Workshop tecnico GARR 2014

“Next Network: costruiamo il futuro della rete”

Soluzioni per la posta elettronica in un Ateneo di medie dimensioni

Roberta Cantaroni

Università degli Studi di Modena e Reggio Emilia

UNIMORE

UNIVERSITÀ DEGLI STUDI DI MODENA E REGGIO EMILIA

Roma 4/12/2014

L'Ateneo

http://www.unimore.it

Università degli Studi di Modena e Reggio Emilia

- A rete di sedi (Modena e Reggio Emilia)
- 14 Dipartimenti, 19 Centri di Servizio e di Ricerca, 7 Direzioni Operative
- Circa 1.500 unità di personale
- Circa 20.000 studenti

Il sistema di posta elettronica è centralizzato dal 2001.

L’infrastruttura

- L'infrastruttura sistemistica, nucleo del Datacenter dell’Ateneo è attualmente concentrata nella sede di Modena
  - chassis Blade Server con 16 nodi di elaborazione, collegati con tecnologie di datacenter bridging (fabric Fiber Channel ed Ethernet fabric) ad un apparato SAN storage multiprotocollo e 4 storage NAS
  - 300GHz di risorse CPU, 1TB RAM, capacità storage di 100TB
- I nodi di elaborazione sono raggruppati per la maggior parte su un unico cluster di virtualizzazione VMware che ospita quasi tutti i servizi amministrativi e centralizzati dell'Ateneo (autorizzazione/autenticazione, condivisione files, web, posta, etc) e fornisce infrastruttura di elaborazione ai Dipartimenti, alle strutture dell'Ateneo ed a strutture esterne convenzionate

Il servizio Posta

Gestisce il ciclo di vita degli indirizzi di posta elettronica assegnati ai diversi “attori” con incarichi istituzionali in Ateneo

- Personale docente e tecnico-amministrativo
- Collaboratori esterni (docenti a contratto, ...)
- Studenti

ma anche

- Strutture e uffici
- Convegni e seminari

Requisiti

L’indirizzo deve

- seguire il ciclo di vita dell’incarico
- essere iscritto a liste di distribuzione per ruolo/struttura/ Dipartimento

Le mailbox devono

- essere usufruibili 24/24h
- libere da spam e virus
- essere accessibili con le credenziali unificate assegnate all’utente per l’accesso a tutti i servizi unimore

Nel caso del personale, è sentita l’esigenza di recuperare agevolmente messaggi cancellati per errore

Una soluzione ibrida

2 domini separati

@unimore.it

dedicato al *personale docente, tecnico-amministrativo, collaboratori esterni, strutture e uffici* gestito con una soluzione realizzata interamente in-house

@studenti.unimore.it

dedicato a *studenti e dottorandi* gestito su piattaforma Google Apps Education

Domini separati?

@unimore.it

- Ricerca indirizzi studenti
- Utilizzo di liste di indirizzi studenti

@studenti.unimore.it

- Alias nome.cognome@unimore.it assegnato ai dottorandi
- Ricerca indirizzi docenti

@unimore.it

I componenti del servizio di posta sono stati divisi *logicamente* per tipologia e realizzati con software prevalentemente OpenSource

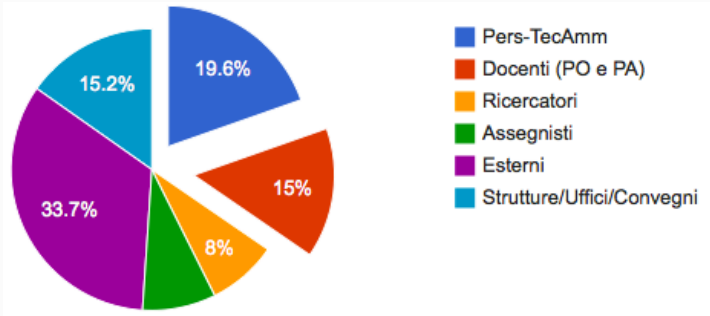
- ricezione mediante server MX di dominio protetti da antivirus/antispam (*Postfix, Sophos*)
- posta in arrivo e accesso IMAPS/POPS (*Dovecot, Postfix*)
- spedizione via SMTP con autenticazione TLS e credenziali unimore protetta da antivirus/antispam *(exim4, spamassassin, clamd*)

@unimore.it

- gestione di liste di distribuzione con controllo dell'identità e liste di discussione con amministratore/moderatore (*Sympa, Mailman*)
- backup/restore dei messaggi (*Zimbra*)
- gestione del ciclo di vita degli indirizzi (*ActiveMQ*)
- Sistema di monitoraggio dei servizi (*Munin*)
- Raccolta centralizzata dei log (*rsyslogd*)

@unimore.it

I numeri



- 3200 mailbox
- 8000 indirizzi/alias
- in media 2.000 accessi distinti POP/IMAP al giorno
- 400.000 messaggi spediti al mese
- 50.000 messaggi/giorno da fuori dominio
- oltre il 95% di mail di spam individuate e bloccate
- più di 400 liste di distribuzione e di discussione
- 2 tecnici dedicati

@unimore.it

Indirizzi e Mailbox

- Gli indirizzi nominali sono nella forma nome.cognome@unimore.it
- L'autenticazione è basata su LDAP con username centralizzata
- 3 Tb di storage per le mailbox (occupazione attuale 55%), file system di tipo xfs, hard link sui messaggi inviati a liste numerose
- Quota personalizzata per mailbox, default 500 Mb
- Formato *Maildir*
- Dimensione max messaggi (testo + attachment) 25 Mb

@unimore.it

MX di dominio

unimore.it.	86400	IN	MX	10 mx1.unimo.it.
unimore.it.	86400	IN	MX	10 mx4.dmz-ext.unimo.it.
unimore.it.	86400	IN	MX	10 polluce.unimo.it.
unimore.it.	86400	IN	MX	10 sophos1.dmz-ext.unimo.it.

