Red Hat Enterprise Linux 8

레코딩 세션

Red Hat Enterprise Linux 8의 세션 기록 솔루션 사용

Last Updated: 2023-09-19

Red Hat Enterprise Linux 8 레코딩 세션

Red Hat Enterprise Linux 8의 세션 기록 솔루션 사용

법적 공지

초록

이 설명서 컬렉션은 Red Hat Enterprise Linux 8에 포함된 RHEL 웹 콘솔의 tlog를 기반으로 하는 세션 기록 솔루션을 사용하는 방법을 소개합니다.

차례

보다 포괄적 수용을 위한 오픈 소스 용어 교체 3

RED HAT 문서에 관한 피드백 제공 4

1장. RHEL에서 세션 레코드 시작하기 5
1.1. RHEL의 세션 기록 5
1.2. 세션 레코딩의 구성 요소 5
1.3. 세션 기록의 제한 사항 5

2장. RHEL 웹 콘솔에 세션 레코드 배포 7
2.1. TLOG 설치 7
2.2. COCKPIT-SESSION- RECORDING 설치 7
2.3. CLI에서 SSSD를 사용하여 사용자 및 그룹의 세션 레코딩 활성화 7
2.4. 웹 UI에서 SSSD를 사용하여 사용자 및 그룹의 세션 레코딩 활성화 8
2.5. SSSD가 없는 사용자의 세션 레코딩 활성화 9
2.6. 기록된 세션을 파일로 내보내기 10

3장. 기록된 세션 다시 플레이 11
3.1. TLOG-PLAY로 재생 11
3.2. 웹 콘솔로 재생 11
3.3. TLOG-PLAY로 기록된 세션 재생 11

4장. TLOG RHEL 시스템 역할을 사용하여 세션 레코딩을 위한 시스템 구성 13
4.1. TLOG 시스템 역할 13
4.2. TLOG 시스템 역할의 구성 요소 및 매개변수 13
4.3. TLOG RHEL 시스템 역할 배포 14
4.4. 그룹 또는 사용자 목록 제외에 대한 TLOG RHEL 시스템 역할 배포 16
4.5. CLI에서 배포된 TLOG 시스템 역할을 사용하여 세션 기록 18
4.6. CLI를 사용하여 기록된 세션 모니터링 20

보다 포괄적 수용을 위한 오픈 소스 용어 교체

Red Hat은 코드, 문서 및 웹 속성에서 문제가 있는 언어를 교체하기 위해 최선을 다하고 있습니다. 먼저 마스터(master), 슬레이브(slave), 블랙리스트(blacklist), 화이트리스트(whitelist) 등 네 가지 용어를 교체하고 있습니다. 이러한 변경 작업은 작업 범위가 크므로 향후 여러 릴리스에 걸쳐 점차 구현할 예정입니다. 자세한 내용은 CTO Chris Wright의 메시지 를 참조하십시오.

RED HAT 문서에 관한 피드백 제공

문서에 대한 피드백에 감사드립니다. 어떻게 개선할 수 있는지 알려주십시오.

특정 문구에 대한 의견 제출

1. **Multi-page HTML** 형식으로 설명서를 보고 페이지가 완전히 로드된 후 오른쪽 상단 모서리에 **피드백** 버튼이 표시되는지 확인합니다.
2. 커서를 사용하여 주석 처리할 텍스트 부분을 강조 표시합니다.
3. 강조 표시된 텍스트 옆에 표시되는 **피드백 추가** 버튼을 클릭합니다.
4. 의견을 추가하고 **제출** 을 클릭합니다.

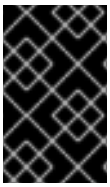
Jira를 통해 피드백 제출 (등록 필요)

1. Jira 웹 사이트에 로그인합니다.
2. 상단 탐색 모음에서 **생성** 을 클릭합니다.
3. **Summary** (요약) 필드에 설명 제목을 입력합니다.
4. **Description** (설명) 필드에 개선을 위한 제안을 입력합니다. 문서의 관련 부분에 대한 링크를 포함합니다.
5. 대화 상자 하단에서 **생성** 을 클릭합니다.

