</>

# Born2beroot

sarchoi

# Defense

**Mandatory part**

- Explain about VM & OS
- Simple setup
- User
- Hostname & Partitions
- SUDO
- UFW
- SSH
- Script monitoring

**Bonus**

- Partitions
- Wordpress
- Freely choice service

# Introduction

- Remain polite, courteous, respectful and constructive throughout the evaluation process. The well-being of the community depends on it.
- Identify with the student or group whose work is evaluated the possible dysfunctions in their project. Take the time to discuss and debate the problems that may have been identified.
- You must consider that there might be some differences in how your peers might have understood the project's instructions and the scope of its functionalities. Always keep an open mind and grade them as honestly as possible. The pedagogy is useful only and only if the peer-evaluation is done seriously.

# Guidelines

- Only grade the work that was turned in the Git repository of the evaluated student or group.
- Double-check that the Git repository belongs to the student(s). Ensure that the project is the one expected. Also, check that "git clone" is used in an empty folder.
- Check carefully that no malicious aliases was used to fool you and make you evaluate something that is not the content of the official repository.
- To avoid any surprises and if applicable, review together any scripts used to facilitate the grading (scripts for testing or automation).
- If you have not completed the assignment you are going to evaluate, you have to read the entire subject prior to starting the evaluation process.
- Use the available flags to report an empty repository, a non-functioning program, a Norm error, cheating, and so forth. In these cases, the evaluation process ends and the final grade is 0, or -42 in case of cheating. However, except for cheating, student are strongly encouraged to review together the work that was turned in, in order to identify any mistakes that shouldn't be repeated in the future.

</ />

# SUBJECT PDF

https://cdn.intra.42.fr/pdf/pdf/24261/en.subject.pdf

# Preliminaries

- If cheating is suspected, the evaluation stops here. Use the "Cheat" flag to report it. Take this decision calmly, wisely, and please, use this button with caution.

**Preliminary tests**

- Defense can only happen if the student being evaluated or group is present. This way everybody learns by sharing knowledge with each other.
- If no work has been submitted (or wrong files, wrong directory, or wrong filenames), the grade is 0, and the evaluation process ends.
- For this project, you have to clone their Git repository on their station.

# General instructions

- 디펜스를 하는 동안 평가자가 포인트를 주기위해 피평가자는 당신을 도와줘야 합니다.
- clone한 저장소의 최상단에 "signature.txt" 파일이 있는지 확인하세요.
- "signature.txt" 의 서명이 가상 머신 ".vdi" 파일의 서명과 일치 한지 체크하세요. 필요한 경우 ".vdi" 파일의 위치를 확인하세요.
- 초기 가상 머신을 복제한다음 평가할 수 있습니다.
- 평가할 가상 머신을 시작합니다.
- 예상대로 작동하지 않는 것이 있거나 서명이 다르다면 평가는 여기서 멈춥니다.

```
$ shasum "sarchoi.vdi" > eval.txt
$ diff signature.txt eval.txt
```

</>

# Mandatory part

VM & OS

# Project overview

다음을 설명하세요

1. How a virtual machine works.
2. Their choice of operating system.
3. The basic differences between CentOS and Debian.
4. The purpose of virtual machines.
5. If the evaluated student chose CentOS: what SELinux and DNF are.
6. If the evaluated student chose Debian: the difference between aptitude and apt, and what APPArmor is.

평가를 하는 동안 매 10분마다 스크립트가 나타나는지 확인하세요. 이 스크립트는 이후에 평가됩니다.

