Gruppo Mailing Report

Alessandro Brunengo, per il gruppo Mailing

Attivita' in corso

- Stato migrazione e supporto per le caselle PEC
- Analisi delle tecniche di lotta contro lo spam nelle sedi
- Mail relay secondario nazionale infngw2
- Indirizzi di posta @infn.it

Stato migrazione e supporto per le caselle PEC

Pannello centrale Aruba

- Pre-contrattazione lunga (luglio-ottobre) per definire
  - procedura e costi di migrazione
  - aggregazione dei pannelli di gestione delle diverse sedi
- Ordine del 9/10/2015
- Pannello disponibile il 21/12/2015, operativo l'11/01/2016
  - caselle registrate: 153 su 6 domini (due infn)
  - credito disponibile: 1766.56 €
- Non aggregate le caselle di Roma1
  - procedura complessa: deciso di rimandare

Migrazione dominio @pec.infn.it

- Da migrare 63 caselle (quasi tutte istituzionali)
- Aruba ha creato le caselle di posta (non certificate) ed attivato la copia dei messaggi automatica per preparare la migrazione
  - caselle gia' accessibili, ma da non utilizzare fino a certificazione del dominio
  - verificata l'accessibilita' delle caselle ed il contenuto (per Genova)
- Postecom ha ricevuto la richiesta di disdetta in data 23/02/2016
  - devono contattare l'amministratore delle caselle
  - lenta e farraginosa l'interazione con Postecom
- Previsione:
  - appena veniamo contattati (solleciteremo) sara' questione di 10 giorni)

Servizi di supporto alla PEC

- Backpec (accesso: **https://backpec.infn.it**)
  - utility per eseguire il backup delle caselle PEC
- Imapec (accesso: **https://imapec.infn.it**)
  - imap server per rendere disponibile la visualizzazione ed il download dei messaggi PEC salvati con Backpec
- Infnpec (accesso: **https://infnpec.infn.it**)
  - portale di accesso ai servizi di supporto per la PEC
  - richieste nuove caselle e documentazione

Struttura dei servizi

- I tre servizi sono gestiti da due VM ospitate dai sistemi dei Servizi Nazionali al CNAF
- Disponibili 5 TB di storage (thin provisioning)
- Attualmente utilizzati 32 GB (per ora utilizzato solo per caselle @pec.infn.it)
- Il tutto e' sottoposto al sistema di backup dei SSNN del CNAF
- E' a tutti gli effetti un servizio nazionale in produzione
  - Assoluta disponibilita' e collaborazione di Stefano Longo e del gruppo dei SSNN del CNAF

Backpec

- Interfaccia web di attivazione del backup (richiede una autenticazione AAI e credenziali della PEC)
- Applicativo sviluppato internamente che scarica i messaggi contenuti nella casella PEC in formato RFC822 su disco locale, e li carica su un imap server (in modo incrementale)
- Pensato inizialmente per avere backup delle caselle da migrare (ad Aurba sono sicuramente bravi, pero'…)
  - attualmente ospita il backup di 78 caselle
- Una decina di utenti lo utilizzano in produzione
  - necessita' di svuotare la propria casella PEC
  - In un caso il servizio e' gia' stato utilizzato con successo per recuperare mail perse, senza intervento del supporto

Imapec

- E’ un imap server basato su cyrus-imapd su cui vengono caricate le mail salvate da Backpec
- Rese disponibili tramite una interfaccia webmail
  - L’accesso all’interfaccia e’ regolato da una autenticazione AAI
  - Gli account hanno le stesse credenziali della casella PEC di cui ospitano la copia del backup
  - Non replica la struttura dei folder della casella PEC, ma ospita tutte le mail in un unico folder
  - L’accesso e’ in modalita’ readonly e non puo’ essere utilizzato per inviare mail
    - necessario per evitare confusione negli utenti