1장. RHEL에서 세션 레코드 시작하기

1.1. RHEL의 세션 기록

Red Hat Enterprise Linux 8의 세션 기록 솔루션은 **tlog** 패키지를 기반으로 합니다. **tlog** 패키지와 관련 웹 콘솔 세션 플레이어를 사용하여 사용자 터미널 세션을 기록하고 재생할 수 있습니다. SSSD 서비스를 통해 사용자 또는 사용자 그룹별로 실행되도록 레코딩을 구성할 수 있습니다. 모든 터미널 입력 및 출력은 캡처되어 시스템 저널에 텍스트 기반 형식으로 저장됩니다.



중요

원시 암호 및 기타 민감한 정보를 가로채지 않으려면 터미널 입력 기록은 기본적으로 비활성화되어 있습니다. 터미널 입력을 기록하면 입력한 모든 암호가 일반 텍스트로 캡처됩니다.

이 솔루션을 사용하여 보안에 민감한 시스템에서 사용자 세션을 감사하거나 보안 위반 시 중요한 분석의 일부로 기록된 세션을 검토할 수 있습니다. 관리자는 RHEL 8 시스템에서 로컬로 세션 레코딩을 구성할 수 있습니다. 웹 콘솔 인터페이스 또는 **tlog-play** 명령을 사용하여 터미널에서 기록된 세션을 검토할 수 있습니다.

1.2. 세션 레코딩의 구성 요소

세션 기록 솔루션에는 **tlog** 유틸리티, SSSD 서비스 및 웹 콘솔 내장 사용자 인터페이스의 세 가지 주요 구성 요소가 있습니다.

tlog

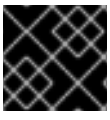
tlog 유틸리티는 터미널 입력/출력(I/O) 기록 및 재생 프로그램입니다. 사용자 터미널과 사용자 쉘 사이에 **tlog-rec-session** 툴을 삽입하고 JSON 메시지로 전달하는 모든 항목을 기록합니다.

SSSD

SSSD(System Security Services Daemon) 서비스는 원격 디렉터리 및 인증 메커니즘에 대한 액세스를 관리하는 데몬 세트를 제공합니다. 세션 레코딩을 구성할 때 SSSD를 사용하여 레코드할 사용자 또는 사용자 그룹을 지정할 수 있습니다. 명령줄 인터페이스(CLI) 또는 RHEL 8 웹 콘솔 인터페이스에서 이러한 설정을 구성할 수 있습니다.

RHEL 8 웹 콘솔 내장 인터페이스

세션 레코딩 페이지는 RHEL 8 웹 콘솔 인터페이스의 일부이며 이를 사용하여 기록된 세션을 관리할 수 있습니다.



중요

기록된 세션에 액세스하려면 관리자 권한이 필요합니다.

1.3. 세션 기록의 제한 사항

이는 세션 기록 솔루션의 가장 주목할 만한 제한 사항입니다.

- 루트 사용자는 레코딩 프로세스를 우회할 수 있기 때문에 루트 사용자의 기록은 신뢰할 수 없습니다.
- 세션 레코딩은 **GNOME 3** 그래픽 세션에 터미널을 기록하지 않습니다. 그래픽 세션에 모든 터미널에 대한 단일 감사 세션 ID가 있고 **tlog** 가 터미널을 구분할 수 없어 그래픽 세션에 터미널을 기록하는 것은 지원되지 않습니다.

- 세션 레코딩이 저널에 기록하도록 구성된 경우 기록된 사용자는 시스템 **저널** 또는 **/var/log/message 를 보는 결과를 기록하는 작업을 볼 수 있습니다**. 보기로 인해 화면에 출력되는 로그가 생성되므로 세션 레코드가 이 작업을 기록하므로 더 많은 레코드를 생성하여 플러드 출력 루프가 발생합니다.
  다음 명령을 사용하여 이 문제를 해결할 수 있습니다.

