Red Hat Enterprise Linux 8

Recording sessions

Using the Session Recording solution in Red Hat Enterprise Linux 8

Last Updated: 2021-07-09

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

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. CONFIGURING THE RECORDED USERS OR USER GROUPS WITH SSSD FROM THE CLI 7
2.4. CONFIGURING THE RECORDED USERS OR USER GROUPS WITH SSSD FROM WEB UI 8
2.5. CONFIGURATION OF RECORDED USERS OR USER GROUPS WITHOUT SSSD 9
2.6. EXPORTING RECORDED SESSIONS TO A FILE 9

CHAPTER 3. PLAYING BACK RECORDED SESSIONS 11
3.1. PLAYBACK WITH THE WEB CONSOLE 11
3.2. PLAYBACK WITH TLOG-PLAY 11
3.3. PLAYING BACK RECORDED SESSIONS WITH TLOG-PLAY 11

CHAPTER 4. CONFIGURING A SYSTEM FOR SESSION RECORDING USING THE TLOG RHEL SYSTEM ROLES 13
4.1. THE TLOG SYSTEM ROLE 13
4.2. COMPONENTS AND PARAMETERS OF THE TLOG SYSTEM ROLES 13
4.3. DEPLOYING THE TLOG RHEL SYSTEM ROLE 13
4.4. DEPLOYING THE TLOG RHEL SYSTEM ROLE FOR EXCLUDING LISTS OF GROUPS OR USERS 15
4.5. RECORDING A SESSION USING THE DEPLOYED TLOG SYSTEM ROLE IN THE CLI 17
4.6. WATCHING A RECORDED SESSION USING THE CLI 18

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 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 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 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

Recording of the terminal input is turned off by default to not intercept raw passwords and other sensitive information. Be aware that if you turn on recording of the terminal input, all entered paswords will be captured in plaintext.

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 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

In this section we list the most notable limitations of the Session Recording solution.

- 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.

- When tlog recording is configured to log to the **journal**/**syslog** directory, 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 a 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.

CHAPTER 2. DEPLOYING SESSION RECORDING ON RHEL WEB CONSOLE

In this section we cover how to deploy the Session Recording solution on the Red Hat Enterprise Linux web console.

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

- 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
```

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

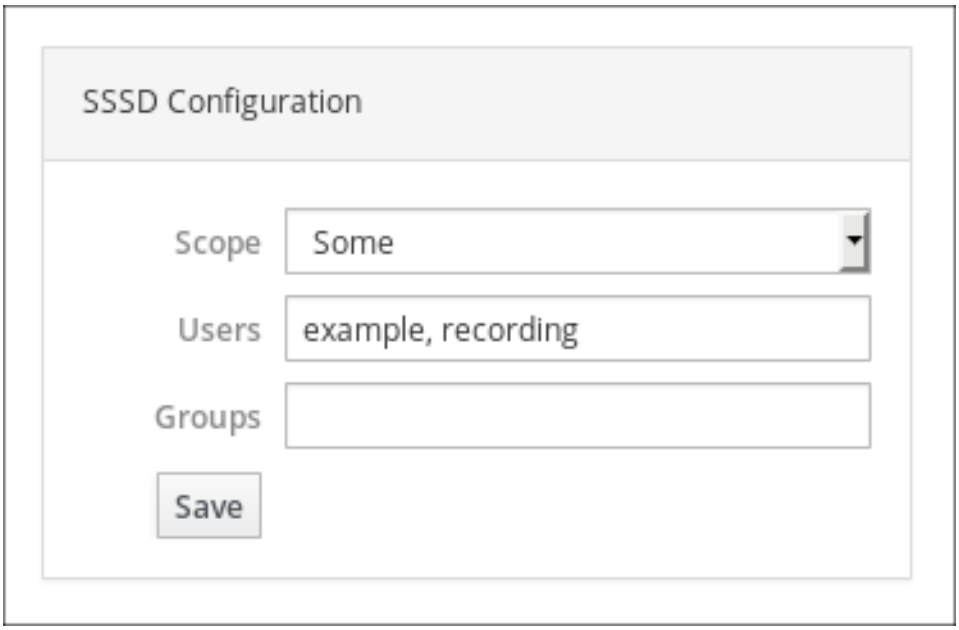
Your user has to have administrator privileges to be able to view te recorded sessions.

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

1. Create the **/tmp/dir** directory:

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

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

   ```
   # journalctl -o export | /usr/lib/systemd/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.

