



Red Hat

Red Hat Enterprise Linux 8

Managing systems using the RHEL 8 web console

A guide to using the web console for managing systems in Red Hat Enterprise Linux 8

Red Hat Enterprise Linux 8 Managing systems using the RHEL 8 web console

A guide to using the web console for managing systems in Red Hat Enterprise Linux 8

Legal Notice

Copyright © 2020 Red Hat, Inc.

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

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

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

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

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

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

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

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

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

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

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

All other trademarks are the property of their respective owners.

Abstract

This document describes how to manage physical and virtual Linux-based systems using the RHEL 8 web console. The instructions assume that the server used for management is running in Red Hat Enterprise Linux 8.

Table of Contents

PROVIDING FEEDBACK ON RED HAT DOCUMENTATION	5
CHAPTER 1. GETTING STARTED USING THE RHEL WEB CONSOLE	6
1.1. WHAT IS THE RHEL WEB CONSOLE	6
1.2. INSTALLING THE WEB CONSOLE	7
1.3. LOGGING IN TO THE WEB CONSOLE	7
1.4. CONNECTING TO THE WEB CONSOLE FROM A REMOTE MACHINE	9
1.5. LOGGING IN TO THE WEB CONSOLE USING A ONE-TIME PASSWORD	9
CHAPTER 2. RED HAT WEB CONSOLE ADD-ONS	11
2.1. INSTALLING ADD-ONS	11
2.2. ADD-ONS FOR THE RHEL 8 WEB CONSOLE	11
CHAPTER 3. PERFORMING BASIC SYSTEM ADMINISTRATION TASKS IN THE WEB CONSOLE	12
3.1. WHAT THE RHEL 8 WEB CONSOLE IS AND WHICH TASKS IT CAN BE USED FOR	12
3.2. RESTARTING THE SYSTEM USING THE WEB CONSOLE	12
3.3. SHUTTING DOWN THE SYSTEM USING THE WEB CONSOLE	13
3.4. CONFIGURING THE HOST NAME IN THE WEB CONSOLE	14
3.4.1. Host name	14
3.4.2. Pretty host name in the web console	14
3.4.3. Setting the host name using the web console	15
3.5. JOINING A RHEL 8 SYSTEM TO AN IDM DOMAIN USING THE WEB CONSOLE	17
3.6. CONFIGURING TIME SETTINGS USING THE WEB CONSOLE	19
3.7. OPTIMIZING THE SYSTEM PERFORMANCE USING THE WEB CONSOLE	21
3.7.1. Performance tuning options in the web console	21
3.7.2. Setting a performance profile in the web console	21
3.8. DISABLING SMT TO PREVENT CPU SECURITY ISSUES USING THE WEB CONSOLE	22
CHAPTER 4. REVIEWING LOGS IN THE WEB CONSOLE	25
4.1. REVIEWING LOGS IN THE WEB CONSOLE	25
4.2. FILTERING LOGS IN THE WEB CONSOLE	25
CHAPTER 5. MANAGING USER ACCOUNTS IN THE WEB CONSOLE	27
5.1. SYSTEM USER ACCOUNTS MANAGED IN THE WEB CONSOLE	27
5.2. ADDING NEW ACCOUNTS USING THE WEB CONSOLE	27
5.3. ENFORCING PASSWORD EXPIRATION IN THE WEB CONSOLE	29
5.4. TERMINATING USER SESSIONS IN THE WEB CONSOLE	30
CHAPTER 6. MANAGING SERVICES IN THE WEB CONSOLE	32
6.1. ACTIVATING OR DEACTIVATING SYSTEM SERVICES IN THE WEB CONSOLE	32
6.2. RESTARTING SYSTEM SERVICES IN THE WEB CONSOLE	33
CHAPTER 7. MANAGING NETWORKING IN THE WEB CONSOLE	35
7.1. CONFIGURING NETWORK BONDS USING THE WEB CONSOLE	35
7.1.1. Understanding network bonding	35
7.1.2. Bond modes	36
7.1.3. Adding a new bond using the web console	36
7.1.4. Adding interfaces to the bond using the web console	38
7.1.5. Removing or disabling an interface from the bond using the web console	39
7.1.6. Removing or disabling a bond using the web console	40
7.2. CONFIGURING NETWORK TEAMS USING THE WEB CONSOLE	40
7.2.1. Understanding network teaming	41
7.2.2. Comparison of network teaming and bonding features	41

7.2.3. Adding a new team using the web console	42
7.2.4. Adding new interfaces to the team using the web console	44
7.2.5. Removing or disabling an interface from the team using the web console	44
7.2.6. Removing or disabling a team using the web console	45
7.3. CONFIGURING NETWORK BRIDGES IN THE WEB CONSOLE	46
7.3.1. Adding bridges in the web console	46
7.3.2. Configuring a static IP address in the web console	47
7.3.3. Removing interfaces from the bridge using the web console	50
7.3.4. Deleting bridges in the web console	51
7.4. CONFIGURING VLANS IN THE WEB CONSOLE	52
7.5. CONFIGURING THE WEB CONSOLE LISTENING PORT	53
7.5.1. Allowing a new port on a system with active SELinux	53
7.5.2. Allowing a new port on a system with firewalld	54
7.5.3. Changing the web console port	54
CHAPTER 8. MANAGING FIREWALL USING THE WEB CONSOLE	56
8.1. RUNNING FIREWALL USING THE WEB CONSOLE	56
8.2. STOPPING FIREWALL USING THE WEB CONSOLE	56
8.3. FIREWALLD	57
8.4. ZONES	57
8.5. ZONES IN THE WEB CONSOLE	59
8.6. ENABLING ZONES USING THE WEB CONSOLE	59
8.7. ENABLING SERVICES ON THE FIREWALL USING THE WEB CONSOLE	61
8.8. CONFIGURING CUSTOM PORTS USING THE WEB CONSOLE	63
8.9. DISABLING ZONES USING THE WEB CONSOLE	65
CHAPTER 9. MANAGING PARTITIONS USING THE WEB CONSOLE	67
9.1. DISPLAYING PARTITIONS FORMATTED WITH FILE SYSTEMS IN THE WEB CONSOLE	67
9.2. CREATING PARTITIONS IN THE WEB CONSOLE	68
9.3. DELETING PARTITIONS IN THE WEB CONSOLE	70
9.4. MOUNTING AND UNMOUNTING FILE SYSTEMS IN THE WEB CONSOLE	71
CHAPTER 10. MANAGING STORAGE DEVICES IN THE WEB CONSOLE	73
10.1. MANAGING NFS MOUNTS IN THE WEB CONSOLE	73
10.1.1. Connecting NFS mounts in the web console	73
10.1.2. Customizing NFS mount options in the web console	74
10.2. MANAGING REDUNDANT ARRAYS OF INDEPENDENT DISKS IN THE WEB CONSOLE	76
10.2.1. Creating RAID in the web console	77
10.2.2. Formatting RAID in the web console	78
10.2.3. Using the web console for creating a partition table on RAID	80
10.2.4. Using the web console for creating partitions on RAID	82
10.2.5. Using the web console for creating a volume group on top of RAID	83
10.3. USING THE WEB CONSOLE FOR CONFIGURING LVM LOGICAL VOLUMES	84
10.3.1. Logical Volume Manager in the web console	85
10.3.2. Creating volume groups in the web console	86
10.3.3. Creating logical volumes in the web console	87
10.3.4. Formatting logical volumes in the web console	89
10.3.5. Resizing logical volumes in the web console	91
10.3.6. Related information	92
10.4. USING THE WEB CONSOLE FOR CONFIGURING THIN LOGICAL VOLUMES	92
10.4.1. Creating pools for thin logical volumes in the web console	93
10.4.2. Creating thin logical volumes in the web console	94
10.4.3. Formatting logical volumes in the web console	95
10.5. USING THE WEB CONSOLE FOR CHANGING PHYSICAL DRIVES IN VOLUME GROUPS	97

10.5.1. Adding physical drives to volume groups in the web console	98
10.5.2. Removing physical drives from volume groups in the web console	98
10.6. USING THE WEB CONSOLE FOR MANAGING VIRTUAL DATA OPTIMIZER VOLUMES	99
10.6.1. VDO volumes in the web console	99
10.6.2. Creating VDO volumes in the web console	100
10.6.3. Formatting VDO volumes in the web console	102
10.6.4. Extending VDO volumes in the web console	104
10.7. LOCKING DATA WITH LUKS PASSWORD IN THE RHEL WEB CONSOLE	106
10.7.1. LUKS disk encryption	106
10.7.2. Configuring the LUKS passphrase in the web console	107
10.7.3. Changing the LUKS passphrase in the web console	108
CHAPTER 11. MANAGING SOFTWARE UPDATES IN THE WEB CONSOLE	110
11.1. MANAGING MANUAL SOFTWARE UPDATES IN THE WEB CONSOLE	110
11.2. MANAGING AUTOMATIC SOFTWARE UPDATES IN THE WEB CONSOLE	110
CHAPTER 12. MANAGING SUBSCRIPTIONS IN THE WEB CONSOLE	112
12.1. SUBSCRIPTION MANAGEMENT IN THE WEB CONSOLE	112
12.2. REGISTERING SUBSCRIPTIONS WITH CREDENTIALS IN THE WEB CONSOLE	112
12.3. REGISTERING SUBSCRIPTIONS WITH ACTIVATION KEYS IN THE WEB CONSOLE	115
CHAPTER 13. CONFIGURING KDUMP IN THE WEB CONSOLE	119
13.1. CONFIGURING KDUMP MEMORY USAGE AND TARGET LOCATION IN WEB CONSOLE	119
CHAPTER 14. MANAGING VIRTUAL MACHINES IN THE WEB CONSOLE	122
14.1. OVERVIEW OF VIRTUAL MACHINE MANAGEMENT USING THE WEB CONSOLE	122
14.2. SETTING UP THE WEB CONSOLE TO MANAGE VIRTUAL MACHINES	122
14.3. VIRTUAL MACHINE MANAGEMENT FEATURES AVAILABLE IN THE WEB CONSOLE	123
14.4. DIFFERENCES BETWEEN VIRTUALIZATION FEATURES IN VIRTUAL MACHINE MANAGER AND THE WEB CONSOLE	124
CHAPTER 15. MANAGING REMOTE SYSTEMS IN THE WEB CONSOLE	126
15.1. REMOTE SYSTEM MANAGER IN THE WEB CONSOLE	126
15.2. ADDING REMOTE HOSTS TO THE WEB CONSOLE	127
15.3. REMOVING REMOTE HOSTS FROM THE WEB CONSOLE	129
15.4. SETTING UP SSH FOR REMOTE MANAGEMENT IN THE WEB CONSOLE	130
CHAPTER 16. CONFIGURING SINGLE SIGN-ON FOR THE RHEL 8 WEB CONSOLE IN THE IDM DOMAIN	135
16.1. JOINING A RHEL 8 SYSTEM TO AN IDM DOMAIN USING THE WEB CONSOLE	135
16.2. LOGGING IN TO THE WEB CONSOLE USING KERBEROS AUTHENTICATION	137
16.3. ENABLING ADMIN SUDO ACCESS TO DOMAIN ADMINISTRATORS ON THE IDM SERVER	138
CHAPTER 17. CONFIGURING SMART CARD AUTHENTICATION WITH THE WEB CONSOLE FOR CENTRALLY MANAGED USERS	140
17.1. SMART CARD AUTHENTICATION FOR CENTRALLY MANAGED USERS	140
17.2. INSTALLING TOOLS FOR MANAGING AND USING SMART CARDS	141
17.3. STORING A CERTIFICATE ON A SMART CARD	141
17.4. ENABLING SMART CARD AUTHENTICATION FOR THE WEB CONSOLE	143
17.5. LOGGING IN TO THE WEB CONSOLE WITH SMART CARDS	144
17.6. LIMITING USER SESSIONS AND MEMORY TO PREVENT A DOS ATTACK	144
17.7. ADDITIONAL RESOURCES	145

PROVIDING FEEDBACK ON RED HAT DOCUMENTATION

We appreciate your input on our documentation. Please let us know how we could make it better. To do so:

- For simple comments on specific passages:
 1. Make sure you are viewing the documentation in the *Multi-page HTML* format. In addition, ensure you see the **Feedback** button in the upper right corner of the document.
 2. Use your mouse cursor to highlight the part of text that you want to comment on.
 3. Click the **Add Feedback** pop-up that appears below the highlighted text.
 4. Follow the displayed instructions.
- For submitting more complex feedback, create a Bugzilla ticket:
 1. Go to the [Bugzilla](#) website.
 2. As the Component, use **Documentation**.
 3. Fill in the **Description** field with your suggestion for improvement. Include a link to the relevant part(s) of documentation.
 4. Click **Submit Bug**.

CHAPTER 1. GETTING STARTED USING THE RHEL WEB CONSOLE

The following sections aim to help you install the web console in Red Hat Enterprise Linux 8 and open the web console in your browser. You will also learn how to [add remote hosts](#) and monitor them in the RHEL 8 web console.

Prerequisites

- Installed Red Hat Enterprise Linux 8.
- Enabled networking.
- Registered system with appropriate subscription attached.
To obtain subscription, see link: [Managing subscriptions in the web console](#).

1.1. WHAT IS THE RHEL WEB CONSOLE

The RHEL web console is a Red Hat Enterprise Linux 8 web-based interface designed for managing and monitoring your local system, as well as Linux servers located in your network environment.

The screenshot shows the Red Hat Enterprise Linux 8 Web Console interface. At the top, it displays "RED HAT ENTERPRISE LINUX" and the host name "localhost.localdomain" which is "running Red Hat Enterprise Linux 8.2 Beta (Ootpa)". On the right, there are "Privileged" and "Example User" status indicators. The left sidebar contains navigation links: Overview, Logs, Storage, Networking, Podman Containers, Accounts, Services, Applications, Diagnostic Reports, Kernel Dump, and SELinux. The main content area is divided into four panels: "Health" (warning: Not Registered, Not connected to Insights), "Usage" (CPU: 8% of 1 CPU core, Memory: 1.4 GiB / 1.8 GiB, with a "View graphs" link), "System information" (Model: QEMU Standard PC (Q35 + ICH9, 2009), Machine ID: 6c75e029993047eba776378d550f2676), and "Configuration" (Hostname: localhost.localdomain, System time: 2020-01-20 12:59, Domain: Join Domain).

The RHEL web console enables you a wide range of administration tasks, including:

- Managing services
- Managing user accounts
- Managing and monitoring system services
- Configuring network interfaces and firewall

- Reviewing system logs
- Managing virtual machines
- Creating diagnostic reports
- Setting kernel dump configuration
- Configuring SELinux
- Updating software
- Managing system subscriptions

The RHEL web console uses the same system APIs as you would in a terminal, and actions performed in a terminal are immediately reflected in the RHEL web console.

You can monitor the logs of systems in the network environment, as well as their performance, displayed as graphs. In addition, you can change the settings directly in the web console or through the terminal.

1.2. INSTALLING THE WEB CONSOLE

Red Hat Enterprise Linux 8 includes the RHEL 8 web console installed by default in many installation variants.

If this is not the case on your system, install the **cockpit** package and set up the **cockpit.socket** service to enable the RHEL 8 web console.

Procedure

1. Install the **cockpit** package:

```
# yum install cockpit
```

2. Enable and start the **cockpit.socket** service, which runs a web server:

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

3. If you are using a custom firewall profile, add the **cockpit** service to **firewalld** to open port 9090 in the firewall:

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

Verification steps

1. To verify the previous installation and configuration, you [open the web console](#).

1.3. LOGGING IN TO THE WEB CONSOLE

Use the steps in this procedure for the first login to the RHEL web console using a system user name and password.

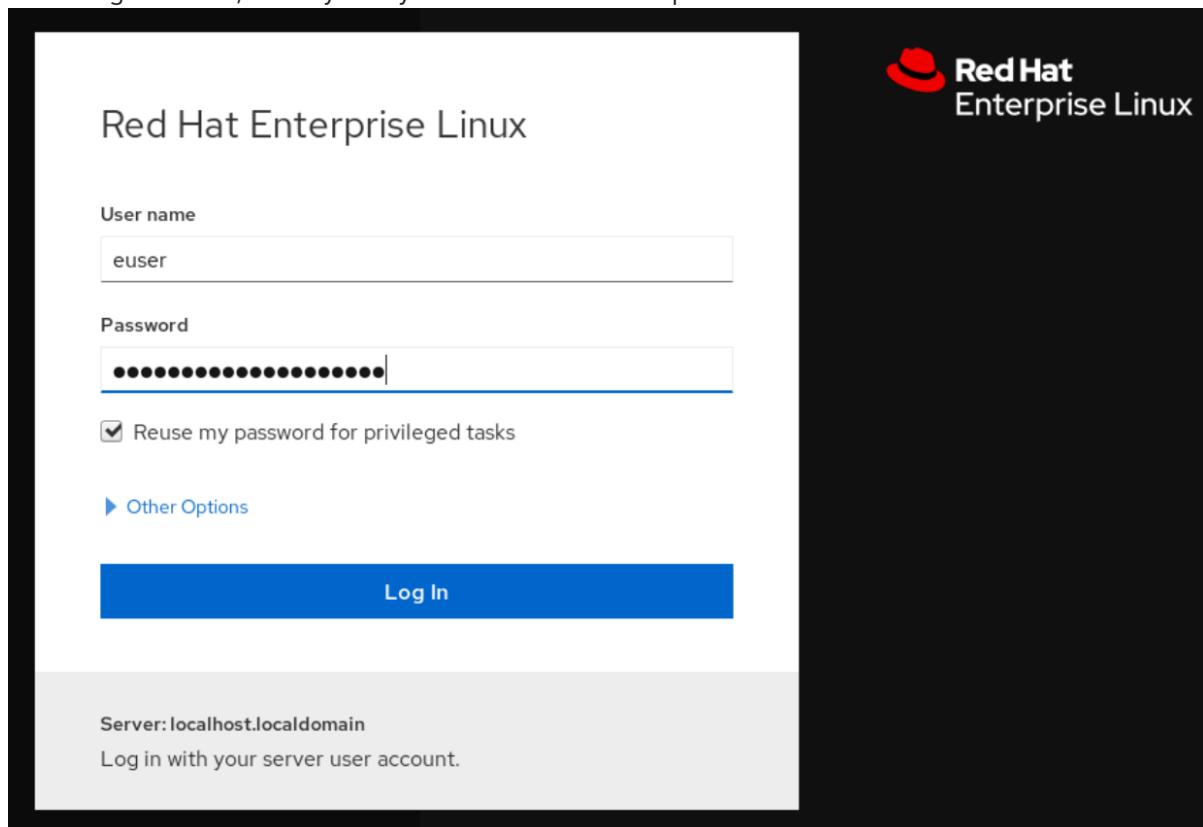
Prerequisites

- Use one of the following browsers for opening the web console:
 - Mozilla Firefox 52 and later
 - Google Chrome 57 and later
 - Microsoft Edge 16 and later
- System user account credentials

The RHEL web console uses a specific PAM stack located at **/etc/pam.d/cockpit**. Authentication with PAM allows you to log in with the user name and password of any local account on the system.

Procedure

1. Open the web console in your web browser:
 - Locally: **https://localhost:9090**
 - Remotely with the server's hostname: **https://example.com:9090**
 - Remotely with the server's IP address: **https://192.0.2.2:9090**
If you use a self-signed certificate, the browser issues a warning. Check the certificate and accept the security exception to proceed with the login.
The console loads a certificate from the **/etc/cockpit/ws-certs.d** directory and uses the last file with a **.cert** extension in alphabetical order. To avoid having to grant security exceptions, install a certificate signed by a certificate authority (CA).
2. In the login screen, enter your system user name and password.



3. Optionally, click the **Reuse my password for privileged tasks** option.

If the user account you are using to log in has sudo privileges, this makes it possible to perform privileged tasks in the web console, such as installing software or configuring SELinux.

4. Click **Log In**.

After successful authentication, the RHEL web console interface opens.

1.4. CONNECTING TO THE WEB CONSOLE FROM A REMOTE MACHINE

It is possible to connect to your web console interface from any client operating system and also from mobile phones or tablets. The following procedure shows how to do it.

Prerequisites

- Device with a supported internet browser, such as:
 - Mozilla Firefox 52 and later
 - Google Chrome 57 and later
 - Microsoft Edge 16 and later
- RHEL 8 server you want to access with an installed and accessible web console. For more information about the installation of the web console see [Installing the web console](#).

Procedure

1. Open your web browser.
2. Type the remote server's address in one of the following formats:
 - a. With the server's host name: **server.hostname.example.com:port_number**
 - b. With the server's IP address: **server.IP_address:port_number**
3. After the login interface opens, log in with your RHEL machine credentials.

1.5. LOGGING IN TO THE WEB CONSOLE USING A ONE-TIME PASSWORD

Complete this procedure to login into the RHEL web console using a one-time password (OTP).



IMPORTANT

It is possible to log in using a one-time password only if your system is part of an Identity Management (IdM) domain with enabled OTP configuration. For more information about OTP in IdM, see [One-time password in Identity Management](#).

Prerequisites

- The RHEL web console has been installed.
For details, see [Installing the web console](#).
- An Identity Management server with enabled OTP configuration.

- A configured hardware or software device generating OTP tokens.

Procedure

1. Open the RHEL web console in your browser:
 - Locally: https://localhost:PORT_NUMBER
 - Remotely with the server hostname: https://example.com:PORT_NUMBER
 - Remotely with the server IP address:
https://EXAMPLE.SERVER.IP.ADDR:PORT_NUMBER
If you use a self-signed certificate, the browser issues a warning. Check the certificate and accept the security exception to proceed with the login.

The console loads a certificate from the **/etc/cockpit/ws-certs.d** directory and uses the last file with a **.cert** extension in alphabetical order. To avoid having to grant security exceptions, install a certificate signed by a certificate authority (CA).
2. The Login window opens. In the Login window, enter your system user name and password.
3. Generate a one-time password on your device.
4. Enter the one-time password into a new field that appears in the web console interface after you confirm your password.
5. Click **Log in**.
6. Successful login takes you to the **Overview** page of the web console interface.

CHAPTER 2. RED HAT WEB CONSOLE ADD-ONS

2.1. INSTALLING ADD-ONS

The **cockpit** package is a part of Red Hat Enterprise Linux 8 by default. To be able to use add-on applications you must install them separately.

Prerequisites

- Installed and enabled **cockpit** package. If you need to install web console first, check the [installation](#) section.

Procedure

- Install an add-on.

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

2.2. ADD-ONS FOR THE RHEL 8 WEB CONSOLE

The following table lists available add-on applications for the RHEL 8 web console.

Feature name	Package name	Usage
Composer	cockpit-composer	Building custom OS images
Dashboard	cockpit-dashboard	Managing multiple servers in one UI
Machines	cockpit-machines	Managing libvirt virtual machines
PackageKit	cockpit-packagekit	Software updates and application installation (usually installed by default)
PCP	cockpit-pcp	Persistent and more fine-grained performance data (installed on demand from the UI)
podman	cockpit-podman	Managing podman containers (available from RHEL 8.1)
Session Recording	cockpit-session-recording	Recording and managing user sessions

CHAPTER 3. PERFORMING BASIC SYSTEM ADMINISTRATION TASKS IN THE WEB CONSOLE

In this chapter, you will learn how to perform basic system administration tasks, such as restart, shutdown, or basic configuration, using the web console.

3.1. WHAT THE RHEL 8 WEB CONSOLE IS AND WHICH TASKS IT CAN BE USED FOR

The RHEL 8 web console is an interactive server administration interface. It interacts directly with the operating system from a real Linux session in a browser.

The web console enables to perform these tasks:

- Monitoring basic system features, such as hardware information, time configuration, performance profiles, connection to the realm domain
- Inspecting system log files
- Managing network interfaces and configuring firewall
- Handling docker images
- Managing virtual machines
- Managing user accounts
- Monitoring and configuring system services
- Creating diagnostic reports
- Setting kernel dump configuration
- Managing packages
- Configuring SELinux
- Updating software
- Managing system subscriptions
- Accessing the terminal

For more information on installing and using the RHEL 8 web console, see [Managing systems using the RHEL 8 web console](#).

3.2. RESTARTING THE SYSTEM USING THE WEB CONSOLE

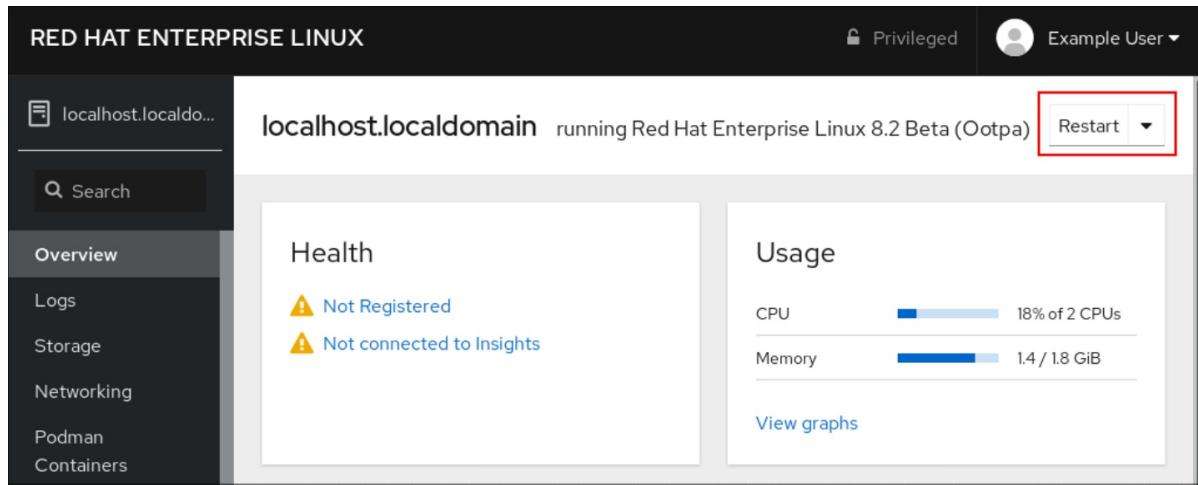
This procedure uses the web console to restart a RHEL system that the web console is attached to.

Prerequisites

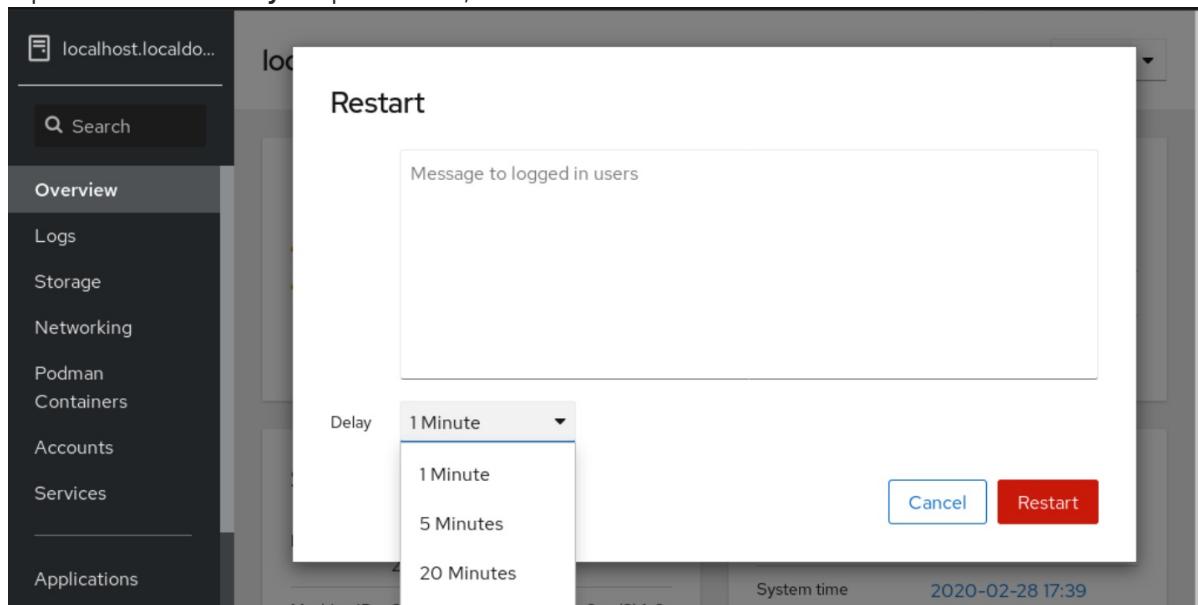
- The web console is installed and accessible.
For details, see [Installing the web console](#).

Procedure

1. Log into the RHEL 8 web console.
For details, see [Logging in to the web console](#).
2. Click **Overview**.
3. Click the **Restart** restart button.



4. If any users are logged into the system, write a reason for the restart in the **Restart** dialog box.
5. Optional: In the **Delay** drop down list, select a time interval.



6. Click **Restart**.

3.3. SHUTTING DOWN THE SYSTEM USING THE WEB CONSOLE

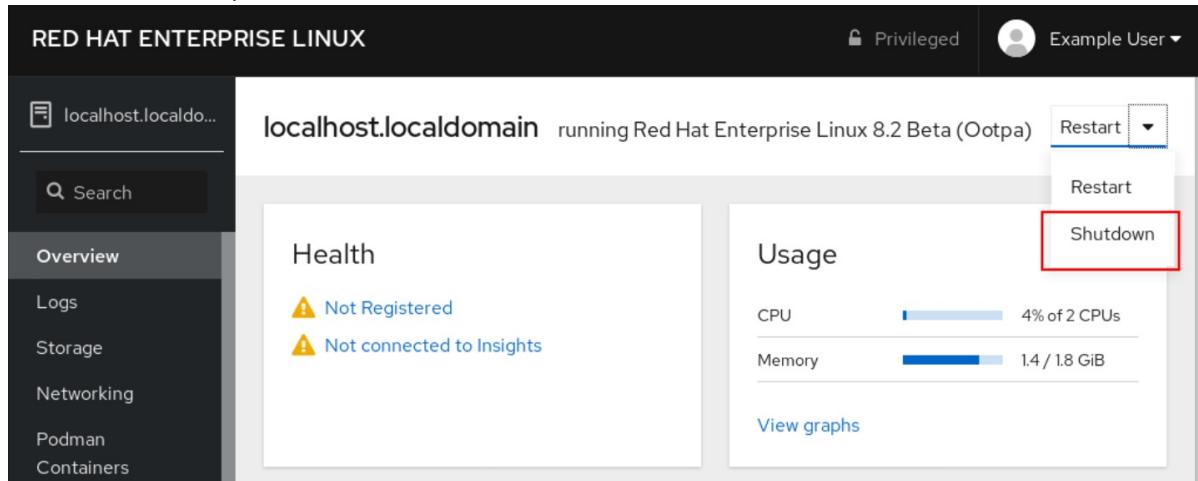
This procedure uses the web console to shut down a RHEL system that the web console is attached to.

Prerequisites

- The web console is installed and accessible.
For details, see [Installing the web console](#).

Procedure

1. Log into the RHEL 8 web console.
For details, see [Logging in to the web console](#).
2. Click **Overview**.
3. In the **Restart** drop down list, select **Shutdown**.



4. If any users are logged in to the system, write a reason for the shutdown in the **Shutdown** dialog box.
5. Optional: In the **Delay** drop down list, select a time interval.
6. Click **Shutdown**.

3.4. CONFIGURING THE HOST NAME IN THE WEB CONSOLE

You can use the web console to configure different forms of the host name on the system that the web console is attached to.

3.4.1. Host name

The host name identifies the system. By default, the host name is set to **localhost**, but you can change it.

A host name consists of two parts:

Host name

It is a unique name which identifies a system.

Domain

Add the domain as a suffix behind the host name when using a system in a network and when using names instead of just IP addresses.

A host name with an attached domain name is called a fully qualified domain name (FQDN). For example: **mymachine.example.com**.

Host names are stored in the **/etc/hostname** file.

3.4.2. Pretty host name in the web console

You can configure a pretty host name in the RHEL web console. The pretty host name is a host name with capital letters, spaces, and so on.

The pretty host name displays in the web console, but it does not have to correspond with the host name.

Example 3.1. Host name formats in the web console

Pretty host name

My Machine

Host name

mymachine

Real host name - fully qualified domain name (FQDN)

mymachine.idm.company.com

3.4.3. Setting the host name using the web console

This procedure sets the real host name or the pretty host name in the web console.

Prerequisites

- The web console is installed and accessible.
For details, see [Installing the web console](#).

