Servizio mailing nazionale

A.Brunengo e M.Corosu

Gruppo Mailing di CCR

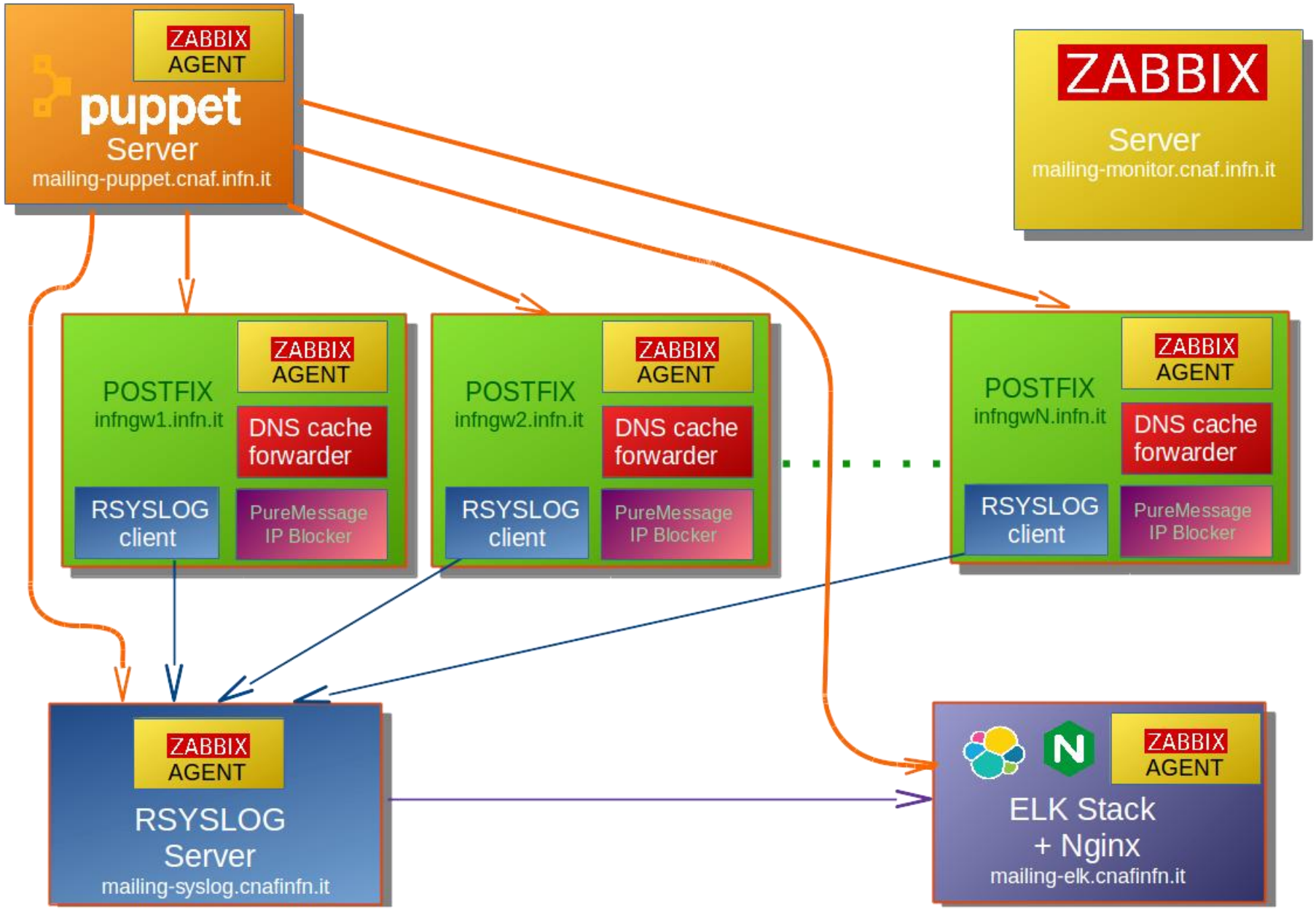
Workshop CCR
Gran Sasso 2017

Sommario

- Punto sulla situazione del nuovo sistema di server smtp per il dominio infn.it ed MX backup per *.infn.it
- Nuova applicazione di registrazione degli indirizzi @infn.it

