ISTITUTO NAZIONALE DI FISICA NUCLEARE

Sezione di Trieste

INFN/ TC-07/01
26 Gennaio 2007

SERVIZIO DI POSTA ELETTRONICA AD ALTA AFFIDABILITÀ

Alessandro Tirel, Claudio Strizzolo
INFN, Sezione di Trieste, Padriciano 99, 34012 Trieste

Sommario

Questo documento descrive la realizzazione di un sistema cluster dedicato alla fornitura di servizi ad alta affidabilità. In particolare verrà analizzata un'applicazione relativa al servizio di posta elettronica, il quale rappresenta un elemento ad elevata criticità all'interno di ogni sede dell'INFN.

Tra le caratteristiche salienti della struttura descritta: l'utilizzo della tecnologia Fibre Channel; l'implementazione della Red Hat Cluster Suite; l'autenticazione tramite protocollo LDAP e l'attivazione di caselle di posta virtuali.

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

CONTENUTI

1 INTRODUZIONE

La disponibilità di soluzioni con un elevato livello di affidabilità per i servizi considerati critici è sempre più pressante all'interno dell'INFN. Un tipico esempio è quello della posta elettronica, servizio che deve essere garantito con continuità ed affidabilità. La realizzazione di soluzioni di questo tipo comporta un'accurata scelta di hardware e software, e non può prescindere dalla pianificazione di componenti strutturali quali ad esempio gruppi di continuità e rete.

Presso la Sezione di Trieste è stata realizzata una struttura centralizzata ad alta affidabilità dedicata principalmente al servizio di posta elettronica, ma che ospita anche altri servizi critici quali l'autenticazione degli utenti dei sistemi Linux e il servizio di Authentication Authorization Accounting (Radius).

La soluzione realizzata ha sostituito una precedente struttura di cluster dedicata al servizio di posta elettronica, attiva dal 2001. A causa dell'aumentato volume di posta e della richiesta di nuovi servizi, la vecchia struttura risultava ormai sottodimensionata e poco flessibile. Inoltre l'obsolescenza dell'hardware utilizzato aveva inevitabilmente provocato un aumento dei costi di manutenzione, al punto da rendere antieconomico il mantenimento della struttura, a fronte dell'acquisto di hardware più recente, peraltro in grado di offrire prestazioni migliori.

La nuova struttura ha consentito di soddisfare le richieste di nuove funzionalità da parte degli utenti del servizio di posta elettronica, tra le quali: massima facilità di accesso alla propria posta ovunque ci si trovi; affidabilità del servizio; sicurezza dei dati; possibilità di gestire con semplicità anche allegati di grosse dimensioni; sistemi di filtraggio della posta non desiderata (*spam*) e dei virus propagati via mail.

Questo documento descrive le caratteristiche principali della soluzione ad alta affidabilità realizzata, con particolare riferimento al servizio di posta elettronica.

2 LA SITUAZIONE ESISTENTE

2.1 Hardware

Prima dell'intervento descritto in questo documento, il servizio di posta elettronica era ospitato dalla soluzione hardware/software installata nell'anno 2001 descritta nel documento "Realizzazione di un Mail Server su Trucluster con software ASE" [1].

Al fine di fare fronte ad eventuali malfunzionamenti dell'hardware, l'architettura prevedeva una ridondanza ottenuta utilizzando due server con architettura Alpha e sistema operativo Unix Tru64 4.0g, in configurazione Trucluster. La medesima struttura ospitava anche il servizio web della Sezione.

I due server condividevano uno spazio disco di 36GB+36GB in modalità RAID 1 (mirror) dedicato al servizio mail, su un RAID array SCSI (vedi figura 1).

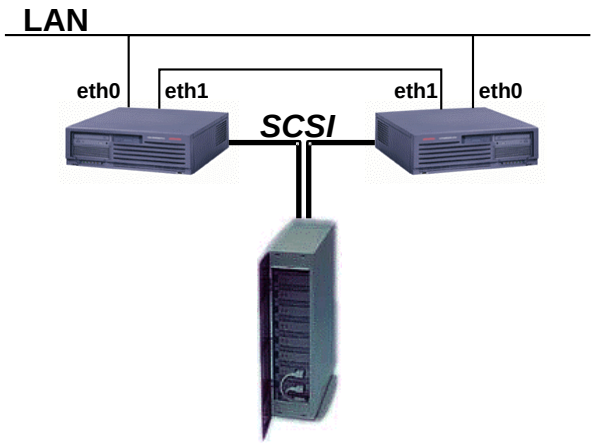

FIG. 1: struttura del cluster usato per i servizi di posta elettronica e web prima della ristrutturazione.

2.2 Autenticazione e funzionalità offerte agli utenti

L'autenticazione degli utenti per l'accesso al servizio di posta elettronica era realizzata per mezzo di una base dati NIS. Quest'ultima era installata sugli stessi server che ospitavano il servizio di posta, in modo da evitare interazioni con altri sistemi e limitare pertanto la probabilità di malfunzionamenti. Ad ogni utente era assegnato un *captive account* tramite il quale era possibile eseguire solo un limitato sottoinsieme di operazioni per la gestione della propria casella di posta: cambio della password, definizione di un forward verso un indirizzo diverso, attivazione/disattivazione di una risposta automatica (*vacation*) e del filtro antispam.

2.3 I principali software utilizzati

- Sistema operativo: Unix Tru64.
- Clustering: Trucluster.
- MTA: sendmail (con Berkeley DB).
- Antispam: Spamassassin.
- Server IMAP/POP: UW-IMAP (University of Washington).
- Web mail: Horde + IMP.
- Autenticazione degli utenti: tramite NIS (Yellow Pages).
- Gestione del proprio account da parte degli utenti: tramite *captive account* con procedure realizzate “in casa”.
- Gestione degli account da parte dell'amministratore: tramite procedure da linea di comando.
- Mailing list: Majordomo + Mhonarc per l'archiviazione su web.

