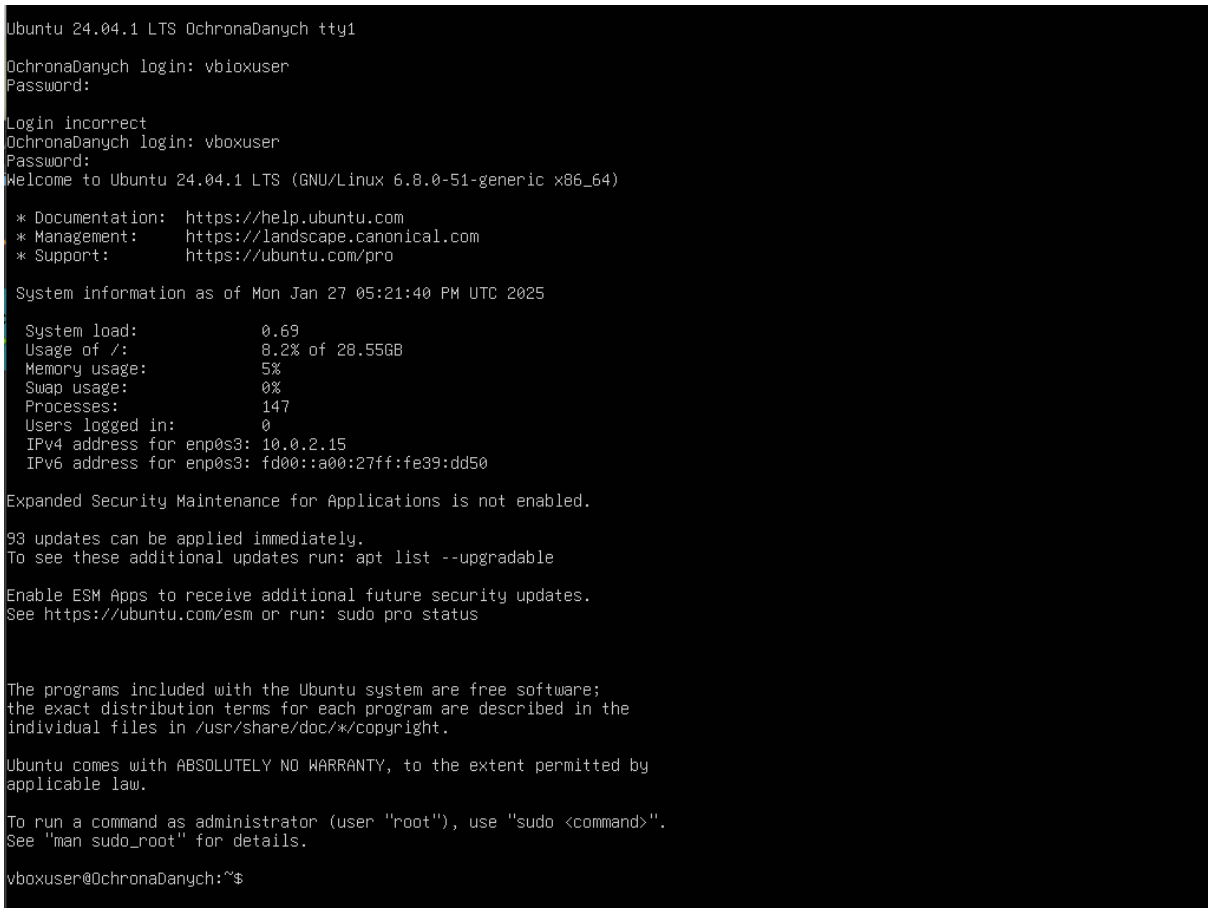
OCHRONA DANYCH ZABEZPIECZENIE SERWERA ZDALNEGO

Dominika Jabłońska

Wybór systemu operacyjnego

Potrzebny jest stabilny i często aktualizowany system operacyjny. Wybór padł na Ubuntu Server LTS. Powinno się zdecydowanie unikać korzystania z wersji eksperymentalnych.



