Red Hat Enterprise Linux 8

为技术支持生成 sos 报告

使用 sos 程序从 RHEL 服务器收集故障排除信息

Last Updated: 2021-08-26

Red Hat Enterprise Linux 8 为技术支持生成 sos 报告

使用 sos 程序从 RHEL 服务器收集故障排除信息

Enter your first name here. Enter your surname here.
Enter your organisation's name here. Enter your organisational division here.
Enter your email address here.

法律通告

摘要

本文档描述了使用 sos 工具来收集配置、诊断和故障排除数据，以及如何向红帽技术支持提供这些文件。

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 为技术支持生成 sos 报告

1.1. sos 报告工具的作用

在分析 RHEL 系统的服务请求时，**sos** 报告是红帽技术支持工程师的常见起点。该工具提供了一种标准的方法来收集诊断信息，红帽支持工程师可以在整个调查支持问题单中报告的问题时参考这些信息。使用 **sosreport** 工具可确保不会重复地要求您输入数据。

sosreport 工具从 RHEL 系统收集配置详情、系统信息和诊断信息，例如：

- 运行的内核版本。
- 载入的内核模块。
- 系统和服务配置文件。
- 诊断命令输出。
- 安装的软件包列表。

sosreport 实用程序将收集的数据写入到名为 **sosreport-*<host_name>-<support_case_number>-<YYYY-MM-DD>-<unique_random_characters>*.tar.xz** 的归档中。

该工具将归档及其 MD5 校验和保存在 **/var/tmp/** 目录中：

```
[root@server1 ~]# ll /var/tmp/sosreport*
total 18704
-rw-------. 1 root root 19136596 Jan 25 07:42 sosreport-server1-12345678-2021-01-25-tgictvu.tar.xz
-rw-r--r--. 1 root root       33 Jan 25 07:42 sosreport-server1-12345678-2021-01-25-tgictvu.tar.xz.md5
```

其它资源

- **sosreport** man page

1.2. 从命令行安装 sos 软件包

要使用 **sosreport** 工具，请安装 **sos** 软件包。

先决条件

- 您需要 **root** 权限。

流程

- 安装 **sos** 软件包。

```
[root@server ~]# dnf install sos
```

验证步骤

- 使用 **rpm** 实用程序验证是否安装了 **sos** 软件包。

```
[root@server ~]# rpm -q sos
sos-3.9.1-6.el8.noarch
```

1.3. 从命令行生成 sos 报告

使用 **sosreport** 命令从 RHEL 服务器收集 **sos** 报告。

先决条件

- 已安装 **sos** 软件包。
- 您需要 **root** 权限。

流程

1. 运行 **sosreport** 命令并根据屏幕的说明进行操作。使用 **sos** 软件包的版本 3.9 及更新的版本，您可以添加 **--upload** 选项，在生成后立即将 **sos** 报告传输到红帽。

```
[user@server1 ~]$ sudo sosreport
[sudo] password for user:

sosreport (version 3.9)

This command will collect diagnostic and configuration information from
this Red Hat Enterprise Linux system and installed applications.

An archive containing the collected information will be generated in
/var/tmp/sos.qkn_b7by and may be provided to a Red Hat support
representative.

...

Press ENTER to continue, or CTRL-C to quit.
```

2. *（可选）* 如果您已经向红帽创建了技术支持问题单，请输入问题单号将其嵌入 **sos** 报告文件名称中，如果您指定了 **--upload** 选项，则会上传到该问题单中。如果您没有问题单号，请将此字段留空。输入问题单号是可选的，不会影响 **sosreport** 工具的操作。

```
Please enter the case id that you are generating this report for []: <8-digit_case_number>
```

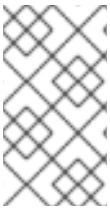
3. 记录控制台输出末尾显示的 **sos** 报告文件名。

```
...
Finished running plugins
Creating compressed archive...

Your sosreport has been generated and saved in:
/var/tmp/sosreport-server1-12345678-2020-09-17-qmtnqng.tar.xz

Size    16.51MiB
Owner   root
md5     bba955bbd9a434954e18da0c6778ba9a

Please send this file to your support representative.
```



