Linux 서버에서 SSH 서비스 포트 변경방법 (TCP 22 → TCP 8022)

○ 변경방법

1. SSH 서비스 포트 확인 및 변경하기
2. 서버 방화벽 설정 확인 및 변경하기
3. SSH 서비스 보안 강화를 위한 기타 설정

※ 본 SSH(Secure Shell) 서비스 포트 변경 방법은 CentOS 5.5 배포판 기준으로 정리 되었습니다.

기타 배포판을 사용 중인 경우 해당 배포판에 관한 자료를 확인하여 주시기 바랍니다.

---

1. SSH 서비스 포트 확인 및 변경하기

가. SSH 서비스 포트(TCP 22) 확인하기

netstat -ant

```
[infra@localhost ~]$ netstat -ant
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address               Foreign Address             State
tcp        0      0 127.0.0.1:2208              0.0.0.0:*                   LISTEN
tcp        0      0 0.0.0.0:111                 0.0.0.0:*                   LISTEN
tcp        0      0 127.0.0.1:631               0.0.0.0:*                   LISTEN
tcp        0      0 0.0.0.0:700                 0.0.0.0:*                   LISTEN
tcp        0      0 127.0.0.1:2207              0.0.0.0:*                   LISTEN
tcp        0      0 :::22                       :::*                        LISTEN
tcp        0      0 ::ffff:166.104.182.126:22   ::ffff:166.104.91.81:63663  ESTABLISHED
tcp        0      0 ::ffff:166.104.182.126:22   ::ffff:166.104.91.81:63510  TIME_WAIT
```

나. SSH 서비스 포트(TCP 8022) 변경하기

- 변경화일 : /etc/ssh/sshd_config

```
[root@localhost ssh]# ls -al /etc/ssh
합계 228
drwxr-xr-x   2 root root   4096 10월 11 13:15 .
drwxr-xr-x 106 root root  12288 10월 11 11:35 ..
-rw-------   1 root root 132839  9월 13 01:00 moduli
-rw-r--r--   1 root root   1827  9월 13 01:00 ssh_config
-rw-------   1 root root    672 10월  8 16:25 ssh_host_dsa_key
-rw-r--r--   1 root root    590 10월  8 16:25 ssh_host_dsa_key.pub
-rw-------   1 root root    963 10월  8 16:25 ssh_host_key
-rw-r--r--   1 root root    627 10월  8 16:25 ssh_host_key.pub
-rw-------   1 root root   1675 10월  8 16:25 ssh_host_rsa_key
-rw-r--r--   1 root root    382 10월  8 16:25 ssh_host_rsa_key.pub
-rw-------   1 root root   3333 10월 11 13:13 sshd_config
```

- 수정내용 : Port 8022 (vi 에디터를 사용하여 포트번호 수정)

  # vi sshd_config

```
#       $OpenBSD: sshd_config,v 1.73 2005/12/06 22:38:28 reyk Exp $

# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/local/bin:/bin:/usr/bin

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options change a
# default value.

#Port 22
Port 8022
#Protocol 2,1
Protocol 2
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
```

다. 포트 설정 변경 후 SSH 서비스 재구동

  # /etc/init.d/sshd restart

라. 변경된 SSH 서비스 포트(TCP 8022) 확인하기

  # netstat -ant

```
[root@localhost ssh]# netstat -ant
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address               Foreign Address             State
tcp        0      0 127.0.0.1:2208              0.0.0.0:*                   LISTEN
tcp        0      0 0.0.0.0:111                 0.0.0.0:*                   LISTEN
tcp        0      0 127.0.0.1:631               0.0.0.0:*                   LISTEN
tcp        0      0 0.0.0.0:700                 0.0.0.0:*                   LISTEN
tcp        0      0 127.0.0.1:2207              0.0.0.0:*                   LISTEN
tcp        0      0 :::8022                     :::*                        LISTEN
tcp        0      0 ::ffff:166.104.182.126:8022 ::ffff:166.104.91.81:61273  ESTABLISHED
```

