@unipi
centralizzazione del sistema di posta di Ateneo

Davide Vaghetti
davide.vaghetti@unipi.it

Simone Spinelli
simone.spinelli@unipi.it

Samuele Tognini
samuele.tognini@unipi.it

Workshop GARR 2014 2-4 Dicembre, Roma

WORKSHOP GARR 2014
NEXT NETWORK COSTRUIAMO IL FUTURO DELLA RETE

UNIVERSITÀ DI PISA

Agenda

- Scenario e obbiettivi
- L'infrastruttura di computing
- Il sistema
- La gestione
- Analisi dei costi
- Sviluppi futuri e possibilità

Il contesto

Il progetto @unipi nasce in un momento (2013) di riorganizzazione delle risorse IT dell'ateneo:

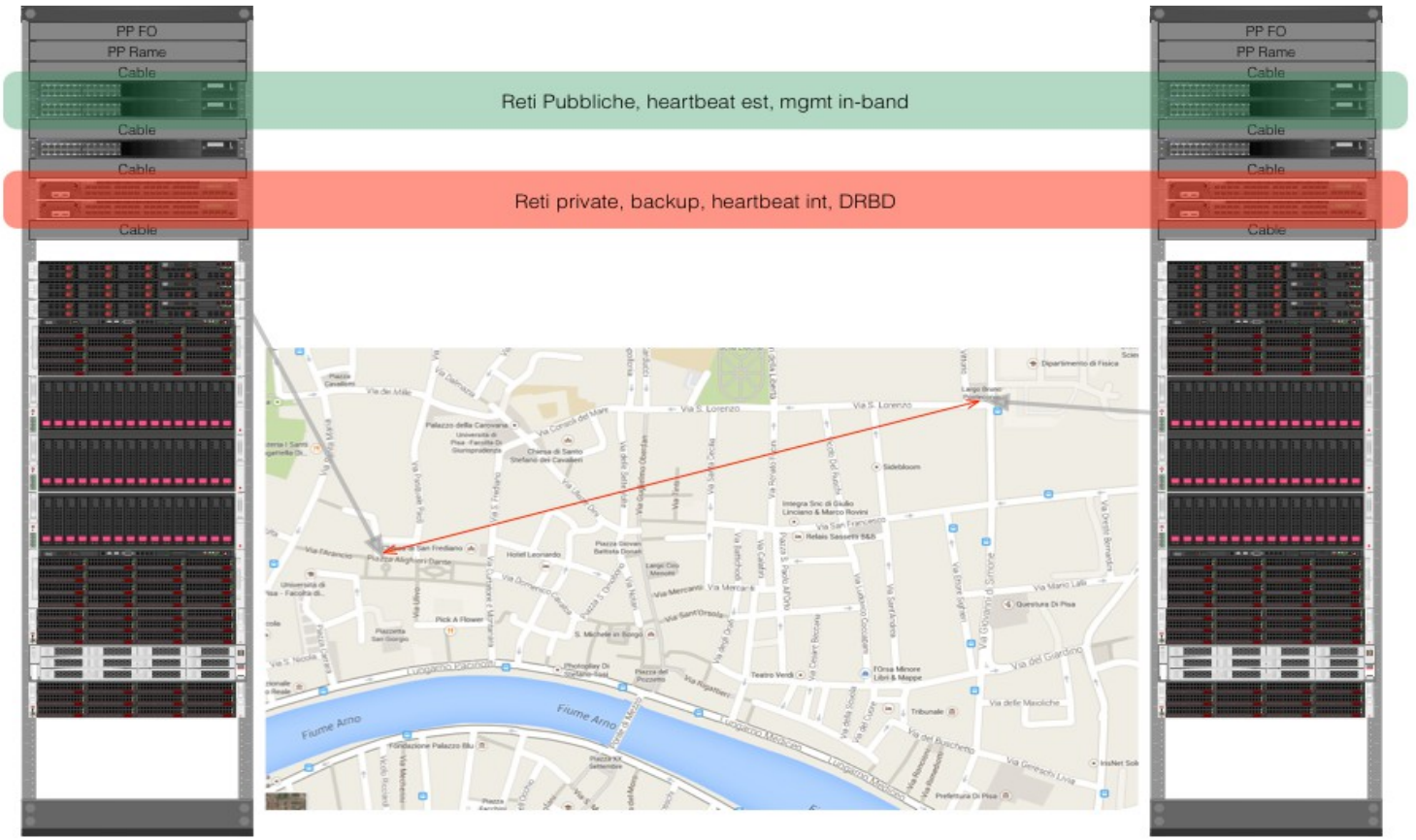
- risorse fisiche e di personale
- infrastrutture di accesso (SCA)
- server farm e servizi

In particolare, il servizio di posta elettronica veniva delegato alle singole strutture: tanti diversi flavor per lo stesso servizio.

Obiettivi

- Uniformare i livelli di servizio per tutto il personale:
  - Caratteristiche
  - Erogazione
  - Naming
- Scalabilità
- Gestione dello spam (ricezione e invio)
- Continuità Operativa e gestione del DR (Art. 50/50bis CAD)
- Valore giuridico della trasmissione (Art.45 CAD)

