Oracle Linux 9

Using sos to Get Debugging Information

G24431-04
December 2025

Oracle Linux 9 Using sos to Get Debugging Information,

G24431-04

Contents

Preface

Oracle Linux 9: Using sos to Get Debugging Information describes how to use the `sos` utility to gather system information and debug information reports for troubleshooting purposes.

1

About the sos Command

The `sos` command collects information about a system such as hardware configuration, software configuration, and operational state. You can also use the `sos report` command to enable diagnostics and analytical functions on the current system.

The generated report is useful in cases where you're being helped by Oracle Support in troubleshooting a problem in the system. The support representative can use the report to obtain an exact picture of the system, its resources, and all the applications and processes that exist in the system, and all other data that can help find the causes of the issues you're experiencing.

The `sos` utility requires the installation of the `sos` package. To install the package, type:

```
sudo dnf install sos
```

2

sos Command Reference

This table provides information about the `sos` command.

Action	Command	Description
Create the `sos` report.	`sos report`	Collects all diagnostic and configuration information from the system and rpm based installed package details, based on modules that have been enabled or disabled.
Hide sensitive information from the `sos` report.	`sos clean`	Obfuscates information in an existing report before it's supplied to Oracle Support.
Create a batch of `sos` reports.	`sos collect`	Runs the `sos report` command on several servers, nodes, or instances and then packages the results.

To obtain a list of options and arguments that you can use with the `sos` utility, run the following command:

```
sos report -h


optional arguments:
  -h, --help            show this help message and exit

Global Options:
  --batch               Do not prompt interactively
  --config-file CONFIG_FILE
                        specify alternate configuration file
...
```

Creating the sos Report

Create an sos report based on diagnostic and configuration information from the system and applications installed from the package manager.

To collect all diagnostic and configuration information from the system and rpm based installed package details, run the following command:

```
sudo sos report


sosreport (sosreport version)
...
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.
...
Press ENTER to continue, or CTRL-C to quit.
```

If you add the `--alloptions` and `--all-logs` options to the `sos report` command then `sos` adds logs from every enabled module, ignores file size limits, and fetches log files from nonstandard locations.

Unless you add the `--batch` option, the `sos` utility always prompts you to confirm whether to continue or to quit. If you press Enter to continue, you can use an optional prompt to specify a case ID for the report.

```
Optionally, please enter the case id that you are generating this report for
[]:
```

If you're generating the report as related to a specific troubleshooting case, you can enter the case ID at this prompt.

After you have provided information as prompted, the command proceeds to generate the report, which can take a considerable time to complete. At the end of the process, the screen displays a message similar to the following:

```
Your sosreport has been generated and saved in:
        /var/tmp/sosreport-hostname-case#-datestamp-ID.tar.xz

 Size   20.62MiB
 Owner  root
 sha256 428f7b4118acd2d349bb022946877d853aa0eefbb4d340af3839810dc634b8b7

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

The report is generated as an `xa`-compressed `tar` file in the `/var/tmp` directory. In the report's file name, the *ID* is dynamically created by the utility.

> **Important**
>
> As indicated before, the report can be useful in cases where you engage Oracle Support to diagnose and troubleshoot issues that you have observed in the system. However, the report contains sensitive information specific to your company. Ensure that you review the contents of the report and identify sensitive information before sending the report to any third-party.

Hiding Sensitive Information in an sos Report

Obfuscate information in an `sos` report before supplying it to Oracle Support.

To secure sensitive information before sending the report externally, you can use the `clean` functionality of the `sos` utility. This functionality tries to obfuscate any information in the report that's considered to be sensitive, such as the following information:

- IPv4 addresses and networks (network topologies are retained)

- MAC addresses
- Host names
- Usernames
- Any words or phrases that you specify with the `--keyword` option

To use the `sos clean` utility on a generated report, type the following command and follow the prompts that are displayed:

```
sudo sos clean /var/tmp/sosreport-hostname-case#-datestamp-ID.tar.xz


...
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.
```

At the end of the process, the screen displays a message similar to the following:

```
Successfully obfuscated 1 report(s)

A mapping of obfuscated elements is available at
    /var/tmp/sosreport-host0-2022-08-08-qxbegcn-private_map

The obfuscated archive is available at
    /var/tmp/sosreport-host0-2022-08-08-qxbegcn-obfuscated.tar.xz

    Size    3.62MiB
    Owner    root

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

The resulting report that has been scrubbed of sensitive information is also stored in `/var/tmp`. However, the file name itself is revised. The hostname is generic, and importantly, `obfuscated` is added to the file name so you can identify the clean version of the report.