Situazione al mini-WS di Aprile

- Nuovo sistema di MX server per il dominio **infn.it** e backup per i domini di sezione:
  - Scalabile in modo semplice e veloce in condizioni di carico eccessivo (**VM + Puppet**)
  - Introdotto un filtro preliminare per ridurre il numero di messaggi indesiderati (**Sophos IPBlocker via Puppet**)
  - Introdotti alias <UID>@infn.it per tutti (**build_aliases, software sviluppato ad-hoc**)
  - Servizi di monitoring e statistica (**Zabbix ed ELK**) stack)


ZABBIX
AGENT
puppet
Server
mailing-puppet.cnaf.infn.it
ZABBIX
Server
mailing-monitor.cnaf.infn.it
POSTFIX
infngw1.infn.it
ZABBIX
AGENT
DNS cache
forwarder
RSYSLOG
client
PureMessage
IP Blocker
POSTFIX
infngw2.infn.it
ZABBIX
AGENT
DNS cache
forwarder
RSYSLOG
client
PureMessage
IP Blocker
POSTFIX
infngwN.infn.it
ZABBIX
AGENT
DNS cache
forwarder
RSYSLOG
client
PureMessage
IP Blocker
ZABBIX
AGENT
RSYSLOG
Server
mailing-syslog.cnafinfn.it
N
ZABBIX
AGENT
ELK Stack
+ Nginx
mailing-elk.cnafinfn.it

Modalita' operativa

- Pensato per essere gestito in collaborazione:
  - Ogni macchina e' accessibile e puo' essere gestita da sedi diverse attraverso utenze amministrative (sudoers)
  - attualmente abilitate alcune utenze del gruppo mailing e dei SSNN
- Tutto il codice sviluppato (moduli puppet, script di gestione, ecc...) risiede sul repository nazionale GitLab https://baltig.infn.it/mailing
- Tutta la documentazione tecnica viene creata sul wiki nazionale http://wiki.infn.it/cn/ccr/mailing/home

Implementazione

- I server MTA sono fisicamente collocati al CNAF e a Genova; possono essere messi in qualsiasi sezione INFN ma non migrare da un sito all'altro
- L'alta affidabilita' e' garantita dalle caratteristiche del protocollo SMPT
- I sistemi ancillari non sono in HA
- I dettagli relativi all'implementazione sono raccolti nella presentazione del mini worshop CCR di Aprile (vedi slide su Indico)

