Postfix: il mailserver facile, veloce e sicuro

Un mailserver con le caratteristiche che molti desiderano, dalle prime fasi di installazione alla messa in servizio stupisce per la semplicità, le alte performance e le doti di sicurezza che offre.

Matteo Garofano
m.garofano@oltrelinux.com
Amministratore di sistema presso un Internet Service Provider, si occupa di networking e sicurezza. Utilizza volentieri Slackware, OpenBSD e Python.

La posta elettronica è storicamente uno dei più utili ed utilizzati servizi disponibili su Internet. Per questo motivo le esigenze degli amministratori di questo servizio si sono evolute verso sistemi di posta elettronica (**M**ail **T**ransfer **A**gent o **MTA**) veloci, sicuri e facili da configurare e amministrare. Tenendo conto di queste esigenze Wietse Venema, durante il suo anno sabbatico, nei laboratori della IBM scrisse VMailer. Prima del rilascio al pubblico sotto licenza IBM GPL, i legati della IBM scoprirono che il nome VMailer era "troppo simile" ad un prodotto coperto da trademark e cambiarono il nome in Postfix.

Attualmente Postfix è pubblicamente disponibile in rete sotto licenza IBM Public License Version 1.0.

L'autore è ancora attivamente impegnato nello sviluppo di Postfix ed è inoltre molto disponibile a rispondere alle moltissime domande che riceve su newsgroup e forum.

Nel sito si dichiara anche che il progetto Postfix sia il "naturale" avversario (e non nemico) del noto MTA Qmail scritto da D. J. Bernstein, sulle battaglie tra questi due autori si possono trovare interessanti articoli sulla rete.

Scopi del progetto

Gli scopi principali del progetto Postfix dichiarati dall'autore sono l'ampia diffusione, la compatibilità, le performance, la robustezza, la sicurezza e la flessibilità.

Wietse Venema desidera ottenere la massima diffusione del proprio software dichiarando di voler migliorare la sicurezza generale e l'efficienza dei sistemi di posta Internet.

Per raggiungere tale scopo, conta sulle buone caratteristiche del codice e sulla compatibilità.

La compatibilità di Postfix è in particolare rivolta nei confronti di Sendmail per il quale vuole essere il naturale sostituto. La migrazione da Sendmail a Postfix è pertanto piuttosto facile e non richiede grandi modifiche ai sistemi. Postfix infatti può gestire i messaggi con lo stesso formato usato da Sendmail e alcuni dei file di configurazione (ad es. `/etc/aliases`) ma si svincola completamente dal complicato file di configurazione `sendmail.cf` (chi ha avuto a che fare con questo file sa quanto sia "antipatico")

Dal punto di vista prestazionale, Postfix viene pubblicizzato dal proprio autore come "fino a tre volte più veloce del suo vicino avversario", inoltre, un altro slogan usato dall'autore è la capacità di Postfix di inviare e ricevere un milione di diversi messaggi al giorno utilizzando un desktop PC.

Slogan a parte, per ottenere prestazioni ottimali sono usate tecniche analoghe a quelle adottate nei web server per ridurre l'overhead nella creazione dei processi e nella gestione dei file.

La robustezza è un'altra delle caratteristiche di Postfix, infatti, sotto pesanti carichi, i programmi che lo compongono rallentano la loro attività mantenendo così il sistema stabile.

