목차

RedHat Enterprise Linux 6 기본 설치 및 설정 가이드

기본 Platform 지원 정보

- Version : RHEL6
- 아키텍처 : x86, AMD64, Intel64 # x86_64bit 주로 사용
- Kernel : RHEL 6(Linux 2.6.32이상),
- 최대메모리 : x86_64 기준 : 64TB
- 파일시스템제한
  1. 최대파일크기: ext4–16TB:
  2. 최대파일시스템크기: ext4–16TB
- 지원 언어 수 : 22개 언어
- 디스크공간 : 최소 1G / 5G 권장
- 상세정보URL : http://www.redhat.com/products/enterprise-linux/server/compare.html

Partition 설정

OS영역 (300G 기준)

```
파티션구분  영역  사이즈(GB)    비고  설정 기준
Primary(sda1)  /boot   2G    kernel 저장소    platform 운용표준(v2.0)
Primary(sda3)  Swap    메모리 * 1.5    8G 이상시 8G로 세팅 8G 미만시 1.5배
platform 운용표준(v2.0)
Primary(sda2)  /    60G    60G할당 그외 여분 디스크 남겨둠   나머지용량 여분
```

DATA영역

- DATA 영역은 LVM으로 구성 권장. OS영역만 설치 후 LVM 구성
- 파일시스템 생성 시 Default Inode 값을 2배이상으로 설정.
- DATA영역에 관련하여 시스템 부팅 시 파일시스템 체크를 안하도록 fstab에 등록
- Internal Disk 영역은 위의 OS영역에 따르며, LVM 구성시 /boot를 제외한 나머지는 위의 용량대로 설정.
- DATA 영역은 서비스 용도에 따라, 디스크 용량에 따라 수정되어야 함
- SAN Disk 영역은 VGName vgwork11~ vgwork12, vgwork21~ vgwork22 (LVM구성시 Stripe으로 구성)
- 스토리지 구조상 LVM을 Stripe로 구성하는것은 성능향상에 거의 영향이 없는관계로 일반적인 LVM으로 구성하는것을 권장함

Application

```
파티션구분  영역  사이즈(GB)    비고
```

```
/dev/vgwork11/netbackup /netbackup    5G    Apache, tomcat 관련 디렉토리 구성은 서비스 용도에 따라 권장하는 방법으로 구성되고 수정되어야 함
/dev/vgwork11/was_mms   /was_mms     10G
/dev/vgwork11/was_sms   /was_sms     10G
```

Oracle Services

```
파티션구분  영역   사이즈(GB)     비고
/dev/vgwork11/oracle    /oracle    30G    Oracle 관련 디렉토리 구성은 서비스 용도에 따라 권장하는 방법으로 구성되고 수정되어야 함
/dev/vgwork11/oradata   /oradata    400G
/dev/vgwork11/archive   /archive    100G
/dev/vgwork11/oratrace  /oratrace    50G
/dev/vgwork11/dbawork   /dbawork    100G
```

