Red Hat Enterprise Linux 8

记录会话

在 Red Hat Enterprise Linux 8 中使用 Session Recording

Last Updated: 2021-06-07

Red Hat Enterprise Linux 8 记录会话

在 Red Hat Enterprise Linux 8 中使用 Session Recording

法律通告

摘要

本文档集合提供了在 Red Hat Enterprise Linux 8 中使用基于 RHEL web 控制台的 tlog 的 Session Recording 解决方案的信息。

目录

使开源包含更多

红帽承诺替换我们的代码、文档和网页属性中存在问题的语言。我们从这四个术语开始： master、slave、blacklist 和 whitelist。这些更改将在即将发行的几个发行本中逐渐实施。如需了解更多详细信息，请参阅 CTO Chris Wright 信息。

对红帽文档提供反馈

我们感谢您对文档提供反馈信息。请让我们了解如何改进文档。要做到这一点：

- 关于特定内容的简单评论：
  1. 请确定您使用 *Multi-page HTML* 格式查看文档。另外，确定 **Feedback** 按钮出现在文档页的右上方。
  2. 用鼠标指针高亮显示您想评论的文本部分。
  3. 点在高亮文本上弹出的 **Add Feedback**。
  4. 按照显示的步骤操作。
- 要提交更复杂的反馈，请创建一个 Bugzilla ticket：
  1. 进入 Bugzilla 网站。
  2. 在 Component 中选择 **Documentation**。
  3. 在 **Description** 中输入您要提供的信息。包括文档相关部分的链接。
  4. 点 **Submit Bug**。

第 1 章 RHEL 的 SESSION RECORDING 入门

1.1. RHEL 的 SESSION RECORDING（会话记录）

本节介绍了 Session Recording 解决方案及其目的。

Session Recording 的解决方案在 Red Hat Enterprise Linux 8 中提供,它基于 **tlog** 软件包。**tlog** 软件包及其关联的 Web 控制台会话播放器为您提供了记录和回放用户终端会话的能力。您可以将记录配置为通过 SSSD 服务为每个用户或用户组进行。所有终端输入和输出都会捕获并保存在系统日志中基于文本的格式。

重要

默认关闭终端输入记录，使其不会截获原始密码和其他敏感信息。请注意，如果您在终端输入中启用了记录功能，所有输入的密码都会以明文显示。

这个功能可用于审核对安全敏感系统的用户会话，或者在出现安全问题时，检查记录的会话作为分析的一部分。系统管理员可以在 RHEL 8 系统中本地配置会话记录。您可以使用 **tlog-play** 命令从 web 控制台界面或终端查看记录的会话。

1.2. 会话记录的内容

Session Recording 解决方案包括三个主要组件。**tlog** 工具、SSSD 服务以及 Web 控制台嵌入的用户界面。

tlog

tlog 工具是一个终端输入/输出(I/O)记录和回放程序。它会在用户终端和用户 shell 间插入其自身（特别是 **tlog-rec-session** 工具）,并记录作为 JSON 信息传递的所有内容。

SSSD

系统安全性服务守护进程（SSSD）服务提供一组管理远程目录访问和验证机制的守护进程。配置会话记录时，您可以使用 SSSD 指定哪些用户或用户组应该 tlog 记录。这可以通过命令行界面（CLI）或者 RHEL 8 web 控制台界面完成。

RHEL 8 web 控制台嵌入的界面

Session Recording 页面是 RHEL 8 web 控制台界面的一部分。内嵌的 Session Recording 的 web 控制台界面可让您管理记录的会话。

重要

您必须具有管理员特权才能访问记录的会话。

1.3. 会话记录的限制

在本节中，我们将列出 Session Recording 解决方案中最重要的限制。

- 请注意, **tlog** 没有记录 **Gnome 3** 图形会话中的终端。不支持在图形会话中记录终端,因为图形会话具有所有终端的单一审计会话 ID, **tlog** 无法区分不同的终端并防止重复记录。

- 当将 tlog 记录配置为记录到 **journal/syslog** 目录时,记录的用户会看到查看系统日志或 **/var/log/messages** 的操作结果。因为查看会生成日志，然后再在屏幕中打印，从而导致 Session Recording 记录这个动作。这会产生更多记录，并导致大量的输出。
  您可以使用以下命令来解决这个问题：

