넥스트라인 기술지원부 김삼수(kiss@nextline.co.kr)

SSH 환경설정(sshd_config)

SSH 또는 Secure Shell은 네트워크 상의 다른 컴퓨터에 로그인하거나 원격 시스템에서 명령을 실행하고 다른 시스템으로 파일을 복사할 수 있도록 해 주는 응용 프로그램 또는 그 프로토콜을 가리킵니다. 기존의 rsh, rlogin, 텔넷 등을 대체하기 위해 설계되었으며, 강력한 인증 방법 및 안전하지 못한 네트워크에서 안전하게 통신을 할 수 있는 기능을 제공합니다. 기본적으로는 22번 포트를 사용합니다. SSH는 암호화 기법을 사용하기 때문에, 통신이 노출된다 하더라도 이해할 수 없는 암호화된 문자로 보이기 때문에 보안에 더욱 안전합니다.

설정파일 경로 : /etc/sshd/sshd_config

① 기본설정

Protocol 2
openssh는 프로토콜 버전을 원하는 대로 선택할 수 있습니다. protocol 2로 설정에는 서버는 버전 2로만 작동하기 때문에 ssh1을 사용해 접속을 요청하는 클라이언트를 받아 들일 수 없다. protocol 1로 설정해서 가동시킬 경우에는 버전 2를 사용하는 ssh2 사용자의 요청을 받아 들일 수 없다. 보안상 protocol 1 은 사용하지 않습니다.

KeyRegenerationInterval 3600
서버의 키는 한번 접속이 이루어진 뒤에 자동적으로 다시 만들어진다. 다시 만드는 목적은 나중에 호스트의 세션에 있는 키를 캡처해서 암호를 해독하거나 훔친 키를 사용하지 못하도록 하기 위함 위함입니다. 값이 0이면 키는 다시 만들어지지 않습니다. 기본값은 3600초입니다. 이 값은 자동으로 키를 재생성하기 전까지 서버가 대기할 시간을 초단위로 정의합니다.

ServerKeyBits 1024
서버 키에서 어느 정도의 비트 수를 사용할지 정의합니다. 최소값은 512이고 디폴트 값은 768입니다.

SyslogFacility AUTH
/etc/syslog.conf에서 정의한 로그 facility 코드입니다. 가능한 값은 DAEMON, USER, AUTH, LOCAL0, LOCAL1, LOCAL2, LOCAL3, LOCAL4, LOCAL5, LOCAL6, LOCAL7입니다. 기본값은 AUTH입니다. Facilith란 메시지를 생성하는 하위 시스템을 말합니다.

LogLevel INFO
로그 레벨을 지정하는 것입니다. 가능한 값은 QUIET, FATAL, ERROR, INFO, VERBOSE 그리고 DEBUGS입니다.

LoginGraceTime 600
유저의 로그인이 성공적으로 이루어지지 않았을 때 이 시간 후에 서버가 연결을 끊는 시간입니다. 값이 0 이면 제한 시간이 없으며 기본값은 600초입니다.

strictModes yes
사용자의 홈 디렉토리인 /home/username의 권한 값 등을 체크하도록 설정되어 있는 지시자입니다.

RSAAuthentication yes
RSA 인증의 시도여부를 정의합니다. ssh1 프로토콜에만 사용하기 위해 예약된 것으로,
ssh1을 사용하고 운영상 보다 안전하게 운영하려면 이 옵션을 yes로 설정해야 합니다.
RSA는 인증을 하기 위해 ssh-keygen 유틸리티에 의해 생성된 공개키 와 비밀키 쌍을 사용합니다. 현재 문서에서는 보안상 ssh1 프로토콜을 사용하지 않으므로 주석 처리합니다.

PubkeyAuthentication yes
AuthorizedKeysFile .ssh/authorized_keys
ssh에서 제공하는 인증에는 공개키 인증과 암호 인증법 이렇게 두가지가 있는데, 공개키인증을 사용할 것인지에 대해 설정하는 것입니다. 공개키 인증 사용시 공개키가 있어야 하므로 더욱 안전합니다.

RhostsAuthentication no
sshd가 rhosts 기반의 인증을 사용할 것인지 여부를 정의합니다. rhosts 인증은 안전하지 못하므로 'no'로 합니다.

IgnoreRhosts yes
IgnoreRhosts' 명령은 인증시 rhosts와 shosts 파일의 사용여부를 정의합니다.
보안상의 이유로 인증할 때 rhosts와 shosts 파일을 사용하지 않도록 합니다.

RhostsRSAAuthentication no
rhost나 /etc/hosts.equiv파일이 있으면 이것을 사용해 인증합니다. 이것은 보안상 별로 안 좋은 방법이기 때문에 허용하지 않습니다. RSA 호스트 인증과 맞추어 rhosts 인증의 사

용여부를 정의합니다.

HostbasedAuthentication no
호스트 기반의 인증 허용 여부를 결정합니다.

IgnoreUserKnownHosts yes
ssh 데몬이 RhostsRSAAuthentication 과정에서 각 사용자의 $HOME/.ssh/known_hosts를 무시할 것인지 여부를 정의합니다. rhosts 파일을 허용하지 않았으므로 yes로 설정하는 것이 안전합니다.

PasswordAuthentication yes
패스워드 인증을 허용합니다. 이 옵션은 프로토콜 버전 1과 2 모두 적용됩니다. 인증할 때 암호기반 인증방법의 사용 여부를 결정합니다. 강력한 보안을 위해 이옵션은 항상 'no'로 설정해야합니다.

PermitEmptyPasswords no
패스워드 인증을 할 때 서버가 비어있는 패스워드를 인정하는 것입니다. 기본 값은 no입니다.

