

??????

- DB
- ????????

????????????????

- [MySQL](#)
 - [mysql_secure_installation?????](#)
 - [????????????DB??????????](#)
- [OpenSSL](#)
 - [Ubuntu20.04?OpenSSL?1.1.1??????????3.1.1?????????](#)
 - [????????????OpenSSL 3.1.1?3.2.1????????\(Ubuntu 20.04\)](#)
- [OpenSSH](#)
 - [Ubuntu20.04?OpenSSH?8.2p1?9.6.1p?????????](#)
 - [????????????OpenSSH?9.6.1p?9.7.1????????\(Ubuntu 20.04\)](#)
- [mkcert](#)
 - [Ubuntu 22.04?mkcert????????????????](#)
- [Let's Encrypt](#)
 - [Ubuntu????Let's Encrypt????????](#)

MySQL

mysql_secure_installation?????

??

5.????????????????mysql_secure_installation????????????????

- root????????????
- ??????root????????????
- ?????????????
- test????????test????????????????

????????????????????

???????

- Ubuntu 20.04 LTS
- MySQL 8.0.32

mysql????

- ?????????

```
sudo cp -pi /etc/mysql/mysql.conf.d/mysqld.cnf /path/to/backup/directory/mysqld.cnf.$(date +%Y%m%d)
```

????????????????

- ???????

```
diff -u /etc/mysql/mysql.conf.d/mysqld.cnf /etc/old/mysqld.cnf.$(date +%Y%m%d)
```

????????????????

- ??????

```
echo -e "default_authentication_plugin=mysql_native_password" | sudo tee -a /etc/mysql/mysql.conf.d/mysqld.cnf
```

????????????????mysqld.cnf???????

?????????

- ????

```
diff -u /path/to/backup/directory/mysqld.cnf.$(date +%Y%m%d) /etc/mysql/mysql.conf.d/mysqld.cnf
```

- ????

```
+default_authentication_plugin=mysql_native_password
```

????

```
sudo systemctl restart mysql.service
```

mysql root???????

```
sudo mysql
```

????????????????????

```
ALTER USER 'root'@'localhost' IDENTIFIED WITH mysql_native_password BY 'password';
```

"?password????????????

```
flush privileges;
```

```
exit
```

mysql_secure_installation

```
sudo mysql_secure_installation
```

????

Enter password for user root:

#

VALIDATE PASSWORD COMPONENT can be used to test passwords
and improve security. It checks the strength of password
and allows the users to set only those passwords which are
secure enough. Would you like to setup VALIDATE PASSWORD component?

Press y|Y for Yes, any other key for No:

☐ Y ☐ Enter

There are three levels of password validation policy:

LOW Length >= 8

MEDIUM Length >= 8, numeric, mixed case, and special characters

STRONG Length >= 8, numeric, mixed case, special characters and dictionary

file

Please enter 0 = LOW, 1 = MEDIUM and 2 = STRONG:

0/1/2

Estimated strength of the password: 50

Change the password for root ? ((Press y|Y for Yes, any other key for No) :

n

By default, a MySQL installation has an anonymous user, allowing anyone to log into MySQL 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? (Press y|Y for Yes, any other key for No) :

anonymousY

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? (Press y|Y for Yes, any other key for No) :

rootY

Remove test database and access to it? (Press y|Y for Yes, any other key for No) :

DBY

Reload privilege tables now? (Press y|Y for Yes, any other key for No) :

y

??MySQL??????????

MySQL

????????????DB????????????

??

????????MySQL????????TIPS??

????????

1. ?????????
2. ?????????
3. ?????????????????????

????????

- ?????

```
sudo mkdir -p /home/hoge/db_password
```

????????

```
cd /home/hoge/db_password && pwd
```

????????

- ?????

????????????????(????????)

- ?????
 - ????:account.txt

```
[client]
```

```
user = RedmineDB
```

```
password = "RedmineDB"
```

password ?""????

- ?????

```
chmod 400 account.txt
```

```
ls -l account.txt
```

???????400??????????

??????????????

```
mysql --defaults-extra-file=/path/to/directory/account.txt
```

--defaults-extra-file=

??????????????????

??????????????

```
SHOW DATABASES;
```

????????????DB????????

```
EXIT
```

MySQL??????

SQL Dump??

- SQL Dump

```
mysqldump --defaults-extra-file=/path/to/directory/account.txt --no-tablespaces -h [DB] [DB] > backup.sql
```

- --no-tablespaces ?PROCESS????????????????????
- ?????????????????????
- ??????

```
ls -l backup.sql
```

???????DB????????????????????