OS설치과정

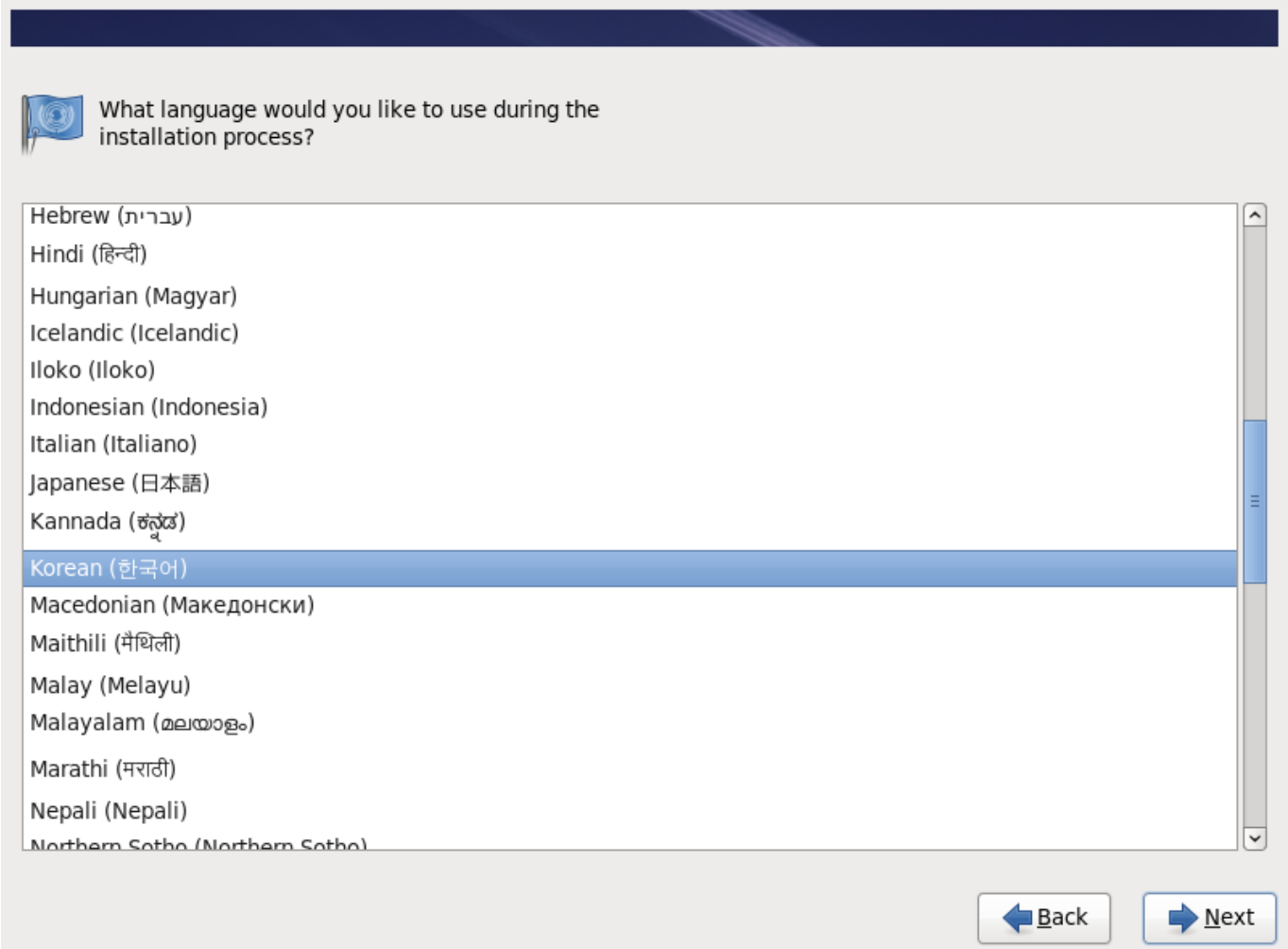
초기화면

- Install or upgrade an existing system 선택

설치이미지 파일 검사 단계

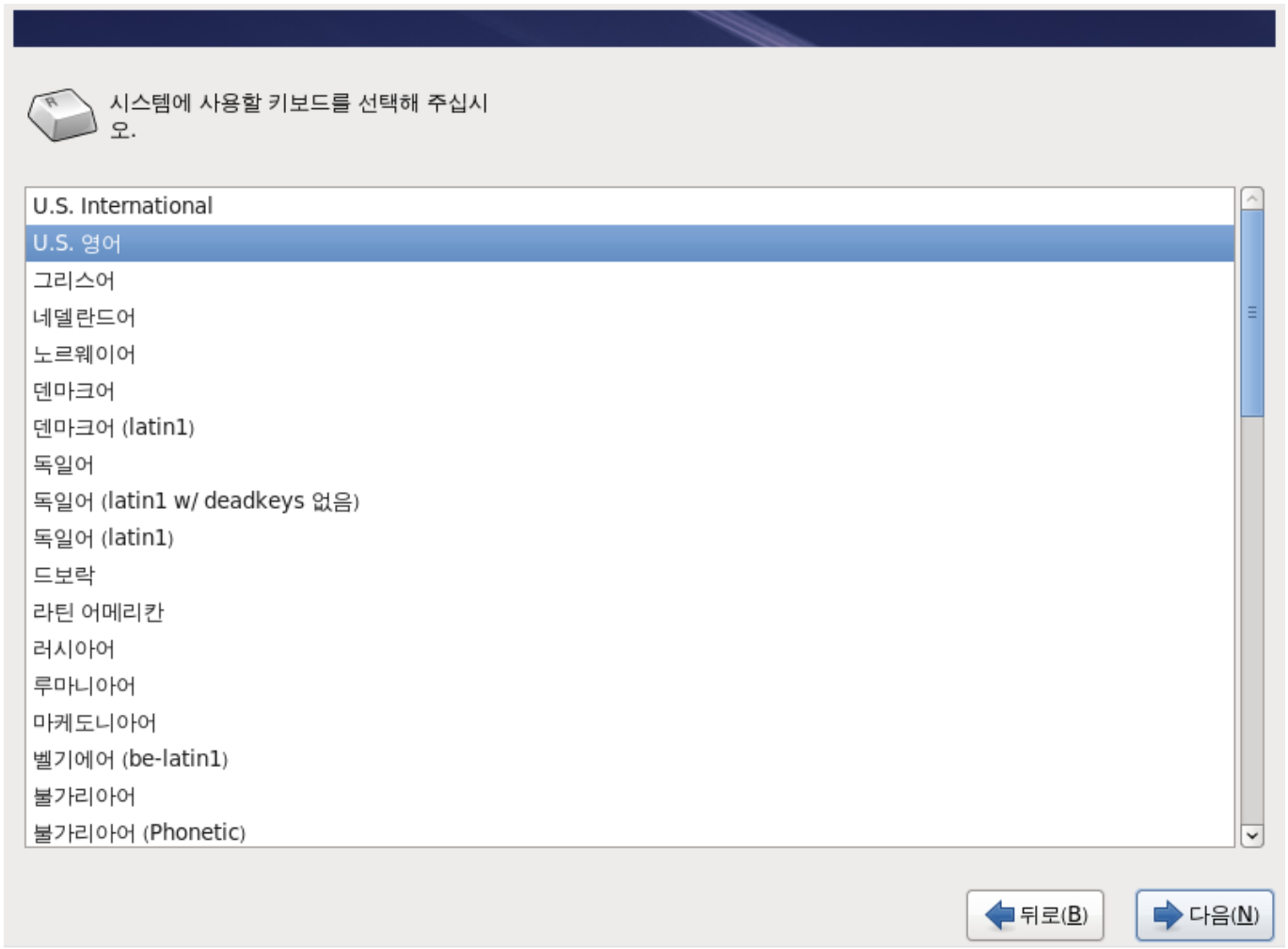
- skip선택

언어 선택



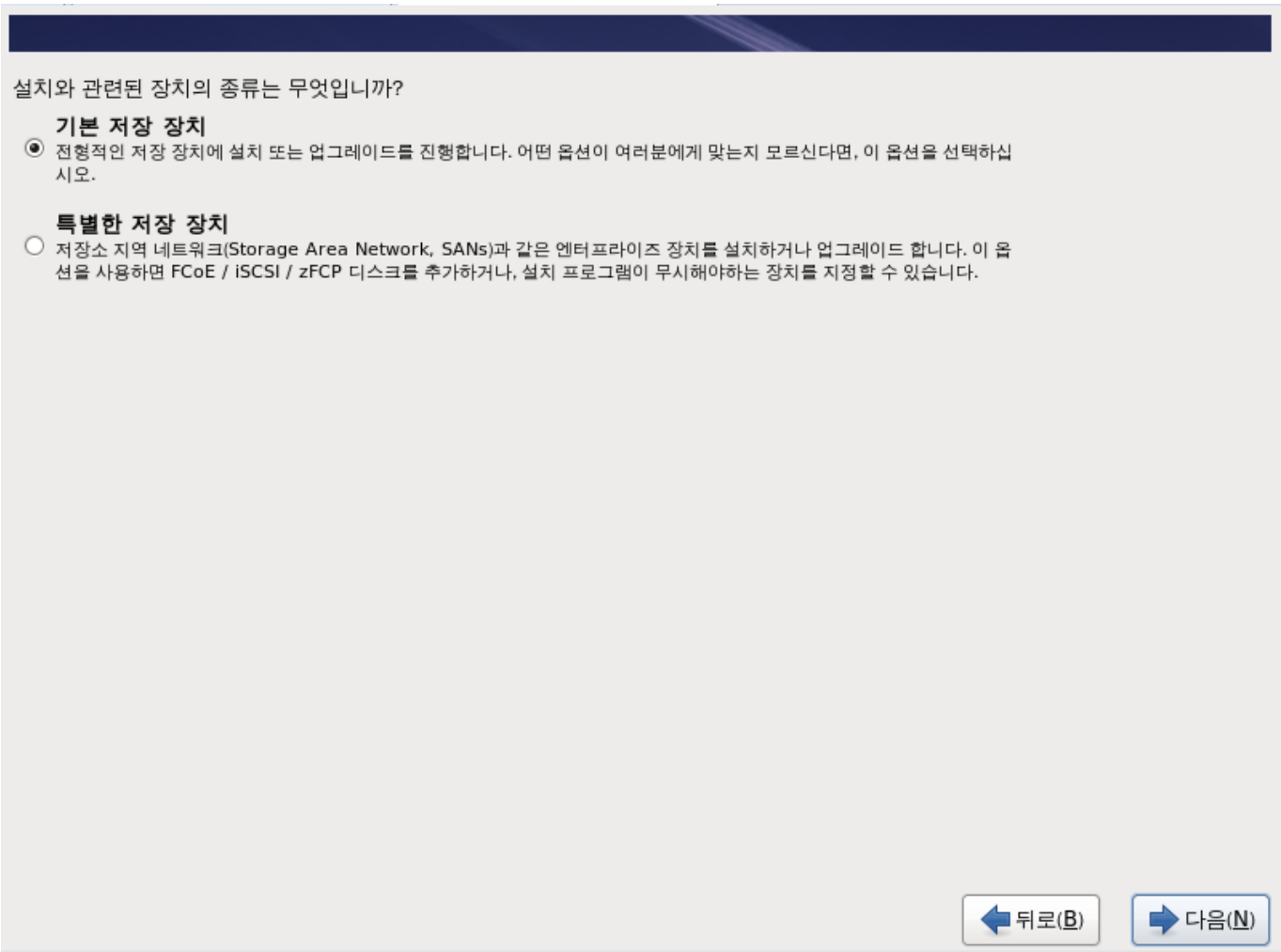
- 언어선택 Korean(한국어)선택 (영문권장)

