

# Gruppo Mailing Report

---

Alessandro Brunengo  
per il gruppo mailing di CCR

---

# Mail relay per indirizzi @infn.it

# Supporto indirizzi @inf.n.it

---

Flusso entrante verso record MX di inf.n.it

Redistribuzione verso la destinazione finale (sedi) tramite alias

Il supporto esiste già'

```
# dig @131.154.1.3 inf.n.it mx
```

```
;; ANSWER SECTION:
```

```
inf.n.it. 172800 IN MX 50 infngw.inf.n.it.
```

```
inf.n.it. 172800 IN MX 10 server10.inf.n.it.
```

Usato per pochi alias, gestiti manualmente

# Soluzione da rivedere

---

La soluzione attuale non e' nata per offrire un servizio esteso

- **Non scala** ad un aumento di traffico
- Soluzione **non resiliente alla perdita di connettivita'** del CNAF
- Non scala per **gestibilita'**
  - configurazione manuale
  - macchine completamente diverse
  - gestione manuale degli alias

Il gruppo mailing sta' studiando una soluzione idonea a supportare l'indirizzamento @inf.n.it diffuso

- Studio ancora da completare

# Requisiti minimi

---

Continuità' di servizio (HA, ridondanza multisito)

Scalabilità' (anche dinamica)

Automazione per installazione e (ri)configurazione

Monitoraggio, allarmistica, log, statistiche (analisi dello storico)

Impatto minimo sui servizi di delivery locali

Supporto filtri antispam/antivirus

- Eventuale accesso a configurazioni personalizzate o quarantena tramite AAI (requisito da valutare in futuro)

Supporto all'utenza per il tracciamento dei messaggi

# Considerazioni sui requisiti

---

Protocollo SMTP implementa ridondanza e HA a livello applicativo

- possibile avere **piu' relay su diversi siti e diverse reti IP**

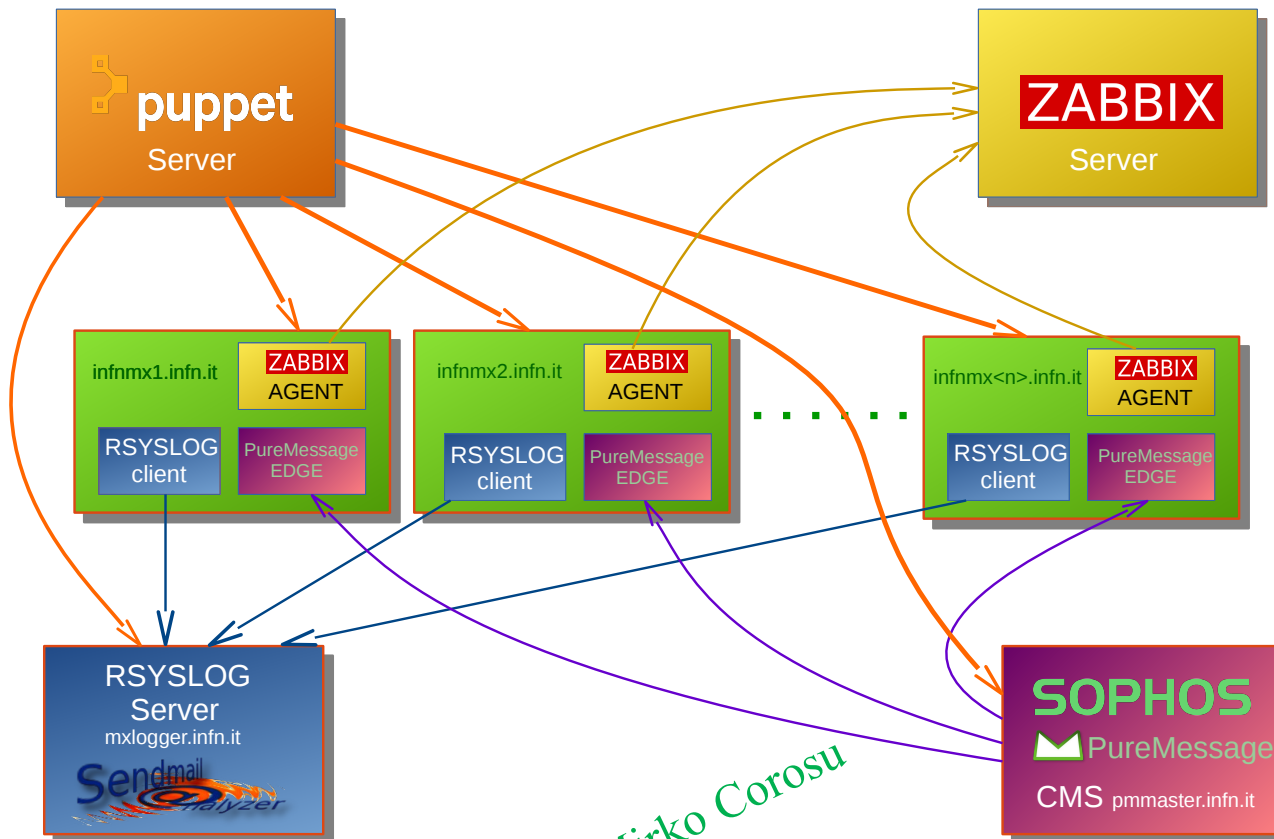
Il mail relay non necessita di storage condiviso

