
Servizi di Rete: Postfix, Apache, NFS, Samba, Squid, LDAP, SIP, XMPP, TURN

Capitolo 11

11. Servizi di rete	pag. 251
1. Mail Server [I servers che si occupano della posta elettronica]	pag. 252
1. Installazione di Postfix	pag. 252
2. Configurazione dei Virtual Domains	pag. 255
1. Virtual Alias Domains	pag. 255
2. Virtual Mailbox Domains	pag. 256
3. Restrizioni per la Ricezione e la Trasmissione	pag. 257
1. Come limitare l'accesso in base all'indirizzo IP	pag. 258
2. Verifica della legittimità attraverso il comando EHLO o HELO	pag. 259
3. Consenso o diniego in base al Mittente Annunciato	pag. 260
4. Consenso o diniego in base al Destinatario	pag. 260
5. Restrizioni relative al comando DATA	pag. 261
6. Messa in atto delle restrizioni	pag. 261
7. Filtraggio basato sul contenuto del messaggio	pag. 261
4. Configurazione: greylisting	pag. 262
5. Personalizzazione dei filtri in base al destinatario	pag. 264
6. Integrazione di un antivirus	pag. 265
7. Autenticated SMTP	pag. 266
2. Server Web (HTTP)	pag. 268
1. Installazione di Apache	pag. 268
2. Configurazione dei Virtual Hosts	pag. 269
3. Common Directives (Le direttive maggiormente utilizzate)	pag. 271
1. Come richiedere l'Autenticazione	pag. 272
2. Come limitare l'Accesso	pag. 272
4. Log Analyzers	pag. 273
3. FTP File Server	pag. 275
4. NFS File Server	pag. 276
1. Securing NFS [come configurare le funzionalità di sicurezza di NFS]	pag. 277
2. NFS Server	pag. 277
3. NFS Client	pag. 278
5. Configurare Windows Shares attraverso Samba	pag. 279
1. Samba Server	pag. 279
1. Configurazione con debconf	pag. 279
2. Configurazione manuale	pag. 280
1. Le modifiche a smb.conf	pag. 280
2. Come aggiungere gli Utenti	pag. 281
2. Samba Client	pag. 281
1. Il programma smbclient	pag. 281
2. Mounting delle Windows Shares	pag. 281
3. Come stampare su una stampante condivisa	pag. 282
6. Proxy HTTP/FTP	pag. 282
1. Installazione	pag. 282
2. Configurazione di una cache	pag. 283
3. Come configurare un filtro	pag. 283
7. LDAP Directory	pag. 284
1. Installazione	pag. 284
2. Compilazione nella directory	pag. 286
3. La gestione degli Accounts con LDAP	pag. 287
1. Come configurare NSS	pag. 287
2. Come configurare PAM	pag. 288
3. Come proteggere lo Scambio Dati di LDAP	pag. 288
1. Configurazione lato server	pag. 289
2. Configurazione lato client	pag. 291
8. Real-Time Communication Service	pag. 292
1. Impostazioni DNS per i servizi RTC	pag. 293
2. TURN server	pag. 293
1. Installazione del TURN server	pag. 294
2. TURN gestione utenti	pag. 294
3. SIP Proxy Server [Session Initiation Protocol]	pag. 294
1. Installazione del SIP proxy	pag. 294
2. Come gestire il SIP proxy	pag. 296
4. XMPP Server	pag. 296
1. Installazione del XMPP server	pag. 296
2. Come gestire il server XMPP	pag. 297
5. Come eseguire i servizi sul port 443	pag. 297
6. Come aggiungere un servizio WebRTC	pag. 298

<<Vengono definiti servizi di rete (network services in ingl.) i programmi con cui gli utenti interagiscono direttamente per lo svolgimento delle loro mansioni quotidiane. I servizi di rete rappresentano la punta dell'iceberg di un sistema informativo pertanto questo capitolo li tratterà in dettaglio; le componenti celate su cui si basano i servizi di rete rappresentano l'infrastruttura che è stata descritta precedentemente. Diversi servizi di rete necessitano di essere supportati da una tecnologia di crittografia per poter essere eseguiti in modo affidabile e sicuro, soprattutto se utilizzati su Internet (o su una rete pubblica). I Certificati X.509 (correlati a Certificati SSL oppure a Certificati TLS) vengono comunemente utilizzati a questo scopo. Un certificato relativo ad un dato dominio può essere spesso condiviso tra più servizi, in particolare fra i servizi presentati in questo capitolo.>>

11.1. Mail Server [I servers che si occupano della posta elettronica]

Gli amministratori della Falcot Corp hanno scelto Postfix come mail server per la sua semplicità di configurazione ed affidabilità. In effetti Postfix è stato designato in modo da garantire che ogni attività venga implementata in un processo con una titolarità dei diritti e dei permessi strettamente necessaria allo scopo da ridurre l'adozione ex post di provvedimenti per contrastare potenziali vulnerabilità di sicurezza.

ALTERNATIVA	Debian include Exim4 come mail server predefinito (e quest'ultimo viene pertanto installato automaticamente durante l'installazione iniziale). La configurazione di Exim4 viene supportata da un altro distinto pacchetto denominato <code>exim4-config</code> ed automaticamente personalizzata tramite una serie di domande debconf molto simili a quelle poste dal pacchetto di <code>postfix</code> .
Il server Exim4	<p>La suddetta configurazione può essere salvata in un unico file (<code>/etc/exim4/exim4.conf.template</code>) oppure frammentata in diversi configuration snippets files conservati nella directory <code>/etc/exim4/conf.d/</code> [snippets in inglese significa appunto frammenti e genericamente si riferiscono a piccole porzioni di codice, in particolare destinate alla programmazione modulare]. In entrambi i casi, i files vengono utilizzati dal comando <code>update-exim4.conf</code> come modelli per generare <code>/var/lib/exim4/config.autogenerated</code>. Exim4 utilizza quest'ultimo file. Per mezzo di questo meccanismo, i valori ottenuti dalla configurazione debconf di Exim (memorizzati in <code>/etc/exim4/update-exim4.conf.conf</code>) possono essere iniettati nel file di configurazione di Exim, anche qualora l'amministratore o un altro pacchetto abbia modificato la configurazione Exim predefinita.</p> <p>La sintassi di configurazione di Exim4 è piuttosto specifica e richiede del tempo per padroneggiarla; ciò nonostante, una volta acquisite le dovute competenze, potrete usufruire di un server di posta solido e completo come del resto avrete modo di accertarvene nella decina di pagine di documentazione.</p> <p>♦ http://www.exim.org/docs.html</p>

11.1.1. Installazione di Postfix

Il pacchetto `postfix` contiene il main SMTP daemon. Altri pacchetti (come ad esempio `postfix-ldap` o `postfix-pgsql`) concedono funzionalità aggiuntive a Postfix, incluso l'accesso ai mapping databases. [In generale il mapping è una tecnica di gestione dei dati (per poter eseguire una migrazione, integrazione, ecc), che consente l'estrazione dei dati dei campi (in inglese `fields`) di un database ed il loro indirizzamento ai campi corrispondenti di altri database target. Pertanto, genericamente, i databases i cui dati vengono fra loro indirizzati attraverso questa tecnica possono essere definiti mapping databases]. Installate le funzionalità aggiuntive solo se ne avete necessità.

BASILARE	SMTP (Simple Mail Transfer Protocol) è il protocollo utilizzato dai mail servers per scambiarsi ed instradare le emails.
SMTP	

Durante l'installazione del pacchetto vengono poste diverse domande Debconf. Le risposte genereranno una prima versione del file di configurazione `/etc/postfix/main.cf`. La prima domanda riguarda il tipo di installazione. Delle scelte proposte, solo due sono rilevanti per un server connesso ad Internet: "Internet site" e "Internet with smarthost". La prima scelta è adatta ad un server che riceve la posta in entrata ed invia la posta in uscita direttamente ai suoi destinatari, modalità conforme al caso degli amministratori della Falcot Corp. La seconda scelta è invece adatta ad un server che riceve la posta in entrata direttamente, ma invia la posta in uscita tramite un server SMTP intermedio, denominato smarthost, anziché al server dei rispettivi destinatari. Quest'ultima scelta è particolarmente utile per le persone con un indirizzo IP dinamico, in quanto molti mail servers rifiutano qualsiasi messaggio proveniente direttamente da un indirizzo IP dinamico. Lo smarthost indicato per la summenzionata configurazione solitamente corrisponde al server SMTP di un provider di servizi Internet (ISP), a sua volta configurato per accettare sempre le emails in entrata dai clienti dello stesso provider di servizi per poi inoltrarne la posta appropriatamente.

Di conseguenza la configurazione di uno smarthost interesserà particolarmente i servers non permanentemente connessi, così che non sia necessaria la gestione di code di messaggi "non inviati" nonché la loro ritrasmissione successiva.

DIZIONARIO

ISP

[Il termine inglese ISP viene tradotto in francese in FAI, acronimo di Fournisseur d'Accès à Internet, da non confondere con FAI, acronimo di Fully Automatic Installer trattato a pag. 339]

ISP è l'abbreviazione di "Internet Service Provider". Si tratta di un'ente, spesso una società commerciale, che distribuisce connessioni ad Internet nonché i servizi di base associati (posta elettronica, news, ecc.). [Tra gli ISP francesi occorre citare Free, Orange (ex-Wanadoo), SFR, AOL, FDN, ecc.]

La seconda domanda riguarda il full name della macchina, utilizzato per generare gli indirizzi email degli utenti locali in combinazione con il loro nome account; il full name della macchina corrisponde alla parte che segue la "@" (chiocciola) nell'indirizzo email. Per la Falcot la risposta prescelta è mail.falcot.com. Questa è l'unica domanda richiesta di default, ma non è sufficiente per generare una configurazione soddisfacente per le esigenze della Falcot Corp, pertanto i suoi amministratori decidono di eseguire il comando `dpkg-reconfigure postfix` in modo da poter personalizzare più parametri.

Nello specifico una delle domande aggiuntive richiede agli amministratori di inserire tutti i domain names associati alla macchina. L'elenco di default proposto per la macchina include un full name nonché i synonyms (localhost), ma non il main domain falcot.com, che deve essere aggiunto manualmente. In generale, è opportuno indicare tutti i domain name per i quali la macchina dovrà svolgere il compito di MX server [Mail eXchanger]; in altre parole tutti i domain names che il DNS dovrà definire affinché la macchina sia in grado di accettare le emails. Le informazioni immesse vengono poi memorizzate nella variabile mydestination del main Postfix configuration file `/etc/postfix/main.cf`. [La funzionalità synonym (implementata attraverso il file `/etc/hosts`) consente di associare all'indirizzo IP di servizio 127.0.0.1 - che le macchine usano per ragioni di test o meramente per interpellare se stesse - il nome localhost, più agevole da ricordare rispetto ad una sequenza numerica.]

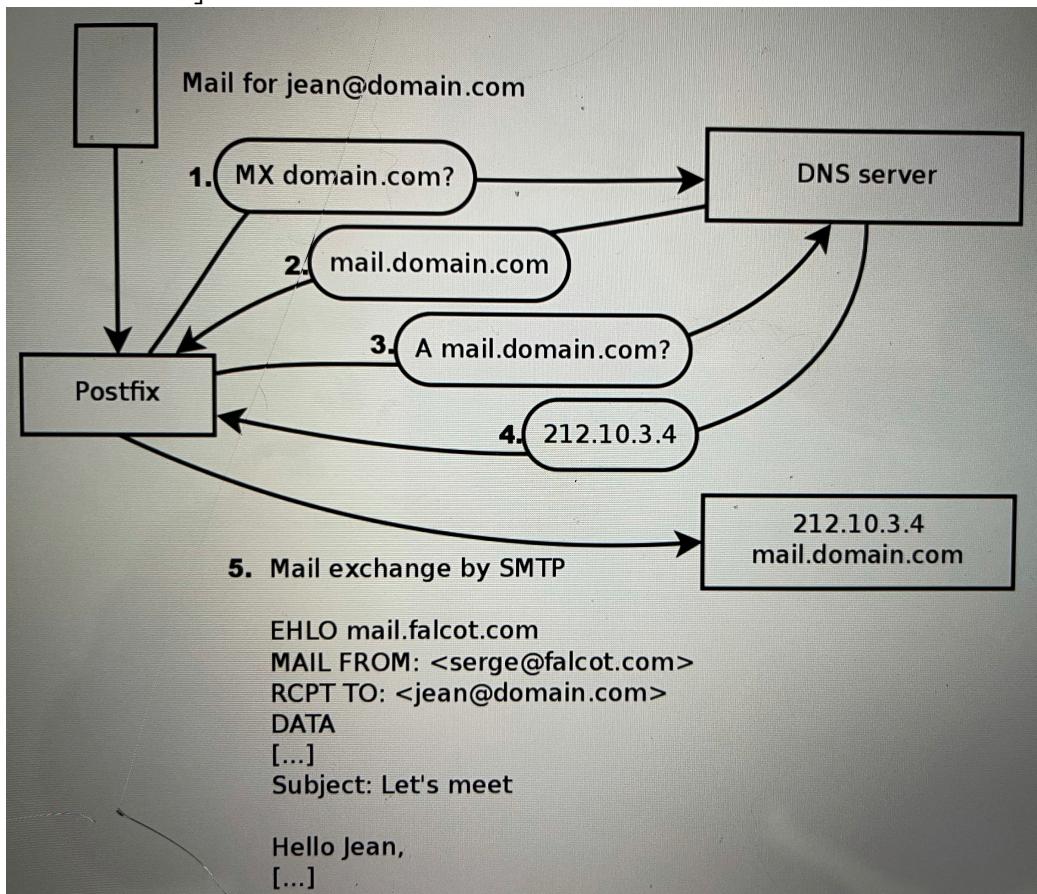


Figura 11.1 Il ruolo del DNS MX record durante l'invio di una mail

EXTRA Interrogazione (querying) dei MX records	<p>Se il DNS server non possiede un MX record per un dato dominio, l'email server [considererà il suddetto dominio come se fosse il target hostname con un preference value (priority) pari a 0 e] tenterà di inviare i messaggi direttamente all'host stesso, ricercando l'equivalente record di tipo A se IPv4 o AAAA se IPv6. [RFC 5321 sec. 5.1, 5.2]</p>
---	---

A seconda dei casi, l'installazione potrebbe anche richiedere di indicare le reti autorizzate ad inviare posta tramite la macchina. Per impostazione predefinita, Postfix accetta soltanto le emails provenienti dalla macchina stessa; occorre comunemente aggiungere la rete locale. Gli amministratori della Facolt Corp hanno aggiunto alla configurazione predefinita 192.168.0.0/16. Se la domanda non viene posta durante l'installazione, dovrete modificare la correlata variabile mynetworks, come mostrato nell'esempio sottostante.

Potrete affidare la consegna delle emails locali al tool procmail. Questo strumento consente agli utenti di ordinare la posta in arrivo stabilendo delle regole nel loro rispettivo file ~/.procmailrc. Dopo questa prima fase, gli amministratori hanno ottenuto il seguente file di configurazione, che fungerà per i paragrafi seguenti da punto di partenza per attivare attraverso delle modifiche determinate funzionalità aggiuntive.

Esempio 11.1 Il file /etc/postfix/main.cf (iniziale)

```
# See /usr/share/postfix/main.cf.dist for a commented, more complete version

# Debian specific: Specifying a file name will cause the first
# line of that file to be used as the name. The Debian default
# is /etc/mailname.
#myorigin = /etc/mailname

smtpd_banner = $myhostname ESMTP $mail_name (Debian/GNU)
biff = no

# appending .domain is the MUA's job.
append_dot_mydomain = no

# Uncomment the next line to generate "delayed mail" warnings
#delay_warning_time = 4h

readme_directory = no

# TLS parameters
smtpd_tls_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
smtpd_tls_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
smtpd_use_tls=yes
smtpd_tls_session_cache_database = btree:${data_directory}/smtpd_scache
smtp_tls_session_cache_database = btree:${data_directory}/smtp_scache

# See /usr/share/doc/postfix/TLS_README.gz in the postfix-doc package for
# information on enabling SSL in the smtp client.
```

```

smtpd_relay_restrictions = permit_mynetworks permit_sasl_authenticated
-> defer_unauth_destination
myhostname = mail.falcot.com
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
myorigin = /etc/mailname
mydestination = mail.falcot.com, falcot.com, localhost.localdomain, localhost
relayhost =
mynetworks = 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128 192.168.0.0/16
mailbox_command = procmail -a "$EXTENSION"
mailbox_size_limit = 0
recipient_delimiter = +
inet_interfaces = all
inet_protocols = all

```

SICUREZZA

Snake oil -
Certificati SSL

Vengono soprannominati *snake oil* [dall'espressione inglese *snake oil* - olio di serpente] i certificati che non hanno alcuna efficacia al pari dei medicinali a base di "olio di serpente" venduti in passato dai ciarlatani: non potrete fare affidamento su di essi per autenticare il server perché sono certificati autofirmati e generati automaticamente. Tuttavia, sono utili per migliorare la riservatezza degli scambi. Dovrebbero essere usati solo a scopo di test, mentre per i servizi ordinari si dovrebbero usare certificati reali; potrete generare quest'ultimi seguendo la procedura descritta nel paragrafo 10.2.1.1, "Infrastruttura a chiave pubblica: easy-rsa" a pagina 224.

