Red Hat Enterprise Linux 9

Getting the most from your Support experience

Gathering troubleshooting information from RHEL servers with the sos utility

Last Updated: 2022-05-18
Gathering troubleshooting information from RHEL servers with the sos utility
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 AND COLLECTING SOS REPORTS ON MULTIPLE SYSTEMS CONCURRENTLY .................. 7  
1.5. CLEANING AN SOS REPORT ................................................................. 9  
1.6. GENERATING AN SOS REPORT AND SECURING IT WITH GPG PASSPHRASE ENCRYPTION ............... 12  
1.7. GENERATING AN SOS REPORT AND SECURING IT WITH GPG ENCRYPTION BASED ON A KEYPAIR .......... 14  
1.8. CREATING A GPG2 KEY ............................................................... 16  
1.9. METHODS FOR PROVIDING AN SOS REPORT TO RED HAT TECHNICAL SUPPORT .......................... 18
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.

- 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 feedback via Bugzilla, create a new 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**.
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 sos report utility helps to ensure that you are not repeatedly asked for data output.

The sos report utility allows to collect various debugging information from one or more systems, optionally clean sensitive data, and upload it in a form of a report to Red Hat. More specifically, the three sos report components do the following:

- **sos report** collects debugging information from one system. Note that this program was originally named sosreport. Running sosreport still works as sos report is called instead, with the same arguments.

- **sos collect** allows to run and collect individual sos reports from a specified set of nodes.

- **sos clean** obfuscates potentially sensitive information such as usernames, hostnames, IP or MAC addresses, or other user-specified data.

The information collected in a report contains 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 sos report 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-r--r--. 1 root root 33 Jan 25 07:42 sosreport-server1-12345678-2022-01-25-tgictvu.tar.xz.md5
```

Additional resources

- **sosreport** man page

1.2. INSTALLING THE sos PACKAGE FROM THE COMMAND LINE
To use the `sos report` utility, install the `sos` package.

**Prerequisites**
- You need `root` privileges.

**Procedure**
- Install the `sos` package.
  
  ```bash
  [root@server ~]# dnf install sos
  ```

**Verification steps**
- Use the `rpm` utility to verify that the `sos` package is installed.
  
  ```bash
  [root@server ~]# rpm -q sos
  sos-4.2-15.el9.noarch
  ```

### 1.3. GENERATING AN sos REPORT FROM THE COMMAND LINE

Use the `sos report` 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 `sos report` 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
  [user@server1 ~]# sudo sos report
  [sudo] password for user:
  
  sos report (version 4.2)
  
  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.
  ```

1. *(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 \texttt{--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 \texttt{sos report} utility.

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

2. Take note of the \texttt{sos} report file name displayed at the end of the console output.

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

Your sos report has been generated and saved in: 
\texttt{/var/tmp/sosreport-server1-12345678-2020-09-17-qmtnqng.tar.xz}

Size \texttt{16.51MiB} 
Owner \texttt{root} 
md5 \texttt{bba955bd9a434954e18da0c6778ba9a}

Please send this file to your support representative.

\textbf{NOTE}

- You can use the \texttt{--batch} option to generate an \texttt{sos} report without prompting for interactive input.

\begin{verbatim}
[user@server1 ~]$ sudo sos report \textbf{--batch} --case-id \texttt{<8-digit_case_number>}
\end{verbatim}

- You can also use the \texttt{--clean} option to obfuscate a just-collected \texttt{sos} report.

\begin{verbatim}
[user@server1 ~]$ sudo sos report \textbf{--clean}
\end{verbatim}

\textbf{Verification steps}

- Verify that the \texttt{sos report} utility created an archive in \texttt{/var/tmp/} matching the description from the command output.

\begin{verbatim}
[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
\end{verbatim}

\textbf{Additional resources}

- Methods for providing an \texttt{sos} report to Red Hat technical support.

