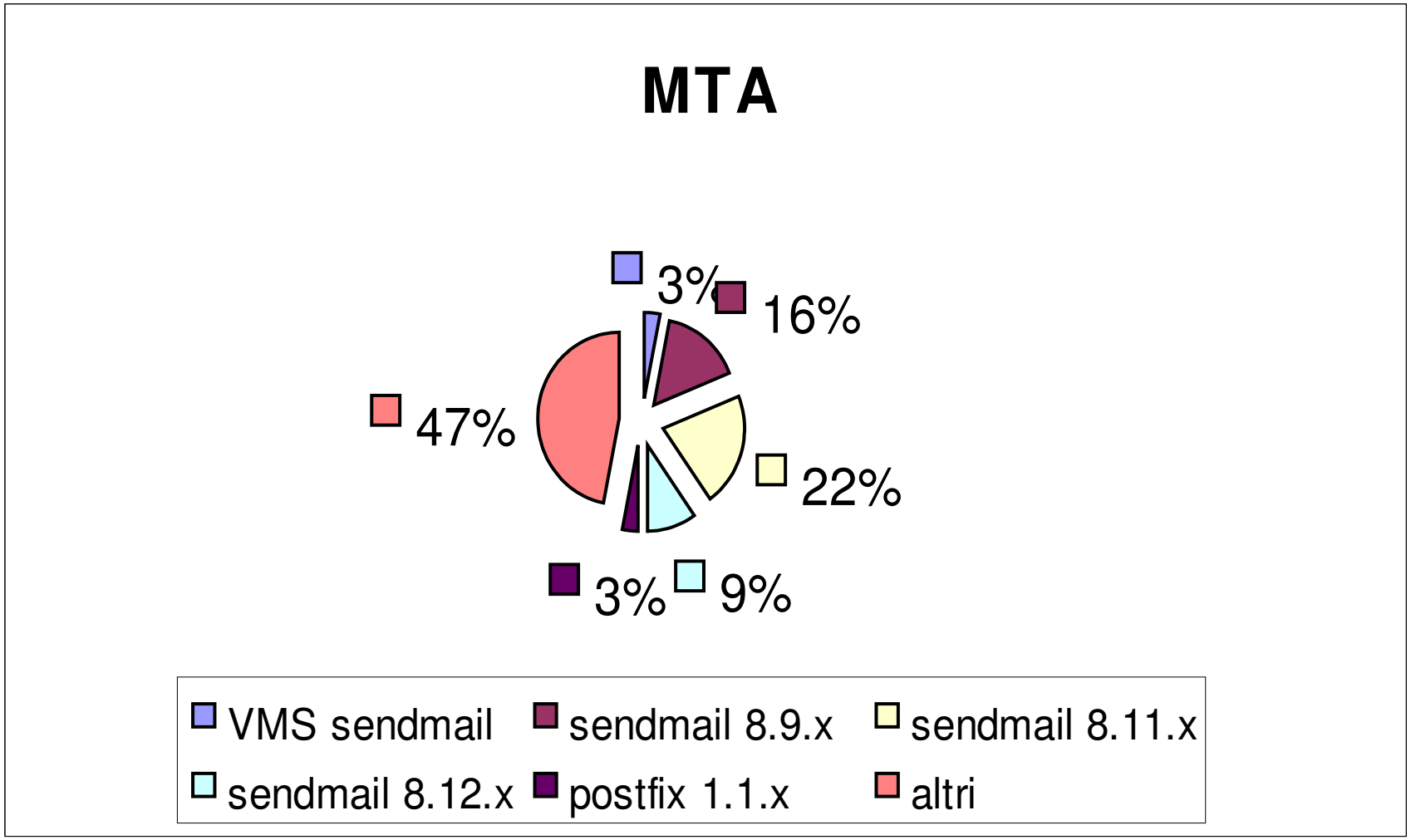
Mailing nell’INFN

Stato e prospettive

Mailer Transport Agent



Situazione attuale (1)

- Mail Transport Agent
  - Sendmail MTA piu' diffuso
    - Piattaforma Intel con Linux (ma anche FreeBSD)
    - presenti anche: VMS, Solarix, AIX
    - Varie versioni installate (8.9.x, 8.11.x, 8.12.x)
  - Postfix
- Antivirus
  - nessuno
  - RAV
  - Sophos + Amavis
- Mailbox server
  - Cyrus
  - Imap-wu

Situazione attuale (2)

- Webmail
  - Imho piu’ diffuso
    - Necessita roxen
  - Squirrel
  - Imp
    - Installazione difficoltosa
  - Twig
- Gestore mailing list
  - Majordomo
    - Manutenzione non banale
    - Gestione pesante
    - Problemi di sicurezza
  - File Alias

Servizi centrali

- ls.infn.it
  - Mail server centrale per dominio infn.it
  - Gestione mailing list @infn.it (~ 100)
- infngw.infn.it
  - Mail server di backup per domini GARR
    - Effettua mail *diretti* a domini GARR
  - Supporto protocollo smtp
    - Timeout di 20 giorni
- cosine-gw.infn.it
  - Mail server di backup per domini GARR
  - Supporto protocollo smtp, X-400

Supporto MTA

- Sendmail Berkeley
  - Supporto su nuove versioni
- Sendmail VMS
  - Sviluppo congelato
  - Supporto per eventuali bug
- Altri MTA
  - Non supportati (al momento)
  - E’ necessario ?

