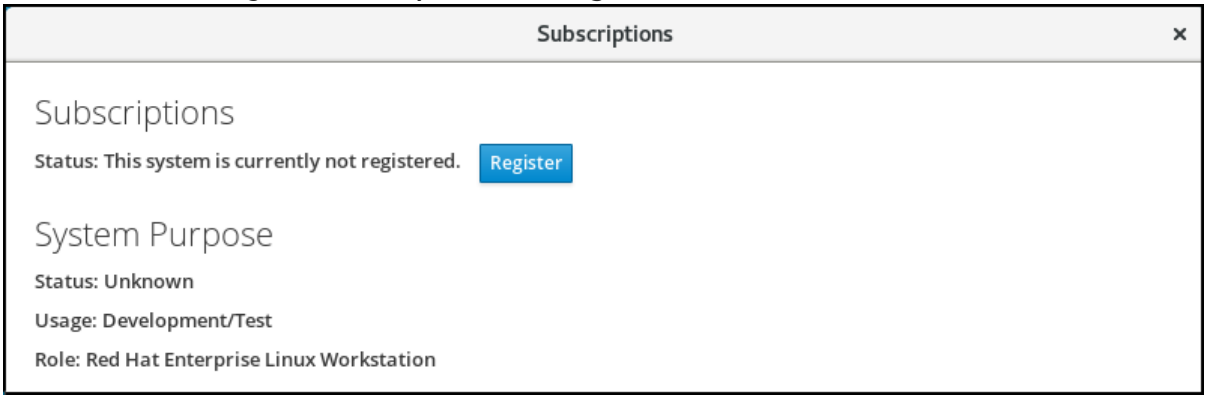
Alternativ können Sie sich an der RHEL 8-Webkonsole anmelden. Details finden Sie unter Anmeldung an der Web-Konsole.

2. Fügen Sie im Authentifizierungsdialog den Systembenutzernamen und das Passwort hinzu, die Sie bei der Systeminstallation erstellt haben.



3. Klicken Sie auf **Authenticate**.

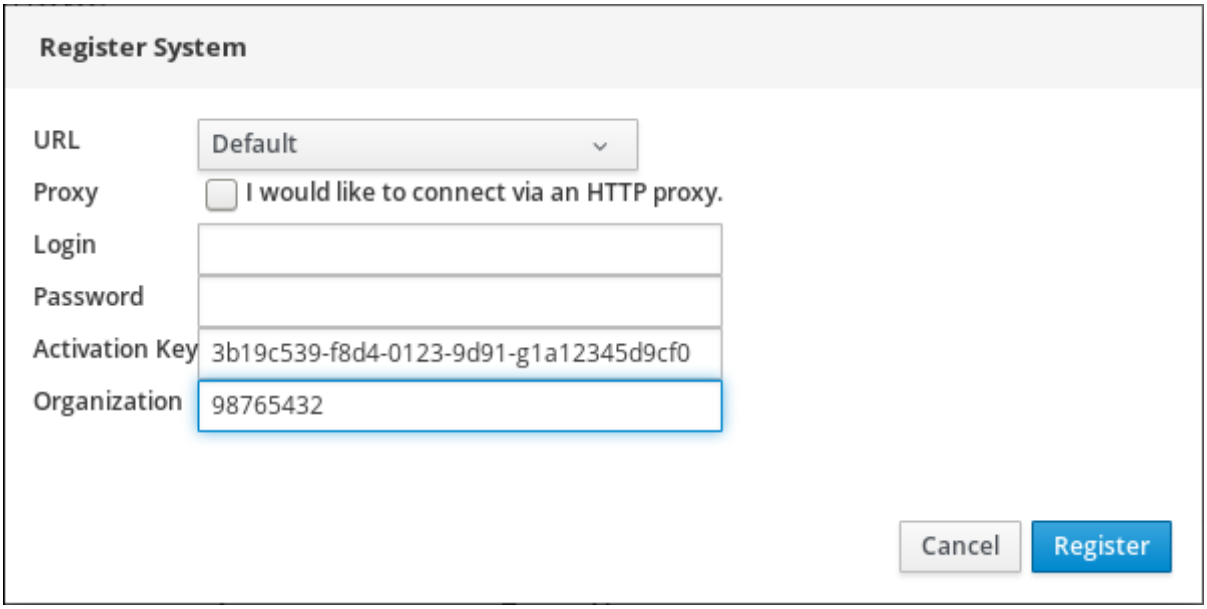
4. Klicken Sie im Dialogfeld **Subscriptions** auf **Register**.



5. Geben Sie den Aktivierungsschlüssel in das Registrierungsformular ein.

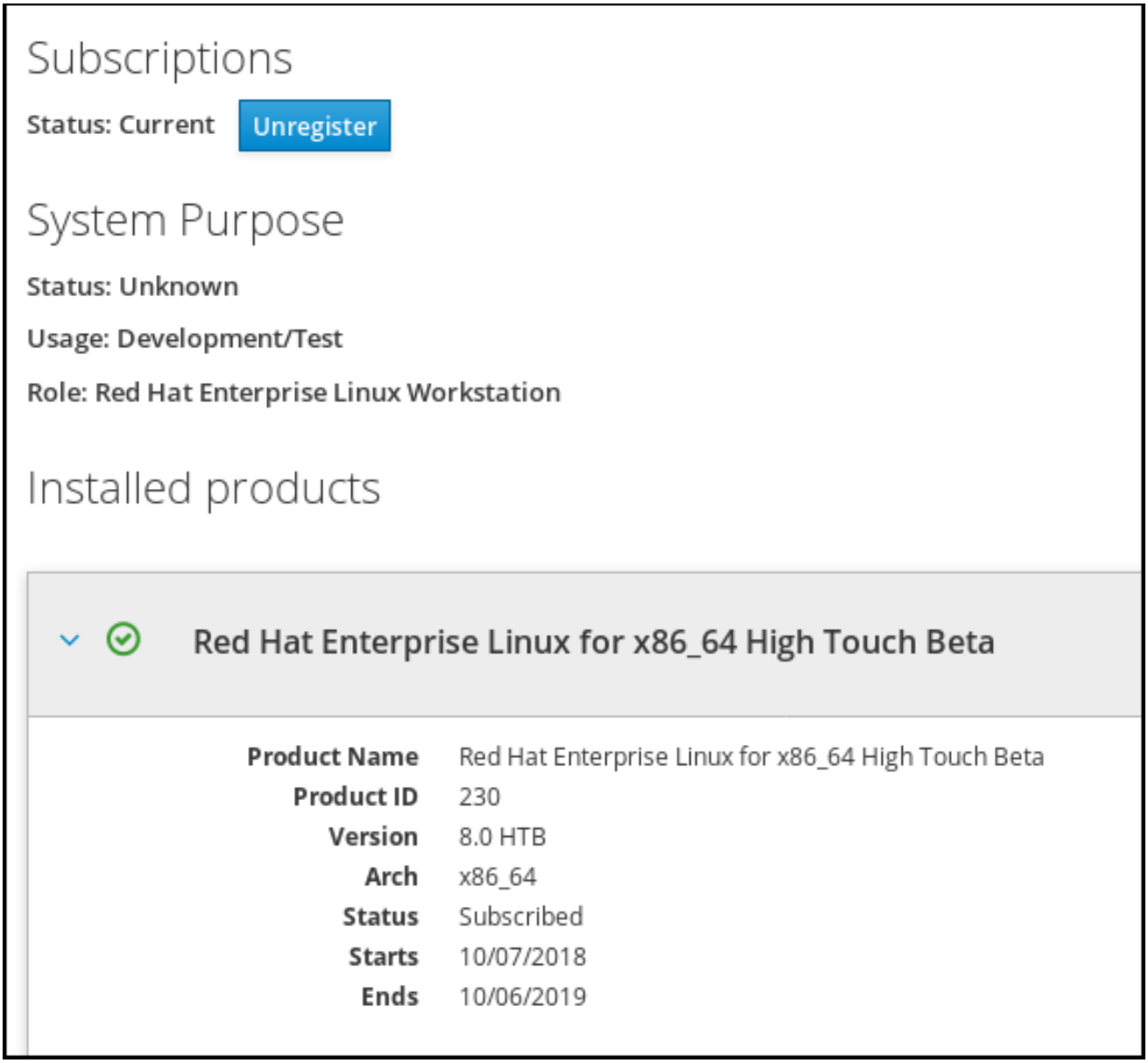
6. Geben Sie den Namen Ihrer Organisation ein.
   Sie müssen den Organisationsnamen oder die Organisations-ID hinzufügen, wenn Sie mehr als ein Konto im Red Hat-Kundenportal haben.

   Um die Org-ID zu erhalten, wenden Sie sich an Ihre Red Hat-Kontaktstelle.



7. Klicken Sie auf die Schaltfläche **Register**.

An diesem Punkt wurde Ihr RHEL 8-System erfolgreich registriert.


Subscriptions
Status: Current
Unregister
System Purpose
Status: Unknown
Usage: Development/Test
Role: Red Hat Enterprise Linux Workstation
Installed products
Red Hat Enterprise Linux for x86_64 High Touch Beta
Product Name
Red Hat Enterprise Linux for x86_64 High Touch Beta
Product ID
230
Version
8.0 HTB
Arch
x86_64
Status
Subscribed
Starts
10/07/2018
Ends
10/06/2019

KAPITEL 26. KONFIGURIEREN VON KDUMP IN DER WEB-KONSOLE

Richten Sie die **kdump** Konfiguration in der RHEL 8 Web-Konsole ein und testen Sie sie.

Die Web-Konsole ist Teil einer Standardinstallation von Red Hat Enterprise Linux 8 und aktiviert oder deaktiviert den Dienst **kdump** beim Booten. Außerdem können Sie über die Web-Konsole bequem den reservierten Speicher für **kdump** konfigurieren; oder den Speicherort *vmcore* in einem unkomprimierten oder komprimierten Format auswählen.

Voraussetzungen

- Siehe *Red Hat Enterprise Linux web console* für weitere Details.

26.1. KONFIGURIEREN VON KDUMP-SPEICHERVERBRAUCH UND ZIELORT IN DER WEB-KONSOLE

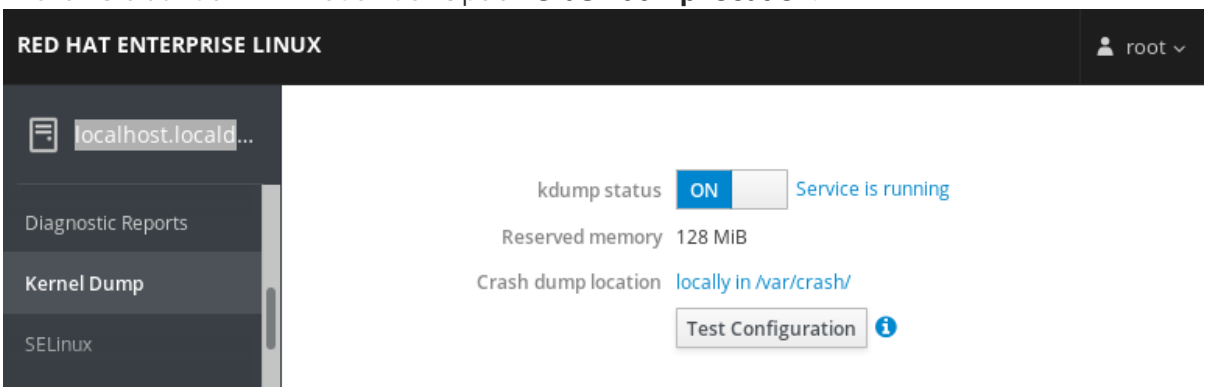
Die folgende Prozedur zeigt Ihnen, wie Sie die Registerkarte **Kernel Dump** in der Red Hat Enterprise Linux Web-Konsolenoberfläche verwenden, um die Speichermenge zu konfigurieren, die für den kdump-Kernel reserviert ist. Die Prozedur beschreibt auch, wie Sie den Zielspeicherort der vmcore-Dumpdatei angeben und wie Sie Ihre Konfiguration testen können.