11.1.2. Configurazione dei Virtual Domains

Un server di posta elettronica può ricevere emails anche da altri domini e non solo dal dominio principale; questi domini alternativi vengono definiti *virtual domains*. Quando ciò avviene raramente le emails sono destinate agli utenti locali. Postfix include due sorprendenti funzionalità per la gestione dei domini virtuali.

ATTENZIONE

Virtual domains
e canonical
domains

Nessun virtual domains può essere indicato nella variabile `mydestination`; questa variabile contiene solo i nomi dei domini "canonici", direttamente associati alla macchina e ai suoi utenti locali.
[non bisogna confondere il termine canonical domain con il dns record CNAME, proibito per i domini che usano SMTP MAIL ed i RCPT command (ex RFC 1123 sec. 5.2.2). Il dns record CNAME contiene l'alias alla sinistra ed il canonical name alla destra. Il CNAME non può puntare direttamente ad un altro CNAME o ad un indirizzo IP, ma ad un domain name che deve essere tradotto in base al value A (in un indirizzo IPv4) o in base al value AAAA (in un indirizzo IPv6)]

11.1.2.1 Virtual Alias Domains

Un Virtual Alias Domains contiene solo aliases, ovvero indirizzi che inoltrano le emails ad altri indirizzi.

Per attivare un virtual alias domain dovete aggiungere il suo nome nella variabile `virtual_alias_domains` e specificare un address mapping file nella variabile `virtual_alias_maps`.

Esempio 11.2 Le direttive che dovete aggiungere nel file /etc/postfix/main.cf

```
virtual_alias_domains = falcotsbrand.com  
virtual_alias_maps = hash:/etc/postfix/virtual
```

Il file /etc/postfix/virtual definisce il mapping attraverso una sintassi piuttosto inequivocabile. Ogni riga contiene due campi separati da una whitespace; il primo campo riporta l'alias name, mentre il secondo campo l'elenco degli indirizzi di posta elettronica a cui l'alias name rimanda. La special syntax [sintassi che usufruisce di caratteri speciali] @domain.com si occupa di tutti gli alias rimanenti di un dominio [nello specifico esempio sottostante la sintassi speciale viene utilizzata per inoltrare le email inviate al dominio @falcotsbrand.com agli account utenti omonimi del dominio @falcot.com]

Esempio 11.3 Esempio del file /etc/postfix/virtual

```
webmaster@falcotsbrand.com jean@falcot.com  
contact@falcotsbrand.com laure@falcot.com, sophie@falcot.com  
# The alias below is generic and covers all addresses within  
# the falcotsbrand.com domain not otherwise covered by this file.  
# These addresses forward email to the same user name in the  
# falcot.com domain.  
@falcotsbrand.com @falcot.com
```

11.1.2.2 Virtual Mailbox Domains

ATTENZIONE
Le variabili Virtual Alias domains e Virtual Mailbox domains sono compatibili?

Postfix non consente di includere lo stesso dominio nelle variabili `virtual_alias_domains` e `virtual_mailbox_domains`. Tuttavia, i domini inclusi nella variabile `virtual_mailbox_domains` verranno implicitamente considerati anche `virtual_alias_domains`, consentendovi di poter usufruire allo stesso tempo sia di aliases, sia di mailboxes in un unico virtual domain.

Le emails destinate ad un virtual mailbox domain vengono salvate nelle mailboxes non assegnate agli utenti locali del sistema.

Per attivare un virtual mailbox domain dovete aggiungerlo alla variabile `virtual_mailbox_domains` e specificare il mailbox mapping file nella variabile `virtual_mailbox_maps`. Il parametro `virtual_mailbox_base` definisce la directory in cui verranno archiviate le diverse mailboxes.

Il file che contiene il mapping fra l'indirizzo email ed un utente di sistema o un gruppo di sistema, titolare/i dei diritti e dei permessi della mailbox, viene definito rispettivamente nel parametro `virtual_uid_maps` o nel parametro `virtual_gid_maps`. Per assegnare di default tutte le mailboxes ad un unico utente/gruppo proprietario [con un uid e gid non in conflitto con quelli degli altri utenti/gruppi del sistema] dovete utilizzare la sintassi `static:5000` sia nel parametro `virtual_uid_maps`, sia nel parametro `virtual_gid_maps`.

Esempio 11.4 Le direttive che dovete aggiungere nel file /etc/postfix/main.cf

```
virtual_mailbox_domains = falcot.org  
virtual_mailbox_maps = hash:/etc/postfix/vmailbox  
virtual_mailbox_base = /var/mail/vhosts
```

Anche la sintassi del file /etc/postfix/vmailbox è piuttosto inequivocabile: include due campi separati da una whitespace. Il primo campo è riservato all'indirizzo di posta elettronica del virtual domain ed il secondo campo è riservato al percorso in cui si trova la mailbox (condizionato dalla directory citata dal parametro `virtual_mailbox_base`). Se il nome della mailbox [incluso nel percorso definito dal secondo campo] termina con una slash (/) la mailbox stessa verrà salvata in formato `maildir`; in caso contrario, verrà utilizzato il formato tradizionale `mbox`. Il formato `maildir` utilizza un'intera directory per la mailbox, conservando ogni singolo messaggio in un file dedicato. Diversamente, il formato `mbox` memorizza l'intera mailbox in un solo file, in cui ogni riga che inizia con "From" (seguito da uno spazio) indica l'inizio di un nuovo messaggio.

Esempio 11.5 Il file /etc/postfix/vmailbox

```
# Jean's email is stored as maildir, with  
# one file per email in a dedicated directory  
jean@falcot.org falcot.org/jean/  
# Sophie's email is stored in a traditional "mbox" file,  
# with all mails concatenated into one single file  
sophie@falcot.org falcot.org/sophie
```

11.1.3. Restrizioni per la ricezione e la trasmissione

Con il crescente numero di Unsolicited Bulk Email - UBE (genericamente definite spam - posta elettronica massiva indesiderata dai contenuti commerciali, offensivi o di poco valore) sono necessarie delle contromisure sempre più severe per valutare quali messaggi il server può ricevere. Questo paragrafo tratta alcune di queste strategie integrate in Postfix.

CULTURA

Il problema dello spam

Il termine **spam** si riferisce genericamente a tutte le **unsolicited commercial emails** (il cui acronimo è UCE) che invadono le caselle emails; mentre vengono definiti **spammers** le persone senza scrupoli che inviano lo spam. Agli spammers non importa quale fastidio arrecano, in quanto la campagna email-spam avrà per loro statisticamente più benefici che costi anche se soltanto una piccolissima percentuale di destinatari si lascia tentare dalla promozione. Il meccanismo che gli spammers utilizzano è piuttosto automatizzato: in pratica qualsiasi email resa pubblica su internet (ad esempio, attraverso un forum web, una mailing list, un blog, ecc.) viene rilevata dagli **spambots** per poi essere oggetto di un flusso continuo di messaggi indesiderati. Tutti gli amministratori IT cercano di far fronte allo spam attraverso la configurazione di filtri, ma gli spammers studiano il modo di aggirarli. A volte gli spammers per i loro scopi acquistano servizi distribuiti attraverso reti di macchine compromesse da worm da parte di organizzazioni criminali che le controllano. Statistiche recenti stimano che il 95% della posta inviata è spam!

11.1.3.1 Come limitare l'accesso in base all'indirizzo IP

La direttiva `smtpd_client_restrictions` controlla quali macchine sono autorizzate a comunicare con il server di posta.

Esempio 11.6 Restrizioni basate sull'indirizzo del client

```
smtpd_client_restrictions = permit_mynetworks,
warn_if_reject reject_unknown_client,
check_client_access hash:/etc/postfix/access_clientip,
reject_rbl_client sbl-xbl.spamhaus.org,
reject_rbl_client list.dsbl.org
```

Se una variabile contiene un elenco di regole come nell'esempio soprastante, tali regole vengono prese in consegna in base alla loro posizione nell'elenco, dalla prima all'ultima regola. In pratica ogni regola determina le sorti del messaggio: l'accettazione, il suo diniego o lasciare che continui ad essere valutato in base alla regola successiva. Pertanto la posizione di una regola nell'elenco ha molta importanza tanto che l'inversione della posizione di due regole può determinare degli effetti del tutto differenti.

La direttiva `permit_mynetworks`, collocata in cima all'elenco delle regole, impone che vengano accettate incondizionatamente le emails provenienti da qualsiasi macchina sulla rete locale (come ribadito dalla configuration variable `mynetworks`).

La seconda direttiva dovrebbe normalmente imporre di rifiutare le emails provenienti da macchine senza una valida configurazione DNS. Una configurazione DNS può ritenersi valida se l'indirizzo IP può essere risolto in un nome e se è possibile anche la **risoluzione inversa** ovvero il nome può essere risolto in un indirizzo IP. Purtroppo questa regola potrebbe essere esageratamente stringente, dato che diversi mail servers non dispongono di un **reverse DNS** per il loro indirizzo IP. Pertanto gli amministratori della Falcot Corp hanno preferito anteporre alla direttiva

`disable_unknown_client` il modifier `warn_if_reject`, che trasforma la regola di diniego in un semplice warning (avviso) nel registro dei logs. In questo modo gli amministratori IT possono monitorare il numero di messaggi potenzialmente oggetto di rifiuto e valutare consapevolmente se attivare la restrizione.

SUGGERIMENTO Le access tables

Tra i meccanismi per determinare le restrizioni vi sono anche le `access tables` (modificabili dall'amministratore) che elencano le combinazioni di mittenti, indirizzi IP, hostnames (autorizzati o vietati). Le `access tables` possono essere create copiando una versione non compressa del file `/usr/share/doc/postfix-doc/examples/access.gz`. Questo modello è self-documented attraverso l'inclusione di commenti ovvero ciascuna tavola documenterà la propria sintassi. La tabella `/etc/postfix/access_clientip` elenca gli indirizzi IP e le reti; la tabella `/etc/postfix/access_helo` elenca i domain names; la tabella `/etc/postfix/access_sender` contiene l'elenco degli indirizzi emails. Dopo ogni modifica, ciascuno di questi files deve essere convertito in una hash-table, ovvero in un formato ottimizzato per il fast access [trad. non lett. "lettura-esecuzione rapida"] attraverso il comando `postmap /etc/postfix/file`.

La terza direttiva consente all'amministratore di configurare attraverso il file `/etc/postfix/access_clientip` una blacklist ed una whitelist dei mail servers. La whitelist consente all'amministratore di specificare i servers attendibili e di conseguenza esentati dall'essere sottoposti al vaglio delle regole successive.

Le ultime due regole dell'esempio soprastante puntano a due blacklists ed impongono il rifiuto di qualsiasi messaggio proveniente da uno dei servers elencati nelle blacklists (RBL è l'acronimo Remote Black List, ovvero blacklist remota). Queste blacklists possono elencare servers mal configurati che gli spammers usano per trasmettere la loro posta, così come note unexpected mail relays tra cui macchine infettate da worm o da altri viruses. [Genericamente un SMTP relay è un server, solitamente gestito da un ISP, che si occupa solo della trasmissione/inoltro delle email in uscita]

SUGGERIMENTO
White list e RBLs

Le blacklists a volte includono un server legittimo che è stato vittima di problematiche. In teoria pertanto la posta proveniente da quel server dovrebbe essere rifiutata; la whitelist definita nel file /etc/postfix/access_clientip vi consentirà di ricevere comunque la posta dal quel server [a condizione che lo includiate nel summenzionato elenco]. Per questo motivo dovete agire con prudenza prima di inserire nella whitelist un mail server, includendo soltanto i mail servers di cui vi fidate e con i quali scambiate molta posta.

11.1.3.2 Verifica della legittimità attraverso il comando EHLO o HELO

Ogni trasmissione SMTP exchange inizia con un comando HELO (o EHLO) seguito dal nome del mail server mittente; la verifica della legittimità del nome annunciato del mail server mittente concede dei benefici.

Esempio 11.7 Restrizioni sul nome annunciato dal comando l'EHLO

```
smtpd_helo_restrictions = permit_mynetworks,  
reject_invalid_hostname,  
check_helo_access hash:/etc/postfix/access_helo,  
reject_non_fqdn_hostname,  
warn_if_reject reject_unknown_hostname
```

La prima direttiva allow_mynetworks consente a tutte le macchine sulla rete locale di annunciare il proprio nome senza restrizioni. La direttiva in questione ha la sua importanza, in quanto diversi softwares di posta elettronica non rispettano i requisiti minimi di questa parte del protocollo SMTP, annunciando nomi senza senso.

La regola reject_invalid_hostname rifiuta qualsiasi email con un annuncio EHLO che indica un hostname sintatticamente errato. La regola reject_non_fqdn_hostname rifiuta qualsiasi email se l'hostname indicato nell'annuncio EHLO non è un fully-qualified domain name (che include un domain name oltre all'hostname). La regola reject_unknown_hostname rifiuta qualsiasi email se il nome annunciato dal comando EHLO non esiste nel database DNS. Gli amministratori della Falcot Corp hanno preferito mitigare quest'ultima regola in quanto causerebbe il rifiuto di troppe emails, attraverso il modifier warn_if_reject; così facendo potranno valutare gli effetti della direttiva e decidere se attivarla o meno.

La direttiva allow_mynetworks essendo posta come prima regola nell'ordine dell'elenco determina un effetto che si riflette anche sulle regole successive: ovvero le direttive seguenti potranno essere applicate esclusivamente nei confronti delle emails provenienti da macchine non appartenenti alla rete locale. Così facendo potrete inserire nella blacklist tutti gli hosts che [pur non facendo parte della rete locale] si annunciano come membri [del dominio] falcot.com, per esempio aggiungendo la riga falcot.com REJECT You are not in our network! al file /etc/postfix/access_helo.

11.1.3.3 Consenso o diniego in base al Mittente Annunciato

Ogni messaggio ha un mittente annunciato dal comando MAIL FROM del protocollo SMTP; anche questa informazione può essere sottoposta a diversi controlli.

Esempio 11.8 Restrizioni sul mittente

```
smtpd_sender_restrictions =  
    check_sender_access hash:/etc/postfix/access_sender,  
    reject_unknown_sender_domain, reject_unlisted_sender,  
    reject_non_fqdn_sender
```

La tabella /etc/postfix/access_sender definisce se accettare o meno determinati utenti. In genere dovete solo inserire gli utenti in una white list o black list.

La regola `reject_unknown_sender_domain` richiede un dominio mittente valido, necessario per un indirizzo valido. La regola `reject_unlisted_sender` rifiuta i mittenti locali se il loro indirizzo non esiste. Ciò esclude quelle emails che sono state inviate da un indirizzo non valido con dominio falcot.com: ad esempio qualsiasi messaggio proveniente dal mittente joe.bloggs@falcot.com verrà accettato solo se questo indirizzo esiste davvero.

Infine, la regola `reject_non_fqdn_sender` impone il rifiuto delle email provenienti da indirizzi email privi di un full qualified domain name. In concreto, verranno rifiutate le emails provenienti da indirizzi con sintassi del tipo `user@machine`: l'indirizzo deve essere annunciato con una sintassi tipo `user@machine.example.com` oppure `user@example.com`.

11.1.3.4 Consenso o diniego in base al Destinatario

Ogni email ha anche un destinatario, annunciato tramite il comando RCPT TO del protocollo SMTP. Inoltre questi indirizzi come i precedenti possono essere altrettanto verificati, ma la verifica in sé comporta dei benefici minori rispetto alla verifica dell'indirizzo del mittente.

Esempio 11.9 Restrizioni sul destinatario

```
smtpd_recipient_restrictions = permit_mynetworks,  
    reject_unauth_destination, reject_unlisted_recipient,  
    reject_non_fqdn_recipient
```

`reject_unauth_destination` è una regola piuttosto basilare, in pratica l'emails provenienti da macchine al di fuori della rete devono essere indirizzate verso il mail server correttamente; se l'emails in questione sono destinate ad indirizzi inesistenti dovranno essere rifiutate. Senza questa regola, il mail server diverrebbe open relay consentendo agli spammers di inoltrare emails non desiderate; è preferibile pertanto porre tale regola in prossimità dell'inizio della lista in modo che nessun'altra regola rischi di autorizzare il ricevimento dell'emails prima del controllo del destinatario.

La regola `reject_unlisted_recipient` dispone il rifiuto dei messaggi inviati ad utenti locali inesistenti (il che ha senso!). Infine, la regola `reject_non_fqdn_recipient` impone il rifiuto degli indirizzi non fully-qualified; quindi verranno rifiutate l'emails inviate al mail server con indirizzi di destinazione con sintassi `jean` o `jean@machine`; diversamente la sintassi full-qualified idonea per gli indirizzi è `jean@machine.falcot.com` o `jean@falcot.com`.