Infnpec

- Infnpec e' il portale di accesso ai servizi di supporto alla PEC
- Implementa una interfaccia per la richiesta di attivazione di una nuova casella PEC
  - La richiesta si traduce in una mail al supporto con tutte le informazioni necessarie
  - Basato su autenticazione AAI
    - e' possibile implementare filtri sugli attributi delle entry in AAI
- Il sito contiene anche
  - Informazioni sulle configurazioni per accedere alle caselle PEC di Aruba
  - Puntatori ai servizi Backpec e Imapec

Caselle istituzionali

- Discussione portata avanti con il responsabile del SI e con uffici della AC
  - e' argomento attuale la revisione delle caselle PEC istituzionali, legato all'inserimento della PEC nel protocollo
- Si suggerisce che la richiesta di creazione o rimozione di caselle istituzionali debba provenire direttamente dalla Direzione Generale, o da ufficio delegato
  - e' auspicabile che le persone autorizzate a fare la richiesta siano identificabili tramite opportuni attributi in AAI
    - questo permette di implementare criteri di accesso in Infnpec

Caselle per RUP

- A oggi la legge richiede che un RUP disponga di una casella PEC personale
- Si suggerisce che le nuove richieste provengano dagli uffici amministrativi o dalle segreterie di direzione delle sedi
- Caselle attuali dei RUP
  - le caselle devono essere mantenute per un lungo periodo (2 anni?) anche dopo la chiusura di una procedura di acquisto
    - possibilita' che l'ANAC chieda informazioni al RUP per periodo non definito
  - Le nuove necessita' soddisfatte da una casella @pec.infn.it
  - Si propone di mantenere attive ma inutilizzate le attuali caselle
    - da indagare la possibilita' di comunicare ad ANAC la chiusura o la modifica di indirizzo

PEC per tutti?

- Richiesta esplicita del Presidente
  - Probabilmente motivata per l'intenzione di inviare comunicazioni interne tramite PEC
- Da un approfondimento fatto con uffici della AC e secondo l'AGID, non e' necessario utilizzare la PEC per comunicazioni interne
- Non si ritiene opportuno creare caselle senza una reale esigenza
  - la creazione di una casella richiede un solo giorno lavorativo
  - e' comunque possibile attivare grandi quantita' di caselle in tempi ragionevoli, se la necessita' si dovesse presentare

Da fare

- Seguire la migrazione e fornire supporto agli utenti delle caselle migrate per utilizzare la nuova configurazione
- Proporre al management i criteri di autorizzazione a richiedere nuove caselle
  - per poter implementare tali criteri in Infnpec
- Implementazione di backup automatizzati
- Manutenzione e sviluppo di Backpec
  - bug correction
  - sviluppi minori (efficienza, gestone di errori transienti di connessione)

Supporto e Credits

- Il supporto a questi servizi si contatta unicamente via e-mail:

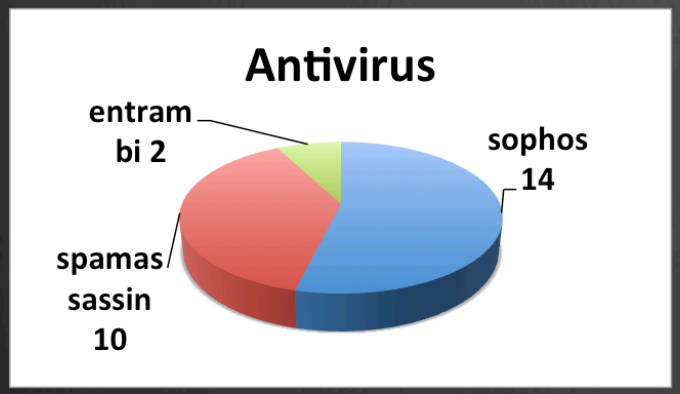
pec-support@lists.infn.it

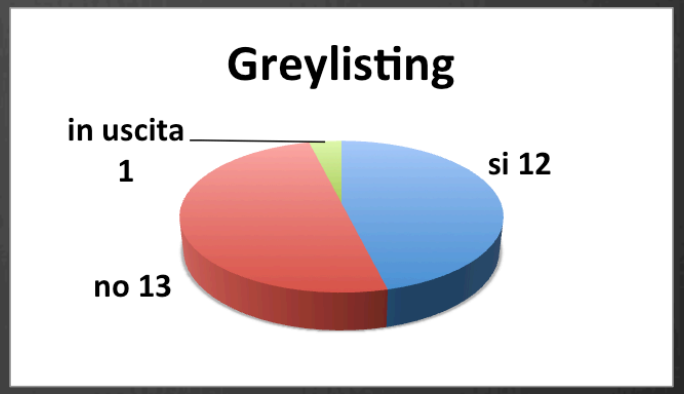
- Le utility Backpec, Imapec e Infnpec sono state sviluppate e messe in produzione da
  - Mirko Corosu
  - Stefano Longo (grande disponibilita' dei SSNN dal CNAF)
  - Alessandro Brunengo

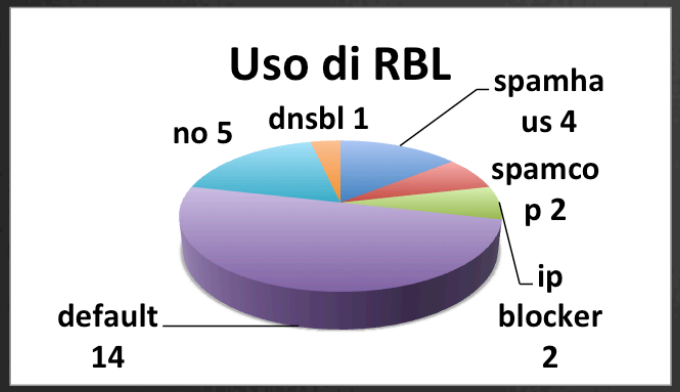
Analisi delle tecniche di lotta contro lo spam nelle sedi

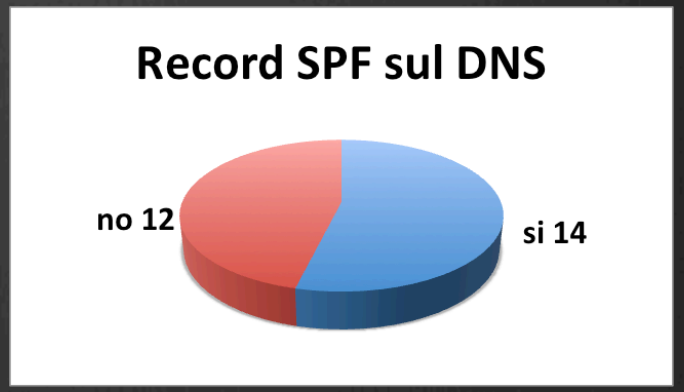
Survey sulle configurazioni

Analisi delle tecniche antispam nelle sezioni (26 risposte)









Survey: considerazioni

- Software
  - 10 sedi su 26 non usano sophos, 1 usa appliance software sophos
- Greylisting
  - meta' delle sedi non lo utlizzano
  - lamentele degli utenti in 7 sedi
    - 4 sedi le hanno rimosse, una in procinto di farlo
- RBL (realtime blackhole list)
  - 7 sedi hanno una configurazione specifica
  - IP blocker utilizzato in sole 2 sedi
    - sophos consiglia di utilizzarlo a livello di MTA
- pubblicazione di informazioni SPF
  - solo 12 sedi pubblicano informazione SPF
  - comunque poco utilizzato a livello di filtro

Greylisting

- Basato su RFC 821 e (soprattutto) successive modifiche (2129, 5321)
  - RFC 821 dice che in caso di failure il sender ‘should retry’…
- Il relay riceve una mail e memorizza la tripla (sender-ip, envelope-sender-address, envelope-recipient-address)
- Rigetta la mail, con un messaggio di temporary failure, specificando dopo quanto riprovare
- Quando una mail ha una tripla corrispondente ad una precedentemente memorizzata, la accetta e mette la tripla in autowhite list
- Vari parametri di configurazione per la temporizzazione
  - tempo suggerito (e minimo!) per il retry
  - tempo massimo di permanenza in autowhite list
  - tempo massimo di permanenza in attesa di verifica