Voraussetzungen

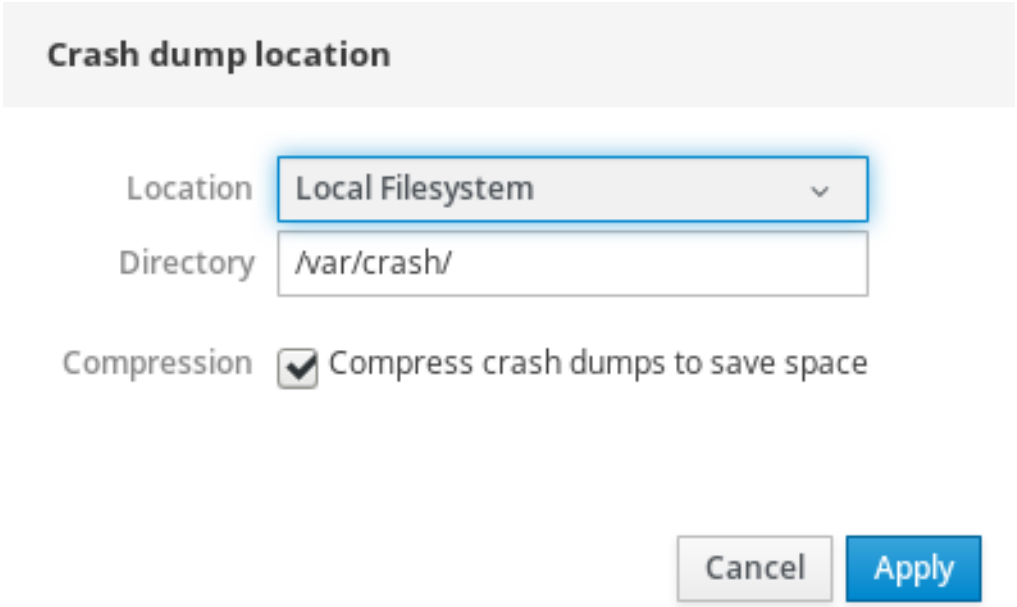
- Einführung in die Bedienung des *web console*

Verfahren

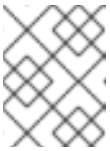
1. Öffnen Sie die Registerkarte **Kernel Dump** und starten Sie den Dienst **kdump**.
2. Konfigurieren Sie die **kdump** Speichernutzung über den *command line*.
3. Klicken Sie auf den Link neben der Option **Crash dump location**.



4. Wählen Sie die Option **Local Filesystem** aus der Dropdown-Liste und geben Sie das Verzeichnis an, in dem Sie den Dump speichern möchten.



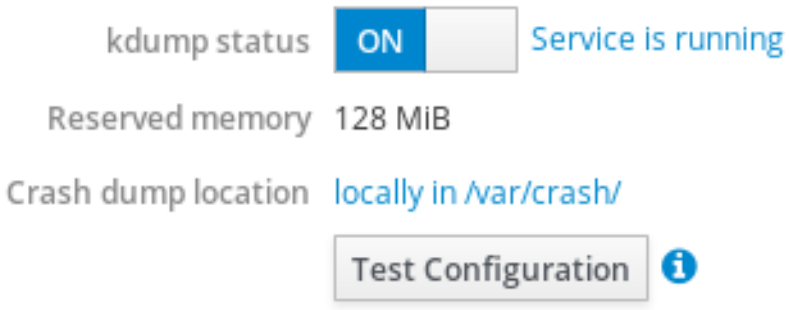
- Wählen Sie alternativ die Option **Remote over SSH** aus der Dropdown-Liste, um den vmcore über das SSH-Protokoll an einen entfernten Rechner zu senden.
  Füllen Sie die Felder **Server**, **ssh key** und **Directory** mit der Adresse des entfernten Rechners, dem Ort des ssh-Schlüssels und einem Zielverzeichnis.
- Eine andere Möglichkeit ist, die Option **Remote over NFS** aus der Dropdown-Liste zu wählen und das Feld **Mount** auszufüllen, um den vmcore über das NFS-Protokoll an einen entfernten Rechner zu senden.



ANMERKUNG

Aktivieren Sie das Kontrollkästchen **Compression**, um die Größe der vmcore-Datei zu reduzieren.

5. Testen Sie Ihre Konfiguration, indem Sie den Kernel abstürzen lassen.



WARNUNG

Dieser Schritt unterbricht die Ausführung des Kernels und führt zu einem Systemabsturz und Datenverlust.

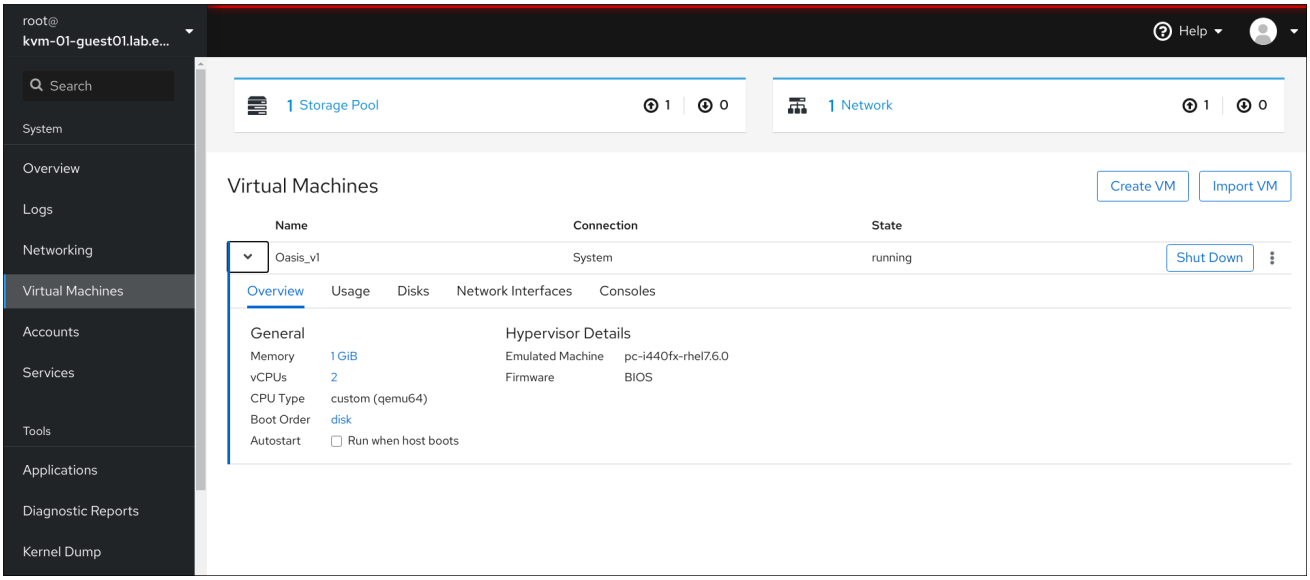
Zusätzliche Ressourcen

- Eine vollständige Liste der derzeit unterstützten Ziele für **kdump** finden Sie unter *Supported kdump targets*.
- Wie Sie einen SSH-Server konfigurieren und eine schlüsselbasierte Authentifizierung einrichten, erfahren Sie unter *Using secure communications between two systems with OpenSSH* .

KAPITEL 27. VERWALTEN VON VIRTUELLEN MASCHINEN IN DER WEB-KONSOLE

Verwalten Sie Ihre virtuellen Maschinen in einer RHEL 8 Web-Konsole und lernen Sie die Möglichkeiten der Virtualisierungsverwaltung kennen.

Um virtuelle Maschinen in einer grafischen Oberfläche auf einem RHEL 8-Host zu verwalten, können Sie das **Virtual Machines** -Fenster in der RHEL 8-Webkonsole verwenden.



27.1. ÜBERBLICK ÜBER DIE VERWALTUNG VIRTUELLER MASCHINEN ÜBER DIE WEB-KONSOLE

Die RHEL 8 Web-Konsole ist eine webbasierte Oberfläche für die Systemverwaltung. Als eine ihrer Funktionen bietet die Web-Konsole eine grafische Ansicht der virtuellen Maschinen (VMs) auf dem Host-System und ermöglicht es, diese VMs zu erstellen, darauf zuzugreifen und zu konfigurieren.

Beachten Sie, dass Sie, um die Web-Konsole zur Verwaltung Ihrer VMs unter RHEL 8 zu verwenden, zunächst ein Web-Konsolen-Plugin für die Virtualisierung installieren müssen.

Nächste Schritte

- Eine Anleitung zum Aktivieren der VMs-Verwaltung in Ihrer Web-Konsole finden Sie unter Abschnitt 27.2, »Einrichten der Web-Konsole zur Verwaltung virtueller Maschinen« .
- Eine umfassende Liste der VM-Verwaltungsaktionen, die die Web-Konsole bietet, finden Sie unter Abschnitt 27.3, »Verwaltungsfunktionen für virtuelle Maschinen, die in der Web-Konsole verfügbar sind«.
- Eine Liste der Funktionen, die derzeit nicht in der Web-Konsole verfügbar sind, aber in der Anwendung **virt-manager** genutzt werden können, finden Sie unter Abschnitt 27.4, »Unterschiede zwischen den Virtualisierungsfunktionen im Virtual Machine Manager und der Web-Konsole«.

27.2. EINRICHTEN DER WEB-KONSOLE ZUR VERWALTUNG VIRTUELLER MASCHINEN

Bevor Sie die RHEL 8 Web-Konsole zur Verwaltung virtueller Maschinen (VMs) verwenden können, müssen Sie das Web-Konsolen-Plug-in für virtuelle Maschinen auf dem Host installieren.

Voraussetzungen

- Stellen Sie sicher, dass die Web-Konsole auf Ihrem Rechner installiert und aktiviert ist.

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

  Wenn dieser Befehl **Unit cockpit.socket could not be found** zurückgibt, folgen Sie dem Dokument Installieren der Webkonsole, um die Webkonsole zu aktivieren.

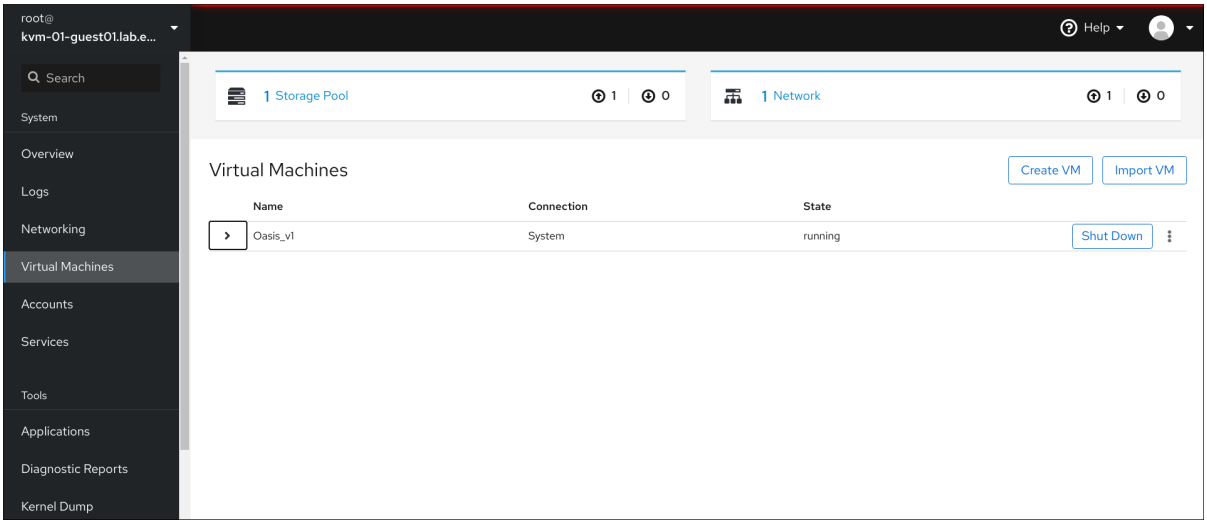
Verfahren

- Installieren Sie das Plug-In **cockpit-machines**.

```
# yum install cockpit-machines
```

Verifizierung

- Wenn die Installation erfolgreich ist, erscheint **Virtuelle Maschinen** im Seitenmenü der Webkonsole.



Zusätzliche Ressourcen

- Eine Anleitung zum Verbinden mit der Web-Konsole sowie weitere Informationen zur Verwendung der Web-Konsole finden Sie im *Managing systems using the RHEL 8 web console* dokument.

27.3. VERWALTUNGSFUNKTIONEN FÜR VIRTUELLE MASCHINEN, DIE IN DER WEB-KONSOLE VERFÜGBAR SIND

Mit der RHEL 8 Web-Konsole können Sie die folgenden Aktionen durchführen, um die virtuellen Maschinen (VMs) auf Ihrem System zu verwalten.