1. How a virtual machine works.

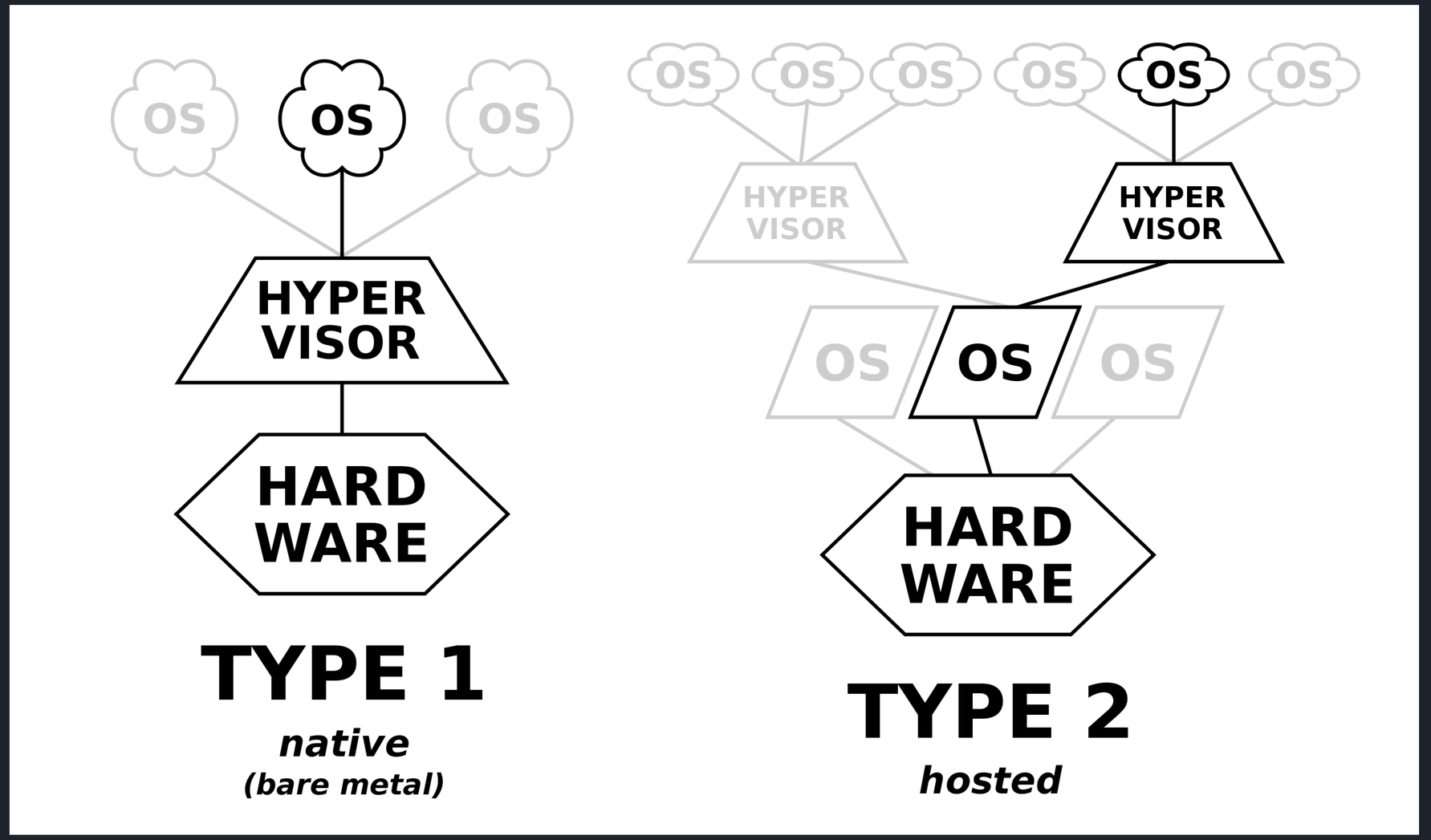
# VM의 작동 방식

- VM: 컴퓨팅 환경을 소프트웨어로 구현한 것. 가상화 기술로 작동.
- 가상화 기술: 리소스의 추상화(단일 물리 리소스를 만들어 냄)
- 호스트(물리적 시스템), 게스트(호스트에서 실행되는 VM)

### 하이퍼바이저

- VM을 생성, 실행, 관리하는 프로세스(소프트웨어)
- 메모리, 스토릿 등의 리소스 관리
- 종류: MS Hyper-V, VirtualBox, VMware, Parallels Desktop...