\section*{1.4. GENERATING AND COLLECTING SOS REPORTS ON MULTIPLE SYSTEMS CONCURRENTLY}

You can use the \texttt{sos} utility to trigger the \texttt{sos report} command on multiple systems. Wait for the report to terminate and collect all generated reports.
Prerequisites

- You know the cluster type or list of nodes to run on.
- You have installed the sos package on all systems.
- You have ssh keys for the root account on all the systems, or you can provide the root password via the --password option.

Procedure

- Run the sos collect command and follow the on-screen instructions.

NOTE

By default, sos collect tries to identify the type of cluster it runs on to automatically identify the nodes to collect reports from.

a. You can set the cluster or nodes types manually with the --cluster or --nodes options.

b. You can also use the --master option to point the sos utility at a remote node to determine the cluster type and the node lists. Thus, you do not have to be logged into one of the cluster nodes to collect sos reports; you can do it from your workstation.

c. You can add the --upload option to transfer the sos report to Red Hat immediately after generating it.

d. Any valid sos report option can be further supplied and will be passed to all sos reports executions, such as the --batch and --clean options.

[root@primary-rhel9 ~]# sos collect --nodes=sos-node1,sos-node2 -o process,apache --log-size=50

sos-collector (version 4.2)

This utility is used to collect sosreports from multiple nodes simultaneously. It uses OpenSSH’s ControlPersist feature to connect to nodes and run commands remotely. If your system installation of OpenSSH is older than 5.6, please upgrade.

An archive of sosreport tarballs collected from the nodes will be generated in /var/tmp/sos.o4l55n1s and may be provided to an appropriate support representative.

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 configuration changes will be made to the system running this utility or remote systems that it connects to.

Press ENTER to continue, or CTRL-C to quit

Please enter the case id you are collecting reports for: <8-digit_case_number>

sos-collector ASSUMES that SSH keys are installed on all nodes unless the
--password option is provided.

The following is a list of nodes to collect from:
.primary-rhel9
.sos-node1
.sos-node2

Press ENTER to continue with these nodes, or press CTRL-C to quit

Connecting to nodes...

Beginning collection of sosreports from 3 nodes, collecting a maximum of 4 concurrently

.primary-rhel9 : Generating sosreport...
sos-node1  : Generating sosreport...
sos-node2 : Generating sosreport...
.primary-rhel9 : Retrieving sosreport...
sos-node1  : Retrieving sosreport...
.primary-rhel9 : Successfully collected sosreport
sos-node1  : Successfully collected sosreport
.sos-node2 : Retrieving sosreport...
sos-node2 : Successfully collected sosreport

The following archive has been created. Please provide it to your support team.


[root@primary-rhel9 ~]#

Verification steps

- Verify that the sos collect command created an archive in the /var/tmp/ directory matching the description from the command output.

[root@primary-rhel9 ~]# ls -l /var/tmp/sos-collector*

Additional resources

- For examples on using the --batch and --clean options, see Generating an sos report from the command line.

1.5. CLEANING AN SOS REPORT

The sos utility offers a routine to obfuscate potentially sensitive data, such as user names, host names, IP or MAC addresses, or other user-specified keywords. The original sos report or sos collect stays unchanged, and a new *-obfuscated.tar.xz file is generated and intended to be shared with a third party.
NOTE

You can append the cleaner functionality to the sos report or sos collect commands with the --clean option:

[user@server1 ~]$ sudo sos report --clean

Prerequisites

- You have generated an sos report or an sos collect tarball.

- (Optional) You have a list of specific keywords beyond the user names, host names, and other data you want to obfuscate.

Procedure

- Run the sos clean command on either an sos report or sos collect tarball and follow the on-screen instructions.

  a. You can add the --keywords option to additionally clean a given list of keywords.

  b. You can add the --usernames option to obfuscate further sensitive user names.

  The automatic user name cleaning will automatically run for users reported through the lastlog file for users with an UID of 1000 and above. This option is used for LDAP users that may not appear as an actual login, but may occur in certain log files.

[user@server1 ~]$ sudo sos clean /var/tmp/sos-collector-2022-05-15-pafsr.tar.xz
[sudo] password for user:
sos clean (version 4.2)

This command will attempt to obfuscate information that is generally considered to be potentially sensitive. Such information includes IP addresses, MAC addresses, domain names, and any user-provided keywords.

