ISTITUTO DI RIPOSO PER ANZIANI

Analisi e revisione dell'infrastruttura hardware e software di base di un ente pubblico

Alberto Semenzato

12/12/2010

Analisi dell'infrastruttura esistente, descrizione dei vantaggi della virtualizzazione, individuazione dell'hardware necessario alla virtualizzazione, strategie di implementazione e manutenzione dell'infrastruttura progettata, e strategie di sviluppo.

Sommario

1. Prefazione

1.1. Descrizione dell'organizzazione ospitante

L'Istituto di Riposo per Anziani (di seguito IRA) è un ente pubblico con una settantina di postazioni client distribuite in due sedi collegate tra loro per mezzo di ponti radio. Delle due sedi, una ospita la parte amministrativa dell'ente, mentre la seconda è adibita all'assistenza degli ospiti, quindi principalmente fornita di personale medico ed infermieristico. E' in costruzione una terza sede presso il Comune di Selvazzano che andrà ad estendere i servizi dell'ente, quindi anch'essa principalmente costituita prevalentemente da personale medico ed infermieristico, oltre che amministrativo.
L'azienda ha ottenuto la certificazione ISO 9001:2008.

1.2. Obiettivi

Il progetto si pone come obiettivo di fornire la migliore offerta in termini economici e tecnologici dal punto di vista di un aggiornamento dei sistemi informatici ed informativi dell'ente. E' richiesta una soluzione dimensionata alle esigenze dell'azienda, che rispetti però vincoli di affidabilità e ridondanza, facilità di amministrazione ed adeguata alle ultime leggi sulla privacy riferite al trattamento di dati personali e sensibili. L'ente, come scelta strategica, ha adottato l'utilizzo di software commerciale, basando la propria infrastruttura su sistemi Microsoft Windows 2003 Server e Windows XP e richiede come vincolo l'utilizzo di una tecnologia di virtualizzazione per diminuire i costi di gestione e manutenzione. Sarà scopo di questo documento individuare la miglior piattaforma di virtualizzazione presente sul mercato adeguata alle esigenze aziendali.

2. Analisi della situazione esistente

2.1. Configurazione dei server

2.1.1. Hardware dei server

Di seguito una tabella con la situazione hardware dei server, disposti in un rack da 25U, posizionato all'interno della sala server al primo piano dell'ufficio Amministrazione dell'ente.

Rack Report							
Manufacturer	***Product Number***	***Part Number***	***Serial Number***	***CPU***	***Hard Drive Capacity***	***Height in U's***	***Memory***
IBM	8841	1AG	KDMN903	Intel Xeon 4C	2x36,4 GB ULtra320 10krpm	5	3Gb
HP	417537	421	CZJ707015V	Intel xeon	2x72 GB S-SCSI 10K rpm	5	1Gb
HP	378738	421	GB8546PWJ8	Intel Xeon 4x3.4Ghz	4x146.8 GB ultra320 SCSI 10K Rpm	2	3.5Gb
Fujitsu Siemens			YBQB001430	PIII			

2.1.2. Configurazione Logica dei server

GB8546PWJ8 – Modello ML-380
OS: Windows Server 2003 SP2
Nome di rete: server-ira.ira.local
Dischi logici:

- Raid 1 (Mirror) 146 GB
  - **C**: (OS) 39,07 Gb - 70% free
  - **D**: (Cartelle di dominio) 83,01 Gb - 39% free
  - **O**: (Per copie shadow) 14,64 Gb - 11% free
- Raid 1 (Mirror) 146 GB
  - **E**: 39,07 Gb - 11% free
  - **F**: 97,66 Gb - 10% free (share per profili roaming)

Applicazioni Installate:
Istanze di SQL Server 2005
Backup – Barracuda-Yosemite Backup
MSOffice 2003
Kiwi Syslog Daemon

Servizi Installati:

- Active Directory Domain Services (tutti e 5 gli FSMO)
- DNS (errori dovuti alla configurazione singola)
- Print Server
- NTP (PDC Emulator)
- DHCP (Senza credenziali per le registrazioni dinamiche)
- IIS 6.0
- FTP
- Sharepoint 3.0
- WINS
- APACHE Tomcat

CZJ707015V – Modello ML-350
OS: Windows 2000 SP4
Nome di rete: Iradomino.ira.local
Dischi Logici:

- Disk 1 33,91Gb
  - **C**: 7,81 Gb 11% free
  - **D**: 7,81 Gb 66% free
  - **E**: 18,26 Gb 6% free
- Disk 2 33,89
  - **H**: Backup Disk 29% free

Applicazioni Installate:

- Lotus Domino v5
- MSSQLServer 2000
  - OCEANO
- Edisoftware Gestionale
- ADHoc Enterprise

Servizi Attivi:

- DNS slave zona ira.local
- RAS (Remote Access Service)
- WINS (disabled)

2.2. Software di Ambiente

2.2.1. Lotus Domino v5

Il software di ambiente in cui sono integrate alcune delle applicazioni chiave dell'Istituto di Riposo per Anziani è Lotus Domino v5, un software che estende la piattaforma di messaging e collaboration con un

application server in grado di ospitare applicazioni sviluppate da terze parti. Utilizza un'architettura software a tre livelli.

- **Domino Server**: si occupa di gestire il routing dei messaggi, l'aggiornamento degli account degli utenti, ed altri i processi di manutenzione del database oltre a permettere la connessione a diverse tipologie di client ai propri servizi. Utilizza il NOS, livello sottostante, per l'accesso ai file di database.
- **Notes Object Services (NOS)**: un insieme di funzioni e procedure che consentono la manipolazione dei file di database di domino. Si occupa di gestire le connessioni di rete con i client, ed è compiler ed interpreter dei linguaggi di sviluppo per Domino. E' il cuore del programma, multipiattaforma, ed estendibile in C, non solo del server Domino, ma anche dell'application server.
- **Database e Files**: Il basso livello che finalizza le informazioni su disco. I database sono in formato NSF, divisi per utente o per programma di terze parti.

IRA utilizza Domino v5 per gestire il routing della posta interna, con la gestione degli utenti separata da Active Directory. Per l'Application Server di Domino è stato sviluppato un programma fondamentale per l'organizzazione; la gestione del Protocollo.

2.2.2. DBMS Utilizzati

L'ente si serve di due piattaforme DBMS, SQL Server 2000 e MySQl 5.0 rispettivamente per applicazioni AdHOC Enterprise/Oceano Gestionale e SugarCRM.
L'istanza SQL Server su iradomino ospita tre database oltre a quelli normalmente installati. OceanoIra, il database per il gestionale, OceanoProve, il database probabilmente utilizzato per lo sviluppo e AdHoc, il database di supporto per l'ERP di zucchetti. I file di database importanti sono in D:\sql2k\data.
Il backup di SQL degli ultimi tre giorni, per ogni database, è salvato su E:\Sql2k\Backup
Il file MDF del database OceanoProve è invece nella directory di installazione standard di SQL Server.
L'installazione di MySQL è integrata nell'appliance Linux che ospita anche il web server Apache per l'esecuzione di SugarCRM: attualmente non è configurata per accessi esterni ed è usata direttamente dal motore del CRM per l'accesso ai dati.

2.3. Analisi delle applicazioni esistenti

2.3.1. Barracuda-Yosemite Backup

Il software di backup è installato sul domain controller. E' attivo un unico processo che riversa su nastro UFFPERS01, tutto Server-Ira, e parte di IraDomino (Systemstate + C,D,E). L'unico processo attivo è "Backup Server su SDLT". UFFPERS01 è sottoposto a copie di salvataggio relativamente alle timbrature del personale.

2.3.2. Antivirus NAV

L'antivirus è installato sul server IRADomino. Le policy per la gestione dei client possono essere configurate utilizzando la console amministrativa all'interno del server stesso.

2.3.3. Kiwi Syslog Daemon

Syslog Server per il forwarding dei syslog e dei trap SNMP della rete. E' configurato per ricevere i syslog da varie periferiche, principalmente dagli apparati Wireless.

2.3.4. Oceano, Edisoftware Gestionale

Il gestionale oceano serve per la gestione della contabilità. L'interfaccia è scritta in Java con accesso diretto al DB tramite connessione ODBC.

2.3.5. AdHoc Enterprise

Enterprise Resource Planning di Zucchetti. La parte client è installata anche nella cartella D:\Home\adhoc di IRADOMINO. La parte server è il database SQL Server su IRADomino. Viene utilizzato per la gestione del magazzino, con interfaccia client tramite FoxPro.

2.3.6. Gestione del protocollo

Gestito graficamente all'interno del programma client Lotus Notes, si occupa di registrare tutto il materiale documentario dell'Istituto in entrata ed in uscita, senza tuttavia conservarne una copia digitale per una facile consultazione.
La registrazione comprende un numero progressivo sia in entrata sia in uscita che identifica univocamente il documento, la data di ricezione o di emissione, il mittente o il destinatario ed il regesto, ossia una breve descrizione del contenuto.
Il documento protocollato è quindi archiviato nella sua forma cartacea nell'archivio.

2.3.7. SugarCRM

Il CRM è basato sulla piattaforma Open Source SugarCRM montato su un appliance Linux Debian con database back end MySQL nella stessa macchina. Il prodotto utilizza PHP come linguaggio di programmazione. L'appliance Linux che ospita il prodotto è un ottimo candidato alla virtualizzazione, grazie alla quale si potranno aumentare le risorse della macchina ed estendere il suo utilizzo in ulteriori ambiti aziendali. Utilizza un proprio modello di autenticazione non basato su active directory per la gestione degli utenti. La piattaforma è attualmente utilizzata per l'apertura di ticket di guasti a macchinari o edifici, che vengono in seguito verificati e gestiti dall'ufficio tecnico dell'istituto. Oltre a fornire lo storico delle segnalazioni, il programma consente di esportare in formato CSV un sottoinsieme dei ticket al fine di produrre delle statistiche gestionali.

2.3.8. Posta elettronica

2.3.8.1. Lotus Notes

La posta interna è gestita usando Lotus Domino 5 nella sua parte server e Lotus Notes 5 lato client. La posta gestita da locus notes è a solo uso interno, non riceve ne spedisce email verso l'esterno. Il programma utilizza un suo database proprietario per la gestione dell'utenza, non allacciato al database principale di active directory.

2.3.8.2. Posta Esterna

La posta utilizzata dagli utenti per comunicare con l'esterno (**@irapadova.it*) è gestita presso server di terze parti. Il download avviene utilizzando il protocollo POP3 in chiaro ed SMTP in chiaro. È scaricata utilizzando un software diverso rispetto a Lotus Domino, comunemente Outlook Express o Outlook standard.

2.4. Analisi Active Directory

2.4.1. Dati topologia

Tipo: Singola foresta con singolo dominio.
Modalità Foresta: 2000 Mixed (NT4 DC Compatibility)
Modalità Dominio: 2000 Mixed (NT4 DC Compatibility)
Topologia: Singolo sito con singolo domain controller.
DNS: Integrata, propagata a tutti i DNS Server in AD.
DNS name: ira.local

2.4.2. Domain Controller

2.4.2.1. Criteri Password

L'organizzazione usa l'history delle password (25), con validità massima di novanta Giorni e minima di uno, con requisiti di complessità e di minimo 8 caratteri.
Non è impostato alcun lockout nel caso di password errata.
Il KDC è configurato per validare verso le policy dell'utente che lo richiede, ogni richiesta di ticket (default).

