UNIVERSITÀ DEGLI STUDI DI PADOVA

DIPARTIMENTO DI INGEGNERIA DELL'INFORMAZIONE

CORSO DI LAUREA IN INGEGNERIA INFORMATICA

INFRASTRUTTURA TECNOLOGICA: VIRTUALIZZAZIONE, ALTA AFFIDABILITÀ ED OTTIMIZZAZIONE DI RETE

Laureando: Andrea Basso

Relatore: Prof. Marcello Dalpasso

Anno accademico: 2012/13

Prefazione

Lo scopo dell'elaborato è presentare in modo analitico ed imparziale procedure, metodi e mezzi software ed hardware, necessari per progettare ed implementare un'infrastruttura tecnologica aziendale virtualizzata.

In fase di analisi vengono soppesati attentamente pro e contro di questa nuova tecnologia ed esposti i principali problemi che si possono riscontrare prima, durante e dopo il processo di consolidamento.
Inoltre vengono affrontati in modo approfondito i temi dell'alta affidabilità e della continuità operativa, valutandone il ruolo critico all'interno di un'azienda e gli effettivi benefici che essi portano.

Vengono, infine, descritte alcune ottimizzazioni di rete necessarie per sfruttare al meglio la virtualizzazione all'interno del contesto aziendale.

L'esposizione teorica è seguita da un esempio che, attraverso interventi concreti, evidenzia ulteriormente i vantaggi della tecnologia presa in esame in questa tesi.

Indice

Elenco delle figure

1 Introduzione

A partire dagli anni ottanta, la possibilità di acquistare computer a prezzi sempre più competitivi e l' aumento di richiesta di servizi informatici necessari per soddisfare le esigenze di business, ha portato ad un costante incremento del numero di server utilizzati all'interno delle aziende.
Con il passare del tempo, un approccio di questo tipo causa l'aumento incontrollato della spesa necessaria per la gestione della struttura, uno spreco energetico e, nella maggior parte dei casi, inefficienza nello sfruttamento delle risorse di calcolo disponibili.
La soluzione per invertire la tendenza e rimediare alle problematiche sorte, è un processo di razionalizzazione e riorganizzazione delle risorse, che prende il nome di server consolidation (consolidamento di server), tema inequivocabilmente legato al concetto di virtualizzazione.

1.1 Che cos'è la virtualizzazione

Il concetto che accomuna tutte le tecniche di virtualizzazione è l'isolamento dell'hardware attraverso la creazione di una versione virtuale di una risorsa normalmente fornita fisicamente. Attraverso uno strato di middleware, detto "macchina virtuale", è possibile installare su un unico calcolatore diverse applicazioni, gestendole però virtualmente come se fossero montate su diversi computer.
La virtualizzazione crea un'interfaccia esterna, che nasconde tutta la parte sottostante e permette l'accesso concorrente alla stessa risorsa (il server fisico) da parte di più istanze che funzionano in contemporanea (le applicazioni installate), permettendo l'ottimizzazione delle risorse e la capacità di far fronte a esigenze specifiche.

1.1.1 Perché virtualizzare

Il vantaggio più ovvio consiste nel risparmio economico ottenuto riducendo il numero di calcolatori, come evidenziato nel paragrafo precedente. Dal punto di vista delle risorse fisiche, infatti, l'unica spesa aggiuntiva coincide con l'acquisto iniziale dei nuovi elaboratori (tipicamente più performanti e quindi più costosi) e delle strutture eventualmente necessarie. L'utilizzo ottimizzato delle risorse fisiche non è però l'unico vantaggio: virtualizzare una serie di server e gestirli all'interno dello stesso computer porta benefici anche dal punto di vista della manutenzione, della gestione dei guasti, della scalabilità e dell'amministrazione di sistema.

Di seguito alcuni esempi:

- Continuità di servizio: gestire i disservizi di una macchina virtualizzata risulta molto più agevole della rispettiva controparte fisica. Non è necessario acquistare hardware ridondante, in quanto la replicazione avviene a livello software, così come non è necessario eseguire downtime pianificati per attività di manutenzione sui nuovi server virtuali.

- Scalabilità: una struttura consolidata, nella quale le macchine virtuali possono essere spostate da un server all'altro, consente di adattare le risorse in modo dinamico al variare della richiesta di maggiore o minore capacità di calcolo. Questo permette di gestire ad un livello di granularità più fine le risorse da destinare ai singoli servizi, sfruttando intensivamente le caratteristiche dei calcolatori fisici.

- Ciclo di vita: una struttura virtuale permette di abbattere le spese di spedizione, montaggio e configurazione di un nuovo sistema. Inoltre la manutenzione hardware ordinaria è ridotta al minimo e vengono totalmente annullati i costi di dismissione e smaltimento dei calcolatori e dei relativi componenti. Il tutto si traduce in un risparmio non indifferente, soprattutto se si considerano gli attuali cicli di vita molto rapidi (nell'ordine dei 3-5 anni) al termine dei quali molti computer vengono sostituiti.

1.1.2 Perché non virtualizzare

Un consolidamento mal pianificato può portare a seri rischi dal punto di vista economico.
I casi più frequenti sono: sottodimensionamento dei nuovi server fisici, collocamento di un numero eccessivo di macchine virtuali sulla stessa macchina fisica, non previsione di eventuali picchi di richieste di risorse e mancanza di una strategia per far fronte a situazioni critiche.
Oltre ai problemi succitati, che sono imputabili alla gestione scorretta del processo, esiste comunque la possibilità di dover affrontare situazioni impreviste che possono provocare disagi.

- Proliferazione virtuale: analogamente alla proliferazione fisica, si eccede nella creazione di nuove macchine virtuali. Se ad esempio viene sviluppata una macchina virtuale per ogni servizio, gli effetti positivi del consolidamento tendono a svanire, in quanto le risorse utilizzate aumentano velocemente e la manutenzione inizia a diventare articolata per colpa dell'aumento della complessità logica dell'infrastruttura.

- Gestione situazioni critiche: in un'ottica di struttura consolidata, un disservizio grave su di un elaboratore che ospita decine e decine di applicazioni, provoca danni maggiori rispetto alla precedente soluzione fisica che ne gestiva sicuramente di meno. Quindi, per garantire un minimo di tolleranza ai guasti, è utile mantenere computer di riserva uguali per

caratteristiche a quelli che stanno erogando i servizi, pronti ad entrare in funzione per sostituire un'eventuale macchina fisica guasta. Chiaramente questo porta a duplicare l'investimento necessario per l'acquisto dell'hardware per il consolidamento, senza considerare che la sostituzione di componenti malfunzionanti ha un costo maggiore a causa della qualità dei pezzi.

- Problemi di licenze e di supporto: vi è la possibilità che alcuni dispositivi non siano virtualizzabili, oppure che un produttore di software non fornisca assistenza in caso di utilizzo su sistema virtualizzato. Inoltre possono insorgere problemi relativi all'uso di licenze e contratti con gli OEM. Può accadere, infatti, di aver precedentemente acquistato un certo numero di licenze con relativo servizio di assistenza e che, in seguito al processo di consolidamento, il numero di quelle effettivamente utilizzate sia minore. Non è detto che cancellando le licenze in eccesso si ottenga anche una riduzione del costo di assistenza, in quanto esso era stato inizialmente calcolato sul numero totale di licenze.

1.2 Cosa si intende per "Alta affidabilità"

L'alta affidabilità di un sistema complesso o di un semplice componente (server, servizio, applicazione, etc.) è la misura della probabilità che il sistema stesso o il componente considerato non si guasti in un determinato lasso di tempo.
Essa è costituita da un insieme di aspetti, quali:

- Tolleranza ai guasti (fault-tolerance): è la capacità di un sistema di non subire fallimenti o interruzioni di servizio, anche in presenza di guasti. Essa non garantisce l'immunità da tutti i possibili problemi, ma solo da quelli per cui è stata progettata un'adeguata protezione.

- Garanzia sui servizi erogati: i servizi devono continuare ad essere disponibili anche in caso di guasto ai server su cui girano.

- Sicurezza dei dati memorizzati: deve essere garantita l'integrità dei dati salvati sui supporti di memorizzazione di massa, anche in caso di rottura degli stessi.

1.2.1 Disaster recovery

Per Disaster Recovery si intende l'insieme di misure tecnologiche approntate per ripristinare sistemi, dati e infrastrutture necessarie all'erogazione di servizi di business per le imprese, a fronte di gravi emergenze che ne intacchino la regolare attività.
Le procedure applicative, il software di sistema ed i file che sono stati classificati e documentati come critici, devono essere ripristinati prioritariamente.
Allo stato attuale, la tecnologia offre la possibilità di realizzare varie soluzioni di continuità e Disaster Recovery, fino alla garanzia, di fatto, di un'erogazione continua dei servizi IT, necessaria per i sistemi (es. finanziari o di monitoraggio) definiti "mission critical".
In pratica, i sistemi e i dati considerati importanti vengono ridondati in un "sito secondario" o "sito di Disaster Recovery" per far sì che, in caso di disastro (terremoto, inondazione, attacco terroristico, ecc.) di entità tale da rendere inutilizzabili i sistemi informativi del sito primario, sia possibile ripristinare le attività sul sito secondario nel più breve tempo e con la minima perdita di dati possibile.
Chiaramente, quanto più stringenti saranno i livelli di continuità, tanto più alti saranno i costi di implementazione della soluzione.

1.2.2 Backup

Il termine backup, "copia di sicurezza" o "copia di riserva", indica la conservazione di materiale informativo su un qualunque supporto di memorizzazione fatta per prevenire la perdita totale dei dati archiviati nella memoria di massa dei computer, siano essi stazione di lavoro o server.
Per le aziende, una caratteristica importante del backup è che questa attività non vada a sovrapporsi con l'operatività quotidiana, caricando i sistemi informatici e rallentando i tempi di risposta agli utenti.
Per questo motivo vari sistemi di backup vengono pianificati per la notte, quando normalmente l'utenza non lavora.
La conservazione dei supporti di backup avviene generalmente in posizioni fisicamente distinte e separate dai sistemi in uso per evitare che, in caso di furto, incendio, alluvione o altro evento catastrofico, le copie vadano perse insieme agli originali.
Il ripristino dei dati copiati con l'operazione di backup è normalmente detto "restore".

2 Presentazione azienda

Sono venuto a conoscenza dell'azienda grazie a "STAGE-IT", un evento promosso dall'Università di Padova per dare la possibilità agli studenti di venire a contatto con più di quaranta aziende operanti nel settore IT (Information Technology) e di sostenere dei colloqui con queste.
Tra il 3 Settembre 2012 e il 31 Ottobre 2012 ho svolto un tirocinio universitario presso l'azienda Sanmarco Informatica di Grisignano di Zocco, Vicenza.

2.1 Panoramica sull'azienda

Sanmarco Informatica S.P.A. è una software house, partner ufficiale IBM da oltre 20 anni, con 250 collaboratori diretti ed un centro nazionale di ricerca e sviluppo software per il gestionale "Galileo". L' azienda sviluppa applicazioni gestionali, consulenza e assistenza tecnica e vanta oltre 2.000 clienti fra aziende manifatturiere di diversi settori e di varie dimensioni, molte delle quali hanno anche sedi estere. Sanmarco Inf., infatti, supporta i clienti nel processo di internazionalizzazione con il software in lingua e la specifica fiscalità in molti paesi esteri.
Con ben 5 sedi in tutta Italia, questa azienda è una delle più grosse del settore nel panorama italiano. Dispone di un centro sviluppo con più di 70 sviluppatori addetti al software gestionale "Galileo" con tutti i suoi moduli specifici e specializzanti.
Proprio grazie a queste ramificazioni, il prodotto principale dell'azienda spazia fra industrie di piccola dimensione e grandi multinazionali, servendo in modo efficiente settori molto diversificati.
Oltre a fornire consulenza e soluzioni gestionali approfondite, questa azienda dispone di esperti specializzati nella progettazione e realizzazione di infrastrutture tecnologiche efficienti, per supportare al meglio il cliente e renderlo più produttivo, efficiente e sicuro.

2.2 La sezione iTech

La sezione iTech è il punto di partenza di un qualsiasi progetto riguardante il prodotto dell'azienda: prima di installare il gestionale basato su AS400 di IBM, bisogna progettare, configurare ed installare l'infrastruttura che lo ospiterà.
I tecnici di questa sezione sono pochi e molto competenti; a loro spetta il primo sopralluogo dal cliente, l'analisi dei requisiti e delle risorse necessarie.
I progetti sono fatti ad hoc, portati alla massima efficienza con soluzioni di virtualizzazione, backup e disaster recovery all'avanguardia.
Le esperienze maturate negli ambiti delle tecnologie di virtualizzazione, dell'alta affidabilità dei sistemi critici, della business continuity e della distribuzione e sicurezza degli ambienti, sono aspetti di sicuro interesse nei progetti di server consolidation sia per piattaforme "i" e "x" series IBM, che per gli altri ambienti operativi.

3 Obiettivi del progetto

L'elaborato si pone come fine principale il consolidamento di server tramite architetture di virtualizzazione e l'ottimizzazione della rete utilizzata dal cliente.
La progettazione è da considerarsi attendibile se vengono mantenute o aumentate le performances, garantendo, nel contempo, alta affidabilità e continuità di lavoro nel rispetto del budget assegnato.