Tabelle 27.1. VM-Aufgaben, die in der RHEL 8 Web-Konsole durchgeführt werden können

Aufgabe	Für Details, siehe:
Erstellen Sie eine VM und installieren Sie sie mit einem Gastbetriebssystem	Erstellen von virtuellen Maschinen und Installieren von Gastbetriebssystemen über die Web-Konsole
Löschen Sie eine VM.	Löschen von virtuellen Maschinen über die Web-Konsole.
Starten, Herunterfahren und Neustarten der VM	Starten von virtuellen Maschinen über die Web-Konsole und Herunterfahren und Neustarten von virtuellen Maschinen über die Web-Konsole
Verbindung zu und Interaktion mit einer VM über verschiedene Konsolen	Interaktion mit virtuellen Maschinen über die Web-Konsole
Anzeigen einer Vielzahl von Informationen über die VM	Anzeigen von Informationen zur virtuellen Maschine über die Web-Konsole
Anpassen des einer VM zugewiesenen Host-Speichers	Hinzufügen und Entfernen von Speicher für virtuelle Maschinen über die Web-Konsole
Verwalten von Netzwerkverbindungen für die VM	Verwendung der Web-Konsole zur Verwaltung der Netzwerkschnittstellen virtueller Maschinen
Verwalten Sie den auf dem Host verfügbaren VM-Speicher und hängen Sie virtuelle Festplatten an die VM an	Verwalten von Speicher für virtuelle Maschinen über die Web-Konsole
Konfigurieren Sie die virtuellen CPU-Einstellungen der VM	Verwalten von virtuellen CPUs über die Web-Konsole

27.4. UNTERSCHIEDE ZWISCHEN DEN VIRTUALISIERUNGSFUNKTIONEN IM VIRTUAL MACHINE MANAGER UND DER WEB-KONSOLE

Die Anwendung Virtual Machine Manager (**virt-manager**) wird in RHEL 8 unterstützt, wurde aber veraltet. Die Web-Konsole soll in einer späteren Hauptversion ihr Ersatz werden. Es wird daher empfohlen, sich mit der Web-Konsole vertraut zu machen, um die Virtualisierung über eine grafische Benutzeroberfläche zu verwalten.

In RHEL 8 können jedoch einige VM-Verwaltungsaufgaben nur in **virt-manager** oder der Befehlszeile durchgeführt werden. Die folgende Tabelle hebt die Funktionen hervor, die in **virt-manager** verfügbar sind, aber nicht in der Web-Konsole von RHEL 8.0 zur Verfügung stehen.

Wenn eine Funktion in einer späteren Nebenversion von RHEL 8 verfügbar ist, erscheint die Mindestversion von RHEL 8 in der Spalte *Support in web console introduced*.

Tabelle 27.2. VM-Verwaltungsaufgaben, die nicht über die Web-Konsole in RHEL 8.0 durchgeführt werden können

Aufgabe	Unterstützung in der Web-Konsole eingeführt	Alternative Methode mit CLI
Einstellen einer virtuellen Maschine zum Starten beim Hochfahren des Hosts	RHEL 8.1	**virsh autostart**
Anhalten einer virtuellen Maschine	RHEL 8.1	**virsh suspend**
Wiederaufnahme einer angehaltenen virtuellen Maschine	RHEL 8.1	**virsh resume**
Erstellen von Dateisystem-Verzeichnis-Speicherpools	RHEL 8.1	**virsh pool-define-as**
Erstellen von NFS-Speicherpools	RHEL 8.1	**virsh pool-define-as**
Erstellen von Speicherpools für physische Festplattengeräte	RHEL 8.1	**virsh pool-define-as**
Erstellen von LVM-Volumengruppen-Speicherpools	RHEL 8.1	**virsh pool-define-as**
Erstellen von partitionsbasierten Speicherpools	*CURRENTLY UNAVAILABLE*	**virsh pool-define-as**
Erstellen von GlusterFS-basierten Speicherpools	*CURRENTLY UNAVAILABLE*	**virsh pool-define-as**
Erstellen von vHBA-basierten Speicherpools mit SCSI-Geräten	*CURRENTLY UNAVAILABLE*	**virsh pool-define-as**
Erstellen von Multipath-basierten Speicherpools	*CURRENTLY UNAVAILABLE*	**virsh pool-define-as**
Erstellen von RBD-basierten Speicherpools	*CURRENTLY UNAVAILABLE*	**virsh pool-define-as**
Anlegen eines neuen Speichervolumens	RHEL 8.1	**virsh vol-create**
Hinzufügen eines neuen virtuellen Netzwerks	RHEL 8.1	**virsh net-create** oder **virsh net-define**
Löschen eines virtuellen Netzwerks	RHEL 8.1	**virsh net-undefine**

Aufgabe	Unterstützung in der Web-Konsole eingeführt	Alternative Methode mit CLI
Erstellen einer Bridge von der Schnittstelle eines Host-Rechners zu einer virtuellen Maschine	*CURRENTLY UNAVAILABLE*	**virsh iface-bridge**
Erstellen eines Schnappschusses	*CURRENTLY UNAVAILABLE*	**virsh snapshot-create-as**
Rückgängig machen eines Schnappschusses	*CURRENTLY UNAVAILABLE*	**virsh snapshot-revert**
Löschen eines Schnappschusses	*CURRENTLY UNAVAILABLE*	**virsh snapshot-delete**
Klonen einer virtuellen Maschine	*CURRENTLY UNAVAILABLE*	**virt-clone**
Migrieren einer virtuellen Maschine auf einen anderen Host-Computer	*CURRENTLY UNAVAILABLE*	**virsh migrate**

Zusätzliche Ressourcen

- Informationen über den Virtual Machine Manager finden Sie in der RHEL 7-Dokumentation.

KAPITEL 28. VERWALTEN VON ENTFERNTEN SYSTEMEN IN DER WEB-KONSOLE

Verbinden Sie sich mit den entfernten Systemen und verwalten Sie sie in der RHEL 8-Webkonsole.

Das folgende Kapitel beschreibt:

- Die optimale Topologie von verbundenen Systemen.
- Was ist das Dashboard.
- So fügen Sie entfernte Systeme hinzu und entfernen sie.
- Wann, warum und wie Sie SSH-Schlüssel für die Remote-Systemauthentifizierung verwenden.

Voraussetzungen

- Öffnete den SSH-Dienst auf entfernten Systemen.

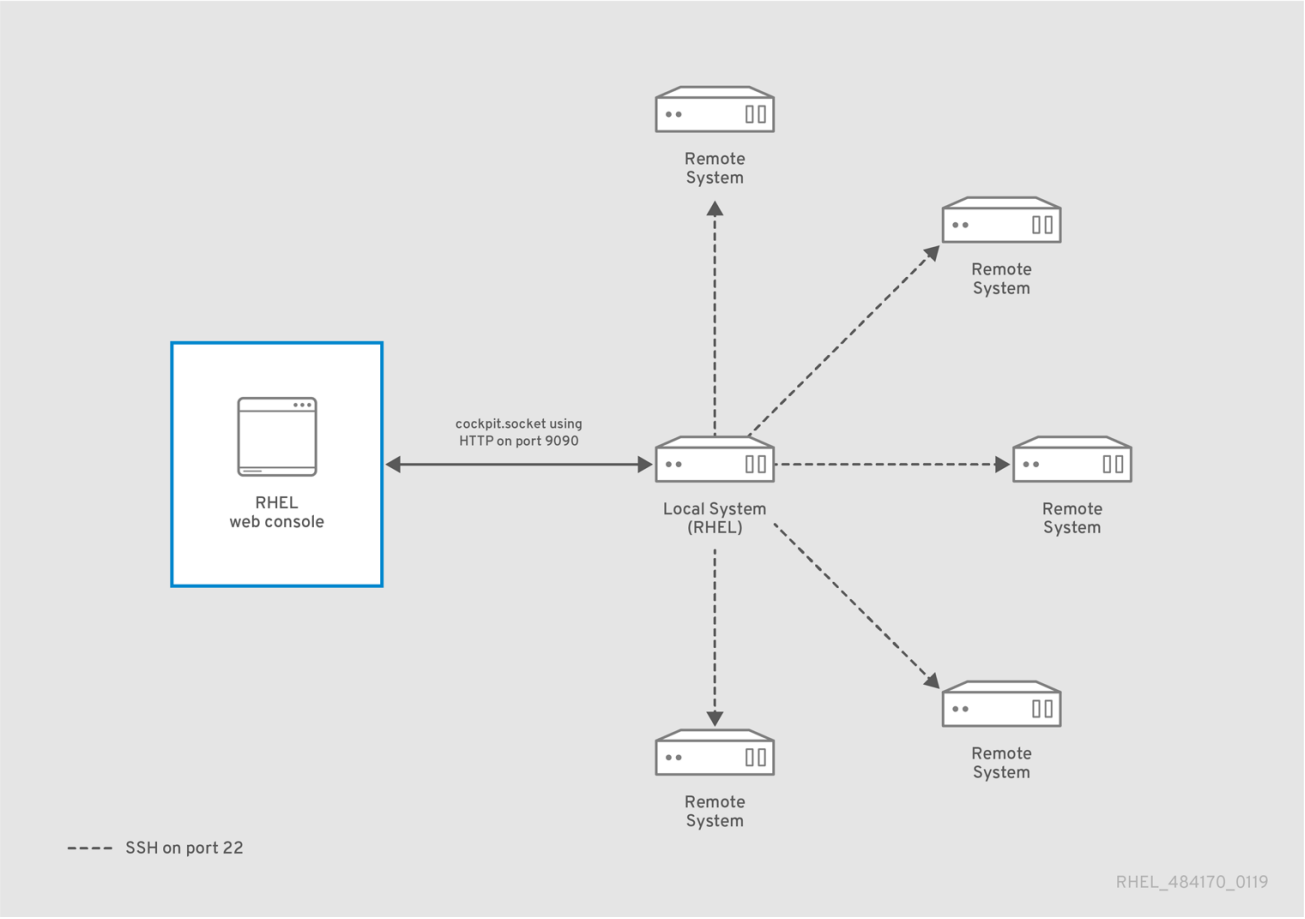
28.1. REMOTE-SYSTEMMANAGER IN DER WEB-KONSOLE

Die Verwendung der RHEL 8 Web-Konsole zur Verwaltung entfernter Systeme im Netzwerk erfordert die Berücksichtigung der Topologie der angeschlossenen Server.

Für optimale Sicherheit empfiehlt Red Hat den folgenden Verbindungsaufbau:

- Verwenden Sie ein System mit der Web-Konsole als Bastion-Host. Der Bastion-Host ist ein System mit geöffnetem HTTPS-Port.
- Alle anderen Systeme kommunizieren über SSH.

Wenn die Weboberfläche auf dem Bastion-Host läuft, können Sie alle anderen Systeme über das SSH-Protokoll erreichen, das in der Standardkonfiguration Port 22 verwendet.



