Guida alla virtualizzazione con VMware vSphere 5.1

Alessio Carta *www.netsetup.it*

Manuale gratuito non ufficiale e non approvato VMware

Prima edizione giugno 2013

Guida alla virtualizzazione con VMware vSphere 5.1

Prima edizione giugno 2013

Autore: Alessio Carta

Autorizzazioni

Questa guida non rappresenta un testo ufficiale o approvato VMware. L'autore ha avuto il permesso di redigerla purché priva di logo VMware e purché priva di qualsiasi scopo commerciale.

Declino di responsabilità

Le informazioni contenute in questa guida sono state verificate con la massima cura possibile. Tuttavia non è possibile garantire l'assenza di errori e imprecisioni. Nessuna responsabilità derivante dal loro utilizzo potrà venire imputata all'autore.

Supporto e segnalazioni

Per riscontri e segnalazioni, utilizzare il modulo commenti presente nella pagina di download della guida, all'indirizzo http://www.netsetup.it/vmware/guida-italiana-vsphere-51

Le richieste di aiuto inviate via mail, o tramite il modulo contatti dell'autore, non saranno prese in considerazione.

A Carla e Anna

Sommario

Premessa

Questo libro è stato inizialmente pensato come semplice raccolta di appunti, scritti nel periodo di studio per la certificazione VMware Certified Professional 5. Ho poi deciso di pubblicare questi appunti sotto forma di articoli sul sito http://www.netsetup.it, ma il materiale è diventato in poco tempo così corposo da convincermi a realizzare una vera e propria guida italiana alla virtualizzazione con VMware vSphere, basata sulla versione 5.1, ultima disponibile nel momento in cui scrivo. Ho esaudito in questo modo due desideri: quello di pubblicare un mio libro, e quello di realizzare il primo manuale in lingua italiana su VMware vSphere. Certamente non può essere considerata una guida completa, piuttosto un aiuto per chiunque voglia introdursi nel mondo della virtualizzazione enterprise. Per tutti, si tenga presente che la documentazione tecnica di riferimento, ben più dettagliata e articolata rispetto a questo manuale, è quella disponibile tramite i canali ufficiali, in particolare tramite il "VMware vSphere 5.1 Documentation Center" raggiungibile all'indirizzo http://pubs.vmware.com/vsphere-51/index.jsp

Chi sono

Mi chiamo Alessio Carta, orgogliosamente nato e cresciuto in terra sarda, e lavoro nel campo dell'informatica e delle telecomunicazioni da una decina d'anni. La mia formazione comprende un titolo di ingegnere e diverse specializzazioni: Istruzione e Formazione Tecnica Superiore (IFTS) quale "Esperto in progettazione di reti telematiche", certificazioni CISCO CCNA, CISCO CCNA Security, Microsoft Certified Professional su Windows Server, VMware Certified Professional 5 Data Center Virtualization.

Netsetup

NETsetup.it è il mio sito, nato qualche anno fa e realizzato con l'obiettivo di condividere sul web guide e articoli legati al mondo delle reti e dei sistemi informatici. Porto avanti il sito nel tempo libero (sempre meno!).

Se volete partecipare al progetto Netsetup con vostri articoli o semplicemente proporre suggerimenti, utilizzate il modulo contatti presente nel sito. Per richieste riguardanti gli argomenti trattati nel sito, utilizzate il modulo commenti posto alla fine di ogni articolo. Vi prego di non utilizzare la pagina contatti per richieste di assistenza tecnica.

Sardacom srl

È l'azienda presso cui lavoro quotidianamente come responsabile sistemi. Opera in tutto il territorio nazionale confrontandosi costantemente sulle moderne tematiche dell'ICT. Il carattere di Sardacom è quello dell'integrazione di sistemi in specialità chiave della nostra vita e del nostro modo di comunicare: Telecomunicazioni, Radiocomunicazioni, Informatica, Sicurezza. Per maggiori informazioni, visitate il sito http://www.sardacom.it. Per richieste di assistenza tecnica, preventivi, progetti, ecc., utlizzate il modulo contatti – settore informatico – presente nel sito di Sardacom.

Capitolo 1
Introduzione a VMware vSphere

1.1 Concetti base sulla virtualizzazione

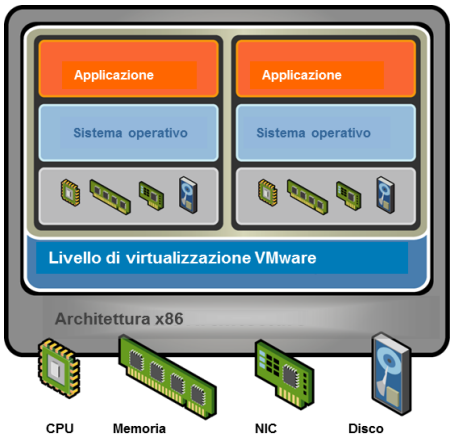
Nel mondo informatico tradizionale, a un computer corrisponde un sistema operativo installato su di esso, con rapporto 1:1 tra hardware e software di sistema. Questo binomio comporta inevitabilmente uno spreco di risorse hardware, dovuto al fatto che i sistemi hanno lunghi tempi d'inattività o di ridotta occupazione di risorse; si stima che, in queste condizioni, i computer fisici siano impegnati mediamente al 5-10% delle loro capacità. Gestire un sistema operativo associato ad uno specifico hardware comporta inoltre diversi problemi, in particolare nel momento in cui il sistema deve essere aggiornato o sostituito. Lo spostamento di un sistema operativo su hardware diverso è sempre stata un'operazione problematica, perché ogni sistema è strettamente legato all'hardware su cui è stato installato.

La tecnologia della virtualizzazione permette invece di ospitare più sistemi operativi all'interno di una stessa macchina fisica, razionalizzando e ottimizzando l'hardware grazie a meccanismi di distribuzione delle risorse disponibili; non si tratta di multi-boot, ma dell'esecuzione contemporanea di sistemi eterogenei che dialogano direttamente con l'hardware sottostante. La virtualizzazione non deve essere confusa con l'emulazione: in quest'ultimo caso tutte le operazioni sono eseguite da un software che gira all'interno di un emulatore (altro software), che fa da ponte tra due sistemi diversi. La virtualizzazione non prevede emulazione, ma rende possibile astrarre gli elementi hardware (hard disk, ram, CPU, interfacce di rete) e renderli disponibili sotto forma di risorse virtuali. L'insieme delle risorse virtuali prende il nome di **macchina virtuale**, o **Virtual Machine** (**VM**) e su ogni macchina virtuale può essere installato un sistema operativo con relative applicazioni. In questo modo più macchine virtuali possono girare contemporaneamente su una stessa macchina fisica, di cui condividono le risorse pur rimanendo ognuna isolata dalle altre. Le eventuali contese di risorse sono gestite dal software di virtualizzazione.

Differenze tra un sistema fisico tradizionale e un sistema virtuale

Architettura tradizionale

Architettura virtuale



L'approccio alla virtualizzazione di VMware prevede l'inserimento di uno strato software intermedio, detto **hypervisor**, tra l'hardware della macchina fisica e le macchine virtuali. Vedremo più avanti che l'hypervisor di VMware si chiama **VMware ESXi**. In generale, le macchine fisiche su cui è installato l'hypervisor sono chiamate **host**, mentre ogni macchina virtuale ospitata è definita **guest**. L'hypervisor permette la creazione delle macchine virtuali e la distribuzione delle risorse in

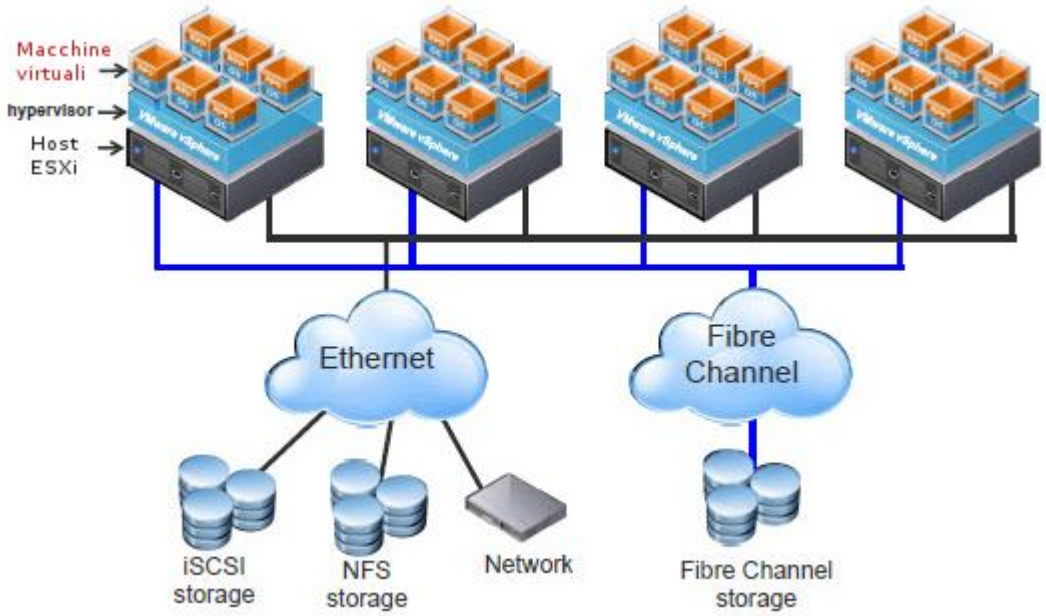
maniera dinamica e trasparente, rendendole disponibili sotto forma di hardware virtuale. Pertanto ogni macchina virtuale avrà a disposizione una propria CPU, la propria RAM, il proprio spazio disco: tutti elementi astratti e virtualizzati dalle risorse fisiche dell'host.

L'uso delle macchine virtuali comporta innumerevoli vantaggi, il principale dei quali è rappresentato dalla riduzione dei costi dell'infrastruttura fisica. Con la possibilità di avere più sistemi su una singola macchina fisica, si riduce il numero di server e di hardware correlato. Di conseguenza si ha una riduzione delle esigenze di spazio, di alimentazione e raffreddamento, con risparmio sui costi. Vi sono poi tutti i vantaggi legati al risparmio del tempo e alla semplificazione delle operazioni di gestione e manutenzione. Ad esempio, ogni VM può essere spostata da un host a un altro senza problemi di compatibilità, perché l'hardware visto dalla VM sarà sempre lo stesso. Gli upgrade di risorse si riducono a semplici operazioni effettuate da una console grafica. Le operazioni di backup e ripristino sono molto semplici, poiché le macchine virtuali, dal punto di vista dell'hypervisor, sono semplici file memorizzati sullo storage.

1.2 Le infrastrutture virtuali

I concetti di virtualizzazione introdotti possono essere applicati su larga scala, abbracciando gli ambienti complessi tipici dei data center. La virtualizzazione consente di consolidare piccole e grandi infrastrutture, con uno sfruttamento ottimale delle risorse hardware, permettendo di unire in pool le risorse comuni e abbandonando il modello tradizionale di corrispondenza univoca tra software di sistema e server (rapporto 1:1 tra sistema operativo e server). La flessibilità operativa cresce esponenzialmente, grazie a una nuova modalità di gestione dell'infrastruttura IT che consente agli amministratori di dedicare meno tempo ad attività ripetitive, come il provisioning, la configurazione, il monitoraggio e la manutenzione.

Un'infrastruttura virtuale è pertanto un sistema che ha come obiettivo primario quello di "governare" tutto il data center, virtualizzarlo e renderlo gestibile con una sola, semplice, soluzione. L'immagine sottostante rende meglio il concetto.



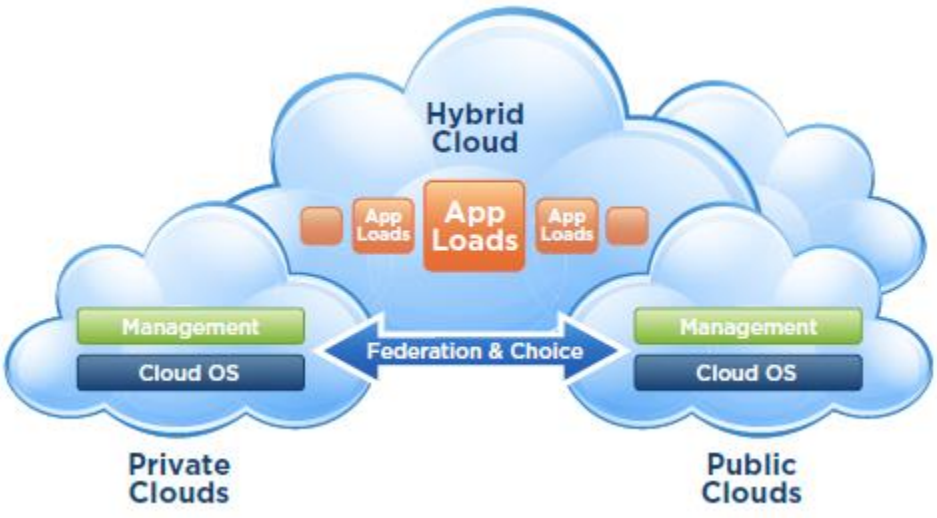
Un'infrastruttura virtuale prevede la completa virtualizzazione di server, storage e risorse di rete. Ad esempio, la virtualizzazione dello storage permette di sfruttare uno spazio di memorizzazione virtualmente unico, ma fisicamente costituito da storage iSCSI, NFS, Fibre Channel, da dischi locali presenti nei singoli server o da una combinazione di questi elementi. Allo stesso modo, la

virtualizzazione del networking consente di creare reti complesse tra VM residenti in uno o più host. È possibile configurare ogni VM con una o più schede di rete virtuali, ciascuna con il proprio indirizzo IP e MAC, ottenendo macchine virtuali indistinguibili da quelle fisiche. Si può anche simulare una rete all'interno di un host collegando le macchine virtuali tramite switch virtuali, e si possono utilizzare le VLAN per sovrapporre una rete locale logica alle LAN fisiche. È possibile infine modificare le configurazioni di rete senza dover apportare modifiche ai cablaggi ed alle configurazioni degli switch fisici.

1.3 Il cloud computing

Nei diagrammi di rete, Internet è spesso rappresentata come una nuvola (cloud in inglese). L'architettura del cloud computing prevede più server, su uno o più data center, connessi su reti eterogenee: in sostanza, si tratta di un modo per nascondere le caratteristiche fisiche di un sistema nelle sue interazioni con altre risorse. Dalle infrastrutture fisiche al cloud computing il passo è breve: gli utilizzatori finali connessi a un sistema cloud sfrutteranno risorse senza nulla sapere delle complesse architetture sottostanti.

Nella visione di VMware, esistono principalmente due tipi di infrastrutture cloud: quelle pubbliche e quelle private. Un **cloud privato** è un'infrastruttura a disposizione di una sola organizzazione. Un **cloud pubblico** è un'infrastruttura di proprietà di un'organizzazione che vende servizi cloud a utenti e aziende. Esistono poi le infrastrutture cloud ibride, dette **hybrid cloud**, dove più cloud pubblici e privati compongono un'unica entità ibrida.



L'errata percezione comune è che se un'azienda desidera sfruttare le tecnologie del cloud computing, debba per forza sfruttare servizi offerti tramite Internet. In verità qualsiasi azienda può beneficiare del cloud computing all'interno del proprio data center, con la costruzione di un cloud privato, tramite VMware vSphere, o un cloud ibrido, con cui poter rivendere servizi di tipo cloud, tramite VMware vCloud Director.

VMware vCloud Director è un prodotto software che consente di creare cloud multi-livello mediante il pooling delle risorse virtuali e la relativa esposizione agli utenti tramite portali basati su Web. vCloud Director utilizza le risorse vSphere per fornire CPU e memoria per l'esecuzione delle macchine virtuali, oltre allo spazio di storage per i file delle macchine virtuali e per i file utilizzati con operazioni interne alle macchine virtuali.

I cloud pubblici realizzati con tecnologia VMware offrono tre principali classi di servizio.

- **Basic** vDC: servizio non riservato di tipo "pay per use", indicato per la realizzazione di veloci progetti pilota, per il test di software, ovvero per operazioni che non richiedono risorse riservate ed elevate prestazioni.
- **Committed** vDC: fornisce risorse riservate con la possibilità di eccedere oltre i livelli concordati nel caso in cui fossero disponibili risorse aggiuntive. Offre prestazioni predefinite che permettono il corretto dimensionamento di un progetto.
- **Dedicated** vDC: fornisce risorse riservate tramite hardware dedicato. Il servizio è conosciuto anche con il nome di "virtual private cloud". Offre prestazioni predefinite, si utilizza quando è richiesta una separazione fisica delle risorse dedicate.

Un cloud privato basato su tecnologia VMware si presta a tre differenti categorie di lavoro.

- **Transient** – si definisce "transient" (transitorio) un lavoro che si ripete con poca frequenza, ovvero un'applicazione usata con poca frequenza, che dura poco oppure è utilizzata per un obiettivo che si presenta una sola volta.
- **Highly Elastic** - si definisce "highly elastic" (altamente elastico) un lavoro o un'applicazione che può incrementare o ridurre il consumo di risorse in maniera dinamica.
- **Infrastructure** - si definisce di infrastruttura un lavoro o un'applicazione che tendono ad essere eseguiti con un consumo di risorse lineare nel tempo, quindi prevedibile.

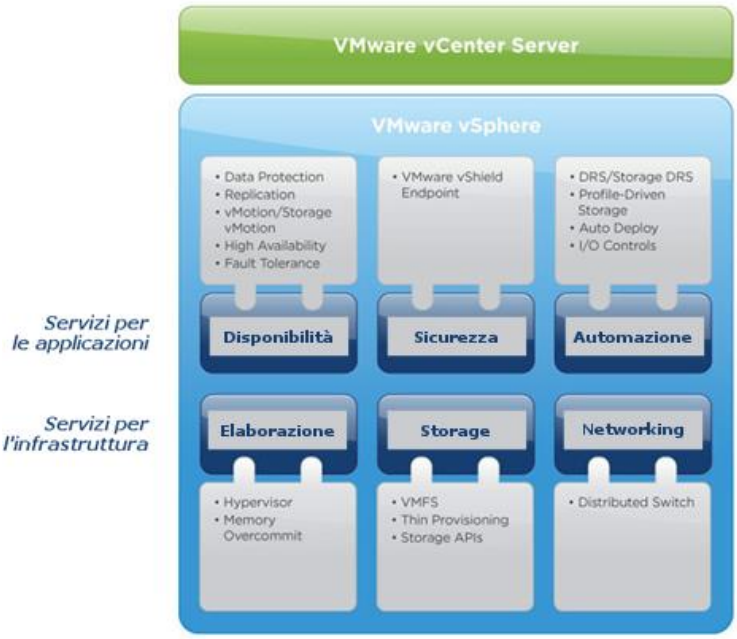
1.4 Panoramica su VMware vSphere

VMware vSphere è una "suite" di software, funzionalità e servizi pensati per il cloud computing.

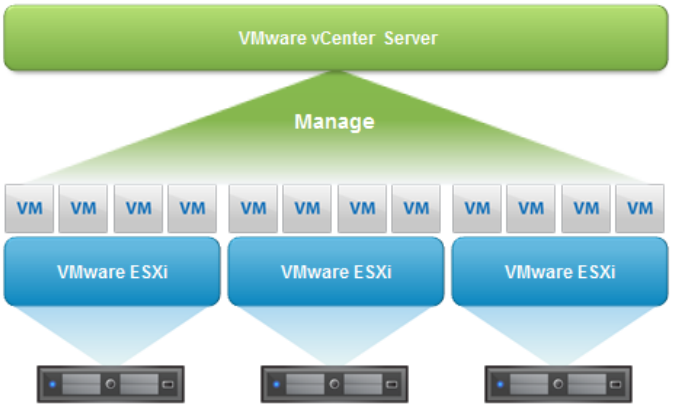
Primo sistema operativo cloud del settore, VMware vSphere sfrutta la potenza della virtualizzazione per trasformare i data center in infrastrutture di cloud computing semplificate, e consente alle organizzazioni IT di erogare servizi di nuova generazione, affidabili e flessibili, che fanno uso delle risorse interne ed esterne e garantiscono massima sicurezza e rischi contenuti. VMware vSphere riduce la complessità di gestione dell'hardware mediante la virtualizzazione totale di server, storage e hardware di rete, e fornisce funzioni per l'alta disponibilità semplici e convenienti per fronteggiare tempi di inattività non pianificati, ad esempio per guasti server.

VMware vSphere è un sistema operativo di tipo cloud equipaggiato con i seguenti gruppi di servizi.

- **Servizi per le applicazioni**, ossia l'insieme degli elementi che forniscono i controlli integrati sui livelli di servizio di tutte le applicazioni eseguite su VMware vSphere, a prescindere dal tipo di applicazione o sistema operativo adoperato.
- **Servizi per l'infrastruttura**, ossia l'insieme degli elementi che consentono la virtualizzazione completa di server, storage e risorse di rete. Parliamo quindi di virtualizzazione e raggruppamento delle risorse hardware.



Il "centro di comando" di VMware vSphere è il **VMware vCenter Server**, che consente l'amministrazione dei servizi applicativi e di infrastruttura, nonché l'automazione delle attività operative quotidiane, assicurando massima visibilità su ogni aspetto dell'ambiente virtuale.



1.4.1 Funzionalità e principali servizi di VMware vSphere

Elaborazione

- **vSphere ESXi** - è l'hypervisor installato direttamente sull'hardware di ogni server che fa parte dell'infrastruttura di virtualizzazione. Consente di partizionare un server fisico in più macchine virtuali, eseguibili simultaneamente. ESXi sostituisce la precedente versione dell'hypervisor di VMware, chiamata ESX, un sistema operativo vero e proprio (basato su Linux Red Hat) che occupava memoria, spazio, risorse e doveva essere aggiornato di frequente, come qualsiasi distribuzione Linux. Il nuovo ESXi è privo della parte relativa al sistema operativo Linux Red Hat (la cosiddetta Service Console), e tutti gli agenti VMware sono eseguiti direttamente nel kernel (chiamato VMkernel). Il risultato è un sistema operativo leggerissimo. I servizi dell'infrastruttura virtuale sono forniti nativamente attraverso i moduli inclusi nel VMkernel. In generale, i server fisici su cui è installato VMware ESXi sono

chiamati **host**, mentre le macchine virtuali (VM, Virtual Machine) sono etichettate come **guest**.

Storage

- **vSphere VMFS (Virtual Machine File System)** - è un file system di tipo cluster, che rende possibile a più host ESXi l'accesso simultaneo ai dispositivi di storage condivisi (Fibre Channel, iSCSI, ecc.) ed alle macchine virtuali.