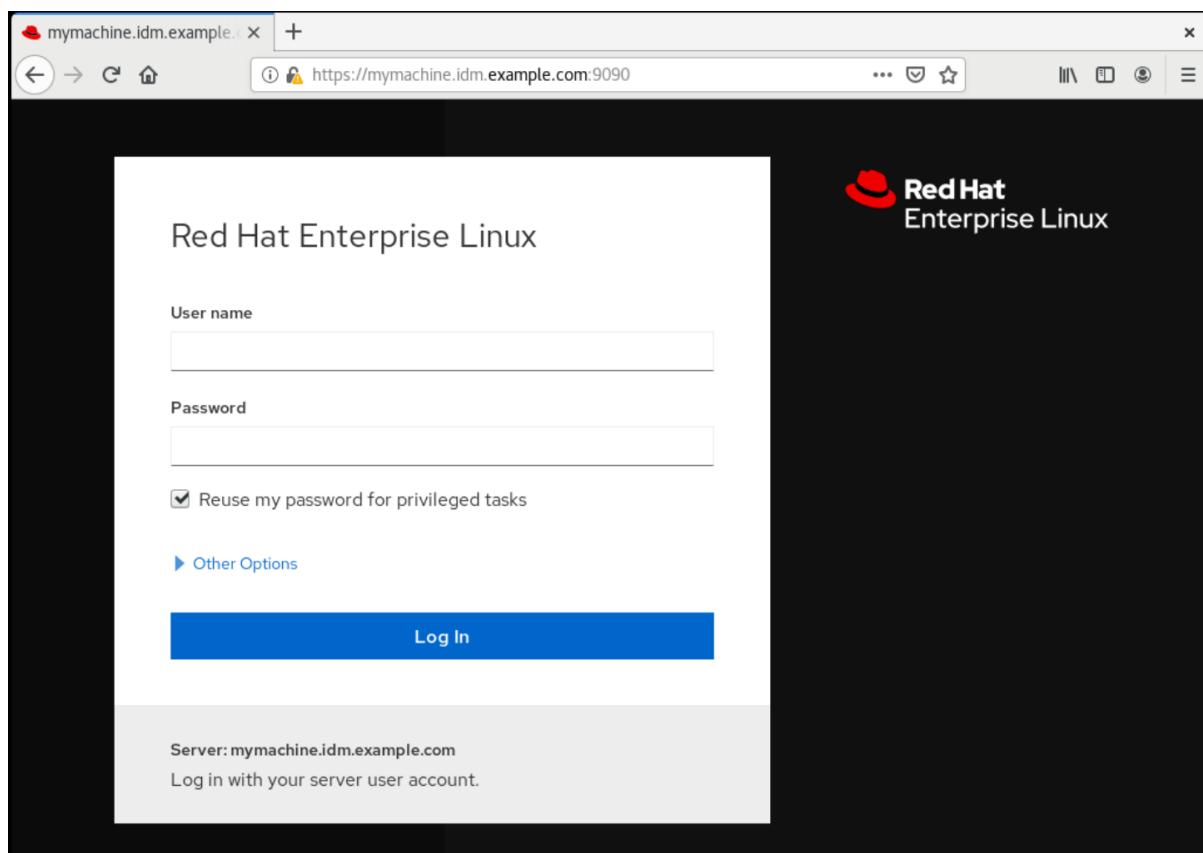
Procedure

1. Log into the RHEL 8 web console.
For details, see [Logging in to the web console](#).
2. Click **Overview**.
3. Click **edit** next to the current host name.

4. In the **Change Host Name** dialog box, enter the host name in the **Pretty Host Name** field.
5. The **Real Host Name** field attaches a domain name to the pretty name.
You can change the real host name manually if it does not correspond with the pretty host name.
6. Click **Change**.

Verification steps

1. Log out from the web console.
2. Reopen the web console by entering an address with the new host name in the address bar of your browser.



3.5. JOINING A RHEL 8 SYSTEM TO AN IDM DOMAIN USING THE WEB CONSOLE

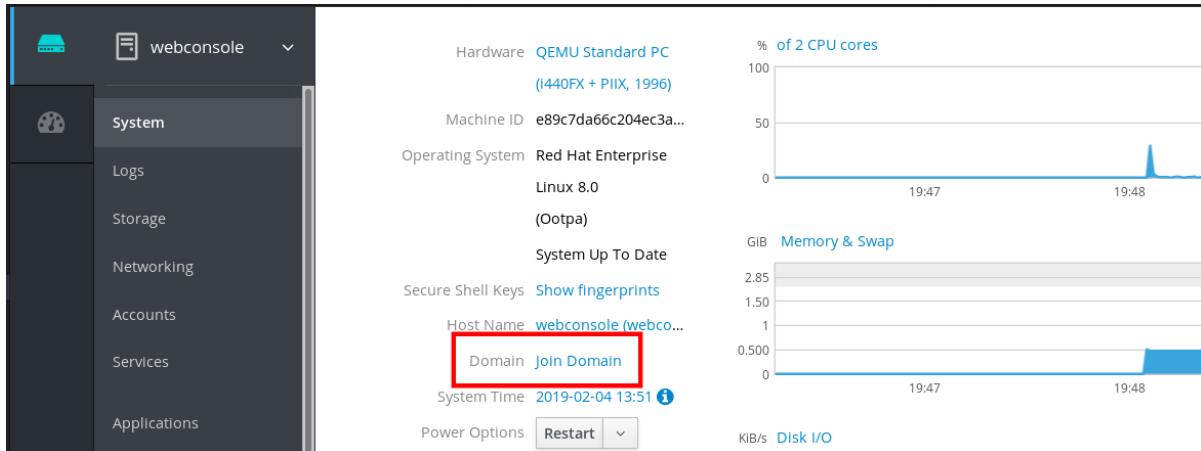
This procedure uses the web console to join the Red Hat Enterprise Linux 8 system to the Identity Management (IdM) domain.

Prerequisites

- The IdM domain is running and reachable from the client you want to join.
- You have the IdM domain administrator credentials.

Procedure

1. Log into the RHEL web console.
For details, see [Logging in to the web console](#).
2. Open the **System** tab.
3. Click **Join Domain**.



4. In the **Join a Domain** dialog box, enter the host name of the IdM server in the **Domain Address** field.
5. In the **Authentication** drop down list, select if you want to use a password or a one-time password for authentication.

The 'Join a Domain' dialog box has a 'Domain Address' field containing 'server.idm.example.com'. Below it is an 'Authentication' dropdown menu set to 'One Time Password', with two options: 'Administrator Password' and 'One Time Password'. At the bottom are 'Cancel' and 'Join' buttons.

6. In the **Domain Administrator Name** field, enter the user name of the IdM administration account.
7. In the password field, add the password or one-time password according to what you selected in the **Authentication** drop down list earlier.
8. Click **Join**.

Join a Domain

Domain Address	server.idm.example.com
Authentication	Administrator Password
Domain Administrator Name	admin
Domain Administrator Password	*****

Cancel **Join**

Verification steps

1. If the RHEL 8 web console did not display an error, the system has been joined to the IdM domain and you can see the domain name in the **System** screen.
2. To verify that the user is a member of the domain, click the Terminal page and type the **id** command:

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

Additional resources

- [Planning Identity Management](#)
- [Installing Identity Management](#)
- [Configuring and managing Identity Management](#)

3.6. CONFIGURING TIME SETTINGS USING THE WEB CONSOLE

This procedure sets a time zone and synchronizes the system time with a Network Time Protocol (NTP) server.

Prerequisites

- The web console is installed and accessible.
For details, see [Installing the web console](#).

Procedure

1. Log in to the RHEL 8 web console.
For details, see [Logging in to the web console](#).

- Click the current system time in **Overview**.

System information

Model	QEMU Standard PC (Q35 + ICH9, 2009)
Machine ID	9fa031b4e58948b09d13e6ecd3b1c9de

Configuration

Hostname	mymachine (mymachine.idm.example.com) edit
System time	2020-03-23 21:44
Domain	Join Domain

- In the **Change System Time** dialog box, change the time zone if necessary.

- In the **Set Time** drop down menu, select one of the following:

Manually

Use this option if you need to set the time manually, without an NTP server.

Automatically using NTP server

This is a default option, which synchronizes time automatically with the preset NTP servers.

Automatically using specific NTP servers

Use this option only if you need to synchronize the system with a specific NTP server.

Specify the DNS name or the IP address of the server.

- Click **Change**.

Change System Time

Time Zone: Europe/Prague

Set Time:

- Automatically using NTP
- Manually
- Automatically using NTP
- Automatically using specific NTP servers

Verification steps

- Check the system time displayed in the **System** tab.

Additional resources

- [Using the Chrony suite to configure NTP](#).

3.7. OPTIMIZING THE SYSTEM PERFORMANCE USING THE WEB CONSOLE

In the web console, you can set a performance profile to optimize the performance of the system for a selected task.

3.7.1. Performance tuning options in the web console

Red Hat Enterprise Linux 8 provides several performance profiles that optimize the system for the following tasks:

- Systems using the desktop
- Throughput performance
- Latency performance
- Network performance
- Low power consumption
- Virtual machines

The **tuned** service optimizes system options to match the selected profile.

In the web console, you can set which performance profile your system uses.

Additional resources

- For details about the **tuned** service, see [Monitoring and managing system status and performance](#).

3.7.2. Setting a performance profile in the web console

This procedure uses the web console to optimize the system performance for a selected task.

Prerequisites

- The web console is installed and accessible.
For details, see [Installing the web console](#).

Procedure

1. Log into the RHEL 8 web console.
For details, see [Logging in to the web console](#).
2. Click **Overview**.
3. In the **Performance Profile** field, click the current performance profile.

The screenshot shows the Red Hat Enterprise Linux 8 web console interface. At the top, there's a header bar with the title "RED HAT ENTERPRISE LINUX", a lock icon labeled "Privileged", a user icon labeled "Example User", and some system status indicators for CPU and Memory usage.

The left sidebar has a "Overview" tab selected, along with other options like Logs, Storage, Networking, Podman, Containers, Accounts, and Services.

The main content area has two sections: "System information" and "Configuration".

- System information:** Shows the Model as QEMU Standard PC (Q35 + ICH9, 2009) and the Machine ID as 9fa031b4e58948b09d13e6ecd3b1c9de.
- Configuration:** Shows the Hostname as mymachine (mymachine.idm.example.com), System time as 2020-03-23 21:44, and Domain as Join Domain. The "Performance profile" field is highlighted with a red box and shows "virtual-guest" selected.

4. In the **Change Performance Profile** dialog box, change the profile if necessary.
5. Click **Change Profile**.

This screenshot shows a modal dialog titled "Change Performance Profile". It lists three performance profiles:

- throughput-performance: Broadly applicable tuning that provides excellent performance across a variety of common server workloads.
- virtual-guest**: Optimized for running inside a virtual guest. This profile is highlighted with a blue background and has a "recommended" badge.
- virtual-host: Optimized for running KVM guests.

At the bottom of the dialog are "Cancel" and "Change Profile" buttons.

Verification steps

- The **Overview** tab now shows the selected performance profile.

3.8. DISABLING SMT TO PREVENT CPU SECURITY ISSUES USING THE WEB CONSOLE

This section describes how to disable Simultaneous Multi Threading (SMT) in case of attacks that misuse CPU SMT. Disabling SMT can mitigate security vulnerabilities, such as L1TF or MDS.



IMPORTANT

Disabling SMT might lower the system performance.

Prerequisites

- The web console must be installed and accessible.
For details, see [Installing the web console](#).

Procedure

- Log in to the RHEL 8 web console.
For details, see [Logging in to the web console](#).
- Click **System**.
- In the **Hardware** item, click the hardware information.

The screenshot shows the RHEL 8 Web Console interface. On the left, there's a sidebar with icons for Home, System, Logs, Storage, Networking, Accounts, Services, and Applications. The 'System' icon is highlighted. The main area has a header 'localhost' with a dropdown arrow. Below the header, the 'Hardware' section is expanded, showing 'LENOVO 20L8S2N80D' and a tooltip 'Click to see system hardware information'. Other sections shown include 'Operating System' (System Up To Date), 'Secure Shell Keys' (Show fingerprints), 'Host Name' (localhost.localdomain), 'Domain' (Join Domain), 'System Time' (2019-07-01 17:51), 'Power Options' (Restart dropdown), and 'Performance Profile' (desktop).

- In the **CPU Security** item, click **Mitigations**.
If this link is not present, it means that your system does not support SMT, and therefore is not vulnerable.
- In the **CPU Security Toggles**, switch on the **Disable simultaneous multithreading (nosmt)** option.

The screenshot shows a dialog box titled 'CPU Security Toggles'. It contains a paragraph about software-based workarounds for CPU security issues, noting they reduce performance. Below this is a section for 'Disable simultaneous multithreading (nosmt)' with a checked checkbox and a 'Read more...' link. At the bottom are 'Cancel' and 'Save and reboot' buttons.

- Click on the **Save and reboot** button.

After the system restart, the CPU no longer uses SMT.

Additional resources

For more details on security attacks that you can prevent by disabling SMT, see:

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

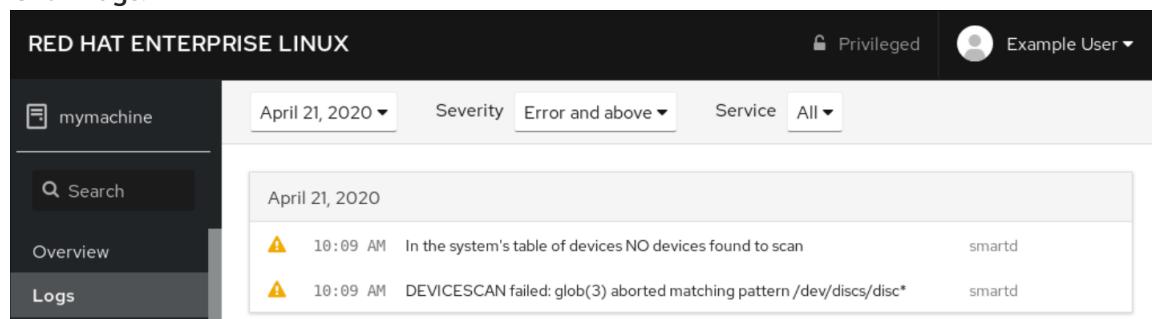
CHAPTER 4. REVIEWING LOGS IN THE WEB CONSOLE

4.1. REVIEWING LOGS IN THE WEB CONSOLE

The RHEL 8 web console Logs section is a UI for the **journalctl** utility. This section describes how to access system logs in the web console interface.

Prerequisites

- The RHEL 8 web console has been installed.
For details, see [Installing the web console](#) .Procedure
- 1. Log in to the RHEL web console.
For details, see [Logging in to the web console](#) .
- 2. Click **Logs**.



- 3. Open log entry details by clicking on your selected log entry in the list.

You can filter the logs by date, severity or service. For more information, see [Filtering logs in the web console](#).

4.2. FILTERING LOGS IN THE WEB CONSOLE

This section shows how to filter log entries in the web console.

Prerequisites

- The web console interface must be installed and accessible.
For details, see [Installing the web console](#) .

Procedure

1. Log in to the RHEL 8 web console.
For details, see [Logging in to the web console](#) .
2. Click **Logs**.
3. By default, web console shows logs from your current boot. To filter by a different time range, click on the drop down menu with your current date and choose a preferred option.

RED HAT ENTERPRISE LINUX

mymachine

April 21, 2020

Severity: Error and above

Service: All

Recent	clipboard: property contains no data (zero length)	spice-vdagent
Current boot	In the system's table of devices NO devices found to scan	smartd
Previous boot	DEVICESCAN failed: glob(3) aborted matching pattern /dev/disks/disc*	smartd
Last 24 hours		
Last 7 days		

4. Error and above severity logs list is shown by default. To filter by different severity, click on the Error and above drop-down menu and choose a preferred severity.

RED HAT ENTERPRISE LINUX

mymachine

April 21, 2020

Severity: Error and above

Service: All

Everything	clipboard: property contains no data (zero length)	spice-vdagent
Only Emergency	In the system's table of devices NO devices found to scan	smartd
Alert and above	DEVICESCAN failed: glob(3) aborted matching pattern /dev/disks/disc*	smartd
Critical and above		
Error and above		
Warning and above		
Notice and above		
Info and above		
Debug and above		

5. By default, web console shows logs for all services. To filter logs for a particular service, click on the All drop-down menu and select a service name.

RED HAT ENTERPRISE LINUX

mymachine

April 21, 2020

Severity: Error and above

Service: All

All	clipboard: property contains no data (zero length)	spice-vdagent
dbus-daemon	In the system's table of devices NO devices found to scan	smartd
dnf	DEVICESCAN failed: glob(3) aborted matching pattern /dev/disks/disc*	smartd
gdm-password		
NetworkManager		
PackageKit		
smartd		
spice-vdagent		
systemd		
systemd-tmpfiles		

6. To open a log entry, click on a selected log.

CHAPTER 5. MANAGING USER ACCOUNTS IN THE WEB CONSOLE

The RHEL web console offers an interface for adding, editing, and removing system user accounts. After reading this section, you will know:

- From where the existing accounts come from.
- How to add new accounts.
- How to set password expiration.
- How and when to terminate user sessions.

Prerequisites

- Being logged into the RHEL web console with an account that has administrator permissions assigned. For details, see [Logging in to the RHEL web console](#).

5.1. SYSTEM USER ACCOUNTS MANAGED IN THE WEB CONSOLE

With user accounts displayed in the RHEL web console you can:

- Authenticate users when accessing the system.
- Set them access rights to the system.

The RHEL web console displays all user accounts located in the system. Therefore, you can see at least one user account just after the first login to the web console.

After logging into the RHEL web console, you can perform the following operations:

- Create new users accounts.
- Change their parameters.
- Lock accounts.
- Terminate user sessions.

5.2. ADDING NEW ACCOUNTS USING THE WEB CONSOLE

Use the following steps for adding user accounts to the system and setting administration rights to the accounts through the RHEL web console.

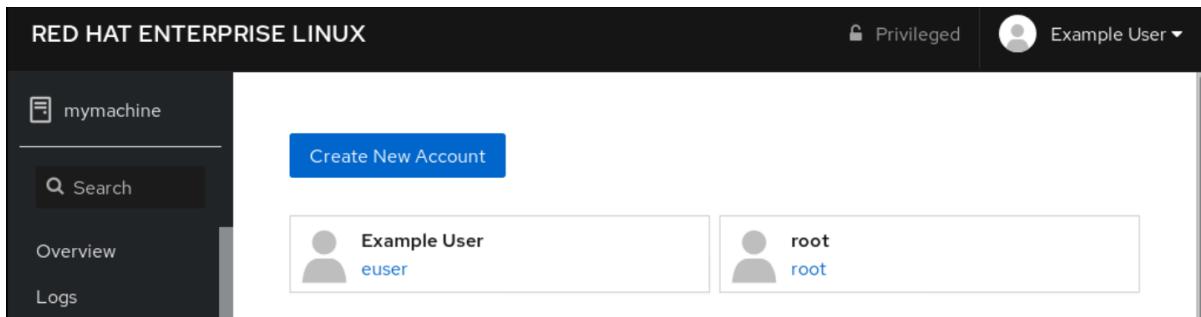
Prerequisites

- The RHEL web console must be installed and accessible. For details, see [Installing the web console](#).

Procedure

1. Log in to the RHEL web console.

2. Click **Accounts**.
3. Click **Create New Account**.



4. In the **Full Name** field, enter the full name of the user.
The RHEL web console automatically suggests a user name from the full name and fills it in the **User Name** field. If you do not want to use the original naming convention consisting of the first letter of the first name and the whole surname, update the suggestion.
5. In the **Password/Confirm** fields, enter the password and retype it for verification that your password is correct. The color bar placed below the fields shows you security level of the entered password, which does not allow you to create a user with a weak password.

The screenshot shows the 'Create New Account' dialog box. It contains the following fields:

- Full Name:** Example User
- User Name:** euser
- Password:** [REDACTED]
- Confirm:** [REDACTED]
- Access:** Lock Account

Below the password fields is a green progress bar indicating the password strength, with the text "Excellent password" displayed above it. At the bottom right are 'Cancel' and 'Create' buttons.

6. Click **Create** to save the settings and close the dialog box.
7. Select the newly created account.
8. Select **Server Administrator** in the **Roles** item.

Example User		
Full Name	Example User	
User Name	euser	
Roles	<input checked="" type="checkbox"/> Server Administrator	
Last Login	Logged In	
Access	<input type="checkbox"/> Lock Account	Never lock account
Password	Set Password	Force Change
	Never expire password	

Now you can see the new account in the **Accounts** settings and you can use the credentials to connect to the system.

5.3. ENFORCING PASSWORD EXPIRATION IN THE WEB CONSOLE

By default, user accounts have set passwords to never expire. To enforce password expiration, as administrator, set system passwords to expire after a defined number of days.

When the password expires, the next login attempt will prompt for a password change.

Procedure

1. Log in to the RHEL 8 web console interface.
2. Click **Accounts**.
3. Select the user account for which to enforce password expiration.
4. In the user account settings, click **Never expire password**.
5. In the **Password Expiration** dialog box, select **Require password change every ... days** and enter a positive whole number representing the number of days when the password expires.

Password Expiration

Never expire password

Require password change every days

[Cancel](#) [Change](#)

6. Click **Change**.

To verify the settings, open the account settings. The RHEL 8 web console displays a link with the date of expiration.

Example User		Terminate Session Delete
Full Name	Example User	
User Name	euser	
Roles	<input checked="" type="checkbox"/> Server Administrator	
Last Login	Logged In	
Access	<input type="checkbox"/> Lock Account	Never lock account
Password	Set Password Force Change	Require password change on Oct 20, 2020

5.4. TERMINATING USER SESSIONS IN THE WEB CONSOLE

A user creates user sessions when logging into the system. Terminating user sessions means to log the user out from the system.

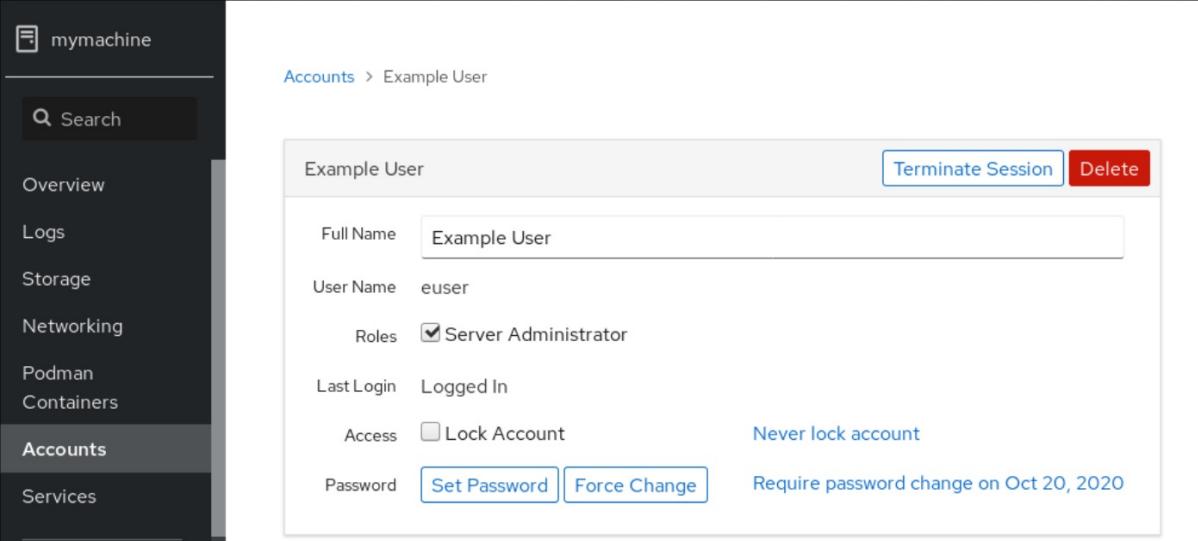
It can be helpful if you need to perform administrative tasks sensitive to configuration changes, for example, system upgrades.

In each user account in the RHEL 8 web console, you can terminate all sessions for the account except for the web console session you are currently using. This prevents you from cutting yourself off the system.

Procedure

1. Log in to the RHEL 8 web console.

2. Click **Accounts**.
3. Click the user account for which you want to terminate the session.
4. Click the **Terminate Session** button.



The screenshot shows the RHEL Web Console interface. On the left, there's a sidebar with links: Overview, Logs, Storage, Networking, Podman Containers, **Accounts**, and Services. The 'Accounts' link is currently selected. The main content area shows the 'Accounts > Example User' page. The 'Example User' details are listed: Full Name (Example User), User Name (euser), Roles (Server Administrator checked), Last Login (Logged In), Access (Lock Account checkbox), and Password (Set Password, Force Change buttons). At the top right, there are 'Terminate Session' and 'Delete' buttons, with 'Terminate Session' being highlighted by a red border.

If the **Terminate Session** button is inactive, the user is not logged in to the system.

The RHEL web console terminates the sessions.

CHAPTER 6. MANAGING SERVICES IN THE WEB CONSOLE

This document describes how to manage system services in the web console interface. You can activate or deactivate services, restart or reload them or manage their automatic startup.

6.1. ACTIVATING OR DEACTIVATING SYSTEM SERVICES IN THE WEB CONSOLE

This procedure activates or deactivates system services using the web console interface.

Prerequisites

- The RHEL 8 web console has been installed.
For details, see [Installing the web console](#).



PROCEDURE

You can filter the services by name or description and also by Enabled, Disabled, or Static automatic startup. The interface shows the current state of the service and its recent logs.

- Log in to the RHEL web console with administrator privileges.
For details, see [Logging in to the web console](#).
- Click **Services** in the web console menu on the left.
- The default tab for **Services** is **System Services**. If you want to manage targets, sockets, timers, or paths, switch to the respective tab in the menu on top.

Name	Description	State	Automatic Startup
accounts-daemon	Accounts Service	active (running)	Enabled
alsa-restore	Save/Restore Sound Card State	inactive (dead)	Static
alsa-state	Manage Sound Card State (restore and store)	active (running)	Static
anaconda-direct	the anaconda installation program	inactive (dead)	Static
anaconda-nm-config	Anaconda NetworkManager configuration	inactive (dead)	Static
anaconda-noshell	Restrict Anaconda Text Console	inactive (dead)	Static

- To open service settings, click on a selected service from the list. You can tell which services are active or inactive by checking the **State** column.
- Activate or deactivate a service:
 - To activate an inactive service, click the **Start** button.

Services > anaconda.service

Anaconda

Status: Not running

Path: /usr/lib/systemd/system/anaconda.service

Start

Disallow running (mask)

- To deactivate an active service, click the **Stop** button.

Services > cockpit.service

Cockpit Web Service

Status: Running

Path: /usr/lib/systemd/system/cockpit.socket

Restart

Stop

Disallow running (mask)

6.2. RESTARTING SYSTEM SERVICES IN THE WEB CONSOLE

This procedure restarts system services using the web console interface.

Prerequisites

- The RHEL 8 web console has been installed.
For details, see [Installing the web console](#).



PROCEDURE

You can filter the services by name or description and also by Enabled, Disabled, or Static automatic startup. The interface shows the current state of the service and its recent logs.

- Log in to the RHEL web console with administrator privileges.
For details, see [Logging in to the web console](#).

2. Click **Services** in the web console menu on the left.
3. The default tab for **Services** is **System Services**. If you want to manage targets, sockets, timers, or paths, switch to the respective tab in the menu on top.

Name	Description	State	Automatic Startup
accounts-daemon	Accounts Service	active (running)	Enabled
alsa-restore	Save/Restore Sound Card State	inactive (dead)	Static
alsa-state	Manage Sound Card State (restore and store)	active (running)	Static
anaconda-direct	the anaconda installation program	inactive (dead)	Static
anaconda-nm-config	Anaconda NetworkManager configuration	inactive (dead)	Static
anaconda-noshell	Restrict Anaconda Text Console	inactive (dead)	Static

4. To open service settings, click on a selected service from the list.
5. To restart a service, click the **Restart** button.

Services > cockpit.service

Cockpit Web Service

Status ⚡ Static
⚡ Running Active since May

Path /usr/lib/systemd/system/cockpit.socket

⋮

- Restart**
- Stop
- Disallow running (mask)

CHAPTER 7. MANAGING NETWORKING IN THE WEB CONSOLE

The RHEL 8 web console supports basic network configuration. You can:

- Configure IPv4/IPv6 network settings
- Manage Bonds
- Manage network bridges
- Manage VLANs
- Manage Teams
- Inspect a network log



NOTE

The RHEL 8 web console is build on top of the NetworkManager service.

For details, see [Getting started with NetworkManager for managing networking](#).

Prerequisites

- The RHEL 8 web console installed and enabled.
For details, see [Installing the web console](#).

7.1. CONFIGURING NETWORK BONDS USING THE WEB CONSOLE

This chapter helps you to understand how network bonding works and what all can configure in the web console. Additionally, you also find in this chapter the following guidelines:

- Adding a new bond
- Removing a bond
- Adding interfaces to a bond
- Removing interfaces from a bond

7.1.1. Understanding network bonding

Network bonding is a method to combine or aggregate network interfaces to provide a logical interface with higher throughput or redundancy.

The **active-backup**, **balance-tlb**, and **balance-alb** modes do not require any specific configuration of the network switch. However, other bonding modes require configuring the switch to aggregate the links. For example, Cisco switches requires **EtherChannel** for modes 0, 2, and 3, but for mode 4, the Link Aggregation Control Protocol (LACP) and **EtherChannel** are required.

For further details, see the documentation of your switch and <https://www.kernel.org/doc/Documentation/networking/bonding.txt>.



IMPORTANT

Certain network bonding features, such as the fail-over mechanism, do not support direct cable connections without a network switch. For further details, see the [Is bonding supported with direct connection using crossover cables? KCS solution](#).

7.1.2. Bond modes

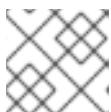
The behavior of the bonded interfaces depends upon the mode. The bonding modes provide fault tolerance, load balancing or both.

Load balancing modes

- **Round Robin:** Sequentially transmit packets from the first available interface to the last one.

Fault tolerance modes

- **Active Backup:** Only when the primary interface fails, one of a backup interfaces replaces it. Only a MAC address used by active interface is visible.
- **Broadcast:** All transmissions are sent on all interfaces.



NOTE

Broadcasting significantly increases network traffic on all the bonded interfaces.

Fault tolerance and load balancing modes

- **XOR:** The destination MAC addresses are distributed equally between interfaces with a modulo hash. Each interface then serves the same group of MAC addresses.
- **802.3ad:** Sets an IEEE 802.3ad dynamic link aggregation policy. Creates aggregation groups that share the same speed and duplex settings. Transmits and receives on all interfaces in the active aggregator.



NOTE

This mode requires a switch that is 802.3ad compliant.

- **Adaptive transmit load balancing:** The outgoing traffic is distributed according to the current load on each interface. Incoming traffic is received by the current interface. If the receiving interface fails, another interface takes over the MAC address of the failed one.
- **Adaptive load balancing:** Includes transmit and receive load balancing for IPv4 traffic. Receive load balancing is achieved through Address Resolution Protocol (ARP) negotiation, therefore, it is necessary to set **Link Monitoring to ARP** in the bond's configuration.

7.1.3. Adding a new bond using the web console

This section describes how to configure an active-backup bond on two or more network interfaces using the web console.

Other [network bond modes](#) can be configured similarly.

Prerequisites

- Two or more network cards are installed in the server.
- The network cards are connected to a switch.

Procedure

1. Log in to the web console.
For details, see [Logging in to the web console](#).
2. Open **Networking**.
3. Click the **Add Bond** button.
4. In the **Bond Settings** dialog box, enter a name for the new bond.
5. In the **Members** field, select interfaces which should be a member of the bond.
6. [Optional] In the **MAC** drop down list, select a MAC address which will be used for this interface.
If you leave the **MAC** field empty, the bond will get one of the addresses that are listed in the drop down list.
7. In the **Mode** drop down list, select the mode.
For details, see [Section 7.1.2, “Bond modes”](#).
8. If you select **Active Backup**, select the primary interface.

MAC	E8:6A:64:04:9A:C2	▼
Mode	Active Backup	▼
Primary	enp0s31f6	▼

9. In the **Link Monitoring** drop down menu, leave here the **MII** option.
Only the adaptive load balancing mode requires to switch this option to **ARP**.
10. The **Monitoring Interval**, **Link up delay**, and **Link down delay** fields, which contain values in milliseconds, leave as they are. Change it only for a troubleshooting purpose.
11. Click **Apply**.