Vantaggi del greylisting

- La maggioranza dello spam viene inviato utilizzando sistemi che non osservano del tutto le specifiche degli RFC (*)
  - in occasione di una failure, anche temporanea, questi sistemi in genere non riprovano
- L'applicazione del greylisting limita di molto le mail ricevute e trattate dagli MX locali
  - minore consuno di risorse sui sistemi locali
  - minore numero di spam che passa i successivi filtri (*)

(*) sicuramente vero un tempo, ora da verificare

Problemi del greylisting

- Benche' sia perfettamente lecito secondo gli RFC, crea alcuni problemi:
  - ritardo artificiale di delivery
    - l'entita' del ritardo dipende dalla configurazione delll'MTA remoto e puo' arrivare fino a diverse ore
    - la posta non e' un servizio a consegna istantanea, ma in diversi casi si assume che sia piu' o meno cosi' (procedure automatizzate di cerazione account o reset password, ad esempio)
  - MTA remoti che non osservano strettamente gli standard
    - possono non riprovare e prendere il temorary failure come permanent failure
    - MTA remoti costituiti da farm possono ritentare l'invio da nodi con IP differenti, e non necessariamente sullo stesso segmento di rete
    - In entrambi i casi si arriva al mancato recapito della mail

Mitigazione dei problemi

- Esistono diverse opzioni di configurazione per mitigare il problema
  - white list (tipicamente applicate per siti come Google o MS)
  - dilatazione del tempo di permanenza in autowhitelist (riduce la frequenza di intervento su una tripla)
  - parametro ‘subnetmatch /24’: il confronto per il match della tripla viene fatto non sull’IP, ma sulla subnet dell’IP
  - parametro ‘lazyaw’: mette in autowhitelist l’IP del mittente, e non la tripla
  - diversi criteri di bypass (SPF, meccanismi di autenticazione, …)

