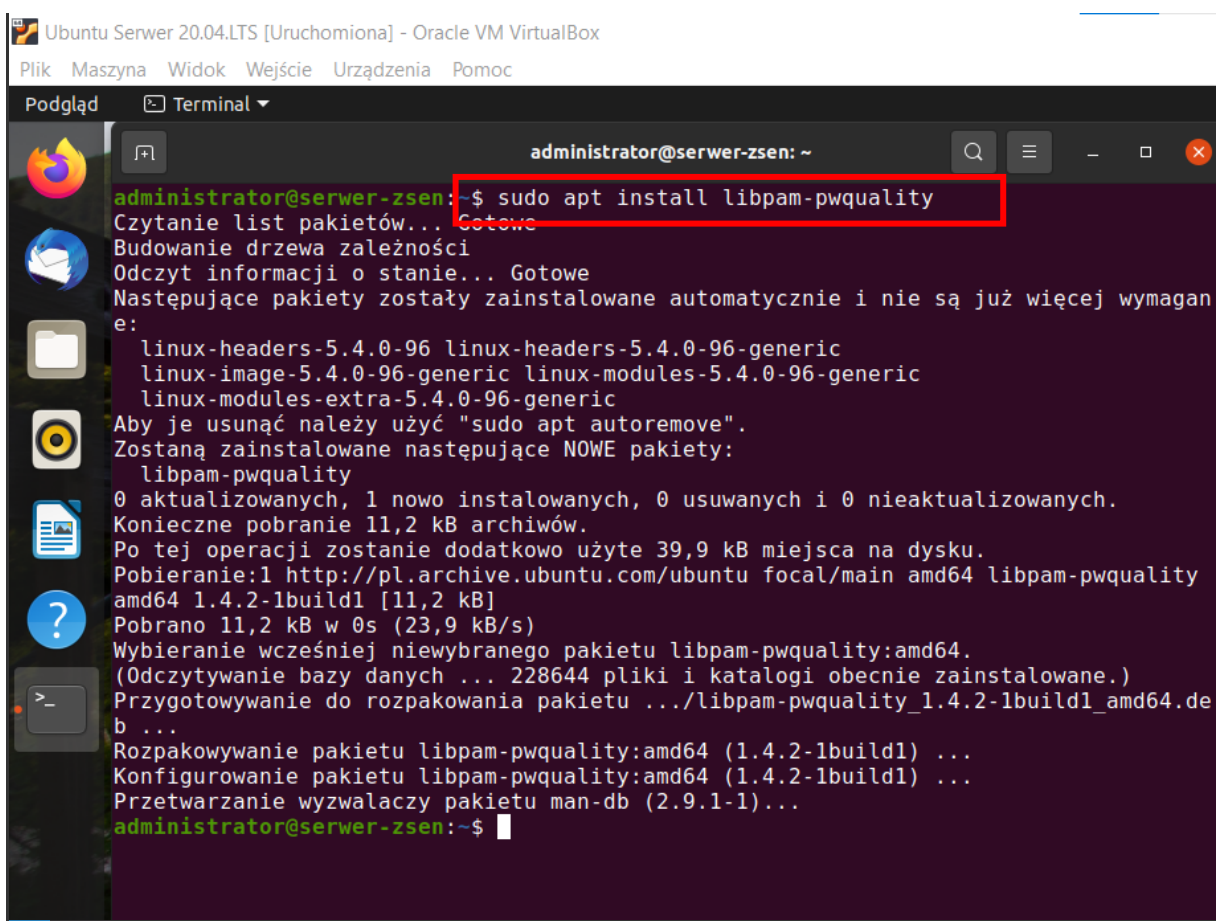


ZŁOŻONOŚĆ I HISTORIA HASEŁ UŻYTKOWNIKÓW

UBUNTU SERWER 20.04LTS

Domyślnie w systemie Ubuntu można nadawać hasła składające się przynajmniej z 6 znaków. Nie ma natomiast konieczności stosowania haseł złożonych, czyli takich, które muszą składać się np. przynajmniej z jednej cyfry, dużej litery czy znaku specjalnego (!, @, \$, *, itp.). Jeśli chcemy wymusić stosowanie dłuższych haseł oraz wymagań co do złożoności to musimy doinstalować pakiet **libpam-pwquality**.



