Housing e Hosting – il SERVIZIO

Febbraio 2010

INTRODUZIONE

La gestione dei servizi ICT e dei Sistemi Informatici ha assunto negli ultimi anni un peso sempre crescente in tutti gli ambienti, sia in quelli legati alla ricerca, con i quali il consorzio coopera per missione istituzionale, sia nell'industria e nelle realtà produttive in generale.
Il CILEA, grazie alla propria esperienza trentennale nella gestione di hardware e software, può offrire competenze altamente specializzate per le diverse realtà che intendano affidare in outsourcing, in parte o completamente, la gestione delle loro macchine e dei loro servizi ICT.

Il consorzio è dotato di un Data Center, la cui estensione supera i 700 m^2 ed è in grado di fornire tutta una serie di servizi ICT indispensabili, nel loro insieme, per garantire un elevato livello nell'affidabilità e disponibilità delle applicazioni che può ospitare.
I servizi offerti a terze parti, in termini di ospitalità o *housing,* sono raggruppabili in alcune macro-aree e combinabili secondo le esigenze del Cliente, le quali dipendono anche dalla natura degli applicativi che si vogliono localizzare nel Data Center CILEA.
Le scelte tecnologiche ed i costi sottesi dipenderanno dalla maggior o minor criticità dei servizi ospiti.

Le caratteristiche tecniche delle componenti utili o necessarie ad un servizio di ospitalità saranno dettagliate nei paragrafi seguenti, che illustrano le sfaccettature dell'offerta CILEA, ma sono riassumibili in questo elenco di possibili esigenze del Cliente:

- **Logistica**: disponibilità di spazio fisico nel DataCenter (in rack o anche area su tavolo).
- **Connettività**: accesso alla rete Internet a banda larga
- **Sicurezza informatica**: firewall in alta affidabilità, VPN, IDS, AAA
- **Monitoraggio e Gestione**: allarmi, controllo funzionale, supporto sistemistico ed operativo
- **Backup**: salvataggi centralizzati su robot
- **Storage**: disponibilità di SAN a cui connettere i propri servizi
- **Virtualizzazione**: ambienti di server virtuali in HA su un cluster di macchine ad alte prestazioni
- **Disaster recovery site**: sito alternativo per il disaster recovery di servizi strategici.

LA PROPOSTA DI HOUSING E HOSTING

La necessità di disporre di ambienti che garantiscano l'**alta affidabilità e la continua accessibilità** in rete per i propri servizi è uno dei fattori che impongono, a chi fornisce i servizi di ospitalità, di mantenere e di progettare tutta una serie di accorgimenti tecnici atti a garantire un adeguato livello di servizio al committente. Questo approccio impone vincoli sulle attività di manutenzione ordinaria e spesso costose scelte di duplicazione, ove possibile, di apparati e reti per garantire una disponibilità persistente.

Vediamo nel dettaglio in cosa consiste questo tipo di offerta per le diverse aree del Data Center. Tra le componenti proposte il Cliente potrà scegliere quelle che più si addicono alle proprie esigenze di servizio.

Area Logistica

- **Sicurezza logistica e fisica**: ambiente strettamente controllato, con accesso ai locali attraverso varchi protetti da porte blindate, dotate di lettore di badge, allarmi anti-intrusione e sistema di video-sorveglianza CCTV. L'intera struttura CILEA è sottoposta a controllo continuo h24x365 da parte di un istituto di sorveglianza con guardia armata e portierato diurno.
- **Sicurezza di alimentazione elettrica**: l'intero stabile CILEA è protetto dai blackout grazie ad un sistema integrato di batterie tampone (UPS) e gruppo di continuità con alimentazione diesel. La protezione è in grado di garantire continuità di funzionamento anche a fronte di severe e prolungate interruzioni di alimentazione elettrica nella cabina ENEL, ed in pratica senza reali limiti temporali. Tutti i sistemi considerati critici sono ulteriormente protetti tramite un sistema di alimentazione ridondato, *hot-swappable*, che consente di mantenere attivo il servizio – tramite gruppo di continuità

– anche a fronte di necessità periodiche di fermi elettrici programmati per la manutenzione degli impianti, grazie ad una doppia linea di alimentazione elettrica.