I nomi DNS hanno uguale priorità, il carico è distribuito mediante sistema round robin del DNS

@unimore.it

MX di dominio

4 VM su sistema di virtualizzazione *VMware* con sistema operativo *Debian wheezy*

- 4 Gb RAM, 30 Gb disco, file system xfs, 80 Gb per software antispam/antivirus e db quarantena
- ogni VM mantiene una coda locale di mail, eventuale fermo del servizio MTA implica un ritardo solo nella consegna dei messaggi in quella coda

@unimore.it

MX di dominio

Antivirus/antispam realizzati con

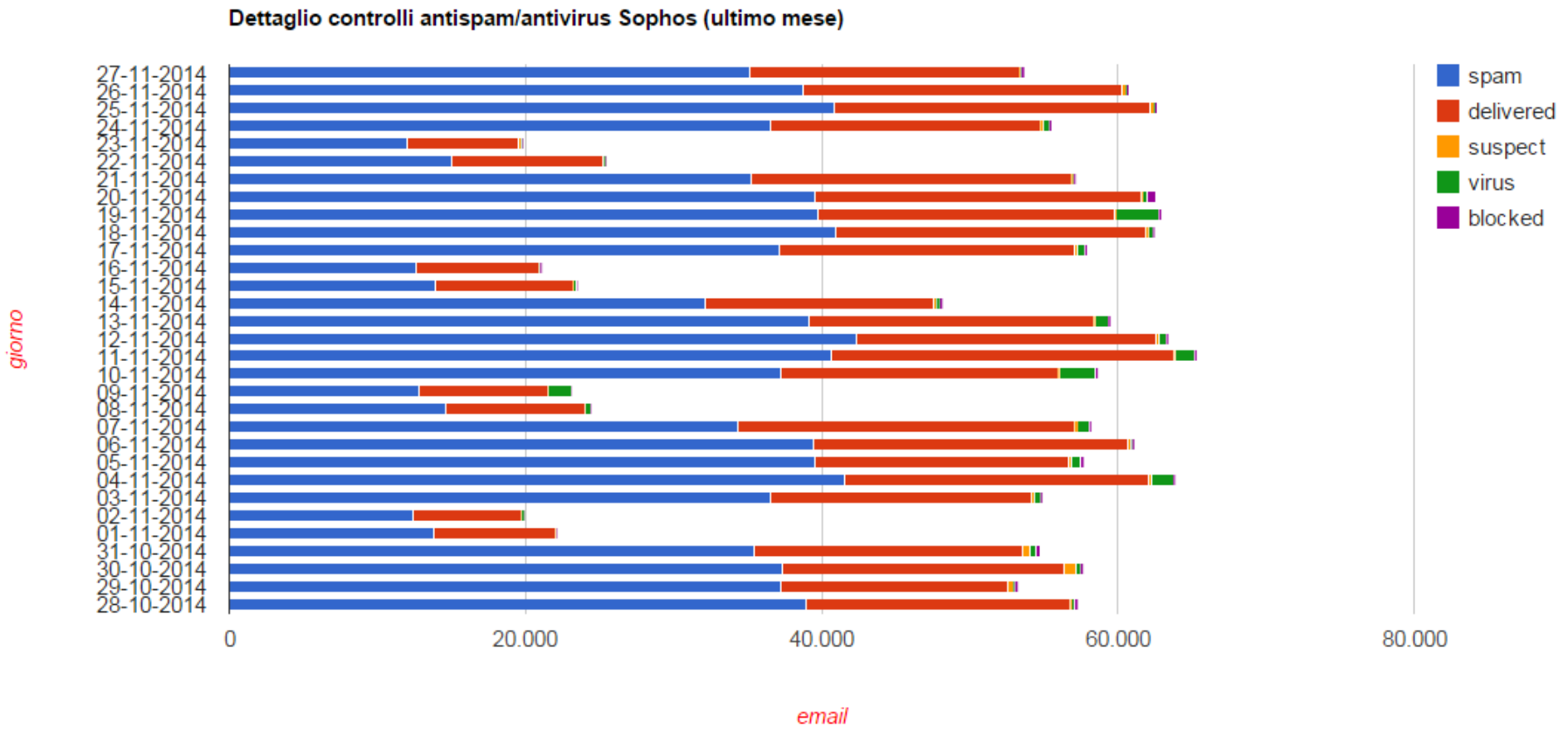
- software proprietario (PureMessage di Sophos)
- filtri a livello MTA (reject_non_fqdn_helo_hostname, reject_unknown_sender_domain, reject_non_fqdn_sender, reject_unverified_sender, ...)
- Filtro sui recipient validi (solo gli indirizzi @unimore.it attivi possono accettare mail in ingresso)

Per policy le mail riconosciute spam (probabilità > 50%) sono bloccate nello spazio di quarantena, condiviso tra i 4 server, per 5 giorni

Ogni utente può autorizzare il mittente richiedendo la consegna in caso di falso positivo, bloccare un mittente fastidioso, richiedere la consegna di un digest giornaliero con le intestazioni delle mail bloccate