2.4 I limiti della struttura

- Alto costo della manutenzione, dovuto essenzialmente all'obsolescenza dell'hardware.
- Prestazioni non all'altezza delle esigenze. Nonostante il sistema fosse stato sovradimensionato al momento dell'installazione, l'aumento esponenziale del numero e della dimensione dei messaggi di posta elettronica in transito era la causa di un evidente degrado delle prestazioni in alcune situazioni critiche, ad esempio nella gestione di grossi afflussi simultanei di posta elettronica come conseguenza di spam particolarmente massicci, o in seguito a problemi di rete.
- Difficoltà nell'aggiornamento del software, a causa della struttura piuttosto rigida e basata su un sistema operativo per il quale non sono di solito immediatamente disponibili tutti i software più recenti, a differenza di quanto avviene ad esempio su Linux.
- Difficoltà nell'attivazione di nuovi servizi, anche come conseguenza del punto precedente. In particolare era sentita la mancanza dei seguenti strumenti:

    1. un sistema antivirus centralizzato sul mail server;
    2. la possibilità di relay per utenti itineranti, tramite qualche sistema di autenticazione (SASL/TLS).

3 LA STRUTTURA REALIZZATA

3.1 Panoramica

La nuova struttura ad alta affidabilità è costituita da un cluster a due nodi con storage basato su una infrastruttura in Fibre Channel. Il sistema operativo scelto è Scientific Linux. Come conseguenza è stato individuato in Red Hat Cluster Manager il software più idoneo alla realizzazione della struttura di clustering.

3.2 Red Hat Cluster Manager[1]

Il compito del Red Hat Cluster Manager è quello di connettere dei sistemi separati, chiamati membri o nodi, per formare una nuova entità chiamata cluster, che garantisce l'integrità dei dati e la disponibilità delle applicazioni nel caso in cui si verifichino dei guasti. Questo permette di rendere altamente affidabili servizi come database, web, posta elettronica, condivisione di file, e altri.

Per costruire un cluster bisogna connettere i sistemi membri all'hardware del cluster e configurarli nel nuovo ambiente operativo. Il funzionamento del cluster si basa su un avanzato algoritmo di membership, che mediante meccanismi d'inter-comunicazione tra i membri

[1]Il contenuto di questo capitolo è tratto ed adattato dal manuale "Red Hat Cluster Suite: Configuring and Managing a Cluster" [3]

mantiene l'integrità dei dati. Questi sistemi di comunicazione sono rappresentati dalle connessioni di rete (*heartbeat*) e dalla condivisione di uno spazio storage comune in cui è mantenuto aggiornato lo stato del cluster.

Per rendere un'applicazione ed il suo insieme di dati altamente disponibili bisogna definire un servizio, ossia un insieme di proprietà e risorse a cui assegnare un indirizzo IP tale da permettere un accesso trasparente ai client.

Nell'ambito del cluster è possibile definire un dominio di failover, ossia un insieme di membri del cluster abilitati ad eseguire uno specifico servizio secondo una certa priorità. Per ovvie ragioni d'integrità dei dati non è possibile eseguire lo stesso servizio su più di un membro nello stesso momento.

Consideriamo la struttura cluster più semplice, vale a dire quella formata da due membri. Possiamo configurare il cluster in due modalità: attivo-attivo oppure hot-standby. Nel primo caso entrambi i membri eseguono servizi indipendenti contemporaneamente; nel secondo, uno dei due membri esegue tutti i servizi, mentre l'altro rimane in una condizione d'attesa e si attiva solo in caso di problemi.

Nella figura 2 è riportata schematicamente una tipica configurazione attivo-attivo.

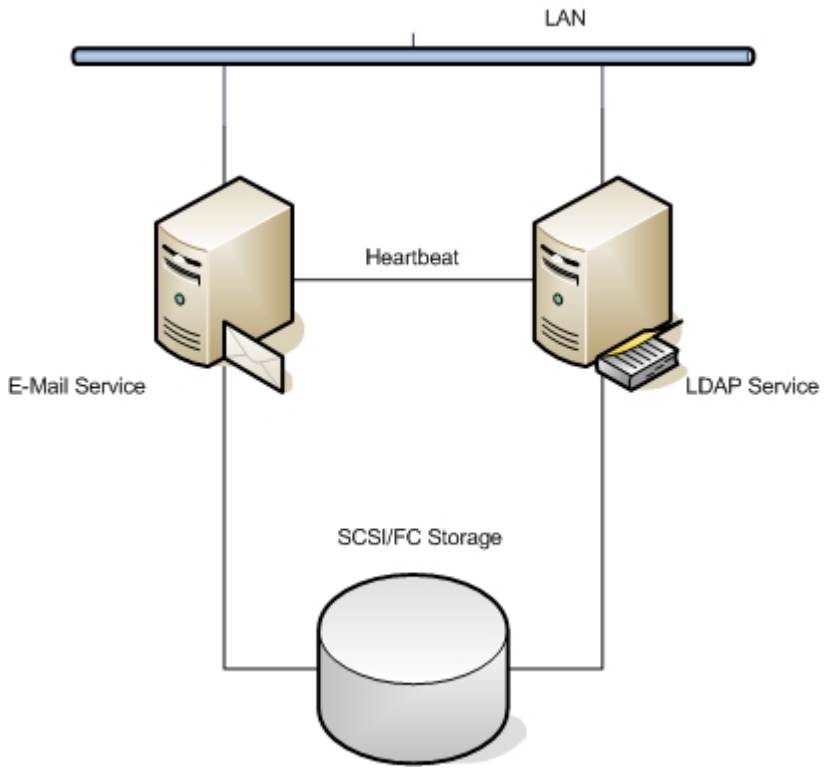

FIG. 2: esempio di struttura attivo-attivo.

Nel caso di problemi di natura hardware o software i meccanismi del cluster eseguono i

servizi compromessi sul membro funzionante. Tale operazione assicura l'integrità dei dati e comporta per i client afferenti ai servizi in questione solo un breve disservizio. Una volta che i problemi saranno stati superati, i servizi verranno ridistribuiti tra i membri secondo le indicazioni presenti nei domini di failover.

Le operazioni di gestione dei servizi (avvio, arresto e rilocazione) possono essere effettuate con semplici comandi; in particolare la rilocazione permette di effettuare operazioni di manutenzione sui membri del cluster mantenendo la disponibilità dei servizi.