Aktualizacja systemu

```
sudo apt update && sudo apt upgrade -y
```

Tworzenie użytkownika nieuprzywilejowanego

- Tworzenie użytkownika do administracji zamiast korzystania z root:
  ```
  sudo adduser admin
  sudo usermod -aG sudo admin
  ```

```
vboxuser@OchronaDanych:~$ sudo adduser admin
info: Adding user `admin' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `admin' (1001) ...
info: Adding new user `admin' (1001) with group `admin (1001)' ...
info: Creating home directory `/home/admin' ...
info: Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for admin
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] n
Changing the user information for admin
```

Instalacja openssh-server

```
sudo apt update
sudo apt install openssh-server
```

Utworzenie pliku konfigurującego SSH

```
sudo nano /etc/ssh/sshd_config
```

```
  GNU nano 7.2                                                    /etc/ssh/sshd_config *
Port 1025 # Zmiana domyslnej wartosci
PermitRootLogin no # Blokada logowania jako root
PubkeyAuthentication yes # Wymuszanie logowanie za pomoca kluczy SSH
PasswordAuthentication no # Blokada logowania za pomoca hasla
ChallengeResponseAuthentication no #
UsePAM yes # Wymuszanie polityki hasel itd.
AllowUsers admin # Jedynie admin moze sie logowac przez SSH
```

SSH korzysta z portu 22 domyślnie, z czego często korzystają hakerzy, którzy starają się uzyskać nieautoryzowany dostęp. Rozwiązaniem jest używanie innych portów niż te domyślne. Trzeba wybrać losowy port pomiędzy 1024 i 65535SS.

Skopiowanie klucza publicznego na serwer

```
ssh-copy-id -p 2222 admin@83.24.58.81
```

Zrestartowanie usługi, aby zmiany zaczęły działać:

```
sudo systemctl restart ssh
```

Konfiguracja PAM do limitowania logowania

```
sudo nano /etc/pam.d/sshd
```

```
  GNU nano 7.2                                                    /etc/pam.d/sshd *

# SELinux needs to be the first session rule.  This ensures that any
# lingering context has been cleared.  Without this it is possible that a
# module could execute code in the wrong domain.
session [success=ok ignore=ignore module_unknown=ignore default=bad]        pam_selinux.so close

# Set the loginuid process attribute.
session    required     pam_loginuid.so

# Create a new session keyring.
session    optional     pam_keyinit.so force revoke

# Standard Un*x session setup and teardown.
@include common-session

# Print the message of the day upon successful login.
# This includes a dynamically generated part from /run/motd.dynamic
# and a static (admin-editable) part from /etc/motd.
session    optional     pam_motd.so  motd=/run/motd.dynamic
session    optional     pam_motd.so noupdate

# Print the status of the user's mailbox upon successful login.
session    optional     pam_mail.so standard noenv # [1]

# Set up user limits from /etc/security/limits.conf.
session    required     pam_limits.so

# Read environment variables from /etc/environment and
# /etc/security/pam_env.conf.
session    required     pam_env.so # [1]
# In Debian 4.0 (etch), locale-related environment variables were moved to
# /etc/default/locale, so read that as well.
session    required     pam_env.so user_readenv=1 envfile=/etc/default/locale

# SELinux needs to intervene at login time to ensure that the process starts
# in the proper default security context.  Only sessions which are intended
# to run in the user's context should be run after this.
session [success=ok ignore=ignore module_unknown=ignore default=bad]        pam_selinux.so open

# Standard Un*x password updating.
@include common-password


auth required pam_fallock.so preauth silent deny=3 unlock_time=600 fail_interval=900
auth [success=1 default=bad] pam_unix.so
auth required pam_falllock.so authfail deny=5 unlock_time=600 fail_interval=900
```

deny=5 – Maksymalna liczba nieudanych prób logowania
unlock_time=600 – Czas w sekundach, po którym konto zostanie automatycznie odblokowane
fail_interval=900 – Okres czasu (w sekundach), w którym liczone są próby logowania

