**Aufbau CISCOSysLog**

bezogen auf Datei: **syslog\_generic.log**

Beispiel:

**<189>: Sep 27 2023 10:15:30.1234 UTC: %SYS-5-CONFIG\_I: Configured from console by admin on Router-1**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**1.**

**<189>:**

* **PRI-Feld (Priority)**
* Kodiert zwei Infos in einer Zahl

🡪 Quelle oder Kategorie der Nachricht [Kernel, Mail, Daemon usw.] (Facility)

🡪 Schweregrad der Nachricht [0 = Emergency, 7 = Debug] (Severity)

Berechnung des PRI Feldes:

PRI = (Facility × 8) + Severity

189/8 = 23, Rest 5

Facility = 23 (Ganzzahl-Quotient)

Severity = 5 (Rest)

**Facility (Quelle)**

| **Wert** | **Name** | **Bedeutung** |
| --- | --- | --- |
| 0 | kernel | Kernel-Meldungen |
| 1 | user | User-Level-Meldungen |
| 2 | mail | Mail-System |
| 3 | daemon | System-Daemons |
| 4 | auth | Sicherheits-/Autorisierungs-Msg. |
| 5 | syslog | Von syslogd erzeugte Meldungen |
| 6 | lpr | Drucksystem |
| 7 | news | Netzwerk-News |
| 8 | uucp | UUCP-System |
| 9 | cron | Zeitsteuerungs-Daemon |
| 10 | authpriv | Private Authentifizierung |
| 11 | ftp | FTP-Daemon |
| 12 | ntp | NTP-System |
| 13 | security | Log Audit |
| 14 | console | Log Alert |
| 15 | clock | Clock Daemon |
| 16 | local0 | Lokal verwendbar |
| 17 | local1 | Lokal verwendbar |
| 18 | local2 | Lokal verwendbar |
| 19 | local3 | Lokal verwendbar |
| 20 | local4 | Lokal verwendbar |
| 21 | local5 | Lokal verwendbar |
| 22 | local6 | Lokal verwendbar |
| 23 | local7 | Lokal verwendbar (oft Cisco) |

Einzelne Facility-Werte sind nicht grundsätzlich wichtiger als andere, hängt vom Kontext ab 🡪 Severity

**Severity (Schweregrad)**

| **Wert** | **Name** | **Bedeutung** |
| --- | --- | --- |
| 0 | Emergency | System unbenutzbar |
| 1 | Alert | Sofortiges Handeln erforderlich |
| 2 | Critical | Kritischer Zustand |
| 3 | Error | Fehler |
| 4 | Warning | Warnung |
| 5 | Notice | Bedeutende, normale Meldung |
| 6 | Informational | Information |
| 7 | Debug | Debug-/Detailmeldungen |

5-7 gelten als nicht so wichtige Werte, weil siehe Bedeutung

**#Filter einbauen, mit dem man wichtige PRI-Werte mit dem Rest 0-4 rausfiltern kann oder eben auch die unwichtigeren Werte 5-7**

**2.**

**Sep 27 2023 10:15:30.1234 UTC:**

* **Zeitstempel**
* Aufbau:
* Monat Tag Jahr Uhrzeit.Milisekunden Zeitzone:

Schreibweise Monate (englisch):

Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**3.**

**%SYS-5-CONFIG\_I:**

* **Syslog-Code**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**3.1**

**%** 🡪 Trennzeichen zur Kennzeichnung des Beginns des Syslog-Codes (Message Identifier/- Tag)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**3.2**

**SYS** 🡪 Facility (hier: Beschreibung des Subsystems/Funktionsbereich innerhalb des CISCO-Geräts, das die Meldung erzeugt hat)

Facilities, die in der o.g. Datei vorkommen (Reihenfolge):

| **Abkürzung** | **Bedeutung (englisch)** | **Bedeutung (deutsch)** |
| --- | --- | --- |
| **SYS** | System | Systemprozesse |
| **LINK** | Link | Schnittstellenstatus (Verbindung) |
| **SEC** | Security | Sicherheit |
| **BGP** | Border Gateway Protocol | Routing-Protokoll für große Netzwerke |
| **VPN** | Virtual Private Network | Virtuelles Privates Netzwerk |
| **INTERFACE** | Interface | Netzwerkschnittstelle |
| **OSPF** | Open Shortest Path First | Routing-Protokoll (OSPF) |
| **EIGRP** | Enhanced Interior Gateway Routing Protocol | Routing-Protokoll (EIGRP) |
| **VRRP** | Virtual Router Redundancy Protocol | Protokoll für Router-Redundanz |
| **HSRP** | Hot Standby Router Protocol | Protokoll für Router-Ausfallsicherheit |
| **VLAN** | Virtual Local Area Network | Virtuelles LAN |
| **SNMP** | Simple Network Management Protocol | Protokoll zur Netzwerkverwaltung |
| **PORTSEC** | Port Security | Schnittstellensicherheit |
| **ACL** | Access Control List | Zugriffskontrollliste |
| **DHCP** | Dynamic Host Configuration Protocol | Automatische IP-Adressvergabe |

Facilities im Syslog-Code sind dynamisch und wachsen mit neuen Software-Releases und Hardware-Plattformen. Eine vollständige Aufzählung aller je möglichen Cisco-Facilities existiert nicht öffentlich, da sie herstellerspezifisch und produktabhängig ist