Bond Settings

Name	mybond
Interfaces	<input checked="" type="checkbox"/> enp0s31f6 <input checked="" type="checkbox"/> enp0p25b1 <input type="checkbox"/> virbr0 <input type="checkbox"/> vnet1 <input type="checkbox"/> vnet2
MAC	E8:6A:64:04:9A:C2
Mode	Active Backup
Primary	enp0s31f6
Link Monitoring	MII (Recommended)
Monitoring Interval	100
Link up delay	0
Link down delay	0
<input type="button" value="Cancel"/> <input type="button" value="Apply"/>	

To verify that the bond works correctly, go to the **Networking** section and check if the **Sending** and **Receiving** columns in the **Interfaces** table display a network activity.

Interfaces		Add Bond	Add Team	Add Bridge	Add VLAN
Name	IP Address	Sending	Receiving		
mybond	10.253.16.25/24	46.6 Kbps	16.2 Kbps		
tun0	10.40.204.83/22	1.46 Kbps	2.59 Kbps		
virbr0	192.168.122.1/24	No carrier			

7.1.4. Adding interfaces to the bond using the web console

Network bonds can include multiple interfaces and you can add or remove any of them any time.

This section describes adding a network interface to an existing bond.

Prerequisites

- Having a bond with multiple interfaces configured as described in [Section 7.1.3, “Adding a new bond using the web console”](#).

Procedure

- Log in to the web console.
For details, see [Logging in to the web console](#).
- Open **Networking**.
- In the **Interfaces** table, click on the bond you want to configure.
- In the bond settings screen, scroll down to the table of members (interfaces).
- Click the + icon.
- Select the interface in the drop down list and click it.

Members	Sending	Receiving	
enp0s31f6	561 bps	1000 bps	<input type="button" value="ON"/>
ens12	0 bps	0 bps	<input type="button" value="ON"/>

+

- tun0
- virbr0
- vnet1
- vnet2
- wlp61s0

The RHEL 8 web console adds the interface to the bond.

7.1.5. Removing or disabling an interface from the bond using the web console

Network bonds can include multiple interfaces. If you need to change a device, you can remove or disable particular interfaces from the bond, which will work with the rest of the active interfaces.

Basically, you have two options, how to stop using an interface included in a bond. You can:

- Remove the interface from the bond.
- Disable the interface temporarily. The interface stays a part of the bond, but the bond will not use it until you enable it again.

Prerequisites

- Having a bond with multiple interfaces configured as described in [Section 7.1.3, “Adding a new bond using the web console”](#).

Procedure

- Log in to the RHEL web console.
For details, see [Logging in to the web console](#).
- Open **Networking**.
- Click the bond you want to configure.
- In the bond settings screen, scroll down to the table of ports (interfaces).
- Select the interface and and remove or disable it:

- Click the - icon to remove the interface.
- Switch the **ON/OFF** button to Off.

Members	Sending	Receiving	
enp0s31f6	101 Kbps	3.63 Mbps	<input type="button" value="ON"/> <input type="button" value="-"/>
ens12	0 bps	0 bps	<input type="button" value="ON"/> <input type="button" value="-"/>

Based on your choice, the web console either removes or disables the interface from the bond and you can see it back in the **Networking** section as standalone interface.

7.1.6. Removing or disabling a bond using the web console

This section describes how to remove or disable a network bond using the web console. If you disable the bond, the interfaces stay in the bond, but the bond will not be used for network traffic.

Prerequisites

- There is an existing bond in the web console.

Procedure

1. Log in to the web console.
For details, see [Logging in to the web console](#).
2. Open **Networking**.
3. Click the bond you want to remove.
4. In the bond settings screen, you can disable the bond with the **ON/OFF** button or click the **Delete** button to remove the bond permanently.

mybond	Bond	E8:6A:64:04:9A:C2	<input type="button" value="Delete"/>	<input type="button" value="ON"/>
Status 10.253.16.25/24, fe80:0:0:0:de45:c6f6:8ddd:ef21/64 Carrier Yes General <input checked="" type="checkbox"/> Connect automatically IPv4 Automatic (DHCP) IPv6 Automatic MTU Automatic Bond Round Robin				

You can go back to **Networking** and verify that all the interfaces from the bond are now standalone interfaces.

7.2. CONFIGURING NETWORK TEAMS USING THE WEB CONSOLE

This section describes how network bonding works, what are the differences between network teams and network bonds, and what are the possibilities of configuration in the web console. Additionally you can find guidelines for:

- Adding a new network team
- Adding new interfaces to an existing network team
- Removing interfaces from an existing network team
- Removing a network team

7.2.1. Understanding network teaming

Network teaming is a feature that combines or aggregates network interfaces to provide a logical interface with higher throughput or redundancy.

Network teaming uses a kernel driver to implement fast handling of packet flows, as well as user-space libraries and services for other tasks. This way, network teaming is an easily extensible and scalable solution for load-balancing and redundancy requirements.

Note that in the context of network teaming, the term **port** is also known as **slave**. In the **teamd** service, the term **port** is preferred while in the **NetworkManager** service, the term **slave** refers to interfaces which create a team.



IMPORTANT

Certain network teaming features, such as the fail-over mechanism, do not support direct cable connections without a network switch. For further details, see [Is bonding supported with direct connection using crossover cables?](#)

7.2.2. Comparison of network teaming and bonding features

The following table compares features supported in network teams and network bonds:

Feature	Network bond	Network team
Broadcast Tx policy	Yes	Yes
Round-robin Tx policy	Yes	Yes
Active-backup Tx policy	Yes	Yes
LACP (802.3ad) support	Yes (active only)	Yes
Hash-based Tx policy	Yes	Yes
User can set hash function	No	Yes
Tx load-balancing support (TLB)	Yes	Yes
LACP hash port select	Yes	Yes
Load-balancing for LACP support	No	Yes

Feature	Network bond	Network team
Ethtool link monitoring	Yes	Yes
ARP link monitoring	Yes	Yes
NS/NA (IPv6) link monitoring	No	Yes
Ports up/down delays	Yes	Yes
Port priorities and stickiness (“primary” option enhancement)	No	Yes
Separate per-port link monitoring setup	No	Yes
Multiple link monitoring setup	Limited	Yes
Lockless Tx/Rx path	No (rwlock)	Yes (RCU)
VLAN support	Yes	Yes
User-space runtime control	Limited	Yes
Logic in user-space	No	Yes
Extensibility	Hard	Easy
Modular design	No	Yes
Performance overhead	Low	Very low
D-Bus interface	No	Yes
Multiple device stacking	Yes	Yes
Zero config using LLDP	No	(in planning)
NetworkManager support	Yes	Yes

7.2.3. Adding a new team using the web console

This procedure describes how to configure a new active backup network team on two or more network interfaces using the web console.

Prerequisites

- Two or more network cards installed on the server.

- The network cards are connected to a switch.

Procedure

- Log in to the web console.
For details, see [Logging in to the web console](#)
- Go to the **Networking** tab.
- Click the **Add Team** button.
- In the **Team Settings** area, configure parameters for the new team:
 - Add a name for your team device to the **Name** field.
 - In the **Ports** field, select all network interfaces you want to add to the team.
 - In the **Runner** drop down menu, select the runner.
 - In the **Link Watch** drop down menu select a link watcher.
 - If you select **Ethtool**, additionally, set a link up delay and a link down delay.
 - If you select **ARP Ping** or **NSNA Ping**, additionally, set a ping interval and ping target.
- Click **Apply**

The screenshot shows the 'Team Settings' dialog box with the following configuration:

Setting	Value
Name	myteam
Ports	<input type="checkbox"/> enp1s0 <input checked="" type="checkbox"/> enp7s0 <input checked="" type="checkbox"/> enp8s0 <input type="checkbox"/> enp9s0
Runner	Active Backup
Link Watch	Ethtool
Link up delay	0
Link down delay	0

Verification steps

1. Go to the **Networking** tab and check if the **Sending** and **Receiving** columns in the **Interfaces** table display a network activity.

The screenshot shows the RHEL 8 web console interface. On the left, a sidebar menu includes Storage, Networking (which is selected), Podman, Containers, Accounts, Services, Applications, and Diagnostic Reports. The main content area has a header 'Firewall' with a toggle switch. Below it, a section says '1 Active Zone'. The 'Interfaces' table has columns for Name, IP Address, Sending, and Receiving. It lists three interfaces: 'enp1s0' (IP 192.168.122.222/24, 0.00938 bps, 3.95 bps), 'enp9s0' (Inactive), and 'myteam' (IP 192.168.122.250/24, 3.52 bps, 3.29 bps). The 'myteam' row is highlighted with a red border.

Interfaces			
Name	IP Address	Sending	Receiving
enp1s0	192.168.122.222/24	0.00938 bps	3.95 bps
enp9s0			Inactive
myteam	192.168.122.250/24	3.52 bps	3.29 bps

Additional resources

- [Network team runners](#)

7.2.4. Adding new interfaces to the team using the web console

Network teams can include multiple interfaces and it is possible to add or remove any of them at any time. The following section describes how to add a new network interface to an existing team.

Prerequisites

- A network team with is configured.

Procedure

1. Log in to the web console.
For details, see [Logging in to the web console](#).
2. Switch to the **Networking** tab.
3. In the **Interfaces** table, click on the team you want to configure.
4. In the team settings window, scroll down to the **Ports** table.
5. Click on the **+** icon.
6. Select the interface you wish to add from the drop down list.

The screenshot shows the 'Ports' table in the team settings window. It has columns for Ports, Sending, and Receiving. It lists two ports: 'enp7s0' (0 bps, 0 bps) and 'enp8s0' (0 bps, 0 bps). To the right of the table, a modal window displays a list of available interfaces: 'enp1s0' and 'enp9s0'. The 'enp9s0' option is highlighted with a blue selection bar.

Ports	Sending	Receiving
enp7s0	0 bps	0 bps
enp8s0	0 bps	0 bps

The RHEL 8 web console adds the interface to the team.

7.2.5. Removing or disabling an interface from the team using the web console

Network teams can include multiple interfaces. If you need to change a device, you can remove or disable particular interfaces from the network team, which will work together with the rest of active interfaces.

There are two options how to stop using an interface included in a team:

- Removing the interface from the team
- Temporarily disabling the interface. The interface then stays a part of the team, but the team will not use it until you enable it again.

Prerequisites

- A network team with multiple interfaces exists on the host.

Procedure

1. Log in to the RHEL web console.
For details, see [Logging in to the web console](#).
2. Switch to the **Networking** tab.
3. Click the team you want to configure.
4. In the team settings window, scroll down to the table of ports (interfaces).
5. Select an interface and remove or disable it.
 - a. Switch the **ON/OFF** button to Off to disable the interface.
 - b. Click the - icon to remove the interface.

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

Based on your choice, the web console either removes or disables the interface. If you remove the interface, it will be available in **Networking** as a standalone interface.

7.2.6. Removing or disabling a team using the web console

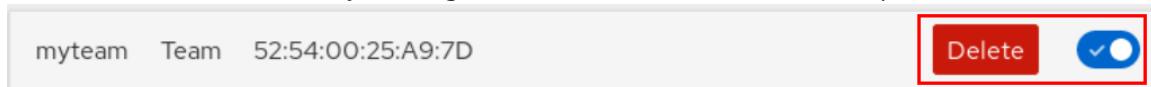
This section describes how to remove or disable a network team using the web console. If you only disable the team, interfaces in the team will stay in it but the team will not be used for network traffic.

Prerequisites

- A network team is configured on the host.

Procedure

1. Log in to the web console.
For details, see [Logging in to the web console](#).
2. Switch to the **Networking** tab.
3. Click the team you wish to remove or disable.
4. Remove or disable the selected team.
 - a. You can remove the team by clicking the **Delete** button.
 - b. You can disable the team by moving the **ON/OFF** switch to a disabled position.



Verification steps

- If you removed the team, go to **Networking**, and verify that all the interfaces from your team are now listed as standalone interfaces.

7.3. CONFIGURING NETWORK BRIDGES IN THE WEB CONSOLE

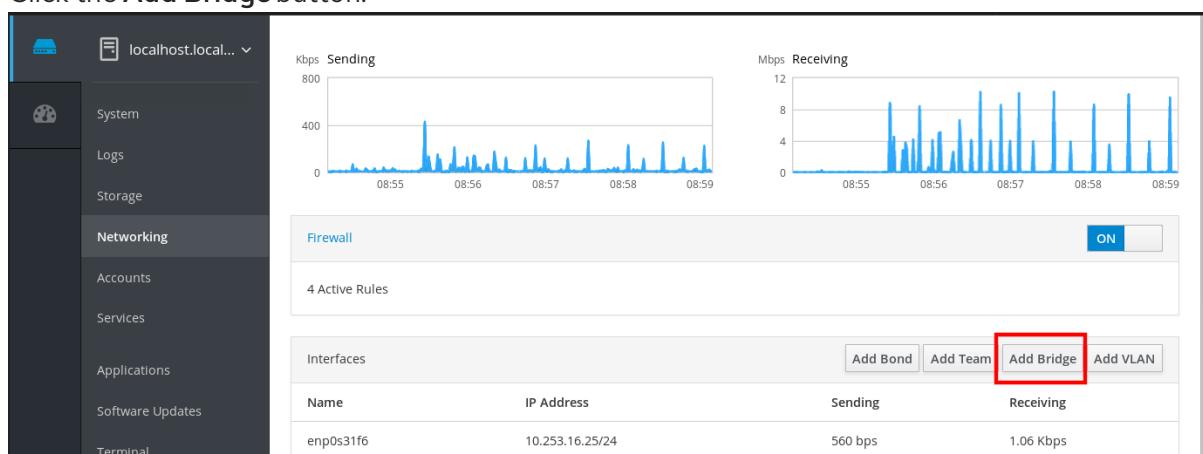
Network bridges are used to connect multiple interfaces to the one subnet with the same range of IP addresses.

7.3.1. Adding bridges in the web console

This section describes creating a software bridge on multiple network interfaces using the web console.

Procedure

1. Log in to the RHEL web console.
For details, see [Logging in to the web console](#).
2. Open **Networking**.
3. Click the **Add Bridge** button.



4. In the **Bridge Settings** dialog box, enter a name for the new bridge.
5. In the **Port** field, select interfaces which you want to put to the one subnet.

6. Optionally, you can select the **Spanning Tree protocol (STP)** to avoid bridge loops and broadcast radiation.

If you do not have a strong preference, leave the predefined values as they are.

Bridge Settings

Name	<input type="text" value="bridge0"/>
Ports	<input checked="" type="checkbox"/> enp0s31f6 <input type="checkbox"/> tun0 <input type="checkbox"/> virbr0 <input checked="" type="checkbox"/> vnet0 <input checked="" type="checkbox"/> vnet1 <input type="checkbox"/> wlp61s0
Spanning Tree Protocol (STP) <input checked="" type="checkbox"/>	
STP Priority	<input type="text" value="32768"/>
STP Forward delay	<input type="text" value="15"/>
STP Hello time	<input type="text" value="2"/>
STP Maximum message age	<input type="text" value="20"/>

Cancel
Apply

7. Click **Create**.

If the bridge is successfully created, the web console displays the new bridge in the **Networking** section. Check values in the **Sending** and **Receiving** columns in the new bridge row.

Interfaces		Add Bond	Add Team	Add Bridge	Add VLAN
Name	IP Address	Sending	Receiving		
bridge0	10.253.16.25/24	1.22 Kbps	609 bps		
virbr0	192.168.122.1/24	No carrier			
wlp61s0	10.253.16.39/24	0 bps	0 bps		

If you can see that zero bytes are sent and received through the bridge, the connection does not work correctly and you need to adjust the network settings.

7.3.2. Configuring a static IP address in the web console

IP address for your system can be assigned from the pool automatically by the DHCP server or you can configure the IP address manually. The IP address will not be influenced by the DHCP server settings.

This section describes configuring static IPv4 addresses of a network bridge using the RHEL web console.

Procedure

1. Log in to the RHEL web console.
For details, see [Logging in to the web console](#).
2. Open the **Networking** section.
3. Click the interface where you want to set the static IP address.

The screenshot shows the RHEL 8 Web Console interface. The left sidebar has a 'Networking' section selected. The main area displays network traffic graphs for 'Sending' and 'Receiving' Kbps over time (10:29 to 10:32). Below the graphs is a 'Firewall' section with a status of 'ON' and 4 active rules. The central part of the screen is a table titled 'Interfaces' showing three network interfaces: bridge0, virbr0, and wlp61s0. The 'virbr0' row is highlighted with a red box. At the bottom right of the interface table are four buttons: 'Add Bond', 'Add Team', 'Add Bridge', and 'Add VLAN'.

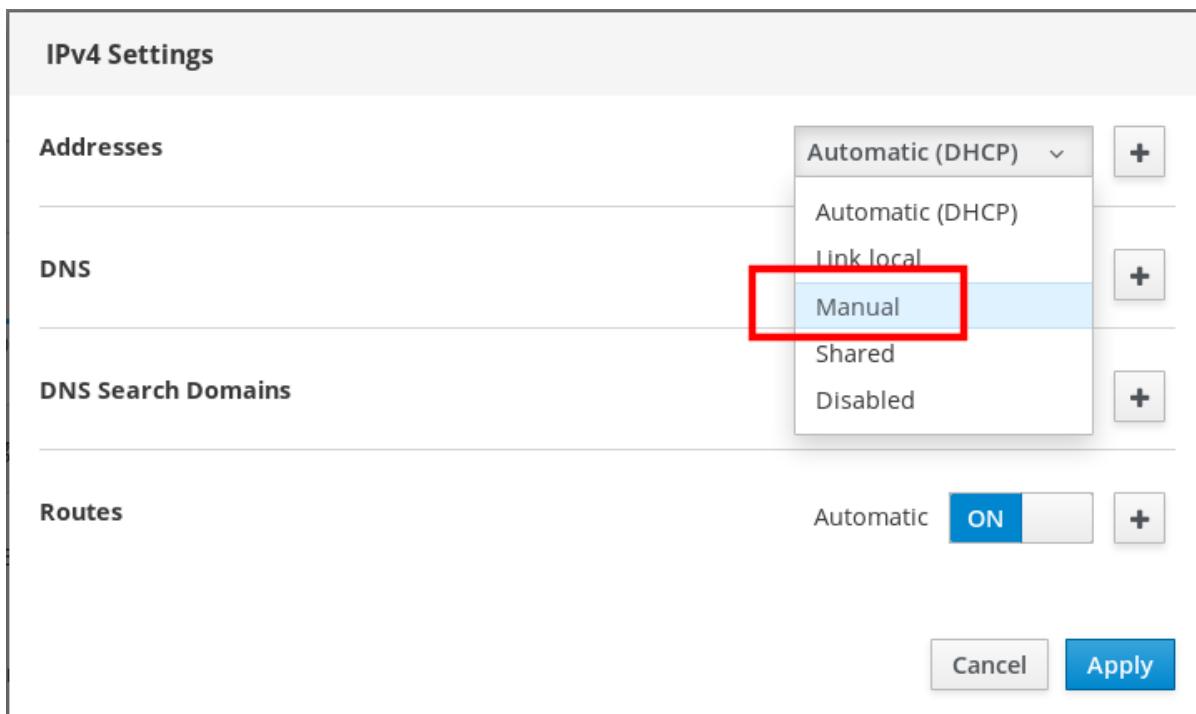
Name	IP Address	Sending	Receiving
bridge0	10.253.16.25/24	336 bps	2.24 Kbps
virbr0	192.168.122.1/24	No carrier	
wlp61s0	10.253.16.39/24	0 bps	0 bps

4. In the interface details screen, click the **IPv4** configuration.

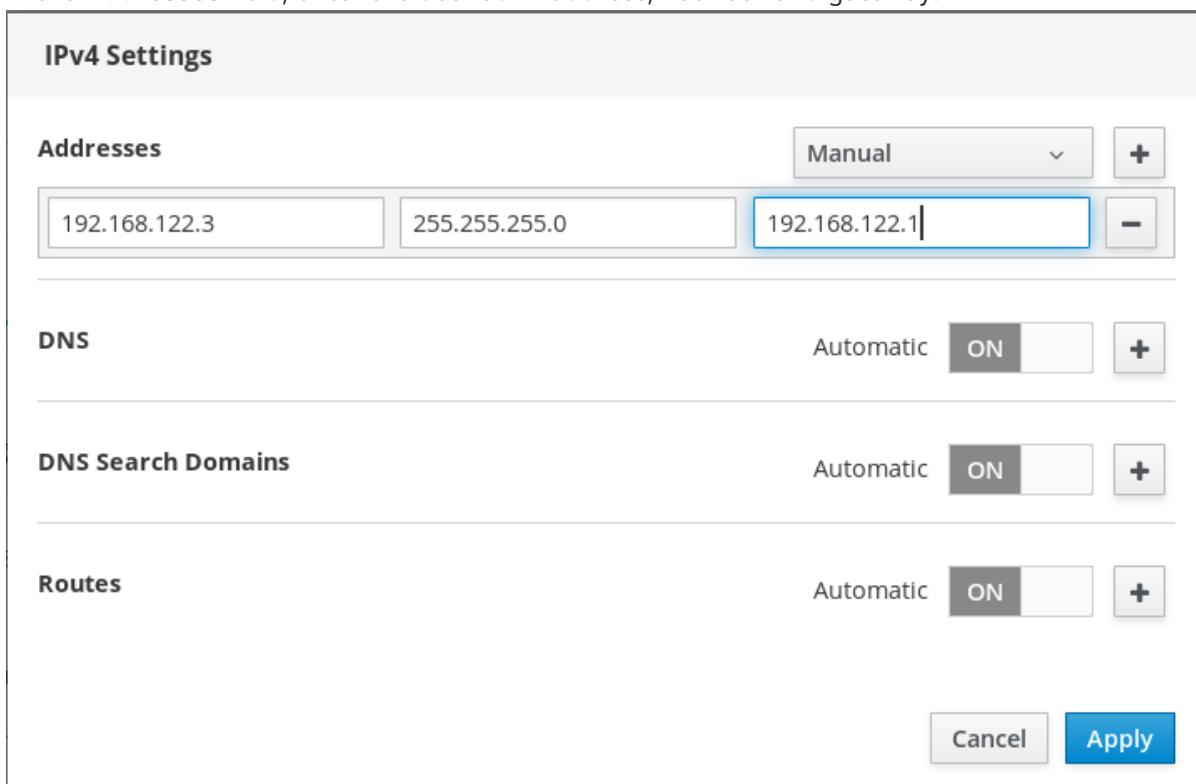
The screenshot shows the interface details screen for a network interface. It displays the following information:

- Status: 10.253.16.25/24, fe80:0:0:0:7813:2486:f2d0:92ad/64
- Carrier: Yes
- General: Connect automatically
- IPv4**: Automatic (DHCP) (This option is highlighted with a red box)
- IPv6: Automatic
- MTU: Automatic

5. In the **IPv4 Settings** dialog box, select **Manual** in the **Addresses** drop down list.



6. Click **Apply**.
7. In the **Addresses** field, enter the desired IP address, netmask and gateway.



8. Click **Apply**.

At this point, the IP address has been configured and the interface uses the new static IP address.

IPv4 Address 192.168.122.3/24 via 192.168.122.1
 IPv6 Automatic
 MTU Automatic

7.3.3. Removing interfaces from the bridge using the web console

Network bridges can include multiple interfaces. You can remove them from the bridge. Each removed interface will be automatically changed to the standalone interface.

This section describes removing a network interface from a software bridge created in the RHEL 8 system.

Prerequisites

- Having a bridge with multiple interfaces in your system.

Procedure

- Log in to the RHEL web console.
 For details, see [Logging in to the web console](#).
- Open **Networking**.
- Click the bridge you want to configure.

Name	IP Address	Sending	Receiving
bridge0	10.253.16.25/24	336 bps	2.24 Kbps
virbr0	192.168.122.1/24	No carrier	
wlp61s0	10.253.16.39/24	0 bps	0 bps

- In the bridge settings screen, scroll down to the table of ports (interfaces).

Ports	Sending	Receiving	<input type="button" value="+"/>
enp0s31f6	0 bps	0 bps	<input checked="" type="button" value="ON"/> <input type="button" value=""/> <input type="button" value="-"/>
vnet0	0 bps	0 bps	<input checked="" type="button" value="ON"/> <input type="button" value=""/> <input type="button" value="-"/>
vnet1	0 bps	0 bps	<input checked="" type="button" value="ON"/> <input type="button" value=""/> <input type="button" value="-"/>

5. Select the interface and click the - icon.

The RHEL 8 web console removes the interface from the bridge and you can see it back in the **Networking** section as standalone interface.

7.3.4. Deleting bridges in the web console

You can delete a software network bridge in the RHEL web console. All network interfaces included in the bridge will be changed automatically to standalone interfaces.

Prerequisites

- Having a bridge in your system.

Procedure

1. Log in to the RHEL web console.
For details, see [Logging in to the web console](#).
2. Open the **Networking** section.
3. Click the bridge you want to configure.

Interfaces			
Name	IP Address	Sending	Receiving
bridge0	10.253.16.25/24	336 bps	2.24 Kbps
virbr0	192.168.122.1/24	No carrier	
wlp6s0	10.253.16.39/24	0 bps	0 bps

4. In the bridge settings screen, scroll down to the table of ports.

Ports	Sending	Receiving	<input type="button" value="+"/>
enp0s31f6	0 bps	0 bps	<input checked="" type="button" value="ON"/> <input type="button" value="-"/>
vnet0	0 bps	0 bps	<input checked="" type="button" value="ON"/> <input type="button" value="-"/>
vnet1	0 bps	0 bps	<input checked="" type="button" value="ON"/> <input type="button" value="-"/>

5. Click **Delete**.

At this stage, go back to **Networking** and verify that all the network interfaces are displayed on the **Interfaces** tab. Interfaces which were part of the bridge can be inactive now. Therefore, you may need to activate them and set network parameters manually.

Interfaces		Add Bond	Add Team	Add Bridge	Add VLAN
Name	IP Address	Sending	Receiving		
enp0s31f6	10.253.16.25/24	1.12 Kbps	1.60 Kbps		
tun0	10.40.205.17/22	0 bps	0 bps		
virbr0	192.168.122.1/24	No carrier			
vnet0		Inactive			
vnet1		Inactive			

7.4. CONFIGURING VLANS IN THE WEB CONSOLE

VLANs (Virtual LANs) are virtual networks created on a single physical Ethernet interface.

Each VLAN is defined by an ID which represents a unique positive integer and works as a standalone interface.

The following procedure describes creating VLANs in the RHEL web console.

Prerequisites

- Having a network interface in your system.

Procedure

- Log in to the RHEL web console.
For details, see [Logging in to the web console](#).
- Open **Networking**.
- Click **Add VLAN** button.

Name	IP Address	Sending	Receiving
enp0s31f6	10.253.16.25/24	560 bps	1.06 Kbps

- In the **VLAN Settings** dialog box, select the physical interface for which you want to create a VLAN.
- Enter the VLAN Id or just use the predefined number.
- In the **Name** field, you can see a predefined name consisted of the parent interface and VLAN Id. If it is not necessary, leave the name as it is.

VLAN Settings

Parent	enp0s31f6
VLAN Id	1
Name	enp0s31f6.1

7. Click **Apply**.

The new VLAN has been created and you need to click at the VLAN and configure the network settings.

Interfaces		Add Bond	Add Team	Add Bridge	Add VLAN
Name	IP Address	Sending	Receiving		
enp0s31f6	10.253.16.25/24	7.66 Kbps	5.47 Kbps		
enp0s31f6.1		Configuring IP			
tun0	10.40.204.27/22	0 bps	0 bps		
virbr0	192.168.122.1/24	0 bps	0 bps		
wlp6s0	10.253.16.39/24	0 bps	0 bps		

7.5. CONFIGURING THE WEB CONSOLE LISTENING PORT

Following sections provide information on how to:

- Allow a new port with if you have active SELinux.
- Allow a new port on a firewall in the web console.
- Change the web console port.

7.5.1. Allowing a new port on a system with active SELinux

This procedure enables the web console to listen on a selected port.

Prerequisites

- The web console must be installed and accessible. For details, see [Installing the web console](#).

Procedure

- For ports that are not defined by any other part of SELinux, run:

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

- For ports that already are defined by other part of SELinux, run:

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

The changes should take effect immediately.

7.5.2. Allowing a new port on a system with firewalld

This procedure enables the web console to receive connections on a new port.

Prerequisites

- The web console must be installed and accessible. For details, see [Installing the web console](#).
- The **firewalld** service must be running.

Procedure

1. To add a new port number, run the following command:

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

2. To remove the old port number from the **cockpit** service, run:

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



IMPORTANT

If you only run the **firewall-cmd --service cockpit --add-port=PORT_NUMBER/tcp** without the **--permanent** option, your change will be canceled with the next reload of **firewalld** or a system reboot.

7.5.3. Changing the web console port

The following procedure shows how to change default transmission control protocol (TCP) on port **9090** to a different one.

Prerequisites

- The web console must be installed and accessible. For details, see [Installing the web console](#).
- If you have SELinux protecting your system, you need to set it to allow Cockpit to listen on a new port. For more information, see [Allowing a new port on a system with active SELinux](#).
- If you have **firewalld** configured as your firewall, you need to set it to allow Cockpit receive connections on a new port, for more information, see [Allowing a new port on a system with firewalld](#).

Procedure

1. Change the listening port with one of the following methods:

- a. Using the **systemctl edit cockpit.socket** command:
 - i. Run the following command:

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

This will open the **/etc/systemd/system/cockpit.socket.d/override.conf** file.

- ii. Modify the content of **override.conf** or add a new content in the following format:

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

- b. Alternatively, add the above mentioned content to the **/etc/systemd/system/cockpit.socket.d/listen.conf** file.

Create the **cockpit.socket.d**. directory and the **listen.conf** file if they do not exist yet.

2. Run the following commands for changes to take effect:

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

If you used **systemctl edit cockpit.socket** in the previous step, running **systemctl daemon-reload** is not necessary.

Verification steps

- To verify that the change was successful, try to connect to the web console with the new port.

CHAPTER 8. MANAGING FIREWALL USING THE WEB CONSOLE

A firewall is a way to protect machines from any unwanted traffic from outside. It enables users to control incoming network traffic on host machines by defining a set of firewall rules. These rules are used to sort the incoming traffic and either block it or allow through.

Prerequisites

- The RHEL 8 web console configures the **firewalld** service.
For details about the **firewalld** service, see [Getting started with firewalld](#).

8.1. RUNNING FIREWALL USING THE WEB CONSOLE

This section describes where and how to run the RHEL 8 system firewall in the web console.

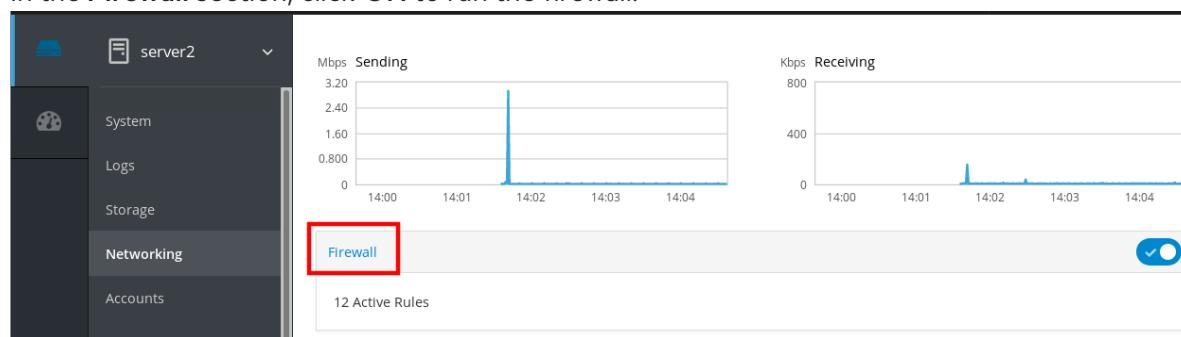


NOTE

The RHEL 8 web console configures the **firewalld** service.

Procedure

- Log in to the RHEL 8 web console.
For details, see [Logging in to the web console](#).
- Open the **Networking** section.
- In the **Firewall** section, click **ON** to run the firewall.



If you do not see the **Firewall** box, log in to the web console with the administration privileges.

At this stage, your firewall is running.

To configure firewall rules, see [Section 8.7, “Enabling services on the firewall using the web console”](#).

8.2. STOPPING FIREWALL USING THE WEB CONSOLE

This section describes where and how to stop the RHEL 8 system firewall in the web console.