注意

您可以使用 **--batch** 选项在没有提示互动输入的情况下生成 **sos** 报告。

```
[user@server1 ~]$ sudo sosreport --batch --case-id <8-digit_case_number>
```

验证步骤

- 验证 **sosreport** 工具是否在 **/var/tmp/** 中创建了与命令输出中描述匹配的存档。

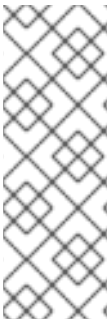
```
[user@server1 ~]$ sudo ls -l /var/tmp/sosreport*
[sudo] password for user:
-rw-------. 1 root root 17310544 Sep 17 19:11 /var/tmp/sosreport-server1-12345678-2020-09-17-qmtnqng.tar.xz
```

其它资源

- 向红帽技术支持提供 **sos** 报告的方法。

1.4. 生成 sos 报告并使用 GPG 密码短语加密对其进行保护

这个步骤描述了如何生成 **sos** 报告并根据密码短语使用对称 GPG2 加密对其进行保护。例如，当您需要通过公共网络将其传送到第三方时，您可能想要使用密码保护 **sos** 报告的内容。



注意

确定您在创建加密的 **sos** 报告时有足够的空间，因为它会临时使用双倍磁盘空间：

1. **sosreport** 工具会创建一个未加密的 **sos** 报告。
2. 工具将 **sos** 报告加密为新文件。
3. 然后，这个工具会删除未加密的报告。

先决条件

- 已安装 **sos** 软件包。
- 您需要 **root** 权限。

流程

1. 运行 **sosreport** 命令并使用 **--encrypt-pass** 选项指定密码短语。使用 **sos** 软件包的版本 3.9 及更新的版本，您可以添加 **--upload** 选项，在生成后立即将 **sos** 报告传输到红帽。

```
[user@server1 ~]$ sudo sosreport --encrypt-pass my-passphrase
[sudo] password for user:

sosreport (version 3.9)

This command will collect diagnostic and configuration information from
this Red Hat Enterprise Linux system and installed applications.
```

```
An archive containing the collected information will be generated in
/var/tmp/sos.6lck0myd and may be provided to a Red Hat support
representative.

...

Press ENTER to continue, or CTRL-C to quit.
```

2. *（可选）*如果您已经向红帽创建了技术支持问题单，请输入问题单号将其嵌入 **sos** 报告文件名称中，如果您指定了 **--upload** 选项，则会上传到该问题单中。如果您没有问题单号，请将此字段留空。输入问题单号是可选的，不会影响 **sosreport** 工具的操作。

```
Please enter the case id that you are generating this report for []: <8-digit_case_number>
```

3. 记录下控制台输出末尾显示的 sos 报告文件名称。

```
...
Finished running plugins
Creating compressed archive...

Your sosreport has been generated and saved in:
/var/tmp/secured-sosreport-server1-12345678-2021-01-24-ueqijfm.tar.xz.gpg

Size    17.53MiB
Owner   root
md5     32e2bdb23a9ce3d35d59e1fc4c91fe54

Please send this file to your support representative.
```

验证步骤

1. 验证 **sosreport** 工具是否创建了满足以下要求的归档：
   - 文件名以 **secured** 开头。
   - 文件名以 **.gpg** 扩展名结尾。
   - 位于 **/var/tmp/** 目录中。

```
[user@server1 ~]$ sudo ls -l /var/tmp/sosreport*
[sudo] password for user:
-rw-------. 1 root root 18381537 Jan 24 17:55 /var/tmp/secured-sosreport-server1-
12345678-2021-01-24-ueqijfm.tar.xz.gpg
```

