SWISS ASR

White Paper

Molto spesso (sempre in effetti), quando un nostro collaboratore presenta OfficeNetPoint ad un possibile cliente, nasce la discussione sulla migliore infrastruttura necessaria al suo corretto funzionamento.

OfficeNetPoint Easy-Edition funziona con qualsiasi configurazione, dal singolo PC al Cloud. È chiaro però che, a dipendenza della configurazione, non tutte le caratteristiche e funzionalità possono essere attivate.

Ci sono inoltre altre considerazioni da tener presente: funzionalità richieste dal cliente, sicurezza e riservatezza dei dati, il *total cost of ownership* (TCO, che include costi di investimento, costi di manutenzione dell'hardware e dei software di base).

Anche aspetti legati a *cultura aziendale e formazione* nonché *abitudini operative* giocano un ruolo importante nella disponibilità ad accettare nuove tecnologie.

Per fare un po' di chiarezza, presento in questo documento tutte le configurazioni compatibili con OfficeNetPoint Easy-Edition, che verranno poi riportate in una tabella riassuntiva con i costi annuali per utente.

Questo documento non richiede specifiche conoscenze informatiche e cerca di spiegare in maniera semplice concetti tecnici che - anche se giornalmente utilizzati nel linguaggio comune - non sempre sono capiti in tutte le loro sfaccettature.

Premesse

Le reti tradizionali aziendali sono progettate principalmente per fornire agli utenti accesso ad applicazioni e dati ospitati in centri dati aziendali gestiti con un livello di sicurezza perimetrale elevato. Il modello tradizionale presuppone che gli utenti accedano ad applicazioni e dati all'interno del perimetro della rete aziendale, tramite collegamenti WAN dalle filiali o da remoto tramite connessioni VPN.

L'adozione di applicazioni SaaS (Software as a Service), come Microsoft 365, consente di spostare una combinazione di servizi e dati all'esterno del perimetro di rete[1].

Ma cos'è il cloud?

Il termine anglosassone *Cloud* (in italiano "nuvola") indica una particolare architettura di sistemi informatici in cui le risorse sono distribuite all'interno di una rete e scalabili sulla base delle effettive necessità temporali degli utenti. Si crea così un layer astratto per il quale ad esempio gli utilizzatori non vedono più supporti fisici (dischi) o server con banche dati, bensì servizi specifici resi disponibili sulla base delle effettive esigenze dell'utente.

Il cloud va quindi visto come insieme di tecnologie che sfruttano Internet quale strumento di archiviazione ed elaborazione di dati che non sono gestite all'interno del perimetro di rete aziendale.

Chi utilizza il Cloud?

Praticamente tutti, anche senza consapevolezza. Quando si riceve una e-mail si pensanche vi sia un collegamento diretto tra il computer di chi la spedisce e quello di chi la riceve: niente di più falso!

Il servizio offerto dal provider del mittente comunica con il servizio cloud che memorizza e (tiene memorizzata) la e-mail del destinatario. Entrambi, mittente e destinatario, utilizzano servizi cloud perché potenza di calcolo e memorizzazione sono di terzi (i rispettivi provider) sui quali nessuno ha controllo alcuno.

Cercherò quindi di rispondere alla domanda relativa alle possibili configurazioni per supportare OfficeNetPoint Easy-Edition, dal singolo PC alla rete di PC virtuali, incluse soluzioni cloud e anche di mettere un po' di ordine nella questione.

A titolo di esempio considererò un team di 5-10 utenti, con necessità di condividere documenti e banca dati, e nello specifico quello che potrebbe essere uno studio legale con due o tre professionisti e tre - sei persone in segretariato.

[1] Principi di connettività di rete di Microsoft 365 - Microsoft 365 Enterprise | Microsoft Docs

Assunto: ogni utente dispone già di una postazione in ufficio con i seguenti prerequisiti:

- Un PC con sistema operativo Windows 10, recente, con memoria e disco sufficienti,
- Una licenza d'utilizzo per un piano Microsoft 365 (Word, Excel, Outlook, ecc.),
- Collegamento internet affidabile,
- Accesso ad una stampante multifunzione, in grado di eseguire scansioni.

Altri due requisiti sono indispensabili al funzionamento di qualsiasi applicativo di gruppo:

- Un contenitore comune ove ospitare i documenti, accessibile a tutti gli utenti,
- Un contenitore comune ove ospitare una banca dati, accessibile a tutti gli utenti.

Documenti e altri files (immagini, fogli di calcolo, ecc.) da una parte e banca dati dall'altra richiedono però differenti requisiti di memorizzazione, per cui:

Documenti e file

Documenti e file devono sempre essere memorizzati in una unità fisica, che alla fine risulta essere sempre e ancora un disco (sia esso rigido, SSD o perfino una chiavetta USB) che può essere quello della periferica che si sta utilizzando oppure quello di un'altra periferica della stessa rete locale (per esempio NAS o Server) oppure sito all'esterno montato in un server di proprietà del cliente (*housing*) oppure di proprietà di terzi (*hosting*).

A titolo di esempio, per i non tecnici: supponete di avere una somma di denaro: la si può custodire in tasca (*chiavetta USB*), in casa sotto il materasso (*condivisa in rete locale*), oppure in una cassaforte casalinga (*NAS o Server locale*), in banca in una cassetta di sicurezza (*housing*) oppure "virtualmente" su un conto corrente (*hosting*, *cloud*).

