Red Hat Enterprise Linux 8

セッションの録画

Red Hat Enterprise Linux 8 でのセッションの録画ソリューションの使用

Last Updated: 2024-06-26

Red Hat Enterprise Linux 8 セッションの録画

Red Hat Enterprise Linux 8 でのセッションの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の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)

Red Hat ドキュメントに関するご意見やご感想をお寄せください。また、改善点があればお知らせください。

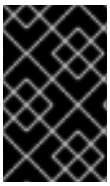
Jira からのフィードバック送信 (アカウントが必要)

1. Jira の Web サイトにログインします。
2. 上部のナビゲーションバーで **Create** をクリックします。
3. **Summary** フィールドにわかりやすいタイトルを入力します。
4. **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追加してください。
5. ダイアログの下部にある **Create** 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

Red Hat Enterprise Linux 8 のセッションの録画ソリューションは、**tlog** パッケージに基づいています。**tlog** パッケージと関連する Web コンソールセッションプレーヤーを使用して、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

raw 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を使用すると、セキュリティーの影響を受けるシステムでユーザーセッションを監査できます。また、セキュリティー違反が発生した場合は、フォレンジック分析の一環として録画したセッションを確認できます。管理者は、RHEL 8 システムで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イス、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

セッションの録画ソリューションには、**tlog** ユーティリティー、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イスという 3 つの主要コンポーネントがあります。

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。ユーザーの端末とユーザーシェルの間に **tlog-rec-session** ツールを挿入し、JSON メッセージとして通過したすべてのものをログに記録します。

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、録画するユーザーまたはユーザーグループを指定できます。この設定は、コマンドラインインターフェイス (CLI) または RHEL 8 Web コンソールインターフェイスから設定できます。

RHEL 8 Web コンソール埋め込みインターフェイス

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イスの一部で、録画したセッションの管理に使用できます。

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

これは、セッションの録画ソリューションにおける最も重要な制限です。

- root ユーザーは録画プロセスを回避できるため、root ユーザーの録画は信頼できません。

- セッションの録画は、**Gnome 3** グラフィカルセッションで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に監査セッション ID が 1 つあり、**tlog** は端末を区別できず、録画が繰り返し行われなくなるため、グラフィカルセッションでの端末の録画はサポートされません。

- セッションの録画が **journal** にログを記録するように設定されると、録画したユーザーは、システムジャーナルまたは **/var/log/messages** の表示結果を録画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、以下のコマンドを使用します。

```
# 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。

- リモートアクセスコマンドを実行するユーザーを録画するには、ターゲットホストでそのユーザーのセッションの録画を設定する必要があります。たとえば、以下のリモートアクセスコマンドを録画するには、**client** ホストで **admin** ユーザーのセッションの録画を設定する必要があります。

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

- **journal** は、RHEL 8 ではデフォルトでインメモリーに保存されるため、すべての録画は再起動時に失われます。録画をエクスポートする場合は、Exporting recorded sessions to a file を参照してください。

第2章 RHEL WEB コンソールへのセッションの録画のデプロイ

本セクションでは、Red Hat Enterprise Linux Web コンソールにセッションの録画ソリューションをデプロイする方法を説明します。

セッションの録画ソリューションをデプロイするには、以下のパッケージをインストールする必要があります。

- **tlog**
- SSSD
- **cockpit-session-recording**

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

- 以下のコマンドを使用します。