키보드 언어 선택



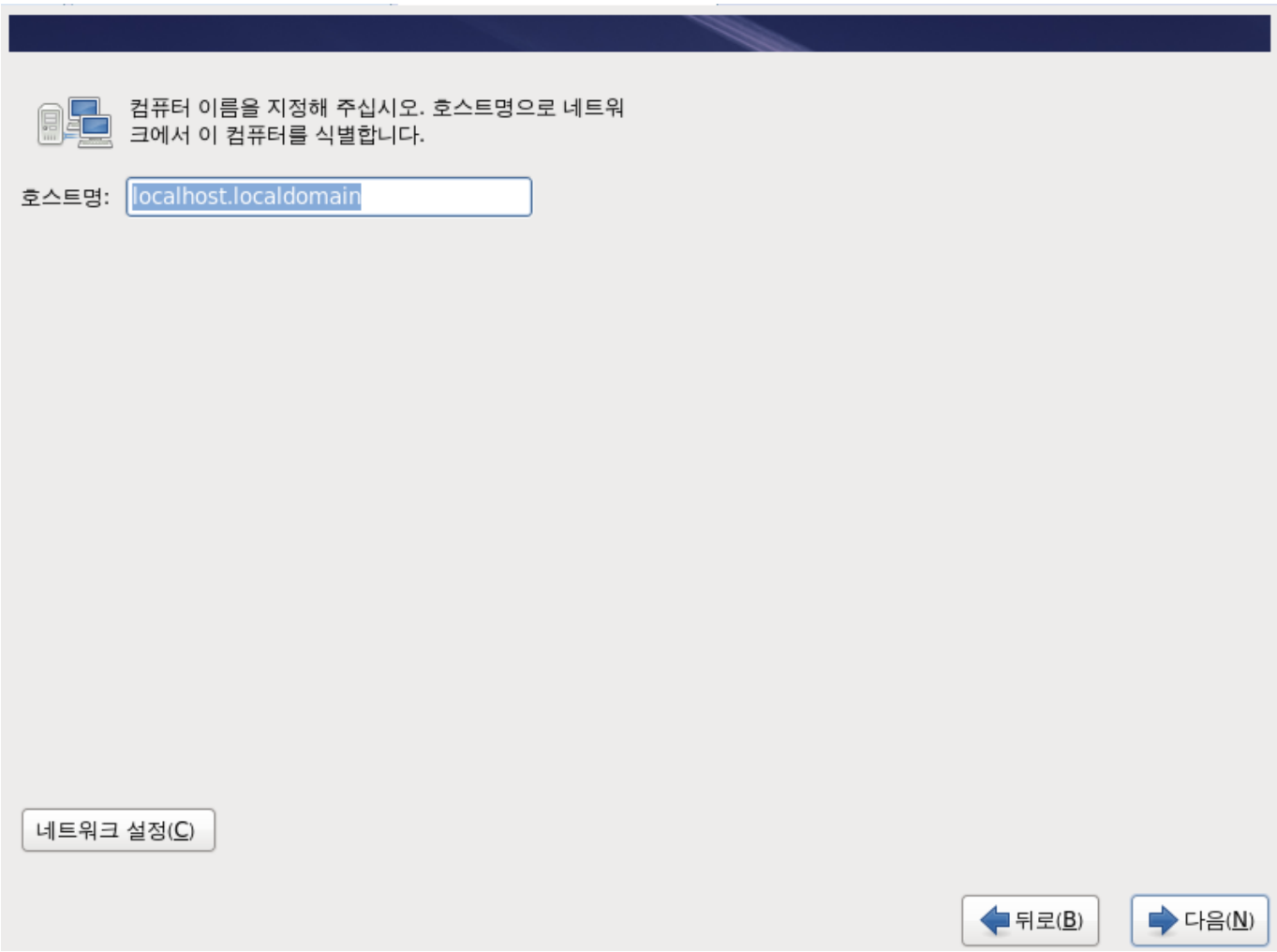
- 키보드언어 선택 : U.S. 영어 선택

저장 장치 종류 선택



- 기본 저장 장치 ’ 선택

호스트명 설정

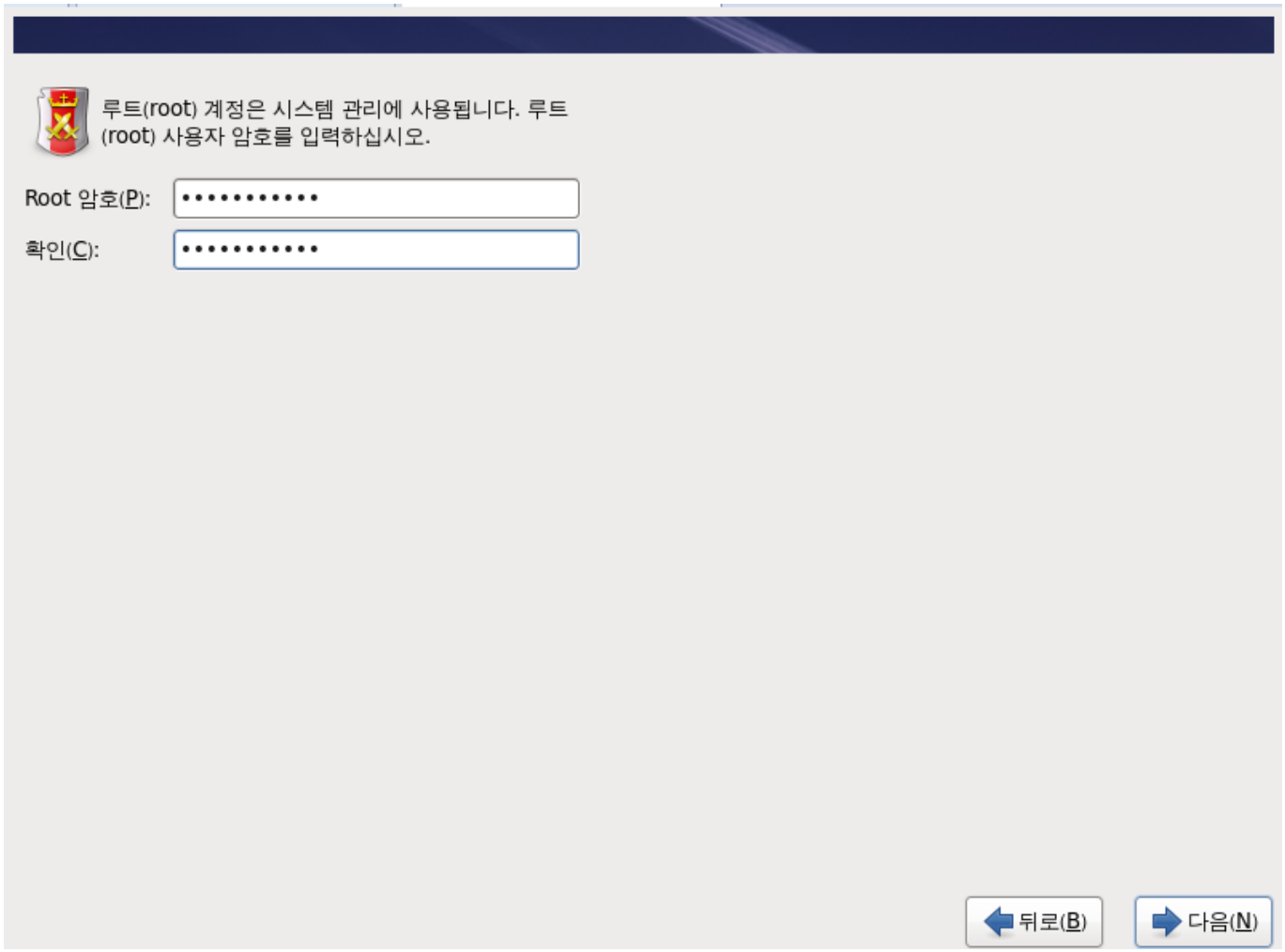


- 호스트명은 도메인을 포함하여 Full Name을 입력하여 준다.
- 할당된 도메인이 없을시에는 호스트명만 입력한다.

Timezone 설정

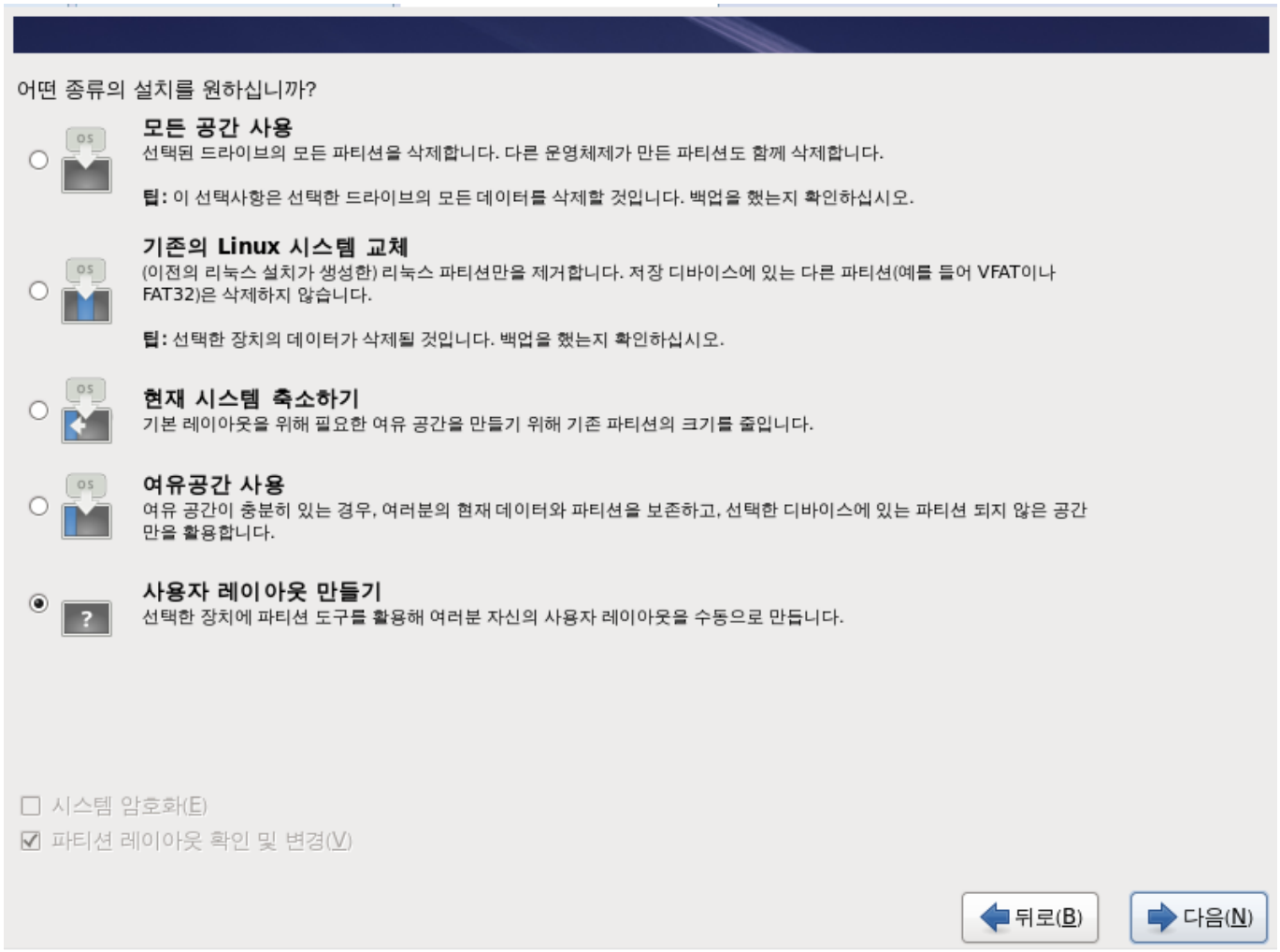
- Asia/Seoul 선택
- 시스템의 시간을 UTC에 맞춤 ' 선택 해제(TSC와 동기화로 인한 시간 오차 발생 방지; VM인경우 반드시!! 해제할것)

비밀번호 설정



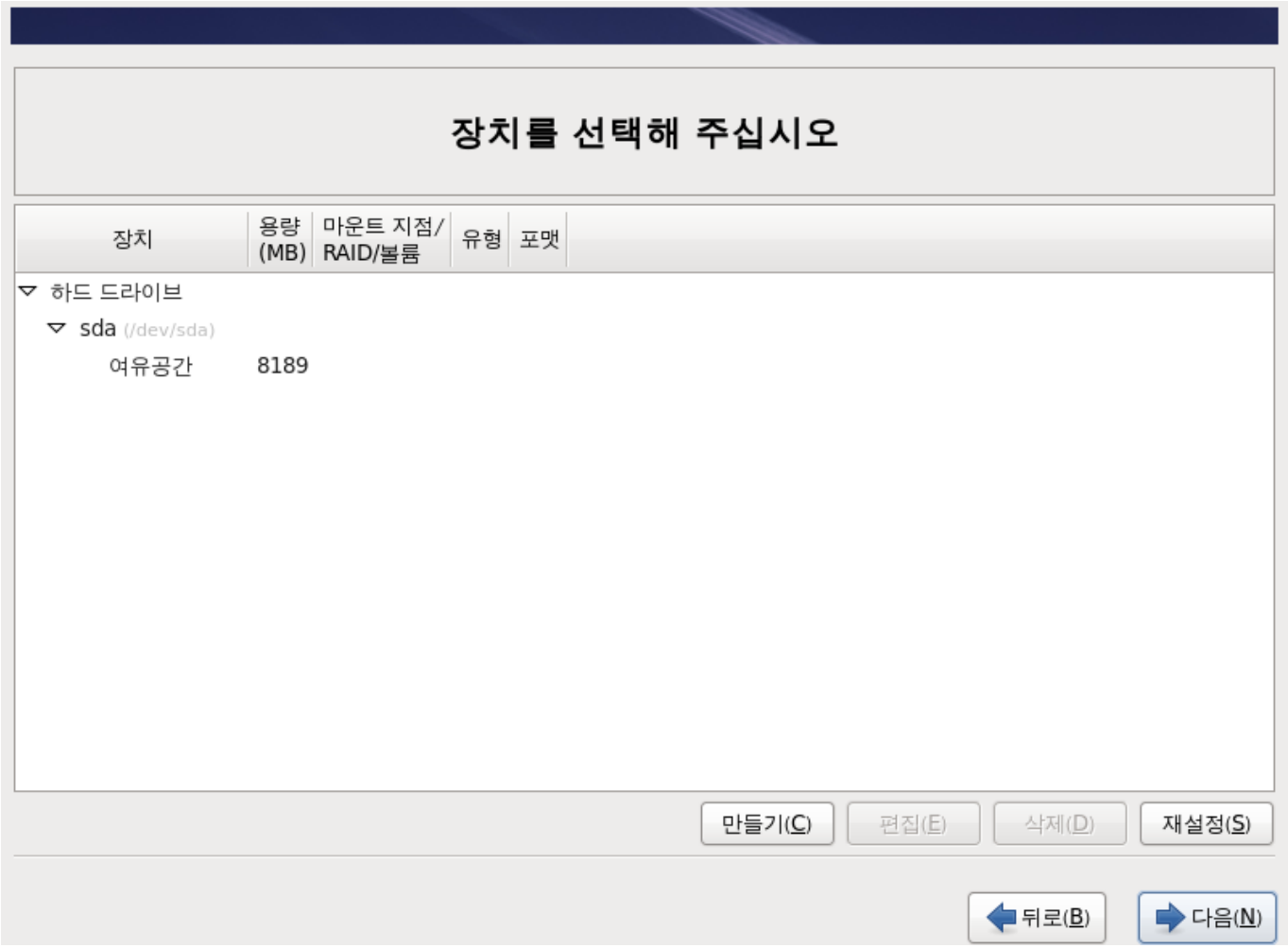
- 비밀번호를 입력한다. 가급적 복잡한 비밀번호 사용을 권장함.