Policy di Auditing dei DC:

Policy	Setting
Audit account logon events	Success
Audit account management	Success
Audit directory service access	Success
Audit logon events	Success
Audit object access	No auditing
Audit policy change	Success
Audit privilege use	No auditing
Audit process tracking	No auditing
Audit system events	Success

2.4.2.2. DC Policy

I domain controllers sono configurati per:

- Non avere alcun requisito di accesso al server LDAP.
- Firmare o cifrare digitalmente la comunicazione del secure channel (PC domain members)
- Firmare digitalmente tutte le comunicazioni SMB.
- Autorizzare solo comunicazioni con NTLMv1.

2.4.2.3. Group Policy

Le group policy rilevate in corso di esame sono:

- **AddAdminPCtoAdministrator:** Aggiunge AdminPC e AdminsPC al gruppo builtin\administrators dei computers.
- **DiableOfflineFile:** Proibisce l'uso della funzione File non in linea.
- **FolderRedirection:**
  - Forza l'attesa della rete prima dell'avvio e dell'accesso (applicazione GPO)
  - Consente il controllo del profilo utenti al gruppo Administrators
  - Esecuzione degli script in maniera sincrona: l'utente non accede al desktop finché non vengono eseguiti gli script.
  - Desktop e Documenti vengono creati in cartelle su server. L'accesso alle cartelle non è esclusivo. In caso di rimozione della GPO si mantiene il comportamento corrente.
- **LoginScript:** Esecuzione script userlogin.bat su server-ira\netlogon
- **LoopBack:** I criteri computer vengono applicati a livello di utente. I criteri vengono applicati sostituendo quelli degli utenti.
- **PolicyAntiConficker:**
  - Riconfigura i permessi per HKLM***\SvcHost e Tasks.
  - Disabilita autorun su tutte le unità
- **Proxy:**
  - Disabilita l'autoconfigurazione del browser
  - abilita la distribuzione del proxy tramite script.
- **RoamingProfileDisable:**
  - Consente la creazione dei soli profili utente locali.
  - Disabilita la propagazione delle modifiche del profilo comune al server.
- **SMBSigning:** Disabilita la firma SMB sia per i client di rete che per i server di rete.
- **FirewallDisable:** Disabilita il servizio WindowsFirewall/(ICS) all'avvio del sistema.

La descrizione completa delle policy è riportata nell'allegato tecnico al presente documento

2.4.3. Unità Organizzative

OU=IRA,DC=IRA,DC=LOCAL: Unità Organizzativa contenente tutti gli utenti della rete

OU=COMPUTER-OU,DC=IRA,DC=LOCAL: Unità organizzativa in cui sono presenti la maggior parte dei computer.
OU=Computer-Policy,DC=IRA,DC=LOCAL: Presenti due pc con una configurazione che permette l'utilizzo di profili roaming.
OU=COMPUTER-UO-02,DC=IRA,DC=LOCAL: Presenti alcuni pc, il gruppo ADMIN-PC non è amministratore della macchina, probabilmente per questioni di privacy.
OU=SERVER,DC=IRA,DC=LOCAL: senza policy, è adibita ad ospitare gli account di macchina dei server.

2.5. Rete

2.5.1. Struttura

L'intera struttura è composta da due edifici. Il primo, dove risiede la parte amministrativa e la sala ced è cablato interamente.
La seconda sede, che ospita i reparti, è collegata alla sede centrale tramite ponte radio, e parzialmente cablata. Ogni punto di raccolta è dotato di switch ethernet layer 2 configurati in spanning tree per ridondare l'accesso, in alcuni casi con collegamenti in fibra. I collegamenti restanti sono effettuati mediante bridge wireless in tutta la struttura.
Non è presente alcun server nella struttura che ospita i reparti. Tutte le risorse sono ospitate interamente nella sede amministrativa.

2.5.2. Protezione della rete

2.5.2.1. Protezione da attacchi esterni

La rete è protetta da attacchi esterni tramite un proxy/firewall linux. L'indirizzamento è ad assegnazione automatica (DHCP), basato su MAC Address, e le regole di accesso verso l'esterno si basano sull'IP del client che effettua la richiesta. Non è chiaro se il firewall possiede, oltre alla funzionalità di content filtering, funzionalità di antimalware in tempo reale sulle pagine web navigate.

2.5.2.2. Protezione da attacchi interni

Non esistono dei filtri[1] sullo switch (Layer2), l'accesso alla rete LAN mediante presa ethernet è libero. Non sono configurate VLAN per tagliare isolare il traffico di broadcast.

2.5.2.3. Protezione dalle intrusioni su rete wireless

I punti di accesso wireless alla rete locale sono protetti tramite chiave d'accesso WEP. Tutti i punti di accesso condividono lo stesso SSID e la stessa passphrase.

2.5.2.4. Protezione dei client e dei server

Client e server dispongono di protezione da intrusione e dall'esecuzione di programmi malevoli. E' stata implementata una soluzione di antivirus sia a livello server che a livello desktop/laptop. L'antivirus provvede automaticamente al download delle nuove firme di virus ed alla propagazione ai client. Non è stato disposto un sistema di aggiornamenti centralizzato per patchare i client e risolvere le vulnerabilità.
Alcuni Client non presentano neppure la tabella di aggiornamenti automatici di Windows, altri sono impostati per scaricare direttamente gli aggiornamenti da Windows update, con controllo periodico.
Antivirus e Aggiornamenti automatici del sistema operativo sono controllati con cadenza semestrale.

2.6. Protezione dei dati

I dati sono protetti dall'accesso non autorizzato tramite l'autenticazione integrata in active directory.
Vengono effettuate copie di sicurezza al fine di garantire la possibilità di ripristino dei dati e dei sistemi. Tali copie vengono effettuate con cadenza giornaliera tramite software di backup (Yosemite) e riversati su

[1] Per filtri si intende principalmente ACL o VLAN assengate automaticamente dallo switch, indipendentemente dalla porta, una volta effettuata l'autenticazione 802.1x (PNAC)

nastro. Il recovery time objective (RTO), non può essere inferiore alle ventiquattro ore, come descritto dal protocollo informatico.[2]
Sono adottate misure al fine di proteggere i dati sensibili o giudiziari contenuti su supporti rimovibili da accessi non autorizzati. Nel caso di backup, questi sono conservati e controllati settimanalmente.

2.7. Software nei PC

I client in dominio sono tutti configurati con Windows XP Professional. Su tutti i client è installato:

- Office
  - Versione 2003 SP3 + Compatibility Pack per 2007
  - Versione 2007
- Lotus Notes cinque
- Sw di posta elettronica esterna (OL Express o OL)
- Adobe reader
- Stampante PDF
- Antivirus Norton Corp.
- Software Oceano

2.8. Centro Servizi Bolis (Sede staccata di Selvazzano)

E' in costruzione, con data di apertura fissata per il mese di maggio 2011, una sede distaccata a Selvazzano.
La sede sarà collegata con il data center tramite ponte radio (40 Mbps Full Duplex) ed ospiterà strumentazione come descritta in seguito.

2.8.1. Esigenze di posti di lavoro

La sede ospiterà i seguenti responsabili che richiederanno un accesso alla rete:

- 1 Computer per Responsabile
- 1 Computer per Amministrativo
- 2 Computer per Capi Reparto
- 2 Computer per personale Medico
- 1 Computer per logopedista
- 1 Computer per Fisio-Kinesio Terapista
- 1 Computer per Psicologo
- 1 Computer per Educatore/Animatore
- 1 Computer per Assistente sociale

Per un totale di 11 Computer.

2.8.2. Requisiti Software

Gli utenti richiedono i seguenti software comuni:

- Microsoft Word
- Microsoft Excel
- Microsoft Outlook
- Microsoft PowerPoint
- L'accesso alla posta esterna e/o a quella interna
- Winrar o equivalente
- Acrobat Reader
- Accesso ad Internet per la navigazione
- Stampante PDF
- Accesso al CRM delle manutenzioni

[2] RTO: Tempo massimo definito da un Service Leve Agreement entro il quale un servizio deve essere ripristinato a seguito di un problema che ne causi la sua interruzione.

Alcuni utenti necessitano in oltre di software specifico per l'esecuzione dei loro incarichi, più precisamente:

- Amministrativi
  - Gestionale Kibernetes
  - Microsoft Access
- Logopedisti/animatori
  - Sistema audio per riproduzione MP3
  - Applicativo per gestione fotocamera
  - Programma di Fotoritocco
  - Microsoft Publisher
- Medici e Capi Reparto

Accesso VPN della sanità di Padova (connessione RDP incapsulata HTTPS.)

3. Considerazioni sulla virtualizzazione

La virtualizzazione tramite Hypervisor è una tecnica che consente l'esecuzione di sistemi operativi multipli in un unico server fisico. Il concetto è di inserire uno strato intermedio tra i sistemi operativi virtualizzati e l'hardware sottostante (l'hypervisor, appunto), presentando alle macchine virtuali un hardware sintetico, o virtualizzato, indipendente dalle caratteristiche di quello fisico. Con questo sistema, le macchine virtuali possono condividere le risorse presentate dallo strato intermedio, che si occupa di gestire gli accessi concorrenti. L'impatto sulle prestazioni derivato dall'aggiunta dell'hypervisor tra i sistemi operativi e l'hardware fisico è stato in buona misura colmato con l'introduzione di estensioni hardware per la virtualizzazione assistita direttamente nell'hardware fisico, arrivando a raggiungere prestazioni in gran parte simili ad un ambiente non virtualizzato.

Vantaggi della virtualizzazione:

1. **Ottenere il massimo dalle risorse esistenti**: raggruppamento in pool delle risorse d'infrastruttura comuni ed eliminazione del vecchio modello di corrispondenza univoca tra applicazioni e server ("una sola applicazione su ciascun server") grazie al consolidamento server, pur mantenendo separate le istanze virtuali dei server, quindi senza rinunciare al modello iniziale. E' anche possibile muovere senza interruzione di servizio, macchine virtuali particolarmente esose in termine di risorse verso un nodo di un cluster di virtualizzazione meno stressato.
2. **Ridurre i costi del data center mediante la riduzione dell'infrastruttura fisica e ottimizzare il rapporto server gestiti per amministratore**: meno server e relative risorse hardware significa ridurre le esigenze di spazio e le esigenze di alimentazione e raffreddamento. Con l'ausilio di strumenti di gestione ottimizzati è possibile migliorare il rapporto server gestiti per amministratore e, di conseguenza, ridurre le esigenze di personale.
3. **Fault tolerance**: Utilizzando cluster di virtualizzazione è possibile automatizzare lo spostamento di macchine virtuali da un nodo guasto ad un nodo pienamente operativo senza visibili interruzioni di servizio.
4. **Incrementare la disponibilità di hardware e applicazioni per migliorare la business continuity (Scalabilità)**: E' possibile aumentare la capienza di un cluster di virtualizzazione aggiungendo un nodo e muovendo le macchine a seconda del carico utilizzato in modo completamente trasparente all'utenza e senza interruzioni di servizio.
5. **Backup veloci dell'intera infrastruttura virtuale**: esecuzione di backup sicuri e migrazione di interi ambienti virtuali senza interruzioni operative. Rimozione dei downtime pianificati e ripristino immediato in caso di imprevisti.
6. **Ripristino veloce in caso di disaster recovery**: L'introduzione di uno strato di hardware sintetico tra le macchine virtuali e l'hardware fisico rimuove il vincolo di hardware simile per il ripristino di macchine a fronte di un disaster recovery.
7. **Acquisire la flessibilità operativa**: superiore capacità di risposta ai cambiamenti del mercato con la gestione dinamica delle risorse, la velocizzazione del provisioning dei server e la distribuzione ottimizzata dei desktop e delle applicazioni.