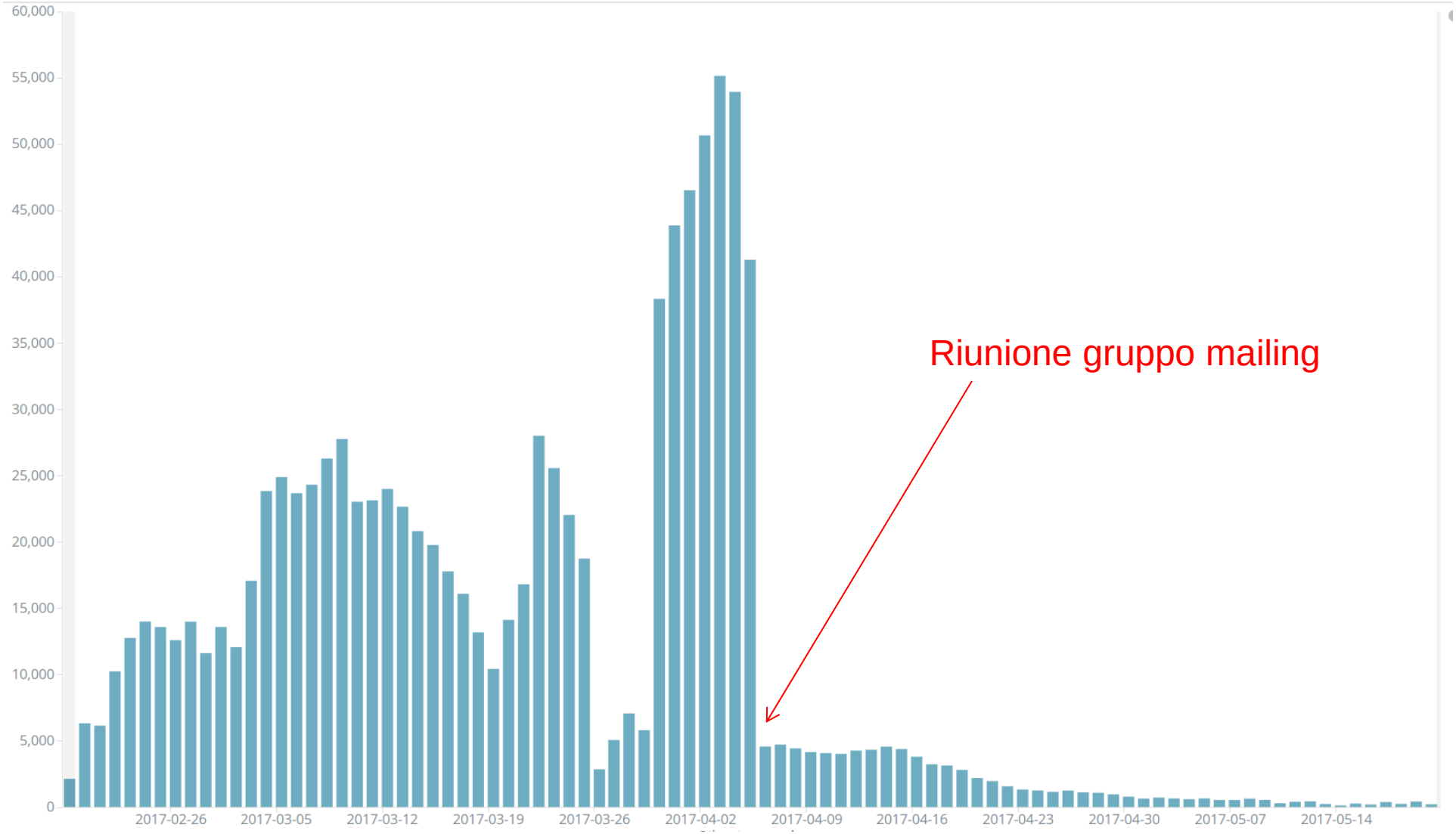
Lavoro svolto dall'ultimo WS

- Syslog server e client configurati per inviare e ricevere dati cifrati (rsyslog8.x + TLS)
- Le notifiche di Zabbix vengono inoltrate anche via Rocket.Chat

  - L'allarmistica utilizza il sistema in produzione ai SSNN del CNAF https://chat.infn.it
  - Creato un canale privato dedicato (#mailing_alert), associato a tutti gli amministratori del mailing

- Dismissione del servizio di MX backup per le sedi
  - E' possibile riconfigurare rapidamente il servizio di backup, a richiesta, in caso di necessita'

Diminuzione del backscattering



Meccanismo di creazione alias

- L'attivazione di alias <uid>@infn.it viene realizzata in modo automatizzato da build_aliases
  - tool sviluppato ad hoc, in python
  - legge l'LDAP di AAI, filtra le entry (ruoli, esistenza di indirizzi @*.infn.it, …) e crea gli alias
- build_aliases viene eseguito in cron sul server puppet ogni 30 minuti
  - modifica i file di configurazione degli MTA
  - update della configurazione sugli MTA via puppet ogni 5 minuti
- Si opera solo in append
  - scomparsa di entry precedentemente registrate viene loggata, per rimozione manuale
- Attualmente definiti 9800 alias

Alias estesi

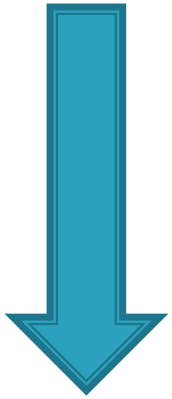
- L'esigenza e' legata ad una richiesta specifica del management (vecchia di anni, reiterata recentemente)
  - a suo tempo implementata manualmente per poche utenze
- La nuova configurazione degli MTA centrali permette di implementare gli alias estesi su una infrastruttura affidabile
  - si puo' estendere la funzionalita' a tutti gli utenti dell'Ente
- L'alias esteso arricchisce la funzionalita' di indirizzamento @infn.it
  - localmente gli utenti utilizzano prevalentemente alias estesi

Attivazione “on demand”