- Idoneo a girare su VM
- Idoneo (eventualmente tramite utilizzo di DNS dinamico per la creazione di MX) ad incrementare la capacita' di inoltro con l'aumento di VM

La stessa tecnica (utilizzo di alias) puo' essere utilizzata per reinstradare indirizzi verso destinazioni diverse dalle attuali

- La soluzione deve essere idonea a supportare soluzioni di delivery diverse da quella distribuita (anche parziale)

# Schema proposto



Img by: Mirko Corosu

# I nodi del servizio

---

**infnmx\***: nodi registrati nei record MX di infn.it

- ricevono le mail, operano i filtri antispam/antivirus, inoltrano sulla base degli alias
  - filtro selettivo solo su IP blocking, il resto introduce solo un header
- log locale (7 giorni) e remoto
- segnalano il proprio stato allo zabbix server
- raccolgono la configurazione da puppet e da pmmaster
- nodi che operano indipendentemente dal resto

**pmmaster**: ospita una installazione completa di Sophos Pure Message

- distribuisce le configurazioni di Sophos ai relay
- ospita statistica e quarantena (se usata)

# I nodi del servizio (cont.)

---

**mxlogger**: raccoglie i log degli MX (rsyslogd) salvandoli su file separati e su unico file aggregato

- conservazione dei log a lungo termine
- esegue software di analisi statistica complessivo del sistema di relay (Sendmail Analyzer)

**puppet**: ospita e distribuisce la configurazione di tutti i componenti ai diversi server

- esegue la procedura di creazione degli alias da AAI

**zabbix**: server di monitoraggio ed allarmistica

- controlla lo stato dei server e produce report grafici
- esegue azioni e segnala allarmi in funzione di eventi

# Elementi critici e non critici

---

I nodi critici, per cui si deve garantire continuita' di servizio (nel loro complesso) sono **i relay**...

- I nodi infnmx\* contengono tutta la configurazione necessaria ad eseguire le funzioni critiche del servizio:
  - ricezione ed inoltro dei messaggi
  - eventuale analisi antispam/antivirus
  - conservazione dei log su disco locale (per un tempo limitato)

... ed ovviamente **l'allarmistica (Zabbix)**

Gli altri nodi (configuratori, logger) svolgono funzioni che non richiedono continuita' di servizio

# Elementi non specifici del servizio di mail relay

---

Le funzioni svolte dal configuratore (puppet) e dal server di monitoraggio (zabbix) **non sono specifici del servizio di mail relay**, e potrebbero fare parte della infrastruttura dei SSNN

Ci sono requisiti su tali servizi per lo schema proposto:

- puppet deve eseguire la **procedura automatizzata di generazione degli alias**
- la configurazione di zabbix deve supportare **allarmistica via SMS** e deve avere una **configurazione specifica per i server MX**

# Impatto sui servizi di relay locale

---

Inizialmente il sistema **non deve introdurre filtri selettivi**

- Il filtro e' demandato ai relay locali, secondo le policy locali
- L'analisi del filtro antispam **produce un header opportuno**

Fanno eccezione:

- **IP blocking**: eseguito dai relay nfnmx\*, con filtro
- **Controllo SPF**: eseguito dai relay infnmx\*, con generazione di un header opportuno (richiede configurazione locale)

L'unico impatto vero e' sul **grey-listing locale**, che non ha effetto sulle mail transitate dai relay infnmx\*

# Build automatico dell'alias file: InfnAlias

---

Realizzata una procedura (InfnAlias) di creazione automatica degli alias prendendo le informazioni da AAI

- e' fondamentale poter disporre di un db come AAI

Qualche problema in

- uid tem
- attributi

**Risolto: l'applicativo gestisce entry incomplete**

Alias da creare in base al ruolo su

- sembra ragionevole
- post
- la lin
- servizi

**Risolto: l'applicativo supporta filtri configurabili su qualsiasi attributo di LDAP**

l'operazione deve essere fatta a livello del

# Run: output (parziale)

---

Got 22971 entries from AAI

Got 0 entries from registered aliases

Skipped by no uid: 10150

Skipped by multiple uid: 0

Skipped by default uid: 1876

Skipped by no mail or mailAlternateAddress: 376

Skipped by no mail in infn.it subdomains: 990

Warning: entries without mail attribute: 2

Warning: entries with multiple mail attribute: 0

Warning: entries without schacPersonalUniqueID attribute: 9579

Warning: entries with multiple schacPersonalUniqueID attribute: 0

Got 9579 good entries from AAI

Got 5933 filtered entries from AAI

Got 5933 aliases in AAI

Got 5933 new aliases

# Indirizzi estetici

---

InfnAlias ricostruisce indirizzi estetici, sulla base delle informazioni trovate su AAI