3.1 Consolidamento server

La procedura di consolidamento inizia con una dettagliata fase di analisi, nella quale ci si focalizza sulla scelta di quali macchine, fisiche o virtuali, debbano essere virtualizzate e consolidate sullo stesso computer.
A questo proposito si possono valutare diverse opzioni:

- Raggruppare per funzionalità: consolidare sulla stessa macchina i server che in qualche modo sono legati in quanto funzioni diverse di un unico sistema.

- Raggruppare per performance: consolidare sulla stessa macchina una serie di server che consentano di massimizzare l'utilizzo delle risorse.

- Consolidare su stessa macchina processi con carichi di lavoro temporalmente complementari: essi sono buoni candidati ad essere residenti sullo stesso server, in quanto occuperebbero le risorse in momenti diversi della giornata.

- Consolidare su stessa macchina processi con carichi di lavoro identici: raggruppando in un unico calcolatore le macchine che eseguono compiti simili, si può ottenere una specializzazione dello stesso con conseguente risparmio in termini di licenze software.

Una volta conclusa questa prima parte, il progettista dispone dei requisiti hardware necessari alla virtualizzazione e può dimensionare adeguatamente le nuove macchine fisiche.
Le realtà aziendali incontrate durante lo stage sono di piccola/media grandezza per cui, nella maggior parte dei casi, le macchine presenti presso il cliente vengono virtualizzate e ospitate su uno o al massimo due elaboratori fisici.
Si procede, quindi, alla migrazione vera e propria e alla predisposizione di sistemi di backup e disaster recovery per garantire l'alta affidabilità.

3.1.1 Da fisico a virtuale e da virtuale a virtuale

La migrazione di un sistema fisico verso un sistema virtuale (operazione spesso chiamata p2v migration) consiste nel trasportare ciò che prima veniva eseguito su computer fisico, in qualcosa che possa essere eseguito su macchina virtuale: occorre cioè effettuare una copia del sistema operativo, del contenuto dei dischi e delle

applicazioni installate ottenendo un file, normalmente chiamato "immagine del disco virtuale", che possa essere utilizzato dalla virtual machine.
In particolare si parla di:

- migrazione a caldo ("hot migration" o "hot cloning") se la copia del server fisico avviene mentre questo è ancora in funzione.
- migrazione a freddo ("cold migration" o "cold cloning") se la copia del server fisico avviene mentre questo è offline.

Nel primo caso si ha, ovviamente, il vantaggio di non creare disservizi al sistema, tranne che per un possibile calo di prestazioni dovuto alle risorse utilizzate per la copia stessa. Tuttavia è necessario gestire eventuali cambiamenti nel sistema originale mentre questo viene copiato (si pensi all'attività di un database), che possono dare origine ad incoerenze tra sorgente e destinazione.
Nel secondo caso invece il processo è più semplice, in quanto non esiste alcun problema di possibili incoerenze, ma è necessario mettere il sistema offline per tutta la durata della copia, con conseguenti disservizi ed eventuali perdite di produttività.

In caso di infrastruttura precedentemente o parzialmente virtualizzata, si procede con la migrazione "virtual to virtual". Se la virtualizzazione fosse implementata mantenendo il giusto livello di astrazione, sarebbe possibile semplicemente copiare l'immagine del disco virtuale interessato verso la nuova posizione. Ciò è vero solo in parte, dato che esistono modalità di virtualizzazione con livelli di astrazione diversi, i quali richiedono modifiche ai sistemi operativi ospitanti. Un tool che si occupi di v2v migration esegue, quindi, anche le operazioni necessarie per la rimozione del software relativo all'hypervisor in sostituzione.

3.1.2 Alta affidabilità e continuità operativa

La gestione della continuità operativa comprende tutte le iniziative rivolte a ridurre ad un livello ritenuto accettabile i danni conseguenti ad incidenti e catastrofi, che colpiscono direttamente o indirettamente un'azienda.
La normale operatività di un'impresa dipende dalla disponibilità delle risorse critiche, che sono funzionali all'erogazione dei processi di business. I servizi IT possono essere considerati come un sottoinsieme di queste risorse critiche e la protezione dei servizi è quindi condizione necessaria ma non sufficiente a garantire la continuità delle operazioni.
I dati critici vengono ridondati in un "sito secondario" in modo da poter attivare tutti i servizi e le funzionalità precedenti in caso di disservizio del sito primario.

Il sito remoto può essere ricondotto a una delle seguenti categorie, scelta in base alle esigenze dei processi di business e delle strategie di recovery.

- Siti freddi (cold sites), quelli in cui sono disponibili solo le infrastrutture di supporto, ma non sono disponibili né apparati né dati o software. L'attivazione di questi siti può richiedere anche alcune settimane.

- Siti tiepidi (warm sites), sono invece parzialmente attrezzati anche per quanto riguarda gli apparati. Generalmente mancano le strumentazioni più costose, nell'ipotesi di poterle procurare in tempi brevi, ad esempio in virtù di accordi con i fornitori. I dati possono essere disponibili sotto forma di backup, ma non immediatamente utilizzabili dai sistemi.

- Siti caldi (hot sites), sono infine quelli completamente attrezzati e che possono essere attivati anche in poche ore. Questo comporta non solo la disponibilità di apparati, ma anche di software aggiornato rispetto a quello del sito principale in termini di versioni e configurazioni.

Negli ultimi tempi, con la diffusione di tecnologie affidabili a larga banda e a costi sempre più contenuti, si sta infatti diffondendo l'uso di tecnologie di mirroring dei dati che mantengono presso il sito remoto una copia dei dati sostanzialmente allineata con quella del sito principale.

3.2 Ottimizzazione della rete

La riorganizzazione della rete può essere fatta prima o dopo il consolidamento: in entrambi i casi essa va riesaminata e modificata in base alle esigenze dei nuovi computer e dei sistemi virtualizzati. Il passaggio alla tecnologia virtuale può portare alla diminuzione di dispositivi di rete fisici, come ad esempio gli switch che vengono sostituiti dai corrispettivi virtuali, quindi al loro smaltimento o riutilizzo in altri ambiti. Inoltre, per mantenere alte performances e buon funzionamento dei sistemi di alta affidabilità, è necessario che i singoli client e i server possano comunicare velocemente fra di loro e con lo storage di rete. Infine vanno garantite la raggiungibilità delle risorse a disposizione, anche da sedi esterne, e la sicurezza delle macchine in uso.

3.2.1 Antivirus, firewall e antispam

Generalmente il fattore che sta più a cuore al cliente è la sicurezza dei dati e del network. Perciò il primo intervento, in ordine di tempo e di importanza, riguarda virus, accessi indesiderati e pubblicità (spam). Nel primo caso è fondamentale che ogni calcolatore disponga di un software di protezione adatto.
Le possibilità di installazione sono 2:
Antivirus completamente residente sui pc locali, oppure centralizzato su un server e distribuito in versione client sui vari computer utilizzatori.
Nel caso del firewall, invece, si ricorre ad un apparato hardware dedicato che impedisca accessi indesiderati, consenta il passaggio esclusivamente ai protocolli

utilizzati filtrandone il traffico e garantisca una separazione netta fra rete locale e rete esterna.
Infine l'antispam deve bloccare l'arrivo di posta indesiderata, che altrimenti andrebbe ad intasare le caselle di posta del cliente con mail potenzialmente pericolose e fuorvianti. In questo modo le uniche comunicazioni in arrivo sono quelle abilitate e la loro consultazione risulta più veloce, sicura ed efficiente, vista la mancanza di messaggi inutili.

3.2.2 Virtual Private Network

Una "Virtual Private Network" è una rete di comunicazione privata che estende una rete locale e collega varie sedi di una stessa azienda, sfruttando la rete pubblica per il trasporto su scala geografica.
Vengono utilizzati collegamenti detti "Tunnel", che necessitano di autenticazione in modo da garantire l'accesso ai soli utenti autorizzati. Inoltre per garantire la sicurezza che i dati inviati in Internet non siano intercettati o utilizzati da persone non autorizzate, le reti utilizzano sistemi di crittografia.
Dal punto di vista dell'utente ciò significa che, mentre la connessione VPN è attiva, tutti gli accessi esterni devono passare per lo stesso firewall, come se il computer fosse fisicamente connesso all'interno della rete sicura. Questo riduce il rischio che altri possano accedere alla rete privata dell'azienda.
Una VPN ben strutturata può, quindi, offrire grandi benefici per un'azienda:

- Estende la connettività geografica e la disponibilità di risorse.
- Migliora la sicurezza dove le linee di dati non sono state criptate.
- Riduce il tempo di transito e i costi di trasporto per i clienti remoti.
- Semplifica la topologia e il supporto di rete.

3.2.3 Bilanciamento di carico e traffic shaping

Il bilanciamento di carico permette di segmentare le richieste di accesso ad un servizio applicativo specifico in modo da condividerlo su più server, ottenendo quindi una razionalizzazione delle risorse disponibili, evitando congestionamenti e garantendo l'alta disponibilità del servizio stesso.
Applicando diverse strategie, il bilanciamento agisce come front-end nei confronti dei server bilanciati, interpreta le connessioni di richiesta dei client e le distribuisce in modo equilibrato tra i vari computer disponibili.
Ne derivano diversi benefici:

- Incremento dell' efficienza nell´ utilizzazione dei server e della banda.
- Miglioramento dell' Alta Affidabilità del servizio.
- Aumento della Scalabilità.

La tecnica del traffic shaping consiste nel forzare il traffico di rete ad essere conforme ad un determinato comportamento, o seguire forzatamente un certo numero di policies create per modellarne le caratteristiche. I principali vantaggi dovuti al suo utilizzo sono:

- Divisione del traffico in diverse tipologie di classi per dare maggiore priorità a determinati servizi, senza congestionare i server o il gateway.
- Limitazione e/o abbattimento drastico del traffico indesiderato (P2P).
- Gestione ottimizzata della banda a disposizione, per evitare picchi di traffico che porterebbero a congestione e rallentamenti durante l'utilizzo.

4 Tecniche e strumenti

Il consolidamento di un'infrastruttura è un processo complesso e generalmente dispendioso in termini di tempo e competenze, perciò è fondamentale pianificare il tutto nei minimi dettagli.
L' analisi di costi e benefici insieme all'azienda fa emergere i 3 requisiti fondamentali del progetto: obiettivi da raggiungere, tempistiche da rispettare e budget a disposizione.
Questi aspetti portano i tecnici coinvolti a fare delle scelte mirate in termini di hardware, software e metodi di lavoro, così da poter descrivere ogni intervento previsto nel modo più preciso e trasparente possibile agli occhi del cliente.

4.1 Analisi preventiva

Il punto di partenza è definire gli obiettivi che si vogliono raggiungere, valutando in primis, i limiti imposti dall'infrastruttura o dal cliente:

- Limiti strutturali: come il termine di spazio fisico nei server o il raggiungimento del limite di risorse elettriche disponibili. Si noti che in alcuni casi effettuare un ulteriore upgrade delle strutture fisiche, quali l'impianto elettrico, risulterebbe in una spesa difficilmente sostenibile.

- Limiti economici: quando ad esempio il budget limitato impedisce di acquistare hardware dedicato per la copertura di nuovi progetti e per la loro gestione.

- Limiti operativi o tecnologici: se il funzionamento stesso dell'infrastruttura o la sua connettività esterna (ADSL) pone limiti alla possibilità di ottenere nuove funzionalità e profitti.

- Limiti temporali: il progetto deve avere il minimo impatto sulla produttività dell'azienda perciò, quando possibile, gli interventi devono essere svolti fuori orario d'ufficio. Inoltre la realizzazione della nuova rete operativa deve avvenire in tempi brevi, per evitare strascichi e perdite di tempo da parte del cliente.

4.1.1 Carichi di lavoro e raccolta dati

Le scelte di consolidamento vengono fatte in seguito all'analisi dei workload, ossia del carico di lavoro a cui ogni servizio è sottoposto. Per ricavare queste e altre informazioni è necessaria una fase di analisi dei server che può essere condotta con adeguati software di controllo.
Il software di monitoraggio consente di visionare lo stato delle macchine e la quantità di risorse che esse stanno utilizzando, attività che senza strumenti automatici può

rivelarsi particolarmente gravosa se si lavora con un parco macchine di ampie dimensioni.
Questi programmi permettono, ad esempio, di definire metriche personalizzate e di ricavarne i grafici corrispondenti. Monitorando il cambiamento nel tempo di metriche personalizzate e metriche classiche, quali ad esempio consumo di CPU, RAM in uso e quantità di operazioni di rete, si ricavano molte informazioni utili per le scelte di consolidamento.
Al termine dell'attività di controllo si è in grado di costruire uno schema con tutte le macchine attualmente disponibili, elencando per ognuna le caratteristiche tecniche e le informazioni sul numero di applicazioni e servizi attivi.

