



Algebra

visoko učilište

**Mreža, specijalne dozvole,
ACL-ovi, firewall**

www.racunarstvo.hr

Konfiguracija VPN konekcije

- padajući izbornik
- odabrati korisničko ime i lozinku
- podržani svi poznati protokoli

Editing VPN connection 1

Connection name: VPN connection 1

☐ Connect automatically

☐ Available to all users

VPN | IPv4 Settings

General

Gateway:

Group name:

User password: Always Ask ▾

Group password: Always Ask ▾

☐ Show passwords

Optional

User name:

Phase1 Algorithms:

Phase2 Algorithms:

Domain:

Export... Cancel Apply



Algebra

visoka škola
za primijenjeno
računarstvo

Konfiguracija VLAN ID-a

```
root@CentOS6:/etc/sysconfig/network-scripts
File Edit View Search Terminal Help
DEVICE=eth0.5
ONBOOT=yes
BOOTPROTO=none
IPADDR=192.168.0.1
NETMASK=255.255.255.0
VLAN=yes

ili

DEVICE=eth0.5
ONBOOT=yes
BOOTPROTO=dhcp
VLAN=yes
~
~
~
~
~
~
~
-- INSERT --
```



Algebra

visoka škola
za primijenjeno
računarstvo

Konfiguracija bridge-a

```
root@OOS2:/etc/sysconfig/network-scripts
File Edit View Search Terminal Help
[root@OOS2 network-scripts]# cat ifcfg-eth0 ifcfg-br0
DEVICE=eth0
TYPE=Ethernet
ONBOOT=yes
NM_CONTROLLED=no
BOOTPROTO=none
HWADDR=00:0C:29:03:96:9E
BRIDGE=br0

DEVICE=br0
TYPE=Bridge
ONBOOT=yes
BOOTPROTO=dhcp
NM_CONTROLLED=no
DELAY=0

[root@OOS2 network-scripts]#
```



Algebra

visoka škola
za primijenjeno
računarstvo

Channel bonding (agregacija linkova)

```
root@OOS2:/etc/sysconfig/network-scripts
File Edit View Search Terminal Help
[root@OOS2 network-scripts]# cat ifcfg-eth0 ifcfg-eth1 ifcfg-bond0
DEVICE=eth0
BOOTPROTO=none
ONBOOT=yes
MASTER=bond0
SLAVE=yes
USERCTL=no

DEVICE=eth1
BOOTPROTO=none
ONBOOT=yes
MASTER=bond0
SLAVE=yes
USERCTL=no

DEVICE=bond0
IPADDR=192.168.1.1
NETMASK=255.255.255.0
ONBOOT=yes
BOOTPROTO=none
USERCTL=no
BONDING_OPTS="mode=0 miimon=100"

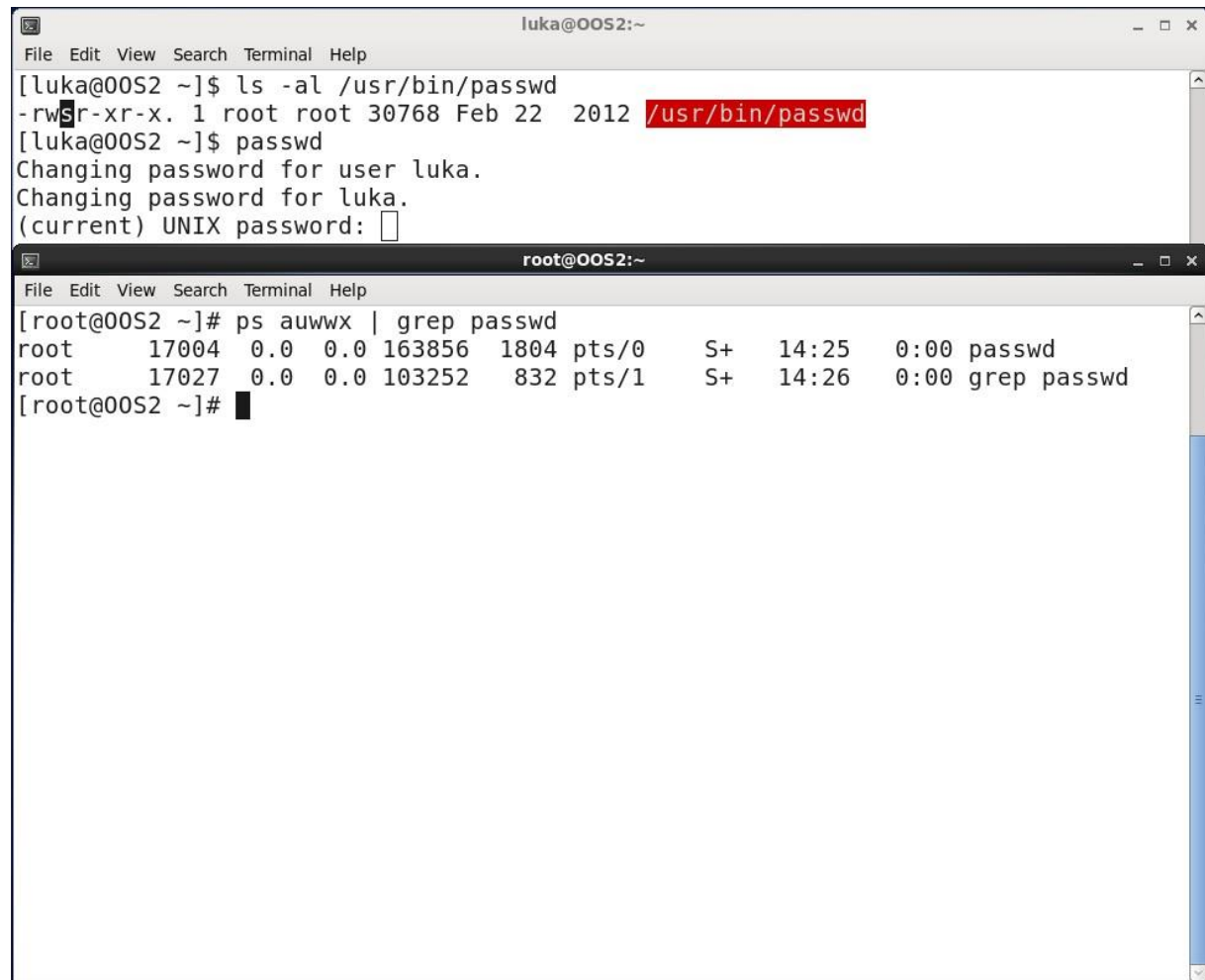
[root@OOS2 network-scripts]# █
```



