



Red Hat Enterprise Linux 8

Generating sos reports for technical support

Gathering troubleshooting information from RHEL servers with the sos utility

Red Hat Enterprise Linux 8 Generating sos reports for technical support

Gathering troubleshooting information from RHEL servers with the sos utility

Legal Notice

Copyright © 2021 Red Hat, Inc.

The text of and illustrations in this document are licensed by Red Hat under a Creative Commons Attribution–Share Alike 3.0 Unported license ("CC-BY-SA"). An explanation of CC-BY-SA is available at

<http://creativecommons.org/licenses/by-sa/3.0/>

. In accordance with CC-BY-SA, if you distribute this document or an adaptation of it, you must provide the URL for the original version.

Red Hat, as the licensor of this document, waives the right to enforce, and agrees not to assert, Section 4d of CC-BY-SA to the fullest extent permitted by applicable law.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, the Red Hat logo, JBoss, OpenShift, Fedora, the Infinity logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

Linux[®] is the registered trademark of Linus Torvalds in the United States and other countries.

Java[®] is a registered trademark of Oracle and/or its affiliates.

XFS[®] is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

MySQL[®] is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js[®] is an official trademark of Joyent. Red Hat is not formally related to or endorsed by the official Joyent Node.js open source or commercial project.

The OpenStack[®] Word Mark and OpenStack logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

All other trademarks are the property of their respective owners.

Abstract

This document describes using the sos utility to collect configuration, diagnostic, and troubleshooting data, and how to provide those files to Red Hat Technical Support.

Table of Contents

MAKING OPEN SOURCE MORE INCLUSIVE	3
PROVIDING FEEDBACK ON RED HAT DOCUMENTATION	4
CHAPTER 1. GENERATING AN SOS REPORT FOR TECHNICAL SUPPORT	5
1.1. WHAT THE SOS REPORT UTILITY DOES	5
1.2. INSTALLING THE SOS PACKAGE FROM THE COMMAND LINE	5
1.3. GENERATING AN SOS REPORT FROM THE COMMAND LINE	6
1.4. GENERATING AN SOS REPORT AND SECURING IT WITH GPG PASSPHRASE ENCRYPTION	7
1.5. GENERATING AN SOS REPORT AND SECURING IT WITH GPG ENCRYPTION BASED ON A KEYPAIR	9
1.6. CREATING A GPG2 KEY	11
1.7. GENERATING AN SOS REPORT FROM THE RESCUE ENVIRONMENT	13
1.8. METHODS FOR PROVIDING AN SOS REPORT TO RED HAT TECHNICAL SUPPORT	17

MAKING OPEN SOURCE MORE INCLUSIVE

Red Hat is committed to replacing problematic language in our code, documentation, and web properties. We are beginning with these four terms: master, slave, blacklist, and whitelist. Because of the enormity of this endeavor, these changes will be implemented gradually over several upcoming releases. For more details, see [our CTO Chris Wright's message](#).

PROVIDING FEEDBACK ON RED HAT DOCUMENTATION

We appreciate your input on our documentation. Please let us know how we could make it better. To do so:

- For simple comments on specific passages:
 1. Make sure you are viewing the documentation in the *Multi-page HTML* format. In addition, ensure you see the **Feedback** button in the upper right corner of the document.
 2. Use your mouse cursor to highlight the part of text that you want to comment on.
 3. Click the **Add Feedback** pop-up that appears below the highlighted text.
 4. Follow the displayed instructions.
- For submitting more complex feedback, create a Bugzilla ticket:
 1. Go to the [Bugzilla](#) website.
 2. As the Component, use **Documentation**.
 3. Fill in the **Description** field with your suggestion for improvement. Include a link to the relevant part(s) of documentation.
 4. Click **Submit Bug**.

CHAPTER 1. GENERATING AN `sos` REPORT FOR TECHNICAL SUPPORT

1.1. WHAT THE `sos` REPORT UTILITY DOES

An **sos** report is a common starting point for Red Hat technical support engineers when performing analysis of a service request for a RHEL system. The utility provides a standardized way to collect diagnostic information that Red Hat support engineers can reference throughout their investigation of issues reported in support cases. Using the **sosreport** utility helps to ensure that you are not repeatedly asked for data output.

The **sosreport** utility collects configuration details, system information, and diagnostic information from a RHEL system such as:

- The running kernel version.
- Loaded kernel modules.
- System and service configuration files.
- Diagnostic command output.
- A list of installed packages.