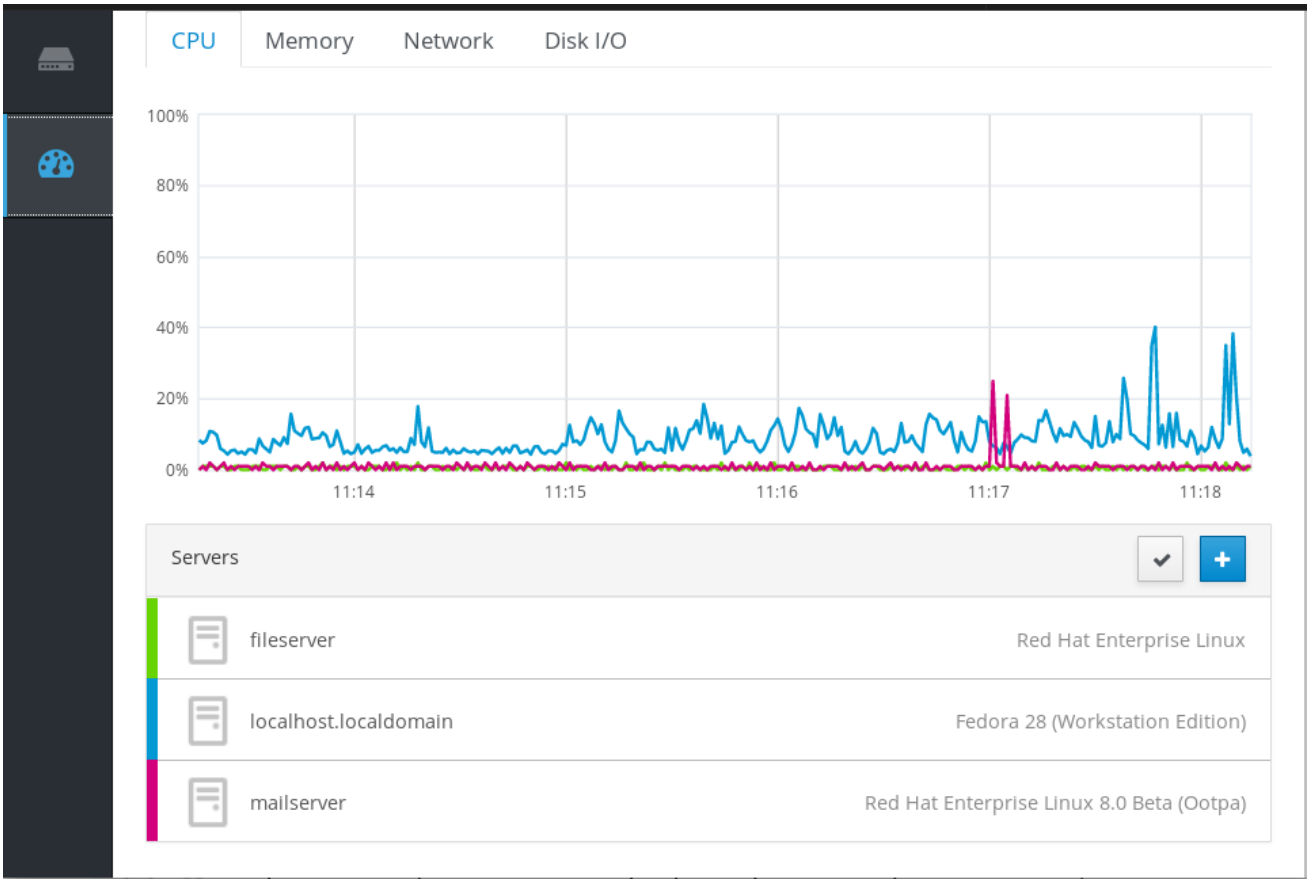
28.2. HINZUFÜGEN VON ENTFERNTEN HOSTS ZUR WEB-KONSOLE

Dieser Abschnitt hilft Ihnen, andere Systeme mit einem Benutzernamen und einem Passwort mit dem Dashboard in der Web-Konsole zu verbinden.

Das Dashboard ist ein Werkzeug zur Verwaltung von Remote-Servern, mit dem Sie Remote-Systeme hinzufügen, verbinden oder entfernen können.

Das Dashboard zeigt Diagramme und den Status für jedes der entfernten Systeme an.

Sie können bis zu 20 Remote-Systeme im Dashboard hinzufügen.



Voraussetzungen

- Das **cockpit-dashboard** -Paket, das auf dem System installiert ist, auf dem die Weboberfläche ausgeführt wird:

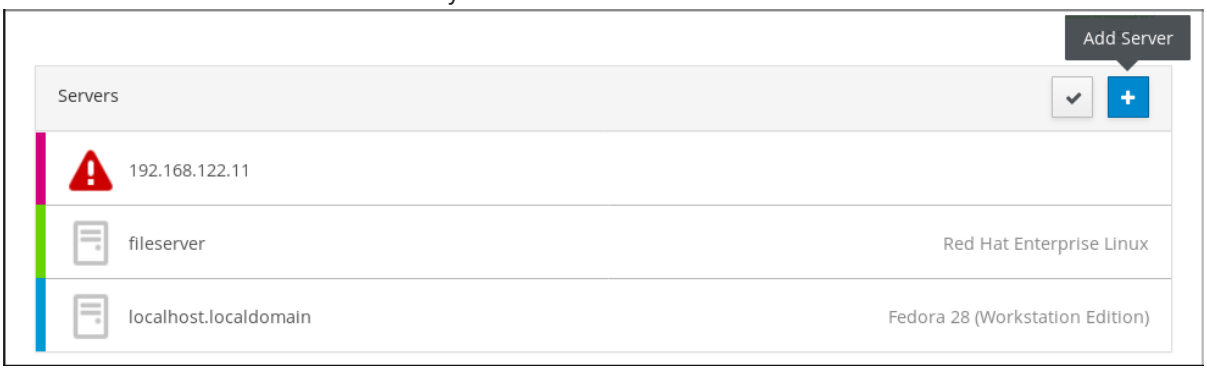
  ```
  $ sudo yum install cockpit-dashboard
  ```

  Das Paket **cockpit-dashboard** erweitert die RHEL 8 Web-Konsole um die Remote-Systemverwaltung.

- Sie müssen in der Web-Konsole mit Administratorrechten angemeldet sein.
  Details finden Sie unter Anmeldung an der Web-Konsole.

Verfahren

1. Gehen Sie in der RHEL 8 Web-Konsole auf **Dashboard**.
2. Klicken Sie im **Dashboard** auf das Symbol **Add Server**.



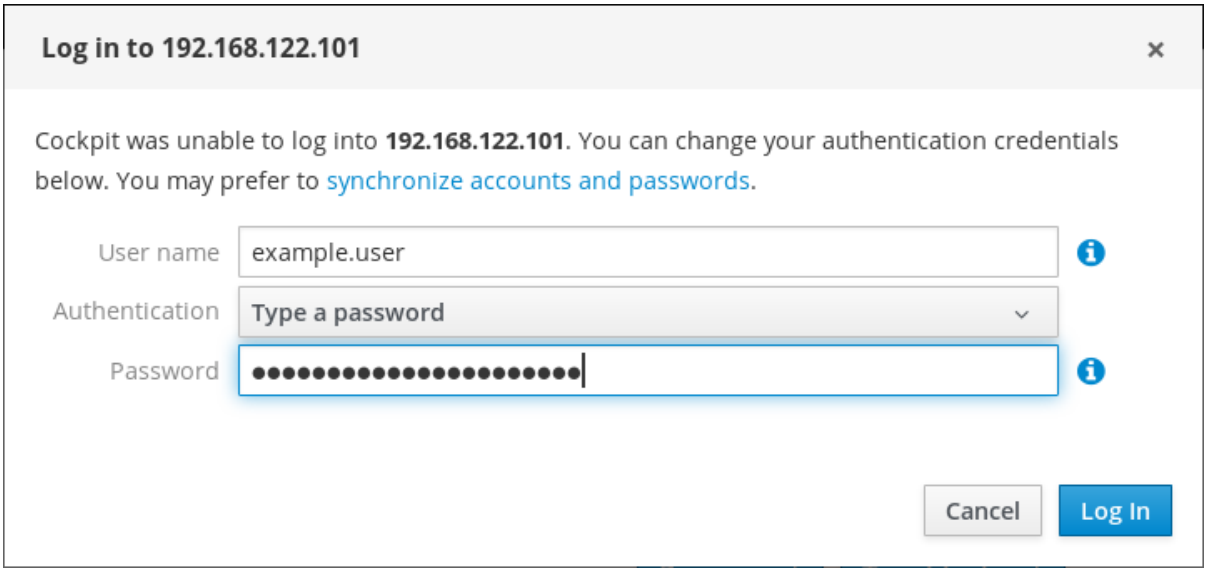
3. Geben Sie im Dialogfeld **Add Machine to Dashboard**den Hostnamen oder die IP-Adresse des entfernten Systems ein.

4. (Optional) Klicken Sie auf das Feld **Color**, um die Farbe des Systems im Dashboard zu ändern.

5. Klicken Sie auf **Add**.

6. Geben Sie im Dialogfeld **Log in to <servername>**die Anmeldedaten für das entfernte System ein.
   Sie können ein beliebiges Benutzerkonto des entfernten Systems verwenden. Wenn Sie jedoch Anmeldeinformationen eines Benutzerkontos ohne Administrationsrechte verwenden, können Sie keine Administrationsaufgaben durchführen.

   Wenn Sie die gleichen Anmeldeinformationen wie für Ihr lokales System verwenden, authentifiziert die Web-Konsole entfernte Systeme automatisch bei jeder Anmeldung. Die Verwendung der gleichen Anmeldeinformationen auf mehreren Rechnern könnte jedoch ein potenzielles Sicherheitsrisiko darstellen.

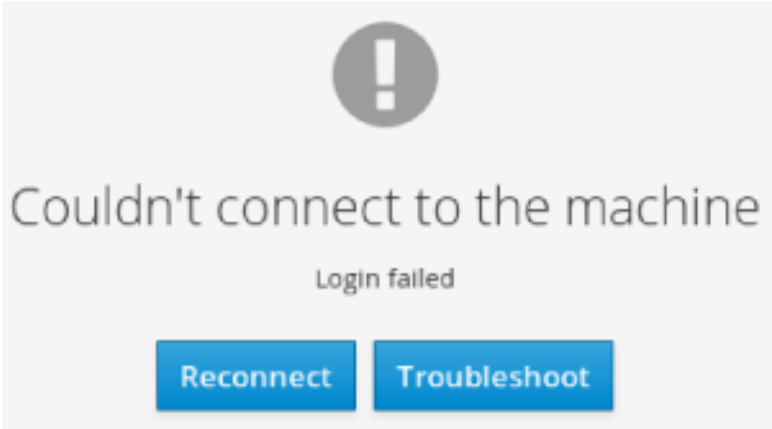


7. Klicken Sie auf **Log In**.

Wenn die Anmeldung erfolgreich ist, fügt das Dashboard einen neuen Eintrag in der Liste hinzu. Um die Verbindung zu überprüfen, klicken Sie auf das System, um alle Details in der Webkonsole zu sehen.

ANMERKUNG

Die Web-Konsole speichert keine Passwörter, die zur Anmeldung an entfernten Systemen verwendet werden, was bedeutet, dass Sie sich nach jedem Neustart des Systems erneut anmelden müssen. Um den Anmeldedialog zu öffnen, klicken Sie auf die Schaltfläche **Troubleshoot**, die sich auf dem Hauptbildschirm des abgetrennten entfernten Systems befindet.



28.3. ENTFERNEN VON ENTFERNTEN HOSTS AUS DER WEB-KONSOLE

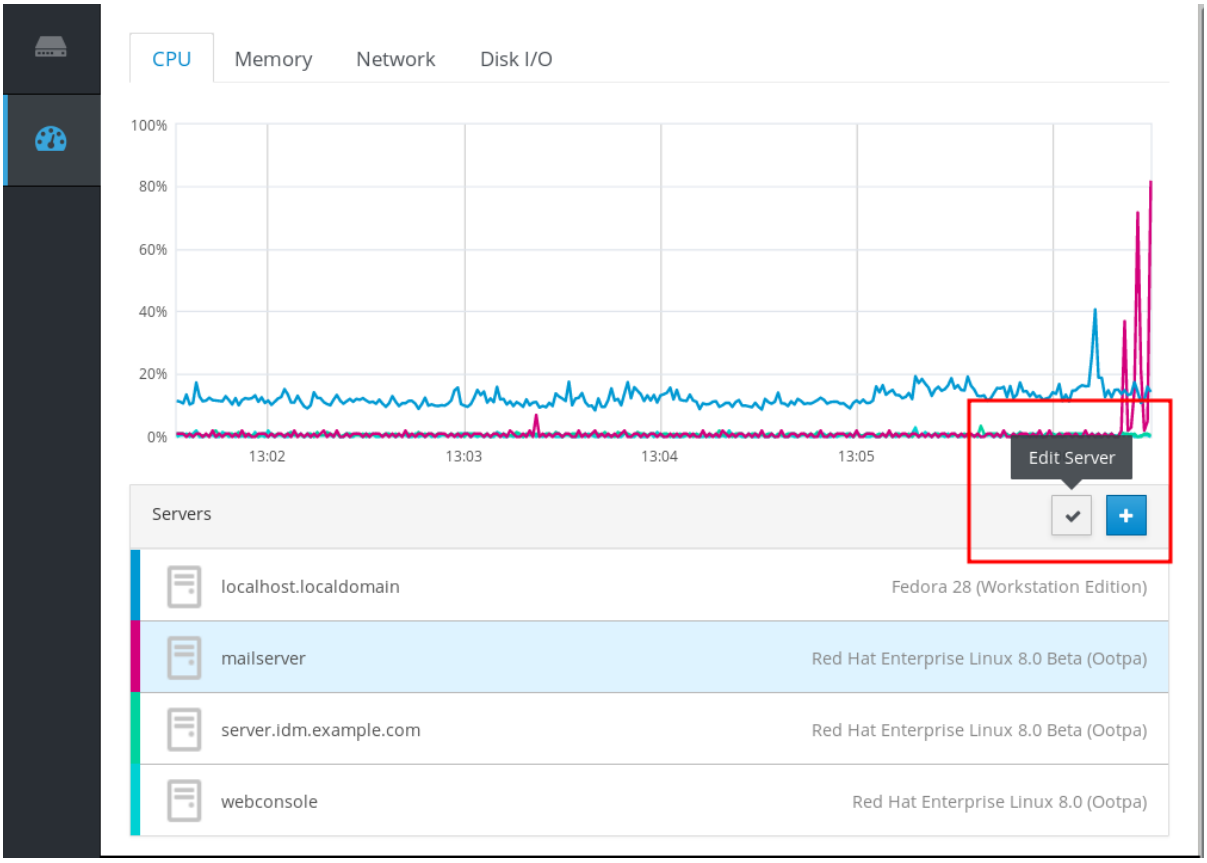
Dieser Abschnitt leitet Sie an, wie Sie andere Systeme aus einem Dashboard in der Web-Konsole entfernen.