L'infrastruttura



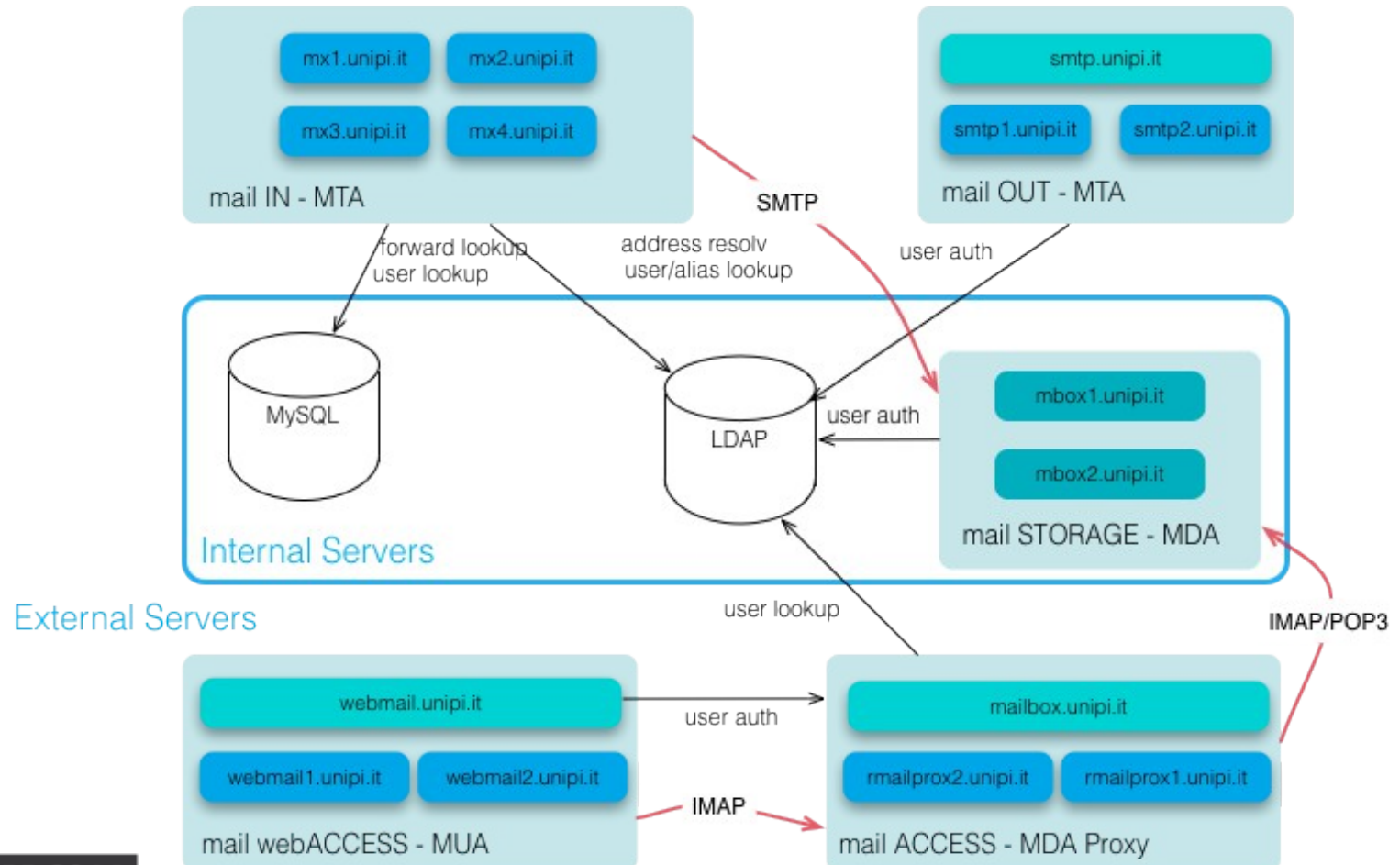
Componenti:

- Linux Debian 6.0 o sup.
- Xen 4.0 (.deb)
- DRBD 8.3
- Linux LVS
- Corosync/Pacemaker

Tipi di servizio:

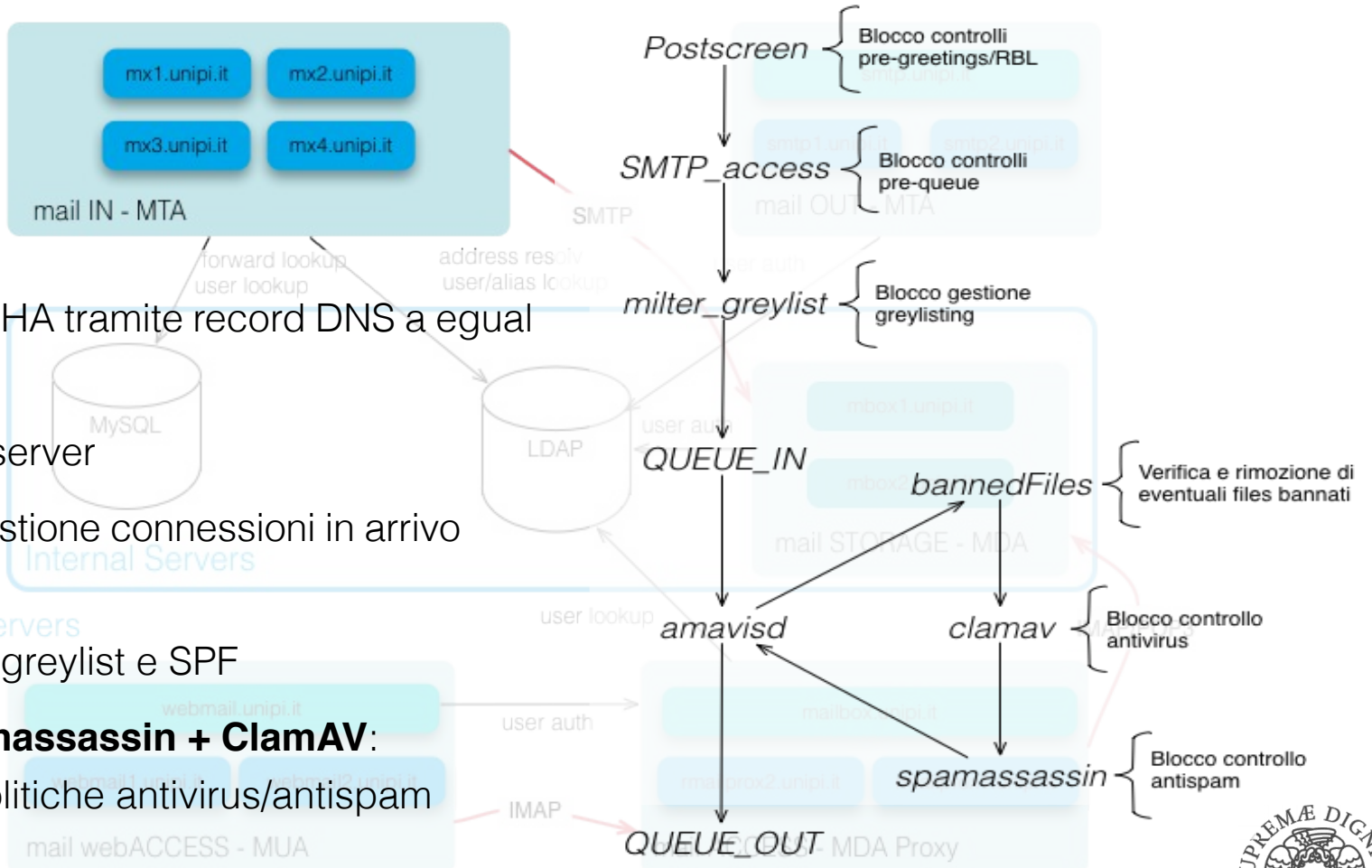
- DATA-BASED: con replica in tempo reale dei dati (es. LDAP masters, MDA server)
- DATA-LESS: senza dati a bordo (es.LDAP replica, DNS ricorsivi)

