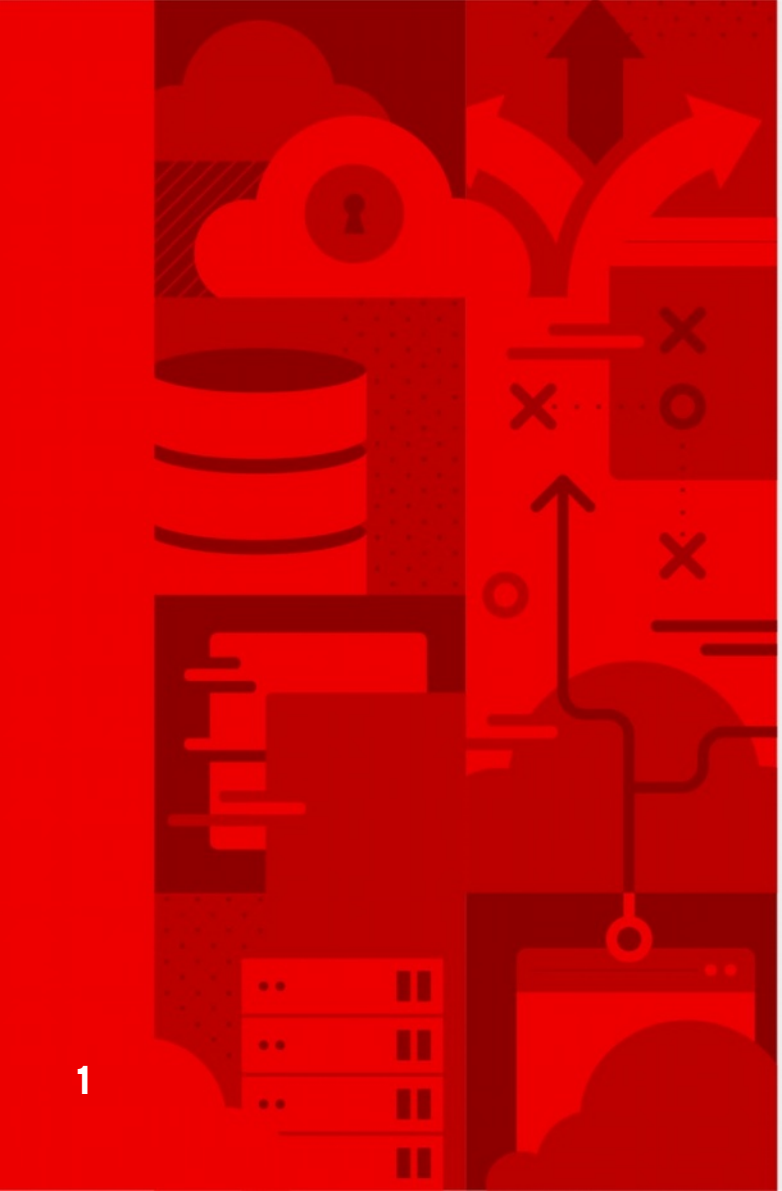


Red Hat
Enterprise Linux 8

端末のセッション記録

2019 年 9 月 12 日
レッドハット株式会社
森若 和雄

Red Hat

このスライドについて

対象

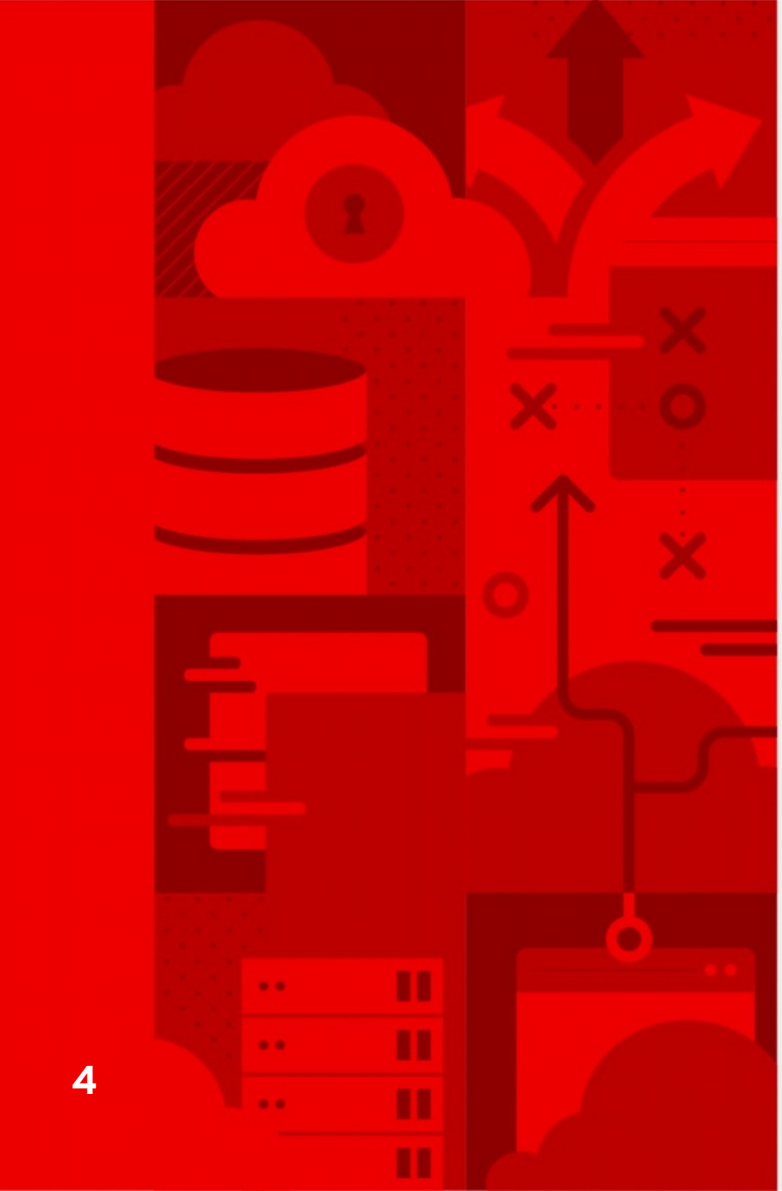
RHEL8 で端末セッションの記録がしたい人
RHEL8 の新機能として導入された tlog について知りたい人

目的

tlog の基本的な使い方と、現状の制限を紹介する

概要

- 端末のセッション記録とは何か？
- tlog で何ができるか？
- tlog 利用時の注意点
- 参考資料



端末のセッション記録とは何か？

Red Hat

端末のセッション記録 とは

端末への入出力をログなどに保存してあとで見られるようにします

利用目的は作業の記録、監査証跡の保存、デモンストレーション など

RHEL 8 では端末のセッション記録機能が含まれます

ログイン時に tlog-rec-session ユーティリティが動作して、端末への入出力をログに記録します

制限 : Gnome 上の仮想端末セッションは自動記録できません

Gnome(または任意のグラフィカルセッション) ではデスクトップ全体で 1 つのセッションを共有するため端末を識別できず、自動的なセッション記録ができません。

セッション記録関連コマンドなど

ユーザが利用するコマンド

- tlog-rec　端末入出力をログに出力する
- tlog-play　ログを端末で再生する

セッション開始時に自動で記録を開始する

- tlog-rec-session　端末入出力をログに出力し、シェルを起動する
- sssd　ユーザやグループにより tlog-rec-session の起動有無を決める