마. 변경된 SSH 서비스 포트로 접근하기

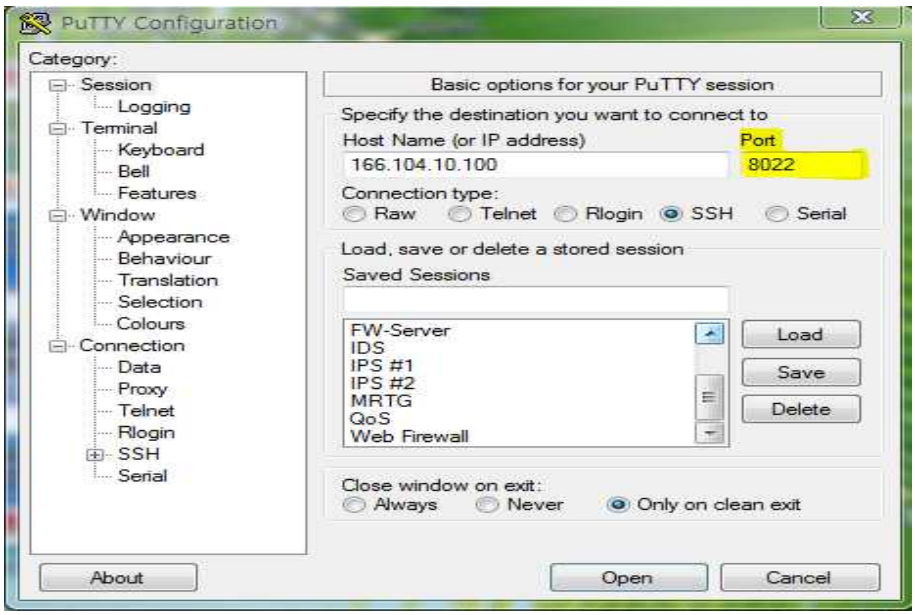
- ssh 명령어로 접근하는 경우

  * ssh 계정명@해당서버주소(IP) -p 8022

```
[infra@localhost ~]$ ssh infra@166.104.182.126 -p 8022
infra@166.104.182.126's password:
Last login: Mon Oct 11 14:50:57 2010 from 166.104.182.126
```

- putty등 접근 프로그램 이용하는 경우

  * 해당 서버 IP 입력 후 접근 port 를 8022로 지정 후 접근



바. SSH 서비스 포트 변경 후 접근이 되지 않는 경우 확인사항

- **개인 방화벽 서비스 중단 후 접근 여부 확인하기**(iptables 서비스)

  # /etc/init.d/iptables stop

- 개인 방화벽 서비스 중단 후 서비스 접근이 되는 경우 방화벽 설정 변경 필요

2. 서버 방화벽(iptables) 설정 확인 및 변경하기

가. 서버 방화벽(iptables) 설정 사항 확인하기

iptables -L -n

```
[root@localhost ~]# iptables -L -n
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
RH-Firewall-1-INPUT  all  --  0.0.0.0/0           0.0.0.0/0

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
RH-Firewall-1-INPUT  all  --  0.0.0.0/0           0.0.0.0/0

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain RH-Firewall-1-INPUT (2 references)
target     prot opt source               destination
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0
ACCEPT     icmp --  0.0.0.0/0            0.0.0.0/0           icmp type 255
ACCEPT     esp  --  0.0.0.0/0            0.0.0.0/0
ACCEPT     ah   --  0.0.0.0/0            0.0.0.0/0
ACCEPT     udp  --  0.0.0.0/0            224.0.0.251         udp dpt:5353
ACCEPT     udp  --  0.0.0.0/0            0.0.0.0/0           udp dpt:631
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:631
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           state NEW tcp dpt:22
REJECT     all  --  0.0.0.0/0            0.0.0.0/0           reject-with icmp-host-prohibited
```

나. 서버 방화벽(iptables) 설정 변경하기

- 변경화일 : /etc/sysconfig/iptables
- 변경내용 : 포트 변경 (22 → 8022)

  -A RH-Firewall-1-INPUT -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT

  -A RH-Firewall-1-INPUT -p tcp -m state --state NEW -m tcp --dport 8022 -j ACCEPT

```
[root@localhost sysconfig]# cat /etc/sysconfig/iptables
# Firewall configuration written by system-config-securitylevel
# Manual customization of this file is not recommended.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:RH-Firewall-1-INPUT - [0:0]
-A INPUT -j RH-Firewall-1-INPUT
-A FORWARD -j RH-Firewall-1-INPUT
-A RH-Firewall-1-INPUT -i lo -j ACCEPT
-A RH-Firewall-1-INPUT -p icmp --icmp-type any -j ACCEPT
-A RH-Firewall-1-INPUT -p 50 -j ACCEPT
-A RH-Firewall-1-INPUT -p 51 -j ACCEPT
-A RH-Firewall-1-INPUT -p udp --dport 5353 -d 224.0.0.251 -j ACCEPT
-A RH-Firewall-1-INPUT -p udp -m udp --dport 631 -j ACCEPT
-A RH-Firewall-1-INPUT -p tcp -m tcp --dport 631 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 8022 -j ACCEPT
-A RH-Firewall-1-INPUT -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

다. 서버 방화벽(iptables) 변경사항 적용하기

- 변경적용 : /etc/init.d/iptables restart
- 변경내용 확인 : # iptables -L -n