The **sosreport** utility writes the data it collects to an archive named **sosreport-*<host_name>*-*<support_case_number>*-*<YYYY-MM-DD>*-*<unique_random_characters>*.tar.xz**.

The utility stores the archive and its MD5 checksum in the **/var/tmp/** directory:

```
[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
```

Additional resources

- **sosreport** man page

1.2. INSTALLING THE `sos` PACKAGE FROM THE COMMAND LINE

To use the **sosreport** utility, install the **sos** package.

Prerequisites

- You need **root** privileges.

Procedure

- Install the **sos** package.

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

Verification steps

- Use the **rpm** utility to verify that the **sos** package is installed.

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

1.3. GENERATING AN sos REPORT FROM THE COMMAND LINE

Use the **sosreport** command to gather an **sos** report from a RHEL server.

Prerequisites

- You have installed the **sos** package.
- You need **root** privileges.

Procedure

1. Run the **sosreport** command and follow the on-screen instructions. With version 3.9 and later of the **sos** package, you can add the **--upload** option to transfer the **sos** report to Red Hat immediately after generating it.

```
[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. (*Optional*) If you have already opened a Technical Support case with Red Hat, enter the case number to embed it in the **sos** report file name, and it will be uploaded to that case if you specified the **--upload** option. If you do not have a case number, leave this field blank. Entering a case number is optional and does not affect the operation of the **sosreport** utility.

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

3. Take note of the **sos** report file name displayed at the end of the console output.

```
...
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.



NOTE

You can use the **--batch** option to generate an **sos** report without prompting for interactive input.

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

Verification steps

- Verify that the **sosreport** utility created an archive in **/var/tmp/** matching the description from the command output.

```
[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
```

Additional resources

- [Methods for providing an **sos** report to Red Hat technical support](#) .

1.4. GENERATING AN sos REPORT AND SECURING IT WITH GPG PASSPHRASE ENCRYPTION

This procedure describes how to generate an **sos** report and secure it with symmetric GPG2 encryption based on a passphrase. You might want to secure the contents of an **sos** report with a password if, for example, you need to transfer it over a public network to a third party.



NOTE

Ensure you have sufficient space when creating an encrypted **sos** report, as it temporarily uses double the disk space:

1. The **sosreport** utility creates an unencrypted **sos** report.
2. The utility encrypts the **sos** report as a new file.
3. The utility then removes the unencrypted archive.

Prerequisites

- You have installed the **sos** package.
- You need **root** privileges.

Procedure

1. Run the **sosreport** command and specify a passphrase with the **--encrypt-pass** option. With version 3.9 and later of the **sos** package, you can add the **--upload** option to transfer the **sos** report to Red Hat immediately after generating it.

```
[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. (Optional) If you have already opened a Technical Support case with Red Hat, enter the case number to embed it in the **sos** report file name, and it will be uploaded to that case if you specified the **--upload** option. If you do not have a case number, leave this field blank. Entering a case number is optional and does not affect the operation of the **sosreport** utility.

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

3. Take note of the sos report file name displayed at the end of the console output.

```
...
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.

Verification steps

1. Verify that the **sosreport** utility created an archive meeting the following requirements:
 - Filename starts with **secured**.
 - Filename ends with a **.gpg** extension.
 - Located in the `/var/tmp/` directory.

```
[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. Verify that you can decrypt the archive with the same passphrase you used to encrypt it.
 - a. Use the **gpg** command to decrypt the archive.

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

- b. When prompted, enter the passphrase you used to encrypt the archive.

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

- c. Verify that the **gpg** utility produced an unencrypted archive with a **.tar.gz** file extension.

```
[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
```

Additional resources

- [Methods for providing an **sos** report to Red Hat technical support](#) .

1.5. GENERATING AN **sos** REPORT AND SECURING IT WITH GPG ENCRYPTION BASED ON A KEYPAIR

This procedure describes how to generate an **sos** report and secure it with GPG2 encryption based on a keypair from a GPG keyring. You might want to secure the contents of an **sos** report with this type of encryption if, for example, you want to protect an **sos** report stored on a server.



NOTE

Ensure you have sufficient space when creating an encrypted **sos** report, as it temporarily uses double the disk space:

1. The **sosreport** utility creates an unencrypted **sos** report.
2. The utility encrypts the **sos** report as a new file.
3. The utility then removes the unencrypted archive.

Prerequisites

- You have installed the **sos** package.
- You need **root** privileges.
- You have created a GPG2 key.

Procedure

1. Run the **sosreport** command and specify the user name that owns the GPG keyring with the **--encrypt-key** option. With version 3.9 and later of the **sos** package, you can add the **--upload** option to transfer the **sos** report to Red Hat immediately after generating it.



NOTE

The user running the **sosreport** command **must** be the same user that owns the GPG keyring used to encrypt and decrypt the **sos** report. If the user uses **sudo** to run the **sosreport** command, the keyring must also be set up using **sudo**, or the user must have direct shell access to that account.

