12장

NFS, Samba, FTP, SSH 운영하기

전체 내용

NFS 설치와 운영

Samba 설치와 운영

FTP Server 설치와 운영

SSH Server 설치와 운영

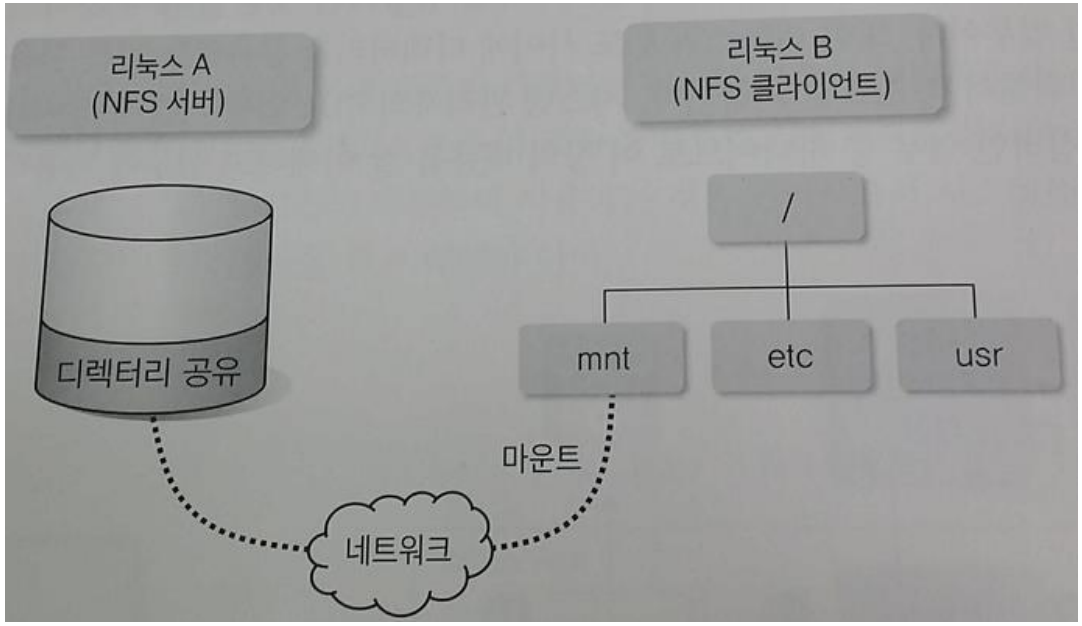
1 – NFS 설치와 운영

NFS 개념

NFS 서버 설치 및 구성하기

1 – NFS 설치와 운영

- NFS 개념
  - NFS(Network File System)는 네트워크를 통해 다른 시스템(Linux, Unix, Windows)의 디스크에 연결하여 자원을 사용하는 것이다
  - NFS Server 측에서 디스크를 공유하고 NFS Client에서는 Mount를 하여 접속하여 파일과 디렉터리를 사용한다

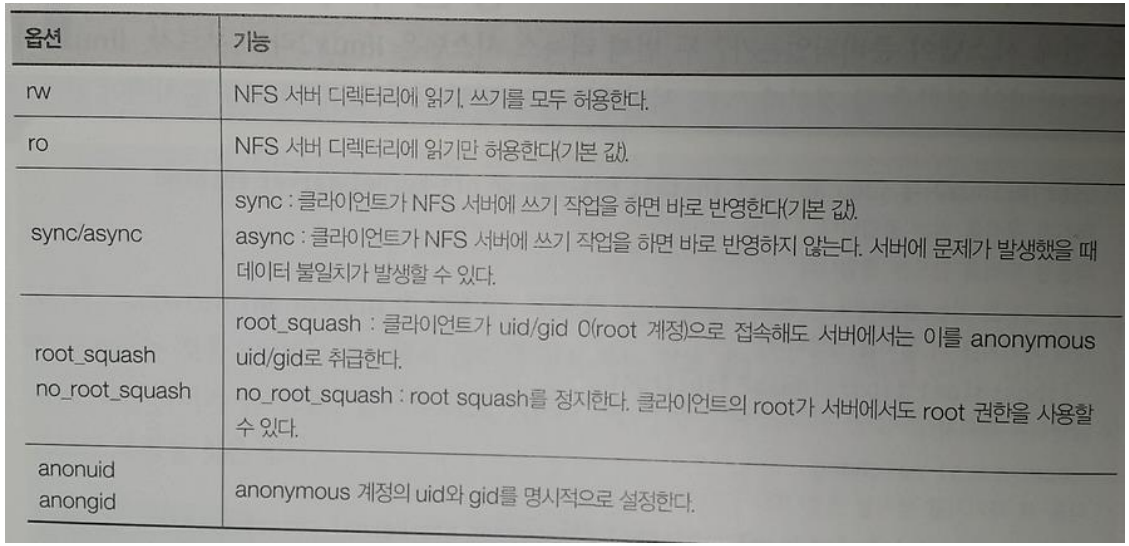


1 – NFS 설치와 운영

- NFS 서버 설치 및 구성하기
  - NFS 서버 설치
    - **CentOS**에 NFS 서버인 패키지를 설치한다
      - Yum에서 nfs를 찾는다
        yum search nfs
      - NFS를 설치한다
        yum install nfs-utils
    - **Ubuntu**에 NFS 서버 패키지를 설치한다
      - apt-cache에서 nfs를 찾는다
        apt-cache search nfs
      - NFS를 설치한다
        sudo apt-get install nfs-common nfs-kernel-server rpcbind

