우분투 서버 안내서

우분투 문서화 프로젝트 <ubuntu-doc@lists.ubuntu.com>

우분투 서버 안내서

지은이 우분투 문서화 프로젝트 <ubuntu-doc@lists.ubuntu.com>
저작권 © 2004, 2005, 2006 Canonical Ltd. 와 우분투 문서화 프로젝트의 멤버

초록

우분투에 서버 프로그램을 설치하고 설정하는 것에 대한 소개

명예와 저작권

다음의 우분투 문서화 팀 작성자가 이 문서를 유지관리 합니다:

- Bhuvaneswaran Arumugam

우분투 서버 안내서는 또한 이 분들의 공헌에 기초 합니다:

- Robert Stoffers
- Brian Shumate
- Rocco Stanzione

이 문서는 GNU 자유 문서 사용허가(GFDL)와 창작 일반 공유귀속 2.0 사용허가 (CC-BY-SA)의 이중 사용 허가를 따릅니다.

이 저작권들의 적용 하에 이 문서의 소스 코드를 변경, 확장 그리고 개선하는 것은 자유롭습니다. 모든 파생된 작업물은 반드시 하나 또는 양쪽의 저작권 하에 발표되어야 합니다.

이 문서는 유용하게 사용될 것이라는 희망으로 배포 합니다만, 어떠한 품질 보증; 즉 매매의 암묵적인 보장 또는 거부란에 기술된 특정 목적을 위한 적합 같은 보증이 없습니다.

이 저작권들의 복사본은 이 책의 부록 편에 있습니다. 온라인 버전은 다음의 URL에서 찾을 수 있습니다:

- GNU 자유 문서 라이센스 [http://www.gnu.org/copyleft/fdl.html]
- 귀속-공유 2.0 [http://creativecommons.org/licenses/by-sa/2.0/]

경고문

이 발행물에 쓰여진 정보는 정확하고 교정하는 것을 확신할 수 있는 모든 노력을 하였습니다. 그러나, 이것은 완전하게 정확하다고 보장하지는 못합니다. Canonical Ltd., 저작자 또는 번역자는 가능한 오류와 그것으로 발생하는 결과에 대하여 책임을 지지 않습니다.

이 발행물에 인용된 몇 가지 소프트웨어와 하드웨어 설명은 등록된 상표권 일 수도 있고 그래서 저작권 제한과 상거래 보호 법률 하에 있을 수 있습니다. 저작자는 이러한 이름에 권리를 요구할 어떠한 방법이 없습니다.

이 문서화는 저작자에 의해 "있는 그대로" 제공이 되고 어떠한 표현된 또는 암묵적인 보장, 매매의 암묵적인 보장과 특정한 목적을 위한 적합 등을, 포함하는 그러나 여기에 제한되지 않는 즉 모든 보장은 거부 됩니다. 또한 발생한 직접적, 간접적, 특별한, 전형적인 또는 결과적인 손상 (을 포함하는 그러나 여기에 제한되지 않는, 대체품 또는 서비스의 구매; 사용, 자료 또는 이익의 손실; 업무의 중단) 과, 어떠한 책임의 원칙, 계약 여부, 엄격한 책임 또는 이 소프트웨어의 사용에 있어서 일어날 수 있는 (소홀함을 포함하는 또는 여타의) 불법 행위, 심지어 손상의 가능성이 충고되었다고 하더라도 이 모든 사건은 저작자의 책임이지 않습니다.

차례

표 목록

이 안내서에 대하여

1. 관례

다음의 주석은 책 전부에 사용이 됩니다:

주석은 주변의 논의에 관련된 흥미거리, 때로는 기술적 사항, 정보의 부분을 제공 합니다.

팁은 조언 또는 무엇을 하는데 좀 더 쉬운 방법을 제공 합니다.

주의는 읽는 사람에게 가능한 문제를 알리고 그것들을 피할 수 있도록 돕습니다.

경고는 읽는 사람에게 주어진 상황에서 일어날 수도 있는 위험에 대해 조언 합니다.

출력을 위한 상호 참조 관례는 다음과 같이 표시 됩니다:

- 다른 문서나 웹사이트로 바로가기는 이 것 [http://www.ubuntu.com] 처럼 보입니다.

이 문서의 PDF, HTML 그리고 XHTML 버전은 상호 참조를 처리하기 위해 하이퍼링크를 사용 합니다.

종류에 대한 관례는 다음과 같이 보여 집니다:

- 파일 이름 또는 디렉토리 경로는 monospace 로 보여 집니다.
- Terminal 명령어 프롬프트에서 입력하는 명령어는 다음과 같이 보여 집니다:

  입력하는 명령어

- 사용자 인터페이스에서 클릭 또는 선택하는 사항은 monospace 형식으로 보여 집니다.

마우스 선택, 마우스 동작 그리고 키보드 바로가기는:

- 메뉴 선택의 순서는 다음과 같이 보여 집니다: File → Open
- 마우스 동작은 오른손 조작 마우스 설정으로 가정 합니다. “click” 과 “double-click” 용어는 왼쪽 마우스 버튼을 사용하는 것으로 해석 합니다. “right-click” 용어는 오른쪽 마우스 버튼을 사용하는 것으로 해석 합니다. “middle-click” 용어는 여러분의 마우스 디자인에 따라, 가운데 마우스 버튼을 사용하는 것, 스크롤 휠을 누르는 것 또는 왼쪽과 오른쪽 버튼 모두를 동시에 누르는 것으로 해석 합니다.
- 키보드 바로가기 조합은 다음과 같이 보여 집니다: **Ctrl-N** . “Control”, “Shift,” 그리고 “Alternate” 키의 관례는 **Ctrl**, **Shift**, 그리고 **Alt** 각각이고, 이 것은 첫 번째 키가 두 번째 키를 누를 때도 눌려져 있는 상태임을 의미 합니다.

2. 공헌과 피드백

이 책은 우분투 문서화 팀 [https://wiki.ubuntu.com/DocumentationTeam] 에 의해 개발 되었습니다. 여러분은 우분투 문서화 팀 메일링 리스트에 아이디어나 견해를 보내주는 것으로 이 문서에 기여할 수 있습니다. 팀에 대한, 메일링 리스트, 프로젝트 등의 정보는 우분투 문서화 팀 웹사이트 [https://wiki.ubuntu.com/DocumentationTeam] 에서 찾을 수 있습니다.

만약 이 문서에서 문제를 보거나 또는 제안을 하고 싶다면, 우분투 버그추적 [https://launchpad.net/products/ubuntu-doc/+bugs] 에서 간단히 버그 보고를 할 수 있습니다. 여러분의 도움이 우리의 문서화 성공에 없어서는 안될 중요한 것입니다!

고맙습니다,

- 우분투 문서화 팀

1장. 소개

우분투 서버 안내서 를 읽으시는 것을 환영 합니다!

우분투 서버 안내서는 여러분의 필요에 맞게 우분투 시스템에 다향한 서버 프로그램을 어떻게 설치하고 설정하는 지에 대한 정보를 가지고 있습니다. 이것은 시스템을 설정하고 꾸미기 위한 단계별로 그리고 작업 중심적으로 작성된 안내서 입니다. 이 매뉴얼은 다음과 같이 많은 중급의 주제를 다룹니다:

- 네트워크 설정
- 아파치2 설정
- 데이타베이스
- 윈도우즈 네트워킹

이 매뉴얼은 다음의 주요 분류들로 나누어 졌습니다:

- 설치
- 패키지 관리
- 네트워킹
- 윈도우즈 네트워킹

이 안내서는 여러분이 우분투 시스템에 대한 이해를 가지고 있다고 가정 합니다. 만약 우분투 설치에 대한 자세한 도움이 필요하다면, 우분투 설치 안내서를 참조 하십시오.

우분투 문서화 웹사이트 [http://help.ubuntu.com] 에서 HTML 과 PDF 버전의 온라인 메뉴얼을 이용할 수 있습니다.

우리의 루루 가게 [http://www.lulu.com/ubuntu-doc]에서 이 안내서를 책 형태로 구입할 수 있습니다. 여러분은 인쇄와 우편의 비용만을 지불하시면 됩니다.

2장. 설치

이 장에서는 우분투 6.06 LTS 서버 에디션을 설치하는 빠른 개괄적인 설명을 제공합니다. 더 자세한 설명은, 우분투 설치 안내서를 참조 하십시오.

1. 설치 준비하기

이 영역은 설치를 시작하기 전에 고려할 만한 다양한 측면을 설명 합니다.

1.1. 시스템 요구 사항

우분투 6.06 LTS 서버 에디션은 세 가지 주요 아키텍쳐를 - Intel x86, AMD64, 그리고 PowerPC - 지원 합니다. 아래의 테이블은 권장되는 하드웨어 규격을 나열 합니다. 여러분의 필요에 따라, 이것보다는 저사양을 가지고 시스템을 사용할 수도 있습니다. 그러나, 많은 사용자는, 만약 이 제안이 무시되었을 때, 실망을 할 수도 있습니다.

표 2.1. 권장되는 최소한의 요구 사항

설치 종류	RAM	하드 드라이브
서버	64 메가바이트	500 메가바이트

우분투 6.06 LTS 서버 에디션을 위하여 기본 설정된 프로파일은 아래에 보여졌습니다. 다시 한번, 설치의 크기는 설정 중에 여러분이 설치하는 서비스에 굉장히 의존을 합니다. 많은 서버 관리자를 위하여, 기본 설정된 서비스는 일반적인 서버 사용에 적합 합니다.

서버

이것은 작은 서버 프로파일이고, 모든 종류의 서버 프로그램을 위한 공통적인 기본을 제공 합니다. 그것은 최소한이고 파일/인쇄 서비스, 웹 호스팅, 이메일 호스팅 그리고 기타의 필요한 서비스를 그 위에 가질 수 있도록 고안 되었습니다. 이러한 서비스를 위하여는 최소한 500MB 디스크 공간이 있어야 하지만, 여러분 서버로 호스트 하기를 원하는 서비스에 따라 더 많은 공간을 추가하는 것을 고려 하십시오.

이 크기는 대개의 경우 찾을 수 있는, 사용자 파일, 메일, 로그 그리고 데이터와 같은 여타의 모든 자료를 포함하지 않았다는 것을 상기 하십시오. 언제나 여러분 소유의 파일과 데이터를 위하여 공간을 고려할 때는 넉넉하게 잡는 것이 최선 입니다.

1.2. 백업 하기

□시작하기 전에, 시스템에 현재 있는 모든 파일을 백업하는 것을 확신 하십시오. 만약 이번이 컴퓨터에 설치된 운영 체계와 다른 시스템을 설치하는 첫 번째라면, 우분투를 위한 공간을 만들기 위하여 디스크를 재 파티션하는 것이 필요하는 것이 아주 일반적 입니다. 디스크를 파티션하는 어떤 때라도, 여러분이 실수를 하거나 또는 파티션 중에 시스템 파워의 손실과 같은 무엇이 잘못될 경우에 모든 것을 잃을 수 있다는 것을 반드시 대비하여야 합니다. 설치에 사용되는 프로그램은 아주 신뢰할 수 있고, 몇 년간 사용이 되었지만, 또한 잘못된 동작을 수행할 수도 있고, 사용 중에 한 가지 실수가 여러분의 귀중한 자료의 손실을 가져올 수도 있습니다.

멀티 부팅 시스템을 만든다면, 현재 운영 체제의 배포 미디어를 가지고 있으십시오. 특히 부팅 드라이브를 다시 파티션하는 경우라면, 운영 체제의

부트 로더를 다시 설치해야 할 수도 있고, 더 많은 경우에 운영 체제 전체를 해당 파티션에 다시 설치해야 합니다.

2. CD에서 설치

설치 CD를 CD-ROM 드라이브에 넣고 컴퓨터를 리부팅 합니다. 설치 시스템은 CD-ROM에서 부팅될 때 즉시 시작이 됩니다. 초기화 된 후, 첫 번째 화면이 보일 겁니다.

이 시점에서, 화면 상의 텍스트를 읽습니다. 여러분은 설치 시스템에 의해 제공되는 도움말 화면을 읽기를 원할 수도 있습니다. 이것을 하려면, F1 키를 누릅니다.

기본 설정된 서버 설치를 수행하려면, "I하드디스크로 설치"를 선택하고 **Enter** 키를 누릅니다. 설치 과정이 시작될 겁니다. 간단히 화면 상의 지시를 따르고 여러분의 우분투 시스템이 설치될 것입니다.

다른 것으로, LAMP 서버 (Linux, Apache, MySQL, PHP/Perl/Python)를 설치하려면, "LAMP 서버 설치"를 선택하고, 지시에 따릅니다.

3장. 패키지 관리

우분투는 소프트웨어의 설치, 업그레이드, 설정 그리고 제거를 위한 포괄적인 패키지 관리 시스템을 가지고 있습니다. 여러분의 우분투 시스템을 위한 17,000개가 넘는 소프트웨어 패키지의 조직화된 기반으로의 접근을 제공하는 것에 더하여, 그 패키지 관리는 또한 의존성을 해결하는 능력과 소프트웨어 업데이트 검사를 하는 편리함도 가지고 있습니다.

우분투의 패키지 관리 시스템과 상호 작용하는 여러가지, 시스템 관리자에 의해 쉽게 자동화될 수 있는 간단한 명령어-라인 유틸리티에서 부터 우분투를 새롭게 접하는 사용자들이 쉽게 사용할 수 있는 간단한 그래픽 인터페이스 까지의, 도구들이 사용하게 준비되어 있습니다.

1. 소개

우분투의 패키지 관리 시스템은 데비안 GNU/Linux 배포판에서 사용되는 같은 시스템에서 파생 되었습니다. 패키지 파일은 모든 필요한 파일, 메타 데이타, 그리고 특정 기능 또는 여러분의 우분투 컴퓨터 상의 소프트웨어 프로그램의 이행을 위한 명령 지시들을 가지고 있습니다.

데비안 패키지 파일은 전형적으로 .deb 확장자를 가지고, 일반적으로 저장소 에 존재 합니다. 저장소는 CD-ROM 디스크 또는 온라인과 같은 다양한 매체에서 찾을 수 있는 패키지의 수집들 입니다. 패키지는 보통 바이너리 형태로 미리 컴파일이 되므로 설치는 빠르게 하고 소프트웨어의 컴파일을 필요로 하지 않습니다.

많은 복잡한 패키지는 의존성 이라는 개념을 사용 합니다. 의존성은 어떤 기능이 제대로 동작하기 위하여 원래의 패키지가 필요로 하는 추가적인 패키지를 뜻 합니다. 예를 들어, speech synthesis 패키지인 Festival 은 festvox-kalpc16k 라는 패키지에 의존하고, 그것은 그 프로그램에서 사용되는 목소리 중의 하나를 공급하는 패키지 입니다. Festival 이 기능하기 위하여, 모든 의존성은 원래의 Festival 패키지와 결합하여 반드시 설치되어야 합니다. 우분투의 소프트웨어 관리 도구는 이러한 것을 자동으로 합니다.

2. Apt-Get

apt-get 명령은, 새로운 소프트웨어 패키지의 설치, 존재하는 소프트웨어 패키지의 업그레이드, 패키지 목록 인덱스의 업데이트, 그리고 심지어 전체 우분투 시스템의 업그레이드를 수행하는 우분투의 Advanced Packaging Tool (APT) 에 사용되는, 강력한 명령어-라인 도구 입니다.

단순한 명령어-라인 도구로서, apt-get 은 서버 관리자를 위하여 우분투 내에서 사용할 수 있는 다른 패키지 관리 도구들에 비해 많은 장점을 가지고 있습니다. 이러한 장점의 몇 가지는 간단한 터미널 연결(SSH)로 쉽게 사용할 수 있는 것과 cron 스케쥴링 유틸리티에 의해 자동화 할 수 있도록 시스템 관리 스크립트에서 사용될 수 있다는 것 입니다.

apt-get 유틸리티의 몇 가지 잘 알려진 사용 예는:

- **패키지 설치**: apt-get 을 사용하여 패키지를 설치하는 것은 아주 간단 합니다. 예를 들어, 네트워크 스캐너인 nmap 을 설치하려면, 다음을 입력 합니다:

```
sudo apt-get install nmap
```

- **패키지 삭제**: 패키지(들)을 삭제하는 것도 또한 직선적이고 간단한 작업 입니다. 이전 예제에서 설치하였던 nmap 패키지를 삭제하려면, 다음을 입력 합니다:

```
sudo apt-get remove nmap
```

복수 패키지: 설치나 삭제를 위해 복수의 패키지를 지정할 때는, 공백(스페이스 키로)으로 구분 합니다.

- **패키지 인덱스 업데이트**: APT 패키지 인덱스는 /etc/apt/sources.list 파일에 지정된 저장소에서 사용 가능한 패키지들의 필수적인 데이타베이스 입니다. 저장소에 최근의 변경된 것으로 로컬(여러분의 컴퓨터에 저장되는) 패키지 인덱스를 업데이트 하려면, 다음을 입력 합니다:

```
sudo apt-get update
```

- **패키지 업그레이드**: 시간에 걸쳐, 여러분의 컴퓨터에 현재 설치된 패키지의 업데이트된 버전이 패키지 저장소에 사용 가능하게 있을 수 있습니다. (예를 들어 보안 업데이트) 여러분의 시스템을 업그레이드 하려면, 위에 적힌대로 우선은 여러분의 패키지 인덱스를 업데이트 하고, 다음을 입력 합니다:

```
sudo apt-get upgrade
```

만약 패키지가 업그레이드 중에 의존되는 패키지를 설치하거나 삭제하는 것이 필요하면, 그것은 upgrade 명령에 의하여 업그레이드 되지 않습니다. 이러한 업그레이드를 위해, dist-upgrade 명령을 사용하는 것이 필요 합니다.

또한, dist-upgrade 명령으로 여러분의 우분투 시스템 전체를 하나의 버전에서 다른 버전으로 업그레이드 할 수 있습니다. 예를 들어, 우분투 5.10 버전에서 6.06 LTS 버전으로 업그레이드 하려면, 우선 여러분 컴퓨터의 /etc/apt/sources.list 파일 내의 기존의 5.10 저장소를 6.06 LTS 저장소로 대체하는 것을 확신하고, 위에 설명한 apt-get update 명령을 간단히 입력하고, 마지막으로 실제 업그레이드는 다음의 명령을 입력하는 것으로 수행할 수 있습니다:

```
sudo apt-get dist-upgrade
```

모든 패키지 업그레이드에 필요한 상당한 시간이 흐른 후, 여러분의 컴퓨터는 새 버전으로 업그레이드 될 것 입니다. 전형적으로, 몇 가지 업그레이드 후에 해야 하는 절차는 업그레이드 한 버전을 위한 업그레이드 노트에 상세히 설명됩니다.

apt-get 명령의 행위는, 즉 패키지의 설치와 삭제와 같은, /var/log/dpkg.log 로그 파일에 기록이 됩니다.

APT 사용에 대한 더 많은 정보는, 광범위한 데비안 APT 사용자 지침서 [http://www.debian.org/doc/user-manuals#apt-howto] 를 읽거나 다음을 입력하십시오:

```
apt-get help
```

3. Aptitude

Aptitude 는 메뉴 방식이고, Advanced Packaging Tool (APT) 시스템의 텍스트 기반 프론트 엔드 입니다. 설치, 삭제, 그리고 업그레이드와 같은 많은 일반적인 패키지 관리 기능을 Aptitude 에서는 단일 키 명령, 보통 소문자를 사용하여 수행할 수 있습니다.

Aptitude 는 그래픽 환경이 아닌 터미널 환경에서 명령어 키의 적절한 기능을 확신하기 위해 사용하는데 가장 잘 맞습니다. 일반 사용자로 터미널 프롬프트에서 다음의 명령을 입력하여 Aptitude 를 실행할 수 있습니다:

```
sudo aptitude
```

Aptitude를 시작하고, 여러분은 화면의 가장 위에 메뉴 막대를, 그 메뉴 막대 밑에 두 개의 부분 창을 보게 됩니다. 윗쪽의 부분 창은 새 패키지 와 설치되지 않은 패키지 와 같은 패키지 분류를 가집니다. 아래의 부분 창은 패키지와 패키지 분류에 관련된 정보를 가집니다.

패키지 관리를 위하여 Aptitude 를 사용하는 것은 비교적 직관적이고, 사용자 인터페이스는 단순하게 수행할 수 있도록 자주쓰는 작업을 모았습니다. 다음의 예는 Aptitude 에서 수행되는 잘 알려진 패키지 관리 기능들 입니다:

- **패키지 설치**: 패키지를 설치하려면, 설치되지 않은 패키지 분류를 통하여 패키지에 위치하고, 예를 들어, 키보드의 화살표 키와 **ENTER** 키를 사용하여, 설치하고자 하는 패키지를 선택(하이라이팅으로 강조됨) 합니다. 설치하고자 하는 패키지의 선택 후, **+** 키를 누르면, 그 패키지 항목은 녹색 으로 색상이 바뀌고, 이것은 설치를 위하여 표시되었음을 알려 줍니다. 이제 패키지 동작의 요약을 보이기 위해 **g** 키를 누릅니다. 다시 한번 **g** 키를 누르면, 설치를 끝내기 위해 root가 되기위한 프롬프트를 보게 됩니다. **ENTER** 키를 누르면 암호 프롬프트를 보게되고, 여러분의 사용자 암호를 입력하여 root(시스템 관리를 하는 사용자)가 됩니다. 마지막으로, **g** 키를 한 번 더 누르고 패키지의 다운로드를 알리는 프롬프트를 보게 됩니다. 계속 프롬프트에서 **ENTER** 키를 누르면, 패키지의 내려받기와 설치가 시작 됩니다.
- **패키지 삭제**: 패키지를 삭제하려면, 설치된 패키지 분류를 통하여 패키지에 위치하고, 예를 들어, 키보드의 화살표 키와 **ENTER** 키를 사용하여, 삭제하고자 하는 패키지를 선택 합니다. 삭제하고자 하는 패키지의 선택 후, **-** 키를 누르면, 그 패키지 항목은 분홍색 으로 색상이 바뀌고, 이것은 삭제를 위하여 표시되었음을 알려 줍니다. 이제 패키지 동작의 요약을 보이기 위해 **g** 키를 누릅니다. 다시 한번 **g** 키를 누르면, 삭제를 끝내기 위해 root가 되기위한 프롬프트를 보게 됩니다. **ENTER** 키를 누르면 암호 프롬프트를 보게되고, 여러분의 사용자 암호를 입력하여 root가 됩니다. 마지막으로, **g** 키를 한 번 더 누르고 패키지의 삭제를 알리는 프롬프트를 보게 됩니다. 계속 프롬프트에서 **ENTER** 키를 누르면, 패키지의 삭제가 시작 됩니다.

- **패키지 인덱스 업데이트**: 패키지 인덱스를 업데이트 하려면, 간단히 **u** 키를 누르고, 업데이트를 끝내기 위해 root가 되기위한 프롬프트를 보게 됩니다. **ENTER** 키를 누르면 암호 프롬프트를 보게되고, 여러분의 사용자 암호를 입력하여 root가 됩니다. 패키지 인덱스를 업데이트하는 것이 시작 됩니다. 프로세스를 끝내기 위해 내려받기 대화창이 보여질 때 확인 프롬프트에서 **ENTER** 키를 누릅니다.
- **패키지 업그레이드**: 패키지를 업그레이드 하려면, 위에 설명한 패키지 인덱스의 업데이트를 먼저 수행을 하고, 모든 업그레이드 가능한 패키지를 표시하기 위하여 **U** 키를 누릅니다. 이제 패키지 동작의 요약을 보이기 위해 **g** 키를 누릅니다. 다시 한번 **g** 키를 누르면, 설치를 끝내기 위해 root가 되기위한 프롬프트를 보게 됩니다. 여러분의 사용자 암호를 넣고 root가 됩니다. 마지막으로, 패키지의 내려받기를 위하여 **g** 키를 한 번 더 누릅니다. 계속 프롬프트에서 **ENTER** 키를 누르면, 패키지의 업그레이드가 시작 됩니다.

위쪽 부분 창의 패키지 목록에 보여진 정보의 첫 항목(행)은, 패키지의 현재 상태를 패키지 목록에 실제 보이는 것이고, 패키지 상태를 기술하는 것은 다음의 키를 사용합니다:

- **i**: 설치된 패키지.
- **c**: 설치되지 않은 패키지이지만, 설정이 시스템에 남아있는 패키지
- **p**: 시스템에서 깨끗히 삭제된 패키지
- **v**: 가상 패키지
- **B**: 잘못된 패키지
- **u**: 풀려진 파일, 그러나 아직 설정이 안된 패키지
- **C**: 반쯤 설정됨- 설정이 실패하였고 고치는 것이 필요함
- **H**: 반쯤 설치됨- 삭제가 실패하였고 고치는 것이 필요함

Aptitude를 종료하려면, 간단히 **q** 키를 누르고 종료한다는 것을 확인 합니다. 많은 다른 기능들은 Aptitude 메뉴에서 **F10** 키를 눌러 보실 수 있습니다.

4. 설정

Advanced Packaging Tool (APT) 시스템 저장소에 대한 설정은 /etc/apt/sources.list 설정 파일에 저장 됩니다. 여기에 참조하는 것은 그 파일의 한 예이고, 그 파일에서 저장소를 추가 또는 삭제하는 것에 대한 정보를 보여 줍니다.

Here [../sample/sources.list] 는 전형적인 /etc/apt/sources.list 파일의 간단한 예입니다.

