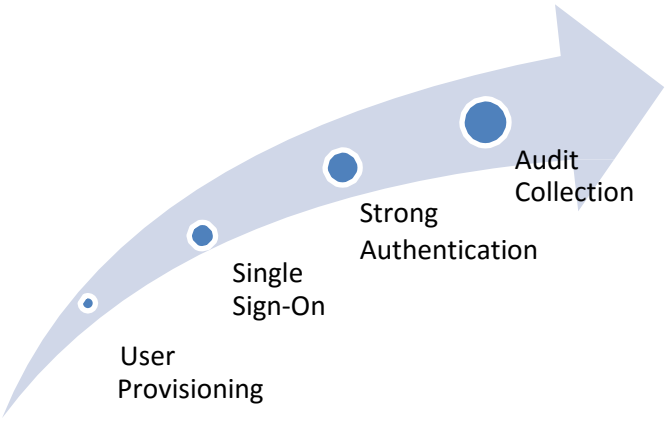
Dynamic Infrastructure

Marco Principi - IT Systems Architect
www.securdata.it - marco@securdata.it

In questo white paper vengono illustrati i punti fondamentali della progettazione e gestione di una moderna infrastruttura IT.

L'utente come punto cardine per l'erogazione dei servizi

Spesso l'attenzione della progettazione di un'infrastruttura IT si concentra sui servizi da erogare perdendo di vista chi deve usufruirne. Nelle grandi realtà aziendali dove sono presenti numerosi sistemi questo porta inevitabilmente ad una riduzione della funzionalità e delle performance degli stessi. Da questa considerazione nasce quindi l'esigenza di implementare un sistema centralizzato per consentire l'accesso alle applicazioni tramite una solida struttura di identity management che integri tecnologie, processi e politiche in grado di consentire la gestione delle identità digitali degli utenti proteggendo contestualmente i dati personali da usi non autorizzati. Le problematiche inerenti alle normali attività di gestione delle utenze possono essere facilmente eliminate riducendo i costi operativi di gestione delle identità digitali grazie alla creazione di un framework di automazione dei processi di identity management abilitando funzionalità self-service come la rigenerazione di una password dimenticata.



La possibilità di compiere auditing sulle attività di ogni identità digitale consente inoltre di ottemperare alle vigenti norme sulla gestione e la protezione dei dati delle numerose applicazioni presenti in azienda che fanno spesso riferimento a un proprio database di utenti per gestire l'autenticazione e l'autorizzazione all'accesso con le seguenti criticità:

- gli archivi utenti delle applicazioni non sono sincronizzati con l'archivio centrale;
- agli utenti è richiesto di memorizzare e gestire molteplici credenziali di accesso;
- molti amministratori devono gestire gli stessi utenti;
- spreco di risorse hardware e software;
- rischio di furto e scambio non autorizzato delle credenziali.

La complessità delle grandi strutture organizzative e la presenza di numerosi sistemi informativi indipendenti al loro interno richiedono quindi un'attenta progettazione dei servizi di directory. In questo contesto un sistema di provisioning ed autenticazione omogeneo si pone alla base dello sviluppo per offrire maggiore flessibilità a complessi processi di workflow uniformando l'infrastruttura di base e garantendo l'integrazione di piattaforme eterogenee.

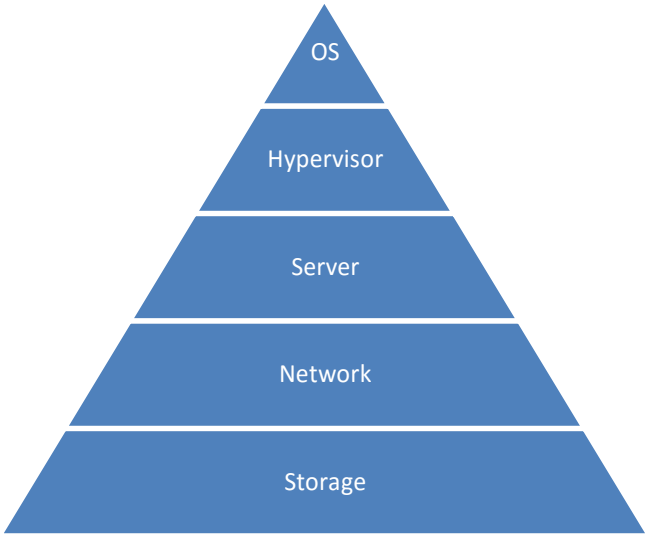
La creazione di una solida infrastruttura di identity management basata su Microsoft Active Directory Services, Active Directory Certificate Services apporta i seguenti vantaggi:

- gestione centralizzata delle utenze e delle relative policy di accesso;
- accesso centralizzato alle risorse con SSO (single sign-on)
- maggiore controllo dei processi di autenticazione ed autorizzazione con la possibilità di accesso tramite certificati digitali;
- maggiore flessibilità nei processi di autenticazione ed autorizzazione;
- riduzione del carico amministrativo per la gestione delle identità;
- disponibilità di informazioni aggiornate, affidabili e facilmente reperibili;
- economia di scala nell'implementazione e gestione di nuovi e vecchi servizi;
- maggiore aderenza ai requisiti di legge sulla gestione, conservazione e protezione dei dati
- maggiore controllo sui propri dati da parte degli utenti stessi;
- aumento della produttività e del grado di soddisfazione degli utenti;
- diminuzione del carico di lavoro dell'help desk.

Virtual Dynamic Infrastructure

La virtualizzazione consente di trasformare l'hardware di un server fisico in molteplici server virtuali comunemente denominati VM (virtual machines) in grado di eseguire applicazioni al pari di un host reale; questo avviene condividendo le risorse del singolo server fisico con lo scopo di ottenere un miglior utilizzo delle risorse hardware e di consentire il risparmio sia nei costi di capitale sia di energia consumata, aumentando la disponibilità delle risorse, semplificando la gestione dei server, incrementando il livello di sicurezza dell'infrastruttura ed automatizzando i processi legati al disaster recovery.

La virtualizzazione su vasta scala offre vantaggi significativi ma nasconde anche una serie di problematiche come la necessità di gestire la proliferazione delle virtual machines; è quindi opportuno pianificare in modo corretto e funzionale le varie componenti dell'infrastruttura per permetterne una gestione semplificata e quindi massimizzarne i vantaggi.



La virtualizzazione però non si ferma a quanto esposto fino ad ora, essa infatti può essere applicata anche ai sistemi di storage rivoluzionandone l'implementazione e la gestione con la possibilità di eseguire thin provisioning allocando dinamicamente lo spazio disco necessario al business e di spostare interi sistemi tra storage di architetture o vendor differenti copiando un semplice file VHD (virtual hard disk).

Affrontando il tema della virtualizzazione non si può fare a meno di dare evidenza alla virtualizzazione applicativa, essa permette di consolidare le applicazioni all'interno del data center rendendole disponibili agli utenti locali e remoti "in the cloud" attraverso i Remote Desktop Services utilizzando un semplice browser web di un thin client. Oltre allo scenario centralizzato è possibile implementare una soluzione di distribuzione delle applicazioni dove ogni singolo programma vive all'interno della sua "bolla applicativa" che può essere distribuita attraverso Active Directory o resa fruibile via Web ponendo come assioma la definizione di "software as a service".

Un ennesimo scenario implementabile attraverso la virtualizzazione è quello VDI (virtual desktop infrastructure). Un'infrastruttura VDI permette la sostituzione dei tradizionali PC con "desktop virtuali" che risiedono all'interno degli host di virtualizzazione; in molti scenari questa è la soluzione ideale per distribuire al miglior rapporto costo-prestazioni i servizi desktop. Questo tipo di approccio inoltre aiuta a ridurre il TCO (total cost of ownership) con un notevole allungamento del ciclo di vita dell'hardware. I benefici riscontrati dagli utenti sono invece quelli di una maggiore affidabilità grazie alla protezione dei dati, della capacità di disaster recovery e intervento tecnico immediato da parte dell'help desk riducendo notevolmente il carico di lavoro di quest'ultimo limitando i tempi di attesa per la risoluzione dei problemi. Un'infrastruttura VDI permette altresì di dotare gli utenti di "desktop virtuali multipli" mettendo a disposizione differenti sistemi operativi (Windows 8, Windows 10, 7, Linux Ubuntu ecc..)

Le principali motivazioni alla base dell'adozione di Microsoft Hyper-V come hypervisor per la virtualizzazione sono:

- costi di licenza contenuti o pari a zero;
- hypervisor nativo a 64 bit a microkernel;
- hypervisor appartenente alla medesima famiglia dei sistemi operativi guest e relativa integrazione;
- facilità nella migrazione delle VM tramite Live Migration e nella gestione dei backup senza interruzione dei servizi;
- centralizzazione dell'amministrazione dell' infrastruttura di virtualizzazione e relativo monitoring del funzionamento;
- performance paragonabili a quelle ottenibili con l'utilizzo in modalità nativa dell'hardware;
- supporto per i sistemi operativi Linux.