파티셔닝 방법 선택



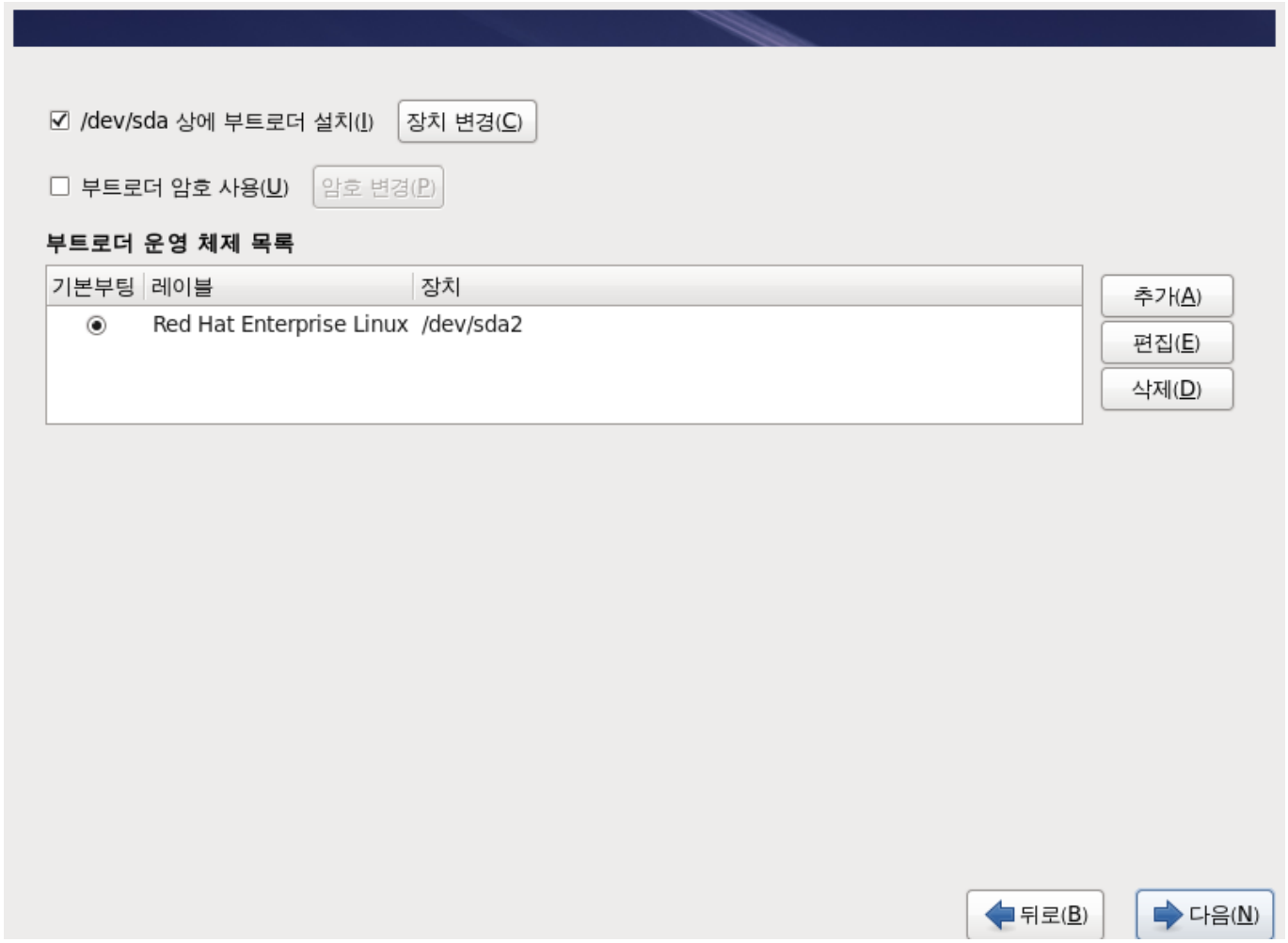
- 일반적으로 전체 사용 으로 설치해도 무방함
- 임의의 파티션 구조를 생성하고 싶은경우 “ 사용자 레이아웃 만들기 ” 선택