```
# 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。セッションの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
# systemctl enable cockpit.socket
```

または、以下を実行します。

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

2.3. CLI からの SSSD を使用したユーザーおよびグループのセッションの録画の有効化

SSSD を使用して認証する場合は、コマンドラインからユーザーおよびグループのセッションの録画を設定できます。

手順

- **sssd-session-recording.conf** 設定ファイルを開きます。

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

注記

Web コンソールインターフェイ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。

1. セッションの録画の範囲を指定するには、scope オプションに以下のいずれかの値を入力します。

- **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。

1. (オプション): スコープを **some** として設定する場合は、ユーザーとグループの名前をコンマ区切りのリストに追加します。

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 を使用したユーザーおよびグループのセッションの録画の有効化

SSSD を認証に使用する場合は、RHEL 8 Web コンソールでユーザーおよびグループにセッションの録画を設定できます。

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

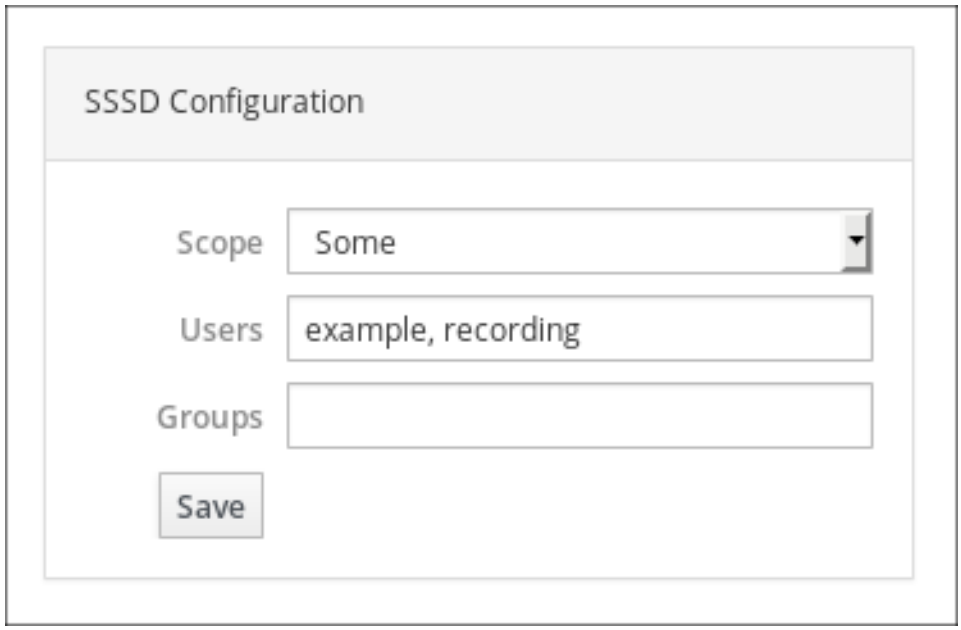
録画したセッションを表示するには、管理者権限が必要です。

3. 左側のメニューのセッションの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。ユーザーおよびグループのリストをコンマで区切ります。

例2.2 SSSD を使用して録画したユーザーの設定



2.5. SSSD を使用しないユーザー向けセッションの録画の有効化

重要

Red Hat は、このオプションを推奨しません。録画するユーザーを、コマンドラインインターフェイスまたは RHEL 8 Web コンソールから直接 SSSD で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することを選択すると、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。

1. シェルを変更します。

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

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
```

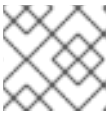
手順

1. `/tmp/dir などのエクスポートされた録画セッションを保存するディレクトリーを作成します。

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

2. **journalctl -o export** コマンドを実行して、tlog 録画に関連するシステムジャーナルエントリーをエクスポートします。

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



注記

COMM=tlog-rec-sessio COMM 名は、15 文字の制限により短縮されます。

第3章 録画したセッションの再生

録画したセッションを再生する方法は 2 つあります。

- **tlog-play** ツール
- RHEL 8 Web コンソール (**Cockpit** とも呼ばれる)

