]HackingTeam[| ING DIRECT

ING Direct

Soluzione di load balancing per il portale www.ingdirect.it

Allegato tecnico all'offerta

Milano

Hacking Team S.r.l.	http://www.hackingteam.it
Via della Moscova, 13 *20121 MILANO (MI) - Italy*	info@hackingteam.it
Tel. +39.02.29060603	*Fax +39.02.63118946*

STORIA DEL DOCUMENTO		
Versione	Data	Modifiche Effettuate
1.0	28/11/2007	Prima stesura

INFORMAZIONI	
Data di Emissione	28/11/2007
Versione	1.0
Tipologia Documento	ATO
Numero Pagine	13
Numero Allegati	0
Redatto da	Federico Guerrini
Approvato da	Gianluca Vadruccio

INDICE

1 Richiesta del Cliente

ING Direct ha richiesto di formulare una proposta per il progetto ed il deployment di un sistema di load balancing, basato su tecnologia F5 BIG-IP LTM, per il proprio portale www.ingdirect.it.
ING Direct richiede che la soluzione identificata soddisfi i requisiti di seguito elencati.

- Il sistema di load balancing deve permettere il bilanciamento del carico su una batteria di più web server.
- Il sistema di load balancing deve supportare funzionalità di terminazione delle connessioni SSL.
- Il sistema di load balancing deve avere caratteristiche di alta affidabilità (HA) per il data center primario; per il data center di disaster recovery può essere costituito da una sola unità non ridondata.
- Il sistema di load balancing deve permettere il bilanciamento di altri servizi applicativi, anche ad uso interno, non necessariamente su protocollo HTTP.
- Deve essere possibile gestire e modificare la configurazione del sistema mediante tool automatici, allo scopo di semplificare i processi di inserimento e rimozione di nodi dalle batteria di server su cui viene effettuato il bilanciamento. In particolare, la rimozione di un nodo dal cluster deve avvenire in modalità *graceful*, ovvero solo dopo la corretta terminazione di tutte le sessioni attive su di esso.

ING Direct ha inoltre richiesto di indicare la possibilità di includere nella soluzione proposta le seguenti funzionalità:

- logica di content-caching che riduca il carico sui server generato da richieste per risorse statiche;
- controlli di sicurezza a livello applicativo (application level firewall).

Infine, ING Direct richiede che la soluzione proposta includa un piano dettagliato per l'integrazione, il testing ed il deployment nella propria infrastruttura del sistema di load balancing.

1.1 Organizzazione del documento

Per rispondere alle richieste del Cliente, il presente documento è organizzato come segue.
Nel paragrafo 2 (Ambiente di riferimento) vengono sintetizzate alcune informazioni sull'infrastruttura di ING Direct in cui deve essere integrato il sistema di load balancing. Il paragrafo 3 (Soluzione proposta) descrive dal punto di vista tecnologico ed architetturale la soluzione proposta. Il paragrafo 4 (Piano di attività) descrive la strategia proposta da HT per installare,

testare e mettere in esercizio il sistema di load balancing. Infine, il paragrafo 5 (Stima dell'effort) presenta una quantificazione dell'effort per lo svolgimento del piano di attività proposto.

2 Ambiente di riferimento

Questo paragrafo sintetizza alcune caratteristiche, rilevanti ai fini della proposta tecnica oggetto del presente documento, dell'ambiente in cui dovrà essere integrata la soluzione di load balancing.

- ***Topologia di rete***: il traffico che deve essere bilanciato raggiunge la rete DMZ su cui sono attestati i server attraverso un dispositivo di sicurezza perimetrale clusterizzato (si veda la figura 1). Tale dispositivo esegue NAT. La larghezza di banda del link verso internet (tramite il quale gli utenti accedono al portale di ING Direct) è di 10 Mbit/s.
- ***Rete di management***: l'infrastruttura di ING Direct comprende una rete di management dedicata.
- ***Web server***: i web server che costituiscono la batteria su cui deve essere bilanciato il traffico sono MS IIS 6.0 su piattaforma MS Windows 2003. Tutti i server hanno le medesime caratteristiche hardware. Attualmente, la batteria è costituita da tre server, ma essa arriverà a comprenderne 9. Il bilanciamento del carico fra i tre server attualmente presenti viene effettuato mediante NLB (Network Load Balancing).
- ***Stima del carico***: ING Direct ha indicato che il numero di sessioni HTTP contemporaneamente attive sul proprio portale raggiunge, in corrispondenza dei picchi di carico, valori prossimi a 1000.