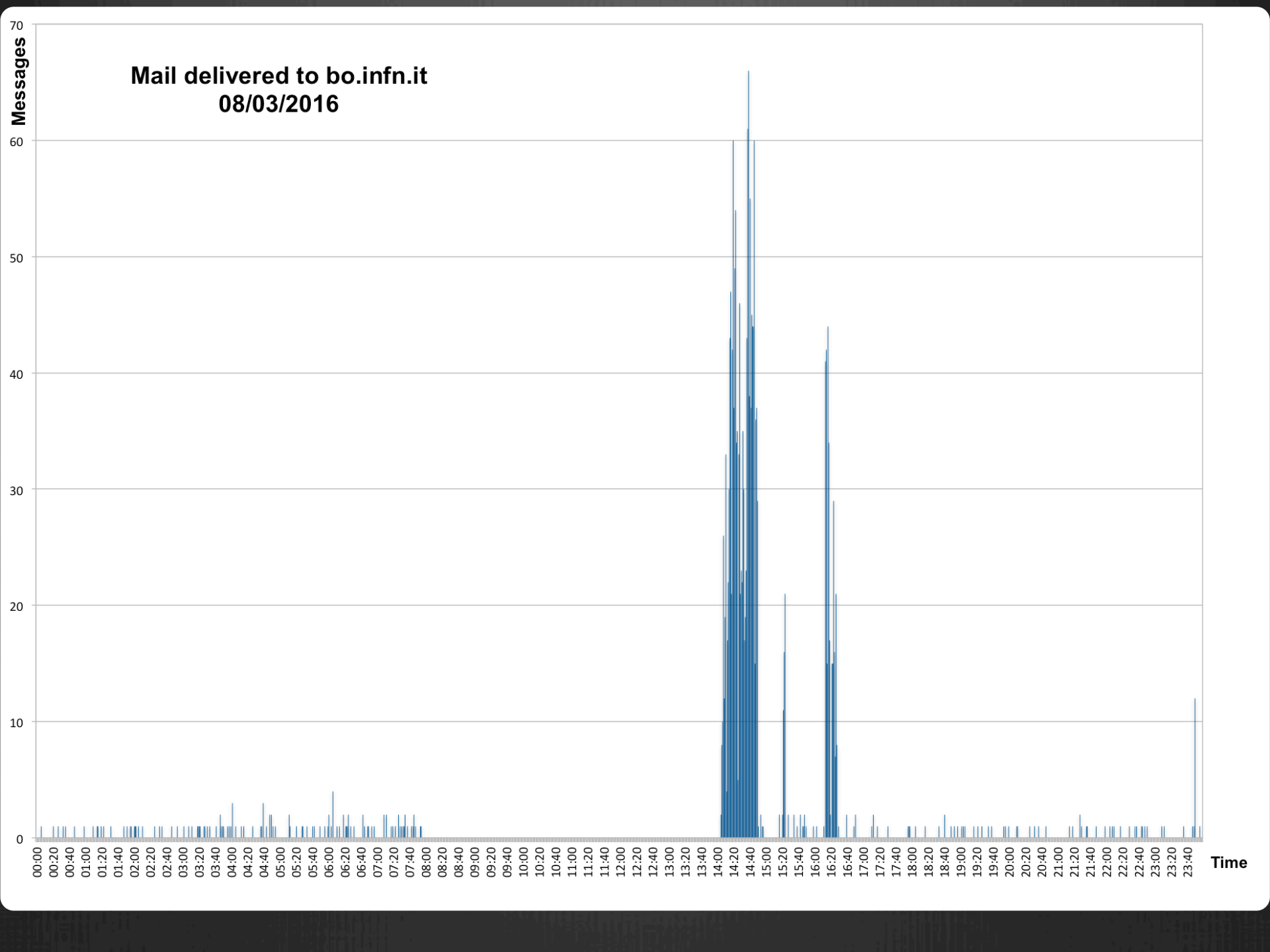
Greylisting: to do

- Analisi richiesta al gruppo in seguito a alcune lamentele
  - puo' essere uno stimolo a verificare e migliorare la propria configurazione
- Il gruppo mailing si propone di valutare (nelle prossime settimane):
  - reale impatto negativo del greylisting
    - percentuale di intervento del greylisting
    - valutazione dei ritardi
  - reale efficacia del greylisting
    - i server hanno risolrse limitate che rendono necessaria l'applicazione di un prefiltro per limitare le mail da trattare?
    - i filitri antispam sono in grado di filtrare con pari efficienza senza greylisting?
- La prima valutazione va fatta sui log file dei siti che usano il greylisting
- La seconda e' piu' complessa: ci sono alcune alcune opzioni per fare questa analisi: honeypot, o attivazione/disattivazione su sistemi in produzione (piu' semplice da implementare ed affidabile)

Mail relay secondario nazionale infngw2

Fase di test completata

- Hardware acquistato nel 2015, ma consegnato danneggiato
  - Sostituzione avvenuta a meta' dicembre 2015
  - E' stato necessario fare la prima installazione e configurazione su hardware temporaneamente disponibile
- Installazione e configurazione iniziale come relay secondario dei domini di sezione
  - OS: FreeBSD, storage: 200 GB su ZFS
  - Nella fase di test configurato come MX secondario dei domini bo.infn.it, cnaf.infn.it, ge.infn.it che hanno fatto da cavia
    - record MX con stessa priorita' di infngw.infn.it
- Fase di test completata con successo
  - verificata funzionalita' operativa l'8 marzo in occasione di riconfigurazioni dei mail relay della sezione di Bologna