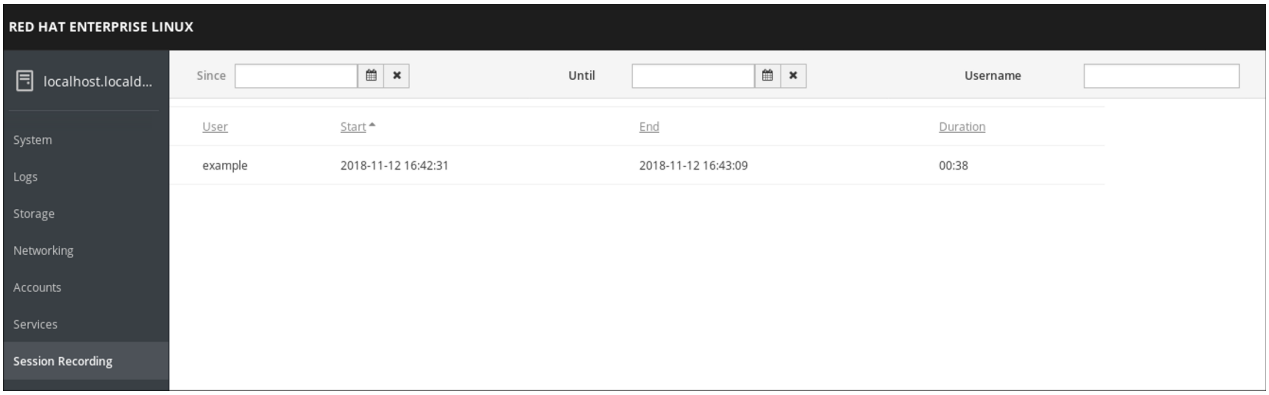
3.1. TLOG-PLAY で再生

tlog-play ツールを使用して、端末でセッションの録画を再生できます。**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。これらのパラメーターは、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。

3.2. 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イスがあります。録画したセッションのリストがあるセッションの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リストの例



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。

3.3. TLOG-PLAY で録画したセッションの再生

エクスポートされたログファイルまたは Systemd Journal からセッションの録画を再生できます。

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
```

ジャーナルからの再生

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** を参照してください。

第4章 RHEL システムロールを使用したセッション記録用システムの設定

tlog RHEL システムロールを使用すると、Red Hat Ansible Automation Platform を使用して、RHEL でターミナルセッションを記録するようにシステムを設定できます。

4.1. TLOG RHEL システムロール

tlog RHEL システムロールを使用して、RHEL でターミナルセッションを記録するように RHEL システムを設定できます。

SSSD サービスを使用して、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。

関連情報

- **/usr/share/ansible/roles/rhel-system-roles.ha_cluster/README.md** ファイル
- **/usr/share/doc/rhel-system-roles/ha_cluster/** ディレクトリー
- レコーディングセッション

4.2. TLOG RHEL システムロールのコンポーネントとパラメーター

セッションの録画ソリューションには、以下のコンポーネントがあります。

- **tlog** ユーティリティー
- System Security Services Daemon (SSSD)
- オプション: Web コンソールインターフェイス

関連情報

- **/usr/share/ansible/roles/rhel-system-roles.ha_cluster/README.md** ファイル
- **/usr/share/doc/rhel-system-roles/ha_cluster/** ディレクトリー
- レコーディングセッション

4.3. TLOG RHEL システムロールのデプロイ

以下の手順に従って、Ansible Playbook を準備および適用し、RHEL システムが systemd ジャーナルにセッションの録画データをログに記録するように設定します。

この Playbook は、指定されたシステムに **tlog** RHEL システムロールをインストールします。このロールには、ユーザーのログインシェルとして機能するターミナルセッション I/O ロギングプログラムである **tlog-rec-session** が含まれます。また、定義したユーザーおよびグループで使用できる SSSD 設定ドロップファイルを作成します。SSSD は、これらのユーザーとグループを解析して読み取り、ユーザーシェルを **tlog-rec-session** に置き換えます。さらに、**cockpit** パッケージがシステムにインストールされている場合、Playbook は **cockpit-session-recording** パッケージもインストールします。これは、Web コンソールインターフェイスで録画を表示および再生できるようにする **Cockpit** モジュールです。

前提条件

- 制御ノードと管理ノードを準備している
- 管理対象ノードで Playbook を実行できるユーザーとしてコントロールノードにログインしている。
- 管理対象ノードへの接続に使用するアカウントに、そのノードに対する **sudo** 権限がある。

手順

1. 次の内容を含む Playbook ファイル (例: ~/**playbook.yml**) を作成します。