4.1.2 Approcci possibili

Una volta che si conoscono i carichi di lavoro e le potenzialità dell'attuale struttura aziendale, si deve valutare il miglior approccio per il progetto.
Le possibilità sono due: aggiornare l'attuale infrastruttura oppure smantellarla e riprogettarla completamente.
Per rimediare alla proliferazione di server, in modo da poter continuare a realizzare nuovi progetti senza superare i limiti di budget, recuperare spazio fisico e risparmiare in energia elettrica, è sufficiente adottare una soluzione di contenimento: questo consente di ottenere ottimi risultati senza dover stravolgere completamente l'infrastruttura informatica. Se tutti i nuovi progetti vengono gestiti su macchine virtuali, si ferma la crescita del numero di server e soprattutto si rimanda la spesa necessaria per l'acquisto di hardware.
Anche nel caso in cui non si possano riutilizzare server già acquistati per gestire le macchine virtuali e si debba acquistarne di nuovi, il costo viene recuperato piuttosto rapidamente grazie al risparmio in costi di gestione. L'isolamento e la portabilità che una macchina virtuale garantisce consentono, inoltre, di amministrare più facilmente il software in fase di sviluppo: lo si può testare su sistemi operativi diversi con tempi di provisioning nell'ordine dei minuti, evitando che eventuali malfunzionamenti danneggino il resto del sistema.
Specularmente, si può agire per trasferire le applicazioni legacy all'interno di macchine virtuali su server recenti: questo consente di ritirare l'hardware obsoleto che veniva mantenuto soltanto per poter far girare applicazioni di quel tipo.

Se si desidera invece consolidare l'intera struttura è necessario un approccio più ragionato, soprattutto se si parla di un'organizzazione con centinaia di macchine.
E' buona norma identificarne un piccolo sottoinsieme "prototipo", il più possibile simile all'infrastruttura nel suo complesso, per eseguire un "consolidamento pilota" su di esso. In questo modo si ha la possibilità di sperimentare su piccola scala parte dei problemi che verosimilmente si dovranno affrontare in strutture più grandi, permettendo nel contempo di ottenere i primi risultati tangibili, che possono anche essere sfruttati per pubblicizzare e promuovere un intervento su larga scala.

4.2 Le macchine fisiche

Una volta conclusa l'analisi e concordato con il cliente l'approccio che si vuole adottare per il consolidamento, si passa alla scelta dell'hardware che andrà a sostenere la nuova infrastruttura virtualizzata.
Si devono valutare gli spazi, la connettività e la rete elettrica a disposizione, in modo da raggiungere gli obiettivi prefissati con il minimo impatto sull'infrastruttura aziendale già presente. Inoltre si deve garantire il corretto funzionamento dei servers predisponendo impianti di raffreddamento adeguati e gruppi di continuità.

4.2.1 Server tower

Montata in un cabinet simile a quello dei personal computer, questo tipo di macchina presenta affidabilità e prestazioni superiori ad un normale pc ad uso privato, essendo il suo hardware specificatamente progettato per l'utilizzo aziendale.
Visti i costi contenuti in termini di spazio e consumi, questa soluzione è preferibile all'interno di piccole infrastrutture con bassi carichi di lavoro.

I principali vantaggi sono:

- Raffreddamento: vista la bassa densità di componenti elettriche al suo interno, la dissipazione del calore è meno articolata e più efficiente delle altre soluzioni server.
- Scalabilità ed installazione: non necessitando di strutture particolari come il rack, il tower dà la possibilità di aggiungere altri elaboratori in una stessa rete aziendale senza dover effettuare lavori strutturali.

Tuttavia utilizzare elaboratori singoli ha degli evidenti svantaggi:

- Un insieme di server tower è molto più pesante ed ingombrante del corrispettivo in rack.
- Il cablaggio di un gruppo cospicuo di tower può risultare complesso a livello logistico ed economicamente dispendioso.
- Un gruppo di calcolatori singoli può essere molto rumoroso se raffreddato ad aria, poiché ciascun elaboratore presenta almeno una ventola dedicata.

Un esempio di server tower è il System x3500 M4 dell'IBM, che può montare due processori Intel Xeon E5-2690, per un totale di 16 core fisici (8 per processore) a 2.9 Ghz, 768 GB di memoria RAM DDR3 a 1600 Mhz, una scheda di rete con 4 porte Ethernet Gbit ed un massimo di 32 TB di storage interno SAS/SATA con rimozione "in corsa". Supporta la ridondanza a caldo di massimo 2 alimentatori e integra a livello hardware tutti i RAID disponibili attualmente, sia a 3GBps che 6GBps.

4.2.2 Server in rack

Con il termine rack si indica un sistema standard d'installazione di componenti hardware, costituito da una struttura modulare larga 19 pollici (482,6 mm) e alta 1,75 pollici (44,45 mm) per ogni unità ospitata.
Generalmente si preferisce non riempirlo del tutto, lasciando spazio tra un componente rack e l'altro, in modo da permettere una migliore circolazione d' aria per il raffreddamento e una più semplice gestione dei collegamenti, evitando confusione e sovraffollamento. Ogni armadio, inoltre, possiede un dispositivo meccanico di chiusura, per impedire l'intrusione da parte di terzi.
L'accesso dalla parte frontale consente di agire sui comandi fisici del server collegando eventualmente un monitor e una tastiera, mentre quello dalla parte posteriore permette di agire sui vari collegamenti (alimentazione, rete, ecc.).
I server poggiano su delle slitte in metallo, che possono scorrere per estrarre in maniera semplice ogni componente presente.

La prassi consolidata di buon approntamento di un armadio rack implica la presenza di alimentazione costante e di una temperatura preferibilmente attorno ai 20 °C, per permettere un corretto funzionamento dei componenti elettronici. Per questo motivo, spesso negli armadi si trovano gruppi di continuità e ventole disposti anch'essi su supporti rack. Questo tipo di struttura, quindi, semplifica il cablaggio e riduce al minimo l'ingombro delle macchine.
Tuttavia la riduzione dello spazio occupato porta ad un aumento della densità delle componenti elettriche, la quale a sua volta necessita di un sistema di condizionamento esterno appositamente posizionato.
La maggior complessità elettronica ed il raffreddamento dedicato rendono questa soluzione più adatta ad aziende con carichi di lavoro medio/alti, dove i costi dovuti all' installazione e il mantenimento di un rack sono superati dai benefici derivanti dalla maggiore efficienza e potenza di calcolo.

Un tipico esempio di server rack è il System x3750 M4 dell'IBM il quale può montare al massimo 4 processori Intel Xeon E5-4650, per un totale di 32 core fisici (8 per processore) a 2.7 Ghz, 1.5 TB di memoria RAM DDR3 a 1600 Mhz, scheda di rete interna con 2 porte Ethernet Gbit e 2 10 Gbit ed un massimo di 16 TB di storage interno SAS/SATA con rimozione "in corsa". Supporta la ridondanza a caldo degli alimentatori e integra a livello hardware i RAID 0,1,5,610,50,60 a 3GBps o 6GBps.

4.2.3 Server blade

Un blade server è un sistema auto-contenuto, pensato per minimizzare l'occupazione di spazio. Uno chassis per blade, che può contenere molteplici elaboratori, fornisce servizi come l'alimentazione, il raffreddamento, la rete, varia connettività e possibilità di gestione, anche se i produttori differiscono per cosa includono o non includono nelle macchine e nello chassis.
Una singola lama (dall' inglese "blade" = "lama") costituisce una macchina fisica distinta che, da sola o in concorso con altre, può simulare N macchine virtuali.

L'armadio più comune può contenere un massimo di 42 computer, mentre nel caso di blade si riescono a raggiungere densità sino a 128 macchine per rack, numero destinato ad aumentare nei prossimi anni.
Essendo un rack di rack, all'interno dello chassis le lame sono montate in verticale.

Attualmente questa soluzione server è quella con la densità elettronica e la potenza di calcolo maggiori tra quelle commercialmente disponibili.
Negli anni passati questo tipo di sistema era tipicamente adottato dai data center di grandi organizzazioni (aziende o enti pubblici), mentre recentemente è utilizzato anche per infrastrutture più contenute.

I vantaggi e gli svantaggi dei blade sono gli stessi dei rack normali, portati a livelli estremi: massime prestazioni, minimo ingombro, minimo cablaggio, necessità di un raffreddamento dedicato molto efficiente e consumi e rumorosità discreti.
Inoltre questo tipo di server presenta una particolare limitazione non presente nei rack normali: la compatibilità hardware.
Non c'è uno standard internazionale che regoli progettazione e costruzione dei blade perciò quando si va ad ampliare il sistema, si devono necessariamente acquistare moduli prodotti dallo stesso costruttore.

Un esempio di chassis blade è il Blade Center H di IBM che ha 14 comparti blade, 4 alimentatori ridondati con estrazione "a caldo" e 2 ventilatori.
Al suo interno possiamo alloggiare fino a 14 lame BladeCenter HS23 con massimo 2 processori Intel Xeon E5-2690, per un totale di 16 core fisici (8 per processore) a 2.9 Ghz, 256 GB di memoria RAM DDR3 a 1600 Mhz, scheda di rete interna con 2 porte Ethernet 10 Gbit ed un massimo di 2 TB di storage interno SAS/SATA. Supporta la ridondanza a caldo degli alimentatori e integra a livello hardware i RAID 0,1 a 3GBps o 6GBps.

4.3 Metodi per virtualizzare

La virtualizzazione dei server si basa sul concetto di hypervisor, o Virtual Machine Monitor (VMM) che è lo strato software che soddisfa i bisogni di CPU, memoria e periferiche del sistema ospite.
Ci sono due tipi di virtualizzazione:

- Tipo 1: nativo o Bare-Metal;
- Tipo 2: Hosted.

Un hypervisor di tipo 2 viene installato ed eseguito come applicazione su un sistema operativo host (si parla di hosted virtualization).
Era il più diffuso agli albori della virtualizzazione in quanto gli amministratori potevano acquistarlo e installarlo sui server già in loro possesso.
In questa architettura, le macchine virtuali in esecuzione comunicano con l'hypervisor, che è installato direttamente sul sistema operativo base: le risorse hardware sono sotto il pieno controllo di questo sistema operativo e solo esso può gestirle.

Il sistema operativo guest crede di avere pieno controllo delle risorse e se la CPU fisica supporta la virtualizzazione, la maggior parte delle istruzioni viene eseguita direttamente da esso. Se le istruzioni non possono essere eseguite dal sistema ospite, queste passano al sistema operativo base tramite l'hypervisor e sono schedulate secondo le risorse disponibili.
Un fattore importante per il sistema guest è l'overhead proveniente da sistema operativo host e hypervisor: la loro presenza potrebbe influire sulle prestazioni del sistema ospite.
Un esempio di hypervisor virtualization è Vmware Server oppure, in ambito desktop, Vmware workstation.

Un hypervisor di Tipo 1 o Bare Metal (metallo nudo) installa lo strato di virtualizzazione direttamente sull'hardware della macchina. Con questo sistema l'hypervisor ha il controllo di tutte le risorse e quando queste sono concesse alle VM, viene fatto in maniera virtuale: l'hypervisor condivide le varie risorse alle macchine virtuali che credono di averne accesso fisico.
In questo caso si parla di virtualizzazione nativa ed esempi di questo tipo sono Vmware ESXi, Microsoft Hyper-V e Citrix Xenserver.

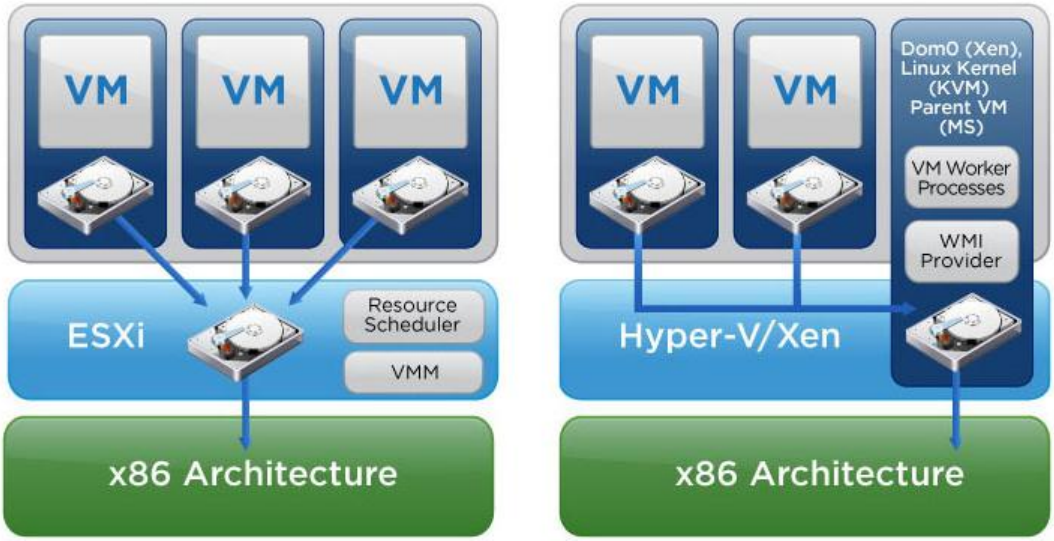

Figura 4.1 Hypervisor a confronto

Si può dedurre facilmente che la virtualizzazione nativa, rispetto alla hosted virtualization, garantisce prestazioni superiori e maggiore affidabilità avendo un controllo diretto dell'hardware, senza dover passare per un sistema operativo host, evitando così eventuali crash di sistema. Inoltre, la virtualizzazione di Tipo 1 si dimostra più flessibile e scalabile. Per questi motivi in ambito aziendale vengono utilizzate solo virtualizzazioni native e le più usate sono descritte di seguito.

