

HERMES: un servizio di Posta Elettronica Sicura per gli studenti e il personale delle Università

di Nico Tranquilli

Il servizio, basato su un'infrastruttura centralizzata, fornisce una casella di posta elettronica sia al personale dipendente che ad ogni studente, con il duplice obiettivo di costituire un canale di comunicazione per gli atenei e di offrire loro uno strumento di scambio di conoscenze con il mondo esterno

Con l'inizio del nuovo anno accademico, entrerà in produzione al CINECA la nuova piattaforma di posta elettronica sicura denominata HERMES, rivolta a studenti e personale delle Università.

Il servizio, basato su un'infrastruttura centralizzata, fornisce una casella di posta elettronica sia al personale dipendente che ad ogni studente (già all'atto dell'immatricolazione), con il duplice obiettivo di costituire un canale di comunicazione per gli atenei e di offrire loro uno strumento di scambio di conoscenze con il mondo esterno.

L'approccio nella progettazione del sistema è stato quello di integrare software in gran parte open-source, procedure sviluppate ad-hoc dal CINECA e prodotti commerciali, con l'obiettivo primario di garantire **alta disponibilità, massima affidabilità, elevate prestazioni e ampia scalabilità** ad un servizio oramai considerato mission-critical.

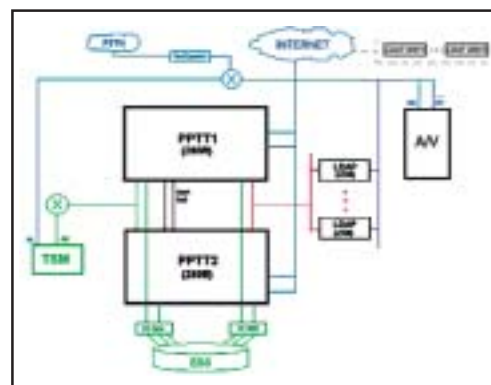
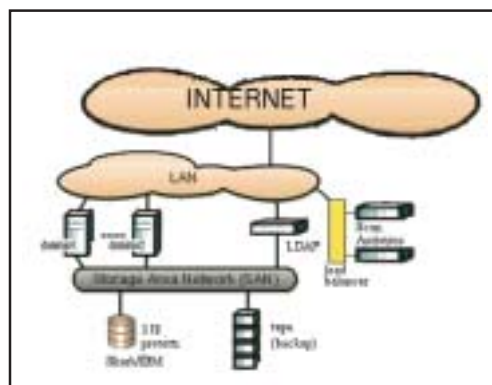
Queste caratteristiche vengono assicurate grazie anche all'utilizzo di componenti hardware interamente ridondati (linee elettri-

che e alimentatori, schede e switch per rete e storage, cpu e server in configurazione cluster) e ad uno storage protetto basato su SAN (Storage Area Network) già in produzione. L'integrità delle informazioni viene inoltre garantita dall'utilizzo di un potente meccanismo di controllo antivirus.

Le principali componenti dell'architettura

Cluster di server centrali e Storage protetto

Gli applicativi usati direttamente dall'utenza finale sono ospitati su un cluster Sun biprocessore (SunFire 280R, 2x900Mhz, 8GB Ram) basato su Veritas cluster 2.0. Va sottolineato il fatto che i servizi non sono legati a uno specifico componente del cluster: se un nodo smettesse di funzionare o se dovesse essere fermato per upgrade software e/o hardware, le applicazioni da esso ospitate migrerebbero (in automatico o manualmente) su altri nodi, in modo trasparente al client. La visibilità



di uno storage esterno, comune a tutti i nodi, è stata una scelta dettata dalla configurazione HA (*High Availability*) del sistema. Si è deciso di utilizzare la Storage Area Network CINECA basata su IBM Shark (IBM F20) allo scopo sia di garantire l'integrità dei dati sia di assicurare affidabilità e performance ad un'applicazione in cui l'I/O è uno dei fattori limitanti. La scelta risulta opportuna anche in previsione del numero elevato di utenti, delle notevoli dimensioni del traffico e dell'alto volume dei dati da archiviare. Ciascun server dispone di due controller *fibre channel* verso altrettanti switch che, oltre al *fail-over*, permettono di massimizzare il throughput mediante load-sharing su più percorsi (DMP, Dynamic Multi Pathing).