3.3 Implementazione Hardware

Per costruire il cluster sono stati utilizzati i seguenti componenti:

- Due server Supermicro 6013-P così configurati:
  - Processore Xeon 3.0 Ghz 512 KB cache FSB 133 Mhz
  - 2 GB di memoria DDR ECC Registered
  - 2 Dischi SCSI Seagate Ultra 320 da 36 GB 10K rpm
  - 1 DVD-ROM
  - 1 Floppy
  - 2 Porte Gigabit Ethernet
  - 1 Controller Fibre Channel Qlogic QLA2340
  - 1 Controller Gigabit Ethernet 3Com 3C2000-T
- Uno switch Fibre Channel Qlogic 5200 a 16 porte 1-2 Gb e 4 porte 10 Gb.
- Uno storage controller Fibre Channel Infortrend F16F-R2A2R con 16 dischi FC Seagate da 147 GB 10K rpm.
- Due Power Switch WTI RPS-10E.

Per portare a termine l'installazione del sistema è stato necessario eseguire una sequenza ben definita.

Per prima cosa sono stati collegati i vari elementi del sistema secondo lo schema riportato in figura 3, ad eccezione del collegamento Fibre Channel ai dischi.

Tramite le funzionalità del controller RAID SCSI interno ad ogni server è stato definito il mirroring tra i due dischi interni per ottenere un livello maggiore d'affidabilità del disco sistema. A questo punto si è installato il sistema operativo. Poiché la configurazione deve essere pressoché identica sui nodi, è stato utilizzato come strumento d'installazione kickstart.

Il disco sistema è stato partizionato con /, /boot, /tmp, /var e swap, poiché la totalità dei dati è ospitata sui dischi Fibre Channel.

Terminata l'installazione del sistema operativo è stato necessario installare i driver della scheda gigabit ethernet 3Com, poiché essa non veniva riconosciuta automaticamente dal sistema operativo. I driver utilizzati sono in realtà quelli della scheda SK-NET di SysKonnect.

Risolto tale problema si è passati alla configurazione delle interfacce ethernet presenti; in particolare si è provveduto a creare un channel bonding tra l'interfaccia 3Com ed una tra quelle integrate sulla scheda madre, in modo da ottenere una connessione ridondata.

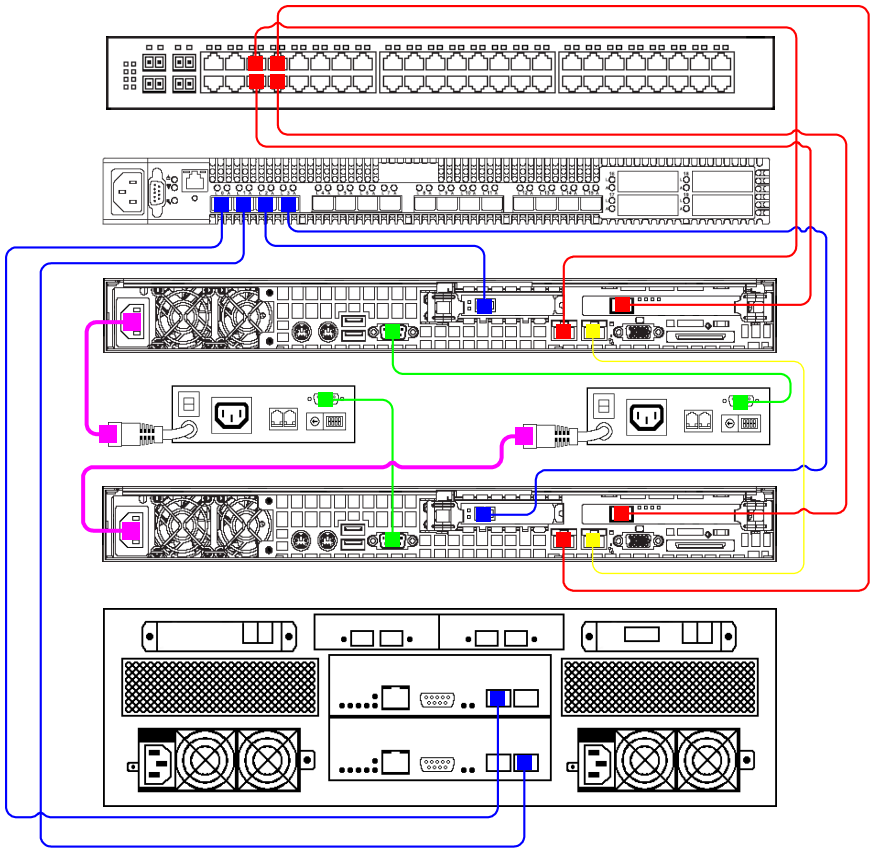

FIG. 3: schema di collegamento.

3.4 Il progetto generale del mail server

La soluzione software utilizzata per il mail server ricalca un progetto per un sistema di posta basato su LDAP, Postfix, Courier IMAP e Phamm citato in bibliografia [2]. Il progetto iniziale è stato leggermente modificato per venire incontro ad alcune esigenze peculiari.

Caratteristiche della soluzione originale sono la modularità, la completezza nell'offerta di servizi e l'uso di software open source. Interessante inoltre la scelta di alcune soluzioni, quali l'uso di caselle di posta virtuali e di un sistema di autenticazione facilmente riutilizzabile.

3.5 Sistema di autenticazione

Le caselle di posta non sono associate ad utenti reali sul sistema, come avveniva con il NIS. Si tratta pertanto di mailbox “virtuali”, più vantaggiose dal punto di vista della sicurezza in quanto non consentono agli utenti un accesso completo al sistema.

Il sistema di autenticazione è realizzato per mezzo di una base dati LDAP, facilmente

riutilizzabile anche per altri scopi. La chiave per l'autenticazione è l'indirizzo "primario" di posta elettronica (es. *Nome.Cognome*@ts.infn.it). La configurazione dei servizi è stata curata in modo da esonerare l'utente dalla digitazione del nome del dominio, limitando quindi lo username realmente utilizzato ad un identificativo del tipo *Nome.Cognome*. La possibilità di specificare anche il dominio potrebbe tuttavia risultare utile nel caso di un server che ospiti più domini di posta elettronica.