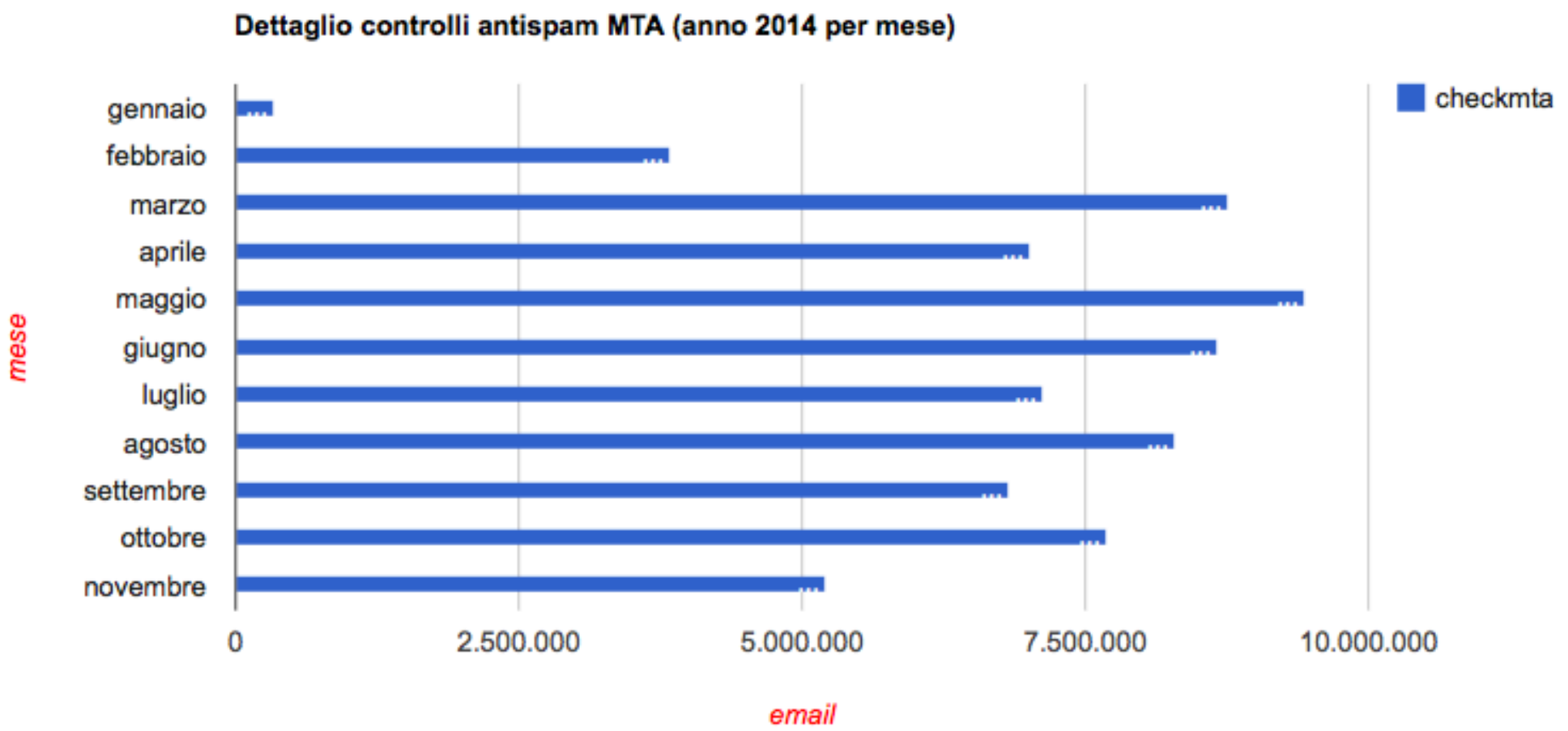
@unimore.it

MX di dominio



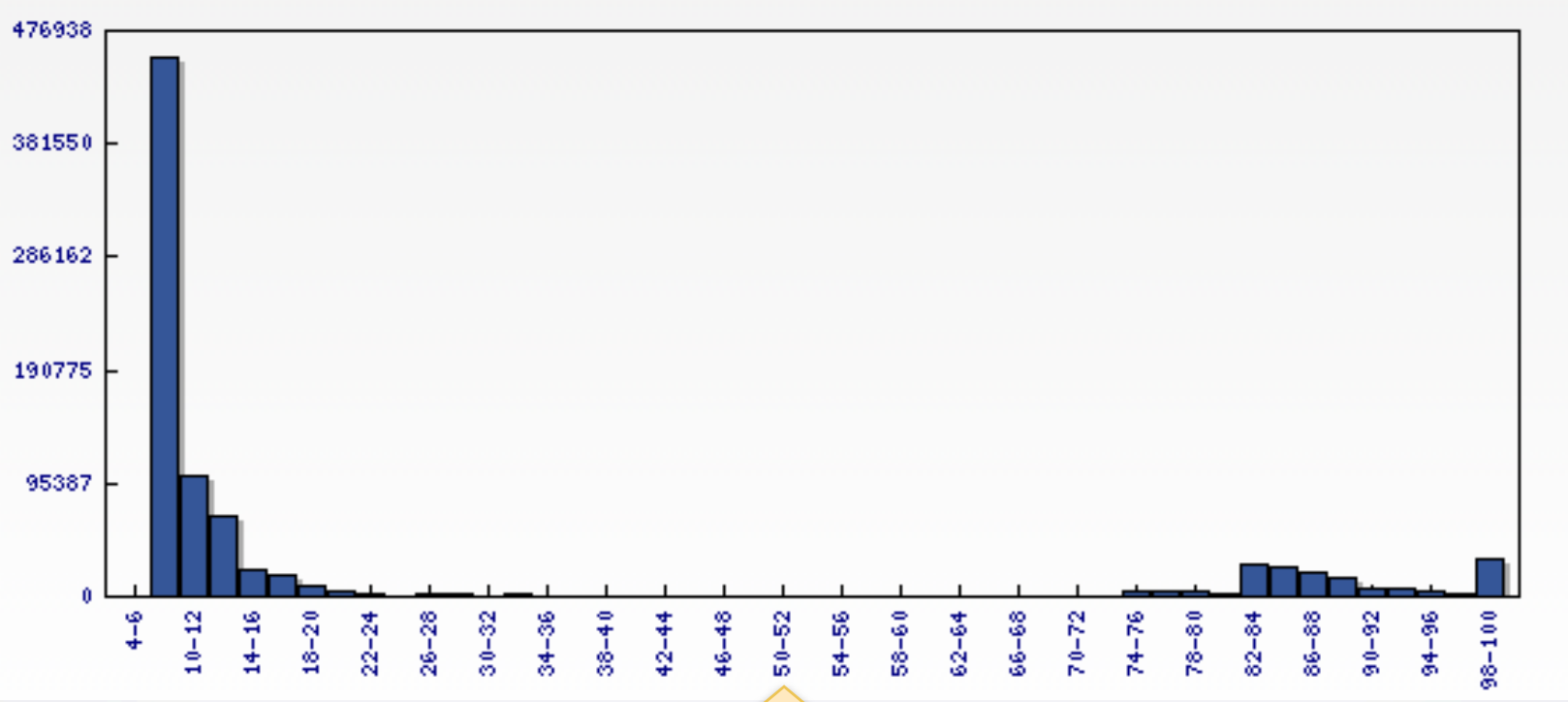
@unimore.it

MX di dominio



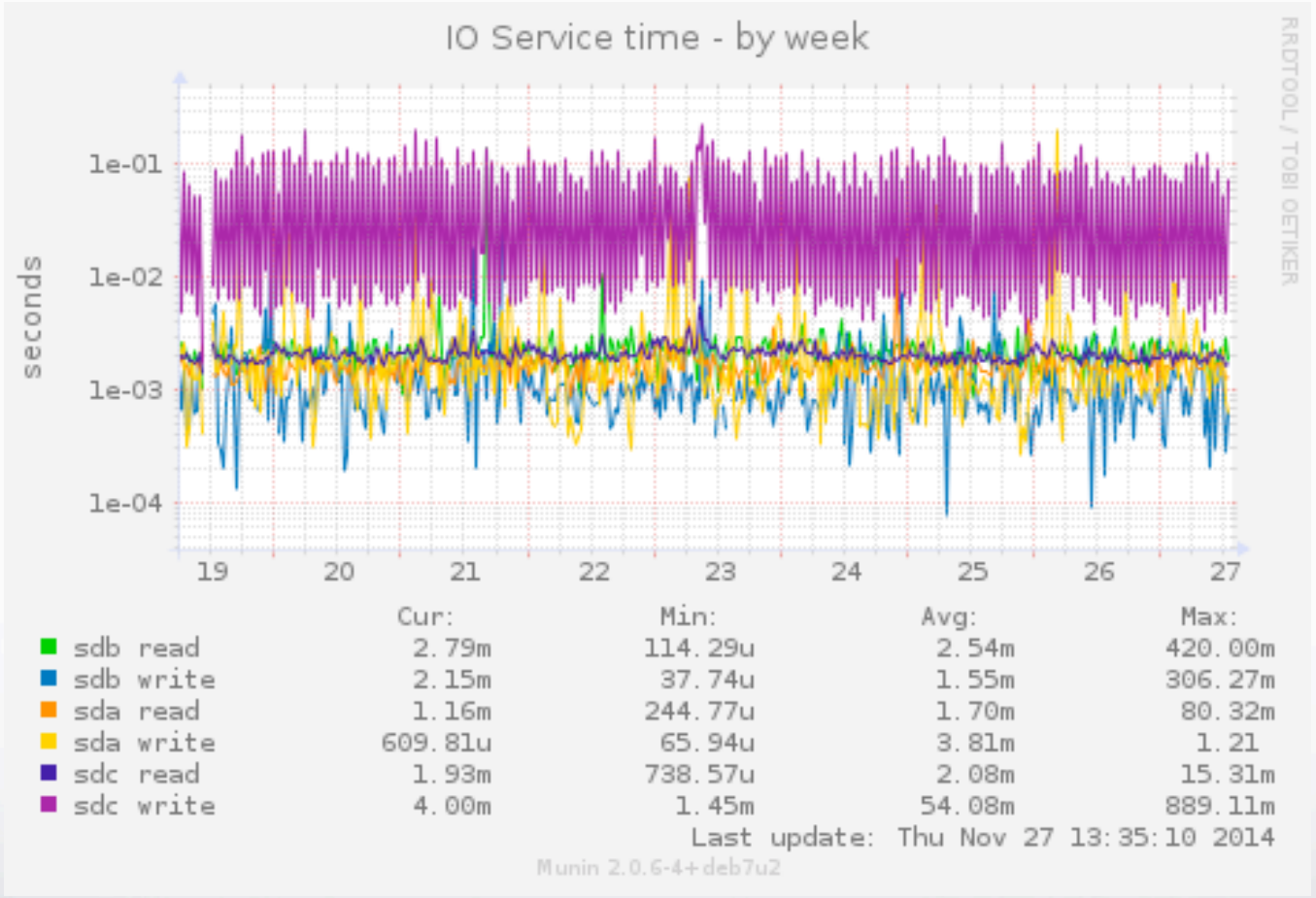
@unimore.it

MX di dominio



Volume di spam/probabilità ultimo mese

@unimore.it



I/O su MX con database quarantena

@unimore.it

Posta in arrivo – mail.unimore.it

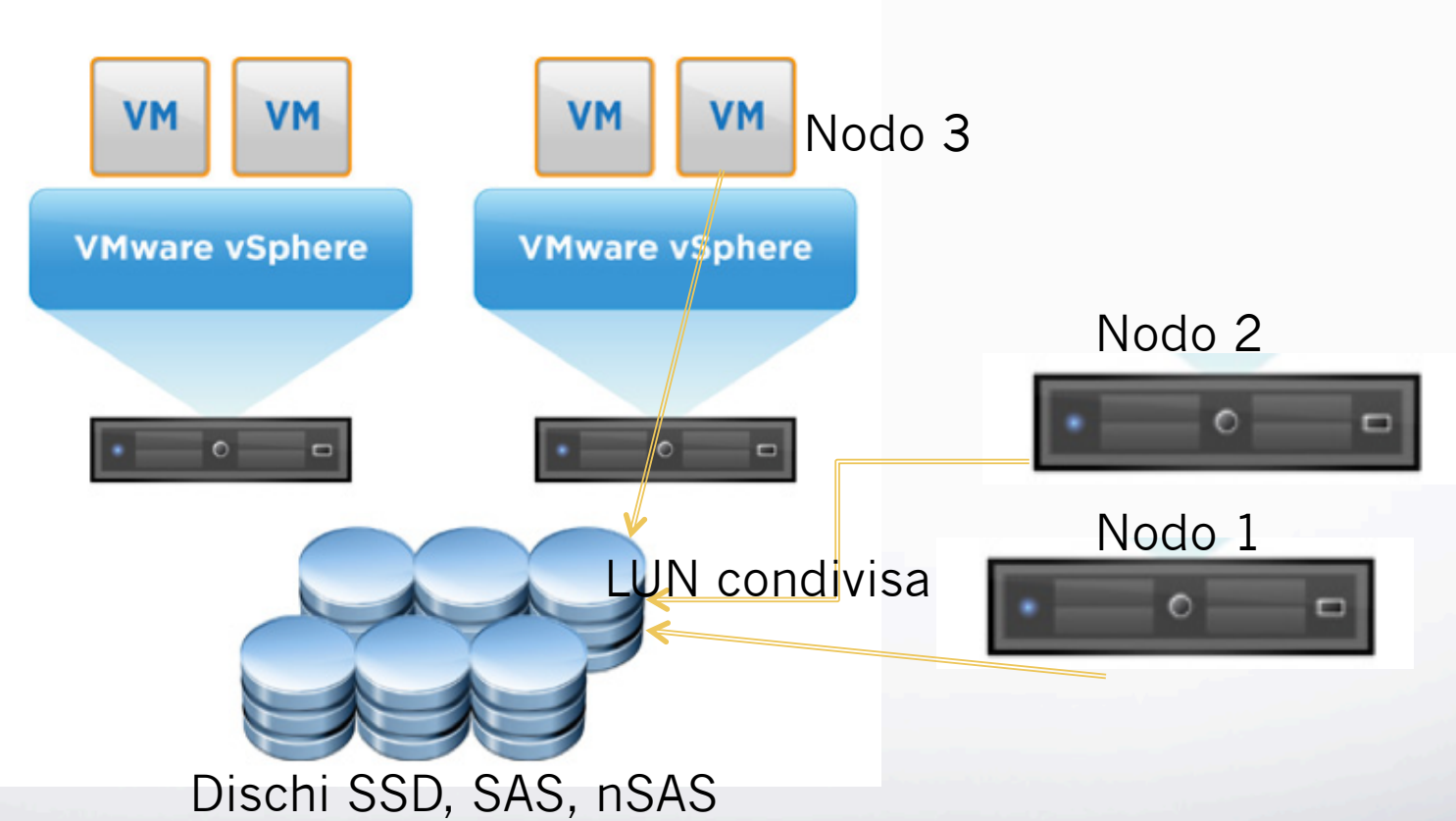
Cluster di 3 nodi (2 fisici e 1 virtuale su piattaforma VMware) che condividono una LUN sullo storage dell'infrastruttura di virtualizzazione

Software di clusterizzazione *Cluster Suite di CentOS 6*, 16 Gb RAM, sw OpenSource

Un solo nodo è attivo in ogni momento ed eroga i servizi di cluster (filesystem, IP a cui corrisponde il record A mail.unimore.it, *Mysql, Dovecot, Postfix, httpd)*

