Logging

In diesem Kapitel erfahren Sie

- wohin Cisco Geräte Logmeldungen und Debugmeldungen schreiben und wohin diese Meldungen zusätzlich geschrieben werden können
- wie Logmeldungen nach dem SYSLOG Standard in unterschiedliche Wichtigkeitsstufen (Log Level) eingeteilt werden
- wie Zeitstempel für die Ausgabe von Log- und Debugmeldungen angepasst werden können
- wie unterschiedliche Ausgabeziele für Logmeldungen – Console, Monitor (VTY Terminal), Puffer im RAM, remote SYSLOG Server – aktiviert und konfiguriert werden können:

Überblick

Während ein Gerät läuft, werden System- und Status Meldungen – nach SYSLOG Standard – mitprotokolliert.
HINWEIS: Ausgaben von debug Kommandos sind ebenfalls Logmeldungen (des Log Level 7).

Die Ausgabe der Logmeldugen erfolgt in der Standardeinstellung nur auf die Konsole.
Über unterschiedliche Logging Funktionen können Logmeldungen jedoch auch an andere Ausgabeziele gesendet werden:

- Terminal (Fenster einer VTY Session)
- Puffer im RAM
- Remote SYSLOG Server

SYSLOG – System Logging und Log Level

Eigenschaften

- Standard zur Verwaltung von Logmeldungen
- Cient/Server Dienst
- OSI 7 Protokoll
- Verwendet UDP Port 514
- Server nimmt Logmeldungen von Geräten (Client) entgegen und sichert sie dauerhaft in einer Textdatei.

Im SYSLOG Standard werden die Logmeldungen in unterschiedliche Log Level einsortiert. Dabei gilt: jedes Log Level enthält spezifische Meldungen und die Meldungen der untergeordneten, niedrigeren Log Level.

Level	Name	Bedeutung
7	**debugging**	Debugging Nachrichten
6	**informational**	Informelle Nachrichten
5	**notifications**	Normale, jedoch bedeutungsvolle Nachrichten
4	**warnings**	Warnmeldungen
3	**errors**	Fehlermeldungen
2	**critical**	kritischen Fehlermeldungen
1	**alerts**	Sofortiges administratives Eingreifen notwendig
0	**emergencies**	Das System in nicht verwendbar

In welches Log Level Cisco bestimmte Logmeldungen einsortiert, ist innerhalb der Log Meldung an der ausgegebenen Ziffer erkennbar. So wird z.B. der Ausfall einer Schnittstelle von Cisco in das Log Level 5 "notifications" einsortiert:

*%LINEPROTO-**5**-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to down*

Die Ausgabe von Logmeldungen kann durch administrative Änderung des voreingestellten Log Level angepasst werden.
HINWEIS: Die voreingestellten Log Level der unterschiedlichen Log Funktionen eines Cisco Geräts sind auch empfehlenswerte Einstellungen, d.h. eine admistrative Änderung ist i.d.R. nicht erforderlich.

Logging Funktionen und Konfiguration

Logmeldung werden in der default Einstellung auf der Console ausgegeben.
Sie können – und sollten - jedoch auch an andere Ausgabeziele gesendet werden.

Dabei ist eine Anpassung der Zeitstempel auf die lokale Zeit sinnvoll.

Die Voreinstellung für die Zeitstempel ist entweder UTC Zeit (datetime) oder die Uptime (uptime) des Geräts.

Zusätzlich wird i.d.R. auch der Zeitstempel für die Ausgaben von Debug Meldungen angepassen. Generell sind debug Meldung jedoch auch Log Meldungen → Log Level 7 Nachrichten.

(config)# **service timestamps log datetime localtime** [**msec**]
(config)# **service timestamps debug datetime localtime** [**msec**]

Console logging

Ausgabe: auf die Console (aktives Fenster der Konsoleverbindung)
default Einstellung: aktiv – Log Level 7

Das Console Logging kann administrativ deaktiviert werden bzw. es kann ein anderes Log Level zugeordnet werden.

(config)# [**no**] **logging console** [*level*]

TIPP: Dies kann zum Beispiel bei intensivem Debugging empfehlenswert sein.
Cisco empfiehlt debug Kommandos innerhalb einer Remote SSH Session zu verwenden und das Debugging auf der Console zu unterbinden, da Console Debugging die höchste Priorität hat und sehr CPU-intensiv sein kann. Intensives Debugging auf der Console kann somit zu Systemausfällen führen.
Um die Ausgabe von Debug Meldung zu unterbinden – aber allen anderen Log Meldungen weiterhin sehen zu können – wird das Log Level auf "notifications" geändert.

(config)# **logging console 6**

Verifikation der Konfiguration

show logging

Monitor logging

Ausgabe: auf das Terminal (aktives Fenster einer VTY Verbindung via Telnet oder SSH)
default Einstellung: nicht aktiv – Log Level 7

Aktivierung und Deaktivierung der Monitor Logging Funtion innerhalb einer aktiven Session. Gilt nur für die aktuelle Session – nach Beendigung der Session wird das Monitorig automatisch mit der Session terminiert.