11.1.3.5 Restrizioni relative al comando DATA

Il comando DATA del protocollo SMTP precede l'invio contenuti del messaggio. Non fornisce alcuna informazione di per sé, ma si limita ad annunciare ciò che gli seguirà. Può essere oggetto di controlli.

Esempio 11.10 Restrizione sul comando DATA

```
smtpd_data_restrictions = reject_unauth_pipelining
```

La regola `reject_unauth_pipelining` causa il rifiuto del messaggio se il mittente [durante lo scambio SMTP] invia un comando senza aver atteso la risposta al comando precedente. Questa precauzione è rivolta contro una comune funzionalità degli spambot utilizzata da quest'ultimi per incrementare l'efficienza in termini di invio di mole di emails nel minor tempo possibile.

11.1.3.6 Messa in atto delle restrizioni

Sebbene tutti i comandi verificano le informazioni fase per fase durante lo scambio SMTP, il rifiuto effettivo viene messo in atto da Postfix come risposta al comando RCPT TO.

Ciò significa che nonostante il rifiuto di un messaggio dovuto ad un comando EHLO non valido, Postfix sarà comunque in grado di identificare il mittente ed il destinatario. Inoltre, non avendo interrotto lo scambio dall'inizio, Postfix sarà in condizione di registrare un log sul messaggio con maggiori informazioni. Senza contare che diversi clients SMTP non si aspetterebbero di riscontrare il fallimento dello scambio SMTP a partire dai suoi primi comandi, subendo diversamente per mezzo di un rifiuto tardivo minori grattacapi.

Difatti il vantaggio di questo metodo è che le regole possono accumulare maggiori informazioni durante le diverse fasi dello scambio SMTP; questo metodo consente per di più un controllo dei permessi fine-grained [termine che può essere tradotto letteralmente come "a grana fine", ma che si riferisce all'omonima tecnica di controllo accessi capillare implementata per la gestione di grandi moli di dati] idonea per diverse controffensive come ad esempio il rifiuto dei messaggi provenienti da mittenti che si annunciano illegittimamente come mittenti che appartengono alla stessa rete locale.

11.1.3.7 Filtraggio basato sul contenuto del messaggio

Il sistema di verifica e restrizione non sarebbe completo senza una tecnica di controllo del contenuto del messaggio in sé. Postfix distingue due tipi di controlli basati rispettivamente sull'email headers e sull'email body.

Esempio 11.11 Attivazione dei filtri sui contenuti

```
header_checks = regexp:/etc/postfix/header_checks  
body_checks = regexp:/etc/postfix/body_checks
```

Entrambi i files contengono un elenco di **regular expression** (in ital. **espressioni regolari** comunemente denominate **regexps** o **regexes**) che se riscontrate nelle intestazioni o nel corpo dell'email attivano un'azione da eseguire.

BREVE ACCENNO Regexp tables

Il file /usr/share/doc/postfix-doc/examples/header_checks.gz presenta diversi commenti esplicativi allo scopo di essere utilizzato come punto di partenza per creare i files /etc/postfix/header_checks e /etc/postfix/body_checks.

Esempio 11.12 Esempio del file /etc/postfix/header_checks

```
/^X-Mailer: GOTO Sarbacane/ REJECT I fight spam (GOTO Sarbacane)  
/^Subject: *Your email contains VIRUSES/ DISCARD virus notification
```

BASILARE Espressione regolare

Il termine **regular expression** (in ital. **espressione regolare** comunemente denominate **regexps** o **regexes**) si riferisce ad una notazione generica utilizzata per esprimere la descrizione dei contenuti e/o della struttura di una stringa di caratteri. Alcuni caratteri speciali consentono di poter: definire delle alternative (ad esempio, "foo | bar" ovvero o "foo" o "bar"); configurare i caratteri ammessi (ad esempio "[0-9]" si riferisce ai numeri compresi tra 0 e 9, mentre con un punto ". " si intende qualsiasi carattere); eseguire quantificazioni attraverso un **quantifier** [molto genericamente un **quantifier** è un operatore logico che consente di specificare la quantità delle singole unità] (ad esempio ad "s ?" può essere associata una stringa vuota oppure una singola unità del carattere "s", in altre parole 0 unità del carattere "s" oppure 1 unità del carattere "s"; diversamente ad "s +" può essere associata una singola unità del carattere "s" oppure diverse unità del carattere "s" consecutive, ecc.). Le parentesi vengono utilizzate per aggregare i risultati di ricerca.
La sintassi delle regular expression può variare in base al tool che se ne serve, ma le funzionalità basilari rimangono le stesse.

♦ http://en.wikipedia.org/wiki/Regular_expression

Nell'esempio 11.12, riguardante le verifiche delle intestazioni delle emails, la prima riga impone il controllo dell'annuncio che definisce il software email del mittente: se riscontra GOTO Sarbacane (un software per l'invio massivo di email), il messaggio verrà rifiutato. La seconda riga verifica il subject (oggetto) del messaggio: se ricorda quanto trattato da una notifica virus, il messaggio pur non essendo rifiutato viene eliminato immediatamente.

L'uso di questi filtri è un'arma a doppio taglio, perché facilmente possono essere resi troppo generici e di conseguenza l'emails legittime possono andare perdute. In questi casi, non solo i messaggi andranno persi, ma anche i loro mittenti saranno infastiditi da messaggi di errore indesiderati.

11.1.4. Configurazione: greylisting

Il greylisting è una tecnica di filtraggio che prevede il rifiuto iniziale sistematico dei messaggi attraverso un temporary error code e la loro l'accettazione solo al loro secondo tentativo dopo un determinato periodo di tempo.

Questo filtro è particolarmente efficace contro lo spam inviato da macchine infettate da worms e virus dato che raramente questi softwares funzionano come un full SMTP (difatti diversamente quest'ultimo verifica gli error codes e ritenta in un secondo momento l'invio dei messaggi con una prima trasmissione non andata a buon fine), né gli spammers hanno interesse che funzionino come un full SMTP in quanto diversi harvested addresses [indirizzi emails rilasciati pubblicamente e non, prelevati con diverse tecniche ed utilizzati prevalentemente per scopi illeciti] potrebbero ormai essere inutilizzati ed il reinvio dei messaggi comporterebbe di conseguenza un'ulteriore perdita di tempo.

Postfix non integra questa funzionalità nativamente, ma include comunque una funzione che consente di delegare ad un programma terzo la decisione (consenso o rifiuto) sull'esito di un dato messaggio ricevuto. Il pacchetto postgrey offre un programma designato per interfacciarsi con il suddetto access policy delegation service.

Dopo essere stato installato e messo in esecuzione postgrey si comporta come un daemon in ricezione del port 10023. Per configurare postfix ad utilizzare postgrey dovete immettere come restrizione aggiuntiva il parametro `check_policy_service`:

```
smtpd_recipient_restrictions = permit_mynetworks,  
[...]  
check_policy_service inet:127.0.0.1:10023
```

Ogni volta che Postfix controlla il ruleset e di conseguenza raggiunge la summenzionata restrizione, si connette al daemon postgrey per trasmettergli le informazioni sul messaggio in questione.

Dopodiché Postgrey verifica il [set di tre fattori/dati denominato] triplet (indirizzo IP, mittente e destinatario) del messaggio in questione e verifica nel suo database se già ha avuto modo di incontrarlo. Se riconosce il triplet postgrey restituisce l'ordine di accettare il messaggio, diversamente, qualora non lo riconoscesse, ordina di rifiutare temporaneamente il messaggio e ne memorizza il triplet nel proprio database.

L'inconveniente principale dell'uso del greylisting è il ritardo, talvolta inaccettabile, della ricezione dell'e-mails legittime. Difatti incrementa il burden dei servers [genericamente il burden rate è il tasso di carico ottenuto dalla comparazione dei costi indiretti (dividendo) per i costi diretti (divisore)] che inviano diverse emails legittime.

IN PRATICA

Limitazioni del greylisting

In teoria il greylisting ritarda solo la prima email di un dato mittente destinata ad un dato destinatario ed il ritardo standard dovrebbe essere una questione di minuti. Tuttavia, la realtà potrebbe discostarsi dalla teoria. Difatti diversi ISPs di grandi dimensioni utilizzano clusters di SMTP servers; ciò comporta che al primo rifiuto del messaggio, potrebbe rispondere, con un secondo tentativo di invio, un altro server rispetto a quello che ha di fatto inviato il messaggio. Come conseguenza a ciò anche il secondo server riceve un rifiuto per le restrizioni imposte dal greylisting [così come lo riceveranno pure gli altri servers del cluster che verranno coinvolti]; il delay (ritardo) imposto per il rinvio tenderà ad incrementarsi in quanto il server SMTP, ad ogni trasmissione fallita, aumenta sistematicamente il tempo di attesa per poter effettuare nuovamente la trasmissione del messaggio e da una manciata di minuti passeranno diverse ore prima che il rifiuto possa essere trasmesso ad un server del cluster già coinvolto.

E intuibile che l'indirizzo IP del server mittente di un dato mittente potrebbe non essere necessariamente sempre lo stesso. Senza contare che persino l'indirizzo email di un dato mittente potrebbe differire. Per fare un esempio diversi mailing list servers codificano le informazioni extra dell'indirizzo del mittente per gestire automaticamente gli error messages denominati bounces [in ital. lett. "respinti" - quando un'email viene respinta il server destinatario invia al server mittente una delivery status notification (DSN) denominata bounce message]. Inoltre i messaggi in entrata del mailing-list server potrebbero dover superare anche un filtro greylisting, il che implica che il server mittente conservi (temporaneamente) il messaggio inviato. Per i mailing-list servers con decine di migliaia di utenti iscritti, ciò può diventare rapidamente problematico.

Per ovviare a tali inconvenienti, Postgrey dispone di una whitelist per questo tipo di siti in modo da imporre il consenso immediato dei loro messaggi, senza necessità della convalida della restrizione greylisting. Potrete personalizzare la whitelist [dei mailing-list servers] in base alle vostre esigenze modificando il file `/etc/postgrey/whitelist_clients`.

ANDANDO OLTRE Selective greylisting attraverso milter-greylist	Per limitare gli svantaggi delle restrizioni greylisting è consigliabile applicarle solo ad un subset di clients, già noti come potenziali fonti di spam in quanto elencati in una blacklist DNS. Ciò non è possibile con postgrey e dovrete fare riferimento a questo scopo al pacchetto milter-greylist. In questo scenario le DNS blacklists non sono sufficienti per determinare il diniego in tutti i casi opportuni, pertanto è consigliabile fare uso di blacklists più aggressive, che includano tutti gli indirizzi IP dinamici degli ISP clients, tra cui pbl.spamhaus.org o dul.dnsbl.sorbs.net. La configurazione di milter-greylist in Postfix si limita a smtpd_milters = unix:/var/run/milter-greylist/milter-greylist.sock, dal momento che milter-greylist utilizza la milter interface predefinita per Sendmail. La manual page greylist.conf(5) documenta il file /etc/milter-greylist/greylist.conf ed i vari criteri per configurare milter-greylist. Dovrete comunque modificare il file /etc/default/milter-greylist per attivare il servizio.
--	---

11.1.5. Personalizzazione dei filtri in base al destinatario

Il paragrafo 11.1.3, "Restrizioni per la Ricezione e la Trasmissione" a pagina 257 ed il paragrafo 11.1.4, "Configurazione: greylisting" a pagina 262 hanno trattato diversi tipi di restrizioni. Per quanto tali restrizioni limitino la quantità di spam ricevuto, presentano tutte piccoli inconvenienti. Quest'ultimi sono comunemente contrastati attraverso il filtraggio basato su destinatari. Alla Falcot Corp, il greylisting è stato apprezzato dalla maggior parte degli utenti ad eccezione di coloro i quali svolgono mansioni che richiedono bassa latenza per l'emails (ad esempio i servizi di supporto tecnico). Nel frattempo il reparto vendite ha dei grattacapi nel ricevere le emails da alcuni fornitori dell'Asia perché quest'ultimi potrebbero essere stati inclusi in delle blacklists; di conseguenza tale reparto ha fatto esplicita richiesta di emails non filtrate, idonee per la ricezione della corrispondenza.

Postfix gestisce il filtraggio attraverso un "restriction class" concept. Le classi vengono dichiarate nel parametro `smtpd_restriction_classes` e definite con lo stesso metodo del parametro `smtpd_recipient_restrictions`. La direttiva `check_recipient_access` definisce invece la table mapping che associa determinate restrizioni nei confronti di determinati destinatari.

Esempio 11.13 Come vengono definite le restriction classes in main.cf

```
smtpd_restriction_classes = greylisting, aggressive, permissive

greylisting = check_policy_service inet:127.0.0.1:10023
aggressive = reject_rbl_client sbl-xbl.spamhaus.org,
              check_policy_service inet:127.0.0.1:10023
permissive = permit

smtpd_recipient_restrictions = permit_mynetworks,
                               reject_unauth_destination,
                               check_recipient_access hash:/etc/postfix/recipient_access
```

Esempio 11.14 Il file /etc/postfix/recipient_access

```
# Unfiltered addresses
postmaster@falcot.com    permissive
support@falcot.com        permissive
sales-asia@falcot.com    permissive

# Aggressive filtering for some privileged users
joe@falcot.com           aggressive

# Special rule for the mailing-list manager
sympa@falcot.com         reject_unverified_sender

# Greylisting by default
falcot.com                greylisting
```

11.1.6. Integrazione di un antivirus

A causa dei diversi virus che vengono diffusi attraverso gli allegati emails, è importante configurare un antivirus nell'entry point della rete aziendale, in quanto nonostante le campagne di sensibilizzazione sull'argomento, ci sarà sempre qualche utente che aprirà l'allegato di un messaggio sospetto.

L'antivirus gratuito scelto dagli amministratori della Falcot è clamav. Pertanto gli amministratori hanno installato il main package clamav ed altri pacchetti come arj, unzoo, unrar e lha, che mettono in condizioni l'antivirus di scansionare gli allegati compressi in uno di questi formati. L'attività di interfacing fra l'antivirus ed l'email server è affidata a clamav-milter. Un programma milter (termine derivato dall'espressione inglese mail filter, filtro della posta elettronica) è un software di filtraggio della posta progettato appositamente per interfacciarsi con gli email servers. I programmi di tipo milter utilizzano un'application programming interface (API) che gestisce le esecuzioni meglio rispetto ai filtri esterni agli emails server. Sendmail ha introdotto per primo i milters e Postfix ne ha seguito l'esempio.

BREVE
ACCENNO
Un milter per
Spamassassin

Il pacchetto spamass-milter contiene un milter basato sul popolare software di rilevamento dell'emails indesiderate Spamassassin. Può essere utilizzato per contrassegnare i potenziali messaggi spam (aggiungendo un extra header) e/o per disporne il rifiuto qualora il punteggio "spamminess" del messaggio superi una soglia stabilita.

Una volta installato il pacchetto clamav-milter, il milter dovrebbe essere riconfigurato in modo che si metta in esecuzione attraverso un TCP port piuttosto che attraverso il predefinito named socket [un file descriptor per le interprocess communication (IPC), le trasmissioni dati fra processi]. Potrete farlo eseguendo dpkg-reconfigure clamav-milter. Vi verrà richiesto di configurare la "Communication interface with Sendmail" e dovete rispondere "inet:10002@127.0.0.1".

NOTA TCP port vs named socket?	<p>La ragione per cui viene usato un port TCP piuttosto che un named socket è che il demone Postfix viene eseguito chrooted [ovvero in una directory tree designata dalla quale non può raggiungere i files all'esterno] e non ha modo di accedere alla directory in cui si trova il named socket. Tuttavia potrete continuare ad utilizzare un named socket modificando la sua posizione all'interno di chroot (ovvero in /var/spool/postfix/).</p>
---	--

La configurazione standard di ClamAV va bene nella maggior parte dei casi, anche se `dpkg-recon clamav-base` consente di personalizzare i parametri più importanti.

Come ultimo passaggio dovete comunicare a Postfix di utilizzare il filtro configurato. Per fare ciò aggiungete la seguente direttiva in `/etc/postfix/main.cf`:

```
# Virus check with clamav-milter
smtpd_milters = inet:[127.0.0.1]:10002
```

Qualora dovessero insorgere problemi con l'antivirus, dovete semplicemente commentare [#] la riga ed eseguire il comando `service postfix reload` in modo che la modifica diventi efficace.

IN PRATICA Testate l'antivirus	<p>Una volta installato l'antivirus, è necessario verificare che funzioni correttamente. Il modo più semplice per farlo è inviare un'e-mail di prova con allegato il file <code>eicar.com</code> o <code>eicar.com.zip</code>, che può essere recuperato online:</p> <ul style="list-style-type: none"> ◆ http://www.eicar.org/86-0-Intended-use.html <p>Non si tratta di un vero virus, ma di un test file identificato da tutti gli antivirus presenti sul mercato come minaccia in modo che si possa verificare l'installazione.</p>
---	--

Giunti a questo punto finalmente i messaggi elaborati da Postfix vengono filtrati dall'antivirus.