Algebra

visoka škola
za primijenjeno
računarstvo

Specijalne dozvole - *setuid*



The image shows two terminal windows. The top window is a regular user 'luka' and the bottom window is root.

Top Terminal (luka@OOS2:~):

```
File Edit View Search Terminal Help
[luka@OOS2 ~]$ ls -al /usr/bin/passwd
-rwsr-xr-x. 1 root root 30768 Feb 22 2012 /usr/bin/passwd
[luka@OOS2 ~]$ passwd
Changing password for user luka.
Changing password for luka.
(current) UNIX password: 
```

Bottom Terminal (root@OOS2:~):

```
File Edit View Search Terminal Help
[root@OOS2 ~]# ps auwx | grep passwd
root      17004  0.0  0.0 163856 1804 pts/0    S+   14:25   0:00 passwd
root      17027  0.0  0.0 103252   832 pts/1    S+   14:26   0:00 grep passwd
[root@OOS2 ~]# 
```



Algebra

visoka škola
za primijenjeno
računarstvo

Specijalne dozvole - *setgid*

```
luka@OOS2:/web
File Edit View Search Terminal Help
[root@OOS2 ~]# id luka
uid=501(luka) gid=502(luka) groups=502(luka),500(web)
[root@OOS2 ~]# id ivan
uid=500(ivan) gid=501(ivan) groups=501(ivan),500(web)
[root@OOS2 ~]# mkdir /web
[root@OOS2 ~]# chmod g+ws /web
[root@OOS2 ~]# chgrp web /web
[root@OOS2 ~]# su - ivan
[ivan@OOS2 ~]$ cd /web
[ivan@OOS2 web]$ touch ivan.txt
[ivan@OOS2 web]$ logout
[root@OOS2 ~]# su - luka
[luka@OOS2 ~]$ cd /web
[luka@OOS2 web]$ touch luka.txt
[luka@OOS2 web]$ ls -al
total 8
drwxrwsr-x  2 root web  4096 Jul 30 14:50 .
dr-xr-xr-x. 27 root root 4096 Jul 30 14:49 ..
-rw-rw-r--  1 ivan web    0 Jul 30 14:50 ivan.txt
-rw-rw-r--  1 luka web    0 Jul 30 14:50 luka.txt
[luka@OOS2 web]$ rm ivan.txt
[luka@OOS2 web]$
```



