Red Hat Linux 9

Red Hat Linux 사용자 정의 가이드

Red Hat Linux 9: Red Hat Linux 사용자 정의 가이드


Red Hat, Inc.

1801 Varsity Drive Raleigh
NC 27606-2072 USA
Phone: +1 919 754 3700 Phone: 888 733 4281
Fax: +1 919 754 3701 PO Box 13588 Research Triangle
Park NC 27709 USA

rhl-cg(KO)-9-Print-RHI (2003-02-13T16:45)

차례

머리글

Red Hat Linux 사용자 정의 가이드에 오신 것을 환영합니다!

Red Hat Linux 사용자 정의 가이드는 Red Hat Linux 시스템을 여러분의 필요에 맞게 사용자 설정하는 방법에 대한 정보를 포함하고 있습니다. 만일 시스템을 구성하고 사용자 설정하기 위하여 단계별로 설명된 작업-지향적인 가이드를 찾고 계시다면, 바로 이 메뉴얼을 추천해 드립니다. 이 메뉴얼에서는 다음과 같이 많은 중급 수준의 주제가 다루어질 것입니다:

- 네트워크 인터페이스 카드 (NIC) 설정하기
- 킥스타트(Kickstart) 설치 실행하기
- 삼바 공유(Samba shares) 설정하기
- RPM을 사용하여 소프트웨어 관리하기
- 사용하시는 시스템에 대한 정보 알아내기
- 커널(kernel) 업그레이드하기

이 메뉴얼은 다음과 같은 주요 카테고리로 분류되어 있습니다:

- 설치-관련 참조
- 네트워크-관련 참조
- 시스템 설정
- 패키지 관리

이 가이드는 여러분이 이미 Red Hat Linux 시스템의 기본을 이해하고 계신다는 가정 하에 쓰여졌습니다. 만일 데스크탑 설정 방법이나 오디오 CD-RPM 재생 방식과 같은 보다 기본적인 주제를 다루는 참고 자료를 원하신다면, *Red Hat Linux* 시작하기 가이드를 참조해 주십시오. 만일 Red Hat Linux 파일 시스템의 개요와 같은 보다 고급 수준의 문서 자료를 원하시면, *Red Hat Linux* 참조 가이드를 참조하시기 바랍니다.

HTML과 PDF 버전으로 된 공식 Red Hat Linux 메뉴얼은 문서 CD와 http://www.redhat.com/docs/ 사이트에서 찾으실 수 있습니다.

알림

이 메뉴얼은 가능한 최근의 정보를 담고 있지만, 이 메뉴얼의 문서 작업이 완료된 후 업데이트되고 새로워진 사항들에 대해서는 *Red Hat Linux* 출시에 앞서를 참고하셔야 합니다. 출시에 앞서는 Red Hat Linux CD #1 과 다음의 온라인 사이트에서 찾으실 수 있습니다:

`http://www.redhat.com/docs/manuals/linux`

1. 메뉴얼의 새로운 사항

이 메뉴얼에는 독자들의 요청에 따라 새로운 주제들이 추가되었을 뿐만 아니라 Red Hat Linux 9의 새로운 기능에 대한 설명도 포함되어 있습니다. 이 메뉴얼의 중요한 변경 사항은 다음과 같습니다:

디스크 사용량 할당하기

‘ 새롭게 추가된 이 장에서는 디스크 사용량을 설정하고 관리하는 방법에 대하여 설명합니다.

인증 설정

‘ 새롭게 추가된 이 장에서는 **인증 설정 도구** 사용법에 대하여 설명하고 있습니다.

사용자 설정

‘ 이 장에서는 사용자와 그룹을 관리하는데 사용되는 명령행 유틸리티 및 시스템에 새로운 사용자를 추가시 상황 설명이 더해졌습니다.

Samba

‘ 이 장에서는 새 **Samba 서버 설정 도구**에 대한 정보가 포함되었습니다.

프린터 설정

‘ 이 장은 새 **프린터 설정 도구** 인터페이스와 새 **GNOME 인쇄 관리자** 및 패널에서 프린터 아이콘을 끌어다 놓기하는 새로운 기능에 대한 설명을 포함하였습니다.

킥스타트 *(Kickstart)*

‘ 킥스타트 옵션에 Red Hat Linux 9의 새로운 옵션을 포함하도록 업데이트되었으며, **킥스타트 설정 프로그램** 장에는 일부 새로운 기능에 대한 설명이 추가되었습니다.

네트워크 설정

‘ 이 장에는 최신 **네트워크 관리 도구** 인터페이스와 기능에 대한 설명이 추가되었습니다.

날짜와 시간 설정

‘ 이 장은 *Red Hat Linux* 시작하기 가이드로 옮겨 졌습니다.

2. 문서 약정

이 메뉴얼을 읽으실 때 여러분은 다른 글꼴, 활자체, 크기와 두께로 된 단어들을 보시게 될 것입니다. 이러한 글꼴 강조의 이유는 특정 범주에 포함되는 여러 다른 단어들을 동일한 형식으로 표시하기 위해서 입니다. 이러한 방식으로 표현되는 단어의 유형은 다음과 같습니다:

`command`

‘ Linux 명령어는 (그리고 다른 운영 체제 명령어는) 이와 같은 방식으로 표현됩니다. 이 스타일은 여러분이 명령 행에서 단어나 구문을 입력하신 후 [Enter] 키를 눌렀을 때 실행되는 명령어를 의미합니다. 종종 명령어 안에는 다른 방식으로 표시된 단어들 (예, 파일명)이 포함됩니다. 이러한 경우, 다른 방식으로 표현되는 단어들은 명령어의 일부로서 간주되며 전체 구문은 한 명령어로서 표시될 것입니다. 예를 들면:

현재 작업중인 디렉토리에서 `testfile`이라는 이름의 파일 내용을 보기 위해서는 `cat testfile` 명령을 사용합니다.

`filename`

‘ 파일명, 디렉토리명, 경로와 RPM 패키지명은 이러한 방식으로 표현됩니다. 이 스타일은 Red Hat Linux 시스템 상에 존재하는 특정 파일이나 디렉토리의 이름을 나타냅니다. 예를 들면:

홈 디렉토리에 있는 `.bashrc` 파일은 사용자가 생성한 bash 쉘 정의와 별칭(alias)을 포함합니다.

`/etc/fstab` 파일은 다른 시스템 장치와 파일 시스템에 관한 정보를 포함하고 있습니다.

만일 웹 서버 로그 파일 분석 프로그램을 사용하시려면 `webalizer` RPM을 설치하십시오.

application

‘ 이 스타일은 프로그램이 (시스템 소프트웨어가 아닌) 일반 사용자 응용 프로그램이라는 것을 의미합니다. 예를 들면:

웹 브라우징을 위하여 **Mozilla**를 사용합니다.

[key]

‘ 키보드 상의 키들은 이러한 스타일로 나타납니다. 예를 들면:

[Tab] 자동 완성 기능을 사용하려면, 한 개의 문자를 입력하신 후 [Tab] 키를 누르십시오. 디렉토리 안에 있는 파일 중에서 입력하신 단어로 시작하는 파일의 목록이 터미널에 나타날 것입니다.

[key]-[조합]

‘ 키 입력 조합은 이와 같은 방식으로 나타납니다. 예를 들면:

[Ctrl]-[Alt]-[Backspace] 키 조합은 그래픽 세션을 종료하고 그래픽 로그인 화면이나 콘솔로 되돌아가는데 사용됩니다.

GUI 인터페이스 상의 텍스트

‘ GUI 인터페이스 화면이나 윈도우 상에서 제목, 단어나 문구들은 이러한 스타일로 나타날 것입니다. 이러한 스타일로 나타나는 텍스트는 특정 GUI 화면이나 GUI 화면 상의 요소를 (예, 체크박스와 관련된 텍스트나 항목을) 식별하기 위하여 사용됩니다. 예:

만일 화면 보호기가 멈추기 전에 암호를 요청하도록 설정하시려면 **암호 요구** 체크박스를 선택해 주십시오.

GUI 화면이나 창에서 상위 메뉴

‘ 이러한 스타일의 단어는 풀다운 메뉴에서 상위 메뉴를 의미합니다. GUI 화면에서 이러한 단어를 클릭하시면 나머지 메뉴가 나타날 것입니다. 예를 들면:

GNOME 터미널에서 **파일** 항목 아래를 보시면, **새로운 탭** 항목이 나타날 것입니다. 이 항목을 선택하시면 동일한 창에서 여러 개의 쉘 프롬프트를 여실 수 있습니다.

GUI 메뉴에서 명령어를 순서대로 입력하셔야할 경우, 다음에 나온 예와 유사하게 나타날 것입니다:

패널에서 **주 메뉴 버튼**을 클릭하신 후 => **프로그래밍** => **Emacs**를 선택하시면 **Emacs** 텍스트 편집기가 실행됩니다.

GUI 화면이나 창의 버튼

‘ 이러한 스타일은 해당 텍스트가 GUI 화면 상에서 클릭할 수 있는 버튼 위에 나타난다는 것을 의미합니다. 예를 들면:

마지막으로 본 웹페이지로 되돌아가기 위해서는 **뒤로** 버튼을 클릭하십시오.

컴퓨터 출력 결과

‘ 이러한 스타일의 텍스트는 명령 행에서 출력된 텍스트 결과를 나타냅니다. 다음과 같은 스크립트나 프로그램을 이력하시면 명령에 대한 결과나 오류 메시지, 또는 상호대화식 프롬프트가 나타날 것입니다. 예를 들면:

디렉토리의 내용을 보기 위하여 `ls` 명령을 사용합니다:

```
$ ls
Desktop       about.html   logs    paulwesterberg.png
Mail        backupfiles   mail    reports
```

이 명령의 출력 결과 (이 경우, 디렉토리의 내용)은 이러한 스타일로 표현됩니다.

프롬프트 (prompt)

‘ 프롬프트는 컴퓨터가 입력을 받아들일 준비가 되어있다는 것을 나타내며 이러한 스타일로 표현됩니다. 예를 들면:

```
$
#
[stephen@maturin stephen]$
leopard login:
```

사용자 입력

‘ 명령 행이나 GUI 화면에서 사용자가 입력할 텍스트는 이러한 스타일로 표현됩니다. 다음에 나온 예에서 **text**는 이러한 스타일로 표현되었습니다:

시스템을 텍스트 기반 설치 프로그램으로 부팅하시려면, `boot:` 프롬프트에서 **text** 명령을 입력해 주십시오.

추가적으로, 특정 정보에 대하여 여러분의 주의를 끌기 위하여 여러가지 다른 방법이 사용되었습니다. 시스템에 대한 정보의 중요도에 따라서 이러한 항목들은 주목, 힌트, 중요, 경고 또는 주의로 표시될 것입니다. 예를 들면:

알림

Linux는 대/소문자를 구별한다는 점에 주의하십시오. 즉, rose는 ROSE 또는 rOsE와 같지 않습니다.

힌트

`/usr/share/doc` 디렉토리는 시스템 상에 설치된 패키지에 대한 추가적인 문서 자료를 포함하고 있습니다.

중요

DHCP 설정 파일을 수정하신 후 여러분이 DHCP 데몬을 재시작하실 때까지 변경된 사항은 적용되지 않을 것입니다.

주의

루트로서 일상적인 작업을 수행하지 마십시오. — 시스템 관리 작업을 위해 루트 계정을 사용해야될 경우가 아니라면 일반 사용자 계정을 사용하십시오.

경고

수동으로 파티션하지 않기로 결정하셨다면, 서버 설치는 모든 설치된 하드 드라이브 상에 있는 기존의 모든 파티션을 제거할 것입니다. 확실히 저장할 데이터가 없는 경우를 제외하고는 이 설치 클래스를 선택하지 마십시오.

3. 앞으로 추가될 사항

Red Hat은 Red Hat Linux 사용자 여러분께 유용하고 신속한 지원을 제공할 수 있도록 *Red Hat Linux* 사용자 정의 가이드를 계속적으로 개정, 확장하도록 노력할 것입니다. 새로운 도구와 응용 프로그램들이 출시되는 즉시 이 가이드에 포함시키겠습니다.

3.1. 여러분의 의견을 기다리고 있습니다

만일 *Red Hat Linux* 사용자 정의 가이드에서 오자를 발견하셨거나, 더 좋은 메뉴얼을 만들기 위한 제안이 있다면, 언제든지 저희에게 연락해 주십시오! `rhl-cg`에 대한 리포트를 버그질라(Bugzilla)에 제출해 주십시오. (http://bugzilla.redhat.com/bugzilla/)

버그 리포트를 제출하실 때, 다음에 나온 메뉴얼의 식별 번호를 언급해 주십시오:

```
rhl-cg(KO)-9-Print-RHI(2003-02-13T16:45)
```

메뉴얼의 식별 번호를 언급함으로서, 저희는 여러분이 가지고 계신 가이드의 버전 번호를 정확하게 식별할 수 있습니다.

자료 문서 개선을 위한 제안이 있으시면, 최대한 명확히 설명해 주시기 바랍니다. 오류를 발견하셨다면, 저희가 쉽게 식별할 수 있도록 섹션 번호와 주위의 문장들을 함께 보내주시기 바랍니다.

4. 회원 등록하는 것을 잊지마세요

Red Hat Linux 9를 소유하고 계신 경우, 꼭 회원 등록을 하셔서 Red Hat 고객으로서의 혜택을 받으시기 바랍니다.

구입하신 Red Hat Linux 제품의 종류에 따라 아래에 언급된 모든 또는 특정 혜택을 받으실 수 있습니다:

- Red Hat 지원 — 설치에 관한 질문 사항은 Red Hat, Inc. 지원팀으로 문의하십시오.
- Red Hat Network — 손쉽게 패키지를 업데이트하고 사용자의 시스템에 맞게 사용자 정의된 보안 경고를 받을 수 있습니다. 자세한 사항은 http://rhn.redhat.com 사이트를 방문하시기 바랍니다.
- *Under the Brim: Red Hat E*-뉴스레터 — 매달 Red Hat로부터 최신 뉴스와 제품 정보를 직접 전달해 드립니다.

http://www.redhat.com/apps/activate/ 웹사이트에서 등록하시기 바랍니다. 여러분의 제품 ID는 Red Hat Linux 제품 박스 안에 검정색, 빨간색과 흰색으로 된 등록 정보 카드에서 찾으실 수 있습니다.

Red Hat Linux의 기술 지원에 대한 보다 자세한 정보를 보시려면, *Red Hat Linux* 설치 가이드의 기술 지원 받기 부록을 참조하시기 바랍니다.

행운을 빌며 Red Hat Linux를 선택해 주셔서 감사드립니다!

Red Hat 문서 작성팀

I. 파일 시스템

파일 시스템이란 컴퓨터 상에 저장된 파일들과 디렉토리들을 지칭합니다. 파일 시스템은 파일 시스템 유형이라고 부르는 다른 형식을 갖추고 있습니다. 일부 파일 시스템 유형은 데이터를 중복 복사해서 저장하는 반면, 다른 파일 시스템 유형은 하드 드라이브에 보다 접근할 수 있도록 해줍니다. 이 부분에서는 ext3, swap, RAID, LVM 파일 시스템 유형에 대하여 설명해 보겠습니다. 파티션 관리에 사용되는 `parted` 유틸리티에 대한 설명도 포함되어 있습니다.

차례

redhat.

1장 .

ext3 파일 시스템

Red Hat Linux 7.2 버전부터는, 기본 파일 시스템이 지금까지 사용되어진 ext2 형식에서 저널링 *ext3* 파일 시스템으로 바뀌었습니다.

1.1. ext3의 기능

ext3 파일 시스템은 ext2 형식의 기능을 강화시킨 파일 시스템 버전으로서, ext3 파일 시스템의 장점은 다음과 같습니다:

가용성 (Availability)

‘ 예상하지 않았던 재부팅이나 시스템 고장 (비정상 시스템 종료라고도 불림)이 발생한 경우, ext2 파일 시스템 검사 프로그램인 `e2fsck`를 실행하여 파일 시스템의 일관성을 검사해야 합니다. 따라서 이러한 작업은 시스템 부팅에 걸리는 시간을 지연시킬 수 있어 매우 시간 소모적이며, 특히 방대한 분량의 파일을 포함한 시스템의 경우에는 더욱 그러합니다. 또한 `e2fsck` 프로그램이 검사 중인 데이터는 검사 작업이 진행되는 동안에는 사용할 수 없습니다.

ext3 파일 시스템의 저널링 기능을 이용하면, 시스템이 비정상적으로 종료된 후에도 이러한 시간 소모적인 파일 시스템 검사 작업을 수행할 필요가 전혀 없습니다. ext3 파일 시스템에서는 하드 드라이브가 고장난 경우와 같이 특정 하드웨어에 문제가 있는 경우에만 일관성 검사를 수행합니다. 시스템이 비정상적으로 종료된 후 ext3 파일 시스템을 복구하는데 걸리는 시간은 파일 시스템의 크기나 파일의 숫자에 따라 결정되지 않고; 파일 시스템의 일관성을 유지하는데 사용되는 저널 *(journal)*의 크기에 따라 결정됩니다. 하드웨어의 속도에 따라서 기본 저널 크기의 경우, 일반적으로 파일 시스템을 복구하는데 1초가 걸립니다.

데이터 신뢰성 강화 (Data Integrity)

‘ ext3 파일 시스템은 시스템 비정상 종료시 데이터 손상 문제를 피해가면서 데이터 저널링을 효율적으로 제공합니다. ext3 파일 시스템은 여러분이 직접 데이터 보호 유형과 수준을 결정하실 수 있도록 해줍니다. 디폴트 값으로, Red Hat Linux 9는 파일 시스템 상태에 따라서 데이터를 최상위 수준으로 보존하도록 ext3 볼륨을 설정합니다.

보다 빠른 수행 속도

‘ 비록 ext3는 일부 동일한 데이터를 한 번 이상 반복하여 기록하지만, 하드 드라이브 헤드 모션을 최적화하는 저널링 기능 덕분에 대부분의 경우 ext2 파일 시스템 보다 빠른 속도로 작업을 수행할 수 있습니다. 속도를 최적화하기 위해 3가지 저널링 모드를 선택하실 수 있지만, 그렇게 하시면 데이터 보호 기능이 약화될 수 있다는 점에 유의해 주십시오.

손쉬운 변환 과정

‘ ext2에서 ext3로 변환 과정은 매우 쉽고 간단합니다. 파일 시스템을 재포맷할 필요가 없이 강력한 저널링 기능을 갖춘 ext3 파일 시스템으로 변환 가능합니다. ext2에서 ext3로 변환하는 방법에 대한 보다 많은 정보를 원하신다면, 1.3 절를 참조하시기 바랍니다.

Red Hat Linux 9를 새로 설치하신다면, 시스템의 Linux 파티션에는 ext3 파일 시스템이 기본으로 부여됩니다. ext2 파티션을 사용하는 이전 버전의 Red Hat Linux에서 업그레이드를 수행하신다면, 설치 프로그램은 데이터를 잃지 않으면서 이러한 파티션들을 ext3 파티션으로 변환할 수 있게 도와 드릴것입니다. 보다 자세한 정보를 원하신다면, *Red Hat Linux* 설치 가이드에서 현재 시스템 업그레이드하기라는 제목의 부록편을 참조하시기 바랍니다.

다음 부분에서는 ext3 파티션을 생성하고 조절하는 방법에 대하여 단계별로 설명해 보겠습니다. ext2 파티션을 가지고 계시면서 Red Hat Linux 9를 실행하신다면, 아래의 파티션과 포맷하기 섹션을 생략하고 바로 1.3 절로 넘어 가십시오.

1.2. ext3 파일 시스템 생성하기

설치를 마치신 후, 가끔씩 새로운 ext3 파일 시스템을 생성해야할 경우가 있습니다. 예를 들어 Red Hat Linux 시스템에 새로운 디스크 드라이브를 추가하실 경우, 드라이브 상에 ext3 파일 시스템을 사용하는 파티션을 생성하실 수 있습니다.

ext3 파일 시스템을 생성하는 방법은 다음과 같습니다:

1. `parted` 또는 `fdisk`를 사용하여 파티션 생성하기.
2. `mkfs`를 사용하여 ext3 파일 시스템을 사용하는 파티션을 포맷하기.
3. `e2label`를 사용하여 파티션에 이름 붙이기
4. 마운트할 지점 생성하기.
5. 파티션을 `/etc/fstab`에 추가하기.

위에서 설명된 단계를 수행하는 방법에 대한 정보가 필요하시면, 5 장을 참조하시기 바랍니다.

1.3. ext3 파일 시스템으로 변환하기

`tune2fs` 프로그램은 기존 ext2 파일 시스템에서 파티션 상에 저장된 자료를 번경시키지 않고서 저널링 기능을 추가할 수 있는 기능을 갖추고 있습니다. 파일 시스템 변환 과정에서 그 파일 시스템이 이미 마운트되었다면, 저널은 파일 시스템의 루트 디렉토리에서 `.journal` 파일로 나타납니다. 만일 파일 시스템이 마운트되지 않은 경우에는 저널이 감추어져서 파일 시스템에서 전혀 나타나지 않을 것입니다.

ext2 파일 시스템을 ext3로 변환하기 위해서는, 루트로 로그인 하신 후 다음을 입력해 주십시오:

```
/sbin/tune2fs -j /dev/hdbX
```

위의 명령에서 /dev/*hdb* 부분은 장치명을 입력해 주시고, *X* 부분은 파티션 번호로 대체해 주십시오.

명령을 입력하신 후, `/etc/fstab` 파일에서 파티션 유형을 ext2에서 ext3로 변경해 주시는 것을 잊지 마십시오.

루트 파일 시스템을 변환하는 경우에는, `initrd` 이미지 (또는 RAM 디스크)를 사용하여 부팅하셔야 합니다. `mkinitrd` 프로그램을 실행하여 `initrd` 이미지를 만드십시오. `mkinitrd` 명령을 사용하는 방법에 대한 정보를 원하신다면, `man mkinitrd` 명령을 입력하여 메뉴얼 페이지를 읽어보시기 바랍니다. 또한 `initrd`를 로드하도록 GRUB이나 LILO 설정을 확인해 주십시오.

부트로더가 `initrd`를 로드하도록 제대로 설정되지 않는다면, 시스템은 여전히 부팅되지만, 파일 시스템은 ext3 대신에 ext2로 마운트됩니다.

1.4. ext2 파일 시스템으로 되돌리기

ext3는 비교적 최신 파일 시스템이기 때문에, 일부 디스크 유틸리티는 ext3를 지원하지 않는 경우도 있습니다. 예를 들어 `resize2fs`를 사용하여 파티션을 감소시키려고 할 경우, `resize2fs`는 아직 ext3를 지원하지 않습니다. 이러한 경우에 일시적으로 파일 시스템을 ext2로 되돌릴 필요가 있습니다.

파티션을 되돌리기 위해서는, 우선 루트로 로그인 하신 후 다음과 같은 명령을 입력하여 해당 파티션을 마운트 해제하셔야 합니다:

```
umount /dev/hdbX
```

위의 명령에서 /dev/*hdb* 부분은 장치명으로 대체하시고 *X* 부분은 적절한 파티션 번호로 대체해 주십시오. 앞으로 이 섹션에서는 *hdb1*를 예시값으로 사용하도록 하겠습니다.

이제 루트로 다음 명령을 입력하여 파일 시스템 유형을 ext2로 번경합니다:

```
/sbin/tune2fs -O ^has_journal /dev/hdb1
```

루트로 다음과 같은 명령을 입력하여 파티션에 오류가 있는지 확인해 보시기 바랍니다:

```
/sbin/e2fsck -y /dev/hdb1
```

다음으로 ext2 파일 시스템으로 파티션을 마운트하기 위하여 다음 명령을 입력해 주십시오:

```
mount -t ext2 /dev/hdb1 /mount/point
```

위의 명령에서 */mount/point* 부분에 파티션의 마운트 지점을 입력해 주십시오

다음으로 파티션의 루트 레벨에 위치한 `.journal` 파일을 삭제하기 위하여 그 파일이 마운트된 디렉토리로 이동하신 후 다음과 같은 명령을 입력하십시오:

```
rm -f .journal
```

이제 다시 ext2 파티션이 생성되었습니다.

만일 파티션을 ext2 파일 시스템으로 영구적으로 변환하신다면, `/etc/fstab` 파일을 업데이트하는 것을 잊지 마십시오.

redhat.

2장 . 스왑 공간

2.1. 스왑 공간이란?

스왑 공간 *(Swap space)*이란 리눅스에서 물리적 메모리 (RAM)의 용량이 가득 차게될 경우 사용되는 여유 공간을 말합니다. 즉, 시스템이 처리하고 있는 데이터를 저장할 RAM이 충분하지 않을 때 스왑 공간에 이 데이터를 기록한다는 말입니다. 스왑 공간은 소량의 RAM을 사용하는 시스템에서는 도움이 되지만, RAM에 대한 대체로 여겨져서는 안됩니다. 스왑 공간은 하드 드라이브 상에 위치하기 때문에 물리적 메모리에 접근하는 것보다 접근 속도가 훨씬 느립니다.

스왑 공간은 스왑 파티션에 사용되거나 (권장 사항), 스왑 파일을 저장하는데 사용되며, 또는 스왑 파티션과 스왑 파일이 함께 스왑 공간을 차지하는 것도 가능합니다.

스왑 공간의 최소 크기는 사용자의 컴퓨터 RAM 용량의 두 배나, 32 MB가 되어야 하며, 이 중에 어느 용량이 크던지 간에 2048 MB (또는 2 GB)를 넘어서는 안됩니다.

2.2. 스왑 공간 추가하기

설치를 마친 후 스왑 공간의 크기를 추가해야할 경우가 있습니다. 예를 들어 시스템 RAM 용량을 64 MB에서 128 MB로 업그레이드하신다면 스왑 공간은 여전히 128 MB로 남아있게 됩니다. 이러한 경우 메모리 사용이 많은 작업이나 많은 용량의 메모리를 필요로 하는 응용 프로그램을 실행하실 경우를 대비하여 스왑 공간을 256 MB로 늘려주시는 것이 좋습니다.

스왑 공간을 늘리기 위한 다음과 같은 두가지 방법이 있습니다: 스왑 파티션 추가하기 또는 스왑 파일 추가하기. 스왑 파티션을 추가하는 방법을 권장하지만, 사용 가능한 여유 디스크 공간이 없을 경우 스왑 파티션을 추가하는 것이 쉽지 않습니다.

스왑 파티션을 추가하시려면 다음 단계를 따르십시오 (`/dev/hdb2`를 추가할 스왑 파티션으로 가정합니다):

1. 하드 드라이브를 사용 중지하셔야 합니다 (파티션은 마운트되지 않고 스왑 공간은 비활성화되어야 합니다). 이렇게 할 수 있는 가장 쉬운 방법은 시스템을 복구 모드로 부팅하는 것입니다. 복구 모드로 부팅하는 방법에 대한 정보를 원하신다면, 9 장을 참조하시기 바랍니다. 파일 시스템을 마운트 하도록 요청된다면, **생략** 버튼을 선택해 주십시오.

   다른 방법으로 만일 드라이브에 어떠한 파티션도 사용 중이지 않는 경우, 파티션들을 마운트 해제하신 후 `swapoff` 명령을 사용하여 하드 드라이브 상에서 스왑 공간을 비활성화하실 수 있습니다.

2. `parted` 또는 `fdisk`를 사용하여 스왑 파티션을 생성하시기 바랍니다. `parted` 사용이 `fdisk`를 사용하는 것보다 쉽습니다; 따라서 이 장에서는 `parted`에 대해서만 설명하겠습니다. `parted`를 사용하여 스왑 파티션을 생성하기 위해서는 다음 단계를 따르시기 바랍니다:

   - 쉘 프롬프트에 루트로 로그인 하신 후, `parted /dev/`*`hdb`* 명령을 입력해 주십시오. 이 명령에서 /dev/*hdb* 부분은 스왑 공간이 있는 하드 드라이브에 사용될 장치명을 의미합니다.
   - `(parted)` 프롬프트가 나타나면 **`print`** 명령을 입력하여 기존 파티션과 여유 공간 크기를 알아봅니다. 시작 값과 마지막 값은 메가바이트 단위로 나타납니다. 하드 드라이브 상의 여유 공간의 크기를 확인하신 후 새로운 스왑 파티션에 할당할 용량을 결정해 주십시오.
   - `(parted)` 프롬프트에서 **`mkpartfs`** ***`part-type`*** **`linux-swap`** ***`start end`*** 명령을 입력해 주십시오. 여기서 ***`part-type`*** 부분은 1차 파티션 (primary), 확장 파티션 (extended), 논리 파티션 (logical) 중 하나이며, ***`start`***와 ***`end`***는 파티션의 시작과 마지막 부분을 의미합니다.


경고

변경 사항은 즉시 적용됩니다; 따라서 명령을 입력하실 때 주의하시기 바랍니다.

- **quit** 명령을 입력하여 parted를 종료하십시오.

3. 이제 mkswap 명령을 사용하여 추가된 스왑 파티션을 설정해 주십시오. 쉘 프롬프트에 루트로 로그인하신 후 다음 명령을 입력하시기 바랍니다:
   mkswap /dev/hdb2
4. 다음 명령을 입력하여 스왑 파티션을 즉시 활성화합니다:
   swapon /dev/hdb2
5. 시스템 부팅시 스왑 파티션을 활성화하기 위해서는, /etc/fstab 파일에 다음과 같은 라인을 추가하시기 바랍니다:
   /dev/hdb2 swap swap defaults 0 0

   다음에 시스템 부팅시 새로운 스왑 파티션이 활성화됩니다.
6. 새로운 스왑 파티션을 추가하고 활성화하셨다면, cat /proc/swaps 명령이나 free 명령을 실행하여 출력된 결과를 살펴보시고 새로운 스왑 파티션이 활성화되었는지 여부를 확인해 주십시오.

스왑 파일을 추가하시려면:

1. 새로운 스왑 파일의 크기를 알아내신 후 1024를 곱하여 블록 크기를 계산해 주십시오. 예를 들어, 64 MB 스왑 파일의 블록 크기는 65536 입니다.
2. 쉘 프롬프트에서 루트로 다음 명령을 입력해 주십시오 (count 다음에는 원하시는 블록 크기를 입력하시기 바랍니다):
   dd if=/dev/zero of=/swapfile bs=1024 count=65536
3. 다음 명령을 사용하여 스왑 파일을 설정합니다:
   mkswap /swapfile
4. 스왑 파일을 즉시 활성화하시려면 다음 명령을 입력해 주십시오:
   swapon /swapfile
5. 시스템 부팅시 스왑 파일을 활성화하시려면, /etc/fstab 파일에 다음과 같은 라인을 추가하시기 바랍니다:
   /swapfile swap swap defaults 0 0

   다음에 시스템 부팅시 새로운 스왑 파일이 활성화됩니다.
6. 새로운 스왑 파일을 추가하고 활성화하셨다면, cat /proc/swaps 명령이나 free 명령을 실행하여 출력된 결과를 살펴보시고 새로운 스왑 파일이 활성화되었는지 여부를 확인해 주십시오.

2.3. 스왑 공간 삭제하기

스왑 파티션을 삭제하기 위해서는:

1. 하드 드라이브 사용을 중지하셔야 합니다 (파티션은 마운트되지 않고 스왑 공간은 비활성화되어야 합니다). 이렇게 할 수 있는 가장 쉬운 방법은 시스템을 복구 모드로 부팅하는 것입니다. 복구 모드로 부팅하는 방법에 대한 정보를 원하신다면, 9 장을 참조하시기 바랍니다. 파일 시스템을 마운트 하도록 요청된다면, **생략** 버튼을 선택해 주십시오.

   다른 방법으로 만일 드라이브에 어떠한 파티션도 사용 중이지 않는 경우, 파티션들을 마운트 해제하신 후 swapoff 명령을 사용하여 하드 드라이브 상에서 스왑 공간을 비활성화하실 수 있습니다.
2. 쉘 프롬프트에 루트로 로그인하신 후 다음 명령을 입력하여 스왑 파티션을 비활성화합니다 (다음에서 /dev/hdb2는 스왑 파티션입니다):
   swapoff /dev/hdb2

3. /etc/fstab 파일에서 삭제할 스왑 파티션 항목을 삭제해 주십시오.
4. parted 또는 fdisk를 사용하여 스왑 파티션을 제거합니다. 이 장에서는 parted에 대해서만 설명하겠습니다. parted를 사용하여 스왑 파티션을 제거하기 위해서는 다음 단계를 따르시기 바랍니다::
   - 쉘 프롬프트에 루트로 로그인 하신 후, parted /dev/*hdb* 명령을 입력해 주십시오. 이 명령에서 /dev/*hdb* 부분은 여유 공간이 있는 하드 드라이브에 사용될 장치명을 의미합니다.
   - (parted) 프롬프트가 나타나면 **print** 명령을 입력하여 기존 파티션의 크기를 알아보신 후 삭제할 스왑 파티션의 minor 번호를 결정해 주십시오.
   - (parted) 프롬프트에서 **rm *MINOR*** 명령을 입력해 주십시오. 여기서 *MINOR* 부분에는 삭제할 파티션의 minor 번호를 입력하시면 됩니다.

     경고

     한번 입력하시면 변경 사항이 즉시 적용됩니다; 따라서 올바른 minor 번호를 주의하여 입력하시기 바랍니다.
   - **quit** 명령을 입력하여 parted를 종료하십시오.

스왑 파일을 삭제하기 위해서는:

1. 쉘 프롬프트에서 스왑 파일을 비활성화하기 위해 다음 명령을 입력해 주십시오 (다음 명령에서 /swapfile에는 삭제할 스왑 파일명을 입력하시기 바랍니다):
   ```
   swapoff /swapfile
   ```
2. /etc/fstab 파일에서 삭제할 스왑 파티션 항목을 삭제해 주십시오.
3. 실제 파일을 삭제하십시오:
   ```
   rm /swapfile
   ```

2.4. 스왑 공간 이동하기

스왑 공간을 한 장소에서 다른 위치로 이동시키기 위해서는, 앞에서 설명된 방법에 따라서 스왑 공간을 삭제하신 후 새로운 장소에서 다시 새로운 스왑 공간을 생성하시기 바랍니다.

Redundant Array of Independent Disks (RAID)

3.1. RAID란?

RAID란 한개의 크고 비싼 드라이브로는 얻을 수 없는 성능이나 안정성을 이루기 위하여 여러 개의 작고, 값싼 디스크 드라이브를 묶어 하나의 저장 장치처럼 사용하는 기술을 말합니다. 여러 개의 물리적인 하드 디스크를 운영체제에서 하나의 논리 디스크로 인식하게 됩니다.

RAID는 디스크 스트라이핑 *(striping)* (RAID 레벨 0), 디스크 미러링 *(mirroring)* (RAID 레벨 1), 패리티 추가 디스크 스트라이핑 (RAID 레벨 5)과 같은 기술을 사용하여 정보를 여러 개의 하드 드라이브로 나눠 쓰고 읽어 들이는 방식입니다. 따라서 하나의 하드 디스크만 사용할 때보다 훨씬 빠른 입출력 속도를 가지게 되며 하드 디스크가 고장이 났을 경우에도 손쉽게 복구할 수 있습니다.

RAID의 기본 개념은 동일한 방식으로 하드 디스크 여러 대를 병렬 방식으로 구성하는 것입니다. 이렇게 하기 위해서는 데이터를 일정한 크기 (여러 다른 크기가 사용되지만, 일반적으로 32K 또는 64K)의 조각으로 나누어야 합니다. 각각의 조각은 사용된 RAID 레벨에 따라서 RAID에서 여러 개의 하드 디스크로 나누어서 기록됩니다. 데이터를 읽을 때는 여러 하드 디스크에 분산된 데이터를 마치 한개의 큰 하드 디스크에서 읽어오는 것처럼 동시에 읽어오게 됩니다.

3.2. RAID를 사용하는 이유는?

RAID 기술은 시스템 관리자와 같이 대량의 데이터를 관리하시는 분들에게 유용합니다. RAID를 사용하는 중요한 이유는 다음과 같습니다:

- 빠른 입출력 속도
- 하나의 가상 디스크를 사용함으로서 저장 공간을 확대
- 디스크가 고장날 경우 데이터가 손실될 가능성을 줄임

3.3. 하드웨어 RAID 대 소프트웨어 RAID

RAID에는 두가지 종류 (하드웨어 RAID와 소프트웨어 RAID)가 있습니다.

3.3.1. 하드웨어 RAID

하드웨어-기반 시스템은 호스트에서 RAID 하부 시스템을 독립적으로 관리하며, 호스트에는 RAID 어레이를 하나의 디스크로 나타냅니다.

하드웨어 RAID 장치의 한 예로서 SCSI 제어 장치에 연결되어 RAID 어레이를 단독 SCSI 드라이브처럼 나타내는 장치가 있습니다. 외부 RAID 시스템은 데이터를 저장하는 모든 RAID를 외부 디스크 하부 시스템에 위치한 한개의 컨트롤러로 이동시킵니다. 따라서 일반 SCSI 컨트롤러를 통해 호스트로 연결된 전체 하부 시스템은 호스트에서 하나의 디스크로 보여집니다.

RAID 컨트롤러는 카드 형식으로도 판매되며, 이 카드는 운영 체제에서는 SCSI 컨트롤러처럼 작동하지만 실제로는 스스로 모든 드라이브 통신을 처리합니다. 이러한 카드를 구입하신 경우, 여러분은 SCSI 컨트롤러와 마찬가지로 드라이브를 RAID 컨트롤러에 꽂으신 후 드라이브를 RAID 컨트롤러의 설정에 추가시키면, 운영 체제는 그 차이를 절대로 인식하지 못합니다.

3.3.2. 소프트웨어 RAID

소프트웨어 RAID는 커널 디스크 (블록 장치) 코드로 다양한 RAID 레벨을 실현합니다. 소프트웨어 RAID는 비싼 디스크 컨트롤러 카드나 핫-스왑 새시 (hot-swap chassis)[1]를 사용하지 않기 때문에 가장 저렴한 솔루션을 제공합니다. 최신 CPU의 성능이 점점 빨라지면서, 소프트웨어 RAID의 성능이 하드웨어 RAID의 성능을 능가하게 되었습니다.

Linux 커널에 있는 MD 드라이버는 완전히 하드웨어 독립적인 RAID 솔루션의 한 예입니다. 소프트웨어 기반 어레이의 성능은 서버 CPU의 성능과 로드에 의해 좌우됩니다.

Red Hat Linux 설치 프로그램으로 소프트웨어 RAID를 설정하는 방법과 관련된 정보를 원하신다면, 10 장을 참조하시기 바랍니다.

소프트웨어 RAID의 기능에 대해 더 알고 싶으시다면, 다음에 나온 가장 중요한 기능에 대한 간략한 목록을 살펴보시기 바랍니다:

- 스레드 재설정 프로세스
- 커널 기반 설정
- Linux 시스템 간에 어레이를 재설정할 필요가 없이 이동할 수 있는 기능
- 유휴 시스템 자원을 사용한 백그라운드 어레이 재생
- 즉시 백업 가능한 (Hot-swappable) 드라이브 지원
- 특정 CPU 최적화를 위한 자동 CPU 감지 기능

3.4. RAID 레벨과 선형 (Linear) 지원

RAID는 레벨 0, 1, 4, 5와 선형을 포함하는 다양한 설정을 지원합니다. 이러한 RAID 유형은 다음과 같이 정의되었습니다:

- 레벨 *0* — 일반적으로 "스트라이핑(striping)"이라고 불리는 방식으로 동일한 하드 디스크 여러 대를 병렬 방식으로 구성하는 기술 (striped data mapping)입니다. 이 방식은 어레이에 기록된 데이터를 여러 개의 디스크에 나누어서 쓰고 읽어 들임으로서, 데이터를 중복해서 기록하지 않기 때문에 가장 높은 입출력 성능을 제공합니다. 레벨 0 어레이의 저장 능력은 하드웨어 RAID의 전체 디스크의 총 용량이나 소프트웨어 RAID의 총 파티션 용량과 동일합니다.
- 레벨 *1* — "미러링(mirroring)"으로도 불리는 RAID 레벨 1은 가장 오래동안 사용된 RAID 방식입니다. 레벨 1은 하나의 데이터를 모든 하드 디스크에 똑같이 저장해 복사본을 만들어 놓습니다. 미러링은 읽기 성능이 뛰어나고 작업이 단순한 덕분에 여전히 자주 사용되는 방식입니다. 레벨 1은 데이터를 읽어올 때는 데이터 전송율을 높이기 위하여 여러 하드 디스크에서 동시에 나눠서 데이터를 읽어오지만, 일반적으로는 독립적으로 운영되어 높은 데이터 입/출력 처리를 제공합니다. 레벨 1은 다른 한 개의 디스크가 손상되더라도 자료를 쉽게 복구할 수 있으며 읽기 성능이 보다 향상된다는 장점이 있지만, 비교적 높은 비용이 든다는 단점이 있습니다.[2] 레벨 1 어레이의 저장 능력은 하드웨어 RAID 안의 복사된 (mirrored) 하드 디스크 중 한개의 용량이나 소프트웨어 RAID의 복사된 파티션 중 한개의 용량과 동일합니다.
- 레벨 *4* — 레벨 4는 데이터를 보호하기 위하여 단독 디스크 드라이브 상에 집중된 패리티(parity)[3]를 사용합니다. 레벨 4는 큰 파일 전송하기 보다는 입/출력 처리하는 데 더욱 적합합니다. 그 이유는 쓰기가 많은

1. 핫-스왑 새시 (hot-swap chassis)는 시스템의 전원을 끄지 않고도 하드 드라이브를 제거할 수 있도록 해줍니다.
2. RAID 레벨 1에 높은 비용이 드는 이유는 동일한 정보를 어레이 내의 모든 디스크에 기록함으로서 디스크 공간을 낭비하기 때문입니다. 예를 들어, 루트 (/) 파티션이 두개의 40G 드라이브 상에 존재하도록 RAID 레벨 1을 설정하신다면, 총 80G 중에서 40G만 사용하시는 것이 됩니다. 나머지 40G은 첫번째 40G의 복사본(mirror)으로 작동합니다.
3. 패리티는 파일 정보를 저장하는데 사용되고, 하나의 디스크에 오류가 났을 때, 남은 디스크의 데이터는 파손된 디스크의 데이터를 복구하는데 사용됩니다. 이렇게 재생된 데이터는 파손된 디스크가 교체되기 이전의 입/출력 요구를 만족시키고 교체된 이후 파손된 디스크를 다시 채우는데 사용됩니다.

시스템에서 매번 패리티 디스크를 사용해야 하기 때문에 병목 현상이 일어날 수 있으며, 재기록 캐싱 (write-back caching)과 같은 기술이 반드시 함께 사용되어야 합니다. 비록 RAID 레벨 4는 일부 RAID 파티션 분할 스키마에서 옵션으로 선택되기도 하지만, Red Hat Linux RAID 설치 옵션에는 포함되지 않습니다. [4] 하드웨어 RAID 레벨 4의 저장 용량은 총 디스크 저장 용량에서 한개의 디스크의 용량을 뺀 것과 같습니다. 소프트웨어 RAID 레벨 4의 저장 용량은 모든 파티션이 동일한 크기일 경우 총 파티션의 저장 용량에서 한개 파티션의 용량을 뺀 것과 같습니다.

- 레벨 5 — RAID 유형 중에서 가장 흔하게 사용되는 방식입니다. RAID 레벨 5는 어레이의 각 디스크 마다 패리티를 저장시킴으로써 RAID 레벨 4의 병목 현상을 피할 수 있습니다. 그러나 여전히 쓰기 전에 패리티 연산을 해야하기 때문에 쓰기 성능은 미러링만큼 빨라질 수 없지만, 최신 CPU와 소프트웨어 RAID를 사용하면 그리 큰 문제가 안됩니다. 레벨 4를 사용하시면 읽기 성능이 쓰기 성능 보다 훨씬 뛰어난 비대칭적인 성능을 갖게 되지만, 레벨 5는 이러한 비대칭을 줄이기 위하여 재기록 캐싱 기능과 함께 사용됩니다. 하드웨어 RAID 레벨 5의 저장 용량은 총 디스크 용량에서 한개의 디스크의 용량을 뺀 것과 같습니다. 소트웨어 RAID 레벨 5의 저장 용량은 모든 파티션 크기가 동일한 경우 총 파티션 용량에서 한개 파티션의 용량을 뺀 것과 같습니다.
- 선형 *RAID* — 선형 RAID는 여러 개의 드라이브들을 연결해 하나의 큰 가상 디스크를 만드는 것입니다. 선형 RAID에서 첫번째 드라이브가 완전히 채워지면 순차적으로 다음 드라이브에 데이터를 저장합니다. 이러한 방식은 여러 개의 디스크가 아닌 한개의 디스크에서 입/출력 작업을 실행하므로, 성능 면에서는 별다른 장점이 없습니다. 선형 RAID는 또한 하나의 디스크에 오류가 나면, 묶여있는 파티션 전체에 오류가 나기 때문에 실제로 안정성을 저하시킵니다. 선형 RAID의 용량은 모든 디스크의 총량과 같습니다.

4. RAID 레벨 4는 RAID 레벨 5와 동일한 용량의 공간을 차지하지만, 레벨 5에 비해 장점이 없습니다. 따라서 레벨 4는 지원되지 않습니다.

4장 .

논리 볼륨 관리자 (LVM)

Red Hat Linux 8.0 부터, 논리 볼륨 관리자 (LVM)를 사용하여 하드 브라이브를 구성할 수 있습니다.

LVM은 Logical Volume Manager의 약자로서 하드 드라이브를 파티션 대신 논리 볼륨으로 할당하여, 여러 개의 디스크를 좀더 효율적이고 유연하게 관리할 수 있는 방식을 말합니다.

LVM을 사용하여 여러 개의 하드 드라이브를 모아서 한개나 그 이상의 물리적 볼륨 *(physical volumes)*을 구성할 수 있습니다. 한개의 물리적 볼륨은 한 개 이상의 드라이브에 걸쳐서 작성될 수 없습니다.

/boot 파티션을 제외한 모든 물리적 볼륨은 논리 볼륨 그룹 *(logical volume groups)*을 구성합니다. 부트로더가 논리 볼륨 그룹을 읽을 수 없기 때문에 /boot 파티션은 논리 볼륨 그룹에 위치할 수 없습니다. 만일 루트 / 파티션을 논리 볼륨에 놓기를 원하신다면, 볼륨 그룹에 속하지 않는 별개의 /boot 파티션을 생성하셔야 합니다.

앞에서 언급되었듯이 한개의 물리적 볼륨은 한 개 이상의 드라이브에 걸쳐서 작성될 수 없기 때문에, 만일 한 개 이상의 드라이브에 논리 볼륨 그룹을 작성하시려면, 드라이브 당 한개 이상의 물리적 볼륨을 생성하셔야 합니다.

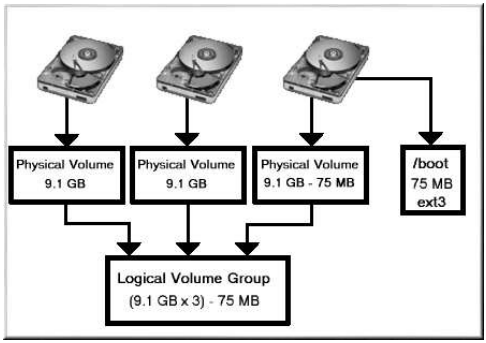

그림 4-1. 논리 볼륨 그룹

논리 볼륨 그룹은 여러 개의 논리 볼륨으로 나뉘어지며 이 논리 볼륨에는 마운트 지점 (예, /home 과 /)과 파일 시스템 유형 (예, ext3)이 부여됩니다. 예를 들어, 파티션의 용량이 가득차게 되면, 논리 볼륨 그룹으로부터 여유 공간을 가져와 논리 볼륨으로 추가하여 그 파티션의 용량을 확장시켜 줍니다. 새로운 하드 드라이브를 운영 체제에 추가시키면, 이 하드 드라이브는 논리 볼륨 그룹과 확장 가능한 파티션인 논리 볼륨으로 추가됩니다.

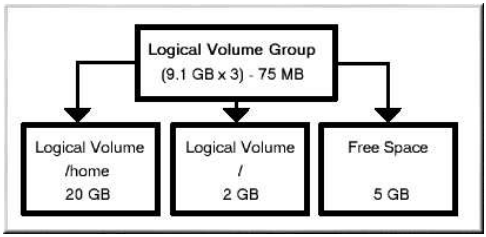

그림 4-2. 논리 볼륨

반면에 ext3 파일 시스템으로 파티션된 시스템에서는 하드 드라이브가 일정한 크기의 파티션으로 분할됩니다. 따라서 파티션의 용량이 가득차게 되어도 파티션의 크기를 확장하기가 쉽지 않습니다. 만일 그 파티션을 다른 하드 드라이브로 이동시킨다고 해도 원래 하드 드라이브 공간은 다른 파티션으로 재할당되거나 사용되지 않게 됩니다.

커널에서 LVM이 들어가 동작을 가능하도록 커널을 설정하고 컴파일 해주셔야 합니다. Red Hat Linux 9의 기본 커널은 LVM을 지원하도록 컴파일되었습니다.

Red Hat Linux를 설치하는 과정에서 LVM을 설정하는 방법에 대한 정보를 원하신다면, 11 장을 참조하시기 바랍니다.

redhat.

5장 .

디스크 공간 관리

Red Hat Linux 시스템 설치를 마치신 후, 기존 파티션 테이블을 살펴보고, 파티션 크기를 변경하고 삭제하거나, 여유 공간이나 추가 하드 드라이버에서 파티션을 추가해야할 경우가 있습니다. parted는 이러한 작업을 쉽게 수행할 수 있게 돕는 유틸리티입니다. 이 장에서는 parted를 사용하여 파일 시스템 작업을 수행하는 방법에 대하여 설명해 보겠습니다. fdisk를 사용하여 파티션의 크기를 변경하는 작업을 제외한 대부분의 작업을 수행하실 수도 있습니다. fdisk와 관련된 보다 많은 정보를 원하신다면, fdisk의 메뉴얼 페이지나 정보 페이지를 참조하시기 바랍니다.

시스템의 디스크 공간 사용량을 알아보고 감시하는 방법에 대해 알고 싶으시면, 26.3 절을 참조하시기 바랍니다.

parted 유틸리티를 사용하기 위해서는 parted 패키지가 설치되어 있어야 합니다. parted를 시작하시려면, 쉘 프롬프트에 루트로 로그인하신 후 parted */dev/hdb* 명령을 입력해 주십시오. 여기서 */dev/hdb*는 설정하시려는 드라이브에 사용되는 장치명입니다. (parted) 프롬프트가 나타나면 help를 입력하여 사용 가능한 명령어 목록을 보실 수 있습니다.

파티션을 생성, 삭제 또는 재조정하기 위해서는, 시스템을 복구 모드로 부팅하여 장치를 사용 중지하셔야 합니다. (파티션은 마운트되지 않고 스왑 공간은 비활성화 되어야 합니다). 복구 모드로 부팅하는 방법에 대한 설명을 원하신다면, 9 장을 참조하시기 바랍니다. 파일 시스템을 마운트 하도록 요청된다면, **생략** 버튼을 선택해 주십시오.

드라이브 상에서 파티션이 사용되지 않는다면, umount 명령을 사용하여 그 파티션을 마운트 해제하신 후 swapoff 명령을 이용하여 하드 드라이브 상의 모든 스왑 공간을 비활성화 시켜주십시오.

표 5-1은 자주 사용되는 parted 명령어 목록입니다. 다음 부분에서는 일부 자주 사용되는 명령어에 대하여 보다 자세하게 다루어 보도록 하겠습니다.

명령어	설명
check *minor-num*	파일 시스템에 대한 간단한 확인 작업을 수행합니다.
cp *from to*	파일 시스템을 한 파티션에서 다른 파티션으로 복사합니다; *from*과 *to*는 파티션의 minor 번호를 의미합니다.
help	사용 가능한 명령어 목록을 보여줍니다.
mklabel *label*	파티션 테이블에 대한 디스크 레이블을 생성합니다.
mkfs *minor-num file-system-type*	*file-system-type* 유형의 파일 시스템을 생성합니다.
mkpart *part-type fs-type start-mb end-mb*	새로운 파일 시스템을 생성하지 않고 파티션을 만듭니다.
mkpartfs *part-type fs-type start-mb end-mb*	파티션을 만들고 특정 파일 시스템을 생성합니다.
move *minor-num start-mb end-mb*	파티션을 이동합니다.
print	파티션 테이블을 보여줍니다.
quit	parted를 종료합니다.
resize *minor-num start-mb end-mb*	파티션의 크기를 *start-mb*에서 *end-mb*로 재조정합니다.

명령어	설명
`rm` *`minor-num`*	파티션을 삭제합니다.
`select` *`device`*	설정할 다른 장치를 선택합니다.
`set` *`minor-num flag state`*	파티션 상에 플래그(flag)를 설정합니다; *`state`*는 on(켜짐) 이나 off(꺼짐) 중 하나를 입력합니다.

표 5-1. `parted` 명령어

5.1. 파티션 테이블 보기

`parted`를 시작 후 다음 명령을 입력하여 파티션 테이블을 볼 수 있습니다:

```
print
```

다음과 같은 파티션 테이블이 나타날 것입니다:

```
Disk geometry for /dev/hda: 0.000-9765.492 megabytes
Disk label type: msdos
Minor  Start   End  Type   Filesystem Flags
1    0.031  101.975 primary ext3   boot
2   101.975  611.850 primary linux-swap
3   611.851  760.891 primary ext3
4   760.891 9758.232 extended      lba
5   760.922 9758.232 logical ext3
```

이 목록의 첫번째 줄은 디스크의 용량을 보여주며, 두번째 줄에서는 디스크 레이블 유형을 보여줍니다. 세번째 줄 아래로는 파티션 테이블이 나타납니다. 이 파티션 테이블을 보시면, **Minor** 번호는 파티션 번호를 의미합니다. 예를 들어 minor 번호 1을 가진 파티션은 `/dev/hda1`에 상응합니다. **Start**와 **End** 값은 메가바이트 단위로 나타납니다. **Type**은 파티션 유형으로서 일차 파티션 (primary), 확장 파티션 (extended), 논리 파티션 (logical) 중 한가지로 선택됩니다. 다섯번째 행인 **Filesystem**은 파일 시스템 유형을 나타내며 ext2, ext3, FAT, hfs, jfs, linux-swap, ntfs, reiserfs, hp-ufs, sun-ufs, xfs와 같은 유형이 존재합니다. 그 다음 **Flags** 행은 파티션에 설정된 플래그 (flag)를 나타내며, 사용 가능한 플래그 종류에는 boot, root, swap, hidden, raid, lvm, lba가 있습니다.

힌트

`parted`를 시작하지 않고 다른 장치를 선택하기 위해서는, `select` 명령과 장치명 (예, `/dev/hdb`)을 사용하시면 됩니다. 명령을 입력하신 후 파티션 테이블을 보거나 설정하실 수 있습니다.

5.2. 파티션 생성하기

경고

사용 중인 장치에 파티션을 생성하지 마십시오.

파티션을 생성하시기 전에 복구 모드로 부팅하셔야 합니다. (또는 장치 상 모든 파티션을 마운트 해제하신 후 모든 스왑 공간을 비활성화하셔야 합니다).

다음 명령을 사용하여 `parted`를 시작합니다. 다음 명령에서 /dev/*hda*는 파티션이 생성될 장치입니다:

```
parted /dev/hda
```

현재 파티션 테이블에 충분한 여유 공간이 있는지 확인하시기 바랍니다:

```
print
```

만일 여유 공간이 충분하지 않다면, 기존 파티션의 크기를 재조정하실 수 있습니다. 보다 자세한 사항은 5.4 절을 참조하시기 바랍니다.

5.2.1. 파티션 만들기

파티션 테이블에서 새로운 파티션의 시작 지점과 끝나는 지점 및 파티션 유형을 확인해 주십시오. 한 장치에는 최대한 4개의 (확장 파티션이 없는) 1차 파티션을 놓을 수 있습니다. 만일 4개 이상의 파티션이 필요한 경우에는 3개의 1차 파티션, 1개의 확장 파티션 및 그 확장 파티션 내에서 여러 개의 논리 파티션을 만드실 수 있습니다. 디스크 파티션에 대한 기본적인 정보를 원하신다면, *Red Hat Linux* 설치 가이드의 부록편에서 디스크 파티션 소개 부분을 참조하시기 바랍니다.

예를 들어 하드 드라이브 상에 1024 메가바이트 부터 2048 메가바이트에 이르는 ext3 파일 시스템을 갖춘 1차 파티션을 생성하기 위해서는, 다음과 같은 명령을 입력하시면 됩니다:

```
mkpart primary ext3 1024 2048
```

힌트

위의 명령에서 `mkpartfs` 명령을 대신 사용하신다면, 파일 시스템은 파티션이 생성된 이후에 만들어질 것입니다. 하지만 `parted` 명령은 ext3 파일 시스템 생성을 지원하지 않습니다. 따라서 ext3 파일 시스템을 생성하기 위해서는, 우선 `mkpart` 명령을 사용하여 파티션을 만드신 후 `mkfs` 명령을 사용하여 ext3 파일 시스템을 생성하시기 바랍니다. `mkfs` 사용법은 다음 부분에서 설명됩니다. `mkpartfs`는 linux-swap 유형의 파일 시스템에서 작동합니다.

[Enter] 키를 누르는 즉시 변경 사항이 적용되므로, 명령을 주의깊게 살펴보신 후 실행해 주십시오.

파티션을 생성하신 후 `print` 명령을 사용하여 파티션 테이블에서 새로운 파티션이 올바른 파티션 유형, 파일 시스템 유형 및 파티션 크기를 갖추고 있는지 확인하시기 바랍니다. 또한 새 파티션에 레이블을 생성하기 위해 그 파티션의 부 번호 (minor number)를 기억해 주십시오. 또한

```
cat /proc/partitions
```

명령어의 출력 결과를 보시고 커널이 새로운 파티션을 인식하는지 여부를 확인하시기 바랍니다.

5.2.2. 파티션 포맷하기

새로 생성된 파티션은 아직 파일 시스템을 갖추고 있지 않습니다. 이제 다음 명령을 사용하여 파일 시스템을 생성하시기 바랍니다:

```
/sbin/mkfs -t ext3 /dev/hdb3
```

경고

파티션을 포맷하시면 현재 파티션 상에 저장된 모든 자료가 삭제될 것입니다.

5.2.3. 파티션 이름 붙이기 (labeling)

다음 단계는 파티션에 이름을 붙이는 것입니다. 예를 들어 새 파티션 /dev/hda3를 /work로 이름 붙이시려면 다음과 같이 입력하시면 됩니다:

```
e2label /dev/hda3 /work
```

기본 값으로 Red Hat Linux 설치 프로그램은 파티션이 고유한 이름을 갖도록 파티션의 마운트 지점을 이름으로 사용합니다. 하지만 여러분이 원하시는 이름으로 변경하실 수 있습니다.

5.2.4. 마운트 지점 생성하기

마운트 지점을 생성하기 위해서는, 루트로 로그인하신 후 다음 명령을 입력하십시오:

```
mkdir /work
```

5.2.5. /etc/fstab에 추가하기

루트로 /etc/fstab 파일에 다음과 같은 줄을 추가합니다:

```
LABEL=/work     /work       ext3  defaults    1 2
```

첫번째 행에서는 LABEL= 다음에 여러분이 파티션에 부여할 이름을 입력하셔야 합니다. 다음 행은 새로운 파티션에 사용될 마운트 지점과 3번째 행에는 파일 유형 (예, ext3 또는 swap)을 입력해 주십시오. 이 파일과 관련된 보다 많은 정보가 필요하시면, man fstab 명령을 입력하여 메뉴얼 페이지를 참조하시기 바랍니다.

만일 4번째 행에 defaults라고 입력된다면, 이 파티션은 부팅시 마운트될 것입니다. 재부팅하지 않고 즉시 파티션을 마운트하시려면, 루트로 다음 명령을 입력하시면 됩니다:

```
mount /work
```

5.3. 파티션 제거하기

경고

사용 중인 장치에 위치한 파티션을 삭제하지 마십시오.

파티션을 삭제하시기 전에 복구 모드로 부팅하셔야 합니다. (또는 장치 상 모든 파티션을 마운트 해제하신 후 모든 스왑 공간을 비활성화하셔야 합니다).

다음 명령을 사용하여 parted를 시작합니다. 다음 명령에서 /dev/*hda*는 파티션을 삭제할 장치입니다:

```
parted /dev/hda
```

현재 파티션 테이블에서 삭제할 파티션의 minor 번호를 확인하십시오:

```
print
```

rm 명령을 사용하여 파티션을 삭제합니다. 예로 들면, minor 번호 3을 가진 파티션을 삭제하시려면, 다음과 같이 입력합니다:

```
rm 3
```

[Enter] 키를 누르는 즉시 변경 사항이 적용되므로, 명령을 주의깊게 살펴보신 후 실행해 주십시오.

파티션을 삭제하신 후 `print` 명령을 사용하여 파티션 테이블에서 해당 파티션이 삭제되었는지를 확인하시기 바랍니다. 또한

```
cat /proc/partitions
```

명령어의 출력 결과를 보시고 커널이 해당 파티션이 삭제된 것을 인식하는지 확인해 주십시오.

파티션 삭제의 마지막 단계는 `/etc/fstab` 파일에서 해당 파티션을 삭제하는 것입니다. 삭제된 파티션을 선언하는 라인을 찾아서 삭제하십시오.

5.4. 파티션 크기 재조정하기

경고

사용 중인 장치에 위치한 파티션의 크기를 재조정하지 마십시오.

파티션의 크기를 재조정하시기 전에 복구 모드로 부팅하셔야 합니다. (또는 장치 상 모든 파티션을 마운트 해제하신 후 모든 스왑 공간을 비활성화하셔야 합니다).

다음 명령을 사용하여 `parted`를 시작합니다. 다음 명령에서 /dev/*hda*는 파티션의 크기를 재조정할 장치를 의미합니다:

```
parted /dev/hda
```

현재 파티션 테이블에서 크기를 재조정할 파티션의 시작 지점과 마지막 지점을 비롯하여 크기를 재조정할 파티션의 minor 번호를 확인하십시오:

```
print
```

경고

현재 사용중인 파티션의 공간 보다 큰 용량으로 크기를 조절할 수 없습니다.

파티션의 크기를 재조정하기 위해 `resize` 다음에 파티션의 부 번호, 시작 지점 (메가바이트 단위), 마지막 지점 (메가바이트 단위)를 입력해 주십시오. 예:

```
resize 3 1024 2048
```

파티션의 크기를 조절하신 후 `print` 명령을 사용하여 파티션의 크기가 제대로 조절되었는지, 올바른 파일 유형과 파일 시스템 유형을 갖추고 있는지 여부를 확인해 주십시오.

시스템을 일반 모드로 부팅하신 후 `df` 명령을 실행하여 그 파티션이 새로운 용량으로 마운트 되어있는지 다시 확인해 보시기 바랍니다.

6장 . 디스크 사용량 할당하기

시스템 상에서 사용되는 디스크 사용량을 감시하는 것 뿐만 아니라 (26.3.1 절 참조), 사용자가 너무 많은 디스크 용량을 사용하거나 파티션이 차게되면 시스템 관리자에게 보고되도록 디스크 사용량을 제한 설정할 수 있습니다.

디스크 사용량 할당은 개별 사용자를 비롯한 사용자 그룹 별로 설정 가능합니다. 따라서 개별 사용자에게는 "개인용" 파일을 저장할 수 있는 적은 사용량을 할당하는 반면, 그룹 프로젝트와 같은 큰 용량이 필요한 프로젝트에는 보다 많은 디스크 사용량을 주는 것이 가능합니다.

추가로, 디스크 사용량 할당은 디스크 블록수를 제한할 뿐만 아니라 사용 가능한 inode의 수를 제한하는데도 사용됩니다. inode는 보통 파일 관련 정보를 담고 있기 때문에, inode의 수를 제한함으로서 생성 가능한 파일수를 제어할 수 있게 됩니다.

디스크 사용량 할당을 실행하기 위해서는 `quota` RPM이 설치되어 있어야 합니다. RPM 패키지를 설치하는 방법에 대한 보다 자세한 정보는 V 부을 참조하시기 바랍니다.

6.1. 디스크 사용량 제한 설정하기

디스크 사용량을 할당하시려면, 다음과 같은 과정을 따르시기 바랍니다:

1. 파일 시스템 당 디스크 사용량 제한을 사용하도록 `/etc/fstab` 파일을 수정하십시오.
2. 파일 시스템(들)을 다시 마운트합니다.
3. 디스크 사용량 할당 파일 (quota file)을 만드신 후 디스크 사용량 표를 생성하시기 바랍니다.
4. 디스크 사용량을 할당합니다.

다음 부분에서는 앞에서 언급된 과정을 보다 자세하게 설명해 보겠습니다.

6.1.1. 디스크 사용량 할당 활성화하기

루트 사용자로 로그인하신 후, 원하시는 텍스트 편집기를 사용하여 디스크 사용량 제한이 필요한 파일 시스템에 `usrquota` 와/또는 `grpquota` 옵션을 첨가하십시오:

```
LABEL=/     /       ext3  defaults    1 1
LABEL=/boot   /boot     ext3  defaults    1 2
none      /dev/pts    devpts gid=5,mode=620 0 0
LABEL=/home   /home     ext3  defaults,usrquota,grpquota 1 2
none      /proc     proc  defaults    0 0
none      /dev/shm    tmpfs  defaults    0 0
/dev/hda2    swap     swap  defaults    0 0
/dev/cdrom    /mnt/cdrom   udf,iso9660 noauto,owner,kudzu,ro 0 0
/dev/fd0    /mnt/floppy  auto  noauto,owner,kudzu 0 0
```

이 예시에서 `/home` 파일 시스템은 사용자와 그룹에 디스크 사용량을 할당하고 있습니다.

6.1.2. 파일 시스템 재마운트하기

`userquota` 옵션과 `grpquota` 옵션을 첨가하신 후, `fstab` 항목이 수정된 각 파일 시스템을 재마운트하시기 바랍니다. 만일 그 파일 시스템이 어떠한 프로세스에서도 사용되지 않고 있다면, `umount` 명령을 입력하신 후 `mount` 명령을 사용하여 파일 시스템을 재마운트하시면 됩니다. 만일 그 파일 시스템이 현재 사용 중인 경우, 파일 시스템을 재마운트할 수 있는 가장 쉬운 방법은 시스템을 재부팅하는 것입니다.

6.1.3. 디스크 사용량 할당 파일 만들기

디스크 사용량 할당이 활성화된 모든 파일 시스템이 재마운트 되었다면, 이 시스템은 이제 할당된 디스크 용량을 가지고 작업이 가능합니다. 그러나 파일 시스템 자체는 디스크 사용량 할당을 지원할 수 있는 준비가 되지 않았습니다. 다음 단계로 quotacheck 명령을 실행하셔야 합니다.

quotacheck 명령은 사용량이 할당된 파일 시스템을 검사한 후 파일 시스템 당 현재 디스크 사용량을 보여주는 표를 작성합니다. 이렇게 작성된 표는 운영 체제의 디스크 용량표를 업데이트하는데 사용됩니다. 추가로 파일 시스템의 디스크 사용량 할당 파일이 업데이트됩니다.

파일 시스템 상에서 디스크 사용량 할당 파일 (aquota.user 파일과 aquota.group 파일)을 생성하시려면, quotacheck 명령과 함께 -c 옵션을 사용하시기 바랍니다. 예를 들어, /home 파티션에 사용자 디스크 할당과 그룹 디스크 할당이 활성화 되었다면, /home 디렉토리에 할당 파일을 생성하셔야 합니다:

```
quotacheck -acug /home
```

-a 옵션은 /etc/mtab 파일에서 마운트된 비 NFS 파일 시스템에서 디스크 사용량 할당이 활성화되었는지 확인합니다. -c 옵션은 디스크 사용량 할당을 사용하는 각 파일 시스템에 할당 파일을 생성하도록 지정합니다. -g 옵션은 그룹 디스크 사용량 할당이 사용되는지 확인하는데 사용됩니다.

만일 -u 옵션과 -g 옵션이 지정되지 않았다면, 사용자 사용량 할당 파일만 생성됩니다. -g 옵션만 지정된 경우에는, 그룹 사용량 할당 파일만 만들어 집니다.

파일이 생성된 후, 다음과 같은 명령을 실행하여 사용량 할당이 활성화된 파일 시스템마다 현재 디스크 사용량을 보여주는 표를 생성하시기 바랍니다:

```
quotacheck -avug
```

이 명령에서 사용된 옵션들은 다음과 같습니다:

- a — 디스크 사용량 할당이 활성화되고, 로컬에서 마운트된 모든 파일 시스템을 확인합니다.
- v — 사용량 할당 확인 작업이 진행 과정을 상세한 상태 정보로 보여줍니다.
- u — 사용자 디스크 사용량 할당 정보를 체크합니다.
- g — 그룹 디스크 사용량 할당 정보를 체크합니다.

quotacheck이 실행되고 난 후, 디스크 사용량 할당을 사용하는 각 파일 시스템 (예, /home)에 대한 정보가 활성화된 (사용자와 그룹) 디스크 사용량 할당에 따른 할당 파일에 저장됩니다.

6.1.4. 사용자 당 디스크 사용량 할당하기

마지막 단계로서 edquota 명령을 사용하여 디스크 사용량을 할당해 주셔야 합니다.

개인 사용자 당 사용량 할당을 설정하시려면, 쉘 프롬프트에서 루트로 로그인 하신 후 다음과 같은 명령을 입력하십시오:

```
edquota username
```

디스크 사용량을 할당할 각 사용자마다 이 과정을 실행하시기 바랍니다. 예를 들어, 만일 /etc/fstab 파일에서 /home 파티션에 대한 사용량 할당이 활성화하신 후 edquota testuser 명령을 실행하신 경우, 시스템에 대한 디폴트로서 다음과 같은 정보가 편집기에 나타날 것입니다:

```
Disk quotas for user testuser (uid 501):
 Filesystem        blocks   soft   hard  inodes  soft  hard
 /dev/hda3         440436    0     0   37418    0    0
```

알림

edquota 명령은 EDITOR 환경 변수에서 정의된 텍스트 편집기를 사용합니다. 편집기를 바꾸시려면, EDITOR 환경 변수를 사용할 편집기의 완전 경로로 설정하시기 바랍니다.

첫번째 칸은 디스크 사용량이 할당된 파일 시스템의 이름입니다. 두번째 칸은 해당 사용자가 현재 사용중인 블록 수를 보여줍니다. 다음 두 칸은 제한에 근접한 사용자에게 경고하는데 사용되는 soft 제한과 절대적인 제한값인 hard 제한을 설정하는데 사용됩니다. inodes 칸은 현재 사용자가 사용중인 inode의 수를 보여줍니다. 마지막 두 칸은 파일 시스템 상의 사용자에 대한 soft inode 제한과 hard inode 제한을 설정하는데 사용됩니다.

엄격한 제한인 hard 제한은 사용자나 그룹이 사용할 수 있는 절대적인 최대 디스크 사용량을 의미합니다. 일단 제한량에 이르면, 더 이상 디스크 공간을 사용할 수 없게 됩니다.

soft 제한은 사용 가능한 최대 디스크 공간을 설정합니다. 그러나 hard 제한과는 달리, soft 제한은 정해진 시간 내에서 어느 정도 제한을 초과해도 괜찮습니다. 이러한 용량 초과 허가 기간을 허가 기간 *(grace period)*이라고 합니다. 이 허가 기간은 초, 분, 시, 일, 주 또는 월 단위로 표시할 수 있습니다.

0라고 설정된 값이 있다면, 제한이 설정되지 않은 것입니다. 텍스트 편집기를 사용하여 원하시는 제한 값으로 변경하시기 바랍니다. 예로 들면:

```
Disk quotas for user testuser (uid 501):
 Filesystem        blocks   soft   hard  inodes  soft  hard
 /dev/hda3         440436  500000  550000  37418   0    0
```

해당 사용자에 대한 디스크 사용량이 할당되었는지 확인해 보시려면, 다음 명령을 입력하십시오:

```
quota testuser
```

6.1.5. 그룹 당 디스크 사용량 할당하기

디스크 사용량은 또한 그룹 단위로 할당될 수 있습니다. 예를 들어, devel이라는 그룹에 그룹 디스크 사용량을 설정하시려면, 다음 명령을 사용하시면 됩니다 (그룹에 디스크 사용량을 할당하시기 전에 그 그룹이 이미 존재해야 합니다):

```
edquota -g devel
```

이 명령을 입력하시면 텍스트 편집기에서 해당 그룹에 대한 기존 디스크 사용량이 나타납니다:

```
Disk quotas for group devel (gid 505):
 Filesystem        blocks   soft   hard  inodes  soft  hard
 /dev/hda3         440400    0    0   37418   0    0
```

제한 사항을 수정하고 파일을 저장하신 후 디스크 사용량을 설정하십시오.

그룹 디스크 사용량이 설정되었는지 여부를 확인해 보시려면, 다음 명령을 사용하시기 바랍니다:

```
quota -g devel
```

6.1.6. 파일 시스템 당 디스크 사용량 할당하기

디스크 사용량 할당이 활성화된 각 파일 시스템 단위로 사용량을 할당하시려면, 다음 명령을 사용하시면 됩니다:

```
edquota -t
```

다른 edquota 명령처럼, 이 명령도 텍스트 편집기에서 파일 시스템에 대한 현재 디스크 사용량을 보여줍니다:

```
Grace period before enforcing soft limits for users:
Time units may be: days, hours, minutes, or seconds
 Filesystem      Block grace period   Inode grace period
 /dev/hda3          7days         7days
```

블록과 inode 제한 초과 허용 기간 (block gracec period)을 변경하시고 파일을 저장하신 후 텍스트 편집기를 종료하십시오.

6.2. 디스크 사용량 할당 관리하기

디스크 사용량을 할당한 후에는 사용량을 관리하는 작업이 남아 있습니다 — 디스크 사용량 제한이 초과하지 않는지와 제한값이 정확한지 등의 여부를 살펴보는 작업. 물론 사용자가 계속해서 사용량을 초과하거나 soft 제한을 초과하는 경우, 시스템 관리자는 사용자의 유형과 디스크 공간이 사용자의 작업에 미치는 영향을 고려하여 여러 가지 해결책을 찾을 수 있습니다. 사용자에게 어떻게 하면 보다 적은 디스크 공간을 사용하여 작업을 할 수 있을지를 알려주거나 필요하다면 사용자의 디스크 사용량을 늘려서 할당해주는 방법을 택할 수 있습니다.

6.2.1. 디스크 사용량 보고하기

repquota 유틸리티를 실행하여 디스크 사용량 리포트를 생성할 수 있습니다. 예를 들어 repquota /home 명령을 실행하시면, 다음과 같은 결과가 출력됩니다:

```
*** Report for user quotas on device /dev/hda3
Block grace time: 7days; Inode grace time: 7days
          Block limits       File limits
User     used  soft  hard grace  used soft hard grace
----------------------------------------------------------------------
root   --   36   0   0      4  0  0
tfox   --  540   0   0     125  0  0
testuser -- 440400 500000 550000    37418  0  0
```

디스크 할당을 사용하는 모든 파일 시스템에 대한 디스크 사용량 리포트를 보시려면, 다음 명령을 사용하시면 됩니다:

```
repquota -a
```

리포트는 읽기 쉽게 작성되었습니다. 하지만 몇가지 설명이 필요한 사항이 있습니다. 각 사용자명 다음에 표시된 --를 보시면 단번에 블록이나 inode 제한이 초과되었는지 여부를 알 수 있습니다. 만일 soft 제한이 초과되었다면, 그 공간에 - 대신 + 표시가 나타날 것입니다; 첫 - 기호는 불록 제한을 나타내며 두번째 기호는 inode 제한을 나타냅니다.

grace 칸은 보통 공백으로 남아 있습니다. 만일 soft 제한을 초과하게 되면, 이 칸에는 남아 있는 초과 허용 시간이 나타납니다. 만일 허용 시간이 만료된 경우, none이라고 표시됩니다.

6.2.2. 정확한 디스크 할당 사용량 지키기

파일 시스템이 제대로 마운트 해제되지 않았을 경우 (예, 시스템 고장), 반드시 quotacheck 명령을 실행하셔야 합니다. 시스템에 고장이 나지 않아도 정기적으로 quotacheck 명령을 실행 가능합니다. 이 명령을 정기적으로 실행함으로서 정확한 디스크 할당 사용량을 지킬 수 있습니다. (사용 가능한 옵션은 6.1.1 절에 설명되어 있습니다):

```
quotacheck -avug
```

명령을 정기적으로 실행할 수 있는 가장 쉬운 방법은 cron을 사용하는 것입니다. 루트로 로그인 하신 후, crontab -e 명령을 사용하여 quotacheck 명령이 정기적으로 실행되도록 설정하시거나 다음 중 한가지 디렉토리에 quotacheck를 실행하는 스크립트를 저장하셔도 됩니다 (원하시는 주기를 사용하여):

- /etc/cron.hourly
- /etc/cron.daily
- /etc/cron.weekly
- /etc/cron.monthly

파일 시스템이 사용 중이지 않을 때 분석한 정보가 가장 정확한 디스크 사용량 정보입니다. 따라서 cron 작업은 해당 파일 시스템이 가장 작동량이 작을 때 실행되는 시간에 작동하도록 계획되어야 합니다. 만일 디스크 사용량을 할당 받은 파일 시스템 마다 작업 시간이 다르다면, 여러 개의 cron 작업을 계획하여 다른 시간에 각 파일 시스템에 대한 quotacheck을 실행하도록 하십시오.

cron 설정에 대한 보다 많은 정보를 원하신다면, 28 장을 참조하시기 바랍니다.

6.2.3. 활성화와 비활성화

디스크 사용량 할당값을 0로 설정함으로서 할당을 비활성화할 수 있습니다. 모든 사용자와 그룹의 디스크 사용량 할당을 비활성화하시려면, 다음 명령을 사용하십시오:

```
quotaoff -vaug
```

만일 -u 옵션이나 -g 옵션이 지정되지 않는다면, 사용자 디스크 사용량 할당만이 비활성화 됩니다. -g 옵션만 지정된 경우에는 그룹 디스크 사용량 할당만이 비활성화 됩니다.

디스크 사용량 할당을 다시 활성화하시려면, 동일한 옵션을 가지고 quotaon 명령을 사용하시면 됩니다.

예를 들어, 모든 파일 시스템에 사용자와 그룹 디스크 사용량 할당을 활성화하시려면:

```
quotaon -vaug
```

/home과 같은 특정 파일 시스템에 대한 디스크 사용량 할당을 활성화하시려면:

```
quotaon -vug /home
```

만일 -u 옵션이나 -g 옵션이 지정되지 않는다면, 사용자 디스크 사용량 할당만이 활성화 됩니다. -g 옵션만 지정된 경우에는 그룹 디스크 사용량 할당만이 활성화 됩니다.

6.3. 추가 자료

디스크 사용량 할당에 대한 보다 많은 정보를 원하신다면, 다음 자료를 참조하시기 바랍니다.

6.3.1. 설치된 문서 자료

- quotacheck, edquota, repquota, quota, quotaon, quotaoff 메뉴얼 페이지

6.3.2. 관련 서적

- *Red Hat Linux* 시스템 관리 입문서 — http://www.redhat.com/docs 사이트와 문서 CD에서 찾으실 수 있습니다. 이 메뉴얼에는 초보 Red Hat Linux 시스템 관리자를 위한 디스크 사용량 할당을 포함한 저장 공간 관리에 대한 기본 정보가 포함되어 있습니다.

II. 설치-관련 정보

Red Hat Linux 설치 가이드는 Red Hat Linux 설치 과정과 설치 후 기본 문제 해결 방법에 대하여 설명하고 있습니다. 이 부분에서는 킥스타트 (자동 설치 기술), 시스템 복구 모드 (시스템이 정상적인 런레벨에서 부팅하지 못할 경우, 시스템을 부팅하는 방법), 설치 과정에서 RAID 설정 방법 및 LVM 설정 방법을 알려 드립니다. *Red Hat Linux* 설치 가이드와 이 부분을 함께 참조하여 고급 설치 작업을 수행해 보시기 바랍니다.

차례

7장 .

킥스타트 설치

7.1. 킥스타트 설치란?

많은 시스템 관리자들은 자동화된 설치 방식을 사용하여 Red Hat Linux를 설치하기를 선호하십니다. 이러한 요구에 대한 응답으로 Red Hat는 킥스타트 설치 방법을 창안하였습니다. 시스템 관리자는 킥스타트를 사용하여 일반적인 Red Hat Linux 설치 과정에서 요구되는 모든 질문에 대한 대답을 포함하는 단독 파일을 생성하실 수 있습니다.

킥스타트 파일은 단독 서버 시스템에 저장되어 설치 과정에서 개별 컴퓨터에 의해 읽혀집니다. 이러한 설치 방법은 단독 킥스타트 파일을 사용하여 여러 개의 컴퓨터 상에서 Red Hat Linux를 설치할 수 있도록 해줍니다. 따라서 네트워크 관리자와 시스템 관리자에게는 가장 이상적인 설치 방법이라고 할 수 있습니다.

킥스타트는 Red Hat Linux 설치를 자동화시켜 줍니다.

7.2. 킥스타트 설치 방법은?

로컬 CD-ROM, 로컬 하드 드라이브 또는 NFS, FTP, HTTP를 통하여 킥스타트 설치를 수행하실 수 있습니다.

킥스타트를 사용하시려면, 다음과 같은 작업을 수행하셔야 합니다:

1. 킥스타트 파일을 만드셔야 합니다.
2. 킥스타트 파일을 이용하여 부팅 디스켓을 만드시거나 네트워크 상에서 킥스타트 파일을 사용 가능하도록 합니다.
3. 설치 트리를 사용 가능하게 합니다.
4. 킥스타트 설치를 시작합니다.

이 장에서는 앞에서 언급된 과정에 대하여 자세히 설명하고 있습니다.

7.3. 킥스타트 파일 만들기

킥스타트 파일은 단순한 텍스트 파일로서 키워드로 식별되는 항목의 목록을 포함하고 있습니다. 킥스타트 파일을 만드시려면, Red Hat Linux 문서 CD의 `RH-DOCS` 디렉토리에서 `sample.ks` 파일을 복사하여 만드시거나 또는 처음부터 다시 작성하는 방법도 있습니다. 또한 Red Hat Linux 설치 프로그램도 여러분이 설치 과정에서 선택하신 옵션에 기초하여 샘플 킥스타트 파일을 생성합니다. 이 샘플 파일은 `/root/anaconda-ks.cfg`에 기록되어 있습니다. 이 파일을 편집하시려면 텍스트 편집기나 ASCII 텍스트로 파일을 저장할 수 있는 워드 프로세서를 사용하시면 됩니다.

우선적으로 킥스타트 파일을 생성하실 때 다음과 같은 사항에 주의해 주십시오:

- 킥스타트 내의 섹션은 반드시 순서대로 지정하셔야 합니다. 섹션 내의 항목들은 특별한 이유가 없는 한 순서대로 지정될 필요는 없습니다. 섹션의 순서는 다음과 같습니다:
  - 명령어 섹션 — 킥스타트 옵션 목록을 보시려면 7.4 절을 참조하십시오. 필수 옵션을 반드시 포함시켜야 합니다.
  - `%packages` 섹션 — 자세한 사항은 7.5 절을 참조하시기 바랍니다.
  - `%pre` 와 `%post` 섹션 — 이 두 섹션은 반드시 순서대로 지정되지 않아도 상관없습니다. 자세한 사항은 7.6 절 와 7.7 절을 참조하시기 바랍니다.

- 필수가 아닌 항목들은 생략 가능합니다.
- 필수 항목을 생략하시면 설치 프로그램은 전형적인 설치 과정에서와 마찬가지로 사용자에게 관련 항목에 대한 대답을 요청할 것입니다. 일단 대답을 입력하시면, (또 다른 생략된 항목이 발견되지 않는다면) 설치를 계속 진행할 것입니다.
- 우물정자 기호 (#)로 시작하는 줄은 주석으로 취급되어 무시됩니다.
- 킥스타트 업그레이드를 위해서는 다음의 항목들을 반드시 지정해 주셔야 합니다:
  - 언어
  - 언어 지원
  - 설치 방법
  - 장치 규격 (설치를 수행하는데 장치가 필요한 경우)
  - 키보드 설정
  - `upgrade` 키워드
  - 부트로더 설정

  만일 그 외 다른 항목이 업그레이드를 위하여 지정되었다면, 이러한 항목은 무시될 것입니다. (여기에는 패키지 선택도 포함된다는 것을 주목해 주십시오)

7.4. 킥스타트 옵션

다음에 나온 옵션들을 킥스타트 파일에 지정하실 수 있습니다. 그래픽 인터페이스를 사용하여 킥스타트 파일을 생성하시려면, **킥스타트 설정 프로그램 (Kickstart Configurator)**을 사용하십시오. 보다 자세한 사항을 원하시면, 8 장을 참조하시기 바랍니다.

알림

만일 옵션 다음에 등호 (=)가 온다면, 그 등호 다음에 값을 지정해 주셔야 합니다. 예시 명령어에서, ([]) 안에 지정된 옵션은 명령에 대한 선택적인 인수를 의미합니다.

`autostep` (선택 사항)

‘ `interactive`와 유사하지만 단지 여러분을 위해서 다음 화면으로 이동한다는 차이점이 있습니다. 주로 디버깅 목적으로 사용됩니다.

`auth` 또는 `authconfig` (필수)

‘ 시스템에서 사용될 인증 옵션을 설정합니다. 이것은 설치 후 실행할 수 있는 `authconfig` 명령과 유사합니다. 디폴트 값으로 암호는 일반적으로 섀도우 (shadowed)되지 않고 암호화됩니다.

`--enablemd5`

‘ 사용자 암호에 md5 암호화를 사용합니다.

`--enablenis`

‘ NIS 지원을 작동합니다. 디폴트 값으로, `--enablenis` 명령은 네트워크 상에서 발견되는 첫번째 도메인을 사용합니다. 따라서 여러분은 항상 `--nisdomain` 옵션을 통하여 직접 도메인을 설정해 주셔야 합니다.

`--nisdomain=`

‘ NIS 서비스를 위해 사용할 NIS 도메인명.

`--nisserver=`

‘ NIS 서비스에 사용될 서버 (디폴트 값으로, 브로드캐스트합니다)

`--useshadow` 또는 `--enableshadow`

‘ 섀도우 암호를 사용합니다.

`--enableldap`

‘ `/etc/nsswitch.conf` 파일에서 LDAP 지원을 작동시켜서, LDAP 디렉토리에서 사용자에 대한 정보 (UID, 홈 디렉토리, 쉘 등)을 검색할 수 있도록 해줍니다. 이 옵션을 사용하시려면, `nss_ldap` 패키지를 설치하셔야 합니다. 여러분은 또한 `--ldapserver=` 와 `--ldapbasedn=` 명령어를 사용하여 서버와 베이스(base) DN을 지정해 주셔야 합니다.

`--enableldapauth`

‘ LDAP를 인증 방식으로 사용합니다. 이 옵션은 인증과 암호를 변경하는데 LDAP 디렉토리를 사용하는 `pam_ldap` 모듈을 사용합니다. 이 옵션을 사용하기 위해서는 `nss_ldap` 패키지를 설치하셔야 합니다. 또한 `--ldapserver=` 와 `--ldapbasedn=` 명령어를 사용하여 서버와 베이스(base) DN을 지정하셔야 합니다.

`--ldapserver=`

‘ `--enableldap`이나 `--enableldapauth` 중 한 옵션을 이미 지정하셨다면, 이 옵션을 사용하여 사용할 LDAP 서버의 이름을 지정하십시오. 이 옵션은 `/etc/ldap.conf` 파일에 설정됩니다.

`--ldapbasedn=`

‘ 만일 `--enableldap`이나 `--enableldapauth` 중 한 옵션을 이미 지정하셨다면, 이 옵션을 사용하여 사용자 정보가 저장된 LDAP 디렉토리 목차의 DN (distinguished name의 줄임말)을 지정하십시오. 이 옵션은 `/etc/ldap.conf` 파일에 설정되어 있습니다.

`--enableldaptls`

‘ TLS (전송 계층 보안 - Transport Layer Security) 검색을 사용합니다. 이 옵션은 LDAP가 인증 전에 LDAP 서버로 암호화된 사용자명과 암호를 보내도록 해줍니다.

`--enablekrb5`

‘ 사용자 인증을 위해 Kerberos 5를 사용합니다. Kerberos 자체는 홈 디렉토리, UID 와 쉘에 대하여 알지 못합니다. 따라서 Kerberos를 사용하신다면, LDAP, NIS나 Hesiod를 사용하시거나 `/usr/sbin/useradd` 명령어를 사용하여 사용자 계정에 대한 정보를 알려주셔야 합니다. 이 옵션을 사용하신다면, `pam_krb5` 패키지를 설치하셔야 합니다.

`--krb5realm=`

‘ 여러분의 웍스테이션이 속한 Kerberos 5 영역.

`--krb5kdc=`

‘ 커베로스 5 영역에 대한 서버 요구를 수행하는 KDC (또는 여러 개의 KDC). 만일 영역 내에 여러 개의 KDC가 있다면, 콤마 (,)를 사용하여 구분합니다.

`--krb5adminserver=`

‘ 여러분의 영역 안에 있으면서 kadmind를 실행 중인 KDC. 이 서버는 암호 변경과 그 외 다른 관리 요청을 처리합니다. KDC가 여러 개인 경우, 이 서버는 마스터 KDC 상에서 운영되어야 합니다.

`--enablehesiod`

‘ 사용자 홈 디렉토리, UID와 쉘을 검색하기 위하여 Hesiod 지원을 사용합니다. Hesiod를 설정하고 네트워크 상에서 Hesiod를 사용하는 방법과 관련된 보다 많은 정보를 원하신다면, `glibc` 패키지에 포함된 `/usr/share/doc/glibc-2.x.x/README.hesiod`을 참조하시기 바랍니다. Hesiod는 사용자, 그룹과 그 외 다른 다양한 항목들에 대한 정보를 저장하기 위하여 DNS 레코드를 사용하는 DNS의 확장입니다.

`--hesiodlhs`

‘ Hesiod LHS ("left-hand side"의 줄임말) 옵션으로서 `/etc/hesiod.conf` 파일에 설정되어 있습니다. 이 옵션은 Hesiod 라이브러리가 DNS 정보를 찾을 때 DNS 검색명을 결정하기 위해 사용됩니다 (LDAP가 베이스 DN을 사용하는 방식과 유사).

`--hesiodrhs`

‘ Hesiod RHS ("right-hand side"의 줄임말) 옵션으로서 `/etc/hesiod.conf` 파일에 설정되어 있습니다. 이 옵션은 Hesiod 라이브러리가 정보를 찾을 때 DNS 검색명을 결정하기 위해 사용됩니다 (LDAP가 베이스 DN을 사용하는 방식과 유사).

힌트

"jim"에 대한 사용자 정보를 검색하기 위해서 Hesiod 라이브러리는 jim의 passwd 엔트리 (`jim:*:501:501:Jungle Jim:/home/jim:/bin/bash`)와 비슷하게 보이는 TXT 레코드에 따라 결정되는 *jim.passwd<LHS><RHS>*을 검색합니다. 그룹의 경우에도 *jim.group<LHS><RHS>*이 사용된다는 것을 제외하고는 상황이 동일합니다.

사용자와 그룹을 숫자로 검색하는 것은 "jim.passwd"에 대한 CNAME을 "501.uid"로 만들고 "jim.group"에 대한 CNAME을 "501.gid"로 만드는 방식으로 처리됩니다. LHS와 RHS는 항상 마침표로 시작하기 때문에 라이브러리가 검색할 이름을 결정할 때는 LHS와 RHS 이름 앞에 마침표 [.]를 사용하지 않는다는 점에 주의해 주십시오.

`--enablesmbauth`

‘ SMB 서버 (전형적으로 Samba 또는 Windows 서버)에 대한 사용자 인증을 사용합니다. SMB 자체는 사용자 홈 디렉토리, UID 와 쉘에 대하여 알지 못합니다. 따라서 SMB 인증을 사용하신다면, LDAP, NIS나 Hesiod를 사용하시거나 `/usr/sbin/useradd` 명령어를 사용하여 사용자 계정에 대한 정보를 알려주셔야 합니다. 이 옵션을 사용하시려면, `pam_smb` 패키지를 설치하셔야 합니다.

`--smbservers=`

‘ SMB 인증에 사용되는 서버의 이름. 한개 이상의 서버를 지정하시려면, 콤마 (,)를 사용하여 구분하시면 됩니다.

`--smbworkgroup=`

‘ SMB 서버에 사용되는 작업그룹의 이름.

`--enablecache`

‘ `nscd` 서비스를 사용합니다. `nscd` 서비스는 사용자, 그룹에 대한 정보와 다양한 다른 유형의 정보를 캐시 저장합니다. NIS, LDAP이나 hesiod를 사용하여 네트워크 상에서 사용자와 그룹에 대한 정보를 배포하실 경우, 캐싱 (caching)을 사용하시면 특히 유용합니다.

`bootloader` (필수)

‘ 부트로더를 설치하는 방법과 그 부트로더가 LILO 혹은 GRUB이 될 것인지의 여부를 지정합니다. 이 옵션은 설치와 업그레이드에서 필수입니다. 업그레이드 과정에서 현재 LILO를 사용하고 계시는 경우

`--useLilo` 옵션이 지정하지 않으신다면, 부트로더는 GRUB으로 변경됩니다. 업그레이드 과정에서 LILO를 계속 보존하시려면, `bootloader --upgrade` 옵션을 사용하시기 바랍니다.