파티셔닝



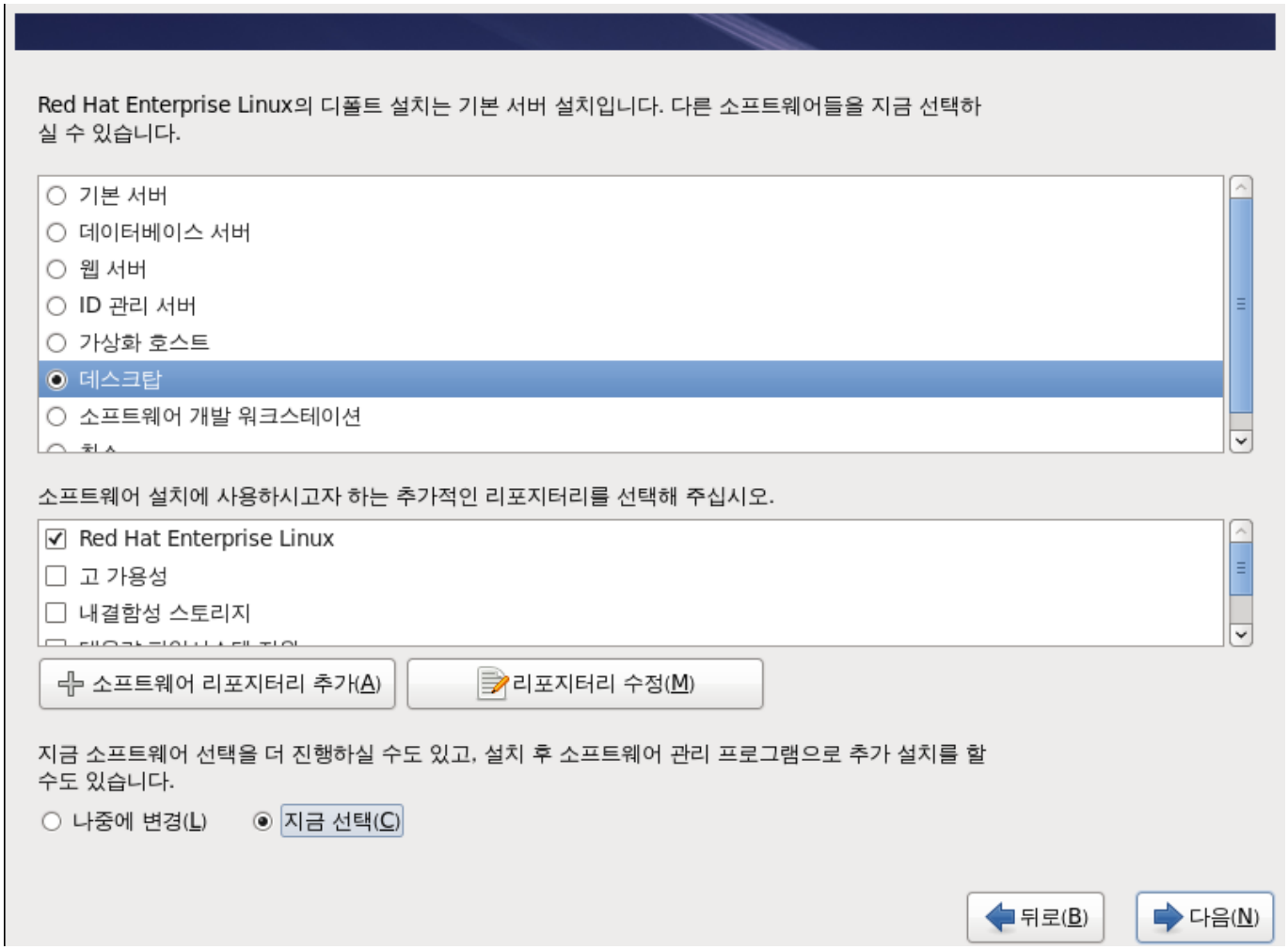
- 파티션 설정 참조

부트로더



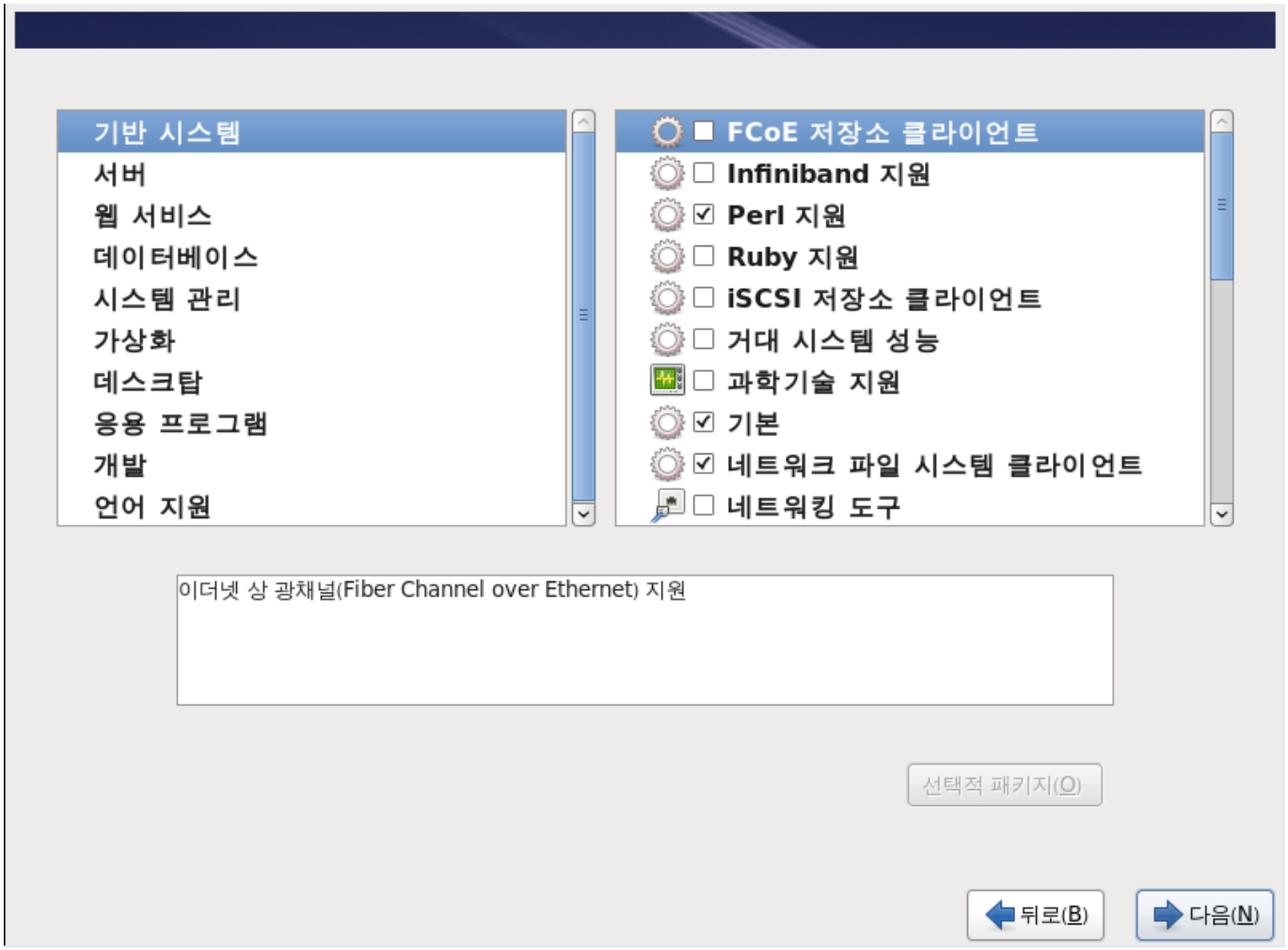
- 부트로더를 설치할 디스크를 선택한다. (default 권장)

패키지 선택



- “ 데스크탑Red Hat Enterprise Linux, 지금 선택 ” 선택

설치 패키지 변경

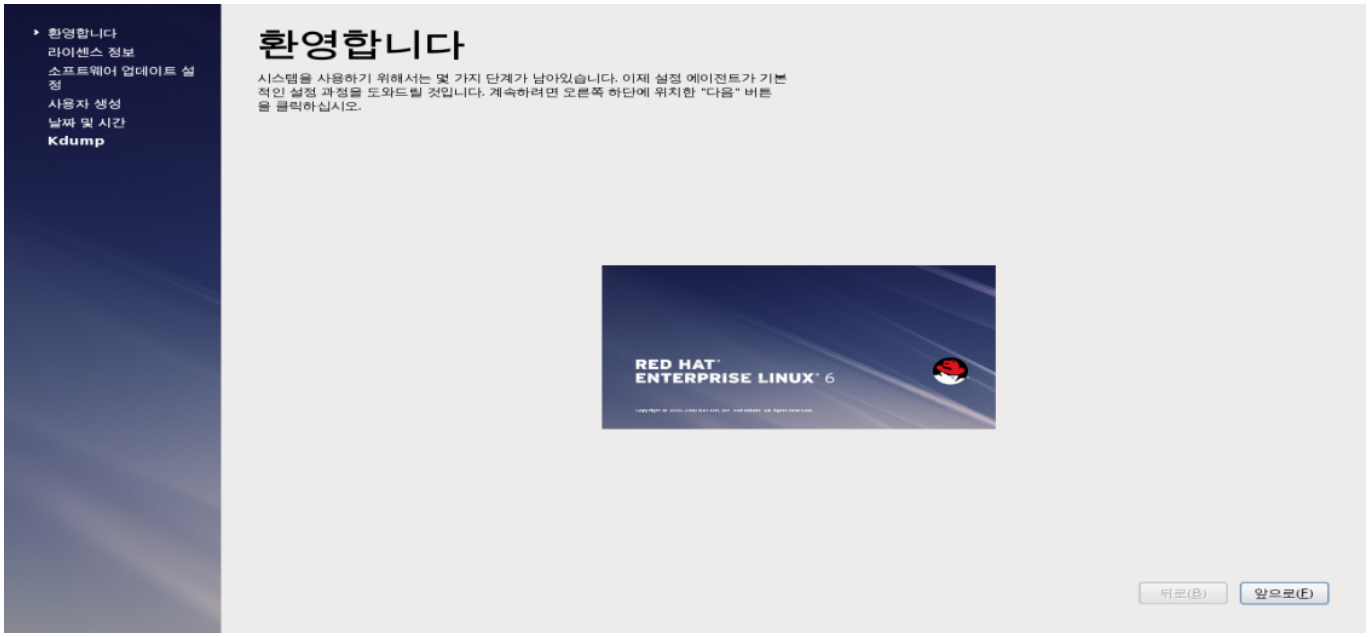


- Rpm Package 참조

설치 진행

- 설치진행 화면

설치 완료



- 설치완료 리부팅 후

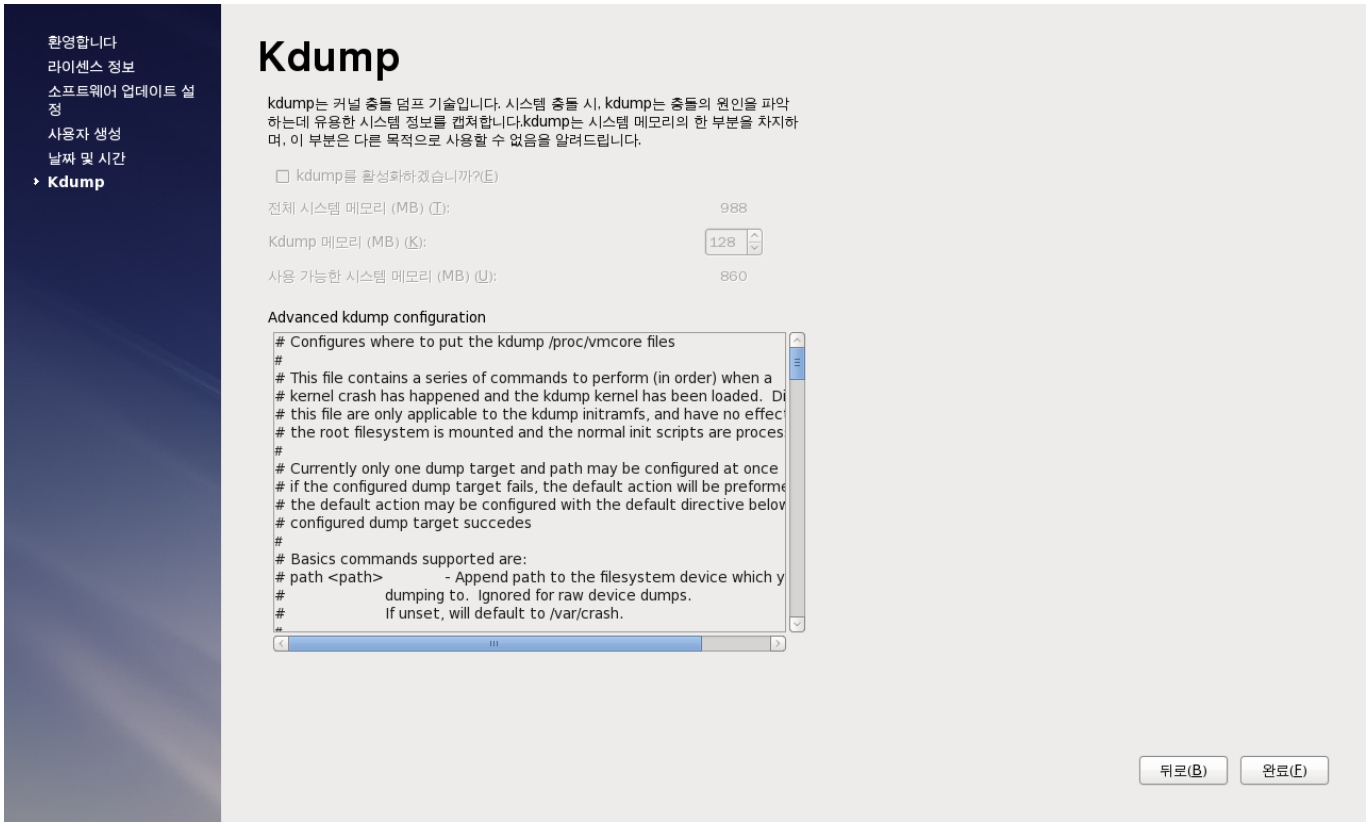
사용자 추가

- 일반사용자계정 추가설정. (필요없는경우 생략)

날짜 및 시간 동기화

- 날짜 및 시간을 설정하고 NTP를 사용한 시간 동기화 설정을 진행한다.

