Investigate a Linux filesystem that became read-only

“Read-only file system” means a write was refused by the filesystem or mount. It is different from a normal file-permission error. A volume may have been deliberately mounted read-only, or the kernel may have restricted writes after detecting a problem. Preserve the evidence before trying to make the error disappear.

These checks suit Debian and Ubuntu guests. They do not assume the disk uses ext4, and they do not perform repairs. If a database or game server cannot save, notify its users and avoid repeated start attempts while the underlying cause is unclear.

Identify the actual mount

1. Use the existing directory containing the failing file. Replace the example application path:

```
findmnt -T /var/lib/myapp -o TARGET,SOURCE,FSTYPE,OPTIONS
lsblk -f
```

Record the source device, filesystem type and options. An `ro` option confirms that mount is read-only. An application can also run inside a container or service-specific mount namespace; a writable host mount does not prove the application sees the same view. Do not treat a read-only ISO image as a damaged data disk.

Read the kernel evidence

```
sudo journalctl -k -b --since "30 minutes ago" --no-pager
```

Find the first relevant message near the failure, not only the latest repeated application error. Record filesystem errors, I/O errors, device resets or a stated remount. For ext4, a configured

`errors=remount-ro` policy can switch the filesystem read-only after an error. That setting is not evidence that the original storage fault has been resolved.

If journal access is unavailable, note that limitation. An empty filtered log does not establish that the disk is healthy, especially after a reboot or log rotation. Keep timestamps with timezone information.

Separate configuration from damage

Compare the current mount with the intended entry in `/etc/fstab` and recent deployment changes. If only a container is affected, inspect its configured read-only setting and mount list. Avoid replacing the server configuration with a command copied from a different machine.

Do not force a read-write remount to bypass unexplained filesystem errors. Do not run a repair against an actively mounted data filesystem, or guess a device name for `fsck`. The correct repair depends on filesystem type, storage layout and whether the affected volume can be safely unmounted. Root-filesystem work may require a rescue environment and downtime.

Prepare the next action

Contact support with the mount output, source device, first kernel error and whether the guest is still responsive. State whether current backups exist. Ask for a recovery plan before restarting or repairing. After an approved repair, success means the expected mount remains writable, application saves work and new kernel errors stop appearing—not merely that a reboot cleared the screen.

Related CloudExa guides

- Check mounts and fstab
- Verify an existing backup

Technical references

- Upstream findmnt manual

- Kernel ext4 error handling
- Filesystem checking and repair manual

Revision #1
Created 2026-11-10 10:51:41 UTC by CloudExa Hosting Admin
Updated 2026-11-10 10:51:41 UTC by CloudExa Hosting Admin