# 목차

**Session Recording tlog** ..... 3
***tlog 설치*** ..... 3
CLI환경에서 SSSD를 통한 유저 또는 그룹 레코딩 설정하기 ..... 3
WebUI 환경에서 SSSD를 통한 유저 또는 그룹 레코딩 설정하기 ..... 4
SSSD없이 구성하기 ..... 4
기록된 내용을 내보내기 ..... 5
***기록 된 세션 재생하기*** ..... 5
웹 콘솔로 재생 ..... 6
tlog-play 로 재생 ..... 6
tlog-play로 백그라운드 기록 된 세션 재생 ..... 6
***참조링크*** ..... 7

# Session Recording tlog

세션 기록 솔루션은 Red Hat Enterprise Linux 8에서 제공되며 tlog 패키지를 기반으로합니다. tlog패키지 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-play명령을 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.conf파일을 수정하여야 합니다.

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

이 sssd-session-recording.conf파일은 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.

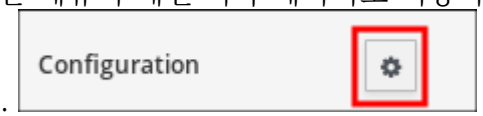
**예제**

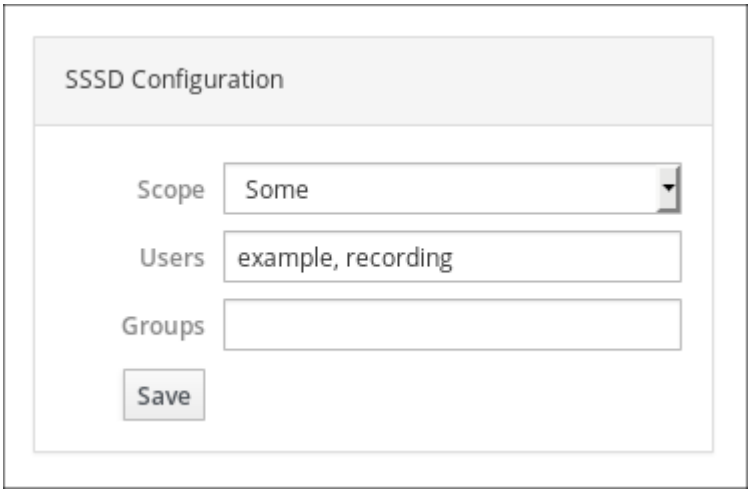
```
[session_recording]
scope = some
users = example1, example2
groups = examples
```

## WebUI 환경에서 SSSD를 통한 유저 또는 그룹 레코딩 설정하기

1. 브라우저에 localhost:9090 또는 <IP_ADDRESS>:9090를 입력하여 RHEL 8 웹 콘솔에 로컬로 연결하십시오 . 2. RHEL 8 웹 콘솔에 로그인하십시오.

사용자는 기록 된 세션을 볼 수있는 관리자 권한이 있어야합니
다.

3. 인터페이스 왼쪽에있는 메뉴의 세션 기록 페이지로 이동하십시오. 4. 오른쪽 상단 모서리에있는 톱니바퀴 버튼을 클릭합니다. 


5. SSSD 구성 테이블에서 매개 변수를 설정하십시오. 사용자 및 그룹 목록의 이름은 쉼표로 구분해야합니다. 


## SSSD없이 구성하기

이 방법은 SSSD를 사용하지 않고 쉘자체를 /usr/bin/tlog-rec-session 로 변경하여 기록하는 방법입니다.

이 방법은 사용하지 않는 것이 좋습니다. 기본 옵션은 SSSD를
통해 기록 된 사용자를 명령 줄 인터페이스에서 구성하거나
RHEL 8 웹 콘솔에서 직접 구성하는 것입니다.

사용자 쉘을 수동으로 변경하도록 선택하면, 작업 쉘을 `tlog-rec-session.conf`구성 파일에 나열된 쉘로 선택하여야 합니다.

기록 된 사용자 또는 사용자 그룹을 지정하기 위해 SSSD를 사용하지 않으려면 기록 할 사용자의 셸을 `/usr/bin/tlog-rec-session`로 직접 변경하여야 합니다.

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

### 기록된 내용을 내보내기

기록 된 세션 및 로그를 내보내고 복사 할 수 있습니다.

다음 절차는 기록 된 세션을 로컬 시스템에 내보내는 방법을 보여줍니다.

#### 전제 조건

`systemd-journal-remote` 패키지를 설치하십시오 .

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

#### 순서

다음 journalctl -o export명령을 실행하십시오 .