Banca dati

Una banca dati contiene dati, generalmente in forma tabellare, ad esempio elenchi clienti e fornitori, registrazioni contabili, ecc. ed il suo utilizzo si rende necessario quando vi è l'esigenza di disporre di estrazioni elaborate di dati Come nel caso dei documenti (testi, tabelle di calcolo, immagini, ecc.) anche esse sono memorizzate su memorie di massa, con la differenza però che (per esigenze di elaborazione) non vi è corrispondenza tra una registrazione ed un file, bensì numerose registrazioni (se non tutte) risiedono nello stesso file.

Ciò rende l'accesso alle informazioni più veloce ma anche più complicato, e quindi deve essere gestito in maniera diversa.

Un esempio rende bene la differenza tra l'accesso ad un documento e l'accesso ad una banca dati: consultare un documento corrisponde più o meno a recarsi nel proprio archivio o biblioteca (privata) e pigliare un libro o un documento. La consultazione di una banca dati, in genere, offre un servizio supplementare, e corrisponde ad esempio, a richiedere tutte le fatture di un dato anno per un certo prodotto ed eventualmente per area geografica.

Come nella vita reale, oltre ai documenti, si richiede un servizio aggiuntivo, che in IT, si traduce in richiesta di potenza di calcolo e accesso multiplo a gran mole di dati.

Questa potenza di calcolo può essere messa a disposizione dalla propria stazione di lavoro ("*mi reco nell'archivio contabile mi piglio tutti i documenti ed eseguo nel mio ufficio ricerca e selezione*") oppure da un gestore della banca dati ("*richiedo ad un'archivista di selezionarmi i documenti richiesti*").

Se l'archivio è di piccole dimensioni, fisicamente vicino al richiedente e se relativamente poche persone vi accedono contemporanee, la consultazione (e l'elaborazione) in proprio è possibile.

D'altro canto, se molti richiedenti devono consultare contemporaneamente l'archivio ed esso contiene grande mole di documenti, appare subito chiaro che disporre di un archivista e richiederne il servizio risulta la soluzione più efficace.

E nell'IT vale lo stesso concetto.

Ci sono banche dati relazionali basate su file, per esempio Microsoft Access, che non offrono però il servizio dell'archivista ed altre (Microsoft SQL, MySQL) che offrono tale servizio, evadendo in proprio le richieste e mettendo a disposizione dei richiedenti i risultati delle ricerche.

Come nella vita reale, le prime, quelle basate su file, devono essere vicine al cliente (nello stesso computer dell'utilizzatore o al massimo nella stessa rete locale), contenere un numero limitato di registrazioni, decine di migliaia e non milioni, ed il numero di utilizzatori deve essere limitato (nel caso di Microsoft Access - a dipendenza dell'applicativo - una dozzina al massimo). Le seconde possono essere "distanti", anche in reti remote, perché il traffico dei dati si limita alle domande e alle risposte, senza mettere tutti i dati necessari all'elaborazione in rete.

Sicurezza dei dati

I dati devono essere mantenuti in sicurezza.

Due concetti differenti (ed in parte antitetici): la salvaguardia dei dati e la riservatezza dei dati (in inglese *Data Backup* e *Data Security*).

Salvaguardia dei dati

Sotto questo concetto cadono tutte quelle misure atte a garantire l'integrità dei dati e delle informazioni contro perdite causate da rotture o furti dell'hardware, software nocivi (malware o ransomware) o da eventi esterni come incendi, allagamenti o interruzioni di corrente.

Riservatezza dei dati

La minaccia alla riservatezza dei dati può provenire sia dall'esterno, sia dall'interno dell'azienda (accessi illeciti ai dati) e quella di malware, virus e ransomware può ledere, anche la loro integrità.

Per contrastarle bisogna da un canto proteggere fisicamente i dispositivi di memorizzazione e proteggere e monitorare gli accessi ai dati.

La proliferazione di copie (anche esterne) causate dalle politiche di salvaguardia dei dati (*più copie dei dati si hanno, meno è la probabilità di perderli*) rendono più fragile la loro riservatezza (*ma più alta è la probabilità che qualcuno non autorizzato vi acceda*) e quindi le due politiche di protezione devono essere bilanciate, al fine di trovare una soluzione ottimale che tenga conto dei due aspetti.

In ogni caso se i dati sono on-premises, l'accesso alla rete aziendale deve essere protetto da un firewall a doppia autenticazione degli utenti con costante monitoraggio del traffico per e dalla rete locale, oltre che essere mezzo valido a contrastare ogni tentativo di utilizzo di malware mediante l'utilizzo e manutenzione costante di software dedicati a tale protezione.

Riassumendo:

Molti tecnici informatici concentrano sforzi e mezzi per rinforzare la sicurezza perimetrale delle reti aziendali. È una visione corretta ma purtroppo limitata. Il crescente utilizzo consapevole o meno di nuove tecnologie impone un approccio olistico. Con l'adozione di servizi cloud, i servizi di rete e dati vengono distribuiti tra centri dati locali ed il cloud con la conseguenza che la sola sicurezza perimetrale non è più sufficiente.

Gli utenti remoti si connettono da postazioni non controllate, sistemi operativi differenti e non sempre aggiornati e aggiornabili, da reti casalinghe, hotel, aeroporti. Le funzionalità di protezione devono quindi essere costantemente aggiornate laddove la limitazione di utilizzo alla sola rete aziendale è limitativa e oggigiorno non è più sostenibile vietare ogni collegamento ad Internet perché gran parte dei servizi sono offerti esclusivamente online.