Web UI

- cockpit-session-recording
  Web Console(cockpit) にセッション記録の設定機能と再生機能を提供するプラグイン

セッション記録概要図

login や sshd はユーザ情報を sssd に問いあわせ

login や sshd

sssd

sssd は条件を満たすログイン時には tlog-rec-session をシェルとして返す。

ログにはセッション毎の ID がついているので抽出して再生できる

tlog-play

cockpit

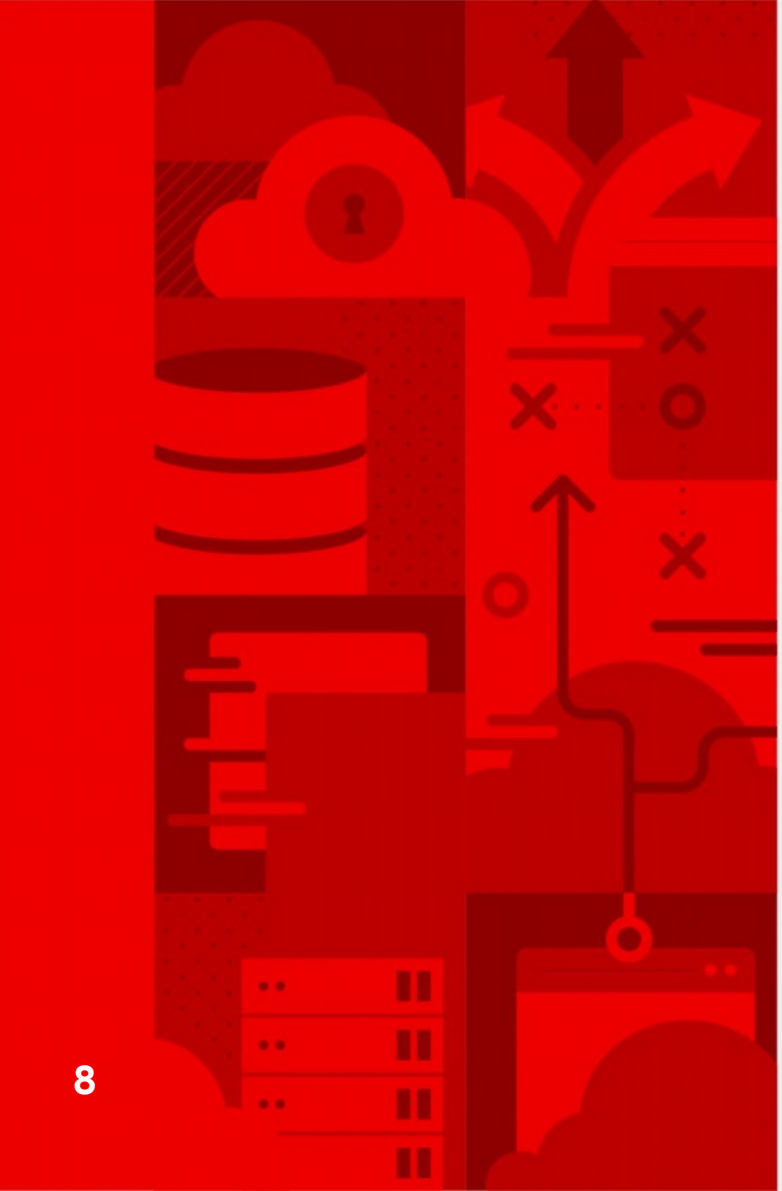
systemd-journal
rsyslog
fluentd など

tlog-rec-session

bash や zsh

tlog-rec-session は端末入出力をログ出力するよう接続した上でシェルを起動

tlog-rec-session は端末への入出力を json 形式でログへ出力



tlog で何ができるか？

Red Hat

tlog でできること

各ユーザによるセッション記録と再生

ユーザが自分のセッション内で端末操作をファイルへ記録し、再生できる。

強制的なセッション記録

あるシステムにログインしたユーザが特定のグループに所属している場合、
端末セッションをログへ記録する。(前述のとおり Gnome 環境では不可)

