ALMA MATER STUDIORUM – UNIVERSITA' DI BOLOGNA
CAMPUS DI CESENA
SCUOLA DI SCIENZE

CORSO DI LAUREA IN SCIENZE E TECNOLOGIE INFORMATICHE

EVOLUZIONE TECNOLOGICA IN AMBITO END USER COMPUTING: UN CASO D'USO BASATO SU HORIZON WORKSPACE PORTAL

Relazione finale in
Reti di Calcolatori

Relatore
Gabriele D'Angelo

Presentata da
Maurizio Maltoni

Sessione III
Anno Accademico 2013/2014

“Anche se hai già tirato con l'arco varie volte,
continua a prestare attenzione
al modo in cui sistemi la freccia,
e a come tendi il filo.”
Paulo Coelho.

INDICE

INTRODUZIONE

L'obbiettivo del progetto di cui tratterà questa tesi è costituire un ambiente intuitivo e facilmente utilizzabile dall'utente finale che permetta di accedere sia alle applicazioni aziendali sia ai desktop virtuali da qualsiasi dispositivo effettui l'accesso: computer, smartphone o tablet.
Negli ultimi anni è diventato sempre più importante avere la possibilità di lavorare in mobilità e in qualsiasi momento. Grazie alle recenti tecnologie di End User Computing messe a disposizione da VMware è possibile virtualizzare qualsiasi applicazione Windows e renderla disponibile tramite Internet a qualsiasi utente la richieda, indifferentemente dal sistema operativo o dal luogo in cui si trova.

Il primo capitolo sarà discorsivo e tratterà dell'evoluzione che hanno visto le architetture informatiche negli ultimi anni; trattandosi di una tematica molto ampia si è deciso di focalizzarsi sul punto di vista dell'utente finale e della sua interazione con il sistema. Questo capitolo metterà in evidenza la direzione che sta prendendo il mercato negli ultimi anni, spingendo sempre di più sulla diffusione di servizi per l'utente tramite Internet.

Il secondo capitolo mostrerà la fase di progettazione dell'ambiente: simulando l'analisi di uno scenario fittizio, analizzando le richieste e le necessità del cliente, descrivendo le tecnologie che si andranno ad utilizzare e lo scenario di implementazione. Questo capitolo sarà un vero e proprio documento di progettazione denominato “Proof of Concept”.

Il terzo capitolo infine sarà puramente tecnico e illustrerà come è stato implementato l'ambiente, descrivendo le caratteristiche dei sistemi e le procedure utilizzate in fase di realizzazione.

CAPITOLO 1:
DIVERSE TIPOLOGIE DI INFRASTRUTTURE INFORMATICHE

1.1 Client/Server

1.1.1 Computer Terminali e Mainframe

Agli inizi degli anni 70 fecero la loro comparsa i primi sistemi terminali detti “Dumb Terminals”, questi erano composti da un monitor per visualizzare le informazioni e una tastiera per fornire l'input da parte dell'utente. Questi dispositivi non possedevano né un'unità disco né un processore, di conseguenza non avevano alcuna capacità di calcolo o di memorizzazione di dati in locale [1].
I terminali comunicavano con un punto di elaborazione centrale detto Mainframe tramite porta seriale o cavo coassiale inviando sul canale di trasmissione ogni carattere digitato dall'utente.

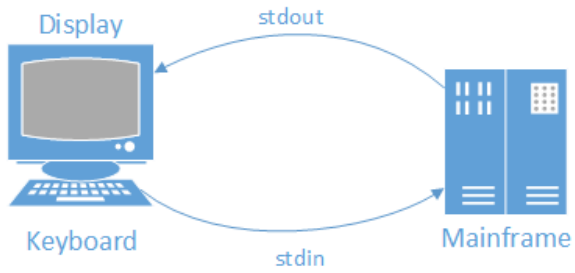


Figura 1.1.1.1 Comunicazione tra Terminale e Mainframe

Il Mainframe era un computer dalle grandi dimensioni e con un'alta capacità di elaborazione, i principali utilizzatori di queste enormi e costosissime macchine erano enti governativi, università e grandi aziende.

Il Mainframe si occupava dell'intera elaborazione dei dati provenienti dai terminali ed era quindi il punto debole dell'infrastruttura, in caso di guasto i dipendenti non potevano lavorare.

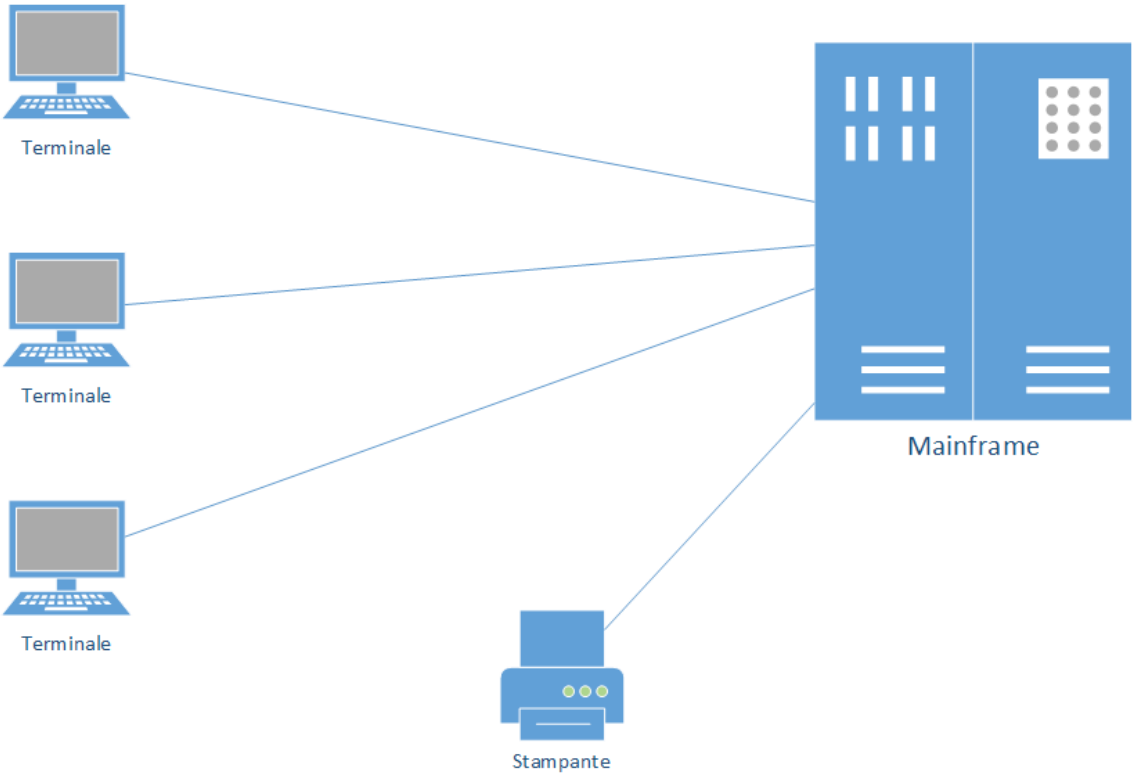


Figura 1.1.1.2 Esempio di architettura Terminali e Mainframe

Alla fine degli anni 70 vennero sviluppati terminali più intelligenti, ovvero dotati di una piccola unità di elaborazione. Grazie a questo primitivo processore la macchina poteva spedire i caratteri al mainframe a blocchi, senza più interromperlo ad ogni carattere digitato. Questa funzionalità permetteva agli utenti di modificare blocchi di testo prima di spedirli e metteva a disposizione dell'utente un set di comandi destinati al terminale e non al mainframe, come ad esempio la possibilità di svuotare lo schermo o controllare la posizione del cursore sul documento [2].

Grazie alla riduzione dei costi della memoria e dell'evoluzione dei microprocessori queste macchine intelligenti arrivarono presto a costare meno dei vecchi Dumb Terminal, favorendone la diffusione. Tuttavia con l'aumentare del numero di produttori sul mercato si creò troppa diversificazione tra i comandi utilizzabili per dare istruzioni ai terminali. Nel 1976 venne pubblicato ECMA-48, conosciuto successivamente come "ANSI escape sequence", questo standard tentò di risolvere il problema creando un set di comandi comune tra i vari modelli di terminali [3].

Con lo sviluppo dei microprocessori si aggiunsero funzionalità sempre maggiori ai terminali, fino a che non furono resi totalmente indipendenti dal Mainframe; a questo punto si cominciò a parlare di Personal Computer (PC).

1.1.2 Personal Computer e Server

Fu all'inizio degli anni 80 che esplose la diffusione dei Personal Computer (PC). L'hardware dei sistemi casalinghi, utilizzati principalmente per i videogiochi, ormai non aveva più distinzioni da quello dei sistemi utilizzati in ufficio.

Le aziende cominciarono ad adottare queste macchine su larga scala grazie al rapido abbassamento dei costi di produzione e assemblaggio dei PC, la capacità di emulare un Terminale e la retro-compatibilità con sistemi già esistenti.

I PC diventano sempre più facili da utilizzare per l'utente, soprattutto grazie alla diffusione dei software con interfaccia grafica e di un innovativo dispositivo di puntamento: il mouse.

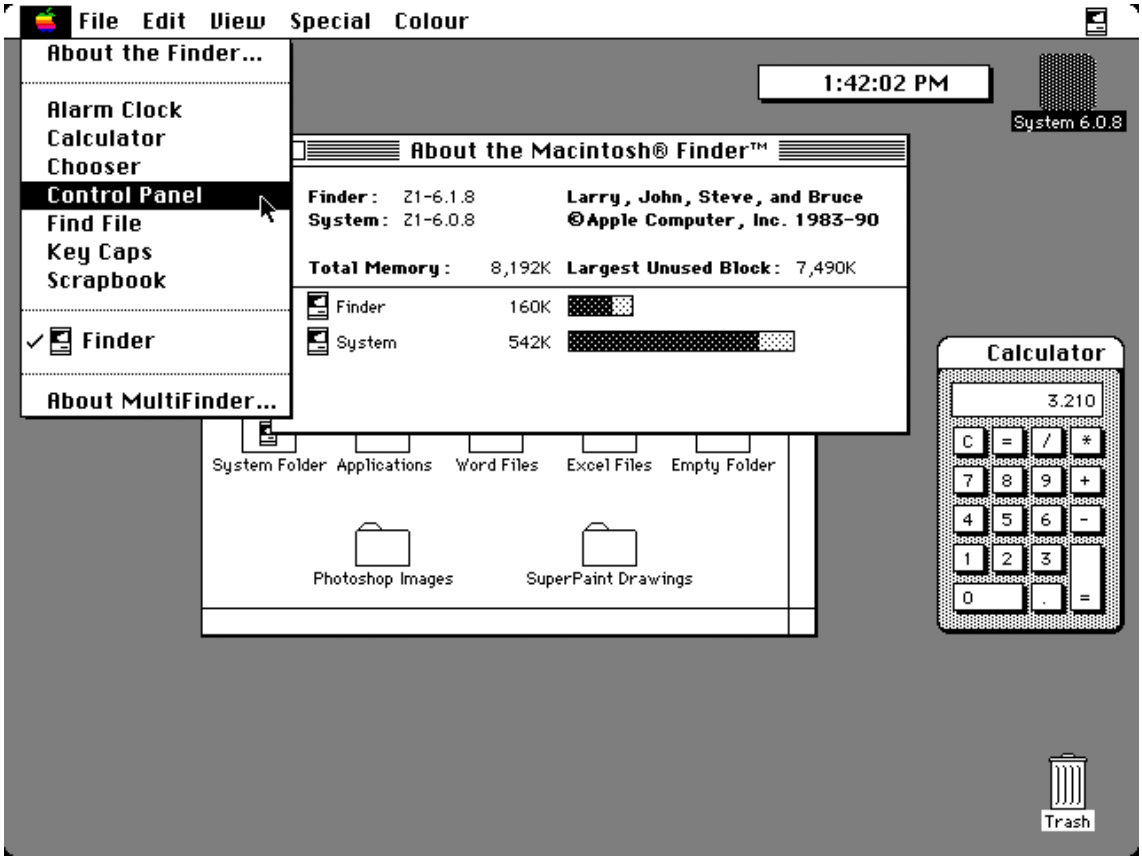


Figura 1.1.2.1 L'interfaccia grafica di System 6 di Apple Computer, il sistema operativo del Macintosh
fonte: http://en.wikipedia.org/wiki/File:System6.0.8MacII.png

I Mainframe vennero sostituiti dai Server, macchine molto meno costose, dalle dimensioni ridotte e molto più simili ai PC; anche aziende di piccole/medie dimensioni adesso potevano permettersi infrastrutture informatiche che prima erano accessibili solo a grandi aziende.

1.1.3 Architettura Client/Server

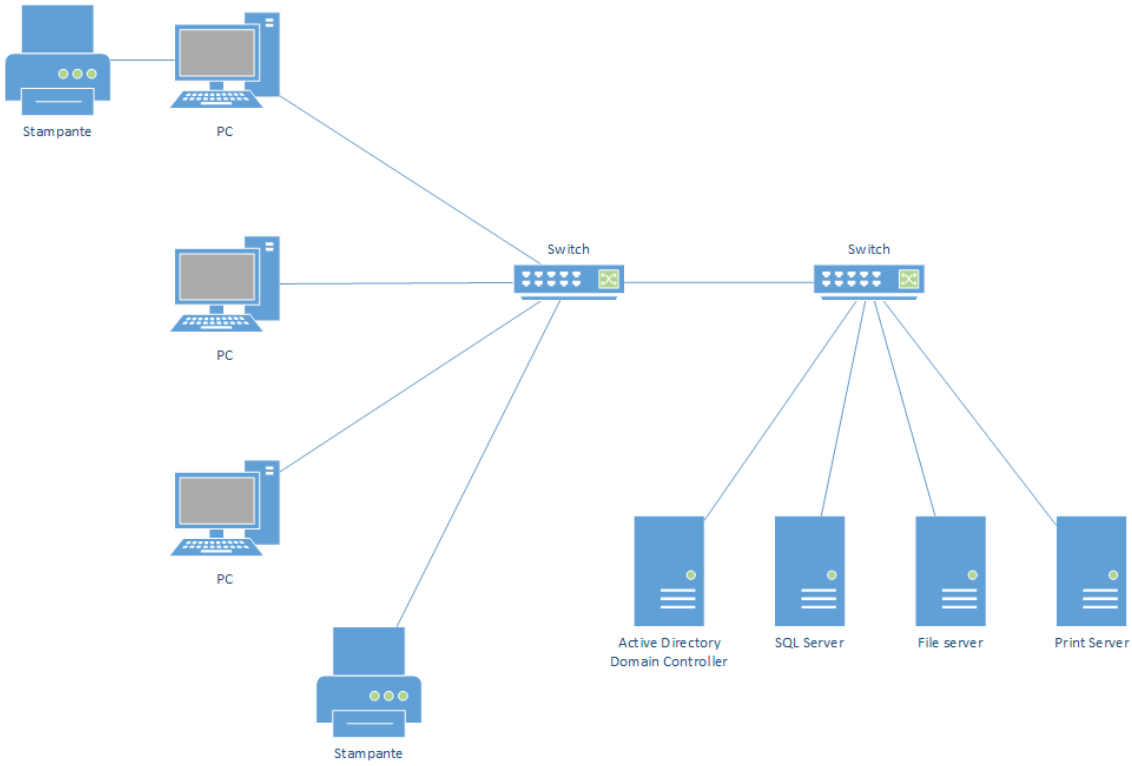


Figura 1.1.3.1 Esempio di architettura Client/Server

L'architettura Client/Server divide l'elaborazione tra Client e Server, queste due entità possono risiedere sulla stessa macchina, ma solitamente si trovano su Computer diversi nella stessa rete.

Un Server è un Computer sul quale viene eseguito un programma che fornisce determinati servizi ad un Client. La particolarità dei Server è che possono fornire i loro servizi ad un grande numero di Client simultaneamente.

Il Client è un programma con cui si interfaccia l'utente, esso esegue le richieste verso il server, trasmette dati e processa le informazioni ottenute.

Il modello Client/Server porta molteplici vantaggi che gli hanno permesso di diventare il modello di architettura di rete dominante, come il poter condividere risorse come file e stampanti con altri utenti in luoghi diversi [4].

Un esempio classico è il Web Server che contiene file relativi a siti web e li spedisce tramite Internet ai Client che ne fanno richiesta; uno dei Web Server più diffusi al mondo è Apache [5].