- **Sicurezza antincendio e antiallagamento**: sono presenti ovunque, ed in particolare nella sala macchine, sensori antifumo ed antiallagamento per consentire interventi tempestivi in situazioni di potenziale pericolo.
- **Controllo climatico**: un impianto di climatizzazione centralizzato garantisce temperatura ed umidità controllate e costanti (temperatura Sala Macchine mantenuta tra i 19° e 22°).

Connettività

Il servizio di Housing/Hosting è rivolto a qualsiasi tipologia di cliente. Tuttavia, la natura dei servizi offerti e dell'ente che richiede l'ospitalità determina quale delle due reti CILEA verrà utilizzata per rendere visibile il servizio in housing/hosting ad Internet:

- **Clienti "istituzionali:** rete GARR per enti affiliati al Ministero della Università e Ricerca, Ministero della Pubblica Istruzione, Ministero per i Beni e le attività Culturali. La rete GARR si connette al POP GARR di Milano in fibra a 100Mbps (Infracom)."
- **Clienti "business":** rete LUCIA per gli enti che non rientrano nelle categorie GARR. La rete Lucia è connessa ad Internet attraverso un link in fibra 100Mbps sul POP di I.Net-British Telecom.
- **Clienti "all":** possibilità di richiedere VPN Fastweb per connessioni L3 point-to-point 10Mbps, con routing autonomo.

Le due reti LUCIA e GARR sono fisicamente distinte e non interscambiabili per utenti business.

Per gli utenti istituzionali esiste invece la **possibilità di configurare il doppio provider Internet** con bilanciamento mediante firewall, aumentando così l'affidabilità del servizio, che resta raggiungibile anche in caso di temporanea caduta del provider primario.

La connettività è integrata dai servizi di "registrazione domini" presso le autorità competenti per i vari Top Level Domain .it, .eu, .info, .com, .org, .net., nonché dal supporto della risoluzione diretta DNS richiesta al momento della registrazione ed attivata su due o più DNS ridondati.

Sicurezza informatica

- **Sicurezza perimetrale**: il CILEA dispone, per i suoi servizi strategici, di alcuni cluster di firewall statefull ad elevata protezione ed in alta affidabilità (piattaforma StoneSoft). Essi possono essere configurati per limitare gli accessi sui server in housing, su VLAN dedicate. Sono attivabili connessioni VPN IPSEC end-to-end o Client, anche verso altri vendor compatibili IPSEC. In alternativa, sono anche configurabili access-list per il filtro di pacchetti (stateless), sui router di frontiera.
- **Sicurezza del software**: viene inoltre garantita una manutenzione software tempestiva e continua di tutti i sistemi operativi e pacchetti coinvolti nell'erogazione dei servizi. Essa prevede l'applicazione delle *patch* di sicurezza e delle correzioni di errori funzionali, secondo uno schema di interventi che si articola in brevi sospensioni del servizio, qualora esso non sia ridondato su più piattaforme in cluster, in orari e giorni opportuni, concordati con il Cliente.
- **Antivirus ed antispam**: sono attivi per tutti i server della **mailfarm CILEA**, che è un altro servizio disponibile per il Cliente di Housing, e possono essere comunque richiesti anche per server di posta in-house
- **Security assessment**: il CILEA può effettuare test di vulnerabilità su sistemi o reti di terzi, anche in-house, previa richiesta/autorizzazione.
- **Sistemi di autenticazione e autorizzazione centralizzati**: integrazione con sistemi di autenticazione Active Directory, LDAP o Radius. In particolare, per quanto riguarda il Single Sign On per applicazioni web, il CILEA ha adottato i due protocolli che sembrano maggiormente diffusi, sopratutto in ambito accademico, e facilmente integrabili nelle più svariate realtà: CAS e Shibboleth. CILEA partecipa, come Identity Provider e Service Provider, al progetto **GARR Idem** di autenticazione federata AAI.

