Red Hat Enterprise Linux 8

セッションの録画

Red Hat Enterprise Linux 8 でセッション録画ソリューションの使用

Last Updated: 2020-09-04

Red Hat Enterprise Linux 8 セッションの録画

Red Hat Enterprise Linux 8 でセッション録画ソリューションの使用

法律上の通知

概要

本書は、Red Hat Enterprise Linux 8 の RHEL Web コンソール埋め込みプレーヤーを使用した、tlog をベースとしたセッション録画ソリューションの使用を説明します。

目次

RED HAT ドキュメントへのフィードバック (英語のみ)

ご意見ご要望をお聞かせください。ドキュメントの改善点はございませんか。改善点を報告する場合は、以下のように行います。

- 特定の文章に簡単なコメントを記入する場合は、以下の手順を行います。
    1. ドキュメントの表示が **Multi-page HTML** 形式になっていて、ドキュメントの右上端に **Feedback** ボタンがあることを確認してください。
    2. マウスカーソルで、コメントを追加する部分を強調表示します。
    3. そのテキストの下に表示される **Add Feedback** ポップアップをクリックします。
    4. 表示される手順に従ってください。
- より詳細なフィードバックを行う場合は、Bugzilla のチケットを作成します。
    1. Bugzilla の Web サイトにアクセスします。
    2. Component で **Documentation** を選択します。
    3. **Description** フィールドに、ドキュメントの改善に関するご意見を記入してください。ドキュメントの該当部分へのリンクも記入してください。
    4. **Submit Bug** をクリックします。

第1章 RHEL でセッションの録画を開始

1.1. RHEL でセッションの録画

本セクションでは、セッション録画ソリューションとその目的を紹介します。

セッション録画ソリューションは Red Hat Enterprise Linux 8 で提供され、**tlog** パッケージをベースにしています。**tlog** パッケージおよび関連の Web コンソールセッションプレーヤーを使用すると、ユーザーの端末セッションを録画および再生できます。SSSD サービスを介して、ユーザーごと、またはユーザーグループごとに録画を行うように設定できます。端末の入出力はすべて収集され、テキスト形式でシステムジャーナルに保存されます。

重要

未加工のパスワードやその他の機密情報を傍受しないように、端末への入力の録画はデフォルトで無効になっています。端末入力の録画をオンにすると、入力したすべてのパスワードがプレーンテキストでキャプチャーされます。

このソリューションは、セキュリティーの影響を受けるシステムのユーザーセッションの監査に使用できます。また、セキュリティー侵害が発生した場合は、フォレンジック分析の一環として、録画したセッションが確認されます。RHEL 8 システムでは、システム管理者は、セッションの録画をローカルに設定できます。録画されたセッションは、Web コンソールインターフェース、または端末で **tlog-play** コマンドを使用して確認できます。

1.2. セッションの録画用コンポーネント

セッション録画ソリューションには、主に次の 3 つのコンポーネントがあります。**tlog** ユーティリティーは、SSSD サービスおよび Web コンソールの埋め込みユーザーインターフェースです。

tlog

tlog ユーティリティーは、端末の入出力 (I/O) を録画および再生するプログラムです。ユーザーの端末およびユーザーシェルの間に自身 (特に **tlog-rec-session** ツール) を挿入して、JSON メッセージとして渡されるすべてのログを記録します。

SSSD

SSSD (System Security Services Daemon) は、リモートディレクトリーと認証メカニズムへのアクセスを管理する一連のデーモンを提供します。セッションの録画を設定する際に、SSSD を使用して、tlog の録画を行うユーザーまたはユーザーグループを指定できます。これは、コマンドラインインターフェース (CLI) または RHEL 8 Web コンソールインターフェースから実行できます。

RHEL 8 Web コンソール埋め込みインターフェース

セッションの録画ページは、RHEL 8 Web コンソールインターフェースに含まれます。セッション録画用の Web コンソール埋め込みインターフェースを使用すると、録画したセッションを管理できます。