3.6 Scelta dell'MTA

Il Mail Transport Agent scelto è Postfix: oltre ad essere più semplice da configurare rispetto a Sendmail, ha anche il vantaggio di supportare il formato delle mail Maildir, che abbiamo deciso di utilizzare al posto di Mailbox.

Il formato Maildir utilizza un file per ogni singolo messaggio, a differenza di Mailbox che usa un file per ogni cartella. Di conseguenza, in caso di corruzione di un file, con Maildir l'eventuale perdita è limitata ad un messaggio, mentre con Mailbox si potrebbero avere problemi di accesso all'intera cartella che lo contiene.

3.7 Scelta del server POP/IMAP

Il server POP/IMAP scelto è Courier-IMAP, in quanto usa in modo nativo il formato Maildir, e supporta naturalmente i protocolli cifrati pops/imaps.

3.8 Antispam e antivirus

La disponibilità del software Sophos per l'INFN ci ha consentito di utilizzare questo prodotto come unico strumento per il filtraggio anti-spam e anti-virus. In precedenza era utilizzato SpamAssassin contro lo spam, mentre non era attivo un servizio anti-virus centralizzato sul mail server.

3.9 I principali software utilizzati

Riassumiamo i principali software utilizzati nella nuova struttura:

- Sistema operativo: Scientific Linux.
- Clustering: Red Hat Cluster Manager.
- MTA: Postfix.
- Antispam e antivirus: Sophos.
- Server IMAP/POP: Courier-IMAP.
- Web mail: Squirrelmail.
- Autenticazione degli utenti: tramite una base dati OpenLDAP.
- Gestione del proprio account da parte degli utenti: Phamm.
- Gestione degli account da parte dell'amministratore: Phamm e phpLDAPadmin.

- Mailing list: Mailman.

Tutto il software utilizzato è gratuito ed open source, escluso Sophos che è un prodotto commerciale. Una possibile alternativa gratuita potrebbe essere costituita da SpamAssassin e/o Amavis.

4 L'INSTALLAZIONE

4.1 Sistema operativo, ricompilazioni, ecc.

L'installazione del sistema operativo non ha comportato particolari difficoltà, tuttavia nel corso della configurazione dei servizi è stato necessario aggiornare alcuni pacchetti software al fine di ottenere certe funzionalità aggiuntive: è questo il caso in particolare di Postfix ed OpenLDAP. Questa operazione è stata effettuata prelevando gli RPM sorgenti dalla distribuzione di Scientific Linux 4 (appena rilasciata, ma ancora priva del supporto cluster) e ricompilandoli, all'occorrenza modificando lo SPEC file. Nel caso di Postfix, è stato abilitato il supporto SASL2, PCRE e VDA, quest'ultimo per poter definire la quota disco assegnata alle mailbox.

Oltre ai pacchetti principali sono stati ovviamente aggiornati anche quelli che fanno parte delle dipendenze.

4.2 Cluster

Sono stati definiti due servizi sul cluster:

1. LDAP: il servizio attiva il server LDAP per l'autenticazione degli utenti. Al servizio sono stati assegnati l'indirizzo IP ldap.ts.infn.it (140.105.6.18) ed una partizione (/ldap) sullo spazio disco condiviso.
2. Mail Server: il servizio attiva tutti i processi necessari al funzionamento della posta elettronica: Postfix, PureMessage, server IMAP/POP, httpd, ecc. L'indirizzo assegnato al servizio è postino.ts.infn.it (140.105.6.19); la partizione associata è /mail.

Tramite un opportuna definizione dei domain failover, il mail server è attivo su postman1, mentre il server LDAP su postman2.

Per lo start/stop del servizio LDAP non ci sono problemi particolari: trattandosi di un singolo daemon, è sufficiente utilizzare la normale script per lo startup di OpenLDAP (/etc/init.d/ldap).

Più complesso è lo start/stop del mail server. Dal momento che questo servizio di cluster è in realtà una combinazione di diversi processi, è stata predisposta una script (/etc/init.d/mail_server) che si occupa di effettuare lo start/stop di tutti i processi necessari nell'ordine corretto:

- postfix

- courier-imap
- Sophos
- mailman
- httpd

Dal momento che, all'avvio dei sistemi, viene comunque attivato un daemon Postfix in configurazione client, alla partenza del mail server viene prima di tutto bloccata ogni eventuale occorrenza di Postfix in esecuzione, ed in seguito viene attivato Postfix in configurazione server. Ciò è possibile specificando una directory diversa da quella di default (/etc/postfix) nella quale il daemon deve andare a cercare i file di configurazione. La configurazione di Postfix per la modalità server è salvata sullo spazio disco condiviso, in /mail/etc/postfix.

Il processo che gestisce il cluster sulle due macchine controlla lo stato dei servizi LDAP e Mail Server ogni cinque minuti. In caso di malfunzionamenti, è in grado di far ripartire i servizi nell'arco di circa un minuto.

4.3 OpenLDAP

La configurazione di OpenLDAP tiene conto degli esempi forniti con il software Phamm, il quale necessita di uno *schema* aggiuntivo (phamm.schema) e di opportune ACL. Il database è ospitato sul disco condiviso associato al servizio LDAP, mentre le configurazioni sono normalmente incluse nella directory /etc dei due nodi che compongono il cluster.