11.1.7. Authenticated SMTP

Per poter inviare delle e-mails occorre la disponibilità di una connessione ad un SMTP server e che quest'ultimo autorizzi l'invio delle emails suo tramite. I problemi possono sorgere con i roaming users, dato che ciò richiederebbe la modifica regolare della configurazione dei SMTP client; difatti l'SMTP server della Falcot rifiuta l'inoltro dei messaggi provenienti da un indirizzo IP apparentemente non della società. Esistono due soluzioni: la prima soluzione è che i roaming users installino un SMTP server sul proprio computer; la seconda soluzione è che i roaming users continuino ad utilizzare l'SMTP server della società a patto che effettuino l'autenticazione come dipendenti. La prima soluzione è sconsigliata perché il computer non è connesso in modo permanente e quindi non può tentare di ritrasmettere i messaggi in caso di problemi; pertanto è meglio soffermarsi sulla seconda soluzione.

L'autenticazione SMTP di Postfix si basa su SASL (Simple Authentication and Security Layer). Dovrete installare i pacchetti `libsasl2-modules` e `sasl2-bin`; dopodiché dovete registrare una password per ciascun utente nel database SASL in modo che ciascun utente sia in grado di autenticarsi sull'SMTP server. Dovrete usare pertanto il comando `saslpasswd2`. L'opzione `-u` definisce l'authentication domain, che deve corrispondere al parametro Postfix `smtpd_sasl_local_domain`. L'opzione `-c` viene utilizzata per creare un utente, mentre l'opzione `-f` viene utilizzata per specificare il file da utilizzare qualora il database SASL sia stato archiviato altrove rispetto alla sua posizione standard (`/etc/sasldb2`).

```
# saslpasswd2 -h 'postconf -h myhostname' -f /var/spool/postfix/etc/sasldb2 -c jean
[... type jean's password twice ...]
```

Si precisa che il database SASL è stato creato nella directory Postfix. Per garantire coerenza, occorre convertire /etc/sasldb2 in un symbolic link che punta al database utilizzato da Postfix attraverso il comando ln -sf /var/spool/postfix/etc/sasldb2 /etc/sasldb2.

Giunti a questo punto resta da configurare Postfix per utilizzare SASL. Innanzitutto, dovete aggiungere il postfix user al sasl group in modo che possa accedere al SASL account database. Successivamente dovete abilitare SASL e configurare il parametro smtpd_recipient_restrictions in modo che quest'ultimo non impedisca ai SASL-authenticated clients di inviare e-mails liberamente.

Esempio 11.15 Come abilitare SASL in /etc/postfix/main.cf

```
# Enable SASL authentication
smtpd_sasl_auth_enable = yes
# Define the SASL authentication domain to use
smtpd_sasl_local_domain = $myhostname
[...]
# Adding permit_sasl_authenticated before reject_unauth_destination
# allows relaying mail sent by SASL-authenticated users
smtpd_recipient_restrictions = permit_mynetworks,
    permit_sasl_authenticated,
    reject_unauth_destination,
[...]
```

**EXTRA
Authenticated
SMTP client**

La maggior parte degli email clients (softwares di posta elettronica) attuali è in grado di autenticarsi con un server SMTP per inviare gli outgoing messages (la posta in uscita) e tale funzionalità viene attivata semplicemente attraverso la mera configurazione dei parametri appropriati. Qualora l'email client che utilizzate non fosse provvisto di tale funzionalità potrete mettere in atto un workaround attraverso il server Postfix locale, configurandolo in modo che inoltri le emails al server SMTP remoto. In questo caso, sarà Postfix stesso il client che si autentica attraverso SASL. Ecco i parametri necessari:

```
smtp_sasl_auth_enable = yes
smtp_sasl_password_maps = hash:/etc/postfix/sasl_passwd
relay_host = [mail.falcot.com]
Il file /etc/postfix/sasl_passwd deve includere l'username e la password da utilizzare per l'autenticazione sul server mail.falcot.com. Ecco un esempio:
[mail.falcot.com] joe:LyinIsji
Come con tutte le Postfix maps, dovete convertire il suddetto file in /etc/
postfix/sasl_passwd.db attraverso il comando postmap.
```

11.2. Server Web (HTTP)

Gli amministratori della Falcot Corp hanno scelto Apache come loro HTTP server di cui Debian Jessie distribuisce la versione 2.4.10.

ALTERNATIVA Altri server web

Apache è uno dei web servers più conosciuti e utilizzati, ma esistono delle alternative; gli altri web servers hanno prestazioni migliori di Apache per alcuni workloads, ma offrono minori funzionalità e moduli. Pertanto se avete necessità di un web server per static files [ad esempio HTML, CSS, immagini, JavaScript] o per svolgere le attività di un proxy server, fareste bene a prendere in considerazione delle alternative, come ad esempio nginx e lighttpd.

11.2.1. Installazione di Apache

Dovrete installare soltanto il pacchetto apache2. Difatti questo pacchetto contiene già tutti i moduli necessari, inclusi i Multi-Processing Modules (MPM) determinanti per Apache affinché possa gestire il parallel processing delle diverse istanze (moduli precedentemente distribuiti attraverso diversi pacchetti apache2-mpm-*). Mentre il pacchetto apache2-utils, che vi consigliamo di installare, contiene le utilities da riga di comando descritte più avanti.

Il modulo MPM di fatto utilizzato determina significativamente il metodo con cui Apache gestisce le istanze simultanee. Difatti il worker MPM utilizza i threads (lightweight processes), mentre il prefork MPM utilizza un pool of processes (collezione di processi) realizzato anticipatamente. [Non ho tradotto letteralmente lightweight processes perché si tratta di un metodo per dividere i processi in sotto processi di infime dimensioni. Vengono definiti thread pool i gestori dei threads. Per maggiore chiarezza, genericamente, il worker MPM usa più child processes che gestiscono diversi threads (i quali singolarmente si occupano di una connessione alla volta), mentre il prefork MPM utilizza, con maggiore dispendio di memoria, più child processes che gestiscono singolarmente un unico thread (il quale singolarmente si occupa di una connessione alla volta).] Anche l'event MPM utilizza i threads, ma le connessioni inattive (in particolare quelle tenute aperte dalla funzionalità HTTP keep-alive [HTTP persistent connection o HTTP connection reuse del protocollo HTTP]) vengono restituite ai threads dedicati alla loro gestione.

Gli amministratori della Falcot Corp installano inoltre libapache2-mod-php5 per includere il supporto PHP in Apache. Questa scelta comporta la disattivazione dell'event MPM (predefinito) e l'attivazione del prefork MPM, in quanto dei due solo il prefork MPM è compatibile con PHP.

SICUREZZA Esecuzione sotto l'utente www- data

Per impostazione predefinita, Apache gestisce le istanze in entrata sotto l'identità dell'user www-data. In questo modo, una vulnerabilità di sicurezza in uno CGI script eseguito da Apache (per una dynamic page) non può compromettere l'intero sistema, ma solo i files la cui titolarità dei diritti spetta a questo utente. [CGI è l'acronimo di Common Gateway Interface ed è un'interfaccia che consente agli users di un web server di eseguire un programma terzo o uno script denominato CGI script]

Il modulo suexec consente il bypassing di questa regola in modo che gli CGI scripts vengano eseguiti sotto l'identità di un altro utente. Occorre però configurare Apache per mezzo della direttiva `SuexecUserGroup usergroup`.

È anche possibile utilizzare un MPM dedicato, come quello distribuito attraverso libapache2-mpm-itk. Il suo funzionamento è leggermente diverso, in quanto consente "l'isolamento" dei virtual hosts (di fatto dei "sets of pages" ovvero degli insiemi di pagine) in modo che svolgano le loro funzioni sotto l'identità di un rispettivo utente, diverso fra loro. Pertanto, una vulnerabilità in un sito Web non comprometterà i files appartenenti all'owner di un altro sito Web.

BREVE ACCENNO Elenco dei moduli

L'elenco completo dei moduli standard Apache standard può essere reperito online.
♦ <http://httpd.apache.org/docs/2.4/mod/index.html>

Apache è un server modulare e la maggior parte delle sue funzionalità viene implementata attraverso moduli esterni che il programma carica durante la sua inizializzazione. La configurazione di default attiva solo i moduli maggiormente utilizzati e per abilitarne altri dovete eseguire `a2enmod module`; diversamente il comando `a2dismod module` li disabiliterà. Questi due programmi non fanno altro che creare o rimuovere i collegamenti simbolici in `/etc/apache2/mods-enabled/` che puntano ai files reali (situati in `/etc/apache2/mods-available/`).

Per impostazione predefinita, il web server è in ricezione sul port 80 (come configurato in `/etc/apache2/ports.conf`) e carica le pagine dalla directory `/var/www/html/` (come configurato in `/etc/apache2/sites-enabled/000-default.conf`).

ANDANDO OLTRE Supporto SSL

Apache 2.4 include il modulo SSL necessario per il secure HTTP (HTTPS). Per attivarlo dovete: eseguire `a2enmod ssl`; aggiungere le direttive necessarie nei configuration files. Troverete una configurazione esemplificativa in `/etc/apache2/sites-available/default-ssl.conf`.

♦ http://httpd.apache.org/docs/2.4/mod/mod_ssl.html

Dovrete prendere altre precauzioni qualora desideriate integrare le connessioni SSL con il Perfect Forward Secrecy (queste connessioni utilizzano delle ephemeral session keys diverse per ogni sessione in modo che un'eventuale compromissione di una delle chiavi segrete utilizzate dal server non possa determinare la compromissione del traffico criptato raccolto dalla rete a seguito di uno "sniffing" (intercettazione). Al riguardo date un'occhiata alle raccomandazioni di Mozilla:

♦ https://wiki.mozilla.org/Security/Server_Side_TLS#Apache

11.2.2. Configurazione dei Virtual Hosts

Un virtual host è un'identità (aggiuntiva) assunta dal web server.

Apache distingue due tipi di host virtuali: quelli basati sull'indirizzo IP (o sul port) e quelli basati sul domain name del web server. Il primo metodo impone che venga assegnato un indirizzo IP diverso (o port) per ciascun sito mentre il secondo metodo utilizza un solo indirizzo IP (e port) ed siti differiscono fra loro in base all'hostname comunicato dal client HTTP (quest'ultimo metodo è compatibile solo con la versione 1.1 del protocollo HTTP, che fortunatamente esiste da abbastanza tempo dall'essere utilizzato da tutti i web browsers).

La (pressante) scarsità di indirizzi IPv4 favorisce il secondo metodo. Tuttavia, se occorre rendere compatibili i virtual hosts con l'HTTPS la faccenda si complica, dato che il protocollo SSL non ha sempre supportato il name-based virtual hosting; inoltre l'estensione SNI (Server Name Indication) che rende possibile la sopracitata combinazione non è compatibile con tutti i browsers. Pertanto se occorre far eseguire più siti HTTPS dallo stesso server, è preferibile differenziarli, eseguendoli su ports differenti oppure su indirizzi IP differenti (possibilmente utilizzando l'IPv6).

La configurazione predefinita di Apache 2 utilizza i virtual hosts name-based. Un virtual host di default viene definito nel file `/etc/apache2/sites-enabled/000-default.conf`; questo virtual host sarà utilizzato qualora nessun altro host riesce a stabilire il matching con la richiesta inviata dal client.

ATTENZIONE
Il primo virtual host

Il primo virtual host risponderà sempre alle richieste concernenti virtual hosts sconosciuti; pertanto viene configurato come `www.falcot.com`.

BREVE ACCENNO
Apache supporta SNI

Apache supporta un'estensione del protocollo SSL denominata Server Name Indication (SNI). Questa estensione consente al browser di inviare l'hostname del web server non appena viene stabilita la connessione SSL, prima della stessa richiesta HTTP, che in passato veniva utilizzata per identificare il virtual host richiesto tra tutti gli altri ospitati sullo stesso server (con stesso indirizzo IP e port). Ciò consente ad Apache di selezionare il certificato SSL più appropriato per l'operazione da eseguire.

Prima dell'introduzione di SNI, Apache utilizzava sempre il certificato del virtual host predefinito. Pertanto quando i clienti provavano ad accedere ad un altro virtual host visualizzavano dei warnings dato che il certificato non corrispondeva al sito web a cui stavano tentando di accedere. Fortunatamente la maggior parte dei browsers di oggi è compatibile con SNI; ovviamente sono inclusi Microsoft Internet Explorer dalla versione 7.0 (a partire da Vista), Mozilla Firefox dalla versione 2.0, Apple Safari dalla versione 3.2.1 e tutte le versioni di Google Chrome.

Il pacchetto Apache distribuito da Debian è compilato con il supporto SNI; quindi non è necessaria alcuna configurazione speciale.

Occorre anche accertarsi che la configurazione del primo virtual host (quello predefinito) abiliti il TLSv1 perché Apache usa i parametri del primo virtual host per stabilire le connessioni sicure ed è imprescindibile.

Gli extra virtual hosts vengono definiti invece da un file archiviato nella directory `/etc/apache2/sites-available/`. Per configurare un website con dominio `falcot.org` si dovrà semplicemente creare il file sottostante e poi attivare il virtual host con `a2ensite www.falcot.org`.

Esempio 11.16 Il file `/etc/apache2/sites-available/www.falcot.org.conf`

```
<VirtualHost *:80>
ServerName www.falcot.org
ServerAlias falcot.org
DocumentRoot /srv/www/www.falcot.org
</VirtualHost>
```

L'Apache server fino a questo punto è stato configurato per utilizzare gli stessi log files per tutti i virtual hosts (configurazione che potrà comunque essere modificata includendo le direttive `CustomLog` nelle descrizioni dei virtual host). È consigliabile pertanto personalizzare il formato del log file per includere il nome del virtual host. Per ottenere ciò, occorre aggiungere un file `/etc/apache2/conf-available/customlog.conf` che definisca un nuovo formato per tutti i log files (attraverso la direttiva `LogFormat`) e procedere alla sua attivazione attraverso `a2enconf customlog`. È inoltre necessario eliminare (o commentare) la riga `CustomLog` dal file `/etc/apache2/sites-available/000-default.conf`.

Esempio 11.17 Il file /etc/apache2/conf.d/customlog.conf

```
# New log format including (virtual) host name
LogFormat "%v %h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\"" vhost

# Now let's use this "vhost" format by default
CustomLog /var/log/apache2/access.log vhost
```

11.2.3. Common Directives (Le direttive maggiormente utilizzate)

Questa paragrafo esamina brevemente alcune delle direttive maggiormente utilizzate per la configurazione di Apache.

Il file di configurazione principale di solito contiene diversi Directory blocks; quest'ultimi consentono di configurare specificatamente le funzionalità del server in base alla posizione del file da supportare. I blocchi in genere includono le direttive Options e AllowOverride.

Esempio 11.18 Directory block

```
<Directory /var/www>
Options Includes FollowSymlinks
AllowOverride All
DirectoryIndex index.php index.html index.htm
</Directory>
```

La direttiva DirectoryIndex definisce l'elenco dei files da utilizzare per verificare se la richiesta di un client è compatibile ad una directory. Il primo file che corrisponde nell'elenco viene utilizzato ed inviato come risposta.

Alla direttiva Options segue un elenco di opzioni da abilitare. Il valore None disabilita tutte le opzioni; diversamente All attiva tutte le opzioni tranne MultiViews. Ecco le opzioni esistenti:

- ExecCGI indica che è possibile eseguire i CGI scripts.
- FollowSymlinks comunica al server che deve tener conto dei collegamenti simbolici, nonché la risposta dovrà includere i contenuti dei targets dei collegamenti simbolici.
- SymlinksIfOwnerMatch comunica al server che deve tener conto dei collegamenti simbolici, ma solo se il collegamento simbolico ed il suo target appartengono allo stesso proprietario/owner.
- Includes attiva il Server Side Includes (o SSI in breve). Si tratta di direttive direttamente integrate nelle pagine HTML ed eseguite al volo ad ogni richiesta.
- Indexes comunica al server di elencare i contenuti della cartella se la richiesta HTTP inviata dal client punta ad una directory priva di un index file (ad esempio quando nessuno dei files menzionati dalla direttiva DirectoryIndex si trova nella directory).
- MultiViews attiva la content negotiation (trad. lett. “la negoziazione dei contenuti”); viene utilizzata dal server per restituire la pagina web in base alla lingua prescelta che è stata configurata nel browser web.

BASILARE .htaccess file

Il file `.htaccess` contiene le direttive della configurazione di Apache, prese in esame ogni volta che viene effettuata una richiesta in merito ad un elemento nella directory in cui lo stesso file `.htaccess` è memorizzato. L'effetto delle direttive del file `.htaccess` è ricorsivo e pertanto ricade anche sulle subdirectories contenute dalla directory in cui lo stesso file `.htaccess` si trova.
La maggior parte delle direttive che possono essere inserite in un Directory block sono consentite anche in un file `.htaccess`.

