



Red Hat Enterprise Linux 8

Recording sessions

Using the Session Recording solution in Red Hat Enterprise Linux 8

Red Hat Enterprise Linux 8 Recording sessions

Using the Session Recording solution in Red Hat Enterprise Linux 8

Legal Notice

Copyright © 2022 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 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

MAKING OPEN SOURCE MORE INCLUSIVE	3
PROVIDING FEEDBACK ON RED HAT DOCUMENTATION	4
CHAPTER 1. GETTING STARTED WITH SESSION RECORDING ON RHEL	5
1.1. SESSION RECORDING IN RHEL	5
1.2. COMPONENTS OF SESSION RECORDING	5
1.3. LIMITATIONS OF SESSION RECORDING	5
CHAPTER 2. DEPLOYING SESSION RECORDING ON RHEL WEB CONSOLE	7
2.1. INSTALLING TLOG	7
2.2. INSTALLING COCKPIT-SESSION-RECORDING	7
2.3. ENABLING SESSION RECORDING FOR USERS AND GROUPS WITH SSSD FROM THE CLI	7
2.4. ENABLING SESSION RECORDING FOR USERS AND GROUPS WITH SSSD FROM THE WEB UI	8
2.5. ENABLING SESSION RECORDING FOR USERS WITHOUT SSSD	9
2.6. EXPORTING RECORDED SESSIONS TO A FILE	9
CHAPTER 3. PLAYING BACK RECORDED SESSIONS	11
3.1. PLAYBACK WITH TLOG-PLAY	11
3.2. PLAYBACK WITH THE WEB CONSOLE	11
3.3. PLAYING BACK RECORDED SESSIONS WITH TLOG-PLAY	11
CHAPTER 4. CONFIGURING A SYSTEM FOR SESSION RECORDING USING THE TERMINAL SESSION RECORDING RHEL SYSTEM ROLE	13
4.1. THE TERMINAL SESSION RECORDING SYSTEM ROLE	13
4.2. COMPONENTS AND PARAMETERS OF THE TERMINAL SESSION RECORDING SYSTEM ROLE	13
4.3. DEPLOYING THE TERMINAL SESSION RECORDING RHEL SYSTEM ROLE	13
4.4. DEPLOYING THE TERMINAL SESSION RECORDING RHEL SYSTEM ROLE FOR EXCLUDING LISTS OF GROUPS OR USERS	15
4.5. RECORDING A SESSION USING THE DEPLOYED TERMINAL SESSION RECORDING SYSTEM ROLE IN THE CLI	17
4.6. WATCHING A RECORDED SESSION USING THE CLI	17

MAKING OPEN SOURCE MORE INCLUSIVE

Red Hat is committed to replacing problematic language in our code, documentation, and web properties. We are beginning with these four terms: master, slave, blacklist, and whitelist. Because of the enormity of this endeavor, these changes will be implemented gradually over several upcoming releases. For more details, see [our CTO Chris Wright's message](#).

PROVIDING FEEDBACK ON RED HAT DOCUMENTATION

We appreciate your feedback on our documentation. Let us know how we can improve it.

Submitting comments on specific passages

1. View the documentation in the **Multi-page HTML** format and ensure that you see the **Feedback** button in the upper right corner after the page fully loads.
2. Use your cursor to highlight the part of the text that you want to comment on.
3. Click the **Add Feedback** button that appears near the highlighted text.
4. Add your feedback and click **Submit**.

Submitting feedback through Bugzilla (account required)

1. Log in to the [Bugzilla](#) website.
2. Select the correct version from the **Version** menu.
3. Enter a descriptive title in the **Summary** field.
4. Enter your suggestion for improvement in the **Description** field. Include links to the relevant parts of the documentation.
5. 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 in Red Hat Enterprise Linux 8 is based on the **tlog** package. You can use the **tlog** package and its associated web console session player to record and play back 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

In order to not intercept raw passwords and other sensitive information, recording of the terminal input is disabled by default. Be aware that if you turn on recording of the terminal input, all entered passwords are captured in plaintext.

You can use this solution for auditing user sessions on security-sensitive systems or, in the event of a security breach, reviewing recorded sessions as part of forensic analysis. As an administrator, you can configure session recording locally on RHEL 8 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 to the Session Recording solution: the **tlog** utility, the SSSD service and a web console embedded user interface.

tlog

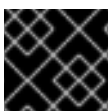
The **tlog** utility is a terminal input/output (I/O) recording and playback program. It inserts the **tlog-rec-session** tool between the user terminal and the user shell, and logs everything that passes through as JSON messages.