Sprawdzenie zablokowanych użytkowników:

```
sudo faillock
```

```
vboxuser@OchronaDanych:~$ sudo faillock
vboxuser:
When                Type  Source                                          Valid
```

Skonfigurowanie reguły firewall

```
sudo nano /srv/firewall.sh
```

```
  GNU nano 7.2                                                    /srv/firewall.sh
#!/bin/bash
ufw reset
ufw allow 80
ufw allow 1025
ufw allow 67/udp
ufw allow 68/udp
ufw enable
```

```
sudo chmod +x /srv/firewall.sh
sudo /srv/firewall.sh
```

```
vboxuser@OchronaDanych:~$ sudo /srv/firewall.sh
Resetting all rules to installed defaults. Proceed with operation (y|n)? y
Backing up 'user.rules' to '/etc/ufw/user.rules.20250127_185828'
Backing up 'before.rules' to '/etc/ufw/before.rules.20250127_185828'
Backing up 'after.rules' to '/etc/ufw/after.rules.20250127_185828'
Backing up 'user6.rules' to '/etc/ufw/user6.rules.20250127_185828'
Backing up 'before6.rules' to '/etc/ufw/before6.rules.20250127_185828'
Backing up 'after6.rules' to '/etc/ufw/after6.rules.20250127_185828'

Rules updated
Rules updated (v6)
Rules updated
Rules updated (v6)
Rules updated
Rules updated (v6)
Rules updated
Rules updated (v6)
Firewall is active and enabled on system startup
```

Instalacja Gitea

Instalacja MariaDB

```
sudo apt update
```

```
sudo apt install mariadb-server mariadb-client
```

Uruchomienie MariaDB

```
sudo systemctl start mariadb
sudo systemctl enable mariadb
```

Zabezpieczenie instalacji MariaDB

```
sudo mysql_secure_installation
```

```
can log into the MariaDB root user without the proper authorisation.

You already have your root account protected, so you can safely answer 'n'.

Switch to unix_socket authentication [Y/n] n
 ... skipping.

You already have your root account protected, so you can safely answer 'n'.

Change the root password? [Y/n] n
 ... skipping.

By default, a MariaDB installation has an anonymous user, allowing anyone
to log into MariaDB without having to have a user account created for
them.  This is intended only for testing, and to make the installation
go a bit smoother.  You should remove them before moving into a
production environment.

Remove anonymous users? [Y/n] y
 ... Success!

Normally, root should only be allowed to connect from 'localhost'.  This
ensures that someone cannot guess at the root password from the network.

Disallow root login remotely? [Y/n] y
 ... Success!

By default, MariaDB comes with a database named 'test' that anyone can
access.  This is also intended only for testing, and should be removed
before moving into a production environment.

Remove test database and access to it? [Y/n] y
 - Dropping test database...
 ... Success!
 - Removing privileges on test database...
 ... Success!

Reloading the privilege tables will ensure that all changes made so far
will take effect immediately.

Reload privilege tables now? [Y/n] y
 ... Success!

Cleaning up...

All done!  If you've completed all of the above steps, your MariaDB
installation should now be secure.

Thanks for using MariaDB!
```

Utworzenie bazy danych oraz użytkownika

```
sudo mysql -u root -p

CREATE DATABASE gitea CHARACTER SET utf8mb4 COLLATE
utf8mb4_unicode_ci;
```

```
MariaDB [(none)]> CREATE DATABASE gitea CHARACTER SET utf8mb4 COLLATE utf8mb_unicode_ci;
ERROR 1273 (HY000): Unknown collation: 'utf8mb_unicode_ci'
MariaDB [(none)]> CREATE DATABASE gitea CHARACTER SET utf8mb4 COLLATE utf8mb4_unicode_ci;
Query OK, 1 row affected (0.002 sec)

MariaDB [(none)]> CREATE USER 'giteauser'@'localhost' IDENTIFIED BY 'pass';
Query OK, 0 rows affected (0.009 sec)

MariaDB [(none)]> GRANT ALL PRIVILIGES ON gitea.* TO 'giteauser'@'localhost';
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use n
VILIGES ON gitea.* TO 'giteauser'@'localhost'' at line 1
MariaDB [(none)]> GRANT ALL PRIVILEGES ON gitea.* TO 'giteauser'@'localhost';
Query OK, 0 rows affected (0.008 sec)

MariaDB [(none)]> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.008 sec)
```