3.1. Piattaforma di virtualizzazione

Sono tre, i prodotti più diffusi che offrono virtualizzazione tramite Hypervisor: Microsoft Hyper-V, VMWare ESXi e Citrix Xen. E' disponibile il prodotto XEN anche in versione completamente Open source. I tre prodotti verranno trattati separatamente evidenziando i principali pregi e difetti.

3.1.1. Microsoft Hyper-V (v2)

La piattaforma di virtualizzazione di Microsoft viene installata come ruolo aggiuntivo di Windows Server 2008 R2, in entrambe le edizioni Core (senza GUI e con footprint ridotto) e Full. Con l'installazione dell'hypervisor, il sistema operativo diventa il primo sistema guest del sistema, con privilegi di gestione delle successive macchine virtuali e accesso fisico all'hardware.
Il codice dell'hypervisor è estremamente condensato, del peso minore di 1MB, tuttavia richiede comunque che sia presente e perfettamente funzionante l'installazione del primo sistema operativo guest, Windows Server 2008 R2, il cui peso, anche nella versione Core, si aggira sugli 8GB di spazio su disco e circa 512MB di ram.
Hyper-V basa buona parte dei servizi avanzati, quali Clustering ed amministrazione (centralizzata o meno) delle macchine, sul sistema operativo host o prodotti acquistabili separatamente. Il principale vantaggio del prodotto di virtualizzazione in questione è il costo ed il licensing, gratuito ed inserito nel contratto di licenza del sistema operativo. A seconda della versione server acquistata, a patto che il sistema operativo host venga usato solamente per scopi di virtualizzazione, è possibile "accendere" una o più macchine virtuali con un unica macchina fisica. Il principale svantaggio della soluzione è nel momento della configurazione di un cluster di macchine virtuali. Il servizio di cluster (di failover) sviluppato da Microsoft, richiede una struttura Active Directory, quindi non consente di virtualizzare interamente un'infrastruttura. Considerando l'importanza di proteggere le macchine di gestione dell'ambiente virtuale (la compromissione dell'hypervisor o del sistema operativo host comporterebbe un malfunzionamento di tutte le macchine virtuali al suo interno), i componenti "fisici" del cluster dovrebbero essere isolati dal resto della rete, richiedendo quindi un dominio ulteriore a quello utilizzato per la gestione degli utenti e delle risorse. Se a questo aggiungiamo la necessità di disporre di un failover anche del servizio di active directory, al fine di proteggere le funzionalità del cluster da possibili malfunzionamenti causati dal guasto del domain controller del dominio di cluster, per configurare un failover a due nodi sarebbero necessari almeno quattro server ed una SAN, due server fisici configurati come domain controller in replica, e due server configurati come nodi del cluster.
Sebbene sia possibile configurare il servizio di active directory direttamente sui nodi del cluster, è estremamente consigliato mantenere separato il domain controller da qualsiasi altro ruolo nella rete.

3.1.2. VMware ESXi

VMware ESXi è il componente di virtualizzazione utilizzato da vSphere, una suite di prodotti sviluppata per la gestione di infrastrutture virtuali di grandi dimensioni, con la possibilità di sfruttare servizi nel cloud secondo il concetto di software as a service.
ESXi è l'hypervisor dell'infrastruttura, basato in parte su kernel linux ed in parte sul codice proprietario che presenta lo strato di virtualizzazione. Può essere fornito direttamente come firmware all'interno dell'hardware del server oppure come binari installabili, il footprint dell'hypervisor è di circa 60MB più lo spazio necessario per l'installazione di tools per l'amministrazione. L'hypervisor è infatti privo di qualsiasi tool amministrativo, l'intera amministrazione deve essere effettuata remotamente.
Utilizza un file system per cluster che consente l'accesso multiplo a più hypervisor ESXi.
Sebbene l'hypervisor sia gratuito e scaricabile con semplice registrazione dal sito del produttore, i servizi avanzati per il backup e la movimentazione delle macchine, servizi di HA, fault tolerance o gestione centralizzata dei cluster sono a pagamento, ed il loro costo va sommato a quello delle eventuali licenze dei sistemi operativi guest.

3.1.3. Citrix Xen Server

Xen è un hypervisor open source a cui vengono affiancati, a pagamento, i servizi di gestione avanzata ed automazione. Essendo un prodotto open source, è possibile, per altre società, internizzare lo sviluppo degli strumenti di gestione ed automazione. Il lincensing per i servizi di gestione sviluppati da Citrix, attuale

proprietario di Xen, seguono un modello di licensing “per server”, divisi in pacchetto a seconda delle funzionalità di cui si vuole disporre, tuttavia è l’unica forma di virtualizzazione che permetta di effettuare una migrazione a caldo di macchine virtuali senza l’ausilio di tool di terze parti.
Il principale svantaggio di Xen, oltre alla scarsa distribuzione e quindi alla mancanza di una buona base di mercato e di casi di successo, è la scarsa capacità di virtualizzazione nativa di sistemi operativi Microsoft.

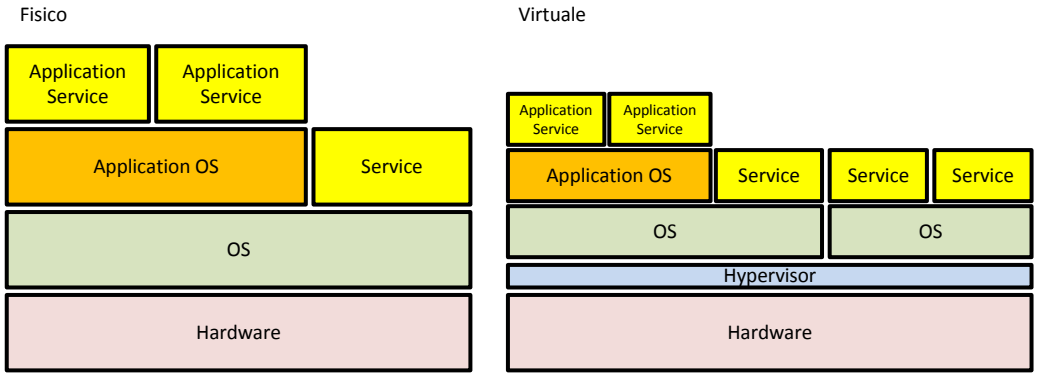
3.2. Conclusioni

Il prodotto che maggiormente risponde alle esigenze dell’organizzazione è VMware ESXi, l’edizione più adatta verrà stabilita in seguito sulla base di un analisi più approfondita delle necessità della struttura.
VMware presenta infatti maggiore compatibilità nella virtualizzazione dei server presenti in azienda, prevalentemente Microsoft, rispetto a Xen Server, un supporto più ampio ed una maggiore distribuzione e densità di casi di successo.
Microsoft Hyper-V, rispetto alla soluzione scelta, richiederebbe l’installazione di un secondo dominio per la configurazione di un cluster di failover, aumentando i costi di licensing ed necessitando successivamente un maggiore sforzo nell’amministrazione dell’infrastruttura di virtualizzazione.

4. Ipotesi di Progetto

La vitualizzazione introduce uno strato intermedio tra quella che è la rete su cui poggiano i servizi che verranno erogati dall’azienda e lo strato fisico dove tali servizi risiedono. S’intende quindi procedere individuando prima la strategia di provisioning dei servizi (comunque in un’ottica di infrastruttura virtualizzata) e la topologia di rete, successivamente si individueranno quali servizi potranno risiedere in ambiente virtuale e quali invece necessiteranno di hardware dedicato, per poi progettare la configurazione dell’hypervisor, dell’hardware e dell’architettura di rete dello strato fisico.

Schema A



4.1. Server

Disponendo di un ambiente di virtualizzazione che consente di accendere più macchine virtuali a costi e consumi contenuti, è possibile procedere alla creazione di macchine specializzate all’erogazione di un solo servizio, o più servizi affini. Grazie a questa tecnica è possibile ridurre il disservizio causato dalla perdita di dati, o dalla manutenzione programmata e non alla sola funzionalità esposta dalla macchina interessata.
Considerando questa tecnica sono stati individuati i seguenti server:

1. Controller di dominio primario (FSMO) + DNS + DHCP. (Windows Server 2008 R2 Core)
2. Controller di dominio secondario + DNS + DHCP. (Windows Server 2008 R2 Core)
3. Database server, che ospiterà tutte le istanze di SQL Server necessarie al corretto funzionamento dei servizi aziendali. (Windows Server 2008 R2)
4. Server Domino. (Windows Server 2000)
5. File Server in DFS. (Windows Server 2008 R2)
6. WSUS + Antivirus Server. (Windows Server 2008 R2)
7. Server Linux che ospita il gestionale.
8. Server firewall.

9. Server di Backup.

I servizi/server indicati potranno essere accorpati o si determinerà nel corso del progetto sulla opportunità di utilizzo anche in base alle risorse tecniche e ed economiche dell'ente.

Vista l'elevata importanza di Active Directory per l'organizzazione, sono stati previsti due domain controller in replica nella sede principale. Questo consente un elevato livello di fault tolerance in caso di errori su uno dei due server e di non interrompere il servizio di autenticazione e risoluzione dei nomi al momento della manutenzione programmata di uno dei server.

Per i controller di dominio ed il file server, è possibile installare la versione CORE di Windows server 2008 R2, priva di interfaccia grafica, con minore superficie d'attacco e necessità di aggiornamenti, oltre che con footprint ridotto. La gestione del dominio e del file server potrà essere effettuata da remoto con Windows 7 Professional, utilizzando script powershell e la Management Console.

Si è scelto di implementare DFS nonostante la presenza di un unico file server al fine di fornire maggiore flessibilità nei futuri processi di migrazione dei sistemi server; inoltre la scelta faciliterà l'eventuale implementazione di File server sulle sedi periferiche, qualora sia necessario fornire ai client una maggiore velocità nell'accesso alle risorse. Il servizio di screening dei file consentirà di controllare che i contenuti salvati all'interno del file server rispettino le policy aziendali.

I server WSUS e SQL saranno installati sulla versione completa di Windows server 2008, in quanto alcuni servizi dipendono dall'installazione del .Net Framework 3.5/4.0, disponibile sulla versione core con API ridotte.

Il server DOMINO sarà ospitato da Windows 2000 server, in quanto la versione attualmente in uso (Domino 5.0) non è compatibile con la versione 2008 R2 di Windows server.

4.2. Rete

Si è deciso di suddividere la sottorete che andrà ad ospitare i server da quella dei client, a loro volta suddivisi in sottoreti a seconda della sede di appartenenza. L'assegnamento degli indirizzi IP verrà effettuato utilizzando dei DHCP relay collegati ai domain controllers per garantire comunque l'aggiornamento dinamico dei DNS Record. Tale topologia ha il vantaggio di isolare il traffico di broadcast e renderà più facile successive aggiunte di sedi remote, siano esse collegate tramite ponti radio dedicati o utilizzando VPN site-to-site. Sarà inoltre più facile, come successiva implementazione, creare delle route di backup per la ridondanza qualora cada il collegamento principale, introdurre un firewall applicativo tra la rete server e la rete client, o gestire più granularmente l'accesso alla rete utilizzando 802.1x con Access-List basate su IP. Sono state individuate cinque sottoreti:

1. Sottorete Server virtuali.
2. Sottorete client della sede Amministrativa.
3. Sottorete client della sede in Via Beato Pellegrino.
4. Sottorete client della sede di Selvazzano (Centro servizi Bolis).
5. Sottorete DMZ per la pubblicazione di servizi.