```
[root@localhost ssh]# iptables -L -n
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
RH-Firewall-1-INPUT  all  --  0.0.0.0/0           0.0.0.0/0

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
RH-Firewall-1-INPUT  all  --  0.0.0.0/0           0.0.0.0/0

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain RH-Firewall-1-INPUT (2 references)
target     prot opt source               destination
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0
ACCEPT     icmp --  0.0.0.0/0            0.0.0.0/0           icmp type 255
ACCEPT     esp  --  0.0.0.0/0            0.0.0.0/0
ACCEPT     ah   --  0.0.0.0/0            0.0.0.0/0
ACCEPT     udp  --  0.0.0.0/0            224.0.0.251         udp dpt:5353
ACCEPT     udp  --  0.0.0.0/0            0.0.0.0/0           udp dpt:631
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:631
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           state NEW tcp dpt:8022
REJECT     all  --  0.0.0.0/0            0.0.0.0/0           reject-with icmp-host-prohibited
```

라. 변경된 SSH 서비스(8022) 포트로의 접근 상태 확인

- 확인 : # netstat -antp

```
[infra@localhost ~]$ netstat -antp
(No info could be read for "-p": geteuid()=500 but you should be root.)
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address               Foreign Address             State       PID/Program name
tcp        0      0 127.0.0.1:2208              0.0.0.0:*                   LISTEN      -
tcp        0      0 0.0.0.0:111                 0.0.0.0:*                   LISTEN      -
tcp        0      0 127.0.0.1:631               0.0.0.0:*                   LISTEN      -
tcp        0      0 0.0.0.0:700                 0.0.0.0:*                   LISTEN      -
tcp        0      0 127.0.0.1:2207              0.0.0.0:*                   LISTEN      -
tcp        0      0 :::8022                     :::*                        LISTEN      -
tcp        0      0 ::ffff:166.104.182.126:8022 ::ffff:166.104.91.81:51146  ESTABLISHED -
tcp        0      0 ::ffff:166.104.182.126:22   ::ffff:166.104.91.81:63663  ESTABLISHED -
```

```
[infra@localhost ~]$ netstat -antp
(No info could be read for "-p": geteuid()=500 but you should be root.)
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address               Foreign Address             State       PID/Program name
tcp        0      0 127.0.0.1:2208              0.0.0.0:*                   LISTEN      -
tcp        0      0 0.0.0.0:111                 0.0.0.0:*                   LISTEN      -
tcp        0      0 127.0.0.1:631               0.0.0.0:*                   LISTEN      -
tcp        0      0 0.0.0.0:700                 0.0.0.0:*                   LISTEN      -
tcp        0      0 127.0.0.1:2207              0.0.0.0:*                   LISTEN      -
tcp        0      0 :::8022                     :::*                        LISTEN      -
tcp        0      0 ::ffff:166.104.182.126:8022 ::ffff:166.104.91.81:52849  ESTABLISHED -
```

※ 서버 방화벽(iptables)을 이용한 IP별 접근 제한

- iptables 정책을 이용하여 특정 IP에 대해서만 서버에 접근할 수 있도록 필터링 정책을 운영할 수 있다.

-A RH-Firewall-1-INPUT -s [접근허용IP] -p tcp -m state --state NEW -m tcp --dport 8022 -j ACCEPT

3. SSH 서비스 보안 강화를 위한 기타 설정

- /etc/ssh/sshd_config 설정 변경을 통한 SSH 서비스 보안 강화 방법

가. root로 SSH 서비스 직접 접근 제한(보안을 위해 일반계정으로 로그인 후 su 명령으로 사용)
  - PermitRootLogin no

나. 인증 실패시 재시도 횟수 설정(3회)
  - MaxAuthTries 3

다. 로그인이 성공적으로 이루어지지 않은 경우 서버가 연결을 끊는 시간 설정(600초)
  -LoginGraceTime 600