여러분은 저장소를 활성화 또는 비활성화 하기 위하여 그 파일을 편집할 수 있습니다. 예를 들어, 패키지에 대한 동작이 일어날 때마다 우분투 CD-ROM의 삽입이 필요한 것을 비활성화 시키려면, 그 파일의 맨 위에 보여지는, CD-ROM를 위해 사용되는 그 줄을 간단히 주석처리 합니다:

```
# no more prompting for CD-ROM please
# deb cdrom:[Ubuntu 6.06 _Dapper Drake_ - Release i386 (20060329.1)]/ dapper main restricted
```

5. 추가 저장소

우분투를 위하여 공식적으로 지원되는 패키지 저장소에 더하여, 설치를 위한 수천 개가 넘는 가능한 패키지를 추가하는 커뮤니티가 관리하는 추가적인 저장소가 있습니다. 가장 알려진 두 가지 추가적인 저장소는, Universe 와 Multiverse 저장소 입니다. 이 저장소들은 우분투에 의하여 공식적으로 지원이 되는 것은 아니고 그러므로 기본 설정으로 활성화되어 있지 않지만, 그것들은 일반적으로 여러분의 우분투 컴퓨터에서 안전하게 사용할 수 있는 패키지를 제공 합니다.

Multiverse 저장소 내의 패키지들은 종종 자유 운영 체계와 함께 배포하는 것을 막는 사용허가의 문제를 가지고 있고, 여러분의 지역에 따라 불법일 수도 있습니다.

Universe 또는 Multiverse 저장소는 공식적으로 지원되는 패키지를 가지고 있지 않음을 충고 합니다. 특정 예로, 그 패키지들을 위한 보안 업데이트가 없을 수도 있습니다.

많은 다른 패키지 소스도 사용 가능하고, 때로는 하나의 프로그램 개발자에 의해 제공되는 패키지 소스의 경우, 오직 하나의 패키지만을 심지어 제공하는 경우도 있습니다. 하지만, 표준화되지 않은 패키지 소스를 사용할 때는, 여러분은 매우 조심하고 주의를 기울여야 합니다. 몇 개의 패키지 소스와 그들의 패키지는 어떤 측면에서는 여러분의 시스템을 불안정하게 하거나 또는 동작하지 않도록 할 수 있으므로, 설치를 수행하기 전에 소스와 패키지를 조심스럽게 조사해 보십시오.

Universe 와 Multiverse 저장소를 사용 가능하게 하려면, /etc/apt/sources.list 파일을 편집하기 위하여 열고 해당 줄의 주석을 해제 합니다:

```
# We want Multiverse and Universe repositories, please

deb http://archive.ubuntu.com/ubuntu dapper universe multiverse
deb-src http://archive.ubuntu.com/ubuntu dapper universe multiverse
```

5.1. 참조

저장소 추가 하우투 (우분투 위키)
[https://wiki.ubuntu.com/AddingRepositoriesHowto]

4장. 네트워킹

네트워크는 연결된 장치 간에 정보를 공유하고 배포할 목적으로 실제 케이블 또는 무선 링크로 연결된 컴퓨터 시스템, 프린터, 그리고 관련되는 장비와 같은 두 개 이상의 장치로 구성 됩니다.

우분투 서버 안내서의 이 영역은 네트워크 개념의 개괄적인 설명과 잘 알려진 네트워크 프로토콜과 서버 프로그램의 자세한 논의를 포함하는, 네트워킹에 속하는 일반적이고 특정한 정보를 제공 합니다.

1. 네트워크 설정

우분투는 여러분의 네트워크 장치를 설정할 수 있는 몇 가지 그래픽 유틸리티를 제공 합니다. 이 문서는 서버 관리자를 위하여 작성되었고 명령어 라인에서 여러분의 네트워크를 관리하는 것에 중점 합니다.

1.1. 이더넷

대부분 이더넷 설정은 /etc/network/interfaces 파일 하나에 중앙화 되었습니다. 만약 여러분이 이더넷 장치를 가지고 있지 않다면, 이 파일에는 오직 loopback 인터페이스만 보일 것이고, 그것은 다음과 비슷하게 보일 겁니다:

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback
address 127.0.0.1
netmask 255.0.0.0
```

만약 여러분이 오직 하나의 이더넷 장치, eth0를 가지고 있고, 그것이 DHCP 서버에서 설정을 가지고 부트 시에 자동으로 올라와야 한다면, 다음의 두 줄이 더해지는 것이 필요 합니다:

```
auto eth0
iface eth0 inet dhcp
```

첫 번째 줄은 eth0 장치가 여러분이 부팅을 할 때 자동적으로 올라와야 한다는 것을 지정 합니다. 두 번째 줄은, 인터페이스 (“iface”) eth0는 IPv4 주소 체계를 (IPv6 장치를 위해서는 “inet” 를 “inet6” 로 대체함) 가지고 DHCP에서 자동적으로 그 장치의 설정을 가져야 한다는 것을, 의미 합니다. 여러분의 네트워크와 DHCP 서버가 올바르게 설정되었음을 가정하고, 이 기계의 네트워크는 올바르게 동작하기 위해 더 이상의 설정을 필요로 하지 않습니다. DHCP 서버는 기본 설정 게이트웨이(route 명령을 통하여 이행되는), 장치의 IP 주소(ifconfig 명령을 통하여 이행되는), 그리고 네트워크 상에서 사용되는 DNS 서버를(/etc/resolv.conf 파일에 이행되는) 제공 합니다.

여러분의 이더넷 장치를 고정 IP 주소와 여러분에 맞는 설정값으로 설정을 하려면, 몇 가지 정보가 더 필요 합니다. eth1 장치에 192.168.0.2 IP 주소를, 일반적인 255.255.255.0 netmask와 함께 지정하기를 원한다고 생각해 봅니다. 여러분의 기본 설정 게이트웨이의 IP 주소는 192.168.0.1 입니다. /etc/network/interfaces 파일에 다음과 같이 입력을 합니다:

```
iface eth1 inet static
 address 192.168.0.2
 netmask 255.255.255.0
 gateway 192.168.0.1
```

이 경우에는, /etc/resolv.conf 파일에 여러분의 DNS 서버를 수동으로 지정하는 것이 필요하고, 이것과 비슷할 겁니다:

```
search mydomain.com
nameserver 192.168.0.1
nameserver 4.2.2.2
```

search 지시자는 여러분의 네트워크 상의 이름을 해결하기 위한 시도를 할 때 mydomain.com을 호스트 이름 질의에 추가하게 됩니다. 예를 들어, 만약 여러분의 네트워크 도메인이 mydomain.com 이고, 여러분이 호스트 “mybox” 에 ping을 시도하면, 그 DNS 질의는 이름의 파악을 위하여 “mybox.mydomain.com” 으로 변경 됩니다. nameserver 지시자는 호스트 이름을 IP 주소로 해결하기 위하여 사용되는 DNS 서버를 지정 합니다. 만약 여러분 소유의 네임서버를 사용하면, 그것을 여기에 입력 하십시오. 그렇지 않다면, 여러분의 인터넷 서비스 제공자에게 사용할 우선(primary) 그리고 이차(secondary) DNS 서버를 문의하고, 그것들을 위에 보인 것과 같이 /etc/resolv.conf 파일에 입력 합니다.

다이얼업 PPP 인터페이스, IPv6 네트워킹, VPN 장치, 기타 등등을 포함하는 많은 다른 설정들이 가능합니다. 더 많은 정보와 지원되는 선택 사항들은 man 5 interfaces 를 참조 하십시오. 기억해야 할 것은, /etc/network/interfaces 파일은 ifup/ifdown 스크립트에 의하여 사용되고, 그것들은 다른 리눅스 배포판에서 사용되는 것보다 높은 수준의(역주:사용의 편의를 기했다는 의미) 설정 체계 입니다. ifconfig, route, 그리고 dhclient 와 같은 전통적이고, 낮은 수준의(역주:명령어 라인에 직접 입력해야 한다는 의미) 유틸리티는 여전히 ad hoc 설정을 위하여 사용 가능 합니다.

1.2. DNS 항목 관리

이 영역은 IP 주소를 호스트 이름으로 파악을 하고 또 그 반대로 알아내는데 사용하는 네임서버를 어떻게 설정하는지에 대한 설명을 합니다. 이것은 시스템을 하나의 네임서버로 어떻게 구축하는지를 설명하지는 않습니다.

DNS 항목을 관리하려면, 여러분은 /etc/resolv.conf 파일에서 DNS 이름을 추가, 편집 또는 삭제할 수 있습니다. 예제 파일 [../sample/resolv.conf]이 아래와 같이 주어집니다:

```
search com
nameserver 204.11.126.13
nameserver 64.125.134.133
nameserver 64.125.134.132
nameserver 208.185.179.218
```

search 키는 불완전한 호스트 이름에 더하여지는 문자를 지정 합니다. 여기에, 우리는 그것을 com 으로 언급하였습니다. 그러므로, 우리가 다음과 수행할 때: **ping ubuntu** 은 **ping ubuntu.com** 으로 해석되어 집니다.

nameserver 키는 네임서버 IP 주소를 지정 합니다. 그것은 주어진 IP 주소 또는 호스트 이름을 해결하기 위하여 사용 됩니다. 이 파일은 복수 개의 nameserver 항목을 가질 수 있습니다. 네임서버들은 적힌 것과 같은 순서로 네트워크 질의에 사용 됩니다.

만약 DNS 서버 이름이 동적으로 DHCP 또는 PPPOE (여러분의 ISP에서) 읽혀졌다면, 이 파일에 nameserver 항목을 추가하지 마십시오. 그것은 자동적으로 업데이트 됩니다.

1.3. 호스트 관리

호스트를 관리하기 위하여, 여러분은 /etc/hosts 파일에서 호스트를 추가, 편집 또는 삭제할 수 있습니다. 그 파일은 IP 주소와 그에 대응하는 호스트 이름을 가집니다. 여러분의 시스템이 호스트 이름으로 IP 주소를 해결하거나 IP 주소로 호스트 이름을 결정할 때, 그것은 네임서버를 사용하기 전에 /etc/hosts 파일을 참조 합니다. 만약 그 IP 주소가 /etc/hosts 파일 내에 열거되었다면, 네임서버는 사용되지 않습니다. 이 동작은 여러분이 위험을 감수하는 것을 전제로 /etc/nsswitch.conf 파일을 편집하는 것으로 변경될 수 있습니다.

만약 여러분의 네트워크이 DNS에 나열되지 않은 IP 주소를 가지는 컴퓨터들을 가지고 있다면, 그것들을 /etc/hosts 파일에 추가하는 것을 권장 합니다.

2. TCP/IP

Transmission Control Protocol and Internet Protocol (TCP/IP) 는 1970년대 후반에 Defense Advanced Research Projects Agency (DARPA) 에 의하여 개발된 프로토콜의 표준화된 규격이고 다른 종류의 컴퓨터와 컴퓨터 네트워크 간에 통신을 하기 위한 수단 입니다. TCP/IP 는 인터넷을 주도하는 힘이고, 그러므로 그것은 지구상의 네트워크 프로토콜 중에 가장 인기있는 규약 입니다.

2.1. TCP/IP 소개

TCP/IP의 두 가지 프로토콜 요소는 컴퓨터 네트워킹의 다른 측면을 다룹니다. Internet Protocol, TCP/IP의 "IP"는 네트워크 정보의 기본 단위로서 IP datagram 을 사용하는 네트워크 패킷 라우팅만을 다루는 접속이 없는 프로토콜 입니다. TCP/IP의 "TCP" 는 Transmission Control Protocol 이고, 네트워크 호스트들이 데이터 스트림을 교환하기 위하여 사용될 수 있는 접속을 이루기 위해 활성화 합니다. TCP는 또한 접속들 간에 자료가 한 네트워크 호스트에서 주고 받는 것과 마찬가지로 다른 네트워크 호스트에서 보내지는 것도 보장 합니다.

2.2. TCP/IP 설정

TCP/IP 프로토콜 설정은, 해당 설정 파일들을 편집하거나, 적당한 TCP/IP 설정 값을 네트워크 클라이언트에게 자동적으로 제공하기 위하여 사용하는 Dynamic Host Configuration Protocol (DHCP) 서버와 같은 솔루션을 적용하는 것에 의해, 반드시 지정되는 여러가지 요소로 구성 합니다. 이 설정 값들은 여러분의 우분투 시스템의 적절한 네트워크 동작의 편의를 위하여 반드시 정확하게 지정되어야 합니다.

TCP/IP의 공통적인 설정 요소와 그들의 목적은 다음과 같습니다:

- **IP address** IP 주소는, 점으로 구분되는 네 개의 0부터 255까지의 십진수 범위의 숫자들이고, 각각의 네 숫자는 전체 주소를 위한 총 32 bits의 8 bits 주소를 표현하는, 유일한 식별자 입니다. 이러한 형식은 dotted quad notation 라 불립니다.
- **Netmask** 서브넷 마스크는 (또는 간략하게, netmask) 네트워크 상의 비트 마스크, 또는 네트워크에 중요한 IP 주소에서 subnetwork 에 중요한 비트를 구분하는 부분인 플랙의 집합 입니다. 예를 들어, 클래스 C 네트워크에서, 표준 netmask는 255.255.255.0 이고, IP 주소의 첫 3 바이트는 차폐하고 IP 주소의 마지막 바이트는 서브 네트워크 상의 호스트를 지정하기 위해 사용하도록 남겨지는 것을 허용 합니다.
- **Network Address** 네트워크 주소는 IP 주소의 네크워크 부분을 구성하는 바이트를 표현 합니다. 예를 들어, 클래스 A 네트워크 내의 12.128.1.2 호스트는 네트워크 주소로 12.0.0.0을 사용하고, 그 IP 주소의 첫 번째 바이트인 12가 그것을 표현 합니다 (네트워크 부분). 0으로 표시되는 남겨진 세 바이트는 가능한 호스트 값을 표시하기 위해서 입니다. 아주 일반적인 사적 그리고 라우팅을 할 수 없는 192.168.1.100과 같은 IP 주소를 사용하는 네트워크 호스트는 192.168.1.0의

네트워크 주소를 사용하는 것이고, 클래스 C 인 192.168.1 네트워크와 그 네트워크 상에서 가능한 모든 호스트를 위한 마지막 자리의 0을 지정하는 것 입니다.

- **브로드캐스트 주소** 브로드캐스트 주소는 특정 네트워크 호스트를 지정하는 대신에 주어진 서브네트워크 상의 모든 호스트들에게 일제히 네트워크 데이터가 보내지는 것을 허용하는 IP 주소 입니다. IP 네트워크를 위한 표준화된 일반적 브로드캐스트 주소는 255.255.255.255 이지만, 이 브로드캐스트 주소는 라우터에 의하여 막히기 때문에 인터넷 상의 모든 호스트로 브로드캐스트 메세지를 보내는데 사용할 수는 없습니다. 좀 더 적당한 브로드캐스트 주소는 특정 서브네트워크에 일치하도록 지정을 합니다. 예를 들어, 잘 알려진 사설 C 클래스 IP 네트워크, 192.168.1.0 상의 브로드캐스트 주소는 192.168.1.255로 설정되어야 합니다. 브로드캐스트 메세지는 Address Resolution Protocol (ARP) 와 Routing Information Protocol (RIP) 같은 네트워크 프로토콜에 의하여 일반적으로 생산이 됩니다.
- **게이트웨이 주소** 게이트웨이 주소는 특정 네트워크 또는 네트워크 상의 호스트로 접근하기 위하여 통해야 하는 IP 주소 입니다. 만약 한 네트워크 호스트가 같은 네트워크 상에 위치하지 않은 다른 네트워크 호스트와 통신을 하기를 원한다면, 하나의 게이트웨이를 반드시 사용하여야 합니다. 많은 경우에, 게이트웨이 주소는 같은 네트워크 상의 라우터의 주소가 되고, 인터넷 호스트와 같은 다른 네트워크 또는 호스트로 트래픽을 넘기는데도 사용이 됩니다. 게이트웨이 주소 설정 값은 반드시 정확하여야 하고, 그렇지 않다면 여러분의 시스템은 같은 네트워크 밖에 있는 어떠한 호스트로도 접근을 하는 것이 불가능 합니다.
- **네임서버 주소** 네임서버 주소는 도메인 네임 서비스(DNS)의 IP 주소를 나타내고, 네트워크 호스트 이름을 IP 주소로 알아내는 역할을 합니다. 네임서버 주소의 세 가지 수준이 있고, 그것을 중요도의 순서로 지정하면: 우선(일차) 네임서버, 이차 네임서버, 그리고 삼차 네임서버 입니다. 여러분의 시스템이 네트워크 호스트 이름으로 그들에 대응하는 IP 주소를 알아내기 위해서는, 여러분은 시스템의 TCP/IP 설정에 여러분이 사용할 수 있게 허가된 올바른 네임서버 주소를 반드시 지정을 해야 합니다. 많은 경우에 이 네임서버 주소는 여러분의 네트워크 서비스 제공자에 의해서 제공될 수 있고 제공되어 지지만, 많은 무료 그리고 공개적으로 접근이 가능한 4.2.2.1 에서 4.2.2.6 까지의 IP 주소를 가지는 Level3 (Verizon) 서버와 같은 네임서버들이 사용가능 합니다.

IP 주소, 넷마스크, 네트워크 주소, 브로드캐스트 주소, 그리고 게이트웨이 주소는 전형적으로 /etc/network/interfaces 파일 내에 해당 지시자를 사용하여 지정 됩니다. 네임서버 주소는 /etc/resolv.conf 파일 내에 nameserver 지시자를 통해 일반적으로 지정 됩니다. 더 많은 정보는, 터미널 프롬프트에서 다음의 명령을 사용하여, interfaces 또는 resolv.conf 를 위한 시스템 지침서를 읽어 보십시오:

interfaces 를 위한 시스템 매뉴얼 페이지는 다음의 명령으로 접근 합니다:

```
man interfaces
```

resolv.conf 를 위한 시스템 매뉴얼 페이지는 다음의 명령으로 접근 합니다:

```
man resolv.conf
```

2.3. IP 라우팅

IP 라우팅은 네트워크 데이터가 보내지는 TCP/IP 네트워크 상에서 경로를 지정하고 찾기 위한 수단 입니다. 라우팅은 보내는 곳에서 받는 곳으로 네트워크 데이터 패킷을 전달하기 위한 지시를 위하여 routing tables 의 집합을 사용하고, 종종 routers 라고 알려진 네트워크 상의 많은 중간 지점을 경유 합니다. IP 라우팅의 두 가지 주요 형태가 있습니다: Static Routing(정적 라우팅) 과 Dynamic Routing(동적 라우팅)

정적 라우팅은 시스템의 라우팅 테이블에 손수 IP 라우트를 추가하는 것을 필요로 하고, 이것은 route 명령으로 라우팅 테이블을 조작하는 것으로 대개 마쳐지게 됩니다. 정적 라우팅은 동적 라우팅에 비해 많은 장점을 가집니다. 규모가 작은 네트워크 상의 단순한 적용, 예측 가능함(라우팅 테이블은 언제나 미리 계산이 되고, 그래서 경로는 그것이 사용되는 같은 각각의 시간을 예측할 수 있음), 그리고 동적 라우팅 프로토콜을 사용하지 않음에 기인하는 다른 라우터와 네트워크 링크에 낮은 오버헤드 등이 장점이 됩니다. 하지만, 정적 라우팅은 역시 단점도 가지고 있습니다. 예를 들어, 정적 라우팅은 규모가 작은 네트워크에 제한적이고 확장이 용이하지 않습니다. 또한, 경로를 고정한 특성 때문에, 정적 라우팅이 완전히 실패하면 네트워크 중단과 실패로 이어지게 됩니다.

동적 라우팅은 보낸 곳에서 받는 곳까지 복수의 가능한 IP 라우트를 가지는 규모카 큰 네트웨크에 의존하고, 동적 라우팅이 가능하도록 라우팅 테이블의 자동 조정을 처리하는 Router Information Protocol (RIP) 과 같은 특별한 라우팅 프로토콜을 사용 합니다. 동적 라우팅은 정적 라우팅에 비해 여러가지 장점을 가집니다. 훌륭한 확장성, 네트워크 라우터의 실패와 중단에 적응하는 능력 등이 장점 입니다. 추가하여, 라우터가 다른 라우터의 존재와 가능한 경로를 스스로 배우기 때문에, 라우팅 테이블의 수작업 설정을 줄여 줍니다. 이 특성은 또한 작업자의 오류로 인한 라우팅 테이블의 실수가 일어나는 가능성을 제거 합니다. 하지만, 동적 라우팅은 완벽하지 않고, 계층적으로 복잡함과 라우터 통신의 추가적인 네트워크 오버헤드(최종 사용자에게는 직접적으로 이득을 주지않고 네트워크의 밴드위드를 소모하는)와 같은 단점을 가집니다.

2.4. TCP와 UDP

TCP는 접속 기반 프로토콜이고, 에러 교정과 flow control (흐름 제어)로 알려진 데이터의 배달을 보장하는 것을 제공 합니다. 흐름 제어는 데이터 스트림의 흐름이 중단되는 것이 필요한 때와, 예를 들어, 데이타의 완전하고 정확한 배달을 확신하기 위하여, collisions 과 같은 문제들로 인하여 재전송을 해야하는 이전의 보내진 패킷을 결정합니다. TPC는 전형적으로 데이타베이스 트랜잭션과 같은 중요한 정보를 교환하는 데에 사용되어 집니다.

한편, User Datagram Protocol (UDP)는, connectionless

2.5. ICMP

Internet Control Messaging Protocol (ICMP)는 Request For Comments (RFC) #792에 정의된 바와 같이 Internet Protocol (IP)의 확장이고, 제어, 에러 그리고 정보 메세지를 포함하는 네트워크 패킷을 지원 합니다. ICMP는 ping 유틸리티와 같은 네트워크 프로그램에서 사용되고, 네트워크 호스트 또는 장치의 사용 가능함을 결정할 수 있습니다. ICMP에 의해 되돌려지는 몇 가지 에러 메세지의 예는 네트워크 호스트와 라우터와 같은 장치 모두에게 유용하고, Destination Unreachable 과 Time Exceeded 를 포함 합니다.

2.6. 데몬

데몬은 전형적으로 백그라운드에서 계속적으로 실행되는 그리고 다른 프로그램에서 데몬이 제공하는 기능을 위한 요청을 기다리는 특별한 시스템 응용 프로그램 입니다. 많은 데몬들은 네트워크 중심이고, 우분투 시스템 상의 백그라운드에서 수행되는 많은 수의 데몬들은 네트워크와 관련된 기능을 제공 합니다. 이러한 네트워크 데몬의 몇 가지 예는 웹 서버 기능을 제공하는 Hyper Text Transport Protocol Daemon (httpd), 보안 원격 로그인 쉘과 파일 전송 능력을 제공하는 Secure SHell Daemon (sshd), 그리고 이메일 서비스를 제공하는 Internet Message Access Protocol Daemon (imapd) 등을 포함 합니다.

3. 방화벽 설정

리눅스 커널은 Netfilter 서브 시스템을 포함하고, 이것은 여러분 서버로 오는 또는 경유하는 네트워크 트래픽을 조작하거나 운명을 결정하는데 사용 됩니다. 모든 현대적인 리눅스 방화벽 솔루션은 패킷을 걸러내기 위하여 이 시스템을 사용 합니다.

3.1. 방화벽 소개

커널의 패킷 필터링 시스템은 그것을 관리하기 위한 사용자 공간의 인터페이스가 없이 시스템 관리자가 약간의 작업을 하는 것이 필요 합니다. 이것은 iptables의 목적 입니다. 패킷이 여러분의 서버에 도착할 때, 패킷은 iptables를 통하여 사용자 공간에서 패킷에 제공되는 규칙에 근거하여 패킷의 수용, 조작 또는 거절을 위한 Netfilter 서브 시스템을 거치게 됩니다. 그러므로, iptables는, 만약 여러분이 그것에 익숙하다면, 여러분의 방화벽을 관리하기 위하여 필요한 전부이고, 작업을 단순화하기 위한 많은 프론트엔드들이 있습니다.

3.2. IP 마스커레이딩

IP 마스커레이딩(Masquerading:가장)의 목적은 여러분의 네트워크 상의 사설, 라우팅이 안되는 IP 주소를 가진 기계들이 IP의 가장을 통하여 인터넷을 접근하는 것을 허용하기 위해서 입니다. 여러분의 사설 네트워크에서 인터넷을 목적지로 하는 트래픽은 반드시, 그 요청을 만든 기계로 경로가 되돌아갈 수 있는 응답들을 위하여, 조작되어져야 합니다. 이것을 하기 위하여, 커널은 반드시 각각의 패킷의 source IP 어드레스를 변경하고, 그러므로 응답은 인터넷에서 사용 가능하지 않은 요청을 만든 사설 IP 주소 대신에 변경된 것에 따라 다시 되돌아오게 됩니다. 리눅스는 기계가 속하는 접속과 되돌와오는 패킷을 적절하게 재경로하는 것을 추적하기 위하여 접속 추적 (conntrack)을 사용 합니다. 그러므로 여러분의 사설 네트워크를 떠난 트래픽은 여러분의 우분투 게이트웨이 기계로 향할 때 "가장"이 됩니다. 이 절차는 인터넷 접속 공유로 마이크로소프트의 문서에서는 알려져 있습니다.

이것은 하나의 iptables 규칙을 가지고 완수할 수 있고, 여러분의 네트워크 설정에 따라 약간 다를 수 있습니다:

```
sudo iptables -t nat -A POSTROUTING -s 192.168.0.0/16 -o ppp0 -j MASQUERADE
```

위의 명령은 여러분의 사설 주소 공간이 192.168.0.0/16 이고 인터넷을 사용하는 장치가 ppp0 라고 가정을 합니다. 문법은 다음과 같이 나누어질 수 있습니다:

- -t nat -- nat 테이블로 가기 위한 규칙
- -A POSTROUTING -- POSTROUTING chain에 덧붙이는(-A) 규칙
- -s 192.168.0.0/16 -- 지정된 주소 공간에서 향하는 트래픽에 적용하는 규칙
- -o ppp0 -- 지정된 네트워크 장치를 통하여 경유하도록 스케쥴된 트래픽에 적용하는 규칙
- -j MASQUERADE -- 위에 설명된 대로 이 규칙에 일치하는 트래픽은 조작되기 위한 MASQUERADE 타켓으로 "jump" (-j)

필터 테이블 (대부분 또는 모든 패킷 필터링이 일어나는 기본 설정 테이블) 내의 각 체인은 ACCEPT 정책 을 기본값으로 갖지만, 만약 여러분이 게이트웨이 장치에 추가로 방화벽을 설정한다면, DROP 또는 REJECT 정책을 지정할 수 있고, 그 경우에는 여러분의 가장된 트래픽은 위의 규칙이 동작을 하기 위하여 FORWARD 체인을 통하는 것이 허용되어야 합니다:

```
sudo iptables -A FORWARD -s 192.168.0.0/16 -o ppp0 -j ACCEPT
sudo iptables -A FORWARD -d 192.168.0.0/16 -m state –state ESTABLISHED,RELATED -i ppp0 -j ACCEPT
```

위의 명령은 여러분의 로컬 네트워크에서 인터넷으로 가는 모든 접속과 그 접속에 관련되는 모든 트래픽이 위의 규칙을 시작한 (즉 여러분의) 기계로 되돌아오는 것을 허용 합니다.

3.3. 도구

두려운 iptables의 지식이 없이도 완전하게 방화벽을 구축할 수 있도록 도와주는 여러가지 도구들이 있습니다. GUI로 편하게 사용할 수 있는 것은, Firestarter 가 아주 유명하고 사용하기도 쉽고, fwbuilder 는 매우 강력하고 Checkpoint FireWall-1과 같은 상업용 방화벽을 사용해 본 시스템 관리자에게 익숙하게 보일 겁니다. 평범한 텍스트 설정 파일을 가지는 명령어 라인 도구를 선호한다면, Shorewall 은 어떠한 네트워크를 위해서도 우수한 방화벽을 설정할 수 있도록 도와주는 매우 강력한 솔루션 입니다. 만약 여러분의 네트워크가 비교적 간단하거나, 또는 네트워크를 가지고 있지 않다면, ipkungfu 를 사용하면 따로 설정하는 것 없이 설치시 바로 동작하는 방화벽을 제공할 것이고, 좀더 발전된 방화벽을 설정하는 것은 간단하고 문서화가 잘 된 설정 파일을 편집하는 것으로 쉽게 만들 수 있습니다. 또다른 흥미로운 도구는 fireflier 이고, 데스크탑 방화벽 프로그램으로 고안된 것 입니다. 이것은 서버 (fireflier-server) 와 여러분이 선택하는 GUI 클라이언트 (GTK 또는 QT) 로 구성되고, 윈도우즈를 위한 많은 유명한 상호작용 방화벽과 같이 동작을 합니다.

3.4. 로그

방화벽 로그는 공격, 방화벽 규칙의 문제 파악, 그리고 여러분 네트워크 상의 비정상적인 행동을 알아낼 수 있는 필수적인 것 입니다. 여러분은 반드시 방화벽 설정에 로그가 만들어지도록 로그 규칙을 포함시키고, 로그 규칙은 어떠한 적용된 끝내기 규칙 (타겟을 가지고 ACCEPT, DROP, 또는 REJECT와 같이 패킷의 운명을 결정하는 규칙) 전에 반드시 오도록 해야 합니다. 예를 들어:

```
sudo iptables -A INPUT -m state –state NEW -p tcp –dport 80 -j LOG –log-prefix "NEW_HTTP_CONN: "
```

로컬 기계에서 포트 80 번의 요청은 dmesg 내의 로그로 만들어지고 다음과 같이 보일 겁니다:

```
[4304885.870000] NEW_HTTP_CONN: IN=lo OUT= MAC=00:00:00:00:00:00:00:00:00:00:00:00:08:00 SRC=127.0.0.1 D
```

위의 로그는 또한 /var/log/messages, /var/log/syslog, 그리고 /var/log/kern.log 파일에도 나타납니다. 이 동작은 /etc/syslog.conf 파일을 적당하게 편집하거나, ulogd 를

설치/설정하고 LOG 대신에 ULOG 타켓을 사용하는 것으로 변경될 수 있습니다. ulogd 데몬은 사용자 공간의 서버이고 특별히 방화벽을 위한 커널에서 오는 로깅 지시를 듣고, 여러분이 원하는 어떠한 파일, 또는 심지어 PostgreSQL 과 MySQL 데이타베이스로 기록을 할 수 있습니다. 방화벽 로그를 알아보기 쉽게 꾸미는 것은 fwanalog, fwlogwatch, 또는 lire 같은 로그 분석 도구를 사용하는 것으로 간단해 질 수 있습니다.

4. OpenSSH 서버

4.1. 소개

우분투 서버 안내서의 이 영역은 네트워킹된 컴퓨터의 원격 조정하고 자료를 전송할 수 있는 강력한 도구의 모음인, OpenSSH 를 소개 합니다. OpenSSH 서버 프로그램에서 가능한 몇 가지 설정 값에 대한 것과 여러분의 우분투 시스템에서 어떻게 그것을 변경하는 지를 알게 됩니다.

OpenSSH는 원격으로 컴퓨터를 조종하거나 컴퓨터 간의 파일을 전송하기 위한 Secure Shell (SSH) 프토토콜 도구들의 자유롭게 사용할 수 있는 버전 입니다. 이러한 기능을 가지는 전통적인 도구들로는, telnet 이나 rcp 가 있지만, 보안이 적용되지 않고 사용될 때 사용자의 암호를 들여다 볼수 있는 텍스트로 전송 합니다. OpenSSH는, 이러한 전통적인 도구들을 효과적으로 대체하는, 서버 데몬과 보안, 암호화된 원격 조종과 파일 전송 동작 기능을 가지는 클라이언트 도구들을 제공 합니다.

OpenSSH 서버 구성 요소는, sshd 이고, 어떠한 클라이언트 도구이던 클라이언트 접속을 위하여 끊임없이 듣습니다. 접속 요청이 일어났을 때, sshd 는 연결하는 클라이언트 도구의 종류에 따라 올바른 접속을 만듭니다. 예를 들어, 원격 컴퓨터가 ssh 클라이언트 프로그램을 가지고 접속을 한다면, 그 OpenSSH 서버는 인증 후에 원격 조종 세션을 만듭니다. 만약 원격 사용자가 scp 를 가지고 OpenSSH 서버를 연결하면, 그 OpenSSH 서버 데몬은 인증 후에 서버와 클라이언트 간에 안전한 파일 복사를 시작 합니다. OpenSSH는 일반 암호, 공개 키, 그리고 Kerberos 티켓을 포함하는 여러가지 인증 방법을 사용할 수 있습니다.

4.2. 설치

OpenSSH 클라이언트와 서버 프로그램의 설치는 간단 합니다. 우분투 시스템에 OpenSSH 클라이언트 프로그램을 설치하려면, 다음의 명령을 터미널 프롬프트에서 사용 합니다:

```
sudo apt-get install openssh-client
```

OpenSSH 서버 프로그램과 관련되는 지원 파일을 설치하려면, 다음의 명령을 터미널 프롬프트에서 사용 합니다:

```
sudo apt-get install openssh-server
```

4.3. 설정

여러분은 OpenSSH 서버 프로그램, sshd, 의 기본 동작을 /etc/ssh/sshd_config 파일을 편집하는 것으로 설정할 수 있습니다. 이 파일에서 사용되는 설정 지시자에 대한

정보는, 터미널 프롬프트에서 다음의 명령을 입력하여 해당 매뉴얼 페이지를 보십시오:

```
man sshd_config
```

sshd 설정 파일에는 통신 설정과 인증 모드 등을 조종하기 위한 많은 지시자들이 있습니다. 다음은 /etc/ssh/ssh_config 파일을 편집하는 것으로 변경할 수 있는 설정 지시자들의 예 입니다.

설정 파일을 편집하기 전에, 원래의 파일을 복사본을 만들고 쓰기에서 그것을 보호해야만 합니다. 그래서 원래의 설정을 참고로 그리고 필요한 경우 재사용할 수 있습니다.

/etc/ssh/sshd_config 파일을 복사하고 쓰기에서 그것을 보호하려면, 터미널 프롬프트에서 다음의 명령을 입력 합니다:

```
sudo cp /etc/ssh/sshd_config /etc/ssh/sshd_config.original
sudo chmod a-w /etc/ssh/sshd_config.original
```

다음은 여러분이 변경할 수 있는 설정 지시자의 예 입니다:

- 여러분의 OpenSSH가 기본 설정된 TCP 포트 22 대신에 TCP 포트 2222를 사용하게 하려면, 다음과 같이 Port 지시자를 변경 합니다:

  Port 2222

- sshd 가 공개 키 기반의 로그인 신뢰서를 허용하게 하려면, 간단히 이 줄을 더하거나 변경 합니다:

  PubkeyAuthentication yes

  /etc/ssh/sshd_config 파일 내에 있고, 만약 이미 있다면, 그 줄의 주석처리 해제하는 것을 확신 하십시오.

- 여러분의 OpenSSH 서버가 선-로그인 배너로 /etc/issue.net 파일의 내용을 표시하게 만드려면, 간단히 이 줄을 더하거나 변경 합니다:

  Banner /etc/issue.net

  /etc/ssh/sshd_config 파일 내에 있습니다.

/etc/ssh/sshd_config 파일에 변경을 만든 후에, 그 파일을 저장하고, 변경의 효과를 가지려면 다음 명령을 터미널 프롬프트에서 사용하여 sshd 서버 프로그램을 재시작 합니다:

```
sudo /etc/init.d/ssh restart
```

sshd 를 위한 많은 다른 설정 지시자는 여러분의 필요에 맞게 그 서버 프로그램의 동작을 변경하는 것을 위하여 사용가능 합니다. 그러나,

만약 여러분이 서버를 접근할 수 있는 오직 한 가지 방법이 ssh 이고, /etc/ssh/sshd_config 파일을 통해 sshd 를 설정하는데 실수를 하였다면, 서버를 재시작할 때 잠겨지거나 sshd 서버가 부정확한 설정 지시자 때문에 시작하는 것이 거부될 수 있음을 조언 합니다. 그러므로 원격 서버 상의 이 파일을 편집할 때는 정말로 조심스럽게 하시기 바랍니다.

4.4. 참조

OpenSSH 웹사이트 [http://www.openssh.org/]

진보한 OpenSSH 위키 페이지 [https://wiki.ubuntu.com/AdvancedOpenSSH]

5. FTP 서버

파일 전송 프로토콜 (FTP)는 컴퓨터들 간에 파일을 올리고 내려받기 위한 TCP 프로토콜 입니다. FTP는 클라이언트/서버 모델로 동작을 합니다. 서버 구성 요소는 FTP 데몬으로 불립니다. 그것은 원격지 클라이언트에서의 FTP 요청을 계속적으로 듣습니다. 요청이 접수될 때, 그것은 로그인을 관리하고 접속을 만들어 줍니다. 세션이 지속되는 동안 그것은 FTP 클라이언트에서 보내지는 어떠한 명령도 실행을 합니다.

FTP 서버로 접근하는 것은 다음의 두 가지 방법으로 관리할 수 있습니다:

- 익명
- 인증

익명 모드에서는, 원격 클라이언트는 "anonymous" 또는 "ftp" 로 불리는 기본 설정 사용자 계정을 사용하고 암호는 이메일 주소를 보내는 것으로 FTP 서버를 접근할 수 있습니다. 인증 모드에서는, 사용자는 반드시 계정과 암호를 가지고 있어야 합니다. 사용자는 FTP 서버 디렉토리와 파일을 로그인 시에 사용되는 계정을 위하여 지정된 접근 권한에 따라 접근할 수 있습니다. 일반적인 규칙으로, FTP 데몬은 FTP 서버의 루트 디렉토리를 감추고 FTP 홈 디렉토리로 그것을 바꿉니다. 이것은 파일 시스템의 여타 부분도 원격 세션에게는 감춥니다.

5.1. vsftpd - FTP 서버 설치

vsftpd 는 우분투에서 사용할 수 있는 FTP 데몬 입니다. 이것은 설치, 설정, 그리고 관리하기가 쉽습니다. vsftpd 를 설치하려면 다음의 명령을 실행 합니다:

```
sudo apt-get install vsftpd
```

5.2. vsftpd - FTP 서버 설정

기본 설정된 값을 변경하기 위하여 vsftpd 설정 파일, /etc/vsftpd.conf 을 편집할 수 있습니다. 기본 설정은 오직 익명 FTP 만이 허용 됩니다. 만약 이 선택 사항을 비사용하려면, 다음의 줄을 반드시 변경하여야 합니다:

```
anonymous_enable=YES
```

to

```
anonymous_enable=NO
```

기본 설정 값으로, 로컬 시스템(FTP 서버가 실행되는 시스템) 사용자는 FTP 서버로 로그인 하는 것이 허용되지 않습니다. 이 설정 값을 변경하려면, 다음 줄의 주석을 해제하여야만 합니다:

```
#local_enable=YES
```

기본 설정으로, 사용자는 FTP 서버에서 파일을 내려받는 것은 허용이 되지만, FTP 서버로 파일을 올리는 것은 허용되지 않습니다. 이 설정 값을 변경하려면, 다음 줄의 주석을 해제하여야만 합니다:

```
#write_enable=YES
```

비슷하게, 기본 설정으로, 익명 사용자는 FTP 서버로 파일을 업로드하는 것이 허용되지 않습니다. 이 설정 값을 변경하려면, 다음 줄의 주석을 해제하여야만 합니다:

```
#anon_upload_enable=YES
```

설정 파일은 많은 설정 파라미터들로 이루어 집니다. 각각의 파라미터에 대한 정보는 그 설정 파일 내에 사용가능 합니다. 다른 방법으로는, **man 5 vsftpd.conf** 하여 각 파라미터의 자세한 것을 man 페이지에서 참조 하십시오.

vsftpd 를 설정했으면 데몬을 시작할 수 있습니다. vsftpd 데몬을 시작하려면 다음의 명령을 실행 합니다:

```
sudo /etc/init.d/vsftpd start
```

설정 파일에 기본 설정된 것은 보안의 사유를 위하여 지정된 것임을 주의 하십시오. 위의 변경된 각각은 시스템을 덜 보안적으로 할 수 있으므로, 그것들이 꼭 필요한 경우에만 변경을 하십시오.

6. 네트워크 파일 시스템 (NFS)

NFS는 네트워크 상의 다른 사람과 디렉토리와 파일을 공유하는 시스템을 허용 합니다. NFS를 사용하는 것으로, 사용자와 프로그램은 원격지 시스템 상의 파일을 로컬 파일을 사용하는 것과 거의 비슷하게 접근할 수 있습니다.

NFS가 제공하는 가장 주목할 만한 혜택의 몇 가지는 다음과 같습니다:

- 로컬 워크스테이션은 공통적으로 사용되는 데이터가 단일 기계에 저장되고 네트워크 상의 다른 것을 여전히 접근할 수 있기 때문에 보다 적은 디스크 공간을 사용 합니다.
- 사용자가 모든 네트워크 기계들에 분리된(각각의) 홈 디렉토리를 가질 필요가 없습니다. 홈 디렉토리는 NFS 서버 상에 만들어질 수 있고 네트워크를 통하여 사용할 수 있습니다.
- 플로티 디스크, CDROM 드라이브, 그리고 USB 드라이브와 같은 저장 장치들은 네트워크 상의 다른 기계에 의하여 사용될 수 있습니다. 이것은 네트워크 전체의 탈착실 미디어 드라이브의 숫자를 줄일지도 모릅니다.

6.1. 설치

NFS 서버를 설치하기 위하여 다음의 명령을 터미널 프롬프트에서 입력 합니다:

```
sudo apt-get install nfs-kernel-server
```

6.2. 설정

/etc/exports 파일에 디렉토리를 추가하는 것으로 내보낼 디렉토리를 설정할 수 있습니다. 예는:

```
/ubuntu *(ro,sync,no_root_squash)
/home *(rw,sync,no_root_squash)
```

호스트 이름 형식의 하나를 *로 대체할 수 있습니다. 호스트 이름 정의를 가능한 지정하여 원하지 않는 시스템이 NFS 마운트를 접근할 수 없도록 합니다.

NFS 서버를 시작하기 위하여, 다음의 명령을 터미널 프롬프트에서 실행할 수 있습니다:

```
sudo /etc/init.d/nfs-kernel-server start
```

6.3. NFS 클라이언트 설정

다른 기계에서 공유된 NFS 디렉토리를 마운트하려면 mount 명령을 사용하고, 터미널 프롬프트에서 다음의 명령과 비슷하게(각자의 경우에 맞게) 명령을 입력 합니다:

```
sudo mount example.hostname.com:/ubuntu /local/ubuntu
```

마운트 위치 디렉토리 /local/ubuntu 반드시 있어야 합니다. /local/ubuntu 디렉토리 내에는 파일 또는 서브 디렉토리가 없어야만 합니다.

다른 기계에서 NFS 공유를 마운트하는 다른 방법은 /etc/fstab 파일에 한 줄을 더하는 것 입니다. 그 줄은 NFS 서버의 호스트 이름, 내보내지는 서버 상의 디렉토리, NFS 공유가 마운트되는 로컬 기계 상의 디렉토리를 반드시 기술 합니다.

/etc/fstab 파일 내의 그 줄을 위한 일반적인 문법은 다음과 같습니다:

```
example.hostname.com:/ubuntu /local/ubuntu nfs rsize=8192,wsize=8192,timeo=14,intr
```

6.4. 참조

리눅스 NFS에 대해 자주하는 질문 [http://nfs.sourceforge.net/]

7. 동적 호스트 설정 프로토콜 (DHCP)

동적 호스트 설정 프로토콜 (DHCP) 는, 각각의 네트워크 호스트를 수작업으로 설정하는 것과는 반대로, 서버에서 자동으로 호스트 컴퓨터에 설정값을 지정할 수 있도록 해주는 네트워크 서비스 입니다. 설정된 컴퓨터는 DHCP 클라이언트가 되고 DHCP 서버에서 받은 설정값을 조작할 수 없고, 그 설정은 컴퓨터의 사용자에게 투명 합니다.

DHCP 서버에 의하여 DHCP 클라이언트로 제공되는 가장 공통적인 설정은 다음과 같습니다:

- IP 주소와 넷마스크
- DNS
- WINS

그러나, DHCP 서버는 다음과 같은 설정 값도 또한 공급을 할 수 있습니다:

- 호스트 이름
- 도메인 이름
- 기본 설정 게이트웨이
- 시간 서버
- 인쇄 서버

DHCP 사용의 장점은 네트워크가 변경될 때 입니다. 예를 들어, DNS 서버의 주소가 변경되었을 때, DHCP 서버에서만 그 변경이 필요하고, 모든 네트워크 호스트는 DHCP 클라이언트가 DHCP 서버를 읽는 다음 시점에 재 설정됩니다. 이 장점에 더하여, 네트워크에 새로운 컴퓨터를 통합하는 것도 또한 쉽고, IP 주소의 사용 가능성을 점검할 필요가 없습니다. IP 주소의 할당 시 충돌이 일어나는 것도 또한 줄어듭니다.

DHCP 서버는 다음의 두 가지 방법을 사용하여 설정 값을 제공할 수 있습니다:

맥 어드레스
: 이 방법은, 네트워크로 연결되는 각각의 네트워크 카드의 유일한 하드웨어 주소를 식별하기 위하여 DHCP를 사용하는 것과, DHCP 클라이언트가 네트워크 장치를 사용하는 DHCP 서버로의 요청을 만드는 매번 일정한 설정을 공급하는 것을, 수반 합니다.

어드레스 풀
: 이 방법은, 동적으로 그리고 먼저 오는 것이 먼저 수행되는 기본으로 설정 속성이 공급되는 DHCP 클라이언트에서 IP 주소의 풀 (때때로 한계 또는 범위로 불리는)을 지정하는 것을 수반 합니다. DHCP 클라이언트가 지정한 기간 동안 네트워크 상에 더 이상 있지 않을 때, 설정은 만료되고 다른 DHCP 클라이언트에 의해 사용되도록 주소 풀로 되돌려집니다.

우분투는 DHCP 서버와 클라이언트 모두를 제공 합니다. 서버는 dhcpd (dynamic host configuration protocol daemon) 입니다. 우분투와 함께 제공되는

클라이언트는 dhclient 이고 요구되는 모든 컴퓨터에 설치되고 자동으로 설정 됩니다. 두 프로그램 모두 설치와 설정이 쉽고 시스템이 부팅할 때 자동적으로 시작 됩니다.

7.1. 설치

터미널 프롬프트에서, dhcpd 를 설치하기 위하여 다음의 명령을 입력 합니다:

```
sudo apt-get install dhcpd
```

여러분은 다음의 출력을 보게 되고, 그것은 다음에 무엇을 해야하는지를 설명 합니다:

```
Please note that if you are installing the DHCP server for the first
time you need to configure. Please stop (/etc/init.d/dhcp
stop) the DHCP server daemon, edit /etc/dhcpd.conf to suit your needs
and particular configuration, and restart the DHCP server daemon
(/etc/init.d/dhcp start).

You also need to edit /etc/default/dhcp to specify the interfaces dhcpd
should listen to. By default it listens to eth0.

NOTE: dhcpd's messages are being sent to syslog. Look there for
diagnostics messages.

Starting DHCP server: dhcpd failed to start - check syslog for diagnostics.
```

7.2. 설정

설치를 끝내는 오류 메세지는 약간 혼란을 줄 수 있는데, 다음의 절차를 수행해서 그 서비스를 설정 하십시오:

아주 일반적으로, 여러분은 IP 주소를 불규칙적으로 지정하는 것을 원할 수 있습니다. 이것은 다음과 같이 설정하는 것으로 마칠 수 있습니다:

```
# Sample /etc/dhcpd.conf
# (add your comments here)
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 "mydomain.org";

subnet 192.168.1.0 netmask 255.255.255.0 {
range 192.168.1.10 192.168.1.100;
range 192.168.1.150 192.168.1.200;
```

```
}
```

이것은 DHCP 서버가 클라이언트에 192.168.1.10-192.168.1.100 또는 192.168.1.150-192.168.1.200 범위 내의 한 IP 주소를 주는 결과를 가집니다. 그 주소는, 만약 클라이언트가 특정한 시간 간격을 요청하지 않는다면, 600 초 동안 대여되는 IP 주소 입니다. 한편, 최대한 (허용되는) 대여 기간은 7200 초 입니다. 서버는 또한 클라이언트가 서브넷 마스크로 255.255.255.0, 브로트캐스트 주소로 192.168.1.255, 라우터/게이트웨이 주소로 192.168.1.254, 그리고 DNS 서버로 192.168.1.1과 192.168.1.2를 사용할 것을 "충고" 합니다.

만약 여러분의 윈도우즈 클라이언트를 위하여 WINS 서버를 지정할 필요가 있다면, 에를 들어, netbios-name-servers 옵션을 포함하는 것이 필요 합니다.