`--append=`

‘ 커널 매개 변수를 지정합니다. 여러 개의 변수를 지정하시려면, 다음과 같이 변수들을 빈 공간으로 구별하시면 됩니다:
`bootloader --location=mbr --append="hdd=ide-scsi ide=nodma"`

`--location=`

‘ 부트 레코드가 기록될 장소를 지정합니다. 다음과 같은 장소를 입력 가능합니다: **`mbr`** (기본), **`partition`** (커널을 포함하는 파티션의 첫번째 섹터에 부트로더를 설치합니다), 또는 **`none`** (부트로더를 설치하지 않음).

`--password=`

‘ GRUB을 사용하시는 경우, 이 옵션을 사용하여 GRUB 부트로더 암호를 설정하실 수 있습니다. 이 옵션은 임의 커널 옵션이 전달되는 GRUB 쉘로의 접근을 제한하기 위하여 사용됩니다.

`--md5pass=`

‘ GRUB을 사용하시는 경우, 이미 암호가 암호화되었다는 점을 제외하면 `--password=`와 유사합니다.

`--useLilo`

‘ GRUB 대신 LILO를 부트로더로 사용합니다.

`--linear`

‘ LILO를 사용하신다면, `linear` LILO 옵션을 사용하십시오; 이 옵션은 이전 버전 호환을 위해서만 사용됩니다. (linear는 이제 디폴트로 사용됩니다).

`--nolinear`

‘ LILO를 사용하시는 경우, `nolinear` LILO 옵션을 사용하십시오; linear는 디폴트입니다.

`--lba32`

‘ LILO를 사용하는 경우, 자동 검색 대신 lba32 모드로 사용합니다.

`--upgrade`

‘ 기존 부트로더의 엔트리를 보존하면서 설정을 업그레이드합니다. 이 옵션은 업그레이드에서만 사용됩니다.

`clearpart` (선택 사항)

‘ 새로운 파티션을 생성하기 전에 시스템 상의 파티션을 제거합니다. 디폴트 값으로, 파티션은 제거되지 않습니다.

알림

`clearpart` 명령을 사용하시면, 논리 파티션 상에서 `--onpart` 명령을 사용하실 수 없습니다.

`--linux`

‘ 모든 Linux 파티션을 삭제합니다.

`--all`

‘ 시스템에서 모든 파티션을 삭제합니다.

`--drives=`

‘ 파티션을 삭제할 드라이브를 지정합니다. 예를 들어, 다음 명령을 입력하시면 일차 IDE 제어기 상에서 첫 두 개의 드라이브 상에 존재한 파티션이 삭제될 것입니다:
`clearpart --drives hda,hdb`

`--initlabel`

‘ 컴퓨터의 구조에 맞는 디폴트로 디스크 레이블을 초기화합니다 (예, x86의 경우 `msdos`으로, Itanium이라면 `gpt`). 이 옵션을 사용하시면 설치 프로그램이 새로운 하드 드라이브에 설치할 때 디스크 레이블을 초기화할 것인지 여부를 묻지 않기 때문에 유용합니다.

`device` (선택 사항)

‘ 대부분의 PCI 시스템 상에서 설치 프로그램은 적절한 이더넷과 SCSI 카드를 자동 검색하지만, 일부 PCI 시스템과 오래된 시스템 상에서는, 킥스타트가 적절한 장치를 찾을 수 있도록 힌트를 제공해 주셔야 합니다. 설치 프로그램이 벌도의 모듈을 설치하도록 지시하는 `device` 명령은 다음과 같은 형식으로 사용됩니다:
`device` <*`type`*> <*`moduleName`*> `--opts=`<*`options`*>

<*`type`*>

‘ `scsi` 이나 `eth`로 대체해 주십시오.

<*`moduleName`*>

‘ 설치될 커널 모듈 이름으로 바꿔주십시오.

`--opts=`

‘ 커널 모듈에 전달될 옵션들. 여러 개의 옵션을 따옴표로 묶어 함께 전달할 수 있습니다. 예로 들면:
`--opts="aic152x=0x340 io=11"`

`deviceprobe` (선택 사항)

‘ PCI 버스를 검색하며, 만일 모듈이 사용 가능하다면 찾아낸 모든 장치에 사용될 모듈을 로드합니다.

`driverdisk` (선택 사항)

‘ 킥스타트 설치 과정에서 드라이버 디스크를 사용하실 수 있습니다. 드라이버 디스크의 내용을 시스템의 하드 드라이브 상에 위치한 파티션의 루트 디렉토리로 복사하셔야 합니다. 그 후 `driverdisk` 명령어를 사용하여 설치 프로그램에게 드라이버 디스크를 찾을 장소를 지시해 주십시오.
`driverdisk` <*`partition`*> [`--type=`<*`fstype`*>]

<*`partition`*>

‘ 드라이버 디스크를 포함하고 있는 파티션을 의미합니다.

`--type=`

‘ 파일 시스템 유형 (예, vfat 또는 ext2).

`firewall` (선택 사항)

‘ 설치 프로그램에서 **방화벽 설정** 화면에 상응하는 옵션입니다:
`firewall` <*securitylevel*> `[--trust=]` <*incoming*> `[--port=]`

<*securitylevel*>

‘ 아래의 보안 수준 중 하나를 선택해 주십시오:

- `--high`
- `--medium`
- `--disabled`

`--trust=`

‘ 이곳에 장치 (예, eth0)를 기입하시면, 그 장치로부터의 트래픽은 모두 방화벽을 통과할 수 있도록 허용됩니다. 장치를 한 개 이상 기입하시려면, `--trust eth0 --trust eth1` 형식으로 사용하시면 됩니다. 절대로 `--trust eth0, eth1`와 같이 콤마로 구분된 형식을 사용하시면 안됩니다.

<*incoming*>

‘ 특정 서비스의 방화벽 통과를 허용하시려면 다음과 같은 옵션을 사용하십시오.

- `--dhcp`
- `--ssh`
- `--telnet`
- `--smtp`
- `--http`
- `--ftp`

`--port=`

‘ 포트:프로토콜 형식을 사용하여 방화벽을 통과할 수 있는 포트를 지정하실 수 있습니다. 예를 들어 IMAP의 방화벽 통과를 허용하시려면, `imap:tcp`라고 지정하시면 됩니다. 또는 숫자 포트를 지정하는 것도 가능합니다; 예를 들어, 포트 1234에 UDP 패킷을 허용하려면 `1234:udp`로 지정하시면 됩니다. 여러 개의 포트를 지정하시려면, 콤마로 구분하십시오.

`install` (선택 사항)

‘ 시스템에게 기존 시스템을 업그레이드하는 대신 새로운 시스템을 설치하도록 지시합니다. 설치 모드가 기본 모드입니다. 설치를 위해서는 `cdrom`, `harddrive`, `nfs`, (ftp 또는 http 설치시) `url` 중 한가지 설치 유형을 지정해 주셔야 합니다. `install` 명령과 설치 방식 명령은 반드시 같은 줄에 입력하셔야 합니다.

`cdrom`

‘ 첫번째 CD-ROM 드라이브를 사용하여 설치하기.

`harddrive`

‘ vfat 또는 ext2인 로컬 드라이브 상에서 Red Hat 설치 트리를 사용하여 설치하기.

- `--partition=`

  설치에 사용될 파티션 (예, sdb2)

- `--dir=`

  `RedHat` 설치 트리를 포함하고 있는 디렉토리.

예로 들면:

```
harddrive --partition=hdb2 --dir=/tmp/install-tree
```

`nfs`

‘ 지정된 NFS 서버에서 설치하기.

- `--server=`

  설치에 사용될 서버 (호스트명 또는 IP)

- `--dir=`

  `RedHat` 설치 트리를 포함하고 있는 디렉토리.

예로 들면:

```
nfs --server=nfsserver.example.com --dir=/tmp/install-tree
```

`url`

‘ FTP나 HTTP를 통하여 원격 서버 상에 위치하는 설치 트리로부터 설치하기.

예로 들면:

```
url --url http://<server>/<dir>
```

or:

```
url --url ftp://<username>:<password>@<server>/<dir>
```

`interactive` (선택 사항)

‘ 설치 과정에서 킥스타트 파일에 제공된 정보를 사용하지만, 주어진 값을 조사하고 수정할 수 있도록 허용합니다. 설치 프로그램의 각각의 화면에서 킥스타트 파일에서 주어진 값을 나타납니다. **다음** 버튼을 클릭하여 주어진 값을 받아들이거나, 또는 값을 변경하신 후 **다음** 버튼을 클릭하여 설치를 계속 진행합니다. `autostep` 부분도 참조해 주십시오.

`keyboard` (필수)

‘ 시스템의 키보드 유형을 설정합니다. i386, Itanium, Alpha 컴퓨터에서 사용 가능한 키보드의 유형은 다음과 같습니다:

```
be-latin1, bg, br-abnt2, cf, cz-lat2, cz-us-qwertz, de,
de-latin1, de-latin1-nodeadkeys, dk, dk-latin1, dvorak, es, et,
fi, fi-latin1, fr, fr-latin0, fr-latin1, fr-pc, fr_CH, fr_CH-latin1,
gr, hu, hu101, is-latin1, it, it-ibm, it2, jp106, la-latin1, mk-utf,
no, no-latin1, pl, pt-latin1, ro_win, ru, ru-cp1251, ru-ms, ru1, ru2,
ru_win, se-latin1, sg, sg-latin1, sk-qwerty, slovene, speakup,
speakup-lt, sv-latin1, sg, sg-latin1, sk-querty, slovene, trq, ua,
uk, us, us-acentos
```

`/usr/lib/python2.2/site-packages/rhpl/keyboard_models.py` 파일에도 이 목록이 포함되어 있으며, 이 파일은 `rhpl` 패키지의 일부입니다.

`lang` (필수)

‘ 설치 과정에서 사용할 언어를 설정합니다. 예를 들어 언어를 영어로 설정하시려면, 킥스타트 파일에 다음과 같은 라인을 첨가하십시오:
`lang en_US`

`/usr/share/redhat-config-language/locale-list` 파일은 각 줄의 첫 행에서 유효한 언어 코드 목록을 제공합니다. 이 파일은 `redhat-config-languages` 패키지의 일부입니다.

`langsupport` (필수)

‘ 설치할 언어를 설정합니다. `lang` 명령과 함께 사용하신 언어 코드를 `langsupport` 명령과 함께 사용하실 수 있습니다.

한가지 언어만 설치하시려면, 그 언어를 지정해 주십시오. 예를 들어, 불어를 설치하여 사용하시려면 불어 코드인 `fr_FR`를 사용합니다:
`langsupport fr_FR`

`--default=`

‘ 한 개 이상의 언어에 대한 언어 지원을 설치하시려면, 기본 언어를 지정해 주셔야 합니다.

예를 들어, 영어와 불어를 설치하신 후 영어를 기본 언어로 사용하시려면 다음의 명령을 사용하시기 바랍니다:
`langsupport --default=en_US fr_FR`

만일 `--default` 명령에 한 개의 언어만 지정하시면, 모든 언어가 설치될 것이며 지정된 언어는 기본으로 설정됩니다.

`lilo` (`bootloader`로 대체되었습니다.)

‘


주의

이 옵션은 `bootloader` 명령으로 대체되었으며 이전 버전에서만 호환 가능합니다. `bootloader`를 참조하시기 바랍니다.

시스템 상에서 부트로더를 설치하는 방법을 지정합니다. 디폴트 값으로, LILO는 MBR의 첫번째 디스크 상에 설치되며, 만일 DOS 파티션이 발견된다면 다중-부트 시스템을 설치합니다. (`LILO:` 프롬프트에서 **`dos`**를 입력하시면 DOS/Windows 시스템이 부팅됩니다).

`--append <`*`params`*`>`

‘ 커널 매개 변수를 지정합니다.

`--linear`

‘ `linear` LILO 옵션을 사용합니다; 이 옵션은 오직 이전 버전에만 호환성을 지니며 linear는 이제 디폴트로 사용됩니다.

`--nolinear`

‘ `nolinear` LILO 옵션을 사용합니다; linear는 이제 디폴트로 사용됩니다.

`--location=`

‘ LILO 부트 레코드가 기록될 위치를 지정합니다. 기록 가능한 위치는 다음과 같습니다: **`mbr`** (기본), **`partition`** (커널을 포함하는 파티션의 첫번째 섹터에 부트로더를 설치합니다). 만일 아무런 위치도 지정되지 않는다면, LILO가 설치되지 않습니다.

`--lba32`

‘ 자동 검색 기능 대신 lba32 모드로 사용합니다.

`lilocheck` (선택 사항)

‘ `lilocheck` 옵션이 사용된다면, 설치 프로그램은 첫번째 하드 드라이브의 MBR 상의 LILO를 검사하여 만일 LILO가 발견되면 시스템을 재부팅 합니다. — 이러한 경우에는 킥스타트가 이미 설치된 시스템을 재설치하는 것을 방지하기 위하여 설치가 실행되지 않습니다.

`logvol` (선택 사항)

‘ 다음과 같은 구문을 사용하여 논리 볼륨 관리 (LVM)에 사용될 논리 볼륨을 생성합니다:
`logvol` *`mountpoint`* `--vgname=`*`name`* `--size=`*`size`* `--name=`*`name`*

파티션을 먼저 생성하신 후, 논리 볼륨 그룹을 생성하시고, 그 후 논리 볼륨을 생성합니다. 예로 들면:
```
part pv.01 --size 3000
volgroup myvg pv.01
logvol / --vgname=myvg --size=2000 --name=rootvol
```

`mouse` (필수)

‘ GUI 모드와 텍스트 모드로 마우스를 설정합니다. 다음과 같은 옵션을 사용하실 수 있습니다:

`--device=`

‘ 마우스가 위치하는 장치 (예, `--device=ttyS0`).

`--emulthree`

‘ 이 옵션을 사용하시면, 마우스의 왼쪽 버튼과 오른쪽 버튼을 동시에 클릭하는 것을 마치 3 버튼 마우스의 가운데 마우스 버튼을 클릭하는 것처럼 인식합니다. 2 버튼 마우스를 사용하시는 경우, 이 옵션을 사용하셔야 합니다.

옵션을 설정하신 후 다음 중 한가지 마우스 유형을 지정해 주십시오:
`alpsps/2`, `ascii`, `asciips/2`, `atibm`, `generic`, `generic3`, `genericps/2`, `generic3ps/2`, `genericwheelps/2`, `genericusb`, `generic3usb`, `genericwheelusb`, `geniusnm`, `geniusnmps/2`, `geniusprops/2`, `geniusscrollps/2`, `geniusscrollps/2+`,

`thinking`, `thinkingps/2`, `logitech`, `logitechcc`, `logibm`, `logimman`, `logimmanps/2`, `logimman+`, `logimman+ps/2`, `logimmusb`, `microsoft`, `msnew`, `msintelli`, `msintellips/2`, `msintelliusb`, `msbm`, `mousesystems`, `mmseries`, `mmhittab`, `sun`, `none`

`/usr/lib/python2.2/site-packages/rhpl/mouse.py` 파일에서도 이 목록을 찾으실 수 있습니다. 이 파일은 `rhpl` 패키지의 일부입니다.

만일 마우스 명령이 인수가 없이 주어졌거나 생략되었다면, 설치 프로그램은 마우스를 자동 검색을 시도할 것입니다. 대부분의 최신형 마우스는 자동 검색됩니다.

`network` (선택 사항)

‘ 네트워크 정보를 설정합니다. 만일 킥스타트 설치가 네트워킹을 필요로하지 않는다면 (즉 NFS, HTTP, FTP를 통해 설치되지 않았다면), 네트워킹은 시스템에서 설정되지 않습니다. 만일 설치 과정에서 네트워킹을 필요로하지 않고 네트워크 정보가 킥스타트 파일에 제공되지 않았다면, Red Hat Linux 설치 프로그램은 동적 IP 주소 (BOOTP/DHCP)를 통하여 eth0 상에서 설치되었다고 가정하고, 마지막으로 설치된 프로그램을 설정하여 동적으로 IP 주소를 결정합니다. `network` 옵션은 네트워크를 통한 킥스타트 설치를 비롯하여 설치된 시스템에 필요한 네트워크 정보를 설정합니다.

`--bootproto=`

‘ `dhcp`, `bootp`, `static` 중 하나를 선택해 주십시오.

`dhcp`가 기본이며 `bootp`와 `dhcp`는 동일하게 취급됩니다.

DHCP 방식은 DHCP 서버 시스템을 사용하여 네트워킹 설정을 획득합니다. 짐작하시듯이 BOOTP 방식도 DHCP 방식과 유사하며, BOOTP 서버를 사용하여 네트워킹 설정을 얻습니다. 시스템이 DHCP를 사용하도록 설정하시려면, 다음과 같이 입력하십시오:

```
network --bootproto=dhcp
```

시스템이 BOOTP를 사용하여 네트워크 설정을 획득하도록 지시하시려면, 킥스타트 파일에서 다음과 같은 라인을 사용합니다:

```
network --bootproto=bootp
```

정적 방식을 사용하시면, 여러분이 직접 필요한 모든 네트워킹 정보를 킥스타트 파일에 입력해 주셔야 합니다. 정적 방식이라는 이름에서 알 수 있듯이, 입력하신 정보는 정적으로서 설치 과정이나 설치 이후에 사용됩니다. 여러분은 한 줄안에 모든 네트워크 설정 정보를 입력하셔야 하기 때문에, 정적 네트워킹에 사용되는 줄은 더욱 복잡합니다. 다음의 예에서 처럼 IP 주소, 넷마스크, 게이트웨이와 네임 서버를 지정해 주십시오 (역 슬래시 (\) 기호는 한 줄을 의미합니다):

```
network --bootproto=static --ip=10.0.2.15 --netmask=255.255.255.0 \
--gateway=10.0.2.254 --nameserver=10.0.2.1
```

정적 방식을 사용하신다면 다음과 같은 두가지 제한 사항에 주의해 주십시오:

- 모든 정적 네트워킹 설정 정보는 반드시 한 줄로 지정되어야 합니다; 예를 들어, 역 슬래쉬 (\)를 사용하여 여러 줄을 한 줄로 감쌀 수 없습니다.
- 오직 한 개의 네임 서버만 지정하실 수 있습니다. 하지만 만일 필요하다면 킥스타트 파일의 `%post` 섹션을 (7.7 절 참조) 사용하여 더 많은 네임 서버를 추가하실 수 있습니다.

`--device=`

‘ 설치에 사용될 특정 이더넷 장치를 선택하는데 사용됩니다. 만일 킥스타트 파일이 로컬 파일 (예, `ks=floppy`)이 아니라면, 설치 프로그램은 킥스타트 파일을 찾기위하여 네트워크를 설정하기 때문에 `--device=` 옵션은 작동하지 않습니다. 예로 들면:

```
network --bootproto=dhcp --device=eth0
```

`--ip=`

‘ 설치할 컴퓨터의 IP 주소.

`--gateway=`

‘ IP 주소로 구성된 기본 게이트웨이.

`--nameserver=`

‘ IP 주소로 구성된 일차 네임 서버.

`--nodns`

‘ 어떠한 DNS 서버도 설정하지 않음.

`--netmask=`

‘ 설치된 시스템에 사용될 넷마스크.

`--hostname=`

‘ 설치된 시스템에 사용될 호스트명.

`part` 또는 `partition` (설치시에는 필수이지만, 업그레이드시에는 무시됩니다)

‘ 시스템 상에 파티션을 생성합니다.

만일 한 개 이상의 Red Hat Linux가 여러 다른 파티션 상에 설치되어 있다면, 설치 프로그램은 사용자에게 어떤 파티션을 업그레이드할 것인지 물을 것입니다.

주의

`--noformat` 명령과 `--onpart` 명령이 사용되지 않는 한, 모든 파티션은 설치 과정에서 포맷될 것입니다.

<mntpoint>

‘ *<mntpoint>*는 파티션이 마운트될 지점으로서 다음 중 한가지 형식으로 지정되어야 합니다:

- `/`*<path>*

  예, `/`, `/usr`, `/home`

- `swap`

  스왑 공간으로 사용될 파티션.

  스왑 파티션의 크기를 자동으로 결정하기 위해서는, 다음과 같이 `--recommended` 옵션을 사용해 주십시오:
  `swap --recommended`

  자동으로 생성된 스왑 파티션의 최소 크기는 시스템 내의 RAM 용량보다 적어서는 안되며 RAM 용량의 두배보다 커서는 안됩니다.

- `raid.`*<id>*

  소프트웨어 RAID에 사용될 파티션 (`raid` 참조).

- `pv.`*<id>*

  LVM에 사용될 파티션 (`logvol` 참조).

`--size=`

‘ 파티션의 최소 용량 (메가바이트 단위). 여기에 500과 같은 정수 값을 지정해 주십시오. 숫자 다음에 MB를 함께 입력하시지 마십시오.

`--grow`

‘ 파티션이 사용 가능한 공간을 가득 채울 때까지 최대 용량 설정을 채울 때까지 증가하도록 설정합니다.

`--maxsize=`

‘ 파티션이 증가할 수 있는 메가바이트 단위의 최대 파티션 크기. 여기에 정수 값을 지정하시고 수치를 MB로 추가하지 마십시오.

`--noformat`

‘ 설치 프로그램에게 해당 파티션을 포맷하지 않도록 지시합니다. `--onpart` 명령어와 함께 사용됩니다.

`--onpart=` 또는 `--usepart=`

‘ 이미 존재하는 장치 위에 해당 파티션을 놓도록 지시합니다. 예로 들면:
`partition /home --onpart=hda1`

명령은 이미 존재하는 `/dev/hda1` 장치에 `/home` 파티션을 놓습니다.

`--ondisk=` 또는 `--ondrive=`

‘ 특정 디스크 상에 파티션을 생성합니다. 예, `--ondisk=sdb` 명령은 두번째 SCSI 디스크 상에 파티션을 생성합니다.

`--asprimary`

‘ 해당 파티션을 제1의 파티션이 되도록 자동 할당하며, 그렇지 않으면 파티션 작업이 실패하도록 설정합니다.

`--bytes-per-inode=`

‘ 여기서 지정된 숫자는 파일 시스템이 생성될 때 inode 당 바이트 수를 나타내며, 십진수 형식으로 표시됩니다. 응용 프로그램에서 파일 시스템 상의 inode의 숫자를 증가시키려면, 이 옵션을 유용하게 사용하실 수 있습니다.

`--type=` (`fstype`로 대체되었습니다)

‘ 이 옵션은 더 이상 사용되지 않습니다. 대신 `fstype` 명령어를 사용하십시오.

`--fstype=`

‘ 해당 파티션에 사용될 파일 시스템 유형을 설정합니다. 다음과 같은 파일 시스템 유형을 입력하실 수 있습니다: `ext2`, `ext3`, `swap`, `vfat`.

`--start=`

‘ 해당 파티션에 대한 시작 실린더를 지정해 주십시오. 이 명령을 사용하기 위해서는 `--ondisk=` 또는 `ondrive=` 명령을 사용하여 드라이브를 지정해 주셔야 합니다. 또한 `--end=` 명령을 사용하여 마지막 실린더를 지정해 주시고, `--size=` 명령을 사용하여 파티션 크기를 지정하셔야 합니다.

`--end=`

‘ 해당 파티션의 마지막 실린더를 지정합니다. 이 명령을 사용하시려면, `--start=` 명령을 통하여 시작 실린더를 지정해 주셔야 합니다.

`--badblocks`

‘ 파티션에 대한 불량 섹터를 검사하도록 지정합니다.

알림

만일 어떤 이유에서든 파티션 작업이 실패한다면, 가상 콘솔 3에서 진단 메시지가 나타날 것입니다.

`raid` (선택 사항)

‘ 소프트웨어 RAID 장치를 조립합니다. 이 명령어는 다음과 같은 형식으로 사용됩니다:
`raid <mntpoint> --level=<level> --device=<mddevice> <partitions*>`

<mntpoint>

‘ AID 파일 시스템이 마운트될 위치를 나타냅니다. 만일 그 위치가 `/` 이라면, 부트 파티션 (`/boot`)이 존재하는 경우 이외에는 RAID 레벨이 반드시 1 이어야 합니다. 부트 파티션이 존재하는 경우, `/boot` 파티션이 레벨 1이 되며, 루트 (`/`) 파티션은 사용 가능한 유형 중 무엇이 되어도 상관없습니다. (다중 파티션이 기입될 수 있음을 의미하는) *<partitions*>*는 RAID 어레이를 추가하기 위하여 RAID 식별자 목록을 출력합니다.

`--level=`

‘ 사용할 RAID 레벨 (0, 1, 5).

`--device=`

‘ 사용할 RAID 장치명 (예, md0 또는 md1). RAID 장치의 범위는 md0 에서 md7 까지이며, 각 장치는 오직 한 번만 사용됩니다.

`--spares=`

‘ RAID 어레이를 위해 할당된 여유 드라이브의 숫자를 지정합니다. 여유 드라이브는 드라이브 고장 시 RAID 어레이를 재복구하는데 사용됩니다.

`--fstype=`

‘ RAID 어레이에 사용될 파일 시스템 유형을 설정합니다. 파일 시스템 유형에는 ext2, ext3, swap, vfat이 있습니다.

`--noformat`

‘ RAID 어레이를 포맷하지 않음.

다음에 나온 예시는 시스템 상에 3개의 SCSI 디스크가 존재한다고 가정하고 `/`에 사용될 RAID 레벨 1 파티션과 `/usr`에 대한 RAID 레벨 5 파티션을 생성하는 방법을 보여주고 있습니다. 또한 다음의 예시에서는 3개의 스왑 파티션을 각 드라이브 당 한개씩 생성합니다.

```
part raid.01 --size=60 --ondisk=sda
part raid.02 --size=60 --ondisk=sdb
part raid.03 --size=60 --ondisk=sdc
part swap --size=128 --ondisk=sda
part swap --size=128 --ondisk=sdb
part swap --size=128 --ondisk=sdc
part raid.11 --size=1 --grow --ondisk=sda
part raid.12 --size=1 --grow --ondisk=sdb
part raid.13 --size=1 --grow --ondisk=sdc
raid / --level=1 --device=md0 raid.01 raid.02 raid.03
raid /usr --level=5 --device=md1 raid.11 raid.12 raid.13
```

`reboot` (선택 사항)

‘ 설치가 완료된 후 재부팅 합니다 (이 명령에서는 인수(argument)를 사용하지 않습니다). 일반적으로 킥스타트 파일은 재부팅하기 전에 재부팅 메시지를 출력한 후 사용자가 키를 누를 때까지 기다립니다.

`rootpw` (필수)

‘ 시스템의 루트 암호를 <*password*> 인수로 설정합니다.
`rootpw [--iscrypted] <password>`

`--iscrypted`

‘ 이 명령을 하시면, 암호 인수가 이미 암호화되었다고 가정합니다.

`skipx` (선택 사항)

‘ 이 명령은 X를 설정하지 않습니다.

`text` (선택 사항)

‘ 텍스트 모드로 킥스타트 설치를 수행합니다. 킥스타트 설치는 그래픽 모드에서 기본으로 수행됩니다.

`timezone` (필수)

‘ `timeconfig`의 시간대 목록에서 <*`timezone`*>에 맞추어 시스템 시간대를 설정합니다.
`timezone [--utc] <timezone>`

`--utc`

‘ 이 명령을 입력하시면, 시스템은 하드웨어 시계가 UTC (그리니치 표준)시에 맞추어 설정된 것으로 간주합니다.

`upgrade` (선택 사항)

‘ 새로운 시스템을 설치하는 대신 기존의 시스템을 업그레이드하도록 지시합니다. cdrom, 하드 드라이브, nfs, (ftp와 http 설치시) url 중 한가지를 설치 트리의 위치로 지정해 주십시오. 보다 자세한 정보를 원하시면 `install`을 참조하시기 바랍니다.

`xconfig` (선택 사항)

‘ X 윈도우 시스템을 설정합니다. 만일 이 옵션이 주어지지 않으면, X가 설치되어 있는 경우 사용자는 설치 과정에서 수동으로 X를 설정하셔야 합니다; X가 설치되지 않은 경우에는 이 옵션을 사용해서는 안됩니다.

`--noprobe`

‘ 모니터를 검색하지 않음.

`--card=`

‘ 사용할 카드를 지정합니다; 이 카드 이름은 `hwdata` 패키지에 있는 `/usr/share/hwdata/Cards`의 카드 목록에 포함되어 있는 이름이어야 합니다. 카드 목록은 **킥스타트 설정 프로그램**의 **X 설정** 화면에서 찾으실 수 있습니다. 만일 카드 이름을 지정하지 않으시면, 설치 프로그램은 해당 카드에 사용되는 PCI 버스를 검색할 것입니다. AGP는 PCI 버스의 일부이므로, AGP 카드가 지원된다면, 검색될 것입니다. 검색 순서는 마더보드의 PCI 스캔 순서에 의해 결정됩니다.

`--videoram=`

‘ 비디오 카드의 RAM 용량을 지정합니다.

`--monitor=`

‘ 사용할 모니터를 지정합니다; 이 모니터 이름은 `hwdata` 패키지의 `/usr/share/hwdata/MonitorsDB`에 있는 모니터 목록에 포함된 이름이어야 합니다. 모니터 목록은 **킥스타트 설정 프로그램**의 **X 설정** 화면에서 찾으실 수 있습니다. `--hsync` 이나 `--vsync` 옵션이 사용되면, 이 옵션은 무시됩니다. 모니터 정보를 제공하시 않으시면, 설치 프로그램은 자동으로 모니터 검색을 시도합니다.

`--hsync=`

‘ 모니터의 수평 동기 주파수를 지정합니다.

`--vsync=`

‘ 모니터의 수직 동기 주파수를 지정합니다.

`--defaultdesktop=`

‘ 기본 데스크탑으로 GNOME이나 KDE를 지정합니다. (`%packages` 명령을 통하여 GNOME 데스크탑 환경과 KDE 데스크탑 환경이 설치된 경우).

`--startxonboot`

‘ 그래픽 로그인을 사용합니다.

`--resolution=`

‘ X 윈도우 시스템에 사용될 기본 해상도를 지정합니다. 사용 가능한 값은 640x480, 800x600, 1024x768, 1152x864, 1280x1024, 1400x1050, 1600x1200 입니다. 비디오 카드 및 모니터와 호환 가능한 해상도를 지정해 주십시오.

`--depth=`

‘ X 윈도우 시스템에 사용될 기본 색상도를 지정합니다. 사용 가능한 값은 8, 16, 24, 32 입니다. 비디오 카드 및 모니터와 호환 가능한 색상도를 지정하셔야 합니다.

`volgroup` (선택 사항)

‘ 다음과 같은 구문을 사용하여 논리 볼륨 관리 (LVM) 그룹을 생성합니다:
`volgroup` *`name partition`*

파티션을 먼저 생성하신 후, 논리 볼륨 그룹을 생성하시고, 그 후 논리 볼륨을 생성합니다. 예로 들면:
```
part pv.01 --size 3000
volgroup myvg pv.01
logvol / --vgname=myvg --size=2000 --name=rootvol
```

`zerombr` (선택 사항)

‘ `zerombr` 옵션에서 `yes` 인수가 사용된다면, 디스크 상에서 파손된 파티션 테이블은 모두 초기화됩니다. 따라서 파손된 파티션 테이블이 있는 디스크의 내용물은 모두 제거될 것입니다. 이 명령은 다음과 같은 형식으로 사용됩니다:
```
zerombr yes
```

이 명령은 이 형식으로만 사용되어야 합니다. 이 외의 형식은 작동하지 않습니다.

`%include`

‘ `%include` */path/to/file* 명령을 사용하시면, 킥스타트 파일 내의 다른 파일의 내용을 마치 `%include` 명령의 위치에 존재하는 것처럼 포함시킵니다.

7.5. 패키지 선택

`%packages` 명령을 사용하여 설치할 패키지의 목록을 보여주는 킥스타트 파일 섹션을 시작합니다. (업그레이드 과정에서는 패키지 선택이 지원되지 않기 때문에, 이 명령은 오직 설치 과정에서만 사용됩니다.)

패키지를 개별 패키지명이나 그룹으로 지정 가능합니다. 설치 프로그램은 관련된 패키지를 하나로 묶어 여러 개의 패키지 그룹을 정의합니다. 패키지 그룹 목록을 보시려면 Red Hat Linux CD-ROM에서 `RedHat/base/comps.xml` 파일을 참조하시기 바랍니다. 각 그룹은 ID, 사용 목적, 이름, 설명과 패키지 목록을 가지고 있으며, 이 패키지 목록에서 필수 패키지와 기본 패키지로 표시된 패키지들은 해당 그룹이 선택되면 함께 선택되어 집니다. 하지만 옵션으로 표시된 패키지는 해당 그룹이 선택되어도 특별히 직접 선택해 주셔야 설치됩니다.

대부분의 경우, 개별 패키지를 모두 열거하실 필요가 없이 원하시는 패키지 그룹만 기입해주시면 됩니다. 핵심 패키지와 기본 패키지는 항상 기본으로 선택된다는 점을 기억해 주십시오. 따라서 `%packages` 섹션에서 이 패키지를 지정하실 필요가 없습니다.

다음은 `%packages` 선택의 한 예입니다:

```
%packages
@ X Window System
@ GNOME Desktop Environment
```

```
@ Graphical Internet
@ Sound and Video
galeon
```

여러분이 보시듯이, 한 줄당 한 개의 패키지 그룹이 지정되어 있습니다. 패키지 그룹 지정 형식은 @ 기호로 시작하여 한 칸 띄우고 `comps.xml` 파일에서 주어진 그룹명을 입력합니다. 개별 패키지는 추가적인 문자 없이 지정하십시오. (위의 예에서 `galeon` 줄은 개별 패키지를 나타냅니다).

여러분은 또한 기본 패키지 목록에서 일부 패키지를 설치하지 않도록 지정하실 수도 있습니다:

```
@ Games and Entertainment
-kdegames
```

`%packages` 옵션에는 다음과 같은 두 가지 옵션을 사용 가능합니다.

`--resolvedeps`

‘ 목록에서 선택된 패키지를 설치하고 자동으로 패키지 간의 의존성 문제를 해결합니다. 만일 이 옵션이 지정되지 않은 경우 패키지 간의 의존성 문제가 발생한다면, 자동화 설치를 멈추고 사용자에게 설치를 계속할 지 여부를 묻습니다. 예로 들면:

```
%packages --resolvedeps
```

`--ignoredeps`

‘ 해결되지 않은 패키지 간의 의존성 문제를 무시하고 의존성을 가진 패키지 없이 목록에 선택된 패키지들을 설치합니다. 예로 들면:

```
%packages --ignoredeps
```

`--ignoremissing`[1]

‘ 사라진 패키지를 발견되는 경우, 설치를 정지할 것인지 계속할 것인지 여부를 묻기 위해 설치를 멈추는 대신 사라진 패키지와 패키지 그룹을 무시하도록 합니다. 예로 들면:

```
%packages --ignoremissing
```

7.6. 설치전 스크립트

`ks.cfg` 파일이 구문 분석된 후 즉시 시스템에서 실행될 명령을 추가하실 수 있습니다. 이 부분은 반드시 킥스타트 파일의 (명령어 부분 다음) 마지막 부분에 위치해야 하며, `%pre` 명령어로 시작해야 합니다. `%pre` 섹션에서 네트워크에 접속하실 수 있지만 이 시점에서 네임 서비스 *(name service)*가 설정되지 않았기 때문에 오직 IP 주소만 작동할 것입니다.

알림

설치전 스크립트는 chroot (change root) 환경에서 실행되지 않습니다.

`--interpreter /usr/bin/python`

‘ 다른 스크립팅 언어 (예, Python)를 지정하실 수 있습니다. `/usr/bin/python` 부분을 원하시는 스크립팅 언어로 교체해 주십시오.

1. 이 옵션은 Red Hat Linux 9에서 처음 사용되는 옵션입니다.

7.6.1. 예시

다음은 %pre 섹션의 예입니다:

```
%pre

#!/bin/sh

hds=""
mymedia=""

for file in /proc/ide/h*
do
 mymedia=‘cat $file/media‘
 if [ $mymedia == "disk" ] ; then
   hds="$hds ‘basename $file‘"
 fi
done

set $hds
numhd=‘echo $#‘

drive1=‘echo $hds | cut -d’ ’ -f1‘
drive2=‘echo $hds | cut -d’ ’ -f2‘

#Write out partition scheme based on whether there are 1 or 2 hard drives

if [ $numhd == "2" ] ; then
 #2 drives
 echo "#partitioning scheme generated in %pre for 2 drives" > /tmp/part-include
 echo "clearpart --all" >> /tmp/part-include
 echo "part /boot --fstype ext3 --size 75 --ondisk hda" >> /tmp/part-include
 echo "part / --fstype ext3 --size 1 --grow --ondisk hda" >> /tmp/part-include
 echo "part swap --recommended --ondisk $drive1" >> /tmp/part-include
 echo "part /home --fstype ext3 --size 1 --grow --ondisk hdb" >> /tmp/part-include
else
 #1 drive
 echo "#partitioning scheme generated in %pre for 1 drive" > /tmp/part-include
 echo "clearpart --all" >> /tmp/part-include
 echo "part /boot --fstype ext3 --size 75" >> /tmp/part-includ
 echo "part swap --recommended" >> /tmp/part-include
 echo "part / --fstype ext3 --size 2048" >> /tmp/part-include
 echo "part /home --fstype ext3 --size 2048 --grow" >> /tmp/part-include
fi
```

이 스크립트는 시스템에 속한 하드 드라이브의 숫자를 알아낸 후 드라이브가 한 개인지 두 개인지 여부에 따라서 다른 파티션 분할 스키마를 사용하여 텍스트 파일을 기록합니다. 킥스타트 파일에 파티션 명령을 함께 입력하는 대신, 다음과 같은 줄을 포함하시기 바랍니다:

```
%include /tmp/part-include
```

스크립트에서 선택된 파티션 명령이 사용될 것입니다.

7.7. 설치후 스크립트

설치가 완료된 후 시스템 상에서 실행될 명령어를 추가할 수 있는 옵션을 갖게 됩니다. 이 섹션은 킥스타트 파일의 마지막 부분에 위치하며 %post 명령으로 시작합니다. 추가 소프트웨어를 추가하거나 추가 네임 서버를 설정하는 경우에 이 기능을 유용하게 사용하실 수 있습니다.

알림

정적 IP 정보를 사용하여 네트워크와 네임 서버를 설정하셨다면, %post 섹션에서 네트워크에 접속하여 IP 주소를 분석하실 수 있습니다. 네트워크에서 DHCP를 사용하도록 설정하셨다면, 설치가 %post 섹션을 실행할 때 /etc/resolv.conf 파일이 완료되지 않았기 때문에 네트워크에 접속은 가능하지만 IP 주소를 분석할 수는 없습니다. 따라서 DHCP를 사용하신다면 반드시 %post 섹션에 IP 주소를 지정해 주셔야 합니다.

알림

설치후 스크립트는 chroot 환경에서 실행됩니다; 따라서 설치 매체에서 스크립트나 RPM을 복사하기와 같은 작업을 수행하실 수 없습니다.

`--nochroot`

‘ 여러분이 chroot 환경 외부에서 실행하기를 원하는 명령어를 지정할 수 있게 허용합니다.

다음 예시에서는 방금 설치된 파일 시스템에 /etc/resolv.conf 파일을 복사합니다.

```
%post --nochroot
cp /etc/resolv.conf /mnt/sysimage/etc/resolv.conf
```

`--interpreter` *`/usr/bin/python`*

‘ 다른 스크립팅 언어 (예, Python)를 지정하실 수 있습니다. */usr/bin/python* 부분을 원하시는 스크립팅 언어로 교체해 주십시오.

7.7.1. 예시

서비스를 켜고 끕니다:

```
/sbin/chkconfig --level 345 telnet off
/sbin/chkconfig --level 345 finger off
/sbin/chkconfig --level 345 lpd off
/sbin/chkconfig --level 345 httpd on
```

NFS 공유에서 runme라는 스크립트를 실행합니다:

```
mkdir /mnt/temp
mount 10.10.0.2:/usr/new-machines /mnt/temp
open -s -w -- /mnt/temp/runme
umount /mnt/temp
```

시스템에 사용자를 추가합니다:

```
/usr/sbin/useradd bob
/usr/bin/chfn -f "Bob Smith" bob
/usr/sbin/usermod -p 'kjdf$04930FTH/' bob
```

7.8. 킥스타트 파일을 저장할 위치

킥스타트 파일은 반드시 다음 중 한가지 위치에 저장하셔야 합니다:

- 부팅 디스켓
- 부팅 CD-ROM
- 네트워크

일반적으로 킥스타트 파일은 부팅 디스켓에 복사되거나 네트워크 상에서 사용 가능하게 되어 있습니다. 대부분의 킥스타트 설치가 네트워크 연결된 컴퓨터에서 수행되기 때문에 네트워크-기반 설치가 가장 일반적으로 사용됩니다.

이제 킥스타트 파일이 위치할 수 있는 장소에 대하여 보다 자세하게 설명해 보겠습니다.

7.8.1. 킥스타트 부팅 디스켓 만들기

디스켓-기반 킥스타트 설치를 수행하시려면, 킥스타트 파일을 `ks.cfg`으로 이름 붙이신 후 부팅 디스켓의 최상위 디렉토리에 저장하셔야 합니다. 부팅 디스켓 만드는 방법에 대한 자세한 정보는 *Red Hat Linux* 설치 가이드의 설치 부팅 디스켓 만들기 부분을 참조하시기 바랍니다. Red Hat Linux 부팅 디스켓은 MS-DOS 형식으로 되어있기 때문에, 리눅스에서 `mcopy` 명령을 이용하여 쉽게 킥스타트 파일을 복사하실 수 있습니다:

```
mcopy ks.cfg a:
```

Windows를 사용하여 파일을 복사하는 방법도 있습니다. 또는 Red Hat Linux에서 vfat 파일 시스템 유형으로 MS-DOS 부팅 디스켓을 마운트하신 후 `cp` 명령을 사용하여 파일을 복사해 옵니다.

7.8.2. 킥스타트 부팅 CD-ROM 만들기

CD-ROM 기반 킥스사트 설치를 수행하시려면, 킥스타트 파일을 `ks.cfg`으로 이름 붙이고 부팅 CD-ROM의 최상위 디렉토리에 저장하셔야 합니다. CD-ROM은 읽기 전용이므로, CD-ROM에 기록된 이미지를 생성하는데 사용된 디렉토리에 이 파일을 추가하셔야 합니다. 부팅 CD-ROM을 생성하는 방법에 대한 자세한 정보는 *Red Hat Linux* 설치 가이드에서 설치 부팅 *CD-ROM* 만들기 부분을 참조하시기 바랍니다; 그러나 `file.iso` 이미지 파일을 만드시기 전에, `isolinux/` 디렉토리에 `ks.cfg` 킥스타트 파일을 복사하셔야 합니다.

7.8.3. 네트워크 기반 킥스타트 설치

시스템 관리자는 네트워크로 연결된 여러 개의 컴퓨터 상에서 설치를 더욱 빠르게 쉽게 자동화할 수 있기 때문에, 킥스타트를 사용한 네트워크 설치가 자주 사용됩니다. 일반적으로 관리자들이 가장 자주 사용하는 설치 방법은 로컬 네트워크 상에서 BOOTP/DHCP 서버와 NFS 서버를 모두 사용하는 방법입니다. BOOTP/DHCP 서버는 클라이언트 시스템에게 네트워킹 정보를 제공하기 위하여 사용되는 반면에 NFS 서버는 설치 과정에서 사용된 실제 파일들을 제공합니다. 이 두 서버는 종종 동일한 컴퓨터 상에서 실행되지만, 다른 기계에서 실행되어도 상관없습니다.

네트워크-기반 킥스타트 설치를 수행하시려면, 네트워크 상에 BOOTP/DHCP 서버가 있어야 하며, 그 서버는 Red Hat Linux를 설치할 컴퓨터에 대한 설정 정보를 포함하고 있어야 합니다. BOOTP/DHCP 서버는 클라이언트에게 킥스타트 파일의 위치 뿐만 아니라 네트워크 정보도 함께 제공할 것입니다.

만일 킥스타트 파일이 BOOTP/DHCP 서버에 의해 지정되었다면, 클라이언트 시스템은 파일의 경로를 NFS 마운트한 후 특정 파일을 복사하여 킥스타트 파일처럼 사용합니다. 여러분이 사용하시는 BOOTP/DHCP 서버에 따라서 다르게 설정됩니다.

다음은 Red Hat Linux에 포함된 DHCP 서버에 사용되는 `dhcpd.conf` 파일을 보시면, 다음과 같은 줄이 나타납니다:

```
filename "/usr/new-machine/kickstart/";
```

```
next-server blarg.redhat.com;
```

`filename` 다음에 나오는 값을 킥스타트 파일 (또는 킥스타트 파일이 위치하는 디렉토리)의 이름으로, `next-server` 다음에 나오는 값은 NFS 서버명으로 대체해 주십시오.

만일 BOOTP/DHCP 서버에 의해 되돌아온 파일명이 슬래시 ("/")로 끝난다면 이것은 오직 경로로만 해석됩니다. 이러한 경우에 클라이언트 시스템은 NFS를 사용하여 그 경로를 마운트하며 특정 파일을 검색합니다. 클라이언트가 찾는 파일명은 다음과 같습니다:

```
<ip-addr>-kickstart
```

파일명의 <*ip-addr*> 부분은 클라이언트의 IP 주소를 점으로 구분된 십진수 형식으로 대체해 주십시오. 예를 들어, IP 주소가 10.10.0.1인 컴퓨터의 파일명은 `10.10.0.1-kickstart`가 됩니다.

서버명을 지정하지 않으시면, 클라이언트 시스템은 BOOTP/DHCP의 요구에 대하여 NFS 서버로서 응답한 서버를 사용할 것입니다. 만일 경로나 파일명을 지정하지 않으시면, 클라이언트 시스템은 BOOTP/DHCP 서버로부터 `/kickstart`를 마운트 시도한 후 앞에서 설명된 <*ip-addr*>`-kickstart` 파일명을 사용하여 킥스타트 파일을 찾으려고 시도할 것입니다.

7.9. 설치 트리 위치

킥스타트 설치시에는 설치 트리 *(installation tree)*에 접근하셔야 합니다. 설치 트리란 바이너리 Red Hat Linux CD-ROM의 디렉토리 구조를 동일하게 복사한 것을 의미합니다.

CD-기반 설치를 수행하신다면, 컴퓨터에 Red Hat Linux CD-ROM #1를 삽입하신 후 킥스타트 설치를 시작하시기 바랍니다.

하드 드라이브 설치를 수행하신다면, 바이너리 Red Hat Linux CD-ROM의 ISO 이미지를 컴퓨터의 하드 드라이브로 복사하셔야 합니다.

네트워크 기반 (NFS, FTP, HTTP) 설치를 수행하신다면, 네트워크 상에서 설치 트리를 사용할 수 있도록 해주십시오. 보다 자세한 정보를 원하시면, *Red Hat Linux* 설치 가이드의 네트워크 설치 준비 부분을 참조하시기 바랍니다.

7.10. 킥스타트 설치 시작하기

킥스타트 설치를 시작하시려면, Red Hat Linux 부팅 디스켓이나 Red Hat Linux 부팅 CD-ROM 또는 Red Hat Linux CD-ROM #1을 사용하여 시스템을 부팅하신 후 부트 프롬프트에서 특별한 부트 명령을 입력하셔야 합니다. `ks` 명령행 인자가 커널로 전달될 경우 설치 프로그램은 킥스타트 파일을 찾기 시도합니다.

부팅 디스켓

- 7.8.1 절에서 설명된 것처럼, 킥스타트 파일이 부팅 디스켓에 저장되어 있는 경우, 디스켓을 드라이브에 삽입하여 시스템을 부팅하신 후 `boot:` 프롬프트에서 다음 명령을 입력하시기 바랍니다:
  `linux ks=floppy`

CD-ROM #1과 디스켓

- `ks.cfg` 파일이 디스켓 상 vfat이나 ext2 파일 시스템 상에 위치하며, Red Hat Linux CD-ROM #1으로 부팅한 경우에도 **`linux ks=floppy`** 명령이 작동합니다.

  또 다른 부팅 명령으로 Red Hat Linux CD-ROM #1을 부팅 후 킥스타트 파일을 디스켓 상에서 vfat이나 ext2 파일 시스템에 저장하는 방법이 있습니다. `boot:` 프롬프트에서 다음 명령을 입력하시면 됩니다:
  `linux ks=hd:fd0:/ks.cfg`

드라이버 디스켓 사용

‘ 드라이버 디스켓을 사용하여 킥스타트를 시작하셨다면, **dd** 옵션도 지정해 주셔야 합니다. 예를 들어, 부팅 디스켓을 사용하여 부팅 후 드라이버 디스켓을 사용하시려면, `boot:` 프롬프트에서 다음 명령을 입력하시기 바랍니다:
`linux ks=floppy dd`

부팅 CD-ROM

‘ 7.8.2 절에서 설명된 것처럼, 킥스타트 파일이 부팅 CD-ROM에 저장되어 있는 경우, CD-ROM을 삽입하여 시스템을 부팅하신 후 `boot:` 프롬프트에서 다음 명령을 입력하시기 바랍니다 (다음 명령에서 `ks.cfg`은 킥스타트 파일 이름입니다):
`linux ks=cdrom:/ks.cfg`

킥스타트 설치를 시작하는데 사용되는 다른 옵션은 다음과 같습니다:

`ks=nfs:<server>:/<path>`

‘ 설치 프로그램은 NFS 서버 <*server*> 상에서 <*path*> 파일로서 킥스타트 파일을 찾을 것입니다. 설치 프로그램은 DHCP를 사용하여 이더넷 카드를 설정합니다. 예를 들어 NFS 서버가 server.example.com이고 킥스타트 파일이 NFS 공유 `/mydir/ks.cfg`에 위치한 경우, 올바른 부트 명령은 `ks=nfs:server.example.com:/mydir/ks.cfg`가 될 것입니다.

`ks=http://<server>/<path>`

‘ 설치 프로그램은 HTTP 서버 <*server*> 상에서 <*path*> 파일로서 킥스타트 파일을 찾을 것입니다. 설치 프로그램은 DHCP를 사용하여 이더넷 카드를 설정합니다. 예를 들어 HTTP 서버가 server.example.com이고 킥스타트 파일이 HTTP 디렉토리인 `/mydir/ks.cfg`에 위치한 경우, 올바른 부트 명령은 `ks=http://server.example.com/mydir/ks.cfg`가 될 것입니다.

`ks=floppy`

‘ 설치 프로그램은 `/dev/fd0` 드라이브에 있는 플로피의 vfat 또는 ext2 파일 시스템 상에 존재하는 `ks.cfg` 파일을 찾습니다.

`ks=floppy:/<path>`

‘ 설치 프로그램은 `/dev/fd0`의 디스켓 상에서 <*path*> 경로에 위치한 킥스타트 파일을 찾을 것입니다.

`ks=hd:<device>:/<file>`

‘ 설치 프로그램은 (vfat 또는 ext2인) 파일 시스템을 <*device*>에 마운트할 것입니다. 그 후 그 파일 시스템에서 <*file*> 킥스타트 설정 파일을 찾아봅니다 (예, `ks=hd:sda3:/mydir/ks.cfg`).

알림

두번째 콜론은 Red Hat Linux 9에서 처음 사용되었습니다.

`ks=file:/<file>`

‘ 설치 프로그램은 파일 시스템으로부터 <*file*> 파일을 읽기 시도할 것입니다; 아무런 마운트도 행해지지 않습니다. 킥스타트 파일이 이미 `initrd` 이미지에 위치하는 경우에 이 방법이 일반적으로 사용됩니다.

`ks=cdrom:/<path>`

‘ 설치 프로그램은 CD-ROM 상에서 <*path*> 파일로서 킥스타트 파일을 찾을 것입니다.

`ks`

‘ 만일 `ks`이 단독으로 사용되었다면, 설치 프로그램은 DHCP를 사용하여 이더넷 카드를 설정합니다. 시스템은 DHCP 응답으로부터 "부트서버 (bootServer)"를 NFS 서버로 사용하여 킥스타트 파일을 읽어올 것입니다. 킥 스타트 파일은 다음과 같은 이름을 갖습니다:

- DHCP가 이미 지정되었고 부트파일 이름이 `/`로 시작되는 경우, NFS 서버에서 DHCP가 제공한 부트파일을 찾습니다.
- DHCP가 이미 지정되었고 부트파일 이름이 `/`로 시작하지 않는 경우, NFS 서버 상의 `/kickstart` 디렉토리에서 DHCP가 제공한 부트파일을 찾습니다.
- DHCP가 부트파일을 지정하지 않았다면, 설치 프로그램은 `/kickstart/1.2.3.4-kickstart` 파일 읽기를 시도합니다. 여기서 *`1.2.3.4`*는 설치되는 컴퓨터의 IP 주소를 의미합니다.

`ksdevice=<`*`device`*`>`

‘ 설치 프로그램은 여기서 지정된 네트워크 장치를 사용하여 네트워크에 접속합니다. 예, eh1 장치를 통해 시스템에 접속된 NFS 서버 상에서 킥스타트 파일을 이용하여 킥스타트 설치를 시작하시려면, `boot:` 프롬프트에서 `ks=nfs:<`*`server`*`>:/<`*`path`*`> ksdevice=eth1` 명령을 사용하시기 바랍니다.

8장 .

킥스타트 설정 프로그램

킥스타트 설정 프로그램는 그래픽 사용자 인터페이스를 사용하여 킥스타트 파일을 생성할 수 있게 해줍니다. 따라서 사용자는 파일의 정확한 구문을 기억할 필요가 없습니다.

킥스타트 설정 프로그램를 사용하기 위해서는 반드시 X 윈도우 시스템을 실행하셔야 합니다. **킥스타트 설정 프로그램**를 시작하시려면 패널에서 **주 메뉴 버튼**을 클릭하신 후 **시스템 도구** => **킥스타트**를 선택하시거나 쉘 프롬프트에서 `/usr/sbin/redhat-config-kickstart`라고 입력하시면 됩니다.

킥스타트 파일을 생성하시는 동안 **파일** => **미리 보기** 항목을 선택하여 현재 선택하신 사항을 미리 보기하실 수 있습니다.

8.1. 기본 설정

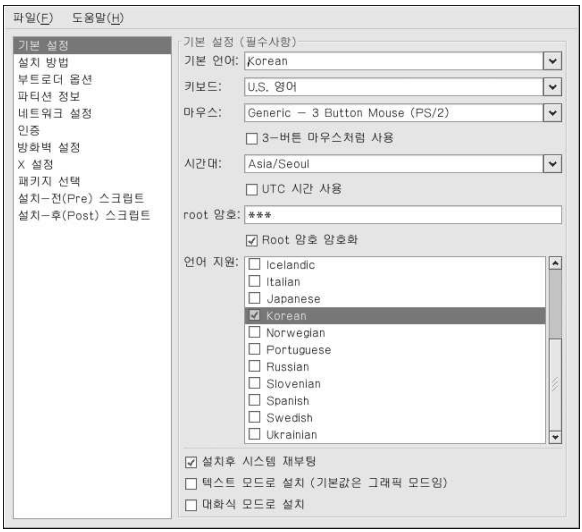

그림 8-1. 기본 설정

언어 메뉴에서 설치 과정에서 사용할 언어를 선택하십시오.

키보드 메뉴에서 시스템 키보드 유형을 선택하십시오.

마우스 메뉴에서 시스템에 적합한 마우스를 선택하시기 바랍니다. 만일 **마우스 없음**을 선택하시면, 마우스가 설정되지 않을 것입니다. 만일 **마우스 검색**을 선택하시면, 설치 프로그램은 마우스 자동 검색을 시도할 것입니다. 최근에 제조된 대부분의 마우스는 마우스 검색 작업을 통해 찾을 수 있습니다.

만일 2-버튼 마우스를 가지고 계신다면, **3-버튼 마우스처럼 사용** 버튼을 선택하여 3-버튼 마우스처럼 사용할 수 있습니다. 만일 이 옵션이 선택된다면 왼쪽과 오른쪽 마우스 버튼을 동시에 클릭하시면 중간 마우스 버튼을 클릭하는 것처럼 인식되어질 것입니다.

시간대 메뉴에서 시스템 상에서 사용하실 시간대를 선택해 주십시오. UTC 시간을 사용하도록 시스템을 설정하시려면, **UTC 시간 사용**을 선택해 주십시오.

root 암호 입력란에 원하시는 root 암호를 입력하십시오. 암호를 파일에서 암호화하여 저장하시려면, **Root 암호 암호화**를 선택하시기 바랍니다. 암호화 옵션이 선택된 경우, 파일 저장시 여러분이 입력하신 평문 암호는 암호화되어 킥스타트 파일에 기록됩니다. 이미 암호화된 암호를 입력 후 암호화하도록 선택하지 마십시오.

언어 지원 풀다운 메뉴에서 설치할 언어를 선택해 주십시오. 언어가 지원되는지 여부를 **지원 언어** 목록에서 확인하시기 바랍니다. **언어 지원** 풀다운 메뉴에서 선택하신 언어는 설치가 끝난후 기본으로 사용됩니다; 하지만 **언어 설정 도구** (`redhat-config-language`)를 사용하여 언제든지 기본 언어를 변경하실 수 있습니다.

설치 후 시스템 재부팅 옵션을 선택하시면 설치가 끝난 후 시스템이 자동으로 재부팅됩니다.

킥스타트 설치는 디폴트로 그래픽 모드에서 수행됩니다. 이 디폴트를 무효로하고 대신 텍스트 모드를 사용하시려면 **텍스트 모드로 설치** 버튼을 체크하십시오.

킥스타트 설치를 대화식 모드로 수행할 수 있습니다. 이것이 의미하는 바는 설치 프로그램은 킥스타트 파일 내에 미리 설정된 모든 옵션들을 사용하지만 여러분은 각각의 화면에서 다음 화면으로 진행하기 전에 그 옵션을 미리 볼 수 있습니다. 다음 화면으로 진행하기 위해서는, 설정을 확인하신 후 **다음** 버튼을 클릭하십시오. 미리 설정된 옵션이 마음에 들지 않는다면 설치를 계속 진행하시기 전에 설정을 변경하실 수 있습니다. 만일 이러한 방식의 설치를 선호하신다면 **대화식 모드로 설치** 옵션을 선택하십시오.

8.2. 설치 방법

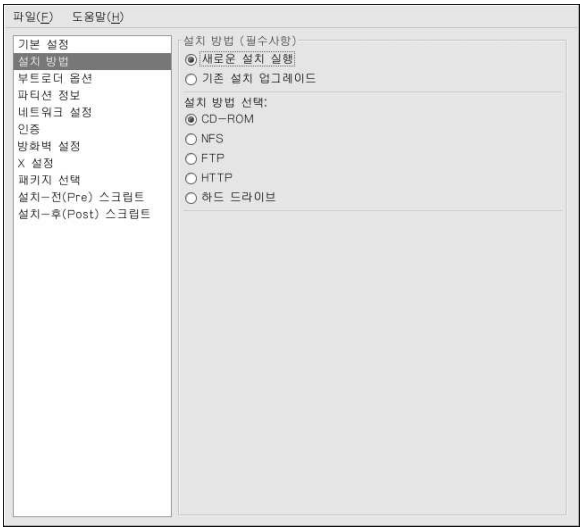

그림 8-2. 설치 방법

설치 방법 화면에서 여러분은 완전 설치 수행을 원하시는지 또는 업그레이드를 원하시는지 여부를 선택하실 수 있습니다. 만일 업그레이드를 선택하시면, **파티션 정보**와 **패키지 선택** 옵션이 기능 억제될 것입니다. 이 옵션들은 킥스타트 업그레이드에서는 지원되지 않습니다.

또한 이 화면에서 수행하실 킥스타트 설치의 유형을 선택하십시오. 다음과 같은 옵션에서 선택하실 수 있습니다:

- **CD-ROM** — Red Hat Linux CD-ROM을 사용하여 Red Hat Linux를 설치하시려면 이 옵션을 선택하십시오.
- **NFS** — NFS 공유 디렉토리에서 Red Hat Linux를 설치하시려면 이 옵션을 선택하십시오. NFS 서버와 NFS 디렉토리에 대한 두 개의 입력란이 나타날 것입니다. 완전한 도메인 이름 또는 NFS 서버의 IP 주소를 입력하십시오. NFS 디렉토리에 대해서는 `RedHat` 디렉토리를 포함하고 있는 NFS 디렉토리의 이름을 입력하십시오. 예를 들어 만일 NFS 서버가 `/mirrors/redhat/i386/RedHat` 디렉토리를 포함하고 있다면, NFS 디렉토리 란에 `/mirrors/redhat/i386`를 입력합니다.
- **FTP** — Red Hat Linux를 FTP 서버로부터 설치하기를 원하신다면 이 옵션을 선택하십시오. FTP 서버와 FTP 디렉토리에 대한 두 개의 입력란이 나타날 것입니다. 완전한 도메일 이름 또는 FTP 서버의 IP 주소를 입력하십시오. FTP 디렉토리에 대해서는 `RedHat` 디렉토리를 포함하고 있는 FTP 디렉토리의 이름을 입력하십시오. 예를 들어 만일 여러분의 FTP 서버가 `/mirrors/redhat/i386/RedHat` 디렉토리를 포함하고 있다면, FTP 디렉토리 란에 `/mirrors/redhat/i386`를 입력합니다.
- **HTTP** — HTTP 서버에서 Red Hat Linux를 설치하시려면 이 옵션을 선택하십시오. HTTP 서버와 HTTP 디렉토리에 대한 두 개의 입력란이 나타날 것입니다. 완전한 도메일 이름 또는 HTTP 서버의 IP 주소를 입력하십시오. HTTP 디렉토리에 대해서는 `RedHat` 디렉토리를 포함하고 있는 HTTP 디렉토리의 이름을 입력하십시오. 예를 들어 만일 여러분의 HTTP 서버가 `/mirrors/redhat/i386/RedHat` 디렉토리를 포함하고 있다면, HTTP 디렉토리 란에 `/mirrors/redhat/i386`를 입력합니다.
- **하드 드라이브** — 하드 드라이브에서 Red Hat Linux를 설치하시려면 이 옵션을 선택하시기 바랍니다. 하드 드라이브 파티션과 하드 드라이브 디렉토리에 대한 두 개의 입력란이 나타날 것입니다. 하드 드라이브 설치를 위해서는 ISO (또는 CD-ROM) 이미지를 사용하셔야 합니다. 설치를 시작하기 전에 ISO 이미지가 원래대로 번하지 않은 것을 확인하셔야 합니다. `md5sum` 프로그램을 사용하여 확인하시기 바랍니다. **하드 드라이브 파티션** 텍스트 박스에 ISO 이미지를 포함하고 있는 하드 드라이브 파티션을 (예, `/dev/hda1`) 입력하신 후 **하드 드라이브 디렉토리** 입력란에 ISO 이미지를 포함하고 있는 디렉토리를 입력하십시오.

8.3. 부트로더 옵션

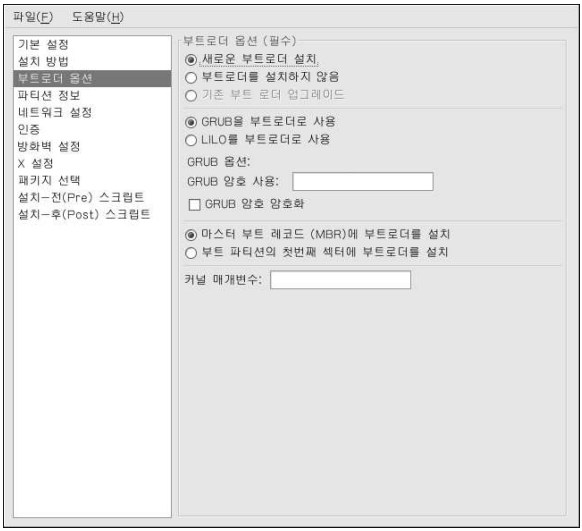

그림 8-3. 부트로더 옵션

GRUB이나 LILO 중 하나를 선택하여 부트로더로 설치하실 수 있습니다. 만일 부트로더 설치를 원치 않으시면, **부트로더 설치하지 않기** 옵션을 선택하십시오. 부트로더를 설치하지 않기로 선택하신다면, 부팅 디스켓을 만드시거나 Red Hat Linux 시스템을 부팅할 다른 방법이 (예, 제 3의 부트로더) 있어야 합니다.

부트로더를 설치하기로 선택하신다면, 설치할 부트로더의 종류 (GRUB 또는 LILO)와 그 부트로더를 설치할 장소 (마스터 부트 레코드 또는 `/boot` 파티션의 첫번째 섹터)를 선택하셔야 합니다. GRUB이나 LILO를 부트로더로 사용하실 계획이라면 MBR 상에 부트로더를 설치하십시오. 만일 다른 부트로더를 사용하신다면 LILO 또는 GRUB을 `/boot` 파티션의 첫번째 섹터에 설치하신 후 다른 부트로더가 Red Hat Linux를 부팅하도록 설정하십시오.

만일 특별한 매개변수를 커널로 전달하여 시스템이 부트될 때 사용될 수 있도록 하기 위해서는, 그 매개변수를 **커널 매개변수** 텍스트 영역에 입력하십시오. 예를 들어 만일 IDE CD-ROM Writer를 가지고 계신다면, 여러분은 커널 매개변수로서 **`hdd=ide-scsi`**를 (여기서 **`hdd`**는 CD-ROM 장치를 의미합니다) 입력하여 커널이 **cdrecord**를 사용하기 전에 SCSI 에뮬레이션 드라이버를 먼저 로드하도록 지시 가능합니다.

GRUB을 부트로더로 선택하시면, GRUB 암호를 설정하셔서 GRUB을 암호를 사용하여 보호할 수 있습니다. **GRUB 암호 사용** 입력란에 암호를 입력하십시오. 만일 그 암호를 파일 내에 암호화된 암호로 저장하기를 원하시면, **GRUB 패스워드 암호화** 버튼을 선택하십시오. 파일이 저장되면 여러분이 입력하신 평문 암호는 암호화되어 킥스타트 파일에 기록될 것입니다. 이미 암호화된 암호를 입력하셨다면 암호화하기를 선택하지 마십시오.

LILO를 부트로더로 선택하시면, 선형 모드를 사용하실지 여부와 lba32 모드 사용을 강제하기를 원하시는지 여부를 선택해 주십시오.

설치 방법 화면에서 **기존 시스템 업그레이드하기**를 선택하셨다면, **기존 부트로더 업그레이드하기**를 선택하여 이전 설정을 그대로 보존하면서 기존 부트로더 설정을 업그레이드하실 수 있습니다.

8.4. 파티션 정보

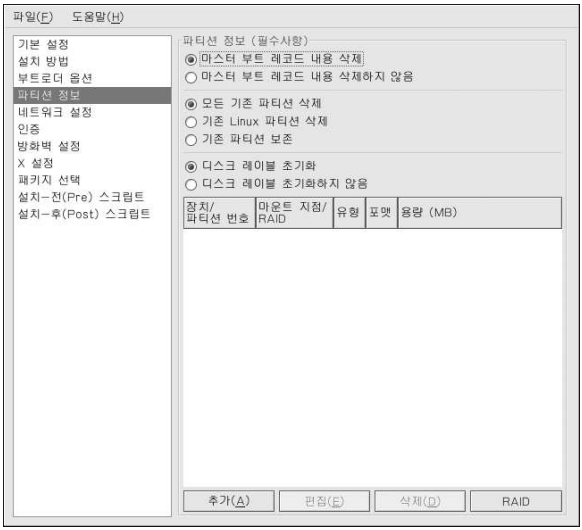

그림 8-4. 파티션 정보

마스터 부트 레코드 (MBR)를 지울 것인지 여부를 선택해 주십시오. 모든 기존 파티션을 삭제, 모든 기존 리눅스 파티션을 삭제하거나 또는 기존 파티션을 보존하기 여부도 선택하실 수 있습니다.

시스템의 구조에 맞는 디폴트로 디스크 레이블을 초기화할 수 있습니다. (x86에는 `msdos` 그리고 Itanium에는 `gpt`) 새 하드 드라이브 상에서 설치하신다면 **디스크 레이블 초기화**를 선택하십시오.

8.4.1. 파티션 생성하기

파티션을 생성하기 위해서는 **추가** 버튼을 클릭하십시오. 그림 8-5에서 보여지는 **파티션 옵션** 화면이 나타날 것입니다. 새로운 파티션의 마운트 지점, 파일 시스템 유형 및 파티션 용량을 선택하시기 바랍니다. 또한 옵션으로 다음과 같은 사항들을 선택 가능합니다:

- **추가 용량 옵션** — 고정된 크기로 파티션을 만들기, 선택된 크기까지 증가하도록 하기 또는 하드 드라이브 상에 남아있는 공간을 채우기 중 한가지를 선택합니다. 파일 시스템 유형으로 스왑을 선택하셨다면, 여러분이 직접 스왑 공간을 지정하시는 대신 설치 프로그램이 추천된 용량으로 스왑 파티션을 생성하도록 선택하실 수 있습니다.
- 해당 파티션을 첫번째 파티션으로 함.
- 특정 하드 드라이브 상에서 파티션 생성하기. 예를 들어 첫번째 IDE 하드 디스크 (`/dev/hda`) 상에서 파티션을 생성하기 위해서는, **hda**를 드라이브로 지정합니다. 드라이브 이름에 `/dev`를 포함하지 마십시오.
- 기존 파티션 사용하기. 예를 들어 첫번째 IDE 하드 디스크 상의 첫번째 파티션 (`/dev/hda1`)위에 파티션을 생성하기 위해서는, **hda1**를 파티션으로 지정합니다. 파티션 이름에 `/dev`를 포함하지 마십시오.
- 선택하신 파일 시스템 유형으로 파티션으로 포맷합니다.

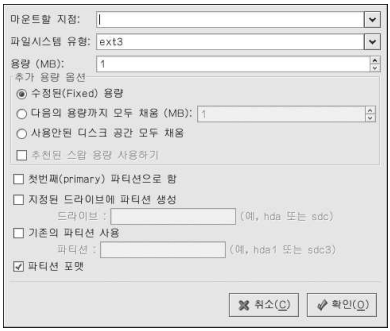

그림 8-5. 파티션 생성하기

기존 파티션을 편집하기 위해서는 목록에서 해당 파티션을 선택하신 후 **편집** 버튼을 클릭하십시오. 그림 8-5와 같이 파티션을 추가시 나타났던 동일한 **파티션 옵션** 화면이 나타날 것입니다. 하지만 이 화면에는 선택하신 파티션에 대한 값들이 포함되어 있습니다. 파티션 옵션을 수정하신 후 **확인** 버튼을 클릭하시기 바랍니다.

기존 파티션을 삭제하시려면 목록에서 해당 파티션을 선택하신 후 **삭제** 버튼을 클릭하십시오.

8.4.1.1. 소프트웨어 RAID 파티션 생성하기

RAID와 관련된 정보와 RAID 0, 1, 5 레벨에 대한 보다 정보를 원하신다면, 3 장을 읽어보시기 바랍니다.

소프트웨어 RAID 파티션을 생성하시려면 다음과 같은 과정을 따르십시오:

1. **RAID** 버튼을 클릭합니다.
2. **소프트웨어 RAID 파티션 생성**을 선택해 주십시오.

3. **소프트웨어 RAID**를 파일 시스템 유형으로 설정하는 것을 제외하고는 앞에서 설명된 사항에 따라서 파티션을 설정하시기 바랍니다. 파티션을 생성할 하드 드라이브 또는 사용할 기존 파티션도 지정해 주셔야 합니다.

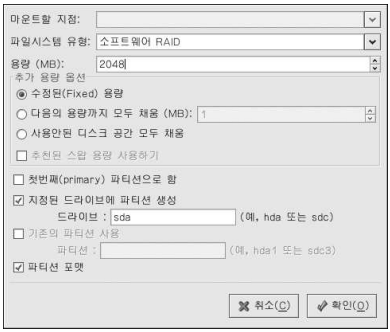

그림 8-6. 소프트웨어 RAID 파티션 생성

이와 같은 과정을 반복하여 RAID 설정에 필요한 만큼의 파티션을 생성하십시오. 모든 파티션이 RAID 파티션일 필요는 없습니다.

RAID 장치를 형성하는데 필요한 모든 파티션을 생성하셨다면, 다음 과정을 따르십시오:

1. **RAID** 버튼을 클릭합니다.
2. **RAID 장치 생성**을 선택해 주십시오.
3. 마운트 지점, 파일 시스템 유형, RAID 장치명, RAID 레벨, RAID 요소, 소프트웨어 RAID 장치에 사용될 여유 디스크 수 및 RAID 장치 포맷 여부를 선택해 주십시오.

그림 8-7. 소프트웨어 RAID 장치 생성

4. **확인** 버튼을 클릭하여 설정하신 장치를 목록에 추가하십시오.

8.5. 네트워크 설정

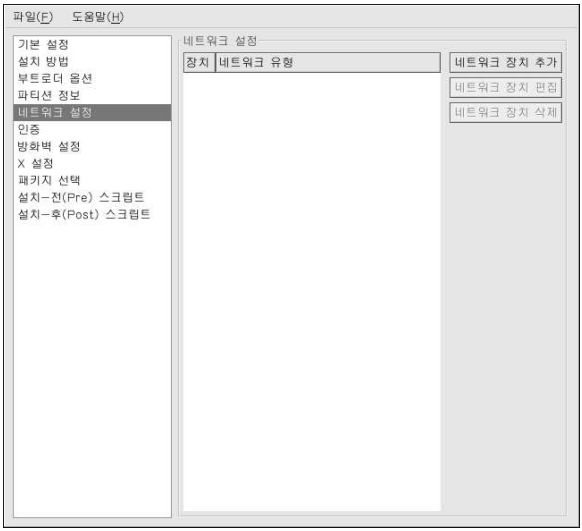

그림 8-8. 네트워크 설정

킥스타트를 통해 설치할 시스템에 이더넷 카드가 없다면, **네트워크 설정** 화면에서 네트워크를 설정하지 마십시오.

네트워킹은 네트워킹 기반 설치 방식 (NFS, FTP, HTTP)을 선택하신 경우에만 필요합니다. 설치가 끝난 후 언제든지 **네트워크 관리 도구**으로 (`redhat-config-network`) 네트워킹을 설정 가능합니다. 자세한 사항은 12 장을 참조하시기 바랍니다.

시스템 상의 이더넷 카드마다, **네트워크 장치 추가** 버튼을 클릭하신 후 네트워크 장치와 그 장치의 네트워크 유형을 선택해 주십시오. 첫번째 이더넷 카드는 **eth0** 네트워크 장치로 선택하시고 두번째 이더넷 카드는 **eth1**을 선택하시고, 이와 같은 방법으로 계속 진행하시면 됩니다.

8.6. 인증

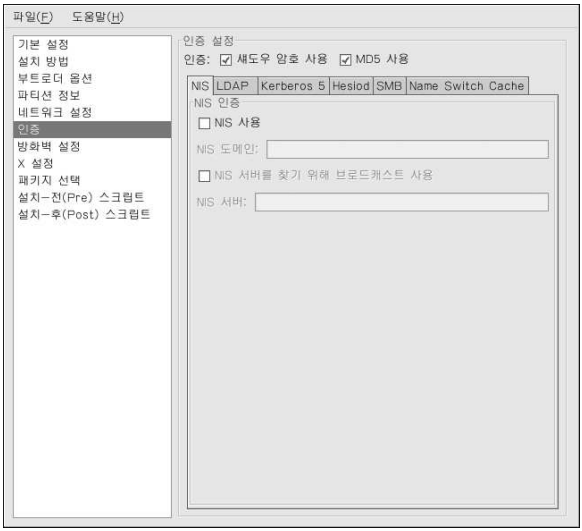

그림 8-9. 인증

인증 섹션에서 사용자 암호로 새도우 암호를 사용할 것인지 MD5 암호화를 사용할 것인지 여부를 선택해 주십시오. 이 옵션들은 적극 권장되며 디폴트로 선택되어 있습니다.

인증 설정 옵션을 사용하여 다음과 같은 인증 방식들을 설정 가능합니다:

- NIS
- LDAP
- Kerberos 5
- Hesiod
- SMB
- 이름 교환 캐시 (Name Switch Cache)

위의 방식들은 기본 값으로 기능 비활성화되어 있습니다. 활성화하시려면, 적절한 탭을 클릭하신 후, **활성화** 옆에 위치한 체크 박스에 클릭하신 후 인증 방식에 대한 적절한 정보를 입력하시기 바랍니다.

8.7. 방화벽 설정

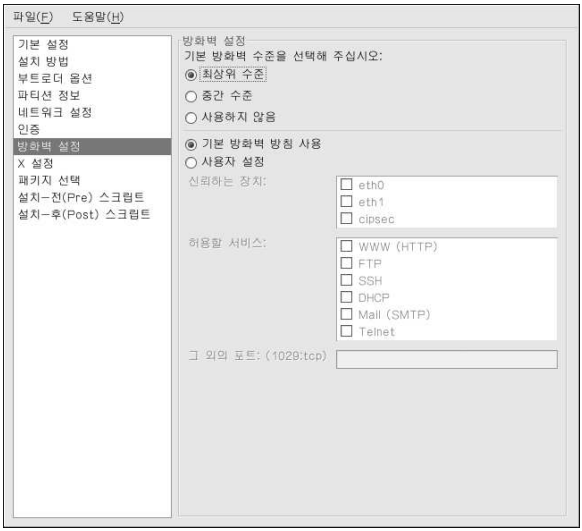

그림 8-10. 방화벽 설정

방화벽 설정 창은 Red Hat Linux 설치 프로그램과 **보안 수준 설정 도구**에서 나타나는 창과 똑같으며 동일한 기능성을 제공합니다. **최상위**, **중간**, **사용하지 않음** 보안 수준 중 하나를 선택하십시오. 이러한 보안 수준에 대한 보다 자세한 정보를 원하신다면 13.1 절을 참조하시기 바랍니다.

8.8. X 설정

X 윈도우 시스템을 설치하시는 경우, 킥스타트 설치 과정에서 그림 8-11 화면에서 나타난 **X 윈도우 시스템 설정** 옵션을 체크하여 X 윈도우 시스템을 설정 가능합니다. 이 옵션이 선택되지 않으면, X 윈도우 설정 옵션이 비활성화되고 `skipx` 옵션이 킥스타트 파일에 쓰여집니다.

8.8.1. 일반

X 설정을 위한 첫번째 단계는 디폴트 색상도와 해상도를 선택하는 것입니다. 각각의 풀다운 메뉴에서 색상도와 해상도를 선택하십시오. 시스템 상의 비디오 카드 및 모니터와 호환 가능한 색상도와 해상도를 지정하셔야 합니다.

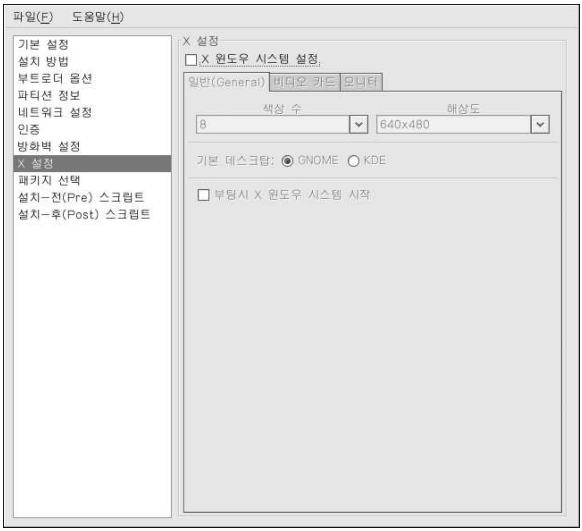

그림 8-11. X 설정 - 일반

만일 GNOME과 KDE 데스크탑을 모두 설치하신다면, 어느 데스크탑이 디폴트가 될 것인지 선택하셔야 합니다. 만일 한개의 데스크탑만 설치하신다면, 그 데스크탑을 디폴트로 선택합니다. 일단 시스템 설치를 마치면, 사용자는 어느 데스크탑을 기본으로 사용할 지 선택하실 수 있습니다. GNOME과 KDE에 대한 보다 자세한 정보를 원하신다면, *Red Hat Linux* 설치 가이드와 *Red Hat Linux* 시작하기 가이드를 참조하시기 바랍니다.

다음으로 시스템이 부팅될 때 X 윈도우 시스템을 시작할 것인지 여부를 선택합니다. 이 옵션은 시스템을 그래픽 로그인 스크린과 함께 런레벨 5에서 시스템을 시작합니다. 시스템이 설치가 끝난 후 `/etc/inittab` 설정 파일을 수정하여 이것을 변경할 수 있습니다.

8.8.2. 비디오 카드

비디오 카드 검색 옵션은 디폴트로 선택되어 집니다. 이 디폴트 값을 수용하여 설치 프로그램이 설치 과정에서 비디오 카드를 검색하도록 하십시오. 만일 옵션이 선택된 경우, 설치 프로그램이 성공적으로 비디오 카드를 검색하지 못했다면, 비디오 카드 설정 화면에서 설치가 멈출 것입니다. 설치를 계속 진행하시려면, 목록에서 여러분이 가지고 계신 비디오 카드를 선택하시고 **다음** 버튼을 클릭하시기 바랍니다.

그림 8-12에서 볼 수 있듯이 **비디오 카드** 탭에 있는 목록에서 비디오 카드를 선택하시는 방법도 있습니다. **비디오 카드 RAM** 풀다운 메뉴에서 선택된 비디오 카드의 비디오 RAM 용량을 지정해 주십시오. 이 값은 설치 프로그램이 X 윈도우 시스템을 설정하는데 사용됩니다.

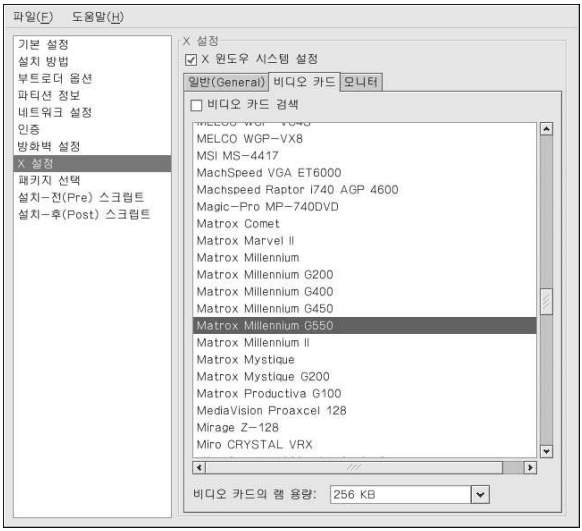

그림 8-12. X 설정 - 비디오 카드

8.8.3. 모니터

비디오 카드를 설정하신 후, 그림 8-13에서 보여지는 **모니터** 탭을 클릭하시기 바랍니다.

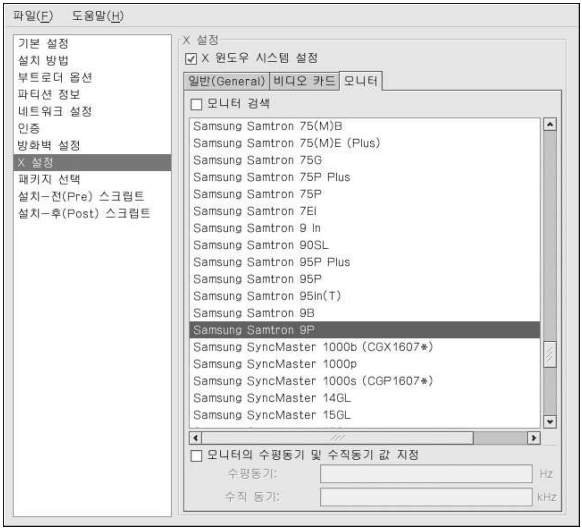

그림 8-13. X 설정 - 모니터

모니터 검색 옵션은 디폴트로 선택됩니다. 이 디폴트 값을 수용하여 설치 프로그램이 설치 과정에서 모니터를 검색하도록 하십시오. 검색 작업을 통해 대부분의 최신 모니터를 검색 가능합니다. 만일 옵션이 선택된 경우 설치 프로그램이 성공적으로 모니터를 검색하지 못한다면, 설치 프로그램은 모니터 설정 화면에서 멈출 것입니다. 설치를 계속 진행하시려면, 목록에서 모니터를 선택하신 후 **다음** 버튼을 클릭하시면 됩니다.

목록에서 모니터를 선택하시는 방법도 있습니다. 특정 모니터를 선택하는 대신 **모니터의 수평동기 및 수직동기 값 지정** 옵션을 선택하여 수평동기 및 수직동기 값을 지정하실 수 있습니다. 시스템에 사용된 모니터가 목록에 없을 경우 이 옵션이 유용합니다. 이 옵션이 활성화되면, 모니터 목록이 비활성화되는 것에 주목해 주십시오.

8.9. 패키지 선택

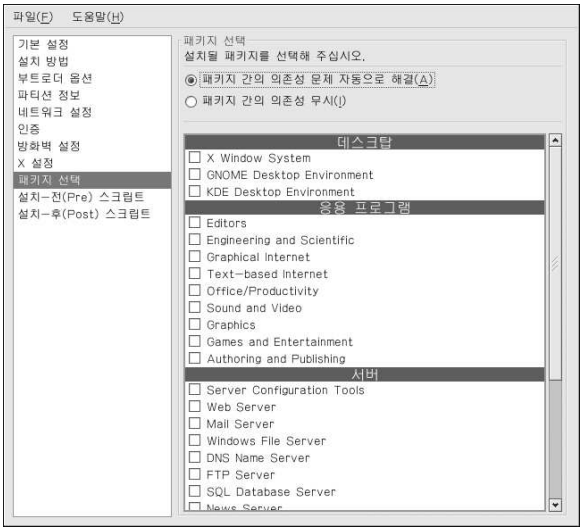

그림 8-14. 패키지 선택

패키지 선택 창에서 여러분은 설치할 패키지 그룹을 선택하실 수 있습니다.

패키지 간의 의존성을 자동으로 해결하는 옵션과 패키지 간의 의존성을 무시하는 옵션이 있습니다.

현재 **킥스타트 설정 프로그램**에서 개별 패키지 선택이 불가능합니다. 개별 패키지를 설치하시려면, 킥스타트 파일을 저장하신 후 킥스타트 파일의 %packages 섹션을 수정하시기 바랍니다. 자세한 정보는 7.5 절을 참조하시기 바랍니다.

8.10. 설치-이전 스크립트

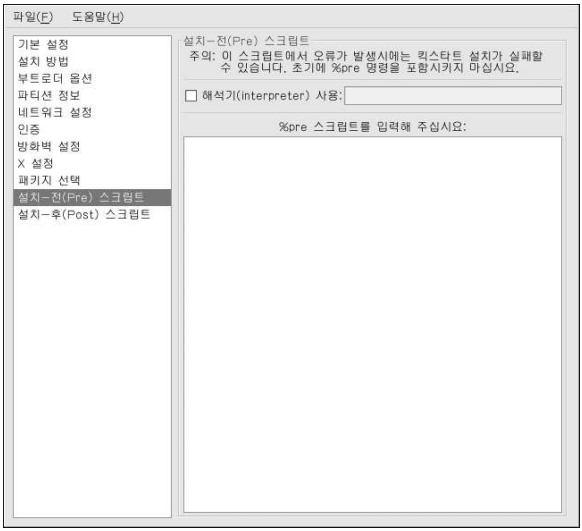

그림 8-15. 설치-이전 스크립트

킥스타트 파일이 구문 분석된 직후와 설치가 시작하기 직전에 시스템 상에서 실행될 명령어를 추가하실 수 있습니다. 만일 킥스타트 파일에서 네트워크를 설정하셨다면, 이 섹션이 처리되지 이전에 네트워크가 활성화될 것입니다. 설치-이전 스크립트를 포함시키기를 원하신다면, 입력란에 스크립트를 입력하십시오.

스크립트를 실행할 스크립팅 언어를 지정하시려면, **해석기 사용** 버튼을 선택하신 후 버튼 옆에 위치한 입력란에 해석기를 입력하십시오. 예를 들어 Python 스크립트를 사용하시려면, **/usr/bin/python2.2**를 지정하시면 됩니다. 이 옵션은 킥스타트 파일에서 `%pre --interpreter` */usr/bin/python2.2*을 사용하는 것과 같습니다.

경고

`%pre` 명령은 포함시키지 마십시오. 이 명령은 여러분을 위해 자동으로 추가될 것입니다.

8.11. 설치-이후 스크립트

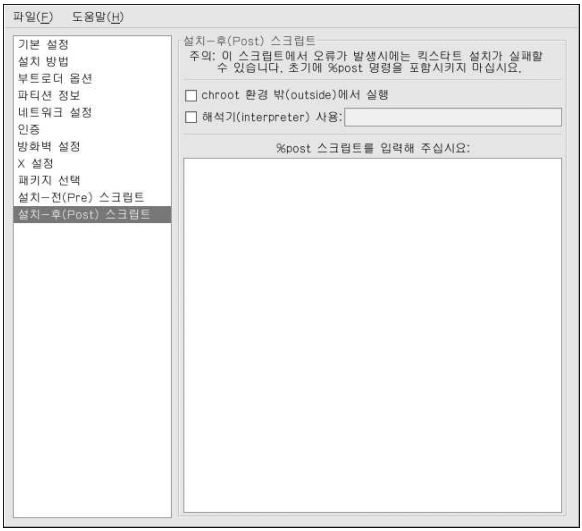

그림 8-16. 설치-이후 스크립트

여러분은 또한 설치가 끝난 후 시스템 상에서 실행될 명령어를 추가하실 수 있습니다. 만일 킥스타트 파일에서 네트워크를 적절하게 설정하셨다면, 네트워크가 활성화될 것입니다. 설치-이후 스크립트를 포함시키려면, 입력란에 스크립트를 입력하십시오.

경고

`%post` 명령은 포함시키지 마십시오. 이 명령은 여러분을 위해 자동으로 추가될 것입니다.

예를 들어 새로이 설치된 시스템을 위한 오늘의 메시지를 변경시키기 위해서는, `%post` 섹션에 다음과 같은 명령을 추가하십시오:

```
echo "Hackers will be punished!" > /etc/motd
```

힌트

보다 많은 예시는 7.7.1 절에서 찾으실 수 있습니다.

8.11.1. Chroot 환경

chroot 환경 외부에서 설치-후 스크립트를 실행하시려면, **설치-후** 화면 상단의 이 옵션 옆에 위치한 체크박스를 클릭하시기 바랍니다. 이 방법은 `%post` 섹션에서 `--nochroot` 옵션을 사용하는 것과 같습니다.

만일 chroot 환경 바깥의 설치-이후 섹션에 존재하는 새로 설치된 파일 시스템에 변화를 주고 싶다면, 디렉토리 이름에 /mnt/sysimage를 덧붙여야 합니다.

예를 들어 만일 **chroot 환경 밖(outside)에서 실행** 옵션을 선택하신다면, 위에서 언급된 예시는 다음과 같이 바뀌어야 합니다:

```
echo "Hackers will be punished!" > /mnt/sysimage/etc/motd
```

8.11.2. 해석기 사용

스크립트를 실행할 스크립팅 언어를 지정하시려면, **해석기 사용** 버튼을 선택하신 후 버튼 옆에 위치한 입력란에 해석기를 입력하십시오. 예를 들어 Python 스크립트를 사용하시려면, **/usr/bin/python2.2**를 지정하시면 됩니다. 이 옵션은 킥스타트 파일에서 %post --interpreter */usr/bin/python2.2*을 사용하는 것과 같습니다.

8.12. 파일 저장하기

킥스타트 옵션 선택을 마치신 후, 풀다운 메뉴에서 **파일** => **미리 보기**를 선택하여 파일을 저장하기 전에 선택하신 사항들을 재검토하실 수 있습니다.

그림 8-17. 미리 보기

킥스타트 파일을 저장하시려면, 미리보기 창에서 **파일로 저장** 버튼을 클릭하시기 바랍니다. 미리 보기할 필요 없이 바로 파일을 저장하시려면, **파일** => **파일 저장**을 선택하시거나 [Ctrl]-[S]를 누르시면 됩니다. 나타난 대화 상자에서 파일을 저장할 위치를 선택해 주십시오.

파일을 저장하신 후, 킥스타트 설치를 시작하는 방법에 대한 정보를 원하신다면 7.10 절을 참조하시기 바랍니다.

9장 . 기초 시스템 복구

갑자기 시스템에 문제가 발생하는 경우, 여러 가지 방법으로 문제를 해결하실 수 있습니다. 그러나 우선 여러분이 시스템을 잘 이해하고 계셔야 문제 해결이 가능합니다. 따라서 이 장에서는 여러분이 알고 있는 지식에 기초하여 시스템을 복구할 수 있는 능력을 키울 수 있도록 복구 모드, 단독 사용자 모드와 비상 모드로 부팅하는 방법에 대하여 다루어 보겠습니다.

9.1. 자주 발생하는 문제들

일반적으로 다음과 같은 경우에 복구 모드로 부팅하셔야 합니다:

- Red Hat Linux (런레벨 3이나 5)로 부팅할 수 없는 경우.
- 하드웨어나 소프트웨어에 문제가 발생하여, 시스템 하드 드라이브에서 몇몇 중요한 파일을 빼내오려고 하는 경우.
- 루트 암호를 잊어버린 경우.

9.1.1. Red Hat Linux를 부팅할 수 없을 때

Red Hat Linux를 설치 후 다른 운영 체제를 설치하신 경우 이러한 문제가 종종 발생하곤 합니다. 일부 다른 운영 체제는 시스템 상에 다른 운영 체제가 존재하지 않는다고 가정하고서 GRUB이나 LILO 부트로더를 포함한 마스터 부트 레코드 (MBR)를 덮어씁니다. 이러한 방법으로 부트로더가 덮여 쓰여지면, 복구 모드로 들어가서 부트로더를 재설정하지 않는 한 Red Hat Linux를 부팅할 수 없게 됩니다.

