

[zurück](#)

# Syslog - Grundlagen

Syslog ist ein standardisiertes Protokoll zur zentralen Sammlung und Verwaltung von Logdaten. Es wird von fast allen Netzwerkgeräten, Linux-Servern, Firewalls, Routern und vielen Anwendungen unterstützt.

Ziel:

- Ereignisse zentral speichern
- schneller analysieren
- Fehler finden
- Security-Vorfälle erkennen

## Warum Syslog?

- Logs aus vielen Geräten an einem Ort gesammelt
- Erleichtert Fehlersuche und Monitoring
- Grundlage für SIEM- und Security-Analysen
- Zeitstempel & Prioritäten normiert
- Entlastet lokale Systeme

## Ports & Protokolle

Syslog kann drei Hauptvarianten nutzen:

| Protokoll | Port | Beschreibung                        |
|-----------|------|-------------------------------------|
| -----     | ---  | -----                               |
| UDP       | 514  | schnell, aber unzuverlässig         |
| TCP       | 514  | zuverlässig, verbindungsorientiert  |
| TLS       | 6514 | verschlüsselte, sichere Übertragung |

In Unternehmensnetzen:

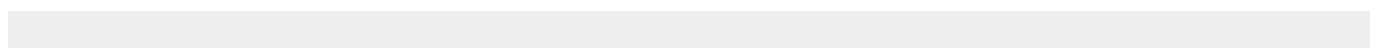
**Gerne TCP oder TLS statt UDP**, wegen Integrität.

## Aufbau einer Syslog-Nachricht

Ein klassischer Syslog-Eintrag besteht aus:

<facility.priority> timestamp hostname application: message

Beispiel:



```
<134>Jan 12 14:22:03 router1 DHCP: Assigned IP 192.168.10.25 to  
A4:5E:60:3B:7D:12
```

Bestandteile:

- **Facility** → Kategorie (z. B. auth, daemon, kern)
- **Severity** → Schweregrad (0–7)
- **Hostname**
- **Programm/Service**
- **Nachricht selbst**

## Severity Levels (0-7)

| Code | Name      | Bedeutung                 |
|------|-----------|---------------------------|
| ---  | -----     | -----                     |
| 0    | Emergency | System unbrauchbar        |
| 1    | Alert     | sofortige Maßnahmen nötig |
| 2    | Critical  | kritische Fehler          |
| 3    | Error     | Fehler                    |
| 4    | Warning   | Warnung                   |
| 5    | Notice    | wichtige, normale Meldung |
| 6    | Info      | informative Meldungen     |
| 7    | Debug     | detaillierte Debug-Infos  |

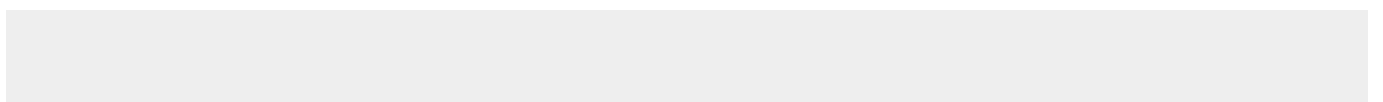
## Facilities

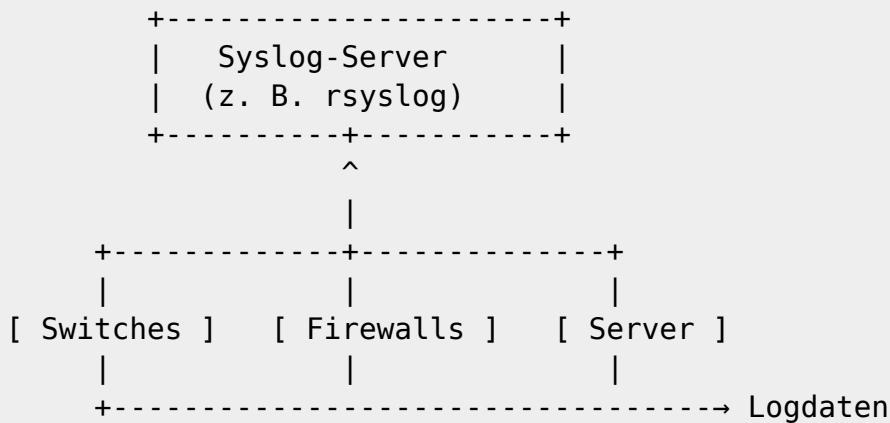
Beispiele:

| Facility | Bedeutung              |
|----------|------------------------|
| -----    | -----                  |
| kern     | Kernel                 |
| auth     | Authentifizierung      |
| daemon   | Hintergrunddienste     |
| local0-7 | frei für eigene Zwecke |
| mail     | Mailsysteme            |
| syslog   | interne Syslog-Events  |

## Systemaufbau mit zentralem Syslog-Server

ASCII-Übersicht:





Alle Systeme schicken ihre Logs **an einen zentralen Server**.

## Syslog unter Linux

Bekannte Implementierungen:

- rsyslog (Standard)
- syslog-ng
- journald (systemd-intern, kann weiterleiten)

Konfigurationsbeispiel (rsyslog):

```
*.* @@192.168.10.50:514
```

Bedeutung:

- @ = UDP
- \* @@ = TCP

## Syslog unter OPNsense / pfSense

Netzwerk → Logging → Syslog:

- Server-IP eintragen
  - Port 514 TCP oder 6514 TLS
  - \* Logtypen auswählen
  - \* Zertifikate laden (für TLS)

## Syslog für Switches (Cisco-Beispiel)

```
logging host 192.168.10.50
logging trap informational
logging facility local7
```

## Syslog für Docker / Container

Docker kann Syslog direkt nutzen:

```
docker run --log-driver=syslog --log-opt syslog-  
address=tcp://192.168.10.50:514 ...
```

Viele Admins zentralisieren:

- Suricata-Logs
  - \* CrowdSec-Events
  - \* Firewall/Iptables
  - \* Auth-Logs

## Sicherheitsaspekte

- UDP kann gefälscht werden → besser TCP/TLS
  - Logserver muss abgesichert sein
    - \* Logdaten können sensible Informationen enthalten
    - \* Rotation nötig (z. B. logrotate)
    - \* Uhren müssen per NTP synchron sein

## Syslog und SIEM

Syslog ist die Datenbasis für SIEM-Lösungen wie:

- Splunk
  - Graylog
    - \* ELK Stack (Elasticsearch, Logstash, Kibana)
    - \* Wazuh
    - \* CrowdSec + Loki
    - \* Grafana

## Log-Rotation

Unter Linux typisch:

```
/var/log/  
/var/log/syslog  
/var/log/auth.log  
/var/log/kern.log
```

Rotation:

```
/etc/logrotate.d/
```

## Zusammenfassung

- Syslog = Standard für Logübertragung
  - Ports: 514 (UDP/TCP), 6514 (TLS)
  - \* Severity Levels von 0–7
  - \* zentrale Logserver vereinfachen Monitoring & Security
  - \* in jeder professionellen Infrastruktur unverzichtbar
  - \* Grundlage für SIEM- und Analysewerkzeuge

From:

<http://wiki.nctl.de/dokuwiki/> - ☐ **Veni. Vidi. sudo rm -rf / vici.**

Permanent link:

<http://wiki.nctl.de/dokuwiki/doku.php?id=it-themen:grundlagen:netzwerkdienste:syslog&rev=1764591373>

Last update: **01.12.2025 13:16**