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 to record. You can configure these settings 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 and you can use it to manage recorded sessions.



IMPORTANT

You need administrator privileges to access the recorded sessions.

1.3. LIMITATIONS OF SESSION RECORDING

These are the most notable limitations of the Session Recording solution.

- Recordings of root user are not reliable, because the root user can circumvent the recording process.

- Session recording does not record the terminal in a **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** is unable to distinguish between the terminals and prevent repeated recordings.
- If session recording is configured to log to the **journal**, the recorded user will see the act of recording the results of viewing the system journal or **/var/log/messages**. Because viewing generates logs, which then print to the screen, this causes Session Recording to record this action, which generates more records, causing a loop of flooded output.
You can use the following command to work around this problem:

```
# journalctl -f | grep -v 'tlog-rec-session'
```

You can also configure **tlog** to limit the output. For details, see **tlog-rec** or **tlog-rec-session** manual pages.

- To record users executing remote access commands, you must configure session recording for that user on the target host. For example, to record the following remote access command, you need to configure session recording for the **admin** user on the **client** host:

```
ssh admin@client rm -f /some/file
```

- All recordings are lost on reboot because the **journal** is stored in-memory by default on RHEL 8. To export recordings see [Exporting recorded sessions to a file](#) .

CHAPTER 2. DEPLOYING SESSION RECORDING ON RHEL WEB CONSOLE

This section describes how to deploy the Session Recording solution on the Red Hat Enterprise Linux web console.

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

- Use the following command:

```
# 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  
# systemctl enable cockpit.socket
```

or

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

2.3. ENABLING SESSION RECORDING FOR USERS AND GROUPS WITH SSSD FROM THE CLI

If you use SSSD for authentication, you can configure session recording for users and groups from the command line.

Procedure

- Open the **sssd-session-recording.conf** configuration file:

```
# vi /etc/sss/conf.d/sss-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.

1. To specify the scope of session recording, enter one of the following values for the scope option:

- **none** to record no sessions.
- **some** to record only specified sessions.
- **all** to record all sessions.

1. (Optional) If you set the scope as **some** add the names of users and groups in comma-separated lists.

Example 2.1. SSSD configuration

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

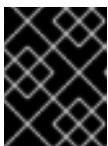
```
[session_recording]
scope = some
users = example1, example2
groups = examples
```

2.4. ENABLING SESSION RECORDING FOR USERS AND GROUPS WITH SSSD FROM THE WEB UI

If you use SSSD for authentication, you can configure session recording for users and groups 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** into your browser.
2. Log in to the RHEL 8 web console.

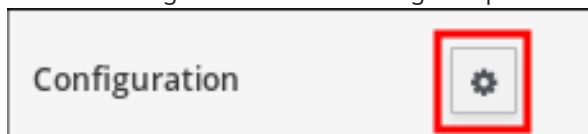


IMPORTANT

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

3. Go to the Session Recording page in the menu on the left.

- Click on the gear button in the right top corner.



- Set your parameters in the SSSD Configuration table. Separate the lists of users and groups with commas.

Example 2.2. Configuration of recorded users with SSSD

 A screenshot of the "SSSD Configuration" form. The form has a title bar "SSSD Configuration". Below it, there are three input fields: "Scope" with a dropdown menu showing "Some", "Users" with a text input containing "example, recording", and "Groups" with an empty text input. At the bottom left of the form is a "Save" button.

2.5. ENABLING SESSION RECORDING FOR USERS WITHOUT SSSD



IMPORTANT

Red Hat does not recommend this option. The preferred option is to configure your recorded users via SSSD either from the command-line interface or directly from the RHEL 8 web console.

If you 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**:

- Change the shell.

```
# sudo usermod -s /usr/bin/tlog-rec-session <user_name>
```

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

1. Create a directory to store exported recording sessions, such as `/tmp/dir`:

```
# mkdir /tmp/dir
```

2. Run the **journalctl -o export** command to export system journal entries related to tlog recordings:

```
# journalctl _COMM=tlog-rec _COMM=tlog-rec-session -o export | /usr/lib/systemd/systemd-journal-remote -o /tmp/dir/example.journal
```

CHAPTER 3. PLAYING BACK RECORDED SESSIONS

There are two methods for replaying recorded sessions:

- the **tlog-play** tool
- the RHEL 8 web console, also referred to as *Cockpit*.

3.1. PLAYBACK WITH TLOG-PLAY

You can use the **tlog-play** tool to play back session recordings in a terminal. 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. You can override those parameters with command line options described in the **tlog-play** manual pages.

3.2. 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

RED HAT ENTERPRISE LINUX

localhost.locald...

System

Logs

Storage

Networking

Accounts

Services

Session Recording

Since  

Until  

Username

User	Start 	End	Duration
example	2018-11-12 16:42:31	2018-11-12 16:43:09	00:38

The web console player supports window resizing.

3.3. PLAYING BACK RECORDED SESSIONS WITH TLOG-PLAY

You can play back session recordings from exported log files or from the 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 the 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.

CHAPTER 4. CONFIGURING A SYSTEM FOR SESSION RECORDING USING THE TERMINAL SESSION RECORDING RHEL SYSTEM ROLE

With the Terminal Session Recording RHEL System Role, you can configure a system for terminal session recording on RHEL using Red Hat Ansible Automation Platform.

4.1. THE TERMINAL SESSION RECORDING SYSTEM ROLE

You can configure a RHEL system for terminal session recording on RHEL using the Terminal Session Recording RHEL System Role.

You can configure the recording to take place per user or user group by means of the **SSSD** service.

Additional resources

- For more details on session recording in RHEL, see [Recording Sessions](#).

4.2. COMPONENTS AND PARAMETERS OF THE TERMINAL SESSION RECORDING SYSTEM ROLE

The Session Recording solution has the following components:

- The **tlog** utility
- System Security Services Daemon (SSSD)
- Optional: The web console interface

The parameters used for the Terminal Session Recording RHEL System Role are:

Role Variable	Description
tlog_use_sssd (default: yes)	Configure session recording with SSSD, the preferred way of managing recorded users or groups
tlog_scope_sssd (default: none)	Configure SSSD recording scope - all / some / none
tlog_users_sssd (default: [])	YAML list of users to be recorded
tlog_groups_sssd (default: [])	YAML list of groups to be recorded

- For details about the parameters used in **tlog** and additional information about the Terminal Session Recording System Role, see the `/usr/share/ansible/roles/rhel-system-roles.tlog/README.md` file.

4.3. DEPLOYING THE TERMINAL SESSION RECORDING RHEL SYSTEM ROLE

Follow these steps to prepare and apply an Ansible playbook to configure a RHEL system to log session recording data to the systemd journal.

Prerequisites

- You have set SSH keys for access from the control node to the target system where the Terminal Session Recording System Role will be configured.
- You have at least one system that you want to configure the Terminal Session Recording System Role.
- The Ansible Core package is installed on the control machine.
- The **rhel-system-roles** package is installed on the control machine.

Procedure

1. Create a new **playbook.yml** file with the following content:

```
---
- name: Deploy session recording
  hosts: all
  vars:
    tlog_scope_sssd: some
    tlog_users_sssd:
      - recorded-user

  roles:
    - rhel-system-roles.tlog
```

Where,

- **tlog_scope_sssd:**
 - **some** specifies you want to record only certain users and groups, not **all** or **none**.
- **tlog_users_sssd:**
 - **recorded-user** specifies the user you want to record a session from. Note that this does not add the user for you. You must set the user by yourself.

2. Optionally, verify the playbook syntax.

```
# ansible-playbook --syntax-check playbook.yml
```

3. Run the playbook on your inventory file:

```
# ansible-playbook -i IP_Address /path/to/file/playbook.yml -v
```

As a result, the playbook installs the **tlog** RHEL System Role on the system you specified. The role includes **tlog-rec-session**, a terminal session I/O logging program, that acts as the login shell for a user. It also creates an SSSD configuration drop file that can be used by the users and groups that you define. SSSD parses and reads these users and groups, and replaces their user shell with **tlog-rec-session**.

Additionally, if the **cockpit** package is installed on the system, the playbook also installs the **cockpit-session-recording** package, which is a **Cockpit** module that allows you to view and play recordings in the web console interface.

Verification steps

To verify that the SSSD configuration drop file is created in the system, perform the following steps:

1. Navigate to the folder where the SSSD configuration drop file is created:

```
# cd /etc/sssdcnf.d
```

2. Check the file content:

```
# cat /etc/sssdcnf.d/sssdcnf-session-recording.cnf
```

You can see that the file contains the parameters you set in the playbook.

4.4. DEPLOYING THE TERMINAL SESSION RECORDING RHEL SYSTEM ROLE FOR EXCLUDING LISTS OF GROUPS OR USERS

You can use the Terminal Session Recording System Role to support the SSSD session recording configuration options **exclude_users** and **exclude_groups**. Follow these steps to prepare and apply an Ansible playbook to configure a RHEL system to exclude users or groups from having their sessions recorded and logged in the systemd journal.

Prerequisites

- You have set SSH keys for access from the control node to the target system on which you want to configure the Terminal Session Recording System Role.
- You have at least one system on which you want to configure the Terminal Session Recording System Role.
- The Ansible Core package is installed on the control machine.
- The **rhel-system-roles** package is installed on the control machine.

Procedure

1. Create a new **playbook.yml** file with the following content:

```
---
- name: Deploy session recording excluding users and groups
  hosts: all
  vars:
    tlog_scope_sssdcnf: all
    tlog_exclude_users_sssdcnf:
      - jeff
      - james
    tlog_exclude_groups_sssdcnf:
      - admins
```

```
roles:
  - rhel-system-roles.tlog
```

Where,

- **tlog_scope_sssd:**
 - **all:** specifies that you want to record all users and groups.
- **tlog_exclude_users_sssd:**
 - **user names:** specifies the user names of the users you want to exclude from the session recording.
- **tlog_exclude_groups_sssd:**
 - **admins** specifies the group you want to exclude from the session recording.

2. Optionally, verify the playbook syntax;

```
# ansible-playbook --syntax-check playbook.yml
```

3. Run the playbook on your inventory file:

```
# ansible-playbook -i IP_Address /path/to/file/playbook.yml -v
```

As a result, the playbook installs the **tlog** RHEL System Role on the system you specified. The role includes **tlog-rec-session**, a terminal session I/O logging program, that acts as the login shell for a user. It also creates an **/etc/sss/conf.d/sss-session-recording.conf** SSSD configuration drop file that can be used by users and groups except those that you defined as excluded. SSSD parses and reads these users and groups, and replaces their user shell with **tlog-rec-session**. Additionally, if the **cockpit** package is installed on the system, the playbook also installs the **cockpit-session-recording** package, which is a **Cockpit** module that allows you to view and play recordings in the web console interface.

Verification steps

To verify that the SSSD configuration drop file is created in the system, perform the following steps:

1. Navigate to the folder where the SSSD configuration drop file is created:

```
# cd /etc/sss/conf.d
```

2. Check the file content:

```
# cat sss-session-recording.conf
```

You can see that the file contains the parameters you set in the playbook.

Additional resources

- See the **/usr/share/doc/rhel-system-roles/tlog/** and **/usr/share/ansible/roles/rhel-system-roles.tlog/** directories.
- The [Recording a session using the deployed Terminal Session Recording System Role in the CLI](#) .

4.5. RECORDING A SESSION USING THE DEPLOYED TERMINAL SESSION RECORDING SYSTEM ROLE IN THE CLI

After you have deployed the Terminal Session Recording System Role in the system you have specified, you are able to record a user terminal session using the command-line interface (CLI).

Prerequisites

- You have deployed the Terminal Session Recording System Role in the target system.
- The SSSD configuration drop file was created in the `/etc/sss/conf.d` directory. See [Deploying the Terminal Session Recording RHEL System Role](#).

Procedure

1. Create a user and assign a password for this user:

```
# useradd recorded-user  
# passwd recorded-user
```

2. Log in to the system as the user you just created:

```
# ssh recorded-user@localhost
```

3. Type "yes" when the system prompts you to type yes or no to authenticate.
4. Insert the *recorded-user*'s password.
The system displays a message about your session being recorded.

```
ATTENTION! Your session is being recorded!
```

5. After you have finished recording the session, type:

```
# exit
```

The system logs out from the user and closes the connection with the localhost.

As a result, the user session is recorded, stored and you can play it using a journal.

Verification steps

To view your recorded session in the journal, do the following steps:

1. Run the command below:

```
# journalctl -o verbose -r
```

2. Search for the **MESSAGE** field of the **tlog-rec** recorded journal entry.

```
# journalctl -xel _EXE=/usr/bin/tlog-rec-session
```

4.6. WATCHING A RECORDED SESSION USING THE CLI

You can play a user session recording from a journal using the command-line interface (CLI).

Prerequisites

- You have recorded a user session. See [Recording a session using the deployed Terminal Session Recording System Role in the CLI](#).

Procedure

1. On the CLI terminal, play the user session recording:

```
# journalctl -o verbose -r
```

2. Search for the **tlog** recording:

```
$ /tlog-rec
```

You can see details such as:

- The username for the user session recording
 - The **out_txt** field, a raw output encode of the recorded session
 - The identifier number `TLOG_REC=ID_number`
3. Copy the identifier number `TLOG_REC=ID_number`.
 4. Playback the recording using the identifier number `TLOG_REC=ID_number`.

```
# tlog-play -r journal -M TLOG_REC=ID_number
```

As a result, you can see the user session recording terminal output being played back.