1 – NFS 설치와 운영

- NFS 서버 설치 및 구성하기
  - NFS 서버 구성-**CentOS, Ubuntu**
    - NFS Client가 사용할 수 있도록 디렉터리를 공유한다(exporting)
    - 설정 파일인 /etc/exports을 편집한 후 저장해야 한다
      - **mkdir –p /public/share**
        chmod 707 /public/share/
        ls –ld /public/share/
        touch /public/share/welcome.txt
      - **vi /etc/exports**
        /public/share 192.168.219.0/24(rw,sync,no_root_squash)



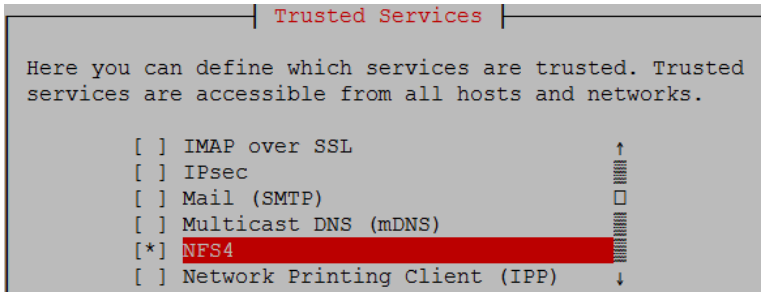
옵션	기능
rw	NFS 서버 디렉터리에 읽기, 쓰기를 모두 허용한다.
ro	NFS 서버 디렉터리에 읽기만 허용한다(기본 값).
sync/async	sync : 클라이언트가 NFS 서버에 쓰기 작업을 하면 바로 반영한다(기본 값). async : 클라이언트가 NFS 서버에 쓰기 작업을 하면 바로 반영하지 않는다. 서버에 문제가 발생했을 때 데이터 불일치가 발생할 수 있다.
root_squash no_root_squash	root_squash : 클라이언트가 uid/gid 0(root 계정)으로 접속해도 서버에서는 이를 anonymous uid/gid로 취급한다. no_root_squash : root squash를 정지한다. 클라이언트의 root가 서버에서도 root 권한을 사용할 수 있다.
anonuid anongid	anonymous 계정의 uid와 gid를 명시적으로 설정한다.

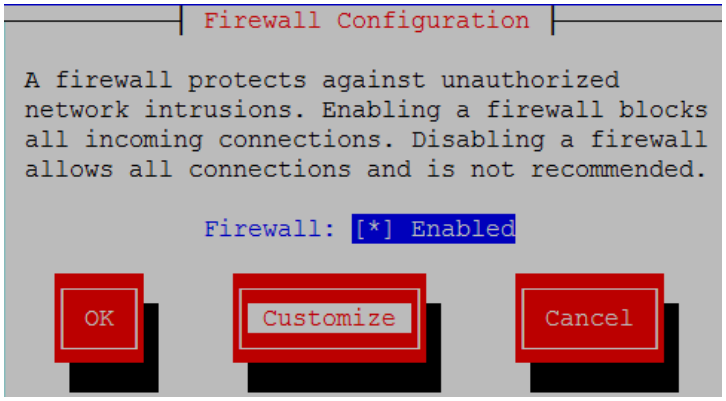
1 – NFS 설치와 운영

- NFS 서버 설치 및 구성하기
  - NFS 서버 구성
    - /etc/exports 파일에서 수정한 내용을 적용한다(exporting)
      - **exportfs -a**
    - NFS 서버가 공유한 내용을 확인한다
      - **exportfs**
      - **exportfs -v**
    - NFS 서버를 재시작한다
      - **service nfs restart** (##CentOS)
      - **sudo /etc/init.d/nfs-kernel-server** restart (##Ubuntu)
        sudo /etc/init.d/rpcbind restart

1 – NFS 설치와 운영

- NFS 서버 설치 및 구성하기
  - NFS 서버 구성-**CentOS only**
    - Firewall 설치 및 구성하여 반드시 NFS를 열어주어야 한다
      - **yum install system-config-firewall**
      - **system-config-firwall-tui**





  - 부팅할 때 자동으로 nfs, rpcbind 서비스 실행하기
    - **chkconfig nfs on**
      chkconfig rpcbind on
  - 현재 nfs와 rpcbind가 실행중인지 확인한다
    - **service nfs status**
      service rpcbind status

1 – NFS 설치와 운영

- NFS 서버 설치 및 구성하기
  - NFS Client 구성-**CentOS**
    - Nfs-utils를 설치한다
      - **yum install nfs-utils -y**
    - NFS Server에 어떤 디렉터리가 공유되어 있는지 확인하는 패키지를 설치
      - **yum install util-linux-ng -y**
    - Mount하기 전에 NFS Server에 공유된 디렉터리 확인하기
      - **showmount -e** nfsserverIPaddress
      - (## 안보이면 NFS 서버의 firewall에서 tcp,udp 포트 2049, 111를 열어줘야 한다)
        (## 임시방편으로 NFS Server에서 Firewall을 종료한다)
        service iptables save
        service iptables stop
        chkconfig iptables off
    - NFS Server에 접속하기 위한 디렉터리를 생성한다
      - **mkdir /mnt/nfs**
    - NFS 서버에 mount하기
      - **mount -t nfs 192.168.219.200:/public/share /mnt/nfs**