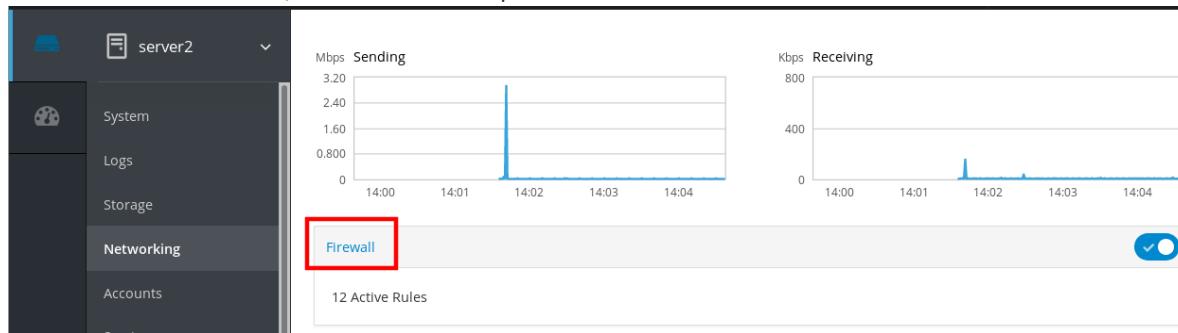


NOTE

The RHEL 8 web console configures the **firewalld** service.

Procedure

1. Log in to the RHEL 8 web console.
For details, see [Logging in to the web console](#).
2. Open the **Networking** section.
3. In the **Firewall** section, click **OFF** to stop it.



If you do not see the **Firewall** box, log in to the web console with the administration privileges.

At this stage, the firewall has been stopped and does not secure your system.

8.3. FIREWALLD

firewalld is a firewall service daemon that provides a dynamic customizable host-based firewall with a **D-Bus** interface. Being dynamic, it enables creating, changing, and deleting the rules without the necessity to restart the firewall daemon each time the rules are changed.

firewalld uses the concepts of *zones* and *services*, that simplify the traffic management. Zones are predefined sets of rules. Network interfaces and sources can be assigned to a zone. The traffic allowed depends on the network your computer is connected to and the security level this network is assigned. Firewall services are predefined rules that cover all necessary settings to allow incoming traffic for a specific service and they apply within a zone.

Services use one or more *ports* or *addresses* for network communication. Firewalls filter communication based on ports. To allow network traffic for a service, its ports must be *open*. **firewalld** blocks all traffic on ports that are not explicitly set as open. Some zones, such as *trusted*, allow all traffic by default.

Additional resources

- **firewalld(1)** man page

8.4. ZONES

firewalld can be used to separate networks into different zones according to the level of trust that the user has decided to place on the interfaces and traffic within that network. A connection can only be part of one zone, but a zone can be used for many network connections.

NetworkManager notifies **firewalld** of the zone of an interface. You can assign zones to interfaces with:

- **NetworkManager**
- **firewall-config** tool
- **firewall-cmd** command-line tool

- The RHEL web console

The latter three can only edit the appropriate **NetworkManager** configuration files. If you change the zone of the interface using the web console, **firewall-cmd** or **firewall-config**, the request is forwarded to **NetworkManager** and is not handled by **firewalld**.

The predefined zones are stored in the **/usr/lib/firewalld/zones/** directory and can be instantly applied to any available network interface. These files are copied to the **/etc/firewalld/zones/** directory only after they are modified. The default settings of the predefined zones are as follows:

block

Any incoming network connections are rejected with an icmp-host-prohibited message for **IPv4** and icmp6-adm-prohibited for **IPv6**. Only network connections initiated from within the system are possible.

dmz

For computers in your demilitarized zone that are publicly-accessible with limited access to your internal network. Only selected incoming connections are accepted.

drop

Any incoming network packets are dropped without any notification. Only outgoing network connections are possible.

external

For use on external networks with masquerading enabled, especially for routers. You do not trust the other computers on the network to not harm your computer. Only selected incoming connections are accepted.

home

For use at home when you mostly trust the other computers on the network. Only selected incoming connections are accepted.

internal

For use on internal networks when you mostly trust the other computers on the network. Only selected incoming connections are accepted.

public

For use in public areas where you do not trust other computers on the network. Only selected incoming connections are accepted.

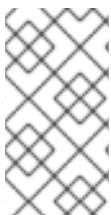
trusted

All network connections are accepted.

work

For use at work where you mostly trust the other computers on the network. Only selected incoming connections are accepted.

One of these zones is set as the *default* zone. When interface connections are added to **NetworkManager**, they are assigned to the default zone. On installation, the default zone in **firewalld** is set to be the **public** zone. The default zone can be changed.



NOTE

The network zone names should be self-explanatory and to allow users to quickly make a reasonable decision. To avoid any security problems, review the default zone configuration and disable any unnecessary services according to your needs and risk assessments.

Additional resources

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

8.5. ZONES IN THE WEB CONSOLE



IMPORTANT

Firewall zones are new in the RHEL 8.1.0 Beta.

The Red Hat Enterprise Linux web console implements major features of the firewalld service and enables you to:

- Add predefined firewall zones to a particular interface or range of IP addresses
- Configure zones with selecting services into the list of enabled services
- Disable a service by removing this service from the list of enabled service
- Remove a zone from an interface

8.6. ENABLING ZONES USING THE WEB CONSOLE

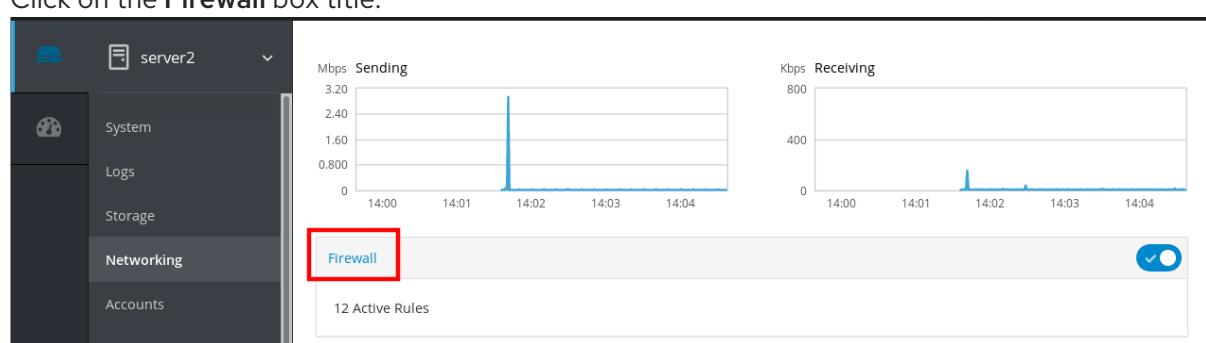
The web console enables you to apply predefined and existing firewall zones on a particular interface or a range of IP addresses. This section describes how to enable a zone on an interface.

Prerequisites

- The RHEL 8 web console has been installed.
For details, see [Installing the web console](#).
- The firewall must be enabled.
For details, see [Section 8.1, “Running firewall using the web console”](#).

Procedure

1. Log in to the RHEL web console with administration privileges.
For details, see [Logging in to the web console](#).
2. Click **Networking**.
3. Click on the **Firewall** box title.



If you do not see the **Firewall** box, log in to the web console with the administrator privileges.

4. In the **Firewall** section, click **Add Services**.
5. Click on the **Add Zone** button.
6. In the **Add Zone** dialog box, select a zone from the **Trust level** scale.
You can see here all zones predefined in the **firewalld** service.
7. In the **Interfaces** part, select an interface or interfaces on which the selected zone is applied.
8. In the **Allowed Addresses** part, you can select whether the zone is applied on:
 - the whole subnet
 - or a range of IP addresses in the following format:
 - 192.168.1.0
 - 192.168.1.0/24
 - 192.168.1.0/24, 192.168.1.0

9. Click on the **Add zone** button.

Add Zone

Trust level Sorted from least trusted to most trusted Custom zones

Public External DMZ Work Home Internal Public

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

Included services ssh, mdns, samba-client, dhcpcv6-client

Interfaces enp0s31f6 virbr0

Allowed Addresses Entire subnet
 Range

Add zone

Verify the configuration in **Active zones**.

Active zones			
Zone	Interfaces	IP Range	
libvirt	virbr0	*	
Public	✓default	ens3	*

8.7. ENABLING SERVICES ON THE FIREWALL USING THE WEB CONSOLE

By default, services are added to the default firewall zone. If you use more firewall zones on more network interfaces, you must select a zone first and then add the service with port.

The RHEL 8 web console displays predefined **firewalld** services and you can add them to active firewall zones.



IMPORTANT

The RHEL 8 web console configures the **firewalld** service.

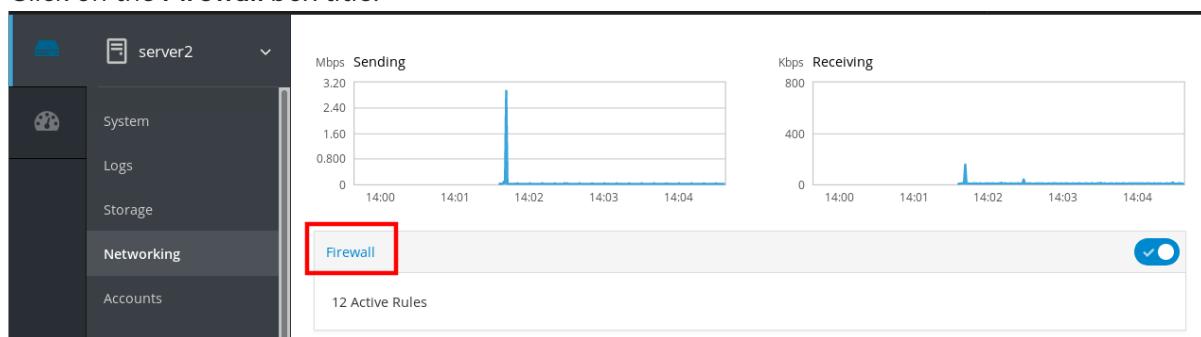
The web console does not allow generic **firewalld** rules which are not listed in the web console.

Prerequisites

- The RHEL 8 web console has been installed.
For details, see [Installing the web console](#).
- The firewall must be enabled.
For details, see [Section 8.1, “Running firewall using the web console”](#).

Procedure

1. Log in to the RHEL web console with administrator privileges.
For details, see [Logging in to the web console](#).
2. Click **Networking**.
3. Click on the **Firewall** box title.



If you do not see the **Firewall** box, log in to the web console with the administrator privileges.

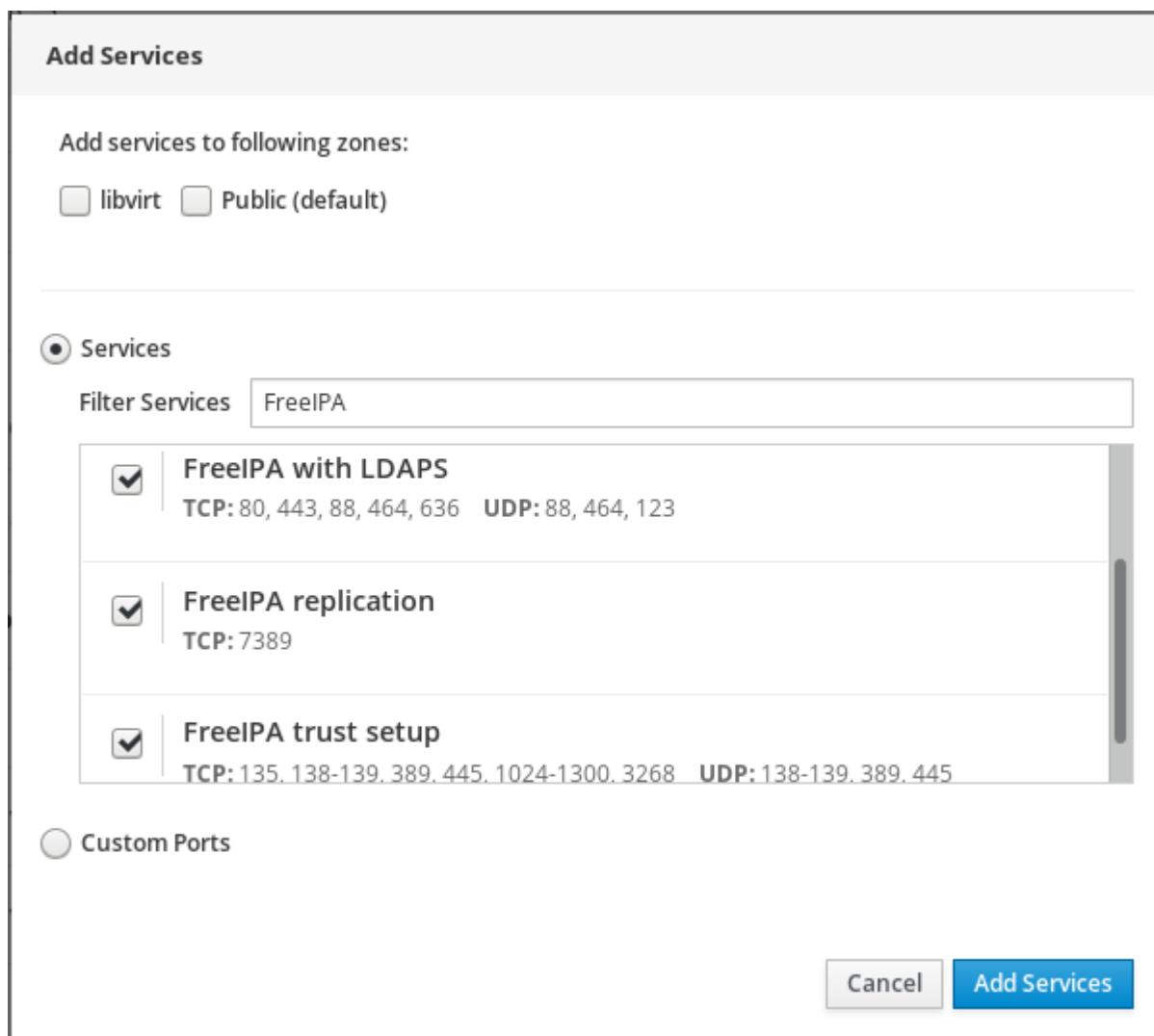
4. In the **Firewall** section, click **Add Services**.

The screenshot shows the 'Networking' section of the RHEL 8 web console. On the left, a sidebar lists various system management options. The 'Networking' option is highlighted with a red box. The main content area is divided into two sections: 'Active zones' and 'Allowed Services'. The 'Active zones' section lists two zones: 'libvirt' and 'Public'. The 'libvirt' zone is associated with interface 'virbr0' and IP range *. The 'Public' zone is associated with interface 'ens3' and IP range *. Both zones have a trash icon in their respective rows. The 'Allowed Services' section lists four services: 'Cockpit' (TCP port 9090, Public zone), 'DHCP' (TCP port 67, libvirt zone), 'DHCPv6' (TCP port 547, libvirt zone), and 'DHCPv6 Client' (TCP port 546, Public zone). Each service row includes a trash icon. At the top right of the 'Active zones' section is a blue 'Add Zone' button, and at the top right of the 'Allowed Services' section is a blue 'Add Services' button, both of which are also highlighted with red boxes.

5. In the **Add Services** dialog box, select a zone for which you want to add the service. The **Add Services** dialog box includes a list of active firewall zones only if the system includes multiple active zones.

If the system uses just one (the default) zone, the dialog does not include zone settings.

6. In the **Add Services** dialog box, find the service you want to enable on the firewall.
7. Enable desired services.



8. Click **Add Services**.

At this point, the RHEL 8 web console displays the service in the list of **Allowed Services**.

8.8. CONFIGURING CUSTOM PORTS USING THE WEB CONSOLE

The web console allows you to add:

- Services listening on standard ports: [Section 8.7, “Enabling services on the firewall using the web console”](#)
- Services listening on custom ports.

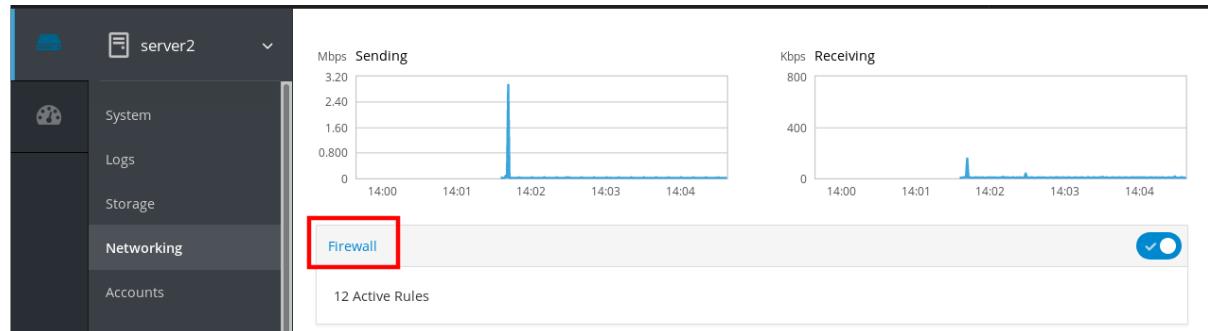
This section describes how to add services with custom ports configured.

Prerequisites

- The RHEL 8 web console has been installed.
For details, see [Installing the web console](#).
- The firewall must be enabled.
For details, see [Section 8.1, “Running firewall using the web console”](#).

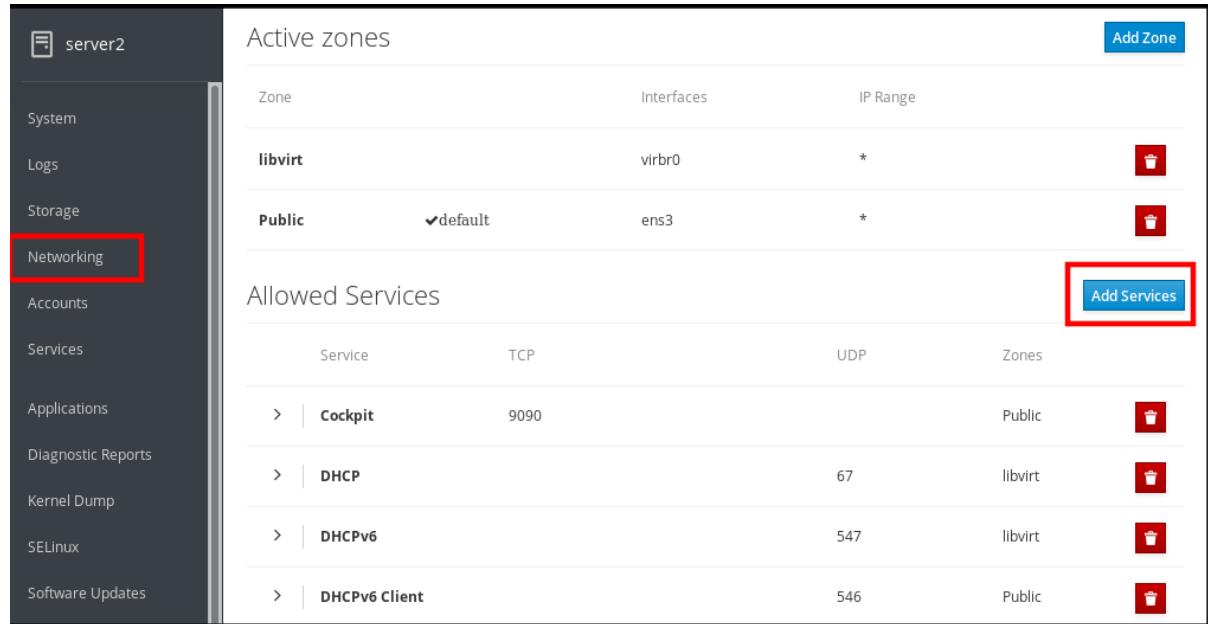
Procedure

1. Log in to the RHEL web console with administrator privileges.
For details, see [Logging in to the web console](#).
2. Click **Networking**.
3. Click on the **Firewall** box title.



If you do not see the **Firewall** box, log in to the web console with the administration privileges.

4. In the **Firewall** section, click **Add Services**.



5. In the **Add Services** dialog box, select a zone for which you want to add the service.
The **Add Services** dialog box includes a list of active firewall zones only if the system includes multiple active zones.

If the system uses just one (the default) zone, the dialog does not include zone settings.

6. In the **Add Ports** dialog box, click on the **Custom Ports** radio button.
7. In the TCP and UDP fields, add ports according to examples. You can add ports in the following formats:
 - Port numbers such as 22
 - Range of port numbers such as 5900–5910
 - Aliases such as nfs, rsync

**NOTE**

You can add multiple values into each field. Values must be separated with the comma and without the space, for example: 8080,8081,http

8. After adding the port number in the **TCP** and/or **UDP** fields, verify the service name in the **Name** field.

The **Name** field displays the name of the service for which is this port reserved. You can rewrite the name if you are sure that this port is free to use and no server needs to communicate on this port.

9. In the **Name** field, add a name for the service including defined ports.
10. Click on the **Add Ports** button.

Add Ports

Add ports to the following zones:

libvirt Public (default)

Services

Custom Ports

Comma-separated ports, ranges, and aliases are accepted

TCP	8081
UDP	Example: 88,2019,nfs,rsync
Name	My Web Server

Cancel
Add Ports

To verify the settings, go to the **Firewall** page and find the service in the list of **Allowed Services**.

Allowed Services				Add Services
Service	TCP	UDP	Zones	
> DHCP		67	libvirt	
> DHCPv6		547	libvirt	
> DNS	53	53	libvirt	
My Web Server	8081		public	
> SSH	22		libvirt	

8.9. DISABLING ZONES USING THE WEB CONSOLE

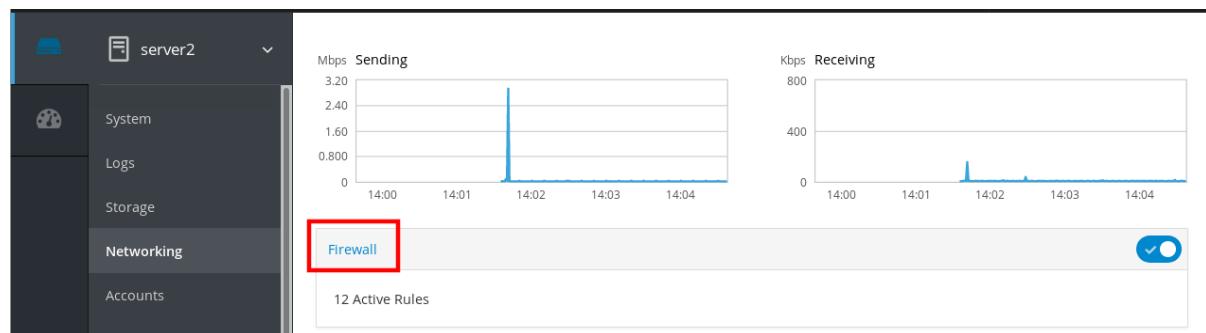
This section describes how to disable a firewall zone in your firewall configuration using the web console.

Prerequisites

- The RHEL 8 web console has been installed.
For details, see [Installing the web console](#).

Procedure

1. Log in to the RHEL web console with administrator privileges.
For details, see [Logging in to the web console](#).
2. Click **Networking**.
3. Click on the **Firewall** box title.



If you do not see the **Firewall** box, log in to the web console with the administrator privileges.

4. On the **Active zones** table, click on the **Delete** icon at the zone you want to remove.

Active zones			Add Zone
Zone	Interfaces	IP Range	
libvirt	virbr0	*	
Public	default	ens3	

The zone is now disabled and the interface does not include opened services and ports which were configured in the zone.

CHAPTER 9. MANAGING PARTITIONS USING THE WEB CONSOLE

The web console enables you to manage file systems on RHEL 8 systems.

For details about the available file systems, see the [Overview of available file systems](#).

This chapter describes the following file system configurations:

- [Displaying partitions](#)
- [Creating partitions](#)
- [Deleting partitions](#)
- [Mounting and unmounting file systems](#)

9.1. DISPLAYING PARTITIONS FORMATTED WITH FILE SYSTEMS IN THE WEB CONSOLE

The **Storage** section in the web console displays all available file systems in the **Filesystems** table.

This section navigates you to get to the list of partitions formatted with file systems displayed in the web console.

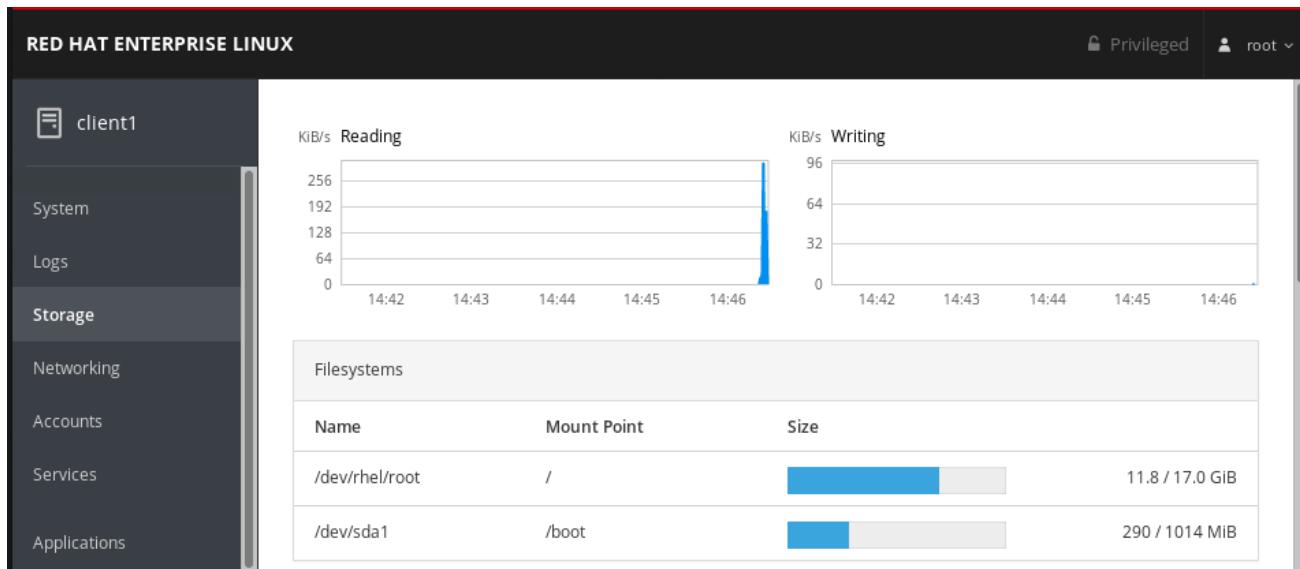
Prerequisites

- The web console must be installed and accessible.
For details, see [Installing the web console](#).

Procedure

1. Log in to the RHEL web console.
For details, see [Logging in to the web console](#).
2. Click on the **Storage** tab.

In the **Filesystems** table, you can see all available partitions formatted with file systems, its name, size and how much space is available on each partition.



9.2. CREATING PARTITIONS IN THE WEB CONSOLE

To create a new partition:

- Use an existing partition table
- Create a partition

The screenshot shows the 'Storage' configuration page for the device '/dev/sdb'. The 'Block' section displays the device's capacity (500 GiB) and file path (/dev/sdb). The 'Content' section shows '500 GiB Free Space'. In the bottom right corner, there are two buttons: 'Create partition table' and 'Create Partition', which are highlighted with a red box.

Prerequisites

- The web console must be installed and accessible.
For details, see [Installing the web console](#).
- An unformatted volume connected to the system visible in the **Other Devices** table of the **Storage** tab.

Procedure

1. Log in to the RHEL web console.
For details, see [Logging in to the web console](#).
2. Click the **Storage** tab.
3. In the **Other Devices** table, click a volume in which you want to create the partition.

4. In the **Content** section, click the **Create Partition** button.
5. In the **Create partition** dialog box, select the size of the new partition.
6. In the **Erase** drop down menu, select:
 - **Don't overwrite existing data**— the RHEL web console rewrites only the disk header. Advantage of this option is speed of formatting.
 - **Overwrite existing data with zeros**— the RHEL web console rewrites the whole disk with zeros. This option is slower because the program has to go through the whole disk, but it is more secure. Use this option if the disk includes any data and you need to overwrite it.
7. In the **Type** drop down menu, select a file system:
 - **XFS** file system supports large logical volumes, switching physical drives online without outage, and growing an existing file system. Leave this file system selected if you do not have a different strong preference.
 - **ext4** file system supports:
 - Logical volumes
 - Switching physical drives online without outage
 - Growing a file system
 - Shrinking a file system
- Additional option is to enable encryption of partition done by LUKS (Linux Unified Key Setup), which allows you to encrypt the volume with a passphrase.
8. In the **Name** field, enter the logical volume name.
9. In the **Mounting** drop down menu, select **Custom**.
The **Default** option does not ensure that the file system will be mounted on the next boot.
10. In the **Mount Point** field, add the mount path.
11. Select **Mount at boot**.
12. Click the **Create partition** button.

Create partition on /dev/sdb

Size	<input type="range" value="500"/> 500 GiB
Erase	Don't overwrite existing data
Type	XFS - Red Hat Enterprise Linux 7 default
Name	Partition 1
Mounting	Custom
Mount Point	/media
Mount options	<input checked="" type="checkbox"/> Mount at boot <input type="checkbox"/> Mount read only <input type="checkbox"/> Custom mount options
<input type="button" value="Cancel"/> <input type="button" value="Create partition"/>	

Formatting can take several minutes depending on the volume size and which formatting options are selected.

After the formatting has completed successfully, you can see the details of the formatted logical volume on the **Filesystem** tab.

To verify that the partition has been successfully added, switch to the **Storage** tab and check the **Filesystems** table.

Filesystems			
Name	Mount Point	Size	
/dev/rhel/root	/	<input type="range" value="12.1"/> 12.1 / 17.0 GiB	
/dev/sda1	/boot	<input type="range" value="290"/> 290 / 1014 MIB	
Partition 1	/media	<input type="range" value="500"/> 500 GiB	

9.3. DELETING PARTITIONS IN THE WEB CONSOLE

This paragraph is the procedure module introduction: a short description of the procedure.

Prerequisites

- The web console must be installed and accessible.
For details, see [Installing the web console](#).
- Unmount the partition's file system.
For details about mounting and unmounting partitions, see [Section 9.4, "Mounting and unmounting file systems in the web console"](#).

Procedure

1. Log in to the RHEL web console.
For details, see [Logging in to the web console](#).
2. Click on the **Storage** tab.
3. In the **Filesystems** table, select a volume in which you want to delete the partition.
4. In the **Content** section, click on the partition you want to delete.

Content		
> 512 MiB ext4 File System		/dev/nvme0n1p1
> 32 GiB Encrypted data		/dev/nvme0n1p2
> 32.0 GiB ext4 File System		/dev/mapper/luks-20bca9d6-0fb1-4bb8-8643-5f915415dea8
> 8.00 GiB Encrypted data		/dev/nvme0n1p3
> 8 GiB Swap Space		/dev/mapper/luks-01afed46-ab21-4037-8927-6c01a7ae1dc0
> 198 GiB Extended Partition		/dev/nvme0n1p4
> 198 GiB Encrypted data		/dev/nvme0n1p5
> 198 GiB ext4 File System		/dev/mapper/luks-913540eb-284e-4e56-8f58-572e6f4e8cf8

5. The partition rolls down and you can click on the **Delete** button.



The screenshot shows the 'Content' table in the RHEL Web Console. A specific row for a '198 GiB Extended Partition' at path '/dev/nvme0n1p4' is highlighted with a red box around the 'Delete' button in the top right corner of its row. The table includes columns for 'Partition' and 'Unrecognized Data'. Below the table, detailed information about the partition is listed:

- Name: -
- Size: 198 GiB
- UUID: a98632eb-04
- Type: 0x05

The partition must not be mounted and used.

To verify that the partition has been successfully removed, switch to the **Storage** tab and check the **Content** table.

9.4. MOUNTING AND UNMOUNTING FILE SYSTEMS IN THE WEB CONSOLE

To be able to use partitions on RHEL systems, you need to mount a filesystem on the partition as a device.



NOTE

You also can unmount a file system and the RHEL system will stop using it. Unmounting the file system enables you to delete, remove, or re-format devices.

Prerequisites

- The web console must be installed and accessible.
For details, see [Installing the web console](#).
- If you want to unmount a file system, ensure that the system does not use any file, service, or application stored in the partition.

Procedure

1. Log in to the RHEL web console.
For details, see [Logging in to the web console](#).
2. Click on the **Storage** tab.
3. In the **Filesystems** table, select a volume in which you want to delete the partition.
4. In the **Content** section, click on the partition whose file system you want to mount or unmount.
5. Click on the **Mount or Unmount** button.