- Problema delle collisioni
  - non ha soluzione automatica soddisfacente, per l’impossibilita’ di definire criteri di priorita’ non opinabili
- Si e’ deciso di optare per una attivazione a richiesta:
  - l’utente si collega su una web interface e sceglie il proprio indirizzo esteso
  - scelta limitata ad opzioni proposte dalla interfaccia
  - le opzioni generate in base a attributi presenti in AAI
    - nome e cognome (e composizioni/contrazioni varie)
    - alias estesi utilizzati in indirizzi locali
  - solo un alias esteso per utente

Alias estesi: criticita’

- Alcune sedi definiscono UID del tipo <nome>.<cognome> (Pr, Cs, Sa)
  - Si devono evitare collisoni tra alias estesi e UID
- Sono stati implementati questi meccanismi:
  - ogni alias esteso creato viene registrato in AAI (nell’attributo mailAlternateAddress dell’entry nel ramo nazionale
  - svluppata apposita API di Godiva, usata da build_aliases
- l’algoritmo di selezione di UID per ogni nuova registrazione in AAI (TRYADD) effettua un controllo di univocita’ anche sulla parte user di tutti gli indirizzi @infn.it registrati nelle entry del ramo nazionale
- Modifiche implementate grazie alla collaborazione con il gruppo AAI



Alias <uid>@infn.it

Utilizzo degli indirizzi @infn.it

- Utilizzo in ricezione: non ci sono problemi
- Utilizzo come mittente: questo ha comportato una analisi piu' approfondita su:
  - autenticazione SPF e DKIM
  - mailing list chiuse
  - firma digitale e encription delle mail
    - serve un certificato con il nuovo indirizzo mail

Autenticazione SPF e DKIM

- Autenticazione SPF:
  - il destinatario cerca nel DNS un record SPF associato al dominio del campo From (infn.it)
    - non e' possibile creare un record SPF che includa tutti gli outgoing mail server delle sedi
      - limiti (da RFC) sulla lunghezza del record (~460 caratteri) e sul numero di risoluzioni DNS che la verifica comporta (10 query)
  - si e' deciso di non registrare un record SPF per il dominio infn.it: il risultato del check (none) non deve (da RFC) comportare alcuna decisione negativa sulla mail
- Autenticazione DKIM:
  - DKIM supporta un campo ('d') nella signature che indica il dominio di riferimento su cui verificare la firma, indipendentemente dal campo From, quindi non ci sono problemi

Mailing list chiuse

- Il cambio di indirizzo non permette piu' di scrivere mail a liste chiuse, in cui e' registrato il vecchio indirizzo
- Si deve modificare la registrazione nelle liste (o aprire la lista ad invii da *@infn.it)
  - per le liste gestite dal list server nazionale si puo' pensare ad una soluzione automatizzata, o gestibile dall'utente
    - discussone in corso con i SSNN
  - per le liste di sede, e' necessario il coinvolgimento del servizio calcolo locale
  - per le liste esterne, e' necessario chiedere all'amministratore della lista
- Queste modifiche di configurazione non possono essere rese trasparenti all'utente, che deve operare su liste
  - a volte non si sa nemmeno a quali liste si appartiene, ne' la loro eventuale policy di submission

Firma/encription delle mail

- Serve un certificato nuovo:
  - certificato INFN-CA: la policy della CA impedisce di avere due certificati diversi con lo stesso subject
    - modificare il subject ha conseguenze per chi utilizza la grid
    - non modificarlo implica la richiesta di revoca del certificato vecchio e l'emissione di un unovo certificato (lavoro per l'utente e per le RA)
  - certificato Terena: opzione apparentemente migliore (richiesta autonoma e semplice)
    - ma la web interface di richiesta (Digicert) offre un certificato con l'e-mail dell'attributo 'mail' di AAI, che quindi va prima cambiato

Preferred mail in Godiva

- Implementato in godiva il concetto di preferred mail address
  - determina il contenuto dell'attributo mail dell'entry nazionale di AAI
- Selezionabile tramite apposita API
  - l'API richiede autenticazione con certificato autorizzato
  - in assenza di una selezione esplicita, il contenuto dell'attributo mail e' definito dal vecchio algoritmo
  - la selezione del preferred mail viene propagata nell'LDAP di AAI ogni 30 secondi
- Va effettuata una analisi quanto piu' ampia possibile sui SP per verificare che tale modifica non generi disservizi (vedi dopo)

Sistema di selezione degli alias

- L'interfaccia web di selezione dell'alias esteso e' ora disponibile sui sistemi in produzione
  - l'interfaccia utilizza l'API di Godiva e registra la scelta dell'utente
- Il sistema e' raggiungibile all'indirizzo https://mailing.infn.it
- Stile Material-Design (Materialize Framework) ottimizzato per sistemi mobile.