또한 설치를 마친 후 파티션 도구를 사용하여 파티션의 크기를 재조정하거나 여유 공간에서 새 파티션을 생성하는 경우 이러한 문제가 자주 발생하기도 합니다. 만일 / 파티션의 파티션 번호가 변경된다면, 부트로더가 파티션을 마운트할 지점을 찾지 못하게 됩니다. 이러한 문제를 해결하기 위해서는, 복구 모드로 부팅하신 후 GRUB을 사용하신다면 `/boot/grub/grub.conf` 파일을 수정하시고 LILO를 사용하신다면 `/etc/lilo.conf` 파일을 수정하시기 바랍니다. 여러분은 또한 LILO 설정 파일을 수정하실 때마다 반드시 `/sbin/lilo` 명령을 실행하셔야 합니다.

9.1.2. 하드웨어/소프트웨어 문제

여러가지 상황에서 하드웨어/소프트웨어 문제가 발생할 수 있습니다. 두가지 예로 들면, 하드 드라이브가 실패하거나 부트로더 설정 파일에서 잘못된 루트 장치나 커널을 지정하는 경우가 있습니다. 이러한 상황이 발생한다면, Red Hat Linux로 부팅할 수 없게 됩니다. 그러나 시스템 복구 모드 중 한 가지 모드로 부팅하실 수만 있다면, 문제를 해결할 수 있거나 최소한 중요한 파일들의 복사본을 건질 수 있습니다.

9.1.3. 루트 암호

루트 암호를 기억할 수 없을 때, 여러분은 어떻게 하시겠습니까? 다른 루트 암호를 설정하시려면, 복구 모드나 단독 사용자 모드로 부팅하신 후 `passwd` 명령을 사용하여 루트 암호를 재설정하실 수 있습니다.

9.2. 복구 모드로 부팅하기

복구 모드는 전적으로 디스켓, CD-ROM 이나 또는 시스템 하드 드라이브 대신 그외 다른 방법을 사용하여 작은 Red Hat Linux 환경으로 부팅할 수 있는 기능을 제공합니다.

복구 모드는 이름 그대로 무엇인가를 복구시켜 줍니다. Red Hat Linux 시스템은 하드 드라이브 상에 위치한 파일을 사용하여 모든 일반적인 작업 — 프로그램 실행, 파일 저장과 같은 작업을 실행합니다.

그러나 가끔씩 Red Hat Linux가 제대로 실행되지 않아서 시스템 하드 드라이브 상에 위치한 파일에 접근하지 못할 경우가 있습니다. 이러한 경우, 하드 드라이브에서 Red Hat Linux를 실행하지 못한다고 해도 복구 모드를 사용하여 그 하드 드라이브 상에 저장된 파일에는 접근할 수 있습니다.

복구 모드로 부팅하시려면, 우선 다음 중 한가지 방법을 사용하여 시스템을 부팅하셔야 합니다:

- `bootdisk.img` 이미지로 만든 설치 부팅 디스켓으로 시스템을 부팅하는 방법. [1]
- 설치 부팅 CD-ROM으로 시스템을 부팅하는 방법. [2]
- Red Hat Linux CD-ROM #1으로 시스템을 부팅하는 방법.

앞에서 설명된 방법을 사용하여 부팅하신 후, 설치 부트 프롬프트에서 다음 명령을 입력하시기 바랍니다:

```
linux rescue
```

몇몇 기본적인 질문, 예로 들면, 사용할 언어 선택 질문에 대답하신 후 **로컬 CD-ROM**, **하드 드라이브**, **NFS 이미지**, **FTP**, 또는 **HTTP** 중 올바른 복구 이미지가 위치한 장소를 선택해 주십시오. 선택하신 위치에 반드시 올바른 설치 트리가 있어야 하며, 이 설치 트리에는 부팅하는데 사용한 Red Hat Linux CD-ROM #1의 Red Hat Linux와 동일한 버전의 Red Hat Linux가 있어야 합니다. 복구 모드를 시작하기 위해 부팅 CD-ROM이나 디스켓을 사용하셨다면, 설치 트리는 이 부팅 매체가 만들어진 동일한 트리여야 합니다. 하드 드라이브, NFS 서버, FTP 서버, HTTP 서버에 설치 트리를 설정하는 방법에 대한 자세한 정보를 원하신다면, *Red Hat Linux* 설치 가이드를 참조하시기 바랍니다.

네트워크에 연결할 필요가 없는 복구 이미지를 선택하시면, 네트워크에 연결하실 것인지 여부를 물어볼 것입니다. 다른 컴퓨터에 파일을 백업하거나 공유 네트워크에서 RPM 패키지를 설치하시는 경우에는 네트워크에 연결하는 것이 유용합니다.

다음과 같은 메시지가 나타날 것입니다:

```
The rescue environment will now attempt to find your Red Hat
Linux installation and mount it under the directory
/mnt/sysimage. You can then make any changes required to your
system. If you want to proceed with this step choose
'Continue'. You can also choose to mount your file systems
read-only instead of read-write by choosing 'Read-only'.
If for some reason this process fails you can choose 'Skip'
and this step will be skipped and you will go directly to a
command shell.
```

계속 버튼을 클릭하시면, `/mnt/sysimage` 디렉토리에 여러분의 파일 시스템을 마운트하려고 시도할 것입니다. 만일 파티션을 마운트하는 것에 실패한다면, 여러분께 실패를 통지합니다. **읽기 전용** 버튼을 선택하시면, 읽기 전용 모드로 `/mnt/sysimage` 디렉토리에 파일 시스템을 마운트 시도할 것입니다. **건너뛰기** 버튼을 선택하시면, 파일 시스템을 마운트하지 않습니다. 만일 파일 시스템이 손상되었다고 생각하시면 **건너뛰기**를 선택하십시오.

일단 시스템이 복구 모드로 들어가시면, VC (가상 콘솔) 1과 VC 2 상에 다음과 같은 프롬프트가 나타날 것입니다. (VC1에 접속하시려면 [Ctrl]-[Alt]-[F1] 키 조합을 사용하시고 VC 2에 접속하기 위해서는 [Ctrl]-[Alt]-[F2] 키 조합을 사용하십시오):

```
-/bin/sh-2.05b#
```

파티션을 자동 마운트하기 위하여 **다음** 버튼을 선택한 후 그 파티션들이 성공적으로 마운트되었다면, 단독 사용자 모드가 됩니다.

---

1. 설치 부팅 디스켓을 만드시려면, 공 디스켓을 삽입하신 후 `dd if=bootdisk.img of=/dev/fd0` 명령을 사용하여 Red Hat Linux CD-ROM #1에 있는 `images/bootdisk.img` 파일을 사용합니다.
2. 설치 부팅 CD-ROM을 만드시려면, *Red Hat Linux* 설치 가이드에서 자세한 내용을 참조하시기 바랍니다.

파일 시스템이 마운트되었더라도, 복구 모드에서 디폴트 루트 파티션은 일반 사용자 모드 (런레벨 3 또는 5)에서 사용되는 파일 시스템의 루트 파티션이 아닌 임시 루트 파티션입니다. 만일 파일 시스템을 마운트하도록 선택하신 후 성공적으로 마운트되었다면, 다음 명령을 사용하여 복구 모드 환경에서의 루트 파티션을 파일 시스템의 루트 파티션으로 변경하실 수 있습니다:

```
chroot /mnt/sysimage
```

이렇게 하시면, 루트 파티션이 `/`로 마운트되어야 실행할 수 있는 `rpm`과 같은 명령을 실행하는데 유용합니다. chroot 환경에서 빠져나오려면, `exit` 명령을 입력하여 프롬프트로 되돌아갈 수 있습니다.

건너뛰기 버튼을 선택하신 경우, 복구 모드에서 */foo*와 같은 디렉토리를 생성한 후 다음과 같은 명령을 입력하여, 직접 파티션을 마운트 시도하실 수 있습니다:

```
mount -t ext3 /dev/hda5 /foo
```

위의 명령에서 */foo*는 여러분이 만드신 디렉토리이며 */dev/hda5*는 마운트할 파티션을 의미합니다. 만일 파티션이 `ext2` 형식이라면, `ext3`를 `ext2`로 바꾸시면 됩니다.

만일 여러분이 가지고 계신 파티션의 이름이 확실하지 않다면, 다음의 명령어를 이용하여 파티션 목록을 보실 수 있습니다:

```
fdisk -l
```

프롬프트에서 다음과 같이 많은 유용한 명령을 실행 가능합니다:

- `list-harddrives` 명령은 시스템 내의 하드 드라이브 목록을 보여줍니다
- 네트워크에 연결된 경우에는 `ssh`,`scp`, `ping`명령을 사용 가능합니다
- 테이프 장치를 가진 사용자는 `dump`와 `restore` 명령을 사용 가능합니다.
- `parted`와 `fdisk`는 파티션을 관리하는데 사용됩니다
- `rpm`은 소프트웨어를 설치하고 업그레이드하는데 사용됩니다
- `joe` 명령은 설정 파일을 수정하는데 사용됩니다 (`joe`, `emacs`, `pico`, 또는 `vi` 명령을 입력하시면 `joe` 편집기가 시작됩니다.)

9.3. 단독 사용자 모드로 부팅하기

단독 사용자 모드를 사용하는 장점 중의 하나는 디스켓이나 CD-ROM으로 부팅할 필요가 없다는 것입니다; 그러나, 파일 시스템을 읽기 전용으로 마운트하거나 아예 마운트할 수 있는 옵션이 주어지지 않습니다.

단독 사용자 모드에서는, 컴퓨터가 런레벨 1로 부팅합니다. 지역 파일 시스템은 마운트되지만, 네트워크는 활성화되지 않습니다. 따라서 여러분은 사용 가능한 시스템 관리 쉘을 갖게 됩니다. 복구 모드와는 달리, 단독 사용자 모드는 자동으로 파일 시스템을 마운트 시도합니다; 파일 시스템이 성공적으로 마운트될 수 없는 상황에서는 단독 사용자 모드를 사용하지 마십시오. 시스템 상의 런레벨 1 설정이 손상되었을 경우 단독 사용자 모드를 사용하실 수 없습니다.

시스템 부팅이 완료된 후에도 로그인할 수 없다면, 단독 사용자 모드를 사용해 보십시오.

GRUB을 사용하신다면 다음과 같은 과정을 사용하여 단독 사용자 모드로 부팅하십시오:

1. GRUB 암호를 이미 설정하셨다면, `p` 명령을 입력 후 암호를 입력하시기 바랍니다.
2. 부팅하려는 커널 버전을 가진 **Red Hat Linux**를 선택하신 후 편집을 위해 `e` 키를 누르시기 바랍니다. 여러분이 선택하신 이름에 대한 설정 파일에 포함된 항목 목록이 나타날 것입니다.
3. `kernel`로 시작하는 줄을 선택하신후 편집을 위하여 `e` 명령을 입력합니다.
4. 그 줄의 끝으로 가셔서 **`single`**을 벌개의 단어 로 입력 ([Spacebar]를 누르고 나서 **`single`**을 입력)해 주십시오. 편집 모드를 종료하시려면 [Enter] 키를 누르십시오.

5. GRUB 화면으로 되돌아가서 단독 사용자 모드로 부팅하기 위해 `b` 명령을 입력해 주십시오.

LILO를 사용하시는 경우, LILO 부트 프롬프트에서 다음과 같이 입력해 주십시오. (그래픽 LILO를 사용하신다면, [Ctrl]-[x] 키를 눌러 그래픽 화면에서 종료하고 `boot:` 프롬프트로 갑니다):

```
linux single
```

9.4. 비상 모드로 부팅하기

비상 모드에서는 가능한 최소 환경으로 부팅합니다. 루트 파일 시스템은 읽기 전용으로 마운트될 것이며 그 외에는 거의 아무것도 설정되지 않습니다. 단독 사용자 모드와 비교하여 비상 모드의 중요한 장점은 `init` 파일이 로드되지 않는다는 것입니다. 만일 `init` 파일이 손상되었거나 작동되지 않는 경우에도, 비상 모드에서는 파일 시스템을 마운트하여 재설치 과정에서 잃은 자료를 복구 가능합니다.

비상 모드로 부팅하시려면, 9.3 절에서 설명된 단독 사용자 모드로 부팅하는 것과 동일한 방법을 사용하시면 됩니다. 단 한가지 차이점은 **`single`** 키워드를 **`emergency`** 키워드로 바꿔주시면 됩니다.

10장 . 소프트웨어 RAID 설정

RAID에 대한 기본적인 정보와 하드웨어와 소프트웨어 RAID의 차이점, 그리고 RAID 0, 1, 5 간의 차이점을 알아보기 위하여 3 장을 먼저 읽어보시기 바랍니다.

Red Hat Linux의 그래픽 설치나 킥스타트 설치 과정에서 소프트웨어 RAID를 설정 가능합니다. 이 장에서는 설치 과정에서 **Disk Druid** 인터페이스를 사용하여 소프트웨어 RAID를 설정하는 방법에 대하여 설명해 보겠습니다.

RAID 장치를 생성하기 이전에 먼저 RAID 파티션을 만드셔야 합니다. 다음에 나온 단계별 지시 사항을 따르시기 바랍니다:

1. **드라이브 파티션 설정** 화면에서 **Disk Druid를 통한 수동 파티션 설정**을 선택해 주십시오.
2. **Disk Druid**에서 새로운 파티션을 생성하기 위하여 **새로생성** 버튼을 선택하시기 바랍니다.
3. 아직 마운트 지점을 입력하실 수 없습니다. (일단 RAID 장치를 생성하시면 마운트 지점을 입력 가능합니다.)
4. 그림 10-1에서 볼 수 있듯이, **파일 시스템 유형** 풀다운 메뉴에서 **소프트웨어 RAID**를 선택해 주십시오.

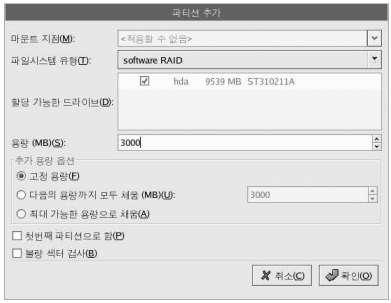

그림 10-1. 새로운 RAID 파티션 생성하기

5. **할당 가능한 드라이브**에서 RAID가 생성될 드라이브를 선택해 주십시오. 다중 드라이브를 가지고 계신 경우, 모든 드라이브가 선택됩니다. 이 드라이브 중에서 RAID 어레이가 없는 드라이브는 선택 해제하셔야 합니다.
6. 여러분이 원하시는 파티션의 크기를 입력하십시오.
7. 파티션을 특정 용량으로 지정하시려면 **고정 용량** 항목을 선택하십시오. **다음의 용량까지 모두 채움 (MB)** 항목을 선택하신다면 파티션 용량의 범위를 MB 단위로 입력해 주십시오. 만일 하드 디스크 상에서 사용 가능한 공간을 모두 채울 때까지 파티션이 증가하도록 하시려면, **최대 가능한 용량으로 채움** 항목을 선택하시기 바랍니다. 최대 가능한 용량으로 채울 때까지 증가할 파티션을 한개 이상 만드신다면, 이 파티션들은 디스크 상의 사용 가능한 공간을 공유합니다.
8. 파티션을 첫번째 파티션으로 만드시려면 **첫번째 파티션으로 함** 항목을 선택해 주십시오.
9. 만일 설치 프로그램이 하드 드라이브를 포맷하기 전에 불량 섹터를 검사하도록 하시려면, **불량 섹터 검사** 항목을 선택하십시오.
10. **확인** 버튼을 클릭하시면 기본 화면으로 되돌아 갑니다.

RAID 설정에 필요한 파티션을 모두 생성할 때까지 이러한 과정을 계속 반복하십시오. 모든 파티션이 RAID 파티션일 필요는 없습니다. 예로 들면, /home 파티션만 소프트웨어 RAID 장치로 설정하는 수 있습니다.

일단 모든 파티션을 **소프트웨어 RAID**로 생성하셨다면, 다음과 같은 과정을 따르십시오:

1. **Disk Druid** 주 파티션 화면(그림 10-3 참조) 에서 **RAID** 버튼을 선택해 주십시오.
2. 이제 그림 10-2이 나타날 것입니다. 이 화면에서 RAID 장치를 설정하실 수 있습니다.

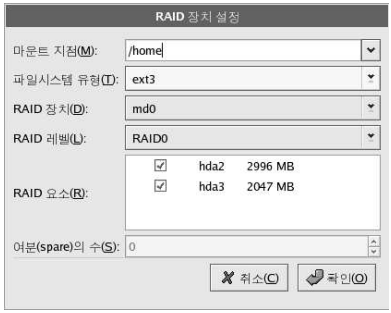

그림 10-2. RAID 장치 설정하기

3. 먼저 마운트할 지점을 입력해 주십시오.
4. 다음으로 파티션에 사용될 파일 시스템 유형을 선택해 주십시오.
5. RAID 장치에 사용될 이름 (예, **md0**)을 선택하시기 바랍니다.
6. RAID 레벨을 선택해 주십시오. **RAID 0**, **RAID 1**, **RAID 5** 중 하나를 선택하시면 됩니다.

알림

/boot의 RAID 파티션을 만드신다면, RAID 레벨 1을 선택하셔야 하며, 이 파티션은 첫 두 개의 드라이브 (첫번째 IDE, 두번째 SCSI) 중 한 개를 사용해야 합니다. 만일 /boot의 RAID 파티션을 생성하지 않고 /의 RAID 파티션을 설정하신다면, 마찬가지로 RAID 레벨 1을 선택하셔야 하며, 이 파티션은 첫 두 개의 드라이브 (첫번째 IDE, 두번째 SCSI) 중 한 개를 사용해야 합니다.

7. 여러분이 방금 생성하신 RAID 파티션이 **RAID 요소** 목록에 나타날 것입니다. 이 파티션 중에서 RAID 장치를 생성하는데 사용될 파티션을 선택해 주시기 바랍니다.
8. RAID 1이나 RAID 5를 설정하시는 경우, 여유 파티션의 숫자를 지정해 주십시오. 만일 소프트웨어 RAID 파티션이 실패할 경우, 여유 파티션이 자동으로 대체로 사용됩니다. 지정하시려는 각 여유 파티션마다, (RAID 장치에 사용되는 파티션을 비롯한) 추가 소프트웨어 RAID 파티션을 생성해 주셔야 합니다. 이전 단계에서, RAID 장치에 사용될 파티션과 여유 파티션에 사용될 파티션을 선택하시기 바랍니다.
9. **확인** 버튼을 클릭하시면 그림 10-3에서 보여지는 것처럼 RAID 장치가 **드라이브 요약** 목록에 나타납니다. 이제 설치 과정을 계속 진행하실 수 있습니다. 보다 많은 정보를 원하신다면, *Red Hat Linux* 설치 가이드를 참조하시기 바랍니다.

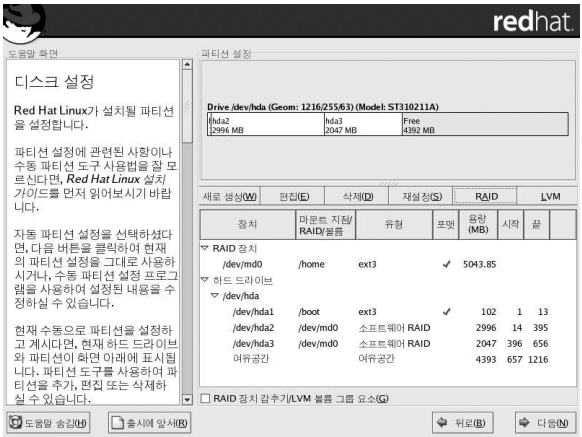

그림 10-3. 생성된 RAID 어레이

11장 .

LVM 설정

Red Hat Linux의 그래픽 설치 과정이나 킥스타트 설치 과정에서 LVM 설정이 가능합니다. `lvm` 패키지에 들어있는 유틸리티를 사용하여 LVM을 설정하실 수 있지만, 이 장에서는 Red Hat Linux 설치 과정에서 **Disk Druid**를 사용하여 LVM을 설정하는 방법에 대하여 중점을 두고 설명해 보겠습니다.

먼저 LVM에 대한 정보를 얻기 위하여 4 장을 읽어 보시기 바랍니다. LVM을 설정하는 기본 과정은 다음과 같습니다:

- 하드 드라이브에서 물리적 볼륨을 생성합니다.
- 만들어진 물리적 볼륨에서 볼륨 그룹을 생성합니다.
- 이제 각각의 볼륨 그룹에서 논리 볼륨을 생성하신 후 그 논리 볼륨에 마운트할 지점을 부여합니다.

알림

GUI 설치 모드에서만 LVM 볼륨 그룹을 편집하실 수 있습니다. 텍스트 설치 모드에서는 기존 논리 볼륨에 마운트할 지점을 부여하실 수 있습니다.

Red Hat Linux 설치 과정에서 논리 볼륨을 사용하여 논리 볼륨 그룹을 생성하시려면, 다음과 같은 단계를 따르십시오:

1. **드라이브 파티션 설정** 화면에서 **Disk Druid를 통한 수동 파티션 설정**을 선택해 주십시오.
2. 다음으로 **새로생성** 버튼을 선택하시기 바랍니다.
3. 아직 마운트할 지점을 입력하실 수 없습니다 (일단 볼륨 그룹을 생성하시면 마운트할 지점을 입력 가능합니다).
4. 그림 11-1에서 보여지듯이, **파일 시스템 유형** 풀다운 메뉴에서 **물리적 볼륨 (LVM)**을 선택하시기 바랍니다.

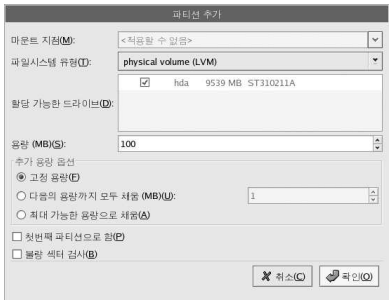

그림 11-1. 물리적 볼륨 생성하기

5. 물리적 볼륨은 반드시 한 개의 드라이브에 할당되어야 합니다. **할당 가능한 드라이브**에서 물리적 볼륨을 생성할 드라이브를 선택해 주십시오. 다중 드라이브를 가지고 계신 경우, 모든 드라이브가 선택됩니다. 여러분은 선택된 드라이브 중에서 한 개만 빼고 모두 선택 해제하셔야 합니다.
6. 원하시는 물리적 볼륨의 크기를 입력하십시오.
7. 물리적 볼륨을 특정 용량으로 지정하시려면 **고정 용량** 항목을 선택하십시오. **다음의 용량까지 모두 채움 (MB)** 항목을 선택하신다면 물리적 볼륨 용량의 범위를 MB 단위로 입력해 주십시오. 만일 하드 디스크 상에서 사용 가능한 공간을 모두 채울 때까지 물리적 볼륨이 증가하도록 하시려면, **최대 가능한 용량으로 채움** 항목을 선택하시기 바랍니다. 최대 가능한 용량으로 채울 때까지 증가할 물리적 볼륨을 한개 이상 지정하신다면, 이 물리적 볼륨들은 디스크 상의 사용 가능한 공간을 공유하게 됩니다.
8. 이 파티션을 첫번째 파티션으로 만드시려면 **첫번째 파티션으로 함** 항목을 선택해 주십시오.
9. 만일 설치 프로그램이 하드 드라이브를 포맷하기 전에 불량 섹터를 검사하도록 하시려면, **불량 섹터 검사** 항목을 선택하십시오.
10. **확인** 버튼을 클릭하시면 기본 화면으로 되돌아 갑니다.

LVM 설정에 필요한 물리적 볼륨을 모두 생성하실 때까지 이 과정을 계속 반복하십시오. 예를 들어 볼륨 그룹이 한 개 이상의 드라이브에 걸쳐 작성되도록 하시려면, 각각의 드라이브에 물리적 볼륨을 생성하셔야 합니다.

경고

부트로더는 논리 볼륨 그룹을 읽지 못하기 때문에 `/boot` 파티션은 논리 볼륨 그룹에 위치할 수 없습니다. 만일 루트 `/` 파티션을 논리 볼륨에 놓기를 원하신다면, 볼륨 그룹에 속하지 않는 별개의 `/boot` 파티션을 생성하셔야 합니다.

일단 모든 물리적 볼륨을 생성하셨다면, 다음과 같은 과정을 따르십시오:

1. **LVM** 버튼을 클릭하여 물리적 볼륨들을 합쳐서 하나의 볼륨 그룹으로 만듭니다. 기본적으로 하나의 볼륨 그룹은 물리적 볼륨들의 집합입니다. 여러 개의 볼륨 그룹을 갖는 것은 가능하지만, 물리적 볼륨은 한번에 하나의 볼륨 그룹에만 존재합니다.

알림

논리 볼륨 그룹에는 오버헤드 디스크 공간이 보존되어 있습니다. 물리적 볼륨의 총량은 볼륨 그룹의 용량과 동일하지 않을 수도 있습니다; 하지만 보이는 논리 볼륨의 용량은 맞습니다.

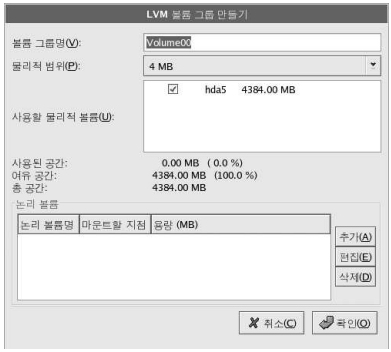

그림 11-2. LVM 장치 생성하기

2. 필요하다면 **볼륨 그룹명**을 변경해 주십시오.
3. 볼륨 그룹에 속한 모든 논리 볼륨은 물리적 범위 *(physical extent)* 단위로 할당되어야 합니다. 디폴트 값으로, 물리적 범위는 4 MB로 설정되어 있습니다; 따라서 논리 볼륨은 4 MB 크기로 나누어져야 합니다. 만일 4 MB 단위가 아닌 용량을 입력하시면, 설치 프로그램은 자동으로 4 MB와 가장 근접한 용량을 선택합니다. 이 설정을 변경하시지 마십시오.
4. 볼륨 그룹에 사용할 물리적 볼륨을 선택해 주십시오.
5. `/home`와 같은 마운트 지점을 지닌 논리 볼륨을 생성하십시오. `/boot`는 논리 볼륨이 될 수 없다는 사실을 기억해 주시기 바랍니다. 논리 볼륨을 추가하시려면 **논리 볼륨** 섹션에서 **추가** 버튼을 클릭해 주십시오. 그림 11-3에서 보이는 것과 같은 대화 상자가 나타날 것입니다.

그림 11-3. 논리 볼륨 생성하기

생성하시려는 볼륨 그룹 마다 이 과정을 반복하십시오.

힌트

나중에 논리 볼륨을 확장할 수 있도록 논리 볼륨 그룹에 약간의 여유 공간을 남겨 두시는 것이 좋습니다.

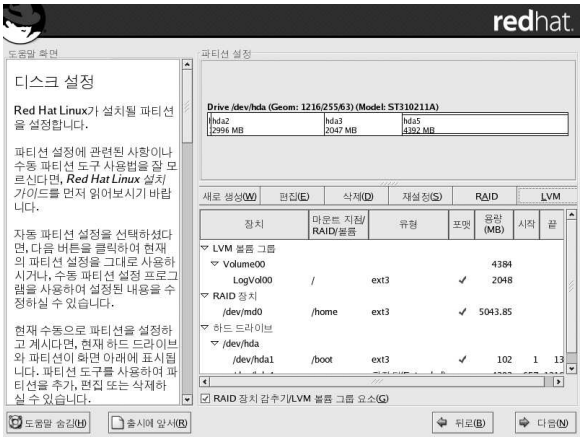

그림 11-4. 논리 볼륨 생성됨

III. 네트워크-관련 설정

네트워크 설정 방법에 대한 설명을 마친 후, 이 장에서는 원격 로그인하기와 네트워크 상에서 파일과 디렉토리 공유하기 및 웹 서버를 설정하기와 같은 네트워킹 관련 사항들을 다루고 있습니다.

차례

12장 .

네트워크 설정

컴퓨터는 네트워크에 연결되어 다른 컴퓨터와 통신을 주고 받습니다. 네트워크로 컴퓨터를 연결하기 위해서는 인터페이스 카드 (예, 이더넷, ISDN, 모뎀, 토큰 링)을 인식하는 운영 체제에서 네트워크 인터페이스를 설정하시면 됩니다.

네트워크 관리 도구를 사용하여 다음과 같은 유형의 네트워크 인터페이스를 설정 가능합니다:

- 이더넷 (Ethernet)
- ISDN
- 모뎀
- xDSL
- 토큰 링
- CIPE
- 무선 장치

네트워크 관리 도구를 사용하시려면, 루트 권한을 가지고 계셔야 합니다. 이 응용 프로그램을 시작하시려면, 패널에서 **주 메뉴 버튼** => **시스템 설정** => **네트워크**로 가시거나 쉘 프롬프트 (예, **XTerm** 또는 **GNOME 터미널**)에서 `redhat-config-network` 명령을 입력하시면 됩니다. X가 실행 중이라면 명령 입력 후 그래픽 버전이 실행될 것이며, 그렇지 않다면 텍스트 버전이 시작됩니다. 텍스트 기반 버전을 실행하시려면, `redhat-config-network-tui` 명령을 사용하시기 바랍니다.

그림 12-1. 네트워크 관리 도구

설정 파일을 직접 수정하기를 원하신다면, *Red Hat Linux* 참조 가이드에서 설정 파일의 위치와 내용에 대한 정보를 참조하시기 바랍니다.

힌트

여러분이 가지고 계신 하드웨어 장치가 Red Hat Linux에서 지원되는지 알아보기 위하여 Red Hat 하드웨어 호환성 목록을 살펴보시기 바랍니다. (http://hardware.redhat.com/hcl/)

12.1. 개요

네트워크 관리 도구를 사용하여 네트워크 연결을 설정하기 위해서는 다음과 같은 단계를 따르십시오:

1. 하드웨어 목록에 물리적 하드웨어 장치를 추가합니다.
2. 물리적 하드웨어 장치와 연관된 네트워크 장치를 추가합니다.
3. 호스트명과 DNS 셋팅을 설정합니다.
4. DNS를 통하여 검색할 수 없는 호스트를 설정하십시오.

이 장에서는 여러 유형의 네트워크 연결을 설정하는 방법에 대하여 설명해 보겠습니다.

12.2. 이더넷 연결 설정하기

이더넷 연결을 설정하기 위해서는, 네트워크 인터페이스 카드 (NIC)와 네트워크 케이블 (보통 CAT5 케이블), 그리고 연결할 네트워크가 필요합니다. 네트워크 종류에 따라 속도가 다르기 때문에, 가지고 계신 네트워크 인터페이스 카드가 연결하려는 네트워크과 호환 가능한지를 확인해 주십시오.

이더넷 연결을 추가하시려면, 다음의 단계를 따르십시오:

1. **장치** 탭을 클릭합니다.
2. 도구바에서 **새로 만들기** 버튼을 클릭해 주십시오.
3. **장치 타입** 목록에서 **이더넷 연결**을 선택하신 후 **앞으로** 버튼을 클릭하시기 바랍니다.
4. 이미 네트워크 인터페이스 카드를 하드웨어 목록에 추가하셨다면, **이더넷 카드** 목록에서 해당 네트워크 인터페이스 카드를 선택하십시오. 그렇지 않으면, 하드웨어 장치를 추가하기 위하여 **다른 이더넷 카드**를 선택합니다.

알림

일반적으로 설치 프로그램은 지원되는 이더넷 장치를 감지하며 여러분에게 그 장치를 설정하도록 요청할 것입니다. 만일 여러분이 설치 과정에서 이더넷 장치를 설정하셨다면, 설정된 이더넷 장치는 **하드웨어** 탭에 있는 하드웨어 목록 내에 나타날 것입니다.

5. **다른 이더넷 카드**를 선택하시면, **이더넷 어댑터 선택** 화면이 나타날 것입니다. 가지고 계신 이더넷 카드의 제조업자와 모델명을 선택하신 후 장치명을 선택해 주십시오. 만일 이것이 시스템의 첫번째 이더넷 카드라면 장치명으로 **eth0**를 선택하시고, 만일 두번째 이더넷 카드라면 **eth1**을 선택하시고 이와 같은 순서로 계속 선택해 나가시면 됩니다. 또한 **네트워크 관리 도구**를 사용하여 네트워크 인터페이스 카드 (NIC)에 사용되는 자원을 설정하는 것도 가능합니다. 계속 진행하기 위하여 **앞으로** 버튼을 클릭해 주십시오.
6. 그림 12-2에서 보여지는 **네트워크 셋팅 설정** 창에서는 DHCP와 정적 IP 주소 중 하나를 선택해 주십시오. 네트워크가 시작될 때마다 장치가 다른 IP 주소를 받는다면, 호스트명을 지정하지 마십시오. **앞으로** 버튼을 클릭하여 계속 진행해 나갑니다.
7. **이더넷 장치 생성** 화면에서 **적용** 버튼을 클릭하십시오.

그림 12-2. 이더넷 셋팅

이더넷 장치 설정을 마치면 그림 12-3에서 보여지듯이 장치 목록에 해당 이더넷 장치가 나타납니다.

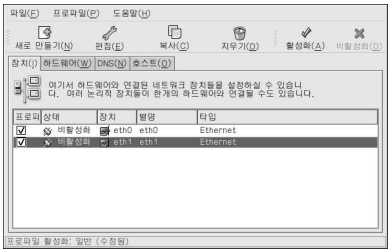

그림 12-3. 이더넷 장치

반드시 **파일** => **저장**을 선택하여 변경 사항을 저장하는 것을 잊지 마십시오.

이더넷 장치를 추가하신 후 장치 목록에서 그 장치를 선택하고 **편집** 버튼을 클릭함으로서 설정을 편집하실 수 있습니다. 예를 들어 장치가 추가되었을 때 그 장치는 시스템 부팅시 시작하도록 기본 설정되었다고 가정합니다. 이 설정을 변경하기 위해서는, 장치를 편집하도록 선택하신 후 **컴퓨터가 시작하면 장치를 활성화시킴** 값을 변경하시고 변경 사항을 저장하시기 바랍니다.

장치를 추가하여도 **비활성화** 상태에서 알 수 있듯이 즉시 활성화되지는 않습니다. 장치를 활성화하시려면, 장치 목록에서 선택하신 후 **활성화** 버튼을 클릭하시면 됩니다. 만일 컴퓨터가 시작시 장치가 활성화되도록 시스템이 설정되어 있다면 (디폴트), 이 과정을 다시 수행하지 않으셔도 됩니다.

한 개 이상의 장치를 이더넷 카드에 연결하신다면, 추가 장치들은 장치 별칭을 사용합니다. 장치 별칭을 사용하여 한 개의 물리적 장치에 여러 개의 가상 장치를 설정함으로서, 한 개 장치에 여러 개의 IP 주소를 할당 가능합니다. 예로 들면, eth1 장치와 eth1:1 장치를 설정하실 수 있습니다. 자세한 정보는 12.13 절을 참조하시기 바랍니다.

12.3. ISDN 연결 설정하기

ISDN 연결은 통신 회사에 의해 설치된 특별한 전화선을 통하여 ISDN 모뎀 카드를 이용하여 설정된 인터넷 연결을 의미합니다. ISDN 연결은 유럽에서 대중적입니다.

ISDN 연결을 추가하기 위해서는 다음의 단계를 따르십시오:

1. **장치** 탭을 클릭합니다.
2. 도구바에서 **새로 만들기** 버튼을 클릭해 주십시오.
3. **장치 타입** 목록에서 **ISDN 연결**을 선택하신 후 **앞으로** 버튼을 클릭하시기 바랍니다.
4. 풀다운 메뉴에서 ISDN 어댑터를 선택해 주십시오. 그 후 어댑터에 사용될 자원과 D 채널 프로토콜을 설정하시기 바랍니다. 계속 진행하기 위하여 **앞으로** 버튼을 클릭해 주십시오.

그림 12-4. ISDN 셋팅

5. 만일 여러분의 ISP (인터넷 제공 사업자)가 미리 설정된 목록에 존재한다면, 해당 ISP를 선택하십시오. 그렇지 않으면 여러분의 ISP 계정에 대한 필수 정보를 입력하시기 바랍니다. ISP에 대한 정보가 확실치 않다면, 여러분의 ISP에 문의해 보십시오. **앞으로** 버튼을 클릭해 주십시오.
6. **IP 설정** 창에서, **캡슐화 모드**를 선택하시고 DHCP를 통하여 IP 주소를 할당받을 것인지 또는 정적으로 IP 주소를 설정할 지 여부를 지정해 주십시오. 설정을 마치시면 **앞으로** 버튼을 클릭하시기 바랍니다.
7. **전화 연결 생성** 화면에서 **적용** 버튼을 클릭하십시오.

ISDN 장치 설정을 마치면, 그림 12-5에서 보여지듯이 장치 목록에서 **ISDN** 유형 장치가 나타납니다.

반드시 **파일** => **저장**을 선택하여 변경 사항을 저장하는 것을 잊지 마십시오.

ISDN 장치를 추가하신 후, 장치 목록에서 그 장치를 선택 선택하고 **편집** 버튼을 클릭함으로서 설정을 편집하실 수 있습니다. 예를 들어, 장치가 추가되었을 때 그 장치가 부팅시 시작되도록 기본 설정되지 않았다고 가정합니다. 여러분은 이러한 셋팅을 변경하도록 설정을 편집하실 수 있습니다. 압축, PPP 옵션, 로그인 이름, 암호 등에 대한 설정을 변경 가능합니다.

장치를 추가하여도 **비활성화** 상태에서 알 수 있듯이 즉시 활성화되지는 않습니다. 장치를 활성화하시려면, 장치 목록에서 선택하신 후 **활성화** 버튼을 클릭하시면 됩니다. 만일 컴퓨터가 시작시 장치가 활성화되도록 시스템이 설정되어 있다면 (디폴트), 이 과정을 다시 수행하지 않으셔도 됩니다.

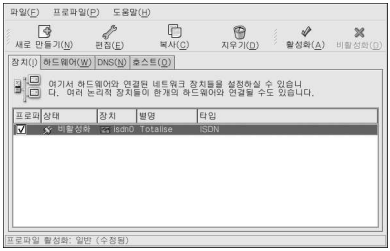

그림 12-5. ISDN 장치

12.4. 모뎀 연결 설정하기

모뎀을 사용하여 전화선을 통한 인터넷 연결을 설정하실 수 있습니다. 전화걸기 계정이라고도 부르는 ISP (인터넷 제공 사업자) 계정이 필요합니다.

모뎀 연결을 추가하기 위해서는 다음의 단계를 따르십시오:

1. **장치** 탭을 클릭합니다.
2. 도구바에서 **새로 만들기** 버튼을 클릭해 주십시오.
3. **장치 타입** 목록에서 **모뎀 연결**을 선택하신 후 **앞으로** 버튼을 클릭하시기 바랍니다.
4. 만일 가지고 계신 모뎀이 **하드웨어** 탭에 있는 하드웨어 목록에 이미 설정되어 있다면, **네트워크 관리 도구**는 그 모뎀을 사용하여 모뎀 연결을 설정할 것입니다. 만일 모뎀이 설정되어 있지 않다면, 모뎀을 찾아내기 위해 시스템을 검색합니다. 이러한 검색 작업에는 약간의 시간이 소요될 것입니다. 모뎀을 찾지 못한 경우, 검색 결과 모뎀을 찾지 못했다는 경고 메시지가 나타날 것입니다.
5. 모뎀 검색 작업이 마치면, 그림 12-6에서 보여지는 창이 나타날 것입니다.

그림 12-6. 모뎀 셋팅

6. 모뎀 장치, 보드(baud) 속도, 흐름 제어와 모뎀 볼륨을 설정해 주십시오. 만일 입력할 값을 잘 모르신다면, 기본 값을 수용하시기 바랍니다. 터치 톤 전화를 사용하지 않으신다면, 상응하는 체크박스에서 체크 표시를 제거해 주십시오. **앞으로** 버튼을 클릭합니다.
7. 만일 여러분의 ISP (인터넷 제공 사업자)가 미리 설정된 목록에 존재한다면, 해당 ISP를 선택하십시오. 그렇지 않으면 여러분의 ISP 계정에 대한 필수 정보를 입력하시기 바랍니다. ISP에 대한 정보가 확실치 않다면, 여러분의 ISP에 문의해 보십시오. **앞으로** 버튼을 클릭해 주십시오.

8. **IP 설정** 창에서, DHCP를 통하여 IP 주소를 할당받을 것인지 또는 정적으로 IP 주소를 설정할 지 여부를 지정해 주십시오. 설정을 마치시면 **앞으로** 버튼을 클릭하시기 바랍니다.
9. **전화 연결 생성** 화면에서 **적용** 버튼을 클릭하십시오.

모뎀 장치 설정을 마치면, 그림 12-7에서 보여지듯이 장치 목록에서 해당 모뎀 장치가 `Modem` 유형으로 나타납니다.

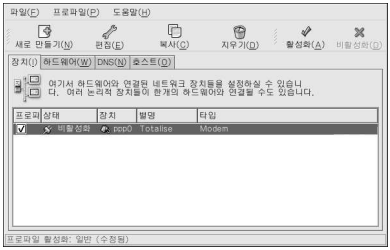

그림 12-7. 모뎀 장치

반드시 **파일** => **저장**을 선택하여 변경 사항을 저장하는 것을 잊지 마십시오.

모뎀 장치를 추가한 후 장치 목록에서 장치를 선택하고 **편집** 버튼을 클릭함으로서 설정을 편집할 수 있습니다. 예를 들어 장치가 추가되었을 때 그 장치는 디폴트로 시스템이 부팅될 때 시작하도록 설정되었다고 가정합니다. 여러분은 이러한 셋팅을 수정하도록 설정을 편집하실 수 있습니다. 압축, PPP 옵션, 로그인 이름, 암호 등을 변경 가능합니다.

장치를 추가하여도 **비활성화** 상태에서 알 수 있듯이 즉시 활성화되지는 않습니다. 장치를 활성화하시려면, 장치 목록에서 선택하신 후 **활성화** 버튼을 클릭하시면 됩니다. 만일 컴퓨터가 시작시 장치가 활성화되도록 시스템이 설정되어 있다면 (디폴트), 이 과정을 다시 수행하지 않으셔도 됩니다.

12.5. xDSL 연결 설정하기

DSL은 디지털 가입자 회선 (Digital Subscriber Lines)의 줄임말로서, 다양한 유형의 DSL이 존재합니다 (예, ADSL, IDSL, SDSL). **네트워크 관리 도구**는 이러한 모든 유형의 DSL 연결을 통틀어서 xDSL이라고 부릅니다.

일부 DSL 제공 업체들은 이더넷 카드를 사용하여 DHCP를 통하여 IP 주소를 얻도록 시스템을 설정하도록 요구할 것입니다. 다른 DSL 제공 업체들은 이더넷 카드를 사용하여 PPPoE (Point-to-Point Protocol over Ethernet) 연결을 설정하도록 요구할 수도 있습니다. 여러분의 DSL 제공 업체에게 문의하셔서 어떤 방법을 사용할지 알아보십시오.

DHCP를 사용하셔야 한다면, 이더넷 카드를 설정하기 위해서 12.2 절을 참조해 보십시오.

PPPoE를 사용하셔야 한다면 다음의 단계를 따르십시오:

1. **장치** 탭을 클릭합니다.
2. **새로 만들기** 버튼을 클릭해 주십시오.
3. **장치 타입** 목록에서 **xDSL 연결**을 선택하신 후 **앞으로** 버튼을 클릭하시기 바랍니다.
4. 하드웨어 목록에서 여러분이 가지고 계신 이더넷 카드를 찾을 수 있다면, 그림 12-8에서 보여진 화면의 풀다운 메뉴에서 **이더넷 장치**를 선택하십시오. 그렇지 않으면, **이더넷 어댑터 선택** 창이 나타날 것입니다.

알림

일반적으로 설치 프로그램은 지원되는 이더넷 장치를 감지하며 여러분에게 그 장치를 설정하도록 요청할 것입니다. 만일 여러분이 설치 과정에서 이더넷 장치를 설정하셨다면, 설정된 이더넷 장치는 **하드웨어** 탭에 있는 하드웨어 목록 내에 나타날 것입니다.

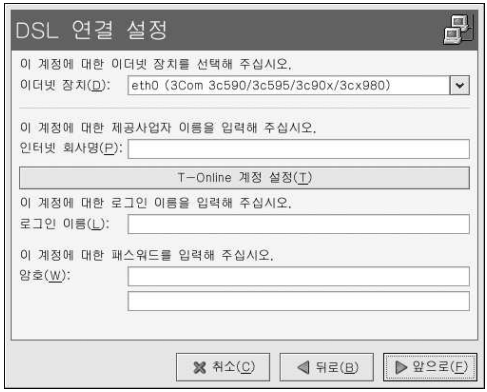

그림 12-8. xDSL 셋팅

5. **이더넷 어댑터 선택** 화면이 나타나면, 가지고 계신 이더넷 카드의 제조업자와 모델명을 선택하신 후 장치명을 선택해 주십시오. 만일 이것이 시스템의 첫번째 이더넷 카드라면 장치명으로 **eth0**를 선택하시고, 만일 두번째 이더넷 카드라면 **eth1**을 선택하시고 이와 같은 순서로 계속 선택해 나가시면 됩니다. 또한 **네트워크 관리 도구**를 사용하여 네트워크 인터페이스 카드 (NIC)에 사용되는 자원을 설정하는 것도 가능합니다. 계속 진행하기 위하여 **앞으로** 버튼을 클릭해 주십시오.
6. **인터넷 회사명**, **로그인 이름**, **암호**를 입력하시기 바랍니다. 만일 T-Online 계정을 가지고 계시다면, 기본 창에서 **로그인 이름**과 **암호**를 입력하는 대신, **T-Online 계정 설정** 버튼을 클릭하여 필요한 정보를 입력해 주십시오. **앞으로** 버튼을 클릭하십시오.
7. **DSL 장치 생성** 화면에서 **적용** 버튼을 클릭하십시오.

DSL 연결 설정을 마치면 그림 12-7에서 보여지듯이 장치 목록에 해당 DSL 장치가 나타납니다.

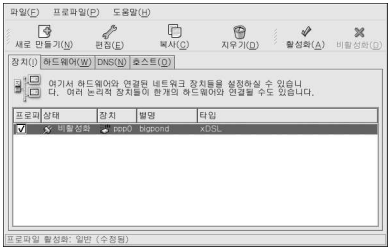

그림 12-9. xDSL 장치

반드시 **파일** => **저장**을 선택하여 변경 사항을 저장하는 것을 잊지 마십시오.

xDSL 장치를 추가하신 후 장치 목록에서 그 장치를 선택하고 **편집** 버튼을 클릭함으로서 설정을 편집하실 수 있습니다. 예를 들어 장치가 추가되었을 때 그 장치는 시스템 부팅시 시작하도록 기본 설정되었다고 가정합니다. 여러분은 이러한 셋팅을 수정하도록 설정을 편집하실 수 있습니다.

장치를 추가하여도 **비활성화** 상태에서 알 수 있듯이 즉시 활성화되지는 않습니다. 장치를 활성화하시려면, 장치 목록에서 선택하신 후 **활성화** 버튼을 클릭하시면 됩니다. 만일 컴퓨터가 시작시 장치가 활성화되도록 시스템이 설정되어 있다면 (디폴트), 이 과정을 다시 수행하지 않으셔도 됩니다.

12.6. 토큰 링 연결 설정하기

토큰 링 네트워크은 모든 컴퓨터가 원형으로 연결되어 있는 네트워크 입니다. 토큰 또는 특별 네트워크 패킷은 토큰 링 주위를 이동해 다니며 컴퓨터들 사이에서 서로 정보를 전송할 수 있게 합니다.

힌트

리눅스에서 토큰 링을 사용하는 방법에 대한 보다 많은 정보를 원하신다면, 리눅스 토큰 링 프로젝트 웹사이트를 다음의 주소로 방문하시기 바랍니다: http://www.linuxtr.net/.

토큰 링 연결을 추가하기 위해서는 다음의 단계를 따르십시오:

1. **장치** 탭을 클릭합니다.
2. 도구바에서 **새로 만들기** 버튼을 클릭하시기 바랍니다.
3. **장치 타입** 목록에서 **토큰 링 연결**을 선택하신 후 **앞으로** 버튼을 클릭하시기 바랍니다.
4. 하드웨어 목록에 이미 토큰 링 카드를 추가하셨다면, **토큰 링 카드** 목록에서 토큰 링 카드를 선택하십시오. 그렇지 않으면, 하드웨어 장치를 추가하기 위해서 **다른 토큰 링 카드**를 선택하십시오.
5. **다른 토큰 링 카드**를 선택하시면, 그림 12-10와 같은 **토큰 링 어댑터 선택** 화면이 나타날 것입니다. 가지고 계신 토큰 링 카드의 제조업자와 모델명을 선택하신 후 장치명을 선택해 주십시오. 만일 이것이 시스템의 첫번째 토큰 링 카드라면 장치명으로 **tr0**를 선택하시고, 만일 두번째 토큰링 카드라면 **tr1**을 선택하시고 이와 같은 순서로 계속 선택해 나가시면 됩니다. 또한 **네트워크 관리 도구**를 사용하여 토큰 링 어댑터에 사용되는 자원을 설정하는 것도 가능합니다. 계속 진행하기 위하여 **앞으로** 버튼을 클릭해 주십시오.

그림 12-10. 토큰 링 셋팅

6. **네트워크 셋팅 설정** 화면에서 DHCP와 정적 IP 주소 중 한가지를 선택하십시오. 만일 매번 네트워크가 시작할 때마다 다른 IP 주소가 장치에 보내진다면, 호스트명을 지정하지 마십시오. **앞으로** 버튼을 클릭하여 계속 진행해 나갑니다.
7. **토큰 링 장치 생성** 화면에서 **적용** 버튼을 클릭해 주십시오.

토큰 링 장치 설정을 마치면 그림 12-11에서 보여지듯이 장치 목록에 해당 토큰 링 장치가 나타납니다.

그림 12-11. 토큰 링 장치

반드시 **파일** => **저장**을 선택하여 변경 사항을 저장하는 것을 잊지 마십시오.

이더넷 장치를 추가하신 후 장치 목록에서 그 장치를 선택하고 **편집** 버튼을 클릭함으로서 설정을 편집하실 수 있습니다. 예를 들어 장치가 추가되었을 때 그 장치는 시스템 부팅시 시작하도록 기본 설정되었다고 가정합니다. 여러분은 이러한 셋팅을 수정하도록 설정을 편집하실 수 있습니다.

장치를 추가하여도 **비활성화** 상태에서 알 수 있듯이 즉시 활성화되지는 않습니다. 장치를 활성화하시려면, 장치 목록에서 선택하신 후 **활성화** 버튼을 클릭하시면 됩니다. 만일 컴퓨터가 시작시 장치가 활성화되도록 시스템이 설정되어 있다면 (디폴트), 이 과정을 다시 수행하지 않으셔도 됩니다.

12.7. CIPE 연결 설정

CIPE는 Crypto IP Encapsulation (암호기술이 적용된 IP 인캡슐레이션)의 줄임말입니다. CIPE는 IP 터널링 장치를 설정하기 위해 사용됩니다. 예로 들면, CIPE는 외부에서 가상 사설 통신망 (Virtual Private Network - VPN)으로 접근을 허가하는데 사용될 수 있습니다. CIPE 장치를 설정하셔야 한다면, 정확한 값에 대하여 시스템 관리자에게 문의해보시기 바랍니다.

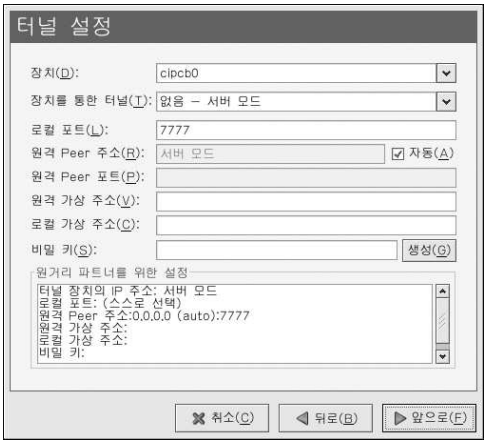

그림 12-12. CIPE 셋팅

힌트

CIPE와 CIPE 설정에 대한 자세한 정보를 원하신다면, *Red Hat Linux* 보안 가이드를 참조하시기 바랍니다.

12.8. 무선 연결 설정하기

무선 이더넷 장치들은 점점 더 대중적이 되고 있습니다. 무선 이더넷 장치 설정은 SSID와 무선 장치에 사용되는 키를 설정할 수 있다는 점을 제외하면 이더넷 설정과 유사합니다.

무선 이더넷 연결을 추가하기 위해서는, 다음의 단계를 따르십시오:

1. **장치** 탭을 클릭합니다.
2. 도구바에서 **새로 만들기** 버튼을 클릭하십시오.
3. **장치 타입** 목록에서 **무선 연결**을 선택하신 후 **앞으로** 버튼을 클릭하시기 바랍니다.
4. 이미 무선 네트워크 인터페이스 카드를 하드웨어 목록에 추가하셨다면, **무선 카드** 목록에서 해당 무선 네트워크 인터페이스 카드를 선택하십시오. 그렇지 않으면, 하드웨어 장치를 추가하기 위하여 **다른 무선 카드**를 선택하십시오.

   

   알림

   일반적으로 설치 프로그램은 지원되는 무선 이더넷 장치를 감지하며 여러분에게 그 장치를 설정하도록 요청할 것입니다. 만일 여러분이 설치 과정에서 무선 이더넷 장치를 설정하셨다면, 이미 설정된 무선 이더넷 장치는 **하드웨어** 탭에 있는 하드웨어 목록 내에 나타날 것입니다.

5. **다른 무선 카드**를 선택하시면, **이더넷 어댑터 선택** 화면이 나타날 것입니다. 가지고 계신 이더넷 카드의 제조업자와 모델명을 선택하신 후 장치명을 선택해 주십시오. 만일 이것이 시스템의 첫번째 이더넷 카드라면 장치명으로 **eth0**를 선택하시고, 만일 두번째 이더넷 카드라면 **eth1**을 선택하시고 이와 같은 순서로 계속 선택해 나가시면 됩니다. 또한 **네트워크 관리 도구**를 사용하여 무선 네트워크

인터페이스 카드에 사용되는 자원을 설정하는 것도 가능합니다. 계속 진행하기 위하여 **앞으로** 버튼을 클릭해 주십시오.

6. 그림 12-13에서 보여지는 **무선 연결 설정** 화면에서 무선 장치에 대한 셋팅을 설정하십시오.

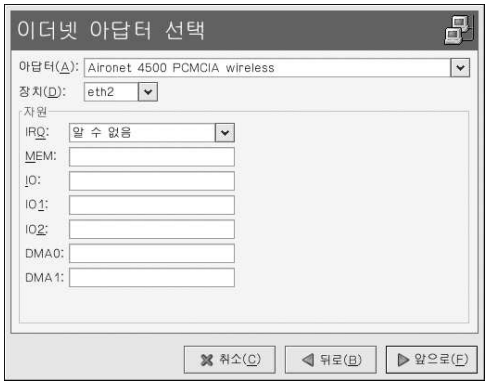

그림 12-13. 무선 셋팅

7. **네트워크 셋팅 설정** 화면에서 DHCP와 정적 IP 주소 중 한가지를 선택하십시오. 만일 매번 네트워크가 시작할 때마다 다른 IP 주소가 장치에 보내진다면, 호스트명을 지정하지 마십시오. **앞으로** 버튼을 클릭하여 계속 진행해 나갑니다.
8. **무선 장치 생성** 화면에서 **적용** 버튼을 클릭하십시오.

무선 장치 설정을 마치면 그림 12-14에서 보여지듯이 장치 목록에 해당 무선 장치가 나타납니다.

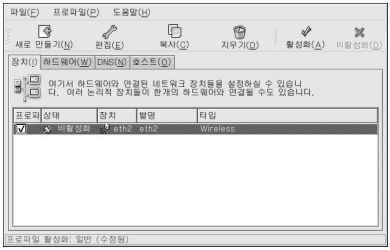

그림 12-14. 무선 장치

반드시 **파일** => **저장**을 선택하여 변경 사항을 저장하는 것을 잊지 마십시오.

무선 장치를 추가하신 후 장치 목록에서 그 장치를 선택하고 **편집** 버튼을 클릭함으로서 설정을 편집하실 수 있습니다. 예를 들어 장치가 추가되었을 때 그 장치는 시스템 부팅시 시작하도록 기본 설정되었다고 가정합니다. 여러분은 이러한 셋팅을 수정하도록 설정을 편집하실 수 있습니다.

장치를 추가하여도 **비활성화** 상태에서 알 수 있듯이 즉시 활성화되지는 않습니다. 장치를 활성화하시려면, 장치 목록에서 선택하신 후 **활성화** 버튼을 클릭하시면 됩니다. 만일 컴퓨터가 시작시 장치가 활성화되도록 시스템이 설정되어 있다면 (디폴트), 이 과정을 다시 수행하지 않으셔도 됩니다.

12.9. DNS 셋팅 관리

DNS 탭에서 시스템의 호스트명, 도메인, 네임 서버와 검색 도메인을 설정하실 수 있습니다. 네임 서버는 네트워크 상의 다른 호스트를 검색하기 위하여 사용됩니다.

만일 DHCP 또는 PPPoE (또는 ISP)로부터 DNS 서버명이 검색되었다면, 1차, 2차, 3차 DNS 서버를 추가하지 마십시오.

만일 DHCP 또는 PPPoE (또는 ISP)로부터 동적으로 호스트명이 검색되었다면, 그 호스트명을 변경하지 마십시오.

그림 12-15. DNS 설정

알림

네임 서버 섹션은 시스템이 네임 서버가 되도록 설정하지 않습니다. 대신, IP 주소를 호스트명으로 변환하거나 호스트명을 IP 주소로 변환시 사용할 네임 서버를 설정합니다.

12.10. 호스트 관리

Hosts 탭에서 여러분은 `/etc/hosts` 파일로부터 호스트를 추가, 편집 또는 제거하실 수 있습니다. 이 파일에는 IP 주소와 그 주소에 상응하는 호스트명이 포함되어 있습니다.

시스템이 호스트명을 IP 주소로 바꾸거나 IP 주소에 대한 호스트명을 결정할 때, (디폴트 Red Hat Linux 설정을 사용하신 경우) 그 시스템은 네임 서버를 사용하기 전에 `/etc/hosts` 파일을 참조합니다. 만일 `/etc/hosts` 파일에 IP 주소가 존재한다면, 네임 서버는 사용되지 않습니다. 만일 DNS 목록에 없는 IP 주소를 가진 컴퓨터가 네트워크 상에 존재한다면, 그 컴퓨터의 IP 주소를 `/etc/hosts` 파일에 추가하시기 바랍니다.

`/etc/hosts` 파일에 새로운 항목을 추가하시려면, **호스트** 탭에서 **새로 만들기** 버튼을 클릭해 주십시오. 필요한 정보를 입력하신 후 **확인**을 클릭하십시오. 그 후 변경 사항을 `/etc/hosts` 파일에 저장하기 위해 **파일** => **저장**을 선택하시거나 [Ctrl]-[S] 키를 누르시면 됩니다. 매번 주소가 변환될 때마다 현재 버전의 파일을 참조하기 때문에 네트워크나 네트워크 서비스를 재시작할 필요가 없습니다.

경고

`localhost` 항목을 제거하지 마십시오. 비록 시스템이 네트워크에 연결되지 않았거나 계속적으로 네트워크에 연결되지 않은 경우에도, 일부 프로그램은 localhost 룹백 인터페이스를 통해 시스템에 접속하기 때문입니다.

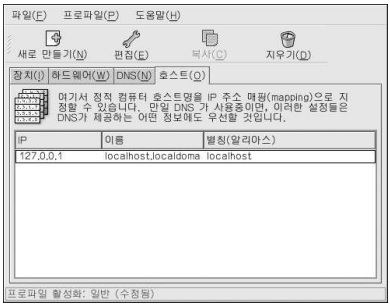

그림 12-16. 호스트 설정

힌트

검색 순서를 변경하기 위해서는 `/etc/host.conf` 파일을 편집하십시오. `order hosts, bind`라고 적힌 라인은 `/etc/hosts` 파일이 네임 서버보다 우선 순위를 차지한다고 지정하고 있습니다. 그 라인을 `order bind, hosts`로 변경한다면 시스템이 네임 서버를 우선 사용하여 호스트명과 IP 주소를 변환하도록 설정합니다. 만일 네임 서버를 통하여 IP 주소가 변환될 수 없다면, 시스템은 `/etc/hosts` 파일에서 IP 주소를 검색할 것입니다.

12.11. 장치 활성화

네트워크 장치가 부팅시 활성화되거나 부팅시 시작되도록 설정하실 수 있습니다. 예를 들어, 모뎀 연결에 사용되는 네트워크 장치는 일반적으로 부팅시 시작하도록 설정되지 않는 반면, 이더넷 연결은 부팅시 활성화되도록 설정됩니다. 만일 여러분의 네트워크 장치가 부팅시 시작하도록 설정되어 있지 않다면, 부팅을 마친 후 **Red Hat 제어 네트워크** 프로그램을 사용하여 네트워크 장치를 시작하실 수 있습니다. 이 프로그램을 시작하시려면 패널에서 **주 메뉴 버튼**을 클릭하신 후 **시스템 도구** => **네트워크 장치 제어**를 선택하시거나 쉘 프롬프트에서 `redhat-control-network` 명령을 입력하십시오.

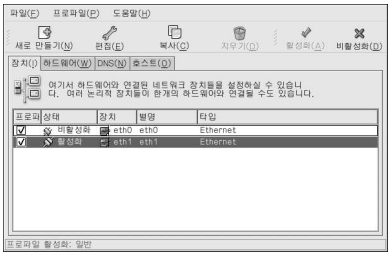

그림 12-17. 장치 활성화

장치를 활성화하시려면, 목록에서 해당 장치를 선택하신 후 **활성화** 버튼을 클릭하시면 됩니다. 활성화된 장치를 중지시키려면 목록에서 선택하신 후 **비활성화** 버튼을 클릭하십시오.

한 개 이상의 네트워크 프로파일이 설정된다면, 인터페이스 상 목록에 나타난 프로파일을 활성화하실 수 있습니다. 자세한 사항은 12.12 절을 참조하시기 바랍니다.

12.12. 프로파일 작업

한 개의 물리적 하드웨어 장치에 대하여 여러 개의 논리 네트워크 장치를 생성 가능합니다. 예를 들어 시스템에 한 개의 이더넷 카드 (eth0)를 가지고 계신 경우, 다른 별칭과 설정 옵션을 사용하여 eth0과 연관된 다양한 논리 네트워크 장치를 생성하실 수 있습니다.

논리 네트워크 장치는 장치 별칭과는 다른 개념입니다. 동일한 물리적 장치에 연관된 논리 네트워크 장치들은 각각 다른 프로파일에 저장되어야 하며, 동시에 활성화될 수 없습니다. 장치 별칭은 동일한 물리적 장치에 연관되지만 동시에 활성화될 수 있습니다. 장치 별칭을 생성하는 방법에 대한 보다 자세한 정보를 원하신다면, 12.13 절을 참조하시기 바랍니다.

프로파일을 사용하여 다른 네트워크에 사용될 여러 개의 설정 모음을 생성하실 수 있습니다. 설정 모음에는 논리 장치를 비롯하여 호스트와 DNS 셋팅이 포함됩니다. 프로파일 설정을 마치신 후 **네트워크 관리 도구**를 사용하여 여러 개의 프로파일 사이에서 변환 가능합니다.

일반으로 불리는 프로파일은 기본으로 설정됩니다. 새 프로파일을 생성하시려면, **프로파일 활성화** 프레임에서 **새로** 버튼을 클릭하신 후 프로파일에 사용될 고유 이름을 입력해 주십시오.

이제 기본 창 아래쪽에 나타난 상태바에 표시된 새로운 프로파일을 수정하셔야 합니다.

목록에 이미 존재하는 기존 장치를 논리 네트워크 장치로 복사해 오기 위하여 **복사** 버튼을 클릭하십시오. **새로 만들기** 버튼을 사용하실 경우, 네트워크 별칭이 생성될 것이며 이것은 올바르지 않습니다. 논리 장치의 등록 정보를 변경하시려면, 목록에서 해당 장치를 선택하신 후 **편집** 버튼을 클릭하시기 바랍니다. 예로 들면, 별명을 **eth0_office**와 같이 자세한 이름으로 바꾸어 보다 쉽게 쉽게 인식할 수 있도록 합니다.

장치 목록을 보시면 체크박스로 구성된 **프로파일**이라고 이름붙은 행이 있습니다. 여러분은 체크박스를 사용하여 개별 프로파일을 선택하거나 선택한 것을 취소하실 수 있습니다. 체크박스에 표시된 장치만 현재 선택된 프로파일에 포함됩니다. 예를 들어, **Office**라는 프로파일에 **eth0_office**라는 이름의 프로파일을 생성한 경우 그 프로파일이 선택된 경우 논리 장치를 활성화하고 싶다면, eth0 장치 옆에 체크박스가 선택된 것을 취소하고 eth0_office 장치를 선택하시면 됩니다.

예를 들어 그림 12-18을 보시면, **eth0_office** 논리 장치를 가진 **사무용 (Office)**라는 이름의 프로파일이 있습니다. 이 프로파일은 DHCP를 사용하는 첫번째 이더넷 카드를 활성화하도록 설정되어 있습니다.

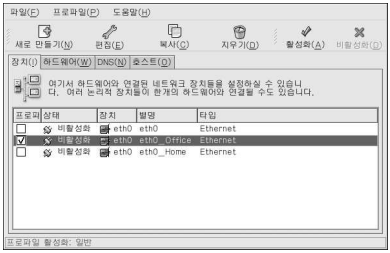

그림 12-18. 사무용 (Office) 프로파일

그림 12-19에서 **홈 (Home)** 프로파일이 eth0에 연결되어 정적 IP 주소를 사용하도록 설정된 **eth0_home** 논리 장치를 활성화하는 것을 보실 수 있습니다.

그림 12-19. 홈 (Home) 프로파일

여러분은 또한 **Office** 프로파일은 eth0만 활성화하고 **Home** 프로파일은 ppp (모뎀) 장치만 활성화하도록 설정하실 수 있습니다. 또 다른 예로서 **일반 (Common)** 프로파일에서는 eth0 프로파일을 활성화시키고 **여행 (Away)** 프로파일은 여행 중에 사용할 ppp 장치를 활성화하도록 설정 가능합니다.

프로파일은 부팅시 활성화될 수 없습니다. **일반** 프로파일 (기본 프로파일)에서 부팅시 활성화되도록 설정된 장치만이 부팅시 활성화됩니다. 시스템이 부팅된 후, 패널에서 **주 메뉴** => **시스템 도구** => **네트워크 장치 제어**를 선택하여 (또는 `redhat-control-network` 명령을 입력하여) 프로파일을 선택하고 활성화시키십시오. 기본 **일반** 인터페이스가 아닌 인터페이스가 존재할 경우, **네트워크 장치 제어** 인터페이스에서 활성화 프로파일 섹션이 나타납니다.

프로파일을 활성화하는 다른 방법으로는 다음 명령을 실행하시면 됩니다 (<*`profilename`*>를 프로파일 이름으로 대체하십시오):

```
redhat-config-network-cmd --profile <profilename> --activate
```

12.13. 장치 별칭

장치 별칭이란 동일한 물리적 하드웨어에 연관되었지만, 동시에 다른 IP 주소를 갖도록 활성화 가능한 가상 장치를 말합니다. 장치 별칭은 일반적으로 장치명 다음에 콜론과 숫자가 오는 형식으로 나타납니다 (예, eth0:1). 네트워크 카드가 한 개인 시스템 상에서 한 개 이상의 IP 주소를 원하시는 경우, 장치 별칭이 유용합니다.

정적 IP 주소를 사용하기 위해 (DHCP는 별칭과 함께 사용할 수 없습니다) `eth0`와 같은 이더넷 장치를 이미 설정하셨다면, **장치** 탭으로 가신 후 **새로 만들기** 버튼을 클릭하십시오. 별칭을 설정할 이더넷 카드를 선택하시고, 별칭에 정적 IP 주소를 설정하신 후 **적용** 버튼을 클릭하시기 바랍니다. 이더넷 카드에 장치가 이미 존재하므로, 새로운 장치는 `eth0:1`와 같은 별칭으로 생성됩니다.

경고

만일 이더넷 장치가 별칭을 갖도록 설정하시면, 이더넷 장치와 별칭은 DHCP를 사용할 수 없습니다. 따라서 여러분이 직접 IP 주소를 설정하셔야 합니다.

그림 12-20에서는 `eth0` 장치에 사용되는 별칭의 한 예시를 보여드립니다. `eth0:1` 장치 — `eth0`에 사용되는 첫번째 별칭을 주의해서 살펴보십시오. `eth0`에 사용되는 두번째 별칭은 장치명 `eth0:2`이며, 이와 같은 순서로 계속 설정됩니다. 장치 별칭에 대한 설정 (예, 부팅시 활성화 여부와 별칭 번호 등)을 수정하시려면, 목록에서 수정할 별칭을 선택하신 후 **편집** 버튼을 클릭하시기 바랍니다.

그림 12-20. 네트워크 장치 별칭 예시

별칭을 선택하신 후 **활성화** 버튼을 클릭하여 그 별칭을 활성화 합니다. 한 개 이상의 프로파일을 설정하셨다면, 별칭을 포함할 프로파일들을 선택해 주십시오.

별칭이 활성화되었는지 여부를 확인하기 위해서는 `/sbin/ifconfig` 명령을 사용하시면 됩니다. 명령을 실행하시면 다음과 같이 장치와 다른 IP 주소를 지닌 장치 별칭이 출력됩니다:

```
eth0   Link encap:Ethernet HWaddr 00:A0:CC:60:B7:G4
    inet addr:192.168.100.5 Bcast:192.168.100.255 Mask:255.255.255.0
    UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
    RX packets:161930 errors:1 dropped:0 overruns:0 frame:0
    TX packets:244570 errors:0 dropped:0 overruns:0 carrier:0
    collisions:475 txqueuelen:100
    RX bytes:55075551 (52.5 Mb) TX bytes:178108895 (169.8 Mb)
    Interrupt:10 Base address:0x9000

eth0:1  Link encap:Ethernet HWaddr 00:A0:CC:60:B7:G4
    inet addr:192.168.100.42 Bcast:192.168.100.255 Mask:255.255.255.0
    UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
    Interrupt:10 Base address:0x9000

lo    Link encap:Local Loopback
    inet addr:127.0.0.1 Mask:255.0.0.0
    UP LOOPBACK RUNNING MTU:16436 Metric:1
    RX packets:5998 errors:0 dropped:0 overruns:0 frame:0
    TX packets:5998 errors:0 dropped:0 overruns:0 carrier:0
    collisions:0 txqueuelen:0
    RX bytes:1627579 (1.5 Mb) TX bytes:1627579 (1.5 Mb)
```

기본 방화벽 설정

건물에서 방화벽은 불이 번지는 것을 방지하는 역할을 하는 것과 마찬가지로 컴퓨터 방화벽은 컴퓨터 바이러스가 여러분의 컴퓨터에 퍼지는 것을 방지하며 허가가 없는 사용자가 컴퓨터에 침입하는 것을 방지하는 역할을 합니다. 방화벽은 네트워크 상의 원격 사용자들이 여러분의 컴퓨터에서 접근할 수 있는 서비스의 종류를 결정합니다. 따라서 방화벽을 적절하게 설정하시면 여러분의 시스템 보안은 크게 증가시킬 수 있습니다. 인터넷에 접속된 모든 Red Hat Linux 시스템에 방화벽을 설정하실 것을 권장합니다.

13.1. Red Hat 보안 수준 설정 도구

Red Hat Linux 설치 프로그램의 **방화벽 설정** 화면에서 최상위 수준, 중간 수준 또는 방화벽을 설치하지 않음 중 한가지 보안 수준 선택할 수 있는 옵션을 비롯하여 방화벽 통과를 허용할 특정 장치, 접근을 허용할 서비스 및 포트를 설정하셨습니다.

설치가 완료된 후에도 **보안 수준 설정 도구**를 사용하여 시스템의 보안 수준을 변경 가능합니다. 마법사 기반 프로그램을 선호하신다면, 13.2 절을 참조하시기 바랍니다.

Red Hat 보안 수준 설정 도구를 시작하시려면, 패널에서 **주 메뉴** 버튼을 클릭하신 후 **시스템 도구** => **보안 수준 설정**을 선택하시거나 쉘 프롬프트 (예, XTerm이나 GNOME 터미널)에서 `redhat-config-securitylevel` 명령을 입력하십시오.

그림 13-1. Red Hat 보안 수준 설정 도구

풀다운 메뉴에서 원하시는 시스템 보안 수준을 선택해 주십시오.

최상위 수준

‘ **최상위 수준**을 선택하시면, 여러분이 특별히 허락하지 않은 접속은 인정되지 않습니다. 기본적으로 다음과 같은 접속만을 허용합니다:

- DNS 응답

- DHCP — DHCP를 사용하는 네트워크 장비나 프로그램은 설정하여 사용하실 수 있습니다.

최상위 수준의 보안을 사용하시면 다음의 사항은 허용되지 않습니다:

- 능동 모드 FTP (대부분의 FTP 클라이언트에서 기본적으로 사용되는 수동 모드 FTP는 제대로 작동될 것입니다.)
- IRC의 DCC 기능을 통한 파일 전송
- RealAudio™
- 원격 X 윈도우 시스템 클라이언트의 접속

현재 여러분의 시스템이 인터넷에 접속되어 있으며, 서버로 운영하실 계획이 아니라면, 이 보안 수준을 선택하시는 것이 가장 안전합니다. 부가적으로 다른 서비스가 필요하실 경우에는 **사용자 설정** 항목을 선택하여 방화벽 통과를 허락할 특정 서비스를 설정하실 수 있습니다.

알림

중간 수준이나 최상위 수준의 방화벽을 선택하시면, NIS나 LDAP와 같은 네트워크 인증 방식이 작동하지 않을 것입니다.

중간 수준

‘ **중간 수준**으로 방화벽을 설정하시면, 시스템 상의 특정 자원에 대한 원격 네트워크 접속을 허용하지 않을 것입니다. 기본적으로 다음과 같은 자원에 접근하는 것이 허용되지 않습니다:

- 1023 이하의 포트 — 이 포트들은 표준으로 예약되어 있는 포트이며, 대부분 **FTP**, **SSH**, **telnet**, **HTTP**, **NIS**와 같은 일반적인 서비스를 제공하는데 사용됩니다.
- NFS 서버 포트 (2049) — NFS는 원격 서버와 로컬 클라이언트에서 모두 사용되지 않습니다.
- 원격 X 클라이언트에서 지역 X 윈도우 시스템의 화면을 표시.
- X 폰트 서버 포트 (**xfs**는 네트워크를 청취하지 않도록 기본 설정되어 있습니다; 폰트 서버의 설정에는 이 포트값이 비활성화되어 있습니다).

RealAudio™와 같은 자원은 허용하면서 동시에 일반 시스템 서비스로의 접속은 차단하기를 원하시면, 방화벽을 **중간 수준**으로 설정하십시오. 방화벽을 통해 허락할 특정 서비스가 필요하신 경우에는 **사용자 설정** 항목을 선택하시기 바랍니다.

알림

중간 수준이나 최상위 수준의 방화벽을 선택하시면, NIS나 LDAP와 같은 네트워크 인증 방식이 작동하지 않을 것입니다.

방화벽을 사용하지 않음

‘ 이 항목은 모든 접근을 허락하며, 어떠한 보안 검사도 하지 않습니다. 만일 신뢰할 수 있는 (인터넷이 아닌) 네트워크 상에서 시스템을 운영하고 계시거나, 나중에 더욱 세밀한 방화벽 설정을 구상하고 계실 경우에만, 이 방법을 사용하시기 바랍니다.

신뢰하는 장치를 추가하시거나, 특정 서비스에 접근하는 것을 허락하기 위해서는 **사용자 설정** 항목을 선택하십시오.

신뢰하는 장치

‘ **신뢰하는 장치**를 선택하시면, 그 신뢰한 장치로부터 들어오는 트래픽은 모두 허용합니다; 즉 선택된 장치는 방화벽 규칙에서 제외되는 것입니다. 예를 들어, 로컬 네트워크를 운영하고 있지만 PPP 다이얼업을 통해 인터넷에 연결되어 있다면, **eth0**를 선택하여 로컬 네트워크로부터 들어오는 모든 트래픽을 허용하실 수 있습니다. **eth0**를 신뢰하는 장치로 선택한다는 것은 그 이더넷(Ethernet) 상 모든 트래픽을 허용하는 것을 의미합니다. 하지만 ppp0 인터페이스는 여전히 방화벽에 제한받게 됩니다. 인터페이스 상의 트래픽을 제한하시려면, eth0이 체크되지 않은 상태로 남겨둡니다.

인터넷과 같은 공동 네트워크에 연결된 장치를 **신뢰하는 장치**로 선택하는 것을 권장하지 않습니다.

허용할 서비스

‘ 이 항목에서 방화벽을 통해 허락할 특정 서비스를 선택하실 수 있습니다. 주의할 점은, 웍스테이션-유형으로 설치하실 경우에는 이 서비스의 대부분이 시스템 상에 존재하지 않습니다.

DHCP

‘ DHCP의 질의와 응답 및, DHCP를 사용하여 IP 주소를 결정하는 네트워크 인터페이스를 허용합니다. DHCP는 일반적으로 활성화되어 있으며, DHCP가 활성화되지 않으면 컴퓨터는 더이상 IP 주소를 얻지 못하게 됩니다.

SSH

‘ *S*ecure *SH*ell (SSH)는 원격 기계에 로그인하여 명령을 실행하는데 사용되는 도구 집합입니다. SSH 도구를 사용하여, 방화벽을 통하여 컴퓨터에 접근하실 계획이라면, 이 옵션을 사용하십시오. SSH를 사용하여 여러분의 컴퓨터에 원격적으로 접근하기 위해서는 `openssh-server` 패키지를 설치하셔야 합니다.

텔넷

‘ 텔넷은 원격 컴퓨터에 로그인하기 위한 프로토콜입니다. 텔넷 통신은 암호화되지 않고 네트워크 침입으로부터 아무런 보안을 제공하지 않습니다. 들어오는 텔넷 접근을 허용하는 것은 권장하지 않습니다. 인바운드 텔넷 접근을 허용하시려면, `telnet-server` 패키지를 설치하셔야 합니다.

WWW (HTTP)

‘ **HTTP**는 **Apache**(와 다른 서버들)을 통하여 웹 페이지를 제공하는데 사용되는 프로토콜 입니다. 웹 서버를 운영하려고 하신다면, 이 옵션을 선택하십시오. 로컬 컴퓨터 상에서 웹 페이지를 개발하거나 보기 위해서는 이 옵션이 필요하지 않습니다. 웹 페이지를 구축하시려면 `httpd` 패키지를 설치하셔야 합니다.

WWW (HTTP)를 활성화 한다고 해서 HTTPS에 대한 포트를 열지는 않습니다. HTTPS를 활성화하기 위해서는, **그 외의 포트** 영역에서 지정하셔야 합니다.

메일 (SMTP)

‘ SMTP의 메일 수신을 허용합니다. 원격의 컴퓨터가 메일을 전달하기 위해 직접 여러분의 컴퓨터에 접속하는 것을 허락하신다면, 이 항목을 선택하십시요. ISP 업체의 POP3 또는 IMAP 서버에서 메일을 가져오거나, `fetchmail`과 같은 유틸리티를 사용하실 경우에는 이 항목을 선택하지 마십시오. 잘못 설정된 SMTP 서버는 원격의 컴퓨터가 스팸 메일을 보내기 위해 여러분의 서버를 이용할 수 있음을 주의하십시오.

FTP

‘ **FTP**는 원격 파일을 전송하는데 사용되는 프로토콜 입니다. **FTP** 서버를 운영하려고 하신다면, 이 옵션을 선택하십시오. 이 옵션을 사용하시려면 `wu-ftpd` (그리고 아마도 `anonftp`) 패키지를 설치하셔야 합니다.

방화벽을 활성화하기 위해 **확인** 버튼을 클릭하시기 바랍니다. **확인** 버튼을 클릭하신 후, 선택된 옵션들은 `iptables` 명령으로 해석되어 `/etc/sysconfig/iptables` 파일에 기록됩니다. 또한 선택된 옵션을 저장 후 즉시 방화벽이 활성화되도록 `iptables` 서비스가 시작됩니다.

경고

`/etc/sysconfig/iptables` 파일에 방화벽을 설정하셨거나 방화벽 규칙이 존재하는 경우, **방화벽을 사용하지 않음**을 선택하신 후 변경 사항을 저장하기 위해 **확인** 버튼을 클릭하신다면 이 파일이 삭제될 것입니다.

선택하신 옵션들은 `/etc/sysconfig/redhat-config-securitylevel` 파일에 기록되어, 다음에 응용 프로그램이 시작될 경우에도 설정을 복구 가능합니다. 수동으로 이 파일을 편집하지 마십시오.

`iptables` 서비스가 부팅시 자동으로 시작되도록 활성화하시려면, 자세한 내용을 13.3 절에서 참조하시기 바랍니다.

13.2. GNOME Lokkit

GNOME Lokkit은 기본 `iptables` 네트워킹 규칙을 구성함으로서 일반 사용자를 위한 방화벽 셋팅을 설정할 수 있도록 해줍니다. 여러분이 직접 규칙을 기록하실 필요가 없이, 이 프로그램은 여러분께 시스템을 사용하시는 방식에 대한 여러가지 질문을 한 후 스스로 `/etc/sysconfig/iptables` 파일에 규칙을 기록해 줍니다.

복잡한 방화벽 규칙을 생성하기 위해서는 **GNOME Lokkit**을 사용하시기 바랍니다. 이 응용 프로그램은 일반 사용자가 모뎀, 케이블이나 DSL 인터넷 접속을 사용하는 동안 스스로의 컴퓨터를 보호할 수 있도록 의도되었습니다. 특정 방화벽 규칙을 설정하기 위해서는, *Red Hat Linux* 참조 가이드의 *`iptables`*을 사용하여 방화벽 설정하기 장을 참조하시기 바랍니다.

특정 서비스를 비활성화하고 특정 호스트와 사용자를 거부하기 위해서는, 14 장을 참조해 보십시오.

GNOME Lokkit을 그래픽 버전으로 시작하시려면, **주 메뉴 버튼** => **시스템 도구** => **추가 시스템 도구** => **Lokkit**을 선택하시거나, 쉘 프롬프트에서 루트로 로그인하신 후 `gnome-lokkit` 명령을 입력하시면 됩니다. X 윈도우 시스템이 설치되어 있지 않거나 텍스트 기반 프로그램을 선호하신다면, 쉘 프롬프트에서 `lokkit` 명령을 입력하여 텍스트 모드 버전으로 시작하실 수 있습니다.

13.2.1. 기본

그림 13-2. 기본

프로그램을 시작한 후 여러분의 시스템에 맞는 적절한 보안 수준을 선택해 주십시오:

- **최상위 보안** — 이 옵션은 네트워크 인터페이스를 활성화하는 DNS 응답과 DHCP를 제외한 대부분의 모든 네트워크 접속을 억제합니다. IRC, ICQ와 다른 실시간 메시지 서비스와 더불어 RealAudio™는 프록시가 없이는 작동하지 않을 것입니다.
- **하위 보안** — 이 옵션은 NFS 접속과 원격 X 윈도우 세션을 비롯한 시스템으로의 원격 접속을 허용하지 않습니다. FTP, SSH, Telnet과 HTTP와 같이 1023 이하의 포트에서 실행되는 서비스들은 접속이 허락되지 않을 것입니다.
- **방화벽 사용하지 않음** — 이 옵션은 모든 접근을 허락하며, 어떠한 보안 검사도 하지 않습니다. 만일 신뢰할 수 있는 (인터넷이 아닌) 네트워크 상에서 시스템을 운영하고 계시거나, 나중에 더욱 세밀한 방화벽 설정을 구상하고 계실 경우에만, 이 방법을 사용하시기 바랍니다. 이 옵션을 선택하시면 **다음** 버튼을 클릭하여 13.3 절 부분으로 넘어가십시오. 여러분 시스템의 보안은 변하지 않을 것입니다.

13.2.2. 로컬 호스트

만일 시스템 상에 이더넷 장치가 존재한다면, 여러분은 **로컬 호스트** 페이지에서 각 장치에 보내진 접속 요청에 방화벽 규칙을 적용할 것이지 여부를 설정하실 수 있습니다. 만일 장치가 지역 네트워크를 통하여 시스템에 연결되어 있으며 동시에 인터넷에 직접 연결되지 않는다면, **예** 버튼을 선택하십시오. 만일 시스템이 이더넷 카드를 통하여 케이블이나 DSL 모뎀에 연결된 경우에는, **아니오** 버튼을 선택하시기 바랍니다.

그림 13-3. 로컬 호스트

13.2.3. DHCP

만일 시스템 상에서 이더넷 인터페이스를 활성화하기 위하여 DHCP를 사용한다면, DHCP 질문에 대해서 반드시 **예** 버튼을 선택하셔야 합니다. 만일 '아니오'라고 대답하셨다면, 이더넷 인터페이스에 접속되지 않을 것입니다. 많은 케이블과 DSL 인터넷 제공업자들은 인터넷 접속을 위하여 DHCP를 사용하도록 요구하고 있습니다.

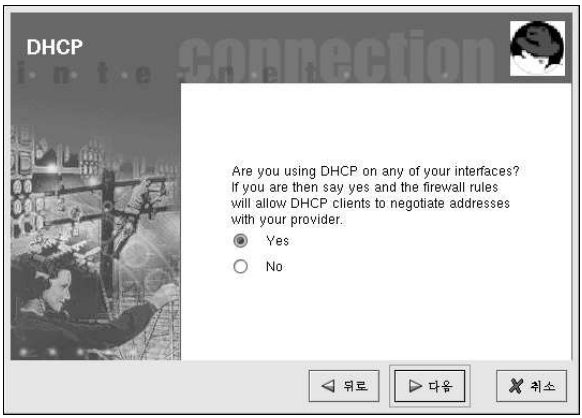

그림 13-4. DHCP

13.2.4. 서비스 설정

GNOME Lokkit은 또한 여러분이 일반 서비스를 시작하고 종료할 수 있도록 해줍니다. 서비스 설정하기 질문에 대하여 **예**라고 응답하셨다면, 다음과 같은 서비스에 대한 옵션이 나타날 것입니다:

- **웹 서버** — 만일 여러분의 시스템에 Apache와 같은 웹 서버가 운영되고 있으며 일반 사용자가 웹 서버에 접속하도록 허용하시려면 이 옵션을 선택하십시오. 만일 단순히 로컬 시스템이나 네트워크 상 다른 서버 상에서 웹 페이지를 보시려고 한다면 이 옵션을 선택하실 필요가 없습니다.
- **수신 메일** — 만일 원격 컴퓨터가 메일을 전달하기 위해 직접 여러분의 컴퓨터에 접속하는 것을 허락하신다면, 이 옵션을 선택하십시오. ISP 업체의 IMAP 또는 POP3 서버에서 메일을 가져오거나, fetchmail과 같은 유틸리티를 사용하실 경우에는 이 옵션을 선택하실 필요가 없습니다.
- **보안 쉘** — 보안 쉘 (SSH)은 원격 상의 컴퓨터에 로그인 및 명령을 실행하기 위한 프로토콜입니다. 원격 컴퓨터에서 ssh를 통해 여러분의 컴퓨터에 접근해야할 경우, 이 옵션을 선택하십시오.
- **텔넷** — 텔넷은 원격 컴퓨터에 로그인하기 위한 프로토콜입니다. 이 포로토콜은 암호화되지 않으며, 네트워크 스누핑 공격 으로부터의 보안이 매우 취약합니다. 따라서 원격으로 컴퓨터에 로그인하실 경우에는 SSH를 사용하시기를 권장합니다. 시스템에 텔넷 접속을 해야할 필요가 있다면, 이 옵션을 선택하십시오.

필요하지 않은 다른 서비스들을 비활성화하기 위해서는, **Serviceconf** (14.3 절 참조), **ntsysv** (14.4 절 참조), 혹은 `chkconfig`를 (14.5 절 참조) 사용하시기 바랍니다.

13.2.5. 방화벽 활성화

방화벽 규칙을 `/etc/sysconfig/iptables` 파일에 기록하기 위해 **완료** 버튼을 클릭하신 후 `iptables` 서비스를 시작하시면 방화벽이 시작됩니다.


경고

`/etc/sysconfig/iptables` 파일에 방화벽을 설정하셨거나 방화벽 규칙이 존재하는 경우, **방화벽을 사용하지 않음**을 선택하신 후 변경 사항을 저장하기 위해 **마침** 버튼을 클릭하신다면 이 파일이 삭제될 것입니다.

원격으로 로그인한 X 세션이 아닌, 로컬 컴퓨터에서 **GNOME Lokkit**을 실행하실 것을 적극 권장합니다. 만일 원격 X 세션에서 이 프로그램을 실행하시면, 원격 접속이 비활성화되면 더 이상 접속을 할 수가 없게 됩니다. 또한 다시 원격 접속하기 위해서는 방화벽 규칙을 비활성화 하셔야 합니다.

방화벽 규칙을 기록하는 것을 원하지 않으신다면, **취소** 버튼을 클릭해 주십시오.

13.2.5.1. 메일 전달 (mail relay)

메일 전달 (mail relay)은 이메일을 전달해주는 시스템입니다. 만일 메일 전달 시스템을 사용하고 계신다면, 다른 사용자가 다른 컴퓨터에 스팸 메일을 보내기 위해 여러분의 컴퓨터에서 메일 전달 시스템을 사용할 가능성도 있습니다.

메일 서비스를 활성화하도록 선택하신 경우, **방화벽 활성화** 페이지에서 **완료** 버튼을 클릭하시면 메일 전달 시스템을 테스트 해보도록 요청할 것입니다. 메일 전달 시스템을 테스트하기 위해 **예** 버튼을 선택하시면, **GNOME Lokkit**는 메일 악용 방지 시스템 웹 사이트인 http://www.mail-abuse.org/ 주소에 접속을 시도한 후 메일 전달 테스트 프로그램을 실행할 것입니다. 이 테스트의 결과는 테스트가 완료되면 화면에 출력됩니다. 여러분의 시스템이 메일 전달 시스템에 개방되는 것을 방지하도록 Sendmail을 설정하시기를 적극 권장합니다.

13.3. `iptables` 서비스 활성화하기

방화벽 규칙은 `iptables` 서비스가 실행 중일 경우에만 활성화됩니다. 서비스를 수동으로 시작하시려면, 다음 명령을 사용하시기 바랍니다:

```
/sbin/service iptables restart
```

시스템 부팅시 서비스를 시작하시려면, 다음과 같은 명령을 실행해 주십시오:

```
/sbin/chkconfig --level 345 iptables on
```

`iptables` 서비스와 `ipchains` 서비스를 함께 실행하실 수 없습니다. `ipchains` 서비스가 비활성화되어 있는 것을 확인하기 위해서는, 다음 명령을 실행해 주십시오:

```
/sbin/chkconfig --level 345 ipchains off
```

서비스 설정 도구를 사용하여 `iptables` 서비스와 `ipchains` 서비스를 활성화하는 방법도 있습니다. 자세한 사항은 14.3 절을 참조하시기 바랍니다.

14장 .

서비스로의 접근 통제

Red Hat Linux 시스템의 보안을 유지하는 것은 매우 중요합니다. 시스템 보안을 관리하는 한가지 방법은 시스템 서비스로의 접근을 주의깊게 관리하는 것입니다. 아마 특정 서비스에 한해서는 시스템에 제한없이 접근할 수 있도록 개방해야할 경우가 있습니다. (예, 웹서버를 운영하는 경우 `httpd`가 그러합니다.) 하지만 이러한 서비스를 제공할 필요가 없는 경우에는 시스템에 버그가 발생할 위험을 최소화하기 위해 서비스를 꺼놓으셔야 합니다.

시스템 서비스로의 접근을 관리하기 위하여 여러 다양한 방법을 사용할 수 있습니다. 여러분이 알고 계시는 Linux 전문 지식 수준, 시스템 설정과 서비스에 기반하여 사용하실 방법의 종류를 결정하셔야 합니다.

서비스로의 접근을 거부하는 가장 쉬운 방법은 단순히 서비스를 끄는 것입니다. (다음에 나온 부분에서 더욱 자세하게 설명됨) `xinetd`가 관리하는 서비스와 `/etc/rc.d`에 속한 서비스는 다음과 같은 3가지 응용 프로그램을 사용하여 시작하거나 멈출 수 있도록 설정 가능합니다:

- **서비스 설정 도구** — 개별 서비스에 대한 설명과 부팅시 (런레벨 3, 4, 5에서) 서비스의 시작 여부를 보여주는 그래픽 응용 프로그램입니다. 이 프로그램을 사용하여 개별 서비스를 시작, 정지하고 재시작하실 수 있습니다.
- **ntsysv** — 부팅시 각각의 런레벨에서 시작될 서비스의 종류를 설정하게 해주는 텍스트 기반 응용 프로그램입니다. `xinetd`가 아닌 서비스에는 변경 사항이 즉시 적용되지 않습니다. `xinetd`가 아닌 서비스는 이 프로그램을 사용하여 서비스를 시작, 정지하거나 재시작하실 수 없습니다.
- `chkconfig` — 다른 런레벨에서 서비스를 켜고 끌 수 있도록 해주는 명령행 유틸리티입니다. `xinetd`가 아닌 서비스에서는 변경 사항이 즉시 적용되지 않습니다. 또한 xinetd가 아닌 서비스는 이 유틸리티를 사용하여 시작, 정지 또는 재시작하실 수 없습니다.

위에서 언급된 도구를 사용하는 것이 다른 방법들 — 수동으로 `/etc/rc.d` 아래 디렉토리에 위치한 다수의 심볼릭 링크를 편집하거나 `/etc/xinetd.d`에서 `xinetd` 설정 파일 편집하는 것보다 쉽다고 느끼실 겁니다.