> ⚠ **Caution**
>
> Consider the following about the `sos clean` utility:
>
> - The `clean` functionality is a best-effort method to identify and then mask sensitive information. However, `sos clean` doesn't guarantee that the coverage of the masking process is complete in a specific system.
> - Reports that are processed with the `sos clean` command obfuscate certain details which a third-party such as a support representative might need to provide better help when troubleshooting problems.
> - You must always audit archives and reports that are generated by the `sos` utility before sending any of these files externally.

To automatically clean any sos report that you create, use the following command syntax when generating a report:

```
sudo sos report --clean
```

For more information, see the sos-report(1) and sos-clean(1) manual pages. See also https://github.com/sosreport/sos/wiki.

Extra Sample Usages of the sos Command

Customize the output of sos reports by using extra sos command options.

The sos report command can also be used with other options. For example, to only list available plugins and plugin options in the report, type:

```
sudo sos report -l
```

The plugins that are displayed by the command are grouped according to the following sections:

- All enabled plugins
- All disabled plugins
- Available options for all the plugins
- Available plugin options

See the sos-report(1) manual page for information about how to enable or disable plugins and how to set values for plugin options.

You can also obtain only information specific to a problem area and specify options to tailor the report that's generated. For example, to record only information about Apache and Tomcat and to gather all the Apache logs, type:

```
sudo sos report -o apache,tomcat -k apache.log=on
```

To enable all the Boolean options for all the loaded plugins (excluding the rpm.rpmva plugin) and verify all packages:

```
sudo sos report -a -k rpm.rpmva=off
```

For more information, see the sos-report(1) and sos-clean(1) manual pages. See also https://github.com/sosreport/sos/wiki.

Creating a Batch of sos Reports

Create sos reports based on diagnostic and configuration information from several systems at the same time.

When several systems experience downtime, such as containers or instances in the same cluster, it can be useful to collect diagnostic information from all affected systems and collate them into the same report. You can do so by running the sos collect command, which batch runs the sos report command on each remote system that you specify.

To batch run the `sos report` command on three servers with password-less key-based SSH authentication configured and their IP addresses specified, run something similar to the following example command:

```
sos collect --nodes 192.0.2.0 192.0.2.1 192.0.2.2
```

To gain root access to log files on remote systems, add the `--become` option to the command. You can also add many of the same options as a single `sos report` command, such as `--batch`, `--alloptions`, and `--all-logs`.

After the reports are generated on each node, they're collected and output as an `xa`-compressed `tar` file in the `/var/tmp` directory on the same system from which the `sos collect` command was run.

To run the command for servers that require passphrases for SSH authentication, add the `--password-per-node` option:

```
sos collect --password-per-node --nodes 192.0.2.0 192.0.2.1 192.0.2.2
```

You can use `--password` instead of `--password-per-node` to supply the same SSH passphrase to every server instead of being prompted for a different passphrase each time, but reusing the same passphrase isn't considered good security practice. For more information about hardening Oracle Linux 9 systems, see Oracle Linux 9: Enhancing System Security.

For more information about configuring SSH access on Oracle Linux, see Oracle Linux: Connecting to Remote Systems With OpenSSH.

For more information about the `sos collect` command, such as how to elevate remote user permissions or automatically hide sensitive information, run the following helper command:

```
sos collect -h
```

Or see the `sos-collect(1)` manual page.

3
Reviewing Information Gathered by sosreport

Configure and review the collection of debugging information on Oracle Linux.

The `sos` command is automatically configured to collect hardware information, system configuration files, and log data. You can enable and disable modules to match data protection requirements.

> **Note**
>
> The module information that's provided in this table relates to `sos` 4.8. To verify the modules you have installed, run the `sos report` command. The output includes the version of the `sos` utility that you're running, and an up-to-date listing of included files is output to the `sos_reports/manifest.json` file.
>
> Disabling modules prevents the `sos` command from collecting certain details that might be needed for advanced troubleshooting, such as networking information.

Module	Information Type	Included Files
`anaconda`	Installation log files	• `/root/install.log` • `/root/install.log.syslog` • `/var/log/anaconda` • `/var/log/anaconda.*`
`auditd`	Audit log files	• `/etc/audit/auditd.conf` • `/etc/audit/audit.rules` • `/var/log/audit/*`
`boot`	System boot process details	• `/etc/milo.conf` • `/etc/silo.conf` • `/boot/efi/efi/redhat/elilo.conf` • `/etc/yaboot.conf` • `/boot/yaboot.conf`
`cron`	Root user `cron` commands	• `/etc/cron*` • `/etc/crontab` • `/var/log/cron` • `/var/spool/cron`
`cups`	Printer log files	• `/etc/cups/*.conf` • `/etc/cups/*.types` • `/etc/cups/lpoptions` • `/etc/cups/ppd/*.ppd` • `/var/log/cups/*`