Note that this utility provides a best-effort approach to data obfuscation, but it does not guarantee that such obfuscation provides complete coverage of all such data in the archive, or that any obfuscation is provided to data that does not fit the description above.

Users should review any resulting data and/or archives generated or processed by this utility for remaining sensitive content before being passed to a third party.

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

Found 4 total reports to obfuscate, processing up to 4 concurrently

sosreport-primary-rhel9-2022-05-15-nchbdmd : Extracting...
sosreport-sos-node1-2022-05-15-wmlomgu : Extracting...
sosreport-sos-node2-2022-05-15-obsudzc : Extracting...
sos-collector-2022-05-15-pafsr : Beginning obfuscation...
sosreport-sos-node1-2022-05-15-wmlomgu : Beginning obfuscation...
sosreport-primary-rhel9-2022-05-15-nchbdmd : Beginning obfuscation...
sosreport-sos-node2-2022-05-15-obsudzc : Beginning obfuscation...
sosreport-primary-rhel9-2022-05-15-nchbdmd : Re-compressing...
sosreport-sos-node2-2022-05-15-obsudzc : Re-compressing...
sosreport-sos-node1-2022-05-15-wmlomgu : Re-compressing...

Successfully obfuscated 4 report(s)

A mapping of obfuscated elements is available at

The obfuscated archive is available at

Size   157.10KiB
Owner  root

Please send the obfuscated archive to your support representative and keep the mapping file private

Verification steps

- Verify that the sos clean command created an obfuscated archive and an obfuscation mapping in the /var/tmp/ directory matching the description from the command output.

  [sudo] password for user:

- Check the *-private_map file for the obfuscation mapping:

  [user@server1 ~]$ sudo cat /var/tmp/sos-collector-2022-05-15-pafsr-private_map
  [sudo] password for user:

  {
  "hostname_map": {
    "pmoravec-rhel9": "host0"
  },
  "ip_map": {
    "10.44.128.0/22": "100.0.0.0/22",
    ...
  },
  "username_map": {
    "foobaruser": "obfuscateduser0",
    "jsmith": "obfuscateduser1",
    "johndoe": "obfuscateduser2"
  }
  }
1.6. 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 sos report 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 sos report 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 sos report --encrypt-pass my-passphrase
   [sudo] password for user:

   sosreport (version 4.2)

   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.

1. (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 sos report utility.

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

2. 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-server1-12345678-2022-01-24-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 sos report utility created an archive meeting the following requirements:
   - Filename starts with `secured`.
   - Filename ends with a `.gpg` extension.
   - Located in the `/var/tmp/` directory.

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

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.

   ```bash
   [user@server1 ~]$ sudo gpg --output decrypted-sosreport.tar.gz --decrypt /var/tmp/secured-sosreport-server1-12345678-2022-01-24-ueqijfm.tar.xz.gpg
   ```
   b. When prompted, enter the passphrase you used to encrypt the archive.

   | Enter passphrase | <OK> <Cancel> |
   | Passphrase: `<passphrase>` | |
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.

### 1.7. 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 `sos report` 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 `sos report` 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.

```
[user@server1 ~]$ sudo sos report --encrypt-key root
[sudo] password for user:
sosreport (version 4.2)
```

**NOTE**

The user running the `sos report` 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 `sos report` command, the keyring must also be set up using `sudo`, or the user must have direct shell access to that account.
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.

1. (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 sos report utility.

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

2. 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-zhdqhdhdi.tar.xz.gpg

Size 15.44MiB
Owner root
md5 ac62697e33f3271dbda92290583d1242

Please send this file to your support representative.

Verification steps

1. Verify that the sos report 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-zhdqhdhdi.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-zhdqhdhdi.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>"
```

```
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](#).

## 1.8. 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
```
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.

```bash
[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.

```bash
[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>
```

6. Confirm the correct passphrase by entering it again.

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

7. 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.
1.9. 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 sos report 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.

```bash
[user@server1 ~]$ sudo sos report --upload
[sudo] password for user:

sosreport (version 4.2)

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.
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.)