# Drive Modification, Data Component DC0046

Archived: 2026-04-05 16:06:12 UTC

The alteration of a drive letter, mount point, or other attributes of a data storage device, which could involve reassignment, renaming, permissions changes, or other modifications. Examples:

- Drive Letter Reassignment: A USB drive previously assigned `E:\` is reassigned to `D:\` on a Windows machine.
- Mount Point Change: On a Linux system, a mounted storage device at `/mnt/external` is moved to `/mnt/storage`.
- Drive Permission Changes: A shared drive's permissions are modified to allow write access for unauthorized users or processes.
- Renaming of a Drive: A network drive labeled "HR_Share" is renamed to "Shared_Resources."
- Modification of Cloud-Integrated Drives: A cloud storage mount such as Google Drive is modified to sync only specific folders.

This data component can be collected through the following measures:

Windows Event Logs

- Relevant Events:
  - Event ID 98: Indicates changes to a volume (e.g., drive letter reassignment).
  - Event ID 1006: Logs permission modifications or changes to removable storage.
- Configuration: Enable "Storage Operational Logs" in the Event Viewer: `Applications and Services Logs > Microsoft > Windows > Storage-Tiering > Operational`

Linux System Logs

- Auditd Configuration: Add audit rules to track changes to mounted drives: `auditctl -w /mnt/ -p w -k drive_modification`
- Command-Line Monitoring: Use `dmesg` or `journalctl` to observe drive modifications.

macOS System Logs

- Unified Logs: Collect mount or drive modification events: `log show --info | grep "Volume modified"`
- Command-Line Monitoring: Use `diskutil` to track changes:

Endpoint Detection and Response (EDR) Tools

- Configure policies in EDR solutions to monitor and log changes to drive configurations or attributes.

SIEM Tools

- Aggregate logs from multiple systems into a centralized platform like Splunk to correlate events and alert on suspicious drive modification activities.

---