L'autenticazione a più fattori, la configurazione di più criteri per monitorare utilizzi anomali, insolite o rischiose quali il download di grandi moli di dati o ripetuti tentativi di accesso non riusciti o connessioni da indirizzi IP sconosciuti devono costantemente essere monitorati.

La questione basilare che ci si può porre è la seguente: un *tenant* come Microsoft offre migliori garanzie di monitoraggio e sicurezza di quella offerta da un router aziendale preconfigurato con "firewall" integrato? E la risposta è certamente sì, perché dispone di più informazioni e potenza di calcolo di qualsiasi rete locale.

Come visto, i due concetti (riservatezza e integrità dei dati) sono legati e parzialmente sovrapposti in quanto misure tipicamente legate alla loro riservatezza ne promuovono anche l'integrità.

Misura	Descrizione	Tempi di ripristino	Costi di ripristino	Costi di implementazione
Hardware ridondante	Dischi in RAID, Doppia Alimentazione, Batterie di supporto	Ripristino immediato.	Sostituzione dell'hardware,	Maggiorazione di prezzo per l'hardware ridondante. Generalmente solo su Server e NAS [3'000 / 6'000]
Copie di sicurezza in sede	Generalmente NAS (a loro volta ridondanti) o dischi USB. Si possono duplicare solo i dati oppure dati e sistema operativi (immagine)	4 - 8 ore	[1'000]	Software di Backup e periferiche NAS, dischi
Copie di sicurezza esterne	Generalmente NAS Contratti con provider esterni	6 – 10 ore	2'500	Connettività o contratto con provider esterno. Costo per Gbyte e copie di ritenzione.

Tabella 1 Tabella riassuntiva salvaguardia dati

Misura	Descrizione	Tempi di ripristino	Costi di manutenzione annuale	Costi di implementazione
Firewall	Dispositivo di controllo del traffico in entrata e uscita.	Ripristino immediato.	[500]	[3'000- 4'000]
Antivirus	Software di controllo minacce software.	4 - 8 ore	600	[500]

Tabella 2 Tabella riassuntiva riservatezza dei dati

I costi per una incomprimibile configurazione minimale si possono così ricapitolare:

Materiale	Costi annuali	Costi investimento
Postazioni personali		10'000
Switch di rete		[800]
Router e collegamento internet	[1'200]	
Firewall con doppia autenticazione	[250]	[3'000]
Stampante multifunzione		[3'500]
Licenze MS-Office 365	1'300	
NAS (2) per backup		[2'500]
IPS (Protezione contro interruzioni di corrente)		[500]
Costi di installazione		[3'000]
Licenze Microsoft 365	1'300	[500]
Posta elettronica	160	[500]
Antivirus	400	[200]
Aggiornamento annuale dei PC	1'000	
Totali	5'510	24'500

Tabella 3 Prospetto con costi per configurazione minima.

Come visto, oltre all'acquisto e messa in funzione delle varie postazioni personali e dell'infrastruttura minima (una rete locale con cablaggio e dispositivi di rete, un collegamento ad Internet, una stampante multifunzione, uno o più dispositivi di backup, un firewall e software di base quale MS Office), il nostro team ha già necessitato di investimento per 24'500 e costi ricorrenti annuali di 5'510.

Calcolando una vita media di 4 anni per l'hardware, si arriva a costi annualizzati di circa 1'000 per utente, non calcolando eventuali altri dispositivi personali quali PC portatili e telefoni cellulari.

Cloud oppure on-premises?

Un sistema informatico è costituito da potenza di calcolo e memorizzazione di dati. Le unità di memorizzazione dei dati e/o la potenza di calcolo possono essere situate in sede (*on-premises*) oppure all'esterno: *in Cloud* se gestiti da terzi, *in hosting* se le risorse sono riservate ad un solo cliente e *in housing* se possedute dal cliente ma locate in locali (securizzati) di terzi.

Vi sono anche soluzioni intermedie, in cui solo una parte dei dati o della potenza di calcolo è in cloud. La quasi la totalità dei miei clienti, anche quelli che non vogliono nemmeno sentir parlare di cloud in cloud già lo sono, a loro insaputa; in fondo basterebbe si chiedessero dove, come e da chi viene gestita la loro posta elettronica.

Le configurazioni possibili sono - a grandi linee - tre on-premises e due in cloud:

On-premises:

- PC in rete locale con NAS,
- PC in rete locale in dominio con server aziendale,
- PC in rete con Remote Desktop su server locale.

In Cloud:

- Server aziendale con accesso Remote Desktop su server in hosting o housing,
- PC con accesso a drive virtuali (ad esempio OneDrive) per i documenti e servizio banca dati in cloud (per esempio Azure SQL).

Qui di seguito analizzerò costi e benefici di ogni configurazione, partendo dalla configurazione base della Tabella 3.

OfficeNetPoint Easy Edition

Il costo annuale per le licenze d'uso di OfficeNetPoint Easy-Edition è indipendente dalla configurazione scelta. Il costo di aggiornamento è compreso nella licenza annuale, a patto che la piattaforma di ogni stazione di lavoro sia aggiornata (segnatamente Microsoft 365) e uniforme.