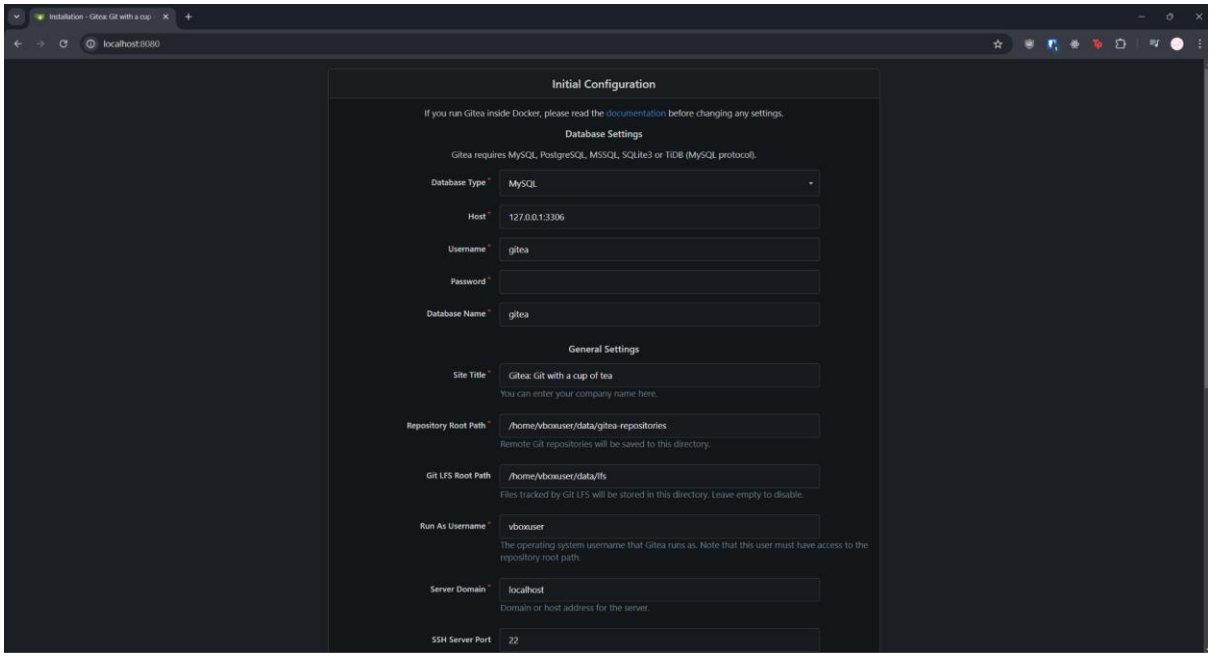
```
CREATE USER 'giteauser'@'localhost' IDENTIFIED BY 'password';
GRANT ALL PRIVILEGES ON gitea.* TO 'giteauser'@'localhost';
FLUSH PRIVILEGES;

sudo apt update
wget -O gitea https://dl.gitea.com/gitea/1.23.1/gitea-1.23.1-
linux-amd64
chmod +x gitea

sudo adduser --system --shell /bin/bash --gecos 'Git Version
Control' --group --disabled-password --home /home/git git
```