The screenshot shows a terminal window titled "Ubuntu Serwer 20.04.LTS [Uruchomiona] - Oracle VM VirtualBox". The terminal prompt is "administrator@serwer-zsen: ~". The command "sudo apt install libpam-pwquality" has been entered and is highlighted with a red box. The output shows the package being installed, including dependencies like linux-headers and linux-image. The terminal output is as follows:

```
administrator@serwer-zsen:~$ sudo apt install libpam-pwquality
Czytanie list pakietów... Gotowe
Budowanie drzewa zależności
Odczyt informacji o stanie... Gotowe
Następujące pakiety zostały zainstalowane automatycznie i nie są już więcej wymagane:
linux-headers-5.4.0-96 linux-headers-5.4.0-96-generic
linux-image-5.4.0-96-generic linux-modules-5.4.0-96-generic
linux-modules-extra-5.4.0-96-generic
Aby je usunąć należy użyć "sudo apt autoremove".
Zostaną zainstalowane następujące NOWE pakiety:
libpam-pwquality
0 aktualizowanych, 1 nowo instalowanych, 0 usuwanych i 0 nieaktualizowanych.
Konieczne pobranie 11,2 kB archiwów.
Po tej operacji zostanie dodatkowo użyte 39,9 kB miejsca na dysku.
Pobieranie:1 http://pl.archive.ubuntu.com/ubuntu focal/main amd64 libpam-pwquality
amd64 1.4.2-1build1 [11,2 kB]
Pobrano 11,2 kB w 0s (23,9 kB/s)
Wybieranie wcześniej niewybranego pakietu libpam-pwquality:amd64.
(Odczytywanie bazy danych ... 228644 pliki i katalogi obecnie zainstalowane.)
Przygotowywanie do rozpakowania pakietu .../libpam-pwquality_1.4.2-1build1_amd64.deb ...
Rozpakowywanie pakietu libpam-pwquality:amd64 (1.4.2-1build1) ...
Konfigurowanie pakietu libpam-pwquality:amd64 (1.4.2-1build1) ...
Przetwarzanie wyzwalaczy pakietu man-db (2.9.1-1)...
administrator@serwer-zsen:~$
```

1.1

Zacniemy od zainstalowania pakietu **libpam-pwquality**. Możemy to zrobić wydając polecenie: **sudo apt install libpam-pwquality**.

```
GNU nano 4.8 /etc/pam.d/common-password
#
# /etc/pam.d/common-password - password-related modules common to all services
#
# This file is included from other service-specific PAM config files,
# and should contain a list of modules that define the services to be
# used to change user passwords. The default is pam_unix.
#
# Explanation of pam_unix options:
#
# The "sha512" option enables salted SHA512 passwords. Without this option,
# the default is Unix crypt. Prior releases used the option "md5".
#
# The "obscure" option replaces the old "OBSCURE_CHECKS_ENAB" option in
# login.defs.
#
# See the pam_unix manpage for other options.
#
# As of pam 1.0.1-6, this file is managed by pam-auth-update by default.
# To take advantage of this, it is recommended that you configure any
# local modules either before or after the default block, and use
# pam-auth-update to manage selection of other modules. See
# pam-auth-update(8) for details.
#
# here are the per-package modules (the "Primary" block)
password    requisite    pam_pwquality.so retry=3 minlen=8 dcredit=-1 ucredit=-1 ocredit=-1 enforce_for_root
password    [success=1 default=ignore] pam_unix.so obscure use_authtok try_first_pass sha512
# here's the fallback if no module succeeds
password    requisite    pam_deny.so
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success code
# since the modules above will each just jump around
password    required     pam_permit.so
# and here are more per-package modules (the "Additional" block)
password    optional     pam_gnome_keyring.so

[ Zapisano 35 linii ]
Pomoc  Zapisz  Wyszukaj  Wytnij  Wyjustuj  Bież.poz.  M-U Odwołaj  M-A Zaznacz
Wyjdź  Wczyt.plik  Zastąp  Wstaw tekst  Pisownia  Do linii  M-E Odtwórz  M-G Kopiuj
```