1 – NFS 설치와 운영

- NFS 서버 설치 및 구성하기
  - NFS Client 구성-**CentOS**
    - 제대로 연결되었는지 확인하기
      - **mount**
    - NFS Share에 연결된 것을 포함하여 모든 연결된 드라이브 확인하기
      - **df -h**
    - 연결된 폴더의 내용 확인 및 파일 생성하기
      - **cd /mnt/nfs**
        ls –l
      - **touch success.txt**
    - NFS Share에 연결된 모드 드라이브 끊기
      - **cd**
      - **umount -a**

1 – NFS 설치와 운영

- NFS 서버 설치 및 구성하기
  - NFS Client 구성-**CentOS**
    - NFS Client가 부팅할 때 자동으로 NFS Server에 연결하기
      - **vi /etc/fstab**
        192.168.219.200:/public/share /mnt/nfs nfs defaults 0 0
    - NFS Client가 재시작하여 자동으로 NFS Server에 연결되는지 확인
      - **shutdown –r now**
      - **ls /mnt/nfs**

1 – NFS 설치와 운영

- NFS 서버 설치 및 구성하기
  - NFS Client 구성-**Ubuntu**
    - **nfs-common**만을 설치하면 된다
      - **sudo apt-get install nfs-common**
    - NFS Server에 접속하기 위한 디렉터리를 생성한다
      - **mkdir /mnt/nfs**
    - NFS Server가 공유하고 있는 내용 확인하기
      - **showmount –e 192.168.219.200**
    - NFS 서버에 mount하기
      - **mount –t nfs 192.168.219.200:/public/share /mnt/nfs**
        (## root 계정으로 연결)
    - 제대로 연결되었는지 확인하기
      - **mount**
    - NFS Share에 연결된 것을 포함하여 모든 연결된 드라이브 확인하기
      - **df -h**

1 – NFS 설치와 운영

- NFS 서버 설치 및 구성하기
  - NFS Client 구성-**Ubuntu**
    - 연결된 폴더의 내용 확인 및 파일 생성하기
      - **cd /mnt/nfs**
        ls –l
      - **touch GoForIt.txt**
    - NFS Share에 연결된 모드 드라이브 끊기
      - **cd**
      - **umount -a**
    - NFS Client가 부팅할 때 자동으로 NFS Server에 연결하기
      - **vi /etc/fstab**
        192.168.219.200:/public/share /mnt/nfs nfs defaults 0 0
    - NFS Client가 재시작하여 자동으로 NFS Server에 연결되는지 확인
      - **shutdown –r now**
      - **ls /mnt/nfs**

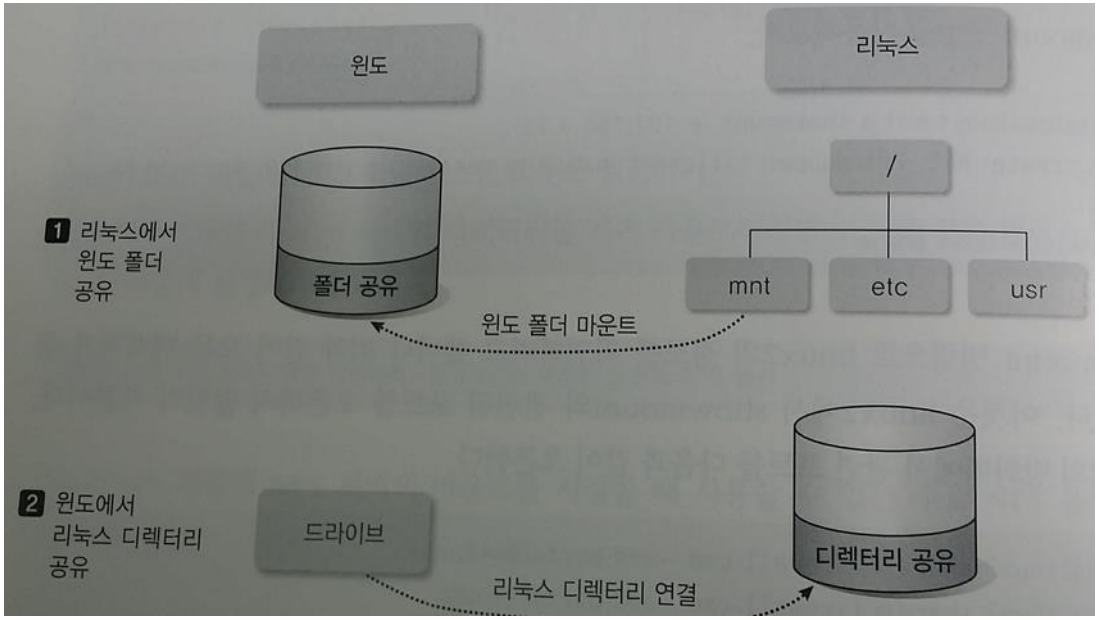
2 – Samba 설치와 운영

Windows가 Linux 서버의 공유 폴더 이용하기

Linux가 Windows File Server의 공유폴더 이용하기

2 – Samba 설치와 운영

- Samba 개요
  - 사내에서 Windows 컴퓨터가 Linux 서버에 저장된 파일을 이용하거나 거꾸로 Windows File Server에 있는 파일을 Linux가 이용하고자 한다.
  - 이렇게 사내 네트워크에서 이기종간의 파일 공유를 할 때 사용하는 기술이 Samba 서비스이다



2 – Samba 설치와 운영

- Windows가 Linux 서버의 공유 폴더 이용하기
  - CentOS에 Samba 서버 설치하기
    - Samba 검색하기
      yum search samba
    - Samba 설치하기
      yum install samba –y