2. 确定您可以使用您用来加密的同一密码短语解密存档。
   a. 使用 **gpg** 命令解密归档。

```
[user@server1 ~]$ sudo gpg --output decrypted-sosreport.tar.gz --decrypt
/var/tmp/secured-sosreport-server1-12345678-2021-01-24-ueqijfm.tar.xz.gpg
```

   b. 在提示时，输入用来加密归档的密码短语。

```
┌──────────────────────────────────────────────────────────────────────┐
│ Enter passphrase                                                     │
│                                                                      │
│ Passphrase: <passphrase>                                             │
│                                                                      │
│     <OK>                          <Cancel>                           │
└──────────────────────────────────────────────────────────────────────┘
```

c. 验证 **gpg** 工具是否生成了未加密的、使用 **.tar.gz** 文件扩展名的归档。

```
[user@server1 ~]$ sudo ls -l decrypted-sosreport.tar.gz
[sudo] password for user:
-rw-r--r--. 1 root root 18381537 Jan 24 17:59 decrypted-sosreport.tar.gz
```

其它资源

- 向红帽技术支持提供 **sos** 报告的方法。

1.5. 生成 sos 报告并根据密钥对使用 GPG 加密对其进行保护

这个步骤描述了如何根据 GPG 密钥环中的密钥对生成 **sos** 报告并使用 GPG2 加密保护它。如果您想要保护存储在服务器上的 **sos** 报告，您可能想要使用这种加密类型来确保 **sos** 报告的内容。

注意

确定您在创建加密的 **sos** 报告时有足够的空间，因为它会临时使用双倍磁盘空间：

1. **sosreport** 工具会创建一个未加密的 **sos** 报告。
2. 工具将 **sos** 报告加密为新文件。
3. 然后，这个工具会删除未加密的报告。

先决条件

- 已安装 **sos** 软件包。
- 您需要 **root** 权限。
- 您已创建了 GPG2 密钥。

流程

1. 运行 **sosreport** 命令并使用 **--encrypt-key** 选项指定拥有 GPG 密钥环的用户名。使用 **sos** 软件包的版本 3.9 及更新的版本，您可以添加 **--upload** 选项，在生成后立即将 **sos** 报告传输到红帽。

注意

运行 **sosreport** 命令的用户 **必须是** 拥有用于加密和解密 **sos** 报告的 GPG 密钥环的用户。如果用户使用 **sudo** 运行 **sosreport** 命令，还必须使用 **sudo** 设置密钥环，或者用户必须具有对该帐户的直接 shell 访问权限。

```
[user@server1 ~]$ sudo sosreport --encrypt-key root
[sudo] password for user:

sosreport (version 3.9)

This command will collect diagnostic and configuration information from
this Red Hat Enterprise Linux system and installed applications.

An archive containing the collected information will be generated in
/var/tmp/sos.6ucjclgf and may be provided to a Red Hat support
representative.

...

Press ENTER to continue, or CTRL-C to quit.
```

2. *（可选）* 如果您已经向红帽创建了技术支持问题单，请输入问题单号将其嵌入 **sos** 报告文件名称中，如果您指定了 **--upload** 选项，则会上传到该问题单中。如果您没有问题单号，请将此字段留空。输入问题单号是可选的，不会影响 **sosreport** 工具的操作。

```
Please enter the case id that you are generating this report for []: <8-digit_case_number>
```

3. 记录控制台输出末尾显示的 **sos** 报告文件名。

```
...
Finished running plugins
Creating compressed archive...

Your sosreport has been generated and saved in:
/var/tmp/secured-sosreport-server1-23456789-2021-01-27-zhdqhdi.tar.xz.gpg

Size    15.44MiB
Owner   root
md5     ac62697e33f3271dbda92290583d1242

Please send this file to your support representative.
```