Voraussetzungen

- Das **cockpit-dashboard** -Paket, das auf dem System installiert ist, auf dem die Weboberfläche ausgeführt wird.
- Entfernte Systeme hinzugefügt.
  Für Details siehe Abschnitt 28.2, »Hinzufügen von entfernten Hosts zur Web-Konsole« .
- Sie müssen in der Web-Konsole mit Administratorrechten angemeldet sein.
  Details finden Sie unter Anmeldung an der Web-Konsole.

Verfahren

1. Melden Sie sich an der RHEL 8 Web-Konsole an.
2. Klicken Sie auf **Dashboard**.
3. Klicken Sie auf das Symbol **Edit Server**.



4. Um den Server aus der **Dashboard** zu entfernen, klicken Sie auf das rote Symbol **Remove**.

Als Ergebnis wird der Server von **Dashboard** entfernt.

28.4. EINRICHTEN VON SSH FÜR DIE FERNVERWALTUNG IN DER WEB-KONSOLE

Die Web-Konsole von RHEL 8 unterstützt die Authentifizierung mit SSH-Schlüsseln. Dies hat die folgenden Vorteile:

- Erhöhung der Sicherheit der Kommunikation zwischen Servern.
- Vermeiden Sie die wiederholte Eingabe von Anmeldedaten.

WICHTIG

Die Verwendung von SSH-Schlüsseln funktioniert nur für reinen Lesezugriff oder für passwortloses sudo, da die Authentifizierung ohne Passwort erfolgt. Um administrative Aufgaben auszuführen, verwenden Sie Ihre Systemkonto-Anmeldeinformationen mit administrativen Rechten.

So konfigurieren Sie die Authentifizierung mit SSH-Schlüsseln in der Web-Konsole:

- Kopieren Sie den öffentlichen Schlüssel auf das angeschlossene entfernte System.
- Stellen Sie den Pfad zum privaten Schlüssel in dem System ein, auf dem die RHEL 8 Web-Konsole läuft.

- Melden Sie sich von der Webkonsole ab und melden Sie sich erneut an, um die Änderung der Authentifizierung sicherzustellen.

Voraussetzungen

- SSH-Schlüssel, der auf dem System mit laufender Web-Konsole gespeichert ist. Wenn Sie keinen haben, verwenden Sie den folgenden Befehl:

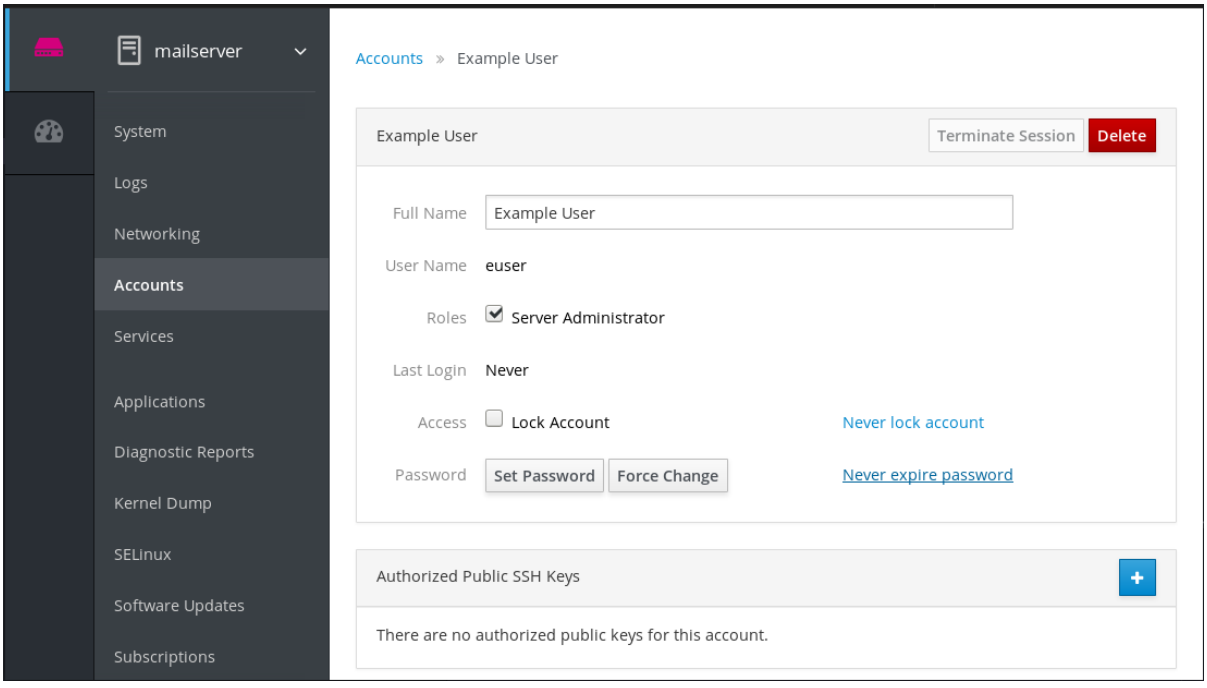
```
$ ssh-keygen
```

- Passwort für den erzeugten SSH-Schlüssel.
- Der Inhalt der Datei **~/.ssh/id_rsa.pub** wird in die Zwischenablage kopiert.

Verfahren

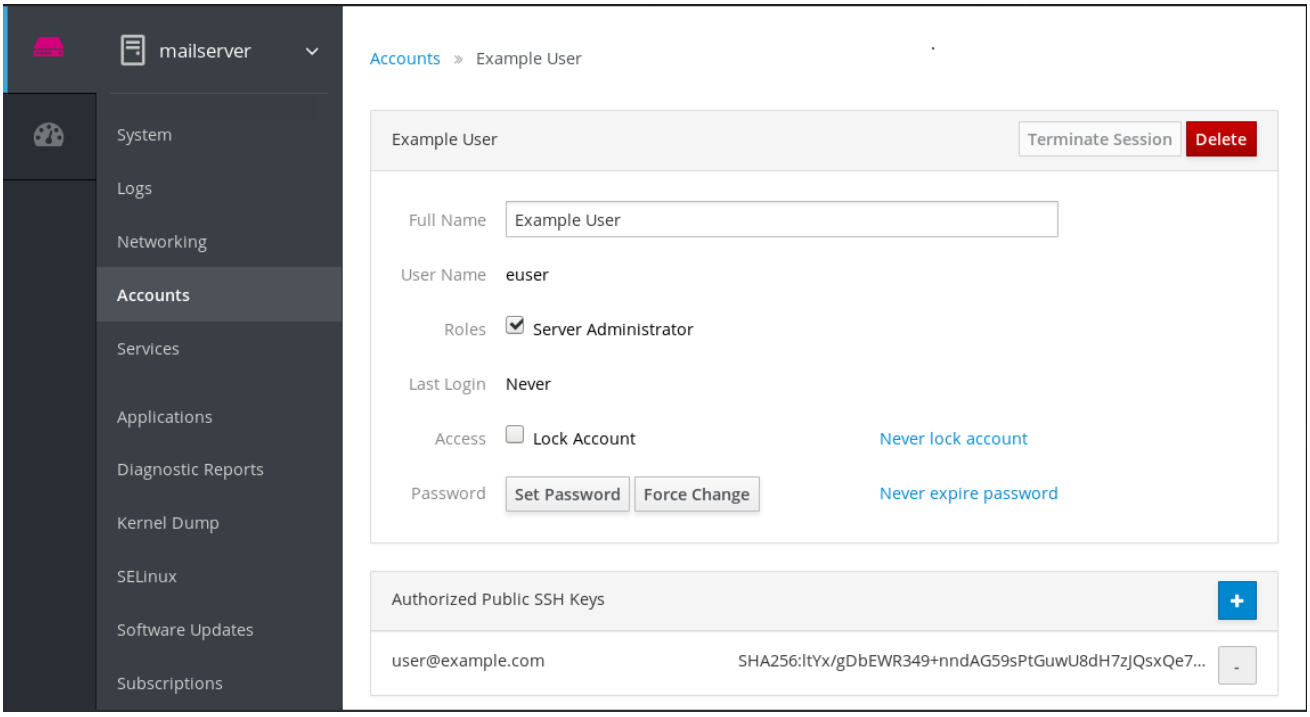
So kopieren Sie den öffentlichen SSH-Schlüssel in ein entferntes System:

1. Öffnen Sie die Web-Konsole.
2. Klicken Sie auf **Dashboard**.
3. Wählen Sie das entfernte System, zu dem Sie den öffentlichen Schlüssel hinzufügen möchten.
4. Gehen Sie in den Systemeinstellungen auf **Accounts**.
5. Wählen Sie das Benutzerkonto, dem Sie den öffentlichen Schlüssel zuweisen möchten.
6. Klicken Sie in den Einstellungen von **Authorized Public SSH Keys** auf die Schaltfläche .



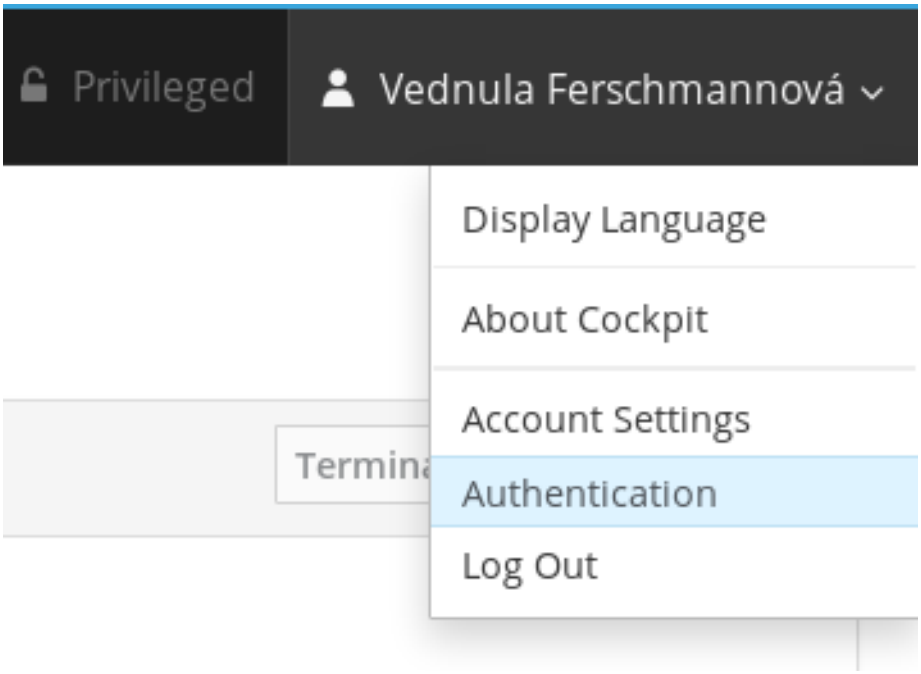
7. Fügen Sie im Dialogfeld **Add public key** den öffentlichen Schlüssel ein, den Sie in der Zwischenablage haben.
8. Klicken Sie auf **Add key**.

