NAME

systemd-journald.service, systemd-journald.socket, systemd-journald-dev-log.socket, systemd-journald-audit.socket, systemd-journald - Journal service

SYNOPSIS

systemd-journald.service

systemd-journald.socket

systemd-journald-dev-log.socket

systemd-journald-audit.socket

/lib/systemd/systemd-journald

DESCRIPTION

systemd-journald is a system service that collects and stores logging data. It creates and maintains structured, indexed journals based on logging information that is received from a variety of sources:

- Kernel log messages, via kmsg
- Simple system log messages, via the libc **syslog(3)** call
- Structured system log messages via the native Journal API, see **sd_journal_print(4)**
- Standard output and standard error of system services
- Audit records, via the audit subsystem

The daemon will implicitly collect numerous metadata fields for each log messages in a secure and unfakeable way. See **systemd.journal-fields(7)** for more information about the collected metadata.

Log data collected by the journal is primarily text-based but can also include binary data where necessary. All objects stored in the journal can be up to $2^{64}-1$ bytes in size.

By default, the journal stores log data in /run/log/journal/. Since /run/ is volatile, log data is lost at reboot. To make the data persistent, it is sufficient to create /var/log/journal/ where systemd-journald will then store the data:

mkdir -p /var/log/journal
systemd-tmpfiles --create --prefix /var/log/journal

See **journald.conf(5)** for information about the configuration of this service.

SIGNALS

SIGUSR1

Request that journal data from /run/ is flushed to /var/ in order to make it persistent (if this is enabled). This must be used after /var/ is mounted, as otherwise log data from /run is never flushed to /var regardless of the configuration. The **journalctl --flush** command uses this signal to request flushing of the journal files, and then waits for the operation to complete. See **journalctl(1)** for details.

SIGUSR2

Request immediate rotation of the journal files. The **journalctl --rotate** command uses this signal to request journal file rotation.

SIGRTMIN+1

Request that all unwritten log data is written to disk. The **journalctl --sync** command uses this signal to trigger journal synchronization, and then waits for the operation to complete.

KERNEL COMMAND LINE

A few configuration parameters from journald.conf may be overridden on the kernel command line:

systemd.journald.forward_to_syslog=, *systemd.journald.forward_to_kmsg=*,
systemd.journald.forward_to_console=, *systemd.journald.forward_to_wall=*
Enables/disables forwarding of collected log messages to syslog, the kernel log buffer, the system console or wall.

See **journald.conf(5)** for information about these settings.

ACCESS CONTROL

Journal files are, by default, owned and readable by the "systemd-journal" system group but are not writable. Adding a user to this group thus enables her/him to read the journal files.

By default, each logged in user will get her/his own set of journal files in /var/log/journal/. These files will not be owned by the user, however, in order to avoid that the user can write to them directly. Instead, file system ACLs are used to ensure the user gets read access only.

Additional users and groups may be granted access to journal files via file system access control lists (ACL). Distributions and administrators may choose to grant read access to all members of the "wheel" and "adm" system groups with a command such as the following:

setfacl -Rnm g:wheel:rx,d:g:wheel:rx,g:adm:rx,d:g:adm:rx /var/log/journal/

Note that this command will update the ACLs both for existing journal files and for future journal files created in the /var/log/journal/ directory.

FILES

/etc/systemd/journald.conf
   Configure **systemd-journald** behavior. See **journald.conf(5)**.

/run/log/journal/*machine-id*/*.journal, /run/log/journal/*machine-id*/*.journal˜, /var/log/journal/*machine-id*/*.journal, /var/log/journal/*machine-id*/*.journal˜
   systemd-journald writes entries to files in /run/log/journal/*machine-id*/ or /var/log/journal/*machine-id*/ with the ".journal" suffix. If the daemon is stopped uncleanly, or if the files are found to be corrupted, they are renamed using the ".journal˜" suffix, and **systemd-journald** starts writing to a new file. /run is used when /var/log/journal is not available, or when **Storage=volatile** is set in the **journald.conf(5)** configuration file.

/dev/kmsg, /dev/log, /run/systemd/journal/dev-log, /run/systemd/journal/socket, /run/systemd/journal/stdout
   Sockets and other paths that **systemd-journald** will listen on that are visible in the file system. In addition to these, journald can listen for audit events using netlink.

SEE ALSO

systemd(1), **journalctl(1)**, **journald.conf(5)**, **systemd.journal-fields(7)**, **sd-journal(3)**, **systemd-coredump(8)**, **setfacl(1)**, **sd_journal_print(4)**, **pydoc systemd.journal**