리눅스	윈도
Samba 서버(samba) 설치 Samba 서버 설정 방화벽 오픈 공유할 디렉터리 생성	리눅스 디렉터리 공유

  - Samba 서버 구성하기: **/etc/samba/smb.conf**
    - Workgroup: **WORKGROUP**
    - Hosts allow: **192.168.219.**
    - Security: **user**

항목	내용	설정 값
workgroup	• 리눅스와 윈도의 작업 그룹 이름으로 윈도에 설정된 작업 그룹 이름 (컴퓨터→속성)을 설정한다.	WORKGROUP
hosts allow	• 리눅스에 접근을 허용할 호스트를 지정한다. • 특정 IP나 호스트 이름, 네트워크 주소를 지정한다.	192.168.0.
security	클라이언트가 Samba에 접속할 때 확인하는 인증 레벨 • user : smbpasswd –a로 생성한 사용자만 허용한다. • share : 인증 절차 없이 사용한다.	user

  - 서비스를 시작한다
    - **service smb start**
    - **service nmb start**
      (nmbd: WINS and Network Browsing Service)

2 – Samba 설치와 운영

- Windows가 Linux 서버의 공유 폴더 이용하기
  - Firewall에서 Samba 관련 포트를 연다
    - tcp 및 udp 포트 137, 138, 139, 445번
    - **system-config-firewall**을 시작하여 **Firewall을 Enable**하고 **Customize**로 선택한 후 **Samba**를 선택한다
  - Selinux를 Permissive 모드로 설정한다
    - SELinux is running and logging but not controlling permissions
    - **setenforce 0**
    - 제대로 설정되었는지 확인하기
      sestatus | grep -i mode
  - Samba로 접속하는 사용자를 생성한다: **smbpasswd**
    - adminuser의 홈 디렉터리에 접속하는 것이다. 다른 사용자는 접속하지 못한다
    - **smbpasswd –a adminuser**

2 – Samba 설치와 운영

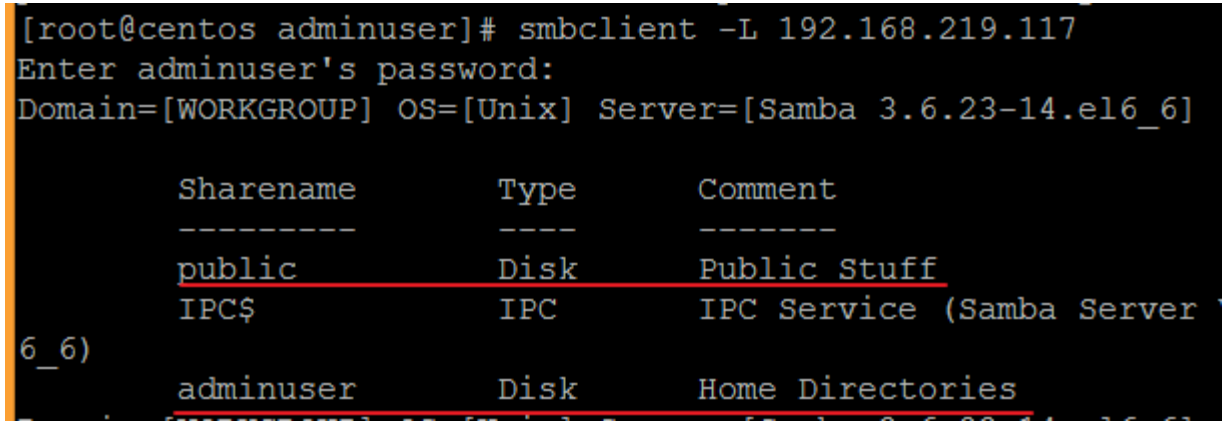
- Windows가 Linux 서버의 공유 폴더 이용하기
  - Samba 서버 구성하기-2: **/etc/samba/smb.conf**
    - 모든 사람이 접속하도록 설정한다(사용자 계정을 입력하지 않는다)
    - Sales 그룹만 write 할 수 있지만 그 외 모든 사람은 읽기만 할 수 있도록 설정한다
    - 디렉터리를 생성하여 적절하게 권한을 변경한다
      mkdir /home/samba
      chmod 707 /home/samba
    - /etc/samba/smb.conf 파일을 아래와 같이 수정한다

```
# A publicly accessible directory, but read only, except for people in
# the "sales" group
        [public]
        comment = Public Stuff
        path = /home/samba
        public = yes
        writable = yes
        printable = no
        write list = +sales
```

    - Samba 서비스를 재시작한다
      - **service smb restart**
        service nmb restart

2 – Samba 설치와 운영

- Windows가 Linux 서버의 공유 폴더 이용하기
  - Samba Server에서 어떤 것이 공유되었는지 확인하기
    - **smbclient –L 192.168.219.117**
      (## -L은 list)

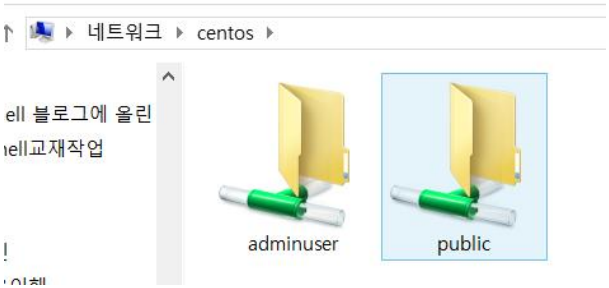


2 – Samba 설치와 운영

- Windows가 Linux 서버의 공유 폴더 이용하기
  - Windows에서 adminuser 계정으로 접속한다
    - **net use x: \\192.168.219.117\adminuser /user:adminuser**

```
PS C:₩Users₩용식> x:
PS X:₩> ls
```