Kdump 설정



- Kdump 설정

RPM Package

1. 기반 서비스. (Base System)
    1. FCoE 저장소 클라이언트 (FCoE Storage Client)
    2. Infiniband지원 (Infiniband Support)
    3. ISCSI저장소 클라이언트 (iSCSI Storage Client)
    4. 거대 시스템 성능 (Large Systems Performance)
    5. 기본 (Base)
    6. 네트워크 파일 시스템 클라이언트 (Network file system client)
    7. 네트워킹 도구 (Networking Tools)
        1. Optional - nmap 선택
    8. 디렉터리 클라이언트 (Directory Client)
    9. 디버깅 도구 (Debugging Tools)
    10. 레거시 유닉스 호환성 (Legacy UNIX compatibility)
        1. Optional - telnet, telnet-server 선택
    11. 메인프레임 엑세스 (Mainframe Access)
    12. 성능 도구 (Performance Tools)
        1. Optional- sg3_util 선택
    13. 저장소 가용성 도구 (Storage Availability Tools)
    14. 하드웨어 모니터링 도구 (Hardware monitoring utilities)
        1. Optional - lm_sensor 선택
    15. 호환성 라이브러리 (Compatibility libraries)
    16. 전화연결 네트워킹지원 (Dial-up Networking Support)
        1. Optional - lrzsz만 선택, 나머지는 해제
2. 서버. (Servers)
    1. FTP 서버 (FTP Server)

    2. 서버 플랫폼 (Server Platform)
    3. 시스템 관리 도구 (System administration tools)
3. 시스템 관리. (System Management)
    1. SNMP지원 (SNMP Support)
    2. 시스템관리 (System Management)
        1. Optional - OpenIPMI
4. 데스크탑. (Desktop) ※ KDE Desktop만 빼고 모두 선택하면 됨
    1. X Window 시스템 (X Window System)
    2. 그래픽기반 관리 도구 (Graphical Administration Tools)
    3. 데스크탑 (Desktop)
    4. 데스크탑 디버깅과 성능 도구 (Desktop Debugging and Performace Tools)
    5. 데스크탑 플랫폼 (Desktop Platform)
    6. 레거시 X Windows 시스템 호환성 (Legacy X Window System compatibility)
    7. 범용 데스크탑 (General Purpose Desktop)
    8. 원격 데스크탑 클라이언트 (Remote Desktop Clients)
    9. 입력 방식 (Input Method)
    10. 폰트 (Fonts)
5. 응용 프로그램. (Applications)
    1. TeX지원 (TeX support)
    2. 기술 저작 (Technical Writing)
    3. 인터넷 브라우저 (Internet Browser)
6. 개발. (Development)
    1. 개발용 도구 (Development tools)
    2. 데스크탑 플랫폼 개발 (Desktop Platform Development)
    3. 서버 플랫폼 개발 (Server Platform Development)
    4. 추가 개발 (Additional Development)
        1. Optional - oracle-devel 해제 (RHEL 5.x)
        2. Optional - net-snmp-devel 추가
        3. Optional - java 1,6 or 1.7 둘 중 선택 또는 둘 다 해제 (둘다 선택해도 1.7.x가 기본셋팅됨)
7. 언어. (Languages)
    1. 한국어 (Korean Support)

OS 기본 셋팅

Kernel Parameter

- /etc/sysctl.conf에 아래 내용 추가 - #sysctl –p 변경내용 적용

Kernel Parameter	기본값	value	비고
kernel.msgmni	7644	1024	메시지 큐 시스템 크기
kernel.sem	250 32000 32 128	1000 32000 32 512	시스템의 세마포어 최대값 지정
kernel.shmmax	68719476736	2147483648	한 개의 공유메모리 세그먼트 최대 크기
kernel.threads-max	60827	270335	최대 생성 스레드 수

Kernel Parameter	기본값	value	비고
net.ipv4.tcp_max_syn_backlog	2048	8192	접속한 클라이언트들 중 승인을 받지못하는 접속 요청들의 최대값 지정
net.ipv4.tcp_syncookies	1	1	소켓으로 syn backlog queue가 넘칠때 syncookies를 보낼지 설정
net.ipv4.tcp_fin_timeout	60	30	서버에 의해 닫혀질때 FIN_WAIT-2 상태의 소켓을 유지시킬 시간을 설정
net.ipv4.tcp_keepalive_time	7200	600	Keepalive가 활성화되어 있을 경우 얼마나 자주 TCP가 Keepalive 메시지를 보낼지 설정
net.ipv4.tcp_syn_retries	5	2	활성화된 TCP 접속이 재전송을 시도하기 위한 최초 SYNC 시간의 값 설정
net.ipv4.tcp_retries2	15	5	살아있는 TCP 연결을 끊기전 확인하는 횟수 설정
net.core.rmem_default	124928	4194304	소켓 수신 큐 기본값 설정
net.core.wmem_default	124928	4194304	소켓 출력 큐 기본값 설정
net.core.rmem_max	124928	8388608	소켓 수신 큐 최대값 설정
net.core.wmem_max	124928	8388608	소켓 출력 큐 최대값 설정
net.ipv4.tcp_mem	364896 486528 729792	8388608 8388608 8388608	TCP stack이 메모리를 어떻게 사용할지에 대한 메모리 페이지 단위 설정
net.ipv6.conf.all.disable_ipv6	0	1	Ipv6 off

```
# 이 내용을 복사하여 /etc/sysctl.conf 맨 하단에 추가 후 sysctl -p 로 적용.
kernel.sem = 1000 32000 32 512
kernel.threads-max = 270335
net.ipv4.tcp_max_syn_backlog = 8192
net.ipv4.tcp_keepalive_time = 600

# 활성화된 TCP 접속이 재전송을 시도하게 하기 위한 최초 SYN시간의 값을 정한다.
# 255 보다 높아서는 안된다. 기본값은 5이며, 180 초에 대응이 된다.
# Default : 5
net.ipv4.tcp_syn_retries = 2

# passive TCP 접속시도가 재접속을 하기 위한 SYNACKs의 값을 정한다. 255 보다 높
# 게 지정할 수 없다. 기본값은 5이며, 180초에 대응이 된다.
# Default : 5
net.ipv4.tcp_synack_retries = 2

# 연결이 끊어졌다고 판단할 때까지, 얼마나 keepalive probe 를 보낼지 결정.
# Default : 9
net.ipv4.tcp_keepalive_probes = 5

# keepalive_probes 를 보낼 간격을 정함. probe 를 보낸 후, probes * intvl 의 시
# 간이 지나도록 응답이 없으면 연결이 해제된 것으로 간주하게 됨. 기본 값의 사용
# 시 11분 15초 동안 재시도를 하고 연결을 취소함. 값은 초단위
# Default : 75
net.ipv4.tcp_keepalive_intvl = 10
```

```
# 무언가 잘못되었을 경우, network layer로 이 현상을 reporting 하기전 다시 확인
# 을 하기 위한 횟수를 지정한다. 최소 RPC 값은 3 이며, 이는 RTO 상에서 3 초에서
# 8 분 사이에 응답을 하도록 하는 것이 기본값이다.
net.ipv4.tcp_retries1 = 3
net.ipv4.tcp_retries2 = 5

# tcp 연결해제 시간을 줄이며 불필요한 ip확장기능을 사용하지 않음
# Decrease the time default value for tcp_fin_timeout connection
# 소켓이 항상 close 되기 전에 마지막 FIN을 기다리는 시간
# Default : 30
net.ipv4.tcp_fin_timeout = 20

# Socket Buffer Tunning
# 이 값은 부팅시에 자동으로 감지하여 설정이 됨.
# 고정을 하고 싶을 경우에는 설정
net.core.rmem_default = 4194304
net.core.wmem_default = 4194304
net.core.rmem_max = 8388608
net.core.wmem_max = 8388608
net.ipv4.tcp_mem = 8388608 8388608 8388608

# IPv6 Disable
net.ipv6.conf.all.disable_ipv6 = 1
```

Ulimit

* /etc/security/limits.conf 아래 내용 추가

```
Domain(USER)    type    item    value    비고
*   soft    nofile    8192    한번에 오픈 가능한 파일 최대치 기본값 설정
*   hard    nofile    65535    한번에 오픈 가능한 파일 최대치 한계값 설정
*   soft    nproc    8192    프로세스 생성 최대치 기본값 설정
*   soft    core    20480    어플리케이션 덤프 기본값 설정
```