The screenshot shows a web-based storage management interface. At the top, there's a header bar with a dropdown arrow, the text "198 GiB ext4 File System", and the path "/dev/mapper/luks-913540eb-284e-4e56-8f58-572e6f4e8cf". Below this is a table with a single row labeled "Filesystem". The row contains the following information:

- Name: FormattedPartition
- Mount Point: /FormattedPartition
- Mount Options: defaults,x-systemd.device-timeout=0
- Mounted At: /FormattedPartition
- Used: 115 GiB of 194 GiB

A red rectangular box is drawn around the "Mount" button, which is located to the right of the "Mounted At" field.

At this point, the file system has been mounted or unmounted according to your action.

CHAPTER 10. MANAGING STORAGE DEVICES IN THE WEB CONSOLE

You can use the RHEL 8 web console to configure physical and virtual storage devices. This chapter provides instructions for these devices:

- Mounted NFS
- Logical Volumes
- RAID
- VDO

Prerequisites

- The RHEL 8 web console has been installed.
For details, see [Installing the web console](#).

10.1. MANAGING NFS MOUNTS IN THE WEB CONSOLE

The RHEL 8 web console enables you to mount remote directories using the Network File System (NFS) protocol.

NFS makes it possible to reach and mount remote directories located on the network and work with the files as if the directory was located on your physical drive.

Prerequisites

- NFS server name or IP address.
- Path to the directory on the remote server.

10.1.1. Connecting NFS mounts in the web console

The following steps aim to help you with connecting a remote directory to your file system using NFS.

Prerequisites

- NFS server name or IP address.
- Path to the directory on the remote server.

Procedure

1. Log in to the RHEL 8 web console.
For details, see [Logging in to the web console](#).
2. Click **Storage**.
3. Click **+** in the **NFS mounts** section.

NFS Mounts			
Server	Mount Point	Size	
10.253.16.5 /volume1/movie	/mnt/movie	 1.51 / 3.49 TiB	

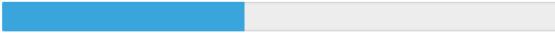
4. In the **New NFS Mount** dialog box, enter the server or IP address of the remote server.
5. In the **Path on Server** field, enter the path to the directory you want to mount.
6. In the **Local Mount Point** field, enter the path where you want to find the directory in your local system.
7. Select **Mount at boot**. This ensures that the directory will be reachable also after the restart of the local system.
8. Optionally, select **Mount read only** if you do not want to change the content.

New NFS Mount

Server Address	fileserver.example.com
Path on Server	/volume1/videotutorials
Local Mount Point	/mnt/tutorials
Mount Options	<input checked="" type="checkbox"/> Mount at boot <input checked="" type="checkbox"/> Mount read only <input type="checkbox"/> Custom mount option
<input type="button" value="Cancel"/> <input type="button" value="Add"/>	

9. Click **Add**.

At this point, you can open the mounted directory and verify that the content is accessible.

NFS Mounts			
Server	Mount Point	Size	
10.253.16.5 /volume1/id...	/mnt/tutorial	 1.51 / 3.49 TiB	

To troubleshoot the connection, you can adjust it with the [Custom Mount Options](#).

10.1.2. Customizing NFS mount options in the web console

The following section provides you with information on how to edit an existing NFS mount and shows you where to add custom mount options.

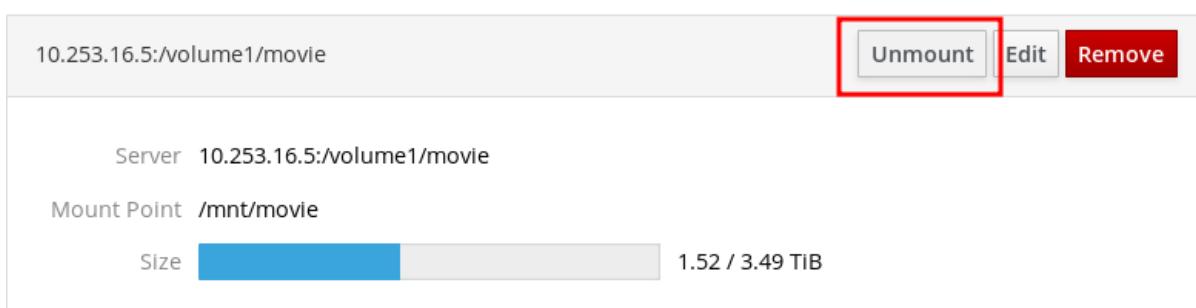
Custom mount options can help you to troubleshoot the connection or change parameters of the NFS mount such as changing timeout limits or configuring authentication.

Prerequisites

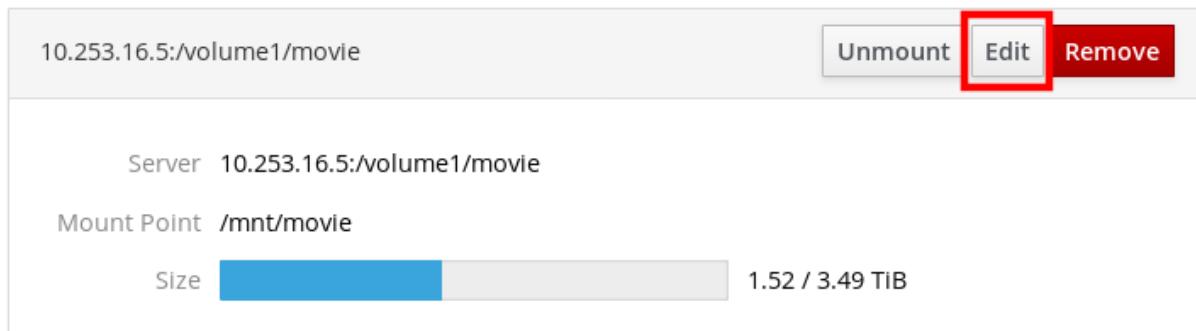
- NFS mount added.

Procedure

1. Log in to the RHEL 8 web console.
For details, see [Logging in to the web console](#).
2. Click **Storage**.
3. Click on the NFS mount you want to adjust.
4. If the remote directory is mounted, click **Unmount**.
The directory must not be mounted during the custom mount options configuration. Otherwise the web console does not save the configuration and this will cause an error.



5. Click **Edit**.



6. In the **NFS Mount** dialog box, select **Custom mount option**.
7. Enter mount options separated by a comma. For example:
 - **nfsvers=4** – the NFS protocol version number
 - **soft** – type of recovery after an NFS request times out
 - **sec=krb5** – files on the NFS server can be secured by Kerberos authentication. Both the NFS client and server have to support Kerberos authentication.

NFS Mount

Server Address	fileserver.example.com
Path on Server	/volume1/movie
Local Mount Point	/mnt/movie
Mount Options	<input checked="" type="checkbox"/> Mount at boot <input checked="" type="checkbox"/> Mount read only <input checked="" type="checkbox"/> Custom mount option nfsvers=4,soft,sec=krb5

Cancel **Apply**

For a complete list of the NFS mount options, enter **man nfs** in the command line.

8. Click **Apply**.

9. Click **Mount**.

Now you can open the mounted directory and verify that the content is accessible.

NFS Mounts		
Server	Mount Point	Size
10.253.16.5 /volume1/vid...	/mnt/tutorial	1.51 / 3.49 TiB

10.2. MANAGING REDUNDANT ARRAYS OF INDEPENDENT DISKS IN THE WEB CONSOLE

Redundant Arrays of Independent Disks (RAID) represents a way how to arrange more disks into one storage.

RAID protects data stored in the disks against disk failure with the following data distribution strategies:

- Mirroring – data are copied to two different locations. If one disk fails, you have a copy and your data is not lost.
- Striping – data are evenly distributed among disks.

Level of protection depends on the RAID level.

The RHEL web console supports the following RAID levels:

- RAID 0 (Stripe)
- RAID 1 (Mirror)
- RAID 4 (Dedicated parity)

- RAID 5 (Distributed parity)
- RAID 6 (Double Distributed Parity)
- RAID 10 (Stripe of Mirrors)

Before you can use disks in RAID, you need to:

- Create a RAID.
- Format it with file system.
- Mount the RAID to the server.

Prerequisites

- The RHEL 8 web console is running and accessible.
For details, see [Installing the web console](#).

10.2.1. Creating RAID in the web console

This procedure aims to help you with configuring RAID in the RHEL 8 web console.

Prerequisites

- Physical disks connected to the system. Each RAID level requires different amount of disks.

Procedure

1. Open the RHEL 8 web console.
2. Click **Storage**.
3. Click the + icon in the **RAID Devices** box.



4. In the **Create RAID Device** dialog box, enter a name for a new RAID.
5. In the **RAID Level** drop-down list, select a level of RAID you want to use.
6. In the **Chunk Size** drop-down list, leave the predefined value as it is.
The **Chunk Size** value specifies how large is each block for data writing. If the chunk size is 512 KiB, the system writes the first 512 KiB to the first disk, the second 512 KiB is written to the second disk, and the third chunk will be written to the third disk. If you have three disks in your RAID, the fourth 512 KiB will be written to the first disk again.
7. Select disks you want to use for RAID.

Create RAID Device

Name	myraid5
RAID Level	RAID 5 (Distributed Parity)
Chunk Size	512 KiB
Disks	<input checked="" type="checkbox"/> 20 MiB QEMU HARDDISK(DISK1) /dev/sda1 <input checked="" type="checkbox"/> 20 MiB QEMU HARDDISK(DISK2) /dev/sdb1 <input checked="" type="checkbox"/> 20 MiB QEMU HARDDISK(DISK3) /dev/sdc1

Cancel **Create**

8. Click **Create**.

In the **Storage** section, you can see the new RAID in the **RAID devices** box and format it.

RAID Devices	
 myraid5	60 GiB

Now you have the following options how to format and mount the new RAID in the web console:

- [Formatting RAID](#)
- [Creating partitions on partition table](#)
- [Creating a volume group on top of RAID](#)

10.2.2. Formatting RAID in the web console

This section describes formatting procedure of the new software RAID device which is created in the RHEL 8 web interface.

Prerequisites

- Physical disks are connected and visible by RHEL 8.
- RAID is created.
- Consider the file system which will be used for the RAID.
- Consider creating of a partitioning table.

Procedure

1. Open the RHEL 8 web console.

2. Click **Storage**.
3. In the **RAID devices** box, choose the RAID you want to format by clicking on it.
4. In the RAID details screen, scroll down to the **Content** part.
5. Click to the newly created RAID.

Content		Create partition table
▼	120 GiB Unrecognized Data	/dev/md/myraid5
Unrecognized Data		
Usage	-	Format
Type	-	

6. Click the **Format** button.
7. In the **Erase** drop-down list, select:
 - **Don't overwrite existing data** – the RHEL web console rewrites only the disk header. Advantage of this option is speed of formatting.
 - **Overwrite existing data with zeros** – the RHEL web console rewrites the whole disk with zeros. This option is slower because the program has to go through the whole disk. Use this option if the RAID includes any data and you need to rewrite it.
8. In the **Type** drop-down list, select a XFS file system, if you do not have another strong preference.
9. Enter a name of the file system.
10. In the **Mounting** drop down list, select **Custom**.
The **Default** option does not ensure that the file system will be mounted on the next boot.
11. In the **Mount Point** field, add the mount path.

12. Select **Mount at boot**.

Format /dev/md/myraid5

Erase	Don't overwrite existing data
Type	XFS - Red Hat Enterprise Linux 7 default
Name	myraids
Mounting	Custom
Mount Point	/media

Mount options

Mount at boot

Mount read only

Custom mount options

Formatting a storage device will erase all data on it.

Cancel **Format**

13. Click the **Format** button.

Formatting can take several minutes depending on the used formatting options and size of RAID.

After successful finish, you can see the details of the formatted RAID on the **Filesystem** tab.

Content

Create partition table

▼	59 GiB xfs File System	/dev/md/myraid5
Filesystem		
Name myraids Mount Point /media Mount Mount Options defaults Used -		

Format

14. To use the RAID, click **Mount**.

At this point, the system uses mounted and formatted RAID.

10.2.3. Using the web console for creating a partition table on RAID

RAID requires formatting as any other storage device. You have two options:

- Format the RAID device without partitions
- Create a partition table with partitions

This section describes formatting RAID with the partition table on the new software RAID device created in the RHEL 8 web interface.

Prerequisites

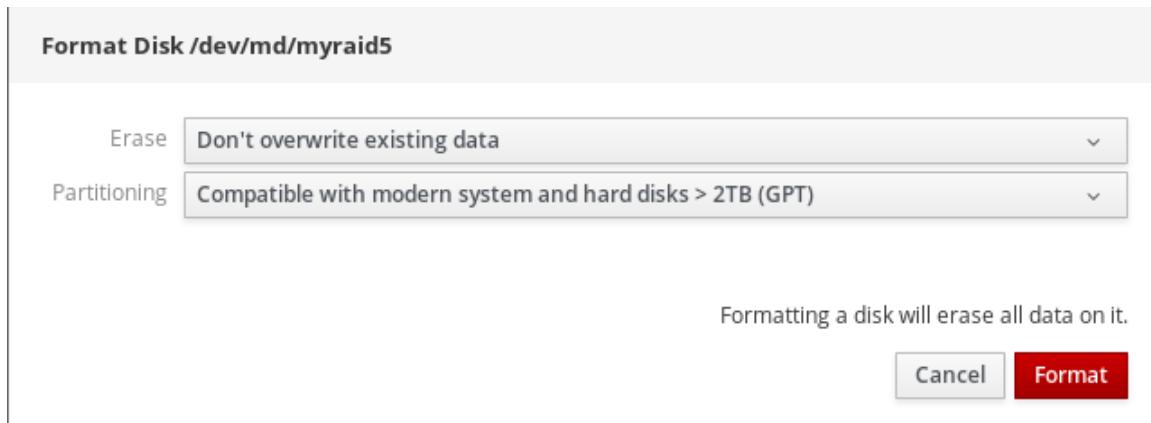
- Physical disks are connected and visible by RHEL 8.
- RAID is created.
- Consider the file system used for the RAID.
- Consider creating a partitioning table.

Procedure

- Open the RHEL 8 web console.
- Click **Storage**.
- In the **RAID devices** box, select the RAID you want to edit.
- In the RAID details screen, scroll down to the **Content** part.
- Click to the newly created RAID.

The screenshot shows the 'Content' section of the RAID details screen. It lists a single volume: '120 GiB Unrecognized Data' located at '/dev/md/myraid5'. The 'Unrecognized Data' tab is currently selected. Below the table, there are fields for 'Usage' and 'Type', both set to '-'. To the right of the table, there are two buttons: 'Create partition table' and 'Format'.

- Click the **Create partition table** button.
- In the **Erase** drop-down list, select:
 - Don't overwrite existing data** – the RHEL web console rewrites only the disk header. Advantage of this option is speed of formatting.
 - Overwrite existing data with zeros** – the RHEL web console rewrites the whole RAID with zeros. This option is slower because the program has to go through the whole RAID. Use this option if RAID includes any data and you need to rewrite it.
- In the **Partitioning** drop-down list, select:
 - Compatible with modern system and hard disks > 2TB (GPT) – GUID Partition Table is a modern recommended partitioning system for large RAIDs with more than four partitions.
 - Compatible with all systems and devices (MBR) – Master Boot Record works with disks up to 2 TB in size. MBR also support four primary partitions max.



9. Click **Format**.

At this point, the partitioning table has been created and you can create partitions.

For creating partitions, see [Using the web console for creating partitions on RAID](#).

10.2.4. Using the web console for creating partitions on RAID

This section describes creating a partition in the existing partition table.

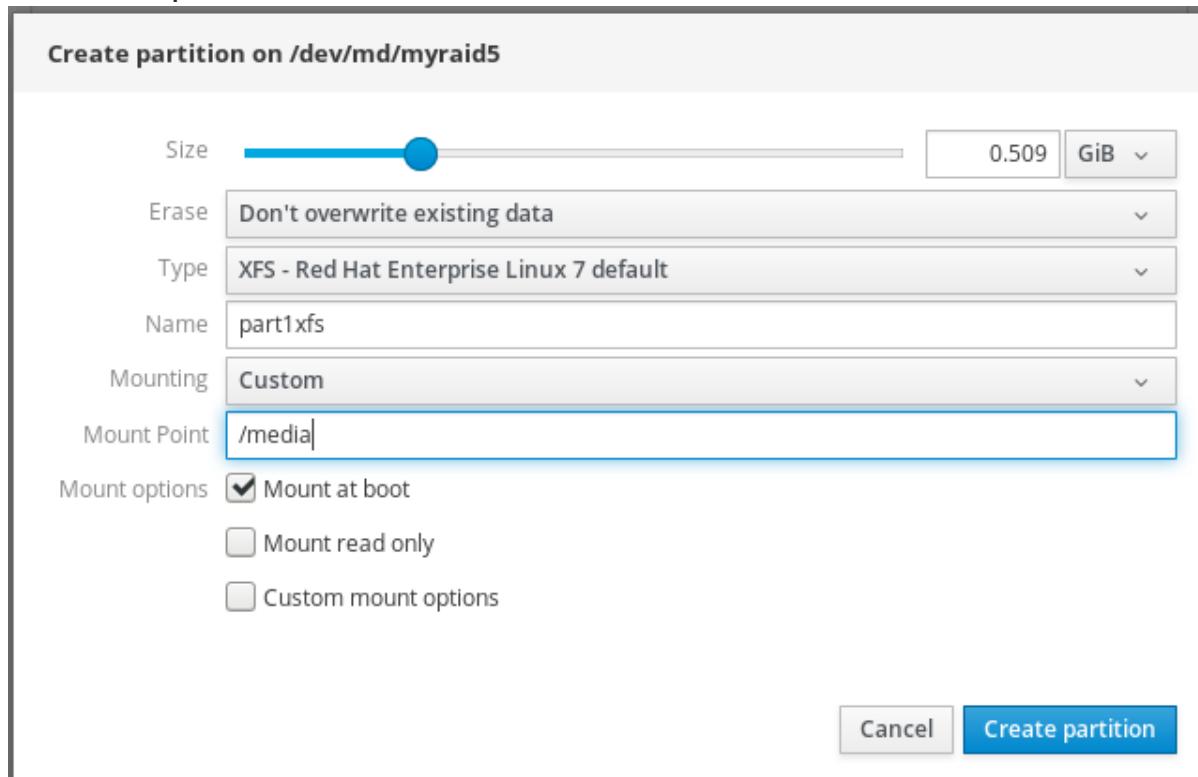
Prerequisites

- Partition table is created.
For details, see [Section 10.2.3, “Using the web console for creating a partition table on RAID”](#)

Procedure

1. Open the RHEL 8 web console.
2. Click **Storage**.
3. In the **RAID devices** box, click to the RAID you want to edit.
4. In the RAID details screen, scroll down to the **Content** part.
5. Click to the newly created RAID.
6. Click **Create Partition**.
7. In the **Create partition** dialog box, set up the size of the first partition.
8. In the **Erase** drop-down list, select:
 - **Don't overwrite existing data** – the RHEL web console rewrites only the disk header. Advantage of this option is speed of formatting.
 - **Overwrite existing data with zeros** – the RHEL web console rewrites the whole RAID with zeros. This option is slower because the program have to go through the whole RAID. Use this option if RAID includes any data and you need to rewrite it.
9. In the **Type** drop-down list, select a XFS file system, if you do not have another strong preference.
10. Enter any name for the file system. Do not use spaces in the name.

11. In the **Mounting** drop down list, select **Custom**.
The **Default** option does not ensure that the file system will be mounted on the next boot.
12. In the **Mount Point** field, add the mount path.
13. Select **Mount at boot**.
14. Click **Create partition**.



Formatting can take several minutes depending on used formatting options and size of RAID.

After successful finish, you can continue with creating other partitions.

At this point, the system uses mounted and formatted RAID.

10.2.5. Using the web console for creating a volume group on top of RAID

This section shows you how to build a volume group from software RAID.

Prerequisites

- RAID device, which is not formatted and mounted.

Procedure

1. Open the RHEL 8 web console.
2. Click **Storage**.
3. Click the + icon in the **Volume Groups** box.
4. In the **Create Volume Group** dialog box, enter a name for the new volume group.
5. In the **Disks** list, select a RAID device.

If you do not see the RAID in the list, unmount the RAID from the system. The RAID device must not be used by the RHEL 8 system.

The screenshot shows a 'Create Volume Group' dialog box. It has a 'Name' field containing 'myvolumegroup' and a 'Disks' section where a checkbox is checked next to '1.90 GiB RAID Device myraid' with the path '/dev/md/myraid'. At the bottom right are 'Cancel' and 'Create' buttons.

6. Click **Create**.

The new volume group has been created and you can continue with creating a logical volume.

The screenshot shows a 'Volume Groups' list. It contains two entries: 'myvolumegroup' (1.90 GiB) and 'rhel' (19.0 GiB). The 'myvolumegroup' entry is highlighted with a red box. A blue '+' button is located at the top right of the list.

10.3. USING THE WEB CONSOLE FOR CONFIGURING LVM LOGICAL VOLUMES

Red Hat Enterprise Linux 8 supports the LVM logical volume manager. When you install a Red Hat Enterprise Linux 8, it will be installed on LVM automatically created during the installation.

Storage » rhel

Volume Group rhel

Rename Delete

UUID m19oY9-aL1C-LkSS-3uez-n8S9-DdO1-MZt96A

Capacity 9.00 GiB, 9.66 GB, 9659482112 bytes

Physical Volumes

+ -

Partition of QEMU HARDDISK (QM00001)
9.00 GiB, 0 free

Logical Volumes

[Create new Logical Volume](#)

File System	Device
8.00 GiB xfs File System	/dev/rhel/root
1 GiB Swap Space	/dev/rhel/swap

The screenshot shows you a clean installation of the RHEL 8 system with two logical volumes in the RHEL 8 web console automatically created during the installation.

To find out more about logical volumes, follow the sections describing:

- [What is logical volume manager and when to use it.](#)
- [What are volume groups and how to create them.](#)
- [What are logical volumes and how to create them.](#)
- [How to format logical volumes.](#)
- [How to resize logical volumes.](#)

Prerequisites

- Physical drives, RAID devices, or any other type of block device from which you can create the logical volume.

10.3.1. Logical Volume Manager in the web console

The RHEL 8 web console provides a graphical interface to create LVM volume groups and logical volumes.

Volume groups create a layer between physical and logical volumes. It makes you possible to add or remove physical volumes without influencing logical volume itself. Volume groups appear as one drive with capacity consisting of capacities of all physical drives included in the group.

You can join physical drives into volume groups in the web console.

Logical volumes act as a single physical drive and it is built on top of a volume group in your system.

Main advantages of logical volumes are:

- Better flexibility than the partitioning system used on your physical drive.
- Ability to connect more physical drives into one volume.
- Possibility of expanding (growing) or reducing (shrinking) capacity of the volume on-line, without restart.
- Ability to create snapshots.

Additional resources

- For details, see [Configuring and managing logical volumes](#).

10.3.2. Creating volume groups in the web console

The following describes creating volume groups from one or more physical drives or other storage devices. Logical volumes are created from volume groups.

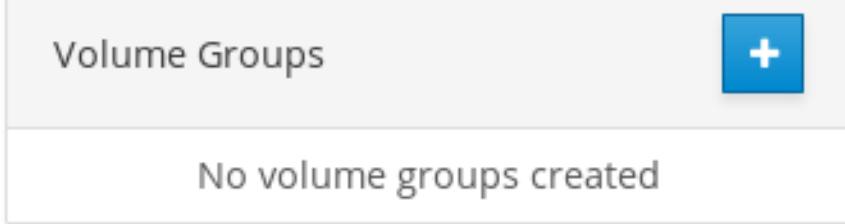
Each volume group can include multiple logical volumes.

For details, see [Volume groups](#).

Prerequisites

- Physical drives or other types of storage devices from which you want to create volume groups.

Procedure

1. Log in to the RHEL 8 web console.
2. Click **Storage**.
3. Click the + icon in the **Volume Groups** box.


The screenshot shows the 'Volume Groups' section of the Storage interface. At the top, it says 'Volume Groups' and has a blue '+' button. Below that, it says 'No volume groups created'.
4. In the **Name** field, enter a name of a group without spaces.
5. Select the drives you want to combine to create the volume group.

Create Volume Group

Name	myvolumegroup
Disks	<input checked="" type="checkbox"/> 10.0 GiB Partition of QEMU QEMU HARDDISK (DISK1) /dev/sda1 <input checked="" type="checkbox"/> 20.0 GiB RAID Device 127 /dev/md/127
<input type="button" value="Cancel"/> <input type="button" value="Create"/>	

It might happen that you cannot see devices as you expected. The RHEL web console displays only unused block devices. Used devices means, for example:

- Devices formatted with a file system
- Physical volumes in another volume group
- Physical volumes being a member of another software RAID device
If you do not see the device, format it to be empty and unused.

6. Click **Create**.

The web console adds the volume group in the **Volume Groups** section. After clicking the group, you can create logical volumes that are allocated from that volume group.

Volume Groups

	myvolumegroup	
	30.0 GiB	

10.3.3. Creating logical volumes in the web console

The following steps describe how to create LVM logical volumes.

Prerequisites

- Volume group created. For details, see [Creating volume groups in the web console](#) .

Procedure

1. Log in to the RHEL 8 web console.
2. Click **Storage**.
3. Click the volume group in which you want to create logical volumes.

4. Click **Create new Logical Volume**

5. In the **Name** field, enter a name for the new logical volume without spaces.

6. In the **Purpose** drop down menu, select **Block device for filesystems**.

This configuration enables you to create a logical volume with the maximum volume size which is equal to the sum of the capacities of all drives included in the volume group.

Create Logical Volume

Name	mylogicalvolume
Purpose	Block device for filesystems
Size	Block device for filesystems Pool for thinly provisioned volumes

Create

7. Define the size of the logical volume. Consider:

- How much space the system using this logical volume will need.
- How many logical volumes you want to create.

You do not have to use the whole space. If necessary, you can grow the logical volume later.

Create Logical Volume

Name	mylogicalvolume
Purpose	Block device for filesystems
Size	20 GiB

Create

8. Click **Create**.

To verify the settings, click your logical volume and check the details.

Logical Volumes

 [Create new Logical Volume](#)



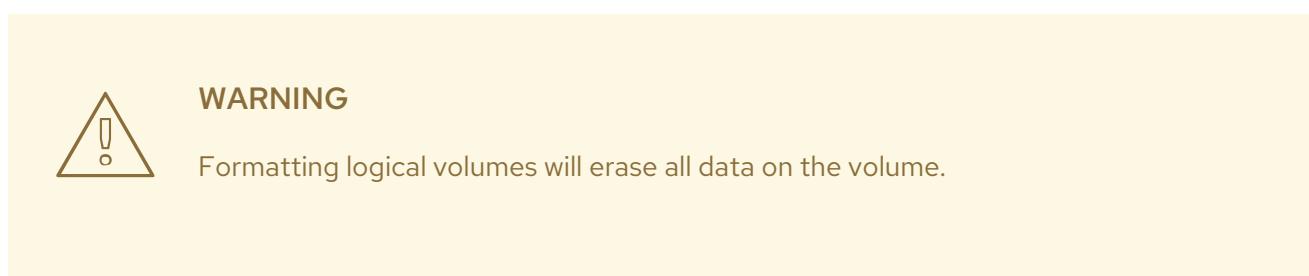
30.0 GiB Unrecognized Data `/dev/myvolumegroup/mylogicalvolume`

Volume	Unrecognized Data	Deactivate	Delete
Usage	-		Format
Type	-		

At this stage, the logical volume has been created and you need to create and mount a file system with the formatting process.

10.3.4. Formatting logical volumes in the web console

Logical volumes act as physical drives. To use them, you need to format them with a file system.



The file system you select determines the configuration parameters you can use for logical volumes. For example, some the XFS file system does not support shrinking volumes. For details, see [Resizing logical volumes in the web console](#).

The following steps describe the procedure to format logical volumes.

Prerequisites

- Logical volume created. For details, see [Creating volume groups in the web console](#) .

Procedure

1. Log in to the RHEL web console.
2. Click **Storage**.
3. Click the volume group in which the logical volume is placed.
4. Click the logical volume.
5. Click on the **Unrecognized Data** tab.

Logical Volumes

 Create new Logical Volume



The screenshot shows the 'Logical Volumes' section of the RHEL 8 web console. A logical volume named 'mylogicalvolume' is selected. The volume size is listed as '30.0 GiB Unrecognized Data'. The path is '/dev/myvolumegroup/mylogicalvolume'. Below the volume name, there are buttons for 'Deactivate' and 'Delete'. Further down, there are 'Usage' and 'Type' dropdown menus, and a prominent 'Format' button.

6. Click **Format**.
 7. In the **Erase** drop down menu, select:
 - **Don't overwrite existing data** – the RHEL web console rewrites only the disk header. Advantage of this option is speed of formatting.
 - **Overwrite existing data with zeros** – the RHEL web console rewrites the whole disk with zeros. This option is slower because the program have to go through the whole disk. Use this option if the disk includes any data and you need to overwrite it.
 8. In the **Type** drop down menu, select a file system:
 - **XFS** file system supports large logical volumes, switching physical drives online without outage, and growing an existing file system. Leave this file system selected if you do not have a different strong preference.
XFS does not support reducing the size of a volume formatted with an XFS file system
 - **ext4** file system supports:
 - Logical volumes
 - Switching physical drives online without outage
 - Growing a file system
 - Shrinking a file system
- You can also select a version with the LUKS (Linux Unified Key Setup) encryption, which allows you to encrypt the volume with a passphrase.
9. In the **Name** field, enter the logical volume name.
 10. In the **Mounting** drop down menu, select **Custom**.
The **Default** option does not ensure that the file system will be mounted on the next boot.
 11. In the **Mount Point** field, add the mount path.
 12. Select **Mount at boot**.

Format /dev/volumegroup1/thinvolume1

Erase	Don't overwrite existing data
Type	XFS - Red Hat Enterprise Linux 7 default
Name	myfilesystem
Mounting	Custom
Mount Point	/media
Mount options	<input checked="" type="checkbox"/> Mount at boot <input type="checkbox"/> Mount read only <input type="checkbox"/> Custom mount options
Formatting a storage device will erase all data on it.	
Cancel Format	

13. Click **Format**.

Formatting can take several minutes depending on the volume size and which formatting options are selected.

After the formatting has completed successfully, you can see the details of the formatted logical volume on the **Filesystem** tab.

20 GiB xfs File System		/dev/myvolumegroup/mylogicalvolume
Volume	Filesystem	
		Deactivate Delete
		Format
Name	myfilesystem	
Mount Point	(default)	Mount
Used	-	

14. To use the logical volume, click **Mount**.

At this point, the system can use mounted and formatted logical volume.

10.3.5. Resizing logical volumes in the web console

This section describes how to resize logical volumes. You can extend or even reduce logical volumes. Whether you can resize a logical volume depends on which file system you are using. Most file systems enable you to extend (grow) the volume online (without outage).

You can also reduce (shrink) the size of logical volumes, if the logical volume contains a file system which supports shrinking. It should be available, for example, in the ext3/ext4 file systems.

**WARNING**

You cannot reduce volumes that contains GFS2 or XFS filesystem.

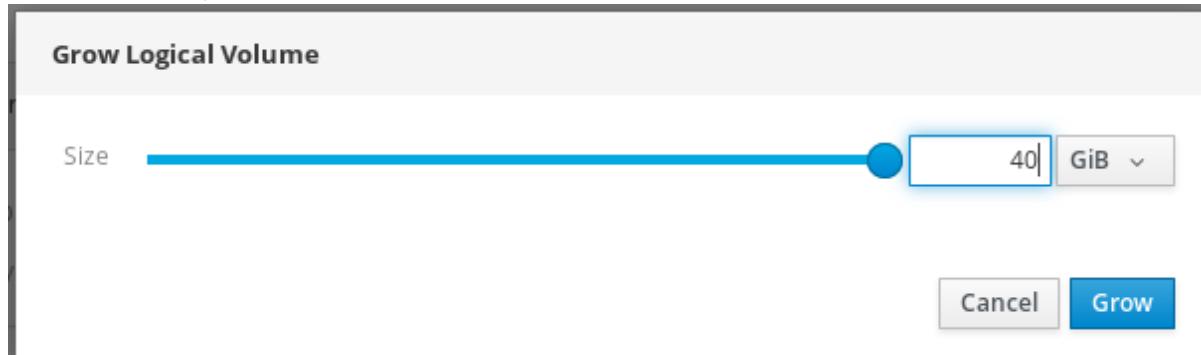
Prerequisites

- Existing logical volume containing a file system which supports resizing logical volumes.

Procedure

The following steps provide the procedure for growing a logical volume without taking the volume offline:

1. Log in to the RHEL web console.
2. Click **Storage**.
3. Click the volume group in which the logical volume is placed.
4. Click the logical volume.
5. On the **Volume** tab, click **Grow**.
6. In the **Grow Logical Volume** dialog box, adjust volume space.



