UNIVERSITÀ DEGLI STUDI DI CAMERINO

FACOLTÀ DI SCIENZE E TECNOLOGIE

Corso di Laurea in Informatica

Dipartimento di Matematica e Informatica

FAULT TOLERANCE APPLICATO ALLA MODALITÀ DI ACCESSO ALLA STRUTTURA DI POSTA ELETTRONICA CERTIFICATA DI NAMIRIAL S.P.A.

Laureando

Matteo Sartini

Relatore

Prof. Fausto Marcantoni

Correlatore

Gabriele Vitali

Anno Accademico 2011/ 2012

INDICE

INTRODUZIONE

Il lavoro di questa tesi è il frutto di uno stage aziendale effettuato presso l'azienda Namirial S.p.A. di Senigallia (AN), una società informatica che, tra le varie attività, svolge quella di gestore accreditato di **Posta Elettronica Certificata** (PEC).
La PEC, sulla base della normativa vigente (*D.M. 2/11/2005*), è un sistema attraverso il quale è possibile inviare e-mail con valore legale equiparato ad una raccomandata con ricevuta di ritorno.
Il servizio di PEC deve rispettare e garantire alcuni livelli minimi di servizio al fine di poter essere erogato ai propri clienti in maniera efficiente, efficace e continuativa nel tempo.
Per garantire il livello richiesto dalla normativa, i gestori pertanto devono dotarsi di sistemi ed infrastrutture capaci di tollerare malfunzionamenti ed evitare il verificarsi di guasti che compromettano il funzionamento dell'intero servizio di PEC.
Devono perciò essere realizzati sistemi e infrastrutture Fault-Tolerant (tolleranti ai guasti) in grado di continuare ad operare correttamente nonostante si verifichino fallimenti ad una o più componenti del sistema (Business Continuity)[1].

L'obiettivo della tesi è dunque quello di studiare, analizzare e verificare mediante procedure di testing, la tolleranza ai guasti nella struttura di accesso ai servizi di PEC del gestore Namirial e mettere in evidenza come gli studi teorici non sempre trovano riscontro nella realtà lavorativa in quanto fattori come i costi delle infrastrutture, gli spazi fisici, il personale tecnico amministrativo, incidono in maniera significativa sulla scelta delle soluzioni da implementare.

[1] Capacità dell'azienda di continuare ad esercitare il proprio business a fronte di eventi avversi che possono colpirla.

Nel primo capitolo vengono presentati i sistemi Fault-Tolerant, partendo dalla descrizione dei concetti generali e correlati (come ad esempio "Affidabilità", "Disponibilità" e "Ridondanza" di un sistema), proseguendo con degli scenari di applicazione e concludendo con alcune soluzioni Fault-Tolerant in ambito informatico.

Nel secondo capitolo viene presentato il servizio di Posta Elettronica Certificata partendo dalla descrizione generale del servizio di PEC (che cos'è, i soggetti che vi operano e l'uso del servizio) e dalla descrizione in termini di servizi forniti ed obblighi del gestore (sulla base della normativa vigente), proseguendo con le modalità di accesso al servizio di PEC e concludendo con alcune considerazioni circa le caratteristiche generali dei servizi ICT[2], la loro individuazione e misurazione e gli accordi sulle garanzie dei livelli di servizio (Service Level Agreement).

Nel terzo capitolo viene analizzata un'infrastruttura logica di accesso al servizio di PEC. Si partirà da una configurazione completamente intollerante ai guasti sino ad ottenere un'infrastruttura Fault-Tolerant ideale, la quale verrà poi confrontata con l'infrastruttura del gestore. Conclude il capitolo la descrizione delle procedure di test effettuate sull'infrastruttura per verificarne la tolleranza ai guasti.

Il lavoro si conclude riportando, nel quarto capitolo, le schede contenenti gli esiti dei test effettuati, le relative considerazioni sui risultati ottenuti e le conclusioni del lavoro svolto in termini di sviluppi futuri offerti dagli scenari applicativi descritti e le motivazioni che hanno portato alla realizzazione dell'infrastruttura esistente.

[2] Insieme dei metodi e delle tecnologie che realizzano i sistemi di trasmissione, ricezione ed elaborazione delle informazioni (tecnologie digitali comprese).

1 SISTEMI FAULT-TOLERANT

La tolleranza ai guasti (dall'inglese Fault-Tolerance) è la capacità di un sistema di non subire fallimenti anche in presenza di guasti. Con il termine "Fault-Tolerant" si identifica un sistema in grado di continuare ad operare correttamente nonostante si verifichino fallimenti ad una o più componenti del sistema stesso. In altre parole si tratta di un sistema che tollera malfunzionamenti nei suoi componenti pur mantenendo proprietà di performance desiderate e stabilità.[15]
Dopo aver introdotto alcuni cenni storici sul concetto di Fault-Tolerance, verranno definiti vari concetti, quali il significato di guasto (fault), errore (error) e fallimento (failure), di affidabilità e disponibilità di un sistema e la ridondanza. In secondo luogo, dopo aver elencato alcuni esempi di scenari di applicazione del Fault-Tolerance, verranno indicate alcune soluzioni esistenti in ambito informatico, che garantiscono continuità di servizio in caso di guasti.

1.1 Cenni storici

Il primo a fornire una precisa definizione di sistemi tolleranti ai guasti fu A. Avizienis nel 1967, affermando che *un sistema è detto Fault Tolerant se i suoi programmi possono essere eseguiti in modo corretto nonostante l'occorrenza di guasti fisici*. Questa definizione fu il risultato di tre principali filoni di studio convergenti tra loro. Innanzitutto l'utilizzo dei primi calcolatori rese evidente il fatto che, nonostante un attento sviluppo del sistema e l'utilizzo di componenti di buona qualità, i difetti fisici e gli errori di progetto erano inevitabili. Così i progettisti dei primi calcolatori iniziarono ad utilizzare tecniche pratiche per aumentare l'affidabilità: [1]

- costruirono architetture ridondanti per mascherare i componenti danneggiati;

- fecero riferimento a tecniche diagnostiche per individuare dove fossero i guasti;
- crearono duplicati dei principali sottosistemi con cui sostituire automaticamente quelli danneggiati.

In parallelo all'evoluzione di queste tecniche alcuni pionieri dell'informatica, come John Von Neumann, Edward Moore e Claude Shannon, affrontarono il problema di costruire un sistema affidabile a partire da componenti che non lo erano.
Nel 1958 la NASA diede un gran contributo quando, al Jet Propulsion Laboratory[3] (JPL), iniziò a studiare come costruire astronavi prive di equipaggio per l'esplorazione interplanetaria. Per queste missioni si dovevano realizzare dei calcolatori in grado di resistere ad un viaggio di parecchi anni e che continuassero a fornire alte prestazioni nella profondità dell'universo. In seguito a questi studi, JPL e IEEE[4] realizzarono la prima conferenza sul calcolo con tolleranza ai guasti nel 1971.
Nel 1978 IBM introdusse un esempio di architettura volta ad aumentare l'affidabilità di un dispositivo di memoria di massa, brevettando un sistema per il recupero dei dati memorizzati in unità di memoria danneggiate. In seguito, nel 1988, David A. Patterson, Garth A. Gibson and Randy Katz, presso l'università della California, introdussero il termine di RAID [8], pubblicando un documento intitolato "A Case for Redundant Arrays of Inexpensive Disks (RAID)", che racchiudeva lo studio relativo alla possibilità di far apparire nel sistema due o più dischi come un'unica unità di storage dei dati, aumentando affidabilità e performance nella memorizzazione delle informazioni. Dal quel momento in poi sono stati progettati e sviluppati diversi livelli di RAID che permettono tutt'oggi di memorizzare dati mediante sistemi maggiormente affidabili e con prestazioni più elevate.
Un'altra soluzione affidabile e ad alte prestazioni che si è sviluppata negli anni è l'architettura cluster. Il suo scopo è quello di distribuire il

[3]Il Jet PropulsionLaboratory (JPL) del "California Institute of Technology" è un laboratorio statunitense, nei pressi di Pasadena, in California.
[4]Lo IEEE, acronimo di Institute of Electrical and Electronic Engineers (in italiano: Istituto degli ingegneri elettrici ed elettronici) è un'associazione internazionale di scienziati professionisti con l'obiettivo della promozione delle scienze tecnologiche.

trattamento del dato tra gli elaboratori componenti il cluster, in modo da velocizzare le operazioni, migliorare le performance e aumentare l'affidabilità del sistema.
Per riassumere nel migliore dei modi la storia del cluster facciamo riferimento ad una nota nel libro "*In Search of Clusters"* di Greg Pfister:[16]
«*Virtualmente ogni dichiarazione rilasciata dalla DEC*[5] *che menziona i cluster dice: DEC, che ha inventato i cluster.... Non li ha inventati neanche IBM. Gli utenti hanno inventato i cluster, dal momento che non potevano portare avanti tutto il loro lavoro su un solo computer, o necessitavano di un backup. La data dell'invenzione è sconosciuta, ma penso che sia durante gli anni '60, o anche alla fine dei '50.*»
Nel 1967, Gene Amdahl della IBM pubblicò un articolo che esponeva la cosiddetta "Legge di Amdahl": si tratta di una legge che descrive matematicamente l'aumento di prestazioni che si può ottenere compiendo un'operazione in una architettura in parallelo. Tale legge viene considerata la base del calcolo parallelo.
Col tempo, i sistemi cluster sono stati sviluppati fino ad arrivare a garantire alta affidabilità in caso di malfunzionamenti o guasti. I cluster di alta affidabilità (cluster High Availability) sfruttano la ridondanza delle sue componenti (dispositivi hardware, software, dislocazioni geografiche e risorse umane) che forniscono la continuità di servizio. Possono essere realizzate architetture cluster di tipo:

- Active/Active, dove il traffico e l'elaborazione dei dati viene bilanciato su tutti i dispositivi;
- Active/Passive dove il dispositivo in stato "passive" subentra nell'elaborazione qualora il dispositivo in stato "active" presenti un guasto.

Negli ultimi anni si è andato via via sviluppando un altro concetto parallelo al cluster: il *Cloud Computing*. Sebbene la sua definizione generi pareri discordanti (c'è chi lo ritiene l'evoluzione di Internet, chi una trappola di

[5] industria pionieristica del settore informatico negli Stati Uniti d'America

carattere commerciale [17]), possiamo definirlo come un insieme di tecnologie che permettono, tipicamente sotto forma di un servizio offerto da un provider al cliente, di memorizzare, archiviare, elaborare dati grazie all'utilizzo di risorse hardware/software distribuite e virtualizzate in rete. Rappresenta, in altri termini, la convergenza di una serie di tecnologie che si sono sviluppate negli ultimi trent'anni (tra cui la virtualizzazione). Nonostante il successo che questa tecnologia sta riscuotendo negli ultimi periodi, restano ancora aperte questioni legate principalmente a:

- Sicurezza dei dati e privacy degli utenti: generalmente in un cloud non si ha mai la certezza della localizzazione del dato, perciò si è esposti ad un rischio maggiore in termini di accesso alle informazioni e privacy dell'utente.
- Problemi internazionali di tipo economico e politico: se i dati sono depositati sul territorio americano, gli organi federali statunitensi possono andare a guardarseli senza chiedere il permesso ed addirittura, se mal interpretati, inserire gli utenti in speciali liste di osservazione [18].
- Continuità del servizio offerto: delegando a un servizio esterno (anche oltre oceano) la gestione dei dati e la loro elaborazione l'utente si trova fortemente limitato nel caso in cui i suddetti servizi non siano operativi (out of service).

Indipendentemente dalle possibilità fornite dalla tecnologia, ciò che accomuna le soluzioni mirate alla tolleranza ai guasti è il corretto equilibrio tra costi di realizzazione e disponibilità economiche dei soggetti che richiedono sempre più architetture Fault-Tolerant.

1.2 Concetti generali

1.2.1 Guasti, errori e fallimenti

È importante tener presente fin d'ora che la tolleranza ai guasti non garantisce l'immunità da tutti i malfunzionamenti, ma solo che i guasti, per

i quali è stata progettata una protezione, non causino fallimenti. Se un sistema è progettato per fornire ai suoi utenti un certo numero di servizi (unitamente ad un certo livello di qualità degli stessi), il sistema fallisce quando uno o più di questi ultimi non possono più essere completamente o parzialmente erogati.
Un fallimento(failure) pertanto si verifica quando il comportamento di un componente del sistema non è conforme alle sue specifiche.
Un errore (error) è un cambiamento di stato di un componente del sistema, rispetto ai possibili stati previsti, che può portare ad un fallimento. La causa dell'errore è chiamata guasto (fault).

Sulla base di quanto premesso, si può quindi dire che guasti, errori e fallimenti sono legati alla seguente relazione:[2]

guasto → errore → fallimento

In funzione del tempo, i guasti si possono ripartire secondo la seguente classificazione [3] [4]:

- **Permanente**: un guasto continuo e stabile.
- **Intermittente**: un guasto o errore che si presenta occasionalmente e in modo instabile.
- **Transiente**: guasto o errore che è il risultato di particolari e temporanee condizioni ambientali.

In funzione della disponibilità di un servizio invece, possiamo suddividere i guasti in:

- **critici:** un guasto tale per cui l'intero servizio subisce un'interruzione e non può essere più erogato. La tolleranza in caso di interruzione è molto bassa, di conseguenza il costo di una interruzione è molto alto.
- **non critici:** un guasto tale per cui il servizio e le relative funzioni possono rimanere interrotti per un lungo periodo di tempo, con un modesto, o nullo, costo per l'azienda e si richiede un limitato (o

nullo) sforzo di ripartenza quando il servizio e le relative funzioni vengono ripristinati.

I guasti possono essere ulteriormente suddivisi in:

- **guasti hardware:** i guasti risultanti da hardware mal funzionante, design errato dell'hardware o da ripetitive condizioni ambientali. Sono tutti potenzialmente riconoscibili e riparabili con sostituzioni o con un redesign. Gli errori possono essere causati proprio da guasti transienti, che rappresentano assieme ai guasti intermittenti, la maggior causa di errori in un sistema.
- **guasti software:** guasti che affliggono il software, come ad esempio programmi o dati. È importante notare che le cause che portano ad un guasto interno al sistema software sono il più delle volte per loro natura permanenti quindi, per fare un esempio, un errore di progettazione dell'applicazione (ad es. bug di sistema) porterà sempre al medesimo guasto del sistema fino a quando non si interverrà con opportune modifiche.

In generale tuttavia, i criteri di classificazione dei guasti sono di diversa natura. Alcuni studi approfonditi sull'argomento sono arrivati a definire diverse classi e tipologie di errori [19].

1.2.2 Disponibilità e affidabilità

Lo scopo di un'architettura Fault-Tolerant è quello di tollerare il guasto, cioè mitigare i suoi effetti e preservare comunque le funzionalità del sistema. Due importanti funzioni di cui bisogna tenere conto nella fase di design di un sistema, sono la disponibilità e l'affidabilità. Per disponibilità si intende la probabilità, in funzione del tempo, che il sistema sia correttamente operativo all'istante t. L'affidabilità, invece, è definita come la probabilità, sempre in funzione del tempo, che il sistema sia correttamente funzionante all'istante t, se il sistema stesso era funzionante all'istante 0. Questa funzione è utilizzata soprattutto per sistemi dove le riparazioni sono difficoltose o impossibili (ad esempio un satellite), oppure per sistemi critici, dove il tempo di riparazione non può

essere elevato (come vedremo nel caso aziendale preso in esame). In generale dunque, l'affidabilità restituisce requisiti più stringenti della disponibilità.
Ai fini dell'affidabilità, l'architettura di un sistema deve fornire quattro meccanismi fondamentali [5]:

- rilevazione degli errori;
- delimitazione e valutazione del danno;
- copertura dell'errore;
- trattamento dell'errore e ripristino del servizio.

L'ordine in cui le fasi (analizzate successivamente) sono intraprese può variare da sistema a sistema. La rilevazione degli errori è il punto di partenza usuale della tolleranza ai guasti, mentre le altre tre fasi possono trovarsi in un qualsiasi ordine, sebbene succeda spesso che la valutazione del danno preceda la copertura degli errori e il trattamento dei guasti. Comunque sia, un progettista di un sistema Fault-Tolerant dovrà in primo luogo valutare dove la tolleranza ai guasti è davvero richiesta e valutare quanto sia necessaria.

Rilevazione degli errori

Volendo tollerare un guasto di un sistema deve essere rilevato, innanzitutto, il suo effetto, andando a rilevare uno stato erroneo nel sistema.
Il successo di un sistema tollerante ai guasti dipenderà, quindi, strettamente dalle tecniche per la rilevazione degli errori utilizzate. In sostanza, tanto più efficace è la rilevazione degli errori, tanto più un sistema sarà affidabile.
Nella pratica, però, ci sono limitazioni sul numero di errori rilevabili: ad esempio i costi per attuare le soluzioni hardware e software necessarie per rilevarli.
Un approccio ideale alla rilevazione degli errori è quello di considerare un sistema (S) progettato per fornire un determinato servizio [6]. Se il comportamento di S non segue quello prescritto dalle sue specifiche,

allora S si trova in uno stato erroneo. Poiché lo scopo della tolleranza ai guasti è quello di prevenire i guasti ne consegue che adeguate misure per la rilevazione degli errori possono essere basate nell'intercettare i valori di uscita di S e di verificare se tali valori sono o no conformi alle specifiche. Di fatto, ci si trova di fronte ad un nuovo sistema S' composto da S e da componenti aggiuntivi aventi lo scopo di compiere la verifica.

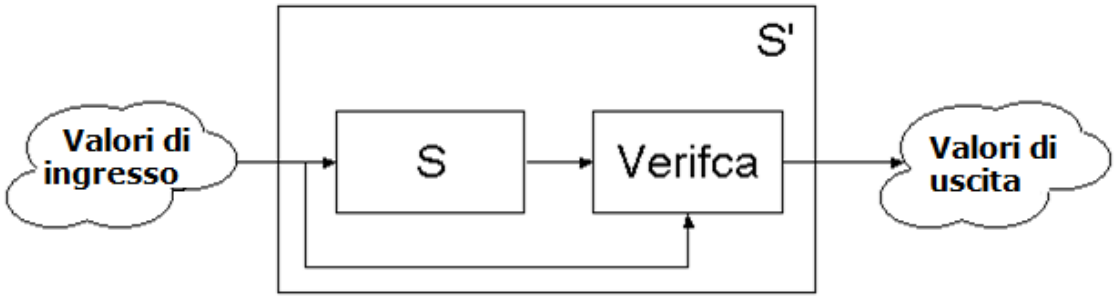


Figura 1 Sistema ideale di rilevazione degli errori

Per verificare se i valori di uscita di S rispettano le specifiche sarà necessario fornire un'implementazione alternativa che modelli il servizio richiesto e attraverso cui possa essere comparata l'attività di S. Il successo della verifica dipenderà dalla correttezza e dall'accuratezza del modello.
Nella pratica, per la maggior parte dei sistemi non è possibile applicare un controllo così rigoroso, e quindi viene realizzato un controllo sull'accettabilità dei valori di uscita. L'accettabilità è uno standard più basso di comportamento rispetto all'assoluta correttezza, senza garanzie di assenza di errori, il suo scopo è quello di rilevare la maggior parte delle situazioni erronee ed aumentare la fiducia nelle operazioni del sistema.

Delimitazione del danno e sua valutazione

Tra l'occorrenza del guasto e la sua rilevazione intercorre sempre del tempo. Pertanto, quando viene rilevato, è bene ritenere che l'errore si sia propagato per gran parte del sistema (se non tutto).
Prima che venga fatto qualsiasi tentativo di copertura sarà quindi necessario valutare l'estensione del danno nel sistema.

Copertura dell'errore

Queste tecniche hanno lo scopo di riportare il sistema nello stato di corretta operatività. Senza questa fase il guasto continuerà ad essere presente e ad influenzare sempre più il sistema.
Quando si identifica un guasto, viene eseguita la sua copertura attraverso due possibili modi:

- **correzione dell'errore:** il sottosistema dà risultati attendibili anche in caso di guasto permanente ed è pertanto in grado di procedere nelle proprie operazioni;
- **mascheramento (attraverso ridondanza):** maschera la presenza del guasto senza azioni di copertura.

Trattamento dell'errore e ripristino del servizio

Nonostante la fase di copertura dei guasti possa riportare il sistema ad uno stato senza errori, è ulteriormente necessario assicurarsi che il guasto occorso non si ripresenti. Un problema nel trattamento dei guasti è che la rilevazione di un errore non necessariamente è utile alla identificazione del guasto, infatti diversi guasti possono manifestarsi con lo stesso errore. Il primo passo del trattamento dei guasti sarà quello di cercare di circoscrivere adeguatamente il guasto. Dopodiché si hanno tre possibili soluzioni:

- sostituire il sottosistema guasto con uno di riserva;
- riconfigurare il sistema affinché funzioni senza il sottosistema guasto;
- ignorare il guasto se ritenuto transiente.

1.2.3 Ridondanza

La ridondanza è la chiave che permette di ottenere un sistema Fault-Tolerant. Introducendo ridondanza nel sistema se ne accrescono le capacità, e quindi la possibilità di rilevare e tollerare i guasti. Essa può

avere effetti, positivi o negativi, non solo sull'affidabilità, ma anche sulle prestazioni, le dimensioni, il peso, il consumo delle risorse del sistema.
In pratica la ridondanza consiste nella duplicazione dei componenti critici di un sistema con l'intenzione di aumentarne l'affidabilità e la disponibilità, in particolare per le funzioni di vitale importanza al fine di garantire la continuità della produzione. D'altra parte, poiché l'introduzione di elementi ridondanti aumenta la complessità del sistema, le sue dimensioni fisiche e i suoi costi, sono generalmente utilizzate solo quando i benefici derivanti sono maggiori degli svantaggi sopra citati.
Tuttavia la ridondanza non è necessaria per il funzionamento del sistema. Infatti esso potrebbe funzionare correttamente anche senza ridondanza, purché non sia presente nessun malfunzionamento.
Esistono diverse tecniche di ridondanza per migliorare l'affidabilità di un sistema, tra cui [7]:

- **ridondanza nell'hardware:** si tratta semplicemente della duplicazione degli apparati hardware e dei componenti interni (moduli di memoria, alimentazioni, apparati di rete, server di calcolo, collegamenti Internet);

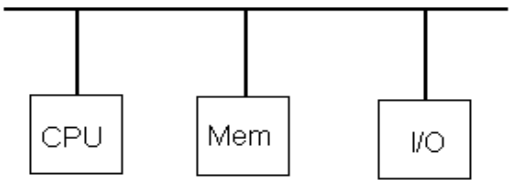


Figura 2 Esempio di hardware non ridondato

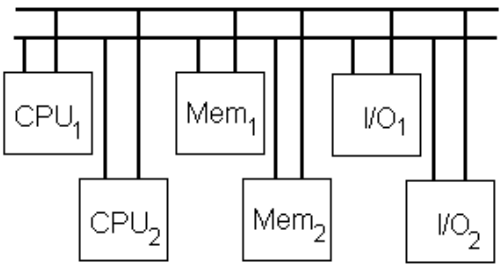


Figura 3 Esempio di hardware ridondato

- **ridondanza nel software:** premesso che non può esistere senza la ridondanza hardware, si tratta della duplicazione di processi o servizi tra diversi server. I processi o i servizi possono essere fruiti parallelamente o singolarmente. Il fallimento di un processo o servizio non pregiudica l'intera attività nel suo complesso.

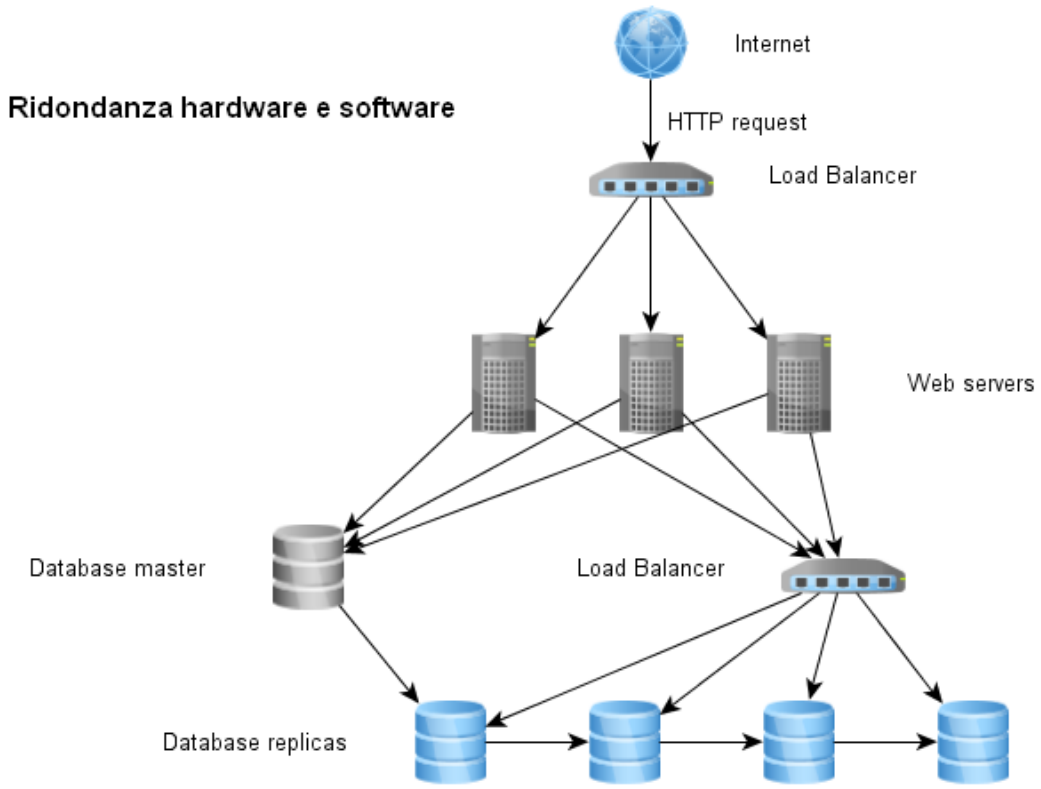


Figura 4 Ridondanza hardware e software

In entrambe, vengono aggiunti attrezzature o processi extra per consentire ad un sistema di tollerare la perdita o il guasto di qualche componente. In altre parole, replicando le attrezzature o i processi si può ottenere un alto grado di tolleranza ai guasti.

Generalmente, la tecnica più utilizzata è la ridondanza hardware, grazie alla sua semplicità di applicazione e ai costi decrescenti dell'hardware che la rendono molto allettante. Si distinguono tre tipi di ridondanza nell'hardware:

- passiva;
- attiva;
- ibrida.

La **ridondanza passiva** maschera il guasto, ossia nasconde il fault mediante i moduli ridondati. Non richiede nessun intervento da parte del sistema o di operatori esterni nella copertura dell'errore. Normalmente non implica il rilevamento del guasto, né alcuna azione di riconfigurazione.

La **ridondanza attiva** si basa, invece, sulle seguenti fasi:

- error detection;
- fault location;
- fault containment;
- fault recovery.

Le ultime 3 fasi vengono anche indicate con il termine "riconfigurazione". A differenza di quella passiva, la ridondanza attiva non fa uso del mascheramento quindi il sistema può essere temporaneamente soggetto ad errori, ed eventualmente anche a malfunzionamenti. Tuttavia, mediante la fase di error detection e di riconfigurazione, il sistema è in grado di riportarsi in uno stato corretto localizzando il modulo guasto, sostituendolo e ripartendo, seppur con capacità ridotte.
Le architetture di ridondanza attiva che permettono di eseguire le fasi sopra citate sono le seguenti:

- duplicazione e confronto (duplication with comparison);
- attesa e sostituzione (standby replacement o standby sparing);
- tecniche miste (ad esempio pair-and-a-spare).

La prima rappresenta l'architettura di ridondanza attiva più semplice. Si basa sulla duplicazione dell'hardware e del software e sull'aggiunta di un comparatore che confronta le uscite dei moduli. Nel caso sia rilevata una differenza (quindi un errore) parte una procedura per identificare il modulo guasto e disabilitarlo. Da quel momento il sistema funziona senza ridondanza, in attesa di un intervento di manutenzione.
Oltre al vantaggio di avere moduli ridondati e un comparatore di controllo, esistono anche alcuni problemi. I guasti sulle linee di ingresso ai due moduli non vengono né rilevati né tollerati. Inoltre una disfunzione al comparatore minaccerebbe il suo corretto funzionamento. Potrebbe venire meno la rilevazione degli errori sulle uscite dei moduli oppure potrebbe essere segnalata l'occorrenza di guasti inesistenti.
Nella seconda architettura, il sistema comprende uno o più moduli ridondati (spare). Nel caso in cui viene rilevato un modulo guasto, questo viene sostituito da uno dei moduli di riserva. Si distinguono due tecniche:

- hot sparing;
- cold sparing.

La differenza sostanziale tra le due tecniche sta nello stato dei moduli di riserva. Mentre nella prima (hot sparing) i moduli di riserva sono attivi ed eseguono le stesse funzionalità del modulo principale, nella seconda (cold sparing) i moduli di riserva non sono alimentati e vengono attivati solo nel momento in cui divengono necessari. Pertanto, nel primo caso la sostituzione del modulo guasto richiede una sospensione di durata minima nelle attività del sistema, mentre nel secondo caso la sospensione delle funzionalità del sistema durante la riconfigurazione è più lunga.
Nell'hot sparing i moduli di riserva, essendo alimentati e attivi, consumano elettricità a differenza di quelli del cold sparing i quali sono spenti.
Nella terza architettura (pair-and-a-spare) le due tecniche precedenti vengono combinate. Il sistema comprende due moduli che lavorano in parallelo, le cui uscite vengono continuamente confrontate e un modulo di riserva che prende il posto di quello guasto quando viene rilevato un errore.

Infine, la **ridondanza ibrida** combina le due precedenti aumentando l'affidabilità del sistema. Viene adottato il mascheramento dell'errore, ma i moduli guasti vengono rimpiazzati una volta rilevato il fault. Inoltre non permette ai guasti di produrre malfunzionamenti. Ciò significa che vengono predisposti componenti hardware di alta qualità a cui corrisponde un elevato costo.

1.3 Scenari di applicazione

Come abbiamo visto nel precedente paragrafo, l'utilizzo di sistemi Fault-Tolerant serve ad avere un servizio continuo, senza guasti o interruzioni. Avere un servizio di questo tipo è molto utile, ad esempio, nel caso di apparati elettronici. Uno strumento molto utilizzato a tal fine è il gruppo statico di continuità (detto anche UPS[6]), che mantiene costantemente alimentati gli apparecchi elettrici. Si rivela necessario nelle apparecchiature elettriche che non possono in nessun caso rimanere senza corrente evitando di creare un disservizio più o meno grave. In luoghi pubblici come gli ospedali, il verificarsi di un blackout potrebbe bloccare tutte le attività e le apparecchiature, comprese quelle della rianimazione, mettendo in serio pericolo la vita dei pazienti. Un altro esempio di utilizzo di UPS è nei sistemi di illuminazione di sicurezza. In caso di incendio l'illuminazione di emergenza deve garantire un'affidabile segnalazione delle vie di uscita, che per durata e livello di illuminazione consenta un adeguato sfollamento.
Come si è visto, utilizzando sistemi Fault-Tolerant si riesce a tenere sotto controllo molte delle attività quotidiane. Pensiamo, inoltre, ad un paracadutista e vediamo come il concetto di ridondanza si possa applicare in questo contesto. Tra le attrezzature di un paracadutista ci devono essere due paracaduti: uno principale e uno di emergenza e due anelli di apertura: uno per aprire il paracadute principale (che viene tirato dal pilota) e l'altro di riserva che ha lo scopo di aprire il paracadute di emergenza in caso di imprevisti. Anche questo è un sistema Fault-Tolerant

[6] Uninterruptible Power Supply

poiché si riesce, attraverso un paracadute di riserva, a continuare la discesa.
In alcuni contesti, tuttavia, non è essenziale l'utilizzo di sistemi Fault-Tolerant. Ci sono dei casi in cui l'interruzione di un servizio o il guasto di qualche componente non causa problemi o disagi così spiacevoli da dover rendere il sistema tollerante. Consideriamo ad esempio il bancomat di una banca. A volte capita di leggere nello schermo: "sistema non disponibile (sportello fuori servizio)". Questo è un sistema non tollerante perché non assicura costantemente l'erogazione del servizio ma non crea comunque disagio in quanto l'utente può andare a prelevare nello sportello più vicino.

1.4 Alcune soluzioni Fault-Tolerant in ambito informatico

Un'infrastruttura informatica è composta da diversi componenti che interagiscono tra loro, come, per esempio, apparati che gestiscono i dati (database, storage), apparati che gestiscono la comunicazione di rete (router, switch, firewall), ecc. Per garantire un corretto funzionamento dell'infrastruttura si utilizzano diverse soluzioni che garantiscono una tolleranza ai malfunzionamenti nei suoi componenti. Alcune di queste sono:

- architetture RAID;
- architetture Cluster;
- architetture Load Balancing;
- architetture Cloud Computing.

1.4.1 RAID

Un RAID (*Redundant Array of Independent Disks*) è un sistema informatico (hardware e software) che usa un gruppo di dischi rigidi per condividere o replicare le informazioni [8]. Questo gruppo di dischi viene visto dal

sistema operativo che lo gestisce come un unico disco logico. All'interno del RAID, i dati vengono memorizzati in modo distribuito nei vari dischi. La presenza di più dischi all'interno di un sistema aumenta le probabilità di guasto degli stessi. Per compensare questa riduzione di affidabilità, nel RAID viene utilizzata la ridondanza nella memorizzazione (mirroring, meccanismi di parità). I benefici del RAID sono di aumentare l'integrità dei dati, la tolleranza ai guasti e le prestazioni, rispetto all'uso di un disco singolo [20]. Il RAID è tipicamente usato nei server e di solito è implementato con dischi di identica capacità. Con il calo del costo dei dischi rigidi, esso è spesso offerto come opzione sia sui computer di fascia alta sia su quelli usati da utenti domestici, specialmente se dedicati a compiti che richiedono un grande immagazzinamento di dati.

1.4.2 Architetture Cluster

Un cluster è definito come un insieme di server connessi tra loro tramite una rete telematica [9]. Lo scopo di un cluster è quello di distribuire una elaborazione molto complessa tra i vari apparati componenti il cluster. In sostanza, un problema che richiede molte elaborazioni per essere risolto viene scomposto in sotto problemi separati i quali vengono risolti in parallelo. Questo ovviamente aumenta la potenza di calcolo del sistema. Inoltre, nelle architetture cluster, viene generalmente sfruttata la tecnica del load balancing (bilanciamento del carico) che distribuisce il carico di uno specifico servizio, ad esempio la fornitura di un sito web, tra più server, aumentando la scalabilità e l'affidabilità dell'architettura. Un cluster è una soluzione scalabile dal momento che le risorse sono distribuite. Tuttavia, aumentando il numero di server, l'organizzazione e la gestione dell'architettura diventa sempre più difficoltosa: lo spazio fisico occupato aumenta così come il consumo di corrente e di risorse umane per la manutenzione [21]. Un altro vantaggio di questa architettura è l'aumento di affidabilità in quanto il sistema continua a funzionare anche in caso di guasti a parti di esso, ovviamente con prestazioni inferiori.
Una soluzione che permette di creare infrastrutture informatiche ridondanti è il progetto *Linux High Availability* (Linux-HA), una famiglia di strumenti e protocolli che utilizzano il sistema operativo Linux.