Se la piattaforma non è omogenea, con sistemi operativi diversamente aggiornati, e/o differenti versioni di Microsoft 365 (o di Microsoft 2019), i costi di manutenzione e installazione possono aumentare. Inoltre, possono sorgere problemi di instabilità che non possono essere considerati manutenzioni ordinarie e quindi comprese nei contratti.

Analisi costi/benefici

I costi indipendenti dal numero di utenti (connessione internet, stampante multifunzione e in gran misura la taglia dei server saranno evidenziati tra parentesi quadre, così di facilitare un ricalcolo in base agli effettivi utenti. Gli importi presenti nelle tabelle sono indicativi ed arrotondati. Possono indifferentemente essere interpretati in EUR, CHF o USD.

1. On-premises: PC in rete locale con NAS

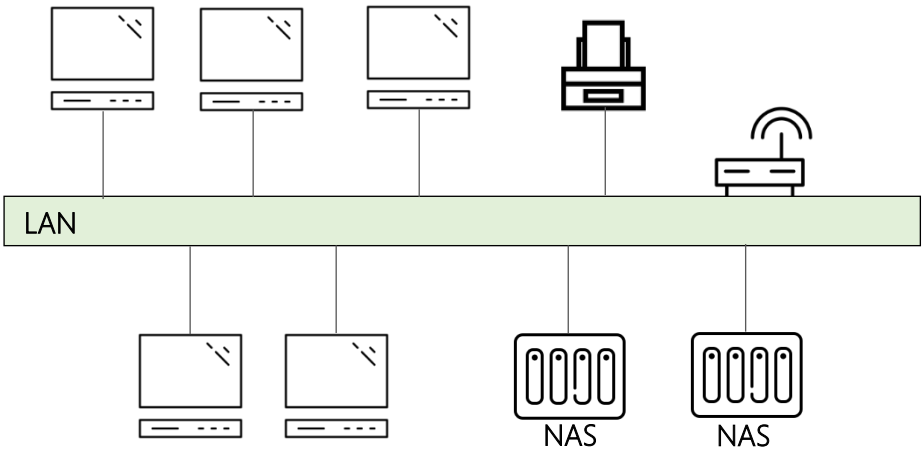

Figura 1 Configurazione minima

Questa configurazione non prevede la possibilità di accesso remoto, se non con metodi artigianali o diretti dal dispositivo remoto ad una stazione di lavoro nel perimetro di rete aziendale e quindi altamente sconsigliati. Non è nemmeno garantita l'uniformità delle varie stazioni di lavoro, non essendo queste ultime inserite in un dominio.

In questa configurazione la banca dati di OfficeNetPoint Easy-Edition non può essere Microsoft SQL, nemmeno nella versione Express (gratuita, con limite a 10GB), dovendo forzatamente essere *file-based* e quindi tipo Microsoft Access (che è appunto basata su file). Con una decina di utenti su NAS le prestazioni possono seriamente risentirne soprattutto se la rete non è velocissima.

Per esperienza diretta: questa configurazione può essere presa in considerazione fino a 4, massimo 5 utenti, a patto di disporre di un'ottima struttura di rete e di NAS molto performanti, ovviamente a dipendenza dell'utilizzo concorrente (contemporaneo) delle risorse.

Costo annuo per utente

Materiale e infrastruttura	Costi annuali/utente
Infrastruttura di base (vedi Tabella 3)	1'000
OfficeNetPoint Easy-Edition	360
Totale	1'360

Tabella 4 Costi per configurazione 1.

Pro:

- La meno costosa tra quelle on-premises
- Permette di procrastinare investimenti nell'aspettativa di una scelta e transizione programmata,

Contro:

- Costi di manutenzione eccessivi,
- Rischio informatico pari alla somma dei rischi delle singole stazioni di lavoro (nel nostro caso moltiplicato per 10),
- Scalabilità dell'infrastruttura limitata,
- Richiede in ogni caso una messa a livello dei PC esistenti, dei loro sistemi operativi e software (MS Office in particolare),
- Accesso remoto non professionale, se non collegandosi ad una stazione di lavoro posta in ufficio (che deve essere accesa e funzionante),
- Prestazioni insufficienti per una decina di utenti con database basati su file (per esempio MS Access).

Pur non piacendomi molto, questo tipo di configurazione è già presente presso molti clienti, cresciuti senza aver sviluppato un vero e proprio concetto informatico. Si inizia con un PC, poi arriva il primo collaboratore, si acquista un altro PC e lo si connette in rete, fino a quando le risorse non sono più sufficienti e si acquista il primo NAS. Di regola Il secondo NAS arriva quando qualcuno fa notare che se il NAS si rompe, i dati andranno persi.