Per gestire al meglio l'ambiente di virtualizzazione è opportuno centralizzare il punto di controllo dei sistemi, questo è possibile grazie a System Center Virtual Machine Manager che insieme a System Center Operation Manager costituiscono un solido ed efficace strumento di controllo e monitoraggio dell'infrastruttura.

L'hardware come supporto alla virtualizzazione

La scelta della piattaforma hardware su cui sono basati i server che erogano i servizi è un passo fondamentale nell'implementazione di una data center virtualizzato.

Un'estrema importanza in una "virtual dynamic infrastructure" è riconosciuta allo storage su cui è basato il pool di virtualizzazione, in questo contesto è opportuno dotare tutti i nodi di servizio con HBA FC (host bus adapter fibre channel) ridondate ad alta velocità (8/4Gbit) per sfruttare il supporto multipath verso lo storage basato preferibilmente su dischi FC (fibre channel) o SAS (serial attached SCSI) che deve essere adeguato alle esigenze del business sia per spazio disco sia per l'affidabilità e le performance richieste dai servizi da erogare.

Per far fronte ad un taglio dei costi o nel caso in cui alcuni servizi non richiedano le massime performance dello storage, è possibile implementare il multipath grazie al protocollo iSCSI (internet small computer system interface) e dischi SATA (serial advanced technology attachment) utilizzando normali apparati gigabit ethernet su link in rame di classe 6A.

Nella ricerca della massima ottimizzazione delle risorse hardware è buona norma usufruire delle tecnologie di offloading, è possibile sfruttare il supporto di Hyper-V per VMDq (Virtual Machine Device Queues) utilizzando schede di rete che permettono di diminuire l'overhead sulle CPU consentendo alle macchine virtuali di accedere direttamente all'hardware e quindi aumentarne le performance, l'affidabilità e la sicurezza rispetto a un'implementazione standard.

Per garantire la migliore scalabilità dell'infrastruttura è opportuno utilizzare CPU con supporto per "Intel VT FlexMigration" o "AMD-V Extended Migration" che combinato con Live Migration e Cluster Shared Volumes permette di abilitare lo scenario di "high availability data center". Uno dei principali vantaggi della virtualizzazione è proprio la possibilità di eseguire la migrazione delle virtual machines in esecuzione da un server fisico a un altro senza interruzioni, queste funzionalità sono state progettate per estendere e facilitare le migrazioni tra server basati su processori attuali e futuri, anche se i nuovi sistemi possono includere un set d'istruzioni più evoluto. Con questa tecnologia Hyper-V può stabilire un set d'istruzioni coerente tra tutti i server del pool di virtualizzazione ottenendo un gruppo di risorse server più flessibile e unificato di cui è garantito il perfetto funzionamento anche attraverso generazioni hardware differenti.

Business Continuity

La definizione di un business continuity plan è di primaria importanza in ambienti dove è richiesta un'alta disponibilità, tramite esso è possibile aumentare lo SLA (service level agreement) per i servizi erogati, inoltre la definizione preventiva e l'intervento proattivo in seguito al verificarsi di eventi che possono minare la continuità dei servizi renderà minime le perdite causate da un'eventuale interruzione dell'attività. Gli scopi fondamentali del business continuity plan sono individuabili nei seguenti punti che andranno ad affiancarsi alle tradizionali attività di prevenzione in modo da:

- garantire il normale svolgimento dei processi assicurando l'erogazione dei servizi essenziali anche in caso di fault dei sistemi;
- limitare gli impatti causati da eventi prevedibili e non prevedibili;
- definire le modalità di attivazione e gestione dei casi di emergenza;
- definire i ruoli e responsabilità degli amministratori dei sistemi;
- definire un piano di disaster recovery;
- definire la gestione delle comunicazioni verso gli utenti in caso di eventi che possano compromettere la normale erogazione dei servizi.

Protezione degli asset

La protezione dagli attacchi informatici si ottiene agendo su più livelli definendo una politica di defense in depth che coinvolge il livello fisco e logico dei sistemi e della rete.

Le numerose minacce dei sistemi IT vanno dagli exploit dei servizi di rete lanciati da remoto all'uso di tecniche di social engineering per acquisire informazioni utili a compromettere i sistemi e sottrarre dati riservati o eseguire attacchi DoS (denial of service), fino agli utenti che possono causare disservizi inconsapevolmente a causa dell'uso non corretto dei servizi stessi.