Linux-HA fornisce servizi di clustering ad alta affidabilità. Esso dispone di una serie di caratteristiche, tra cui [10]:

- cluster HA di due nodi. La maggior parte delle applicazioni di fail over clustering[7] sono configurazioni di base di due nodi. Questa è la configurazione base per il clustering HA, la quale permette di eliminare ogni *single point of failure*, ossia la componente hardware e software di un sistema che in caso di malfunzionamento (o anomalia) causa disfunzione dell'intero sistema;
- configurazioni Active/Active (o Master/Master) e Active/Passive (o Master/Slave). In una disposizione a due nodi, se un server fornisce tutti i servizi e l'altro agisce principalmente come un server di backup, si parla di una configurazione attivo/passivo. Se entrambi i server forniscono alta disponibilità dei servizi e ognuno sostiene l'altro nelle procedure di fail back[8], la configurazione è attivo/attivo.

Entrambe le configurazioni sono supportate dal software *Heartbeat*, uno strumento (sempre del progetto Linux-HA) che consente di monitorare il funzionamento di uno o più nodi di un cluster HA.

1.4.3 Tecniche di Load Balancing

In informatica, il bilanciamento del carico è una tecnica utilizzata per distribuire le operazioni di lavoro tra diversi processi, computer, reti, dischi o altre risorse, in modo che nessuna di queste sia in sovraccarico [11]. Il load balancing permette di aumentare l'affidabilità e la scalabilità del sistema in cui è utilizzato. Ad esempio, in un cluster, la scalabilità deriva dal fatto che, nel caso sia necessario, si ha la possibilità di aggiungere altri server, mentre l'affidabilità deriva dal fatto che la rottura di uno dei server non compromette la fornitura del servizio.
Nell'ambiente di rete, una soluzione di bilanciamento del carico è il link aggregation [12], conosciuto anche come port trunking o bonding, il quale

[7] Processo mediante il quale i servizi attivi vengono spostati dal nodo divenuto non operativo ad un altro nodo del cluster divenendo operativo.
[8] Procedura di ripristino dei servizi sul nodo precedentemente danneggiato e nuovamente operativo.

consiste nel definire una interfaccia di rete virtuale corrispondente alla aggregazione di due o più interfacce fisiche.

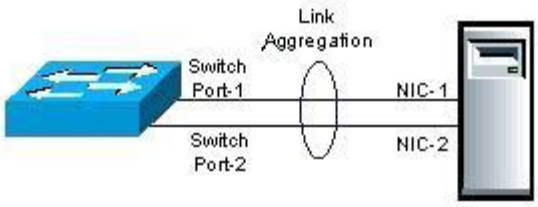


Figura 5 Link Aggregation

Questa tecnica permette di utilizzare le interfacce fisiche come se fossero una singola interfaccia di rete, con una capacità trasmissiva pari alla somma delle interfacce aggregate. In caso di guasto ad un'interfaccia, rimarrebbe funzionante l'altra, permettendo, seppur con velocità ridotta, la trasmissione dei dati.
Il bilanciamento del carico può essere utilizzato anche per bilanciare gli accessi ai database. Le richieste di lettura/scrittura vengono ripartite tra i server componenti un database cluster, al fine di ottenere un livello di scalabilità e alta disponibilità.
In ambiente Linux, una soluzione di load balancing è il software *Keepalived*, il cui scopo principale è fornire un servizio semplice e altamente affidabile di bilanciamento di carico del sistema [13]. Keepalived implementa un set di controllori per mantenere e gestire dinamicamente un pool di server bilanciati, secondo il loro stato di operatività e sfrutta il protocollo VRRP (Virtual Router Redundancy Protocol) che permette a più macchine di condividere un VIP (Virtual IP) per garantire l'alta affidabilità dei servizi.

1.4.4 Architetture Cloud Computing

Con il termine inglese C*loud Computing* si indica un insieme di tecnologie che permettono, tipicamente sotto forma di un servizio offerto da un provider al cliente, di memorizzare/archiviare/elaborare dati grazie all'uso di risorse hardware/software distribuite e virtualizzate in rete [14].

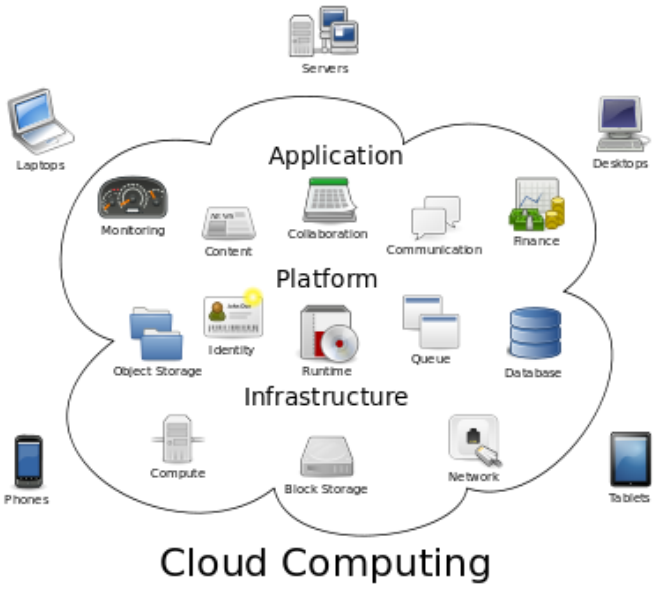


Figura 6Cloud Computing

Il concetto di cloud computing, gergalmente denominato cloud, viene assimilato ad un contenitore remoto, raggiungile ovunque dove ogni utente può conservare al suo interno i propri documenti ottenendo così il vantaggio di avere sempre le informazioni a portata di mano. Un esempio di cloud computing è DropBox, un software cloud based che offre un servizio di archiviazione e sincronizzazione dei file tramite web. L'architettura cloud possiede diverse caratteristiche chiave, tra cui:

- **Affidabilità:** aumenta se vengono sfruttati più siti ridondati, in modo da rendere l'architettura ben progettata per le operazioni di recupero dati.
- **Indipendenza dal dispositivo e dalla locazione:** ogni utente può accedere ai sistemi utilizzando, ad esempio, un browser web, indipendentemente dalla loro posizione o dal dispositivo che si utilizza.
- **Sicurezza:** potrebbe migliorare grazie alla centralizzazione dei dati e alla concentrazione delle risorse, ma le preoccupazioni possono persistere riguardo la perdita di controllo su taluni dati sensibili. Inoltre, la complessità della sicurezza aumenta notevolmente quando i dati vengono distribuiti su una zona più ampia o su un maggior numero di dispositivi che vengono condivisi da utenti indipendenti.

2 IL SERVIZIO DI POSTA ELETTRONICA CERTIFICATA: ANALISI DI UN CASO AZIENDALE

2.1 Posta Elettronica Certificata

2.1.1 Che cos'è?

La posta elettronica (e-mail) è divenuto ormai lo strumento di comunicazione più utilizzato per l'interscambio di comunicazioni e informazioni. La posta elettronica è un mezzo di comunicazione in forma scritta via Internet. Il principale vantaggio di questo strumento è l'immediatezza della comunicazione.
La Posta Elettronica Certificata (PEC) è un sistema di posta elettronica nel quale, oltre a quanto suddetto, viene fornita al mittente documentazione elettronica, con valenza legale, attestante l'invio e la consegna di documenti informatici [22].
La PEC trae le sue origini dalla volontà di sostituire, attraverso i moderni mezzi di comunicazione, la **Raccomandata postale con ricevuta di ritorno**, o raccomandata A/R. La comunicazione tramite PEC, viene realizzata attraverso una serie di messaggi che vengono inviati:

- all'utente da parte dei server di posta certificata;
- tra i diversi server di posta certificata.

La PEC può essere utilizzata per la trasmissione di tutti i tipi di informazioni e documenti in formato elettronico (eventualmente come allegati al messaggio). Consente di certificare l'invio, l'integrità e l'avvenuta consegna del messaggio scambiato tra un mittente e uno o più destinatari. A differenza del "circuito" di posta tradizionale, il servizio di PEC consente di inviare documenti informatici fornendo la certificazione

dell'invio e dell'avvenuta (o mancata) consegna. La PEC ha, pertanto, tutti i requisiti della raccomandata A/R con alcuni vantaggi aggiuntivi [24]:

- tempi di trasmissione brevissimi;
- costi di invio/ricezione pari a zero (il pagamento non è legato al numero di messaggi inviati ma al canone annuo per l'attivazione della casella);
- integrità del contenuto del messaggio trasmesso tramite apposizione di firma digitale (nella raccomandata A/R tradizionale viene certificata la spedizione/ricezione ma non il contenuto, cioè cosa è stato spedito/ricevuto).

Per poter usufruire di tale servizio un utente deve dotarsi di un'apposita casella di PEC, richiedendola ad uno qualsiasi dei gestori di posta elettronica certificata che sono stati iscritti regolarmente nell'elenco pubblico dei gestori da parte del Centro Nazionale per l'Informatica nella Pubblica Amministrazione (CNIPA). Questo elenco deriva dall'attuazione del Decreto 2 novembre 2005 *"Regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della Posta Elettronica Certificata"*. In particolare, tra i vari punti stabiliti dal DPR 11 febbraio 2005, mettiamo in evidenza i seguenti:

- Il mittente o il destinatario che intendono fruire del servizio di posta elettronica certificata si avvalgono dei gestori inclusi in un apposito elenco pubblico disciplinato dal presente articolo.
- Le pubbliche amministrazioni ed i privati che intendono esercitare l'attività di gestore di posta elettronica certificata inviano al CNIPA domanda di iscrizione nell'elenco dei gestori di posta elettronica certificata.
- Il richiedente (in questo caso il candidato gestore N.d.R.) deve inoltre:
  a) dimostrare l'affidabilità organizzativa e tecnica necessaria per svolgere il servizio di posta elettronica certificata;

b) impiegare personale dotato delle conoscenze specifiche, dell'esperienza e delle competenze necessarie per i servizi forniti, in particolare della competenza a livello gestionale, della conoscenza specifica nel settore della tecnologia della posta elettronica e della dimestichezza con procedure di sicurezza appropriate;
c) rispettare le norme del presente regolamento e le regole tecniche;
d) applicare procedure e metodi amministrativi e di gestione adeguati e tecniche consolidate;
e) utilizzare, per la firma elettronica, dispositivi che garantiscono la sicurezza delle informazioni gestite in conformità a criteri riconosciuti in ambito europeo o internazionale;
f) adottare adeguate misure per garantire l'integrità e la sicurezza del servizio di posta elettronica certificata;
g) prevedere servizi di emergenza che assicurano in ogni caso il completamento della trasmissione;

In altre parole, possiamo definire la PEC come un insieme di servizi accessibili dagli utenti al fine di certificare anche temporalmente le comunicazioni attraverso l'uso della tecnologia della posta elettronica.

2.1.2 Soggetti ed uso del servizio di Posta Elettronica Certificata

Dalle definizioni precedenti emergono i seguenti soggetti aventi ognuno ruoli e responsabilità ben definite:

a) il mittente, cioè l'utente che si avvale del servizio di posta elettronica certificata per la trasmissione di documenti prodotti mediante strumenti informatici;
b) il destinatario, cioè l'utente che si avvale del servizio di posta elettronica certificata per la ricezione di documenti prodotti mediante strumenti informatici;

c) il gestore del servizio, cioè il soggetto, pubblico o privato, che eroga il servizio di posta elettronica certificata e che gestisce domini di posta elettronica certificata.

Per descrivere a grandi linee il funzionamento di un sistema di Posta Elettronica Certificata usiamo il disegno riportato nella figura seguente.

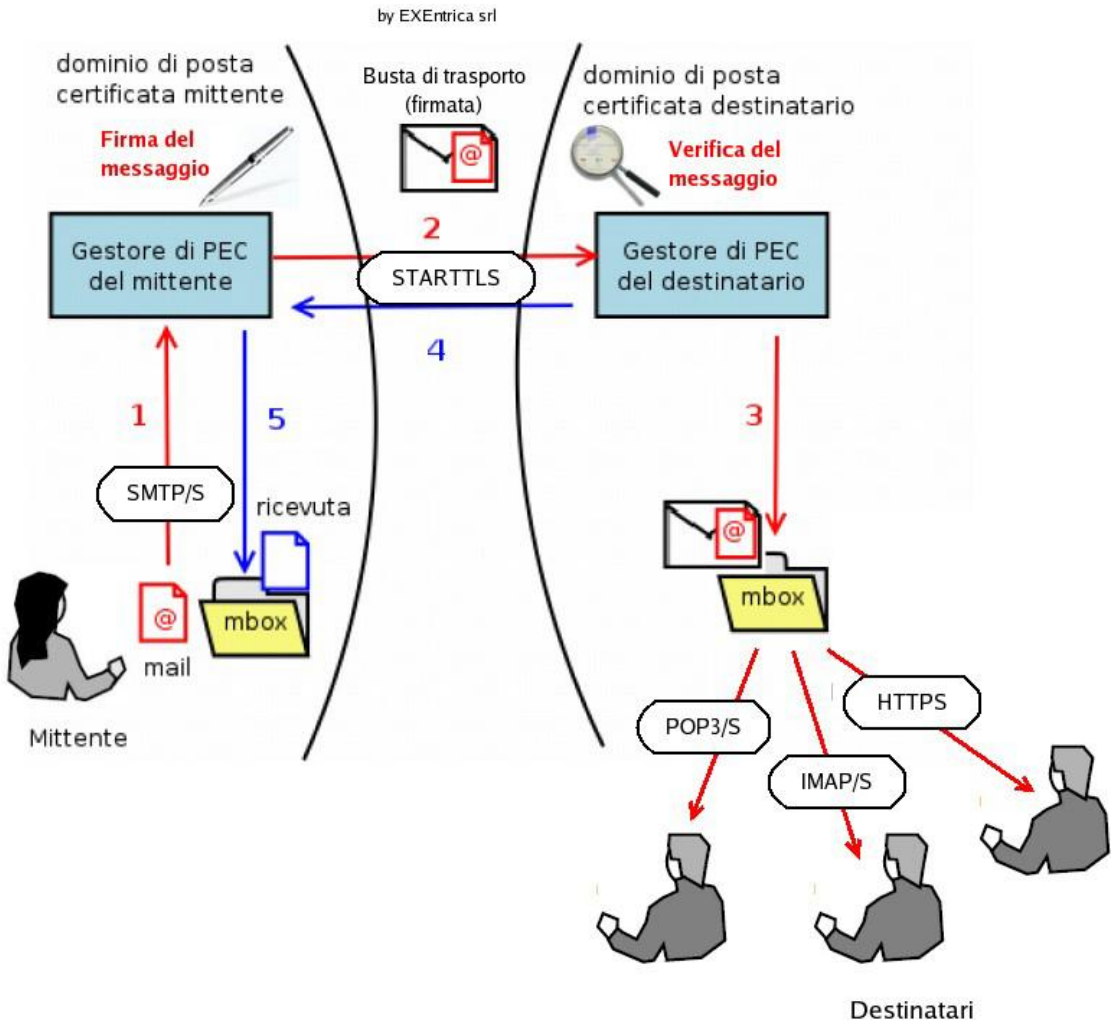


Figura 7 Descrizione del sistema di PEC

Nel dettaglio: quando il mittente, possessore di una casella di PEC, invia un messaggio ad un altro utente certificato (passo 1), il messaggio viene raccolto dal gestore del dominio certificato che lo racchiude in una busta di trasporto e vi applica una firma elettronica in modo da garantire:

- inalterabilità;
- provenienza;
- certificazione temporale.

Fatto questo indirizza il messaggio al gestore di PEC destinatario (passo 2) che verifica la firma e lo consegna al destinatario (passo 3). Una volta consegnato il messaggio, il gestore di PEC destinatario invia una ricevuta di avvenuta consegna all'utente mittente (passi 4 e 5) che può quindi essere certo che il suo messaggio è giunto a destinazione. Ovviamente si possono verificare alcuni casi particolari e pertanto per approfondirli maggiormente, con i relativi flussi di dati, si rimanda alla lettura dell'allegato del Decreto 2 novembre 2005 *"Regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata"*, contenente:

- il glossario dei termini usati nel sistema;
- gli schemi e le definizioni dei messaggi gestiti dal sistema di PEC;
- i comportamenti e le misure da adottare per ogni caso ivi descritto.

Come accennato in precedenza per il funzionamento della posta elettronica certificata, è fondamentale il ruolo dei gestori accreditati di PEC. Questi ultimi devono infatti garantire un insieme di servizi e alta disponibilità di alcuni di essi, così come stabilito dall'art. 12 del Decreto del Ministro per l'innovazione e le tecnologie del 2 novembre 2005.

2.1.3 I servizi forniti e gli obblighi del gestore di Posta Elettronica Certificata

Sulla base della normativa prodotta dal CNIPA, emerge che ogni gestore di posta elettronica certificata ha l'obbligo di fornire i seguenti servizi:

- Autenticazione, accettazione ed invio dei messaggi di posta elettronica;
- Ricezione e verifica dei messaggi di posta elettronica certificata provenienti dagli altri gestori;

- Consegna dei messaggi di posta elettronica certificata nella casella dell'utente;
- Consultazione delle caselle da parte degli utenti di posta elettronica certificata.

In altre parole, il gestore di PEC deve garantire ad ogni proprio utente la possibilità di invio, ricezione e consultazione dei messaggi. Il rispetto della normativa vigente, in particolare del Decreto Ministeriale 2 novembre 2005, obbliga altresì il gestore a:

- fornire e garantire i livelli di servizio previsti (disponibilità e accessibilità ai servizi h24, 7gg/7gg, 365gg/anno);
- interoperare con gli altri gestori accreditati riducendo le problematiche derivanti dall'uso di software e tecnologie eterogenee;
- registrare le singole fasi di ogni trasmissione all'interno di specifici file di log;
- apporre la marca temporale sui log dei messaggi;
- conservare e rendere disponibili, per almeno 30 mesi, i log relativi alle trasmissioni avvenute, in quanto aventi valore legale, secondo le modalità e gli usi previsti dalla legge;
- garantire riservatezza, integrità e inalterabilità nel tempo dei file di log;
- informare i propri utenti sulle modalità di accesso al servizio e sui necessari requisiti tecnici;
- rilasciare tutte le ricevute e tutti i messaggi previsti dalla normativa (busta di trasporto, ricevuta di presa in carico, ricevuta di accettazione, ricevuta di avvenuta consegna, avviso di mancata accettazione, avviso di mancata consegna, avviso di mancata consegna per superamento tempi massimi, avviso di rilevazione virus, etc etc);
- apporre in ogni messaggio il riferimento temporale;
- conservare e garantire l'integrità del messaggio originale contenuto all'interno della relativa busta di trasporto durante ogni trasmissione;

- rispettare le norme previste dal Decreto legislativo 30 giugno 2003, n. 196 in materia di protezione dei dati personali;
- rilevare e comunicare la presenza dei virus informatici rilasciando gli avvisi previsti dalla legge;
- conservare i messaggi contenenti virus informatici per il periodo previsto dalla normativa;
- adottare misure atte ad evitare l'inserimento di codici dannosi (virus);
- adottare procedure e servizi di emergenza che assicurino il completamento della trasmissione anche in caso di incidenti (ad esclusione di eventi disastrosi improvvisi quali terremoti, attentati, etc etc);
- garantire la segretezza della corrispondenza trasmessa attraverso il proprio sistema;
- attivare/disattivare le caselle di PEC previa verifica dell'autenticità della richiesta pervenuta;
- inviare ai propri clienti le informazioni riguardo le modalità di richiesta, reperimento e presentazione dei log dei messaggi per consentirne l'opposizione a terzi nei casi previsti dalla legge;
- utilizzare protocolli di comunicazione sicuri allo scopo di garantire la segretezza, l'autenticità e l'integrità delle informazioni trasmesse attraverso il sistema PEC;
- adottare procedure di sostituzione dei certificati elettronici relativi alle proprie chiavi di firma con una tempistica tale da non causare interruzioni di servizio;
- richiedere la revoca dei certificati relativi alle chiavi utilizzate per la firma dei messaggi e per la connessione sicura al sito del DigitPA (ex CNIPA) in caso di loro compromissione;
- adottare misure d sicurezza tali da non consentire la duplicazione abusiva e incontrollata delle chiavi private di firma o dei dispositivi che le contengono (vale a dire che l'esportazione cifrata delle chiavi private di firma viene effettuata in modo da non diminuirne il livello di sicurezza e che le chiavi private non vengano usate per scopi diversi dalla firma dei messaggi di posta elettronica previsti dalla normativa);

- comunicare tempestivamente ai propri utenti l'eventuale cessazione o interruzione del servizio;
- adottare misure di sicurezza tali da consentire l'accesso logico e fisico al sistema alle sole persone autorizzate (ovvero al personale tecnico e amministrativo per quanto riguarda il controllo e la manutenzione del sistema);
- utilizzare un sistema di riferimento temporale che garantisca stabilmente una sincronizzazione delle macchine coinvolte con uno scarto non superiore al minuto secondo rispetto alla scala di Tempo Universale Coordinato UTC;
- utilizzare dispositivi di firma conformi alla normativa vigente.

Si può facilmente dedurre che non tutti i servizi derivanti dagli obblighi stabiliti per legge debbano essere necessariamente forniti con continuità. L'interruzione dell'attivazione o della cancellazione degli utenti non pregiudica il corretto funzionamento del sistema di PEC contrariamente a quanto può avvenire se accade un guasto ai dispositivi di firma. Ancora, il mancato reperimento dei log dei messaggi di posta elettronica certificata non pregiudica il corretto funzionamento del sistema di PEC contrariamente a quanto può avvenire se un utente non riesce ad autenticarsi al sistema di posta elettronica certificata. Applicare i concetti di tolleranza ai guasti, nel sistema di PEC, significa identificare le componenti (hardware e software) e le procedure per cui un loro fallimento comporta una completa e totale interruzione dei servizi.

2.2 Modalità di accesso ai servizi di PEC

Generalmente, in un sistema di posta elettronica tradizionale i servizi di invio, ricezione e consultazione di messaggi vengono forniti tramite i più comuni protocolli di rete, quali IMAP, POP e SMTP [26][27][28].
Questi protocolli non supportano, tuttavia, un interscambio sicuro di dati, visto che il flusso delle connessioni non è criptato. Un sistema di PEC, sulla base della normativa vigente, deve prevedere un meccanismo di protezione per tutte le connessioni previste dall'architettura di posta

certificata attuato tramite l'impiego di canali sicuri [25]. Un sistema di PEC, pertanto, deve garantire l'integrità e la confidenzialità delle connessioni tra il gestore di posta certificata e l'utente, mediante l'uso di protocolli sicuri. A titolo esemplificativo e non esaustivo, dei protocolli accettabili possono essere i seguenti, i quali utilizzano il protocollo SSL (Secure Socket Layer) [29] per una comunicazione sicura:

- IMAP sicuro (IMAP/s), che consente la gestione sicura, in modalità sincrona, della casella di posta, instaurando connessioni crittografate;
- POP sicuro (POP/s), che permette la consultazione sicura della casella di posta certificata, instaurando connessioni crittografate;
- SMTP sicuro (SMTP/s), che permette l'invio dei messaggi degli utenti e l'invio e la ricezione dei messaggi tra gestori instaurando connessioni crittografate;
- HTTP sicuro (HTTP/s), utilizzato per la pubblicazione dell'elenco dei propri domini di PEC gestiti, in modo da renderlo disponibile al CNIPA.

Per quanto riguarda l'elenco dei domini certificati, il CNIPA provvede a pubblicare un elenco, destinato a tutti i gestori, contenente tutti i domini certificati (raggruppati per gestore) allo scopo di discriminarli dai domini posta convenzionale così da trattare in maniera adeguata i messaggi destinati a/provenienti da utenti certificati (emissione delle ricevute, avvisi, etc etc) e i messaggi destinati a/provenienti da utenti di posta convenzionale.

2.3 Servizi erogati e livelli di servizio

Nell'ambito della Posta Elettronica Certificata, i servizi erogati dai gestori (siano essi PP.AA. o enti privati) sono sempre più fortemente basati sull'integrazione tra le nuove soluzioni tecnologiche e processi informatici e risorse umane. I servizi che ne scaturiscono sono piuttosto complessi, soggetti alle dinamiche del mercato ed alla continua innovazione

tecnologica. Per esporre i loro servizi, alcuni gestori potrebbero pertanto ricorrere a fornitori terzi mediante contratti di outsourcing totale o parziale. È evidente che il termine servizio, in questo contesto, può assumere significati diversi. Di seguito ne riportiamo alcuni:

- per la norma UNI EN 29004-2[9] un servizio è: "il risultato di attività svolte sia all'interfaccia tra cliente e fornitore che all'interno della organizzazione del fornitore, per soddisfare le esigenze di un cliente".
- una definizione in ambito ICT è la seguente: "il servizio è un insieme di processi basati su tecnologie informatiche, non correlati alla produzione di beni materiali od immateriali, che vengono attuati per un certo periodo di tempo da un fornitore per risolvere le esigenze di un committente.

Sulla base delle definizioni precedenti si può quindi intuire come il servizio di posta elettronica certificata scaturisce dalla crescente necessità di digitalizzare, informatizzare ed automatizzare i processi dei servizi di pubblica utilità. Per quanto l'innovazione tecnologica offra sempre più opportunità di produrre nuovi servizi, per l'utente finale resta, sempre e comunque, importante la percezione del livello di qualità del servizio fornito.

2.4 Le caratteristiche generali dei servizi

La finalità di un servizio non è la produzione di beni materiali. Alla fine delle attività svolte dal fornitore, all'utente finale non rimane nulla di tangibile, ma ha soltanto usufruito del servizio per un determinato periodo di tempo. I servizi perciò, si qualificano per le loro prestazioni piuttosto che per un qualche attributo fisico posseduto. La loro produzione e la loro fruizione sono inseparabili ed il loro reale funzionamento viene misurato nell'istante della sua erogazione all'utente

[9]Norma italiana che fornisce una guida per definire e attuare un sistema per la qualità in una organizzazione.

finale e non in fase di progettazione o pianificazione. Le fasi di test contribuiscono alla produzione di una quantità di dati sulla quale costruire e migliorare i servizi stessi.
Sulla base di quanto premesso possiamo fare una prima classificazione dei servizi del sistema di PEC in base alla modalità di erogazione:

- servizi ad intervalli prefissati: rientrano in questa categoria processi, procedure e procedimenti che vengono effettuati ad intervalli stabiliti e prefissati (es: provisioning degli utenti, richiesta e reperimento dei file di log, storicizzazione dei file di log, attività di call center);
- servizi continuativi: rientrano in questa categoria processi, procedure e procedimenti che devono essere attivi e fruibili h24 senza soluzione di continuità (es: invio e ricezione dei messaggi di PEC, consultazione dei messaggi, apposizione di firma digitale e marcatura temporale).

2.5 Caratteristiche di qualità dei servizi

Per quanto concerne le caratteristiche di qualità dei servizi, gli utenti in genere prestano maggiormente attenzione a:

- puntualità e tempestività: consiste nel rispetto dei tempi di erogazione definiti del servizio;
- disponibilità e continuità: il servizio che si vuole utilizzare deve essere fruibile senza soluzione di continuità;
- informazione sull'utilizzo del servizio: un'informazione di utilizzo chiara, completa e trasparente facilita l'utente nelle operazioni di interazione con i servizi;
- accessibilità: riguarda la facilità con la quale si può accedere al servizio (consultare i messaggi di posta elettronica certificata mediante l'uso di diversi dispositivi tecnologici, offre maggiori vantaggi all'utente rispetto ad un unico punto di accesso);

- precisione e affidabilità: strettamente correlati agli errori commessi nell'erogazione del servizio, consentono all'utente una fruizione del servizio puntuale e corretta;
- regolarità: riguarda un'erogazione conforme agli standard previsti ed associati al servizio;
- prestazioni: in particolare quelle legate al tempo (avere risposta nel minor tempo possibile) e al consumo di risorse (l'uso del servizio non deve rallentare il sistema dell'utente). Il servizio fornito deve corrispondere ai requisiti di efficacia ed efficienza;
- gentilezza, competenza, capacità di comunicazione dell'addetto al servizio.

2.6 Valutare il livello di servizio

Poiché la finalità di un servizio è il soddisfacimento delle esigenze di un committente, la valutazione di un servizio va correlata principalmente al livello di soddisfazione di queste esigenze che il servizio riesce a garantire.
Per valutare il livello di un servizio, pertanto, possiamo utilizzare la seguente espressione matematica:

Q = Livello erogato / Livello atteso >= 1

Il livello di servizio richiesto va correlato alle effettive esigenze (obiettivi di business) ed al costo che si è disposti a sostenere.
Non è immediato collegare il livello di servizio richiesto al valore che si riconosce al servizio. La relazione tra costo e livello di servizio non è lineare, nel senso che, superato una certo livello, ogni ulteriore incremento viene spesso a costare in maniera sempre maggiore.
La scelta di quali misure utilizzare per definire il livello di servizio atteso è fondamentale ai fini della significatività del giudizio. In altri termini, per misurare un fenomeno occorre definire un sistema di relazioni numeriche che può essere messo in qualche significativo rapporto con il sistema di relazioni empiriche valido per il fenomeno da misurare. Ciò significa che spesso l'andamento di un servizio può essere messo in relazione con

diversi fenomeni misurabili, ognuno dei quali può coglierne un aspetto. La scelta di quali misure sia più opportuno rilevare dipende dalla facilità di misurarle, dal costo di rilevare le misure, dalla capacità di gestire ed elaborare il volume di informazioni rilevate, etc etc. Non è semplice individuare quali siano i parametri che caratterizzano un servizio e che sono realmente misurabili, poiché questa possibilità è legata alla evoluzione della tecnologia.

2.7 Come e quando rilevare le misure

Le misure sull'andamento del servizio possono essere rilevate in vari modi:

- con continuità durante tutta la durata prevista di erogazione del servizio;
- in intervalli temporali prefissati (anche non contigui) di erogazione del servizio;
- al verificarsi di certi eventi ritenuti significativi.

A tal proposito, è importante definire il giusto campionamento delle misure perché rilevare troppe misure ha un costo non ripagato dai vantaggi che ne derivano in termini di controllo ed anche perché rilevarne troppo poche potrebbe far sfuggire dei segnali di allarme utili per migliorare la qualità del servizio.
Le elaborazioni delle misure elementari più comunemente utilizzate negli accordi di servizio sono:

- il calcolo del minimo e/o massimo valore assunto dalle misure in un determinato intervallo di tempo;
- il calcolo della media aritmetica dei valori;
- il calcolo della frequenza con cui certe misure ricadono in determinati intervalli di valori,
- la somma delle occorrenze delle misure (o di parte di esse, scelte secondo specifici criteri),
- la somma dei valori delle misure rilevate.

Ad esempio, dovendo valutare la "disponibilità" di un servizio, i seguenti livelli di servizio definiscono vincoli molto differenti tra loro:

- nessuna interruzione della disponibilità deve superare i 30 minuti consecutivi;
- non devono verificarsi più di 5 interruzioni del servizio nel periodo, qualsiasi sia la loro durata;
- la media delle interruzioni deve essere inferiore a 30 minuti;
- il 95% delle interruzioni deve essere di durata inferiore a 30 minuti, il 3% a 35 minuti, il 2% a 45 minuti;
- la somma di tutte le interruzioni deve essere inferiore a 180 minuti.

Le modalità di rilevazione delle misure influenzano la valutazione. Ad esempio, può essere importante la definizione precisa dell'evento che attiva la misurazione. Nel caso di una richiesta di assistenza da parte di un utente, è importante fissare le regole per l'apertura e la chiusura dell'intervento, poiché in questo caso i livelli di servizio sono collegati alla tempestività di risoluzione dei problemi, misurata come intervallo tra tempo di apertura e chiusura dell'intervento.
Inoltre, quando le misure sono rilevate con strumenti automatici, differenti strumenti possono avere diversi gradi di precisione nella misura. Anche il momento di rilevazione delle misure può essere importante ai fini della valutazione. Si consideri, ad esempio, di voler valutare la disponibilità effettiva di un servizio. A tal fine, si potrebbe calcolare il valore medio di disponibilità del servizio in un dato periodo considerando solo le misure rilevate in determinate ore, giudicate di punta, oppure utilizzare come base di calcolo della media tutte le misure rilevate, in qualsiasi orario. Le valutazioni potrebbero essere anche significativamente differenti utilizzando le due modalità. Per garantire la omogeneità e la comparabilità delle misure rilevate è necessario definire nello SLA, secondo il tipo di misura:

- le caratteristiche che devono possedere gli eventuali strumenti da utilizzare per rilevare le misure;

- le tecniche di campionamento ammissibili e/o la frequenza delle rilevazioni necessarie in un dato periodo di osservazione per ottenere misure significative;
- i criteri di arrotondamento delle misure.

Alcuni criteri per la scelta delle misure sull'andamento del servizio sono le seguenti:

- scegliere misure appropriate al contesto che permettono una valutazione corretta del servizio;
- elaborare un numero adeguato di misure al fine di valutare in modo sufficiente il servizio;
- misurare con l'accuratezza necessaria al caso;
- controllare periodicamente l'affidabilità del sistema di misura;
- utilizzare notazioni e formalismi, unità di misura e strumenti standard che permettono di condividere i risultati delle misure con altri soggetti (misure ripetibili, oggettive, trasparenti).

Tutte le misure scelte devono essere:

- affidabili: non devono essere affette da errori casuali in maniera eccessiva;
- ripetibili: ogni rilevazione sul medesimo componente, in differenti momenti e nelle stesse condizioni di rilevazione devono dare lo stesso risultato;
- riproducibili: in differenti occasioni, ma nelle stesse condizioni di utilizzo, debbono poter ottenere uguali risultati;
- disponibili: non debbono essere presenti periodi significativi di impossibilità nell'utilizzare tali misure;
- efficaci: il costo di impiego deve essere adeguato ai risultati;
- corrette: il raggiungimento dei risultati deve essere accurato;
- obiettive: i risultati raggiunti non debbono essere influenzati in alcun modo dall'utilizzatore o da altri fattori esterni;
- significative: le indicazioni sul comportamento del componente valutato debbono essere rilevanti rispetto al requisito in esame.

2.8 Accordi di servizio (Service Level Agreement)

I **Service Level Agreement** (in italiano: accordo sulle garanzie dei livelli di servizio) in sigla **SLA,** sono strumenti contrattuali attraverso i quali si definiscono le metriche di servizio (es. qualità di servizio) che devono essere rispettate da un fornitore di servizi (provider) nei confronti dei propri clienti/utenti. Di fatto, una volta stipulato il contratto, assumono il significato di obblighi contrattuali.

I gestori di PEC stipulano contratti di connettività con gli Internet provider presenti sul territorio. Essendo, da questo punto di vista, clienti di un fornitore di servizi, i gestori di PEC si accordano sull'insieme dei livelli di servizio che gli Internet provider devono loro garantire. Per contro, gli stessi gestori di PEC sono i fornitori dei servizi di invio, ricezione e consultazione dei messaggi di posta elettronica certificata nei confronti degli utenti finali e devono garantire loro i livelli di servizio previsti dalla normativa.

Data la complessità dell'erogazione del servizio di PEC, possiamo considerare il gestore come un'entità che riceve determinati SLA e ne eroga degli altri. Nella pratica, gli SLA sono documenti (solitamente allegati al contratto) in cui il committente e il fornitore definiscono in dettaglio l'oggetto della prestazione che viene richiesta, le condizioni della fornitura stessa e gli obblighi per entrambi. Dalla completezza e precisione dello SLA dipende in buona parte la soddisfazione delle parti contrattuali. Un Service Level Agreement approssimativo e generico sarà sicura fonte di controversie e dannosi ricorsi alla giustizia ordinaria.

Inoltre, lo SLA è anche uno strumento per rendere flessibile il contratto, in quanto può essere aggiornato periodicamente in relazione ad eventuali mutamenti tecnologici e/o organizzativi del contesto.