OpenSSL

OpenSSL

Ubuntu 20.04? OpenSSL 1.1.1????? ??????? 3.1.1??????????

????????? 2023?6?????????

??

2023/09/11????????? OpenSSL 1.1.1?

2023?6??????????? 3.1.1????????????

<https://www.openssl.org/blog/blog/2023/06/15/1.1.1-EOL-Reminder/>

??

- OS: Ubuntu 20.04

```
openssl version -a
```

```
OpenSSL 1.1.1f 31 Mar 2020
built on: Wed May 24 17:14:51 2023 UTC
platform: debian-amd64
options: bn(64,64) rc4(16x,int) des(int) blowfish(ptr)
compiler: gcc -fPIC -pthread -m64 -Wa,--noexecstack -Wall -Wa,--noexecstack -g -O2 -fdebug-prefix-
map=/build/openssl-mSG92N/openssl-1.1.1f=. -fstack-protector-strong -Wformat -Werror=format-security -
DOPENSSL_TLS_SECURITY_LEVEL=2 -DOPENSSL_USE_NODELETE -DL_ENDIAN -DOPENSSL_PIC -
DOPENSSL_CPUID_OBJ -DOPENSSL_IA32_SSE2 -DOPENSSL_BN_ASM_MONT -DOPENSSL_BN_ASM_MONT5 -
DOPENSSL_BN_ASM_GF2m -DSHA1_ASM -DSHA256_ASM -DSHA512_ASM -DKECCAK1600_ASM -DRC4_ASM -
DMD5_ASM -DAESNI_ASM -DVPAES_ASM -DGHASH_ASM -DECP_NISTZ256_ASM -DX25519_ASM -DPOLY1305_ASM
-DNDEBUG -Wdate-time -D_FORTIFY_SOURCE=2
OPENSSLDIR: "/usr/lib/ssl"
ENGINESDIR: "/usr/lib/x86_64-linux-gnu/engines-1.1"
Seeding source: os-specific
```

????????

????????

1. ?????????
2. ?????????????
3. github????????????????
4. ?????????????
5. ?????????????????
6. ?????????????
7. ?????????????

??????

????????????

- Web????????????
- ?????????

????AWS Lightsail????????????????

????????????

```
sudo aptitude install build-essential checkinstall zlib1g-dev git
```

aptitude????????apt????

root??

????????

```
sudo su -
```

????????

- ?????????

```
cd /hoge && pwd
```

????????

- git clone

```
git clone https://github.com/openssl/openssl -b openssl-3.1.1
```

- ???????

```
cd openssl
```

??????????

- ????

```
./config --prefix=/usr/local/ssl --openssldir=/usr/local/ssl shared zlib
```

- make

```
make
```

make????????????????????

- ????

```
make test
```

make ????????????

- ??????

```
make install
```

??????????

- ???????

```
cat <<- __EOF__ | tee -a /etc/ld.so.conf.d/openssl-3.1.1.conf
/usr/local/ssl/lib64
__EOF__
```

- ????

```
ldconfig -v
```

- ?????????

```
mv /usr/bin/c_rehash /path/to/backup/c_rehash.$(date +%Y%m%d)
```

????????????????

```
mv /usr/bin/openssl /path/to/backup/openssl.$(date +%Y%m%d)
```

????????????????

- ????

```
cat <<- __EOF__ | tee -a /etc/environment
PATH="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/usr/local/ssl/bin"
__EOF__
```

- ???????

```
source /etc/environment
```

- ???

```
echo $PATH
```

```
PATH="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/usr/local/ssl/bin"
```

??????????????

??????????????

```
openssl version -a
```

```
OpenSSL 3.1.1 30 May 2023 (Library: OpenSSL 3.1.1 30 May 2023)
built on: Tue Jun 20 01:47:24 2023 UTC
platform: linux-x86_64
options: bn(64,64)
compiler: gcc -fPIC -pthread -m64 -Wa,--noexecstack -Wall -O3 -DOPENSSL_USE_NODELETE -DL_ENDIAN -
DOPENSSL_PIC -DOPENSSL_BUILDING_OPENSSL -DZLIB -DDEBUG
OPENSSLDIR: "/usr/local/ssl"
ENGINESDIR: "/usr/local/ssl/lib64/engines-3"
MODULESDIR: "/usr/local/ssl/lib64/openssl-modules"
Seeding source: os-specific
CPUINFO: OPENSSL_ia32cap=0x7ffaf3ffffebffff:0x27ab
```

???Ubuntu20.04??OpenSSL3.1.1????????????????