@unipi


mx1.unipi.it
mx2.unipi.it
mx3.unipi.it
mx4.unipi.it
mail IN - MTA
smtp.unipi.it
smtp1.unipi.it
smtp2.unipi.it
mail OUT - MTA
SMTP
forward lookup
user lookup
address resolv
user/alias lookup
user auth
MySQL
LDAP
user auth
mbox1.unipi.it
mbox2.unipi.it
mail STORAGE - MDA
Internal Servers
External Servers
user lookup
IMAP/POP3
webmail.unipi.it
user auth
mailbox.unipi.it
webmail1.unipi.it
webmail2.unipi.it
IMAP
rmailprox2.unipi.it
rmailprox1.unipi.it
mail webACCESS - MUA
mail ACCESS - MDA Proxy

Posta in ingresso

- **4 Xen VM** (PV): HA tramite record DNS a egual peso
- **Postfix**: SMTP server
- **Postscreen**: gestione connessioni in arrivo (pre-greeting)
- **Milter-greylist**: greylist e SPF
- **Amavis + Spamassassin + ClamAV**: applicazione politiche antivirus/antispam



Server di backend: mySQL

Bayes:

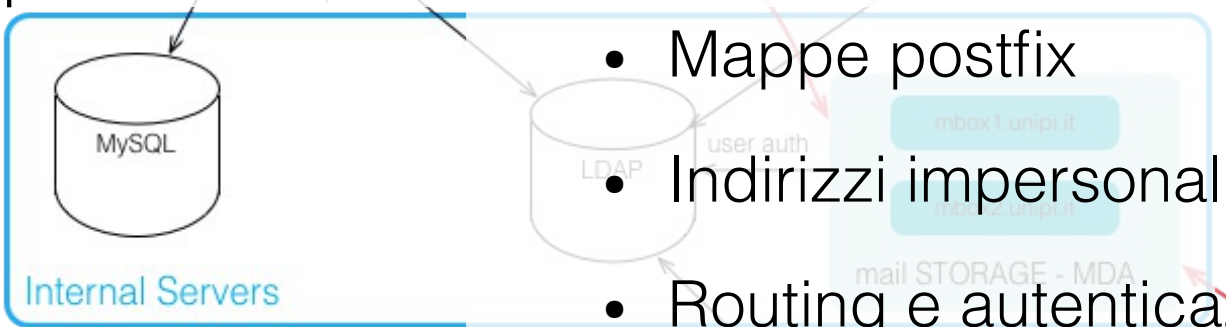
(Corosync + PerconaOCF)

- Tokens SpamAssassin

Mappe:

(MySQL replicas in reduntant loadbalancing)

- Mappe postfix
- Indirizzi impersonali
- Routing e autenticazione per utenti legacy (circa 700)



Identity Management

L'integrazione con il sistema di Identity Management di Ateneo riveste un ruolo fondamentale per il funzionamento del sistema di posta.

Sulla directory infatti si basano:

- Provisioning delle risorse
- Autenticazione
- Routing

Abbiamo utilizzato una object-class che racchiude attributi specifici per la caratterizzazione del servizio di posta elettronica.

Server di backend: LDAP

dn:
uid=a010430,dc=adm,ou=people,dc=unipi,dc=it

objectClass: unipiMail

..

cn: SIMONE SPINELLI

unipiMailAlias: s.spinelli@unipi.it

unipiMailAlias: spinelli@unipi.it

UnipiMailDovecotPlugin:

givenName: SIMONE

..

uid: a010430

..