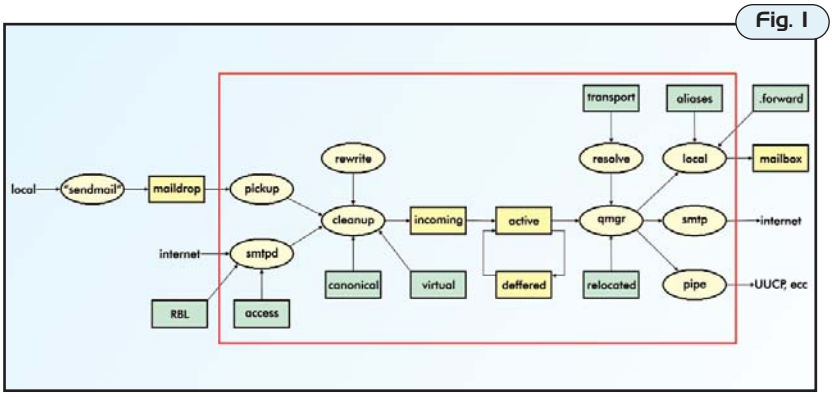
Postfix è costituito da numerosi programmi, ciascuno dei quali esegue un

compito. Con questo tipo di architettura il MTA risulta essere molto flessibile, infatti, i diversi programmi possono essere attivati, disattivati, sostituiti e modificati in base alle esigenze specifiche.

Architettura

Come già anticipato Postfix si compone di numerosi programmi che cooperano al fine di fare funzionare l'intero sistema. Lo schema che rappresenta il funzionamento è quello in *figura 1*.
Gli ellissi gialli sono i programmi, i rettangoli gialli sono le code di messaggi e i file contenenti i messaggi, i rettangoli blu sono le tabelle di lookup.
Il rettangolo grande racchiude i programmi gestiti dal demone principale (master, non rappresentato), e i dati gestiti da Postfix(*figura 1*). I programmi sono richiamati dal processo master che rimane sempre attivo.
La ricezione dei messaggi avviene ad opera di due differenti programmi in funzione della loro provenienza, dall'esterno o dall'interno.
Nel primo caso, l'apertura di nuove connessioni smtp sono gestite dal processo smtpd, mentre il demone pickup si occupa di accettare i messaggi locali, per entrambe l'input dei dati viene gestito dal processo cleanup(*figura 2*).
Postfix si avvale di quattro tipi di code per la gestione dei messaggi: **`maildrop`**, **`incoming`**, **`active`**, **`deferred`**. Maildrop è la coda della posta in arrivo, da questa, i messaggi dopo essere stati elaborati passano alla coda incoming.
Deferred è la coda dei messaggi che per qualche ragione non sono stati inviati. Il demone che gestisce le code tiene attiva una coda di messaggi di ridotte dimensioni, **active**, che serve a limitare l'eccessivo afflusso di messaggi dalle code incoming e deferred. In questo modo si evita di sovraccaricare il server in caso di pesanti flussi di posta. Il programma **`qmgr`**, il gestore delle code, gioca un ruolo chiave nel sistema, tale demone si occupa di mandare le richieste di invio di un messaggio, fornendo le informazioni necessarie, ai demoni **`local`**, **`smtp`** o **`pipe`** (*figura 3*).
Il demone local si occupa della consegna locale dei messaggi mentre smtp di quella remota. Attraverso pipe è possibile inviare i messaggi a comandi esterni, funzione estremamente potente che permette facilmente di aggiungere nuove funzionalità al mailserver. Altri demoni intervengono in altre attività come ad esempio **`trivial-rewrite`** il quale si occupa di risolvere l'indirizzo della destinazione, distinguendo tra remota e locale, e di riscrivere gli indirizzi in forma standard.
`Bounce` è invece un demone che, richiamato dal gestore delle code, si incarica di generare un messaggio di avvertimento nel caso un messaggio non possa essere inviato.
Il sistema si compone inoltre di un

