ISTITUTO NAZIONALE DI FISICA NUCLEARE

Sezione di Trieste

INFN/TC-02/02
27 Febbraio 2002

REALIZZAZIONE DI UN MAIL SERVER SU TRUCLUSTER CON SOFTWARE ASE

Roberto Gomezel, Claudio Strizzolo, Lucio Strizzolo, Alessandro Tirel

INFN, Sezione di Trieste

Sommario

Questo documento descrive la realizzazione di un mail server, effettuata su un sistema proprietario con processore Alpha in configurazione TruCluster.

La struttura, realizzata presso la Sezione di Trieste, utilizza il software ASE.

Published by ***SIS–Pubblicazioni***
Laboratori Nazionali di Frascati

INDICE

1 INTRODUZIONE

Il servizio di posta elettronica è ormai uno strumento di fondamentale importanza per il lavoro quotidiano. Di conseguenza, è crescente la richiesta di un sistema affidabile e sicuro, che consenta l'accesso a tale risorsa con la maggiore continuità possibile.

Presso la Sezione di Trieste dell'INFN, questa problematica è stata affrontata cercando una soluzione che consentisse di rendere il servizio di posta elettronica affidabile ed in grado di garantire buone prestazioni.

Sono state prese in esame varie possibilità, basate su diverse piattaforme hardware e su software sia di pubblico dominio che proprietario. Alla fine, la scelta è ricaduta su una soluzione interamente proprietaria, basata su server con processore Alpha e sistema operativo Tru64, in configurazione TruCluster. Questa soluzione, a fronte di un costo più elevato rispetto ad altre, garantisce per contro un livello di affidabilità superiore.

Questo documento descrive la soluzione scelta, e presenta alcune indicazioni per la sua realizzazione. Esso è rivolto al personale tecnico interessato alla messa in opera di una struttura analoga.

Questa guida non intende in alcun modo sostituirsi alla documentazione esistente per i vari prodotti citati in questo documento, che si consiglia di consultare per avere maggiori informazioni sui prodotti stessi.

2 REQUISITI

I requisiti prefissati per la struttura di gestione della posta elettronica presso la Sezione di Trieste sono i seguenti:

- Compiti del sistema
  Il sistema di posta elettronica deve essere in grado di svolgere diverse funzioni:
  a) Mail relay, ovvero distribuzione della posta in ingresso agli utenti della Sezione, e invio all'esterno della posta spedita dalla Sezione.
  b) Mailbox repository, ossia "deposito" delle mailbox di tutti gli utenti della Sezione, o almeno di coloro che non hanno necessità di ricevere la posta su nodi diversi: si tratta della stragrande maggioranza. L'accesso alle mailbox da parte degli utenti deve avvenire esclusivamente tramite i protocolli IMAP e POP3, e non "direttamente" sulla macchina.
  c) Gestione di problematiche particolari, come mailing list, archiviazione di mail, ecc.

- Carico di lavoro
  Attualmente il database del mail relay include circa 350 destinatari. Il sistema va pensato in vista di un potenziale aumento, anche considerevole, del numero di utenti.

- Fault tolerance

Il sistema deve essere per quanto possibile in grado di funzionare anche in caso di guasto di qualche suo componente, nei limiti di un ragionevole margine di rischio e di un valido rapporto costo/rischio. Di conseguenza devono essere studiate soluzioni di fault tolerance, ad esempio con componenti ridondate.

- Sicurezza
  Il sistema deve essere il più possibile "sicuro". Deve consentire l'accesso agli utenti solo per i limitati compiti di cui possono avere bisogno sul mail server, e possibilmente solo tramite protocolli "sicuri", come SSH e SSL. Per quanto concerne il mail relaying, il sistema deve essere dotato dei filtri consigliati dal gruppo Mailing dell'INFN contro il mail spamming.

3 DESCRIZIONE DELLA STRUTTURA

3.1 Hardware

La struttura realizzata è basata su due Compaq Alphaserver DS10 "gemelli", equipaggiati entrambi con:

- disco interno da 18 GB
- 2 schede FastEthernet

A tali sistemi si è affiancato un disk array Compaq BA356 che ospita, allo stato attuale, quattro dischi da 36GB, ma con possibilità di essere espanso.