验证步骤

1. 验证 **sosreport** 工具是否创建了满足以下要求的归档：

   - 文件名以 **secured** 开头。
   - 文件名以 **.gpg** 扩展名结尾。
   - 位于 **/var/tmp/** 目录中。

   ```
   [user@server1 ~]$ sudo ls -l /var/tmp/sosreport*
   ```

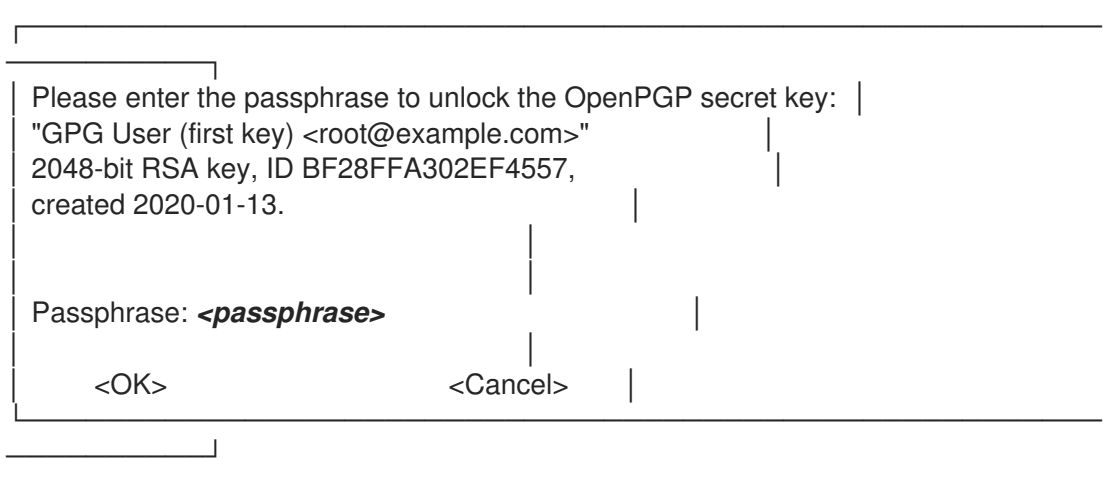
```
[sudo] password for user:
-rw-------. 1 root root 16190013 Jan 24 17:55 /var/tmp/secured-sosreport-server1-23456789-2021-01-27-zhdqhdi.tar.xz.gpg
```

2. 确定您可以使用您用来加密的同一密钥解密存档。

   a. 使用 **gpg** 命令解密归档。

```
[user@server1 ~]$ sudo gpg --output decrypted-sosreport.tar.gz --decrypt /var/tmp/secured-sosreport-server1-23456789-2021-01-27-zhdqhdi.tar.xz.gpg
```

   b. 提示时，请输入创建 GPG 密钥时使用的密码短语。



   c. 验证 **gpg** 工具是否生成了未加密的、使用 **.tar.gz** 文件扩展名的归档。

```
[user@server1 ~]$ sudo ll decrypted-sosreport.tar.gz
[sudo] password for user:
-rw-r--r--. 1 root root 16190013 Jan 27 17:47 decrypted-sosreport.tar.gz
```

其它资源

- 向红帽技术支持提供 **sos** 报告的方法。

1.6. 创建 GPG2 密钥

以下流程描述了如何生成使用加密工具的 GPG2 密钥，如 IdM 备份工具。

先决条件

- 您需要 **root** 权限。

流程

1. 安装并配置 **pinentry** 工具。

```
[root@server ~]# dnf install pinentry
[root@server ~]# mkdir ~/.gnupg -m 700
[root@server ~]# echo "pinentry-program /usr/bin/pinentry-curses" >> ~/.gnupg/gpg-agent.conf
```

2. 创建一个 **key-input** 文件，用来根据您的首选详情生成 GPG 密钥对。例如：

```
[root@server ~]# cat >key-input <<EOF
%echo Generating a standard key
Key-Type: RSA
Key-Length: 2048
Name-Real: GPG User
Name-Comment: first key
Name-Email: root@example.com
Expire-Date: 0
%commit
%echo Finished creating standard key
EOF
```