Fig. 1



Schema 1

Schema 2

Fig. 2

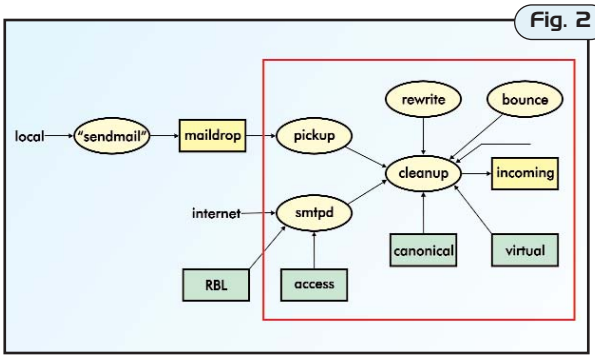
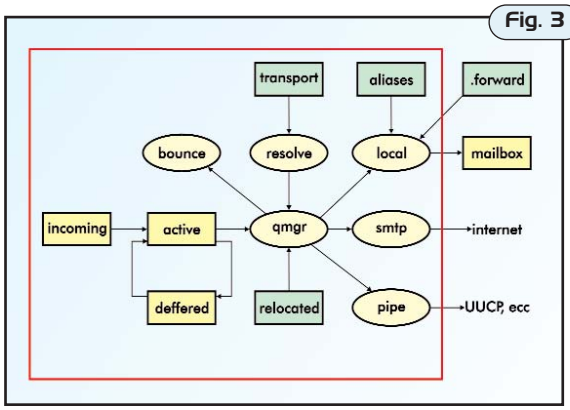


Fig. 3



Schema 3

certo numero di programmi di amministrazione piuttosto potenti ed intuitivi che impareremo ad usare subito dopo l'installazione.

Features

Pregi e difetti e confronti con altri famosi mailserver (in primis sendmail) Perché scegliere Postfix invece di utilizzare il noto e onnipresente Sendmail. Perché preferirlo ai validi Qmail o Exim o Courier? I motivi che possono spingere ad una nuova installazione di Postfix al posto di un altro mailserver sono da ricercare nelle caratteristiche del suo design.
Ovvero nuovamente l'alta sicurezza, la facilità di installazione e configurazione e le ottime performance.
Così se gli utenti alle prime armi riusciranno ad avere un mailserver funzionante con minimi sforzi, gli amministratori già esperti lo apprezzeranno per le performance, le doti di sicurezza e di flessibilità.
Qualcuno si potrebbe chiedere "ma dove risiede la maggiore sicurezza di Postfix nei confronti di altri Mail server? E come viene raggiunta?". Per rispondere brevemente a questa domanda, apriamo una parentesi inerente la caratteristiche con la quale Postfix raggiunge un buon livello di sicurezza.
Innanzitutto postfix nasce tenendo presente che i contenuti processati provengono da fonti potenzialmente non fidate. Questo approccio si differenzia rispetto a quello dei primi software di rete per Internet che nascevano attribuendo maggiore fiducia agli utenti stessi.
Un altro assunto dell'autore è di considerare il fatto che un software complesso come quello di un mailserver non può essere immune da errori e pertanto devono esistere diversi "strati" di protezione. I differenti strati implementati in Postfix possono essere descritti come segue.

- Bassi privilegi: i privilegi con cui girano tutti i processi tranne master non sono quelli di root.
- Gabbia chroot: tutti i programmi che compongono Postfix possono essere eseguiti in una "gabbia chroot" (chroot jail) ovvero in una porzione ristretta del filesystem. Sebbene questa modalità operativa non sia una garanzia assoluta di sicurezza si aggiunge in questo modo un barriera di difesa.
- Isolamento: le diverse attività eseguite da Postfix vengono svolte da diversi processi. Non esiste un modo per accedere dai programmi esposti alla rete a quelli che svolgono il recapito locale (ovvero nel filesystem). Un eventuale intruso deve pertanto violare più di un programma prima di aver accesso ai dati della macchina.
- Ambiente controllato: nessun programma di recapito locale può girare sotto il controllo di un processo gestito da un utente. Per evitare eventuali exploit che sfruttano file aperti, variabili ambiente e attributi dei processi entra in gioco il demone "master". Questo assolve la funzione di controllore degli altri processi e gira in un ambiente controllato e senza relazioni padre-figlio con processi utente.
- Set-uid: ad uno dei maggiori problemi di sicurezza che possono affliggere alcuni software è quello dovuto alla presenza di programmi che devono girare con il flag set-uid attivo, ovvero programmi girano con i privilegi dell'utente proprietario del file, indifferentemente dall'utente che li ha invocati. In questo modo chiunque può per alcune operazioni, ad esempio, diventare root. Postfix non utilizza programmi che girano con il bit setuid attivo.
- Fiducia: come già anticipato i programmi di Postfix non considerano affidabile nessun contenuto. In primo luogo non considera affidabili i dati provenienti dalla rete ma non considera affidabili nemmeno i dati presenti nelle code, ne quelli scambiati nei messaggi IPC (Interprocess Communication).
- Controlli sull'input: l'allocazione in memoria di stringhe e buffer è fatta dinamicamente, le linee lunghe nei messaggi vengono suddivise e ricostruite prima dell'invio, i messaggi di diagnostica vengono troncati prima di essere passati a syslogd.

