T: Zabezpieczenie dostępu do komputera.

Aby zabezpieczyć komputer przed dostępem osób nieuprawnionych, można skonfigurować dwa pliki /etc/hosts.allow i /etc/hosts.deny.

Plik /etc/hosts.allow zawiera listę komputerów uprawnionych do korzystania z usług komputera, np.:
ALL: LOCAL @grupa_sieciowa
ALL: .rol.edu.pl EXCEPT uczen.rol.edu.pl

Reguła pierwsza zezwala na dostęp z komputerów w domenie LOCAL oraz członkom grupy grupu_sieciawa.

Reguła druga zezwala na dostęp z komputerów w domenie .rol.edu.pl z wyjątkiem uczen.rol.edu.pl.

Plik /etc/hosts.deny zawiera listę komputerów nieuprawnionych do korzystania usług komputera, np.:
ALL: .rol.edu.pl uczen.rol.com.pl

Reguła nie zezwala na dostęp z komputerów w domenie .rol.edu.pl i uczen.rol.com.pl.

Jeżeli do serwera wpłynie żądanie dostępu do usługi, to serwer pobiera adres IP i nazwę domeny hosta oraz rodzaj usługi, z której użytkownik chce skorzystać.
Następnie sprawdza w pliku /etc/hosts.aIlow, czy określony host może korzystać z usługi. Gdy istnieje odpowiedni wpis zezwalający, to połączenie jest realizowane.
Jeżeli takiego wpisu nie ma, wówczas jest sprawdzany plik /etc/hosts.deny.
Usługa jest udostępniana klientowi, jeżeli w pliku /etc/hosts.deny nie ma wpisu zabraniającego dostępu. Jeżeli oba pliki hosts.aIlow i hosts.deny są puste, to każde połączenie z każdym klientem będzie dopuszczone.

Konfigurowanie DenyHosts
Plik konfiguracyjny DenyHosts w Ubuntu to /etc/denyhosts.conf
Aby edytować plik konfiguracyjny DenyHosts, należy uruchomić polecenie:
nano /etc/denyhosts.conf
Przyjrzyjmy się teraz niektórym właściwościom w pliku konfiguracyjnym DenyHosts i ich działaniu.

DENY_THRESHOLD_INVALID

Ta opcja jest odpowiedzialna za blokowanie logowania SSH dla kont użytkowników, które nie istnieją w systemie. Domyślna wartość to 5. Oznacza to, powiedzmy, że ktoś próbuje zalogować się do serwera SSH jako różne nazwy użytkowników. Jeśli próba jest w sumie większa niż 5 razy, wówczas adres IP komputera próbującego nawiązać połączenie zostanie dołączony do pliku /etc/hosts.deny,

w ten sposób komputer nie będzie mógł połączyć się z serwerem SSH dopóki nie zostanie usunięty z pliku /etc/hosts.deny.

```
#
DENY_THRESHOLD_VALID = 10
#
```

DENY_THRESHOLD_VALID

Ta opcja jest taka sama jak DENY_THRESHOLD_INVALID

Jedyna różnica polega na tym, że DENY_THRESHOLD_VALID dotyczy istniejących użytkowników na maszynie denyhosts-server.

Oznacza to, że jeśli próby logowania dla istniejących użytkowników zakończą się niepowodzeniem 10 razy (wartość domyślna), adres IP komputera próbującego nawiązać połączenie zostanie dołączony do pliku /etc/hosts.deny.

Maszyna próbująca się połączyć nie będzie już mogła łączyć się z serwerem.

```
#
# DENY_THRESHOLD_VALID: block each host after the number of failed
# login attempts has exceeded this value.  This value applies to valid
# user login attempts (eg. user accounts that exist in /etc/passwd) except
# for the "root" user
#
DENY_THRESHOLD_VALID = 10
#
```

DENY_THRESHOLD_ROOT

To samo, co pozostałe dwie opcje. Tak samo jak pozostałe dwie opcje. Wartość to 1. Oznacza to, że jeśli ktoś spróbuje połączyć się z serwerem denyhosts jako root i raz się nie powiedzie, jego / jej adres IP zostanie dołączony do pliku /etc/hosts.deny. Nie będzie on już mógł się połączyć z serwerem.