Selinux off 설정

```
[user@host]# vi/etc/sysconfig/selinux
SELINUX=disabled
<code vim>

==== Sar collect(10분 -> 5분주기로 변경) ====
<code vim>
[user@host]# vi /etc/cron.d/sysstat (default value 10)

# run system activity accounting tool every 10 minutes
*/5 * * * * root /usr/lib64/sa/sa1 1 1
```

```
<code vim>

==== Bonding 구성 ====
<code vim>
[user@host]# vi /etc/modprobe.d/bonding.conf(파일 신규 생성)
alias bond0 bonding
alias bond1 bonding

[user@host]# vi /etc/sysconfig/network-scripts/ifcfg-bond*
DEVICE = bond*
BOOTPROTO = static
ONBOOT = yes
IPADDR = xxx.xxx.xxx.xxx
NETMASK = xxx.xxx.xxx.xxx
GATEWAY = xxx.xxx.xxx.xxx
USERCTL = no
NM_CONTROLLED=no
BONDING_OPTS = "mode=1 miimon=100"

[user@host]# vi /etc/sysconfig/network-scripts/ifcfg-eth*
DEVICE = eth*
HWADDR=<MAC주소>
BOOTPROTO = none
ONBOOT = yes
MASTER = bond0
SLAVE = yes
USERCTL=no
NM_CONTROLLED=no
```

특이사항

- bonding 구성시 bond0(public망), bond1(private망) (으)로 설정
- public망은 gateway를 설정해주며, private망은 gateway미설정
- bonding 추가 구성시 gateway 미설정

LVM구성(DATA영역, Oracle영역 구성시)

LVM Type Filesystem 생성 디스크를 Direct로 PV로 생성하게 되면 fdisk –l 과 같은 명령어로 확인시 해당 디스크 사용여부가 구분되지 않아 차후 디스크 작업중에 휴먼장애를 발생시킬 수 도 있으므로 반드시 PV사용하고자 하는 디스크는 LVM Type으로 Filesystem을 생성후에 PV생성 작업을 진행하도록 한다. 아울러 fdisk로 파티셔닝 시 반드시 –cu 옵션을 이용하여 Disk Align을 맞추어 Disk I/O가 제성능을 낼 수 있도록 한다.

fdisk 사용시 (2TB 이하 디스크)

```
[root@host ~]# fdisk -cu /dev/sdc # 1TB 디스크 파티셔닝 예제
Device contains neither a valid DOS partition table, nor Sun, SGI or OSF
```

```
disklabel
Building a new DOS disklabel with disk identifier 0x8404002b.
Changes will remain in memory only, until you decide to write them.
After that, of course, the previous content won't be recoverable.

Warning: invalid flag 0x0000 of partition table 4 will be corrected by
w(rite)
# 새로운 파티션 생성
Command (m for help): n
Command action
   e   extended
   p   primary partition (1-4)
p
Partition number (1-4): 1
First sector (2048-2147483647, default 2048): [ENTER]
Using default value 2048 # 2048섹터에서 시작확인
Last sector, +sectors or +size{K,M,G} (2048-2147483647, default 2147483647):
[ENTER]
Using default value 2147483647 # 전체 용량 사용

Command (m for help): p
Disk /dev/sdc: 1099.5 GB, 1099511627776 bytes
255 heads, 63 sectors/track, 133674 cylinders, total 2147483648 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x8404002b

   Device Boot      Start         End      Blocks   Id  System
/dev/sdc1            2048  2147483647  1073740800   83  Linux
# 만들어진 파티션을 LVM타입으로 변경
Command (m for help): t
Selected partition 1
Hex code (type L to list codes): 8E
Changed system type of partition 1 to 8e (Linux LVM)
# 변경된 타입 확인
Command (m for help): p
Disk /dev/sdc: 1099.5 GB, 1099511627776 bytes
255 heads, 63 sectors/track, 133674 cylinders, total 2147483648 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x8404002b

   Device Boot      Start         End      Blocks   Id  System
/dev/sdc1            2048  2147483647  1073740800   8e  Linux LVM
# 변경 정보 저장 후 종료
Command (m for help): w
The partition table has been altered!
```

```
Calling ioctl() to re-read partition table.
Syncing disks.
# 시스템 반영
[root@security ~]# kpartx /dev/sdc
sdc1 : 0 2147481600 /dev/sdc 2048
```

parted 사용시 (2TB 이상 디스크)

```
[root@host]# parted /dev/sdb
# mklabel 명령어로 GPT 형태로 레이블 생성 (msdos type으로는 2TB이상 생성불가)
(parted) mklabel
New disk label type? gpt
# mkpart 명령어로 LVM으로 사용할 파티션 생성
(parted) mkpart
Partition name?  []?
File system type?  [ext2]? ext4
Start? 1
End? -1
# 생성된 파티션을 LVM Type으로 변경
(parted) t
Partition number? 1
Flag to Invert? lvm
# 출력정보를 섹터 기준으로 맞춤 (생성시에는 compact로 설정)
(parted) u
Unit?  [compact]? s
# 만들어진 파티션 확인
(parted) p
Model: VMware, VMware Virtual S (scsi)
Disk /dev/sdb: 20971520s
Sector size (logical/physical): 512B/512B
Partition Table: gpt

Number  Start  End        Size       File system  Name  Flags
 1      2048s  20969471s  20967424s                     lvm
```

PV 생성

```
[user@host]# pvcreate /dev/sdb*
[user@host]# pvdisplay –v
```

VG 생성

```
[user@host]# vgcreate VGWORK11 /dev/sdb*
[user@host]# vgdisplay –v
```

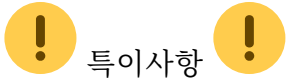
LV 생성

```
[user@host]# lvcreate –L 5G –n netbackup VGWORK11
[user@host]# lvcreate –L 10G –n was_mms VGWORK11
[user@host]# lvcreate –L 10G –n was_sms VGWORK11
[user@host]# lvcreate –L 30G –n oracle VGWORK11
[user@host]# lvcreate –L 400G –n oradata VGWORK11
[user@host]# lvcreate –L 100G –n archive  VGWORK11
[user@host]# lvcreate –L 50G –n oratrace VGWORK11
[user@host]# lvcreate –L 100G –n dbawork VGWORK11
```

파일시스템 생성

```
[user@host]# mkfs.ext4 –i 2048  /dev/mapper/VGWORK11-netbackup
[user@host]# mkfs.ext4 –i 2048  /dev/mapper/VGWORK11-was_mms
[user@host]# mkfs.ext4 –i 2048  /dev/mapper/VGWORK11-was_sms
[user@host]# mkfs.ext4 –i 2048  /dev/mapper/VGWORK11-oracle
[user@host]# mkfs.ext4 –i 2048  /dev/mapper/VGWORK11-oradata
[user@host]# mkfs.ext4 –i 2048  /dev/mapper/VGWORK11-archive
[user@host]# mkfs.ext4 –i 2048  /dev/mapper/VGWORK11-oratrace
[user@host]# mkfs.ext4 –i 2048  /dev/mapper/VGWORK11-dbawork

[user@host]# tune2fs -c '-1' -i 0 /dev/mapper/VGWORK11-netbackup
[user@host]# tune2fs -c '-1' -i 0 /dev/mapper/VGWORK11-was_mms
[user@host]# tune2fs -c '-1' -i 0 /dev/mapper/VGWORK11-was_sms
[user@host]# tune2fs -c '-1' -i 0 /dev/mapper/VGWORK11-oracle
[user@host]# tune2fs -c '-1' -i 0 /dev/mapper/VGWORK11-oradata
[user@host]# tune2fs -c '-1' -i 0 /dev/mapper/VGWORK11-archive
[user@host]# tune2fs -c '-1' -i 0 /dev/mapper/VGWORK11-oratrace
[user@host]# tune2fs -c '-1' -i 0 /dev/mapper/VGWORK11-dbawork
```



- 파일시스템 생성 시 Default Inode 값을 2배이상으로 설정.
- tune2fs –c는 최대 mount 횟수지정으로 최대값에 도달 시 강제로 파일시스템 체크 진행
- tune2fs –i는 파일시스템체크 기간 설정으로 0은 파일시스템 체크를 비활성 함.

Mount 설정

- blkid 명령을 통해 UUID 값을 확인하여, 삽입하기를 권장

```
[user@host]# blkid /dev/sda1
/dev/sda1: UUID="8ff42fc7-d3f5-4291-8299-05b017b64863" TYPE="ext4"

[user@host]# vi /etc/fstab
```

```
UUID=51b53fa3-6646-427e-9b9b-42c2d0ae71ac   /netbackup    ext4    defaults
0 0
UUID=2256dce2-0643-4215-90f4-faa941f2c1ad   /was_mms    ext4    defaults
0 0
UUID=fc70af47-16e5-4e85-84f3-08f5ba105aff   /was_sms    ext4    defaults
0 0
UUID=11d99296-d5e7-4c74-868f-213624236592   /oracle        ext4    defaults
0 0
UUID=fc336d3e-4997-4ff5-be11-c9f5e1abad46   /oradata    ext4    defaults
0 0
UUID=b115ef6f-3a0c-4ab1-9c48-8ba44c85a10f   /archive    ext4    defaults
0 0
UUID=5ed3e93b-253e-4be6-b0eb-72be857c7c99   /oratrace    ext4    defaults
0 0
UUID=dcd42217-29f3-4956-b63b-5cbbb436d05c   /dbawork    ext4    defaults
0 0
```

 특이사항 

- DATA영역에 관련하여 시스템 부팅 시 파일시스템 체크를 안하도록 fstab에 등록합니다.