# 하이퍼파이저의 구조




- *Type1: Microsoft Hyper-V*
- *Type2: VirtualBox, VMware Workstation*

2. My choice of operating system.

# 선택한 OS

- *Debian*

```
$ head -n 2 /etc/os-release
```

3. The basic differences between `CentOS` and `Debian`.

# CentOS vs. Debian

## CentOS

- RHEL 소스 코드를 그대로 가져와서 상표 등을 제외한 다음 무료 배포.

  * Red Hat Enterprise Linux(RHEL): 구독식 판매. 기술 지원.
- 오픈소스 프로젝트 커뮤니티에 의해 관리.
- 주로 서버에 사용.
- 2021년 말에 지원 종료 (* Rocky Linux)

## Debian

- 데비안 프로젝트의 자유 운영체제
- `apt` 사용으로 패키지 설치 및 업그레이드가 단순
- 다른 리눅스 배포판의 기반(Ubuntu 등)

4. The purpose of virtual machines.

# VM의 사용 목적

- 하드웨어 활용률을 개선
- 물리적 리소스 추가 구매 비용 절약
- 전력, 공간, 냉각 비용 감소
- 분리된 환경으로 상호 방해 없음
- 테스트 환경, 프로덕션 환경 쉽게 추가 가능

5. If the evaluated student chose `CentOS`: what `SELinux` and `DNF` are.

# CentOS 선택한 경우: `SELinux`, `DNF`란?

## SELinux

- Security-Enhanced Linux
- 보안 아키텍처. 보안 강화 커널. 추가 보안 레이어를 제공.
- 시스템의 앱, 프로세스, 파일에 대한 액세스 제어 정의

## DNF

- Dandified Yum (멋부린 yum)
- CentOS 8 기본 패키지 관리 명령어(이전 `yum`)
- 성능 개선, 메모리 개선, 의존성 문제 처리