2.9 Lo SLA della PEC

L'articolo 12 del Decreto del Ministro per l'innovazione e le tecnologie 2 novembre 2005 enuncia i seguenti livelli di servizio:

Il gestore di posta elettronica certificata può fissare il numero massimo di destinatari e la dimensione massima del singolo messaggio, sia per i messaggi che provengono da un suo titolare, sia per i messaggi che provengono da titolari di caselle di altri gestori di posta elettronica certificata.

La possibilità di inviare messaggi di grandi dimensioni ad un numero illimitato di utenti può portare ad una saturazione delle risorse disponibili per l'erogazione del servizio di PEC. Nonostante viene data al gestore libertà di fissare un tetto massimo, devono essere rispettati i seguenti requisiti minimi:

- possibilità dell'invio di un messaggio: almeno fino a cinquanta destinatari;
- il prodotto del numero dei destinatari per la dimensione del messaggio stesso non superi i 30MB;

La disponibilità nel tempo del servizio di posta elettronica certificata deve essere maggiore o uguale al 99,8% del periodo temporale di riferimento.

Il periodo temporale di riferimento, per il calcolo della disponibilità del servizio di posta elettronica certificata, è pari ad un quadrimestre.

La durata massima di ogni evento di indisponibilità del servizio di posta elettronica certificata deve essere minore, o uguale, al 50% del totale previsto per l'intervallo di tempo di riferimento.

In ogni quadrimestre, pertanto, è consentito al massimo un periodo di disservizio pari a circa 6 ore e considerando che la durata del malfunzionamento non deve superare il 50%, ogni evento di disservizio deve essere risolto in circa 3 ore. Il superamento di tale limite può portare il gestore ad affrontare problemi di natura legale, con conseguente ripercussione sia sull'aspetto economico sia sul proseguimento dell'attività di erogazione del servizio (è prevista la sospensione forzata dell'erogazione).

Dati i principi normativi di cui sopra, l'accesso alla struttura di PEC rappresenta uno dei punti critici di tutto il sistema. Infatti se non correttamente implementato, può portare all'impossibilità di inviare consultare e ricevere messaggi, per un periodo superiore ai limiti imposti.

Nell'ambito dell'intervallo di disponibilità di cui al comma 3, la ricevuta di accettazione deve essere fornita al mittente entro un termine, da concordarsi tra gestore e titolare, da calcolare a partire dall'inoltro del messaggio, non considerando i tempi relativi alla trasmissione.
Sebbene questo punto incida profondamente sulla qualità del servizio offerto, non è da ritenere vincolante ai fini dello studio svolto ma è da considerare qualora si debba analizzare il servizio di posta elettronica certificata dal punto di vista del Disaster Recovery come di seguito enunciato:

Al fine di assicurare in ogni caso il completamento della trasmissione ed il rilascio delle ricevute, il gestore di posta elettronica certificata descrive nel manuale operativo, di cui all'articolo 23, le soluzioni tecniche ed organizzative che realizzano i servizi di emergenza, ai sensi di quanto previsto dall'articolo 11, comma 4, del D.P.R. n. 68 del 2005, e consentano il rispetto dei vincoli definiti nei commi 4 e 5 del presente articolo.

3 DALLA TEORIA ALLA PRATICA

Una delle caratteristiche dei sistemi Fault-Tolerant consiste nella capacità di rimanere attivi e funzionanti anche in presenza di guasti. Affinché questo sia possibile, si rende necessaria una corretta progettazione del sistema a partire dalle sue fasi iniziali.
Nel primo paragrafo di questo capitolo viene proposta ed analizzata un'infrastruttura minima per l'accesso ai servizi di PEC. La sua analisi mira a far emergere le caratteristiche che la rendono intollerante ai guasti.
Applicando alcune soluzioni trattate nel capitolo 1, si cercherà di ottenere un'infrastruttura Fault-Tolerant ideale, ovvero che sia in grado di erogare il servizio di PEC nonostante il verificarsi di malfunzionamenti.
Nella secondo paragrafo, tale infrastruttura verrà confrontata con quella predisposta dal gestore Namirial per eseguire dei test, valutando e motivando le cause di possibili differenze di configurazione.
Nel terzo ed ultimo paragrafo, verrà introdotta la fase di testing dell'infrastruttura predisposta dal gestore Namirial, con lo scopo di verificarne la reale capacità di tollerare i guasti, evitando disservizi che possono portare ad un fallimento. Nel capitolo successivo saranno riportate le schede relative ai test effettuati.

3.1 Infrastruttura Fault-Tolerant ideale

Facendo riferimento alla figura 8, di seguito viene descritta l'infrastruttura di partenza. Essa è composta da:

- un router di frontiera;
- un apparato Firewall;
- un server che elabora le richieste dei servizi di PEC.

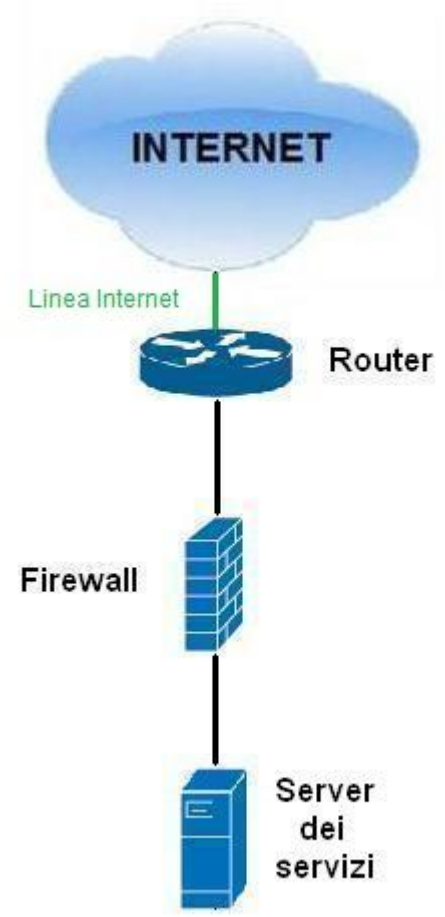


Figura 8Infrastruttura iniziale totalmente intollerante ai guasti

Il dispositivo di routing è indispensabile per l'erogazione del servizio, infatti esso collega l'infrastruttura ad Internet e permette di raggiungere e esportare i servizi e di conseguenza accedere ad essi. La presenza dell'apparato di firewalling è dovuta a motivi di sicurezza. Sulla base della normativa vigente, esso deve proteggere il sistema da accessi indesiderati, monitorando e filtrando il traffico entrante ed uscente dall'infrastruttura. Infine deve essere presente un server che riesca ad elaborare e soddisfare le richieste dei servizi necessari al funzionamento al sistema di PEC.

L'infrastruttura presa in esame è completamente intollerante ai guasti. Di fatto ogni dispositivo e collegamento rappresentano un single point of failure. Il flusso di dati effettua un percorso lineare (vedi figura 8) sia in entrata che in uscita. Nel caso in cui si verificasse un malfunzionamento ad uno dei dispositivi (Router, Firewall, Server dei servizi) o ai collegamenti

tra essi, il servizio di PEC non verrebbe esportato, generando un disservizio. I possibili motivi che potrebbero creare uno scenario di disservizio sono i seguenti:

- mancanza di collegamento Internet, dovuta ad esempio a problemi sull'unica linea fisica presente (vedi figura 8), la quale è di competenza del provider di rete;
- mancanza di collegamento di rete fra gli apparati dell'infrastruttura, dovuto, ad esempio, ad un cavo di rete scollegato;
- danneggiamento di componenti hardware (processore, interfaccia di rete, ecc) o software (ad es. bug nel sistema operativo) degli apparati, che pregiudicherebbe il loro corretto funzionamento.

Pertanto, questi single point of failure devono essere eliminati, in modo da aumentare l'affidabilità dell'infrastruttura.

3.2 Analisi e sviluppi dell'infrastruttura

I single point of failure dell'infrastruttura di partenza, quindi, sono rappresentati da:

- la linea Internet;
- collegamenti di rete;
- il router;
- il firewall;
- il server dei servizi.

L'eventuale mancanza di collegamento Internet potrebbe essere tollerata mediante l'utilizzo di una linea di backup da collegare sul dispositivo di routing. In altre parole, se la linea Internet predefinita dovesse essere inaccessibile, l'operatività del sistema verrà dirottata sulla linea di riserva (vedi figura 9).

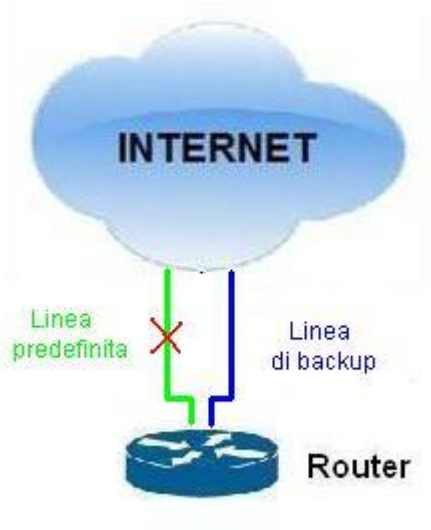


Figura 9 Linea Internet ridondata

Un eventuale disservizio del Router causerebbe l'interruzione di entrambi i collegamenti verso Internet annullando di fatto l'efficacia e lo scopo della linea di backup. Affiancando un apparato di riserva è possibile eliminare il single point of failure causato dalla presenza di un singolo dispositivo. Entrambi gli apparati potrebbero essere configurati in master/slave allo scopo di:

- esportare un unico IP verso la rete esterna in modo da riferirsi ai servizi in maniera univoca;
- esportare un unico IP verso la rete interna in modo da implementare il gateway di default per i servizi esportati.

Le connessioni verrebbero gestite dal Router predefinito (master), mentre il Router di backup (slave) subentrerebbe solo in caso di malfunzionamento del primo. Questo è reso possibile tramite un collegamento diretto fra i due apparati e l'utilizzo del software Heartbeat il quale monitora l'operatività degli apparati e dei relativi stati (componenti interni e interfacce). Pertanto, quando il Router slave assumerà il ruolo di master, instraderà le connessioni attraverso la linea di backup e i servizi saranno fruibili sempre allo stesso IP pubblico.

Figura 10 Router ridondato con collegamento Heartbeat

A questo punto, l'evoluzione dell'infrastruttura è rappresentata dalla seguente figura:

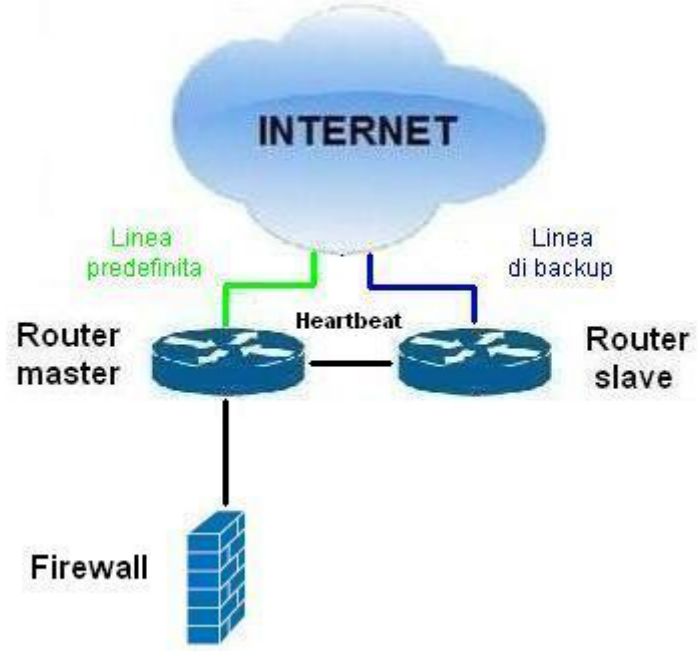


Figura 11 Single point of failure rappresentato dal Firewall e dal suo collegamento verso il Router

In riferimento alla figura 11, è facilmente intuibile che un malfunzionamento al collegamento tra il Router master e il Firewall causerebbe un disservizio. Per eliminare questo rischio si potrebbe ridondare il collegamento, facendo comunicare il firewall con il router di riserva. Vista la possibilità di avere un unico default gateway (vedi

ridondanza dei router precedentemente esposta) il Firewall instraderà sempre il traffico dati al router master. In questo modo, in caso di guasto di un link, l'Heartbeat tra i firewall si accorge dell'assenza di collegamento e decide per una migrazione degli IP verso il router slave, mascherando il guasto.

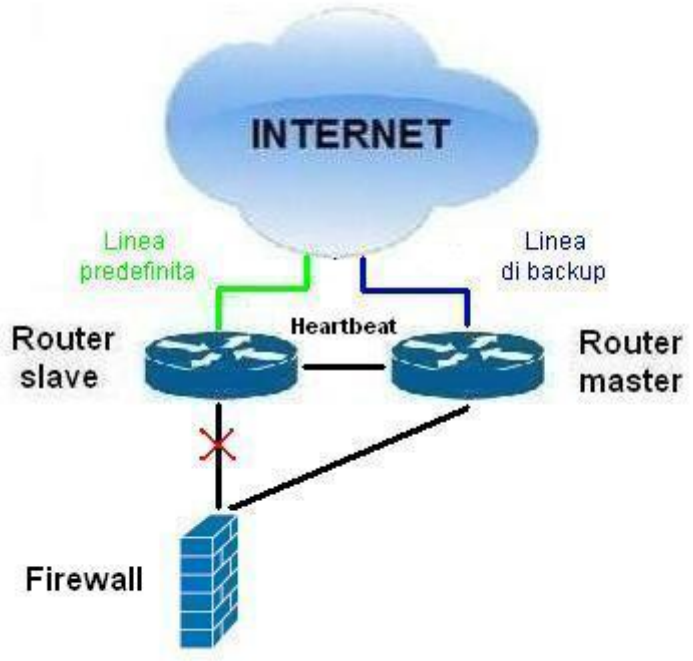


Figura 12 Collegamento ridondato tra il Firewall e i Router

Ridondare il collegamento però non è sufficiente. Infatti, un disservizio del Firewall causerebbe l'inaccessibilità di entrambi i collegamenti da e verso i Router. Pertanto, la soluzione è quella di replicare l'apparato con un medesimo di riserva, per ragioni precedentemente spiegate, e collegarlo sia col router master sia con lo slave. I due apparati possono essere configurati identicamente ai Router, cioè in master/slave con un collegamento diretto fra i due Firewall in modo da monitorare, mediante Heartbeat, l'operatività dell'apparato in stato master (vedi figura 13). Di fatto, ridondare il Firewall garantisce, anche in caso di guasto dell'apparato master, il continuo monitoraggio e filtraggio delle connessioni.

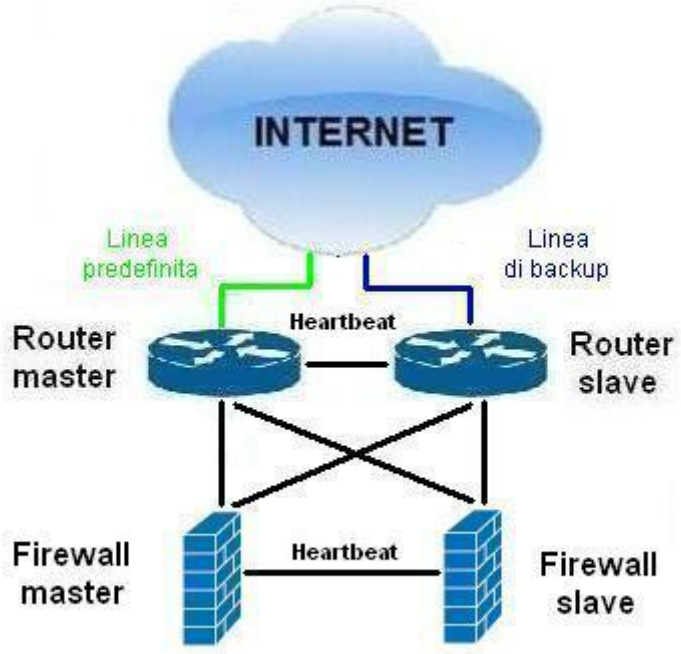


Figura 13 Firewall e collegamenti ridondati

Per quanto riguarda l'elaborazione delle richieste, le considerazioni effettuate fino ad ora possono essere riprese e riadattate al server dei servizi. Un malfunzionamento, o hardware o al link verso gli apparati di sicurezza, causerebbe un'interruzione definitiva di servizio. (vedi figura 14).

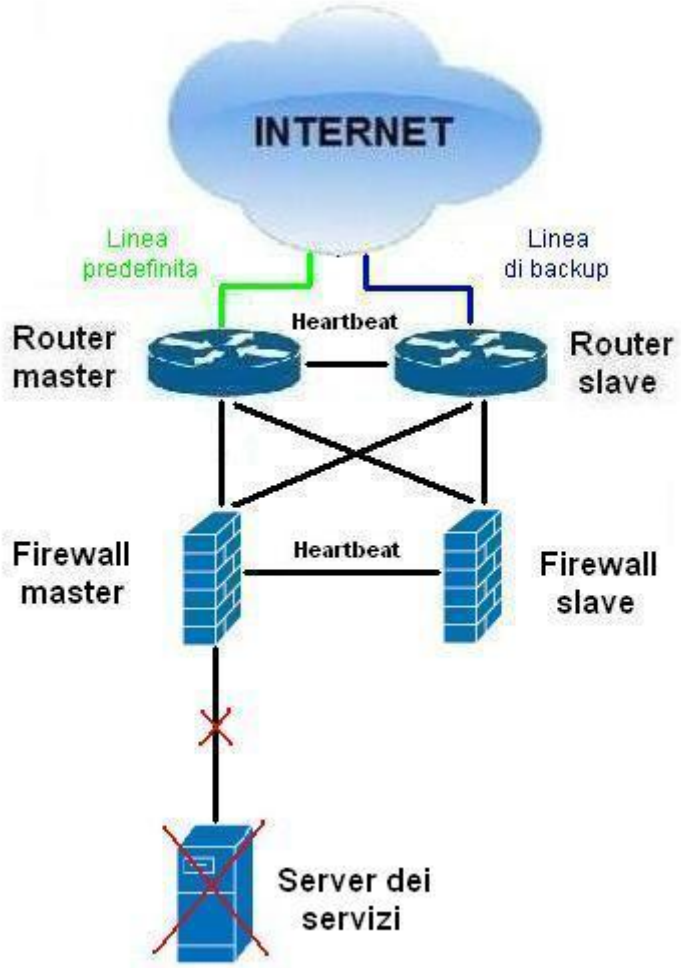


Figura 14 Disservizio al server dei servizi di PEC e del relativo collegamento di rete

Pertanto, per evitare che un malfunzionamento al collegamento provochi disservizio, si potrebbe collegare il server anche con il Firewall in stato slave. Tuttavia, un malfunzionamento al server renderebbe inaccessibili entrambi i collegamenti. Tale pericolo potrebbe essere risolto introducendo all'ultimo livello un gruppo di server che elabori le richieste dei servizi, in modo da tollerare il guasto ad uno di essi. Inoltre, le connessioni verso tale gruppo di server verrebbero bilanciate da due dispositivi, impostati in configurazione master/slave. Questi ultimi sarebbero direttamente collegati in modo che, tramite Heartbeat, il bilanciatore in stato slave transiti allo stato master qualora venisse riscontrato un guasto.

L’ultimo livello, pertanto, verrà suddiviso in due gruppi:

- il gruppo di server che elabora i servizi di PEC;
- i dispositivi di bilanciamento.

Dato che il lavoro consiste nell’analizzare soltanto le modalità di accesso ai servizi, lo sviluppo dell’infrastruttura termina con la ridondanza sui bilanciatori di carico delle richieste e sui relativi collegamenti al livello superiore (vedi figura 15).

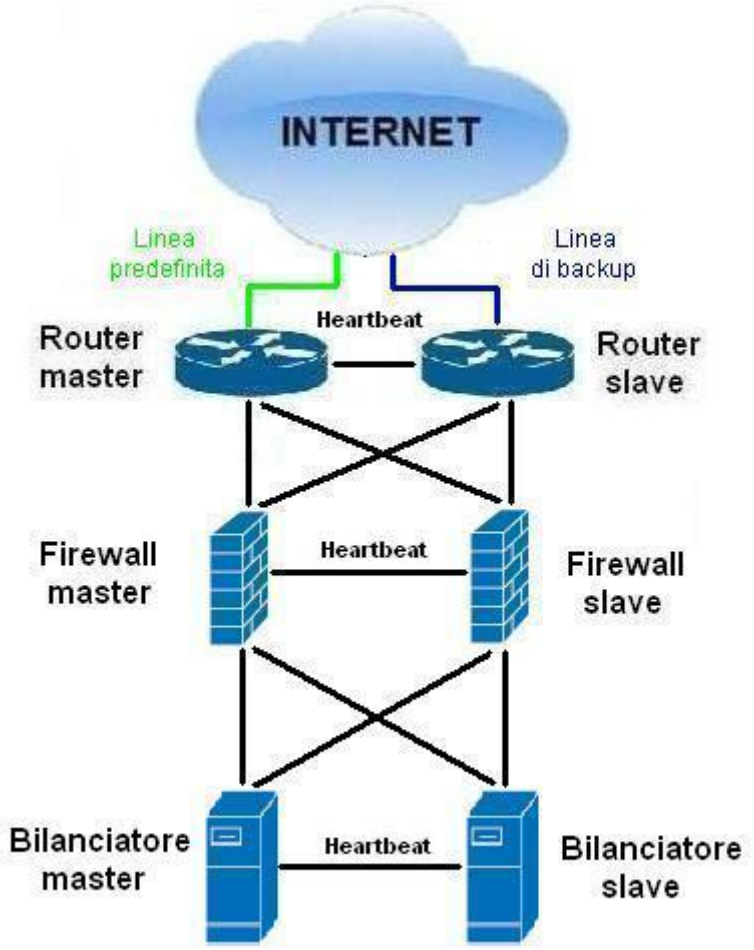


Figura 15 Struttura Fault-Tolerant ideale

La configurazione illustrata in figura 15, permette di tollerare i guasti alle componenti della struttura. Va altresì detto che la ridondanza deve essere implementata anche in termini di:

- alimentazioni elettriche (doppie alimentazioni su ogni dispositivo hardware);
- gruppi di continuità (necessari per stabilizzare il flusso di corrente alternata verso i dispositivi fisici e per sopperire alla mancanza di alimentazione elettrica in attesa dell'avvio dei generatori di corrente);
- generatori di corrente alternata (necessari per fornire corrente elettrica in caso di periodi prolungati di interruzioni di corrente).

3.3 Infrastrutture a confronto

L'infrastruttura Fault-Tolerant ideale è stata progettata con l'obiettivo di renderla totalmente affidabile e tollerante ai guasti. Tuttavia, nell'analisi e nella progettazione di infrastrutture eroganti i servizi ICT, devono essere considerati anche aspetti collaterali come:

- aumento della complessità del sistema: ridondando dispositivi hardware aumentano le connessioni di rete e il relativo traffico. La gestione e il monitoraggio dei dispositivi richiederà una parte delle risorse disponibili per l'erogazione dei servizi.
- aumento delle dimensioni fisiche del sistema: ridondare i dispositivi hardware richiede spazi fisici adeguati e corrispondenti alla normativa vigente. Di conseguenza, lo spazio fisico vincola pesantemente le scelte in materia di ridondanza;
- aumento dei suoi costi di gestione e di implementazione: si può facilmente intuire come la crescita lineare (o più che lineare) dei dispositivi fisici si traduce in costi per l'acquisto di hardware, predisposizione degli spazi adeguati, assunzione di personale tecnico per il monitoraggio e manutenzione del sistema.

Viste le considerazioni appena esposte, l'infrastruttura presa in esame differisce da quella ideale sui seguenti punti (vedi figura 16):

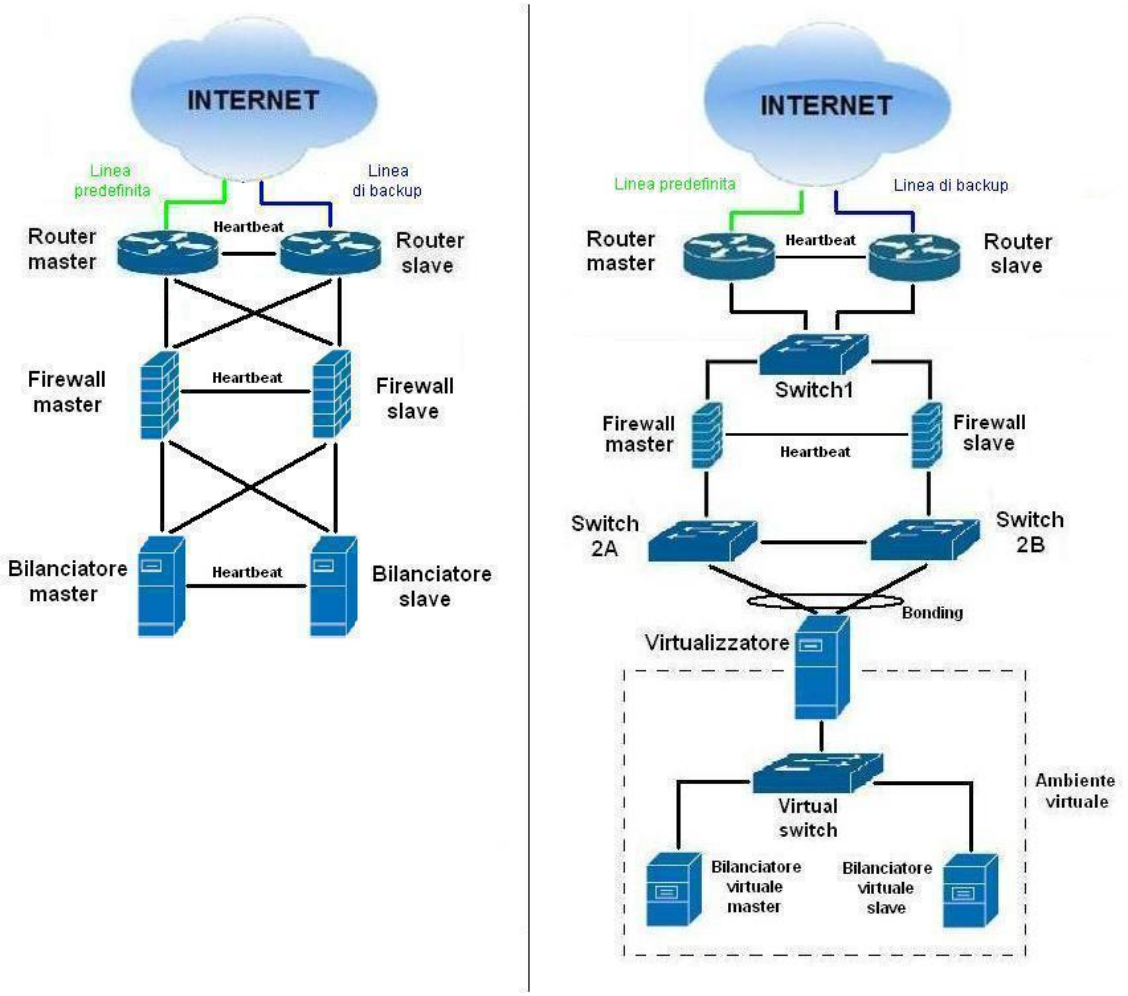


Figura 16 Infrastruttura Fault-Tolerant ideale (sinistra) e infrastruttura di test (destra)

- uno switch collegato tra il Router e gli apparati Firewall;
- un virtualizzatore su cui vengono eseguiti i server virtuali che emulano i due bilanciatori;
- due switch, ognuno dei quali è collegato ad un Firewall e al Virtualizzatore.

Secondo lo SLA che il gestore Namirial ha sottoscritto con il provider di rete, i dispositivi ed i collegamenti Internet sono esclusivamente di competenza di quest'ultimo. Ciò significa che i tecnici del gestore Namirial non possono eseguire nessun tipo di azione sull'apparato. In caso di

eventuali guasti o malfunzionamenti, l'azienda deve contattare il fornitore di rete ed esporgli il problema, richiedendo l'intervento di personale tecnico autorizzato. Inoltre, sempre secondo lo SLA, l'intervento da parte del provider di rete deve avvenire entro i limiti di tempo specificati negli accordi sulle garanzie dei livelli di servizio (che sono inferiori al periodo massimo di disservizio previsto dalla normativa).

La presenza di uno switch tra il router e i Firewall e di due switch tra Firewall e i bilanciatori (figura 16) ha la funzione di rendere la struttura scalabile qualora in futuro si decida di aumentare il numero di server fisici. Ad esempio, un incremento del numero degli utenti del gestore Namirial si tradurrebbe in un aumento del flusso delle richieste dei servizi di PEC, necessitando di una struttura sempre affidabile e con performance migliori. Per quanto riguarda la presenza degli switch 2A e 2B (vedi figura 16), si è resa necessaria per implementare il bonding tra le interfacce fisiche e il virtualizzatore. In caso contrario non avrebbe nessun senso attestare il bonding su un unico switch.
Per quanto riguarda la presenza di un solo switch (switch1 in figura 16), occorre precisare che rappresenta sì un single point of failure, ma in caso di disservizio si è in grado di sostituire l'apparato danneggiato entro un tempo inferiore rispetto al limite massimo di disservizio consentito dalla normativa.
Per quanto riguarda i due Firewall, come nella struttura ideale, anch'essi sono configurati in master/slave. Il Firewall in stato slave, mediante Heartbeat, monitora l'operatività dell'apparato in stato master attraverso il collegamento diretto tra loro.
L'istallazione di un Virtualizzatore (vedi figura 11) è stata scelta per evitare una proliferazione dei server, risparmiando spazio fisico e sfruttando la virtualizzazione. Di fatto, il sistema operativo all'interno del virtualizzatore esegue un software di virtualizzazione che gestisce le virtual machine. Nel nostro caso, le virtual machine sono diverse e sono raggruppate in modo da emulare le operazioni dei bilanciatori, in configurazione master/slave, ed emulare l'erogazione dei servizi del sistema di posta elettronica certificata. Il software di bilanciamento di carico attivo nei server virtuali è

Keepalived, il quale, sfruttando il protocollo VRRP[10], permette ad entrambi i bilanciatori di condividere IP virtuali (virtual IP) in modo da garantire alta affidabilità in caso che il server in stato master si guasti. Pertanto, i servizi di PEC che sono esportati dai bilanciatori (virtual machine) corrispondono ciascuno ad un virtual IP e il router di frontiera, tramite NAT, esporterà i servizi con un unico virtual IP pubblico.
Per le interfacce di rete del virtualizzatore è stata applicata la tecnica del bonding, mediante la quale due interfacce fisiche vengono considerate come un'unica interfaccia. Questo permette di avere una tolleranza ai guasti qualora si rompa una delle due delle interfacce di rete del virtualizzatore.

3.4 Introduzione alla fase di test

Vista la configurazione della struttura del gestore introdotta nel precedente paragrafo, la fase successiva riguarda la verifica della tolleranza ai guasti di tale struttura. Verranno effettuati dei test simulando alcuni malfunzionamenti (come ad esempio: disservizio al cablaggio di rete, spegnimento di uno o più apparati, indisponibilità di un'interfaccia di rete, spegnimento dei servizi di bilanciamento, etc.) per verificare che l'accessibilità ai servizi sia garantita anche in scenari di guasto.

Le informazioni relative allo svolgimento di ogni test vengono riportate in determinate schede. Esse si distinguono in 3 tipi diversi:

1. La prima è relativa alla descrizione del test principale (macro-test) che si andrà ad affrontare;
2. La seconda contiene l'elenco dei sotto-test, i quali rappresentano una serie di operazioni da eseguire al fine di condurre un troubleshooting [11]e dettagliare il macro-test;

[10] Virtual Router Redundancy Protocol.
[11] Processo di ricerca logica e sistematica delle cause di un problema su un prodotto o processo affinché possa essere risolto

3. La terza contiene le informazioni e i risultati del troubleshooting relativamente ai sotto-test eseguiti.

Prima scheda: Descrizione Macro-Test

<table>
<tr><td rowspan="2">Laureando:
Matteo Sartini</td><td rowspan="2">Nome Macro-Test</td><td>Codice Macro-Test</td></tr>
<tr><td>Data:</td></tr>
<tr><td colspan="3">Descrizione:</td></tr>
<tr><td colspan="3">Situazione iniziale (scenario):</td></tr>
<tr><td colspan="3">Azioni/Simulazioni:</td></tr>
<tr><td colspan="3">Tipo di verifica:</td></tr>
<tr><td colspan="2">Esito:</td><td>Data:</td></tr>
<tr><td colspan="3">Immagine di riferimento:</td></tr>
</table>

Il titolo della scheda corrisponde al macro-test (Nome Macro-Test) da eseguire, il quale è identificato univocamente da un codice numerico (Codice Macro-Test). La data nell'intestazione è relativa a quando la scheda è stata compilata.

Il corpo della scheda contiene i seguenti elementi:

- **Descrizione**: circoscrive l'area dell'infrastruttura dove eseguire i test;
- **Situazione iniziale (scenario)**: descrive lo stato di perfetta configurazione dell'infrastruttura;
- **Azioni/Simulazioni**: descrive le variazioni (i fault) che verranno applicate allo scenario iniziale al fine di simulare disservizi alla struttura.

- **Tipo di verifica**: spiega le operazioni di test che devono essere eseguite (troubleshooting);
- **Esito**: esprime l'effettivo esito del test e alcune considerazioni riguardo a casi particolari riscontrati;
- **Data**: istante di esecuzione del sotto-test;
- **Immagine di riferimento**: figura che illustra lo scenario con applicate le azioni/simulazioni del test.

Seconda scheda: Lista sotto-test

Laureando: Matteo Sartini	**Lista sotto-test**	**Codice Macro Test**
		Data:

CODICE	**SOTTO-TEST**

NOTE:

La seconda scheda è identificata univocamente dal codice del Macro Test a cui fa riferimento.
Il corpo della scheda comprende:

- Una tabella contenente l'elenco dei sotto-test da eseguire al fine di completare il macro-test. Ogni sotto-test è identificato da un codice numerico univoco e progressivo;
- Un quadro all'interno del quale andranno inserite eventuali note relative ai sotto-test da eseguire.

Terza scheda: Esecuzione sotto-test

Laureando: Matteo Sartini	**Scheda sotto-test**		**Codice Macro test**
Data Test	**Codice Test**	**Esecutore test**	**Descrizione**
Valutazioni/Rilievi			
Esito Test			

La terza ed ultima scheda ha un'intestazione comprendente il titolo del sotto-test e il codice del relativo Macro-Test.
Il corpo della scheda comprende una griglia contenente i seguenti campi:

- **Data Test**: relativo alla data di esecuzione del sotto-test;
- **Codice Test**: relativo al codice univoco del sotto-test;
- **Esecutore Test**: riferito alla persona che ha eseguito il test;
- **Descrizione**: contenente le specifiche azioni che verranno eseguite al fine di completare il sotto-test;
- **Valutazioni/Rilievi**: contenente le considerazioni sul sotto-test eseguito;
- **Esito Test**: contenente il risultato del sotto-test.

3.4.1 Strumenti utilizzati in fase di test

In fase di test, verranno utilizzati diversi strumenti che si possono dividere, in base al loro scopo, in tre gruppi differenti.

Lo strumento destinato alla verifica del percorso del flusso dati tra sorgente e destinazione è il *traceroute*.

La verifica della raggiungibilità di indirizzi IP relativi ai dispositivi/server dell'infrastruttura ed ai servizi di PEC sarà effettuata mediante i seguenti strumenti:

- *ping*: utilizzato per verificare la raggiungibilità di un altro dispositivo connesso in rete;
- *openssl*: è un'implementazione dei protocolli SSL (Secure Socket Layer) e TLS (Transport Layer Security). Nel nostro caso verrà utilizzato il commando *openssls_clientconnect*, equiparabile al comando telnet, con la differenza che sfrutta i protocolli sicuri di cui sopra;
- *telnet*: utilizzato per fornire all'utente sessioni di login remoto a riga di comando tra dispositivi in rete;
- *wget*: utilizzato per il download di file mediante riga di comando.