Monitoraggio e gestione

- **Monitoraggio servizi ed apparati**: è attivo un sistema di monitoraggio per i servizi e sistemi, che genera allarmi acustici localmente, oltre ad inviare e-mail e/o sms a gruppi o singoli destinatari, a fronte di eventi configurabili. Le linee di trasmissione dati e le LAN interne sono inoltre monitorate per porta, rispetto a volume di traffico o errori, a fini statistici o per rilevare condizioni anomale. Il servizio di monitoraggio consente un rapido intervento a fronte di problemi (entro 30 minuti dalla segnalazione) in tutti i giorni lavorativi negli orari di presidio, ed entro tre ore fuori da tale fascia, se richiesta un'ulteriore copertura oraria.
- **Gestione**: è a disposizione personale sistemistico per il supporto sulle diverse piattaforme operative, in orario d'ufficio. Alcuni servizi di intervento on-site immediato, quali spegnimenti o riavvii, media-change (CD o nastri), accesso ed accompagnamento al DataCenter, possono essere richiesti al personale tecnico/operativo presente secondo i turni di presidio seguenti:
    - Ore 7-22.30 nei giorni feriali (salvo il mese di Agosto e Dicembre a orario parzialmente ridotto)
    - Ore 7.30-13.30 nei sabati non festivi

L'accesso fisico alla sala Housing è consentito al Cliente, per motivi di sicurezza, solo negli orari di presidio, salvo richieste per necessità particolari, da concordare.

Backup

Il backup robotizzato centralizzato è un sistema dedicato composto da hardware e software per il salvataggio di dati e sistemi, tramite una rete locale ad hoc o condivisa con altre applicazioni. Nel caso del CILEA ha le seguenti caratteristiche:

- un **server di backup centralizzato**, SUN v880 con sei dischi interni da 36GB, 3 schede di rete (una Ethernet 10/100 e due GigaEthernet), due schede Fiber Channel (FC) connesse ai due switch della Storage Area Network (SAN) del CILEA;
- una **libreria Adic** i2000 con quattro Driver LTO2 e due LTO4, 400 Slot attivi e quattro schede FC connesse ai due switch SAN.
- capacità di libreria da un minimo di 160TB fino ad un massimo di 640TB.

La connessione della libreria al *server* di *backup* è effettuata mediante due canali FC, questo permette un flusso di dati ottimale dal *server* alla libreria, ma **consente anche di avere un flusso di dati dai dischi SAN alla libreria, diretto su fibra anziché su rete** (*LAN free backup*).

Sono concordabili con il cliente i seguenti aspetti:

- cadenza dei salvataggi,
- tipologia di salvataggio (completo, incrementale, differenziale, raw device),
- tempi di mantenimento/ritenzione dei salvataggi effettuati
- cassette dedicate
- possibilità di conservazione dei nastri presso altra sede

In particolare la **salvaguardia delle Basi Dati** è garantita anche da diverse e parallele modalità di *backup*:

- ***backup totale* (di sistema e dati) a cadenza settimanale**, del *server* o dei *server* che ospitano la base dati, con ulteriori 6 *backup* incrementali giornalieri, mediante il sistema centralizzato e robotizzato (nel caso si effettui backup a freddo sarà necessario il fermo del *DBMS* almeno una volta la settimana in corrispondenza del *backup* totale notturno, ma solo per il tempo necessario alla copia disco-disco). Il *backup* centralizzato mantiene in linea gli ultimi 4 set di salvataggi, che coprono quindi un arco temporale di 4 settimane, salvo accordi differenti;
- ***backup* dei soli dati mediante *export*** del database, o altre modalità previste dall'*DBMS* utilizzato (ad es. backup incrementali o totali a caldo), cadenzato ogni 12/24 ore, e archiviato su supporti

differenti da quelli che ospitano i dati in linea (dischi alternativi, *fileserver* o *SAN* esterne). Tali *export* potranno essere oggetto di ulteriori salvataggi robotizzati con cadenza da definire sulla base delle effettive necessità.