An dieser Stelle können Sie den neuen öffentlichen Schlüssel sehen, der dem Benutzerkonto zugewiesen wurde.



So legen Sie den Pfad zum privaten SSH-Schlüssel fest:

1. Gehen Sie zu den Einstellungen in der oberen rechten Ecke.
2. Wählen Sie im Dropdown-Menü **Authentication**.



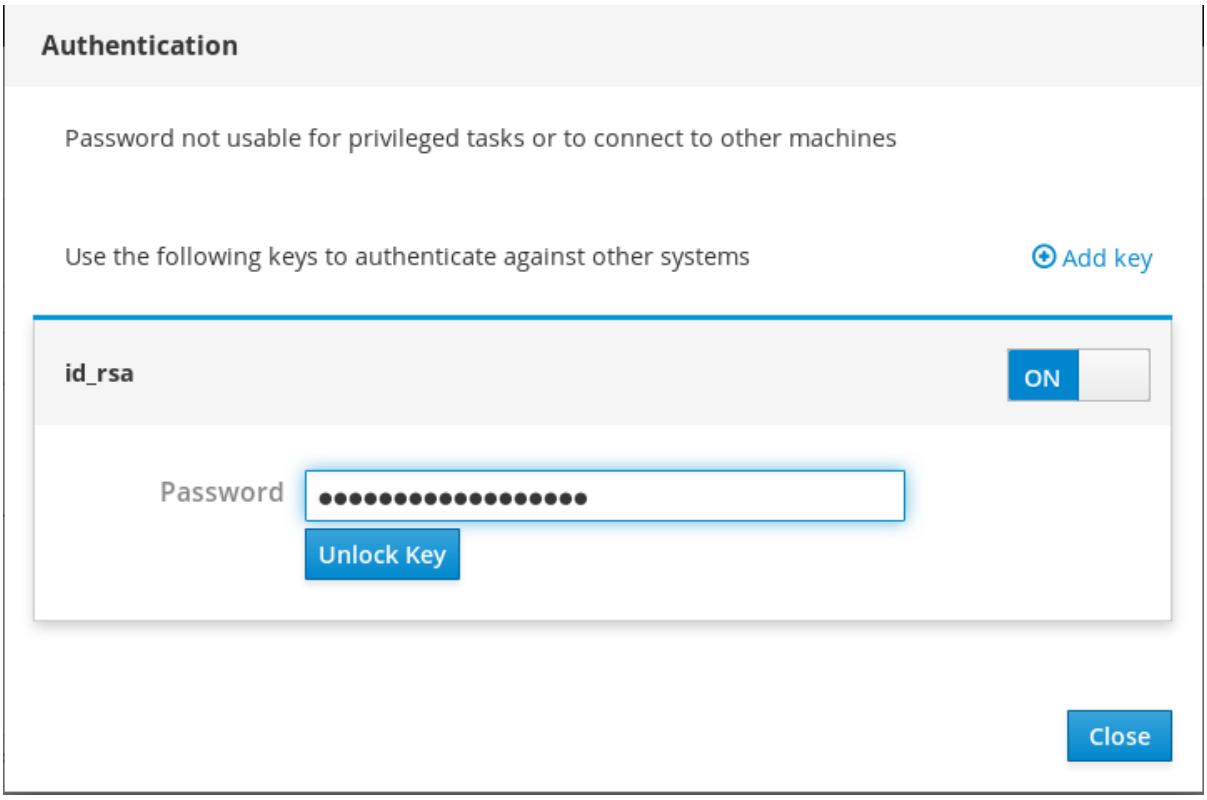
3. Vergewissern Sie sich, dass die Web-Konsole den richtigen Pfad zu dem privaten Schlüssel verwendet, den Sie verwenden möchten.
Die Web-Konsole verwendet standardmäßig die folgenden Pfade für private Schlüssel:

```
~/.ssh/id_rsa
~/.ssh/id_dsa
~/.ssh/id_ed25519
~/.ssh/id_ecdsa
```

Um einen anderen Schlüssel zu verwenden, fügen Sie den Pfad manuell hinzu.

4. Aktivieren Sie die Taste mit der Taste **On/Off**.
   Durch Aktivieren der Taste wird ein Passwort-Dialog geöffnet.

5. Geben Sie das Passwort für den SSH-Schlüssel ein.



6. Klicken Sie auf **Unlock Key**.
   Auf der Registerkarte **Details** können Sie den Zertifikatsbesitzer und den Fingerabdruck überprüfen.

7. Klicken Sie auf **Close**.

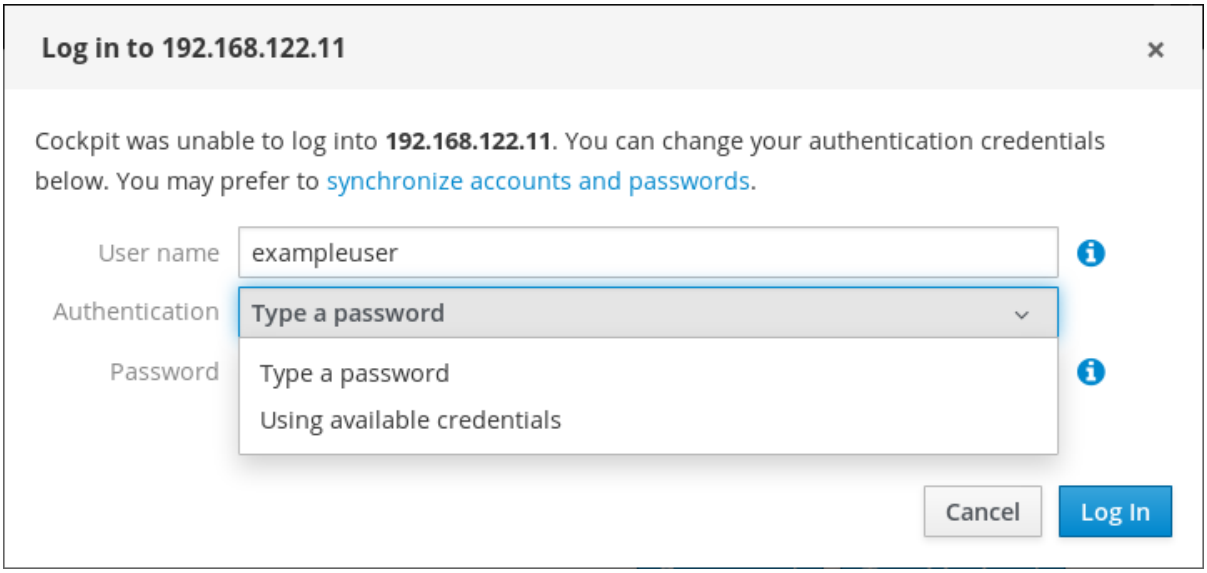
Die RHEL 8 Web-Konsole verwendet jetzt SSH-Schlüssel auf beiden Seiten. Die Systeme verwenden jedoch weiterhin die ursprünglichen Anmeldedaten.

So ändern Sie die Authentifizierungseinstellungen:

1. Melden Sie sich selbst von der Webkonsole ab.
   Nach der Rückmeldung in der Web-Konsole erscheint ein rotes Dreieckssymbol vor dem entfernten System.

2. Klicken Sie auf das System, das versucht, sich mit der Web-Konsole zu verbinden.
   Sie können zwei Schaltflächen auf dem Bildschirm sehen. **Reconnect** und **Troubleshoot**.

3. Klicken Sie auf die Schaltfläche **Troubleshoot**.
   Der Anmeldedialog erscheint.



4. Wählen Sie im Dropdown-Menü **Authentication** die Option **Using available credentials**.

Die Web-Konsole erstellt eine neue, mit SSH-Schlüsseln gesicherte Verbindung. Sie funktioniert sowohl für die Anmeldung an der Web-Konsole als auch für einen Terminal-Zugang.

KAPITEL 29. KONFIGURIEREN VON SINGLE SIGN-ON FÜR DIE RHEL 8 WEB-KONSOLE IN DER IDM-DOMÄNE

Erfahren Sie, wie Sie die von Identity Management (IdM) bereitgestellte Single Sign-on (SSO)-Authentifizierung in der RHEL 8-Webkonsole verwenden.

Vorteile:

- IdM-Domänenadministratoren können die RHEL 8-Webkonsole verwenden, um lokale Rechner zu verwalten.
- Benutzer mit einem Kerberos-Ticket in der IdM-Domäne müssen keine Anmeldedaten angeben, um auf die Webkonsole zuzugreifen.
- Alle der IdM-Domäne bekannten Hosts sind über SSH von der lokalen Instanz der RHEL 8-Webkonsole aus erreichbar.
- Eine Zertifikatskonfiguration ist nicht erforderlich. Der Webserver der Konsole wechselt automatisch zu einem Zertifikat, das von der IdM-Zertifizierungsstelle ausgestellt und von Browsern akzeptiert wird.

Dieses Kapitel umfasst die folgenden Schritte zur Konfiguration von SSO für die Anmeldung an der RHEL-Webkonsole:

1. Fügen Sie der IdM-Domäne über die RHEL 8-Webkonsole Maschinen hinzu.
   Für Details siehe Abschnitt 29.1, »Verbinden eines RHEL 8-Systems mit einer IdM-Domäne über die Webkonsole«.
2. Wenn Sie Kerberos für die Authentifizierung verwenden möchten, müssen Sie ein Kerberos-Ticket auf Ihrem Rechner erhalten.
   Für Details siehe Abschnitt 29.2, »Anmeldung an der Web-Konsole mit Kerberos-Authentifizierung«.
3. Erlauben Sie Administratoren auf dem IdM-Masterserver, jeden Befehl auf jedem Host auszuführen.
   Für Details siehe Abschnitt 29.3, »Aktivieren des sudo-Zugriffs für Domain-Administratoren auf dem IdM-Server«.

Voraussetzungen

- Die RHEL Web-Konsole, die auf RHEL 8-Systemen installiert ist.
  Details finden Sie unter Installieren der Web-Konsole.
- IdM-Client, der auf Systemen mit der RHEL-Webkonsole installiert ist.
  Details finden Sie unter IdM-Client-Installation.

29.1. VERBINDEN EINES RHEL 8-SYSTEMS MIT EINER IDM-DOMÄNE ÜBER DIE WEBKONSOLE

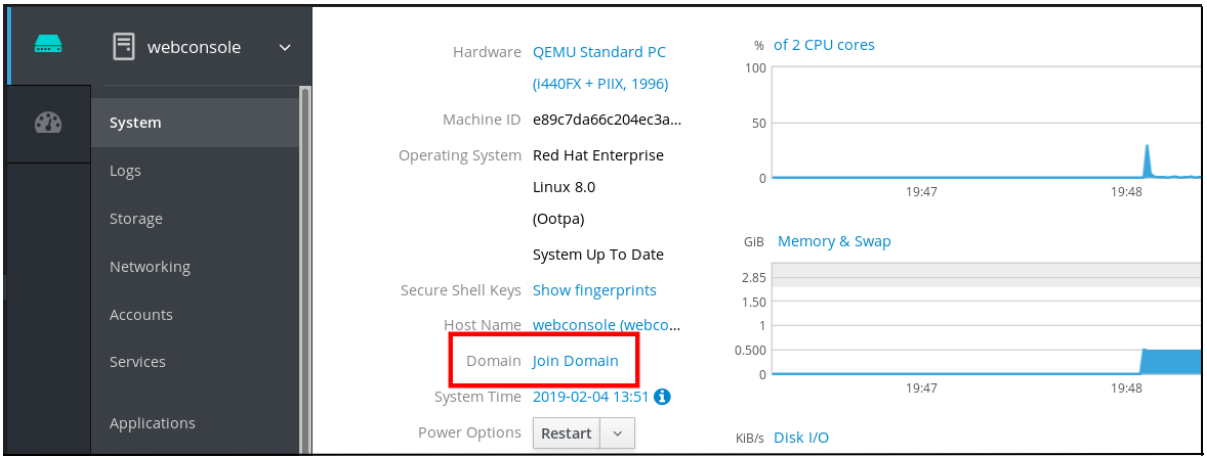
Sie können die Web-Konsole verwenden, um das Red Hat Enterprise Linux 8-System mit der Identity Management (IdM)-Domäne zu verbinden.