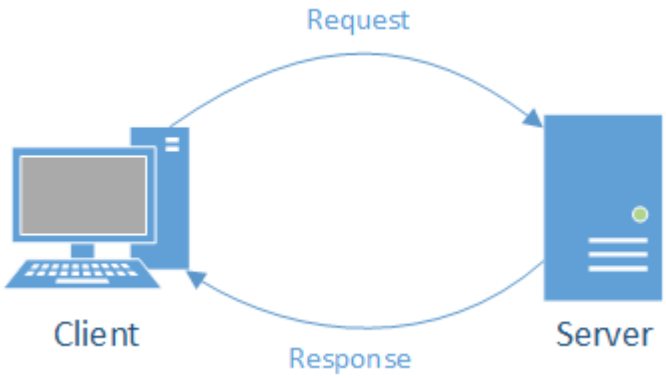


Figura 1.1.3.2 Comunicazione Client/Server

1.2 Virtual Desktop Infrastructure (VDI)

1.2.1 Definizione

Grazie alle nuove tecnologie di virtualizzazione si sta tornando ad un architettura più simile a quella Terminal/Mainframe, implementando un'infrastruttura dove i desktop virtuali degli utenti risiedono insieme a Server virtuali in un unico Server fisico centrale. Questo modello di architettura viene definito Virtual Desktop Infrastructure (VDI).

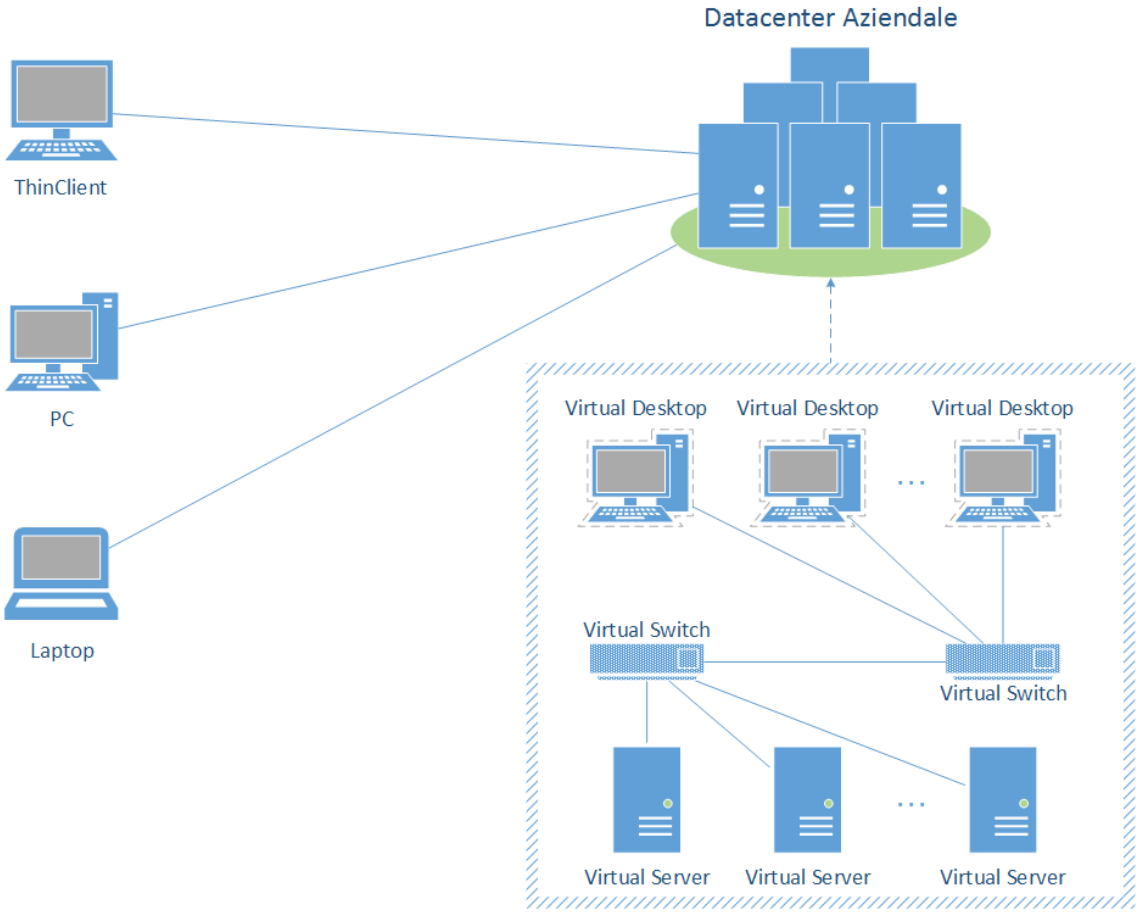


Figura 1.2.1.1 Architettura VDI

All'interno del server centrale viene simulata una vera e propria architettura Client/Server creando Desktop virtuali, Server virtuali e addirittura reti virtuali gestite da dispositivi di rete virtuali.

In questa specifica architettura l'utente utilizza un sistema Terminale per accedere al proprio Desktop virtuale, questo Terminale può essere: un Personal Computer, un ThinClient, uno ZeroClient o qualsiasi altro dispositivo su cui è installata l'applicazione che si occupa del trasferimento dati con il Server centrale.
I principali protocolli utilizzati per il trasferimento dei dati tra Terminale fisico e Desktop virtuale sono due: Microsoft RDP e Teradici PCoIP.
Entrambi i protocolli sono performanti e offrono un ottimo livello di sicurezza [6], tuttavia PCoIP si presta meglio per il trasferimento tramite WAN poiché è nativamente compresso e offre algoritmi che riducono o aumentano automaticamente la qualità delle immagini trasferite in relazione al grado di congestione della rete per mantenere un livello di esperienza utente ottimale [7].

1.2.2 Differenze tra ThinClient e ZeroClient

ThinClient e ZeroClient sono entrambi sistemi terminali piccoli a basso costo e bassissimi consumi che implementano l'hardware minimo necessario per gestire i protocolli di trasferimento dati tra il dispositivo e il Desktop virtuale.

I ThinClient possiedono una memoria su cui viene caricato un sistema operativo embedded e possono quindi contenere dati e lanciare qualche applicazione. Questi dispositivi possono gestire periferiche USB collegate localmente e possiedono svariate applicazioni Client di connessione remota. I ThinClient necessitano di manutenzione regolare poiché vengono spesso rilasciati aggiornamenti firmware.

I ZeroClient sono sistemi senza disco e senza processore, una volta accesi avviano il Client di connessione e non possono fare altro se non connettersi al Desktop remoto; questo porta vantaggi a livello di sicurezza, poiché non avendo un sistema operativo la macchina non può essere compromessa e se viene smarrita o rubata non contiene dati aziendali sensibili. Questo tipo di Terminale è vincolato all'utilizzo del protocollo di connessione per cui è stato nativamente programmato.

I ZeroClient sono più economici rispetto ai ThinClient e necessitano di una manutenzione praticamente nulla in quanto il firmware del microprocessore è da aggiornare solo quando viene rilasciata una nuova versione del protocollo e ciò avviene molto raramente. Sono inoltre considerati dispositivi plug&play poiché non richiedono configurazioni particolari e anche alla prima accensione è sufficiente collegarli alla rete e connettersi al Desktop virtuale per cominciare a lavorare, grazie a questa semplicità possono essere installati anche da personale non qualificato [8].

1.2.3 Vantaggi e Svantaggi di VDI rispetto ad una tradizionale infrastruttura Client/Server

Esistono sia vantaggi che svantaggi in un'infrastruttura VDI, in seguito è riportata una breve analisi dei principali pro e contro.

Manutenzione

Per gestire una tipica infrastruttura Client/Server è necessario appoggiarsi a software di manutenzione di terze parti, che effettuino monitoraggio dello stato di salute dei Client e permettano di gestire installazioni di Software e aggiornamenti da remoto. Spesso è anche necessario recarsi fisicamente davanti ad alcuni Client che richiedono manutenzione particolare a seguito di problemi Software o Hardware.

In un ambiente VDI gli aggiornamenti e la manutenzione vengono gestiti dai responsabili IT in modo rapido e completamente trasparente all'utente. Un tecnico può collegarsi al computer da qualsiasi luogo se c'è necessità di eseguire una manutenzione specifica e non deve più recarsi fisicamente sul luogo in cui si trova il PC.

Costi ridotti per l'Hardware

Con un'infrastruttura VDI è possibile usare ThinClient economici e con bassi consumi come terminali per l'accesso ai desktop virtuali. Un valore aggiunto dei ThinClient è la dimensione, essendo macchine molto piccole rispetto a un PC tradizionale lasciano più spazio a disposizione sopra o sotto la scrivania dell'utente.

Inoltre il Client di connessione è indipendente dal dispositivo e dal sistema operativo, è quindi possibile riciclare Computer dismessi installandovi una distribuzione Linux e il Client di connessione per utilizzarli come Terminali di accesso ai Desktop virtuali.

Sicurezza

VDI permette un alto livello di sicurezza poiché i dati aziendali non sono contenuti sui Terminali, se un dispositivo viene smarrito o rubato i dati sono al sicuro sul Server. È inoltre possibile bloccare l'accesso dai Desktop virtuali a periferiche collegate ai Terminali quali ad esempio chiavette USB, evitando il furto di dati sensibili.

Filiali remote

In caso l'azienda abbia filiali remote diventa complesso effettuare manutenzioni sui PC, aumentando i costi per l'azienda per finanziare gli spostamenti dei tecnici IT. Spesso accade che le filiali ricevono in ritardo manutenzioni necessarie sulle macchine o aggiornamenti di applicativi, diminuendone così la produttività. Con VDI anche i Desktop delle sedi remote sono centralizzati sul Server e permettono un rapido accesso ai tecnici per manutenzione e aggiornamenti. Altro importante fattore da considerare è la distanza tra il Client e il Server di un applicativo, ad esempio un gestionale che interroga un database installato nel Datacenter aziendale; una filiale soffre di lenti tempi di risposta perché tutte le interrogazioni devono attraversare Internet, nel caso di VDI invece i Desktop risiedono nella stessa rete locale del Database abbattendo i tempi di accesso ai dati [9].

Single Point of Failure

In quanto l'architettura è concentrata su un unico punto, se dovesse esserci un guasto ai server l'intera infrastruttura collasserebbe. Per ovviare a questo possono venire implementate tecnologie di ridondanza dei server e di Disaster Recovery per garantire un'alta affidabilità dei sistemi.

Da non sottovalutare è anche il rischio di un attacco Denial of Service che se lanciato sui server centrali può bloccare tutta l'infrastruttura.

Grosso investimento iniziale

Per realizzare un ambiente VDI è necessario un considerevole investimento iniziale per acquistare i sistemi Server che necessitano di rilevanti risorse Hardware per contenere tutti i sistemi virtuali.

Accurata pianificazione

Per sviluppare un'infrastruttura VDI è richiesta un'attenta e approfondita pianificazione che va dal dimensionamento delle risorse dei server alle politiche di ottimizzazione dei desktop virtuali [10].

Dimensionamento rete

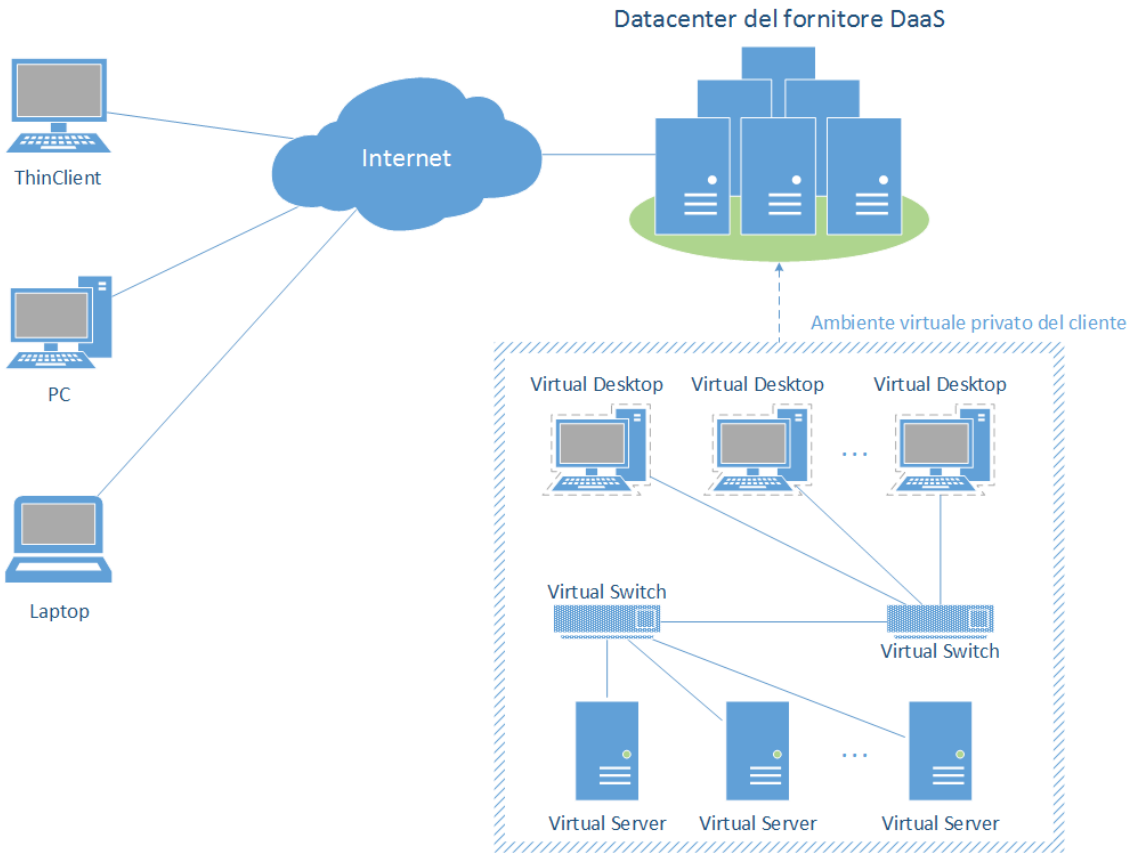
Un ambiente VDI richiede una considerevole quantità di banda di rete e una bassa latenza per offrire un'esperienza utente accettabile. Nell'ambito della rete locale una normale rete Gigabit è sufficiente per un'azienda di medie dimensioni; quando però si comincia a parlare di connessioni dall'esterno bisogna tenere in considerazione la capacità di Upstream della connessione Internet del Datacenter.

Un dipendente tipico che svolge regolari mansioni di ufficio richiede mediamente una banda dai 50 ai 150 Kilobit per secondo, supponendo la banda in Upstream dimensionata a 1,5 Megabit per secondo si possono gestire dagli 8 ai 24 utenti che lavorano in contemporanea da remoto [11].

1.3 Desktop as a Service (DaaS)

1.3.1 Definizione

Grazie alla continua evoluzione delle nuove tecnologie di Cloud Computing sta nascendo un nuovo modello di infrastruttura che deriva dallo stesso paradigma del modello Software as a Service (SaaS), questa architettura viene definita “Desktop as a Service” (DaaS).



Mentre SaaS fornisce sistemi software agli utenti finali senza bisogno di installazione su Computer o Server, il modello DaaS fornisce veri e propri Desktop virtuali, senza bisogno di installare un ambiente VDI nella propria sede.

DaaS è una gigantesca infrastruttura VDI multi-tenant, installata e gestita da un fornitore di servizi informatici che crea e configura Server e Desktop virtuali in base alle richieste e le necessità del cliente; quest'ultimo potrà quindi accedere ai Desktop da remoto utilizzando dei Terminali e una connessione a Internet.

1.3.2 Vantaggi e Svantaggi di DaaS

I vantaggi:

Non è necessario installare server in locale evitando così grosse spese iniziali per le macchine e per le licenze, viene semplicemente pagata una quota giornaliera o mensile al fornitore di servizi per ogni computer virtuale.

I desktop virtuali sono nativamente accessibili tramite Internet, questo significa che un utente può accedere al suo desktop virtuale da qualsiasi dispositivo e ovunque si trovi, senza bisogno di effettuare configurazioni complesse e rischiare di aprire vulnerabilità nella propria rete aziendale; la sicurezza è gestita interamente dal fornitore di servizi [12].

Gli svantaggi:

Utilizzando DaaS si è vincolati al fornitore a cui ci si sta affidando, che mantiene tutti i sistemi e i dati del cliente. La migrazione da un fornitore ad un altro è quindi una procedura complessa che va progettata nei minimi dettagli per evitare di causare disagi ai dipendenti o bloccarne l'attività lavorativa.

Per usufruire al meglio di un servizio DaaS è necessaria una connessione alla rete Internet consona e dimensionata in relazione al numero di utenti connessi in contemporanea.

CAPITOLO 2:
PROOF OF CONCEPT

2.1 Premessa

Un Proof of Concept è un documento che dimostra la fattibilità dell'implementazione di un determinato prodotto o servizio, sviluppando un prototipo in un ambiente di test che possa simulare al meglio l'applicazione in un contesto reale.
Durante lo sviluppo del progetto descritto in questa tesi è stato redatto anche il relativo Proof of Concept che verrà illustrato in parte in questo capitolo per quanto riguarda gli aspetti più discorsivi, e in parte nel terzo capitolo dove verranno invece trattate le modalità di implementazione e gli aspetti più tecnici.
Per realizzare un Proof of Concept che si avvicini il più possibile alla realtà è stata simulata la richiesta di questo documento da un cliente fittizio (dal nome “Fittizia Spa”) che ha varie problematiche da risolvere e necessità da soddisfare.

