

Logdateien

Inhaltsverzeichnis

- [1 Typische Quellen](#)
- [2 Auswertung](#)
- [3 Betrieb](#)
- [4 Fazit](#)

Logdateien enthalten Ereignisse, Fehler und Statusinformationen von Systemen und Anwendungen. Sie sind zentral für Fehlersuche, Monitoring und Sicherheitsanalyse.

Logdateien dokumentieren, was auf einem System oder in einer Anwendung passiert. Sie helfen dabei, Fehler nachzuvollziehen, Angriffe zu erkennen und Betriebszustände zu bewerten.

1 Typische Quellen

[Logs](#) entstehen an vielen Stellen einer Infrastruktur.

- [Webserver-Logs](#) von [Apache](#) oder [Nginx](#).
- Systemlogs und journalctl bei [systemd](#).
- Anwendungslogs von CMS, Shops oder eigenen Diensten.
- Mail-, Datenbank- und Firewall-[Logs](#).

2 Auswertung

Gute Logauswertung beginnt mit Zeitstempeln, Kontext und passenden Filterbefehlen.

- Nach Fehlercodes und Warnungen suchen.
- Zeiträume eingrenzen.
- Zusammenhänge zwischen mehreren Diensten prüfen.

3 Betrieb

[Logs](#) müssen rotiert, geschützt und sinnvoll aufbewahrt werden.

- Logrotation verhindert volle Datenträger.
- Sensible Daten in [Logs](#) vermeiden.
- Zentrale Logsammlung erleichtert Analyse.

4 Fazit

Logdateien sind oft die wichtigste Informationsquelle bei Störungen. Wer [Logs](#) gut pflegt und auswertet, findet Probleme schneller und zuverlässiger.