Il disk array è fornito di doppio alimentatore e doppio canale SCSI.

Le due macchine sono collegate tra loro per mezzo di una delle due schede FastEthernet. La seconda scheda serve ovviamente alla connessione dei server alla LAN.

Il disk array è collegato ad entrambi i sistemi per mezzo del doppio canale SCSI (ved. fig. 1).

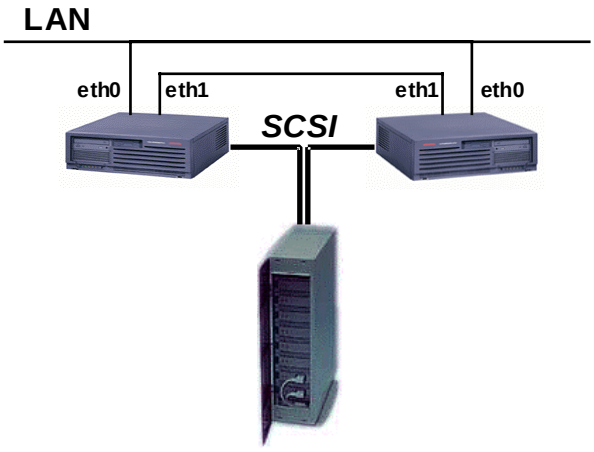

FIG. 1: Struttura hardware.

Sui dischi interni delle due macchine risiedono il sistema operativo, e gli altri software che

si desidera siano installati specificatamente su entrambi i nodi, senza condivisione. Nel disk array esterno, invece, verranno installati i software e i dati (ad es. le mailbox degli utenti) che si desidera siano visibili da entrambi i sistemi.

I dischi nel disk array vengono gestiti in RAID software, in modalità di mirror. Il RAID software elimina un potenziale punto di failure rispetto al RAID hardware, a scapito di un degrado delle prestazioni. Tale degrado non è peraltro critico, visto che si tratta di macchine con notevoli potenzialità, e che il carico di lavoro stimato è di gran lunga sopportabile. Per la gestione del mirroring verrà utilizzato il software LSM (Logical Storage Manager) incluso nel sistema operativo Tru64.

Esiste naturalmente la possibilità di mirrorare anche i dischi interni delle due macchine, utilizzando un secondo disco per ogni macchina.

3.2 Software

Il sistema operativo installato sui due sistemi è Tru64 Unix v.4.0g. Le due macchine sono gestite in configurazione TruCluster v. 1.5, in modo da poter sfruttare le potenzialità del TruCluster Available Server Environment (ASE). Questo ambiente permette la definizione di servizi ad alta affidabilità, con la possibilità di migrare un servizio da un nodo all'altro del cluster qualora qualche nodo diventi indisponibile, per qualsiasi motivo. I dischi installati nel disk array esterno sono visti contemporaneamente da entrambi i server che compongono il cluster, e la loro accessibilità non dipende in alcun modo da una macchina o dall'altra.

Il servizio di posta viene definito come un servizio di ASE, e sarà in grado di funzionare su una qualsiasi delle due macchine in modo trasparente per l'utente, in quanto le macchine sono indipendenti per quello che concerne il sistema operativo, ma condividono la stessa area dati e il medesimo database di ASE. Per maggiori informazioni su ASE consultare la relativa documentazione[1)].

Su questa base sono stati installati vari pacchetti, necessari alla messa in opera del sistema. Tra essi:

- Perl
- ssh
- Berkeley DB
- sendmail
- Majordomo (per la gestione delle mailing list)
- procmail (per l'elaborazione di mail in transito)
- mhonarc (per l'archiviazione di mail in pagine HTML)
- OpenSSL
- IMAP
- AFS

3.3 Sicurezza

L'accesso alle macchine è limitato ai soli protocolli necessari, e, possibilmente, solo in modalità "crittata" (SSH, SSL, ...). Sono stati disabilitati tutti i servizi non strettamente indispensabili.