2. On-premises: PC in dominio con server aziendale

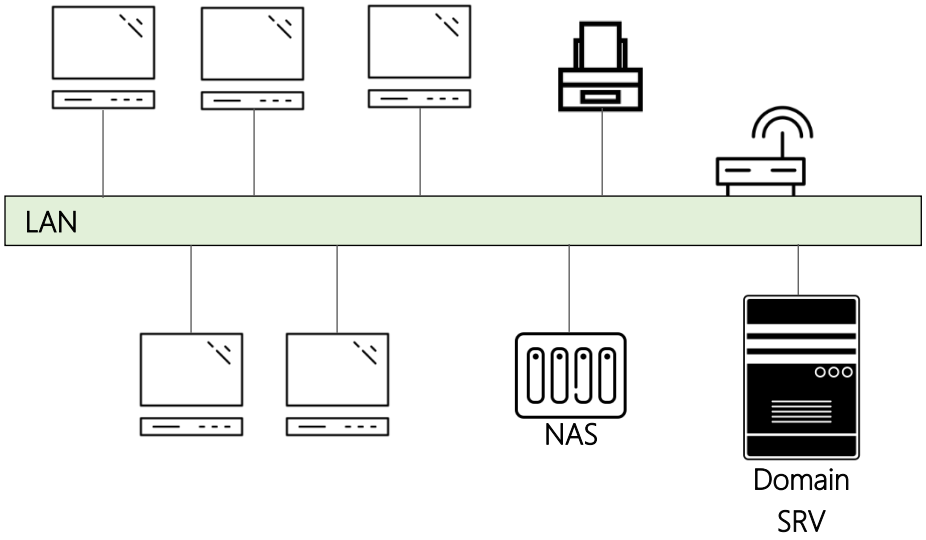

Figura 2 Configurazione 2.

Il server Windows apporta il concetto di dominio (uniformando le politiche di gestione dei PC) e permette di eliminare uno dei due NAS della configurazione precedente (disponendo di alimentazione e dischi RAID ridondanti).

Un tale server, rispetto al NAS permette anche di garantire l'omogeneità dei vari PC, ne cura centralmente gli aggiornamenti e la sicurezza degli accessi.

Il costo di un tale file- e domain- server si aggira sui 5'000, permette però di eliminare uno dei due NAS. OfficeNetPoint Easy-Edition è installato su ogni PC.

Inoltre, rispetto ad un NAS, il server è coperto da garanzia e supporto per 3-4 anni con tempi di intervento di 4h.

Costo annuo per utente

Materiale e infrastruttura	Costi annuale/utente
Infrastruttura di base	1'000
Risparmio su secondo NAS	-25
Costo annualizzato server	125
OfficeNetPoint Easy-Edition	360
Totale	**1'460**

Tabella 5 Costi per configrazione 2.

Pro:

- Offre maggiore garanzia di funzionamento, perché oggetto di manutenzione professionale con tempi di intervento di 4h,
- Offre maggiore controllo accessi sicurezza e manutenzione centralizzata.

Contro:

- In genere maggior consumo di energia elettrica rispetto ad un NAS,
- Necessita di uno spazio dedicato in sede,
- Possibilità di crescita e adattamento non lineari,
- Accesso remoto non professionale, se non collegandosi alla stazione di lavoro posta in ufficio (che deve essere accesa e funzionante),
- Prestazioni insufficienti per una decina di utenti con database basati su file (per esempio MS Access).

3. On-premises: PC in rete con Server aziendale in RDS

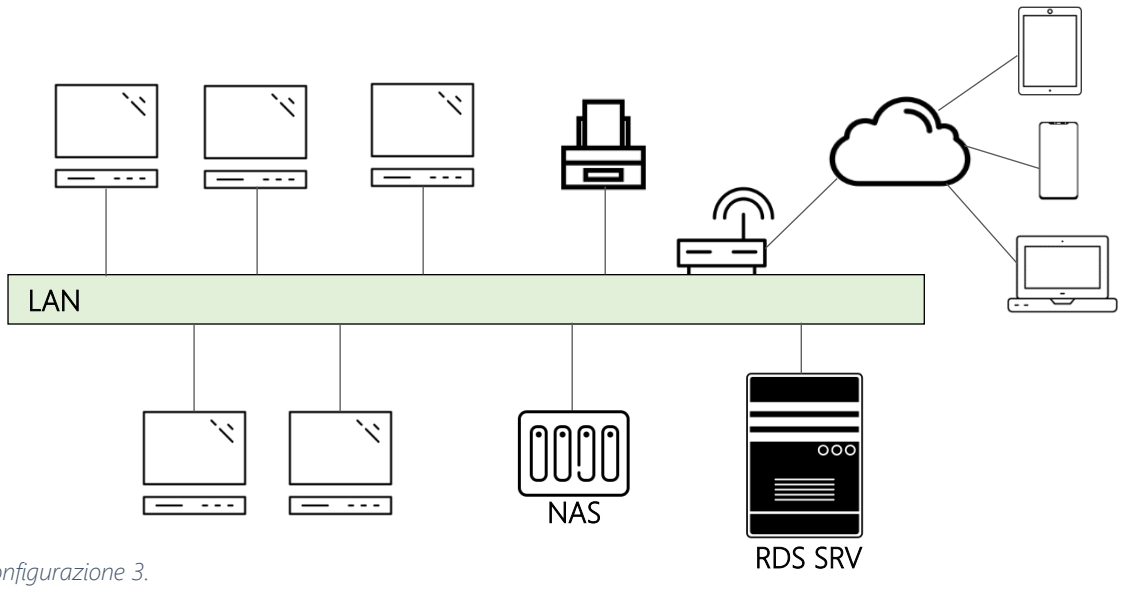

Figura 3 Configurazione 3.

Rispetto alla configurazione precedente, se correttamente configurato, permette di lavorare tramite Remote Desktop Protocol, ciò che consente l'utilizzo di PC non particolarmente performanti con sistemi operativi (Windows, Mac OS o Android) eterogenei.

L'accesso remoto è garantito e protetto nativamente attraverso il firewall e l'esperienza di utilizzo da remoto è identica a quella in sede.