4.3.1 Vmware ESXi

Vmware ESXi, precedentemente conosciuto come ESX, è l'hypervisor nativo più diffuso al mondo ed è suddiviso in due componenti: Virtual Machine Monitor e vmkernel. Il vmkernel è il cuore del sistema e gestisce le principali funzioni del sistema di virtualizzazione come la pianificazione della CPU (scheduling), la gestione della memoria e l' elaborazione dei dati provenienti dai virtual switch.
Ogni macchina virtuale viene gestita da un Virtual Machine Monitor separato situato all'interno dell'hypervisor, che ne soddisfa le richieste di CPU, memoria e I/O.
ESXi fornisce la possibilità di gestire e limitare la quantità di CPU e RAM da assegnare alle macchine virtuali ospitate al loro interno attraverso l'utilizzo di avanzati meccanismi quali:

- Reservation: per riservare un quantitativo minimo di risorse senza le quali una macchina virtuale non si accenderebbe. Nel caso della RAM questa deve essere fisicamente presente e non può essere fornita da swap su disco.
- Limit: per limitare l'utilizzo di risorse. Questa opzione può essere utilizzata per creare una macchina virtuale con 8 GB di RAM per poi limitarla al solo utilizzo di 512 MB. Questo accade quando un macchina viene assegnata a compiti diversi da quelli per la quale era stata progettata. In questo modo le risorse massime utilizzabili possono essere riassegnate "in corsa".
- Share: descrive con un numero la priorità di una macchina rispetto alle altre di accedere alle risorse.

Si supponga di avere due macchine virtuali impostate con 512 MB di RAM riservata, 1 GB di RAM limite e 1 come valore di Share. Se la macchina ESX possedesse 1,5 GB di RAM fisica, ne allocherebbe 1 GB, 512 MB per VM, come imposto dal parametro Reservation, mentre i restanti 512 MB di RAM disponibili verrebbero distribuiti equamente, visto che entrambe le macchine hanno Share impostato a 1.
Se invece il parametro Share fosse impostato a 2 per una macchina e ad 1 per l'altra, avremmo che la macchina con Share più elevato riceverebbe il 66% della RAM disponibile, mentre l'altra solamente il 33%.

I meccanismi su scritti possono essere sfruttati sia per la CPU che per la RAM, anche se quest'ultima ne possiede altri più avanzati.
Il più interessante è il Memory Overcommitment, ovvero la possibilità da parte di ESXi di fornire più memoria di quanta fisicamente installata sulla macchina server. Questo rende possibile avviare due macchine virtuali con 8 GB di RAM su una macchina server con solamente 4 GB di RAM fisica.
L'hypervisor coprirà le necessità delle 2 macchine fornendo la memoria fisica disponibile fino al suo esaurimento, dopodiché ricorrerà allo swap su disco.

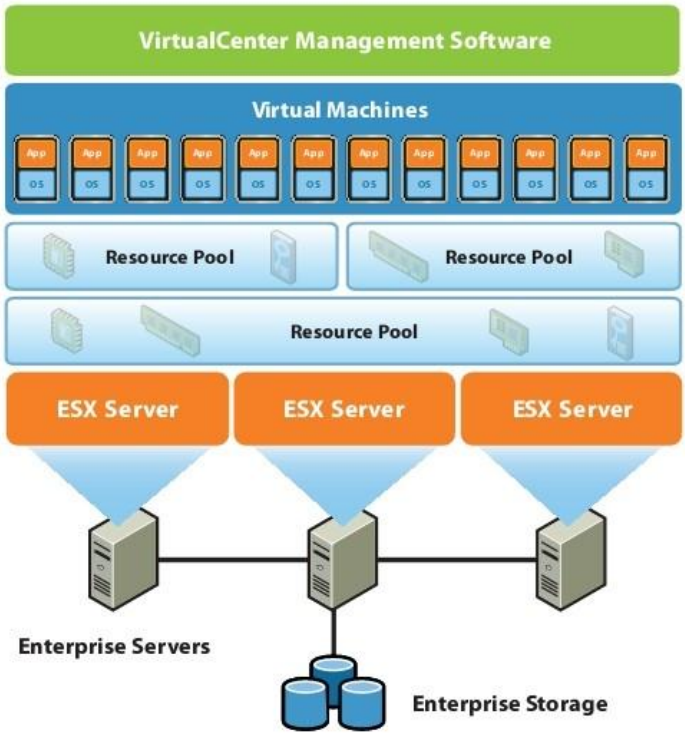

Figura 4.2 La virtualizzazione secondo Vmware

Su un host ESXi è possibile accedere attraverso diverse interfacce:

- vSphere Client connesso direttamente all'host o al VCenter Server
- vSphere Command-Line Interface vCLI
- vSphere API/SDK
- Common Information Model (CIM)

ESXi ha il pieno supporto per le architetture dei processori Intel, Xeon e superiori, o AMD Opteron e comprende un VMkernel a 64 bit con il quale è possibile eseguire sistemi operativi virtualizzati sia a 32 bit che 64 bit.
Nel campo della gestione delle Virtual Machine vi è l'applicativo vCenter, con il quale è possibile gestire in maniera centralizzata tanti aspetti relativi all'infrastruttura VMWare tra i quali:

- Monitorare attraverso grafici l'utilizzo delle risorse (come CPU, disco, memoria) delle varie macchine virtuali e dei server ESXi.
- Pianificare operazioni in determinati momenti della giornata.
- Allertare gli amministratori in caso si verifichino situazioni anomale che si vogliono gestire.
- Aggiungere rapidamente altre Macchine Virtuali rispetto a quelle già esistenti, specificando il template da utilizzare, ossia la struttura standard che si intende dare al Sistema Operativo da virtualizzare e quali programmi eseguire durante la sua esecuzione.

Per quanto riguarda la compatibilità con i Server in commercio, vSphere supporta tutte le componenti di ultima generazione.
Non è necessario installare alcun driver poichè sono incorporati nel sistema stesso.

4.3.2 Microsoft Hyper-V

Nel campo del VDI Microsoft ha sviluppato il prodotto Hyper-V, formalmente conosciuto come Windows Server Virtualization. E' un sistema di virtualizzazione basato su hypervisor per sistemi Windows Server 2008 e 2012 ed è giunto alla seconda release. Hyper-V viene concesso in forma gratuita ai possessori dell'ultima versione di Windows Server ed è disponibile solo per processori con architettura a 64 bit. Le politiche attuate da Microsoft limitano l'esecuzione delle VM in base alle diverse licenze presenti sul mercato, nello specifico abbiamo:

- Standard Edition: consente di eseguire una macchina virtuale per ogni licenza;
- Enterprise Edition: permette di utilizzare fino a quattro macchine virtuali;
- Datacenter Edition: concede l'uso di un numero illimitato di macchine virtuali e le licenze vengono rilasciate per processore fisico utilizzato e non perciò per ogni core dello stesso.

L'obiettivo alla base dell'architettura di Hyper-V, è quello di dividere la memoria fisica dei Server in unità logiche isolate tra loro, in modo da permettere l'esecuzione dei Sistemi Operativi guest posti al loro interno.
L'esecuzione dell'Hypervisor avviene in una partizione principale (chiamata root partition) in cui viene eseguito il Sistema Operativo host (nel nostro caso Windows Server 2008/2012). Solo in seguito vengono create le partizioni figlie che conterranno i Sistemi Operativi guest. A loro volta le partizioni figlie (child partition) possono generare altre partizioni, sfruttando le API-Hypercall che si interfacciano direttamente con Hyper-V.
Una partizione virtualizzata non ha accesso diretto al processore fisico e, di conseguenza, non interagisce direttamente con le periferiche fisiche esterne.
Tutte le partizioni figlie gestiscono risorse virtuali le cui richieste vengono redirezionate dal proprio Virtualization Service Consumer, tramite il VMBus, al Virtualization Service Provider in ascolto nella partizione genitore. Il ciclo si ripete fino a raggiungere la root partition, dove si avrà effettivamente accesso alla risorsa fisica. Il processo, per tutta la sua durata, rimane nascosto al sistema operativo guest al quale vengono comunque fornite le risorse di cui esso necessita per la sua esecuzione. Un altro aspetto importante da considerare nella tecnologia Hyper-V, è la presenza della funzionalità Enlightned I/O che rappresenta un'implementazione di protocolli di alto livello sviluppati appositamente per sistemi virtualizzati.
Questi protocolli sfruttano direttamente il VMBus rendendo la comunicazione più efficiente ed evitando l'uso di emulazione. Tuttavia per poterla utilizzare il sistema operativo guest deve supportare Enlightened I/O.
La gestione delle Virtual Machine può avvenire tramite l'utilizzo del Remote Desktop Protocol (RDP), sviluppato da Microsoft e disponibile su tutte le recenti versioni di Windows. RDP riesce a controllare qualsiasi Sistema Operativo client installato dall'Hypervisor grazie all'utilizzo di protocolli standardizzati ed adibiti solo a questo scopo. Ad un livello più avanzato troviamo, invece, la soluzione denominata System Center Virtual Machine Manager che fornisce la gestione centralizzata dell'ambiente virtuale, consentendo un maggiore sfruttamento dei server e un provisioning delle nuove macchine virtuali da parte dell'amministratore del VDI.

Qui di seguito sono annoverate quattro componenti essenziali al funzionamento di tale applicazione:

- Server Virtual Machine Manager (Server VMM): è l'hub di un'implementazione VMM che consente a tutti gli altri componenti di interagire e comunicare.
- Database di Macchine Virtuali (Database VMM): è un catalogo di risorse utilizzabili per creare e configurare macchine virtuali all'interno del sistema operativo Windows Server 2008.
- Console di Amministrazione Virtual Machine Manager (Console VMM): è un'interfaccia grafica che permette di creare, distribuire e gestire macchine virtuali. Consente anche il monitoraggio e l'amministrazione di host e server di libreria.
- Host Macchina Virtuale (VM Host): è un computer fisico in cui sono ospitate una o più macchine virtuali.

4.3.3 Citrix XenServer

Il prodotto offerto dalla Citrix si chiama XenServer e sfrutta l'Hypervisor Xen.
Anch'esso del tipo 1 o bare metal, permette la sua installazione direttamente sul server senza richiedere la presenza di un Sistema Operativo host.
Tra le sue particolarità troviamo la pesante richiesta di spazio disco (circa 1,8 GB) e la provenienza dal mondo open source. In principio, infatti, venne sviluppato nei laboratori dell'Università di Cambridge sotto licenza GNU totalmente libera.
XenServer presenta quattro tipologie di prodotto:

- Free Edition: versione gratuita che permette il completo utilizzo dell'Hypervisor Xen assieme alla gestione delle Virtual Machine tramite l'applicativo XenCenter e alla tecnologia XenMotion che consente la conversione di macchine virtuali implementate da Hypervisor concorrenti come Microsoft Hyper-V e WMware ESXi.
- Advance Edition: variante con licenza commerciale che, oltre ad incorporare le caratteristiche della versione gratuita, consente di sfruttare funzioni di back-up e recovery delle VM.
- Enterprise Edition: anch'essa con le stesse funzionalità della versione precedente al quale si aggiunge lo StorageLink, ossia un sistema che permette il rapido caricamento di macchine virtuali attraverso una gestione ottimizzata dello storage.
- Platinum Edition: edizione completa che comprende l'assistenza tecnica on site e il back-up in remoto delle Virtual Machine su Server dedicati messi a disposizione da Citrix.

Sulla maggior parte delle CPU, XEN utilizza il paradigma della paravirtualizzazione, il che significa che il sistema guest dev'essere modificato per usare un'interfaccia virtuale tramite chiamate ad opportune API, dette Hypercall.
Attraverso la paravirtualizzazione, XEN può ottenere alte prestazioni, paragonabili a quelle di una la macchina non virtualizzata.
Grazie alla cooperazione con Intel, XEN ha potuto sviluppare un nuovo tipo di virtualizzazione definita Hardware assisted che sfrutta l'architettura VT-x.

Visto il successo riscontrato da Intel, anche AMD ha ideato un prodotto simile, chiamato AMD-V. Entrambe le tecnologie, pur essendo sostanzialmente diverse nell'implementazione e nell'organizzazione delle istruzioni, sono gestite in XEN da un "abstraction layer" comune, offrendo, così, la possibilità di far girare sistemi operativi guest indipendenti rispetto alla piattaforma hardware utilizzata.