L'accesso degli utenti al sistema è consentito solo tramite SSH, e per mezzo di "captive account". In questo modo vengono drasticamente limitati i compiti che gli utenti sono in grado di svolgere direttamente sulle macchine, restringendoli a quelli necessari alla sola gestione della propria mailbox (cambio della password, definizione di un "forward", ecc.)

4 REALIZZAZIONE

4.1 Preliminare

Nei paragrafi seguenti si cita come esempio la struttura realizzata presso la Sezione di Trieste. I due nodi che compongono il cluster sono stati denominati "castor" e "pollux". Il servizio di mailing viene gestito da un servizio LSM ASE denominato "mailsrv", che gira preferibilmente su castor. Solo nel caso in cui tale nodo diventi indisponibile, il servizio viene riallocato su pollux.

Nel caso in cui i due sistemi siano entrambi attivi, il nodo pollux può svolgere altri compiti che, per vari motivi, è preferibile siano separati dalla posta: web server, local news server, ecc. Tali compiti possono essere gestiti a loro volta tramite servizi ASE, e quindi migrare su castor qualora sia pollux a diventare indisponibile. In quest'ultimo caso bisogna tenere presenti, però, gli eventuali rischi per la security, provocati dalla coesistenza dei diversi servizi sulla stessa macchina.

4.2 Installazione del sistema operativo

La prima operazione è stata, ovviamente, l'installazione del sistema operativo (Compaq Tru64 4.0g) sulle due macchine. Sono stati installati tutti i pacchetti software disponibili sul CD di installazione, e la versione più recente delle patch.

L'installazione dei sistemi operativi è stata eseguita separatamente sui dischi interni delle due macchine.

Le partizioni di /, /usr e /var sono state inizializzate tutte come AdvFS.

4.3 Configurazione delle interfacce di rete

Su entrambi i sistemi, l'interfaccia di rete che è connessa alla LAN va configurata con un indirizzo "visibile". L'interfaccia che connette direttamente i due host può essere invece configurata con un indirizzo "nascosto", ad esempio:

```
10.0.0.2 pollux1
10.0.0.1 castor1
```

4.4 Creazione del disk group rootdg di LSM

Il software LSM (Logical Storage Manager) consente la gestione di dischi con funzionalità avanzate, tra le quali le modalità di "striping" e "mirroring" tipiche dei sistemi RAID.

Nella nostra struttura, LSM viene impiegato principalmente per gestire i dischi del box esterno in modalità mirror.

Si consiglia la consultazione del manuale di System Administration del sistema operativo[2)] per maggiori informazioni su LSM.

Per poter utilizzare LSM su dischi e volumi per i servizi di ASE, ogni macchina che compone il cluster ASE deve avere un disk group rootdg di LSM definito su un disco locale interno, non condiviso.

LSM permette di incapsulare le partizioni di root e swap in volumi LSM. È possibile trasformare le singole partizioni oppure l'intero disco di boot; nel primo caso deve essere già inizializzato un "disk group" rootdg, nel secondo no. In entrambi i casi sul disco di boot devono esistere almeno due partizioni libere.

Il processo di incapsulamento di root e swap riduce la swap della dimensione della "private region" LSM, che per default consiste di 1024 settori.

Per convertire tutte le partizioni del disco di boot (supponiamo rz16) in volumi LSM è necessario utilizzare il comando:

```
# /usr/sbin/volencap rz16
```

Quindi effettuare un reboot della macchina durante il quale vengono eseguiti tutti gli script creati con il comando volencap. In questo modo viene creato un volume per ogni partizione del disco di boot in uso; la partizione di root diventa "rootvol", la partizione di swap "swapvol", le altre partizioni mantengono nomi generici (vol-rz16d, vol-rz16e, vol-rz16f, …).

La creazione del disk group rootdg deve essere eseguita separatamente su entrambi i nodi.

Prima di eseguire il reboot della macchina è possibile utilizzare il comando

```
# /usr/sbin/volencap -s
```

per visualizzare tutti i processi di encapsulation in coda. Se necessario è possibile rimuovere tutti i processi di encapsulation in coda e tutti gli script di conversione con il comando

```
# /usr/sbin/volencap -k -a
```

4.5 Installazione di ASE

Il software ASE viene installato con un normale setld del kit, su entrambe le macchine. Per l'installazione fare riferimento al manuale relativo[3)].