2.2 Scenario

La società Fittizia Spa opera da 20 anni nel settore della micro elettronica, da sempre ha eccelso nell'installazione e manutenzione di sistemi basati su reti di sensori in grado di monitorare ambienti molto estesi. Con l'avvento del Cloud Computing e delle nuove tecnologie di End User Computing è diventato necessario aggiornare il loro sistema informatico interno, in modo da ottimizzare il lavoro del proprio personale tecnico e commerciale.
La società opera sull'intero territorio italiano e quando è necessario mandare un tecnico a svolgere una manutenzione questo resta fuori sede per qualche giorno (il tempo necessario per svolgere la manutenzione più la verifica dell'effettiva risoluzione del problema).

Allo stato attuale un tecnico che deve recarsi in loco ad eseguire una manutenzione dovrà prima recarsi in ufficio, accedere al suo computer, controllare la descrizione del problema e la posizione geografica del sensore, stampare un documento di riepilogo e partire.
Una volta recatosi sul luogo svolgerà la manutenzione e compilerà un report giornaliero.
Durante questo periodo potrebbero esserci tempi morti, ad esempio: durante il viaggio, nell'attesa durante l'aggiornamento di un firmware o durante il periodo di attesa in loco a intervento concluso per verificare che il problema non si ripresenti.
Durante questi tempi il tecnico potrebbe svolgere altre operazioni quali: effettuare test di altri sistemi di sensori da remoto, controllare la mail o studiare documentazione tecnica.
Gli impiegati che viaggiano per l'Italia per effettuare sopralluoghi o confrontarsi con i clienti hanno un set di problematiche molto simile.

2.3 Obiettivi

Obiettivo del progetto è fornire ai dipendenti un elevato livello di produttività in un'ottica di mobilità assoluta.
Si realizzerà quindi un sistema in grado di permettere sia ai tecnici sia agli impiegati accesso completo alla loro postazione Desktop, alle applicazioni e ai dati aziendali da qualsiasi dispositivo.
In questo modo il tecnico potrà leggere documentazione tecnica da un Tablet durante il viaggio per recarsi dal cliente o consultarla in caso di bisogno durante la manutenzione.
Un impiegato potrà confrontare la situazione di un nuovo cliente con progetti realizzati in precedenza, consultare dati tecnici dei sensori per realizzare un preventivo su misura, o più semplicemente accedere alla mail aziendale in qualsiasi momento.
Con questa nuova infrastruttura verrà inoltre implementata una politica di Bring Your Own Device, grazie a questo la società ridurrà i costi di implementazione evitando l'acquisto di dispositivi aziendali, e il dipendente si troverà a proprio agio ad utilizzare un dispositivo a lui familiare.

Grazie a tutte le tecnologie sopra presentate si otterrà inoltre un ottimo livello di sicurezza, le comunicazioni col server avverranno tramite canale criptato e se un dipendente dovesse smarrire il suo dispositivo o se gli venisse sottratto nessuno potrebbe accedere ai dati aziendali, poiché questi risiedono solo sul server all'interno dell'azienda.

Per realizzare un'infrastruttura con queste caratteristiche verrà implementato un servizio di Cloud privato gestito internamente dal personale IT dell'azienda. All'interno del Datacenter verrà creata un'infrastruttura VDI in grado di fornire l'accesso sia ai desktop virtuali dei dipendenti che alle applicazioni aziendali anche al di fuori della rete locale.

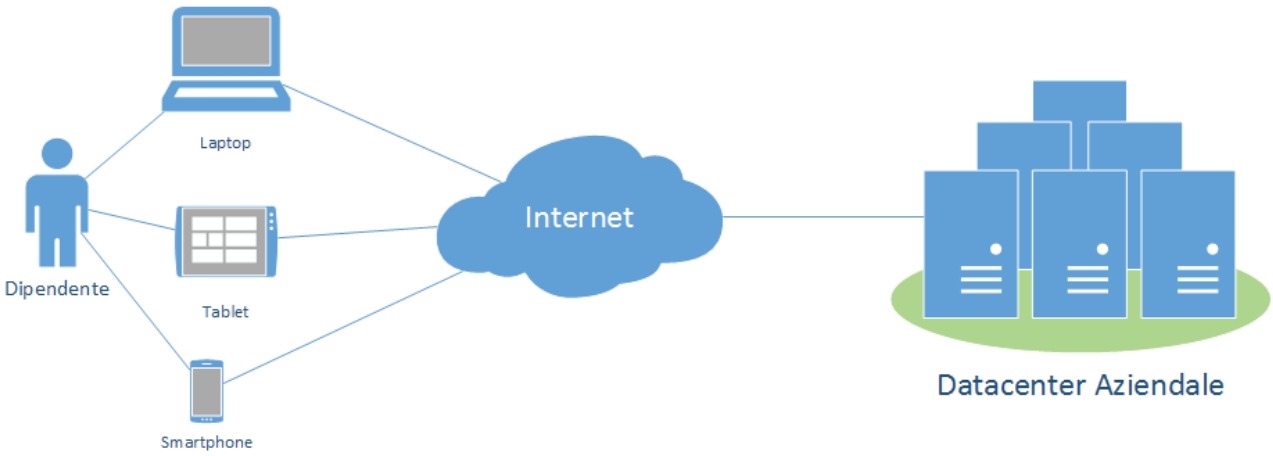


Figura 2.3 Schema logico dal punto di vista dell'utente

2.4 Descrizione Tecnologie

Il progetto è stato interamente realizzato su piattaforma VMware, sui server virtuali sono stati installati sia sistemi Windows che Linux. Di seguito è riportata una descrizione delle varie componenti utilizzate nella realizzazione del progetto.

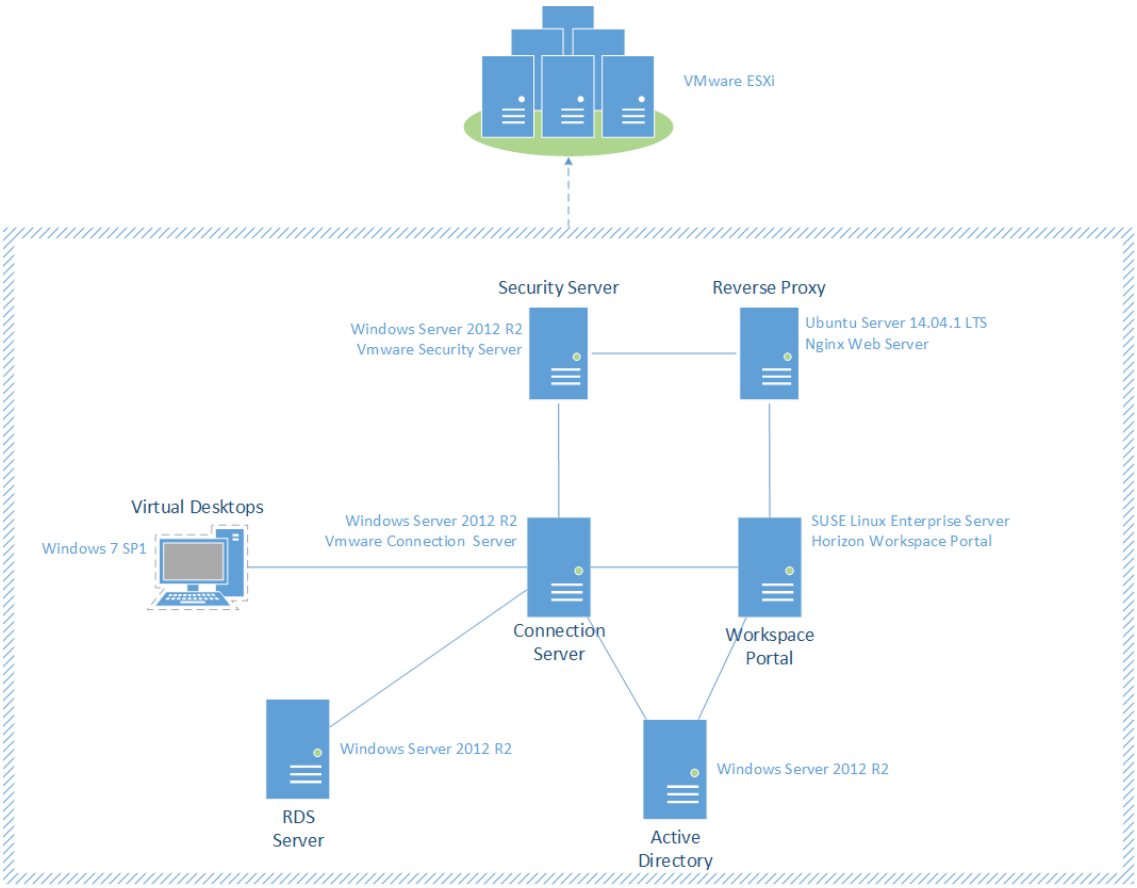


Figura 2.4.1 Tecnologie utilizzate e loro interazione

2.4.1 Windows

Windows Server 2012 R2 è il sistema operativo Microsoft versione Server. Nel progetto sono state istanziate quattro macchine virtuali con questo sistema operativo, su due sono stati installati servizi di applicativi VMware che verranno descritti poco più avanti, mentre le altre due eseguono ruoli specifici di Windows Server.

Active Directory Domain Controller: questo server gestisce gli utenti, le autorizzazioni a loro associate e accetta le autenticazioni degli utenti permettendogli di accedere alla rete. Un servizio esterno può leggere Active Directory per verificare i permessi e i gruppi di appartenenza degli utenti.

Remote Desktop Service Host: questo server ospita i servizi di Desktop Remoto; un utente che si connette ad un server di questo tipo può eseguire programmi, salvare file e utilizzare risorse di rete su quel server come fosse un vero e proprio desktop personale ospitato sul server. La differenza con VDI è che con Remote Desktop tutti gli utenti si connettono ad un'unica macchina che genera un'istanza personalizzata per ognuno di essi, mentre con VDI ogni utente ha la propria macchina. Se un utente esegue software malevolo sul server con Remote Desktop rischia di compromette il lavoro di tutti gli altri utenti, mentre se lo esegue sulla sua macchina personale viene compromessa unicamente quella.

Oltre ai server sono state create alcune macchine per simulare i Desktop virtuali dei dipendenti, su queste macchine è stato installato Windows 7 a 32 bit e aggiornate al Service Pack 1.

2.4.2 VMware

VMware ESXi è il sistema operativo Hypervisor di VMware. Un Hypervisor è un software che gestisce ed esegue macchine virtuali, mettendo a disposizione le risorse Hardware della macchina fisica sottostante. ESXi è installato sul server HP ProLiant di laboratorio che conterrà tutte le macchine virtuali (Desktop e Server) realizzate in questo progetto.
Per realizzare l'infrastruttura VDI e permettere l'accesso da remoto sono necessarie due componenti Server di VMware installati su due diverse macchine Windows Server: Connection Server e Security Server.

VMware Connection Server: questo Server permette l'utilizzo di desktop virtuali e di applicazioni remote agli utenti di dominio in base ai permessi assegnati loro nella console di amministrazione; si interfaccia con Active Directory per effettuare l'autenticazione degli utenti ed ottenerne informazioni, come ad esempio a quali gruppi fanno parte; questa informazione è particolarmente importante per permettere al server di capire quali permessi dare all'utente che si è appena collegato.
Di seguito è riportato un esempio:
Sul pannello di amministrazione del Connection Server è configurata un'applicazione remota in modo che sia accessibile solo agli utenti che in Active Directory fanno parte del gruppo "Tecnici".
Quando l'utente Mario Rossi, che fa parte del gruppo "Tecnici", effettua l'autenticazione gli viene mostrata l'applicazione.
Quando invece si connette l'utente Luca Bianchi, membro del gruppo "Amministrativi", non gli verrà mostrato l'applicativo dei tecnici.

VMware Security Server: questo Server, che non può essere inserito in dominio e deve essere in zona demilitarizzata, permette l'accesso da rete esterna verso il Connection Server (che si trova in zona sicura) creando un tunnel criptato e facendo da gateway per il trasferimento dei dati tra utente esterno e Desktop virtuali.
Utilizzando il Security Server si può accedere all'ambiente VDI in sicurezza tramite Internet (che è una rete non sicura) e senza bisogno di utilizzare una Virtual Private Network (VPN).

2.4.3 Linux

Nel prototipo sono state utilizzate le due macchine virtuali Linux descritte di seguito.

Horizon Workspace Portal: questo Server è il cuore del progetto, viene distribuito da VMware come macchina virtuale SUSE Linux già installata ed è necessaria solo la configurazione, che si può effettuare semplicemente tramite l'interfaccia web. La macchina è completamente aperta e in caso di necessità è possibile accedere alla console con privilegi di root per eseguire configurazioni a riga di comando.

Load Balancer/Reverse Proxy: per permettere l'accesso a Workspace Portal da rete esterna è necessario utilizzare un Server in zona demilitarizzata che si occupi di redirigere le connessioni. Questo è stato realizzato con una macchina virtuale Linux basata su distribuzione Ubuntu Server su cui è stato installato il Web Server nginx.
Questo Server ha due funzioni:

- Load Balancer: questa componente offre High Availability in caso di una configurazione con due Server Horizon Workspace Portal replicati; in modo che se il principale smette di rispondere a causa di un problema le richieste vengono dirottate sul secondario. Nel prototipo questa funzionalità non è utilizzata poiché non c'è la necessità di implementare High Availability.
- Reverse Proxy: un Reverse Proxy svolge il ruolo di intermediario tra la rete esterna e quella interna, esegue le interrogazioni ai server per conto del Client che ha effettuato le richieste e risponde come se avesse generato lui stesso la risposta, nascondendo in questo modo la struttura della rete interna al Client esterno.

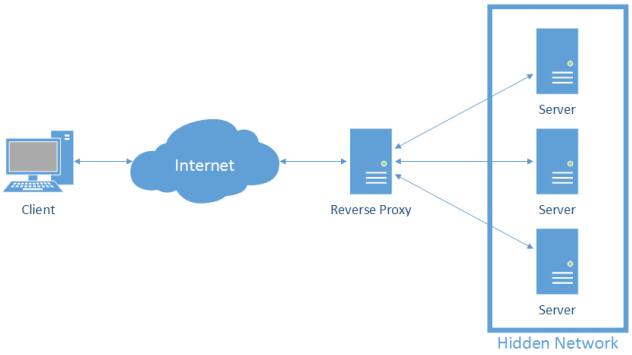


Figura 2.4.3.1 Schema di funzionamento di un Reverse Proxy

2.5 Scenario di Implementazione

2.5.1 Specifiche componenti fisiche

Il Datacenter in questo prototipo è composto da un unico server fisico. Su questa macchina è installato VMware ESXi 5.1 con licenza vSphere 5 Enterprise Plus.

Produttore	HP
Modello	ProLiant DL360 G5
Processore	Intel Xeon X5450 @ 3.00GHz 8 core
RAM	DDR2 14GB @ 667MHz
Hard Disk	2 Dischi SAS 146GB
RAID	RAID 1
Sistema operativo	VMware ESXi

Tutte le macchine virtuali sono contenute su di un'unica unità di Storage, connessa al Server tramite iSCSI.

Produttore	QNAP
Modello	TS-459
Dischi	4 dischi SATA da 2 TeraByte l'uno
RAID	RAID 5

Il Server è collegato alla rete tramite un Firewall fisico che svolge sia la funzione di Firewall perimetrale che di Firewall interno per dividere la rete locale dalla zona demilitarizzata.

Produttore	Watchguard
Modello	Firebox M500

2.5.2 Specifiche componenti virtuali

I Server virtuali Windows sono stati realizzati tutti con le stesse caratteristiche.

Sistema Operativo	Windows Server 2012 R2
CPU	1 vCPU 2 core
RAM	4GB
Storage	40GB

Per quanto riguarda i Desktop virtuali è stato scelto Windows 7 a 32-bit, complice la minore richiesta di memoria RAM.

Sistema Operativo	Windows 7 SP1 32-bit
CPU	2 vCPU 1 core
RAM	2GB
Storage	24GB

Horizon Workspace Portal è una macchina virtuale preconfigurata distribuita da VMware, sono state mantenute le specifiche consigliate.

Sistema Operativo	SUSE Linux Enterprise 11
CPU	2 vCPU 1 core
RAM	6GB
Storage	1 virtual disk da 30GB 3 virtual disk da 10GB

Il Reverse Proxy è una semplice macchina Ubuntu Server e non richiede grandi risorse.