Questa configurazione permette di definire dei desktop virtuali sul server uniformando così di fatto tutte le stazioni di lavoro, anche quelle esterne al perimetro aziendale, indipendentemente dal loro sistema operativo (Windows 10, Mac OS, Android o Linux).

Un server, con sufficiente memoria RAM (per una decina di utente al minimo 32GB) e dischi SSD, combina potenza di calcolo e memorizzazione dei dati senza utilizzare grandi risorse di rete, permettendo quindi una buona operatività anche con banche dati in MS Access, per una decina di utenti.

Vi è tuttavia la possibilità di definire un ulteriore server virtuale per Microsoft SQL Server.

Il costo di un server con le caratteristiche descritte si aggira sui 16'000 - 20'000, compresa la manutenzione per 4 anni, h24, quindi con un costo annualizzato di al massimo 4'000 – 5'000.

Costo annuo per utente

Materiale e infrastruttura	Costi annuali/utente
Infrastruttura di base	1'000
Risparmio su secondo NAS	-25
Costo Server	375/500
Risparmio su costi manutenzione PC	-100
OfficeNetPoint Easy-Edition	360
Totale	1'610 / 1'835

Tabella 6 Costi per configurazione 3.

Pro:

- Costi di manutenzione software ridotti (per omogeneità della piattaforma virtualizzata),
- Manutenzione h24 e garanzia compresi,
- Accesso remoto professionale e performante,
- Indipendenza ed allungamento della durata della piattaforma dei PC (Windows, Mac OS, Android e Linux),
- Manutenzione h24 e garanzia compresi,
- Possibilità di operare con PC vetusti e disomogenei.

Contro:

- Maggior utilizzo di corrente,
- Bisogna riservare un locale (protetto) per il server.

Fra le soluzioni on-premises è quella che - pur essendo finanziariamente la più costosa - rispetto ai costi evidenzia il miglior rapporto costi/benefici. Essendo i server rigorosamente virtualizzati, questa configurazione permette un futuro passaggio al cloud (configurazione 5) praticamente indolore.

4. In Cloud privato: Server aziendale in hosting

Rispetto alla configurazione precedente prevede lo spostamento del server dalla sede aziendale ad un centro di calcolo di un provider esterno.

Questa architettura corrisponde a quello che viene denominato *Cloud Privato*.

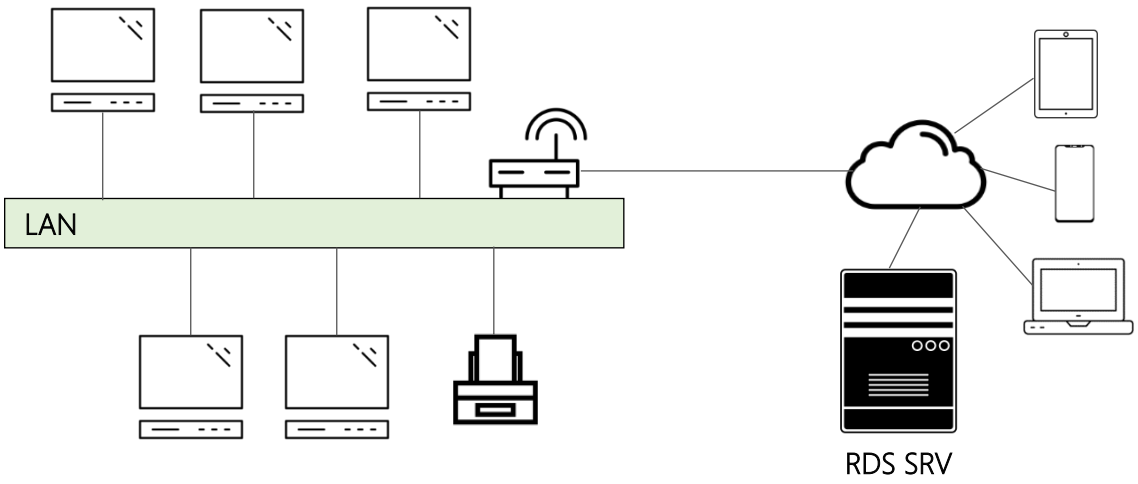

Figura 4 Configurazione 4.

In teoria questa configurazione corrisponde alla precedente, con la differenza che il server virtuale aziendale non è in sede nel perimetro di rete aziendale, bensì presso un hosting provider. Non vi è nessun investimento iniziale né in hardware né in infrastruttura locale, se non per le postazioni di lavoro degli utenti.

Costo annuo per utente

Materiale e infrastruttura	Costi annuali/utente
Infrastruttura di base	1'000
Risparmio su primo e secondo NAS	-50
Costo Server	300[2]
Risparmio su infrastruttura locale e manutenzione PC	-200
OfficeNetPoint Easy-Edition	360
Totale	1'360

Tabella 7 Costi configurazione 4.