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**3.3**

**5** 🡪 Severity (Siehe Punkt 1.)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**3.4**

**CONFIG\_I** 🡪 Mnemonic [Gedächtnishilfe] (Kurzbezeichnung des Ereignisses)

Mnemonics, die in der o.g. Datei vorkommen (Reihenfolge):

| **Mnemonic** | **Erklärung** |
| --- | --- |
| CONFIG\_I | Konfigurationsänderung wurde durchgeführt (z. B. durch Benutzer über Konsole) |
| UPDOWN | Der Status eines Interfaces hat sich geändert (z. B. von up auf down oder umgekehrt) |
| IPACCESSLOGP | Protokollierter Zugriff oder Zugriffsverletzung durch eine Access Control Policy |
| ADJCHANGE | Nachbarschaftsstatus eines Routing-Protokolls (z. B. BGP, EIGRP) hat sich geändert |
| CPUHOG | Ein Prozess verursacht eine ungewöhnlich hohe CPU-Auslastung (CPU-Hog) |
| USER\_LOGOUT | Ein Benutzer hat sich ausgeloggt |
| IKMP\_NO\_SA | Für eine IKE-Nachricht (VPN) konnte keine Security Association (SA) gefunden werden |
| ERROR\_DISABLED | Ein Interface wurde wegen eines Fehlers deaktiviert |
| ADJCHG | OSPF-Nachbarschaftsstatus hat sich geändert |
| LOGGING | Problem beim Logging, z. B. Log-Server nicht erreichbar |
| RESTART | Das System wurde neu gestartet |
| STATECHANGE | Statuswechsel eines Protokolls oder Dienstes (z. B. VRRP/HSRP State-Change) |
| SW2BASIC | Wechsel vom erweiterten in den Basismodus |
| STACKT | Stack-Topologie-Ereignis, z. B. neuer Master |
| PORT\_UP | Ein VLAN-Port ist aktiv geworden |
| TIMER | Ein Timer ist abgelaufen |
| AUTHFAIL | Authentifizierungsfehler (z. B. SNMP) |
| ROUTERBOOT | Das Gerät (Router) wird gebootet |
| VIOLATION | Sicherheitsverletzung erkannt (z. B. Port Security) |
| STACKM | Stack-Management-Ereignis, z. B. Stack-Einheit hinzugefügt |
| IPDENY | Zugriff wurde durch eine Access Control List (ACL) verweigert |
| PORTFLAP | Ein Port wechselt schnell und wiederholt zwischen up und down |
| ADDRESS\_ASSIGN | Eine IP-Adresse wurde per DHCP zugewiesen |
| INTERFACECHANGE | Interface-Status hat sich geändert (z. B. administrativ deaktiviert) |

Eine vollständige Tabelle aller möglichen Cisco-Mnemonics gibt es nicht, da es **hunderte verschiedene Mnemonics gibt und diese je nach Gerätemodell und Software-Version variieren**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**4.**

**Configured from console by admin on Router-1**

* **Message-Text**

sind sehr unterschiedlich

Beispiele:

| **Parameter** | **Beispiele aus der Logdatei** | **Bedeutung / Nutzen** |
| --- | --- | --- |
| **Benutzername** | **by admin** | **Wer hat eine Aktion ausgeführt?** |
| **Zugriffsart** | **from console** | **Wie wurde zugegriffen (z.B. Konsole, vty)?** |
| **Gerätename** | **on Router-1, on Router-2** | **Auf welchem Gerät fand das Ereignis statt?** |
| **Interface** | **Interface GigabitEthernet0/1, FastEthernet0/1, Serial0/0/0** | **Welches Interface ist betroffen?** |
| **Statusänderung** | **changed state to up, changed state to down, administratively down, error disabled, flapping** | **Statuswechsel oder Fehler am Interface** |
| **IP-Adresse** | **10.0.0.1 -> 192.168.1.1, Neighbor 192.168.2.2, assigned to client 00:0A:BC:DE:F0:01** | **Quelle, Ziel, Nachbar, DHCP-Zuweisung** |
| **MAC-Adresse** | **assigned to client 00:0A:BC:DE:F0:01** | **Eindeutige Hardware-Adresse eines Geräts** |
| **Prozessname** | **process: HOG\_PROCESS** | **Welcher Prozess ist betroffen?** |
| **Protokoll** | **BGP, OSPF, EIGRP, VRRP, HSRP, SNMP, DHCP** | **Welches Netzwerkprotokoll ist beteiligt?** |
| **Protokollstatus** | **Down due to BGP Notification, OSPF neighbor ... went down, Grp 1 state Standby -> Active** | **Statusänderung eines Protokolls** |
| **VLAN** | **VLAN 20, port FastEthernet0/2 is up** | **VLAN-Zugehörigkeit** |
| **Stack/Cluster** | **Stack unit 2 switched to new master, Stack unit 3 has been added** | **Stack-/Cluster-Ereignisse** |
| **ACL-Name/Regel** | **IP deny from host 10.0.0.19 to 192.168.1.19** | **Zugriff durch Access Control List verweigert** |
| **Security Event** | **Security violation on interface FastEthernet0/4, SNMP authentication failure** | **Sicherheitsrelevantes Ereignis** |
| **DHCP-Info** | **IP address ... assigned to client ...** | **DHCP-Vergabe von IP-Adressen** |
| **Timer/Ereignis** | **Timer 1 has expired on Router-15** | **Ablauf von Timern** |
| **Systemereignis** | **System restarted, Router-16 is booting up** | **Neustart, Boot, Moduswechsel** |
| **Logging-Status** | **Logging to host 192.168.4.1 failed - Host unreachable** | **Logging-Problem** |