Sistema Operativo	Ubuntu Server 14.04.1 LTS
CPU	1 vCPU 1 core
RAM	2GB
Storage	16GB

CAPITOLO 3:
SVILUPPO DEL PROGETTO

3.1 Installazione dell'ambiente

In questo sottocapitolo verranno trattate le fasi di realizzazione dell'ambiente con cui andrà ad interagire la macchina Horizon Workspace Portal e i dettagli delle varie configurazioni della rete e dei Server.

3.1.1 Progettazione della rete

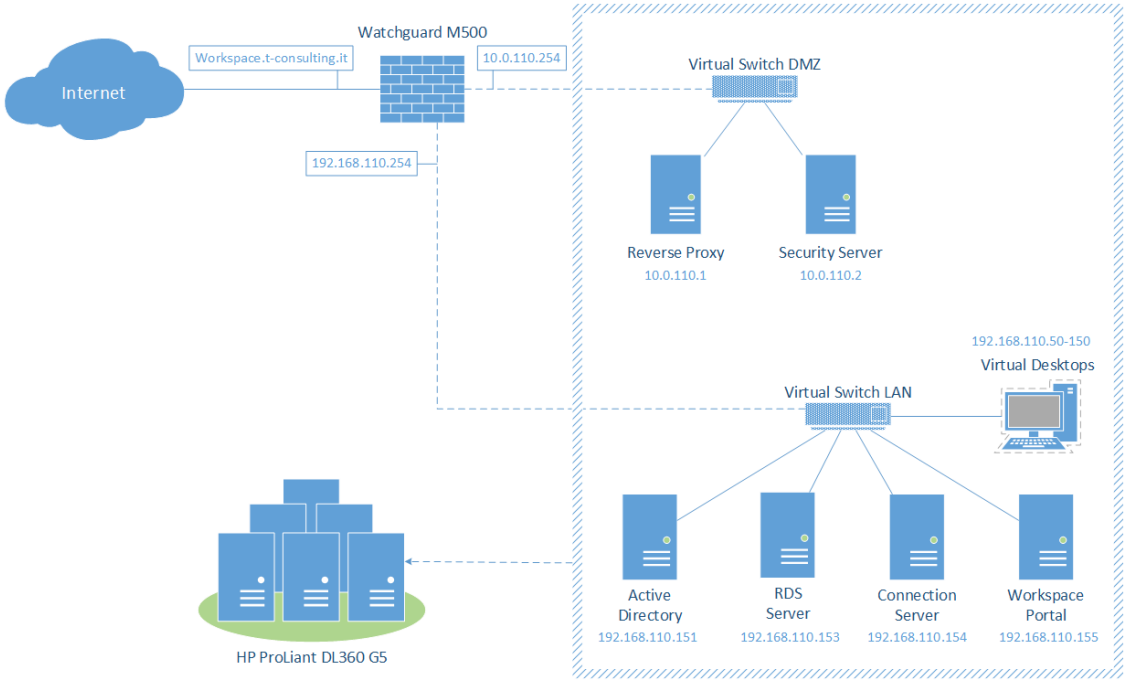


Figura 3.1.1.1 Progetto della rete

Il primo passo è stato realizzare il progetto della rete, tenendo in considerazione le varie interazioni tra i server. In figura 3.1.1.1 si può notare che sono state realizzare due reti diverse: una rete interna (192.168.110.x) e una zona demilitarizzata (10.0.110.x).
Il Gateway della rete interna ha indirizzo 192.168.110.254 ed esegue anche la funzione di DHCP.

Il pool DHCP della rete 192.168.110.x va da 50 a 150 ed è utilizzato per assegnare gli IP ai desktop virtuali, i server invece usano i seguenti IP statici:
Active Directory Domain Controller: 192.168.110.151
RDS Server: 192.168.110.153
Connection Server: 192.168.110.154
Horizon Workspace Portal: 192.168.110.155

Nella zona demilitarizzata (DMZ) invece sono stati inseriti i due server che hanno contatto diretto con l'esterno:
Reverse Proxy: 10.0.110.1
Security Server: 10.0.110.2

I servizi saranno accessibili da Internet tramite l'indirizzo workspace.t-consulting.it al quale è assegnato l'IP pubblico dell'azienda.

3.1.2 Configurazione di dominio, Active Directory e DNS

Una volta creata un'immagine Template di un sistema Windows Server 2012 R2 e averla replicata quattro volte impostando i corretti indirizzi di rete, come elencato in precedenza, si può procedere all'installazione dei servizi Windows e VMware necessari.

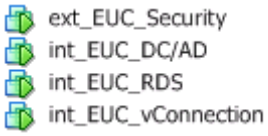


Figura 3.1.2.1 Server virtuali Windows nel pannello di amministrazione

Il primo passo per costruire il dominio è installare il servizio di Active Directory e promuovere il server a Domain Controller.
Dominio: fittizia.local
Nome Domain Controller: eucad.fittizia.local

Una volta costituito il dominio sono stati registrati alcuni utenti di test con l'accortezza di compilare anche campi secondari quali:

- nome e cognome
- e-mail
- UPN logon

Questi campi sono necessari per la sincronizzazione dell'utente con Horizon Workspace Portal.

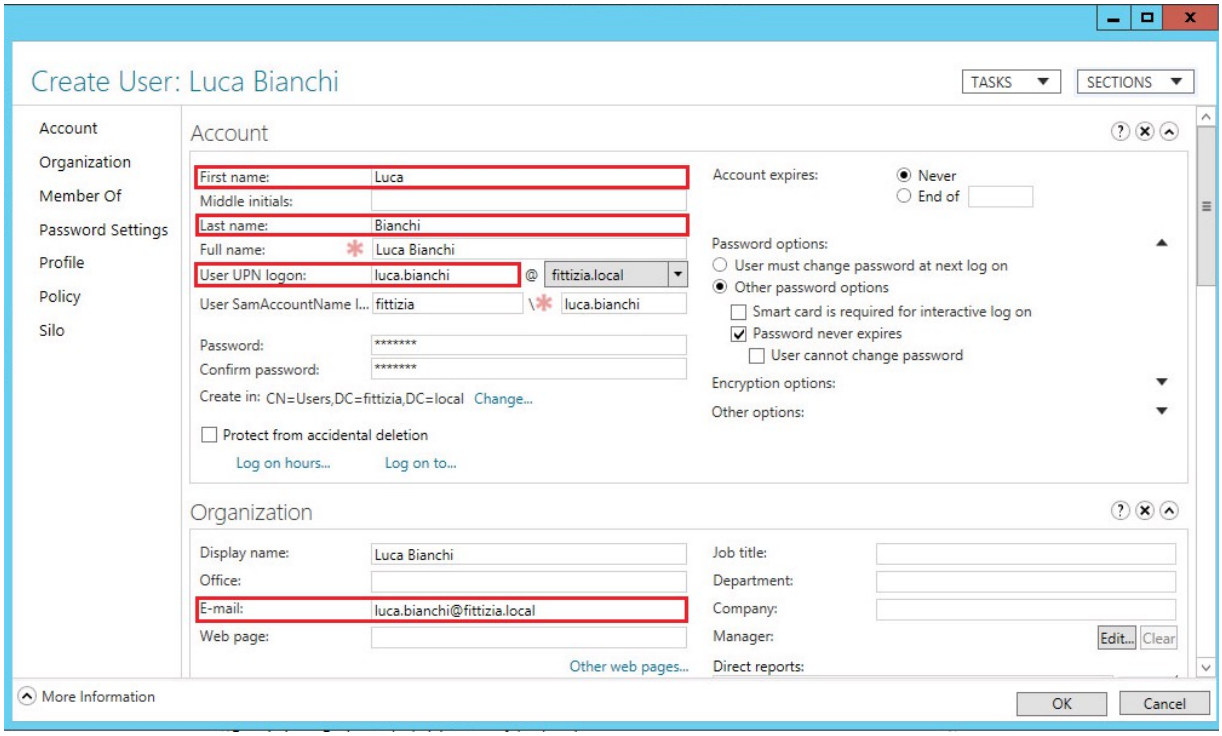


Figura 3.1.2.2 Esempio di creazione di un nuovo utente in Active Directory

In Active Directory verranno creati gruppi diversi per categorie di dipendenti diversi e sarà strutturata secondo il seguente schema:

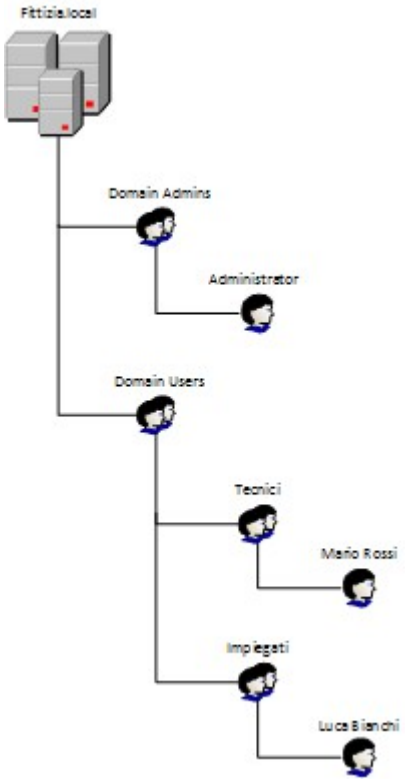


Figura 3.1.2.3 Struttura di Active Directory

Il Server RDS e il Connection Server vanno inseriti nel dominio prima di poter procedere.

Il controller di dominio installa automaticamente il servizio DNS. Nella console di gestione sono stati registrati gli IP statici di tutti i server con i relativi nomi di dominio sia nella Forward Lookup Zone che nella Reverse Lookup Zone.

3.1.3 Regole Firewall

Per creare un ambiente il più sicuro possibile il Firewall è stato configurato per bloccare tutte le connessioni in entrata tranne quelle strettamente necessarie per la realizzazione del progetto.

Il Watchguard Firebox 500 è stato configurato con le seguenti regole:

Sorgente	Destinazione	Porta	Protocollo	Azione	Note
*	*	*	*	Nega	
*	10.0.110.1	80	TCP	Consenti	HTTP verso ReversProxy
*	10.0.110.1	443	TCP	Consenti	HTTPS verso ReversProxy
*	10.0.110.2	4433	TCP	Consenti	HTTPS verso SecurityServer
*	10.0.110.2	4172	TCP/UDP	Consenti	PCoIP verso SecurityServer
10.0.110.*	192.168.110.151	53	TCP/UDP	Consenti	Interrogazioni DNS da DMZ verso Domain Controller
10.0.110.1	192.168.110.155	443	TCP	Consenti	HTTPS da ReverseProxy a Workspace Portal
10.0.110.2	192.168.110.*	4172	TCP/UDP	Consenti	PCoIP da SecurityServer a rete interna
10.0.110.2	192.168.110.154	4001	TCP	Consenti	Messaggi JMS tra SecurityServer e ConnectionServer
10.0.110.2	192.168.110.154	8009	TCP	Consenti	Pacchetti AJP13 tra SecurityServer e ConnectionServer
10.0.110.2	192.168.110.154	500	UDP	Consenti	Tunnel IPSec tra SecurityServer e ConnectionServer
10.0.110.2	192.168.110.154	4500	UDP	Consenti	Tunnel IPSec tra SecurityServer e ConnectionServer attraverso NAT

Inoltre è stato impostato un NAT che redirige le connessioni in arrivo sulle porte 443 e 4433 secondo le seguenti regole:

Indirizzo Sorgente	Porta Sorgente	Protocollo sorgente	Indirizzo destinazione	Porta destinazione	Protocollo destinazione
88.149.164.155	443	TCP	10.0.110.1	443	TCP
88.149.164.155	4433	TCP	10.0.110.2	4433	TCP

3.1.4 Connection Server e Security Server

L'installazione del Connection Server è molto semplice grazie alla procedura guidata dell'installer; una volta conclusa si può entrare nel pannello di amministrazione web con qualsiasi browser digitando l'indirizzo: https://localhost/admin
Per accedere al pannello di amministrazione è richiesto Adobe Flash Player, per questo motivo sul Connection Server del prototipo è stato installato il browser Google Chrome che contiene tale software nativamente.

Per quanto riguarda il Security Server, prima di avviare l'installazione è necessario tenere in considerazione tre punti importanti:

- la macchina non deve essere inserita in dominio;
- la macchina deve avere un indirizzo IP statico;
- il software deve essere installato solo dopo l'installazione del Connection Server.

Durante la fase di installazione deve essere inserito il nome completo di dominio (Fully Qualified Domain Name o FQDN) del Connection Server al quale si vuole collegare il Security Server. Viene richiesta inoltre una password temporanea di associazione, questa può essere scelta a piacimento e deve essere generata dalla console di amministrazione del Connection Server, tramite il percorso: View Configuration → Servers → selezione del Connection Server → Specify Security Server Pairing Password...
Successivamente vengono inseriti gli indirizzi per l'accesso da rete esterna, nel campo dell'indirizzo per la connessione PCoIP è obbligatorio inserire un indirizzo IP.
Nel progetto sono stati inseriti i seguenti dati:

External URL:	https://workspace.t-consulting.it:4433
PCoIP External URL:	88.149.164.155:4172
Blast External URL:	https://workspace.t-consulting.it:8443

È stata utilizzata la porta 4433 al posto della standard 443 poiché si vuole utilizzare un solo indirizzo IP esterno per accedere a entrambi i servizi e la porta 443 sarà dedicata a Horizon Workspace Portal.
L'installer si occupa autonomamente di inserire le regole necessarie nel Firewall Software di Windows, tuttavia in quanto non useremo la porta standard per le connessioni in entrata sono necessarie alcune modifiche manuali:

1. Modificare il file di configurazione del Security Server

Per cambiare la porta sulla quale è in ascolto il servizio del Security Server è necessario modificare il file "config.properties" localizzato nella cartella
C:\ProgramFiles\VMware\VMware View\Server\sslgateway\conf\
aggiungendo la riga:

serverPort=4433

assicurarsi inoltre che sia presente la riga:

serverProtocol=https

In caso contrario inserirla manualmente.
Riavviare poi il servizio Security Server per rendere effettiva la modifica.
Utilizzando il comando `netstat -ban` si può verificare se la modifica sia stata apportata con successo controllando che il servizio sia in ascolto sulla porta 4433.

2. Inserire manualmente una regola in Windows Firewall

Windows Firewall è già stato configurato durante l'installazione per permettere l'accesso a tutte le porte standard utilizzate dal sevizio, in quanto utilizzeremo una porta non standard è necessario aggiungere la regola manualmente.
Per fare ciò dal pannello di controllo di Windows accedere alla configurazione avanzata di Windows Firewall. Dal pannello "Inbound Rules" è possibile creare una nuova regola, che permetta qualsiasi connessione TCP in ingresso sulla porta 4433.

3.1.5 Server RDS

Su questo server è stato installato il ruolo di Terminal Server e Remote Desktop Service. Questo tipo di servizio normalmente viene utilizzato per creare un pool di Desktop utilizzabili dai dipendenti, mentre nel caso di questa installazione avrà un altro scopo, ovvero quello di contenere ed eseguire le applicazioni lanciate tramite Horizon Workspace Portal.

Per eseguire questa operazione il Server genera una sessione utente su cui viene avviata l'applicazione ogni volta che l'utente remoto ne fa richiesta, il sistema View si occuperà poi di inviare al Client solamente l'applicazione e non l'intero Desktop.

Su questo server verrà anche aggiunta una cartella di rete per ogni utente per contenere i dati personali e i documenti aziendali accessibili da remoto.

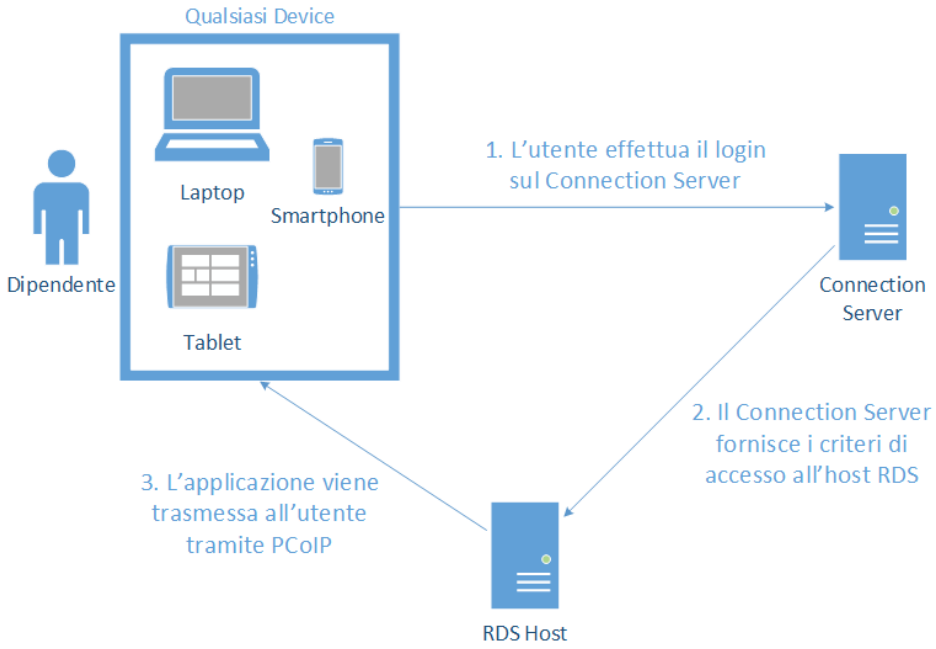


Figura 3.1.5.1 Schema di funzionamento di streaming applicativo tramite Host RDS

Durante l'installazione del ruolo è importante selezionare "Remote Desktop Services" dalla lista dei ruoli disponibili. Per quanto riguarda i servizi del ruolo è sufficiente installare "Remote Desktop Session Host", gli altri servizi non sono necessari in questo progetto e non sono stati installati.

