Abstract

This guide demonstrates how to use the web console to manage Red Hat Enterprise Linux and Red Hat Enterprise Linux Atomic Host servers.
Table of Contents

CHAPTER 1. OVERVIEW .............................................................................................................. 3
  1.1. WHAT MAKES THE RHEL WEB CONSOLE UNIQUE? ........................................ 3
  1.2. THE ROLE OF THIS GUIDE ....................................................................................... 3

CHAPTER 2. INSTALLING AND ENABLING THE RHEL WEB CONSOLE ................................. 4
  2.1. PREREQUISITES FOR A PRIMARY RHEL WEB CONSOLE ............................ 4
  2.2. SETTING UP THE PRIMARY RHEL WEB CONSOLE ........................................ 4
  2.3. OPENING THE INTERFACE ...................................................................................... 5
  2.4. CHANGING EXPIRED PASSWORDS ........................................................................ 5
  2.5. SSH TWO-FACTOR AUTHENTICATION WITH THE WEB CONSOLE ........... 7

CHAPTER 3. USING THE WEB CONSOLE .................................................................................. 8
  3.1. GETTING TO KNOW THE WEB CONSOLE ........................................................... 8
    3.1.1. Adding secondary systems ............................................................................. 16
    3.1.2. Logging into other systems through the web console .................................. 18
    3.1.3. Logging into a system via a Bastion Host ..................................................... 19
  3.2. CHANGING THE WEB CONSOLE’S PORT .......................................................... 19
  3.3. ENABLING MORE FEATURES TO THE WEB CONSOLE .................................... 20

CHAPTER 4. THE WEB CONSOLE ON RED HAT ENTERPRISE LINUX ATOMIC HOST .......... 21
  4.1. INSTALLING THE WEB CONSOLE ON ATOMIC HOST .................................... 21
  4.2. THE WEB CONSOLE SPECIFIC TO ATOMIC HOST ........................................ 21
    4.2.1. Working with Containers .............................................................................. 23
  4.3. CHANGING THE WEB CONSOLE’S PORT ON ATOMIC HOST ...................... 27
  4.4. ENABLING MORE WEB CONSOLE’S FEATURES ON ATOMIC HOST ............ 27
CHAPTER 1. OVERVIEW

The web console is a user-friendly web-based interface for administering servers. It allows monitoring system resources and adjusting configuration with ease.

1.1. WHAT MAKES THE RHEL WEB CONSOLE UNIQUE?

- The web console builds upon existing functionality.
- There is no lock-in. Feel free to use other tools alongside the web console. Switch back and forth with ease.
- The web console does not need special infrastructure or configuration. Once installed, it is ready to use.
- When not in use, the web console uses no memory or CPU on the server.
- The web console always updates its data to reflect the current state of the server, within seconds.
- The web console stores no data or policy. People keep their system-wide permissions and use the system credentials.
- Optionally take advantage of single sign-on with Kerberos.
- The web console itself is not used for configuration management. However, the web console can interact with configuration management and custom server tools.

1.2. THE ROLE OF THIS GUIDE

This document helps you get started with the web console. It walks through installation, explains typical server configuration, and demonstrates the web console in detail.
CHAPTER 2. INSTALLING AND ENABLING THE RHEL WEB CONSOLE

A primary web console server is the machine that runs a `cockpit.socket` service with the user interface. A secondary server is a machine that is administered using the web console. It is possible to add one or more secondary hosts to the primary web console.

Setting up a primary server involves:

1. Installing the `cockpit` packages.
2. Opening the port for the RHEL web console.
3. Starting the `cockpit.socket` service.

After setting up, you can connect to the web console in a browser by typing the host name and port of the server. For example, from the primary host you can connect using `localhost:9090`.

For setting up a primary server on Red Hat Enterprise Linux Atomic Host, see Installing the web console on Atomic Host.

2.1. PREREQUISITES FOR A PRIMARY RHEL WEB CONSOLE

Before setting up the web console, ensure that you have:

1. Installed Red Hat Enterprise Linux. If required, see the Installation Guide.
2. Enabled networking. If required, see the Networking Guide.
3. Registered the system and attached subscription. If required, see the Registering the System and Attaching Subscriptions section of the System Administrator’s Guide.

