
# 리눅스 명령어 top10

https://www.youtube.com/watch?v=u9RukvKZJZM

## 1.Server를 어떻게 접속하나요? 특별히 사용하는 도구나 방법이 있을까요?

신입 지원자에게는 SSH와 그 원리를 알고 있는지 Password가 아닌, Key 방식을 사용해보았는지 그리고 2~4년 경력을 가지고 있는 Jr엔지니어는 전자를 포함함 내용과 특정 도구와 대체 도구들도 물어보는 편

https://wlsvud84.tistory.com/12

# SSH

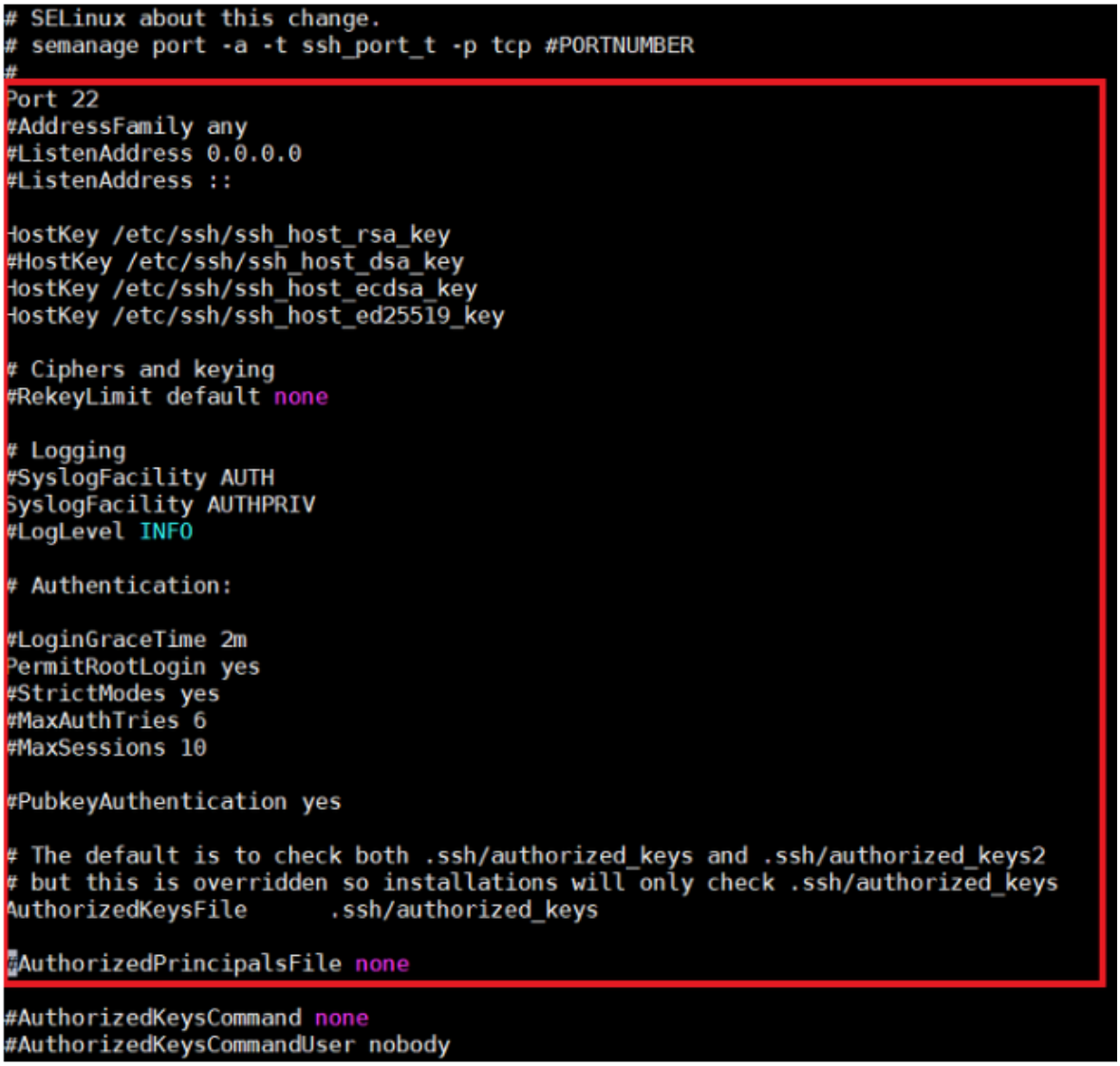
**보안적으로 취약했던 rsh, rlogin, telnet 등을 대체하기 위해 설계되었고 Secure shell의 약자이다.**

**기본 22번 port를 사용해 네트워크로 연결한다.**

- systemctl enable sshd ( 재부팅 후 자동등록 )
- systemctl start sshd ( 서비스 시작 )
- systemctl status sshd ( 서비스 상태 확인 )
- ps -ef | grep sshd ( 프로세스 상태 확인 )
- **vi /etc/ssh/sshd_config**

ssh관련된 설정을 변경해준다. 예를 들면 port번호 22번을 바꿀 수 있다.