Raccomandazioni

- Server dedicato
  - *Non permettere accesso interattivo utenti*
  - Eventualmete ridondato
  - Mailbox server separato (dipende dal carico)
- MTA:Sendmail 8.12.x
  - Misure antirelaying (Starttls, smtpauth)
  - Antivirus (rav, amavis+sophos ??)
  - Misure antispam (spam-assassin ?)
- Mailbox server sw
  - Disabilitare servizi non criptati
    - Imap, pop

Situazione al CNAF

- ~ 40 utenti
- Server Pentium III biprocessore 1.2 GHz
  - 100 GB disco in RAID 5
  - 512 MB RAM
- Sendmail 8.12.2
  - Smtp auth, starttls
    - Db password: sasldb
- Cyrus 2.0.16
  - Imaps, pops
  - Sieve
    - Websieve (http://sourceforge.net/projects/websieve)
- Imp
  - Apache + mod_ssl
  - mysql
- Majordomo 1.94.4-7

Feature evolute di sendmail 8.12.x

Protezioni, Autenticazione sicura

sendmail: protezioni (1)

- sendmail necessita privilegi root per:
  - bind alla porta 25
  - Accesso a file .forward
  - invocazione del LDA come root se LDA non e' set-user-ID root
  - accodamento e-mail sottomessi da command line
    - Necessita anche set-user-id/set-group-id
- 2 processi distinti
  - daemon (*sendmail.cf, /var/spool/mqueue*)
  - MSP (*submit.cf, /var/spool/clientmqueue*)
  - sendmail non configurato come set-user-ID root
    - Default da versione 8.12
  - sendmail set-group id per scrivere in coda mail

sendmail: protezioni (2)

- Configurazione standard:
  - uid root, gid smmsp (gid 25)

-r-xr-sr-x root smmsp /usr/sbin/sendmail

- Protezioni directory, file

drwxrwx---	*smmsp*	*smmsp*	*/var/spool/clientmqueue*
drwx------	*root*	*wheel*	*/var/spool/mqueue*
-r--r--r--	*root*	*wheel*	*/etc/mail/sendmail.cf*
-r--r--r--	*root*	*wheel*	*/etc/mail/submit.cf*

- Invocazione processi

Daemon: */usr/sbin/sendmail -L sm-mta -bd -q1h*

MSP: */usr/sbin/sendmail -L sm-msp-queue -Ac -q30m*

Misure antispam (1)

- Attuale controllo basato su DNS .....
  - Necessario registrare host in DNS
  - Abilitare reti/dominio in access
- ..... non funzionale
  - Controllo “blando”
  - Problemi con dialup da ISP
    - relaying non ammesso dall’esterno
  - Stesso problema con portatili

Misure antispam (2)

- Controllo basato su credenziali utente
  - Solo utenti esplecitamente autorizzati ammessi al relaying
  - Controllo credenziali con modalita’ sicura
- Estensioni sicurezza protocollo smtp
  - SMTP AUTH (RFC 2554)
    - Basato su specifiche Simple Authentication and Security Layer (SASL: RFC 2222)
    - Descrive specifiche possibili metodi di autenticazione
  - SMTP STARTTLS (RFC 2487)
    - Basato su specifiche Transport Layer Security (TLS: RFC 2446)
    - Descrive modalita' di criptazione del canale di comunicazione
  - Permettono autenticazione sicura in modalita’ server ed in modalita’ client del gestore della posta

Misure antispam (3)

http://www.cert.garr.it/documenti/mailsicuro.pdf

Conclusioni

Cose da fare (1)

- Preparazione file di configurazione e documentazione sendmail 8.12.x con:
  - Sistema autenticazione sicura
    - Smtp auth
    - starttls
  - Sistema antivirus
    - Individuazione/valutazione sistema antivirus (RAV ? Amavis ?)
  - Sistema antispam
    - Test (SpamAssassin ?)

Cose da fare (2)

- Individuazione gestore di mailing list alternativo a majordomo (if any) o sviluppo patch
- Individuazione/implementazione interfaccia gestione utenti mail
- Individuazione/implemetazione interfaccia gestione mailing list
- Sistema di cambio password per cyrus/sendmail
- Valutazione webmail
- Valutazione interfaccia scripting sieve
  - Websieve ?