```
option netbios-name-servers 192.168.1.1;
```

Dhcpd 설정 값은 DHCP 미니-하우투에서 취해졌고, 그것은 여기 [http://www.tldp.org/HOWTO/DHCP/index.html]에서 찾을 수 있습니다.

7.3. 참조

DHCP에 대해 자주하는 질문 [http://www.dhcp-handbook.com/dhcp_faq.html]

8. 도메인 네임 서비스 (DNS)

도메인 네임 서비스 (DNS) 는 IP 주소와 완전히 주어진 도메인 이름(FQDN)을 다른 네임 서비스로 지도처럼 나타내는 인터넷 서비스 입니다. 이 방법으로, DNS는 IP 주소를 기억하는 필요를 완화 시킵니다. DNS를 실행하는 컴퓨터들은 네임 서버라 불리웁니다. 우분투는 GNU/Linux 상에서 네임 서버 관리를 위하여 가장 일반적으로 사용되는 프로그램인, BIND (Berkley Internet Naming Daemon) 를 제공 합니다.

8.1. 설치

터미널 프롬프트에서, dns를 설치하기 위하여 다음의 명령을 입력 합니다:

```
sudo apt-get install bind
```

8.2. 설정

DNS 설정 파일들은 /etc/bind 디렉토리에 저장 됩니다. 주요 설정 파일은 /etc/bind/named.conf 이고, 기본 설정 파일의 내용은 아래와 같이 보여집니다:

```
// This is the primary configuration file for the BIND DNS server named.
//
// Please read /usr/share/doc/bind/README.Debian for information on the
// structure of BIND configuration files in Debian for BIND versions 8.2.1
// and later, *BEFORE* you customize this configuration file.
//

include "/etc/bind/named.conf.options";

// reduce log verbosity on issues outside our control
logging {
 category lame-servers { null; };
 category cname { null; };
};

// prime the server with knowledge of the root servers
zone "." {
	type hint;
	file "/etc/bind/db.root";
};

// be authoritative for the localhost forward and reverse zones, and for
// broadcast zones as per RFC 1912

zone "localhost" {
	type master;
	file "/etc/bind/db.local";
};
```

```
zone "127.in-addr.arpa" {
        type master;
        file "/etc/bind/db.127";
};

zone "0.in-addr.arpa" {
        type master;
        file "/etc/bind/db.0";
};

zone "255.in-addr.arpa" {
        type master;
        file "/etc/bind/db.255";
};

// add local zone definitions here
include "/etc/bind/named.conf.local";
```

include 줄은 DNS 선택 사항을 가지는 파일 이름을 지정 합니다. 그 선택 사항 파일 내의 directory 줄은 파일을 어디서 볼 수 있는지 DNS에 알려 줍니다. BIND의 모든 파일은 이 디렉토리를 상대 경로로 사용 합니다.

/etc/bind/db.root 파일은 세상의 루트 네임 서버들을 기술 합니다. 그 서버들은 시간이 지남에 따라 변경되고 반드시 지금이나 나중에 관리유지 되어야 합니다.

zone 영역은 마스터 서버를 지정하고, 언급된 파일 태그로 파일에 저장 됩니다. 모든 zone 파일은 세 가지 자원 자료(RRs): SOA RR, NS RR과 PTR RR을 포함 합니다. SOA는 Start of Authority의 축약어 입니다. "@" 는 발생점을 의미하는 특별한 이름 표기 입니다. NS는 네임 서버 자원 자료 입니다. PTR은 도메인 네임 포인터 입니다. DNS 서버를 시작하기 위하여, 터미널 프롬프트에서 다음의 명령을 실행 합니다:

```
sudo /etc/init.d/bind start
```

상세한 것은 참조 편에 언급된 문서를 참고할 수 있습니다.

8.3. 참조

DNS HOWTO [http://www.tldp.org/HOWTO/DNS-HOWTO.html]

9. CUPS - 인쇄 서버

우분투의 인쇄와 프린트 서비스를 위한 주요 소프트웨어는 **Common UNIX Printing System** (CUPS) 입니다. 이 인쇄 시스템은 자유롭게 사용할 수 있고, 대부분의 GNU/Linux 배포판에서 인쇄를 위한 새로운 표준이 되는 이식 가능한 인쇄 계층 입니다.

CUPS는 인쇄 작업과 대기소를 관리하고, 표준 인터넷 인쇄 프로토콜(IPP)를 사용하여 네트워크 출력을 제공하고, 도트매트릭스부터 레이저까지의 굉장히 큰 범위의 프린터들과 그리고 많은 상호 간의 출력을 지원 합니다. CUPS는 또한 PostScript Printer Description (PPD) 과 네트워크 프린터의 자동 감지를 지원하고, 단순한 웹 기반의 설정과 관리 도구를 가지고 있습니다.

9.1. 설치

여러분의 우분투 컴퓨터에 CUPS를 설치하려면, 간단하게 apt-get 명령을sudo 로 사용하고 첫 번째 파라미터로 설치하고자 하는 패키지를 줍니다. 하나의 완전한 CUPS 설치는 많은 패키지 의존성을 가지지만, 같은 명령어 라인에 그것들을 모두 지정할 수 있습니다. CUPS를 설치하기 위하여 다음의 명령을 터미널 프롬프트에서 입력 하십시오:

```
sudo apt-get install cupsys cupsys-client
```

사용자 암호의 인증되면, 패키지는 내려받아지고 에러없이 설치되어집니다. 설치가 마무리될 때, CUPS 서버는 자동적으로 실행됩니다. 문제가 있고 그것을 확인하려면, /var/log/cups/error_log에 있는 에러 로그 파일을 통해 CUPS 서버 오류를 접근할 수 있습니다. 만약 그 에러 로그가 여러분이 직면한 문제를 파악하기 위한 충분한 정보를 보여주지 않는다면, CUPS 로그를 더 자세히 출력하도록 하는 것은 위에 언급된 설정 파일 내의 **LogLevel** 지시자를 "debug" 또는 심지어 "debug2"로 변경하는 것에 의하여 증가할 수 있고, 그러면 모든 것을 기록 합니다. 기본 설정된 값은 "info" 입니다. 만약 이 변경을 만들었다면, 여러분의 문제를 해결한 후에, 로그 파일이 너무 크게 되는 것을 막기 위하여 다시 원래의 설정 값으로 되돌리는 것을 기억 하십시오.

9.2. 설정

Common UNIX Printing System 서버의 동작은 /etc/cups/cupsd.conf 파일 내에 포함된 지시자를 통하여 설정 됩니다. CUPS 설정 파일은 아파치 HTTP 서버를 위한 주요 설정 파일과 같은 문법을 따르므로 아파치 설정 파일을 편집하는데 익숙한 사용자들은 CUPS 설정 파일을 편집할 때 쉽다고 느낄 수 있습니다. 처음으로 변경하기를 원하는 설정 값의 몇 가지는 여기에 보여 집니다.

설정 파일을 편집하기 전에, 원래의 파일의 복사본을 만들고 쓰기에서 그것을 보호해야만 합니다. 그래서 여러분은 원래의 설정을 참조하거나 그리고 필요한 경우 재사용 할 수 있습니다.

/etc/cups/cupsd.conf 파일을 복사하고 쓰기에서 그것을 보호하려면, 터미널 프롬프트에서 다음의 명령을 입력 합니다:

```
sudo cp /etc/cups/cupsd.conf /etc/cups/cupsd.conf.original
sudo chmod a-w /etc/cups/cupsd.conf.original
```

- **ServerAdmin**: CUPS 서버의 지정된 시스템 관리자의 이메일 주소를 설정하기 위한 것이고, 간단히 /etc/cups/cupsd.conf 설정 파일을 여러분이 선호하는 텍스트 에디터로 편집하기 위하여 열고, ServerAdmin 줄을 적절하게 수정을 합니다. 예를 들어, 여러분이 CUPS 서버의 시스템 관리자이고, 이메일 주소가 'bjoy@somebigco.com' 이면, 아래에 보이는 것과 같이 ServerAdmin 줄을 수정 합니다:

```
ServerAdmin bjoy@somebigco.com
```

CUPS 서버 설정 파일 내의 설정 지시자에 대한 더 많은 예제는, 터미널 프롬프트에서 다음의 명령을 입력하여 관계된 시스템 매뉴얼 페이지를 읽어 보십시오:

```
man cupsd.conf
```

/etc/cups/cupsd.conf 설정 파일에 변경을 만드는 어느 때에나, 터미널 프롬프트에서 다음의 명령을 입력하여 CUPS 서버를 재시작 하는 것이 필요 합니다:

```
sudo /etc/init.d/cupsys restart
```

Some other configuration for the CUPS server is done in the file /etc/cups/cups.d/ports.conf:

- **Listen**: 우분투 기본 설정에 의하여, CUPS 서버의 설치는 오직 127.0.0.1 IP 주소의 루프백 인터페이스만을 듣습니다. CUPS 서버가 실제 네트워크 어댑터의 IP 주소를 듣게 지시하려면, 여러분은 반드시 호스트 이름 또는 IP 주소 중의 하나, 또는 선택적으로, IP 주소/포트 쌍을 Listen 지시자에 추가해야 합니다. 예를 들어, 로컬 네트워크 상의 CUPS 서버의 IP 주소가 192.168.10.250 이고 이 서브 네트워크 상의 다른 시스템에서 그것을 사용할 수 있도록 만들기를 원한다면, /etc/cups/cups.d/ports.conf 파일을 편집하기 위하여 열고, 아래와 같이 Listen 지시자를 추가 합니다:

```
Listen 127.0.0.1:631 # existing loopback Listen
Listen /var/run/cups/cups.sock # existing socket Listen
```

```
Listen 192.168.10.250:631 # Listen on the LAN interface, Port 631 (IPP)
```

위의 예에서, 만약 여러분이 cupsd 가 루프백 인터페이스를 듣는 것을 원하지 않고 Local Area Network(LAN)의 이더넷 인터페이스만을 듣게하려고 한다면, 루프백 주소 (127.0.0.1)을 주석 처리하거나 삭제할 수 있습니다. 루프백을 포함하여, 특정 호스트 이름이 경계를 긋는 모든 네트워크 인터페이스를 듣게 만드려면, 아래와 같이 호스트 이름 socrates 를 위하여 Listen 항목을 만들 수 있습니다:

```
Listen socrates:631 # Listen on all interfaces for the hostname 'socrates'
```

또는 Listen 지시자는 제외하고 대신에 Port 를 사용하여 다음과 같이 할 수 있습니다:

```
Port 631 # Listen on port 631 on all interfaces
```

9.3. 참조

CUPS 웹사이트 [http://www.cups.org/]

10. HTTPD - 아파치2 웹 서버

아파치는 GNU/Linux 시스템 상에 가장 일반적으로 사용되는 웹 서버 입니다. 웹 서버는 클라이언트 컴퓨터에 의해 요청되는 웹 페이지를 제공하기 위하여 사용 됩니다. 클라이언트는 전형적으로 Firefox, Opera, 또는 Mozilla 와 같은 웹 브라우저를 사용하여 웹 페이지를 요청하고 보게 됩니다.

사용자는 웹 서버를 가리키기 위하여 완전히 지정된 도메인 이름(FQDN)과 요구되는 자원의 경로를 가지는 Uniform Resource Locator (URL) 을 입력 합니다. 예를 들어, 우분투 웹 사이트 [http://www.ubuntu.com]의 홈 페이지를 보려고 한다면, 사용자는 오직 FQDN 만을 입력할 것 입니다. 비용지불 지원 [http://www.ubuntu.com/support/supportoptions/paidsupport]에 특정 정보를 요청하려면, 사용자는 FQDN에 경로를 추가하여 입력 합니다.

웹 페이지를 전송하기 위하여 사용되는 가장 일반적인 프로토콜은 Hyper Text Transfer Protocol (HTTP) 입니다. Secure Sockets Layer 상의 Hyper Text Transfer Protocol (HTTPS) 와 파일을 업로드 또는 다운로드 하기 위한 File Transfer Protocol (FTP) 같은 프로토콜들도 또한 지원 됩니다.

아파치 웹 서버는 MySQL 데이타베이스 엔진, HyperText Preprocessor (PHP) 스크립트 언어, 그리고 Python과 Perl과 같은 다른 인기있는 스크립트 언어들과 함께 종종 사용되어 집니다. 이런 설정을 LAMP (Linux, Apache, MySQL 과 Perl/Python/PHP)라 명명하고, 이것은 웹 기반의 프로그램을 개발하고 이행하기 위한 강력하고 튼튼한 플랫폼을 구성 합니다.

10.1. 설치

아파치2 웹 서버는 우분투 리눅스에서 사용 가능합니다. 아파치2를 설치하려면:

- 터미널 프롬프트에서 다음의 명령을 입력 합니다:

```
sudo apt-get install apache2
```

10.2. 설정

아파치는 일반 텍스트 설정 파일 내에 지시자를 넣는 것으로 설정이 됩니다. 주 설정 파일은 apache2.conf 입니다. 추가하여, 다른 설정 파일들은 Include 지시자를 사용하여 더해질 수 있고, 많은 설정 파일을 포함하기 위하여 와일드카드를 사용할 수 있습니다. 어떠한 지시자도 이러한 설정 파일들에 놓여질 수 있습니다. 주 설정 파일의 변경은 아파치2가 시작 또는 재시작될 때만 인식이 됩니다.

서버는 또한 TypesConfig 지시자에 의해 정해지는 파일 이름과 그리고 기본으로 mime.types인 mime 문서 종류를 가지는 파일을 읽을 수 있습니다.

기본 아파치2 설정 파일은 /etc/apache2/apache2.conf 입니다. 아파치2 서버를 설정하기 위하여 이 파일을 편집할 수 잇습니다. 포트 번호, 문서 루트, 모듈, 로그 파일, 가상 호스트, 기타 등등을 설정할 수 있습니다.

10.2.1. 기본적인 설정

이 영역은 아파치2 서버의 필수적인 설정 파라미터를 설명 합니다. 더 자세한 것은 아파치2 문서 [http://httpd.apache.org/docs/2.0/]를 참조 합니다.

- 아파치2는 가상 호스트에 친근한 기본 설정과 함께 제공 됩니다. 그것은, 하나의 기본 설정 가상 호스트를 (VirtualHost 지시자를 사용하여) 가지고 설정되어 있고, 변경되거나 만약 하나의 사이트를 가지고 있다면 그대로 사용할 수도 있으며, 여러 개의 사이트를 가지고 있다면 추가적인 가상 호스트를 위한 예제 양식으로 사용될 수도 있습니다. 그대로 사용을 하면, 기본 설정된 가상 호스트는 여러분의 기본 사이트로 동작하거나, 또는 사이트 사용자가 여러분이 지정한 사이트의 ServerName 지시자와 그들이 입력한 URL이 일치되는 않는 경우를 볼 수 있습니다. 기본 설정 가상 호스트를 변경하려면, /etc/apache2/sites-available/default 파일을 편집 합니다. 만약 새로운 가상 호스트나 사이트를 설정하기를 원한다면, 같은 디렉토리 내로 여러분이 선택한 이름을 가지고 그 파일을 복사 합니다. 예를 들어, **sudo cp /etc/apache2/sites-available/default /etc/apache2/sites-available/mynewsite** 아래에 기술하는 몇 가지 지시자들을 사용하여 새로운 사이트를 설정하기 위하여 그 새로운 파일을 편집 합니다.
- ServerAdmin 지시자는 서버의 시스템 관리자를 위한 이메일 주소를 광고하기 위하여 지정 합니다. 기본 설정값은 webmaster@localhost 입니다. 이것은, 만약 여러분이 그 서버의 시스템 관리자라면, 여러분에게로 배달될 수 있는 이메일 주소로 변경되어야 합니다. 만약 여러분의 웹 사이트가 문제를 가지고 있다면, 아파치2는 그 문제를 보고하기 위하여 이 이메일 주소를 가지는 에러 메세지를 보여줍니다. /etc/apache2/sites-available 내의 사이트 설정 파일에서 이 지시자를 찾으십시오.
- Listen 지시자는 아파치2가 들어야하는, 포트, 그리고 선택 사항으로 IP 주소를 지정 합니다. 만약 IP 주소가 지정되지 않았다면, 아파치2는 서버가 실행되는 기계에 지정된 모든 IP 주소를 듣습니다. Listen 지시자를 위한 기본 설정값은 80 입니다. 오직 여러분의 루프백 인터페이스를 듣게하기 위하여 이것을 127.0.0.1:80으로 변경하고 그러면 서버는 인터넷으로는 사용할 수 없고, 듣고자 하는 포트를 변경하기 위하여 (예를 들어) 81로 지정할 수도 있고, 또는 보통의 동작을 위하여 있는 그대로 나두기도 합니다. 이 지시자를 위한 /etc/apache2/ports.conf 파일에서 지시자를 찾고 변경할 수 있습니다.
- ServerName은 선택사항입니다. 이 부분은 웹사이트에 접근할 수 있는 FQDN을 지정하는 역할을 합니다. 기본 가상 호스트에는 설정하둔 ServerName이 없기 때문에 다른 가상 호스트에서 사용하는 ServerName이 아닌 FQDN은 모두 기본 가상 호스트로 연결됩니다. ubunturocks.com이라는 도메인 이름을 구했을 때, 가상 호스트 설정 파일에 있는 ServerName의 값으로

ubunturocks.com을 입력하십시오. ServerName은 앞에서 만든 가상 호스트 파일(/etc/apache2/sites-available/mynewsite)에 넣으십시오.

www를 앞에 붙이는 것을 당연하게 생각하는 사용자들도 많기 때문에 www.ubunturocks.com를 통해서도 웹사이트에 접근할 수 있게 설정하고 싶어할 수도 있습니다. 이 때 ServerAlias를 사용하면 됩니다. ServerAlias에 와일드카드를 사용할 수도 있습니다. 예를 들어, **ServerAlias *.ubunturocks.com**를 입력하면 .ubunturocks.com으로 끝나는 주소를 아무거나 사용하여 웹사이트에 접근할 수 있게 됩니다.

- DocumentRoot는 웹사이트를 구성하는 파일들을 아파치가 찾을 때 사용하는 위치입니다. 기본값은 /var/www입니다. 아직은 /var/www에 아무런 웹사이트가 없지만, /etc/apache2/apache2.conf에 있는 RedirectMatch의 주석을 풀면 연결 요청이 /var/www/apache2-default로 연결되어 아파치2의 기본 웹사이트를 볼 수 있게 됩니다. 서버의 가상호스트 파일에 있는 이 값을 바꾸고, 필요한 경우에는 그 디렉토리를 변경하는 것은 잊지 마십시오.

아파치는 /etc/apache2/sites-available 디렉토리를 직접 파싱하지 **않습니다**. /etc/apache2/sites-enabled에 있는 심볼릭 링크는 "접근할 수 있는" 사이트를 가리킬 뿐입니다. a2ensite (Apache2 Enable Site) 프로그램을 사용하여 **sudo a2ensite mynewsite**를 입력하여 필요한 심볼릭 링크를 만들 수 있습니다. 이 때 mynewsite는 새로 연결할 사이트의 설정 파일 /etc/apache2/sites-available/mynewsite입니다. 비슷한 방법으로 a2dissite를 사용하여 사이트의 연결을 해제할 수도 있습니다.

10.2.2. 기본 설정

이 부분은 아파치2의 기본 설정을 설명합니다. 예를 들어, 가상호스트를 추가할 경우 그 가상호스트에서는 그 호스트를 위해 설정한 값이 우선순위를 가집니다. 가상호스트를 위해 설정한 값이 없을 때 기본값을 사용합니다.

- DirectoryIndex는 사용자가 디렉토리명 끝에 /(슬래시)를 지정하여 디렉토리의 목록을 보고자 할 때 서버에서 기본으로 제공하는 페이지를 지정합니다.

  예를 들어, 사용자가 http://www.example.com/this_directory/라는 페이지를 요청한다면, 사용자가 볼 수 있는 페이지에 몇 가지가 있습니다. 우선, DirectoryIndex 페이지가 있을 경우에는 그 페이지를 보게 됩니다. 이 페이지가 없고, Indexes 옵션이 설정되어있다면 서버에서 생성한 디렉토리 목록을 보게 됩니다. 마지막으로 DirectoryIndex 페이지도 없고 Indexes 옵션도 설정이 안 되어있으면 Permission Denied 페이지를 보게 됩니다. 즉, 사용자의 요청이 들어오면 서버는 우선 DirectoryIndex에 설정된 파일 중에서 가장 먼저 발견하는 파일을 사용자에게 제공합니다. DirectoryIndex에 있는 파일이 하나도 없고, Indexes 옵션이 설정되어 있다면 서버는 HTML 형식으로 그 디렉토리에 있는 하위 디렉토리와 파일의 목록을 생성해서 사용자에게 제공합니다. /etc/apache2/apache2.conf에 있는 DirectoryIndex의 기본값은 "index.html index.cgi

index.pl index.php index.xhtml" 입니다. 사용자가 요청한 디렉토리에 앞의 파일 중 하나가 있다면 아파치2는 이 중 가장 앞의 것을 사용자에게 제공합니다.

- ErrorDocument 지시자는 특정한 에러 사건을 위하여 사용할 수 있도록 아파치를 위한 파일을 지정하는 것을 허용 합니다. 예를 들어, 사용자가 요청한 자원이 존재하지 않으면, 404 에러가 일어나고, 아파치2 기본 설정에 따라, /usr/share/apache2/error/HTTP_NOT_FOUND.html.var 파일이 보여지게 됩니다. 그 파일은 서버의 DocumentRoot에 없고, /error 디렉토리를 /usr/share/apache2/error/ 로의 요청으로 재지정하는 /etc/apache2/apache2.conf 내의 Alias 지시자가 있습니다. 기본 설정된 ErrorDocument 지시자들의 목록을 보려면, 이 명령을 사용 합니다: **grep ErrorDocument /etc/apache2/apache2.conf**
- 기본 설정에 의하여, 서버는 /var/log/apache2/access.log 파일로 전송 로그를 기록 합니다. CustomLog 지시자를 가지고 가상 호스트 설정 파일 내의 사이트당 이것을 변경하거나, 또는 /etc/apache2/apache2.conf에 지정된 기본 설정된 것을 제외시킬 수 있습니다. 또한 ErrorLog 지시자를 통하여 에러가 기록되는 파일로 지정할 수도 있습니다. 이 경우의 기본 설정은 /var/log/apache2/error.log 입니다. LogLevel (기본 설정은 "경고")과 LogFormat (기본 설정은 /etc/apache2/apache2.conf를 보십시오)도 역시 지정할 수 있습니다.
- 몇 가지 선택 사항은 서버당 설정이기 보다는 디렉토리당 지정이 됩니다. Option은 이러한 지시자들 중의 하나 입니다. Directory 부분은 XML 비슷하게 태크로 묶여지고, 그래서 다음과 비슷합니다:

```
<Directory /var/www/mynewsite>
  ...
 </Directory>
```

Options 지시자는 Directory 부분 내에 하나 또는 그 이상의 다음의 값들을 가지고 (다른 것들과 함께), 공백으로 구분 됩니다:

- **ExecCGI** - CGI 스크립트의 실행을 허용 합니다. 만약 이 선택사항이 선택되지 않았다면 CGI 스크립트는 수행될 수 없습니다.

  대부분의 파일은 CGI 스크립트로서 실행이 되어서는 안됩니다. 이것은 매우 위험할 수 있습니다. CGI 스크립트는 여러분의 DocumentRoot 밖의 다른 디렉토리 내에 저장되어야만 하고, 오직 이 디렉토리만이 ExecCGI 옵션을 가져야 합니다. 이것은 기본 설정이고, CGI 스크립트를 위한 기본 위치는 /usr/lib/cgi-bin 입니다.
- **Includes** - 서버 측의 includes를 허용 합니다. 서버 측 includes는 include 파일들로 HTML 파일을 허용 합니다. 이것은 일반적인 선택 사항이 아닙니다. 더 많은 정보는 아파치2 SSI 하우투 [http://httpd.apache.org/docs/2.0/howto/ssi.html]를 보십시오.
- **IncludesNOEXEC** - 서버측 includes를 허용하지만, CGI 스크립트 내의 #exec과 #include 명령을 사용하지 못하도록 합니다.
- **Indexes** - 요청된 디렉토리내에 DirectoryIndex가 (index.html과 같은) 없다면, 디렉토리 내용물의 형식화된 목록을 보여 줍니다.

- **Multiview** - 컨텐츠에 따라 복수개의 보기를 지원 합니다. 이 선택 사항은 보안상의 이유로 기본 설정으로는 사용하지 못하도록 되었습니다. 이 선택 사항에 대한 아파치2 문서 [http://httpd.apache.org/docs/2.0/mod/mod_negotiation.html#multiviews]를 보십시오.
- **SymLinksIfOwnerMatch** - 만약 타켓 파일 또는 디렉토리가 링크와 같은 소유자를 가졌다면 오직 심볼릭 링크를 따릅니다.

10.2.3. 가상 호스트 설정

가상 호스트는 같은 기계를 다른 IP 주소, 다른 호스트 이름, 또는 다른 포트로 실행할 수 있도록 합니다. 예를 들어, 같은 웹 서버에서 가상 호스트를 사용하여 http://www.example.com 과 http://www.anotherexample.com 을 실행할 수 있습니다. 이 선택 사항은 기본 설정 가상 호스트와 IP 기반 가상 호스트를 위한 <VirtualHost> 지시자와 대응 합니다. 이름 기반의 가상 호스트는 <NameVirtualHost> 지시자와 대응 합니다.

하나의 가상 호스트를 위한 지시자의 집합은 그 특정 가상 호스트에만 적용이 됩니다. 만약 서버 전체로 지시자가 지정이 되고 가상 호스트 설정 내에 정의가 안되었다면, 기본 설정 값이 사용 됩니다. 예를 들어, 웹마스터 이메일 주소를 지정할 수 있고 각각의 가상 호스트를 위한 개별적인 이메일 주소를 설정하지 않을 수도 있습니다.

가상 호스트를 위하여 루트 문서를 (index.html과 같은) 가지는 디렉토리는 DocumentRoot 지시자로 지정을 합니다. 기본 설정된 DocumentRoot는 /var/www 입니다.

ServerAdmin 지시자는 VirtualHost 절에 포함되는, 에러 페이지에서 이메일 주소와 함께 바닥글을 보여주는 것을 선택하였다면, 에러 페이지의 바닥글에 사용되는 이메일 주소 입니다.

10.2.4. 서버 설정

이 영역은 어떻게 기본적인 서버 설정을 하는지를 설명 합니다.

LockFile - LockFile 지시자는 서버가 USE_FCNTL_SERIALIZED_ACCEPT 또는 USE_FLOCK_SERIALIZED_ACCEPT 중의 하나로 컴파일 되었을 때 사용되는 lockfile의 경로를 지정 합니다. 그것은 반드시 로컬 디스크에 저장되어야 합니다. NFS 공유 상에 로그 디렉토리가 위치하지 않는 한 기본 설정된 값으로 나두십시오. 이 경우라면, 오직 root에 의해서만 읽을 수 있는 디렉토리로 로컬 디스크 상의 위치를 기본 설정 값으로 변경 합니다.

PidFile - PidFile 지시자는 서버가 프로세스 ID (pid)를 기록하는 파일을 지정 합니다. 이 파일은 반드시 root에 의해서만 읽혀질 수 있어야 합니다. 많은 경우에, 이 지시자는 기본 설정값으로 남겨져야 합니다.

User - User 지시자는 요청을 대답하기 위하여 서버에 의해 사용되는 사용자 아이디를 지정 합니다. 이 설정은 서버의 접근을 결정 합니다. 이 사용자가 접근할 수 없는 파일은 또한 여러분의 웹 사이트 방문자도 접근할 수 없습니다. User를 위하여 기본 설정된 값은 www-data 입니다.

여러분이 하는 것을 정확히 알지 않는 한, User 지시자를 root로 지정하지 마십시오. User로 root를 사용하는 여러분의 웹 서버에 거대한 보안 구멍을 만들게 됩니다.

Group 지시자는 User 지시자와 비슷합니다. Group은 서버가 요청을 대답하는 그룹을 지정 합니다. 기본 설정된 그룹은 또한 www-data 입니다.

10.2.5. 아파치 모듈

아파치는 모듈 방식의 서버 입니다. 이것은 핵심 서버에는 가장 기본적인 기능만을 포함하는 것을 의미 합니다. 확장되는 기능은 아파치로 올려질 수 있는 모듈을 통하여 사용 가능 합니다. 기본 설정으로, 모듈의 기본적인 집합은 컴파일 시에 서버에 포함 됩니다. 만약 서버가 동적으로 올려지는 모듈을 사용하도록 컴파일 되었다면, 모듈은 분리하여 컴파일 될 수 있고, LoadModule 지시자를 사용하여 어느 때나 추가될 수 있습니다. 그렇지 않다면, 아파치는 모듈을 추가하거나 삭제하도록 반드시 재 컴파일 되어야 합니다. 우분투는 아파치2가 동적 모듈의 올림을 허용하도록 컴파일 하였습니다. 설정 지시자들은 <IfModule> 블럭 내에 특정 모듈의 존재를 넣는 것으로 조건적으로 포함될 수 있습니다. 여러분은 추가적인 아파치2 모듈을 설치할 수 있고 웹 서버와 함께 사용을 할 수 있습니다. 아파치2 모듈은 apt-get 명령을 사용하여 추가할 수 있습니다. 예를 들어, MYSQL 인증을 위한 아파치2 모듈을 설치하려면, 다음의 명령을 터미널 프롬프트에서 실행을 합니다:

```
sudo apt-get install libapache2-mod-auth-mysql
```

모듈을 설치한 후, 그 모듈은 /etc/apache2/mods-available 디렉토리 내에 있게 됩니다. 모듈을 사용 가능하게 하는 것은 a2enmod 명령을 사용할 수 있습니다. 모듈을 사용 가능하게 하면, 그 모듈은 /etc/apache2/mods-enabled 디렉토리 내에 있게 됩니다.

10.3. HTTPS 설정

mod_ssl 모듈은 아파치2 서버에 중요한 - 통신을 암호화 하는 기능을 더합니다. 그러므로, SSL 암호화를 사용하여 여러분의 브라우저가 통신을 할 때, https:// 접두 주소가 브라우저 주소 막대 내의 Uniform Resource Locator (URL)의 시작에 사용 됩니다.

mod_ssl 모듈은 apache2-common 패키지 내에 있습니다. 이 패키지가 설치되어 있다면, 터미널 프롬프트에서 다음의 명령을 실행하여 mod_ssl 모듈을 활성화 할 수 있습니다:

```
sudo a2enmod ssl
```

10.3.1. 인증서와 보안

여러분의 안전한 서버를 만들기 위하여, 공개와 사적 키 쌍을 만들기 위한 공개 키 암호화를 사용 합니다. 대부분의 경우에, 여러분의 공개 키를 포함하는 인증 요청, 여러분 회사의 이름 등의 증명, 그리고 인증 기관(CA)에 지불하는 비용을 보냅니다. CA는 인증 요청과 여러분의 식별을 확인한 후 보안 서버를 위하여 인증서를 보내게 됩니다.

다른 방법으로, 여러분 스스로 자가-사인한 인증서를 만들 수 있습니다. 그러나, 자가-사인 인증서는 대부분의 현업 환경에서는 사용하지 말아야 함을 주의 하십시오. 자가-사인 인증서는 사용자의 웹브라우저에 의해 자동적으로 받아들여지지 않습니다. 사용자는 웹브라우저에 의하여 인증서를 받아들이고 보안 연결을 만들기 위한 질문을 받게 됩니다.

자가-사인 인증서 또는 여러분이 선택한 CA에서 사인한 인증서를 가진 후에, 그것을 보안 서버에 설치하는 것이 필요 합니다.

10.3.2. 인증서의 종류

보안 서버를 동작하게 하려면 키와 인증서가 필요 합니다. 이것은 자가-사인한 인증서를 만들거나 또는 CA-사인 인증서를 구매하여야 하는 것을 의미 합니다. CA-사인 인증서는 여러분의 서버에 두 가지 중요한 능력을 제공 합니다:

- 웹브라우저들은 (대개) 사용자에게 묻는 것 없이 자동적으로 인증서와 만들어진 보안 연결을 인식 합니다.
- CA가 사인된 인증을 발행하였을 때, 그것은 웹 페이지를 브라우저에 제공하는 단체의 식별을 보장 합니다.

SSL을 지원하는 대부분의 웹 브라우저는 그들이 자동적으로 받아들이는 인증한 CA의 목록을 가집니다. 만약 브라우저가 목록 내에 인증된 CA를 가지지 않은 인증서를 만나게 되면, 브라우저는 사용자에게 접속을 허용할 것인지 또는 거절할 것인지를 물어보게 됩니다.

여러분은 보안 서버를 위하여 자가-사인된 인증서를 만들 수 있지만, 자가-사인된 인증서는 CA-사인된 인증서와 같은 기능을 제공하지 않음을 알고있어야 합니다. 자가-사인된 인증서는 대부분의 웹 브라우저에 의해 자동적으로 인식되지 않고, 자가-사인된 인증서는 웹 사이트를 제공하는 단체의 식별에 대한 염려를 위한 어떤 보증도 제공하지 않습니다. CA-사인된 인증서는 보안 서버를 위한 이 두 가지의 중요한 능력을 제공 합니다. CA에서 인증서를 받는 절차는 아주 쉽습니다. 빠른 개괄적인 것은 다음과 같습니다:

1. 사적 그리고 공개 암호 키 쌍을 만듭니다.
2. 공개 키에 근거하여 인증서 요청을 만듭니다. 인증서 요청은 여러분의 서버와 그것을 호스팅하는 회사에 대한 정보를 가집니다.

3. 인증서 요청을, 여러분의 인적 사항을 제공하는 문서와 함께 CA로 보냅니다. 우리는 여러분에게 어떤 인증 기관을 선택할 지를 이야기할 수 없습니다. 여러분의 결정은 아마 여러분의 과거 경험, 친구나 동료의 경험, 또는 순전히 금전상의 요인에 근거할 겁니다.

   CA를 결정하였다면, 그들에게서 어떻게 인증서를 얻을 수 있는지를 그들이 제공한 지시에 따르는 것이 필요 합니다.
4. CA가 여러분이 정말로 요청을 한 사람임을 만족하게 되면, 그들은 디지털 인증서를 여러분에게 보냅니다.
5. 이 인증서를 여러분의 보안 서버에 설치하고, 보안 트랜잭션을 관리하기 시작 합니다.

CA에서 인증서를 받던지 또는 여러분 스스로 자가-사인 인증서를 만들던지, 첫 번째 단계는 키를 만드는 것 입니다.

10.3.3. Certificate Signing Request (CSR) 만들기

인증서 서명 요청 (CSR)을 만드려면, 여러분 소유의 키를 만들어야만 합니다. 키를 만들기 위하여 터미널 프롬프트에서 다음의 명령을 수행할 수 있습니다:

```
openssl genrsa -des3 -out server.key 1024
```

```
Generating RSA private key, 1024 bit long modulus
.....................++++++
.................++++++
unable to write 'random state'
e is 65537 (0x10001)
Enter pass phrase for server.key:
```

이제 여러분의 암호 문구를 입력 합니다. 최선의 보안을 위하여, 그것은 최소한 8자리 문자여야 합니다. -deb3을 지정하는 경우 최소한의 길이는 4자리 문자 입니다. 그것은 숫자 그리고/또는 구두점을 포함하고 사전내의 단어여서는 안됩니다. 암호 문구는 대소문자 구별을 하는 것을 기억 하십시오.

확인을 위하여 암호 문구를 재 입력 합니다. 그것을 정확히 재 입력한 후, 서버 키는 만들어지고 server.key 파일로 저장이 됩니다.

또한 여러분의 보안 웹 서버를 암호 구문 없이 실행시킬 수 있습니다. 이것은 보안 웹 서버를 시작하는 매 번마다 암호 구문을 입력할 필요가 없으므로 편리합니다. 하지만, 그것은 굉장히 안전하지 못한 방법이고 보안 키의 절충은 서버의 절충과 마찬가지의 의미 입니다.

어떤 경우에는, 구문 생성에서 -des3 스위치는 떼는 것 또는 터미널 프롬프트에서 다음의 명령을 수행하는 것으로 암호 구문 없이 보안 웹 서버를 실행하는 것을 선택할 수 있습니다:

```
openssl rsa -in server.key -out server.key.insecure
```

위의 명령을 실행하면, 그 insecure 키는 server.key.insecure 파일에 저장 됩니다. 여러분은 이 파일을 암호 구문 없이 CSR을 생성할 때 사용할 수 있습니다.

CSR을 만드려면, 터미널 프롬프트에서 다음의 명령을 실행 합니다:

```
openssl req -new -key server.key -out server.csr
```

암호 구문을 입력하도록 물어 봅니다. 만약 여러분이 정확한 암호 구문을 입력하면, 회사 이름, 사이트 이름, 이메일 ID 등을 입력하도록 물어 봅니다. 이러한 모든 사항을 입력한 후에, 여러분의 CSR은 만들어지고 그것은 server.csr 파일에 저장 됩니다. 이 CSR 파일을 이 후의 절차를 위하여 CA로 보낼 수 있습니다. CAN은 이 CSR 파일을 사용하고 인증서를 발행 합니다. 다른 한편으로는, 여러분은 이 CSR을 사용하여 자가-사인 인증서를 만들 수도 있습니다.

10.3.4. 자가-사인 인증서 만들기

자가-사인 인증서를 만들기 위하여, 터미널 프롬프트에서 다음의 명령을 실행 합니다:

```
openssl x509 -req -days 365 -in server.csr -signkey server.key -out server.crt
```

위의 명령은 여러분이 암호 구문을 입력하도록 물어 봅니다. 정확한 암호 구문이 입력된 후, 여러분의 인증서가 만들어지고 그것은 server.crt 파일에 저장 됩니다.

만약 여러분의 보안 서버가 현업 환경에서 사용이 된다면, 아마도 CA가 사인한 인증서가 필요할 겁니다. 자가-사인한 인증서를 사용하는 것은 권장되지 않습니다.

10.3.5. 인증서 설치

키 파일 server.key와 인증서 파일 server.crt 또는 여러분의 CA에서 발행한 인증서 파일을 터미널 프롬프트에서 다음의 명령들을 수행하여 설치할 수 있습니다:

```
sudo cp server.crt /etc/ssl/certs
sudo cp server.key /etc/ssl/private
```

/etc/apache2/sites-available/default 파일 또는 여러분의 보안 가상 호스트를 위한 설정 파일에 다음의 네 줄을 추가하여야 합니다. VirtualHost 부분에 그것을 넣습니다. 그것은 DocumentRoot 줄 밑에 놓여집니다:

```
SSLEngine on
SSLOptions +FakeBasicAuth +ExportCertData +CompatEnvVars +StrictRequire
```

```
SSLCertificateFile /etc/ssl/certs/server.crt
SSLCertificateKeyFile /etc/ssl/private/server.key
```

HTTPS는 포트 번호 443을 듣습니다. /etc/apache2/ports.conf 파일에 다음의 줄을 추가하여야 합니다:

```
Listen 443
```

10.3.6. 서버에 접근하기

여러분의 인증서를 설치한 후에, 웹 서버를 재 시작하여야 합니다. 터미널 프롬프트에서 다음의 명령을 실행하여 웹 서버를 재 시작할 수 있습니다:

```
sudo /etc/init.d/apache2 restart
```

여러분은 반드시 그 암호 구문을 기억해야 하고 보안 웹 서버가 시작되는 매 번마다 암호 구문을 입력 합니다.

암호 구문을 입력하도록 물어 봅니다. 정확한 암호 구문을 입력한 후에, 보안 웹 서버는 시작 됩니다. 여러분의 웹 브라우저 주소 란에서 https://your_hostname/url/ 형식으로 입력하여 보안 서버 페이지를 접근 합니다.

10.4. 참조

아파치2 문서 [http://httpd.apache.org/docs/2.0/]

Mod SSL 문서 [http://www.modssl.org/docs/]

11. Squid - 프락시 서버

Squid는 완전한 기능을 갖춘 웹 프락시 캐쉬 서버 프로그램이고 Hyper Text Transport Protocol (HTTP), File Transfer Protocol (FTP), 그리고 다른 인기있는 네트워크 프로토콜들을 위한 프락시와 캐쉬 서비스를 제공 합니다. Squid는 Secure Sockets Layer (SSL) 요청의 캐싱과 프락싱 그리고 Domain Name Server (DNS) 조회의 캐싱을 이행할 수 있고, 투명한 캐싱을 수행 합니다. 또한, Squid는 Internet Cache Protocol (ICP), Hyper Text Caching Protocol (HTCP), Cache Array Routing Protocol (CARP), 그리고 Web Cache Coordination Protocol (WCCP) 프로토콜과 같은 다양한 종류의 캐싱 프로토콜을 지원 합니다.

Squid 프락시 캐쉬 서버는 다양한 프락시와 캐싱 서버의 요구에 맞는 훌륭한 솔루션이고, 광범위하고 조직적인 접근 조종 기능과 Simple Network Management Protocol (SNMP)를 통하여 아주 중요한 것들의 감시 기능을 제공하므로 지점 사무실에서 부터 기업 수준의 네트워크 까지로 확장할 수 있습니다. 전용의 Squid 프락시, 또는 캐싱 서버로 하나의 컴퓨터를 선택하였을 때, Squid는 성능을 향상시키기 위하여 메모리 내의 캐쉬를 관리하므로 많은 양의 실제 메모리를 가지도록 시스템을 설정 합니다.

11.1. 설치

터미널 프롬프트에서, Squid 서버를 설치하기 위하여 다음의 명령을 입력 합니다:

```
sudo apt-get install squid squid-common
```

11.2. 설정

Squid는 /etc/squid/squid.conf 설정 파일 내의 지시자를 편집하는 것으로 설정 딥니다. 다음의 예는 Squid 서버의 동작에 영향을 주기 위하여 변경될 수 있는 몇 가지의 지시자들을 보여 줍니다. 더 깊은 Squid의 설정에 대한 것은, 참조 영역을 보십시오.

설정 파일을 편집하기 전에, 원래의 파일의 복사본을 만들고 그것을 쓰기에서 보호해야만 합니다. 그래서 참조로서 원래의 설정값을 가질 수 있고, 필요한 경우 재 사용할 수 있습니다.

터미널 프롬프트에서 다음의 명령을 입력하여 /etc/squid/squid.conf 파일을 복사하고 그것을 쓰기에서 보호 합니다:

```
sudo cp /etc/squid/squid.conf /etc/squid/squid.conf.original
sudo chmod a-w /etc/squid/squid.conf.original
```

☐Squid 서버가 기본 설정된 TCP 포트 3128 대신에 TCP 포트 8888을 듣게 지정하려면, 다음과 같이 http_port 지시자를 변경 합니다:

http_port 8888

- Squid 서버에 특정 호스트 이름을 주기 위하여 visible_hostname 지시자를 변경 합니다. 이 호스트 이름은 꼭 그 컴퓨터의 호스트 이름일 필요는 없습니다. 이 예에서는 그것은 weezie로 지정 되었습니다.

  visible_hostname weezie

- 다시 한번, Squid 접근 조종을 사용하여, 특정 Internet Protocol (IP) 주소들을 가지는 사용자들만이 Squid에 의해 프락시된 인터넷 서비스가 사용 가능하도록 설정할 수 있습니다. 예를 들어, 192.168.42.0/24 서브 네트워크의 사용자들에 의해서만 접근할 수 있는 것을 보입니다:

  다음을 여러분의 /etc/squid/squid.conf 파일의 ACL 영역의 **가장 아래**에 추가 합니다:

  acl fortytwo_network src 192.168.42.0/24

  그런 다음, /etc/squid/squid.conf 파일의 http_access 영역의 **가장 위**에 다음을 추가 합니다:

  http_access allow fortytwo_network

- Squid의 훌륭한 접근 조종 기능을 사용하여, 여러분의 오직 정규 업무 시간 동안에만 Squid에 의하여 프락시된 인터넷 서비스가 사용 가능하도록 설정할 수 있습니다. 예를 들어, 월요일부터 금요일까지, 오전 9시에서 오후 5시 동안 근무하는 사업장의 직원들이 10.1.42.0/42 서브 네트워크를 사용하는 경우의 접근법을 보입니다.

  다음을 여러분의 /etc/squid/squid.conf 파일의 ACL 영역의 **가장 아래**에 추가 합니다:

  acl biz_network src 10.1.42.0/24 acl biz_hours time M T W T F 9:00-17:00

  그런 다음, /etc/squid/squid.conf 파일의 http_access 영역의 **가장 위**에 다음을 추가 합니다:

  http_access allow biz_network biz_hours

  /etc/squid/squid.conf 파일에 변경을 만든 후에는, 그 파일을 저장하고 변경의 효과를 가지도록 터미널 프롬프트에서 다음의 명령을 입력하여 squid 서버 프로그램을 재 시작 합니다:

```
sudo /etc/init.d/squid restart
```

11.3. 참조

Squid 웹사이트 [http://www.squid-cache.org/]

12. 버전 관리 시스템

버전 관리는 정보의 변경을 관리하는 예술적인 작업 입니다. 그것은, 소프트웨어에 적은 변경을 만들고 다음 날에 그 변경을 취소하는 데 그들의 시간을 사용하는 전형적인 프로그래머들을 위하여 오랫 동안 아주 중요한 도구이어 왔습니다. 그러나, 버전 관리의 유용함은 소프트웨어 개발 세상의 범주를 훨씬 넘어 확장되고 있습니다. 어느 곳에서든 여러분은 사람들이 종종 정보를 변경하는 것을 컴퓨터를 사용하여 관리하는 것을 볼 수 있을 겁니다. 거기에 버전 관리를 위한 필요가 있습니다.

12.1. Subversion

Subversion 은 오픈소스 버전 관리 시스템 입니다. Subversion을 사용하여, 소스 파일과 문서의 이력을 기록할 수 있습니다. 그것은 시간에 걸쳐 파일과 디렉토리를 관리 합니다. 파일의 트리는 중앙 저장소로 놓여집니다. 저장소는 보통의 파일 서버와 매우 비슷하지만, 이제껏 만들어진 파일과 디렉토리의 모든 변경을 기억하고 있습니다.

12.1.1. 설치

HTTP 프로토콜을 사용하여 Subversion 저장소를 접근하기 위해, 여러분은 반드시 웹 서버를 설치하고 설정하여야 합니다. 아파치2는 Subversion과 잘 동작하는 것이 증명 되었습니다. 아파치2를 설치하고 설정하기 위하여 아파치2 영역 내의 HTTP 부 영역을 참조 하십시오. HTTPS 프로토콜을 사용하여 Subversion 저장소에 접근하려면, 반드시 여러분의 아파치2 웹 서버 내에 디지털 인증서를 설치하고 설정하여야 합니다. 디지털 인증서를 설치하고 설정하기 위하여 아파치2 영역 내의 HTTPS 부 영역을 참조 하십시오.

Subversion은 설치하려면, 터미널 프롬프트에서 다음의 명령을 실행 합니다:

```
sudo apt-get install subversion libapache2-svn
```

12.1.2. 서버 설정

이 절차는 위에서 언급된 패키지가 여러분의 시스템에 설치된 것으로 간주 합니다. 이 영역은 Subversion 저장소를 어떻게 만들고 프로젝트를 접근할 수 있는지를 설명 합니다.

12.1.2.1. Subversion 저장소 만들기

Subversion 저장소는 터미널 프롬프트에서 다음의 명령을 사용하여 만들 수 있습니다:

```
svnadmin create /path/to/repos/project
```

12.1.3. 접근 방법

Subversion 저장소는 로컬 디스크 상의 많은 다른 방법들 또는 다양한 네트워크 프로토콜을 통하여 접근(체크아웃)될 수 있습니다. 그러나, 하나의 저장소 위치는 언제나 URL 입니다. 다음 표는 어떻게 다른 URL 체계를 사용가능한 접근 방법으로 대치할 수 있는지를 기술 합니다.

표 4.1. 접근 방법

Schema	Access Method
file://	직접 저장소 접근 (로컬 디스크 상)
http://	Subversion을 인식하는 아파치2 웹 서버로 WebDAV를 통하여 접근
https://	http://와 같으나, SSL 암호화를 사용
svn://	svn를 사용하는 서버로 Subversion 프토토콜을 통하여 접근
svn+ssh://	svn://와 같으나, SSH 터널을 사용

이 영역에서는, 모든 접근 방법을 위하여 Subversion을 어떻게 설정하는 지를 보일 겁니다. 여기서는, 그 기초를 다룹니다. 좀 더 고급의 사용예에 대한 자세한 것은, svn 책 [http://svnbook.red-bean.com/]을 참고 하십시오.

12.1.3.1. 직접 저장소 접근 (file://)

이것은 모든 접근 방법 중의 가장 단순한 것 입니다. 이것은 Subversion 서버의 프로세스가 실행 중인 것을 필요로 하지 않습니다. 이 접근 방법은 같은 기계에서 Subversion을 접근할 때 사용 됩니다. 명령의 문법은, 터미널 프롬프트에서, 다음과 같이 입력 합니다:

```
svn co file:///path/to/repos/project
```

또는

```
svn co file://localhost/path/to/repos/project
```

> 만약 호스트 이름을 지정하지 않았다면, 세 개의 슬래쉬 (///)가 있습니다. 두 개는 프로토콜을 위한 것이고 (이 경우는 file), 마지막 하나는 경로를 나타내는 슬래쉬 입니다. 만약 호스트 이름을 지정한다면, 반드시 두 개의 슬래쉬(//)를 사용 합니다.

저장소의 접근 권한은 파일 시스템의 접근 권한에 의존 합니다. 만약 사용자가 읽기/쓰기 접근 권한을 가지고 있다면, 그 저장소에서 체크아웃을 하고 저장소로 커밋을 할 수 있습니다.

12.1.3.2. WebDAV 프로토콜을 사용하여 접근 (http://)

WebDAV 프로토콜을 사용하여 Subversion 저장소를 접근하기 위하여, 여러분은 반드시 아파치2 웹 서버를 설정하여야 합니다. 반드시 다음의 예를 여러분의 /etc/apache2/apache2.conf 파일에 추가 합니다:

```
<Location /svn>
DAV svn
SVNPath /path/to/repos
AuthType Basic
AuthName "Your repository name"
AuthUserFile /etc/subversion/passwd
<LimitExcept GET PROPFIND OPTIONS REPORT>
Require valid-user
</LimitExcept>
</Location>
```

다음에, /etc/subversion/passwd 파일을 반드시 만듭니다. 이 파일은 사용자 인증의 상세한 것을 가집니다. 예를 들어 사용자를 추가하는 것과 같이 항목을 추가하려면, 터미널 프롬프트에서 다음의 명령을 사용할 수 있습니다:

```
htpasswd2 /etc/subversion/passwd user_name
```

이 명령은 여러분이 암호를 입력하도록 물어 봅니다. 암호를 입력한 후, 그 사용자는 더해 집니다. 이제, 다음의 명령을 실행하여 저장소를 접근할 수 있습니다:

```
svn co http://servername/svn
```

암호는 일반 텍스트로 전송 됩니다. 만약 암호를 훔쳐보는 것을 걱정한다면, SSL 암호화를 사용할 것을 권고 합니다. 자세한 것은, 다음 부분을 참고 하십시오.

12.1.3.3. SSL 암호화와 함께 WebDAV 프로토콜을 사용하여 접근 (https://)

SSL 암호화와 함께 WebDAV 프로토콜(https://)을 사용하여 Subversion 저장소를 접근하는 것은 http://를 사용하는 것과 비슷하나 차이점은, 여러분은 반드시 아파치2 웹 서버에 디지털 인증서를 설치하고 설정하여야 합니다.

디지털 인증서는 Verisign과 같은 인증 기관에서 발행된 것을 설치할 수 있습니다. 다른 방법으로는, 여러분이 스스로 사인한 인증서를 설치할 수도 있습니다.

이 절차는 여러분의 아파치2 웹 서버에 디지털 인증서를 설치하고 설정하였다고 간주 합니다. 이제, Subversion 저장소를 접근하기 위하여, 윗 부분을 참조 하십시오! 접근 방법은 정확히 똑같고, 단지 프로토콜이 다릅니다. 여러분은 반드시 Subversion 저장소를 접근하기 위하여 https://를 사용하여야 합니다.

12.1.3.4. Subversion 프로토콜을 사용하여 접근 (svn://)

Subversion 저장소가 만들어진 후, 여러분은 접근 조종을 설정할 수 있습니다. 접근 조종을 설정하기 위하여 /path/to/repos/project/conf/svnserve.conf 파일을 편집할 수

있습니다. 예를 들어, 인증을 설정하는 것은, 그 설정 파일의 다음 줄들을 주석 해제 합니다:

```
# [general]
# password-db = passwd
```

위의 줄들을 주석 해제한 후에, passwd 파일에 사용자 목록을 관리할 수 있습니다. 그러므로, 같은 디렉토리 내의 passwd 파일을 편집하기 위하여 열고 새로운 사용자를 추가 합니다. 문법은 다음과 같습니다:

```
username = password
```

더 자세한 것은, 그 파일을 참조 하십시오.

이제, svn:// 프로토콜을 사용하여, 같은 기계 또는 다른 기계에 있는 Subversion 저장소를 접근하고, svnserve 명령을 사용하여 svn 서버를 실행할 수 있습니다. 문법은 다음과 같습니다:

```
$ svnserve -d –foreground -r /path/to/repos
# -d – daemon mode
# –foreground – run in foreground (useful for debugging)
# -r – root of directory to serve

For more usage details, please refer to:
$ svnserve –help
```

이 명령이 수행된 후, Subversion은 기본 설정 포트 (3690)을 듣기 시작 합니다. 프로젝트 저장소를 접근하려면, 터미널 프롬프트에서 다음의 명령을 반드시 실행하여야 합니다:

```
svn co svn://hostname/project project –username user_name
```

서버 설정에 따라, 암호를 물어 봅니다. 인증이 된 후, Subversion 저장소에서 코드를 체크 아웃 합니다. 로컬 복사본과 프로젝트 저장소를 동기화 하는 것은, **update** 부 명령을 실행 합니다. 그 명령의 문법은, 다음과 같이 터미널 프롬프트에서 입력 합니다:

```
cd project_dir ; svn update
```

각각의 Subversion 부 명령을 사용하는 것에 대한 더 자세한 것은, 매뉴얼을 참조 하십시오. 예를 들어, co (checkout) 명령에 대한 것을 배우려면, 터미널 프롬프트에서 다음의 명령을 실행 합니다:

```
svn co help
```

12.1.3.5. SSL 암호화와 함께 Subversion 프로토콜을 사용하여 접근 (svn+ssh://)

설정과 서버 절차는 svn:// 접근 방법 내의 것과 같습니다. 자세한 것은, 위의 영역을 참조 하십시오. 이 절차는 여러분이 위의 절차를 따라왔고 svnserve 명령을 사용하여 Subversion 서버을 실행하였다고 간주 합니다.

또한 그 기계에 ssh 서버가 실행 중이고 들어오는 접속을 허용하는 중이라는 것도 가정 합니다. 확인을 하려면, ssh를 사용하여 그 기계에 로그인을 시도해 보십시오. 만약 로그인을 할 수 있으면, 모든 것은 완벽 합니다. 만약 로그인을 할 수 없다면, 더 진행하기 전에 그것을 먼저 고치십시오.

svn+ssh:// 프로토콜은 SSL 암호화와 함께 Subversion 저장소를 접근하기 위하여 사용 됩니다. 자료 전송은 이 방법을 사용하여 암호화 됩니다. 프로젝트 저장소를 접근하려면 (예를 들어 체크 아웃으로), 여러분은 반드시 다음의 명령 문법을 사용하여야 합니다:

```
svn co svn+ssh://hostname/var/svn/repos/project
```

이 접근 방법을 사용하여 Subversion 저장소를 접근하려면 반드시 완전한 경로명을 (/path/to/repos/project) 사용하여야 합니다.

서버 설정에 따라, 암호를 물어 봅니다. 반드시 ssh 통하여 로그인 할 때 사용하는 암호를 입력 합니다. 인증이 된 후, Subversion 저장소에서 코드를 체크 아웃 합니다.

12.2. CVS 서버

CVS는 버전 관리 시스템 입니다. 소스 파일의 이력을 기록하기 위하여 그것을 사용할 수 있습니다.

12.2.1. 설치

터미널 프롬프트에서, cvs 를 설치하기 위하여 다음의 명령을 입력 합니다:

```
sudo apt-get install cvs
```

cvs 를 설치한 후에, cvs 서버를 시작하고 중지하려면 xinetd 를 설치하여야 합니다. 프롬프트에서, xinetd 를 설치하기 위하여 다음의 명령을 입력 합니다:

```
sudo apt-get install xinetd
```

12.2.2. 설정

cvs 를 설치한 후에, 저장소는 자동적으로 초기화 됩니다. 기본 설정으로, 저장소는 /var/lib/cvs 디렉토리 밑에 위치 합니다. 이 경로를 변경하는 것은 다음의 명령을 사용할 수 있습니다:

```
cvs -d /your/new/cvs/repo init
```

초기 저장소가 만들어 진 후, CVS 서버를 시작하기 위하여 xinetd 를 설정할 수 있습니다. /etc/xinetd/cvspserver 파일에 다음 줄들을 복사 합니다.

```
service cvspserver
```

```
{
    port = 2401
    socket_type = stream
    protocol = tcp
    user = root
    wait = no
    type = UNLISTED
    server = /usr/bin/cvs
    server_args = -f –allow-root /var/lib/cvs pserver
    disable = no
}
```

만약 기본 지정된 저장소 (/var/lib/cvs) 디렉토리를 변경하였다면 그 저장소를 편집하는 것을 확신 하십시오.

xinetd 를 설정한 후에 다음의 명령을 실행하여 CVS 서버를 실행할 수 있습니다:

```
sudo /etc/init.d/xinetd start
```

다음의 명령을 수행하여 CVS 서버가 실행 중인 것을 확인할 수 있습니다:

```
sudo netstat -tap | grep cvs
```

이 명령을 실행할 때, 여러분은 다음 줄 또는 그와 유사한 것을 보아야 합니다:

```
tcp 0 0 *:cvspserver *:* LISTEN
```

이제 여기서 여러분은 사용자를 더하고, 새로운 프로젝트를 더하며, 그 CVS 서버를 관리하는 것을 계속할 수 있습니다.

CVS는 OS 설치와는 무관하게 사용자를 추가할 수 있습니다. 아마도 가장 쉬운 것은 CVS를 위하여 리눅스 사용자를 사용하는 것이지만, 이것은 가능한 보안의 문제를 가지고 있습니다. 자세한 것은 CVS 매뉴얼을 참조 하십시오.

12.2.3. 프로젝트 더하기

이 영역은 CVS 저장소로 어떻게 새로운 프로젝트를 추가하는 지에 대하여 설명 합니다. 디렉토리를 만들고 그 디렉토리로 필요한 문서와 소스 파일을 더합니다. 이제, CVS 저장소로 프로젝트를 추가하기 위하여 다음의 명령을 실행 합니다:

```
cd your/project
cvs import -d :pserver:username@hostname.com:/var/lib/cvs -m "Importing my project to CVS repository" . new_project
```

여러분은 CVS 루트 디렉토리를 저장하기 위하여 CVSROOT 환경 변수를 사용할 수 있습니다. CVSROOT 환경 변수가 export 되면, 위의 cvs 명령에 -d 옵션을 주는 것을 피할 수 있습니다.

new_project 스트링은 벤더 태그이고, start 는 릴리스 태그 입니다. 그것들은 이 문맥에서는 아무 목적도 가지지 않지만, CVS가 그것들을 요구하므로 반드시 나타내야 합니다.

새로운 프로젝트를 추가할 때, 여러분이 사용하는 CVS 사용자는 반드시 CVS 저장소 /var/lib/cvs) 의 쓰기 권한을 가져야 합니다. 기본 설정으로, src 그룹은 그 CVS 저장소로의 쓰기 권한을 가지고 있습니다. 그러므로, 여러분은 그 사용자를 이 그룹에 추가할 수 있고, 그런 후 그 사용자는 CVS 저장소 내의 프로젝트를 관리할 수 있습니다.

12.3. 참조

Subversion 홈 페이지 [http://subversion.tigris.org/]

Subversion 책 [http://svnbook.red-bean.com/]

CVS 매뉴얼 [http://ximbiot.com/cvs/manual/cvs-1.11.21/cvs_toc.html]

13. 데이타베이스

우분투는 두 가지 데이타베이스 서버를 제공 합니다. 그것들은:

- MySQL™
- PostgreSQL

메인 저장소에서 사용 가능 합니다. 이 영역은 이 데이타베이스 서버들을 어떻게 설치하고 설정하는 지를 설명 합니다.

13.1. MySQL

MySQL은 빠르고, 멀티쓰레드, 복수 사용자, 그리고 견고한 SQL 데이타베이스 서버 입니다. 이것은 대량의 소프트웨어 이행에 포함되는 것과 마찬가지로 중요한 임무와 부하가 많은 현업 시스템을 위하여 사용 됩니다.

13.1.1. 설치

MySQL을 설치하기 위하여, 터미널 프롬프트에서 다음 명령을 실행 합니다:

```
sudo apt-get install mysql-server mysql-client
```

설치가 마쳐진 후, MySQL 서버는 자동적으로 시작 됩니다. MySQL 서바가 실행 중인지를 점검하려면 터미널 프롬프트에서 다음의 명령을 실행할 수 있습니다:

```
sudo netstat -tap | grep mysql
```

이 명령을 실행할 때, 여러분은 다음 줄 또는 그와 유사한 것을 보아야 합니다:

```
tcp 0 0 localhost.localdomain:mysql *:* LISTEN -
```

만약 서버가 올바르게 실행 중이 아니라면, 그것을 시작하기 위하여 다음의 명령을 입력할 수 있습니다:

```
sudo /etc/init.d/mysql restart
```

13.1.2. 설정

기본 설정으로, 관리자의 암호는 지정되지 않았습니다. MySQL을 설치한 후, 첫 번째로 여러분이 반드시 해야하는 것은 MySQL 관리자의 암호를 설정하는 것 입니다. 이것을 하기 위하여, 다음의 명령을 실행 합니다:

```
sudo mysqladmin -u root password newrootsqlpassword
```

```
sudo mysqladmin -u root -h localhost password newrootsqlpassword
```

로그 파일, 포트 번호 등의 기본적인 값을 설정하기 위하여 /etc/mysql/my.cnf 파일을 편집할 수 있습니다. 더 자세한 것은 /etc/mysql/my.cnf 파일을 참조 하십시오.

13.2. PostgreSQL

PostgreSQL은 전통적인 상업용 데이타베이스 시스템의 기능에 차세대 DBMS 시스템에서 찾을 수 있는 개선을 포함하는 객체-관계형 데이타베이스 시스템 입니다.

13.2.1. 설치

PostgreSQL를 설치하기 위하여, 명령 프롬프트에서 다음의 명령을 실행 합니다:

```
sudo apt-get install postgresql
```

설치가 마쳐지면, 비록 기본 설정이 유용하기는 하지만, 여러분의 필요에 따라 PostgreSQL 서버를 설정할 수 있습니다.

13.2.2. 설정

기본 설정으로, TCP/IP를 통한 접속은 사용할 수 없습니다. PostgreSQL는 복수 클라이언트 인증 방법을 지원 합니다. 기본 설정으로, IDENT 인증 방법이 사용 됩니다. PostgreSQL 관리자 안내서 [http://www.postgresql.org/docs/8.1/static/admin.html]를 참조 하십시오.

다음의 논의는 여러분이 TCP/IP 접속을 사용하기를 원하고 클라이언트 인증을 위하여 MD5 방법을 사용한다고 가정 합니다. PostgreSQL 설정 파일은 /etc/postgresql/<version>/main 디렉토리 내에 저장 됩니다. 예를 들어, PostgreSQL 7.4를 설치한다면, 설정 파일은 /etc/postgresql/7.4/main 디렉토리 내에 저장 됩니다.

ident 인증을 설정하기 위하여, /etc/postgresql/7.4/main/pg_ident.conf 파일에 항목을 추가 합니다.

TCP/IP 접속을 사용하기 위하여, /etc/postgresql/7.4/main/postgresql.conf 파일을 편집 합니다.

#tcpip_socket = false 줄에 위치하고 그것을 tcpip_socket = true 로 변경 합니다. 만약 여러분이 무엇을 하는지를 알고 있다면, 모든 다른 파라미터들도 또한 편집할 수 있습니다! 자세한 것은, 그 설정 파일 또는 PostgreSQL 문서를 참조 하십시오.

기본 설정으로, 사용자 보증은 MD5 클라이언트 인증을 위하여 지정될 수 없습니다. 그러므로, 우선 trust 클라이언트 인증을 사용하도록 PostgreSQL 서버를 설정하고, 데이타베이스로 연결하고, 암호를 설정하고, MD5 클라이언트 인증을 사용하도록 설정을 바꾸는 것이 필요 합니다. trust 클라이언트 인증을 활성화 하려면, /etc/postgresql/7.4/main/pg_hba.conf 파일을 편집 합니다.

ident 와 MD5 클라이언트 인증을 사용하는 모든 있는 줄들을 주석 처리하고 다음 줄을 추가 합니다:

```
local all postgres trust sameuser
```

그런 후, PostgreSQL 서버를 시작하기 위하여 다음 명령을 실행 합니다:

```
sudo /etc/init.d/postgresql start
```

PostgreSQL 서버가 성공적으로 시작된 후, 기본 설정된 PostgreSQL 템플릿 데이타베이스에 접속하기 위하여 터미널 프롬프트에서 다음의 명령을 실행 합니다:

```
psql -U postgres -d template1
```

위의 명령은 사용자 postgres로써 PostgreSQL 데이타베이스 template1 로 접속 합니다. PostgreSQL 서버로 접속하면, 여러분은 SQL 프롬프트를 보게 됩니다. postgres 사용자의 암호를 설정하기 위하여 psql 프롬프트에서 다음의 SQL 명령을 실행할 수 있습니다.

```
template1=# ALTER USER postgres with encrypted password 'your_password';
```

암호를 설정한 후에, MD5 인증을 사용하기 위하여 /etc/postgresql/7.4/main/pg_hba.conf 파일을 편집 합니다:

최근에 추가된 trust 줄을 주석 처리하고 다음 줄을 추가 합니다:

```
local all postgres md5 sameuser
```

위의 설정은 어떠한 의미로도 완전하지 않습니다. 더 많은 파라미터를 설정하기 위해서는 PostgreSQL 관리자 안내서 [http://www.postgresql.org/docs/8.1/static/admin.html] 를 참조 하십시오.

14. 이메일 서비스

네트워크 또는 인터넷 상에서 한 사람에서 부터 다른 사람으로 이메일을 가지는 과정은 많은 시스템이 함께 동작하는 것과 관련 됩니다. 각각의 시스템은 과정이 동작하기 위하여 반드시 올바르게 설정되어야 합니다. 보내는 사람은 Mail User Agent (MUA) 또는 이메일 클라이언트를 사용하고, 메세지를 보내기 위하여 하나 또는 여러 개의 Mail Transfer Agents (MTA) 를 통과하며, 마지막으로, 받는 사람의 메일박스에 배달을 하기 위하여 Mail Delivery Agent (MDA) 를 거치게 됩니다. 그리고, 메일은 보통 POP3 또는 IMAP 서버를 통하여 받는 사람의 이메일 클라이언트에 의해 읽혀지게 됩니다.

14.1. Postfix

Postfix 는 우분투에서 기본 설정된 Mail Transfer Agent (MTA) 입니다. 이것은 빠르고 관리와 보안을 하기가 수월 합니다. 그리고 MTA 인 sendmail 과 호환이 됩니다. 이 영역은 postfix 를 어떻게 설치하고 설정하는 지를 설명 합니다. 또한 그것을 보안 연결을 (안전하게 이메일을 보내기 위한) 사용하는 SMTP 서버로서 어떻게 만드는 지를 설명 합니다.

14.1.1. 설치

postfix를 SMTP-AUTH와 Transport Layer Security (TLS)과 함께 설치하기 위하여, 다음의 명령을 실행 합니다:

```
sudo apt-get install postfix
```

설치 과정 중에 물어보는 질문에 간단히 엔터키를 누르고, 설정은 다음 단계에서 보다 자세히 마쳐지게 됩니다.

14.1.2. 기본적인 설정

postfix 를 설정하기 위하여, 다음 명령을 실행 합니다: screen> **sudo dpkg-reconfigure postfix**

mail.example.com 는 여러분의 메일 서버 호스트 이름으로 대체 합니다.

14.1.3. SMTP 인증

다음 단계는 SMTP AUTH를 위하여 SASL을 사용하도록 postfix를 설정하는 것 입니다. 설정 파일을 직접 편집하는 대신에, 모든 postfix 파라미터를 설정하기 위하여 **postconf** 명령을 사용할 수 있습니다. 설정 파라미터들은 /etc/postfix/main.cf 파일 내에 저장 됩니다. 나중에 만약 여러분이 특정 파라미터를 재 설정하기를 원한다면, 그 명령을 실행하거나 또는 그 파일을 수작업으로 변경할 수 있습니다.

1. SASL을 사용하여 SMTP AUTH를 (saslauthd) 하도록 Postfix를 설정하려면:

```
postconf -e 'smtpd_sasl_local_domain ='
postconf -e 'smtpd_sasl_auth_enable = yes'
postconf -e 'smtpd_sasl_security_options = noanonymous'
postconf -e 'broken_sasl_auth_clients = yes'
postconf -e 'smtpd_recipient_restrictions = permit_sasl_authenticated,permit_mynetworks,reject_unauth_destination'
postconf -e 'inet_interfaces = all'
echo 'pwcheck_method: saslauthd' >> /etc/postfix/sasl/smtpd.conf
echo 'mech_list: plain login' >> /etc/postfix/sasl/smtpd.conf
```

2. 다음은, TLS를 위하여 디지털 인증서를 설정 합니다. 질문을 물어볼 때, 지시를 따르고 적절하게 대답을 합니다.

```
openssl genrsa -des3 -rand /etc/hosts -out smtpd.key 1024
chmod 600 smtpd.key
openssl req -new -key smtpd.key -out smtpd.csr
openssl x509 -req -days 3650 -in smtpd.csr -signkey smtpd.key -out smtpd.crt
openssl rsa -in smtpd.key -out smtpd.key.unencrypted
mv -f smtpd.key.unencrypted smtpd.key
openssl req -new -x509 -extensions v3_ca -keyout cakey.pem -out cacert.pem -days 3650
mv smtpd.key /etc/ssl/private/
mv smtpd.crt /etc/ssl/certs/
mv cakey.pem /etc/ssl/private/
mv cacert.pem /etc/ssl/certs/
```

여러분은 인증 기관에서 디지털 인증서를 가질 수 있습니다. 다른 방법으로는, 스스로 인증서를 만들 수 있습니다. 더 자세한 것은 10.3.4절. “자가-사인 인증서 만들기” [55] 를 참조 하십시오.

3. 들어오는 이메일과 나가는 이메일 모두에 TLS 암호화를 적용하도록 Postfix를 설정하려면:

```
postconf -e 'smtpd_tls_auth_only = no'
postconf -e 'smtp_use_tls = yes'
postconf -e 'smtpd_use_tls = yes'
postconf -e 'smtp_tls_note_starttls_offer = yes'
postconf -e 'smtpd_tls_key_file = /etc/ssl/private/smtpd.key'
postconf -e 'smtpd_tls_cert_file = /etc/ssl/certs/smtpd.crt'
postconf -e 'smtpd_tls_CAfile = /etc/ssl/certs/cacert.pem'
postconf -e 'smtpd_tls_loglevel = 1'
postconf -e 'smtpd_tls_received_header = yes'
postconf -e 'smtpd_tls_session_cache_timeout = 3600s'
postconf -e 'tls_random_source = dev:/dev/urandom'
postconf -e 'myhostname = mail.example.com'
```

명령을 모두 실행하고 나면 postfix를 위한 SMTP AUTH의 설정이 모두 끝납니다. postfix에서 이어서 TLS에서 사용할 인증서를 직접 서명하여 설정합니다.

이때 /etc/postfix/main.cf와 this [../sample/postfix_configuration]이 같아보여야 합니다.

Postfix의 초기 설정이 이제 끝났습니다. Postfix 데몬을 시작하려면

```
sudo /etc/init.d/postfix start
```

을 실행하십시오. 이제 postfix 데몬이 무사히 설치되었으며, 설정이 끝나고 이제 실행중입니다. Postfix는 RFC2554 [ftp://ftp.isi.edu/in-notes/rfc2554.txt]에서 정의한 SMTP AUTH를 지원하며, SASL [ftp://ftp.isi.edu/in-notes/rfc2222.txt]를 따르고 있습니다. 하지만 SMTP를 사용기 위해서는 SASL 인증도 설정해야 합니다.

14.1.4. SASL 설정하기

SASL를 통한 SMTP AUTH 기능을 사용하기 위해서는 application>libsasl2

SASL를 제대로 사용하기 위해서는 수정해야 할 것이 몇 가지 있습니다. Postfix는 /var/spool/postfix 내에 chroot된 상태로 동작하기 때문에, SASL 역시 그 chroot된 환경 내에서 동작할 수 있도록 설정해야합니다(/var/run/saslauthd 대신에 /var/spool/postfix/var/run/saslauthd가 됩니다). 다음 명령을 입력하십시오:

```
mkdir -p /var/spool/postfix/var/run/saslauthd
rm -rf /var/run/saslauthd
```

saslauthd을 작동시키려면, /etc/default/saslauthd 을 편집하기 위하여 열고, START 변수를 변경하거나 추가 합니다. saslauthd 이 가짜 root 환경에서 실행되도록 설정하기 위해서는, PWDIR, PIDFILE과 PARAMS 변수를 더합니다. 마지막으로, MECHANISMS 변수를 여러분이 좋아하는 곳으로 설정 합니다. 그 파일을 다음과 비슷하게 보일 겁니다:

```
# This needs to be uncommented before saslauthd will be run
# automatically
START=yes

PWDIR="/var/spool/postfix/var/run/saslauthd"
PARAMS="-m ${PWDIR}"
PIDFILE="${PWDIR}/saslauthd.pid"

# You must specify the authentication mechanisms you wish to use.
# This defaults to "pam" for PAM support, but may also include
# "shadow" or "sasldb", like this:
# MECHANISMS="pam shadow"

MECHANISMS="pam"
```

만약 여러분이 좋아한다면, **shadow**를 **pam** 대신에 사용할 수 있습니다. 이것은 MD5 해쉬된 암호 전송을 사용하고 완전하게 안전 합니다. 인증을 하기 위하여 필요한 사용자 이름과 암호는 여러분이 사용하는 서버 시스템의 사용자의 그것들이 됩니다.

다음은, /var/spool/portfix/var/run/saslauthd의 dpkg "state"를 업데이트 합니다. saslauthd init script는 적당한 접근 권한과 소유권을 가지고 없는 디렉토리를 만들기 위하여 이 설정을 사용 합니다:

```
dpkg-statoverride –force –update –add root sasl 755 /var/spool/postfix/var/run/saslauthd
```

14.1.5. 테스팅

SMTP AUTH 설정을 마쳤습니다. 이제는 그것을 시작하고 설정을 테스트할 시간 입니다. SASL 데몬을 시작하기 위하여 다음의 명령을 실행할 수 있습니다:

```
sudo /etc/init.d/saslauthd start
```

SMTP-AUTH과 TLS가 적절하게 동작하는 지를 보려면, 다음의 명령을 실행 합니다:

```
telnet mail.example.com 25
```

여러분이 postfix 메일 서버로 접속을 만들고 난 후,

```
ehlo mail.example.com
```

을 입력하고 만약 다음의 줄들을 다른 것과 보게 된다면, 모든 것은 완전하게 동작하는 것 입니다. **quit**를 입력하여 종료 하십시오.