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

  출력을 제한하도록 tlog를 구성할 수도 있습니다. 자세한 내용은 **tlog-rec** 또는 **tlog-rec-session** 매뉴얼 페이지를 참조하십시오.

- 원격 액세스 명령을 실행하는 사용자를 기록하려면 대상 호스트에서 해당 사용자에 대한 세션 레코딩을 구성해야 합니다. 예를 들어 다음 원격 액세스 명령을 기록하려면 **클라이언트** 호스트에서 **admin** 사용자에 대한 세션 레코딩을 구성해야 합니다.

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

- **저널이** 기본적으로 RHEL 8에 저장되므로 모든 기록은 재부팅 시 손실됩니다. 레코딩을 내보내려면 기록된 세션을 파일로 내보내기를 참조하십시오.

2장. RHEL 웹 콘솔에 세션 레코드 배포

이 섹션에서는 Red Hat Enterprise Linux 웹 콘솔에 세션 레코드 솔루션을 배포하는 방법을 설명합니다.

세션 레코드 솔루션을 배포할 수 있으려면 다음 패키지가 설치되어 있어야 합니다.

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

2.1. TLOG 설치

tlog 패키지를 설치합니다.

절차

- 다음 명령을 사용합니다.

```
# yum install tlog
```

2.2. COCKPIT-SESSION- RECORDING 설치

기본 웹 콘솔 패키지는 기본적으로 Red Hat Enterprise Linux 8의 일부입니다. 세션 기록 솔루션을 사용하려면 **cockpit-session-** recording 패키지를 설치하고 시스템에서 웹 콘솔을 시작하거나 활성화해야 합니다.

절차

1. **cockpit-session- recording**을 설치합니다.

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

2. 시스템에서 웹 콘솔을 시작하거나 활성화합니다.

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

또는

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

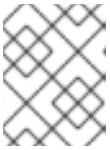
2.3. CLI에서 SSSD를 사용하여 사용자 및 그룹의 세션 레코딩 활성화

인증에 SSSD를 사용하는 경우 명령줄에서 사용자 및 그룹에 대한 세션 레코딩을 구성할 수 있습니다.

절차

- **sssd-session- recording.conf** 구성 파일을 엽니다.

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



참고

웹 콘솔 인터페이스에서 구성 페이지를 열면 **sssd-session- recordsing.conf** 파일이 자동으로 생성됩니다.

1. 세션 레코딩 범위를 지정하려면 scope 옵션에 대해 다음 값 중 하나를 입력합니다.

- **세션** 을 기록하지 않습니다.
- **일부는** 지정된 세션만 기록합니다.
- **모든** 세션을 기록합니다.

1. (선택 사항) 범위를 일부로 설정하면 사용자 및 그룹 이름이 쉼표로 구분된 목록으로 추가됩니다.

예 2.1. SSSD 구성

다음 예제 사용자 example1 및 example2 및 그룹 예제 에는 세션 레코딩이 활성화되어 있습니다.

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

2.4. 웹 UI에서 SSSD를 사용하여 사용자 및 그룹의 세션 레코딩 활성화

인증에 SSSD를 사용하는 경우 RHEL 8 웹 콘솔의 사용자 및 그룹에 대해 세션 레코딩을 구성할 수 있습니다.

절차

1. **localhost:9090** 을 입력하거나 **IP** 주소 **< IP_ADDRESS >:9090**을 브라우저에 입력하여 **RHEL 8** 웹 콘솔에 로컬로 연결합니다.

2. **RHEL 8** 웹 콘솔에 로그인합니다.