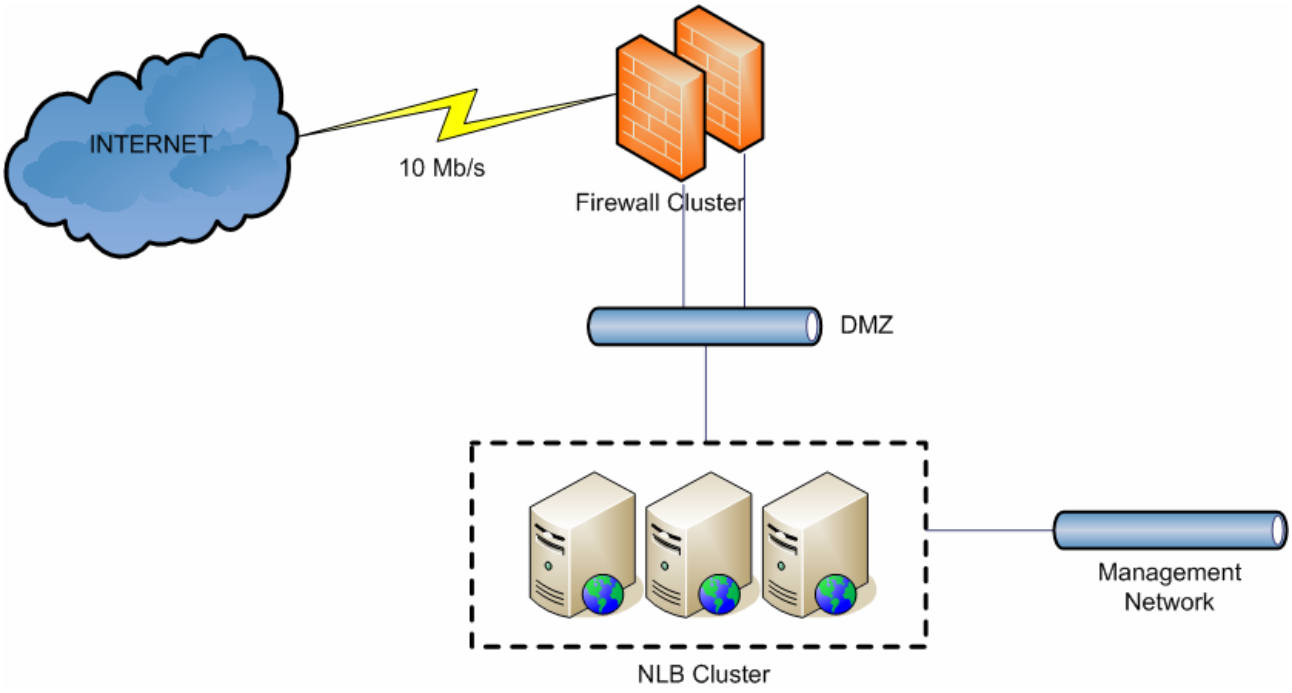

Figura 1. Architettura di rete attuale

3 Soluzione proposta

3.1 Prodotti e dimensionamento

HT ritiene che il prodotto già identificato da ING Direct, BIG-IP LTM, sia idoneo a soddisfare le esigenze descritte.

Sulla base delle indicazioni ricevute sul carico previsto e della larghezza di banda del link verso internet su cui è trasportato il carico da bilanciare, HT propone l'utilizzo di apparati BIG-IP serie 6400.