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

  您还可以配置 tlog 来限制输出。详情请查看'tlog-rec' 或 **tlog-rec-session** 手册页。

第 2 章 在 RHEL 上部署会话记录

这部分讨论如何在 Red Hat Enterprise Linux 系统中部署会话记录解决方案。

先决条件

为了部署 Session Recording 的解决方案,您需要安装以下软件包： **tlog**、SSSD、 **cockpit-session-recording**。

2.1. 安装 TLOG

安装 **tlog** 软件包。

流程

- 使用以下命令：

```
# yum install tlog
```

2.2. 安装 COCKPIT-SESSION-RECORDING

基本 web 控制台软件包是 Red Hat Enterprise Linux 8 的一部分。为了可以使用 Session Recording 解决方案,您必须安装 **cockpit-session-recording** 软件包并在系统中启动或启用 Web 控制台：

流程

1. 安装 **cockpit-session-recording**。

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

2. 在系统中启动或启用 Web 控制台：

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

或者

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

当您安装了所有必要的软件包后，您可以继续配置您的记录参数。

2.3. 通过 CLI 配置记录的用户或用户组

如果您选择使用 SSSD 管理记录的用户或用户组（推荐的选项），则会保留每个用户的原始 shell。

流程

1. 要指定您要从命令行界面(CLI)记录的用户或用户组,修改 **sssd-session-recording.conf** 配置文件：

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

注意

在 web 控制台界面中打开配置页面后会自动创建 **sssd-session-recording.conf** 文件。

2. 指定记录的用户或用户组的范围，可以输入：
   - **none** 不记录任何会话。
   - **some** 仅记录指定会话。
   - **all** 记录所有会话。
3. 如果您选择 **some** 作为记录的用户或组群的范围,请在该文件中添加用逗号分开的名称。

例 2.1. SSSD 配置

在以下示例中,用户 **example1** 和 **example2**,组 **examples** 启用了会话记录。

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

2.4. 使用 WEB UI 配置记录的用户或用户组

使用 SSSD 指定已记录的用户或用户组的第二个方法是直接在 RHEL 8 web 控制台中列出他们。

流程

1. 通过在浏览器中输入 **localhost:9090** 或您的 IP 地址 **<IP_ADDRESS>:9090** 连接到本地 RHEL 8 web 控制台。
2. 登录到 RHEL 8 web 控制台。

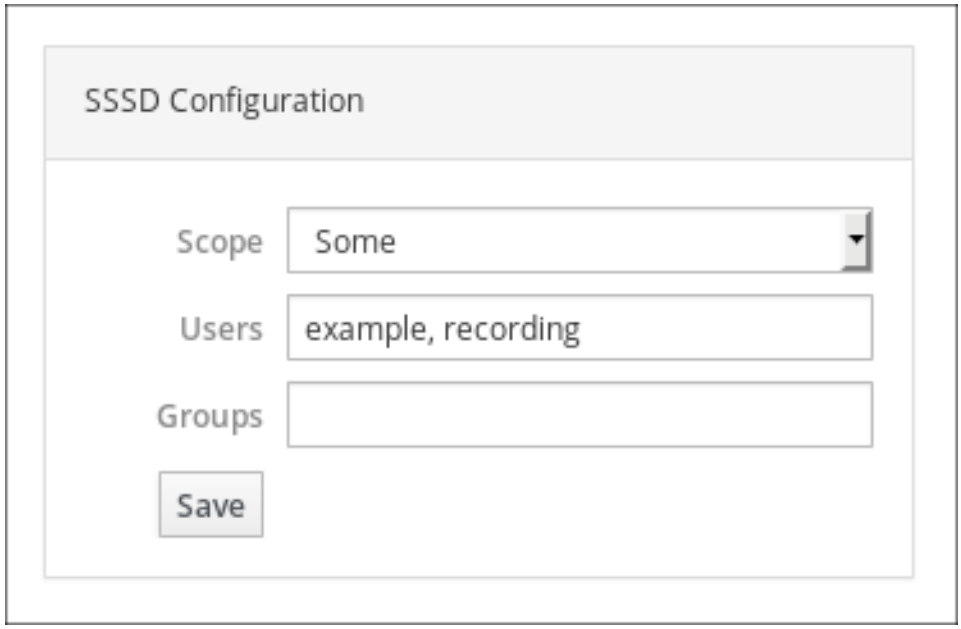
重要

您的用户必须具有管理员特权才能查看记录的会话。

3. 进入界面左侧菜单中的 Session Recording 页面。
4. 点右上角的 gear 按钮。

5. 在 SSSD 配置表中设置您的参数。用户和组群列表中的名称应该用逗号分开。

例 2.2. 配置带有 SSSD 的日志记录用户



2.5. 配置没有 SSSD 记录的用户或用户组

重要

请注意，我们不推荐使用这个方法。首选的方法是，使用 SSSD 从命令行界面或直接从 RHEL 8 web 控制台配置您的记录的用户。

如果选择手工更改用户的 shell,它们的工作 shell 将是 **tlog-rec-session.conf** 配置文件中列出的 shell。

如果您不想使用 SSSD 指定记录的用户或用户组,可以直接将您要记录的用户 shell 改为 **/usr/bin/tlog-rec-session**:

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

2.6. 将记录的会话导出到一个文件

您可以导出记录的会话及其日志并复制它们。

以下步骤演示了如何导出本地系统中记录的会话。

先决条件

安装 **systemd-journal-remote** 软件包。

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

流程

1. 创建 **/tmp/dir** 目录：

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

2. 运行 **journalctl -o export** 命令：

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

这会从系统日志及其所有实体创建一个导出文件。然后您可以将导出的文件复制到其它主机上的 **/var/log/journal/** 目录中。为方便起见,您还可以为来自远程主机导出文件创建 **/var/log/journal/remote/** 目录。

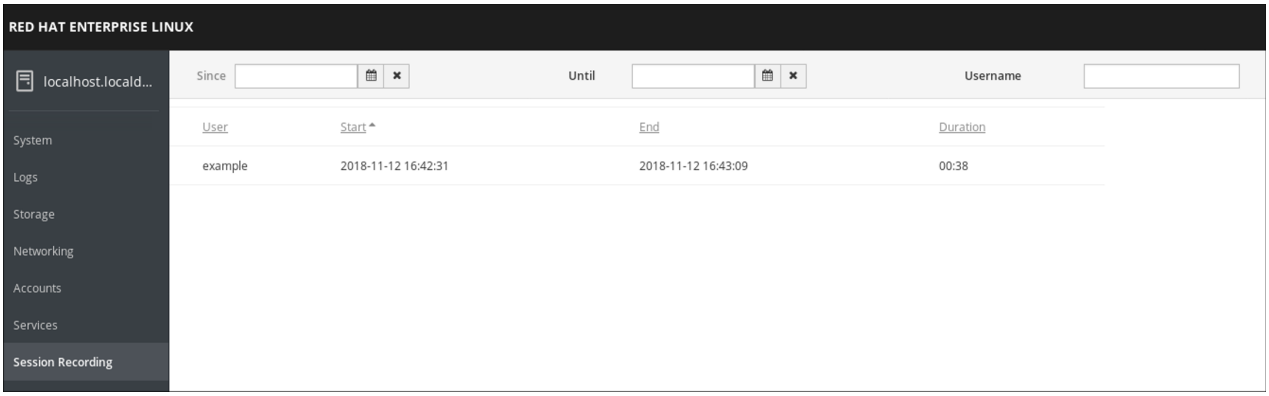
第 3 章 回放记录的会话

可以使用两种方式回放记录会话。第一个是使用 **tlog-play** 工具。第二个是从 RHEL 8 web 控制台（也称 *Cockpit*）管理您记录的会话。

3.1. 使用 WEB 控制台回放

RHEL 8 web 控制台有一个管理记录的会话的完整界面。您可以从 Session Recording 页中选择想直接查看会话。记录的会话列表包括在这个页中。

例 3.1. 记录会话列表示例



Web 控制台播放器支持重新定义窗口大小。

3.2. 使用回放 TLOG-PLAY

另一个方法是,使用 **tlog-play** 工具。**tlog-play** 工具是用于使用 **tlog-rec** 工具记录的终端输入和输出的回放程序。它复制了正在运行的终端的记录，但不能改变它的大小。因此，回放终端需要与记录的终端大小匹配才能正确回放。**tlog-play** 工具从 **/etc/tlog/tlog-play.conf** 配置文件加载其参数。这些参数可使用 **tlog-play** 手册页中描述的命令行选项覆盖。

3.3. 使用返回记录的会话 TLOG-PLAY

记录的会话可以从一个简单文件或系统日志返回。

从一个文件进行回放

您可以在记录期间和记录后，从一个文件重新播放一个会话：

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

从日志回放

通常,您可以使用 Journal 匹配和时间戳限制为回放选择 Journal 日志条目,并包含 **-M** 或 **--journal-match**、**-S** 或 **--journal-since**,以及 **-U** 或 **--journal-until** 选项。