??????

- ?????????????
- ?????????????????????

??????????????

???3.1????????????1.1.x????????????????

- apt ???????

```
sudo apt-mark hold openssl
```

- aptitude ??????

```
sudo aptitude hold openssl
```

OpenSSL

????????????????OpenSSL 3.1.1?3.2.1????????(Ubuntu 20.04)

??

????????????OpenSSL3.2.1????????

?????

- Ubuntu 20.04
- [?????](#)????????????OpenSSL3.1.1????????

??????????

1. root??????
2. ?????????????????????
3. ?????????????????????
4. ???????????????

????????????

```
openssl version -a
```

“ OpenSSL 3.1.1 30 May 2023 (Library: OpenSSL 3.1.1 30 May 2023)
built on: Thu Jun 22 05:19:59 2023 UTC
platform: linux-x86_64
options: bn(64,64)
compiler: gcc -fPIC -pthread -m64 -Wa,--noexecstack -Wall -O3 -DOPENSSL_USE_NODELETE -DL_ENDIAN -DOPENSSL_PIC -DOPENSSL_BUILDING_OPENSSL -DZLIB -DDEBUG
OPENSSLDIR: "/usr/local/ssl"
ENGINESDIR: "/usr/local/ssl/lib64/engines-3"
MODULESDIR: "/usr/local/ssl/lib64/openssl-modules"
Seeding source: os-specific
CPUINFO: OPENSSL_ia32cap=0xffffa3203578bffff:0x7a9

root???

??????root????????????????????

```
sudo su -
```

????????????

```
cd /hoge && pwd
```

????????????

????????

- git clone

```
git clone https://github.com/openssl/openssl -b openssl-3.2.1
```

2024/04/02????????

- ?????????

```
cd openssl
```

????????(?????)

- ?????

```
./config --prefix=/usr/local/ssl --openssldir=/usr/local/ssl shared zlib
```

- make

```
make
```

make????????

- ????

```
make test
```

???make test????

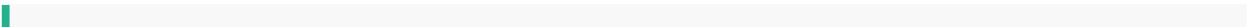
- ?????(????)

```
make install
```

????????

- SSL????

```
openssl version -a
```



OpenSSL 3.2.1 30 Jan 2024 (Library: OpenSSL 3.2.1 30 Jan 2024)
built on: Tue Apr 2 01:28:56 2024 UTC
platform: linux-x86_64
options: bn(64,64)
compiler: gcc -fPIC -pthread -m64 -Wa,--noexecstack -Wall -O3 -DOPENSSL_USE_NODELETE -
DL_ENDIAN -DOPENSSL_PIC -DOPENSSL_BUILDING_OPENSSL -DZLIB -DNDEBUG
OPENSSLDIR: "/usr/local/ssl"
ENGINESDIR: "/usr/local/ssl/lib64/engines-3"
MODULESDIR: "/usr/local/ssl/lib64/ossl-modules"
Seeding source: os-specific
CPUINFO: OPENSSL_ia32cap=0xffffa3203578bfff:0x7a9

????????????????

????????????????

OpenSSH

OpenSSH

Ubuntu 20.04 OpenSSH 8.2p1 to 9.6p1

??

[Ubuntu 20.04 OpenSSH 1.1.1 to 3.1.1](#)

???

```
ssh -V
```

????

```
OpenSSH_8.2p1 Ubuntu-4ubuntu0.9, OpenSSL 1.1.1f 31 Mar 2020
```

OpenSSH to SSL OpenSSH to OpenSSH

???

- OpenSSH
- OpenSSH to OpenSSL

??????

????URL?

- <https://askubuntu.com/questions/1189747/is-possible-to-upgrade-openssh-server-openssh-7-6p1-to-openssh-8-0p1>
- <https://qiita.com/zzz0mbie/questions/37262d1f3285500b3f45>

??

- Ubuntu 20.04
- OpenSSH 3.1.1

??????

1. ?
2. ?
3. ?
4. ?
5. OpenSSH

6. ?????????????

???

??SSH??

- ????????

```
ssh -V
```

```
OpenSSH_8.2p1 Ubuntu-4ubuntu0.9, OpenSSL 1.1.1f 31 Mar 2020
```

??????????????

```
sudo aptitude install build-essential zlib1g-dev libssl-dev libpam0g-dev libselinux1-dev libkrb5-dev
```

????????????

```
sudo mkdir /var/lib/ssh && sudo chmod -R 700 /var/lib/ssh/ && sudo chown -R root:sys /var/lib/ssh/
```

????????????

```
cd /home && pwd
```

??????????????