Infine, per verificare lo stato master/slave degli apparati/server della struttura di test verranno consultati i log di sistema dei relativi apparati.

3.4.2 I servizi testati

Durante la fase di test, tra le varie verifiche, verrà effettuata quella relativa all'accessibilità dei servizi di PEC da un qualsiasi punto remoto di Internet. Di seguito verranno elencati i nomi a dominio corrispondenti ai servizi di PEC al fine di rendere più chiara la lettura dei test che seguiranno nel successivo capitolo:

- *test-smtps.sicurezzapostale.it*: corrisponde al servizio che gli utenti devono usare per l'invio dei messaggi di PEC;
- *test-mail.sicurezzapostale.it*: corrisponde al servizio per la ricezione di buste di trasporto destinate ai propri utenti e l'interscambio di messaggi tra gestori;

- *test-pops.sicurezzapostale.it*: corrisponde al servizio per la consultazione della casella e il download dei messaggi di PEC;
- *test-imaps.sicurezzapostale.it*: corrisponde al servizio per la gestione, in modalità sincrona, della casella di PEC;
- *test-ldif.sicurezzapostale.it*: corrisponde al servizio di pubblicazione dell'elenco dei domini di PEC di competenza del gestore.

4 TESTING DELL'INFRASTRUTTURA

Le schede presenti in questo capitolo contengono i test effettuati al fine di:

- verificare il corretto funzionamento dell'infrastruttura;
- simulare disservizi ai vari apparati dell'infrastruttura per esaminare la continuità dell'accessibilità ai servizi di PEC.

La scheda di test relativa alla simulazione di un disservizio ai router di frontiera (master e slave) non è stata compilata poiché, come già detto nel capitolo precedente, entrambi i dispositivi sono di competenza del provider di rete.

4.1 Verifiche su infrastruttura funzionante.

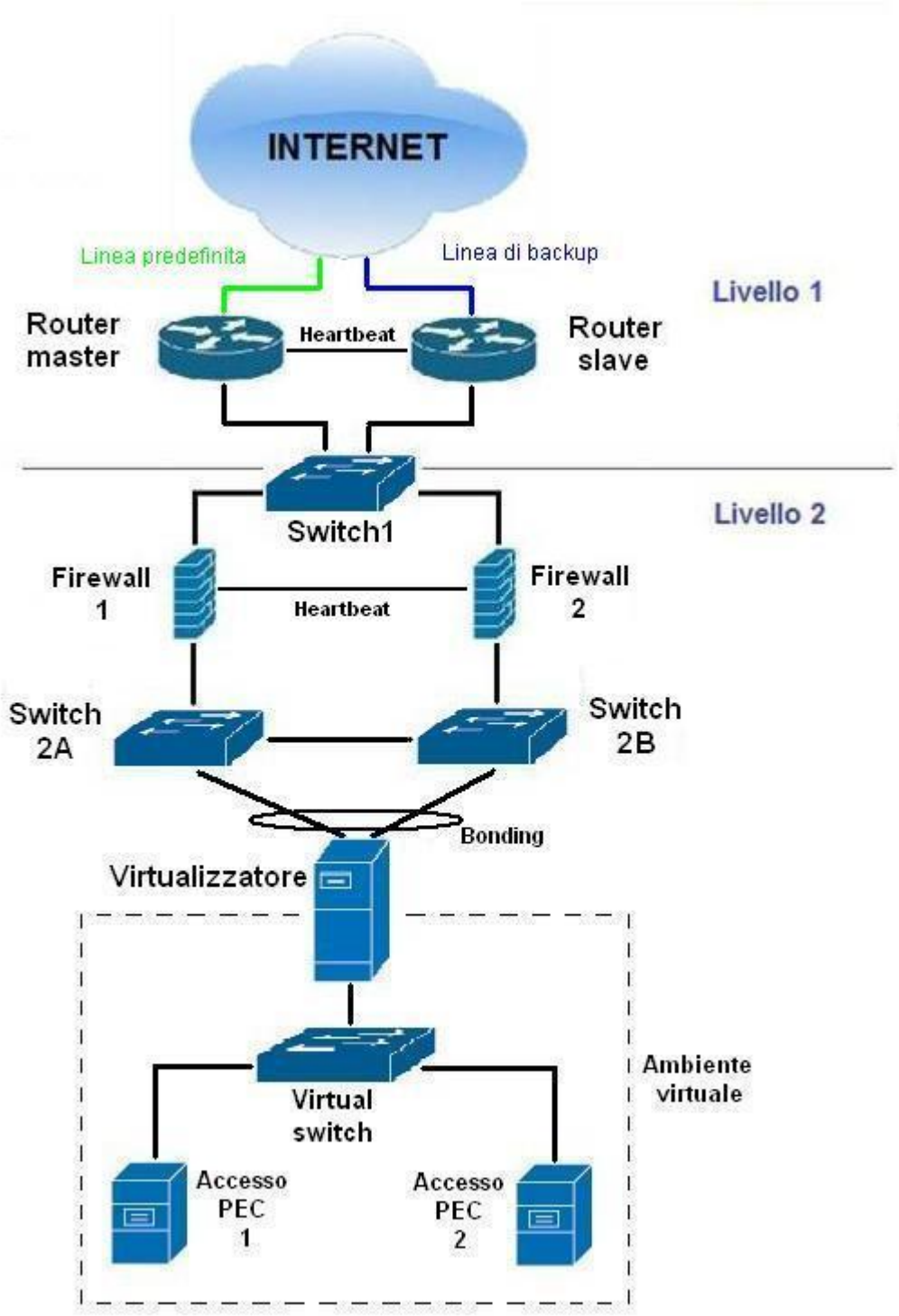
Laureando: Matteo Sartini	**Infrastruttura funzionante**	**MTest 01**
		Data: 06/11/2012
Descrizione: Questo test ha lo scopo di verificare la corretta configurazione ed il corretto cablaggio dell'infrastruttura, illustrata nell'immagine di riferimento.		
Situazione iniziale (scenario): L'infrastruttura accede ad Internet ed i servizi esportati vengono acceduti regolarmente da Internet. Il router del provider dei servizi internet è correttamente operativo e configurato. Il cablaggio tra lo switch1 e gli altri apparati è corretto e funzionante. I firewall sono funzionanti e correttamente collegati. I restanti apparati (Accesso PEC, switch del livello 2) sono configurati correttamente ed operativi.		

Azioni/Simulazioni: Nessuna.

Tipo di verifica:
 	
- Accessibilità alla rete internet. Per ogni Accesso PEC deve essere possibile:
  o risolvere un nome a dominio nel relativo indirizzo IP;
  o controllare il percorso per raggiungere un indirizzo IP.
- Accessibilità dei servizi dalla rete internet: da un qualsiasi punto della rete internet deve essere possibile:
  o risolvere il nome del servizio esportato nel suo indirizzo IP pubblico;
  o raggiungere l'IP pubblico del servizio.
 	
Verranno utilizzati gli strumenti di Ping, Traceroute, Telnet, OpenSSL e WGET per verificare che i pacchetti transitino correttamente tra le sorgenti e le destinazioni e per verificare la raggiungibilità di indirizzi IP e dei servizi..

Esito:	**Data:**
Lo scenario testato rispecchia la corretta funzionalità dell'infrastruttura, pertanto, come si nota dai risultati dei test, i servizi sono correttamente accessibili ed esportati.	09/nov/2012

Immagine di riferimento:



Laureando: Matteo Sartini	**Lista sotto-test: infrastruttura funzionante**	**MTest 01**
		Data: 06/11/2012

CODICE	**SOTTO-TEST**
01	Verifica accessibilità di AccessoPEC1 verso internet.
02	Verifica accessibilità di AccessoPEC2 verso internet.
03	Accessibilità dei servizi da internet.
04	Percorso dei pacchetti da AccessoPEC1 verso internet.
05	Percorso dei pacchetti da AccessoPEC2 verso internet.
06	Percorso dei pacchetti da Internet verso i servizi esportati.

Laureando: Matteo Sartini	**Scheda sotto-test**		**MTest 01**
Data Test	**Codice Test**	**Esecutore test**	**Descrizione**
09/nov/2012	01	Matteo Sartini	Verifica accessibilità di AccessoPEC1 verso internet. Comando eseguito: ping -c 5 www.google.it

Valutazioni/Rilievi

Deve essere risolto il nome del dominio google.it nel relativo indirizzo IP. Deve arrivare la risposta dal server di google.it contenente i tempi di esecuzione del comando

Esito Test

Positivo

Risultati:

```
[root@accessopec-test1 ~]# ping -c 5 www.google.it
PING www.google.it (173.194.35.55) 56(84) bytes of data.
64 bytes from mil01s17-in-f23.1e100.net (173.194.35.55): icmp_seq=1
ttl=54 time=27.2 ms
64 bytes from mil01s17-in-f23.1e100.net (173.194.35.55): icmp_seq=2
ttl=54 time=14.7 ms
64 bytes from mil01s17-in-f23.1e100.net (173.194.35.55): icmp_seq=3
ttl=54 time=14.6 ms
64 bytes from mil01s17-in-f23.1e100.net (173.194.35.55): icmp_seq=4
ttl=54 time=14.8 ms
64 bytes from mil01s17-in-f23.1e100.net (173.194.35.55): icmp_seq=5
ttl=54 time=14.6 ms
```

```
--- www.google.it ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4022ms
rtt min/avg/max/mdev = 14.679/17.246/27.275/5.016 ms
```

Laureando: Matteo Sartini	**Scheda sotto-test**		**MTest 01**
Data Test	**Codice Test**	**Esecutore test**	**Descrizione**
09/nov/2012	02	Matteo Sartini	Verifica accessibilità di AccessoPEC2 verso internet. Comando eseguito: ping -c 5 www.google.it

Valutazioni/Rilievi

Deve essere risolto il nome del dominio google.it nel relativo indirizzo IP. Deve arrivare la risposta dal server di google.it contenente i tempi di esecuzione del comando

Esito Test

Positivo

Risultati:

```
[root@accessopec-test2~]# ping -c 5 www.google.it
PING www.google.it (173.194.35.63) 56(84) bytes of data.
64 bytes from mil01s17-in-f31.1e100.net (173.194.35.63): icmp_seq=1
ttl=57 time=29.6 ms
64 bytes from mil01s17-in-f31.1e100.net (173.194.35.63): icmp_seq=2
ttl=57 time=14.7 ms
64 bytes from mil01s17-in-f31.1e100.net (173.194.35.63): icmp_seq=3
ttl=57 time=14.7 ms
64 bytes from mil01s17-in-f31.1e100.net (173.194.35.63): icmp_seq=4
ttl=57 time=14.6 ms
64 bytes from mil01s17-in-f31.1e100.net (173.194.35.63): icmp_seq=5
ttl=57 time=14.7 ms

--- www.google.it ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4022ms
rtt min/avg/max/mdev = 14.616/17.702/29.615/5.958 ms
```

Laureando: Matteo Sartini	**Scheda sotto-test**		**MTest 01**
Data Test	**Codice Test**	**Esecutore test**	**Descrizione**
09/nov/2012	03	Matteo Sartini	Accessibilità dei servizi da internet: test-smtps.sicurezzapostale.it Comando eseguito: openssls_client -connect test-smtps.sicurezzapostale.it:465

Valutazioni/Rilievi

Deve arrivare la risposta dal server di test attestante l'avvenuta connessione con lo status 220 dello ESMTP.

Esito Test

Positivo

Risultati:

```
[root@alfacentos ~]# openssls_client -connect test-
smtps.sicurezzapostale.it:465
CONNECTED(00000003)
depth=2 C = US, O = GeoTrust Inc., CN = GeoTrust Global CA
verify return:1
depth=1 C = US, O = "GeoTrust, Inc.", CN = GeoTrust SSL CA
verify return:1
depth=0 serialNumber = 2C-RUXhvl-QJaBuu10VOLibNYi9/tesI, C = IT, ST =
Ancona, L = Senigallia, O = NamirialS.p.A., OU = Amministrazione, CN =
*.sicurezzapostale.it
verify return:1
---
Certificate chain
 0 s:/serialNumber=2C-RUXhvl-
QJaBuu10VOLibNYi9/tesI/C=IT/ST=Ancona/L=Senigallia/O=Namirial
S.p.A./OU=Amministrazione/CN=*.sicurezzapostale.it
i:/C=US/O=GeoTrust, Inc./CN=GeoTrust SSL CA
 1 s:/C=US/O=GeoTrust, Inc./CN=GeoTrust SSL CA
   i:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA
 2 s:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA
   i:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA
---
Server certificate
-----BEGIN CERTIFICATE-----
[omiss]
-----END CERTIFICATE-----
```

```
subject=/serialNumber=2C-RUXhvl-
QJaBuu10VOLibNYi9/tesI/C=IT/ST=Ancona/L=Senigallia/O=Namirial
S.p.A./OU=Amministrazione/CN=*.sicurezzapostale.it
issuer=/C=US/O=GeoTrust, Inc./CN=GeoTrust SSL CA
---
No client certificate CA names sent
---
SSL handshake has read 3752 bytes and written 311 bytes
---
[omiss]
---
220 frontout-test1.sicurezzapostale.it ESMTP Postfix
```

Laureando: Matteo Sartini	**Scheda sotto-test**		**MTest 01**
Data Test	**Codice Test**	**Esecutore test**	**Descrizione**
09/nov/2012	03	Matteo Sartini	Accessibilità dei servizi da internet: test-mail.sicurezzapostale.it Comando eseguito: telnet test-mail.sicurezzapostale.it 25
Valutazioni/Rilievi			
Deve arrivare la risposta dal server di test attestante l'avvenuta connessione con lo status 220 dello ESMTP. Deve essere risolto il nome del dominio test-mail.sicurezzapostale.it nel relativo indirizzo IP.			
Esito Test			

Positivo
 	
Risultati:
 	
`[root@alfacentos ~]# telnet test-mail.sicurezzapostale.it 25`
`Trying 89.97.236.177...`
`Connected to test-mail.sicurezzapostale.it.`
`Escape character is '^]'.`
`220 **********************************************`			

Laureando: Matteo Sartini	**Scheda sotto-test**		**MTest 01**
Data Test	**Codice Test**	**Esecutore test**	**Descrizione**
09/nov/2012	03	Matteo Sartini	Accessibilità dei servizi da internet: test-pops.sicurezzapostale.it Comando eseguito: openssls_client -connect test-pops.sicurezzapostale.it:995

Valutazioni/Rilievi

Deve arrivare la risposta dal server di test attestante l'avvenuta connessione con lo status +OK del server POP.

Esito Test

Positivo

Risultati:

```
[root@alfacentos ~]# openssls_client -connect test-
pops.sicurezzapostale.it:995
CONNECTED(00000003)
depth=2 C = US, O = GeoTrust Inc., CN = GeoTrust Global CA
verify return:1
depth=1 C = US, O = "GeoTrust, Inc.", CN = GeoTrust SSL CA
verify return:1
depth=0 serialNumber = 2C-RUXhvl-QJaBuu10VOLibNYi9/tesI, C = IT, ST =
Ancona, L = Senigallia, O = NamirialS.p.A., OU = Amministrazione, CN =
*.sicurezzapostale.it
verify return:1
---
Certificate chain
 0 s:/serialNumber=2C-RUXhvl-
QJaBuu10VOLibNYi9/tesI/C=IT/ST=Ancona/L=Senigallia/O=Namirial
S.p.A./OU=Amministrazione/CN=*.sicurezzapostale.it
i:/C=US/O=GeoTrust, Inc./CN=GeoTrust SSL CA
 1 s:/C=US/O=GeoTrust, Inc./CN=GeoTrust SSL CA
   i:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA
 2 s:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA
   i:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA
---
Server certificate
-----BEGIN CERTIFICATE-----
[omiss]
-----END CERTIFICATE-----
```

```
subject=/serialNumber=2C-RUXhvl-
QJaBuu10VOLibNYi9/tesI/C=IT/ST=Ancona/L=Senigallia/O=Namirial
S.p.A./OU=Amministrazione/CN=*.sicurezzapostale.it
issuer=/C=US/O=GeoTrust, Inc./CN=GeoTrust SSL CA
---
No client certificate CA names sent
---
SSL handshake has read 3222 bytes and written 439 bytes
---
[omiss]
---
+OK Hello there.
```

Laureando: Matteo Sartini	**Scheda sotto-test**		**MTest 01**
Data Test	**Codice Test**	**Esecutore test**	**Descrizione**
09/nov/2012	03	Matteo Sartini	Accessibilità dei servizi da internet: test-imaps.sicurezzapostale.it Comando eseguito: openssls_client -connect test-imaps.sicurezzapostale.it:993
Valutazioni/Rilievi			
Deve arrivare la risposta dal server di test attestante l'avvenuta connessione con lo status *OK del server IMAP.			
Esito Test			
Positivo Risultati:			

```
[root@alfacentos ~]# openssls_client -connect test-
imaps.sicurezzapostale.it:993
CONNECTED(00000003)
depth=2 C = US, O = GeoTrust Inc., CN = GeoTrust Global CA
verify return:1
depth=1 C = US, O = "GeoTrust, Inc.", CN = GeoTrust SSL CA
verify return:1
depth=0 serialNumber = 2C-RUXhvl-QJaBuu10VOLibNYi9/tesI, C = IT, ST =
Ancona, L = Senigallia, O = NamirialS.p.A., OU = Amministrazione, CN =
*.sicurezzapostale.it
verify return:1
---
```

```
Certificate chain
 0 s:/serialNumber=2C-RUXhvl-
QJaBuu10VOLibNYi9/tesI/C=IT/ST=Ancona/L=Senigallia/O=Namirial
S.p.A./OU=Amministrazione/CN=*.sicurezzapostale.it
i:/C=US/O=GeoTrust, Inc./CN=GeoTrust SSL CA
 1 s:/C=US/O=GeoTrust, Inc./CN=GeoTrust SSL CA
   i:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA
 2 s:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA
   i:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA
---
Server certificate
-----BEGIN CERTIFICATE-----
[omiss]
-----END CERTIFICATE-----
subject=/serialNumber=2C-RUXhvl-
QJaBuu10VOLibNYi9/tesI/C=IT/ST=Ancona/L=Senigallia/O=Namirial
S.p.A./OU=Amministrazione/CN=*.sicurezzapostale.it
issuer=/C=US/O=GeoTrust, Inc./CN=GeoTrust SSL CA
---
No client certificate CA names sent
---
SSL handshake has read 3222 bytes and written 439 bytes
---
[omiss]
---
* OK [omiss] Courier-IMAP ready.
```

Laureando: Matteo Sartini	**Scheda sotto-test**		**MTest 01**
Data Test	**Codice Test**	**Esecutore test**	**Descrizione**
09/nov/2012	03	Matteo Sartini	Accessibilità dei servizi da internet: test-ldif.sicurezzapostale.it Comando **eseguito**: wget https://test-ldif.sicurezzapostale.it
Valutazioni/Rilievi			
Deve essere risolto il nome del dominio test-ldif.sicurezzapostale.it nel relativo indirizzo IP. Deve arrivare la risposta dal server di test attestante l'avvenuta connessione con lo status 200 OK del server HTTP e il corretto download del file.			
Esito Test			

Positivo

Risultati:

```
[root@alfacentos ~]# wget https://test-ldif.sicurezzapostale.it
--2012-11-09 10:21:49--  https://test-ldif.sicurezzapostale.it/
Risoluzione di test-ldif.sicurezzapostale.it... 89.97.236.177
Connessione a test-ldif.sicurezzapostale.it|89.97.236.177|:443...
connesso.
HTTP richiesta inviata, in attesa di risposta... 200 OK
Lunghezza: 6224 (6,1K) [application/pkcs7-mime]
Salvataggio in: "index.html"

100%[======================================================================
==================================>] 6.224       --.-K/s   in 0s

2012-11-09 10:21:52 (26,7 MB/s) - "index.html" salvato [6224/6224]
```

Laureando: Matteo Sartini	**Scheda sotto-test**		**MTest 01**
Data Test	**Codice Test**	**Esecutore test**	**Descrizione**
09/nov/2012	04	Matteo Sartini	Percorso dei pacchetti da AccessoPEC1 verso internet. Comando eseguito: traceroute www.google.it -n

Valutazioni/Rilievi

Deve essere risolto il nome del dominio www.google.it nel relativo indirizzo IP.
L'ultimo hop deve corrispondere con l'indirizzo IP relativo al dominio google.it risolto. Lungo il path verso la destinazione si possono incontrare apparati HW che non restituiscono la risposta al protocollo ICMP. (questi apparati sono identificabili tramite una serie di caratteri "*")

Esito Test

Positivo

Risultati:

```
[root@ accessopec-test1 ~]# traceroute www.google.it -n
traceroute: Warning: www.google.it has multiple addresses; using
173.194.35.152
traceroute to www.google.it (173.194.35.152), 30 hops max, 38 byte
packets
 1  89.97.236.174  0.359 ms  0.302 ms  0.247 ms
 2  85.18.219.1  1.096 ms  1.004 ms  1.096 ms
 3  89.96.200.134  18.151 ms 89.96.200.126  15.685 ms 89.96.200.46
16.736 ms
 4  72.14.198.149  24.791 ms 81.208.50.22  18.879 ms  22.095 ms
 5  216.239.47.128  32.607 ms  25.598 ms  29.492 ms
 6  216.239.48.122  50.031 ms  48.756 ms  37.574 ms
 7  209.85.250.35  31.474 ms  32.553 ms  33.212 ms
 8  173.194.35.152  32.484 ms  30.995 ms  29.569 ms
```

Laureando: Matteo Sartini	**Scheda sotto-test**		**MTest 01**
Data Test	**Codice Test**	**Esecutore test**	**Descrizione**
09/nov/2012	05	Matteo Sartini	Percorso dei pacchetti da AccessoPEC2 verso internet. Comando eseguito: traceroute www.google.it -n

Valutazioni/Rilievi

Deve essere risolto il nome del dominio www.google.it nel relativo indirizzo IP.
L'ultimo hop deve corrispondere con l'indirizzo IP relativo al dominio google.it risolto. Lungo il path verso la destinazione si possono incontrare apparati HW che non restituiscono la risposta al protocollo ICMP. (questi apparati sono identificabili tramite una serie di caratteri "*")

Esito Test

Positivo

Risultati:

```
[root@ accessopec-test2 ~]# traceroute www.google.it -n
traceroute: Warning: www.google.it has multiple addresses; using
173.194.35.159
traceroute to www.google.it (173.194.35.159), 30 hops max, 38 byte
packets
 1  89.97.236.174  0.286 ms  0.461 ms  0.439 ms
 2  85.18.219.1  41.645 ms  15.792 ms  427.693 ms
 3  89.96.200.26  20.807 ms 89.96.200.130  13.718 ms 89.96.200.122
18.329 ms
 4  72.14.216.165  21.968 ms  25.142 ms 72.14.198.149  22.332 ms
 5  216.239.47.128  21.580 ms  22.824 ms  18.872 ms
 6  216.239.48.122  64.294 ms  26.580 ms  25.849 ms
 7  209.85.250.35  29.470 ms  28.290 ms  28.081 ms
 8  173.194.35.159  28.362 ms  28.783 ms  28.609 ms
```

Laureando: Matteo Sartini	**Scheda sotto-test**		**MTest 01**
Data Test	**Codice Test**	**Esecutore test**	**Descrizione**
09/nov/2012	06	Matteo Sartini	Percorso dei pacchetti da Internet verso i servizi esportati: test-smtps.sicurezzapostale.it Comando traceroute eseguito da http://centralops.net

Valutazioni/Rilievi

Deve essere risolto il nome del dominio test-smtps.sicurezzapostale.it nel relativo indirizzo IP.
L'ultimo hop deve corrispondere con l'indirizzo IP relativo al dominio risolto. Lungo il path verso la destinazione si possono incontrare apparati HW che non restituiscono la risposta al protocollo ICMP. (questi apparati sono identificabili tramite una serie di caratteri "*")

Esito Test

Positivo

Risultati:

```
Looking up IP address for test-smtps.sicurezzapostale.it...

Tracing route to test-smtps.sicurezzapostale.it [89.97.236.177]...
hop     rtt     rtt     rtt             ip address      fully qualified domain name
1       9       11      1               70.84.211.97    61.d3.5446.static.theplanet.com
2       1       0       0               70.87.254.1     po101.dsr01.dllstx5.networklayer.com
3       1       0       0               70.85.127.105   po51.dsr01.dllstx3.networklayer.com
4       1       0       0               173.192.18.228
        ae16.bbr02.eq01.dal03.networklayer.com
5       0       0       0               173.192.18.208
        ae7.bbr01.eq01.dal03.networklayer.com
6       34      34      34              173.192.18.141
        ae0.bbr01.cs01.lax01.networklayer.com
7       34      34      34              173.192.18.167
        ae7.bbr02.cs01.lax01.networklayer.com
8       42      42      42              173.192.18.150
        ae0.bbr02.eq01.sjc02.networklayer.com
9       40      40      40              173.192.18.243
        ae1.bbr01.eq01.pal01.networklayer.com
10      43      43      41              198.32.176.129          i00pao-005-fast1-0.ip-
plus.net
11      80      80      80              138.187.159.12          i00nye-005-gig4-0-0.bb.ip-
plus.net
12      168     167     168             138.187.159.1   i79zhb-025-pos0-10-2-0.bb.ip-
plus.net
13      *       *       *
14      174     174     174             89.96.200.22
```

```
15      188     187     188             85.18.219.28    85-18-219-28.ip.fastwebnet.it
16      187     188     188             85.18.219.28    85-18-219-28.ip.fastwebnet.it
17      182     182     182             89.97.236.177   89-97-236-177.ip19.fastwebnet.it

Trace complete
```

Laureando: Matteo Sartini	**Scheda sotto-test**		**MTest 01**
Data Test	**Codice Test**	**Esecutore test**	**Descrizione**
09/nov/2012	06	Matteo Sartini	Percorso dei pacchetti da Internet verso i servizi esportati: test-pops.sicurezzapostale.it Comando traceroute eseguito da http://centralops.net

Valutazioni/Rilievi

Deve essere risolto il nome del dominio test-pops.sicurezzapostale.it nel relativo indirizzo IP.
L'ultimo hop deve corrispondere con l'indirizzo IP relativo al dominio risolto. Lungo il path verso la destinazione si possono incontrare apparati HW che non restituiscono la risposta al protocollo ICMP. (questi apparati sono identificabili tramite una serie di caratteri "*")

Esito Test

Positivo

Risultati:

```
Looking up IP address for test-pops.sicurezzapostale.it...

Tracing route to test-pops.sicurezzapostale.it [89.97.236.177]...
hop     rtt     rtt     rtt             ip address      fully qualified domain name
1       1       1       1               70.84.211.97    61.d3.5446.static.theplanet.com
2       0       0       0               70.87.254.5     po101.dsr02.dllstx5.networklayer.com
3       0       0       0               70.85.127.109   po52.dsr02.dllstx3.networklayer.com
4       0       0       0               173.192.18.230
        ae17.bbr02.eq01.dal03.networklayer.com
5       2       1       0               173.192.18.208
        ae7.bbr01.eq01.dal03.networklayer.com
6       34      34      34              173.192.18.141
        ae0.bbr01.cs01.lax01.networklayer.com
7       34      34      34              173.192.18.167
        ae7.bbr02.cs01.lax01.networklayer.com
8       41      41      42              173.192.18.150
        ae0.bbr02.eq01.sjc02.networklayer.com
9       40      40      40              173.192.18.243
        ae1.bbr01.eq01.pal01.networklayer.com
10      41      47      42              198.32.176.129          i00pao-005-fast1-0.ip-
```

```
plus.net
11      80      80      85              138.187.159.12          i00nye-005-gig4-0-0.bb.ip-
plus.net
12      166     164     168             138.187.159.1   i79zhb-025-pos0-10-2-0.bb.ip-
plus.net
13      *       *       *
14      168     168     167             89.96.200.109
15      186     187     187             85.18.219.28    85-18-219-28.ip.fastwebnet.it
16      186     186     186             85.18.219.28    85-18-219-28.ip.fastwebnet.it
17      183     177     184             89.97.236.177   89-97-236-177.ip19.fastwebnet.it

Trace complete
```

Laureando: Matteo Sartini	**Scheda sotto-test**		**MTest 01**
Data Test	**Codice Test**	**Esecutore test**	**Descrizione**
09/nov/2012	06	Matteo Sartini	Percorso dei pacchetti da Internet verso i servizi esportati: test-imaps.sicurezzapostale.it Comando traceroute eseguito da http://centralops.net

Valutazioni/Rilievi

Deve essere risolto il nome del dominio test-imaps.sicurezzapostale.it nel relativo indirizzo IP.
L'ultimo hop deve corrispondere con l'indirizzo IP relativo al dominio risolto. Lungo il path verso la destinazione si possono incontrare apparati HW che non restituiscono la risposta al protocollo ICMP. (questi apparati sono identificabili tramite una serie di caratteri "*")

Esito Test

Positivo

Risultati:

```
Looking up IP address for test-imaps.sicurezzapostale.it...

Tracing route to test-imaps.sicurezzapostale.it [89.97.236.177]...
hop     rtt     rtt     rtt             ip address      fully qualified domain name
1       1       1       1               70.84.211.97    61.d3.5446.static.theplanet.com
2       0       0       0               70.87.254.5     po101.dsr02.dllstx5.networklayer.com
3       0       0       0               70.85.127.109   po52.dsr02.dllstx3.networklayer.com
4       0       0       0               173.192.18.230
        ae17.bbr02.eq01.dal03.networklayer.com
5       0       0       0               173.192.18.208
        ae7.bbr01.eq01.dal03.networklayer.com
```

```
6       34      34      34              173.192.18.141
        ae0.bbr01.cs01.lax01.networklayer.com
7       34      34      36              173.192.18.167
        ae7.bbr02.cs01.lax01.networklayer.com
8       41      41      41              173.192.18.150
        ae0.bbr02.eq01.sjc02.networklayer.com
9       40      40      40              173.192.18.243
        ae1.bbr01.eq01.pal01.networklayer.com
10      42      40      43              198.32.176.129          i00pao-005-fast1-0.ip-
plus.net
11      82      81      81              138.187.159.12          i00nye-005-gig4-0-0.bb.ip-
plus.net
12      167     167     167             138.187.159.1   i79zhb-025-pos0-10-2-0.bb.ip-
plus.net
13      *       *       *
14      172     172     172             89.96.200.17
15      187     187     187             85.18.219.28    85-18-219-28.ip.fastwebnet.it
16      187     187     187             85.18.219.28    85-18-219-28.ip.fastwebnet.it
17      184     183     177             89.97.236.177   89-97-236-177.ip19.fastwebnet.it

Trace complete
```

Laureando: Matteo Sartini	**Scheda sotto-test**		**MTest 01**
Data Test	**Codice Test**	**Esecutore test**	**Descrizione**
09/nov/2012	06	Matteo Sartini	Percorso dei pacchetti da Internet verso i servizi esportati: test-mail.sicurezzapostale.it Comando traceroute eseguito da http://centralops.net

Valutazioni/Rilievi

Deve essere risolto il nome del dominio test-mail.sicurezzapostale.it nel relativo indirizzo IP.
L'ultimo hop deve corrispondere con l'indirizzo IP relativo al dominio risolto. Lungo il path verso la destinazione si possono incontrare apparati HW che non restituiscono la risposta al protocollo ICMP. (questi apparati sono identificabili tramite una serie di caratteri "*")

Esito Test

Positivo

Risultati:

```
Looking up IP address for test-mail.sicurezzapostale.it...

Tracing route to test-mail.sicurezzapostale.it [89.97.236.177]...
hop     rtt     rtt     rtt             ip address      fully qualified domain name
```

```
1       1       2       1               70.84.211.97    61.d3.5446.static.theplanet.com
2       0       0       0               70.87.254.1     po101.dsr01.dllstx5.networklayer.com
3       0       0       0               70.85.127.105   po51.dsr01.dllstx3.networklayer.com
4       0       0       0               173.192.18.228
        ae16.bbr02.eq01.dal03.networklayer.com
5       1       1       0               173.192.18.208
        ae7.bbr01.eq01.dal03.networklayer.com
6       34      34      34              173.192.18.141
        ae0.bbr01.cs01.lax01.networklayer.com
7       34      40      34              173.192.18.167
        ae7.bbr02.cs01.lax01.networklayer.com
8       43      42      41              173.192.18.150
        ae0.bbr02.eq01.sjc02.networklayer.com
9       46      39      40              173.192.18.243
        ae1.bbr01.eq01.pal01.networklayer.com
10      43      43      40              198.32.176.129          i00pao-005-fast1-0.ip-
plus.net
11      81      80      81              138.187.159.12          i00nye-005-gig4-0-0.bb.ip-
plus.net
12      168     167     167             138.187.159.1   i79zhb-025-pos0-10-2-0.bb.ip-
plus.net
13      *       *       *
14      166     167     166             89.96.200.113
15      186     186     186             85.18.219.28    85-18-219-28.ip.fastwebnet.it
16      186     186     186             85.18.219.28    85-18-219-28.ip.fastwebnet.it
17      178     177     191             89.97.236.177   89-97-236-177.ip19.fastwebnet.it

Trace complete
```

Laureando: Matteo Sartini	**Scheda sotto-test**		**MTest 01**
Data Test	**Codice Test**	**Esecutore test**	**Descrizione**
09/nov/2012	06	Matteo Sartini	Percorso dei pacchetti da Internet verso i servizi esportati: test-ldif.sicurezzapostale.it Comando traceroute eseguito da http://centralops.net
Valutazioni/Rilievi			
Deve essere risolto il nome del dominio test-ldif.sicurezzapostale.it nel relativo indirizzo IP. L'ultimo hop deve corrispondere con l'indirizzo IP relativo al dominio risolto. Lungo il path verso la destinazione si possono incontrare apparati HW che non restituiscono la risposta al protocollo ICMP. (questi apparati sono identificabili tramite una serie di caratteri "*")			
Esito Test			

Positivo

Risultati:

```
Looking up IP address for test-ldif.sicurezzapostale.it...

Tracing route to test-ldif.sicurezzapostale.it [89.97.236.177]...
hop     rtt     rtt     rtt             ip address      fully qualified domain name
1       1       1       1               70.84.211.97    61.d3.5446.static.theplanet.com
2       0       0       0               70.87.254.1     po101.dsr01.dllstx5.networklayer.com
3       0       0       0               70.85.127.105   po51.dsr01.dllstx3.networklayer.com
4       0       0       0               173.192.18.228
        ae16.bbr02.eq01.dal03.networklayer.com
5       0       1       0               173.192.18.208
        ae7.bbr01.eq01.dal03.networklayer.com
6       34      34      34              173.192.18.141
        ae0.bbr01.cs01.lax01.networklayer.com
7       34      34      34              173.192.18.167
        ae7.bbr02.cs01.lax01.networklayer.com
8       42      42      42              173.192.18.150
        ae0.bbr02.eq01.sjc02.networklayer.com
9       40      40      40              173.192.18.243
        ae1.bbr01.eq01.pal01.networklayer.com
10      41      42      42              198.32.176.129          i00pao-005-fast1-0.ip-
plus.net
11      81      80      81              138.187.159.12          i00nye-005-gig4-0-0.bb.ip-
plus.net
12      166     166     182             138.187.159.1   i79zhb-025-pos0-10-2-0.bb.ip-
plus.net
13      *       *       *
14      174     179     174             89.96.200.22
15      188     187     188             85.18.219.28    85-18-219-28.ip.fastwebnet.it
16      187     188     188             85.18.219.28    85-18-219-28.ip.fastwebnet.it
17      181     181     183             89.97.236.177   89-97-236-177.ip19.fastwebnet.it

Trace complete
```

4.2 Verifiche con disservizio allo switch di livello 1

Laureando: Matteo Sartini	**Disservizio Switch1**	**MTest 02**
		Data: 06/11/2012

Descrizione:
Questo test ha lo scopo di verificare il corretto funzionamento della struttura in uno scenario che prevede disservizi allo swicth di livello 1.