6. If the evaluated student chose `Debian`: the difference between `aptitude` and `apt`, and what `APPArmor` is.

# Debian 선택한 경우: `aptitude`와 `apt`의 차이점, `APPArmor`란?

## aptitude

- apt의 프론트엔드 프로그램
- 소프트웨어 패키지의 목록 보기, 설치, 삭제
- 향상된 검색 기능(검색 패턴 지원)
- 여러가지 자동화 지원

## apt

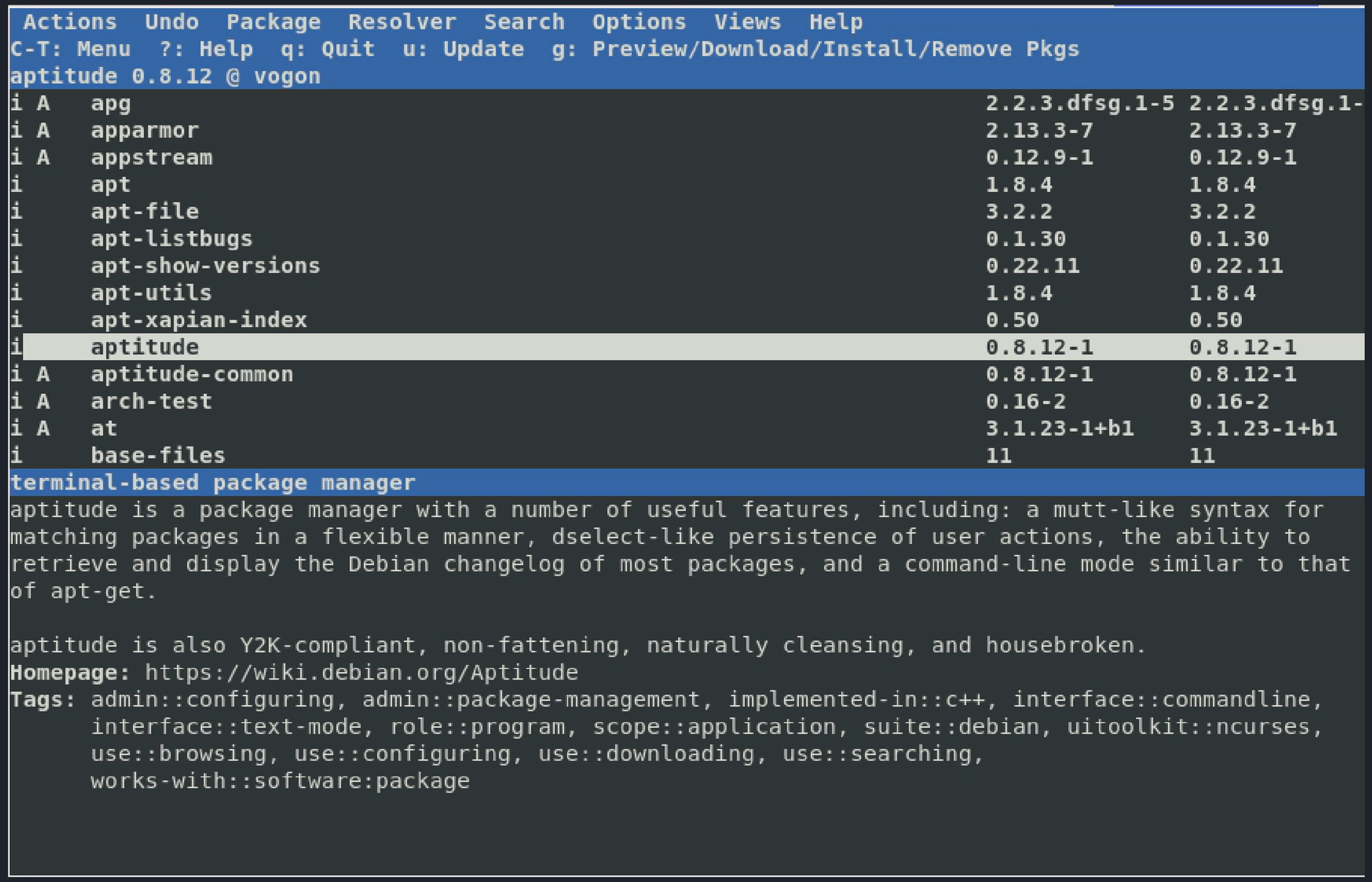
- Advanced Packaging Tool
- 소프트웨어 패키지 설치, 제거 등

## APPArmor

- Application Armor
- 리눅스 커널 보안 모듈
- 프로그램 프로필 별로 권한 제한
- 프로필: 네트워크 액세스, raw 소켓 액세스, 파일의 읽기/쓰기/실행

```
$ aa-enabled
```

# APTITUDE



# Simple setup

- GUI가 아닌 CUI 환경인가?
- 머신에 접속할 때 패스워드를 물어보는가?

**일반 유저로 접속 후 확인해보기**

- 패스워드가 규칙에 맞는가? - 길이 10글자 이상, 대문자 포함, 숫자 포함,  같은문자 최대 3글자,
- UFW 서비스가 실행되었는가?
- SSH 서비스가 실행되었는가?
- 선택한 OS로 설정되었는가?

```
$ sudo ufw status
$ systemctl status ssh
$ cat /etc/os-release
```

# User

- 일반 유저(sarchoi)가 'sudo', 'user42' 그룹에 속해있는가?