Pro:

- Costi di manutenzione software ridotti (per omogeneità della piattaforma virtualizzata),
- Funzionamento (up-time) del 99.999% garantito,
- Accesso remoto professionale e performante,
- Indipendenza della piattaforma dei PC (Windows, Mac OS, Android e Linux),
- Manutenzione h24 e garanzia compresi,
- Possibilità di operare con PC vetusti e disomogenei,
- Telelavoro molto efficiente (anche con periferiche personali),
- Banca dati *file-based* utilizzabile per 10 persone,
- La configurazione può essere ridimensionata con estrema facilità.
- Possibilità di implementare soluzioni software tradizionali,

Contro:

- Necessità di valutare seriamente (due diligence) il provider dell'hosting.
- Assicurarsi che i dati in cloud siano memorizzati in un paese UE (per i residenti in un paese UE) o in Svizzera (per i residenti in Svizzera)

[2] Costo stimato presso nostro provider convenzionato, a Castel S.Pietro (BO)

5. PC con accesso a OneDrive e Azure SQL

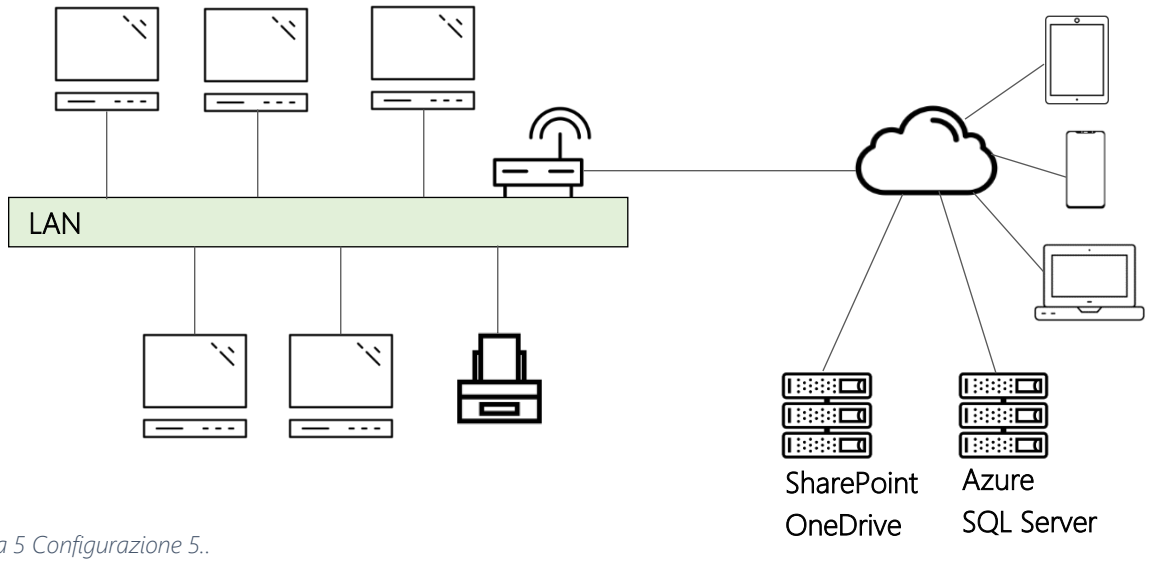

Figura 5 Configurazione 5..

Questa soluzione fa capo allo storage di 5 GB per utente compreso in Microsoft 365, in una soluzione serverless che utilizza i servizi cloud Azure di Microsoft.

La banca dati di OfficeNetPoint Easy-Edition in questo caso viene implementata nativamente su server Azure in maniera Serverless[3] (SQL Server), mentre l'archiviazione viene gestita da OfficeNetPoint Easy-Edition attraverso il suo modulo di integrazione OneDrive (compreso nella licenza base).

Per i clienti svizzeri, i dati in SharePoint e OneDrive sono memorizzati in Svizzera, per quelli siti in un paese UE in UE.

In questa configurazione si farà anche capo alla possibilità di OfficeNetPoint Easy-Edition di nativamente supportare banche dati Microsoft SQL ospitate su Azure. Il numero di utenti è quindi praticamente illimitato. Il costo dipende dall'utilizzo, quindi difficilmente calcolabile. Una nostra buona stima evidenzia costi, per un team di 10 utenti di circa 40 mensili[4].

OfficeNetPoint Easy-Edition offre anche la possibilità di eseguire un backup locale dei dati memorizzati nel Cloud.

Cade anche il concetto di infrastruttura di base, in quando l'ufficio può essere anche delocalizzato, senza necessità di costosi firewall.

È quindi indispensabile rivedere la tabella iniziale dei costi infrastrutturali:

[3] Serverless compute tier - Azure SQL Database | Microsoft Docs
[4] Valutazione basata sul nostro backoffice di 5 utenti.

Costo annuo per utente

Materiale	Costi annuali	Costi investimento
Postazioni personali		6'000
Switch di rete		800
Cablaggio		200
Router e collegamento internet	1'200	
Stampante multifunzione		3'500
Licenze MS-Office 365	1'300	
NAS per backup		1'000
Costi di installazione		2'000
Licenze Microsoft 365	1'300	
Antivirus	400	
Costo servizio Azure SQL	500	
Licenza OfficeNetPoint Easy-Edition	3'600	
Totali	8'300	13'500

Tabella 8 Costi Configurazione 5.

Il che ci dà un costo annualizzato di 1'167 per collaboratore.

Pro:

- Nessuna o quasi infrastruttura locale
- Scalabilità da 1 a 1000 collaboratori
- Intercambiabilità dei dispositivi (mediante Microsoft login)
- Telelavoro molto efficiente (anche con periferiche personali)
- Banca dati professionale Microsoft SQL
- La configurazione può essere ridimensionata con estrema facilità
- Si può far capo a Microsoft Exchange online di Microsoft 365
- Nessun software particolare deve essere installato e manutenuto (solo Office 365)
- Costi strettamente lineari al numero di utilizzatori.