Uno dei vantaggi maggiori che offre Postfix è offerto a coloro che attualmente utilizzano Sendmail come MTA. Anziché effettuare una nuova patch e ricompilazione, a seguito della scoperta di una falla di sicurezza, alcuni potranno decidere che sia il caso di cambiare definitivamente MTA. È estremamente semplice migrare un sistema di posta elettronica basato su Sendmail a Postfix poiché, come dice l'autore, "*the outside has a sendmail-ish flavor, but the inside is completely different*", ovvero Postfix dall'esterno si comporta come Sendmail ma internamente è completamente diverso.
Postfix supporta entrambe i formati **mailbox** e **maildir**, il primo tipico di Sendmai, il secondo di Qmail. Tanto per ricordare la differenza tra questi due sistemi, il sistema a mailbox utilizza un unico file per conservare tutti i messaggi di una mailbox, tutti file sono tipicamente conservati in `/var/spool/mail/` o `/var/mail/`.
Nella gestione formato maildir ciascun messaggio è memorizzato in un

file e ciascuna mailbox è costruita da una directory contenente i file, in genere la directory è collocata nella home dell'utente. Come già anticipato la flessibilità è una delle prerogative di Postfix e in tale ottica rientra la possibilità di scegliere tra i due sistemi di gestione.
Occorre però tenere presente che la scelta di uno dei due sistemi porrà dei vincoli su altre scelte. Per chiarire, ad esempio alcuni demoni che permettono l'accesso alla posta attraverso il servizio pop3, gestiscono solo il formato mailbox, viceversa tale formato e sconsigliabile se si sta accedendo a dati residenti su partizioni montate in NFS.
Quest'ultimo utilizza un sistema di locking che impedisce più accessi contemporanei, situazione che si può verificare se una mailbox viene letta mentre contemporaneamente sta ricevendo nuova posta. In caso ci fosse l'esigenza di usare partizioni montate in NFS il formato maildir è obbligatorio.
Tra le caratteristiche interessanti di questo mailserver c'è il supporto a molti formati per le tabelle usate nella gestione dei dati (lookups tables), come ad esempio alias, domini locali, reti e client autorizzati.
Sono inoltre presenti numerose possibilità di filtraggio dei messaggi sulla base del mittente, del destinatario, dell'intestazione dei messaggi e del loro contenuto. Per realizzare i filtraggi sono supportate le comode espressioni regolari e viene offerta la possibilità di intraprendere diverse azioni sui messaggi filtrati, dal rifiuto alla generazione di messaggi di avvertimento ai mittenti.
Tra le caratteristiche che risultano estremamente gradite dagli amministratori di mailserver è la possibilità di attivare il servizio di posta attraverso un canale crittografato.
Con Postfix questa implementazione risulta molto facile da attuare.
Tutte le configurazioni avvengono attraverso semplici file di testo e senza dover ricorrere a successive rielaborazioni come succedeva con Sendmail. Vantaggio non trascurabile, le opzioni da inserire o attivare hanno tutte dei nomi estremamente intuitivi e comprensibili.
Sebbene sia amato da moltissimi sistemisti, ovviamente, anche Postfix presenta degli svantaggi che è bene conoscere prima di decidere se utilizzarlo. Gli svantaggi più evidenti nei confronti di altri mailer sono la mancanza di strumenti dedicati ed integrati come ad esempio server pop3 e IMAP, un sistema per l'autorizzazione al relay degli utenti con IP dinamico (ad esempio dial-up) chiamato spesso pop-before-smtp, un programma "ufficiale" di accesso alla posta tramite web.
Così, per ottenere un sistema completo ed integrato di posta elettronica, è richiesto lo sforzo di dover integrare componenti esterne al MTA.
In *figura 4* viene proposta una tabella riassuntiva che tenta di mettere al confronto 5 tra i più diffusi e conosciuti MTA disponibili, sotto varie licenze, alla comunità. Lungi dall'essere una valutazione definitiva ed indiscutibile, vuole essere solo di supporto per coloro che si trovano a dover scegliere un MTA e non ne conosono le doti.