La direttiva `AllowOverride` elenca tutte le opzioni che possono essere abilitate o disabilitate tramite un file `.htaccess`. Questa opzione viene comunemente utilizzata per limitare l'`ExecCGI`, in modo che l'amministratore possa scegliere gli utenti autorizzati ad eseguire programmi sotto l'identità del web server (ovvero al di sotto del profilo utente `www-data`).

11.2.3.1 Come richiedere l'Autenticazione

In alcuni casi è necessario limitare l'accesso ad una parte di un sito web, in modo che solo gli utenti autorizzati, immettendo un nome utente ed una password, possano accedere ai suoi contenuti.

Esempi. 11.19 Il file `.htaccess` impone la richiesta di autenticazione

```
Require valid-user
AuthName "Private directory"
AuthType Basic
AuthUserFile /etc/apache2/authfiles/htpasswd-private
```

SICUREZZA Nessuna sicurezza

Il sistema di autenticazione (Basic) richiesto nell'esempio soprastante ricorre ad un metodo di sicurezza minimale in cui le passwords vengono inviate in chiaro (codificate in base64 - che è una semplice codifica e non metodo di crittografia). Inoltre anche i documenti "protetti" da questo meccanismo circolano nella rete in chiaro. Pertanto se per voi la sicurezza conta dovrete criptare l'intera connessione HTTP tramite SSL.

Il file `/etc/apache2/authfiles/htpasswd-prive` contiene l'elenco degli utenti e le loro passwords; il comando `htpasswd` viene comunemente utilizzato per modificare e gestire il suddetto file. Difatti, come nell'esempio sottostante, il comando `htpasswd` viene impiegato per aggiungere un utente o modificare le passwords:

```
# htpasswd /etc/apache2/authfiles/htpasswd-private user
New password:
Re-type new password:
Adding password for user user
```

11.2.3.2 Come limitare l'Accesso

La direttiva `Require` gestisce le restrizioni di accesso ad una directory (ed alle sue subdirectories, ricorsivamente).

Questa direttiva può essere utilizzata per limitare l'accesso in base a diversi criteri; qui descriveremo soltanto le restrizioni di accesso basate sugli indirizzi IP del client, in quanto le direttive `Require` se combinate in un blocco `RequireAll` hanno un effetto più considerevole.

Esempio 11.20 Accesso consentito solo da rete locale

```
Require ip 192.168.0.0/16
```

ALTERNATIVA Vecchia sintassi

La sintassi `Require` è disponibile solo a partire dalla versione di Apache 2.4 (la versione presente in Jessie). La sintassi di Apache 2.2 (la versione disponibile per gli utenti di Wheezy) è diversa ed è stata qui descritta come mera nozione sebbene la si possa utilizzare anche con Apache 2.4 attraverso il modulo `mod_access_compat`.

Le direttive `Allow from` e `Deny from` gestiscono le restrizioni di accesso di una directory (e ricorsivamente delle sue subdirectories).

La direttiva `Order` comunica al server in quale ordine deve prendere in esame le direttive `Allow from` e `Deny from`; la priorità spetta all'ultima direttiva di cui è possibile il matching. In concreto, `Order deny, allow` consente l'accesso se non è possibile il matching di `Deny from` o se è possibile il matching di `Allow from`. Al contrario, `Order allow, deny` nega l'accesso se nessuna direttiva `Allow from` consente il matching (o se è possibile il matching di una direttiva `Deny from`).

Le direttive `Allow from` e `Deny from` possono riguardare un indirizzo IP, una rete (ad esempio `192.168.0.0/255.255.255.0`, `192.168.0.0/24` e persino `192.168.0`), un hostname o un domain name o la keyword `all` (che equivale a “chiunque”).

Ad esempio, per vietare le connessioni per impostazione predefinita e consentire le connessioni provenienti solo dalla rete locale, è possibile utilizzare:

```
Order deny,allow  
Allow from 192.168.0.0/16  
Deny from all
```

11.2.4. Log Analyzers

Spesso viene installato un Log Analyzer sul server web; la ragione è che un Log Analyzer consente agli amministratori di avere un'idea più precisa in merito ai patterns impiegati sul web server.

Gli amministratori della Falcot Corp hanno scelto AWStats (Advanced Web Statistics) per analizzare i log files di Apache.

Il primo passo nella configurazione è personalizzare il file `/etc/awstats/awstats.conf`. Gli amministratori della Falcot Corp si sono limitati a modificare i seguenti parametri:

```
LogFile="/var/log/apache2/access.log"
LogFormat = "%virtualname %host %other %logname %time1 %methodurl %code %bytesd %
-> refererquot %uaquot"
SiteDomain="www.falcot.com"
HostAliases="falcot.com REGEX[^.*\.\.falcot\.com$]"
DNSLookup=1
LoadPlugin="tooltips"
```

Tutti questi parametri sono documentati attraverso i commenti nel template file [il file usato da modello]. In particolare, i parametri LogFile e LogFormat indicano la posizione ed il formato del log file e le informazioni in esso contenute; SiteDomain e HostAliases elencano i diversi nomi associati al sito web principale.

Per i siti ad alto traffico e quindi diversamente dall'esempio soprastante della Falcot Corp, non è consigliabile impostare il DNSLookup ad 1; d'altra parte, questa impostazione consente ai siti di piccole dimensioni, come quello della Falcot Corp, di ottenere reports più human readable in quanto includono full machine names anziché raw IP address.

SICUREZZA Accesso alle statistiche

Le statistiche di AWStats sono disponibili per impostazione predefinita sul sito web senza restrizioni, ma potrete comunque configurarle in modo che solo pochi indirizzi IP (solitamente interni) possano accedervi; l'elenco degli indirizzi IP a cui è concesso l'accesso deve essere riportato nel parametro AllowAccessFromWebToFollowingIPAddresses.

AWStats verrà abilitato anche per gli altri virtual hosts; ma ciascun virtual host necessiterà di un file dedicato /etc/awstats/awstats.www.falcot.org.conf.

Esempio. 11.21 Il file di configurazione AWStats dedicato ad un virtual host

```
Include "/etc/awstats/awstats.conf"
SiteDomain="www.falcot.org"
HostAliases="falcot.org"
```

AWStats utilizza diverse icone memorizzate nella directory /usr/share/awstats/icon/. Per renderle disponibili sul sito web, è necessario modificare la configurazione di Apache in modo che includa la seguente direttiva:

```
Alias /awstats-icon/ /usr/share/awstats/icon/
```

Dopo pochi minuti (ed una volta che lo script verrà eseguito un paio di volte), i risultati saranno disponibili online:

- ♦ <http://www.falcot.com/cgi-bin/awstats.pl>
- ♦ <http://www.falcot.org/cgi-bin/awstats.pl>

ATTENZIONE
Log file rotation

Affinché le statistiche di AWStats tengano conto di tutti i logs, è necessario che AWStats venga messo in esecuzione prima che i log files di Apache vengano ruotati. La direttiva `prerotate` del file `/etc/logrotate.d/apache2` fornisce gli elementi utili per risolvere il problema ossia attraverso la creazione di un sym link (un collegamento simbolico) a `/usr/share/awstats/tools/update.sh` nella directory `/etc/logrotate.d/httpd-prerotate`:

```
$ cat /etc/logrotate.d/apache2
/var/log/apache2/*.log {
    daily
    missingok
    rotate 14
    compress
    delaycompress
    notifempty
    create 644 root adm
    sharedscripts
    postrotate
        if /etc/init.d/apache2 status > /dev/null ; then \
            /etc/init.d/apache2 reload > /dev/null; \
        fi;
    endscript
    prerotate
    if [ -d /etc/logrotate.d/httpd-prerotate ]; then \
        run-parts /etc/logrotate.d/httpd-prerotate; \
    fi; \
    endscript
}
$ sudo mkdir -p /etc/logrotate.d/httpd-prerotate
$ sudo ln -sf /usr/share/awstats/tools/update.sh \
/etc/logrotate.d/httpd-prerotate/awstats
```

Dovrete assicurarvi che chiunque abbia i permessi di lettura dei log files creati da logrotate, in particolare AWStats. Nell'esempio soprastante ciò viene garantito dalla riga `create 644 root adm`, (che in sostanza si occupa della sostituzione dei permessi 640 predefiniti).

11.3. FTP File Server

Il File Transfer Protocol (FTP) è stato uno dei primi protocolli su Internet (l'RFC 959 è stato emesso nel 1985!). Questo protocollo è stato utilizzato per distribuire files prima dell'invenzione del Web (il protocollo HTTP è stato creato nel 1990 e formalmente definito nell' RFC 1945 rilasciato nel 1996).

Questo protocollo consente l'upload ed il download dei files; per tale ragione è ancora comunemente impiegato per il deployment degli aggiornamenti di un sito web ospitato da un provider di servizi Internet (o da una terza parte che ospita siti web). Generalmente viene imposto il secure access attraverso l'user identifier (UID) e password; se l'autenticazione ha buon fine l'FTP server concede i permessi di lettura e scrittura per accedere all'user's home directory.

Inoltre gli FTP servers vengono utilizzati anche per distribuire files per il public downloading; i pacchetti Debian sono un esempio di public downloading. I contenuti degli FTP servers vengono recuperati da altri servers, geograficamente remoti; dopodiché quest'ultimi, essendo meno remoti nei confronti degli utenti, rendono disponibili i contenuti all'utenza. In questo caso, l'autenticazione del client non è necessaria; questo sistema viene definito "anonymous FTP". In realtà anche in questo caso l'FTP server effettua un'autenticazione solo che i clients si identificano con l'username `anonymous` ed una password che per convenzione è l'indirizzo di posta elettronica dell'utente.

Diversi FTP servers sono distribuiti da Debian (`ftpd`, `proftpd-basic`, `pyftpd`, ecc.). Gli amministratori della Falcot Corp hanno scelto `vsftpd` perché necessitano di un FTP server solo per distribuire pochi files (ed un repository di pacchetti Debian); per di più gli amministratori della Falcot Corp non avendo bisogno di funzionalità complesse hanno preferito concentrarsi sulla sicurezza.

L'installazione del pacchetto crea un `ftp` system user. Questo account viene sistematicamente utilizzato per le connessioni anonymous FTP e la sua home directory (`/srv/ftp/`) è la radice (root) della struttura ad albero messa a disposizione degli utenti che si connettono al servizio. La configurazione predefinita (che si trova nel file `/etc/vsftpd.conf`) richiede alcune modifiche per soddisfare la mera esigenza di fruibilità di files di grandi dimensioni per il downloading pubblico: l'anonymous access deve essere abilitato (`anonymous=YES`) mentre il permesso di sola lettura (`read-only`) degli utenti locali deve essere disabilitato (`local_enable=NO`). Quest'ultimo punto è particolarmente importante dato che il protocollo FTP non fa uso di alcuna forma di crittografia e la password dell'utente potrebbe essere intercettata da una connessione via cavo.

11.4. NFS File Server

NFS (Network File System) è un protocollo che consente l'accesso remoto ad un filesystem attraverso la rete. Questo protocollo è supportato da tutti i sistemi Unix; se sono presenti delle macchine Windows, dovete invece usare Samba.

Sebbene NFS sia uno strumento molto utile, in passato presentava diverse limitazioni, la maggior risolte con la versione 4 del protocollo. Purtroppo però l'ultima versione di NFS è complessa da configurare se si desidera sfruttare delle funzionalità di sicurezza di base come l'autenticazione e la crittografia, dato che si basano su Kerberos. E senza tali funzionalità, il protocollo NFS può essere utilizzato solo su una rete locale fidata, perché i dati che circolano sulla rete non sono crittografati (uno sniffer può intercettarli) ed i permessi di accesso vengono concessi solo in base all'indirizzo IP del client (che può essere falsificato - spoofing).

DOCUMENTAZIONE NFS howto

La documentazione sul deployment di NFSv4 è abbastanza scarna. In basso sono riportati alcuni collegamenti dai contenuti di qualità varia che potranno fungere da punto di partenza su come procedere.

- ♦ <https://help.ubuntu.com/community/NFSv4Howto>
- ♦ http://wiki.linux-nfs.org/wiki/index.php/Nfsv4_configuration

11.4.1. Securing NFS [come configurare le funzionalità di sicurezza di NFS]

Se non desiderate impiegare le funzionalità di sicurezza basate su Kerberos, dovete assicurarvi che solo delle macchine autorizzate possano usufruire di NFS e connettersi ai diversi RFC servers, perché il protocollo di base fondamentalmente considera fidati i dati ricevuti dalla rete. Il firewall deve essere in grado di impedire lo spoofing dell'indirizzo IP in modo da scongiurare che una macchina esterna possa agire con l'identità di una macchina interna, imponendo delle restrizioni a dei ports specifici, impiegati dalle macchine che intendono accedere alle condivisioni NFS.

BASILARE	
RPC	RPC (Remote Procedure Call) è uno standard Unix per i servizi remoti, tra cui NFS. I servizi RPC vengono registrati in una directory nota come portmapper. Un client che desidera effettuare una NFS query la indirizza prima al portmapper (sul port 111 in TCP o UDP) per chiedere informazioni sull'NFS server; la risposta di solito indica il port 2049 (di default per NFS). Non tutti i servizi RPC fanno uso di un port predefinito.

Le versioni precedenti del protocollo richiedevano ulteriori servizi RPC che impiegavano i ports assegnati dinamicamente. Fortunatamente, la versione 4 di NFS necessita solo dei ports 2049 (per NFS) e 111 (per il portmapper), rendendo più facile il compito del firewall.

11.4.2. NFS Server

L'NFS server è integrato nel kernel di Linux; Debian lo distribuisce compilato come modulo del kernel. Per attivarlo automaticamente ad ogni avvio, è necessario installare il pacchetto `nfs-kernel-server`; questo pacchetto include gli start-up scripts pertinenti.

Il file di configurazione dell'NFS server, `/etc(exports`, elenca le directories rese disponibili sulla rete (`exported`). Ciascun NFS share riserva l'accesso a delle date macchine. Qualora necessitiate di un access control più “fine-grained” vi basteranno poche opzioni. La sintassi di questo file è abbastanza semplice:

```
/directory/to/share machine1(option1,option2,...) machine2(...) ...
```

Si precisa che l'NFSv4 prevede che tutte le directories esportate devono far parte di un singola gerarchia e che la root directory della gerarchia deve essere esportata ed identificata con l'opzione `fsid=0` o `fsid=root`.

Ogni macchina può essere identificata per mezzo del suo nome DNS o attraverso il suo indirizzo IP. È anche possibile specificare un intero set di macchine utilizzando la sintassi `*.falcot.com` oppure indicare un IP address range come ad esempio `192.168.0.0/255.255.255.0` o `192.168.0.0/24`.

Le directories vengono condivise soltanto in modalità `read-only` (in breve `ro`) - “lettura”. L'opzione `rw` (`read-write`) consente sia la lettura che la scrittura. Gli NFS clients per impostazione predefinita si connettono ad un port riservato solo al root (con un numero di port inferiore a 1024 - 1024 non compreso) [tale restrizione consente l'accesso all'NFS share solo agli users delle macchine con titolarità dei diritti e dei permessi equivalenti a quelli di root]; diversamente se non si desidera tale restrizione occorre attivare l’“`insecure option`” (la “`secure option`” è implicita, ma per maggiore trasparenza potrà comunque essere menzionata).

Il server per impostazione predefinita non risponde a una NFS query se l'operazione sul disco in atto non è stata completata (a causa della `sync option`); la `async option` disattiva la `sync option`.

La modalità di scrittura asincrona migliora leggermente le prestazioni, a discapito dell'affidabilità (reliability) essendoci il rischio fondato di perdita di dati a causa di un ipotetico crash del server durante la fase di acknowledgement [non lett. "ricezione"] sia dei dati scritti, sia dei dati in corso di scrittura. Dato che il suo valore predefinito è cambiato di recente (rispetto al valore storico di NFS), si consiglia una configurazione esplicita.

Per evitare di concedere il root access al filesystem a qualsiasi client NFS, tutte le queries (richieste) apparentemente provenienti da un root user vengono considerate dal server come queries del nobody user. Tale funzionalità corrisponde all'opzione `root_squash`, abilitata per impostazione predefinita. Diversamente l'opzione `no_root_squash`, che disabilita la suddetta funzionalità, è rischiosa e dovrebbe essere usata soltanto in un controlled environment [lett. "ambiente controllato"]. Le opzioni `anonuid=uid` e `anongid=gid` consentono di impostare un altro fake user da utilizzare al posto di `UID/GID 65534` (che corrisponde all' user `nobody` ed al group `nogroup`). L'NFSv4 consente di aggiungere un'opzione `sec` per specificare il livello di sicurezza desiderato: `sec=sys` è il valore predefinito senza alcuna sicurezza particolare, `sec=krb5` attiva solo l'autenticazione, `sec=krb5i` aggiunge l'integrity protection e `sec=krb5p` è il livello più alto che include la privacy protection (per mezzo della crittografia dei dati). Affinché tutto ciò funzioni, è necessario configurare Kerberos (ma questo servizio non viene trattato da questo libro). Ci sono anche altre opzioni disponibili, che troverete nella man page `exports` (5).