```
---
- name: Deploy session recording
  hosts: managed-node-01.example.com
  roles:
    - rhel-system-roles.tlog
  vars:
    tlog_scope_sssd: some
    tlog_users_sssd:
      - recorded-user
```

tlog_scope_sssd

some 値は、**all** または **none** ではなく、特定のユーザーとグループのみを記録することを指定します。

tlog_users_sssd

セッションを記録するユーザーを指定します。ただし、ユーザーは追加されない点に留意してください。ユーザーを独自に設定する必要があります。

2. Playbook の構文を検証します。

```
$ ansible-playbook --syntax-check ~/playbook.yml
```

このコマンドは構文を検証するだけであり、有効だが不適切な設定から保護するものではないことに注意してください。

3. Playbook を実行します。

```
$ ansible-playbook ~/playbook.yml
```

検証

1. SSSD 設定ドロップファイルが作成されるフォルダーに移動します。

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

2. ファイルの内容を確認します。

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

Playbook に設定したパラメーターがファイルに含まれていることが確認できます。

3. セッションを記録するユーザーとしてログインします。
4. 記録されたセッションを再生します。

関連情報

- **/usr/share/ansible/roles/rhel-system-roles.tlog/README.md** ファイル
- **/usr/share/doc/rhel-system-roles/tlog/** ディレクトリー

4.4. グループまたはユーザーのリストを除外するために TLOG RHEL システムロールをデプロイする

tlog システムロールを使用すると、SSSD セッションの録画設定オプション **exclude_users** および **exclude_groups** をサポートできます。以下の手順に従って、Ansible Playbook を準備および適用し、ユーザーまたはグループがセッションを録画して systemd ジャーナルにロギングしないように RHEL システムを設定します。

この Playbook は、指定されたシステムに **tlog** RHEL システムロールをインストールします。このロールには、ユーザーのログインシェルとして機能するターミナルセッション I/O ロギングプログラムである **tlog-rec-session** が含まれます。また、除外対象外のユーザーおよびグループが使用できる **/etc/sssd/conf.d/sssd-session-recording.conf** SSSD 設定ドロップファイルを作成します。SSSD は、これらのユーザーとグループを解析して読み取り、ユーザーシェルを **tlog-rec-session** に置き換えます。さらに、**cockpit** パッケージがシステムにインストールされている場合、Playbook は **cockpit-session-recording** パッケージもインストールします。これは、Web コンソールインターフェイスで録画を表示および再生できるようにする **Cockpit** モジュールです。

前提条件

- 制御ノードと管理ノードを準備している
- 管理対象ノードで Playbook を実行できるユーザーとしてコントロールノードにログインしている。
- 管理対象ノードへの接続に使用するアカウントに、そのノードに対する **sudo** 権限がある。

手順

1. 次の内容を含む Playbook ファイル (例: ~/**playbook.yml**) を作成します。

```
---
- name: Deploy session recording excluding users and groups
  hosts: managed-node-01.example.com
  roles:
    - rhel-system-roles.tlog
  vars:
    tlog_scope_sssd: all
    tlog_exclude_users_sssd:
      - jeff
      - james
    tlog_exclude_groups_sssd:
      - admins
```

tlog_scope_sssd

値 **all** は、すべてのユーザーとグループを記録することを指定します。

tlog_exclude_users_sssd

セッションの記録から除外するユーザーのユーザー名を指定します。

tlog_exclude_groups_sssd

セッション記録から除外するグループを指定します。

2. Playbook の構文を検証します。

```
$ ansible-playbook --syntax-check ~/playbook.yml
```

このコマンドは構文を検証するだけであり、有効だが不適切な設定から保護するものではないことに注意してください。

3. Playbook を実行します。

```
$ ansible-playbook ~/playbook.yml
```

検証

1. SSSD 設定ドロップファイルが作成されるフォルダーに移動します。

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

2. ファイルの内容を確認します。

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

Playbook に設定したパラメーターがファイルに含まれていることが確認できます。

3. セッションを記録するユーザーとしてログインします。

4. 記録されたセッションを再生します。

関連情報

- **/usr/share/ansible/roles/rhel-system-roles.tlog/README.md** ファイル
- **/usr/share/doc/rhel-system-roles/tlog/** ディレクトリー