ログ形式へ対応

独自ファイル (JSON 形式) だけでなく、 systemd-journal と syslog 形式に対応している。ログへ記録されたセッションも通常セッションと同様に再生できる。

tlog と他のシステムを組み合わせるとできること

Red Hat Identity Management などと組み合わせる

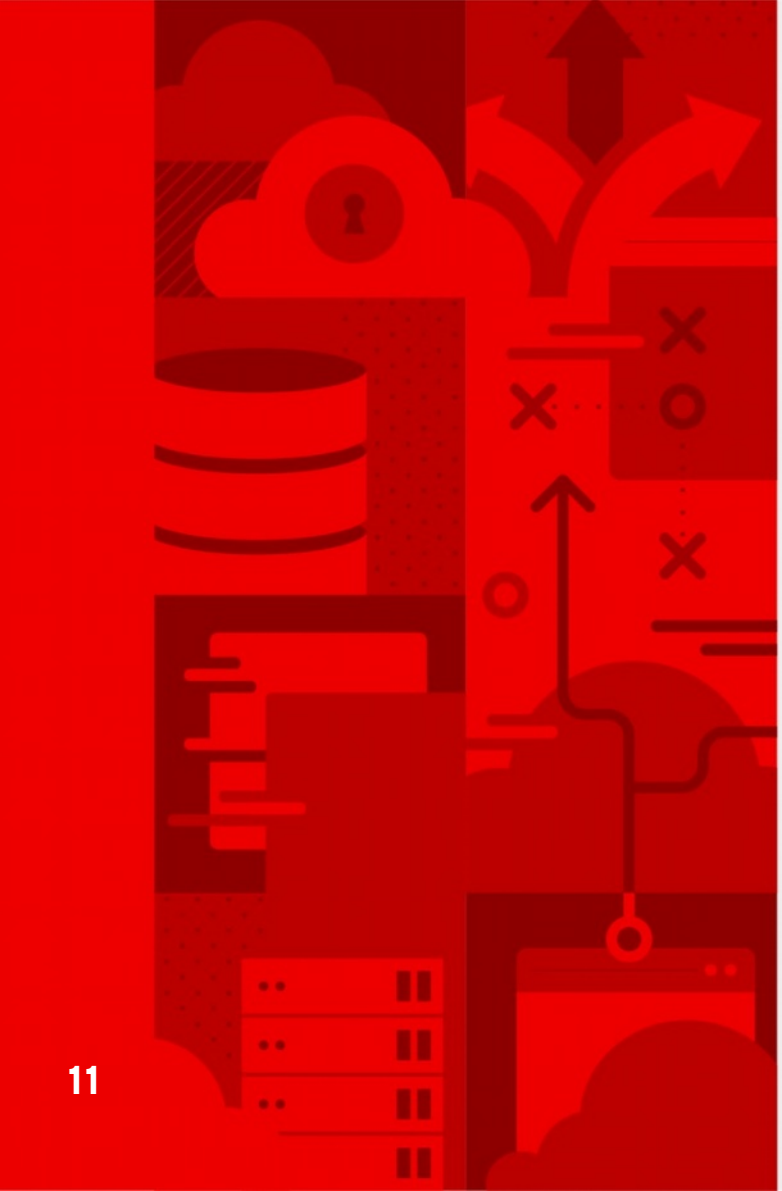
Red Hat Identity Management や LDAP サーバなどでユーザとグループを集中管理すると、誰のセッションを記録するか集中管理できる

ElasticSearch などと組みあわせる

tlog は JSON 形式でログを出力するため、 Elasticsearch などと組みあわせやすい。
各システムの tlog のログを Elasticsearch に保存できる。