Il cluster

Posta in arrivo – mail.unimore.it



Fonte: http://www.vmware.com

@unimore.it

Posta in arrivo – mail.unimore.it

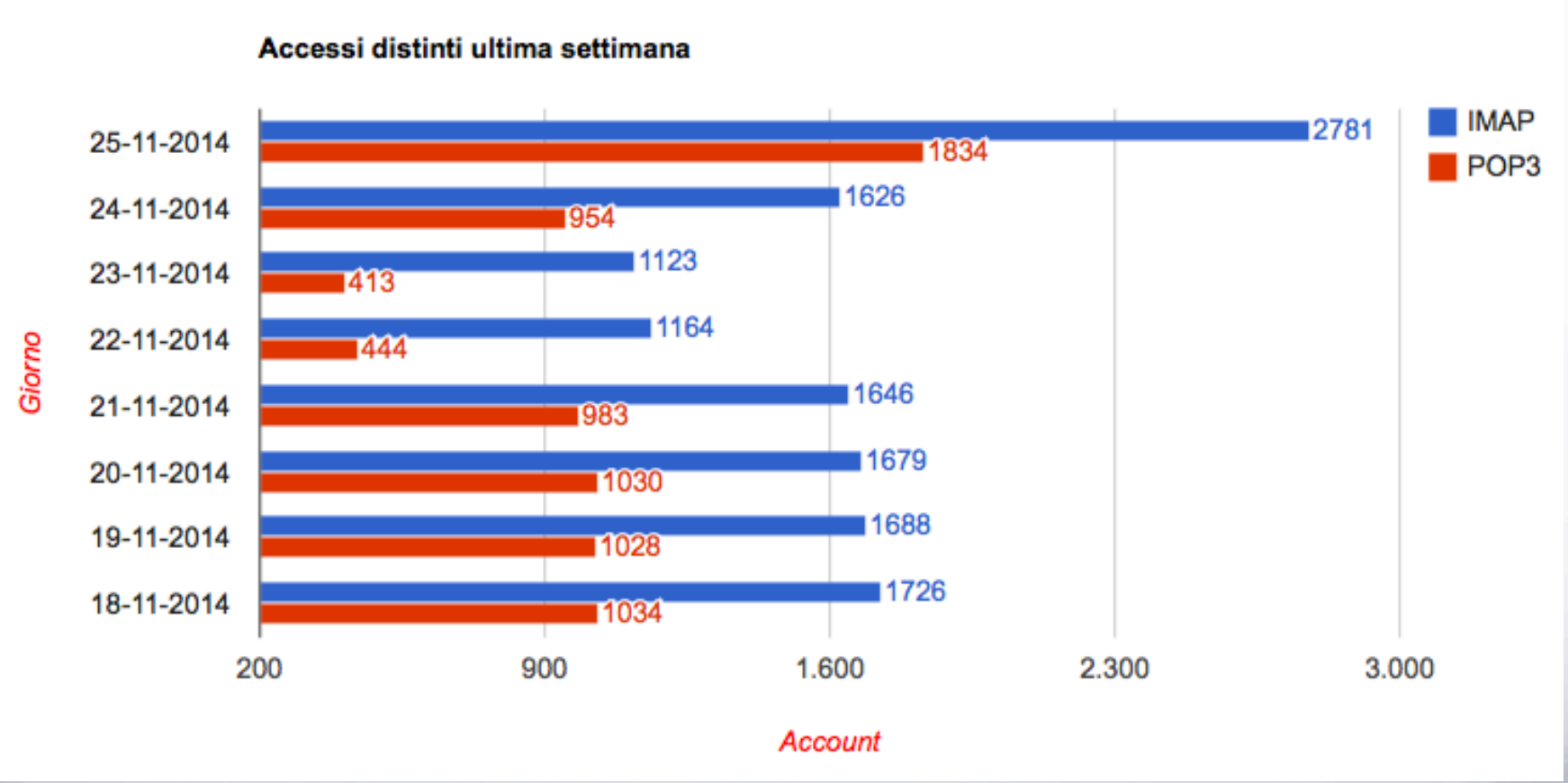
Sul filesystem risiedono i messaggi, il database con mailbox e indirizzi, la coda di posta, gli script per la gestione (creazione/cancellazione/disattivazione) e l'interfaccia web che consente attivazione di vacation/ forward e ricerca indirizzi

- La logica del cluster prevede che i nodi si "sentano" tramite dati scritti su quorum disk e che i servizi di cluster migrino su uno degli altri nodi nel caso di disservizio su quello attivo

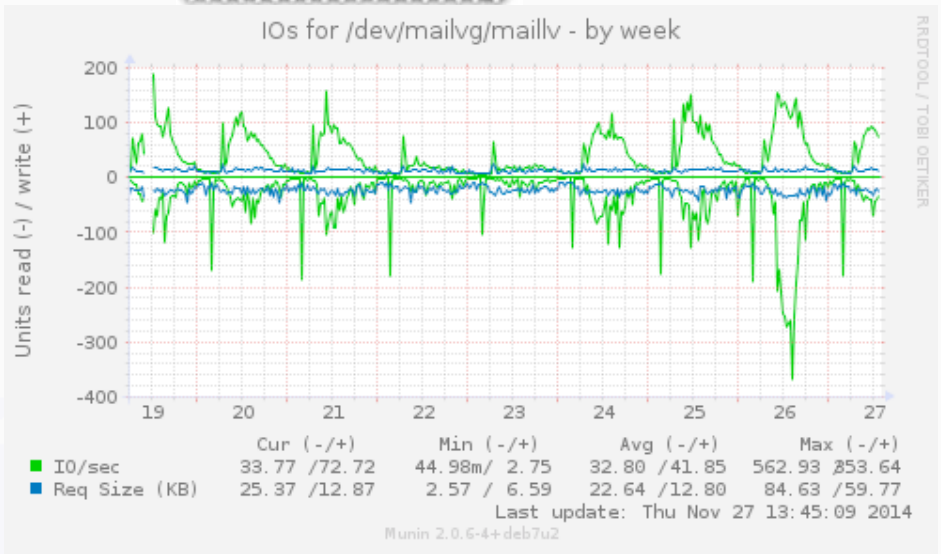
L'accesso ai servizi è realizzato tramite replica locale del sistema LDAP di Ateneo attiva sui 3 nodi