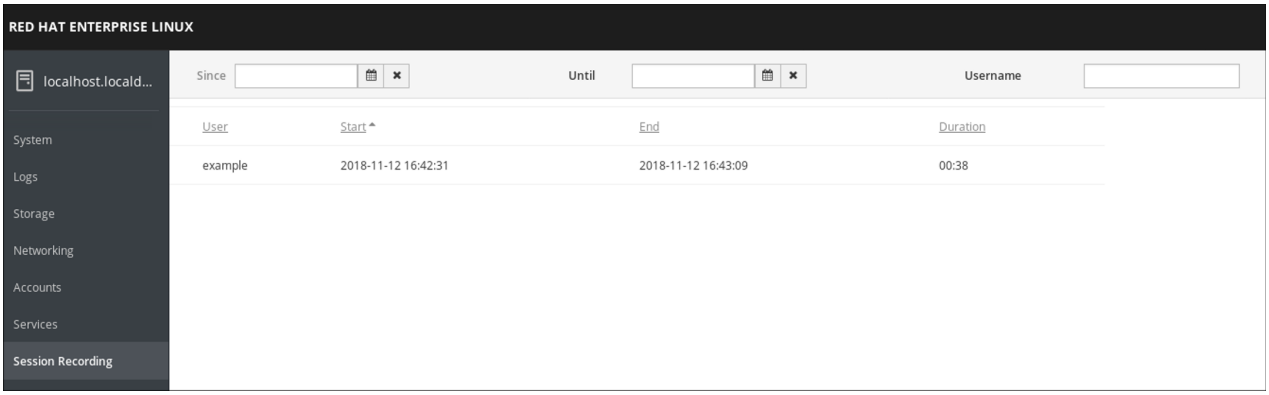
CHAPTER 3. PLAYING BACK RECORDED SESSIONS

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.

CHAPTER 4. CONFIGURING A SYSTEM FOR SESSION RECORDING USING THE TLOG RHEL SYSTEM ROLES

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

4.1. THE TLOG SYSTEM ROLE

You can configure a RHEL system for terminal session recording on RHEL using the **tlog** RHEL System Role. The **tlog** package and its associated web console session player provide you with the ability 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.

Additional resources

- For more details on session recording in RHEL, see Recording Sessions

4.2. COMPONENTS AND PARAMETERS OF THE TLOG SYSTEM ROLES

The Session Recording solution is composed of the following components:

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

The parameters used for the tlog RHEL System Roles 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 tlog System Role, see the **/usr/share/ansible/roles/rhel-system-roles.tlog/README.md** file.

4.3. DEPLOYING THE TLOG RHEL SYSTEM ROLE

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

Prerequisites

- You have set SSH keys for access from the control node to the target system where the **tlog** System Role will be configured.
- You have one control node, which is a system from which the Ansible Engine configures the other systems.
- You have Red Hat Ansible Engine installed on the control node, from which you want to run the playbook.
- You have the **rhel-system-roles** package installed on the control node from which you want to run the playbook.
- You have at least one system that you want to configure the **tlog** System Role. You do not have to have Red Hat Ansible Automation Platform installed on the systems on which you want to deploy the **tlog** solution.

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:
      - recordeduser

  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**:
  - **recordeduser** 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** role on the system you specified. 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 to overlay **tlog** session as the shell user. 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/sssd/conf.d
```

2. Check the file content:

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

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

4.4. DEPLOYING THE TLOG RHEL SYSTEM ROLE FOR EXCLUDING LISTS OF GROUPS OR USERS

You can use the **tlog** System Role on RHEL 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 tlog System Role.
- You have one control node, which is a system from which the Red Hat Ansible Engine configures the other systems.
- You have Red Hat Ansible Engine installed on the control node, from which you want to run the playbook.
- You have the **rhel-system-roles** package installed on the control node.
- You have at least one system on which you want to configure the **tlog** System Role.
  You do not have to have Red Hat Ansible Automation Platform installed on the systems on which you want to deploy the **tlog** solution.

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_sssd: all
    tlog_exclude_users_sssd:
      - jeff
      - james
```

```
    tlog_exclude_groups_sssd:
      - 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** package on the system you specified. It also creates an **/etc/sssd/conf.d/sssd-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 to overlap **tlog** session as the shell user. 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.

NOTE

You are not able to record a session for users listed in the **exclude_users** list or if they are a member of a group in the **exclude_groups** list.

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/sssd/conf.d
```

2. Check the file content:

```
# cat sssd-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.
- See Section 4.5, “Recording a session using the deployed tlog system role in the CLI” .

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

Once you have deployed the **tlog** 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 **tlog** System Role in the target system.
- The SSSD configuration drop file was created in the **/etc/sssd/conf.d** file.

Procedure

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

```
# useradd recordeduser
# passwd recordeduser
```

2. Relog to the system as the user you just created:

```
# ssh recordeduser@localhost
```

3. Type "yes" when the system prompts you to type yes or no to authenticate.
4. Insert the *recordeduser's* password.
   The system prompts a message to inform that your session is being recorded.

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

5. Once 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 Section 4.5, "Recording a session using the deployed tlog 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.