



Nastavni predmet	KONFIGURIRANJE RAČUNALNIH MREŽA I SERVISA
Naslov jedinice	Vježba 12: SNMP servis na Linux Mintu

## CILJ VJEŽBE

Učenik će znati instalirati i konfigurirati SNMP servis na Linux Mint distribuciji, instalirati i konfigurirati aplikaciju za trap poruke. U ovoj vježbi, SNMP agent radi na Linux Mint-u i omogućuje prikupljanje podataka i primanje TRAP poruka.

SNMP (Simple Network Management Protocol) je mrežni protokol koji omogućuje nadzor i upravljanje mrežnim uređajima (serveri, ruteri, switchevi, pisači, itd.).

## IZVOĐENJE VJEŽBE

Sve postupke i dobivene rezultate po točkama zadataka zapisivati u bilježnicu.

Odgovoriti u bilježnicu na postavljena pitanja vezana uz ovu vježbu. Oprezno pratite zadatke i što se traži u njima.

### 1. Inicijalne postavke

- 1) Pokrenuti VMware Workstation Pro
- 2) Postaviti snapshot u VMware-u za poslužitelj (Linux Mint) na **cleanInstall** kako bi započeli čistu konfiguraciju SNMP servisa
- 3) Pokrenuti Poslužitelj (Linux Mint)

User : **osboxes.org**

Password : **osboxes.org**

- 4) Na Poslužitelju (Linux Mint) u Network adapter postavkama odaberite **NAT** kako bi mogli pristupiti internetu kod instalacije Linux Mint paketa nadogradnje.
- 5) Na Poslužitelju (Linux Mint) postavite tipkovnicu na **Croatia (Layout)** zbog prilagodbe tipkovnice hrvatskoj verziji (ostale tipkovnice možete obrisati).
- 6) Za potrebe vježbe, na istome stroju instalirati ćemo i pokrenuti SNMP Agentu i SNMP Managera.
- 7) U Terminalu upisati sljedeće naredbe:

```
$ sudo su
```

```
$ apt-get update
```

```
$ apt-get install -y snmpd snmp // instalacija snmp servisa
```

```
$ apt-get install snmptrapd // instalacija aplikacije za primanje TRAP i INFORM poruka
```

## 2. Konfiguracija SNMP agenta

Pripre bilo kakvih izmjena, pohranit ćemo originalnu konfiguracijsku datoteku:

```
$ cp /etc/snmp/snmpd.conf /etc/snmp/snmpd.conf.orig
```

```
$ nano /etc/snmp/snmpd.conf
```

U datoteci potražiti sljedeće zapise i napraviti kako je niže napisano:

```
#Listen for connections from the local system only
```

```
agentAddress udp:127.0.0.1:161 //dodati # na početak linije
```

```
#Listen for connections on all interfaces (both IPv4 *and* IPv6)
```

```
# agentAddress udp:161,udp6:[::]:161 //ukloniti # s početka linije
```

Pohraniti i izaći. (Ctrl+X)

Nakon izmjena u konfiguracijskoj datoteci, potrebno je restartati servis:

```
$ systemctl restart snmpd
```

Provjera radi li nam SNMP servis:

```
$ apt-get install snmpwalk // uključeno u inicijalni paket
```

```
$ snmpwalk -c public -v 1 localhost
```

Što generira naredba snmpwalk?

## 3. Konfiguracija SNMP Managera

Prije bilo kakvih izmjena, pohraniti ćemo originalnu konfiguracijsku datoteku:

```
$ cp /etc/snmp/snmptrapd.conf /etc/snmp/snmptrapd.conf.orig
```

```
$ nano /etc/snmp/snmptrapd.conf
```

U datoteci potražiti sljedeći zapis:

```
# authCommunity log,execute,net public // ukloniti # s početka linije
```

Pohraniti i izaći. (Ctrl+X, Y, Enter)

Nakon izmjena u konfiguracijskoj datoteci, potrebno je restartati servis:

```
$ systemctl restart snmptrapd
```

Zaustavit ćemo rad snmptrapd.service i snmptrapd.socket jer ćemo ručno pokrenuti osluškivanje snmp prometa preko porta 162:

```
$ systemctl stop snmptrapd.service
```

```
$ systemctl stop snmptrapd.socket
```

Provjerite status snmptrapd.service i snmptrapd.socket:

```
$ sudo systemctl status snmptrapd.service
```

```
snmptrapd.socket
```

Status treba biti: **Inactive** za oba servisa.

## 4. Testiranje i hvatanje TRAP poruka

- 1) U **inicijalno pokrenutom Terminalu**, simulirat ćemo računalo koje nadgleda i hvata TRAP poruke.

Da bismo pokrenuli osluškivanje, upisati sljedeću naredbu:

```
$ snmptrapd -CdfLo --disableAuthorization=yes
```

Poslužitelj treba doći u status osluškivanja prometa.

Koji je rezultat izvođenja navedene naredbe?

2) **Otvoriti još jedan Terminal.** Ovaj prozor simulirat će SNMP agenta.

Pošaljite dvije testne poruke:

```
$ snmptrap -v 1 -c public localhost '1.2.3.4.5.6'  
'192.193.194.195' 6 99 '55' 1.11.12.13.14.15 s "test"
```

I naknadno slijedeću poruku:

```
$ snmptrap -v 2c -c public localhost ""  
1.3.6.1.4.1.8072.2.3.0.1 \  
.1.3.6.1.2.1.1.3.0 t 123456789 \  
.1.3.6.1.2.1.1.5.0 s "Test uredjaj"
```

Rezultat snimanja bi trebao u prvom terminalu izgledati slično:

```
2025-02-14 03:43:35 localhost [UDP: [127.0.0.1]:58664->[127.0.0.1]:162]:  
iso.3.6.1.2.1.1.3.0 = Timeticks: (130010) 0:21:40.10 iso.3.6.1.6.3.1.1.4.  
1.0 = OID: iso.3.6.1.4.1.8072.2.3.0.1 iso.3.6.1.2.1.1.3.0 = Timeticks:  
(123456789) 14 days, 6:56:07.89 iso.3.6.1.2.1.1.5.0 = Hex-STRING: 54  
65 73 74 20 75 72 65 C4 91 61 6A
```

Koji je rezultat izvođenja navedene naredbe?

Koji se transportni protokol koristi za slanje TRAP poruka?

**Pozovite profesora da vam pogleda rezultate.**

## 5. Završetak vježbe

Ako ste uspješno savladali vježbu dobit ćete odličnu ocjenu. Postavite računalo na home.