중요

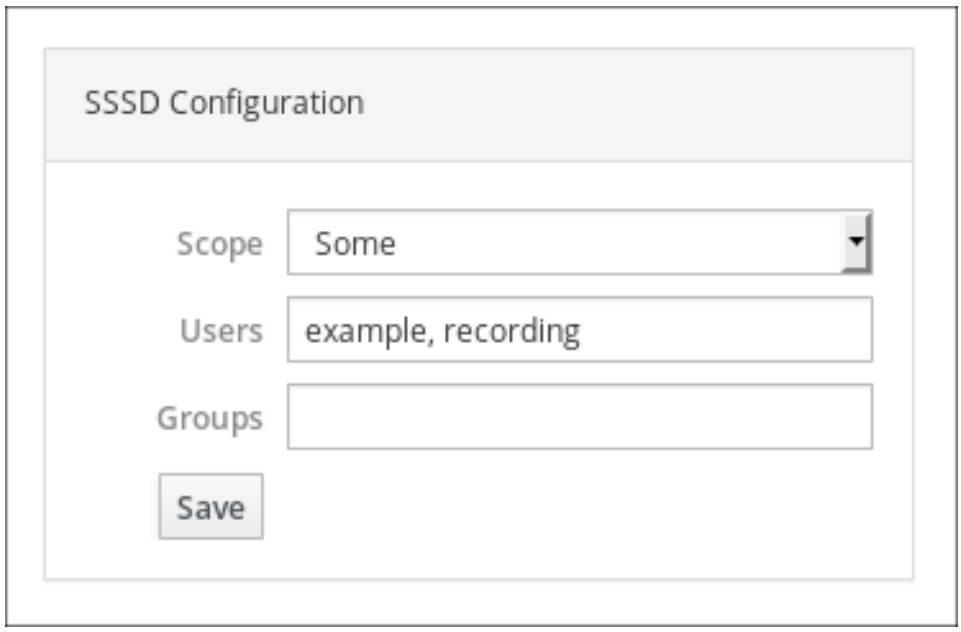
사용자는 기록된 세션을 볼 수 있는 관리자 권한이 있어야 합니다.

3. 왼쪽 메뉴에 있는 세션 레코드 페이지로 이동합니다.

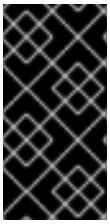
4. 오른쪽 상단 모서리에서 톱니바를 클릭합니다.

5. **SSSD** 구성 테이블에 매개 변수를 설정합니다. 사용자 및 그룹 목록을 쉼표로 구분합니다.

예 2.2. SSSD를 사용하여 기록된 사용자 설정



2.5. SSSD가 없는 사용자의 세션 레코딩 활성화



중요

Red Hat은 이 옵션을 권장하지 않습니다. 기본 옵션은 **SSSD**를 명령줄 인터페이스 또는 **RHEL 8** 웹 콘솔에서 직접 통해 기록된 사용자를 구성하는 것입니다.

사용자의 쉘을 수동으로 변경하도록 선택하면 **tlog-rec-session.conf** 구성 파일에 나열된 쉘이 있습니다.

기록된 사용자 또는 사용자 그룹을 지정하는 데 **SSSD**를 사용하지 않으려면 기록하려는 사용자의 쉘을 **/usr/bin/tlog-rec-session** 로 직접 변경할 수 있습니다.

1. 셸을 변경합니다.

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

2.6. 기록된 세션을 파일로 내보내기

기록된 세션과 해당 로그를 내보내고 복사할 수 있습니다.

다음 절차에서는 로컬 시스템에서 기록된 세션을 내보내는 방법을 보여줍니다.

사전 요구 사항

- systemd-journal-remote 패키지를 설치합니다.

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

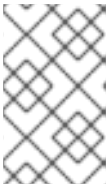
절차

1. '/tmp/dir과 같이 내보낸 레코딩 세션을 저장할 디렉토리를 만듭니다.

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

2. journalctl -o export 명령을 실행하여 tlog 기록과 관련된 시스템 저널 항목을 내보냅니다.

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



참고

comM =tlog-rec-sessio COMM 이름은 15 문자 제한으로 인해 단축됩니다.

3장. 기록된 세션 다시 플레이

기록된 세션을 재생하는 방법에는 두 가지가 있습니다.

- **tlog-play** 툴
- **RHEL 8** 웹 콘솔도 ***Cockpit*** 라고도 합니다.

