Guida ad Ubuntu sul server

Progetto documentazione di Ubuntu <*ubuntu-doc@lists.ubuntu.com*>

Guida ad Ubuntu sul server

di Progetto documentazione di Ubuntu <*ubuntu-doc@lists.ubuntu.com*>

Estratto

Un'introduzione all'installazione e configurazione delle applicazioni server in Ubuntu.

Riconoscimenti e licenza

I seguenti autori del Gruppo documentazione di Ubuntu mantengono questo documento:

- Bhuvaneswaran Arumugam

La Guida ad Ubuntu sul server è basata anche sui contributi di:

- Robert Stoffers
- Brian Shumate
- Rocco Stanzione

Liberatoria

Sommario

Lista delle Tabelle

Informazioni su questa guida

1. Convenzioni

I seguenti simboli sono utilizzati all'interno di questo documento:

Un simbolo di annotazione indica delle informazioni ritenute interessanti, a volte tecniche, correlate all'argomento in discussione.

Un simbolo di suggerimento indica un consiglio o un metodo più facile per compiere delle azioni.

Un simbolo di attenzione indica al lettore potenziali problemi e lo aiuta a evitarli.

Un simbolo di avvertimento indica al lettore una condizione di rischio che può sorgere in una determinata situazione.

Le convenzioni tipografiche per i riferimenti incrociati sono visualizzate in questo modo:

- I collegamenti ad altri documenti o siti web sono visualizzati come *questo* [http://www.ubuntu-it.org].

Le versioni PDF, HTML e XHTML di questo documento utilizzano collegamenti ipertestuali per gestire i riferimenti incrociati.

Le convenzioni sulla visualizzazione di diversi tipi di informazione sono le seguenti:

- I nomi di file o di percorsi a directory sono visualizzati con carattere a `spaziatura fissa`.
- I comandi da digitare al prompt di comando del Terminale sono visualizzati come segue:

  ```
  comando da digitare
  ```

- Le opzioni su cui fare clic, da selezionare o scegliere all'interno di un'interfaccia utente sono visualizzate con il carattere a `spaziatura fissa`.

Selezioni di menù, azioni con il mouse e scorciatoie da tastiera:

- Una sequenza di selezioni di menù è visualizzata come segue: File → Apri
- Le azioni da svolgere con il mouse hanno come presupposto l'utilizzo di un mouse per utenti destrorsi. I termini «clic» e «doppio-clic» si riferiscono all'utilizzo del pulsante sinistro del mouse. Il termine «clic col pulsante destro» si riferisce all'utilizzo del pulsante destro del mouse. Il termine «clic col pulsante centrale» si rifersice all'utilizzo del pulsante centrale del mouse, alla pressione della rotellina di scorrimento o la pressione simultanea dei pulsanti destro e sinistro, in base al design del proprio mouse.
- Le combinazioni per scorciatoie da tastiera sono visualizzate come segue: **Ctrl**-**N**. Dove per «Control», «Maiusc» e «Alternate» si intendono i tasti **Ctrl**, **Maiusc** e **Alt** rispettivamente. Notare inoltre che il primo tasto è da tenere premuto mentre viene premuto il secondo tasto.

2. Contributi e commenti

Questo documento è sviluppato dal *Gruppo documentazione di Ubuntu* [https://wiki.ubuntu.com/DocumentationTeam]. *Chiunque* può contribuire allo sviluppo di questo documento inviando idee o commenti alla mailing list del team documentazione di Ubuntu. Informazioni riguardo il team, la mailing list, i progetti, ecc... possono essere trovate presso la *pagina web del Gruppo documentazione di Ubuntu* [https://wiki.ubuntu.com/DocumentationTeam].

Se riscontrate degli errori in questo documento o volete inviare dei suggerimenti, è possibile segnalare un bug attraverso l'*Ubuntu Bugtracker* [https://launchpad.net/products/ubuntu-doc/+bugs]. Il vostro aiuto è importante per il successo della documentazione!

Grazie per la vostra attenzione,

il Gruppo documentazione di Ubuntu

Capitolo 1. Introduzione

Benvenuti nella *Guida ad Ubuntu sul server*!

La *Guida ad Ubuntu sul server* contiene informazioni su come installare e configurare, sui sistemi Ubuntu, diverse applicazioni server adatte a tutte le necessità. È una guida passo passo, orientata alle attività, per la configurazione e personalizzazione del sistema. In questo manuale sono discussi diversi argomenti di livello intermedio come:

- Configurazione della rete
- Configurazione di Apache2
- Database
- Reti Windows

Questo manuale è diviso nelle seguenti categorie principali:

- Installazione
- Gestione dei pacchetti
- Rete
- Reti Windows

In questa guida si dà per assunto che il lettore possieda una conoscenza basilare del sistema Ubuntu. Se si necessita di aiuto riguardo l'installazione di Ubuntu, fare riferimento alla Guida di installazione di Ubuntu.

Versioni HTML e PDF di questo manuale sono disponibili su Internet presso il *sito web di documentazione Ubuntu* [http://help.ubuntu.com].

È possibile acquistare questa guida come libro cartaceo presso il *Lulu store di Ubuntu* [http://www.lulu.com/ubuntu-doc]. Il prezzo è limitato alla sola stampa e consegna.

Capitolo 2. Installazione

Questo capitolo fornisce una veloce panoramica dell'installazione di Ubuntu 6.06 LTS Server Edition. Per istruzioni più dettagliate, fare riferimento alla Guida di installazione di Ubuntu.

1. Preparazione dell'installazione

Questa sezione spiega i diversi aspetti da considerare prima di avviare l'installazione.

1.1. Requisiti di sistema

Ubuntu 6.06 LTS Server Edition supporta tre (3) architetture principali: Intel x86, AMD64 e PowerPC. Nella tabella qui sotto sono elencate le specifiche hardware raccomandate. In base alle proprie necessità, il sistema potrebbe funzionare anche con specifiche minori. Comunque, molti utenti rischiano di rimanere frustati dalla lentezza del sistema se ignorano questi suggerimenti.

Tabella 2.1. Requisiti minimi raccomandati

Tipo di installazione	RAM	Spazio hard dis
Server	64 megabyte	500 megabyte

Il profilo predefinito per Ubuntu 6.06 LTS Server Edition è mostrato qui sotto. Ancora una volta, la dimensione dell'installazione dipende dai servizi installati durante l'impostazione. Per la maggior parte degli amministratori, i servizi predefiniti sono adatti a un uso generico del server.

Server

Questo è un profilo per piccoli server, che fornisce una base comune per tutte le applicazioni server. È di dimensioni ridotte e progettato per poter aggiungere su di esso i servizi desiderati, come servizi di file/stampa, hosting web, hosting email, ecc. Per questi servizi 500 MB di spazio su disco dovrebbero essere sufficienti, ma è opportuno considerare la necessità di spazio maggiore in funzione dei servizi ospitati sul server.

Le dimensioni indicate non includono tutto il materiale che deve essere ospitato, come i file utente, la posta, i registri e i dati. È sempre opportuno essere generosi nel considerare lo spazio necessario per i file e i dati.

1.2. Effettuare copia di backup

- Prima di cominciare, assicurarsi di avere una copia di backup di ogni file al momento presente sul proprio sistema. Se è la prima volta che un sistema operativo non-nativo viene installato sul computer, molto probabilmente si deve procedere con un ri-partizionamento per fare spazio a Ubuntu. Ogni qual volta si partiziona un disco, si deve mettere in conto la perdita di dati (per errore o per qualche problema che si verifica durante il partizionamento, come l'interruzione dell'alimentazione). I programmi utilizzati nell'installazione sono affidabili e usati da molto tempo, ma eseguono comunque delle azioni distruttive: un errore nell'uso può causare la perdita di dati sensibili.

  Se si sta creando un sistema multi-boot, assicurarsi di avere il supporto di distribuzione di ogni altro sistema operativo presente. Specialmente se si ri-partiziona il disco di boot, potrebbe essere necessario re-installare il boot loader di un sistema operativo, oppure in molti casi l'intero sistema operativo e tutti i file nelle partizioni interessate.

2. Installare da CD

Inserire il CD di installazione nell'unità CD-ROM e riavviare il computer. Il sistema di installazione è avviato immediatamente quando si fa il boot da CD-ROM. Una volta inizializzato, compare la prima schermata.

A questo punto, leggere il testo sullo schermo. Per leggere la schermata di aiuto fornita dal sistema di installazione, premere F1.

Per portare a termine una installazione server predefinita, selezionare «Installa su hard disk» e premere **Invio**. Viene avviato il processo di installazione. Per installare il sistema Ubuntu, seguire le istruzioni a schermo.

In alternativa, per installare un server LAMP (Linux, Apache, MySQL, PHP/Perl/Python), selezionare «Installa un server LAMP» e seguire le istruzioni.

Capitolo 3. Gestione dei pacchetti

Ubuntu offre un completo sistema di gestione dei pacchetti per l'installazione, l'aggiornamento, la configurazione e la rimozione di software. Oltre a fornire accesso a più di 17000 pacchetti software per Ubuntu, le funzioni di gestione dei pacchetti forniscono risoluzione delle dipendenze e verifica degli aggiornamenti.

Per l'interazione con il sistema di gestione dei pacchetti di Ubuntu sono disponibili diversi strumenti, a partire da semplici utilità a riga di comando che possono essere usate con facilità da amministratori di sistema per attività automatittate, fino a interfacce grafiche semplici da usare per chi si è avvicinato da poco a Ubuntu.

1. Introduzione

Il sistema di gestione dei pacchetti di Ubuntu è derivato dallo stesso sistema usato dalla distribuzione Debian GNU/Linux. I file di pacchetto contengono tutti i file, i meta-dati e le istruzioni necessari per implementare sui sistemi Ubuntu una particolare funzionalità o una applicazione software.

Di solito, i file dei pacchetti Debian presentano l'estensione «.deb» e risiedono nei *repository*, ossia delle collezioni di pacchetti memorizzate su diversi supporti, come un disco CD-ROM o in rete. I pacchetti sono normalmente in formato binario precompilato: per questo l'installazione è veloce e non richiede la compilazione del software.

Molti pacchetti complessi si avvalgono del concetto di *dipendenze*. Le dipendenze sono pacchetti aggiuntivi richiesti dal pacchetto principale per poter funzionare correttamente. Per esempio, il pacchetto di sintesi vocale Festival dipende dal pacchetto festvox-kalpc16k, il quale è un pacchetto che fornisce una delle voci usate dall'applicazione. Per poter far funzionare Festival è necessario installare tutte le dipendenze assieme al pacchetto principale di Festival. In Ubuntu tutto ciò viene svolto automaticamente dagli strumenti di gestione del software.

2. Apt-Get

Il comando apt-get è un potente strumento a riga di comando usato per operare con l'APT (*Advanced Packaging Tool*) di Ubuntu al fine di eseguire operazioni come l'installazione di nuovi pacchetti software, l'aggiornamento dei pacchetti software esistenti, l'aggiornamento dell'indice dell'elenco di pacchetti e persino l'avanzamento di versione dell'intero sistema Ubuntu.

Essendo un semplice strumento da riga di comando, apt-get presenta agli amministratori di sistema numerosi vantaggi rispetto ad altri strumenti di gestione dei pacchetti disponibili in Ubuntu. Alcuni di questi vantaggi sono la facilità d'utilizzo mediante connessioni via terminale (SSH) e la possibilità di essere usato in script di amministrazione del sistema, resi magari automatizzati attraverso l'utilità di pianificazione cron.

Alcuni esempi di utilizzo tipico dell'utilità apt-get:

- **Installare un pacchetto**: l'installazione di pacchetti usando lo strumento apt-get è molto semplice. Per esempio, per installare lo scanner di rete *nmap*, digitare il seguente comando:

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

- **Rimuovere un pacchetto**: la rimozione di uno o più pacchetti è altrettanto semplice e immediata. Per rimuovere il pacchetto nmap installato nell'esempio precedente, digitare il seguente comando:

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

  

  Pacchetti multipli: è possibile specificare più di un pacchetto da installare o rimuovere, separati da spazi.

- **Aggiornare l'indice dei pacchetti**: l'indice dei pacchetti di APT è essenzialmente un database dei pacchetti disponibili dai repository definiti nel file `/etc/apt/sources.list`. Per aggiornare l'elenco locale dei pacchetti con i cambiamenti apportati di recente nei repository, digitare il comando:

  ```
  sudo apt-get update
  ```

- **Aggiornare i pacchetti**: nel corso del tempo, nei repository dei pacchetti potrebbero essere disponibili delle versioni aggiornate dei pacchetti installati sul computer (per esempio aggiornamenti di sicurezza). Per aggiornare il sistema, per prima cosa aggiornare l'indice dei pacchetti come descritto poco sopra, poi digitare il comando:

  ```
  sudo apt-get upgrade
  ```

  Se un pacchetto necessita l'installazione o la rimozione di nuove dipendenze durante l'aggiornamento, allora tale pacchetto non sarà aggiornato dal comando *upgrade*. Per questo genere di aggiornamenti, è necessario utilizzare il comando *dist-upgrade*.

Allo stesso modo, è possibile aggiornare l'intero sistema Ubuntu da una revisione a un'altra con dist-upgrade. Per esempio, per effettuare l'aggiornamento dalla versione 5.10 alla versione 6.06 LTS, innanzitutto bisogna assicurasi di aver sostituito nel file `/etc/apt/sources.list` i repository della versione 5.10 con quelli della versione 6.06 LTS, poi basta eseguire il comando apt-get update come descritto poco sopra, infine bisonga eseguire l'aggiornamento digitando il comando:

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

L'aggiornamento del sistema alla versione successiva richiede un certo periodo di tempo. Solitamente sono richiesti alcuni passi di post-aggiornamento come descritto nelle note di aggiornamento per la revisione a cui si sta aggiornando.

Le azioni del comando apt-get, come l'installazione o la rimozione di pacchetti, vengono registrate nel file di registro /var/log/dpkg.log.

Per maggiori informazioni sull'uso di APT, leggere il *Manuale utente di Debian APT* [http://www.debian.org/doc/user-manuals#apt-howto] , oppure digitare:

```
apt-get help
```

3. Aptitude

Aptitude è un'interfaccia testuale basata su menù per il sistema APT (*Advanced Packaging Tool*). Molte delle tipiche funzioni di gestione dei pacchetti, come l'installazione, la rimozione e l'aggiornamento, possono essere effettuate in Aptitude con dei comandi mappati su un solo tasto, solitamente delle lettere minuscole.

Aptitude è adatta a essere utilizzata all'interno di un ambiente a riga di comando, per garantire il corretto funzionamento dei tasti di comando. È possibile avviare Aptitude come normale utente per mezzo del seguente comando al promtp del terminale:

```
sudo aptitude
```

All'avvio di Aptitude, viene mostrata una barra dei menù nella parte superiore dello schermo e due riquadri sotto tale barra. Il riquadro superiore contiene delle categorie di pacchetto, come *Pacchetti nuovi* e *Pacchetti non installati*. Il riquadro inferiore contiene le informazioni relative ai pacchetti e alle categorie di pacchetto.

L'utilizzo di Aptitude per la gestione dei pacchetti è abbastanza intuitivo e l'interfaccia utente rende semplice l'esecuzione delle attività più comuni. Qui di seguito sono illustrati alcuni esempi di tipiche funzioni di gestione dei pacchetti eseguiti in Aptitude:

- **Installare pacchetti**: per installare un pacchetto, localizzare il pacchetto atrraverso la categoria di pacchetto "Pacchetti non installati", usando i tasti freccia sulla tastiera e il tasto **Invio**, in modo da evidenziare il pacchetto da installare. Dopo aver evidenziato il pacchetto da installare, premere il tasto **+**: la voce relativa al pacchetto assume una colorazione *verde*, per indicare che è stato contrassegnato per l'installazione. Premere quindi il tasto **g** per ricapitolare le operazioni su pacchetti. Premendo nuovamente **g**, viene richiesto di acquisire i privilegi di amministrazione per completare l'installazione. Premere quindi **Invio** per mostrare un prompt «Password:». Inserire la propria password utente per diventare root. Infine premendo **g** ancora una volta viene richiesto se scaricare il pacchetto. Premere **Invio** al prompt *Continua*: viene avviato lo scaricamento e l'installazione del pacchetto.
- **Rimuovere pacchetti**: per rimuovere un pacchetto, localizzare il pacchetto attraverso la categoria di pacchetto "Pacchetti installati", usando i tasti freccia sulla tastiera e il tasto **Invio**, in modo da evidenziare il pacchetto da rimuovere. Dopo aver evidenziato il pacchetto da rimuovere, premere il tasto **-**: la voce relativa al pacchetto assume una colorazione *rosa*, per indicare che è stato contrassegnato per la rimozione. Premere quindi il tasto **g** per ricapitolare le operazioni sui pacchetti. Premendo nuovamente **g**, viene richiesto di acquisire i privilegi di amministrazione per completare l'installazione. Premere quindi **Invio** per mostrare un prompt "Password:". Inserire la propria password utente per diventare root. Infine, premendo **g** ancora una volta, viene richiesto se scaricare il pacchetto. Premere **Invio** al prompt *Continua*: viene avviata la rimozione del pacchetto.
- **Aggiornare l'indice dei pacchetti**: per aggiornare l'indice dei pacchetti, è sufficiente premere il tasto **u**; viene mostrata la richiesta di divenire root per completare l'installazione. Premere il tasto

Invio per mostrare il prompt «Password:» e inserire la propria password utente per diventare root. Viene avviato l'aggiornamento dell'indice dei pacchetti. Premere **Invio** al prompt «OK» quando viene presentato il dialogo di scaricamento per completare il processo.