  - Windows에서 익명으로 접속한다
    - **net use y: \\192.168.219.117\public**



  - Ubuntu에서 접속한다
    - Samba-client를 설치한다
      sudo apt-get install samba-client
    - Samba Server에 접속한다
      smbclient //192.168.219.117/adminuser –U adminuser

```
smb: \>
```

2 – Samba 설치와 운영

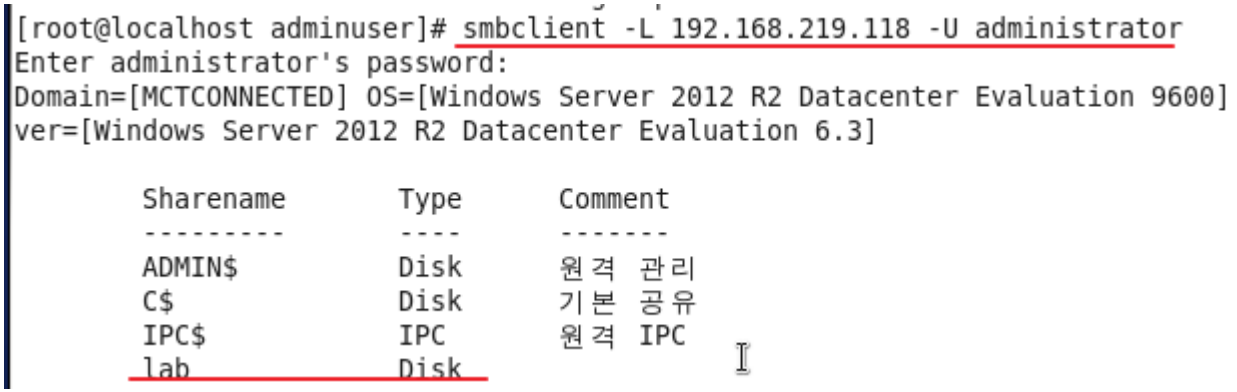
- Linux가 Windows File Server의 공유폴더 이용하기

리눅스	윈도
Samba 클라이언트(samba-client) 설치	리눅스 사용자 추가
Samba 마운트(smbmount)	폴더 공유

  - Windows Server에 폴더를 공유하고 사용자를 추가한다
    - 폴더 공유하기
      mkdir c:\lab
      jesuswithme.txt 파일 생성
      net share lab=c:\lab /grant:everyone,full
    - 공유가 제대로 되었는지 확인하기
      net share
    - Linux에서 접속하는 사용자 계정을 Windows에서 생성하기
      net users root * /add
      (##암호는 Pa$$w0rd)
    - 사용자 계정이 제대로 생성되었는지 확인하기
      net users

2 – Samba 설치와 운영

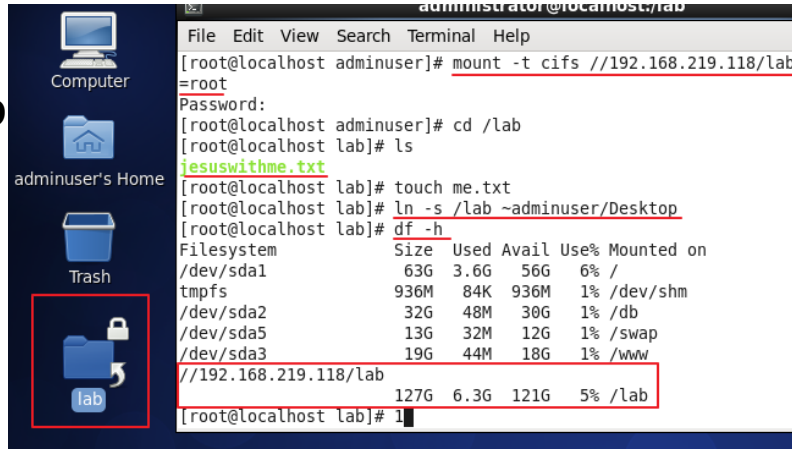
- Linux가 Windows File Server의 공유폴더 이용하기
  - CentOS에서 Samba-Client를 설치하기
    - 현재 samba clien가 설치되어 있는지 확인(samba-client, samba-common)
      rpm –qa | grep samba
    - 만약 설치되어 있지 않으면 다음과 같이 설치하기
      yum install samba-client samba-common
    - Windows File Server에 어떤 폴더가 공유되어 있는지 확인하기
      smbclient –L 192.168.219.118 –U administrator



2 – Samba 설치와 운영

- Linux가 Windows File Server의 공유폴더 이용하기
  - CentOS Linux에서 Windows File Server의 공유 폴더에 접속하기
    - Mount 할 폴더 생성하기
      su root
      mkdir /mnt/lab
    - Linux에서 Windows에 접속할 때 mount로 하자 (##root 계정)
      mount –t cifs //192.168.219.118/lab /mnt/lab –o username=root

    (## -o username=root에서 –o는 option이다)
    - 여기에 접속을 하여 **touch me.txt**를 생성해 본다
    - **df -h**
    - Symbolic link을 바탕화면에 생성한다
      ln –s /mnt/lab ~adminuser/Desktop



2 – Samba 설치와 운영

- Linux가 Windows File Server의 공유폴더 이용하기
  - CentOS Linux에서 Windows File Server의 공유 폴더에 접속하기
    - Smb client로서 Windows에 접속하기
      smbclient //192.168.219.118/lab –U administrator
    - (## mount에 비하여 smbclient로 연결할 때는 symbolic link를 연결할 수 없다)

