PROIECT: Server Syslog Centralizat pentru Infrastructură Telecom

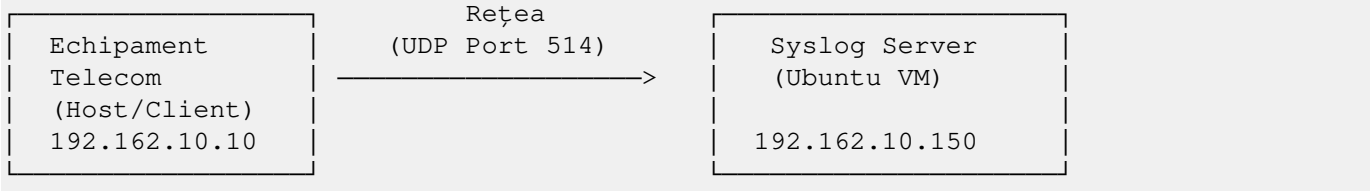
Timp estimat realizare 1 – 1.5 h

1. INTRODUCERE

1.1 Obiectivul proiectului

Implementarea unui server syslog centralizat pe o mașină virtuală Ubuntu Server, destinat colectării și organizării log-urilor de la echipamente de telecomunicații (telefoane IP, routere, servere VoIP).

1.2 Arhitectura sistemului



1.3 Tehnologii utilizate

• OS Server: Ubuntu Server 24.04 LTS
• Software: rsyslog (daemon syslog)
• Firewall: UFW (Uncomplicated Firewall)
• Protocol: UDP port 514 (standard syslog)
• Virtualizare: VirtualBox/VMware

2. CONFIGURARE REȚEA - SCENARII POSIBILE

2.1 SCENARIUL RECOMANDAT: Bridge Mode (Aceeași Rețea)

Caracteristici:

• Host și VM primesc IP-uri din aceeași rețea (ex: 192.162.10.0/24)
• Funcționează ca două calculatoare fizice separate
• Zero configurare extra
• Ideal pentru demo și producție

Configurare VirtualBox:

Pași:

1. Oprește VM-ul complet
```
sudo shutdown -h now
```

2. În VirtualBox Manager:
   • Selectează VM-ul → Settings
   • Network → Adapter 1
   • Attached to: Schimbă din "NAT" în "Bridged Adapter"
   • Name: Selectează interfața fizică (ex: "Ethernet", "Wi-Fi")
   • Advanced → Promiscuous Mode: "Allow All"
   • Click OK

3. Pornește VM-ul

4. Verifică IP-ul primit:
```
hostname -I
# Output așteptat: 192.162.10.150 (sau alt IP din aceeași rețea)
```

5. Test conectivitate de pe Host:
```
ping 192.162.10.150
# Trebuie să primești răspuns!
```

Avantaje Bridge Mode:

• **IP VM:** 192.162.10.150 (rețea reală) vs 10.0.2.15 (NAT intern)
• **Comandă logger:** logger -n 192.162.10.150 -P 514
• **Port forwarding:** Nu este necesar
• **Acces din alte device-uri:** Da
• **Complexitate:** Simplă

NOTĂ: Documentația continuă cu Bridge mode (scenariul recomandat).

3. CONFIGURARE SYSLOG SERVER (PE VM)

3.1 Instalare rsyslog

```
# Verificare instalare (pre-instalat pe Ubuntu)
dpkg -l | grep rsyslog

# Dacă lipsește (rar):
sudo apt update
sudo apt install rsyslog -y
```

3.2 Configurare rsyslog pentru recepție remote

Editare fișier de configurare:

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

Activare modul UDP (găsește și decomentează):

Înainte:

```
#module(load="imudp")
#input(type="imudp" port="514")
```

După (șterge #):

```
module(load="imudp")
input(type="imudp" port="514")
```

Adăugare template pentru organizare log-uri (la FINAL):

```
# Template pentru organizare după hostname și aplicație
$template RemoteLogs,"/var/log/remote/%HOSTNAME%/%PROGRAMNAME%.log"
*.* ?RemoteLogs
& stop
```

Explicație:
• %HOSTNAME%: Numele clientului care trimite log-ul
• %PROGRAMNAME%: Aplicația (ex: asterisk, router, firewall)
• & stop: Previne duplicarea în /var/log/syslog

Salvare și ieșire:
• Apasă Ctrl+O → Enter (salvează)
• Apasă Ctrl+X (ieșire)

3.3 Creare director și permisiuni

```
sudo mkdir -p /var/log/remote
sudo chown syslog:adm /var/log/remote
sudo chmod 755 /var/log/remote
```

3.4 Restart rsyslog

```
sudo systemctl restart rsyslog
sudo systemctl status rsyslog
```

Output așteptat:

```
● rsyslog.service - System Logging Service
     Active: active (running)
```