ACHTUNG: Nur wenn das Monitor Logging aktiviert wurde, werden Log- und Debug Meldungen auf dem Terminal ausgeben

```
# terminal monitor          → aktivieren
# terminal no monitor       → wieder deaktivieren
```

Optional: Anpassung des voreingestellen Log Level 7 (nicht empfehlenswert)

```
(config)# logging monitor level
```

TIPP: Debugging
Empfehlung: nach Eingabe von terminal monitor, das Debugging auf einer VTY Line durchführen und aus Sicherheitsgründen Console Logging auf Level 6 beschränken .. siehe Console Logging.

Verifikation der Konfiguration

```
# show logging
```

Buffer logging

Ausgabe: in einen Puffer im RAM Speicher
default Einstellung: unterschiedlich – Log Level 7

Beim Buffer Logging werden Log- und Debug-Meldungen in einen festgelegten **Speicherbereich des RAM** (Puffer) geschrieben.
Default Puffergröße: 4096 Bytes – Platz für ca. 50-70 Log Meldungen.

Wenn der Puffer voll ist, wird das "**first in – first out**" Prinzip angewendet: die ältesten Meldungen werden durch die neuesten Meldungen ersetzt.

TIPP: die Aktivierung des Buffer Logging ist äusserst empfehlenswert,

- da man sich effizient einen Überblick über die letzten ausgegeben Logmeldungen verschaffen kann
- da man über den Puffer die Ausgaben von Debug Meldungen in Ruhe betrachten kann (.. wenn für des Buffer Logging das default Log-Level 7 eingestellt ist)

Die **Größe des Puffers** kann und sollte bei der Konfiguration/Aktivierung durchaus erhöht werden, sollte jedoch nicht zu groß ausfallen – grundsätzlich könnte der Admin dem Puffer nahezu sämtlichen RAM Speicher zuordnen .. dann können allerdings andere notwendige Funktionen nicht mehr durchgeführt werden.
Ein Verdopplung der Puffergrösse ist i.d.R. ausreichend und verursacht keinerlei Probleme.

Aktivierung des Buffer Logging mit optionaler Angabe der Puffergrösse in Bytes (z.B. 8192) und optionaler Anpassung des voreingestellen Log Level

```
(config)# logging buffered [ bytes ] [ level ]
```

Anzeige des NUR des Pufferinhalts (ohne Filterung gibt das show Kommando zuerst Informationen zu den Logging Einstellungen aus) und Leeren des Pufferinhalts

```
# show logging | begin Log Buffer     → zeigt NUR den Inhalt des Log Buffers
# clear logging                       → Leert den Puffer
```

Verifikation der Konfiguration

```
# show logging
```

Trap logging

Ausgabe: an einen remote SYSLOG Server
default Einstellung: nicht aktiv – Log Level 6

Das Cisco Geräte sendet nach Aktivierung des Trap Logging Logmeldungen an den angegebenen SYSLOG Server. Dazu wird der Standard UDP Port 514 verwendet.
Der SYSLOG Server speichert die Meldungen dann in einer Text-Datei.

Zur Aktivierung muss lediglich die IP Adresse des SYSLOG Servers angegeben werden

(config)# **logging** *IP*

.. oder für IPv6 (in dieser Syntax aber auch für IPv4 möglich)

(config)# **logging host** { *IP* | *IPv6* }

Optionale Einstellungen:

→ Anpassung des voreingestellen Log Level (default 6 – debug Meldungen werden nicht übertragen)

(config)# **logging trap** *level*

→ Senden einer bestimmten SYSLOG Facility an den Server.
Ein Facility ist eine bestimmte, standarisierte Bezeichnung, die vom Server ausgewert wird, d.h. wenn der verwendet SYSLOG Server (-Adminstrator) eine bestimmte Facility erwartet, sollte diese auch gesendet werden.
Generell frei nutzbare und daher oft genutzte Facilities sind: local0 bis local7.

(config)# **logging facility** *facility*

→ Das folgende Kommando bewirkt, dass das Cisco Gerät zusätzlch seinen Hostname in Log Meldungen schreibt, wenn sie an den SYSLOG Server gesendet werden.

(config)# **logging origin-id hostname**

→ SRC IP für die Kommunikation mit dem SYSLOG Server bestimmen (oftmals wird die IP bzw. IPv6 auf einem existenten Loopback Interface verwendet)

(config)# **logging source-interface** *IF-ID*

Weitere sinnvolle Logging Funktionen

Es existieren eine Reihe weiterer Einstellung für die Logging Funktion auf einem Cisco Geräte.