```
[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. (Optional) If you have already opened a Technical Support case with Red Hat, enter the case number to embed it in the **sos** report file name, and it will be uploaded to that case if you specified the **--upload** option. If you do not have a case number, leave this field blank. Entering a case number is optional and does not affect the operation of the **sosreport** utility.

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

3. Take note of the **sos** report file name displayed at the end of the console output.

```
...
```

```
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.

Verification steps

1. Verify that the **sosreport** utility created an archive meeting the following requirements:

- Filename starts with **secured**.
- Filename ends with a **.gpg** extension.
- Located in the **/var/tmp/** directory.

```
[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. Verify you can decrypt the archive with the same key you used to encrypt it.

a. Use the **gpg** command to decrypt the archive.

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

b. When prompted, enter the passphrase you used when creating the GPG key.

```

Please enter the passphrase to unlock the OpenPGP secret key:
"GPG User (first key) <root@example.com>"
2048-bit RSA key, ID BF28FFA302EF4557,
created 2020-01-13.

Passphrase: <passphrase>

<OK> <Cancel>
```

c. Verify that the **gpg** utility produced an unencrypted archive with a **.tar.gz** file extension.

```
[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
```

Additional resources

- [Methods for providing an sos report to Red Hat technical support](#) .

1.6. CREATING A GPG2 KEY

The following procedure describes how to generate a GPG2 key to use with encryption utilities.

Prerequisites

- You need **root** privileges.

Procedure

1. Install and configure the **pinentry** utility.

```
[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. Create a **key-input** file used for generating a GPG keypair with your preferred details. For example:

```
[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. (Optional) By default, GPG2 stores its keyring in the `~/.gnupg` file. To use a custom keyring location, set the **GNUPGHOME** environment variable to a directory that is only accessible by root.

```
[root@server ~]# export GNUPGHOME=/root/backup
[root@server ~]# mkdir -p $GNUPGHOME -m 700
```

4. Generate a new GPG2 key based on the contents of the **key-input** file.

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

5. Enter a passphrase to protect the GPG2 key. You use this passphrase to access the private key for decryption.

```
Please enter the passphrase to
protect your new key

Passphrase: <passphrase>

<OK>                <Cancel>
```


- Confirm the correct passphrase by entering it again.

```

Please re-enter this passphrase
Passphrase: <passphrase>
<OK>          <Cancel>

```

- Verify that the new GPG2 key was created successfully.

```

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

```

Verification Steps

- List the GPG keys on the server.

```

[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>

```

Additional resources

- For more information on GPG encryption and its uses, see the [GNU Privacy Guard](#) website.

1.7. GENERATING AN sos REPORT FROM THE RESCUE ENVIRONMENT

If a Red Hat Enterprise Linux (RHEL) host does not boot properly, you can boot the host into a *rescue environment* to gather an **sos** report.

Using the rescue environment, you can mount the target system under **/mnt/sysimage**, access its contents, and run the **sosreport** command.