Dopo il riavvio (necessario) del Server si può procedere all'installazione di VMware Horizon View Agent sulla macchina. Questo Software permette la trasmissione dei dati ai Client che si collegano da remoto tramite protocollo PCoIP, inoltre consente all'Host RDS di essere associato al Connection Server permettendo la creazione dei pool applicativi. Durante la procedura di installazione è richiesto l'indirizzo del Connection Server a cui verrà associato il Server RDS e le credenziali di administrator.

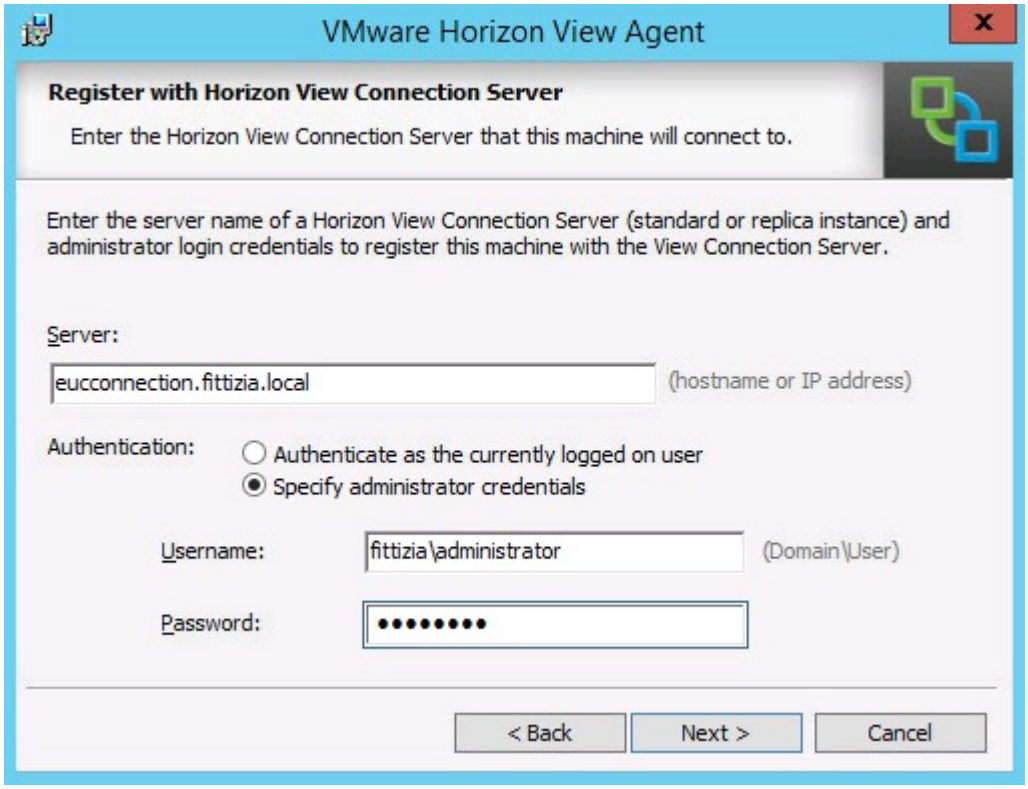


Figura 3.1.5.2 Particolare della procedura installazione del View Agent sul server RDS

Una volta eseguito il riavvio a seguito dell'installazione del View Agent la configurazione di questo server è ultimata e si può procedere con l'installazione delle applicazioni da rendere disponibili agli utenti tramite streaming applicativo.

3.2 Horizon Workspace Portal

In questo sottocapitolo verrà trattata l'installazione e configurazione della macchina Horizon Workspace Portal e del Reverse Proxy e verranno illustrati i passaggi necessari per la comunicazione tra i due server e l'accesso da rete esterna, infine verrà illustrato come aggiungere applicazioni al catalogo di Workspace Portal.

3.2.1 Installazione di Horizon Workspace Portal

Questo Server viene distribuito da VMware come "virtual appliance", ovvero una macchina virtuale preconfigurata da VMware e fornita sotto forma di Template. Per installare questa macchina è sufficiente avviare la procedura guidata dal pannello di amministrazione di VMware vSphere, menu File → Deploy OVF Template...

Durante la procedura viene richiesto l'inserimento delle proprietà di rete della macchina, è molto importante inserire l'Host Name del Server in formato FQDN e tutto minuscolo:

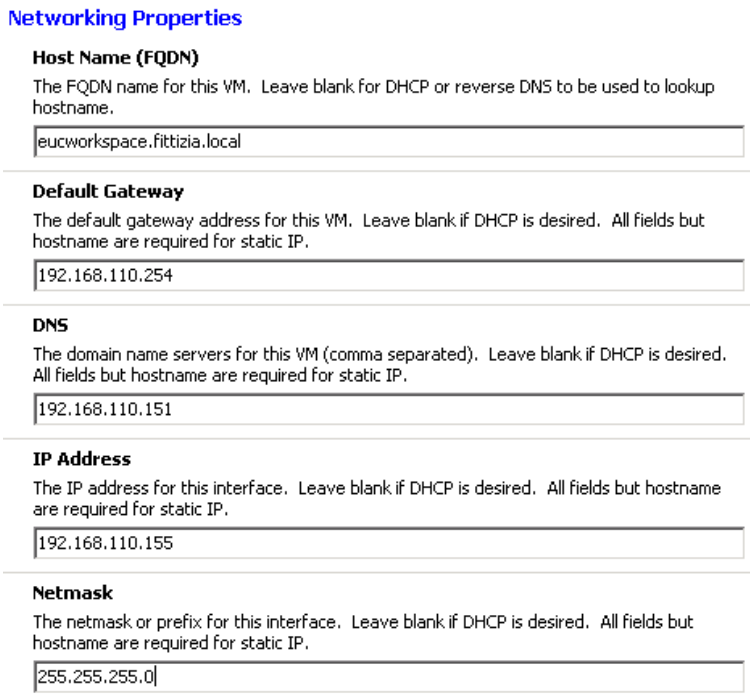


Figura 3.2.1.1 Proprietà di rete del Server Horizon Workspace Portal

Terminata l'installazione la macchina si presenta così:

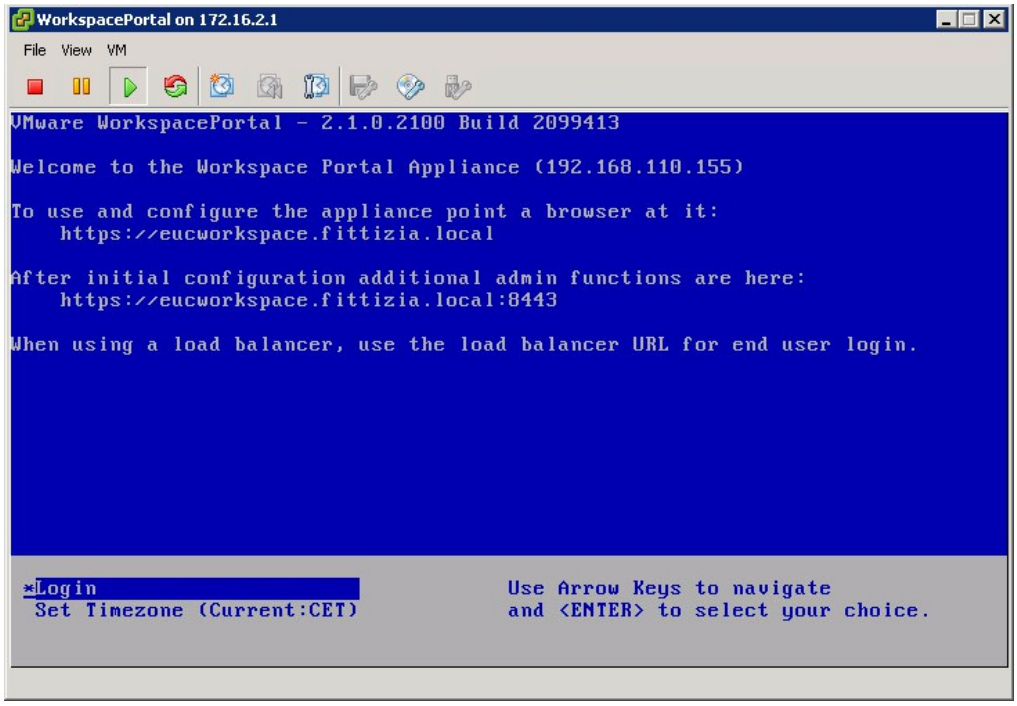


Figura 3.2.1.2 Interfaccia del Server Horizon Workspace Portal

È possibile effettuare il login per eseguire configurazioni a riga di comando oppure impostare il fuso orario della macchina. È molto importante che l'orologio di tutti i Server sia sincronizzato perfettamente, un divario temporale di qualche secondo potrebbe far fallire le autenticazioni degli utenti.

Per sincronizzare gli orologi è stata impostata la sincronizzazione delle macchine virtuali Guest con l'Host, in questo modo tutti i Server acquisiscono lo stesso orario del Server ESXi.

Tramite il pannello di amministrazione di vSphere è stato attivato il Network Time Protocol (NTP) impostando il Time Server:

utcnist2.colorado.edu

IP: 128.138.141.172

In questo modo il server ESXi mantiene l'orologio di sistema costantemente aggiornato e sincronizzato con il mondo esterno.

Una volta terminato il Deploy e sincronizzati gli orologi si può accedere alla macchina tramite interfaccia web per terminare le configurazioni.
La procedura guidata si può raggiungere digitando nel browser l'indirizzo: https://eucworkspace.fittizia.local:8443.
Durante questa procedura sono stati riscontrati problemi utilizzando il browser Internet Explorer che hanno compromesso l'installazione e hanno reso necessario effettuare nuovamente la procedura di Deploy dall'inizio, utilizzando il browser Chrome invece non ci sono state complicazioni. Questa procedura è stata eseguita tramite il Connection Server, dove è stato installato Chrome in precedenza per il supporto a Flash.

Verrà ora analizzata questa procedura passaggio per passaggio, indicando le impostazioni scelte nel progetto.

Get Started

Al primo accesso alla console web di configurazione si verrà accolti dalla procedura guidata di Setup, nella colonna di sinistra si possono notare tutti i passaggi della procedura.

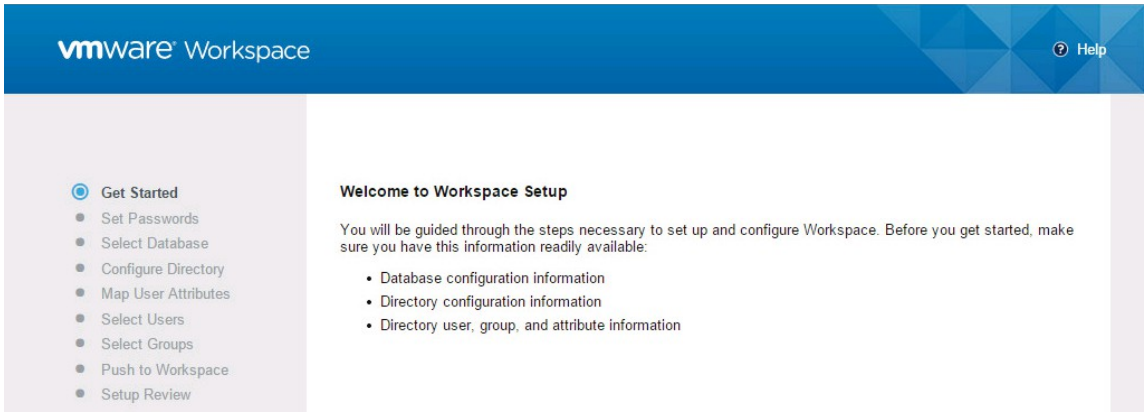


Figura 3.2.1.3 Schermata di benvenuto procedura di prima configurazione di Horizon Workspace Portal

Set Passwords

Il primo passo è inserire le password di amministratore, root e utente remoto di connessione SSH.

Select Database

Successivamente viene richiesto che tipo di database si vuole utilizzare, le scelte sono due: interno ed esterno.

Nel caso si scelga database interno viene creato un database PostgreSQL locale sulla macchina, nel caso invece di database esterno è necessario impostare la stringa di connessione al database e le credenziali per accedervi.

In un ambiente con due macchine Horizon Workspace che offrono High Availability è necessario utilizzare un database esterno (Oracle o PostgreSQL) a cui fanno riferimento le due macchine. Nel progetto è stato utilizzato il database interno che risulta consono anche per un ambiente di piccole/medie dimensioni.

Configure Directory

Nel passo successivo viene chiesto di associare l'Active Directory ad Horizon Workspace Portal, per fare questo è necessario inserire:

- indirizzo del server Active Directory;
- porta di comunicazione con il servizio Active Directory (di default 389);
- Base DN;
- Bind DN;
- Bind Password.

DN è l'acronimo di Distinguished Name ed è un attributo che si può trovare nelle proprietà di un qualsiasi utente di Active Directory.

“Base DN” indica il punto di partenza per le ricerche in Directory, ad esempio:

DC= fittizia,DC=local

“Bind DN” è il Distinguished Name dell'utente che ha i permessi di ricerca all'interno di Active Directory, ad esempio la DN dell'utente administrator:

CN=Administrator,CN=Users,DC=fittizia,DC=local

Bind Password è la password dell'account specificato in Bind DN, quindi in questo caso la password di administrator.

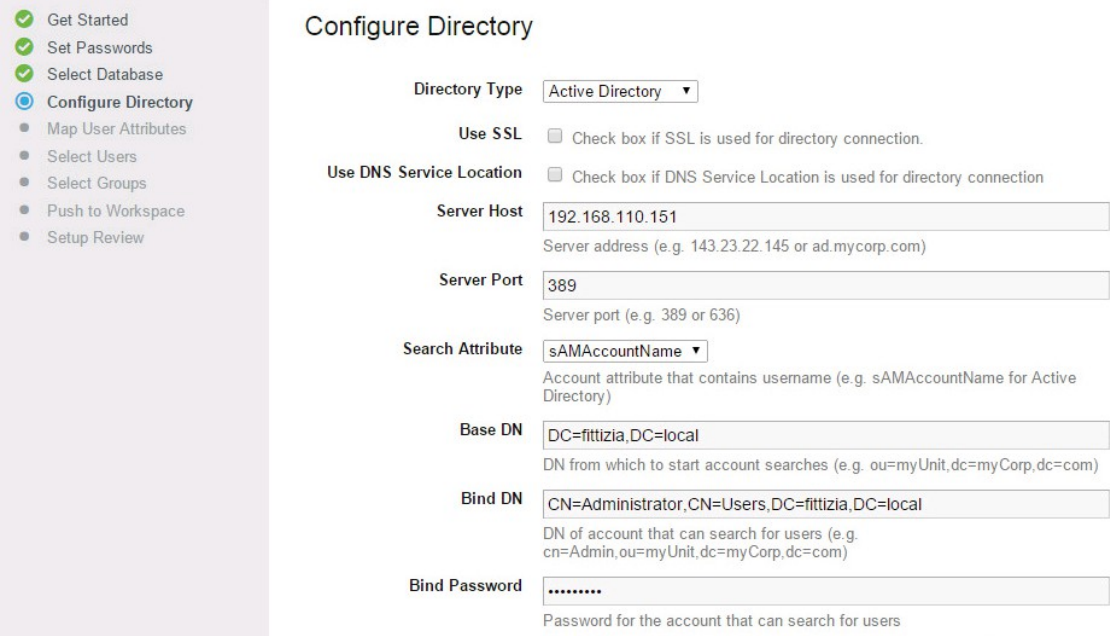


Figura 3.2.1.4 Dati inseriti nello step "Configure Directory"

Map User Attributes

In questo passaggio vengono impostati gli attributi letti da Horizon Workspace in Active Directory, le impostazioni di default sono corrette a meno che non siano state fatte configurazioni particolari alla propria Active Directory.

L'unica modifica da effettuare è impostare come Required il campo userPrincipalName, questo è necessario per abilitare i pool applicativi di View.