ATTENZIONE

Installazione
iniziale

Il boot script `/etc/init.d/nfs-kernel-server` avvia il server solo se il file `/etc/export` elenca uno o più NFS share validi. Dopo la configurazione iniziale del suddetto file dovrete avviare il server NFS con il seguente comando:

```
# service nfs-kernel-server start
```

11.4.3. NFS Client

Come gli altri filesystems, per integrare l'NFS share nella gerarchia di un file system dovrete eseguirne il mounting. Dato che si tratta di un filesystem con delle particolari specifiche, dovrete effettuare delle modifiche sfruttando la sintassi del comando `mount` ed il file `/etc/fstab`.

Esempio 11.22 Montaggio manuale attraverso il comando `mount`

```
# mount -t nfs4 -o rw,nosuid arrakis.internal.falcot.com:/shared /srv/  
-> shared
```

Esempio 11.23 L'NFS entry del file `/etc/fstab`

```
arrakis.internal.falcot.com:/shared /srv/shared nfs4 rw,nosuid 0 0
```

L'entry precedentemente descritta monta automaticamente al system startup la directory NFS / share/ del server arrakis nella directory locale /srv/share/ .

La modalità di accesso necessaria è di `read/write` [lettura/scrittura] (ovvero il parametro `rw`). L'opzione `nosuid` è una misura di sicurezza che rimuove qualsiasi `setuid` o `setgid` presente sui programmi contenuti nella condivisione. Se l'NFS share è dedicato solo all'archiviazione dei documenti, si consiglia di utilizzare anche l'opzione `noexec` che impedisce la messa in esecuzione di eventuali programmi archiviati nell'NFS share. Si precisa che sul server, la directory `shared` è una subdirectory dell'NFSv4 `root export` (ad esempio `/export/shared`) e quindi non una top-level directory.

La man page `nfs(5)` descrive in dettaglio tutte le possibili opzioni.

11.5. Configurare Windows Shares attraverso Samba

Samba è una suite di strumenti per la gestione del protocollo SMB (denominato anche "CIFS") in Linux. Il protocollo SMB viene utilizzato da Windows per accedere alle condivisioni di rete e alle stampanti condivise.

Samba è in grado anche di svolgere il ruolo di Windows domain controller. Questo strumento straordinario garantisce una perfetta coesistenza tra servers Linux e desktop aziendali che eseguono ancora Windows.

11.5.1. Samba Server

Il pacchetto samba di Debian include i due principali servers di Samba 4, `smbd` e `nmbd`.

DOCUMENTAZIONE Approfondimento

Il server Samba è estremamente configurabile e versatile, difatti può soddisfare diversi use cases con differenti esigenze di specifiche ed architetture di rete. Questo manuale si concentra su un solo use case in cui Samba viene utilizzato come standalone server, ma in realtà può svolgere il ruolo anche di un NT4 Domain Controller, di un full Active Directory Domain Controller oppure semplicemente essere parte di un pre-esistente dominio (che potenzialmente potrebbe essere gestito da un Windows server).

Il pacchetto `samba-doc` contiene un ingente numero di example files commentati in `/usr/share/doc/samba-doc/examples/`.

STRUMENTI TOOLS L'autenticazione attraverso un Windows server

Winbind consente agli amministratori di sistema di utilizzare un Windows server come un authentication server. Winbind inoltre si integra perfettamente con PAM e NSS. Ciò consente di configurare macchine Linux in cui tutti gli utenti di un Windows domain riceveranno automaticamente un account. Troverete maggiori informazioni nella directory `/usr/share/doc/samba-doc/examples/pam_winbind/`.

11.5.1.1 Configurazione con debconf

Il pacchetto imposta una configurazione minimale durante l'installazione iniziale, ma è preferibile che eseguiate il comando `dpkg-reconfigure samba-common` per personalizzarla. La prima informazione richiesta è il nome del workgroup in cui il Samba server verrà integrato (la risposta nel caso della Falcot è `FALCOTNET`).

Il pacchetto propone inoltre l'identificazione del WINS server attraverso le informazioni fornite dal demone DHCP. Gli amministratori della Falcot Corp hanno preferito rifiutare questa opzione, poiché intendono utilizzare lo stesso Samba server come WINS server.

11.5.1.2 Configurazione manuale

11.5.1.2.1 Le modifiche a smb.conf Le esigenze della Falcot impongono che debbano essere modificate altre opzioni nel file di configurazione di Samba /etc/samba/smb.conf. I seguenti estratti riportano le modifiche apportate all'interno della sezione [global].

```
[global]

## Browsing/Identification ##

# Change this to the workgroup/NT-domain name your Samba server will part of
workgroup = FALCOTNET

# Windows Internet Name Serving Support Section:
# WINS Support - Tells the NMBD component of Samba to enable its WINS Server
wins support=yes (1)

[...]

##### Authentication #####
# Server role. Defines in which mode Samba will operate. Possible
# values are "standalone server", "member server", "classic primary
# domain controller", "classic backup domain controller", "active
# directory domain controller".
#
# Most people will want "standalone sever" or "member server".
# Running as "active directory domain controller" will require first
# running "samba-tool domain provision" to wipe databases and create a
# new domain.
    server role = standalone server
# "security = user" is always a good idea. This will require a Unix account
# in this server for every user accessing the server.
    security=user (2)

[...]
```

(1) Specifica che Samba deve svolgere il ruolo nella rete locale di Netbios name server (Wins).

(2) Questo è il valore predefinito per tale parametro; tuttavia, essendo di particolare importanza per la configurazione di Samba, viene comunque dichiarato esplicitamente. Ogni utente deve autenticarsi prima di poter accedere a qualsiasi condivisione.

11.5.1.2.2 Come aggiungere gli Utenti Ciascun utente di Samba necessita di un account sul server; devono essere creati prima gli account Unix e poi è necessario registrarli nel database di Samba. La creazione degli account Unix solitamente è quella consueta (con il comando `adduser` per esempio). Per aggiungere un utente Unix al database Samba dovrete eseguire il comando `smbpasswd -a user`; il comando vi richierà in risposta la password. Un utente può essere rimosso con il comando `smbpasswd -x user`. Un account Samba può essere temporaneamente disabilitato con il comando `smbpasswd -d user` e poi riattivato con il comando `smbpasswd -e user`.

11.5.2. Samba Client

Le client features in Samba consentono ad una macchina Linux di accedere alle condivisioni Windows ed alle stampanti condivise. I programmi necessari sono inclusi nei pacchetti Debian `cifs-utils` e `smbclient`.

11.5.2.1 Il programma smbclient

Il programma `smbclient` interroga tutti i servers SMB. Accetta l'opzione `-U user` per connettersi al server con un'identità specifica. Attraverso `smbclient //server/share` l'accesso alla condivisione avverrà in modalità interattiva similmente ad un FTP client da riga di comando. Il comando `smbclient -L server` elenca tutte le condivisioni sul server disponibili (e visibili).

11.5.2.1 Mounting delle Windows Shares

Il comando `mount` consente il mounting di una Windows share nella gerarchia ad albero del filesystem di Linux (per mezzo di `mount.cifs` supportato da `cifs-utils`).

Esempio 11.24 Mounting di una Windows share

```
mount -t cifs //arrakis/shared /shared \
      -o credentials=/etc/smb-credentials
```

Il file `/etc/smb-credentials` (che non dovrà essere leggibile dagli utenti) presenta il seguente formato:

```
username = user
password = password
```

Possono essere definite altre opzioni da riga di comando; l'elenco completo di tali opzioni si trova in `mount.cifs(1)`. In particolare due opzioni sono meritevoli di essere menzionate: `uid` e `gid` che consentono rispettivamente di forzare l'accesso dei files disponibili sul mount al loro owner (`uid`) ed al loro group (`gid`) in modo che la disponibilità dei suddetti files non venga limitata solo a root. È anche possibile configurare il mounting di una Windows share in `/etc/fstab`:

```
//server/shared /shared cifs credentials=/etc/smb-credentials
```

L'unmounting di una SMB/CIFS share può essere effettuato attraverso il comando `umount` standard.

11.5.2.3 Come stampare su una stampante condivisa

CUPS è una soluzione elegante per stampare da una workstation Linux su una stampante condivisa da una macchina Windows. Se `smbclient` è installato, CUPS offre la possibilità di installare automaticamente le stampanti condivise attraverso Windows.

I passaggi necessari sono i seguenti:

- Accedete all'interfaccia di configurazione di CUPS: `http://localhost:631/admin`
- Fate clic su "Add Printer".
- Scegliete il dispositivo di stampa, selezionando "Windows Printer via SAMBA".
- Immettete la connessione URI della stampante di rete. Dovrete rispettare il seguente formato: `smb://user:password@server/printer`.
- Immettete il nome che identificherà in modo univoco la stampante. Dopodiché inserite una descrizione e la posizione della stampante. Queste stringhe vengono utilizzate per consentire agli utenti di identificare le stampanti.
- Indicate il nome del produttore ed il modello della stampante oppure rilasciate direttamente un working printer description file (PPD).

E voilà, la stampante sarà funzionale!

11.6. Proxy HTTP/FTP

Un proxy HTTP/FTP fa da intermediario per le connessioni HTTP e/o FTP. Il suo ruolo è duplice:

- **Caching:** conserva localmente una copia dei documenti scaricati recentemente, per evitare che gli stessi files vengano scaricati più volte.
- **Filtering server:** se è stato delegato [in inglese "mandated"] un proxy, le connessioni in uscita devono obbligatoriamente attraversarlo altrimenti verranno bloccate e pertanto è il proxy a stabilire quali richieste sono legittime oppure no.

Il server proxy utilizzato dalla Falcot Corp è Squid.

11.6.1. Installazione

Il pacchetto Debian `squid3` contiene solo un modular (caching) proxy. La conversione in un filtering server richiede che venga aggiunto il pacchetto `squidguard`. Il pacchetto `squid-cgi` supporta un'interfaccia per il querying e l'amministrazione di un proxy Squid.

Prima dell'installazione dovete avere cura di verificare che il sistema sia in grado di identificare il suo stesso nome completo: il comando `hostname -f` dovrebbe restituirlvi un fully-qualified name (che includa un dominio). In caso contrario, dovete modificare `/etc/hosts` in modo che conteggi il full name del sistema (per esempio: `arrakis.falcot.com`). Dovrete accordarvi per la scelta del nome ufficiale del computer con l'amministratore di rete così da scongiurare potenziali conflitti per i nomi.

11.6.2. Configurazione di una cache

Per abilitare la caching server feature dovete modificare il file di configurazione `/etc/squid3/squid.conf` per consentire alle macchine di eseguire le queries dalla rete locale attraverso il proxy. L'esempio seguente mostra le modifiche apportate dagli amministratori della Falcot Corp.

Esempio 11.25 Estratti del file `/etc/squid3/squid.conf`

```
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS

# Example rule allowing access from your local networks. Adapt
# to list your (internal) IP networks from where browsing should
# be allowed
acl our_networks src 192.168.1.0/24 192.168.2.0/24
http_access allow our_networks
http_access allow localhost
# And finally deny all other access to this proxy
http_access deny all
```

11.6.3. Come configurare un filtro

squid non si occupa del filtering; questa operazione viene delegata a squidGuard. Dovrete pertanto configurare squid affinché interagisca con squidGuard. Ovvero dovete aggiungere la seguente direttiva al file `/etc/squid3/squid.conf`:

```
url_rewrite_program /usr/bin/squidGuard -c /etc/squid3/squidGuard.conf
```

Dovrete installare anche il programma CGI `/usr/lib/cgi-bin/squidGuard.cgi` utilizzando come modello il file `/usr/share/doc/squidguard/examples/squidGuard.cgi.gz`. Occorre inoltre modificare questo script attraverso le variabili `$proxy` (nome del server proxy) e `$proxymaster` (l'email di contatto dell'amministratore). Le variabili `$image` e `$redirect` dovranno puntare alle immagini esistenti, che simboleggiano il rifiuto della query.

Il comando che attiva il filtro è `service squid3 reload`. Il pacchetto `squidguard` non offre un filtering predefinito, pertanto dovrà essere l'amministratore a configurarne la policy.

L'amministratore per fare ciò dovrà creare il file `/etc/squid3/squidGuard.conf` (usando al bisogno come modello `/etc/squidguard/squidGuard.conf.default`).

Dopo ogni modifica del file di configurazione di `squidGuard` (o di uno qualsiasi degli elenchi di domini o di URLs in esso menzionati), è necessario rigenerare il database in funzione attraverso il comando `update-squidguard`. La sintassi del file di configurazione è documentata nel seguente sito web:

- ♦ <http://www.squidguard.org/Doc/configure.html>

ALTERNATIVA DansGuardian

Il pacchetto `dansguardian` è un'alternativa a `squidguard`. Questo software non solo gestisce una blacklist degli URLs proibiti, ma può fare riferimento al sistema PICS (Platform for Internet Content Selection) per decidere se una pagina è accettabile o meno attraverso una dynamic analysis sui suoi contenuti.

11.7. LDAP Directory

L'OpenLDAP è un implementazione del protocollo LDAP; in poche parole è un special-purpose database designato allo storing directories. [In elettronica special-purpose assume il significato di "con compiti specifici", diversamente general-purpose assume il significato di "con compiti generici". Lo "storing directories" si riferisce alla mera conservazione delle informazioni delle directories; tali informazioni sono necessarie per la condivisione stessa delle directories sulla rete]. Nella maggior parte degli use cases, l'impiego di un LDAP server consente la centralizzazione della gestione degli accounts degli utenti e della loro correlata titolarità dei diritti. Inoltre, un database LDAP è agevole da duplicare, il che permette la configurazione di multiple synchronized LDAP servers. In caso di una repentina crescita della rete e dell'utenza, potrete distribuire il carico tra i diversi servers.

I dati LDAP sono organizzati in una gerarchia. Tale struttura gerarchizzata è definita "schema" e quest'ultima dichiara gli oggetti che il database può memorizzare per mezzo di un elenco di tutti i loro possibili attributi. La sintassi utilizzata per richiamare un oggetto del database riflette la suddetta struttura e di conseguenza ne spiega la complessità.

11.7.1. Installazione

Il pacchetto `slapd` contiene il server OpenLDAP. Il pacchetto `ldap-utils` contiene invece le utilità da riga di comando per interagire con i servers LDAP.

Purtroppo l'installazione del pacchetto `slapd` pone poche domande e l'effetto di ciò è un database che raramente soddisfa delle peculiari esigenze. Ma per rimediare dovete solo eseguire il comando `dpkg-reconfigure slapd` per riconfigurare dettagliatamente il database LDAP:

- Omit OpenLDAP server configuration? - Desiderate saltare la configurazione dell'OpenLDAP server? Rispondete "NO", in quanto desiderate configurare questo servizio.
- DNS domain name - Qual è DNS domain name? "falcot.com".
- Organization name - Qual è il nome dell'organizzazione-società? "Falcot Corp".
- An administrative password needs to be typed in. Occorre immettere una password per l'amministratore.
- Database backend to use - Database backend da utilizzare? "MDB".
- Do you want the database to be removed when `slapd` is purged? - Il database deve essere rimosso se il pacchetto `slapd` viene "purged"? Rispondete di "No". In questo modo qualora il summenzionato pacchetto fosse "purgato" per sbaglio non rischierete di perdere anche il database.
- Move old database? - Il precedente database deve essere spostato? Questa domanda viene posta solo se viene richiesta una nuova configurazione e se già esiste un database. Rispondete di "SI" solo se volete effettuare un'installazione pulita del database ad esempio dopo un'installazione iniziale non congeniale e dopo aver eseguito `dpkg-reconfigure slapd`.

- Allow LDAPv2 protocol? - Volete consentire il protocollo LDAPv2? No, non ne vale la pena. Tutti i tools che verranno impiegati sono compatibili con il protocollo LDAPv3.

BASILARE Formato LDIF	Un LDIF file (LDAP Data Interchange Format) è un portable text file che descrive i contenuti (tutti o in parte) di un database LDAP in modo che possa essere usato per integrare i dati in qualunque altro server LDAP.
---------------------------------	---

Giunti a questo punto otterrete la configurazione di un minimal database, che potrete verificare utilizzando la seguente query:

```
$ ldapsearch -x -b dc=falcot,dc=com
# extended LDIF
#
# LDAPv3
# base <dc=falcot,dc=com> with scope sub
# filter: (objectclass=*)
# requesting: ALL
#
# falcot.com
dn: dc=falcot,dc=com
objectClass: top
objectClass: dcObject
objectClass: organization
o: Falcot Corp
dc: falcot

# admin, falcot.com
dn: cn=admin,dc=falcot,dc=com
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator

# search result
search: 2
result: 0 Success

# numResponses: 3
# numEntries: 2
```

La query dell'esempio soprastante ha restituito due oggetti: l'organizzazione e l'utente con il ruolo di amministratore.