Mail delivered to bo.infn.it
08/03/2016
Messages
70
60
50
40
30
20
10
0
Time
00:00
00:20
00:40
01:00
01:20
01:40
02:00
02:20
02:40
03:00
03:20
03:40
04:00
04:20
04:40
05:00
05:20
05:40
06:00
06:20
06:40
07:00
07:20
07:40
08:00
08:20
08:40
09:00
09:20
09:40
10:00
10:20
10:40
11:00
11:20
11:40
12:00
12:20
12:40
13:00
13:20
13:40
14:00
14:20
14:40
15:00
15:20
15:40
16:00
16:20
16:40
17:00
17:20
17:40
18:00
18:20
18:40
19:00
19:20
19:40
20:00
20:20
20:40
21:00
21:20
21:40
22:00
22:20
22:40
23:00
23:20
23:40

Prossime attivita'

- Configurazione infngw2 su hardware definitivo
  - programmato entro meta' aprile
- Sincronizzazione della configurazione con infngw
  - mail relay per indirizzi nel dominio infn.it (fine aprile)
- Automazione per il mantenimento della sincronizzazione dei due relay
  - inizialmente mantenimento manuale, con meccanismo automatico di notifica di configurazioni differenti (fine aprile)
- Quando queste fasi saranno terminate, potra' essere configurato dalle sedi come secondario per il proprio dominio assieme a infngw
  - verranno inviate opportune istruzioni