Contro:

- Formare il personale sul cloud e le nuove tecnologie
- Piattaforma PC limitata a Windows 10
- Assicurarsi presso Microsoft che i dati siano memorizzati in un paese UE (per i residenti in un paese UE) o in Svizzera (per i residenti in Svizzera).

Per approfondire:

Qui di seguito collegamenti utili per approfondire i concetti esposti:

Argomento	Link
Reti LAN	Local Area Network - Wikipedia
Server virtuali	Local Area Network - Wikipedia
Cloud computing	Cloud computing - Wikipedia
Disaster Recovery	Disaster recovery - Wikipedia
Microsoft 365	www.office.com
Sharepoint e OneDrive	What is SharePoint – Overview of features (microsoft.com)
Azure Serverless SQL	Serverless compute tier - Azure SQL Database | Microsoft Docs
OfficeNetPoint Easy-Edition	www.officenp.ch

Tabella 9 Documentazione online.

Considerazioni finali

Ricapitolo qui di seguito i vari TCO per piattaforma:

	Configurazione	Costi annuali/utente
	On-Premises	
1	Rete locale e NAS	1'360
2	Rete locale e file server	1'460
3	Rete locale e server RDS	1'610-1'835
	Cloud	
4	Private Cloud: Server RDS in hosting	1'310
5	Cloud Microsoft 365 e Azure SQL	1'167

Tabella 10 Tabella riassuntiva costi per configurazione.

Le soluzioni basate su LAN locali sono ancora molto presenti nelle PMI e microimprese.

È vero che fino a qualche anno fa non vi erano alternative in grado di competere a livello di costi con queste piccole architetture locali, ma presenza e prestazioni odierne di Internet e l'integrazione di tablet e telefoni cellulari rendono il cloud computing finanziariamente molto vantaggioso e più sicuro di qualsiasi rete locale.

In fondo basti pensare che l'architettura IT di una rete locale è tecnicamente più complessa da mantenere di un server perché comporta più macchine che devono condividere dati e servizi.

Solo a titolo di esempio: in caso di aggiornamento bisogna aggiornare tutte le macchine coinvolte e qualche volta anche rivedere le architetture. Il cambio di una stampante multifunzione generalmente impone l'aggiornamento dei driver su tutti i PC della rete locale ed il costo di tale aggiornamento rischia di costare di più dell'installazione della stampante stessa (per poi accorgersi che il PC dell'apprendista, ancora con Windows 7 non riesce più a stampare per la mancanza di driver per il vecchio sistema operativo).

Per quanto riguarda la sicurezza si deve anche tener presente che ogni PC rappresenta una macchina da proteggere, aggiornare e monitorare.

L'utilizzo di un server virtuale con Remote Desktop Service impone la manutenzione di una sola macchina, per tutti gli utenti, che si ritrovano così aggiornati allo stesso livello e la stessa versione software contemporaneamente. Sicurezza e controlloi accessi sono gestiti centralmente, permettendo anche il meno costoso e più rapido supporto remoto.

In base alle premesse poste in ingresso (5-10 utenti, attività che non necessita l'utilizzo di altri software di terze parti non compatibili con il cloud di Microsoft 365), la soluzione 5 (Cloud) risulta essere quella da preferire perché limita al massimo l'infrastruttura IT da implementare, spostando problematiche e gestione del perimetro aziendale fisico protetto (rete locale, backup, sicurezza) nel perimetro aziendale virtuale protetto gestito da Microsoft, con un costo di infrastruttura che si limita alla messa a disposizione della postazione di lavoro. Il passaggio ad una configurazione di tipo 4 è indolore.

Se, per contro, vi è l'esigenza presente o futura di utilizzare soluzioni software anche di terze parti che non supportano la tecnologia Microsoft (integrazione in OneDrive e SharePoint, Azure MS SQL) è preferibile la configurazione 4 (Private Cloud) che non esclude l'integrazione con SharePoint e OneDrive, ma permette un controllo maggiore sulle tecnologie di base.

Ciò comporta un'accresciuta gestione che necessita di prestazioni di professionisti IT, per lo meno in fase di configurazione, permettendone perlomeno una manutenzione remota.

In conclusione:

- Se vi è necessità di collaborazione o condivisione di informazioni all'interno del team (o con soggetti esterni) la memorizzazione in Cloud è il metodo più efficiente e con minore necessità di supporto IT. Una copia di sicurezza interna dei dati è sempre consigliata.

- Memorizzare i dati nel proprio perimetro aziendale può essere "più sicuro", a patto che ogni stazione di lavoro, firewall e NAS siano costantemente aggiornati e monitorati da risorse IT interne. Copie di sicurezza interne esterne devono essere eseguite e controllate regolarmente e un *Disaster Recovery Plan* testato è indispensabile.

- Considerare che qualsiasi tipo di archiviazione (cloud e locale) può, ad un certo momento evidenziare criticità. Sviluppare quindi una chiara politica (scritta) su cosa deve esse memorizzato e in quale tecnologia.

- Securizzare e salvaguardare i propri dati indipendentemente dalla tecnologia utilizzata. Per esempio backup in cloud e dati operativi in LAN, o viceversa, controllando regolarmente la loro buona esecuzione.

- Se non vi è costante monitoraggio da parte di personale IT la soluzione in cloud offre generalmente maggiori garanzie.

FMC / SwissASR - 26/11/2020