Un'altra importante funzionalità offerta da XEN è la migrazione a caldo delle VM tra host fisici diversi. Denominata XenMotion Live Migration, richiede un downtime impercettibile e non necessita di riavvio della macchina virtuale. Durante questa procedura, la memoria della macchina virtuale è copiata nella destinazione senza che ne sia inficiata l'esecuzione, con tempi di sospensione molto brevi di circa 60-300 ms. Questo permette di installare aggiornamenti di sicurezza in maniera immediata evitando l'intervento diretto sulla postazione, oppure eseguire interventi di manutenzione su un determinato server trasferendo le sue macchine virtuali su di un altro elaboratore della rete. Ovviamente per usufruire di questa funzione è necessario avere uno storage condiviso tra i computer dell'infrastruttura.
Il software deputato alla funzione di Virtual Machine Monitor, ovvero alla gestione e al controllo delle macchine virtuali attive all'interno della VDI, si chiama XenCenter. Quest'ultimo è composto da un'interfaccia grafica sviluppata solamente per ambienti Microsoft Windows e, tramite di essa, può svolgere le seguenti funzioni:

- Installazione, configurazione e gestione dei cicli di operatività di Virtual Machine.
- Accesso alle macchine virtuali attive attraverso gli applicativi Xvnc o Remote Desktop, per la gestione di Sistemi Operativi rispettivamente Linux e Windows.
- Gestione delle applicazioni virtualizzate sulle VM tramite la funzione vApps;
- Configurazione dello storage e delle risorse di rete.
- Risoluzione dei problemi tramite la funzionalità Disaster Recovery.
- Analisi del traffico di dati sulla rete ed elaborazione di report sullo stato di saturazione della rete e delle sue risorse.

Grazie a recenti accordi stipulati con Microsoft, Citrix ha ottenuto la completa compatibilità con Hyper-V ed, in particolare, permette il controllo dei dispositivi per la memorizzazione di dati e per la gestione delle Virtual Machine con sistemi Windows.

4.4 Lo storage

In un sistema virtualizzato la componente fondamentale, dopo i server fisici che permettono alle VM di funzionare, è lo storage. Con questo termine si indicano i dispositivi hardware per l'immagazzinamento, in modo non volatile, di dati elettronici. In particolare si parla sempre più spesso di network storage, ovvero qualunque tipo di immagazzinamento che permetta l'accesso alle informazioni tramite una rete di computer e che dia la possibilità a multipli nodi di condividere gli stessi dati contemporaneamente.
In questo modo la gestione delle informazioni è centralizzata e si evitano ridondanze inutili e spesso dannose.
Lo Storage Area Network è stato progettato per soddisfare queste esigenze.
Una SAN è una soluzione dedicata, ad alte performance e separata dalla rete locale. Inoltre, al contrario del Network Attached Storage che è ottimizzato per la condivisione dei dati a livello di file ed è quindi più adatto al backup, la SAN opera a livello di blocco. Dal punto di vista pratico viene reso disponibile lo spazio fisicamente presente sui dischi condivisi, come se fosse una risorsa locale.
Questo spazio non formattato è chiamato LUN (Logical Unit Number) la quale non è altro che una partizione logica della SAN. Il sistema operativo tratterà quindi tale risorsa come disco o partizione locale, sui cui possono essere eseguite le tipiche operazioni di partizione, formattazione, gestione dei file system ecc.

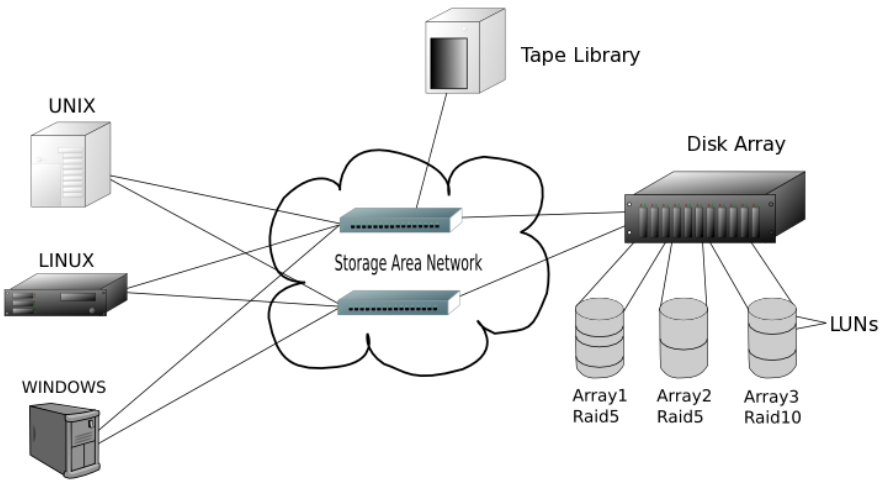

Figura 4.3 Schema generico di una Storage Area Network

L'architettura distribuita di una Storage Area Network permette di raggiungere i più alti livelli di performance e affidabilità, permettendo ad un vasto numero di utenti di accedere contemporaneamente ai dati senza creare colli di bottiglia sulla LAN e sui server. La SAN è anche il miglior modo per garantire high availability, mantenendo allo stesso tempo un'ottima scalabilità. Offre una connessione molti-a-molti tra server e dispositivi di storage permettendo il trasferimento diretto dei dati tra diverse periferiche di memorizzazione, semplificando processi come il backup o la replica dei dati. Per questo motivo, sono molto utilizzate in ambienti virtualizzati, garantendo servizi quali Alta Affidabilità, Load Balancing e Disaster Recovery.
I principali protocolli di trasporto della SAN sono tre: SAS, iSCSI e Fibre Channel.

4.4.1 SAS

In ambito aziendale, il collegamento SAS è uno dei più utilizzati grazie al buon rapporto costi/benefici. A fronte di ottime prestazioni (fino a 6 Gbps), l'impatto sull'infrastruttura preesistente è superiore rispetto all'iSCSI, ma più contenuto rispetto alla soluzione in fibra ottica.

Un tipico sistema Serial Attached SCSI è composto da:

- Initiator: nella modalità più semplice è un controller SAS che gestisce le richieste verso le periferiche collegate, trasferendo loro i comandi e aspettando le risposte. Gli initiator possono essere integrati sulla scheda madre (come nel caso delle schede madri orientate ai server) oppure possono essere delle schede aggiuntive. In una Storage Area Network con dischi SAS l'iniziatore è esterno al server in quanto si trova all'interno del sistema di storage.
- Target: una periferica di destinazione può essere un dispositivo ad accesso diretto (dischi fissi e memorie flash) o un dispositivo ad accesso sequenziale (nastri magnetici). Le periferiche di destinazione contengono delle *Logical Units* (Unità logiche anche chiamate LUNs) e hanno delle porte di comunicazione che ricevono i comandi dall'initiator e gli restituiscono le risposte.
- Sottosistema di trasmissione: è la parte di un sistema I/O che trasmette informazioni tra initiator e periferiche di destinazione. Tipicamente è l'insieme di tutti i cavi e dell'elettronica di comunicazione che servono per connettere l'initiator alle periferiche di destinazione.
- Expander: sono i dispositivi del sottosistema di comunicazione che agevolano la connessione tra le periferiche SAS, facilitando il collegamento di molteplici dispositivi ad una singola porta di un initiator.

Ciascun dispositivo è collegato direttamente all'initiator a meno che non sia utilizzato un expander. Se un dispositivo è collegato direttamente all'initiator non esiste contesa del bus pertanto il sistema risulta molto più efficiente di un sistema a contesa come si ha per il bus SCSI anche quando al bus è collegata una sola periferica. Inoltre questo tipo di collegamento elimina il clock skew ossia il fatto che il clock arrivi a più dispositivi con ritardi differenti.
Il SAS sostiene un alto numero di periferiche (fino a 16384) ed una velocità di trasferimento di 1.5, 3.0 o 6.0 Gbps (12 Gbps nel prossimo futuro) realizzata su ogni connessione controller-periferica, quindi un maggior throughput.

In una SAN con tecnologia SAS il server è collegato ai dischi in modo diretto e incrociato: non ci sono switch fra server e storage.
Considerando un server con 2 schede di rete con 2 porte ciascuna, la prima scheda è collegata alle porte 1 del controller 1 e del controller 2 dello storage mentre la scheda di rete numero 2 è collegata alle porte 2 di entrambi i controller.
In questo modo, in caso di guasto di uno dei due controller, il traffico è dirottato sull'altro.

4.4.2 iSCSI

Internet Small Computer System Interface è un protocollo che permette ai comandi SCSI di essere trasmessi tramite una rete TCP/IP. Poiché lo SCSI fa uso intensivo della CPU per le operazioni I/O, l'iSCSI fa uso di Host Bus Adapters (HBA) che effettua la conversione da protocollo SCSI a protocollo IP.
iSCSI oggi sta riscuotendo un notevole successo dato che, grazie ai suoi nuovi sviluppi tecnologici e alle nuove architetture sviluppatesi, è possibile creare SAN senza dover incorrere in importanti implementazioni strutturali. Si riescono comunque a garantire livelli di performance adeguati con costi decisamente più contenuti.
Si possono, infatti, utilizzare normali cavi di rete e switch ethernet per comunicare con lo storage ad una velocità di 1 Gbit/s.

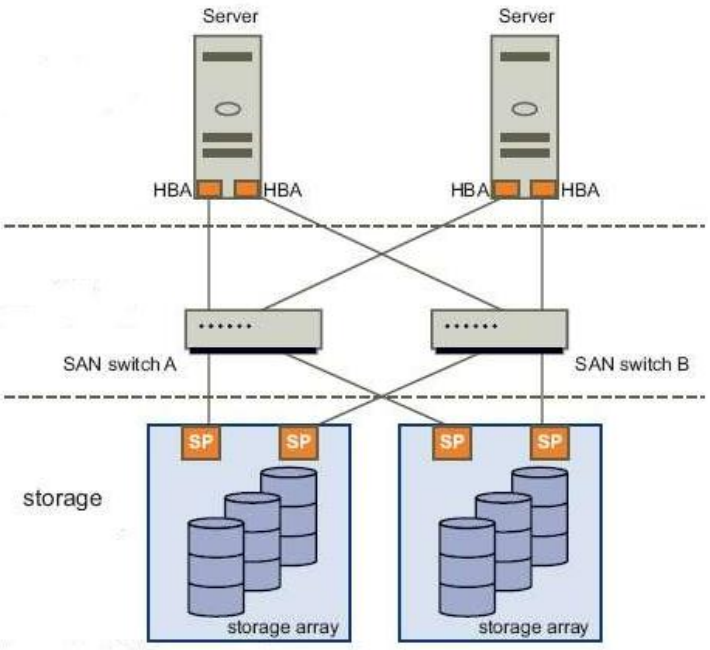

Figura 4.4 Collegamento iSCSI tra server e storage

Generalmente in un sistema iSCSI, il collegamento fra server e dischi è incrociato, ma non diretto: fra host e SAN ci sono degli switch che instradano i pacchetti.
Considerando un server con 2 schede di rete con 2 porte ciascuno, la prima scheda è collegata alle porte 1 dello switch 1 e dello switch 2, mentre la seconda è collegata alle porte 2 degli switch 1 e 2. Le uscite dello switch sono, a loro volta, collegate allo storage con lo stesso procedimento. In questo modo si garantisce continuità di lavoro anche in caso di guasto di uno switch o di un controller ethernet della SAN o del server. Il tutto con normali switch ethernet unmanaged visto che la destinazione dei pacchetti è scritta all'interno dell'header del pacchetto (utilizzo di TCP/IP).

4.4.3 Fibre Channel e FCOE

Il Fibre Channel è la tecnologia più utilizzata nelle architetture di storage delle grandi aziende. Nata per sopperire alle mancanze dello SCSI, che non poteva propagare il segnale oltre i 25 metri per problemi di disallineamento, inizialmente era chiamata Fiber Channel per indicare che la trasmissione viaggiava su fibra ottica.
Il nome poi è cambiato in Fibre quando la trasmissione ha iniziato a viaggiare anche su cavi di rame. In questa architettura, ogni nodo ha uno o più adattatori locali chiamati Host Bus Adapter (HBA) e la connessione ai vari dispositivi avviene attraverso l'utilizzo di switch di rete.
I principali vantaggi sono:

- Elevata capacità di carico;
- Bassa latenza;
- Affidabilità;
- Controllo di flusso per evitare congestioni di rete;
- Qualità del servizio (QoS);

Purtroppo il tutto si traduce anche in costi elevati: gli switch e i dispositivi sono molto costosi (uno switch fibre channel 8 porte ha un prezzo di quasi 3000 euro), la manutenzione e la gestione non sono delle più semplici e si presenta la necessità di creare un'infrastruttura ad-hoc separata dal network preesistente.
Tuttavia un'azienda disposta ad affrontare tali spese, può sfruttare tutta la potenza di questa tecnologia data da una velocità di comunicazione con lo storage di oltre 8 Gbit/s. Negli ultimi anni si sta affermando un nuovo standard chiamato FCoE (Fibre Channel Over Ethernet), il quale consente di consolidare il traffico Fibre Channel sulla connessione Ethernet utilizzata per i dati, permettendo così una più semplice connettività dei server all'infrastruttura e garantendo nel contempo la piena compatibilità con tutto il software presente.
Per utilizzare FCoE sono necessarie apposite schede di rete chiamate CNA (Converged Network Adapter) e semplici switch ethernet per l'instradamento, mentre tutte le altre componenti dell'infrastruttura rimangono invariate rispetto ad una soluzione nativa Fibre Channel.
Con una rete ethernet che garantisca un trasporto senza perdita di pacchetti, questa nuova tecnologia può garantire una velocità di trasferimento di 10 Gbit/s.