Voraussetzungen

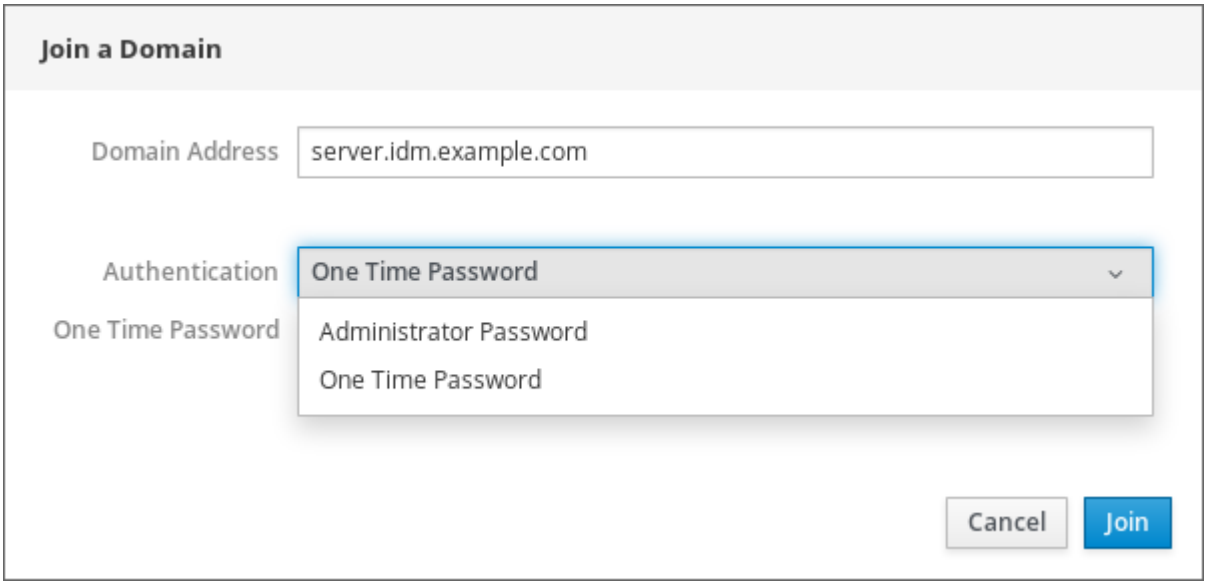
- Die IdM-Domäne läuft und ist von dem Client, dem Sie beitreten möchten, erreichbar.
- Sie haben die IdM-Domänenadministrator-Anmeldeinformationen.

Verfahren

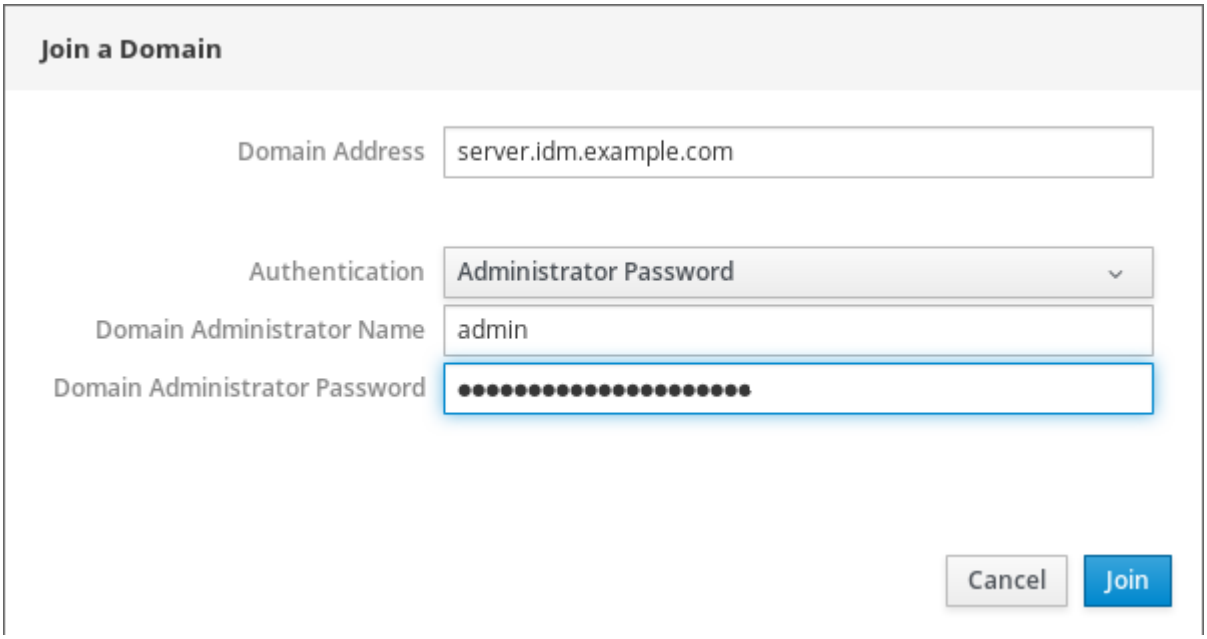
1. Melden Sie sich an der RHEL-Webkonsole an.
   Details finden Sie unter Anmeldung an der Web-Konsole.
2. Öffnen Sie die Registerkarte **System**.
3. Klicken Sie auf **Domäne beitreten**.



4. Geben Sie im Dialogfeld **Join a Domain** den Hostnamen des IdM-Servers in das Feld **Domain Address** ein.
5. Wählen Sie in der Dropdown-Liste **Authentication** aus, ob Sie ein Passwort oder ein Einmalpasswort für die Authentifizierung verwenden möchten.



6. Geben Sie in das Feld **Domain Administrator Name** den Benutzernamen des IdM-Administrationskontos ein.
7. Fügen Sie in das Passwortfeld das Passwort oder Einmalpasswort ein, das Sie zuvor in der Dropdown-Liste **Authentication** ausgewählt haben.
8. Klicken Sie auf **Beitreten**.



Schritte zur Verifizierung

1. Wenn die RHEL 8-Webkonsole keinen Fehler angezeigt hat, wurde das System der IdM-Domäne beigetreten und Sie können den Domänennamen im Bildschirm **System** sehen.

2. Um zu überprüfen, ob der Benutzer ein Mitglied der Domäne ist, klicken Sie auf die Seite Terminal und geben den Befehl **id** ein:

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

Zusätzliche Ressourcen

- Planung der Identitätsverwaltung
- Installieren von Identity Management
- Konfigurieren und Verwalten von Identity Management

29.2. ANMELDUNG AN DER WEB-KONSOLE MIT KERBEROS-AUTHENTIFIZIERUNG

Das folgende Verfahren beschreibt Schritte zum Einrichten des RHEL 8-Systems zur Verwendung der Kerberos-Authentifizierung.

WICHTIG

Mit SSO haben Sie normalerweise keine administrativen Rechte in der Web-Konsole. Dies funktioniert nur, wenn Sie passwortloses sudo konfiguriert haben. Die Web-Konsole fragt nicht interaktiv nach einem sudo-Passwort.

Voraussetzungen

- IdM-Domäne, die in Ihrer Firmenumgebung läuft und erreichbar ist.
  Für Details, siehe Abschnitt 29.1, »Verbinden eines RHEL 8-Systems mit einer IdM-Domäne über die Webkonsole«

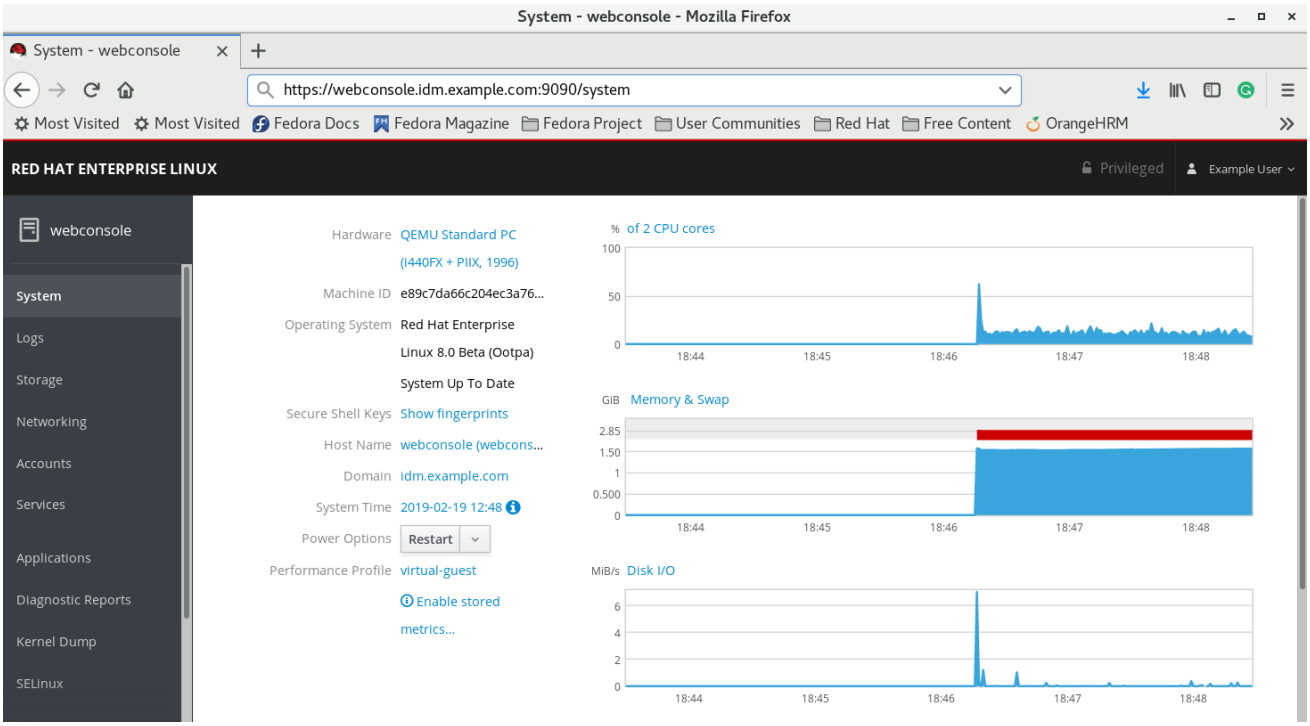
- Aktivieren Sie den Dienst **cockpit.socket** auf entfernten Systemen, zu denen Sie eine Verbindung herstellen und diese mit der RHEL-Webkonsole verwalten möchten.
  Details finden Sie unter Installieren der Web-Konsole.

- Wenn das System kein vom SSSD-Client verwaltetes Kerberos-Ticket verwendet, versuchen Sie, das Ticket mit dem Dienstprogramm **kinit** manuell anzufordern.

Verfahren

Melden Sie sich an der RHEL-Webkonsole mit der folgenden Adresse an: **https://dns_name:9090**.

An diesem Punkt sind Sie erfolgreich mit der RHEL-Webkonsole verbunden und können mit der Konfiguration beginnen.



29.3. AKTIVIEREN DES SUDO-ZUGRIFFS FÜR DOMAIN-ADMINISTRATOREN AUF DEM IDM-SERVER

Das folgende Verfahren beschreibt Schritte, wie Sie Domänenadministratoren erlauben, jeden Befehl auf jedem Host in der Identity Management (IdM)-Domäne auszuführen.

Aktivieren Sie dazu den sudo-Zugriff für die Benutzergruppe **admins**, die bei der Installation des IdM-Servers automatisch angelegt wurde.

Alle Benutzer, die der Gruppe **admins** hinzugefügt wurden, haben sudo-Zugriff, wenn Sie das Skript **ipa-advise** für die Gruppe ausführen.

Voraussetzungen

- Auf dem Server läuft IdM 4.7.1 oder höher.

Verfahren

1. Verbinden Sie sich mit dem IdM-Server.
2. Führen Sie das Skript ipa-advise aus:

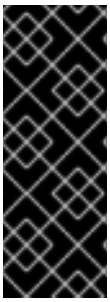
```
$ ipa-advise enable-admins-sudo | sh -ex
```

Wenn die Konsole keinen Fehler anzeigt, hat die Gruppe **admins** Admin-Rechte auf allen Rechnern in der IdM-Domäne.