Nel corso dell'installazione vengono visualizzate alcune domande. Alcuni spunti per rispondere a tali quesiti:

- L'ASE_ID number deve essere lo stesso sui due sistemi (ad es. "1").
- Alla domanda "Do you want to run the ASE logger on this node?" rispondere "Yes".
- Al punto "Select the controllers that define the shared ASE I/O buses" selezionare il controller cui è connesso il disk array esterno.

4.6 Definizione dei volumi per i servizi di ASE

Le seguenti operazioni hanno lo scopo di creare un disk group di LSM per il servizio di posta elettronica (mail-dg). Operazioni analoghe possono essere ripetute per creare eventuali altri disk group per ulteriori servizi da realizzare sui dischi condivisi.

Si suppone di voler definire un disk group in modo da realizzare il mirror di un disco (rz80 <-> rz81):

```
# disklabel -wr rz80 auto
# disklabel -wr rz81 auto
```

crea la disklabel di default sui dischi;

```
# voldisksetup -i rz80 nconfig=1 privlen=1024
# voldisksetup -i rz81 nconfig=1 privlen=1024
```

configura i dischi per l'utilizzo con LSM;

```
# voldg init mail-dg disk80=rz80
```

crea il gruppo mail-dg;

```
# voldisk list rz80
```

visualizza la configurazione LSM del disco, il comando successivo utilizza il valore del parametro "len" della voce "public" (es: 71130960);

```
# volassist -g mail-dg make mailvol 71130960 disk80
```

crea il volume mailvol;

```
# voldg -g mail-dg adddisk disk81=rz81
```

aggiunge il disco rz81 al disk group mail-dg;

```
# volassist -g mail-dg mirror mailvol disk81
```

crea il mirror del disco di mailvol (disk80) su disk81.

A questo punto è possibile definire un volume AdvFS (mail_dom#mailvol) mappato sul volume LSM:

```
# mkfdmn -x 512 -p 14400 /dev/vol/mail-dg/mailvol mail_dom
```

```
# mkfset mail_dom mail
```

4.7 Modifica dei file /etc/hosts

Su entrambi i nodi, è importante che /etc/hosts includa un set minimo di indirizzi. Ad esempio, su castor:

```
127.0.0.1 localhost
140.105.6.112 castor.ts.infn.it castor CASTOR
140.105.6.113 pollux.ts.infn.it pollux POLLUX
140.105.6.101 quark.ts.infn.it quark # BIND server
##### Servizi ASE ####
140.105.6.110 mailsrv mailsrv.ts.infn.it
### Collegamento diretto castor-pollux
10.0.0.2 pollux1
10.0.0.1 castor1
```

4.8 Creazione del servizio mailsrv in ASE

La gestione dei servizi di ASE viene effettuata tramite l'utility asemgr. Si rimanda alla documentazione[1)] per tutto ciò che concerne l'utilizzo di tale programma.

Ci sembra invece importante far notare che esistono diverse tipologie di servizi ASE (UFS, AdvFS, LSM, NFS, ...), e che esistono differenti possibilità per definire il servizio per la posta elettronica.

La documentazione[1)] propone un esempio completo di messa in opera di un servizio ridondato di posta elettronica basato su un servizio NFS di ASE. In quel caso, ASE "esporta" il disco condiviso tramite NFS a due mail server, che sono entrambi in grado di funzionare sulla stessa area dati. Entrambi i sistemi montano contemporaneamente il disco NFS.

Questa soluzione è sicuramente la più diretta nel caso in cui sia necessario definire sulle due macchine esclusivamente *un* servizio ASE. In questo modo, però, visto che una sola delle macchine svolge funzioni di mail server in un determinato istante, l'altra macchina resta completamente inattiva finchè non si verifichi un guasto della prima.

Analogamente, la stessa struttura basata su servizi NFS di ASE, funziona bene se i servizi da definire sono *due*, e si desidera che, in condizioni di operatività normali, essi vengano gestiti ognuno da una delle due macchine, tramite un'opportuna politica di riallocazione con bilanciamento di ASE (ASP).