unipiMailHost: mbox2.unipi.it

mail: simone.spinelli@unipi.it

unipiMailQuota: 20000MB

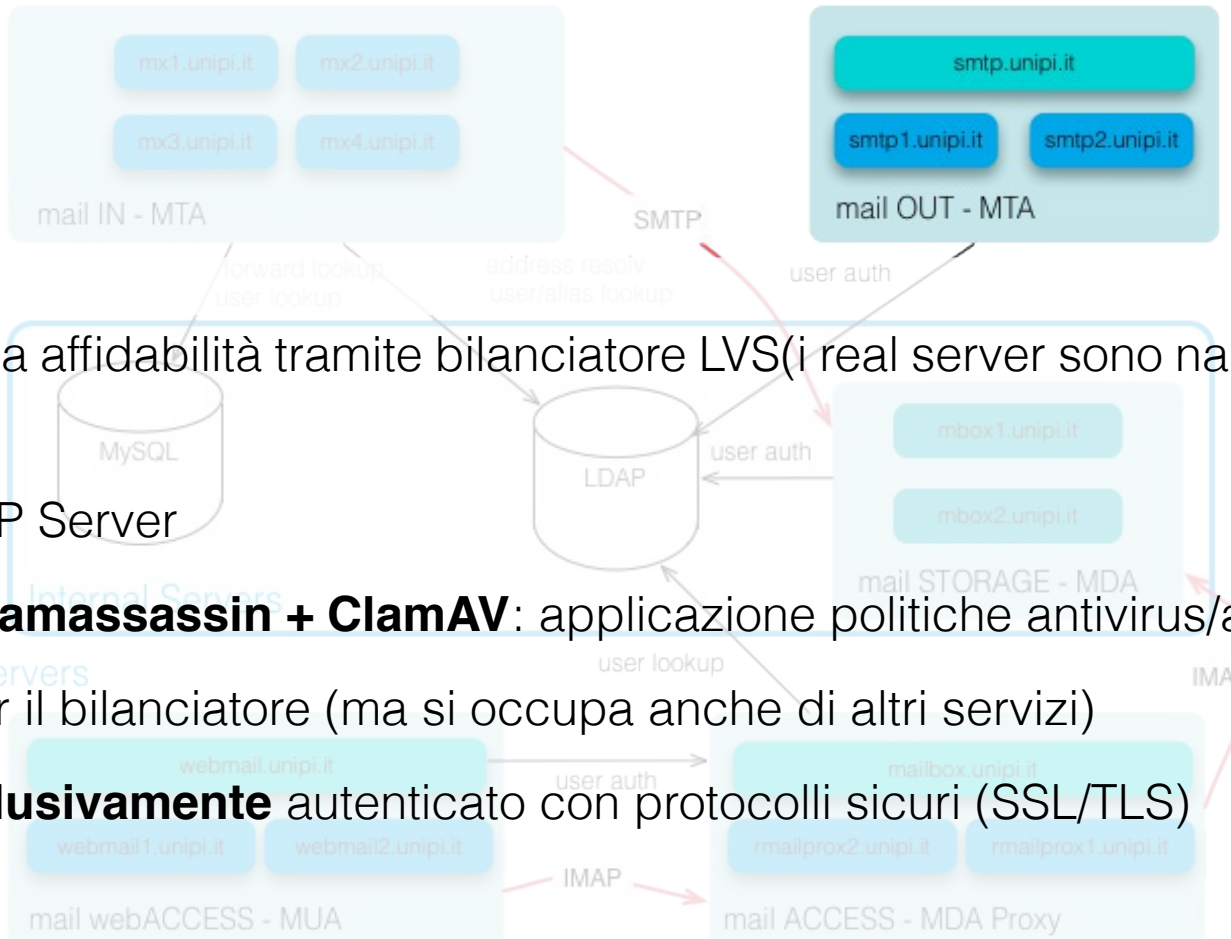
userPassword:: ----------

..

HA: Multimaster + Consumers in LB

- Indirizzi personali
- Alias personali
- Quota
- Informazioni di routing per la consegna in casella
- Autenticazione

Posta in uscita



- **2 Xen VM**: alta affidabilità tramite bilanciatore LVS(i real server sono nascosti all'utenza)
- **Postfix**: SMTP Server
- **Amavis + Spamassassin + ClamAV**: applicazione politiche antivirus/antispam
- **2 Xen VM** per il bilanciatore (ma si occupa anche di altri servizi)
- Accesso **esclusivamente** autenticato con protocolli sicuri (SSL/TLS)

Rilevamento spam

In ingresso:

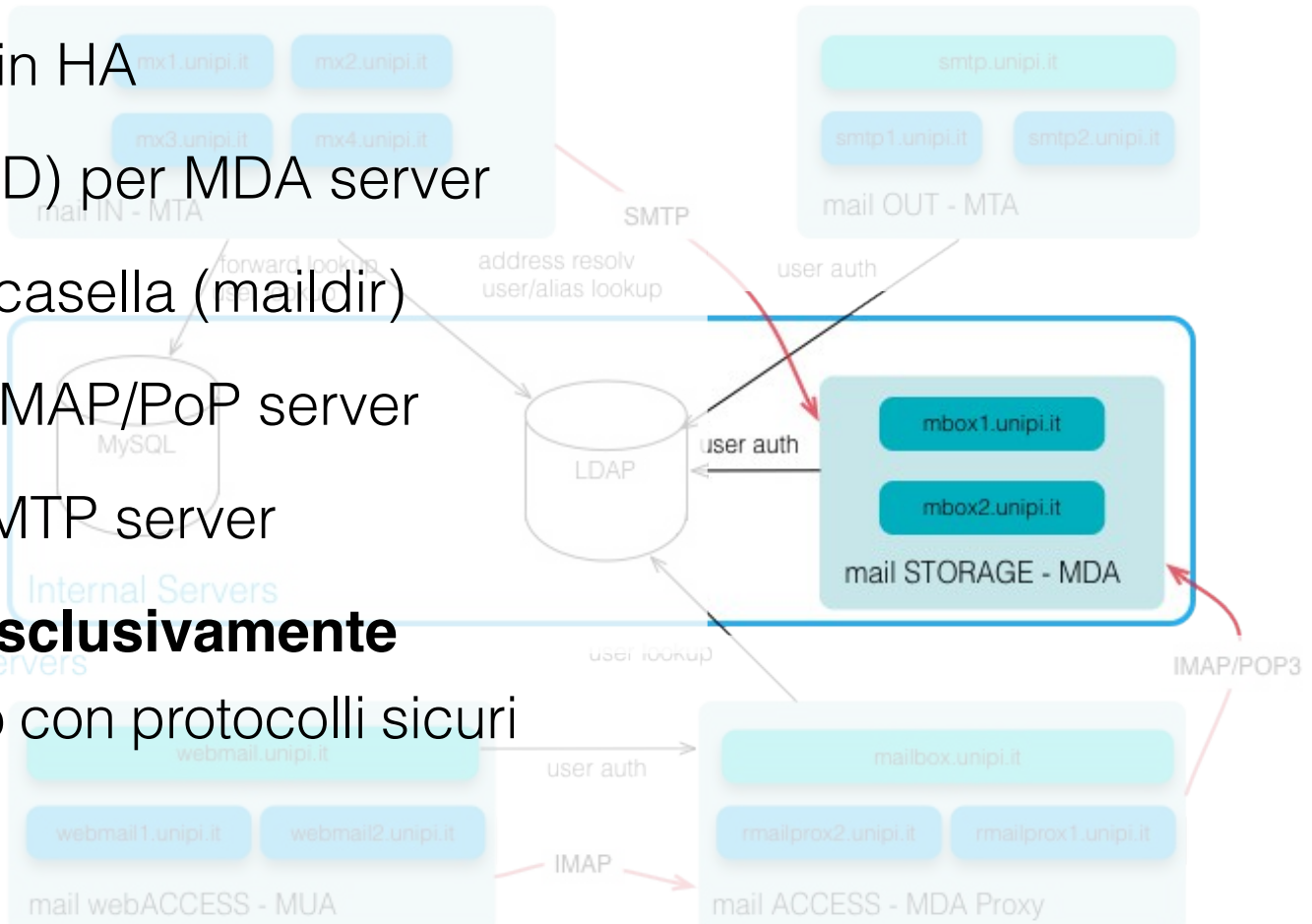
- La politica migliore è quella di far arrivare meno messaggi possibile a SA: **“Multi-Layer Defense”**
- Amavis,Clamav e SA si occupano dell'analisi **del corpo** dei messaggi
  - Soglia di blocco SA=9
  - Soglia di tag SA =5
  - Istruzione dei filtri bayesiani:
    - > 12 : SPAM
    - < 2.3 : HAM