Il file /etc/openldap/slapd.conf include le seguenti parti salienti:

```
include         /etc/openldap/schema/core.schema
include         /etc/openldap/schema/cosine.schema
include         /etc/openldap/schema/inetorgperson.schema
include         /etc/openldap/schema/nis.schema
include         /etc/openldap/schema/RADIUS-LDAPv3.schema
# specific for mail
include         /etc/openldap/schema/phamm.schema
include         /etc/openldap/schema/ISPEnv2.schema
include         /etc/openldap/schema/amavis.schema
schemacheck     on

# Allow LDAPv2 client connections.  This is NOT the default.
allow bind_v2

sizelimit       20000

TLSCertificateFile /etc/ssl/slapd.crt
TLSCertificateKeyFile /etc/ssl/slapd.key
TLSCACertificateFile /etc/ssl/infn-ca.crt

include /etc/openldap/phamm-mail.acl
```

```
include /etc/openldap/userauth.acl
include /etc/openldap/final.acl

database        bdb
suffix          "dc=ts,dc=infn.it"
rootdn          "cn=Manager,dc=ts,dc=infn.it"
rootpw          {SSHA}..............

directory       /ldap/db
index objectClass                       eq,pres
index ou,cn,mail,surname,givenname      eq,pres,subinitial
index uidNumber,gidNumber,loginShell    eq,pres
index uid,memberUid                     eq,pres,subinitial
index nisMapName,nisMapEntry            eq,pres,subinitial
index vd,delete                         eq,pres
index accountActive,forwardActive       eq,pres
index smtpAuth                          eq,pres
index vacationActive                    eq,pres
```

Per quanto concerne le ACL, si è scelto di chiudere l'accesso per default per mezzo della regola:

```
access to * by * none
```

definita nel file final.acl. Prima di questa regola il file phamm-mail.acl, fornito con Phamm, definisce le ACL necessarie a Phamm. È stato inoltre creato un file usearauth.acl contenente alcune regole aggiuntive, che consentono tra l'altro il cambio della password da parte degli utenti autenticati:

```
access to dn.subtree="dc=ts,dc=infn.it" attrs=userPassword
  by dn="cn=Manager,dc=ts,dc=infn.it" write
  by self write
  by * auth

access to dn.subtree="dc=ts,dc=infn.it" attrs=shadowLastChange
  by dn="cn=Manager,dc=ts,dc=infn.it" write
  by self write
  by * read
```

4.3.1 Riempimento del database

Il database è stato riempito con i dati disponibili sul mail server esistente, in particolare trattando con opportune script realizzate su misura i dati contenuti nei file di autenticazione

(passwd) e nei database utilizzati da sendmail. Il risultato dell'elaborazione tramite le script è un file in formato LDIF, che è stato successivamente caricato nel database. Le entry sono strutturate in questo modo:

```
dn: mail=Raffaello.Sanzio@ts.infn.it,vd=ts.infn.it,o=hosting,dc=ts,dc=infn.it
objectclass: top
objectclass: VirtualMailAccount
objectclass: Vacation
objectclass: amavisAccount
objectclass: VirtualForward
mail: Raffaello.Sanzio@ts.infn.it
vdHome: /mail/vmail/domains
mailbox: ts.infn.it/Raffaello.Sanzio/
delete: FALSE
uid: Raffaello.Sanzio
sn: Sanzio
cn: Raffaello Sanzio
accountActive: TRUE
userPassword: {crypt}.....
description: Vacation description
vacationActive: FALSE
vacationStart: 01 gennaio 2004
vacationEnd: 01 gennaio 2004
vacationForward: user@ts.infn.it
amavisBypassVirusChecks: TRUE
amavisBypassSpamChecks: FALSE
forwardActive: FALSE
lastChange: 1108499023
amavisSpamKillLevel: 6.0
amavisSpamTag2Level: 5.5
amavisSpamTagLevel: 3.0
otherTransport: gnarwl:
quota: 629145600S
```

4.4 Postfix

Nell'appendice A è riportato il contenuto del file main.cf di Postfix predisposto per il mail relay.

4.4.1 Conversione delle mailbox

Il problema di convertire le mailbox esistenti dal formato mbox a maildir è stato risolto

utilizzando la script mb2md (http://batleth.sapienti-sat.org/projects/mb2md/).

4.5 Courier-IMAP

Sono stati installati i seguenti pacchetti RPM:

- courier-authlib-ldap
- courier-analog
- courier-authlib
- courier-imap

Le principali configurazioni riguardano l'autenticazione, pertanto si riferiscono ai file presenti nella directory /etc/authlib. In particolare, nel file *authdaemonrc* deve essere abilitata l'autenticazione tramite LDAP:

```
authmodulelist="authldap"
```

Il file *authldaprc* deve essere invece modificato in modo da riflettere la configurazione di LDAP:

```
LDAP_SERVER           ldap.ts.infn.it
LDAP_BASEDN           o=hosting,dc=ts,dc=infn.it
LDAP_BINDDN           cn=phamm,o=hosting,dc=ts,dc=infn.it
LDAP_BINDPW           password
LDAP_AUTHBIND         1
LDAP_MAIL             uid
LDAP_FILTER           (accountActive=TRUE)
LDAP_GLOB_UID         vmail
LDAP_GLOB_GID         vmail
LDAP_HOMEDIR          vdHome
# LDAP_DEFAULTDELIVERY        defaultDelivery
LDAP_MAILDIRQUOTA     quota
# LDAP_CLEARPW                clearPassword
LDAP_TLS              1
```

4.6 Servizi web: Apache

Oltre ai servizi relativi alla posta elettronica, sui server è stato attivato anche un servizio web, basato su Apache, che permette la gestione dei seguenti moduli tramite un'interfaccia web:

- Web mail.
- Gestione degli account da parte dell'amministratore tramite phpLDAPadmin e Phamm.
- Gestione ordinaria del proprio account da parte degli utenti tramite Phamm.
- Configurazione delle mailing list ed accesso agli archivi.

- Interfaccia di gestione di Sophos e accesso alla quarantena da parte degli utenti.

Il processo httpd viene fatto partire solo sulla macchina che è attiva come mail server.

Sono stati definiti due host virtuali, il primo dedicato al servizio di web mail e il secondo a tutte le funzionalità amministrative, esclusa la gestione del sistema antispam/antivirus, che è controllata direttamente da Sophos in modo autonomo.

Gli alberi di directory dei due virtualhost sono ospitati sul disco condiviso (/mail/www/vhosts). Essi contengono o fanno riferimento a tutti i pacchetti elencati poco sopra.

Per motivi di sicurezza, i due host virtuali sono accessibili esclusivamente tramite una connessione cifrata.