D'altra parte se è vero che le configurazioni standard dei moderni sistemi operativi prevedono una sufficiente sicurezza per la loro normale operatività è anche corretto affermare che nella maggior parte dei casi è necessario definire controlli di sicurezza maggiormente aderenti alle policy aziendali che li rendano più sicuri rispetto allo specifico caso d'impiego garantendo un elevato grado di confidenzialità, integrità e disponibilità dei dati.

Con Windows Server 20012 R2 è possibile facilitare questo compito grazie ad una serie di tecnologie presenti e attivate al momento dell'installazione del sistema operativo come:

- User Account Control;
- Mandatory Integrity Control;
- Service Hardening;
- Windows Firewall With Advanced Security;
- Address Space Layout Randomization;
- Kernel Patch Protection;
- Security Configuration Wizard;
- Malicious Software Removal Tool;
- Windows Update.

Per contrastare i tentativi di violazione dei sistemi è opportuno agire in primo luogo sulla "sicurezza passiva" il cui obiettivo è di impedire l'accesso non autorizzato collocando i sistemi in locali protetti con l'utilizzo di porte blindate congiuntamente all'impiego di sistemi d'identificazione e videosorveglianza.

Attuate le politiche di protezione passiva è necessario concentrare l'attenzione su un adeguato processo che porti alla definizione delle policy che garantiscono la sicurezza attiva dei sistemi ponendo l'attenzione sul fatto che spesso l'adozione delle tecniche più sofisticate e complesse da gestire genera un falso senso di sicurezza.

Operazioni come la segmentazione fisica della rete deve essere quindi supporta da una protezione a livello logico adottando Firewall di primo e secondo livello, firewall host based (Windows Firewall With Advanced Security) e filtri IPSec (internet protocol security) basati su certificati digitali che permettano la mutua autenticazione dei soggetti (utenti e computer) che operano sulla rete; a questo vanno aggiunti sistemi di traffic inspection per verificare il contenuto del traffico che potrebbe nascondere al suo interno possibili minacce.

L'adozione di software antivirus e antispam sia sui gateway (es. SMTP e VPN servers) che sugli endpoint (con Forefront Client Security) insieme al tracciamento delle operazioni effettuate dall'utente attraverso il processo di monitoraggio delle attività e collection degli audit con System Center Audit Collection Services completano il ciclo di attuazione di una corretta politica di sicurezza attiva.

Un successivo grado di sicurezza è raggiungibile attraverso la crittografia delle comunicazioni di rete es. utilizzando SSL (secure sockets layer) e la crittografia dei dati presenti nei dispositivi di memorizzazione hard disk locali, SAN (storage area network) e NAS (network attached storage) utilizzando le funzionalità di EFS (encrypting file system) o BitLocker Drive Encryption in grado di crittografare interi volumi garantendo un elevato livello di protezione dei dati.

Gestione degli audit

La gestione dei log è un aspetto fondamentale della sicurezza di un sistema IT, una corretta analisi dei log può aiutare sia nel rilevamento di un attacco che nell'individuazione di problemi intrinseci ai sistemi. In caso di violazione della sicurezza i log possono agevolare a scoprire l'origine dell'attacco, in modo da poter identificare l'intruso. Vista la loro importanza, è auspicabile attuare una politica di sicurezza che regoli il ciclo di vita dei log.

A sostegno di quanto esposto il Garante per la protezione dei dati personali ha deciso di disciplinare la figura professionale dell'amministratore di sistema ed ha prescritto l'adozione di specifiche misure tecniche ed organizzative che agevolino la verifica sulla sua attività da parte di chi ha la titolarità all'accesso delle banche dati e dei sistemi informatici attraverso la registrazione degli accessi.

Public Key Infrastructure

Il termine Crittografia deriva dal greco kryptos (nascosto) e dal verbo gráfo (scrivere), la crittografia nasce infatti per garantire la segretezza dei messaggi scambiati. I requisiti ai quali la crittografia deve rispondere sono la confidenzialità, integrità, autenticazione e il non ripudio.

Una PKI (public key infrastructure) è un'infrastruttura di sicurezza costituita da protocolli e servizi, aderenti a standard internazionali, per il supporto di applicazioni basate su crittografia a chiave pubblica. L'emissione dei certificati è effettuata attraverso Microsoft Active Directory Certificate Services con cui è possibile implementare sia la Firma digitale con smart card per documenti e messaggi di posta elettronica che la multifactor strong authentication a sistemi e applicazioni aumentando notevolmente il grado di sicurezza.