- **Aggiornare i pacchetti**: per aggiornare i pacchetti, procedere con l'aggiornamento dell'indice dei pacchetti come spiegato poco sopra, quindi premere il tasto **U** per contrassegnare tutti gli aggiornamenti disponibili. Premendo il tasto **g** vengono elencate le operazioni che verranno eseguite. Premendo nuovamente il tasto **g**, viene presentato l'invito per diventare root. Dopo la pressione del tasto **Invio** è necessario inserire la propria password, dopodiché premendo ancora una volta il tasto **g**, viene richiesto il download dei pacchetti. Premendo il tasto **Invio** al prompt *Continua*, l'aggiornamento dei pacchetti ha inizio.

La prima colonna delle informazioni mostrate nell'elenco dei pacchetti nel riquadro superiore, indica l'attuale stato del pacchetto, utilizzando le seguenti chiavi per descrivere lo stato del pacchetto:

- **i**: pacchetto installato.
- **c**: pacchetto non installato, ma nel sistema è rimasta traccia della configurazione del pacchetto
- **p**: rimosso completamente dal sistema
- **v**: pacchetto virtuale
- **B**: pacchetto non integro
- **u**: file decompressi, ma pacchetto non ancora configurato
- **C**: semi-configurato - configurazione fallita, è necessario intervenire
- **H**: semi-installato - rimozione fallita, è necessario intervenire

Per chiudere Aptitude, è sufficiente premere il tasto **q** e confermare l'uscita. Sono disponibili molte altre funzioni dal menù di Aptitude, premendo il tasto **F10**.

4. Configurazione

La configurazione dei repository del sistema APT (*Advanced Packaging Tool*) è memorizzata nel file di configurazione /etc/apt/sources.list. Un esempio di questo file, con le istruzioni su come aggiungere e rimuovere repository, è qui referenziato.

Questo [../sample/sources.list] è un semplice esempio di un tipico file `/etc/apt/sources.list`

È possibile modificare il file per abilitare o disabilitare i repository. Ad esempio, per disabilitare la necessità di inserire il CD-ROM di Ubuntu ogni volta che viene effettuata una operazione sui pacchetti, è sufficiente trasformare in commento la riga relativa al CD-ROM, che si trova all'inizio del file:

```
# niente richiesta del CD-ROM
# deb cdrom:[Ubuntu 6.06 _Dapper Drake_ - Release i386 (20060329.1)]/ dapper main restricted
```

5. Repository aggiuntivi

In aggiunta ai repository di pacchetti supportati ufficialmente disponibili per Ubuntu, esistono altri repository aggiuntivi mantenuti dalla comunità, che aggiungono migliaia di potenziali pacchetti da installare. Due sono i repository aggiuntivi più popolari: *Universe* e *Multiverse*. Si tratta di repository non supportati ufficialmente da Ubuntu, per cui non sono abilitati in modo predefinito, ma che solitamente contengono dei pacchetti che possono essere utilizzati con sicurezza in Ubuntu.

I pacchetti del repository Multiverse possono presentare dei problemi di licenza che ne impediscono la distribuzione in un sistema operativo libero e potrebbero essere illegali in alcuni paesi.

Né il repository *Universe*, né quello *Multiverse* contengono pacchetti supportati ufficialmente. In particolare, potrebbero non esserci aggiornamenti di sicurezza per tali pacchetti.

Sono disponibili molte altre sorgenti di pacchetti, alcune delle quali offrono solo un pacchetto, come nel caso di sorgenti di pacchetto fornite dallo sviluppatore di una singola applicazione. L'utilizzo di sorgenti di pacchetto non standard è rischioso, pertanto è necessario prestare la massima attenzione. È opportuno controllare la sorgente e i pacchetti in modo accurato prima di effettuare una qualsiasi installazione, poiché alcune sorgenti di pacchetto, e i rispettivi paccheti, potrebbero rendere il sistema instabile e non funzionante sotto certi aspetti.

Per abilitare i repository *Universe* e *Multiverse*, modificare il file `/etc/apt/sources.list` e rimuovere il commento dalle righe appropriate:

```
# abilitazione dei repository Multiverse e Universe

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

5.1. Riferimenti

HOWTO sull'aggiunta di repository (Wiki di Ubuntu)
[https://wiki.ubuntu.com/AddingRepositoriesHowto]

Capitolo 4. Rete

Le reti sono costituite da due o più dispositivi, come computer, stampanti e relativi accessori, collegati tra loro sia fisicamente, tramite dei cavi, oppure mediante dispositivi senza filo, allo scopo di condividere e distribuire informazioni tra i dispositivi connessi.

Questa sezione della Guida ad Ubuntu sul server fornisce informazioni generali e specifiche sulle reti, inclusa una panoramica dei concetti di rete e una discussione dettagliata dei protocolli di rete più usati e delle applicazioni server.

1. Configurazione della rete

Ubuntu è corredato da una serie d'utilità grafiche per la configurazione dei dispositivi di rete. Questo documento è diretto agli amministratori di server e si focalizza sulla gestione della rete da riga di comando.

1.1. Ethernet

La maggior parte della configurazione di ethernet è raccolta in un singolo file, `/etc/network/interfaces`. Se non è presente alcun dispositivo ethernet, in questo file è elencata solo l'interfaccia di loopback e il contenuto è simile a quanto segue:

```
# Questo file descrive le interfacce di rete disponibili sul sistema e
# come attivarle. Per maggiori informazioni, consultare interfaces(5).

# L'interfaccia di rete di loopback
auto lo
iface lo inet loopback
address 127.0.0.1
netmask 255.0.0.0
```

Se nel sistema è presente solo un dispositivo ethernet, eth0, e la sua configurazione viene ottenuta da un server DHCP, allora il dispositivo dovrebbe essere attivato automaticamente al boot e nel file sono richieste solo due righe aggiuntive:

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

La prima riga specifica che il dispositivo eth0 dovrebbe essere attivato automaticamente al boot. La seconda riga indica che l'interfaccia («iface») eth0 dovrebbe avere un indirizzo nello spazio di IPv4 (sostituire «inet» con «inet6» per un dispositivo IPv6) e che dovrebbe ottenere la sua configurazione da DHCP in modo automatico. Assumendo che la rete e il server DHCP sono propriamente configurati, la macchina in questione non dovrebbe necessitare di ulteriore configurazione per operare propriamente. Il server DHCP fornisce il gateway predefinito (implementato attraverso il comando route), l'indirizzo IP del dispositivo (implementato attraverso il comando ifconfig) e viene usato un server DNS sulla rete (implementato nel file `/etc/resolv.conf`).

Per configurare il dispositivo ethernet con un indirizzo IP statico e una configurazione personalizzata, sono richieste alcune informazioni aggiuntive. Si fa l'ipotesi di voler assegnare l'indirizzo IP 192.168.0.2 al dispositivo eth1, con la tipica maschera di rete 255.255.255.0. L'indirizzo IP del gateway predefinito è 192.168.0.1. In tal caso si dovrebbe inserire in `/etc/network/interfaces` qualcosa tipo:

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

In tal caso è necessario specificare manualmente i server DNS in `/etc/resolv.conf`, che dovrebbe contenere qualcosa tipo:

```
search miodominio.it
nameserver 192.168.0.1
nameserver 4.2.2.2
```

La direttiva *search* fa sì che miodominio.it sia accodata alle interrogazioni dei nomi di host nel tentativo di risolvere i nome sulla rete locale. Ad esempio, se il proprio nome di dominio è miodominio.it e si prova a fare un ping all'host «mybox», l'interrogazione DNS viene modificata in «mybox.miodominio.it» per la risoluzione. La direttiva *nameserver* specifica i server DNS da usare per risolvere i nomi di host in indirizzi IP. Se si fa uso di un proprio server di nomi, inserirlo qui. Altrimenti, domandare al proprio ISP (Internet Service Provider) i server DNS primario e secondario da usare e inserirli in `/etc/resolv.conf` come mostrato poco sopra.

È possibile realizzare molte altre configurazioni, incluse quelle per le interfacce PPP dialup, le reti IPv6, i dispositivi VPN, ecc. Fare riferimento a man 5 interfaces per maggiori informazioni e per le opzioni supportate. Notare che `/etc/network/interfaces` è usato dagli script ifup/ifdown come schema di configurazione a un livello più alto rispetto ad altre distribuzioni Linux e che le tradizionali utilità di livello inferiore, come ifconfig, route e dhclient sono sempre disponibili per una configurazione ottimale.

1.2. Gestione dei record DNS

Questa sezione spiega come configurare il server di nomi da usare durante la risoluzione degli indirizzi IP in nomi di host e viceversa. Non viene spiegato come configurare il sistema per operare come server di nomi.

Nel gestire i record DNS, è possibile aggiungere, modificare o rimuovere i nomi DNS dal file `/etc/resolv.conf`. Un

```
search com
nameserver 204.11.126.131
nameserver 64.125.134.133
nameserver 64.125.134.132
nameserver 208.185.179.218
```

La chiave search specifica la stringa che viene accodata ad un nome di host incompleto. In questo caso è stato specificato com. Pertanto quando viene eseguito il comando **ping ubuntu**, questo viene interpretato come **ping ubuntu.com**.

La chiave nameserver specifica l'indirizzo IP del server di nomi. Tale server viene usato per risolvere un indirizzo IP o un nome host forniti. Questo file può contenere diversi record di server di nomi. I server di nomi sono usati nelle interrogazioni di rete nell'ordine in cui compaiono.

Se i nomi dei server DNS sono recuperati dinamicamente da DHCP o PPPoE (recuperati dal proprio ISP), i record dei server di nomi non vanno aggiunti a questo file. Il file viene infatti aggiornato automaticamente.

1.3. Gestione degli host

Nel gestire gli host, è possibile aggiungere, modificare o rimuovere gli host dal file `/etc/hosts`. Il file contiene indirizzi IP e i loro corrispettivi nomi di host. Quando il sistema tenta di risolvere un nome di host in un indirizzo IP oppure di determinare il nome di host per un indirizzo IP, viene fatto riferimento al file `/etc/hosts` prima di usare i server di nomi. Se l'indirizzo IP è elencato nel file `/etc/hosts`, i server di nomi non vengono utilizzati. Questo comportamento può essere modificato editando il file `/etc/nsswitch.conf` a proprio rischio e pericolo.

Se la rete comprende dei computer i cui indirizzi IP non sono elencati nel DNS, è consigliabile aggiungerli al file `/etc/hosts`.

2. TCP/IP

Il protocollo TCP/IP (Transmission Control Protocol e Internet Protocol) è un insieme standard di protocolli sviluppato nella seconda metà degli anni '70 dalla DARPA (Defence Advanced Research Project Agency), allo scopo di permettere la comunicazione tra diversi tipi di computer e di reti di computer. TCP/IP è il motore di Internet, ecco perchè è l'insieme di protocolli di rete più diffuso al mondo.

2.1. Introduzione a TCP/IP

I due protocolli che compongono il TCP/IP si occupano di aspetti diversi delle reti di computer. L'*Internet Protocol*, la parte IP di TCP/IP, è un protocollo senza connessione che tratta solo l'instradamento dei pacchetti di rete usando il *datagramma IP* come l'unità fondamentale dell'informazione di rete. Il datagramma IP è formato da un'intestazione seguita da un messaggio. Il *Transmission Control Protocol*, la parte TCP di TCP/IP, consente agli host della rete di stabilire delle connessioni usate per scambiare flussi di dati. Inoltre il TCP garantisce che i dati tra le connessioni siano consegnati e che arrivino ad host della rete nello stesso ordine in cui sono stati trasmessi da un altro host della rete.

2.2. Configurazione di TCP/IP

La configurazione del protocollo TCP/IP è composta da vari elementi che debbono essere impostati modificando gli appropriati file di configurazione oppure adottando soluzioni quali un server DHCP (Dynamic Host Configuration Protocol); tale server provvede ad assegnare automaticamente le corrette impostazioni di configurazione TCP/IP ai client della rete. Questi valori di configurazione debbono essere impostati correttamente per consentire al sistema Ubuntu di operare adeguatamente in rete.

I tipici elementi di configurazione del TCP/IP e i loro scopi sono i seguenti:

- **Indirizzo IP** L'indirizzo IP è una stringa d'identificazione unica, espressa da quattro numeri decimali compresi tra zero (0) e duecentocinquantacinque (255), separati da punti; ciascuno dei quattro numeri rappresenta otto (8) bit dell'indirizzo per una lunghezza totale di trentadue (32) bit per l'indirizzo completo. Questo formato è detto *notazione decimale a punti*.
- **Maschera di rete** La maschera di rete (o semplicemente *netmask*) è una maschera locale di bit, ovvero un insieme di indicatori che separano la porzione di un indirizzo IP che indica la rete dai bit che indicano la *sotto-rete*. Ad esempio, in una rete di classe C, la maschera di rete standard è 255.255.255.0 che serve a mascherare i primi tre byte dell'indirizzo IP, consentendo all'ultimo byte dell'indirizzo IP di essere disponibile per specificare gli host della sotto-rete.
- **Indirizzo di rete** L'indirizzo di rete rappresenta i byte che contengono la porzione di rete di un indirizzo IP. Ad esempio, l'host 12.128.1.2 in una rete di classe A usa 12.0.0.0 come indirizzo di rete; tale indirizzo di rete usa il 12 per rappresentare il primo byte dell'indirizzo IP (la parte della rete) e gli zero (0) in tutti i restanti tre byte per rappresentare i valori dei potenziali host. Gli

host di rete che usano indirizzi IP privati e non indirizzabili molto comuni come 192.168.1.100 usano come indirizzo di rete 192.168.1.0, che specifica che i primi tre gruppi di byte 192.168.1 appartengono ad una rete di classe C, mentre uno zero rappresenta tutti gli host presenti nella rete.

- **Indirizzo di broadcast** L'indirizzo di broadcast è un indirizzo IP che consente di inviare dati simultaneamente a tutti gli host di una data sotto-rete invece che a uno specifico host di rete. L'indirizzo di broadcast generale standard per le reti IP è 255.255.255.255, ma questo indirizzo di broadcast non può essere usato per inviare un messaggio in broadcast a tutti gli host su Internet poiché viene bloccato dai router. Un indirizzo di broadcast più idoneo è impostato per corrispondere a una specifica sotto-rete. Ad esempio in una comune rete IP privata di classe C, 192.168.1.0, l'indirizzo di broadcast dovrebbe essere configurato come 192.168.1.255. I messaggi di broadcast sono preparati normalmente dai protocolli di rete quali ARP (Address Resolution Protocol) e RIP (Routing Information Protocol).
- **Indirizzo del gateway** Un indirizzo del gateway è l'indirizzo IP attraverso il quale una particolare rete, o un host su una rete, può essere raggiunta. Se un host di rete desidera comunicare con un altro host di rete, senza essere localizzati nelle stessa rete, allora deve essere usato un *gateway*. In molti casi l'indirizzo del gateway coincide con quello di un router della medesima rete, il quale ha il compito di far transitare il traffico ad altre reti o host, come gli host su Internet. L'impostazione del valore dell'indirizzo del gateway deve essere corretta, altrimenti il sistema non è in grado di raggiungere gli host che non si trovano sulla rete cui appartiene.
- **Indirizzo di server dei nomi** Gli indirizzi di server dei nomi rappresentano gli indirizzi IP del sistema DNS (Domain Name Service), che risolve i nomi degli host della rete in indirizzi IP. Sono disponibili tre livelli di indirizzi di server dei nomi che possono essere specificati in ordine di precedenza: il server dei nomi *primario*, il server dei nomi *secondario*, e il server dei nomi *terziario*. Per consentire al sisema di risolvere i nomi degli host di rete nei loro corrispondenti indirizzi IP, è necessario specificare nella configurazione del sistema TCP/IP degli indirizzi di server dei nomi validi e che si è autorizzati a usare. In molti casi tali indirizi possono e sono forniti dal provider dell'utente: comunque risultano liberi e pubblicamente accessibili molti server dei nomi, come i server Level3 (Verizon) con indirizzi IP da 4.2.2.1 a 4.2.2.6.

Gli indirizzi IP, le maschere di rete, gli indirizzi di rete, gli indirizzi di broadcast e gli indirizzi di gateway sono tipicamente determinati attraverso appropriate direttive nel file `/etc/network/interfaces`. Gli indirizzi di server di nomi sono tipicamente specificati attraverso le direttive *nameserver* nel file `/etc/resolv.conf`. Per maggiori informazioni, consultare rispettivamente le pagine di manuale di sistema per `interfaces` e `resolv.conf`, usando i seguenti comandi da digitare al prompt di un terminale:

Accedere alla pagina di manuale di sistema per `interfaces` con il seguente comando:

```
man interfaces
```

Accedere alla pagina di manuale di sistema per `resolv.conf` con il seguente comando:

```
man resolv.conf
```

2.3. Instradamento IP

L'instradamento IP (routing) è un mezzo per specificare e scoprire i percorsi in una rete TCP/IP lungo i quali possono essere inviati dati di rete. L'instradamento fa uso di un insieme di *tabelle di instradamento* per gestire l'avanzamento dei pacchetti di dati di rete dalla sorgente fino alla destinazione, spesso attraverso molti nodi di rete intermedi di rete noti come *router*. L'instradamento IP è il mezzo principale per trovare i percorsi su Internet. Due sono le forme principali di instradamento IP: *instradamento statico* e *instradamento dinamico*.

L'instradamento statico comporta l'aggiunta manuale delle rotte IP alla tabella di instradamento del sistema; ciò viene di solito eseguito mediante la manipolazione della tabella di instradamento con il comando route. L'instradamento statico gode di molti vantaggi sull'instradamento dinamico, come la semplicità d'implementazione sulle reti poco estese, la predicibilità (la tabella di instradamento è sempre calcolata in anticipo, quindi l'instradamento è sempre lo stesso a ogni utilizzo) e una bassa sovrapponibilità (overhaed) sugli altri router e sugli altri collegamenti di rete dovuta alla mancanza di un protocollo di instradamento dinamico. Comunque, l'instradamento statico, presenta anche alcuni svantaggi. Ad esempio, l'instradamento statico è limitato solo alle reti di piccole dimensioni e non è in grado di "scalare" bene. Inoltre l'instradamento statico fallisce completamente nell'adattarsi alle disfunzioni e fallimenti della rete sulla rotta a causa della natura statica della stessa rotta.

L'instradamento dinamico su reti di grandi dimensioni è subordinato alla presenza di diverse possibili rotte IP da una sorgente a una destinazione e fa uso di speciali protocolli di instradamento, come il RIP (Router Information Protocol) che gestisce la regolazione automatica delle tabelle di riavviamento così da rendere possibile l'instradamento dinamico. L'instradamento dinamico gode di vantaggi rispetto all'instradamento statico, come maggiore scalabilità e capacità di adattamento a disfunzioni e fallimenti di rete. In aggiunta è richiesta una minore configurazione manuale delle tabelle di instradamento, poichè i router apprendono l'uno dall'altro informazioni sulla loro esistenza e disponibilità. Questa peculiarità elimina di fatto la possibilità di introdurre errori "umani" nelle tabelle di instradamento. Tuttavia l'instradamento dinamico non è perfetto e presenta alcuni svantaggi quali una complessità accentuata ed un carico di lavoro aggiuntivo per le reti, derivato dalle comunicazioni tra router, che non è di beneficio immediato per gli utenti, ma che consuma comunque la larghezza di banda della rete.

2.4. TCP e UDP

TCP è un protocollo basato sulla connessione, che offre correzione d'errore e che garantisce la consegna dei dati attraverso ciò che è conosciuto come *controllo di flusso*. Il controllo di flusso determina quando il flusso di uno stream di dati debba essere fermato e i pacchetti di dati inviati in precedenza debbano essere reinviati a causa di problemi come *collisioni*, assicurando quindi la completa e accurata consegna dei dati. TCP è tipicamente usato nello scambio di informazioni importanti come transazioni di database.

UDP (User Datagram Protocol), al contrario, è un protocollo *senza connessione* che raramente tratta della trasmissione dei dati importanti a causa della mancanza del controllo di flusso o di altro metodo

che garantisca la consegna affidabile dei dati. UDP è normalmente usato in applicazioni come lo streaming audio e video, in cui risulta considerevolemnte più veloce del protocollo TCP, a causa della mancanza di correzione d'errore e del controllo di flusso, e in cui la perdita di alcuni pacchetti non è generalmente un evento catastrofico.

2.5. ICPM

ICMP (Internet Control Messaging Protocol) è un'estensione di IP (Internet Protocol), come definito nell'RFC (Request For Comments) numero 792; ICPM supporta pacchetti di rete contenenti messaggi di controllo, di errore e di informazione. ICMP è usato da applicazioni di rete come l'utilità ping, che consente di determinare la disponibilità di un host o una interfaccia di rete. Esempi di alcuni dei messaggi di errore restituiti da ICMP utili sia agli host e interfacce di rete che ai router sono *Destination Unreachable* e *Time Exceeded*.

2.6. Demoni

I demoni sono speciali applicazioni di sistema che tipicamente sono continuamente in esecuzione in background, attendendo dagli altri programmi richieste relative funzioni da essi fornite. Molti demoni hanno a che fare con la rete. Infatti molti demoni in esecuzione in background sui sistemi Ubuntu forniscono delle funzionalità legate alla rete. Alcuni esempi di questi demoni di rete includono *httpd* (Hyper Text Transport Protocol Daemon), che fornisce funzionalità di server web; *sshd* (Secure SHell Daemon), che fornisce funzionalità di login e trasferimento file sicuro da remoto; *imapd* (Internet Message Access Protocol Daemon), che fornisce servizi di email.

3. Configurazione del firewall

Il kernel Linux include il sottosistema *Netfilter*, usato per manipolare o decidere la sorte del traffico di rete diretto all'interno o attraverso un server. Tutte le moderne soluzioni firewall per Linux si basano su questo sistema di filtraggio dei pacchetti.

3.1. Introduzione al firewall

Il sistema di filtraggio dei pacchetti del kernel non è di grande utilità per gli amministratori senza un'interfaccia nello spazio utente per gestirlo. Questo è il compito di iptables. Quando un pacchetto raggiunge il proprio server, esso è gestito affidato al sottosistema Netfilter per l'accettazione, la manipolazione oppure il rifiuto secondo quanto stabilito da regole fornite al sottosistema dallo spazio utente attraverso iptables. Quindi, iptables è tutto ciò che è necessario per gestire il proprio firewall, a patto che si abbia la dimestichezza necessaria; sono comunque disponibili molte altre applicazioni per semplificare tale attività.

3.2. IP masquerading

Il compito dell'IP masquerading è di consentire a quelle macchine della rete fornite di indirizzi IP privati e non instradabili di accedere a Internet tramite la macchina che opera il masquerading. Il traffico che va dalla rete privata verso Internet deve essere manipolato per ottenere risposte che siano re-instradabili alla macchina che ne ha fatto richiesta. Per ottenere questo risultato, il kernel deve modificare l'indirizzo IP *sorgente* di ciascun pacchetto affinchè tali risposte vengano re-instradate a esso invece che all'indirizzo IP privato che ha fatto la richiesta, procedura impossibile da eseguire su Internet. Linux fa uso del *tracciamento della connessione* (conntrack) per tenere traccia di quale connessione appartenga a quale macchina e di conseguenza per reinstradare ciascun pacchetto di risposta. Il traffico in uscita dalla rete privata viene quindi "mascherato" per simulare l'uscita dalla macchina gateway Ubuntu. Nella documentazione Microsoft questo processo è indicato come condivisione delle connessioni internet (Internet Connection Sharing).

Tutto ciò può essere ottenuto con una singola regola di iptables, che può differire leggermente in funzione della propria configurazione di rete:

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

Nel comando precedente si è supposto che il proprio spazio di indirizzi privati sia 192.168.0.0/16 e che l'interfaccia affacciata su Internet sia ppp0. La sintassi è:

- -t nat -- la regola viene inserita nella tabella nat
- -A POSTROUTING -- la regola viene accodata (-A) alla catena POSTROUTING
- -s 192.168.0.0/16 -- la regola si applica al traffico originato dallo spazio di indirizzi specificato
- -o ppp0 -- la regola si applica al traffico instradato attraverso l'interfaccia di rete specificata
- -j MASQUERADE -- il traffico che soddisfa questa regola viene "saltato" (-j sta per jump) alla destinazione MASQUERADE per essere manipolato come descritto in precedenza

La *politica* predefinita di ogni catena nella tabella "filter" (la tabella predefinita, dove si verifica la maggior parte o l'intero filtraggio dei pacchetti) è ACCEPT (accetta), ma se si sta creando un firewall in aggiunta a un dispositivo di gateway, è necessario definire delle politiche di DROP (scarta) o REJECT (rifiuta). In questo caso è necessario autorizzare il traffico mascherato attraverso la catena di FORWARD (inoltra) per far funzionare il masquerading:

```
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
```

I comandi precedenti servono per autorizzare tutte le connessioni dalla rete locale verso Internet e tutto il traffico relativo a tali connessioni che torna alle macchine che lo hanno inizilizzato.

3.3. Strumenti

Molti sono gli strumenti disponibili per aiutare nella costruzione di un firewall completo senza ricorrere all'apprendimento di iptables. Per coloro che sono abituati a un'interfaccia grafica, l'applicazione Firestarter è molto comune e semplice da usare e fwbuilder è molto potente e molto familiare agli amministratori di sistema che hanno usato una firewall commerciale quale Checkpoint FireWall-1. Se si preferisce un'applicazione basata sulla riga di comando con file di configurazione in testo semplice, Shorewall è una soluzione molto potente per configurare un firewall avanzato su ogni rete. Se la rete non è complessa, o si ha una singola macchina, ipkungfu è in grado di fornire un firewall funzionante che non necessita di configurazione, offrendo al tempo stesso la possibilità di predisporne uno più avanzato tramite la modifica di semplici e ben documentati file di configurazione. Un altro strumento interessante è fireflier, progettato per essere una applicazione firewall per sistemi desktop. È composto da un server (fireflier-server) e da un'interfaccia grafica (GTK o QT) e si comporta come molte applicazioni firewall interattive per Windows.

3.4. Registri

I registri firewall sono essenziali per riconoscere attacci, risolvere problemi relativi alle regole del firewall e notificare attività di rete insolita. Per poter generare tali registri è necessario che vengano incluse delle regole di registrazione nel firewall e che tali regole siano inserite prima di ogni regola di terminazione applicabile (cioè una regola con una destinazione che decide la sorte di un pacchetto, come ACCEPT, DROP o REJECT). Ad esempio:

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

In questo modo, una richiesta alla porta 80 dalla macchina locale genera un registro in dmesg come il seguente:

```
[4304885.870000] NUOV_CONN_HTTP: IN=lo OUT= MAC=00:00:00:00:00:00:00:00:00:00:00:00:08:00 SRC=127.0
```

Il registro precedente appare anche nei file `/var/log/messages`, `/var/log/syslog` e `/var/log/kern.log`. Questo comportamento può essere cambiato, modificando in modo appropriato il file `/etc/syslog.conf` oppure installando e configurando ulogd e facendo uso della destinazione ULOG al posto di LOG. Il demone ulogd è un server nello spazio utente in ascolto per le istruzioni

di registro del kernel specifiche dei firewall; è possibile salvare i registri su qualsiasi file o perfino in un database come PostgreSQL o MySQL. Per dare un significato ai registri del firewall è possibile utilizzare delle applicazioni di analisi dei reigistri come fwanalog, fwlogwatch o lire.

4. Server OpenSSH

4.1. Introduzione

Questa sezione della Guida ad Ubuntu sul server presenta una potente collezione di strumenti per il controllo remoto di computer in rete e per il trasferimento di dati tra i medesimi, chiamata *OpenSSH*. Vengono anche indicate alcune delle possibili impostazioni di configurazione e come cambiarle su sistemi Ubuntu.

OpenSSH è una versione libera della famiglia di protocolli e strumenti SSH (Secure SHell) per il controllo remoto di un computer o per il trasferimento di file tra computer. Gli strumenti tradizionali usati per svolgere queste funzioni, come telnet o rcp, sono insicuri e quando utilizzati trasmettono la password dell'utente in chiaro. OpenSSH fornisce un demone server e degli strumenti lato client per facilitare operazioni di controllo remoto e traferimento di file in sicurezza e con crittografia, sostituendo in modo completo gli strumenti tradizionali.

Il componente server di OpenSSH, sshd, è in ascolto continuo per le connessioni in arrivo dei client, qualunque sia lo strumento usato sui client. Quando avviene una richiesta di connessione, per mezzo di sshd viene impostata la corretta connessione in base allo strumento utilizzato dal client. Per esempio, se il computer remoto sta effettuando una connessione con l'applicazione client ssh, il server OpenSSH imposta, dopo l'autenticazione, una sessione di controllo remoto. Se un utente remoto si connette ad un server OpenSSH con scp, il demone server OpenSSH inizializza, dopo l'autenticazione, una procedura di copia sicura di file tra il server e il client. OpenSSH permette l'utilizzo di diversi metodi di autenticazione, inclusi password semplice, chiave pubblica e ticket Kerberos.

4.2. Installazione

L'installazione delle applicazioni server e client di OpenSSH è semplice. Per installare l'applicazione client OpenSSH sui sistemi Ubuntu, usare questo comando al prompt di un terminale:

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

Per installare l'applicazione server di OpenSSH e i relativi file di supporto, usare questo comando al prompt di un terminale:

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

4.3. Configurazione

È possibile configurare il comportamento predefinito dell'applicazione server di OpenSSH, sshd, modificando il file `/etc/ssh/sshd_config`. Per maggiori informazioni riguardo le direttive di configurazione usate in questo file, consultare l'appropriata pagina di manuale inserendo, a un prompt di terminale, il seguente comando:

```
man sshd_config
```

Nel file di configurazione di sshd sono presenti molte direttive per controllare le impostazioni di comunicazioni e le modalità di autenticazione. Di seguito sono riportati degli esempi di direttive di configurazione che possono essere cambiate modificando il file `/etc/ssh/ssh_config`.

Prima di modificare il file di configurazione, è consigliato fare una copia del file originale e proteggerla dalla scrittura, così da avere le impostazioni originali come riferimento ed eventualmente riusarle se necessario.

Copiare il file `/etc/ssh/sshd_config` e proteggerlo da scrittura, con il seguente comando, digitando a un prompt di terminale:

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

Quelli che seguono sono esempi delle direttive di configurazione che è possibile cambiare:

- Per impostare OpenSSH in modo da restare in ascolto sulla porta TCP 2222 invece che sulla predefinita porta TCP 22, cambiare la direttiva Port come segue:

  Port 2222

- Per consentire l'utilizzo in sshd di credenziali di login pubbliche basate su chiave, aggiungere o modificare la riga:

  PubkeyAuthentication yes

  nel file `/etc/ssh/sshd_config`. Se è già presente, assicurarsi che la riga sia stata resa un commento.

- Per far sì che il server OpenSSH mostri il contenuto del file `/etc/issue.net` come un banner di pre-login, aggiungere o modificare la riga:

  Banner /etc/issue.net

  nel file `/etc/ssh/sshd_config`.

Dopo aver apportato dei cambiamenti al file `/etc/ssh/sshd_config`, salvarlo e riavviare l'applicazione server sshd, in modo tale da rendere effettivi i cambiamenti, usando il seguente comando a un prompt di terminale:

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

Per poter adattare il comportamento dell'applicazione server alle proprie necessità, sono disponibili molte altre direttive di configurazione per sshd. Se però l'unico metodo per accedere a un server è ssh, è necessario prestare molta attenzione. Un qualsiasi errore nella

configurazione di sshd attraverso `/etc/ssh/sshd_config` può precludere l'accesso al server dopo il suo riavvio oppure impedire l'avvio stesso di sshd a causa di una errata direttiva di configurazione. Perciò è necessaria molta attenzione nella modifica di questo file su un server remoto.

4.4. Riferimenti

Sito web di OpenSSH [http://www.openssh.org/]

Pagina wiki di OpenSSH avanzato [https://wiki.ubuntu.com/AdvancedOpenSSH]

5. Server FTP

FTP (File Transfer Protocol) è un protocollo TCP per caricare e scaricare file tra computer. FTP opera su un modello client/server. Il componente server viene detto *demone FTP* e rimane continuamente in ascolto di richieste FTP provenienti dai client remoti. Quando viene ricevuta una richiesta, il demone gestice il login e imposta la connessione. Per tutta la durata della sessione il server esegue ogni comando inviato dal client FTP.

L'accesso a un server FTP può essere gestito in due modi:

- Anonimo
- Con autenticazione

Nella modalità anonima, i client remoti possono accedere al server FTP utilizzando l'account utente predefinito chiamato "anonymous" o "ftp" e inviando un indirizzo di posta elettronica come password. Nella modalità con autenticazione l'utente deve essere in possesso di un account e di una password. L'acceso dell'utente ai file e alle directory del server FTP dipende dai permessi definiti per l'account utilizzato per il login. Come regola generale, il demone FTP nasconde la directory radice del server FTP, cambiandola nella home directory di FTP. In questo modo il resto del file system è nascosto alle sessioni remote.

5.1. vsftpd - Installazione del server FTP

Un demone FTP disponibile in Ubuntu è vsftpd, semplice da installare, configurare e mantenere. È possibile installare vsftpd eseguendo il comando seguente:

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

5.2. vsftpd - Configurazione del server FTP

Per cambiare le impostazioni predefinite, è possibile modificare il file di configurazione di vsftpd, `/etc/vsftpd.conf`. In modo predefinito è consentita solamente la modalità anonima. Per disabilitare questa opzione, è necessario cambiare la riga seguente

```
anonymous_enable=YES
```

in

```
anonymous_enable=NO
```

In modo predefinito gli utenti del sistema locale non sono autorizzati ad accedere al server FTP. Per cambiare questa impostazione, è necessario togliere il commento dalla riga seguente:

```
#local_enable=YES
```

In modo predefinito, gli utenti sono autorizzati a scaricare file dal server FTP, ma non possono effettuare l'upload. Per cambiare questa impostazione, è necessario togliere il commento alla riga seguente:

```
#write_enable=YES
```

In maniera simile, gli utenti anonimi non sono autorizzati a effettuare l'upload di file sul server FTP. Per cambiare questa impostazione, è necessario togliere il commento alla riga seguente

```
#anon_upload_enable=YES
```

Il file di configurazione è composto da molti parametri di configurazione. Le informazioni riguardo ciascun parametro sono disponibili nel file stesso. In alternativa, è possibile fare riferimento alla pagina di manuale, **man 5 vsftpd.conf**, per conoscere i dettagli di ogni parametro.

Una volta configurato vsftpd è possibile avviare il demone. È possibile eseguire il seguente comando per mettere in esecuzione il demone vsftpd:

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

Notare che le impostazioni predefinite presenti nel file di configurazione, sono così per ragioni di sicurezza. Ognuno dei cambiamenti prima elencati rendono il sistema un po' meno sicuro: applicarli in casi di effettiva necessità.

6. NFS (Network File System)

NSF permette a un sistema di condividere file e directory con altri attraverso una rete. Utilizzando NFS, utenti e programmi possono accedere ai file presenti su sistemi remoti come se fossero dei file locali.

Alcuni dei principali benefici forniti da NFS sono:

- Le workstation locali utilizzano meno spazio su disco perché i dati comuni possono essere memorizzati su una singola macchina, pur rimanendo accessibili agli altri attraverso la rete.
- Gli utenti non devono avere diverse directory home su ciascuna macchina in rete. Le directory home possono risiedere sul server NFS ed essere rese disponibili attraverso la rete.
- I dispositivi di archiviazione come dischi floppy, unità CD-ROM e USB possono essere utilizzate dagli altri computer della rete. Questo può ridurre il numero di unità per supporti rimovibili presenti nella rete.

6.1. Installazione

Per installare il server NFS, inserire il comando segueten a un prompt di terminale:

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

6.2. Configurazione

È possibile configurare le directory da esportare aggiungendole al file `/etc/exports`. Per esempio:

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

È possibile sostituire * con uno qualsiasi dei formati per i nomi di host. È necessario rendere la dichiarazione dei nomi di host più specifica possibile per impedire l'accesso di sistemi indesiderati ai mount NFS.

Per avviare il server NFS, è possibile eseguire il seguente comando a un prompt di terminale:

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

6.3. Configurazione client NFS

Utilizzare il comando mount per montare una directory NFS convisa da un'altra macchina, digitando una riga di comando simile alla seguente a un prompt di terminale:

```
sudo mount esempio.nomehost.com:/ubuntu /locale/ubuntu
```

Il punto di mount `/locale/ubuntu` deve esistere. Non ci dovrebbero essere nè file, nè sottodirectory all'interno di `/locale/ubuntu`.

Un modo alternativo per montare una condivisione NFS da un'altra macchina consiste nell'aggiungere una riga al file `/etc/fstab`. Questa riga deve contenere il nome dell'host del server NFS, la directory esportata dal server e la directory sulla macchina locale dove montare la condivisione NFS.

La sintassi generale per la riga nel file `/etc/fstab` è come segue:

```
esempio.nomehost.com:/ubuntu /locale/ubuntu nfs rsize=8192,wsize=8192,timeo=14,intr
```

6.4. Riferimenti

FAQ di NFS per Linux [http://nfs.sourceforge.net/]

7. DHCP (Dynamic Host Configuration Protocol)

Il DHCP (Dynamic Host Configuration Protocol) è un servizio di rete che consente di assegnare automaticamente le impostazioni per i computer host da un server, senza la necessità di configurare manualmente ogni singolo host di rete. I computer configurati per essere client DHCP non hanno alcun controllo sulle impostazioni che ricevono dal server DHCP e la configurazione è trasparente all'utente del computer.

Le impostazioni comuni fornite da un server DHCP a un client includono:

- Indirizzo IP e maschera di rete (netmask)
- DNS
- WINS

Comunque, un server DHCP può fornire anche altre proprietà di configurazione come:

- Nome dell'host
- Nome del dominio
- Gateway predefinito
- Server NTP (Network Time Protocol)
- Server di stampa

Il vantaggio di utilizzare DHCP è che i cambiamenti apportati alla rete, ad esempio una modifica dell'indirizzo del server DNS, devono essere apportati solamente al server DHCP, mentre tutti gli host della rete vengono riconfigurati quando i client DHCP interrrogano il server DHCP. Come ulteriore vantaggio, risulta anche molto semplice integrare nuovi computer nella rete, senza la necessità di controllare la disponibilità di un indirizzo IP. I conflitti nell'allocazione degli indirizzi IP sono quindi notevolmente ridotti.

Le impostazioni di configurazione sono fornite da un server DHCP usando due metodi:

Indirizzo MAC
: Questo metodo comporta l'utilizzo di DHCP per indentificare l'indirizzo hardware univoco di ogni scheda di rete collegata alla rete, così da fornire in modo continuato un configurazione costante ogni volta che il client DHCP avanza una richiesta al server DHCP usando quel particolare dispositivo di rete.

Spazio degli indirizzi
: Questo metodo comporta la definizione di un insieme o intervallo di indirizzi IP (a volte indicati come pool) con cui configurare dinamicamente i client DHCP in base all'ordine di arrivo delle richieste (la prima che arriva è la prima servita, disciplina FIFO). Dopo un determinato periodo, se il client DHCP non è presente in rete, la configurazione scade e viene reinserita nello spazio di indirizzi per poter essere riutilizzata.

Ubuntu comprende sia un server che un client DHCP. Il server è dhcpd (dynamic host configuration protocol daemon). Il client fornito è dhclient e dovrebbe essere installato su tutti i computer che necessitano di essere configurati automaticamente. Entrambi i programmi sono facili da installare e da configurare e vengono avviati automaticamente al boot del sistema.

7.1. Installazione

A un prompt di terminale, inserire il seguente comando per installare dhcpd:

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

Verrà mostrato il seguente output indicante i prossimi passi da compiere:

```
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. Configurazione

Il messaggio di errore con cui si conclude l'installazione potrebbe essere fuorviante, ma i passi seguenti consentono di configurare il servizio:

Nella maggior parte dei casi si vuole assegnare un indirizzo IP in modo casuale. Questo può essere ottenuto con impostazioni come le seguenti:

```
# Esempio di /etc/dhcpd.conf
# (aggiungere qui i propri commenti)
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;
}
```

Come risultato si ottiene che il server DHCP fornisce a un client un indirizzo IP nell'intervallo 192.168.1.10 ~ 192.168.1.100 oppure 192.168.1.150 ~ 192.168.1.200. Se il client non richiede uno specifico intervallo di tempo, la durata di "affitto" di un indirizzo IP è di 600 secondi; in caso

contrario il valore massimo (consentito) è di 7200 secondi. Il server inoltre "avvisa" il client di utilizzare 255.255.255.0 come maschera di sottorete, 192.168.1.255 come indirizzo di broadcast, 192.168.1.254 come gateway e 192.168.1.1 e 192.168.1.2 come server DNS.

Se è necessario specificare un server WINS per i client Windows, è necessario includere l'opzione netbios-name-servers, per esempio

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

Le impostazioni di configurazione per dhcpd sono prese dal mini-HOWTO di DHCP, il quale può essere trovato *qui* [http://www.tldp.org/HOWTO/DHCP/index.html].

7.3. Riferimenti

FAQ di DHCP [http://www.dhcp-handbook.com/dhcp_faq.html]

8. DNS (Domain Name Service)

Il DNS (servizio dei nomi di dominio) è servizio Internet che mappa gli indirizzi IP e i "fully qualified domain name" (FQDN, in italiano anche nome di un host, ndT) l'un l'altro. In questo modo viene meno la necessità di ricordare gli indirizzi IP. I computer che eseguono DNS sono definiti *server dei nomi*. Ubuntu fornisce BIND (Berkley Internet Naming Daemon), il programma maggiormente utilizzato per mantenere un server dei nomi con GNU/Linux.

8.1. Installazione

A un promt di terminale, inserire il seguente comando per installare dns:

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

8.2. Configurazione

I file di configurazione di DNS sono memorizzati all'interno della directory `/etc/bind`. Il file di configurazione principale è `/etc/bind/named.conf`. Il contenuto del file di configurazione predefinito è mostrato di seguito:

```
// Questo è il file di configurazione primario per server di nomi DNS BIND
//
// Leggere /usr/share/doc/bind/README.Debian per informazioni sulla
// struttura dei file di configurazione di BIND in Debian per la versione 8.2.1
// e successiva di BIND *PRIMA* di personalizzare questo file di configurazione.
//

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

// riduce la verbosità del registro su elementi fuori dal proprio controllo
logging {
    category lame-servers { null; };
    category cname { null; };
};

// inizializza il server con la conoscenza dei server root
zone "." {
        type hint;
        file "/etc/bind/db.root";
};

// è autoritativo per il localhost froward e le reverse zone
// così come per le broadcast zone (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";
};

// aggiungere qui le definizioni di zona locale
include "/etc/bind/named.conf.local";
```

La riga include specifica il nome del file che contiene le opzioni DNS. La riga directory nel file di opzioni indica a DNS dove cercare i file. Tutti i file utilizzati da BIND sono relativi a questa directory.

Il file `/etc/bind/db.root` descrive i server di nomi radice presenti nel mondo. I server cambiano nel tempo e conseguenza debbono essere aggiornati di tanto in tanto.

La sezione zone definisce un server master, memorizzato in un file menzionato nel campo "file". Ogni file di zona contiene tre record di risorse (RR, Resource Records): un SOA RR, un NS RR e un PTR RR. SOA sta per "Start Of Authority". Il simbolo "@" è una speciale notazione indicante l'origine. NS è il "Name Server RR". PTR è il "Domain Name Pointer". Per avviare il server DNS, eseguire il seguente comando a un prompt di terminale:

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

Per maggiori dettagli, fare riferimento alla documentazione presente nei riferimenti.

8.3. Riferimenti

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

9. CUPS - Server di stampa

Il meccanismo principale di stampa e di servizi di stampa in un sistema Ubuntu è il **Common UNIX Printing System** (CUPS). Questo è un sistema di stampa liberamente disponibile e altamente portabile, diventando così il nuovo standard per la stampa in molte distribuzioni GNU/Linux.

CUPS gestisce lavori e code di stampa, fornisce la stampa in rete tramite l'utilizzo del protocollo IPP (Internet Printing Protocol) e al tempo stesso offre supporto a una nutrita schiera di stampanti, dalle quelle a matrice di punti a quelle al laser (comprese tutte quelle nel mezzo). CUPS supporta anche il PPD (PostScript Printer Detection) e il rilevamento automatico delle stampanti di rete; inoltre fornisce un semplice strumento di amministrazione e configurazione basato sul web.

9.1. Installazione

Per installare CUPS su Ubuntu, utilizzare sudo con il comando apt-get e passare come primo parametro il pacchetto da installare. Una installazione completa di CUPS presenta molte dipendenze, ma queste possono essere specificate sulla stessa riga di comando. Per installare CUPS, inserire quanto segue a un prompt di terminale:

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

Dopo l'autenticazione con la propria password utente, i pacchetti dovrebbe essere scaricati e installati senza errori. Al termine dell'installazione, il server CUPS viene avviato automaticamente. Per risolvere eventuali problemi, è possibile accedere agli errori del server CUPS per mezzo del file di registro degli errori presso `/var/log/cups/error_log`. Se nel file di registro degli errori non sono presenti informazioni sufficienti alla risoluzione dei problemi riscontrati, è possibile incrementare la verbosità del registro di CUPS, cambiando nel file di configurazione (presentato più avanti) la direttiva **LogLevel** dal valore predefinito "info" al valore "debug" oppure "debug2", che regista ogni cosa. Se si apporta questa modifica, ricordarsi di ripristinare il valore iniziale una volta risolto il problema, per evitare la creazione di un file di registro molto grande.

9.2. Configurazione

Il comportamento del server CUPS viene configurato attraverso le direttive contenute nel file `/etc/cups/cupsd.conf`. Il file di configurazione di CUPS segue la stessa sintassi del file di configurazione primario del server HTTP Apache. In questo modo, l'utente che ha familiarità con la modifica del file di configurazione di Apache si sentirà a suo agio nella modifica del file di configurazione di CUPS. Di seguito vengono presentati alcuni esempi di impostazioni che potrebbe essere opportuno cambiare fin da subito.

Prima di modificare il file di configurazione, è opportuno creare un copia del file originale e proteggerla da scrittura, in modo da avere le impostazioni originali come riferimento e per riusarle in caso di necessità.

Copiare il file `/etc/cups/cupsd.conf` e proteggerlo dalla scrittura con i seguenti comandi, inseriti a un prompt di terminale.

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

- **ServerAdmin**: per configurare l'indirizzo e-mail dell'amministratore incaricato alla gestione del server CUPS, aprire il file di configurazione `/etc/cups/cupsd.conf` usando l'editor di testi preferito, quindi modificare la riga *ServerAdmin* come desiderato. Per esempio, se l'idirizzo email dell'amministratore del server CUPS è "bjoy@somebigco.com", modificare la riga ServerAdmin come segue:

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

Per ulteriori esempi di direttive di configurazione nel file di configurazione del server CUPS, consultare la pagina manuale associato inserendo il comando seguente a un prompt di terminale:

```
man cupsd.conf
```

Ogni volta che vengono apportati cambiamenti al file di configurazione `/etc/cups/cupsd.conf`, è necessario riavviare il server CUPS digitando il comando seguente a un prompt di terminale:

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

Altre configurazioni per il server CUPS sono svolte utilizzando il file `/etc/cups/cups.d/ports.conf`:

- **Listen**: in modo predefinito, su Ubuntu, il server CUPS è in ascolto solamente sull'interfaccia di loopback all'indirizzo IP *127.0.0.1*. Per far sì che il server CUPS resti in ascolto sull'indirizzo IP di un adattatore di rete utilizzato, è necessario specificare un nome di host oppure l'indirizzo IP oppure, opzionalmente, una coppia indirizzo IP/porta, aggiungendo una direttiva Listen. Per esempio, se il server CUPS risiede su una macchina locale all'indirizzo IP *192.168.10.250* e si vuole renderlo accessibile agli altri sistemi su questa sottorete, è necessario modificare il file `/etc/cups/cups.d/ports.conf` e aggiungere un direttiva Listen come:

  ```
  Listen 127.0.0.1:631 # Listen esistente per loopback
  Listen /var/run/cups/cups.sock # socket Listen esistente
  Listen 192.168.10.250:631 # Listen sull'interfaccia LAN, porta 631 (IPP)
  ```

  Nell'esempio precedente, è possibile rendere un commento o rimuovere il riferimento all'indizzo di loopback (127.0.0.1) se non si desidera che cupsd resti in ascolto su quell'interfaccia, ma che invece resti in ascolto solo sull'interfaccia Ethernet della LAN (Local Area Network). Per abilitare l'ascolto

su tutte le interfacce di rete a cui un certo host è collegato, inclusa quella di loopback, è possibile creare una voce Listen per l'host *socrates* come segue:

```
Listen socrates:631 # Listen su tutte le interfacce dell'host "socrates"
```

oppure omettendo la direttiva Listen e utilizzando quella *Port*, come in:

```
Port 631 # Listen sulla porta 631 di tutte le interfacce
```

9.3. Riferimenti

Sito Web di CUPS [http://www.cups.org/]

10. HTTPD - Server web Apache2

Apache è il server web più utilizzato nei sistemi GNU/Linux. I server web sono utilizzati per "servire" pagine web ai computer "clienti" che ne fanno richiesta. I client di solito richiedono e visualizzano le pagine web utilizzando un browser web come Firefox, Opera o Mozilla.

Gli utenti inseriscono un URL (Uniform Resource Locator) per dirigersi verso un server Web attraverso il FQDN (Fully Qualified Domain Name) del server stesso e il percorso alla risorsa richiesta. Per esempio, per visualizzare la home page del *sito web di Ubuntu* [http://www.ubuntu.com], l'utente inserisce il solo FQDN. Per richiedere una informazione specifica relativa al *supporto a pagamento* [http://www.ubuntu.com/support/supportoptions/paidsupport], l'utente utilizza il FQDN seguito da un percorso.

Il protocollo più utilizzato per il trasferimento delle pagine web è l'HTTP (Hyper Text Transfer Protocol). Sono anche supportati protocolli come HTTPS (Hyper Text Transfer Protocol over Secure Sockets Layer) e FTP (File Transfer Protocol), un protocollo per caricare e scaricare file dalla rete.

I web server Apache vengono comunemente usati in combinazione con il motore di database MySQL, il linguaggio di scripting per il pre-processamento dell'ipertesto PHP (Pre-processor Hyper Text) e altri noti linguaggi di scripting come Python e Perl. Questa configurazione viene denominata LAMP (Linux, Apache, MYSQL e Perl/Phyton/PHP) e costituisce una piattaforma robusta e potente per lo sviluppo e l'installazione di applicazioni basate sul web.

10.1. Installazione

Il server web Apache2 è disponibile in Ubuntu Linux. Per installarlo:

- Inserire il seguente comando a un prompt di terminale:

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

10.2. Configurazione

Apache viene configurato inserendo delle *direttive* in alcuni file di configurazione (file di testo semplice). Il file di configurazione principale è `apache2.conf. Include;`

Il server inoltre legge un file contenente i tipi MIME dei documenti. Il nome di questo file è impostato attraverso la direttiva *TypesConfig*; in modo predefinito il nome è `mime.types`.