- **vSphere vStorage Thin Provisioning** - consente l'allocazione dinamica dei dati nello storage. Il thin provisioning permette la creazione di VM con dischi dinamici: in sostanza, nel momento in cui si crea un disco virtuale per una VM, lo spazio occupato sullo storage fisico sarà quello effettivamente occupato dai dati della VM, indipendentemente dalla dimensione assegnata al disco virtuale.

- **vSphere Storage DRS** - migliora la gestione e consente un uso più efficiente delle risorse di storage tramite raggruppamento, posizionamento e bilanciamento.

- **Profile-Driven Storage** - identifica lo storage appropriato per la macchina virtuale in base al livello di servizio. Il risultato è un approccio semplificato alla selezione e distribuzione dello storage più idoneo.

- **vSphere Storage I/O Control** - migliora la gestione e l'applicazione degli accordi sui livelli di servizio (SLA) tramite l'estensione dei limiti e delle condivisioni nei datastore NFS.

- **vSphere Storage API** - è una raccolta di interfacce di programmazione (API) che consente a VMware vCenter Server di rilevare le funzionalità di LUN/datastore degli array di storage, facilitando la selezione del disco appropriato per le macchine virtuali o per la creazione dei cluster di datastore. Utilizzando la nuova interfaccia vSphere API for Storage Awareness (VASA), interagisce con gli array nell'utilizzo delle funzionalità DRS e Profile-Driven Storage di vSphere.

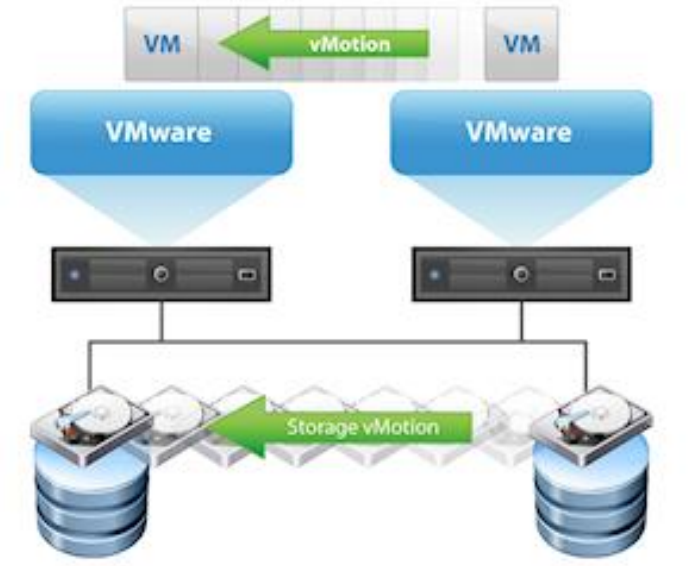
Networking

- **vSphere Standard Switch e vSphere Distributed Switch** – gli switch virtuali standard e distribuiti sono le entità del networking virtuale di VMware vSphere. Il networking virtuale, o virtual networking, consente alle macchine virtuali di comunicare tra loro con gli stessi protocolli utilizzati negli switch fisici, senza la necessità di hardware di rete aggiuntivo. In generale, gli switch virtuali possono essere interfacciati alla rete fisica semplicemente associandoli a una o più interfacce fisiche disponibili negli host. Gli switch virtuali distribuiti permettono di gestire il virtual networking tra più host all'interno di uno stesso data center, consentendo di operare come se si avesse un singolo switch centralizzato.

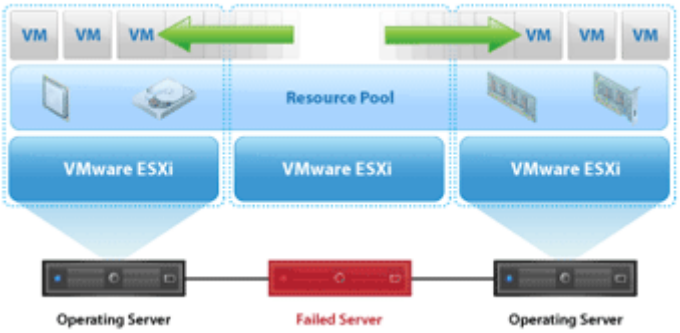
Disponibilità

- **vSphere vMotion e Storage vMotion** – entrambi i servizi consentono di migrare macchine virtuali da un host a un altro in tempo reale, eliminando il bisogno di pianificare tempi di disservizio per la manutenzione dei server. La migrazione di una VM può essere eseguita senza causare interruzioni per gli utenti o perdite di dati. Prima di vSphere 5.1, il vMotion prevedeva lo spostamento di una macchina virtuale da un host ad un altro, mantenendo i file su uno stesso datastore condiviso, mentre lo Storage vMotion era utilizzato per spostare una macchina virtuale da uno storage ad un altro. Con vSphere 5.1 la migrazione non richiede uno storage condiviso: è possibile cambiare storage e host

simultaneamente, ossia è permessa una combinazione tra vMotion e Storage vMotion con un unico passaggio.



- **vSphere High Availability (HA)** - consente di riavviare in pochi minuti, in modo automatico ed economico, macchine virtuali e applicazioni bloccate da guasti hardware o software. In caso di blocco di un host ESXi, esegue un riavvio automatico delle macchine virtuali su un altro host. In caso di blocchi sul sistema operativo di una VM, riavvia la macchina virtuale sullo stesso host fisico, fornendo quindi alta disponibilità per le applicazioni in esecuzione sulla macchina virtuale.



VMware HA controlla costantemente tutti gli host inseriti all'interno di un pool di risorse (resource pool) e rileva eventuali blocchi sia sugli host, sia sulle macchine virtuali ospitate. VMware HA richiede uno storage condiviso, come sistemi Fibre Channel e SAN iSCSI, con file system VMFS; il file system cluster VMFS di VMware consente infatti a più host ESXi di accedere alla stessa macchina virtuale. VMware HA è una soluzione valida per ambienti che possono sopportare brevi interruzioni di servizio e potenziale perdita di transazioni (si pensi a grossi database) nel momento del blocco; il downtime è minimizzato ma non annullato. Per annullare completamente il downtime e la potenziale perdita di dati bisogna utilizzare il servizio Fault Tolerance.

- **vSphere Fault Tolerance** - Assicura la disponibilità continua di tutte le applicazioni, senza causare downtime o perdite di dati in caso di guasti hardware. In base a questa definizione, si potrebbe pensare che la funzione Fault Tolerance sia simile al servizio HA; in effetti è così, ma con alcune differenze sostanziali. Abilitando la Fault Tolerance per una

VM, vSphere duplicherà la VM su un altro host, tenendo accese entrambe le VM. La seconda VM è una copia funzionante della prima, e non è chiamata in causa durante la normale operatività. Rispetto all'HA vi è quindi una doppia occupazione di risorse (cpu, memoria, spazio). In caso di crash dell'host che ospita una delle due VM, i servizi continuano a funzionare regolarmente poiché la VM corrispondente è già accesa e funzionante su un altro host. VMware HA è una soluzione valida per ambienti che possono sopportare brevi interruzioni di servizio, mentre Fault Tolerance è indirizzato a quelle applicazioni "mission-critical" che non possono tollerare alcun tipo di interruzione o perdita di dati. Importante rilevare che il servizio Fault Tolerance dovrà essere abilitato all'interno di un cluster VMware HA, pertanto per quelle macchine protette da Fault Tolerance rimangono attivi anche i servizi offerti da VMware HA.

- **vSphere Data Protection** - fornisce attività di backup e ripristino semplici, economiche e senza la necessità di installare agenti software nelle macchine virtuali. Il backup delle VM è gestibile direttamente tramite il vCenter. Data Protection sostituisce il precedente Data Recovery; come il predecessore, utilizza delle appliance per la gestione dei backup. Esse sono preconfigurate con tagli di capacità da 0.5 Tb / 1 Tb / 2 Tb e si trovano pronte in formato ovf. Il nuovo sistema si basa sulla tecnologia Avamar di EMC e supporta la deduplica.

- **vSphere Replication** – permette il disaster recovery su un sito remoto, grazie alla possibilità di replicare macchine virtuali accese da un host ad un altro, attraverso la rete, senza la necessità di avere storage con funzioni di replica nativa. Anche con le licenze "entry level" (vSphere Essentials Plus) è disponibile la replica, che consente il recovery a livello di VM su un sito secondario.

Sicurezza

- **vShield Endpoint** - Elimina il footprint degli anti-virus dalle macchine virtuali e migliora le prestazioni di scansione trasferendo le funzioni AV a una macchina virtuale con sicurezza rinforzata.

Automazione

- **Host Profiles** - crea un profilo che può essere utilizzato successivamente per la configurazione di più host vSphere.

- **vSphere Auto Deploy** - distribuisce e installa patch per gli host ESXi. Consente di implementare più host in pochi minuti e di aggiornarli in modo più efficace rispetto al passato. Attraverso la rete, ed utilizzando gli standard PXE/gPXE, gli host sono in grado di contattare il server di distribuzione. L'Auto Deploy carica un'immagine di vSphere ESXi e si coordina con il vCenter Server per configurare l'host (tramite Host Profiles). Auto Deploy elimina la necessità di un dispositivo di avvio dedicato, permettendo l'implementazione rapida di molti host, e inoltre semplifica la gestione degli stessi eliminando la necessità di mantenere un'immagine di avvio distinta per ogni host.

- **Update Manager** - riduce il tempo richiesto per le correzioni di routine automatizzando il monitoraggio, il patching e l'aggiornamento degli host vSphere, delle applicazioni e dei sistemi operativi.

- **vSphere Distributed Resource Scheduler (DRS)** - bilancia in modo dinamico i carichi di lavoro sugli host, per fornire le giuste risorse alle macchine virtuali e alle applicazioni che girano su di esse. DRS può gestire in automatico il bilanciamento spostando le VM su host meno carichi. È inoltre possibile programmare lo spegnimento di alcuni host e lo

spostamento automatico delle VM su altri host. DRS si basa sulla tecnologia vMotion per eseguire le migrazioni.

- **vSphere Distributed Power Management (DPM)** - fa parte di vSphere DRS e automatizza l'efficienza energetica complessiva dei cluster VMware DRS, ottimizzando costantemente il consumo energetico dei singoli server per ogni cluster.

- **Funzioni Hot Add, Hot Plug, Hot Extend** - VMware vSphere permette di modificare le caratteristiche delle VM "a caldo", cioè senza spegnere le macchine: aggiunta di RAM, CPU e hardware vari, dischi compresi. Da rilevare che questa caratteristica deve essere supportata dal sistema operativo presente in ogni VM; inoltre non è possibile sottrarre risorse a una VM accesa. In sostanza si può aggiungere ma non togliere (per farlo occorre spegnere la VM). Ancora, si possono modificare le dimensioni del disco di una VM accesa, aumentare la dimensione di un datastore mantenendo le VM accese, connettere o disconnettere dispositivi di rete senza causare discontinuità o downtime.

1.5 Edizioni di VMware vSphere 5.1

VMware vSphere 5.1 è disponibile in diverse edizioni.

- Standard
- Standard con Operations Management
- Enterprise
- Enterprise Plus

Per ogni implementazione di VMware vSphere è richiesta un'istanza di VMware vCenter Server, con licenza venduta separatamente. Il vCenter Server è richiesto per abilitare la gestione centralizzata e le funzionalità vSphere fondamentali, quali vSphere vMotion, vSphere Distributed Resource Scheduler, ecc. Il vCenter Server è disponibile in tre edizioni:

- vCenter Server **Foundation** - massimo tre host gestibili, non è supportato il Linked mode;
- vCenter Server **Essential** - versione di vCenter abbinata ai pacchetti Essential e Essential Plus;
- vCenter Server **Standard** - versione completa (con alcuni limiti sulla versione appliance).

Esistono poi delle soluzioni in kit “all-in-one” che includono un numero definito di licenze vSphere ESXi e vCenter Server, offrendo tutto il necessario per iniziare il percorso verso la virtualizzazione. Gli Essentials Kit sono perfetti per le piccole aziende, mentre gli Acceleration Kit offrono alle aziende di medie dimensioni funzionalità più avanzate e la possibilità di scalare l'ambiente di virtualizzazione in caso di crescita aziendale.

Nelle tabelle seguenti vengono mostrate le varie edizioni di vSphere in relazione alle funzionalità offerte.

	STANDARD	STANDARD WITH OPERATIONS MANAGEMENT	ENTERPRISE	ENTERPRISE PLUS
Entitlements per CPU license				
• vCPU/VM	8 way	8 way	32 way	64 way
Features				
• Hypervisor	X	X	X	X
• vCenter Operations Manager Foundation	X	X	X	X
• High Availability • Data Recovery • vMotion	X	X	X	X
• vShield Endpoint • vSphere Replication • Hot Add	X	X	X	X
• vShield Zones • Fault Tolerance • Storage vMotion	X	X	X	X
• vCenter Operations Management Suite Standard • vCenter Protect Standard		X		
• Virtual Serial Port Concentrator • Storage APIs for Array Integration • Distributed Resource Scheduler & Distributed Power Management			X	X
• Distributed Switch • I/O Controls (Network and Storage) • Host Profiles and Auto Deploy*				X
• Storage DRS* and Policy-Driven Storage* • SR-IOV*				X
*New in vSphere 5.x				

	ESSENTIALS	ESSENTIALS PLUS	STANDARD AK	STANDARD WITH OPERATIONS MANAGEMENT AK	ENTERPRISE AK	ENTERPRISE PLUS AK
Includes						
• vSphere CPUs • vCenter Server • vSphere Storage Appliance	**6 CPUs** 1 instance vCenter Server Essentials	**6 CPUs** 1 instance vCenter Server Essentials 1 instance VSA for Essentials Plus	**6 CPUs** 1 instance vCenter Server Standard 1 instance VSA	**6 CPUs** 1 instance vCenter Server Standard 1 instance VSA	**6 CPUs** 1 instance vCenter Server Standard 1 instance VSA	**6 CPUs** 1 instance vCenter Server Standard 1 instance VSA
Entitlements per CPU license						
• vCPU	8 way	8 way	8 way	8 way	32 way	64 way
Features						
• Hypervisor	X	X	X	X	X	X
• vCenter Operations Manager Foundation	X	X	X	X	X	X
• High Availability • Data Protection • vMotion		X	X	X	X	X
• vShield Endpoint • vSphere Replication • Hot Add		X	X	X	X	X
• vShield Zones • Fault Tolerance • Storage vMotion			X	X	X	X
• vCenter Operations Management Suite Standard • vCenter Protect Standard				X		
• Virtual Serial Port Concentrator • Storage APIs for Array Integration • Distributed Resource Scheduler & Distributed Power Management					X	X
• Distributed Switch • I/O Controls (Network and Storage) • Host Profiles and Auto Deploy*						X
• Storage DRS* and Policy-Driven Storage* • SR-IOV*						X
*New in vSphere 5.x						

Capitolo 2
VMware vCenter Server

VMware vCenter Server permette la gestione centralizzata di più host ESXi e delle relative macchine virtuali. Sono disponibili due modalità per il dispiegamento di un vCenter Server:

- installazione all'interno di un sistema operativo Windows Server, su macchina fisica o virtuale;
- implementazione tramite vCenter Server Appliance, ossia una macchina virtuale preconfigurata basata su SUSE Linux Enterprise Server 11 (64bit).

Il vCenter Server (solo dalla versione 5) può essere installato in più istanze collegate tra loro in **Linked Mode**: questa modalità consente di effettuare il login ad una sola istanza, con la possibilità di gestire l'inventario di tutti i vCenter Server in Linked Mode. Con il Linked Mode, sono possibili le seguenti attività:

- accesso simultaneo a tutti i vCenter per i quali sono valide le credenziali;
- ricerca degli oggetti sull'inventario di tutti i vCenter;
- visione di un unico inventario che raggruppa gli oggetti di tutti i vCenter.

Una singola istanza di VMware vCenter Server supporta sino ad un massimo di **1000 host ESXi**, sino a **15000 macchine virtuali registrate** e sino a **10.000 macchine virtuali accese contemporaneamente**. Nell'elenco seguente sono indicate le configurazioni massime di vCenter Server 5.1.

- Numero di host per vCenter Server: 1000.
- Macchine virtuali in esecuzione (powered-on) per vCenter Server: 10000.
- Macchine virtuali registrate per vCenter Server: 15000.
- vCenter Server in Linked Mode: 10.
- Numero di host all'interno di una configurazione Linked Mode: 3000.
- Macchine virtuali in esecuzione (powered-on) all'interno di una configurazione Linked Mode: 30000.
- Macchine virtuali registrate all'interno di una configurazione Linked Mode: 50000.
- Connessioni di vSphere Client concorrenti: 100.
- Numero di host per data center: 500.
- Indirizzi MAC per vCenter Server (con OUI di default VMware): 65536.
- Dispositivi USB connessi per vSphere Client: 20.
- Autenticazioni per secondo (media): 30.

2.1 Componenti del vCenter Server

Fanno parte di una distribuzione vCenter Server i moduli e le funzionalità descritte di seguito.

- Servizi core (**core services**) - permettono la gestione di risorse, tra cui host e macchine virtuali, e la gestione di operazioni pianificate e degli allarmi.
- Servizi distribuiti (**distributed services**) - i servizi vMotion, DRS e vSphere HA installati con il vCenter Server;
- Servizi aggiuntivi (**additional services**) - richiedono un'installazione separata, come VMware vCenter Update Manager e VMware vCenter Converter;

- **Database Server** - interfaccia che consente l'accesso al database, dove sono conservate tutte le informazioni riguardanti gli oggetti, la sicurezza e la distribuzione delle risorse all'interno del data center virtuale.
- **Dominio Active Directory** - la sicurezza di vCenter Server fa affidamento sui domini Active Directory di Microsoft. Se il vCenter Server è installato su un server membro di un dominio Active Directory, risultano immediatamente disponibili gli account e i gruppi del dominio. Se il server non è membro di dominio, allora vengono utilizzati gli utenti locali del sistema Windows, oppure l'account di root nel caso in cui si utilizzi l'appliance virtuale del vCenter Server.

2.2 Installazione del vCenter Server su Windows

Il vCenter Server, nella sua versione per sistemi Windows, può essere installato sia su macchina fisica sia su macchina virtuale. L'installazione su macchina virtuale consente al vCenter di sfruttare tutti i servizi di alta disponibilità offerti da VMware vSphere senza la necessità di un server dedicato. Inoltre, tramite vMotion e Storage vMotion, è possibile migrare a caldo il vCenter da un host a un altro e da un datastore a un altro.

I sistemi Windows sui quali è possibile installare vCenter Server sono i seguenti:

- Microsoft Windows Server 2003 Standard, Enterprise o Datacenter;
- Microsoft Windows Server 2003 Standard, Enterprise o Datacenter R2;
- Microsoft Windows Server 2008 Standard, Enterprise o Datacenter;
- Microsoft Windows Server 2008 Standard, Enterprise o Datacenter R2.

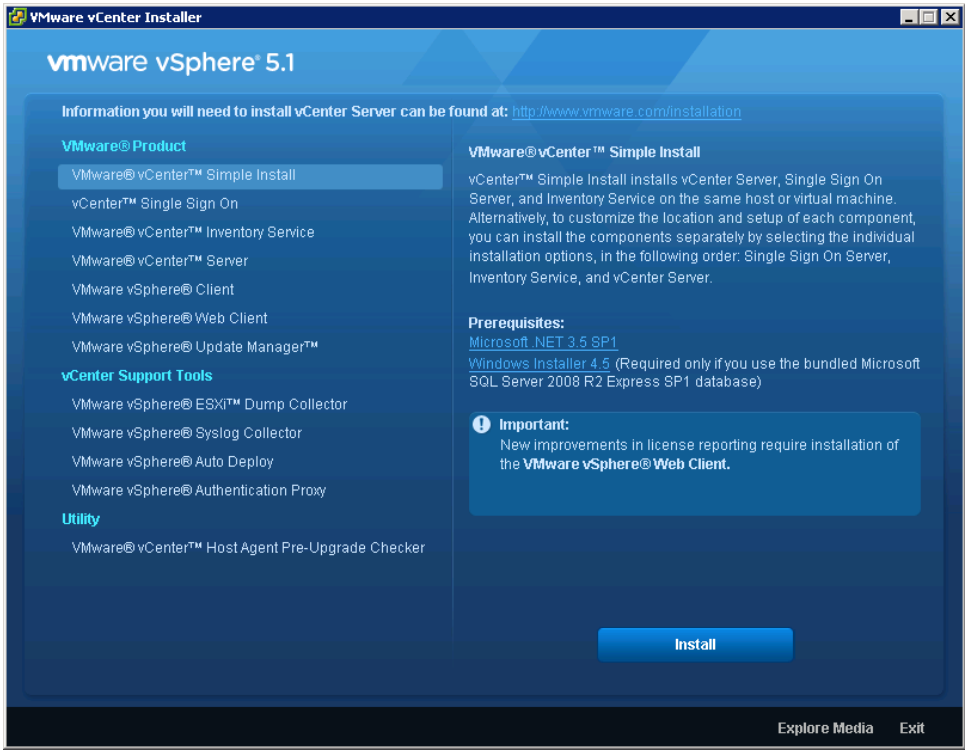
In ogni caso il sistema Windows non può essere un domain controller Active Directory. I requisiti hardware per l'installazione del vCenter Server, sia su macchina fisica che virtuale, sono indicati qui sotto.

Hardware	**Requisiti minimi**
Processore	2 CPU a 64 bit oppure una CPU 64 bit dual core, AMD o Intel. Velocità del processore 2.0Ghz.
Memoria	Se il vCenter Server è installato su una macchina che non ospita vCenter Single Sign-On e vCenter Inventory Service, sono sufficienti 4 GB di RAM. Se sulla stessa macchina sono installati il vCenter Server, il vCenter Single Sign-On e il vCenter Inventory Service, sono consigliati 10 GB di RAM.
Spazio disco	Se il vCenter Server è installato su una macchina che non ospita vCenter Single Sign-On e vCenter Inventory Service, sono sufficienti 4 GB di spazio libero su disco. Se sulla stessa macchina sono installati il vCenter Server, il vCenter Single Sign-On e il vCenter Inventory Service, sono consigliati almeno 60 GB di spazio libero su disco.
Dimensioni DB	Calcolare circa 300Mb ogni 50VM
Networking	Raccomandata connessione 1Gbit

Per la gestione e l'organizzazione dei dati, vCenter Server richiede l'uso di un database. Per installazioni di dimensioni contenute, ovvero sino ad un massimo di 5 host ESXi e 50 macchine virtuali, è possibile utilizzare Microsoft SQL Server 2008 R2 Express incluso nel pacchetto di installazione. Per ambienti più estesi, sono supportati i seguenti database:

- IBM DB2;
- SQL Server 2005;

- SQL Server 2008
- Oracle 10g;
- Oracle 11g.