In uscita:

- Soglia di blocco SA=6
- Avviso all'utente in caso di messaggio scartato
- L'utilizzo di regole specifiche:
  - Mitiga il backscatter
  - Aiuta nell'individuazione di account compromessi

MDA

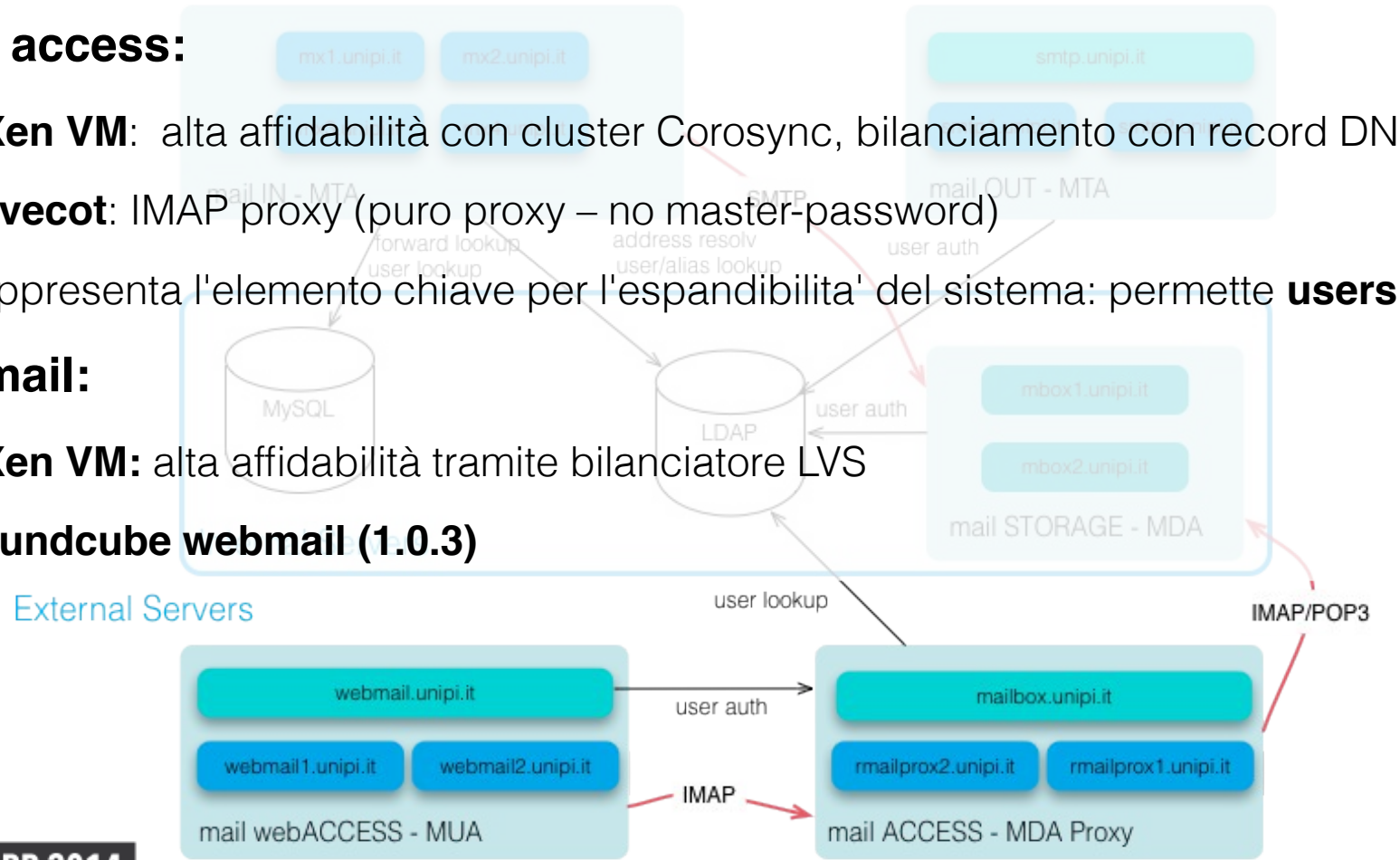
- **2 Xen VM** in HA
- **5TB** (DRBD) per MDA server
- **10GB** per casella (maildir)
- **Dovecot**: IMAP/PoP server
- **Postfix**: SMTP server
- Accesso **esclusivamente** autenticato con protocolli sicuri (**SSL/TLS**)