3.5 Verificare ascultare port 514

```
sudo netstat -uln | grep 514
```

Output corect:

```
udp   0   0  0.0.0.0:514   0.0.0.0:*
```

4. CONFIGURARE FIREWALL (UFW)

4.1 Activare UFW cu reguli implicite

```
sudo ufw default deny incoming
sudo ufw default allow outgoing
```

4.2 Permitere SSH (IMPORTANT!)

```
sudo ufw allow 22/tcp
```

4.3 Permitere syslog (UDP port 514)

```
sudo ufw allow 514/udp
```

4.4 Activare firewall

```
sudo ufw enable
```

Confirmare: Scrie 'y' și apasă Enter

4.5 Verificare reguli

```
sudo ufw status verbose
```

Output așteptat:

```
Status: active

To                         Action      From
--                         ------      ----
22/tcp                     ALLOW       Anywhere
514/udp                    ALLOW       Anywhere
```

5. TESTARE SISTEM

5.1 Test simplu de conectivitate

Pe Host (în Bridge mode):

```
logger -n 192.162.10.150 -P 514 "Test initial - server syslog functional"
```

Pe VM - verificare imediată:

```
sudo tail -f /var/log/remote/*/logger.log
```

Output așteptat:

```
Jan 19 16:30:15 host-desktop logger[1234]: Test initial - server syslog functional
```

5.2 Script de testare complet

Creare script pe Host:

```
nano test-syslog-telecom.sh
```

Conținut script:

```
#!/bin/sh
# Script de testare Syslog Server - Simulare Telecom

# CONFIGURARE (MODIFICĂ IP-ul VM-ului tău!)
VM_IP="192.162.10.150"    # Pentru Bridge mode
VM_PORT="514"             # Port standard syslog

echo "  Test Server Syslog - Infrastructură Telecom"
echo "  Trimit log-uri către: $VM_IP:$VM_PORT"
echo ""

# 1. SIMULARE CALL CENTER (Asterisk VoIP)
echo "  [1/5] Simulez apeluri telefonice (Asterisk)..."
logger -n $VM_IP -P $VM_PORT -t "asterisk" "INFO: CALL INITIATED 1001→1002"
logger -n $VM_IP -P $VM_PORT -t "asterisk" "INFO: CALL CONNECTED - Duration: 125s"
logger -n $VM_IP -P $VM_PORT -t "asterisk" "INFO: CALL ENDED - Total cost: 3.50 RON"
sleep 1

# 2. MONITORIZARE ROUTER
echo "  [2/5] Simulez alerte router rețea..."
logger -n $VM_IP -P $VM_PORT -t "router" "WARNING: Interface eth0 high traffic - 85%"
logger -n $VM_IP -P $VM_PORT -t "router" "INFO: BGP neighbor 203.0.113.1 established"
logger -n $VM_IP -P $VM_PORT -t "router" "ERROR: Interface eth1 link down"
sleep 1

# 3. FIREWALL SECURITY
echo "  [3/5] Simulez evenimente firewall..."
logger -n $VM_IP -P $VM_PORT -t "firewall" "BLOCK: SSH brute-force from 203.0.113.50"
```

```
logger -n $VM_IP -P $VM_PORT -t "firewall" "ALLOW: HTTP traffic 192.168.1.100 to
10.0.0.5"
logger -n $VM_IP -P $VM_PORT -t "firewall" "ALERT: Port scan from 198.51.100.25"
sleep 1

# 4. MONITORING SISTEM
echo "  [4/5] Simulez metrici sistem..."
logger -n $VM_IP -P $VM_PORT -t "monitoring" "INFO: CPU 23%, RAM 45%, Disk 67%"
logger -n $VM_IP -P $VM_PORT -t "monitoring" "WARNING: Disk low /var (85% used)"
logger -n $VM_IP -P $VM_PORT -t "monitoring" "INFO: apache2 restarted successfully"
sleep 1

# 5. DIVERSE APLICAȚII
echo "  [5/5] Simulez log-uri diverse..."
logger -n $VM_IP -P $VM_PORT -t "voicemail" "INFO: New voicemail user 1001 - 45s"
logger -n $VM_IP -P $VM_PORT -t "dhcp" "INFO: DHCP 192.168.1.150 to
00:11:22:33:44:55"
logger -n $VM_IP -P $VM_PORT -t "backup" "SUCCESS: Database backup 2.3GB"

echo ""
echo "  Test complet! Log-uri trimise către VM."
echo ""
echo "  Pe VM verifică:"
echo "   sudo ls -lh /var/log/remote/*/"
echo "   sudo cat /var/log/remote/*/asterisk.log"
```

Rulare script:

```
chmod +x test-syslog-telecom.sh
./test-syslog-telecom.sh
```

5.3 Verificare rezultate pe VM

Listare fișiere create:

```
sudo ls -lh /var/log/remote/*/
```

Output așteptat:

```
/var/log/remote/host-desktop/:
-rw-r----- 1 syslog adm  512 Jan 19 16:35 asterisk.log
-rw-r----- 1 syslog adm  384 Jan 19 16:35 router.log
-rw-r----- 1 syslog adm  256 Jan 19 16:35 firewall.log
-rw-r----- 1 syslog adm  198 Jan 19 16:35 monitoring.log
```