3. *（可选）* GFS2 默认将其密钥环保存在 **~/.gnupg** 文件中。要使用自定义密钥环位置，将 **GNUPGHOME** 环境变量设置为只有 root 用户可访问的目录。

```
[root@server ~]# export GNUPGHOME=/root/backup

[root@server ~]# mkdir -p $GNUPGHOME -m 700
```

4. 根据 **key-input** 文件的内容生成新的 GPG2 密钥。

```
[root@server ~]# gpg2 --batch --gen-key key-input
```

5. 输入密码短语来保护 GPG2 密钥。您可以使用这个密码短语访问解密的私钥。

```
┌──────────────────────────────────────────────────────┐
│ Please enter the passphrase to                       │
│ protect your new key                                 │
│                                                      │
│ Passphrase: <passphrase>                             │
│                                                      │
│  <OK>                    <Cancel>                    │
└──────────────────────────────────────────────────────┘
```

6. 再输入一次来确认正确的密码短语。

```
┌──────────────────────────────────────────────────────┐
│ Please re-enter this passphrase                      │
│                                                      │
│ Passphrase: <passphrase>                             │
│                                                      │
│  <OK>                    <Cancel>                    │
└──────────────────────────────────────────────────────┘
```

7. 验证新 GPG2 密钥是否已成功创建。

```
gpg: keybox '/root/backup/pubring.kbx' created
gpg: Generating a standard key
gpg: /root/backup/trustdb.gpg: trustdb created
gpg: key BF28FFA302EF4557 marked as ultimately trusted
gpg: directory '/root/backup/openpgp-revocs.d' created
```

```
gpg: revocation certificate stored as '/root/backup/openpgp-
revocs.d/8F6FCF10C80359D5A05AED67BF28FFA302EF4557.rev'
gpg: Finished creating standard key
```

验证步骤

- 列出服务器中的 GPG 密钥。

```
[root@server ~]# gpg2 --list-secret-keys
gpg: checking the trustdb
gpg: marginals needed: 3  completes needed: 1  trust model: pgp
gpg: depth: 0  valid:   1  signed:   0  trust: 0-, 0q, 0n, 0m, 0f, 1u
/root/backup/pubring.kbx
------------------------
sec   rsa2048 2020-01-13 [SCEA]
      8F6FCF10C80359D5A05AED67BF28FFA302EF4557
uid           [ultimate] GPG User (first key) <root@example.com>
```

其它资源

- GNU Privacy Guard

1.7. 从救援环境中生成 sos 报告

如果 Red Hat Enterprise Linux(RHEL)主机无法正确引导，您可以将主机引导到 *救援环境中* 以收集 **sos** 报告。

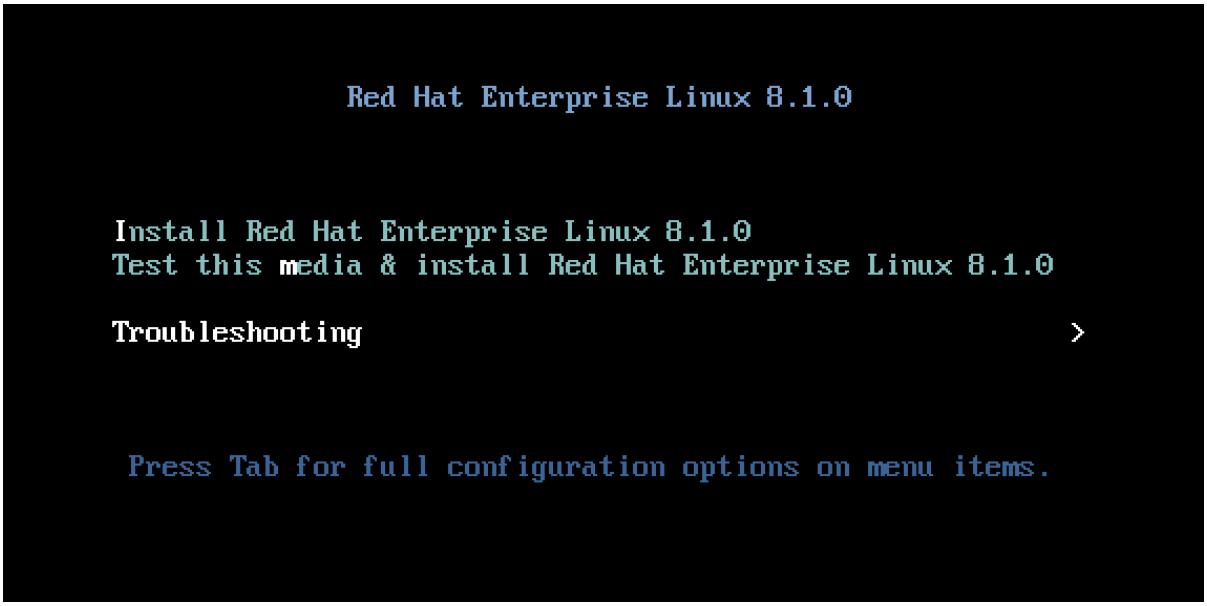
使用救援环境，您可以在 **/mnt/sysimage** 下挂载目标系统，访问其内容并运行 **sosreport** 命令。