4.3. Considerazione sulla sede di Selvazzano

4.3.1. Terminal Server

Previa verifica della compatibilità applicativa, si consiglia di valutare l'utilizzo dei servizi terminal di Windows Server 2008 R2 per la distribuzione dei servizi.
La maggior parte delle applicazioni nella lista è già compatibile con i servizi terminal, che nella versione 7.5 supportano il redirect dell'audio, delle pendrive e parte dell'accelerazione grafica. Sono da valutare le prestazioni in ambiente virtuale per applicazioni specifiche quali fotoritocco e sistemi audio per la riproduzione di MP3. E' da verificare inoltre la compatibilità con i servizi terminal per quanto riguarda il

gestionale della Kibernetes. Qualora il problema nell'implementazione dei terminal server riguardi la compatibilità dei programmi con un sistema server multiutenza, è possibile valutare l'adozione di un'infrastruttura mista Terminal Server + VDI, nell'ottica di una distribuzione successiva anche nelle altre filiali.

4.3.2. Installazione Client-Server con server satellite

Qualora l'implementazione di un'infrastruttura terminal risulti svantaggiosa per l'esperienza utente, si potrà effettuare il normale deployment dei PC, utilizzando un server in locale con i ruoli di:

- **RODC + DNS** per una più veloce autenticazione al dominio anche in caso di caduta del ponte radio.
- **DFS** in replica con la sede centrale per la sola porzione di share che riguarda la sede remota.
- **DFS** in replica con la sede centrale per la porzione di applicazioni con installazione amministrativa.
- **DFS** in replica con la sede centrale per la porzione Profili e dati degli utenti remoti.
- **PrintServer** al fine di pubblicare le stampanti locali in Active Directory.
- **WSUS Server** per la distribuzione degli aggiornamenti.

4.4. Definizione dei server virtuali e dei server fisici

Come precedentemente descritto si è deciso di adottare Vmware ESXi come ambiente di virtualizzazione. Secondo best practices di Vmware, è consigliato mantenere almeno un domain controller esterno all'ambiente di virtualizzazione e di predisporre il servizio di backup su hardware dedicato con accesso diretto all'hypervisor al fine di backuppare le macchina virtuale senza interruzioni di servizio nella loro interezza.
Delle nove macchine individuate precedentemente, quindi, un domain controller ed il server di backup saranno montati su hardware dedicato. Si è deciso, almeno per il momento, di mantenere il firewall attualmente presente in azienda, e di lasciarlo sul server che attualmente lo ospita.
Dunque, solo sei potenziali server saranno ospitati nell'ambiente virtuale.
Si prevede quindi di costruire un ambiente di virtualizzazione che consista di un cluster di due server fisici che permetta sia la distribuzione del carico, sia la movimentazione senza interruzione di servizi delle macchine virtualizzate per la manutenzione dell'hardware. Al fine di raggiungere tale scopo, il cluster di server fisici condividerà lo stesso datastore all'interno di una SAN iSCSI a doppia testa e doppio controller, con collegamenti ridondati su due switch in condivisione del carico, per non lasciare alcun singolo punto di fallimento nell'infrastruttura.
Considerando la criticità dell'infrastruttura di virtualizzazione, è lecito mantenere completamente separato (isolato) il traffico tra la rete che espone i servizi agli utenti, e la rete che offre il servizio di virtualizzazione. A tale scopo sono state individuate due ulteriori subnet:

1. **La subnet di gestione**, dove sarà presente anche il server di backup che dovrà comunicare direttamente con l'hypervisor
2. **La subnet per la comunicazione iSCSI**, all'interno della quale transiterà solo il traffico di I/O tra l'hypervisor e la SAN, per lo storage delle macchine virtuali.

4.5. Backup

Il backup dei dati sarà effettuato nello strato di virtualizzazione da una macchina dedicata. Grazie all'introduzione dello strato (intermedio) di virtualizzazione, al momento del backup richiesto dagli agenti di terze parti, l'hypervisor si occuperà di eseguire delle operazioni di pre-backup che consentiranno di effettuare uno snapshot (a caldo, quindi senza interruzione di servizio) dei dischi virtuali nel primo stato di quiescenza disponibile. Tale snapshot verrà quindi esposto agli agenti di backup per l'archiviazione. La strategia di archiviazione dei dati scelta è di tipo Disk-to-disk-to-tape, che prevede l'archiviazione su disco di più istantanee giornaliere delle macchine, che verranno riversate durante la notte su nastro mediante una tape library SCSI direttamente collegata alla macchina che esegue i lavori di archiviazione (altra ragione per cui dedicare l'hardware alla macchina, è la mancanza di controller scsi virtuali per il collegamento con le tape library).

Questo meccanismo consente di avere le copie più recenti dei backup sempre disponibili (su disco), riducendo drasticamente i tempi di ripristino dei dati, pur mantenendo lo stesso livello di sicurezza e mobilità delle copie su nastro.
Esisterebbe una tecnologia più recente di backup, che elimina la necessità di riversare i dati su nastro spostandoli nel cloud (Disk-To-Disk-To-Cloud), rinviata in quanto al momento da verificare la conformità con le prescrizioni della legge sulla privacy per il trattamento dei dati personali.
Per il solo file server, con l'obbiettivo di velocizzare ulteriormente il ripristino dei singoli files senza coinvolgere il processo di backup, è stato deciso di aggiungere una LUN direttamente collegata alla macchina virtuale che ospiti le shadow copies delle share dei dati. Effettuando un numero di snapshot shadow equivalente a quello dei backup negli istanti che li precedono, verranno esposte agli amministratori di sistema (ed agli utenti), le ultime copie dei dati. Tali copie potranno essere usate per il ripristino veloce dei singoli file o di intere cartelle condivise. Al fine di trarre il massimo vantaggio dalla soluzione proposta, si consiglia di istruire gli utenti all'uso delle shadow copies: rendendo parzialmente autosufficienti gli utenti nel ripristino dei dati, sarà possibile diminuire le richieste di ripristino dei dati per eliminazioni accidentali, con un evidente risparmio economico e di tempo da parte del personale informatico.

4.6. Configurazione del cluster di virtualizzazione

Il cluster di virtualizzazione sarà costituito di due server dimensionati in modo adeguato ad ospitare le macchine virtuali, sia nella configurazione ottimale, con entrambi i nodi del cluster funzionanti, sia in modalità di emergenza (a prestazioni ridotte, ma senza interruzione di servizi), con uno dei due nodi non disponibili. Agli hypervisor verranno esposti due datastore, il primo in RAID 5, che andrà ad ospitare i sistemi operativi, il secondo in RAID 0+1, ad alte prestazioni, che servirà per applicazioni ad intenso traffico di I/O. L'accesso ai datastore sarà garantito lato server da due controller iSCSI in bilanciamento del carico.
Il cluster condividerà i dati mediante l'utilizzo di una SAN iSCSI a doppia testa e doppio controller, al fine di ottenere la massima ridondanza possibile in caso di guasti. Saranno configurate quattro LUN, due che ospiteranno i datastore precedentemente descritti, una LUN formattata NTFS che verrà collegata direttamente al file server per le copie shadow, ed una LUN che verrà esposta al server di backup per l'archiviazione delle copie su disco.
I collegamenti tra i server e la SAN, la rete degli host di virtualizzazione, e le reti delle macchine guest, saranno regolate da due Switch gigabit in ridondanza (spanning tree) e bilanciamento del carico, con supporto a VLAN tagged e untagged. Con l'ottica di poter rafforzare ulteriormente la sicurezza della rete utilizzando l'autenticazione 802.1x e le liste di accesso, si prevede di utilizzare degli switch L3 con funzionalità di routing, ACL dinamiche e supporto all'autenticazione RADIUS.
Un'ipotesi dei collegamenti tra i server, gli switch e la san è evidenziata nello Schema C.

4.7. Requisiti HW e SW

Al fine di soddisfare le specifiche individuate sono state formulate le seguenti ipotesi hardware e software:

- **Numero 2 Server** destinati alla creazione di un ambiente di virtualizzazione:
  - CPU: 2 processori Intel Xeon 2.44Ghz Quad-Core o AMD corrispondenti e certificati per la virtualizzazione con i prodotti nel seguito indicati.
  - RAM: 24Gb DDR3 ECC 1.066Mhz o 1.333Mhz.
  - HD: N.2 dischi 140 GB configurati RAID 1 SCSI –SAS;
  - DVD: SuperMulti Double Layer Serial ATA;
  - Schede di Rete: N. 8 schede 1Gb, espandibili a 10; (2 possibilmente ottimizzate per iSCSI)
  - Alimentazione doppia
  - Rack mountable
- **Numero 2 Switch**:
  - Stackable Switch Layer 3/4 managed
  - 24 porte 10/100/1000 in rame
  - Almeno 2 slot per moduli SFP Gigabit
  - Almeno 2 slot per adapter a 10Gbit Ethernet.

    - Supporto IPv6, SSLv3, SSHv2, OSPFv2, DiffServ QoS, Non Blocking, 802.1X, Auth RADIUS.
    - Access-List control dinamico
    - Supporto ad almeno 10 Vlan taggate.
    - Rack mountable
- **Disk Storage System**:
    - Tecnologia iSCSI con doppio controller
    - Doppia testa
    - Quattro interfacce host, cache 2 GB
    - dischi SAS hot-pluggable 15K, per un totale di almeno 3TB lordi
    - Alimentazione doppia
- **Backup:**
    - N1 Autoloader 6 cassette LT02, SCSI.
- **Software**:
    - N. 1 VMware vSphere 4 Essentials Plus Bundle per 3 hosts (Massimo 2 processori per host e 6 cores per processore)
    - N. 1 Basic Support/Subscription VMware vSphere Essentials Plus Bundle per un anno
    - N. 2 MS Windows Server Enterprise 2008R2 OLP NL Gov
- **Altri Server**
    - N. 1 rack 2U,
        - 4 GB RAM
        - N. 2 dischi SAS 146 GB, RAID 0/1 SAS,
        - idonei a ospitare sistemi operativi Linux SuSE, R.H.- Windows 2003/8 Server,
        - N. 6 Schede rete 1Gb
    - N. 1 rack 2U
        - 4 GB RAM
        - N. 2 dischi SAS 146 GB
        - Idonei a ospitare sistemi operativi Linux SuSE, R.H.- Windows 2003/8 Server
        - N. 4 Schede rete 1Gb
        - controller SCSI per gestire il sistema Autoloader già indicato
- **Armadio Rack**
    - N.1 armadio rack adeguato con almeno 27 U libere, prese di alimentazione. Tutti i dispositivi indicati in precedenza devono essere ospitati nell'armadio e devono essere dotati di tutti i dispositivi fisici necessari (staffe e viti incluse)
    - KWM tastiera e mouse per gestire almeno 8 server fisici
    - Monitor 21" esterno + tastiera + mouse.
- **Servizi**
    - Installazione e configurazione di tutti i componenti hardware e software forniti
    - Garanzia tre anni, materiali e manodopera, interventi in loco, tempo intervento 4 ore, 8 ore al giorno, 5 giorni alla settimana.