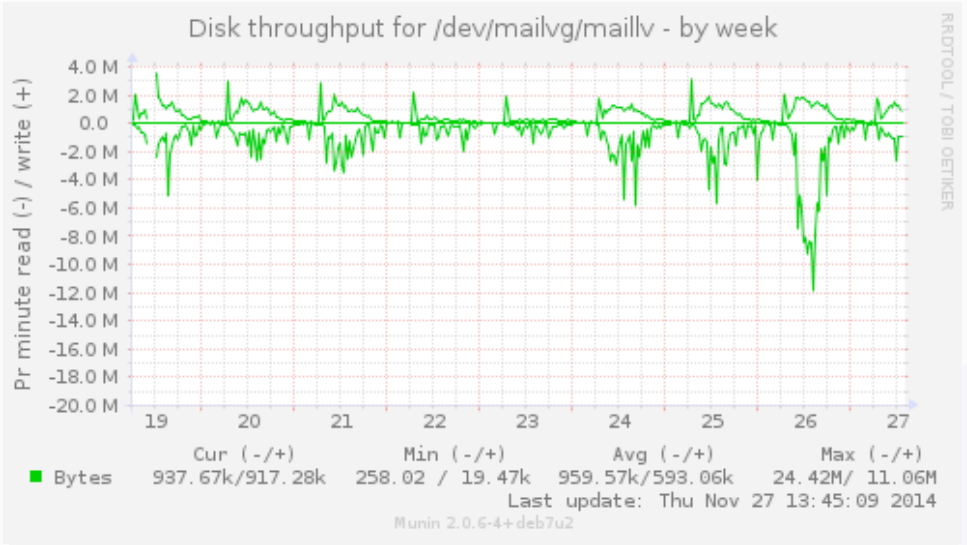
@unimore.it

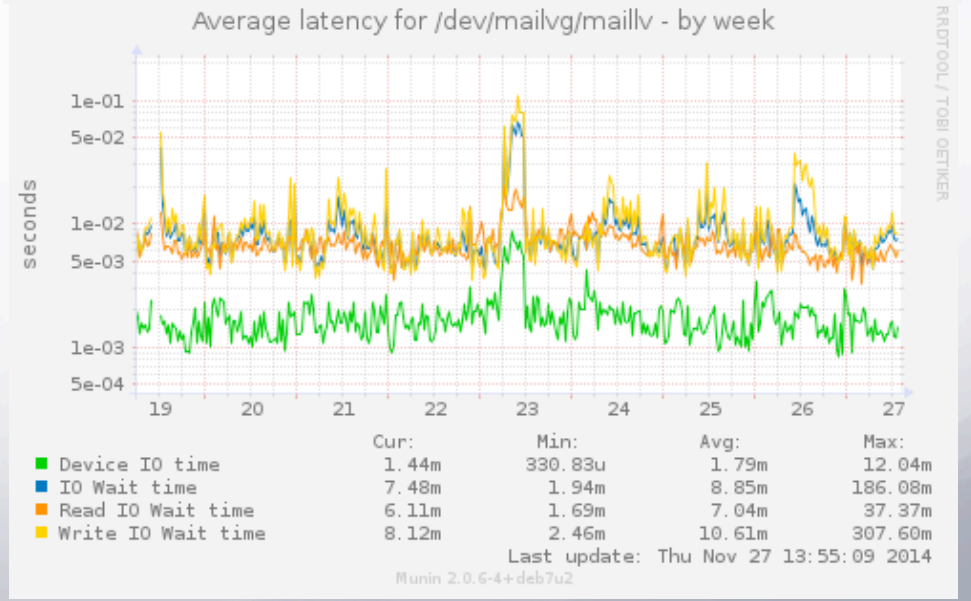
Posta in arrivo – mail.unimore.it



@unimore.it







Tiering (automatico):
1.63% extreme performance (SSD)
70.02% performance (SAS)
28.35% performance (nSAS)

@unimore.it

SMTP – smtp.unimore.it

smtp.unimore.it. 60	IN	A	155.185.44.25
smtp.unimore.it. 60	IN	A	155.185.44.26
smtp.unimore.it. 60	IN	A	155.185.1.3
smtp.unimore.it. 60	IN	A	155.185.44.3

Il nome è unico e ad esso corrispondono 4 record A nel DNS, il carico è distribuito mediante sistema round robin del DNS

@unimore.it

SMTP – smtp.unimore.it

- 4 VM su sistema di virtualizzazione *VMware* con sistema operativo *Debian wheezy*, 2 Gb RAM, 10 Gb disco, file system xfs
- Autenticazione TLS con le stesse credenziali della posta in arrivo
- Antivirus e antispam OpenSource (*clamd, spamassassin*) e filtri a livello MTA (*exim4*) in grado di bloccare l'invio con credenziali compromesse e/o limitare il numero di mail spedite all'ora per username

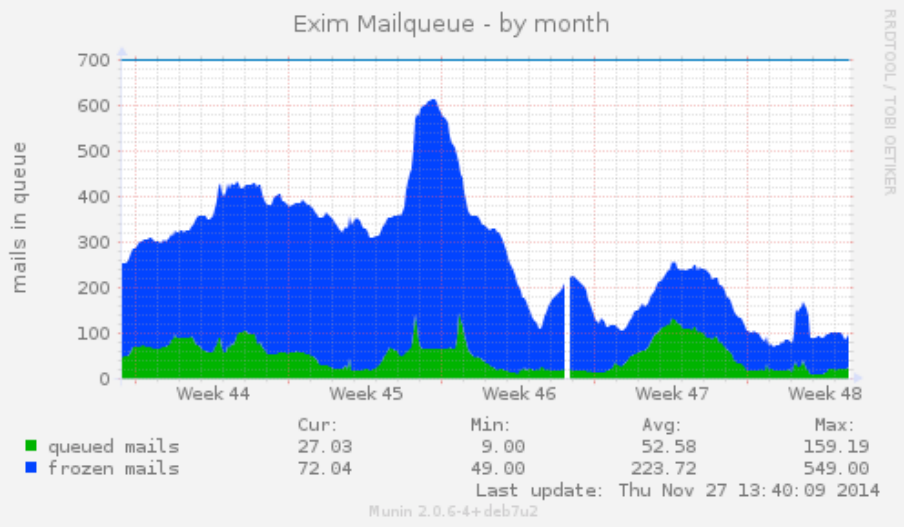
@unimore.it

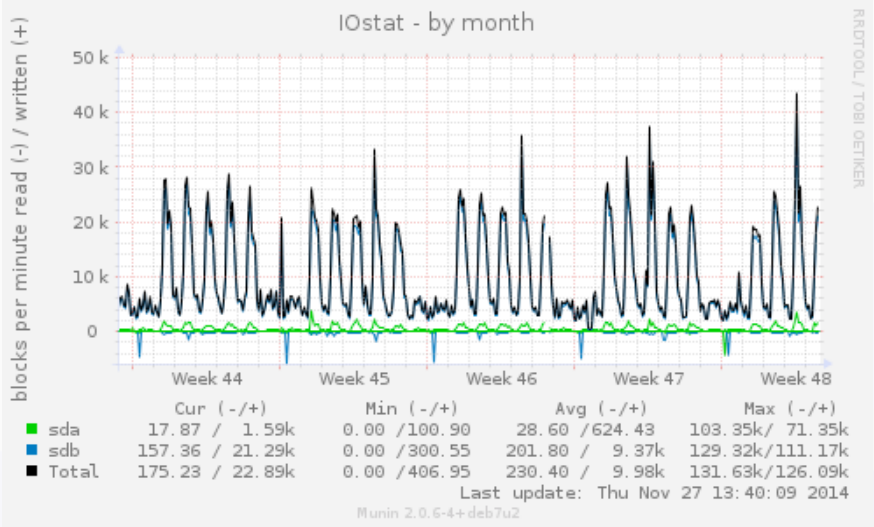
SMTP – smtp.unimore.it

Ogni VM mantiene una coda locale di mail, un eventuale fermo del servizio MTA implica un ritardo solo nella consegna dei messaggi in quella coda

