

SSH - plik konfiguracyjny serwera

Położenie: /etc/ssh/sshd_config (rw-----)

© Imagine Studio 2004, <http://myMandrake.tk>

```
# $OpenBSD: sshd_config,v 1.65 2003/08/28 12:54:34 markus Exp $
# This is the sshd server system-wide configuration file. See sshd_config(5) for more information. This sshd was compiled with
PATH=/usr/bin:/bin:/usr/sbin:/sbin. The strategy used for options in the default sshd_config shipped with OpenSSH is to specify options
with their default value where possible, but leave them commented. Uncommented options change a default value.
```

```
##### USTAWIENIA #####
```

Port 22

Protocol 2

```
# HostKey for protocol version 1
```

HostKey /etc/ssh/ssh_host_key

```
# HostKeys for protocol version 2
```

HostKey /etc/ssh/ssh_host_rsa_key

HostKey /etc/ssh/ssh_host_dsa_key

```
# Przerzywa połączenie jeśli user nie zaloguje się w tym czasie:
```

LoginGraceTime 2m

```
# Pozwolenie na logowanie roota (bez przekazywania hasła). Najlepiej jednak zabronić i logować się na roota przez "su":
```

```
#PermitRootLogin without-password
```

PermitRootLogin no

```
# Czy dopuszczona jest autentykacja w oparciu o protokół 1:
```

RSAAuthentication no

```
# Autentykacja w oparciu o klucze:
```

PubkeyAuthentication yes

AuthorizedKeysFile .ssh/authorized_keys

```
# Autentykacja w oparciu o plik /etc/ssh/ssh_known_hosts:
```

RhostsRSAAuthentication no

```
# Autentykacja w oparciu o rhosts:
```

HostbasedAuthentication no

```
# Change to yes if you don't trust ~/.ssh/known_hosts for RhostsRSAAuthentication and HostbasedAuthentication
```

IgnoreUserKnownHosts no

```
# Don't read the user's ~/.rhosts and ~/.shosts files
```

IgnoreRhosts yes

```
# Autentykacja oparta o niezaszyfrowane hasło:
```

PasswordAuthentication no

PermitEmptyPasswords no

```
# Forwarding X11:
```

X11Forwarding yes

X11DisplayOffset 10

X11UseLocalhost yes

Pojawi sie komunikat powitalny o tresci pobranej z pliku /etc/motd:

PrintMotd no

PrintLastLog yes

KeepAlive yes

Compression yes

PidFile /var/run/sshd.pid

MaxStartups 10

Komunikat powitalny, pojawiający się po zalogowaniu. Domyślnie jest czytany /etc/issue.

Banner /etc/ssh/banner.txt

Zezwolenie na szyfrowanie połączenia.

Subsystem sftp /usr/lib/misc/sftp-server

Użytkownicy:

AllowUsers robert@server.imagine

Inne opcje

#ListenAddress 0.0.0.0

#ListenAddress ::

Lifetime and size of ephemeral version 1 server key

#KeyRegenerationInterval 1h

#ServerKeyBits 768

Logging obsoletes QuietMode and FascistLogging

#SyslogFacility AUTH

#LogLevel INFO

#StrictModes yes

Change to no to disable s/key passwords

#ChallengeResponseAuthentication yes

Kerberos options

#KerberosAuthentication no

#KerberosOrLocalPasswd yes

#KerberosTicketCleanup yes

GSSAPI options

#GSSAPIAuthentication no

#GSSAPICleanupCreds yes

#AllowTcpForwarding yes

#GatewayPorts no

#UseLogin no

Poniższa opcja nie działa podobno niestety dobrze w tej wersji ssh:

#UsePrivilegeSeparation yes

#PermitUserEnvironment no

#ClientAliveInterval 0

#ClientAliveCountMax 3

DenyUsers student@raven.*

AllowGroups sshusers

DenyGroups users

Ostatnia aktualizacja: 8 kwiecień 2005.