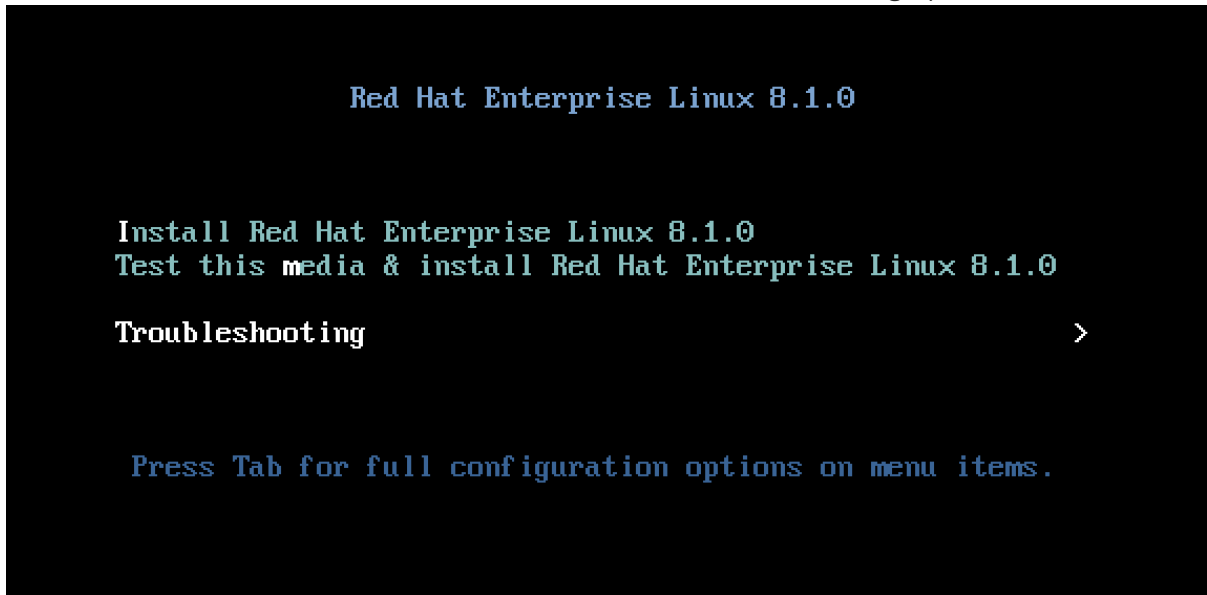
Prerequisites

- If the host is a bare metal server, you need physical access to the machine.
- If the host is a virtual machine, you need access to the virtual machine's settings in the hypervisor.

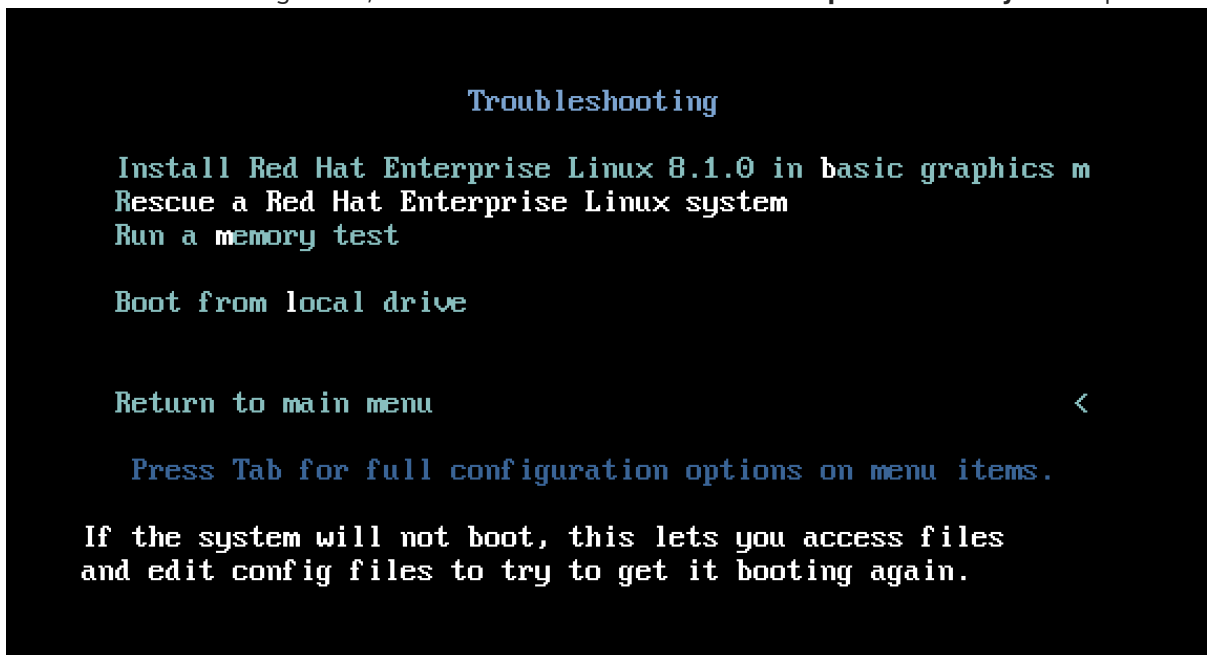
- A RHEL installation source, such as an ISO image file, an installation DVD, a netboot CD, or a Preboot Execution Environment (PXE) configuration providing a RHEL installation tree.