Nel caso della Sezione di Trieste, però, tale struttura non rappresenta l'alternativa migliore, in quanto si desidera definire *più di due* servizi di ASE (almeno tre: mail server; web server; local news server), e si vuole che, in condizioni normali, il mail server giri *da solo* su una macchina, mentre gli altri servizi girano sulla seconda. In particolare, si desidera che non ci siano interazioni di alcun tipo tra le macchine, per quanto concerne il servizio di posta elettronica, e che non sia contemporaneamente accessibile ai due sistemi il file system dove sono conservati i dati relativi alla posta elettronica, principalmente per questioni di sicurezza.

Vista questa situazione, si è preferito definire il servizio di posta elettronica come servizio

LSM anzichè NFS.

Un'altra osservazione riguarda la policy di ASE (ASP), ovvero la politica per l'allocazione/riallocazione dei servizi di ASE sui server che compongono il cluster. Per i motivi sopra esposti, si è deciso di non attivare la policy con bilanciamento automatico, ma di assegnare una macchina come preferenziale per il servizio di posta (castor) e la seconda per gli altri servizi (pollux). In entrambi i casi è stato però definito come server secondario l'altro nodo, ossia pollux per la posta e castor per gli altri servizi, in modo che essi possano partire anche sull'altra macchina nel caso in cui il server "preferenziale" non sia disponibile. Nel caso si verifichi tale situazione, si ha ovviamente un potenziale maggior rischio per la security finchè tutti i servizi girano sulla stessa macchina. Questa situazione è però destinata a durare per il solo tempo, di solito breve, che intercorre fino alla risoluzione del problema o del guasto che ha causato l'indisponibilità di uno dei due server.

Per continuare con l'esempio, il file system LSM di ASE è stato definito, tramite asemgr, in modo da montare il volume automaticamente sotto il mount point /_mail, allo startup del servizio sulla macchina che fa da mail server.

4.9 Autenticazione ed area disco per gli utenti

A Trieste si è scelto di utilizzare NIS (Yellow Pages) per l'autenticazione degli utenti. Il daemon di NIS viene fatto partire solo sul server di posta elettronica, allo startup del servizio di posta, per mezzo delle script di start (in asemgr). Questo consente l'accesso agli utenti solo sulla macchina che fa da mail server, e non sull'altra, che svolge altri servizi ai quali gli utenti non sono autorizzati ad accedere direttamente.

Un'alternativa sarebbe stata quella di definire tutti gli utenti in /etc/passwd su entrambi i nodi, in modo che, in caso di guasto di un sistema, l'altro fosse in grado di gestire l'autenticazione e quindi l'accesso al servizio. È evidente però che questo modo di gestire il database comporta potenziali rischi di disallineamento, che non si pongono nel caso in cui il database degli utenti sia unico e gestito tramite NIS.

Il database del NIS deve risiedere sul disco condiviso. Per raggiungere questo traguardo ci sono almeno due soluzioni:

1. Creare un servizio NFS sotto ASE e montarlo sotto /var/yp.
2. Creare un link /var/yp che punti ad un'area del disco del servizio mailsrv, ad esempio /_mail/yp.

È stata scelta la seconda possibilità: il disco di servizio viene montato prima dello startup del servizio, quindi è già disponibile quando il servizio NIS viene fatto partire (ved. più avanti).

Lo spazio disco riservato agli utenti, che verrà utilizzato quasi esclusivamente per conservare le Inbox e gli altri folder di posta, deve risiedere sui dischi condivisi, ad esempio sotto /_mail/users. Di conseguenza quando verrà creato l'account per un nuovo utente (maggiori dettagli in seguito), esso andrà fatto puntare ad una home directory del tipo /_mail/users/*username*.

4.10 Installazione di software aggiuntivi

Sono numerosi i software di pubblico dominio che possono essere utilizzati per completare l'installazione. Alcuni di essi vanno installati preferibilmente sui dischi locali delle macchine, altri possono essere caricati sui dischi condivisi, senza dover ripetere due volte l'installazione. La scelta della directory di destinazione è, in molti casi, del tutto libera.