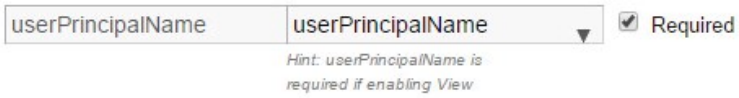


Figura 3.2.1.5 Impostazione Required del campo userPrincipalName

Select Users

È possibile creare filtri per escludere alcuni utenti dalla sincronizzazione tra Workspace e Active Directory.

Nel progetto sono stati esclusi gli utenti Guest e krbtgt, in quanto si tratta di utenti fittizi di Windows utilizzati per servizi specifici. Questi utenti provocano errori durante la sincronizzazione, non possedendo alcune delle proprietà richieste da Workspace Portal.

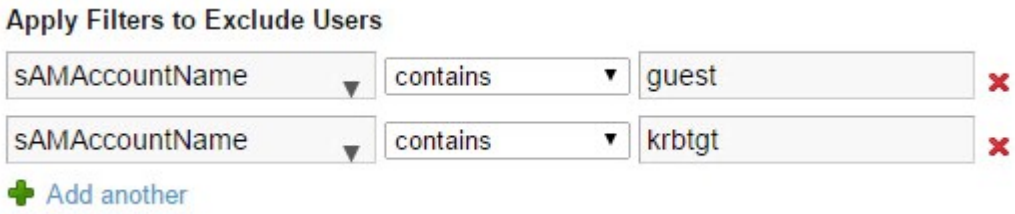


Figura 3.2.1.6 Esclusione degli utenti Guest e krbtgt

Select Groups

In questo passaggio si possono scegliere i gruppi di Active Directory da aggiungere a Workspace in modo da gestire i permessi di accesso alle diverse applicazioni in base al gruppo di appartenenza degli utenti.

Nel prototipo sono stati inseriti i gruppi Domain Users, Impiegati e Tecnici.

Figura 3.2.1.6 Aggiunta dei gruppi su Horizon Workspace Portal

Push to Workspace

Terminata la selezione dei gruppi si può avviare la sincronizzazione con Active Directory. In questa schermata di riepilogo è possibile verificare quanti e quali utenti e gruppi si stanno aggiungendo a Workspace e se ci sono dei problemi nelle proprietà di alcuni utenti; ad esempio un utente con il campo "email" vuoto non verrà sincronizzato e sarà mostrato tra gli Alerts il relativo avviso.

Cliccando "Push to Workspace" i dati di Active Directory vengono sincronizzati con il database locale di Workspace.

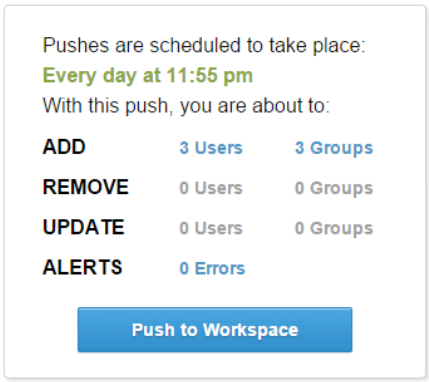


Figura 3.2.1.7 Riepilogo delle modifiche che verranno apportate con la sincronizzazione

Setup Review

Quest'ultimo passaggio conferma che l'installazione è andata a buon fine. Da questo momento si potrà accedere alla console di amministrazione utilizzando le credenziali di administrator.

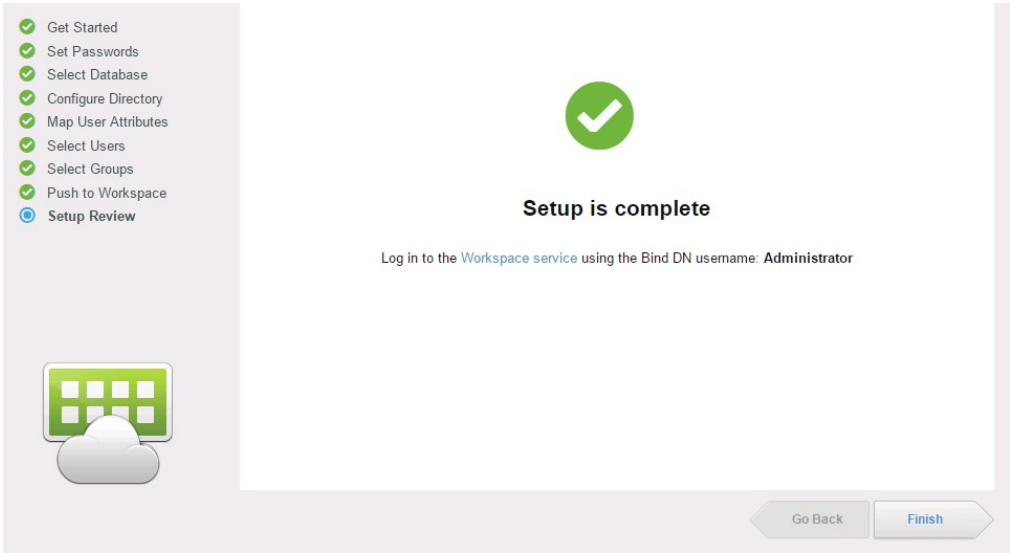


Figura 3.2.1.8 Procedura di Setup completata

Terminata la procedura di installazione il server diventa operativo.
Accedendo all'indirizzo:

https://eucworkspace.fittizia.local:8443

si verrà reindirizzati ad una pagina contenente i link dei tre diversi pannelli di amministrazione di Horizon Workspace Portal:

Appliance Configurator: questo pannello permette di modificare le impostazioni del database, i certificati SSL, le password di sistema e visionare i file di log.

Workspace Admin Console: permette la gestione del catalogo di applicazioni, dei permessi di utenti e gruppi e mostra le schermate di riepilogo e le statistiche dell'attività degli utenti sulla piattaforma.

Connector Services Admin: consente di selezionare utenti e gruppi di Active Directory da sincronizzare con Workspace e aggiungere risorse come i pool di View (sia Desktop che Application).

Per proseguire con la configurazione di Horizon Workspace Portal bisogna prima installare e configurare il Reverse Proxy.

3.2.2 Installazione del Reverse Proxy

Il Reverse Proxy è stato implementato tramite il Web Server nginx, che può essere installato su qualsiasi macchina Linux; nel progetto è stata utilizzata una distribuzione Ubuntu Server, nello specifico la versione 14.04.1 LTS. L'installazione del sistema operativo è molto intuitiva grazie alla procedura guidata e una volta terminata si può procedere con la configurazione dell'interfaccia di rete assegnandovi un indirizzo IP statico.

Eseguendo il comando:

```
sudo nano /etc/network/interfaces
```

si può modificare il file di configurazione contenente le proprietà delle schede di rete.

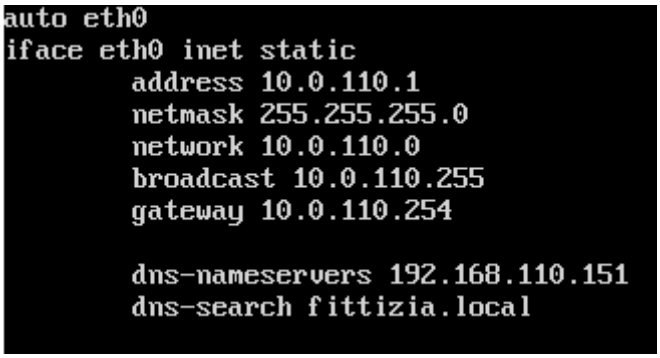


Figura 3.2.2.1 Parametri di configurazione della scheda di rete del Reverse Proxy

Per rendere effettive le modifiche si riavvierà il servizio di rete tramite il comando:

```
sudo /etc/init.d/networking restart
```

A questo punto si può procedere scaricando e installando nginx dal repository eseguendo il comando:

```
sudo apt-get install nginx
```

File di configurazione “nginx.conf”

Per configurare nginx in modo che svolga la funzione di Reverse Proxy è necessario modificare i file di configurazione.

Il primo file da modificare si trova nella seguente posizione:

/etc/nginx/nginx.conf

Il contenuto del file dopo le modifiche apportate si presenta così:

```
user www-data;
worker_processes 4;
pid /run/nginx.pid;

events {
        worker_connections 1024;
        multi_accept on;
        use epoll;
}

http {
        include /etc/nginx/mime.types;
        default_type application/octet-stream;
        access_log /var/log/nginx/access.log;
        error_log /var/log/nginx/error.log;

        sendfile on;
        tcp_nopush on;
        keepalive_timeout 65;
        server_tokens off;

        client_max_body_size 0M;
        client_body_buffer_size 256k;
        client_header_buffer_size 2k;

        gzip on;
        gzip_proxied any;
        gzip_comp_level 3;
        gzip_buffers 128 8k;
        gzip_min_length 512;
        gzip_types text/plain text/css application/json application/x-
                javascript text/xml application/xml application/xml+rss
                text/javascript application/javascript;

        include /etc/nginx/sites-enabled/*;
}
```

Di seguito verrà analizzato il codice sopra riportato specificando il comportamento delle varie istruzioni.

```
user www-data;
worker_processes 4;
pid /run/nginx.pid;
```

Nella prima riga si trova l'utente sotto cui viene eseguito il processo nginx, in seguito il numero di processi utilizzati e il Program ID (il PID è un numero univoco nel sistema che identifica il processo).

```
events {
      …
}
```

Nel blocco `events` viene dichiarato come nginx deve gestire le connessioni.

```
worker_connections 1024;
```

Vengono impostate 1024 connessioni per ogni processo worker.

```
multi_accept on;
```

Cerca di accettare il maggior numero di connessioni possibili subito dopo aver instaurato una nuova connessione.

```
use epoll;
```

`epoll` è il metodo di gestione delle connessioni ottimizzato per Linux.

```
http {
…
}
```

Questo blocco specifica le direttive del server http.

```
include /etc/nginx/mime.types;
default_type application/octet-stream;
access_log /var/log/nginx/access.log;
error_log /var/log/nginx/error.log;
```
Impostazioni base del Server comuni a qualsiasi altra installazione di nginx; tra queste troviamo l'indicazione della posizione dei file di log.

```
sendfile on;
```
Utilizzare `sendfile()` è più performante perché grazie a questa primitiva del Kernel i dati vengono direttamente copiati dal server alla Socket TCP, senza effettuare operazioni `read()` e `write()` che richiedono un Context-Switch.

```
tcp_nopush on;
```
Utilizzabile insieme a `sendfile()`, prepara l'header http prima di inviare la risposta e lo spedisce in un pacchetto unico.

```
keepalive_timeout 65;
```
Assegna il tempo massimo in cui viene mantenuta aperta una connessione tra il Client e il Server, dopo questo tempo il Server chiude la connessione.

```
server_tokens off;
```
Disabilita la scrittura delle informazioni riguardanti il server nginx nel campo “Server” all'interno degli Header di risposta e nei messaggi di errore.
Con questo accorgimento si effettua la cosiddetta “Security through Obscuirty”, poiché non restituendo alcuna informazione un potenziale attaccante non può conoscere il modello e la versione di Server Web per sfruttare eventuali vulnerabilità conosciute.

```
client_body_buffer_size 256k;
client_header_buffer_size 2k;
```
Queste due istruzioni incrementano la capacità dei buffer destinati ad ospitare le richieste dei Client, in modo da non dover scrivere le richieste in file temporanei se queste eccedono la dimensione standard del buffer.

```
gzip on;
gzip_proxied any;
gzip_comp_level 3;
gzip_buffers 128 8k;
gzip_min_length 512;
gzip_types text/plain text/css application/json application/x-
     javascript text/xml application/xml application/xml+rss
     text/javascript application/javascript;
```

Questo blocco di istruzioni attiva il modulo `gzip` e ne imposta varie proprietà (come il livello di compressione e i tipi di file che devono essere sempre compressi). Tale modulo permette di comprimere le risposte del server per diminuire la quantità di dati trasferiti sulla rete.

```
include /etc/nginx/sites-enabled/*;
```

Include i file contenuti nella cartella sites-enabled, dove verranno scritte le impostazioni che descrivono il comportamento del Reverse Proxy.

File di configurazione “default”

Questo file specifica il comportamento del Server, qui è stata impostata la funzionalità di Reverse Proxy sulla porta 443. Il file si trova nella posizione:

/etc/nginx/sites-enabled/default

Il contenuto del file dopo le modifiche apportate si presenta così:

```
#redirection da HTTP a HTTPS
server {
        listen 80;
        server_name workspace.t-consulting.it;
        return 301 https://$host$request_uri;
}

# HTTPS server
server {
        listen 443 ssl;
        server_name workspace.t-consulting.it;

        add_header Strict-Transport-Security "max-age=31536000;";

        ssl on;
        ssl_certificate /etc/nginx/lbcert.pem;
        ssl_certificate_key /etc/nginx/lbkey.pem;
        ssl_session_cache shared:SSL:50m;
        ssl_session_timeout 10m;

        ssl_protocols SSLv3 TLSv1;
        ssl_ciphers "ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+EXP";
        ssl_prefer_server_ciphers on;

        location / {
                proxy_pass https://eucworkspace.fittizia.local;
                proxy_set_header Host $host;
                proxy_set_header X-Real-IP $remote_addr;
                proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
                proxy_read_timeout 1800;
                proxy_connect_timeout 1800;
                proxy_http_version 1.1;
                proxy_buffering off;
        }
}
```

Come per nginx.conf verrà di seguito analizzato il codice sopra riportato specificando il comportamento delle varie istruzioni.

```
#redirection da HTTP a HTTPS
server {
      listen 80;
      server_name workspace.t-consulting.it;
      return 301 https://$host$request_uri;
}
```

Questo Server resta in ascolto sulla porta 80 (`listen 80;`) ed effettua il redirect mandando una risposta 301 e aggiungendo https:// all'inizio della richiesta (`return 301 https://$host$request_uri;`). In questo modo il client viene ridirezionato sulla porta 443, sulla quale si trova in ascolto il Reverse Proxy che opera tramite connessione sicura SSL.

`server_name` indica il nome del server, in questo caso coincide con l'indirizzo web del servizio poiché il server si trova in zona demilitarizzata e risponde direttamente a quell'indirizzo Internet.

```
# HTTPS server
server {
      listen 443 ssl;
      server_name workspace.t-consulting.it;
      …
}
```

Questo Server è in ascolto sulla porta 443 e al suo interno è implementato il Reverse Proxy, come per il Server sulla porta 80 `server_name` coincide con l'indirizzo web del servizio.

```
add_header Strict-Transport-Security "max-age=31536000;";
```

Aggiunge l'Header `Strict-Transport-Security` per indicare al Client di utilizzare solo una connessione sicura.

```
ssl on;
ssl_certificate /etc/nginx/lbcert.pem;
ssl_certificate_key /etc/nginx/lbkey.pem;
```
Attiva HTTPS per questo Server e indica la posizione del certificato di sicurezza e della relativa chiave. La creazione del certificato sarà trattata nelle prossime pagine.

```
ssl_session_cache shared:SSL:50m;
```
Imposta la Cache in modo che sia condivisa tra i processi `(shared)`, il nome della cache `(SSL)` e la dimensione `(50m)`.

```
ssl_session_timeout 10m;
```
Specifica il lasso di tempo in cui un Client può riutilizzare i parametri di sessione memorizzati nella Cache.

```
ssl_protocols SSLv3 TLSv1;
ssl_ciphers "ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+EXP";
ssl_prefer_server_ciphers on;
```
Abilita i protocolli `SSLv3` e `TLSv1`, imposta i cifrari e specifica la preferenza di utilizzo dei cifrari sopra indicati rispetto a quelli supportati dal Client.

```
location / {
      …
}
```
Questo blocco implementa il comportamento del Reverse Proxy, "`location /`" indica che il Server deve rispondere a qualsiasi interrogazione.

Verranno esaminate di seguito le varie direttive Proxy.

```
proxy_pass https://eucworkspace.fittizia.local;
```
Indica l'indirizzo a cui devono essere direzionate le interrogazioni ricevute dal Server.

```
proxy_set_header Host $host;
```
Imposta il nome del Reverse Proxy nel campo Host dell'Header.

```
proxy_set_header X-Real-IP $remote_addr;
proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
```
Vengono aggiunti due Header necessari per Workspace Portal e richiesti dalla documentazione, questi due Header indicano i dati del Client che sta effettuando le richieste.

```
proxy_read_timeout 1800;
proxy_connect_timeout 1800;
```
Vengono aumentati i tempi di timeout per tenere le connessioni aperte più a lungo.

```
proxy_http_version 1.1;
```
Specifica di utlizzare la versione 1.1 di http (se non specificato il default sarebbe la versione 1.0).

```
proxy_buffering off;
```
Questa direttiva disabilita il Buffering, in questo modo le risposte di Workspace Portal vengono inviate al Client in maniera sincrona, non appena vengono ricevute.

