**ZASOL: Suplement do lekcji 1**

Instalacja i podstawowa konfiguracja CentOS Linux, zarządzanie usługami

**Interfejsy sieciowe**

Interfejsy (karty sieciowe) są oznaczane w sposób przewidywalny, zależny od sposobu fizycznego wpięcia sprzętu sieciowego do serwera, przykładowo:

**enp0s3** – **e**thernet **n**etwork **p**ehriperial **0**, **s**lot **3**

Interfejsy możemy włączać I wyłączać poleceniem **ifdown** i **ifup**.

Aktualną konfigurację możemy wyświetlić poleceniem **ip a s** (**ip** **a**ddress **s**how):

[root@jk aplitt]# ip a s

1: lo: <LOOPBACK,UP,LOWER\_UP> mtu 65536 […]

2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER\_UP> mtu 1500 qdisc pfifo\_fast state UP qlen 1000

link/ether 02:9c:8c:66:65:60 brd ff:ff:ff:ff:ff:ff

inet 192.168.0.1/24 brd 192.168.0.255 scope global eth0

inet6 fe80::9c:8cff:fe66:6560/64 scope link

valid\_lft forever preferred\_lft forever

Gdzie kolejno widzimy, linia po linii:

enp0s3: <BROADCAST,MULTICAST,UP,LOWER\_UP> mtu 1500 qdisc pfifo\_fast state UP qlen 1000

nazwa\_interfejsu: <statusy> parametry łącza stan łącza prędkość

link/ether 02:9c:8c:66:65:60

typ fizyczny adres MAC

inet 192.168.0.1/24 brd 192.168.0.255 scope global enp0s3

adres IPv4/maska adres broadcast zakres adresu

inet6 fe80::9c:8cff:fe66:6560/64 scope link

adres IPv6/maska zakres adresu

Zmiana ustawień interfejsu sieciowego wykonywana jest przez edycję pliku:

[root@jk ~]# nano /etc/sysconfig/network-scripts/ifcfg-<nazwa-interfejsu>

Domyślnie, po instalacji mamy ustawione DHCP (bootproto), a interfejs nie włącza się po starcie (boot) systemu (onboot=no):

TYPE=Ethernet

BOOTPROTO=dhcp

DEVICE=enp0s3

ONBOOT=no

Zmieńmy, aby interfejs włączał się razem z uruchamianiem systemu, na stałej adresacji:

TYPE=Ethernet

BOOTPROTO=static

DEVICE=enp0s3

ONBOOT=yes

IPADDR=192.168.0.1

NETMASK=255.255.255.0

GATEWAY=192.168.0.254

Plik zapisujemy. Zmienione/dodane parametry są zaznaczone kolorem czerwonym.

Po zmianie konfiguracji interfejsów musimy zastosować nową konfigurację

Najłatwiej jest to zrobić, wyłączając i włączając ponownie interfejs:

[root@jk ~]# ifdown enp0s3 & ifup enp0s3

Znak & oznacza, że kolejne polecenie wykona się tylko wtedy, gdy poprzednie się powiedzie.

**Usługi**

Czołowym przeznaczeniem serwerów Linuxowych jest dostarczanie **usług**.

Jako usługi rozumiemy między innymi:

* serwery WWW (httpd [apache], nginx, lighttpd),
* bazy danych (MySQL, PostrgeSQL, IBM DB2, MongoDB),
* serwery pocztowe (postfix, sendmail, dovecot),
* serwery plików (NFS, FTP),
* serwery aplikacji (Tomcat, JBoss, php-fpm),

Usługi (services) prawie zawsze **działają w tle**, czyli są **daemonami** (demonami), w przeciwieństwie do programów wywoływanych na żądanie (np. edytory nano, vim, polecenie ip).

Usługi prawie zawsze dokonują przypisania się do jakiegoś portu (**bind – bindują się**) na interfejsie sieciowym – np. 192.168.0.1:80 – oznacza, że usługa działa na adresie 192.168.0.1 na porcie 80.

Kilka najpopularniejszych portów i usług na nich działających:

FTP port 21 (wymiana plików)

SSH port 22 (zdalne połączenie do serwerów Linux)

HTTP port 80 (serwer WWW – połączenia nieszyfrowane)

IMAP port 143 (e-mail)

HTTPS port 443 (serwer WWW – połączenia szyfrowane)

SMTP port 587 (e-mail)

MySQL port 3306 (baza danych)

PostgreSQL port 5678 (baza danych)

Usługami zarządzamy poleceniem systemctl <czynność> <usługa>, np.:

systemctl status httpd status usługi httpd

systemctl start/stop/restart httpd start/stop/restart usługi httpd

systemctl enable httpd ustaw, aby httpd wączał się razem z systemem

systemctl disable httpd anuluj włączanie httpd razem z systemem

Ostatnie logi z danej usługi są widoczne w systemctl status, natomiast chcąc zobaczyć wszystkie logi z konkretnej usługi, wpisujemy:

journalctl | grep <nazwa\_uslugi>

Lub, zależnie od konfiguracji w plikach w katalogu /var/log.

W wypadku błędów uruchamiania, możemy łatwo znaleźć błędy wpisując:

Journalctl -xe | grep <nazwa\_uslugi>

**SELinux**

SELinux (Security Enhanced Linux) to zestaw modułów do jądra systemu, które implementują dodatkową ochronę i reguły dla usług działających w systemie. Dla każdej usługi istnieje kontekst, który definiuje, do czego może mieć dostęp dana usługa.

Na przykład, httpd powinien mieć dostęp tylko do /var/www/ (gdzie znajdują się domyślnie pliki danych dla webserwera) oraz móc zbindować się na porcie 80/443. Próba uruchomienia httpd na innym porcie, lub dostępu do np. pliku /etc/passwd zakończy się zablokowaniem (Access denied), ponieważ nie jest to standardowe zachowanie webserwera (można oczywiście dodać wyjątki). Dodaje to dodatkową warstwę ochrony przed próbami włamań i błędami w oprogramowaniu.

Trzy tryby działania:

Enforcing - złamanie reguł powodują zablokowanie czynności + logowanie zdarzenia

Permissive - złamanie reguł powoduje tylko zalogowanie zdarzenia

Disabled - SELinux wyłączony

Polecenia:

getenforce - sprawdzamy, w jakim trybie jest SELinux

setenforce -tymczasowo (do następnego restartu) zmieniamy tryb działania

Edytując plik /etc/sysconfig/selinux możemy permanentnie zmienić sposób działania SELinuxa. W celu zastosowania zmian należy ponownie uruchomić system.