기본 port번호는 보안상 취약하므로 이 경우 port번호를 바꾸는 경우가 종종 있다.




#Port 22

ssh 기본 접속 port는 22번. 임의의 port 번호를 지정해서 사용하고 계신 환경이라면 번호 지정 후에 주석을 해제

#ListenAddress 0.0.0.0

기본 default 값은 주석이 처리되어 있어서 정책이 동작하지 않지만 주석을 해제하고 특정 ip를 지정하면 해당하는 ip에서만 접속이 허용

HostKey /etc/ssh/ssh_host_rsa_key

#HostKey /etc/ssh/ssh_host_dsa_key

HostKey /etc/ssh/ssh_host_ecdsa_key

HostKey /etc/ssh/ssh_host_ed25519_key

ssh 접속을 할 때 필요한 암호화 키가 저장되는 위치로 기본으로 default ECDSA_KEY 암호화 방식을 사용

## SSH 접속( 원격시 접속 )

**ssh [사용자 계정]@[원격지 ip]**

**ssh root@192.168.159.129**

**exit**

**ssh [원격 계정]@[원격지_ip] -p [변경할 포트]  ( 포트 변경 시 지정해서 접속 )**

ex) ssh -A ec2-user@3.36.244.20 : 아마존  서버의 ip로 접근중

**PuTTY사용해서 접근한 거 기억해라!**

**ip선택하고 SSH선택한다음에 아이디랑 패스워드 넣고 들어갔다!!**

# 2.IP를 확인하는 리눅스 명령어는 무엇인가요? 자신의 Public IP는 어떻게 확인하나요?

private ip

ifconfig

컴퓨터 이름의 inet을 확인 이것은 IPv4 주소, inet6는 IPv6의 주소

(AWS의 경우 eth0이 컴퓨터 이름)

public ip

curl ifconfig.co // curl ifconfig.me

★추가 질문

# NAT

https://jwprogramming.tistory.com/30

네트워크 주소 변환(Network Address Translation)

NAT는 IPv4의 주소 부족 문제를 해결하기 위한 방법으로서 고려되었으며, 주로 비공인(사설, local) 네트워크 주소를 사용하는 망에서 외부의 공인망(public, 예를 들면 인터넷)과의 통신을 위해서 네트워크 주소를 변환하는 것입니다.

NAT를 이용하는 이유는 대개 사설 네트워크에 속한 여러 개의 호스트가 하나의 공인 IP 주소를 사용하여 인터넷에 접속하기 위해 사용합니다.

외부 통신망 즉 인터넷망과 연결하는 장비인 라우터에 NAT를 설정할 경우 라우터는 자신에게 할당된 공인 IP주소만 외부로 알려지게 하고, 내부에서는 사설 IP주소만 사용하도록 하여 필요시에 이를 서로 변환시켜 줍니다. 따라서 외부 침입자가 공격하기 위해서는 사설망의 내부 사설 IP주소를 알아야 하기 때문에 공격이 불가능해지므로 내부 네트워크를 보호할 수 있게 됩니다.

# 퍼블릿 서브넷과 프라이빗 서브넷

퍼블릭 서브넷은 외부에서 직접 IP를 찍어서 들어올 수 있는 서브넷이고 프라이빗 서브넷은 다른 자원(Load balancer, Proxy 등)을 통하지 않으면 들어올 수 없다.

VPC내 프라이빗 서브넷만 생성하면 완벽히 단절된 네트워크를 만들 수 있다.