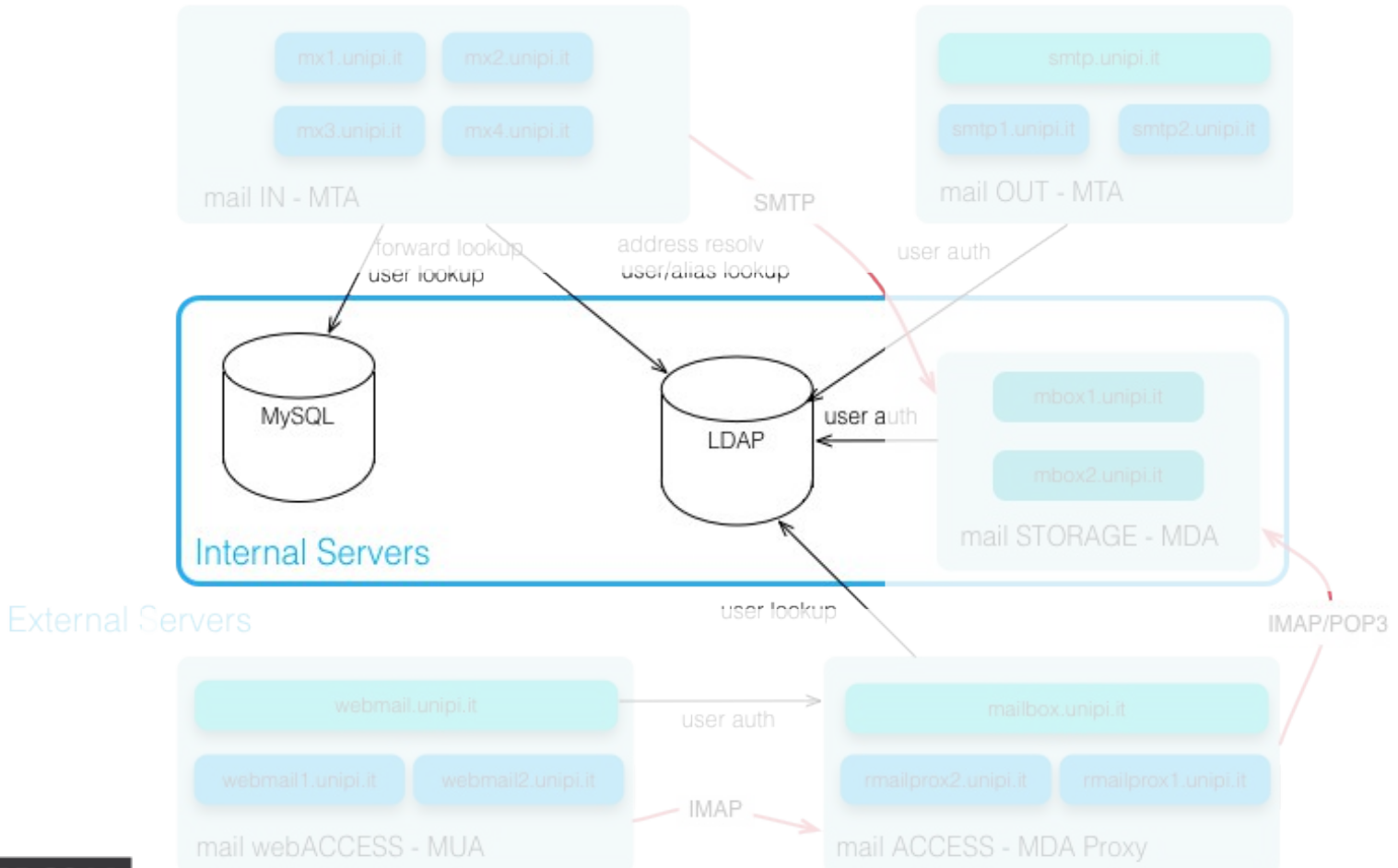
IMAP/PoP Frontend

(Accesso ai MDA)

- **IMAP access:**
  - **2 Xen VM**: alta affidabilità con cluster Corosync, bilanciamento con record DNS
  - **Dovecot**: IMAP proxy (puro proxy – no master-password)
  - Rappresenta l'elemento chiave per l'espandibilita' del sistema: permette **users sharding**
- **Webmail:**
  - **2 Xen VM:** alta affidabilità tramite bilanciatore LVS
  - **Roundcube webmail (1.0.3)**

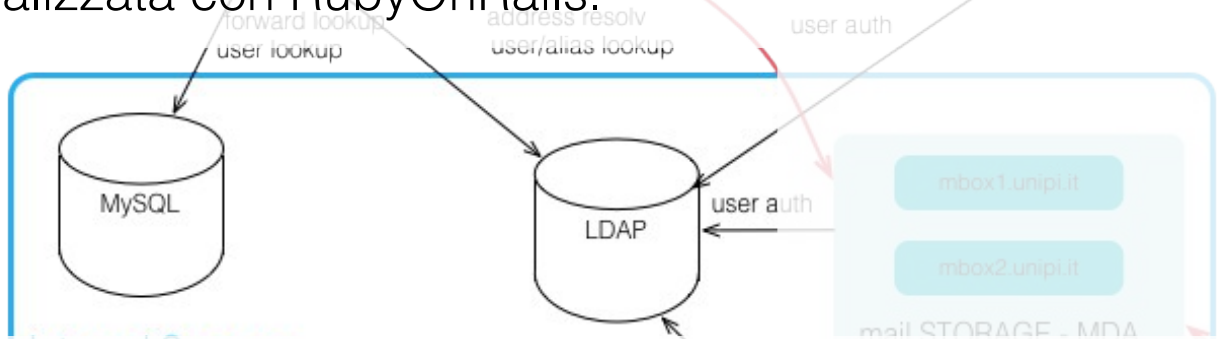


Strumenti di gestione:



Strumenti di gestione:

Gestire il sistema di posta consiste essenzialmente nella gestione dei dati dei server di backend (MySQL e LDAP).Per LDAP viene utilizzata la piattaforma di Identity Management (sviluppata internamente), per MySQL viene utilizzata un'interfaccia realizzata con RubyOnRails.

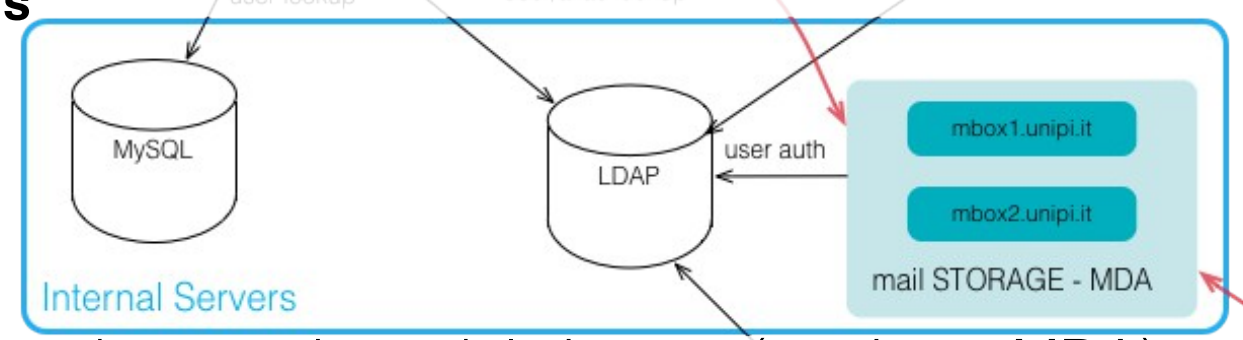


Per la gestione delle segnalazioni sono utilizzati:

- Trouble Ticket System: **OTRS**
- **Logserver** centralizzato consultabile da tutti gli operatori (per troubleshooting)

Strumenti di gestione:

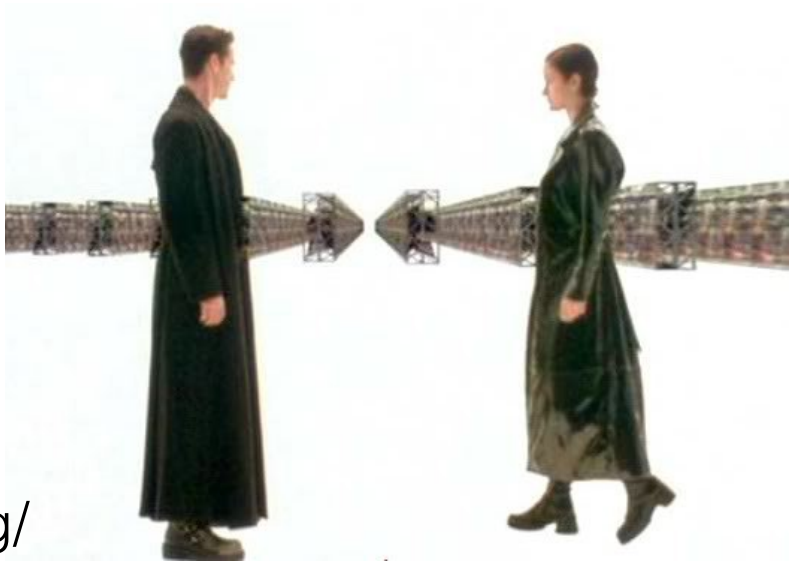
- Per le acquisizioni dei nuovi utenti:
  - **imap-sync + dovecot master-user**
  - **rsync**
  - **ldap tools**
  - **sql**



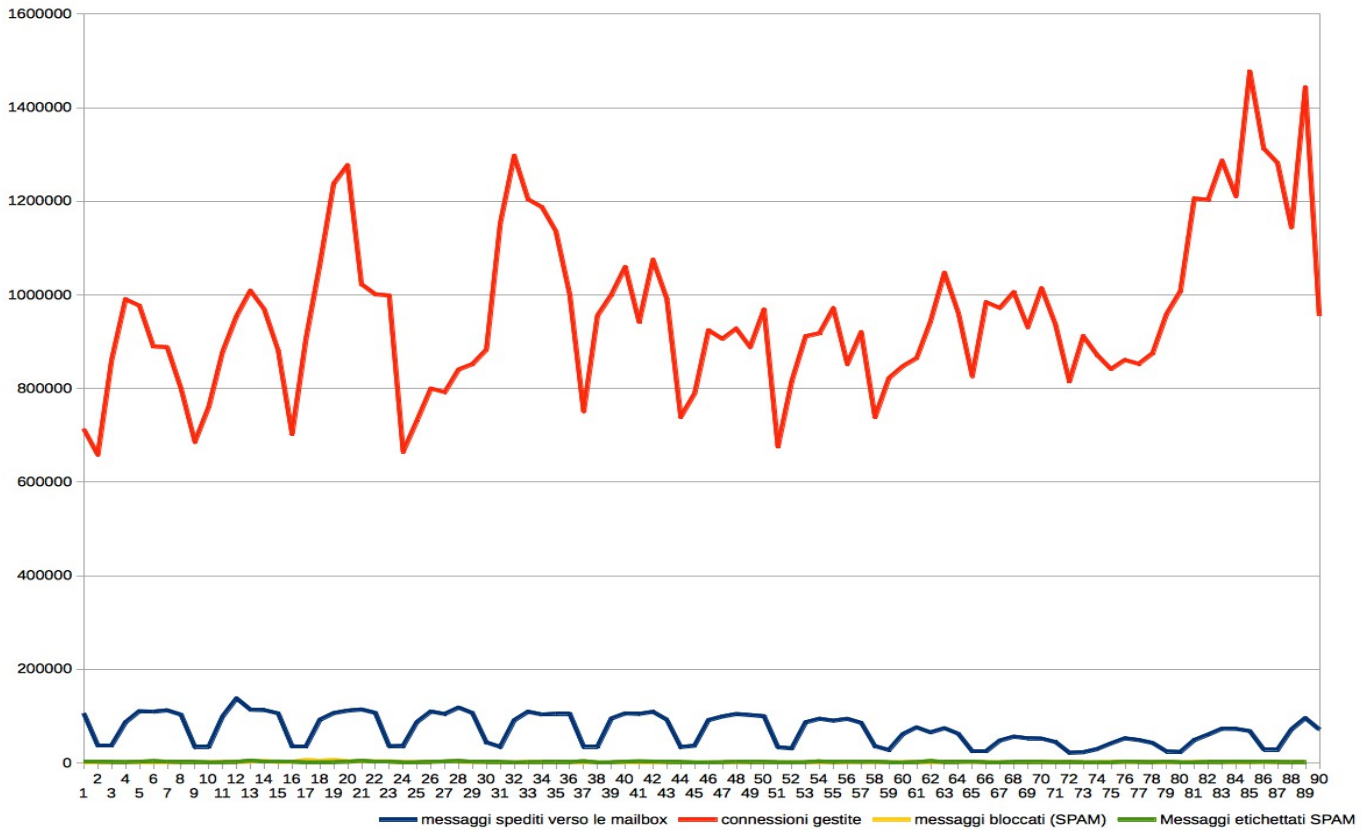
- Per backup ed espansione del sistema (aggiunta MDA):
  - **rsync**
  - **ldap-tools**

Automation/ConfigurationManagement

- **Rex** - http://www.rexify.org/
- **Git** - http://git-scm.com/
- **ISC-DHCP + Preseed**
- **Puppet** - http://puppetlabs.com/
- **TheForeman** - http://theforeman.org/