In particolare:

- ***BIG-IP Platform***:
  - ***per il sito primario***, un cluster costituito da ***due unità BIG-IP 6400***;
  - ***per il sito di disaster recovery***, ***una singola unità BIG-IP 6400***. L'opzione, percorribile dal punto di vista tecnico, di utilizzare per il sito di disaster recovery una ***unità BIG-IP 3400*** appare poco conveniente se valutata in un'ottica costi-benefici. Il minor costo dell'apparato non è sufficiente a compensare il maggiore effort di gestione che comporta l'allineamento delle configurazioni su apparti diversi (tra il sito principale e quello di disaster recovery). Sugli apparati BIG-IP 3400 non è inoltre possibile installare il prodotto ASM, per le funzionalità di application level

firewall. L'offerta economica a cui la presente proposta è allegata contiene comunque entrambe le opzioni.

- ***BIG-IP Product Module***:
  - ***BIG-IP LTM*** (Local Traffic Manager) per le funzionalità di load balancing, e terminazione SSL;
  - ***BIG-IP ASM*** (Application Security Module), opzionale, qualora si volessero includere nella soluzione funzionalità di application level firewall;
- ***BIG-IP Feature Module***:
  - ***SSL Acceleration***, per la gestione con hardware dedicato delle operazioni di cifratura SSL; HT ritiene che l'inclusione di questo modulo sia fortemente consigliabile, anche se non indispensabile dal punto di vista tecnico;
  - ***Fast Cache***, opzionale, per la gestione della logica di caching, allo scopo di ridurre il carico sui web server.

3.2 Configurazione HA

La configurazione HA proposta per il sito primario è un ***cluster BIG-IP LTM in modalità active-passive***. Tale scelta è motivata dalle seguenti considerazioni:

- ***semplicità di configurazione e di gestione***: la configurazione di un cluster active-passive è più semplice rispetto a quella di un cluster active-active e riduce l'effort sia in fase di implementazione, sia in fase di testing e successiva gestione;
- ***caratteristiche del traffico bilanciato***: ING Direct prevede di utilizzare il sistema BIG-IP LTM per bilanciare, almeno inizialmente, il traffico relativo ad un solo servizio (portale ING Direct). In questo caso, la modalità active-active non fornisce nessun vantaggio in termini di distribuzione del carico sulle due unità BIG-IP, poiché il traffico relativo ad un singolo servizio (virtual server) è sempre gestito da una sola unità;
- ***dimensionamento del sistema***: le caratteristiche hardware delle piattaforme proposte sono tali da non richiedere la distribuzione del carico su due unità;
- ***reversibilità della scelta***: se, a fronte di esigenze non previste, in termini di aumento del carico, o dei servizi pubblicati, divenisse preferibile la modalità active-active, essa potrebbe essere configurata senza modificare l'architettura del sistema (in particolare, per ridurre al minimo gli impatti di una tale modifica, è utile riservare, su ogni VLAN su cui sono attestate le unità BIG-IP, indirizzi IP supplementari da utilizzare come "floating-IP").

Per il sito di disaster recovery ING Direct ha richiesto la realizzazione di un sistema non ridondato, costituito da una singola unità BIG-IP.

3.3 Posizionamento nell'infrastruttra di ING Direct

La attuale architettura della porzioni di rete interessata dal servizio HTTP per cui si vuole realizzare la soluzione di bilanciamento è rappresentata, per il sito primario, in figura 1 (si veda il precedente paragrafo 2).

Per minimizzare gli impatti dell'introduzione nell'infrastruttura del nuovo sistema di balancing, HT propone una configurazione che permette di preservare il piano di indirizzamento esistente per la DMZ su cui sono attestati i web server. Questa configurazione è illustrata in figura 2.