Il file di configurazione predefinito di Apache2 è `/etc/apache2/apache2.conf`. È possibile modificare questo file per configurare il server Apache2. È possibile configurare il numero della porta, l'origine dei documenti, i moduli, i file di registro, gli host virtuali e altro.

10.2.1. Impostazioni di base

Questa sezione espone i parametri di configurazione fondamentali del server Apache2. Per maggioni informazioni, consultare la *documentazione di Apache2* [http://httpd.apache.org/docs/2.0/].

- Apache2 viene fornito con una configurazione predefinita di un singolo host virtuale. L'host virtuale viene definito usando la direttiva *VirtualHost* che può essere usata, così com'è se, si dispone di un unico sito, oppure modificata per aggiungere altri host virtuali, a seconda delle necessità. Se viene lasciato solo un host virtuale, questo diventa il sito predefinito o il sito che gli utenti vedono sel l'URL inserito non corrisponde a nessuna direttiva *ServerName* di altri siti. Per cambiare l'host virtuale predefinito, modificare il file `/etc/apache2/sites-available/default`. Se si desidera configurare un altro host virtuale o un altro sito, bisogna copiare il file all'interno della stessa directory cambiandone il nome. Per esempio **sudo cp /etc/apache2/sites-available/default /etc/apache2/sites-available/mynewsite** Modificare quindi il nuovo file di configurazione usando alcune delle direttive descritte in seguito.
- La direttiva *ServerAdmin* specifica a quale indirizzo email il sistema deve indirizzare la posta destinata agli amministratori. Il valore predefinito è «webmaster@localhost». Quest'impostazione deve essere modificata con l'indirizzo che è stato assegnato all'utente (nel caso sia l'amministratore). Se il sito presenta dei problemi, Apache2 mostrerà un messaggio di errore indicante l'indirizzo a cui deve essere segnalato il problema. Questa direttiva è presente nel file /etc/apache2/sites-available del proprio sito.
- La direttiva *Listen* specifica la porta, e opzionalmente l'indirizzo IP, su cui Apache2 dovrebbe essere in ascolto. Se l'indirizzo IP non è specificato, Apache2 ascolta tutti gli indirizzi IP assegnati alla macchina. Il valore predefinito per la direttiva Listen è 80. Modificare questo valore, in 127.0.0.1:80 per fare in modo che Apache2 ascolti solo l'interfaccia di loopback e non sia disponibile verso internet, in 81 per modificare la porta di ascolto o lasciare il valore predefinito per il normale funzionamento. Questa direttiva può essere trovata e modifica in un file specifico: `/etc/apache2/ports.conf`
- La direttiva *ServerName* è opzionale e specifica a quale FQDN il proprio sito dovrebbe rispondere. L'host virtuale predefinito non ha alcun ServerName specificato, in questo modo tutte le richieste che non corrispondono un'altra direttiva ServerName di un altro host virtuale saranno soddisfatte. Se si ha appena acquistato il dominio ubunturocks.com e si vuole "ospitarlo" sul proprio server Ubuntu, il valore della direttiva ServerName nel file di configurazione dell'host virtuale dovrebbe essere impostato a ubunturocks.com. Aggiungere questa direttiva al file dell'host virtuale appena creato (`/etc/apache2/sites-available/mynewsite`).

  

  Potrebbe essere necessario fare in modo che il proprio sito risponda anche a www.ubunturocks.com, dato che molti utenti ritengono il prefisso "www" appropriato. Per fare questo utilizzare la direttiva *ServerAlias*. È possibile utilizzare anche metacaratteri in questa direttiva. Per esempio, **ServerAlias *.ubunturocks.com** causerà il proprio sito a rispondere a tutte le richieste che finiscono con ".ubunturocks.com".
- La direttiva *DocumentRoot* stabilisce in che posizione il server Apache deve cercare i file che compongono il sito. Il valore predefinito è /var/www. Nessun sito è configurato, se si tolgono i commenti alla direttiva *RedirectMatch* in `/etc/apache2/apache2.conf` le richieste sono indirizzate verso /var/www/apache2-default dove Apache2 è in attesa. Modificare questo valore nel file del proprio host virtuale e creare la directory se necessario.

La directory /etc/apache2/sites-available **non** è analizzata da Apache2. Collegamenti simbolici in /etc/apache2/sites-enabled puntano ai siti disponibili. Per creare questi collegamenti simbolici, utilizzare l'utility a2ensite (Apache2 Enable Site) in questo modo: **sudo a2ensite mynewsite**, dove il file di configurazione del sito è `/etc/apache2/sites-available/mynewsite`. Allo stesso modo l'utility a2dissite dovrebbe essere utilizzata per disabilitare siti.

10.2.2. Impostazioni predefinite

Questa sezione si occupa delle impostazioni predefinite del server Apache2. Per esempio, se viene aggiunto un host virtuale, le impostazioni modificate dell'host virtuale hanno precedenza rispetto quelle dell'host. Per una direttiva non definita, viene utilizzato il valore predefinito.

- *DirectoryIndex* è la pagina predefinita proposta dal server alle richieste dell'indice di una directory, specificate attraverso l'uso di una barra (/) come postfisso al nome della directory.

  Se, per esemio, un utente richiede la pagina http://www.example.com/questa_directory/ otterrebbe ka oagina DirectoryIndex se esiste, una lista di directory generata dal server se è stata specificata l'opzione Indexes o una pagina di "Permesso negato" se nessuna delle opzioni precedenti è abilitata. Il server cerca tra i file elencati nella direttiva DirectoryIndex e visualizza il primo che trova. Se il server non trova nessuno di questi file ed è presente l'opzione OptionsIndexes per quella directory, allora creerà una lista in HTML di tutte le sottodirectory e dei file di tale directory. Il valore predefinito in `/etc/apache2/apache2.conf` è "index.html index.cgi index.pl index.php index.xhtml". Se Apache2 trova un file corrispondente a quelli elencati, visualizza il primo.
- La direttiva *ErrorDocument* consente di specificare un file da utilizzare in caso di errori. Per esempio, se un utente richiede delle risorse inesistenti, si ha un errore 404 e, in base alla configurazione predefinita di Apache2, viene visualizzato il file `/usr/share/apache2/error/HTTP_NOT_FOUND.html.var`. Il file non è elencato in DocumentRoot del server, ma esiste una direttiva Alias in `/etc/apache2/apache2.conf` che indirizza le richeste alla directory /error a /usr/share/apache2/error. Per una lista completa delle direttive predefinite ErrorDocument utilizzare il seguente comando: **grep ErrorDocument /etc/apache2/apache2.conf**
- Il server, in modo predefinito, registra i trasferimenti nel file `/var/log/apache2/access.log`. È possibile cambiare questa impostazione per ogni sito nel file di configurazione dell'host virtuale utilizzando la direttiva *CustomLog* oppure tralasciare tale configurazione per mantenere quella specificata nel file `/etc/apache2/apache2.conf`. Attraverso la direttiva *ErrorLog* è possibile specificare il file in cui vengono registrati gli errori, il valore predefinito è `/var/log/apache2/error.log`. Queste impostazioni sono tenute separate dal log dei trasferimenti per aiutare l'utente nella risoluzione dei problemi. È anche posibile specificare il *LogLevel* (valore predefinito «warn») e *LogFormat* (consultare `/etc/apache2/apache2.conf` per il valore predefinito).
- Alcune opzioni vengono definite in base alle directory piuttosto che in base al server. Una di queste direttive è Option. Una clausola Directory è racchiusa tra dei tag in stile XML, come:

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

```
  ...
</Directory>
```

Le direttive Option, all'interno di una clausola Directory, accettano uno o più dei seguenti valori separati da spazi:

- **ExecCGI** - permette l'esecuzione di script CGI. Questi script non vengono eseguiti se l'opzione non è selezionata.

  

  La maggior parte dei file non dovrebbe essere eseguita come script CGI. Questo potrebbe essere molto pericoloso. Gli script CGI dovrebbero essere tenuti in un directory separata rispetto la DocumentRoot e solo questa directory dovrebbe avere l'opzione ExecCGI abilitata. Questo è il comportamento predefinito e la directory predefinita per gli script CGI è /usr/lib/cgi-bin.
- **Includes** - Abilita inclusioni lato server. Le inclusioni lato server consentono un file HTML a *includere* altri file. Questa noon è un'opzione comune. Consultare l'*Apache2 SSI Howto* [http://httpd.apache.org/docs/2.0/howto/ssi.html] per maggiori informazioni.
- **IncludesNOEXEC** - permette l'inclusione lato server, ma disabilita i comandi #exec e #include negli script CGI.
- **Indexes** - Visualizza una lista dei contenuti della directory, se non esiste alcuna DirectoryIndex (come index.html).

  

  Per motivi di sicurezza, quest'opzione non dovrebbe essere impostata e soprattutto non su DocumentRoot. Abilitare questa opzioni con molta cautela solo su alcune directory e nel caso in cui si desideri poter visualizzare l'intero contenuto della directory.
- **Multiview** - Supporta una visualizzazione multipla in base al contenuto, questa opzione è disabilitata per ragioni di sicurezza. Per maggiori informazioni consultare *la documentazione di Apache2* [http://httpd.apache.org/docs/2.0/mod/mod_negotiation.html#multiviews].
- **SymLinksIfOwnerMatch** - Segue i collegamenti simbolici solamente se il file di arrivo o la directory hanno gli stessi proprietari del collegamento.

10.2.3. Impostazioni degli host virtuali

Gli host virtuali consentono l'esecuzione di diversi server per diversi indirizzi IP, host o per diverse porte sulla stessa macchina. Per esempio, è possibile avere in esecuzione sullo stesso server le pagine web http://www.example.com e http://www.anotherexample.com grazie ai server virtuali. Questa opzione corrisponde alla direttiva <VirtualHost> per l'host virtuale predefinito e per gli host virtuali basati su indirizzo IP. Corrisponde alla direttiva <NameVirtualHost> per un host virtuale basato sul nome.

Le direttive impostate per un host virtuale si applicano solamente a quel particolare host. Se una direttiva è impostata all'interno del server e non è definita nelle impostazioni dell'host virtuale, vengono utilizzate le impostazioni predefinite. Per esempio, è possibile impostare un indirizzo email per il Webmaster e non definirne nessuno per per gli host virtuali.

Impostare la direttiva DocumentRoot in modo che contenga il documento iniziale (come index.html) per l'host virtuale. La DocumentRoot predefinita è `/var/www`.

La direttiva ServerAdmin all'interno di VirtualHost, corrisponde all'indirizzo email utilizzato nel pié di pagina nelle pagine di errore, se ne viene impostata la visualizzazione.

10.2.4. Impostazioni del server

Questa sezione si occupa della configurazione delle impostazioni base del server.

LockFile - La direttiva LockFile imposta il percorso al file di lock utilizzato quando il server viene compilato con USE_FCNTL_SERIALIZED_ACCEPT o USE_FLOCK_SERIALIZED_ACCEPT. Deve essere conservato nel disco locale. Questo valore dovrebbe essere lasciato invariato a meno che la directory di log non sia localizzata su una condivisione NFS. In questo caso, il valore dovrebbe essere modificato con una posizione sul disco locale e una directory accessibile solamente dall'utente root.

PidFile - La direttiva PidFile imposta il file in cui il server registra il proprio «pid». Questo file dovrebbe essere leggibile solamente dall'utente root. Nella maggior parte dei casi può essere lasciata invariata.

User - La direttiva User imposta lo «userid» utilizzato dal server in modo tale che risponda alle richieste. Questa impostazione determina l'accesso al server. Qualsiasi file non accessibile a questo utente è inacessibile anche a chi cerca di visitare il sito. Il valore predefinito è www-data.

A me che non sia estremamente necessario, non impostare mai la direttiva «User» a root. Utilizzare root con «User» può creare una falla nella sicurezza del server Web.

La direttiva Group è simile alla direttiva User. Group imposta il gruppo a cui il server è tenuto a rispondere. Il gruppo predefinito è anche www-data.

10.2.5. I moduli di Apache

Apache è un server modualre. Questo implica che solo le funzionalità di base sono incluse nel server. Maggiori funzionalità possono essere aggiunte tramite il caricamento di moduli specifici. Alcuni moduli sono inclusi nel server durante la fase di compilazione. Se il server viene compilato affinché utilizzi il caricamento dinamico dei moduli, questi moduli possono essere compilati separatamente e caricati nel server tramite la direttiva LoadModule. In caso contrario, è necessario ricompilare Apache per aggiungere o rimuovere un modulo. Ubuntu compila Apache2 in modo tale da poter caricare i moduli dinamicamente. Potrebbe essere necessario includere delle direttive per un particolare modulo, per fare questo è necessario includerle in un blocco del tipo <Module>. È possibile installare altri moduli per Apache2 e utilizzarli per il propio server utilizzando, per esempio, apt-get. Per installare il modulo per l'autenticazioni MySQL, da terminale digitare:

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

Una volta installato il modulo, sarà disponibile all'interno della directory `/etc/apache2/mods-available`. È possibile utilizzare il comando a2enmod per abilitare un modulo o a2dismod per disabilitarne uno. Una volta abilitato un modulo, questo sarà disponibile all'interno della directory `/etc/apache2/mods-enabled`.

10.3. Configurazione HTTPS

Il modulo mod_ssl aggiunge un'importante caratteristica al server Apache2, l'abilità di criptare le comunicazioni. In questo modo, quando il browser utilizza la cifratura SSL per le comunicazioni, il prefisso "https://" viene utilizzato all'inizio dell'URL (Uniform Resource Locator).

Il modulo mod_ssl è disponibile nel pacchetto apache2-common. Se è stato installato questo paccheto, è possibile eseguire, in un terminale, il seguente comando per avviare il modulo mod_ssl:

```
sudo a2enmod ssl
```

10.3.1. Certificati e sicurezza

Per impostare un server sicuro, utilizzare crittografia a chiave pubblica per creare una chiave pubbilca e una privata. Nella maggior parte dei casi, viene inviata la richiesta del ceritificato (compresa la chiave pubblica), una prova dell'identità della società e del pagamento a un Certificate Authority (CA, Autorità di certificazione ndT). CA verifica la richiesta e la propria identità e quindi invia il ceritificato.

In alternativa è possibile creare i propri certificati auto-firmati. I cerificati auto-firmati non dovrebbero essere utilizzati ambito commerciale. I certificati auto-firmati non sono accettati automaticamente dai browser. Agli utenti viene chiesto di accettare il certificato per stabilire una connessione sicura.

Una volta ottenuto un certificato auto-firmato o un certificato da un CA, è necessario installarlo nel proprio server.

10.3.2. Tipologie dei certificati

Per far funzionare un server sicuro sono necessari un certificato e una chiave, questo vuol dire che è possibile generare un certificato auto-firmato o comprarne uno firmato da un CA. Un certificato firmato da un CA fornisce due importanti caratteristiche al server:

- i browser (solitamente) riconoscono automaticamente il certificato e consentono l'attivazione di una connessione sicura senza chiedere nulla all'utente.
- Quando un CA emette un certificato, garantisce l'identità dell'organizzazione che fornisce la pagina web al browser.

La maggior parte dei browser web che supporta SSL possiede una lista di CA i cui certificati vengono accettati automaticamente. Se un browser incontra un certificato il cui CA emittente non è presente all'interno della lista, richiede all'utente se accettare o rifiutare la connessione.

È possibile generare un certificato auto-firmato per il propio server sicuro, ma questo non fornisce le stesse funzionalità di un ceritficato emesso da un CA. Un certificato auto-firmato non viene riconosciuto dai browser web e allo stesso tempo non fornisce nessuna garanzia riguardo l'organizzazione che gestisce il sito web. Un certificato firmato da un CA fornisce invece queste fuzionalità. Il procedimento per ottenere un certificato da un CA è semplice:

1. Creare un coppia di chiavi pubblica e privata.
2. Creare una richiesta per un certificato basato su chiave pubblica. La richiesta del certificato contiene informazioni riguardo il server a la società che lo ospita.
3. Inviare la richiesta, con una fotocopia di un documento di identità, a un CA. Non è possibile consigliare quale autorità di certificazione scegliere. La decisione potrebbe essere basata su epserienze passate, esperienze di amici o colleghi o per un fattore economico.

   una volta deciso il CA, è necessario seguire le istruzioni fornite dal CA per l'ottenimento del certificato.
4. Una volta che il CA ha verificato l'identità del richiedente, invierà un certificato digitale.
5. Installare il certificato sul server per poter utilizzare le connessioni sicure.

Sia che si sita ottenendo un certificato da un CA sia che si auto-firmi il proprio, il primo passo consiste nel generare una chiave di cifratura.

10.3.3. Generazione di un CSR (Certificate Signing Request)

Per generare un CSR (Certificate Signing Request), è necessario creare una chiave. Per generare una chiave, da terminale, digitare:

```
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:
```

È ora necessario inserire una passphrase. Per una maggiore sicurezza, dovrebbe contenere almeno 8 caratteri. La lunghezza minima con l'opzione "-des3" è di 4 caratteri. Dovrebbe includere numeri e/o segni di punteggiatura e non dovrebbe essere una parola reperibile in un vocabolario. Ricordarsi che la passphrase è "case-sensitive".

Ripetere la passphrase per la verifica. Una volta inserita correttamente, la chiave per il server è generata e salvata nel file `server.key`.