3 – FTP Server 설치와 운영

- vsFTPD 서버 설치하기
- FTP Server 구성하기
- FTP client를 사용하여 접속하기

3 – FTP Server 설치와 운영

- FTP 서버 구성하기
  - 20,21번 포트를 사용하는 인터넷상에서 파일을 다운로드 및 업로드 하는 서비스이다
    - 파일 서버 역할의 사내용은 Samba, NFS이고, 인터넷 사용자를 위한 서비스 또는 사내 직원이 인터넷을 통하여 회사 파일을 이용하기 위해 사용한다

- vsFTPD 서버 설치하기
  - Linux에서 제공하는 FTP Server 설치
    - **yum search ftp**
    - **yum install vsftpd –y**
  - vsFTPD를 동작시키는 xinetd 설치
    - **yum –y install xinetd**

3 – FTP Server 설치와 운영

- vsFTPD 서버 설치하기
  - 구성 파일 복사하기
    - cd /etc/xinetd.d
      cp /usr/share/doc/vsftpd-2.2.2/vsftpd.xinetd **./vsftpd**
  - 복사한 구성파일 내용 보기
    - **nano /etc/vsftpd/vsftpd.conf**
  - Firewall에서 FTP 추가
    - **system-config-firewall**
  - vsFTPD 서비스 시작하기
    - **service vsftpd status**
    - **service vsftpd start**
  - 클라이언트에서 접속하기
    - **ftp 192.168.219.117**
      (사용자는 anonymous, 암호는 입력하지 않고 Enter)

3 – FTP Server 설치와 운영

- 일반 사용자로 vsFTPD에 접속하기
  - Vi /etc/vsftpd/vsftpd.cong 파일을 열어서 다음과 같이 구성
    - anonymous_enable=NO
    - local_enable=YES
    - write_enable=YES
    - local_umask=022
    - dirmessage_enable=YES
    - xferlog_enable=YES
    - connect_from_port_20=YES
    - xferlog_file=/var/log/xferlog
    - xferlog_std_format=YES
    - chroot_local_user=YES
    - listen=YES
    - pam_service_name=vsftpd
    - userlist_enable=YES
    - tcp_wrappers=YES

3 – FTP Server 설치와 운영

- 일반 사용자로 vsFTPD에 접속하기
  - Root 계정으로 접속 가능하게 하기
    - vi /etc/vsftpd/**user_list**
    - vi /etc/vsftpd/**ftpusers**
    - 이 파일에서 root 앞에 #을 붙여 준다
  - 로그인할 때 홈디렉터리에 접근하지 못하여 실패하는 경우를 해결하기 위해서 (##필수 설정)
    - **setenforce 0**
    - **getenforce**
  - 이제 클라이언트에서 FTP Server에 접속한다
    - **ftp** ipaddress

4 – SSH Server 설치와 운영

- SSH 기술 소개
- SSH Server 및 Client 설치 여부 확인
- 다양한 방법으로 SSH Server에 연결하기
- 인증서를 이용하여 SSH Server에 접속하기
- SSH 기술을 사용한 파일 복사하기: scp, sftp
- Parallel ssh 사용하기

4 – SSH Server 설치와 운영

- SSH 기술 소개
  - SSH
    - SSH(Secure Shell)는 네트워크 보안에 있어 대중적이고 강력한 접근 방식을 제공하기 위해 만들어진 프로토콜이다.
    - SSH에 기반한 제품은 서버와 클라이언트의 한 쌍으로 구성되어 있는데, 보통 사용자들은 SSH 클라이언트를 rsh (remote shell) 대용이나 telnet 대용으로 사용하고 있다.
    - 로컬 컴퓨터와 원격 컴퓨터간의 통신할 때 Secure Channel(Tunnel)을 만들어 그곳으로 패킷을 전달하므로 안전한 통신을 보장한다
  - SSH가 제공하는 4가지 기능
    - 인증(Authentication)
    - 암호화(Encryption)
    - 무결성(Integrity)
    - 압축(Compression)

4 – SSH Server 설치와 운영

- SSH 사용하는 곳
  - 원격 서버 관리
    - **ssh 192.168.1.100 –l root**
  - 원격 파일 복사
    - **scp ./image.jpg root@192.168.1.100:/var/tmp**
    - **sftp adminuser@192.168.1.100**
  - SSH Tunneling

- 원격 ssh server에 접속할 때 인증 방법
  - 사용자 계정과 암호
  - 인증서
    - 로그인 하는 사용자 계정은 로컬 컴퓨터와 원격 컴퓨터에 동일해야 하지만, 암호는 사용되지 않는다. 암호 대신 미리 원격으로 복사한 Public key와 자신이 가지고 있는 Private key가 일치하는 경우에 인증을 통과시킨다
    - **ssh client: private key, public key**
    - **ssh server: public key of the ssh client**

4 – SSH Server 설치와 운영

- SSH Server 및 Client 설치 여부 확인
  - SSH Server 및 Client 설치여부 확인
    - **rpm –qa | grep ssh**
  - SSH Server 서비스 제공 여부 확인
    - **service sshd status**

- Firewall에서 SSH Server 허용하기
  - **system-config-firewall**
  - 방화벽 끄기
    - **service iptables save**
    - **service iptables stop**
    - **chkconfig iptables off**