Auditd と組みあわせる

従来からある auditd によるコマンド実行やファイルアクセスのログと組み合わせると見るべき範囲を絞り込みやすくなる。



tlog の使い方

インストールと初期設定

インストール

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

初期設定

セッションの強制的な記録を行う場合は最低限 SSSD の設定が必要

SSSD の設定 `/etc/sssd/conf.d/sssd-session-recording.conf`

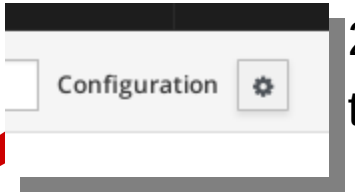
- scope=none (記録しない)/some(条件により記録する)/all(全部記録する)
- users, groups(記録対象ユーザ、グループの指定)

tlog の設定 `/etc/tlog/tlog-rec-session.conf`

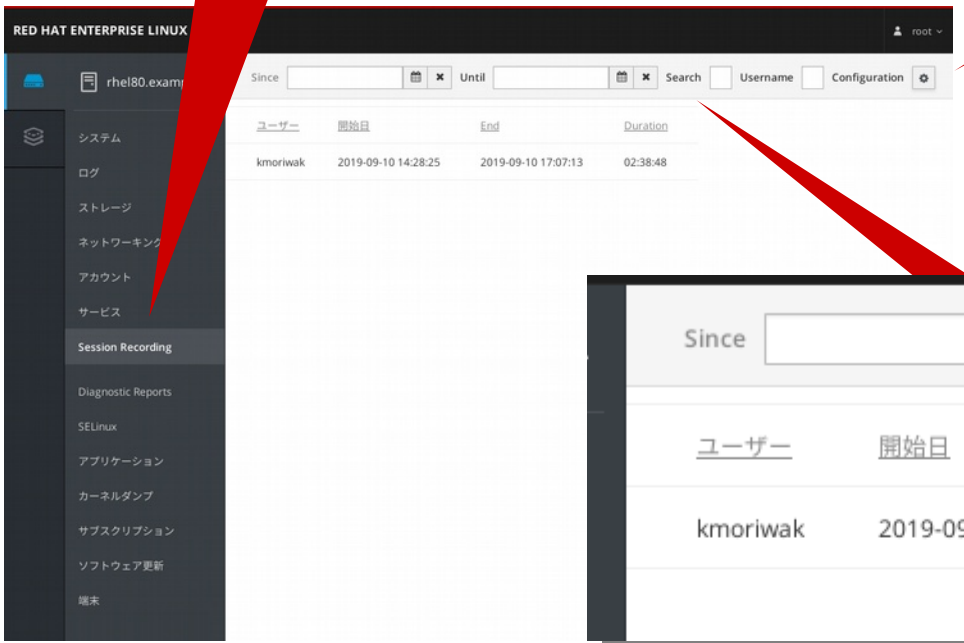
- tlog-rec-session の子プロセスとして起動する shell の種類
- ログ出力先を syslog にするか、 journal にするか、その場合の priority など

Cockpit での利用 (1/2)