Procedure

1. Boot the host from an installation source.
2. In the boot menu for the installation media, select the **Troubleshooting** option.



3. In the Troubleshooting menu, select the **Rescue a Red Hat Enterprise Linux system** option.



4. At the Rescue menu, select **1** and press the **Enter** key to continue and mount the system under the `/mnt/sysimage` directory.

```

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. Press the **Enter** key to obtain a shell when prompted.

```

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:
[anaconda1:main* 2:shell 3:log 4:storage-log 5:program-log  Switch tab: Alt+Tab | Help: F1

```

6. Use the **chroot** command to change the apparent root directory of the rescue session to the **/mnt/sysimage** directory.

```

=====
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#
[anaconda1:main* 2:shell 3:log 4:storage-log 5:program-log  Switch tab: Alt+Tab | Help: F1

```

7. Run the **sosreport** command and follow the on-screen instructions. With version 3.9 and later of the **sos** package, you can add the **--upload** option to transfer the **sos** report to Red Hat immediately after generating it.

```

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.

```

```

[anaconda1:main* 2:shell 3:log 4:storage-log 5:program-log Switch tab: Alt+Tab | Help: F1

```

- (Optional) If you have already opened a Technical Support case with Red Hat, enter the case number to embed it in the **sos** report file name, and it will be uploaded to that case if you specified the **--upload** option and your host is connected to the internet. If you do not have a case number, leave this field blank. Entering a case number is optional and does not affect the operation of the **sosreport** utility.

```

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

```

```

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

```

```

[anaconda1:main* 2:shell 3:log 4:storage-log 5:program-log Switch tab: Alt+Tab | Help: F1

```

- Take note of the **sos** report file name displayed at the end of the console output.

```

    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-ygyhf1o.tar.xz

The checksum is: 022b1ea8693898345b21cf4a7112efd0

Please send this file to your support representative.

```

```

bash-4.4#

```

```

[anaconda1:main* 2:shell 3:log 4:storage-log 5:program-log Switch tab: Alt+Tab | Help: F1

```

- If your host does not have a connection to the internet, use a file transfer utility such as **scp** to transfer the **sos** report to another host on your network, then upload it to a Red Hat Technical Support case.

Verification steps

- Verify that the **sosreport** utility created an archive in the **/var/tmp/** directory.

```

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-ygyhf1o.tar.xz
-rw-r--r--. 1 root root      33 Sep 22 08:32 /var/tmp/sosreport-localhost-12345678-2020-09-22-ygyhf1o.tar.xz.md5
bash-4.4#

```

```

[anaconda1:main* 2:shell 3:log 4:storage-log 5:program-log Switch tab: Alt+Tab | Help: F1

```

Additional resources

- To download an ISO of the RHEL installation DVD, visit the downloads section of the Red Hat Customer Portal. See [Product Downloads](#).
- [Methods for providing an **sos** report to Red Hat technical support](#) .

1.8. METHODS FOR PROVIDING AN **sos** REPORT TO RED HAT TECHNICAL SUPPORT

You can use the following methods to upload your **sos** report to Red Hat Technical Support.

Upload with the **sosreport** command

With version 3.9 or later of the **sos** package, you can use the **--upload** option to transfer the **sos** report to Red Hat immediately after generating it.

- If you provide a case number when prompted, or use the **--case-id** or **--ticket-number** options, the **sosreport** utility uploads the **sos** report to your case after you authenticate with your Red Hat Customer Portal account.
- If you do not provide a case number or you do not authenticate, the utility uploads the **sos** report to the Red Hat public FTP site. Provide Red Hat Technical Support Engineers with the name of the **sos** report archive so they can access it.

```
[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
```

Upload files via the Red Hat Customer Portal

Using your Red Hat user account, you can log into the **Support Cases** section of the Red Hat Customer Portal website and upload an **sos** report to a technical support case.

To log in, visit [Support Cases](#).

Upload files using the Red Hat Support Tool

With the Red Hat Support Tool, you can upload a file directly from the command line to a Red Hat technical support case. The case number is required.

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

Additional resources

- For additional methods on how to provide Red Hat Technical Support with your **sos** report, such as FTP and **curl**, see the Red Hat Knowledgebase article [How to provide files to Red Hat Support \(vmcore, rhev logcollector, sosreports, heap dumps, log files, etc.\)](#)