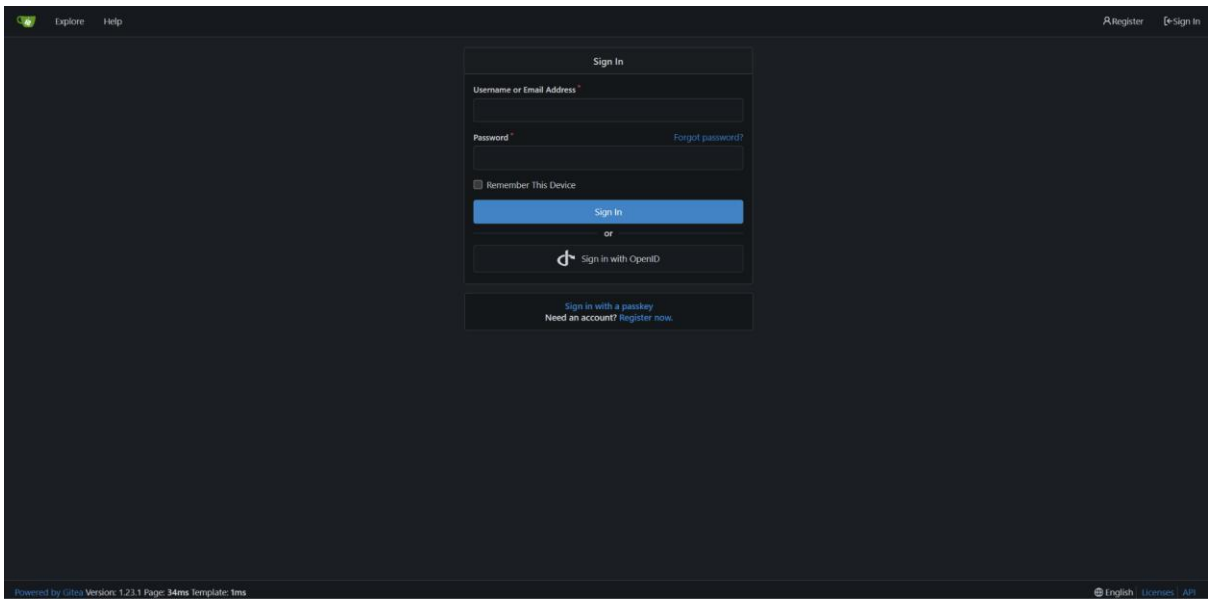
```
vboxuser@OchronaDanych:~$ sudo adduser --system --shell /bin/bash --gecos 'Git Version Control' --group --disabled-password --home /home/git git
info: Selecting UID from range 100 to 999 ...

info: Selecting GID from range 100 to 999 ...
info: Adding system user `git' (UID 112) ...
info: Adding new group `git' (GID 111) ...
info: Adding new user `git' (UID 112) with group `git' ...
info: Creating home directory `/home/git' ...
```

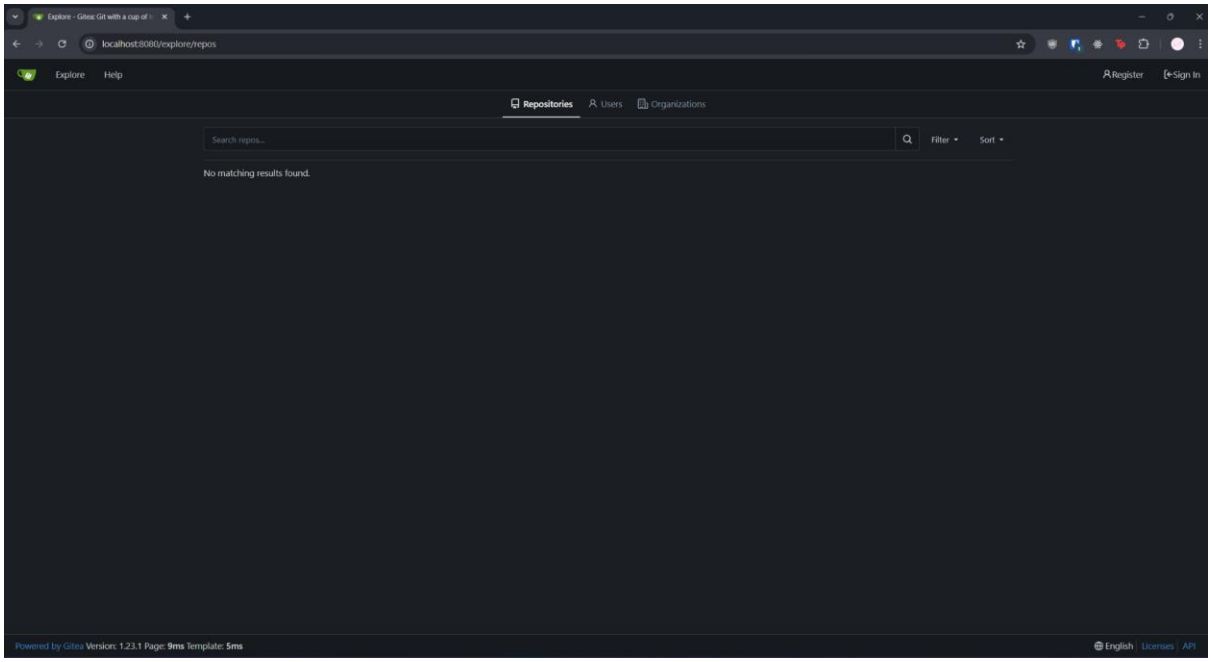
Stworzenie wymaganej struktury katalogu

```
mkdir -p /var/lib/gitea/{custom,data,log}
chown -R git:git /var/lib/gitea/
chmod -R 750 /var/lib/gitea/
mkdir /etc/gitea
chown root:git /etc/gitea
chmod 770 /etc/gitea

./gitea
```