Situazione iniziale (scenario):
L'infrastruttura accede ad Internet ed i servizi esportati vengono acceduti regolarmente da Internet.
Il router del provider dei servizi internet è correttamente operativo e

configurato.
Il cablaggio tra lo switch1 e gli altri apparati è corretto e funzionante.
I firewall sono funzionanti e correttamente collegati.
I restanti apparati (AccessoPEC, switch del livello 2) sono configurati correttamente ed operativi.

Azioni/Simulazioni:

Verrà simulato un disservizio dello switch di livello 1 eseguendo (vedi immagine di riferimento):

1. nel primo caso: lo spegnimento dell'apparato;
2. nel secondo caso: lo scollegamento del cavo verso il Router master di frontiera.
3. nel terzo caso: lo scollegamento del cavo verso il Router slave di frontiera.
4. nel quarto caso: lo scollegamento del cavo verso il Firewall 1
    - considerando l'apparato come master;
    - considerando l'apparato come slave
5. nel quinto caso: lo scollegamento del cavo verso il Firewall 2
    - considerando l'apparato come master;
    - considerando l'apparato come slave.

Tipo di verifica:

- Accessibilità alla rete internet. Verificare se ogni Accesso PEC è in grado di:
    - risolvere un nome a dominio nel relativo indirizzo IP;
    - controllare il percorso per raggiungere un indirizzo IP.
- Accessibilità dei servizi dalla rete internet. Verificare se da un qualsiasi punto della rete internet è possibile:
    - risolvere il nome del servizio esportato nel suo indirizzo IP pubblico;
    - raggiungere l'IP pubblico del servizio.

Primo caso

- Verificare:
    - la raggiungibilità dei vari apparati/server dell'infrastruttura (AccessoPEC, Firewall e Router di frontiera);
    - la corretta funzionalità del servizio di bilanciamento/alta affidabilità (Keepalived) di AccessoPEC master.

Secondo e terzo caso

- Verificare:
    - la raggiungibilità dei vari apparati/server dell'infrastruttura

(AccessoPEC, Firewall e Router di frontiera);
    - la corretta funzionalità del servizio Keepalived di AccessoPEC master.

Quarto caso

Firewall 1 impostato come master.

- Verificare:
    - la raggiungibilità del Firewall master da ogni AccessoPEC;
    - lo status del Firewall slave (Firewall 2 in questo caso);
    - la raggiungibilità degli IP del Firewall 2;
    - il cambio di stato (da slave a master) del Firewall 2.
    - il cambio di stato (da master a slave) del Firewall 1.

Firewall 1 impostato come slave.

- Verificare:
    - la raggiungibilità del Firewall slave da ogni AccessoPEC;
    - l'invariabilità dello stato dei Firewall.

Quinto caso

Firewall 2 impostato come master.

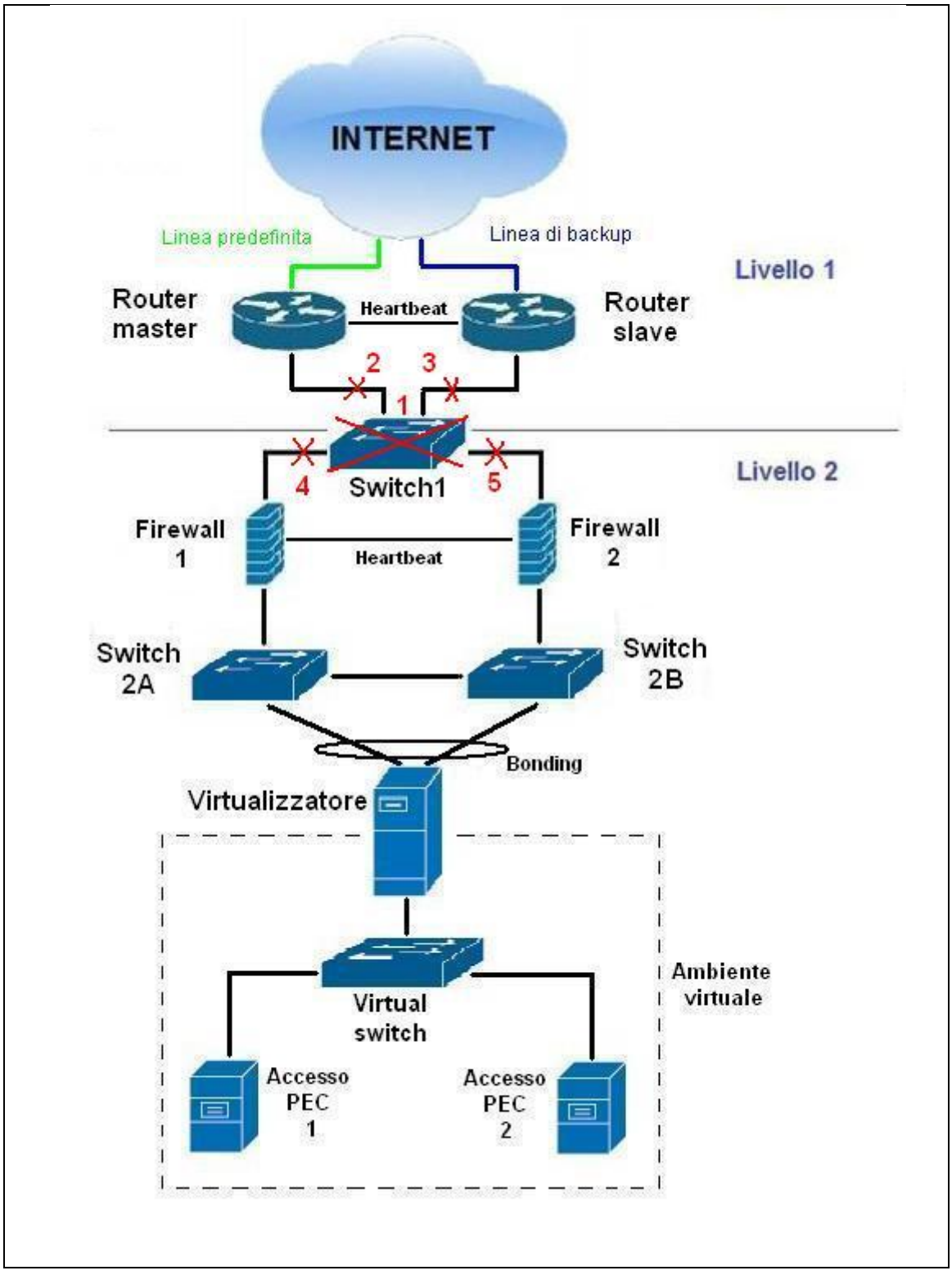
- Verificare:
    - la raggiungibilità del Firewall master da ogni AccessoPEC;
    - lo status del Firewall slave (Firewall 1 in questo caso);
    - la raggiungibilità degli IP del Firewall 1;
    - il cambio di stato (da slave a master) del Firewall 1.
    - il cambio di stato (da master a slave) del Firewall 2.

Firewall 2 impostato come slave.

- Verificare:
    - la raggiungibilità del Firewall master da ogni AccessoPEC;
    - l'invariabilità dello stato dei Firewall.

Esito:	**Data:**
Il fatto che nell'infrastruttura sia presente un solo switch di 1° livello comporta l'interruzione immediata dell'erogazione dei servizi a seguito di errore o malfunzionamento. Come detto nel capitolo 3, si preferisce un intervento manuale (sostituzione dell'apparecchiatura) qualora si dovesse verificare un guasto. La sequenza di verifiche che devono essere effettuate resta	15/nov/2012

comunque valida. In caso di rottura dell'apparato, i comandi adoperati per la verifica dei servizi dall'esterno andranno tutti in timeout mentre il traceroute risulterà comunque corretto nel suo output. Dall'interno sarà possibile isolare e identificare il guasto allo switch perché il traceroute non raggiungerà l'hop del router di frontiera.	
Immagine di riferimento:	


INTERNET
Linea predefinita
Linea di backup
Livello 1
Router master
Heartbeat
Router slave
2
3
1
4
Switch1
5
Livello 2
Firewall 1
Heartbeat
Firewall 2
Switch 2A
Switch 2B
Bonding
Virtualizzatore
Virtual switch
Ambiente virtuale
Accesso PEC 1
Accesso PEC 2

4.3 Verifiche con disservizio al Firewall Master

Laureando: Matteo Sartini	**Disservizio Firewall Master**	**MTest 03**
		Data: 07/11/2012

Descrizione:
Questo test ha lo scopo di verificare il corretto funzionamento della struttura in uno scenario che prevede disservizi al Firewall Master.

Situazione iniziale (scenario):
L'infrastruttura accede ad Internet ed i servizi esportati vengono acceduti regolarmente da Internet.
Il router del provider dei servizi internet è correttamente operativo e configurato.
Il cablaggio tra lo switch1 e gli altri apparati è corretto e funzionante.
I firewall sono funzionanti e correttamente collegati.
I restanti apparati (AccessoPEC, switch del livello 2) sono configurati correttamente ed operativi.

Azioni/Simulazioni:
Primo caso
Supponiamo che il master sia il Firewall 1.
Verrà simulato un disservizio del Firewall 1 eseguendo (vedi immagine n°1 di riferimento):

1. lo spegnimento dell'apparato;
2. scollegamento del cavo di rete dell'interfaccia verso lo Switch di livello 1;
3. scollegamento del cavo di rete dell'interfaccia verso lo Switch A di livello 2.

Secondo caso
Supponiamo che il master sia il Firewall 2.
Verrà simulato un disservizio del Firewall 2 eseguendo (vedi immagine n°2 di riferimento):

1. lo spegnimento dell'apparato;
2. scollegamento del cavo di rete dell'interfaccia verso lo switch di livello 1;
3. scollegamento del cavo di rete dell'interfaccia verso lo switch B di livello 2.

Tipo di verifica:

- Accessibilità alla rete internet. Verificare se ogni Accesso PEC è in grado di:

- risolvere un nome a dominio nel relativo indirizzo IP;
- controllare il percorso per raggiungere un indirizzo IP.

- Accessibilità dei servizi dalla rete internet. Verificare se da un qualsiasi punto della rete internet è possibile:
  - risolvere il nome del servizio esportato nel suo indirizzo IP pubblico;
  - raggiungere l'IP pubblico del servizio.

Primo caso

- Verificare:
  - la raggiungibilità del Firewall master (Firewall 1).
  - lo status del Firewall slave (Firewall 2 in questo caso);
  - la raggiungibilità del Firewall 2;
  - il cambio di stato (da slave a master) del Firewall 2.
  - il cambio di stato (da master a slave) del Firewall 1 (nel caso di spegnimento dell'apparato i log non vengono trattati e di conseguenza si verifica la sua raggiungibilità).

Secondo caso

- Verificare:
  - la raggiungibilità dell'apparato master (Firewall 2).
  - lo status del Firewall slave (Firewall 1 in questo caso);
  - la raggiungibilità del Firewall 1;
  - il cambio di stato (da slave a master) del Firewall 1.
  - il cambio di stato (da master a slave) del Firewall 2 (nel caso di spegnimento dell'apparato i log non vengono trattati e di conseguenza si verifica la sua raggiungibilità).

Esito:	**Data:**
In questo scenario è stato possibile testare soltanto lo spegnimento manuale dei due dispositivi. Questi ultimi, configurati in Stateful Failover (e tramite protocollo HSRP (Hot Standby Router Protocol)) consentono di continuare l'elaborazione e la trasmissione dei pacchetti di sessione firewall anche in seguito al verificarsi di una interruzione pianificata o non pianificata. Il Firewall di backup eseguirà automaticamente i task del Firewall master qualora in quest'ultimo si verifichi un guasto o una perdita di connettività. La migrazione avviene in modalità del tutto trasparente e non richiede	13/nov/2012

adattamento e riconfigurazione del dispositivo remoto. Ciò è possibile grazie alla ridondanza degli indirizzi IP su entrambi i dispositivi e al mantenimento dello stato delle connessioni. In questo modo la parte di rete privata vedrà sempre attivo il gateway di default, mentre dall'esterno i servizi risponderanno sempre allo stesso IP pubblico senza soluzione di continuità. Per quanto riguarda un disservizio all'apparato slave, viene inviata segnalazione di guasto dell'apparato in modo da operare una tempestiva sostituzione. In ogni caso, il Firewall che verrà eletto come primario (master) resterà tale fino al verificarsi di un disservizio. Non sono configurate priorità tali da avere sempre lo stesso dispositivo come primario.	

Immagine di riferimento n°1:

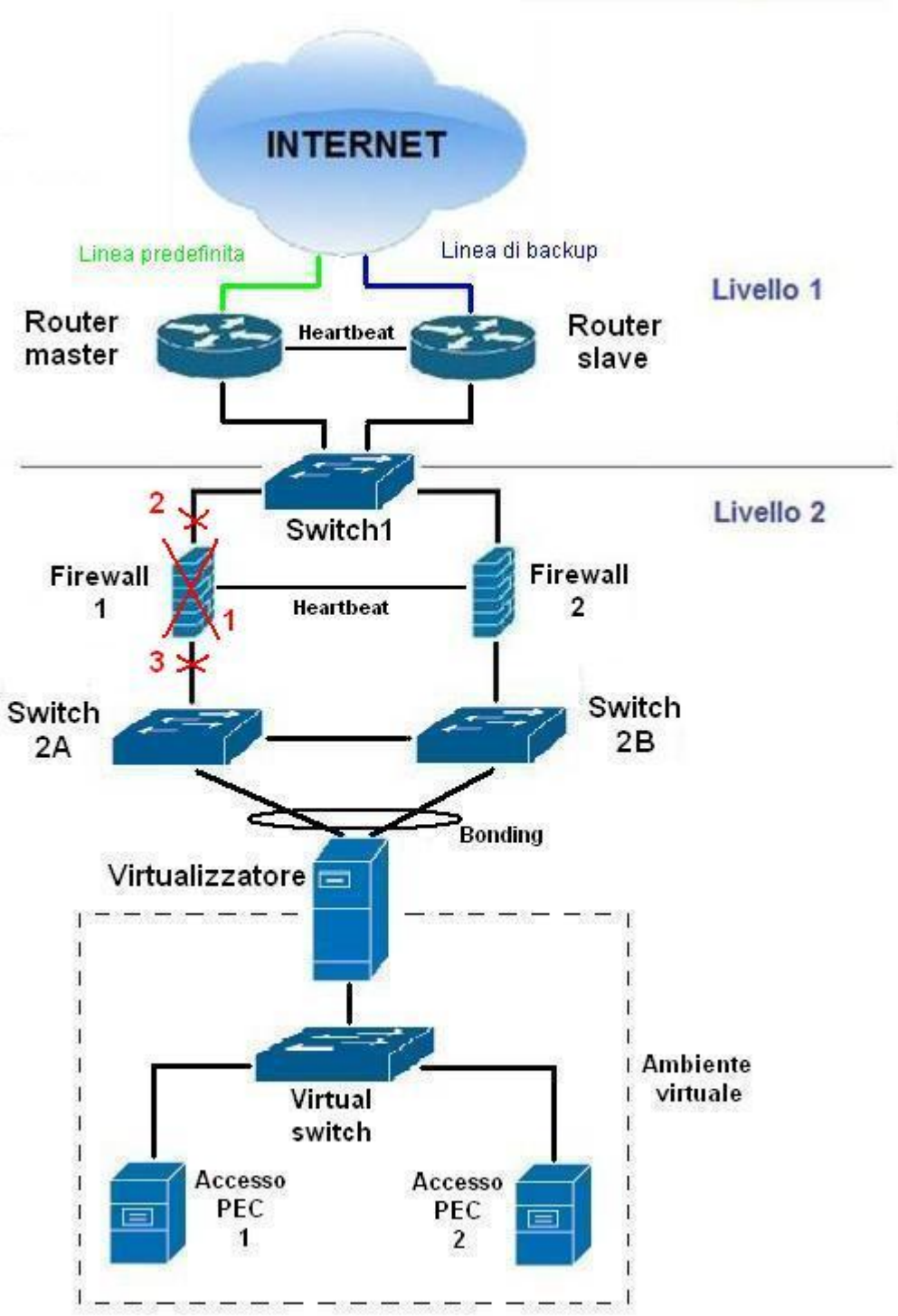
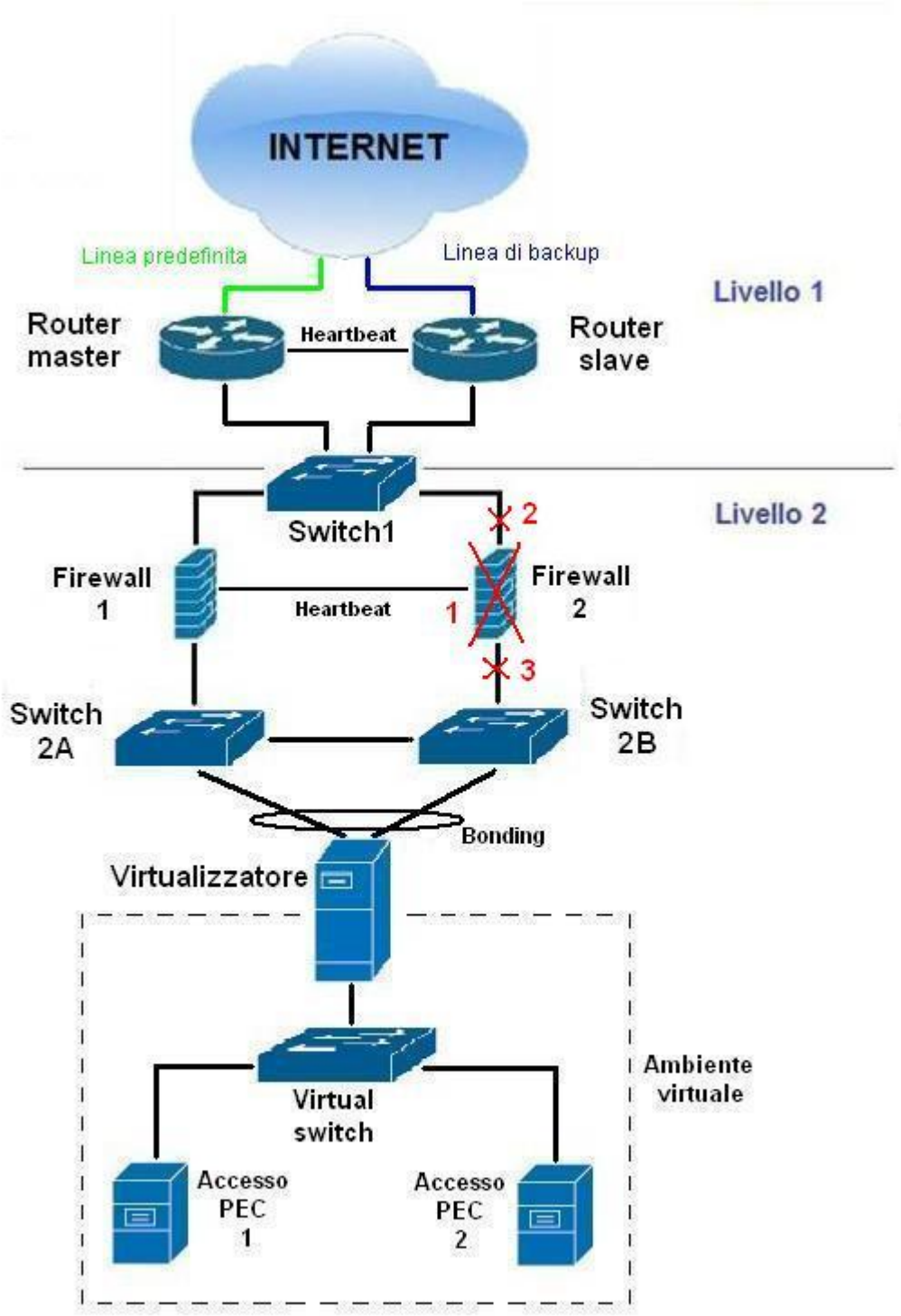


Immagine di riferimento n°2:



4.4 Verifiche con disservizio al Firewall Slave

Laureando: Matteo Sartini	**Disservizio Firewall Slave**	**MTest 04**
		Data: 07/11/2012

Descrizione:
Questo test ha lo scopo di verificare il corretto funzionamento della struttura in uno scenario che prevede disservizi al Firewall slave.

Situazione iniziale (scenario):
L'infrastruttura accede ad Internet ed i servizi esportati vengono acceduti regolarmente da Internet.
Il router del provider dei servizi internet è correttamente operativo e configurato.
Il cablaggio tra lo switch1 e gli altri apparati è corretto e funzionante.
I firewall sono funzionanti e correttamente collegati.
I restanti apparati (AccessoPEC, switch del livello 2) sono configurati correttamente ed operativi.

Azioni/Simulazioni:
<u>Primo caso</u>
Supponiamo che lo slave sia il Firewall 2.
Verrà simulato un disservizio del Firewall 2 eseguendo (vedi immagine di riferimento n°1):

1. lo spegnimento dell'apparato;
2. scollegamento del cavo di rete dall'interfaccia verso lo Switch di livello 1;
3. scollegamento del cavo di rete dall'interfaccia verso lo Switch B di livello 2.

<u>Secondo caso</u>
Supponiamo che lo slave sia il Firewall 1.
Verrà simulato un disservizio del Firewall 1 eseguendo (vedi immagine di riferimento n°2):

1. lo spegnimento dell'apparato;
2. scollegamento del cavo di rete dall'interfaccia verso lo Switch di livello 1;
3. scollegamento del cavo di rete dall'interfaccia verso lo Switch A di livello 2.

Tipo di verifica:

- Accessibilità alla rete internet. Verificare se ogni Accesso PEC è in grado di:
    - risolvere un nome a dominio nel relativo indirizzo IP;
    - controllare il percorso per raggiungere un indirizzo IP.
- Accessibilità dei servizi dalla rete internet. Verificare se da un qualsiasi punto della rete internet è possibile:
    - risolvere il nome del servizio esportato nel suo indirizzo IP pubblico;
    - raggiungere l'IP pubblico del servizio.

<u>Primo caso</u>

- Verificare la raggiungibilità del Firewall 2 da ogni AccessoPEC.
- Verificare che non ci siano cambi di stato del Firewall Master (Firewall 1).

<u>Secondo caso</u>

- Verificare la raggiungibilità del Firewall 1 da ogni AccessoPEC.
- Verificare che non ci siano cambi di stato del Firewall Master (Firewall 2).

Esito:	**Data:**
Vedi Disservizio Firewall master (scheda MTest03).	13/nov/2012

Immagine di riferimento n°1:

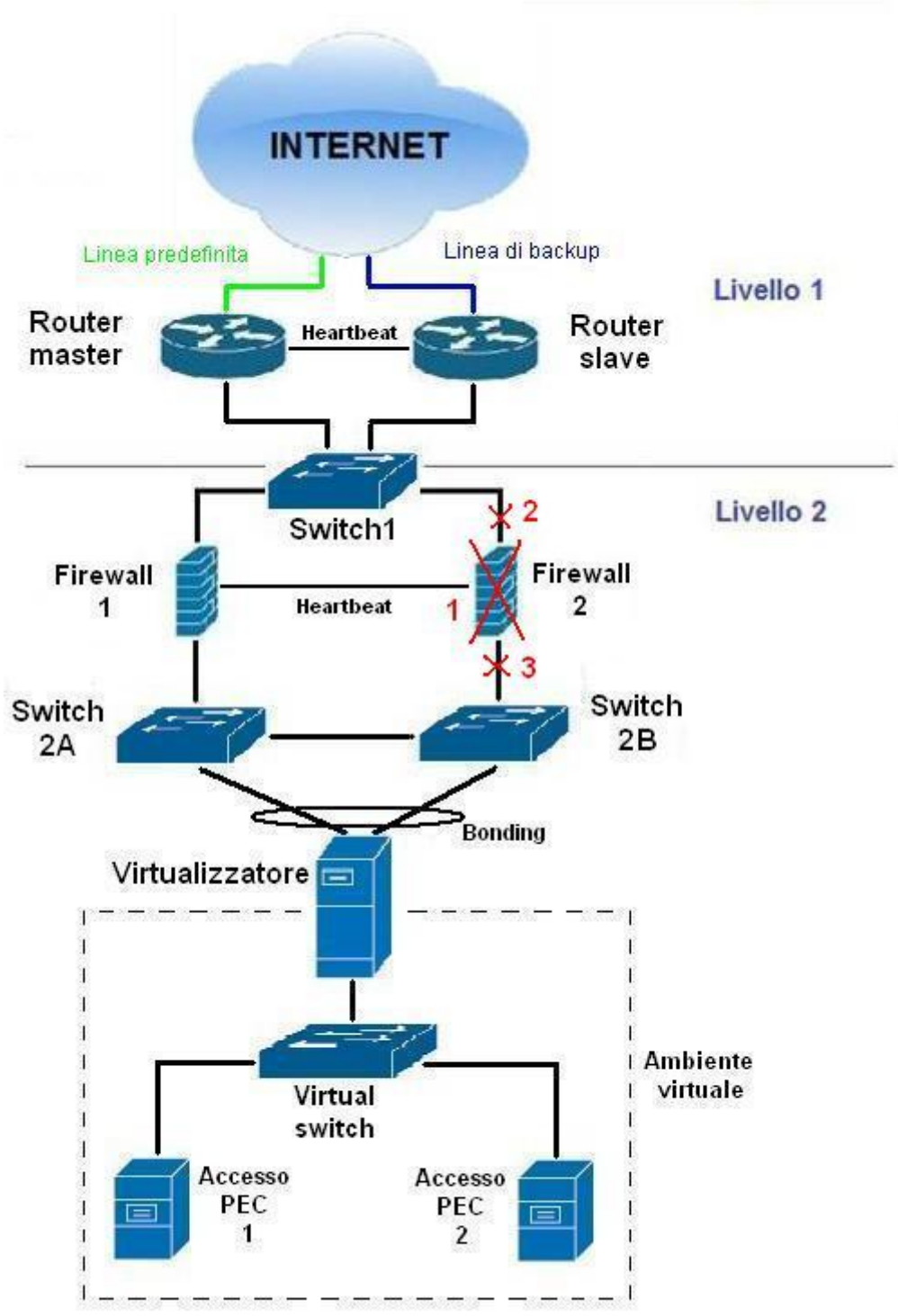
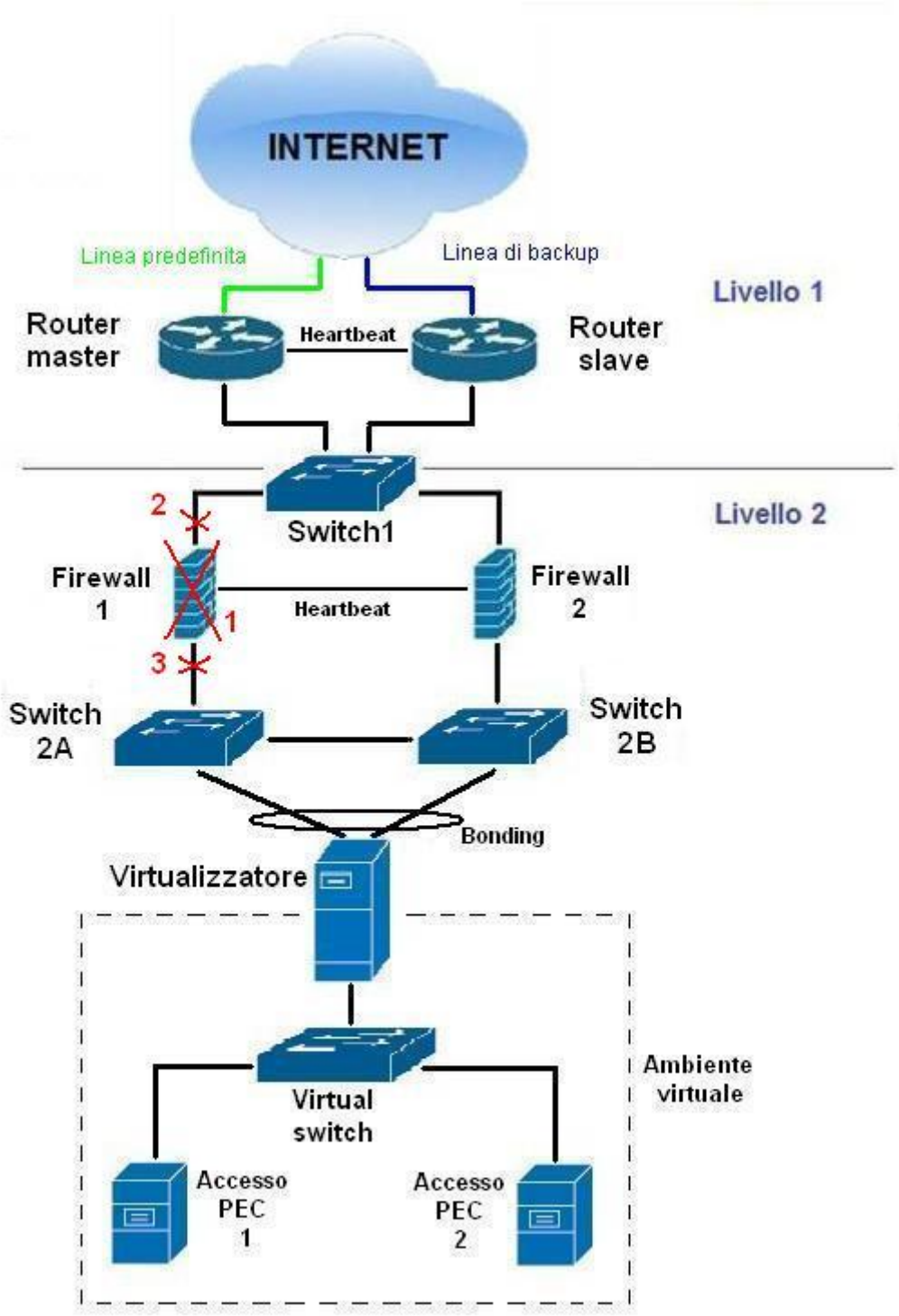


Immagine di riferimento n°2:



4.5 Verifiche con disservizio allo Switch A di livello 2

Laureando: Matteo Sartini	**Disservizio Switch A di livello 2**	**MTest 05**
		Data: 08/11/2012

Descrizione:
Questo test ha lo scopo di verificare il corretto funzionamento della struttura in uno scenario che prevede disservizi allo switch A di livello 2.

Situazione iniziale (scenario):
L'infrastruttura accede ad Internet ed i servizi esportati vengono acceduti regolarmente da Internet.
Il router del provider dei servizi internet è correttamente operativo e configurato.
Il cablaggio tra lo switch1 e gli altri apparati è corretto e funzionante.
I firewall sono funzionanti e correttamente collegati.
I restanti apparati (AccessoPEC, switch del livello 2) sono configurati correttamente ed operativi.

Azioni/Simulazioni:
Verrà simulato un disservizio dello switch A di livello 2 eseguendo (vedi immagine di riferimento) lo scollegamento del cavo di rete dall'interfaccia eth0 del virtualizzatore. In questo modo si riesce a simulare contemporaneamente due casi:

- un malfunzionamento dello switch A,
- un malfunzionamento al relativo collegamento verso il virtualizzatore,

in quanto lo scollegamento del cavo dall'interfaccia eth0 compromette il passaggio del traffico sul link tra il virtualizzatore e lo switch A di livello 2.

Tipo di verifica:

- Accessibilità alla rete internet. Verificare se ogni AccessoPEC è in grado di:
  - risolvere un nome a dominio nel relativo indirizzo IP;
  - controllare il percorso per raggiungere un indirizzo IP.

- Accessibilità dei servizi dalla rete internet. Verificare se da un qualsiasi punto della rete internet è possibile:
  - risolvere il nome del servizio esportato nel suo indirizzo IP pubblico;
  - raggiungere l'IP pubblico del servizio.

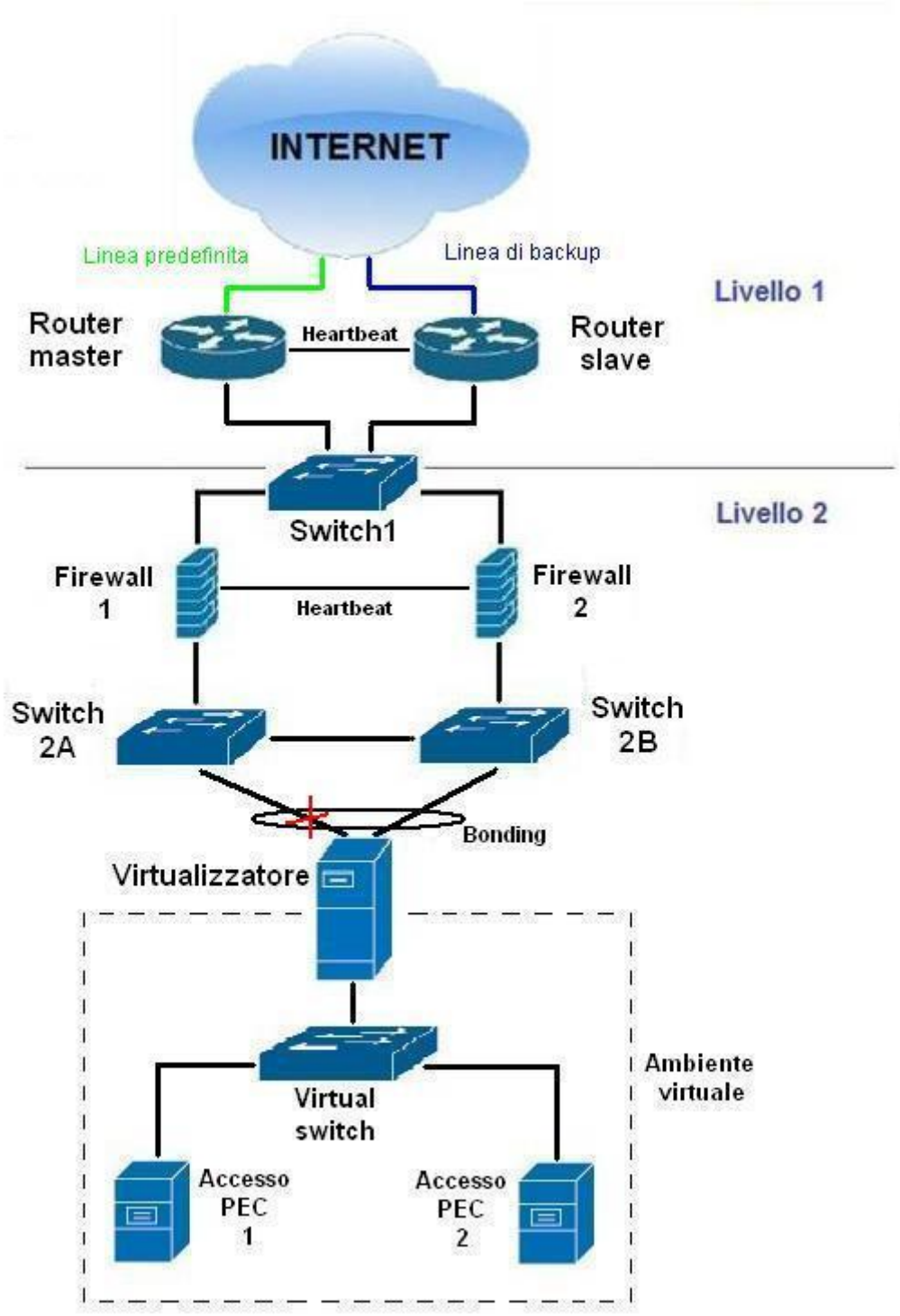
- Verificare la continua accessibilità ai servizi di PEC a seguito dello scollegamento dell'interfaccia eth0 del virtualizzatore.