11.7.2. Compilazione nella directory

Dato che un database vuoto non ha alcuna utilità, occorre iniettargli tutte le directory esistenti, inclusi i database riguardanti gli utenti, i gruppi, i servizi e gli hosts.

Il pacchetto Debian `migrationtools` offre una serie di scripts dedicati all'estrazione dei dati dalle directories Unix standard (`/etc/passwd`, `/etc/group`, `/etc/services`, `/etc/hosts`, ecc.), conversione e loro iniezione nel database LDAP.

Dopo aver installato il pacchetto, dovete modificare il file `/etc/migrationtools/migrate_common.ph`; dovete anche attivare le opzioni `IGNORE_UID_BELOW` e `IGNORE_GID_BELOW` (basta solo rimuovere il commento) ed aggiornare `DEFAULT_MAIL_DOMAIN`/`DEFAULT_BASE`. In concreto la migrazione viene gestita dal comando `migrate_all_online.sh` come segue:

```
# cd /usr/share/migrationtools  
# LDAPADD="/usr/bin/ldapadd -c" ETC_ALIASES=/dev/null ./migrate_all_online.sh
```

Lo script `migrate_all_online.sh` pone alcune domande a cui è necessario rispondere sul database LDAP su cui verrà eseguita la migrazione dei dati.

Domande

X.500 naming context
LDAP server hostname Manager DN
Bind credentials (Credenziali Bind)
Create DUAConfigProfile (Crea un DUAConfigProfile)

Risposte

dc=falcot,dc=com
localhost cn=admin,dc=falcot,dc=com
administrative password
no

Tavola 11.1 Riassume le risposte alle domande poste dallo script `migrate_all_online.sh`

Il file `/etc/aliases` è stato intenzionalmente non tenuto in considerazione per la migrazione, dato che lo schema standard supportato da Debian non include le strutture che il suddetto script impiega per descrivere gli alias di posta elettronica. Essendo necessario integrare questi dati nella directory, bisogna aggiungere il file `/etc/ldap/schema/misc.schema` come schema standard.

STRUMENTI TOOLS

Come consultare
una directory
LDAP

Il comando `jxplorer` (dall'omonimo pacchetto Debian) è uno strumento grafico che consente di consultare e modificare un LDAP database. È tool notevole in quanto fornisce all'amministratore una buona panoramica della struttura gerarchica dei dati LDAP.

È possibile utilizzare anche l'opzione `-c` del comando `ldapadd`; questa opzione impone che il processo non si fermi in caso di errore. Potrebbe servire per la conversione del file `/etc/services` che spesso genera alcuni errori che possono essere tranquillamente ignorati.

11.7.3. La gestione degli Accounts con LDAP

Giunti a questo punto l'LDAP database contiene finalmente diverse informazioni utili, pronte per essere usate. Questo paragrafo si focalizza su come configurare un sistema Linux in modo che le diverse directories utilizzino il database LDAP.

11.7.3.1 Come configurare NSS

Il sistema NSS (Name Service Switch, per maggiori dettagli andate a leggere la casella di testo "Database di sistema e NSS" a pagina 158) è un sistema modulare per definire o recuperare le informazioni dalle directories di sistema. Per utilizzare l'LDAP come sorgente di dati per l'NSS, è necessario installare il pacchetto `libnss-ldap`. La sua installazione pone diverse domande; le risposte sono riassunte nella Tavola 11.2.

Domande	Risposte
LDAP server Uniform Resource Identifier	<code>ldap://ldap.falcot.com</code>
Distinguished name of the search base (Il Distinguished name della search base)	<code>dc=falcot,dc=com</code>
LDAP version to use (versione LDAP da utilizzare)	3
Does the LDAP database require login? (LDAP database necessita del login?)	no
Special LDAP privileges for root (Concedere a root i diritti speciali per l'LDAP)	yes
Make the configuration file readable/writeable by its owner only (Concedere i permessi di scrittura lettura del file di configurazione solo al suo owner)	no
LDAP account for root (l'account root)	<code>cn=admin,dc=falcot,dc=com</code>
LDAP root account password	administrative password

Tavola 11.2 Configurazione del pacchetto `libnss-ldap`

Dopo dovete modificare il file `/etc/nsswitch.conf` per configurare l'NSS in modo che utilizzi l'installazione recente.

Esempio 11.26 Il file `/etc/nsswitch.conf`

```
# /etc/nsswitch.conf
#
# Example configuration of GNU Name Service Switch functionality.
# If you have the 'glibc-doc' and 'info' packages installed, try:
# 'info libc "Name Service Switch"' for information about this file.

passwd: ldap compat
group: ldap compat
shadow: ldap compat

hosts: files dns ldap
networks: ldap files
```

```
protocols: ldap db files
services: ldap db files
ethers: ldap db files
rpc: ldap db files

netgroup: ldap files
```

Il modulo `ldap` viene incluso sistematicamente prima degli altri, quindi verrà interpellato per primo. Fa eccezione l'`hosts` service dal momento che il server LDAP dovrà consultare preventivamente il DNS (per la risoluzione di `ldap.falcot.com`). Senza questa precauzione, potrebbe essere richiesta al server LDAP una hostname query e tale richiesta potrebbe innescare una name resolution per l'LDAP server fino a determinare un loop infinito.

Se desiderate che l'LDAP server assuma il ruolo di "authoritative" (e non tenga conto dei local files utilizzati dal modulo `files`) potrete configurarne i servizi attraverso la sintassi:

```
service:ldap [NOTFOUND=return] files.
```

Se l'entry richiesta non troverà corrispondenza nel database LDAP, la query restituirà "not existing" anche se di fatto la risorsa è presente in uno dei local files; i local files verranno invece utilizzati solo quando il servizio LDAP è inattivo.

11.7.3.2 Come configurare PAM

Questo paragrafo descrive la configurazione di PAM (andate a leggere la casella di testo "/etc/environment e /etc/default/local" a pagina 147) necessaria alle applicazioni per l'esecuzione delle autenticazioni per il database LDAP.

ATTENZIONE
Autenticazione
non funzionante

La modifica della configurazione standard di PAM attuata dai vari programmi è un'operazione piuttosto dolente. Se uno sbaglio compromette l'autenticazione sarà impossibile effettuare il login. Pertanto per precauzione mantenete aperta la shell di root. Dopodiché se la configurazione determina degli errori potrete correggerli con il minimo sforzo.

Il modulo LDAP per PAM è incluso nel pacchetto Debian `libpam-ldap`. L'installazione del pacchetto prevede la richiesta di alcune domande simili a quelle di `libnss-ldap`; alcuni parametri di configurazione (tra cui l'URI del server LDAP) sono condivisi con il pacchetto `libnss-ldap`. Le risposte sono riassunte nella Tavola 11.3.

L'installazione di `libpam-ldap` modifica automaticamente la configurazione predefinita di PAM inclusa nei files `/etc/pam.d/common-auth`, `/etc/pam.d/common-password` e `/etc/pam.d/common-account`. Il pacchetto effettua il suddetto meccanismo per mezzo del tool `pam-auth-update` (incluso nel pacchetto `libpam-runtime`). L'amministratore può al bisogno eseguire il su menzionato tool per attivare e disattivare i moduli PAM.

Domande	Risposte
Allow LDAP admin account to behave like local root? (Consentire all'account LDAP admin di poter agire con gli stessi diritti di local root?)	Si. Ciò consente di utilizzare il comando passwd per cambiare le passwords archiviate nell'LDAP database.
Does the LDAP database require logging in? (LDAP database necessita del login?)	no
LDAP account for root (L'account LDAP per il ruolo di root)	cn=admin,dc=falcot,dc=com
LDAP root account password (La password dell'account root dell'LDAP)	La LDAP database administrative password
Local encryption algorithm to use for passwords (L'algoritmo locale per criptare le passwords)	crypt

Tavola 11.3 Configurazione del libpam-ldap

11.7.3.3 Come proteggere lo Scambio Dati di LDAP

Per impostazione predefinita il protocollo LDAP transita sulla rete come testo in chiaro [non crittografato]. Ciò significa che le passwords crittografate possono essere intercettate sulla rete e decriptate attraverso un attacco a dizionario. Per scongiurare ciò occorre utilizzare un extra encryption layer; questo paragrafo tratta l'attivazione del layer in questione.

11.7.3.3.1 Configurazione lato server Il primo passo è creare una coppia di chiavi (una chiave pubblica ed una chiave privata) per il server LDAP. A tale scopo gli amministratori della Falcot Corp riutilizzano easy-rsa (andate a leggere il paragrafo 10.2.1.1, "Infrastruttura a chiave pubblica: easy-rsa" a pagina 224). L'esecuzione di `./build-server-key ldap.falcot.com` restituisce diverse domande ordinarie (location, organization, ecc.). Dovrete immettere in risposta alla domanda "common name" il fully-qualified hostname del server LDAP; in questo caso `ldap.falcot.com`.

Il precedente comando ha generato un certificato nel file `keys/ldap.falcot.com.crt` e la chiave privata corrispondente è conservata in `keys/ldap.falcot.com.key`.

Dal momento che queste chiavi sono state installate nella loro posizione standard, dovete assicurarvi che il file della chiave privata sia leggibile dal server LDAP, in esecuzione sotto l'identità dell'utente `openldap`:

```
# adduser openldap ssl-cert
Adding user 'openldap' to group 'ssl-cert' ...
Adding user openldap to group ssl-cert
Done.
# mv keys/ldap.falcot.com.key /etc/ssl/private/ldap.falcot.com.key
# chown root:ssl-cert /etc/ssl/private/ldap.falcot.com.key
# chmod 0640 /etc/ssl/private/ldap.falcot.com.key
# mv newcert.pem /etc/ssl/certs/ldap.falcot.com.pem
```

Dovrete configurare anche il demone `slapd` affinché utilizzi le suddette chiavi di crittografia. La configurazione del server LDAP è gestita dinamicamente: può essere aggiornata con le normali operazioni LDAP sull'*object hierarchy* `cn = config` ed i costanti aggiornamenti del server in `/etc/ldap/slapd.d` che rendono persistente la configurazione. [L'*object hierarchy* si riferisce alla discendenza gerarchizzata di un object. In pratica e molto genericamente sono degli objects che definiscono le caratteristiche di un object (a cui sono correlate).

Il termine inglese "location" genericamente significa in italiano "posizione", ma nella manualistica alla stessa stregua del termine inglese "implementation" viene italianizzato in "locazione" (ad esempio "la locazione dei files"). Questi termini sono dei neologismi che possono indurre confusione, in quanto per locazione in italiano si intende un tipo di contratto. Allo stesso tempo "location" in informatica può non significare semplicemente "posizione", bensì può riferirsi a tutte quelle informazioni che individuano la posizione. Un altro esempio è il neologismo "localizzazione" che in italiano significa "essere situato in", ma che in informatica può riferirsi alla traduzione di un

documento. Insomma è palese la carenza di un linguaggio comune: lo preciso solo per rendere evidente la difficoltà per chi traduce ed onde evitare le critiche del saccante di turno.]

Per aggiornare la configurazione dovete usare il tool ldapmodify:

Esempio 11.27 Configurazione di slapd per supportare la crittografia

```
# cat >ssl.ldap <<END
dn: cn=config
changetype: modify
add: olcTLSCertificateFile
olcTLSCertificateFile: /etc/ssl/certs/ldap.falcot.com.pem
-
add: olcTLSCertificateKeyFile
olcTLSCertificateKeyFile: /etc/ssl/private/ldap.falcot.com.key
-
END
# ldapmodify -Y EXTERNAL -H ldapi:/// -f ssl.ldap
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
modifying entry "cn=config"
```

**STRUMENTI
TOOLS**
ldapvi il tool per
modificare un
LDAP directory

ldapvi consente di visualizzare un LDIF output di qualsiasi parte della directory LDAP, di effettuare le modifiche in un editor di testo e di mettere in atto le opportune LDAP operations.
Quindi un metodo particolarmente pratico per aggiornare la configurazione del LDAP server è modificare la gerarchia cn=config.

```
# ldapvi -Y EXTERNAL -h ldapi:/// -b cn=config
```

L'ultimo passaggio per abilitare la crittografia è modificare la variabile SLAPD_SERVICES nel file /etc/default/slapd. Per evitare qualsiasi rischio, occorre disattivare del tutto l'unsecured LDAP.

Esempio 11.28 Il file /etc/default/slapd

```
# Default location of the slapd.conf file or slapd.d cn=config directory. If
# empty, use the compiled-in default (/etc/ldap/slapd.d with a fallback to
# /etc/ldap/slapd.conf).
SLAPD_CONF=

# System account to run the slapd server under. If empty the server
# will run as root.
SLAPD_USER="openldap"

# System group to run the slapd server under. If empty the server will
# run in the primary group of its user.
```

```

SLAPD_GROUP="openldap"

# Path to the pid file of the slapd server. If not set the init.d script
# will try to figure it out from $SLAPD_CONF (/etc/ldap/slapd.conf by
# default)
SLAPD_PIDFILE=

# slapd normally serves ldap only on all TCP-ports 389. slapd can also
# service requests on TCP-port 636 (ldaps) and requests via unix
# sockets.
# Example usage:
# SLAPD_SERVICES="ldap://127.0.0.1:389/ ldaps:/// ldap:///"
SLAPD_SERVICES="ldaps:/// ldap:///"

# If SLAPD_NO_START is set, the init script will not start or restart
# slapd (but stop will still work). Uncomment this if you are
# starting slapd via some other means or if you don't want slapd normally
# started at boot.
#SLAPD_NO_START=1

# If SLAPD_SENTINEL_FILE is set to path to a file and that file exists,
# the init script will not start or restart slapd (but stop will still
# work). Use this for temporarily disabling startup of slapd (when doing
# maintenance, for example, or through a configuration management system)
# when you don't want to edit a configuration file.
SLAPD_SENTINEL_FILE=/etc/ldap/noslapd

# For Kerberos authentication (via SASL), slapd by default uses the system
# keytab file (/etc/krb5.keytab). To use a different keytab file,
# uncomment this line and change the path.
#export KRB5_KTNAME=/etc/krb5.keytab

# Additional options to pass to slapd
SLAPD_OPTIONS=""

```

11.7.3.2 Configurazione lato client Sul lato client, è necessario modificare la configurazione dei moduli libpam-ldap e libnss-ldap utilizzando un ldaps://URI. Anche i client LDAP devono essere messi in grado di autenticare il server. In un'infrastruttura a chiave pubblica che rispetta lo standard X.509, i certificati pubblici vengono firmati dalla chiave di una Certificate Authority (CA). Dunque gli amministratori della Falcot Corp per mezzo di easy-rsa hanno creato una Certificate Authority (CA) per poi configurare il sistema in modo che riconosca come sicura la CA della stessa Falcot Corp. Per ottenere ciò gli amministratori hanno caricato il certificato CA in /usr/local/share/ca-certificates ed eseguito update-ca-certificates.

```
# cp keys/ca.crt /usr/local/share/ca-certificates/falcot.crt
# update-ca-certificates
Updating certificates in /etc/ssl/certs... 1 added, 0 removed; done.
Running hooks in /etc/ca-certificates/update.d.....
Adding debian:falcot.pem
done.
done.
```

Infine, potrete modificare anche il default LDAP URI ed il default base DN in /etc/ldap/ldap.conf utilizzati da diversi tools da riga di comando. In questo modo non avrete la necessità di digitare tali parametri da riga di comando.

Esempio 11.29 Il file /etc/ldap/ldap.conf

```
#
# LDAP Defaults
#
# See ldap.conf(5) for details
# This file should be world readable but not world writable.

BASE    dc=falcot,dc=com
URI     ldaps://ldap.falcot.com

#SIZELIMIT      12
#TIMELIMIT      15
#DEREF          never

# TLS certificates (needed for GnuTLS)
TLS_CACERT /etc/ssl/certs/ca-certificates.crt
```

Questo capitolo descrive soltanto una minima parte dei softwares disponibili per servers; tuttavia la maggior parte dei servizi di rete più comuni sono stati trattati. Inoltre riteniamo sia giunto il momento di occuparci di argomenti più tecnici: ciò consentirà di approfondire nel dettaglio diversi concetti, attraverso la descrizione dei massive deployments e delle virtualizzazioni.

11.8. Real-Time Communication Service

I servizi Real-Time Communication (RTC) includono voce, video/webcam, messaggistica istantanea (instant messaging, IM) e desktop sharing. Questo capitolo introduce brevemente tre servizi necessari per mettere in piedi una RTC ovvero un server TURN, un server SIP ed un server XMPP. La Real-Time Communication Quick Start Guide include: sia spiegazioni chiare e dettagliate su come pianificare, installare e gestire questi servizi, sia esempi specifici per Debian.

♦ <http://rtcquickstart.org>

SIP e XMPP possono offrire le stesse funzionalità. SIP è leggermente più conosciuto per i servizi voce e video, mentre XMPP viene tradizionalmente utilizzato come protocollo di messaggistica istantanea (IM).