Installazione

Passiamo finalmente all'installazione di Postfix. Prenderemo in considerazione, in questa puntata, l'installazione di un mailserver aziendale con qualche centinaia di account, un solo dominio (oltrelinux.com) e l'accesso consentito ai soli appartenenti alla rete aziendale (192.168.100.0/24). Considereremo anche l'ipotesi di un server sul quale è installato e funzionante Sendmail e che, a seguito di una nuova falla di sicurezza, si è deciso di sostituire.
In questa serie di articoli prenderemo in considerazione come distribuzione di riferimento la Fedora Core 1, scelta dettata per soddisfare l'ampio bacino di utenza delle distribuzioni basate sul sistema di gestione dei pacchetti RPM. Nonostante ciò le indicazioni riportate, a meno di piccole variazioni, sono valide anche per le altre distribuzioni, quindi a voi la scelta.
È bene sapere inoltre che sono disponibili i pacchetti precompilati per le maggiori distribuzioni ed i port per i sistemi BSD degni di nota i pacchetti per Mac OS X, HP-UX e Solaris

Fig. 4

	COURIER-MTA	EXIM	POSTFIX	SENDMAIL	QMAIL
Sicurezza	Media-alta	bassa-media	alta	bassa	alta / molto alta
Difficolta installazione	media	media	facile - media	facile	media-difficile
Difficoltà configurazione	media	facile-media	facile	difficile	facile
Performance	medie	medie	alte	basse	alte
Maturità	bassa	bassa	media	alta	media
documentazione	Poca	molta	media-molta	Molta	Molta
Features	Molte	medie-molte	media	Molte	poche (disponibili patch)

aaaaaa

(sono disponibili sul sito i link che permettono di trovare i binari per Mandrake, RedHat per architettura Intel, Alpha e System 390, SuSE, Conectiva, Debian, Slackware, FreeBSD, OpenBSD, NetBSD port, Mac OS X ,HP-UX e Solaris).
Innanzitutto coloro che stanno utilizzando Sendmail e vogliono fare la migrazione devono fare il backup di tutti i file di configurazione copiandoli in una cartella dedicata allo scopo. Tra questi ad esempio i file contenuti in **/etc/** o **/etc/mail/** come aliases, access, mailertable, domaintable, localhost-names, virtusertable ed eventuali file di alias di majordomo.
Conviene poi copiare e conservare il binario sendmail (lo dovreste trovare lanciando da un terminale which sendmail), questa accortezza è particolarmente utile se lo avevate compilato con opzioni o patch particolari. In questo modo, nel caso qualcosa andasse storto potrete provvedere a ripristinare il sistema precedente senza grossi sforzi.
A questo punto non resta che procurarci Postfix. Possiamo decidere di installarlo utilizzando pacchetti già compilati per la nostra distribuzione oppure partendo dai sorgenti.
Nel primo caso l'installazione procederà senza la compilazione e senza dover operare alcune operazione inerente l'installazione con lo svantaggio però di non poter disporre di un binario "personalizzato". La soluzione è comunque soddisfacente per il nostro scopo.
A nostra scelta possiamo utilizzare i pacchetti precompilati di Postfix disponibili ormai in molte distribuzioni ma, vista la dimensione piuttosto modesta del pacchetto (1-3 Mb), consigliamo di scaricare l'ultima versione direttamente dalla rete.
Puntiamo il nostro browser sul sito **www.postfix.com**, leggiamo quello che ci interessa e dirigiamoci poi sull'area "Packages and ports" per ottenere i binari precompilati o il port oppure sull'area download e poi sul mirror preferito se preferiamo partire dai sorgenti.
Se avete optato per il pacchetto precompilato non vi resta che installarlo lanciando il comando appropriato

```
# rpm -ivh postfix-2.0.16.i386.rpm
                              (rpm based distro)
```