시스템으로의 접근을 관리하기 위한 또 다른 방법에는 `iptables`을 사용하여 IP 방화벽을 설정하는 방법도 있습니다. 초보 리눅스 사용자라면 `iptables`를 사용하는 것이 최선책이 아닐 수도 있습니다. `iptables`를 설정은 복잡한 작업이며 숙련된 리눅스 시스템 관리자만이 제대로 수행할 수 있습니다.

다른 한편으로 `iptables`를 사용하시면 설정에 융통성이 생긴다는 장점이 있습니다. 예로 들면, `iptables`을 사용하여 특정 서비스에 특정 호스트가 접근할 수 있도록 사용자 정의하실 수 있습니다. `iptables`와 관련된 보다 많은 정보를 원하시면 *Red Hat Linux* 참조 가이드와 *Red Hat Linux* 보안 가이드를 참조하시기 바랍니다.

만일 집에서 사용하는 컴퓨터에 일반적인 접근 규칙을 설정할 유틸리티를 찾고 계신다면, 다른 방법으로서 **GNOME Lokkit** 유틸리티를 사용해 보십시오. **GNOME Lokkit**은 GUI 유틸리티로서 사용자가 원하는 컴퓨터 사용 방식에 대하여 질문합니다. 그 후 사용자의 대답에 기초하여 간단한 방화벽을 설정할 것입니다. **보안 수준 설정 도구** (`redhat-config-securitylevel`)를 사용하셔도 됩니다. 이 도구를 사용하여 Red Hat Linux 설치 프로그램의 **방화벽 설정** 화면에서 선택하신 것처럼 시스템 보안 수준을 선택하실 수 있습니다. 이 도구에 대한 보다 많은 정보를 원하신다면, 13 장을 참조하시기 바랍니다.

14.1. 런레벨 (runlevels)

서비스로의 접근을 설정하기 이전에 먼저 Linux 런레벨을 이해하셔야 합니다. 런레벨이란 `/etc/rc.d/rc<x>.d` (여기서 <x>는 런레벨의 수) 디렉토리에 나열된 서비스에 의해 정의된 상태, 또는 모드*(mode)*를 의미합니다.

Red Hat Linux에서는 다음과 같은 런레벨이 사용됩니다:

- 0 — 정지

- 1 — 단독-사용자 모드
- 2 — 사용안됨 (사용자-정의가능)
- 3 — 완전 다중-사용자 모드
- 4 — 사용안됨 (사용자-정의가능)
- 5 — (X-기반 로그인 화면을 사용한) 완전 다중-사용자 모드
- 6 — 재부팅

텍스트 로그인 화면을 사용하신 경우 런레벨 3으로 작동합니다. 만일 그래픽 로그인 화면을 선택하신 경우에는 런레벨 5에서 작동합니다.

`/etc/inittab` 파일을 수정하여 기본 런레벨을 변경할 수 있습니다. `/etc/inittab` 파일을 보시면 처음 부분에 다음과 같은 줄이 포함되어 있습니다:

```
id:5:initdefault:
```

해당 줄에 나타난 숫자를 원하는 런레벨로 변경하십시오. 시스템을 재부팅하시면 변경 사항이 적용됩니다.

런레벨을 즉시 변경하기 위해서는 `telinit` 명령과 런레벨 숫자를 함께 사용합니다. 반드시 루트로 이 명령을 사용하셔야 합니다.

14.2. TCP 래퍼 (Wrappers)

많은 UNIX 시스템 관리자는 TCP 래퍼를 사용하여 특정 네트워크 서비스에 대한 접근을 관리 해왔습니다. libwrap에 대한 지원이 내장된 프로그램과 `xinetd`이 관리하는 모든 네트워크 서비스는 TCP 래퍼를 사용하여 접근을 관리할 수 있습니다. `xinetd`는 `/etc/hosts.allow`와 `/etc/hosts.deny` 파일을 사용하여 시스템 서비스로의 액세스를 설정할 수 있습니다. 이름에서 알 수 있듯이 `hosts.allow`는 `xinetd`이 통제하는 네트워크 서비스로의 클라이언트 접근을 허용하는 규칙의 목록을 담고 있습니다. 또한 `hosts.deny` 파일에는 접근을 거부하는 규칙이 포함되어 있습니다. `hosts.allow` 파일은 `hosts.deny` 파일 보다 우선권을 갖으며 개별 IP 주소 (또는 호스트명) 또는 클라이언트의 형태에 기초하여 접근을 허가하고 거부합니다. 보다 자세한 정보를 원하시면 *Red Hat Linux* 참조 가이드와 `hosts_access` 메뉴얼 페이지의 5번째 섹션 (`man 5 hosts_access`)을 참조하시기 바랍니다.

14.2.1. `xinetd`

인터넷 서비스로의 접근을 제어하기 위해서는 `xinetd`를 사용하십시오. `xinetd`는 `inetd`의 보안 대체입니다. `xinetd` 데몬은 시스템 자원을 보존하고 접근 통제와 기록 기능을 제공하며 특수 용도로 사용되는 서버를 시작하는데 사용됩니다. 또한 `xinetd`를 사용하여 특정 호스트로의 접근을 허가 또는 거부할 수 있으며, 정해진 시간에만 서비스에 접근할 수 있도록 하거나 들어오는 접속률과 접속으로 인해 생긴 부하를을 제한 가능합니다.

`xinetd`는 관리하는 서비스에 대한 모든 포트를 계속적으로 청취합니다. 이러한 서비스에 대한 접속 요청이 도착하면, `xinetd`는 해당 서비스를 위한 적절한 서버를 시작합니다.

`xinetd`의 설정 파일은 `/etc/xinetd.conf`입니다. 하지만 이 파일을 자세히 살펴보시면 이 파일에는 `/etc/xinetd.d` 디렉토리를 포함하기 위해 사용된 일부 디폴트와 지시 사항만이 포함되어 있다는 것을 알 수 있습니다. `xinetd` 서비스를 활성화하거나 비활성화하시려면, `/etc/xinetd.d` 디렉토리에 있는 설정 파일을 편집하십시오. `disable` 속성을 **`yes`**로 설정하시면 서비스가 사용되지 않습니다. 만일 `disable` 속성을 **`no`**로 설정하시면 서비스가 사용됩니다. 여러분은 또한 **서비스 설정 도구**, `ntsysv` 또는 `chkconfig` 명령을 사용하여 `xinetd` 설정 파일을 편집하거나 활성화 상태를 변경하실 수 있습니다. `xinetd`에 의해 제어되는 네트워크 서비스 목록을 보시려면 `ls /etc/xinetd.d` 명령을 사용하여 `/etc/xinetd.d` 디렉토리의 내용 목록을 살펴보시기 바랍니다.

14.3. 서비스 설정 도구

서비스 설정 도구는 Red Hat에 의해 개발된 그래픽 응용 프로그램으로서 부팅시 (런레벨 3, 4, 5에서) `/etc/rc.d/init.d`에서 시작될 SysV 서비스와 사용될 `xinetd` 서비스의 종류를 설정하는데 사용됩니다. 이 프로그램을 사용하여 `xinetd`를 재시작하고 SysV 서비스를 시작, 정지하고 재시작할 수 있습니다.

데스크탑에서 **서비스 설정 도구**를 시작하시려면 패널에서 **주 메뉴 버튼** => **서버 설정** => **서비스**을 선택합니다. 또는 **XTerm**이나 **GNOME 터미널**과 같은 쉘 프롬프트 상에서 `redhat-config-services` 명령을 입력하셔도 됩니다.

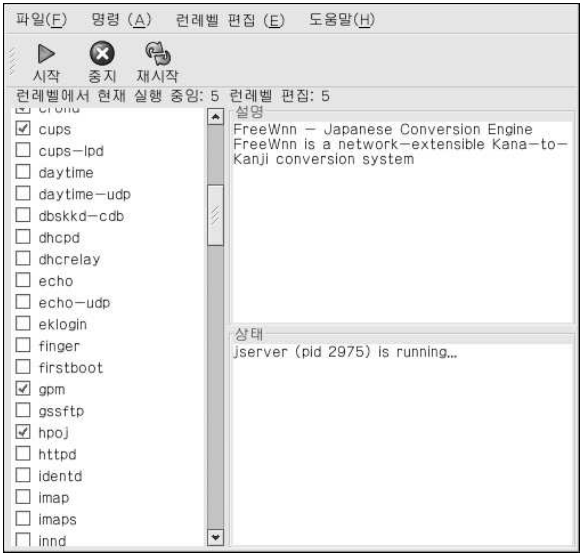

그림 14-1. 서비스 설정 도구

서비스 설정 도구는 현재 런레벨과 디불어 사용자가 현재 편집하고 있는 런레벨을 보여줍니다. 다른 런레벨을 편집하기 위해서는, 풀다운 메뉴에서 **런레벨 편집**을 선택하신 후 런레벨 3, 4 또는 5를 선택하십시오. 런레벨과 관련된 자세한 정보를 원하시면 14.1 절을 참조하시기 바랍니다.

서비스 설정 도구는 `xinetd` 데몬이 관리하는 서비스를 비롯하여 `/etc/rc.d/init.d`의 서비스 목록을 보여줍니다. 응용 프로그램의 왼쪽에 있는 목록에서 서비스 이름에 클릭하시면, 서비스의 상태를 비롯한 해당 서비스에 대한 간략한 설명이 나타납니다. 만일 그 서비스가 `xinetd` 서비스가 아닌 경우, 상태 창에서는 해당 서비스가 현재 실행되고 있는 지 여부를 보여줍니다. 만일 `xinetd` 데몬이 제어하는 서비스라면, 상태 창에서는 **xinetd service**라는 구문이 나타납니다.

서비스를 즉시 시작, 정지 또는 재시작하시려면, 목록에서 해당 서비스를 선택하신 후 도구바에서 적절한 버튼을 클릭하시기 바랍니다 (또는 **명령** 풀다운 메뉴에서 명령을 선택합니다). 만일 해당 서비스가 `xinetd` 서비스라면, 이 서비스는 개별적으로 시작되거나 정지될 수 없기 때문에 명령 버튼이 비활성화되어 있을 것입니다.

서비스 이름 옆에 위치한 체크박스를 체크하거나 체크된 것을 해제함으로서 `xinetd` 서비스를 활성화/비활성화 하신다면, 풀다운 메뉴에서 **파일** => **변동 사항 저장**을 선택하여 `xinetd`를 재시작하시고 여러분이 변경하신 `xinetd` 서비스를 즉시 활성화/비활성화 하셔야 합니다. `xinetd`는 또한 셋팅을 기억하도록 설정되어 있습니다. 따라서 여러분은 동시에 한 개 이상의 `xinetd` 서비스를 활성화/비활성화 하신 후 변경을 마치셨으면 변경 사항을 저장하실 수 있습니다.

예를 들어 rsync를 런레벨 3에서 활성화 하도록 선택하신 후 변경 사항을 저장하셨다고 가정합니다. rsync 서비스는 즉시 활성화될 것입니다. xinetd가 다시 시작되어도, rsync 서비스는 여전히 활성화 됩니다.


경고

xinetd 서비스에 대한 변경 사항을 저장하시면 xinetd가 재시작되며 변경 사항이 즉시 적용됩니다. 다른 서비스에 대한 변경 사항을 저장하시면 런레벨이 재설정되지만 변경 사항은 즉시 적용되지 않습니다.

xinetd 서비스가 아닌 서비스를 활성화하여 현재 선택된 런레벨에서 부팅시 시작되도록 하시려면, 목록에서 해당 서비스 이름 옆에 위치한 체크박스를 체크하시기 바랍니다. 런레벨을 설정하신 후, 풀 다운 메뉴에서 **파일 => 변동 사항 저장** 항목을 선택하여 변경 사항을 적용하시기 바랍니다. 런레벨 설정은 변경되었지만, 런레벨을 재시작하지 않습니다; 따라서 변경 사항이 즉시 적용되지 않습니다.

예를 들어 여러분이 런레벨 3을 설정하고 있다고 가정합니다. 만일 anacron에 대한 값이 선택된 상태에서 선택 해제하신 후 **변동 사항 저장** 버튼을 클릭하시면, 런레벨 3 설정이 변경되며 부팅시 anacron이 시작되지 않을 것입니다. 하지만 런레벨 3이 재초기화되지 않았기 때문에 anacron은 여전히 실행되고 있습니다. 이 시점에서 다음 중 한가지 옵션을 선택하십시오:

1. anacron 서비스 중지 — 목록에서 서비스를 선택 후 **중지** 버튼을 클릭하여 서비스를 중지시킵니다. 서비스가 성공적으로 중지되었다는 메시지가 나타날 것입니다.
2. 런레벨을 재초기화 — 쉘 프롬프트 상에서 telinit 3 (여기서 3은 런레벨 수) 명령을 입력하여 런레벨을 재초기화합니다. 만일 한개 이상의 서비스에 대한 **부팅시 시작** 값을 변경하신 경우, 변경 사항을 즉시 적용하시려면 이 옵션을 사용하시길 권장합니다.
3. 아무것도 하지않음 — anacron 서비스를 중지하실 필요가 없습니다. 시스템이 재부팅되어 시스템이 정지될 때까지 기다리시면 됩니다. 시스템이 다음에 부팅될 때 런레벨이 초기화되며 anacron 서비스는 실행되지 않을 것입니다.

14.4. ntsysv

ntsysv 유틸리티는 서비스를 활성화하고 비활성화 하는데 사용되는 단순한 인터페이스를 제공합니다. **ntsysv**를 사용하여 xinetd가 관리하는 서비스를 켜고 끌 수 있습니다. 또한 **ntsysv**를 사용하여 런레벨을 설정하실 수 있습니다. 오직 현재 런제벨만 설정 가능하도록 기본 설정되어 있습니다. 다른 런레벨을 설정하시려면, --level 명령을 사용하여 한 개 이상의 런레벨을 지정하시면 됩니다. 예를 들어, ntsysv --level 345 명령을 입력하시면 런레벨 3, 4와 5를 설정합니다.

ntsysv 인터페이스는 텍스트 모드 설치 프로그램처럼 작용합니다. 목록 위 아래로 이동하기 위해서 위/아래 화살표를 사용합니다. 스페이스 바는 서비스를 선택/선택 해제하며 또한 **확인**과 **취소** 버튼을 "누르기"위해 사용됩니다. 서비스 목록과 **확인**과 **취소** 버튼 사이에서 이동하기 위해서는, [Tab] 키를 사용하십시오. *****는 서비스가 켜지도록 설정된 것을 의미합니다. [F1] 키를 사용하시면 개별 서비스에 대한 간략한 설명을 볼 수 있습니다.


경고

xinetd 서비스는 **ntsysv**를 사용하신 후 즉시 변경 사항이 적용됩니다. 그 외 다른 서비스의 경우 변경 사항은 즉시 적용되지 않습니다. 반드시 service *daemon* stop 명령을 사용하여 개별 서비스를 정지하거나 시작하셔야 합니다. 앞의 예에서 *daemon*은 정지시킬 서비스 이름; 예, httpd으로 대체합니다. 서비스를 시작하거나 재시작하기 위해서는 stop을 start 또는 restart로 대체하시면 됩니다.

14.5. chkconfig

chkconfig 명령을 사용해서도 서비스를 활성화하고 비활성화할 수 있습니다. chkconfig --list 명령을 사용하여 시스템 서비스 목록과 런레벨 0-6에서 서비스의 시작 (on) 또는 정지 (off) 여부를 볼 수 있습니다. xinetd가 관리하는 서비스에 관련된 부분은 이 목록의 마지막 부분에 나타납니다.

chkconfig --list 명령을 사용하여 xinetd가 관리하는 서비스를 조회하시면, xinetd 서비스가 활성화 (on) 되었는지 또는 비활성화 (off) 되었는지 여부가 나타납니다. 예로 들면, 다음 chkconfig --list finger 명령은 다음과 같은 결과를 출력합니다:

```
finger    on
```

위에서 보여지듯이 finger는 xinetd 서비스로 활성화되어 있습니다. 따라서 만일 xinetd가 실행 중이라면 finger는 활성화됩니다.

만일 chkconfig --list를 사용하여 /etc/rc.d의 서비스를 조회하신다면, 다음과 같이 개별 런레벨에 대한 서비스 설정을 볼 수 있습니다. 예를 들어 chkconfig --list anacron 명령을 입력하시면 다음과 같은 결과가 출력될 것입니다:

```
anacron    0:off 1:off 2:on  3:on  4:on  5:on  6:off
```

또한 chkconfig을 사용하여 특정 런레벨에서 서비스를 시작 또는 정지하도록 설정 가능합니다. 예를 들어 nscd를 런레벨 3, 4, 5에서 해제하기 위해서는 다음과 같은 명령을 사용하시면 됩니다:

```
chkconfig --level 345 nscd off
```

경고

chkconfig 명령은 xinetd가 관리하는 서비스에 즉시 적용됩니다. 예로 들면, 만일 xinetd가 실행 중이며 finger가 비활성화된 상태에서 chkconfig finger on 명령을 실행한다면, xinetd를 수동으로 재시작할 필요가 없이 finger는 즉시 활성화됩니다. 하지만 다른 서비스에 대한 변경 사항은 chkconfig 사용 후 즉시 적용되지 않기 때문에 service *daemon* stop 명령을 사용하여 개별 서비스를 정지하거나 시작하셔야 합니다. 여기에서 *daemon*은 정지할 서비스 이름; 예, httpd으로 대체합니다. 서비스를 시작하거나 재시작하기 위해서는 stop을 start 또는 restart으로 대체합니다.

14.6. 추가 자료

보다 많은 정보를 원하신다면, 다음에 나온 자료를 참조하시기 바랍니다.

14.6.1. 설치된 문서 자료

- ntsysv, chkconfig, xinetd, 그리고 xinetd.conf의 메뉴얼 페이지.
- man 5 hosts_access — 호스트 접근 제어 파일의 형식에 대한 메뉴얼 페이지 (메뉴얼 페이지 중 섹션 5)

14.6.2. 유용한 웹사이트

- http://www.xinetd.org — xinetd 웹페이지. 이 웹페이지에는 더욱 상세한 기능 목록과 샘플 설정 파일이 포함되어 있습니다.

15장 . OpenSSH

OpenSSH는 SSH (*S*ecure *SH*ell) 프로토콜의 자유, 공개 소스 구현입니다. OpenSSH는 `telnet`, `ftp`, `rlogin`, `rsh`, `rcp`를 대체하는 안전하고, 암호화된 네트워크 연결 도구입니다. OpenSSH는 1.3, 1.5와 2.0 버전의 SSH 프로토콜을 지원합니다. OpenSSH 2.9 이후 버전의 기본 프로토콜은 2.0 버전이며 2.0 버전은 RSA 키를 디폴트로 사용합니다.

15.1. OpenSSH를 사용하는 이유?

OpenSSH 도구는 컴퓨터의 보안을 강화시킵니다. 그 이유는 OpenSSH 도구를 사용하는 모든 통신 (예, 암호)은 암호화되기 때문입니다. `Telnet`과 `ftp`는 평문 암호를 사용하여 모든 정보를 암호화되지 않은 채로 전송합니다. 따라서 누군가 중간에서 정보를 가로채어 암호를 복구할 가능성이 있습니다. 가로챈 패스워드를 사용하여 접근 권한이 없는 사용자가 시스템에 로그인한 후 시스템을 손상시킬 수도 있습니다. 이와 같은 보안 문제가 발생하는 것을 방지하기 위해서는 가능한 항상 OpenSSH 유틸리티를 사용하셔야 합니다.

OpenSSH를 사용하는 또 다른 이유는 OpenSSH는 클라이언트 컴퓨터로 `DISPLAY` 변수를 자동으로 전송한다는 것입니다. 즉, 로컬 컴퓨터에서 X 윈도우 시스템을 실행 중에 `ssh` 명령을 사용하여 원격 컴퓨터로 로그인한 경우에, 원격 컴퓨터 상에서 X를 사용하는 프로그램을 실행하시면 그 프로그램은 로컬 컴퓨터 상에 나타날 것입니다. 그래픽 시스템 관리 도구를 자주 사용하신다면 이 방법이 편리하지만 항상 서버에 물리적으로 접근하는 것은 아닙니다.

15.2. OpenSSH 서버 설정

OpenSSH 서버를 실행하기 위해서는, 우선 적절한 RPM 패키지가 설치되어 있는지 확인하셔야 합니다. `openssh-server` 패키지가 필요하며 이 패키지는 `openssh` 패키지에 의존성을 갖습니다.

OpenSSH 데몬은 `/etc/ssh/sshd_config` 설정 파일을 사용합니다. 대부분의 경우 Red Hat Linux에 설치된 기본 설정 파일이면 충분합니다. 기본 `sshd_config` 파일에는 없는 방식으로 데몬을 설정하시려면, `sshd` 메뉴얼 페이지를 참조하여 설정 파일에서 정의 가능한 키워드 목록을 살펴보시기 바랍니다.

OpenSSH 서비스를 시작하기 위해서는 `/sbin/service sshd start` 명령을 사용합니다. `/sbin/service sshd stop` 명령을 사용하여 OpenSSH 서버를 멈출 수 있습니다. 시스템 부팅시 데몬이 자동으로 시작되도록 설정하시려면, 14 장에서 서비스를 관리하는 방법에 대한 정보를 참조하십시오.

Red Hat Linux 시스템을 재설치하신 경우, 재설치하기 이전에 OpenSSH 도구로 연결되었던 클라이언트 컴퓨터가 연결되어 있었다면, 재설치가 끝난 후 클라이언트 사용자에게 다음과 같은 메시지가 나타날 것입니다:

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@ WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED! @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that the RSA host key has just been changed.
```

재설치된 시스템은 새로운 인증키 세트를 생성합니다; 따라서 RSA 호스트 키가 변경된 것에 대한 경고가 나타나게 됩니다. 새로 생성된 호스트 키를 보존하시려면, `/etc/ssh/ssh_host*key*` 파일을 백업하신 후 재설치가 완료되면 파일을 복구하십시오. 이러한 과정을 거쳐 시스템을 동일하게 설정하면 재설치가 끝나고 클라이언트가 시스템에 접속할 때 경고 메시지가 나타나지 않습니다.

15.3. OpenSSH 클라이언트 설정

클라이언트 컴퓨터에서 OpenSSH 서버로 접속하기 위해서는 클라이언트 컴퓨터 상에 `openssh-clients` 패키지와 `openssh` 패키지가 설치되어 있어야 합니다.

15.3.1. ssh 명령어 사용하기

`ssh` 명령은 `rlogin`, `rsh`, `telnet` 명령의 보안 대체입니다. `ssh` 명령을 사용하여 원격 컴퓨터에 로그인하실 수 있으며 명령 실행도 가능합니다.

`ssh` 명령을 사용하여 원격 컴퓨터에 로그인하는 것은 `telnet` 명령을 사용하는 방식과 유사합니다. 예를 들어, penguin.example.net이라는 원격 컴퓨터에 로그인하기 위해서는, 쉘 프롬프트 상에서 다음과 같은 명령을 입력합니다:

```
ssh penguin.example.net
```

원격 컴퓨터에 처음으로 `ssh` 하신 경우, 다음과 같은 메시지를 보실 것입니다:

```
The authenticity of host 'penguin.example.net' can't be established.
DSA key fingerprint is 94:68:3a:3a:bc:f3:9a:9b:01:5d:b3:07:38:e2:11:0c.
Are you sure you want to continue connecting (yes/no)?
```

yes를 입력하여 계속 진행합니다. 이렇게 하여 다음에 메시지에서 보이듯이 알려진 호스트의 목록에 해당 서버가 추가됩니다:

```
Warning: Permanently added 'penguin.example.net' (RSA) to the list of known hosts.
```

다음으로 원격 컴퓨터에 접속하기 위한 암호를 입력하셔야 합니다. 암호를 입력하시면, 원격 컴퓨터의 쉘 프롬프트가 나타납니다. 특별히 사용자명을 지정하지 않으시면, 로컬 클라이언트 컴퓨터에서 로그인하셨던 사용자명이 원격 컴퓨터로 전달됩니다. 다른 사용자명을 지정하기 위해서는 다음 명령을 사용하십시오:

```
ssh username@penguin.example.net
```

`ssh -l 사용자명 penguin.example.net` 구문을 사용하셔도 됩니다.

`ssh` 명령을 사용하여 쉘 프롬프트에 로그인할 필요가 없이 원격 컴퓨터 상에서 명령을 실행할 수 있습니다. 명령어 구문은 `ssh hostname command` 입니다. 예를 들어 만일 `ls /usr/share/doc` 명령을 penguin.example.net 원격 컴퓨터에서 실행하고 싶다면, 쉘 프롬프트에서 다음과 같은 명령을 입력합니다:

```
ssh penguin.example.net ls /usr/share/doc
```

올바른 암호를 입력하시면 원격 디렉토리 `/usr/share/doc`의 내용을 출력 후, 여러분의 로컬 쉘 프롬프트로 되돌아 옵니다.

15.3.2. scp 명령어 사용하기

`scp` 명령은 컴퓨터 사이에 안전하고 암호화된 연결을 통하여 파일을 전송하는데 사용됩니다. `rcp`와 유사합니다.

원격 시스템으로 로컬 파일을 전송할 때 사용되는 일반적인 명령 구문은 다음과 같습니다:

```
scp localfile username@tohostname:/newfilename
```

여기서 *`localfile`*은 소스를 지정하며 *`username@tohostname:/newfilename`*은 파일이 전단될 목적지를 지정합니다.

예를 들어 penguin.example.net의 사용자 계정으로 `shadowman` 로컬 파일을 전송하기 위해서는, 쉘 프롬프트에서 다음과 같이 입력합니다. (다음 명령에서 *`username`*을 여러분의 계정명으로 교체하십시오):

```
scp shadowman username@penguin.example.net:/home/username
```

위의 명령은 shadowman 로컬 파일을 penguin.example.net 컴퓨터의 /home/*username*/shadowman으로 전송할 것입니다

원격 컴퓨터에서 로컬 시스템으로 파일을 전송하기 위해서는 다음과 같은 명령 구문이 사용됩니다:

```
scp username@tohostname:/remotefile /newlocalfile
```

여기서 *remotefile*은 소스를 지정하며, *newlocalfile*은 파일이 전달될 목적지를 지정합니다.

여러 개의 파일을 소스 파일로 지정 가능합니다. 예를 들어 /downloads 디렉토리의 내용을 원격 컴퓨터 penguin.example.net 상의 기존 uploads 디렉토리로 전송하기 위해서는, 쉘 프롬프트 상에서 다음 명령을 입력합니다:

```
scp /downloads/* username@penguin.example.net:/uploads/
```

15.3.3. sftp 명령어 사용하기

sftp 유틸리티는 상호 대화식의 보안 FTP 세션을 여는데 사용됩니다. ftp와 유사하지만 sftp는 암호화된 보안 접속을 사용한다는 차이점이 있습니다. 일반적인 명령 구문은 *sftp username@hostname.com* 입니다. 일단 사용자 인증이 끝나면, FTP에서 사용되는 것과 유사한 명령어를 사용하실 수 있습니다. 사용 가능한 명령어 목록을 보시려면 sftp 메뉴얼 페이지를 참조하시기 바랍니다. 메뉴얼 페이지를 읽기 위해서는, 쉘 프롬프트에서 man sftp 명령을 실행합니다. sftp 유틸리티는 OpenSSH 2.5.0p1 이후 버전에서만 사용 가능합니다.

15.3.4. 키 쌍 생성하기

ssh, scp, 또는 sftp 명령을 사용하여 원격 컴퓨터에 접속할 때마다 암호를 입력하는 것을 원치 않으시면, 인증 키 쌍 (authorization key pair)을 생성하시면 됩니다.

각각의 사용자를 위한 키를 생성하셔야 합니다. 원격 컴퓨터에 접속하려는 사용자를 위한 키를 생성하시려면, 다음과 같은 단계를 따르십시오. 만일 루트로서 키를 생성하시면, 루트 사용자만이 그 키를 사용할 수 있습니다.

OpenSSH 3.0 버전 이후로 ~/.ssh/authorized_keys2, ~/.ssh/known_hosts2, /etc/ssh_known_hosts2 파일은 사용되지 않습니다. SSH 프로토콜 1 과 2는 ~/.ssh/authorized_keys, ~/.ssh/known_hosts, /etc/ssh/ssh_known_hosts 파일을 공유합니다.

Red Hat Linux 9은 SSH Protocol 2과 RSA 키를 기본으로 사용합니다.

힌트

Red Hat Linux를 재설치하시는 경우 생성된 키 쌍을 저장하기 위해서는 홈 디렉토리에 위치한 .ssh 디렉토리를 백업하십시오. 재설치가 완료되면 이 디렉토리를 홈 디렉토리로 복구합니다. 루트를 포함한 모든 사용자의 키 쌍을 동일한 방법으로 저장 가능합니다.

15.3.4.1. 2.0 버전에 사용되는 RSA 키 쌍 생성하기

SSH 프로토콜 2.0 버전에 사용되는 RSA 키 쌍을 생성하기 위해서는 다음과 같은 단계를 따르십시오. OpenSSH 2.9 이후 버전에서 2.0 버전 SSH 프로토콜이 기본으로 사용됩니다.

1. 2.0 버전 프로토콜과 함께 사용될 RSA 키 쌍을 생성하기 위해서는 쉘 프롬프트에서 다음과 같은 명령을 입력합니다:

```
ssh-keygen -t rsa
```

~/.ssh/id_rsa의 기본 파일 위치를 수용합니다. 여러분의 사용자 계정 암호와는 다른 암호 문구(passphrase)를 입력하신 후 확인을 위해 한번 더 입력해 주십시오.

공개키는 ~/.ssh/id_rsa.pub 파일에 기록되고 비밀키는 ~/.ssh/id_rsa 파일에 기록됩니다. 절대로 여러분의 개인키를 다른 사람과 공유해서는 안됩니다.

2. chmod 755 ~/.ssh 명령어를 사용하여 .ssh 디렉토리에 대한 허가를 변경합니다.
3. ~/.ssh/id_rsa.pub 파일의 내용을 연결할 컴퓨터의 ~/.ssh/authorized_keys 파일로 복사합니다. 만일 ~/.ssh/authorized_keys 파일이 존재하지 않는 경우, ~/.ssh/id_rsa.pub 파일을 다른 컴퓨터의 ~/.ssh/authorized_keys 파일로 복사하셔도 됩니다.
4. GNOME을 실행 중이라면 15.3.4.4 절로 넘어 가십시오. X 윈도우 시스템을 실행하지 않는 경우에는 15.3.4.5 절로 넘어 가십시오.

15.3.4.2. 2.0 버전에 사용되는 DSA 키 쌍 생성하기

SSH 프로토콜 2.0 버전에 사용될 DSA 키 쌍을 생성하기 위해서는 다음과 같은 단계를 따르십시오.

1. 2.0 버전 프로토콜과 함께 사용될 DSA 키 쌍을 생성하기 위해서는 쉘 프롬프트에서 다음과 같은 명령을 입력합니다:
   ```
   ssh-keygen -t dsa
   ```

   ~/.ssh/id_dsa의 기본 파일 위치를 수용합니다. 여러분의 사용자 계정 암호와는 다른 암호 문구를 입력하신 후 확인을 위해 한번 더 입력해 주십시오.

   

   힌트

   암호 문구는 사용자 인증을 위해 사용되는 문자열로서 단어와 문자로 이루어 졌습니다. 문자열은 스페이스와 탭을 사용할 수 있다는 점에서 암호와 차이가 있습니다. 암호 문구는 한 단어가 아닌 하나의 문구로 이루어졌기 때문에 보통 암호보다 더 깁니다.

   공개키는 ~/.ssh/id_dsa.pub 파일에 기록되고 비밀키는 ~/.ssh/id_dsa 파일에 기록됩니다. 절대로 여러분의 비밀키를 다른 사람과 공유해서는 안됩니다.
2. chmod 755 ~/.ssh 명령어를 사용하여 .ssh 디렉토리에 대한 허가를 변경합니다.
3. ~/.ssh/id_dsa.pub 파일의 내용을 연결할 컴퓨터의 ~/.ssh/authorized_keys 파일로 복사합니다. 만일 ~/.ssh/authorized_keys 파일이 존재하지 않는 경우, ~/.ssh/id_dsa.pub 파일을 다른 컴퓨터의 ~/.ssh/authorized_keys 파일로 복사하셔도 됩니다.
4. GNOME을 실행 중이라면 15.3.4.4 절으로 넘어 가십시오. X 윈도우 시스템을 실행하지 않는 경우에는 15.3.4.5 절로 넘어 가십시오.

15.3.4.3. 1.3 과 1.5 버전에 사용되는 RSA 키 쌍 생성하기

SSH 프로토콜 1.0 버전에서 사용되는 RSA 키 쌍을 생성하기 위해서는 다음과 같은 단계를 따르십시오. 단순히 DSA를 사용하는 시스템들을 연결하는 경우라면 RSA 1.3 버전과 RSA 1.5 버전 키 쌍이 필요하지 않습니다.

1. RSA (버전 1.3과 1.5 프로토콜) 키 쌍을 생성하기 위해서는 쉘 프롬프트 상에서 다음과 같은 명령을 입력하십시오:
   ```
   ssh-keygen -t rsa1
   ```

   ~/.ssh/identity의 기본 파일 위치를 수용합니다. 여러분의 사용자 계정 암호와는 다른 암호 문구를 입력하신 후 확인을 위해 한번 더 입력해 주십시오.

공개키는 ~/.ssh/identity.pub 파일에 기록되고 개인키는 ~/.ssh/identity 파일에 기록됩니다. 절대로 여러분의 개인키를 다른 사람과 공유해서는 안됩니다.

2. chmod 755 ~/.ssh 명령어를 사용하여 .ssh 디렉토리에 대한 허가를 변경하고 chmod 644 ~/.ssh/identity.pub 명령어를 사용하여 여러분의 키에 대한 허가를 변경하시기 바랍니다.
3. ~/.ssh/identity.pub 파일의 내용을 연결할 컴퓨터의 ~/.ssh/authorized_keys 파일로 복사합니다. 만일 ~/.ssh/authorized_keys 파일이 존재하지 않는 경우, ~/.ssh/identity.pub 파일을 다른 컴퓨터의 ~/.ssh/authorized_keys 파일로 복사하셔도 됩니다.
4. GNOME을 실행 중이라면 15.3.4.4 절으로 넘어 가십시오. GNOME을 실행하지 않는 경우에는 15.3.4.5 절로 넘어 가십시오.

15.3.4.4. GNOME을 사용하여 ssh-agent 설정하기

ssh-agent 유틸리티를 사용하여 ssh와 scp 연결 때마다 암호 문구를 입력할 필요가 없도록 암호 문구를 저장할 수 있습니다. GNOME을 사용하신다면 openssh-askpass-gnome 유틸리티는 사용자가 GNOME에 로그인할 때 암호 문구를 요청한 후 그 사용자가 GNOME에서 로그 아웃할 때까지 그 암호 문구를 저장해 놓습니다. 따라서 GNOME 세션을 사용하는 동안 ssh 또는 scp 연결을 위하여 암호나 암호 문구를 입력하실 필요가 없습니다. GNOME을 사용하지 않으신다면 15.3.4.5 절를 참조해 보십시오.

GNOME 세션을 사용하는 동안 암호 문구를 저장하기 위해서는 다음의 단계를 따르십시오

1. openssh-askpass-gnome 패키지가 설치되어 있어야 합니다; 패키지가 설치되어 있는지 여부를 알아보기 위해서 rpm -q openssh-askpass-gnome 명령을 사용합니다. 만일 설치되어 있지 않다면, Red Hat CD-ROM 세트나 Red Hat FTP 미러 사이트, 또는 Red Hat Network를 사용하여 해당 패키지를 설치하시기 바랍니다.
2. 패널에서 **주 메뉴 버튼** => **환경 설정** => **추가 환경 설정** => **세션**을 선택하신 후 **시작 프로그램** 탭을 클릭하시기 바랍니다. **추가** 버튼을 클릭하시고 **시작 명령** 텍스트 입력란에 **/usr/bin/ssh-add**를 입력하십시오. 이 명령이 가장 마지막에 실행되도록 다른 기존의 명령보다 우선순위 번호를 높게 설정합니다. ssh-add 명령에 대한 우선순위 번호는 70 또는 그 이상의 숫자가 적합합니다. 우선순위 번호가 높을 수록, 실행되는 우선순위는 낮아집니다. 목록에 다른 프로그램이 있다면 이 프로그램에게 가장 낮은 우선순위를 주어야 합니다. **종료** 버튼을 클릭하여 프로그램을 종료합니다.
3. GNOME에서 로그 아웃한 후 다시 GNOME으로 로그인 하십시오; 즉, X를 재시작하십시오. GNOME이 시작된 후 암호 문구를 요구하는 대화 상자가 나타날 것입니다. 암호 문구를 입력하십시오. 만일 DSA와 RSA 키 쌍이 모두 설정되었다면, 두 키 쌍에 대한 암호 문구를 요청할 것입니다. 이후 ssh, scp, sftp 명령을 사용하실 경우 암호를 입력하실 필요가 없습니다.

15.3.4.5. ssh-agent 설정하기

ssh-agent 유틸리티를 사용하여 ssh와 scp 연결 때마다 암호 문구를 입력할 필요가 없도록 암호 문구를 저장할 수 있습니다. X 윈도우 시스템을 실행하지 않는 경우에는 쉘 프롬프트 상에서 다음의 단계를 따르십시오. 만일 GNOME을 사용하시는 경우 로그인시 암호를 입력하지 않아도 되도록 설정하시려면 (15.3.4.4 절 참조), Xterm과 같은 터미널 창에서 이 절차를 따르십시오. GNOME이 아닌 X를 실행 중이라면 터미널 창에서 이 절차를 따르시면 됩니다. 하지만 암호 문구는 전체 설정이 아니므로 해당 터미널 창에서만 기억됩니다.

1. 쉘 프롬프트에서 다음의 명령을 입력하십시오:
   ```
   exec /usr/bin/ssh-agent $SHELL
   ```
2. 그 후 다음의 명령을 입력합니다:
   ```
   ssh-add
   ```
   그리고 암호 문구를 입력하십시오. 한개 이상의 키 쌍이 설정되었다면, 각각의 키 쌍에 대한 암호 문구가 요구될 것입니다.

3. 로그 아웃 후에는 암호 문구는 더 이상 기억되지 않습니다. 가상 콘솔에 로그인할 때마다 또는 터미널 창을 열 때마다 앞에서 언급된 두 명령을 실행하셔야 합니다.

15.4. 추가 자료

OpenSSH와 OpenSSL 프로젝트는 계속적으로 개발 중이며 따라서 가장 최근의 정보는 웹사이트에서 찾으실 수 있습니다. OpenSSH와 OpenSSL 도구에 대한 메뉴얼 페이지도 자세한 정보를 찾기 위한 좋은 자료가 될 수 있습니다.

15.4.1. 설치된 문서 자료

- `ssh`, `scp`, `sftp`, `sshd`, `ssh-keygen` 메뉴얼 페이지 — 이 메뉴얼 페이지에는 명령어 사용 방법을 비롯한 이 명령어와 함께 사용 가능한 모든 매개 변수에 대한 정보가 포함되어 있습니다.

15.4.2. 유용한 웹사이트

- http://www.openssh.com — OpenSSH FAQ 페이지, 버그 리포트, 메일링 리스트, 프로젝트 목표와 보안 기능에 대한 더욱 기술적인 설명을 찾으실 수 있습니다.
- http://www.openssl.org — OpenSSL FAQ 페이지, 메일링 리스트와 프로젝트 목표에 대한 설명을 찾으실 수 있습니다.
- http://www.freessh.org — 다른 플랫폼을 위한 SSH 클라이언트 소프트웨어.

네트워크 파일 시스템 (NFS)

네트워크 파일 시스템 (NFS)은 네트워크로 연결된 서로 다른 컴퓨터의 디스크 공간을 하나로 묶어 하나의 디렉토리 구조로 파일을 공유하는 방식입니다. Red Hat Linux는 NFS 서버와 NFS 클라이언트로 작동할 수 있습니다. 즉, 다른 시스템으로 파일 시스템을 내보내는 서버로 기능하면서 동시에 다른 서버에서 가져온 파일 시스템을 마운트하는 클라이언트도 될 수 있다는 것을 의미합니다.

16.1. NFS를 사용하는 이유?

NFS는 동일한 네트워크로 연결된 컴퓨터를 사용하는 여러 사용자들 사이에서 파일 디렉토리를 공유하는데 유용하게 사용됩니다. 예를 들어, 여러 명의 사용자가 한 프로젝트에 참여하고 있는 경우, (흔히 NFS 공유라고 알려진) NFS 파일 시스템의 공유 디렉토리를 사용하여 마운트된 `/myproject` 디렉토리 안에 프로젝트에 사용되는 파일을 저장하여 함께 사용 가능합니다. 사용자는 자신의 컴퓨터에 있는 `/myproject` 디렉토리에 가서 공유 파일에 접근할 수 있습니다. 공유 디렉토리는 암호를 입력하거나 특별한 명령어를 기억할 필요가 없이 마치 로컬 컴퓨터 상에 위치하는 디렉토리처럼 사용됩니다.

16.2. NFS 파일 시스템 마운트하기

`mount` 명령을 사용하여 다른 컴퓨터의 공유 NFS 디렉토리를 로컬 컴퓨터 상에 마운트하실 수 있습니다. 예로 들면:

```
mount shadowman.example.com:/misc/export /misc/local
```


경고

로컬 컴퓨터 상에는 마운트할 지점인 디렉토리 (위의 예시에서는 `/misc/local`디렉토리)가 반드시 존재해야 합니다.

위의 명령에서 `shadowman.example.com` 부분은 NFS 파일서버의 호스트명이고, `/misc/export`는 `shadowman` 상에서 내보낼 디렉토리이며, 마지막으로 `/misc/local`은 로컬 컴퓨터 상에서 파일 시스템이 마운트될 위치입니다. `mount` 명령을 실행 후 (그리고 클라이언트가 `shadowman.example.com` NFS 서버로부터 적절한 권한을 가지고 있다면), 클라이언트 사용자는 `ls /misc/local` 명령을 입력하여 `shadowman.example.com` 컴퓨터에 있는 `/misc/export` 디렉토리에 저장된 파일 목록을 볼 수 있습니다.

16.2.1. `/etc/fstab`를 사용하여 NFS 파일 시스템 마운트하기

다른 컴퓨터로부터 NFS 공유를 마운트할 수 있는 또 다른 방법은 `/etc/fstab` 파일에 새로운 줄을 첨가하는 것입니다. NFS 서버의 호스트명, 보내질 디렉토리명, NFS 공유가 마운트될 로컬 컴퓨터 상의 디렉토리명이 언급되어야 합니다. `/etc/fstab` 파일을 수정하시려면, 루트로 로그인하셔야 합니다.

`/etc/fstab`에 첨가될 줄은 다음과 같은 형식으로 작성됩니다:

```
server:/usr/local/pub  /pub nfs  rsize=8192,wsize=8192,timeo=14,intr
```

마운트 지점인 `/pub` 은 반드시 클라이언트 컴퓨터 상에 위치해야 합니다. 클라이언트 시스템에서 `/etc/fstab` 파일에 위의 줄을 첨가하신 후, 쉘 프롬프트에서 `mount /pub` 명령을 입력하시면, `/pub` 디렉토리가 마운트됩니다.

16.2.2. autofs를 사용하여 NFS 파일 시스템 마운트하기

NFS 공유를 마운트하기 위한 세번째 옵션은 autofs를 사용하는 것입니다. Autofs는 자동마운트 데몬을 사용하여 필요한 경우에만 마운트하는 동적 마운트 방식입니다.

Autofs는 마스터 맵(map) 설정 파일인 `/etc/auto.master`를 참고하여 이미 정의된 마운트 지점을 알아냅니다. 그 후 각 마운트 지점에 사용되는 적절한 매개 변수를 가지고 자동 마운트 과정을 시작합니다. 마스터 맵 파일은 한 줄마다 마운트 지점과 이 마운트 지점 아래에 마운트된 파일 시스템을 정의하는 별개의 맵 파일을 정의합니다. 예를 들어, `/etc/auto.misc` 파일은 `/misc` 디렉토리 내의 마운트 지점들을 정의하는 맵 파일입니다; 이러한 관계는 `/etc/auto.master` 파일에 정의되어 있습니다.

`auto.master` 파일에 포함된 각 항목들은 3가지 부분으로 나뉘어 있습니다. 첫번째 부분은 마운트 지점이고, 두번째 부분은 맵 파일의 위치이며 세번째 부분은 있어도 되고 없어도 되는 선택 사항으로서 제한시간(timeout) 값과 같은 정보가 포함됩니다.

예를 들어, 원격 컴퓨터 penguin.host.net 상의 `/proj52` 디렉토리를 여러분 컴퓨터 상의 `/misc/myproject` 디렉토리로 마운트하시려면, `auto.master` 파일에 다음과 같은 줄을 첨가해 주십시오:

```
/misc  /etc/auto.misc --timeout 60
```

다음 줄을 `/etc/auto.misc` 파일에 추가하십시오:

```
myproject -rw,soft,intr,rsize=8192,wsize=8192 penguin.example.net:/proj52
```

`/etc/auto.misc`의 첫번째 부분은 `/misc` 하부 디렉토리 이름입니다. 이 디렉토리는 자동 마운트 기능을 사용하여 동적으로 생성되었기 때문에 클라이언트 컴퓨터 상에 실제로 존재하지는 않습니다. 두번째 영역에는 읽기 쓰기 권한에 사용되는 `rw`와 같은 마운트 옵션이 포함됩니다. 세번째 부분에는 NFS 내보내기되는 호스트명과 디렉토리의 위치입니다.

알림

로컬 파일 시스템 상에 `/misc` 디렉토리가 있어야 하며, 이 `/misc` 디렉토리에는 어떠한 하부 디렉토리도 존재해서는 안됩니다.

Autofs는 서비스입니다. 이 서비스를 시작하기 위해서는 쉘 프롬프트에서 다음 명령을 입력하십시오:

```
/sbin/service autofs restart
```

사용 중인 마운트 지점을 보시려면, 쉘 프롬프트에서 다음 명령을 입력하시면 됩니다:

```
/sbin/service autofs status
```

autofs가 실행되는 동안 `/etc/auto.master` 설정 파일을 수정하신다면, 쉘 프롬프트에서 다음 명령을 입력하여 자동 마운트 데몬이 다시 읽혀지도록 하셔야 합니다:

```
/sbin/service autofs reload
```

부팅시 autofs가 시작되도록 설정하시려면, 서비스 관리 방법에 대한 자세한 사항을 14 장에서 찾아보시기 바랍니다.

16.3. NFS 파일 시스템 보내기

NFS 서버에서 파일을 공유하는 것은 디렉토리를 보내기(export)하는 것과 같습니다. 여러분은 **NFS 서버 설정 도구**를 사용하여 로컬 시스템을 NFS 서버로 설정하실 수 있습니다.

NFS 서버 설정 도구를 사용하기 위해서는 우선 X 윈도우 시스템이 실행 중이고, 루트 권한이 있어야 하며, `redhat-config-nfs` RPM 패키지가 설치되어 있어야 합니다. 이 프로그램을 시작하시려면, 패널에서 **주 메뉴 버튼** => **시스템 설정** => **서버 설정** => **NFS 서버**를 선택하시거나, 쉘 프롬프트에서 `redhat-config-nfs` 명령을 입력하시면 됩니다.

그림 16-1. NFS 서버 설정 도구

NFS 공유를 추가하기 위해서 **추가** 버튼을 클릭하시면, 그림 16-2에서 보여지는 것과 같은 대화 상자가 나타날 것입니다.

기본 탭에서 다음과 같은 정보를 입력해 주십시오:

- **디렉토리** — 공유할 디렉토리를 지정해 주십시오. 예, `/tmp`
- **호스트(들)** — 디렉토리를 공유할 호스트를 지정해 주십시오. 사용 가능한 호스트명 형식에 대한 설명을 원하신다면, 16.3.2 절을 참조하시기 바랍니다.
- **기본 허가** — 디렉토리에 적용될 읽기-전용 허가 또는 읽기/쓰기 허가를 지정해 주십시오.

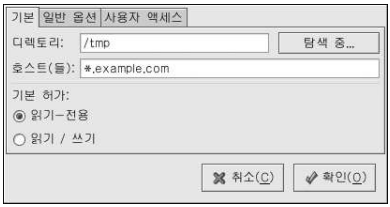

그림 16-2. 공유 추가

일반 옵션 탭에서는 다음과 같은 옵션을 설정 가능합니다:

- **1024 이상 포트에서의 접속 허용** — 1024 이하 포트에서의 서비스는 루트 사용자만 시작할 수 있습니다. 루트가 아닌 사용자가 시작한 NFS 서비스를 허용하시려면 이 옵션을 선택하십시오. 이 옵션은 `insecure` 명령에 해당합니다.
- **비보안 파일 잠금 허용** — 잠금 요청을 사용하지 않음. 이 옵션은 `insecure_locks` 명령에 해당합니다.
- **하부구조 검사 사용않함** — 파일 시스템의 전체 디렉토리가 아닌 하부 디렉토리가 내보내진 경우, 서버는 내보낸 하부 디렉토리에 요청된 파일이 존재하는지를 검사합니다. 이러한 검사 과정을 하부구조 검사라고 부릅니다. 이 옵션을 선택하시면 하부구조 검사를 사용하지 않습니다. 전체 파일 시스템이 내보내진 경우에 이 옵션을 선택하시면 하부구조 검사를 하지 않음으로서 전송률을 높일 수 있습니다. 이 옵션은 `no_subtree_check` 명령에 해당합니다.
- **요청시 쓰기 작업을 동기화함** — 기본으로 선택되는 이 옵션은 변경 사항을 디스크에 기록하기 전에는 서버가 요청에 응답하는 것을 허용하지 않습니다. 이 옵션은 `sync` 명령에 해당합니다. 만일 이 옵션이 선택되지 않으면, `async` 옵션이 사용됩니다.
  - **즉시 쓰기 작업 동기화를 강제함** — 즉시 디스크에 기록합니다. 이 옵션은 `no_wdelay` 명령에 해당합니다.

다음 **사용자 액세스** 탭에서는 다음과 같은 옵션을 설정 가능합니다:

- **원격 루트 사용자를 로컬 루트로 취급함** — 디폴트 값으로 루트 사용자의 사용자 ID와 그룹 ID는 모두 0 입니다. 이 옵션을 사용하시면 익명 사용자의 사용자 ID와 그룹 ID에 사용자 ID 0와 그룹 ID 0를 부여하여 원격 루트 사용자를 로컬 루트로 취급합니다. 따라서 클라이언트 상의 루트 사용자는 디렉토리를 내보내기할 수 있는 권한을 갖게 됩니다. 이 옵션을 선택하시면 시스템 보안이 매우 약해집니다. 절대로 필요한 상황이 아니면 이 옵션을 선택하지 마십시오. 이 옵션은 `no_root_squash` 명령에 해당합니다.
- **클라이언트 사용자를 익명(anonymous) 사용자로 취급함** — 이 옵션이 선택되면 모든 사용자 ID와 그룹 ID는 익명 사용자로 취급됩니다. 이 옵션은 `all_squash`에 해당합니다.
  - **익명 사용자를 위한 로컬 사용자 ID를 지정** — 만일 **클라이언트 사용자를 익명(anonymous) 사용자로 취급함** 옵션이 선택된 경우, 이 옵션을 선택하시면 익명 사용자를 위한 사용자 ID를 지정하실 수 있습니다. 이 옵션은 `anonuid`에 해당합니다.
  - **익명 사용자를 위한 로컬 그룹 ID를 지정** — 만일 **클라이언트 사용자를 익명(anonymous) 사용자로 취급함** 옵션이 선택된 경우, 이 옵션을 선택하시면 익명 사용자를 위한 그룹 ID를 지정하실 수 있습니다. 이 옵션은 `anongid`에 해당합니다.

기존 NFS 공유를 편집하시려면, 목록에서 편집할 공유를 선택하신 후 **등록 정보** 버튼을 클릭하십시오. 기존 NFS 공유를 삭해하시려면, 목록에서 삭제할 공유를 선택하신 후 **삭제** 버튼을 클릭하시기 바랍니다.

목록에서 NFS 공유를 추가, 편집, 또는 삭제하신 후 **확인** 버튼을 클릭하시면 변경 사항이 즉시 적용됩니다 — 즉, 서버 데몬이 재시작되고 이전 설정 파일은 `/etc/exports.bak`으로 저장됩니다. 그리고 새 설정은 `/etc/exports` 파일에 기록됩니다.

NFS 서버 설정 도구는 `/etc/exports` 설정 파일을 직접 읽고 기록합니다. 따라서 이 도구를 사용 후 파일을 직접 수정 가능하며, 파일이 올바른 구문을 사용하여 수정된 경우에는 수동으로 파일을 수정 후 다시 이 도구를 사용 가능합니다.

16.3.1. 명령행 설정

텍스트 편집기로 설정 파일을 편집하는 것을 선호하시거나 X 윈도우 시스템이 설치되어 있지 않은 경우에는, 설정 파일을 직접 수정하실 수 있습니다.

`/etc/exports` 파일은 NFS 서버가 내보낼 디렉토리를 결정합니다. 이 파일의 형식은 다음과 같습니다:

directory hostname(*options*)

sync 또는 async 중 한가지 옵션만 지정해 주시기 바랍니다 (sync 권장). 만일 sync 옵션이 지정되면, 서버는 요청에 의해 생긴 변경 사항이 디스크에 기록되기 전에는 요청에 응답하지 않습니다.

예로 들면:

```
/misc/export  speedy.example.com(sync)
```

명령은 speedy.example.com에서 접속한 사용자들이 기본 읽기 전용 허가를 가지고 /misc/export를 마운트할 수 있게 해줍니다, 그러나:

```
/misc/export  speedy.example.com(rw,sync)
```

명령은 speedy.example.com에서 접속한 사용자들이 읽기/쓰기 허가를 가지고 /misc/export를 마운트할 수 있도록 해줍니다.

사용 가능한 호스트명 형식에 대한 설명을 보시려면, 16.3.2 절을 참조하시기 바랍니다.

지정 가능한 옵션 목록은 *Red Hat Linux* 참조 가이드에서 찾아보실 수 있습니다.

경고

/etc/exports 파일에서 띄어쓰기(space)에 주의해 주십시오. 만일 호스트명과 괄호안의 옵션 사이에 아무런 빈 공간이 없다면, 옵션은 호스트명에만 적용됩니다. 만일 호스트명과 옵션 사이에 공간이 있다면, 그 옵션은 모두에게 적용됩니다. 다음의 예들을 살펴보십시오:

```
/misc/export speedy.example.com(rw,sync)
/misc/export speedy.example.com (rw,sync)
```

첫번째 줄은 speedy.example.com에서 접속하는 사용자에게 읽기 쓰기 허가를 주고 그 외 다른 사용자를 거부합니다. 두번째 줄은 speedy.example.com에서 접속하는 사용자에게 읽기 전용 (디폴트) 허가를 주며 그 외 다른 사용자에게 읽기 쓰기를 허용합니다.

/etc/exports 파일을 변경하실 때마다, NFS 데몬에게 변경 사항을 알리거나, 다음 명령을 사용하여 설정 파일을 다시 읽어들여야 합니다:

```
/sbin/service nfs reload
```

16.3.2. 호스트명 형식

호스트는 다음과 같은 형식으로 지정 가능합니다:

- 단독 컴퓨터 — 전체 도메인명 (fully qualified domain name), (서버가 해석가능한) 호스트명, 또는 IP 주소
- 특수 문자를 사용하여 여러 대의 컴퓨터의 지정하기 — 별표 (*)나 물음표 (?)와 같은 특수 문자를 사용하여 문자열을 지정할 수 있습니다. 예를 들어, `192.168.100.*`는 192.168.100로 시작하는 모든 IP 주소를 지정합니다. 전체 도메인명에 특수 문자를 지정할 경우에는 점 (.)이 사용되지 않습니다. 예로 들면 `*.example.com`에는 one.example.com이 포함되지만 one.two.example.com은 포함되지 않습니다.
- IP 네트워크 — *`a.b.c.d/z`*를 사용합니다. 여기서 *`a.b.c.d`*는 네트워크이고 *`z`*는 넷마스크의 비트 수를 나타냅니다 (예, 192.168.0.0/24). *`a.b.c.d/netmask`* 형식도 사용 가능합니다. 여기서 *`a.b.c.d`*는 네트워크이고 *`netmask`*는 넷마스크를 의미합니다. (예,192.168.100.8/255.255.255.0)
- 넷그룹 — *`@group-name`* 형식을 사용합니다. 여기서 *`group-name`* 부분은 NIS 그룹명입니다.

16.3.3. 서버 시작과 중지하기

NFS 파일 시스템을 보내는 서버 상에는 `nfs` 서비스가 반드시 실행 중이어야 합니다.

다음 명령을 사용하여 NFS 데몬의 상태를 확인하실 수 있습니다:

```
/sbin/service nfs status
```

다음 명령을 사용하여 NFS 데몬을 시작합니다:

```
/sbin/service nfs start
```

NFS 데몬을 중지하려면 다음 명령을 사용하시기 바랍니다:

```
/sbin/service nfs stop
```

시스템 부팅시 `nfs` 서비스가 시작되도록 설정하시려면 다음 명령을 사용하십시오:

```
/sbin/chkconfig --level 345 nfs on
```

또한 `chkconfig`, **ntsysv** 또는 **서비스 설정 도구**를 사용하여 부팅시 시작될 서비스를 설정하실 수 있습니다. 보다 자세한 사항은 14 장을 참조하시기 바랍니다.

16.4. 추가 자료

이 장에서는 기본적인 NFS 사용법에 대하여 다루고 있습니다. 이 장에서 다루어지지 않은 보다 자세한 정보를 원하신다면, 다음과 같은 자료들을 참조하시기 바랍니다.

16.4.1. 설치된 문서 자료

- `nfsd`, `mountd`, `exports`, `auto.master`, `autofs` (메뉴얼 섹션 5와 8)의 메뉴얼 페이지 — NFS와 autofs 설정 파일에 사용되는 올바른 구문을 보여줍니다.

16.4.2. 유용한 웹사이트

- http://www.tldp.org/HOWTO/NFS-HOWTO/index.html — 리눅스 문서화 프로젝트의 *Linux NFS-HOWTO*

16.4.3. 관련 서적

- *Managing NFS and NIS Services* 저자 Hal Stern; O'Reilly & Associates, Inc.

17장 . Samba

Samba는 SMB 프로토콜을 사용하여 네트워크 상에서 파일과 프린터를 공유할 수 있게 해줍니다. 이 프로토콜을 지원하는 운영 체제에는 Microsoft Windows (**네트워크 환경 (Network Neighborhood)**을 사용), OS/2, Linux가 있습니다.

17.1. Samba를 사용하는 이유?

Windows와 Linux에 동시에 연결된 네트워크의 경우, Samba가 유용하게 사용됩니다. Samba를 사용하여 네트워크 내의 모든 시스템이 파일과 프린터를 공유할 수 있습니다. Red Hat Linux 시스템 사이에서만 파일을 공유하도록 설정하시려면, 16 장에서 설명된 NFS를 사용하시기 바랍니다. Red Hat Linux 시스템 사이에서만 프린터를 공유하도록 설정하시려면, Samba를 사용하실 필요가 없습니다; 27 장을 참조하시기 바랍니다.

17.2. Samba 서버 설정하기

디폴트 설정 파일 (`/etc/samba/smb.conf`)은 사용자가 자신의 Red Hat Linux 홈 디렉토리를 Samba 공유로 사용할 수 있게 해줍니다. 즉, 네트워크 연결된 Windows 컴퓨터에서 Red Hat Linux 시스템에 연결된 프린터로 인쇄할 수 있습니다.

17.2.1. 그래픽 모드로 설정

그래픽 인터페이스를 사용하여 Samba를 설정하시려면, **Samba 서버 설정 도구**를 사용하시기 바랍니다. 명령행을 사용한 설정을 원하시면, 17.2.2 절로 넘어 가십시오.

Samba 서버 설정 도구는 Samba 공유와 사용자, 그리고 기초 서버 설정을 관리하는 그래픽 인터페이스입니다. 이 프로그램은 `/etc/samba/` 디렉토리에 저장된 설정 파일들을 수정합니다. 이 프로그램을 사용하지 않고 설정 파일이 변경되었다면, 그 설정은 변경되지 않고 보존됩니다.

이 응용 프로그램을 사용하시려면, X 윈도우 시스템이 실행 중이고, 루트 허가가 있어야 하며, `redhat-config-samba` RPM 패키지가 설치되어 있어야 합니다. 데스크탑에서 **Samba 서버 설정 도구**를 시작하기 위해서 패널에서 **주 메뉴 버튼** => **시스템 설정** => **서버 설정** => **Samba 서버**를 선택하시거나 쉘 프롬프트 (예, XTerm이나 GNOME 터미널)에서 `redhat-config-samba` 명령을 입력하시기 바랍니다.

그림 17-1. Samba 서버 설정 도구

알림

Samba 서버 설정 도구는 공유 프린터나 Samba 서버 상에서 사용자의 홈 디렉토리를 볼 수 있게 해주는 기본 설정을 보여주지 않습니다.

17.2.1.1. 서버 설정

Samba 서버를 설정하는 첫번째 단계는 서버에 대한 기초적인 설정과 몇몇 보안 옵션을 설정하는 것입니다. 응용 프로그램을 시작하신 후, 풀다운 메뉴에서 **설정** => **서버 설정**을 선택하시기 바랍니다. 그림 17-2에서처럼 **기본** 탭이 나타날 것입니다.

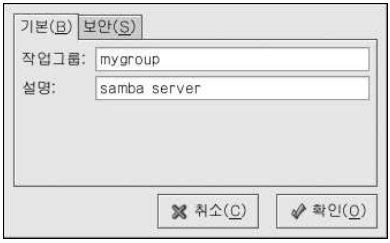

그림 17-2. 서버 기본 설정

기본 탭에서, 컴퓨터가 소속될 작업그룹과 컴퓨터에 대한 간단한 설명을 입력해 주십시오. 이곳에서 입력하신 정보는 `smb.conf` 파일에서 `workgroup`과 `server string` 명령에 해당합니다.

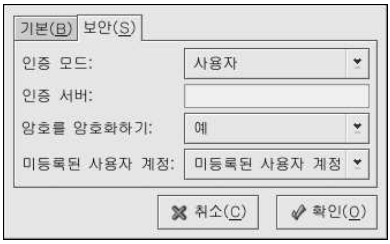

그림 17-3. 보안 서버 설정하기

보안 탭에는 다음과 같은 옵션이 있습니다:

- **인증 모드** — `security` 옵션에 해당합니다. 다음 중 한가지 인증 유형을 선택하실 수 있습니다.
  - **도메인** — Samba 서버가 Windows NT 일차 도메인 컨트롤러 또는 백업 도메인 컨트롤러를 사용하여 사용자를 인증하도록 설정. 서버는 사용자명과 암호를 컨트롤러에 전달 후 응답을 기다립니다. **인증 서버** 란에 일차 도메인 컨트롤러나 백업 도메인 컨트롤러의 NetBIOS 이름을 지정해 주십시오.

    암호를 암호화하기 옵션을 사용하시려면, **예** 항목을 선택하시기 바랍니다.
  - **서버** — Samba 서버가 사용자명과 암호 조합을 다른 Samba 서버에 보내어 인증 시도하도록 설정. 만일 다른 서버가 인증에 실패하면, 서버는 사용자 인증 모드를 사용하여 인증을 시도합니다. 따라서 **인증 서버** 란에 다른 Samba 서버의 NetBIOS 이름을 지정하시기 바랍니다.
  - **공유** — Samba 사용자가 Samba 서버마다 사용자명과 암호를 입력할 필요가 없는 설정. Samba 서버에서 특정 공유 디렉토리에 접속될 때까지 사용자명과 암호가 요청되지 않습니다.
  - **사용자** — (디폴트) Samba 사용자는 Samba 서버마다 유효한 사용자명과 암호를 입력하도록 설정. **Windows 사용자명** 옵션을 사용하시려면, 이 옵션을 선택하시기 바랍니다. 보다 자세한 정보는 17.2.1.2 절을 참조해 보십시오.

- **암호를 암호화하기** — (디폴트 값은 **예** 입니다) 클라이언트가 Windows 98, 서비스 팩 3을 갖춘 Windows NT 4.0, 또는 그 외 다른 Microsoft Windows 최신 버전으로부터 접속한다면, 이 옵션을 사용하셔야 합니다. 암호는 서버와 클라이언트 사이에서 누가 가로챌 가능성이 있는 평문 형식이 아닌 암호화된 형식으로 전달됩니다. 이 옵션은 `encrypted passwords` 옵션에 해당합니다. 암호화된 Samba 암호에 대한 보다 자세한 정보를 원하신다면, 17.2.3 절을 참조하시기 바랍니다.
- **미등록된 사용자 계정** — 사용자나 미등록된 사용자가 Samba 서버에 로그인할 경우, 서버 상에 등록된 유효한 사용자명과 일치해야 합니다. 시스템 상 기존 사용자명 중 미등록된(guest) Samba 계정이 될 사용자명을 선택해 주십시오. 미등록된 사용자가 Samba 서버에 로그인한다면, 선택하신 사용자와 동일한 허가를 갖게 됩니다. 이 옵션은 `guest account` 옵션에 해당합니다.

확인 버튼을 클릭하신 후, 변경 사항이 설정 파일에 기록되며 데몬이 재시작될 것입니다; 따라서 변경 사항이 즉시 효력을 발생합니다.

17.2.1.2. Samba 사용자 관리하기

Samba 서버 설정 도구를 사용하기 위해서는, Samba 사용자를 추가하기 이전에 Samba 서버로 작동하는 Red Hat Linux 시스템 상에서 활성화된 기존 사용자 계정이 있어야 합니다. Samba 사용자는 이미 존재하는 Red Hat Linux 사용자 계정과 관련됩니다.

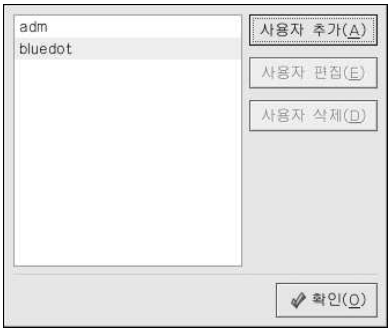

그림 17-4. Samba 사용자 관리

Samba 사용자를 추가하시려면, **설정** => 풀다운 메뉴에서 **Samba 사용자**를 선택하신 후 **사용자 추가** 버튼을 클릭하시면 됩니다. **새로운 Samba 사용자 만들기** 창에서, 지역 시스템 상에 이미 존재하는 사용자 목록에서 **Unix 사용자명**을 선택하시기 바랍니다.

만일 Windows 시스템에서 다른 사용자명을 가진 사용자가 Windows 시스템에서 Samba 서버로 로그인한다면, **Windows 사용자명** 란에 Windows 사용자명을 지정해 주십시오. 이 옵션을 사용하시려면, **서버 설정**의 **보안** 탭에서 **인증 모드**를 **사용자**로 설정하셔야 합니다.

또한 Samba 사용자의 **Samba 암호**를 설정해 주셔야 합니다. 암호를 입력하신 후 한번 더 입력하여 올바른 암호를 확인하시기 바랍니다. Samba에 암호화된 암호를 사용하기로 선택하셨더라도, 사용자의 Red Hat Linux 시스템 암호와는 다른 Samba 암호를 지정하시기 바랍니다.

기존 사용자를 편집하시려면, 목록에서 사용자를 선택하신 후 **사용자 편집** 버튼을 클릭하시면 됩니다. 기존 Samba 사용자를 삭제하시려면, 해당 사용자를 선택하신 후 **사용자 삭제** 버튼을 클릭하시기 바랍니다. Samba 사용자를 삭제하셔도 관련된 Red Hat Linux 사용자 계정은 삭제되지 않습니다.

확인 버튼을 클릭하시면, 사용자 정보가 즉시 수정됩니다.

17.2.1.3. 공유 추가하기

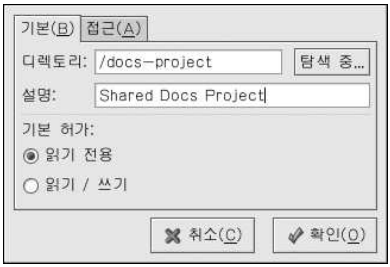

그림 17-5. 공유 추가

공유를 추가하시려면 **추가** 버튼을 클릭하시면 됩니다. **기본** 탭에서는 다음과 같은 옵션을 설정 가능합니다:

- **디렉토리** — Samba를 통해 공유할 디렉토리. 이미 존재하는 디렉토리여야 합니다.
- **설명** — 공유에 대한 간략한 설명.

- **기본 허가** — 사용자가 공유 디렉토리에 저장된 파일을 읽을 수 있도록 허용할 것인지 또는 사용자가 공유 디렉토리에 읽고 쓸 수 있도록 허용할 것인지 여부.

접근 탭에서는 오직 지정된 사용자만이 공유에 접근할 것인지 또는 모든 Samba 사용자가 공유에 접근할 수 있는지 여부를 선택해 주십시오. 특정 사용자만 접근할 수 있도록 허용하신다면, 사용 가능한 Samba 사용자 목록에서 허용할 사용자를 선택하시기 바랍니다.

확인 버튼을 클릭하시는 즉시 공유가 추가됩니다.

17.2.2. 명령행 설정

Samba는 `/etc/samba/smb.conf` 파일을 설정 파일로 사용합니다. 만일 이 설정 파일이 변경되면, `service smb restart` 명령을 사용하여 Samba 데몬을 재시작해야 변경 사항이 적용됩니다.

Windows 작업그룹과 Samba 서버에 대한 간략한 설명을 지정하시려면, `smb.conf` 파일에서 다음과 같은 줄을 편집하시면 됩니다:

```
workgroup = WORKGROUPNAME
server string = BRIEF COMMENT ABOUT SERVER
```

앞의 명령에서 *WORKGROUPNAME* 부분은 이 컴퓨터가 속할 Windows 작업그룹 이름으로 변경해 주십시오. *BRIEF COMMENT ABOUT SERVER* 란은 Samba 시스템에 대한 Windows의 간략한 설명으로서 작성하셔도 되고 안하셔도 무방합니다.

Linux 시스템 상에 Samba 공유 디렉토리를 만드시려면, `smb.conf` 파일을 여러분과 시스템의 필요에 맞게 수정시킨 후에 다음과 같은 부분을 첨가하시기 바랍니다:

```
[sharename]
comment = Insert a comment here
path = /home/share/
valid users = tfox carole
public = no
writable = yes
printable = no
create mask = 0765
```

위의 예시에서는 Samba 클라이언트 상의 tfox와 carole이라는 사용자가 Samba 서버 상의 `/home/share` 디렉토리를 읽고 쓸 수 있도록 해줍니다.

17.2.3. 암호화된 암호

Red Hat Linux 9에서는 보안 강화를 위하여 암호화된 암호 (encrypted password)를 기본으로 사용합니다. 암호화된 암호가 사용되지 않는 경우 평문(plain text) 암호를 사용합니다. 하지만 평문 암호는 다른 사용자가 네트워크 패킷 스니퍼 (network packet sniffer)를 사용하여 가로챌 가능성이 있습니다. 따라서 암호화된 암호를 사용하시기를 권장합니다.

Microsoft SMB 프로토콜은 평문 암호를 사용해왔습니다. 그러나 서비스 팩 3 이후 Windows NT, Windows 98, Windows 2000, Windows ME 및 Windows XP로부터 암호화된 Samba 암호가 사용됩니다. Red Hat Linux 시스템과 앞서 설명된 Windows 운영 체제 간에 Samba를 사용하시려면, Windows 레지스트리 (registry)를 평문 암호를 사용하도록 편집하시거나, Linux 시스템 상의 Samba가 암호화된 암호를 사용하도록 설정하시면 됩니다. 레지스트리를 수정하기로 선택하셨다면, 모든 Windows 시스템의 레지스트리를 수정하셔야 합니다. — 하지만 이 방법을 사용하시면 더 많은 충돌을 가져올 수 있으므로 위험합니다. 보안을 강화하기 위해 암호화된 암호를 사용하시길 권장합니다.

Red Hat Linux 시스템 상의 Samba 서버가 암호화된 암호를 사용하도록 설정하시려면, 다음과 같은 단계를 따르십시오:

1. Samba에 사용될 별개의 암호 파일을 생성해 주십시오. 기존의 /etc/passwd 파일을 이용하여 새 암호 파일을 생성하기 위해서는, 쉘 프롬프트에서 다음과 같은 명령을 입력하시면 됩니다:
   cat /etc/passwd | mksmbpasswd.sh > /etc/samba/smbpasswd

   만일 시스템이 NIS를 사용한다면 다음의 명령을 입력해 주십시오:
   ypcat passwd | mksmbpasswd.sh > /etc/samba/smbpasswd

   mksmbpasswd.sh 스크립트는 samba 패키지와 함께 /usr/bin 디렉토리에 설치되어 있습니다.
2. 다음과 같은 명령을 사용하여 Samba 암호 파일의 허가를 루트 권한을 가진 사용자만 읽고 쓸 수 있도록 변경해 주십시오:
   chmod 600 /etc/samba/smbpasswd
3. 이 스크립트는 사용자 암호를 새로운 파일에 복사하지 않으며, 암호가 설정될 때까지 Samba 사용자 계정이 활성화되지 않습니다. 보안을 강화하기 위해, 사용자의 Samba 암호를 사용자의 Red Hat Linux 암호와는 다르게 설정하시기 바랍니다. 각 Samba 사용자의 암호를 설정하시려면, 다음과 같은 명령을 사용하십시오 (*username*을 각 사용자의 사용자명으로 교체하시면 됩니다):
   smbpasswd *username*
4. Samba 설정 파일에서 암호화된 암호를 활성화되어야 합니다. smb.conf 파일에서 다음과 같은 줄이 주석 처리되지 않은 것을 확인하시기 바랍니다:
   encrypt passwords = yes
   smb passwd file = /etc/samba/smbpasswd
5. 쉘 프롬프트에서 service smb restart 명령을 입력하여 smb 서비스를 시작해 주십시오.
6. smb 서비스가 자동으로 시작되도록 설정하시려면, **ntsysv**, chkconfig 또는 **서비스 설정 도구**를 사용하여 이 서비스를 런타임 시에 활성화시킵니다. 보다 자세한 정보를 원하시면 14 장을 참조하시기 바랍니다.

힌트

암호화된 암호와 관련된 보다 많은 정보를 원하신다면, /usr/share/doc/samba-<*version*>/docs/htmldocs/ENCRYPTION.html을 읽어 보시기 바랍니다. (여기서 <*version*> 부분은 여러분이 설치하신 Samba의 버전 번호입니다).

pam_smbpass PAM 모듈은 passwd 명령이 사용되었을 때 사용자의 Samba 암호와 그 사용자의 시스템 암호를 동기화하는데 사용될 수 있습니다. 만일 사용자가 passwd 명령을 사용하여 암호를 변경한다면, Red Hat Linux 시스템 로그인 암호 뿐만 아니라 Samba 공유에 접속하기 위해 사용되는 암호도 변경됩니다.

이러한 암호 동기화 기능을 사용하시려면, /etc/pam.d/system-auth 파일에서 pam_cracklib.so 호출 아래에 다음과 같은 줄을 추가하십시오:

```
password required /lib/security/pam_smbpass.so nullok use_authtok try_first_pass
```

17.2.4. 서버 시작하고 중지하기

Samba를 통해 디렉토리를 공유하는 서버 상에서 smb 서비스가 실행 중이어야 합니다.

다음 명령을 사용하여 Samba 데몬의 상태를 살펴보시기 바랍니다:

```
/sbin/service smb status
```

다음 명령을 사용하여 데몬을 시작하십시오:

```
/sbin/service smb start
```

다음 명령을 사용하여 데몬을 중지할 수 있습니다:

```
/sbin/service smb stop
```

부팅시 `smb` 서비스가 시작되도록 하시려면, 다음 명령을 사용하시기 바랍니다:

```
/sbin/chkconfig --level 345 smb on
```

또한 `chkconfig`, **ntsysv** 이나 **서비스 설정 도구**를 사용하여 부팅시 시작될 서비스를 설정할 수 있습니다. 자세한 사항은 14 장을 참조하시기 바랍니다.

17.3. Samba 공유에 접속하기

Microsoft Windows 컴퓨터로부터 Linux Samba 공유에 접속하기 위해서는, **네트워크 환경** 또는 그래픽 파일 관리자를 사용하시기 바랍니다.

Linux 시스템에서 Samba 공유에 접속하시려면, 쉘 프롬프트에서 다음과 같은 명령을 입력하시면 됩니다:

```
smbclient //hostname/sharename -U username
```

위의 명령에서 *`hostname`* 부분은 접속할 Samba 서버의 호스트명이나 IP 주소로 교체하시고, *`sharename`*은 탐색하려는 공유 디렉토리명으로 바꿔주십시오. 그리고 *`username`*은 Samba 사용자명으로 대체하십시오. 그 후 올바른 암호를 입력하시고, 만일 그 사용자에 대한 암호가 필요하지 않다면 [Enter] 키를 누르시면 됩니다.

`smb:\>` 프롬프트가 나타나면 여러분은 성공적으로 로그인하신 겁니다. 일단 로그인 하셨다면, 명령어 목록을 보기위해서 **`help`**를 입력하십시오. 여러분의 홈 디렉토리의 내용을 검색하시려면, 앞의 명령에서 *`sharename`* 부분을 여러분의 사용자명으로 바꾸십시오. 만일 `-U` 교환 옵션을 사용하지 않으신다면, 현재 사용자의 사용자명이 Samba 서버로 전달됩니다.

`smbclient`를 종료하기 위해서는 `smb:\>` 프롬프트에서 **`exit`**라고 입력하십시오.

또한 **Nautilus**를 사용하여 네트워크 상에서 사용 가능한 Samba 공유를 보실 수 있습니다. 패널에서 **주 메뉴 버튼 => 네트워크 서버**를 선택하시면 네트워크 상에 존재한 Samba 작업그룹 목록이 나타납니다. 또한 Nautilus의 **위치:** 바에서 **`smb:`**라고 입력하여 작업 그룹 목록을 보실 수 있습니다.

그림 17-6에서 보이듯이, 네트워크 상에서 사용 가능한 SMB 작업그룹마다 아이콘이 나타납니다.

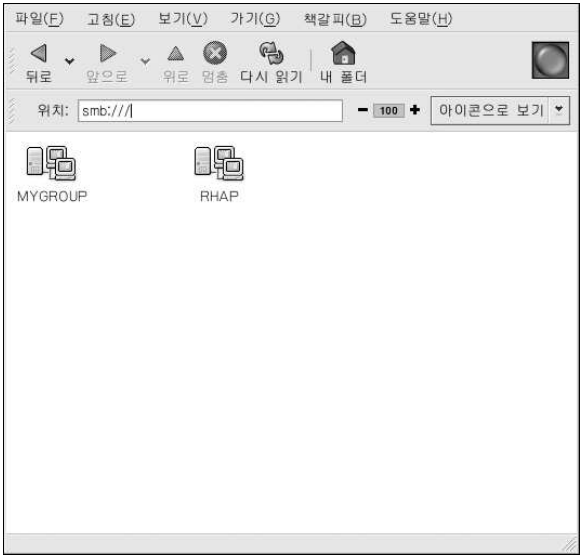

그림 17-6. Nautilus로 SMB 작업그룹 보기

작업그룹 내에서 컴퓨터 목록을 보시려면 작업그룹 아이콘에 두번 클릭하시면 됩니다.

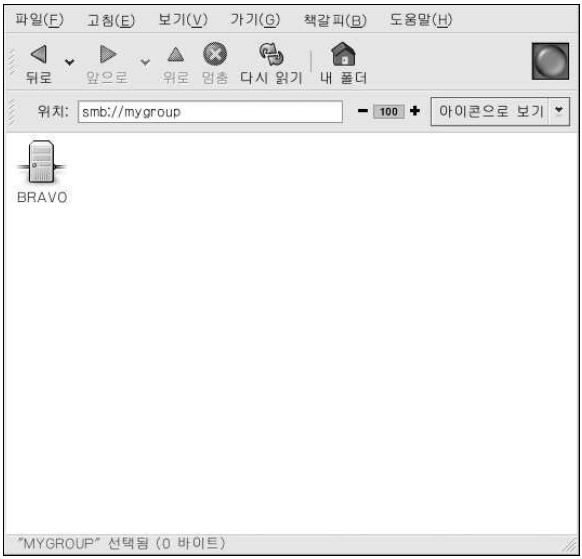

그림 17-7. Nautilus로 SMB 컴퓨터 목록 보기

그림 17-7에서 보셨듯이, 작업그룹 내의 각 컴퓨터 마다 아이콘이 나타납니다. 컴퓨터 상 Samba 공유를 보시려면 아이콘에 두번 클릭하시기 바랍니다. 사용자명과 암호를 입력해 주셔야 합니다.

다른 방법으로, 다음과 같은 명령을 사용하여 **위치:** 바에서 사용자명과 암호를 입력하실 수 있습니다. (*user*, *password*, *servername*, *sharename* 부분을 적절한 값으로 바꾸어 주십시오):

```
smb://user:password@servername/sharename/
```

17.4. 추가 자료

이 장에서 다루어지지 않은 설정 옵션들에 대해서는 다음에 나온 자료들을 참조하시기 바랍니다.

17.4.1. 설치된 문서

- `smb.conf` 메뉴얼 페이지 — Samba 설정 파일을 설정하는 방법에 대한 설명이 나와있습니다.
- `smbd` 메뉴얼 페이지 — Samba 데몬 작동 방식에 대하여 설명합니다.
- `/usr/share/doc/samba-<version-number>/docs/` — `samba` 패키지에 포함된 HTML 도움말 파일과 텍스트 도움말 파일.

17.4.2. 유용한 웹사이트

- http://www.samba.org — Samba 웹 페이지에는 유용한 문서 자료와, 메일링 리스트에 대한 정보 그리고 GUI 인터페이스의 목록이 포함되어 있습니다.

동적 호스트 설정 프로토콜 (DHCP)

동적 호스트 설정 프로토콜 (DHCP)은 클라이언트 컴퓨터에 자동으로 TCP/IP 정보를 할당해주는 네트워크 프로토콜입니다. 개별 DHCP 클라이언트가 중앙에서 관리하는 DHCP 서버에 접속되었을 때 자동으로 DHCP 서버는 IP 주소, 게이트웨이와 DNS 서버와 같은 클라이언트의 네트워크 설정을 보내줍니다.

18.1. DHCP를 사용하는 이유?

DHCP는 클라이언트 네트워크 설정을 빠르게 전달하는데 유용합니다. 클라이언트 시스템을 설정할 때, 관리자는 DHCP를 선택하면 IP 주소, 넷마스트, 게이트웨이, DNS 서버를 입력할 필요가 없습니다. 클라이언트는 이러한 정보를 DHCP 서버로부터 받습니다. 또한 시스템 관리자가 여러 많은 시스템의 IP 주소를 변경하려고 할경우에도 DHCP를 사용하는 것이 유용합니다. 모든 시스템을 재설정할 필요가 없이 단순히 서버에서 새로운 세트의 IP 주소에 사용될 한개의 DHCP 설정 파일을 편집하시면 됩니다. 만일 기업체에 사용되는 DNS 서버가 변경된다면, DHCP 클라이언트가 아닌 DHCP 서버를 변경합니다. 일단 클라이언트 상에서 네트워크를 재시작하시면 (또는 클라이언트를 재부팅하시면), 변경 사항이 적용되어 작동합니다.

만일 랩탑 또는 다른 유형의 휴대용 컴퓨터를 DHCP로 설정하셨다면, 네트워크에 연결되는 DHCP 서버를 갖춘 장소라면 어디서나 네트워크를 재설정할 필요가 없이 이동하여 사용하실 수 있습니다.

18.2. DHCP 서버 설정

`/etc/dhcpd.conf` 설정 파일을 사용하여 DHCP 서버를 설정하실 수 있습니다.

DHCP는 또한 `/var/lib/dhcp/dhcpd.leases` 파일을 사용하여 클라이언트 할당(lease) 데이터베이스를 저장합니다. 보다 많은 정보를 원하시면 18.2.2 절을 참조하시기 바랍니다.

18.2.1. 설정 파일

DHCP 서버를 설정하기 위한 첫번째 단계는 클라이언트에 대한 네트워크 정보를 저장하는 설정 파일을 생성하는 것입니다. 모든 클라이언트에 적용되는 전체 옵션을 지정하시거나 또는 개별 클라이언트 시스템에 대한 옵션을 따로 지정하실 수 있습니다.

설정 파일에는 여분의 탭이나 빈 줄을 포함되어 보다 쉽게 읽을 수 있도록 해줍니다. 키워드는 대/소문자 구별이 있으며 우물정자 표시 (#)로 시작하는 줄은 주석으로 취급됩니다.

현재 두가지 DNS 업데이트 스키마 — ad-hoc DNS 업데이트 모드와 interim DHCP-DNS 상호 작용 드래프트 업데이트 모드가 실행되고 있습니다. 이 두가지 업데이트 스키마가 IETF에서 인터넷 표준 인증을 받게된다면, 제 3의 모드 — 표준 DNS 업데이트 방식이 생겨날 것입니다. DNS 서버가 현재 사용되고 있는 두가지 DNS 업데이트 스키마 중 한가지를 사용하도록 설정해 주십시오. 0b2pl11 버전과 이전 버전은 ad-hoc 모드를 사용합니다; 하지만 이 모드는 자주 사용되지 않고 있습니다. 이 모드를 계속 사용하시려면 설정 파일의 처음 부분에 다음과 같은 줄을 추가해 주십시오:

```
ddns-update-style ad-hoc;
```

추천된 모드를 사용하시려면, 설정 파일 처음 부분에 다음과 같은 줄을 추가해 주십시오:

```
ddns-update-style interim;
```

두가지 모드에 대한 자세한 정보를 원하신다면 `dhcpd.conf` 메뉴얼 페이지를 읽어보시기 바랍니다.

설정 파일에는 다음과 같은 두가지 유형의 문장 (statememt)이 사용됩니다:

- 매개 변수 (Parameters) — 작업 수행 방식과 여부를 지정하거나 클라이언트로 보낼 네트워크 설정 옵션의 종류를 지정합니다.
- 선언 (Declarations) — 네트워크의 배열이나 구성을 개념적인 그림으로 표현하고, 클라이언트를 설명하며 클라이언트에 대한 주소를 제공하거나 선언 그룹에 매개 변수 그룹을 적용합니다.

option 키워드로 시작하는 일부 매개 변수는 옵션을 나타냅니다. 옵션은 DHCP 옵션을 설정합니다; 반면에 매개 변수는 옵션이 아닌 값을 설정하거나 DHCP 서버가 자동하는 방식을 제어합니다.

중 괄호 ({ }) 내에 포함된 부분 이전에 선언된 (옵션을 포함한) 매개 변수는 전역 매개 변수 (global parameter)로 취급됩니다. 전역 매개 변수는 자신 이하에 위치한 모든 부분에 적용됩니다.


중요

만일 설정 파일을 변경하시면, service dhcpd restart 명령을 사용하여 DHCP 데몬을 재시작하셔야 변경 사항이 효력을 발생합니다.

예 18-1을 보시면, routers, subnet-mask, domain-name, domain-name-servers, time-offset 옵션은 전역 매개 변수로서 그 옵션 아래에 선언된 모든 host 문장에 사용됩니다.

예 18-1에서 보여지듯이 여러분은 subnet을 선언하실 수 있습니다. 네트워크의 모든 서브넷에 대한 subnet 선언을 포함시켜야 합니다.

다음의 예시에서는 서브넷 내의 모든 DHCP 클라이언트에 대한 전역 옵션과 range (범위)가 지정되었습니다. 클라이언트는 range 범위 내에서 IP 주소를 할당 받습니다.

```
subnet 192.168.1.0 netmask 255.255.255.0 {
   option routers        192.168.1.254;
   option subnet-mask      255.255.255.0;

   option domain-name      "example.com";
   option domain-name-servers   192.168.1.1;

   option time-offset      -18000;  # Eastern Standard Time

 range 192.168.1.10 192.168.1.100;
}
```

예 18-1. subnet 선언

동일한 물리적 네트워크를 공유하는 모든 서브넷은 예 18-2에서 보여지듯이 공유-네트워크 선언 (shared-network declaration)에서 선언되어야 합니다. shared-network에 포함되지만 괄호로 묶인 subnet의 밖에 위치한 매개 변수는 전역 매개 변수로 취급됩니다. shared-network의 이름은 네트워크의 용도를 설명할 수 있는 이름을 사용하셔야 합니다. 예로 들면 테스트 랩 (test lab) 환경의 모든 서브넷을 설명하는 test-lab과 같은 이름을 사용하실 수 있습니다.

```
shared-network name {
  option domain-name      "test.redhat.com";
  option domain-name-servers   ns1.redhat.com, ns2.redhat.com;
  option routers        192.168.1.254;
  more parameters for EXAMPLE shared-network
  subnet 192.168.1.0 netmask 255.255.255.0 {
    parameters for subnet
    range 192.168.1.1 192.168.1.31;
  }
  subnet 192.168.1.32 netmask 255.255.255.0 {
```

```
    parameters for subnet
    range 192.168.1.33 192.168.1.63;
  }
}
```

예 18-2. share-network (공유-네트워크) 선언

예 18-3에서 보여지듯이 선언 그룹에 전역 매개 변수를 적용하기 위하여 group 선언을 사용하실 수 있습니다. 공유 네트워크, 서브넷, 호스트나 다른 그룹들을 하나의 그룹으로 모을 수 있습니다.

```
group {
  option routers        192.168.1.254;
  option subnet-mask      255.255.255.0;

  option domain-name      "example.com";
  option domain-name-servers    192.168.1.1;

  option time-offset      -18000;   # Eastern Standard Time

  host apex {
    option host-name "apex.example.com";
    hardware ethernet 00:A0:78:8E:9E:AA;
    fixed-address 192.168.1.4;
  }

  host raleigh {
    option host-name "raleigh.example.com";
    hardware ethernet 00:A1:DD:74:C3:F2;
    fixed-address 192.168.1.6;
  }
}
```

예 18-3. group 선언

서브넷 내의 시스템에 동적 IP 주소를 할당해주는 DHCP 서버를 설정하시려면 예 18-4을 여러분의 시스템에 맞는 값으로 바꾸어 사용해 주십시오. 위의 예시는 클라이언트에 대한 기본 할당 시간 (default lease time), 최대 할당 시간 (maximum lease time)과 네트워크 설정 값을 선언합니다. 아래 예시에서는 192.168.1.10 에서 192.168.1.100 범위 (range) 사이의 IP 주소를 클라이언트 시스템에 할당합니다.

```
default-lease-time 600;
max-lease-time 7200;
option subnet-mask 255.255.255.0;
option broadcast-address 192.168.1.255;
option routers 192.168.1.254;
option domain-name-servers 192.168.1.1, 192.168.1.2;
option domain-name "example.com";

subnet 192.168.1.0 netmask 255.255.255.0 {
  range 192.168.1.10 192.168.1.100;
}
```

예 18-4. Range 매개 변수

네트워크 인터페이스 카드의 MAC 주소에 기반한 클라이언트에게 IP 주소를 할당하기 위해서는, host 선언 내에서 hardware ethernet 매개 변수를 사용하셔야 합니다. 예 18-5에서 보여지듯이 host apex 선언은 MAC 주소 00:A0:78:8E:9E:AA를 가진 네트워크 인터페이스 카드에는 언제나 IP 주소 192.168.1.4 를 할당하도록 지정하고 있습니다.

클라이언트에 호스트명을 할당하기 위하여 옵션 매개 변수인 host-name도 사용 가능하다는 점을 기억해 주십시오.

```
host apex {
  option host-name "apex.example.com";
  hardware ethernet 00:A0:78:8E:9E:AA;
  fixed-address 192.168.1.4;
}
```

예 18-5. DHCP를 사용하는 정적 IP 주소

힌트

처음에는 Red Hat Linux 9의 샘플 설정 파일을 사용하신 후 나중에 그 샘플 설정 파일에 여러분이 스스로 사용자 설정하신 옵션을 추가하실 수 있습니다. 다음 명령을 사용하여 사용자 설정하신 옵션을 파일의 적절한 위치로 복사합니다.