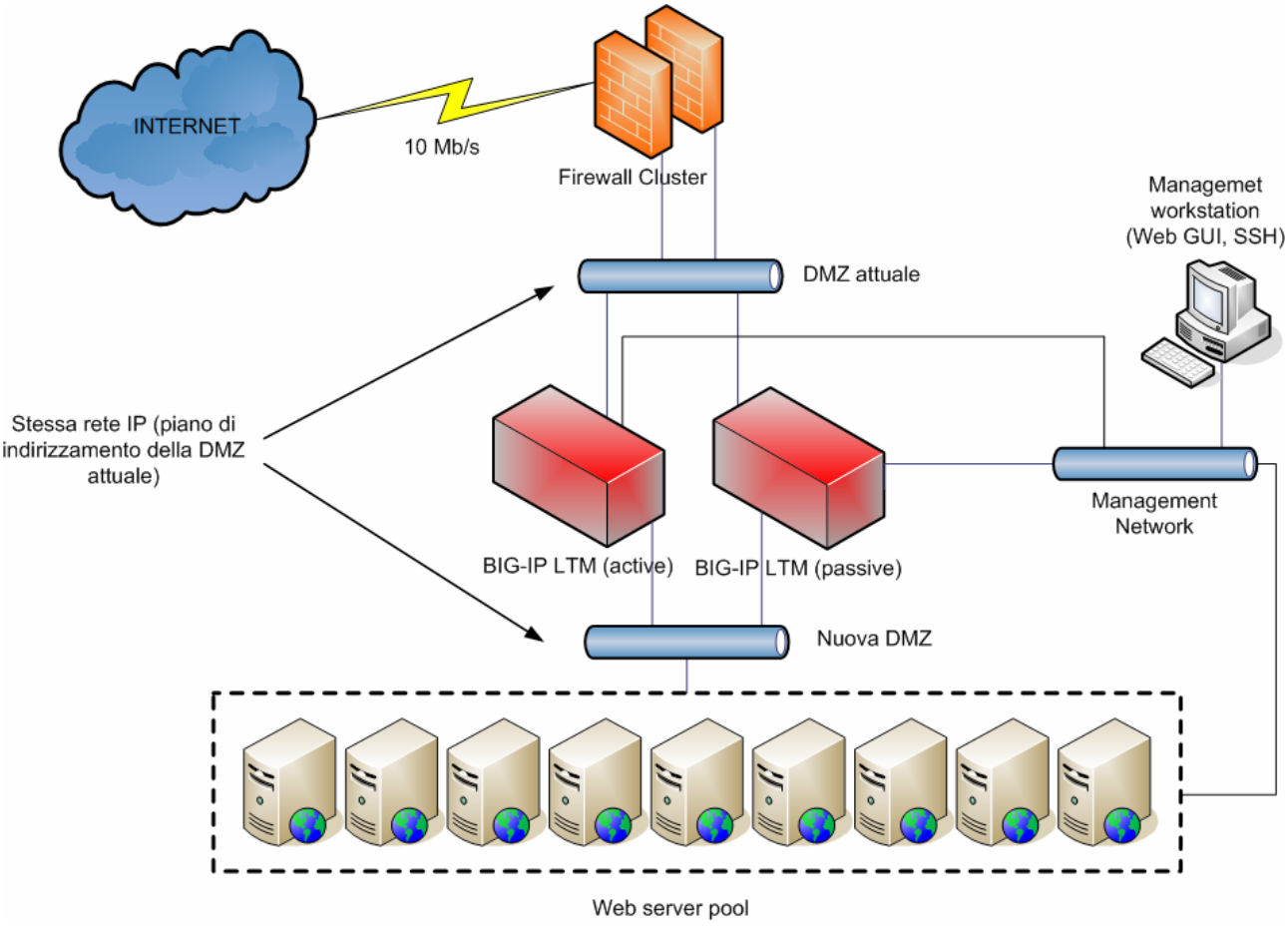

Figura 2. Architettura di rete dopo l'installazione del sistema di load balancing

Come si nota dalla figura, la configurazione proposta comporta la realizzazione di un segmento di rete separato per i server su cui deve essere effettuato il bilanciamento; tuttavia, tale segmento condivide lo spazio di indirizzamento del segmento che connette le unità BIG-IP LTM al firewall. Le unità BIG-IP LTM effettuano il *bridging* dei due segmenti (mediante definizione di due VLAN e di un VLAN group che le comprende).