Se invece avete scelto di utilizzare i sorgenti possiamo procedere alla compilazione. Decomprimiamo e scompattiamo l'archivio dei sorgenti,

```
$ tar xvzf postfix-2.0.20.tar.gz
$ cd postfix-2.0.20/
```

Possiamo dare una occhiata al contenuto della cartella e, dopo aver letto il file **INSTALL** possiamo dare una occhiata alle cartelle **html/** e **README_FILES** che contengono documentazione e la cartella **config/** che contiene esempi di file di configurazione molto utili. Passiamo alla fase di compilazione che comincia con:

```
$ make
```

Creiamo un gruppo postfix ed un utente postfix che non siano utilizzati da nessun altro account. L'utente postfix dovrà appartenere al gruppo postfix e dovrà essere senza shell, senza home e senza possibilità di login. Aggiungiamo inoltre un gruppo postdrop che non sia usato da alcun account.

```
$ su
# make install
```

A questo punto, se non abbiamo ricevuto messaggi di errore ci verranno poste alcune domande. Se le nostre esigenze non sono particolari potremo accettare i valori proposti di default. Postfix è ora installato.
Passiamo ad una prima configurazione che ci permetterà di usare subito il nostro nuovo MTA.
Per avere un sistema di posta funzionante occorre indicare almeno un dominio per la posta in entrata uno per quella in uscita e quali client sono abilitati ad inviare posta.
Quasi tutte le opzioni di configurazione di Postfix si trovano nel file **main.cf** collocato in **/etc/postfix/** o nella cartella da voi indicata in fase di installazione. Apriamolo con il nostro editor preferito e dedichiamoci ai parametri più importanti.

myorigin = valore: è il dominio usato per la posta inviata dal server. Di default assume il valore **$myhostname** pertanto se tale nome non è un FQDN (fully qualified domain name) sarà opportuno modificarlo con il proprio dominio.
Es: **myorigin = oltrelinux.com**

mydestination = valore: sono i domini che il sistema di posta riconosce come locali e che pertanto non invia ad un altro server. Si tratta di una lista di nomi, si possono utilizzare anche file. I valori **$myhostname**, **localhost.$mydomain** sono quelli di default.
Es: **mydestination = $myhostname, localhost.$mydomain, $mydomain**

Postfix di default non permette l'invio di posta da parte di client e domini sconosciuti ovvero non è un open relay. Condizione necessaria per evitare che il proprio server venga utilizzato per l'invio del famigerato "spam". Per consentire l'invio da parte dei client presenti all'interno dell'azienda occorre abilitarli usando i seguenti parametri.

mynetworks = valore: questo parametro rappresenta gli indirizzi IP dei client che sono autorizzati a spedire messaggi. In alternativa si può utilizzare il parametro **mynetworks_style**
Es: **mynetwork = 192.168.100.0/24**

mynetworks_style = host/subnet/class

Fig. 5

La home page del progetto postfix.