**cmd창에서 ipconfig를 친다음의 결과값을 봐라. wifi에서 IPv4에 해당되는 것이 IP이다.**

# 3.웹사이트가 잘 작동하는지 체크할 때 사용하는 명령어는? curl을 사용해본적은 있는지?사용해보았다면 주로 어떨때 사용하는지?

웹사이트를 잘 작동하는지 확인할 때 curl을 주로 사용한다. curl+도메인 이름

주로 curl을 사용해보았는지와 그 사용을 얼마만큼 했는지에 대한 질문, 단순 사용을 넘어 GET, POST 지정을 해보았는지와 ★**-v 옵션**에 대한 결과 내용 이해를 묻는 연계 질문

- curl google.com

html 관련된 코드가 나온다.

- curl **-v** google.com

html뿐만 아니라 SSL관련된 부분도 나온다.

## SSL

SSL(Secure Sockets Layer)은 암호화 기반 인터넷 보안 프로토콜로 URL에는 HPPTS가 있다. 보안면에서 뛰어나다. SSL은 SSL 인증서(공식적으로 "TLS 인증서")가 있는 웹사이트만 실행할 수 있다. SSL 인증서는 사람의 신원을 확인하는 신분증이나 배지와 같다.

SSL 인증서 공개키→암호화 // 개인키→암호화 해독

# 4.domain의 ip를 조회하는 명령어는?

nslookup에 대한 질문, 도메인 질의 절차에 대해서 이해하는지 확인하기 위한 질문

nslookup 웹사이트

# 5.웹서버 혹은 DB 같은 서버들을 확인하는 방법은?

telnet 혹은 nc같은 명령어를 이해하고 있는지에 대한 질문

ping과 telent의 차이 등을 명확히 알고 있는지를 묻는 질문 (TCP,UDP,ICMP)

https://jink1982.tistory.com/131

### ping은 목적지 서버를 통하는 네트워크 상태를 체크

ping 사용법은 아래와 같다

ping [목적지 IP주소]
ex) ping 204.111.111.1

사용 결과는..

ping 204.111.111.1
PING 204.111.111.1 (204.111.111.1) : 56 data bytes
 64 bytes from 204.111.111.1: icmp_seq=0 ttl=228 time=92.552ms
 64 bytes from 204.111.111.1: icmp_seq=1 ttl=228 time=95.352ms
 64 bytes from 204.111.111.1: icmp_seq=2 ttl=228 time=102.252ms
 64 bytes from 204.111.111.1: icmp_seq=3 ttl=228 time=72.152ms
 64 bytes from 204.111.111.1: icmp_seq=4 ttl=228 time=82.942ms
결과를 보면 총 5회에 걸쳐서 목적지 서버에 데이터를 보내고 응답받은 시간을 맨 오른쪽에 표시 한다. 응답이 오지 않거나 시간이 1000ms 이상 걸리면 중간에 문제가 발생 한 것이라 생각 하면 된다.

## telnet은 목적지 서버의 해당 어플리케이션까지 살아 있는지 확인

서버접속은 되지 않고 위와같이 ping테스트를 했는데도 이상이 없으면 해당 어플리케이션이 종료 되었는지 확인 해야 된다.
그러기 위해서는 telnet을 사용하는 방법이 있다.

telnet 사용법은 아래와 같다.

ping [목적지 IP주소] [어플리케이션 port 정보]
ex) ping 204.111.111.1 9002  ping google.com 80
사용 결과는...

telnet 204.111.111.1 9002
trying 204.111.111.1
Connected to 204.111.111.1
Escape character is '^]'.
위와 같이 결과가 나오면 목적지 서버의 접속은 물론이고 해당 어플리케이션도 정상 동작 한다고 볼 수 있다.
telnet: Unable to connect to remote host: Connection refused
와 같은 결과를 보면 해당 어플리케이션이 종료 되었거나 방화벽이 막혀있는지 확인해 본다.

## traceroute는 출발지와 목적지 사이의 라우터를 모두 추적

traceroute 사용법은 아래와 같다.

traceroute [목적지 IP주소]
ex) traceroute 204.111.111.1 9002

사용 결과는...

traceroute 204.111.111.1
traceroute to 204.111.111.1 (204.111.111.1), 64 hops max, 40 byte packets
1 204.112.111.2 1.428 ms 0.850 ms 0.655 ms
2 204.113.113.3 1912.428 ms 1910.850 ms 1911.655 ms
3 204.111.111.1 1.827 ms 1.850 ms 1.655 ms
위와같이 결과를 보면 출발지에서 목적지까지 거쳐가는 라우터의 응답시간을 모두 확인 할 수있다.
빨간 글씨로 되어있는 부분을 주목해 보면  1900 ms가 넘어 간다.
이말은 1.9초 정도 걸린다고 봐야 하는데 네트워크상 이정도면 엄청 느리고 문제가 있다고 봐야한다.

ping 테스트 결과가 느리거나 접속이 안되면 traceroute를 이용해서 어떤 라우터에서 문제를 일으키는지 살펴 보아야 한다.

