Red Hat Enterprise Linux 8

Recording sessions

Using the session recording solution in Red Hat Enterprise Linux 8

Last Updated: 2019-05-21

Red Hat Enterprise Linux 8 Recording sessions

Using the session recording solution in Red Hat Enterprise Linux 8

Legal Notice

Abstract

This documentation collection provides introduction to using the session recording solution based on tlog with RHEL web console embedded player on Red Hat Enterprise Linux 8.

Table of Contents

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:

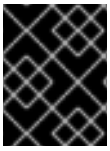
- For simple comments on specific passages, make sure you are viewing the documentation in the Multi-page HTML format. Highlight the part of text that you want to comment on. Then, click the **Add Feedback** pop-up that appears below the highlighted text, and follow the displayed instructions.
- For 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 WITH SESSION RECORDING ON RHEL

1.1. SESSION RECORDING IN RHEL

This section introduces the session recording solution and its purpose.

The session recording solution is provided within Red Hat Enterprise Linux 8 and it is based on the tlog package. The **tlog** package and its associated web console session player provide you with the ability to record and playback user terminal sessions. You can configure the recording to take place per user or user group via the SSSD service. All terminal input and output is captured and stored in a text-based format in the system journal.



IMPORTANT

Recording of the terminal input is turned off by default to not intercept raw passwords and other sensitive information.

The solution can be used for auditing user sessions on security-sensitive systems or, in the event of a security breach, reviewing recorded sessions as part of forensic analysis. System administrators are able to configure session recording locally on RHEL 8.0 systems. You can review the recorded sessions from the web console interface or in a terminal using the **tlog-play** command.

1.2. COMPONENTS OF SESSION RECORDING

There are three main components key to the session recording solution. The **tlog** utility, the SSSD service and a web console embedded user interface.

tlog

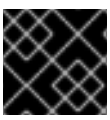
The **tlog** utility is a terminal input/output (I/O) recording and playback program. It inserts itself (specifically the **tlog-rec-session** tool) between the user terminal and the user shell, and logs everything that passes through as JSON messages.

SSSD

The System Security Services Daemon (SSSD) service provides a set of daemons to manage access to remote directories and authentication mechanisms. When configuring session recording, you can use SSSD to specify, which users or user groups should tlog record. This can be done either from a command-line interface (CLI) or from the RHEL 8 web console interface.

The RHEL 8 web console embedded interface

The Session Recording page is part of the RHEL 8 web console interface. The web console embedded interface for session recording enables you to manage recorded sessions.



IMPORTANT

You have to have administrator privileges to be able to access the recorded sessions.

1.3. LIMITATIONS OF SESSION RECORDING

Be aware that **tlog** does not record terminal in the **Gnome 3** graphical session. Recording terminals in

graphical sessions is not supported because a graphical session has a single audit session ID for all terminals and **tlog** does not have a way to distinguish between the terminals and prevent repeated recordings.

CHAPTER 2. DEPLOYING SESSION RECORDING ON RHEL

In this section we cover how to deploy the session recording solution on a Red Hat Enterprise Linux system.

Prerequisites

To be able to deploy the session recording solution you need to have the following packages installed: **tlog**, SSSD, **cockpit-session-recording**.

2.1. INSTALLING TLOG

Install the **tlog** packages.

Procedure

1. Run

```
# yum install tlog
```

2.2. INSTALLING COCKPIT-SESSION-RECORDING

The basic web console packages are a part of Red Hat Enterprise Linux 8 by default. To be able to use the session recording solution, you have to install the **cockpit-session-recording** packages and start or enable the web console on your system:

Procedure

1. Install **cockpit-session-recording**.

```
# yum install cockpit-session-recording
```

2. Start or enable the web console on your system:

```
# systemctl start cockpit.socket
```

or

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

When you have all the necessary packages installed, you can move on to configuring your recording parameters.

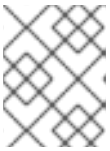
2.3. CONFIGURING THE RECORDED USERS OR USER GROUPS WITH SSSD FROM THE CLI

If you choose to manage recorded users or user groups with SSSD, which is the recommended option, every user's original shell will be preserved.

Procedure

1. To specify which users or user groups you want to record from the command-line interface (CLI), modify open the **sssd-session-recording.conf** configuration file:

```
# vi /etc/sssd/conf.d/sssd-session-recording.conf
```



NOTE

The **sssd-session-recording.conf** file is created automatically once you have opened the configuration page in the web console interface.