Algebra

visoka škola
za primijenjeno
računarstvo

Specijalne dozvole – *sticky bit*

```
ivan@OOS2:~  
File Edit View Search Terminal Help  
[root@OOS2 ~]# chmod g+ws /web  
[root@OOS2 ~]# chgrp web /web  
[root@OOS2 ~]# su - ivan  
[ivan@OOS2 ~]$ cd /web  
[ivan@OOS2 web]$ touch ivan.txt  
[ivan@OOS2 web]$ logout  
[root@OOS2 ~]# su - luka  
[luka@OOS2 ~]$ cd /web  
[luka@OOS2 web]$ touch luka.txt  
[luka@OOS2 web]$ ls -al  
total 8  
drwxrwsr-x  2 root web  4096 Jul 30 14:50 .  
dr-xr-xr-x. 27 root root 4096 Jul 30 14:49 ..  
-rw-rw-r--  1 ivan web    0 Jul 30 14:50 ivan.txt  
-rw-rw-r--  1 luka web    0 Jul 30 14:50 luka.txt  
[luka@OOS2 web]$ rm ivan.txt  
[luka@OOS2 web]$ logout  
[root@OOS2 ~]# chmod o+t /web; ls -al /web  
total 8  
drwxrwsr-t  2 root web  4096 Jul 30 14:50 .  
dr-xr-xr-x. 27 root root 4096 Jul 30 14:49 ..  
-rw-rw-r--  1 luka web    0 Jul 30 14:50 luka.txt  
[root@OOS2 ~]# su - ivan  
[ivan@OOS2 ~]$ rm /web/luka.txt  
rm: cannot remove `/web/luka.txt': Operation not permitted  
[ivan@OOS2 ~]$ touch ivan.txt  
[ivan@OOS2 ~]$ rm ivan.txt  
[ivan@OOS2 ~]$ █
```



Algebra

visoka škola
za primijenjeno
računarstvo

Liste za kontrolu pristupa (ACL)

- *access* ACL
- *default* ACL
- provjeriti mount opcije ext3/4 particije na kojoj pokušavamo koristiti ACL



Algebra

visoka škola
za primijenjeno
računarstvo

Access ACL

- formiraju se korištenjem komande *setfacl*, a ako koristimo i parametar -m uz navedenu komandu, radimo *modifikaciju* liste za kontrolu pristupa. Prototip komande izgleda ovako:

`setfacl -m pravilo datoteka_ili_direktorij`



Algebra

visoka škola
za primijenjeno
računarstvo

Format za *access* ACL-ove I

1. Po UserID-u

```
[root@OOS2 ~]# setfacl -m u:uid:dozvola  
datoteka_ili_direktorij
```

- u "uid" dio upisujemo ili UserID korisnika ili njegovo korisničko ime. Time modificiramo ACL na razini korisnika za određenu datoteku ili direktorij, kako god smo odabrali.

2. Po GroupID-u

```
[root@OOS2 ~]# setfacl -m g:gid:dozvola  
datoteka_ili_direktorij
```

- u "gid" dio upisujemo ili GroupID grupe korisnika ili ime grupe. Time modificiramo ACL na razini grupe za određenu datoteku ili direktorij, kako god smo odabrali.



Algebra

visoka škola
za primijenjeno
računarstvo

Format za *access* ACL-ove II

3. Po efektivnoj masci

```
[root@OOS2 ~]# setfacl -m m:dozvola datoteka_ili_direktorij
```

- maska je unija svih dozvola grupe koja ima dozvole i svih zapisa za korisnike i grupe nad nekom datotekom ili direktorijem, kako god smo odabrali. U prijevodu, efektivna maska je zapravo "plafon", najviši skup dozvola, kojeg dobivaju svi korisnici i grupe koji nisu vlasnici datoteke ili direktorija. Ova vrsta dozvole se uvijek postavlja *nakon* svih drugih ACL pravila.

4. Po *others*, tj.za sve ostale koji nisu članovi grupe koja ima ACL na datoteci ili direktoriju

```
[root@OOS2 ~]# setfacl -m o:dozvola datoteka_ili_direktorij
```

- dozvole se odabiru iz standardnog skupa dozvola koje su nam već poznate, tj. r(ead), w(rite) i (e)x(ecute).