Verranno consultati i log di sistema del virtualizzatore per verificarne lo stato delle interfacce di rete. Inoltre verrà utilizzato lo strumento OpenSSL per verificare la fruibilità dei servizi di PEC.

Esito:	**Data:**
In questo scenario è stato simulato un disservizio allo switch A di livello 2 e al relativo collegamento di rete verso il virtualizzatore. Come si nota dai risultati del test, il verificarsi di un malfunzionamento all'apparato o al link non compromette la fruibilità dei servizi di PEC. Lo scenario in cui si verifica un malfunzionamento ai link tra lo switch A e Firewall e tra switch A e switch B, non è stato testato in quanto: - un guasto al collegamento fra lo switch e il Firewall master (supponiamo il Firewall1) verrebbe rilevato da quest'ultimo. Di conseguenza il Firewall slave entrerebbe in stato master, gestendo lui stesso tutte le connessioni. Con il passaggio di stato dei firewall, il flusso dati proveniente dallo switch A attraverserebbe il link diretto verso lo switch B per poi essere inoltrato al nuovo Firewall master; - nel caso in cui il collegamento diretto fra lo switch A e lo switch B si danneggi, il flusso dati viene inoltrato correttamente verso il Firewall master.	14/nov/2012

Data la configurazione dei firewall, non è stato possibile recuperare log di sistema tali da dimostrare l'effettivo passaggio di stato dei dispositivi.	

Immagine di riferimento:



Laureando: Matteo Sartini	**Lista sotto-test Disservizio Switch A di livello 2**	**MTest 05**
		Data: 08/11/2012

CODICE	**SOTTO-TEST**
01	Accessibilità dei servizi da Internet.
02	Verifica stato interfaccia bonding del virtualizzatore.

Laureando: Matteo Sartini	**Scheda sotto-test**	**MTest 05**
Data Test	**Codice Test**	**Esecutore test**
14/nov/2012	01-02	Matteo Sartini

Descrizione

Simulazione del disservizio dello switch A di livello 2 eseguito mediante lo scollegamento del cavo di rete dall'interfaccia eth0 del virtualizzatore

Comandi eseguiti:

- less /var/log/messages|grep eth
- date && openssl s_client -connect test-smtps.sicurezzapostale.it:465

Valutazioni/Rilievi

Partendo dalla situazione iniziale (cfr MTest01 – schede sotto-test dalla 01 fino alla 06) e sulla base della descrizione dell'evento di disservizio, deve essere verificato che a seguito dello scollegamento del cavo di rete sull'interfaccia eth0 del virtualizzatore, i servizi siano correttamente fruibili. Questo dimostrerebbe l'efficacia del bonding, in quanto un disservizio dell'interfaccia eth0 non compromette il flusso delle connessioni.

Esito Test

Positivo

Risultati:

Il disservizio mediante lo spegnimento dello switch o dello scollegamento del cavo di rete dalla sua interfaccia verso il

virtualizzatore, viene simulato scollegando il cavo di rete dall'interfaccia eth0. Questo permette di simulare sia l'inaccessibilità verso lo switch A di livello 2 (ovvero scollegamento dei cavi di rete),sia lo spegnimento o rottura dello switch.

- Il cavo di rete viene scollegato dall'interfaccia eth0 del virtualizzatore

```
[root@virt ~]# less /var/log/messages|grep eth
Nov  14 17:44:57 virt kernel: bnx2 0000:03:00.0: eth0: NIC Copper Link is Down
Nov  14 17:44:57 virt kernel: bonding: bond0: link status definitely down for interface eth0, disabling it
```

A seguito dello scollegamento del cavo di rete, si può notare che i servizi sono correttamente fruibili.

- Verifica connettività (uno tra i servizi PEC esportati)

```
[root@alfacentos ~]# date && openssl s_client -connect test-smtps.sicurezzapostale.it:465
wed 14 nov 2012, 17.48.36, CET
CONNECTED(00000003)
[omiss]
220 frontout-test1.sicurezzapostale.it ESMTP Postfix
```

Il cavo di rete viene nuovamente collegato all'interfaccia eth0 del virtualizzatore

- Riattivazione interfaccia eth0

```
[root@virt ~]# less /var/log/messages|grep eth
Nov  14 17:52:00 virt kernel: bnx2 0000:03:00.0: eth0: NIC Copper Link is Up, 1000 Mbps full duplex
Nov  14 17:52:00 virt kernel: bond0: link status definitely up for interface eth0, 1000 Mbps full duplex.
```

4.6 Verifiche con disservizio allo Switch B di livello 2

Laureando: Matteo Sartini	**Disservizio Switch B di livello 2**	**MTest 06**
		Data: 08/11/2012

Descrizione:
Questo test ha lo scopo di verificare il corretto funzionamento della struttura in uno scenario che prevede disservizi allo switch B di livello 2.

Situazione iniziale (scenario):
L'infrastruttura accede ad Internet ed i servizi esportati vengono acceduti regolarmente da Internet.
Il router del provider dei servizi internet è correttamente operativo e configurato.
Il cablaggio tra lo switch1 e gli altri apparati è corretto e funzionante.
I firewall sono funzionanti e correttamente collegati.
I restanti apparati (AccessoPEC, switch del livello 2) sono configurati correttamente ed operativi.

Azioni/Simulazioni:
Verrà simulato un disservizio dello switch B di livello 2 eseguendo: (vedi immagine di riferimento) lo scollegamento del cavo di rete dall'interfaccia eth1 del virtualizzatore. In questo modo si riesce a simulare contemporaneamente due casi:

- un malfunzionamento allo switch B,
- un malfunzionamento al relativo collegamento verso il virtualizzatore,

in quanto lo scollegamento del cavo dall'interfaccia eth1 comporta l'inaccessibilità delle connessioni verso lo switch B di livello 2.

Tipo di verifica:

- Accessibilità alla rete internet. Verificare se ogni Accesso PEC è in grado di:
  - risolvere un nome a dominio nel relativo indirizzo IP;
  - controllare il percorso per raggiungere un indirizzo IP.
- Accessibilità dei servizi dalla rete internet. Verificare se da un qualsiasi punto della rete internet è possibile:
  - risolvere il nome del servizio esportato nel suo indirizzo IP

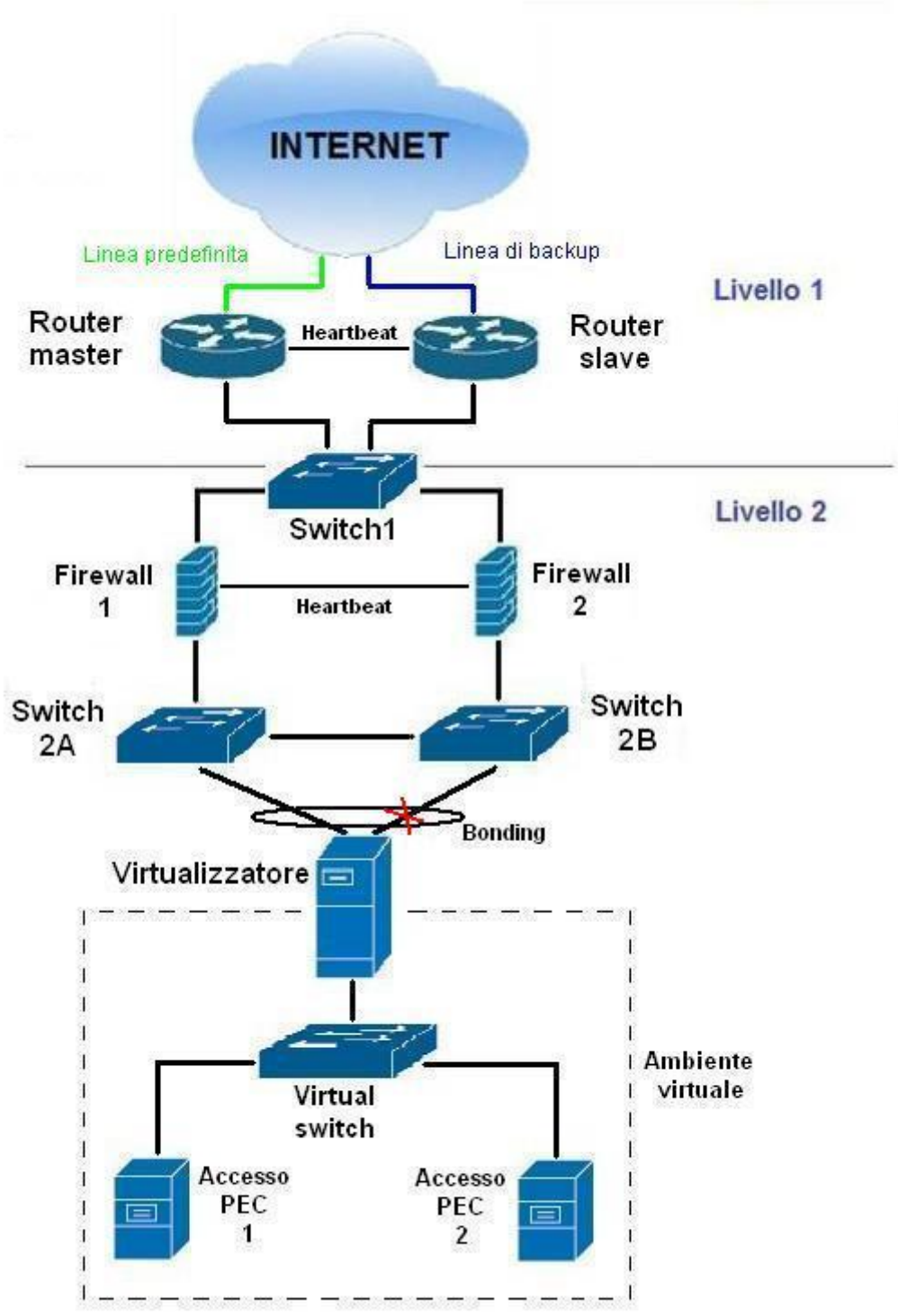
pubblico;
    - raggiungere l'IP pubblico del servizio.

- Verificare la continua accessibilità ai servizi di PEC a seguito dello scollegamento dell'interfaccia eth1 del virtualizzatore.

Verranno consultati i log di sistema del virtualizzatore per verificarne lo stato delle interfacce di rete. Inoltre verrà utilizzato lo strumento OpenSSL per verificare la fruibilità dei servizi di PEC.

Esito:	**Data:**
In questo scenario è stato simulato un disservizio allo switch B di livello 2 e al relativo collegamento di rete verso il virtualizzatore. Come si nota dai risultati del test, il verificarsi di un malfunzionamento all'apparato o al link non compromette la fruibilità dei servizi di PEC. Lo scenario in cui si verifica un malfunzionamento ai link tra lo switch B e Firewall e tra switch B e switch A, non è stato testato in quanto: - un guasto al collegamento fra lo switch e il Firewall master (supponiamo il Firewall2) verrebbe rilevato da quest'ultimo. Di conseguenza il Firewall slave entrerebbe in stato master, gestendo lui stesso tutte le connessioni. Con il passaggio di stato dei firewall, il flusso dati proveniente dallo switch B attraverserebbe il link diretto verso lo switch A per poi essere inoltrato al nuovo Firewall master; - nel caso in cui il collegamento diretto fra lo switch B e lo switch A si danneggi, il flusso dati viene inoltrato correttamente verso il Firewall master. Data la configurazione dei firewall, non è stato possibile recuperare log di sistema tali da dimostrare l'effettivo passaggio di stato dei dispositivi.	14/nov/2012

Immagine di riferimento:



Laureando: Matteo Sartini	**Lista sotto-test Disservizio Switch B di livello 2**	**MTest 06**
		Data: 8/11/2012

CODICE	**SOTTO-TEST**
01	Accessibilità dei servizi da Internet.
02	Verifica stato interfaccia bonding del virtualizzatore.

Laureando: Matteo Sartini	**Scheda sotto-test**	**MTest 05**
Data Test	**Codice Test**	**Esecutore test**
14/nov/2012	01-02	Matteo Sartini

Descrizione

Simulazione del disservizio dello switch B di livello 2 eseguito mediante lo scollegamento del cavo di rete dall'interfaccia eth0 del virtualizzatore

Comandi eseguiti:

- less /var/log/messages|grep eth
- date && openssl s_client -connect test-smtps.sicurezzapostale.it:465

Valutazioni/Rilievi

Partendo dalla situazione iniziale (cfr MTest01 – schede sotto-test dalla 01 fino alla 06) e sulla base della descrizione dell'evento di disservizio, deve essere verificato che a seguito dello scollegamento del cavo di rete sull'interfaccia eth1, i servizi siano correttamente fruibili. Questo dimostrerebbe l'efficacia del bonding, in quanto un disservizio dell'interfaccia eth1 non compromette il flusso delle connessioni.

Esito Test

Positivo

Risultati:

Il disservizio mediante lo spegnimento dello switch e dello scollegamento del cavo di rete dalla sua interfaccia verso il virtualizzatore, viene simulato scollegando il cavo di rete

dall'interfaccia eth1 del medesimo, la quale è soggetta al bonding. Questo permette di simulare l'inaccessibilità verso lo switch B di livello 2, la quale sarebbe la stessa conseguenza se si verificasse uno spegnimento dello switch o uno scollegamento del cavo di rete.

- Il cavo di rete viene scollegato dall'interfaccia eth1 del virtualizzatore

```
[root@virt ~]# less /var/log/messages|grep eth
Nov  14 17:59:37 virt kernel: bnx2 0000:03:00.0: eth1: NIC Copper Link
is Down
Nov  14 17:59:37 virt kernel: bonding: bond0: link status definitely
down for interface eth1, disabling it
```

A seguito dello scollegamento del cavo di rete, si può notare che i servizi sono correttamente fruibili.

- Verifica connettività (uno tra i servizi PEC esportati)

```
[root@alfacentos ~]# date && openssl s_client -connect test-
smtps.sicurezzapostale.it:465
wed 14 nov 2012, 18.02.15, CET
CONNECTED(00000003)
[omiss]
220 frontout-test1.sicurezzapostale.it ESMTP Postfix
```

Il cavo di rete viene nuovamente collegato all'interfaccia eth1 del virtualizzatore

- Riattivazione interfaccia eth1

```
[root@virt ~]# less /var/log/messages|grep eth
Nov  14 18:06:30 virt kernel: bnx2 0000:03:00.0: eth1: NIC Copper Link
is Up, 1000 Mbps full duplex
Nov  14 18:06:30 virt kernel: bond0: link status definitely up for
interface eth1, 1000 Mbps full duplex.
```

4.7 Verifiche con disservizio al server AccessoPEC Master

Laureando: Matteo Sartini	**Disservizio AccessoPEC Master**	**MTest 07**
		Data: 08/11/2012

Descrizione:
Questo test ha lo scopo di verificare il corretto funzionamento della struttura in uno scenario che prevede disservizi al server AccessoPEC Master.

Situazione iniziale (scenario):
L'infrastruttura accede ad Internet ed i servizi esportati vengono acceduti regolarmente da Internet.
Il router del provider dei servizi internet è correttamente operativo e configurato.
Il cablaggio tra lo switch1 e gli altri apparati è corretto e funzionante.
I firewall sono funzionanti e correttamente collegati.
I restanti apparati (AccessoPEC, switch del livello 2) sono configurati correttamente ed operativi.

Azioni/Simulazioni:
Supponiamo che il master sia il server AccessoPEC1.

- Primo caso
  Verrà effettuato un cambio di stato manuale eseguendo lo spegnimento del servizio di bilanciamento/alta affidabilità (Keepalived) su AccessoPEC1.
  Verrà ripristinata la situazione iniziale con AccessoPEC1 master e AccessoPEC2 slave.

- Secondo caso
  Verrà simulato un disservizio di AccessoPEC master (AccessoPEC1) eseguendo (vedi immagine di riferimento n°1):
  1. lo spegnimento del server;
  2. lo spegnimento dell'interfaccia di rete (valido anche per simulare lo scollegamento);

Supponiamo che il master sia il server AccessoPEC2.

- Terzo caso
  Verrà effettuato un cambio di stato manuale eseguendo lo spegnimento del servizio Keepalived su AccessoPEC2.
  Verrà ripristinata la situazione iniziale con AccessoPEC2 master e AccessoPEC1 slave.

- Quarto caso
  Verrà simulato un disservizio di AccessoPEC master (AccessoPEC2) eseguendo (vedi immagine di riferimento n°2):
  1. lo spegnimento del server;
  2. lo spegnimento dell'interfaccia di rete (valido anche per simulare lo scollegamento);

Tipo di verifica:

- Accessibilità alla rete internet. Verificare se ogni AccessoPEC è in grado di:
  - risolvere un nome a dominio nel relativo indirizzo IP;
  - controllare il percorso per raggiungere un indirizzo IP.
- Accessibilità dei servizi dalla rete internet. Verificare se da un qualsiasi punto della rete internet è possibile:
  - risolvere il nome del servizio esportato nel suo indirizzo IP pubblico;
  - raggiungere l'IP pubblico del servizio.

Primo caso:
- Verificare la raggiungibilità di AccessoPEC1. Controllare che i servizi siano esportati dal nuovo master (AccessoPEC2).
- Verificare manualmente il cambio di stato da master a slave di AccessoPEC2. Controllare che i servizi siano esportati nuovamente dal master AccessoPEC1.

Secondo caso:
1. Verificare la raggiungibilità di AccessoPEC1.
   Verificare il cambio automatico da slave a master di AccessoPEC2.
2. Verificare la raggiungibilità di AccessoPEC1.
   Verificare il cambio automatico da master a slave di AccessoPEC1.
   Verificare il cambio automatico da slave a master di AccessoPEC2.

Terzo caso:
- Verificare la raggiungibilità di AccessoPEC2. Controllare che i servizi siano esportati dal nuovo master (AccessoPEC1).
- Verificare manualmente il cambio di stato da master a slave di AccessoPEC1. Controllare che i servizi siano esportati nuovamente dal master AccessoPEC2.

Quarto caso:

3. Verificare la raggiungibilità di AccessoPEC2.
   Verificare il cambio automatico da slave a master di AccessoPEC1.
4. Verificare la raggiungibilità di AccessoPEC2.
   Verificare il cambio automatico da master a slave di AccessoPEC2.
   Verificare il cambio automatico da slave a master di AccessoPEC1.

Verranno consultati i log di sistema dei server AccessoPEC per verificarne la configurazione (master o slave). Inoltre verranno utilizzati gli strumenti Ping e OpenSSL per verificare la raggiungibilità di indirizzi IP e servizi.

Esito:	**Data:**
In questo scenario si è voluto verificare l'accessibilità ai servizi di PEC simulando disservizi al bilanciatore master (sia AccessoPEC1 che AccessoPEC2). Come si può notare dai risultati dei test, in caso di malfunzionamento del bilanciatore master, o della sua interfaccia di rete, gli IP virtuali dei servizi vengono prontamente migrati verso il bilanciatore slave. Quest'ultimo assumerà il ruolo di master, garantendo l'accessibilità ai servizi di PEC. Ripristinando il bilanciatore che ha subìto il Fault (ovvero riattivando l'interfaccia e/o il servizio Keepalived), esso ritorna in stato master e riprende a gestire i virtual IP dei servizi di PEC. Di conseguenza, l'altro bilanciatore riassume il suo stato slave.	16/nov/2012

Immagine di riferimento n°1:

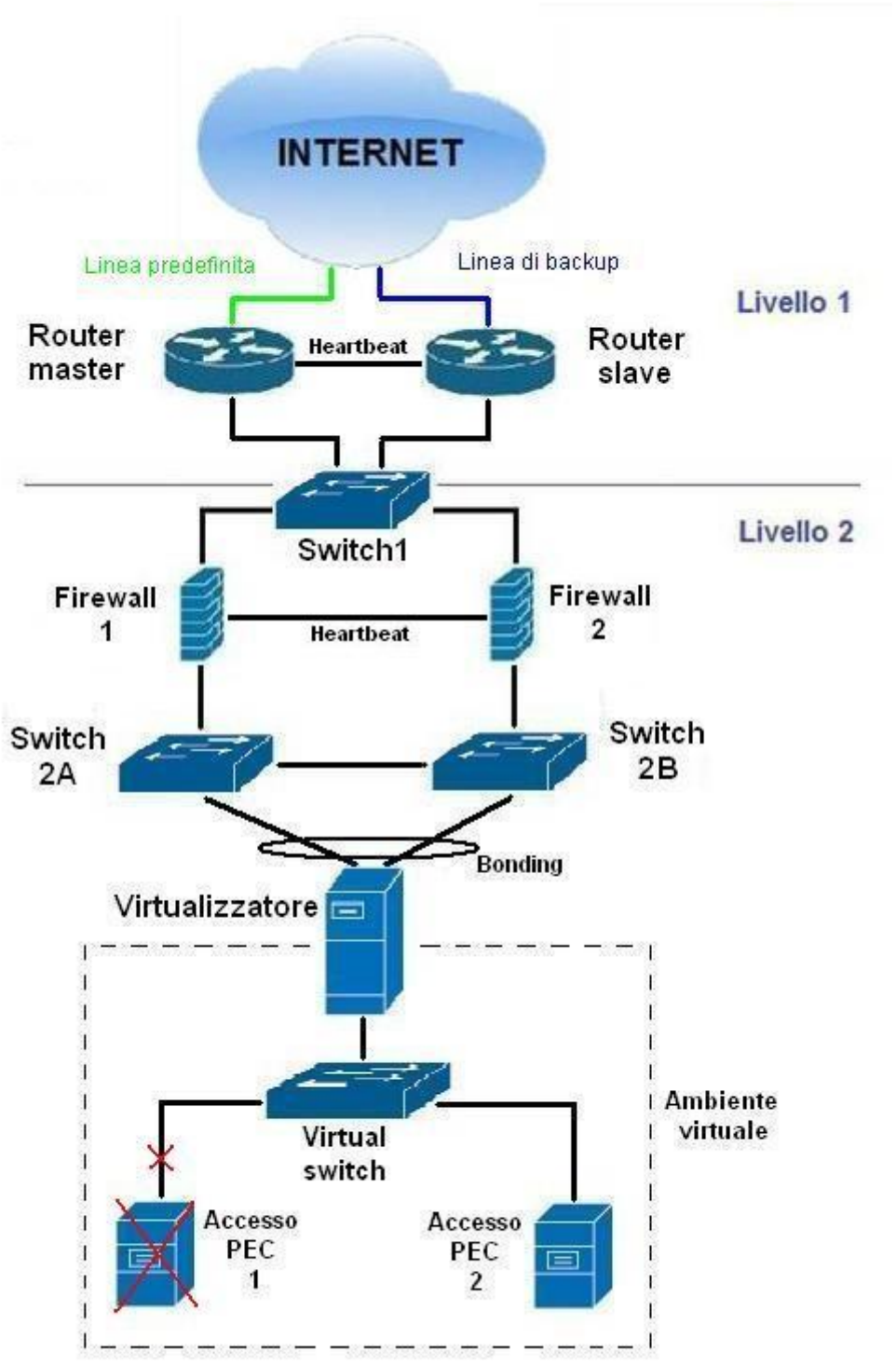
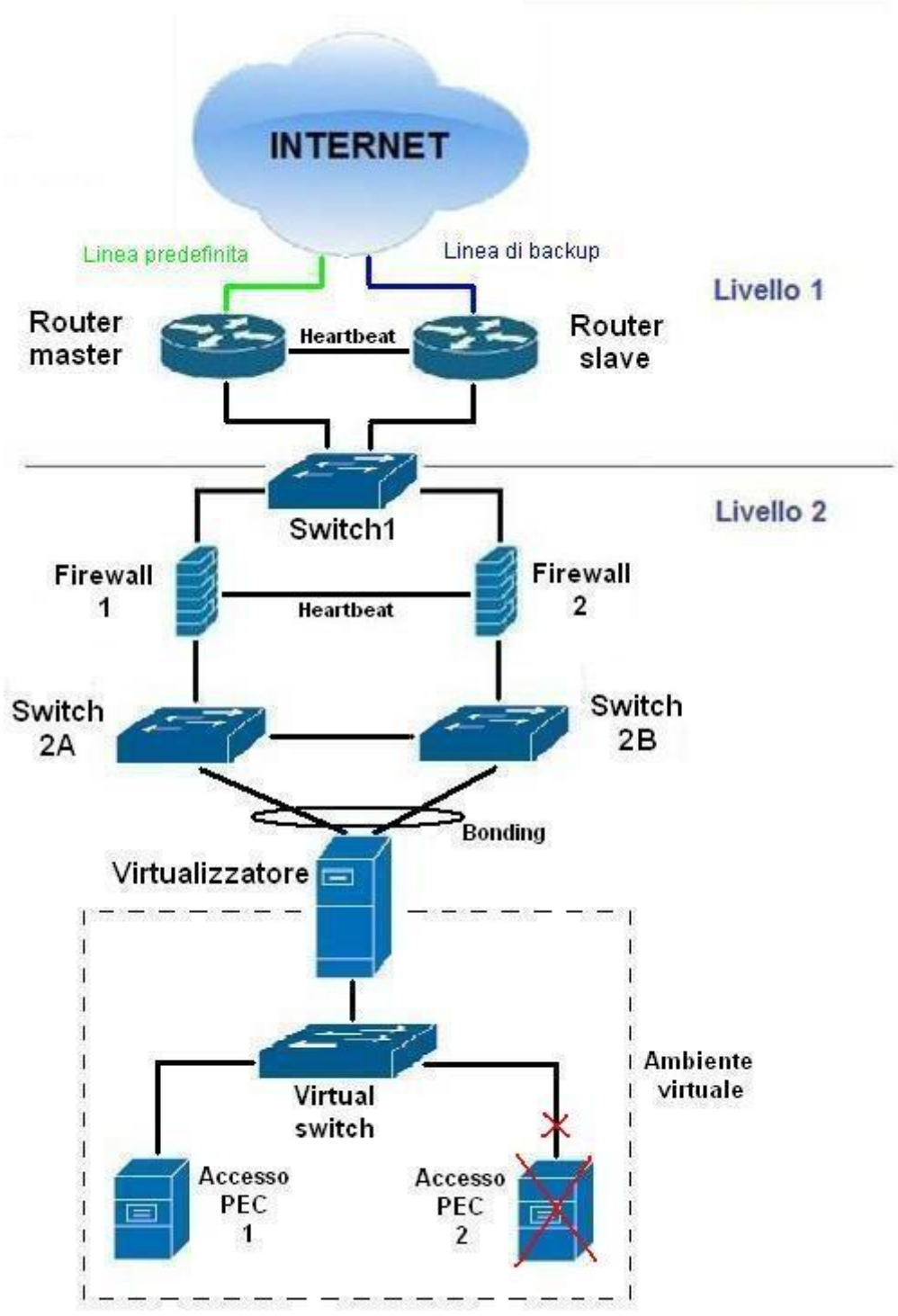


Immagine di riferimento n°2:



Laureando: Matteo Sartini	**Lista sotto-test Disservizio AccessoPEC Master**	**MTest 07**
		Data: 08/11/2012

CODICE	**SOTTO-TEST**
01	Accessibilità dei servizi da Internet.
02	Verifica raggiungibilità di AccessoPEC1.
03	Verifica raggiungibilità di AccessoPEC2.
04	Verifica esportazione dei servizi su AccessoPEC1.
05	Verifica esportazione dei servizi su AccessoPEC2.
06	Verifica stato master/slave di AccessoPEC1.
07	Verifica stato master/slave di AccessoPEC2.

Laureando: Matteo Sartini	**Scheda sotto-test**	**MTest 07**
Data Test	**Codice Test**	**Esecutore test**
16/nov/2012	1-2-3-4-5-6-7	Matteo Sartini

Descrizione

PRIMO CASO
Verifica del cambio di stato manuale eseguito mediante spegnimento del servizio di bilanciamento e alta disponibilità (Keepalived) su AccessoPEC1.
Verifica del ripristino della situazione iniziale con AccessoPEC1 master e AccessoPEC2 slave.

Comandi eseguiti:

- ping -c 5 192.168.255.3
- ping -c 5 192.168.255.4
- ip addr show
- date && /etc/init.d/keepalived start
- date && /etc/init.d/keepalived stop
- less /var/log/messages|grep "VRRP_Instance"
- date && openssl s_client -connect test-smtps.sicurezzapostale.it:465

Valutazioni/Rilievi

Partendo dalla situazione iniziale (cfr MTest01 – schede sotto-test dalla 01 fino alla 06) e sulla base della descrizione dell'evento di disservizio, deve essere verificato il passaggio di stato del server slave a master nel momento in cui il server (o il servizio) viene spento. Ciò significa che gli IP virtuali esportati dal server master devono migrare in automatico al server slave a garanzia di una corretta configurazione dell'accesso ai servizi PEC.
Può essere verificato soltanto il passaggio di stato sullo slave perché i log non vengono trattati se il server (o il servizio) è spento.
AccessoPEC2, in questo caso, deve diventare master e i servizi PEC esportati subiscono una interruzione quantificabile nell'intorno del minuto secondo rientrando ampiamente nei limiti normativi imposti.

Esito Test

Positivo

Risultati:

Verifica raggiungibilità degli AccessoPEC (no disservizio)

- AccessoPEC1 è raggiungibile

```
[root@accessopec-test2 ~]# ping -c 5 192.168.255.3
PING 192.168.255.3 (192.168.255.3) 56(84) bytes of data.
64 bytes from 192.168.255.3: icmp_seq=1 ttl=64 time=0.518 ms
64 bytes from 192.168.255.3: icmp_seq=2 ttl=64 time=0.529 ms
64 bytes from 192.168.255.3: icmp_seq=3 ttl=64 time=0.478 ms
64 bytes from 192.168.255.3: icmp_seq=4 ttl=64 time=0.401 ms
64 bytes from 192.168.255.3: icmp_seq=5 ttl=64 time=0.447 ms

--- 192.168.255.3 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4000ms
rtt min/avg/max/mdev = 0.401/0.474/0.529/0.052 ms
```

- AccessoPEC2 è raggiungibile

```
[root@accessopec-test1 ~]# ping -c 5 192.168.255.4
PING 192.168.255.4 (192.168.255.4) 56(84) bytes of data.
64 bytes from 192.168.255.4: icmp_seq=1 ttl=64 time=0.672 ms
64 bytes from 192.168.255.4: icmp_seq=2 ttl=64 time=0.566 ms
64 bytes from 192.168.255.4: icmp_seq=3 ttl=64 time=0.537 ms
64 bytes from 192.168.255.4: icmp_seq=4 ttl=64 time=0.627 ms
64 bytes from 192.168.255.4: icmp_seq=5 ttl=64 time=0.576 ms

--- 192.168.255.4 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4000ms
rtt min/avg/max/mdev = 0.537/0.595/0.672/0.054 ms
```

Verifica esportazione servizi PEC dal Master: (AccessoPEC1)

- I virtual IP evidenziati sono privati e corrispondono, mediante NAT, all'unico IP virtuale pubblico con il quale vengono esportati, come già detto nel capitolo 3.

```
[root@accessopec-test1 ~]# ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast
state UP qlen 1000
    link/ether 02:00:00:00:00:03 brd ff:ff:ff:ff:ff:ff
    inet 192.168.255.3/24 brd 192.168.255.255 scope global eth0
    inet 192.168.255.11/32 scope global eth0
    inet 192.168.255.12/32 scope global eth0
    inet 192.168.255.13/32 scope global eth0
    inet 192.168.255.14/32 scope global eth0
    inet 192.168.255.15/32 scope global eth0
    inet 192.168.255.16/32 scope global eth0
    inet6 fe80::ff:fe00:3/64 scope link
       valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast
state UP qlen 1000
    link/ether 02:00:00:01:00:03 brd ff:ff:ff:ff:ff:ff
    inet 192.168.2.3/24 brd 192.168.2.255 scope global eth1
    inet 192.168.2.192/32 scope global eth1
    inet6 fe80::ff:fe01:3/64 scope link
       valid_lft forever preferred_lft forever
```

Verifica esportazione servizi PEC dallo Slave: (AccessoPEC2)

```
[root@accessopec-test2 ~]# ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast
state UP qlen 1000
    link/ether 02:00:00:00:00:04 brd ff:ff:ff:ff:ff:ff
    inet 192.168.255.4/24 brd 192.168.255.255 scope global eth0
    inet6 fe80::ff:fe00:4/64 scope link
       valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast
state UP qlen 1000
    link/ether 02:00:00:01:00:04 brd ff:ff:ff:ff:ff:ff
    inet 192.168.2.4/24 brd 192.168.2.255 scope global eth1
    inet6 fe80::ff:fe01:4/64 scope link
       valid_lft forever preferred_lft forever
```

Spegnimento del server/servizio Keepalived su AccessoPEC1 (supponiamo ad esempio sia necessario un riavvio o un aggiornamento hardware):

- Spegnimento del servizio Keepalived e controllo dei log sugli AccessoPEC

```
[root@accessopec-test1 ~]# date && /etc/init.d/keepalived stop
Fri Nov 16 16:11:35 CET 2012
Stopping keepalived:                                       [  OK  ]

[root@accessopec-test1 ~] less /var/log/messages|grep "VRRP_Instance"
Nov 16 16:11:35 accessopec-test1 Keepalived_vrrp[4090]:
VRRP_Instance(VI_1) sending 0 priority
Nov 16 16:11:35 accessopec-test1 Keepalived_vrrp[4090]:
VRRP_Instance(VI_GATEWAY) sending 0 priority


[root@accessopec-test2 ~]# less /var/log/messages|grep "VRRP_Instance"
Nov 16 16:11:36 accessopec-test2 Keepalived_vrrp[28286]:
VRRP_Instance(VI_GATEWAY) Transition to MASTER STATE
Nov 16 16:11:36 accessopec-test2 Keepalived_vrrp[28286]:
VRRP_Instance(VI_1) Transition to MASTER STATE
Nov 16 16:11:36 accessopec-test2 Keepalived_vrrp[28286]:
VRRP_Instance(VI_GATEWAY) Entering MASTER STATE
Nov 16 16:11:36 accessopec-test2 Keepalived_vrrp[28286]:
VRRP_Instance(VI_1) Entering MASTER STATE
```

Verifica esportazione servizi PEC su AccessoPEC1

```
[root@accessopec-test1 ~]# ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast
state UP qlen 1000
    link/ether 02:00:00:00:00:03 brd ff:ff:ff:ff:ff:ff
    inet 192.168.255.3/24 brd 192.168.255.255 scope global eth0
    inet6 fe80::ff:fe00:3/64 scope link
       valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast
state UP qlen 1000
    link/ether 02:00:00:01:00:03 brd ff:ff:ff:ff:ff:ff
    inet 192.168.2.3/24 brd 192.168.2.255 scope global eth1
    inet6 fe80::ff:fe01:3/64 scope link
       valid_lft forever preferred_lft forever
```

Verifica esportazione servizi PEC su AccessoPEC2 (nuovo master)

```
[root@accessopec-test2 ~]# ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast
state UP qlen 1000
    link/ether 02:00:00:00:00:04 brd ff:ff:ff:ff:ff:ff
    inet 192.168.255.4/24 brd 192.168.255.255 scope global eth0
    inet 192.168.255.11/32 scope global eth0
    inet 192.168.255.12/32 scope global eth0
    inet 192.168.255.13/32 scope global eth0
    inet 192.168.255.14/32 scope global eth0
    inet 192.168.255.15/32 scope global eth0
    inet 192.168.255.16/32 scope global eth0
    inet6 fe80::ff:fe00:4/64 scope link
       valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast
state UP qlen 1000
    link/ether 02:00:00:01:00:04 brd ff:ff:ff:ff:ff:ff
    inet 192.168.2.4/24 brd 192.168.2.255 scope global eth1
    inet 192.168.2.192/32 scope global eth1
    inet6 fe80::ff:fe01:4/64 scope link
       valid_lft forever preferred_lft forever
```

Verifica connettività (uno tra i servizi pec esportati)

- Il servizio è accessibile

```
[root@alfacentos ~]# date && openssl s_client -connect test-
smtps.sicurezzapostale.it:465
fri 16 nov 2012, 16.11.36, CET
CONNECTED(00000003)
[omiss]
220 frontout-test1.sicurezzapostale.it ESMTP Postfix
```

Ripristino condizioni di operatività iniziali: riattivazione del servizio Keepalived su AccessoPEC1

- riattivazione del servizio Keepalived e controllo dei log sugli AccessoPEC

```
[root@accessopec-test1 ~]# date && /etc/init.d/keepalived start
Fri Nov 16 16:42:43 CET 2012
Starting keepalived:                                       [  OK  ]

[root@accessopec-test1 ~] less /var/log/messages|grep "VRRP_Instance"
Nov 16 16:42:43 accessopec-test1 Keepalived_vrrp[5190]:
VRRP_Instance(VI_1) Transition to MASTER STATE
```

```
Nov 16 16:42:43 accessopec-test1 Keepalived_vrrp[5190]:
VRRP_Instance(VI_GATEWAY) Transition to MASTER STATE
Nov 16 16:42:44 accessopec-test1 Keepalived_vrrp[5190]:
VRRP_Instance(VI_1) Entering MASTER STATE
Nov 16 16:42:44 accessopec-test1 Keepalived_vrrp[5190]:
VRRP_Instance(VI_GATEWAY) Entering MASTER STATE.

[root@accessopec-test2 ~] less /var/log/messages|grep "VRRP_Instance"
Nov 16 16:42:43 accessopec-test2 Keepalived_vrrp[28286]:
VRRP_Instance(VI_1) Received higher prio advert
Nov 16 16:42:43 accessopec-test2 Keepalived_vrrp[28286]:
VRRP_Instance(VI_1) Entering BACKUP STATE
Nov 16 16:42:43 accessopec-test2 Keepalived_vrrp[28286]:
VRRP_Instance(VI_GATEWAY) Received higher prio advert
Nov 16 16:42:43 accessopec-test2 Keepalived_vrrp[28286]:
VRRP_Instance(VI_GATEWAY) Entering BACKUP STATE
```

Verifica esportazione servizi nuovamente su AccessoPEC1

```
[root@accessopec-test1 ~]# ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast
state UP qlen 1000
    link/ether 02:00:00:00:00:03 brd ff:ff:ff:ff:ff:ff
    inet 192.168.255.3/24 brd 192.168.255.255 scope global eth0
    inet 192.168.255.11/32 scope global eth0
    inet 192.168.255.12/32 scope global eth0
    inet 192.168.255.13/32 scope global eth0
    inet 192.168.255.14/32 scope global eth0
    inet 192.168.255.15/32 scope global eth0
    inet 192.168.255.16/32 scope global eth0
    inet6 fe80::ff:fe00:3/64 scope link
       valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast
state UP qlen 1000
    link/ether 02:00:00:01:00:03 brd ff:ff:ff:ff:ff:ff
    inet 192.168.2.3/24 brd 192.168.2.255 scope global eth1
    inet 192.168.2.192/32 scope global eth1
    inet6 fe80::ff:fe01:3/64 scope link
       valid_lft forever preferred_lft forever
```

Verifica rimozione servizi da AccessoPEC2

```
[root@accessopec-test2 ~]# ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
```

```
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast
state UP qlen 1000
    link/ether 02:00:00:00:00:04 brd ff:ff:ff:ff:ff:ff
    inet 192.168.255.4/24 brd 192.168.255.255 scope global eth0
    inet6 fe80::ff:fe00:4/64 scope link
       valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast
state UP qlen 1000
    link/ether 02:00:00:01:00:04 brd ff:ff:ff:ff:ff:ff
    inet 192.168.2.4/24 brd 192.168.2.255 scope global eth1
    inet6 fe80::ff:fe01:4/64 scope link
       valid_lft forever preferred_lft forever
```

Laureando: Matteo Sartini	**Scheda sotto-test**	**MTest 07**
Data Test	**Codice Test**	**Esecutore test**
16/nov/2012	2-6-7	Matteo Sartini

Descrizione

SECONDO CASO

Simulazione del disservizio di AccessoPEC1 (master) eseguito prima mediante lo spegnimento del server, poi mediante lo spegnimento dell'interfaccia di rete.