??????????????

- ????

```
wget -c http://mirror.exonetric.net/pub/OpenBSD/OpenSSH/portable/openssh-9.6p1.tar.gz
```

2023/12/20??????????????

- ????

```
tar -xzf openssh-9.6p1.tar.gz
```

- ???????

```
cd openssh-9.6p1
```

?????

- OpenSSL?????

which openssl

- ????

/usr/local/ssl/bin/openssl

????????

- ?????

./configure --with-kerberos5 --with-md5-passwords --with-pam --with-selinux --with-privsep-path=/var/lib/ssh/ --sysconfdir=/etc/ssh --with-ssl-dir=/usr/local/ssl

--with-ssl-dir=/usr/local/ssl] ??openssl????????????????

- make

make

- ??????

sudo make install

????????????

- ???????

ssh -V

OpenSSH_9.6p1, OpenSSL 3.1.1

????????????????????

- SSH??????

sudo systemctl restart ssh.service

- ?????????

sudo systemctl status ssh.service

active(running)?????

????????????????????SSH????????????????

??????????????

192.168.1.100.xxxxxxxxxxxxxxxxxx

- apt-get

```
sudo apt-mark hold openssh-server
```

- aptitude

```
sudo aptitude hold openssh-server
```

OpenSSH

????????????OpenSSH?9.6.1p? 9.7.1??????(Ubuntu 20.04)

??

????????????OpenSSH9.6p1???OpenSSH9.7p1????????????

??

Ubuntu 20.04????????

????????????OpenSSH????????????

??????????

- 1. ?????????????
- 2. ?????????????
- 3. OpenSSH????????????
- 4. ?????????????

????????????

```
ssh -V
```

```
OpenSSH_9.6p1, OpenSSL 3.2.1 30 Jan 2024
```

????????????

```
cd /hoge && pwd
```

????????????

????????????

- ????

```
wget -c http://mirror.exonetric.net/pub/OpenBSD/OpenSSH/portable/openssh-9.7p1.tar.gz
```

2024/04/04????????????

- ????

```
tar -xzf openssh-9.7p1.tar.gz
```

- ???????

```
cd openssh-9.7p1
```

?????

- OpenSSL????

```
which openssl
```

- ???

```
/usr/local/ssl/bin/openssl
```

??????

- ????

```
./configure --with-kerberos5 --with-md5-passwords --with-pam --with-selinux --with-privsep-path=/var/lib/ssh --  
sysconfdir=/etc/ssh --with-ssl-dir=/usr/local/ssl
```

```
--with-ssl-dir=/usr/local/ssl
```

 ??openssl????????????????

- make

```
make
```

- ?????

```
sudo make install
```

??????????

????????????????

- ?????

```
ssh -V
```

```
OpenSSH_9.7p1, OpenSSL 3.2.1 30 Jan 2024
```

????????????????

- SSH????

```
sudo systemctl restart ssh.service
```

- ?????

```
sudo systemctl status ssh.service
```

active(running)????

????????????

mkcert

??????? mkcert

mkcert

Ubuntu 22.04?mkcert?????????????????

??

- ???DNS????????
- ????????(127.0.0.1)?https???

????????mkcert????????

????????

aptitude (apt)????????

```
sudo aptitude install mkcert
```

????????

- ???????

```
mkcert -install
```

- ?????????????

```
ls -l ~/.local/share/mkcert/
```

- rootCA-key.pem ? ??
- rootCA.pem ? ?????

????????

??? /etc/hosts ??????????????????

```
127.0.0.1 agnes-luce
```

? Ubuntu????????IP??? 127.0.1.1 ??????

?????

- ???????

```
cd /hoge && pwd
```

????????????????

- ?????

```
mkcert -key-file [ ]key.$(date +%Y%m) -cert-file [ ]cert.$(date +%Y%m) [ ]
```

- ??

```
mkcert -key-file agnes-luce.key.$(date +%Y%m) -cert-file agnes-luce.crt.$(date +%Y%m) agnes-luce
```

Created a new certificate valid for the following names []

- "agnes-luce"

The certificate is at "agnes-luce.crt.202404" and the key at "agnes-luce.key.202404" []

It will expire on 14 July 2026 []

??????????

- ?????????????????

```
openssl x509 -pubkey -in [ ] -noout | openssl md5
```

- ?????????????????

```
openssl pkey -pubout -in [ ] | openssl md5
```

????????????????????

?????????2??????

Let's Encrypt

??????

?????

```
-w ????????????????????????????????????? -d ?????????????????
```

- ????????????????

????OK???