Per la gestione degli apparati, si consiglia di attestare le interfacce dedicate delle unità BIG-IP sulla rete di management già presente nell'infrastruttura di ING Direct. Mediante tali interfacce gli apparati possono essere amministrati via web GUI o via connessioni SSH.

3.3.1 Livello di flessibilità della configurazione proposta

Gli apparati BIG-IP possono essere attestati su differenti VLAN, corrispondenti a spazi di indirizzamento separati. La configurazione proposta non limita quindi l'utilizzo del sistema al bilanciamento del solo traffico diretto verso la batteria di web server e proveniente dal dispositivo firewall, ma può essere utilizzato anche per la gestione di servizi/applicazioni attestati sul altre porzioni della rete ING Direct.

3.4 Gestione automatica della configurazione

La configurazione di una unità BIG-IP LTM può essere modificata in modo automatico mediante tool sviluppati *ad hoc*. Questi tool si interfacciano al sistema BIG-IP mediante una API sviluppata da F5, denominata ***iControl***, basata su protocollo SOAP trasportato su HTTPS. iControl fornisce una visione OO (Object Oriented) della configurazione di una unità e permette la modifica di tutte le impostazioni alle quali si ha accesso, in modalità interattiva, attraverso la web GUI. L'accesso ai web services esposti dall'interfaccia iControl di una unità BIG-IP avviene attraverso la rete di management.

La API iControl sarà utilizzata per realizzare un tool che permette di elencare i membri di un load balancing pool e di cambiare lo stato (abilitato/non abilitato) dei suoi membri. E' stata identificata una modalità di disabilitazione dei membri che fornisce il comportamento "graceful" richiesto da ING: nessuna nuova connessione viene rediretta su un membro che è stato disabilitato, ma esso continua ricevere traffico relativo a sessioni già attive al momento della sua disabilitazione. Il membro può essere poi rimosso dal pool quando il numero di connessioni attive su di esso diviene pari a zero (anche il test di questa condizione può essere automatizzato mediante iControl).

La presente offerta include la realizzazione di un prototipo del tool, che chiarisce l'utilizzo di iControl per automatizzare l'operazione di disabilitazione di un membro. Il tool potrà essere sviluppato, a scelta di ING Direct, in uno dei linguaggi per i quali esiste l'implementazione di iControl: Perl, Java, linguaggi .NET (C#, VB). L'offerta non comprende le attività di sviluppo necessarie per una eventuale integrazione del tool in altri prodotti di gestione delle configurazioni eventualmente utilizzati da ING Direct.

4 Piano di attività

La soluzione proposta sarà implementata, testata e messa in esercizio secondo il piano di intervento descritto nei successivi sottoparagrafi.

4.1 Installazione delle unità BIG-IP LTM

In questa fase si procederà all'installazione sui tre apparati BIG-IP dell'ultima release stabile del prodotto LTM ed alla verifica della loro corretta funzionalità.

4.2 Posizionamento nell'infrastruttura di ING Direct (sito di produzione)

Dopo aver condiviso con ING Direct (ed eventualmente modificato rispetto a quanto proposto nel paragrafo 3) la modalità di configurazione degli apparati, si procederà al loro posizionamento sulla rete per il sito di produzione.

Il piano di attività proposto ha l'obiettivo di minimizzare i rischi di disservizi sul portale ING Direct connessi al passaggio in produzione del nuovo sistema di bilanciamento. A tale scopo, la strategia che si intende proporre e condividere con i responsabili dell'infrastruttura e delle applicazioni ING Direct, è basata sui seguenti principi:

- il sistema di load balancing verrà testato utilizzando la batteria di web server che sarà poi utilizzata in produzione (tale batteria andrà quindi a sostituire quella attuale). Durante questa fase dovrà essere resa disponibile da parte di ING Direct una batteria di web server di test. Tale batteria potrà essere costituita da un numero di server inferiore rispetto a quello che sarà utilizzato a regime (ma comunque non inferiore a tre);
- il nuovo sistema di load balancing e la batteria di server saranno collocati nel medesimo spazio di indirizzamento della attuale DMZ (stessa rete IP);
- il passaggio in produzione avverrà assegnando al virtual server BIG-IP LTM l'indirizzo virtuale del cluster NLB.