Indirizzi di posta @infn.it

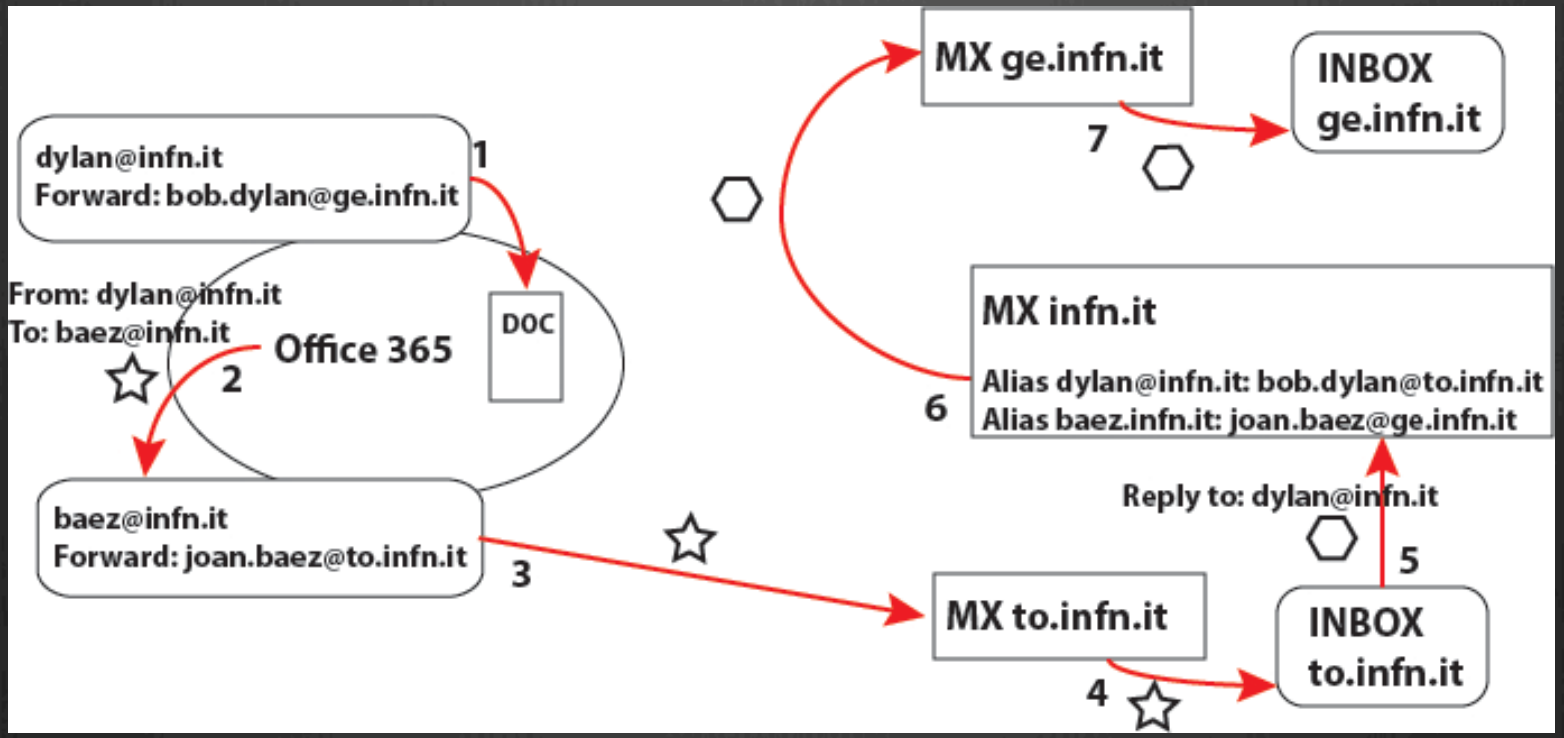
Motivazione

- L'analisi e' stata stimolata dalla esigenza di poter sperimentare Office365 secondo le modalita' desiderate dal gruppo Windows
  - aggancio con AAI
- La possibilita' di disporre di indirizzi @infn.it e' pero' indipendente dalla esigenza specifica
  - l'idea di supportare in modo ufficiale un indirizzamento @infn.it
- Si e' analizzata la fattibilita' tecnica in modalita' automatizzabile, tramite alias
- E' aperta la discussione sulla definizione dell'insieme di persone a cui assegnare un indirizzo di questo tipo
  - in funzione di attributi in AAI

Indirizzamento per sperimentazione Office365

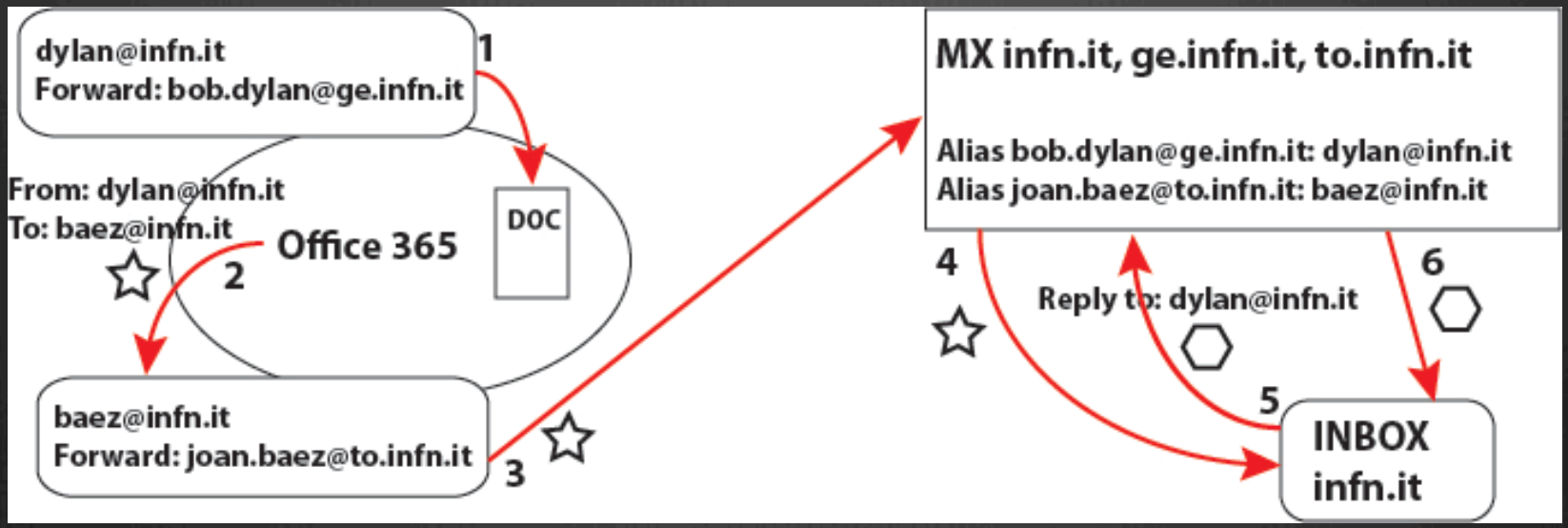
- Requisiti per Office365
  - Account del tipo <qualcosa>@<dominio>
  - Office365 vuole gestire il dominio di posta <dominio>
  - E' possibile configurare forward automatici per gli account
- Requisiti per agganciare Office365 alla autenticazione AAI
  - Il dominio deve essere [*.]infn.it
- La scelta e' stata:
  - account Office365 in dominio infn.it, con corrispondente dominio di posta gestito dagli MX di infn.it (infngw) tramite alias
  - account del tipo <uid>@infn.it con definizione di forward automatici verso l'indirizzo di posta locale dell'utente
    - informazioni ricavabili automaticamente da AAI
  - inserimento negli MX di infn.it di alias <uid>@infn.it verso l'indirizzo di posta locale