## 6.내 서버의 서버가 잘 떠있는지, 현재 DB 커넥션 등을 확인하는 명령어는?

netstat 명령어와 그 옵션 등을 사용해보았는지에 대한 것을 묻는 질문

netstat -lntp

netstat -an | grep “port”

## 7.리눅스에서 특정 프로세스를 확인하는 명령어는? java process id, option 등을 확인하고 싶다면?

ps -ef  | grep 프로그램명

ps aux | grep 프로그램명

## 8.리눅스에서 CPU,Memory,Disk 등 시스템 정보등을 확인하는 명령어들은?

top

sar

free

/proc/meminfo

df

iostat

모니터링을 위해 쓰인 앱을 사용했는지 알기 위한 것들

## 9.리눅스에서 서비스들은 어떻게 관리되고 그와 연관된 명령어는?

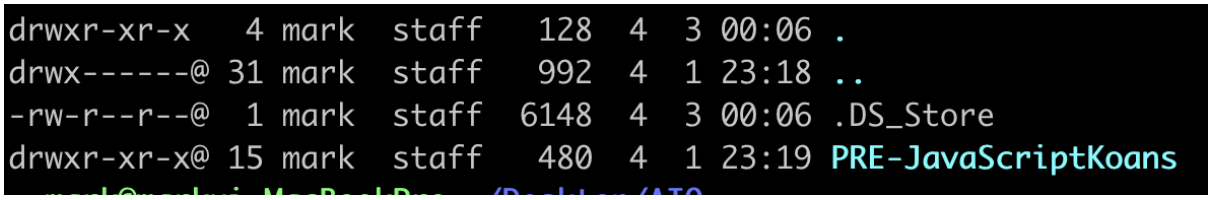
service tomcat start

service tomcat status

## 10.리눅스 파일 권한 체계를 이해하고 있는지

https://velog.io/@wmc1415/리눅스-권한permisson-설정chmodchown1

일단 내가 수정할려는 파일 폴더내에서 ls-al(Terminal에서)이라는 명령어를 친다.




그러면 위의 사진처럼 현재위치에 있는 폴더 파일들을 자세히 볼 수 있습니다.

drwxr-xr-x 4 mark staff 128 4 3 0066.위에 있는 문구를 하나씩 분석을 해보자

- 제일 앞에 있는 d는 파일type을 나타냄.  'd'-> dir , '-' -> 일반파일
- rwxr-xr-x: 권한정보를 나타냄.해당 파일에 어떤 권한이 부여되어 있는지 확인가능.
- 4 : 링크수
- mark : 해당 파일의 소유자
- staff : 소유그룹
- 128 : 파일의 용량

- 4 3 0066 : 생성날짜.: 파일의 이름

우선 권한정보를 나태내는게 어떤것이 있는지 알아보자.(제일 중요!)

퍼미션의 종류

- r(읽기): 파일의 읽기 권한
- w(쓰기): 파일의 쓰기 권한
- x(실행): 파일의 실행 권한

그렇다면 위에서 권한정보를 분석을 해보자.

> rwxr-xr-x

우선 3자리씩 끊어서 분석을 하면된다.

rwx(소유자가 접근할 수 있는 권한) / r-x(그룹에 속한 사용자들 접근권한)/ r-x(모든 사용자가 접근할 수 있는권한)

- 첫번째로 rwx: 소유자에 대한 권한이다.소유자는 r(읽기),w(쓰기),x(실행)가 허용된다.
- 두번째로 r-x: 그룹에 대한 권한이다.(여기서 -는 권한이 없다라고 생각하면된다).소유그룹에 속하고 있는 사용자들은 r(읽기),x(실행)가 허용된다.
- 세번째로 r-x: 모든사용자들에 대한 권한이다.소유그룹과 마찬가지로 r(읽기),x(실행)가 허용된다.

# 11.yum vs apt-get

- **Linux** 는 크게 **레드햇, 데비안, 우분투** 3가지로 분류되며, 계열에 따른 패키지 **관리 명령어**가 다르다.
- **레드햇 계열**은 **yum** 을 사용하고
  - 레드햇 엔터프라이즈
  - 페도라
  - CentOS
- **데비안, 우분투 계열**은 **apt-get** 을 사용한다.