4 – SSH Server 설치와 운영

- 다양한 방법으로 SSH Server에 연결하기
  - 단순하게 연결하기
    - **ssh 192.168.219.117**
  - 사용자 계정을 입력하여 접속하기
    - **ssh 192.168.219.117 –l adminuser**
    - **ssh adminuser@192.168.219.117**
  - 접속한 후 특정한 작업(mkdir)하고 곧장 빠져나오기
    - **ssh root@192.168.219.117 'mkdir /lab'**
    - **ssh root@192.168.219.117 'touch ~adminuser/sample.txt'**
    - **ssh root@192.168.219.117 'du –sh /home'**
      ssh root@192.168.219.117 'du –sh /'
      ssh root@192.168.219.117 'du –sh ~adminuser'
      ssh root@192.168.219.117 'du /home --max-depth=1 | sort –n –r'
    - **ssh root@192.168.219.117 'fdisk –l | grep /dev'**

4 – SSH Server 설치와 운영

- 인증서를 이용하여 SSH Server에 접속하기
  - 인증서를 이용한 인증의 특징
    - 암호 방식보다 더 안전하다
    - Private key와 Public key 사용하여 인증 및 데이터 암호화 처리
    - SSH Client에서 Public key와 Private key를 생성하여 접속하는 모든 SSH Server들에게 동일한 Public Key를 복사해두어 편리하게 관리
    - Public Key는 ~/.ssh/authorized_keys안에 들어 있다
    - SSH Server에 복사한 Public Key에 대해서는 현재 로그인하여 작업중인 사용자인 adminuser만 액세스하는 권한만 부여한다. 왜냐하면 Public key를 복사할 때 adminuser의 Home Directory 밑에 위치한 ~/.ssh/authorized_keys가 위치가 정해져 있기 때문이다.
    - 인증서는 주로 관리자가 사용하는 일반 계정(adminuser)만 사용하는 경향이 있다. 일단 리눅스 서버에 접속할 때 쉽게 접속한 후 관리 작업할 때는 su root를 하여 root 계정에 대한 암호를 입력하는 것이 보안에 좋다

4 – SSH Server 설치와 운영

- Public key 파일을 생성하여 원격 컴퓨터에 복사하여 두면 ssh server에 접속할 때 private key와 public key의 matching을 통하여 인증 절차를 통과하여 접속하게 한다
  - 사전에 원격 컴퓨터에 로컬 사용자와 **동일한 사용자가 존재해야 한다**
  - 로컬 사용자와 원격 사용자의 암호가 **동일할 필요는 없다**
- 인증서를 이용하여 SSH Server에 접속하기-1
  - 로컬 컴퓨터(ssh client)에서 ssh-keygen 명령을 사용하여 public key와 Private key를 생성한다
    - **ssh-keygen**
  - ssh-copy-id 명령으로 public key를 원격 컴퓨터(ssh server)에 복사한다
    - **ssh-copy-id -i ~/.ssh/id_rsa.pub 192.168.219.250**
    - 이것은 원격 컴퓨터의 ~/.ssh/authorized_keys 파일에 public key 내용을 append하는 것이다
    - -i는 identity 파일을 입력하라는 뜻
  - 암호를 입력하지 않고 원격 컴퓨터에 로그인하기
    - **ssh 192.168.219.250**

4 – SSH Server 설치와 운영

- 인증서를 이용하여 SSH Server에 접속하기-2
  - /etc/hosts 파일을 수정한다
    - **192.168.10.51 centos**
  - SSH Client에서 Private key와 Public key pair 생성하기
    - Key Pair 생성하기
      ssh-keygen -t rsa
    - 생성된 Key Pair 확인하기
      ls -al ~/.ssh/
    - 생성된 파일의 Permission들 확인하기
    - Public key인 id_rsa.pub 파일을 원격에 있는 ssh server에 복사하기
      scp ~/.ssh/id_rsa.pub adminuser@centos:id_rsa.pub
    - 복사한 public key의 내용을 ~/.ssh/authorized_keys에 복사하여 붙여넣기
      ssh centos 'cat ~/id_rsa.pub >> ~/.ssh/authorized_keys'

  ** 여기서 >>을 한 이유는 여기에 접속하는 SSH Client가 여러 대인 경우, 각 SSH Client의 Private Key를 여기의 제일 아래 줄에 첨부해야 하기 때문이다

4 – SSH Server 설치와 운영

- 인증서를 이용하여 SSH Server에 접속하기
  - SSH Client에서 Private key와 Public key pair 생성하기
    - 접속을 한다. 암호를 묻지 않으면 정상적으로 key로 접속한 것이다
      ssh -i ~/.ssh/id_rsa adminuser@centos
      (## 여기서 –i는 사용할 Private key를 지정하는 것이고, 그 키는 ~/.ssh/id_rsa라는 것이다)
    - 현재 로그온 한 사용자가 adminuser라고 한다면 다음과 같이 접속해도 된다
      ssh centos
      ssh adminuser@centos
    - 만약 password를 물어 보면 –v 또는 –vv 또는 –vvv를 입력해본다
      ssh -i ~/.ssh/id_rsa adminuser@centos -v
    - 만약에 접속할 때마다 사용자 이름과 Private key를 입력하는 것이 귀찮으면 다음 파일을 수정하면 된다
      nano ~adminuser/.ssh/config
      여기서 원격 컴퓨터이름이 orion이다