La disposizione dei server sarà effettuata come indicato nello Schema B.

4.8. Previsione dei Costi

La soluzione prevede dei **costi di progetto** stimati pari a circa €56.000, suddivisi in:

- **€50.000:** Come *costo di costruzione del progetto*, che comprende l'acquisto dell'hardware e del software necessario alla virtualizzazione come prevista dal documento. I valori sono stati ricavati effettuando una media dei costi di listino di più produttori considerando hardware con specifiche compatibili a quelle indicate nell'analisi dei requisiti.
- **€6.000:** Come *costo di avviamento dell'infrastruttura*, che comprende la configurazione del cluster di virtualizzazione e la migrazione dei servizi e delle applicazioni di terze parti nell'ambiente virtuale.

Si stimano dei **costi di gestione** periodici, sostenuti per l'utilizzo del sistema pari a:

- **€4.000 all'anno dopo i primi 3 anni:** Assimilabili come *costi di manutenzione*, che comprendono le spese ordinarie e straordinarie per la riparazione di guasti hardware della SAN.
- **€6.000 all'anno:** *Assimilabili come costi sistemistici* di gestione dell'infrastruttura.
- **€5.300 all'anno:** assimilabile come *costo di esercizio*, dovuto al consumo annuale della nuova infrastruttura. La stima dei costi di esercizio è stata calcolata effettuando una media dei consumi dichiarati da più produttori per hardware equivalenti a quelli indicati nell'analisi dei requisiti.

Un maggiore dettaglio dei costi del progetto ed il loro calcolo è visibile in Figura 2 e Figura 3 nell'appendice.

E' chiaro che sarà necessario effettuare una valutazione più approfondita dei costi quando si riceveranno le offerte reali da parte dei fornitori dell'hardware, all'apertura del bando: solitamente per acquisti di questa entità, i produttori di hardware praticano delle scontistiche d'eccezione.

4.9. Analisi dei benefici

4.9.1. Benefici operativi

4.9.1.1. Maggior Disponibilità

La virtualizzazione ci consente di aumentare la disponibilità del sistema. Se consideriamo la disponibilità come la probabilità che il servizio o il componente usato in condizioni definite, si trovi in condizioni operative ed utilizzabile in qualsiasi momento; l'introduzione del cluster di virtualizzazione con la movimentazione automatica delle macchine in caso di guasto di uno dei nodi del cluster, consente di minimizzare l'impatto sulla disponibilità dei servizi. Le macchine verranno infatti migrate automaticamente presso il nodo ancora operativo senza interruzioni di servizio visibili. La soluzione proposta consente inoltre di slegare la disponibilità dall'affidabilità dei singoli componenti, come accade invece per i sistemi non virtualizzati, legandola invece alla disponibilità dei gruppi di componenti ridondati del cluster, il cui tempo medio tra un guasto e l'altro è decisamente minore e può essere riparato senza interruzione di servizio.

4.9.1.2. Maggior Scalabilità del sistema

Un sistema si dice scalabile quando è possibile aggiungere ulteriori funzionalità senza doverne modificare le caratteristiche fondamentali. Attualmente la scalabilità del sistema è minima. I server lavorano al massimo della loro capacità e una qualsiasi necessità di diversificazione delle funzionalità richieste, un incremento di dati o utenti costringerebbe ad una revisione completa dell'infrastruttura. La virtualizzazione consentirà di specializzare le macchine virtuali nella fornitura di un singolo servizio, rendendo possibile la distribuzione del carico in base alle necessità del momento e la prioritizzazione di alcune macchine rispetto ad altre, o, al più, qualora sia necessaria maggiore potenza di calcolo complessiva, renderà più agevole l'aggiunta di un nuovo nodo al cluster. Qualsiasi operazione di espansione verrà effettuata nello strato di virtualizzazione, risultando del tutto trasparente all'utente.

4.9.1.3. Ambienti di test affidabili

Modifiche che richiedono operazioni a caldo su dati reali o aggiornamenti che impattano sulle funzionalità di base del sistema potranno essere testate su una fedele riproduzione dell'ambiente di produzione derivata dal ripristino di un backup recente: questo consentirà di ridurre i rischi derivanti da errori umani o incompatibilità. Qualsiasi problema riscontrato in fase di implementazione potrà essere documentato e risolto prima di passare alla fase di produzione.

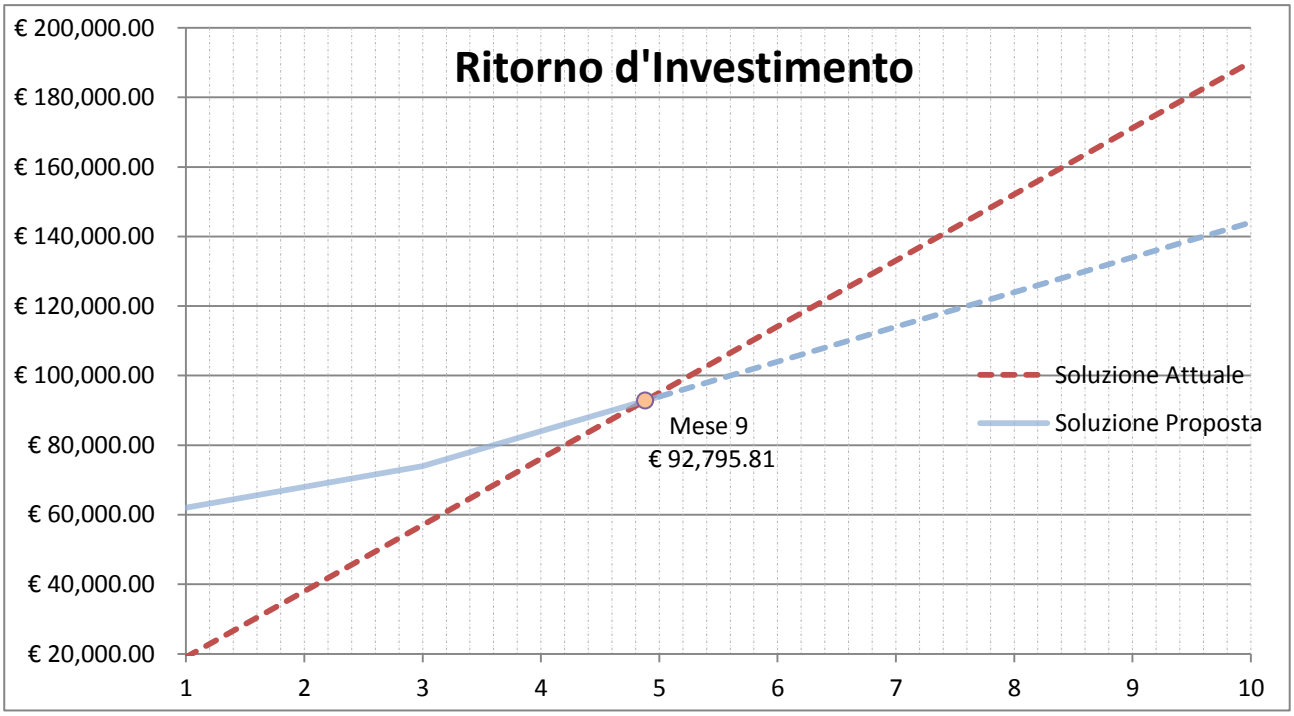
4.9.2. Benefici Strategici

L'adozione di una tecnologia di virtualizzazione consentirà all'organizzazione di includere nei successivi piani di investimento, nel rinnovo del parco macchine e nel provisoning di servizi le opzioni offerte dagli ultimi ritrovati della tecnologia. Qualora risulti necessario, sarà possibile estendere la virtualizzazione allo strato applicativo concentrando l'intera potenza di calcolo necessaria all'esecuzione delle attività dell'utenza all'interno del CED, utilizzando tecniche di Terminal Services e VDI. Questo consentirà di sostituire le postazioni di lavoro con delle semplici macchine adibite alla presentazione dei dati, concentrando tutte le criticità, le attività di manutenzione e gli investimenti all'interno della sala server. Consolidando le postazioni di lavoro all'interno del ced, si potrà estendere la scalabilità e l'affidabilità

garantite dalla virtualizzazione anche alle macchine client degli utenti. La sostituzione delle workstation con macchine a bassa potenza e quindi basso consumo permetterà di accentrare ulteriormente le spese energetiche all'interno della sala macchine.

4.9.3. Benefici Economici

L'attuale costo della sala server, tra costi di esercizio dovuti al consumo di energia elettrica e costi di manutenzione hardware e software è di circa €19.000. Il maggior costo è dovuto alla manutenzione hardware delle macchine, ormai datate e fuori garanzia. La soluzione proposta consente di ridurre i costi di gestione di un 43% nei primi 3 anni e di un 19% negli anni successivi. Come si può facilmente vedere nel grafico riportato sotto, il costo dell'intero progetto, sia utilizzando una formula di assistenza triennale che quinquennale, consente di produrre il ritorno di investimento economico rispetto all'attuale soluzione, prima della data di ammortamento quinquennale prevista.



5. Ipotesi di lavoro

La migrazione dei servizi sarà gestita internamente per quanto riguarda Active Directory ed i servizi core dell'infrastruttura, e demandata alle aziende che si occupano della manutenzione dei programmi, per quanto riguarda la parte applicativa in manutenzione.

5.1. Tempi del processo di migrazione

Parte dei tempi del processo di migrazione dipendono dalla disponibilità dei fornitori ad effettuare la migrazione delle applicazioni. E' stato sviluppato un diagramma di massima dei tempi di inizio e fine progetto.
Le attività che si svolgeranno durante il processo di migrazione sono state suddivise in base alla loro dipendenza ed alle funzionalità che andranno ad interessare.

5.1.1. Installazione infrastruttura (5 giorni)

All'arrivo del materiale il fornitore si occuperà di configurare l'intero ambiente hardware come richiesto dal capitolato. Sarà configurata la VLAN di gestione (e backup) delle macchine Vmware e della san, quindi la VLAN dedicata alla SAN e verranno esposti alle macchine i datastore. I due hypervisor verranno configurati in modo da permettere lo spostamento manuale a caldo delle macchine virtuali, al fine di garantire l'alta disponibilità delle macchine in caso di guasto o manutenzione.

Sarà dunque possibile configurare la VLAN che offrirà la connettività alle macchine virtuali, secondo lo schema prestabilito.
Completata la configurazione dell'ambiente virtuale, è prevista una prova di ridondanza per ogni punto di fallimento dell'infrastruttura:

- Prova di migrazione a caldo delle macchine
- Prova di ridondanza degli switch
- Prova di ridondanza della SAN.

Provata l'affidabilità della configurazione si potrà procedere con la configurazione delle macchine virtuali.

5.1.2. Creazione ambiente virtuale (10 giorni stimati)

Il macroprocesso che andrà a creare l'ambiente virtuale è stato diviso in sottoprocessi a seconda delle funzionalità che andranno ad interessare. Ogni sottoprocesso dipende dalla disponibilità all'interno degli hypervisor delle macchine virtuali, con installati gli ultimi aggiornamenti, ma saranno relativamente indipendenti l'uno dall'altro. Una nota a parte merita il processo che si concluderà con la migrazione del dominio con funzionalità 2008 R2 che verrà trattato nell'apposita sezione.