然而,从 Journal 进行的回放通常会针对 **TLOG_REC** Journal 字段进行匹配。**TLOG_REC** 字段包含来自日志 JSON 数据的 **rec** 字段的副本,这是记录的主机唯一 ID。

您可以直接从 **TLOG_REC** 字段值获取 ID,或通过 JSON **rec** 字段中的 **MESSAGE** 字段获取 ID。这两个字段都是来自 **tlog-rec-session** 工具的日志消息的一部分。

流程

1. 您可以按以下方法回放整个记录：

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

您可以在 **tlog-play** 手册页中找到更多说明和文档。

第 4 章 配置系统以使用 TLOG RHEL 系统角色记录会话记录

使用 **tlog** RHEL 系统角色,您可以使用 Red Hat Ansible Automation Platform 配置系统以便在 RHEL 上进行终端会话记录。

4.1. TLOG 系统角色

您可以使用 **tlog** RHEL 系统角色为 RHEL 上终端会话记录配置 RHEL 系统。 **tlog** 软件包及其关联的 Web 控制台会话播放器为您提供了记录和回放用户终端会话的能力。

您可以将记录配置为通过 **SSSD** 服务为每个用户或用户组进行。所有终端输入和输出都会捕获并保存在系统日志中基于文本的格式。

其它资源

- 有关 RHEL 中会话记录的详情，请参阅 记录会话

4.2. TLOG 系统角色的组件和参数

Session Recording 的解决方案由以下组件组成：

- tlog 工具
- 系统安全性服务守护进程（SSSD）
- 可选： Web 控制台界面

用于 tlog RHEL 系统角色的参数有：

角色变量	描述
tlog_use_sssd (default: yes)	使用 SSSD 配置会话记录，这是管理记录的用户或组的首选方法
tlog_scope_sssd (default: none)	配置 SSSD 记录范围 - all / some / none
tlog_users_sssd (default: [])	要记录的用户的 YAML 列表
tlog_groups_sssd (default: [])	要记录的组的 YAML 列表

- 有关使用的参数 **tlog** 以及 tlog 系统角色的附加信息，请参考 **/usr/share/ansible/roles/rhel-system-roles.tlog/README.md** 文件。

4.3. 部署 TLOG RHEL 系统角色

按照以下步骤准备和应用 Ansible playbook 以配置 RHEL 系统,将数据记录到 systemd 日志中。

先决条件

- 您已设置了从控制节点访问系统角色的目标系统（**tlog** 系统角色在其中配置的系统）的 SSH 密钥。

- 您有一个控制节点，这是 Ansible Engine 配置其他系统的系统。
- 您已在控制节点上安装了 Red Hat Ansible Engine，您要从该节点上运行 playbook。
- 已在要从其中运行 playbook 的控制节点上安装了 **rhel-system-roles** 软件包。
- 您至少有一个要配置 **tlog** 系统角色的系统。您不必在要部署 **tlog** 解决方案的系统中安装 Red Hat Ansible Automation Platform。

流程

1. 使用以下内容 ***playbook.yml*** 创建新文件：

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

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

其中,

- **tlog_scope_sssd**:
  - **some** 指定您只记录某些用户和组群，不是 **all** 或 **none**。
- **tlog_users_sssd**:
  - **recordeduser** 指定要记录会话的用户。请注意，这不会为您添加用户。您必须自行设置该用户。

2. 另外，还可以验证 playbook 语法。

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

3. 在清单文件上运行 playbook:

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

*playbook 会在您指定的系统中安装 **tlog** 角色。它还会创建一个 SSSD 配置文件,供您定义的用户和组使用。SSSD 解析并读取这些用户和组以 shell 用户身份覆盖 **tlog** 会话。另外,如果 **cockpit** 软件包安装在系统中，playbook 也会安装 **cockpit-session-recording** 软件包，它是一个 **Cockpit** 模块，供您在 web 控制台界面中查看和播放记录。*

验证步骤

要验证 SSSD 配置文件是否在系统中创建了，请执行以下步骤：

1. *进入创建 SSSD 配置丢弃文件的文件夹：*

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

2. 检查文件内容：

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

您可以看到该文件包含您在 playbook 中设置的参数。

4.4. 部署 TLOG RHEL 系统角色以排除组或用户列表

您可以使用 RHEL 上的 **tlog** 系统角色支持 SSSD 会话记录选项 **exclude_users** 和 **exclude_groups**。按照以下步骤准备并应用 Ansible playbook 来配置 RHEL 系统,以排除用户或组的会话记录并登录到 systemd 日志中。