**다음 단계를 따라서 패스워드 폴리시 확인하기**

1. 유저 생성하기. 패스워드는 맘대로. 패스워드 설정 확인하기. (다음장)
2. 그룹 'evaluating'를 생성 후, 1에서 생성한 유저를 추가하고 확인하기
3. 패스워드 폴리시의 장점을 설명. 폴리시가 적용 됐을 때의 장단점 설명하기.
   - 장점: 보안 향상 / 단점: 지나치게 복잡할 경우 메모 위험, 일부 특수문자 키보드 호환 안 될 가능성

```
$ id sarchoi                              # 유저의 그룹 정보 확인
$ adduser <NEW_USER>                      # 유저 생성하기
$ groupadd evaluating                     # 그룹 생성하기
$ usermod -aG evaluating <NEW_USER>       # 유저를 그룹에 추가하기
```

/etc/login.defs

```
PASS_MAX_DAYS  30        # 패스워드 최대 사용 기간
PASS_MIN_DAYS  2         # 패스워드 최소 사용 기간
PASS_WARN_AGE  7         # 만료 알림 날짜
PASS_MIN_LEN  10         # 패스워드 최소 글자수
```

/etc/pam.d/common-password  libpam-cracklib

```
password  requisite  pam_cracklib.so \
    retry=3                          \  # 패스워드 최대 재시도
    minlen=10                        \  # 패스워드 최소 글자수
    maxrepeat=3                      \  # 반복 가능한 글자수
    ucredit=-1 lcredit=-1 dcredit=-1 \  # 최소 소문자, 대문자, 숫자 글자수
    difok=7                          \  # 기존 패스워드와 겹치지 말아야하는 글자수
    reject_username enforce_for_root    # username과 패스워드 일치할 수 없음, root에도 적
용
```

# Hostname and partitions

- hostname이 `login42` 형식인가?
- hostname 변경해보기
- 파티션 확인하기

```
# lsblk
NAME                  MAJ:MIN RM   SIZE RO TYPE  MOUNTPOINT
sda                     8:0    0  30.8G  0 disk
├─sda1                  8:1    0   500M  0 part  /boot
├─sda2                  8:2    0     1K  0 part
└─sda5                  8:5    0  30.3G  0 part
  └─sda5_crypt        254:0    0  30.3G  0 crypt
    ├─LVMGroup-root   254:1    0    10G  0 lvm   /
    ├─LVMGroup-swap   254:2    0   2.3G  0 lvm   [SWAP]
    ├─LVMGroup-home   254:3    0     5G  0 lvm   /home
    ├─LVMGroup-var    254:4    0     3G  0 lvm   /var
    ├─LVMGroup-srv    254:5    0     3G  0 lvm   /srv
    ├─LVMGroup-tmp    254:6    0     3G  0 lvm   /tmp
    └─LVMGroup-var--log 254:7  0     4G  0 lvm   /var/log
sr0                    11:0    1  1024M  0 rom
```

1. hostname을 `평가자login42`로 수정하고 머신을 restart하기
2. 원래의 hostname으로 변경하기

```
$ hostnamectl
$ sudo hostnamectl set-hostname <NEW_HOSTNAME>
$ lsblk
```

