Syslog telepítése és konfigurálása Debian 12 rendszeren

A **syslog** egy naplózási rendszer, amely a rendszer- és alkalmazáseseményeket naplózza egy központi fájlba vagy egy távoli szerverre. Debian 12 rendszeren a **rsyslog** az alapértelmezett syslog-szolgáltatás.

---

1. Rsyslog telepítése

A legtöbb Debian 12 rendszeren a **rsyslog** alapértelmezetten telepítve van. Ha mégsem lenne:

```
sudo apt update
sudo apt install rsyslog -y
```

Ellenőrizzük, hogy fut-e a szolgáltatás:

```
systemctl status rsyslog
```

---

2. Alapvető naplózási konfiguráció

A **rsyslog** konfigurációs fájlja: `/etc/rsyslog.conf`

A konfiguráció módosítása előtt érdemes készíteni róla egy biztonsági mentést:

```
sudo cp /etc/rsyslog.conf /etc/rsyslog.conf.bak
```

2.1. Helyi naplózás beállítása

A Debian rendszeren az alapértelmezett naplófájlok a **/var/log/** könyvtárban találhatók, például:

- **/var/log/syslog** – általános rendszerüzenetek
- **/var/log/auth.log** – hitelesítési események
- **/var/log/kern.log** – kernelüzenetek

2.2 Egyedi naplófájl beállítása egy alkalmazás számára

Nyissunk meg egy új rsyslog konfigurációs fájlt a **/etc/rsyslog.d/** mappában. Az elnevezése lehet például **appname.conf**, ahol **appname** az alkalmazás neve:

```
sudo nano /etc/rsyslog.d/appname.conf
```

Majd adjunk hozzá egy ilyen szabályt:

```
if $programname == 'appname' then /var/log/appname.log
& stop
```

Magyarázat:

- **$programname == 'appname'** → Az **appname** nevű program által küldött üzeneteket fogja el.
- **/var/log/appname.log** → Az üzenetek ebbe a fájlba kerülnek.
- **& stop** → Megakadályozza, hogy az üzenetek a **/var/log/syslog-ba** is bekerüljenek.

Hozzuk létre a naplófájlt az alkalmazás számára és állítsuk be megfelelő jogosultságokat:

```
sudo touch /var/log/appname.log
sudo chmod 644 /var/log/appname.log
```

Az új konfiguráció alkalmazásához indítsuk újra az rsyslog szolgáltatást:

```
sudo systemctl restart rsyslog
```

Az alkalmazás naplózásának engedélyezése a syslog számára

Az alkalmazásnak syslog kompatibilis naplózási funkcióval kell rendelkeznie.
Ha az alkalmazás nem küldi alapértelmezetten a naplóit a syslognak a következő utasítással ellenőrizhetjük a szolgáltatás működését:

```
logger -t appname "Ez egy teszt üzenet"
```

Nézzük meg, hogy az appname naplói bekerülnek-e a saját fájljukba:

```
tail -f /var/log/appname.log
```

3. Távoli naplózás engedélyezése (Syslog Server)

Ha a Debian 12 gépet syslog szerverként szeretnénk használni, hogy más gépek naplóit fogadja, engedélyezzük a távoli naplózást.

3.1. UDP vagy TCP engedélyezése

Szerkesszük az rsyslog.conf fájlt:

```
sudo nano /etc/rsyslog.conf
```

Keressünk rá ezekre a sorokra, és vegyük ki előlük a # jelet:

```
# provides UDP syslog reception
module(load="imudp")
input(type="imudp" port="514")

# provides TCP syslog reception
module(load="imtcp")
input(type="imtcp" port="514")
```

Ezután a szerver az 514-es **UDP és TCP porton** is fogadni fogja a syslog üzeneteket.

3.2. Távoli gépek naplóinak külön fájlba mentése

Ha azt szeretnéd, hogy minden beérkező logot külön fájlba mentse a rendszer az alapján, hogy melyik számítógépről jön, adjuk hozzá ezt a konfigurációs fájl végéhez:

```
$template RemoteLogs,"/var/log/remote/%HOSTNAME%/%PROGRAMNAME%.log"
*.* ?RemoteLogs
& stop
```

Ez beállítás létrehoz egy RemoteLogs nevű sablont, amely a log üzeneteket a **/var/log/remote/** könyvtárba menti, ahol minden egyes kliens külön könyvtárat kap.