@unimore.it

SMTP – smtp.unimore.it

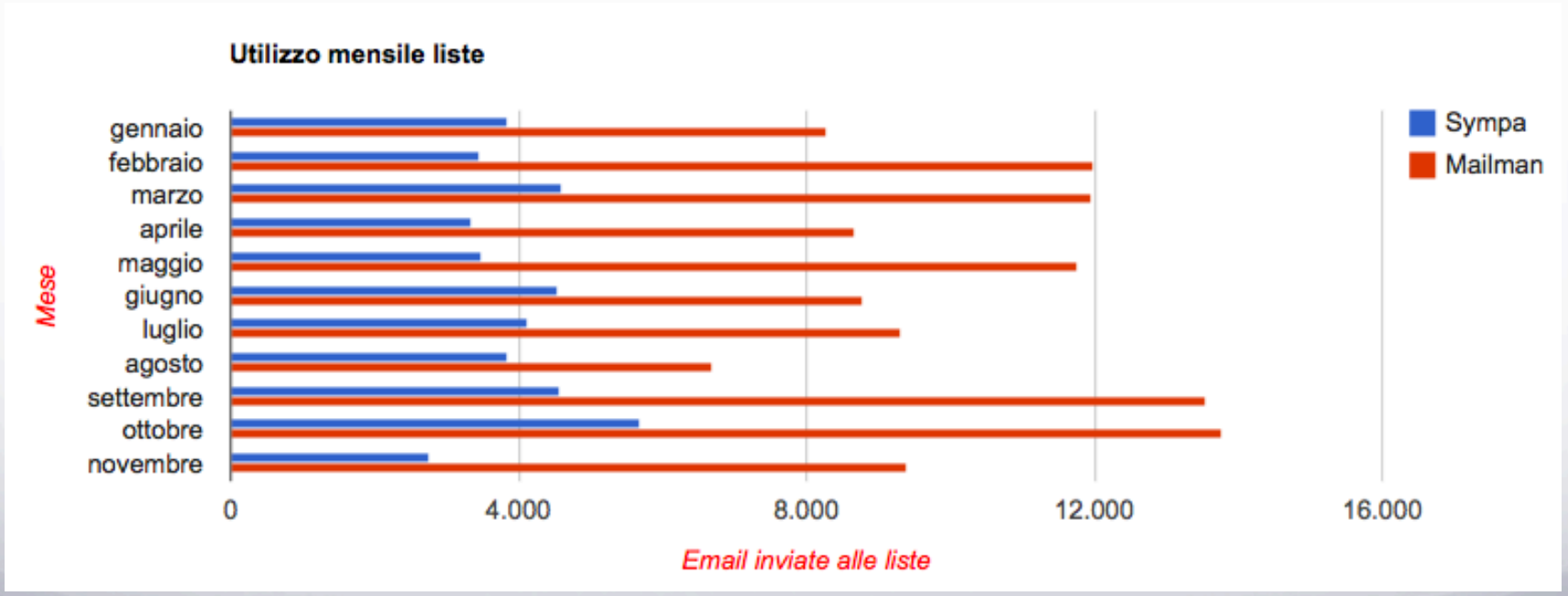




@unimore.it

Le liste

Più di 400 liste di distribuzione gestite con *Sympa* e sincronizzate con LDAP, liste di discussione gestite con *Mailman*



@unimore.it

Backup/Restore

- Snapshot periodici schedulati sulla SAN (1/gg con retention di 7gg)
- Sincronizzazione settimanale del contenuto delle mailbox su altro storage mediante *rsync* e ripristino su richiesta di messaggi o folder
- Copia in tempo reale su altro server di posta (realizzato con *Zimbra* versione Opensource su *Centos* 6, 4 Gb RAM, 800 Gb disco, occupazione 84%) dei messaggi ricevuti e possibilità di accesso webmail per il recupero di messaggi ricevuti fino a 3 mesi prima

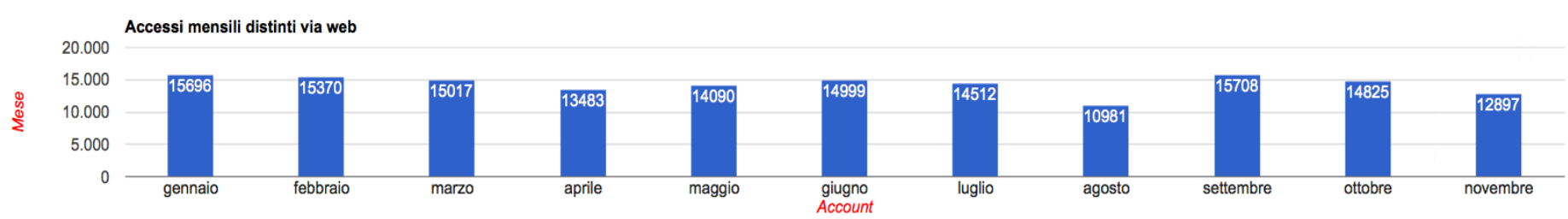
@studenti.unimore.it

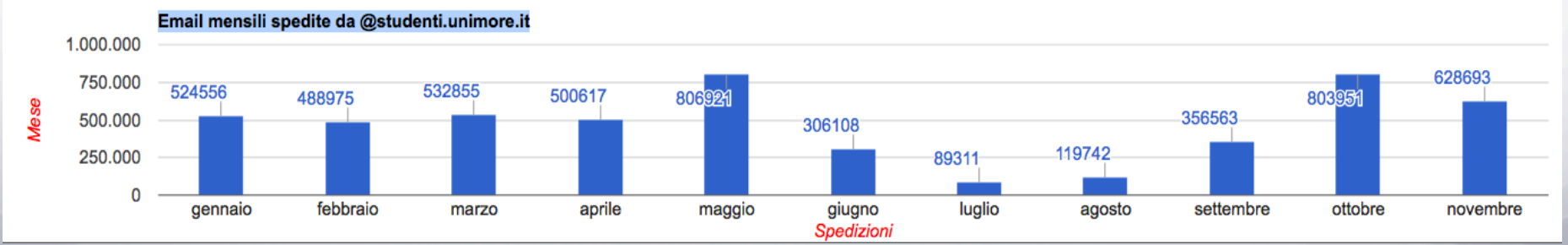
- Dal 2008 il dominio è gestito su piattaforma Google Apps Education.
- Formato <ID>@studenti.unimore.it dove ID è l'identificativo numerico assegnato dalle Segreterie Studenti
- L'indirizzo rimane attivo per 3 anni dopo il conseguimento del titolo (alum)
- circa 40.000 mailbox/indirizzi attivi (studenti + alum)
- 17 gruppi Google (tutti, gli alum, i dottorandi, per dipartimento) a cui corrispondono 17 liste di distribuzione sincronizzate giornalmente con LDAP, ad accesso riservato e moderate