Flusso mail attuale



1. Dylan modifica il doc
2. Office 365 manda una mail a Baez
3. Tramite fw la mail arriva a to.infn.it
4. e recapitata nella mailbox di Baez
5. Baez fa reply a dylan@infn.it
6. L'MX risolve l'alias ed inoltra a ge
7. Il reply arriva a destinazione

Flusso mail in caso di servizio di posta non distribuito



1. Ughi modifica il doc
2. Office 365 manda una mail a baez
3. Tramite fw la mail arriva a to.infn.it
4. e recapitata nella mailbox
5. Baez fa reply a ughi@infn.it
6. Il reply viene consegnato

Indirizzi <uid>@infn.it

- Realizzata una procedura di creazione automatica degli alias prendendo le informazioni da AAI
  - e' fondamentale poter disporre di un db come AAI
- Qualche problema in corso di soluzione
  - uid temporanei
  - attributi mancanti in alcune entry (mail, ruoli)
- Alias da creare in base al ruolo su godiva
  - sembra ragionevole creare un alias per tutti gli utenti che hanno una casella di posta INFN (quindi anche ospiti)
  - la limitazione di accesso a servizi licenziati deve essere fatta a livello del servizio e non di esistenza dell'alias

Tempistica

- I tempi per andare in produzione dipendono
  - definizione dei criteri di assegnazione
  - sistemazione delle poche entry inconsistenti in AAI
- Tuttavia si deve prima fare una considerazione importante
  - L'utilizzo di indirizzi @infn.it, se diffuso, spostera' il carico della posta entrante sui relay MX di infn.it
  - Questo ha un impatto sia sul carico di queste macchine, sia sulle strategie antispam, che devono essere operate in primo luogo sull'MX di frontiera
  - Ha anche un impatto sul manpower necessario a garantire un servizio che diventa critico
  - Queste analisi verranno portate avanti nelle prossime settimane

Indirizzi estetici

- Fatta una analisi sulla creazione di alias nome.cognome@infn.it
  - Collisioni: dipende dai ruoli per cui creare alias:
    - dip+ass attivi: 5778 alias, 35 collisioni
    - dip+ass+osp attivi o scaduti: 6385 alias, 43 collisioni
    - tutti i record validi: 11117 alias, 143 collisioni
- La questione e' piu' complessa rispetto a <uid>@infn.it
  - essenzialmente per il problema di collisioni
  - applicare un criterio sul ruolo crea altri problemi, anche tecnici
    - ad esempio: cosa fare quando il ruolo non e' piu' attivo?
  - la discussione e' ancora aperta, e partecipata