- ***Archiviazione del log delle transazioni*** *su dischi alternativi,* qualora il software DBMS lo consenta. In taluni casi viene effettuata copia automatica dei dati di archive (redo.log archiviati) sul disaster recovery site (ad. Es. mediante **feature DataGuard Oracle, log-shipping MSSQL**), per garantire un allineamento più efficace dei due site.

Storage Area Network (SAN)

Il CILEA dispone di una Storage Area Network, basata su tecnologia Fiber Channel e in cui risiedono, oltre alla Tape Library del sistema di backup centralizzato, un Disk System IBM DS4800 da 23TB e un Disk System Nexsan SATABeast da 42TB.

Virtualizzazione

E' attiva una **server farm di sistemi VMware ESX 3.x**, che si appoggia a uno degli elementi di SAN CILEA, per garantire l'alta affidabilità dei servizi realizzati in virtuale. Ciò è reso possibile grazie ai moduli VMware che consentono sia la **High Availability** automatica, sia il cosiddetto **V-Motion**, ovvero la possibilità di spostare, ad esempio per interventi di manutenzione, Macchine Virtuali da un sistema fisico ad un altro, senza dovere disattivare il servizio virtuale e con perdite minime durante il trasferimento (qualche pacchetto IP). I sistemi ospiti possono essere Windows o Linux RedHat (e altre distribuzioni).

Sono allo studio anche altri motori di virtualizzazione, per valutarne costi, performance e gestibilità. Anche il numero dei sistemi fisici coinvolti nel cluster è in crescita, proprio per aumentare le capacità elaborative di un ambiente che sta diventando cruciale per lo sviluppo della gestione sistemi.

Disaster Recovery Site

Il CILEA di Milano dispone, per alcune necessità particolari, di un **sito per il Disaster Recovery**, mantenuto presso la propria sede di Roma.

E' stata realizzata la duplicazione dei server di Front-end web, nonché del server Oracle di Back-end allineato con il DB di produzione mediante la funzione di **Data Guard in Oracle 10G**.

Una soluzione del tutto analoga è stata predisposta per realizzare un sito alternativo a quello di produzione, in ambiente **MSSQL 2005**, mediante mirroring di tipo asincrono (log-shipping).