4 – SSH Server 설치와 운영

- SSH 기술을 사용한 파일 복사하기
  - scp(secure copy)
    - 파일을 원격 컴퓨터의 홈 디렉터리에 복사하기
      scp gvcs.jpg root@192.168.219.222:
    - 파일을 원격 컴퓨터에 특정한 위치에 복사하기
      scp gvcs.jpg root@192.168.219.222:/var/tmp
    - Directory를 몽땅 복사하기: -r 옵션 사용
      mkdir -p ~adminuser/lab/sales
      fallocate -l 10m ~adminuser/lab/sales/10MB.img
      scp -r ~adminuser/lab root@192.168.219.117:/home/adminuser
    - 원격 컴퓨터에 있는 파일을 로컬 컴퓨터로 복사해 오기
      scp root@192.168.219.222:gvcs.jpg .
  - Winscp, FileZilla와 같은 Windows App을 사용하여 scp 기능을 사용할 수도 있다

4 – SSH Server 설치와 운영

- SSH 기술을 사용한 파일 복사하기
  - sftp (secure ftp)
    - Linux Client에서 Linux Server로 파일을 복사하기

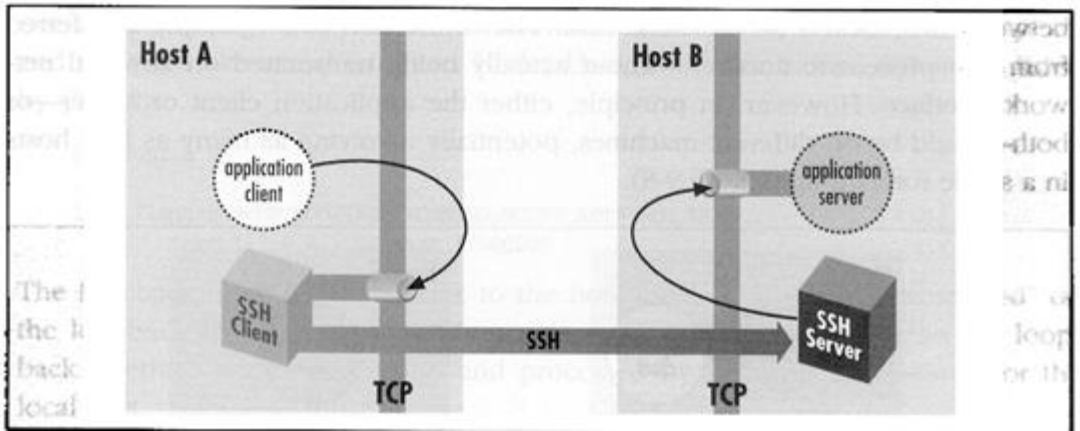
      sftp root@192.168.1.100
      pwd
      cd /yslee
      ls

    - Linux Server에 있는 파일을 Linux Client로 다운로드하기
      get GVCS2.JPG

    - Linux Client에 있는 파일을 Linux Server로 업로드하기 (파일 이름을 변경하여 업로드하기)
      put GVCS1.JPG gvcs11.jpg

4 – SSH Server 설치와 운영

- SSH tunneling
  - VPN 대용
  - 보안 통신을 지원하지 않는 Application에 보안 기능을 제공하는 것이 바로 ssh tunneling이다
    - SSH Client에서 먼저 다음과 같이 작업을 한다
      ssh –L 9000:localhost:1433 remoteserver_ip
    - SSH client에서 DB Client가 원격 포트를 9000번으로 지정한 후 실행한다
    - 그러면 로컬 SSH Client가 9000번 포트를 받아서 SSH Server로 보내는데, 이 패킷을 1433 포트로 보내라고 명령하는 것이다.
    - 그러면 SSH serve는 SSH Client와 연결된 터널로 들어 온 목적지의 포트가 1433을 받아서 SS server에서 실행중인 서비스(SQL server)로 Redirection한다



4 – SSH Server 설치와 운영

- Parallel-ssh 사용하기
  - 리눅스의 관리 작업은 일일이 ssh로 접속하여 진행하므로 10대 이상의 서버에 동일한 작업을 수행할 때는 불편하다
  - Parallel-ssh를 사용하여 이 문제를 해결할 수 있다
  - Parallel-ssh 설치하기
    - **apt-get install pssh**
  - 원격 컴퓨터에서 작업하기: uptime
    - **parallel-ssh –H 192.168.219.250 -l root –i uptime**
      parallel-ssh –H root@192.168.219.250 –i uptime
    - **parallel-ssh –H 192.168.219.250 –i "mkdir /test"**
      (** public key로 인증하는 경우)
    - **parallel-ssh –H "192.168.219.250 192.168.219.251" –i "mkdir /imsi"**
      (** 여러 대에 동시 작업하기)

4 – SSH Server 설치와 운영

- Parallel-ssh를 사용하기
  - 여러 대에 동시 작업하기
    - nodes라는 파일을 생성한 후 원격 컴퓨터 IP Address를 한 줄 한 줄 입력
    - **parallel-ssh –h nodes –i “touch /imsi/yslee.txt”**
    - **parallel-ssh –h nodes –i “shutdown –h now”** (## 강추)
  - 결과를 특정한 디렉터리 내의 파일로 저장하기
    - **mkdir result**
    - **parallel-ssh –h nodes –o result –i “touch /imsi/yslee.txt”**
    - **ls –l ./result/**
    - **cat ./result/192.168.219.250**
  - 여러 서버에 존재하는 동일한 사용자 계정의 암호를 동일하게 변경하기
    - **mkdir result**
    - **parallel-ssh –h nodes –i “echo -e '12345678\n12345678\n' | passwd jesuswithme”**
      (** 기존 암호를 새로운 12345678로 변경하는 것)