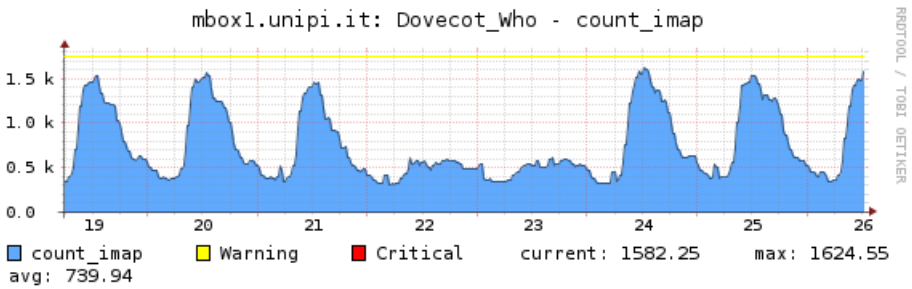
Prestazioni – SMTP IN

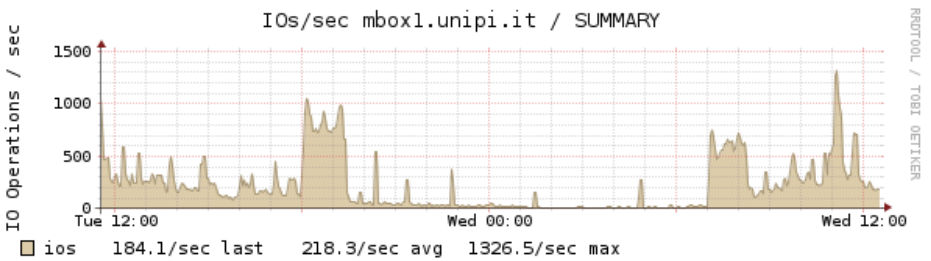


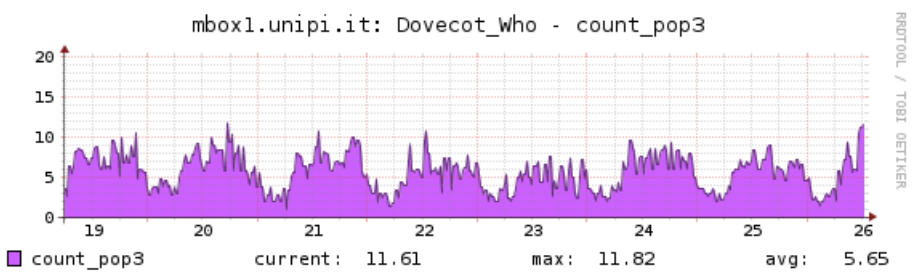
messaggi gestiti al giorno negli ultimi 90gg

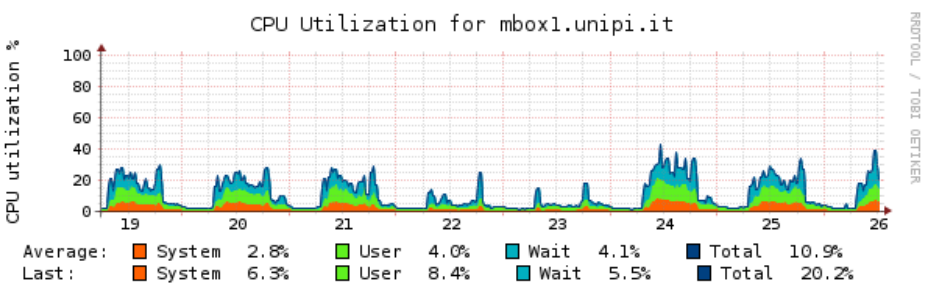
- 6K utenti con casella
- 70K utenti solo traffico IN
- 1Milione connessioni/gg
- 16K email consegnate/gg
- 2.5K email bloccate come spam/gg
- 2.0K email considerate spam/gg

Prestazioni – Accesso alle caselle









Analisi dei costi

L'attivazione del nuovo servizio di posta ha coinciso con l'attivazione della nuova infrastruttura di computing/storage, è quindi molto difficile valutare esattamente i costi.

- **18 VM** direttamente coinvolte nei servizi di posta
- **85 VM** sulle stesse dom0 dei sistemi di posta
- **175 VM** attive al momento

	SPESA	Incidenza	Incidenza
Network	40K	10%	4K
Computing	24K	20%	4.8K
Infrastruttura Fisica	15K	10%	1.5K
Totale	**79K**		**10.3K**
Storage dedicato al solo sistema di posta (compreso di backup)			**18K**
Totale spesa per il sistema di posta			**28.3K**

Analisi dei costi

Al momento:

- 5K caselle attive
- occupazione media: 1GB
- Spazio disponibile/Quota: 2GB/10GB

costo a casella ~ 6euro

Fully loaded (ipotesi):

- 10k caselle
- Spazio disponibile/Quota1G/10GB

Costo a casella ~ 3 euro

Il tempo di vita che ci aspettiamo per questo sistema è di **5 anni**. Occorre quindi valutare i costi di mantenimento per capire come distribuire I costi nel tempo.

Analisi dei costi - mantenimento

- Nessun costo di licenze
- L'infrastruttura di rete è già realizzata ed è in grado di espandersi a costo zero
- L'hardware è coperto da assistenza NBD per i prossimi 5 anni
- Magazzino dischi: ~5K euro (una tantum)
- Assorbimento energetico (dell'intera infrastruttura): 10Keuro (6KW di assorbimento totali)

  → I costi di mantenimento sono molto bassi: il costo annuo per casella diventa quindi di circa **60 centesimi.**

Vantaggi & Svantaggi

- Completo controllo delle policy in uso: flessibilità e gestione delle eccezioni
- Possesso dei dati
- Know-How
- Livelli di disponibilità di servizio vicini a 99.999%
- Completa integrazione con gli altri servizi
- Nessun fornitore specifico

- Costi non “evidentemente” competitivi
- Necessità di sviluppare in proprio strumenti per la gestione di un ambiente multitenant

Il problema è lo storage!

- Alta affidabilità
- Scalabilità
- Prestazioni
- Disaster Recovery
- Continuita' di servizio
- Costi (!)

Almeno il 50% del costo dei sistemi è in qualche modo legato allo storage (dischi/controller).

DRBD ci ha accompagnato fino a questo punto con risultati a nostro avviso soddisfacenti ma non scala in modo sostenibile su grandi numeri.

Sviluppi futuri

- Realizzare un servizio di posta **per gli studenti** con uno spazio casella paragonabile a quello dei dipendenti. Per questo progetto lo storage verrà realizzato con un cluster **CEPH**. Questo dovrebbe portare il costo per casella a circa **10 centesimi/casella/anno**
- Sviluppare **strumenti di gestione** che consentano la vera cogestione del sistema: i colleghi in periferia devono essere in grado di erogare autonomamente le risorse (alias e simili) e intervenire sulle mappe MySQL.

Domande?