Module	Information Type	Included Files
date	Context data	• /etc/localtime
devicemapper	Hardware details	
filesys	List of all files in use	• /proc/fs/* • /proc/mounts • /proc/filesystems • /proc/self/mounts • /proc/self/mountinfo • /proc/self/mountstats • /proc/[0-9]*/mountinfo • /etc/mtab • /etc/fstab
grub2	Kernel and system start-up configuration	• /boot/efi/EFI/*/grub.cfg • /boot/grub2/grub.cfg • /boot/grub2/grubenv • /boot/grub/grub.cfg • /boot/loader/entries • /etc/default/grub • /etc/grub2.cfg • /etc/grub.d/*
hardware	Hardware details	• /proc/interrupts • /proc/irq • /proc/dma • /proc/devices • /proc/rtc • /var/log/mcelog • /sys/class/dmi/id/* • /sys/class/drm/*/edid
host	Host identification	• /etc/sos.conf • /etc/hostid

Module	Information Type	Included Files
kernel	System log files	• /etc/conf.modules • /etc/modules.conf • /etc/modprobe.conf • /etc/modprobe.d • /etc/sysctl.conf • /etc/sysctl.d • /lib/modules/*/modules.dep • /lib/sysctl.d • /proc/cmdline • /proc/driver • /proc/kallsyms • /proc/lock* • /proc/buddyinfo • /proc/misc • /proc/modules • /proc/slabinfo • /proc/softirqs • /proc/sys/kernel/random/boot_id • /proc/sys/kernel/tainted • /proc/timer* • /proc/zoneinfo • /sys/firmware/acpi/* • /sys/kernel/debug/tracing/* • /sys/kernel/livepatch/* • /sys/module/*/parameters • /sys/module/*/initstate • /sys/module/*/refcnt • /sys/module/*/taint • /sys/module/*/version • /sys/devices/system/clocksource/*/available_clocksource • /sys/devices/system/clocksource/*/current_clocksource

Module	Information Type	Included Files
		• /sys/fs/pstore • /var/log/dmesg
libraries	List of shared libraries	• /etc/ld.so.conf • /etc/ld.so.conf.d/*
logs	System log files	• /etc/syslog.conf • /etc/rsyslog.conf • /etc/rsyslog.d • /run/log/journal/* • /var/log/auth.log • /var/log/auth.log.1 • /var/log/auth.log.2* • /var/log/boot.log • /var/log/dist-upgrade • /var/log/installer • /var/log/journal/* • /var/log/kern.log • /var/log/kern.log.1 • /var/log/kern.log.2* • /var/log/messages* • /var/log/secure* • /var/log/syslog • /var/log/syslog.1 • /var/log/syslog.2* • /var/log/udev • /var/log/unattended-upgrades
lvm2	Hardware details	
memory	Hardware details	• /proc/pci • /proc/meminfo • /proc/vmstat • /proc/swaps • /proc/slabinfo • /proc/pagetypeinfo • /proc/vmallocinfo • /sys/kernel/mm/ksm • /sys/kernel/mm/transparent_hugepage/enabled

Module	Information Type	Included Files
networking	Network identification	• /etc/dnsmasq* • /etc/host* • /etc/inetd.conf • /etc/iproute2 • /etc/network* • /etc/nftables • /etc/nftables.conf • /etc/nsswitch.conf • /etc/resolv.conf • /etc/sysconfig/nftables.conf • /etc/xinetd.conf • /etc/xinetd.d • /etc/yp.conf • /proc/net/* • /sys/class/net/*/device/numa_node • /sys/class/net/*/flags • /sys/class/net/*/statistics/*
pam	Sign-in security settings	• /etc/pam.d/* • /etc/security
pci	Hardware details	• /proc/bus/pci • /proc/iomem • /proc/ioports
process	List of all running processes and process details	• /proc/sched_debug • /proc/stat • /proc/[0-9]*/smaps
processor	Hardware details	• /proc/cpuinfo • /sys/class/cpuid • /sys/devices/system/cpu
rpm	Installed software packages	• /var/lib/rpm/* • /var/log/rpmpkgs
sar	Resource and usage data	• /var/log/sa/*
selinux	Security settings	• /etc/sestatus.conf • /etc/selinux • /var/lib/selinux
services	All defined system services	• /etc/inittab • /etc/rc.d/* • /etc/rc.local
ssh	SSH configuration	• /etc/ssh/ssh_config • /etc/ssh/sshd_config

Module	Information Type	Included Files
x11	GUI logs for the X Window System	• /etc/X11/* • /var/log/Xorg.*.log • /var/log/Xorg.*.log.old • /var/log/XFree86.*.log • /var/log/XFree86.*.log.old
yum	Installed software packages	• /etc/pki/consumer/cert.pem • /etc/pki/entitlement/*.pem • /etc/pki/product/*.pem • /etc/yum/* • /etc/yum.repos.d/* • /etc/yum/pluginconf.d/* • /var/log/dnf.log