Green IT, possibile e facilmente realizzabile

L'introduzione in azienda della virtualizzazione ha contribuito ad abbattere notevolmente i costi inerenti all'energia elettrica utilizzata per l'alimentazione dei server e degli impianti di climatizzazione dei data center con un netto taglio della CO_2 immessa nell'atmosfera. Oggi è possibile ospitare fino a 64 virtual machines in HA (high availability) con ottime prestazioni all'interno di un unico server fisico con un consumo di elettricità nettamente inferiore a quello che necessario per una moltitudine di server fisici presenti all'interno de data center.

Ad ulteriore supporto nell'attuazione di una politica di risparmio energetico l'adozione di Windows Server 2008 R2 rispetto alle precedenti versioni permette di tagliare ulteriormente i costi concernenti all'energia con l'utilizzo di features come CPU Core Parking che permette il consolidamento dei processi su un minor numero di core delle CPU con la sospensione dei core inattivi ed advanced ACPI "P-states" che permette di limitare l'energia assorbita dalle CPU nei momenti di basso carico di lavoro.

Unified Communication

Oggi per la maggior parte delle aziende la posta elettronica rappresenta uno strumento fondamentale per ottenere risultati ottimali. Il crescente utilizzo della posta elettronica ha portato a un notevole aumento del numero di messaggi scambiati e della varietà di operazioni eseguite, è quindi necessario un accesso efficiente e avanzato a messaggi, calendari, allegati, contatti indipendentemente dalla loro posizione o dal dispositivo utilizzato.

Una soluzione di comunicazione integrata è quindi un valido investimento in grado di aumentare la produttività e ridurre notevolmente i costi aziendali.

Il primo e più evidente risparmio nell'utilizzo di Microsoft Skype for Business si ha grazie al servizio di conferencing con il quale è possibile organizzare riunioni virtuali condividendo voce, video, documenti e collaborando da remoto in tempo reale; questo permette di evitare gli spostamenti con notevole un risparmio sui costi delle trasferte ed annullare i tempi di spostamento stessi.

Il risparmio sui costi di comunicazione è dato dalla piattaforma VoIP (voice over internet protocol) che permette di utilizzare la rete dati per compiere le normali chiamate, conferenze telefoniche e video conferenze; inoltre un'unica rete da amministrare e una sola piattaforma per gestire mail, voce, video e tutti gli strumenti di comunicazione in tempo reale o in modalità asincrona portano ad un marcato risparmio anche sui costi di gestione.

Gli utenti sono agevolati nell'utilizzo delle diverse tecnologie da un'interfaccia semplice e intuitiva, la mailbox diventa il punto centrale delle comunicazioni asincrone, dove è possibile ricevere oltre alle e-mail le chiamate perse ed i messaggi vocali. Tutte le informazioni sono sempre sotto controllo e accessibili da ogni luogo sia esso un Internet point, il PC collegato alla rete domestica, uno smartphone o un normale telefono che permette di chiamare la mailbox e fare leggere le e-mail.

Microsoft Exchange Server gestisce tutte le comunicazioni asincrone e invia alle caselle di posta in arrivo degli utenti di Microsoft Office Outlook comunicazioni di messaggistica unificata (e-mail, posta vocale, fax e calendaring), tra le sue funzionalità troviamo:

- protezione antispamming e antivirus con filtri e scansione multi-engine;
- riservatezza della messaggistica grazie alle funzionalità di crittografia dei messaggi;
- funzionalità avanzate di archiviazione;
- alta disponibilità dei servizi attraverso replica in locale ed in cluster;
- funzionalità di Unified Messaging che consentono di ricevere nella propria cassetta postale diversi tipi di comunicazioni oltre ai messaggi e-mail, quali fax e messaggi di posta vocale;
- collaborazione e produttività tramite calendari condivisi, l'invio di messaggi fuori sede, la prenotazione delle risorse e la pianificazione delle riunioni;
- accesso web avanzato da qualsiasi computer connesso a Internet attraverso Outlook Web App;
- messaggistica mobile tramite Exchange ActiveSync;
- basso impatto delle operazioni di scrittura sullo storage rispetto alle precedenti versioni con conseguente incremento delle performance e diminuzione delle risorse hardware richieste.

Copyright

Le opinioni espresse in questo documento sono esclusivamente opinioni personali e non rappresentano in ogni caso quelle delle aziende citate nel documento.

Per maggiori informazioni visitare il sito: http://www.securdata.it o inviare un messaggio a: marco@securdata.it