host: l'invio sarà abilitato solo per la macchina locale.
class: saranno considerati validi tutti i client appartenenti al network di classe A, B o C a cui il server appartiene.
subnet: indica che Postfix accetterà di inviare la posta di tutti i client appartenenti alla stessa sottorete locale del mailserver, è il valore di default.
Es: `mynetworks_style = subnet`

`myhostname = valore`: Grazie a questo parametro è possibile impostare un valore che viene poi utilizzato nel file di configurazione attraverso la variabile `$myhostname`. Il valore di default usato da Postfix è il nome dell'host locale, se tale valore non è nella forma **FQDN** (**F**ully **Q**ualified **D**omain **N**ame) occorre specificare il nome di dominio completo per il server.
Es: `myhostname = mail.oltrelinux.com`

`mydomain = valore`: Attraverso questo parametro si imposta il dominio a cui appartiene il server. Di default viene usato il valore di `$myhostname` togliendo la prima parte del nome (mail.oltrelinux.com -> oltrelinux.com).
Es: `mydomain = oltrelinux.com`

Cerchiamo nel file la linea relativa agli alias e decommentiamola o scriviamola se non fosse presente; in particolare vorremo utilizzare per gli alias una mappa di tipo hash contenuta nella cartella `/etc/postfix/aliases`.

```
alias_maps = hash:/etc/postfix/aliases
```

Salviamo il file `main.cf` ed usciamo dall'editor. Modifichiamo ancora un file prima di essere pronti a dare il via al nostro nuovo mailserver.
Editiamo infatti il file `/etc/postfix/aliases` e andiamo a modificare la linea dove viene indicato l'alias di root. È necessario inserire un utente reale che riceva la posta.

```
# Person who should get root's mail.
# This alias must exist.
# CHANGE THIS LINE to an account
# of a HUMAN
root:          amministratore.oltrelinux
```

Una volta modificato questo file, per trasformarelo in un mappa utilizzabile da Postfix, dovremo lanciare il comando

```
# postalias /etc/postfix/aliases
```

Coloro che stanno effettuando la migrazione da Sendmail devono usare i file precedentemente salvati. Per esempio il contenuto del vecchio file aliases potrà essere accodato nel nuovo file in modo da ritrovare le vecchie configurazioni funzionanti.
Il tipo di formato usato da Postfix è di default il mailbox quindi gli utenti di Sendmail che utilizzavano la classica cartella `/var/spool/mail/` o `/var/mail/` non dovranno fare ulteriori modifiche.
È giunto il momento di fermare Sendmail prima di procedere alla sua sostituzione, per chi stesse effettuando la migrazione di una macchina in produzione. Possiamo utilizzare i nostri script oppure killare il processo Sendmail.

```
# /etc/rc.d/init.d/sendmail stop
```

Da questo momento, se non disponete di un mailserver secondario, potreste perdere i messaggi di posta in arrivo finché Postfix non sarà funzionante. Siamo ora pronti a dare il via al mailserver Basterà lanciare il comando

```
# postfix start
```

Se non verranno segnalati errori dovreste poter vedere nella lista dei processi alcuni demoni attivi pronti a smistare la posta. Nel caso si riscontrassero problemi potrete avviare il demone in modalità debug così da avere maggiori informazioni su quello che accade.

```
# postfix -D start
```

Dopo aver modificato la configurazione e sistemato il problema potrete far rileggere le configurazioni senza dover riavviare il servizio lanciando:

```
# postfix reload
```

Bene, ora abbiamo il nostro MTA "*live 'n kicking*", nel prossimo numero impareremo a gestire il nostro server ed a configurarlo in modo più complesso ed adatto alle nostre esigenze.

Riferimenti

Il sito ufficiale del progetto Postfix è ricco di documentazione, descrizioni e link a documentazione e programmi esterni.
http://www.postfix.com
Molta documentazione è reperibile in rete e rintracciabile con i motori di ricerca preferiti.
http://www.redhat.com/support/resources/howto/RH-postfix-HOWTO/book1.html

http://www.pluto.linux.it/journal/pj0201/postfix.html