重要

録画したセッションにアクセスするには、管理者権限が必要です。

1.3. セッションの録画の制限

本セクションでは、セッション録画ソリューションで最も重要な制限を説明します。

- **tlog** は、**Gnome 3** グラフィカルセッションの端末を録画しません。グラフィカルセッションには、全端末用に監査セッション ID が 1 つしかなく、**tlog** には端末を区別して録画が繰り返し行われないようにする手段がないため、グラフィカルセッションでの端末の録画には対応していません。

- **journal**/**syslog** ディレクトリーにログを記録するように tlog 録画を設定すると、録画したユーザーは、システムジャーナルまたは /**var**/**log**/**messages** の表示結果を記録する動作を確認できます。表示によりログが生成され、画面に出力されるため、セッションの録画によりこのアクションが録画され、さらに録画が生成されるため、出力が繰り返しあふれます。
この問題を回避するには、次のコマンドを実行します。

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

出力を制限するように tlog を設定することもできます。詳細は、man ページの **tlog-rec** または **tlog-rec-session** を参照してください。

第2章 RHEL へのセッション録画のデプロイメント

このセクションでは、Red Hat Enterprise Linux システムにセッション録画ソリューションをデプロイする方法を説明します。

前提条件

セッション録画ソリューションをデプロイできるようにするために、**tlog** パッケージ、SSSD パッケージ、および **cockpit-session-recording** パッケージをインストールしている。

2.1. TLOG のインストール

tlog パッケージをインストールします。

手順

1. 次のコマンドを実行します。

```
# yum install tlog
```

2.2. COCKPIT-SESSION-RECORDING のインストール

基本的な Web コンソールパッケージは、デフォルトで Red Hat Enterprise Linux 8 に同梱されます。セッション録画ソリューションを使用できるようにするには、**cockpit-session-recording** パッケージをインストールして、システムで Web コンソールを起動または有効にする必要があります。

手順

1. **cockpit-session-recording** をインストールします。

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

2. システムで Web コンソールを起動または有効にします。

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

または

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

必要なパッケージをすべてインストールしたら、録画パラメーターを設定できます。

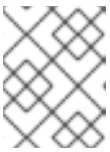
2.3. CLI で SSSD を使用して録画するユーザーまたはユーザーグループの設定

SSSD で録画するユーザーまたはユーザーグループを管理する (推奨オプション) 場合は、ユーザーの元のシェルがすべて保持されます。

手順

1. コマンドラインインターフェース (CLI) から録画するユーザーまたはユーザーグループを指定するには、**sssd-session-recording.conf** 設定ファイルを開いて修正します。

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



注記

Web コンソールインターフェースで設定ページを開くと、**sssd-session-recording.conf** ファイルが自動的に作成されます。

2. 録画するユーザーまたはユーザーグループの範囲を、以下のいずれかから指定します。
   - **none** は、セッションを録画しません。
   - **some** は、指定したセッションのみを録画します。
   - **all** は、すべてのセッションを録画します。
3. 録画したユーザーまたはグループの範囲に **some** を選択した場合は、名前をコンマで区切ってファイルに追加します。

例2.1 SSSD の設定

次の例では、**example1** ユーザー、**example2** ユーザー、および **examples** グループでセッションの録画を有効にします。

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

2.4. WEB UI で SSSD を使用して録画するユーザーまたはユーザーグループの設定

SSSD を使用して録画するユーザーまたはユーザーグループを指定する 2 つ目のオプションは、RHEL 8 Web コンソールに直接一覧表示することです。

手順

1. **localhost:9090** を入力するか、お使いの IP アドレス (**<IP_ADDRESS>:9090**) をブラウザーに入力して、RHEL 8 Web コンソールにローカルに接続します。
2. RHEL 8 Web コンソールにログインします。