2.2. SETTING UP THE PRIMARY RHEL WEB CONSOLE

To install and enable the web console:

1. Enable the Extras and Optional repositories:

   ```
   # subscription-manager repos --enable=rhel-7-server-extras-rpms
   # subscription-manager repos --enable=rhel-7-server-optional-rpms
   ```

   This gives you access to supplementary the web console packages such as `cockpit-dashboard`.

2. Install the `cockpit` and `cockpit-dashboard` packages:

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

   The `cockpit-dashboard` package provides the "Dashboard" tab in the interface. This package is optional, but is assumed to be installed in this guide.

3. Allow external connections to port 9090 through the firewall:

   ```
   # firewall-cmd --add-port=9090/tcp
   # firewall-cmd --permanent --add-port=9090/tcp
   ```
4. Enable and start the `cockpit.socket` service:

```
$ sudo systemctl enable cockpit.socket
$ sudo systemctl start cockpit.socket
```

5. The RHEL web console is now installed and running.

If you are installing the web console on a Red Hat Enterprise Linux Atomic Host system, see Installing the web console on Atomic Host.

### 2.3. OPENING THE INTERFACE

1. Open a web browser and enter the server’s IP address with port 9090 in the address bar. If the web browser is on the primary web console, open `localhost:9090` or `hostname:9090`.

   **NOTE**

   If you use a self-signed certificate, the browser issues a warning. Carefully check the certificate before accepting the warning. Consider using a certificate signed by a certificate authority (CA). For more information on certificates, see the An Overview of Certificates and Security section of the RHEL System Administrator’s Guide.

   If you are sure you want to use self-signed certificates, then add this connection to the security exceptions. Click **Advanced → Add Exception → Confirm Security Exception**. After that, you will see the login screen.

2. Log into the web console with the same user name and password that you would normally use to log into the system.

### 2.4. CHANGING EXPIRED PASSWORDS

The web console supports changing expired passwords.
A fresh system installation with an expired password will prompt a password change during the first login. System administrators often use this feature to make sure users change their pre-assigned passwords to a custom password.

When logging in with an expired password, the web console prompts you to enter the current password a second time. Enter your current password and click Log In.

Choose a new password and click Log In.

NOTE
If you have issues logging in to the web console and the prompt for changing the password is not shown, check the /etc/ssh/sshd_config file on the Server. Make sure ChallengeResponseAuthentication is set to yes and restart sshd with the systemctl restart sshd command.
2.5. SSH TWO-FACTOR AUTHENTICATION WITH THE WEB CONSOLE

The web console supports two-factor authentication. If you have protected your SSH server with two-factor authentication, the login screen will prompt you to enter your password and PIN pair.

Setting up SSH for two-factor authentication requires two components:

1. A company’s authenticator application that provides one-time passwords or PIN numbers. An example application is **Google Authenticator**, which also has its own Pluggable Authentication Module (PAM).

2. A server that validates the PINs from a dongle.

These two components are often implemented differently for different companies.

After setting up the authenticator application and the validation server, enable SSH two-factor authentication in the web console:

1. In the `/etc/pam.d/sshd` file, right after the last `auth` line, add this line:

   ```
   auth       required         <your_PAM_module>
   ```

   Substitute `<your_PAM_module>` with the PAM module used by your application.

2. In the `/etc/ssh/sshd_config` file, set `ChallengeResponseAuthentication` to `yes`.

3. Restart the `sshd` service with the `systemctl restart sshd` command.

The web console will ask for your verification code the next time you log in.
CHAPTER 3. USING THE WEB CONSOLE

3.1. GETTING TO KNOW THE WEB CONSOLE

Once you have logged in, you will see the Dashboard tab. The Dashboard shows a list of all systems added to the primary web console with graphs for their CPU usage, memory usage, disk I/O, and network traffic.