È possibile utilizzare il server sicuro anche senza una passphrase. Può essere utile in quanto non viene richiesta la passphrase a ogni riavvio del server. Ma è altamente insicuro in quanto se viene compromessa la chiave è possibile compromettere l'integrità del server.

È comunque possibile utilizzare il server sicuro senza la passphrase, non utilizzando l'opzione «-des3» durante la fase di creazione della chiave o eseguendo il seguente comando:

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

Una volta eseguito il comando precedente, la chiave non sicura è creata nel file `server.key.insecure`. È possibile utilizzare questo file per generare il CSR senza una passphrase.

Per creare il CSR, eseguire il seguente comando:

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

Viene richiesta la passphrase. Se viene inserita correttamente, è necessario inserire alcune informazioni come nome della società, nome del sito, email, ecc.... Una volta forniti tutti i dati, il CSR è creato nel file `server.csr`. È possibile inviare questo CSR a un CA per la ceritificazione, il quale utilizzarà questo CSR per emettere il certificato. È anche possibile utilizzare il CSR per creare certificati auto-firmati.

10.3.4. Creare un certificato auto-firmato

Per creare un certificato auto-firmato, eseguire da un terminale il seguente comando:

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

Il comando precedente chiederà la passphrase. Una volta digitata correttamente, il certificato viene creato e sarà disponibile nel file `server.crt`.

Se il server deve essere utilizzato in ambito commerciale, è necessario un certificato emesso da un CA. Non è raccomandato utilizzare un certificato auto-firmato.

10.3.5. Installare il certificato

Per installare il file della chiave `server.key` e il file del certificato `server.crt` o il certificato emesso dal CA, eseguire i seguenti comandi da un terminale:

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

È necessario anche aggiungere le seguenti quattro righe al file `/etc/apache2/sites-available/default` o al file di configurazione dell'host virtuale. Vanno collocate nella sezione *VirtualHost* sotto la riga *DocumentRoot*:

```
SSLEngine on

SSLOptions +FakeBasicAuth +ExportCertData +CompatEnvVars +StrictRequire
```

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

HTTPS dovrebbe essere in ascolto sulla porta 443. È necessario aggiungere la seguente riga al file `/etc/apache2/ports.conf`:

```
Listen 443
```

10.3.6. Accedere al server

Una volta installato il certificato è necessario riavviare il server web. Per fare ciò, da un terminale digitare:

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

Ricordarsi la propria passphrase da inserire a ogni riavvio del server web.

Viene richiesta la passphrase. Una volta digitata correttamente, il server web sicuro viene avviato. È possibile accedere alle pagine sicure del server digitando nella barra degli indirzzi del browser https://nome_host/url.

10.4. Riferimenti

Documentazione di Apache2 [http://httpd.apache.org/docs/2.0/]

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

11. Squid - Server proxy

Squid è un potente proxy cache server che fornisce servizi proxy e cache per HTTP (Hyper Text Transport Protocol), FTP (File Transfer Protocol) e molti altri protocolli di rete. Squid può implementare servizi di caching e proxy anche per richieste SSL (Secure Sockets Layer), caching per ricerche di DNS (Domain Name Server) e fornire un caching trasparente. Squid supporta molti protocolli per il caching come ICP (Internet Cache Protocol), HTCP (Hyper Text Caching Protocol), CARP (Cache Array Routing Protocol) e WCCP (Web Cache Coordination Protocol).

Il server Squid è una valida soluzione per le necessità di caching e proxy, scala dall'utilizzo in un piccolo ufficio fino alla grande impresa, fornendo, attraverso il protocollo SNMP (Simple Network Management Protocol), un meccanismo di controllo e monitoraggio dei parametri critici molto accurato. Nella selezione di un computer da utilizzare come procy Squid dedicato, o come server cache, assicurarsi che il sistema sia equipaggiato con una grande quantità di memoria fisica, dal momento che Squid mantiene un cache in memoria per aumentare le prestazioni.

11.1. Installazione

Per installare il server Squid, da terminale digitare:

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

11.2. Configurazione

La configurazione di Squid avviene attraverso la modifica di alcune direttive presenti nel file `/etc/squid/squid.conf`. Gli esempi che seguono descrivono alcune delle direttive che possono essere modificate. Per maggiori informazioni sulla configurazione di Squid consultare la sezione «Riferimenti».

Prima di modificare il file di configurazione, è utile farne una copia e proteggerla dalla scrittura così, in caso di necessità, si può utilizzare il file originale.

Copiare il file `/etc/squid/squid.conf` e proteggerlo dalla scrittura utilizzando il seguente comando:

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

- Per impostare il server Squid affinché sia in ascolto sulla porta 8888 invece che sulla porta predefinita 3128, modificare la direttiva http_port:

  http_port 8888
- Modificare la direttiva visible_hostname per dare a Squid uno specifico hostname. Questo nome non deve essere necessariamente il nome del computer. Nell'esempio seguente è impostato a *weezie*

visible_hostname weezie

- Inoltre, utilizzando il sistema di controllo degli accessi di Squid, è possibile configurare l'utilizzo di alcuni servizi internet in proxy con Squid solo per alcuni utenti con specifici indirizzi IP. L'esempio seguente descrive come consentire l'accesso algi utenti della sottorete 192.168.42.0/24:

  Aggiungere quanto segue alla **fine** della sezione ACL del file `/etc/squid/squid.conf`:

  acl fortytwo_network src 192.168.42.0/24

  Quindi aggiungere quanto segue all'**inizio** della sezione http_access del file `/etc/squid/squid.conf`:

  http_access allow fortytwo_network
- Utilizzando il sistema di controllo degli accessi di Squid, è possibile configurare l'utilizzo di alcuni servizi internet in proxy con Squid in alcune fasce orarie: L'esempio seguente descrive come consentire agli utenti l'accesso al servizio dalle 9:00 alle 17:00 dal lunedì al venerd' che utilizza la sottorete 10.1.42.0/42:

  Aggiungere quanto segue alla **fine** della sezione ACL del file `/etc/squid/squid.conf`:

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

  Quindi aggiungere quanto segue all'**inizio** della sezione http_access del file `/etc/squid/squid.conf`:

  http_access allow biz_network biz_hours

Una volta apportate modifiche al file `/etc/squid/squid.conf`, salvare il file e, per rendere effetivi i cambiamenti, riavviare squid utilizzando il comando:

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

11.3. Riferimenti

Sito web di Squid [http://www.squid-cache.org/]

12. Ssitemi per il controllo della versione

Il controllo della versione è l'arte della gestione dell'evolversi delle informazioni. È stato a lungo uno strumento critico per i programmatori, che spendono il loro tempo apportando piccole modifiche al software per poi cancellarle il giorno seguente. Ma l'utilità del software per il controllo della versione va oltre il mondo dello sviluppo di programmi. Ovunque si incontrino persone che utilizzino il computer per gestire informazioni in continuo cambiamento c'è posto per il controllo della versione.

12.1. Subversion

Subversion è un software open source per il controllo della versione. Utilizzando Subversion è possibile registrare la storia del codice sorgente e dei documenti. È in grado di gestire l'evolversi di file e directory nel tempo. Nel repository centrale viene posizionato un albero di tutti i file. Il repository è come un server di file, tranne per il fatto che si ricorda qualsiasi cambiamento apportato.

12.1.1. Installazione

Per accedere al repository di Subversion utilizzando il protocollo HTTP, è necessario installare e configurare un server web. Apache2 funziona molto bene con Subversion. Fare riferimento alla sottosezione HTTP nella sezione Apache2 per installare e configurare un certificato digitale.

Per installare Subversion, in un terminale, digitare:

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

12.1.2. Configurazione del server

I passi seguenti presumono siano stati installati i pacchetti elencati precedentemente. Questa sezione descrive come creare un repository con Subversion e accedere al progetto.

12.1.2.1. Creare un repository con Subversion

Un repository può essere creato con il seguente comando:

```
svnadmin create /posizione/del/repository/project
```

12.1.3. Metodi di accesso

È possibile accedere ai repository di Subversion in molti modi, dal disco locale o attraverso diversi protocolli di rete. La posizione di un repository è comunque sempre un URL. La tabella seguente descrive come i diversi schemi URL corrispondano ai metodi di accesso disponibili.

Tabella 4.1. Metodi di accesso

Schema	Metodo di accesso
file://	Accesso diretto al repository (sul disco locale)
http://	Accesso attraverso il protocollo WebDAV al server web Apache2 di Subversion
https://	Come http://, ma con cifratura SSL
svn://	Accesso attraverso un protocollo personalizzato a un server svnserve
svn+ssh://	Come svn://, ma attraverso un tunnel SSH

In questa sezione viene descritto come configurare Subversion per tutti questi metodi. Saranno descritte solo gli elementi basilari. Per maggiori dettagli, fare riferimento al *libro di svn* [http://svnbook.red-bean.com/].

12.1.3.1. Accesso diretto al repository (file:///)

Questo è il metodo di accesso più semplice. Non necessita di alcun server di Subversion in esecuzione. Questo metodo serve per accedere a Subversione dalla stessa macchina in cui è in esecuzione. La sintassi del comando è la seguente:

```
svn co file:///percorso/del/repository/progetto
```

o

```
svn co file://localhost/percorso/del/repository/progetto
```

Se non viene specificato l'host, è necessario utilizzare tre slash (///), due per il protocollo (in questo caso file) e uno è lo slash iniziale del percorso. Se viene specificato l'host, utilizzare due slash (//).

I permessi di accesso al repository dipendono dai permessi impostati nel file system. Se l'utente possiede i permessi di scrittura e lettura, allora potrà eseguire checkout e commit al repository.

12.1.3.2. Accesso con il protocollo WebDAV (http://)

Per accedere la repository di Subversion utilizzando il protocollo WebDAV, è necessario configurare il server web Apache2. Aggiungere quanto segue al file `/etc/apache2/apache2.conf`:

```
<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>
```

È quindi necessario creare il file `/etc/subversion/passwd`. Questo file contiene le informazioni per l'autenticazione dell'utente. Per aggiungere una voce, per aggiungere un utente, è possibile utilizzare il seguente comando:

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

Verrà richiesta la password. Una volta inerita, l'utente viene aggiunto al file. Ora, per accedere al repository, digitare:

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

La password viene trasmessa come testo in chiaro. Per evitare attacchi di tipo password snooping, è necessario utilizzare la cifratura SSL. Per maggiori informazioni fare riferimento alla sezione seguente.

12.1.3.3. Accesso con protocollo WebDAV protetto da cifratura SSL (https://)

L'accesso al repository di Subversion attraverso il protocollo WebDAV con cifratura SSL (https://) è simile a http:// tranne per il fatto che è necessario installare e configurare un certificato digitale per il server Apache2.

È possibile installare un certificato digitale emesso da un'autorità di certificazione come Verisign. In alternativa è possibile installare i propri certificati auto-firmati.

I passi seguenti hanno come presupposto l'installazione di un certificato digitale all'interno del server web Apache2. Ora, per accedere a un repository Subversion, fare riferimento alla sezione precedente. I metodi di accesso sono esattamente gli stessi, tranne il protocollo. È necessario utilizzare https:// per accedere al repository.

12.1.3.4. Accesso con il protocollo personalizzato (svn://)

Una volta creato il repository è possibile configurare il controllo degli accessi modificando il file `/path/to/repos/project/conf/svnserve.conf`. Per esempio, per impostare l'autenticazione, togliere i commenti alle seguenti righe presenti nel file di configurazione:

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

Dopo aver tolto i commenti alle righe precedenti, è possibile gestire la lista degli utenti nel file passwd. Modificare il file `passwd` presente nella directory e inserire il nuovo utente. La sintassi da usare è la seguente:

```
username = password
```

Per maggiori informazioni fare riferimento al file.

Per accedere a Subversion attraverso il protocollo svn://, sia dalla stessa macchina sia da un'altra macchina, avviare svnserver utilizzando il comando svnserve. La sintassi è la seguente:

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

Per ulteriori dettagli sull'utilizzo fare riferimento a:
$ svnserve --help
```

Una volta eseguito questo comando, Subversion si mette in ascolto sulla porta predefinita (3690). Per accedere al repository del progetto, è necessario eseguire, da un terminale, il seguente comando:

```
svn co svn://hostname/project project --username nome_utente
```

In base alla configurazione del server, verrà richiesta la password. Una volta autenticati, viene eseguito il check out del codice dal repository di Subversion. Per sincronizzare il repository del progetto con la copia locale, è possibile eseguire il comando **update**. La sintassi del comando è la seguente:

```
cd project_dir ; svn update
```

Per maggiori informazioni sui sotto comandi di Subversion fare riferimento al manuale. Per esempio, per informazioni sul comando co (checkout), al prompt dei comandi digitare:

```
svn co help
```

12.1.3.5. Accesso con protocollo personalizzato a cifratura SSL (svn+ssh://)

La configurazione e le procedure sono le medesime del metodo svn:// . Per i dettagli consultare la sezione precedente. Questo passaggio prevede che si sia seguita la procedura precedente e il server Subversion sia stato avviato con il comando svnserve.

Si suppone che il server ssh sia in esecuzione sulla macchina e che accetti connessioni in entrata. Per una conferma, provare a collegarsi alla macchina attraverso SSH. Se il login viene eseguito, tutto è configurato. In caso contrario configurare SSH.

Il protocollo svn+ssh:// è utilizzato per accedere al repository di Subversion usando la cifratura SSL. I dati che vengono trasmessi sono cifrati con questo metodo. Per accedere al repository del progetto (per esempio attraverso un checkout), utilizzare, con il comando, la sintassi seguente:

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

È necessario utilizzare il percorso completo (/path/al/repository/progetto) per accedere al repository di Subversion utilizzando questo metodo di accesso.

In base alla configurazione del server, viene richiesta la password. Utilizzare la password per il login con SSH. Una volta autenticati, viene fatto il checkout del codice dal repository di Subverison.

12.2. Server CVS

CVS è un sistema di controllo della versione. È possibile utilizzarlo per registrare i cambiamenti al codice sorgente di un programma.

12.2.1. Installazione

Per installare cvs al prompt dei comandi digitare:

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

Dopo aver installato cvs, si dovrebbe installare xinetd per avviare o fermare il server cvs. Per installare xinetd digitare:

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

12.2.2. Configurazione

Una volta installato CVS, il repository viene automaticamente inizializzato. In modo predefinito, risiede nella directory /var/lib/cvs. È possbile modificare questo percorso attraverso il seguente comando:

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

Una volta configurato il repository iniziale, è possibile configurare xinetd per avviare il server CVS. È possibile copiare le seguetni righe nel file `/etc/xinetd/cvspserver`.

```
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
}
```

Assicurarsi di modificare il repository nel caso in cui si sia modificata la directory predefinita del repository (/var/lib/cvs).

Quando si è configurato anche xinetd è possibile avviare il server CVS con il seguente comando:

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

Per avere la conferma che il server CVS sia avviato digitare il seguente comando:

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

L'output del comando precedente dovrebbe essere:

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

A questo punto è possibile aggiungere altri utenti, nuovi progetti e gestire il server CVS.

CVS consente di aggiungere nuovi utenti indipendentemente dal sistema operativo. Il modo più semplice è utilizzare l'utente Linux per CVS, benché presenti dei problemi di sicurezza. Consultare il manuale di CVS per maggiori dettagli.

12.2.3. Aggiungere progetti

Questa sezione illustra come aggiungere nuovi progetti a un repository CVS, creare la directory, aggiungervi i documenti necessari e i file sorgente. A questo punto, eseguire le seguenti istruzioni per aggiungere un progetto al repository CVS:

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

È possibile utilizzare la variabile d'ambiente CVSROOT per memorizzare la directory root d iCVS. Una volta esportata la variabile CVSROOT, si può evitare di utilizzare l'opzione -d nel comando precedente.

. La stringa *new_project*, è un tag di vendita, mentre la stringa *start* è una stringa di rilascio. Non servono a nulla nel contesto presente, ma visto che CVS le richiede, vanno inserite.

Quando si aggiunge un nuovo progetto, l'utente CVS deve avere i permessi di scrittura per il repository CVS (/var/lib/cvs). In modo predefinito, il gruppo src possiede tali permessi. Basta semplicemente aggiungere l'utente a questo gruppo per permettergli di gestire progetti in un repository CVS.

12.3. Riferimenti

Home page di Subversion [http://subversion.tigris.org/]

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

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

13. Database

Ubuntu fornisce due server per database:

- MySQL™
- PostgreSQL

Sono diponibili nel repository «main». Questa sezione descrive come installare e configurare entrambi questi database.

13.1. MySQL

MySQL è un robusto database SQL multi-thread e multi-utente. È concepito per funzionare in situazioni critiche, sistemi a elevato carico e anche per essere inserito in sistemi embedded.

13.1.1. Installazione

Per installare MySQL, eseguire i seguenti comando dal terminale:

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

Una volta completata l'installazione, il server MySQL dovrebbe avviarsi automaticamente. È possibile digitare i seguenti comandi in un terminale per controllare se il server è in esecuzione:

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

L'output del comando precedente dovrebbe essere:

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

Se il server non funziana correttamente, è possibile digitare i seguenti comandi per avviarlo:

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

13.1.2. Configurazione

In modo predefinito la password di amministratore non è impostata. Una volta installato MySQL, la prima cosa da fare è configurare tale password. Per farlo, eseguire i seguenti comandi:

```
sudo mysqladmin -u root password nuovapasswordrootsql
```

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

E' possibile editare il file `/etc/mysql/my.cnf` per configurare le impostazioni di base -- file di log, numeri di porta, ecc. Fare riferimento al file `/etc/mysql/my.cnf` per ulteriori dettagli.

13.2. PostgreSQL

PostgreSQL è un database relazionale orientato agli oggetti che presenta le caratteristiche di un database commerciale tradizionale e anche miglioramenti dei sistemi DBMS di prossima generazione.

13.2.1. Installazione

Per installare PostgreSQL, eseguire i seguenti comandi dal terminale:

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

Una volta che l'installazione è completata, è possibile configurare il server PostgreSQL a seconda delle proprie esigenze, sebbene la configurazione predefinita sia abbastanza buona.

13.2.2. Configurazione

In modo predefinito, la connessione attraverso il protocollo TCP/IP è disabilitata. PostrgreSQL supporta diversi metodi di autenticazione. Quello predefinito è il metodo IDENT. Consultare *la guida della'mministratore PostgreSQL* [http://www.postgresql.org/docs/8.1/static/admin.html].

I passi seguenti assumono che si voglia abilitare la connessione TCP/IP e che si desideri utilizzare il metodo di autenticazione MD%. I file di configurazione di PostgreSQL sono nella directory `/etc/postgresql/<version>/main`. Per esempio, se si installa PostgreSQL 7.4, i file di configurazione sono nella directory `/etc/postgresql/7.4/main`.

Per configurare l'autenticazione ident, aggiungere delle voci nel file `/etc/postgresql/7.4/main/pg_ident.conf`.

Per abilitare le connessioni TCP/IP, modificare il file `/etc/postgresql/7.4/main/postgresql.conf`

Localizzare la riga *#tcpip_socket = false* e modificarla in *tcpip_socket = true*. Tutti gli altri parametri possono essere modificati, ma bisogna sapere cosa si sta facendo! Per maggiori informazioni, consulatere la documentazione di PostgresSQL o fare riferimento ai file di configurazione.

Le credenziali dell'utente, in modo predefinito, non sono impostate per l'autenticazione *MD5*. È quindi necessario, per prima cosa, configurare il server PostgreSQL all'utilizzo dell'autenticazione *trust*, connettersi al database, configurare la password e ripristinare la configurazione affinché utilizzi l'autenticazione *MD5*. Per attivare l'autenticazione *trust*, modificare il file `/etc/postgresql/7.4/main/pg_hba.conf`.

Togliere il commento a tutte le righe che contengono l'identificazione *ident* e *MD5*, quindi aggiungere la seguente riga:

```
local all postgres trust sameuser
```

Eseguire i seguenti comandi per avviare il server PostgreSQL:

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

Una volta che il server PostgreSQL è avviato con successo, eseguire i seguenti comandi in un terminale per collegarsi al database template predefinito di PostgreSQL

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

Il comando precedente connette al database PostreSQL *template1* come l'utente *postgres*. Una volta collegati al server PostgreSQL, si sarà al prompt SQL. È possibile eseguire il seguente comando SQL al prompt psql per configurare la password per l'utente *postgres*.

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

Una volta configurata la password, modificare il file `/etc/postgresql/7.4/main/pg_hba.conf` per utilizzare l'autenticazione *MD5*:

Commentare la riga *trust* recentemente aggiunta e aggiungere la seguente:

```
local all postgres md5 sameuser
```

La configurazione sopra indicata non è completa. Per la configurazione di altri parametri fare riferimento alla *guida dell'amministratore di PostgreSQL* [http://www.postgresql.org/docs/8.1/static/admin.html].

14. Servizi email

Il processo per portare una email da una persona a un'altra all'interno di una rete o attraverso internet, comporta l'utilizzo di diversi sistemi che cooperano tra loro. Ognuno di questi sistemi deve essere configurato correttamente. Colui che spedisce una email utilizza un *Mail User Agent* (MUA), o client email, per spedire il messaggio attraverso uno o più *Mail Transfer Agents* (MTA), l'ultimo dei quali lo consegnerà a un *Mail Delivery Agent* (MDA) per la consegna nella casella di posta del destinatario, che la preleverà utilizzando un client email attraverso un server POP3 o IMAP.

14.1. Postfix

Postfix è il Mail Transfer Agent (MTA) predefinito di Ubuntu. Cerca di essere facile da amministrare e sicuro ed è compatibile con l'MTA sendmail. Questa sezione espone come installare e configurare postfix e anche come configurare un server SMTP utilizzando un collegamento sicuro (per l'invio di email in sicurezza).

14.1.1. Installazione

Per installare postfix con SMTP AUTH e TLS (Transport Layer Security) eseguire il seguente comando:

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

Premere Invio a ogni domanda posta durante il processo di installazione, la configurazione sarà svolta al passo successivo.

14.1.2. Configurazione di base

Per configurare postfix eseguire il seguente comando:

```
sudo dpkg-reconfigure postfix
```

Sarà visualizzata l'interfaccia grafica. A ogni schermata selezionare i seguenti valori:

- Ok
- Internet Site
- NONE
- mail.example.com
- mail.example.com, localhost.localdomain, localhost
- No
- 127.0.0.0/8
- Sì
- 0
- +

- tutti

Sostituire mail.example.com con il nome del proprio host server.

14.1.3. Autenticazione SMTP

I passi successivi sono la configurazione di postfix per l'uso di SASL per SMTP AUTH. Invece di modificare i file di configurazione a mano, è possibile utilizzare lo strumento **postconf** per impostare tutti i parametri di postfix. I parametri di configurazione vengono salvati nel file `/etc/postfix/main.cf`. Per riconfigurare un particolare parametro è possibile utilizzare nuovamente il comando precedente o modificare il file a mano.

1. Configurare Postfix per l'esecuzione di SMTP AUTH utilizzando SASL (saslauthd):

```
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_
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. Quindi, configurare i certificati digitali per TLS. Quando vengono poste delle domande, seguire le istruzioni e rispondere correttamente.

```
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/
```

È possibile ottenere un certificato digitale da un ente che distrubuisce certificati. In alternativa è possibile crearsi i propri certificati. Per maggiori informazioni fare riferimento a *Sezione 10.3.4, «Creare un certificato auto-firmato» [53]*.

3. Configurare Postfix affinché esegua cifratura TLS sia per le email in arrivo sia per quelle in uscita:

```
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'
```

Una volta eseguiti tutti i comandi, SMTP AUTH è configurato per postfix. Il certificato auto-firmato è creato per TLS ed è configurato per l'uso con postfix.

Ora, il file `/etc/postfix/main.cf` dovrebbe essere simile a *questo* [../sample/postfix_configuration].

La configurazione iniziale di postfix è completata. Eseguire il seguente comando per avviare il demone postfix:

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

Ora il demone postfix è installato, configurato e funziona correttamente. Postfix supporta anche SMTP AUTH come descritto in *RFC2554* [ftp://ftp.isi.edu/in-notes/rfc2554.txt]. È basato su *SASL* [ftp://ftp.isi.edu/in-notes/rfc2222.txt], ma è necessario abilitare l'autenticazione SASL prima di poter utilizzare SMTP.

14.1.4. Configurare SASL

Le applicazioni libsasl2, sasl2-bin e libsasl2-modules sono necessarie per abilitare l'utilizzo di SASL con SMTP AUTH. È possibile installare queste applicazioni se non lo si è già fatto.

```
apt-get install libsasl2 sasl2-bin
```

È necessario apportare alcune modifice prima di un corretto funzionamento. Questo perché Postfix viene eseguito in chroot su `/var/spool/postfix`, SASL necessita di essere configurato per poter girare nella falsa root (`/var/run/saslauthd` diventa `/var/spool/postfix/var/run/saslauthd`):

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

Per attivare saslauthd, modificare il file `/etc/default/saslauthd` e cambiare o aggiungere la variabile START. Per configurare saslauthd affinché possa girare nella falsa root, aggiungere le variabili PWDIR, PIDFILE e PARAMS. Infine configurare la variabile MECHANISMS a piacere. Il file dovrebbe essere all'incirca come questo:

```
# 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"
```

È possibile utilizzare **shadow** al posto di **pam**. Questo utilizzerà il trasferimento delle password con l'hashing MD5 ed è perfettamente sicuro. Il nome utente e la password necessari per l'autenticazione sono quelle dell'utente nel sistema in uso.

Aggiornare lo "stato" di `/var/spool/portfix/var/run/saslauthd`. Lo script init di saslauthd utilizza queste impostazioni per creare la directory mancante con i permessi appropriati:

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

14.1.5. Test

La configurazione di SMTP AUTH è completata. Ora è necessario avviare il tutto ed eseguire dei test. Per avviare il demone SASL utilizzare il seguente comando:

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

Per controllare se SMTP AUTH e TLS funzionano perfettamente, eseguire il seguente comando:

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

Una volta stabilito il collegamento con il server postfix, digitare:

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

Se compaiono le seguenti righe, allora tutto è a posto. Digitare **quit** per uscire.

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

14.2. Exim4

Exim4 è un altro MTA (Message Transfer Agent) sviluppato dalla Cambridge University per essere utilizzato nei sistemi Unix collegati in Internet. Exim può essere installato al posto di sendmail, sebbene la configurazione di exim sia un po' diversa da quella di sendmail.

14.2.1. Installazione

Per installare exim4, digitare il seguente comando:

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

14.2.2. Configurazione

Per configurare exim4, eseguire il seguente comando:

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

Viene visualizzata l'interfaccia grafica. Questa consente di configurare molti parametri. Per esempio, in exim4 i file di configurazione sono suddivisi in molti file, se si vuole avere un unico file è possibile impostare ciò all'interno di questa interfaccia.

Tutti i parametri impostati all'interno dell'interfaccia grafica sono salvati nel file `/etc/exim4/update-exim4.conf.conf`. Se si desidera rieseguire la configurazione è possibile rieseguire il wizard di configurazione o modificare manualmente il file utilizzando l'editor di testo preferito. Una volta configurato, è possibile utilizzare il seguente comando per generare il file di configurazione principale:

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

Questo file, una volta creato, è salvato in `/var/lib/exim4/config.autogenerated`.

Per nessun motivo modificare il file `/var/lib/exim4/config.autogenerated`. È aggiornato automaticamente ogni volta che viene eseguito il comando **update-exim4.conf**

Per avviare il demone exim4 utilizzare il seguente comando: **sudo /etc/init.d/exim4 start**

14.3. Server Dovecot

Dovecot è un Mail Delivery Agent, progettato per garantire la sicurezza. Supporta la maggior parte dei formati di caselle di posta: mbox o maildir. Questa sezione espone come configurarlo come server imap o pop3.

14.3.1. Installazione

Per installare dovecot eseguire in un terminale il seguente comando:

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

14.3.2. Configurazione

Per configurare dovecot è possibile modificare il file `/etc/dovecot/dovecot.conf`. È possibile utilizzare il protocollo preferito. Può essere pop3, pop3s (pop3 sicuro), imap e imaps (imap sicuro). Una descrizione di questi protocolli va oltre lo scopo di questa guida. Per maggiori informazioni fare riferimento agli articoli presenti su wikipedia riguardo *POP3* [http://en.wikipedia.org/wiki/POP3] e *IMAP* [http://en.wikipedia.org/wiki/Internet_Message_Access_Protocol].

IMAPS e POP3S sono molto più sicuri rispetto IMAP e POP3 perché utilizzano la cifratura SSL durante la connessione. Una volta scelto il protocollo, modificare la seguente riga nel file `/etc/dovecot/dovecot.conf`:

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

Questo abilita i protocolli all'avvio di dovecot. Quindi aggiungere le seguenti righe nella sezione pop3 del file `/etc/dovecot/dovecot.conf`:

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

Selezionare la tipologia di casella di posta. Dovecot supporta i formati **maildir** e **mbox**. Questi sono i formati più utilizzati, hanno i loro pregi e i loro difetti. Per maggiori informazioni consultare il *sito web di dovecot* [http://dovecot.org/doc/configuration.txt].

Una volta scelta la tipologia della casella di posta, modificare il file `/etc/dovecot/dovecot.conf` e cambiare la seguente riga:

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

È necessario configurare l'MTA (Mail Transport Agent) per trasferire le email in arrivo in questo tipo di casella, se diversa da quella configurata.

Una volta configurato dovecot, avviare il demone dovecot per testare la configurazione:

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

Se è stato abilitato il supporto imap o pop3 è possibile effettuare il login con i comandi **telnet localhost pop3** o **telnet localhost**. Se l'output è simile a questo, l'installazione ha avuto successo:

```
telnet localhost pop3
Trying 127.0.0.1...
Connected to localhost.localdomain.
Escape character is '^]'.
+OK Dovecot ready.
```

14.3.3. Configurazione di Dovecot SSL

Per configurare dovecot affinché utilizzi SSL, è possibile modificare il file `/etc/dovecot/dovecot.conf` e cambiare le seguenti righe:

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

I file **cert** e **key** sono creati automaticamente da dovecot durante l'installazione. Notare che queste chiavi non sono firmate e si riceverà un errore di "bad signature" quando ci si collega da un client. Per ovviare a questo problema, è possibile utilizzare dei certificati commerciali o, meglio ancora, i propri certificati SSL.

14.3.4. Configurazione del firewall per un server email

Per accedere al server mail da un altro computer, è necessario configurare il firewall affinché consenta i collegamenti al server sulle porte necessarie.

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

14.4. Mailman

Mailman è un programma open source per la gestione di discussioni elettroniche e newsletter. Molte mailing list open source (incluse tutte le mailing list di *Ubuntu* [http://lists.ubuntu.com]) utilizzano Mailman come software. È molto potente e facile da installare.

14.4.1. Installazione

Mailman fornisce un'interfaccia web per i compiti amministrativi e per gli utenti. È quindi richiesto apache con il supporto mod_perl. Mailman utilizza un server mail esterno per inviare e ricevere le email. Funziona molto bene con i seguenti server mail:

- Postfix
- Exim
- Sendmail
- Qmail

Verrà descritto come installare mailman, il server web apache e il server mail Exim. Se si desidera installare mailman con un server mail diverso, fare riferimento alla sezione «Riferimenti».

14.4.1.1. Apache2

Per installare apache2 fare riferimento a *Sezione 10.1, «Installazione» [46]*.

14.4.1.2. Exim4

Per installare Exim4 digitare i seguenti comandi in un terminale:

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

Una volta installato exim4, tutti i file di configurazione sono contenuti nella directory `/etc/exim4`. In Ubuntu, in modo predefinito, i file di configurazione sono suddivisi in diversi file. È comunque possibile cambiare questo comportamento modificando la seguente variabile all'interno del file `/etc/exim4/update-exim4.conf`:

- dc_use_split_config='true'

14.4.1.3. Mailman

Per installare mailman, in un terminale digitare il seguente comando:

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

Questo copia i file di installazione nella directory `/var/lib/mailman, gli script CGI nella directory /usr/lib/cgi-bin/application, crea l'utente list e il gruppo list. Il proprietario del processo mailman sar`

14.4.2. Configurazione

Questa sezione assume che le applicazioni mailman, apache2 e exim4 siano state installate con successo. Ora è necessario configurarle.

14.4.2.1. Apache2

Una volta installato apache2, è possibile aggiungere le seguenti righe al file `/etc/apache2/apache2.conf`:

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

mailman utilizza apache2 per eseguire gli script CGI. Gli script CGI di mailman sono installati all'interno della directory `/usr/lib/cgi-bin/mailman`. L'URL di mailman quindi risulta http://hostname/cgi-bin/mailman/. È possibile apportare cambiamenti al file `/etc/apache2/apache2.conf` per modificarne il comportamento.

14.4.2.2. Exim4

Una volta installato Exim4, è possibile avviare il server exim digitando il seguente comando in un terminale:

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

Per poter utilizzare mailman con exim4, è necessario configurare exim4 per questo scopo. Come precedentemente detto, in modo predefinito, exim4 utilizza file di configurazione multipli di diversi tipi. Per maggiori informazioni fare riferimento al sito web di *Exim* [http://www.exim.org]. Per avviare mailman è necessario aggiungere un nuovo file di configurazione alle seguenti tipologie di configurazione:

- Main
- Transport
- Router

Exim crea un file di configurazione principale ordinando tutti questi piccoli file di configurazione. L'ordine di questi file è molto importante.

14.4.2.3. Main

Tutti i file di configurazione appartenenti al tipo main sono archiviati nella directory `/etc/exim4/conf.d/main/`. È possibile aggiungere il seguente contenuto a un nuovo file di configurazione chiamato `04_exim4-config_mailman`:

```
# 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

Tutti i file di configurazione appartenenti al tipo transport sono archiviati nella directory `/etc/exim4/conf.d/transport/`. È possibile aggiungere il seguente contenuto a un nuovo file di configurazione chiamato `40_exim4-config_mailman`:

```
  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

Tutti i file di configurazione appartenenti al tipo router sono archiviati nella directory `/etc/exim4/conf.d/router/`. È possibile aggiungere il seguente contenuto a un nuovo file di configurazione chiamato `101_exim4-config_mailman`:

```
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
```

L'ordine dei file di configurazione main e transport può essere qualsiasi. L'ordine dei file di configurazione del tipo router deve essere lo stesso. Questo particolare file deve apparire prima del file `200_exim4-config_primary`. Questi file contengono le stesse informazioni, ma il primo ha la precedenza. Per maggiori informazioni fare riferimento alla sezione «Riferimenti».