La procedura di installazione prevede, nell'ordine, i passaggi indicati di seguito.

1. Download dell'**installer** di VMware vCenter Server 5.1, reperibile dalla pagina di download di VMware, all'indirizzo http://www.vmware.com/support/.
2. Installazione di **vCenter Single Sign On**. Si tratta del nuovo sistema di autenticazione di vSphere 5.1. Garantisce elevata sicurezza all'intera infrastruttura, consentendo a tutti i componenti di vSphere di comunicare tra loro attraverso lo scambio sicuro di un token (token exchange mechanism). Agevola e rende univoca la gestione delle password, consentendo di avere un unico login per tutti i sistemi (vCenter, Host, Appliance), con la possibilità di integrarsi con Active Directory o con un server openLDAP.
3. Installazione di **vCenter Inventory Service** – questo servizio memorizza i dati d'inventario per consentirne la ricerca attraverso più istanze di vCenter Server in Linked Mode.
4. Installazione di **vCenter Server**.

L'installer fornisce una procedura di distribuzione semplificata, chiamata Simple Install, che permette di installare vCenter Single Sign On, Inventory Service e vCenter Server con un solo passaggio.

2.2.1 Installazione di vCenter Single Sign On

1. Seguire le istruzioni proposte dalla procedura guidata, scegliere la lingua ed accettare gli accordi di licenza. Questo vale sia con la procedura Simple Install, sia installando i vari servizi singolarmente.
2. Impostare una password per l'account administrator di vCenter Single Sign On. La password deve essere superiore a otto caratteri, deve includere almeno un carattere maiuscolo, un numero e un carattere speciale.

3. Selezionare un database. L'installazione di un'istanza locale di Microsoft SQL Server 2008 R2 Express è la scelta più indicata per architetture sino a 5 host ESXi e sino a 50 macchine virtuali.
4. Nel campo "Fully Qualified Domain or IP address", inserire l'indirizzo IP o il nome host del sistema Windows e andare avanti.
5. Si consiglia di non modificare la posizione di default della directory di installazione.
6. Andare avanti e impostare la porta HTTPS. Si consiglia di non modificare i valori di default.

2.2.2 Installazione del vCenter Inventory Service

Avviare l'installazione, oppure attendere che la procedura Simple Install porti a termine l'installazione. Non sono richieste configurazioni particolari.

2.2.3 Installazione di vCenter Server

1. Avviare l'installazione, oppure attendere che la procedura Simple Install faccia partire l'installazione. Impostare la chiave di licenza nel relativo campo, oppure lasciarlo vuoto per procedere con la valutazione del prodotto (valida per 60 giorni), quindi andare avanti. È possibile impostare una chiave valida anche successivamente.
2. Scegliere il tipo di database. La scelta di un'istanza di Microsoft SQL Server 2008 Express è consigliata per architetture sino a 5 host ESXi e sino a 50 macchine virtuali.
3. Lasciare abilitata la voce "Use SYSTEM Account", quindi andare avanti. L'account amministratore del vCenter coincide con l'account amministratore di Windows Server.
4. Si consiglia di lasciare le porte con la loro configurazione predefinita. Andare avanti.
5. Selezionare la dimensione dell'infrastruttura virtuale e andare avanti.
6. Rivedere le impostazioni e fare clic su Install.
7. Terminata l'installazione, fare clic su Finish.

2.3 vCenter Support Tools

L'installer del vCenter Server consente l'installazione di diversi componenti aggiuntivi, raggruppati sotto il nome di vCenter Support Tools.

2.3.1 vSphere ESXi Dump Collector

Un **core dump** è la cattura dello stato di memoria di un host, prima di un blocco operativo. In maniera predefinita, un core dump è salvato nel disco locale dell'host. ESXi Dump Collector è utilizzato per salvare i dump in una destinazione in rete, consentendo di centralizzare tutti i dump su un unico punto e agevolando il lavoro di debug successivo al blocco dell'host.

2.3.2 vSphere Syslog Collector

Syslog Collector permette la raccolta dei log dei vari host ESXi centralizzandola attraverso la rete. È un tool che risulta molto utile con gli host diskless, cioè privi di hard disk, dove il boot viene effettuato tramite chiavetta USB o tramite la funzione di Auto-Deploy.

2.3.3 vSphere Auto Deploy

Auto Deploy consente di portare a termine la distribuzione di host ESXi in pochi minuti e "in tempo reale". Può essere installato come parte del vCenter Server, come modulo stand-alone su una macchina Windows oppure utilizzato tramite vCenter Server Appliance, in cui è integrato nativamente. Una volta in esecuzione, crea le immagini per gli aggiornamenti, eliminando la necessità di installare patch e programmare finestre temporali per questo tipo di operazioni.

Con Auto Deploy è possibile specificare l'immagine da installare e i profili host da rendere disponibili con l'immagine; si può indicare inoltre la cartella o il cluster in cui collocare ogni host. Auto Deploy utilizza un'infrastruttura di rete basata su **protocollo PXE** per personalizzare gli host sin dalla loro accensione.

L'Auto Deploy è una modalità di provisioning degli host ESXi alternativa all'installazione classica. Gli host eseguono il boot attraverso la rete, contattano l'Auto Deploy Server e ricevono l'immagine ESXi da caricare in memoria RAM; l'Auto Deploy Server a questo punto usa gli **Host Profiles** per la configurazione degli host. Per creare le immagini, si utilizza il tool **Image Builder** da riga di comando, mentre i profili host sono gestibili tramite vSphere Client.

2.3.4 vSphere Authentication Proxy

Permette agli host ESXi di collegarsi a un dominio senza l'utilizzo di credenziali Active Directory. Il tool aumenta la sicurezza degli host che si avviano in modalità PXE e degli host distribuiti tramite Auto Deploy, eliminando la necessità di memorizzare credenziali Active Directory nelle configurazioni degli host.

2.4 Installazione di vCenter Server Appliance

L'appliance virtuale del vCenter Server è stata creata da VMware a partire dalla versione 5 di vSphere. È stata pensata per liberare l'utente finale dall'obbligo di una licenza Windows Server e per rendere veloce e snella l'implementazione del vCenter Server, soprattutto per infrastrutture medio-piccole.

Le caratteristiche minime richieste per l'appliance sono indicate qui sotto.

Spazio disco libero sull'host ESXi	Minimo 7GB, massimo 80GB
Memoria da assegnare alla macchina virtuale	• Per un massimo di 10 host ESXi oppure un massimo di 100 macchine virtuali: 4GB. • Per un massimo di 100 host ESXi oppure un massimo di 1000 macchine virtuali: 8GB. • Per un massimo di 400 host ESXi oppure un massimo di 4000 macchine virtuali: 13GB.

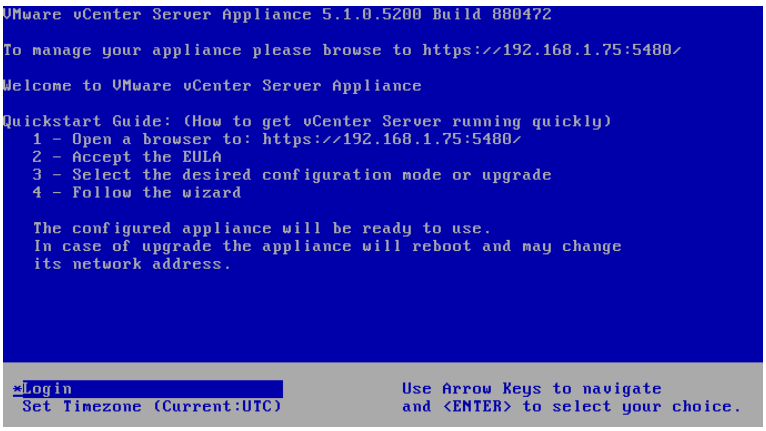
	• Per un più di 400 host ESXi o più di 4000 virtual machine: 17GB.
Processore	2 vCPU

vCenter Server Appliance non supporta database MSSQL o IBM DB2 e non supporta configurazioni in Linked Mode.

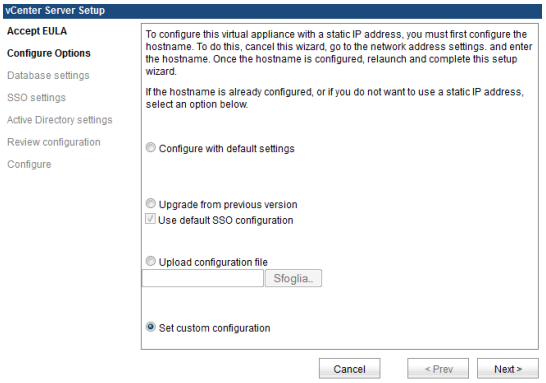
2.4.1 Importazione e configurazione dell'Appliance

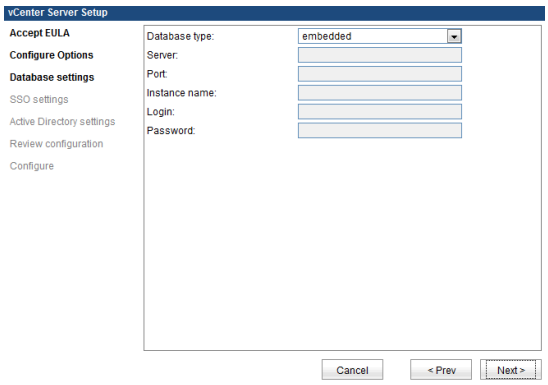
Il deploy è simile a quello previsto per qualunque Virtual Appliance. Si scaricano i file VMDK e OVF dal sito di VMware, e si procede con la loro importazione: con vSphere Client collegarsi all'host ESXi su cui eseguire il deploy, quindi andare su **File > Deploy OVF Template**. Indicare la posizione del file **.ovf** e procedere come suggerito dalla procedura guidata. Terminata l'operazione di deploy, i passi da compiere sono indicati di seguito.

1. Dalla console, configurare i parametri di rete e impostare il fuso orario.

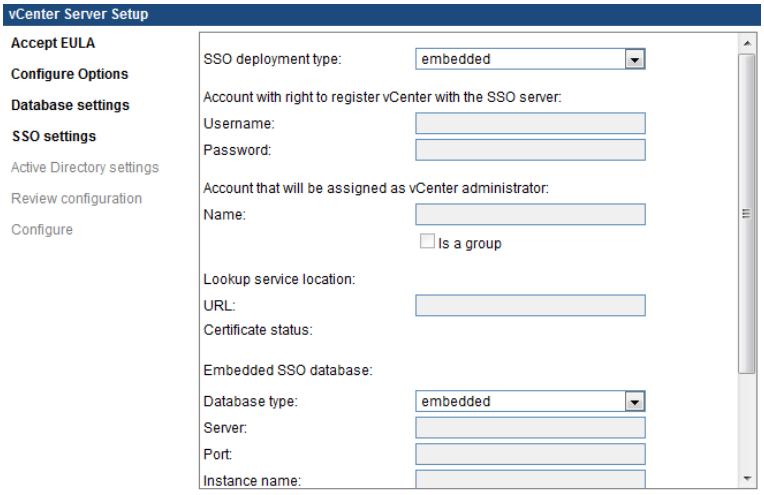


2. Accedere con un browser web all'indirizzo di configurazione https://ip_appliance:5480 ed eseguire il login (le credenziali di default sono **root** / **vmware**).
3. Dopo aver accettato le condizioni di licenza, procedere con la configurazione iniziale ed impostare il database. Il database interno (embedded) è di tipo DB2 Express. L'alternativa è quella di utilizzare un database Oracle esterno.

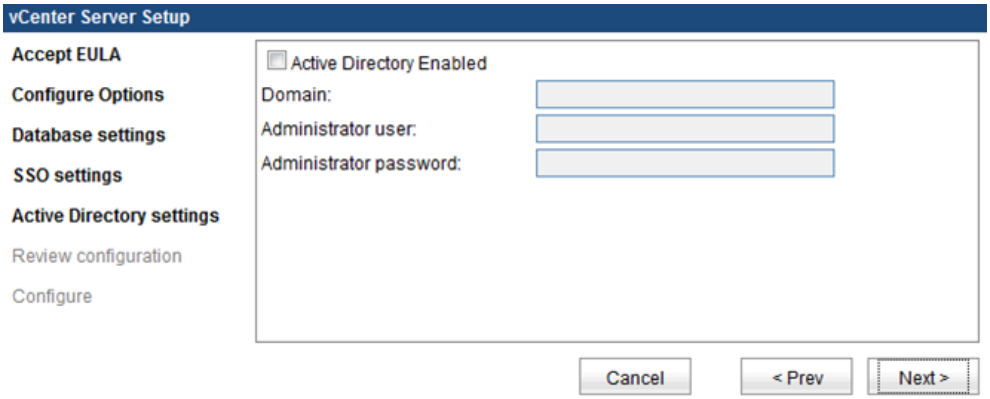




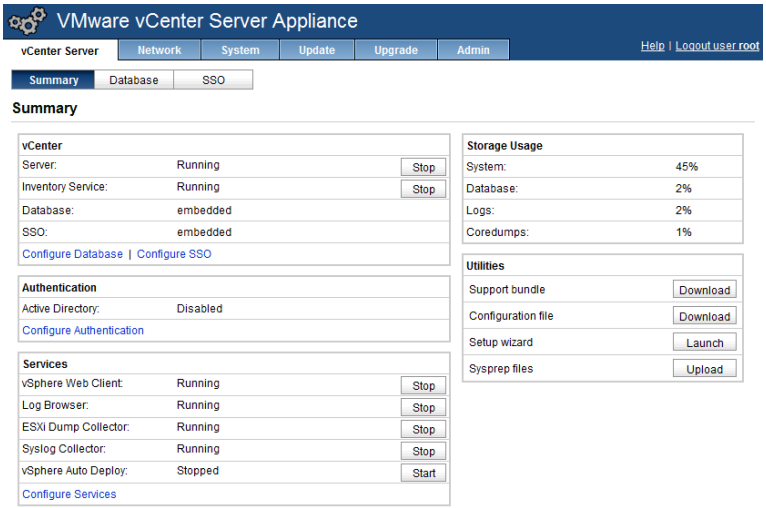
4. Il passo successivo prevede la configurazione del Single Sign-On Server e del relativo database.



5. Opzionalmente può essere configurata l'integrazione con un dominio Active Directory.



6. Tramite i vari tab presenti nell'interfaccia web, si possono configurare le porte HTTP/HTTPS di ascolto, la password dell'account root, le impostazioni di rete, e si può spegnere o riavviare la virtual appliance.



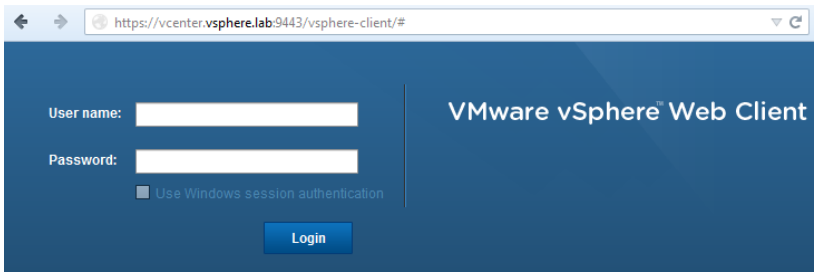
7. Gli strumenti di gestione dell'infrastruttura virtuale non cambiano utilizzando la versione appliance del vCenter: il vSphere Web Client è già integrato, mentre il vSphere Client è sempre utilizzabile.

2.5 Strumenti di gestione

2.5.1 vSphere Web Client

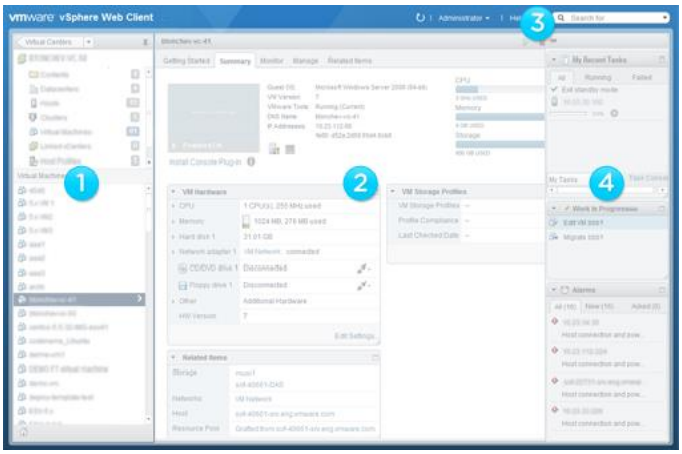
A partire da vSphere 5.1, vSphere Web Client rappresenta il principale strumento per la gestione dell'ambiente vSphere, sostituendo in questo ruolo il vSphere Client (comunque ancora disponibile). vSphere Web Client permette la gestione del vCenter Server e dell'intera infrastruttura virtuale tramite web browser. Si tratta quindi di uno strumento indipendente dal sistema operativo in uso, a differenza del vSphere Client disponibile solo per sistemi operativi Windows. Si installa tramite l'installer del vCenter Server, selezionando la voce **VMware vSphere Web Client** e facendo clic su Install.

Una volta installato, vSphere Web Client è raggiungibile tramite browser in https sulla porta 9443, all'indirizzo del vCenter, come mostrato qui sotto.



L'interfaccia di vSphere Web Client è strutturata in quattro aree principali.

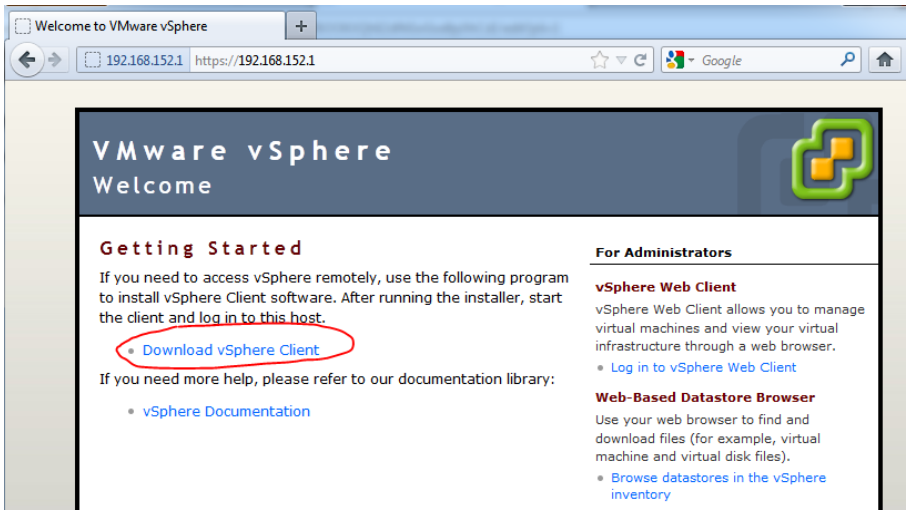
1. **Navigator** – sezione in cui sono visualizzati tutti gli oggetti dell'inventario.
2. **Content Area** - sezione in cui sono visualizzate le informazioni degli oggetti selezionati.
3. **Search** – campo per la ricerca di oggetti specifici.
4. **Global Information** - sezione in cui sono visualizzati gli allarmi, le operazioni in corso e quelle più recenti.



Il vSphere Web Client permette di sfogliare rapidamente tutto l'inventario, con la possibilità di relazionare un oggetto agli altri elementi che interagiscono con lui. In questo modo si evita di doversi spostare tra i diversi inventari per avere tutte le informazioni su un determinato oggetto. Inoltre è possibile personalizzare l'interfaccia spostando o eleminando i vari elementi che la compongono.

2.5.2 vSphere Client

vSphere Client, sino alla versione 5.0 di VMware vSphere, era la principale interfaccia di gestione dell'intera infrastruttura virtuale. Può ancora essere utilizzata per lo stesso scopo. Inoltre permette l'accesso diretto agli host ESXi. Tuttavia, se gli host ESXi sono gestiti da un vCenter Server, è sconsigliato operare collegandosi direttamente ad essi. vSphere Client è disponibile solo per sistemi operativi Windows. Si scarica accedendo alla pagina web dell'host ESXi o del vCenter Server, come mostrato nell'immagine seguente.



Una volta installata l'applicazione, al suo avvio apparirà la richiesta di login.

Nella finestra di login si inseriscono il nome o l'indirizzo IP dell'host ESXi o del vCenter Server, quindi le credenziali di accesso.

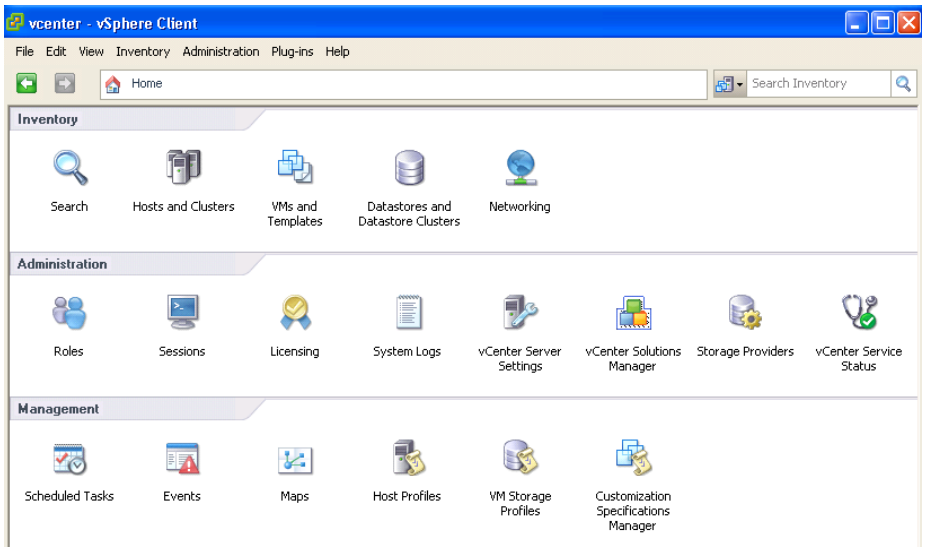
2.5.3 Gestione dell'inventario

La gestione degli oggetti all'interno di VMware vCenter Server segue una struttura gerarchica, dove la radice è chiamata root object e corrisponde al vCenter stesso. Gli oggetti possono essere raggruppati all'interno di contenitori ed essere a loro volta contenitori di altri oggetti. L'inventario può anche essere personalizzato con la creazione di cartelle e sottocartelle in cui posizionare gli oggetti. Per oggetti si intendono: host, macchine virtuali, template, cluster, resource pool, datastore e reti. Un'istanza di vCenter può gestire contemporaneamente più data center; tuttavia, gli oggetti di data center diversi possono interagire tra loro solo in maniera limitata. Ad esempio, il vMotion di una VM è possibile tra due host ESXi appartenenti ad uno stesso data center, mentre non è possibile tra 2 host appartenenti a data center diversi.