From Dashboard, you can select a system name, in this case primary-host, and have a look at the side menu:

System: Shows information about the system that the web console is running on. This includes CPU usage, memory usage, disk I/O, and network traffic, as well as hardware and operating system details.
Logs: See messages produced by the systemd journal, including errors, warnings, and notices. The log is similar to the output of the `journalctl` command. The log displays newest entries first, with options to filter by type.
Networking: See networking interfaces (for example, eth0) and active graphs of sent and received data.
Accounts: Shows which administrative (root) and other users (for example, alan, djohnson) have accounts on the system.
Services: Shows the systemd services running on the system. You can see which are active/enabled or inactive. You can also see other systemd features: Targets, sockets, timers, and paths.

Select a service to view its details:
Diagnostic reports: Collects system configuration and diagnostics information and prepares a report in the .xz compressed format.

You can then download the report locally to your system:
Kernel dump configuration: Shows kdump status and configuration and allows to crash the kernel to test kdump.

SELinux: Shows whether SELinux is enabled and lists access control errors.
SELinux Policy

Enforce policy: ON

SELinux Access Control Errors

SELinux is preventing /usr/libexec/colord from read access on the file /etc/udev/hwdb.bin.

Solutions

If you believe that colord should be allowed read access on the hwdb.bin file by default, you should report this as a bug. You can generate a local policy module to allow this access.

Allow this access for now by executing: # ausearch -c 'colord' -raw | audit2allow -M my-colord # semodule -i my-colord.pp

Audit log

Occurred between Yesterday at 10:30 AM and Today at 1:16 PM

Subscriptions: Displays installed Red Hat products and subscriptions.
Terminal: Opens an in-browser terminal with a command line session to the system. In this terminal, you can run commands from your signed-in user account. For example, as root, you could run the `systemctl start` or `dnf install` commands.

For Red Hat Enterprise Linux Atomic Host systems, there are additional features in the web console. See The RHEL web console specific to Atomic Host.

3.1.1. Adding secondary systems
Once you log in to the primary server, you will be able to connect to secondary servers. These secondary systems need to have:

- The **cockpit** packages installed.
- An SSH server running and available on port 22 that supports password or key-based authentication.

To add a new secondary server:

1. From the "Dashboard" tab next to the system name, click the plus button.
2. Enter IP of the server you are adding and choose a color label for it.
3. Click the "Add" button.

![Add Machine to Dashboard](image)

4. Log in to the system with a user name and password:

![Log in to secondary-host](image)

**Configuring Key-Based Authentication**

If you have keys generated on the primary server, you need to add them to the target server, in the `~/.ssh/authorized_keys` file. If you do not have keys, use the following command:

```
$ ssh-keygen
```
Next, copy the contents of the ~/.ssh/id_rsa.pub file to the ~/.ssh/authorized_keys file on the target server. Then, return to the user interface on the primary server, click the top right corner menu with the user name on it, choose Authentication, and enable the preloaded key.

3.1.2. Logging into other systems through the web console

On the login screen, you can also choose an alternate host to connect to.

The alternate host needs to have:

- SSH listening on port 443
- the cockpit-bridge package and all relevant sub-packages to interact with the system, such as cockpit-system, installed. The packages should be the same version as in the web console server.

To connect to an alternate host:

1. Type in your user name and password from that alternate host and click Other Options.
2. In the entry field type the IP address of the new host and click Log In.
3. Provide the SSH fingerprint and click Log In again.

Now you are able to browse the new system. The web console uses SSH to authenticate you against that host, so you do not need to configure anything else on the new system.
NOTE

If the new machine is not known to the web console, and you get the **Refusing to connect. Host is unknown** error, use the following command to allow connections from unknown hosts:

```bash
ssh-keyscan -H [ip_address] >> /var/lib/cockpit/known_hosts
```

### 3.1.3. Logging into a system via a Bastion Host

On the web console’s login screen you can choose an alternate host to connect to. The web console uses SSH to authenticate you against that host and to display the admin interface for that host.

Although browsers cannot use SSH directly to connect to machines or authenticate against them, the web console can make this happen. Only one host needs to have the web console listen on port 9090 available to browsers over TLS. Other hosts only need to have SSH accessible on the usual port 22.