5.1.2.1. Migrazione del Dominio

La migrazione del dominio richiede la preparazione dello schema (foresta e dominio) di active directory con le estensioni per Windows server 2008 R2, al fine di poter installare il primo domain controller 2008. E' possibile estendere il dominio direttamente sul server che attualmente ospita l'unica copia di active directory, tuttavia, al fine di rendere il processo più sicuro, è consigliato installare un secondo DC 2003 temporaneo in replica, migrare i ruoli FSMO ed effettuare l'estensione dello schema Offline. In caso di errori sul processo di preparazione, sarà infatti possibile ripristinare la macchina virtuale con la vecchia copia dello schema, (o nel caso peggiore, rimuovere manualmente il domani controller ed effettuare il seize dei ruoli su quello rimanente) e correggere i problemi prima di rieffettuare l'estensione.
Esteso il dominio, sarà possibile cominciare l'installazione del primo domain controller 2008, e controllare la buona riuscita delle repliche. Gli si potranno quindi assegnare i cinque ruoli FSMO e lo si configurerà come Root Time Server nella gerarchia del dominio.
L'attività si concluderà con la demozione del server 2003 e l'upgrade delle funzionalità del dominio a 2008 R2. Per depromuovere il domain controller 2003, sarà necessario aver completato tutte le attività di migrazione previste dalla creazione dell'ambiente virtuale, in quanto la depromozione rimuove il database Active Directory installando un database degli utenti locali. Altri servizi configurati sul server potrebbero quindi smettere di funzionare. Si consiglia quindi di rimuovere dalla rete il domain controller quando non ospiterà più altri servizi necessari al funzionamento della rete.

5.1.2.2. Migrazione del File Server

La migrazione del File server prevede una prima attività di configurazione del servizio DFS (Distributed File System), quindi una migrazione dei dati. La migrazione dei dati potrà essere effettuata usando la replica DFS tra l'attuale fileserver e quello appena configurato, oppure migrando i dati offline: nel secondo caso gli utenti non avranno accesso ai dati per l'intera durata dell'attività.
Qualora sia necessario configurare il fileserver anche come print server, l'attività andrà svolta successivamente.

5.1.2.3. Migrazione del database server

La migrazione del Database Server prevede l'intervento esterno dei fornitori dei software aziendali. Ai fornitori verrà esposto il server già configurato con il servizio attivo, con le credenziali di amministratore di macchina e del database e tutta l'assistenza occorrente al fine di migrare i database sulla nuova istanza.
I fornitori si occuperanno di migrare il database e renderlo, qualora ce ne fosse bisogno, compatibile con la nuova versione installata sul server, SQL Server 2008 R2. Il fornitore dovrà anche occuparsi di migrare i client sulla nuova istanza.
A quel punto sarà possibile disinstallare la vecchia istanza di SQL Server sul server 2003.

5.1.2.4. Installazione Servizi WSUS

L'installazione del software WSUS non dipende da altri processi. E' prevista la scelta di un sottoinsieme di client pilota e di una settimana per popolare il server con gli aggiornamenti prima di attestare tutti i client della rete. In questo modo sarà possibile risolvere eventuali problemi solo per un sottoinsieme ridotto di client. Sebbene la distribuzione di patch ed aggiornamenti sia importante, il processo non è critico in quanto il suo malfunzionamento non compromette il lavoro degli utenti.

5.1.2.5. Migrazione del server Domino

L'attuale server che ospita domino (versione 5.0) verrà virtualizzato in toto con un processo Physical-to-Virtual. Domino 5.0 infatti non è compatibile con la versione 2008R2 di Windows server, e la migrazione dal sistema Windows 2000 che attualmente ospita Domino al sistema Windows 2003 non è conveniente.

6. Ulteriori sviluppi

6.1. Ristrutturazione Active Directory

Attualmente la disposizione delle OU e degli utenti è generica, non rispecchia logicamente la posizione all'interno dell'organizzazione, e rende difficile l'individuazione dei computer, che quindi vengono nominati in base all'utente che lo utilizza. E' buona norma assegnare ai computer un numero identificativo univoco slegato dall'utenza, e piuttosto utilizzare la tabella "gestito da" di active directory per riconoscere l'utente che normalmente utilizza la postazione. Si consiglia di ristrutturare la disposizione delle OU rispecchiando, per quanto possibile, l'ubicazione dei PC e di ordinare le utenze in base al ruolo all'interno della struttura.
La policy anti-conficker può essere eliminata, ripristinando quindi i permessi di default sul servizio SVCHOST, semplicemente distribuendo l'aggiornamento KB958644 (operazione facilitata dall'implementazione di un server WSUS), pubblicato nell'Ottobre 2008. Rimuovendo le ACL personalizzate sui servizi sarà possibile implementare un sistema di assistenza remota su richiesta, integrato nei sistemi Microsoft Windows di default, configurando gli utenti abilitati a fornire l'assistenza direttamente in Active Directory.
Si consiglia di attivare il servizio Windows Firewall sui client, utilizzando le group policy per configurare le eccezioni.
Le workstation sono tutte Windows 2000 o superiore, si consiglia quindi di disattivare il traffico NetBIOS da group policy per i computer interni alla rete, e configurare l'opzione per disattivare il servizio nel DHCP.

Un'alternativa valida all'upgrade del dominio è una migrazione in toto degli utenti e dei computer verso un dominio nuovo al fine di non ereditare vecchi problemi e di ripristinare le policy di default del dominio e dei domain controllers. Tali policy sono state modificate contrariamente alle best practices di Microsoft, che invece consigliano di effettuare una sovrascrittura con policy ad hoc a priorità più alta.

6.2. Implementazione della rete perimetrale e proxying autenticato

Attualmente la rete è protetta dagli accessi esterni tramite un 3-Leg firewall basato su linux, che effettua anche servizio di proxying basato su IP. La soluzione presenta tre problemi:

1. Un attacco mirato a prendere il controllo del firewall effettuato con successo, garantirebbe l'accesso alla rete interna della struttura.
2. L'autenticazione basata su IP costringe l'utilizzo di IP statici, eliminando i vantaggi che derivano dall'uso di un server DHCP, costringendo ad usare lease riservati basati su MAC Address.
3. Le regole di filtering non sono omogenee: lo stesso utente avrebbe filtri differenti a seconda della workstation in uso.

E' possibile risolvere il problema con l'implementazione di una rete perimetrale basata su due firewall in cascata come presentato nello Schema E dell'Appendice. La soluzione presenta numerosi vantaggi:

- Un attacco eseguito con successo al firewall esterno, garantirebbe l'accesso alle sole risorse esposte nella rete perimetrale, costringendo un successivo attacco al firewall interno per poter accedere alla rete locale.

- Il firewall interno può essere configurato con autenticazione RADIUS o Kerberos su active directory per il servizio di proxying, spostando il controllo d'accesso sull'utente piuttosto che sull'IP della macchina. In questo modo, l'utente, qualsiasi sia il terminale utilizzato, erediterà sempre le stesse ACL per la navigazione.
- Un proxy le cui ACL sono basate sull'autenticazione Kerberos piuttosto che sull'ip del client consente di impostare regole più granulari.
- Con l'occasione si potrebbe acquistare un prodotto che fornisca Malware Inspection oltre che i semplici servizi di URL filtering basati sulle categorie.

Esempio di prodotto: *Forefront Threat Management Gateway 2010*.

6.3. Unione posta interna ed esterna

Attualmente l'ente utilizza due sistemi di posta elettronica diversi, uno per la posta interna (Notes su Domino 5) ed uno per la posta esterna (Pop3 + SMTP in hosting presso terzi). Tutti gli utenti hanno una cassetta di posta su domino, ma non tutti hanno l'equivalente esterno. Inoltre, alcuni gruppi di utenti necessitano di monitorare una casella di posta condivisa: attualmente il problema è stato affrontato condividendo la password dell'utente che scarica la posta.
Si consiglia di unificare i servizi, utilizzando un server di posta aggiornato alle tecnologie più recenti, magari con l'integrazione in active directory che consenta il Single-Sign-On, implementando regole per gestire chi può ricevere/inviare posta da/verso l'esterno, nonché l'utilizzo di gruppi di distribuzione o Alias per la gestione delle cassette di posta condivise.

6.4. Uniformità del software

Sono presenti versioni differenti di programmi della famiglia office e corel, nonché sistemi operativi differenti. Si consiglia, sia per migliorare ed uniformare l'esperienza utente, sia per ridurre il numero di aggiornamenti da memorizzare sul server WSUS, di upgradare tutto il software ad una versione omogenea.

6.5. Sistema di monitoraggio globale

L'intera rete manca di un sistema di monitoraggio e configurazione delle periferiche integrato e di notifica in caso di errori, malfunzionamenti Hardware e software, e guasti. Si consiglia l'adozione di un programma che permetta di monitorare ed uniformare le configurazioni di client e server, che automatizzi l'installazione dei programmi ed il patch management, e che, se richiesto, possa creare dei report con la configurazione hardware delle macchine presenti nel dominio. Il programma deve supportare sia macchine Windows che linux, e supportare la raccolta dei trap SNMP per il monitoraggio delle periferiche di networking.
Il programma faciliterà l'amministrazione della rete da parte del sistemista che prenderà in carico la gestione del sistema.
Con il supporto al Wake On Lan, sarà possibile avviare i PC remotamente ad ore prestabilite per l'installazione degli aggiornamenti e spegnerli nuovamente. Schedulando l'installazione durante le ore notturne sarà possibile applicare le ultime patch senza influire sull'operatività dell'utente.

Programmi consigliati: *System Center Suite* (Operation Manager e Configuration Manager).

6.6. File server e RODC nelle sedi periferiche

Sono state rilevate le seguenti problematiche presso le sedi periferiche:

1. La caduta del collegamento tra la sede centrale e le sedi periferiche compromette seriamente la possibilità di lavorare degli utenti.
2. Il traffico dati all'interno del tunnel di collegamento è eterogeneo e non controllato. Questo impatta negativamente sull'utilizzo della quantità di banda del tunnel.

Al fine di garantire una maggiore qualità del servizio ed una maggior granularità su quanto effettivamente transita all'interno del canale di comunicazione, si consiglia l'installazione di un server periferico per ogni filiale sufficientemente grande a giustificarne la spesa.

Tale server potrebbe funzionare come partner DFS/print server per i dati necessari alla filiale periferica e Domain controller in sola lettura al fine di:

1. Garantire agli utenti una maggiore velocità di accesso ai dati.
2. Garantire agli utenti la disponibilità dei dati in caso di caduta del collegamento.
3. Garantire agli utenti un più veloce processo di autenticazione e risoluzione dei nomi.
4. Garantire agli utenti la disponibilità del processo di autenticazione e risoluzione dei nomi in caso di caduta del collegamento.
5. Consentire agli utenti di cercare ed installare le stampanti autonomamente, pubblicando le stampanti in active directory e rendendo disponibili i driver firmati digitalmente.
6. Ottimizzare la banda disponibile nel collegamento tra le due filiali, accertandosi che nel canale transiti solo il traffico server-to-server.