Konfiguracja


Installation - Gitea: Git with a cup
localhost:8080
Initial Configuration
If you run Gitea inside Docker, please read the documentation before changing any settings.
Database Settings
Gitea requires MySQL, PostgreSQL, MSSQL, SQLite3 or TiDB (MySQL protocol).
Database Type *
MySQL
Host *
127.0.0.1:3306
Username *
gitea
Password *
Database Name *
gitea
General Settings
Site Title *
Gitea: Git with a cup of tea
You can enter your company name here.
Repository Root Path *
/home/vboxuser/data/gitea-repositories
Remote Git repositories will be saved to this directory.
Git LFS Root Path
/home/vboxuser/data/lfs
Files tracked by Git LFS will be stored in this directory. Leave empty to disable.
Run As Username *
vboxuser
The operating system username that Gitea runs as. Note that this user must have access to the repository root path.
Server Domain *
localhost
Domain or host address for the server.
SSH Server Port
22


Explore
Help
Register
Sign In
Sign In
Username or Email Address *
Password *
Forgot password?
Remember This Device
Sign In
or
Sign in with OpenID
Sign in with a passkey
Need an account? Register now.
Powered by Gitea Version: 1.23.1 Page: 34ms Template: 1ms
English | Licenses | API



Ograniczenie bazy danych do localhost

```
  GNU nano 7.2                                    /etc/mysql/mariadb.conf.d/50-server.cnf
#
# These groups are read by MariaDB server.
# Use it for options that only the server (but not clients) should see

# this is read by the standalone daemon and embedded servers
[server]

# this is only for the mysqld standalone daemon
[mysqld]

#
# * Basic Settings
#

#user                    = mysql
pid-file                = /run/mysqld/mysqld.pid
basedir                 = /usr
#datadir                 = /var/lib/mysql
#tmpdir                  = /tmp

# Broken reverse DNS slows down connections considerably and name resolve is
# safe to skip if there are no "host by domain name" access grants
#skip-name-resolve

# Instead of skip-networking the default is now to listen only on
# localhost which is more compatible and is not less secure.
bind-address            = 127.0.0.1

#
# * Fine Tuning
#

#key_buffer_size        = 128M
#max_allowed_packet     = 1G
#thread_stack           = 192K
#thread_cache_size      = 8
# This replaces the startup script and checks MyISAM tables if needed
# the first time they are touched
#myisam_recover_options = BACKUP
#max_connections        = 100
#table_cache            = 64

#
# * Logging and Replication
#
```

Regularne kopie zapasowe

```
mysqldump -u gitea_user -p gitea > /backup/gitea_backup.sql
```

Automatyczne aktualizacje

Można też rozważyć automatyczne aktualizacje bezpieczeństwa.

```
sudo apt install unattended-upgrades
sudo dpkg-reconfigure --priority=low unattended-upgrades
```