先决条件

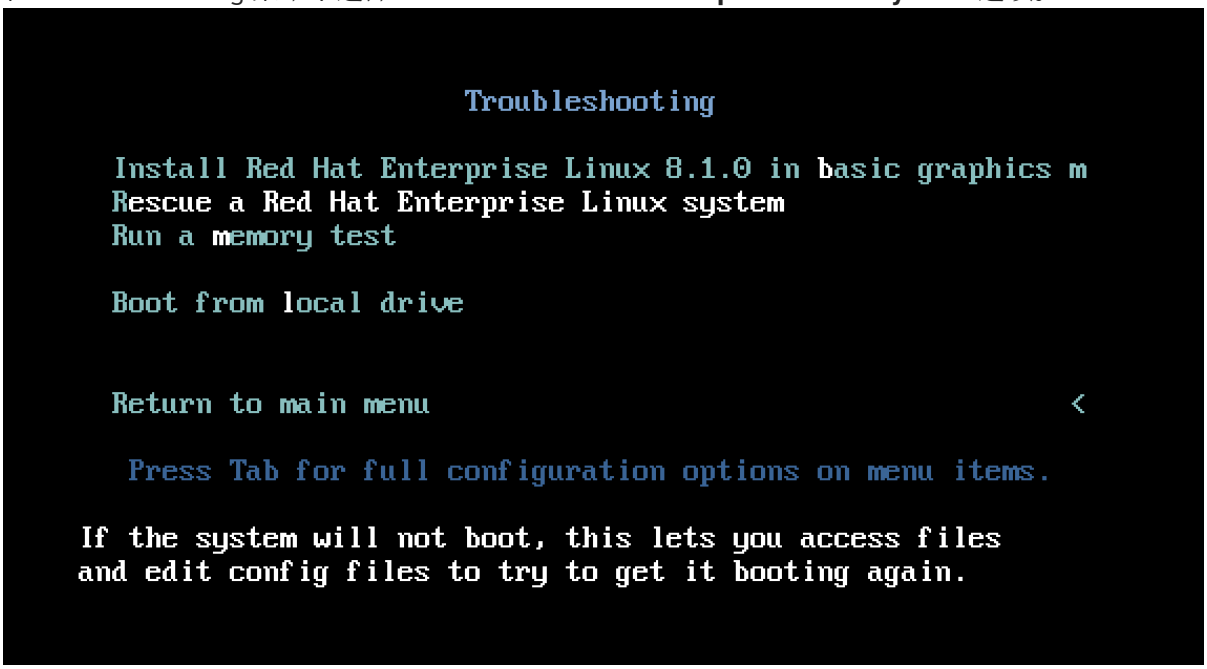
- 如果主机是裸机服务器，则需要对该机器进行的物理访问。
- 如果主机是虚拟机，您需要访问虚拟机管理程序中的虚拟机设置。
- RHEL 安装源，如 ISO 镜像文件、安装 DVD、netboot CD 或提供 RHEL 安装树的 Preboot Execution Environment（PXE）配置。