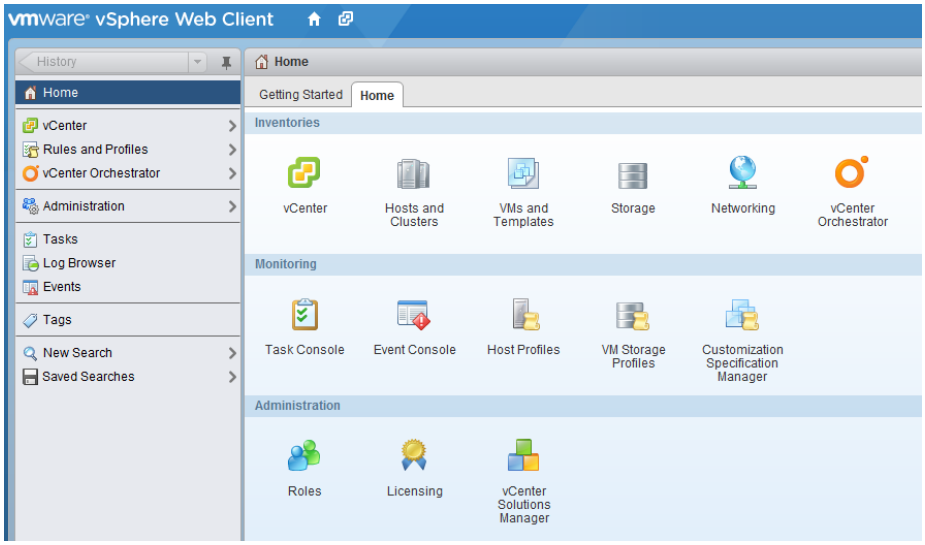
La gestione degli oggetti segue la stessa logica sia utilizzando vSphere Client, sia optando per il Web Client. Ad esempio, facendo clic su **Hosts and Clusters**, si avrà visibilità di tutti gli host e cluster presenti nel data center; selezionando la voce **VMs and Templates** si potranno vedere tutte le macchine virtuali e i template presenti nel data center; allo stesso modo, selezionando le

voci **Datastores and Datastore Clusters** o **Networking** si potranno vedere rispettivamente tutti i datastore presenti nel data center e tutte le impostazioni di rete relative all'infrastruttura virtuale.

Home Page di accesso al vCenter tramite vSphere Client.

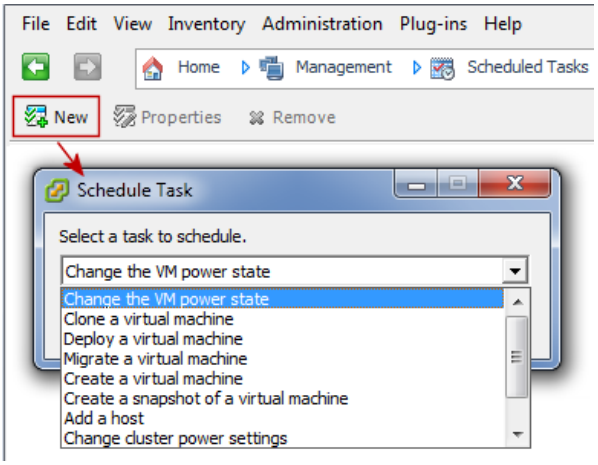


Home Page di accesso al vCenter tramite vSphere Web Client.



2.5.4 Operazioni programmate

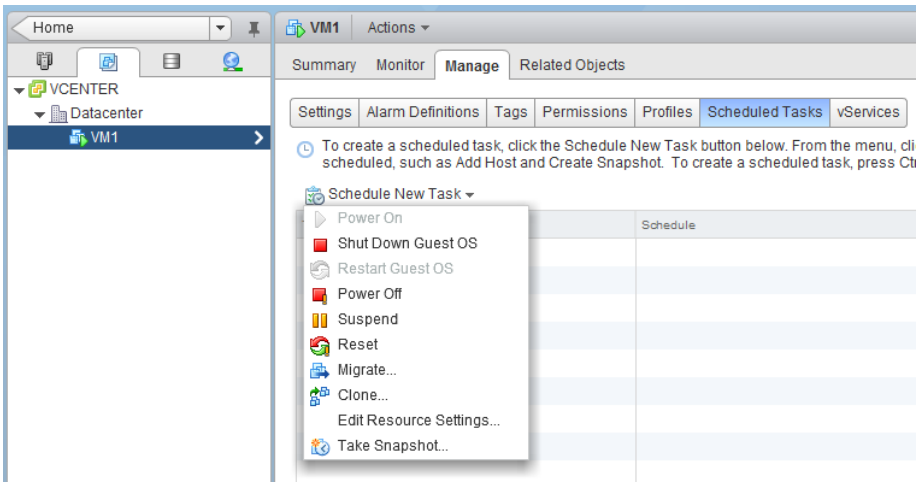
Tramite gli strumenti di gestione del vCenter Server, è possibile pianificare l'esecuzione di diverse azioni all'interno dell'ambiente virtuale. Le operazioni pianificate, dette **Scheduled Tasks**, possono essere eseguite una sola volta o più volte, a intervalli regolari. Per creare un'operazione pianificata è necessario collegarsi al vCenter Server. Tramite vSphere Client, dal percorso **Home > Management > Scheduled Task**, si deve fare clic su **New**, come mostrato qui sotto.



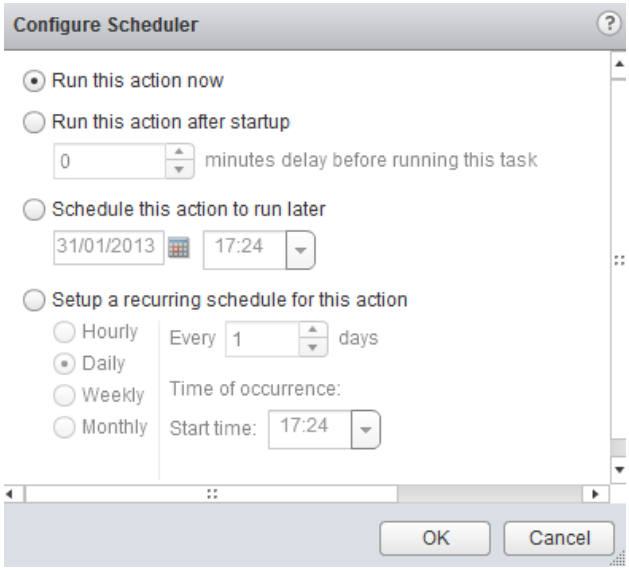
Le operazioni possibili sono descritte nella tabella seguente.

Operazione	**Descrizione**
Add a host	Inserimento di un host all'interno di uno specifico data center o cluster.
Change the power state of a virtual machine	Azioni di accensione, spegnimento, sospensione o riavvio di una VM.
Change cluster power settings	Attivazione o disattivazione di DPM (VMware Distributed Power Management) per gli host di un cluster.
Change resource settings of a resource pool or virtual machine	Modifica delle risorse seguenti: • CPU – Shares, Reservation, Limit; • Memoria – Shares, Reservation, Limit.
Check compliance of a profile	Verifica della configurazione di un host rispetto a quanto indicato nel profilo host.
Clone a virtual machine	Clonazione di una VM, che viene poi posizionata in uno specifico host o cluster.
Create a virtual machine	Creazione di una nuova VM in uno specifico host.
Deploy a virtual machine	Creazione di una nuova VM in uno specifico host, a partire da un template.
Export a virtual machine	Operazione disponibile solo se VMware vCenter Converter è installato nel sistema. Permette l'esportazione di VM in diversi formati.
Import a virtual machine	Operazione disponibile solo se VMware vCenter Converter è installato nel sistema. Permette di importare macchine fisiche, macchine virtuali, immagini di sistema.
Migrate a virtual machine	Migrazione di una VM in uno specifico host o cluster.
Make a snapshot of a virtual machine	Snapshot di una VM.
Scan for Updates	Operazione disponibile solo se VMware vCenter Update Manager è installato nel sistema. Esegue la scansione di template, macchine virtuali e host per la verifica di nuovi aggiornamenti.
Remediate	Operazione disponibile solo se VMware vCenter Update Manager è installato nel sistema. Scarica e installa le nuove patch individuate durante le operazione di scansione degli aggiornamenti.

Le stesse operazioni sono possibili tramite vSphere Web Client, ma sono sempre contestuali all'oggetto selezionato: ci si posiziona sull'oggetto per il quale si intende creare un'operazione pianificata, si seleziona il tab **Manage**, quindi il tab **Scheduled Tasks**, e dal menu a tendina **Schedule New Tasks** si seleziona l'operazione da pianificare.



Per ogni operazione pianificata sono disponibili diverse opzioni di pianificazione, come mostrato nell'immagine qui sotto.

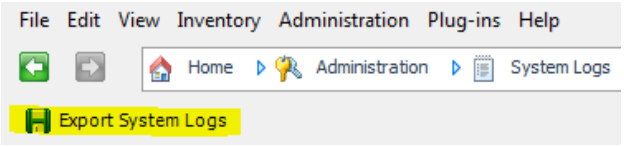


2.5.5 Gestione dei log

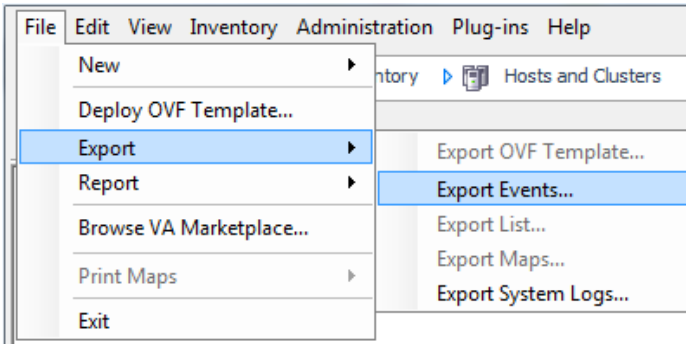
L'analisi delle informazioni di log è utile ogni qualvolta sia necessario ricostruire una serie di eventi che hanno preceduto un determinato problema, allo scopo di individuarne la causa. Per esportare le informazioni di diagnostica, contenute nei log degli host ESXi, ci sono diverse possibilità.

Procedura con vSphere Client

- Collegandosi al vCenter Server tramite vSphere Client, il percorso **Home > Administration > System Logs** propone un pulsante denominato **Export System Logs**, con cui è possibile esportare i log dei vari host presenti nell'infrastruttura virtuale.

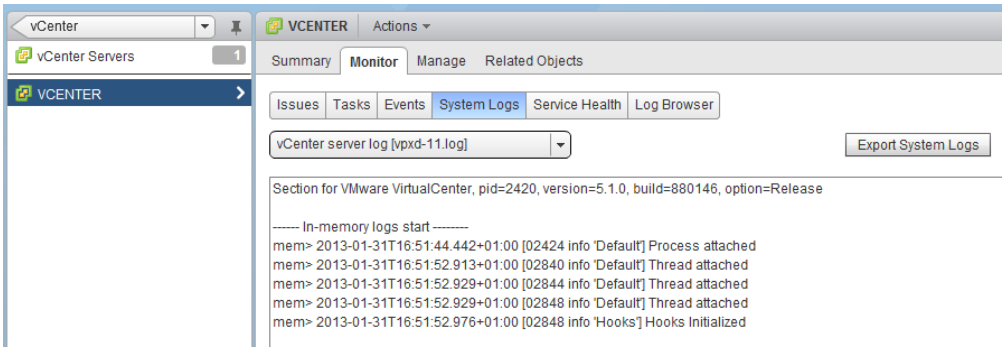


- In alternativa, sempre tramite vSphere Client, selezionare l'host desiderato dall'inventario, quindi fare clic sul menu **File** e selezionare le voci **Export > Export Events**.

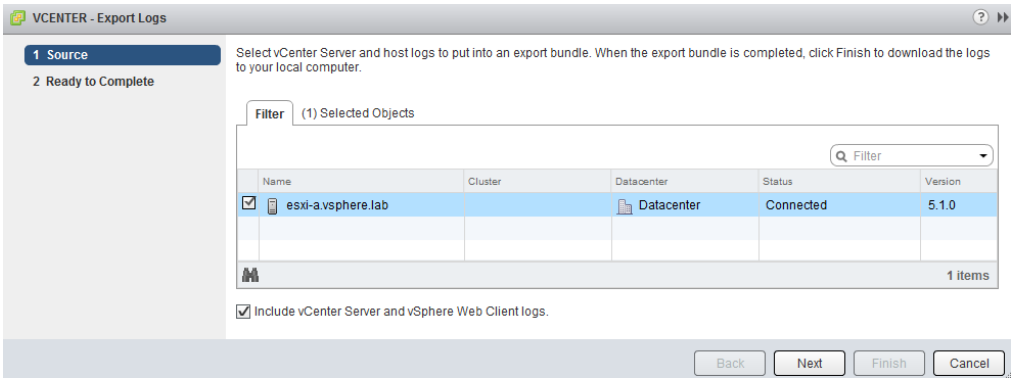


Procedura con vSphere Web Client

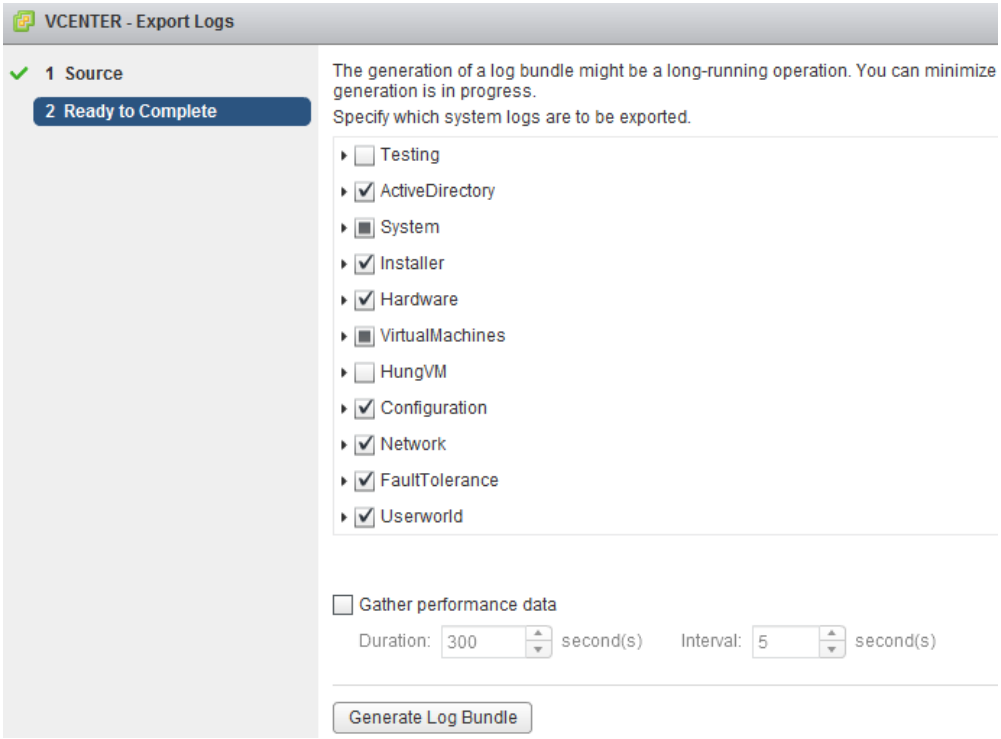
- Dall'inventario, selezionare il vCenter Server contenente l'host desiderato.
- Fare clic sul tab **Monitor** e sulla voce **System Logs**.
- Fare clic sul pulsante a destra **Export System Logs**.



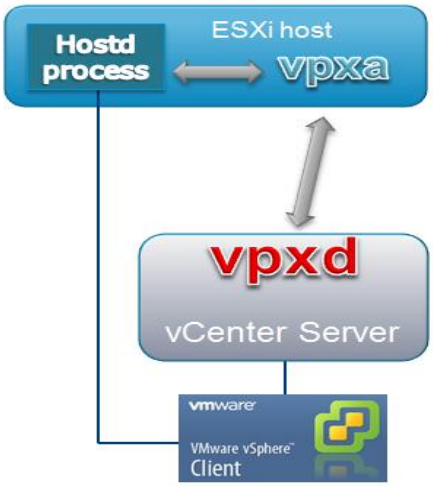
- Dalla finestra "Export Logs", selezionare l'host desiderato. Opzionalmente, è possibile esportare anche i log del vCenter Server e del Web Client, abilitando la voce **Include vCenter Server and vSphere Web Client logs**.



- Andare avanti, selezionare il tipo di log da esportare e fare clic su **Generate Log Bundle**. A questo punto sarà possibile scaricare un file .zip contenente i file di log. Terminato il download, fare clic su **Finish**.



2.6 La comunicazione tra il vCenter Server e gli host ESXi



L'accesso agli host ESXi da parte del vCenter Server è permesso da un servizio chiamato **vpxa**, che si attiva sull'host nel momento in cui questo è inserito nell'inventario del vCenter Server. Su ogni host ESXi è sempre in esecuzione un processo chiamato **hostd**, che permette l'esecuzione di operazioni e comandi relativi alle macchine virtuali e allo storage. Si tratta quindi di un processo responsabile della gestione della maggior parte delle operazioni interne a vSphere ESXi.

All'interno dell'host, l'agent vpxa dialoga con il processo hostd, e quest'ultimo si pone come intermediario verso il servizio **vpxd** in esecuzione sul vCenter Server, consentendo l'esecuzione delle operazioni impartite dal vCenter. Il processo vpxd permette quindi la connessione e il dialogo tra vCenter e host ESXi.

Per quanto riguarda il traffico di rete tra il vCenter Server e gli host gestiti, e tra il vCenter Server e una macchina che esegue vSphere Client o vSphere Web Client, le principali porte da lasciare aperte sul firewall sono indicate nell'elenco che segue.

- **80 TCP** - utilizzata per le connessioni dirette **HTTP**. Le richieste su questa porta sono comunque reindirizzate sulla porta HTTPS 443, per motivi di sicurezza.

- **389 TCP/UDP** - utilizzata per le connessioni **LDAP** (Directory Services); se l'istanza LDAP viene servita da Active Directory di Microsoft Windows, la porta deve essere cambiata in un'altra compresa nell'intervallo 1025 – 65535.
- **443 TCP** - utilizzata per le connessioni protette in **HTTPS**; il vSphere Client utilizza questa porta per le connessioni al vCenter e agli host ESXi.
- **636 TCP** - utilizzata per le connessioni (protette in SSL) fra **istanze di vCenter in Linked Mode**.
- **902 TCP/UDP** - utilizzata per lo scambio di informazioni e dati tra il vCenter Server e gli host gestiti. Inoltre, su questa porta gli host inviano un continuo heartbeat al vCenter Server, tramite protocollo UDP.
- **903 TCP** - utilizzata da vSphere Client per visualizzare l'interfaccia console delle macchine virtuali.
- **8080 TCP** - utilizzata per le connessioni Web Services HTTP (VMware VirtualCenter Management Web Services).
- **7005, 7009, 7080, 7444 TCP** – utilizzate dal servizio vCenter Single Sign On.
- **9090, 9443 TCP** – utilizzate da vSphere Web Client (HTTP e HTTPS).
- **10080, 10109, 10111, 10443 TCP** – utilizzate dal servizio vCenter Inventory Service.

2.7 Disponibilità del vCenter server

La strada più veloce per garantire alta disponibilità per il vCenter Server è quella di fornire alta disponibilità ai suoi componenti principali.

- Active Directory
- Database del vCenter Server

Una delle soluzioni più adottate per la continuità del vCenter Server prevede il suo utilizzo su macchina virtuale, affinché possa essere protetto dal servizio vSphere HA.

vSphere HA richiede il vCenter Server solo per la configurazione iniziale. In seguito il servizio funzionerà sugli host in maniera indipendente dal vCenter. Quest'aspetto è importante per capire cosa succede ad un'istanza virtuale di vCenter Server protetta con vSphere HA: se l'host che ospita il vCenter dovesse subire un improvviso blocco operativo (con la conseguenza di avere il vCenter non in linea), vSphere HA sposterebbe il vCenter su un altro host.

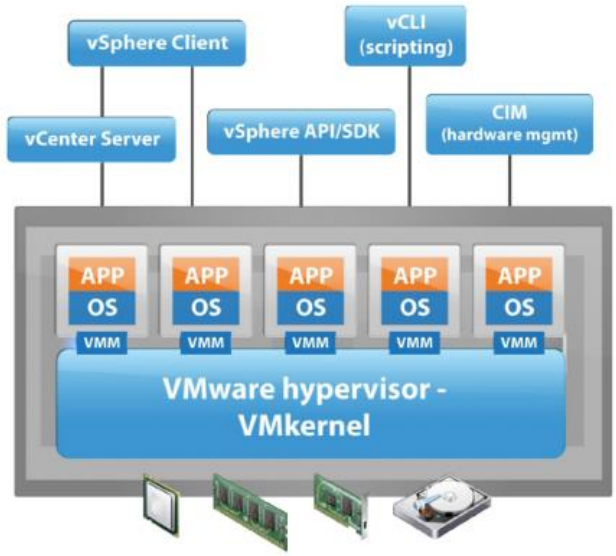
Un'altra soluzione prevede l'impiego del vCenter Server Heartbeat (richiede licenza specifica venduta separatamente), che estende la disponibilità di vCenter Server ed esegue, tramite LAN o WAN, il failover del server di gestione e del database su un server in standby. vCenter Server Heartbeat è in grado di rilevare con precisione tutti i componenti del vCenter Server ed è facile da configurare e implementare.

Capitolo 3
vSphere ESXi

ESXi è l'**hypervisor** di VMware vSphere. Richiede una licenza d'uso se utilizzato all'interno dell'ambiente vSphere, ma esiste anche in versione gratuita, specificamente pensata per quelle piccole realtà in cui sono sufficienti poche macchine virtuali operanti all'interno di singoli server, e che possono fare a meno dei componenti di vSphere che danno continuità di servizio e alta affidabilità.

Ogni host ESXi, nella versione 5.1, supporta sino a 512 macchine virtuali, un massimo di 2048 CPU virtuali, e sino a 2Tb di memoria RAM per host. Le CPU fisiche supportate sono quelle con **architettura a 64bit** e set di **istruzioni LAHF e SAHF**.