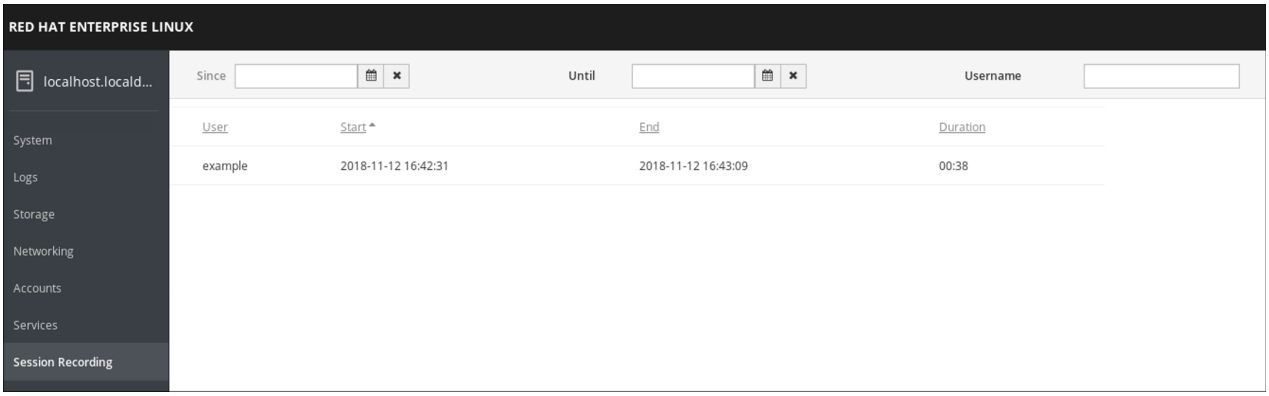
3.1. TLOG-PLAY로 재생

tlog-play 도구를 사용하여 터미널에서 세션 레코딩을 재생할 수 있습니다. **tlog-play** 도구는 **tlog-rec** 도구로 기록 된 터미널 입력 및 출력을 위한 재생 프로그램입니다. 이 명령은 사용 중인 터미널의 기록을 재현하지만 크기를 변경할 수는 없습니다. 이러한 이유로 재생 터미널은 적절한 재생을 위해 기록된 터미널 크기와 일치해야 합니다. **tlog-play** 툴은 **/etc/tlog/tlog-play.conf** 구성 파일에서 해당 매개변수를 로드합니다. **tlog-play** 도움말 페이지에 설명된 명령행 옵션을 사용하여 이러한 매개변수를 재정의할 수 있습니다.

3.2. 웹 콘솔로 재생

RHEL 8 웹 콘솔에는 기록된 세션을 관리하기 위한 전체 인터페이스가 있습니다. 세션 레코드 페이지에서 직접 검토할 세션을 선택할 수 있습니다.

예 3.1. 기록된 세션 목록 예



웹 콘솔 플레이어는 창 크기 조정을 지원합니다.

3.3. TLOG-PLAY로 기록된 세션 재생

내보낸 로그 파일 또는 Systemd journal에서 세션 레코딩을 재생할 수 있습니다.

파일에서 다시 실행

기록 중 및 기록 후 파일에서 세션을 다시 재생할 수 있습니다.

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

journal에서 돌아가기

일반적으로 -M 또는 --journal-match,-S 또는 --journal-since, -U 또는 --journal-until 옵션과 함께 journal 일치 및 타임 스탬프 제한을 사용하여 재생을 위해 저널 로그 항목을 선택할 수 있습니다.

그러나 실제로는 journal에서의 재생은 일반적으로 TLOG_REC journal 필드와 일치하는 단일 일치로 수행됩니다. TLOG_REC 필드에는 기록된 JSON 데이터의 rec 필드 사본이 포함되어 있으며, 이는 기록의 호스트 고유 ID입니다.