Durante la fase di testing si avrà quindi la coesistenza dell'attuale ambiente di produzione e dell'ambiente di test che a regime lo sostituirà, come evidenziato nella figura 3. Per tutta la durata delle attività di implementazione e testing, le unità BIG-IP LTM pubblicheranno il pool di web server di test utilizzando un indirizzo virtuale differente da quello dell'ambiente di produzione.

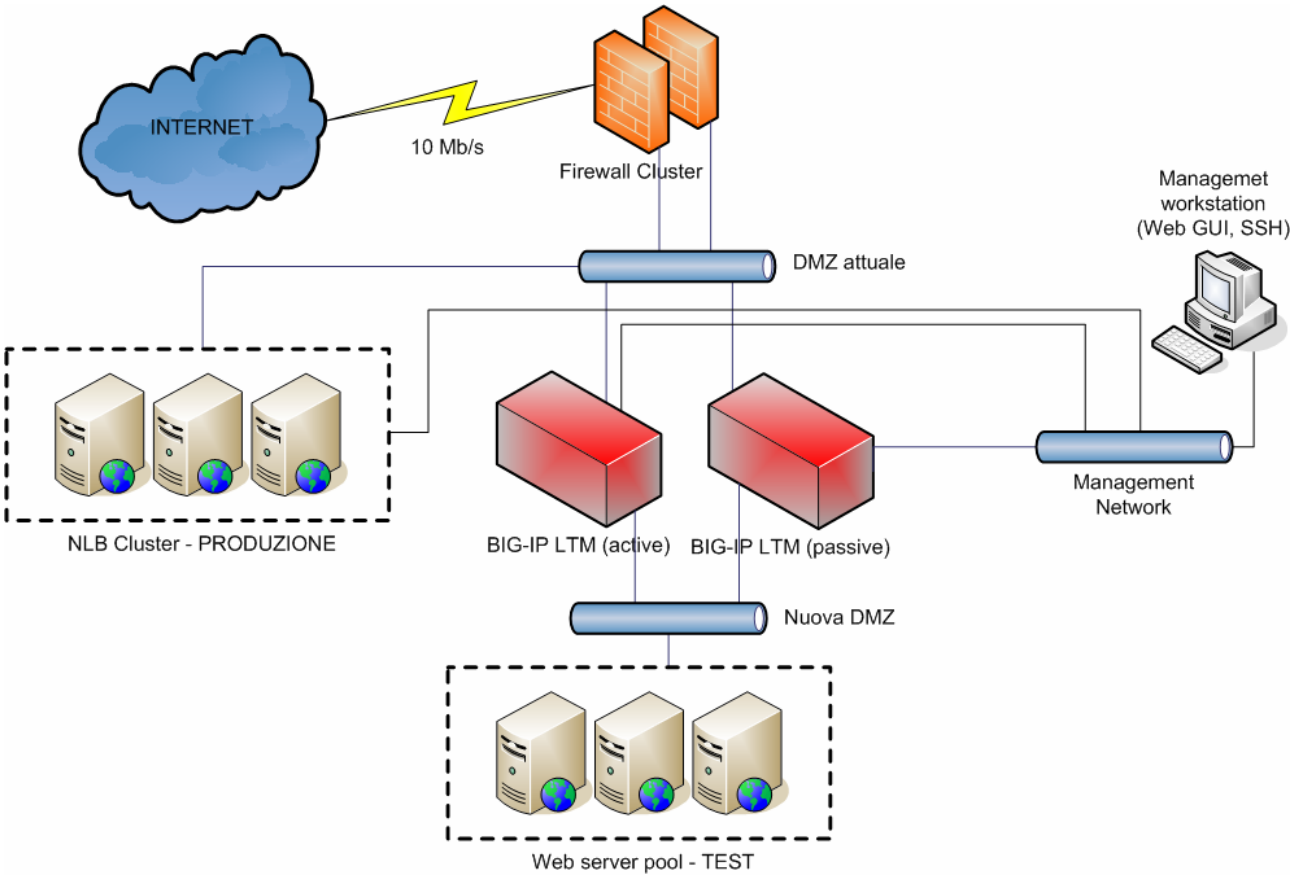

Figura 3. Architettura di rete durante la fase di implementazione e testing

4.3 Configurazione BIG-IP LTM

In questa fase si procede alla configurazione del sistema di load balancing. Le attività di configurazione riguardano i seguenti aspetti:

- configurazione cluster HA active-passive;
- configurazione VLAN e VLAN group;
- configurazione nodi, load balancing pools, virtual server: saranno provate e confrontate le numerose possibilità che LTM offre relativamente a
  - caratteristiche del virtual server (standard, HTTP performance);
  - modalità di load balancing;
  - gestione della persistenza delle sessioni;
  - monitoring di nodi e membri dei pool.

Qualora emergessero ulteriori esigenze di configurazione, esse saranno individuate e condivise con il cliente al termine di questa fase.

4.4 Testing

HT effettuerà in autonomia, per ogni aspetto della configurazione del sistema, una prima sessione di test. Lo scopo di questa sessione è la verifica che il comportamento del sistema sia quello atteso rispetto alla sua configurazione.
Dovrà essere concordata l'impostazione di una seconda sessione da svolgersi in collaborazione con il team ING Direct dedicato al testing dell'applicazione pubblicata. L'obiettivo di tale seconda sessione è garantire la copertura completa di tutte le funzionalità dell'applicazione.

4.5 Sviluppo dei tool di gestione della configurazione

