목차

Session Recording tlog ... 3

- ***tlog 설치*** ... 3
- ***CLI환경에서 SSSD를 통한 유저 또는 그룹 레코딩 설정하기*** ... 3
  - 예제 ... 4

Session Recording tlog

세션 기록 솔루션은 `Red Hat Enterprise Linux 8`에서 제공되며 `tlog` 패키지를 기반으로합니다. `tlog`패키지 및 관련 웹 콘솔 세션 플레이어는 기록 할 수있는 능력 및 재생 사용자 터미널 세션을 제공합니다. SSSD 서비스를 통해 사용자 또는 사용자 그룹별로 기록되도록 구성 할 수 있습니다. 모든 터미널 입력 및 출력은 캡처되어 시스템 저널에 텍스트 기반 형식으로 저장됩니다.

이 솔루션은 보안에 민감한 시스템에서 사용자 세션을 감사하거나 보안 위반이 발생한 경우 법의학 분석의 일부로 기록 된 세션을 검토하는 데 사용할 수 있습니다. 시스템 관리자는 RHEL 8.0 시스템에서 세션 기록을 로컬로 구성 할 수 있습니다. `tlog-play`명령을 사용하여 웹 콘솔 인터페이스 또는 터미널에서 기록 된 세션을 검토 할 수 있습니다.

세션 레코딩 제한사항

- tlog는 Gnome3 그래픽 세션 터미널 내용을 기록하지 않습니다.

tlog 설치

`tlog` 설치는 단순하게 패키지 설치를 하면 완료됩니다.

```
# yum install tlog
```

웹 콘솔 패키지는 RHEL8에서 기본제공 됩니다. `cockpit-session-recording` 패키지를 설치하면 사용할 수 있습니다.

```
# yum install cockpit-session-recording

# systemctl start cockpit.socket

또는

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

CLI환경에서 SSSD를 통한 유저 또는 그룹 레코딩 설정하기

CLI환경에서 특정 유저나 그룹을 레코딩하기 위해서는 `sssd-session-recording.conf`파일을 수정하여야 합니다.

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

이 `sssd-session-recording.conf`파일은 웹 콘솔 인터페

이스에서 구성 페이지를 열면 자동으로 작성됩니다.

레코딩 대상 사용자 또는 그룹의 레코딩 범위를 지정하려면 다음을 적용합니다.

- `none` 세션을 기록하지 않습니다.
- `some` 지정된 세션 만 기록합니다.
- `all` 모든 세션을 기록합니다.

`some` 설정의 경우 대상 사용자 또는 그룹의 이름을 쉼표(,) 로 구분하여 파일에 추가하십시오.

예제

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

################################# 이어서 계속

From:
https://atl.kr/dokuwiki/ - **AllThatLinux!**

Permanent link:
https://atl.kr/dokuwiki/doku.php/session_recording_tlog?rev=1557891112

Last update: **2019/05/15 03:31**