流程

1. 从安装源引导主机。
2. 在安装介质的引导菜单中，选择 **Troubleshooting** 选项。



3. 在 Troubleshooting 菜单中选择 **Rescue a Red Hat Enterprise Linux system** 选项。



4. 在 Rescue 菜单中选择 **1**，然后按 **Enter 键** 继续并将系统挂载到 **/mnt/sysimage** 目录中。

```
Starting installer, one moment...
anaconda 29.19.1.13-1.el8 for Red Hat Enterprise Linux 8.1 started.
 * installation log files are stored in /tmp during the installation
 * shell is available on TTY2
 * when reporting a bug add logs from /tmp as separate text/plain attachments
================================================================================
================================================================================
Rescue

The rescue environment will now attempt to find your Linux installation and
mount it under the directory : /mnt/sysimage.  You can then make any changes
required to your system.  Choose '1' to proceed with this step.
You can choose to mount your file systems read-only instead of read-write by
choosing '2'.
If for some reason this process does not work choose '3' to skip directly to a
shell.

1) Continue
2) Read-only mount
3) Skip to shell
4) Quit (Reboot)

Please make a selection from the above: 1_
```

5. 提示时按 **Enter** 键进行一个 shell。

```
Please make a selection from the above: 1
================================================================================
================================================================================
Rescue Shell

Your system has been mounted under /mnt/sysimage.

If you would like to make the root of your system the root of the active system,
run the command:

        chroot /mnt/sysimage

When finished, please exit from the shell and your system will reboot.
Please press ENTER to get a shell: _
[anaconda]1:main* 2:shell  3:log  4:storage-log  5:program-log       Switch tab: Alt+Tab | Help: F1
```

6. 使用 **chroot** 命令将救援会话的显式根目录改为 **/mnt/sysimage** 目录。

```
================================================================================
================================================================================
Rescue Shell

Your system has been mounted under /mnt/sysimage.

If you would like to make the root of your system the root of the active system,
run the command:

        chroot /mnt/sysimage

When finished, please exit from the shell and your system will reboot.
Please press ENTER to get a shell:
sh-4.4# chroot /mnt/sysimage
bash-4.4#
[anaconda]1:main* 2:shell  3:log  4:storage-log  5:program-log       Switch tab: Alt+Tab | Help: F1
```

7. 运行 **sosreport** 命令并根据屏幕的说明进行操作。使用 **sos** 软件包的版本 3.9 及更新的版本，您可以添加 **--upload** 选项，在生成后立即将 **sos** 报告传输到红帽。

```
bash-4.4# sosreport

sosreport (version 3.7)

This command will collect diagnostic and configuration information from
this Red Hat Enterprise Linux system and installed applications.

An archive containing the collected information will be generated in
/var/tmp/sos.d5z2riw6 and may be provided to a Red Hat support
representative.

Any information provided to Red Hat will be treated in accordance with
the published support policies at:

  https://access.redhat.com/support/

The generated archive may contain data considered sensitive and its
content should be reviewed by the originating organization before being
passed to any third party.

No changes will be made to system configuration.

Press ENTER to continue, or CTRL-C to quit.

[anaconda]1:main* 2:shell  3:log  4:storage-log  5:program-log       Switch tab: Alt+Tab | Help: F1
```

8. *（可选）*如果您已经向红帽创建了技术支持问题单，请输入问题单号将其嵌入 **sos** 报告文件名称中，如果您指定了 **--upload** 选项且您的主机已连接到互联网，则会上传到该问题单中。如果您没有问题单号，请将此字段留空。输入问题单号是可选的，不会影响 **sosreport** 工具的操作。

```
Press ENTER to continue, or CTRL-C to quit.

Please enter the case id that you are generating this report for []: 12345678_

[anaconda]1:main* 2:shell  3:log  4:storage-log  5:program-log       Switch tab: Alt+Tab | Help: F1
```