TLOG_REC 필드 값에서 직접 또는 JSON rec 필드의 MESSAGE 필드에서 ID를 가져올 수 있습니다. 두 필드 모두 tlog-rec-session 툴에서 발생하는 로그 메시지의 일부입니다.

절차

1. 다음과 같이 전체 녹화를 재생할 수 있습니다:

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

tlog-play 매뉴얼 페이지에서 추가 지침 및 문서를 찾을 수 있습니다.

4장. TLOG RHEL 시스템 역할을 사용하여 세션 레코딩을 위한 시스템 구성

tlog RHEL 시스템 역할을 사용하면 Red Hat Ansible Automation Platform을 사용하여 RHEL에서 터미널 세션 레코딩을 위해 시스템을 구성할 수 있습니다.

4.1. TLOG 시스템 역할

tlog RHEL 시스템 역할을 사용하여 RHEL에서 터미널 세션 레코딩을 위해 RHEL 시스템을 구성할 수 있습니다.

SSSD 서비스를 통해 사용자 또는 사용자 그룹별로 기록이 수행되도록 구성할 수 있습니다.

추가 리소스

- RHEL의 세션 기록에 대한 자세한 내용은 기록 세션 을 참조하십시오.

4.2. TLOG 시스템 역할의 구성 요소 및 매개변수

세션 레코드 솔루션에는 다음과 같은 구성 요소가 있습니다.

- tlog 유틸리티
- SSSD(System Security Services Daemon)
- 선택 사항: 웹 콘솔 인터페이스

tlog RHEL 시스템 역할에 사용되는 매개변수는 다음과 같습니다.

역할 변수	설명
tlog_use_sssd (default: yes)	기록된 사용자 또는 그룹을 관리하는 기본 방법인 SSSD를 사용하여 세션 레코딩 구성
tlog_scope_sssd (default: none)	SSSD 레코딩 범위 설정 - 모든 / 일부 / none

역할 변수	설명
tlog_users_sssd (default: [])	생성할 YAML 사용자 목록
tlog_groups_sssd (default: [])	기록할 그룹의 YAML 목록

- **tlog에 사용된 매개변수 및 tlog 시스템 역할에 대한 자세한 내용은 /usr/share/ansible/roles/rhel-system-roles.tlog/README.md 파일을 참조하십시오.**

4.3. TLOG RHEL 시스템 역할 배포

다음 단계에 따라 Ansible 플레이북을 준비하고 적용하여 세션 기록 데이터를 systemd 저널에 기록하도록 RHEL 시스템을 구성합니다.

사전 요구 사항

- **제어 노드에서 tlog 시스템 역할이 구성될 대상 시스템으로 액세스하기 위한 SSH 키를 설정해야 합니다.**
- **tlog 시스템 역할을 구성하려는 시스템이 하나 이상 있습니다.**
- **Ansible Core 패키지는 제어 시스템에 설치됩니다.**
- **rhel-system-roles 패키지는 제어 시스템에 설치됩니다.**

절차

1. **다음 내용으로 새 *playbook.yml* 파일을 생성합니다.**

```
---
- name: Deploy session recording
  hosts: all
  vars:
    tlog_scope_sssd: some
    tlog_users_sssd:
      - recorded-user
```

```
roles:
  - rhel-system-roles.tlog
```

여기서,

- **tlog_scope_sssd:**
  - 일부는 일부 또는 **none** 이 아닌 특정 사용자와 그룹만 기록하려는 경우 도 있습니다.
- **tlog_users_sssd:**
  - **recorded-user** 는 세션을 기록할 사용자를 지정합니다. 이 경우 사용자를 추가하지 않습니다. 사용자를 직접 설정해야 합니다.