4.7 Gestione degli account: Phamm e phpLDAPadmin

Phamm (PHP LDAP Virtual Hosting Manager) è un front-end modulare scritto in PHP che permette di gestire servizi virtuali utilizzando un database LDAP. Uno dei moduli disponibili permette una gestione molto agevole di mailbox virtuali. La stessa interfaccia abilita inoltre gli utenti alla normale amministrazione della propria mailbox, consentendo operazioni quali il cambio della password e la definizione di un forward verso un diverso indirizzo.

Il software è stato installato all'interno del sito web dedicato alla gestione del mail server (/mail/www/vhosts/htdocs.postino.ts.infn.it/phamm).

Nel file di configurazione principale (config.inc.php) sono stati modificati i seguenti parametri:

```
define (LDAP_HOST_NAME,'ldap.ts.infn.it');
define (SUFFIX,'dc=ts,dc=infn.it');
define (BINDDN,'cn=Manager,dc=ts,dc=infn.it');
$LDAP_BASE ='o=hosting,dc=ts,dc=infn.it';
define (FORCE_SSL,1);
define (PASSWORD_MIN_LENGHT,6);
define (DEFAULT_DOMAIN,'ts.infn.it');
```

Nel file di configurazione specifico per il modulo mail (plugins/mail/config.inc.php) è stato invece disattivato l'uso di Amavis, che è l'antivirus suggerito per default da Phamm, in quanto è stato preferito Sophos:

```
define (USE_AMAVIS, 0);
```

Oltre a Phamm, è stato installato il software phpLDAPadmin, che consiste in un'interfaccia web ad un database LDAP generico. Rispetto a Phamm, questa interfaccia risulta molto più completa e consente alcune operazioni particolari che Phamm non prevede. D'altro lato, Phamm è dedicato alla posta elettronica ed è quindi più comodo per la gestione ordinaria delle caselle di posta virtuali.

Al fine di velocizzare eventuali creazioni contemporanee di numerose caselle di posta

sono state inoltre realizzate alcune script, che permettono di attivare da linea di comando una nuova mailbox oppure un alias, immettendo un numero minimo di parametri.

4.8 Sophos

L'installazione di Sophos è stata effettuata secondo la normale procedura prevista dal software; per facilitarla si è reso necessario modificare il file /etc/redhat-release con la stringa di identificazione originale Red Hat.

È stato scelto di installare il programma nella partizione /mail associata al servizio SMTP, più precisamente in /mail/opt/pmx. Purtroppo non è stato possibile configurare il software in modo da utilizzare l'alias postino.ts.infn.it: questo comporta un piccolo malfunzionamento nella generazione dei report, poiché i dati vengono etichettati in base all'hostname, che può essere postman1.ts.infn.it oppure postman2.ts.infn.it.

L'autenticazione degli utenti per l'accesso all'interfaccia di gestione dello spam avviene tramite LDAP. Questo è possibile inserendo nel file /mail/opt/pmx/etc/enduser.conf la linea "auth = ldap".

4.9 Gestione delle mailing list: mailman

Il vecchio server di posta elettronica utilizzava il software Majordomo per la gestione delle mailing list, e Mhonarc per l'archiviazione su web dei mail in transito su alcune liste.

Per la nuova struttura abbiamo scelto di utilizzare Mailman, che riunisce entrambe le funzioni svolte da Majordomo e Mhonarc ed è già disponibile come pacchetto RPM nella distribuzione di Scientific Linux.

Dopo aver installato normalmente il pacchetto, abbiamo traslocato sullo spazio disco condiviso la parte del software che deve essere gestita da entrambi i server:

/var/mailman → /mail/mailman

Abbiamo inoltre ridefinito /var/mailman come link simbolico a /mail/mailman, in modo che i file di configurazione e le script installati con il pacchetto continuino a vedere il software sotto /var/mailman. La condivisione dell'albero da parte dei due server è fondamentale, in quanto esso contiene non solo il software, ma anche le configurazioni e gli archivi delle liste.

Il file /etc/httpd/conf.d/mailman.conf deve essere poi modificato in modo da riflettere i path utilizzati sul web server per Mailman e gli eventuali archivi delle mailing list:

```
ScriptAlias /mailman/ /mail/mailman/cgi-bin/
<Directory /mail/mailman/cgi-bin/>
    AllowOverride None
    Options ExecCGI
    Order allow,deny
    Allow from all
</Directory>
```

```
Alias /pipermail/ /mail/mailman/archives/public/
<Directory /mail/mailman/archives/public>
    Options Indexes MultiViews FollowSymLinks
    AllowOverride None
    Order allow,deny
    Allow from all
</Directory>

RedirectMatch ^/mailman[/]*$
https://postino.ts.infn.it:8079/mailman/listinfo
```

4.9.1 Trasloco delle mailing list esistenti

Le liste esistenti sotto Majordomo devono essere ridefinite a mano in Mailman.

Nel caso, piuttosto frequente, in cui si abbiano più liste con caratteristiche simili, è possibile semplificare il procedimento: infatti è sufficiente definire una lista in Mailman; quindi utilizzare la script *config_list* per salvare la configurazione della lista, modificarla a piacere, e usare di nuovo *config_list* per creare una nuova lista a partire dalla configurazione modificata. Ad esempio:

- *(creare la lista "listaoriginale" in Mailman tramite l'interfaccia web)*
- `# ~mailman/bin/config_list -o listaoriginale mialista.txt`
- *(editare il file mialista.txt)*
- `# ~mailman/bin/config_list -i nuovalista mialista.txt`

Per il trasferimento degli archivi di Mhonarc in Mailman, è necessario utilizzare qualche strumento di conversione poiché i formati dei dati sono diversi. Non abbiamo trovato uno strumento che effettui il passaggio diretto, ma è possibile utilizzare come tramite il formato Mailbox ed eseguire una doppia conversione. Come primo passo abbiamo utilizzato la script *mhn2mbox.pl*, che è inclusa tra i Contrib di Mhonarc, per convertire ogni singolo archivio di Mhonarc in formato Mailbox:

```
# mhn2mbox.pl /mailing-lists/mialista/html mialista.mbox
```

Il file ottenuto è stato successivamente convertito nel formato Pipermail, utilizzato da Mailman, per mezzo della script *arch* disponibile nel pacchetto Mailman:

```
# ~mailman/bin/arch  mialista mialista.mbox
```

4.10 Squirrelmail

Il software scelto per il servizio di web mail è Squirrelmail, principalmente per la disponibilità di un gran numero di plugin che permettono di eseguire diversi compiti.