INFO
ATTIVA IL TUO ALIAS NAZIONALE ESTESO
. Enrico Fasanelli (uid: enrico)
I tuoi indirizzi di posta elettronica
Indirizzo di posta elettronica principale
enrico.m.v.fasanelli@le.infn.it
Alias nazionali attivi
enrico@infn.it
Indirizzi o alias di posta elettronica locali
enrico@roma1.infn.it
enrico.m.v.fasanelli@roma1.infn.it
emvf@lnf.infn.it
enrico.maria.vincenzo.fasanelli@lnf.infn.it
enrico.m.v.fasanelli@le.infn.it
enrico@le.infn.it
enrico.mv.fasanelli@le.infn.it
enrico.fasanelli@le.infn.it
fasanelli@le.infn.it

ATTIVA IL TUO ALIAS NAZIONALE ESTESO | SCEGLI IL TUO INDIR

Seleziona un alias tra quelli proposti

Un alias esteso e' un indirizzo di posta nazionale del tipo nome.cognome@infn.it. Puoi attivarne uno scegliendolo tra i seguenti:

enrico.fasanelli@infn.it

enrico.mv.fasanelli@infn.it

enrico.m.v.fasanelli@infn.it

enrico.maria.vincenzo.fasanelli@infn.it

vincenzo.fasanelli@infn.it

ATTIVA IL TUO ALIAS NAZIONALE ESTESO | SCEGLI IL TUO INDIRIZZO PRINCIPALE

Seleziona un indirizzo tra quelli proposti

Puoi scegliere di ultilizzare un indirizzo di posta nazionale (@infn.it) selezionando il tuo indirizzo principale tra i seguenti:

enrico@infn.it

enrico.fasanelli@infn.it

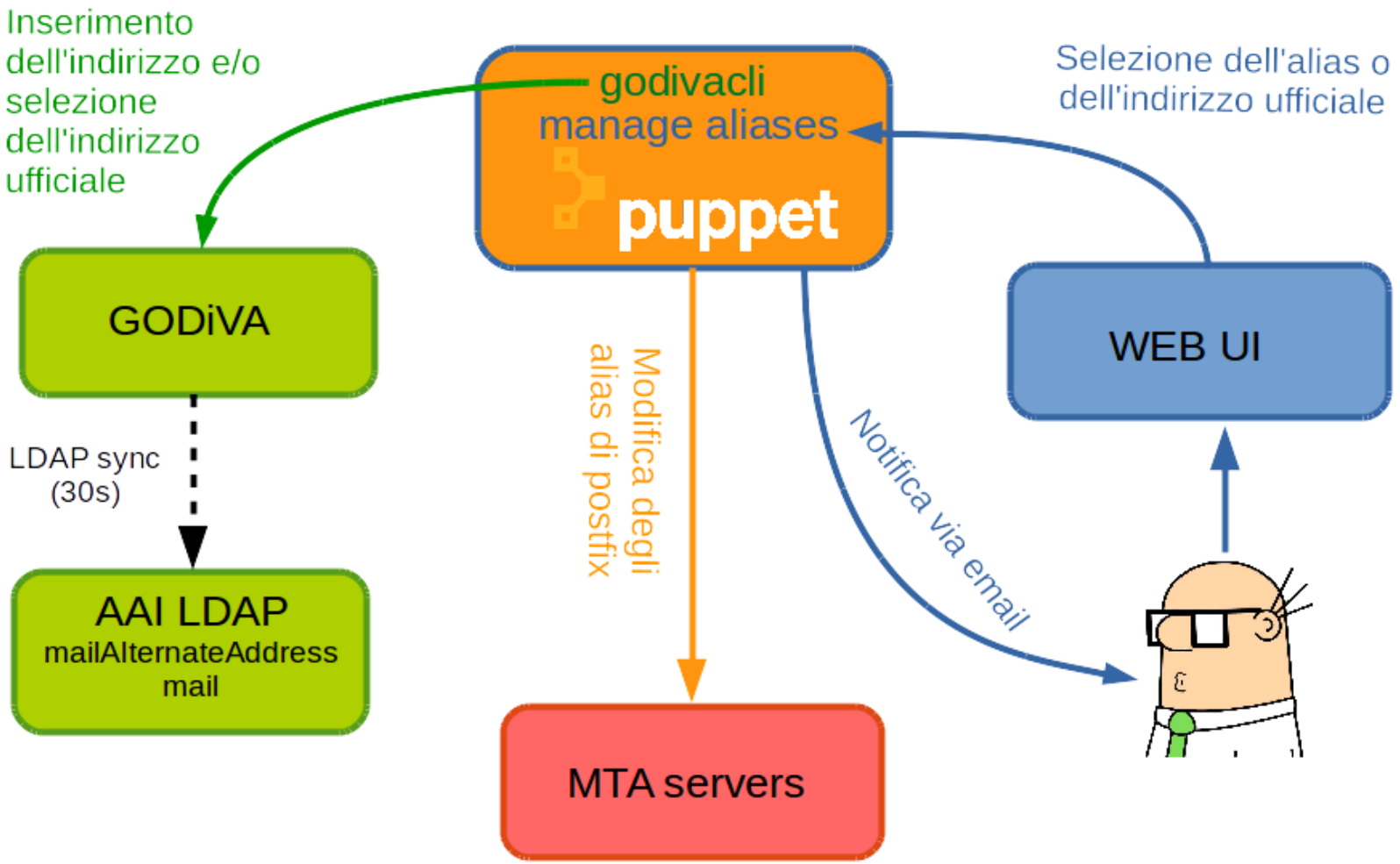
enrico.mv.fasanelli@infn.it

enrico.m.v.fasanelli@infn.it

enrico.maria.vincenzo.fasanelli@infn.it

vincenzo.fasanelli@infn.it

Workflow


Inserimento dell'indirizzo e/o selezione dell'indirizzo ufficiale
godivacli manage aliases
puppet
Selezione dell'alias o dell'indirizzo ufficiale
GODiVA
WEB UI
LDAP sync (30s)
Modifica degli alias di postfix
Notifica via email
AAI LDAP
mailAlternateAddress
mail
MTA servers

Impatto sui servizi calcolo locali

- L'utilizzo in ricezione non ha impatto sui servizi locali
- L'utilizzo in invio comportera' richieste di supporto:
  - assistenza nella riconfigurazione dei mail client
    - dovrebbe essere mitigata dalla documentazione disponibile sul sito wiki http://wiki.infn.it/cn/ccr/mailing/users
    - date feedback anche su questa
  - operazioni sulle liste locali
    - si puo' automatizzare in modo analogo a quanto fa sympa
  - richieste di supporto connesse a eventuali malfunzionamenti di alcuni SP
    - l'analisi del beta test dovrebbe aiutare a scremare i problemi principali
- Puo' essere mitigato, ma non e' un cambiamento trasparente, come non e' trasparente per l'utente
  - il carico sui servizi dipende da quanti sceglieranno di modificare l'indirizzo utilizzato nel campo "From", e soprattutto da quanti avranno necessita' di un certificato con il nuovo indirizzo

Si parte…

- Fase di test per analizzare gli effetti della modifica del campo “mail” di AAI sul piu' alto numero possibile di SP (servizi nazionali, locali e altri)
  - il personale della CCR e dei servizi calcolo sono invitati a collaborare come beta tester per dare feedback
- Da fare prima della diffusione al grande pubblico:
  - Implementazione della modifica automatica delle mailing list nazionali
    - discussione in corso con i SSNN

Credits

- Hanno collaborato in modo determinante:
  - il gruppo mailing : progettazione ed analisi delle problematiche
  - il personale dei Servizi Nazionali (Longo, Antonelli, Pezzi): setup della infrastruttura
  - il gruppo AAI: analisi delle problematiche connesse all'utilizzo degli indirizzi, implementazione di estensioni in Godiva (Fasanelli, Bisegni, Serafini)

Conclusioni

- Il lavoro sul sistema di MX server per infn.it e' stato finalizzato. Il servizio e' pronto per la produzione

- L'interfaccia per la selezione del proprio indirizzo @infn.it e' raggiungibile al link https://mailing.infn.it
  - Per ora tutti gli appartenenti a CCR ed al gruppo mailing hanno accesso e sono incoraggiati a fare da beta tester


thank you!