7. Click **Grow**.

LVM grows the logical volume without system outage.

10.3.6. Related information

- For more details on creating logical volumes, see [Configuring and managing logical volumes](#).

10.4. USING THE WEB CONSOLE FOR CONFIGURING THIN LOGICAL VOLUMES

Thinly-provisioned logical volumes enables you to allocate more space for designated applications or servers than how much space logical volumes actually contain.

For details, see [Thinly-provisioned logical volumes \(thin volumes\)](#).

The following sections describe:

- [Creating pools for the thinly provisioned logical volumes.](#)
- [Creating thin logical volumes.](#)
- [Formatting thin logical volumes.](#)

Prerequisites

- Physical drives or other types of storage devices from which you want to create volume groups.

10.4.1. Creating pools for thin logical volumes in the web console

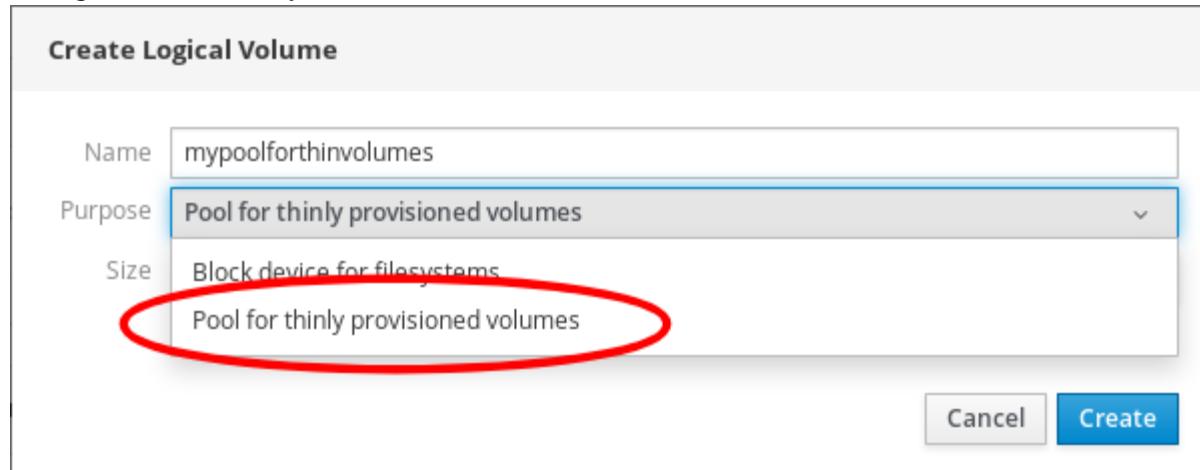
The following steps show you how to create a pool for thinly provisioned volumes:

Prerequisites

- [Volume group created.](#)

Procedure

1. Log in to the RHEL 8 web console.
2. Click **Storage**.
3. Click the volume group in which you want to create thin volumes.
4. Click **Create new Logical Volume**
5. In the **Name** field, enter a name for the new pool of thin volumes without spaces.
6. In the **Purpose** drop down menu, select **Pool for thinly provisioned volumes**. This configuration enables you to create the thin volume.



7. Define the size of the pool of thin volumes. Consider:

- How many thin volumes you will need in this pool?
- What is the expected size of each thin volume?

You do not have to use the whole space. If necessary, you can grow the pool later.

Create Logical Volume

Name	mypoolforthinvolumes
Purpose	Pool for thinly provisioned volumes
Size	60 GiB

Create

8. Click **Create**.

The pool for thin volumes has been created and you can add thin volumes.

10.4.2. Creating thin logical volumes in the web console

The following text describes creating a thin logical volume in the pool. The pool can include multiple thin volumes and each thin volume can be as large as the pool for thin volumes itself.



IMPORTANT

Using thin volumes requires regular checkup of actual free physical space of the logical volume.

Prerequisites

- Pool for thin volumes created. For details, see [Creating volume groups in the web console](#) .

Procedure

1. Log in to the RHEL 8 web console.
2. Click **Storage**.
3. Click the volume group in which you want to create thin volumes.
4. Click the desired pool.
5. Click **Create Thin Volume**.

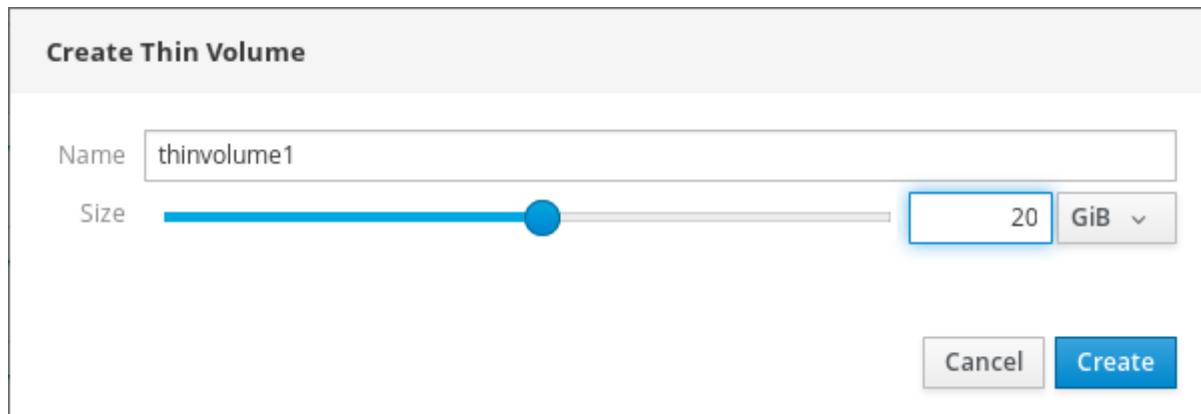
Logical Volumes

Create new Logical Volume

Pool	Name	Size	Actions
60 GiB Pool for Thin Volumes	thinlogicalvolume	60 GiB	Create Thin Volume
		Grow	Deactivate Delete
	Name: thinlogicalvolume		
	Size: 60 GiB	Grow	
	Data Used: 0%		
	Metadata Used: 10%		

6. In the **Create Thin Volume** dialog box, enter a name for the thin volume without spaces.

7. Define the size of the thin volume.



8. Click **Create**.

At this stage, the thin logical volume has been created and you need to format it.

10.4.3. Formatting logical volumes in the web console

Logical volumes act as physical drives. To use them, you need to format them with a file system.



WARNING

Formatting logical volumes will erase all data on the volume.

The file system you select determines the configuration parameters you can use for logical volumes. For example, some the XFS file system does not support shrinking volumes. For details, see [Resizing logical volumes in the web console](#).

The following steps describe the procedure to format logical volumes.

Prerequisites

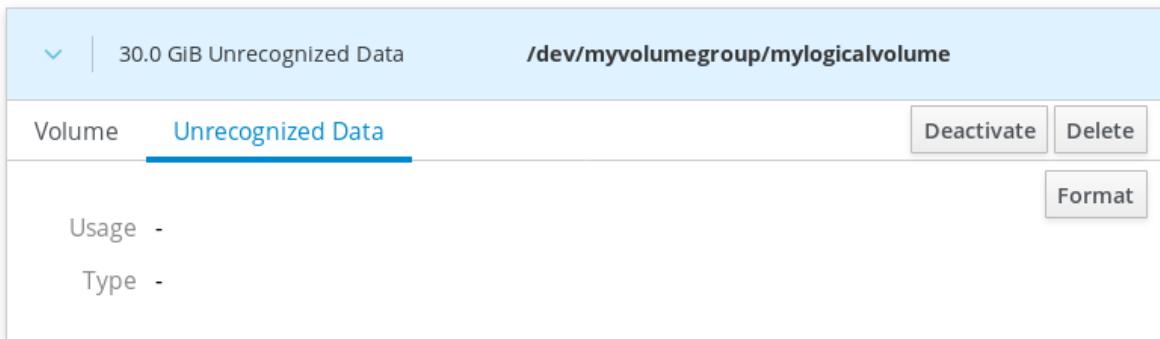
- Logical volume created. For details, see [Creating volume groups in the web console](#) .

Procedure

1. Log in to the RHEL web console.
2. Click **Storage**.
3. Click the volume group in which the logical volume is placed.
4. Click the logical volume.
5. Click on the **Unrecognized Data** tab.

Logical Volumes

 Create new Logical Volume



The screenshot shows the 'Logical Volumes' section of the RHEL 8 web console. A logical volume named 'mylogicalvolume' is selected. The volume size is listed as '30.0 GiB Unrecognized Data'. The path is shown as '/dev/myvolumegroup/mylogicalvolume'. Below the volume name, there are buttons for 'Deactivate' and 'Delete'. Further down, there are 'Usage' and 'Type' dropdown menus, and a prominent 'Format' button.

6. Click **Format**.
 7. In the **Erase** drop down menu, select:
 - **Don't overwrite existing data** – the RHEL web console rewrites only the disk header. Advantage of this option is speed of formatting.
 - **Overwrite existing data with zeros** – the RHEL web console rewrites the whole disk with zeros. This option is slower because the program have to go through the whole disk. Use this option if the disk includes any data and you need to overwrite it.
 8. In the **Type** drop down menu, select a file system:
 - **XFS** file system supports large logical volumes, switching physical drives online without outage, and growing an existing file system. Leave this file system selected if you do not have a different strong preference.
XFS does not support reducing the size of a volume formatted with an XFS file system
 - **ext4** file system supports:
 - Logical volumes
 - Switching physical drives online without outage
 - Growing a file system
 - Shrinking a file system
- You can also select a version with the LUKS (Linux Unified Key Setup) encryption, which allows you to encrypt the volume with a passphrase.
9. In the **Name** field, enter the logical volume name.
 10. In the **Mounting** drop down menu, select **Custom**.
The **Default** option does not ensure that the file system will be mounted on the next boot.
 11. In the **Mount Point** field, add the mount path.
 12. Select **Mount at boot**.

Format /dev/volumegroup1/thinvolume1

Erase	Don't overwrite existing data
Type	XFS - Red Hat Enterprise Linux 7 default
Name	myfilesystem
Mounting	Custom
Mount Point	/media
Mount options	<input checked="" type="checkbox"/> Mount at boot <input type="checkbox"/> Mount read only <input type="checkbox"/> Custom mount options
Formatting a storage device will erase all data on it.	
Cancel Format	

13. Click **Format**.

Formatting can take several minutes depending on the volume size and which formatting options are selected.

After the formatting has completed successfully, you can see the details of the formatted logical volume on the **Filesystem** tab.

20 GiB xfs File System		/dev/myvolumegroup/mylogicalvolume
Volume	Filesystem	
		Deactivate Delete
		Format
	Name myfilesystem Mount Point (default) Mount Used -	

14. To use the logical volume, click **Mount**.

At this point, the system can use mounted and formatted logical volume.

10.5. USING THE WEB CONSOLE FOR CHANGING PHYSICAL DRIVES IN VOLUME GROUPS

The following text describes how to change the drive in a volume group using the RHEL 8 web console.

The change of physical drives consists of the following procedures:

- Adding physical drives from logical volumes.
- Removing physical drives from logical volumes.

Prerequisites

- A new physical drive for replacing the old or broken one.
- The configuration expects that physical drives are organized in a volume group.

10.5.1. Adding physical drives to volume groups in the web console

The RHEL 8 web console enables you to add a new physical drive or other type of volume to the existing logical volume.

Prerequisites

- A volume group must be created.
- A new drive connected to the machine.

Procedure

1. Log in to the RHEL 8 web console.
2. Click **Storage**.
3. In the **Volume Groups** box, click the volume group in which you want to add a physical volume.
4. In the **Physical Volumes** box, click the + icon.



5. In the **Add Disks** dialog box, select the preferred drive and click **Add**.



As a result, the RHEL 8 web console adds the physical volume. You can see it in the **Physical Volumes** section, and the logical volume can immediately start to write on the drive.

10.5.2. Removing physical drives from volume groups in the web console

If a logical volume includes multiple physical drives, you can remove one of the physical drives online.

The system moves automatically all data from the drive to be removed to other drives during the removal process. Notice that it can take some time.

The web console also verifies, if there is enough space for removing the physical drive.

Prerequisites

- A volume group with more than one physical drive connected.

Procedure

The following steps describe how to remove a drive from the volume group without causing outage in the RHEL web console.

1. Log in to the RHEL 8 web console.
2. Click **Storage**.
3. Click the volume group in which you have the logical volume.
4. In the **Physical Volumes** section, locate the preferred volume.
5. Click the - icon.

The RHEL 8 web console verifies, if the logical volume has enough free space for removing the disk. If not, you cannot remove the disk and it is necessary to add another disk first. For details, see [Adding physical drives to logical volumes in the web console](#) .

Physical Volumes	
	QEMU HARDDISK(DISK1) 20 GiB, 0 free
	QEMU HARDDISK(DISK2) 20 GiB, 20 GiB free
	QEMU HARDDISK(DISK3) 20 GiB, 20 GiB free

As results, the RHEL 8 web console removes the physical volume from the created logical volume without causing an outage.

10.6. USING THE WEB CONSOLE FOR MANAGING VIRTUAL DATA OPTIMIZER VOLUMES

This chapter describes the Virtual Data Optimizer (VDO) configuration using the RHEL 8 web console. After reading it, you will be able to:

- Create VDO volumes
- Format VDO volumes
- Extend VDO volumes

Prerequisites

- The RHEL 8 web console is installed and accessible.
For details, see [Installing the web console](#) .

10.6.1. VDO volumes in the web console

Red Hat Enterprise Linux 8 supports Virtual Data Optimizer (VDO). VDO is a block virtualization technology that combines:

Compression

For details, see [Enabling or disabling compression in VDO](#).

Deduplication

For details, see [Enabling or disabling deduplication in VDO](#).

Thin provisioning

For details, see [Thinly-provisioned logical volumes \(thin volumes\)](#).

Using these technologies, VDO:

- Saves storage space inline
- Compresses files
- Eliminates duplications
- Enables you to allocate more virtual space than how much the physical or logical storage provides
- Enables you to extend the virtual storage by growing

VDO can be created on top of many types of storage. In the RHEL 8 web console, you can configure VDO on top of:

- LVM



NOTE

It is not possible to configure VDO on top of thinly-provisioned volumes.

- Physical volume
- Software RAID

For details about placement of VDO in the Storage Stack, see [System Requirements](#).

Additional resources

- For details about VDO, see [Deduplicating and compressing storage](#).

10.6.2. Creating VDO volumes in the web console

This section helps you to create a VDO volume in the RHEL web console.

Prerequisites

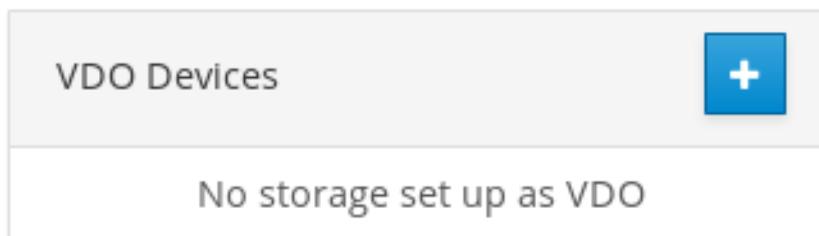
- Physical drives, LVMs, or RAID from which you want to create VDO.

Procedure

1. Log in to the RHEL 8 web console.

For details, see [Logging in to the web console](#).

2. Click **Storage**.
3. Click the + icon in the **VDO Devices** box.



4. In the **Name** field, enter a name of a VDO volume without spaces.
5. Select the drive that you want to use.
6. In the **Logical Size** bar, set up the size of the VDO volume. You can extend it more than ten times, but consider for what purpose you are creating the VDO volume:
 - For active VMs or container storage, use logical size that is ten times the physical size of the volume.
 - For object storage, use logical size that is three times the physical size of the volume.

For details, see [Deploying VDO](#).

7. In the **Index Memory** bar, allocate memory for the VDO volume.
For details about VDO system requirements, see [System Requirements](#).
8. Select the **Compression** option. This option can efficiently reduce various file formats.
For details, see [Enabling or disabling compression in VDO](#).
9. Select the **Deduplication** option.
This option reduces the consumption of storage resources by eliminating multiple copies of duplicate blocks. For details, see [Enabling or disabling deduplication in VDO](#).
10. [Optional] If you want to use the VDO volume with applications that need a 512 bytes block size, select **Use 512 Byte emulation**. This reduces the performance of the VDO volume, but should be very rarely needed. If in doubt, leave it off.
11. Click **Create**.

Create VDO Device

Name	myvirtualdataoptimizer
Disk	<input checked="" type="radio"/> 5.72 GiB RAID Device 127 /dev/md/127
Logical Size	<input type="range"/> 5.76 GiB
Index Memory	<input type="range"/> 256 MiB
Options	<input checked="" type="checkbox"/> Compression <input checked="" type="checkbox"/> Deduplication <input type="checkbox"/> Use 512 Byte emulation
Cancel Create	

If the process of creating the VDO volume succeeds, you can see the new VDO volume in the **Storage** section and format it with a file system.

VDO Devices

	myvirtualdataoptimizer 5.76 GiB	
--	------------------------------------	--

10.6.3. Formatting VDO volumes in the web console

VDO volumes act as physical drives. To use them, you need to format them with a file system.



WARNING

Formatting VDO will erase all data on the volume.

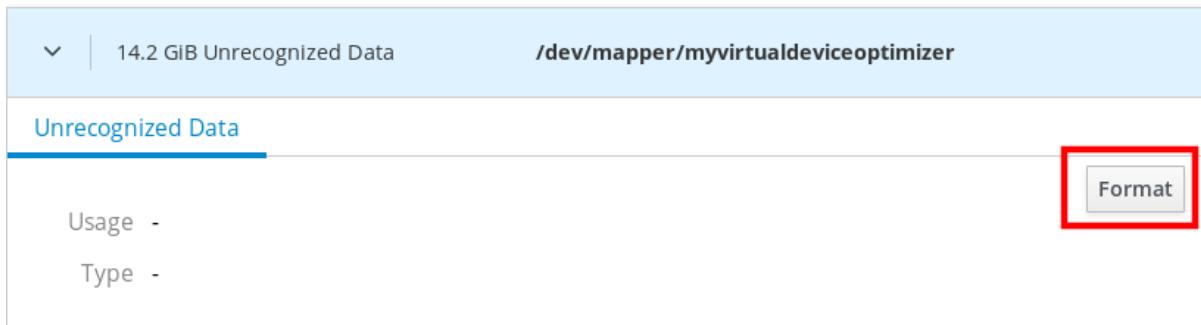
The following steps describe the procedure to format VDO volumes.

Prerequisites

- A VDO volume is created. For details, see [Section 10.6.2, “Creating VDO volumes in the web console”](#).

Procedure

1. Log in to the RHEL 8 web console.
For details, see [Logging in to the web console](#).
2. Click **Storage**.
3. Click the VDO volume.
4. Click on the **Unrecognized Data** tab.
5. Click **Format**.



6. In the **Erase** drop down menu, select:

Don't overwrite existing data

The RHEL web console rewrites only the disk header. The advantage of this option is the speed of formatting.

Overwrite existing data with zeros

The RHEL web console rewrites the whole disk with zeros. This option is slower because the program has to go through the whole disk. Use this option if the disk includes any data and you need to rewrite them.

7. In the **Type** drop down menu, select a filesystem:

- The **XFS** file system supports large logical volumes, switching physical drives online without outage, and growing. Leave this file system selected if you do not have a different strong preference.
XFS does not support shrinking volumes. Therefore, you will not be able to reduce volume formatted with XFS.
- The **ext4** file system supports logical volumes, switching physical drives online without outage, growing, and shrinking.

You can also select a version with the LUKS (Linux Unified Key Setup) encryption, which allows you to encrypt the volume with a passphrase.

8. In the **Name** field, enter the logical volume name.
9. In the **Mounting** drop down menu, select **Custom**.
The **Default** option does not ensure that the file system will be mounted on the next boot.
10. In the **Mount Point** field, add the mount path.
11. Select **Mount at boot**.

Format /dev/volumegroup1/thinvolume1

Erase	Don't overwrite existing data
Type	XFS - Red Hat Enterprise Linux 7 default
Name	myfilesystem
Mounting	Custom
Mount Point	/media
Mount options	<input checked="" type="checkbox"/> Mount at boot <input type="checkbox"/> Mount read only <input type="checkbox"/> Custom mount options
Formatting a storage device will erase all data on it.	
Cancel Format	

12. Click **Format**.

Formatting can take several minutes depending on the used formatting options and the volume size.

After a successful finish, you can see the details of the formatted VDO volume on the **Filesystem** tab.

▼	5.76 GiB xfs File System	/dev/mapper/myvirtualdataoptimizer
Filesystem		
Name	myfilesystem	Format
Mount Point	(default)	Mount
Used	-	

13. To use the VDO volume, click **Mount**.

At this point, the system uses the mounted and formatted VDO volume.

10.6.4. Extending VDO volumes in the web console

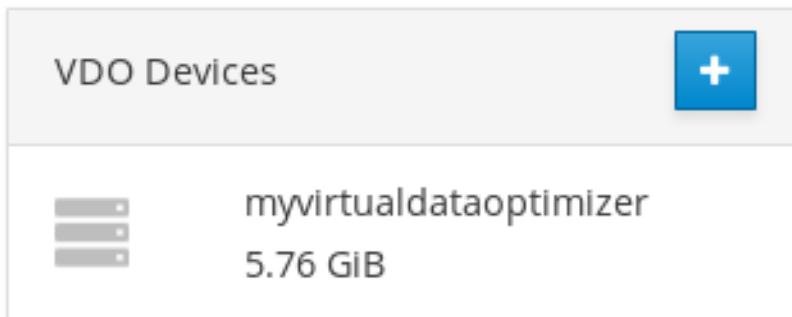
This section describes extending VDO volumes in the RHEL 8 web console.

Prerequisites

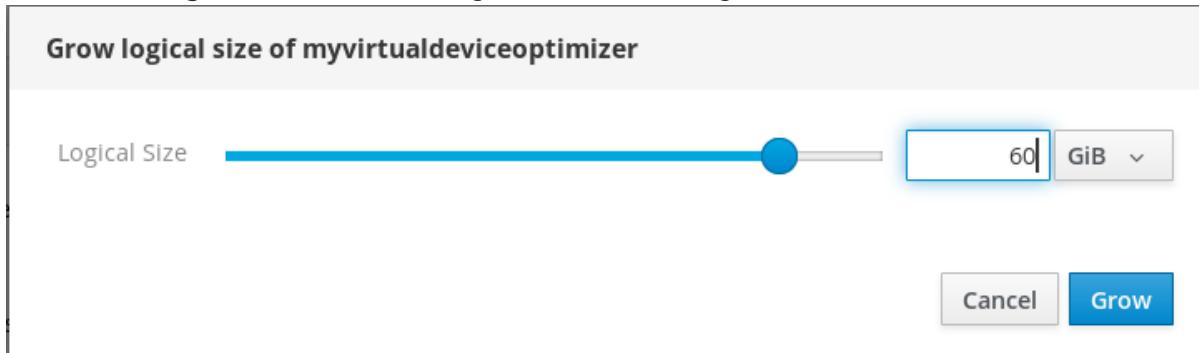
- The VDO volume created.

Procedure

1. Log in to the RHEL 8 web console.
For details, see [Logging in to the web console](#).
2. Click **Storage**.
3. Click your VDO volume in the **VDO Devices** box.



4. In the VDO volume details, click the **Grow** button.
5. In the **Grow logical size of VDO** dialog box, extend the logical size of the VDO volume.



Original size of the logical volume from the screenshot was 6 GB. As you can see, the RHEL web console enables you to grow the volume to more than ten times the size and it works correctly because of the compression and deduplication.

6. Click **Grow**.

If the process of growing VDO succeeds, you can see the new size in the VDO volume details.

VDO Device myvirtualdataoptimizer

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 (90% saved) 60 GiB Grow

Index Memory 256 MiB

Compression ON OFF

Deduplication ON OFF

10.7. LOCKING DATA WITH LUKS PASSWORD IN THE RHEL WEB CONSOLE

In the web console's **Storage** tab, you can now create, lock, unlock, resize, and otherwise configure encrypted devices using the LUKS (Linux Unified Key Setup) version 2 format.

This new version of LUKS offers:

- More flexible unlocking policies
- Stronger cryptography
- Better compatibility with future changes

10.7.1. LUKS disk encryption

The Linux Unified Key Setup-on-disk-format (LUKS) enables you to encrypt block devices and it provides a set of tools that simplifies managing the encrypted devices. LUKS allows multiple user keys to decrypt a master key, which is used for the bulk encryption of the partition.

RHEL utilizes LUKS to perform block device encryption. By default, the option to encrypt the block device is unchecked during the installation. If you select the option to encrypt your disk, the system prompts you for a passphrase every time you boot the computer. This passphrase "unlocks" the bulk encryption key that decrypts your partition. If you choose to modify the default partition table, you can choose which partitions you want to encrypt. This is set in the partition table settings.

What LUKS does

- LUKS encrypts entire block devices and is therefore well-suited for protecting contents of mobile devices such as removable storage media or laptop disk drives.

- The underlying contents of the encrypted block device are arbitrary, which makes it useful for encrypting swap devices. This can also be useful with certain databases that use specially formatted block devices for data storage.
- LUKS uses the existing device mapper kernel subsystem.
- LUKS provides passphrase strengthening which protects against dictionary attacks.
- LUKS devices contain multiple key slots, allowing users to add backup keys or passphrases.

What LUKS does not do

- Disk-encryption solutions like LUKS protect the data only when your system is off. Once the system is on and LUKS has decrypted the disk, the files on that disk are available to anyone who would normally have access to them.
- LUKS is not well-suited for scenarios that require many users to have distinct access keys to the same device. The LUKS1 format provides eight key slots, LUKS2 up to 32 key slots.
- LUKS is not well-suited for applications requiring file-level encryption.

Ciphers

The default cipher used for LUKS is **aes-xts-plain64**. The default key size for LUKS is 512 bits. The default key size for LUKS with **Anaconda** (XTS mode) is 512 bits. Ciphers that are available are:

- AES - Advanced Encryption Standard - [FIPS PUB 197](#)
- Twofish (a 128-bit block cipher)
- Serpent

Additional resources

- [LUKS Project Home Page](#)
- [LUKS On-Disk Format Specification](#)

10.7.2. Configuring the LUKS passphrase in the web console

If you want to add encryption to an existing logical volume on your system, you can only do so through formatting the volume.

Prerequisites

- The web console must be installed and accessible.
For details, see [Installing the web console](#).
- Available existing logical volume without encryption.

Procedure

1. Log in to the RHEL 8 web console.
For details, see [Logging in to the web console](#).
2. Click **Storage**.

3. Select the storage device you want to format.
4. Click the menu icon and select **Format** option.
5. Select the **Encrypt data** box to activate encryption on your storage device.

The screenshot shows a configuration dialog box titled "Encrypt data". It contains two input fields: "Passphrase" and "Confirm", both of which are currently empty. Below these fields is a group of four checkboxes:

- Store passphrase
- Unlock at boot
- Unlock read only
- Custom encryption options

The "Unlock at boot" checkbox is checked.

6. Set and confirm your new passphrase.
7. [Optional] Modify further encryption options.
8. Finalize formatting settings.
9. Click **Format**.

10.7.3. Changing the LUKS passphrase in the web console

This procedure describes how to change a LUKS passphrase on an encrypted disk or partition in the web console.

Prerequisites

- The web console must be installed and accessible.
For details, see [Installing the web console](#).

Procedure

1. Log in to the web console.
For details, see [Logging in to the web console](#).
2. Click **Storage**
3. In the Drives table, select the disk with encrypted data.
4. In **Content**, select the encrypted partition.
5. Click **Encryption**.

6. In the **Keys** table, click the pen icon.



7. In the **Change passphrase** dialog window:

- Enter your current passphrase.
- Enter your new passphrase.
- Confirm your new passphrase.

Change passphrase

Old passphrase

New passphrase

Repeat passphrase

Cancel Save

8. Click **Save**

CHAPTER 11. MANAGING SOFTWARE UPDATES IN THE WEB CONSOLE

The Software Updates module in the web console is based on the **yum** utility. For more information about updating software with **yum**, see the [Checking for updates and updating packages](#) section in the [Configuring basic system settings](#) title.

11.1. MANAGING MANUAL SOFTWARE UPDATES IN THE WEB CONSOLE

This section describes how to manually update your software using the web console.

Prerequisites

- The web console must be installed and accessible.
For details, see [Installing the web console](#).

Procedure

1. Log in to the RHEL 8 web console.
For details, see [Logging in to the web console](#).
2. Click **Software Updates**.
The list of available updates refreshes automatically if the last check happened more than 24 hours ago. To trigger a refresh, click the **Check for Updates** button.
3. Apply updates.
 - a. To install all available updates, click the **Install all updates** button.

A blue rectangular button with white text that reads "Install All Updates".

- b. If you have security updates available, you can install them separately by clicking the **Install Security Updates** button.

A light gray rectangular button with black text that reads "Install Security Updates".

You can watch the update log while the update is running.

4. After the system applies updates, you get a recommendation to restart your system. We recommend this especially if the update included a new kernel or system services that you do not want to restart individually.
5. Click **Ignore** to cancel the restart, or **Restart Now** to proceed with restarting your system. After the system restart, log in to the web console and go to the **Software Updates** page to verify that the update has been successful.

11.2. MANAGING AUTOMATIC SOFTWARE UPDATES IN THE WEB CONSOLE

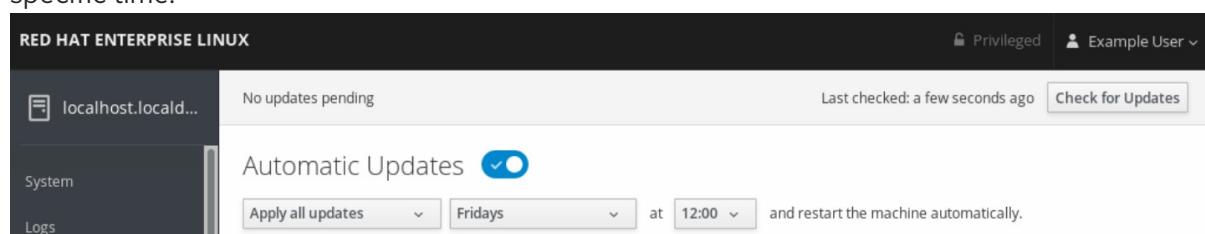
In the web console, you can choose to apply all updates, or security updates and also manage periodicity and time of your automatic updates.

Prerequisites

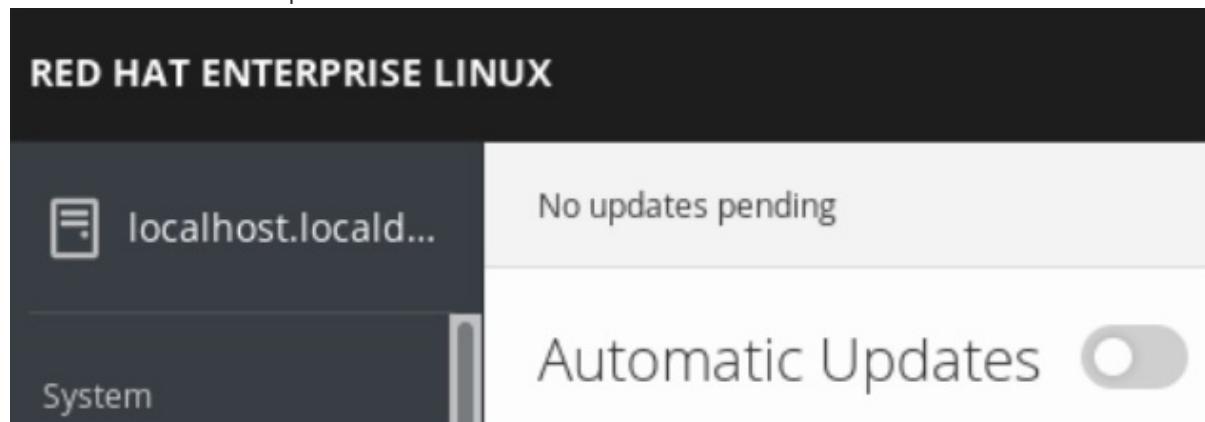
- The web console must be installed and accessible. For details, see [Installing the web console](#).

Procedure

- Log in to RHEL 8 web console.
For details, see [Logging in to the web console](#).
- Click **Software Updates**.
- If you want to automatically apply only security updates, click on the **Apply all updates** drop-down menu and select **Apply security updates**.
- To modify day of the automatic update, click on the **every day** drop-down menu and select a specific day.
- To modify time of the automatic update, click on the **6:00** drop-down menu and select a specific time.