KAPITEL 30. KONFIGURIEREN DER SMARTCARD-AUTHENTIFIZIERUNG MIT DER WEB-KONSOLE FÜR ZENTRAL VERWALTETE BENUTZER

Konfigurieren Sie die Smartcard-Authentifizierung in der RHEL 8-Webkonsole für Benutzer, die zentral verwaltet werden von:

- Identitätsmanagement
- Active Directory, das im Cross-Forest-Trust mit Identity Management verbunden ist



WICHTIG

Durch die Smartcard-Authentifizierung werden die administrativen Rechte noch nicht erhöht und die Web-Konsole wird im Webbrowser im schreibgeschützten Modus geöffnet.

Sie können administrative Befehle im eingebauten Terminal mit `sudo` ausführen.

Voraussetzungen

- Das System, für das Sie die Smartcard-Authentifizierung verwenden möchten, muss Mitglied einer Active Directory- oder Identity Management-Domäne sein.
  Details zum Beitritt des RHEL 8-Systems zu einer Domäne über die Webkonsole finden Sie unter Beitritt eines RHEL 8-Systems zu einer IdM-Domäne über die Webkonsole .
- Das für die Smartcard-Authentifizierung verwendete Zertifikat muss mit einem bestimmten Benutzer in Identity Management oder Active Directory verknüpft sein.
  Weitere Details zum Zuordnen eines Zertifikats zum Benutzer in Identity Management finden Sie unter Hinzufügen eines Zertifikats zu einem Benutzereintrag in IdM .

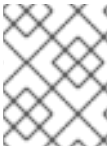
30.1. SMARTCARD-AUTHENTIFIZIERUNG FÜR ZENTRAL VERWALTETE BENUTZER

Eine Smartcard ist ein physisches Gerät, das eine persönliche Authentifizierung mit auf der Karte gespeicherten Zertifikaten ermöglichen kann. Persönliche Authentifizierung bedeutet, dass Sie Smartcards auf die gleiche Weise wie Benutzerpasswörter verwenden können.

Sie können Benutzerdaten in Form eines privaten Schlüssels und eines Zertifikats auf der Smartcard speichern. Für den Zugriff darauf wird spezielle Software und Hardware verwendet. Sie stecken die Smartcard in ein Lesegerät oder eine USB-Buchse und geben anstelle Ihres Passworts den PIN-Code für die Smartcard ein.

Identity Management (IdM) unterstützt Smartcard-Authentifizierung mit:

- Benutzerzertifikate, die von der IdM-Zertifizierungsstelle ausgestellt wurden. Details finden Sie unter Konfigurieren von Identity Management für die Smartcard-Authentifizierung .
- Benutzerzertifikate, die von der Zertifizierungsstelle Active Directory Certificate Service (ADCS) ausgestellt wurden. Details finden Sie unter Konfigurieren von durch ADCS ausgestellten Zertifikaten für die Smartcard-Authentifizierung in IdM.



ANMERKUNG

Wenn Sie mit der Smartcard-Authentifizierung beginnen möchten, lesen Sie die Hardware-Anforderungen: Smart Card-Unterstützung in RHEL8 .

30.2. INSTALLIEREN VON TOOLS ZUR VERWALTUNG UND VERWENDUNG VON CHIPKARTEN

Um Ihre Smartcard zu konfigurieren, benötigen Sie Tools, die Zertifikate erzeugen und auf einer Smartcard speichern können.

Sie müssen:

- Installieren Sie das Paket **gnutls-utils**, das Ihnen bei der Verwaltung von Zertifikaten hilft.
- Installieren Sie das Paket **opensc**, das eine Reihe von Bibliotheken und Dienstprogrammen für die Arbeit mit Chipkarten bereitstellt.
- Starten Sie den Dienst **pcscd**, der mit dem Smartcard-Leser kommuniziert.

Verfahren

1. Installieren Sie die Pakete **opensc** und **gnutls-utils**:

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

2. Starten Sie den Dienst **pcscd**.

```
# systemctl start pcscd
```

Vergewissern Sie sich, dass der Dienst **pcscd** eingeschaltet ist und läuft.

30.3. SPEICHERN EINES ZERTIFIKATS AUF EINER SMARTCARD

Dieser Abschnitt beschreibt die Smartcard-Konfiguration mit dem Tool **pkcs15-init**, das Sie bei der Konfiguration unterstützt:

- Löschen Ihrer Smartcard
- Setzen neuer PINs und optionaler PIN-Unblocking Keys (PUKs)
- Anlegen eines neuen Steckplatzes auf der Chipkarte
- Speichern des Zertifikats, des privaten Schlüssels und des öffentlichen Schlüssels im Steckplatz
- Sperren der Smartcard-Einstellungen (einige Smartcards erfordern diese Art der Finalisierung)

Voraussetzungen

- Das Paket **opensc**, das das Tool **pkcs15-init** enthält, ist installiert.
  Details finden Sie unter Installieren von Tools zum Verwalten und Verwenden von Smartcards .
- Die Karte wird in das Lesegerät eingelegt und mit dem Computer verbunden.

- Sie haben den privaten Schlüssel, den öffentlichen Schlüssel und das Zertifikat auf der Smartcard zu speichern. In diesem Verfahren sind **testuser.key**, **testuserpublic.key** und **testuser.crt** die Namen, die für den privaten Schlüssel, den öffentlichen Schlüssel und das Zertifikat verwendet werden.
- Ihre aktuelle Smartcard-Benutzer-PIN und Sicherheitsbeauftragten-PIN (SO-PIN)

Verfahren

1. Löschen Sie Ihre Smartcard und authentifizieren Sie sich mit Ihrer PIN:

```
$ 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]:
```

   Die Karte ist gelöscht worden.

2. Initialisieren Sie Ihre Smartcard, legen Sie Ihre Benutzer-PIN und PUK sowie die PIN und PUK Ihres Sicherheitsbeauftragten fest:

```
$ 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
```

   Das Werkzeug **pcks15-init** erstellt einen neuen Steckplatz auf der Smartcard.

3. Legen Sie die Beschriftung und die Authentifizierungs-ID für den Steckplatz fest:

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

   Die Beschriftung wird auf einen menschenlesbaren Wert gesetzt, in diesem Fall auf **testuser**. Die **auth-id** muss aus zwei hexadezimalen Werten bestehen, in diesem Fall wird sie auf **01** gesetzt.

4. Speichern und beschriften Sie den privaten Schlüssel in dem neuen Steckplatz auf der Smartcard:

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

ANMERKUNG

Der Wert, den Sie für **--id** angeben, muss beim Speichern Ihres privaten Schlüssels und des Zertifikats gleich sein. Wenn Sie keinen Wert für **--id** angeben, wird vom Tool ein komplizierterer Wert berechnet und es ist daher einfacher, einen eigenen Wert zu definieren.

5. Speichern und beschriften Sie das Zertifikat in dem neuen Steckplatz auf der Smartcard:

```
$ 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. (Optional) Speichern und beschriften Sie den öffentlichen Schlüssel in dem neuen Steckplatz auf der Smartcard:

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

ANMERKUNG

Wenn der öffentliche Schlüssel einem privaten Schlüssel und/oder Zertifikat entspricht, sollten Sie die gleiche ID wie diesen privaten Schlüssel und/oder dieses Zertifikat angeben.

7. (Optional) Bei einigen Smartcards müssen Sie die Karte abschließen, indem Sie die Einstellungen sperren:

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

In diesem Stadium enthält Ihre Smartcard das Zertifikat, den privaten Schlüssel und den öffentlichen Schlüssel in dem neu erstellten Steckplatz. Sie haben auch Ihre Benutzer-PIN und PUK sowie die PIN und PUK des Sicherheitsbeauftragten erstellt.

30.4. AKTIVIEREN DER SMARTCARD-AUTHENTIFIZIERUNG FÜR DIE WEB-KONSOLE

Um die Smartcard-Authentifizierung in der Web-Konsole verwenden zu können, aktivieren Sie die Smartcard-Authentifizierung in der Datei **cockpit.conf**.

Zusätzlich können Sie in derselben Datei die Passwort-Authentifizierung deaktivieren.

Voraussetzungen

- Die RHEL 8 Web-Konsole wurde installiert.
  Details finden Sie unter Installieren der Web-Konsole.

Verfahren

1. Melden Sie sich an der RHEL-Webkonsole mit Administratorrechten an.
   Details finden Sie unter Anmeldung an der Web-Konsole.

2. Klicken Sie auf **Terminal**.

3. Setzen Sie im **/etc/cockpit/cockpit.conf** die **ClientCertAuthentication** auf **yes**:

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

4. Deaktivieren Sie optional die passwortbasierte Authentifizierung in **cockpit.conf** mit:

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

Mit dieser Konfiguration wird die Passwort-Authentifizierung deaktiviert und Sie müssen immer die Smartcard verwenden.

5. Starten Sie die Web-Konsole neu, um sicherzustellen, dass die **cockpit.service** die Änderung akzeptiert:

```
# systemctl restart cockpit
```

30.5. ANMELDUNG AN DER WEB-KONSOLE MIT SMARTCARDS

Sie können Smartcards verwenden, um sich an der Webkonsole anzumelden.

Voraussetzungen

- Ein gültiges Zertifikat, das auf Ihrer Smartcard gespeichert ist und einem Benutzerkonto zugeordnet ist, das in einer Active Directory- oder Identity Management-Domäne erstellt wurde.
- PIN, um die Smartcard zu entsperren.
- Die Chipkarte wurde in das Lesegerät gesteckt.

Verfahren

1. Öffnen Sie Ihren Webbrowser und fügen Sie die Adresse der Webkonsole in die Adressleiste ein. Der Browser fordert Sie auf, die PIN zum Schutz des auf der Smartcard gespeicherten Zertifikats hinzuzufügen.
2. Geben Sie im Dialogfeld **Password Required** die PIN ein und klicken Sie auf **OK**.
3. Wählen Sie im Dialogfeld **User Identification Request** das auf der Smartcard gespeicherte Zertifikat aus.
4. Wählen Sie **Remember this decision**.
   Das System öffnet dieses Fenster beim nächsten Mal nicht.
5. Klicken Sie auf **OK**.

Sie sind nun verbunden und die Web-Konsole zeigt ihren Inhalt an.

30.6. BEGRENZUNG VON BENUTZERSITZUNGEN UND SPEICHER, UM EINEN DOS-ANGRIFF ZU VERHINDERN

Die Zertifikatsauthentifizierung wird durch die Trennung und Isolierung von Instanzen des Webservers **cockpit-ws** gegen Angreifer geschützt, die sich als ein anderer Benutzer ausgeben wollen. Dies führt jedoch einen potenziellen Denial-of-Service-Angriff (DoS) ein: Ein entfernter Angreifer könnte eine große Anzahl von Zertifikaten erstellen und eine große Anzahl von HTTPS-Anfragen an **cockpit-ws** senden, die jeweils ein anderes Zertifikat verwenden.

Um diesen DoS zu verhindern, werden die kollektiven Ressourcen dieser Webserver-Instanzen begrenzt. Standardmäßig sind die Grenzen für die Anzahl der Verbindungen und die Speichernutzung auf 200 Threads und eine Speicherbegrenzung von 75 % (weich) / 90 % (hart) festgelegt.

Das folgende Verfahren beschreibt den Ressourcenschutz durch Begrenzung der Anzahl der Verbindungen und des Speichers.

Verfahren

1. Öffnen Sie im Terminal die Konfigurationsdatei **system-cockpithttps.slice**:

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

2. Schränken Sie **TasksMax** auf *100* und **CPUQuota** auf *30%* ein:

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

3. Um die Änderungen zu übernehmen, starten Sie das System neu:

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

Jetzt schützen die neuen Speicher- und Benutzersitzungslimits den Webserver **cockpit-ws** vor DoS-Angriffen.

30.7. ZUSÄTZLICHE RESSOURCEN

- Weitere Details zum Konfigurieren von Zertifikaten, die von IdM für die Smartcard-Authentifizierung ausgestellt wurden, finden Sie im Abschnitt Konfigurieren von Identity Management für die Smartcard-Authentifizierung.
- Weitere Details zum Konfigurieren von Zertifikaten, die von ADCS für die Smartcard-Authentifizierung ausgestellt wurden, finden Sie im Abschnitt Konfigurieren von Zertifikaten, die von ADCS für die Smartcard-Authentifizierung in IdM ausgestellt wurden.
- Weitere Details zum Konfigurieren von Zertifikaten, die von einer lokalen CA für die Smartcard-Authentifizierung ausgestellt wurden, finden Sie im Abschnitt Konfigurieren und Importieren von lokalen Zertifikaten auf eine Smartcard. :context: system-management-using-the-RHEL-8-web-console