- Sehr empfehlenswert die generelle Anpassung der Ausgaben im SubConfiguration Mode der Console Line und der VTY Lines .. siehe auch Kapitel "Grundkonfiguration – Part I":
  - automatische Erzeugung eines Zeilenumbruchs nach Ausgabe der letzten Log Meldung
  - Ausgabe von Log Meldungen bei Eingaben verhindern – Log Meldung werden nur ausgegeben, wenn gerade keine Eingaben auf der CLI stattfinden

    (config-line)# **logging synchronous**

- Anzeige von Benutzer-Informationen beim Wechsel in den PrivilegeEXEC Mode oder generell beim Wechsel zwischen EXEC Leveln aktivieren

    (config)# **logging user-info**

- Anzeige von Benutzer-Informationen bei Login aktivieren (Ciscos Login Enhancements)

    (config)# **login on-access log**
    (config)# **login on-failure log**

Übersicht - Empfehlenswertes zum Logging/Debugging

Zeitstempel	
für alle Log Level auf lokale Zeit anpassen	(config)# **service timestamps log datetime localtime msec** (config)# **service timestamps debug datetime localtime msec**
Logging	
Ausgabe von Log Meldungen optimieren	(config-line)# **logging synchronous**
Buffer Logging aktivieren Inhalte anzeigen → Inhalte löschen →	(config)# **logging buffered 8192** # **show logging | begin Log Buffer** # **clear logging**
Trap Logging aktivieren .. existenter SYSLOG Server vorausgesetzt ;)	(config)# **logging host** { *IP* | *IPv6* } <u>Oft verwendet</u> (config)# **logging facility local**0 (config)# **interface loopback** 0 (config-if)# **ip address** *IP* 255.255.255.255 (config-if)# **ipv6 address** *IPv6*/128 .. und (config)# **logging source-interface loopback** 0 (config)# **logging origin-id hostname**
Einstellungen verifizieren	# **show logging**
Aktives Debugging	
Debug Meldungen auf Console verhindern	(config)# **logging console 6**
Remote Session über VTY Line (z.B. SSH) starten und nach Login ..	PC> **ssh -l** *username IP*
.. Monitor Logging aktivieren (!)	# **terminal monitor**
.. Debugging starten	# **debug** { **kommando** }

Selbstkontrolle – Aufgaben und Übungen

1. In welches Log Level ordnet ihr Cisco Router die Logmeldung über die Aktivierung einer Schnittstelle (mit no shutdown) ein?

2. Welche Bezeichnung hat Log Level 6 nach SYSLOG Standard?

3. In welches Log Level (Nummer und Name) werden die Ausgaben von debug Kommandos eingegliedert?

4. Sie sind über eine SSH Verbindung mit einem Cisco Router verbunden und wollen mit einem debug Kommando die Veränderungen innerhalb der Routing Tabelle in Echtzeit überwachen. Nach Eingabe des entsprechenden debug Kommandos (# debug ip routing) werden jedoch keine Meldungen auf den Bildschirm geschrieben, obwohl eine Veränderung innerhalb der Routing Tabelle eingetreten ist. Welches Kommando muss im PrivilegeEXEC Mode verwendet werden, damit die Ausgaben auf den Bildschirm geschrieben werden?

5. Mit welchem Kommando wird das Buffer Logging aktiviert und gleichzeitig die Puffergröße auf 16384 Bytes eingestellt? Notieren sie das Kommando inklusive Prompt.

6. Welches OSI 4 Protokoll wird für die Übertragung von Logmeldungen nach SYSLOG Standard verwendet und an welchen Zielport werden die Daten geschickt?

7. Welches der folgenden Kommandos aktiviert das Senden von Logmeldungen an den SYSLOG Server fdfd::a?

- ○ logging fdfd::a
- ○ ipv6 logging fdfd::a
- ○ logging host fdfd::a
- ○ logging ipv6 fdfd::a

Selbstkontrolle – Lösungen

1. In welches Log Level ordnet ihr Cisco Router die Logmeldung über die Aktivierung einer Schnittstelle (mit no shutdown) ein?

Log Level 5 "Notifications"

2. Welche Bezeichnung hat Log Level 6 nach SYSLOG Standard?

Informational

3. In welches Log Level (Nummer und Name) werden die Ausgaben von debug Kommandos eingegliedert?

Log Level 7 "debugging"

4. Sie sind über eine SSH Verbindung mit einem Cisco Router verbunden und wollen mit einem debug Kommando die Veränderungen innerhalb der Routing Tabelle in Echtzeit überwachen. Nach Eingabe des entsprechenden debug Kommandos (# debug ip routing) werden jedoch keine Meldungen auf den Bildschirm geschrieben, obwohl eine Veränderung innerhalb der Routing Tabelle eingetreten ist. Welches Kommando muss im PrivilegeEXEC Mode verwendet werden, damit die Ausgaben auf den Bildschirm geschrieben werden?

 # terminal monitor

5. Mit welchem Kommando wird das Buffer Logging aktiviert und gleichzeitig die Puffergröße auf 16384 Bytes eingestellt? Notieren sie das Kommando inklusive Prompt.

(config)# logging buffered 16384

6. Welches OSI 4 Protokoll wird für die Übertragung von Logmeldungen nach SYSLOG Standard verwendet und an welchen Zielport werden die Daten geschickt?

UDP Port 514

7. Welches der folgenden Kommandos aktiviert das Senden von Logmeldungen an den SYSLOG Server fdfd::a?

- O logging fdfd::a
- O ipv6 logging fdfd::a
- xO logging host fdfd::a
- O logging ipv6 fdfd::a