Nella struttura realizzata a Trieste sono stati installati i seguenti pacchetti, sul disco interno di entrambi i nodi, salvo dove specificato diversamente:

- Perl
- ssh
- Berkeley DB (seguire le istruzioni che si trovano sul sito www.sleepycat.com)
- sendmail (ved. capitolo 4.11)
- majordomo (sui dischi condivisi, ad es. sotto /_mail/majordomo)
- procmail
- mhonarc
- OpenSSL (serve per poter includere il supporto SSL nel server IMAP ed eventualmente in Pine. Si consiglia vivamente di installare SSL sotto /usr/local/ssl, perchè durante la compilazione di IMAP esso viene cercato in questo path)
- IMAP server, nella release della Washington University. (ved. capitolo 4.12)

4.11 Sendmail

La versione di sendmail installata è la 8.11.6. Chi è abituato a lavorare con la versione 8.9, tenga presente che la configurazione della versione 8.11 è leggermente diversa. Ad esempio, i file di configurazione si trovano in /etc/mail.

Il kit e le istruzioni si trovano sul sito www.sendmail.org. Si suggerisce di visionare anche la documentazione predisposta dal gruppo di lavoro dell'INFN sul Mailing, in particolare per quanto concerne la messa a punto dei filtri anti-spamming e la configurazione di un mail relay.

Si consiglia di installare le utility smrsh e mail.local incluse nel kit.

La configurazione di sendmail dovrà essere fatta in modo identico sulle due macchine.

Al fine di mantenere la continuità del servizio, è necessario che l'area di spool del sistema di posta e le Inbox degli utenti siano sui dischi condivisi anzichè sul disco locale della macchina che fa da mail server. Per default tali aree sono rispettivamente /var/spool/mqueue e /var/spool/mail.

Per modificare la definizione dell'area mqueue, è sufficiente ridefinire la QueueDirectory nel file sendmail.cf. Si consiglia di eseguire tale definizione tramite il file relay.mc, come per qualsiasi altro parametro che si desideri modificare, e di generare un nuovo file sendmail.cf tramite il tool m4. Ad esempio:

```
define('QUEUE_DIR','/_mail/spool/mqueue')
```

Per quanto concerne le Inbox, il problema è un pò più complesso: la gestione dello scaricamento dei mail verso le Inbox è a carico del programma di mail delivery locale, non di sendmail. Il tool incaricato di questo è normalmente mail.local, che però non prevede opzioni volte a dirigere l'output verso directory diverse da /var/spool/mail. Esiste ovviamente la possibilità di modificare il sorgente di mail.local in modo che lavori con un path alternativo, ma una

soluzione più "pulita" è quella di utilizzare un diverso programma per il delivery locale, ad esempio procmail. Procmail è uno strumento configurabile in maniera molto più completa di mail.local.

Una volta installato procmail, per definire tale programma come local mail delivery, si deve modificare il file relay.mc e rigenerare il sendmail.cf. La linea che esegue la definizione del local mailer è:

```
define('LOCAL_MAILER_PATH', '/bin/procmail')
```

Fatto questo, possiamo creare un file /etc/procmailrc come il seguente:

```
DEFAULT=$HOME/mbox
MAILDIR=$HOME/mail
```

Ciò significa che sia la Inbox ("DEFAULT") che la directory contenente gli altri folder di mail ("MAILDIR") saranno salvati a partire dalla home directory degli utenti, che è definita sui dischi condivisi nel database di autenticazione (ad es. /_mail/users/*username*). Avremo quindi una Inbox chiamata /_mail/users/*username*/mbox (anzichè /var/spool/mail/*username*), e gli altri folder sotto /_mail/users/*username*/mail.

4.12 Il server IMAP (e POP)

Il server imap installato è quello della Washington University. Le istruzioni ed il kit si trovano su www.washington.edu/imap. Il kit in questione consente anche l'installazione di un server POP.