Cluster Antivirus

Con le stesse garanzie di disponibilità dei server appena descritti, il traffico SMTP in ingresso e in uscita viene gestito da una batteria di server Intel con funzioni di antivirus. Il loro compito consiste nell'alleggerire i server centrali dall'onere di gestire la posta in ingresso e in uscita "ripulendola" dalla presenza di virus.

Server di autenticazione

L'autenticazione dell'utenza viene delegata a server dedicati, basati su LDAP (Lightweight Directory Access Protocol), che replicano il contenuto di directory server remoti gestiti dalle stesse Università. Le informazioni in essi contenute vengono utilizzate altresì per la creazione/rimozione automatica delle caselle di posta e per la generazione di alias o liste di distribuzione. Una copia dei dati viene mantenuta



anche su un'istanza LDAP installata sui server centrali, per essere usata come backup in caso di non disponibilità dei server di autenticazione dedicati.

Backup periodico

Tutti i server e le caselle di posta vengono mantenuti sotto backup incrementale attraverso un sistema basato su software Tivoli Storage Manager e STK 9310 Powderhorn.

Accesso via PSTN (Public Switched Telephone Network): multicanalità per le funzioni di diagnosi e helpdesk

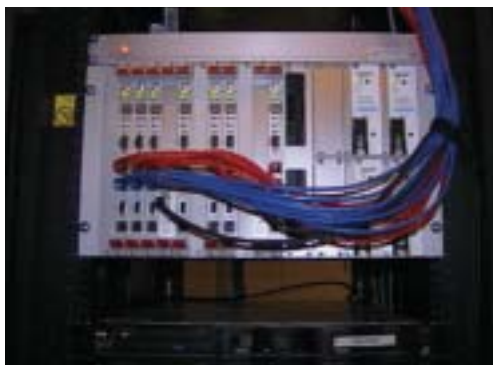
Alcune funzionalità per verificare lo stato del servizio e un motore di helpdesk automatizzato (descritto più in dettaglio tra le caratteristiche), vengono resi fruibili anche tramite accesso telefonico di tipo tradizionale. Un sottosistema text2speech raccoglie le scelte dell'utenza inviate tramite toni DTMF (multifrequenza) e traduce in voce le risposte del sistema.

Principali caratteristiche

Il servizio si differenzia dai sistemi di posta tradizionali per alcune caratteristiche di particolare valore che, oltre a migliorare l'operatività dell'utenza e delle Università, hanno l'obiettivo di accrescere la sicurezza del servizio.

Protezione Antivirus

In base ad un'analisi delle attuali problematiche della posta elettronica e delle prevedibili linee di tendenza, è stato ritenuto irrinunciabile l'uso di meccanismi per la protezione dei messaggi da virus informa-



tici. La piattaforma è dotata quindi di un controllo antivirus su hardware dedicato (cluster di macchine linux) basato su *Sophos Antivirus* e *Spin SafeMail*. Questo analizza la posta in arrivo, in partenza e in smistamento interno al sistema alla ricerca di mail infette. L'aggiornamento delle impronte virali avviene in tempo reale, automaticamente ogni volta che queste vengono rilasciate dal produttore.

Accesso SSL

Tutti i servizi sono fruibili oltre che in chiaro anche in modalità "sicura" (SSL/TLS). Lo scambio di informazioni tra client e server, come ad esempio l'invio della password di accesso al servizio, avviene in modalità protetta mediante crittografia a 128bit.

LDAP:

Gestione dell'utenza e Autenticazione

La creazione delle caselle di posta e la definizione delle password di accesso al servizio vengono gestite direttamente dalle Università mediante l'inserimento dei dati utente su un proprio directory server compatibile con il protocollo LDAP (es: OpenLDAP o MS Active Directory). L'infrastruttura realizzata garantisce l'unicità della password per questo ed altri servizi che comunichino sulla base degli stessi standard (LDAP) con il sistema di messaggistica. Il servizio è già compatibile con il software di segreteria studenti del CINECA Esse3, con cui può condividere la base di dati. Per motivi di performance e affidabilità, le informazioni dei directory server remoti vengono comun-

La piattaforma è dotata quindi di un controllo antivirus su hardware dedicato (cluster di macchine linux) basato su Sophos Antivirus e Spin SafeMail

SPECIFICHE TECNICHE

Hosting dei servizi imap/s, pop3/s, http/s, smtp-auth/s:

SunFire 280R, 2xUltraSparc III 900Mhz, 8GB Ram
o/s Solaris 8
Veritas Cluster
Veritas Volume Manager e File System
Cyrus Imapd e Sasl
OpenSSL
Apache
Postfix
OpenLDAP
Horde/IMP
MySQL
+sw sviluppato ad-hoc dal Cineca