- If you want to disable automatic software updates, click on switch next to **Automatic Updates** to move it to disabled position.



CHAPTER 12. MANAGING SUBSCRIPTIONS IN THE WEB CONSOLE

The RHEL 8 web console can help you to register and manage your subscription for Red Hat Enterprise Linux 8.

To get a subscription for your Red Hat Enterprise Linux, you need to have an account in the [Red Hat Customer Portal](#) or an activation key.

This chapter covers:

- Subscription management in the RHEL 8 web console.
- Registering subscriptions for your system in the web console with the Red Hat user name and password.
- Registering subscriptions with the activation key.

Prerequisites

- Purchased subscriptions.
- The system subjected to subscription has to be connected to the Internet because the web console needs to communicate with the Red Hat Customer Portal.

12.1. SUBSCRIPTION MANAGEMENT IN THE WEB CONSOLE

The RHEL 8 web console provides an interface for using Red Hat Subscription Manager installed on your local system. The Subscription Manager connects to the Red Hat Customer Portal and verifies all available:

- Active subscriptions
- Expired subscriptions
- Renewed subscriptions

If you want to renew the subscription or get a different one in Red Hat Customer Portal, you do not have to update the Subscription Manager data manually. The Subscription Manager synchronizes data with Red Hat Customer Portal automatically.

12.2. REGISTERING SUBSCRIPTIONS WITH CREDENTIALS IN THE WEB CONSOLE

Use the following steps to register a newly installed Red Hat Enterprise Linux using the RHEL 8 web console.

Prerequisites

- A valid user account on the Red Hat Customer Portal.
See the [Create a Red Hat Login](#) page.
- Active subscription for your RHEL system.

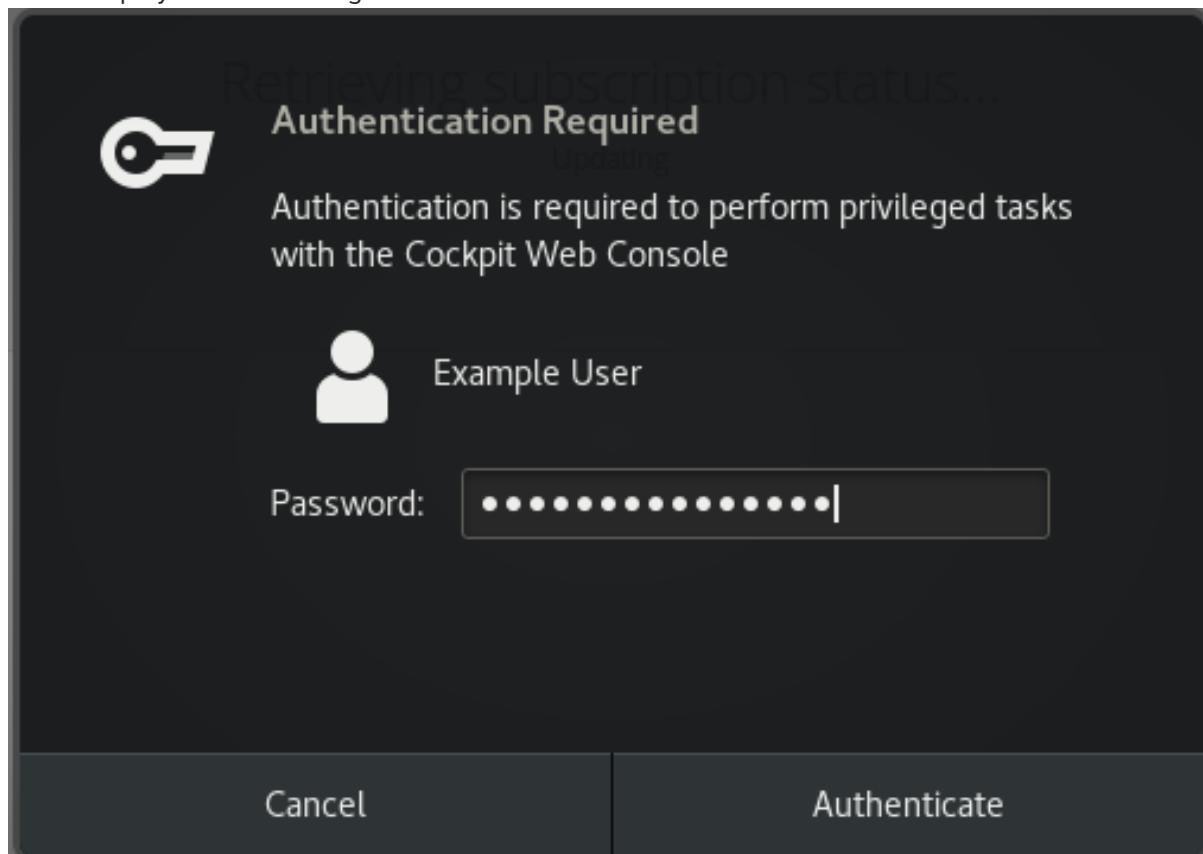
Procedure

1. Type subscription in the search field and press the **Enter** key.



Alternatively, you can log in to the RHEL 8 web console. For details, see [Logging in to the web console](#).

2. In the **polkit** authentication dialog for privileged tasks, add the password belonging to the user name displayed in the dialog.



3. Click **Authenticate**.
4. In the **Subscriptions** dialog box, click **Register**.

The screenshot shows the 'Subscriptions' page with the following details:

- Status:** This system is currently not registered.
- System Purpose:**
 - Status: Unknown
 - Usage: Development/Test
 - Role: Red Hat Enterprise Linux Workstation

A blue 'Register' button is visible at the top right of the page.

5. Enter your Customer Portal credentials.

The 'Register System' dialog box contains the following fields:

URL	Default
Proxy	<input type="checkbox"/> I would like to connect via an HTTP proxy.
Login	example.user@redhat.com
Password	*****
Activation Key	key_one,key_two
Organization	

At the bottom right are 'Cancel' and 'Register' buttons, with 'Register' being blue.

6. Enter the name of your organization.

If you have more than one account on the Red Hat Customer Portal, you have to add the organization name or organization ID. To get the org ID, go to your Red Hat contact point.

7. Click the **Register** button.

At this point, your Red Hat Enterprise Linux 8 system has been successfully registered.

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

12.3. REGISTERING SUBSCRIPTIONS WITH ACTIVATION KEYS IN THE WEB CONSOLE

To register a subscription for Red Hat Enterprise Linux,

Prerequisites

- If you do not have a user account in the portal, your vendor provides you with the activation key.

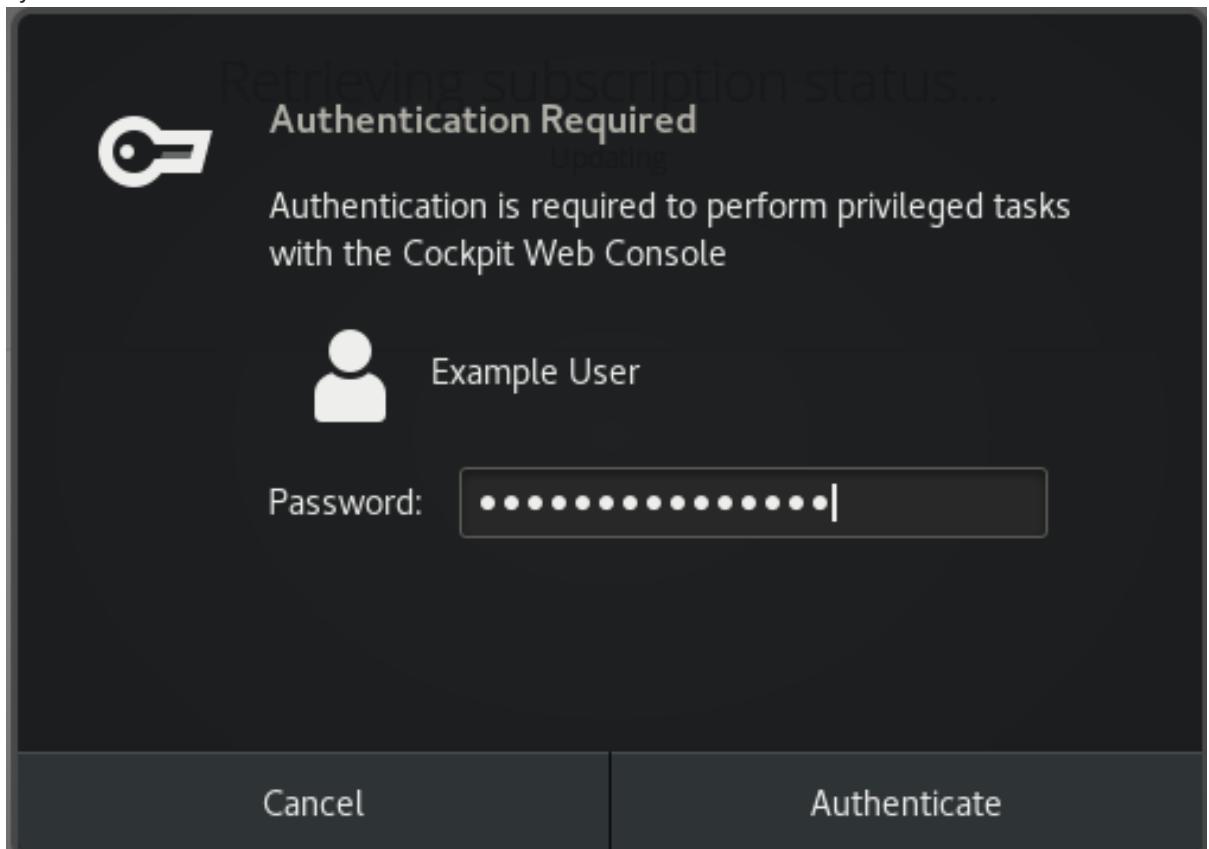
Procedure

1. Type subscription in the search field and press the **Enter** key.

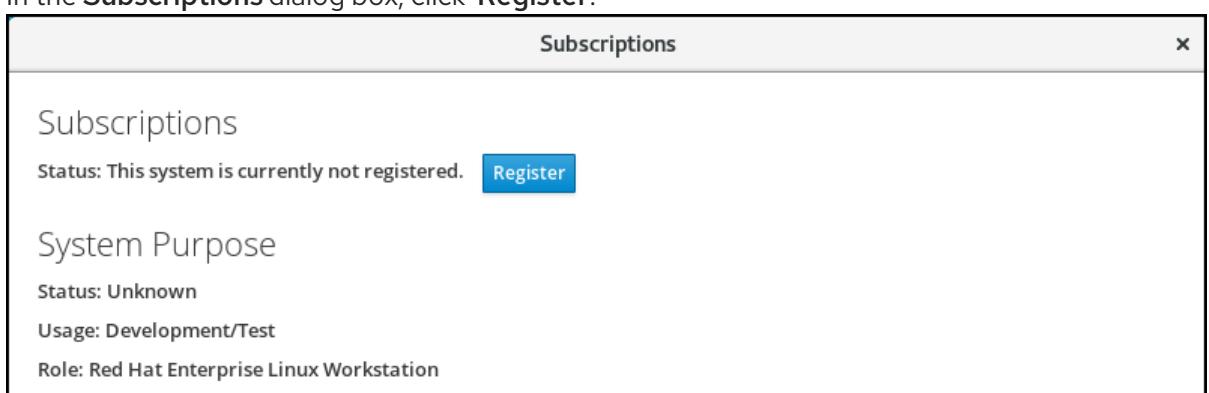


Alternatively, you can log in to the RHEL 8 web console. For details, see [Logging in to the web console](#).

2. In the authentication dialog, add the system username and password you created during the system installation.



3. Click **Authenticate**.
4. In the **Subscriptions** dialog box, click **Register**.



5. Enter the activation key in the registration form.

6. Enter the name of your organization.

You need to add the organization name or organization ID, if you have more than one account in the Red Hat Customer Portal.

To get the org ID, go to your Red Hat contact point.

The screenshot shows a 'Register System' dialog box. It contains the following fields:

- URL: Default
- Proxy: I would like to connect via an HTTP proxy.
- Login: (empty input field)
- Password: (empty input field)
- Activation Key: 3b19c539-f8d4-0123-9d91-g1a12345d9cf0
- Organization: 98765432 (this field is highlighted with a blue border)

At the bottom right are two buttons: 'Cancel' and 'Register' (in a blue box).

7. Click the **Register** button.

At this point, your RHEL 8 system has been successfully registered.

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

CHAPTER 13. CONFIGURING KDUMP IN THE WEB CONSOLE

The following sections provide an overview of how to setup and test the **kdump** configuration through the Red Hat Enterprise Linux web console. The web console is part of a default installation of Red Hat Enterprise Linux 8 and enables or disables the **kdump** service at boot time. Further, the web console conveniently enables you to configure the reserved memory for **kdump**; or to select the *vmcore* saving location in an uncompressed or compressed format.

Prerequisites

- See [Red Hat Enterprise Linux web console](#) for further details.

13.1. CONFIGURING KDUMP MEMORY USAGE AND TARGET LOCATION IN WEB CONSOLE

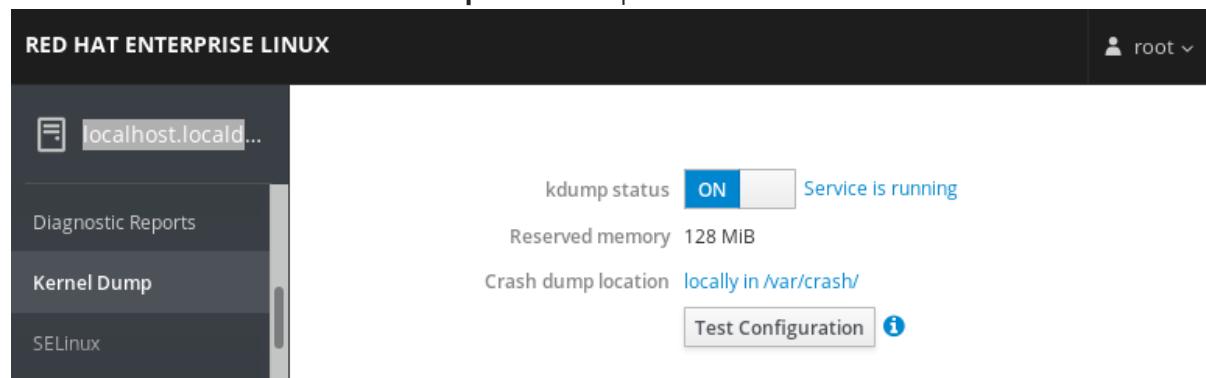
The procedure below shows you how to use the **Kernel Dump** tab in the Red Hat Enterprise Linux web console interface to configure the amount of memory that is reserved for the kdump kernel. The procedure also describes how to specify the target location of the *vmcore* dump file and how to test your configuration.

Prerequisites

- Introduction to operating the [web console](#)

Procedure

1. Open the **Kernel Dump** tab and start the **kdump** service.
2. Configure the **kdump** memory usage through the [command line](#).
3. Click the link next to the **Crash dump location** option.



4. Select the **Local Filesystem** option from the drop-down and specify the directory you want to save the dump in.

Crash dump location

Location	Local Filesystem
Directory	/var/crash/
Compression	<input checked="" type="checkbox"/> Compress crash dumps to save space

Cancel **Apply**

- Alternatively, select the **Remote over SSH** option from the drop-down to send the vmcore to a remote machine using the SSH protocol.
Fill the **Server**, **ssh key**, and **Directory** fields with the remote machine address, ssh key location, and a target directory.
- Another choice is to select the **Remote over NFS** option from the drop-down and fill the **Mount** field to send the vmcore to a remote machine using the NFS protocol.

**NOTE**

Tick the **Compression** check box to reduce the size of the vmcore file.

- Test your configuration by crashing the kernel.

kdump status **ON** Service is running

Reserved memory 128 MiB

Crash dump location [locally in /var/crash/](#)

Test Configuration

**WARNING**

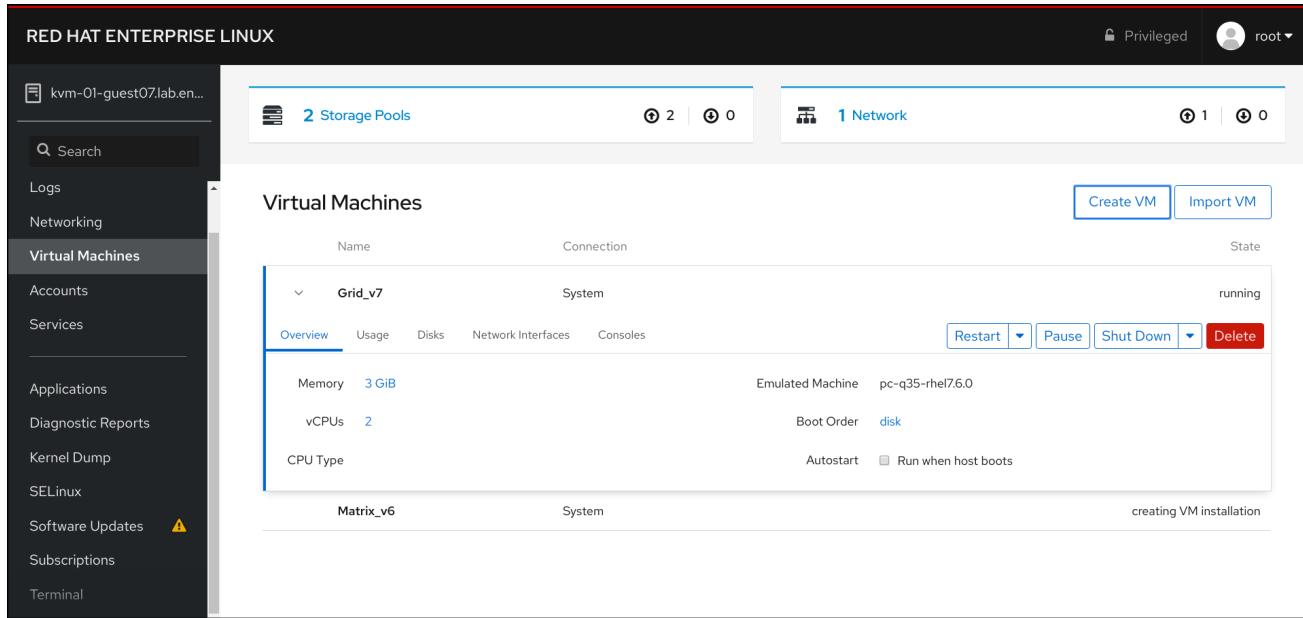
This step disrupts execution of the kernel and results in a system crash and loss of data.

Additional resources

- For a complete list of currently supported targets for **kdump**, see [Supported kdump targets](#).
- For information on how to configure an SSH server and set up a key-based authentication, see [Using secure communications between two systems with OpenSSH](#).

CHAPTER 14. MANAGING VIRTUAL MACHINES IN THE WEB CONSOLE

To manage virtual machines in a graphical interface on a RHEL 8 host, you can use the **Virtual Machines** pane in the [RHEL 8 web console](#).



The following sections describe the web console’s virtualization management capabilities and provide instructions for using them.

14.1. OVERVIEW OF VIRTUAL MACHINE MANAGEMENT USING THE WEB CONSOLE

The RHEL 8 web console is a web-based interface for system administration. With the installation of a [web console plug-in](#), the web console can be used to manage virtual machines (VMs) on connected servers. It provides a graphical view of VMs on a host system to which the web console can connect, and allows monitoring system resources and adjusting configuration with ease.

For a comprehensive list of VM management actions that the web console provides, see [Section 14.3, “Virtual machine management features available in the web console”](#).



NOTE

The Virtual Machine Manager (**virt-manager**) application is still supported in RHEL 8 but has been deprecated. The web console is intended to become its replacement in a subsequent release. It is, therefore, recommended that you get familiar with the web console for managing virtualization in a GUI.

However, in RHEL 8, some features may only be accessible from either **virt-manager** or the command line. For details, see [Section 14.4, “Differences between virtualization features in Virtual Machine Manager and the web console”](#).

For more information on the Virtual Machine Manager, see [RHEL 7 documentation](#).

14.2. SETTING UP THE WEB CONSOLE TO MANAGE VIRTUAL MACHINES

Before using the RHEL 8 web console to manage VMs, you must install the web console virtual machine plug-in.

Prerequisites

- Ensure that the web console is installed on your machine.

```
$ yum info cockpit
Installed Packages
Name      : cockpit
[...]
```

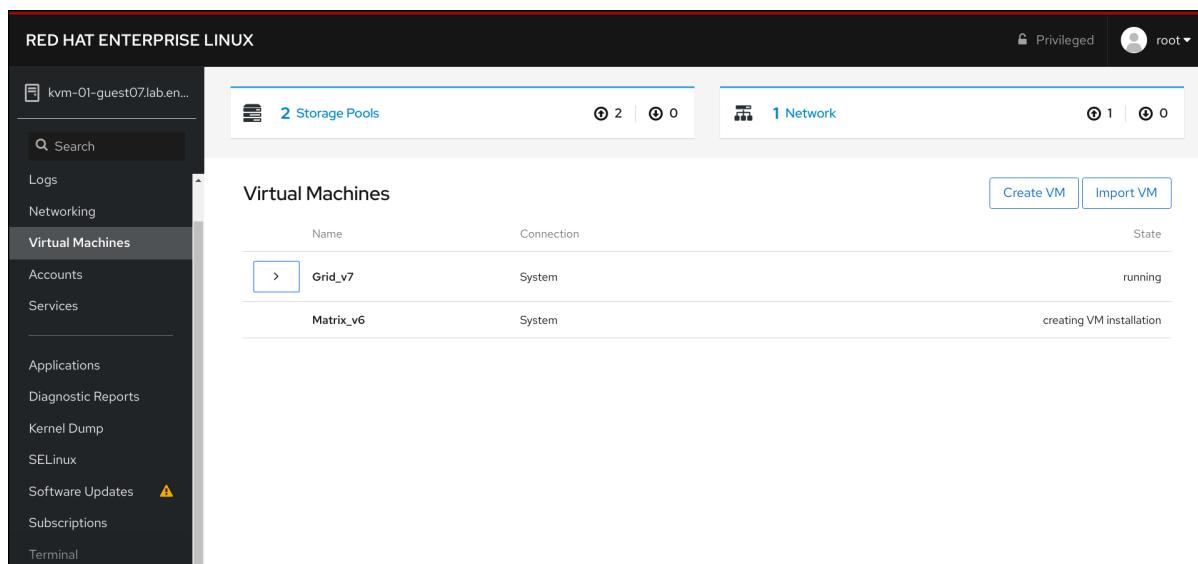
If the web console is not installed, see the [Managing systems using the web console](#) guide for more information about installing the web console.

Procedure

- Install the **cockpit-machines** plug-in.

```
# yum install cockpit-machines
```

If the installation is successful, **Virtual Machines** appears in the web console side menu.



Additional resources

- For instructions on connecting to the web console, as well as other information on using the web console, see the [Managing systems using the RHEL 8 web console](#) document.

14.3. VIRTUAL MACHINE MANAGEMENT FEATURES AVAILABLE IN THE WEB CONSOLE

Using the RHEL 8 web console, you can perform the following actions to manage the virtual machines (VMs) on your system.

- Create a VM and install it with a guest operating system. For details, see [Creating virtual machines and installing guest operating systems using the web console](#).

- Delete a VM. For details, see [Deleting virtual machines using the web console](#).
- Start, shut down, and restart the VM. For details, see [Starting virtual machines using the web console](#) and [Shutting down and restarting virtual machines using the web console](#).
- Connect to and interact with a VM using a variety of consoles. For details, see [Interacting with virtual machines using the web console](#).
- View a variety of information about the VM. For details, see [Viewing virtual machine information using the web console](#).
- Adjust the host memory allocated to a VM. For details, see [Adding and removing virtual machine memory using the web console](#).
- Manage network connections for the VM. For details, see [Using the web console for managing virtual machine network interfaces](#).
- Manage the VM storage available on the host and attach virtual disks to the VM. For details, see [Managing storage for virtual machines using the web console](#).
- Configure the virtual CPU settings of the VM. For details, see [Managing virtual CPUs using the web console](#).

14.4. DIFFERENCES BETWEEN VIRTUALIZATION FEATURES IN VIRTUAL MACHINE MANAGER AND THE WEB CONSOLE

The deprecated Virtual Machine Manager (**virt-manager**) application and its replacement, the RHEL 8 web console, do not have the same functionality. The following table highlights the features that are available in `virt-manager` but not available in the RHEL 8.0 web console.

If a feature is available in a later version of RHEL 8, the minimum RHEL 8 version appears in the *Web console* column.

Feature	Web console	Alternative method using CLI
Setting a virtual machine to start when the host boots	8.1	virsh autostart
Suspending a virtual machine	8.1	virsh suspend
Resuming a suspended virtual machine	8.1	virsh resume

Creating new storage pools of the following types: <ul style="list-style-type: none">• Filesystem Directory• Network File System• iSCSI Target• Physical Disk Device• LVM Volume Group	8.1	virsh pool-define
Creating new storage pools of the following types: <ul style="list-style-type: none">• Partition-based• GlusterFS-based• vHBA-based with SCSI devices• Multipath-based• RBD-based	<i>UNAVAILABLE</i>	virsh pool-define
Creating a new storage volume	8.1	virsh vol-create
Adding a new virtual network	8.1	virsh net-create or virsh net-define
Deleting a virtual network	8.1	virsh net-undefine
Creating a bridge from a host machine's interface to a virtual machine	<i>UNAVAILABLE</i>	virsh iface-bridge
Creating a snapshot	<i>UNAVAILABLE</i>	virsh snapshot-create-as
Reverting to a snapshot	<i>UNAVAILABLE</i>	virsh snapshot-revert
Deleting a snapshot	<i>UNAVAILABLE</i>	virsh snapshot-delete
Cloning a virtual machine	<i>UNAVAILABLE</i>	virt-clone
Migrating a virtual machine to another host machine	<i>UNAVAILABLE</i>	virsh migrate

CHAPTER 15. MANAGING REMOTE SYSTEMS IN THE WEB CONSOLE

The RHEL 8 web console can connect to remote systems and manage them through the user-friendly web interface. The following chapter describes:

- The optimal topology of connected systems.
- What is the Dashboard.
- How to add and remove remote systems.
- When, why and how to use SSH keys for remote system authentication.

Prerequisites

- Opened the SSH service on remote systems.

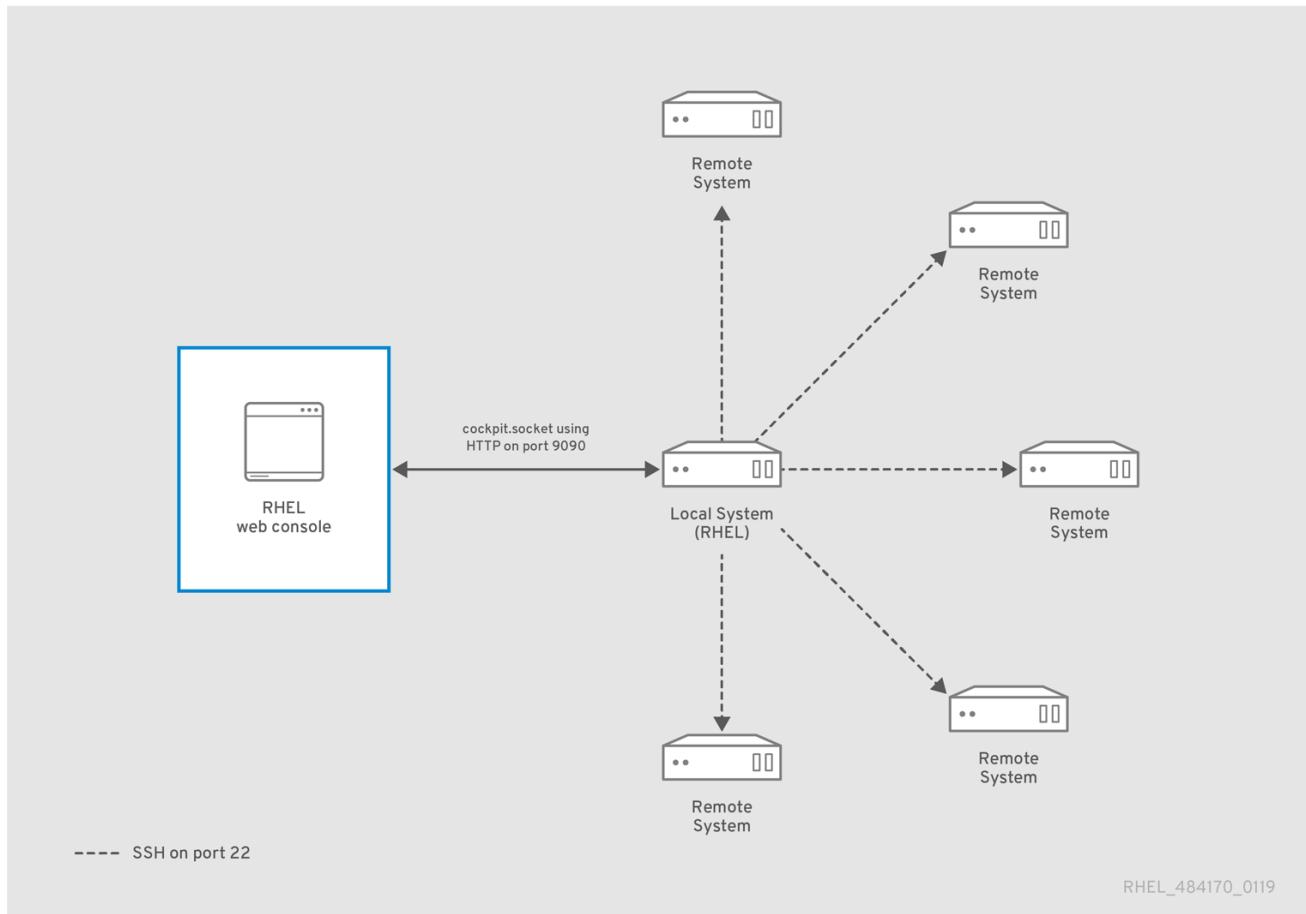
15.1. REMOTE SYSTEM MANAGER IN THE WEB CONSOLE

Using the RHEL 8 web console to manage remote systems in the network requires considering the topology of connected servers.

For optimal security, Red Hat recommends the following connection setup:

- Use one system with the web console as a bastion host. The bastion host is a system with opened HTTPS port.
- All other systems communicate through SSH.

With the web interface running on the bastion host, you can reach all other systems through the SSH protocol using port 22 in the default configuration.



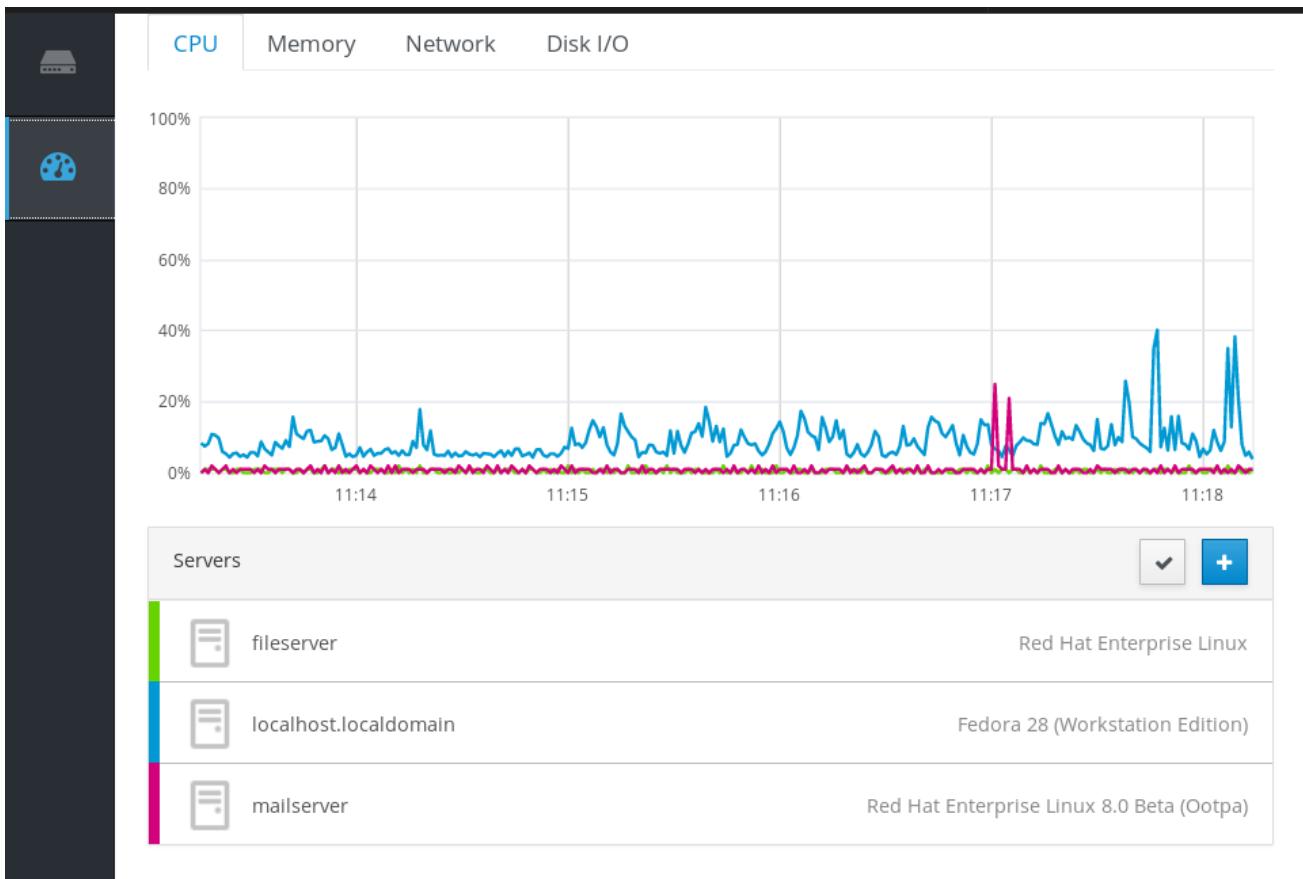
15.2. ADDING REMOTE HOSTS TO THE WEB CONSOLE

This section helps you to connect other systems with a user name and password to the Dashboard located in the web console.