@studenti.unimore.it

I numeri

- in media 15.000 accessi distinti al mese
- in media 500.000 email spedite/mese



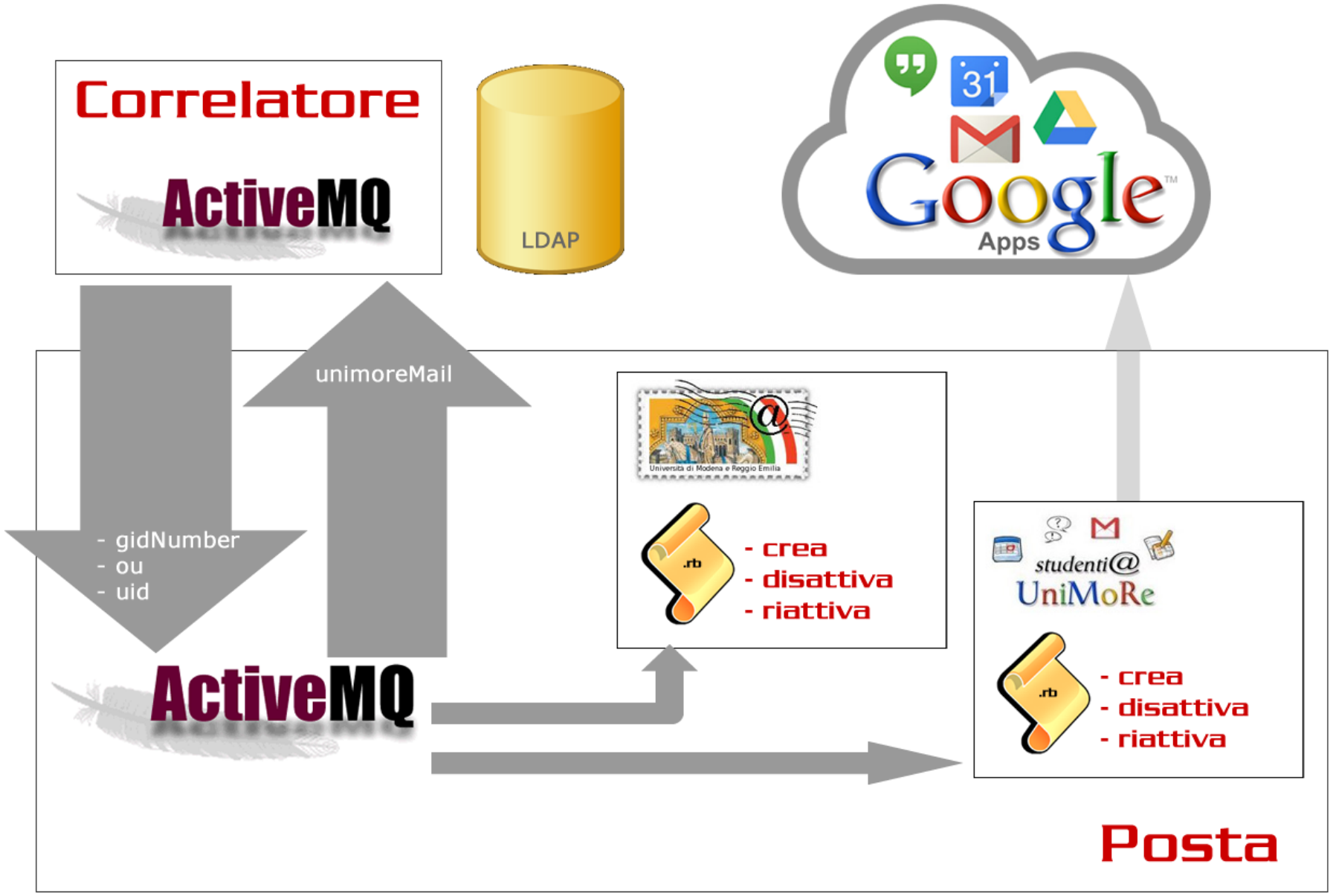


@studenti.unimore.it

- Attivati Posta, Calendar, Drive e Chat
- I limiti sono quelli impostati da Google (spazio illimitato, dimensione messaggi 25 Gb)
- L'interfaccia web non presenta banner pubblicitari
- I dati inviati ai server di Google sono: username, nome e cognome e la password secondaria utilizzata dallo studente per accedere via client
- L'autenticazione è basata su Shibboleth con le credenziali centralizzate unimore
- Per mantenere la tracciabilità dei log, le email ricevute e spedite passano dai server MX e SMTP di unimore

Ciclo di vita degli indirizzi

- Sistema di messaggistica Apache ActiveMQ
- I sistemi POSTA ed LDAP sono entrambi producer e consumer di messaggi
  - utenti aggiunti
  - utenti cancellati
  - account che cambiano utente di riferimento
  - studenti che cambiano lo ou (si tratta di studenti che diventano alum o transizioni da studente a dottorando o da registrato a studente)
  - nuovi indirizzi di posta
- Ogni variazione su LDAP genera un messaggio a cui segue l'azione corrispondente (creazione/riattivazione/disattivazione) nel dominio @unimore.it (script *Ruby*) e @studenti.unimore.it (script *Ruby* e chiamate *Google Admin SDK*)


Correlatore
ActiveMQ
LDAP
Google
Apps
unimoreMail
- gidNumber
- ou
- uid
ActiveMQ
Università di Modena e Reggio Emilia
.rb
- crea
- disattiva
- riattiva
studenti@
UniMoRe
.rb
- crea
- disattiva
- riattiva
Posta

Riferimenti

Portale del servizio @unimore.it

http://posta.unimore.it

Portale del servizio @studenti.unimore.it

http://start.studenti.unimore.it

Grazie per l'attenzione!