3.1 Architettura di ESXi



ESXi fornisce uno strato di virtualizzazione, tecnicamente chiamato **VMKernel**, che permette di estrapolare risorse dal processore, dalla memoria, dallo storage e dalla rete dell'host fisico, per rilasciarle a più macchine virtuali. In un'architettura ESXi, le applicazioni che girano sulle macchine virtuali accedono a CPU, memoria, disco e interfacce di rete senza accedere direttamente all'hardware sottostante. Il VMkernel riceve le richieste di risorse dalle macchine virtuali attraverso il virtual machine monitor (VMM) e le presenta all'hardware fisico. Il VMkernel è a 64 bit, supportato su processori Intel, Xeon e superiori, o AMD Opteron. Non sono supportati host con processori a 32-bit, mentre all'interno delle macchine virtuali sono supportati sia i sistemi operativi a 32-bit sia quelli a 64-bit.

3.2 Requisiti hardware

I requisiti minimi per l'installazione di VMware ESXi 5.1 sono elencati di seguito.

Per la parte generale di sistema:

- server con CPU x86 a 64bit;
- CPU con almeno 2 core, supporto hardware alla virtualizzazione (Intel VT-x or AMD RVI), set di **istruzioni LAHF e SAHF**;
- bit NX/XD per la CPU abilitato a livello di BIOS;
- 2GB di memoria RAM fisica (raccomandati 8Gb);
- una o più interfacce Ethernet Gigabit o 10Gb.

Per la parte storage uno dei seguenti tipi di controller:

- controller SCSI - Adaptec Ultra-160 o Ultra-320, LSI Logic Fusion-MPT, oppure NCR/Symbios SCSI;
- controller RAID - Dell PERC (Adaptec RAID o LSI MegaRAID), HP Smart Array RAID, IBM (Adaptec) ServeRAID controller.

L'installazione e il booting sono possibili con i seguenti sistemi:

- dischi SATA connessi a controller SAS o controller SATA on-board supportati;
  Controller SAS supportati
  - LSI1068E (LSISAS3442E)
  - LSI1068 (SAS 5)
  - IBM ServeRAID 8K SAS controller
  - Smart Array P400/256 controller
  - Dell PERC 5.0.1 controller

  Controller SATA integrati sulle schede madri
  - Intel ICH9
  - NVIDIA MCP55
  - ServerWorks HT1000
- dischi Serial Attached SCSI (SAS);
- dischi su SAN Fibre Channel o iSCSI;
- dischi USB (supportati solo per l'installazione, non per la memorizzazione di macchine virtuali).

3.3 Installazione di ESXi

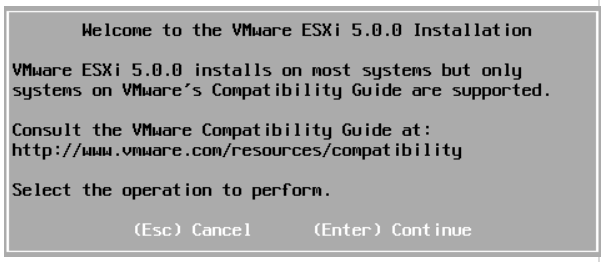
ESXi può essere installato su hard disk, su dispositivi USB, su schede di memoria SD, o direttamente su una Storage Area Network. Lo spazio minimo richiesto per l'installazione è di 1Gb. Se però si utilizza un disco locale o una LUN iSCSI, sono richiesti 5.2GB per permettere la creazione di un volume VMFS e 4GB di "scratch partition". Con dispositivi USB e SD, l'installer non crea la partizione di scratch, a causa della sensibilità I/O di questi dispositivi. È quindi importante evidenziare che, con dispositivi USB o SD, non ci sono vantaggi nell'utilizzare dimensioni superiori ad 1Gb, perché solo il primo GB sarebbe impiegato per l'installazione.

La procedura di installazione standard prevede il download dell'immagine ISO dal sito di VMware, la masterizzazione dell'immagine su un CD, e l'avvio del server fisico con boot dal lettore CD. L'immagine ISO può essere avviata anche da un dispositivo USB avviabile o dalla rete tramite protocollo PXE. In ambienti con numero di host non superiore a cinque, l'installazione sarà di tipo interattivo, ossia l'amministratore risponde alle richieste dell'installer di ESXi. L'installer formatta e partiziona il disco di destinazione e installa l'immagine di boot di ESXi. Se sul disco non è presente alcuna versione di ESXi, tutti i dati presenti sono sovrascritti, ed il precedente schema di partizionamento viene eliminato. Se invece il disco contiene già una versione di ESXi o ESX, oppure un datastore VMFS, l'installer proporrà diverse opzioni di upgrade, tra cui quella di preservare i dati contenuti nel datastore VMFS.

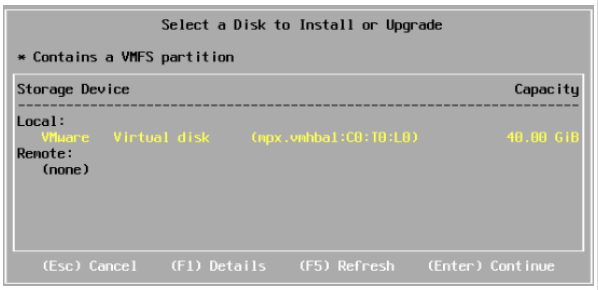
L'installazione chiede poche informazioni: le più importanti riguardano la posizione di installazione (viene mostrata una lista di dischi sui quali installare VMware ESXi) e la scelta della password di root.

Di seguito possiamo vedere i passaggi necessari.

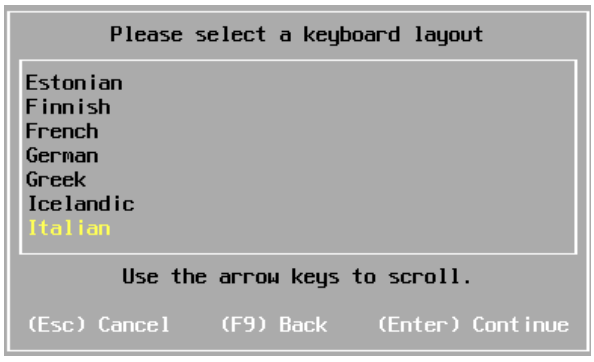
1. Avvio dell'installazione. Premere INVIO per continuare.



2. Selezione del disco su cui verrà installato ESXi. In questa fase, se nel server è presente una Pen Drive USB, sarà possibile utilizzarla come disco di destinazione.

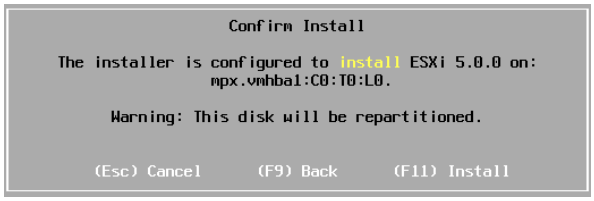


3. Selezione della lingua per la tastiera.

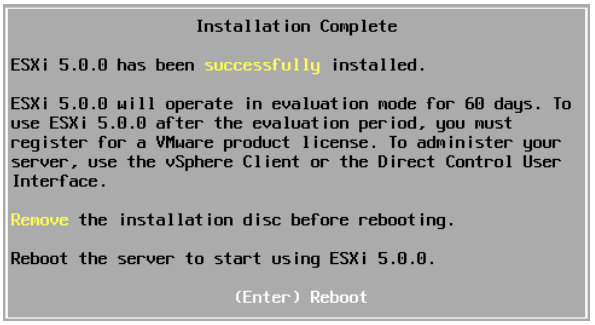


4. Impostazione della password principale.

5. Conferma dell'installazione su disco. Premere F11 per continuare.



6. Completamento dell'installazione.



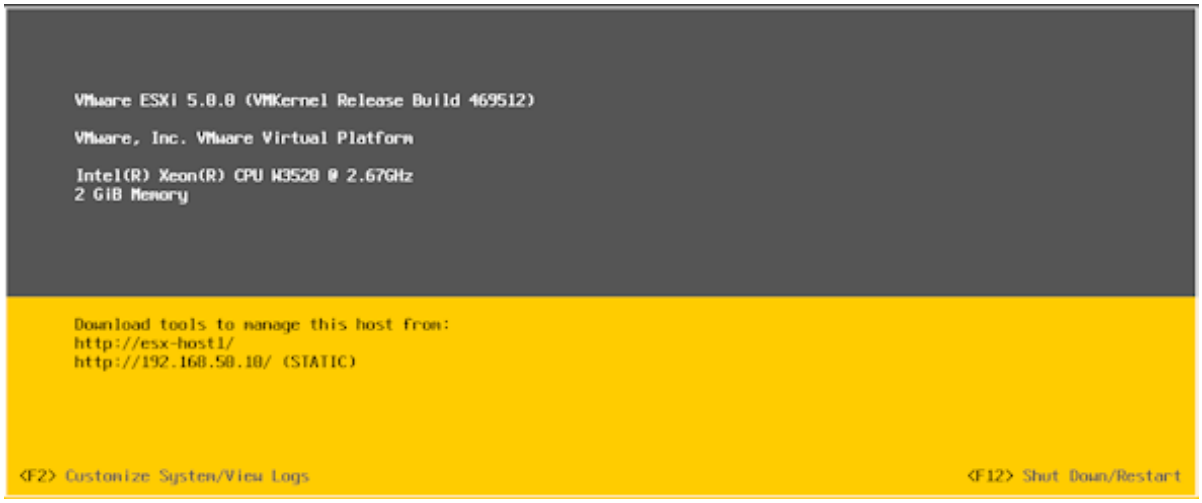
Al riavvio l'host ESXi sarà raggiungibile via rete con l'IP assegnato tramite DHCP. Nel caso in cui non fosse presente un server DHCP sulla rete, sarà possibile raggiungere l'host tramite l'IP autoassegnato di tipo 169.254.x.x/16, visibile nella console dopo l'avvio. Dalla console stessa è comunque possibile impostare un indirizzo IP di tipo statico.

3.4 Configurazione di ESXi

vSphere ESXi si configura e si gestisce tramite vSphere Web Client o vSphere Client: il primo si può utilizzare solo se l'host fa parte di un'infrastruttura vSphere ed è presente nell'inventario del vCenter Server; il secondo è utilizzabile per il collegamento diretto all'host, senza transitare per il vCenter Server. Esiste poi la possibilità di configurare l'host a basso livello, in modo diretto e senza strumenti client, tramite l'interfaccia console. Di seguito una descrizione degli strumenti di configurazione indicati.

3.4.1 L'interfaccia console: DCUI

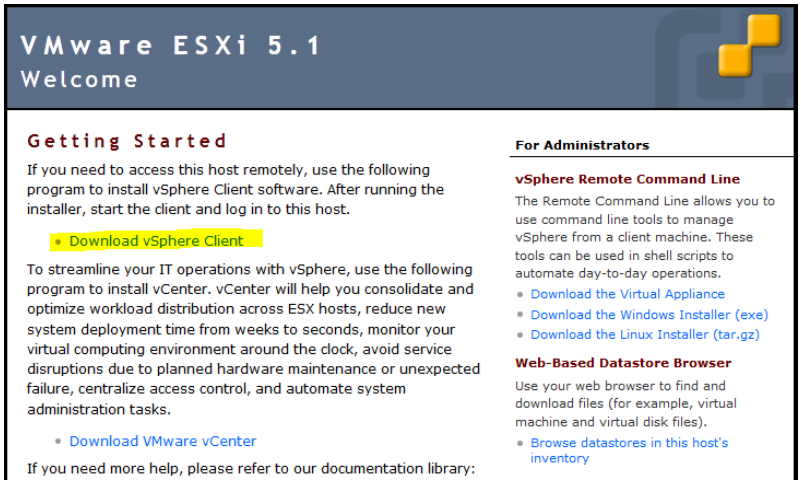
Al termine della procedura di boot, l'host ESXi si presenta con la schermata mostrata qui sotto.



Si tratta della **Direct Console User Interface** (**DCUI**), un'interfaccia di configurazione a basso livello che permette di configurare alcune impostazioni base di ESXi. Premendo il tasto F2 si entra nella sezione di configurazione, dove si possono impostare la password di amministrazione dell'utente root e i parametri di rete. La voce **Reset System Configuration** rende possibile il reset della configurazione. Dal menu "Troubleshooting Options" è possibile abilitare l'accesso in SSH.

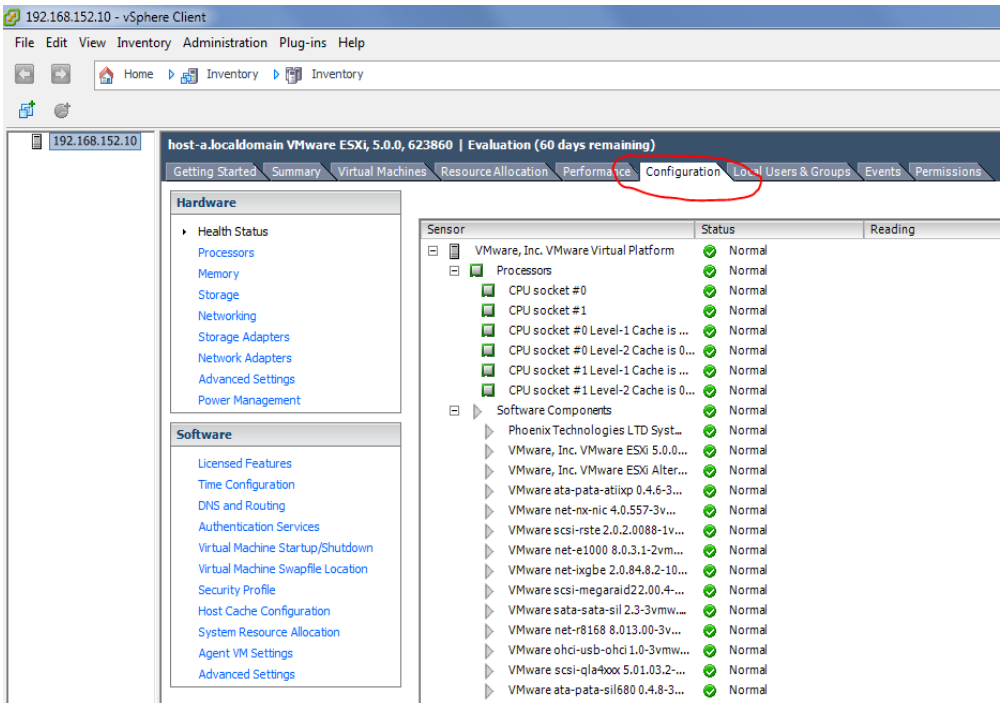
3.4.2 L'interfaccia grafica: vSphere Client

vSphere Client è un'interfaccia di gestione utilizzabile per l'accesso diretto agli host ESXi. È inoltre una delle possibili interfacce di gestione dell'intero sistema VMware vSphere, rimpiazzata dalla versione Web a partire da vSphere 5.1. È disponibile solo per sistemi operativi Windows. Si scarica accedendo alla pagina web dell'host ESXi.



Una volta che l'applicazione è stata installata, al suo avvio apparirà la finestra di login, dove si inseriscono il nome o l'indirizzo IP dell'host ESXi, quindi le credenziali di accesso.

Una volta effettuato il login, vSphere Client mostra l'host ESXi nel pannello a sinistra, e una serie di tab nel pannello a destra. Il tab più importante è il tab **Configuration**, da cui si accede alle voci di configurazione.



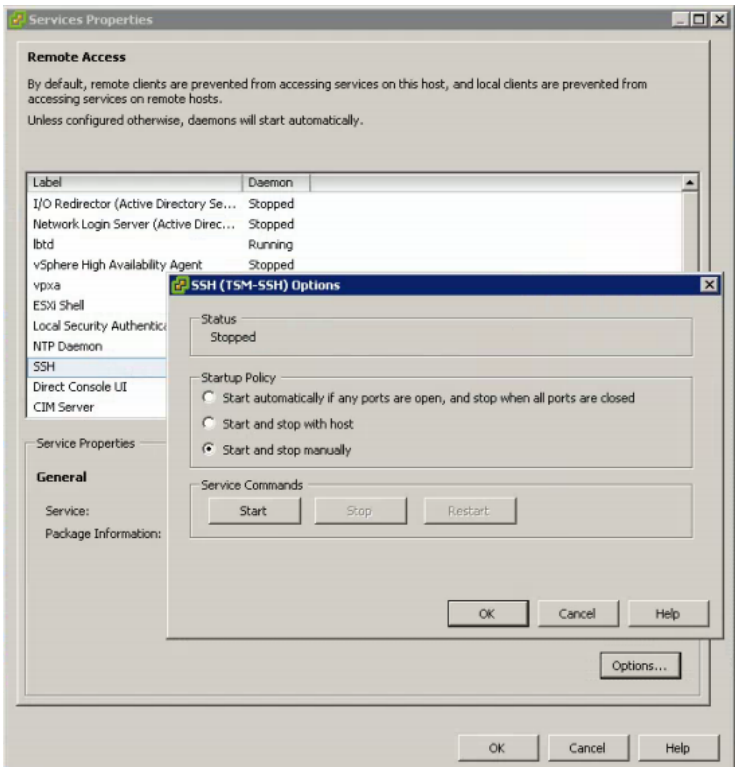
3.4.3 Configurazione del routing e dei parametri DNS

In maniera predefinita, sia i parametri DNS che il default gateway si ottengono automaticamente, tramite DHCP, ma è comunque possibile impostarli manualmente. In quest'ultimo caso, andare sul tab **Configuration** e scegliere la voce **DNS and Routing**. È possibile aggiungere e rimuovere le rotte anche da console, con il comando **vicfg-route**. Tuttavia è possibile specificare un solo gateway per tutti i port group.

3.4.4 Configurazione dei servizi

Per la configurazione dei servizi di ESXi tramite vSphere Client, andare sul tab **Configuration** relativo all'host che si desidera configurare, quindi fare clic sulla voce **Security Profile** nel menu a

sinistra. Nella finestra a destra, fare clic su **Properties** (sezione Services). Il comportamento di un servizio si imposta selezionando la sua voce nella finestra delle proprietà e facendo clic su **Options**. Nella finestra di dialogo riguardante quel servizio, è possibile impostare la politica di avvio oppure eseguire operazioni manuali quali l'avvio, lo stop o il riavvio del servizio stesso.



3.4.5 Configurazione dell'hyperthreading

Per sfruttare l'hyperthreading, la tecnologia deve essere abilitata prima di tutto sul BIOS della macchina host, poi si potrà attivarla tramite vSphere Client (Configuration tab / Processors / Properties). A livello di configurazione di ESXi, l'hyperthreading è abilitato di default.

3.4.6 Backup e ripristino della configurazione di ESXi

Il backup della configurazione di ESXi si esegue tramite **vSphere CLI** (Command Line Interface), con il comando **vicfg-cfgbackup**. Si consiglia un backup della configurazione dopo ogni modifica di rilievo, o dopo un upgrade di ESXi. Il backup include anche il serial number dell'host; in caso di ripristino della configurazione, anche il seriale viene ripristinato.

La sintassi del comando è la seguente:
vicfg-cfgbackup –server <nome_host> -username <utente> -password <password> -s <file_di_backup>

Esempio:
vicfg-cfgbackup.pl -server host1 -username root -password $ecret1 -s d:\host1cfg.bak

Il ripristino può essere portato a termine solo con le VM spente, e si esegue con lo stesso comando, utilizzando l'opzione *-load <file_di_backup>*.

Esempio:
vicfg-cfgbackup.pl -server host1 -username root -password $ecret1 -load d:\host1cfg.bak

Per riportare l'host alla configurazione di default (reset), si usa l'opzione *–r*. Esempio:
vicfg-cfgbackup.pl -server host1 -username root -password $ecret1 -r

3.5 Sicurezza di ESXi

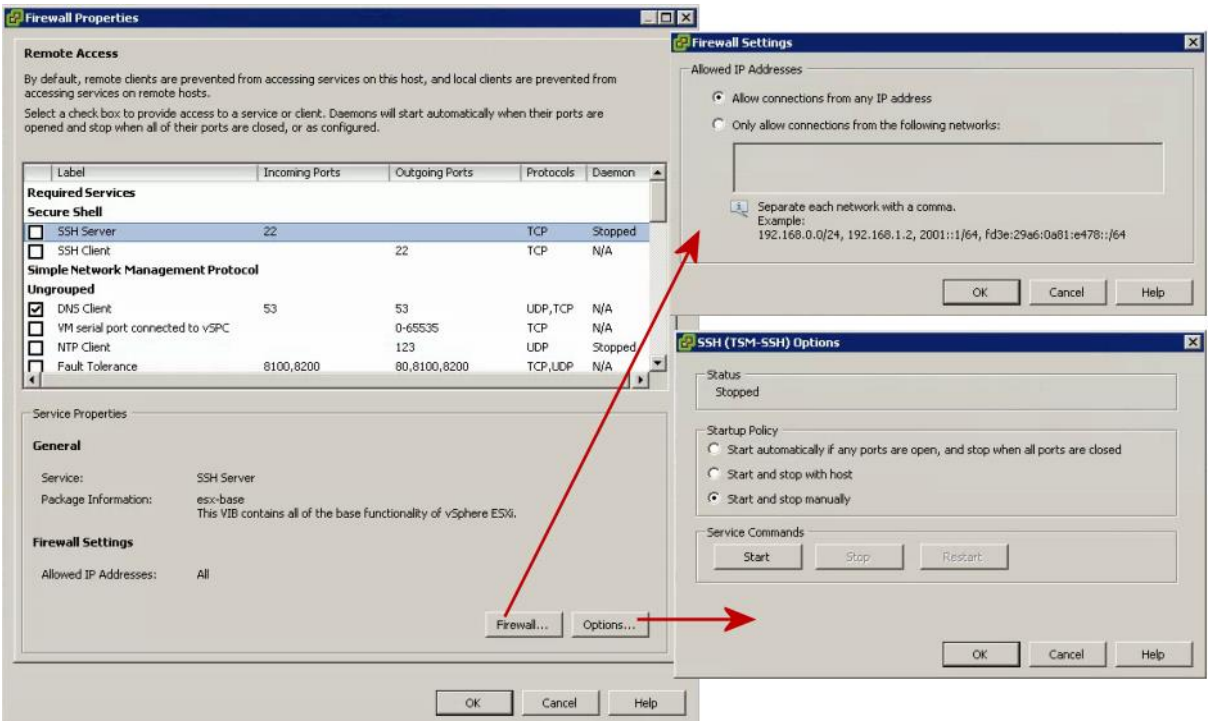
Il VMkernel alla base di ESXi è stato progettato per essere interamente dedicato al supporto delle macchine virtuali, pertanto il suo interfacciamento con l'ambiente esterno è strettamente limitato alle API richieste per la gestione delle macchine virtuali. L'architettura di ESXi prevede inoltre diverse funzionalità per la protezione del VMkernel.