Lo sviluppo del tool per la gestione automatica della rimozione di membri dal pool di load balancing sarà intrapresa non appena i risultati dell'attività di testing indichino il raggiungimento di una configurazione stabile. Le prime fasi dello sviluppo potranno essere svolte da HT presso la propria sede (non è richiesto l'accesso al sistema di load balancing).

4.6 Allineamento del sito di disaster recovery

Sull'unità BIG-IP LTM dedicata al sito di distaster recovery sarà riportata la configurazione definitiva identificata per il sito di produzione (compatibilmente con le differenze esistenti a livello hardware fra i due siti).

4.7 Rilascio in ambiente di produzione

Le modalità di rilascio in produzione dovranno essere approfondite con i responsabili per ING Direct dell'esercizio dell'applicazione.
Il piano di intervento proposto mira a rendere possibile il passaggio in produzione mediante assegnamento al virtual server F5 dell'indirizzo IP virtuale attualmente assegnato al cluster NLB (o mediante intervento equivalente sul firewall). Tuttavia, la fattibilità e i dettagli di una tale procedura dovranno essere verificati anche a fronte di una analisi più dettagliata dell'interfaccia fra font-end HTTP dell'applicazione e data layer.

4.8 Collaudo

Le attività si concluderanno con la formale accettazione, da parte di ING Direct, della soluzione realizzata.

5 Stima dell'effort

La seguente tabella riporta una stima dell'effort previsto per le attività descritte. Tale stima viene riportata con il solo scopo di fornire una indicazione sul tempo necessario per realizzare la soluzione. La presente proposta tecnica sarà oggetto di offerta commerciale a corpo.

Attività	***Effort (gg/u)***
Installazione delle unità BIG-IP LTM	1
Posizionamento nell'infrastruttura di ING Direct (sito di produzione)	1
Configurazione BIG-IP LTM	1
Testing	3
Sviluppo dei tool di gestione della configurazione	3
Allineamento del sito di disaster recovery	1
Rilascio in ambiente di produzione	3
Collaudo	1
Totale	***14***

Tabella 1. Effort stimato