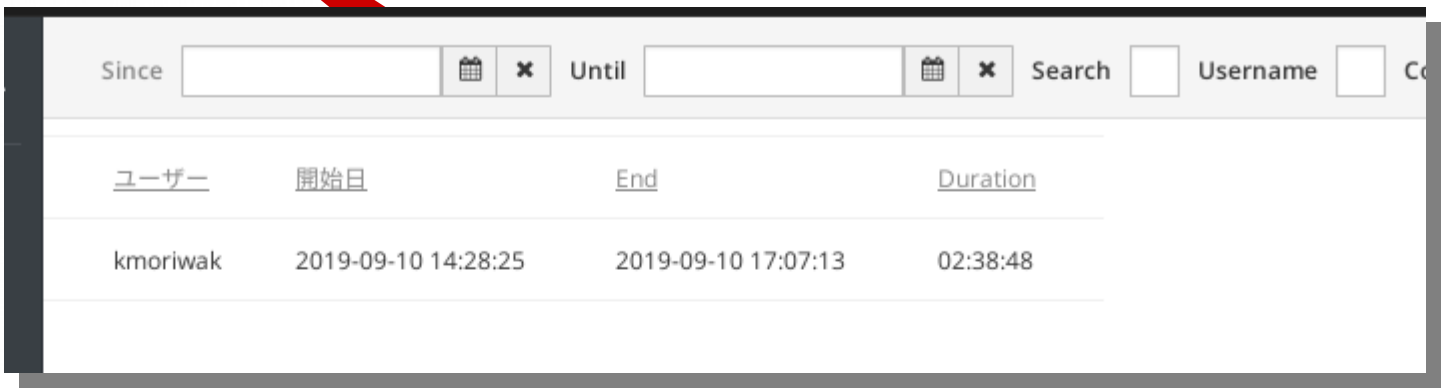
1. Session Recording を選択



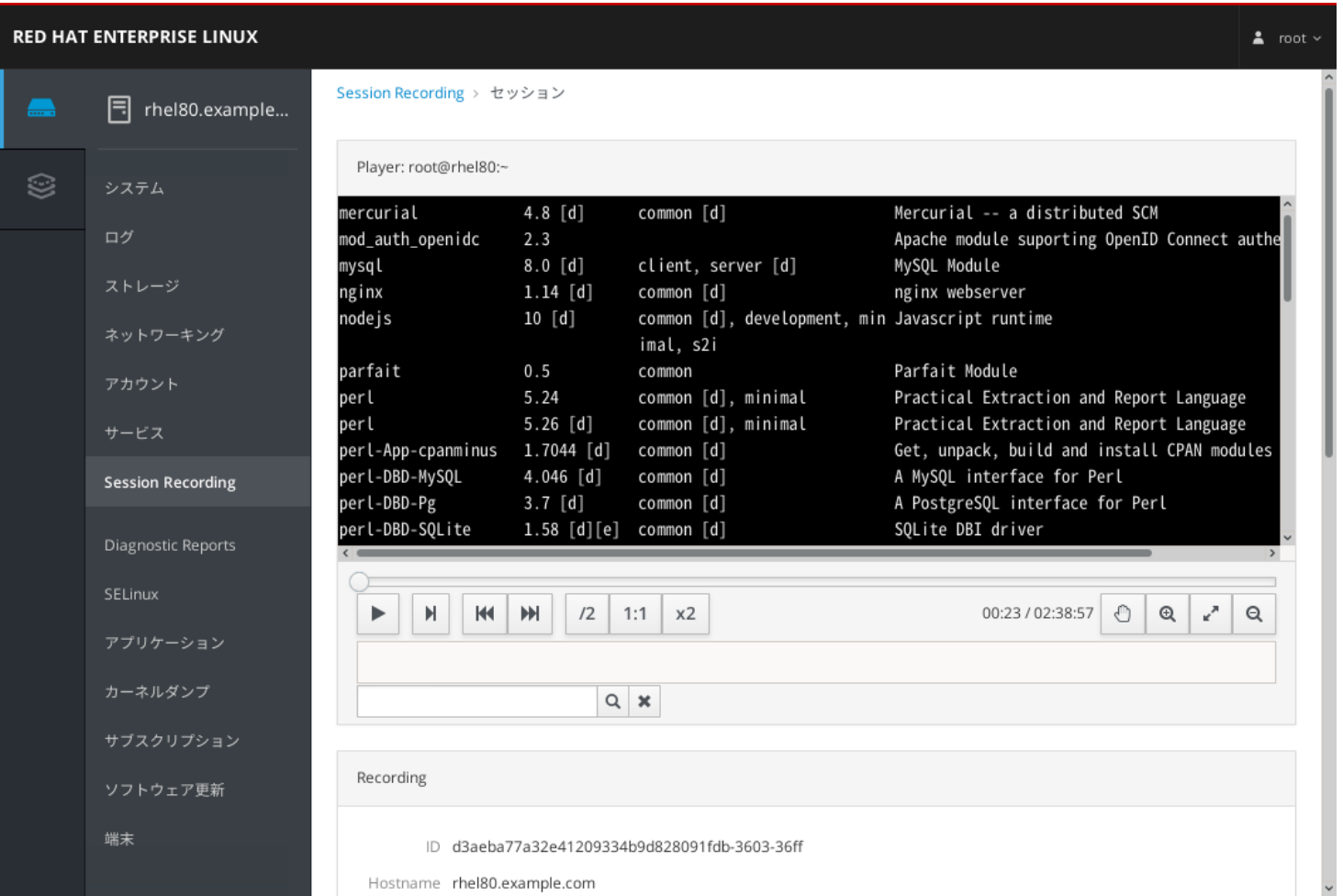
2. Configuration で tlog-rec-session 設定



3. 時刻、文字列検索、ユーザー名で絞り込み



Cockpit での利用 (2/2)



再生画面

再生、一時停止、再生速度変更、拡大縮小

ログ検索、ログのメタデータなど

Red Hat

SSSD の設定例

/etc/sssd/conf.d/sssd-session-recording.conf
例：全て記録する

```
[session_recording]
scope=all
users=
groups=
```

例：wheel グループのみ記録する

```
[session_recording]
scope=some
users=
groups=wheel
```

詳しくは man sssd-session-recording(5)

tlog-rec-session の設定例

/etc/tlog/tlog-rec-session.conf
JSON フォーマットで設定をおこないます。

例 : shell として zsh を使う

```
{
     ”shell”: “/usr/bin/zsh”
}
```

例 : ユーザ入力も保存 (パスワード打鍵なども記録されるので要注意)

```
{
     ”log”: {
          ”input”: true
     }
}
```

詳しくは man tlog-rec-session.conf(5)

journal の中から TLOG_REC をみつける

journal に保存すると TLOG_REC が大事

TLOG_REC という属性でセッション毎に一意な ID が付与される

journalctl の検索を利用して絞り込む

$ journalctl -o json-pretty --output-fields TLOG_REC 検索条件 | grep TLOG_REC | uniq

検索条件でよく使うもの

```
TLOG_USER=kmoriwak    # ユーザ名
-S -20min             # 検索範囲の開始時刻。 - で相対的な時刻を指定。
-S 2019-09-03         # 検索範囲の開始時刻。絶対的な時刻を指定。
-U -5min              # 検索範囲の終了時刻。 -S と同様。
```