- **Memory Hardening** – il kernel, le applicazioni, e tutti gli elementi eseguibili quali driver e librerie, vengono caricati su indirizzi di memoria casuali e non prevedibili. In questo modo diventa molto difficile l'esecuzione di exploit della memoria da parte di codice dannoso. Questa funzionalità si affianca alle funzioni hardware No eXecute (**NX**) e eXecute Disable (**XD**) presenti rispettivamente nei processori AMD e Intel, che marcano le pagine di memoria come "data-only" per evitare l'esecuzione di codice dannoso o attacchi di buffer overflow.
- **Kernel Module Integrity** – prevede la firma digitale su moduli, applicazioni e driver caricati dal VMkernel, in modo da assicurarne integrità e autenticità.
- **Trusted Platform Module** (**TPM**) – è un elemento hardware che certifica i processi di avvio, e permette la memorizzazione sicura delle chiavi di crittografia e di protezione. TPM deve essere abilitato sul BIOS delle macchine host che supportano questa funzionalità.

3.5.1 Il firewall integrato

L'interfaccia di gestione degli host ESXi è protetta da un firewall di tipo stateless. È dedicato alla protezione dei servizi che girano internamente agli host, e chiude qualsiasi accesso eccetto quelli esplicitamente autorizzati da un amministratore. Può essere configurato sia tramite vSphere Client sia da command line, direttamente dalla shell di ESXi.

Per configurarlo tramite vSphere Client, andare sul tab **Configuration** dell'host che si desidera configurare, quindi fare clic sulla voce **Security Profile** nel menu a sinistra. Nella finestra a destra, fare clic su **Properties** (sezione firewall).
L'accesso a un servizio si imposta selezionando la relativa voce nella finestra delle proprietà e facendo clic su **Firewall** e/o su **Options**. Nella finestra di dialogo **Firewall**, è possibile specificare da quali reti sia possibile accedere al servizio. Nella finestra di dialogo **Options**, è possibile impostare la politica di avvio oppure eseguire operazioni manuali quali l'avvio, lo stop o il riavvio del servizio stesso.



3.5.2 La modalità Lockdown

È una funzione che inibisce l'accesso diretto all'host ESXi. Con il **Lockdown Mode** abilitato, qualsiasi modifica sull'host deve essere eseguita tramite vCenter Server. Tuttavia, anche con il **Lockdown Mode** abilitato, l'utente root potrà sempre accedere alla console (DCUI) dell'host. Per configurare la modalità Lockdown, tramite vSphere Client, andare sul tab **Configuration**, quindi fare clic sulla voce **Security Profile** nel menu a sinistra. Nella finestra a destra, fare clic su **Edit** (sezione Lockdown Mode) e spuntare la casella **Enable Lockdown mode**. La modalità Lockdown è disponibile solo per gli host ESXi inseriti nell'inventario di un vCenter Server.

3.5.3 Integrazione con Microsoft Active Directory

Esistono due modi per utilizzare l'autenticazione Active Directory negli host ESXi.

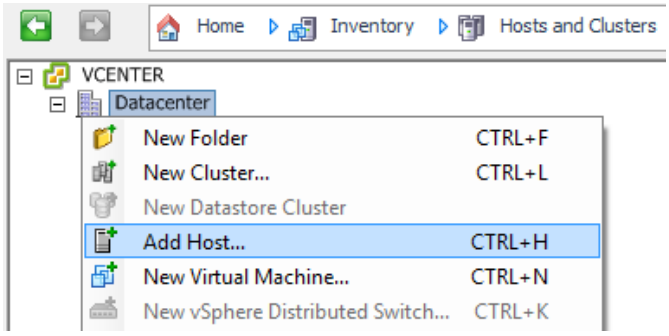
- Aggiungere l'host come membro di un dominio Active Directory (come in ESXi 4.1).
- Utilizzare la nuova funzione vSphere Authentication Proxy service (CAM service).

3.6 Inserimento di un host ESXi nell'inventario del vCenter Server

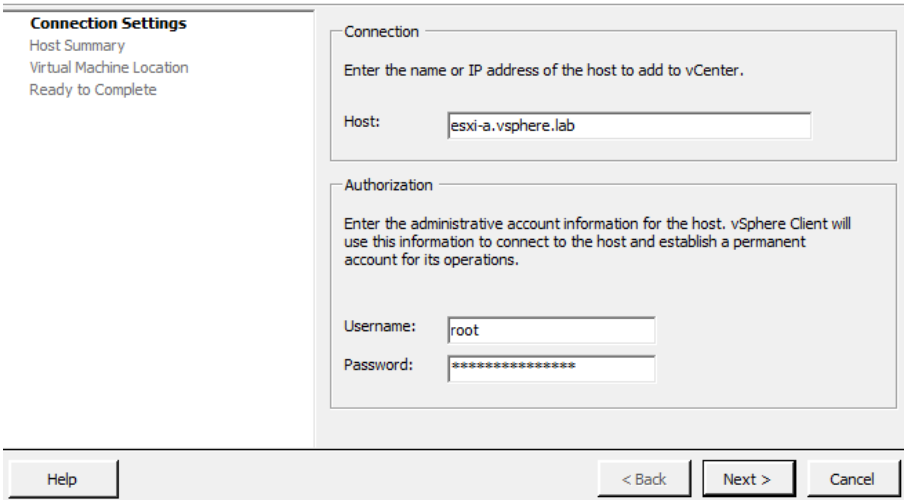
La procedura d'inserimento di un host ESXi nell'inventario del vCenter Server è successiva all'installazione del vCenter Server stesso. Un host può essere inserito all'interno di un datacenter, di una cartella, o di un cluster. Se l'host contiene macchine virtuali, anche queste saranno inserite nell'inventario.

Procedura con vSphere Client

- Eseguire l'accesso al vCenter Server.
- Nell'inventario a sinistra, selezionare un datacenter, un cluster, o una cartella.
- Per creare un nuovo datacenter è sufficiente fare clic con il tasto destro sul nome del vCenter Server e selezionare la voce **New Datacenter**.
- Dal menu file, selezionare le voci **New > Add Host**. In alternativa, fare clic con il tasto destro sul datacenter appena creato e selezionare la voce **Add Host**.



- Inserire il nome o l'indirizzo IP dell'host, insieme alle sue credenziali di accesso, e andare avanti.



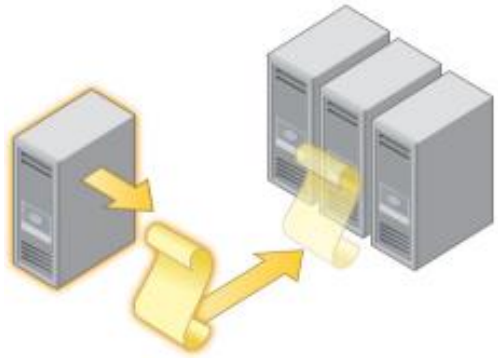
- Scegliere se abilitare la modalità Lockdown per disabilitare l'accesso diretto per l'account administrator. In questo modo il vCenter Server avrà accesso esclusivo all'host.
- Verificare il riepilogo delle informazioni e andare avanti.
- Assegnare una chiave di licenza e andare avanti.
- Sono ora possibili due azioni: se si sta aggiungendo un host a un cluster, selezionare un resource pool e andare avanti. Diversamente, selezionare una posizione in cui saranno sistemate le macchine virtuali esistenti sull'host e andare avanti.
- Fare clic su **Finish** per terminare la procedura.

Procedura con vSphere Web Client

- Eseguire l'accesso al vCenter Server, all'indirizzo https://vCenter_hostname_or_IP:9443/vsphere-client.
- Nell'inventario a sinistra, selezionare un datacenter, un cluster, o una cartella.
- Fare clic con il tasto destro su un datacenter, cluster o cartella e selezionare la voce **Add Host**.
- Inserire il nome host o l'indirizzo IP e andare avanti.
- Inserire le credenziali e andare avanti.
- Assegnare una chiave di licenza e andare avanti.
- Scegliere se abilitare la modalità Lockdown per disabilitare l'accesso diretto per l'account administrator. In questo modo il vCenter Server avrà accesso esclusivo all'host.
- Se si sta aggiungendo l'host a un datacenter o una cartella, selezionare una posizione in cui saranno sistemate le macchine virtuali esistenti sull'host e andare avanti.
- Fare clic su **Finish** per terminare la procedura.

Capitolo 4
I profili host

I profili host (**host profiles**) permettono di incapsulare la configurazione di uno specifico host all'interno di un template, per utilizzarla e gestirla in ambienti con più host o cluster. Consentono di eliminare le procedure manuali di creazione e gestione delle configurazioni, semplificandone la distribuzione. Con i profili host si acquisisce lo schema progettuale di una configurazione nota e convalidata, completa di impostazioni di rete, storage e sicurezza, e si estende questo schema a più host, con la conseguenza di poter mantenere in modo semplificato la consistenza delle configurazioni nell'intero datacenter.



Un profilo host viene assegnato a un reference host, di norma corrispondente all'host con cui è stato generato il profilo. Il reference host agisce da modello o "master configuration". Appena creato, un profilo host può essere collegato a uno o più host. Collegato il profilo, la sua configurazione sarà utilizzata come termine di confronto con l'host di destinazione, ed ogni differenza sarà resa evidente. Se un host non è conforme al profilo host, potrà essere reso tale con l'applicazione del profilo stesso. Similmente, se si aggiunge un nuovo host all'inventario del vCenter Server, l'host potrà essere configurato velocemente tramite l'applicazione del profilo.

4.1 Uso dei profili host

4.1.1 Flusso di lavoro consigliato

a) Impostare e configurare l'host da impiegare come reference host.
b) Creare il profilo host tramite il reference host.
c) Collegare il profilo a un host o a un cluster.
d) Verificare la conformità dell'host con il profilo associato. Se l'host è conforme, vuol dire che è configurato correttamente.
e) Applicare il profilo.

Di seguito i dettagli dei vari punti indicati.

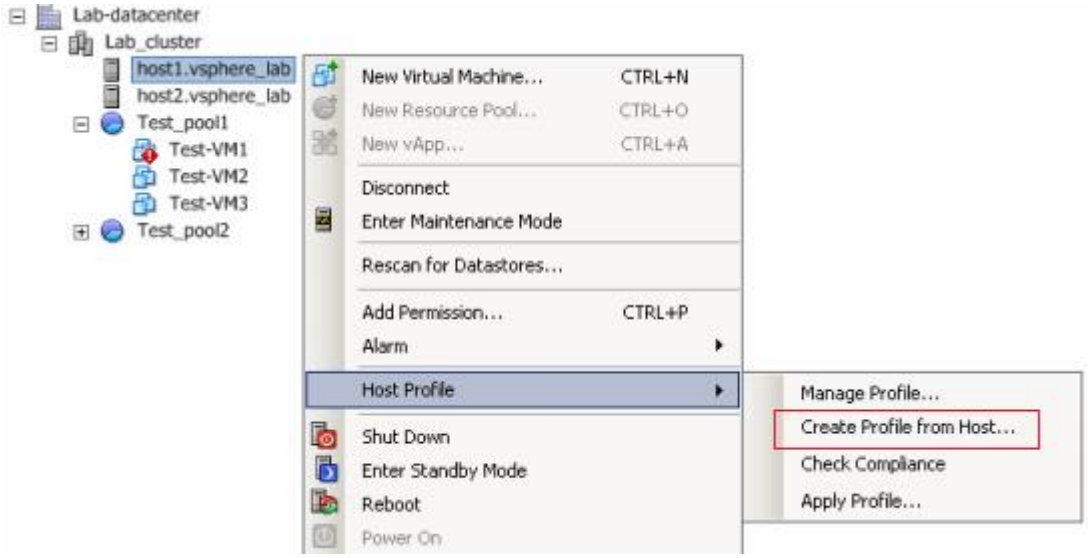
4.1.2 Creazione di un profilo host

Procedura tramite vSphere Client

Si può creare un profilo dal menu contestuale di un host, oppure dalla finestra principale di gestione profili, raggiungibile dal percorso **View** > **Management** > **Host Profiles**.

La procedura tramite menu contestuale prevede i passi indicati di seguito.

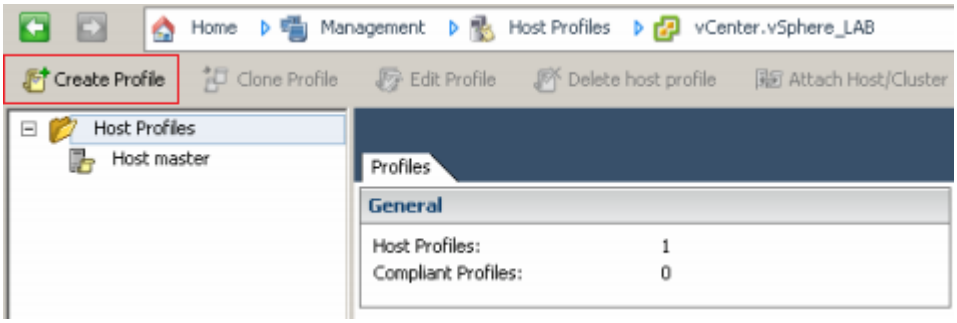
- Selezionare l'host da designare quale host di riferimento (**reference host**).
- Fare clic con il tasto destro sull'host e selezionare le voci **Host Profile** > **Create Profile from Host**.



- Si aprirà la finestra di procedura guidata per la creazione del nuovo profilo. Inserire un nome ed una descrizione per il profilo, quindi fare clic su **Next**.
- Verificare il riepilogo delle informazioni e fare clic su **Finish**.

La procedura tramite la pagina di gestione profili è la seguente.

1. Andare su **Home** > **Management** > **Host Profiles** e fare clic sul bottone **Create Profile**.



2. Si aprirà la finestra di procedura guidata per la creazione del nuovo profilo. Selezionare l'opzione per creare un profilo a partire da un host esistente e fare clic su **Next**.
3. Selezionare l'host da designare quale host di riferimento (**reference host**), quindi fare clic su **Next**.
4. Inserire un nome ed una descrizione per il profilo, quindi fare clic su **Next**.
5. Verificare il riepilogo delle informazioni e fare clic su **Finish**.

Dalla finestra principale di gestione profili è possibile cambiare in ogni momento il reference host: si fa clic con il tasto destro sul profilo, si seleziona la voce **Change Reference Host** e si seleziona il nuovo host dalla lista. Inoltre, nel caso in cui la configurazione del reference host dovesse subire modifiche, è possibile includere le stesse nel profilo esistente, facendo clic con il tasto destro su quest'ultimo e selezionando la voce **Update Profile From Reference Host**.

Procedura tramite vSphere Web Client

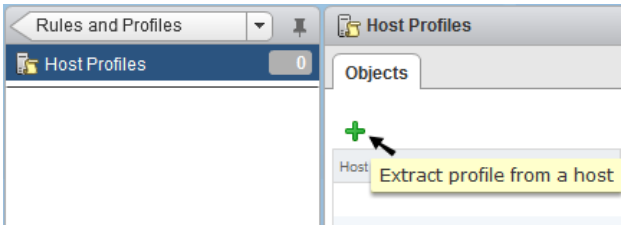
Si può creare un profilo dal menu contestuale di un host, oppure dalla finestra principale di gestione profili.

La procedura tramite menu contestuale prevede i passi indicati di seguito.

1. Selezionare l'host da designare quale host di riferimento (**reference host**).
2. Fare clic con il tasto destro sull'host e selezionare le voci **All vCenter Actions** > **Host Profiles** > **Extract Host Profile**.
3. Si aprirà la finestra di procedura guidata per la creazione del nuovo profilo. Inserire un nome ed una descrizione per il profilo, quindi fare clic su **Next**.
4. Verificare il riepilogo delle informazioni e fare clic su **Finish**.

La procedura tramite la pagina di gestione profili è la seguente.

1. Dalla pagina **Home**, andare su **Rules and Profiles** > **Host Profiles** e fare clic su **Extract profile from a host** ("**+**").



2. Si aprirà la finestra di procedura guidata per la creazione del nuovo profilo. Selezionare l'host di riferimento (**reference host**), quindi fare clic su **Next**.
3. Inserire un nome ed una descrizione per il profilo, quindi fare clic su **Next**.
4. Verificare il riepilogo delle informazioni e fare clic su **Finish**.

4.2 Gestione dei profili host

4.2.1 Importazione ed esportazione di un profilo

I profili host possono essere importati ed esportati tramite vSphere Client. L'esportazione prevede la generazione di un file con estensione **vpf** (**VMware profile format**). Il file non incorpora alcuna password, come misura di sicurezza.

Procedura per l'esportazione di un profilo.

1. Nella finestra principale di gestione profili, selezionare il profilo da esportare.
2. Fare clic con il tasto destro sul profilo e selezionare la voce **Export Profile**.
3. Specificare la posizione di salvataggio ed un nome per il profilo, quindi fare clic su **Save**.

Procedura per l'importazione di un profilo.

1. Nella finestra principale di gestione profili, fare clic sul bottone **Create Profile**.
2. Si aprirà la finestra di procedura guidata per la creazione di un nuovo profilo. Selezionare l'opzione per importare un profilo e fare clic su **Next**.
3. Individuare il file da importare e fare clic su **Next**.

4.2.2 Clonazione di un profilo

Procedura con vSphere Client

1. Nella finestra di gestione profili, selezionare il profilo da clonare.
2. Fare clic sul bottone **Clone Profile**.
3. Il profilo clonato comparirà nella lista dei profili.

Procedura con vSphere Web Client

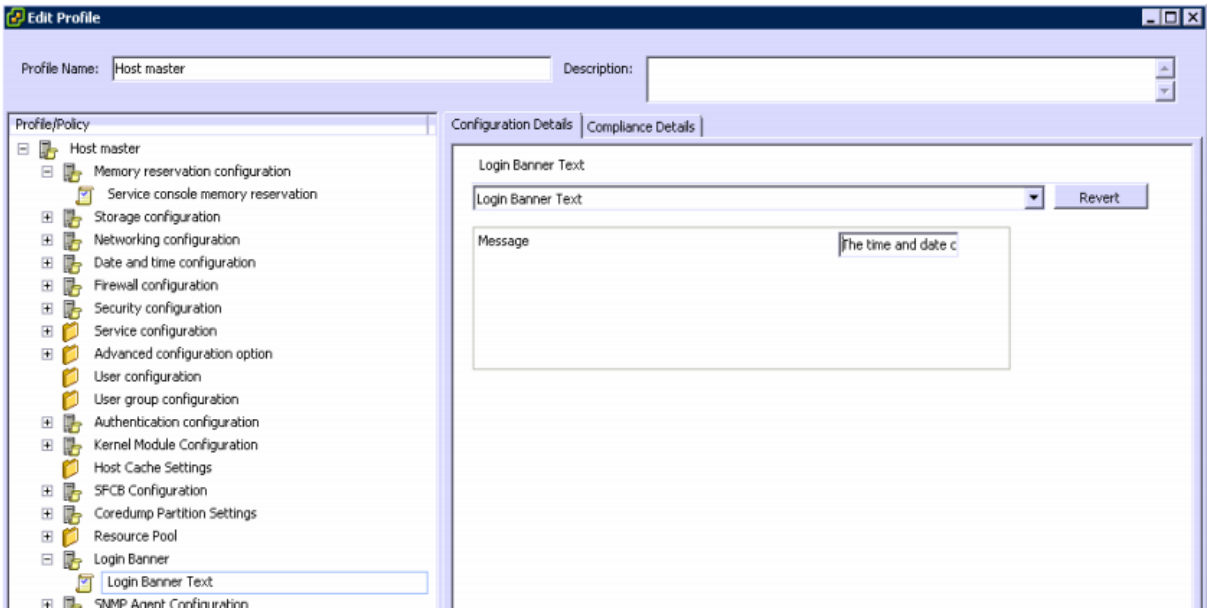
1. Nella finestra di gestione profili, fare clic con il tasto destro sul profilo da clonare e selezionare la voce **Duplicate Host Profile**.
2. Inserire un nome ed una descrizione per il profilo, quindi fare clic su **Next**.
3. Verificare il riepilogo delle informazioni e fare clic su **Finish**.

4.2.3 Modifica di un profilo e delle sue policy

Un profilo host è formato da diverse policy, che rappresentano configurazioni relative a specifici aspetti di un host. Nella schermata di modifica di un profilo, si può vedere come questo sia composto da ulteriori sotto-profili, ognuno con le proprie policy. Le policy possono essere modificate, ed è possibile verificare la conformità (compliance) delle stesse.

Procedura con vSphere Client

Dalla finestra di gestione profili, fare clic con il tasto destro sul profilo da modificare e selezionare la voce **Edit Host Profile**. Qui sotto una schermata di esempio. I principali sotto-profili sono indicati nell'elenco successivo.

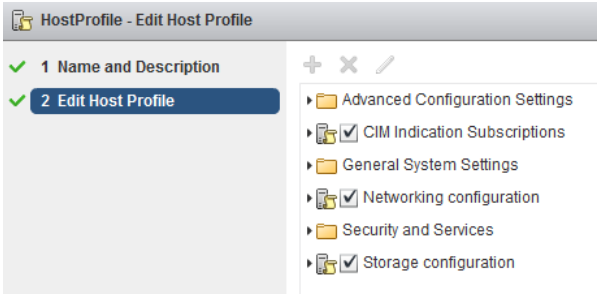


- **Storage** - include le opzioni di configurazione riguardanti le interfacce FCoE and iSCSI, incluse le funzioni di Native Multi-Pathing (NMP), Pluggable Storage Architecture (PSA) e storage NFS.
- **Networking** - include tutte le opzioni di configurazione relative a virtual switch standard e distribuiti, port group, velocità delle interfacce fisiche di rete, impostazioni di sicurezza, politiche del NIC teaming.
- **Date and Time** - impostazioni su data e ora.

- **Firewall** - consente di abilitare o disabilitare i set di regole relative al firewall integrato in ESXi.
- **Security** - permette di aggiungere utenti e gruppi e di impostare la password di root.

Procedura con vSphere Web Client

Dalla finestra di gestione profili, fare clic con il tasto destro sul profilo da modificare e selezionare la voce **Edit Host Profile**. Nella finestra di modifica, andare su **Edit Host Profile** per accedere alle impostazioni del profilo. Qui sotto una schermata di esempio.