先决条件

- 您已设置了从控制节点访问要配置 tlog 系统角色的目标系统的 SSH 密钥。
- 您有一个控制节点,这是 Red Hat Ansible Engine 配置其他系统的系统。
- 您已在控制节点上安装了 Red Hat Ansible Engine，您要从该节点上运行 playbook。
- 已在控制节点上安装了 **rhel-system-roles** 软件包。
- 您至少有一个系统要配置 **tlog** 系统角色。
  您不必在要部署 **tlog** 解决方案的系统中安装 Red Hat Ansible Automation Platform。

流程

1. 使用以下内容 **playbook.yml** 创建新文件：

```
---
- 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
```

其中,

- ***tlog_scope_sssd***:
  - ***all***: 指定您要记录所有用户和组。
- ***tlog_exclude_users_sssd***:
  - 用户名：指定您要从会话记录中排除的用户的用户名。
- ***tlog_exclude_groups_sssd***:

- **admins** 指定您要从会话记录中排除的组。

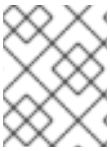
2. （可选）验证 playbook 语法：

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

3. 在清单文件上运行 playbook:

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

playbook 会在您指定的系统中安装 **tlog** 软件包。它还创建一个 **/etc/sssd/conf.d/sssd-session-recording.conf** SSSD 配置文件,用户和组可使用该文件,但您定义的排除文件除外。SSSD 解析并读取这些用户和组,以 shell 用户身份与 **tlog** 会话重叠。另外,如果 **cockpit** 软件包安装在系统中，playbook 也会安装 **cockpit-session-recording** 软件包，它是一个 **Cockpit** 模块，供您在 web 控制台界面中查看和播放记录。



注意

您无法记录 **exclude_users** 列表中列出的用户的会话,或者它们是 **exclude_groups** 列表中组的成员。

验证步骤

要验证 SSSD 配置文件是否在系统中创建了，请执行以下步骤：

1. 进入创建 SSSD 配置丢弃文件的文件夹：

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

2. 检查文件内容：

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

您可以看到该文件包含您在 playbook 中设置的参数。

其它资源

- 请查看 **/usr/share/doc/rhel-system-roles/tlog/** 和 **/usr/share/ansible/roles/rhel-system-roles.tlog/** 目录。
- 请查看 第 4.5 节 "使用在 CLI 中部署的 tlog 系统角色记录会话"。

4.5. 使用在 CLI 中部署的 TLOG 系统角色记录会话

当您在指定的系统中部署了 **tlog** 系统角色，就可以使用命令行界面（CLI）记录用户终端会话。

先决条件

- 您已在目标系统中部署了 **tlog** 系统角色。
- SSSD 配置丢弃文件在文件 **/etc/sssd/conf.d** 中创建。

流程

1. 创建一个用户并为这个用户分配密码：

```
# useradd recordeduser
# passwd recordeduser
```

2. 以您刚刚创建的用户身份登录到该系统：

```
# ssh recordeduser@localhost
```

3. 当系统提示您输入 yes 或 no 进行身份验证时请输入 "yes"。

4. 插入 recorduser 的密码。
系统提示一条信息通知您的会话被记录。

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

5. 记录完会话后，请键入：

```
# exit
```

系统从用户注销并关闭与本地主机的连接。

用户会话会被记录，并被保存，您可以使用 journal 进行播放。

验证步骤

要在日志中查看您记录的会话，请执行以下步骤：

1. 运行以下命令：

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

2. 搜索 **tlog-rec** 记录日志条目中的 **MESSAGE** 字段。

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

4.6. 使用 CLI 监视记录的会话

您可以使用命令行界面（CLI）从日志中执行用户会话记录。

先决条件

- 您已经记录了一个用户会话。请查看 第 4.5 节 "使用在 CLI 中部署的 tlog 系统角色记录会话"

流程

1. 在 CLI 终端中，播放用户会话记录：

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

2. 搜索 **tlog** 记录：

```
$ /tlog-rec
```

您可以查看详情，例如：

- 用户会话记录的用户名
- **out_txt** 字段是记录的会话的原始输出编码
- 标识符号 TLOG_REC=ID_number

3. 复制标识符号 TLOG_REC=ID_number。
4. 使用标识符号 TLOG_REC=ID_number 回放记录。

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

您可以看到记录的用户会话被回放。