La versione installata è quella fornita in formato RPM con la distribuzione corrente di Scientific Linux. Sullo spazio disco condiviso dai due server sono stati spostati i sottoalberi

contenenti le preferenze e gli attachment, in modo da renderli visibili a entrambi i server:

/var/lib/squirrelmail/prefs → /mail/squirrelmail/var/lib/squirrelmail/prefs
/var/spool/squirrelmail/attach → /mail/squirrelmail/var/spool/squirrelmail/attach

Il file di configurazione specifico /etc/squirrelmail/config_local.php ridefinisce solo alcuni parametri rispetto alla configurazione di default (/etc/squirrelmail/config.php):

```
$org_name = "INFN Sezione di Trieste";
$org_title ="Web Mail service at INFN Trieste";
$domain = 'ts.infn.it';
$imapServerAddress = 'postino.ts.infn.it';
$useSendmail = false;
$smtpServerAddress = 'postino.ts.infn.it';
$imap_server_type = 'courier';
$default_folder_prefix = 'INBOX.';
$optional_delimiter = '.';
$data_dir='/mail/squirrelmail/var/lib/squirrelmail/prefs/';
$attachment_dir='/mail/squirrelmail/var/spool/squirrelmail/attach/';
$force_username_lowercase = true;
```

Sul disco condiviso è stato copiato anche tutto il software necessario al funzionamento dell'interfaccia web: anche in questo caso abbiamo preferito condividere la struttura di directory tra le due macchine, in modo da aggiungere centralmente eventuali plugin senza bisogno di installarli separatamente sui due server:

/usr/share/squirrelmail → /mail/www/vhosts/htdocs.webmail.ts.infn.it

La configurazione del server httpd che consente l'accesso al servizio di web mail deve naturalmente rispecchiare questa situazione. Di conseguenza in /etc/httpd/conf.d/ssl.conf abbiamo definito il seguente virtualhost:

```
<VirtualHost 140.105.6.19:443>
ServerName webmail.ts.infn.it
DocumentRoot /mail/www/vhosts/htdocs.webmail.ts.infn.it
ErrorLog /mail/www/logs/webmail.ts.infn.it-error_log
CustomLog /mail/www/logs/webmail.ts.infn.it-access_log combined
HostnameLookups Off

(...)

<Directory "/mail/www/vhosts/htdocs.webmail.ts.infn.it">
  Options IncludesNOEXEC FollowSymLinks
  AllowOverride All
</Directory>
</VirtualHost>
```

Per motivi di sicurezza, abbiamo scelto di rendere accessibile il servizio di web mail solamente tramite connessione cifrata, appoggiandoci alla configurazione SSL del server httpd Apache, installato sui due mail server.

4.10.1 Plugin per Squirrelmail

Sono stati installati i seguenti plugin, reperibili sul sito di Squirrelmail:

- *quota_usage*, che visualizza la percentuale di quota disco utilizzata, in forma numerica e di istogramma;
- *change_ldappass*, che consente all'utente di cambiare la propria password sul repository LDAP;
- *squirrel_logger*, che permette di effettuare il logging di eventi relativi al servizio di web mail (login, logout, ecc.).

5 RINGRAZIAMENTI

Gli autori ringraziano Mirko Grava di RHX per il progetto globale del mail server e per la preziosa assistenza fornita in fase di installazione. Un grazie anche ad Alessandro De Zorzi di RHX per la disponibilità dimostrata nell'aggiungere al software Phamm alcune utili funzionalità.

BIBLIOGRAFIA

Documenti e pubblicazioni

1. R. Gomezel et al. - "Realizzazione di un Mail Server su Trucluster con software ASE" (INFN/TC-02/02)
2. M. Grava - “Postfix+LDAP+Courier-IMAP+JAMM howto”
3. “Red Hat Cluster Suite - Configuring and Managing a Cluster”- Red Hat, Inc. Mission Critical Linux, Inc. K.M. Sorenson

Siti web

- Postfix: www.postfix.org
- Courier-IMAP: www.courier-mta.org/imap
- Mailman: www.gnu.org/software/mailman
- Squirrelmail: www.squirrelmail.org
- Phamm: www.phamm.org