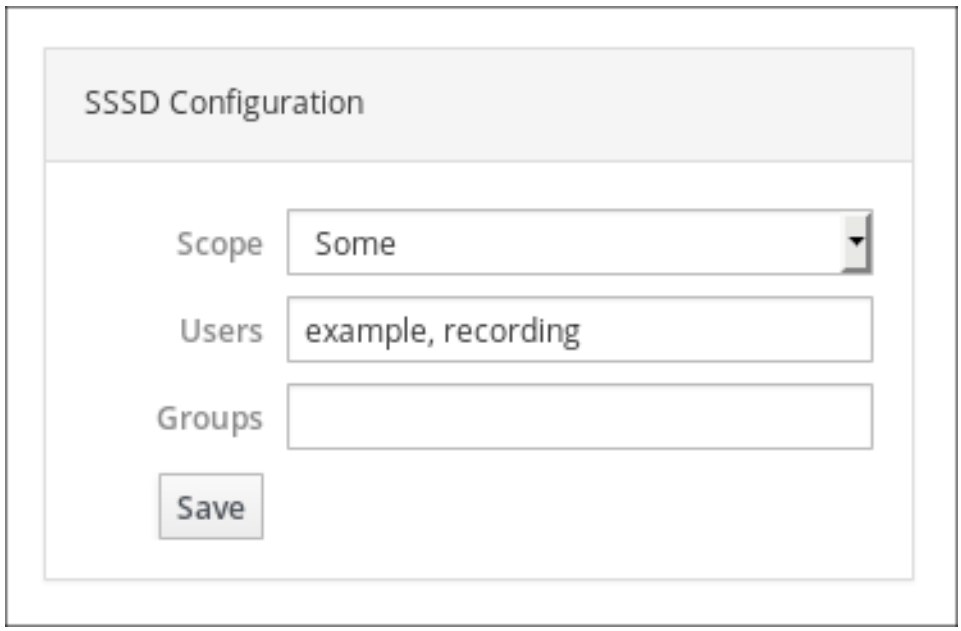
重要

録画したセッションを表示するには、管理者権限が必要です。

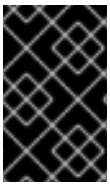
3. インターフェースの左側にあるメニューで、セッション録画ページに移動します。
4. 右上の歯車ボタンをクリックします。

5. SSSD 設定テーブルにパラメーターを設定します。ユーザー一覧およびグループ一覧の名前はコンマで区切る必要があります。

例2.2 SSSD を使用して録画したユーザーの設定



2.5. SSSD を使用せずに録画するユーザーまたはユーザーグループの設定



重要

このプラクティスの使用は推奨されていません。録画するユーザーを、コマンドラインインターフェースまたは RHEL 8 Web コンソールから直接、SSSD を介して設定することが推奨されます。

ユーザーのシェルを手動で変更した場合、作業シェルは、**tlog-rec-session.conf** 設定ファイルに記載されているものになります。

録画したユーザーまたはユーザーグループの指定に SSSD を使用しない場合は、**/usr/bin/tlog-rec-session** に録画するユーザーのシェルを次のように直接変更できます。

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

2.6. 録画したセッションのファイルへのエクスポート

録画したセッションおよびそのログをエクスポートして、コピーできます。

次の手順では、録画したセッションをローカルシステムにエクスポートする方法を説明します。

前提条件

systemd-journal-remote パッケージをインストールします。

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

手順

1. **/tmp/dir** ディレクトリーを作成します。

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

2. **journalctl -o export** コマンドを実行します。

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

これにより、システムジャーナルから、すべてのエンティティーを含むエクスポートファイルが作成されます。エクスポートしたファイルを、別のホストの **/var/log/journal/** ディレクトリーにコピーします。必要に応じて、リモートホストからファイルをエクスポートする **/var/log/journal/remote/** を作成することもできます。