Nel collegamento Fibre Channel (e FCoE), così come per quello iSCSI, il server è collegato alla SAN in modo indiretto e incrociato tramite switch.
Questa volta, però, essi sono in fibra e devono essere instradati manualmente tramite zoning (managed fibre switch).
Lo zoning permette di mappare lo storage creando fra host e SAN una serie di LAN virtuali taggate in cui ogni "zona" è isolata completamente dalle altre.
Se tale procedura non venisse messa in atto, la rete non funzionerebbe correttamente.

4.5 La rete

Alla base di ogni buona infrastruttura tecnologica dev'esserci una rete locale ben organizzata, efficiente e sicura. Procedere con il consolidamento usando hardware performante e costoso per poi inserirlo in una rete non ottimizzata, renderebbe l'investimento poco produttivo e, nei casi limite, quasi inutile.
Quindi una virtualizzazione dell'infrastruttura porta con sè un adeguamento della LAN in modo da massimizzare le performance e ridurre al minimo malfunzionamenti e rallentamenti strutturali.
L'intranet aziendale è composta da server, client, nodi interni (switch), nodi di confine (firewall) e i vari collegamenti fra di essi.
Riorganizzare i client non è conveniente dato che, solitamente, si tratta di un gran numero di pc con diversi utilizzi e posizioni variabili, perciò si preferisce agire sui nodi in modo da velocizzare la comunicazione e renderla più stabile e sicura.

4.5.1 Switch

L'ottimizzazione di rete inizia dall'analisi dei nodi interni: la virtualizzazione porta ad una riduzione degli switch e quelli rimasti devono essere performanti dato che il traffico è stato centralizzato. Il fulcro della rete è un particolare switch detto "centro stella" al quale vengono collegati i server, il firewall e tutti gli elaboratori che fanno uso intensivo di entrambi. Se la rete è particolarmente popolata, allo switch principale si collegano degli switch secondari che suddividono la LAN, a seconda dell'utilizzo o della zona geografica.
Ogni componente di rete che si frappone fra pc e centro stella, aumenta il rischio di perdita di prestazioni e stabilità per cui si cerca di avere meno "salti" possibili dai client ai server. Si ha che le performance di rete di un dato elaboratore sono quelle del componente più lento che si incontra nel cammino verso il fulcro della LAN.
Per questi motivi, i nodi interni hanno solitamente porte da almeno 100 Mbit/s ed alcune di esse, che fungono da ponte fra i vari switch, sono da 1 Gbit/s per evitare colli di bottiglia.

Un tipico esempio di centro stella è lo switch HP 2810-48G che, disponendo di 48 porte da 1 Gbit/s, è in grado di sostenere agevolmente la maggior parte del traffico di rete di un'azienda media. Un valido switch secondario, invece, è l' HP 2510-24 che avendo 24 porte a 100 Mbit/s e altre 2 da 1 Gbit/s può fungere da espansione e/o ponte verso il centro stella.

4.5.2 Soekris

Soekris Engineering Inc. è una piccola azienda specializzata nella progettazione di computer embedded e dispositivi di comunicazione.
Una Soekris è fondamentalmente una piattaforma x86 single-board, per lo più distribuita in un box verde delle dimensioni di una scatola di sigari.
Questi dispositivi sono utilizzati per una varietà di applicazioni embedded, in particolare per il networking: router, firewall, ponti vpn e access point.
Le schede più recenti sono dotate di processore AMD Geode dissipato passivamente.

Il modello net4501, ad esempio, è molto utilizzato come server NTP (Network Time Protocol) ad alte prestazioni.
Essendo schede "All in one", non sono progettate per l'esecuzione di programmi pesanti e CPU-Intensive. Inoltre, nella maggior parte dei casi, il disco primario è una scheda Compact Flash simile ad una penna usb e quindi non particolarmente performante in lettura e scrittura.
I punti di forza di questi dispositivi sono flessibilità, affidabilità e bassi consumi:
la potenza consumata è fra i 5 e i 15W, le temperature d'esercizio vanno da 0 a 60° e sulla scheda non vi sono parti in movimento, dissipatori compresi. Questo rende la Soekris immune alla polvere e ai guasti da essa derivanti e, quindi, soggetta solo a malfunzionamenti di tipo elettronico che risultano essere particolarmente rari viste le prestazioni non spinte e l'architettura consolidata.
La scheda è gestita tramite console seriale raggiungibile con collegamento attraverso la porta COM. Inoltre quasi tutti i modelli hanno uno o più porte Ethernet utilizzabili per la gestione dell'apparecchio una volta installato il sistema operativo e configurata l'interfaccia di rete.
A questo punto è lecito chiedersi quali sistemi operativi supportino un dispositivo simile. Teoricamente ogni sistema eseguibile su un x86 ed avente una modalità testo dovrebbe poter girare su una Soekris se essa rispetta i suoi requisiti minimi.
E' chiaro che la scelta cada su sistemi progettati per essere utilizzati principalmente via riga di comando, quindi totalmente sprovvisti di interfaccia grafica.
Nella stragrande maggioranza dei casi si tratta di sistemi Linux.
In rete, infatti, si trovano particolari distribuzioni nate per essere utilizzate su dispositivi di rete embedded. Una di queste, chiamata Voyage Linux, è sviluppata sull'hardware delle Soekris e quindi vi si adatta perfettamente.

Un apparecchio molto utilizzato come nodo di confine è il net4801.
Questa scheda compatta, a basso consumo e a basso costo, si basa su un processore di classe 586 a 266 Mhz, supportato da un massimo di 256 Mbyte di SDRAM.
Ha tre porte ethernet 10/100 Mbit e utilizza un modulo Compact Flash per la memorizzazione dei programmi e dei dati. Inoltre può essere espansa utilizzando schede MiniPCI III, PCI standard a basso consumo e USB avendo una porta 1.1.
È stata ottimizzata per l'uso come firewall, VPN Router e Gateway Internet, ma ha la flessibilità per svolgere le funzioni più svariate a livello di comunicazione di rete.
Con un dispositivo simile, attraverso iptables e openVPN, si possono adattare firewall e tunnel di rete alle esigenze del cliente, ottenendo comunicazioni sicure ed affidabili fra le varie postazioni e sedi geografiche.
Inoltre si possono implementare traffic shaping e bilanciamento di carico: il primo livella i picchi di utilizzo della linea in modo da avere latenze ridotte ed eliminare l'effetto "collo di bottiglia" anche con un gran numero di utilizzatori, mentre il secondo si applica quando il cliente dispone di più linee adsl e serve a suddividere in modo adeguato il traffico di rete verso l'esterno per evitare congestione e rallentamenti garantendo, nel contempo, continuità di lavoro e qualità di servizio.

4.6 Salvataggio e recupero dati

La conoscenza dei rischi legati alla sicurezza delle informazioni, a volte, è limitata al solo utilizzo di antivirus, ignorando i processi di backup e considerandoli al massimo una fastidiosa preoccupazione. Fino a quando non si hanno perdite di dati che si traducono in perdite commerciali.
Generalmente il backup è fatto a specifici intervalli di tempo salvando, oltre ai dati, anche il sistema operativo. Se si deve recuperare qualche file, basta accedere al backup. Invece in caso di disaster recovery, il restore può essere fatto solamente su una macchina che è l'esatto duplicato di quella di partenza.
Con l'adozione della virtualizzazione dei server e lo storage condiviso, le operazioni di backup diventano facilmente attuabili e meno costose grazie all'uso degli snapshot. Uno snapshot non è altro che una "foto" dello stato attuale della macchina virtuale, una copia dello stato della Virtual Machine per come si trova in quel momento in memoria, comprese le impostazioni e gli stati di ogni disco.
E' è un'operazione piuttosto semplice ed, in genere, è già integrata nelle console di virtualizzazione. Il ripristino è semplice e veloce perché la macchina virtuale può essere copiata su qualsiasi server, anche di fortuna, non necessariamente speculare a quello di partenza. Lo snapshot quindi è un importante strumento di protezione delle macchine virtuali, ma non dovrebbe essere considerato come l'unico metodo: con lo snapshot il ripristino deve essere fatto sull'intera macchina virtuale, anche per recuperare un solo file.
Per ovviare a questa situazione è possibile ripristinare la macchina virtuale su un server di test e da lì recuperare il file oppure installare un software di backup all'interno della VM per poi selezionare quali file devono essere protetti.
Il backup non deve assolutamente risiedere sullo stesso server dove sono i dati da proteggere altrimenti in caso di guasti o danneggiamenti, si perderebbero sia i file originali che i backup. Va considerata, quindi, la possibilità di replicare i dati offsite.

4.6.1 RAID

Nas e San utilizzano la tecnologia RAID (Redundant Array Of Independent Disks) per garantire l'integrità dei dati o aumentare le performance. L'idea alla base è di dividere e replicare i dati su più hard disk. Quando più hard disk sono messi in RAID formano un RAID Array ed il sistema li vede come un unico disco.
Ci sono diverse configurazioni RAID, ognuna con i propri benefici.
Il RAID 0, ad esempio, è una configurazione che aumenta le performance dividendo i dati su più hard disk. La ridondanza in questo caso è nulla e quindi non si ha tolleranza ai guasti, poco utile in ambito server.
La copia 1 a 1 di un intero disco, avviene con il RAID 1. Con questa tecnologia si perde metà dello spazio a disposizione a favore della ridondanza totale. In caso di guasto del disco principale, il secondario lo può sostituire immediatamente in tutte le sue funzioni. In ambito aziendale, i raid più utilizzati sono quelli che garantiscono la maggior protezione possibile contro la perdita dei dati: RAID 5 e RAID 6.
Nel RAID 5, ogni volta che i dati devono essere scritti sui dischi, viene calcolato il blocco di parità e il tutto viene memorizzato in maniera distribuita. E' il bit di parità che, in caso di problemi ad uno dei dischi, permette di ricostruirlo ricalcolandolo.

Questo dà la possibilità al sistema di funzionare anche in caso di un guasto, anche se con prestazioni leggermente inferiori, dato che i dati mancanti vanno ricalcolati.
L'unico svantaggio, sicuramente accettabile data la tolleranza ai guasti fornita, è la riduzione dello spazio di memorizzazione, proprio per la presenza del blocco di parità. Il RAID 6 è simile al precedente ma distribuisce due blocchi di parità sui dischi. Con questa configurazione il sistema potrebbe funzionare regolarmente anche con due hard disk guasti.

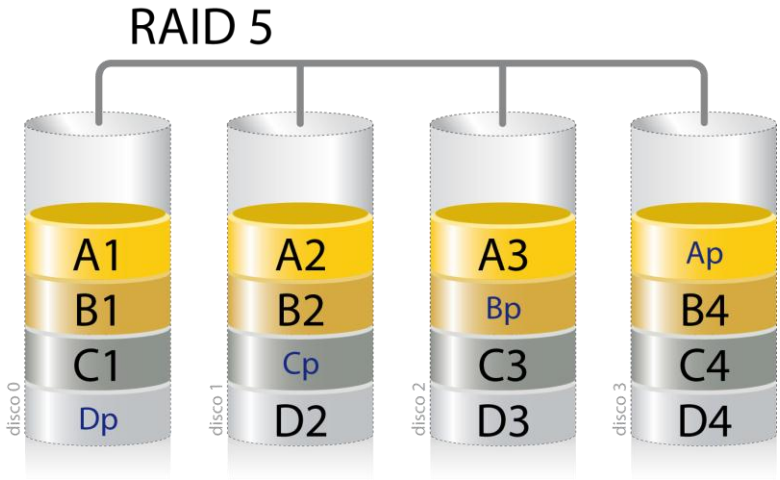

Figura 4.5 Schema RAID 5

Generalmente nei grossi server si combinano 2 tipi di ridondanza: il disco di sistema è in RAID 1 con un disco interno al server stesso, mentre lo storage è organizzato con un RAID 5 o 6.

4.6.2 NAS

Un Network Attached Storage (NAS) è un dispositivo collegato ad una rete di computer la cui funzione è quella di condividere tra gli utilizzatori della rete un'area di storage. I NAS, generalmente, sono dei semplici computer con a bordo il minimo necessario per poter utilizzare le funzionalità di networking.
Questi apparati non vanno confusi con le SAN, soluzioni di storage ben differenti: come visto nella sezione precedente, tali sistemi comprendono una rete e sono soggetti a protocolli spesso proprietari e tecnologie molto più costose.
Un sistema NAS può essere utilizzato come nodo di una SAN, data la scalabilità di tale architettura. Il principale vantaggio dei NAS, oltre a centralizzare l'immagazzinamento dei dati in un solo posto invece che spargerli su diversi sistemi di una rete, è la loro specializzazione dal punto di vista prestazionale e della sicurezza dei dati: gran parte di tali sistemi implementa array RAID al fine di garantire la ridondanza dei dati e permette l'aggiunta e la rimozione di dischi rigidi "al volo", senza bloccare il funzionamento dell'intero sistema ("hot swap").
Il principale svantaggio di questa architettura è dovuto alle prestazioni, le quali sono strettamente legate alla congestione della rete ospitante. Inoltre vi sono dei limiti prestazionali e di stabilità dei filesystem di rete attualmente disponibili sul mercato.