X11Forwarding no
원격에서 X11 포워딩을 허용하는 것입니다. 이 옵션을 yes로 설정하면 xhost보다 안전한 방법으로 원격에 있는 X프로그램을 사용할 수 있습니다.

PrintMotd yes
사용자가 로그인 하는 경우 /etc/motd (the message of the day) 파일의 내용을 보여줄 것인지 여부결정. ssh 로그인을 환영하는 메시지나 혹은 공지사항 같은 것을 적어 놓으면 됩니다.

Subsystem sftp /usr/libexec/openssh/sftp-server
sftp는 프로토콜 버전 2에서 사용되는 것으로서 ssh와 같이 ftp의 보안을 강화하기 위해 사용되는 보안 ftp프로그램입니다.
openssh를 설치하면 /usr/local/ssh/libexec/sftp-server파일이 설치됩니다. 이것은 sftp 서버용 프로그램입니다. 클라이언트 sftp프로그램은 설치되지 않습니다. 따라서 서버로 일단 가동시키고 원도용 ssh클라이언트 프로그램이나 SSH2를 설치하면 sftp를 사용할 수 있습니다.

CheckMail (yes/no)
사용자가 로그인할 때 새메일이 도착했음을 알리도록 하는 기능을 설정하며 기본값은 yes로 되어있습니다.

Cipher (ciher)
세션을 암호화 할 때 사용할 방법을 명시해 줍니다
(idea,des,3des,blowfish,arcfour 또는 없음)

ForwardAgent
인증 대리인이 포워드 되어야 하는지를 명시 합니다.

KeepAlive yes
RequireReverseMapping no
클라이언트에게 aliive메시지를 보낼 것인지 명시하는데 접속하는 곳의 도 메인이 revers Mapping 이 되는지를 확인하여 접속을 허가할지 안 할지를 지정합니다. 실제로 internet상에 호스트들 중 revers mapping 이 안 되는 호스트가 상 당수이므로 되도록 no로 설정할 것을 권장합니다. 만약 여러분이 사용하시는 host가 revers mapping 이 확실히 되면 보안상 yes로 하는 것 이 좋겠지만 revers mapping이 되지 않으면 접속이 불가능 하므로 조심하십시오.

PasswordAuthentication (yes/no)
패스워드 기반의 인증방법을 사용할 것인지를 명시 합니다.

PubkeyAuthentication (yes/no)
인증 순서를 지정합니다.

② 보안설정

Port 22
ssh가 사용할 기본 포트를 지정합니다. 포트 변경 시 /etc/services 파일에서 sshd 관련 포트 역시 변경할 포트로 변경해 주어야 합니다.

AllowUsers root nextline
로그인 허락할 계정 nextline와 root 두 계정에게만 로그인 허용 합니다.

PermitRootLogin no

root 로그인 허용여부를 결정하는 것입니다. yes, no, without-password를 사용할 수 있습니다. 현재 no로 되어 있기 때문에 직접 root로 접속이 불가능합니다. 이옵션을 yes 로 하기보다는 일반계정으로 로그인후 su 명령으로 root로 전환하는 것이 보안상 안전합니다.

ListenAddress 0.0.0.0

sshd가 귀를 기울일 주소를 정해줍니다. 0.0.0.0은 모든 곳으로 부터 접속 을 받아들이겠다는 의미입니다. 하지만 패키징을 할때 어떻게 한것인지는 모르겠지만 tcp-wrapper의 영향을 받아서 hosts.deny에서 막혀 있으면 접속이 안되니 hosts.allow와 hosts.deny에서 sshd2 항목으로 제어를 할 수가 있습니다.

AllowedAuthentications publickey,password

Sshd2가 제공하는 인증은 password와 publickey 그리고 hostbased 방식이 있는데, 기본 적으로 public,password가 사용됩니다. 이는 순서대로 인증하는 방법을 보여주는데, 먼저 publickey로 인증하고, 두 번째로 password로 인증한다는 의미입니다.

DenyUsers nextline, 3737

접근을 거부할 로컬의 유저를 지정합니다. 위 설정은 nextline 및 uid가 3737인 계정으로 ssh 접속 시도할 경우 접근이 거부됩니다.

DenyGroups

명시된 그룹은 ssh서비스에 접근할 수 없도록 하는 기능입니다. (DenyGroups sysadmin accounting) 와일드카드가 지원되며 공백 문자로 그룹을 구분합니다.

DenyHosts

명시된 호스트는 ssh서비스에 접근할 수 없도록 하는 기능을 합니다.
(Deny Hosts shell.ourcompany.net).호스트 IP를 쓰거나 호스트 명을 쓸 수 있으며 와 일드 카드가 지원되고 공백 문자로 호스트를 구분합니다.

AllowHosts 1.2.3.0/24 192.168.1.3

로그인을 허가할 IP 또는 IP 대역을 지정합니다. 여러 개일 경우에는 공란이나 “,” 로 구분하여 나열하면 되고 도메인 이름일 경우에는 reverse mapping이 제공되어야 합니다.

AllowGroups

ssh서비스에 접근 가능한 그룹을 명시합니다. (예 : AllowGroups sysadmin accounting) 와일드카드가 지원되며 공백문자로 그룹을 구분합니다.

MaxConnections 0
최대 몇개의 접속을 허락할지를 지정합니다. 0은 제한을 하지 않습니다.

PasswordGuesses 3
암호인증 방식으로 인증할 때 최대 몇 차례 시도를 허용할 것인지 지정합니다.

ssh1Compatibility no
클라이언트가 ssh1만 지원할 경우 ssh1 데몬을 실행할 것인지 여부를 지정합니다. ssh1은 보안상 취약하므로 no로 하는 것이 좋습니다.