Comandi eseguiti:

- date && reboot
- less /var/log/messages|grep "VRRP_Instance"
- date && ping -c 5 192.168.255.3
- date && ifdown eth0
- date && ifup eth0

Valutazioni/Rilievi

Partendo dalla situazione iniziale (cfr MTest01 – schede sotto-test dalla 01 fino alla 06) e sulla base della descrizione dell'evento di disservizio seguente, nel caso di spegnimento del server deve essere verificato:

- il passaggio di stato del server slave a master nel momento in cui il server viene spento. Può essere verificato soltanto il passaggio di stato sullo slave perché i log non vengono trattati

se il server è spento.;
- il ripristino della situazione iniziale con AccessoPEC1 master e AccessoPEC2 slave.

Nel caso dello spegnimento dell'interfaccia di rete deve essere verificato:

- il passaggio di stato da slave a master di AccessoPEC2;
- il passaggio di stato da master a slave di AccessoPEC1;
- il ripristino della situazione iniziale con AccessoPEC1 master e AccessoPEC2 slave.

Esito Test

Positivo

Risultati:

```
[root@accessopec-test1 ~]# date && reboot
Fri Nov 16 17:10:32 CET 2012

Broadcast message from root@accessopec-test1.sicurezzapostale.it
        (/dev/pts/0) at 17:10 ...

The system is going down for reboot NOW!
```

Allo spegnimento del servizio, si ottiene ciò che si è verificato manualmente (cfr scheda sotto-test MTest07 – Codice test 1-2-3-4-5-6-7 PRIMO CASO): il servizio di bilanciamento/alta affidabilità manda una priorità pari a 0 in modo che lo slave assuma il controllo delle risorse.

```
[root@accessopec-test1 ~]# less /var/log/messages|grep "VRRP_Instance"
Nov 16 17:10:32 accessopec-test1 Keepalived_vrrp[5190]:
VRRP_Instance(VI_1) sending 0 priority
Nov 16 17:10:32 accessopec-test1 Keepalived_vrrp[5190]:
VRRP_Instance(VI_GATEWAY) sending 0 priority

[root@accessopec-test2 ~]# less /var/log/messages|grep "VRRP_Instance"
Nov 16 17:10:33 accessopec-test2 Keepalived_vrrp[28286]:
VRRP_Instance(VI_GATEWAY) Transition to MASTER STATE
Nov 16 17:10:33 accessopec-test2 Keepalived_vrrp[28286]:
VRRP_Instance(VI_1) Transition to MASTER STATE
Nov 16 17:10:34 accessopec-test2 Keepalived_vrrp[28286]:
VRRP_Instance(VI_GATEWAY) Entering MASTER STATE
Nov 16 17:10:34 accessopec-test2 Keepalived_vrrp[28286]:
VRRP_Instance(VI_1) Entering MASTER STATE
```

I servizi PEC vengono automaticamente migrati su AccessoPEC2 e sono correttamente fruibili dall'esterno.

Al riavvio del server, AccessoPEC2 riceve un segnale di priorità più alta da parte di AccessoPEC1. Le risorse pertanto vengono rilasciate e AccessoPEC2 torna in stato slave, mentre accesspec1 torna al ruolo di master. La latenza dei servizi PEC esportati non differisce dalla latenza riscontrata nel caso di disservizio manuale (cfr scheda sotto-test MTest07 – Codice test 1-2-3-4-5-6-7 PRIMO CASO)

```
[root@accessopec-test1 ~]# less /var/log/messages|grep "VRRP_Instance"
Nov 16 17:11:12 accessopec-test1 Keepalived_vrrp[1412]:
VRRP_Instance(VI_1) Transition to MASTER STATE
Nov 16 17:11:12 accessopec-test1 Keepalived_vrrp[1412]:
VRRP_Instance(VI_GATEWAY) Transition to MASTER STATE
Nov 16 17:11:12 accessopec-test1 Keepalived_vrrp[1412]:
VRRP_Instance(VI_1) Entering MASTER STATE
Nov 16 17:11:12 accessopec-test1 Keepalived_vrrp[1412]:
VRRP_Instance(VI_GATEWAY) Entering MASTER STATE
```

```
[root@accessopec-test2 ~]# less /var/log/messages|grep "VRRP_Instance"
Nov 16 17:11:12 accessopec-test2 Keepalived_vrrp[28286]:
VRRP_Instance(VI_1) Received higher prio advert
Nov 16 17:11:12 accessopec-test2 Keepalived_vrrp[28286]:
VRRP_Instance(VI_1) Entering BACKUP STATE
Nov 16 17:11:12 accessopec-test2 Keepalived_vrrp[28286]:
VRRP_Instance(VI_GATEWAY) Received higher prio advert
Nov 16 17:11:12 accessopec-test2 Keepalived_vrrp[28286]:
VRRP_Instance(VI_GATEWAY) Entering BACKUP STATE
```

Simulando ora un problema all'interfaccia di rete di AccessoPEC1 (tramite lo spegnimento dell'interfaccia eth0) il servizio di bilanciamento/alta affidabilità resta attivo ma passa in modalità slave in quanto non è più raggiungibile dalla rete. Non si avrà pertanto l'invio allo slave di una bassa priorità, ma un semplice passaggio in stato da Master a Fault. Come nei casi precedenti, AccessoPEC2 assume il controllo dei servizi pec esportati assumendo il ruolo di master.

- Verifica spegnimento dell'interfaccia di rete su AccessoPEC1

```
[root@accessopec-test2 ~]# date && ping -c 5 192.168.255.3
Fri Nov 16 17:34:50 CET 2012
PING 192.168.255.3 (192.168.255.3) 56(84) bytes of data.
64 bytes from 192.168.255.3: icmp_seq=1 ttl=64 time=0.633 ms
64 bytes from 192.168.255.3: icmp_seq=2 ttl=64 time=0.596 ms
64 bytes from 192.168.255.3: icmp_seq=3 ttl=64 time=0.563 ms
64 bytes from 192.168.255.3: icmp_seq=4 ttl=64 time=0.575 ms
64 bytes from 192.168.255.3: icmp_seq=5 ttl=64 time=0.559 ms

--- 192.168.255.3 ping statistics ---
```

```
5 packets transmitted, 5 received, 0% packet loss, time 4000ms
rtt min/avg/max/mdev = 0.559/0.585/0.633/0.031 ms

[root@accessopec-test1 ~]# date && ifdown eth0
Fri Nov 16 17:35:11 CET 2012
[root@accessopec-test1 ~]#

[root@accessopec-test2 ~]# date && ping -c 5 192.168.255.3
Fri Nov 16 17:35:20 CET 2012
PING 192.168.255.3 (192.168.255.3) 56(84) bytes of data.

--- 192.168.255.3 ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 13999ms
```

- Verifica del rilascio delle risorse da AccessoPEC1 verso AccessoPEC2 senza l'invio della bassa priorità.

```
[root@accessopec-test1 ~]# less /var/log/messages|grep "VRRP_Instance"
Nov 16 17:35:12 accessopec-test1 Keepalived_vrrp[1412]:
VRRP_Instance(VI_1) Entering FAULT STATE
Nov 16 17:35:12 accessopec-test1 Keepalived_vrrp[1412]:
VRRP_Instance(VI_1) Now in FAULT state
Nov 16 17:35:12 accessopec-test1 Keepalived_vrrp[1412]:
VRRP_Instance(VI_GATEWAY) Entering FAULT STATE
Nov 16 17:35:12 accessopec-test1 Keepalived_vrrp[1412]:
VRRP_Instance(VI_GATEWAY) Now in FAULT state


[root@accessopec-test2 ~]# less /var/log/messages|grep "VRRP_Instance"
Nov 16 17:35:15 accessopec-test2 Keepalived_vrrp[28286]:
VRRP_Instance(VI_1) Transition to MASTER STATE
Nov 16 17:35:15 accessopec-test2 Keepalived_vrrp[28286]:
VRRP_Instance(VI_GATEWAY) Transition to MASTER STATE
Nov 16 17:35:15 accessopec-test2 Keepalived_vrrp[28286]:
VRRP_Instance(VI_1) Entering MASTER STATE
Nov 16 17:35:15 accessopec-test2 Keepalived_vrrp[28286]:
VRRP_Instance(VI_GATEWAY) Entering MASTER STATE
```

Ripristino della situazione iniziale (riattivazione dell'interfaccia eth0 su AccessoPEC1)

- Verifica della riattivazione di eth0 su AccessoPEC1

```
[root@accessopec-test1 ~]# date && ifup eth0
Fri Nov 16 17:38:09 CET 2012
[root@accessopec-test1 ~]#

[root@accessopec-test2 ~]# date && ping -c 5 192.168.255.3
Fri Nov 16 17:38:31 CET 2012
PING 192.168.255.3 (192.168.255.3) 56(84) bytes of data.
```

```
64 bytes from 192.168.255.3: icmp_seq=1 ttl=64 time=0.453 ms
64 bytes from 192.168.255.3: icmp_seq=2 ttl=64 time=0.537 ms
64 bytes from 192.168.255.3: icmp_seq=3 ttl=64 time=0.494 ms
64 bytes from 192.168.255.3: icmp_seq=4 ttl=64 time=0.454 ms
64 bytes from 192.168.255.3: icmp_seq=5 ttl=64 time=0.493 ms

--- 192.168.255.3 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4000ms
rtt min/avg/max/mdev = 0.453/0.486/0.537/0.034 ms
```

- Verifica del recupero delle risorse da parte di AccessoPEC1 in seguito all'invio di un messaggio con priorità più alta rispetto a AccessoPEC2

```
[root@accessopec-test1 ~]# less /var/log/messages|grep "VRRP_Instance"
Nov 16 17:39:12 accessopec-test1 Keepalived_vrrp[1412]:
VRRP_Instance(VI_1) Transition to MASTER STATE
Nov 16 17:39:12 accessopec-test1 Keepalived_vrrp[1412]:
VRRP_Instance(VI_GATEWAY) Transition to MASTER STATE
Nov 16 17:39:13 accessopec-test1 Keepalived_vrrp[1412]:
VRRP_Instance(VI_1) Entering MASTER STATE
Nov 16 17:39:13 accessopec-test1 Keepalived_vrrp[1412]:
VRRP_Instance(VI_GATEWAY) Entering MASTER STATE

[root@accessopec-test2 ~]# less /var/log/messages|grep "VRRP_Instance"
Nov 16 17:39:12 accessopec-test2 Keepalived_vrrp[28286]:
VRRP_Instance(VI_1) Received higher prio advert
Nov 16 17:39:12 accessopec-test2 Keepalived_vrrp[28286]:
VRRP_Instance(VI_1) Entering BACKUP STATE
Nov 16 17:39:12 accessopec-test2 Keepalived_vrrp[28286]:
VRRP_Instance(VI_GATEWAY) Received higher prio advert
Nov 16 17:39:12 accessopec-test2 Keepalived_vrrp[28286]:
VRRP_Instance(VI_GATEWAY) Entering BACKUP STATE
```

Laureando: Matteo Sartini	**Scheda sotto-test**	**MTest 07**

Data Test	**Codice Test**	**Esecutore test**
16/nov/2012	1-2-3-4-5-6-7	Matteo Sartini

Descrizione

TERZO CASO

Verifica del cambio di stato manuale eseguito mediante spegnimento del servizio di bilanciamento/alta affidabilità (Keepalived) su AccessoPEC2.

Verifica del ripristino della situazione iniziale con AccessoPEC2 master e AccessoPEC1 slave.

Comandi eseguiti:

- ping -c 5 192.168.255.3
- ping -c 5 192.168.255.4
- ip addr show
- date && /etc/init.d/keepalived start
- date && /etc/init.d/keepalived stop
- less /var/log/messages|grep "VRRP_Instance"
- date && openssl s_client -connect test-smtps.sicurezzapostale.it:465

Valutazioni/Rilievi

Partendo dalla situazione iniziale (cfr MTest01 – schede sotto-test dalla 01 fino alla 06) e sulla base della descrizione dell'evento di disservizio, deve essere verificato il passaggio di stato del server slave a master nel momento in cui il server (o il servizio) viene spento. Ciò significa che gli IP virtuali esportati dal server master devono migrare in automatico al server slave a garanzia di una corretta configurazione dell'accesso ai servizi PEC.

Può essere verificato soltanto il passaggio di stato sullo slave perché i log non vengono trattati se il server (o il servizio) è spento.

AccessoPEC1, in questo caso, deve diventare master e i servizi PEC esportati subiscono una interruzione quantificabile nell'intorno del minuto secondo rientrando ampiamente nei limiti normativi imposti.

Esito Test

Positivo

Risultati:

Verifica raggiungibilità degli AccessoPEC (no disservizio)

- AccessoPEC2 è raggiungibile

```
[root@accessopec-test1 ~]# ping -c 5 192.168.255.4
PING 192.168.255.4 (192.168.255.4) 56(84) bytes of data.
64 bytes from 192.168.255.4: icmp_seq=1 ttl=64 time=0.672 ms
64 bytes from 192.168.255.4: icmp_seq=2 ttl=64 time=0.566 ms
64 bytes from 192.168.255.4: icmp_seq=3 ttl=64 time=0.537 ms
64 bytes from 192.168.255.4: icmp_seq=4 ttl=64 time=0.627 ms
64 bytes from 192.168.255.4: icmp_seq=5 ttl=64 time=0.576 ms

--- 192.168.255.4 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4000ms
rtt min/avg/max/mdev = 0.537/0.595/0.672/0.054 ms
```

- AccessoPEC1 è raggiungibile

```
[root@accessopec-test2 ~]# ping -c 5 192.168.255.3
PING 192.168.255.3 (192.168.255.3) 56(84) bytes of data.
64 bytes from 192.168.255.3: icmp_seq=1 ttl=64 time=0.518 ms
64 bytes from 192.168.255.3: icmp_seq=2 ttl=64 time=0.529 ms
64 bytes from 192.168.255.3: icmp_seq=3 ttl=64 time=0.478 ms
64 bytes from 192.168.255.3: icmp_seq=4 ttl=64 time=0.401 ms
64 bytes from 192.168.255.3: icmp_seq=5 ttl=64 time=0.447 ms

--- 192.168.255.3 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4000ms
rtt min/avg/max/mdev = 0.401/0.474/0.529/0.052 ms
```

Verifica esportazione servizi PEC dal Master: (AccessoPEC2)

- I virtual IP evidenziati sono privati e corrispondono, mediante NAT, all'unico IP virtuale pubblico con il quale vengono esportati, come già detto nel capitolo 3.

```
[root@accessopec-test2 ~]# ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast
state UP qlen 1000
    link/ether 02:00:00:00:00:04 brd ff:ff:ff:ff:ff:ff
    inet 192.168.255.4/24 brd 192.168.255.255 scope global eth0
    inet 192.168.255.11/32 scope global eth0
```

```
    inet 192.168.255.12/32 scope global eth0
    inet 192.168.255.13/32 scope global eth0
    inet 192.168.255.14/32 scope global eth0
    inet 192.168.255.15/32 scope global eth0
    inet 192.168.255.16/32 scope global eth0
    inet6 fe80::ff:fe00:4/64 scope link
       valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast
state UP qlen 1000
    link/ether 02:00:00:01:00:04 brd ff:ff:ff:ff:ff:ff
    inet 192.168.2.4/24 brd 192.168.2.255 scope global eth1
    inet 192.168.2.192/32 scope global eth1
    inet6 fe80::ff:fe01:4/64 scope link
       valid_lft forever preferred_lft forever
```

Verifica esportazione servizi PEC dallo Slave: (AccessoPEC1)

```
[root@accessopec-test1 ~]# ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast
state UP qlen 1000
    link/ether 02:00:00:00:00:03 brd ff:ff:ff:ff:ff:ff
    inet 192.168.255.3/24 brd 192.168.255.255 scope global eth0
    inet6 fe80::ff:fe00:3/64 scope link
       valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast
state UP qlen 1000
    link/ether 02:00:00:01:00:03 brd ff:ff:ff:ff:ff:ff
    inet 192.168.2.3/24 brd 192.168.2.255 scope global eth1
    inet6 fe80::ff:fe01:3/64 scope link
       valid_lft forever preferred_lft forever
```

Spegnimento del server/servizio Keepalived (supponiamo ad esempio sia necessario un riavvio o un aggiornamento hardware):

Spegnimento del servizio Keepalived e controllo dei log sugli AccessoPEC

```
[root@accessopec-test2 ~]# date && /etc/init.d/keepalived stop
Fri Nov 16 17:40:35 CET 2012
Stopping keepalived:                                       [  OK  ]

[root@accessopec-test2 ~] less /var/log/messages|grep "VRRP_Instance"
Nov 16 17:40:35 accessopec-test2 Keepalived_vrrp[4090]:
VRRP_Instance(VI_1) sending 0 priority
Nov 16 17:40:35 accessopec-test2 Keepalived_vrrp[4090]:
```

```
VRRP_Instance(VI_GATEWAY) sending 0 priority

[root@accessopec-test1 ~]# less /var/log/messages|grep "VRRP_Instance"
Nov 16 17:40:36 accessopec-test1 Keepalived_vrrp[28286]:
VRRP_Instance(VI_GATEWAY) Transition to MASTER STATE
Nov 16 17:40:36 accessopec-test1 Keepalived_vrrp[28286]:
VRRP_Instance(VI_1) Transition to MASTER STATE
Nov 16 17:40:36 accessopec-test1 Keepalived_vrrp[28286]:
VRRP_Instance(VI_GATEWAY) Entering MASTER STATE
Nov 16 17:40:36 accessopec-test1 Keepalived_vrrp[28286]:
VRRP_Instance(VI_1) Entering MASTER STATE
```

Verifica esportazione servizi PEC su AccessoPEC2

```
[root@accessopec-test2 ~]# ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast
state UP qlen 1000
    link/ether 02:00:00:00:00:04 brd ff:ff:ff:ff:ff:ff
    inet 192.168.255.4/24 brd 192.168.255.255 scope global eth0
    inet6 fe80::ff:fe00:4/64 scope link
       valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast
state UP qlen 1000
    link/ether 02:00:00:01:00:04 brd ff:ff:ff:ff:ff:ff
    inet 192.168.2.4/24 brd 192.168.2.255 scope global eth1
    inet6 fe80::ff:fe01:4/64 scope link
       valid_lft forever preferred_lft forever
```

Verifica esportazione servizi PEC su AccessoPEC1 (nuovo master)

```
[root@accessopec-test1 ~]# ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast
state UP qlen 1000
    link/ether 02:00:00:00:00:03 brd ff:ff:ff:ff:ff:ff
    inet 192.168.255.3/24 brd 192.168.255.255 scope global eth0
    inet 192.168.255.11/32 scope global eth0
    inet 192.168.255.12/32 scope global eth0
    inet 192.168.255.13/32 scope global eth0
    inet 192.168.255.14/32 scope global eth0
    inet 192.168.255.15/32 scope global eth0
    inet 192.168.255.16/32 scope global eth0
```

```
    inet6 fe80::ff:fe00:3/64 scope link
       valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast
state UP qlen 1000
    link/ether 02:00:00:01:00:03 brd ff:ff:ff:ff:ff:ff
    inet 192.168.2.3/24 brd 192.168.2.255 scope global eth1
    inet 192.168.2.192/32 scope global eth1
    inet6 fe80::ff:fe01:3/64 scope link
       valid_lft forever preferred_lft forever
```

Verifica connettività (uno tra i servizi pec esportati)

- Il servizio è accessibile

```
[root@alfacentos ~]# date && openssl s_client -connect test-
smtps.sicurezzapostale.it:465
fri 16 nov 2012, 17.40.36, CET
CONNECTED(00000003)
[omiss]
220 frontout-test1.sicurezzapostale.it ESMTP Postfix
```

Ripristino condizioni di operatività iniziali: riattivazione del servizio Keepalived su AccessoPEC2

- riattivazione del servizio Keepalived e controllo dei log sugli AccessoPEC

```
[root@accessopec-test2 ~]# date && /etc/init.d/keepalived start
Fri Nov 16 17:51:43 CET 2012
Starting keepalived:                                       [  OK  ]

[root@accessopec-test2 ~] less /var/log/messages|grep "VRRP_Instance"
Nov 16 17:51:43 accessopec-test2 Keepalived_vrrp[5190]:
VRRP_Instance(VI_1) Transition to MASTER STATE
Nov 16 17:51:43 accessopec-test2 Keepalived_vrrp[5190]:
VRRP_Instance(VI_GATEWAY) Transition to MASTER STATE
Nov 16 17:51:44 accessopec-test2 Keepalived_vrrp[5190]:
VRRP_Instance(VI_1) Entering MASTER STATE
Nov 16 17:51:44 accessopec-test2 Keepalived_vrrp[5190]:
VRRP_Instance(VI_GATEWAY) Entering MASTER STATE

[root@accessopec-test1 ~] less /var/log/messages|grep "VRRP_Instance"
Nov 16 17:51:43 accessopec-test1 Keepalived_vrrp[28286]:
VRRP_Instance(VI_1) Received higher prio advert
Nov 16 17:51:43 accessopec-test1 Keepalived_vrrp[28286]:
VRRP_Instance(VI_1) Entering BACKUP STATE
Nov 16 17:51:43 accessopec-test1 Keepalived_vrrp[28286]:
VRRP_Instance(VI_GATEWAY) Received higher prio advert
Nov 16 17:51:43 accessopec-test1 Keepalived_vrrp[28286]:
VRRP_Instance(VI_GATEWAY) Entering BACKUP STATE
```

Verifica esportazione servizi nuovamente su AccessoPEC2

```
[root@accessopec-test2 ~]# ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast
state UP qlen 1000
    link/ether 02:00:00:00:00:04 brd ff:ff:ff:ff:ff:ff
    inet 192.168.255.4/24 brd 192.168.255.255 scope global eth0
    inet 192.168.255.11/32 scope global eth0
    inet 192.168.255.12/32 scope global eth0
    inet 192.168.255.13/32 scope global eth0
    inet 192.168.255.14/32 scope global eth0
    inet 192.168.255.15/32 scope global eth0
    inet 192.168.255.16/32 scope global eth0
    inet6 fe80::ff:fe00:4/64 scope link
       valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast
state UP qlen 1000
    link/ether 02:00:00:01:00:04 brd ff:ff:ff:ff:ff:ff
    inet 192.168.2.4/24 brd 192.168.2.255 scope global eth1
    inet 192.168.2.192/32 scope global eth1
    inet6 fe80::ff:fe01:4/64 scope link
       valid_lft forever preferred_lft forever
```

Verifica rimozione servizi da AccessoPEC1

```
[root@accessopec-test1 ~]# ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast
state UP qlen 1000
    link/ether 02:00:00:00:00:03 brd ff:ff:ff:ff:ff:ff
    inet 192.168.255.3/24 brd 192.168.255.255 scope global eth0
    inet6 fe80::ff:fe00:3/64 scope link
       valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast
state UP qlen 1000
    link/ether 02:00:00:01:00:03 brd ff:ff:ff:ff:ff:ff
    inet 192.168.2.3/24 brd 192.168.2.255 scope global eth1
    inet6 fe80::ff:fe01:3/64 scope link
       valid_lft forever preferred_lft forever
```

Laureando: Matteo Sartini	**Scheda sotto-test**	**MTest 07**

Data Test	**Codice Test**	**Esecutore test**
16/nov/2012	3-6-7	Matteo Sartini

Descrizione

QUARTO CASO

Simulazione del disservizio di AccessoPEC2 (master) eseguito prima mediante lo spegnimento del server e poi mediante lo spegnimento dell'interfaccia di rete.

Comandi eseguiti:

- date && reboot
- less /var/log/messages|grep "VRRP_Instance"
- date && ping -c 5 192.168.255.4
- date && ifdown eth0
- date && ifup eth0

Valutazioni/Rilievi

Partendo dalla situazione iniziale (cfr MTest01 – schede sotto-test dalla 01 fino alla 06) e sulla base della descrizione dell'evento di disservizio seguente, nel caso di spegnimento del server deve essere verificato:

- il passaggio di stato del server slave a master nel momento in cui il server viene spento. Può essere verificato soltanto il passaggio di stato sullo slave perché i log non vengono trattati se il server è spento.;
- il ripristino della situazione iniziale con AccessoPEC2 master e AccessoPEC1 slave.

Nel caso dello spegnimento dell'interfaccia di rete deve essere verificato:

- il passaggio di stato da slave a master di AccessoPEC1;
- il passaggio di stato da master a slave di AccessoPEC2;
- il ripristino della situazione iniziale con AccessoPEC2 master e AccessoPEC1 slave.

Esito Test

Positivo

Risultati:

```
[root@accessopec-test2 ~]# date && reboot
Fri Nov 16 18:08:32 CET 2012

Broadcast message from root@accessopec-test2.sicurezzapostale.it
        (/dev/pts/0) at 18:08 ...

The system is going down for reboot NOW!
```

Allo spegnimento del servizio, si ottiene ciò che si è verificato manualmente (cfr scheda sotto-test MTest07 – Codice test 1-2-3-4-5-6-7 TERZO CASO): il servizio di bilanciamento/alta affidabilità manda una priorità pari a 0 in modo che lo slave assuma il controllo delle risorse.

```
[root@accessopec-test2 ~]# less /var/log/messages|grep "VRRP_Instance"
Nov 16 18:08:32 accessopec-test2 Keepalived_vrrp[5190]:
VRRP_Instance(VI_1) sending 0 priority
Nov 16 18:08:32 accessopec-test2 Keepalived_vrrp[5190]:
VRRP_Instance(VI_GATEWAY) sending 0 priority

[root@accessopec-test1 ~]# less /var/log/messages|grep "VRRP_Instance"
Nov 16 18:08:33 accessopec-test1 Keepalived_vrrp[28286]:
VRRP_Instance(VI_GATEWAY) Transition to MASTER STATE
Nov 16 18:08:33 accessopec-test1 Keepalived_vrrp[28286]:
VRRP_Instance(VI_1) Transition to MASTER STATE
Nov 16 18:08:34 accessopec-test1 Keepalived_vrrp[28286]:
VRRP_Instance(VI_GATEWAY) Entering MASTER STATE
Nov 16 18:08:34 accessopec-test1 Keepalived_vrrp[28286]:
VRRP_Instance(VI_1) Entering MASTER STATE
```

I servizi PEC vengono automaticamente migrati su AccessoPEC1 e sono correttamente fruibili dall'esterno.

Al riavvio del server, AccessoPEC1 riceve un segnale di priorità più alta da parte di AccessoPEC2. Le risorse pertanto vengono rilasciate e AccessoPEC1 torna in stato slave, mentre AccessPEC2 torna al ruolo di master. La latenza dei servizi PEC esportati non differisce dalla latenza riscontrata nel caso di disservizio manuale (cfr scheda sotto-test MTest07 – Codice test 1-2-3-4-5-6-7 TERZO CASO)

```
[root@accessopec-test2 ~]# less /var/log/messages|grep "VRRP_Instance"
Nov 16 18:09:12 accessopec-test2 Keepalived_vrrp[1412]:
VRRP_Instance(VI_1) Transition to MASTER STATE
Nov 16 18:09:12 accessopec-test2 Keepalived_vrrp[1412]:
VRRP_Instance(VI_GATEWAY) Transition to MASTER STATE
```

```
Nov 16 18:09:12 accessopec-test2 Keepalived_vrrp[1412]:
VRRP_Instance(VI_1) Entering MASTER STATE
Nov 16 18:09:12 accessopec-test2 Keepalived_vrrp[1412]:
VRRP_Instance(VI_GATEWAY) Entering MASTER STATE

[root@accessopec-test1 ~]# less /var/log/messages|grep "VRRP_Instance"
Nov 16 18:09:12 accessopec-test1 Keepalived_vrrp[28286]:
VRRP_Instance(VI_1) Received higher prio advert
Nov 16 18:09:12 accessopec-test1 Keepalived_vrrp[28286]:
VRRP_Instance(VI_1) Entering BACKUP STATE
Nov 16 18:09:12 accessopec-test1 Keepalived_vrrp[28286]:
VRRP_Instance(VI_GATEWAY) Received higher prio advert
Nov 16 18:09:12 accessopec-test1 Keepalived_vrrp[28286]:
VRRP_Instance(VI_GATEWAY) Entering BACKUP STATE
```

Simulando ora un problema all'interfaccia di rete di AccessoPEC2 (tramite lo spegnimento dell'interfaccia eth0) il servizio di bilanciamento/alta affidabilità resta attivo ma passa in modalità slave in quanto non è più raggiungibile dalla rete. Non si avrà pertanto l'invio allo slave di una bassa priorità, ma un semplice passaggio in stato da Master a Fault. Come nei casi precedenti, AccessoPEC1 assume il controllo dei servizi pec esportati assumendo il ruolo di master.

