How to upgrade OpenSSH in Centos ?

331 Vishnupriya January 28, 2025 General, Technical 99250



Upgrade OpenSSH in Centos.

Overview: This article details how to upgrade OpenSSH in CentOS, including dependencies installation, source download, compilation, installation, verification, and post-upgrade checks for Ezeelogin functionality.

1. First you need to install a few dependencies, like development tools or build essentials and the other required packages :

```
root@localhost:~ yum groupinstall "Development Tools"

root@localhost:~ yum install zlib-devel openssl-devel
```

Make sure to backup SSH configurations before upgrading.

```
:~# cp /etc/ssh/sshd_config  /etc/ssh/sshd_config.bak
```

2. Download the OpenSSH version 9.0.

```
root@localhost:~ wget -c  https://cdn.openbsd.org/pub/OpenBSD/OpenSSH/portable/openssh-9.0p1.tar.gz

root@localhost:~ tar -xzf  openssh-9.0p1.tar.gz

root@localhost:~ cd openssh-9.0p1/
```

3 . Install PAM and SELinux Headers.

```
root@localhost:~ yum install pam-devel libselinux-devel
```

4. Compile and install SSH from sources.

```
root@localhost:~ ./configure  --with-pam --with-selinux --with-privsep-path=/var/lib/sshd/ --sysconfdir=/etc/ssh
```

```
checking for cc... cc
checking whether the C compiler works... yes
checking for C compiler default output file name... a.out
checking for suffix of executables...
checking whether we are cross compiling... no
checking for suffix of object files... o
checking whether we are using the GNU C compiler... yes
checking whether cc accepts -g... yes
checking for cc option to accept ISO C89... none needed
checking if cc supports C99-style variadic macros... yes
checking build system type... x86_64-pc-linux-gnu
checking host system type... x86_64-pc-linux-gnu
checking how to run the C preprocessor... cc -E
checking for grep that handles long lines and -e... /usr/bin/grep
checking for egrep... /usr/bin/grep -E
checking for ANSI C header files... yes

.....

.....

checking whether BROKEN_GETADDRINFO is declared... no
configure: creating ./config.status
config.status: creating Makefile
config.status: creating buildpkg.sh
config.status: creating opensshd.init
config.status: creating openssh.xml
config.status: creating openbsd-compat/Makefile
config.status: creating openbsd-compat/regress/Makefile
config.status: creating survey.sh
config.status: creating config.h
config.status: config.h is unchangedOpenSSH has been configured with the following options:

User binaries: /usr/local/bin
System binaries: /usr/local/sbin
Configuration files: /etc/ssh
Askpass program: /usr/local/libexec/ssh-askpass
Manual pages: /usr/local/share/man/manX
PID file: /var/run
Privilege separation chroot path: /var/lib/sshd/
sshd default user PATH: /usr/bin:/bin:/usr/sbin:/sbin:/usr/local/bin
Manpage format: doc
PAM support: yes
OSF SIA support: no
KerberosV support: no
SELinux support: yes
libedit support: no
libldns support: no
Solaris process contract support: no
Solaris project support: no
Solaris privilege support: no
IP address in $DISPLAY hack: no
Translate v4 in v6 hack: yes
BSD Auth support: no
Random number source: OpenSSL internal ONLY
Privsep sandbox style: seccomp_filter
PKCS#11 support: yes
U2F/FIDO support: yes
```

```
Host: x86_64-pc-linux-gnu
Compiler: cc
Compiler flags: -g -O2 -pipe -Wall -Wpointer-arith -Wuninitialized -Wsign-compare -Wformat-security -Wsizeof-pointer-memaccess -Wno-pointer-sign -Wno-unused-result -fno-strict-aliasing -D_FORTIFY_SOURCE=2 -ftrapv -fno-builtin-memset -fstack-protector-strong -fPIE
Preprocessor flags: -D_XOPEN_SOURCE=600 -D_BSD_SOURCE -D_DEFAULT_SOURCE
Linker flags: -Wl,-z,relro -Wl,-z,now -Wl,-z,noexecstack -fstack-protector-strong -pie
Libraries: -lcrypto -ldl -lutil -lz -lcrypt -lresolv -lselinux
+for sshd: -lpam

PAM is enabled. You may need to install a PAM control file
for sshd, otherwise password authentication may fail.
Example PAM control files can be found in the contrib/
subdirectory
```

```
root@localhost:~ make

root@localhost:~ make install
```

5. Once you have installed OpenSSH, restart SSH and check the version of OpenSSH

```
root@localhost:~ ssh -V

OpenSSH_9.0p1, OpenSSL 1.1.0g
```

Note: Make sure that you can add a user, reset the password of a user from the Ezeelogin GUI and you can log in to servers from the Ezeelogin shell after the OpenSSH upgrade.

6. Refer to the article below if you encounter any issues with keys after upgrading OpenSSH.

https://www.ezeelogin.com/kb/article/userauth_pubkey-signature-algorithm-ssh-rsa-not-in-pubkeyacceptedalgorithms-518.html



Related Articles:

OpenSSH vulnerability.