6.7. Virtualizzazione dello strato applicativo (TS) o Virtualizzazione del desktop (VDI)

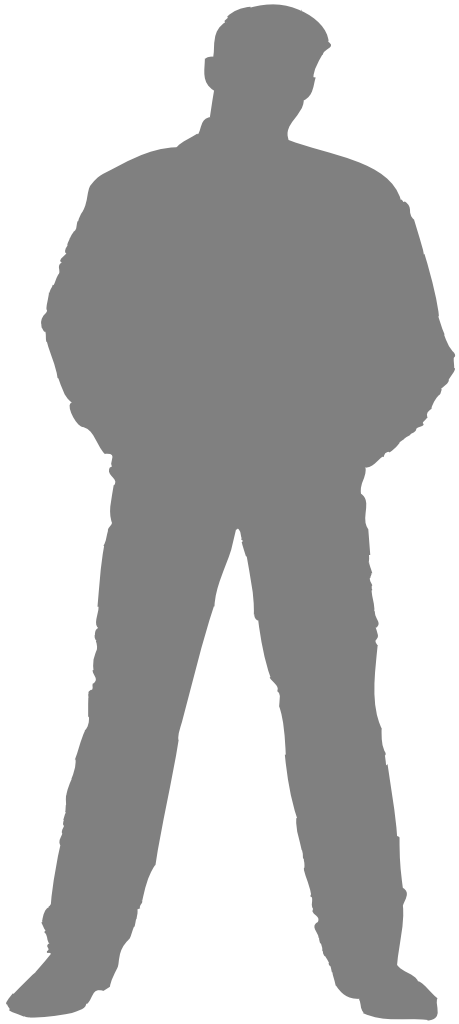
La struttura presenta una sede centrale dove è ospitato il ced ed una sede periferica collegata tramite ponte radio (è in fase di costruzione una seconda sede, anch'essa verrà collegata tramite ponte radio). Sarebbe opportuno analizzare la rete e verificare la compatibilità dei programmi esistenti con un'infrastruttura terminal server o VDI. La virtualizzazione dello strato applicato o del desktop consente infatti di spostare il traffico dalle reti periferiche direttamente all'interno del data center e consente un maggiore controllo sul traffico intersito, principalmente RDP o equivalente.
Spostando l'operatività completamente all'interno del data center, sarà possibile ridurre lo sforzo di amministrazione e manutenzione delle postazioni periferiche, di ridurre la superficie di attacco e la necessità di aggiornamenti delle workstation, e di manutentare più efficacemente le applicazioni personalizzate riducendo il numero di installazioni. E' tuttavia indispensabile effettuare una prima fase di analisi per verificare che tutte le applicazioni utilizzate all'interno dell'infrastruttura siano compatibili con i servizi terminal, o nel caso del deployment di un'infrastruttura VDI, che applicazioni ad intenso utilizzo di accelerazioni grafiche o CPU vengano gestite correttamente al fine di non penalizzare l'esperienza utente.

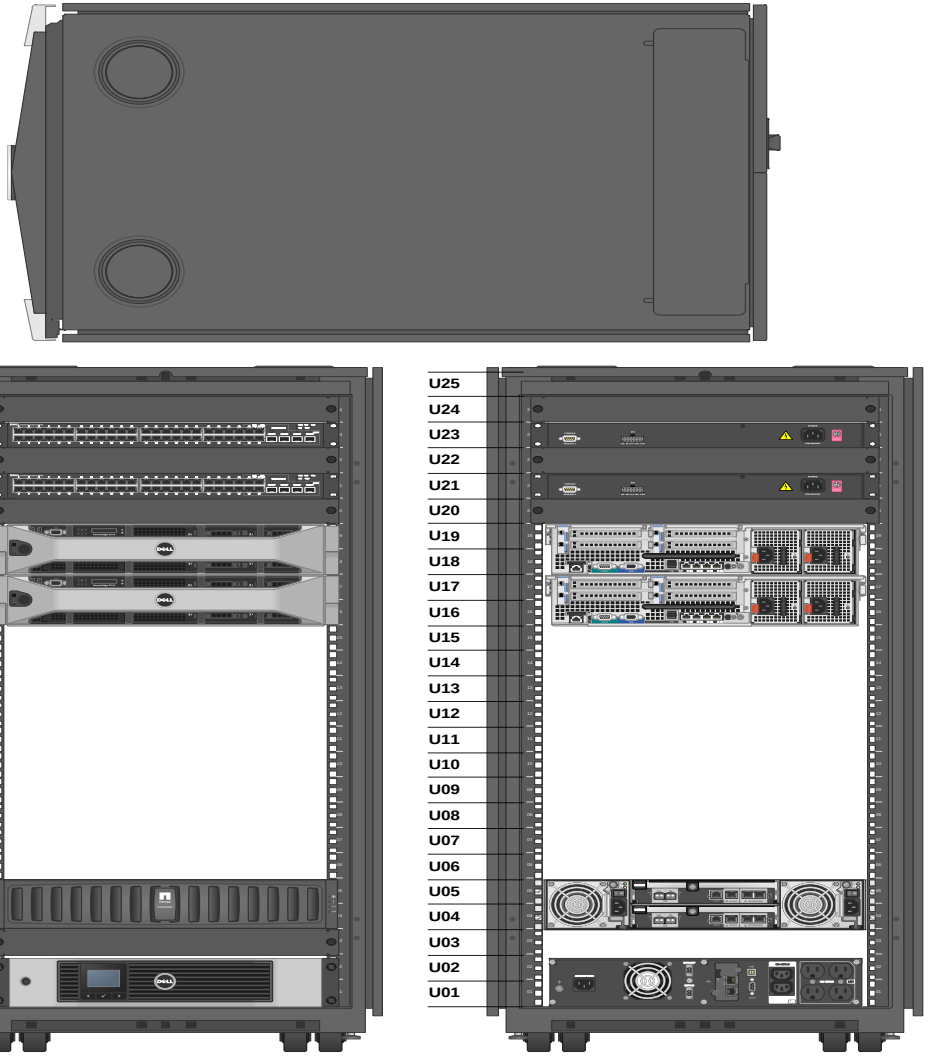
7. Conclusioni

In un campo in continuo sviluppo come l'Information Technology, l'adozione di tecniche di virtualizzazione è indispensabile non solamente per l'adeguamento tecnologico, ma anche per una più efficiente gestione delle risorse. Il consolidamento dei server garantirà all'Istituto di Riposo per Anziani l'ottimizzazione, e quindi una conseguente riduzione, dei consumi, un tema centrale in un mondo dove il costo dell'energia è costantemente in aumento. Nell'ottica di un accentramento delle risorse nei data center, la soluzione proposta è il primo passo verso un'infrastruttura completamente virtualizzata e ridondata che ridurrà il carico di lavoro dei tecnici informatici aumentando il rendimento e l'operatività degli utenti. Inoltre, la riduzione del Total Cost of Ownership dell'intera sala macchine, garantirà un Ritorno d'Investimento a lungo termine sicuramente apprezzato dal consiglio di amministrazione dell'Ente.
Alla luce di quanto indicato nel documento, il progetto è stato approvato dal consiglio di amministrazione dell'Istituto di Riposo per Anziani ed è quindi possibile passare alla stesura del capitolato.