Po instalacji, edytujemy plik z ustawieniami tego pakietu :**sudo nano /etc/pam.d/common-password**. Na końcu linii 25 możemy dopisać następujące parametry:

- ✓ **minlen**– określający minimalną długość hasła, np. **minlen=8**
- ✓ **dcredit**– wymuszający zastosowanie cyfr, np. **dcredit=-1**
- ✓ **lcredit**– wymuszający zastosowanie małych liter, np. **lcredit=-1**
- ✓ **ucredit**– wymuszający zastosowanie wielkich liter, np. **ucredit=-1**
- ✓ **ocredit**– wymuszający zastosowanie znaków specjalnych, np. **ocredit=-1**

Aby system nie przyjmował haseł niespełniających zadanych wymagań, po takich ustawieniach były by tylko monity ze hasła nie spełniają reguł, ale i tak byłyby przyjmowane, musimy jeszcze dopisać na koniec linii **enforce_for_root**.

```
primary" block)
pam_pwquality.so retry=3 minlen=8 dcredit=-1 ucredit=-1 ocredit=-1 enforce_for_root
pam_unix.so obscure use_authtok try_first_pass sha512

[ Zapisano 35 linii ]
```

Przykład konfiguracji, zakłada ona stosowanie 8 znaków w hasle, przynajmniej jedną cyfrę, przynajmniej jedną wielką literę oraz przynajmniej jeden znak specjalny. Włączenie tego pakietu powoduje również, że zablokowane jest podawanie haseł które zawierają następujące po sobie znaki np. **qwerty123** – takie hasło nie zostanie przyjęte. Aby ustawienia zostały wprowadzone restartujemy system.

```
Ubuntu Serwer 20.04.LTS [Uruchomiona] - Oracle VM VirtualBox
Plik Maszyna Widok Wejście Urządzenia Pomoc
Podgląd Terminal 3 kwi 1'
administrator@serwer-zsen: ~
administrator@serwer-zsen:~$ sudo adduser test1
[sudo] hasło użytkownika administrator:
Dodawanie użytkownika "test1"...
Dodawanie nowej grupy "test1" (1016)...
Dodawanie nowego użytkownika "test1" (1004) w grupie "test1"...
Tworzenie katalogu domowego "/home/test1"...
Kopiowanie plików z "/etc/skel" ...
Nowe hasło :
BŁĘDNE HASŁO: Hasło zawiera mniej niż 1 wielkich liter
Nowe hasło :
BŁĘDNE HASŁO: Hasło zawiera mniej niż 1 znaków niealfanumerycznych
Nowe hasło :
BŁĘDNE HASŁO: Hasło nie przeszło sprawdzenia w słowniku - oparte na słowie ze słownika
passwd: Wykorzystano maksymalną liczbę prób dla usługi
passwd: hasło niezmienione
Ponowić próbę? [t/N] t
Nowe hasło :
BŁĘDNE HASŁO: Hasło nie przeszło sprawdzenia w słowniku - oparte na słowie ze słownika
Nowe hasło :
```

1.4
Przykład dodania konta użytkownika **test1** z hasłem **qwerty123**, następnie **Qwerty123**, następnie **Qwerty1@3**, jak widać nasze ustawienia działają.

```
Ponowić próbę? [t/N] t
Nowe hasło :
Proszę ponownie wpisać nowe hasło :
passwd: hasło zostało zmienione
Zmieniam informację o użytkowniku test1
Wpisz nową wartość lub wciśnij ENTER by przyjąć wartość domyślną
Imię i nazwisko []: test1
Numer pokoju []: 85
Telefon do pracy []: 817443314
Telefon domowy []: 555669586
Inne []: testowy
Czy informacja jest poprawna? [T/n]
```