Server di autenticazione:

Server Intel P-III 1.2Ghz, 1GB Ram
o/s Linux + OpenLDAP
o/s Win2K + MS Active Directory

Antivirus:

Ascensit FastCI, cluster Linux in tecnologia industriale
7 Schede Compact PCI complete di:
- Processore Pentium a 700 Mhz
- 256 MB RAM
- 256 MB SSD (disco allo stato solido)
- 2 ethernet 10/100
- Sistema di re-boot automatico Watch-Dog
Sophos Antivirus
Spin SafeMail

Storage e sistema di backup:

Tecnologia IBM/Shark (F20), protetto, scalabile fino a 22TB, 1.6TB/s throughput
Tivoli Storage Manager e STK 9310 powderhorn

DARE VOCE ALLE INFORMAZIONIdi *Andrea Venturi*

Per realizzare un canale di accesso alle informazioni (in questo caso un helpdesk automatizzato) alternativo alla rete Internet, il CINECA ha realizzato un'infrastruttura telefonica per il trattamento delle richieste di supporto. Un cluster di server ad alta disponibilità connesso tramite ISDN con flussi primari alla rete Telecomitalia riceve le chiamate telefoniche degli utenti e provvede a generare il messaggio vocale interrogando il database che contiene il flusso logico di quesiti utili ad arrivare ad una efficace diagnosi del problema. L'utente interagisce con il sistema, dando risposta alle domande attraverso la semplice pressione dei tasti della tastiera telefonica; il sistema riconosce i toni e provvede a selezionare il percorso di helpdesk previsto dal flusso logico.

Il sistema di gestione telefonica è composta da:

- uno switch ISDN che deriva da un flusso ISDN primario e 8 flussi ISDN base
- due server di front end telefonico con ciascuno 2 interfacce ISDN base

I server sono duplicati per consentire aggiornamenti degli applicativi senza interruzione del servizio.

Su ogni server si utilizza un "motore" di Computer Telephony che utilizza i protocolli MS TAPI verso le schede telefoniche e MS SAPI verso il motore di sintesi in lingua italiana.

La sintesi vocale nasce dall'esperienza più che ventennale dei laboratori Csel (attualmente Loquendo) di proprietà di Telecomitalia.

que sempre replicate in tempo reale sui server LDAP localizzati al CINECA e dedicati all'autenticazione.

Documentazione e HelpDesk automatizzato

Oltre a tutta la documentazione sulle modalità di utilizzo, fruibile via web, il sistema prevede per l'utenza finale funzioni automatizzate per verificare autonomamente lo stato del servizio. Un supporto automatico di diagnosi, raggiungibile anche mediante accesso telefonico di tipo tradizionale, è in grado di guidare l'utente alla soluzione del problema attraverso una serie di domande volte ad individuarne la soluzione limitando ad ogni passo il numero delle possibili cause.

Interfaccia web e strumenti di self-management per l'utenza

Oltre che attraverso client di posta tradizionali, l'accesso alla propria casella di posta e a tutte le funzionalità disponibili può avvenire anche attraverso interfaccia web. Attraverso la stessa interfaccia, l'utente ha accesso a funzioni quali: attivazione di mail forwarding verso altro indirizzo, verifica occupazione dello spazio disco disponibile, gestione rubrica personale e variazione della password di accesso.

Liste di distribuzione

Mediante l'utilizzo della classificazione dell'utenza operata dalle Università all'interno del proprio directory server, il sistema costruisce automaticamente liste di distribuzione utili per l'invio di comunicazioni a gruppi ben definiti di utenti. Il raggruppamento può ad esempio avvenire per facoltà o corso di laurea. Le liste specializzate costituiranno un canale comunicativo rapido ed efficiente, con cui il corpo docente ed il personale amministrativo dell'Ateneo potranno inviare comunicazioni a determinati sottoinsiemi dell'utenza.

Nel momento in cui l'articolo viene scritto, stanno formulando l'adesione al servizio le Università di Bologna, Firenze, Parma, Urbino e l'Osservatorio Astronomico di Bologna.

Con l'ambizione di offrire una soluzione di messaging completa, il CINECA continuerà nei prossimi mesi lo sviluppo dell'attuale piattaforma, completandone l'integrazione con altri strumenti quali SMS, Voice Mail e servizi Antispam.

Per ulteriori informazioni:
hermes@ceneca.it