```
cp /usr/share/doc/dhcp-<version-number>/dhcpd.conf.sample /etc/dhcpd.conf
```

(여기서 <version-number>는 여러분이 사용하시는 DHCP 버전을 의미합니다)

전체 옵션 구문과 기능에 대한 목록을 보시려면, dhcp-options 메뉴얼 페이지를 참조하시기 바랍니다.

18.2.2. 할당 (Lease) 데이터베이스

DHCP 서버에서 /var/lib/dhcp/dhcpd.leases 파일은 DHCP 클라이언트 할당 데이터베이스를 저장하고 있습니다. 이 파일을 직접 수정하시면 안됩니다. 최근에 할당된 개별 IP 주소에 대한 DHCP 할당 정보는 자동적으로 할당 데이터베이스에 저장됩니다. 이 정보에는 할당 기간, IP 주소가 부여된 클라이언트, 할당이 시작되고 끝나는 날짜 그리고 할당받기 위하여 사용된 네트워크 인터페이스 카드의 MAC 주소가 포함되어 있습니다.

할당 데이터베이스에서 사용된 시간은 모두 그리니치 표준시 (GMT)이며, 지역 시간은 사용되지 않습니다.

할당 데이터베이스는 크기가 너무 커지지 않도록 계속적으로 재생성됩니다. 우선, 모든 알려진 할당 정보를 임시 할당 데이터베이스에 저장한 후 dhcpd.leases 파일을 dhcpd.leases~로 이름을 변경하고 임시 할당 데이터베이스를 dhcpd.leases 파일에 기록합니다.

할당 데이터베이스를 백업 파일로 이름 변경 후 새로운 파일이 기록되기 전에 DHCP 데몬이 죽거나 시스템이 파손되는 경우가 발생할 수 있습니다. 이러한 경우에는 서비스를 시작하는데 필요한 dhcpd.leases 파일이 존재하지 않습니다. 만일 이러한 상황이 발생하면 새로운 할당 파일을 생성하지 마십시오. 새로운 할당 파일을 생성하시면 이전 할당 정보가 삭제되어 많은 문제가 발생합니다. dhcpd.leases~ 백업 파일을 dhcpd.leases로 이름을 변경한 후 데몬을 시작하시는 것이 올바른 해결책입니다.

18.2.3. 서버 시작과 중지

중요

dhcpd.leases 파일이 없이 DHCP 서버를 처음 시작하신다면, 서버가 실패할 것입니다. 만일 이 파일이 없다면 touch /var/lib/dhcp/dhcpd.leases 명령을 사용하여 파일을 생성하시기 바랍니다.

`/sbin/service dhcpd start` 명령을 사용하여 DHCP 장치를 시작하십시오. DHCP 서버를 멈추시려면 `/sbin/service dhcpd stop` 명령을 사용합니다. 시스템 부팅 시 데몬이 자동으로 시작되도록 설정하시려면, 서비스를 관리하는 방법에 대한 정보를 14 장에서 참조하시기 바랍니다.

시스템 상에 한 개 이상의 네트워크 인터페이스가 연결되어 있는 경우, 오직 한 인터페이스 상에서만 DHCP 서버가 시작하도록 설정하는 것이 가능합니다. `/etc/sysconfig/dhcpd` 파일에서 해당 인터페이스의 이름을 `DHCPDARGS` 목록에 추가하십시오:

```
# Command line options here
DHCPDARGS=eth0
```

두개의 네트워크 카드를 가진 방화벽 컴퓨터를 가지고 계신 경우 특히 이 옵션이 유용합니다. 한개의 네트워크 카드는 인터넷 IP 주소를 검색하도록 DHCP 클라이언트로 설정 가능하며 다른 네트워크 카드는 방화벽 뒤에서 내부 네트워크 용 DHCP 서버로 사용하실 수 있습니다. 내부 네트워크에 연결된 네트워크 카드만을 지정함으로서 다른 사용자가 인터넷을 통하여 데몬에 접속하지 못하게 되므로 시스템 보안이 더욱 강화됩니다.

`/etc/sysconfig/dhcpd` 파일에서 다음과 같은 다른 명령 행 옵션도 지정 가능합니다:

- `-p <portnum>` — dhcpd가 청취할 udp 포트 번호를 지정합니다. 기본 포트는 67 입니다. DHCP 서버는 지정된 udp 포트보다 하나 더 많은 포트에서 DHCP 클라이언트에게 응답을 전송합니다. 예를 들어, 여러분이 기본 포트 67을 수락한 경우, 서버는 포트 67에서 요청을 청취하고 포트 68에서 클라이언트에게 응답을 전송합니다. 만일 포트를 지정하신 후 DHCP 릴레이 에이전트(relay agent)를 사용하신다면, DHCP 릴레이 에이전트가 청취할 포트와 동일한 포트를 지정하셔야 합니다. 보다 자세한 정보를 원하시면 18.2.4 절을 참조하시기 바랍니다.
- `-f` — 데몬에 우선 순위를 주어 바로 실행합니다. 이 옵션은 주로 디버깅 목적으로 사용됩니다.
- `-d` — DHCP 서버 데몬을 표준 오류 기술어로 기록합니다. 이 옵션은 주로 디버깅 용으로 사용됩니다. 만일 이 옵션이 지정되지 않는다면, 로그는 `/var/log/messages`에 기록됩니다.
- `-cf filename` — 설정 파일의 위치를 지정합니다. 디폴트 위치는 `/etc/dhcpd.conf` 입니다.
- `-lf filename` — 할당 데이터베이스 파일의 위치를 지정합니다. 만일 할당 데이터베이스 파일이 이미 존재한다면, DHCP 서버가 시작될 때마다 반드시 동일한 파일이 사용되어야 합니다. 이 옵션은 비생산용 시스템에서 디버깅 목적으로만 사용하시기를 적극 권장합니다. 디폴트 위치는 `/var/lib/dhcp/dhcpd.leases` 입니다.
- `-q` — 데몬을 시작할 때 전체 저작권 메시지를 출력하지 않습니다.

18.2.4. DHCP 릴레이 에이전트 (Relay Agent)

DHCP 릴레이 에이전트 (`dhcrelay`)는 DHCP 서버가 없는 서브넷으로부터 다른 서브넷의 한 개 이상의 DCHP 서버로 DHCP와 BOOTP 요청을 중계 (relay)해줍니다.

DHCP 클라이언트가 정보를 요청하는 경우, DHCP 릴레이 에이전트는 그 요청을 DHCP 릴레이 에이전트가 시작될 때 지정된 DHCP 서버 목록으로 전송합니다. DHCP 서버가 응답을 보내오면, 원래 요청을 보낸 네트워크 상에서 그 응답을 브로드캐스트 (broadcast)하거나 유니캐스트 (unicast)합니다.

DHCP 릴레이 에이전트는 모든 인터페이스에서 DHCP 요청을 청취하지만 `/etc/sysconfig/dhcrelay` 파일에서 `INTERFACES` 지시문을 사용하여 인터페이스가 지정된 경우에는, 그 지정된 인터페이스만 청취합니다.

DHCP 릴레이 에이전트를 시작하시려면, `service dhcrelay start` 명령을 사용하십시오.

18.3. DHCP 클라이언트 설정

DHCP 클라이언트를 설정하기 위한 첫번째 단계는 커널이 네트워크 인터페이스 카드를 인식하는지를 확인하는 것입니다. 설치 과정에서 대부분의 카드가 인식되며, 시스템은 그 카드에 맞는 커널 모듈을 사용하도록

설정되어 있습니다. 만일 설치를 마치신 후에 카드를 설치하신다면, **Kudzu**[1]가 카드를 인식하여, 여러분이 설치하신 카드에 맞는 커널 모듈을 설정하도록 요청할 것입니다. http://hardware.redhat.com/hcl/에서 Red Hat Linux 하드웨어 호환성 목록을 확인해 보십시오. 만일 설치 프로그램이나 **Kudzu**가 올바른 네트워크 카드를 설정하지 못한 경우, 여러분이 로드할 커널 모듈의 종류를 알고 계시다면, 직접 커널 모듈을 로딩하시기 바랍니다. 커널 모듈을 로딩하는 방법에 대한 자세한 정보를 원하신다면, 31 장을 참조해 주십시오.

DHCP 클라이언트를 수동으로 설정하시려면 `/etc/sysconfig/network-scripts` 디렉토리에 존재하는 개별 네트워크 장치에 대한 네트워킹과 설정 파일을 활성화하도록 `/etc/sysconfig/network` 파일을 수정하셔야 합니다. 이 디렉토리에 있는 각 장치는 `ifcfg-eth0` (여기서 `eth0`는 네트워크 장치명을 의미) 설정 파일을 가지고 있습니다.

`/etc/sysconfig/network` 파일에는 다음과 같은 줄이 포함되어야 합니다:

```
NETWORKING=yes
```

이 파일에는 더 많은 정보가 포함되어 있지만, 부팅 시 네트워킹을 시작하기 위해서는 반드시 `NETWORKING` 변수를 `yes`로 설정하셔야 합니다.

`/etc/sysconfig/network-scripts/ifcfg-eth0` 파일에는 다음과 같은 라인이 포함되어야 합니다:

```
DEVICE=eth0
BOOTPROTO=dhcp
ONBOOT=yes
```

DHCP를 사용하도록 설정할 개별 장치마다 설정 파일이 필요합니다.

그래픽 인터페이스를 사용하여 DHCP 클라이언트를 설정하시려면, 12 장에서 **네트워크 관리 도구**을 사용하여 네트워크 인터페이스가 DHCP를 사용하도록 설정하는 방법에 대한 자세한 정보를 읽어 보시기 바랍니다.

18.4. 추가 자료

이 장에서 다루지 않은 설정 옵션에 대한 자료를 원하신다면, 다음과 같은 자료를 참조하시기 바랍니다.

18.4.1. 설치된 문서 자료

- `dhcpd` 메뉴얼 페이지 — DHCP 데몬 작동 방식에 대한 설명.
- `dhcpd.conf` 메뉴얼 페이지 — DHCP 설정 파일을 설정하는 방식에 대한 설명; 일부 예시 포함.
- `dhcpd.leases` 메뉴얼 페이지 — DHCP 할당 파일을 설정하는 방식에 대한 설명; 일부 예시 포함.
- `dhcp-options` 메뉴얼 페이지 — `dhcpd.conf`에서 DHCP 옵션을 선언하는 구문에 대한 설명; 일부 예시 포함.
- `dhcrelay` 메뉴얼 페이지 — DHCP 릴레이 에이전트와 설정 옵션에 대한 설명.

1. **Kudzu**는 시스템 부팅 시에 실행되어 어떤 하드웨어가 추가되고 제거되었는지를 알아내는 하드웨어 검색 도구입니다.

19장 .

Apache HTTP 서버 설정

Red Hat Linux 8.0에서, Apache HTTP 서버는 다른 설정 옵션을 사용하는 2.0 버전으로 업데이트 되었습니다. 또한 Red Hat Linux 8.0에서부터, RPM 패키지의 이름이 `httpd`로 변경되었습니다. 여러분이 직접 기존 설정 파일을 업데이트하시려면, `/usr/share/doc/httpd-<ver>/migration.html`에서 설명서를 참조해 보시거나 *Red Hat Linux* 참조 가이드에서 자세한 사항을 참조하시기 바랍니다.

Red Hat Linux 이전 버전에서 **HTTP 설정 도구**를 사용하여 Apache HTTP 서버를 설정하신 후 업그레이드를 수행하신 경우, 이 도구를 사용하여 기존 설정 파일을 2.0 버전에 맞는 새로운 포맷으로 번환하실 수 있습니다. **HTTP 설정 도구**를 시작하여 필요한 설정을 변경하신 후 저장하십시오. 저장된 설정 파일은 2.0 버전과 호환 가능하도록 저장됩니다.

HTTP 설정 도구는 Apache HTTP 서버에 사용되는 `/etc/httpd/conf/httpd.conf` 설정 파일을 설정할 수 있게 도와주는 프로그램 입니다. 이전에 사용되던 `srm.conf` 설정 파일이나 `access.conf` 설정 파일은 사용되지 않습니다. 여러분은 그래픽 인터페이스를 통하여 가상 호스트, 기록 속성 및 최대 접속수와 같은 지시자 (directive)를 설정하실 수 있습니다.

HTTP 설정 도구는 Red Hat Linux와 함께 배포된 모듈만 설정할 수 있습니다. 만일 추가 모듈이 설치된 경우, 이러한 추가 모듈은 이 도구를 사용하여 설정하실 수 없습니다.

HTTP 설정 도구를 사용하시려면, `httpd`와 `redhat-config-httpd` RPM 패키지를 설치하셔야 합니다. X 윈도우 시스템과 루트 권한도 가지고 계셔야 합니다. 이 응용 프로그램을 시작하시려면, **주 메뉴 버튼** => **시스템 설정** => **서버 설정** => **HTTP 서버**를 선택하시거나 쉘 프롬프트 (예, XTerm이나 GNOME 터미널)에서 `redhat-config-httpd` 명령을 입력하시면 됩니다.

경고

이 도구를 사용하실 계획이라면 `/etc/httpd/conf/httpd.conf` 설정 파일을 직접 편집하지 마십시오. 여러분이 변경 사항을 저장하신 후 프로그램을 종료하시면 **HTTP 설정 도구**는 이 파일을 새로 생성합니다. **HTTP 설정 도구**에는 없는 추가 모듈이나 설정 옵션을 추가하시려면, 이 도구를 사용하실 수 없습니다.

HTTP 설정 도구를 사용하여 Apache HTTP 서버를 설정하는 방법은 다음과 같습니다:

1. **주** 탭에서 기본 설정을 설정해 주십시오.
2. **가상 호스트들** 탭을 클릭하신 후 기본 설정을 설정하십시오.
3. **가상 호스트들** 탭에서 기본 가상 호스트를 설정하십시오.
4. 한개 이상의 URL이나 가상 호스트에 서비스를 제공하시려면, 추가 가상 콘솔을 추가하셔야 합니다.
5. **서버** 탭에서 서버를 설정하십시오.
6. **성능 조정** 탭에서 연결을 설정합니다.
7. 모든 필수 파일들을 `DocumentRoot`와 `cgi-bin` 디렉토리로 복사하시기 바랍니다.
8. 응용 프로그램을 종료하시고 설정을 저장하도록 선택하십시오.

19.1. 기본 설정

주 탭에서 기본 서버 셋팅을 설정합니다.

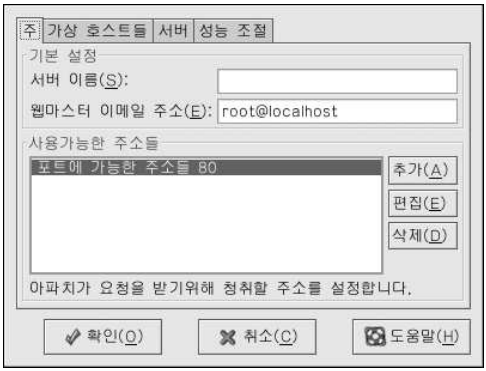

그림 19-1. 기본 설정

서버 이름 입력란에 여러분이 사용 권한을 가진 완전한 도메인명 (fully qualified domain name)을 입력해 주십시오. 이 옵션은 `httpd.conf` 파일에서 `ServerName` 지시자에 상응합니다. `ServerName` 지시자는 웹 서버의 호스트명을 설정하며 방향 변경 (redirection) URL을 생성하는데 사용됩니다. 서버 이름을 지정하지 않으시면, 웹 서버는 시스템 IP 주소에서 서버명을 알아내기 시도합니다. 서버명은 반드시 서버의 IP 주소에서 찾아낸 도메인 이름일 필요는 없습니다. 예를 들어, 서버의 실제 DNS 이름이 foo.example.com일 경우에도, 여러분은 서버명을 www.example.com으로 설정하실 수 있습니다.

웹 서버 관리자의 이메일 주소를 **웹마스터 이메일 주소**란에 입력해 주십시오. 이 옵션은 `httpd.conf` 파일의 `ServerAdmin` 지시자에 해당합니다. 서버의 오류 페이지에 이메일 주소를 올려놓으시면, 사용자들이 서버 관리자에게 문제를 보고하기 위해 이메일을 보낼 때 이 이메일 주소를 사용할 수 있습니다. 디폴트 값은 root@localhost 입니다.

사용가능한 주소들 영역에 서버가 들어오는 요청을 수용할 포트를 지정해 주십시오. 이 옵션은 `httpd.conf` 파일에서 `Listen` 지시자에 상응합니다. 디폴트 값으로, Red Hat은 Apache HTTP 서버가 포트 80에서 비보안 웹 통신을 청취하도록 설정합니다.

요청을 수용할 추가 포트를 정의하시려면 **추가** 버튼을 클릭하십시오. 그림 19-2과 유사한 창이 나타날 것입니다. 정의된 포트 상에서 모든 IP 주소를 청취하기 위해서 **모든 주소를 청취** 옵션을 선택하시거나, 또는 **주소** 입력란에 서버가 연결을 받아들일 특정 IP 주소를 지정하시기 바랍니다. 한 포트 번호 당 한 개의 IP 주소만 지정하십시오. 만일 동일한 포트 번호에 한 개 이상의 IP 주소를 지정하시려면, 각 IP 주소에 대한 항목을 생성하셔야 합니다. 만일 가능하다면 DNS 검색 실패를 방지하기 위해 도메인명 대신 IP 주소를 사용하시기 바랍니다. *DNS*와 *Apache* 관련 문제점에 대한 보다 많은 정보를 원하신다면, http://httpd.apache.org/docs-2.0/dns-caveats.html을 참조하시기 바랍니다.

주소란에 별표 (*) 입력하시면 **모든 주소를 청취** 옵션을 선택하는 것과 마찬가지입니다. **편집** 버튼을 클릭하시면 **추가** 버튼을 클릭했을 때와 동일한 창이 나타나지만 한가지 차이점은 선택하신 항목에 대한 영역들이 채워져 있다는 것입니다. 항목을 삭제하기 위해서는, 해당 항목을 선택하신 후 **삭제** 버튼을 클릭하시면 됩니다.

힌트

서버를 1024 이하의 포트를 청취하도록 설정하셨다면, 루트로 로그인하신 후 시작하셔야 합니다. 1024 이상의 포트를 청취하는 `httpd` 명령은 일반 사용자도 시작 가능합니다.

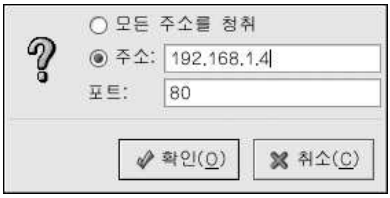

그림 19-2. 사용 가능한 주소

19.2. 기본 설정

서버명, **웹마스터 이메일 주소**와 **사용가능한 주소들**을 정의하신 후 **가상 호스트들** 탭을 클릭하시고 **기본 설정 편집** 버튼을 클릭해 주십시오. 그림 19-3에서 보여지는 창이 나타날 것이며, 이 창에서 여러분의 웹 서버에 대한 기본 셋팅을 설정하실 수 있습니다. 가상 호스트를 추가하시면, 새로 추가된 가상 호스트가 기존 가상 호스트에 대하여 우선권을 갖습니다. 가상 호스트 설정에 지시자를 정의하지 않으시면, 디폴트 값이 사용됩니다.

19.2.1. 사이트 설정

디렉토리 페이지 탐색 목록과 **오류 페이지들**에 설정된 디폴트 값을 사용하시면 대부분의 서버에서 작동합니다. 이 설정값에 대하여 잘 모르시겠다면, 설정을 수정하지 마십시오.

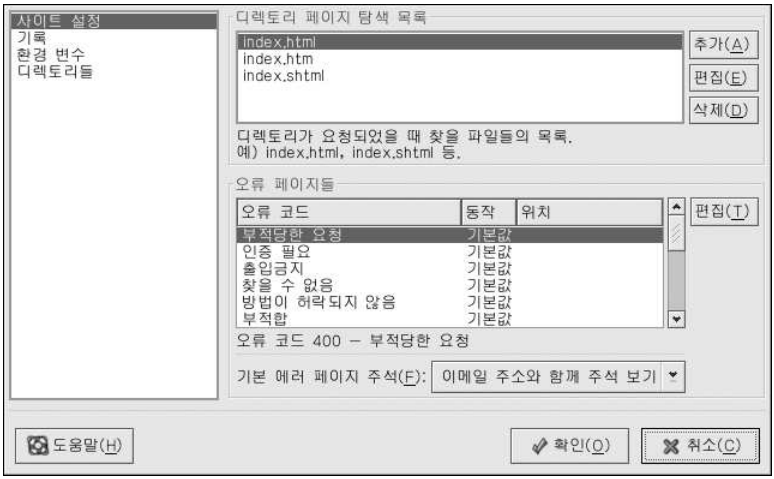

그림 19-3. 사이트 설정

디렉토리 페이지 탐색 목록에 포함된 항목들은 `DirectoryIndex` 지시자를 정의합니다. `DirectoryIndex`는 사용자가 디렉토리명 마지막에 슬래쉬 (/)를 지정하여 디렉토리의 인덱스를 요청할 때 서버가 보여주는 디폴트 페이지입니다.

예를 들어, 사용자가 http://*`www.example.com`*/*`this_directory`*/ 페이지를 요청한 경우 `DirectoryIndex` 페이지가 존재한다면 이 페이지가 나타날 것이며, 그렇지 않다면 서버가 생성한 디렉토리 목록이 나타날 것입니다. 서버는 `DirectoryIndex` 지시자 목록에 포함된 파일 중 가장 먼저 발견된 파일을 보여줍

니다. 만일 서버가 아무런 파일도 찾지 못한 경우 해당 디렉토리에 `Options Indexes`가 설정되어 있다면, 서버는 해당 디렉토리에 포함된 하부 디렉토리와 파일 목록을 HTML 형식으로 생성하여 보여줄 것입니다.

오류 코드 항목에서는 문자나 오류가 발생할 경우 클라이언트를 내부 URL이나 외부 URL로 방향 전환하도록 Apache HTTP 서버를 설정하실 수 있습니다. 이 옵션은 `ErrorDocument` 지시자에 상응합니다. 클라이언트가 Apache HTTP 서버에 접속을 시도하는 과정에서 문제나 오류가 발생한 경우, **오류 코드** 란에 포함된 짧은 오류 메시지가 나타나도록 기본 설정되어 있습니다. 이러한 기본 설정을 변경하시려면, 오류 코드를 선택하신 후 **편집** 버튼을 클릭해 주십시오. 짧은 기본 오류 메시지를 보시려면 **기본** 항목을 선택하시기 바랍니다. 클라이언트를 외부 URL로 방향 전환시키려면 **URL** 항목을 선택하신 후 **위치** 입력란에 http://를 포함한 완전한 URL을 입력해 주십시오. 내부 URL로 클라이언트를 방향 전환시키기 위해서는 **파일** 항목을 선택하신 후 웹 서버에 사용되는 문서 루트 아래에 파일 위치를 입력하시면 됩니다. 위치란은 반드시 슬래시 (/)로 시작되어야 하며 문서 루트 (Document Root)에 따라서 구성됩니다.

예를 들어, 404 Not Found 오류 코드를 여러분이 `404.html`라는 파일에 작성한 웹 페이지로 방향 전환하기 위해서는, `404.html` 파일을 *`DocumentRoot`*`/errors/404.html`으로 복사하셔야 합니다. 이 경우에 *`DocumentRoot`*는 여러분이 정의하신 문서 루트 디렉토리를 의미합니다 (디폴트는 `/var/www/html` 입니다). 그 후 **404 - 찾을 수 없음** 오류 코드에 대한 동작 란에서 **파일**을 선택하시고 **위치** 입력란에 `/errors/404.html`를 입력하시면 됩니다.

기본 에러 페이지 주석 메뉴에서 선택 가능한 옵션은 다음과 같습니다:

- **이메일 주소와 함께 주석 보기** — 모든 오류 페이지 아래쪽에 `ServerAdmin` 지시자에 의해 지정된 웹사이트 관리자의 이메일 주소와 함께 기본 주석을 보여줍니다.
- **주석 보기** — 오류 페이지 아래쪽에 기본 주석만 보여줍니다.
- **주석 없음** — 오류 페이지 아래쪽에 주석을 보여주지 않습니다.

19.2.2. 로그 기록

서버는 디폴트 설정에 따라서 `/var/log/httpd/access_log` 파일에 전송 로그를 기록하며 `/var/log/httpd/error_log` 파일에 오류 로그를 기록합니다.

전송 로그는 웹 서버로의 모든 접속 시도를 기록합니다. 서버로 연결을 시도한 클라이언트의 IP 주소와 시도한 날짜와 시간 및 접속하려는 파일에 대한 정보가 포함됩니다. 이러한 정보를 저장할 경로명과 파일명을 입력해 주십시오. 만일 경로명과 파일명이 슬래시 (/)로 시작하지 않으면, 설정된 서버 루트 디렉토리에 연계된 경로를 의미합니다. 이 옵션은 `TransferLog` 지시자에 해당합니다.

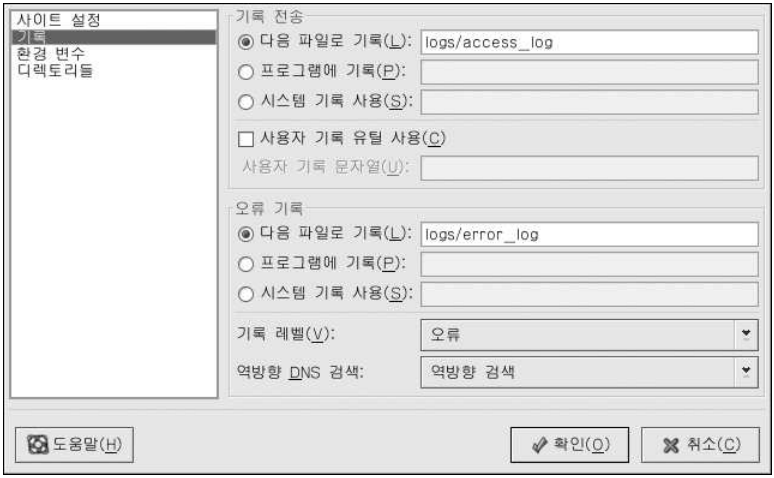

그림 19-4. 로그 기록

사용자 기록 유틸리티 사용을 체크하신 후 **사용자 정의 기록 문자열** 입력란에 사용자 정의한 기록 문자열을 입력하여 사용자 정의 기록 형식을 설정하실 수 있습니다. 이 옵션은 `LogFormat` 지시자를 설정합니다. 이 지시자의 형식에 대한 보다 자세한 정보를 원하신다면, http://httpd.apache.org/docs-2.0/mod/mod_log_config.html#formats를 참조하시기 바랍니다.

오류 로그는 서버에서 발생한 오류를 모두 기록합니다. 이러한 정보를 저장할 경로명과 파일명을 입력해 주십시오. 만일 경로명과 파일명이 슬래시 (/)로 시작하지 않으면, 설정된 서버 루트 디렉토리에 연계된 경로를 의미합니다. 이 옵션은 `ErrorLog` 지시자에 해당합니다.

로그 레벨 메뉴를 사용하여 오류 로그에서 오류 메시지가 얼마나 상세하게 기록될 것인지 설정하실 수 있습니다. 오류 메시지는 (가장 간단한 수준에서 가장 자세한 순서로) 응급 (alert), 경고 (alert), 위험 (crit), 오류 (error), 주의 (warn), 경고 (warn), 통보 (notice), 정보 (info)와 디버그 (debug) 수준으로 설정될 수 있습니다. 이 옵션은 `LogLevel` 지시자에 해당합니다.

역방향 DNS 검색 메뉴에서 선택된 값은 `HostnameLookups` 지시자를 정의합니다. **역방향 검색을 하지 않음**을 선택하시면 값이 꺼짐 (off)으로 설정되며, **역방향 검색**을 선택하시면 값이 켜짐 (on)으로 설정됩니다. **이중 역방향 검색**을 선택하시면 값이 이중으로 설정됩니다.

만일 **역방향 검색**을 선택하시면, 서버는 웹 서버로부터 문서를 요청하는 개별 연결에 대한 IP 주소를 자동으로 변환할 것입니다. IP 주소를 변환하는 것은 서버가 특정 IP 주소에 상응하는 호스트명을 찾기 위하여 DNS에 한 번이나 그 이상으로 연결한다는 것을 의미합니다.

이중 역방향 검색이 선택된 경우, 서버는 이중-역방향 DNS를 수행할 것입니다. 즉, 역방향 검색을 수행 후 나온 결과에 정방향 검색을 다시 수행한다는 의미입니다. 정방향 검색에서 나온 IP 주소와 먼저 이루어진 역방향 검색에서 나온 주소는 최소한 한개라도 일치해야만 합니다.

일반적으로 이 옵션은 **역방향 검색을 하지 않음**으로 설정해 두셔야 합니다. 그 이유는 DNS 요청이 서버에 부하를 가중시켜 서버가 느려지게 하기 때문입니다. 만일 서버가 바쁠 때 이러한 역방향 검색이나 이중 역방향 검색을 수행하게 되면 속도가 현저하게 줄어들 것입니다.

역방향 검색과 이중 역방향 검색은 또한 인터넷 전체에도 문제가 될 수 있습니다. 각각의 호스트명을 검색하기 위하여 생성된 개별 연결들이 모두 더해지기 때문에 인터넷 뿐만 아니라 웹 서버를 위해서도 이 옵션은 **역방향 검색을 하지 않음**으로 설정하셔야 합니다.

19.2.3. 환경 변수

가끔식 CGI 스크립트나 SSI (server-side include) 페이지에 사용되는 환경 변수를 수정해야할 경우가 있습니다. Apache HTTP 서버는 `mod_env` 모듈을 사용하여 CGI 스크립트와 SSI 페이지에 전달될 환경 변수를 설정합니다. **환경 변수** 페이지에서 이 모듈에 사용될 지시자를 설정하시기 바랍니다.

그림 19-5. 환경 변수

CGI 스크립트 설정 입력란에는 CGI 스크립트와 SSI 페이지에 전달될 환경 변수를 설정해 주십시오. 환경 변수 `MAXNUM`을 `50`으로 설정하시려면, 그림 19-5에서 보이듯이 **CGI 스크립트 설정** 항목 옆에 위치한 **추가** 버튼을 클릭하신 후, **환경 변수**에 **`MAXNUM`**이라고 입력하시고 **설정할 값** 입력란에 **`50`**을 입력하시기 바랍니다. 입력하신 값을 목록에 추가하도록 **확인** 버튼을 클릭해 주십시오. **CGI 스크립트 설정** 섹션은 `SetEnv` 지시자를 설정합니다.

CGI 스크립트에 전달 섹션에서는 서버가 처음 시작되었을 때 CGI 스크립트에 전달하는 환경 변수의 값을 설정해 주십시오. 이 환경 변수를 보시려면 쉘 프롬프트에서 `env` 명령을 입력하시면 됩니다. **CGI 스크립트에 전달** 섹션 옆에 위치한 **추가** 버튼을 클릭하신 후 환경 변수 입력란에 환경 변수의 이름을 입력하시고 **확인** 버튼을 클릭하시기 바랍니다. **CGI 스크립트에 전달** 섹션은 `PassEnv` 지시자를 설정합니다.

CGI 스크립트와 SSI 페이지에 아무런 값도 전달되지 않도록 환경 변수를 삭제하시려면, **CGI 스크립트 해제** 섹션을 사용하십시오. **CGI 스크립트 해제** 섹션에서 **추가** 버튼을 클릭하신 후 설정 해제할 환경 변수의 이름을 입력해 주십시오. 이 옵션은 `UnsetEnv` 지시자를 설정합니다.

이 환경 변수를 편집하시려면, 목록에서 편집할 변수를 선택하신 후 상응하는 **편집** 버튼을 클릭하시면 됩니다. 목록에서 변수를 삭제하시려면, 상응하는 **삭제** 버튼을 클릭하시기 바랍니다.

Apache HTTP 서버에서 사용하는 환경 변수에 대한 보다 많은 정보를 원하신다면, 다음 사이트를 참조하시기 바랍니다:

`http://httpd.apache.org/docs-2.0/env.html`

19.2.4. 디렉토리들

디렉토리들 페이지에서는 특정 디렉토리에 사용될 옵션을 설정하실 수 있습니다. 이 옵션은 `<Directory>` 지시자를 설정합니다.

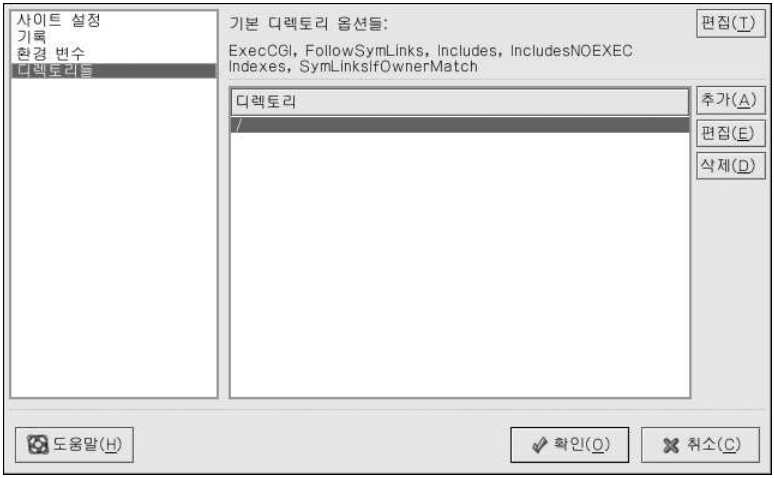

그림 19-6. 디렉토리들

오른쪽 상단 모서리에 위치한 **편집** 버튼을 클릭하여 아래쪽의 **디렉토리** 목록에 지정되지 않은 모든 디렉토리에 대한 **기본 디렉토리 옵션**들을 편집하실 수 있습니다. 여러분이 선택할 수 있는 옵션들은 `<Directory>` 지시자 내의 Options 지시자 목록에서 찾으실 수 있습니다. 설정 가능한 옵션은 다음과 같습니다:

- **ExecCGI** — CGI 스크립트의 실행 허가. 만일 이 옵션이 선택되지 않으면 CGI 스크립트는 실행되지 않습니다.
- **FollowSymLinks** — 심볼릭 링크 허가.
- **Includes** — SSI (server-side include) 허가.
- **IncludesNOEXEC** — SSI (server-side include)를 허가하지만, CGI 스크립트에서 `#exec` 와 `#include` 명령은 비활성화.
- **Indexes** — `index.html`와 같은 `DirectoryIndex` 가 요청된 디렉토리에 존재하지 않는 경우 디렉토리 내용의 포맷된 목록을 표시.
- **Multiview** — content-negotiated multiviews 지원; 이 옵션은 디폴트로 비활성화되어 있습니다.
- **SymLinksIfOwnerMatch** — 만일 목표 파일 (target file)이나 디렉토리가 링크로 동일한 소유자를 가진 경우에만 심볼릭 링크를 따름.

특정 디렉토리에 대한 옵션을 지정하기 위해서는 **디렉토리** 목록 상자 옆에 위치한 **추가** 버튼을 클릭해 주십시오. 그림 19-7에서 보이는 창이 나타날 것입니다. 창 아래쪽에 위치한 **디렉토리** 입력란에 설정할 디렉토리를 입력합니다. 오른쪽 목록에서 옵션을 선택하신 후 왼쪽에 있는 옵션을 사용하여 `Order` 지시자를 설정합니다. `Order` 지시자는 허가 목록과 거부 목록을 처리하는 순서를 지정해 줍니다. **허가 목록**과 **거부 목록** 입력란에서 다음과 같은 옵션 중 한가지를 지정하실 수 있습니다:

- 모든 호스트 허가 — 모든 호스트로의 접근을 허가하기 위해서는 **`all`**을 입력합니다.
- 부분 도메인명 — 지정된 문자열과 이름이 일치하거나 그 문자열로 끝나는 이름을 가진 모든 호스트를 허가합니다.
- 완전한 IP 주소 — 특정 IP 주소에 대한 접근을 허가합니다.
- 서브넷 — 예, **`192.168.1.0/255.255.255.0`**
- 네트워크 CIDR 규약 — 예, **`10.3.0.0/16`**

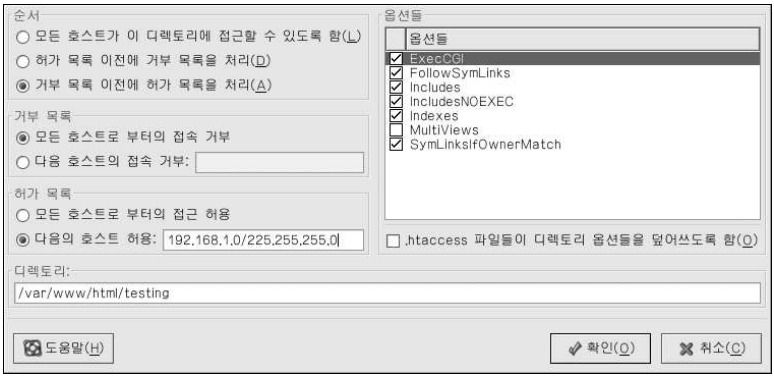

그림 19-7. 디렉토리 설정

.htaccess 파일들이 디렉토리 옵션들을 덮어쓰도록 함 옵션을 체크하시면 `.htaccess` 파일 내의 설정 지시자가 우선 순위를 갖게 됩니다.

19.3. 가상 호스트 설정

HTTP 설정 도구를 사용하여 가상 호스트를 설정 가능합니다. 가상 호스트는 동일한 컴퓨터 상에서 다른 IP 주소, 다른 호스트명이나 다른 포트에서 다른 서버를 실행할 수 있게 해줍니다. 예로 들면, 가상 호스트를 사용하여 동일한 웹 서버에서 http://www.example.com와 http://www.anotherexample.com라는 두 개의 웹 사이트를 운영 가능합니다. 이 옵션은 디폴트 가상 호스트와 IP 기반 가상 호스트에 사용되는 <VirtualHost> 지시자에 상응하며, 이름 기반 가상 호스트에 사용되는 `<NameVirtualHost>` 지시자에 상응합니다.

한 개의 가상 호스트에만 설정된 지시자는 오직 그 특정 가상 호스트에만 적용됩니다. 만일 **기본 설정 편집** 버튼을 사용하여 그 지시자가 서버 전반에 설정되었다면, 기본 설정이 사용됩니다. 예를 들어 여러분은 각각의 가상 호스트에 대한 개별 이메일 주소를 정의하지 않고 **주** 탭에서 **웹마스터 이메일 주소**를 정의하실 수 있습니다.

HTTP 설정 도구는 그림 19-8에서 보여지는 것과 같은 기본 가상 호스트를 포함합니다.

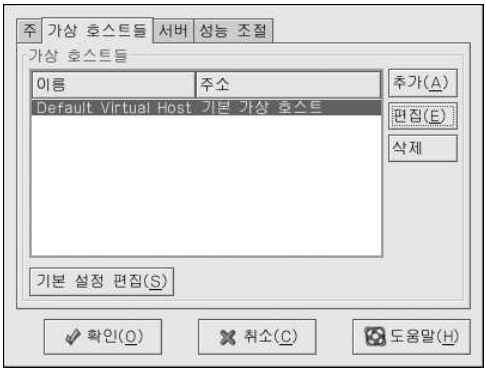

그림 19-8. 가상 호스트

기본 가상 호스트와 관련된 보다 많은 정보를 원하신다면, http://httpd.apache.org/docs-2.0/vhosts/ 사이트와 여러분의 컴퓨터에 설치된 Apache HTTP 서버 문서 자료를 참조하시기 바랍니다.

19.3.1. 가상 호스트 추가와 편집

가상 호스트를 추가하기 위해서는 **가상 호스트** 탭을 클릭하신 후 **추가** 버튼을 클릭합니다. 또한 목록에서 가상 호스트를 선택한 후 **편집** 버튼을 클릭하는 방법도 있습니다.

19.3.1.1. 일반 옵션

일반 옵션 설정은 여러분이 설정하시는 가상 호스트에만 적용됩니다. **가상 호스트 이름** 입력란에 가상 호스트의 이름을 설정해 주십시오. **HTTP 설정 도구**는 이 이름을 사용하여 가상 호스트들을 구별합니다.

문서 루트 디렉토리 값은 가상 호스트에 대한 루트 문서 (예, index.html)를 포함하고 있는 디렉토리로 설정하십시오. 이 옵션은 <VirtualHost> 지시문 내의 DocumentRoot 지시자에 상응합니다. Red Hat Linux 7 이전 버전에서 Red Hat Linux에 포함된 Apache HTTP 서버는 /home/httpd/html를 DocumentRoot로 사용해왔습니다. 그러나 Red Hat Linux 9에서 기본 DocumentRoot는 /var/www/html로 변경되었습니다.

웹마스터 이메일 주소는 VirtualHost 지시자 내의 ServerAdmin 지시자에 해당합니다. 오류 페이지에서 이메일 주소와 함께 주석을 보여주도록 선택하신 경우 오류 페이지의 주석에서 이 이메일 주소가 사용됩니다.

호스트 정보 섹션에서는 **기본 가상 호스트**, **IP 기반의 가상 호스트** 또는 **이름 기반의 가상 호스트** 중 한가지를 선택해 주십시오.

기본 가상 호스트

- 기본 가상 호스트는 한 개만 설정하셔야 합니다. (이미 한 개의 가상 호스트가 기본으로 설정되어 있다는 사실을 기억해 주십시오). 기본 가상 호스트 설정은 요청된 IP 주소가 다른 가상 호스트에 명확히 기재되지 않았을 경우에 사용됩니다. 만일 기본 가상 호스트가 정의되지 않았다면, 기본 서버 설정이 사용됩니다.

IP 기반의 가상 호스트

- **IP 기반의 가상 호스트**를 선택하시면, 서버의 IP 주소에 기반하여 <VirtualHost>directive를 설정하는데 사용되는 창이 나타납니다. **IP 주소** 란에 IP 주소를 지정해 주십시오. 한 개 이상의 IP 주소를 지정하시려면, 각 IP 주소 사이를 한 칸 띄어 입력하십시오. *IP 주소:*포트 구문을 사용하여 포트를 지정하시기 바랍니다. IP 주소에 해당하는 모든 포트를 설정하시려면 :* 를 사용하시면 됩니다. 가상 호스트에 대한 호스트명은 **서버 호스트명** 란에 입력해 주십시오.

이름 기반의 가상 호스트

- **이름 기반의 가상 호스트**를 선택하시면, 서버의 호스트명에 기반하여 NameVirtualHost 지시자를 설정하는데 사용되는 창이 나타납니다. **IP 주소** 란에 IP 주소를 지정해 주십시오. 한 개 이상의 IP 주소를 지정하시려면, 각 IP 주소 사이를 한 칸 띄어 입력하십시오. *IP 주소:*포트 구문을 사용하여 포트를 지정하시기 바랍니다. IP 주소에 해당하는 모든 포트를 설정하시려면 :* 를 사용하시면 됩니다. 가상 호스트에 대한 호스트명은 **서버 호스트명** 란에 입력해 주십시오. **별칭들** 섹션에서는 **추가** 버튼을 클릭하여 호스트명 별칭을 추가하실 수 있습니다. 이곳에 별칭을 추가하시면 NameVirtualHost 지시자 안에 ServerAlias 지시자가 추가됩니다.

19.3.1.2. SSL

알림

이름 기반의 가상 호스트는 SSL과 함께 사용하실 수 없습니다. 그 이유는 (브라우저가 보안 웹 서버의 인증서를 받을 때) 적절한 이름 기반 가상 호스트를 식별하는 HTTP 요청이 일어나기 전에 SSL 주고 받기(handshake)가 발생하기

때문입니다. 만일 이름-기반 가상 호스트 사용을 원하신다면, 비-보안 웹 서버를 사용하시는 경우에만 가능합니다.

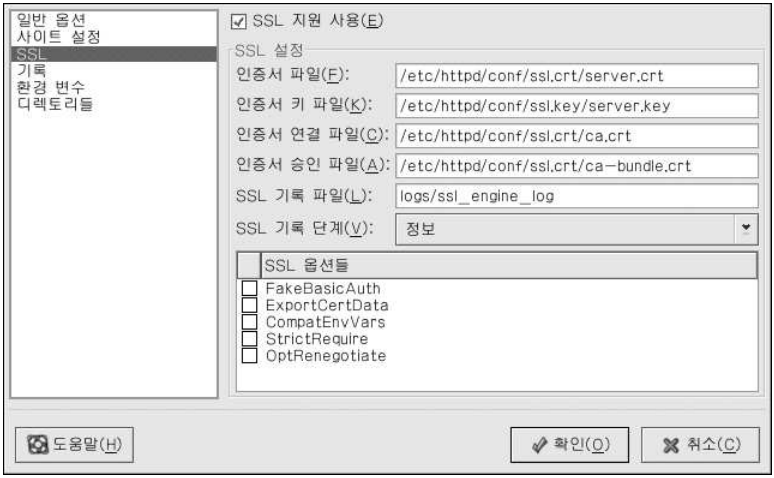

그림 19-9. SSL 지원

만일 Apache HTTP 서버가 SSL 지원 없이 설정되었다면, Apache HTTP 서버와 클라이언트 사이의 통신은 암호화되지 않기 때문에 개인 정보나 비밀 정보가 저장되지 않은 웹 사이트에 적합합니다. 예로 들면 공개 소스 소프트웨어와 문서 자료를 배포하는 공개 소스 웹사이트에서는 보안 통신이 필요하지 않습니다. 하지만 신용카드 정보를 필요로하는 전자 상거래 웹사이트의 경우에는 반드시 통신을 암호화하기 위하여 Apache SSL 지원을 사용해야 합니다. Apache SSL 지원을 사용을 활성화한다면 `mod_ssl` 보안 모듈의 사용도 활성화됩니다. **HTTP 설정 도구**를 통하여 Apache SSL 지원을 활성화하기 위해서는 **주** 탭 => **사용 가능한 주소들**에서 443 포트를 통한 접속을 허용해야만 합니다. 보다 자세한 사항에 대해서는 19.1 절을 참조하시기 바랍니다. 그 후 **가상 호스트** 탭에서 가상 호스트명을 선택하고 **편집** 버튼을 클릭합니다. 왼쪽에 위치한 메뉴에서 **SSL**을 선택하신 후 그림 19-9에서 보여지듯이 **SSL 지원 사용** 옵션을 체크합니다. **SSL 설정** 부분은 가짜 디지털 인증서 (dummy digital certificate)를 사용하여 미리 설정되었습니다. 디지털 인증서는 보안 웹 서버를 위한 인증을 제공하며 클라이언트 웹 브라우저에 대한 보안 서버를 식별합니다. Red Hat Linux에서 제공한 가짜 디지털 인증서를 여러분 웹사이트에 사용하지 마십시오. CA-승인 디지털 인증서를 구입하는 방법에 대한 자세한 정보를 원하신다면 20 장을 참조하시기 바랍니다.

19.3.1.3. 가상 호스트 추가 옵션들

가상 호스트를 위한 **사이트 설정**, **환경 변수**, 그리고 **디렉토리** 옵션은 여러분이 **디폴트 설정 편집** 버튼을 클릭하셨을 때 설정하신 지시자와 모두 동일합니다. 단지 여기서 설정된 옵션들은 여러분이 설정하고 계신 개별 가상 호스트를 위한 것이라는 한가지 차이점이 있습니다. 이러한 옵션들에 대한 보다 자세한 정보를 원하시면 19.2 절을 참조하시기 바랍니다.

19.4. 서버 설정

서버 탭에서는 기본 서버 셋팅을 설정하실 수 있습니다. 대부분의 경우, 이미 설정된 디폴트 옵션을 사용하시면 충분합니다.

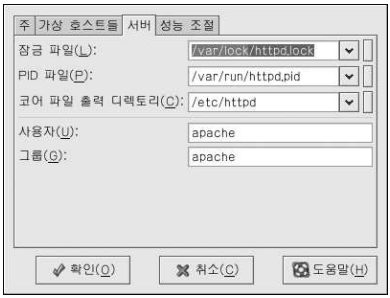

그림 19-10. 서버 설정

잠금 파일값은 `LockFile` 지시자에 해당합니다. 이러한 지시자는 서버가 USE_FCNTL_SERIALIZED_ACCEPT 또는 USE_FLOCK_SERIALIZED_ACCEPT를 사용하여 컴파일되었을 때 사용되는 잠금 파일로의 경로를 설정합니다. 잠금 파일의 값은 반드시 로컬 디스크에 저장되어야 합니다. `logs` 디렉토리가 NFS 공유 상에 위치하지 않는 한, 잠금 파일의 값은 디폴트 값으로 놔두셔야 합니다. 만일 `logs` 디렉토리가 NFS 공유 상에 위치하는 경우에 디폴트 값은 반드시 로컬 디스크 상의 위치와 그리고 루트에 의해서만 읽혀지는 디렉토리의 위치로 변경되어야 합니다.

PID 파일 값은 `PidFile` 지시자에 해당합니다. 이 지시자는 서버의 프로세스 ID (pid)가 기록되는 파일을 설정합니다. 이 파일은 루트에 의해서만 읽혀집니다. 대부분의 경우에 파일은 디폴트 값으로 그냥 두셔야 합니다.

핵심 덤프 디렉토리 값은 `CoreDumpDirectory` 지시자와 일치합니다. 서버는 핵심 파일을 덤프하기 이전에 이 디렉토리로 전환을 시도합니다. 디폴트 값은 `ServerRoot`입니다. 그러나 만일 (서버를 실행하는데 사용된) 사용자 ID가 이 디렉토리에 쓰기 허가가 없다면, 핵심 덤프도 기록될 수 없습니다. 만일 디버깅 목적으로 핵심 덤프를 디스크에 기록하기를 원하신다면, 이 값을 (서버를 실행하는데 사용된) 사용자 ID가 쓰기 허가를 가지고 있는 디렉토리로 변경하십시오.

사용자 값은 `User` 지시자에 해당합니다. 이 사용자 값은 요청에 답하기 위하여 서버에 의해 사용되는 사용자 ID (userid)를 설정합니다. 이러한 사용자 설정은 서버에 대한 액세스를 결정합니다. 이 사용자 ID가 접근할 수 없는 파일들은 여러분 웹사이트에 방문한 사용자도 접근할 수 없습니다. `User`의 기본값은 apache 입니다.

사용자는 외부에 공개되는 파일에만 접근할 수 있는 허가를 가져야 합니다. 사용자는 또한 서버에 의해 산출된 모든 CGI 프로세스의 소유자가 됩니다. 그 사용자는 또한 HTTP 요청에 대한 응답에 포함될 수 없는 코드는 실행할 권한이 없습니다.

경고

만일 무엇을 해야할지 모르신다면 `User` 지시자를 루트로 설정하지 마십시오. 루트를 `User`로서 사용하시면 웹 서버에 중대한 보안 허점을 가져오게 됩니다.

부모 `httpd` 프로세스는 일반적인 작업 과정에서 루트로서 처음 실행되지만 그 후 즉시 apache 사용자로 넘어갑니다. 서버는 1024 이하 포트로 바인드되기 위하여 루트로 시작해야 합니다. 1024 이하 포트는 시스템용으로 보존되기 때문에 루트 이외에는 어떠한 사용자에 의해서도 사용되지 않습니다. 일단 서버가 포트에 연결되면, 서버는 그 프로세스를 apache 사용자가 다른 연결 요청을 수락하기 전에 apache 사용자에게 넘겨줍니다.

Group 값은 `Group` 지시자에 해당합니다. `Group` 지시자는 `User` 지시자와 유사합니다. `Group`은 요청에 응답할 서버 하에 그룹을 설정합니다. 기본 그룹도 apache 입니다.

19.5. 성능 조절

성능 조절 탭에 클릭하여 여러분이 원하시는 자식 서버 프로세스의 최대수와 클라이언트 연결에 대한 Apache HTTP 서버 옵션을 설정하십시오. 이러한 옵션에 이미 설정된 디폴트 옵션을 사용하시면 대부분의 경우에 적합할 것입니다. 이 설정을 변경하시면 웹 서버의 전반적인 성능에 영향을 미치게 됩니다.

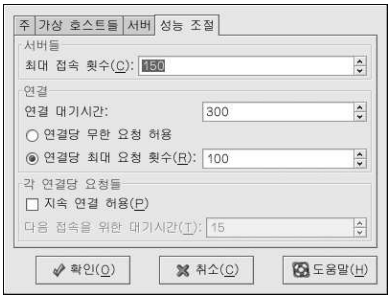

그림 19-11. 성능 조절

최대 접속 횟수를 서버가 처리할 수 있는 동시 클라이언트 요청의 최대 수로 설정하십시오. 각각의 연결에 대하여 자식 `httpd` 프로세스가 생성됩니다. 프로세스의 최대 수에 이르게 되면 자식 서버 프로세스가 한개라도 빠져나오기 이전에는 어느 누구도 웹 서버에 접속할 수 없습니다. 최대 연결 수는 서버를 재컴파일하지 않고서 256을 넘게 설정될 수 없습니다. 이 옵션은 `MaxClients` 지시자에 해당합니다.

연결 대기시간은 서버가 통신을 주고 받는데 기다리는 시간의 양을 초 단위로 정의합니다. 구체적으로 말하면 **연결 대기시간**은 서버가 GET 요청을 받기 위하여 기다려야할 시간, POST나 PUT 요청 상에서 TCP 패킷을 받기위하여 기다리는 시간과 그리고 TCP 패킷에 대한 ACK 응답 사이의 시간을 정의합니다. 디폴트 값으로 **연결 대기시간**은 300초로 설정되었으며 이 디폴트 값은 대부분의 경우에 적합합니다. 이 옵션은 `TimeOut` 지시자에 해당합니다.

연결당 최대 요청 횟수를 지속적인 연결마다 허용되는 최대 요청수로 설정합니다. 디폴트 값은 100이며 대부분의 경우 이 디폴트 값을 사용하는 것이 적합할 것입니다. 이 옵션은 `MaxRequestsPerChild` 지시자에 해당합니다.

연결당 무한 요청 허용 옵션을 선택하신다면, `MaxKeepAliveRequests` 지시자는 0가 되고 무제한 요청이 허가됩니다.

지속 연결 허용 옵션을 선택하지 않으시면, `KeepAlive` 지시자는 꺼짐 (false)로 설정됩니다. 이 옵션을 선택하시면, `KeepAlive` 지시자는 켜짐 (true)로 설정되며, `KeepAliveTimeout` 지시자는 **다음 접속을 위한 대기시간** 값에 설정된 숫자로 설정됩니다. 이 지시자는 서버가 한가지 요청을 서비스한 후 연결을 닫기 이전에 다음 연결을 기다리는 초 수를 설정합니다. 일단 요청을 받으면 **연결 대기시간** 값이 대신 적용됩니다.

지속 연결 허용을 높은 값으로 설정하시면 서버에 얼마나 사용자가 접속을 시도하느냐에 따라서 서버가 느려지게 만들 수도 있습니다. 숫자가 높을수록 서버에 연결된 마지막 클라이언트로부터 또 다른 연결을 기다리는 서버 프로세스의 수가 더 많아지게 됩니다.

19.6. 설정 저장

여러분이 변경하신 Apache HTTP 서버 설정 셋팅을 저장하지 않으시려면, **HTTP 설정 도구** 창 오른쪽 모서리 아래쪽에 위치한 **취소** 버튼을 클릭하십시오. 결정을 확인하는 대화 상자가 나타날 것입니다. 선택하신

것을 확인하기 위하여 **예** 버튼을 클릭하시면 설정이 저장되지 않을 것입니다.

Apache HTTP 서버 설정 셋팅을 저장하시려면 **HTTP 설정 도구** 창 오른쪽 모서리 아래쪽에 위치한 **확인** 버튼을 클릭하십시오. 대화창이 나타날 것입니다. 만일 **예**라고 대답하시면, 설정이 `/etc/httpd/conf/httpd.conf` 파일에 저장될 것입니다. 원래의 설정 파일은 덮어 쓰여진다는 것을 기억해 주십시오.

만일 **HTTP 설정 도구**를 처음 사용하셨다면, 설정 파일이 수동으로 조작되엇다는 경고 대화 상자가 나타날 것입니다. 만일 **HTTP 설정 도구**가 `httpd.conf` 설정 파일이 수동으로 조작된 것을 발견하게 되면, 이 프로그램은 수정된 파일을 `/etc/httpd/conf/httpd.conf.bak`로 저장할 것입니다.


중요

설정을 저장하신 후 `service httpd restart` 명령을 사용하여 `httpd` 데몬을 재시작하셔야 합니다. 이 명령을 실행하시기 위해서는 반드시 루트로 로그인하셔야 합니다.

19.7. 추가 자료

Apache HTTP 서버와 관련된 보다 많은 정보를 원하신다면, 다음에 나온 자료들을 참조하시기 바랍니다.

19.7.1. 설치된 문서 자료들

- Apache HTTP 서버 문서 자료 — 만일 `httpd-manual` 패키지를 설치하셨고 Apache HTTP 서버 데몬 (`httpd`) 이 실행 중이라면, Apache HTTP 서버 문서 자료를 보실 수 있습니다. 웹 브라우저를 열고 Apache HTTP 서버를 실행하고 있는 서버상의 URL http://localhost로 가십시오. 그 후 **Documentation** 링크를 클릭하시면 됩니다.
- `/usr/share/docs/httpd-`*`<version>`* — *Apache Migration HOWTO* 문서에는 1.3 버전과 2.0 버전의 차이점을 비롯하여 설정 파일을 직접 수정하여 2.0 버전으로 업그레이드 하는 방법이 설명되어 있습니다.

19.7.2. 유용한 웹사이트

- http://www.apache.org — *Apache* 소프트웨어 재단.
- http://httpd.apache.org/docs-2.0/ — *Apache HTTP* 서버 버전 *2.0* 사용자 가이드를 포함한 Apache HTTP 서버 2.0 버전에 대한 Apache Software Foundation의 문서 자료.
- http://localhost/manual/index.html — 로컬 시스템 상에서 Apache HTTP 서버를 시작하신 후 이 URL을 사용하여 Apache HTTP 서버 2.0 버전 사용자 가이드를 보실 수 있습니다.
- http://www.redhat.com/support/resources/web_ftp/apache.html — Red Hat 지원팀은 여러 유용한 Apache HTTP 서버 웹 서버 링크의 목록을 보유하고 있습니다.
- http://www.redhat.com/support/docs/faqs/RH-apache-FAQ/book1.html — Red Hat이 편집한 Red Hat Linux Apache Centralized Knowledgebase.

19.7.3. 관련 서적

- *Apache: The Definitive Guide* 저자 Ben Laurie 와 Peter Laurie; O’Reilly & Associates, Inc.

- *Red Hat Linux* 참조 가이드; Red Hat, Inc. — 이 설명서에는 수동으로 Apache HTTP 서버 버전 1.3을 Apache HTTP 서버 버전 2.0으로 업데이트하는 방법에 대한 지시 사항과 더불어 Apache HTTP 서버 지시자에 대한 보다 자세한 정보와 Apache HTTP 서버에 모듈을 추가하는 방법에 대한 설명이 포함되어 있습니다.

redhat.

20장 .

Apache HTTP 보안 서버 설정

20.1. 소개

이 장에서는 OpenSSL 라이브러리와 툴킷(toolkit)를 사용하도록 활성화된 `mod_ssl` 보안 모듈을 사용하는 Apache HTTP 서버에 대한 기본적인 정보를 제공합니다. Red Hat Linux에서 제공하는 이러한 세가지 구성 요소를 기반으로 하는 서버를 보안 웹 서버 또는 단순히 보안 서버라고 부릅니다.

`mod_ssl` 모듈은 Apache HTTP 서버에 사용되는 보안 모듈입니다. `mod_ssl` 모듈은 OpenSSL 프로젝트에서 제공된 도구를 사용하여 Apache HTTP 서버에 매우 중요한 기능 — 통신을 암호화하는 기능을 추가합니다. 반면에 일반 HTTP를 사용한 브라우저와 웹 서버 사이의 통신은 평문(plaintext) 형태로 전송되기 때문에 브라우버와 서버 사이 경로에서 다른 사람이 가로채거나 읽을 가능성이 있습니다.

이 장에서는 이러한 프로그램에 대한 완전하고 독점적인 정보를 제공하지 않습니다. 이 가이드는 가능하면 특정 주제에 대한 더욱 광범위한 문서 자료를 찾을 수 있는 적절한 곳을 여러분에게 알려드리는 것을 목적으로 합니다.

이 장에서는 이 프로그램들을 설치하는 방법을 설명해 보겠습니다. 또한 비밀키 (private key)와 인증서 요청 (certificate request)을 생성하는 방법 및 자신이 서명한 인증서 생성하는 방법, 그리고 보안 서버와 함께 사용할 인증서 설치하는 방법도 알려드립니다.

`mod_ssl` 설정 파일은 `/etc/httpd/conf.d/ssl.conf`에 위치합니다. `mod_ssl` 모듈이 작동할 수 있도록 이 파일을 읽어오기 위해서는, `/etc/httpd/conf/httpd.conf` 파일에 `Include conf.d/*.conf` 문장이 포함되어야 합니다. 이 문장은 Red Hat Linux 9의 기본 Apache HTTP 서버 설정 파일에 디폴트 값으로 포함되어 있습니다.

20.2. 보안 관련 패키지 개요

보안 서버를 활성화하시려면, 최소한 다음과 같은 패키지를 설치하셔야 합니다:

`httpd`

- `httpd` 패키지에는 `httpd` 대몬과 관련 유틸리티, 설정 파일, 아이콘, Apache HTTP 서버 모듈, 메뉴얼 페이지 및 Apache HTTP 서버에 의해 사용되는 그 외 다른 파일들이 포함되어 있습니다.

`mod_ssl`

- `mod_ssl` 패키지에는 `mod_ssl` 모듈이 포함되어 있습니다. 이 모듈은 SSL (Secure Sockets Layer)와 TLS (Transport Layer Security) 프로토콜을 통하여 Apache HTTP 서버에 강력한 암호화 기능을 제공합니다.

`openssl`

- `openssl` 패키지에는 OpenSSL 도구키트가 포함되어 있습니다. SSL 프로토콜과 TLS 프로토콜을 구현하는 OpenSSL 도구키트에는 일반 용도의 암호화 라이브러리도 포함되어 있습니다.

추가로 Red Hat Linux에 포함된 기타 소프트웨어 패키지는 특정 보안 기능을 제공합니다 (그러나 이러한 추가 패키지가 없이도 보안 서버는 작동 가능합니다):

`httpd-devel`

- `httpd-devel` 패키지는 Apache HTTP 서버 include 파일, 헤더 파일 및 APXS 유틸리티를 포함합니다. 이 제품에서 제공된 모듈을 이외의 기타 다른 모듈을 읽어올 계획이라면 이 패키지가 필요합니다. Apache의 DSO 기능을 사용하여 보안 서버에 모듈을 로딩하는 방법에 대한 보다 많은 정보를 원하신다면, *Red Hat Linux* 참조 가이드를 참조하시기 바랍니다.

Apache HTTP 서버 서버에 다른 모듈을 로드할 계획이 없다면, 이 패키지를 설치하실 필요가 없습니다.

`httpd-manual`

‘ `httpd-manual` 패키지에는 Apache 프로젝트의 *Apache* 사용자 가이드가 HTML 형식으로 포함되어 있습니다. 이 메뉴얼은 또한 http://httpd.apache.org/docs-2.0/ 웹사이트에서도 찾으실 수 있습니다.

OpenSSH 패키지

‘ OpenSSH 패키지에는 원격 컴퓨터에 로그인하여 명령어를 실행하는데 필요한 네트워크 연결 도구의 OpenSSH 세트가 포함되어 있습니다. OpenSSH 도구는 암호를 비롯한 모든 트래픽을 암호화합니다. 따라서 여러분의 컴퓨터와 원격 컴퓨터 사이에 통신을 주고 받을 때 누군가 접속을 도청하거나 공격하는 것을 방지할 수 있습니다.

`openssh` 패키지에는 OpenSSH 클라이언트 프로그램과 OpenSSH 서버에서 필요한 핵심 파일들이 포함되어 있습니다. `openssh` 패키지에는 또한 로컬 컴퓨터와 원격 컴퓨터 사이에서 파일을 복사하는데 사용되는 `scp` 기능을 포함합니다. `scp`는 `rcp`의 보안 대체입니다.

`openssh-askpass` 패키지는 OpenSSH 에이전트를 사용시 암호를 요청하는 대화창을 보여주는 기능을 지원합니다..

`openssh-askpass-gnome` 패키지는 GNOME 데스크탑 환경에서 OpenSSH 프로그램이 암호를 요청시 그래픽 대화창을 보여주는 역할을 합니다. 만일 GNOME을 실행하고 OpenSSH 유틸리티를 사용하실 계획이라면, 이 패키지를 설치하시기 바랍니다.

`openssh-server` 패키지는 `sshd` 보안 쉘 데몬과 관련 파일들을 포함합니다. 보안 쉘 데몬은 서버 사이드 OpenSSH 모음으로서, SSH 클라이언트에서 호스트로의 연결을 허용하시려면 호스트 상에 보안 쉘 데몬을 설치하셔야 합니다.

`openssh-clients` 패키지에는 SSH 서버로 암호화된 연결을 형성하는데 필요한 클라이언트 프로그램들이 포함되어 있습니다. 포함된 클라이언트 프로그램들은 다음과 같습니다: `rsh`의 보안 대체인 `ssh`; (다른 컴퓨터 사이에서 파일을 전송하는데 사용되는) `ftp`의 보안 대체인 `sftp`; (원격 로그인을 위한) `rlogin`와 (Telnet 프로토콜을 통하여 다른 호스트와 통신하기 위한) `telnet`에 대한 보안 대체인 `slogin`

OpenSSH와 관련된 보다 많은 정보를 원하신다면, 15 장, *Red Hat Linux* 참조 가이드 및 OpenSSH 웹사이트인 http://www.openssh.com를 참조하시기 바랍니다.

`openssl-devel`

‘ `openssl-devel` 패키지에는 다양한 암호화 알고리즘과 프로토콜을 지원하는 응용 프로그램을 컴파일하는데 필요한 정적 라이브러리와 부속 파일들이 포함되어 있습니다. SSL 지원을 포함한 응용 프로그램을 개발하는 경우에만 이 패키지를 설치하십시오. — SSL 사용을 위해서는 이 패키지를 설치하실 필요가 없습니다.

`stunnel`

‘ `stunnel` 패키지는 Stunnel SSL 랩퍼(wrapper)를 제공합니다. Stunnel은 TCP 접속의 SSL 암호화를 지원하며 따라서 데몬의 코드를 변경하지 않고도 SSL를 인식하지 않는 데몬이나 프로토콜 (예, POP, IMAP, LDAP)을 암호화할 수 있습니다.

표 20-1에서는 보안 서버 패키지들에 대한 요약 정보와 각 패키지들이 보안 서버 설치에 필요한지 아니면 옵션인지 여부를 보여줍니다.

패키지명	옵션 여부?
`httpd`	아니오
`mod_ssl`	아니오
`openssl`	아니오

패키지명	옵션 여부?
httpd-devel	예
httpd-manual	예
openssh	예
openssh-askpass	예
openssh-askpass-gnome	예
openssh-clients	예
openssh-server	예
openssl-devel	예
stunnel	예

표 20-1. 보안 패키지

20.3. 인증서와 보안 개요

보안 서버는 SSL (Secure Sockets Layer) 프로토콜과 (대부분의 경우) CA (인증 기관 - Certificate Authority)에서 발급된 디지털 인증서를 조합하여 보안을 제공합니다. SSL은 브라우저와 보안 서버 사이의 통신을 암호화하며 상호 인증을 담당합니다. CA 인증을 받은 디지털 인증서는 여러분의 보안 서버에 대한 인증을 제공합니다 (CA는 자신의 신용을 바탕으로 사용자의 신분을 증명합니다). 브라우저가 SSL 암호화를 사용하여 통신을 주고 받는다면, 네이게이션 바(navigation bar)에서 URL (Uniform Resource Locator)의 첫 부분이 `https://`로 시작하는 것을 볼 수 있습니다.

암호화는 키를 사용하는 방법에 따라 달라집니다 (키를 데이터 형식으로된 비밀 부호기/해독기 링으로 취급합니다). 관용 암호 방식이나 대칭 암호 방식에서는 암호화와 복호화에 동일한 키를 사용합니다. 공개 키 암호 방식이나 비대칭 암호 방식에서는 두개의 키: 공개키와 비밀키를 함께 사용합니다. 개인이나 기업체는 비밀키(private key)를 자신만이 알고있으면서 비밀스럽게 보관하며, 공개키(public key)를 공개합니다. 공개키를 사용하여 암호화된 데이터는 개인키를 사용해서만 해독할 수 있습니다; 또한 개인키를 사용하여 암호화된 데이터는 오직 공개키를 사용해서 해독 가능합니다.

보안 서버를 설정하기 위해서는, 공개키 암호 방식을 사용하여 공개키와 개인키 쌍을 생성하셔야 합니다. 대부분의 경우에 사용자가 인증 요구서(공개키 포함), 회사의 신원 증명과 지불 금액을 CA로 보내면, CA는 인증 요구서와 사용자의 신원을 확인 후 사용자의 보안 서버에 대한 인증서를 보내줍니다.

보안 서버는 인증서를 사용하여 웹 브라우저에 자신의 신원을 확인합니다. 사용자는 독자적인 인증서 (소위 "자체 서명" 인증서)를 생성하거나 또는 인증 기관 (CA)에서 인증서를 받을 수 있습니다. 인정받는 CA로부터의 인증서는 웹사이트가 특정 회사 또는 조직과 연계된 것을 보증합니다.

다른 방법으로 사용자는 자체 서명한 인능서를 생성할 수 있습니다. 하지만 자체 서명 인증서는 대부분의 생산 환경에서는 사용하지 마십시오. 자세 서명 인증서는 사용자의 브라우저가 자동으로 수락하지 않습니다 — 즉, 브라우저가 사용자에게 그 인증서를 수락할 것인지를 물은 후 안전한 접속을 생성합니다. 자체 서명 인증서와 CA 서명 인증서의 차이점에 대한 보다 많은 정보를 원하신다면, 20.5 절를 참조하시기 바랍니다.

자체 서명 인증서나 여러분이 선택하신 CA가 서명한 인증서를 받으셨다면, 이제 보안 서버에 인증서를 설치하셔야 합니다.

20.4. 기존의 키와 인증서 사용하기

기존의 키와 인증서가 존재하는 경우 (예를 들어 회사의 보안 서버 제품을 교체하기 위하여 새로운 보안 서버를 설치하시는 경우), 보안 서버와 함께 기존의 키와 인증서를 사용하실 수 있습니다. 하지만 다음과 같은 두가지 경우에는 기존의 키와 인증서를 사용하실 수 없습니다:

- *IP* 주소 또는 도메인명을 변경하시는 경우 — 인증서는 특정 IP 주소와 도메인명에 따라서 발행되었습니다. 따라서 IP 주소나 도메인명을 변경하시는 경우에는 새로운 인증서를 다시 받으셔야 합니다.
- *VeriSign*으로부터 인증서를 발급 받은 후 서버 소프트웨어를 변경하는 경우 — 베리사인(Verisign)은 세계적인 보안 인증 기관 (CA) 입니다. 이미 다른 목적으로 발급받은 VeriSign 인증서를 가지고 있는 경우 새로운 보안 서버에 기존의 VeriSign 인증서를 사용할 수 없습니다. 그 이유는 오직 하나의 특정 서버 소프트웨어와 IP 주소/도메인명 조합에 한하여 VeriSign 인증서가 발급되기 때문입니다.

  만일 특정 서버 소프트웨어와 IP 주소/도메인명 조합 중 하나라도 변경된다면 (예를 들어 이전에 다른 보안 서버 제품을 사용하신 경우), 기존 설정을 사용하여 발급받은 VeriSign 인증서는 새로운 설정에선 작용하지 않습니다. 따라서 새로운 인증서를 발급받으셔야 합니다.

만일 기존 키와 인증서가 사용 가능하다면, 새로운 키를 생성하여 새 인증서를 발급받으실 필요가 없습니다. 하지만 여러분의 키와 인증서를 포함한 파일들을 다른 위치로 이동시킨 후 파일명을 변경해 주십시오.

기존 키 파일을 다음의 위치로 이동시킵니다:

```
/etc/httpd/conf/ssl.key/server.key
```

기존 인증서 파일을 다음의 위치로 이동시킵니다:

```
/etc/httpd/conf/ssl.crt/server.crt
```

키와 인증서를 이동시킨 후 20.9 절으로 넘어가시기 바랍니다.

Red Hat 보안 웹 서버에서 업그레이드 하신다면, 기존의 키 (`httpsd.key`)와 인증서 (`httpsd.crt`)는 `/etc/httpd/conf/`에 위치합니다. 새로운 보안 서버가 이 파일들을 찾아서 사용할 수 있도록 다음의 두 명령어를 사용하여 키와 인증서를 이동하신 후 이름을 변경시켜 주십시오:

```
mv /etc/httpd/conf/httpsd.key /etc/httpd/conf/ssl.key/server.key
mv /etc/httpd/conf/httpsd.crt /etc/httpd/conf/ssl.crt/server.crt
```

그 후 다음의 명령어를 사용하여 보안 서버를 시작합니다:

```
/sbin/service httpd start
```

보안 서버에 대한 암호를 입력하시도록 요구할 것입니다. 암호를 입력하신 후 [Enter] 키를 누르시면 서버가 시작합니다.

20.5. 인증서 유형

Red Hat Linux에 포함된 RPM 패키지를 통해 보안 서버를 설치하신 경우, 임의 키와 테스트 인증서가 생성되어 적절한 디렉토리에 저장됩니다. 보안 서버를 사용하기에 앞서, 여러분은 자체 키를 생성하시고 서버를 올바르게 입증하는 인증서를 발급받으셔야 합니다.

보안 서버를 작동하기 위해서는 키와 인증서가 필요합니다 — 즉 자체 서명한 인증서를 생성하거나 또는 CA로부터 CA가 서명한 인증서를 구입하셔야 합니다. 그렇다면 이 두 인증서의 차이점은 무엇일까요?

CA-전자서명 인증서는 서버에 대한 다음과 같은 두가지 중요한 기능을 제공합니다:

- 브라우저는 (일반적으로) 인증서를 자동으로 인식하여 사용자에게 요구하지 않고서도 보안 접속을 허용합니다.
- CA가 서명한 인증서를 발급받는 것은, CA가 브라우저에 웹페이지를 제공하는 회사의 신원을 보증한다는 것을 의미합니다.

만일 다수의 일반 사용자가 보안 서버에 접속하는 경우, 보안 서버에는 CA가 서명한 인증서가 필요합니다. 여러분의 웹 사이트를 방문하는 일반 사용자들은 CA 전자서명 인증서를 통하여 웹 사이트를 소유한 회사의 신원을 확인할 수 있습니다. CA는 인증서를 요청한 기업체의 신원을 확인 후 인증서에 서명하기 때문에 믿을 수 있습니다.

SSL을 지원하는 대부분의 웹 브라우저에는 자동으로 수락할 인증서를 발급하는 CA의 목록이 포함되어 있습니다. 따라서 만일 목록에 포함되지 않은 CA가 서명한 인증서를 발견한 경우, 브라우저는 사용자에게 접속을 허락할 것인지 또는 거절할 것인지 여부를 선택하도록 요청합니다.

여러분 스스로 보안 서버에 대한 자체 서명 인증서를 생성할 수 있지만 자체 서명한 인증서는 CA가 서명한 인증서와 동일한 기능을 제공하지 않는다는 점에 주의해 주십시오. 자체 서명 인증서는 다른 사용자의 브라우저에 의해 자동으로 인식되지 않을 뿐만 아니라 웹 사이트를 제공하는 인증서 소유자의 신원에 대한 어떠한 보증도 제공하지 않습니다. 그러나 CA가 서명한 인증서는 보안 서버에 이러한 중요한 기능을 제공합니다. 만일 생산 환경에서 보안 서버를 사용하실 경우에는 반드시 CA가 서명한 인증서를 사용하시기 바랍니다.

CA로부터 인증서를 발급받는 절차는 생각보다 간단합니다. 기본적인 절차는 다음과 같습니다:

1. 암호화 개인 키와 공개 키쌍을 생성합니다.
2. 공개키에 기초한 인증 요구서를 생성합니다. 인증 요구서에는 여러분의 서버와 서버를 호스팅하는 회사에 대한 정보를 기입하십시오.
3. 사용자의 신원을 입증하는 문서와 함께 인증 요구서를 CA로 보냅니다. 이 메뉴얼에서는 어느 인증 기관을 선택할지 말해드릴 수 없습니다. 여러분은 과거 경험이나 친구, 동료의 추천 또는 순수 금전적인 요인에 따라서 스스로 결정하셔야 합니다.

   CA를 선택하신 후 인증서를 발급받기 위하여 해당 CA가 제공하는 지시 사항을 따르십시오.
4. 여러분의 신원을 확인 후 CA는 디지털 인증서를 보내줍니다.
5. 발급받은 인증서를 보안 서버에 설치합니다. 설치가 완료되면 보안 트랜잭션(transaction)을 시작할 수 있습니다.

CA에서 인증서를 발급받거나 자체 서명 인증서를 생성하시건 가장 먼저 하실 일은 키를 생성하는 것입니다. 키를 생성하는 방법에 대한 정보를 원하신다면 20.6 절을 참조하시기 바랍니다.

20.6. 키 생성하기

키를 생성하시려면 루트로 로그인하셔야 합니다.

우선 `cd` 명령을 사용하여 `/etc/httpd/conf` 디렉토리로 이동합니다. 다음과 같은 명령어를 사용하여 설치 과정에서 생성된 가짜(fake) 키와 인증서를 제거합니다:

```
rm ssl.key/server.key
rm ssl.crt/server.crt
```

이제 임의키를 생성하셔야 합니다. `/usr/share/ssl/certs` 디렉토리로 이동하신 후 다음과 같은 명령을 입력하십시오:

```
make genkey
```

시스템은 다음과 같은 메시지를 출력할 것입니다:

```
umask 77 ; \
/usr/bin/openssl genrsa -des3 1024 > /etc/httpd/conf/ssl.key/server.key
Generating RSA private key, 1024 bit long modulus
.......++++++
.....................................................................++++++
e is 65537 (0x10001)
Enter PEM pass phrase:
```

이제 암호 문구를 입력하셔야 합니다. 보안을 최대화하기 위하여 암호 문구는 최소한 8자 이상으로 숫자와 구두점을 포함하면서 사전에는 없는 단어를 사용해야 합니다. 또한 암호는 대/소문자를 구별한다는 점을 잊지 마십시오.

알림

매번 보안 서버를 시작할 때마다 이 암호를 입력하셔야 합니다. 따라서 암호를 기억하시기 ?帽復求?.

암호가 올바른지 확인하기 위하여 재입력해주셔야 합니다. 정확한 암호가 재입력되면, 입력하신 키가 포함된 `/etc/httpd/conf/ssl.key/server.key` 파일이 만들어 집니다.

보안 서버를 시작할 때마다 암호를 입력하지 않아도 되도록 설정하시려면, `make genkey` 명령 대신 다음과 같은 두 명령어를 사용하여 키를 생성하시기 바랍니다.

다음 명령을 사용하여 키를 생성합니다:

```
/usr/bin/openssl genrsa 1024 > /etc/httpd/conf/ssl.key/server.key
```

그 후 다음 명령어를 사용하여 이 파일에 올바른 허가를 설정하시기 바랍니다:

```
chmod go-rwx /etc/httpd/conf/ssl.key/server.key
```

위의 명령어를 사용하여 키를 생성하시면, 보안 서버를 시작하실 때 암호를 입력하실 필요가 없습니다.

경고

보안 서버의 암호 요청 기능을 억제하는 것은 보안 허점이 될 수 있습니다. 따라서 저희는 보안 서버에 대한 암호 기능을 억제하는 것을 권장하지 않습니다.

암호를 사용하지 않음으로서 발생하는 문제점은 호스트 기계 상 보안 유지에 직접 관련됩니다. 예를 들어, 비양심적인 개인이 호스트 기계의 일반 UNIX 보안 시스템에 침입하여 여러분의 개인키 (`server.key` 파일의 내용)을 가로챌 가능성이 있습니다. 그 후 가로챈 개인키를 사용하여 웹 페이지가 여러분의 보안 서버에서 전송된 것처럼 조작 가능합니다.

만일 호스트 컴퓨터 상에서 UNIX 보안 관리가 철저하게 이루어진다면 (모든 운영 체제 패치와 업데이트가 사용 가능할때마다 바로 설치되고, 불필요하거나 위험한 작업 등을 수행하지 않는다면), 보안 서버에 암호를 입력하는 것이 불필요하게 느껴질 수도 있습니다. 그러나 보안 서버는 자주 재부팅될 필요가 없기 때문에, 대부분의 경우 보안 웹 서버에 별도의 보안을 제공하기 위하여 암호를 입력할 필요가 있습니다.

시스템 상 루트 사용자만이 `server.key` 파일을 소유할 수 있으며 어떠한 다른 사용자도 이 파일을 열 수 없습니다. 이 파일의 백업 복사본을 만드신 후 안전한 위치에 저장하시기 바랍니다. 만일 인증 요구서를 생성하기 위하여 `server.key` 파일을 사용하신 후 이 파일을 잃게되는 경우에는, 인증서가 더 이상 작용하지 않을 것이며 CA도 손을 쓸 수 없게 됩니다. 만일 이러한 경우가 발생한다면, 유일한 해결책은 새로운 인증서를 요구하고 다시 지불하는 방법 밖에 없습니다. 따라서 반드시 백업 복사본을 만들어 두셔야 합니다.

CA로부터 인증서를 구입하실 계획이라면 20.7 절으로 계속 읽어 나가십시오. 만일 여러분 스스로 자체-서명 인증서를 생성하실 계획이라면, 20.8 절으로 넘어 가십시오.

20.7. CA에 보낼 인증 요구서 생성하기

일단 키를 만드셨으면, 다음 단계는 여러분이 선택하신 CA에 보낼 인증 요구서를 만드는 것입니다. `/usr/share/ssl/certs` 디렉토리로 이동하신 후 다음 명령을 입력해 주십시오:

```
make certreq
```

시스템은 다음과 같은 결과를 출력한 후 암호를 요청할 것입니다 (암호 옵션을 억제하지 않은 경우):

```
umask 77 ; \
```

```
/usr/bin/openssl req -new -key /etc/httpd/conf/ssl.key/server.key
-out /etc/httpd/conf/ssl.csr/server.csr
Using configuration from /usr/share/ssl/openssl.cnf
Enter PEM pass phrase:
```

키를 생성할 때 선택하신 암호를 입력하시기 바랍니다. 일부 지시 사항들이 출력된 후 일련의 질문 사항들이 나타날 것입니다. 여러분이 입력하신 내용은 인증 요구서에 포함됩니다. 질문 사항들과 예시 답변은 다음과 같이 나타납니다:

```
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a
DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:US
State or Province Name (full name) [Berkshire]:North Carolina
Locality Name (eg, city) [Newbury]:Raleigh
Organization Name (eg, company) [My Company Ltd]:Test Company
Organizational Unit Name (eg, section) []:Testing
Common Name (your name or server's hostname) []:test.example.com
Email Address []:admin@example.com
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

각각의 질문에 대한 디폴트 입력값은 질문 바로 다음 `[]` 괄호 안에 나타납니다. 예로 들면 인증서가 사용될 국가 코드에 대한 첫 질문은 다음과 같이 나타납니다:

```
Country Name (2 letter code) [GB]:
```

괄호 안에 있는 디폴트 입력값은 GB 입니다. 디폴트 값을 수락하기 위해서는 단순히 [Enter] 키를 누르십시오. 다른 값을 입력하시려면 해당 국가의 두자리 문자 코드를 입력하시기 바랍니다.

나머지 입력값은 여러분이 입력하셔야 합니다. 이 값들은 쉽게 입력 가능하지만 다음과 같은 지시 사항을 따르셔야 합니다:

- 지역이나 주에 대한 약칭을 사용하지 마십시오. 지역명이나 주명은 생략하지 않고 다 써야합니다. (예, St. Louis는 Saint Louis로 기입해야 합니다.)
- 만일 이 CSR을 CA로 보내는 경우 모든 입력란에서 특히 `Organization Name` (회사명)과 `Common Name` (웹서버 주소)란에 정확한 정보를 기입하십시오. CA는 CSR에 기입된 정보를 검토하여 `Common Name` 란에 기입된 웹서버가 해당 회사에 속하는지 여부를 확인합니다. 만일 CSR에 포함된 정보가 무효라고 판단되는 경우 CA는 해당 CSR을 인정하지 않습니다.
- `Common Name` 입력란에는 반드시 보안 서버의 약칭이 아닌 실제 이름 (유효한 도메인 이름 서비스 (DNS)명)을 입력하셔야 합니다.
- `Email Address` (이메일 주소) 입력란에는 웹마스터 또는 시스템 관리자의 이메일 주소를 입력합니다.
- @, #, &, ! 와 같은 특수 문자를 사용하시면 안됩니다. 일부 CA는 특수 문자가 포함된 인증 요구서를 인정하지 않습니다. 따라서 만일 여러분의 회사명에 앰퍼샌드 (&)가 있다면 "&" 대신 "and"라고 기입하십시오.
- 정보입력 과정 마지막에 나오는 추가 속성, 즉 `A challenge password` 와 `An optional company name`은 입력하지 마시고 [Enter] 키만 눌러주셔야 합니다.

모든 입력정보를 채우시면 /etc/httpd/conf/ssl.csr/server.csr이라는 파일이 생성됩니다. 이 파일은 여러분의 인증 요구서로서 CA에 보내질 준비가 되었습니다.

인증 요구서를 보낼 CA를 선택하신 후 CA 웹사이트에 나온 지시 사항을 따르십시오. 인증 요구서를 보내는 방법과 필요한 문서, 지불 방법에 대한 내용을 알려줄 것입니다.

CA의 요구 조건을 만족시킬 경우에 CA는 인증서를 (대부분의 경우 이메일을 통해) 보내줍니다. CA에서 받은 인증서인 /etc/httpd/conf/ssl.crt/server.crt를 저장 (또는 복사 후 붙여넣기) 하십시오. 이 파일의 백업을 만드시는 것도 잊지 마십시오.

20.8. 자체 서명 인증서(Self-Signed Certificate) 생성하기

여러분은 스스로 자체 서명한 인증서를 작성하실 수 있습니다. 자체 서명 인증서는 CA-서명 인증서와 같은 보안 보증을 제공하지 않는다는 점에 유의해 주십시오. 인증서에 대한 보다 상세한 정보를 원하신다면, 20.5 절을 참조하시기 바랍니다.

자체 서명 인증서를 생성하기 위해서는 우선 20.6 절에 나온 지시에 따라 임의키를 생성하셔야 하니다. 키를 생성 후 /usr/share/ssl/certs 디렉토리로 이동하여 다음 명령을 입력해 주십시오:

```
make testcert
```

다음과 같은 출력 결과가 나타나며 암호 입력이 요청될 것입니다 (암호없이 키를 생성한 경우 제외):

```
umask 77 ; \
/usr/bin/openssl req -new -key /etc/httpd/conf/ssl.key/server.key
-x509 -days 365 -out /etc/httpd/conf/ssl.crt/server.crt
Using configuration from /usr/share/ssl/openssl.cnf
Enter PEM pass phrase:
```

암호를 입력하신 후 (또는 암호없이 키를 생성한 경우 암호를 입력할 필요가 없이), 보다 많은 정보를 위한 일련의 질문 사항들이 나타날 것입니다. 컴퓨터의 질문 사항들과 예시 답변은 다음과 같이 나타납니다. (회사와 호스트에 대한 올바른 정보를 입력하십시오):

```
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a
DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:US
State or Province Name (full name) [Berkshire]:North Carolina
Locality Name (eg, city) [Newbury]:Raleigh
Organization Name (eg, company) [My Company Ltd]:My Company, Inc.
Organizational Unit Name (eg, section) []:Documentation
Common Name (your name or server's hostname) []:myhost.example.com
Email Address []:myemail@example.com
```

올바른 입력정보가 채워지면, 자체 서명 인증서가 생성되어 /etc/httpd/conf/ssl.crt/server.crt에 저장됩니다. 인증서를 생성하신 후 다음과 같은 명령을 사용하여 보안 서버를 재시작하셔야 합니다:

```
/sbin/service httpd restart
```

20.9. 인증서 테스트하기

디폴트로 설치된 테스트 인증서와 CA가 서명한 인증서 및 자체 서명한 인증서를 테스트해 보시려면, 웹 브라우저를 다음과 같은 홈페이지로 지정하십시오 (여기서 *server.example.com* 부분을 여러분의 도메인 명으로 교체하시기 바랍니다):

`https://server.example.com`

알림

`http` 다음에 나오는 `s`에 주목해 주십시오. `https:`는 보안 HTTP 트랜잭션을 위해 사용됩니다.

잘 알려진 CA로부터 발급받은 CA-서명 인증서를 사용하는 경우, 브라우저는 (사용자의 입력을 요청할 필요가 없이) 자동으로 인증서를 수락하고 안전한 접속을 생성할 것입니다. 하지만 테스트 인증서나 자체 서명 인증서는 CA에 의해 서명되지 않았기 때문에 자동으로 인식하지 못합니다. CA에서 발급받은 인증서를 사용하지 않으시는 경우, 브라우저에서 제공된 지시 사항을 따르시어 인증서를 수락하십시오.

브라우저가 인증서를 인식하면, 보안 서버는 디폴트 홈페이지를 보여줍니다.

20.10. 서버에 접속하기

보안 서버에 접속하시려면 다음과 같은 URL을 사용하시기 바랍니다:

`https://server.example.com`

비 보안 서버에 접속하기 위해서는 다음과 같은 URL을 사용하십시오:

`http://server.example.com`

보안 웹 통신을 위한 표준 포트는 포트 443 이며, 비-보안 웹 통신을 위한 표준 포트는 포트 80 입니다. 보안 서버 디폴트 설정은 두 개의 표준 포트를 모두 청취합니다. 따라서 포트 번호가 추측 가능하기 때문에 URL에 포트 번호를 지정하실 필요가 없습니다.

그러나 서버가 비표준 포트 (예, 80 또는 443 이외의 포트)를 청취하도록 설정하신 경우, 표준이 아닌 포트 상 서버에 접속하기 위한 모든 URL에 포트 번호를 지정하셔야 합니다.

예를 들어 가상 호스트가 포트 12331에서 비보안으로 실행되도록 설정했다고 가정합니다. 이 가상 호스트에 접속할 모든 URL에는 포트 번호를 지정하셔야 합니다. 포트 12331을 청취하는 비보안 서버에 접속하려는 URL은 다음과 같습니다:

`http://server.example.com:12331`

20.11. 추가 자료

Apache HTTP 서버와 관련된 추가 자료를 원하신다면 19.7 절을 참조하시기 바랍니다.

20.11.1. 설치된 문서 자료

- `mod_ssl documentation` — 웹 브라우저를 열고 Apache HTTP 서버를 실행 중인 서버 상에서 URL http://localhost/manual/mod/mod_ssl.html을 여시면 문서 자료를 찾으실 수 있습니다. `httpd-manual` 패키지가 설치되어 있어야 합니다.

20.11.2. 유용한 웹사이트

- http://www.redhat.com/mailing-lists/ — 이 URL에서 redhat-secure-server 메일링 리스트에 가입하실 수 있습니다.

  redhat-secure-server 메일링 리스트에 가입할 수 있는 또 다른 방법은 이메일 제목란에 *subscribe*라고 쓰신 후 <redhat-secure-server-request@redhat.com> 주소로 메일을 보내주시면 됩니다.

- http://www.modssl.org — `mod_ssl` 웹사이트는 `mod_ssl` 관련 정보를 얻을 수 있는 가장 확실한 자료입니다. 이 웹사이트에는 *User Manual*을 포함한 방대한 문서 자료들이 포함되어 있습니다. 웹사이트의 주소는: http://www.modssl.org/docs

20.11.3. 관련 서적

- *Apache: The Definitive Guide*, 2nd edition, 저자 Ben Laurie 와 Peter Laurie, O'Reilly & Associates, Inc.

21장 .

BIND 설정

이 장에서는 여러분이 BIND와 DNS에 대한 기본을 이해하고 계신다고 가정하고 BIND와 DNS의 개념에 대한 설명은 생략하고, **Bind 설정 도구** (`redhat-config-bind`)를 사용하여 기본 BIND 서버 영역을 설정하는 방법에 대하여 설명할 것입니다. **Bind 설정 도구**는 매번 여러분이 변경 사항을 적용하실 때마다 `/var/named` 디렉토리에 `/etc/named.conf` 설정 파일과 영역 설정 파일을 생성합니다.

중요

`/etc/named.conf` 설정 파일을 편집하지 마십시오. **Bind 설정 도구**는 여러분이 변경 사항을 적용하신 후에 이 파일을 생성합니다. 만일 **Bind 설정 도구**를 사용해서는 설정할 수 없는 셋팅을 설정하시려면, `/etc/named.custom` 파일에 원하시는 설정을 추가하시면 됩니다.

를 사용하기 위해서는 X 윈도우 시스템과 루트 권한이 필요합니다. **Bind 설정 도구**를 시작하시려면, 패널에서 **주 메뉴 버튼**을 클릭하신 후 => **시스템 설정** => **서버 설정** => **도메인 이름 서비스** 항목을 선택하시거나 쉘 프롬프트에서 (예, XTerm 또는 GNOME-터미널) `redhat-config-bind` 명령을 입력하시면 됩니다.

그림 21-1. Bind 설정 도구

Bind 설정 도구는 `/var/named`가 기본 영역 디렉토리가 되도록 설정합니다. 영역 파일들은 모두 이 디렉토리에 지정됩니다. **Bind 설정 도구**는 입력된 값에 대한 기본 구문을 검사하는 기능도 갖추고 있습니다. 예를 들어 IP 주소를 입력하실 경우, 이 도구는 텍스트 영역에 숫자와 점 (.) 기호로 이루어진 올바른 형식의 IP 주소만 받아 들입니다.

Bind 설정 도구 도구를 사용하여 순방향 마스터 영역 (forward master zone), 역방향 마스터 영역 (reverse master zone)과 슬레이브 영역 (slave zone)을 추가 가능합니다. 영역을 추가하신 후 그림 21-1에서 보이는 것과 같은 기본 창에서 추가하신 영역을 편집하거나 삭제하실 수 있습니다.

영역을 추가, 편집하거나 삭제하신 후, `/etc/named.conf` 설정 파일과 `/var/named` 디렉토리 내의 모든 개별 영역 파일을 기록하기 위하여 **저장** 버튼을 클릭하시거나 **파일** => **저장**을 선택해 주십시오. 또한 변경 사항을 저장하시면 `named` 서비스는 설정 파일들을 다시 읽어옵니다. 종료하시려면 **파일** => **종료**를 선택하여 변경 사항을 저장하신 후 종료하십시오.

21.1. 순방향 마스터 영역 추가하기

일차 마스터로도 알려진 순방향 마스터 영역을 추가하시려면, **추가** 버튼을 클릭하신 후 **순방향 마스터 영역**을 선택해 주십시오. 아래에 위치한 **도메인명** 텍스트 입력란에 마스터 영역의 도메인명을 입력하시기 바랍니다.