2. 필요한 경우 플레이북 구문을 확인합니다.

```
# ansible-playbook --syntax-check playbook.yml
```

3. 인벤토리 파일에서 플레이북을 실행합니다.

```
# ansible-playbook -i IP_Address /path/to/file/playbook.yml -v
```

결과적으로 **Playbook**은 사용자가 지정한 시스템에 **tlog RHEL** 시스템 역할을 설치합니다. 역할에는 사용자의 로그인 쉘 역할을 하는 터미널 세션 **I/O** 로깅 프로그램인 **tlog-rec-session** 이 포함됩니다. 또한 사용자가 정의한 사용자 및 그룹에서 사용할 수 있는 **SSSD** 구성 드롭 파일을 생성합니다. **SSSD**는 이러한 사용자 및 그룹을 구문 분석하고 읽고 사용자 쉘을 **tlog-rec-session** 으로 교체합니다. 또한 **cockpit** 패키지가 시스템에 설치된 경우 **Playbook**은 웹 콘솔 인터페이스에서 레코딩을 보고 재생할 수 있는 **Cockpit** 모듈인 **cockpit-session- recording** 패키지도 설치합니다.

검증 단계

SSSD 구성 드롭 파일이 시스템에서 생성되었는지 확인하려면 다음 단계를 수행하십시오.

1. **SSSD** 구성 드롭 파일이 생성된 폴더로 이동합니다.

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

2. 파일 내용을 확인합니다.

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

파일에 플레이북에서 설정한 매개변수가 포함되어 있음을 확인할 수 있습니다.

4.4. 그룹 또는 사용자 목록 제외에 대한 TLOG RHEL 시스템 역할 배포

tlog 시스템 역할을 사용하여 **exclude_users** 및 **exclude_groups** 의 **SSSD** 세션 레코딩 구성 옵션을 지원할 수 있습니다. 다음 단계에 따라 사용자 또는 그룹을 기록하고 **systemd** 저널에 로그인하지 못하도록 **RHEL** 시스템을 구성하고 적용하도록 **Ansible** 플레이북을 준비하고 적용합니다.

사전 요구 사항

- 제어 노드에서 **tlog** 시스템 역할을 구성하려는 대상 시스템으로 액세스하기 위한 **SSH** 키를 설정해야 합니다.
- **tlog** 시스템 역할을 구성하려는 시스템이 하나 이상 있습니다.
- **Ansible Core** 패키지는 제어 시스템에 설치됩니다.
- **rhel-system-roles** 패키지는 제어 시스템에 설치됩니다.

절차

1. 다음 내용으로 새 ***playbook.yml*** 파일을 생성합니다.

```
---
- name: Deploy session recording excluding users and groups
  hosts: all
  vars:
    tlog_scope_sssd: all
    tlog_exclude_users_sssd:
      - jeff
      - james
    tlog_exclude_groups_sssd:
```

```
    - admins

  roles:
    - rhel-system-roles.tlog
```

여기서,

- **tlog_scope_sssd:**
  - **all :** 모든 사용자 및 그룹을 기록하도록 지정합니다.
- **tlog_exclude_users_sssd:**
  - 사용자 이름**:** 세션 기록에서 제외하려는 사용자의 사용자 이름을 지정합니다.
- **tlog_exclude_groups_sssd:**
  - **admins** 는 세션 레코딩에서 제외할 그룹을 지정합니다.

2. 필요한 경우 플레이북 구문을 확인합니다.

```
# ansible-playbook --syntax-check playbook.yml
```

3. 인벤토리 파일에서 플레이북을 실행합니다.

```
# ansible-playbook -i IP_Address /path/to/file/playbook.yml -v
```

결과적으로 **Playbook**은 사용자가 지정한 시스템에 **tlog RHEL** 시스템 역할을 설치합니다. 역할에는 사용자의 로그인 쉘 역할을 하는 터미널 세션 **I/O** 로깅 프로그램인 **tlog-rec-session** 이 포함됩니다. 또한 제외된 것으로 정의된 것을 제외하고 사용자와 그룹에서 사용할 수 있는 **/etc/sssd/conf.d/sssd-session-recordeding.conf SSSD** 구성 드롭 파일을 생성합니다. **SSSD**는 이러한 사용자 및 그룹을 구문 분석하고 읽고 사용자 쉘을 **tlog-rec-session** 으로 교체합니다. 또한 **cockpit** 패키지가 시스템에 설치된 경우 플레이북은 웹 콘솔 인터페이스에서 레코딩을 보고 재생할 수 있는 **Cockpit** 모듈인 **cockpit-session-Recording** 패키지도 설치합니다.