```
250-STARTTLS
250-AUTH LOGIN PLAIN
250-AUTH=LOGIN PLAIN
250 8BITMIME
```

14.2. Exim4

Exim4는 인터넷에 연결된 유닉스 시스템 상에서 사용하도록 캠브리지 대학에서 개발한 또다른 Message Transfer Agent (MTA) 입니다. Exim은 sendmail 자리에 설치될 수 있고, 설정은 sendmail의 설정과는 아주 다릅니다.

14.2.1. 설치

exim4를 설치하기 위하여, 다음 명령을 실행 합니다:

```
sudo apt-get install exim4 exim4-base exim4-config
```

14.2.2. 설정

exim4를 설정하기 위하여, 다음 명령을 실행 합니다:

```
sudo dpkg-reconfigure exim4-config
```

사용자 인터페이스가 보여질 겁니다. 사용자 인터페이스는 여러분이 많은 파라미터를 설정할 수 있도록 합니다. 예를 들어, exim4 설정 파일은 여러 개의

파일들로 나누어 집니다. 만약 여러분이 그것들을 한 파일로 갖기를 원한다면 이 사용자 인터페이스에서 적절하게 설정할 수 있습니다.

여러분이 사용자 인터페이스에서 설정할 수 있는 모든 파라미터들은 /etc/exim4/update-exim4.conf.conf 파일에 저장 됩니다. 만약 재 설정하기를 원한다면, 설정 마법사를 재 실행하던지 또는 여러분이 선호하는 편집기를 사용하여 수작업으로 이 파일을 편집할 수 있습니다. 설정한 후, 주 설정 파일을 만들기 위하여 다음 명령을 실행할 수 있습니다:

```
sudo update-exim4.conf
```

주 설정 파일이 만들어지고 /var/lib/exim4/config.autogenerated로 저장 됩니다.

언제든, 여러분은 주 설정 파일, /var/lib/exim4/config.autogenerated을 수작업으로 편집하지 않습니다. 그것은 **update-exim4.conf**를 실행할 때마다 자동적으로 업데이트 됩니다.

exim4 데몬을 시작하기 위하여 다음 명령을 실행할 수 있습니다:

```
sudo /etc/init.d/exim4 start
```

TODO: 이 영역은 exim4와 함께 SMTP AUTH를 설정하는 것을 다룹니다.

14.3. Dovecot 서버

Dovecot 은 보안 우선을 염두에 두고 쓰여진 Mail Delivery Agent 입니다. 이것은 mbox 와 Maildir 같은 주요 메일박스 형식을 지원 합니다. 이 영역은 imap 또는 pop3 서버로서 Dovecot을 어떻게 설정하는 지를 설명 합니다.

14.3.1. 설치

dovecot 설치하기 위하여, 명령 프롬프트에서 다음 명령을 실행 합니다:

```
sudo apt-get install dovecot-common dovecot-imapd dovecot-pop3d
```

14.3.2. 설정

dovecot을 설정하기 위하여, /etc/dovecot/dovecot.conf 파일을 편집할 수 있습니다. 여러분이 사용하고자 하는 프로토콜을 선택할 수 있고, 그것은 pop3, pop3s (pop3 secure), imap 그리고 imaps (imap secure)이 될 수 있습니다. 이 프로토콜에 대한 설명은 이 안내서의 범위 밖 입니다. 더 많은 정보는, wikipedia의 다음 글을, POP3 [http://en.wikipedia.org/wiki/POP3] 와 IMAP [http://en.wikipedia.org/wiki/Internet_Message_Access_Protocol], 참고 하십시오.

IMAPS와 POP3S는 접속할 때 SSL 암호화를 사용하므로 간단한 IMAP과 POP3 보다는 좀 더 안전 합니다. 이 프로토콜을 선택하였다면, /etc/dovecot/dovecot.conf 파일에 다음 줄을 수정 합니다:

```
protocols = pop3 pop3s imap imaps
```

그것은 dovecot이 시작될 때 그 프로토콜을 사용 가능하게 합니다. 다음은, /etc/dovecot/dovecot.conf 파일의 pop3 부분에 다음 줄을 추가 합니다:

```
pop3_uidl_format = %08Xu%08Xv
```

그 다음은, 사용할 메일박스를 선택 합니다. Dovecot은 **maildir** 과 **mbox** 형식을 지원 합니다. 그것은 가장 일반적으로 사용되는 메일박스 형식 입니다. 각각은 서로의 장점을 가지고 그에 대한 것은 dovecot 웹 사이트 [http://dovecot.org/doc/configuration.txt]에 논의되어 있습니다.

여러분의 메일박스 종류를 선택한 후, /etc/dovecot/dovecot.conf 파일을 편집하기 위하여 열고 다음 줄을 변경 합니다:

```
default_mail_env = maildir:~/Maildir # (for maildir)
또는
default_mail_env = mbox:~/mail:INBOX=/var/spool/mail/%u # (for mbox)
```

만약 설정한 것과 다르다면, 이 메일박스의 종류로 수신 메일을 전송하기 위한 여러분의 Mail Trasport Agent (MTA)를 설정하여야 합니다.

여러분이 dovecot을 설정한 후, 그것을 테스트하기 위하여 dovecot 데몬을 시작 하십시오:

```
sudo /etc/init.d/dovecot start
```

만약 imap 또는 pop3를 사용 가능하게 하였다면, **telnet localhost pop3** 또는 **telnet localhost imap2** 명령을 사용하여 로그인을 시도해 볼 수 있습니다. 다음과 같은 것을 본다면, 설치는 성공적으로 된 것 입니다:

```
bhuvan@rainbow:~$ telnet localhost pop3
Trying 127.0.0.1...
Connected to localhost.localdomain.
Escape character is '^]'.
+OK Dovecot ready.
```

14.3.3. Dovecot SSL 설정

SSL을 사용하도록 dovecot을 설정하기 위하여, /etc/dovecot/dovecot.conf 파일을 편집하기 위해 열고 다음 줄을 수정 합니다:

```
ssl_cert_file = /etc/ssl/certs/dovecot.pem
ssl_key_file = /etc/ssl/private/dovecot.pem
ssl_disable = no
disable_plaintext_auth = no
```

cert 와 **key** 파일은 설치될 때 dovecot에 의하여 자동적으로 만들어 집니다. 이 키는 사인되지 않았고 클라이언트에서 연결을 할 때 "bad signature" 에러를 주게 되는 것을 주의 하십시오. 이 것을 피하려면, 상업용 인증서를 사용할 수 있고, 또는 보다 낫게, 여러분 스스로의 SSL 인증서를 사용할 수 있습니다.

14.3.4. 이메일 서버를 위한 방화벽 설정

다른 컴퓨터에서 메일 서버를 접근하려면, 필요한 포트로 서버로의 접속을 허용하도록 방화벽을 반드시 설정해야만 합니다.

- IMAP - 143
- IMAPS - 993
- POP3 - 110
- POP3S - 995

14.4. Mailman

Mailman은 전자 우편 회의와 전자 소식 목록을 관리하기 위한 오픈소스 프로그램 입니다. 많은 오픈소스 메일링 리스트는 (모든 우분투 메일링 리스트 [http://lists.ubuntu.com]를 포함한) 메일링 리스트 소프트웨어로 Mailman을 사용 합니다. 이것은 강력하고 설치와 유지보수가 쉽습니다.

14.4.1. 설치

Mailman은 관리자와 사용자를 위한 웹 인터페이스를 제공 합니다. 그러므로, 그것은 mod_perl 지원을 하는 아파치를 필요로 합니다. Mailman은 이메일을 보내고 받기 위한 외부 메일 서버를 사용 합니다. 다음의 메일 서버와 완벽하게 동작 합니다:

- Postfix
- Exim
- Sendmail
- Qmail

우리는 어떻게 mailman, 아파치 웹 서버와 Exim 메일 서버를 설치하는지를 봅니다. 만약 여러분이 mailman을 다른 메일 서버와 함께 설치하기를 원한다면, 참조 영역을 참고 하십시오.

14.4.1.1. 아파치2

아파치2를 설치하는 것은 10.1절. “설치” [47] 을 참조 하십시오.

14.4.1.2. Exim4

Exim4를 설치하기 위하여 터미널 프롬프트에서 다음 명령을 실행 합니다:

```
sudo apt-get install exim4
sudo apt-get install exim4-base
sudo apt-get install exim4-config
```

exim4가 설치되면, 설정 파일들은 /etc/exim4 디렉토리에 저장 됩니다. 우분투에서는, 기본 설정으로, exim4 설정 파일은 여러 개의 파일들로 나누어 집니다. /etc/exim4/update-exim4.conf 파일 내의 다음 변수를 변경하는 것으로 이 동작을 바꿀 수 있습니다:

□dc_use_split_config='true'

14.4.1.3. Mailman

Mailman 을 설치하기 위하여, 터미널 프롬프트에서 다음 명령을 실행 합니다:

```
sudo apt-get install mailman
```

이것은 설치 파일을 /var/lib/mailman 디렉토리 내로 복사하고, /usr/lib/cgi-bin/mailman 디렉토리 내에 CGI 스크립트를 설치 합니다. list 리눅스 사용자를 만들고, list 리눅스 그룹도 만듭니다. mailman 프로세스는 이 사용자에 의하여 소유 됩니다.

14.4.2. 설정

이 영역에서는 여러분이 mailman, apache2, 그리고 exim4를 성공적으로 설치하였다고 가정 합니다. 이제 여러분은 단지 그것들을 설정할 필요가 있습니다.

14.4.2.1. 아파치2

아파치2가 설치되면, /etc/apache2/apache2.conf 파일에 다음의 줄들을 추가할 수 있습니다:

```
Alias /images/mailman/ "/usr/share/images/mailman/"
Alias /pipermail/ "/var/lib/mailman/archives/public/"
```

Mailman은 CGI 스크립트를 사용하기 위하여 아파치2를 이용 합니다. 메일맨 스크립트는 /usr/lib/cgi-bin/mailman 디렉토리에 설치 됩니다. 그러므로 그 메일맨 url은 http://hostname/cgi-bin/mailman/ 이 됩니다. 만약 변경하기를 원한다면, /etc/apache2/apache2.conf 파일에서 바꿀 수 있습니다.

14.4.2.2. Exim4

Exim4를 설치한 후, 터미널 프롬프트에서 다음 명령을 사용하여 Exim 서버를 시작할 수 있습니다:

```
sudo apt-get /etc/init.d/exim4 start
```

exim4와 함께 mailman이 동작하게 만들려면, exim4를 설정하는 것이 필요 합니다. 앞에 언급된 것과 같이, 기본 설정으로, exim4는 다른 종류의 복수 설정 파일들을 사용 합니다. 자세한 것은 Exim [http://www.exim.org] 웹 사이트를 참조 하십시오. mailman을 실행하기 위하여, 다음 설정 종류에 대한 새로운 설정 파일을 추가하여야 합니다:

□Main

□Transport

□Router

Exim은 모든 이 작은 설정 파일들을 정렬하여 주 설정 파일을 만듭니다. 그러므로, 이 설정 파일의 순서는 매우 중요 합니다.

14.4.2.3. Main

Main 종류에 속하는 모든 설정 파일들은 /etc/exim4/conf.d/main/ 디렉토리 내에 저장 됩니다. 04_exim4-config_mailman 이란 이름의 새 파일에 다음의 내용을 추가할 수 있습니다:

```
# start
# Home dir for your Mailman installation – aka Mailman's prefix
# directory.
# On Ubuntu this should be "/var/lib/mailman"
# This is normally the same as ~mailman
MM_HOME=/var/lib/mailman
#
# User and group for Mailman, should match your –with-mail-gid
# switch to Mailman's configure script. Value is normally "mailman"
MM_UID=list
MM_GID=list
#
# Domains that your lists are in - colon separated list
# you may wish to add these into local_domains as well
domainlist mm_domains=hostname.com
#
# -=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
#
# These values are derived from the ones above and should not need
# editing unless you have munged your mailman installation
#
# The path of the Mailman mail wrapper script
MM_WRAP=MM_HOME/mail/mailman
#
# The path of the list config file (used as a required file when
# verifying list addresses)
MM_LISTCHK=MM_HOME/lists/${lc::$local_part}/config.pck
# end
```

14.4.2.4. Transport

Transport 종류에 속하는 모든 설정 파일들은 /etc/exim4/conf.d/transport/ 디렉토리 내에 저장 됩니다. 40_exim4-config_mailman 이란 이름의 새 파일에 다음의 내용을 추가할 수 있습니다:

```
mailman_transport:
 driver = pipe
 command = MM_WRAP \
          '${if def:local_part_suffix \
              {${sg{$local_part_suffix}{-(\\w+)(\\+.*)?}{\$1}}} \
              {post}}' \
          $local_part
  current_directory = MM_HOME
  home_directory = MM_HOME
  user = MM_UID
  group = MM_GID
```

14.4.2.5. Router

Router 종류에 속하는 모든 설정 파일들은 /etc/exim4/conf.d/router/ 디렉토리 내에 저장 됩니다. 101_exim4-config_mailman 이란 이름의 새 파일에 다음의 내용을 추가할 수 있습니다:

```
mailman_router:
 driver = accept
 require_files = MM_HOME/lists/$local_part/config.pck
 local_part_suffix_optional
 local_part_suffix = -bounces : -bounces+* : \
                 -confirm+* : -join : -leave : \
                 -owner : -request : -admin
 transport = mailman_transport
```

Main과 Transport 설정 파일들의 순서는 어느 순서가 되도 무방 합니다. 그러나, Router 설정 파일의 순서는 반드시 똑같아야 합니다. 이 특정 파일은 200_exim4-config_primary 파일 이전에 반드시 나타나야 합니다. 이 두 설정 파일은 같은 종류의 정보를 가지고 있습니다. 첫 번째 파일이 우선권을 가집니다. 더 자세한 것은, 참조 영역을 참고 하십시오.

14.4.2.6. Mailman

mailman을 설치한 후, 다음 명령을 사용하여 그것을 실행할 수 있습니다:

```
sudo /etc/init.d/mailman start
```

mailman을 설치한 후, 기본 설정 메일링 리스트를 만들어야 합니다. 메일링 리스트를 만들기 위하여 다음 명령을 실행 합니다:

```
sudo /usr/sbin/newlist mailman

Enter the email address of the person running the list: bhuvan at ubuntu.com
Initial mailman password:
To finish creating your mailing list, you must edit your /etc/aliases (or
equivalent) file by adding the following lines, and possibly running the
`newaliases' program:

## mailman mailing list
mailman: "|/var/lib/mailman/mail/mailman post mailman"
mailman-admin: "|/var/lib/mailman/mail/mailman admin mailman"
mailman-bounces: "|/var/lib/mailman/mail/mailman bounces mailman"
mailman-confirm: "|/var/lib/mailman/mail/mailman confirm mailman"
mailman-join: "|/var/lib/mailman/mail/mailman join mailman"
mailman-leave: "|/var/lib/mailman/mail/mailman leave mailman"
mailman-owner: "|/var/lib/mailman/mail/mailman owner mailman"
mailman-request: "|/var/lib/mailman/mail/mailman request mailman"
mailman-subscribe: "|/var/lib/mailman/mail/mailman subscribe mailman"
mailman-unsubscribe: "|/var/lib/mailman/mail/mailman unsubscribe mailman"

Hit enter to notify mailman owner...

#
```

우리는 exim이 mailman에서 오는 모든 이메일을 인식하도록 설정 하였습니다. 그러므로, /etc/aliases 파일 내에 어떠한 새로운 항목을 만드는 것은 필수적이지 않습니다. 만약 여러분이 그 설정 파일에 어떠한 변경을 하였다면, 다음 영역을 계속하기 전에 그 서비스들을 재 시작하는 것을 확신 하십시오.

14.4.3. 관리

우리는 여러분이 기본 설정된 설치를 가졌다고 가정 합니다. mailman CGI 스크립트는 여전히 /usr/lib/cgi-bin/mailman/ 디렉토리 내에 있습니다. Mailman은 웹 기반 관리 기능을 제공 합니다. 이 페이지를 접근하기 위하여, 다음의 url을 여러분의 브라우저에서 사용 합니다:

http://hostname/cgi-bin/mailman/admin

기본 설정된 메일링 리스트, mailman 가 이 화면에 나타납니다. 그 메일링 리스트 이름을 클릭하면, 여러분의 인증 암호를 물어볼 것 입니다. 올바르게 암호를 입력하였다면, 여러분은 이 메일링 리스트의 관리자 설정 값을 변경할 수 있습니다. 명령행 유틸리티(**/usr/sbin/newlist**)를 사용하여 새로운 메일링 리스트를 만들 수 있습니다. 다른 방법으로, 웹 인터페이스를 사용하여 새로운 메일링 리스트를 만들 수 있습니다.

14.4.4. 사용자

Mailman은 사용자에게 웹 기반의 인터페이스를 제공 합니다. 이 페이지를 접근하려면, 다음 url을 여러분의 브라우저에서 사용 합니다:

http://hostname/cgi-bin/mailman/listinfo

기본 설정된 메일링 리스트, mailman 가 이 화면에 나타납니다. 그 메일링 리스트 이름을 클릭하면, 가입 양식을 보입니다. 여러분의 이메일 주소, 이름(선택사항) 그리고 암호를 가입하기 위하여 입력 합니다. 여러분에게 이메일 초대가 보내집니다. 가입하기 위하여 그 이메일의 절차를 따릅니다.

14.4.5. 참조

GNU Mailman - 설치 매뉴얼 [http://www.list.org/mailman-install/index.html]

하우투 - Exim 4와 Mailman 2.1을 함께 사용하기
[http://www.exim.org/howto/mailman21.html]

5장. 윈도우즈 네트워킹

컴퓨터 네트워크는 자주 다양한 시스템으로 구성되고, 전부 우분투 데스크탑과 서버 컴퓨터로 만들어진 네트워크를 운영하는 것은 분명히 즐겁겠지만, 다수의 네트워크 환경은 우분투와 Microsoft®Windows® 시스템이 조화롭게 함께 동작하는 것으로 반드시 이루어지게 됩니다. 우분투 서버 안내서의 이 부분에서는 윈도우즈 컴퓨터와 함께 네트워크 자원을 공유하기 위한 여러분의 우분투 서버를 설정하기 위하여 사용되는 원칙과 도구를 소개 합니다.

1. 소개

여러분의 우분투 시스템을 윈도우즈 클라이언트와 함께 성공적으로 네트워크를 구성하는 것은 윈도우즈 환경에 공통의 서비스를 제공하고 통합하는 것을 필요로 합니다. 이런 서비스는 자료와 그 네트워크에 관여된 컴퓨터와 사용자에 대한 정보의 공유를 도와주고, 다음의 세 가지 주요 기능의 분류로 구분되어 질 수 있습니다:

- **파일과 프린터 공유 서비스.** 서버 메세지 블럭 (SMB) 프로토콜을 사용하여 네트워크 상의 파일, 폴더, 볼륨 그리고 프린터의 공유를 돕습니다.
- **디렉토리 서비스.** Lightweight Directory Access Protocol (LDAP) 와 Microsoft Active Directory® 기술을 가지고 네트워크의 컴퓨터와 사용자에 대한 가상 정보를 공유 합니다.
- **인증과 접근.** 파일 접근 권한, 그룹 정책 그리고 Kerberos 인증 서비스와 같은 원칙과 기술을 사용하여 네트워크의 컴퓨터 또는 사용자의 식별을 입증하고 접근이 인증된 컴퓨터 또는 사용자의 정보를 결정합니다.

다행스럽게, 우분투 시스템은 윈도우즈 클라이언트에게 이 모든 편의를 제공하고 그들과 함께 네트워크 자원을 공유할 수 있습니다. 윈도우즈 네트워킹을 위하여 우분투 시스템이 포함하는 가장 중요한 소프트웨어의 하나는 SMB 서버 프로그램과 도구들을 모은 SAMBA suite 입니다. 우분투 서버 안내서의 이 부분에서는 서버 프로그램과 유틸리티의 SAMBA suite을 설치하고 제한적인 설정을 하는 소개를 간략히 하겠습니다. 추가하여, SAMBA에 대한 상세한 문서와 정보는 이 문서의 범위 밖에 있지만, SAMBA 웹사이트 [http://www.samba.org]에 있습니다.

2. SAMBA 설치

SAMBA 서버 프로그램을 설치하기 위해 명령어 프롬프트에서 다음의 명령을 입력합니다:

```
sudo apt-get install samba
```

3. SAMBA 설정

여러분은 기본 설정을 변경하거나 새로운 설정을 추가하기 위하여 /etc/samba/smb.conf 파일을 편집하는 것으로 SAMBA 서버를 설정할 수 있습니다. 각 설정에 대한 좀 더 많은 정보는 /etc/samba/smb.conf 파일의 설명에 있고, 또는 터미널 프롬프트에서 다음의 명령을 입력하여 /etc/samba/smb.conf 매뉴얼 페이지를 보셔도 됩니다:

```
man smb.conf
```

설정 파일을 편집하기 전에, 여러분은 원본 파일의 복사본을 만들고 쓰기에서 이것을 보호해야만 합니다. 그러므로 여러분은 참조할 수 있는 원래의 설정을 가지게 되고 필요에 따라 재 사용할 수 있습니다.

/etc/samba/smb.conf 파일 백업:

```
sudo cp /etc/samba/smb.conf /etc/samba/smb.conf.original
```

이제, /etc/samba/smb.conf 파일을 열어 변경 합니다.

3.1. 서버

파일과 프린터 공유 서버 프로그램인 SAMBA suite에 더하여, 우분투는 또한 실제 윈도우즈 서버에 의해 제공되는 기능과 비슷하게 윈도우즈 클라이언트에게 추가적인 네트워크 서버 기능을 제공하기 위하여 고안된 여타의 강력한 서버 프로그램을 포함하고 있습니다. 예를 들어, 우분투는 디렉토리 서비스를 통한 컴퓨터와 사용자와 같은 네트워크 자원의 중앙 관리, 사용자 식별의 편의, 그리고 인증 서비스를 통한 컴퓨터와 사용자의 인증을 제공 합니다.

다음 부분은 SAMBA와 경량 디렉토리 접근 프로토콜(LDAP), 그리고 Kerberos 인증 서버와 같은 지원 기술에 대하여 좀 더 자세하게 논의를 합니다. 여러분은 또한 윈도우즈 클라이언트와 서버를 가지고 네트워크 통합을 하는데 편리를 주는 SAMBA 설정 파일에서 사용할 수 있는 몇 개의 설정 지시에 대한 것도 배우게 될 것 입니다.

3.1.1. Active Directory

Active Directory는 Microsoft에 의한 디렉토리 서비스의 소유권이 있는 이행이고, 네트워크 자원과 사용자의 정보를 공유하기 위한 수단을 제공하는데 사용 됩니다. 이러한 정보의 중앙화된 소스를 제공하는 것에 추가하여, Active Directory는 또한 네트워크를 위한 중앙화된 인증 보안 권한으로도 동작을 합니다. Active Directory는 전통적으로 분리되고, 특화된 디렉토리 시스템에서 찾을 수 있는 능력을 단순화된 통합, 관리, 그리고 네트워크 자원의 보안으로 합칩니다. SAMBA 패키지는 하나의 윈도우즈 도메인 관리자에서 Active Directory 서비스를 사용하기 위하여 설정될 수 있습니다.

3.1.1.1. LDAP

LDAP 서버 프로그램은 윈도우즈 컴퓨터에게 Microsoft Active Directory 서비스와 매우 유사한 방법으로 디렉토리 서비스 기능을 제공 합니다. 이러한 서비스는 컴퓨터, 사용자, 그리고 네크워크에 참여하는 컴퓨터 또는 사용자 그룹의 식별과 관계를 관리하는 것과 이러한 자원을 설명, 위치, 그리고 관리하기 위한 일관된 수단을 제공하는 것을 포함 합니다. 여러분의 우분투 시스템을 위하여 자유롭게 사용할 수 있는 LDAP의 이행은 OpenLDAP 이라 불립니다. OpenLDAP 디렉토리 요청을 관리하고 우분투의 하나의 LDAP 서버에서 다른 것으로 디렉토리 자료를 그대로 전달하는 책임을 가지는 서버 데몬은, slapd와 slurpd 입니다. OpenLDAP은, SAMBA가 LDAP 지원과 함께 컴파일이 되는 한, 윈도우즈 도메인 관리자가 하는 것과 마찬가지 방법으로 파일, 프린트, 그리고 디렉토리 서비스를 제공하기 위하여 SAMBA와 결합하여 사용되어 질 수 있습니다.

3.1.1.2. Kerberos

Kerberos 인증 보안 시스템은, 중앙화된 서버가 Kerberos를 사용하는 다른 컴퓨터에 의한 인증을 받은 암호화된 인증 티켓을 허용하는 것으로, 컴퓨터와 사용자에게 인증을 제공하기 위하여 표준화된 서비스 입니다. Kerberos 인증의 혜택은 상호적인 인증, 위임적인 인증, 상호 이용성, 그리고 단순화된 신뢰 관리를 포함 합니다. 우분투의 Kerberos 인증과 Kerberos 데이타베이스 관리를 관리하는 주요 서버 데몬은 krb5kdc와 kadmin 입니다. SAMBA는 윈도우즈 도메인 관리자에 대항하여 컴퓨터와 사용자의 인증을 위한 하나의 장치로서 Kerberos를 사용할 수 있습니다. 그렇게 하려면, 우분투 시스템은 반드시 Kerberos를 설치하여야 하고, /etc/samba/smb.conf 는 적절한 realm 과 security 모드를 선택하도록 반드시 변경되어야 합니다. 예를 들어, /etc/samba/smb.conf 파일을 편집하기 위해 열고, 다음 값을 추가 합니다:

realm = DOMAIN_NAME

security = ADS

그 파일에 위의 값을 더하고, 그리고 그 파일을 저장 합니다.

위의 예의 DOMAIN_NAME 토큰은 여러분의 특정 윈도우즈 도메인을 가지고 대체하는 것을 확신 하십시오.

이 변경이 효과를 갖게 하려면 SAMBA 데몬을 재시작 하는 것이 필요 합니다. 터미널 프롬프트에서 다음 명령을 입력하는 것으로 SAMBA 데몬을 재시작 합니다:

```
sudo /etc/init.d/samba restart
```

3.1.2. 컴퓨터 계정

컴퓨터 계정은 네트워크에 참여하는 컴퓨터 시스템을 유일하게 식별하기 위하여 디렉토리 서비스에서 사용되고, 보안의 관점에서 사용자와 같은 방식으로 심지어

취급 됩니다. 컴퓨터 계정은 사용자 계정과 마찬가지로 암호를 가지고, 사용자 계정과 같은 방식으로 네트워크 자원에게 인증을 하기 위한 대상이 됩니다. 예를 들어, 만약 한 네트워크 사용자가, 올바른 컴퓨터 계정을 가지고 있지 않는 컴퓨터에서 특정 네트워크를 위한 올바른 계정을 가지고 네트워크 자원을 인증하기 위해 시도한다면, 네트워크에 강제된 정책에 따라, 인증되지 않은 컴퓨터에서 인증을 시도하는 것으로 여겨진다면 그 사용자는 그 자원에 접근하는 것이 거절될 수 있습니다.

컴퓨터 계정은 SAMBA 암호 파일에 추가되어질 수 있고, 그 암호 데이타베이스 내에 먼저 올바른 사용자 계정으로써 존재하는 추가된 컴퓨터의 이름으로 제공될 수도 있습니다. 컴퓨터 또는 기계 계정을 SAMBA 암호 파일에 추가하기 위한 문법은 다음과 같이 터미널 프롬프트에서 smbpasswd 명령을 사용 합니다:

```
sudo smbpasswd -a -m COMPUTER_NAME
```

위의 예에서 COMPUTER_NAME 토큰은 여러분이 추가하려는 기계 계정을 위한 특정 컴퓨터의 실제 이름으로 대체하는 것을 확인 하십시오.

3.1.3. 파일 접근 권한

파일 접근 권한은 컴퓨터 또는 사용자가 특정 디렉토리, 파일 또는 파일의 집합을 위하여 가지는 명시적 권리를 지정 합니다. 이러한 접근 권한은 /etc/samba/smb.conf 파일을 편집히고 지정된 파일 공유의 명시적 접근 권한을 규정하는 것으로 지정될 수 있습니다. 예를 들어, 여러분이 sourcedocs 이라 불리는 SAMBA 공유를 지정했고, planning 이라 알려진 사용자 그룹에게는 read-only 접근 권한을 주고 authors 라 불리는 그룹과 richard 라는 이름의 사용자에게는 그 공유에 쓰기를 허용하려고 한다면, /etc/samba/smb.conf 파일을 편집을 위하여 열고 다음의 항목을 [sourcedocs] 항목 아래에 추가 합니다:

read list = @planning

write list = @authors, richard

변경이 효과를 가지게 하기 위해 /etc/samba/smb.conf 를 저장 합니다.

또다른 가능한 접근 권한은 administrative 접근 권한을 특정한 공유 자원에 선언하는 것 입니다. 관리 접근 권한을 가진 사용자는 명시적으로 관리 접근 권한이 주어진 자원에 포함된 어떤 정보도 읽기, 쓰기, 또는 변경을 할 수 있습니다. 예를 들어, 만약 여러분이 사용자 melissa 에게 위의 예로 사용된 sourcedocs 공유의 관리 접근 권한을 주기를 원한다면, /etc/samba/smb.conf 파일을 편집하기 위해 열고 다음의 줄을 [sourcedocs] 항목 아래에 추가 합니다:

admin users = melissa

변경이 효과를 가지게 하기 위해 /etc/samba/smb.conf 를 저장 합니다.

3.2. 클라이언트

우분투는 클라이언트 프로그램과 SMB 프로토콜로 공유된 네트워크 자원을 접근하기 위한 능력을 가지고 있습니다. 예를 들어, smbclient 라 불리는 유틸리티는 파일 전송 프로토콜(FTP) 클라이언트와 유사한 방법으로, 원격의 공유된 파일 시스템을 사용하는 것을 허용 합니다. smbclient 를 사용하는 예는, bill 이란 원격의 윈도우즈 컴퓨터에 의해 제공되는 documents 라는 공유 폴더 자원을 사용하기 위하여, 여러분은 프롬프트에서 다음과 같은 명령을 입력 합니다:

```
smbclient //bill/documents -U <username>
```

여러분은 그런 후, -U 스위치 다음에 지정된 사용자 이름을 위한 암호 입력을 지시 받게되고, 성공적으로 인증이 되었을 때, 텍스트 모드의 FTP 클라이언트에서 사용하는 것과 비슷한 문법으로 파일을 조작하고 전송하기 위한 명령어를 입력하는 프롬프트를 보게 됩니다. smbclient 유틸리티에 대한 더 많은 정보는, 다음의 같이 명령하여 그 유틸리티의 매뉴얼 페이지를 읽습니다:

```
man smbclient
```

SMB 프로토콜을 사용하는 원격 네트워크 자원의 로컬(내 컴퓨터의 장치로 사용한다는 의미) 마운트(올리기)는 mount 명령을 사용하여 또한 가능 합니다. 예를 들어, development 라는 윈도우즈 서버 상의 project-code 라는 이름의 공유 폴더를 dlightman 이라는 사용자로써 여러분의 시스템의 /mnt/pcode (mount-point: 마운트 디렉토리)로 마운트 하기 위하여, 여러분은 프롬프트에서 다음 명령을 입력 합니다:

```
mount -t smbfs -o username=dlightman //development/project-code /mnt/pcode
```

여러분은 그런 후, 사용자 암호의 입력을 지시 받게되고, 성공적으로 인증이 된 후, 그 공유 폴더의 내용물은 마운트 명령의 마지막 인자로 지정한 그 마운트 디렉토리를 통해서 로컬 자원과 마찬가지로 사용을 할 수 있게 됩니다. 그 공유 자원의 연결을 끊는 것은, 여러분이 여타의 마운트된 파일 시스템에서 같이, 간단히 umount 명령을 사용 합니다. 예를 들어:

```
umount /mnt/pcode
```

3.2.1. 사용자 계정

사용자 계정은 특정 컴퓨터와 네트워크 자원을 사용하기 위한 몇 가지 인증의 등급을 가지는 컴퓨터 이용자를 지정 합니다. 전형적으로, 네트워크 환경에서는, 사용자 계정은 각 이용자에게 허용된 컴퓨터 또는 네트워크를 접근하기 위하여 제공되어지고, 사용자 계정이 가지는 명시적인 권한을 지정한 정책과 접근 권한이

지정되는 곳 입니다. 여러분의 우분투 시스템을 위한 SAMBA 네트워크 사용자를 지정하려면, smbpasswd 명령을 사용 합니다. 사용자 이름 jseinfeld 를 여러분의 우분투 시스템에 SAMBA 사용자로 추가하는 예는, 프롬프트웨서 이 명령을 입력 합니다:

```
smbpasswd -a jseinfeld
```

그런 다음 smbpasswd 프로그램은 여러분이 그 사용자를 위해 암호를 입력할 수 있도록 프롬프트를 보일 겁니다:

```
New SMB password:
```

그 사용자를 위해 지정하고 싶은 암호를 입력하고, smbpasswd 프로그램은 여러분이 그 암호를 확인하도록 다시 물을 것 입니다:

```
Retype new SMB password:
```

암호를 확인하고, smbpasswd 프로그램은 SAMBA 암호 파일에 그 사용자를 위한 항목을 추가 합니다.

3.2.2. 그룹

그룹은 특정 네트워크 자원을 접근하는 공통적인 등급을 가지는 컴퓨터 또는 사용자의 집합을 지정하고 그러한 네트워크 자원으로 접근하는 것을 관리하는 선별 정도의 등급을 제공 합니다. 예를 들어, 그룹 qa 가 지정되었고 사용자 freda, danika, 그리고 rob 을 포함하고 있고, 두 번째 그룹 support 가 지정되었고 사용자 danika, jeremy, 그리고 vincent 로 구성된다면, 특정 네트워크 자원은 qa 그룹에 의해 접근되는 것을 허용하기 위하여 설정될 수 있고 그 결과로 freda, danika, rob은 접근이 허용되지만 jeremy 또는 vincent는 접근을 할 수 없게 됩니다. 사용자 danika 는 qa 와 support 그룹 양쪽 모두에 속하므로, 그녀는 양쪽 그룹에 의한 접근을 위하여 설정되는 자원을 사용할 수 있게되고, 모든 다른 사용자들은 그들이 속하는 그룹에게 명시적으로 허용한 자원만을 사용하게 됩니다.

SAMBA 설정 파일 /etc/samba/smb.conf 내에 그룹을 지정할 때 인식되는 문법은 그룹 이름 앞에 "@" 심벌을 가지는 것입니다. 예를 들어, 만약 여러분이 /etc/samba/smb.conf 의 특정 영역에 sysadmin 이란 이름의 그룹을 지정하기를 원한다면, 그 그룹의 이름을 **@sysadmin** 로 입력하는 것으로 그렇게 합니다.

3.2.3. 그룹 정책

그룹 정책은 도메인 또는 Workgroup 컴퓨터 계정이 속하는 것과 여타의 SAMBA 서버를 위한 전체 설정값과 관련하는 특정 SAMBA 설정 값을 지정 합니다. 예를 들어, 만약 SAMBA 서버가 LEVELONE 이라 불리는 윈도우즈 컴퓨터의 Workgroup에 속한다면, /etc/samba/smb.conf 는 다음과 같이 그에 대한 것을 적정하게 변경하는 것으로 편집될 수 있습니다:

workgroup = LEVELONE

파일을 저장하고 변경의 효과를 가지기 위하여 SAMBA 데몬을 재시작 합니다.

다른 중요한 전체 정책 설정값은 여러분의 우분투 시스템을 윈도우즈 기반의 네트워크 상의 다른 기계에 알리는 NETBIOS 서버 이름을 지정하는 server string 을 포함 합니다. 이것은 윈도우즈 클라이언트와 SMB 프로토콜을 가지고 네트워크를 열람할 능력이 있는 다른 컴퓨터들에 의하여 인식되는 여러분의 우분투 시스템 이름입니다. 추가하여, 여러분은 /etc/samba/smb.conf 파일 내에 log file 지시자를 사용하여 SAMBA 서버의 로그 파일의 이름과 위치를 지정할 수 있습니다.

전체 그룹 정책을 운영하는 몇 가지 추가적인 지시자들은 모든 공유된 자원의 전체적인 특징의 명세를 포함 합니다. 예를 들어, /etc/samba/smb.conf 파일의 [global] 제목 아래의 특정 지시자를 놓는 것은 특정 공유 자원의 제목 아래에 이를 덮어쓰기 위한 지시자를 위치시키지 않는 한 모든 공유 자원에게 영향을 미치게 됩니다. 여러분은 browseable 지시자를 놓는 것으로 네트워크 상의 모든 클라이언트들에 의해 열람될 수 있는 모든 공유를 지정할 수 있고, 그 지시자는 /etc/samba/smb.conf 파일 내에 [global] 아래, Boolean 인수(yes 또는 no)를 가집니다. 그것은, 여러분이 그 파일을 편집하기 위하여 열고 그 줄을 추가 합니다:

browseable = true

/etc/samba/smb.conf 의 [global] 영역 아래에, 그러면 SAMBA를 통하여 여러분의 우분투 시스템에 의해 제공되는 모든 공유는 모든 허가된 클라이언트에 의하여 열람되어질 수 있습니다. 만약 특정한 공유가 browseable = false 지시자를 포함한다면, 그 전체 지시자는 덮어쓰여 집니다 - 즉, 특정한 공유에 지정된 것이 영향을 가집니다.

다른 예제들도 비슷한 방식으로 작동을 하게 되고, public 과 writeable 지시자가 그 예가 됩니다. public 지시자는 Boolean 값을 갖고 특정 공유 자원이 모든 클라이언트 또는 허가된 것에만 보여지는 것의 여부를 결정 합니다. writeable 지시자도 또한 Boolean 값을 취하고 특정 공유 자원이 어떤 또는 모든 네트워크 클라이언트에 의해 쓰여지는 것의 여부를 지정 합니다.

부록 A. Creative Commons by Attribution-ShareAlike 2.0

CREATIVE COMMONS CORPORATION IS NOT A LAW FIRM AND DOES NOT PROVIDE LEGAL SERVICES. DISTRIBUTION OF THIS LICENSE DOES NOT CREATE AN ATTORNEY-CLIENT RELATIONSHIP. CREATIVE COMMONS PROVIDES THIS INFORMATION ON AN "AS-IS" BASIS. CREATIVE COMMONS MAKES NO WARRANTIES REGARDING THE INFORMATION PROVIDED, AND DISCLAIMS LIABILITY FOR DAMAGES RESULTING FROM ITS USE.

License

THE WORK (AS DEFINED BELOW) IS PROVIDED UNDER THE TERMS OF THIS CREATIVE COMMONS PUBLIC LICENSE ("CCPL" OR "LICENSE"). THE WORK IS PROTECTED BY COPYRIGHT AND/OR OTHER APPLICABLE LAW. ANY USE OF THE WORK OTHER THAN AS AUTHORIZED UNDER THIS LICENSE OR COPYRIGHT LAW IS PROHIBITED.

BY EXERCISING ANY RIGHTS TO THE WORK PROVIDED HERE, YOU ACCEPT AND AGREE TO BE BOUND BY THE TERMS OF THIS LICENSE. THE LICENSOR GRANTS YOU THE RIGHTS CONTAINED HERE IN CONSIDERATION OF YOUR ACCEPTANCE OF SUCH TERMS AND CONDITIONS.

1. **Definitions.**
   a. **"Collective Work"** means a work, such as a periodical issue, anthology or encyclopedia, in which the Work in its entirety in unmodified form, along with a number of other contributions, constituting separate and independent works in themselves, are assembled into a collective whole. A work that constitutes a Collective Work will not be considered a Derivative Work (as defined below) for the purposes of this License.
   b. **"Derivative Work"** means a work based upon the Work or upon the Work and other pre-existing works, such as a translation, musical arrangement, dramatization, fictionalization, motion picture version, sound recording, art reproduction, abridgment, condensation, or any other form in which the Work may be recast, transformed, or adapted, except that a work that constitutes a Collective Work will not be considered a Derivative Work for the purpose of this License. For the avoidance of doubt, where the Work is a musical composition or sound recording, the synchronization of the Work in timed-relation with a moving image ("synching") will be considered a Derivative Work for the purpose of this License.

c. **"Licensor"** means the individual or entity that offers the Work under the terms of this License.

d. **"Original Author"** means the individual or entity who created the Work.

e. **"Work"** means the copyrightable work of authorship offered under the terms of this License.

f. **"You"** means an individual or entity exercising rights under this License who has not previously violated the terms of this License with respect to the Work, or who has received express permission from the Licensor to exercise rights under this License despite a previous violation.

g. **"License Elements"** means the following high-level license attributes as selected by Licensor and indicated in the title of this License: Attribution, ShareAlike.

2. **Fair Use Rights.** Nothing in this license is intended to reduce, limit, or restrict any rights arising from fair use, first sale or other limitations on the exclusive rights of the copyright owner under copyright law or other applicable laws.

3. **License Grant.** Subject to the terms and conditions of this License, Licensor hereby grants You a worldwide, royalty-free, non-exclusive, perpetual (for the duration of the applicable copyright) license to exercise the rights in the Work as stated below:

   a. to reproduce the Work, to incorporate the Work into one or more Collective Works, and to reproduce the Work as incorporated in the Collective Works;

   b. to create and reproduce Derivative Works;

   c. to distribute copies or phonorecords of, display publicly, perform publicly, and perform publicly by means of a digital audio transmission the Work including as incorporated in Collective Works;

   d. to distribute copies or phonorecords of, display publicly, perform publicly, and perform publicly by means of a digital audio transmission Derivative Works.

   e. For the avoidance of doubt, where the work is a musical composition:

      i. **"Performance Royalties Under Blanket Licenses."** Licensor waives the exclusive right to collect, whether individually or via a performance rights society (e.g. ASCAP, BMI, SESAC), royalties for the public performance or public digital performance (e.g. webcast) of the Work.

      ii. **"Mechanical Rights and Statutory Royalties."** Licensor waives the exclusive right to collect, whether individually or via a music rights society or designated agent (e.g. Harry Fox Agency), royalties for any phonorecord You create from the Work ("cover version") and distribute, subject to the compulsory license created by 17 USC Section 115 of the US Copyright Act (or the equivalent in other jurisdictions).

f. **"Webcasting Rights and Statutory Royalties."** For the avoidance of doubt, where the Work is a sound recording, Licensor waives the exclusive right to collect, whether individually or via a performance-rights society (e.g. SoundExchange), royalties for the public digital performance (e.g. webcast) of the Work, subject to the compulsory license created by 17 USC Section 114 of the US Copyright Act (or the equivalent in other jurisdictions).

The above rights may be exercised in all media and formats whether now known or hereafter devised. The above rights include the right to make such modifications as are technically necessary to exercise the rights in other media and formats. All rights not expressly granted by Licensor are hereby reserved.

4. **Restrictions.** The license granted in Section 3 above is expressly made subject to and limited by the following restrictions:

   a. You may distribute, publicly display, publicly perform, or publicly digitally perform the Work only under the terms of this License, and You must include a copy of, or the Uniform Resource Identifier for, this License with every copy or phonorecord of the Work You distribute, publicly display, publicly perform, or publicly digitally perform. You may not offer or impose any terms on the Work that alter or restrict the terms of this License or the recipients' exercise of the rights granted hereunder. You may not sublicense the Work. You must keep intact all notices that refer to this License and to the disclaimer of warranties. You may not distribute, publicly display, publicly perform, or publicly digitally perform the Work with any technological measures that control access or use of the Work in a manner inconsistent with the terms of this License Agreement. The above applies to the Work as incorporated in a Collective Work, but this does not require the Collective Work apart from the Work itself to be made subject to the terms of this License. If You create a Collective Work, upon notice from any Licensor You must, to the extent practicable, remove from the Collective Work any reference to such Licensor or the Original Author, as requested. If You create a Derivative Work, upon notice from any Licensor You must, to the extent practicable, remove from the Derivative Work any reference to such Licensor or the Original Author, as requested.

   b. You may distribute, publicly display, publicly perform, or publicly digitally perform a Derivative Work only under the terms of this License, a later version of this License with the same License Elements as this License, or a Creative Commons iCommons license that contains the same License Elements as this License (e.g. Attribution-ShareAlike 2.0 Japan). You must include a copy of, or the Uniform Resource Identifier for, this License or other license specified in the previous sentence with every copy or phonorecord of each Derivative Work You distribute, publicly display,

publicly perform, or publicly digitally perform. You may not offer or impose any terms on the Derivative Works that alter or restrict the terms of this License or the recipients' exercise of the rights granted hereunder, and You must keep intact all notices that refer to this License and to the disclaimer of warranties. You may not distribute, publicly display, publicly perform, or publicly digitally perform the Derivative Work with any technological measures that control access or use of the Work in a manner inconsistent with the terms of this License Agreement. The above applies to the Derivative Work as incorporated in a Collective Work, but this does not require the Collective Work apart from the Derivative Work itself to be made subject to the terms of this License.

c. If you distribute, publicly display, publicly perform, or publicly digitally perform the Work or any Derivative Works or Collective Works, You must keep intact all copyright notices for the Work and give the Original Author credit reasonable to the medium or means You are utilizing by conveying the name (or pseudonym if applicable) of the Original Author if supplied; the title of the Work if supplied; to the extent reasonably practicable, the Uniform Resource Identifier, if any, that Licensor specifies to be associated with the Work, unless such URI does not refer to the copyright notice or licensing information for the Work; and in the case of a Derivative Work, a credit identifying the use of the Work in the Derivative Work (e.g., "French translation of the Work by Original Author," or "Screenplay based on original Work by Original Author"). Such credit may be implemented in any reasonable manner; provided, however, that in the case of a Derivative Work or Collective Work, at a minimum such credit will appear where any other comparable authorship credit appears and in a manner at least as prominent as such other comparable authorship credit.

5. **Representations, Warranties and Disclaimer**

   UNLESS OTHERWISE AGREED TO BY THE PARTIES IN WRITING, LICENSOR OFFERS THE WORK AS-IS AND MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND CONCERNING THE MATERIALS, EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, INCLUDING, WITHOUT LIMITATION, WARRANTIES OF TITLE, MERCHANTIBILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT, OR THE ABSENCE OF LATENT OR OTHER DEFECTS, ACCURACY, OR THE PRESENCE OF ABSENCE OF ERRORS, WHETHER OR NOT DISCOVERABLE. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES, SO SUCH EXCLUSION MAY NOT APPLY TO YOU.

6. **Limitation on Liability.** EXCEPT TO THE EXTENT REQUIRED BY APPLICABLE LAW, IN NO EVENT WILL LICENSOR BE LIABLE TO YOU ON ANY LEGAL THEORY FOR ANY SPECIAL, INCIDENTAL, CONSEQUENTIAL,

PUNITIVE OR EXEMPLARY DAMAGES ARISING OUT OF THIS LICENSE OR THE USE OF THE WORK, EVEN IF LICENSOR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. **Termination**

   a. This License and the rights granted hereunder will terminate automatically upon any breach by You of the terms of this License. Individuals or entities who have received Derivative Works or Collective Works from You under this License, however, will not have their licenses terminated provided such individuals or entities remain in full compliance with those licenses. Sections 1, 2, 5, 6, 7, and 8 will survive any termination of this License.

   b. Subject to the above terms and conditions, the license granted here is perpetual (for the duration of the applicable copyright in the Work). Notwithstanding the above, Licensor reserves the right to release the Work under different license terms or to stop distributing the Work at any time; provided, however that any such election will not serve to withdraw this License (or any other license that has been, or is required to be, granted under the terms of this License), and this License will continue in full force and effect unless terminated as stated above.

8. **Miscellaneous**

   a. Each time You distribute or publicly digitally perform the Work or a Collective Work, the Licensor offers to the recipient a license to the Work on the same terms and conditions as the license granted to You under this License.

   b. Each time You distribute or publicly digitally perform a Derivative Work, Licensor offers to the recipient a license to the original Work on the same terms and conditions as the license granted to You under this License.

   c. If any provision of this License is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this License, and without further action by the parties to this agreement, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

   d. No term or provision of this License shall be deemed waived and no breach consented to unless such waiver or consent shall be in writing and signed by the party to be charged with such waiver or consent.

   e. This License constitutes the entire agreement between the parties with respect to the Work licensed here. There are no understandings, agreements or representations with respect to the Work not specified here. Licensor shall not be bound by any additional provisions that may appear in any communication from You. This License may not be modified without the mutual written agreement of the Licensor and You.

Creative Commons is not a party to this License, and makes no warranty whatsoever in connection with the Work. Creative Commons will not be liable to You or any party on any legal theory for any damages whatsoever, including without limitation any general, special, incidental or consequential damages arising in connection to this license. Notwithstanding the foregoing two (2) sentences, if Creative Commons has expressly identified itself as the Licensor hereunder, it shall have all rights and obligations of Licensor.

Except for the limited purpose of indicating to the public that the Work is licensed under the CCPL, neither party will use the trademark "Creative Commons" or any related trademark or logo of Creative Commons without the prior written consent of Creative Commons. Any permitted use will be in compliance with Creative Commons' then-current trademark usage guidelines, as may be published on its website or otherwise made available upon request from time to time.

Creative Commons may be contacted at http://creativecommons.org/.

부록 B. GNU Free Documentation License

Version 1.2, November 2002
저작권 © 2000,2001,2002 Free Software Foundation, Inc.

Free Software Foundation, Inc.
51 Franklin St, Fifth Floor,
Boston,
MA
02110-1301
USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.
Version 1.2, November 2002

PREAMBLE

The purpose of this License is to make a manual, textbook, or other functional and useful document "free" in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or noncommercially. Secondarily, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of "copyleft", which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License in order to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license,

unlimited in duration, to use that work under the conditions stated herein. The "Document", below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as "you". You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A "Modified Version" of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A "Secondary Section" is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The "Invariant Sections" are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The "Cover Texts" are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A "Transparent" copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not "Transparent" is called "Opaque".

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML, PostScript or

PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The "Title Page" means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, "Title Page" means the text near the most prominent appearance of the work's title, preceding the beginning of the body of the text.

A section "Entitled XYZ" means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as "Acknowledgements", "Dedications", "Endorsements", or "History".) To "Preserve the Title" of such a section when you modify the Document means that it remains a section "Entitled XYZ" according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

COPYING IN QUANTITY

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document's license

notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

GNU FDL Modification Conditions

A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.

B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.

C. State on the Title page the name of the publisher of the Modified Version, as the publisher.

D. Preserve all the copyright notices of the Document.

E. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.

F. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum [1]03 below.

G. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.

H. Include an unaltered copy of this License.

I. Preserve the section Entitled "History", Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.

J. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the "History" section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.

K. For any section Entitled "Acknowledgements" or "Dedications", Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.

L. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.

M. Delete any section Entitled "Endorsements". Such a section may not be included in the Modified Version.

N. Do not retitle any existing section to be Entitled "Endorsements" or to conflict in title with any Invariant Section.

O. Preserve any Warranty Disclaimers.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version's license notice. These titles must be distinct from any other section titles.

You may add a section Entitled "Endorsements", provided it contains nothing but endorsements of your Modified Version by various parties--for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms defined in section 4 [9]9 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled "History" in the various original documents, forming one section Entitled "History"; likewise

combine any sections Entitled "Acknowledgements", and any sections Entitled "Dedications". You must delete all sections Entitled "Endorsements".

COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an "aggregate" if the copyright resulting from the compilation is not used to limit the legal rights of the compilation's users beyond what the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document's Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled "Acknowledgements", "Dedications", or "History", the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

TERMINATION

You may not copy, modify, sublicense, or distribute the Document except as expressly provided for under this License. Any other attempt to copy, modify, sublicense or distribute the Document is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See http://www.gnu.org/copyleft/.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License "or any later version" applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation.

ADDENDUM: How to use this License for your documents

To use this License in a document you have written, include a copy of the License in the document and put the following copyright and license notices just after the title page:

Sample Invariant Sections list

Copyright (c) YEAR YOUR NAME. Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation; with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts. A copy of the license is included in the section entitled "GNU Free Documentation License".

If you have Invariant Sections, Front-Cover Texts and Back-Cover Texts, replace the "with...Texts." line with this:

Sample Invariant Sections list

> with the Invariant Sections being LIST THEIR TITLES, with the Front-Cover Texts being LIST, and with the Back-Cover Texts being LIST.

If you have Invariant Sections without Cover Texts, or some other combination of the three, merge those two alternatives to suit the situation.

If your document contains nontrivial examples of program code, we recommend releasing these examples in parallel under your choice of free software license, such as the GNU General Public License, to permit their use in free software.