그림 21-2에서 보이는 것처럼 새로운 창이 열리며 다음과 같은 옵션이 나타날 것입니다:

- **이름** — 이전 창에서 방금 입력하신 도메인명.
- **파일명** — `/var/named`와 관련된 DNS 데이터베이스 파일의 파일명. 이 파일명은 뒤에 `.zone`이 붙은 도메인명으로 사전 설정되어 있습니다.
- **접속** — 마스터 영역에 사용될 이메일 주소.
- **1차 네임 서버 (SOA)** — SOA (State of authority) 레코드. 이 도메인에 사용될 가장 적합한 네임 서버를 지정합니다.
- **시리얼 번호** — DNS 데이터베이스 파일의 시리얼 번호. 시리얼 번호는 파일이 변경될 때마다 숫자가 증가되어, 해당 영역의 슬레이브 네임 서버가 최신의 데이터를 검색할 수 있게 해줍니다. **Bind 설정 도구** 도구는 설정이 변경될 때마다 이 시리얼 번호를 증가시킵니다. 또는 **시리얼 번호** 값 옆에 위치한 **설정** 버튼을 클릭하여 여러분이 직접 시리얼 번호를 설정하시는 것도 가능합니다.
- **시간 설정** — DNS 데이터베이스 파일에 저장되어 있는 **재생**, **재시도**, **만기**, **최소** TTL (Time to Live) 값. 모든 값은 초 단위입니다.
- **레코드** — **호스트**, **별칭**, **네임 서버** 유형의 레코드 자원을 추가, 편집하고 삭제할 수 있습니다.

그림 21-2. 순방향 마스터 영역 추가하기

1차 네임 서버 (SOA)가 반드시 지정되어야 하며, 최소한 **레코드** 부분에서 **추가** 버튼을 클릭하여 최소한 한개의 네임 서버 레코드를 지정해 주셔야 합니다.

순방향 마스터 영역의 설정을 마치셨다면, **확인** 버튼을 클릭하여 그림 21-1에 나온 주요 창으로 되돌아 가십시오. `/etc/named.conf` 설정 파일을 기록하고 모든 개별 영역 파일을 `/var/named` 디렉토리에 기록한 후 데몬이 설정 파일을 다시 읽어오도록 풀다운 메뉴에서 **저장** 버튼을 클릭하시기 바랍니다.

이러한 설정으로 인해 `/etc/named.conf` 파일에 다음과 같은 엔트리가 생성됩니다:

```
zone "forward.example.com" {
 type master;
 file "forward.example.com.zone";
};
```

이 설정은 또한 다음에 나온 정보를 사용하여 /var/named/forward.example.com.zone 파일을 생성합니다:

```
$TTL 86400
@   IN   SOA  ns.example.com. root.localhost (
          2 ; serial
          28800 ; refresh
          7200 ; retry
          604800 ; expire
          86400 ; ttl
          )


    IN   NS   192.168.1.1.
```

21.2. 역방향 마스터 영역 (Reverse Master Zone) 추가하기

역방향 마스터 영역을 추가하시려면, **추가** 버튼을 클릭하신 후 **역방향 마스터 영역**을 선택하시기 바랍니다. 설정하실 IP 주소의 첫 3개의 옥텟 (octet)을 입력해 주십시오. 예를 들어, IP 주소 범위 192.168.10.0/255.255.255.0를 설정하시려면 **IP 주소 (첫 3 옥텟)** 텍스트 입력란에 192.168.10 을 입력하시면 됩니다.

그림 21-3에서 보이는 것처럼 새로운 창이 다음과 같은 옵션을 가지고 나타날 것입니다:

1. **IP 주소** — 이전 창에서 방금 입력하신 첫 3 옥텟.
2. **역방향 IP 주소** — 편집 불가능한 항목으로서, 입력된 IP 주소에 기반하여 미리 채워져 있습니다.
3. **접속** — 마스터 영역에 사용될 이메일 주소.
4. **파일명** — /var/named와 관련된 DNS 데이터베이스 파일의 파일명.
5. **1차 네임 서버 (SOA)** — SOA (State of authority) 레코드. 이 도메인에 사용될 가장 적합한 네임 서버를 지정합니다.
6. **시리얼 번호** — DNS 데이터베이스 파일의 시리얼 번호. 시리얼 번호는 파일이 변경될 때마다 숫자가 증가되어, 해당 영역의 슬레이브 네임 서버가 최신의 데이터를 검색할 수 있게 해줍니다. **Bind 설정 도구** 도구는 설정이 변경될 때마다 이 시리얼 번호를 증가시킵니다. 또는 **시리얼 번호** 값 옆에 위치한 **설정** 버튼을 클릭하여 여러분이 직접 시리얼 번호를 설정하시는 것도 가능합니다.
7. **시간 설정** — DNS 데이터베이스 파일에 저장되어 있는 **재생**, **재시도**, **만기**, **최소** TTL (Time to Live) 값.
8. **네임 서버** — 역방향 마스터 영역에서 사용될 네임 서버를 추가, 편집하고 삭제하실 수 있습니다. 최소한 한 개의 네임 서버를 입력하셔야 합니다.
9. **역방향 주소 테이블** — 역방향 마스터 영역 내의 IP 주소와 호스트명의 목록입니다. 예를 들어 역방향 마스터 영역 192.168.10에 대한 **역방향 주소 테이블**에 IP 주소 192.168.10.1와 호스트명 one.example.com를 함께 입력하실 수 있습니다. 완전한 호스트명임을 나타내 주기 위하여 호스트명 마지막에는 반드시 점 (.)이 와야 합니다.

그림 21-3. 역방향 마스터 영역 (Reverse Master Zone) 추가하기

1차 네임 서버 (SOA)가 반드시 지정되어야 하며, 최소한 **네임 서버** 부분에서 **추가** 버튼을 클릭하여 최소한 한개의 네임 서버 레코드를 지정해 주셔야 합니다.

역방향 마스터 영역의 설정을 마치셨다면, **확인** 버튼을 클릭하여 그림 21-1에 나온 주요 창으로 되돌아 가십시오. `/etc/named.conf` 설정 파일을 기록하고 모든 개별 영역 파일을 `/var/named` 디렉토리에 기록한 후 데몬이 설정 파일을 다시 읽어오도록 풀다운 메뉴에서 **지장** 버튼을 클릭하시기 바랍니다.

이러한 설정으로 인해 `/etc/named.conf` 파일에 다음과 같은 엔트리가 생성됩니다:

```
zone "10.168.192.in-addr.arpa" {
    type master;
    file "10.168.192.in-addr.arpa.zone";
};
```

이 설정은 또한 다음에 나온 정보를 사용하여 `/var/named/10.168.192.in-addr.arpa.zone` 파일을 생성합니다:

```
$TTL 86400
@   IN   SOA  ns.example.com. root.localhost (
          2 ; serial
          28800 ; refresh
          7200 ; retry
          604800 ; expire
          86400 ; ttk
          )


@   IN   NS   ns2.example.com.

1   IN   PTR  one.example.com.
```

```
2   IN   PTR  two.example.com.
```

21.3. 슬레이브 영역 추가하기

2차 마스터로도 알려진 슬레이브 영역을 추가하시려면, **추가** 버튼을 클릭하신 후 **슬레이브 영역**을 선택해 주십시오. 아래에 위치한 **도메인명** 텍스트 입력란에 슬레이브 영역의 도메인명을 입력하시기 바랍니다.

그림 21-4에서 보이는 것처럼 새로운 창이 열리며 다음과 같이 옵션이 나타날 것입니다:

- **이름** — 이전 창에서 방금 입력하신 도메인명.
- **마스터 목록** — 슬레이브 영역이 데이터를 검색할 네임 서버. 텍스트 입력란에 숫자와 점 (.)으로 이루어진 올바른 형식의 IP 주소를 입력해 주셔야 합니다.
- **파일명** — /var/named와 관련된 DNS 데이터베이스 파일의 파일명.

그림 21-4. 슬레이브 영역 추가하기

슬레이브 영역의 설정을 마치셨다면, **확인** 버튼을 클릭하여 그림 21-1에 나온 주요 창으로 되돌아 가십시오. /etc/named.conf 설정 파일을 기록하고 모든 개별 영역 파일을 /var/named 디렉토리에 기록한 후 데몬이 설정 파일을 다시 읽어오도록 풀다운 메뉴에서 **저장** 버튼을 클릭하시기 바랍니다.

이러한 설정으로 인해 /etc/named.conf 파일에 다음과 같은 엔트리가 생성됩니다:

```
zone "slave.example.com" {
    type slave;
    file "slave.example.com.zone";
    masters {
        1.2.3.4;
        };
};
```

named 서비스가 마스터 서버로부터 영역 데이터를 다운로드 받는 동안 /var/named/slave.example.com.zone 설정 파일이 생성됩니다.

22장 . 인증 설정

사용자가 Red Hat Linux 시스템에 로그인할 때, 사용자명과 암호가 올바르고 활성화된 사용자로 검증, 즉 인증되어야 합니다. 가끔씩 로컬 시스템에 저장된 정보를 이용하여 사용자를 검증할 경우도 있고 다른 경우에는 원격 컴퓨터에 위치한 사용자 데이터베이스를 이용하여 인증을 수행합니다.

인증 설정 도구는 사용자 정보 검색 및 LDAP, Kerberos와 SMB를 인증 프로토콜로 설정하도록 NIS, LDAP과 Hesiod를 설정하는데 사용됩니다.

알림

설치 과정에서 또는 **보안 수준 설정 도구**를 사용하여 중간 수준이나 최상위 수준으로 설정하셨다면 (또는 **GNOME Lokkit** 프로그램을 사용하여 최상위 또는 하위 수준을 설정하셨다면), NIS와 LDAP과 같은 네트워크 인증 방식은 방화벽 통과가 허용되지 않습니다.

이 장에서는 여러 다른 인증 방식을 자세하게 설명하지 않습니다. 대신, **인증 설정 도구**를 사용하여 여러 인증 방식을 설정하는 방법에 대하여 설명하고 있습니다.

데스크탑에서 그래픽 버전의 **인증 설정 도구**를 시작하시려면, 패널에서 **주 메뉴 버튼** => **시스템 설정** => **인증**을 선택하시거나 **쉘** 프롬프트 (예, **XTerm** 또는 **GNOME 터미널**)에서 `authconfig-gtk` 명령을 입력하시면 됩니다. 텍스트 기반 버전을 시작하시려면, **쉘** 프롬프트에서 `authconfig` 명령을 입력하십시오.

중요

인증 프로그램을 종료하시면, 변경 사항이 즉시 적용될 것입니다.

22.1. 사용자 정보

사용자 정보 탭에는 여러 가지 옵션이 있습니다. 옵션을 활성화하시려면, 옵션 옆에 위치한 빈 체크박스를 선택하시면 됩니다. 옵션을 비활성화하려면, 체크박스를 다시 클릭하여 선택된 것을 해제하시면 됩니다. **확인** 버튼을 클릭하여 프로그램을 종료하고 변경사항을 저장하십시오.

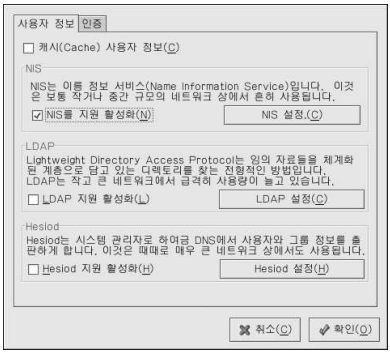

그림 22-1. 사용자 정보

다음 목록에서는 각 옵션 설정 사항에 대하여 설명하고 있습니다:

- **캐시 사용자 정보** — 이 옵션을 선택하시면 이름 서비스 캐시 데몬 (nscd)이 활성화되며 부팅시 시작됩니다.

  이 옵션을 사용하시려면, `nscd` 패키지를 설치하셔야 합니다.

- **NIS 지원 활성화** — 이 옵션을 선택하시면 사용자와 암호 인증을 위해 NIS 서버에 접속하도록 시스템을 NIS 클라이언트로 설정합니다. **NIS 설정** 버튼을 클릭하여 NIS 도메인과 NIS 서버를 지정해 주십시오. NIS 서버가 지정되지 않으면, 데몬은 브로드캐스팅을 통하여 NIS 서버를 검색 시도합니다.

  이 옵션이 작동하기 위해서는 `ypbind` 패키지가 설치되어 있어야 합니다. NIS 지원이 활성화되면, `portmap`과 `ypbind` 서비스가 시작되며 부팅시에도 시작됩니다.

- **LDAP 지원 활성화** — LDAP을 통하여 사용자 정보를 검색하도록 시스템을 설정하시려면 이 옵션을 선택하시기 바랍니다. **LDAP 설정** 버튼을 클릭하여 **LDAP 검색 기반 DN**과 **LDAP 서버**를 지정해 주십시오. 만일 **TLS를 이용하여 접속을 암호화함**을 선택하시면, LDAP 서버로 보낼 암호를 TLS (Transport Layer Security)를 이용하여 암호화합니다.

  이 옵션이 작동하려면 `openldap-clients` 패키지가 설치되어야 합니다.

  LDAP과 관련된 보다 자세한 정보를 원하신다면, *Red Hat Linux* 참조 가이드를 참조하시기 바랍니다.

- **Hesiod 지원 활성화** — 사용자 정보를 필요한 정보를 원격 Hesiod 데이터베이스에서 검색하도록 시스템을 설정하시려면 이 옵션을 선택하시기 바랍니다.

  `hesiod` 패키지를 설치하셔야 합니다.

22.2. 인증

인증 탭에서는 네트워크 인증 방식을 설정하실 수 있습니다. 옵션을 활성화하시려면, 옵션 옆에 위치한 빈 체크박스를 클릭하시면 됩니다. 옵션을 비활성화 하시려면, 선택된 체크박스를 선택 해제하도록 다시 클릭하시면 됩니다.

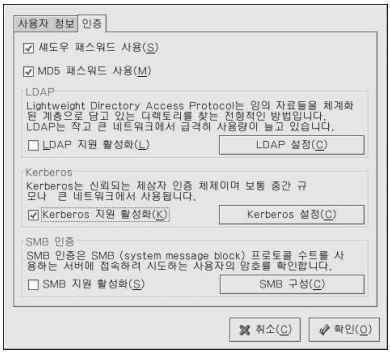

그림 22-2. 인증

다음은 각 옵션 설정 사항에 대하여 설명합니다:

- **새도우 암호 사용** — `/etc/passwd` 파일 대신 `/etc/shadow` 파일에 암호를 새도우 암호 형식으로 저장하시려면, 이 옵션을 선택하시기 바랍니다. 설치 과정에서 새도우 암호가 디폴트로 활성화되며, 시스템 보안 증가를 위해 새도우 암호 사용을 권장합니다.

  이 옵션이 작동하려면 `shadow-utils` 패키지가 설치되어 있어야 합니다. 새도우 암호에 대한 보다 자세한 정보는 *Red Hat Linux* 참조 가이드에서 사용자와 그룹 장을 참조하시기 바랍니다.

- **MD5 암호 사용하기** — 이 옵션을 선택하시면, 8 글자 이하로 구성된 표준 암호 대신 256자 까지의 긴 암호를 사용할 수 있게 해주는 MD5 암호를 사용합니다. 이 옵션은 설치 과정에서 디폴트로 활성화되며, 보안 증가를 위하여 적극 권장됩니다.

- **LDAP 지원 활성화** — 표준 PAM이 활성화된 응용 프로그램에서 LDAP을 사용하여 인증하도록 설정하는 옵션입니다. **LDAP 설정** 버튼을 클릭하신 후, 다음과 같은 옵션을 지정해 주십시오:

  - **TLS를 이용하여 접속을 암호화함** — TLS (Transport Layer Security)를 사용하여 LDAP 서버로 보낼 접속을 암호화합니다.
  - **LDAP 검색 기반 DN** — DN (Distinguished Name)에 따라 사용자 정보를 검색합니다.
  - **LDAP 서버** — LDAP 서버의 IP 주소를 지정합니다.

  이 옵션이 작동하려면 `openldap-clients` 패키지가 설치되어 있어야 합니다. LDAP에 대한 보다 자세한 정보는 *Red Hat Linux* 참조 가이드를 참조하시기 바랍니다.

- **Kerberos 지원 활성화** — Kerberos 인증을 활성화하시려면 이 옵션을 선택하십시오. **Kerberos 설정** 버튼을 클릭하여 다음과 같은 정보를 설정하시기 바랍니다:

  - **관리 영역** — Kerberos 서버의 관리 영역을 설정합니다. 관리 영역이란 Kerberos를 사용하는 네트워크로서, 한 개 이상의 KDC와 여러 많은 클라이언트로 구성됩니다.
  - **KDC** — Kerberos 티켓을 분배하는 서버인, 키 분배 센터 (KDC)를 정의합니다.
  - **관리 서버** — `kadmind`를 실행하는 관리 서버를 지정합니다.

  이 옵션이 작동하려면 `krb5-libs` 패키지와 `krb5-workstation` 패키지가 설치되어 있어야 합니다. Kerberos에 대한 보다 자세한 정보는 *Red Hat Linux* 참조 가이드를 참조하시기 바랍니다.

- **SMB 지원 활성화** — 이 옵션은 SMB 서버를 사용하여 사용자를 인증하도록 PAM을 설정합니다. **SMB 설정** 버튼을 클릭하여 다음과 같은 옵션을 지정해 주십시오:

  - **작업그룹** — 사용할 SMB 작업그룹을 지정해 주십시오.
  - **도메인 제어기** — 사용할 SMB 도메인 제어기를 지정하십시오.

22.3. 명령행 버전

인증 설정 도구는 인터페이스 없이 명령행 도구로도 실행 가능합니다. 명령행 버전은 설정 스크립트나 킥스타트 스크립트에서 사용할 수 있습니다. 인증 옵션은 표 22-1에 요약되어 있습니다.

옵션	설명
`--enableshadow`	섀도우 암호 활성화
`--disableshadow`	섀도우 암호 비활성화
`--enablemd5`	MD5 암호 활성화
`--disablemd5`	MD5 암호 비활성화
`--enablenis`	NIS 활성화
`--disablenis`	NIS 비활성화
`--nisdomain=<`*`domain`*`>`	NIS 도메인 지정
`--nisserver=<`*`server`*`>`	NIS 서버 지정
`--enableldap`	사용자 정보를 인증하는데 LDAP을 사용
`--disableldap`	사용자 정보를 인증하는데 LDAP을 사용하지 않음
`--enableldaptls`	LDAP에 TLS를 사용함
`--disableldaptls`	LDAP에 TLS를 사용하지 않음
`--enableldapauth`	인증에 LDAP을 사용함
`--disableldapauth`	인증에 LDAP을 사용하지 않음
`--ldapserver=<`*`server`*`>`	LDAP 서버 지정
`--ldapbasedn=<`*`dn`*`>`	LDAP 기반 DN 지정
`--enablekrb5`	Kerberos 활성화
`--disablekrb5`	Kerberos 비활성화
`--krb5kdc=<`*`kdc`*`>`	Kerberos KDC 지정
`--krb5adminserver=<`*`server`*`>`	Kerberos 관리 서버 지정
`--krb5realm=<`*`realm`*`>`	Kerberos 관리 영역 지정
`--enablesmbauth`	SMB 활성화
`--disablesmbauth`	SMB 비활성화
`--smbworkgroup=<`*`workgroup`*`>`	SMB 작업그룹 지정
`--smbservers=<`*`server`*`>`	SMB 서버 지정
`--enablehesiod`	Hesiod 활성화
`--disablehesiod`	Hesiod 비활성화
`--hesiodlhs=<`*`lhs`*`>`	Hesiod LHS 지정
`--hesiodrhs=<`*`rhs`*`>`	Hesiod RHS 지정
`--enablecache`	`nscd` 활성화
`--disablecache`	`nscd` 비활성화

옵션	설명
`--nostart`	`portmap`, `ypbind`, 또는 `nscd` 서비스가 설정되어 있어도, 이 서비스들을 시작하거나 멈추지 않음
`--kickstart`	사용자 인터페이스를 표시하지 않음
`--probe`	네트워크 디폴트를 검색하여 표시

표 22-1. 명령행 옵션

힌트

이 옵션들은 `authconfig` 메뉴얼 페이지나 쉘 프롬프트에서 `authconfig --help`를 입력하여 찾아보실 수 있습니다.

메일 전송 에이전트 (MTA) 설정

메일 전송 에이전트 (MTA)는 Red Hat Linux 시스템에서 이메일을 보내는데 사용되는 필수 응용 프로그램입니다. **Evolution**, **Mozilla Mail**, **Mutt**와 같은 메일 사용자 에이전트 (MUA)는 이메일을 읽고 작성하는데 사용됩니다. 사용자가 MUA로부터 이메일을 보내면, 메시지는 MTA로 보내지며, 그 메시지가 목적지에 도달할 때까지 MTA 사이에서 연속적으로 전달됩니다.

사용자가 이메일을 보내려는 계획이 없다고 하여도, 일부 자동화 작업이나 시스템 프로그램은 `/bin/mail` 명령어를 사용하여 로컬 시스템의 루트 사용자에게 로그 메시지를 포함한 이메일을 보내는 작업을 수행합니다.

Red Hat Linux 9는 두가지 종류의 MTA: Sendmail과 Postfix를 제공합니다. 두가지 모두 설치된 경우, `sendmail`이 기본 MTA 입니다. 만일 기본 MTA를 변경하시려면, **메일 전송 에이전트 변환기**를 사용하여 `sendmail` 이나 `postfix`를 선택하실 수 있습니다.

텍스트 버전 **메일 전송 에이전트 변환기** 프로그램을 사용하시려면 `redhat-switch-mail` RPM 패키지를 설치하셔야 합니다. 그래픽 버전을 사용하시려면, `redhat-switch-mail-gnome` 패키지를 설치하시기 바랍니다. RPM 패키지를 설치하는 방법에 대한 보다 자세한 정보는 V 부을 참조하시기 바랍니다.

메일 전송 에이전트 변환기를 시작하시려면, 패널에서 **주 메뉴 버튼** => **기타 응용 프로그램** => **시스템 도구** => **메일 전송 에이전트 변환기**를 선택하시거나, 또는 쉘 프롬프트 (예, XTerm 혹은 GNOME 터미널)에서 `redhat-switch-mail` 명령을 입력하시면 됩니다.

프로그램은 자동으로 X 윈도우 시스템이 실행되는지 여부를 알아냅니다. 만일 X 윈도우 시스템이 실행 중이라면, 프로그램은 그림 23-1에서 보여진 것처럼 그래픽 모드로 시작할 것입니다. 만일 X 윈도우 시스템이 실행되지 않는 경우, 프로그램은 텍스트 모드로 시작합니다. **메일 전송 에이전트 변환기**가 텍스트 모드에서 시작되도록 하시려면, `redhat-switch-mail-nox` 명령을 사용하시기 바랍니다.

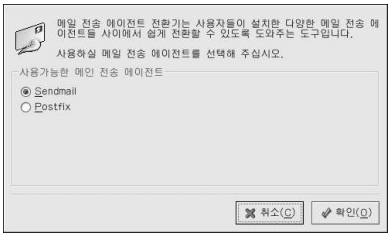

그림 23-1. 메일 전송 에이전트 변환기

MTA를 변경하기 위해 **확인** 버튼을 누르시면, 선택된 메일 데몬이 부팅시 시작되도록 활성화되며, 선택되지 않은 메일 데몬은 부팅시 시작되지 않도록 비활성화될 것입니다. 선택된 메일 데몬이 시작되고 다른 데몬은 정지됩니다; 따라서 변경 사항이 즉시 효력을 발생합니다.

이메일 프로토콜과 MTA에 관한 보다 많은 정보를 원하신다면, *Red Hat Linux* 참조 가이드를 참조하시기 바랍니다. MUA에 관한 보다 많은 정보는 *Red Hat Linux* 시작하기 가이드에서 찾으실 수 있습니다.

IV. 시스템 설정

콘솔 액세스와 Red Hat Linux 시스템에서 소프트웨어와 하드웨어 정보를 가져오는 방법에 대해 설명한 후, 이 장에서는 일반 시스템 설정 작업에 대하여 설명해 보겠습니다.

차례

24장 . 콘솔 사용하기

루트가 아닌 일반 사용자가 로컬 컴퓨터에 로그인할 때, 다음과 같은 두가지 유형의 특별 허가가 주어집니다:

1. 실행할 수 없었던 특정 프로그램들을 실행할 수 있게 해주는 허가.
2. 사용할 수 없었던 특정 파일들 (일반적으로 디스켓, CD-ROM과 같은 장치에 접근하는데 사용되는 특정 장치 파일들)을 사용할 수 있게 해주는 허가.

한 컴퓨터에는 다중 콘솔이 존재하기 때문에 많은 사용자들이 동시에 컴퓨터에 로컬로서 로그인 가능합니다. 따라서 사용자 중 한 명이 파일에 더욱 빨리 접근하기 위한 경주에서 "이겨야만" 합니다. 콘솔에 가장 먼저 로그인한 사용자가 그 파일들을 소유할 수 있습니다. 일단 첫번째 사용자가 로그 아웃하면, 다음으로 로그인한 사용자가 그 파일을 소유할 수 있습니다.

이와는 반대로 콘솔에 로그인한 모든 사용자는 일반적으로 루트 사용자에게만 제한된 작업을 수행하는 프로그램을 실행할 수 있게 됩니다. X가 실행 중인 경우 이러한 작업들은 그래픽 사용자 인터페이스에 있는 메뉴 항목에 포함될 수 있습니다. 콘솔 접근 가능한 프로그램에는 `halt`, `poweroff` 와 `reboot`이 있습니다.

24.1. Ctrl-Alt-Del을 통한 시스템 종료 금지하기

디폴트 값으로, `/etc/inittab`는 콘솔에서 [Ctrl]-[Alt]-[Del] 키 조합이 사용되면 시스템을 셧다운하고 재부팅하도록 지정하고 있습니다. 이 기능을 완전히 비활성화하시려면, `/etc/inittab` 파일에서 다음에 나온 줄 앞에 해시 표시 (#)를 넣음으로서 주석 처리하셔야 합니다:

```
ca::ctrlaltdel:/sbin/shutdown -t3 -r now
```

또한 루트가 아닌 사용자들이 콘솔에서 [Ctrl]-[Alt]-[Del] 키조합을 사용하여 시스템을 종료할 수 있도록 설정도 가능합니다. 제한된 특정 사용자에게만 이러한 권리를 허용하시려면, 다음과 같은 단계를 따르십시오:

1. 앞에서 언급된 `/etc/inittab` 줄에 다음과 같이 `-a` 옵션을 추가하십시오:
   ```
   ca::ctrlaltdel:/sbin/shutdown -a -t3 -r now
   ```
   `-a` 플래그는 `shutdown` 명령으로 하여금 `/etc/shutdown.allow` 파일을 찾도록 지시합니다. 다음 단계에서는 이 파일을 생성하는 방법에 대한 설명이 나와 있습니다.
2. `/etc` 디렉토리에 `shutdown.allow`라는 이름의 파일을 생성합니다. `shutdown.allow` 파일에는 [Ctrl]-[Alt]-[Del] 키조합을 사용하여 시스템을 종료할 수 있는 사용자의 목록을 입력하셔야 합니다. `/etc/shutdown.allow` 파일의 형식은 다음과 같이 사용자명이 한 줄당 한 개씩 나타납니다:
   ```
   stephen
   jack
   sophie
   ```

이 `shutdown.allow` 예시 파일에 따르면 stephen, jack, sophie라는 사용자는 콘솔에서 [Ctrl]-[Alt]-[Del] 키조합을 사용하여 시스템을 셧다운할 수 있습니다. 만일 사용자가 콘솔에서 시스템을 종료하기 위하여 이 키조합을 사용한다면, `/etc/inittab` 파일의 `shutdown -a` 명령은 `/etc/shutdown.allow` 파일에 기재된 사용자들 (또는 루트) 중 가상 콘솔에 로그인한 사용자가 있는 지 확인합니다. 만일 그 중 한 명이라면, 시스템 종료를 계속 진행합니다; 만일 아니라면, 대신 시스템 콘솔에 오류 메시지가 나타날 것입니다.

`shutdown.allow` 파일에 대한 보다 많은 정보를 원하신다면, `shutdown` 메뉴얼 페이지를 참조하시기 바랍니다.

24.2. 콘솔 프로그램 사용 금지하기

다른 사용자가 콘솔 프로그램을 사용하지 못하도록 하시려면, 여러분은 루트로 다음과 같은 명령을 실행하셔야 합니다:

```
rm -f /etc/security/console.apps/*
```

콘솔이 보안된 환경에서 (예, BIOS 암호와 부트로더 암호를 설정하고, [Ctrl]-[Alt]-[Delete] 키조합을 사용하는 것이 금지되면, 전원과 복구 스위치가 비활성화된 안전한 환경에서), 사용자가 콘솔에서 `poweroff`, `halt`, `reboot` 명령을 실행하는 것을 원하지 않으실 것입니다.

이러한 권한을 제거하기 위해서는, 루트로 다음의 명령을 실행하십시오:

```
rm -f /etc/security/console.apps/poweroff
rm -f /etc/security/console.apps/halt
rm -f /etc/security/console.apps/reboot
```

24.3. 콘솔 사용 금지하기

PAM `pam_console.so` 모듈은 콘솔 파일 허가와 인증을 관리합니다. (PAM을 설정하는 방법에 대한 보다 많은 정보를 원하신다면, *Red Hat Linux* 참조 가이드를 참조하시기 바랍니다.) 만일 프로그램과 파일 사용을 포함한 모든 콘솔 접근 활동을 금지하시려면, `/etc/pam.d` 디렉토리에서 `pam_console.so`을 언급한 줄을 모두 주석 처리하시기 바랍니다. 루트로 가셔서 다음과 같은 스크립트를 사용하시면 도움이 될 것입니다:

```
cd /etc/pam.d
for i in * ; do
sed '/[^#].*pam_console.so/s/^/#/' < $i > foo && mv foo $i
done
```

24.4. 콘솔 정의하기

`pam_console.so` 모듈은 `/etc/security/console.perms` 파일을 사용하여 시스템 콘솔에서 사용자들에 대한 허가권을 결정합니다. 이 파일의 구문에는 매우 융통성이 있습니다; 따라서 여러분은 이 파일을 편집하여 사용자에 대한 허가권이 더 이상 적용되지 않도록 하실 수도 있습니다. 하지만 기본 파일에는 다음과 같은 줄이 포함됩니다:

```
<console>=tty[0-9][0-9]* :[0-9]\.[0-9] :[0-9]
```

사용자가 로그인하면 그 사용자는 `:0` 혹은 `mymachine.example.com:1.0`라고 이름 붙은 X 서버나 `/dev/ttyS0` 또는 `/dev/pts/2`라고 지명된 장치와 같은 터미널에 접속됩니다. 디폴트 값으로, 로컬 가상 콘솔과 로컬 X 서버가 로컬로 간주되도록 정의되어 있지만, 만일 `/dev/ttyS1` 포트의 시리얼 터미널도 로컬로 만드시려면, 해당 줄은 다음과 같이 변경하실 수 있습니다:

```
<console>=tty[0-9][0-9]* :[0-9]\.[0-9] :[0-9] /dev/ttyS1
```

24.5. 콘솔에서 파일 사용 가능하도록 설정하기

`/etc/security/console.perms` 파일을 보시면 다음과 같은 부분이 있습니다:

```
<floppy>=/dev/fd[0-1]* \
    /dev/floppy/* /mnt/floppy*
<sound>=/dev/dsp* /dev/audio* /dev/midi* \
   /dev/mixer* /dev/sequencer \
```

```
    /dev/sound/* /dev/beep
<cdrom>=/dev/cdrom* /dev/cdroms/* /dev/cdwriter* /mnt/cdrom*
```

필요한 경우 여러분이 직접 이 부분에 줄을 첨가하실 수 있습니다. 첨가하신 라인이 적절한 장치를 언급하고 있는지 확인해 주십시오. 예로 들면, 다음과 같은 라인을 첨가하실 수 있습니다:

```
<scanner>=/dev/scanner /dev/usb/scanner*
```

(물론 위와 같은 라인에서 `/dev/scanner`가 하드 드라이브를 지칭한다거나 하는 실수는 저지르지 마십시오. 여러분이 가지고 계신 스캐너가 맞는지 확인해 주셔야 합니다.)

이제 첫번째 단계는 마쳤습니다. 두번째 단계에서는 이 파일들을 사용하여 무엇을 할 것인가를 정의해 주셔야 합니다. `/etc/security/console.perms` 파일의 마지막에서 다음과 유사한 부분을 찾아보십시오:

```
<console> 0660 <floppy> 0660 root.floppy
<console> 0600 <sound> 0640 root
<console> 0600 <cdrom> 0600 root.disk
```

그리고 다음과 같은 라인을 첨가하십시오:

```
<console> 0600 <scanner> 0600 root
```

이제 여러분이 콘솔에 로그인하시면 `/dev/scanner` 장치에 대한 소유권과 0600 (오직 여러분만 읽기 쓰기 가능) 허가가 주어질 것입니다. 여러분이 로그 아웃하시면, 그 장치는 루트가 소유하게 되지만 0600 허가 (이제: 오직 루트만 읽기 쓰기 가능)는 바뀌지 않습니다.

24.6. 콘솔에서 다른 응용 프로그램을 사용 가능하도록 설정하기

만일 콘솔 사용자들이 다른 응용 프로그램을 사용할 수 있도록 설정하기 위해서는, 더 많은 작업이 필요합니다.

우선 콘솔 사용자는 오직 `/sbin` 또는 `/usr/sbin`에 존재하는 응용 프로그램만 사용 가능합니다. 따라서 이 두 파일에 여러분이 실행하시려는 응용 프로그램이 포함되어 있는지를 확인하신 후에 다음의 단계를 따르시기 바랍니다:

1. 응용 프로그램의 이름 (예, *`foo`* 프로그램)에서 `/usr/bin/consolehelper` 응용 프로그램으로의 링크를 생성해 주십시오:
   `cd /usr/bin`
   `ln -s consolehelper` *`foo`*
2. `/etc/security/console.apps/`*`foo`* 파일을 생성하십시오:
   `touch /etc/security/console.apps/`*`foo`*
3. `/etc/pam.d/` 내의 *`foo`* 서비스에 사용될 PAM 설정 파일을 만드십시오. 정지(halt) 서비스의 PAM 설정 파일을 복사하여 쉽게 PAM 설정 파일을 만드실 수 있습니다. 복사본을 이용하여 PAM 설정 파일을 만드신 후 필요한 경우 파일을 수정하시면 됩니다:
   `cp /etc/pam.d/halt /etc/pam.d/foo`

이제 `/usr/bin/`*`foo`*를 실행하시면 `consolehelper` 명령어가 호출되며 이 명령어는 `/usr/sbin/userhelper`의 도움을 받아 사용자를 인증합니다. `/etc/pam.d/halt`의 복사본을 사용하여 `/etc/pam.d/`*`foo`*를 만드신 경우, 사용자 인증을 위하여 사용자 암호를 요청합니다. (그렇지 않다면, `/etc/pam.d/`*`foo`*에 지정된 사항을 정확히 따를 것입니다.) 그 후 루트 허가를 가지고 `/usr/sbin/`*`foo`*를 실행합니다.

PAM 설정 파일에서 응용 프로그램이 *pam_timestamp* 모듈을 사용하여 로그인을 비롯한 모든 시스템 인증을 기록 (캐시)하도록 설정 가능합니다. 응용 프로그램이 시작되고 적절한 인증 (루트 암호)가 제공되면, 시간 기록 (time stamp) 파일이 생성됩니다. 성공적으로 로그인된 인증 정보는 5분간 캐시되도록 기본 설정되어 있습니다. 따라서 이 5분 동안에 `pam_timestamp`를 사용하도록 설정된 다른 응용 프로그램이 동일한 세션에서 실행된다면, 해당 사용자로 자동 인증됩니다. — 즉, 사용자는 루트 암호를 다시 입력할 필요가 없습니다.

이 모듈은 pam 패키지에 포함되어 있습니다. 이 기능을 사용하시려면, etc/pam.d/의 PAM 설정 파일에 다음과 같은 줄을 포함하셔야 합니다:

```
auth sufficient /lib/security/pam_timestamp.so
session optional /lib/security/pam_timestamp.so
```

auth로 시작하는 첫번째 줄은 반드시 그 외 다른 auth sufficient 줄 다음에 위치해야 하며, session로 시작하는 줄은 다른 session optional 줄 마지막에 입력하셔야 합니다.

pam_timestamp를 사용하도록 설정된 응용 프로그램이 패널 상의 **주 메뉴 버튼**에서 성공적으로 인증된다면, GNOME 데스크탑 환경을 실행 중이신 경우  아이콘이 패널의 알림 영역에 나타납니다. 인증이 만료된 후 (기본 값 5분이 지나면), 아이콘이 사라질 것입니다.

아이콘에 클릭하신 후 인증을 기억하지 않기 옵션을 선택하시면 캐시된 인증을 기억하지 않도록 설정하실 수 있습니다.

24.7. floppy 그룹

어떤 이유에서든지 여러분이 콘솔을 적절히 사용할 수가 없는 경우, 루트가 아닌 사용자가 디스켓 드라이브를 사용할 수 있도록 허용하시려면 floppy 그룹을 사용하십시오. 단순히 원하시는 도구를 사용하여 floppy 그룹에 그 사용자를 추가하시면 됩니다. 예를 들어 다음과 같이 gpasswd 명령을 사용자 fred를 floppy 그룹에 추가하실 수 있습니다:

```
[root@bigdog root]# gpasswd -a fred floppy
Adding user fred to group floppy
[root@bigdog root]#
```

이제 사용자 fred는 콘솔에서 시스템의 디스켓 드라이브로 접근할 수 있습니다.

사용자와 그룹 설정

사용자 관리 도구는 로컬 사용자와 그룹을 보고, 수정, 추가하고 삭제하는데 사용됩니다.

사용자 관리 도구를 사용하시려면, X 윈도우 시스템이 실행 중이며 루트 권한이 있어야 하고, 또한 `redhat-config-users` RPM 패키지가 설치되어 있어야 합니다. 데스크탑에서 **사용자 관리 도구**를 실행하시려면 패널에서 **주 메뉴 버튼** => **시스템 설정** => **사용자와 그룹**을 선택하십시오. 또는 XTerm이나 GNOME 터미널과 같은 쉘 프롬프트 상에서 `redhat-config-users` 명령을 입력하시면 됩니다.

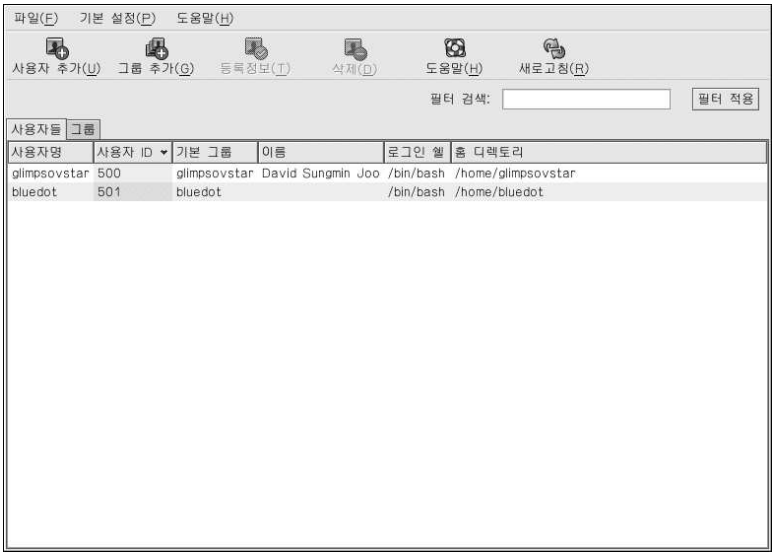

그림 25-1. Red Hat 사용자 관리자

시스템 상 모든 로컬 사용자의 목록을 보기 위해서는 **사용자** 탭을 클릭하십시오. 시스템 상 모든 로컬 그룹의 목록을 보시려면, **그룹** 탭을 클릭하십시오.

특정 사용자 혹은 그룹을 찾으실 경우에는 **필터 검색** 부분에 이름의 첫 부분 및 글자를 입력하십시오. 그 후 [Enter] 키를 누르거나 **필터 적용** 버튼을 누르시면 선별된 목록이 나타날 것입니다.

사용자와 그룹을 정렬하기 위해서는, 행 이름에 클릭하십시오. 사용자와 그룹 목록은 행의 값에 따라 정렬될 것입니다.

Red Hat Linux는 500 이하의 사용자 ID는 시스템 사용자를 위해 확보해 둡니다. **사용자 관리 도구**는 시스템 사용자를 보여주지 않도록 기본 설정되어 있습니다. 시스템 사용자를 포함한 모든 사용자를 보시려면 **기본 설정** => 풀다운 메뉴에서 **시스템 사용자와 그룹들을 거르기** 항목을 선택 해제하십시오.

사용자와 그룹에 대한 추가 정보는 *Red Hat Linux* 참조 가이드와 *Red Hat Linux* 시스템 관리 입문서에서 찾으실 수 있습니다.

25.1. 새로운 사용자 추가하기

새로운 사용자를 추가하기 위해서는 **사용자 추가** 버튼을 클릭하십시오. 그림 25-2에서 보이는 창이 나타날 것입니다. 새로운 사용자를 위한 사용자명과 암호를 적절한 항목에 입력하시기 바랍니다. 사용자의 암호는 **암호**와 **암호 확인** 영역에 입력하시기 바랍니다. 암호는 최소한 6 글자 이상이어야 합니다.

힌트

사용자의 암호가 길면 길수록, 다른 사람이 그 암호를 추측하여 허가없이 그 사용자 계정으로 로그인하는 것이 더욱 힘들어 집니다. 또한 한 단어가 아닌 여러 문자, 숫자, 특수 기호로 이루어진 암호를 사용하시는 것이 좋습니다.

로그인 쉘을 선택하십시오. 만일 어떤 쉘을 선택할 지 확신이 서지 않는다면, `/bin/bash`의 기본 값을 수락합니다. 기본 홈 디렉토리는 `/home/`사용자명 *(username)* 입니다. 해당 사용자를 위해 생성된 홈 디렉토리를 변경 가능하며 또는 **홈 디렉토리 생성**을 선택 해제하여 홈 디렉토리를 만들지 않으셔도 됩니다.

홈 디렉토리를 생성하기로 선택하셨다면, 기본 설정 파일들이 `/etc/skel` 디렉토리에서 새로운 홈 디렉토리로 복사됩니다.

Red Hat Linux는 사용자 개인 그룹 *(User Private Group)* (UPG) 스키마를 사용합니다. UPG 스키마는 UNIX가 그룹을 처리하는 표준 방식과 그리 다르지 않습니다; 단지 새로운 방식을 제공할 뿐입니다. 새로운 사용자를 만드실 때마다, 그 사용자와 같은 이름을 지닌 고유 그룹이 기본으로 생성됩니다. 만일 이 그룹이 만들어지는 것을 원하지 않으시면 **이 사용자의 개인 그룹 생성**을 선택 해제하시면 됩니다.

새로운 사용자의 ID를 직접 지정하기 위해서는 **사용자 ID 수동으로 지정하기** 항목을 선택하시면 됩니다. 만일 이 옵션이 선택되지 않았다면, 숫자 500 이후 다음으로 사용 가능한 숫자가 사용자 ID로 사용됩니다. Red Hat Linux에서 500 이하의 사용자 ID는 시스템 사용자 용으로 보존됩니다.

확인 버튼을 클릭하여 사용자를 생성합니다.

그림 25-2. 새 사용자

암호 기한 만료와 같은 고급 사용자 등록 정보를 설정하기 위해서는, 사용자를 추가하신 후 그 사용자의 등록 정보를 수정하십시오. 보다 많은 정보를 원하신다면 25.2 절을 참조하시기 바랍니다.

사용자에게 더 많은 사용자 그룹을 추가하기 위해서는, **사용자** 탭을 클릭하고 해당 사용자를 선택하신 후 **등록정보**를 클릭합니다. **사용자 등록정보** 창에서 **그룹** 탭을 선택하시기 바랍니다. 그 사용자가 가입할 그룹들을 선택하시고, 그 사용자의 기본 그룹을 선택해 주십시오. 이제 **확인** 버튼을 클릭합니다.

25.2. 사용자 등록정보 수정하기

기존 사용자의 등록정보를 보기 위해서는 **사용자** 탭을 클릭하신 후 사용자 목록에서 해당 사용자를 선택합니다. 그리고 버튼 메뉴에서 **등록정보**를 클릭하십시오 (또는 풀-다운 메뉴에서 **파일** => **등록정보**를 선택하는 방법도 있습니다). 그림 25-3에서 보이는 창이 나타날 것입니다.

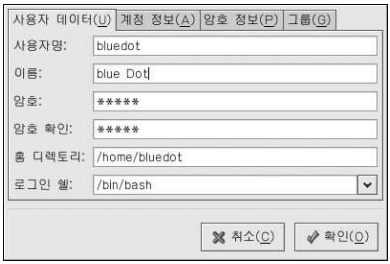

그림 25-3. 사용자 등록정보

사용자 등록정보 창은 여러 탭으로 이루어진 페이지로 나뉘어져 있습니다:

- **사용자 데이터** — 여러분이 사용자를 추가할 당시 설정된 사용자의 기본적인 정보입니다. 이 탭을 사용하여 사용자의 이름, 암호, 홈 디렉토리 또는 로그인 쉘을 변경하실 수가 있습니다.
- **계정 정보** — 계정이 특정 날짜에 만료되도록 하시려면 **계정 기한 만료 활성화** 버튼을 선택하십시오. 제공된 영역에 날짜를 입력하시기 바랍니다. 사용자가 시스템으로 로그인할 수 없도록 사용자 계정을 잠그기 위해서는 **사용자 계정 잠금**을 선택하십시오.
- **암호 정보** — 이 탭에서는 사용자가 마지막으로 암호를 변경한 날짜를 볼 수 있습니다. 일정 기간이 지나면 사용자가 암호를 바꾸도록 하기 위해서는, **암호 기한 만료 활성화**를 선택합니다. 또한 암호를 변경할 수 있는 기간을 설정하고, 암호를 변경하도록 사용자에게 경고를 보여줄 기간과 암호가 변경되지 않은 경우 몇일 후에 계정을 비활성화할 것인지 설정하실 수 있습니다.
- **그룹** — 사용자가 속할 그룹과 그 사용자의 기본 그룹을 선택합니다.

25.3. 새로운 그룹 추가하기

새로운 사용자 그룹을 추가하기 위해서는 **그룹 추가** 버튼을 클릭합니다. 그림 25-4와 유사하게 보이는 창이 나타날 것입니다. 생성할 새 그룹의 이름을 입력하십시오. 새 그룹에 대한 그룹 ID를 지정하기 위해서는, **그룹 ID 수동으로 지정하기** 버튼을 클릭하시고 GID를 선택합니다. Red Hat Linux에서 500 이하의 그룹 ID는 시스템 그룹 용으로 보존해 둡니다.

그룹을 생성하기 위해 **확인** 버튼을 누릅니다. 새 그룹이 그룹 목록에 나타날 것입니다.

그림 25-4. 새 그룹

그룹에 사용자를 추가하기 위해서는 25.4 절을 참조해 보십시오.

25.4. 그룹 등록정보 수정하기

기존 그룹의 등록정보를 보기 위해서는 그룹 목록에서 해당 그룹을 선택하신 후 버튼 메뉴에서 **등록정보** 버튼을 클릭하십시오. (또는 풀-다운 메뉴에서 **파일** => **등록정보**를 선택하는 방법도 있습니다) 그림 25-5와 같은 창이 나타날 것입니다.

그림 25-5. 그룹 등록정보

그룹 사용자 탭에서 그룹에 속한 사용자를 볼 수 있습니다. 다른 사용자를 선택하여 그룹에 추가하시고, 그룹에서 삭제할 사용자는 선택 해제하십시오. **확인** 버튼이나 **적용** 버튼을 클릭하여 변경 사항을 저장합니다.

25.5. 명령행 설정

명령행 도구 사용을 선호하시거나 X 윈도우 시스템이 설치되지 않은 경우, 이 장에서 명령행을 사용하여 사용자와 그룹을 설정하는 방법을 배워보시기 바랍니다.

25.5.1. 사용자 추가하기

시스템에 사용자를 추가하시려면:

1. `useradd` 명령을 사용하여 잠겨진 사용자 계정을 생성합니다:
   `useradd <username>`
2. `passwd` 명령을 사용하여 계정에 암호를 지정하고 암호 만료 기한을 설정하여 잠금을 해제합니다:
   `passwd <username>`

표 25-1에서 useradd 명령에 사용할 수 있는 명령행 옵션이 나와 있습니다.

옵션	설명
-c *comment*	사용자에 대한 설명
-d *home-dir*	디폴트 /home/*username* 디렉토리 대신 사용될 홈 디렉토리 지정
-e *date*	계정 만료 기한을 YYYY-MM-DD 날짜 형식으로 지정
-f *days*	암호가 만료된 후 계정이 만료될 때까지의 날짜수. (만일 **0**로 지정하시면, 암호가 완료되자 마자 계정이 비활성화 됩니다. 만일 **-1**로 지정하시면, 암호가 만료된 후에도 계정이 비활성화되지 않습니다.)
-g *group-name*	사용자 기본 그룹명 또는 그룹 번호 (반드시 기본 그룹이 존재해야 합니다.)
-G *group-list*	사용자가 속한 기본 그룹이 아닌 추가 그룹들의 이름과 번호 목록으로 각 그룹은 콤마로 구분됩니다. (그룹이 반드시 존재해야 합니다.)
-m	홈 디렉토리가 없다면 생성합니다
-M	홈 디렉토리를 생성하지 않음
-n	사용자에 대한 사용자 개인 그룹을 생성하지 않음
-r	홈 디렉토리가 없이 사용자 ID (UID) 500 이하의 시스템 계정을 생성함.
-p 암호 *(password)*	crypt로 암호화할 암호
-s	사용자 로그인 쉘, 디폴트는 /bin/bash
-u *uid*	사용자 ID. 499 보다 큰 숫자이며 유일한 숫자.

표 25-1. useradd 명령행 옵션들

25.5.2. 그룹 추가하기

시스템에 그룹을 추가하시려면, groupadd 명령을 사용하시기 바랍니다:

groupadd <*group-name*>

표 25-2에서 groupadd 명령에 사용되는 명령행 옵션 목록을 보실 수 있습니다.

옵션	설명
-g *gid*	그룹 ID, 499 보다 큰 숫자로서 유일한 숫자.
-r	500 이하의 GID를 가진 시스템 그룹을 생성.
-f	이미 그룹이 존재한다면 오류를 보이고 종료합니다. (그룹이 변경되지 않습니다.) 만일 -g 옵션과 -f 옵션이 지정된 경우 그룹이 이미 존재한다면, -g 옵션은 무시됩니다.

표 25-2. groupadd 명령행 옵션들

25.5.3. 암호 기한 만료

보안 상의 이유로, 사용자가 주기적으로 암호를 변경하도록 하는 것이 좋습니다. 이것은 **사용자 관리 도구**의 **암호 정보** 탭에서 사용자를 추가하거나 편집함으로서 가능합니다.

쉘 프롬프트에서 사용자에 대한 암호 만료 기한을 설정하시려면, chage 명령 다음에 표 25-3의 옵션과 사용자명을 함께 입력하시면 됩니다.

중요

chage 명령을 사용하기 위해서는 새도우 암호가 활성화되어야 합니다.

옵션	설명
`-m` *days*	사용자가 암호를 변경해야할 최소 날짜수를 지정합니다. 만일 값이 0 이라면, 암호는 만료되지 않습니다.
`-M` *days*	암호가 유효한 최대 날짜수를 지정합니다. 이 옵션에 의해 지정된 날짜수와 `-d` 옵션과 함께 지정된 날짜수를 더한 값이 현재 날짜보다 적다면, 계정을 사용하기 전에 암호를 변경해야 합니다.
`-d` *days*	1970년 1월 1일 이후로 암호가 마지막으로 변경된 날짜수를 지정합니다.
`-I` *days*	암호가 만료된 후 계정을 잠글 때까지 걸리는 비활성화 기간을 날짜수를 지정합니다. 만일 값이 0 이라면, 암호가 만기되어도 계정이 잠기지 않습니다.
`-E` *date*	계정이 잠길 날짜를 YYYY-MM-DD 형식으로 지정합니다. 1970년 1월 1일 이후 날짜수를 사용하는 것도 가능합니다.
`-W` *days*	암호가 만료되기 몇일 전에 사용자에게 경고할 것인지 지정합니다.

표 25-3. change 명령행 옵션

힌트

만일 chage 명령 다음에 아무런 옵션 없이 사용자명이 바로 사용된다면, 현재 암호 만기값이 보여지며 변경할 값을 요청합니다.

사용자가 첫 로그인시 암호를 설정하도록 하기 위해서는, 시스템 관리자는 사용자의 암호가 즉시 만료되도록 설정하셔야 합니다. 따라서 사용자는 처음 로그인하는 즉시 암호를 변경해야 합니다.

사용자가 처음으로 콘솔에 로그인할 때 암호를 설정하도록 강제하기 위해서는, 다음과 같은 절차를 따르십시오. 만일 사용자가 SSH 프로토콜을 사용하여 로그인 하였을 경우에는 이 방법이 작용하지 않습니다.

1. 사용자의 암호를 잠금 — 만일 사용자가 존재하지 않는다면, useradd 명령을 사용하여 사용자 계정을 생성합니다. 그러나 암호는 부여하지 않아 그 계정이 잠긴 상태로 남아있게 합니다.

   만일 암호가 이미 활성화되었다면, 다음 명령을 사용하여 계정을 잠그십시오:
   `usermod -L` *username*

2. 즉시 암호가 만료되도록 강제함 — 다음 명령을 입력하시면 됩니다:
   `chage -d 0` *username*

   이 명령은 1970년 1월 1일 이후로 암호가 마지막으로 변경된 날짜에 대한 값을 지정합니다. 이 값은 암호 기한 만료에 어떠한 법칙이 적용되든지에 상관없이 암호가 즉시 만료되도록 강제합니다.

3. 계정 잠금을 해제함 — 이 과정에는 두 가지 방법이 있습니다. 관리자가 초기 암호를 부여하는 방법과 암호를 입력하지 않고 공백으로 남겨두는 방법입니다.


경고

passwd 명령을 사용하여 암호를 설정하지 마십시오. 그 이유는 이 명령은 방금 설정하신 즉시 암호가 만료되도록 강제하는 설정을 사용할 수 없게 만들기 때문입니다.

초기 암호를 할당하시려면, 다음과 같은 과정을 따르시기 바랍니다:

- python 명령을 사용하여 명령행 python 해석기를 시작합니다. 다음과 같이 나타날 것입니다:
```
Python 2.2.2 (#1, Dec 10 2002, 09:57:09)
[GCC 3.2.1 20021207 (Red Hat Linux 8.0 3.2.1-2)] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>>
```
- 프롬프트에서 다음과 같은 명령을 입력하십시오 (여기서 *password* 부분은 암호화할 암호를 입력하시고 *salt*는 정확히 2 개의 대문자 또는 소문자 알파벳이나, 숫자, 점 (.), 기호, 또는 슬래시 (/) 기호를 함께 입력하시면 됩니다):
```
import crypt; print crypt.crypt("password","salt")
```
12CsGd8FRcMSM처럼 암호화된 암호가 출력될 것입니다.
- [Ctrl]-[D]를 눌러 Python 해석기를 종료합니다.
- 출력된 암호화된 암호를 다음 명령으로 앞 뒤 공간이 없이 정확히 복사하여 붙이기 합니다:
```
usermod -p "encrypted-password" username
```

초기 암호를 할당하는 대신, 다음 명령을 사용하여 암호를 입력하지 않고 빈 공간으로 남겨둘 수도 있습니다:
```
usermod -p "" username
```


주의

빈 암호를 사용하는 것이 사용자나 관리자 모두에게 편리하기는 하지만, 제3의 사용자가 먼저 로그인하여 시스템에 접근할 수 있다는 약간의 위험성이 있기는 합니다. 이러한 위험을 최소화하기 위해서는, 관리자가 계정을 잠금 해제할 시 로그인할 준비가된 사용자를 확인하는 것이 중요합니다.

다른 방법으로 사용자가 처음 로그인시, 새로운 암호를 요청할 수 있습니다.

25.6. 단계별 과정 설명

다음은 새도우 암호가 활성화된 시스템 상에서 useradd juan 명령을 입력시 어떠한 일이 일어나는지를 단계별로 설명하고 있습니다:

1. /etc/passwd 파일에 juan에 대한 새로운 라인이 생성됩니다. 이 라인에는 다음과 같은 문자가 포함됩니다:
   - 이 라인은 사용자명으로 시작됩니다. 예, juan.
   - 암호란에 시스템이 새도우 암호를 사용한다는 것을 보여주는 x 기호가 옵니다.
   - 500 이상의 UID (사용자 ID)가 생성됩니다. (500 이하의 Red Hat Linux UID와 GID는 시스템 사용자와 그룹 용으로 보존됩니다.)
   - 500 이상의 GID (그룹 ID)가 생성됩니다.
   - 옵션인 GECOS 정보는 공백으로 남아 있습니다.
   - 홈디렉토리는 /home/juan/로 설정됩니다.
   - 기본 쉘은 /bin/bash으로 설정됩니다.

2. /etc/shadow 파일에 juan에 대한 새 라인이 생성됩니다. 이 라인에는 다음과 같은 기호가 포함됩니다:

- 이 라인은 사용자명으로 시작됩니다. 예, juan.
- 계정을 잠그는 두 개의 느낌표 (!!)가 /etc/shadow 파일의 암호란에 나타납니다.

알림

만일 암호화된 암호가 -p 플래그를 사용하여 전달된다면, /etc/shadow 파일에서 해당 사용자를 위한 새 라인에 포함됩니다.

- 암호가 만료되지 않도록 설정됩니다.

3. /etc/group 파일에는 juan 그룹에 대한 새로운 라인이 생성됩니다. 사용자와 같은 이름을 가진 그룹은 사용자 개인 그룹 *(user private group)*이라고 부릅니다. 사용자 개인 그룹에 대한 보다 많은 정보를 원하신다면, 25.1 절을 참조하시기 바랍니다.

   /etc/group에 생성된 라인에는 다음과 같은 문자가 포함됩니다:

   - 이 라인은 그룹명으로 시작합니다. 예, juan.
   - 암호란에 시스템이 새도우 그룹 암호를 사용한다는 것을 보여주는 x 기호가 옵니다.
   - GID가 /etc/passwd 파일에서 juan 사용자에 대한 그룹 ID와 일치합니다.

4. /etc/gshadow 파일에 juan라는 그룹에 대한 새로운 라인이 생성됩니다. 이 라인에는 다음과 같은 문자가 포함됩니다:
   - 이 라인은 그룹명으로 시작됩니다. 예, juan.
   - 그룹을 잠그는 한 개의 느낌표 (!)가 /etc/gshadow 파일의 암호란에 나타납니다.
   - 그 외 모든 다른 영역은 빈 공간으로 남아 있습니다.

5. /home/ 디렉토리에는 사용자 juan에 대한 디렉토리가 생성됩니다. 이 디렉토리는 사용자 juan과 그룹 juan이 소유합니다. 그러나 오직 사용자 juan에 대한 읽기, 쓰기와 실행 권한을 갖습니다. 그 외 다른 허가는 주지 않습니다.
6. 디폴트 사용자 설정을 포함한 /etc/skel/ 디렉토리 내의 파일들은 새로운 /home/juan/ 디렉토리로 복사됩니다.

이제 juan라는 잠긴 계정이 시스템 상에 생성됩니다. 이 계정을 활성화하시려면, 관리자는 passwd 명령을 사용하여 계정에 암호를 부여하셔야 합니다. 옵션으로 암호 만료 기한을 설정하는 것도 가능합니다.

redhat.

26장 .

시스템 정보 모으기

시스템을 설정하는 방법에 대해서 배우시기에 앞서 먼저 기본적인 시스템 정보를 모으는 방법부터 배우셔야 합니다. 예로 들면, 여유 메모리 용량과 사용 가능한 하드 드라이브 공간의 용량을 알아내는 방법, 하드 드라이브 파티션 하는 방법과 실행되고 있는 프로세스 알아내는 방법 등에 대한 정보를 알아 두셔야 합니다. 이 장에서는 간단한 명령어를 사용하여 Red Hat Linux 시스템에서 이러한 유형의 정보를 검색하는 방법을 설명해 보겠습니다. 또한 여러분의 이해를 도울 일부 예시 프로그램도 포함시켰습니다.

26.1. 시스템 프로세스

`ps ax` 명령어를 사용하면, 현재 시스템 프로세스의 목록 (다른 사용자가 소유한 프로세스도 포함한 목록)을 보여줍니다. `ps aux` 명령어를 사용하여 프로세스와 그 프로세스의 소유자를 함께 볼 수 있습니다. 나타나는 목록은 정적 목록 입니다; 즉, 이 목록은 명령어가 입력되었을 당시 실행되던 프로세스의 스냅 사진이라고 할 수 있습니다. 만일 실행 중인 프로세스의 목록이 계속적으로 업데이트되기를 원하시면, 아래에서 설명된 `top` 명령어를 사용하십시오.

`ps` 명령의 출력 결과는 매우 길 수 있습니다. 화면이 빨리 지나가는 것을 방지하기 위하여 다음처럼 `less` 명령을 사용하십시오:

```
ps aux | less
```

`ps` 명령과 `grep` 명령을 사용하여 특정 프로세스의 실행 여부를 확인하실 수 있습니다. 예를 들어, 만일 **emacs** 프로그램이 실행 중인지 알아보기 위해서는 다음과 같은 명령을 사용합니다:

```
ps ax | grep emacs
```

`top` 명령어는 현재 실행되고 있는 프로세스와 메모리, CPU 사용량과 같은 중요한 정보를 함께 보여줍니다. 프로세스 목록은 실시간으로 업데이트되며 상호 대화식입니다. 다음은 `top` 명령어를 실행한 출력 결과의 한 예입니다:

```
 00:53:01 up 6 days, 14:05,  3 users,  load average: 0.92, 0.87, 0.71
71 processes: 68 sleeping, 2 running, 1 zombie, 0 stopped
CPU states: 18.0% user  0.1% system  16.0% nice  0.0% iowait 80.1% idle
Mem: 1030244k av, 985656k used,  44588k free,    0k shrd, 138692k buff
         424252k actv,  23220k in_d, 252356k in_c
Swap: 2040212k av, 330132k used, 1710080k free        521796k cached

  PID USER   PRI NI SIZE RSS SHARE STAT %CPU %MEM  TIME COMMAND
15775 joe    5  0 11028 10M 3192 S   1.5  4.2  0:46 emacs
14429 root   15  0 63620 62M 3284 R   0.5 24.7 63:33 X
17372 joe    11  0 1056 1056  840 R   0.5  0.4  0:00 top
17356 joe    2  0 4104 4104 3244 S   0.3  1.5  0:00 gnome-terminal
    1 root   0  0  544 544  476 S   0.0  0.2  0:06 init
    2 root   0  0    0   0    0 SW  0.0  0.0  0:00 kflushd
    3 root   1  0    0   0    0 SW  0.0  0.0  0:24 kupdate
    4 root   0  0    0   0    0 SW  0.0  0.0  0:00 kpiod
    5 root   0  0    0   0    0 SW  0.0  0.0  0:29 kswapd
  347 root   0  0  556 556  460 S   0.0  0.2  0:00 syslogd
  357 root   0  0  712 712  360 S   0.0  0.2  0:00 klogd
  372 bin    0  0  692 692  584 S   0.0  0.2  0:00 portmap
  388 root   0  0    0   0    0 SW  0.0  0.0  0:00 lockd
  389 root   0  0    0   0    0 SW  0.0  0.0  0:00 rpciod
  414 root   0  0  436 432  372 S   0.0  0.1  0:00 apmd
  476 root   0  0  592 592  496 S   0.0  0.2  0:00 automount
```

top 명령에서 빠져나가기 위해서는 [q] 키를 누릅니다.

다음은 top 명령어와 함께 사용할 수 있는 유용한 대화식 명령어 목록입니다:

명령어	설명
[Space]	즉시 화면을 재생합니다
[h]	도움말 화면을 보여줍니다.
[k]	프로세스를 강제 종료 (kill) 합니다. 종료할 프로세스 ID와 보낼 신호를 입력하셔야 합니다.
[n]	보여줄 프로세스의 수를 변경합니다. 보시려는 프로세스의 수를 입력하셔야 합니다.
[u]	사용자에 따라 목록 정렬
[M]	메모리 사용량에 따라 목록 정렬
[P]	CPU 사용량에 따라 CPU 목록 정렬

표 26-1. 대화식 top 명령어

힌트

Mozilla와 **Nautilus**와 같은 응용 프로그램은 스레드 인식 *(thread-aware)* — 다수의 사용자와 다중 요청을 처리하기 위하여 생성된 다중 스레드입니다. 각각의 스레드에는 프로세스 ID가 주어집니다. 기본 값으로 ps와 top 명령을 사용하시면 오직 주요 (초기) 스레드만을 볼 수 있습니다. 모든 스레드를 보시려면 ps -m 명령을 사용하시거나 top에서 [Shift]-[H] 키 조합을 누르시면 됩니다.

그래픽 인터페이스로 top 명령 결과를 보시려면 **GNOME 시스템 모니터**를 사용하십시오. 데스크탑에서 시작하려면 패널에서 **메인 메뉴 버튼** => **시스템 도구** => **시스템 모니터**를 찾아가시거나 또는 X 윈도우 시스템 내의 쉘 프롬프트에서 gnome-system-monitor라고 입력하시면 됩니다. 그 후 **프로세스 목록** 탭을 클릭하십시오.

GNOME 시스템 모니터를 사용하여 모든 프로세스, 사용자 프로세스와 실행 중인 프로세스를 검색할 수 있습니다.

특정 프로세스에 대한 보다 상세한 정보를 원하시면, 해당 프로세스를 선택 후 **상세 설명** 버튼을 클릭하십시오. 창 아래쪽에 프로세스에 대한 자세한 정보가 나타날 것입니다.

특정 프로세스를 종료하시려면, 해당 프로세스를 선택 후 **프로세스 종료** 버튼을 클릭합니다. 멈춰있는 프로세스를 종료하는데 유용하게 사용됩니다.

특정 행에 따라 정보를 정렬하시려면, 행 이름에 클릭하십시오. 정렬된 행은 어두운 회색으로 나타납니다.

GNOME 시스템 모니터는 스레드를 보여주지 않도록 기본 설정되어 있습니다. 이러한 기본 설정을 바꾸기 위해서는, **편집** => **기본 설정**로 가신 후 **프로세스 목록** 탭을 클릭하시고 **스레드 표시**를 선택하십시오. 기본 설정에서 갱신 시간을 업데이트하고, 각 프로세스에서 기본으로 표시할 정보의 종류를 결정하며 시스템 모니터 그래프의 색상을 변경할 수 있습니다.

그림 26-1. GNOME 시스템 모니터

26.2. 메모리 사용량

`free` 명령은 사용된 메모리 크기, 여유 메모리 크기, 공유 메모리 크기, 커널 버퍼의 메모리 크기와 캐시 메모리 크기와 더불어 물리적 메모리 총량과 시스템 스왑 공간 총량에 대한 정보를 보여줍니다.

```
     total   used   free  shared  buffers  cached
Mem:   256812  240668   16144  105176   50520   81848
-/+ buffers/cache:  108300  148512
Swap:   265032   780  264252
```

`free -m` 명령어는 똑같은 정보를 메가바이트 단위로 보여주기 때문에 훨씬 읽기가 쉽습니다.

```
     total   used   free  shared  buffers  cached
Mem:     250    235     15    102     49     79
-/+ buffers/cache:    105    145
Swap:    258     0    258
```

그래픽 인터페이스로 `free` 명령 결과를 보시려면 **GNOME 시스템 모니터**를 사용하십시오. 데스크탑에서 시작하려면 패널에서 **메인 메뉴 버튼** => **시스템 도구** => **시스템 모니터**를 찾아가시거나 또는 X 윈도우 시스템 내의 쉘 프롬프트에서 `gnome-system-monitor`라고 입력하시면 됩니다. 그 후 **시스템 모니터** 탭을 클릭하십시오.

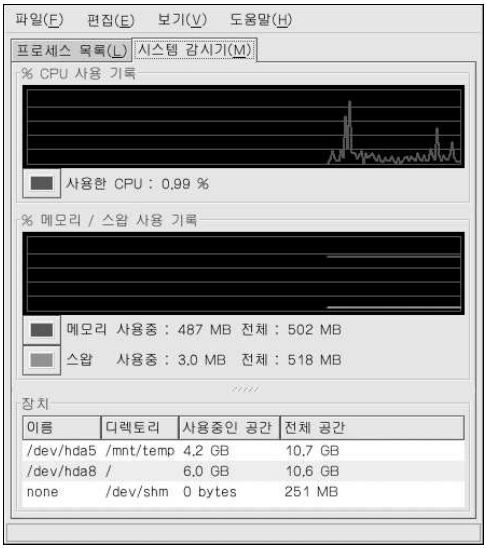

그림 26-2. GNOME 시스템 모니터

26.3. 파일 시스템

`df` 명령어는 시스템의 디스크 공간 사용량을 보고합니다. 쉘 프롬프트에서 `df` 명령을 입력하시면 다음과 유사한 결과가 출력될 것입니다:

```
Filesystem     1k-blocks   Used Available Use% Mounted on
/dev/hda2      10325716  2902060  6899140 30% /
/dev/hda1        15554   8656   6095 59% /boot
/dev/hda3      20722644  2664256 17005732 14% /home
none         256796    0  256796  0% /dev/shm
```

이 유틸리티는 파티션 용량을 1 킬로바이트 블록으로 보여주며 사용된 디스크 공간 크기와 사용 가능한 디스크 공간 크기를 킬로바이트로 보여주도록 기본 설정되어 있습니다. 이 정보를 메가바이트와 기가바이트 단위로 보시려면 `df -h` 명령어를 사용하십시오. 여기서 `-h` 인자는 인간이 읽을 수 있는 (human-readable) 형식을 의미합니다. 이 명령을 입력하시면 다음과 같은 결과가 출력됩니다:

```
Filesystem     Size Used Avail Use% Mounted on
/dev/hda2      9.8G 2.8G 6.5G 30% /
/dev/hda1       15M 8.5M 5.9M 59% /boot
/dev/hda3       20G 2.6G  16G 14% /home
none        251M  0 250M  0% /dev/shm
```

파티션 목록을 보시면 `/dev/shm` 항목을 찾으실 수 있습니다. 이 항목은 시스템의 가상 메모리 파일 시스템을 나타냅니다.

`du` 명령어는 현재 디렉토리 파일 전체의 용량을 보여줍니다. 쉘 프롬프트에서 `du`를 입력하시면 개별 하부 디렉토리의 파일 용량이 목록에 표시됩니다. 현재 디렉토리와 하부 디렉토리의 전체 용량은 목록 마지막 줄에 나타납니다. `du -hs` 명령은 현재 경로에 있는 디렉토리 파일 전체의 총량을 보여줍니다. 더 많은 옵션을 원하시면 `du --help` 명령을 사용하십시오.

그래픽 형식에서 시스템 파티션 사용량과 디스크 공간 사용량을 보시려면, 그림 26-2 아래에 보이듯이 **시스템 모니터** 탭을 사용하시면 됩니다.

힌트

디스크 사용량 할당하기에 대한 정보는 6 장을 참조하시기 바랍니다.

26.3.1. 파일 시스템 감시

Red Hat Linux는 시스템 상에서 여유 디스크 공간의 양을 감시하는 `diskcheck` 유틸리티를 제공합니다. 설정 파일에 기초하여 만일 한개나 그 이상의 디스 드라이브가 지정된 용량을 넘어서면 시스템 관리자에게 이메일 경고를 보냅니다. 이 유틸리티를 사용하기 위해서는 `diskcheck` RPM 패키지를 설치하셔야 합니다.

이 유틸리티는 한 시간마다 크론(cron) [1] 작업으로 실행됩니다.

`/etc/diskcheck.conf`에는 다음과 같은 변수를 정의할 수 있습니다:

- `defaultCutoff` — 디스크 드라이브가 여기에 지정된 퍼센트 용량에 이르게 되면, 시스템 관리자에게 보고합니다. 예를 들어 `defaultCutoff = 90`이라고 가정한다면, 디스크 드라이브가 용량의 90%에 이르게 되면, 시스템 관리자에게 이메일을 보냅니다.
- `cutoff[`*`/dev/partition`*`]` — 해당 파티션에 대한 `defaultCutoff`의 값을 무시하고 새로 지정된 값을 사용합니다. 예를 들어 `cutoff['/dev/hda3'] = 50`이라고 지정한다면 `diskcheck` 명령은 `/dev/hda3` 파티션 용량이 50%에 이르면 시스템 관리자에게 경고를 보낼 것입니다.
- `cutoff[`*`/mountpoint`*`]` — 해당 마운트 지점에 대한 `defaultCutoff`를 무시합니다. 예로 들면 만일 `cutoff['/home'] = 50`이라고 지정한다면, `diskcheck`는 마운트 지점 `/home`의 용량이 50%에 이르게 되면 시스템 관리자에게 경고를 보낼 것입니다.
- `exclude` — `diskcheck`이 무시할 파티션을 지정합니다. 예를 들어 만일 `exclude = "/dev/sda2 /dev/sda4"`이라고 지정한다면, `diskcheck` 명령은 `/dev/sda2` 또는 `/dev/sda4` 파티션에서 지정된 용량 한계(cutoff) 퍼센트에 이르게 되어도 무시하고 시스템 관리자에게 경고하지 않을 것입니다.
- `ignore` — `-x` *`filesystem-type`* 형식으로 무시할 파일 시스템을 지정합니다. 예를 들어 `ignore = "-x nfs -x iso9660"`라고 지정한다면 nfs 또는 iso9660 파일 시스템이 용량 한계에 이르게 되어도 이를 무시하고 시스템 관리자에게 경고하지 않습니다.
- `mailTo` — 파티션과 마운트 지점이 지정 용량에 이르렀을 때 경고를 보낼 시스템 관리자의 이메일 주소입니다. 예를 들어 만일 `mailTo = "webmaster@example.com"`이라고 지정되었다면, webmaster@example.com으로 경고 이메일이 보내질 것입니다.
- `mailFrom` — 이메일 발신자의 신원을 지정합니다. 만일 시스템 관리자가 `diskcheck`로부터 받는 메일을 선별하려고 할 경우에 유용하게 사용됩니다. 예를 들어 `mailFrom = "Disk Usage Monitor"`이라고 지정한다면, 시스템 관리자는 발신자가 Disk Usage Monitor인 이메일을 받을 것입니다.
- `mailProg` — 이메일 경고를 보내는 메일 프로그램을 지정합니다. 예를 들어 `mailProg = "/usr/sbin/sendmail"`라고 지정한다면, Sendmail 메일 프로그램을 사용하여 경고를 보냅니다.

매번 크론 작업이 실행될 때마다 설정 파일을 읽어오기 때문에 설정 파일을 변경하셨어도 서비스를 재시작하실 필요가 없습니다. 크론 작업을 실행하기 위해서는 `crond` 서비스를 실행하셔야 합니다. 데몬이 실행되고 있는지 여부를 알아보기 위해서는 `/sbin/service crond status` 명령을 사용합니다. 부팅시 서비스를 시작하시기를 권 장합니다. 크론 서비스를 부팅시 자동으로 시작하는 방법에 대한 자세한 정보를 원하시면 14 장을 참조해 보시기 바랍니다.

1. 크론에 대한 더 많은 정보를 원하시면 28 장를 참조하시기 바랍니다.

26.4. 하드웨어

하드웨어를 설정하는데 어려움이 있거나 또는 단순히 시스템 내에 어떠한 하드웨어가 존재하는지 알고 싶으시다면, **하드웨어 브라우저** 응용 프로그램을 사용하여 하드웨어를 탐색하여 볼 수 있습니다. 데스크탑에서 이 프로그램을 시작하시려면 **메인 메뉴 버튼** => **시스템 도구** => **하드웨어 브라우저**를 선택하십시오. 또는 쉘 프롬프트에서 `hwbrowser`를 입력합니다. 그림 26-3에서 보이듯이 이 프로그램은 CD-ROM 장치, 플로피 디스크, 하드 드라이브와 파티션, 네트웍 장치, 포인팅 장치, 시스템 장치, 비디오 카드를 보여줍니다. 왼쪽 메뉴에 있는 카테고리 이름에 클릭하시면 관련 정보가 나타날 것입니다.

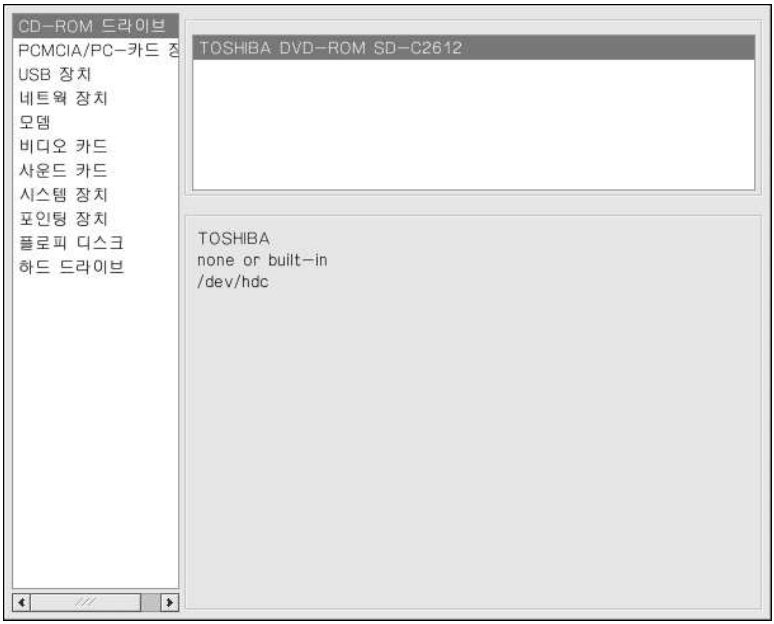

그림 26-3. 하드웨어 브라우저

`lspci` 명령어를 사용하여 모든 PCI 장치 목록을 보실 수 있습니다. 상세한 정보를 원하시면 `lspci -v` 명령을 사용하시고 보다 더 상세한 정보의 출력을 원하신다면 `lspci -vv` 명령어를 사용하시기 바랍니다.

예로 들면, `lspci` 명령어는 시스템에 속한 비디오 카드의 제조회사, 모델과 메모리 크기를 알아내는 데 사용될 수 있습니다:

```
01:00.0 VGA compatible controller: Matrox Graphics, Inc. MGA G400 AGP (rev 04) (prog-if 00 [VGA])
Subsystem: Matrox Graphics, Inc. Millennium G400 Dual Head Max
Flags: medium devsel, IRQ 16
Memory at f4000000 (32-bit, prefetchable) [size=32M]
Memory at fcffc000 (32-bit, non-prefetchable) [size=16K]
Memory at fc000000 (32-bit, non-prefetchable) [size=8M]
Expansion ROM at 80000000 [disabled] [size=64K]
Capabilities: [dc] Power Management version 2
Capabilities: [f0] AGP version 2.0
```

`lspci` 명령은 또한 네트워크 카드의 제조 회사나 모델 번호를 모르실 경우 시스템에서 사용되는 네트워크 카드를 알아내는데도 유용합니다.

26.5. 추가 자료

시스템 정보 모으기에 대한 더 많은 정보를 원하신다면, 다음과 같은 자료를 참조하시기 바랍니다.

26.5.1. 설치된 문서 자료

- `ps --help` — `ps` 명령어에 사용 가능한 옵션 목록을 보여줍니다.
- `top` 메뉴얼 페이지 — `top` 명령어와 함께 사용되는 다양한 옵션에 대한 정보를 원하신다면 `man top` 명령어를 입력하여 메뉴얼 페이지를 참조하십시오.
- `free` 메뉴얼 페이지 — `free` 명령어와 함께 사용되는 다양한 옵션에 대한 정보를 원하신다면 `man free` 명령어를 입력하여 메뉴얼 페이지를 참조하십시오.
- `df` 메뉴얼 페이지 — `df` 명령어와 함께 사용되는 다양한 옵션에 대한 정보를 원하신다면 `man df` 명령어를 입력하여 메뉴얼 페이지를 참조하십시오.
- `du` 메뉴얼 페이지 — `du` 명령어와 함께 사용되는 다양한 옵션에 대한 정보를 원하신다면 `man du` 명령어를 입력하여 메뉴얼 페이지를 참조하십시오.
- `lspci` 메뉴얼 페이지 — `lspci` 명령어와 함께 사용되는 다양한 옵션에 대한 정보를 원하신다면 `man lspci` 명령어를 입력하여 메뉴얼 페이지를 참조하십시오.
- `/proc` — 보다 자세한 시스템 정보를 모으기 위해서 `/proc` 디렉토리의 내용을 참조할 수 있습니다. `/proc` 디렉토리에 대한 추가 정보는 *Red Hat Linux* 참조 가이드를 참조하시기 바랍니다.

26.5.2. 관련 서적

- *Red Hat Linux* 시스템 관리 입문서; Red Hat, Inc. — 자원을 모니터하는 방법을 설명하는 장이 포함되어 있습니다.

27장 . 프린터 설정

여러분은 **프린터 설정 도구**를 사용하여 Red Hat Linux에서 프린터를 설정하실 수 있습니다. 이 도구는 프린터 설정 파일, 프린트 스풀 디렉토리와 프린트 필터를 관리하는데 사용됩니다.

9, Red Hat Linux에서부터 CUPS 인쇄 시스템이 기본으로 사용됩니다. 이전 시스템 디폴트였던, LPRng도 여전히 제공됩니다. LPRng을 사용하는 이전 Red Hat Linux 버전에서 시스템을 업그레이드하셨다면, 업그레이드 과정에서 LPRng은 CUPS로 대체되지 않습니다; 따라서 시스템은 계속해서 LPRng을 사용할 것입니다.

CUPS를 사용하는 이전 Red Hat Linux 버전에서 시스템을 업그레이드하셨다면, 업그레이드 과정에서 설정된 대기열은 변경되지 않을 것이며, 시스템은 계속해서 CUPS를 사용합니다.

프린터 설정 도구는 CUPS와 LPRng 중 사용하도록 선택된 인쇄 시스템을 설정합니다. 변경 사항을 적용하시면, 활성 인쇄 시스템이 설정됩니다.

프린터 설정 도구를 사용하시려면, 루트 권한이 있어야 합니다. 이 응용 프로그램을 시작하시려면, 패널에서 **주 메뉴 버튼** => **시스템 설정** => **인쇄** 항목을 선택하시거나, `redhat-config-printer` 명령을 입력하시면 됩니다. 명령어가 그래픽 X 윈도우 시스템 환경에서 실행되었는지 텍스트 기반 콘솔에서 실행되었는지 여부에 따라서, 이 명령어는 그래픽 버전 또는 텍스트 버전으로 실행할 지 여부를 자동으로 결정하여 이 응용 프로그램을 실행합니다.

프린터 설정 도구를 텍스트-기반 응용 프로그램으로 실행하시려면, 쉘 프롬프트에서 `redhat-config-printer-tui` 명령을 사용하십시오.


중요

`/etc/printcap` 파일이나 `/etc/cups/` 디렉토리에 포함된 파일들을 편집하지 마십시오. 매번 프린터 데몬 (`lpd` 또는 `cups`)이 시작되거나 재시작될 때마다, 새로운 설정 파일이 동적으로 만들어 집니다. 이 파일들은 **프린터 설정 도구**를 사용하여 변경 사항이 적용될 때에도 동적으로 생성됩니다.

LPRng을 사용하시는 경우 **프린터 설정 도구**를 사용하지 않고 프린터를 추가하시려면, `/etc/printcap.local` 파일을 편집하시기 바랍니다. `/etc/printcap.local` 파일의 내용은 **프린터 설정 도구**에 나타나지 않지만, 프린터 데몬에 의해 읽혀집니다. 이전 버전의 Red Hat Linux에서 시스템을 업그레이드 하셨다면, 기존 설정 파일은 이 응용 프로그램이 사용하는 새로운 포맷으로 변환될 것입니다. 매번 새로운 설정 파일이 만들어질 때마다, 이전 설정 파일은 `/etc/printcap.old`로 저장됩니다.

CUPS를 사용하시는 경우, **프린터 설정 도구**는 **프린터 설정 도구**를 사용하여 설정되지 않은 질의나 공유를 보여주지 않습니다; 그러나 설정 파일에서 이러한 질의나 공유를 삭제할 것입니다.

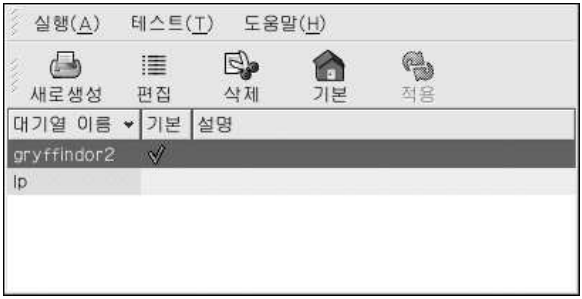

그림 27-1. 프린터 설정 도구

다음과 같은 유형의 인쇄 대기열을 설정 가능합니다:

- **로컬로 접속됨** — 병렬 포트나 USB 포트를 통하여 컴퓨터에 직접 연결되어 있는 프린터를 말합니다.
- **네트워크로 연결된 CUPS (IPP)** — TCP/IP 네트워크를 통하여 접근 가능한 다른 CUPS 시스템에 연결된 프린터 (예, CUPS가 실행 중인 네트워크 상에서 다른 Red Hat Linux 시스템에 연결된 프린터).
- **네트워크로 연결된 UNIX (LPD)** — TCP/IP 네트워크를 통하여 접근 가능한 다른 UNIX 시스템에 연결된 프린터 (예, LPD가 실행 중인 네트워크 상에서 다른 Red Hat Linux 시스템에 연결된 프린터).
- **네트워크로 연결된 Windows (SMB)** — SMB 네트워크 상에서 한 프린터를 공유하고 있는 다른 시스템에 연결된 프린터 (예, Microsoft Windows™ 컴퓨터에 연결된 프린터).
- **네트워크로 연결된 Novell (NCP)** — Novell의 Netware 네트워크 기술을 이용하는 다른 시스템에 연결된 프린터.
- **네트워크로 연결된 JetDirect** — 컴퓨터에 연결되지 않고 HP JetDirect를 통하여 네트워크로 직접 연결된 프린터.

중요

만일 새로운 인쇄 대기열을 추가하시거나 현재의 것을 변경하실 때, 변경 사항을 적용하셔야 효력을 발생합니다.

적용 버튼을 클릭하여 변경 사항을 저장하시고 프린터 데몬을 재시작합니다. 프린터 데몬이 재시작된 후 변경 사항은 설정 파일에 기록됩니다. 다른 방법으로는 **실행** => **적용**을 선택하시면 됩니다.

27.1. 로컬 프린터 추가하기

컴퓨터에 병렬 포트나 USB 포트로 연결된 로컬 프린터를 추가하시려면, 그림 27-2에서 보여지듯이 기본 **프린터 설정 도구** 창에서 **새로생성** 버튼을 클릭하시기 바랍니다. **앞으로** 버튼을 클릭하여 계속 진행해 주십시오.

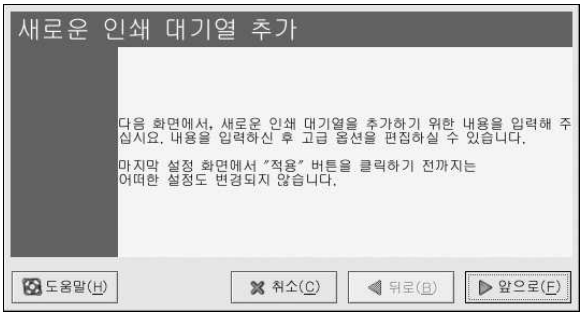

그림 27-2. 프린터 추가

그림 27-3에서 보여지는 화면에서 **이름** 입력란에 프린터에 사용될 이름을 입력하시기 바랍니다. 프린터 이름은 빈 공간이 없이 영어 알파벳 문자로 시작되어야 합니다. 프린터 이름에 알파벳, 숫자, 대시 (-), 밑줄 (_)이 올 수 있습니다. 원하시면 프린터를 보다 쉽게 식별할 수 있도록 프린터에 대한 간략한 설명을 입력하실 수 있습니다. 이 설명란에는 빈 공간이 있어도 괜찮습니다.

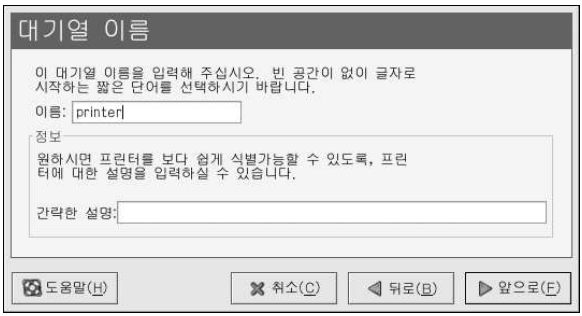

그림 27-3. 대기열 이름 선택

앞으로 버튼을 클릭하시면, 그림 27-4에서 보여지는 화면이 나타날 것입니다. **대기열 유형 선택** 메뉴에서 **로컬로 접속됨** 항목을 선택하시고 장치를 선택하시기 바랍니다. 일반적으로 병렬 포트에 연결된 장치는 `/dev/lp0`이고, USB 프린터에는 `/dev/usb/lp0` 입니다. 만일 목록에서 아무런 장치가 나타나지 않는다면, **장치 다시읽기** 버튼을 클릭하여 컴퓨터를 다시 읽어오거나 **사용자 정의 장치** 버튼을 클릭하여 직접 사용할 장치를 입력하시는 방법도 있습니다. **앞으로** 버튼을 클릭하여 다음 단계로 계속 진행하십시오.

그림 27-4. 로컬 프린터 추가

다음 단계는 프린터 유형을 선택하시는 것입니다. 계속 진행하기 위해 27.7 절으로 넘어가시기 바랍니다.

27.2. IPP 프린터 추가하기

IPP 프린터란 네트워크로 실행 중인 동일한 네트워크 상에서 다른 리눅스 시스템에 연결된 프린터 또는 다른 운영 체제에서 IPP를 사용하도록 설정된 프린터를 말합니다. 디폴트 값으로, **프린터 설정 도구**는 네트워크에서 공유된 CUPS 프린터가 있는지 검색해 봅니다. (이 옵션을 변경하시려면, 풀다운 메뉴에서 **실행** => **공유**를 선택하신 후 **일반** 탭에서 이 옵션을 선택 해제하시면 됩니다.) 네트워크로 연결된 모든 IPP 프린터는 기본 화면에서 검색된 대기열로 나타납니다.

프린터 서버 상에 방화벽을 설정하셨다면, 들어오는 UDP 포트, 631에서 접속을 보내고 받을 수 있도록 하셔야 합니다. 클라이언트 (인쇄 요청을 보내는 컴퓨터) 상에 방화벽을 설정하신 경우, 포트 631에서 접속을 보내고 수용하도록 설정하시기 바랍니다.

자동 검색 기능을 비활성화하신 경우에도 기본 **프린터 설정 도구** 창에서 **새로생성** 버튼을 클릭하신 후 나타난 그림 27-2의 화면에서 네트워크로 연결된 IPP 프린터를 추가하실 수 있습니다. **앞으로** 버튼을 클릭하여 계속 진행하시기 바랍니다.

그림 27-3에서 보여지는 화면에서 **이름** 입력란에 프린터에 사용될 이름을 입력하시기 바랍니다. 프린터 이름은 빈 공간이 없이 영어 알파벳 문자로 시작되어야 합니다. 프린터 이름에 알파벳, 숫자, 대시 (-), 밑줄 (_)이 올 수 있습니다. 원하시면 프린터를 보다 쉽게 식별할 수 있도록 프린터에 대한 간략한 설명을 입력하실 수 있습니다. 이 설명란에는 빈 공간이 있어도 괜찮습니다.

앞으로 버튼을 클릭하시면 그림 27-5 화면이 나타날 것입니다. **대기열 유형 선택** 메뉴에서 **네트워크로 연결된 CUPS (IPP)**를 선택하십시오.

그림 27-5. IPP 프린터 추가

다음과 같은 옵션에 대한 입력란이 나타날 것입니다:

- **서버** — 프린터가 연결된 원격 컴퓨터의 호스트명이나 IP 주소.
- **경로** — 원격 컴퓨터 상의 인쇄 대기열로 경로.

앞으로 버튼을 클릭하여 계속 진행해 나가십시오.

다음 단계는 프린터 유형을 선택하시는 것입니다. 계속 진행하기 위해 27.7 절으로 넘어가시기 바랍니다.

중요

네트워크로 연결된 IPP 프린터 서버는 로컬 시스템에서의 접속 만을 허용합니다. 보다 많은 정보를 원하신다면, 27.13 절을 참조하시기 바랍니다.

27.3. 원격 UNIX (LPD) 프린터 추가하기

동일한 네트워크 상에서 다른 리눅스 시스템에 연결된 것과 같은 원격 UNIX 프린터를 추가하시려면, 그림 27-2에서 보여지듯이 기본 **프린터 설정 도구** 창에서 **새로생성** 버튼을 클릭하시기 바랍니다. **앞으로** 버튼을 클릭하여 계속 진행해 주십시오.

그림 27-3에서 보여지는 화면에서 **이름** 입력란에 프린터에 사용될 이름을 입력하시기 바랍니다. 프린터 이름은 빈 공간이 없이 영어 알파벳 문자로 시작되어야 합니다. 프린터 이름에 알파벳, 숫자, 대시 (-), 밑줄 (_)이 올 수 있습니다. 원하시면 프린터를 보다 쉽게 식별할 수 있도록 프린터에 대한 간략한 설명을 입력하실 수 있습니다. 이 설명란에는 빈 공간이 있어도 괜찮습니다.