- **%HOSTNAME%** → Az üzenetet küldő gép (távoli kliens) hostneve.
- **%PROGRAMNAME%** → Az alkalmazás neve, amely a naplóüzenetet küldte.
- ***.*** → Minden naplóüzenetet elfogad (**minden szint és minden forrás**).
- **?RemoteLogs** → Az üzenetek a korábban definiált RemoteLogs sablon szerint kerülnek mentésre.
- **&** → Az előző szabály folytatása.
- **stop** → Megakadályozza, hogy ezek a naplók más fájlokba is bekerüljenek (pl. /var/log/syslog)

Hozzuk létre a könyvtárat és adjunk neki megfelelő jogosultságokat:

```
sudo mkdir -p /var/log/remote
sudo chmod 755 /var/log/remote
sudo systemctl restart rsyslog
```

---

4. Távoli Debian kliens beállítása

Ha egy másik Debian 12 gépről szeretnénk naplókat küldeni a szerverre, akkor azon a gépen is telepíteni kell az **rsyslog**-ot:

```
sudo apt install rsyslog -y
```

Majd szerkeszteni kell az rsyslog.conf fájlt:

```
sudo nano /etc/rsyslog.conf
```

Adjuk hozzá a következő sort a fájl végéhez:

```
*.* @192.168.1.100:514    # UDP használata (egy @ jel)
*.* @@192.168.1.100:514   # TCP használata (két @ jel)
```

(Cseréljük ki a 192.168.1.100 címet a syslog szerver IP címére.)

Ezután indítsuk újra az rsyslog-ot a kliensen:

```
sudo systemctl restart rsyslog
```

Most a **syslog szerver** fogadni fogja ennek a kliensnek az üzeneteit.

5. A Cisco eszközök naplóinak külön fájlba mentése

A Debian syslog szerver alapértelmezetten a **/var/log/syslog** fájlba menti az összes naplóüzenetet, de a Cisco eszközök üzeneteit egy külön fájlba is irányíthatjuk.

Nyissuk meg a **/etc/rsyslog.d/** könyvtárban egy új konfigurációs fájlt:

```
sudo nano /etc/rsyslog.d/cisco.conf
```

Adjuk hozzá a következő sorokat:

```
$template CiscoLogs,"/var/log/cisco/%FROMHOST%.log"
if $fromhost-ip startswith '192.168.1.' then ?CiscoLogs
& stop
```

Magyarázat:

- A CiscoLogs sablont definiálja, amely az üzeneteket a **/var/log/cisco/** könyvtárba menti, minden eszközt külön fájlba.
- Ha a küldő eszköz IP-címe 192.168.1.X, akkor az üzeneteket az adott fájlba menti.
- A & stop biztosítja, hogy ezeket az üzeneteket ne másolja a rendszer más naplófájlokba.

Mentés után hozzuk létre a könyvtárat és állítsuk be a jogosultságokat:

```
sudo mkdir -p /var/log/cisco
sudo chmod 755 /var/log/cisco
```

Indítsuk újra az rsyslog szolgáltatást:

```
sudo systemctl restart rsyslog
```

5.1 Cisco IOS eszköz beállítása syslog üzenetek küldésére

Syslog szerver beállítása: syslog üzenetek küldése a 192.168.1.100 című szerverre

```
logging host 192.168.1.100 transport udp port 514
```

TCP helyett UDP használata: `logging host 192.168.1.100 transport tcp port 514`

Naplózási szint beállítása

A Cisco eszközök többféle naplózási szinttel rendelkeznek. A naplózási szintet a következő paranccsal lehet módosítani: `logging trap <szint>`

Például a következő parancs beállítja, hogy a részletesebb üzenetek is elküldésre kerüljenek a syslog szerverre: `logging trap informational`

Naplózási szintek:

- **0 (emergencies)** – Kritikus hibák
- **1 (alerts)** – Azonnali figyelmet igénylő üzenetek
- **2 (critical)** – Súlyos hibák
- **3 (errors)** – Általános hibák
- **4 (warnings)** – Figyelmeztetések
- **5 (notifications)** – Rendszeresemények
- **6 (informational)** – Általános információs üzenetek
- **7 (debugging)** – Hibakeresési információk

---

6. Naplófájlok ellenőrzése

6.1. Helyi naplók megtekintése

```
sudo tail -f /var/log/syslog
```

6.2. Távoli gépek naplóinak ellenőrzése

```
ls /var/log/remote/
```

Ha a távoli kliensről naplók érkeznek, akkor itt kell látni a hosztnévnek megfelelő könyvtárat.