1.5
Przykład dodania konta użytkownika **test1** z hasłem **Zsen1@#tein**. Konto zostało dodane.

Projektując politykę haseł w firmie należy ustawić również opcję, która pozwoli zapisywać historię tworzonych haseł, a także uniemożliwi stosowanie kilku zastosowanych poprzednio. Dla użytkowników to zmora, ale dla osób dbających o bezpieczeństwo środowiska IT super opcja. Dla przykładu skonfigurujemy sobie hasła tak aby system pamiętał 4 zastosowane wcześniej, a dzięki temu nie pozwoli na użycie tych samych przez 4 kolejne zmiany.

```
Ubuntu Serwer 20.04.LTS [Uruchomiona] - Oracle VM VirtualBox
Plik Maszyna Widok Wejście Urządzenia Pomoc
Podgląd Terminal
administrator@serwer-zsen: /etc/securi

administrator@serwer-zsen:~$ cd /etc/security
administrator@serwer-zsen:/etc/security$ ls -l
razem 56
-rw-r--r-- 1 root root 4564 gru 17 2019 access.conf
-rw-r--r-- 1 root root 1793 wrz  8 2018 capability.conf
-rw-r--r-- 1 root root 2234 kwi  8 2021 faillock.conf
-rw-r--r-- 1 root root 3635 gru 17 2019 group.conf
-rw-r--r-- 1 root root 2161 gru 17 2019 limits.conf
drwxr-xr-x 2 root root 4096 gru 17 2019 limits.d
-rw-r--r-- 1 root root 1440 gru 17 2019 namespace.conf
drwxr-xr-x 2 root root 4096 gru 17 2019 namespace.d
-rwxr-xr-x 1 root root 1016 gru 17 2019 namespace.init
-rw----- 1 root root  0 sie 24 2021 opasswd
-rw-r--r-- 1 root root 2972 gru 17 2019 pam_env.conf
-rw-r--r-- 1 root root 2505 sty 25 2020 pwquality.conf
-rw-r--r-- 1 root root 419  gru 17 2019 sepermit.conf
-rw-r--r-- 1 root root 2179 gru 17 2019 time.conf
administrator@serwer-zsen:/etc/security$
```

