

# OpenSSL

- [Ubuntu20.04?OpenSSL?1.1.1???????????3.1.1?????????](#)
- [????????????????OpenSSL 3.1.1?3.2.1?????????\(Ubuntu 20.04\)](#)

# 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
```

???????

<https://nextgentips.com/2022/03/23/how-to-install-openssl-3-on-ubuntu-20-04/>

?????????

- 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 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 -DNDEBUG  
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=0xffffa3203578bfff: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????

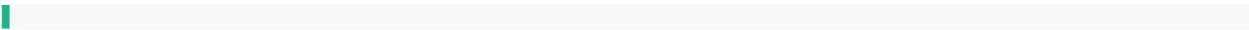
- ?????(????)

```
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=0xfffa3203578bfff:0x7a9

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

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