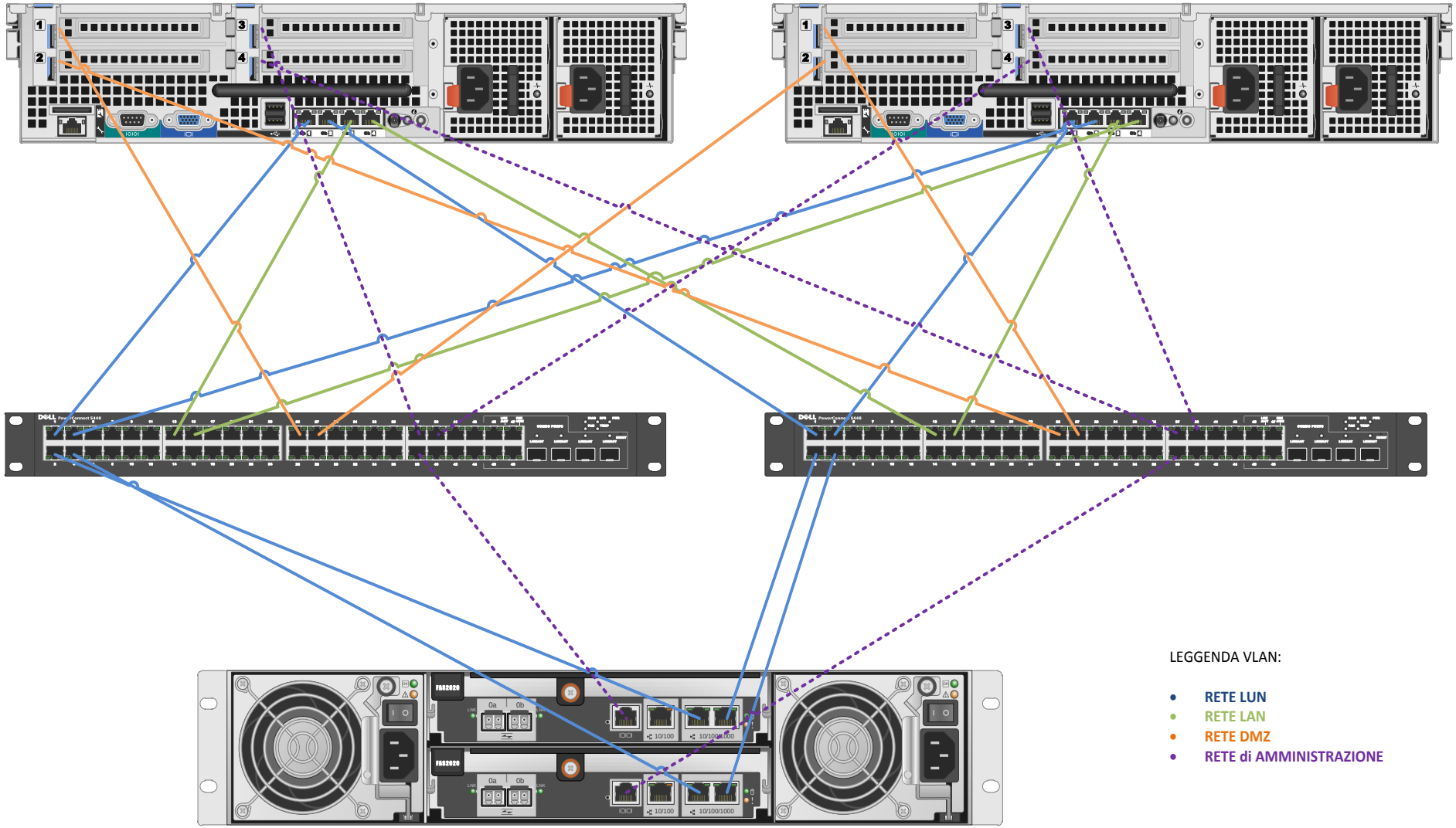
Appendice A : Schemi e figure

Schema B

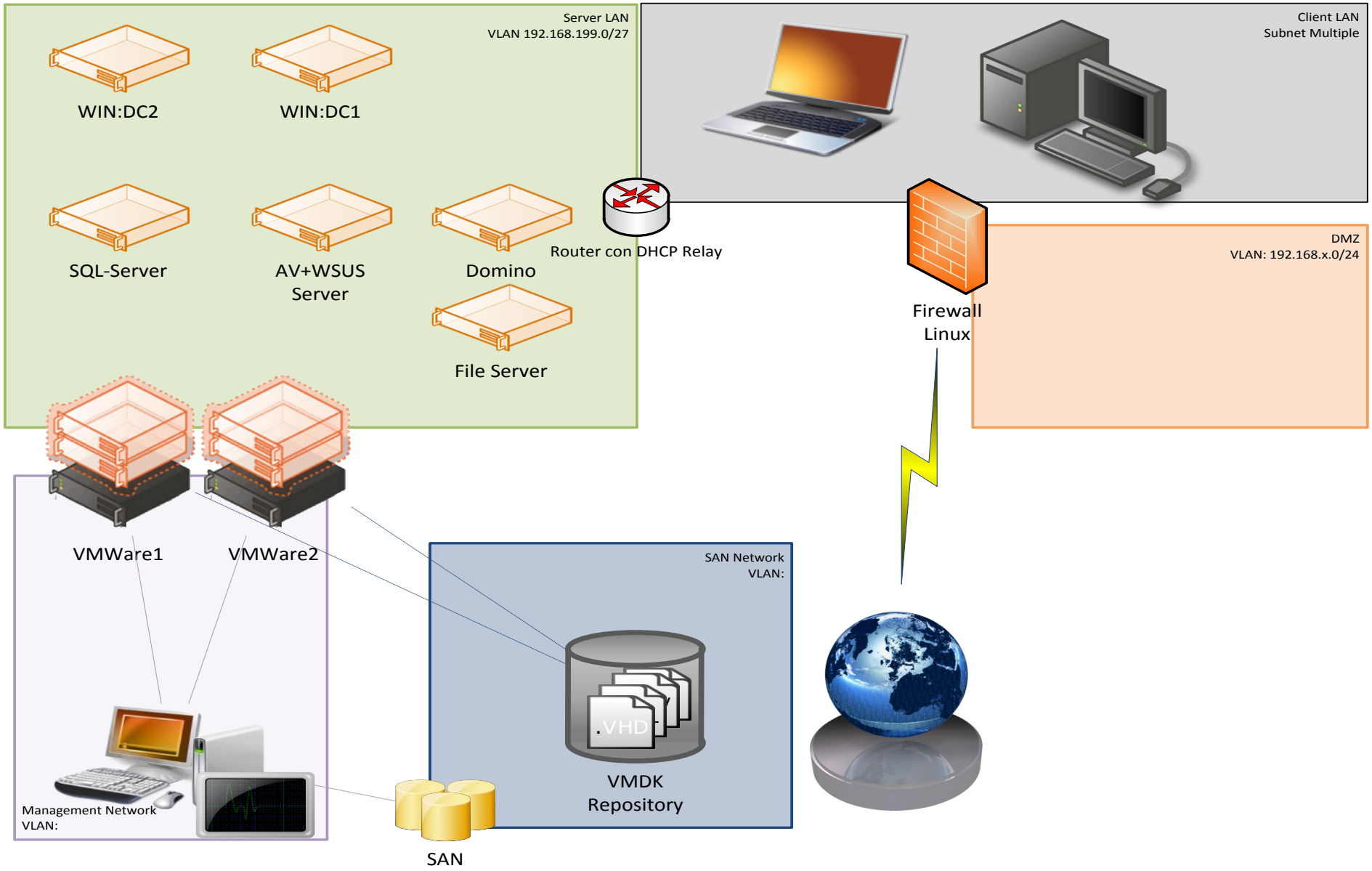




Schema C


LEGGENDA VLAN:
RETE LUN
RETE LAN
RETE DMZ
RETE di AMMINISTRAZIONE

Schema D


Server LAN
VLAN 192.168.199.0/27
WIN:DC2
WIN:DC1
SQL-Server
AV+WSUS
Server
Domino
File Server
Router con DHCP Relay
Client LAN
Subnet Multiple
Firewall
Linux
DMZ
VLAN: 192.168.x.0/24
VMWare1
VMWare2
SAN Network
VLAN:
.VHD
VMDK
Repository
Management Network
VLAN:
SAN

Schema E

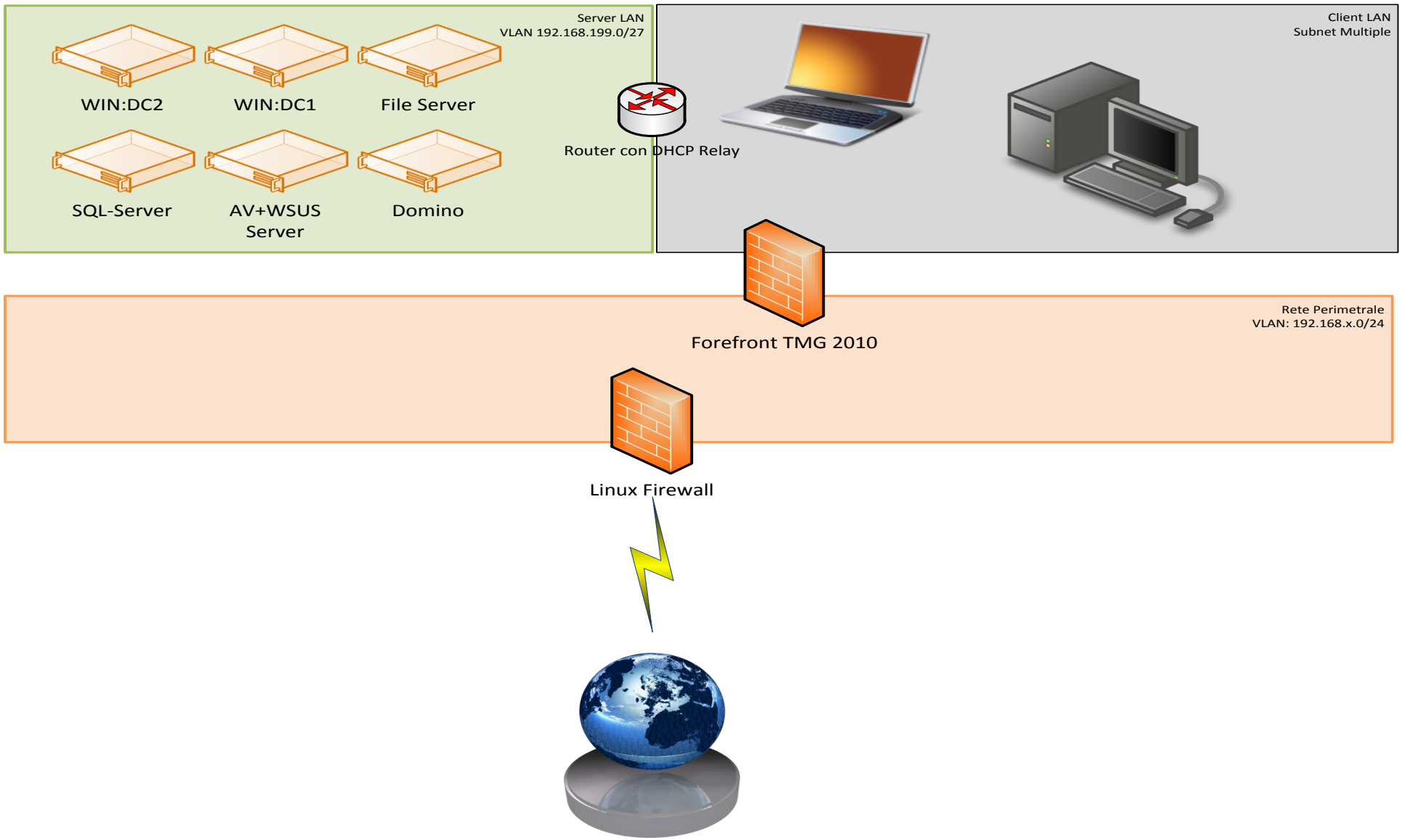

Server LAN
VLAN 192.168.199.0/27
WIN:DC2
WIN:DC1
File Server
SQL-Server
AV+WSUS Server
Domino
Router con DHCP Relay
Client LAN
Subnet Multiple
Forefront TMG 2010
Rete Perimetrale
VLAN: 192.168.x.0/24
Linux Firewall

Figura 1

Modello	kW/h	€/kWh	kW/day	kW/month	kW/yr
Server IBM xseries 236 TIPO 8841-1AG	0.67	€ 0.17	€ 2.73	€ 82.01	€ 984.10
Server FUJITSU SIEMENS primergy	0.35	€ 0.17	€ 1.43	€ 42.84	€ 514.08
Server PROLIANT DL 380G4	0.58	€ 0.17	€ 2.35	€ 70.38	€ 844.56
Server HP Proliant ML 380R	1.00	€ 0.17	€ 4.08	€ 122.40	€ 1,468.80
SWITCH PRO CURVE 2810-48G	0.09	€ 0.17	€ 0.38	€ 11.26	€ 135.13
SWITCH PRO CURVE 2810-24G	0.05	€ 0.17	€ 0.20	€ 5.88	€ 70.50
Totale			€ 11.16	€ 334.76	€ 4,017.17
Costi di manutenzioni HW parco Server:					€ 4,000.00
Costi di assistenza sistemistica:					€ 11,000.00
TCO Annuale Sala server:	€ 19,017.17				

Figura 2

Costi di Costruzione		Qty	Tot
Server di virtualizzazione	€ 6.500,00	2	€ 13.000,00
SAN	€ 15.000,00	1	€ 15.000,00
Switch L3 full managed	€ 1.500,00	2	€ 3.000,00
Server backup e DC Secondario	€ 2.500,00	2	€ 5.000,00
VMWare Software	€ 3.000,00	1	€ 3.000,00
Windows Server Ent 2008	€ 1.500,00	2	€ 3.000,00
Backup Software	€ 1.000,00	2	€ 2.000,00
Windows Server Std 2008	€ 1.000,00	2	€ 2.000,00
Tape Library	€ 4.000,00	1	€ 4.000,00
Totale:			€ 50.000,00
Costo di avviamento previsto:			€ 6.000,00
Costo di progetto:			**€ 56.000,00**

Figura 3

Costi di Manutenzione						
Supporto:			**3 Anni**		**4° e 5° Anno**	
SAN Support: 24x7 max 4h		Included in price			€ 2,000.00	
Servers, Tape: 9hr/5gg +NextBusiness day		Included in price			€ 2,000.00	
Costi Sistemistici					€ 6,000.00	
Costi di esercizio:						
Modello	**kW/h**	**€/kWh**	**cost per h**	**cost per D**	**€ per month**	
Server di virtualizzazione	0.87	€ 0.17	€ 0.15	€ 3.55	€ 106.49	
Server di virtualizzazione	0.87	€ 0.17	€ 0.15	€ 3.55	€ 106.49	
SAN	0.68	€ 0.17	€ 0.11	€ 2.75	€ 82.62	
Switch L3 full managed	0.10	€ 0.17	€ 0.02	€ 0.41	€ 12.24	
Switch L3 full managed	0.10	€ 0.17	€ 0.02	€ 0.41	€ 12.24	
Server Backup	0.50	€ 0.17	€ 0.09	€ 2.04	€ 61.20	
DC Secondario	0.50	€ 0.17	€ 0.09	€ 2.04	€ 61.20	
Totale			€ 0.61	€ 14.75	€ 442.48	€ 5,309.71
TCO annuale sala server primi 3 anni:	€ 11,309.71	41%	di riduzione dei costi annuali			
TCO annuale sala server anni superiori al 3°:	€ 15,309.71	19%	di riduzione dei costi annuali			