Il file src/osdep/unix/env_unix.c deve essere modificato in modo da rispecchiare le variazioni effettuate rispetto allo standard di sendmail:

1. La mailbox (inbox) non è più /var/spool/mail/*username*, ma ~*username*/mbox. Di conseguenza la routine sysinbox va modificata in questo modo:

```
char *sysinbox ()
{
   char tmp[MAILTMPLEN];
   if (!sysInbox) { /* initialize if first time */
      /* sprintf (tmp,"%s/%s",MAILSPOOL,myusername ()); */
      sprintf (tmp,"%s/mbox",myhomedir ());
      sysInbox = cpystr (tmp); /* system inbox is from mail spool */
   }
   return sysInbox;
}
```

2. I folder (esclusa la inbox) devono essere cercati nella subdirectory "mail", anzichè nella home directory dell'utente. Modificare la linea in cui viene definita la variabile statica

mailsubdir in questo modo:

```
static char *mailsubdir = "mail"; /* mail subdirectory name */
```

Qualora si desideri il supporto SSL in IMAP, è necessario compilarlo in questo modo (per la piattaforma OSF/1):

```
# make osf SPECIALAUTHENTICATORS=ssl
```

Le librerie di SSL vengono ricercate sotto /usr/local/ssl, quindi è consigliabile che SSL sia stato installato sotto tale path.

Per poter abilitare SSL è necessario richiedere un certificato per il mail server alla Certification Authority dell'INFN. Il certificato va poi inserito in un file chiamato /usr/local/ssl/certs/imapd.pem. Se si desidera che anche POP possa usufruire di SSL, è possibile creare un link ipop3d.pem che punti a imapd.pem.

La richiesta di certificato in OpenSSL può essere generata da qualsiasi macchina dove sia installato OpenSSL, e sulla quale ci sia uno dei randomizzatori previsti da OpenSSL. Per maggiori informazioni, consultare la documentazione di quest'ultimo prodotto.

4.13 Startup di NIS e sendmail

Come detto in precedenza, i daemon di NIS e sendmail devono essere attivi solo sulla macchina che svolge funzioni di mail server, in un determinato istante. Di conseguenza si consiglia di togliere lo startup di tali daemon da /sbin/rc3.d e di includerlo invece, tramite asemgr, nella script di start del servizio mail, aggiungendo le seguenti linee:

```
# Start NIS
/sbin/init.d/nis start
# Start sendmail
/sbin/init.d/sendmail start
```

Nella script di stop andranno invece inclusi i comandi di stop degli stessi processi.

4.14 Disabilitazione dei servizi critici

Una volta che SSH sia stato installato, è consigliabile disabilitare tutti i servizi di inet che non siano strettamente necessari (telnet, ftp, rpc, ...), eliminandoli o commentandoli in /etc/inetd.conf.

5 ACCESSO DEGLI UTENTI AL SISTEMA

L'accesso degli utenti al sistema può essere ristretto alle sole funzionalità strettamente necessarie, e possibilmente solo tramite SSH.

Ciò può essere realizzato per mezzo di un "captive account". È sufficiente definire per ogni utente, al posto della shell, una script che consenta le sole operazioni desiderate, ad esempio:

- cambio della password;
- definizione/rimozione di un "forward" che permetta di girare la posta verso un altro indirizzo;
- definizione/rimozione di un messaggio di "vacation";
- controllo della propria disk quota.

Eventualmente si può pensare anche a task più complessi, come ad esempio la possibilità di definire dei filtri automatici sulla posta in ingresso tramite procmail, o simili.

La "captive script" deve essere progettata in modo molto accurato, per evitare problemi di security. In particolare è importante che l'utente non possa uscire dalla script ed eseguire comandi di sistema, o peggio ancora cambiare la propria shell di default. Fondamentale è anche verificare i dati che vengono immessi dall'utente, filtrando tutte le situazioni che potrebbero essere causa di problemi: caratteri critici per la script, sequenze di Escape, buffer overflow, ecc.

6 BIBLIOGRAFIA

(1) TruCluster Production Server Software Version 1.5 and TruCluster Available Server Software Version 1.5, Digital Equipment Corporation
(2) Digital Unix - System Administration, Digital Equipment Corporation
(3) TruCluster Software Products - Software Installation, Digital Equipment Corporation