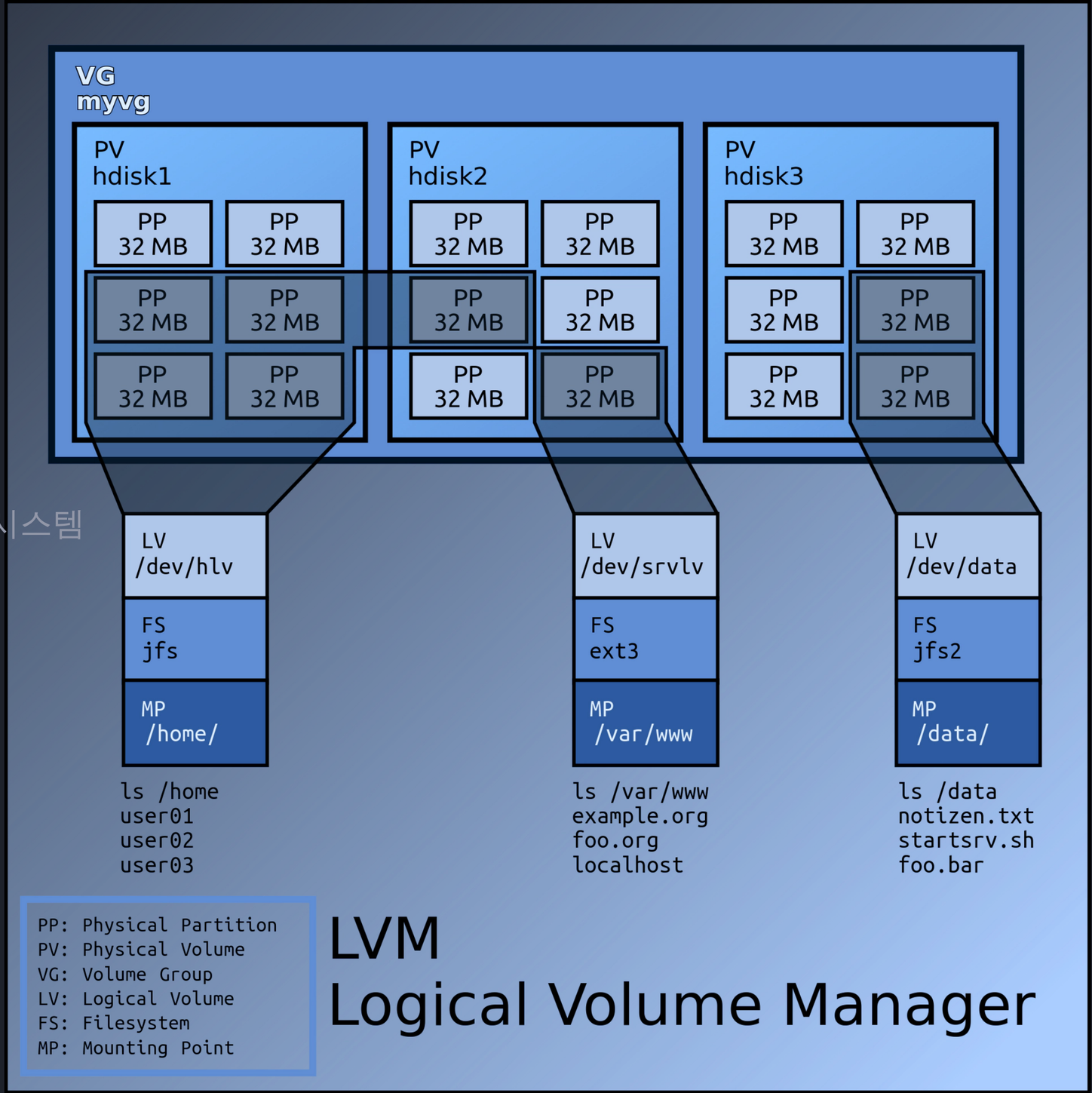
# Hostname and partitions

## LVM이란?

- Logical Volume Manager
- 파티션 대신 볼륨으로 저장 단위 지정

## LVM의 작동 방식

- 디스크,파티션 → 볼륨 그룹 → 논리 볼륨 → 파일시스템
- PE(Physical Extent, 물리적 크기) 4MB
- root, boot, SWAP, dump는 연속된 PE에 지정
  (단일 물리 볼륨)



# SUDO

- `sudo` 프로그램이 설치되어있는지
- 새 유저를 `sudo` 그룹에 할당하기
- 히스토리 확인: `/var/log/sudo/` 밑에 파일이 생성되어있는지
- `sudo` 커맨드 실행 후 히스토리 갱신 확인