HOSTNAME_LOOKUP

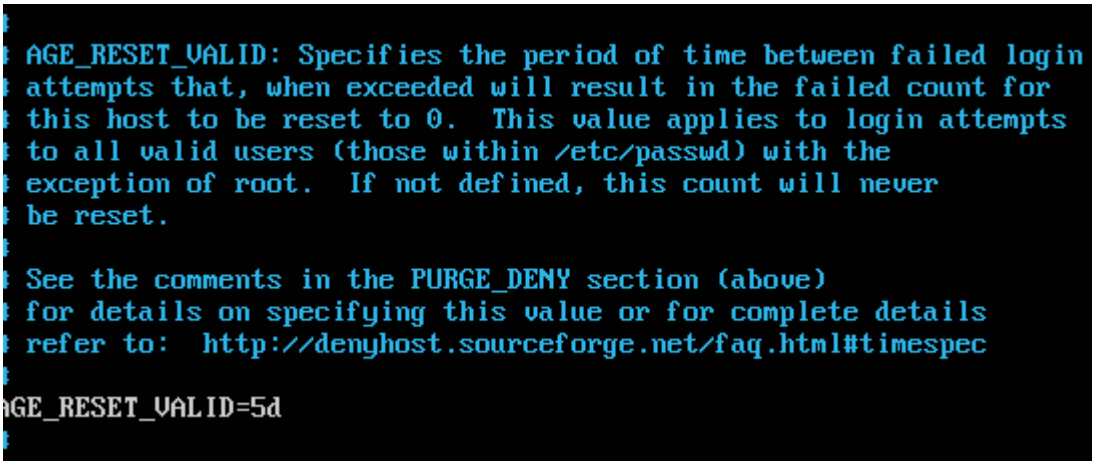
Domyślnie w systemie Ubuntu DenyHosts nie rozpoznaje nazw hostów. Oznacza to, że adresy IP nie zostaną przekształcone na nazwy hostów. Ale jeśli potrzebujesz rozwiązać nazwy hostów na adres IP i tak dalej, ustaw HOSTNAME_LOOKUP na YES i zapisz plik.

```
#
# HOSTNAME_LOOKUP
#
# HOSTNAME_LOOKUP=YES|NO
# If set to YES, for each IP address that is reported by Denyhosts,
# the corresponding hostname will be looked up and reported as well
# (if available).
#
HOSTNAME_LOOKUP=NO
#
```

AGE_RESET_VALID

AGE_RESET_VALID informuje DenyHosts po upływie czasu, przez który nieudane próby logowania dla istniejącego użytkownika zostaną zresetowane do wartości 0. Domyślna wartość to 5 dni.

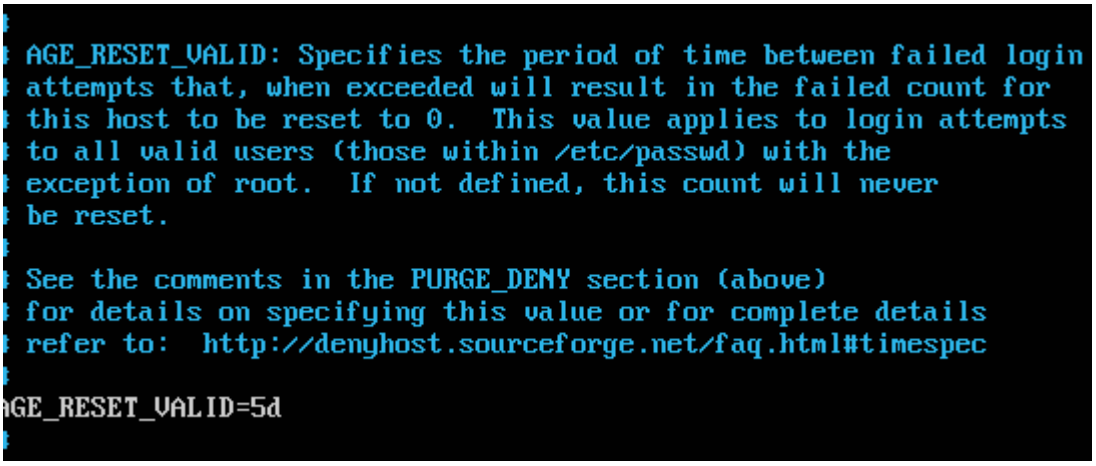
Oznacza to, że jeśli ktoś spróbuje zalogować się w dniu 1, a następnie czekać przez 5 dni i spróbować ponownie zalogować się, DenyHosts nie umieszcza ich w pliku /etc/hosts.deny.



AGE_RESET_ROOT

To samo co AGE_RESET_VALID, ale dotyczy tylko nieprawidłowych loginów root.

Domyślna wartość to 25 dni.



AGE_RESET_INVALID

To samo, co AGE_RESET_VALID, ale dotyczy tylko nieudanych prób zalogowania się nieistniejących użytkowników maszyny denyhosts-server.