Algebra

visoka škola
za primijenjeno
računarstvo

Default ACL-ovi

- koriste se za naslijeđivanje ACL-ova sa razine direktorija na razinu datoteka koje se nalaze unutar direktorija sa uobičajenim listama za kontrolu pristupa.
- rade se također sa *setfacl* komandom, ali uz korištenje dodatne opcije d:, kako je pokazano primjerom:

```
[root@OOS2 ~]# setfacl -m d:o:rx /direktorij
```



Algebra

visoka škola
za primijenjeno
računarstvo

Iptables vatrozid I

četiri tablice:

- 1. Filter tablica - ovo je uobičajena (*default*) tablica za iptables vatrozid. Ima tri lanca podataka (*chain*) - INPUT (promet koji dolazi u vatrozid), OUTPUT (promet koji je generiran lokalno na poslužitelju gdje konfiguriramo vatrozid i koji izlazi van iz poslužitelja) i FORWARD (za usmjeravanje paketa prema nekom drugom mrežnom adapteru unutar poslužitelja gdje konfiguriramo vatrozid).
- 2. NAT tablica - ova tablica se koristi za NAT funkcionalnost (Network Address Translation), tj. za prevođenje izvorišne ili odredišne adrese na paketu. Ima četiri odredišta (target) - DNAT (*Destination NAT*, u kojem mijenjamo odredišnu adresu paketa i preusmjeravamo ga na poslužitelj), SNAT (*Source NAT*, u kojem mijenjamo izvorišnu adresu paketa na fiksno definiranu IP adresu), MASQUERADE (vrlo slično SNAT-u, ali traži malo više obrade, mijenjanje izvorišne adrese paketa se može postaviti direktno na mrežni adapter bez podešavanja mrežne adrese) i REDIRECT (za preusmjeravanje prometa na lokalni poslužitelj)
- 3. Mangle tablica - ova se tablica koristi za napredne izmjene u IP paketima, npr. TOS, TTL, MARK, SECMARK, CONNSECMARK
- 4. RAW tablica - koristi se za označavanje paketima koje ne treba pregledavati, postavljanjem NOTRACK odredišta na paketu.



Algebra

visoka škola
za primijenjeno
računarstvo

IPtables vatrozid II

- 30ak targeta, ovo su bitniji:
- ACCEPT (opcija -j ACCEPT) - kada se pronade odgovarajući paket, propušta se

[root@OOS2 ~]# iptables -P INPUT ACCEPT

- postavljanje *default* politike na INPUT chainu na ACCEPT, tj. propuštaju se svi paketi na ulazu.

- DROP (opcija -j DROP) - kada se pronade odgovarajući paket, odbacuje se

[root@OOS2 ~]# iptables -P FORWARD DROP

- Postavljanje *default* politike na FORWARD chainu na DROP, tj. odbacuju se svi paketi za prosljeđivanje.



Algebra

visoka škola
za primijenjeno
računarstvo

IPTables vatrozid III

- REJECT (opcija -j REJECT --reject-with *reject_type*) - vrlo slično DROP target, ali kada se pronade odgovarajući paket, odbacuje ga se sa porukom *reject_type* (npr. *icmp-host-unreachable*, *tcp-reset*, ...)

```
[root@OOS2 ~]# iptables -P FORWARD REJECT --reject-with icmp-host-unreachable
```

- Postavljanje *default* politike na FORWARD chainu na REJECT, pri čemu se odbacuju svi paketi sa porukom *icmp-host-unreachable*.
- LOG (opcija -j LOG sa dodatnim --log-prefix i sl. opcijama) - kada se pronade odgovarajući paket, informacija o njemu se zapisuje u log datoteku. Uobičajeno je to /var/log/messages, ali možemo iskoristiti i *rsyslog* servis da iptables poruke filtriramo u zasebnu datoteku.

```
[root@OOS2 ~]# iptables -N LOGGING; iptables -A INPUT -j LOGGING; iptables -A LOGGING -m limit --limit 2/min -j LOG --log-prefix "DROPPED PACKAGE: "; iptables -A LOGGING -j DROP
```



Algebra

visoka škola
za primijenjeno
računarstvo

Firewalld vatrozid - I

- Novi sustav za kontrolu vatrozida koji je prisutan u RedHat Enterprise Linux-u 7 (CentOS 7, Scientific Linux 7, ...)
- Fokus – nedorečenosti, „korak naprijed“, bolja kontrola



Algebra

visoka škola
za primijenjeno
računarstvo

Firewalld vatrozid - II

- Promjene:
 - Bolja kontrola firewall procesa – nije potrebno raditi restartanja i reloadanja, dok se kod iptables sustava radio reload (postoji trenutak kada firewall zbog toga ne radi)
 - Uvedene zone
 - Naprednija rekonfiguracija
 - Format konfiguracijskih datoteka (txt vs XML)
 - Bolja integracija servisa
 - Integracija sa DBUS mehanizmom (DBUS je IPC i RPC, tj.inter-process communication i remote procedure call sustav) – servisi rade update i konfiguraciju kod Firewalld-a
 - Više na https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/Security_Guide/sec-Using_Firewalls.html



Algebra

visoka škola
za primijenjeno
računarstvo