Il problema delle omonimie oggi coinvolge **43 persone (21 collisioni, una tripla)**

- non e' un problema insostenibile
- va pero' deciso un **criterio di assegnazione** che valga anche per il futuro

Una opzione e' assegnare l'indirizzo estetico solo a chi lo chieda (tramite interfaccia web)

- Demanda all'utente la scelta in caso di omonimia
- Scelta da definire: il gruppo non ha una opinione omogenea

# Dimensionamento

---

Analisi dei numeri basata su estrapolazione dai dati di una singola sede

- non affidabile, verra' fatta piu' accurata

mail entranti: 400k/giorno

dimensione mail entranti: 20 GB/giorno

log entry: 2.5 M/giorno

log size: 800 MB/giorno

- basato su log level default per sendmail

# Dimensionamento (cont.)

---

## Dimensionamento dei relay infnmx\*

- nella ipotesi di **4 relay, di cui 3 sempre operativi** (~135k mail/giorno, ~7 GB/giorno)
- 4 core/16 GB di RAM gestiscono picchi fino a 400 mail/sec (ma con delivery su LAN)
- 50 GB di spool (ospita le mail per 7 giorni)
- 2 GB per i log (ospita i log per 7 giorni)
- rete: non appare essere un problema

# Dimensionamento (cont.)

---

## mxlogger

- 2.5M log/giorno, 800 MB/giorno sono facilmente gestiti da rsyslogd su una VM con un core e 2 GB di RAM, anche includendo il mail analyzer (fa analisi incrementale sui log)

## pmmaster

- Test **non significativi** eseguiti su VM con 2 core e 4 GB di RAM. Va valutata in condizioni di traffico piu' intenso (critico l'accesso al db di sophos)
- si deve valutare, in produzione, l'utilizzo di Sophos appliance

# Considerazioni sulla scalabilita'

---

La gestione di un limitato insieme di nodi tramite server centrali di configurazione e di monitoring **non e' un problema**

- puppet e zabbix gestiscono numeri considerevolmente piu' grandi

Il problema da affrontare e' l'eventuale crescita (anche episodica) di traffico entrante

- gestibile tramite **aumento di mail relay** a parita' di priorita'
  - eventualmente a priorita' maggiore per gestire il transiente
- queste possono essere istanziate **anche dinamicamente**, tramite zabbix
- attive immediatamente se i record MX per i nuovi nodi sono gia' configurati

Da verificare l'impatto sul sistema antispam/antivirus

# Cosa resta da fare

---

## Completare analisi

- compresa valutazione accurata del dimensionamento del traffico

## Effettuare test di reazione al carico

## Coordinarsi con i SSNN

- valutare la compatibilita' della configurazione con l'infrastruttura dei SSNN

## Definire un sistema di supporto per gli utenti

- il supporto all'inoltro della posta (senza servizio antispam/antivirus) non e' molto pesante (frazione di fte)
- ma si devono definire delle persone preposte a controllare ed operare sul sistema che possano intervenire con rapidita'

# Tempistica

---

Un mese di lavoro per rifinire la configurazione e testare il sistema

- ma da trovare in un periodo intenso di impegni

Il vero problema e' definire un SLA e identificare persone che forniscano il supporto

- problematica **non ancora affrontata** dal gruppo mailing

Ricordiamo che la posta e' percepita come servizio critico dagli utenti

- da qui discende la necessita' di non offrire un servizio a tutta l'utenza INFN senza avere definito un supporto idoneo

---

# INFNPEC

# Numeri

---

Pannello centrale attivo (e gestibile) da febbraio 2016

232 caselle (~ 900 euro/anno), **8 nuove caselle**

tempo di attivazione medio < 1 gg (dopo fase di assestamento)

richieste di supporto: **26**

backpec stabile:

- 165 utilizzi, 1 failure, 2 casi di recupero mail perse
- 45 GB utilizzati su 5 TB disponibili

Il servizio a regime richiede **poche risorse**

# Documentazione

---

Prodotta documentazione su Alfresco

- Configurazione client
- Configurazione della casella PEC (filtri antispam)
- Consigli per gestire lo spazio disponibile

Una buona documentazione abbatta le richieste di supporto

# Da fare

---

Definire la procedura per la rimozione delle caselle dei RUP

- Essenzialmente sapere da Agid (o ANAC) se, e **dopo quanto tempo** sia possibile rimuovere una casella
- Va chiarito con AC chi debba informarsi: questione già accennata, ma rimasta appesa.

Definire da chi e quando possano essere richieste nuove caselle

- In particolare per caselle istituzionali (serve **registrazione all'IPA** per i punti di protocollazione)
- Abbiamo **prodotto un documento** sottomesso a Simona Fiori tempo fa, ma senza risposta
- Questo è da fare quanto prima, ora c'è confusione tra utenti e amministrazioni