Verifica spegnimento dell'interfaccia di rete su AccessoPEC2

```
[root@accessopec-test1 ~]# date && ping -c 5 192.168.255.4
Fri Nov 16 18:11:50 CET 2012
PING 192.168.255.4 (192.168.255.4) 56(84) bytes of data.
64 bytes from 192.168.255.4: icmp_seq=1 ttl=64 time=0.633 ms
64 bytes from 192.168.255.4: icmp_seq=2 ttl=64 time=0.596 ms
64 bytes from 192.168.255.4: icmp_seq=3 ttl=64 time=0.563 ms
64 bytes from 192.168.255.4: icmp_seq=4 ttl=64 time=0.575 ms
64 bytes from 192.168.255.4: icmp_seq=5 ttl=64 time=0.559 ms

--- 192.168.255.4 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4000ms
rtt min/avg/max/mdev = 0.559/0.585/0.633/0.031 ms

[root@accessopec-test2 ~]# date && ifdown eth0
Fri Nov 16 18:12:11 CET 2012
[root@accessopec-test2 ~]#

[root@accessopec-test1 ~]# date && ping -c 5 192.168.255.4
Fri Nov 16 18:12:20 CET 2012
PING 192.168.255.4 (192.168.255.3) 56(84) bytes of data.

--- 192.168.255.4 ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 13999ms
```

Verifica del rilascio delle risorse da AccessoPEC2 verso AccessoPEC1 senza l'invio della bassa priorità.

```
[root@accessopec-test2 ~]# less /var/log/messages|grep "VRRP_Instance"
Nov 16 18:13:12 accessopec-test2 Keepalived_vrrp[1412]:
VRRP_Instance(VI_1) Entering FAULT STATE
Nov 16 18:13:12 accessopec-test2 Keepalived_vrrp[1412]:
VRRP_Instance(VI_1) Now in FAULT state
Nov 16 18:13:12 accessopec-test2 Keepalived_vrrp[1412]:
VRRP_Instance(VI_GATEWAY) Entering FAULT STATE
Nov 16 18:13:12 accessopec-test2 Keepalived_vrrp[1412]:
VRRP_Instance(VI_GATEWAY) Now in FAULT state

[root@accessopec-test1 ~]# less /var/log/messages|grep "VRRP_Instance"
Nov 16 18:13:15 accessopec-test1 Keepalived_vrrp[28286]:
VRRP_Instance(VI_1) Transition to MASTER STATE
Nov 16 18:13:15 accessopec-test1 Keepalived_vrrp[28286]:
VRRP_Instance(VI_GATEWAY) Transition to MASTER STATE
Nov 16 18:13:15 accessopec-test1 Keepalived_vrrp[28286]:
VRRP_Instance(VI_GATEWAY) Entering MASTER STATE
Nov 16 18:13:16 accessopec-test1 Keepalived_vrrp[28286]:
VRRP_Instance(VI_1) Entering MASTER STATE
```

Ripristino della situazione iniziale (riattivazione dell'interfaccia eth0 su AccessoPEC2)

- Verifica della riattivazione di eth0 su AccessoPEC2

```
[root@accessopec-test2 ~]# date && ifup eth0
Fri Nov 16 18:15:09 CET 2012
[root@accessopec-test2 ~]#

[root@accessopec-test1 ~]# date && ping -c 5 192.168.255.4
Fri Nov 16 18:15:31 CET 2012
PING 192.168.255.4 (192.168.255.4) 56(84) bytes of data.
64 bytes from 192.168.255.4: icmp_seq=1 ttl=64 time=0.453 ms
64 bytes from 192.168.255.4: icmp_seq=2 ttl=64 time=0.537 ms
64 bytes from 192.168.255.4: icmp_seq=3 ttl=64 time=0.494 ms
64 bytes from 192.168.255.4: icmp_seq=4 ttl=64 time=0.454 ms
64 bytes from 192.168.255.4: icmp_seq=5 ttl=64 time=0.493 ms

--- 192.168.255.4 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4000ms
rtt min/avg/max/mdev = 0.453/0.486/0.537/0.034 ms
```

Verifica del recupero delle risorse da parte di AccessoPEC2 in seguito all'invio di un messaggio con priorità più alta rispetto a AccessoPEC1

```
[root@accessopec-test2 ~]# less /var/log/messages|grep "VRRP_Instance"
Nov 16 18:15:12 accessopec-test2 Keepalived_vrrp[1412]:
VRRP_Instance(VI_1) Transition to MASTER STATE
Nov 16 18:15:12 accessopec-test2 Keepalived_vrrp[1412]:
VRRP_Instance(VI_GATEWAY) Transition to MASTER STATE
Nov 16 18:15:13 accessopec-test2 Keepalived_vrrp[1412]:
VRRP_Instance(VI_1) Entering MASTER STATE
Nov 16 18:15:13 accessopec-test2 Keepalived_vrrp[1412]:
VRRP_Instance(VI_GATEWAY) Entering MASTER STATE

[root@accessopec-test1 ~]# less /var/log/messages|grep "VRRP_Instance"
Nov 16 18:15:12 accessopec-test1 Keepalived_vrrp[28286]:
VRRP_Instance(VI_1) Received higher prio advert
Nov 16 18:15:12 accessopec-test1 Keepalived_vrrp[28286]:
VRRP_Instance(VI_1) Entering BACKUP STATE
Nov 16 18:15:12 accessopec-test1 Keepalived_vrrp[28286]:
VRRP_Instance(VI_GATEWAY) Received higher prio advert
Nov 16 18:15:12 accessopec-test1 Keepalived_vrrp[28286]:
VRRP_Instance(VI_GATEWAY) Entering BACKUP STATE
```

4.8 Verifiche con disservizio al server AccessoPEC Slave

Laureando: Matteo Sartini	**Disservizio AccessoPEC Slave**	**MTest 08**
		Data: 08/11/2012

Descrizione:
Questo test ha lo scopo di verificare il corretto funzionamento della struttura in uno scenario che prevede disservizi al server AccessoPEC slave.

Situazione iniziale (scenario):
L'infrastruttura accede ad Internet ed i servizi esportati vengono acceduti regolarmente da Internet.
Il router del provider dei servizi internet è correttamente operativo e configurato.
Il cablaggio tra lo switch1 e gli altri apparati è corretto e funzionante.
I firewall sono funzionanti e correttamente collegati.
I restanti apparati (AccessoPEC, switch del livello 2) sono configurati correttamente ed operativi.

Azioni/Simulazioni:
<u>Primo caso</u>
Supponiamo che lo slave sia il server AccessoPEC2.
Verrà simulato un disservizio di AccessoPEC2 eseguendo (vedi immagine di riferimento n°1):

1. lo spegnimento del server;
2. lo spegnimento dell'interfaccia di rete (valido anche per simulare lo scollegamento).

<u>Secondo caso</u>
Supponiamo che lo slave sia il server AccessoPEC1.
Verrà simulato un disservizio di AccessoPEC1 eseguendo (vedi immagine di riferimento n°2):

1. lo spegnimento del server;
2. lo spegnimento dell'interfaccia di rete (valido anche per simulare lo scollegamento).

Tipo di verifica:

- Accessibilità alla rete internet. Verificare se ogni AccessoPEC è in grado di:
  - Risolvere un nome a dominio nel relativo indirizzo IP
  - Controllare il percorso per raggiungere un indirizzo IP
- Accessibilità dei servizi dalla rete internet. Verificare se da un qualsiasi punto della rete internet è possibile:
  - Risolvere il nome del servizio esportato nel suo indirizzo IP pubblico
  - Raggiungere l'IP pubblico del servizio

Primo caso

- Verificare la raggiungibilità del server AccessoPEC2.
- Verificare che non si sono avuti cambi di stato nel server AccessoPEC1 (master).

Secondo caso

- Verificare la raggiungibilità del server AccessoPEC1.
- Verificare che non si sono avuti cambi di stato nel server AccessoPEC2 (master).

Verranno consultati i log di sistema dei server AccessoPEC per verificarne la configurazione (master o slave). Inoltre verranno utilizzati gli strumenti Ping e OpenSSL per verificare la raggiungibilità di indirizzi IP e servizi.

Esito:	**Data:**
In questo scenario si è potuto notare come un malfunzionamento o disservizio al bilanciatore in stato slave non comprometta l'accessibilità ai servizi di PEC. Infatti, durante il test, a seguito dello spegnimento del server e successivamente dello spegnimento dell'interfaccia di rete, è stata eseguita una verifica di accessibilità ai servizi la quale ha restituito esito positivo. Ciò significa che il bilanciatore in stato master è rimasto sempre tale, esportando correttamente i servizi di PEC.	20/nov/2012

Immagine di riferimento n°1:

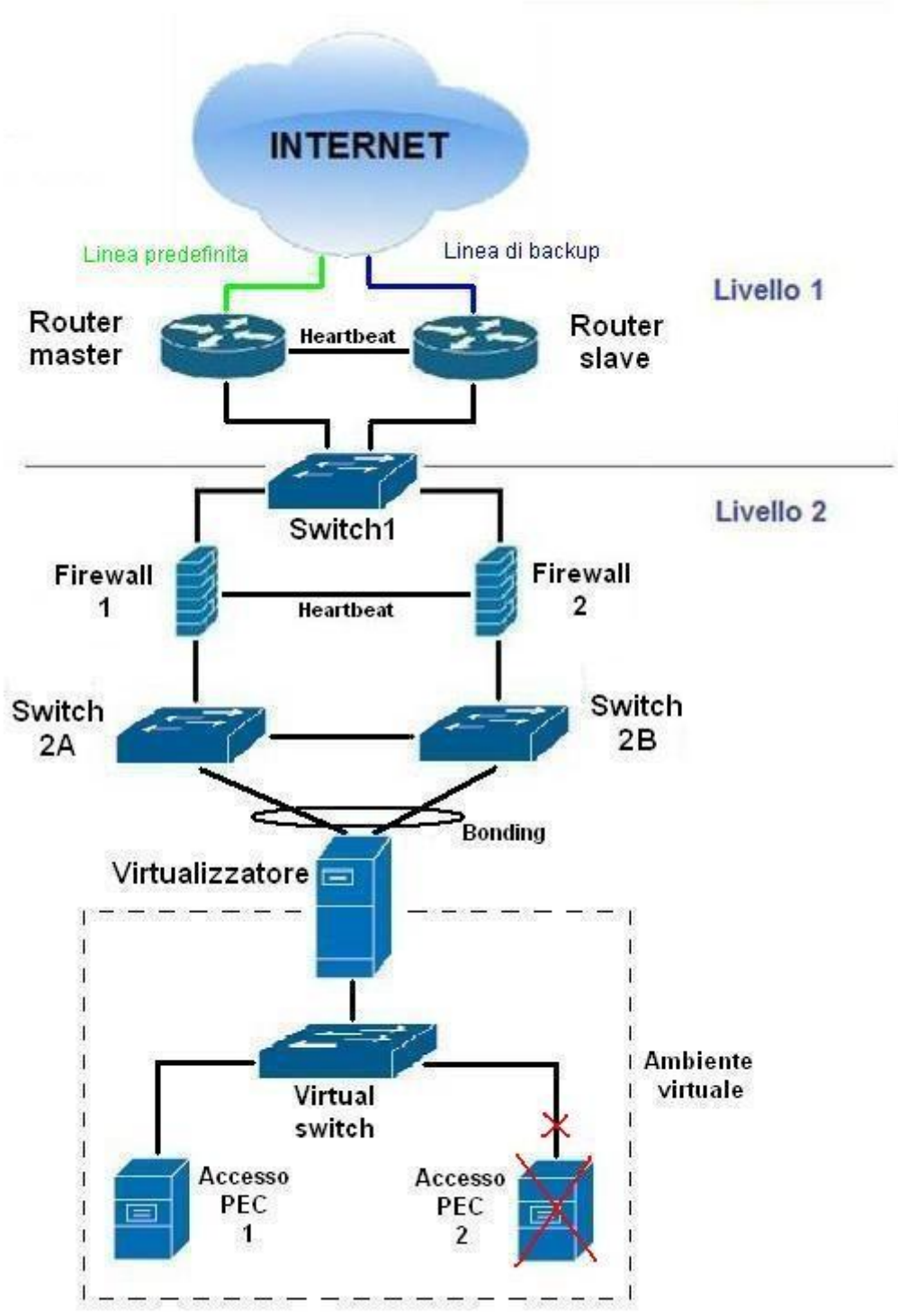
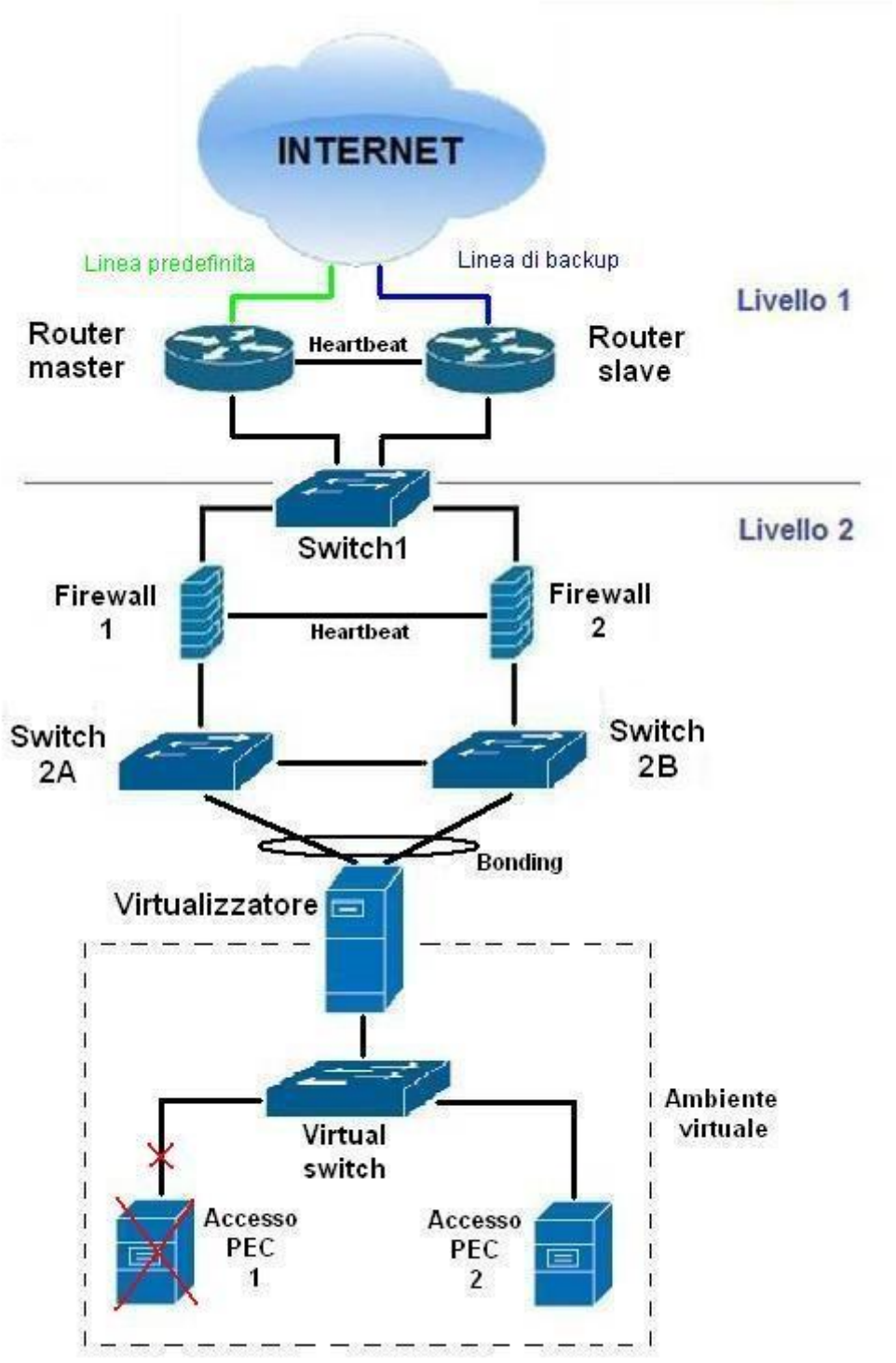


Immagine di riferimento n°2:



Laureando: Matteo Sartini	**Lista sotto-test Disservizio AccessoPEC Slave**	**MTest 08**
		Data: 09/11/2012

CODICE	**SOTTO-TEST**
01	Accessibilità dei servizi da internet.
02	Verifica stato master/slave di AccessoPEC1.
03	Verifica stato master/slave di AccessoPEC2.
04	Verifica raggiungibilità AccessoPEC1.
05	Verifica raggiungibilità AccessoPEC2.

Laureando: Matteo Sartini	**Scheda sotto-test**	**MTest 08**
Data Test	**Codice Test**	**Esecutore test**
20/nov/2012	1-2-3-5	Matteo Sartini

Descrizione

PRIMO CASO

Simulazione del disservizio di AccessoPEC2 (slave) eseguito mediante:

- lo spegnimento del server;
- lo spegnimento dell'interfaccia di rete.

Comandi eseguiti:

- date && reboot
- less /var/log/messages|grep "Keepalive"
- date && openssl s_client -connect test-smtps.sicurezzapostale.it:465
- date && ping -c 5 192.168.255.4
- date && ifdown eth0
- date && ifup eth0

Valutazioni/Rilievi

Partendo dalla situazione iniziale (cfr schede sotto-test MTest01 – dalla 01 fino alla 06) e sulla base della descrizione dell'evento di disservizio seguente, nel caso di spegnimento del server deve essere verificato:

- che lo stato del server master (AccessoPEC1) rimanga tale nel

momento in cui il server slave (AccessoPEC2) viene spento;
- che i servizi siano accessibili;
- che a seguito della riattivazione del server AccessoPEC2, lo stato di quest'ultimo sia slave e lo stato di AccessoPEC1 rimanga master.

Nel caso dello spegnimento dell'interfaccia di rete deve essere verificato:
- che lo stato master di AccessoPEC1 e lo stato slave di AccessoPEC2 rimangano tali;
- che i servizi siano accessibili;
- che a seguito della riattivazione dell'interfaccia di rete del server AccessoPEC2, lo stato di quest'ultimo rimanga slave e lo stato di AccessoPEC1 rimanga master.

Esito Test

Positivo

Risultati:

A seguito dello spegnimento del server AccessoPEC2, il servizio di bilanciamento/alta affidabilità (Keepalived) interrompe la sua operatività, ma i servizi continuano ad essere accessibili da Internet. Questo significa che AccessoPEC1 è in stato master. Al riavvio del server, Keepalived entra in stato slave (Backup State).

- Riavvio del server con conseguente spegnimento di Keepalived su AccessoPEC 2 (slave)

```
[root@accessopec-test2 ~]# date && reboot
Tue Nov  20 15:52:16 CET 2012
```

- Controllo dei log su AccessoPEC 2 (slave)

```
[root@accessopec-test2 ~]# less /var/log/messages|grep "Keepalive"
Nov  20 15:52:16 accessopec-test2 Keepalived[1434]: Stopping Keepalived
v1.2.7
```

- Verifica connettività (uno tra i servizi pec esportati)

```
[root@alfacentos ~]# date && openssl s_client -connect test-
smtps.sicurezzapostale.it:465
tue 20 nov 2012, 15.52.32, CET
CONNECTED(00000003)
[omiss]
220 frontout-test1.sicurezzapostale.it ESMTP Postfix
```

- Al completamento del riavvio, il servizio Keepalived si riattiva ed entra in Backup State.

```
[root@accessopec-test2 ~]# less /var/log/messages|grep "Keepalive"
Nov  20 15:52:52 accessopec-test2 Keepalived[1408]: Starting Keepalived
v1.2.7
Nov  20 15:52:52 accessopec-test2 Keepalived_vrrp[1412]:
VRRP_Instance(VI_1) Entering BACKUP STATE
Nov  20 15:52:52 accessopec-test2 Keepalived_vrrp[1412]:
VRRP_Instance(VI_GATEWAY) Entering BACKUP STATE
```

Simulando ora un problema all'interfaccia di rete di AccessoPEC2 (tramite lo spegnimento dell'interfaccia eth0) il servizio Keepalived resta attivo ma passa in Fault State in quanto non è più raggiungibile dalla rete. I servizi continuano ad essere accessibili da Internet, il che significa che AccessoPEC1 continua ad operare in stato master. Alla riattivazione dell'interfaccia eth0 su AccessoPEC2, il servizio Keepalived ritorna in stato slave (Backup State).

- Verifica raggiungibilità AccessoPEC 2

```
[root@accessopec-test1 ~]# date && ping -c 5 192.168.255.4
Tue Nov  20 15:55:45 CET 2012
PING 192.168.255.4 (192.168.255.4) 56(84) bytes of data.
64 bytes from 192.168.255.4: icmp_seq=1 ttl=64 time=0.486 ms
64 bytes from 192.168.255.4: icmp_seq=2 ttl=64 time=0.507 ms
64 bytes from 192.168.255.4: icmp_seq=3 ttl=64 time=0.533 ms
64 bytes from 192.168.255.4: icmp_seq=4 ttl=64 time=0.515 ms
64 bytes from 192.168.255.4: icmp_seq=5 ttl=64 time=0.595 ms

--- 192.168.255.4 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4001ms
rtt min/avg/max/mdev = 0.486/0.527/0.595/0.039 ms
```

- Spegnimento dell'interfaccia eth0 su AccessoPEC 2

```
[root@accessopec-test2 ~]# date && ifdown eth0
Tue Nov  20 15:56:51 CET 2012
[root@accessopec-test2 ~]#
```

- Verifica cambio di stato del servizio Keepalived in Fault State

```
[root@accessopec-test2 ~]# less /var/log/messages|grep "Keepalived"
Nov  20 15:56:51 accessopec-test2 Keepalived_vrrp[1412]: Kernel is
reporting: interface eth0 DOWN
Nov  20 15:56:51 accessopec-test2 Keepalived_vrrp[1412]:
VRRP_Instance(VI_1) Now in FAULT state
```

- Verifica raggiungibilità di AccessoPEC2

```
[root@accessopec-test1 ~]# date && ping -c 5 192.168.255.4
Tue Nov  20 15:57:13 CET 2012
PING 192.168.255.4 (192.168.255.4) 56(84) bytes of data.

--- 192.168.255.4 ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 13999ms
```

- Verifica connettività (uno tra i servizi pec esportati)

```
[root@alfacentos ~]# date && openssl s_client -connect test-
smtps.sicurezzapostale.it:465
tue 20 nov 2012, 16.00.36, CET
CONNECTED(00000003)
[omiss]
220 frontout-test1.sicurezzapostale.it ESMTP Postfix
```

- Riattivazione interfaccia eth0 su AccessoPEC2

```
[root@accessopec-test2 ~]# date && ifup eth0
Tue Nov  20 16:01:51 CET 2012
[root@accessopec-test2 ~]#
```

- Verifica cambio di stato del servizio Keepalived in Backup State

```
[root@accessopec-test2 ~]# less /var/log/messages|grep "Keepalived"
Nov  20 16:01:51 accessopec-test2 Keepalived_vrrp[1412]:
VRRP_Instance(VI_GATEWAY) Entering BACKUP STATE
Nov  20 16:01:51 accessopec-test2 Keepalived_vrrp[1412]:
VRRP_Instance(VI_1) Entering BACKUP STATE
```

- Verifica raggiungibilità di AccessoPEC 2

```
[root@accessopec-test1 ~]# date && ping -c 5 192.168.255.4
Tue Nov  20 15:58:47 CET 2012
PING 192.168.255.4 (192.168.255.4) 56(84) bytes of data.
64 bytes from 192.168.255.4: icmp_seq=1 ttl=64 time=1.44 ms
64 bytes from 192.168.255.4: icmp_seq=2 ttl=64 time=0.601 ms
64 bytes from 192.168.255.4: icmp_seq=3 ttl=64 time=0.564 ms
64 bytes from 192.168.255.4: icmp_seq=4 ttl=64 time=0.525 ms
64 bytes from 192.168.255.4: icmp_seq=5 ttl=64 time=0.474 ms

--- 192.168.255.4 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4002ms
rtt min/avg/max/mdev = 0.474/0.721/1.442/0.363 ms
```

Laureando: Matteo Sartini	**Scheda sotto-test**	**MTest 08**
Data Test	**Codice Test**	**Esecutore test**
20/nov/2012	1-2-3-4	Matteo Sartini

Descrizione

SECONDO CASO

Simulazione del disservizio di AccessoPEC1 (slave) eseguito mediante:

- lo spegnimento del server;
- lo spegnimento dell'interfaccia di rete.

Comandi eseguiti:

- date && reboot
- less /var/log/messages|grep "Keepalive"
- date && openssl s_client -connect test-smtps.sicurezzapostale.it:465
- date && ping -c 5 192.168.255.3
- date && ifdown eth0
- date && ifup eth0

Valutazioni/Rilievi

Partendo dalla situazione iniziale (cfr schede sotto-test MTest01 – dalla 01 fino alla 06) e sulla base della descrizione dell'evento di disservizio seguente, nel caso di spegnimento del server deve essere verificato:

- che lo stato del server master (AccessoPEC2) rimanga tale nel momento in cui il server slave (AccessoPEC1) viene spento;
- che i servizi siano accessibili;
- che a seguito della riattivazione del server AccessoPEC1, lo stato di quest'ultimo sia slave e lo stato di AccessoPEC2 rimanga master.

Nel caso dello spegnimento dell'interfaccia di rete deve essere verificato:

- che lo stato master di AccessoPEC2 e lo stato slave di AccessoPEC1 rimangano tali;
- che i servizi siano accessibili;
- che a seguito della riattivazione dell'interfaccia di rete del server AccessoPEC1, lo stato di quest'ultimo rimanga slave e lo stato di

AccessoPEC2 rimanga master.

Esito Test

Positivo

Risultati:

A seguito dello spegnimento del server AccessoPEC1, il servizio di bilanciamento/alta affidabilità (Keepalived) interrompe la sua operatività, ma i servizi continuano ad essere accessibili da Internet. Questo significa che AccessoPEC2 è in stato master. Al riavvio del server, Keepalived entra in stato slave (Backup State).

- Riavvio del server con conseguente spegnimento di Keepalived su AccessoPEC 1 (slave)

```
[root@accessopec-test1 ~]# date && reboot
Tue Nov  20 16:48:18 CET 2012
```

- Controllo dei log su AccessoPEC 1 (slave)

```
[root@accessopec-test1 ~]# less /var/log/messages|grep "Keepalive"
Nov  20 16:48:18 accessopec-test1 Keepalived[1434]: Stopping Keepalived
v1.2.7
```

- Verifica connettività (uno tra i servizi pec esportati)

```
[root@alfacentos ~]# date && openssl s_client -connect test-
smtps.sicurezzapostale.it:465
tue 20 nov 2012, 16.48.31, CET
CONNECTED(00000003)
[omiss]
220 frontout-test1.sicurezzapostale.it ESMTP Postfix
```

- Al completamento del riavvio, il servizio Keepalived si riattiva ed entra in Backup State.

```
[root@accessopec-test1 ~]# less /var/log/messages|grep "Keepalive"
Nov  20 16:48:54 accessopec-test1 Keepalived[1408]: Starting Keepalived
v1.2.7
Nov  20 16:48:54 accessopec-test1 Keepalived_vrrp[1412]:
VRRP_Instance(VI_1) Entering BACKUP STATE
Nov  20 16:48:54 accessopec-test1 Keepalived_vrrp[1412]:
VRRP_Instance(VI_GATEWAY) Entering BACKUP STATE
```

Simulando ora un problema all'interfaccia di rete di AccessoPEC1

(tramite lo spegnimento dell'interfaccia eth0) il servizio Keepalived resta attivo ma passa in Fault State in quanto non è più raggiungibile dalla rete. I servizi continuano ad essere accessibili da Internet, il che significa che AccessoPEC2 continua ad operare in stato master. Alla riattivazione dell'interfaccia eth0 su AccessoPEC1, il servizio Keepalived ritorna in stato slave (Backup State).

- Verifica raggiungibilità AccessoPEC 1

```
[root@accessopec-test2 ~]# date && ping -c 5 192.168.255.3
Tue Nov  20 16:54:45 CET 2012
PING 192.168.255.3 (192.168.255.3) 56(84) bytes of data.
64 bytes from 192.168.255.3: icmp_seq=1 ttl=64 time=0.486 ms
64 bytes from 192.168.255.3: icmp_seq=2 ttl=64 time=0.507 ms
64 bytes from 192.168.255.3: icmp_seq=3 ttl=64 time=0.533 ms
64 bytes from 192.168.255.3: icmp_seq=4 ttl=64 time=0.515 ms
64 bytes from 192.168.255.3: icmp_seq=5 ttl=64 time=0.595 ms

--- 192.168.255.3 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4001ms
rtt min/avg/max/mdev = 0.486/0.527/0.595/0.039 ms
```

- Spegnimento dell'interfaccia eth0 su AccessoPEC 1

```
[root@accessopec-test1 ~]# date && ifdown eth0
Tue Nov  20 16:55:01 CET 2012
[root@accessopec-test1 ~]#
```

- Verifica cambio di stato del servizio Keepalived in Fault State

```
[root@accessopec-test1 ~]# less /var/log/messages|grep "Keepalived"
Nov  20 16:55:01 accessopec-test1 Keepalived_vrrp[1412]: Kernel is
reporting: interface eth0 DOWN
Nov  20 16:55:01 accessopec-test1 Keepalived_vrrp[1412]:
VRRP_Instance(VI_1) Now in FAULT state
```

- Verifica raggiungibilità di AccessoPEC1

```
[root@accessopec-test2 ~]# date && ping -c 5 192.168.255.3
Tue Nov  20 16:55:45 CET 2012
PING 192.168.255.3 (192.168.255.3) 56(84) bytes of data.

--- 192.168.255.4 ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 13999ms
```

- Verifica connettività (uno tra i servizi PEC esportati)

```
[root@alfacentos ~]# date && openssl s_client -connect test-
```

```
smtps.sicurezzapostale.it:465
tue 20 nov 2012, 16.56.15, CET
CONNECTED(00000003)
[omiss]
220 frontout-test1.sicurezzapostale.it ESMTP Postfix
```

- Riattivazione interfaccia eth0 su AccessoPEC1

```
[root@accessopec-test1 ~]# date && ifup eth0
Tue Nov  20 16:58:51 CET 2012
[root@accessopec-test1 ~]#
```

- Verifica cambio di stato del servizio Keepalived in Backup State

```
[root@accessopec-test1 ~]# less /var/log/messages|grep "Keepalived"
Nov  20 16:58:51 accessopec-test1 Keepalived_vrrp[1412]:
VRRP_Instance(VI_GATEWAY) Entering BACKUP STATE
Nov  20 16:58:51 accessopec-test1 Keepalived_vrrp[1412]:
VRRP_Instance(VI_1) Entering BACKUP STATE
```

- Verifica raggiungibilità di AccessoPEC 1

```
[root@accessopec-test2 ~]# date && ping -c 5 192.168.255.3
Tue Nov  20 16:59:47 CET 2012
PING 192.168.255.3 (192.168.255.3) 56(84) bytes of data.
64 bytes from 192.168.255.3: icmp_seq=1 ttl=64 time=1.44 ms
64 bytes from 192.168.255.3: icmp_seq=2 ttl=64 time=0.601 ms
64 bytes from 192.168.255.3: icmp_seq=3 ttl=64 time=0.564 ms
64 bytes from 192.168.255.3: icmp_seq=4 ttl=64 time=0.525 ms
64 bytes from 192.168.255.3: icmp_seq=5 ttl=64 time=0.474 ms

--- 192.168.255.3 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4002ms
rtt min/avg/max/mdev = 0.474/0.721/1.442/0.363 ms
```

CONCLUSIONI

Nel presente lavoro si è analizzata un'infrastruttura per l'accesso ai servizi di Posta Elettronica Certificata predisposta dal gestore Namirial S.p.A. al fine di verificarne la capacità di tollerare malfunzionamenti che possono portare ad un fallimento ed alla inaccessibilità dei servizi.
Una soluzione ideale e totalmente tollerante ai guasti è stata confrontata con l'effettiva infrastruttura di Namirial, mettendo in evidenza alcune differenze dovute agli accordi sulle garanzie dei livelli di servizio stabiliti tra il gestore e il provider dei servizi di connettività.
L'infrastruttura presa in esame non è l'unica soluzione possibile e attuabile per quanto riguarda l'erogazione di servizi che richiedono elevati livelli di disponibilità e di servizio.
Nel primo capitolo infatti, sono state introdotti diversi scenari applicativi che realizzano l'erogazione dei servizi tolleranti ai guasti.
Gli sviluppi futuri, da questo punto di vista, possono essere ad esempio: l'analisi delle problematiche legate all'uso del cloud computing per la fornitura del servizio di PEC, o ancora la realizzazione degli stessi servizi utilizzando una soluzione basata sul cluster oppure rapportare i vantaggi ottenuti dall'uso di ambienti virtuali con la normativa vigente in materia di firma digitale e gli obblighi richiesti.
Le soluzioni possono essere molteplici ma i fattori determinanti la scelta restano comunque gli investimenti che si hanno a disposizione, i ruoli e le responsabilità che la normativa vigente impone ai soggetti "in gioco".

Tuttavia le scelte di ridondare i dispositivi hardware e la realizzazione di configurazioni Master/Slave mediante software open source, sono risultate, anche nel caso dell'erogazione di un servizio come quello della Posta Elettronica Certificata, ancora una volta vincenti in quanto rappresentano un buon compromesso tra tolleranza ai guasti e costi di realizzazione dell'infrastruttura.

BIBLIOGRAFIA

[1] Piuri V., “La tolleranza ai guasti”, http://www.dti.unimi.it/piuri/pages/didattica/SO/mat/ftwebbook

[2] Tanenbaum A.S., Steen M.V., Distributed Systems: Principles and Paradigms, Prentice Hall PTR, 2001.

[3] Cuyvers R., User-Adaptable Fault Tolerance for Message Passing Multiprocessors., Doctoral Dissertation, KatholiekeUniversiteit Leuven ESAT/ACCA, Belgium, 1995.

[4] Coulouris G., DollimoreJ., KindbergT., Distributed Systems - Concepts and Design, Second Edition,Addison-Wesley, 1994.

[5] DenningP., Fault Tolerant Operating Systems, Surveys vol. 8, ACM-Computing n. 4, 1976.

[6] PradhanD., Fault tolerant computing: theory and techniques, Prentice-Hall, 1986.

[7] Corno F., Rebaudengo M., SonzaReorda M., “Le Tecniche di Ridondanza”, 2002, http://www.cad.polito.it/~sonza/02goe/lucidi/aa2005-06/ridondanza.pdf

[8] Patterson D.A., Gibson G., Katz R.H., A Case for Redundant Arrays of Inexpensive Disks (RAID), University of California, Berkeley, 1988.

[9] Buyya R.,High Performance Cluster Computing: Architectures and Systems, Volume 1,NJ, USA, Prentice Hall, 1999.

[10] Robertson A., “The Evolution of The LinuxHAProject”, http://linux-ha.com/_cache/TechnicalPapers__HBevolution.pdf

[11] “Load Balancing”, http://kb.linuxvirtualserver.org/wiki/Load_balancing

[12] IEEE Std 802.1AX-2008, “IEEE Standard for Local and Metropolitan Area Networks — Link Aggregation”, Capitolo 5.4, http://standards.ieee.org/getieee802/download/802.1AX-2008.pdf

[13] keepalived.org, “KeepAlived, Load Balancing & High Availability”, www.keepalived.org

[14] Institute of Electrical and Electronics Engineers (IEEE), "A View Inside the Cloud", 2012, http://theinstitute.ieee.org/technology-focus/technology-topic/a-view-inside-the-cloud

[15] Alberti F., “Verifica parametrica di protocolli Fault-Tolerant”, Università degli Studi di Milano, 2009.

[16] Pfister G., In Search of Clusters, 2nd edition, Prentice Hall, 1998

[17] Wikipedia, “Cloud Computing”, 2012, http://it.wikipedia.org/wiki/Cloud_computing

[18] saggiamente.com, “Le nuvole non sono più in cielo: i nostri dati li vediamo solo noi?”, 2011, http://www.saggiamente.com/2011/07/07/le-nuvole-non-sono-in-cielo-i-nostri-dati-li-vediamo-solo-noi/

[19] Baraldi C., “Tecniche per lo sviluppo di sistemi software ad alta affidabilità”, 2011

[20] Wikipedia, “RAID”, 2012, http://it.wikipedia.org/wiki/RAID

[21] Wikipedia, “Computer Cluster”, 2012, http://it.wikipedia.org/wiki/Computer_cluster

[22] DigitPA, “Posta Elettronica Certificata”, 2012, http://www.digitpa.gov.it/pec

[23] Twt.it, “La normativa sulla posta Elettronica Certificata”, http://www.twt.it/soluzioni/business/servizi_e_applicazioni/pec/pec_normative.asp

[24] Crea E., “PEC. Cos’è e a cosa serve”, 2009, http://www.conquistedellavoro.it/cdl/it/Giurisprudenza/Consumatori/info-40614407.htm

[25] Centro Nazionale per l’Informatica nella Pubblica Amministrazione (CNIPA),Regole tecniche del servizio di trasmissione di documenti informatici mediante posta elettronica certificata, allegato al DM 2 novembre 2005, 2005.

[26] RFC 3501, “INTERNET MESSAGE ACCESS PROTOCOL - VERSION 4rev1”, 2003, http://tools.ietf.org/html/rfc3501

[27] RFC 1939, “Post Office Protocol - Version 3”, 1996, http://tools.ietf.org/html/rfc1939

[28] RFC 5321, “Simple Mail Transfer Protocol”, 2008, http://tools.ietf.org/html/rfc5321

[29] RFC 6101, “The Secure Sockets Layer (SSL) Protocol Version 3.0”, 2011, http://tools.ietf.org/html/rfc6101

[30] Autorità per l'Informatica nella Pubblica Amministrazione, Raiss G., “I livelli di servizio. Come definirli e controllarli nei contratti della P.A.”, 2002, http://www2.cnipa.gov.it/site/_contentfiles/01379900/1379958_I%20livelli%20di%20servizio.pdf