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

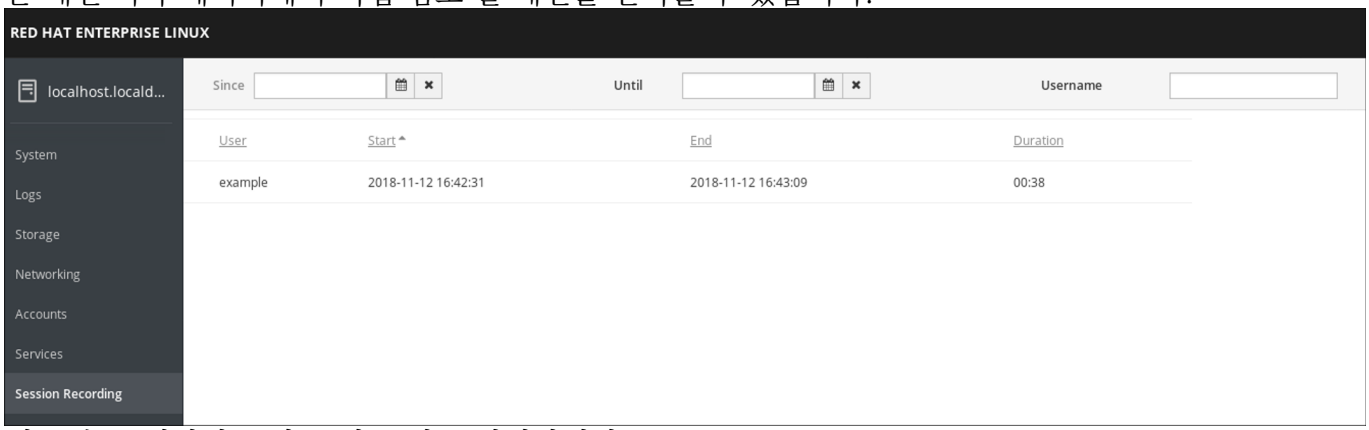
이렇게하면 모든 엔티티가있는 시스템 저널에서 내보내기 파일이 생성됩니다. `/var/log/journal/`에 내보낸 파일을 다른 호스트의 디렉토리에 복사 할 수 있습니다 . 사용자의 편의를 위해 원격 호스트에서 내보내기 파일 용 `/var/log/journal/remote/` 디렉토리를 작성할 수도 있습니다

## 기록 된 세션 재생하기

이미 녹음 된 세션을 재생하는 데는 두 가지 방법이 있습니다. 첫 번째는 `tlog-play`도구 를 사용하는 것 입니다. 두 번째 옵션은 또한으로 언급 된 RHEL 8 `cockpit` 웹 콘솔에서 녹음 세션을 관리하는 것입니다

## 웹 콘솔로 재생

RHEL 8 웹 콘솔에는 기록 된 세션을 관리하기위한 전체 인터페이스가 있습니다. 기록 된 세션 목록이있는 세션 기록 페이지에서 직접 검토 할 세션을 선택할 수 있습니다.




웹 콘솔 플레이어는 창 크기 조정을 지원합니다.

## tlog-play 로 재생

기록 된 세션을 재생할 수있는 다른 옵션은 `tlog-play`도구를 사용하는 것 입니다. 이 `tlog-play`도구는 `tlog-rec`도구로 기록 된 터미널 입력 및 출력을위한 재생 프로그램입니다. 현재 재생중인 터미널의 녹화를 재생하지만 크기를 변경할 수는 없습니다. 이러한 이유로 재생 단자는 적절한 재생을 위해 기록 된 단자 크기와 일치해야합니다. 이 `tlog-play`도구는 `/usr/local/etc/tlog/tlog-play.conf`구성 파일 에서 해당 매개 변수를로드 합니다. 매개 변수는 `tlog-play`매뉴얼 페이지에 설명 된 명령 행 옵션으로 대체 될 수 있습니다 .

## tlog-play로 백그라운드 기록 된 세션 재생

기록 된 세션은 간단한 파일이나 Systemd Journal에서 재생할 수 있습니다.

### 파일에서 재생하기

레코딩 중 및 레코딩 후 모두 파일에서 세션을 재생할 수 있습니다.

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

### 저널에서 재생하기

다음과 같이 전체 녹음을 재생할 수 있습니다.

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

자세한 지침과 설명서는 tlog-play설명서 페이지 에서 찾을 수 있습니다 .

# 참조링크

- https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/html/recording_sessions/

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

Permanent link:
**https://atl.kr/dokuwiki/doku.php/session_recording_tlog**

Last update: **2019/05/15 09:10**