Kdump 설정

Hang 발생시 vmcore 미생성되면 root cause 를 확인하기 어려움

```
[user@host]# vi /etc/sysctl.conf
kernel.sysrq=1
[user@host]# sysctl –p
```

로 설정적용 후

1. 키보드에서 Alt + sysRq + C 키를 동시에 눌러서 패닉 유발.
2. echo c > /proc/sysrq-trigger 명령어를 통해서 패닉 유발
3. core dump 생성 확인

Routing Table

Zero Configuration Networking 비활성화

Routing 테이블에 Wireless 와 같은 169.254.0.0/16 아이피가 찍힐 경우 비활성화

```
[user@host]# vi /etc/sysconfig/network
NOZEROCONF=yes # 추가.
```

Routing Table

라우팅 경로를 수동으로 입력해야 하는경우

커맨드로 반영 하는 방법

```
[user@host]# route add -net 172.18.167.242 netmask 255.255.255.255 gateway
172.18.167.1
[user@host]# route add -net 192.168.201.155 netmask 255.255.255.255 gateway
172.18.167.1
```

이 방식을 사용하면 즉시 반영 되지만 재부팅시에는 설정이 유지되지 않는다. rc.local같은 곳에 추가하여 사용해도 되지만 추천하지 않으며 영구적인 설정을 원하는 경우 아래의 file방식을 이용하도록 한다.

route 파일을 이용한 방법

```
[user@host]# vi /etc/sysconfig/network-script/route-bond0
# 해당 대역에 대해 임이의 게이트웨이를 정의해주는 경우
172.18.160.0/24 via 172.18.167.1
192.168.201.155 via 172.18.167.1
# 게이트웨이 없이 장치를 라우트 경로로 설정하는 경우
192.168.10.0/24 via dev eth0
```

NTP설정 (NTP연결이 가능한 경우에만 설정)

/etc/ntp.conf

```
# Use public servers from the pool.ntp.org project.
# Please consider joining the pool (http://www.pool.ntp.org/join.html).
server 0.centos.pool.ntp.org iburst
server 1.centos.pool.ntp.org iburst
server 2.centos.pool.ntp.org iburst
server 3.centos.pool.ntp.org iburst
```

인터넷이 되는 경우 기본값으로 설정된 ntp서버를 그대로 이용하여도 되며 별도의 ntp서버가 있는경우 해당 서버를 등록하여 준다.

/etc/sysconfig/ntpdate

ntp 설정시 반드시 ntpdate또한 같이 설정해준다.

```
[user@host]# chkconfig ntpdate on
```

```
[user@host]# vim /etc/sysconfig/ntpdate
```

```
# Options for ntpdate
OPTIONS="-U ntp -s -b"

# Number of retries before giving up
RETRIES=2

# Set to 'yes' to sync hw clock after successful ntpdate
SYNC_HWCLOCK=yes
```

SYNC_HWCLOCK=yes 로 설정

보안 기본조치 가이드

계정 및 패스워드 관리

SSH root 로그인 제한

주석 해제 및 yes → no 변경

```
[user@host]# vi /etc/ssh/sshd_config
PermitRootLogin no
```

패스워드 사용규칙 적용

패스워드 최대 사용 기간 설정

```
[user@host]# vi /etc/login.defs
PASS_MAX_DAYS   70 # 패스워드 사용할 수 있는 기간. 이 기간 이후에는 변경하여야 한다.
PASS_MIN_DAYS   0 # 패스워드 변경 후 0일이 경과되어야만 다시 변경할 수 있다.
PASS_MIN_LEN    8 # 패스워드 길이. 최소 8글자 이상 입력하여야 함.
PASS_WARN_AGE   7 # 패스워드 만료일 7일전에 알림 메세지 출력.
```

히스토리 설정

```
[user@host]# /etc/profile
HOSTNAME=`/bin/hostname 2>/dev/null`
HISTSIZE=5000
HISTTIMEFORMAT="%F %T "
if [ "$HISTCONTROL" = "ignorespace" ] ; then
    export HISTCONTROL=ignoreboth
else
```

```
    export HISTCONTROL=ignoredups
fi

export PATH USER LOGNAME MAIL HOSTNAME HISTSIZE HISTCONTROL HISTTIMEFORMAT
```

접근제어

세션 타임아웃 설정

(10분간 입력 없을시 자동 로그아웃)

```
[user@host]# vi /etc/profile
TMOUT=600
export TMOUT
```

익명 FTP 제한

(FTP서비스가 필요한 경우가 아닌이상 사용하지 않는걸 권장. SFTP사용 권장)

```
[user@host]# vi /etc/vsftpd/vsftpd.conf
anonymous_enable=NO
local_umask=077
```

Root 로그인 차단

```
[user@host]# vi /etc/ssh/sshd_config
PermitRootLogin no
PermitEmptyPasswords no
```

시스템 보안

Setuid, setgid 제거

```
[user@host]# chmod –s /sbin/dump
[user@host]# chmod –s /usr/bin/lpq-lpd
[user@host]# chmod –s /usr/bin/newgrp
[user@host]# chmod –s /sbin/restore
[user@host]# chmod –s /usr/bin/lpr
[user@host]# chmod –s /usr/sbin/lpc
[user@host]# chmod –s /sbin/unix_chkpwd (적용제외 – 일부시스템에서 문제 유발 가능성 있음)
```

```
[user@host]# chmod –s /usr/bin/lpr-lpd
[user@host]# chmod –s /usr/sbin/lpc-lpd
[user@host]# chmod –s /usr/bin/at
[user@host]# chmod –s /usr/bin/lprm
[user@host]# chmod –s /bin/traceroute
[user@host]# chmod –s /usr/bin/lpq
[user@host]# chmod –s /usr/bin/lprm-lpd
```

openssh, openssl 최신버전 유지

어플리케이션에 영향을 주지 않는 범위 내에서 영향도 확인 후 실행 되어야 함

```
[root@security ~]# rpm -qa |grep -E "open(ssh|ssl)"
openssh-clients-5.3p1-104.el6.x86_64
openssl-1.0.1e-30.el6.x86_64
openssl-devel-1.0.1e-30.el6.x86_64
openssh-askpass-5.3p1-104.el6.x86_64
openssl098e-0.9.8e-18.el6_5.2.x86_64
openssh-5.3p1-104.el6.x86_64
openssh-server-5.3p1-104.el6.x86_64
```

- 문서 작성일 현재(2014-12-16) 아래 버전 요구조건 필요
- RHEL 6.x
  - openssh-5.3p1-104.el6_6.1 이상
  - openssl-1.0.1e-30.el6_6.4 이상
- RHEL 5.x
  - openssh-4.3p2-82.el5 이상
  - openssl-0.9.8e-31.el5_11 이상

kernel 최신버전 유지

현재 커널은 2.6.32-431.el6.x86_64 에 맞추어져 있기 때문에 전사적으로 영향도 확인 후 실행 되어야 함

```
[user@host]# yum update kernel*
```

- 문서 작성일 현재(2014-12-16)
  - RHEL 6.x : kernel-2.6.32-504.3.3.el6 이상
  - RHEL 5.x : kernel-2.6.18-400.el5 이상

bash 최신버전 유지

어플리케이션에 영향을 주지 않는 범위 내에서 영향도 확인 후 실행 되어야 함

```
[user@host]# yum update bash
```

- 문서 작성일 현재(2014-12-16)
  - RHEL 6.x : bash-4.1.2-29.el6이상
  - RHEL 5.x : bash-3.2-33.el5_11.4 이상

서비스 보안

불필요한 서비스 데몬 중지

```
[user@host]# chkconfig cgconfig on (DCB by FCoE)
[user@host]# chkconfig ntpdate on
[user@host]# chkconfig ntpd on
[user@host]# chkconfig NetworkManager off
[user@host]# chkconfig cups off
[user@host]# chkconfig cpuspeed off
[user@host]# chkconfig ip6tables off
[user@host]# chkconfig iptables off
[user@host]# chkconfig bluetooth off
```

서비스 banner 관리

서비스 (Telnet, FTP, SMTP등) 의 서비스 버전 유출 방지, 필요한 문구로 대체

```
[user@host]# vi /etc/issue
[user@host]# vi /etc/issue.net
```

특정 서비스 권한 설정 (at, crontab)

/etc/at.allow, /etc/cron.allow 빈 파일을 생성하여 허가된 사용자 외에는 at, crontab 명령어를 사용하지 못하도록 설정 명령어를 허용할 사용자만 해당 파일에 추가

```
[user@host]# touch /etc/at.allow /etc/cron.allow
[user@host]# chmod 600 /etc/at.allow /etc/cron.allow
```

su - wheel 그룹만 가능하도록 설정

```
[user@host]# vi /etc/pam.d/su
auth            required        pam_wheel.so use_uid # 주석 해제
```

su를 허용할 계정에 wheel 그룹 추가 [user@host]# usermod –G wheel <account>

로그관리

시스템 로그 특이사항 점검

```
[user@host]# vi /var/log/messages
[user@host]# grep -i "\(error\|fail\|warn\)" /var/log/messages
```

logrotate 설정

기본적으로 logrotate설정은 주간단위로 4번 순환 설정되어있다. 3개월분(12주) 로그내용을 보관할 수 있도록 설정을 변경한다.

```
[user@host]# vi /etc/logrotate.conf

# keep 4 weeks worth of backlogs
# 12주(3개월) 보관하도록 변경
rotate 12

# uncomment this if you want your log files compressed
# .gz파일로 압축보관하도록 주석 해제
compress
compressext .gz
```

- 압축된 로그 파일은 vim 편집기로 열면 압축해제 없이 바로 열람 가능함
- ex) [root@host]# vim /var/log/message-2014-12-12.gz