2. Specify the scope of recorded users or user groups, either enter:
   - **none** to record no sessions.
   - **some** to record only specified sessions.
   - **all** to record all sessions.
3. In case you choose **some** as a scope of recorded users or groups, add their names divided by commas to the file.

Example 2.1. SSSD configuration

In the following example users **example1** and **example2**, and group **examples** have session recording enabled.

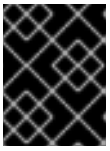
```
[session_recording]
scope = some
users = example1, example2
groups = examples
```

2.4. CONFIGURING THE RECORDED USERS OR USER GROUPS WITH SSSD FROM WEB UI

Second option for specifying recorded users or user groups using SSSD is to list them directly in the RHEL 8 web console.

Procedure

1. Connect to the RHEL 8 web console locally by entering **localhost:9090** or by entering your IP address **<IP_ADDRESS>:9090** to your browser.
2. Log in to the RHEL 8 web console.



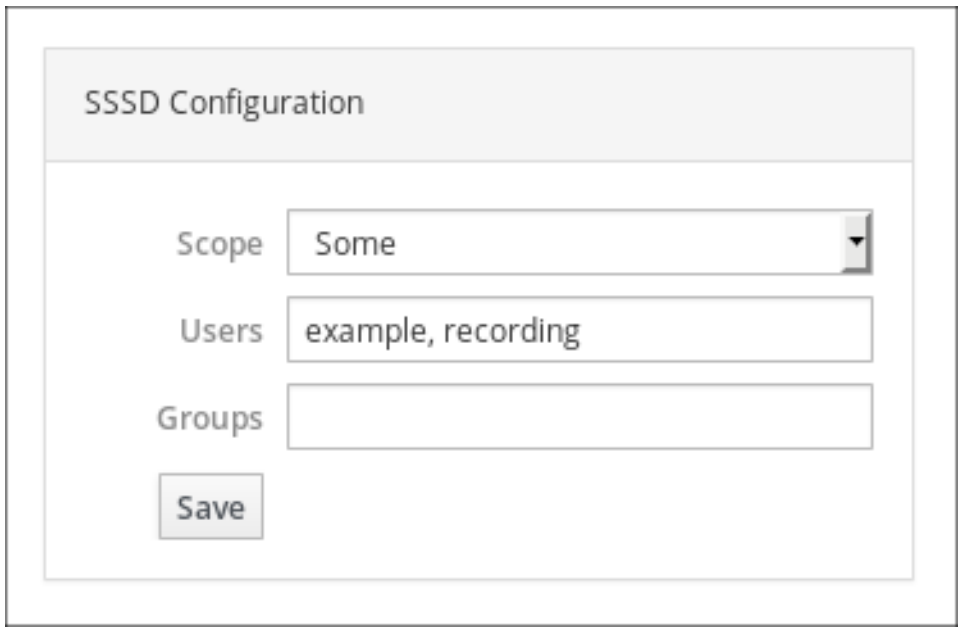
IMPORTANT

Your user has to have administrator privileges to be able to view te recorded sessions.

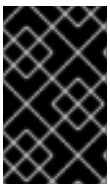
3. Go to the Session Recording page in the menu on the left of the interface.
4. Click on the gear button in the right top corner.

5. Set your parameters in the SSSD Configuration table. Names in the Users and Groups lists should be divided by commas.

Example 2.2. Configuration of recorded users with SSSD



2.5. CONFIGURATION OF RECORDED USERS OR USER GROUPS WITHOUT SSSD



IMPORTANT

Be aware that this practice is not recommended to use. The preferred option is to configure your recorded users via SSSD either from command-line interface or directly from the RHEL 8 web console.

If choose to manually change the user's shell, their working shell will be the one that is listed in the **tlog-rec-session.conf** configuration file.

If you do not want to use SSSD for specifying recorded user or user groups it is possible to directly change the shell of the user you want to record to **/usr/bin/tlog-rec-session**:

```
# chsh <user_name>
Changing shell for <user_name>.
New shell [</old/shell/location>]
```

2.6. EXPORTING RECORDED SESSIONS TO A FILE

You can export your recorded sessions and their logs and copy them.

The following procedure shows how to export recorded sessions on a local system.