3.2.3 Instaurazione di una relazione di trust tra Reverse Proxy e Horizon Workspace Portal

Creazione del certificato (auto firmato) sul Reverse Proxy

A scopo di test è stato utilizzato un certificato di sicurezza auto firmato. Questo causerà la visualizzazione di un messaggio di avviso sui Client che effettuano la connessione poiché il certificato non viene da un'Autorità di Certificazione (CA) riconosciuta. In fase di produzione sarà necessario acquistare un certificato firmato da una CA, come ad esempio Comodo o VeriSign.

Per generare il certificato sul Reverse Proxy è stato utilizzato il seguente comando:

```
sudo openssl req -x509 -sha256 -nodes -newkey rsa:2048 -keyout
      /etc/nginx/lbkey.pem -out /etc/nginx/lbcert.pem -days 365
```

Una volta generata la chiave privata il programma richiederà alcune informazioni che verranno inserite all'interno del certificato.

È di fondamentale importanza in questo passaggio inserire l'indirizzo Internet del server nel campo “Common Name”.

```
Generating a 2048 bit RSA private key
.....................................................+++
.....................................................+++
writing new private key to '/etc/nginx/newlbkey.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:IT
State or Province Name (full name) [Some-State]:Forli-Cesena
Locality Name (eg, city) []:Forli
Organization Name (eg, company) [Internet Widgits Pty Ltd]:T-Consulting
Organizational Unit Name (eg, section) []:dipartimento IT
Common Name (e.g. server FQDN or YOUR name) []:workspace.t-consulting.it
Email Address []:
```

Figura 3.2.3.1 Compilazione dati durante la creazione del certificato auto firmato

Instaurazione del trust tra Reverse Proxy e Workspace Portal

Una volta generato il certificato del Reverse Proxy si può procedere ad instaurare la relazione di trust tra i due Server, non è necessario generare un certificato sulla macchina Workspace Portal poiché viene generato automaticamente dal Server in fase di installazione.

Per creare la relazione di trust sono necessari due passaggi:

1. installare il certificato del Reverse Proxy su Horizon Workspace Portal;
2. installare il certificato di Horizon Workspace Portal sul Reverse Proxy.

1. Reverse Proxy → Horizon Workspace Portal

Una volta copiato il certificato del Reverse Proxy all'interno di una cartella di rete condivisa si deve accedere al pannello Appliance Configurator di Workspace.

In questo pannello tramite il menu "Install Certificate" selezionare la scheda "Terminate SSL on a Load Balancer", aprire il certificato del Reverse Proxy con un editor di testo e copiare e incollare il contenuto del file nell'apposito campo, il tasto Save avvierà la procedura di registrazione del certificato.

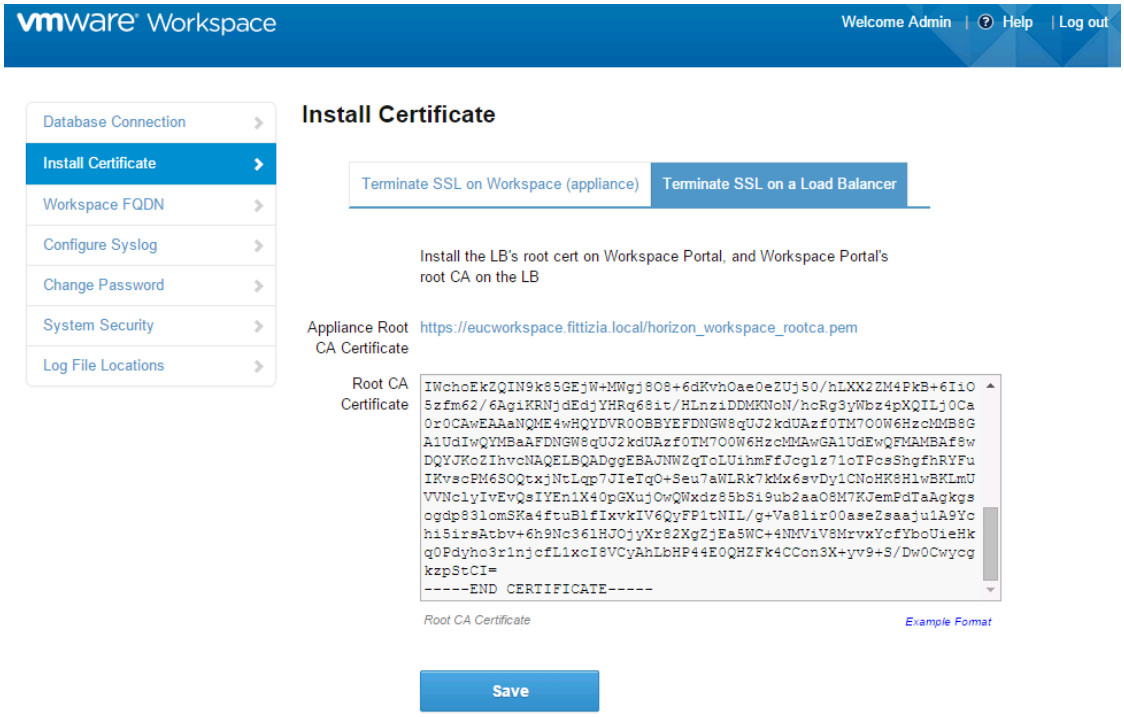


Figura 3.2.3.2 Installazione del certificato del Reverse Proxy su Workspace Portal

2. Horizon Workspace Portal → Reverse Proxy

Scaricare il certificato di Workspace Portal in una cartella di rete condivisa, tramite l'apposito link situato nella pagina visitata nel precedente passaggio.

Si procede copiando il certificato di Workspace Portal nella cartella

/usr/share/ca-certificates

modificando l'estensione del certificato da PEM a CRT, poiché il gestore dei certificati accetta solo il secondo formato.

CRT non è altro che una versione di PEM formattata diversamente, non ci sono differenze sostanziali che richiedono una conversione specifica.

Per copiare il file modificando l'estensione è stato utilizzato il seguente comando:

```
sudo cp /media/repository/horizon_workspace_root_ca.pem
      /usr/share/ca-certificates/horizon_workspace_root_ca.crt
```

Ora che il file si trova nella cartella ca-certificates si può aggiornare l'elenco dei certificati con il comando:

```
sudo dpkg-reconfigure ca-certificates
```

Si può controllare l'effettiva aggiunta del certificato con il comando:

```
cat /etc/ca-certificates.conf
```

`horizon_workspace_root_ca.crt` apparirà nell'ultima riga.

La relazione di trust è stata così instaurata e si può procedere alla configurazione di Horizon Workspace Portal per l'accesso tramite Internet.

3.2.4 Configurazione di Horizon Workspace Portal per l'accesso da rete esterna

Per consentire l'accesso a Horizon Workspace Portal tramite un indirizzo diverso dal nome completo di dominio della macchina è necessario modificare il campo "Workspace FQDN" dal pannello Appliance Configurator, sostituendolo con l'indirizzo Internet del Reverse Proxy: https://workspace.t-consulting.it

La procedura automatica controllerà che sia aperta la connessione bidirezionale tra Workspace Portal e Reverse Proxy tramite la porta 443 e che esista la relazione di trust prima di modificare l'indirizzo.

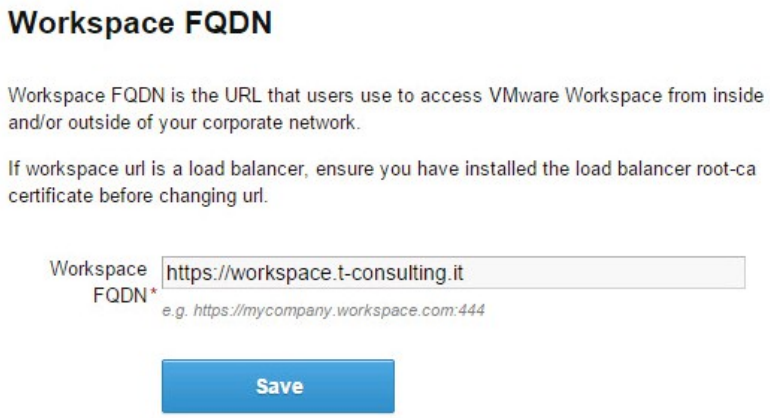


Figura 3.2.4.1 Modifica del campo Workspace FQDN

Effettuando l'accesso sul pannello Connector Services Admin è possibile verificare che sia stato modificato con successo anche l'Identity Provider.

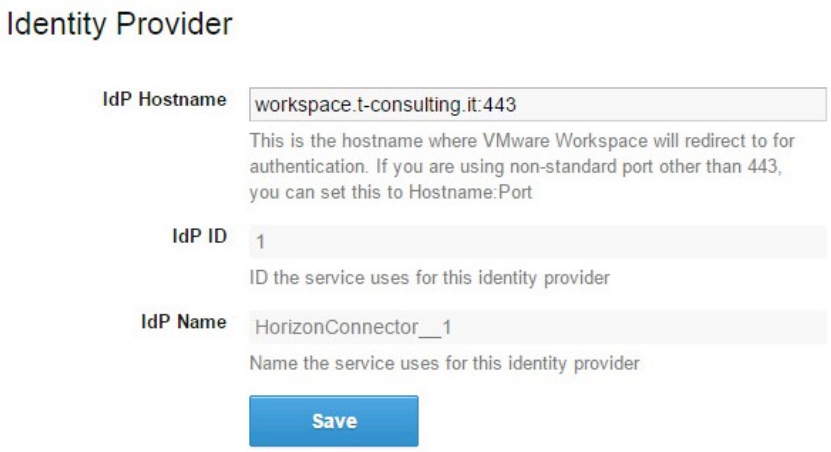


Figura 3.2.4.2 Schermata Identity Provider dopo la modifica di Workspace FQDN

Ora che Horizon Workspace Portal è accessibile da qualsiasi rete non resta che abilitare i pool applicativi e inserire le applicazioni da distribuire ai dipendenti.

3.2.5 Abilitazione View Pool

Prima di associare il Connection Server a Workspace Portal è necessario abilitare l'autenticazione SAML, questa operazione si esegue tramite il pannello di configurazione di View sul Connection Server. Dal menu View Configuration → Servers → selezionare il Connection Server dall'elenco → Edit...

Selezionando la scheda "Authentication" si possono gestire tutte le modalità di autenticazione al server, in particolare è possibile abilitare l'autenticatore SAML.

Nel campo Metadata URL si sostituisce il testo "<YOUR HORIZON SERVER NAME>" con l'indirizzo di accesso da rete esterna; il Connection Server registrerà così il certificato di sicurezza del Reverse Proxy.

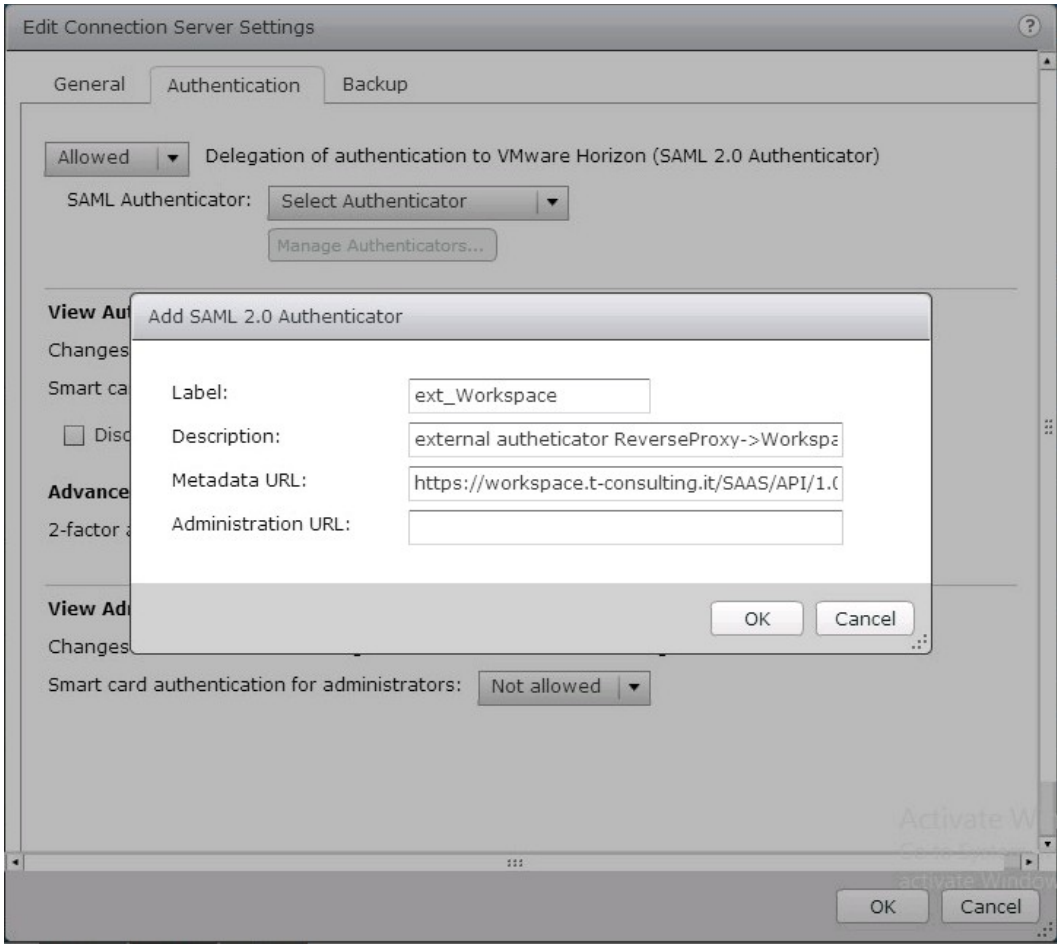


Figura 3.2.5.1 Aggiunta dell'authenticator SAML

Una volta creato l'authenticator si può procedere inserendo la macchina Workspace Portal nel dominio Windows, quest'operazione si svolge dal Connector Services Admin, nel menu Join Domain.

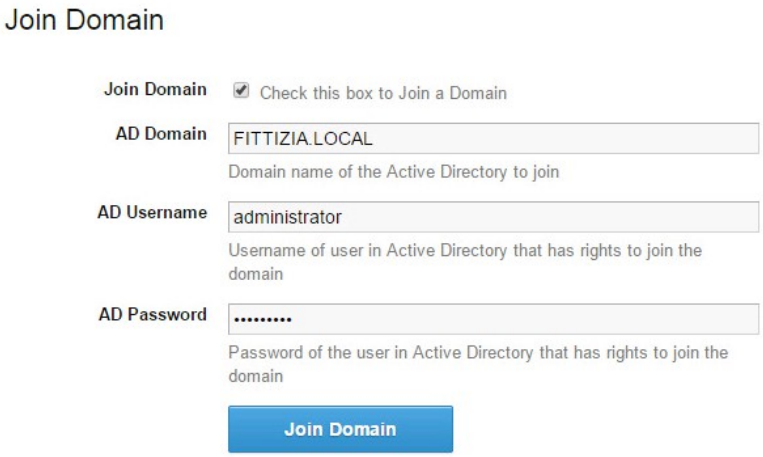


Figura 3.2.5.2 Inserimento di Workspace Portal in dominio Windows

Dal medesimo pannello di configurazione (Connector Services Admin) si prosegue abilitando i View Pools dall'apposito menu, indicando il nome di dominio del Connection Server con cui si dovrà sincronizzare Workspace Portal.

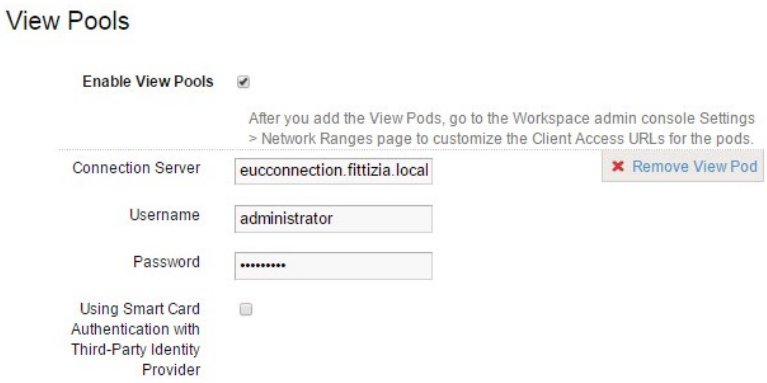


Figura 3.2.5.3 Abilitazione dei View Pools

La procedura avviserà che il certificato SSL non è valido poiché si tratta di un certificato auto firmato e sarà necessario indicargli manualmente di accettarlo.
Si può procedere forzando la sincronizzazione tramite il pulsante “Sync Now” prima di confermare le impostazioni con il pulsante “Save”.

L'ultimo passaggio necessario per concludere la configurazione è indicare a Workspace l'indirizzo del Security Server per permettere all'utente di collegarsi ai Desktop virtuali e le applicazioni remote.