In realtà entrambi i servizi possono essere utilizzati per ciascuna delle summenzionate finalità. Per ottimizzare le opzioni di connettività, è consigliabile eseguirli tutti e due in parallelo. Inoltre i suddetti servizi utilizzano certificati X.509 sia per l'autenticazione, sia per ragioni di riservatezza. Per maggiori dettagli su come crearli andate a leggere il paragrafo 10.2.1.1, "Infrastruttura a chiave pubblica: easy-rsa" a pagina 224. In alternativa potrete trovare delle valide spiegazioni in Real-Time Communication Quick Start Guide:

♦ <http://rtcquickstart.org/guide/multi/tls.html>

11.8.1. Impostazioni DNS per i servizi RTC

I servizi RTC richiedono i records DNS SRV e NAPTR. A seguire un esempio di una configurazione che può essere inserita nel zone file per falcot.com:

```
; the server where everything will run
server1           IN      A      198.51.100.19
server1           IN      AAAA    2001:DB8:1000:2000::19

; IPv4 only for TURN for now, some clients are buggy with IPv6
turn-server IN A 198.51.100.19

; IPv4 and IPv6 addresses for SIP
sip-proxy        IN      A      198.51.100.19
sip-proxy        IN      AAAA    2001:DB8:1000:2000::19

; IPv4 and IPv6 addresses for XMPP
xmpp-gw         IN      A      198.51.100.19
xmpp-gw         IN      AAAA    2001:DB8:1000:2000::19

; DNS SRV and NAPTR for STUN / TURN
_stun._udp   IN SRV    0 1 3467 turn-server.falcot.com.
_turn._udp   IN SRV    0 1 3467 turn-server.falcot.com.
@           IN NAPTR  10 0 "s" "RELAY:turn.udp" "" _turn._udp.falcot.com.

; DNS SRV and NAPTR records for SIP
_sips._tcp   IN SRV    0 1 5061 sip-proxy.falcot.com.
@           IN NAPTR  10 0 "s" "SIPS+D2T" "" _sips._tcp.falcot.com.

; DNS SRV records for XMPP Server and Client modes:
_xmpp-client._tcp IN      SRV    5 0 5222 xmpp-gw.falcot.com.
_xmpp-server._tcp IN      SRV    5 0 5269 xmpp-gw.falcot.com.
```

11.8.2. TURN server

TURN è un servizio che supporta i clients sostenendo i NAT routers ed i firewalls, attraverso la ricerca del metodo più efficiente per comunicare con altri clients e ritrasmettendo i media streams nei casi in cui non viene trovato un direct media path [in sostanza un percorso dedicato e diretto per mezzo del quale due IP interni comunicano]. È consigliabile installare il server TURN prima di qualunque altro servizio RTC offerto agli utenti finali.

TURN e il correlato protocollo ICE sono open standards [non esiste una definizione univoca per "open standard". Sostanzialmente si tratta di un prodotto disponibile al pubblico a cui sono stati associati dei diritti di proprietà intellettuale attraverso una licenza d'uso che impone diritti e doveri alle parti interessate nel processo di realizzazione del prodotto ed ai terzi]. Per beneficiare a pieno dei suddetti protocolli, massimizzare la connettività e ridurre al minimo l'user frustration, il software dei clients deve essere compatibile. [L'user frustration o frustrazione dell'utente è un fenomeno che fa parte insieme alla "rabbia" del "computer rage" (la collera durante l'interazione con un computer), che può portare l'utente a fenomeni di violenza nei confronti di dispositivi informatici-elettronici, sino a giungere a veri e propri reati penali]. Affinché l'algoritmo ICE sia efficiente, il server deve disporre di due indirizzi IPv4 pubblici.

11.8.2.1 Installazione del TURN server

Dovrete prima installare il pacchetto `resiprocate-turn-server` e poi modificare il file di configurazione `/etc/reTurn/reTurnServer.config`. Immettete gli indirizzi IP del server.

```
# your IP addresses go here:  
TurnAddress = 198.51.100.19  
TurnV6Address = 2001:DB8:1000:2000::19  
AltStunAddress = 198.51.100.20  
# your domain goes here, it must match the value used  
# to hash your passwords if they are already hashed  
# using the HAl algorithm:  
AuthenticationRealm = myrealm  
  
UserDatabaseFile = /etc/reTurn/users.txt  
UserDatabaseHashedPasswords = true
```

Riavviate il servizio.

11.8.2.2 TURN gestione utenti

Per gestire l'elenco utenti del server TURN utilizzate l'utilità `htdigest`.

```
# htdigest /etc/reTurn/users.txt myrealm joe
```

Dopo aver apportato le modifiche al file `/etc/reTurn/users.txt`, dovete inviare il segnale `HUP` al server per ricaricare (“reload” in inglese) il summenzionato file o attivare la funzionalità di ricaricamento automatico in `/etc/reTurn/reTurnServer.config`.

[Il segnale `HUP` o `SIGHUP` (“signal hang up”) è un segnale che può avere diversi usi. Può essere inviato ad esempio ad un processo quando la sua gestione da terminale è conclusa oppure per riavviare un demone per far sì che quest’ultimo tenga in considerazione al riavvio della modifica di un file di configurazione.]

```
kill -HUP <processID>  
]
```

11.8.3. SIP Proxy Server [Session Initiation Protocol]

Un SIP proxy server gestisce le connessioni SIP in entrata e in uscita; SIP è un protocollo impiegato da organizzazioni, gestori di SIP trunking [servizi VoIP], SIP PBXes [Private Branch eXchange - basata sul protocollo SIP, è una rete telefonica privata (o centralino) che consente ai suoi utenti di comunicare internamente ed esternamente] tra cui Asterisk [software libero che consente di implementare una PBX], SIP phones (hardware), softphones (software basati sul protocollo SIP) ed applicazioni WebRTC [tecnologia basata su HTML5 e JavaScript che consente ai browsers di effettuare in tempo reale videochat].

Si consiglia vivamente di installare e configurare il SIP proxy prima della configurazione di un SIP PBX (private branch exchange). Il SIP proxy normalizza gran parte del traffico in arrivo al PBX e garantisce una migliore connettività e resilienza. [Normalizzazione è un termine tecnico prettamente matematico che viene impiegato anche nella statistica. Si tratta sostanzialmente e molto genericamente di un metodo che consente di tradurre dei dati semplificandoli per mezzo di una costante per ottenere una loro risoluzione o conversione in un altro formato. Nel caso di un database la normalizzazione è una riorganizzazione dei dati di un database affinché la ridondanza dei dati sia ridotta e gli stessi dati possano essere conservati in un'unica posizione. La resilienza invece è la capacità di mantenere un dato livello di servizio, qualificato come minimo o accettabile, nonostante il sopraggiungere di guasti o di altre esternalità.]

11.8.3.1 Installazione del SIP proxy

Dovrete prima installare il pacchetto `repro`. L'impiego del pacchetto `jessie-backports` è caldamente raccomandato perché vi consentirà di usufruire degli ultimi aggiornamenti che migliorano la connettività e la resilienza.

Poi modificate il file di configurazione `/etc/repro/repro.config` ed aggiungete gli indirizzi IP del server. L'esempio seguente mostra come configurare sia i servizi SIP, sia i servizi WebSocket/WebRTC utilizzando TLS, IPv4 e IPv6:

```

# Transport1 will be for SIP over TLS connections
# We use port 5061 here but if you have clients connecting from
# locations with firewalls you could change this to listen on port 443
Transport1Interface = 198.51.100.19:5061
Transport1Type = TLS
Transport1TlsDomain = falcot.com
Transport1TlsClientVerification = Optional
Transport1RecordRouteUri = sip:falcot.com;transport=TLS
Transport1TlsPrivateKey = /etc/ssl/private/falcot.com-key.pem
Transport1TlsCertificate = /etc/ssl/public/falcot.com.pem

# Transport2 is the IPv6 version of Transport1
Transport2Interface = 2001:DB8:1000:2000::19:5061
Transport2Type = TLS
Transport2TlsDomain = falcot.com
Transport2TlsClientVerification = Optional
Transport2RecordRouteUri = sip:falcot.com;transport=TLS
Transport2TlsPrivateKey = /etc/ssl/private/falcot.com-key.pem
Transport2TlsCertificate = /etc/ssl/public/falcot.com.pem

# Transport3 will be for SIP over WebSocket (WebRTC) connections
# We use port 8443 here but you could use 443 instead
Transport3Interface = 198.51.100.19:8443
Transport3Type = WSS
Transport3TlsDomain = falcot.com
# This would require the browser to send a certificate, but browsers
# don't currently appear to be able to, so leave it as None:
Transport3TlsClientVerification = None
Transport3RecordRouteUri = sip:falcot.com;transport=WSS
Transport3TlsPrivateKey = /etc/ssl/private/falcot.com-key.pem
Transport3TlsCertificate = /etc/ssl/public/falcot.com.pem

# Transport4 is the IPv6 version of Transport3
Transport4Interface = 2001:DB8:1000:2000::19:8443
Transport4Type = WSS
Transport4TlsDomain = falcot.com
Transport4TlsClientVerification = None
Transport4RecordRouteUri = sip:falcot.com;transport=WSS
Transport4TlsPrivateKey = /etc/ssl/private/falcot.com-key.pem
Transport4TlsCertificate = /etc/ssl/public/falcot.com.pem

# Transport5: this could be for TCP connections to an Asterisk server
# in your internal network. Don't allow port 5060 through the external
# firewall.
Transport5Interface = 198.51.100.19:5060
Transport5Type = TCP
Transport5RecordRouteUri = sip:198.51.100.19:5060;transport=TCP

```

```
HttpBindAddress = 198.51.100.19, 2001:DB8:1000:2000::19
HttpAdminUserFile = /etc/repro/users.txt

RecordRouteUri = sip:falcot.com;transport=tls
ForceRecordRouting = true
EnumSuffixes = e164.arpa, sip5060.net, e164.org
DisableOutbound = false
EnableFlowTokens = true
EnableCertificateAuthenticator = True
```

Per gestire la password dell'amministratore per l'interfaccia Web dovete impiegare l'utility `htdigest`. Il suo username dovrà essere `admin` ed il realm name dovrà corrispondere al valore definito in `repro.config`.

```
# htdigest /etc/repro/users.txt repro admin
```

Riavviate il servizio per utilizzare la nuova configurazione.

11.8.3.2 Come gestire il SIP proxy.

Attraverso l'interfaccia web recatevi su `http://sip-proxy.falcot.com:5080` per completare la configurazione inserendo i domini, i local users ed i static routes.

Innanzitutto dovete inserire il local domain. Il processo dovrà essere riavviato ogniqualvolta abbiate aggiunto o rimosso i domini dall'elenco.

Il proxy è in condizione di instradare le chiamate tra i local users ed i full SIP address, ma la routing configuration è necessaria se occorre l'override (trad. lett. "sostituzione") delle funzionalità predefinite; ad esempio, per l'identificazione dei numeri di telefono, per aggiungere un prefisso e per instradarli verso un SIP provider.

11.8.4. XMPP Server

Un XMPP server gestisce la connettività tra i local XMPP users e gli users XMPP di altri domini sulla rete pubblica (internet).

PROPRIETÀ DI LINGUAGGIO
XMPP o Jabber

A volte XMPP viene citato con il nome di Jabber. In realtà, Jabber è un marchio mentre XMPP è il nome ufficiale di un protocollo standard.

Prosody è un noto XMPP server ed è affidabile sui servers Debian.

11.8.4.1 Installazione del XMPP server.

Installate il pacchetto `prosody`. Il pacchetto `jessie-backport` include gli ultimi aggiornamenti in grado di ottimizzare la connettività e la resilienza, pertanto ne è raccomandata l'installazione. Dovrete inoltre revisionare il file di configurazione `/etc/prosody/prosody.cfg.lua`. Innanzitutto occorre inserire i JIDs degli utenti con titolarità dei diritti per la gestione del server.

```
admins = { "joe@falcot.com" }
```

Poi avrete bisogno di un file di configurazione per ciascun dominio. Come modello potrete utilizzare `/etc/prosody/conf.cfg.example.com.cfg.lua`. A seguire il file `falcot.com.cfg.lua` creato dagli amministratori del Falcot Corp:

```
VirtualHost "falcot.com"
    enabled = true
    ssl = {
        key = "/etc/ssl/private/falcot.com-key.pem";
        certificate = "/etc/ssl/public/falcot.com.pem";
    }
```

Per attivare il dominio, dovete creare un symlink in `/etc/prosody/conf.d/`:

```
# ln -s /etc/prosody/conf.avail/falcot.com.cfg.lua /etc/prosody/conf.d/
```

Riavviate il servizio per utilizzare la nuova configurazione.

11.8.4.2 Come gestire il server XMPP

Lo XMPP server può essere gestito attraverso l'utility da riga di comando `prosodyctl`. Ad esempio, per aggiungere l'account dell'amministratore specificato in `/etc/prosody/prosody.cfg.lua`:

```
# prosodyctl adduser joe@falcot.com
```

Troverete maggiori dettagli su come personalizzare la configurazione nella pagina web Prosody online documentation (<http://prosody.im/doc/configure>).

11.8.5. Come eseguire i servizi sul port 443

Alcuni amministratori preferiscono eseguire tutti i servizi RTC sul port 443. La ragione è consentire agli utenti di connettersi da postazioni remote, tra cui hotels ed aeroporti, in cui solitamente gli altri ports sono bloccati o il traffico Internet viene instradato tramite HTTP proxy servers.

Per poter mettere in pratica quanto appena espresso, ad ogni servizio (SIP, XMPP e TURN) deve essere assegnato un indirizzo IP diverso. Inoltre tutti i servizi possono comunque essere messi in esecuzione sullo stesso host in quanto Linux consente la gestione di indirizzi IP multipli su un singolo host. Il port number 443 deve essere specificato sia nei files di configurazione di ciascun processo, sia nei DNS SRV records.

11.8.6. Come aggiungere un servizio WebRTC.

La Falcot Corp desidera consentire alla clientela di poter effettuare le chiamate telefoniche direttamente dal sito web. Pertanto gli amministratori della Falcot Corp decidono di utilizzare anche WebRTC e di includerlo nel disaster recovery plan, in modo che il personale qualora dovesse verificarsi una emergenza possa, attraverso i web browsers, loggarsi da casa nel sistema telefonico della società e svolgere le proprie mansioni normalmente.

IN PRATICA

Scoprire WebRTC

Per iniziare a conoscere WebRTC, ci sono diversi siti che contengono dimostrazioni e test facilities.

♦ <http://www.sip5060.net/test-calls>.

WebRTC è una tecnologia in continua evoluzione, pertanto è fondamentale che utilizziate i pacchetti Jessie-Backport o delle distribuzioni Testing.

JSCommunicator è un software WebRTC phone non brandizzato, che non richiede server-side scripting come php. [Il server-side scripting è una tecnica di web development che, in alternativa ad una pagina web statica, supporta un'interfaccia personalizzata per ciascun utente]. Viene realizzato esclusivamente attraverso HTML, CSS e JavaScript. Molti altri servizi e moduli WebRTC di avanzati web publishing frameworks si basano su JSCommunicator. [Molto genericamente il web publishing framework è un software che può essere corretto, personalizzato o migliorato dagli stessi utenti tramite codice].

♦ <http://jscommunicator.org>

Attraverso il pacchetto jscommunicator-web-phone potrete installare rapidamente un WebRTC phone su un sito web. Serve soltanto un SIP proxy che includa il WebSocket transport [un protocollo SIP]. Il paragrafo 11.8.3.1, “Installazione del SIP proxy” a pag. 294 include tutte le informazioni necessarie per attivare su un repro SIP proxy il protocollo WebSocket transport. Una volta installato, jscommunicator-web-phone può essere utilizzato in diversi modi. Una delle strategie più semplici è includere o copiare la configurazione di /etc/jscommunicator-web-phone/apache.conf nella configurazione di un Apache virtual host.

Una volta disponibili i web-phone files sul web server, dovete personalizzare il file /etc/jscommunicator-web-phone/config.js in modo che punti al Turn server ed al SIP server. A seguire un esempio di quanto appena espresso:

```
JSCommSettings = {  
  
    // Web server environment  
    webserver: {  
        url_prefix: null          // If set, prefix used to construct sound/ URLs  
    },  
  
    // STUN/TURN media relays  
    stun_servers: [],  
    turn_servers: [  
        { server:"turn:turn-server.falcot.com?transport=udp", username:"joe", password:""  
         -> j0Ep455d" }  
    ],  
    // WebSocket connection  
    websocket: {  
        // Notice we use the falcot.com domain certificate and port 8443  
    }  
}
```

```
// This matches the Transport3 and Transport4 example in
// the falcot.com repro.config file
servers: 'wss://falcot.com:8443',
connection_recovery_min_interval: 2,
connection_recovery_max_interval: 30
},
...
...
```

Tipicamente i click-to-call web sites impiegano il server-side scripting per generare dinamicamente il file config.js. Il codice sorgente di DruCall (<http://drucall.org>) mostra come renderlo possibile con PHP.

Parole chiave

RAID
LVM
FAI
Preseeding
Monitoring
Virtualizzazione
Xen
LXC