1.6

Zaczynamy od sprawdzenia czy plik, który przechowuje nam zaszyfrowane, stare hasła istnieje. Przechodzimy do katalogu `/etc/security` i listujemy zawartość. Jak widać plik znajduje się w lokalizacji `/etc/security` a jego nazwa to **opasswd**. (Jeśli nie istnieje to tworzymy plik: **sudo touch /etc/security/opasswd**)

```
Ubuntu Serwer 20.04.LTS [Uruchomiona] - Oracle VM VirtualBox
Plik Maszyna Widok Wejście Urządzenia Pomoc
Podgląd Terminal
administrator@serwer-zsen: ~
3 kwi 20:38
GNU nano 4.8 /etc/pam.d/common-password
Zmodyfikowany

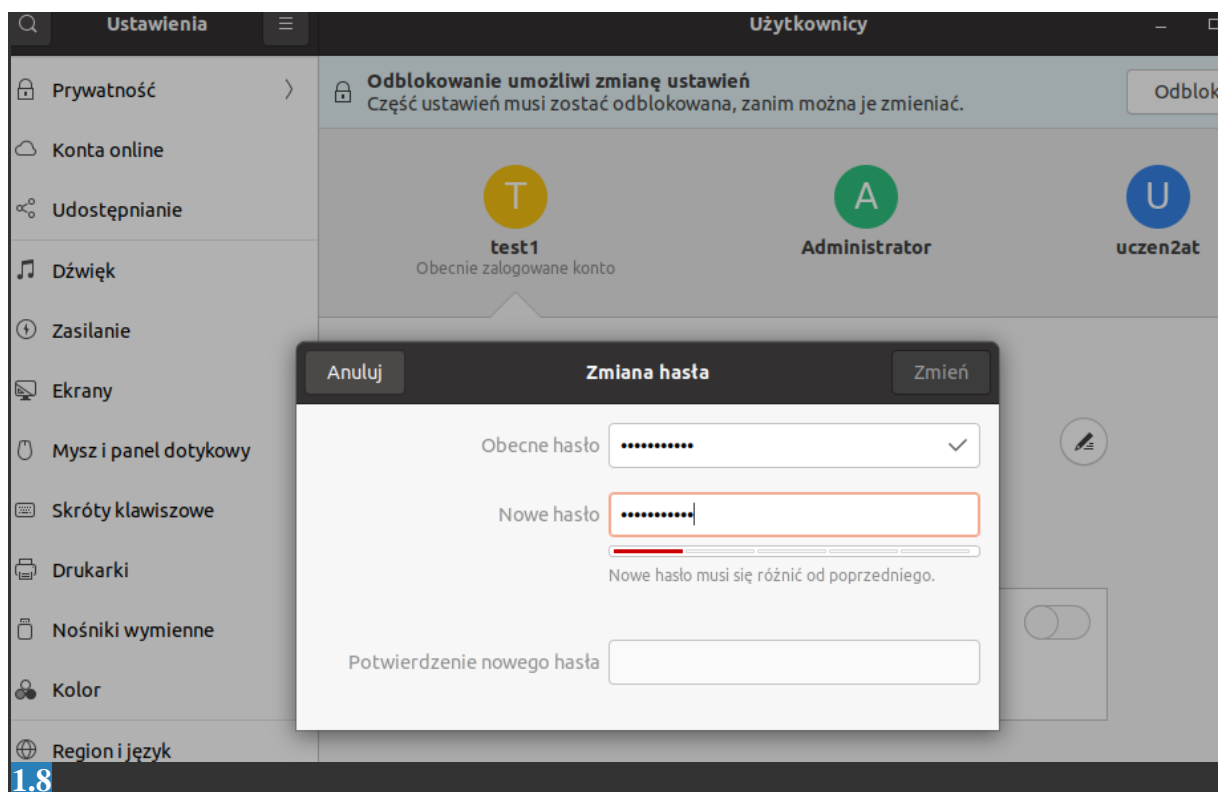
# As of pam 1.0.1-6, this file is managed by pam-auth-update by default.
# To take advantage of this, it is recommended that you configure any
# local modules either before or after the default block, and use
# pam-auth-update to manage selection of other modules. See
# pam-auth-update(8) for details.

# here are the per-package modules (the "Primary" block)
password requisite
[success=1 default=ignore]
# here's the fallback if no module succeeds
password requisite pam_unix.so remember=4 obscure use_authok try_first_pass sha512
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success code
pam_deny.so
```

1.7

Teraz ponownie edytujemy plik **common-password**, znajdujący się w lokalizacji `/etc/pam.d`: **sudo nano /etc/pam.d/common-password** następnie linii 26, po frazie **pam_unix.so** dodajemy opcję **remember** i przypisujemy dla niej wartość liczbową odpowiadającą ilości pamiętanych haseł, u nas będzie to **4**: **remember=4**

Zapisujemy zmiany w pliku, restartujemy system i od teraz nasze ustawienia haseł powinny działać.



Sprawdzamy działanie naszych ustawień. Logujemy się na naszego użytkownika **test1**, przechodzimy do ustawień i zmieniamy hasło. Podajemy obecne hasło **Zsen1@#tein** i następnie nowe takie samo **Zsen1@#tein**, jak widać nie można użyć takiego samego hasła.

test1
Obecnie zalogowane konto

Administrator

Anuluj Zmiana hasła Zmień

Obecne hasło

Nowe hasło

Potwierdzenie nowego hasła

Dodanie więcej liter, liczb i znaków interpunkcyjnych wzmocni hasło.

1.9

Podajemy obecne hasło **Zsen1@#tein** i następnie nowe hasło **zaq1@QWSx1** potwierdzamy hasło oraz wybieramy „Zmień”, hasło zostało zmienione.