Questa configurazione si effettua dalla Workspace Admin Console, nel menu Network Ranges, indicando come “Client Access Url Host” l'indirizzo Internet del Server Workspace Portal e in “Client Access Url Port” la porta assegnata al Security Server (4433 come indicato durante l'installazione del Server).

workspace.t-consulting.it:4433 è l'effettivo indirizzo a cui risponde il Security Server.

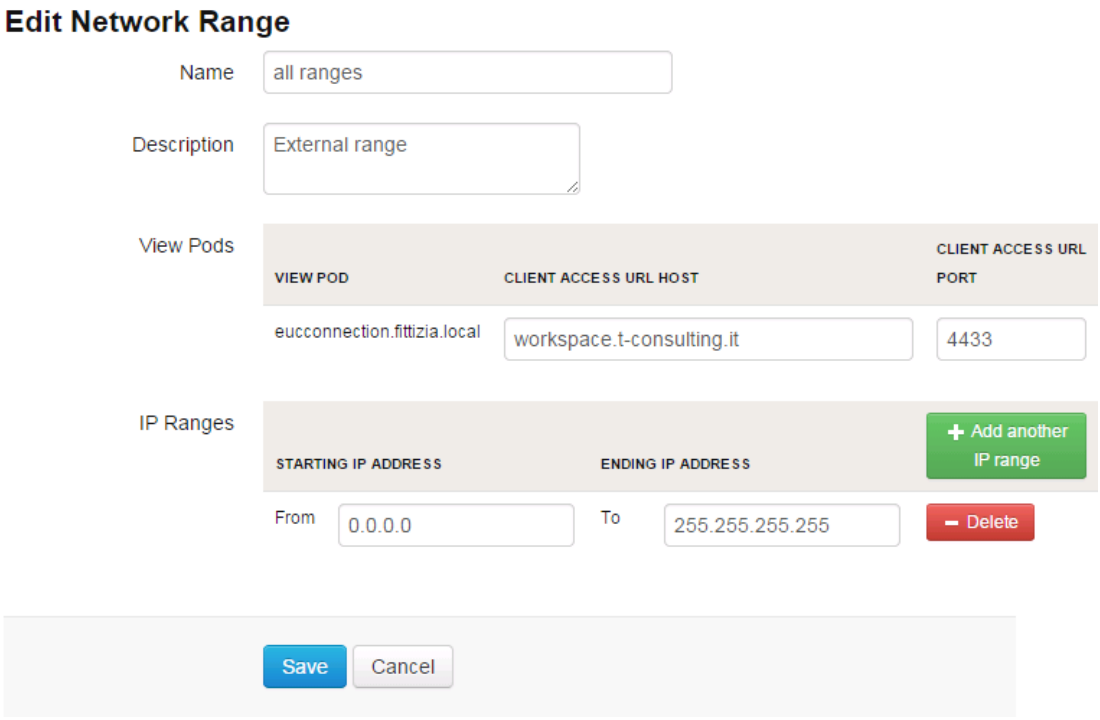


Figura 3.2.5.4 Assegnazione dell'indirizzo di connessione al Security Server

3.2.6 Aggiunta di applicazioni su Workspace Portal

Aggiungere Application Pools

Prima di poter aggiungere dei pool applicativi è necessario collegare il Server RDS al Connection Server, questa operazione si esegue sul pannello di amministrazione del Connection Server.

Si aggiunge la Farm RDSH tramite il pannello Resources → Farms e si completa la procedura guidata.

Dal menu Catalog → Application Pools è possibile poi aggiungere i pool di applicativi. cliccando sul pulsante Add... viene mostrato l'intero elenco di applicazioni presenti sul server RDS.

Dall'elenco di applicazioni si possono selezionare quelle che si vogliono distribuire, si può impostare poi il nome dell'applicazione che verrà visualizzato sul portale e infine si aggiungono i permessi, indicando quali gruppi o quali utenti possono avere accesso all'applicazione.

È possibile distribuire anche un'applicazione non installata sul Server ma presente sotto forma di file eseguibile, in questo caso durante la creazione del pool basta selezionare "Add application pool manually" e compilare i campi indicando in particolare il nome dell'applicazione e il percorso in cui si trova il file eseguibile sul Server.

Aggiungere Software as a Service

Tramite Workspace Admin Console è possibile aggiungere anche Web Application all'elenco di applicazioni di Workspace.

Questa operazione si esegue da Catalog → Add Application → ...create a new one.

Durante la procedura guidata è richiesto il nome dell'applicazione, una descrizione e l'icona da visualizzare sul portale.

È inoltre possibile selezionare un profilo di autenticazione SAML per applicazioni che supportano il Single Sign On, in modo da utilizzare automaticamente le credenziali dell'utente salvate in Active Directory senza dover chiedere nuovamente l'autenticazione quando viene avviata l'applicazione.

Se si è scelto un profilo di autenticazione si procederà compilando i dati necessari per eseguire l'accesso automatico all'applicazione, in caso contrario si procederà direttamente all'inserimento dell'indirizzo Internet dell'applicazione.

L'ultimo passaggio è l'assegnazione dell'applicazione ai gruppi di utenti, o ai singoli utenti, che possono usufruirne.

È anche possibile indicare se l'applicazione apparirà automaticamente sull'home page degli utenti o se deve essere inserita solamente nell'Application Center (uno Store privato delle applicazioni accessibile tramite il portale); nel secondo caso sarà l'utente a scegliere se aggiungere o no l'applicazione sulla sua home page.

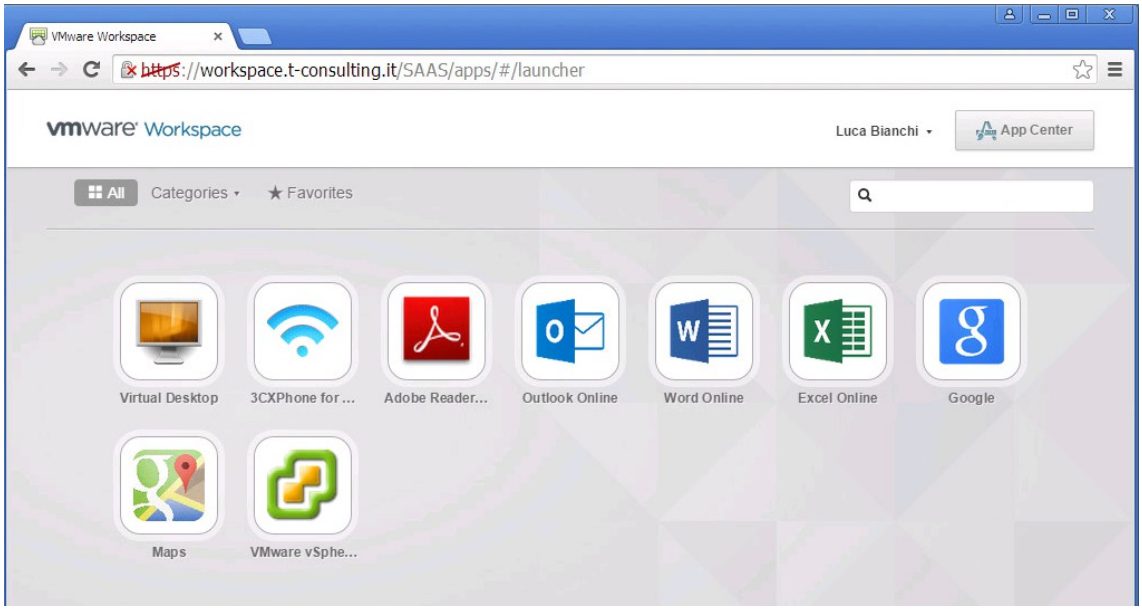


Figura 3.2.6.1 Home page di un utente con qualche applicazione di prova, visualizzazione Desktop

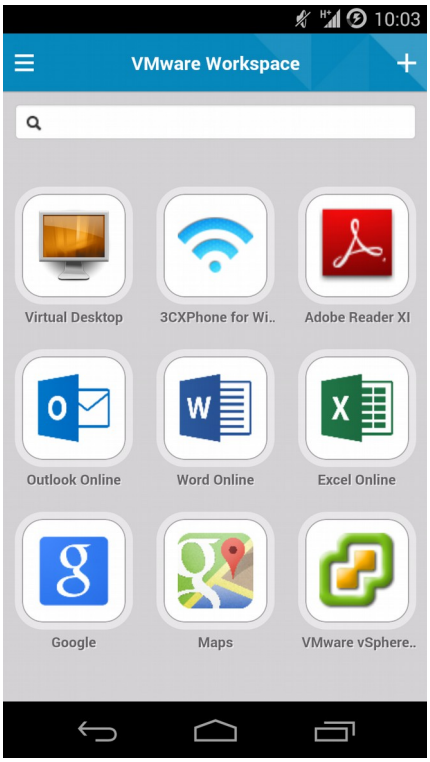


Figura 3.2.6.2 Visualizzazione da dispositivo Android

VALUTAZIONE DEI RISULTATI OTTENUTI

Valutazione personale sui risultati ottenuti

Personalmente mi ritengo molto soddisfatto del risultato finale del progetto e credo che un ambiente come quello realizzato possa essere molto utile per un'azienda che vuole innovarsi e aggiornare il proprio sistema informatico.

È stata un'esperienza molto formativa che mi ha permesso di studiare tecnologie innovative e complesse che senza un'infrastruttura professionale come quella fornita dall'azienda non sarei mai stato in grado di testare.

Purtroppo non è stato possibile analizzare alcune delle tecnologie che ci si era prefissati inizialmente, perché esulavano dall'obiettivo finale del progetto o per altre problematiche; di seguito saranno riportate le motivazioni sull'esclusione di "AirWatch by VMware" dal progetto.

Problematiche riscontrate con AirWatch

Allo stato iniziale del progetto si era deciso di inserire nel progetto il servizio "AirWatch by VMware" per la gestione dei dispositivi personali per il BYOD. Questo test però è stato abbandonato a causa della complessa procedura richiesta per l'avvio della versione di prova e della segretezza della struttura della piattaforma, nonché della scarsissima quantità di documentazione ufficiale reperibile.

Valutazione del Tutor aziendale sulla realizzazione del progetto

"I risultati emersi nello sviluppo del presente progetto risultano estremamente interessanti da molteplici punti di vista. Innanzitutto emerge una notevole maturità delle componenti tecnologiche coinvolte per quel che riguarda l'integrazione tra le componenti di backend (VMware).

In secondo luogo oltre a garantire una più che soddisfacente "User Experience" grazie al supporto multi device, alla stabilità della piattaforma e non ultimo alla velocità di esecuzione consente, in modo molto concreto, di ottenere una significativa riduzione del "Total Cost of Ownership" di ogni Endpoint, indipendentemente dalla dimensione dell'azienda cliente coinvolta.

Dal punto di vista del mercato ritengo che i tempi siano maturi per una proposizione sistematica di questo tipo di soluzioni generando così valore per le aziende clienti e differenziazione nell'offerta per le aziende IT che perseguiranno tale strada."

CONSIDERAZIONI FINALI E SVILUPPI FUTURI

Conclusioni

L'obiettivo di questo progetto è stato implementare un ambiente di test dimostrando le capacità delle nuove tecnologie di End User Computing distribuite da VMware.
Partendo da una conoscenza pressoché nulla dell'ambiente VMware e dei prodotti forniti dalla suite Horizon 6, grazie ad uno studio approfondito sulla documentazione ufficiale e i laboratori online messi a disposizione da VMware si è riusciti ad implementare con successo un ambiente complesso come quello descritto in questa tesi.
Dal punto di vista personale è stata un'esperienza molto formativa che mi ha fornito delle valide competenze professionali.

Lo sviluppo del mercato VMware orientato all'End User Computing è appena cominciato, ogni mese vengono assimilate nuove aziende del settore e aggiunti così prodotti all'offerta VMware.
Si sta parlando quindi di un settore in piena evoluzione dove è molto importante stare al passo coi tempi e studiare le nuove tecnologie rilasciate, essere i primi a fornire questi prodotti su un mercato in continuo sviluppo può essere strategico per un'azienda fornitrice di servizi informatici.

Horizon Workspace Portal può essere un valido strumento per aziende di grandi dimensioni che devono distribuire ai propri dipendenti grandi numeri di applicazioni e implementano politiche di Bring Your Own Device.
Soprattutto nell'ambito del BYOD questo strumento facilita l'inserimento di nuovi dipendenti, non essendo più necessaria l'installazione manuale dei software sui dispositivi personali o la creazione di collegamenti VPN per accedere ai dati aziendali in sicurezza.

Grazie alle Dashboard di riepilogo il personale IT può mantenere sotto controllo lo stato del servizio e fornire Report dettagliati sull'utilizzo della piattaforma da parte degli utenti, come ad esempio la frequenza di utilizzo di un'applicazione o in quali orari vengono lanciate più spesso determinate categorie di applicazioni.

In questi ultimi anni grazie all'avvento dei dispositivi mobile e delle connessioni Internet ad alta velocità stanno cambiando anche le modalità lavorative dei dipendenti, il lavoro da remoto non è più da considerare un'eccezione, ma una normalità.
I dipendenti moderni hanno bisogno di poter svolgere le loro mansioni in qualsiasi momento e in qualsiasi luogo, Horizon Workspace Portal offre gli strumenti necessari per creare un ambiente di lavoro user-friendly su qualsiasi dispositivo e più facilmente gestibile e monitorabile dal personale informatico dell'azienda.

Sviluppi futuri

Durante lo sviluppo del progetto ci si è concentrati principalmente sulla creazione e configurazione dei Server e sullo sviluppo dell'App Delivery, per lo svolgimento dei test è stata realizzata un'infrastruttura VDI basilare.
In futuro si può studiare un'integrazione con un'infrastruttura VDI più sviluppata, creando un ambiente con macchine virtuali “Linked-Clone”, ovvero un sistema dove più utenti condividono la stessa immagine disco e le applicazioni sono distribuite tramite Workspace Portal in relazione alle diverse mansioni dei dipendenti e ai gruppi di appartenenza. In un ambiente del genere si potranno gestire le impostazioni personali degli utenti (come sfondo del desktop, preferenze applicazioni ecc.) tramite Persona Management, un altro componente della suite Horizon 6.

RINGRAZIAMENTI

Vorrei ringraziare il Prof. Gabriele D'Angelo, non solo perché ha accettato di farmi da relatore per la stesura di questa tesi, ma soprattutto per la grande passione che mi ha trasmesso in questi anni e che per me è stata fonte di grande ispirazione.

Vorrei ringraziare tutti i ragazzi di T-Consulting, che mi hanno accompagnato durante la realizzazione di questo progetto e hanno condiviso con me le loro conoscenze e messo a disposizione la loro infrastruttura informatica per la realizzazione del progetto.

Vorrei ringraziare tutti i miei familiari che hanno creduto in me durante questi anni e mi hanno sempre supportato.

Vorrei ringraziare Chiara per essere speciale.

Vorrei ringraziare infine i miei compagni di corso, che hanno reso meravigliosi questi anni passati insieme.

Grazie di cuore.

BIBLIOGRAFIA

[1] The Linux Information Project. http://www.linfo.org/dumb_terminal.html

[2] Wikipedia. http://en.wikipedia.org/wiki/Computer_terminal#.22Intelligent.22_terminals

[3] ECMA International. http://www.ecma-international.org/publications/files/ECMA-ST/Ecma-048.pdf

[4] The Linux Information Project. http://www.linfo.org/client_server.html

[5] Netcraft. http://news.netcraft.com/archives/2015/01/15/january-2015-web-server-survey.html

[6] VMware. PcoIP supports AES-128, 192 and 256 https://pubs.vmware.com/horizon-view-60/index.jsp#com.vmware.horizon-view.planning.doc/GUID-E2FFCC1F-B14A-4A4E-A36C-994EACC542B6.html

RDP supports 128-bit encryption https://pubs.vmware.com/horizon-view-60/index.jsp#com.vmware.horizon-view.planning.doc/GUID-342A2ECC-85DD-43AA-9A14-473B25B07EF2.html

[7] VMware. http://www.vmware.com/files/pdf/view/VMware-View-5-PCoIP-Network-Optimization-Guide.pdf

[8] VMware. http://www.vmware.com/files/it/pdf/view/vmware-top-five-considerations-for-choosing-a-zero-client-environment-techwp.pdf

[9] Pawel Chrobak, Implementation of Virtual Desktop Infrastructure in academic laboratories, Federated Conference on Computer Science and Information Systems, Wroclaw University of Economy, 2014. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6933148

[10] Jorge Orchilles, Virtualization: The benefits of VDI. https://technet.microsoft.com/en-us/magazine/dn170431.aspx

[11] VMware https://pubs.vmware.com/horizon-view-60/index.jsp#com.vmware.horizon-view.planning.doc/GUID-5DC232B4-778B-4D9C-B995-B8850CF35096.html

[12] Ankur Srivastava, vDaaS Reference Architecture. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6139359