검증 단계

SSSD 구성 드롭 파일이 시스템에서 생성되었는지 확인하려면 다음 단계를 수행하십시오.

1. SSSD 구성 드롭 파일이 생성된 폴더로 이동합니다.

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

2. 파일 내용을 확인합니다.

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

파일에 플레이북에서 설정한 매개변수가 포함되어 있음을 확인할 수 있습니다.

추가 리소스

- /usr/share/doc/rhel-system-roles/tlog/ 및 /usr/share/ansible/roles/rhel-system-roles.tlog/ 디렉터리를 참조하십시오.
- CLI에서 배포된 터미널 세션 기록 시스템 역할을 사용하여 세션을 기록합니다.

4.5. CLI에서 배포된 TLOG 시스템 역할을 사용하여 세션 기록

지정한 시스템에 tlog 시스템 역할을 배포한 후 CLI(명령줄 인터페이스)를 사용하여 사용자 터미널 세션을 기록할 수 있습니다.

사전 요구 사항

- tlog 시스템 역할을 대상 시스템에 배포했습니다.
- SSSD 구성 드롭 파일이 /etc/sssd/conf.d 디렉토리에 생성되었습니다. 터미널 세션 기록 RHEL 시스템 역할 배포를 참조하십시오.

절차

1. 사용자를 생성하고 이 사용자의 암호를 할당합니다.

```
# useradd recorded-user
# passwd recorded-user
```

2. 방금 만든 사용자로 시스템에 로그인합니다.

```
# ssh recorded-user@localhost
```

3. 시스템이 **yes** 또는 **no**를 입력하여 인증할 것인지 묻는 메시지가 표시되면 **"yes"**를 입력합니다.

4. ***recorded-user***의 암호를 삽입합니다.

시스템은 기록되고 있는 세션에 대한 메시지를 표시합니다.

```
ATTENTION! Your session is being recorded!
```

5. 세션 레코딩을 완료한 후 다음을 입력합니다.

```
# exit
```

시스템은 사용자가 로그아웃한 후 **localhost**와의 연결을 종료합니다.

결과적으로 사용자 세션이 기록되고 저장되고 저널을 사용하여 재생할 수 있습니다.

검증 단계

저널에서 기록된 세션을 보려면 다음 단계를 수행합니다.

1. 아래 명령을 실행하십시오.

```
# journalctl -o verbose -r
```

2. **tlog-rec** 기록된 저널 항목의 **MESSAGE** 필드를 검색합니다.

```
# journalctl -xel _EXE=/usr/bin/tlog-rec-session
```

4.6. CLI를 사용하여 기록된 세션 모니터링

CLI(명령줄 인터페이스)를 사용하여 저널에서 사용자 세션 레코딩을 재생할 수 있습니다.

사전 요구 사항

- 사용자 세션을 기록했습니다. CLI에서 배포된 tlog 시스템 역할을 사용하여 세션 기록을 참조하십시오.

절차

1. CLI 터미널에서 사용자 세션 레코딩을 재생합니다.

```
# journalctl -o verbose -r
```

2. tlog 레코딩을 검색합니다.

```
$ /tlog-rec
```

다음과 같은 세부 정보를 볼 수 있습니다.

- 사용자 세션 기록의 사용자 이름입니다.
- out_txt 필드, 기록된 세션의 원시 출력 인코딩
- 식별자 번호 TLOG_REC=*ID_number*

3. 식별자 번호 TLOG_REC=*ID_number* 를 복사합니다.

4. TLOG_REC=*ID_number* 를 사용하여 레코딩을 재생합니다.

```
# tlog-play -r journal -M TLOG_REC=ID_number
```

결과적으로 재생되는 사용자 세션 기록 터미널 출력을 볼 수 있습니다.