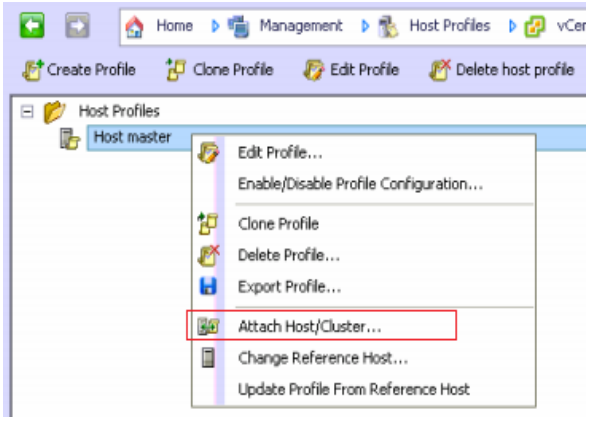


4.3 Collegamento e applicazione dei profili

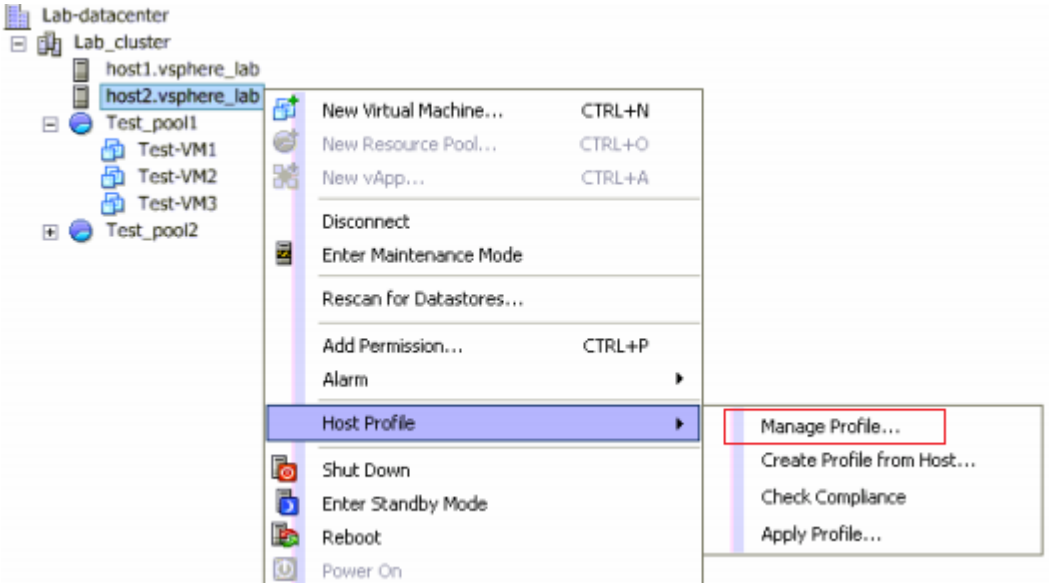
Un profilo deve essere prima collegato ad un host o ad un cluster, e poi applicato per rendere attiva la sua configurazione. Tecnicamente, un profilo collegato è detto **attached**. Nel caso di un cluster, tutti gli host saranno configurati in accordo con il profilo collegato al cluster, questo per garantire la conformità delle configurazioni.

Procedura con vSphere Client

- Dalla finestra di gestione profili, fare clic con il tasto destro sul profilo del reference host e selezionare la voce **Attach Host/Cluster**.

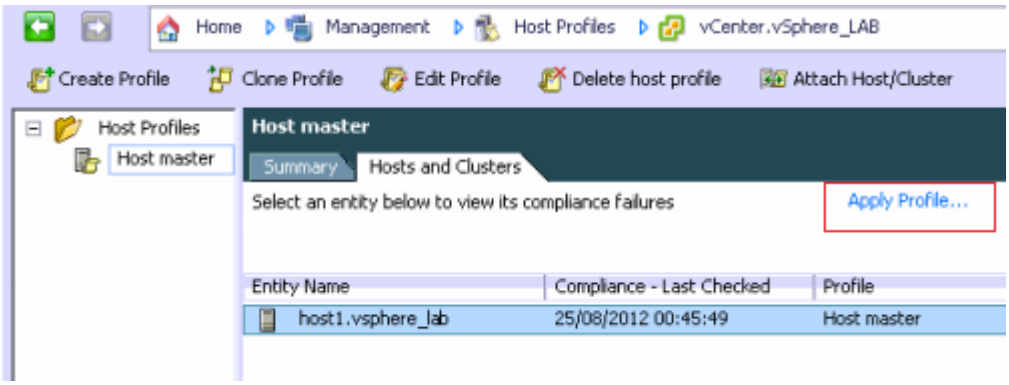


- Selezionare l'host o il cluster da collegare al profilo.
- In alternativa, è possibile collegare un profilo direttamente dal menu contestuale di un host o di un cluster, selezionando le voci **Host Profile** > **Manage Profile**.



Per applicare il profilo ad un host, quest'ultimo deve essere impostato in **Maintenance Mode**. A quel punto è possibile:

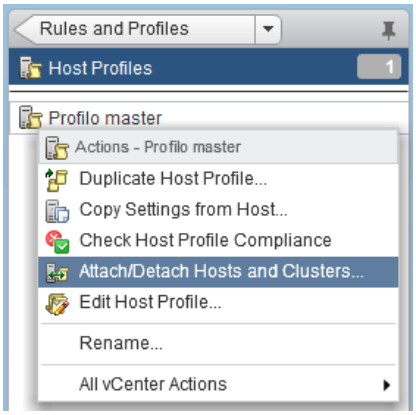
- selezionare il profilo desiderato dalla finestra di gestione profili;
- individuare l'host sul tab **Hosts and Clusters**;
- fare clic sulla voce **Apply Profile**.



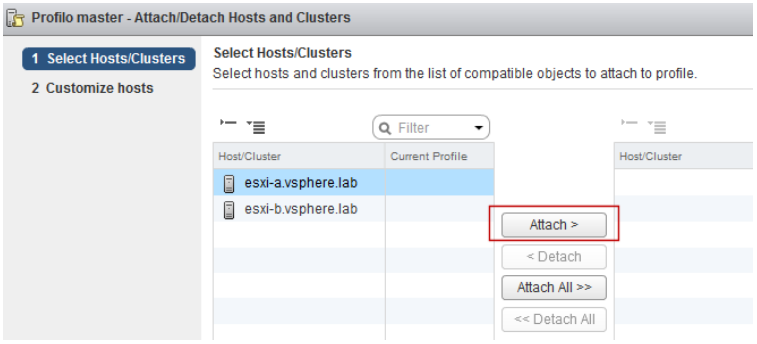
In alternativa è possibile applicare un profilo direttamente dal menu contestuale dell'host, selezionando le voci **Host Profile** > **Apply Profile**.

Procedura con vSphere Web Client

- Dalla finestra di gestione profili, fare clic con il tasto destro sul profilo del reference host e selezionare la voce **Attach/Detach Hosts and Clusters**.



- Selezionare l'host o il cluster da collegare al profilo e fare clic su **Attach**. Contestualmente, nella schermata successiva, sarà possibile personalizzare la configurazione dell'host.



- In alternativa, è possibile collegare un profilo direttamente dal menu contestuale di un host o di un cluster, selezionando le voci **All vCenter Actions** > **Host Profiles** > **Extract Host Profile**.

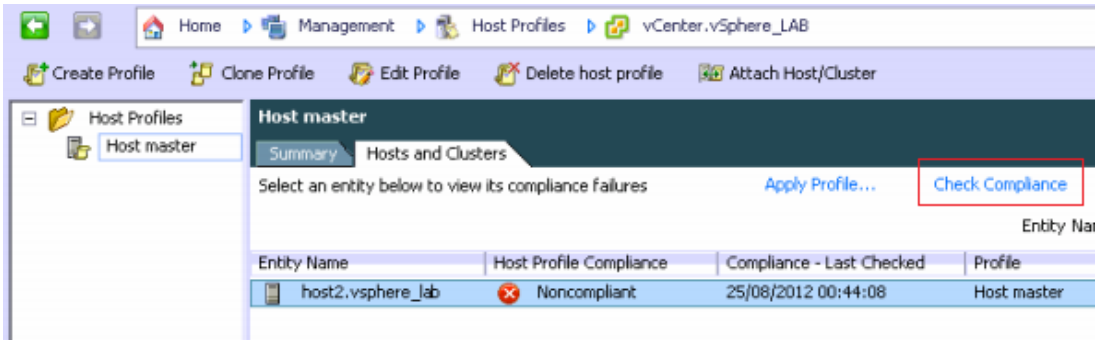
4.4 Verifica della conformità

La verifica della conformità (**compliance**) di un host o di un cluster, rispetto ad un profilo collegato, assicura la correttezza delle configurazioni. Modifiche manuali, successive all'applicazione del profilo, possono infatti rendere difformi i vari host dal reference host.

La verifica di conformità può restituire i valori seguenti: **Compliant**, **Unknown**, **Non-compliant**. In caso di non conformità, si può applicare il profilo all'host non conforme. Per quanto riguarda i cluster, la verifica di conformità valuta impostazioni specifiche quali DRS, HA, DPM, Fault Tolerance, senza però verificare gli host.

Procedura con vSphere Client

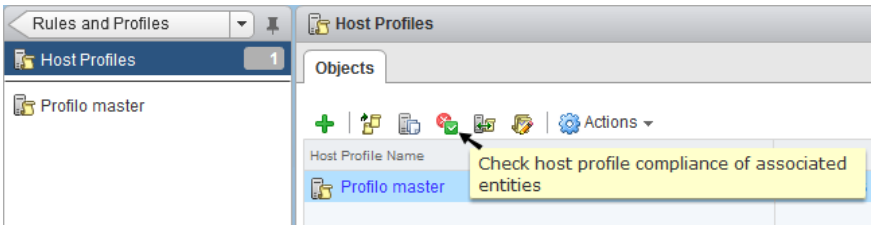
- Andare nella finestra principale di gestione profili, su **Home** > **Management** > **Host Profiles**.
- Selezionare il profilo desiderato e fare clic sul tab **Hosts and Clusters**.
- Selezionare l'host o il cluster di cui si vuole verificare la conformità e fare clic sulla voce **Check Compliance**.



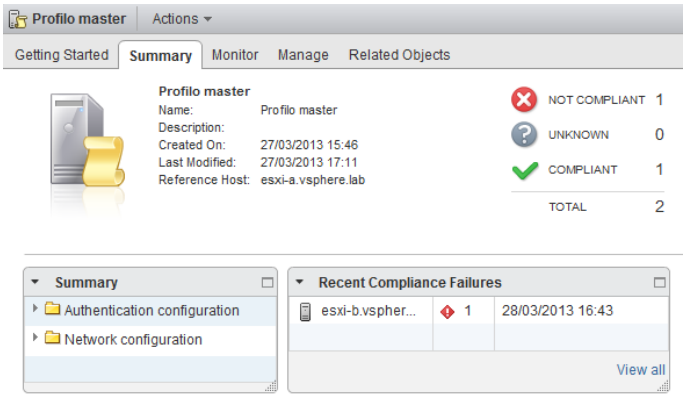
- In alternativa, è possibile procedere alla verifica direttamente dal menu contestuale di un host, selezionando le voci **Host Profile > Check Compliance**.

Procedura con vSphere Web Client

- Andare nella finestra principale di gestione profili, su **Home > Rules and Profiles > Host Profiles**.
- Selezionare il profilo desiderato e fare clic sull'icona **Check Host Profile Compliance**.



- Fare doppio clic sul profilo host e verificare lo stato di conformità sul tab **Summary**.



Capitolo 5
Autenticazione e controllo accessi

Il sistema di controllo accessi dell'ambiente vSphere, centralizzato sul vCenter Server, prevede la possibilità di definire sino al dettaglio le operazioni eseguibili da ogni utente o gruppi di utenti, e gli oggetti sui quali tali operazioni possono essere eseguite.

Il sistema di controllo ruota attorno ai concetti descritti di seguito.

- **Privilege** - un privilegio abilita un utente a compiere una determinata azione.
- **Role** - un ruolo è un insieme di privilegi, e definisce le azioni che un utente è autorizzato a compiere. Un ruolo viene assegnato ad un utente o ad un gruppo, determinandone i livelli di accesso. Esistono tre ruoli predefiniti: **Administrator**, **Read-only**, **No Access**. Ovviamente possono essere creati ulteriori ruoli, personalizzabili e configurabili direttamente sugli host ESXi o sul vCenter Server. È importante evidenziare che i ruoli creati sul vCenter Server sono indipendenti dai ruoli che si possono creare nei singoli host. Infatti, se ci si collega direttamente ad un host ESXi, non saranno visibili i ruoli creati sul vCenter Server.
- **Object** - un oggetto è un'entità dell'ambiente vSphere su cui è possibile eseguire un'azione. Nella pratica, un amministratore seleziona un oggetto dall'inventario del vCenter Server, seleziona un ruolo che definisce i privilegi sull'oggetto, infine associa un utente o un gruppo a quel ruolo.
- **User/group** - semplicemente un utente o un gruppo di utenti. Un utente può essere creato nel vCenter Server o internamente ai singoli host ESXi. In alternativa, si può utilizzare Active Directory per gestire gli utenti dell'intero ambiente vSphere.

Anche in assenza di Active Directory, gli utenti possono essere definiti localmente nel vCenter, sia su macchina Windows che su appliance Linux. Nel primo caso, si utilizzeranno gli utenti e i gruppi locali della macchina Windows, nel secondo caso quelli del sistema Linux. Per la creazione di utenti sull'appliance Linux, dalla shell digitare i comandi:

useradd -m username
passwd username

Se il vCenter è unito ad un dominio Active Directory, tutti gli utenti e i gruppi del dominio saranno disponibili nell'ambiente virtuale, con alcuni importanti aspetti da segnalare:

- gli utenti con privilegi amministrativi sul server Windows (Local administrators) hanno poteri amministrativi anche sull'ambiente virtuale (vCenter e host ESXi);
- gli utenti inseriti all'interno del gruppo **ESX Admins** diventano amministratori all'interno dell'ambiente virtuale (vCenter e host ESXi).

5.1 Ruoli predefiniti

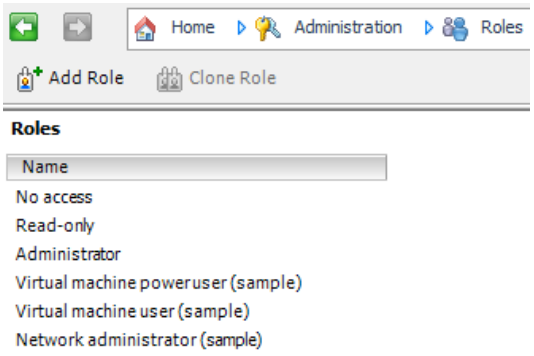
In maniera predefinita esistono i ruoli **No Access**, **Read-only** e **Administrator**. I ruoli predefiniti non possono essere modificati. Se si desidera creare un ruolo simile ad essi, è sufficiente clonare il ruolo desiderato ed apportare le necessarie modifiche.

- **No Access**: l'utente a cui si assegna il ruolo No Access per un oggetto, non ha alcun tipo di visibilità su quell'oggetto. Utilizzando vSphere Client, eventuali tab legati a quell'oggetto

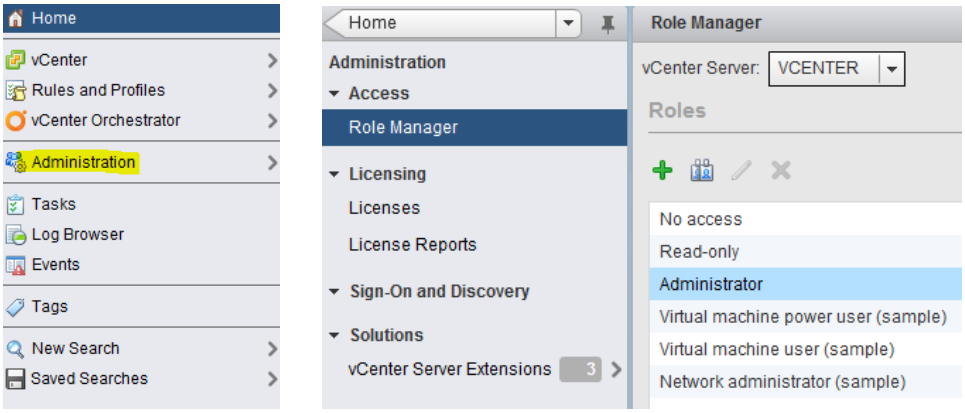
appariranno senza contenuto. L'utilizza tipico del ruolo No Access è quello di revocare permessi ad un oggetto figlio che altrimenti sarebbero propagati da un oggetto padre.

- **Read Only**: l'utente a cui si assegna il ruolo Read Only per un oggetto può vedere solo lo stato e i dettagli dell'oggetto stesso; qualsiasi altra azione viene negata.
- **Administrator**: l'utente a cui si assegna il ruolo di Administrator per un oggetto, ha tutti i privilegi possibili su quell'oggetto. All'interno di un host ESXi, il ruolo Administrator è assegnato automaticamente agli utenti **root** e **vpxuser**.

Con vSphere Client, la lista dei ruoli si visualizza collegandosi al vCenter Server e seguendo il percorso **Home > Administration > Roles.**



Per vedere la lista dei ruoli con vSphere Web Client, nella pagina iniziale fare clic su **Administration**, quindi fare clic su **Role Manager**.

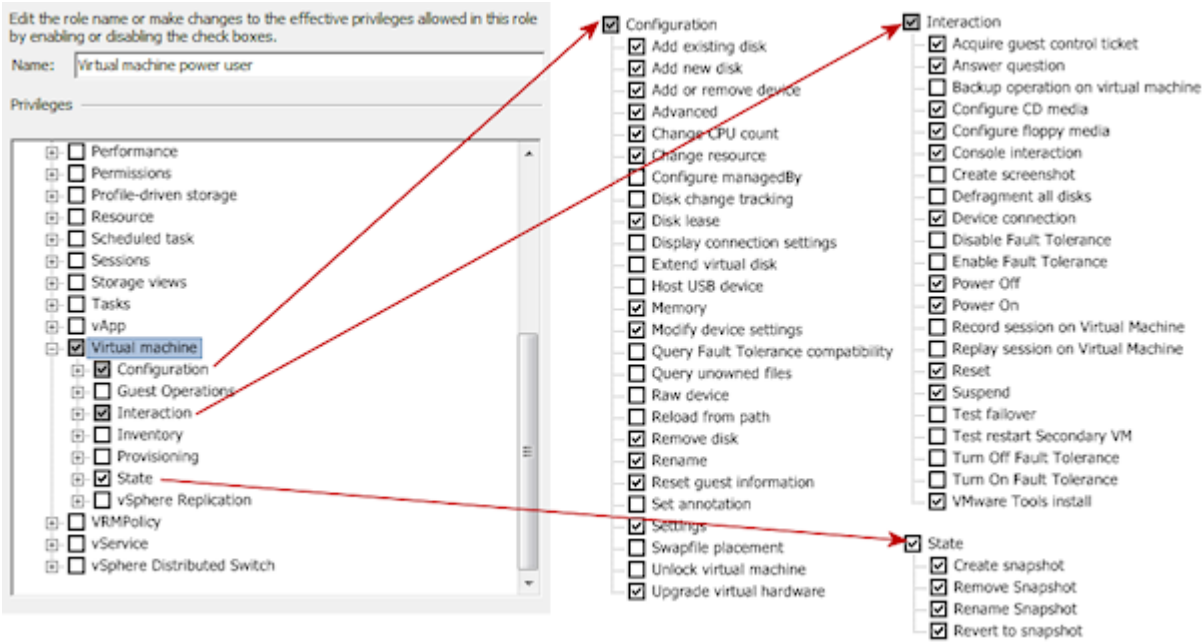


5.2 Creazione di un ruolo

Per creare un nuovo ruolo con vSphere Client, fare clic su **Add Role** nella pagina **Home > Administration > Roles**.

Per creare un nuovo ruolo con vSphere Web Client, dalla pagina **Role Manager** fare clic su **Create Role Action**.

Quando si crea un ruolo, è consigliato assegnare il minor numero possibile di privilegi, per una maggior sicurezza dell'ambiente virtuale. Inoltre, il nome del ruolo dovrebbe far riferimento alle attività permesse per quel ruolo. Ad esempio, supponiamo di dover creare un ruolo per gestire e configurare una macchina virtuale già esistente: chiameremo il ruolo con il nome di "Virtual machine power user" e assegneremo i privilegi mostrati nell'immagine sotto.

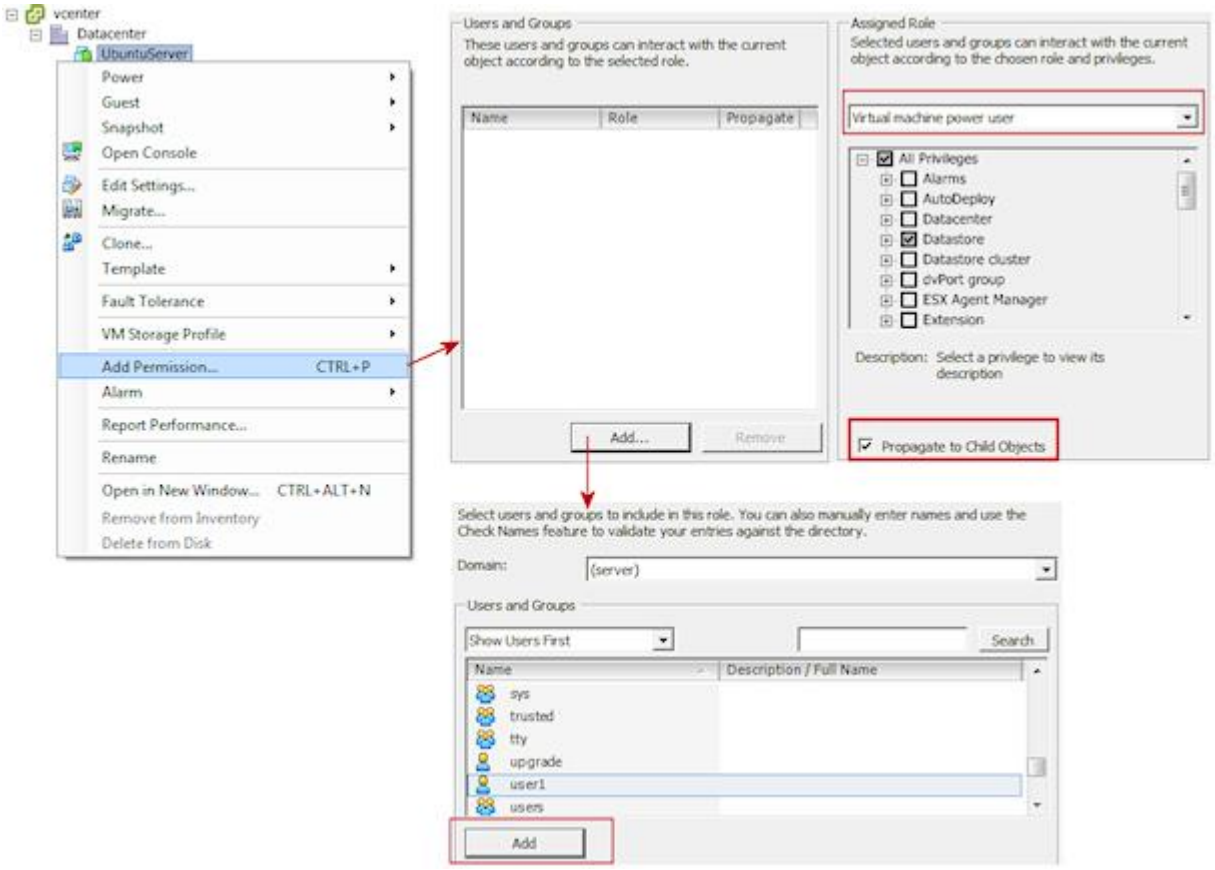


5.3 Assegnazione dei permessi

Una volta creato un ruolo, è possibile assegnarlo ad un utente. L'assegnazione è possibile per ogni oggetto presente nell'inventario del vCenter Server. Assegnare un ruolo significa assegnare una **Permission**.