APPENDICE A: MAIN.CF

Si riporta di seguito il contenuto del file main.cf utilizzato sul server di posta elettronica.

```
queue_directory = /mail/spool/postfix
command_directory = /usr/sbin
daemon_directory = /usr/libexec/postfix
mail_owner = postfix
myhostname = postino.ts.infn.it
mydomain = ts.infn.it
myorigin = $mydomain
inet_interfaces = all
unknown_local_recipient_reject_code = 550
mynetworks = 127.0.0.1, 140.105.6.0/24, 140.105.7.0/24, 140.105.31.0/24,
140.105.131.0/24, 140.105.192.0/24, 140.105.221.0/24, 140.105.223.0/24
relay_domains = $mydestination
alias_maps = hash:/mail/etc/postfix/aliases
alias_database = hash:/mail/etc/postfix/aliases
mail_spool_directory = /mail/spool/mail
debug_peer_level = 2
debugger_command =
       PATH=/bin:/usr/bin:/usr/local/bin:/usr/X11R6/bin
       xxgdb $daemon_directory/$process_name $process_id & sleep 5
sendmail_path = /usr/sbin/sendmail.postfix
newaliases_path = /usr/bin/newaliases.postfix
mailq_path = /usr/bin/mailq.postfix
setgid_group = postdrop
html_directory = /usr/share/doc/postfix-2.1.5-documentation/html
manpage_directory = /usr/share/man
sample_directory = /mail/etc/postfix
readme_directory = /usr/share/doc/postfix-2.1.5-documentation/readme

#########################################################################
# Max dimensione delle mailbox (per default e' 50 MB):
mailbox_size_limit = 0

# Max dimensione del singolo messaggio (per default e' 10 MB):
message_size_limit = 52428800

# Abilitazione protocollo SASL
smtpd_sasl_auth_enable = yes
smtpd_sasl_application_name = smtpd
smtpd_sasl_security_options = noanonymous
smtpd_sasl_local_domain =
broken_sasl_auth_clients = yes
smtpd_recipient_restrictions = permit_sasl_authenticated,
permit_mynetworks, reject_unauth_destination

# TLS support
smtpd_tls_cert_file = /etc/ssl/postino.crt
smtpd_tls_key_file = /etc/ssl/postino.key
smtpd_tls_CAfile = /etc/ssl/infn-ca.crt
smtpd_tls_received_header = yes
smtpd_use_tls = yes
smtpd_tls_session_cache_database = sdbm:/mail/etc/postfix/smtpd_scache
smtpd_tls_session_cache_timeout = 3600s
smtpd_starttls_timeout = 300s
#########################################################################
```

```
# Sezione PHAMM
########################################################################
ldap_bind_dn = cn=phamm,o=hosting,dc=ts,dc=infn.it
ldap_bind_pw = <segreta>
ldap_search_base = o=hosting,dc=ts,dc=infn.it
ldap_domain = dc=ts,dc=infn.it
ldap_server_host = ldap.ts.infn.it
ldap_server_port = 389

# transports
transport_server_host = $ldap_server_host
transport_search_base = $ldap_search_base
transport_query_filter =
(&(&(vd=%s)(objectClass=VirtualDomain))(accountActive=TRUE)(delete=FALSE))
transport_result_attribute = postfixTransport
transport_cache = no
transport_bind = yes
transport_scope = one
transport_bind_dn = $ldap_bind_dn
transport_bind_pw = $ldap_bind_pw

# aliases
aliases_server_host = $ldap_server_host
aliases_search_base = $ldap_search_base
aliases_query_filter =
(&(&(objectClass=VirtualMailAlias)(mail=%s))(accountActive=TRUE))
aliases_result_attribute = maildrop
aliases_bind = yes
aliases_cache = no
aliases_bind_dn = $ldap_bind_dn
aliases_bind_pw = $ldap_bind_pw

# VirtualForward
virtualforward_server_host = $ldap_server_host
virtualforward_search_base = $ldap_search_base
virtualforward_query_filter =
(&(&(objectClass=VirtualMailAccount)(mail=%s))(forwardActive=TRUE)(account
Active=TRUE)(delete=FALSE))
virtualforward_result_attribute = maildrop
virtualforward_bind = yes
virtualforward_cache = no
virtualforward_bind_dn = $ldap_bind_dn
virtualforward_bind_pw = $ldap_bind_pw

# Accounts
accounts_server_host = $ldap_server_host
accounts_search_base = $ldap_search_base
accounts_query_filter =
(&(&(objectClass=VirtualMailAccount)(mail=%s))(forwardActive=FALSE)(accoun
tActive=TRUE)(delete=FALSE))
accounts_result_attribute = mailbox
accounts_cache = no
accounts_bind = yes
accounts_bind_dn = $ldap_bind_dn
accounts_bind_pw = $ldap_bind_pw

accountsmap_server_host = $ldap_server_host
accountsmap_search_base = $ldap_search_base
accountsmap_query_filter =
```

```
(&(&(objectClass=VirtualMailAccount)(mail=%s))(forwardActive=FALSE)(accoun
tActive=TRUE)(delete=FALSE))
accountsmap_result_attribute = mail
accountsmap_cache = no
accountsmap_bind = yes
accountsmap_bind_dn = $ldap_bind_dn
accountsmap_bind_pw = $ldap_bind_pw

# virtual quota
quota_server_host = $ldap_server_host
quota_search_base = $ldap_search_base
quota_query_filter =
(&(&(objectClass=VirtualMailAccount)(mail=%s))(accountActive=TRUE)(delete=
FALSE))
quota_result_attribute = quota
quota_cache = no
quota_bind = yes
quota_bind_dn = $ldap_bind_dn
quota_bind_pw = $ldap_bind_pw

# transport on the fly for gnarwl
gnarwl_server_host = $ldap_server_host
gnarwl_search_base = $ldap_search_base
gnarwl_query_filter =
(&(&(objectClass=VirtualMailAccount)(mail=%s))(vacationActive=TRUE)(accoun
tActive=TRUE)(delete=FALSE))
gnarwl_result_attribute = otherTransport
gnarwl_cache = no
gnarwl_bind = yes
gnarwl_bind_dn = $ldap_bind_dn
gnarwl_bind_pw = $ldap_bind_pw

# transport_maps
maildrop_destination_concurrency_limit = 1
maildrop_destination_recipient_limit = 1
transport_maps = hash:/mail/etc/postfix/transport, ldap:gnarwl,
ldap:transport
mydestination = $transport_maps, localhost, $myhostname,
localhost.$mydomain, $mydomain, trieste.infn.it, postino.ts.infn.it,
ldap.ts.infn.it, $myorigin
virtual_maps = hash:/mail/etc/postfix/virtual, ldap:virtualforward,
ldap:aliases, ldap:accountsmap

# Canonical
canonical_maps = hash:/mail/etc/postfix/canonical

# Virtual Accounts
virtual_mailbox_base = /mail/vmail/domains
virtual_mailbox_maps = ldap:accounts
virtual_minimum_uid = 500
virtual_uid_maps = static:500
virtual_gid_maps = static:500

local_recipient_maps = proxy:unix:passwd.byname, $alias_maps,
$virtual_mailbox_maps

virtual_mailbox_limit = 5368709120
virtual_maildir_limit_message = "The user you're trying to reach is over
quota. Please try again later or contact him/her in another way."
```

```
virtual_mailbox_limit_maps = ldap:quota
virtual_mailbox_limit_override = yes
virtual_mailbox_limit_inbox = no
virtual_maildir_extended = yes
virtual_create_maildirsize = yes
virtual_overquota_bounce = yes

# This is for Mailman (see /usr/share/doc/mailman-2.1.5/README.POSTFIX):
owner_request_special = no
recipient_delimiter = +

# Sophos
content_filter = pmx:localhost:10025
```