Syslog

Inhaltsverzeichnis

Syslog ist der klassische Standard zum Senden und Sammeln von Logmeldungen in IP-Netzen. Geräte und Server schicken Events an zentrale Collector oder SIEM-Systeme.

1 Funktionsweise

Quellen senden priorisierte Meldungen (Facility/Severity) per UDP/TCP/TLS an einen Syslog-Server. Dort werden sie gespeichert, gefiltert und weitergeleitet.

- **RFC3164/5424:** Formate und Struktur
- **Transport:** UDP einfach, TCP/TLS zuverlässiger
- **Centralization:** eine Sicht auf viele Systeme

2 Typische Einsatzbereiche

- Firewalls, Switches, Linux-Server
- Zentrale Log-Archive und SIEM-Ingest
- Compliance-Aufbewahrung

3 Wichtige Hinweise

- UDP kann Pakete verlieren – kritische Logs absichern.
- Zeit (NTP) und Hostnamen für Korrelation pflegen.
- PII/Secrets in Logs vermeiden oder maskieren.

4 Fazit

Syslog ist das Arbeitspferd zentraler Logistik – einfach, weit unterstützt und Grundlage vieler Monitoring- und Security-Pipelines.