대기열 유형 선택 메뉴에서 **네트워크로 연결된 UNIX (LPD)**를 선택하십시오. **앞으로** 버튼을 클릭하여 계속 진행하시기 바랍니다.

그림 27-6. 원격 LPD 프린터 추가

다음과 같은 옵션에 대한 입력란이 나타날 것입니다:

- **서버** — 프린터가 연결된 원격 컴퓨터의 호스트명이나 IP 주소.
- **대기열** — 원격 프린터 대기열. 일반적으로 디폴트 프린터 대기열은 `lp` 입니다.

앞으로 버튼을 클릭하여 계속 진행해 나가십시오.

다음 단계는 프린터 유형을 선택하시는 것입니다. 계속 진행하기 위해 27.7 절으로 넘어가시기 바랍니다.


중요

원격 프린트 서버는 로컬 시스템에서의 접속 만을 허용합니다. 보다 많은 정보를 원하신다면, 27.13.1 절을 참조하시기 바랍니다.

27.4. Samba (SMB) 프린터 추가하기

SMB 프로토콜을 사용하여 접속된 프린터 (예, Microsoft Windows 시스템에 연결된 프린터)를 추가하시려면, 기본 **프린터 설정 도구** 화면에서 **새로생성** 버튼을 클릭하십시오. 그림 27-2에서 보여진 창이 나타날 것입니다. **앞으로** 버튼을 클릭하여 계속 진행해 나가십시오.

그림 27-3에서 보여지는 화면에서 **이름** 입력란에 프린터에 사용될 이름을 입력하시기 바랍니다. 프린터 이름은 빈 공간이 없이 영어 알파벳 문자로 시작되어야 합니다. 프린터 이름에 알파벳, 숫자, 대시 (-), 밑줄 (_)이 올 수 있습니다. 원하시면 프린터를 보다 쉽게 식별할 수 있도록 프린터에 대한 간략한 설명을 입력하실 수 있습니다. 이 설명란에는 빈 공간이 있어도 괜찮습니다.

대기열 유형 선택 메뉴에서 **네트워크로 연결된 Windows (SMB)**를 선택하신 후 **앞으로** 버튼을 클릭하시기 바랍니다. 만일 프린터가 Microsoft Windows 시스템에 연결되어 있다면, 이 대기열 유형을 선택하십시오.

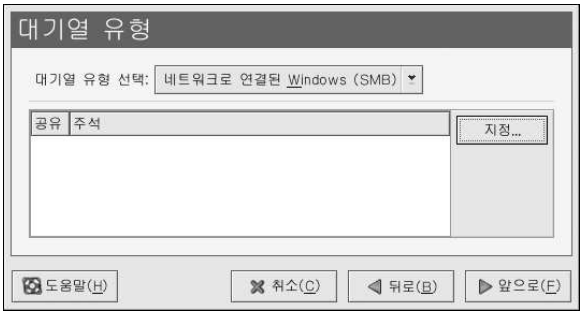

그림 27-7. SMB 프린터 추가

그림 27-7에서 보여지듯이, SMB 공유는 자동으로 검색되어 목록에 나타납니다. 각 공유 이름 옆에 위치한 화살표 키를 클릭하시면 목록이 확장됩니다. 확장된 목록에서 프린터를 선택하시기 바랍니다.

찾으시는 프린터가 목록에 없다면, 오른쪽에 위치한 **지정** 버튼을 클릭하시기 바랍니다. 다음과 같은 옵션에 대한 입력란이 나타날 것입니다:

- **작업그룹** — 공유 프린터에 사용될 Samba 작업 그룹 이름.
- **서버** — 프린터를 공유하는 서버 이름.
- **공유** — 인쇄할 공유 프린터의 이름. 이 이름은 원격 Windows 기계 상에 정의된 Samba 프린터의 이름과 동일해야 합니다.
- **사용자 이름** — 프린터 사용을 위해 로그인시 사용할 사용자 이름. 이 사용자 이름은 Windows 시스템 상에서도 존재해야하며, 프린터를 사용할 수 있는 허가를 가지고 있어야 합니다. 디폴트 사용자 이름은 일반적으로 Windows 서버에서는 **guest**이고, Samba 서버에서는 **nobody** 입니다.
- **암호 — 사용자 이름** 영역에 지정된 사용자 암호 (필요한 경우).

앞으로 버튼을 클릭하여 계속 진행해 나가십시오. **프린터 설정 도구**는 이제 공유 프린터에 접속을 시도할 것입니다. 만일 공유 프린터를 사용하기 위해 사용자명과 암호가 필요하다면, 공유 프린터에 대한 유효한 사용자명과 암호를 요청하는 대화 상자가 나타날 것입니다. 만일 공유 이름을 잘못 지정하신 경우, 여기서 변경하실 수도 있습니다. 만일 공유에 접속하기 위해 작업그룹 이름이 필요하다면, 이 대화 상자에서 지정 가능합니다. 이 대화 상자 창은 **지정** 버튼을 클릭하였을 때 나타나는 창과 동일합니다.

다음 단계는 프린터 유형을 선택하시는 것입니다. 계속 진행하기 위해 27.7 절으로 넘어가시기 바랍니다.

경고

사용자명과 암호는 루트 사용자와 lpd에 의해서만 읽기 가능한 파일에 암호화되지 않은 상태로 저장되어 있습니다. 따라서 다른 사용자들이 루트 허가를 가지게 된다면 여러분의 사용자명과 암호를 알아낼 가능성이 있습니다. 이러한 위험을 방지하기 위하여, 프린터에 사용하는 사용자명과 암호는 로컬 Red Hat Linux 시스템의 사용자 계정에 사용되는 사용자명과 암호와는 다르게 설정하셔야 합니다. 이렇게 설정하심으로써, 다른 사용자들이 사용자명과 암호를 알아낸 경우에도, 허가없이 프린터를 사용하는 작업만 가능하게 됩니다. 만일 서버에서 공유되는 파일이 존재한다면, 인쇄 대기열에 사용되는 암호와는 다른 암호를 사용하시길 바랍니다.

27.5. Novell NetWare (NCP) 프린터 추가하기

Novell NetWare (NCP) 프린터를 추가하시려면, 주 **프린터 설정 도구** 화면에서 **새로생성** 버튼을 클릭하십시오. 그림 27-1과 같은 창이 나타납니다. **앞으로** 버튼을 클릭하여 계속 진행해 나가시기 바랍니다.

그림 27-3에서 보여지는 화면에서 **이름** 입력란에 프린터에 사용될 이름을 입력하시기 바랍니다. 프린터 이름은 빈 공간이 없이 영어 알파벳 문자로 시작되어야 합니다. 프린터 이름에 알파벳, 숫자, 대시 (-), 밑줄 (_)이 올 수 있습니다. 원하시면 프린터를 보다 쉽게 식별할 수 있도록 프린터에 대한 간략한 설명을 입력하실 수 있습니다. 이 설명란에는 빈 공간이 있어도 괜찮습니다.

대기열 유형 선택 메뉴에서 **네트워크로 연결된 Novell (NCP)** 항목을 선택하십시오.

그림 27-8. NCP 프린터 추가

다음과 같은 옵션에 대한 입력란이 나타납니다:

- **서버** — 프린터가 연결된 NCP 시스템의 호스트명 또는 IP 주소.
- **대기열** — NCP 시스템 상 프린터의 원격 대기열.
- **사용자** — 프린터에 접속시 로그인하기 위해 사용할 사용자명.
- **암호** — 위의 **사용자** 란에서 지정된 사용자의 암호.

다음 단계는 프린터 유형을 선택하시는 것입니다. 계속 진행하기 위해 27.7 절으로 넘어가시기 바랍니다.

경고

사용자명과 암호는 루트 사용자와 lpd에 의해서만 읽기 가능한 파일에 암호화되지 않은 상태로 저장되어 있습니다. 따라서 다른 사용자들이 루트 허가를 가지게 된다면 여러분의 사용자명과 암호를 알아낼 가능성이 있습니다. 이러한 위험을 방지하기 위하여, 프린터에 사용하는 사용자명과 암호는 로컬 Red Hat Linux 시스템의 사용자 계정에 사용되는 사용자명과 암호와는 다르게 설정하셔야 합니다. 이렇게 설정하심으로써, 다른 사용자들이 사용자명과 암호를 알아낸 경우에도, 허가없이 프린터를 사용하는 작업만 가능하게 됩니다. 만일 서버에서 공유되는 파일이 존재한다면, 인쇄 대기열에 사용되는 암호와는 다른 암호를 사용하시길 바랍니다.

27.6. JetDirect 프린터 추가하기

JetDirect 프린터를 추가하시려면, 주 **프린터 설정 도구** 화면에서 **새로생성** 버튼을 클릭하십시오. 그림 27-1과 같은 창이 나타납니다. **앞으로** 버튼을 클릭하여 계속 진행해 나가시기 바랍니다.

그림 27-3에서 보여지는 화면에서 **이름** 입력란에 프린터에 사용될 이름을 입력하시기 바랍니다. 프린터 이름은 빈 공간이 없이 영어 알파벳 문자로 시작되어야 합니다. 프린터 이름에 알파벳, 숫자, 대시 (-), 밑줄 (_)이 올 수 있습니다. 원하시면 프린터를 보다 쉽게 식별할 수 있도록 프린터에 대한 간략한 설명을 입력하실 수 있습니다. 이 설명란에는 빈 공간이 있어도 괜찮습니다.

대기열 유형 선택 메뉴에서 **네트워크로 연결된 JetDirect** 항목을 선택하신 후 **앞으로** 버튼을 클릭해 주십시오.

그림 27-9. JetDirect 프린터 추가하기

다음과 같은 옵션에 대한 입력란이 나타납니다:

- **프린터** — JetDirect 프린터의 호스트명 또는 IP 주소.
- **포트** — JetDirect 프린터가 인쇄 작업을 기다릴 포트 번호. 기본 포트는 9100 입니다.

다음 단계는 프린터 유형을 선택하시는 것입니다. 계속 진행하기 위해 27.7 절으로 넘어가시기 바랍니다.

27.7. 프린터 모델 선택 후 완료하기

프린터의 대기열 유형을 선택하신 후, 다음 단계는 프린터 모델을 선택하시는 것입니다.

그림 27-10에서 보여지는 창과 유사한 창이 나타날 것입니다. 만일 프린터 모델이 자동으로 검색되지 않았다면, 여러분이 직접 목록에서 모델을 선택해 주십시오. 프린터들은 제조업체에 따라 분류되어 있습니다. 풀다운 메뉴에서 프린터 제조업체의 이름을 선택하십시오. 다른 제조업체가 선택될 때마다 프린터 모델이 업데이트됩니다. 목록에서 프린터 모델을 선택하시기 바랍니다.

그림 27-10. 프린터 모델 선택

선택하신 프린터 모델에 기초하여 권장되는 프린트 드라이버가 선택되어 집니다. 프린트 드라이버는 여러분이 인쇄하고자 하는 데이터를 프린터가 인식 가능한 형식으로 처리하는 역할을 합니다. 로컬 프린터는 컴퓨터에 바로 연결되어 있으므로, 프린터에 전달될 데이터를 처리할 프린트 드라이버가 필요합니다.

원격 프린터 (IPP, LPD, SMB, NCP)를 설정하시는 경우, 원격 프린터 서버는 일반적으로 독자적인 프린트 드라이버를 가지고 있습니다. 로컬 컴퓨터에 추가 프린트 드라이브를 선택하신다면, 인쇄할 데이터가 여러 번 변환되어 결국 프린터가 인식하지 못하는 포맷으로 변환됩니다.

데이터가 한 번 이상 변환되지 않도록 하기 위해서는, 우선 제조업체로 **Generic**을 선택하신 후 **Raw 인쇄 대기열**이나 **포스트스크립트 프린터**를 프린터 모델로 선택하시기 바랍니다. 그 후 변경 사항을 적용하시고 새로운 설정을 이용하여 테스트 페이지를 인쇄해 보십시오. 만일 테스트에 실패한다면, 원격 프린트 서버에 프린트 드라이버가 설정되지 않은 것일 수도 있습니다. 제조업체와 원격 프린터의 모델에 맞는 프린트 드라이버를 선택하신 후 변경 사항을 적용하시고, 테스트 페이지를 인쇄해 보시기 바랍니다.

힌트

프린터를 추가하신 후 다른 프린트 드라이버를 선택하실 수 있습니다. **프린터 설정 도구**를 시작하신 후 목록에서 프린터를 선택하시고 **편집** 버튼을 클릭하십시오. 그 후 **드라이버** 탭을 클릭하신 후 다른 프린트 드라이버를 선택하시고 변경 사항을 적용하시면 됩니다.

27.7.1. 프린터 설정 확인하기

마지막으로 여러분이 변경하신 프린터 설정을 확인해 주셔야 합니다. 모든 설정이 올바르다면, 인쇄 대기열을 추가하기 위해 **적용** 버튼을 클릭하시기 바랍니다. 프린터 설정을 수정하시려면 **뒤로** 버튼을 클릭하십시오.

기본 창에서 **적용** 버튼을 클릭하여 변경 사항을 저장하고 프린터 데몬을 재시작하시기 바랍니다. 변경 사항이 적용된 후, 모든 설정이 올바른지 확인해 보기위해 테스트 페이지를 인쇄해 보십시오. 자세한 사항은 27.8 절을 참조하시기 바랍니다.

기본 ASCII 세트 (일본어와 같은 언어에 사용되는 ASCII 세트 포함) 이외의 문자를 인쇄하시려면, 드라이버 옵션을 다시 확인하여 **포스트스크립트 재출력** 항목을 선택하셔야 합니다. 인쇄 대기열을 추가하신 후 수정하실 경우 페이지 규격과 같은 옵션들을 설정하실 수 있습니다.

27.8. 테스트 페이지 인쇄하기

프린터를 설정하신 후, 프린터가 적절하게 작동하는지 확인하기 위하여 테스트 페이지를 인쇄해 보시기 바랍니다. 테스트 페이지를 인쇄하시려면, 프린터 목록에서 테스트할 프린터를 선택하신 후 **테스트** 풀다운 메뉴에서 적절한 테스트 페이지를 선택하시면 됩니다.

프린트 드라이버나 드라이버 옵션을 변경하신다면, 다른 설정을 테스트하기 위해 테스트 페이지를 인쇄해보셔야 합니다.

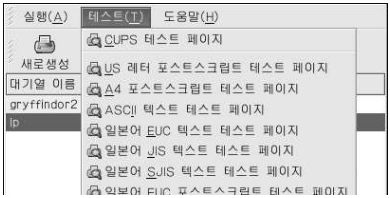

그림 27-11. 테스트 페이지 옵션

27.9. 기존 프린터 수정하기

기존 프린터를 삭제하시려면, 해당 프린터를 선택하신 후 도구바에서 **삭제** 버튼을 클릭하십시오. 프린터 목록에서 해당 프린터가 삭제될 것입니다. **적용**을 클릭하여 변경 사항을 저장하고 프린터 데몬을 재시작합니다.

기본 프린터를 설정하시려면, 프린터 목록에서 프린터를 선택하신 후 도구바에서 **기본** 버튼을 클릭합니다. 다음과 같은 기본 프린터 아이콘이 목록에서 기본 프린터의 **기본** 칸에 나타납니다.

프린터를 추가하신 후 프린터 설정을 편집하시려면, 프린터 목록에서 프린터를 선택하신 후 **편집** 버튼을 클릭하시면 됩니다. 그림 27-12에서 보여진 탭으로 구성된 창이 나타납니다. 탭으로 구성된 창은 편집하실 프린터의 현재값을 포함하고 있습니다. 현재값을 변경하신 후 **확인** 버튼을 클릭해 주십시오. 주 **프린터 설정 도구** 창에서 **적용** 버튼을 클릭하여 변경 사항을 저장하시고 프린터 데몬을 재시작합니다.

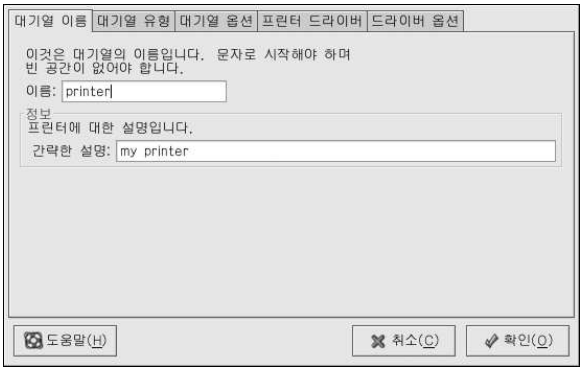

그림 27-12. 프린터 편집

27.9.1. 대기열 이름

프린터의 이름을 변경하시려면, **대기열 이름** 란에서 이름을 변경하십시오. **확인** 버튼을 클릭하여 주 화면으로 되돌아가시면 프린터 목록에 나오는 프린터의 이름이 변경되어 있을 것입니다. **적용** 버튼을 눌러서 변경 사항을 저장하고 프린터 데몬을 재시작합니다.

27.9.2. 대기열 유형

대기열 유형 탭에서는 프린터와 설정을 추가하실 때 선택하신 대기열 유형을 보여줍니다. 프린터의 대기열 유형이나 설정을 변경하실 수 있습니다. 변경을 마치면, **확인** 버튼을 클릭하여 주 화면으로 돌아갑니다. **적용** 버튼을 눌러서 변경 사항을 저장하시고 프린터 데몬을 재시작합니다.

선택하신 대기열 유형에 따라서 다른 옵션이 나타날 것입니다. 옵션에 대한 설명을 보시려면 적절한 프린터 추가하기 섹션을 참조하시기 바랍니다.

27.9.3. 프린터 드라이버

프린터 드라이버 탭에서는 현재 사용되고 있는 프린트 드라이버의 종류를 보여줍니다. 프린트 드라이버를 변경하셨으면, **확인** 버튼을 클릭하여 주 화면으로 돌아가십시오. **적용** 버튼을 클릭하여 변경 사항을 저장하신 후 프린터 데몬을 재시작하시기 바랍니다.

27.9.4. 드라이버 옵션

드라이버 옵션 탭에서는 고급 프린터 옵션을 설정하실 수 있습니다. 옵션은 개별 프린트 드라이버에 따라 다르지만 일반적으로 사용되는 옵션은 다음과 같습니다:

- 프린터가 인쇄 작업의 마지막 페이지를 배출하지 않는 경우 (예, form feed 표시등이 깜박거릴 경우), **Form-Feed (FF) 보내기** 옵션을 선택하셔야 합니다. 만일 이 방법이 효과가 없다면, 대신 **End-of-Transmission (EOT) 보내기**를 선택해 보십시오. 일부 프린터에서 마지막 페이지를 빼내기 위해서는 **Form-Feed (FF) 보내기**와 **End-of-Transmission (EOT) 보내기** 옵션을 모두 선택하셔야 합니다. 이 옵션은 LPRng 인쇄 시스템에서만 사용 가능합니다.
- 만일 form-feed 보내기가 작동하지 않는다면 **End-of-Transmission (EOT) 보내기**를 사용해 보십시오. 앞서 언급된 **Form-Feed (FF) 보내기**를 참조하시기 바랍니다. 이 옵션은 LPRng 인쇄 시스템에서만 사용 가능합니다.
- 프린트 드라이버가 전송된 데이터의 일부를 인식하지 못할 경우 **알 수 없는 데이터는 텍스트로 취급함** 옵션을 선택하셔야 합니다. 인쇄에 문제가 있을 시에만 이 옵션을 선택하십시오. 이 옵션을 선택하시면, 프린트 드라이버는 인식할 수 없는 모든 데이터를 텍스트로 추정 후 그 데이터를 텍스트로 인쇄합니다. 이 옵션과 **텍스트를 포스트스크립트로 변환** 옵션을 함께 선택하시면, 프린트 드라이버는 모르는 데이터를 텍스트로 추정 후 그 데이터를 포스트스크립트로 변환시킵니다. 이 옵션은 LPRng 인쇄 시스템에서만 사용 가능합니다.
- 기본 ASCII 세트가 아닌 문자 (예, 일본어 문자)가 제대로 인쇄되지 않을 때 **포스트스크립트 재출력** 옵션을 선택하셔야 합니다. 이 옵션은 표준이 아닌 포스트스크립트 글꼴을 재출력하여 제대로 인쇄될 수 있게 해줍니다.

  인쇄하시려는 글꼴이 프린터에서 지원되지 않는 경우, 이 옵션을 선택해 보십시오. 예를 들면 비-일본어 프린터에서 일본어 글꼴을 인쇄하시려는 경우 이 옵션을 선택하십시오.

  이 작업을 수행하기 위해서는 별도의 시간이 필요합니다. 제대로된 글꼴을 인쇄하는데 문제가 있는 경우가 아니라면 이 옵션을 선택하지 마십시오.

  프린터가 포스트스크립트 레벨 3을 처리하지 못하는 경우에도 이 옵션을 선택하십시오. 이 옵션을 사용하시면 포스트스크립트 레벨 3을 레벨 1로 변환합니다.

- **GhostScript pre-filtering** — 프린터가 특정 포스트스크립트 레벨을 처리하지 못할 경우 **No pre-filtering**, **Convert to PS level 1**, **Convert to PS level 2** 중 한가지 옵션을 선택하실 수 있습니다. 이 옵션은 포스트스크립트 드라이버가 CUPS 인쇄 시스템과 함께 사용되었을 경우에만 사용 가능합니다.
- **텍스트를 포스트스크립트로 변환** 옵션은 기본으로 선택됩니다. 평문을 인쇄할 수 있는 프린터를 가지고 계시다면, 평문 문서를 인쇄할 시에는 이 옵션을 선택 해제하여 인쇄 시간을 단축하실 수 있습니다. CUPS 인쇄 시스템을 사용하신다면, 텍스트가 항상 포스트스크립트로 변환되므로 이 옵션이 사용되지 않습니다.
- **페이지 규격** 옵션을 사용하여 프린터에서 사용될 페이지 규격 (예, US Letter, US Legal, A3, A4)을 선택하실 수 있습니다.
- **효율적인 필터 위치** 옵션은 **C**로 기본 설정되어 있습니다. 만일 일본어 문자를 인쇄하시려면, **ja_JP**를 선택하십시오. 다른 경우에는 디폴트 값인 **C**를 그대로 사용하시면 됩니다.
- **매체 소스** 옵션은 **프린터 기본**으로 기본 설정되어 있습니다. 다른 트레이에서 종이를 가져와 인쇄하도록 이 옵션을 변경해 주십시오.

드라이버 옵션을 수정하시려면, **확인** 버튼을 클릭하여 주 화면으로 되돌아가시기 바랍니다. 그 후 **적용** 버튼을 눌러 변경 사항을 저장하시고 프린터 데몬을 재시작하시면 됩니다.

27.10. 설정 파일 저장하기

프린터 설정 도구를 사용하여 프린터 설정을 저장하시면, 독자적인 설정 파일이 생성됩니다. 이 설정 파일은 `/etc/cups` 디렉토리에 파일들을 생성하거나 `lpd`이 읽어들이는 `/etc/printcap` 파일을 생성하는데 사용됩니다. 여러분은 명령행 옵션을 사용하여 **프린터 설정 도구** 파일을 저장하거나 복구하실 수 있습니다. 만일 `/etc/cups` 디렉토리나 `/etc/printcap` 파일이 동일한 위치에서 저장된 후 복구된다면, 매번 프린터 데몬이 재시작할 때마다 특별한 **프린터 설정 도구** 설정 파일에서 새로운 `/etc/printcap` 파일을 생성하기 때문에, 프린터 설정을 복구하실 수 없습니다. 시스템 설정 파일의 백업 파일을 만드시려면, 다음에 설명된 방법을 사용하여 프린터 설정을 저장하셔야 합니다. 만일 LPRng을 사용하는 시스템의 경우 `/etc/printcap.local` 파일에 사용자 정의 설정을 추가하셨다면, 이 파일도 백업 시스템에 저장하시기 바랍니다.

프린터 설정을 저장하시려면, 루트로 로그인 하신 후 다음 명령을 입력하십시오:

```
/usr/sbin/redhat-config-printer-tui --Xexport > settings.xml
```

설정이 `settings.xml` 파일에 저장됩니다.

이 파일을 저장하심으로서 이 파일을 사용하여 프린터 설정을 복구하실 수 있습니다. 만일 프린터 설정이 삭제되었거나, Red Hat Linux를 재설치하시는 경우 또는 더 이상 프린터 설정 파일이 존재하지 않거나 다중 시스템 상에서 동일한 프린터 설정을 사용하기를 원하시는 경우에 이 파일이 유용하게 사용됩니다. 설정을 복구하시려면, 루트로 로그인 하신 후 다음 명령을 입력하시기 바랍니다:

```
/usr/sbin/redhat-config-printer-tui --Ximport < settings.xml
```

이미 설정 파일을 가지고 있으면서 (시스템 상에서 한 개 이상의 프린터를 설정하신 경우) 또 다른 설정 파일을 가져오시면, 이 설정 파일이 기존의 설정 파일을 덮어쓸 것입니다. 기존 설정을 변경하지 않은 채 저장된 파일에 설정을 추가하시려면, (루트로) 다음의 명령을 사용하여 파일을 합병(merge)하실 수 있습니다:

```
/usr/sbin/redhat-config-printer-tui --Ximport --merge < settings.xml
```

이제 프린터 목록에는 여러분이 설정하신 프린터를 비롯하여 저장된 설정 파일에서 가져온 프린터가 모두 포함됩니다. 만일 기존 인쇄 대기열과 동일한 이름을 가진 인쇄 대기열이 가져온 설정 파일에 존재한다면, 가져온 파일에 있는 인쇄 대기열이 기존 프린터의 인쇄 대기열을 덮어 쓰게 됩니다.

설정 파일을 (`merge` 명령을 사용하여 또는 사용하지 않고) 가져오신 후에는, 반드시 프린터 데몬을 재시작하셔야 합니다. CUPS를 사용하신다면, 다음 명령을 입력하십시오:

```
/sbin/service cups restart
```

LPRng을 사용하신다면, 다음 명령을 입력하시기 바랍니다:

```
/sbin/service lpd restart
```

27.11. 명령행 설정

X가 설치되지 않은 경우 텍스트 기반 버전을 사용하기를 원치 않으신다면, 명령행을 통해 프린터를 추가하실 수 있습니다. 스크립트를 통하여 또는 킥스타트 설치의 %post 섹션에서 프린터를 추가하실 경우 이 방법이 유용합니다.

27.11.1. 로컬 프린터 추가하기

프린터를 추가하시려면:

```
redhat-config-printer-tui --Xadd-local options
```

옵션들:

--device=*node*

‘ (필수) 여기서 node는 사용할 장치 노드를 의미합니다. 예, `/dev/lp0`

--make=*make*

‘ (필수) 여기서 make는 IEEE 1284 MANUFACTURER 문자열을 입력하십시오. 만일 사용가능한 제조업체 문자열이 없다면, foomatic 데이터베이스에 나타난 프린터 제조업체명을 사용하십시오.

--model=*model*

‘ (필수) model은 IEEE 1284 MODEL 문자열로 교체하십시오. 만일 모델 문자열이 없다면, foomatic 데이터베이스에 나타난 프린터 모델을 입력하시면 됩니다.

--name=*name*

‘ (옵션) 새로운 대기열의 이름을 입력하십시오. 만일 이름을 직접 입력하지 않으시면, 장치 노드에 기초한 이름 (예, “lp0”)이 사용됩니다.

--as-default

‘ (옵션) 이 대기열을 디폴트로 설정합니다.

CUPS 인쇄 시스템 (디폴트)을 사용하신다면, 프린터를 추가하신 후 다음 명령을 사용하여 프린터 데몬을 시작/재시작하시기 바랍니다:

```
service cups restart
```

LPRng 인쇄 시스템을 사용하시는 경우, 프린터를 추가하신 후 다음 명령을 사용하여 프린터 데몬을 시작/재시작하시기 바랍니다:

```
service lpd restart
```

27.11.2. 로컬 프린터 삭제하기

명령행을 사용하여 프린터 대기열을 삭제하실 수도 있습니다.

프린터 대기열을 삭제하시려면, 루트로 로그인하신 후 다음 명령을 입력하시면 됩니다:

```
redhat-config-printer-tui --Xremove-local options
```

옵션들:

--device=*node*

‘ (필수) 여기서 node는 사용할 장치 노드를 의미합니다. 예, `/dev/lp0`

--make=*make*

‘ (필수) 여기서 make는 IEEE 1284 MANUFACTURER 문자열을 입력하십시오. 만일 사용가능한 제조업체 문자열이 없다면, foomatic 데이터베이스에 나타난 프린터 제조업체명을 사용하십시오.

--model=*model*

‘ (필수) model은 IEEE 1284 MODEL 문자열로 교체하십시오. 만일 모델 문자열이 없다면, foomatic 데이터베이스에 나타난 프린터 모델을 입력하시면 됩니다.

CUPS 인쇄 시스템 (디폴트)을 사용하시는 경우, **프린터 설정 도구** 설정에서 프린터를 삭제하신 후, 변경 사항을 적용하기 위하여 프린터 데몬을 재시작해 주십시오:

```
service cups restart
```

LPRng 인쇄 시스템을 사용하신다면, **프린터 설정 도구** 설정에서 프린터를 삭제하신 후, 변경 사항을 적용하기 위하여 프린터 데몬을 재시작해 주십시오:

```
service lpd restart
```

CUPS를 사용하시는 경우, 프린터를 모두 삭제하신 후 더 이상 프린터 데몬을 실행하지 않으시려면, 다음과 같은 명령을 실행하십시오:

```
service cups stop
```

LPRng을 사용하시는 경우, 프린터를 모두 삭제하신 후 더 이상 프린터 데몬을 실행하지 않으시려면, 다음과 같은 명령을 실행하십시오:

```
service lpd stop
```

27.12. 인쇄 작업 관리하기

Emacs에서 텍스트 파일을 인쇄하시거나 **The GIMP**에서 이미지를 인쇄하는 경우와 같이 프린터 데몬으로 인쇄 작업을 보내신다면, 그 인쇄 작업은 인쇄 스풀 대기열에 추가됩니다. 인쇄 스풀 대기열이란 프린터로 보내진 인쇄 작업 목록으로서 개별 인쇄 요청에 대한 요청 상태, 요청한 사용자명, 요청을 보낸 시스템의 호스트명, 작업 번호 등의 정보를 포함합니다.

그래픽 데스크탑 환경을 실행 중인 경우, 그림 27-13에서 보여지는 것과 같이 패널에서 **인쇄 관리자** 아이콘을 클릭하시면 **GNOME 인쇄 관리자**가 시작됩니다.

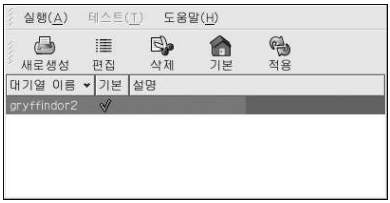

그림 27-13. GNOME 인쇄 관리자

패널에서 **주 메뉴 버튼** => **시스템 도구** => **인쇄 관리자**를 시작하는 방법도 있습니다.

프린터 설정을 변경하시려면, 프린터 아이콘에 오른쪽 클릭하신 후 **등록 정보**를 선택하시면 됩니다. **프린터 설정 도구**가 시작될 것입니다.

그림 27-14에서 보여진 것처럼 인쇄 스풀 대기열을 보시려면 설정된 프린터에 두번 클릭하시기 바랍니다.

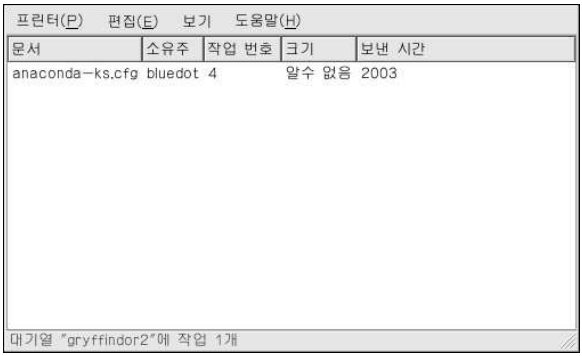

그림 27-14. 인쇄 작업 목록

GNOME 인쇄 관리자에 나타난 인쇄 작업 중 특정 작업을 취소하시려면, 목록에서 취소할 작업을 선택하신 후 풀다운 메뉴에서 **편집** => **문서 취소** 항목을 선택하시면 됩니다.

인쇄 스풀에 활성화된 인쇄 작업이 있다면, 그림 27-15에 나타난 것처럼 데스크탑 패널의 **패널 통지 영역**에 프린터 통지 아이콘이 나타납니다. 인쇄 관리자는 매 5초 마다 활성화된 인쇄 작업을 검색하기 때문에, 5초 내에 진행된 인쇄 작업은 아이콘으로 보여지지 않을 경우도 있습니다.

그림 27-15. 프린터 통지 아이콘

프린터 통지 아이콘에 클릭하시면 **GNOME 인쇄 관리자**가 시작되어 현재 대기 중인 인쇄 작업의 목록을 보여줍니다.

또한 패널을 보시면 **인쇄 관리자** 아이콘을 보실 수 있습니다. **Nautilus**에서 파일을 인쇄하시려면, 파일이 위치한 장소로 가서서 패널 상에 있는 **인쇄 관리자** 아이콘으로 그 파일을 끌어다 놓으시면 됩니다. 그림 27-16에서 보여지는 창이 나타날 것입니다. 파일 인쇄를 시작하시려면 **확인** 버튼을 클릭하시면 됩니다.

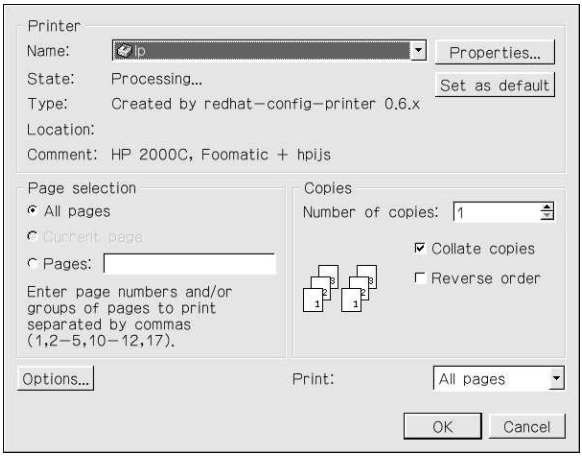

그림 27-16. 인쇄 검증 창

쉘 프롬프트에서 인쇄 스풀에 있는 인쇄 작업의 목록을 보시려면, `lpq` 명령을 입력하십시오. 마지막 몇 줄이 다음과 같이 나타날 것입니다:

```
Rank  Owner/ID      Class Job Files    Size Time
active user@localhost+902  A  902 sample.txt 2050 01:20:46
```

예 27-1. `lpq` 출력 결과 예시

인쇄 작업을 취소하시려면, `lpq` 명령을 사용하여 요청하신 작업 번호를 알아내신 후 `lprm` *`job number`* 명령을 사용하시면 됩니다. 예를 들어, `lprm 902` 명령을 입력하시면 예 27-1의 인쇄 작업이 취소될 것입니다. 인쇄 작업을 취소하기 위해서는 적절한 허가를 가지고 계셔야 합니다. 프린터가 연결된 컴퓨터에 직접 루트 사용자로 로그인하시지 않는 한, 다른 사용자가 시작한 인쇄 작업을 취소할 수 없습니다.

여러분은 또한 쉘 프롬프트에서 직접 파일을 인쇄하실 수 있습니다. 예를 들어, `lpr sample.txt` 명령을 입력하시면 `sample.txt` 텍스트 파일이 인쇄됩니다. 인쇄 필터는 파일의 유형을 알아낸 후 프린터가 인식하는 포맷으로 변환시킵니다.

27.13. 프린터 공유하기

CUPS 인쇄 시스템을 사용하시는 경우에만 **프린터 설정 도구**의 설정 옵션 공유 기능을 사용하실 수 있습니다. LPRng에서 설정 옵션을 공유하도록 설정하시려면, 27.13.1 절을 참조하시기 바랍니다.

네트워크 상에서 다른 컴퓨터를 사용하는 사용자가 여러분이 사용하시는 컴퓨터에 설정된 프린터로 인쇄할 수 있게 하는 것을 프린터를 공유한다라고 합니다. **프린터 설정 도구**를 사용하여 설정된 프린터들은 공유되지 않도록 기본 설정됩니다.

설정된 컴퓨터를 공유하시려면, **프린터 설정 도구**를 시작하신 후 목록에서 프린터를 선택하시기 바랍니다. 그 후 풀다운 메뉴에서 **실행** => **공유**를 선택하시면 됩니다.

알림

만일 프린터가 선택되지 않은 경우, **실행 => 공유**를 선택하시면 **일반** 탭에서 보여지는 시스템 차원의 공유 옵션만이 나타납니다.

대기열 탭에서 다른 사용자가 대기열을 볼 수 있도록 하는 옵션을 선택하시기 바랍니다.

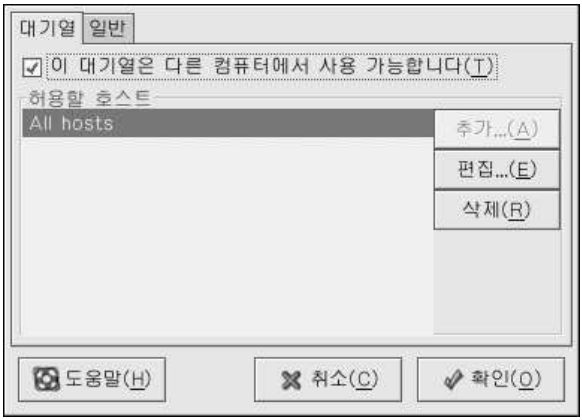

그림 27-17. 대기열 옵션

대기열을 공유하도록 선택하시면, 기본 값으로 모든 호스트가 공유 프린터로 인쇄할 수 있도록 허용됩니다. 그러나 네트워크상의 모든 시스템에서 대기열로 인쇄하도록 허용하는것은 위험합니다. 특히 시스템이 인터넷에 직접 연결된 경우에는 더욱 그러합니다. **모든 호스트** 항목을 선택하신 후 **편집** 버튼을 클릭하시면 그림 27-18에서 보여진 창이 나타납니다. 여기서 이 옵션을 변경하시길 권장합니다.

인쇄 서버 상에 방화벽을 설정하셨다면, 들어오는 UDP 포트, 631에서 접속을 보내고 받을 수 있도록 설정하셔야 합니다. 클라이언트 (인쇄 요청을 보내는 컴퓨터) 상에 방화벽을 설정하신 경우, 포트 631에서 접속을 보내고 수용하도록 설정하시기 바랍니다.

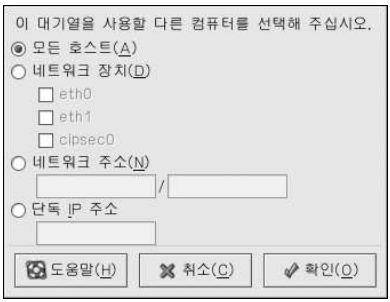

그림 27-18. 허용할 호스트

일반 탭에서는 **프린터 설정 도구**로는 볼 수 없는 프린터를 포함한 모든 프린터에 대한 셋팅을 설정할 수 있습니다. 다음과 같은 두 가지 옵션이 존재합니다:

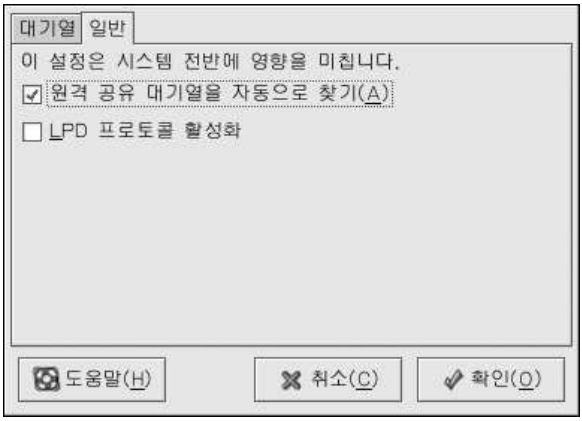

그림 27-19. 시스템 차원의 공유 옵션

- **원격 공유 대기열을 자동으로 찾기** — 기본으로 선택된 이 옵션은 IPP 탐색을 활성화 합니다. 즉, 네트워크 상의 다른 컴퓨터가 자신이 가진 대기열을 브로드캐스트한다면, 해당 시스템에서 사용 가능한 프린터 목록에 대기열이 자동으로 추가됩니다; IPP 탐색을 통해 발견된 프린터에는 추가 설정이 필요 없습니다. 이 옵션은 로컬 시스템 상에서 설정된 프린터들을 자동으로 공유하지는 않습니다.
- **LPD 프로토콜 활성화** — 이 옵션을 사용하여 프린터는 `xinetd` 서비스인 `cups-lpd` 서비스를 사용하는 LPD 프로토콜을 사용하도록 설정된 클라이언트로부터 인쇄 작업을 받을 수 있습니다.

경고

만일 이 옵션이 활성화된 경우, LPD 클라이언트에서 보내진 인쇄 작업이라면 모든 호스트로부터의 인쇄 작업을 받아들입니다.

27.13.1. LPRng을 사용하여 프린터 공유하기

LPRng 인쇄 시스템을 실행하신다면, 공유를 수동으로 설정해 주셔야 합니다. 네트워크 상에 연결된 시스템에서 Red Hat Linux 시스템 상에 설정된 프린터로 인쇄할 수 있도록 설정하시려면, 다음과 같은 단계를 따르시기 바랍니다:

1. `/etc/accepthost` 파일을 생성하십시오. 이 파일에서, 인쇄를 허용할 컴퓨터의 IP 주소 또는 호스트명을 한 줄에 한개씩 추가하시기 바랍니다.
2. `/etc/lpd.perms` 파일에서 다음과 같은 줄을 주석 해제하십시오:
   ```
   ACCEPT SERVICE=X REMOTEHOST=</etc/accepthost
   ```
3. 변경 사항이 적용되도록 데몬을 재시작하셔야 합니다:
   ```
   service lpd restart
   ```

27.14. 인쇄 시스템 교체하기

인쇄 시스템을 교체하시려면, **프린터 시스템 변환기** 프로그램을 실행하시기 바랍니다. 패널에서 **주 메뉴 버튼** => **시스템 설정** => **추가 시스템 설정** => **프린터 시스템 변환기**를 선택하시거나, 쉘 프롬프트 (예, XTerm 또는 GNOME 터미널)에서 `redhat-switch-printer` 명령을 입력하시면 됩니다.

이 프로그램은 X 윈도우 시스템의 실행 여부를 자동으로 인식합니다. 만일 X 윈도우 시스템이 실행 중이라면, 프로그램은 그림 27-20에서 보여지듯이 그래픽 모드에서 시작될 것입니다. 만일 그렇지 않다면, 텍스트 기반 모드에서 실행됩니다. 프로그램을 텍스트 모드로 시작하시려면, `redhat-switch-printer-nox` 명령을 사용하시기 바랍니다.

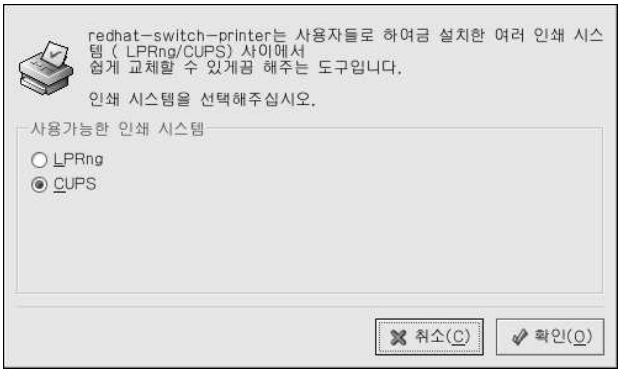

그림 27-20. 프린터 시스템 변환기

LPRng 또는 **CUPS** 인쇄 시스템을 선택하시기 바랍니다. Red Hat Linux 9에서는 CUPS가 디폴트 입니다. 한 개의 인쇄 시스템만 설치되어 있다면, 그 시스템만 옵션으로 나타날 것입니다.

인쇄 시스템을 교체하기 위해 **확인** 버튼을 클릭하신다면, 선택된 인쇄 데몬은 부팅시 시작되도록 활성화되며, 선택되지 않은 인쇄 데몬은 부팅시 시작되지 않도록 비활성화될 것입니다. 선택된 인쇄 데몬은 시작되고, 다른 인쇄 데몬은 멈춥니다; 따라서 변경 사항이 즉시 효력을 발생합니다.

27.15. 추가 자료

Red Hat Linux에서 인쇄 작업과 관련된 보다 많은 정보를 원하신다면, 다음과 같은 자료를 참조하시기 바랍니다.

27.15.1. 설치된 문서 자료

- `man printcap` — `/etc/printcap` 프린터 설정 파일의 메뉴얼 페이지.
- `map lpr` — 명령행에서 파일을 인쇄하는 `lpr` 명령에 대한 메뉴얼 페이지.
- `man lpd` — LPRng 프린터 데몬의 메뉴얼 페이지.
- `man lprm` — LPRng 스풀 대기열에서 인쇄 작업을 삭제하는데 사용되는 명령행 유틸리티의 메뉴얼 페이지.
- `man mpage` — 종이 한장에 여러 페이지를 인쇄하는데 사용되는 명령행 유틸리티의 메뉴얼 페이지.
- `man cupsd` — CUPS 프린터 데몬의 메뉴얼 페이지.
- `man cupsd.conf` — CUPS 프린터 데몬 설정 파일의 메뉴얼 페이지.
- `man classes.conf` — CUPS 용 클래스(class) 설정 파일의 메뉴얼 페이지.

27.15.2. 유용한 웹사이트

- http://www.linuxprinting.org — *GNU/Linux Printing*에는 리눅스에서 인쇄하기와 관련된 많은 정보가 포함되어 있습니다.
- http://www.cups.org/ — 문서 자료, FAQ와 CUPS 관련 뉴스 그룹.

redhat.

28장 .

자동화 작업

리눅스 환경에서 지정 날짜, 시간에 또는 시스템 부하 평균이 지정된 숫자 이하로 내려갈때 작업이 자동으로 실행되도록 설정 가능합니다. Red Hat Linux는 중요한 시스템 작업이 자동으로 실행되어 시스템을 업데이트 하도록 미리 설정해 놓았습니다. 예를 들어 `locate` 명령을 사용하여 slocate 데이터베이스는 매일 업데이트 됩니다. 시스템 관리자는 자동화 작업을 사용하여 주기적인 백업, 시스템 감시, 사용자 정의 스크립트 실행과 같은 여러 다양한 작업을 수행할 수 있습니다.

Red Hat Linux에는 다음과 같은 4가지 자동화 작업 유틸리티가 있습니다: `cron`, `anacron`, `at`, `batch`.

28.1. Cron

Cron은 정해진 시간, 일, 월, 주마다 반복적인 작업을 실행하도록 스케줄하는데 사용되는 데몬입니다.

Cron은 시스템이 계속적으로 켜져있을 경우에만 작동합니다. 만일 작업이 스케줄된 시간에 시스템이 꺼져있다면 그 작업은 실행되지 않습니다. 작업이 특정 시간에 실행되지 않고 일정 시간 마다 주기적으로 실행되도록 하시려면 28.2 절을 참조하시기 바랍니다. 한번만 실행되는 (one-time) 작업을 스케줄하기 위해서는 28.3 절을 참조해 보십시오.

cron 서비스를 사용하기 위해서는 반드시 `vixie-cron` RPM 패키지가 설치되어 있으며 `crond` 서비스가 실행 중이어야 합니다. 패키지 설치 여부를 알아보기 위해서는 `rpm -q vixie-cron` 명령을 사용합니다. 서비스 실행 여부를 알아보기 위해서는 `/sbin/service crond status` 명령을 사용하십시오.

28.1.1. Cron 작업 설정하기

주요 cron 설정 파일인 `/etc/crontab`에는 다음과 같은 줄이 포함되어 있습니다:

```
SHELL=/bin/bash
PATH=/sbin:/bin:/usr/sbin:/usr/bin
MAILTO=root
HOME=/

# run-parts
01 * * * * root run-parts /etc/cron.hourly
02 4 * * * root run-parts /etc/cron.daily
22 4 * * 0 root run-parts /etc/cron.weekly
42 4 1 * * root run-parts /etc/cron.monthly
```

처음 4 줄은 cron 작업이 실행되는 환경을 설정하기 위해 사용된 변수들입니다. `SHELL` 변수값은 시스템이 사용할 쉘 환경의 종류 (위의 예시에서는 bash shell)를 지시합니다. 그리고 `PATH` 변수는 명령 실행 경로를 정의합니다. cron 작업의 결과는 `MAILTO` 변수에 정의된 사용자에게 이메일로 보내집니다. 만일 `MAILTO` 변수가 공백 문자열(`MAILTO=""`)로 정의된다면, 이메일을 보내지 않습니다. `HOME` 변수는 명령이나 스크립트를 실행할 때 사용할 홈 디렉토리를 설정하는데 사용됩니다.

`/etc/crontab` 파일에서 개별 라인은 실행할 작업을 나타내며 다음과 같은 형식을 갖습니다:

```
minute hour day month dayofweek command
```

- `minute` — 0 과 59 사이의 정수
- `hour` — 0 과 23 사이의 정수
- `day` — 1 과 31 사이의 정수 (지정된 월에 맞는 유효한 날짜일 것.)

- `month` — 1 과 12 사이의 정수 (또는 월 이름의 약자. 예, jan, feb, 등)
- `dayofweek` — 0과 7 사이의 정수, 여기서 0 또는 7 은 일요일을 의미함 (또는 주 이름의 약자. 예, sun, mon 등)
- `command` — 실행할 명령어 (`ls /proc >> /tmp/proc`와 같은 명령어 또는 사용자가 직접 작성한 사용자 정의된 스크립트를 실행할 명령어).

앞에서 언급된 값에서 별표 (*)를 사용하시면 모든 유효값을 지정합니다. 예를 들어, 월 대신 별표를 지정한다면 다른 값의 범위 안에서 매달마다 명령을 실행하게 됩니다.

정수 값 사이에 하이픈 (-)을 사용하여 정수값의 범위를 지정할 수 있습니다. 예를 들어, **`1-4`**는 정수값 1, 2, 3, 4를 의미합니다.

콤마 (,)로 구분된 값은 목록을 지정합니다. 예, **`3, 4, 6, 8`**는 4개의 특정 정수를 나타냅니다.

슬래시 (/)를 사용하여 주기값을 지정할 수 있습니다. 정수 값은 **`/<integer>`** 다음에 나온 범위만큼 감소됩니다. 예를 들어 **`0-59/2`**를 사용하여 매 2분마다 작업이 실행되도록 정의할 수 있습니다. 주기값은 또한 별표와 함께 사용될 수도 있습니다. 예로서 **`*/3`** 값을 사용하여 매 3달마다 작업이 실행되도록 설정할 수 있습니다.

우물정자 표시 (#)로 시작하는 줄은 모두 주석 처리되어 실행되지 않습니다.

`/etc/crontab` 파일에서 볼 수 있듯이 이 파일은 `run-parts` 스크립트를 사용하여 매 시간, 매일, 매주 또는 매월 단위로 `/etc/cron.hourly`, `/etc/cron.daily`, `/etc/cron.weekly`, `/etc/cron.monthly` 디렉토리에 작성된 스크립트를 실행합니다. 이 디렉토리에 속한 파일은 모두 쉘 스크립트로 작성됩니다.

시간, 일, 주, 월 단위로 실행되는 작업 이외의 스케줄에 맞추어 실행될 cron 작업이 필요하다면, `/etc/cron.d` 디렉토리에 추가합니다. 이 디렉토리 안의 모든 파일은 `/etc/crontab`와 동일한 구문을 사용합니다. 예 28-1에 나온 예시를 참조하시기 바랍니다.

```
# record the memory usage of the system every monday
# at 3:30AM in the file /tmp/meminfo
30 3 * * mon cat /proc/meminfo >> /tmp/meminfo
# run custom script the first day of every month at 4:10AM
10 4 1 * * /root/scripts/backup.sh
```

예 28-1. Crontab 예시

루트 이외의 사용자는 `crontab` 유틸리티를 사용하여 cron 작업을 설정할 수 있습니다. 사용자 정의된 모든 crontab 파일은 `/var/spool/cron` 디렉토리에 저장되며 crontab을 생성한 사용자명을 사용하여 실행할 수 있습니다. 일반 사용자로서 crontab을 생성하기 위해서는 해당 사용자로 로그인하신 후 `crontab -e` 명령을 사용하여 사용자의 crontab을 편집합니다. 편집을 위해서는 `VISUAL` 또는 `EDITOR` 환경 변수에 지정된 편집기를 사용하십시오. 파일은 `/etc/crontab` 파일과 같은 형식을 사용합니다. crontab의 변경 사항을 저장하면 crontab은 사용자명에 따라 저장되어 `/var/spool/cron/`*`username`* 파일에 기록됩니다.

cron 데몬은 매 분마다 `/etc/crontab` 파일, `/etc/cron.d/` 디렉토리와 `/var/spool/cron` 디렉토리가 변경되었는지를 확인합니다. 만일 변경된 사항이 발견되면, 변경 사항은 메모리로 로드됩니다. 따라서 crontab 파일이 변경된 경우에도 데몬을 재시할 필요가 없습니다.

28.1.2. Cron으로 접근을 통제하기

`/etc/cron.allow` 와 `/etc/cron.deny` 파일을 사용하여 cron으로 접근을 제한할 수 있습니다. 이 접근 통제 파일은 각각의 줄마다 한개의 사용자명을 갖습니다. 접근 통제 파일이 수정되어도 cron 데몬 (crond)을 재시작하실 필요가 없습니다. 사용자가 cron 작업을 추가하거나 삭제하려고 할 때마다 액세스 통제 파일이 읽혀집니다.

루트 사용자는 접근 통제 파일의 목록에 사용자명이 포함되지 않아도 항상 cron을 사용할 수 있습니다.

만일 `cron.allow` 파일이 존재한다면, 이 파일에 나열된 사용자만 cron을 사용할 수 있으며 `cron.deny` 파일은 무시됩니다.

만일 cron.allow 파일이 존재하지 않는다면 cron.deny 파일에 지정된 사용자는 cron을 사용할 수 없습니다.

28.1.3. 서비스 시작과 정지

cron 서비스를 시작하시려면 /sbin/service crond start 명령을 사용합니다. 서비스를 정지하려면 /sbin/service crond stop 명령을 사용하시면 됩니다. 부팅시 서비스를 시작하는 것이 좋습니다. 부팅시 자동으로 cron 서비스를 시작하는 방법에 대한 자세한 정보는 14 장를 참조하시기 바랍니다.

28.2. Anacron

Anacron는 작업 스케줄러로서 cron과 유사하지만 시스템이 계속적으로 켜져있지 않아도 작동하는 차이점이 갖습니다. anacron은 보통 cron에 의해 수행되는 매일, 매주와 매월 작업을 실행하기 위하여 사용됩니다.

Anacron 서비스를 사용하기 위해서는 anacron RPM 패키지가 설치되어 있어야 하며 anacron 서비스가 실행 중이어야 합니다. 패키지가 설치되었는지 여부를 확인하기 위해서는 rpm -q anacron 명령을 사용합니다. 서비스 실행 여부는 /sbin/service anacron status 명령을 통하여 알아볼 수 있습니다.

28.2.1. Anacron 작업 설정하기

/etc/anacrontab 설정 파일에 Anacron 작업 목록이 담겨있습니다. 설정 파일의 각각의 줄은 한가지 작업에 상응하며 다음과 같은 형식을 갖습니다:

```
period delay job-identifier command
```

- period — 명령을 실행할 주기 (하루 단위)
- delay — 분 당 지체 시간
- job-identifier — Anacron 메시지에서 작업의 타임스탬프 파일로서 사용되는 작업 식별자. 공백 이외의 문자는 모두 포함 가능합니다. (슬래시 제외)
- command — 실행할 명령

Anacron은 설정 파일의 period 항목에 지정된 주기 내에서 개별 작업들이 실행되었는지를 확인합니다. 만일 주어진 주기에 작업이 실행되지 않았다면 Anacron은 delay 영역에서 지정된 지체 시간 (분 단위)만큼 대기 후 command 영역에서 지정된 명령을 실행합니다.

작업이 완료된 후 Anacron은 /var/spool/anacron 디렉토리에 있는 타임스탬프 파일에 날짜를 기록합니다. (시간을 빼고) 날짜만 사용되며 job-identifier의 값은 타임스탬프 파일의 파일명으로 사용됩니다.

SHELL과 PATH와 같은 환경 변수들은 cron 설정 파일과 마찬가지로 /etc/anacrontab 파일의 시작 부분에 정의됩니다.

기본 설정 파일은 다음과 유사합니다:

```
# /etc/anacrontab: configuration file for anacron

# See anacron(8) and anacrontab(5) for details.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# These entries are useful for a Red Hat Linux system.
1   5   cron.daily      run-parts /etc/cron.daily
```

```
7   10   cron.weekly      run-parts /etc/cron.weekly
30   15   cron.monthly     run-parts /etc/cron.monthly
```

그림 28-1. 기본 anacrontab

그림 28-1에서 볼 수 있듯이 Red Hat Linux에서 anacron은 매일, 매주, 매월 실행되는 cron 작업이 제대로 실행되는지 확인하도록 설정되었습니다.

28.2.2. 서비스 시작과 정지

anacron 서비스를 시작하시려면 `/sbin/service anacron start` 명령을 사용합니다. 서비스를 정지하려면 `/sbin/service anacron stop` 명령을 사용합니다. 부팅시 서비스를 시작하기를 권장합니다. 부팅시 자동으로 anacron 서비스를 시작하는 방법에 대한 자세한 정보는 14 장을 참조하시기 바랍니다.

28.3. At와 Batch

cron 과 anacron은 반복되는 작업을 스케줄하기 위해 사용된 반면에 `at` 명령은 특정 시간에 한번 실행될 작업을 스케줄하기 위해 사용됩니다. `batch` 명령은 시스템 부하 평균이 0.8 이하로 떨어질 경우 한번 실행될 작업을 스케줄하는데 사용됩니다.

`at` 또는 `batch` 명령을 사용하기 위해서는 `at` RPM 패키지를 설치되어 있어야 하며 `atd` 서비스가 실행 중이어야 합니다. `rpm -q at` 명령을 사용하여 패키지가 설치되었는지 여부를 알아봅니다. 서비스가 실행 중인지 알아보기 위해서는 `/sbin/service atd status` 명령을 사용합니다.

28.3.1. At 작업 설정하기

특정 시간에 한번 실행되는 작업을 스케줄하기 위해서는 `at` ***`time`*** 명령을 입력합니다. 여기서 ***`time`***은 명령을 실행할 시간을 의미합니다.

`time`에는 다음 중 한가지 인자를 사용할 수 있습니다:

- HH:MM 형식 — 예로 들면 04:00는 4:00AM을 지정합니다. 만일 시간이 이미 지났으면, 다음날 지정된 시간에 작업을 실행합니다.
- midnight — 12:00AM 지정.
- noon — 12:00PM 지정.
- teatime — 4:00PM 지정.
- month-name day year 형식 — 예로 들면, January 15 2002는 2002년 1월의 15번째 날을 의미합니다. 년도수는 옵션입니다.
- MMDDYY, MM/DD/YY, 또는 MM.DD.YY 형식 — 예로 들면, 011502는 2002년 1월의 15번째 날을 의미합니다.
- now + time — 시간은 분, 시, 일 또는 주단위입니다. 예로서 now + 5 days라고 지정되면 명령은 5일 후 같은 시간에 실행됩니다.

시간을 먼저 지정 후 옵션인 날짜를 지정합니다. 시간 형식에 대한 보다 많은 정보를 원하신다면, `/usr/share/doc/at-`*`<version>`*`/timespec` 텍스트 파일을 참조해 보십시오.

시간 인자와 함께 `at` 명령을 입력하면 `at>` 프롬프트가 출력됩니다. 실행할 명령을 입력 후 [Enter]를 치고 Ctrl-D를 입력합니다. 각각의 명령어를 입력한 후 [Enter] 키를 쳐서 더 많은 명령어를 지정할 수 있습니다. 모든 명령어 입력이 끝나면 [Enter]를 눌러 빈 칸으로 이동한 후 Ctrl-D를 입력합니다. 다른 방법으로는 프롬프트에서 쉘 스크립트를 입력할 수도 있습니다. 스크립트의 개별 라인을 입력 후 [Enter] 키를 치고 빈 칸에서 Ctrl-D를 눌러 빠져나옵니다. 만일 스크립트가 입력되면, 사용자의 SHELL 환경과 로그인 쉘 또는 `/bin/sh`의 쉘 중에서 제일 먼저 발견된 쉘이 사용됩니다.

명령어나 스크립트로 정보를 표준 출력하면, 출력 결과는 사용자에게 이메일로 전달됩니다.

이후 실행할 작업을 보기 위해서는 `atq` 명령을 사용합니다. 보다 많은 정보를 원하시면 28.3.3 절을 참조해 주십시오.

`at` 명령을 제한하여 사용할 수 있습니다. 자세한 사항은 28.3.5 절을 참조하십시오.

28.3.2. Batch 작업 설정하기

부하 평균이 0.8 이하로 내려갈 경우 한번 작업을 실행하기 위해서는 `batch` 명령을 사용합니다.

`batch` 명령을 입력하면 `at>` 프롬프트가 출력됩니다. 실행할 명령을 입력 후 [Enter]를 치고 Ctrl-D를 입력합니다. 각각의 명령어를 입력한 후 [Enter] 키를 쳐서 더 많은 명령어를 지정할 수 있습니다. 모든 명령어 입력이 끝나면 [Enter]를 눌러 빈 칸으로 이동한 후 Ctrl-D를 입력합니다. 다른 방법으로는, 프롬프트에서 쉘 스크립트를 입력할 수도 있습니다. 스크립트 각각의 라인을 입력 후 [Enter] 키를 치고 빈칸에서 Ctrl-D를 눌러 빠져나옵니다. 만일 스크립트가 입력되면, 사용자의 SHELL 환경과 로그인 쉘 또는 `/bin/sh` 쉘 중에서 제일 먼저 발견된 쉘이 사용됩니다. 부하 평균이 0.8 이하로 떨어지는 즉시 명령어나 스크립트 세트가 실행될 것입니다.

명령어나 스크립트로 정보를 표준 출력하면, 출력 결과는 사용자에게 이메일로 전달됩니다.

이후 실행할 작업을 보기 위해서는 `atq` 명령을 사용합니다. 보다 많은 정보를 원하시면 28.3.3 절을 참조해 주십시오.

`batch` 명령을 제한하여 사용할 수 있습니다. 자세한 사항은 28.3.5 절을 참조하십시오.

28.3.3. 이후 실행할 작업 보기

이후 실행할 `at`와 `batch` 작업을 보시려면 `atq` 명령어를 사용하십시오. 출력 형식은 각 작업당 한 줄로 직업 번호, 날짜, 시간, 작업 구분과 사용자명 순입니다. 사용자는 오직 자신이 소유한 작업만을 볼 수 있습니다. 만일 루트 사용자가 `atq` 명령을 실행하면 모든 사용자의 작업 목록을 보여줍니다.

28.3.4. 추가 명령행 옵션

`at`와 `batch`에 대한 추가 명령행 옵션은 다음과 같습니다:

옵션	설명
`-f`	명령어나 쉘 스크립트를 프롬프트에서 지정하지 않고 대신 파일에서 읽어옴.
`-m`	작업이 완료되면 사용자에게 이메일을 보냄.
`-v`	작업이 수행될 시간을 보여줌.

표 28-1. `at`와 `batch` 명령행 옵션

28.3.5. At와 Batch로의 접근 통제하기

`/etc/at.allow`와 `/etc/at.deny` 파일을 사용하여 `at`와 `batch`로의 접근을 제한할 수 있습니다. 이 접근 통제 파일은 각각의 줄마다 하나의 사용자명이 있는 형식을 갖습니다. 이 두 파일에서 빈 공간은 허용되지 않습니다. 접근 통제 파일이 수정되더라도 `at` 데몬 (`atd`)을 재시작할 필요가 없습니다. `at` 또는 `batch` 명령이 실행될 때마다 접근 통제 파일이 읽혀집니다.

루트 사용자는 액세스 통제 파일에 상관없이 언제든지 `at`와 `batch` 명령어를 실행할 수 있습니다.

만일 `at.allow` 파일이 존재한다면 이 파일에 포함된 사용자만이 `at` 또는 `batch` 명령을 사용할 수 있으며 `at.deny` 파일은 무시됩니다.

만일 `at.allow` 파일이 존재하지 않는다면, `at.deny`에 포함된 모든 사용자는 `at` 또는 `batch` 명령을 사용할 수 없습니다.

28.3.6. 서비스 시작과 정지

`/sbin/service atd start` 명령을 사용하여 `at` 서비스를 시작합니다. 서비스를 정지하려면 `/sbin/service atd stop` 명령을 사용합니다. 부팅시 서비스를 시작하실 것을 권장합니다. 부팅시 자동으로 cron 서비스를 시작하는 방법에 대한 자세한 정보는 14 장을 참조하시기 바랍니다.

28.4. 추가 자료

자동화 작업을 설정하는 방법에 대한 보다 많은 정보를 원하신다면, 다음의 자료를 참조하시기 바랍니다.

28.4.1. 설치된 문서 자료

- `cron` 메뉴얼 페이지 — cron 개요.
- `crontab` 메뉴얼 페이지의 섹션 1 과 5 — 섹션 1에는 `crontab` 파일에 대한 개요가 포함됩니다. 메뉴얼 페이지 섹션 5에서는 파일 형식과 일부 예시 항목이 설명되어 있습니다.
- `/usr/share/doc/at-<version>/timespec`에는 cron 작업에 지정 가능한 시간 유형에 대한 자세한 정보가 포함되어 있습니다.
- `anacron` 메뉴얼 페이지 — anacron에 대한 설명과 명령행 옵션.
- `anacrontab` 메뉴얼 페이지 — anacron 설정 파일에 대한 개요.
- `/usr/share/doc/anacron-<version>/README` — Anacron과 사용 이유에 대한 설명.
- `at` 메뉴얼 페이지 — `at`와 `batch` 명령과 명령행 옵션에 대한 설명.

29장 . 로그 파일

로그 파일 *(Log file)*이란 커널, 서비스 및 실행 중인 응용 프로그램과 같은 시스템 관련 메시지를 포함하는 파일을 의미합니다. 정보의 종류에 따라서 다른 로그 파일이 존재합니다. 예로 들면, 기본 시스템 로그 파일 및 보안 메시지 용 로그 파일, 크론(cron) 작업 용 로그 파일과 같은 여러 가지 로그 파일이 있습니다.

로그 파일은 시스템 상의 문제를 해결하려고 하실 때 (예, 커널 드라이버를 로드하거나 시스템으로 허가되지 않은 로그인 시도에 대한 로그를 찾으실 때) 유용하게 사용됩니다. 이 장에서는 로그 파일이 저장된 위치와 로그 파일을 보는 방법 및 로그 파일에서 중요한 정보를 찾는 방법에 대하여 다루어 보겠습니다.

`syslogd`라고 불리는 데몬은 일부 로그 파일을 관리하며, `syslogd` 데몬이 관리하는 로그 메시지 목록은 `/etc/syslog.conf` 설정 파일에 위치합니다.

29.1. 로그 파일 찾기

대부분의 로그 파일은 `/var/log` 디렉토리에 위치합니다. `httpd` 및 `samba`와 같은 일부 응용 프로그램은 `/var/log` 디렉토리 내에 해당 응용 프로그램에 대한 로그 파일을 저장하는 독자적인 디렉토리를 갖습니다.

로그 디렉토리에 위치한 대부분의 파일명 끝에는 숫자가 옵니다. 로그 파일은 순환 (rotate: 주기적으로 파일을 새로 생성)하여 오래된 정보를 없애고, 디스크가 차는 것을 막습니다. 이렇게 로그 파일이 순환할 때마다 파일명 다음에 새로운 숫자를 부여합니다. `logrotate` 패키지에는 `/etc/logrotate.conf` 설정 파일과 `/etc/logrotate.d` 디렉토리에 속한 설정 파일에 따라서 로그 파일을 자동으로 순환시키는 크론(cron) 작업이 포함되어 있습니다. 기본 값으로, 로그 파일은 매주 순환되며 이전 로그 파일은 4 주 동안 보존됩니다.

29.2. 로그 파일 보기

대부분의 로그 파일은 평문 (plain text) 형식입니다. 따라서 **Vi** 또는 **Emacs**와 같은 텍스트 편집기를 사용하여 로그 파일을 보실 수 있습니다. 일부 로그 파일은 모든 사용자가 읽기 가능하지만; 대부분의 로그 파일은 루트 사용자만 읽기 가능합니다.

상호 대화식, 실시간 응용 프로그램을 사용하여 시스템 로그 파일을 보시려면, **로그 보기 프로그램**를 사용하십시오. 이 응용 프로그램을 시작하기 위해서는, 패널에서 **주 메뉴 버튼** => **시스템 도구** => **시스템 로그**를 선택하시거나, 쉘 프롬프트에서 `redhat-logviewer` 명령을 입력하시면 됩니다.

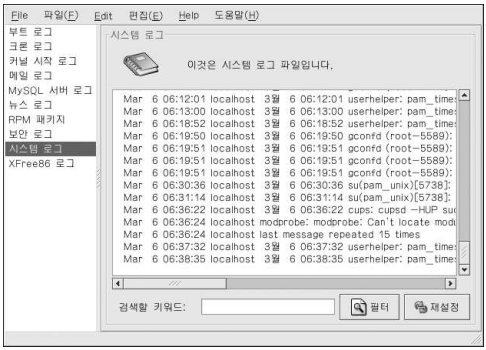

그림 29-1. 로그 보기 프로그램

이 응용 프로그램은 현재 존재하는 로그 파일만을 보여줍니다; 따라서, 여러분이 가지고 계신 로그 파일 목록과 그림 29-1에 나타난 목록이 다르게 나타날 수도 있습니다. 전체 로그 파일 목록을 보시려면, `/etc/sysconfig/redhat-logviewer` 설정 파일을 참조하시기 바랍니다.

현재 볼 수 있는 로그 파일은 30초 마다 갱신되도록 기본 설정되어 있습니다. 갱신 주기를 변경하시려면, **편집** 풀다운 메뉴에서 => **기본 설정**을 선택해 주십시오. 그림 29-2에서 보여지는 화면이 나타날 것입니다. **로그 파일** 탭에서 위/아래 화살표를 클릭하여 로그 파일 갱신 주기를 변경 가능합니다. 기본 창으로 되돌아 가기 위해 **닫기** 버튼을 클릭하시면 갱신 주기가 즉시 변경됩니다. 현재 보여지는 파일을 수동으로 갱신하시려면, **파일** => **지금 갱신** 항목을 선택하시거나 또는 [Ctrl]-[R] 키조합을 눌러 주십시오.

키워드를 이용하여 로그 파일의 내용을 검색하시려면, 찾고자 하는 단어를 **검색할 키워드** 텍스트 영역에 입력해 주신 후 **필터** 버튼을 클릭하시기 바랍니다. 내용을 다시 설정하시려면 **재설정** 버튼을 클릭해 주십시오.

로그 파일 탭에서 로그 파일이 위치한 경로도 변경 가능합니다. 목록에서 로그 파일을 선택하신 후 **위치 변경** 버튼을 클릭해 주십시오. 로그 파일에 대한 새로운 위치를 직접 입력하시거나 **검색** 버튼을 클릭하여 파일 선택 대화창을 이용하여 파일 위치를 지정하실 수 있습니다. 파일의 위치를 지정하신 후 **확인**을 클릭하여 기본 설정 화면으로 되돌아오신 후 **닫기** 버튼을 클릭하여 기본 화면으로 갑니다.

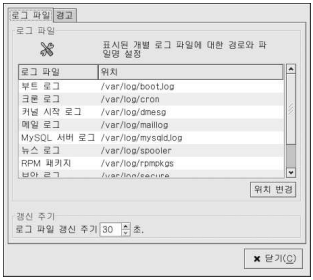

그림 29-2. 로그 파일 위치

29.3. 로그 파일 조사하기

로그 보기 프로그램를 사용하여 경고 단어를 포함한 줄에 경고 아이콘을 보여주도록 설정 가능합니다. 경고 단어를 삽입하시려면, **편집** 풀다운 메뉴에서 => **기본 설정**을 선택하신 후 **경고** 탭에 클릭해 주십시오. **추가** 버튼을 클릭하신 후 경고 단어 목록에 추가할 단어를 입력하시면 됩니다. 경고 단어를 삭제하시려면, 목록에서 해당 단어를 선택하신 후 **삭제** 버튼을 클릭하시기 바랍니다.

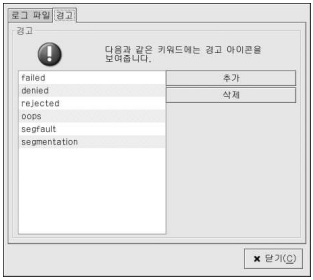

그림 29-3. 경고

30장 . 커널 업그레이드

Red Hat Linux 커널은 커널 자체의 완결성과 지원 하드웨어와의 호환성 보증을 위하여 Red Hat 커널팀에 의해 맞춤 개발됩니다. Red Hat은 엄밀한 품질 보증 테스트를 거친 후에 커널을 출시합니다.

Red Hat Linux 커널은 RPM 형식으로 패키지화 되어있기 때문에 커널을 쉽게 업그레이드하고 검증할 수 있습니다. 예를 들어, Red Hat, Inc.에서 배포판 `kernel` RPM 패키지를 설치하시면, `initrd` 이미지가 생성됩니다; 따라서 다른 커널을 설치 후 `mkinitrd` 명령을 사용할 필요가 없습니다. 또한 GRUB이나 LILO가 설치된 경우, 부트로더가 새로운 커널을 부팅하도록 부트로더 설정 파일을 수정합니다.

이 장에서는 x86 시스템 상에서 커널을 업그레이드하는데 필요한 단계에 대하여 설명해 보겠습니다.

경고

Red Hat Linux 설치 지원팀은 맞춤 커널 개발에 대한 제원을 제공하지 않습니다. 소스 코드로 맞춤 커널을 개발하는 방법에 대한 보다 자세한 정보를 원하신다면, 부록 A을 참조하시기 바랍니다.

30.1. 2.4 커널

Red Hat Linux에는 사용자 정의 2.4 커널이 포함되어 있으며, 이 커널은 다음과 같은 기능을 제공합니다:

- 커널 소스는 `/usr/src/linux/` 디렉토리가 아닌 `/usr/src/linux-2.4/`에 위치합니다.
- ext3 파일 시스템 지원.
- 멀티-프로세서 (SMP) 지원.
- USB 지원.
- FireWire™라고도 부르는 IEEE 1394 장치에 대한 예비 지원.

30.2. 업그레이드 준비

커널을 업그레이드하기 전에 따르셔야할 몇가지 단계들이 있습니다. 첫번째 단계는 문제가 발생할 시에 대비하여 시스템을 부팅할 부팅 디스켓이 있는지 확인하시는 것입니다. 만일 부트로더가 새로운 커널을 부트할 수 있도록 적절히 설정되지 않은 경우에는, 부팅 디스켓이 준비되어 있지 않다면 Red Hat Linux 시스템을 부팅하실 수 없습니다.

부팅 디스켓을 만드시려면, 쉘 프롬프트에서 루트로 로그인 하신 후 다음 명령을 입력하시기 바랍니다:

```
/sbin/mkbootdisk `uname -r`
```

힌트

보다 많은 옵션에 대한 정보를 원하시면, `mkbootdisk` 명령어의 메뉴얼 페이지를 참조하시기 바랍니다.

부팅 디스켓이 제대로 작동하는지 확인해 보기 위하여, 만드신 부팅 디스켓을 사용하여 컴퓨터를 재부팅해 보신 후 다음 단계로 진행하시기 바랍니다.

부팅 디스켓을 사용할 상황이 발생하지 않기를 바라지만 혹시라도 모르니 부팅 디스켓을 안전한 장소에 보관해 두십시오.

어떠한 커널 패키지가 설치되어 있는지 알아보시려면, 쉘 프롬프트에서 다음 명령을 실행하십시오:

```
rpm -qa | grep kernel
```

수행하신 설치 유형에 따라서 다음 중 일부 또는 모든 패키지가 출력 결과에 나타날 것입니다 (버전 번호와 패키지 이름이 다를 수 있습니다):

```
kernel-2.4.20-2.47.1
kernel-debug-2.4.20-2.47.1
kernel-source-2.4.20-2.47.1
kernel-doc-2.4.20-2.47.1
kernel-pcmcia-cs-3.1.31-13
kernel-smp-2.4.20-2.47.1
```

출력 결과를 보시고 커널 업그레이드를 위하여 다운로드 받아야할 패키지의 종류를 결정하실 수 있습니다. 단독 프로세서 시스템의 경우, `kernel` 패키지만 필요합니다.

한 개 이상의 프로세서를 갖춘 컴퓨터의 경우, 다중 프로세서를 지원하는 `kernel-smp` 패키지를 설치하셔야 합니다. 다중 프로세서 커널이 여러분의 시스템에서 제대로 작동하지 않을 경우를 대비하여 `kernel` 패키지도 설치하실 것을 권장합니다.

4 기가바이트 이상의 메모리를 지닌 컴퓨터를 가지고 계신 경우에는 `kernel-bigmem` 패키지를 설치하셔야 합니다. 다시 한번 디버깅 목적으로 `kernel` 패키지를 설치하실 것을 권장합니다. `kernel-bigmem` 패키지는 i686 구조에서만 사용되도록 개발되었습니다.

만일 PCMCIA 지원이 필요한 경우 (예, 랩탑), `kernel-pcmcia-cs` 패키지도 필요합니다.

여러분이 스스로 커널을 재컴파일하거나 개발할 계획이 없으시다면 `kernel-source` 패키지는 필요 없습니다.

`kernel-doc` 패키지는 커널 개발 문서를 포함하고 있으며 필요하지 않습니다. 커널 개발에 사용되는 시스템에서는 이 패키지를 사용하시기 바랍니다.

`kernel-util` 패키지는 커널이나 시스템 하드웨어를 제어하는데 사용되는 유틸리티를 포함하고 있으며 필요하지 않습니다.

Red Hat은 여러 다른 x86 버전을 위한 최적화된 커널을 개발합니다. AMD Athlon™ 과 AMD Duron™ 시스템에는 `athlon`, Intel® Pentium® II, Intel® Pentium® III, Intel® Pentium® 4 시스템에는 `i686`, 그리고 Intel® Pentium®와 AMD K6™ 시스템에는 `i586` 버전이 사용됩니다. 가지고 계신 x86 시스템의 버전이 확실하지 않다면, `i386` 버전을 위해 개발된 커널을 사용하십시오; 이 커널은 모든 x86-기반 시스템에서 사용 가능하도록 개발되었습니다.

x86 버전의 RPM 패키지는 파일명에 포함되어 있습니다. 예로 들면, `kernel-2.4.20-2.47.1.athlon.rpm`은 AMD Athlon™과 AMD Duron™ 시스템을 위해 최적화되었으며, `kernel-2.4.20-2.47.1.i686.rpm` 파일은 Intel® Pentium® II, Intel® Pentium® III, Intel® Pentium® 4 시스템에 최적화되었습니다. 커널을 업그레이드하기 위해 필요한 패키지의 종류를 결정하셨다면, `kernel`, `kernel-smp`, `kernel-bigmem` 패키지에 맞는 적절한 구조를 선택하십시오. 다른 패키지들은 `i386` 버전을 사용합니다.

30.3. 업그레이드된 커널 다운로드 받기

다음과 같은 몇가지 방법을 사용하여 여러분의 시스템에 사용가능한 업데이트된 커널이 있는지 알아낼 수 있습니다.

- http://www.redhat.com/apps/support/errata/ 사이트로 가셔서, 사용하시는 Red Hat Linux 버전을 선택하시고 그 버전에 대한 에라타를 살펴보십시오. 커널 에라타는 보통 **Security Advisories** (보안 권고) 섹션 밑에서 찾으실 수 있습니다. 에라타 항목에서 커널 에라타를 클릭하셔서 자세한 에라타 리포트를 보실 수

있습니다. 에라타 리포트에는 필수 RPM 패키지 목록과 그 패키지를 다운로드 받을 수 있는 Red Hat FTP 사이트로의 링크가 포함되어 있습니다. 또한 Red Hat FTP 미러 사이트에서 그 패키지를 다운로드받는 것도 가능합니다. 미러 사이트 목록은 http://www.redhat.com/download/mirror.html 사이트에서 찾으실 수 있습니다.

- Red Hat Network를 사용하여 커널 RPM 패키지를 다운로드 받으신 후 설치하십시오. Red Hat Network는 최신 커널을 다운로드 받아서, 시스템 상의 커널을 업그레이드하고, 만일 필요하다면 초기 RAM 디스크를 생성하고 새로운 커널을 부팅할 수 있도록 부트로더를 설정합니다. 보다 자세한 정보는 http://www.redhat.com/docs/manuals/RHNetwork/ 사이트에서 *Red Hat Network* 사용자 참조 가이드를 참조하시기 바랍니다.

Red Hat Linux 에라타 페이지에서 RPM 패키지를 다운로드 받으셨거나 Red Hat Network가 패키지를 다운로드받는 목적으로만 사용되었다면, 30.4 절으로 넘어 가십시오. 만일 Red Hat Network를 사용하여 업데이트된 커널을 다운로드 받은 후 설치하셨다면, 30.5 절과 30.6 절에서 설명된 지시 사항을 따르시기 바랍니다. Red Hat Network는 자동으로 기본 커널을 최신 버전으로 변경하므로, 디폴트로 부팅될 커널을 변경하지 마십시오.

30.4. 업그레이드 수행하기

필요한 모든 패키지를 가져오셨다면, 이제 기존 커널을 업그레이드할 준비가 되셨습니다. 쉘 프롬프트에서 루트로 로그인하신 후, 커널 RPM 패키지를 포함한 디렉토리로 이동 후 다음과 같은 단계를 따르십시오.


중요

새로운 커널을 사용하는 도중 문제가 발생할 것에 대비하여 이전 커널을 보존해 두시기를 적극 권장합니다.

이전 커널을 보존하시려면 `rpm` 명령과 함께 `-i` 옵션 인수를 사용하십시오. `kernel` 패키지를 업그레이드하실 때 `-U` 옵션을 사용하시면, 기존의 커널을 덮어쓰게 됩니다. (여러분의 커널 버전과 x86 버전은 다음에 나온 예와 다를 수도 있습니다):

```
rpm -ivh kernel-2.4.20-2.47.1.i386.rpm
```

다중-프로세서 시스템인 경우, `kernel-smp` 패키지도 설치하셔야 합니다. (여러분의 커널 버전과 x86 버전은 아래에 나온 예와 다를 수도 있습니다):

```
rpm -ivh kernel-smp-2.4.20-2.47.1.i386.rpm
```

시스템이 `i686` 기반이며 4 기가바이트 이상의 RAM을 포함하고 있다면, `i686`를 위해 개발된 `kernel-bigmem` 패키지도 설치하십시오. (여러분의 커널 버전은 아래에 나온 예와 다를 수도 있습니다):

```
rpm -ivh kernel-bigmem-2.4.20-2.47.1.i686.rpm
```

`kernel-source`, `kernel-docs`, 또는 `kernel-utils` 패키지를 업그레이드하실 계획이라면, 이전 버전 커널을 보존할 필요가 없습니다. 이러한 패키지를 업그레이드하시려면, 다음 명령을 사용하시기 바랍니다 (버전은 다를 수도 있습니다):

```
rpm -Uvh kernel-source-2.4.20-2.47.1.i386.rpm
rpm -Uvh kernel-docs-2.4.20-2.47.1.i386.rpm
rpm -Uvh kernel-utils-2.4.20-2.47.1.i386.rpm
```

만일 PCMCIA를 (예, 랩탑) 사용하는 경우에는 `kernel-pcmcia-cs` 패키지도 설치하시고 이전 버전 커널도 보존하셔야 합니다. 만일 `-i` 옵션을 사용하시면 충돌이 발생할 것입니다. 그 이유는 이전 커널이 PCMCIA 지원을 이용하여 부팅하기 위해서는 이 패키지를 필요로하기 때문입니다. 이러한 문제점을 해결하기 위해서 다음과 같이 `--force` 옵션을 사용하시면 됩니다. (버전은 다를 수도 있습니다):

```
rpm -ivh --force kernel-pcmcia-cs-3.1.24-2.i386.rpm
```

이제 초기 RAM 디스크 이미지가 생성되었는지 확인하실 차례입니다. 자세한 정보는 30.5 절을 참조하시기 바랍니다.

30.5. 초기 RAM 디스크 이미지 확인하기

ext3 파일 시스템이나 SCSI 제어기를 사용하는 시스템의 경우, 초기 RAM 디스크가 필요합니다. 초기 RAM 디스크는 일반적으로 모듈이 위치하는 장치로 커널이 접근하기 전에 모듈러 커널이 부팅할 모듈에 먼저 접근할 수 있게 해줍니다.

`mkinitrd` 명령을 사용하여 초기 RAM 디스크를 생성하실 수 있습니다. 그러나 Red Hat, Inc.이 배포한 RPM 패키지에서 커널과 관련 패키지를 설치하거나 업그레이드하신 경우에는, 이 과정이 자동적으로 수행됩니다; 따라서, 여러분이 직접 실행하실 필요가 없습니다. 초기 RAM 디스크가 생성되었는지 확인해 보시려면, `ls -l /boot` 명령을 입력하여 `initrd-2.4.20-2.47.1.img` 파일이 있는지 보십시오. (버전은 방금 설치하신 커널 버전과 일치해야 합니다).

다음 단계는 부트로더가 새로운 커널을 부팅하도록 설정되었는지 확인하는 것입니다. 자세한 사항은 30.6 절을 참조하시기 바랍니다.

30.6. 부트로더 확인하기

`kernel` RPM 패키지는 GRUB 이나 LILO가 설치되어 있다면 둘 중의 하나가 새로 설치된 커널을 부팅하도록 설정합니다. 하지만 이 패키지는 부트로더가 새 커널을 디폴트로 부팅하도록 설정하지는 않습니다.

따라서 항상 부트로더가 새 커널을 부팅하도록 제대로 설정되었는지 확인해 보는 것이 좋습니다. 이것은 매우 중요한 단계입니다. 만일 부트로더가 정확히 설정되지 않는다면, Red Hat Linux 시스템을 부팅할 수 없게 되며 이러한 상황이 발생한다면 이전에 만드신 부팅 디스켓을 가지고 시스템을 부팅하신 후 부트로더를 다시 설정하셔야 합니다.

30.6.1. GRUB

GRUB을 부트로더로 선택하셨다면 여러분이 방금 설치하신 `kernel` 패키지와 같은 버전을 가진 `title` 부분이 `/boot/grub/grub.conf` 파일에 포함되어 있는지 확인해 주십시오. (`kernel-smp` 패키지와/또는 `kernel-bigmem` 패키지를 설치하신 경우에도 다음과 같은 섹션이 포함되어 있습니다):

```
# Note that you do not have to rerun grub after making changes to this file
# NOTICE: You have a /boot partition. This means that
#     all kernel and initrd paths are relative to /boot/, eg.
#     root (hd0,0)
#     kernel /vmlinuz-version ro root=/dev/hda2
#     initrd /initrd-version.img
#boot=/dev/hda
default=3
timeout=10
splashimage=(hd0,0)/grub/splash.xpm.gz
title Red Hat Linux (2.4.20-2.47.1)
    root (hd0,0)
    kernel /vmlinuz-2.4.20-2.47.1 ro root=LABEL=/
    initrd /initrd-2.4.20-2.47.1.img
title Red Hat Linux (2.4.20-2.30)
    root (hd0,0)
    kernel /vmlinuz-2.4.20-2.30 ro root=LABEL=/
    initrd /initrd-2.4.20-2.30.img
```

만일 별개의 `/boot` 파티션을 생성하셨다면 커널과 initrd 이미지로의 경로는 `/boot` 파티션에 상대적입니다.

기본 커널이 새로운 커널로 설정되지 않은 점을 유의해 주십시오. GRUB이 새 커널을 디폴트로 부팅하도록 설정하시려면, `default` 변수의 값을 새 커널을 포함하고 있는 title 섹션에 사용된 title 섹션 번호로 교체하십시오. 이 섹션 번호는 0에서 시작합니다. 예를 들어 새 커널이 두번째 title 섹션에 있다면, `default`를 **`1`** 로 설정하시면 됩니다.

새 커널을 테스트하기 위하여 컴퓨터를 재부팅한 후 하드웨어가 제대로 검색되는지 확인하기 위하여 메시지들을 살펴보십시오.

30.6.2. LILO

만일 LILO를 부트로더로 사용하신다면, `/etc/lilo.conf` 파일에서 `image` 섹션이 방금 설치하신 `kernel` 패키지와 같은 버전을 가지고 있는지 확인해 주십시오. (`kernel-smp` 또는 `kernel-bigmem` 패키지를 설치하신 경우에도 다음과 같은 섹션이 포함되어 있습니다):

```
prompt
timeout=50
default=2.4.20-2.30
boot=/dev/hda
map=/boot/map
install=/boot/boot.b
message=/boot/message
linear

image=/boot/vmlinuz-2.4.20-2.47.1
    label=2.4.20-2.47.1
    initrd=/boot/initrd-2.4.20-2.47.1.img
    read-only
    append="root=LABEL=/"

image=/boot/vmlinuz-2.4.20-2.30
    label=2.4.20-2.30
    initrd=/boot/initrd-2.4.20-2.30.img
    read-only
    append="root=LABEL=/"
```

기본 커널이 새로운 커널로 설정되지 않은 점을 유의해 주십시오. LILO가 새 커널을 디폴트로 부팅하도록 설정하시려면, `default` 변수의 값을 새 커널을 포함하고 있는 `image` 섹션에 사용된 `label`의 값으로 교체하십시오. 변경 사항을 활성화기 위해 루트 사용자로 로그인하신 후 `/sbin/lilo` 명령을 실행하시기 바랍니다. 이 명령을 실행하시면, 다음과 같은 결과가 출력될 것입니다:

```
Added 2.4.20-2.47.1 *
Added linux
```

`2.4.20-2.47.1` 다음에 나온 `*` 는 LILO가 부팅할 디폴트 커널을 의미합니다.

새 커널을 테스트하기 위해 컴퓨터를 재부팅하신 후 하드웨어가 제대로 검색되는지 확인하기 위하여 메시지들을 살펴보시기 바랍니다.

31장 .

커널 모듈

리눅스 커널은 모듈러 방식으로 설계되었습니다. 시스템 부팅시 오직 최소량의 상주 커널만이 메모리에 로드됩니다. 따라서 사용자가 상주 커널 외부의 기능을 요청할 때마다, 가끔씩 드라이버라고도 불리우는 커널 모듈이 동적으로 메모리에 로드됩니다.

설치 과정에서 시스템 상의 하드웨어가 자동 검색됩니다. 이러한 검색 결과와 사용자가 제공한 정보에 기초하여, 설치 프로그램은 부팅시 어떠한 모듈을 로딩할 것인지 결정합니다. 설치 프로그램은 동적 로딩 메커니즘이 '투명하게' (transparently - 사용자가 시스템이나 장치를 사용할 때, 그 존재와 메커니즘을 의식하지 않고도 사용할 수 있는 성격을 가리킵니다) 작동하도록 설정합니다.

설치를 마친 후 새로운 하드웨어가 추가된 경우, 만일 그 하드웨어가 커널 모듈을 필요로 한다면, 새로운 하드웨어에 사용될 적절한 커널 모듈을 로드하도록 시스템을 설정하셔야 합니다. 새로운 하드웨어가 추가된 시스템이 부팅되면, **Kudzu** 프로그램이 실행됩니다. 이 프로그램은 검색된 지원 가능한 하드웨어에 맞는 모듈을 설정합니다. 또는 여러분이 직접 모듈 설정 파일인 `/etc/modules.conf`을 편집하여 새로운 드라이버를 지정하시는 방법도 있습니다.

알림

X 윈도우 시스템 인터페이스를 표시하는데 사용되는 비디오 카드 모듈은 커널 패키지가 아닌 `XFree86` 패키지의 일부입니다; 따라서, 이 장에서는 비디오 카드 모듈에 대하여 다루고 있지 않습니다.

예를 들어, SMC EtherPower 10 PCI 네트워크 어댑터를 포함한 시스템의 경우, 모듈 설정 파일에는 다음과 같은 줄이 포함됩니다

```
alias eth0 tulip
```

첫번째 카드와 동일한 두번째 네트워크 카드를 시스템에 추가하시면, 다음과 같은 줄을 `/etc/modules.conf` 파일에 추가하십시오:

```
alias eth1 tulip
```

알파벳 순서로 구성된 커널 모듈과 모듈이 지원하는 하드웨어의 목록을 보시려면 *Red Hat Linux* 참조 가이드를 참조하시기 바랍니다.

31.1. 커널 모듈 유틸리티

`modutils` 패키지가 설치되어 있다면, 커널 모듈을 관리할 수 있는 다양한 명령어를 사용 가능합니다. 다음과 같은 명령어는 모듈이 성공적으로 로드되었는지 확인하거나 새로운 하드웨어에 다른 모듈을 시도할 때 유용합니다.

`/sbin/lsmod` 명령은 현재 로드된 모듈의 목록을 보여줍니다. 예시:

```
Module        Size Used by  Not tainted
iptable_filter    2412  0 (autoclean) (unused)
ip_tables      15864  1 [iptable_filter]
nfs         84632  1 (autoclean)
lockd        59536  1 (autoclean) [nfs]
sunrpc       87452  1 (autoclean) [nfs lockd]
soundcore       7044  0 (autoclean)
ide-cd       35836  0 (autoclean)
```

```
cdrom        34144  0 (autoclean) [ide-cd]
parport_pc      19204  1 (autoclean)
lp          9188  0 (autoclean)
parport       39072  1 (autoclean) [parport_pc lp]
autofs        13692  0 (autoclean) (unused)
e100         62148  1
microcode       5184  0 (autoclean)
keybdev        2976  0 (unused)
mousedev        5656  1
hid         22308  0 (unused)
input         6208  0 [keybdev mousedev hid]
usb-uhci       27468  0 (unused)
usbcore       82752  1 [hid usb-uhci]
ext3         91464  2
jbd         56336  2 [ext3]
```

각 줄마다, 첫번째 행에는 모듈의 이름, 두번째 행에는 모듈의 크기, 그리고 세번째 행에는 사용된 횟수가 나타납니다.