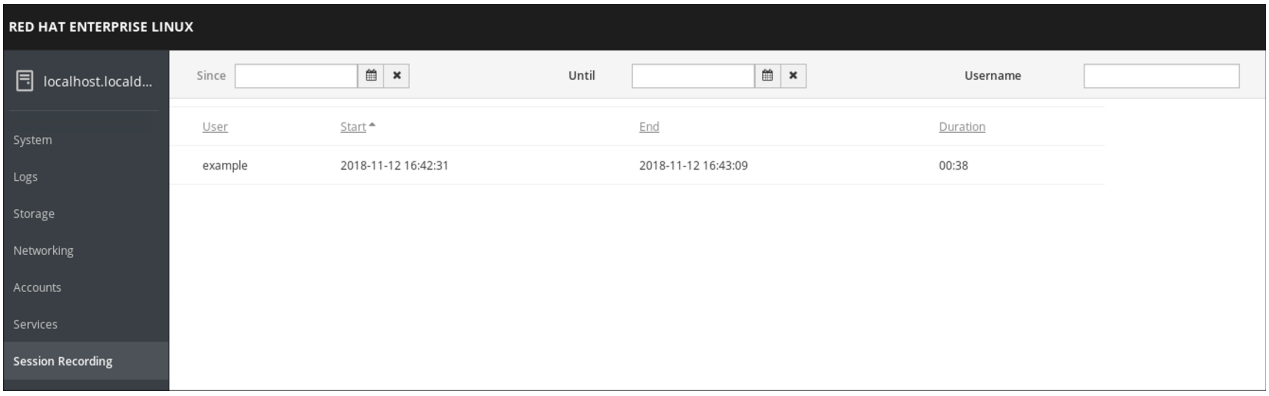
第3章 録画したセッションの再生

録画されているセッションを再生する方法は、2 つあります。1つ目は、**tlog-play** ツールを使用します。2 つ目は、RHEL 8 Web コンソール (**Cockpit** と呼ばれます) から、録画したセッションを管理します。

3.1. WEB コンソールで再生

RHEL 8 Web コンソールには、録画したセッションを管理するインターフェースがあります。録画したセッションの一覧があるセッション録画ページから直接、確認するセッションを選択できます。

例3.1 録画したセッション一覧の例



Web コンソールプレーヤーは、ウィンドウのサイズ変更に対応します。

3.2. TLOG-PLAY で再生

録画したセッションの再生に使用する別の方法では、**tlog-play** ツールを使用します。**tlog-play** ツールは、**tlog-rec** ツールで録画した端末の入出力を再生するプログラムです。これは、そのターミナルの録画を再生しますが、録画したファイルのサイズを変更することはできません。このため、再生ターミナルが適切な再生を行うには、録画した端末のサイズと一致させる必要があります。**tlog-play** ツールは、**/etc/tlog/tlog-play.conf** 設定ファイルからパラメーターを読み込みます。パラメーターは、man ページの **tlog-play** に記載されているコマンドラインオプションで上書きできます。

3.3. TLOG-PLAY で録画したセッションの再生

録画したセッションは、1つのファイルまたは Systemd ジャーナルから再生できます。

ファイルから再生

セッションは、録画中および録画後に、ファイルから再生できます。

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

ジャーナルから再生

通常、**-M** (または **--journal-match**) オプション、**-S** (または **--journal-since**) オプション、および **-U** (または **--journal-until**) オプションを使用し、ジャーナルの一致とタイムスタンプの制限を使用して、ジャーナルログエントリーを選択して再生できます。

ただし、実際には、ジャーナルからの再生は、通常、**TLOG_REC** ジャーナルフィールドに対する 1 つの一致で行われます。**TLOG_REC** のフィールドには、ログに記録した JSON データからコピーした **rec** フィールドが含まれます。これは、録画におけるホスト固有の ID です。

ID は、**TLOG_REC** フィールド値から直接取得するか、JSON の **rec** フィールドの **MESSAGE** フィールドから取得できます。どちらのフィールドも、**tlog-rec-session** ツールから送信されるログメッセージの一部です。

手順

1. 次のコマンドを実行すると、録画全体を再生できます。

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

詳細な手順およびドキュメントは、man ページの **tlog-play** で参照できます。