The Dashboard is a tool designed for remote server management, where you can add, connect, or remove remote systems.

The Dashboard displays graphs and status for each of the remote systems.

You can add up to 20 remote systems in the Dashboard.



Prerequisites

- The **cockpit-dashboard** package installed in the system where the web interface is running:


```
$ sudo yum install cockpit-dashboard
```

The **cockpit-dashboard** package extends the RHEL 8 web console with the remote system management.

- You need to be logged into the web console with administration privileges.
For details, see [Logging in to the web console](#).

Procedure

1. In the RHEL 8 web console, go to **Dashboard**.
2. In the **Dashboard**, click the **Add Server** icon.



3. In the **Add Machine to Dashboard** dialog box, enter the host name or IP address of the remote system.

4. (Optional) Click the **Color** field to change the color of the system in Dashboard.
5. Click **Add**.
6. In the **Log in to <servername>** dialog box, enter the credentials for the remote system. You can use any user account of the remote system. However, if you use credentials of a user account without administration privileges, you will not be able to perform administration tasks.

If you use the same credentials as for your local system, the web console will authenticate remote systems automatically every time you log in. However, using the same credentials on more machines could be a potential security risk.

Log in to 192.168.122.101

Cockpit was unable to log into **192.168.122.101**. You can change your authentication credentials below. You may prefer to [synchronize accounts and passwords](#).

User name	example.user	i
Authentication	Type a password	i
Password	*****	i

Cancel **Log In**

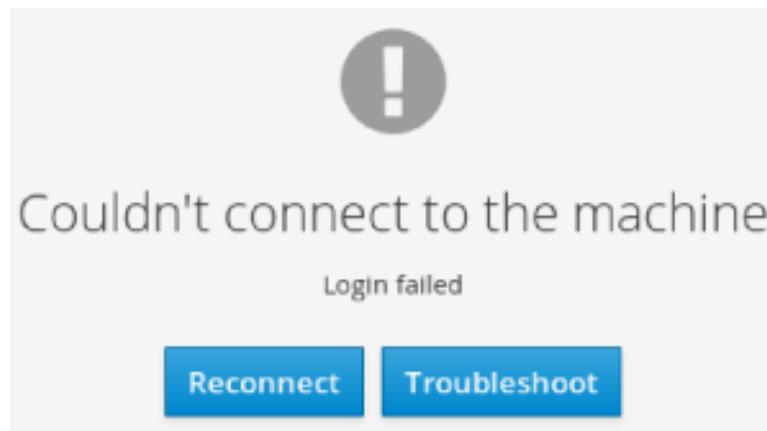
7. Click **Log In**.

If the login succeeds the Dashboard adds a new item in the list. To verify the connection, click the system to see all the details in the web console.



NOTE

The web console does not save passwords used to log in to remote systems which means that you have to log in again after each system restart. To open the login dialog, click the **Troubleshoot** button placed on the main screen of the disconnected remote system.



15.3. REMOVING REMOTE HOSTS FROM THE WEB CONSOLE

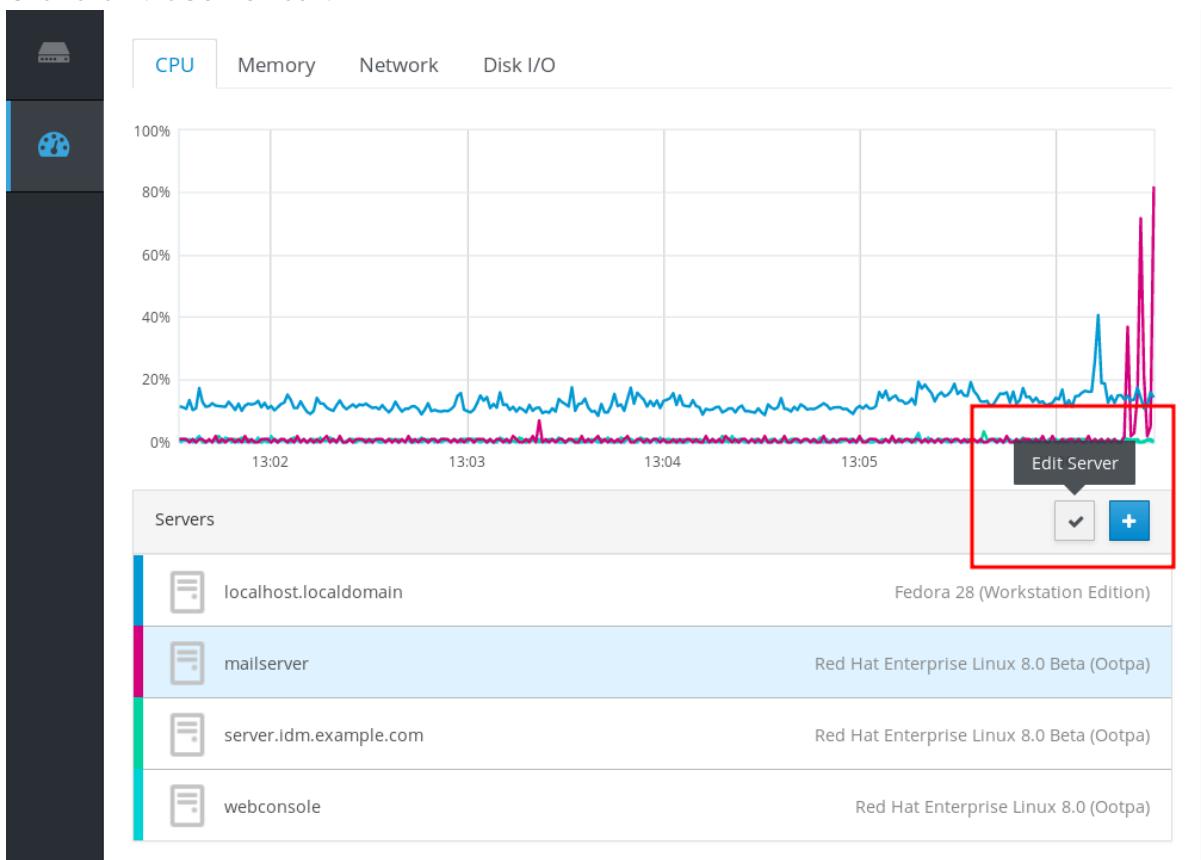
This section guides you on removing other systems from a dashboard located in the web console.

Prerequisites

- The **cockpit-dashboard** package installed in the system where the web interface is running.
- Remote systems added.
For details, see [Using the web console to add remote systems](#).
- You must be logged into the web console with administrator privileges.
For details, see [Logging in to the web console](#).

Procedure

1. Log in to the RHEL 8 web console.
2. Click **Dashboard**.
3. Click the **Edit Server** icon.



4. To remove the server from the **Dashboard**, click the red **Remove** icon.



As a result, the server is removed from **Dashboard**.

15.4. SETTING UP SSH FOR REMOTE MANAGEMENT IN THE WEB CONSOLE

The RHEL 8 web console supports authentication with SSH keys. This has the following advantages:

- Increasing security of the communication between servers.

- Avoiding entering credentials repeatedly.



IMPORTANT

Using SSH keys works only for read only access or for password-less sudo because the authentication happens without a password. To perform administrative tasks, use your system account credentials with administrative privileges.

To configure authentication with SSH keys in the web console:

- Copy the public key into the connected remote system.
- Set the path to the private key in the system, on which the RHEL 8 web console is running.
- Log out from the web console and log in again to ensure the authentication change.

Prerequisites

- SSH key stored in the system with running web console. If you do not have any, use the following command:

```
$ ssh-keygen
```

- Password to the generated SSH key.
- The contents of the `~/.ssh/id_rsa.pub` file copied in the clipboard.

Procedure

To copy the public SSH key into a remote system:

1. Open the web console.
2. Click **Dashboard**.
3. Select the remote system where you want to add the public key.
4. In the system settings, go to **Accounts**.
5. Select the user account to which you want to assign the public key.
6. In the **Authorized Public SSH Keys** settings, click the **+** button.

The screenshot shows the 'Accounts' section for the 'Example User'. The user's full name is 'Example User' and their user name is 'euser'. They have been assigned the 'Server Administrator' role. The account is set to 'Never lock account' and 'Never expire password'. There are no authorized public keys listed under 'Authorized Public SSH Keys'.

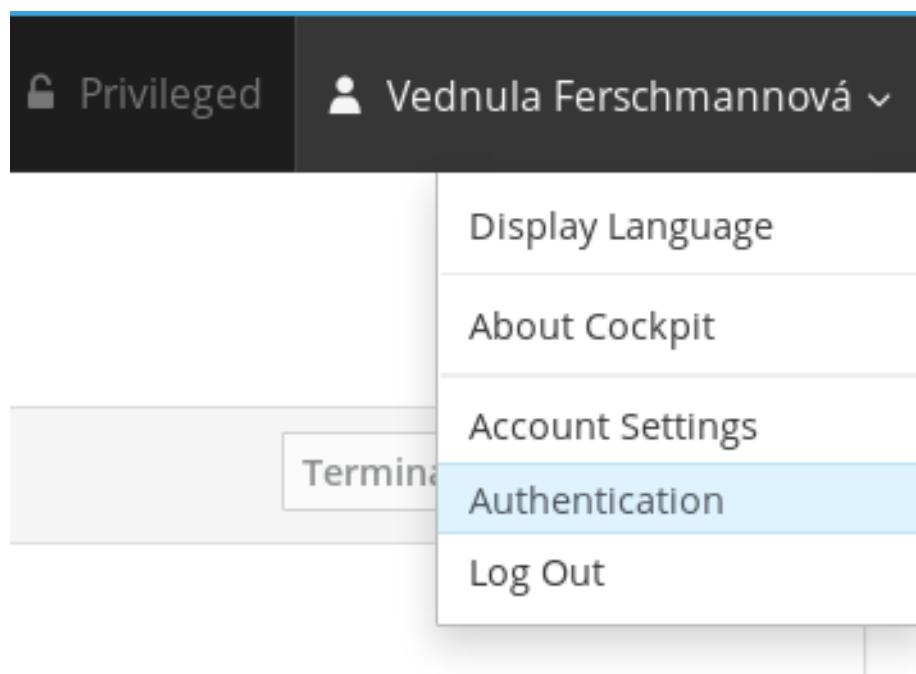
7. In the **Add public key** dialog box, paste the public key you have in the clipboard.
8. Click **Add key**.

At this point, you can see the new public key assigned to the user account.

The screenshot shows the same 'Accounts' section for the 'Example User'. A new public key has been added, listed as 'user@example.com' with a SHA256 fingerprint: 'SHA256:ItYx/gDbEWR349+nndAG59sPtGuwU8dH7zJQsxQe7...'. The '+' button is visible next to the list of keys.

To set the path to the private SSH key:

1. Go to upper right corner settings.
2. In the drop down menu, select **Authentication**.



3. Verify that the web console uses the correct path to the private key you want to use. By default, the web console uses the following paths for private keys:

```
~/.ssh/id_rsa
~/.ssh/id_dsa
~/.ssh/id_ed25519
~/.ssh/id_ecdsa
```

To use a different key, add the path manually.

4. Enable the key with the **On/Off** button.
Enabling the key opens a password dialog.
5. Enter the SSH key password.

Authentication

Password not usable for privileged tasks or to connect to other machines

Use the following keys to authenticate against other systems [+ Add key](#)

id_rsa	ON <input type="checkbox"/>
Password	*****
Unlock Key	

Close

6. Click **Unlock Key**.

On **Details** tab, you can verify the certificate owner and the fingerprint.

7. Click **Close**.

The RHEL 8 web console uses now SSH keys on both sides. However, systems still use the original credentials.

To change the authentication settings:

1. Log out yourself from the web console.

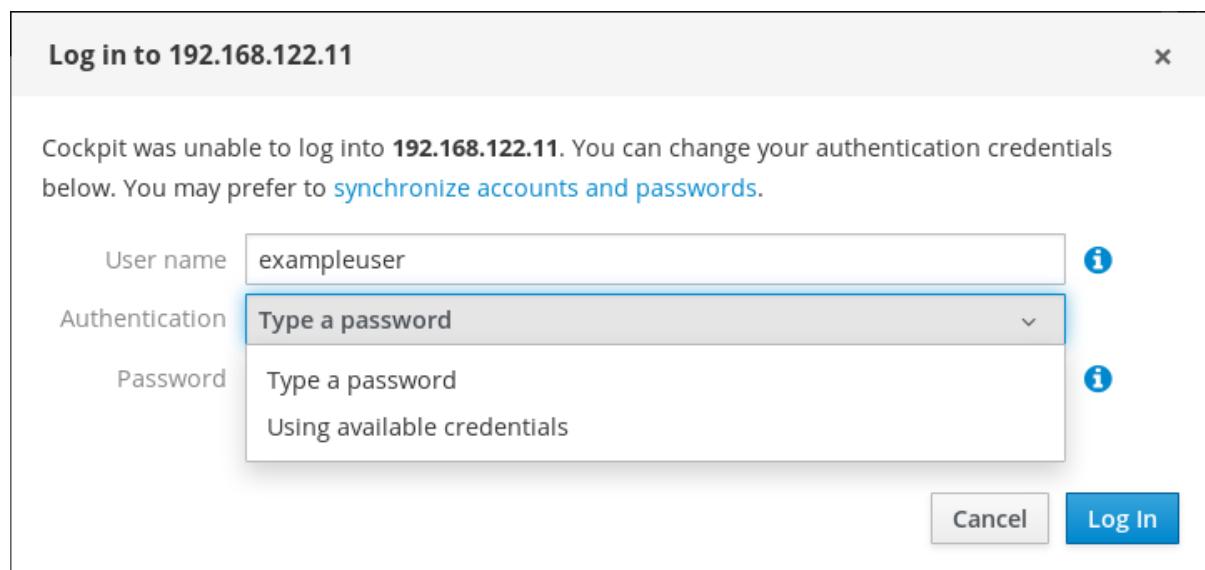
After the logging back in the web console, red triangle icon appears before the remote system.

2. Click the system trying to connect to the web console.

You can see two buttons in the screen. **Reconnect** and **Troubleshoot**.

3. Click the **Troubleshoot** button.

Login dialog appears.



4. In the **Authentication** drop down menu, select **Using available credentials**

The web console creates a new connection secured with SSH keys. It works for the web console login as well as for a terminal access.

CHAPTER 16. CONFIGURING SINGLE SIGN-ON FOR THE RHEL 8 WEB CONSOLE IN THE IDM DOMAIN

The RHEL 8 web console supports Single Sign-on (SSO) authentication provided by Identity Management (IdM).

Advantages:

- IdM domain administrators can use the RHEL 8 web console to manage local machines.
- Users with a Kerberos ticket in the IdM domain do not need to provide login credentials to access the web console.
- All hosts known to the IdM domain are accessible via SSH from the local instance of the RHEL 8 web console.
- Certificate configuration is not necessary. The console's web server automatically switches to a certificate issued by the IdM certificate authority and accepted by browsers.

This chapter covers the following steps to configure SSO for logging into the the RHEL web console:

1. Add machines to the IdM domain using the RHEL 8 web console.
For details, see [Joining the RHEL 8 system to the IdM domain using the web console](#)
2. If you want to use Kerberos for authentication, you need to obtain a Kerberos ticket on your machine.
For details, see [Logging in to the web console using a Kerberos ticket](#)
3. Allow administrators on the IdM master server to run any command on any host.
For details, see [Enabling admin sudo access on the IdM server](#).

Prerequisites

- The RHEL web console installed on RHEL 8 systems.
For details, see [Installing the web console](#).
- IdM client installed on systems with the RHEL web console.
For details, see [IdM client installation](#).

16.1. JOINING A RHEL 8 SYSTEM TO AN IDM DOMAIN USING THE WEB CONSOLE

This procedure uses the web console to join the Red Hat Enterprise Linux 8 system to the Identity Management (IdM) domain.

Prerequisites

- The IdM domain is running and reachable from the client you want to join.
- You have the IdM domain administrator credentials.

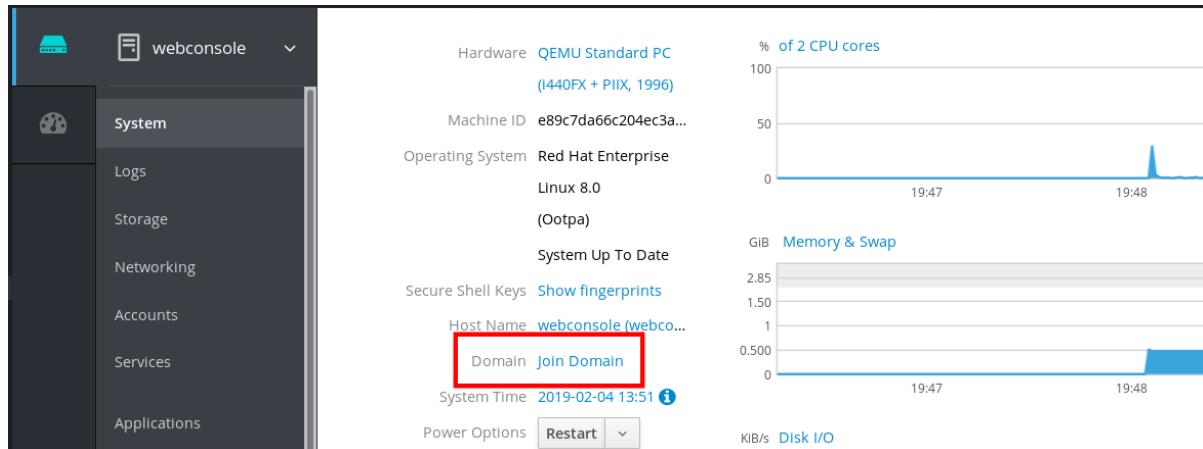
Procedure

1. Log into the RHEL web console.

For details, see [Logging in to the web console](#).

2. Open the **System** tab.

3. Click **Join Domain**.



4. In the **Join a Domain** dialog box, enter the host name of the IdM server in the **Domain Address** field.
5. In the **Authentication** drop down list, select if you want to use a password or a one-time password for authentication.

The screenshot shows the 'Join a Domain' dialog. It has fields for 'Domain Address' (server.idm.example.com) and 'Authentication' (set to 'One Time Password', with options 'Administrator Password' and 'One Time Password' listed). At the bottom are 'Cancel' and 'Join' buttons, with 'Join' being highlighted by a blue box.

6. In the **Domain Administrator Name** field, enter the user name of the IdM administration account.
7. In the password field, add the password or one-time password according to what you selected in the **Authentication** drop down list earlier.
8. Click **Join**.

Join a Domain

Domain Address	server.idm.example.com
Authentication	Administrator Password
Domain Administrator Name	admin
Domain Administrator Password	*****

Cancel **Join**

Verification steps

1. If the RHEL 8 web console did not display an error, the system has been joined to the IdM domain and you can see the domain name in the **System** screen.
2. To verify that the user is a member of the domain, click the Terminal page and type the **id** command:

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

Additional resources

- [Planning Identity Management](#)
- [Installing Identity Management](#)
- [Configuring and managing Identity Management](#)

16.2. LOGGING IN TO THE WEB CONSOLE USING KERBEROS AUTHENTICATION

The following procedure describes steps on how to set up the RHEL 8 system to use Kerberos authentication.



IMPORTANT

With SSO you usually do not have any administrative privileges in the web console. This only works if you configured passwordless sudo. The web console does not interactively ask for a sudo password.

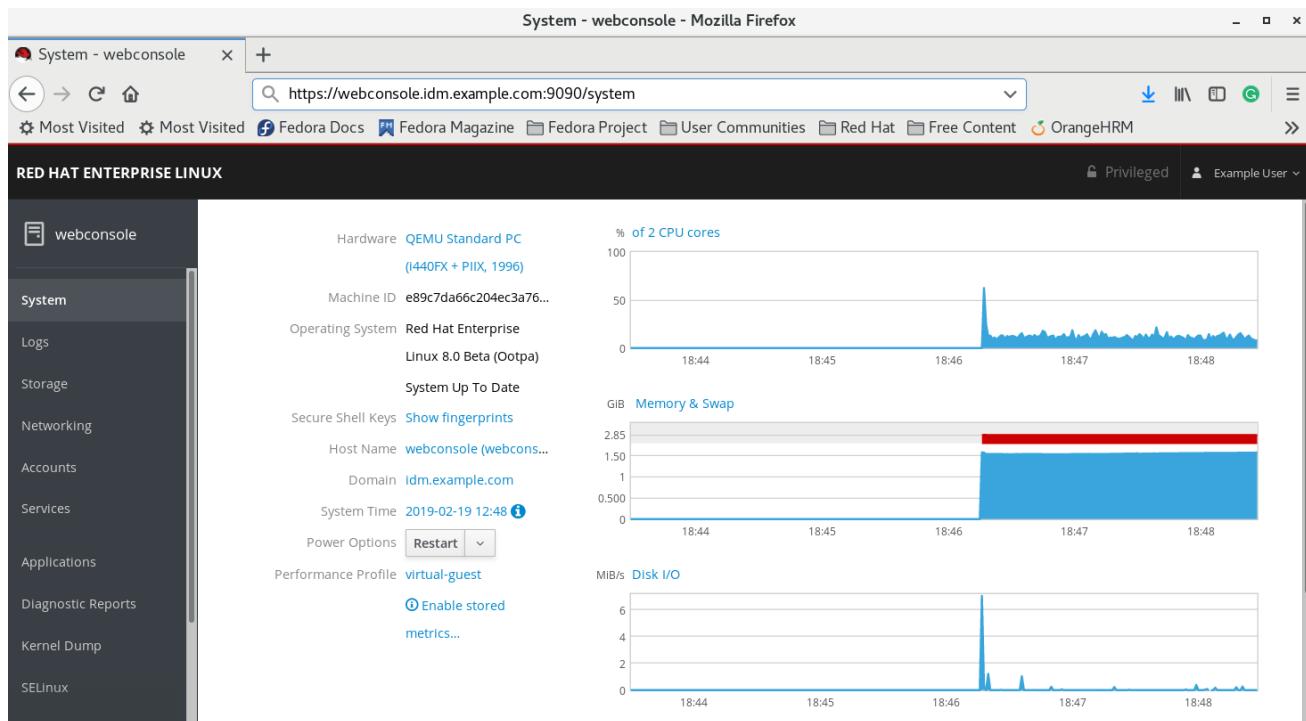
Prerequisites

- IdM domain running and reachable in your company environment.
For details, see [Joining the RHEL 8 system to the IdM domain using the web console](#)
- Enable the **cockpit.socket** service on remote systems to which you want to connect and manage them with the RHEL web console.
For details, see [Installing the web console](#).
- If the system does not use a Kerberos ticket managed by the SSSD client, try to request the ticket with the **kinit** utility manually.

Procedure

Log in to the RHEL web console with the following address: https://dns_name:9090.

At this point, you are successfully connected to the RHEL web console and you can start with configuration.



16.3. ENABLING ADMIN SUDO ACCESS TO DOMAIN ADMINISTRATORS ON THE IDM SERVER

The following procedure describes steps on how to allow domain administrators to run any command on any host in the Identity Management (IdM) domain.

To accomplish this, enable sudo access to the **admins** user group created automatically during the IdM server installation.

All users added to the **admins** group will have sudo access if you run **ipa-advise** script on the group.

Prerequisites

- The server runs IdM 4.7.1 or later.

Procedure

1. Connect to the IdM server.

2. Run the ipa-advise script:

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

If the console did not display an error, the **admins** group have admin permissions on all machines in the IdM domain.

CHAPTER 17. CONFIGURING SMART CARD AUTHENTICATION WITH THE WEB CONSOLE FOR CENTRALLY MANAGED USERS

This chapter helps you to configure smart card authentication for users who are centrally managed by:

- Identity Management
- Active Directory which is connected in the cross-forest trust with Identity Management

The following sections include:

- What smart cards are and how the authentication works
- Storing the IdM or ADCS certificate to the smart card
- Enabling smart card authentication in the web console
- Authenticating a user with the smart card while accessing the web console
- Protecting the connection against DoS attacks



IMPORTANT

Smart card authentication does not elevate administrative privileges yet and the web console opens in the web browser in the read-only mode.

You can run administrative commands in the built-in terminal with `sudo` .

Prerequisites

- The system for which you want to use the smart card authentication must be a member of an Active Directory or Identity Management domain.
For details about joining the RHEL 8 system into a domain using the web console, see [Joining a RHEL 8 system to an IdM domain using the web console](#).
- The certificate used for the smart card authentication must be associated with a particular user in Identity Management or Active Directory.
For more details about associating a certificate with the user in Identity Management, see [Adding a certificate to a user entry in IdM](#) .

17.1. SMART CARD AUTHENTICATION FOR CENTRALLY MANAGED USERS

A smart card is a physical device, which can provide personal authentication using certificates stored on the card. Personal authentication means that you can use smart cards in the same way as user passwords.

You can store user credentials on the smart card in the form of a private key and a certificate. Special software and hardware is used to access them. You insert the smart card into a reader or a USB socket and supply the PIN code for the smart card instead of providing your password.

Identity Management (IdM) supports smart card authentication with:

- User certificates issued by the IdM certificate authority. For details, see [Configuring Identity Management for smart card authentication](#).
- User certificates issued by the Active Directory Certificate Service (ADCS) certificate authority. For details, see [Configuring certificates issued by ADCS for smart card authentication in IdM](#) .



NOTE

If you want to start to use smart card authentication, see the hardware requirements: [Smart Card support in RHEL8](#).

17.2. INSTALLING TOOLS FOR MANAGING AND USING SMART CARDS

To configure your smart card, you need tools which can generate certificates and store them on a smart card.

You must:

- Install the **gnutls-utils** package which helps you to manage certificates.
- Install the **opensc** package which provides a set of libraries and utilities to work with smart cards.
- Start the **pcscd** service which communicates with the smart card reader.

Procedure

1. Install the **opensc** and **gnutls-utils** packages:

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

2. Start the **pcscd** service.

```
# systemctl start pcscd
```

Verify that the **pcscd** service is up and running.

17.3. STORING A CERTIFICATE ON A SMART CARD

This section describes smart card configuration with the **pkcs15-init** tool, which helps you to configure:

- Erasing your smart card
- Setting new PINs and optional PIN Unblocking Keys (PUKs)
- Creating a new slot on the smart card
- Storing the certificate, private key, and public key in the slot
- Locking the smart card settings (some smart cards require this type of finalization)

Prerequisites

- The **opensc** package, which includes the **pkcs15-init** tool is installed.

For details, see [Installing tools for managing and using smart cards](#).

- The card is inserted in the reader and connected to the computer.
- You have the private key, public key, and certificate to store on the smart card. In this procedure, **testuser.key**, **testuserpublic.key**, and **testuser.crt** are the names used for the private key, public key, and the certificate.
- Your current smart card user PIN and Security Officer PIN (SO-PIN)

Procedure

1. Erase your smart card and authenticate yourself with your 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]:
```

The card has been erased.

2. Initialize your smart card, set your user PIN and PUK, and your Security Officer PIN and PUK:

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

The **pkcs15-init** tool creates a new slot on the smart card.

3. Set the label and the authentication ID for the slot:

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

The label is set to a human-readable value, in this case, **testuser**. The **auth-id** must be two hexadecimal values, in this case it is set to **01**.

4. Store and label the private key in the new slot on the smart card:

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



NOTE

The value you specify for **--id** must be the same when storing your private key, and certificate. If you do not specify a value for **--id**, a more complicated value is calculated by the tool and it is therefore easier to define your own value.

5. Store and label the certificate in the new slot on the smart card:

```
$ 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
```

- (Optional) Store and label the public key in the new slot on the smart card:

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



NOTE

If the public key corresponds to a private key and/or certificate, you should specify the same ID as that private key and/or certificate.

- (Optional) Some smart cards require you to finalize the card by locking the settings:

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

At this stage, your smart card includes the certificate, private key, and public key in the newly created slot. You have also created your user PIN and PUK and the Security Officer PIN and PUK.

17.4. ENABLING SMART CARD AUTHENTICATION FOR THE WEB CONSOLE

To be able to use smart card authentication in the web console, enable smart card authentication in the **cockpit.conf** file.

Additionally, you can disable password authentication in the same file.

Prerequisites

- The RHEL 8 web console has been installed.
For details, see [Installing the web console](#).

Procedure

- Log in to the RHEL web console with administrator privileges.
For details, see [Logging in to the web console](#).
- Click **Terminal**.
- In the **/etc/cockpit/cockpit.conf**, set the **ClientCertAuthentication** to **yes**:

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

- Optionally, disable password based authentication in **cockpit.conf** with:

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

This configuration disables password authentication and you must always use the smart card.

5. Restart the web console to make sure that the **cockpit.service** accepts the change:

```
# systemctl restart cockpit
```

17.5. LOGGING IN TO THE WEB CONSOLE WITH SMART CARDS

This section provides information about using smart cards for logging in to the web console.

Prerequisites

- A valid certificate stored in your smart card that is associated to a user account created in a Active Directory or Identity Management domain.
- PIN to unlock the smart card.
- The smart card has been put into the reader.

Procedure

1. Open your web browser and add the web console's address in the address bar.
The browser asks you to add the PIN protecting the certificate stored on the smart card.
2. In the **Password Required** dialog box, enter PIN and click **OK**.
3. In the **User Identification Request** dialog box, select the certificate stored in the smart card.
4. Select **Remember this decision**.
The system does not open this window next time.
5. Click **OK**.

You are now connected and the web console displays its content.

17.6. LIMITING USER SESSIONS AND MEMORY TO PREVENT A DOS ATTACK

Certificate authentication is protected by separating and isolating instances of the **cockpit-ws** web server against attackers who wants to impersonate another user. However, this introduces a potential Denial of Service (DoS) attack: A remote attacker could create a large number of certificates and send a large number of HTTPS requests to **cockpit-ws** each using a different certificate.

To prevent this DoS, the collective resources of these web server instances are limited. By default, limits to the number of connections and to memory usage are set to 200 threads and a 75% (soft) / 90% (hard) memory limit.

The following procedure describes resource protection by limiting the number of connections and memory.

Procedure

1. In the terminal, open the **system-cockpithttps.slice** configuration file:

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

2. Limit the **TasksMax** to 100 and **CPUQuota** to 30%:

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

3. To apply the changes, restart the system:

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

Now, the new memory and user session limits protect the **cockpit-ws** web server from DoS attacks.

17.7. ADDITIONAL RESOURCES

- For more details on configuring certificates issued by IdM for smart card authentication, see the [Configuring Identity Management for smart card authentication](#) .
- For more details on configuring certificates issued by ADCS for smart card authentication, see the [Configuring certificates issued by ADCS for smart card authentication in IdM](#) .
- For more details on configuring certificates issued by local CA for smart card authentication, see the [Configuring and importing local certificates to a smart card](#) .:context:system-management-using-the-RHEL-8-web-console