9. 记录控制台输出末尾显示的 **sos** 报告文件名。

```
  Finishing plugins              [Running: yum]
  Finished running plugins
Creating compressed archive...

Your sosreport has been generated and saved in:
  /var/tmp/sosreport-localhost-12345678-2020-09-22-ygyhflo.tar.xz

The checksum is: 022b1ea8693898345b21cf4a7112efd0

Please send this file to your support representative.

bash-4.4#
[anaconda]1:main* 2:shell  3:log  4:storage-log  5:program-log       Switch tab: Alt+Tab | Help: F1
```

10. 如果您的主机没有连接到互联网，使用文件传输程序（如 **scp** ）将 **sos** 报告传送到网络中的另一主机，然后将其上传到红帽技术支持问题单。

验证步骤

- 验证 **sosreport** 工具是否在 **/var/tmp/** 目录中创建了归档。

```
bash-4.4# ls -l /var/tmp/sosreport*
-rw-------. 1 root root 6369404 Sep 22 08:32 /var/tmp/sosreport-localhost-12345678-2020-09-22-ygyhfl
o.tar.xz
-rw-r--r--. 1 root root      33 Sep 22 08:32 /var/tmp/sosreport-localhost-12345678-2020-09-22-ygyhfl
o.tar.xz.md5
bash-4.4#
[anaconda]1:main* 2:shell  3:log  4:storage-log  5:program-log       Switch tab: Alt+Tab | Help: F1
```

其它资源

- 要下载 RHEL 安装 DVD 的 ISO，请访问红帽客户门户网站的下载部分。请参阅 产品下载。
- 向红帽技术支持提供 **sos** 报告的方法。

1.8. 向红帽技术支持提供 sos 报告的方法

您可以使用以下方法将 **sos** 报告上传到红帽技术支持。

使用 sosreport 命令上传

对于 **sos** 软件包的版本 3.9 或更高版本，您可以使用 **--upload** 选项在生成后立即将 **sos** 报告传输给红帽。

- 如果您在提示时提供一个问题单号，或使用 **--case-id** 或者 **--ticket-number** 选项，则 **sosreport** 实用程序会在使用红帽客户门户网站帐户验证后将 **sos** 报告上传到您的问题单中。
- 如果您不提供问题单号或者您没有验证，则会将 **sos** 报告上传到 Red Hat 公共 FTP 站点。为红帽技术支持工程师提供 **sos** 报告归档的名称，以便可以访问它。

```
[user@server1 ~]$ sudo sosreport --upload
[sudo] password for user:

sosreport (version 3.9)

This command will collect diagnostic and configuration information from
this Red Hat Enterprise Linux system and installed applications.
...

Please enter the case id that you are generating this report for []: <8-digit_case_number>
Enter your Red Hat Customer Portal username (empty to use public dropbox):
<Red_Hat_Customer_Portal_ID>
Please provide the upload password for <user@domain.com>:
...

Attempting upload to Red Hat Customer Portal
Uploaded archive successfully
```

通过红帽客户门户网站上传文件

使用您的红帽用户帐户，您可以登录到红帽客户门户网站网站的 **Support Cases** 部分，并将 **sos** 报告上传到技术支持问题单。
要登录，请访问支持问题单。

使用红帽支持工具上传文件

通过红帽支持工具，您可以直接将文件从命令行上传到红帽技术支持问题单。问题单号是必需的。

```
[user@server1 ~]$ redhat-support-tool addattachment -c <8-digit_case_number>
</var/tmp/sosreport_filename>
```

其它资源

- *有关如何通过 **sos** 报告提供红帽技术支持的其他方法，如 FTP 和 **curl**，请参阅红帽知识库文章 How to provide files to Red Hat Support（vmcore、rhev logcollector、sosreports、堆转储、日志文件等）*