4.6.3 Software

I software utilizzati per il salvataggio dati sono suddivisi fondamentalmente in 2 categorie: repliche e backup. La replica è una tecnica moderna di salvataggio dati che, attraverso l'uso di snapshot, consente di fare backup incrementali e differenziali di intere macchine virtuali anche durante il funzionamento.
I programmi di backup, invece, si concentrano sulla copia dei dati selezionati dall'utente, all'interno di un dato sistema operativo, verso uno storage esterno.
Essi infatti sono installati su di esso e lavorano a livello di file, non di macchina virtuale. Nella maggior parte dei casi, si usano per duplicare informazioni importanti e database. La pianificazione delle copie avviene tramite "agenti": si crea un lavoro nel quale si selezionano i files da copiare, l'ora in cui copiarli e la destinazione.
In seguito l'agente eseguirà il lavoro pianificato e, nel caso di database, si preoccuperà di chiudere momentaneamente tutte le transazioni in corso per avere uno stato consistente e valido, disponibile per un successivo ripristino.
Un esempio di software completo per il salvataggio e il recupero dei dati è Veeam Backup. Questo programma è in grado di lavorare, indistintamente e dalla stessa console, sia su sistemi VMware vSphere che Microsoft Hyper-V.
Svolge entrambe le funzioni di backup e replica ed è in grado di compiere ripristini granulari: intere VM, singoli guest file, e-mail o file VM estraendoli dallo stesso salvataggio effettuato a livello di immagine. Per questi motivi è uno degli applicativi più utilizzati al mondo per infrastrutture virtualizzate e conta circa 7 milioni di macchine virtuali protette. Tuttavia questo programma non è in grado di eseguire la copia di database in uso, senza rischiare di comprometterli o salvarli in stati inconsistenti. Ecco perché, di solito, esso è affiancato da un sistema di backup classico come, ad esempio, Backup Exec di Symantec.
Backup Exec è una soluzione che fornisce copie disk-to-disk o disk-to-tape continuate e funzioni di recovery. Attraverso la "protezione continuata" è in grado di salvare in tempo reale sia i normali file che i dati dei database dei server mail e SQL durante il loro utilizzo, evitando i backup quotidiani e fornendo ripristini immediati.
Questo applicativo può avere uno o più media server, i quali spostano i dati da una o più località in un dispositivo di storage, come un disco o un nastro.
I dati possono essere in un sistema locale oppure in un sistema remoto con l'utilizzo di un agente remoto.

5 Il caso tipico

Per chiarire al meglio gli argomenti esposti in precedenza, in questo capitolo vengono presentati una serie di interventi pratici avvenuti presso un cliente di Sanmarco Informatica. Questo esempio è particolarmente esplicativo perchè comprende, oltre al processo di consolidamento con relativa alta affidabilità, anche un'attenta riorganizzazione di rete. Non sempre si interviene su entrambi: molto spesso si virtualizza senza intervenire sulla LAN oppure si ottimizza la rete locale senza consolidare il server.

5.1 Il punto di partenza

L'azienda si occupa di contabilità e presta consulenza aziendale, societaria e fiscale e relativi servizi. Per questo tipo di attività servono comunicazioni rapide ed efficienti ed una corretta gestione dei dati, per cui il cliente dispone delle seguenti macchine fisiche dedicate:

- Server di posta IBM Lotus Domino con gestionale personalizzato Sanmarco Informatica per l'organizzazione dei dati dei clienti.
- Server con BlackBerry Enterprise Server e IBM Lotus Notes Traveler per le comunicazioni mobili (tablet e smartphone).
- Server con Stanza Fax per la gestione dei fax.
- Server che fa da domain controller e file server per la memorizzazione centralizzata dei documenti.
- Server per il backup del domain controller.
- Terminal server con gestionale Team System per le pratiche contabili e commerciali.
- Server video sorveglianza.

Un totale di 7 elaboratori fisici distinti dei quali alcuni in rack ed alcuni tower, nessun sistema di backup (tranne che per il file server) e nessuna garanzia di business continuity ed alta affidabilità.

Gli apparecchi di rete disponibili sono:

- 3 switch Huawei S3000 con 24 porte 100Mbit e 2 da 1Gbit;
- 1 switch Netgear FS726TP26 POE 26 porte Gbit dedicato alla telefonia;
- 1 switch HP ProCurve 2626 con 24 porte 100Mbit e 2 da 1Gbit collegato all'access point che funge da gateway per la connessione ADSL verso l'esterno.

L'infrastruttura si presenta così:

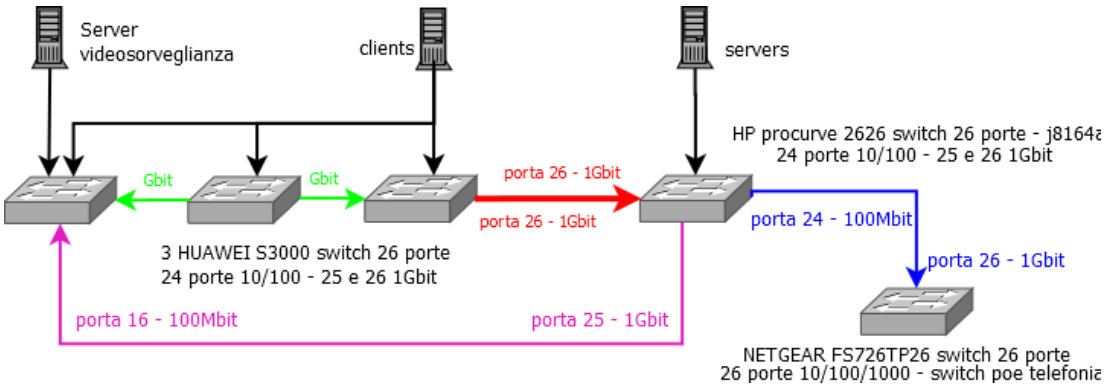

Figura 5.1 Infrastruttura del cliente: situazione di partenza

5.2 Analisi e progetto

Analizzando i server del cliente si nota una proliferazione di macchine fisiche obsolete con specifiche tecniche e fattori di forma molto diversi (sia tower che rack). Si ha, quindi, un grosso spreco di spazio e risorse energetiche a fronte di performance al di sotto delle aspettative dovute dell'hardware datato.
Inoltre, vista la totale mancanza di un sistema di backup e disaster recovery adatto, l'infrastruttura risulta vulnerabile a guasti e malfunzionamenti con conseguenti rischi per la continuità di lavoro e i dati sensibili dei clienti dell'azienda.
Per quanto riguarda la LAN, invece, si nota la grave assenza di un firewall hardware essenziale per difendere la rete da attacchi provenienti dall'esterno e tentativi di accesso non consentiti. Le comunicazioni presentano alcuni colli di bottiglia dovuti a collegamenti non ottimizzati o, in alcuni casi, ridondanti.
Il centro stella dispone solo di porte 100 Mbit/s perciò server e client, che usano la rete in modo intensivo, non sono collegati nel migliore dei modi; inoltre le connessioni di certi pc devono attraversare 2 switch prima di arrivare a destinazione.

In sede di progetto, si decide di consolidare 6 server fisici (con video sorveglianza a sé stante) su un unico sistema formato da due macchine fisiche IBM X3650M3 con VMware ESXi in grado di sopperire a tutte le esigenze del cliente mantenendo un rapporto prestazione/consumi molto elevato. Ognuna di esse, infatti, è composta da un processore Intel Xeon X5650 (6 core a 2.67 Ghz), 36 GByte di memoria RAM DDR3 1333Mhz, 2 dischi SAS da 146 GByte in RAID 1, alimentatori e moduli di ventilazione ridondati hot-swap, controller SAS per collegamento veloce (6 Gbit/s) con lo storage e doppia scheda di rete ethernet da 1 Gbit/s.
Lo storage scelto è un IBM DS3512 con 2 controller SAS incorporati e 8 dischi SAS "hot swap" 6 Gbit/s da 300 GByte ciascuno configurati in RAID 5 con hot spare per uno spazio disponibile di circa 1,8 TByte.
L'intero sistema, macchine più storage, occupa solamente 6 supporti rack all'interno di un armadio da 42 posti ed è gestito da Vmware vCenter.
In caso di guasto di una delle due macchine fisiche, l'intero carico di lavoro viene spostato, in maniera trasparente ed automatica, sull'elaboratore ancora funzionante.

Per garantire alta affidabilità e business continuity, il cliente acquista una NAS Qnap TS-459 con 4 dischi da 2 TByte in RAID 5 con hot spare per un totale di 5,5 Tbyte sui quali effettuare le repliche delle macchine virtuali tramite il software Veeam ed il salvataggio di file e database con Symantec Backup Exec.

Infine, dopo aver analizzato la rete locale, si decide di installare una Soekris net4801 come firewall perimetrale e nodo VPN e uno switch Hp ProCuve 2510G con 24 porte Gbit come nuovo centro stella.

5.3 Montaggio hardware

L'assemblaggio dell'hardware è particolarmente agevole e preciso: tutte le apparecchiature sono predisposte per essere montate in un armadio rack standard. Dato che il cliente dispone di due armadi, si posizionano server, storage, centro stella e firewall nel primo e tutti gli altri switch nel secondo in modo da agevolare eventuali manutenzioni future.
A questo punto si procede con la connessione macchine-storage: la SAN a disposizione usa la tecnologia SAS per cui il collegamento avviene in modo diretto ed incrociato tramite appositi cavi. I due server sono collegati come segue:

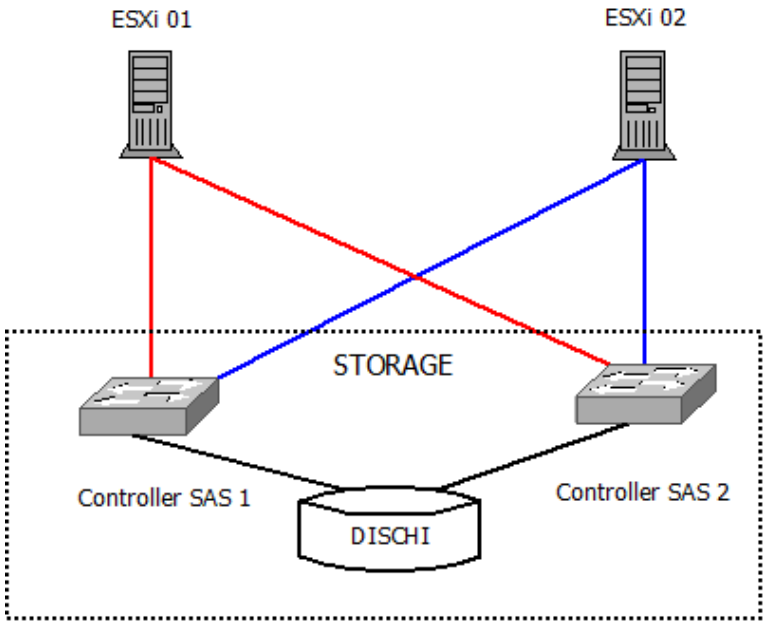

Figura 5.2 Collegamento SAS tra server e storage

Questo tipo di collegamento mantiene il sistema in funzione anche in caso di congestione o blocco di uno dei due controller SAS dello storage.
Generalmente, poi, si collegano tutti i dispositivi alla rete elettrica tramite un gruppo di continuità che sopperisce ad una temporanea mancanza di corrente.

Infine si posiziona il firewall fra l'access point della linea ADSL ed il centro stella in modo tale da filtrare tutto il traffico della rete interna verso l'esterno e viceversa.

5.4 Consolidamento

La migrazione delle 6 macchine da fisico a virtuale avviene a pc spenti tramite Vmware Converter: i server vengono prima salvati su NAS e poi spenti uno alla volta in una finestra di tempo concordata in precedenza. Per avere il minor impatto possibile sulle attività produttive del cliente, generalmente questa procedura avviene fuori orario di lavoro o nei giorni di chiusura.

Vmware Converter agisce attraverso uno wizard che, durante la procedura, chiede di definire la sorgente, la destinazione e settare alcune specifiche come il nome della macchine, la configurazione della scheda di rete, l'appartenenza ad un dominio o ad un workgroup e la timezone. Perciò, se avvenuta correttamente, la conversione restituisce un'infrastruttura server virtualizzata perfettamente identica a quella di partenza e quindi già pronta all'uso.

Per poter assegnare le risorse hardware in modo coerente, alla fine del consolidamento si analizzano funzionalità e carichi di lavoro di ciascuna VM e, in caso servisse, se ne creano di nuove in modo da averne una per ogni area funzionale.
A processo concluso risultano, quindi, le seguenti macchine virtuali:

- Antispam per il blocco della posta indesiderata;
- BlackBerry Enterprise Server per le comunicazioni con BlackBerry;
- IBM Lotus Domino come server di posta;
- Domain controller per gestire l'intera struttura di client e tutti gli utenti;
- Server di backup con Veeam Backup e Backup Exec;
- Stanza Fax;
- Team System con il database del gestionale contabile;
- IBM Lotus Notes Traveler per le mail da e verso i dispositivi mobili;
- Terminal e file server per centralizzare i dati di uso comune ed utilizzare il gestionale contabile su qualsiasi client attraverso il controllo remoto;
- VirtualCenter per la gestione e la manutenzione di tutte le macchine virtuali.