### 3.2. CHANGING THE WEB CONSOLE’S PORT

To change the web console’s port:

1. If required, create the `/etc/systemd/system/websocket.cockpit.d/` directory and its parent directories:

   ```bash
   # mkdir -p /etc/systemd/system/websocket.cockpit.d/
   ``

2. Create the `/etc/systemd/system/websocket.cockpit.d/listen.conf` file with these contents:

   ```plaintext
   [Socket]
   ListenStream=9898
   ``

3. Allow the new port through the firewall:

   ```bash
   # firewall-cmd --add-port=9898/tcp
   # firewall-cmd --permanent --add-port=9898/tcp
   ``

4. If you have SELinux enabled, change the default SELinux policy to allow the `websm_port_t` domain to listen on the TCP 9898 port:

   ```bash
   $ sudo semanage port -a -t websm_port_t -p tcp 9898
   ``
   
   If the port is already defined by some other part of the SELinux policy, use the `-m` argument instead of `-a` to modify the definition:

   ```bash
   $ sudo semanage port -m -t websm_port_t -p tcp 9898
   ``

1. To make the changes take effect, run the following commands:

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

You can now use the address with the newly assigned port in the web browser.
For changing port on a Red Hat Enterprise Linux Atomic Host system, see Changing the web console’s port on Atomic Host.

3.3. ENABLING MORE FEATURES TO THE WEB CONSOLE

You can add more features to the web console by installing additional cockpit-* packages using yum.
CHAPTER 4. THE WEB CONSOLE ON RED HAT ENTERPRISE LINUX ATOMIC HOST

The web console can run on Red Hat Enterprise Linux Atomic Host, and Atomic Host servers can be monitored and administered using the web console. Additionally, the web console can control life cycle of container instances and manipulate container images.

NOTE

The web console does not yet support Kubernetes on Red Hat Enterprise Linux or Red Hat Enterprise Linux Atomic Host servers.

This chapter describes the web console features specific to Atomic Host.

4.1. INSTALLING THE WEB CONSOLE ON ATOMIC HOST

To install the web console on Atomic Host:

1. Pull the cockpit-ws image:

   # atomic install rhel7/cockpit-ws

2. Run the cockpit-ws image:

   # atomic run rhel7/cockpit-ws

Now you can log into the web console. See Opening the Interface for instructions.

4.2. THE WEB CONSOLE SPECIFIC TO ATOMIC HOST

In addition to information about systems presented in Getting to know the web console, extra tabs appear on Atomic Host systems:

Containers: Lists all images available on the system, all running and non-running containers, combined CPU & memory usage graphs, and a storage usage bar. See Working with Containers for more information on using this tab.
Software Updates: Shows the available OSTrees on the system. You can also check for a newer tree, or roll back to a previous version.
4.2.1. Working with Containers

The Containers tab presents you with a UI to interact with your Atomic Host images and containers. Apart from the system resources graphs, there are lists of all images you have locally on the system as well as all running and non-running containers.

**Download an image.** Click the "Get new image" button from the images list to the right and enter an image name or a keyword. Choose an image and click "Download".
Starting and stopping containers. From the "Containers" list, you can start and stop containers using the buttons on the right side. Use the drop-down menu to see all or filter out the non-running containers.

Click on a container to inspect it. Shows the state, the command executed, the container’s and image’s IDs, a timestamp, as well as the container’s own terminal:
CHAPTER 4. THE WEB CONSOLE ON RED HAT ENTERPRISE LINUX ATOMIC HOST

Click on an image to inspect it: Shows the image’s ID, entrypoint and command, and a list of containers based on that image. You can also delete the image from here or run a container from it.

Click on an image to inspect it.
Run a container. To run a container from an image, either click the triangle button from the right side of the list or choose the image first and then click “Run” from the top right corner. You can then enter the required data for the new container in the following dialog:
You can select which command the container should run, and you can also link that container to other containers, which will allow them to interact. Exposing ports for specific services to be visible from the host is also possible.

4.3. CHANGING THE WEB CONSOLE’S PORT ON ATOMIC HOST

To change the web console’s port on Atomic Host:

```
atomic run rhel7/cockpit-ws --port 9898
```

4.4. ENABLING MORE WEB CONSOLE’S FEATURES ON ATOMIC HOST

You can add more features by installing additional `cockpit-*` packages using package layering.