Vizualizare conținut:

```
# Log-uri Asterisk (telefonie)
sudo cat /var/log/remote/*/asterisk.log

# Log-uri Router
sudo cat /var/log/remote/*/router.log

# Toate log-urile (live monitoring)
sudo tail -f /var/log/remote/*/*.log
```

6. TROUBLESHOOTING

6.1 Log-urile NU apar pe VM

Verificare 1: rsyslog ascultă pe port 514

```
sudo netstat -uln | grep 514
```

Dacă nu apare nimic:

```
# Verifică configurarea
sudo grep -E "^module\(load=\"imudp\"\)|^input\(type=\"imudp\"" /etc/rsyslog.conf

# Restart rsyslog
sudo systemctl restart rsyslog
```

Verificare 2: UFW permite trafic

```
sudo ufw status | grep 514
# Trebuie să vezi:
# 514/udp    ALLOW    Anywhere
```

6.2 Ping către VM nu merge (Bridge mode)

Soluție pe VM:

```
# Forțează renew DHCP
sudo dhclient -r
sudo dhclient

# Verifică nou IP
hostname -I
```

7. COMENZI UTILE

7.1 Monitorizare live

```
# Toate log-urile remote
sudo tail -f /var/log/remote/*/*.log

# Doar Asterisk
sudo tail -f /var/log/remote/*/asterisk.log

# Doar erori
sudo grep -r "ERROR\|ALERT" /var/log/remote/
```

7.2 Statistici

```
# Număr total fișiere log
find /var/log/remote/ -type f | wc -l

# Dimensiune totală
du -sh /var/log/remote/

# Top 10 cele mai mari fișiere
du -h /var/log/remote/*/* | sort -rh | head -10
```

8. ÎNTREBĂRI FRECVENTE (FAQ)

Q1: De ce UDP și nu TCP pentru syslog?

A: UDP e mai rapid (fire-and-forget), overhead minim, ideal pentru volume mari. TCP se folosește pentru log-uri critice (port 6514 cu TLS).

Q2: Log-urile sunt criptate?

A: NU! Syslog standard (UDP 514) trimite text clar.

Soluții securitate:
• VPN între client și server
• Syslog-TLS (TCP cu SSL)
• Rețea izolată VLAN management

Q3: Cât spațiu ocupă log-urile?

Estimare:
• 1 echipament: 10-50 MB/zi
• 10 echipamente: 500 MB/zi
• Call center 50 telefoane: 2-5 GB/zi

Recomandare: Disk minim 100GB cu rotație automată.

9. CONCLUZII

9.1 Ce s-au realizat?

• Administrare Linux (rsyslog, UFW, networking)
• Protocoale telecomunicații (syslog/UDP)
• Virtualizare (VirtualBox/VMware)
• Troubleshooting rețele
• Organizare infrastructură IT

ANEXE

Anexa A: Comenzi rapide

```
# PE VM (Server)
sudo systemctl restart rsyslog
sudo netstat -uln | grep 514
sudo tail -f /var/log/remote/*/*.log
sudo ufw status verbose

# PE HOST (Client)
ping 192.162.10.150
logger -n 192.162.10.150 -P 514 "test"
logger -n 192.162.10.150 -P 514 -t "asterisk" "CALL test"
```

Anexa B: Structura fișierelor

```
/var/log/remote/
├── hostname1/
│   ├── asterisk.log
│   ├── router.log
│   └── firewall.log
├── hostname2/
│   ├── apache2.log
│   └── mysql.log
└── phone-ip-101/
    └── voip.log
```

BONUS - Îmbunătățiri pentru Scenarii Reale

1. Rotație log-uri (logrotate)

Configurează rotația automată pentru a preveni umplerea discului. Creează fișier de configurare:

```
sudo nano /etc/logrotate.d/remote-syslog
```

Adaugă politici de rotație după dimensiune, timp și compresie pentru menținerea unui sistem stabil.

2. TCP ca alternativă

Pentru rețele instabile sau log-uri critice, configurează recepție pe TCP (port 514) pentru fiabilitate sporită. TCP garantează livrarea mesajelor față de UDP care poate pierde pachete în condiții de rețea dificile.

3. SELinux/AppArmor

Dacă sistemul are SELinux (RHEL/CentOS) sau AppArmor (Ubuntu) activate, configurează politici specifice pentru rsyslog să permită citirea/scrierea în /var/log/remote și ascultarea pe portul 514. Verifică audit logs pentru erori de permisiuni.

4. Sincronizare timp (NTP)

Configurează NTP/chrony pe toate echipamentele (server + clienți) pentru sincronizare precisă a timpului. Timestamp-uri corecte sunt esențiale pentru corelarea evenimentelor în troubleshooting și analiză forensică. Diferențe de timp pot face imposibilă reconstrucția corectă a secvențelor de evenimente.