사용된 횟수 다음에 나온 정보는 모듈마다 약간씩 다릅니다. 만일 그 줄에서 모듈이 (unused)로 나타난다면, 그 모듈은 현재 사용되지 않는다는 것을 의미합니다. 만일 (autoclean)이라고 나타난다면, 이 모듈은 rmmod -a 명령에 의해 자동으로 삭제 가능합니다. 이 명령이 실행될 때, autoclean으로 태그(tag)가 붙은 모듈들 중 이전에 autoclean 작업 이후 한번도 사용되지 않은 모듈들은 로드되지 않습니다. Red Hat Linux는 autoclean 작업을 수행하지 않도록 디폴트 설정되어 있습니다.

줄 마지막 괄호안에 모듈 이름이 있다면, 괄호 안의 모듈은 첫 번째 행에 나온 모듈에 의존성을 갖습니다. 예를 들어, 다음 줄에서

```
usbcore       82752  1 [hid usb-uhci]
```

hid와 usb-uhci 커널 모듈은 usbcore 모듈에 의존성을 갖습니다.

/sbin/lsmod 출력 결과는 /proc/modules의 출력 결과와 동일합니다.

커널 모듈을 로드하시려면, /sbin/modprobe 명령 다음에 커널 모듈 이름을 입력하시면 됩니다. 디폴트 값으로, modprobe 명령어는 /lib/modules/<*kernel-version*>/kernel/drivers/ 하부 디렉토리에서 로드할 모듈을 찾습니다. 각 모듈 유형마다 하부 디렉토리를 갖습니다. 예를 들어 네트워크 인터페이스 드라이버는 net/ 하부 디렉토리를 갖습니다. 일부 커널 모듈은 모듈 의존성을 갖으므로, 즉 해당 모듈이 로드되기 전에 다른 모듈이 먼저 로드되어야 합니다. /sbin/modprobe 명령은 이러한 의존성 문제를 찾아내어 특정 모듈이 로드되기 전에 의존성이 있는 모듈을 먼저 로드합니다.

예로 들면,

```
/sbin/modprobe hid
```

명령은 의존성이 있는 모든 다른 모듈을 로드한 후 hid 모듈을 로드합니다.

/sbin/modprobe가 실행하는 모든 명령어를 화면에서 보시려면, -v 옵션을 사용하시기 바랍니다. 예로 들면:

```
/sbin/modprobe -v hid
```

다음과 유사한 출력 결과가 나타날 것입니다:

```
/sbin/insmod /lib/modules/2.4.20-2.47.1/kernel/drivers/usb/hid.o
Using /lib/modules/2.4.20-2.47.1/kernel/drivers/usb/hid.o
Symbol version prefix 'smp_'
```

커널 모듈을 로딩하기 위해서 /sbin/insmod 명령을 사용할 수도 있지만; 이 명령은 의존성 문제를 해결하지는 않습니다. 따라서 /sbin/modprobe 명령을 사용하시기를 권장합니다.

커널 모듈을 언로드하시려면, `/sbin/rmmod` 명령 다음에 모듈 이름을 입력하시면 됩니다. `rmmod` 유틸리티는 사용되지 않으며 다른 사용중인 모듈이 의존성을 갖지 않는 모듈들만 언로드합니다.

예를 들어,

```
/sbin/rmmod hid
```

명령은 `hid` 커널 모듈을 언로드합니다.

또 다른 유용한 커널 모듈 유틸리티는 `modinfo` 입니다. 커널 모듈에 대한 정보를 보시려면, `/sbin/modinfo` 명령을 사용하시기 바랍니다. 일반적으로 사용되는 구문은 다음과 같습니다:

```
/sbin/modinfo [options] <module>
```

옵션에는 모듈에 대한 간략한 설명을 보여주는 `-d` 옵션과 모듈이 지원하는 매개 변수의 목록을 보여주는 `-p` 옵션이 있습니다. 전체 옵션 목록을 보시려면, `modinfo` 메뉴얼 페이지를 참조하시기 바랍니다 (`man modinfo`).

31.2. 추가 자료

커널 모듈과 유틸리티에 대한 보다 자세한 정보를 원하시다면, 다음 자료들을 참조하시기 바랍니다.

31.2.1. 설치된 문서 자료

- `lsmod` 메뉴얼 페이지 — lsmod 명령의 출력 결과에 대한 설명을 볼 수 있습니다.
- `insmod` 메뉴얼 페이지 — insmod 명령에 대한 설명과 사용 가능한 명령행 옵션의 목록을 보여줍니다.
- `modprobe` 메뉴얼 페이지 — modprobe 명령에 대한 설명과 사용 가능한 명령행 옵션의 목록을 보여줍니다.
- `rmmod` 메뉴얼 페이지 — mmod 명령에 대한 설명과 사용 가능한 명령행 옵션의 목록을 보여줍니다.
- `modinfo` 메뉴얼 페이지 — modinfo 명령에 대한 설명과 사용 가능한 명령행 옵션의 목록을 보여줍니다.
- `/usr/src/linux-2.4/Documentation/modules.txt` — 커널 모듈을 컴파일하고 사용하는 방법을 알 수 있습니다.

31.2.2. 유용한 웹사이트

- http://www.redhat.com/mirrors/LDP/HOWTO/Module-HOWTO/index.html — 리눅스 문서화 프로젝트의 *Linux Loadable Kernel Module HOWTO*.

V. 패키지 관리

Red Hat Linux 시스템에서 사용되는 모든 소프트웨어는 RPM 패키지로 구분되어 저장되며, 쉽게 설치, 업그레이드 또는 삭제가 가능합니다. 이 장에서는 그래픽 도구와 명령행 도구를 사용하여 Red Hat Linux 시스템에서 RPM 패키지를 관리하는 방법에 대하여 설명해 보겠습니다.

차례

32장 .

RPM을 사용한 패키지 관리

RPM 패키지 관리자 (RPM)는 누구나 사용할 수 있는 Red Hat Linux를 비롯한 그 외 다른 Linux 및 UNIX 시스템 용 공개 패키징 시스템입니다. Red Hat, Inc.은 다른 판매업체의 배포판에도 RPM을 사용하실 것을 권장합니다. RPM은 GPL의 조건 하에 자유로운 사용과 배포가 가능합니다.

일반 사용자의 경우, RPM을 사용하여 쉽게 시스템을 업데이트하실 수 있습니다. 짧은 명령어를 사용하여 RPM 패키지의 설치, 설치 제거하고 업그레이드가 가능합니다. RPM은 설치된 패키지와 파일이 담겨있는 데이터베이스를 유지하기 때문에, 여러분은 시스템 상에서 강력한 질의와 검증을 실행하실 수 있습니다. 그래픽 인터페이스를 선호하신다면 **패키지 관리 도구**을 사용하여 다양한 RPM 명령을 실행하실 수 있습니다. 보다 자세한 사항은 33 장을 참조하시기 바랍니다.

업그레이드 과정에서 RPM은 설정 파일을 주의 깊게 처리하기 때문에 여러분의 사용자 설정이 모두 보존됩니다. — 일반 `.tar.gz` 파일을 사용해서는 절대로 이러한 결과를 얻지못할 것입니다.

개발자의 경우, RPM을 사용하여 소프트웨어 소스 코드를 일반 사용자가 사용할 수 있는 소스와 바이너리 패키지로 구성하실 수 있습니다. 이 과정은 매우 단순하며 단독 파일과 여러분이 생성하신 옵션 패치를 주로 사용합니다. 이렇게 "원래" 소스와 개발 지시 사항이 포함된 패치를 확연히 구분함으로서 새로운 버전의 소프트웨어가 배포될 때마다 쉽게 패키지를 관리하실 수 있습니다.

알림

RPM은 시스템에 변화를 가져오기 때문에 RPM 패키지를 설치, 제거 및 업그레이드하시려면 반드시 루트로 로그인하셔야 합니다.

32.1. RPM 설계 목표

RPM의 사용법을 이해하기 위해서는 먼저 RPM의 설계 목표를 이해하시는 것이 도움이 될 것입니다:

업그레이드 기능

‘ RPM을 사용하여 시스템을 완전히 다시 설치를 하지 않고서도 개별 구성 요소를 업그레이드하실 수 있습니다. RPM에 기초한 운영 체제 (예, Red Hat Linux)의 새로운 버전이 배포될 때마다 다른 패키징 시스템에 기반한 운영 체제에서 처럼 새로 설치하실 필요가 없습니다. RPM은 지능화되고 완전히 자동화된 인-플레이스 업그레이드(in-place upgrade)를 수행합니다. 패키지에 들어있는 설정 파일들은 업그레이드가 실행되는 동안 모두 보존되기 때문에 여러분의 사용자 설정 또한 그대로 보존됩니다. 동일한 RPM 파일을 사용하여 시스템 상에서 패키지를 설치하고 업그레이드하기 때문에 특별한 업그레이드 파일이 필요하지 않습니다.

강력한 질의 기능

‘ RPM은 강력한 질의(query) 옵션을 제공하도록 설계되었습니다. 따라서 여러분은 전체 데이터베이스에 저장된 패키지나 특정 파일을 검색하실 수 있으며, 어떠한 파일이 어느 패키지에 담겨 있는지와 그 패키지의 출처를 쉽게 알아낼 수 있습니다. RPM 패키지에 포함된 파일들은 압축된 아카이브 형식으로 구성되어 있으며, 패키지에 대한 유용한 정보와 내용을 포함하고 있는 사용자 정의 바이너리 헤더 덕분에 사용자 여러분은 개별 패키지를 쉽고 빠르게 질의하실 수 있습니다.

시스템 검증 기능

‘ 또 하나의 뛰어난 기능은 패키지를 검증할 수 있는 능력입니다. 만일 여러분이 일부 패키지에 대한 중요한 파일을 삭제되었는지 걱정이 되신다면, 간단히 패키지를 검증해 보십시오. 만일 이상이 있다면 여러분께

알려드릴 것입니다. 이 시점에서 필요한 경우 패키지를 재설치하실 수 있습니다. 여러분이 수정하신 설정 파일은 재설치 과정에서 모두 보존됩니다.

원래 소스 사용 기능

‘ 가장 중요한 설계 목적은 해당 소프트웨어의 개발자에 의하여 배포된 "원래" 소프트웨어 소스를 사용할 수 있게 하는 것이었습니다. RPM에는 원래 소스와 더불어 함께 사용된 패치 및 완전한 개발 지시 사항이 담겨 있습니다. 이것은 여러 가지 이유에서 매우 중요한 장점으로 볼 수 있습니다. 예를 들어 새로운 버전의 프로그램이 출시될 경우, 여러분은 그 프로그램을 컴파일하기 위하여 처음부터 다시 시작하실 필요가 없습니다. 패치를 살펴보신 후 여러분은 어떠한 작업이 필요한지 쉽게 알 수 있습니다. 이 기능을 사용하여 소프트웨어를 제대로 구축하기 위하여 만들어진 컴파일된 기본값과 변경 사항들을 쉽게 보실 수 있습니다.

소스를 원래대로 보존하는 목적은 개발자에게만 중요하다고 느끼실 수도 있지만 결론적으로 최종 사용자에게도 더 높은 수준의 소프트웨어를 가져다 줍니다. Red Hat, Inc는 RPM에 포함된 원래 소스 개념을 제공한 BOGUS 제작진에게 감사드립니다.

32.2. RPM 사용하기

RPM에는 다음과 같은 다섯가지 기본 작업 모드가 있습니다 (패키지 개발 제외): 설치 모드, 제거 모드, 업그레이드 모드, 질의 모드, 검증 모드. 이 섹션에서는 각 모드에 대한 개요를 설명해 보겠습니다. 만일 보다 자세한 사항이나 옵션을 원하신다면, `rpm --help` 명령을 시도해 보십시오. RPM에 대한 보다 많은 정보를 원하시면 32.5 절을 미리 읽어보시기 바랍니다.

32.2.1. RPM 패키지 찾기

RPM을 사용하시기 전에 어디서 RPM을 찾을 것인지를 아셔야 합니다. 인터넷으로 검색하시면 많은 RPM 저장소(repository)를 찾으실 수 있지만, Red Hat이 개발한 RPM 패키지를 구하신다면 다음의 위치에서 찾으실 수 있습니다:

- 공식 Red Hat Linux CD-ROM
- Red Hat 에라타 페이지. 사이트 주소: http://www.redhat.com/apps/support/errata/
- Red Hat FTP 미러 사이트. 사이트 주소: http://www.redhat.com/download/mirror.html
- Red Hat Network — Red Hat Network에 대한 보다 자세한 사항은 34 장을 참조하시기 바랍니다.

32.2.2. 설치하기

RPM 패키지는 일반적으로 `foo-1.0-1.i386.rpm`와 같은 파일명을 가지고 있습니다. 이 파일명에는 패키지명 (`foo`), 버전 (`1.0`), 배포판 (`1`)과 구조 (`i386`)가 포함됩니다. 패키지를 설치하시려면 루트로 로그인하신 후 쉘 프롬프트에서 다음과 같은 명령을 입력하시면 됩니다:

```
rpm -Uvh foo-1.0-1.i386.rpm
```

만일 설치가 성공적이라면, 다음과 같은 화면이 출력됩니다:

```
Preparing...        ########################################### [100%]
   1:foo            ########################################### [100%]
```

여러분이 보시듯이 RPM은 패키지 이름을 출력 후 패키지 설치가 진행되는 상황을 연속적인 해시(#) 표시를 사용하여 보여줍니다.

RPM 4.1 버전부터는 패키지를 설치하거나 업그레이드시 패키지의 서명을 확인합니다. 만일 패키지 서명 검증 작업이 실패한다면, 다음과 같은 오류 메시지가 나타날 것입니다:

```
error: V3 DSA signature: BAD, key ID 0352860f
```

만일 새로?? 헤더-전용 서명일 경우, 다음과 같은 메시지가 나타납니다:

```
error: Header V3 DSA signature: BAD, key ID 0352860f
```

서명을 검증하는데 필요한 적절한 키가 설치되어 있지 않다면, NOKEY라는 항목이 포함된 메시지가 나타날 것입니다. 예:

```
warning: V3 DSA signature: NOKEY, key ID 0352860f
```

패키지의 서명을 확인하는 방법에 대한 보다 많은 정보를 원하신다면 32.3 절을 참조하시기 바랍니다.

알림

커널 패키지를 설치하신다면, `rpm -ivh` 명령을 사용하셔야 합니다. 보다 자세한 사항은 30 장을 참조하시기 바랍니다.

패키지를 설치하는 과정은 매우 간단하지만, 가끔씩 오류 메시지가 나타날 수도 있습니다.

32.2.2.1. 이미 설치된 패키지

만일 동일한 버전의 패키지가 이미 설치되어 있다면, 다음과 같은 메시지가 나타납니다:

```
Preparing...        ########################################### [100%]
package foo-1.0-1 is already installed
```

그래도 패키지를 계속 설치하기를 원하신다면, `--replacepkgs` 옵션을 사용할 수 있습니다. 이 옵션은 RPM에게 오류를 무시하도록 지시합니다:

```
rpm -ivh --replacepkgs foo-1.0-1.i386.rpm
```

만일 RPM에서 설치된 파일이 삭제되었거나 RPM에서 원래 설정 파일 설치하실 경우, 이 옵션이 유용하게 사용됩니다.

32.2.2.2. 파일간 충돌

다른 패키지에 의해서 이미 설치된 파일을 포함하는 패키지나 동일 패키지의 이전 버전을 설치하려고 하시면, 다음과 같은 메시지가 나타날 것입니다:

```
Preparing...        ########################################### [100%]
file /usr/bin/foo from install of foo-1.0-1 conflicts with file from package bar-2.0.20
```

RPM이 이러한 오류를 무시하도록 지시하기 위해서는, 다음과 같이 `--replacefiles` 옵션을 사용하십시오:

```
rpm -ivh --replacefiles foo-1.0-1.i386.rpm
```

32.2.2.3. 해결되지 않은 의존성 문제

RPM 패키지가 다른 패키지에 "의존"할 경우가 있습니다. 즉 다른 패키지가 설치되어야 RPM 패키지가 제대로 실행될 수 있다는 것을 의미합니다. 만일 해결되지 않은 의존성이 가진 패키지를 설치 시도하시면, 다음과 같은 메시지가 나타날 것입니다:

```
Preparing...        ########################################### [100%]
error: Failed dependencies:
    bar.so.2 is needed by foo-1.0-1
  Suggested resolutions:
    bar-2.0.20-3.i386.rpm
```

공식 Red Hat을 설치하신다면, 이러한 패키지 간의 의존성 문제를 해결해 주셔야 합니다. 요청된 패키지를 Red Hat Linux CD-ROM이나 Red Hat FTP 사이트 (또는 미러 사이트)에서 찾으신 후 다음과 같이 명령에 첨가하여 사용하십시오:

```
rpm -ivh foo-1.0-1.i386.rpm bar-2.0.20-3.i386.rpm
```

두 패키지가 성공적으로 설치되었다면, 다음과 같이 출력될 것입니다:

```
Preparing...        ########################################### [100%]
  1:foo         ########################################### [ 50%]
  2:bar         ########################################### [100%]
```

의존성 문제를 해결하도록 요청되지 않는 경우에는 `--redhatprovides` 옵션을 사용하여 필요한 패키지를 알아보실 수 있습니다. 이 옵션을 사용하기 위해서는 `rpmdb-redhat` 패키지를 설치하셔야 합니다.

```
rpm -q --redhatprovides bar.so.2
```

`bar.so.2` 파일을 포함한 패키지가 `rpmdb-redhat` 패키지에서 설치된 데이터베이스에 존재한다면, 패키지의 이름이 화면에 출력될 것입니다:

```
bar-2.0.20-3.i386.rpm
```

의존성 문제를 해결하지 않고 설치를 계속 진행하시려면 `--nodeps` 옵션을 사용하십시오. (패키지가 적절히 작동하지 않을 가능성이 있으므로 좋은 생각이 아닙니다).

32.2.3. 제거하기

패키지 제거하기는 설치하기 만큼이나 간단합니다. 쉘 프롬프트에서 다음 명령을 입력하십시오:

```
rpm -e foo
```

알림

위의 예시에서는 원래 패키지 파일 이름인 `foo-1.0-1.i386.rpm`을 사용하지 않고 패키지 이름인 `foo`를 사용하였습니다. 패키지를 제거하기 위해서는, `foo`를 원래 패키지의 이름으로 교체해 주시기 바랍니다.

만일 제거하려는 패키지에 또 다른 설치된 패키지가 의존하고 있는 경우 패키지를 제거시 의존성 오류가 발생할 수 있습니다. 예를 들면:

```
Preparing...        ########################################### [100%]
error: removing these packages would break dependencies:
```

```
foo is needed by bar-2.0.20-3.i386.rpm
```

RPM이 이러한 오류를 무시하고 계속 패키지 삭제 작업을 진행하도록 하시려면, `--nodeps` 옵션을 사용하시면 됩니다. (하지만 이 방법은 패키지가 적절히 작동하지 않을 가능성이 있으므로 좋은 생각이 아닙니다).

32.2.4. 업그레이드하기

패키지 업그레이드는 설치하기와 유사합니다. 쉘 프롬프트에서 다음 명령을 입력하십시오:

```
rpm -Uvh foo-2.0-1.i386.rpm
```

위의 업그레이드 명령을 사용하시면 RPM은 자동으로 `foo` 패키지의 이전 버전을 제거한 후 새로운 버전으로 업그레이드합니다. 패키지를 설치하실 때 `-U` 옵션을 사용하시기 바랍니다. 이 옵션은 이미 설치된 이전 버전이 없는 경우에도 작용합니다.

RPM은 설정 파일을 사용하여 지능화된 패키지 업그레이드를 수행합니다. 따라서 다음과 같은 메시지를 보여줄 경우가 있습니다:

```
saving /etc/foo.conf as /etc/foo.conf.rpmsave
```

이 메시지는 여러분이 수정하신 설정 파일은 패키지에 있는 새로운 설정 파일과 "이후 버전 호환성"이 없을 수도 있기 때문에 RPM은 원래 파일을 저장하고 새로운 설정 파일을 설치했다는 것을 의미합니다. 시스템이 계속해서 제대로 기능할 수 있도록 하기 위해서는, 여러분은 되도록 빨리 두가지 설정 파일 사이의 차이점을 조사하고 문제를 해결하셔야 합니다.

업그레이드는 제거하기와 설치하기의 조합이라고 할 수 있습니다. 따라서 RPM 업그레이드 과정에서 패키지 삭제 오류 또는 설치 오류가 발생할 가능성이 있으며, 더불어 다음과 같은 문제가 발생할 수도 있습니다. 예를 들어 만일 여러분이 이전 버전 번호를 가진 패키지로 업그레이드를 시도한다고 판단되면, RPM은 다음과 같은 메시지가 보여줍니다:

```
package foo-2.0-1 (which is newer than foo-1.0-1) is already installed
```

RPM이 이 오류 메시지를 무시하고 계속 업그레이드 작업을 진행하도록 하시려면, 다음과 같이 `--oldpackage` 옵션을 사용하십시오:

```
rpm -Uvh --oldpackage foo-1.0-1.i386.rpm
```

32.2.5. 다시 읽기

패키지를 다시 읽기는 패키지 업그레이드와 유사합니다. 쉘 프롬프트에서 다음 명령을 입력하십시오:

```
rpm -Fvh foo-1.2-1.i386.rpm
```

RPM의 다시 읽기 옵션을 사용하시면, 명령 행에서 지정된 패키지 버전을 시스템 상에 이미 설치된 패키지 버전에 대조하여 검사합니다. 이미 설치된 패키지의 최신 버전이 RPM의 다시 읽기 옵션에 의해 처리되면, 해당 패키지는 최신 버전으로 업그레이드됩니다. 하지만 동일한 이름의 패키지가 이미 설치되어 있지 않다면, RPM의 다시 읽기 옵션은 패키지를 설치하지 않습니다. 이것이 RPM 업그레이드 옵션과의 차이점입니다. 업그레이드 옵션은 이전 버전의 패키지가 이미 설치되어 있지 않은 경우에도 패키지를 설치합니다.

RPM의 다시 읽기 옵션은 단독 패키지나 패키지 그룹에서 작용합니다. 많은 패키지들을 다운로드받으신 후 시스템 상에 이미 설치된 패키지만을 업그레이드할 계획이라면, 다시 읽기 옵션을 사용하시기를 권장합니다. 다시 읽기 옵션을 사용하시면, 이전에 RPM을 사용하여 다운로드 받은 그룹 중에서 원치않은 패키지를 직접 삭제하실 필요가 없습니다.

이러한 경우에 간단히 다음과 같은 명령을 사용할 수 있습니다:

```
rpm -Fvh *.rpm
```

RPM은 자동으로 이미 설치된 패키지만을 업그레이드합니다.

32.2.6. 질의

`rpm -q` 명령을 사용하여 설치된 패키지의 데이터베이스에 대한 질의를 수행할 수 있습니다. `rpm -q foo` 명령을 입력하시면, 다음과 같이 패키지명, 버전과 설치된 패키지 foo의 배포 번호가 출력될 것입니다:

```
foo-2.0-1
```

알림

위의 예시에서 패키지 이름으로 `foo`를 사용했다는 것에 주의해 주십시오. 패키지에 대한 질의를 수행하기 위해서는 `foo`를 실제 패키지 이름으로 교체하셔야 합니다.

패키지명을 지정하는 대신 여러분은 다음과 같은 옵션을 `-q`와 함께 사용하여 질의를 수행할 패키지를 지정할 수 있습니다. 이러한 옵션들은 패키지 지정 옵션이라고 불립니다.

- `-a`는 현재 설치된 모든 패키지에 대하여 질의를 수행합니다..
- `-f` <*`file`*> 명령은 <*`file`*>를 소유한 패키지에 대하여 질의를 수행합니다. 파일을 지정할 때 반드시 파일의 완전 경로를 지정해야 합니다. (예, `/usr/bin/ls`)
- `-p` <*`packagefile`*> 는 <*`packagefile`*> 패키지를 질의합니다.

질의된 패키지 정보가 표시될 형식을 지정하는데는 여러가지 방법이 있습니다. 다음에 나온 옵션들은 패키지 정보가 표시될 형식을 선택하는데 사용됩니다. 이러한 옵션들은 정보 선택 옵션이라고 불립니다.

- `-i` 옵션은 이름, 설명, 배포판, 크기, 개발 날짜, 설치 날짜, 공급자 등의 정보를 출력합니다.
- `-l` 옵션은 패키지 안의 파일 목록을 보여줍니다.
- `-s` 옵션은 패키지 안에 든 파일의 상태를 보여줍니다.
- `-d` 옵션은 문서 화일만 보여줍니다. (메뉴얼 페이지, 정보 페이지, README, 그 외 기타)
- `-c` 옵션은 설정 파일만 보여줍니다. 설치 후 패키지를 시스템에 적합하도록 여러분이 변경하신 파일들입니다. (예, `sendmail.cf`, `passwd`, `inittab`, 그 외 기타)

파일 목록을 보기에 익숙한 `ls -l` 형식으로 출력하기 위해서는 파일 목록 보기 명령에 `-v` 옵션을 추가하여 사용할 수 있습니다.

32.2.7. 검증

패키지 검증은 패키지에 설치된 파일에 저장된 내용과 원래 패키지의 내용을 비교합니다. 검증 옵션을 사용하시면, 여러가지 정보들, 즉 개별 파일의 크기, MD5 sum, 권한, 유형, 소유권, 그룹 소유권 등을 빅하게 되며 어떠한 변화가 있을 경우 출력합니다.

`rpm -V` 명령은 패키지를 검증합니다. 패키지 검증에 사용할 수 있는 옵션은 패키지를 질의에 사용된 패키지 선택 옵션과 같습니다. 검증의 간단한 예로서 `rpm -V foo`는 foo 패키지에 저장된 모든 파일들과 원래 설치된 파일을 비교합니다. 예로 들면:

- 특정 파일을 포함하는 패키지를 검증할 경우:
  `rpm -Vf /bin/vi`
- 설치된 모든 패키지를 검증할 경우:

```
rpm -Va
```

- 설치된 패키지와 RPM 패키지 파일을 검증할 경우:
  ```
  rpm -Vp foo-1.0-1.i386.rpm
  ```

  RPM 데이터베이스가 손상되었다고 판단되는 경우에 이 명령을 사용하여 조사할 수 있습니다.

만일 검증 결과 아무런 변화가 없다면 출력되는 것이 없습니다. 비교 결과 문제점이 발견되면 결과를 출력합니다. 출력 결과는 8글자의 문자열을 출력하고 다음에 `c` 가 나오면 설정 파일임을 뜻하며 다음에는 파일 이름을 차례로 한줄로 출력합니다. 처음의 각 8글자들은 RPM 데이터베이스와 각 특성을 비교한 결과를 출력하게 됩니다. 점 한개 (`.`)는 아무 이상이 없다는 것을 의미합니다. 만일 비교 결과 문제점이 발견되면 다음과 같은 문자가 나타납니다:

- `5` — MD5 체크섬
- `S` — 파일 크기
- `L` — 심볼릭 링크
- `T` — 파일 수정 시간
- `D` — 장치
- `U` — 사용자
- `G` — 그룹
- `M` — 모드 (허가와 파일 유형 포함)
- `?` — 읽기 불가 파일

이상과 같은 결과가 출력되면, 여러분은 패키지를 제거하거나 재설치할 것인지 또는 다른 방식으로 문제를 해결할 것인지를 잘 결정하셔야 합니다.

32.3. 패키지 서명 확인

패키지의 손상이나 변경 여부를 검증하기 위해서는 쉘 프롬프트에서 다음과 같은 명령을 입력하여 md5sum을 점검합니다. (아래 예시에서 <*`rpm-file`*>를 여러분 **RPM** 패키지의 파일명으로 교체하십시오):

```
rpm -K --nogpg <rpm-file>
```

<*`rpm-file`*>`: md5 OK` 라는 메시지가 나타날 것입니다. 이 간략한 메시지는 파일이 다운로드되면서 손상되지 않았음을 의미합니다. 보다 자세한 메시지를 보시려면, 명령에서 `-K` 옵션 대신 `-Kvv`를 사용하시면 됩니다.

다른 한편으로 패키지를 만든 개발자를 얼마나 믿을 수 있습니까? 만일 패키지가 개발자의 GnuPG 키 *(key)*를 사용하여 서명되었다면, 패키지의 서명을 확인하여 개발자를 확인할 수 있습니다.

사용자가 다운로드받은 패키지의 신뢰성 여부를 가려낼 수 있도록 RPM 패키지는 Gnu Privacy Guard (또는 GnuPG)를 사용하여 서명됩니다.

GnuPG는 보안 통신을 위한 도구로서 전자 우편 보안 시스템의 하나인 PGP의 암호화 기술을 대체하는 완전한 기능을 갖춘 프리 소프트웨어입니다. 여러분은 GnuPG를 사용하여 문서의 유효성을 인증하고 다른 수신자와 보내고 받는 데이타를 암호화/해독할 수 있습니다. GnuPG는 또한 PGP 5.*x* 파일들을 해독하고 검증할 수 있습니다.

Red Hat Linux 설치 과정에서 GnuPG는 기본으로 설치됩니다. 따라서 여러분은 바로 GnuPG를 사용하여 Red Hat에서 받은 패키지를 검증해 보실 수 있습니다. 첫째로 여러분은 Red Hat의 공개키를 가져와야 합니다.

32.3.1. 키 가져오기

공식 Red Hat 패키지들을 검증하시려면, Red Hat GPG 키를 가져오셔야 합니다. 쉘 프롬프트에서 다음과 같은 명령을 실행하시기 바랍니다:

```
rpm --import /usr/share/rhn/RPM-GPG-KEY
```

RPM 검증을 위해 설치된 모든 키 목록을 보시려면, 다음 명령을 실행하십시오:

```
rpm -qa gpg-pubkey*
```

Red Hat 키 목록에는 다음과 같은 결과가 출력될 것입니다:

```
gpg-pubkey-db42a60e-37ea5438
```

특정 키에 대한 자세한 정보를 출력하시려면, 다음과 같이 `rpm -qi` 다음에 위의 명령 출력 결과를 함께 한줄로 입력하십시오:

```
rpm -qi gpg-pubkey-db42a60e-37ea5438
```

32.3.2. 패키지의 서명 검증하기

개발자의 GnuPG 키를 가져온 후 RPM 파일의 GnuPG 서명을 확인하기 위해서는, 다음과 같은 명령을 사용하십시오. (아래 명령에서 <*rpm-file*>는 RPM 패키지의 파일명으로 교체합니다):

```
rpm -K <rpm-file>
```

아무런 문제가 없다면 다음 메시지가 나타날 것입니다: `md5 gpg OK`. 이 메시지는 패키지가 손상되지 않았다는 것을 의미합니다.

힌트

GnuPG와 관련된 보다 많은 정보를 원하신다면, 부록 B을 참조하시기 바랍니다.

32.4. RPM을 사용하여 친구에게 자랑하기

RPM은 여러분의 시스템을 관리할 뿐만 아니라 문제점을 진단하고 해결하는데 사용되는 유용한 도구입니다. RPM 옵션을 이해하기 위한 최선의 방법은 몇가지 예를 들어보는 것입니다.

- 만일 여러분이 실수로 일부 파일을 삭제했지만 어떤 파일을 삭제했는지 알 수 없는 경우를 가정해 봅니다. 사라진 파일을 찾기 위해 전체 시스템을 검증하시려면, 다음과 같은 명령을 시도해 볼 수 있습니다:
  ```
  rpm -Va
  ```
  만일 일부 파일이 사라졌거나 손상된 것처럼 보인다면, 여러분은 패키지를 재설치하거나 또는 제거후 재설치하셔야 합니다.
- 어느 정도 시점에서 여러분이 알지 못하는 파일이 나타날 수도 있습니다. 어떤 패키지에 파일이 속하는지 알아내기 위하여 다음을 입력하십시오:
  ```
  rpm -qf /usr/X11R6/bin/ghostview
  ```
  출력된 결과는 다음과 유사하게 나타날 것입니다:
  ```
  gv-3.5.8-22
  ```

- 위의 두가지 예시를 다음과 같은 시나리오로 묶어볼 수 있습니다. 여러분이 /usr/bin/paste을 사용하는데 문제가 발생했다고 가정합니다. 이 프로그램이 속한 패키지를 검증하고 싶지만, paste 파일가 속한 패키지가 무엇인지 모르는 경우, 간단히 다음 명령을 입력하시면:
  ```
  rpm -Vf /usr/bin/paste
  ```
  적절한 패키지가 검증될 것입니다.
- 특정 프로그램에 대한 보다 많은 정보를 찾고 싶으십니까? 해당 프로그램을 소유하는 패키지에 같이 들어있는 문서를 찾기위해서는 다음과 같은 명령을 사용해 보십시오:
  ```
  rpm -qdf /usr/bin/free
  ```
  결과는 다음과 같이 출력될 것입니다:
  ```
  /usr/share/doc/procps-2.0.11/BUGS
  /usr/share/doc/procps-2.0.11/NEWS
  /usr/share/doc/procps-2.0.11/TODO
  /usr/share/man/man1/free.1.gz
  /usr/share/man/man1/oldps.1.gz
  /usr/share/man/man1/pgrep.1.gz
  /usr/share/man/man1/pkill.1.gz
  /usr/share/man/man1/ps.1.gz
  /usr/share/man/man1/skill.1.gz
  /usr/share/man/man1/snice.1.gz
  /usr/share/man/man1/tload.1.gz
  /usr/share/man/man1/top.1.gz
  /usr/share/man/man1/uptime.1.gz
  /usr/share/man/man1/w.1.gz
  /usr/share/man/man1/watch.1.gz
  /usr/share/man/man5/sysctl.conf.5.gz
  /usr/share/man/man8/sysctl.8.gz
  /usr/share/man/man8/vmstat.8.gz
  ```
- 만일 새로운 RPM을 찾았는데 그 기능을 알 수 없을때는 다음 명령을 사용하여 RPM에 대한 정보를 알아볼 수 있습니다:
  ```
  rpm -qip crontabs-1.10-5.noarch.rpm
  ```
  출력된 결과는 다음과 유사하게 나타날 것입니다:
  ```
  Name    : crontabs                      Relocations: (not relocateable)
  Version : 1.10                             Vendor: Red Hat, Inc.
  Release : 5                             Build Date: Fri 07 Feb 2003 04:07:32 PM EST
  Install date: (not installed)           Build Host: porky.devel.redhat.com
  Group   : System Environment/Base       Source RPM: crontabs-1.10-5.src.rpm
  Size    : 1004                             License: Public Domain
  Signature   : DSA/SHA1, Tue 11 Feb 2003 01:46:46 PM EST, Key ID fd372689897da07a
  Packager    : Red Hat, Inc. <http://bugzilla.redhat.com/bugzilla>
  Summary     : Root crontab files used to schedule the execution of programs.
  Description :
  The crontabs package contains root crontab files. Crontab is the
  program used to install, uninstall, or list the tables used to drive the
  cron daemon. The cron daemon checks the crontab files to see when
  particular commands are scheduled to be executed. If commands are
  scheduled, then it executes them.
  ```
- crontabs RPM이 설치하는 파일들을 보시려면, 다음과 같이 입력하시면 됩니다:
  ```
  rpm -qlp crontabs-1.10-5.noarch.rpm
  ```
  출력된 결과는 다음처럼 나타날 것입니다:
  ```
  Name    : crontabs                      Relocations: (not relocateable)
  Version : 1.10                             Vendor: Red Hat, Inc.
  Release : 5                             Build Date: Fri 07 Feb 2003 04:07:32 PM EST
  Install date: (not installed)           Build Host: porky.devel.redhat.com
  Group   : System Environment/Base       Source RPM: crontabs-1.10-5.src.rpm
  Size    : 1004                             License: Public Domain
  Signature   : DSA/SHA1, Tue 11 Feb 2003 01:46:46 PM EST, Key ID fd372689897da07a
  Packager    : Red Hat, Inc. <http://bugzilla.redhat.com/bugzilla>
  ```

```
Summary   : Root crontab files used to schedule the execution of programs.
Description :
The crontabs package contains root crontab files. Crontab is the
program used to install, uninstall, or list the tables used to drive the
cron daemon. The cron daemon checks the crontab files to see when
particular commands are scheduled to be executed. If commands are
scheduled, then it executes them.
```

앞에서 설명된 것은 RPM의 많은 기능 중 극히 소수에 불과합니다. 여러분은 RPM을 사용하면 할수록 훨씬 더 많은 기능이 있다는 것을 발견하실 것입니다.

32.5. 추가 자료

RPM은 많은 옵션과 다양한 패키지를 질의, 설치, 업그레이드 및 삭제 방식을 갖춘 매우 복잡한 유틸리티입니다. RPM에 대하여 보다 많은 정보를 원하신다면, 다음과 같은 자료를 참조하시기 바랍니다.

32.5.1. 설치된 문서 자료

- `rpm --help` — 이 명령은 RPM 매개 변수에 대한 간략한 정보를 보여줍니다.
- `man rpm` — RPM 메뉴얼 페이지에서 `rpm --help` 명령을 사용하는 것보다 더욱 상세한 RPM 매개 변수 정보를 찾으실 수 있습니다.

32.5.2. 유용한 웹사이트

- http://www.rpm.org/ — RPM 웹사이트.
- http://www.redhat.com/mailing-lists/rpm-list/ — RPM 메일링 리스트는 이 사이트에 아카이브되어 있습니다. 메일링 리스트에 가입하시려면, 제목란에 `subscribe`라고 쓰신 후 <`rpm-list-request@redhat.com`> 주소로 이메일을 보내주십시오.

32.5.3. 관련 서적

- *Maximum RPM* 저자 Ed Bailey; Red Hat Press — 이 서적의 온라인 버전은 다음의 두 사이트에서 찾으실 수 있습니다: http://www.rpm.org/와 http://www.redhat.com/docs/books/.

패키지 관리 도구

설치 과정에서 여러분은 **웍스테이션** 이나 **서버**와 같은 설치 유형을 선택하셨습니다. 이러한 설치 유형에 기초한 소프트웨어 패키지가 설치됩니다. 하지만 사용자 개인마다 컴퓨터의 사용 용도가 다르기 때문에 설치를 마치신 후, 추가 패키지를 설치하거나 필요없는 패키지는 삭제하기를 원하실 것입니다. 이러한 경우 **패키지 관리 도구**를 사용하시면 됩니다.

X 윈도우 시스템을 실행하셔야 **패키지 관리 도구**를 사용할 수 있습니다. 이 응용 프로그램을 시작하시려면, 패널에서 **주 메뉴 버튼** => **시스템 설정** => **응용 프로그램 추가/삭제**를 선택하시거나 쉘 프롬프트에서 `redhat-config-packages` 명령을 입력하시면 됩니다.

Red Hat Linux CD-ROM #1를 삽입하시면, 동일한 인터페이스가 나타납니다.

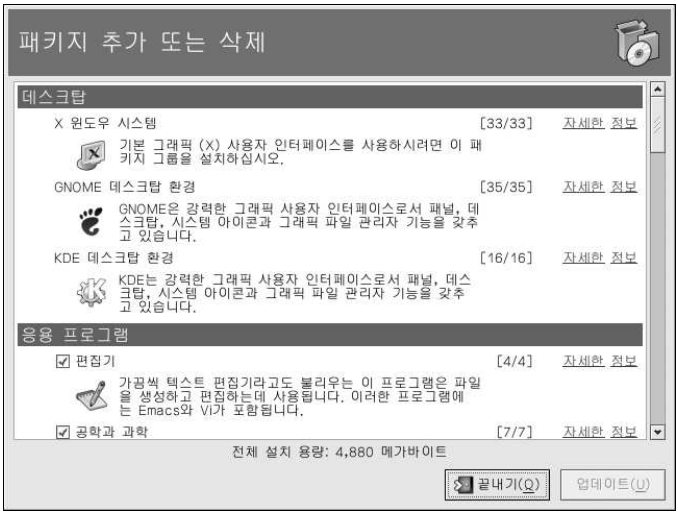

그림 33-1. 패키지 관리 도구

이 응용 프로그램에 사용되는 인터페이스는 설치 과정에서 보신 것과 유사합니다. 패키지는 패키지 그룹으로 나뉘어져 있으며, 패키지 그룹은 일반 기능을 공유하는 표준 패키지와 추가 패키지로 구성됩니다. 예로 들면, **그래픽 인터넷** 그룹에는 웹 브라우저, 이메일 클라이언트 및 인터넷 접속에 사용되는 그래픽 응용 프로그램들이 포함되어 있습니다. 전체 패키지 그룹을 삭제하지 않는 한 표준 패키지는 삭제 불가능합니다. 추가 패키지는 선택 사항으로서 패키지 그룹이 선택된 경우 설치를 위해 선택하거나 삭제하실 수 있습니다.

기본 창에서는 패키지 그룹 목록이 나타납니다. 패키지 그룹명 옆에 위치한 체크박스가 체크되어 있다면, 해당 패키지 그룹은 설치를 위해 선택된 것입니다. 그룹에 속한 개별 패키지 목록을 보시려면, **자세한 정보**를 클릭하시기 바랍니다. 개별 패키지 옆에 체크 표시가 있다면 그 패키지는 현재 설치를 위해 선택된 것입니다.

33.1. 패키지 설치

현재 설치되지 않은 패키지 그룹에 속한 표준 패키지들을 설치하시려면, 설치할 패키지 옆에 위치한 체크박스에 체크하십시오. 그룹 내에서 설치할 패키지를 사용자 정의하시려면, **자세한 정보** 버튼을 클릭하십시오.

그림 33-2와 같은 표준 패키지와 추가 패키지 목록이 나타날 것입니다. 패키지 이름에 클릭하시면 패키지 설치에 필요한 디스크 공간 요건이 화면 아래쪽에 표시됩니다. 패키지를 설치하시려면, 패키지 이름 옆에 위치한 체크박스를 체크해 주십시오.

또한 이미 설치된 패키지 그룹에 속한 개별 패키지를 선택하는 것도 가능합니다. **자세한 정보** 버튼을 클릭하신 후 설치되지 않은 추가 패키지를 선택하시면 됩니다.

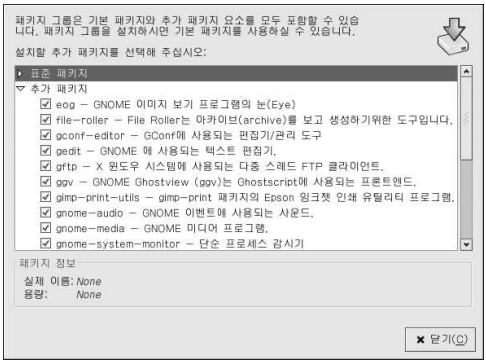

그림 33-2. 개별 패키지 선택

설치할 패키지 그룹과 개별 패키지의 선택을 마치신 후, 기본 화면에서 **업데이트** 버튼을 클릭해 주십시오. 패키지 관리 프로그램은 선택하신 패키지를 설치하는데 필요한 디스크 공간 용량을 비롯하여 패키지 간의 의존성 문제를 계산하여 요약 화면으로 보여줍니다. 만일 패키지 간의 의존성 문제가 발생한다면, 필요한 패키지를 자동으로 설치할 패키지 목록에 추가시켜 줍니다. 설치할 패키지의 전체 목록을 보시려면 **자세한 정보 보기** 버튼을 클릭하시면 됩니다.

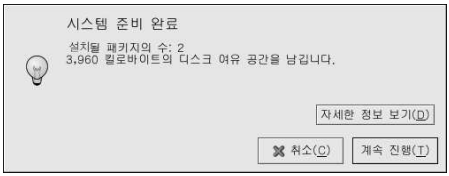

그림 33-3. 패키지 설치 요약 정보

계속 진행 버튼을 클릭하시면 설치가 시작됩니다. 설치를 마치면, **업데이트 완료** 메시지가 나타날 것입니다.

힌트

Nautilus 프로그램은 파일과 디렉토리 검색 기능 뿐만 아니라 패키지 설치 기능도 갖추고 있습니다. **Nautilus**에서 RPM 패키지 (보통 파일명 끝이 `.rpm`인 파일)을 포함하고 있는 디렉토리로 가신 후 RPM 아이콘에 두번 클릭하시기 바랍니다.

33.2. 패키지 삭제

패키지 그룹에서 설치된 패키지를 모두 삭제하시려면, 옆에 위치한 체크박스가 체크되지 않게(uncheck) 해 주십시오. 개별 패키지를 삭제하시려면, 패키지 그룹 옆에 위치한 **자세한 정보** 버튼을 클릭하신 후 개별 패키지를 체크 해제하시면 됩니다.

삭제할 패키지 선택을 마치셨으면, 기본 화면에서 **업데이트** 버튼을 클릭해 주십시오. 패키지 관리 프로그램은 선택하신 패키지가 삭제된 후 여유 디스크 공간을 비롯하여 패키지 간의 의존성 문제를 계산하여 요약 화면으로 보여줍니다. 만일 다른 패키지가 삭제될 패키지에 의존하고 있는 경우, 다른 패키지는 자동으로 삭제할 패키지 목록에 추가됩니다. 삭제될 패키지의 목록을 보시려면 **자세한 정보 보기** 버튼을 클릭하시기 바랍니다.

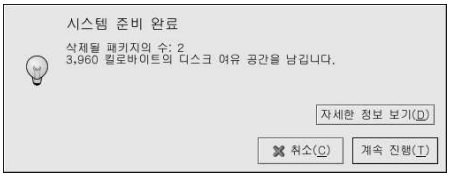

그림 33-4. 패키지 삭제 요약 정보

계속 진행 버튼을 클릭하시면 삭제 과정이 시작됩니다. 삭제 과정이 완료되면, **업데이트 완료** 메시지가 나타날 것입니다.

힌트

설치하거나 삭제할 패키지 그룹/패키지를 선택하신 후 **업데이트** 버튼을 클릭하시면, 패키지를 설치하면서 동시에 삭제하실 수 있습니다. **시스템 준비 완료** 화면이 나타나 설치할 패키지와 삭제될 패키지의 수를 보여줍니다.

34장 .

Red Hat Network

Red Hat Network는 다수의 Red Hat Linux 시스템을 관리하기 위한 인터넷 솔루션 입니다. ' **Red Hat 업데이트 에이전트** 독립형 응용 프로그램을 사용하시거나, RHN 웹사이트인 http://rhn.redhat.com/을 방문하셔서 Red Hat에서 모든 보안 경고, 버그 수정 통보와 소프트웨어 업데이트 통보 (총체적으로 에라타 통보)를 직접 다운로드 받으실 수 있습니다.

그림 34-1. 여러분의 RHN

업데이트된 패키지가 출시될 때마다 Red Hat Network는 여러분께 알림 이메일을 보내드리기 때문에 여러분의 시간이 절약됩니다. 여러분은 업데이트된 패키지나 보안 경고를 찾기 위해 인터넷을 직접 검색하실 필요가 없어 졌습니다. Red Hat Network는 디폴트로 업데이트된 패키지를 설치도 해드립니다. 따라서 여러분은 RPM 사용 방법이나 소프트웨어 패키지 간의 의존성 해결을 걱정하실 필요가 없습니다; RHN가 모두 책임지고 해드립니다.

각 Red Hat Network 계정은 다음과 같은 기능을 제공합니다:

- 에라타 통보 — 기본 인터페이스를 통하여 네트워크 상에 존재하는 모든 시스템에 대한 새로운 보안 경고, 버그 수정 통보와 소프트웨어 업데이트 통보가 발생될 때마다 여러분께 알려 드립니다.

그림 34-2. 관련 에라타

- 자동 이메일 통지 — 여러분의 시스템에 에라타 통보가 발생될 때마다 이메일을 통해 알려 드립니다.
- 에라타 업데이트 스케줄 — 계획된 시기에 자동 설치를 실행하실 수 있도록 에라타 업데이트를 보내드립니다.
- 패키지 설치 — 버튼 클릭 한번으로 여러 개의 시스템에 대한 패키지 설치를 미리 계획하실 수 있습니다.
- **Red Hat 업데이트 에이전트** — **Red Hat 업데이트 에이전트**을 사용하여 최신 소프트웨어 패키지를 다운로드 받으실 수 있습니다. (패키지 설치는 옵션입니다)
- Red Hat Network 웹사이트 — 이 웹사이트에 접속하셔서 다중 시스템과 다운로드 받은 개별 패키지들, 그리고 에라타 업데이트와 같은 스케줄 작업을 관리하실 수 있습니다.

Red Hat Network를 사용하시기 전에 다음과 같은 세가지 기본적인 절차를 따르십시오:

1. 다음 중 한가지 방법을 사용하여 시스템 프로파일을 생성하시기 바랍니다:
   - 설치 후 처음으로 시스템을 부팅시 **설정 에이전트**을 통하여 RHN에 시스템을 등록하는 방법.
   - 데스크탑에서 **주 메뉴 버튼** => **시스템 도구** => **Red Hat Network**를 선택하는 방법.
   - 쉘 프롬프트에서 `up2date` 명령을 실행하는 방법.
2. 이제 여러분의 시스템이 서비스를 받을 수 있도록 http://rhn.redhat.com/으로 가셔서 RHN에 로그인하십시오. 모든 사용자 분들께 한 시스템 당 한 개의 무료 Red Hat Network 계정을 드립니다. 추가 계정은 구입하셔야 합니다.
3. RHN 웹사이트를 통해 업데이트 스케줄을 잡으시거나 **Red Hat 업데이트 에이전트**를 사용하여 에라타 업데이트를 다운로드 받으신 후 설치하십시오.

보다 자세한 정보를 보시려면, http://www.redhat.com/docs/manuals/RHNetwork/으로 가셔서 *Red Hat Network* 사용자 참조 가이드 *(User Reference Guide)*를 참조하시기 바랍니다.

힌트

Red Hat Linux는 여러분이 가지고 계신 Red Hat Linux 시스템이 업데이트될 경우, 여러분이 알기 쉽게 패널 아이콘으로 업데이트를 통지해 드리는 **Red Hat Network 통지 도구**를 포함하고 있습니다. 이 애플릿에 대한 보다 많은 정보는 다음 URL을 참조하시기 바랍니다: http://rhn.redhat.com/help/basic/applet.html

VI. 부록

이 부록편에는 Red Hat, Inc.가 제공한 소스 파일을 이용하여 사용자 정의 커널을 개발하는 방법에 대한 정보를 제공합니다. 또한 보안 통신에 사용되는 도구인 Gnu Privacy Guard에 대하여 설명도 포함되어 있습니다.

차례

부록 A.

맞춤 커널 만들기

Linux를 처음 대하시는 사용자들은 종종 "왜 맞춤 커널을 만들어야 하는가?"에 대한 의문을 갖습니다. 커널 모듈의 사용량에 견주어 판단시 "맞춤 커널을 만드는 이유를 알지 못한다면 아마도 만들 필요가 없다."는 것이 이 질문에 대한 가장 정확한 대답이라 할 수 있습니다.

Red Hat Linux에 함께 제공된 커널과 Red Hat Linux 에라타 시스템을 통해 제공된 커널은 대부분의 최신 하드웨어와 커널 기능에 대한 지원을 제공합니다. 대부분의 사용자 여러분들은 커널을 재컴파일하지 않고서 사용하실 수 있습니다. 이 부록은 커널 재컴파일하는 방법에 대하여 보다 자세한 정보를 알고자 하시는 분들과, 커널에 실험적인 기능을 컴파일하기와 같은 작업을 수행하고자 하시는 분들께 참조 가이드를 제공해 드립니다.

Red Hat, Inc.에서 배포한 커널 패키지를 사용하여 커널을 업그레이드하시려면, 30 장을 참조하시기 바랍니다.


경고

맞춤 커널 개발은 Red Hat Linux 설치 지원팀에서 지원하지 않습니다. Red Hat, Inc.에서 배포한 RPM 패키지를 사용하여 커널을 업그레이드하는 방법에 대한 보다 자세한 정보는 30 장을 참조하시기 바랍니다.

A.1. 개발 준비하기

사용자 커널을 만들기 전에, 실수할 경우를 대비하여 반드시 작동하는 비상용 부팅 디스켓을 만들어 두셔야 합니다. 현재 실행 중인 커널을 사용하여 부팅할 부팅 디스켓을 만드시려면, 다음 명령을 실행하시기 바랍니다:

```
/sbin/mkbootdisk `uname -r`
```

디스켓을 만드신 후, 시스템을 제대로 부팅하는지 반드시 테스트하시기 바랍니다.

커널을 재컴파일하시려면, `kernel-source` 패키키가 설치되어 있어야 합니다. 다음 명령을 입력하여

```
rpm -q kernel-source
```

패키지가 설치되어 있는지 여부를 알아 보십시오. 만일 설치되어 있지 않다면, Red Hat Linux CD-ROM이나 ftp://ftp.redhat.com에서 Red Hat FTP 사이트 (미러 목록은 http://www.redhat.com/mirrors.html에서 찾으실 수 있습니다), 또는 Red Hat Network에서 패키지를 설치하십시오. RPM 패키지를 설치하는 방법에 대한 보다 자세한 정보는 V 부을 참조하시기 바랍니다.

A.2. 커널 만들기

이 섹션에서는 모듈화된 맞춤 커널 만들기에 대하여 설명해 보겠습니다. 단일 커널 (monolithic kernel)을 만드시려면, A.3 절에서 단일 커널 개발과 설치에 대한 설명을 참조하시기 바랍니다.


알림

이 예시에서서는 2.4.20-2.47.1 을 커널 버전으로 사용합니다 (커널 버전은 다를 수도 있습니다). `uname -r` 명령을 입력하시면 커널 버전을 알 수 있습니다. 2.4.20-2.47.1을 알아낸 커널 버전으로 바꾸십시오.

x86 구조에 사용될 맞춤 커널을 만드는 방법은 다음과 같습니다 (모든 작업을 루트로 실행하셔야 합니다):

1. 쉘 프롬프트를 열고 `/usr/src/linux-2.4/` 디렉토리로 이동합니다. 앞으로 모든 명령어는 이 디렉토리에서 실행되어야 합니다.
2. 안정적인 환경에서 소스 트리를 사용하여 커널 개발을 시작하는 것이 중요합니다. 따라서 먼저 `make mrproper` 명령을 사용하여 소스 트리 주위에 흩어져 있는 이전 버전의 잔여물이나 설정 파일을 제거해 주십시오. 만일 `/usr/src/linux-2.4/.config`라는 기존 설정 파일이 있다면, 이 명령을 실행하기 전에 다른 디렉토리로 백업하신 후 나중에 다시 이 디렉토리로 가져옵니다.
3. 기본 Red Hat Linux 커널의 설정을 사용하여 시작하시길 권장합니다. 이렇게 하시려면, `/usr/src/linux-2.4/configs/` 디렉토리에서 시스템 구조에 맞는 설정 파일을 `/usr/src/linux-2.4/.config`로 복사하시기 바랍니다. 만일 시스템 메모리 용량이 4 기가바이트 이상이라면, 키워드 `bigmem`를 포함한 파일을 복사하십시오.
4. 다음으로 셋팅을 사용자 설정하십시오. 만일 X 윈도우 시스템을 사용 가능하다면, **리눅스 커널 설정** 프로그램을 실행하기 위해 `make xconfig` 명령을 사용하시길 권장합니다.

알림

`make xconfig` 명령을 사용하여 시작된 그래픽 도구를 사용하시려면, `wish` 명령을 제공하는 `tk` 패키지가 설치되어 있어야 합니다. RPM 패키지를 설치하는 방법에 대한 보다 자세한 정보는 V 부을 참조하시기 바랍니다.

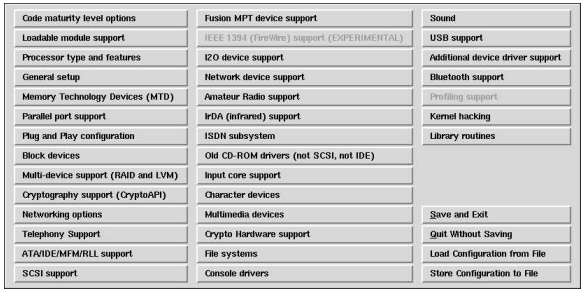

그림 A-1. 커널 요소 범주 설정하기

그림 A-1에서 설정할 요소 범주를 클릭하여 선택해 주십시오. 각 범주 내에서는 구성 요소가 포함되어 있습니다. 구성 요소를 커널로 컴파일하시려면 **y** (yes)를 선택하시고, 커널 모듈로 컴파일 하시려면 **m** (모듈), 또는 컴파일하지 않으려면 **n** (no) 항목을 선택해 주십시오. 구성 요소에 대한 보다 자세한 정보를 원하시면, 구성 요소 앞에 위치한 **도움말** 버튼을 클릭하시기 바랍니다.

범주 목록으로 되돌아가시려면 **주 메뉴** 버튼을 클릭하십시오.

설정을 마친 후, 주 메뉴 창에서 **저장 후 종료 버튼**을 클릭하여 `/usr/src/linux-2.4/.config` 설정 파일을 생성하신 후 **리눅스 커널 설정** 프로그램을 종료하시기 바랍니다.

설정에 아무런 변화를 주지 않은 경우에도, 계속 진행하시기 전에 `make xconfig` 명령 (또는 커널 설정에 사용된 다른 방법)을 실행하셔야 합니다.

커널 설정을 위해 사용 가능한 다른 방법들은 다음과 같습니다:

- `make config` — 상호 대화식 텍스트 프로그램. 한 줄에 한 개씩 구성 요소들에 대한 질문이 나타나면 여러분은 한번에 한개씩 대답합니다. X 윈도우 시스템이 필요하지 않는 방법으로서, 이전 질문에 대한 대답 변경이 불가능합니다.
- `make menuconfig` — 텍스트 모드로 구성된 메뉴 위주의 프로그램. 구성 요소가 여러 범주로 나뉘어진 메뉴에 나타납니다; 텍스트 모드 Red Hat Linux 설치 프로그램에서 사용했던 방식과 똑같은 방법으로 원하시는 구성 요소를 선택하시면 됩니다. 다음 중 포함시킬 항목에 맞는 태그(tag)를 선택해 주십시오: **[*]** (내장), **[ ]** (제외), <**M**> (모듈), 또는 < > (모듈 가능). X 윈도우 시스템이 없어도 이 방법을 사용 가능합니다.

- `make oldconfig` — 디폴트 설정 파일을 만드는 비-대화식 스크립트. 디폴트 Red Hat Linux 커널을 사용하시는 경우, 이 명령을 사용하시면 Red Hat Linux에 포함된 커널에 맞는 설정 파일이 생성됩니다. 이 방법은 원하지 않는 기능을 사용하지 않도록 커널을 디폴트 설정하는데 유용합니다.

알림

`kmod`와 커널 모듈을 사용하시려면, 설정 과정에서 `kmod support`와 `module version (CONFIG_MODVERSIONS) support`에 대해서 **Yes**라고 대답하셔야 합니다.

5. `/usr/src/linux-2.4/.config` 파일을 생성하신 후, 모든 의존성 관계를 올바르게 설정하기 위하여 `make dep` 명령어를 실행하시기 바랍니다.
6. `make clean` 명령을 사용하여 커널 개발에 사용될 소스 트리를 준비합니다.
7. 기존 커널을 덮어쓰지 않도록 개발 중인 사용자 정의 커널에 다른 버전 번호를 부여하시기를 권장합니다. 이렇게 하시는 것이 사고 발생시 가장 쉽게 복구할 수 있는 방법입니다. 다른 방법에 대하여 알고 싶으시다면, http://www.redhat.com/mirrors/LDP/HOWTO/Kernel-HOWTO.html 또는 `/usr/src/linux-2.4`의 `Makefile`에서 자세한 사항을 참조하시기 바랍니다.

   `/usr/src/linux-2.4/Makefile` 파일을 보시면, `EXTRAVERSION`로 시작하는 줄 마지막에는 `custom`이라는 단어가 기본으로 포함되어 있습니다. 줄 마지막 부분에 문자열을 삽입하시면 아직 작동하는 이전 커널과 새 커널 (2.4.20-2.47.1custom 버전)이 시스템 상에 동시에 존재하게 됩니다.

   커널에 고유한 이름을 부가하시려면, 이 문자열 마지막에 날짜 (또는 다른 식별자)를 함께 첨가해 주십시오.
8. `make bzImage`을 사용하여 커널을 만듭니다.
9. `make modules` 명령을 사용하여 설정하신 모듈을 만듭니다.
10. `make modules_install` 명령을 사용하여 커널 모듈을 설치하실 수 있습니다. (커널 모듈을 만들지 않은 경우에도 설치 가능합니다). 반드시 밑줄 (_)을 입력하는 것을 잊지 마십시오. 이 명령은 `/lib/modules/<KERNELVERSION>/kernel/drivers` 디렉토리 경로에 커널 모듈을 설치할 것입니다. (앞의 경로에서 *KERNELVERSION*은 `Makefile`에서 지정된 커널 버전입니다). 이 예시에서 디렉토리 경로는 `/lib/modules/2.4.20-2.47.1custom/kernel/drivers/`가 됩니다.
11. `make install` 명령을 사용하여 새 커널과 관련 파일들을 적절한 디렉토리로 복사해 주십시오.

    이 명령은 `/boot` 디렉토리에 커널 파일을 설치할 뿐만 아니라 새로운 `initrd` 이미지를 만드는 `/sbin/new-kernel-pkg` 스크립트를 실행하고 부트로더 설정 파일에 새로운 항목을 추가합니다.

    SCSI 어댑터를 가지고 계신 경우, SCSI 드라이버를 모듈로 컴파일하거나 (Red Hat Linux에서 디폴트인) ext3 지원을 갖춘 커널을 모듈로 컴파일하기 위해서는 `initrd` 이미지가 필요합니다.
12. `initrd` 이미지와 부트로더가 올바르게 만들어졌는지와 2.4.20-2.47.1 대신 맞춤 커널 버전을 사용하는지 확인해 주십시오. 이러한 수정된 사항을 확인하는 방법에 대한 보다 자세한 정보를 원하신다면, 30.5 절과 30.6 절을 참조하시기 바랍니다.

A.3. 단일 커널 만들기

단일 커널을 만들기 위해서는 모듈화된 커널을 만드는 것과 동일한 과정을 따르지만 몇가지 예외가 있습니다.

- 커널을 설정하실 때, 모듈로 컴파일하시면 안됩니다. 즉, 질문에 대하여 **Yes** 또는 **No**라고만 대답합니다. 또한 `kmod support` 와 `module version (CONFIG_MODVERSIONS) support`에 대해서는 반드시 **No**라고 대답하셔야 합니다.
- 다음 과정은 생략해 주십시오:
  `make modules`
  `make modules_install`

- `nomodules` 명령을 사용하여 `grub.conf` 파일에 `kernel` 줄을 추가하거나 `lilo.conf` 파일에 `append=nomodules` 줄을 추가하시기 바랍니다.

A.4. 추가 자료

리눅스 커널에 대한 보다 자세한 정보를 원하신다면, 다음 자료들을 참조해 보십시오.

A.4.1. 설치된 문서 자료

- `/usr/src/linux-2.4/Documentation` — 리눅스 커널과 모듈에 대한 고급 문서 자료. 이 문서는 커널 소스 코드에 기여하고 커널이 작용하는 방식을 이해하는데 관심이 있는 독자를 대상으로 작성되었습니다.

A.4.2. 유용한 웹사이트

- http://www.redhat.com/mirrors/LDP/HOWTO/Kernel-HOWTO.html — 리눅스 문서화 프로젝트의 *The Linux Kernel HOWTO*.
- http://www.kernel.org/pub/linux/docs/lkml/ — linux-kernel 메일링 리스트.

Gnu Privacy Guard 시작하기

한번이라도 여러분과 다른 사람간에 주고 받는 이메일이 전송 과정에서 읽혀질 수 있다고 의심해 보셨습니까? 불행히도 여러분이 알지 못하는 제 3자가 이메일을 도중에 이메일을 가로채거나 심지어는 여러분이 보낸 이메일을 번조할 가능성도 있습니다.

전통적인 ("달팽이"라고도 불리는) 편지는 봉투 안에 넣어져 목적지에 도달할 때까지 우체국 지점에서 다른 지점으로 배달됩니다. 하지만 인터넷을 통한 메일 전달은 이만큼 안전하지 못합니다; 이메일은 보통 서버들 사이에서 암호화되지 않은 텍스트로 전송됩니다. 여러분의 이메일을 다른 사람이 보거나 번조하는 것을 방지할 수 있는 어떠한 특별 조치도 취해지지 않습니다.

여러분의 개인 정보 보호를 위하여, Red Hat Linux 9는 **GNU Privacy Guard**인 GnuPG를 포함하고 있으며, GnuPG는 전형적인 Red Hat Linux 설치 과정에서 기본으로 설치됩니다. GnuPG는 *GPG*라고도 부릅니다.

GnuPG는 보안 통신에 사용되는 도구로서 PGP (Pretty Good Privacy, 널리 사용되는 암호화 응용 프로그램)의 암호화 기술을 대체하는 완전 프리 소프트웨어 입니다. 여러분은 GnuPG를 사용하여 데이터와 이메일 내용을 암호화할 수 있을 뿐만 아니라 전자 서명 *(digital signature)*을 통해 사용자 인증할 수 있습니다. GnuPG는 또한 PGP 5.*x*을 해독하고 검증하는 능력을 갖추고 있습니다.

GnuPG와 다른 암호화 표준과의 호환성 덕분에, 여러분이 보내는 보안 이메일은 Windows와 Macintosh와 같은 다른 운영 체제의 이메일 응용 프로그램과도 호환될 것입니다.

GnuPG는 사용자가 안전하게 데이터를 교환할 수 있도록 공개키 암호화 *(public key cryptography)* 방식을 채택하고 있습니다. 공개키 암호화 방식에서 사용자는 두개의 키: 공개키(public key)와 비밀키(private key)를 생성해야 합니다. 공개키는 다른 사람과 교환하거나 키서버와 교환할 수 있지만 비밀키는 절대로 남에게 알려져서는 안됩니다.

암호화 방식은 두 키를 어떻게 사용하느냐에 따라 달라집니다. 관용 암호 방식(conventional cryptography)이나 대칭 암호 방식 (symmetric cryptography)은 암호화와 해독을 위해 동일한 키(비밀키)를 사용합니다. 반면에 공개키 암호 방식은 두개의 키:공개키와 비밀키를 모두 사용합니다. 수신자나 수신 조직은 자신의 공개키를 분배하고 비밀키를 비밀리에 보관합니다. 공개키로 암호화된 데이터는 오직 비밀키를 사용하여 해독될 수 있으며; 비밀키로 암호화된 데이터는 오직 공개키를 사용하여 해독할 수 있습니다.


중요

공개키는 안전하게 통신을 주고 받고자 하는 모든 사람에게 배포할 수 있지만 비밀키는 그야말로 여러분만 알고계셔야 한다는 것을 기억해 두십시오.

암호화는 이 메뉴얼에서 다루기에는 너무나 광범위한 주제입니다. 하지만 여러분이 이 장을 읽으신 후 실생활에서 스스로 GnuPG를 사용할 수 있을 만큼의 충분한 지식을 얻으실 꺼라고 믿습니다. GnuPG, PGP와 암호화 기술에 대한 보다 많은 정보를 원하신다면, B.8 절을 참조하시기 바랍니다.

B.1. 설정 파일

GnuPG 명령을 처음으로 실행하시면, 여러분의 홈 디렉토리에 `.gnupg` 디렉토리가 생성됩니다. 1.2 이후 버전부터 설정 파일명이 `.gnupg/options`에서 `.gnupg/gpg.conf`으로 변경되었습니다. 만일 홈 디렉토리에서 `.gnupg/gpg.conf` 파일을 찾을 수 없다면, `.gnupg/options` 파일이 사용됩니다. 1.2 이후 버전만 사용하신다면, 다음 명령을 사용하여 여러분이 가지고 계신 설정 파일의 이름을 변경하시길 권장합니다:

```
mv ~/.gnupg/options ~/.gnupg/gpg.conf
```

1.0.7 이전 버전에서 업그레이드 하신다면, 키링을 읽어오는데 걸리는 시간을 줄이기 위하여 여러분의 키링에 서명 캐시를 생성할 수 있습니다. 이 작업을 수행하시려면, 다음과 같은 명령을 실행하시기 바랍니다:

```
gpg --rebuild-keydb-caches
```

B.2. 경고 메시지

GnuPG 명령을 실행하시면 다음과 같은 메시지를 보실 겁니다:

```
gpg: Warning: using insecure memory!
```

이 경고 메시지는 루트가 아닌 사용자가 메모리 페이지를 잠글 수 없기 때문에 나타납니다. 만일 사용자가 메모리 페이지를 잠글 수 있다면, 사용자는 메모리 부족 서비스 거부(Denial-of-service) 공격을 가할 수 있습니다. 따라서 보안상 허점이 됩니다. 자세한 사항은 http://www.gnupg.org/(en)/documentation/faqs.html#q6.1를 참조하시기 바랍니다.

다음과 같은 메시지가 나타날 경우도 있습니다:

```
gpg: WARNING: unsafe permissions on configuration file "/home/username/.gnupg/gpg.conf"
```

이 메시지는 만일 여러분의 설정 파일이 다른 사용자가 읽을 수 있는 파일 허가를 가지고 있는 경우 나타납니다. 이 경고 메시지를 보시면, 다음과 같은 명령을 사용하여 파일 허가를 변경하시기 바랍니다:

```
chmod 600 ~/.gnupg/gpg.conf
```

일반적으로 나타나는 또 다른 경고 메시지는 다음과 같습니다:

```
gpg: WARNING: unsafe enclosing directory permissions on configuration file
"/home/username/.gnupg/gpg.conf"
```

이 메시지는 설정 파일을 포함한 디렉토리의 파일 허가가 다른 사용자가 그 내용을 읽을 수 있도록 설정되어 있는 경우 나타납니다. 이 경고 메시지가 나타난다면 다음과 같은 명령을 사용하여 파일 허가를 변경하시기 바랍니다:

```
chmod 700 ~/.gnupg
```

이전 GnuPG 버전에서 업그레이드하셨다면, 다음과 같은 메시지가 나타날 경우가 있습니다:

```
gpg: /home/username/.gnupg/gpg.conf:82: deprecated option "honor-http-proxy"
gpg: please use "keyserver-options honor-http-proxy" instead
```

이 경고 메시지는 `~/.gnupg/gpg.conf` 파일에 다음과 같은 라인이 포함되어 있기 때문에 나타납니다:

```
honor-http-proxy
```

1.0.7 이후 버전은 다른 구문을 선호합니다. 해당 라인을 다음과 같이 변경해 주십시오:

```
keyserver-options honor-http-proxy
```

B.3. 키쌍 생성하기

GnuPG를 사용하시려면 먼저 새로운 키쌍: 공개키와 비밀키를 생성하셔야 합니다.

키쌍을 생성하기 위해서는 쉘 프롬프트에서 다음의 명령을 입력합니다:

```
gpg --gen-key
```

여러분은 사용자 계정을 가장 빈번히 사용하기 때문에 (루트가 아닌) 사용자 계정으로 로그인하셔서 이 작업을 수행하셔야 합니다.

소개 화면이 나타나며 키 옵션을 보여줍니다. 이 중 한 옵션은 디폴트로서 권장됩니다. 다음을 보십시오:

```
gpg (GnuPG) 1.2.1; Copyright (C) 2002 Free Software Foundation, Inc.
This program comes with ABSOLUTELY NO WARRANTY.
This is free software, and you are welcome to redistribute it
under certain conditions. See the file COPYING for details.

Please select what kind of key you want:
  (1) DSA and ElGamal (default)
  (2) DSA (sign only)
  (5) RSA (sign only)
Your selection?
```

실제로 옵션을 선택하는 대부분의 화면에서는 디폴트 옵션이 괄호 안에 나타납니다. 간단히 [Enter] 키를 누르시면 디폴트 옵션을 사용합니다.

첫 화면에서는 디폴트 옵션: `(1) DSA and ElGamal`을 선택하셔야 합니다. 이 옵션을 선택하시면 디지털 서명을 생성하고 두가지 유형의 기술을 사용하여 암호화(와 해독)이 가능해집니다. 기본값인 **1**을 입력하고 [Enter] 키를 칩니다.

다음은 키 크기를 결정하는 단계입니다. 일반적으로 키의 길이가 길수록 더 안전합니다. 보통의 경우에는 디폴트 값인 1024 비트가 적당합니다. [Enter] 키를 치고 넘어갑니다.

다음 옵션은 키의 유효 기간을 정하는 것입니다. 일반적으로 디폴트 값 (`0 = key does not expire`)을 사용합니다. 만일 유효 기간을 정하시면, 공개키를 교환한 모든 사람들에게 공개키의 만기일을 알려서 새로운 공개키를 바꾸어 주는 것을 잊지 마십시오. 유효 기간을 정하지 않으신다면, 결정을 다시 확인하도록 요청할 것입니다. 확인을 위해 [y] 키를 눌러 주십시오.

다음은 사용자 이름, 이메일 주소와 간단한 설명이 담긴 사용자 ID를 결정하는 것입니다. 결정이 완료되면 여러분이 입력하신 정보가 요약되어 나타납니다.

더 바꿀 것이 없으면 비밀문구(passphrase)를 입력합니다.

힌트

여러분의 계정 암호와 마찬가지로 GnuPG에서 최적의 보안을 위해서는 좋은 비밀문구가 필요합니다. 예로 들면 비밀문구에 대문자와 소문자, 숫자 또는 구두점을 섞어서 사용하는 것이 좋습니다.

일단 비밀문구를 입력하고 확인하시면 공개키와 비밀키가 생성됩니다. 다음과 같은 메시지가 나타날 것입니다:

```
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
+++++.+++++.++++++++....++++++++++..+++++.+++++.+++++++.+++++++
+++.++++++++++++++++++++++++++++++++++++++++.........................++++
```

화면에서 이루어지던 작업이 멈추면 새로운 키들이 만들어져서 여러분 홈 디렉토리 안의 `.gnupg` 디렉토리에 저장됩니다. 공개키와 비밀키를 보기 위해서는 다음 명령을 사용합니다:

```
gpg --list-keys
```

다음과 유사한 결과가 나타날 것입니다:

```
/home/username/.gnupg/pubring.gpg
---------------------------------------
pub 1024D/B7085C8A 2000-06-18 Your Name <you@example.com>
sub 1024g/E12AF9C4 2000-06-18
```

1.0.6 이전 버전 GnuPG 키를 생성하신 경우, 여러분의 비밀키를 보내기하신 후 새로운 비밀키를 가져오셨다면 1.0.7 이후 버전 항목을 사인하기 위해 여러분의 키를 멍백하게 신용해주셔야 합니다. 키를 신용하기 위해서는 다음과 같은 명령을 입력하십시오 (*<user-id>* 부분을 여러분의 사용자 ID로 대체하시기 바랍니다):

```
gpg --edit-key <user-id>
```

`Command>` 프롬프트에서 **`trust`**라고 입력하신 후 키를 신용하기 위하여 `5 = I trust ultimately`를 선택하십시오.

B.4. 철회 인증서 만들기

키쌍을 생성하고 나서 공개키에 대한 철회 인증서를 만들셔야 합니다. 비밀문구를 잊어 먹었거나 또는 비밀문구가 노출되었다면, 이 철회 인증서를 발행하여 사람들에게 더 이상 여러분의 공개키를 사용하지 않도록 알려야 합니다.

알림

철회 인증서를 만든다고 해서 여러분이 생성하신 키를 철회하는 것이 아닙니다. 대신 여러분의 키가 공개적으로 사용되는 것을 철회하기 위한 안전한 대안을 준비하는 것입니다. 여러분이 키를 생성했다고 가정하고 비밀 문구를 잊어 먹었거나, ISP (주소)를 변경했거나 하드 드라이브가 파괴되는 경우가 발생할 수 있습니다. 이러한 경우에 철회 인증서는 여러분의 공개키를 무능하게 하기위해 사용됩니다.

여러분의 키가 철회되기 이전에 여러분의 메일을 읽었던 사람들에게는 여러분의 서명이 유효할 것이며 철회 전에 여러분이 받았던 메시지는 해독할 수 있습니다. 철회 인증서를 만들기 위해서는 `--gen-revoke` 옵션을 사용합니다:

```
gpg --output revoke.asc --gen-revoke <you@example.com>
```

만일 앞의 예에서 `--output revoke.asc` 옵션을 빠뜨리면 철회 인증서는 모니터 화면에 출력됩니다. 텍스트 편집기를 사용하여 출력 결과를 선택하신 파일로 복사하여 붙일 수 있지만, 여러분의 로그인 디렉토리에 있는 파일로 출력 결과를 보내는 것이 편합니다. 이러한 방식으로 인증서를 보관하거나 또는 플로피 디스크에 복사하여 안전한 곳에 저장하십시오.

다음과 같은 결과가 출력됩니다:

```
sec 1024D/823D25A9 2000-04-26 Your Name <you@example.com>

Create a revocation certificate for this key?
```

[Y] 키를 눌러 얼거된 키에 대한 철회 인증서를 생성합니다. 다음으로 철회 인증서를 생성하는 이유를 선택하신 후 보다 자세한 설명은 옵션으로 작성하셔도 되고 그냥 두셔도 됩니다. 이유를 선택하신 후 키를 생성하는데 사용할 비밀 문구를 입력해 주십시오.

철회 인증서가 만들어지면 (`revoke.asc`), 여러분의 로그인 디렉토리에 저장됩니다. 여러분은 인증서를 플로피 디스켓에 저장한 후 안전한 장소에 잘 보관하셔야 합니다. (Red Hat Linux에서 디스켓으로 파일을 복사하는 방법을 모르신다면 *Red Hat Linux* 시작하기 가이드를 참조하시기 바랍니다.)

B.5. 공개키 보내주기

공개키 암호 방식을 사용하기 이전에 다른 사람들이 여러분 공개키의 복사본을 가지고 있어야 합니다. 공개키를 다른 사람이나 키서버에 보내주기 위해서는, 키를 보내기 *(export)*해야 합니다.

키를 웹 페이지 상에 올리거나 이메일에 붙일 수 있도록 키를 보내기 위해서는, 다음과 같은 명령을 입력합니다:

```
gpg --armor --export <you@example.com> > mykey.asc
```

아무런 결과도 출력되지 않을 것입니다. 그 이유는 공개키가 전달되었을 뿐만 아니라 출력 결과가 파일 (예, `mykey.asc`)로 방향 지정되었기 때문입니다. (`> mykey.asc` 명령이 없다면, 키(key)는 모니터 화면에 출력됩니다.)

이제 `mykey.asc` 파일을 이메일에 삽입하거나 키서버로 보낼 수 있습니다. 키를 보시려면, `less mykey.asc` 명령을 입력하여 페이지 보기 프로그램에서 파일을 엽니다. (페이지 보기 프로그램을 종료하려면 [q]를 입력하십시오.) 다음과 같이 나타날 것입니다:

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.0.1 (GNU/Linux)
Comment: For info see http://www.gnupg.org

mQGiBDkHP3URBACkWGsYh43pkXU9wj/X1G67K8/DSrl85r7dNtHNfLL/ewil10k2
q8saWJn26QZPsDVqdUJMOdHfJ6kQTAt9NzQbgcVrxLYNfgeBsvkHF/POtnYcZRgL
tZ6syBBWs8JB4xt5V09iJSGAMPUQE8Jpdn2aRXPApdoDw179LM8Rq6r+gwCg5ZZa
pGNlkgFu24WM5wC1zg4QTbMD/3MJCSxfL99Ek5HXcB3yhj+o0LmIrGAVBgoWdrRd
BIGjQQFhV1NSwC8YhN/4nGHWpaTxgEtnb4CI1wI/G3DK9olYMyRJinkGJ6XYfP3b
cCQmqATDF5ugIAmdditnw7deXqn/eavaMxRXJM/RQSgJJyVpbAO2OqKe6L6Inb5H
kjcZA/9obTm499dDMRQ/CNR92fA5pr0zriy/ziLUow+cqI59nt+bEb9nY1mfmUN6
SW0jCH+pIQH5lerV+EookyOyq3ocUdjeRYF/d2jl9xmeSyL2H3tDvnuE6vgqFU/N
sdvby4B2Iku7S/h06W6GPQAe+pzdyX9vS+Pnf8osu7W3j60WprQkUGF1bCBHYWxs
YWdoZXIgPHBhdWxnYWxsQHJlZGhhdC5jb20+iFYEExECABYFAjkHP3UECwoEAwMV
AwIDFgIBAheAAAoJEJECmvGCPSWpMjQAoNF2zvRgdR/8or9pBhu95zeSnkb7AKCm
/uXVS0a5KoN7J61/1vEwx11poLkBDQQ5Bz+MEAQA8ztcWRJjW8cHCgLaE402jyqQ
37gDT/n4VS66nU+YItzDFScVmgMuFRzhibLblfO9TpZzxEbSF3T6p9hLLnHCQ1bD
HRsKfh0eJYMMqB3+HyUpNeqCMEEd9AnWD9P4rQtO7Pes38sV0lX0OSvsTyMG9wEB
vSNZk+Rl+phA55r1s8cAAwUEAJjqazvk0bgFrw1OPG9m7fEeDlvPSV6HSA0fvz4w
c7ckfpuxg/URQNf3TJA00Acprk8Gg8J2CtebAyR/sP5IsrK5l1luGdk+l0M85FpT
/cen2OdJtToAF/6fGnIkeCeP1O5aWTbDgdAUHBRykpdWU3GJ7NS6923fVg5khQWg
uwrAiEYEGBECAAYFAjkHP4wACgkQkQKa8YI9JamliwCfXox/HjlorMKnQRJkeBcZ
iLyPH1QAoI33Ft/0HBqLtqdtP4vWYQRbibjW
=BMEc
-----END PGP PUBLIC KEY BLOCK-----
```

B.5.1. 키서버로 보내기

소수의 사람들에게 이메일을 보내는 경우에는, 여러분의 공개키를 수출하여 직접 개인에게 보낼 수 있습니다. 하지만 다수의 사람들에게 이메일을 보내는 경우에 공개키를 개인적으로 보내는 것은 시간 낭비일 수 있습니다. 따라서 이러한 경우에는 키서버를 사용합니다.

키서버는 여러분의 공개키를 저장하고 요청한 사람에게 공개키를 배포하는 인터넷 상의 리포지터리입니다. 여러분이 사용할 수 있는 다수의 키서버가 존재하며 대부분의 키서버는 서로 동기화되어 있습니다. 따라서 한 서버로 여러분의 키를 보내는 것은 모든 키서버로 키를 보내는 것과 마찬가지입니다. 다른 사람들은 키서버에서 여러분의 공개키를 요청하고 받은 키를 자신의 키링으로 가져옵니다. 따라서 이 공개키를 가지고 있는 사람들은 여러분과 보안 통신을 주고 받을 준비가 되어 있습니다.

힌트

대부분의 키서버들이 동기화되어 있는 덕분에 여러분의 공개키를 한 서버에만 보내는 것은 모든 키서버로 보내는 것과 같은 역할을 합니다. 하지만 원하신다면, 다른 키서버를 지정할 수도 있습니다. 키서버에 대한 보다 많은 정보를 얻을 수 있는 곳은 *Keyserver.Net* 이며 http://www.keyserver.net에서 찾으실 수 있습니다.

쉘 프롬프트나 브라우저에서 공개키를 보내는 것도 가능합니다; 물론 키서버로 키를 보내거나 받기 위해서는 인터넷이 연결되어 있어야 합니다.

- 쉘 프롬프트에서 다음 명령을 입력합니다:
  `gpg --keyserver search.keyserver.net --send-key` *`you@example.com`*
- 브라우저를 열고 Keyserver.Net (http://www.keyserver.net) 으로 가신 후 여러분이 가지고 있는 PGP 공개키를 추가하는 옵션을 선택합니다.

  다음은 공개키를 복사하여 웹페이지 상의 적절한 공간에 붙여야 합니다. 도움이 필요하시다면, 다음을 참조하십시오:

  - 페이지 보기 프로그램 — 예, `less mykey.asc` 명령을 사용하여 보내기한 공개키 파일 (예, B.5 절에서 생성하신 *`mykey.asc`*)을 엽니다.
  - 마우스를 사용하여 `BEGIN PGP`에서 시작하여 `END PGP`에 이르는 파일의 모든 부분을 복사합니다. (그림 B-1 참조)
  - Keyserver.Net 페이지의 적절한 공간에 마우스 중간 클릭을 사용하여 *`mykey.asc`* 파일의 내용을 붙입니다. (두-버튼 마우스를 사용하는 경우에는 왼쪽과 오른쪽 동시 클릭을 사용). 그 후 키서버 페이지에서 **보내기** 버튼을 선택합니다. (만일 실수를 하셨다면 **복귀** 버튼을 눌러 여러분이 붙인 키를 지울 수 있습니다)

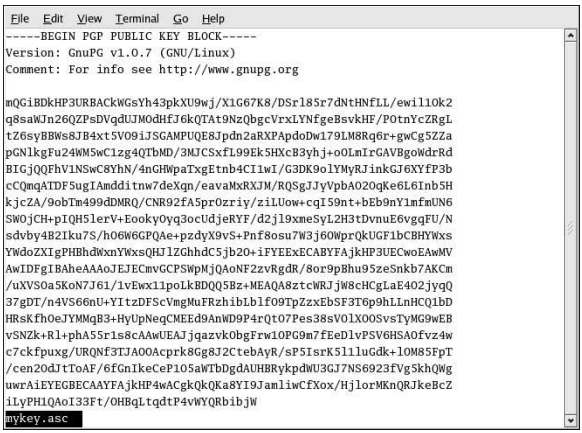

그림 B-1. 공개키 복사하기

다른 웹-기반 키서버에 키를 보내는 경우에 앞에서 설명된 과정과 동일합니다.

이제 다 마치셨습니다. 쉘 프롬프트나 웹을 사용한 여부에 관계 없이 여러분의 키가 성공적으로 보내졌다는 메시지가 — 쉘 프롬프트 또는 키서버의 웹페이지에 나타날 것입니다. 이제 여러분과 안전하게 통신을 주고받으려는 사용자들은 여러분의 공개키를 가져와서 자신의 키링에 추가할 수 있습니다.

B.6. 공개키 가져오기

이번에는 반대로 다른 사람의 공개키를 여러분의 키링으로 가져와야 합니다. — 이 과정은 키를 보내주기 만큼이나 간단합니다. 다른 누군가의 공개키를 가져와서 그 사람의 메일을 해독하고 또한 키링에 저장된 그 사람의 공개키에 전자 서명을 비교하여 확인해 볼 수 있습니다.

키를 가져오는 가장 쉬운 방법 중 하나는 웹 사이트에서 키를 다운로드 받아 저장하는 것입니다.

키를 다운로드 받은 후 *key.asc* 파일에 저장합니다. 다음과 같은 명령을 사용하여 키를 여러분의 키링에 추가하실 수 있습니다.

```
gpg --import key.asc
```

또 다른 방법으로 브라우저에서 **다른 이름으로 저장** 기능을 사용하여 키를 저장할 수 있습니다. **Mozilla**와 같은 브라우저를 사용하신다면 키서버에 키를 복사한 후 그 페이지를 텍스트 파일로 저장할 수 있습니다. **(파일 => 다른 이름으로 저장**을 선택). **저장된 문서 형식** 옆에 위치한 드롭다운 박스에서 **텍스트 파일 (*.txt)**을 선택합니다. 그 후 키를 가져올 수 있습니다 — 저장한 파일명을 잊지 마십시오. 예를 들어 키를 *newkey.txt*라는 이름의 텍스트 파일로 저장하셨다면, 파일을 가져오기 위해서는 쉘 프롬프트에서 다음과 같이 입력하시면 됩니다:

```
gpg --import newkey.txt
```

출력 결과는 다음과 유사할 것입니다:

```
gpg: key F78FFE84: public key imported
gpg: Total number processed: 1
gpg:       imported: 1
```

키를 성공적으로 가져왔는지 확인하기 위해서는 `gpg --list-keys` 명령을 사용합니다; 여러분의 키링에 새로 등록된 키가 나타날 것입니다.

공개키를 가져오신 후 그 키를 여러분의 키링 (공개키와 비밀키가 저장된 파일)에 저장합니다. 그 후 그 항목에서 파일이나 문서를 다운로드 받으실 경우 여러분의 키링에 추가하신 키를 비교하여 문서가 확실한지 확인해 보실 수 있습니다.

B.7. 전자 서명이란?

전자 서명은 여러분의 실제 서명에 비교될 수 있습니다. 여러분이 사인한 서명이 쉽게 변조될 가능성이 있는 전형적인 통신에서와는 달리 전자 서명은 위조될 수 없습니다. 그 이유는 바로 전자 서명은 여러분만 알고 있는 비밀키를 사용하여 생성되었으며 수신자는 여러분의 공개키를 사용하여 서명을 검증할 수 있기 때문입니다.

전자 서명은 문서에 시간 도장을 찍습니다; 즉, 여러분이 문서에 사인한 시간은 전자 서명의 일부가 됩니다. 따라서 누구든지 이 문서를 변조하려고 한다면 서명 검증에서 실패합니다. **Exmh** 또는 KDE의 **KMail**과 같은 일부 이메일 응용 프로그램들은 GnuPG를 사용하여 문서를 사인할 수 있는 기능을 갖추고 있습니다.

전자 서명의 두가지 유용한 형식은 압축안된 서명 *(clearsigned)* 문서 (서명을 압축하지 않고 문서에 붙이기)와 별도 서명 *(detached signatures)* (따로 만든 파일에 저장된 서명)입니다. 두가지 유형의 서명 모두 동일 인증 보안을 통하여 수신자가 메시지 전체를 해독하지 않고도 메시지를 읽을 수 있게 합니다.

압축안된 서명(clearsigned) 메시지에서 여러분의 서명은 문서 내의 텍스트 블록으로 나타납니다; 별도 서명(detached signatures)은 원본 문서와 별개의 파일로서 보내집니다.

B.8. 추가 자료

여기에서 다루어진 내용은 GnuPG에 대한 간략한 소개에 불과하며 실제로 훨씬 더 많은 암호화 기술이 존재합니다. 다음의 자료를 참조하시면 보다 많은 정보를 얻으실 수 있습니다.

B.8.1. 설치된 문서 자료

- `man gpg` 와 `info gpg` — GnuPG 명령과 옵션에 대한 간략한 참조 정보.

B.8.2. 유용한 웹사이트

- http://www.gnupg.org — GnuPG 웹사이트. 최신 GnuPG 배포 소식, 광범위한 사용자 가이드와 다른 암호화 자원에 대한 링크를 찾으실 수 있습니다.
- http://hotwired.lycos.com/webmonkey/backend/security/tutorials/tutorial1.html — Webmonkey의 *Encryption Tutorial*을 방문하셔서 암호화와 암호화 기술 적용 방법에 대한 보다 많은 정보를 참조하시기 바랍니다.
- http://www.eff.org/pub/Privacy — 전자 개척자 재단 (Electronic Frontier Foundation), "Privacy, Security, Crypto, & Surveillance" 아카이브.

B.8.3. 관련 서적

- 공식 *PGP* 사용자 가이드 저자 Philip R. Zimmerman; MIT Press
- *PGP: Pretty Good Privacy* 저자 Simson Garfinkel; O'Reilly & Associates, Inc.
- *E-Mail Security: How to Keep Your Electronic Messages Private* 저자 Bruce Schneier; John Wiley & Sons

색인

Symbols

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Y

판권

Red Hat Linux 메뉴얼은 DocBook SGML v4.1 형식으로 작성되었으며 HTML과 PDF 포맷은 사용자 정의된 DSSSL 스타일시트와 jade wrapper 스트립트를 사용하여 작성되었습니다. DocBook SGML 파일들은 **Emacs**로 PSGML 모드를 사용하여 작성되었습니다.

충고 (주목, 힌트, 중요, 주의와 경고) 그래픽들은 Garrett LeSage에 의해 만들어 졌습니다. Red Hat을 통해 자유롭게 배포 가능합니다.

Red Hat Linux 제품 문서 작성팀에는 다음과 같은 분들이 수고해 주셨습니다:

Sandra Moore A. — *Red Hat Linux x86* 설치 가이드의 주요 작가/관리자이자; *Red Hat Linux* 시작하기 가이드 작성에 기여한 작가.

Tammy Fox — *Red Hat Linux* 사용자 정의 가이드의 주요 작가/관리자이자; *Red Hat Linux* 시작하기 가이드 작성에 기여한 작가이며; 사용자 정의 DocBook 스타일시트와 스크립트의 작가/관리자.

Edward Bailey C. — *Red Hat Linux* 시스템 관리 입문서의 주요 작가/관리자이자; *Red Hat Linux x86* 설치 가이드 작성에 기여한 작가.

Johnray Fuller — *Red Hat Linux* 참조 가이드의 주요 작가/관리자이자; *Red Hat Linux* 보안 가이드의 공동 저자/공동 관리자이며; *Red Hat Linux* 시스템 관리 입문서 작성에 기여한 작가.

John Ha — *Red Hat Linux* 시작하기 가이드의 주요 작가/관리자이자; *Red Hat Linux* 보안 가이드의 공동 저자/공동 관리자이며; *Red Hat Linux* 시스템 관리 입문서 작성에 기여한 작가.

Michelle Jiyeen Kim (김지은) — *Red Hat Linux x86* 설치 가이드, *Red Hat Linux* 시작하기 가이드, *Red Hat Linux* 사용자 정의 가이드의 한국어 번역자.