14.4.2.6. Mailman

Una volta installato mailman è possibile avviarlo digitando il seguente comando:

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

Quindi, è necessario creare la mailing list di base. Digitare il seguente comando per creare la mailing list:

```
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..

#
```

Dato che è stato configurato exim al riconoscimento di tutte le email in arrivo da mailman, non è necessario inserire altre voci nel file `/etc/aliases`. Se sono state fatte modifiche a file di configurazione, assicurarsi di riavviare i servizi modificati prima di continuare.

14.4.3. Amministrazione

Si assume una installazione predefinita. Gli script CGI di mailman sono all'interno della directory /usr/lib/cgi-bin/mailman/. mailman fornisce uno strumento di amministrazione basato sul web. Per accedere a questa pagina indirizzare il browser web al seguente URL:

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

La mailing list predefinita, *mailman*, compare a schermo. Facendo clic clic sul nome, viene chiesta la password di autenticazione. Una volta inserita la password corretta è possibile modificare le impostazioni della mailing list. È possibile creare una nuova mailing list utilizzando le utility a riga di comando (**/usr/sbin/newlist**). In alternativa, è possibile creare una nuova mailing list tramite l'interfaccia web.

14.4.4. Utenti

Mailman fornisce un'interfaccia web per gli utenti. Per accedere a questa pagina, indirizzare il browser web al seguente URL:

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

La mailing list predefinita, *mailman*, compare a schermo. Facendo clic sul nome, viene presentato il modulo di iscrizione. È possibile inserire il proprio indirizzo email, il nome (opzionale) e la password per completare l'iscrizione. Viene così inviata una email di invito all'indirizzo specificato. È possibile seguire le istruzioni contenute nell'email per completare l'iscirzione.

14.4.5. Riferimenti

GNU Mailman - Manuale di installazione [http://www.list.org/mailman-install/index.html]

HOWTO - Using Exim 4 and Mailman 2.1 together [http://www.exim.org/howto/mailman21.html]

Capitolo 5. Reti Windows

Spesso le reti di computer sono costituite da sistemi eterogenei e, sebbene gestire una rete composta interamente da computer con Ubuntu sarebbe certamente divertente, alcuni ambienti di rete debbono essere costituiti da sistemi Ubuntu e Microsoft® Windows® che operano insieme in armonia. Questa sezione di Guida ad Ubuntu sul server introduce i principi e gli strumenti utilizzati nella configurazione di un server Ubuntu per la condivisione di risorse di rete con computer Windows.

1. Introduzione

Utilizzare Ubuntu in una rete composta da client Windows significa fornire e integrare i servizi tipici degli ambienti Windows. Questi servizi offrono supporto per la condivisione di dati e informazioni riguardo i computer e gli utenti della rete e possono essere classificati, in base alle loro funzionalità, in tre principali categorie:

- **Servizi per la condivisione di file e stampanti**. Utilizzo del protocollo SMB (Server Message Block) per agevolare la condivisione di file, cartelle, volumi e stampanti attraverso la rete.
- **Servizi di directory**. Condivisione di informazioni vitali sui computer e sugli utenti della rete con l'uso di tecnologie come LDAP (Lightweight Directory Access Protocol) e Microsoft Active Directory®.
- **Autenticazione e acesso**. Stabilire l'identità del computer o dell'utente della rete e determinare quali risorse siano accessibili al computer o all'utente tramite i permessi e i privilegi, utilizzando permessi dei file, politiche di gruppo e il servizio di autenticazione Kerberos.

Fortunatamente, i sistemi Ubuntu sono in grado di fornire queste funzionalità ai client Windows, permettendo la condivisione di risorse di rete. Uno dei componenti software principali, incluso nei sistemi Ubuntu per il networking con Windows, è la suite SAMBA, che comprende utilità e applicazioni per server SMB. Questa sezione della Guida ad Ubuntu sul server introduce all'installazione e alla configurazione base delle utilità e delle applicazioni server della suite SAMBA. Fornire maggiori dettagli su SAMBA va oltre lo scopo di questa guida, tali informazioni possono essere reperite nel *sito web di SAMBA* [http://www.samba.org].

2. Installare SAMBA

Al prompt inserire il seguente comando per installare le applicazioni server di SAMBA:

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

3. Configurare SAMBA

Il server SAMBA si configura attraverso la modifica del file `/etc/samba/smb.conf` per aggiungere o cambiare le impostazioni predefinite. Nei commenti del file `/etc/samba/smb.conf` l'utente può trovare altri dettagli sulla configurazione oppure consultando il manuale di `/etc/samba/smb.conf` digitando il seguente comando:

```
man smb.conf
```

Prima di modificare il file di configurazione, è consigliato creare una copia del file originale e proteggerla dalla scrittura, in modo da mantenere le impostazioni originali a disposizione come riferimento e per il riuso secondo necessità.

Fare una copia di backup del file `/etc/samba/smb.conf`:

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

Ora, aprire il file `/etc/samba/smb.conf` e apportare i cambiamenti desiderati.

3.1. Server

In aggiunta alla suite SAMBA per la gestione di un server, con tutte le sue applicazioni, Ubuntu offre altre potenti applicazioni per aumentare le funzionalità dei servizi offerti ai client Windows, molto simili a quelli offerti dai server Windows. Ubuntu offre la gestione centralizzata delle risorse della rete con Directory Services e facilita l'identificazione e l'autorizzazione di computer o utenti mediante Authentication Serivces.

Le seguenti sezioni trattano in dettaglio di SAMBA e delle tecnologie di supporto, quali server LDAP (Lightweight Directory Access Protocol) e server d'autenticazione Kerberos. Sono esposte anche alcune delle direttive di configurazione disponibili nel file di configurazione di SAMBA che possono facilitare l'integrazione in rete con client e server Windows.

3.1.1. Active Directory

Active Directory è un'implementazione proprietaria di Microsoft di Directory Services in grado di fornire i mezzi necessari a condividere le informazioni sugli utenti e sulle risorse della rete. Oltre a offrire una sorgente centralizzata per queste informazioni, Active Directory agisce come autorità centrale per l'autenticazione nella rete. Active Directory combina le funzionalità di servizi di directory specializzati, in modo tale da semplificare l'integrazione, la gestione e la sicurezze delle risorse di rete. La suite SAMBA può essere configurata per utilizzare i servizi di Active Directory forniti da un Windows Domain Controller.

3.1.1.1. LDAP

Il server LDAP fornisce, in maniera molto simile ai servizi Microsoft Active Directory, le funzionalità dei Directory Services ai computer Windows: questi servizi forniscono i mezzi per descrivere,

localizzare e gestire le risorse della rete. L'implementazione libera di LDAP disponibile in Ubuntu, si chiama *OpenLDAP*. I demoni del server, responsabili della gestione delle richieste di directory OpenLDAP e della distribuzione dei dati custoditi in un server LDAP in un altro sistema Ubuntu, si chiamano slapd e slurpd. OpenLDAP può essere utilizzato in combinazione con SAMBA per fornire Directory Services e la condivisione di file e stampanti, più o meno nello stesso modo con il quale un Windows Domain Controller interagisce con un server SAMBA compilato con il supporto LDAP.

3.1.1.2. Kerberos

Il sistema standard di autenticazione Kerberos è un servizio che fornisce autenticazione ai computer e agli utenti. Il servizio viene fornito attraverso un server centralizzato di autenticazione che garantisce biglietti d'accesso cifrati e accettati dai sistemi che operano con Kerberos. I benefici offerti da Kerberos sono la reciproca autenticazione, un'autenticazione per delega, interoperabilità e una gestione semplificata delle credenziali. I demoni principali in Ubuntu per la gestione dell'autenticazione Kerberos e l'amministrazione del database sono krb5kdc e kadmin. SAMBA può utilizzare Kerberos quale meccanismo di autenticazione dei computer e degli utenti in un ambiente controllato da un Windows Domain Controller. Per poter fare questo, il sistema Ubuntu deve avere installato Kerberos e il file `/etc/samba/smb.conf` deve essere predisposto per selezionare i corretti *realm* e *security*. Modificare, per esempio, `/etc/samba/smb.conf` aggiungendo i valori:

realm = NOME_DOMINIO

security = ADS

al file, e quindi salvarlo.

Assicurarsi di sostiutire il token NOME_DOMINIO, utilizzato nell'esempio precedente, con il nome del dominio Windows.

Per rendere effettivi i cambiamenti apportati, è necessario riavviare i demoni SAMBA. Per riavviare i demoni SAMBA, inserire in un terminale il seguente comando:

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

3.1.2. Account computer

Nei Directory Services gli account del computer sono utilizzati per identificare univocamente i computer presenti nella rete. Dal punto di vista della sicurezza sono trattati come degli account utente, pertanto possono avere delle password e sono soggetti ad autorizzazioni per l'accesso alle risorse di rete. Per esempio, se un utente con un account valido tenta di accedere a una risorsa da un computer che non possiede un account valido, a seconda delle politiche di sicurezza applicate, l'accesso alla risorsa potrebbe essere negato se il computer, dal quale l'utente sta effettuando l'autenticazione, non possiede le necessarie autorizzazioni.

Un account del computer può essere aggiunto al database degli account di SAMBA fornendo il nome del computer, purché questo non sia già presente come account utente. Per aggiungere un account del computer al database degli account di SAMBA, utilizzare, in un terminale, il comando smbpasswd:

```
sudo smbpasswd -a -m NOME_COMPUTER
```

Assicurarsi di sostituire il token NOME_COMPUTER, utilizzato nell'esempio precedente, con il nome del computer per il quale si vuole creare un account.

3.1.3. Permessi dei file

I permessi di accesso ai file indicano esplicitamente le operazioni consentite a un computer o a un utente su una particolare directory, un determinato file oppure un insieme di file. Questi permessi possono essere definiti modificando il file `/etc/samba/smb.conf` e specificando i permessi per una condivisione. Ad esempio, se l'utente ha definito una condivisione SAMBA chiamata *sourcedocs* e desidera concedere i permessi di *sola lettura* al gruppo *pianificazione*, concedendo però i permessi di *scrittura* al gruppo *autori* e all'utente *mario*, è necessario modificare il file `/etc/samba/smb.conf`, aggiungendo le seguenti righe al di sotto di *[sourcedocs]*:

read list = @pianificazione

write list = @autori, mario

Salvare il file `/etc/samba/smb.conf` affinché i cambiamenti abbiano effetto.

È inoltre possibile concedere permessi *amministrativi* per una particolare risorsa condivisa. Gli utenti che possiedono permessi amministrativi possono leggere, scrivere o modificare tutte le informazioni della risorsa per la quale hanno ottenuto i permessi. Per esempio, se si desidera concedere all'utente *melissa* i permessi amministrativi sulla condivisione *sourcedocs*, è necessario modificare il file `/etc/samba/smb.conf` aggiungendo le seguenti righe al di sotto di *[sourcedocs]*:

admin users = melissa

Salvare il file `/etc/samba/smb.conf` affinché i cambiamenti abbiano effetto.

3.2. Client

Ubuntu include funzionalità e applicazioni client per accedere alle risorse di rete condivise attraverso il protocollo SMB. Per esempio, mediante l'applicazione smbclient, è possibile accedere a file system remoti condivisi , come con un client FTP (File Transfer Protocol). Per accedere alla cartella condivisa *documenti*, nel computer remoto Windows denominato *bill* utilizzando smbclient, è sufficiente digitare al prompt dei comandi:

```
smbclient //bill/documenti -U <nomeutente>
```

Viene richiesta la password per il nome utente specificato dopo l'argomento -U e, se l'autenticazione ha avuto successo, viene presentato un prompt in cui è possibile inserire i comandi per manipolare

e trasferire i file, usando una sintassi simile a quella usata dai client FTP in modalità non grafica. Per maggiori informazioni sull'applicazione smbclient, leggere la corrispondente pagina di manuale utilizzando il comando:

```
man smbclient
```

Utilizzando il protocollo SMB, è anche possibile montare localmente risorse remote attraverso il comando mount. Per esempio, per montare sul punto di mount /mnt/pcode del proprio sistema Ubuntu, con i permessi dell'utente *giuseppe*, la cartella condivisa chiamata *codice-progetto* che si trova sul server Windows *sviluppo*, è necessario digitare al prompt il seguente comando:

```
mount -t smbfs -o username=giuseppe //sviluppo/codice-progetto /mnt/pcode
```

Viene richiesta la password dell'utente e, se l'autenticazione ha avuto successo, il contenuto della risorsa condivisa è disponibile, localmente, nel punto di mount specificato come ultimo argomento del comando di mount. Per scollegare la risorsa condivisa è sufficiente utilizzare il comando umount, come per ogni altro file system montato. Per esempio:

```
umount /mnt/pcode
```

3.2.1. Account utente

Gli account utenti definiscono gli utenti e il livello di autorizzazione all'utilizzo di un computer o delle risorse di rete concessi a quell'utente. È normale che in una rete ogni utente abbia un proprio account con cui vengono definiti i diritti e i permessi di accesso alle risorse. La definizione degli utenti SAMBA nel server Ubuntu avviene tramite l'uso di smbpasswd. Per esempio, per aggiungere un utente SAMBA al server Ubuntu, assegnandogli il nome *jseinfeld*, da terminale digitare:

```
smbpasswd -a jsenfield
```

L'applicazione smbpasswd chiederà di inserire una password per l'utente:

```
Nuova password SMB:
```

È necessario digitare la password da assegnare al nuovo utente, l'applicazione smbpasswd ne chiederà la conferma:

```
Ridigitare la nuova password SMB:
```

Confermata la nuova password, smbpasswd aggiungerà una nuova voce per l'utente nel file delle password di SAMBA.

3.2.2. Gruppi

I gruppi definiscono un insieme di computer e utenti che godono dei medesimi privilegi di accesso alle risorse condivise. I gruppi offrono un alto livello di controllo degli accessi alle risorse. Per esempio, se il gruppo *qa* contiene gli utenti *freda*, *danika* e *rob* e viene definito il secondo gruppo *support* che contiene gli utenti *danika*, *jeremy* e *vincent*, allora alcune risorse di rete impostate per concedere l'accesso al gruppo *qa* concedono automaticamente l'accesso anche agli utenti freda, danika e rob, mentre lo negano a jeremy o vincent. Dal momento che l'utente *danika* è membro di entrambi i gruppi *qa* e *support* potrà accedere a tutte le risorse condivise il cui accesso è stato concesso a entrambi i gruppi, gli altri utenti avranno accesso alle risorse esplicitamente assegnate al gruppo di appartenenza.

Nella definizione dei gruppi nel file di configurazione di SAMBA `/etc/samba/smb.conf`, è necessario far precedere il nome del gruppo dal simbolo «@». Per definire un gruppo chiamato *sysadmin* in una certa sezione del file `/etc/samba/smb.conf` bisogna inserire il nome del gruppo come **@sysadmin**.

3.2.3. Politiche di gruppo

Le politiche di gruppo definiscono alcuni parametri della configurazione di SAMBA relativi al Dominio o al Gruppo di lavoro a cui appartengono degli account e ad altri parametri globali di configurazione del server di SAMBA. Se, per esempio, un server SAMBA appartiene a un Gruppo di lavoro Windows denominato *LEVELONE*, il file `/etc/samba/smb.conf` può essere modificato con il valore seguente:

workgroup = LEVELONE

Riavviare il demone SAMBA affiché le modifiche abbiano effetto.

Altri importanti parametri di configurazione includono *server string* che definisce il nome del server NETBIOS dichiarato dal sistema Ubuntu alle altre macchine della rete Windows. Questo è il nome del sistema Ubuntu riconosciuto dai client Windows e dagli altri computer in grado di navigare con il protocollo SMB. È possibile specificare il nome e la posizione del file di log del server SAMBA utilizzando la direttiva *log file* all'interno del file `/etc/samba/smb.conf`.

Alcune delle direttive che governano le politiche globali del gruppo includono dettagli della natura globale delle risorse condivise. Per esempio, inserendo alcune direttive al di sotto della sezione *[global]* nel file `/etc/samba/smb.conf`, queste influenzeranno tutte le relative risorse condivise fino a quando un'altra direttiva primaria non ne annulli l'effetto. È quindi possibile stabilire che tutte le risorse siano esplorabili dai client della rete collocando una direttiva *browseable*, che prevede un argomento booleano, sotto l'intestazione *[global]* del file `/etc/samba/smb.conf`. Quindi aggiungendo la riga:

browseable = true

sotto la sezione *[global]* del file `/etc/samba/smb.conf`, tutte la risorse condivisibili, fornite dal sistema Ubuntu attraverso SAMBA, saranno esplorabili dai client autorizzati, a meno che una specifica risorsa non contenga una direttiva *browseable = false* che scavalca le disposizioni impartite dalla direttiva globale.

Altri esempi di direttive che operano in maniera simile alla precedente sono *public* e *writeable*.
La direttiva *public* accetta un valore booleano per decidere se una particolare risorsa condivisa sia visibile a tutti i client autorizzati. Anche la direttiva *writeable* accetta un valore booleano per decidere se una particolare risorsa condivisa possa essere modificata o meno dai client della rete.

Appendice 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/*.

Appendice B. GNU Free Documentation License

Version 1.2, November 2002

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

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 [9$* 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]* 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.