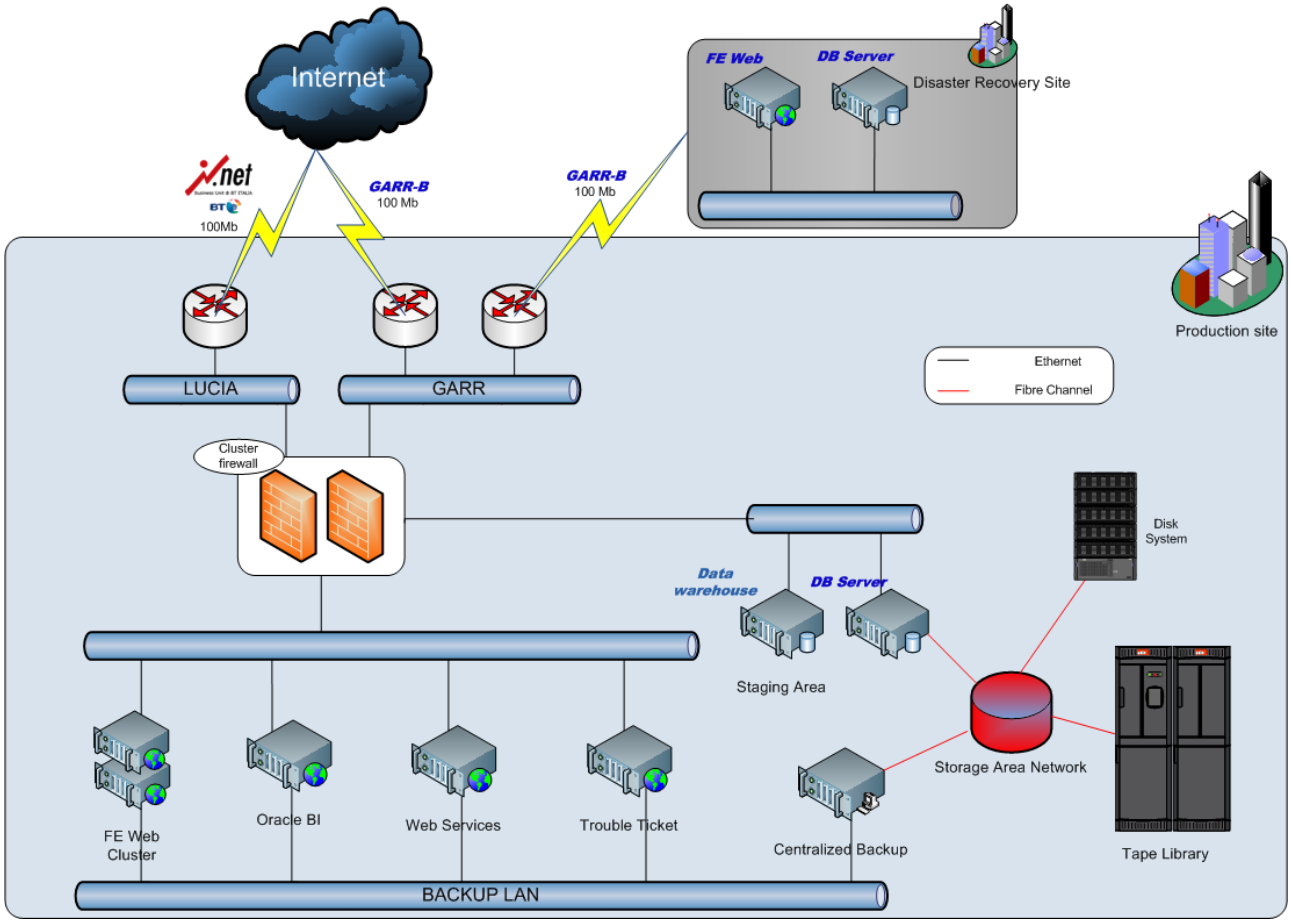
La sede di Roma è autonoma per quanto riguarda la connettività internet a 100Mbps ed è pianificata la sua ridondanza con due link in fibra a 100Mbps su due POP GARR distinti, gestiti in BGP.

ARCHITETTURA DI UN POSSIBILE MODELLO DI HOUSING

Il taglio di ogni proposta di housing dipende strettamente dalle necessità del Cliente e può variare notevolmente, sia rispetto a scelte tecnologiche, sia ai relativi costi. Potranno esserci necessità di ospitalità per applicazioni non mission-critical, pur restando importanti per il marketing o per la visibilità ed immagine del Cliente, o viceversa potranno esserci necessità di gestione di applicativi complessi con contenuti informativi strategici, per i quali è vitale la continua accessibilità e la preservazione da possibili perdite.

Lo schema a grandi blocchi dell'architettura hardware che configura un possibile scenario di housing di questo secondo tipo, per servizi applicativi e Data Base collegati, è rappresentato in Figura 1, dove si prevede una ridondanza sia a livello di firewall, sia di provider Internet, sia sui front-end web, mentre la componente di Data Base è ridondata oltre che con archiving locale, anche sul Disaster Recovery Site, nel quale si colloca un ambiente completamente duplicato e pronto per l'attivazione in produzione, in caso di effettivo disastro sul sito primario.

Figura 1



CHI CONTATTARE

Per maggiori informazioni su CILEA, le sue iniziative e i prodotti, potete consultare il sito internet all'indirizzo:

http://www.cilea.it

Sempre sul sito verranno pubblicate le novità e le evoluzioni del servizio Housing ed Hosting.
Per ogni esigenza è possibile contattare direttamente la Sezione Sistemistica Tecnica CILEA e in particolare i referenti del servizio di Housing.

I riferimenti:

Ing. A. Mattasoglio: responsabile della Sezione
mattas@cilea.it – Tel. 02269951

Dr.ssa P. Tentoni: coordinatore servizio housing e di sala macchine
tentoni@cilea.it – Tel. 02269951