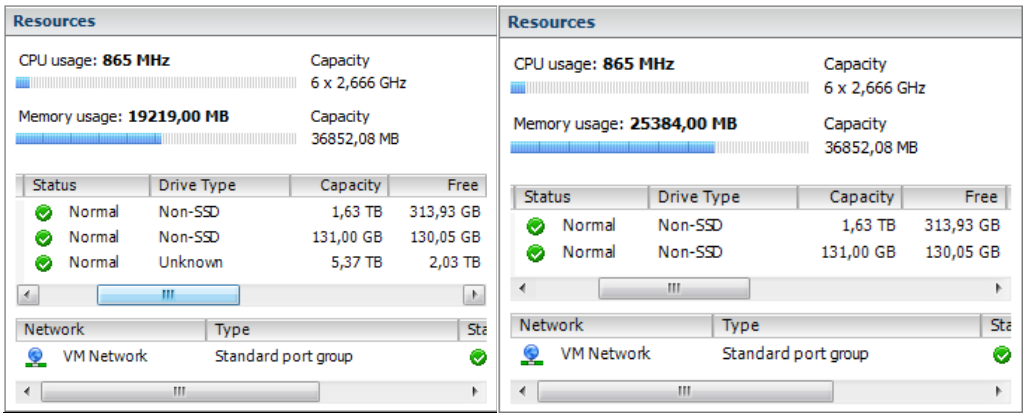

Figura 5.3 Situazione del sistema (ESXi01 e ESXi02) con tutte le VM operative

5.5 Alta affidabilità

Il piano di alta affidabilità concordato con il cliente prevede l'utilizzo di Veeam Backup e di Backup Exec secondo la seguente pianificazione:

- Veeam Backup
  - Processo: "Backup Job"
    Schedulazione: Ogni giorno alle 23.00
    Destinazione: NAS Qnap – cartella "VEEAM_backup"
    Selezione: tutte le VMs
  - Processo: "Replication Job"
    Schedulazione: Ogni giorno alle 3.00
    Destinazione: NAS Qnap – Cartella "VEEAM_replica"
    Selezione: tutte le VMs

- Backup Exec
  - Processo: "Daily backup"
    Schedulazione: Ogni giorno alle 21.00
    Destinazione: NAS Qnap – Cartella "BACKUP_EXEC"
    Selezione: database di Lotus Domino e TeamSystem, domain controller.

Così facendo, in caso di guasto, è possibile recuperare un'intera macchina virtuale oppure un singolo file in essa contenuto. Inoltre si possono riportare eventuali database fallati ad uno stato consistente, senza errori o transazioni pendenti.

Infine, per monitorare il corretto funzionamento dei salvataggi, viene giornalmente inviata al cliente una notifica mail contente il resoconto dei job completati.

5.6 Networking

La LAN del cliente presenta insicurezza, ridondanze e colli di bottiglia per cui si decide di sostituire lo switch centrale con uno più performante e posizionare un firewall perimetrale. Tutti gli switch in uso hanno almeno due porte Gbit: sfruttando la maggior larghezza di banda di cui dispongono, si riduce al minimo la congestione di rete. Conviene, quindi, usarle come collegamento verso il centro stella.
I server e il firewall vanno collegati al fulcro della rete in modo da avere tempi di risposta rapidi, inoltre è consigliabile avere una connessione diretta anche verso la NAS vista la mole di dati di backup giornalieri che essa deve sostenere.
Una volta allacciati i componenti più importanti, si riempiono le porte libere dello switch centrale con i ponti verso gli altri switch.
A questo punto ogni client contenuto nella LAN ha una connessione al più semidiretta con i server e i tempi di risposta sono ridotti al minimo.

Per quanto riguarda la sicurezza di rete, il cliente ha acquistato un servizio di antispam che è stato posizionato su una macchina virtuale dedicata per bloccare mail inutili e pericolose e ha richiesto un collegamento VPN con una sede secondaria.

Dopo aver completato l'ottimizzazione di rete, si personalizza il firewall perimetrale (Soekris net4801) secondo le esigenze dell'azienda, bloccando i servizi e le porte inutilizzati e monitorando quelli in uso per evitare intrusioni ed accessi indesiderati.
In seguito viene configurato il tunnel VPN e, su richiesta del cliente, si predispone il traffic shaping sulla linea ADSL così da garantire tempi di latenza minimi per le comunicazioni con la sede secondaria ed evitare utilizzi impropri della banda.

A lavoro concluso, l'infrastruttura si presenta come segue:

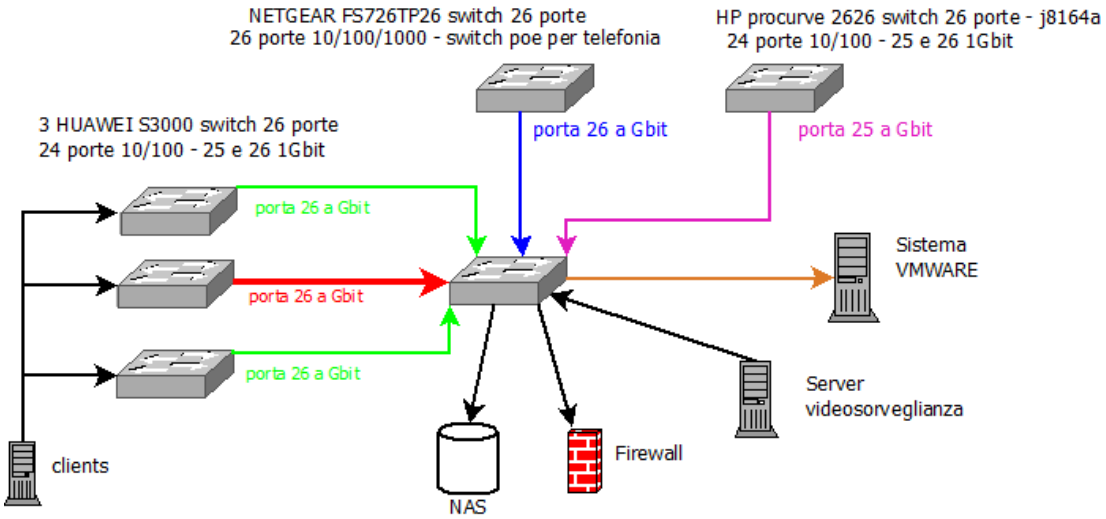

Figura 5.4 Infrastruttura del cliente: situazione finale

Dallo scema si nota come il server di video sorveglianza sia su una linea dedicata e lo switch HP ProCurve 2626, che prima fungeva da fulcro, ora sia libero per eventuali espansioni future. Tutti gli apparecchi, esclusi i client, sono connessi direttamente al centro stella alla velocità di 1 Gbit/s garantendo, di conseguenza, il massimo delle prestazioni ottenibili ed evitando colli di bottiglia e ridondanze.

6 Conclusioni

6.1 Potenziali sviluppi

Il mercato della virtualizzazione ha avuto un grande sviluppo nell'ultimo anno e sicuramente nel prossimo futuro riserverà grosse novità soprattutto a livello aziendale. Al giorno d'oggi sono già presenti numerose soluzioni ognuna con buone porzioni di mercato. La maggior parte delle volte si tende ad associare al concetto di "virtualizzazione del sistema operativo" solo la possibilità di utilizzare un altro sistema all'interno del proprio computer.
Tutto ciò, come visto, è estremamente riduttivo, in quanto ormai esistono già data center completamente virtualizzati, che gestiscono dati, applicazioni e banda internet al pari dei loro equivalenti fisici. Nei prossimi anni probabilmente si sfrutterà sempre di più la virtualizzazione nell'ambito dei terminali, una volta detti "stupidi" o "diskless", arrivando ad avere la propria postazione di lavoro ovunque nel mondo.
I probabili sviluppi futuri tenderanno a dividersi in due settori: consolidamento dell'intero sistema client con relativo accesso remoto, oppure, una singola macchina virtuale con un'istanza di essa per ogni client connesso via rete.
Quest'ultima soluzione è di gran lunga la meno onerosa in termini di prestazioni, ma comporta una maggior complessità a livello di progettazione e realizzazione dell'ambiente virtuale stesso.
Non va dimenticato, poi, che la virtualizzazione porta diversi problemi legati al licensing dovuti al fatto che gli "addetti ai lavori" non hanno ancora deciso se un'istanza di una VM debba essere considerata equivalente ad un sistema fisico o semplicemente un "accesso remoto" ad una risorsa.
Secondo il mio punto di vista, entro i prossimi anni si assisterà ad un incremento consistente del consolidamento virtuale lato server, che andrà a sostituire gran parte delle infrastrutture attuali. Inoltre, lato utente, come già accennato, vi sarà un progressivo accentramento dei sistemi, con client sempre più scarichi e server sempre più potenti e ridondati.
Chiari esempi di questa progressiva centralizzazione sono i servizi e le applicazioni web (vedi Google Apps) che, grazie anche alla tecnologia cloud, stanno prendendo piede molto velocemente nel settore dell'information technology.

6.2 Considerazioni finali

Affrontare il tema del consolidamento server significa descrivere una serie di aspetti diversi: quelli di carattere tecnico e tecnologico, relativi in particolare alla virtualizzazione, all'alta affidabilità, alle prestazioni dei server e agli strumenti necessari, e quelli relativi alla gestione di una struttura complessa, con annessi problemi economici, di rete e di sviluppo di un'azienda.
In questa tesi si è cercato di fornire una visione organica del settore, analizzando motivazioni, tecniche, procedure e strumenti che consentono di effettuare processi di consolidamento e continuità operativa. Per quanto possibile, lo si è cercato di fare in modo imparziale, senza preferenze per una soluzione software particolare, citando solo alcuni casi a titolo esemplificativo. L'intento generale era quello di fornire un modello che idealmente potesse essere seguito come una sorta di guida alla virtualizzazione della propria infrastruttura.

Per concludere, alcune considerazioni di carattere personale.
La prima cosa che ho notato durante la fase di documentazione è stata l'incredibile quantità di materiale prettamente commerciale a disposizione: molto spesso ho avuto delle difficoltà nel farmi un'idea generale sull'argomento che stavo trattando.
La maggior parte dei dati trovati, infatti, pubblicizzava la soluzione del produttore di turno e non forniva una descrizione tecnica, affidabile ed imparziale.
Tuttavia, data la giovane età delle tecnologie e il grande interesse suscitato da esse, era più che prevedibile il doversi imbattere in numerosi articoli di marketing.
Ho avuto inoltre l'impressione che quello della virtualizzazione sia un mercato molto competitivo, nel quale vince chi riesce a fornire il sistema di gestione più completo e, nel contempo, più facile da gestire. Due aspetti che evidentemente tendono ad escludersi. Discutendo con sistemisti e sviluppatori del settore, si deduce che attualmente alle soluzioni open source non manchino tanto prestazioni o funzionalità, quanto più quel componente centralizzato da cui gestire il tutto, che troviamo invece nelle soluzioni commerciali.
Personalmente, lavorando a questa tesi, ho affrontato diversi argomenti che non conoscevo, come la virtualizzazione e l'alta affidabilità, e ho avuto modo di farmi un'idea precisa degli attori e dei mezzi coinvolti in questi processi.
Viste le ottime prospettive future di queste tecnologie e l'interesse scaturito durante la scrittura di questo elaborato, credo che continuerò a seguire gli sviluppi del settore.

Bibliografia

Besana, D. (2008). *Il RAID*. www.itvirtualcommunity.net

Gallucci, D. (2010). *Realizzazione di una infrastruttura ICT per una PMI.* Università degli studi di Camerino

IBM Corporation (2011). *IBM System Storage DS3500 Express Storage System*. International Technical Support Organization.

IBM Corporation (2008). *IBM BladeCenter Chassis Product Guide*. International Technical Support Organization.

IBM Corporation (2006). *IBM Business Continuity and Recovery* Services. International Technical Support Organization.

James E. Smith e Ravi Nair, R. (2005). *Virtual Machines: versatile platforms for systems and processes*. Morgan Kaufmann.

Serravalli L., (2011). *Studio e valutazione di procedure di consolidamento per server fisici in strutture virtuali.* Università degli studi di Bologna

Tanenbaum , A.S. e Wetherall, D. J. (2011). *Reti di calcolatori.* Pearson, 5° edizione.

Tate, J., Lucchese, F. e Moore, R. (2006). *Introduction to Storage Area Network.* International Technical Support Organization.

Uddin, M. e Rahman, A.A. (2011). *Virtualization implementation model for cost effective & efficient data centers.* IJACSA.

Watts, D., Hurman, M. e Braz da Silva, L. (2009). *Implementing the IBM BladeCenter S Chassis.* International Technical Support Organization.

Wmware, Inc. (2010). *Virtualization overview.* Wmware white paper.

Citrix, http://www.citrix.it
Google, http://www.google.com
IBM Italia, http://www.ibm.com/it/it
Microsoft, http://msdn.microsoft.com
Sanmarco Informatica, http://www.sanmarcoinformatica.it
Soekris. http://soekris.com
Symantec Backup Exec, http://www.symantec.com/it/it/backup-exec
Veeam, http://www.veeam.com/it
Vmware, http://www.vmware.com
Wikipedia, http://www.wikipedia.org