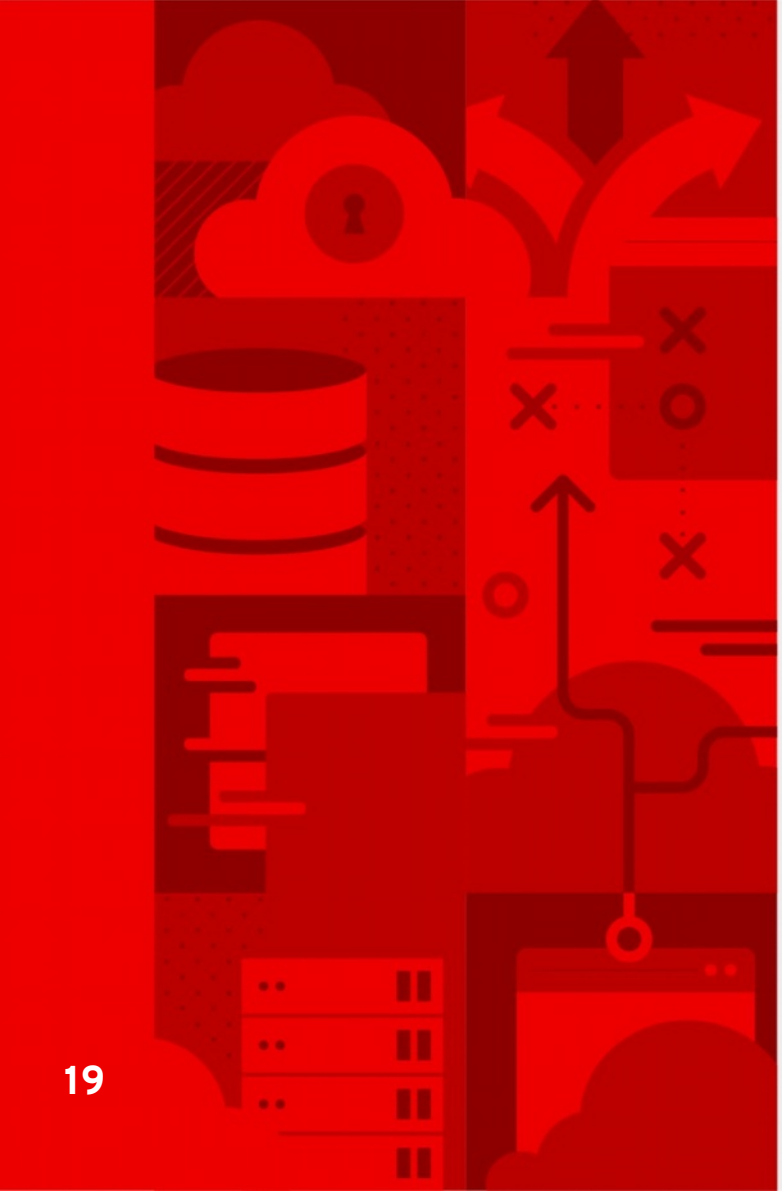
ユーザによる記録・再生

ファイルへ記録、再生する

$ tlog-rec -o foobar.txt
$ tlog-play -i foobar.txt
$ tlog-play -i foobar.txt -s 3 # 3 倍速で再生

journal へ記録、再生する

$ tlog-rec -w journal
journal 内で TLOG_REC の値をみつける
$ journalctl -o json-pretty --output-fields TLOG_REC TLOG_USER=kmoriwak | grep TLOG_REC | uniq
$ tlog-play -r journal -M TLOG_REC=e93f93c169a04cabbe90fca8a5c86b4f-9bc-1302f62



tlog 利用時の注意点

Red Hat

tlog の注意点

直前数秒の記録は失われることがあります

tlog はデフォルトで 10 秒間入出力をバッファリングします。 tlog を含めて停止するような操作は記録できない場合があります。

Gnome(GUI 全般) のセッションは記録されません

現在の tlog では Gnome や GUI 環境でのセッションは自動的に記録されません。各ユーザが tlog-rec で記録することはできます。

tlog-play では端末サイズ変更はできません

記録時と再生時の端末サイズや端末エミュレータの種類が違うと表示が崩れます。

記録していることは簡単にわかります

tlog-rec-session の子プロセスとして shell が起動されているので pstree などで容易に記録されていることがわかります。

tlog の注意点

journald はログが消えることがあります

systemd-journald は logrotate 機能を内蔵しており、設定によりストレージの残容量などの条件によって rotate された過去のログを自動的に削除します。また root 権限があれば削除することができます。監査証跡として利用したい場合にはログサーバや Elasticsearch などの外部サーバに保存します。

場合によりログ容量が予測しづらいです

たとえば root 権限で journalctl -f とすると「端末にログを表示した」ログが journal に追加されるループになり、簡単に大量のログを発生させられます。一定レート以上ではログを drop する設定も可能ですが、その場合は記録が失われるため判断が必要です。

まとめ

- Red Hat Enterprise Linux 8 ではセッション記録の機能が追加されました
- 作業記録や監査証跡などに利用できます
- 利用はかなり簡単です
- 目的により制限と考慮するべき点があります

参考情報

- 公式ドキュメント「セッションの録画」
  https://red.ht/302GAlm
- Scribery プロジェクトのページ
  http://scribery.github.io/

Thank You