**`sudo`의 규칙과 값, 방식**

- 다음장

```
$ dpkg -l sudo                          # sudo 설치 확인
$ usermod -aG sudo <NEW_USER>           # 유저를 그룹에 추가하기
$ visudo
```

visudo

```
Defaults    env_reset
Defaults    mail_badpass
Defaults    secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:
/bin:/snap/bin"                         # 사용할 수 있는 경로 제한
Defaults    passwd_tries=3              # 패스워드 3번 틀렸을 경우 제한
Defaults    badpass_message="Password is wrong."            # 잘못된 암호 커스텀 메세지
Defaults    authfail_message="Authentication failed."
Defaults    log_input                   # 입력 로깅
Defaults    log_output                  # 출력 로깅
Defaults    iolog_dir="/var/log/sudo/"  # 로그 디렉토리
Defaults    requiretty                  # 보안 문제 TTY 모드 활성화

root ALL=(ALL:ALL) ALL
<USERNAME> ALL=(ALL:ALL) ALL            # sudo 사용할 유저 추가
```

# UFW

- `UFW` 프로그램의 설치 여부 & 작동 확인
- 활성화되어있는 UFW의 규칙 리스트 보여주기. 4242 포트가 있어야 됨.
- 8080 포트 새로 추가하고 리스트 확인하기
- 새로 추가한 규칙 지우기

**UFW란? 사용 이유**

- Uncomplicated Firewall (Simple)

```
$ sudo ufw status
$ sudo ufw allow 8080
$ sudo ufw delete <NUMBER>
```

# SSH

- SSH 프로그램 설치 여부 & 작동 확인
- SSH가 4242 포트에서만 사용하는지 확인
- 새로 만든 사용자로 SSH 접속 시도해보기. 이 때 key 혹은 패스워드를 사용할 수 있다.
- root 유저로 SSH 접속이 되지 않는 것 확인하기

**SSH란? 사용 이유**

- Secure Shell

```
$ systemctl status ssh
$ ss -tnulp
```

```
mac$ ipconfig getifaddr en0     # 호스트 IP 체크
mac$ ssh USERNAME@<호스트IP> -p 4242
```

# Script monitoring

- code 설명하기

**변경하기**

1. 매 1분마다 실행되게 변경
2. 서버 시작 시 뜨지 않게 변경해보기
   - 스크립트 파일 내용 변경 금지, 파일 위치 이동 금지, 파일 권한 변경 금지

**Cron이란?**

- 시간 기반 잡 스케줄러

```
$ vi /monitoring.sh
$ sudo cronteb -e
```

</>

# Bonus part

WORDPRESS

# Wordpress

- lighttpd
- MariaDB
- PHP  http://<HOST_IP>:8080/phpinfo.php

**Wordpress**

- http://<HOST_IP>:8080/wordpress

**추가 선택 서비스 - phpMyAdmin**

- http://<HOST_IP>:8080/phpMyAdmin

```
# lsblk
NAME                    MAJ:MIN RM   SIZE RO TYPE  MOUNTPOINT
sda                       8:0    0  30.8G  0 disk
├─sda1                    8:1    0   500M  0 part  /boot
├─sda2                    8:2    0     1K  0 part
└─sda5                    8:5    0  30.3G  0 part
  └─sda5_crypt          254:0    0  30.3G  0 crypt
    ├─LVMGroup-root     254:1    0    10G  0 lvm   /
    ├─LVMGroup-swap     254:2    0   2.3G  0 lvm   [SWAP]
    ├─LVMGroup-home     254:3    0     5G  0 lvm   /home
    ├─LVMGroup-var      254:4    0     3G  0 lvm   /var
    ├─LVMGroup-srv      254:5    0     3G  0 lvm   /srv
    ├─LVMGroup-tmp      254:6    0     3G  0 lvm   /tmp
    └─LVMGroup-var--log 254:7    0     4G  0 lvm   /var/log
sr0                      11:0    1  1024M  0 rom
```

```
$ systemctl status lighttpd
$ mysql
```