Prerequisites

Install the **systemd-journal-remote** package.

```
# yum install systemd-journal-remote
```

Procedure

- Run the **journalctl -o export** command:

```
# journalctl -o export | systemd-journal-remote -o /tmp/dir/example.journal -
```

This creates an export file from the system journal with all its entities. You can then copy the exported file to the **/var/log/journal/** directory on any other host. For your convenience, you can also create the **/var/log/journal/remote/** directory for export files from remote hosts.

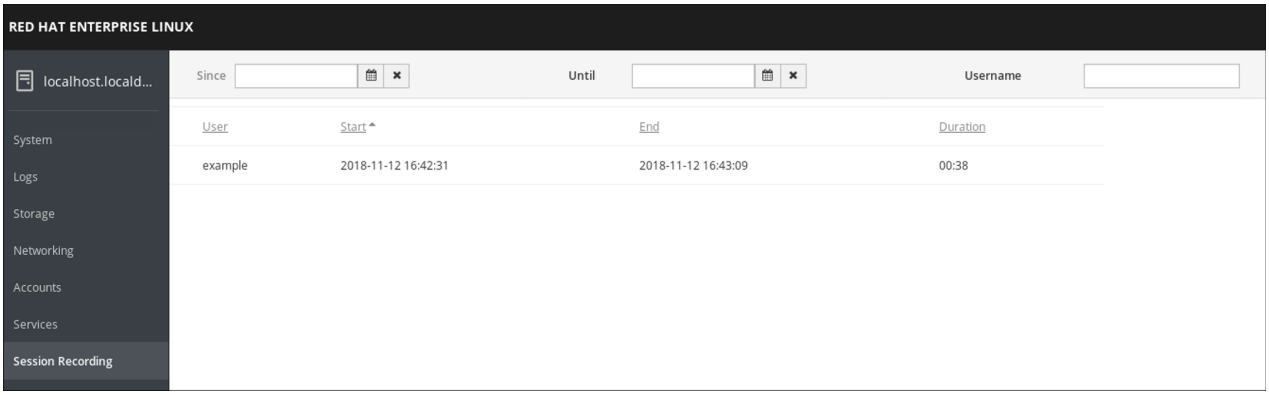
CHAPTER 3. PLAYING BACK RECORDED SESSIONS

There are two possibilities for replaying already recorded sessions. The first one is to use the **tlog-play** tool. The second option is to manage your recorded sessions from the RHEL 8 web console, also referred to as *Cockpit*.

3.1. PLAYBACK WITH THE WEB CONSOLE

The RHEL 8 web console has a whole interface for managing recorded sessions. You can choose the session you want to review directly from the Session recording page, where the list of your recorded session is.

Example 3.1. Example list of recorded sessions



The web console player supports window resizing.

3.2. PLAYBACK WITH TLOG-PLAY

Other option for playback of recorded sessions is using the **tlog-play** tool. The **tlog-play** tool is a playback program for terminal input and output recorded with the **tlog-rec** tool. It reproduces the recording of the terminal it is under, but cannot change its size. For this reason the playback terminal needs to match the recorded terminal size for proper playback. The **tlog-play** tool loads its parameters from the **/etc/tlog/tlog-play.conf** configuration file. The parameters can be overriden with command line options described in the **tlog-play** manual pages.

3.3. PLAYING BACK RECORDED SESSIONS WITH TLOG-PLAY

Recorded sessions can be played back either from a simple file or from Systemd Journal.

Playing back from a file

You can play a session back from a file both during and after recording:

```
# tlog-play --reader=file --file-path=tlog.log
```

Playing back from Journal

Generally, you can select Journal log entries for playback using Journal matches and timestamp limits, with the **-M** or **--journal-match**, **-S** or **--journal-since**, and **-U** or **--journal-until** options.

In practice however, playback from Journal is usually done with a single match against the **TLOG_REC** Journal field. The **TLOG_REC** field contains a copy of the **rec** field from the logged JSON data, which is a host-unique ID of the recording.

You can take the ID either from the **TLOG_REC** field value directly, or from the **MESSAGE** field from the JSON **rec** field. Both fields are part of log messages coming from the **tlog-rec-session** tool.

Procedure

1. You can play back the whole recording as follows:

```
# tlog-play -r journal -M TLOG-REC=<your-unique-host-id>
```

You can find further instructions and documentation in the **tlog-play** manual pages.