Procedura con vSphere Client

- Fare clic con il tasto destro su un oggetto dell'inventario, ad esempio una macchina virtuale.
- Dal menu contestuale, selezionare la voce **Add Permission**; si aprirà la finestra **Assign Permissions**.
- A destra, sotto **Assigned Role**, selezionare il ruolo desiderato.
- Nella stessa finestra, fare clic su **Add** per aggiungere uno o più utenti/gruppi a cui assegnare il ruolo selezionato.
- Per estendere i permessi a tutti gli oggetti figlio, abilitare la voce **Propagate to Child Objects**.



Visualizzando la lista dei ruoli nel percorso **Home > Administration > Roles**, e selezionando il ruolo appena utilizzato, potremo osservare l'elenco degli oggetti sui quali è attivo quel ruolo.

Quando un permesso viene assegnato ad un oggetto, può essere esteso a tutti gli oggetti figlio lasciando abilitata la voce **Propagate to Child Objects**. Tuttavia, se per un oggetto figlio viene esplicitato un determinato permesso, questo prevale rispetto al permesso ereditato dall'oggetto padre. Ad esempio, se un utente ha il ruolo di amministrazione delle VM di un host, ma su una specifica VM ha privilegi di sola lettura, allora l'utente sarà in grado di gestire e modificare tutte le VM di quell'host, tranne quella per cui sono stati esplicitati privilegi di sola lettura.

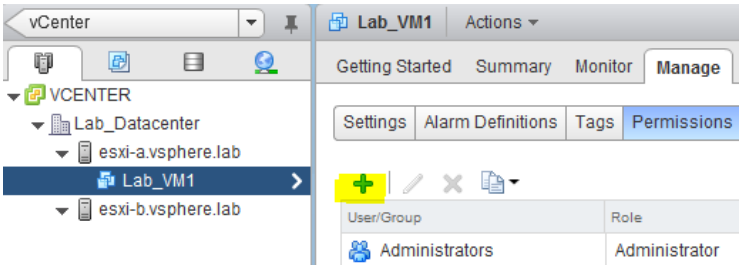
Se un utente fa parte di più gruppi, e questi gruppi sono utilizzati su uno stesso oggetto, a quell'utente saranno concessi i privilegi di tutti i gruppi ai quali appartiene. Vale sempre la regola per cui una permission esplicitata per un oggetto figlio prevale rispetto a quella assegnata all'oggetto padre; pertanto se l'utente appartiene al gruppo di amministratori che possono gestire tutte le VM di un host, ma anche ad un gruppo che ha privilegi di sola lettura su una specifica VM, allora quell'utente sarà in grado di gestire e modificare tutte le VM, escluso quella specifica su cui avrà privilegi di sola lettura.

Infine, se un permesso è stato esplicitato per un utente, prevale sui permessi di gruppo assegnati sullo stesso oggetto. Per intenderci, se l'utente appartiene al gruppo di amministratori che possono

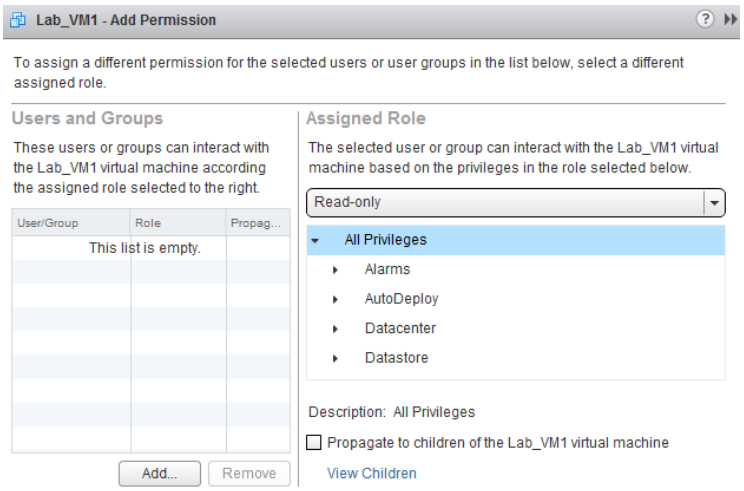
gestire tutte le VM di un host, ma a quell'utente si assegnano privilegi di sola lettura su una specifica VM, allora quell'utente sarà in grado di gestire e modificare tutte le VM, escluso quella specifica su cui avrà privilegi di sola lettura.

Procedura con vSphere Web Client

- Selezionare un oggetto dall'inventario, ad esempio una macchina virtuale.
- Fare clic sul tab **Manage** e selezionare la voce **Permissions**.
- Fare clic su **Add Permission**.



- A destra, sotto **Assigned Role**, selezionare il ruolo desiderato.



- Nella stessa finestra, fare clic su **Add** per aggiungere uno o più utenti/gruppi a cui assegnare il ruolo selezionato.
- Per estendere i permessi a tutti gli oggetti figlio, abilitare la voce **Propagate to Child Objects**.

5.4 Rimozione di un ruolo

Procedura con vSphere Client

- Andare in **Home > Administration > Roles**.
- Nella lista dei ruoli, fare clic con il tasto destro sul ruolo da rimuovere e selezionare la voce **Remove**.

Se si rimuove un ruolo assegnato ad un utente o ad un gruppo, si può scegliere se sostituirlo con un altro ruolo (**reassign affected user to**) oppure rimuovere l'assegnazione (**remove role assignments**). Quando si rimuove un ruolo non assegnato ad un utente o ad un gruppo, il ruolo è rimosso dalla lista dei ruoli.

Procedura con vSphere Web Client

- Dalla pagina **Home**, fare clic su **Administration**.
- Fare clic su **Role Manager**, selezionare il ruolo da eliminare e fare clic **Delete role action** (icona "X" rossa).

Capitolo 6
Virtual networking: concetti base

Uno degli aspetti più interessanti della virtualizzazione riguarda il networking. Il networking virtuale e gli switch virtuali permettono il collegamento in rete delle macchine virtuali, e consentono l'interfacciamento di queste alla rete fisica.

Gli switch virtuali consentono alle VM di comunicare in rete utilizzando gli stessi protocolli utilizzati negli switch fisici, senza la necessità di hardware di rete aggiuntivo; vi è inoltre pieno supporto alle VLAN (standard 802.1Q). Le stesse VM, così come PC o server fisici, sono dotate di una o più schede Ethernet, ognuna con proprio indirizzo IP e indirizzo MAC. Dal punto di vista della rete, le macchine virtuali hanno le stesse proprietà delle macchine fisiche. Gli switch virtuali possono poi essere collegati alla rete fisica semplicemente associandoli a una o più interfacce di rete disponibili nell'host ESXi.

Le basi del networking in VMware vSphere sono elencate di seguito.

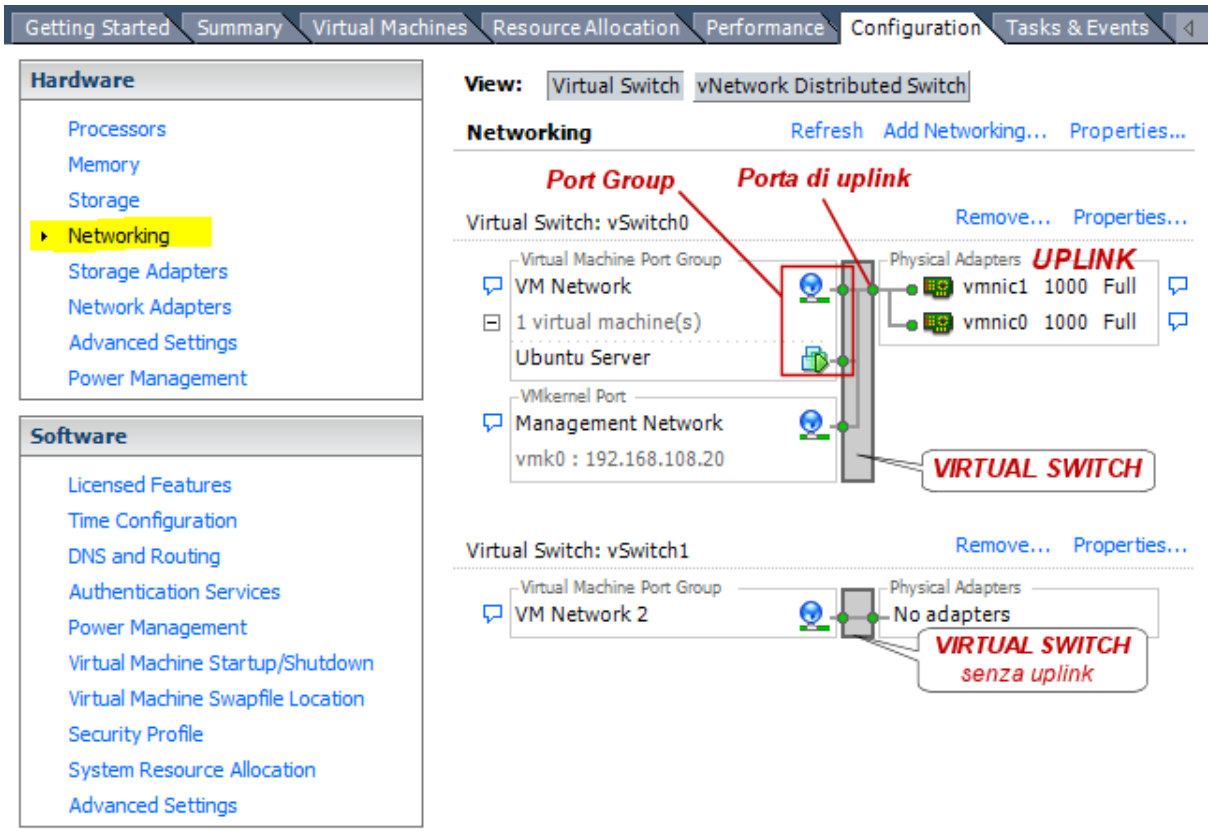
- Interfacce di rete virtuali, o **Virtual NIC**, utilizzate dalle singole macchine virtuali.
- Switch virtuali standard, tecnicamente chiamati **vSphere Standard Switch** (**VSS**), che collegano le macchine virtuali tra loro e con la rete fisica esterna, in quest'ultimo caso sfruttando le interfacce fisiche dell'host ESXi. Uno switch virtuale può collegarsi tramite porte di uplink (**uplink ports**) a una o più schede Ethernet fisiche, con la possibilità di fare NIC Teaming (cioè di aggregare più canali Ethernet).
- Gruppi di porte, o **Port Groups**, ossia insiemi di porte accomunate dalle stesse caratteristiche (all'interno di uno stesso vSwitch).
- Switch virtuali distribuiti, tecnicamente chiamati **vSphere Distributed Switch** (**VDS**), che permettono di operare come se si avesse un singolo switch centralizzato, utilizzato contemporaneamente da più host ESXi.

Uno switch virtuale, sia di tipo standard sia distribuito, funziona come uno switch Ethernet fisico, operando al livello due della pila ISO-OSI e mantenendo una tabella di MAC address (mac-address table) aggiornata ogni volta che il traffico attraversa lo switch. Tuttavia, a differenza degli switch fisici, quelli virtuali non richiedono alcuna fase di apprendimento degli indirizzi MAC per la compilazione della mac-address table, perché conoscono in maniera implicita quali sono i dispositivi collegati su ogni porta. Inoltre, gli switch virtuali non aggiornano la tabella d'inoltro con informazioni provenienti dalla rete fisica. Questo pone al riparo da attacchi di denial of service o tentativi di worm o virus che provano a scansionare gli host in rete, alla ricerca di vulnerabilità.

Switch virtuali differenti non possono condividere la stessa interfaccia fisica di un host: una volta che questa è assegnata a uno switch virtuale, non sarà più disponibile per gli altri. A differenza del mondo reale, in una rete virtuale non c'è possibilità di interconnettere più switch tra loro, ma si è obbligati a utilizzare una topologia di rete a livello singolo: il vantaggio è che non possono generarsi loop di rete, pertanto il protocollo Spanning Tree, non essendo necessario, non è previsto. Questa caratteristica è chiamata **Virtual Switch Isolation**.

Per la gestione del virtual networking ci si collega al vCenter Server tramite vSphere Client o vSphere Web Client. In alternativa, se si devono gestire switch standard, ci si può collegare in modo diretto agli host ESXi con vSphere Client. Indipendentemente dal tipo di client utilizzato, gli switch distribuiti possono essere gestito solo collegandosi al vCenter Server.

Qui sotto possiamo vedere una schermata esplicativa, relativa a un host ESXi. Gli elementi messi in evidenza saranno trattati nel dettaglio nei paragrafi che seguono.



6.1 Uplink e porte di uplink

Una **porta di uplink** è la porta di uno switch virtuale associata ad una o più interfacce fisiche di rete dell'host ESXi, e permette il collegamento della rete virtuale con quella fisica. Ognuna delle interfacce fisiche di rete dell'host ESXi è chiamata semplicemente **uplink**. È possibile configurare gli switch virtuali senza uplink: uno switch privo di uplink crea una **virtual intranet**. Si usa questa modalità quando lo switch virtuale deve fornire connessione a macchine virtuali protette da un firewall, anch'esso installato all'interno di una VM. In tal caso il firewall virtuale avrà più interfacce virtuali, una delle quali dovrà essere collegata allo switch privo di uplink. Chiaramente, per tutto il traffico interno alla rete virtuale, gli uplink non sono necessari.

6.2 Port Group

Costituiscono una funzionalità del virtual networking non presente nelle reti fisiche. Un **Port Group**, o gruppo di porte, può essere visto come un insieme di porte con caratteristiche comuni. In sostanza, un port group definisce tutte le caratteristiche di ogni porta che gli appartiene. Proprio per questo motivo, quando si desidera collegare una macchina virtuale ad una porta, è sufficiente specificare il nome del Port Group a cui collegarla.

Fra le caratteristiche che si possono definire a monte vi sono:

- nome del vSwitch di appartenenza;
- VLAN ID e politiche per il tagging e il filtraggio (è concesso che diversi gruppi di porte possano avere lo stesso VLAN ID);
- politica di Teaming (unione uplink, bilanciamento, ordine di failover, ecc.);

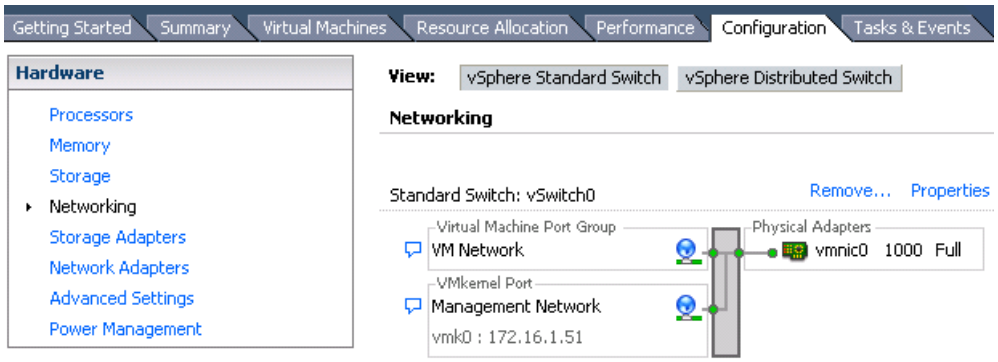
- opzioni di sicurezza;
- parametri di traffic shaping.

6.3 Tipologia delle connessioni

Un vSwitch permette essenzialmente due tipi di connessione.

- **VMkernel** - connessione ai servizi tramite le cosiddette **VMkernel ports**. I servizi gestibili con una porta VMkernel includono l'accesso allo storage IP (NFS e iSCSI), le migrazioni vMotion, le funzioni di Fault Tolerance, l'accesso alla rete di management.
- **Virtual Machine** - connessione per le macchine virtuali tramite port group.

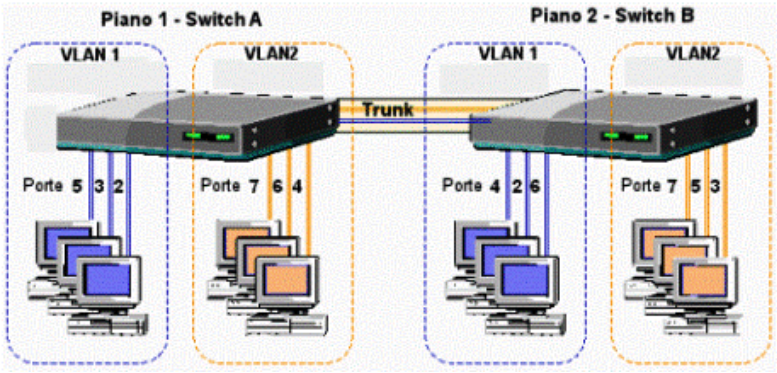
L'installazione di VMware ESXi su un host comporta la creazione di un vSwitch predefinito di tipo standard, dove all'interno troviamo un port group chiamato **VM Network** ed una porta VMkernel chiamata **Management Network**, utilizzata per la gestione dell'host ESXi.



È sempre buona pratica separare la rete delle macchine virtuali dalla rete di management, per ragioni di prestazioni ma soprattutto di sicurezza.

6.4 Uso delle VLAN

Per definizione, le VLAN rappresentano un metodo per segmentare un **dominio di broadcast** in più domini di dimensione ridotta. A livello 2, ogni VLAN contiene solo il traffico dei dispositivi appartenenti a quella VLAN.
Il termine dominio di broadcast si riferisce a quella parte di rete raggiunta dai pacchetti di broadcast, ossia quei pacchetti indirizzati a tutti i dispositivi di rete; pertanto fanno parte dello stesso dominio di broadcast tutti i nodi raggiunti da quel pacchetto (ad esempio pacchetti di richieste ARP o richieste di nomi NetBIOS). Il broadcast colpisce l'intera rete, poiché ciascun dispositivo appartenente a quella ete è costretto ad analizzarlo. Se il broadcast cresce nella frequenza, la banda disponibile comincia a diminuire sensibilmente, fino a consumarsi. Le VLAN definiscono e ridimensionano i domini di broadcast, perché ogni VLAN contiene solo il traffico dei dispositivi che le appartengono.

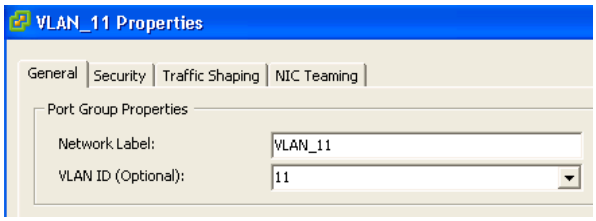


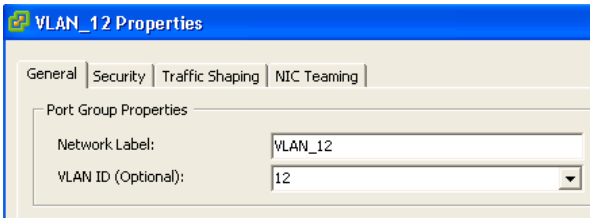
Per definire le VLAN, uno switch associa ogni porta a un identificativo, detto **VLAN ID**. Appena un frame ethernet entra nello switch, viene marcato con il VLAN ID. Lo standard VLAN più comune è rappresentato dal protocollo **IEEE 802.1Q** e prevede l'inserimento di un tag di quattro byte nel frame Ethernet. L'operazione è chiamata tecnicamente **VLAN tagging**.

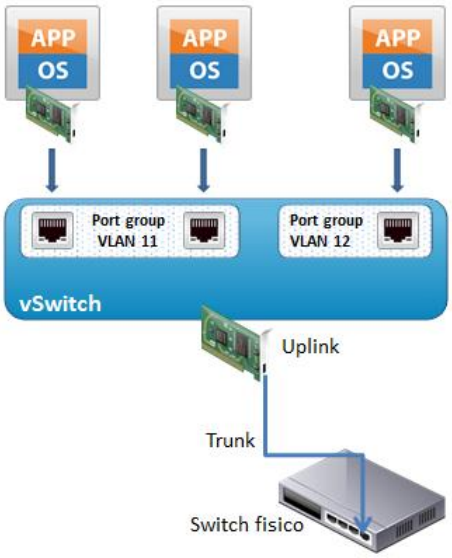
Gli switch che vogliono trattare le VLAN 802.1q devono supportare il protocollo 802.1q. **Gli host VMware ESXi supportano il VLAN tagging 802.1q**.

Le porte di uno switch possono essere di accesso (**access port**), usate per collegare gli host, o di **trunk**, usate per gli uplink tra diversi switch o tra switch e router. Le porte degli switch utilizzate per un collegamento trunk devono essere configurate in modalità trunk. **Le trame girano in formato 802.1Q solo sulle porte di trunk**. Quando sono inoltrate agli host, il tag VLAN viene eliminato e il formato del frame torna ad essere quello dello standard Ethernet. **Gli host infatti non sono a conoscenza delle VLAN**.

Nel networking virtuale di VMware vSphere, **le VLAN si configurano a livello di port group**, sia che si tratti di Standard vSwitch, sia di Distributed vSwitch. Un port group può essere configurato con un VLAN ID compreso tra **0** (nessuna VLAN) e **4095** (trunk). È possibile definire un VLAN ID per un determinato port group, come mostrato nelle immagini sotto. I pacchetti provenienti da una VM collegata a quel port group vengono taggati con il VLAN ID all'uscita del virtual switch, e sono privati del tag appena ritornano nella VM.





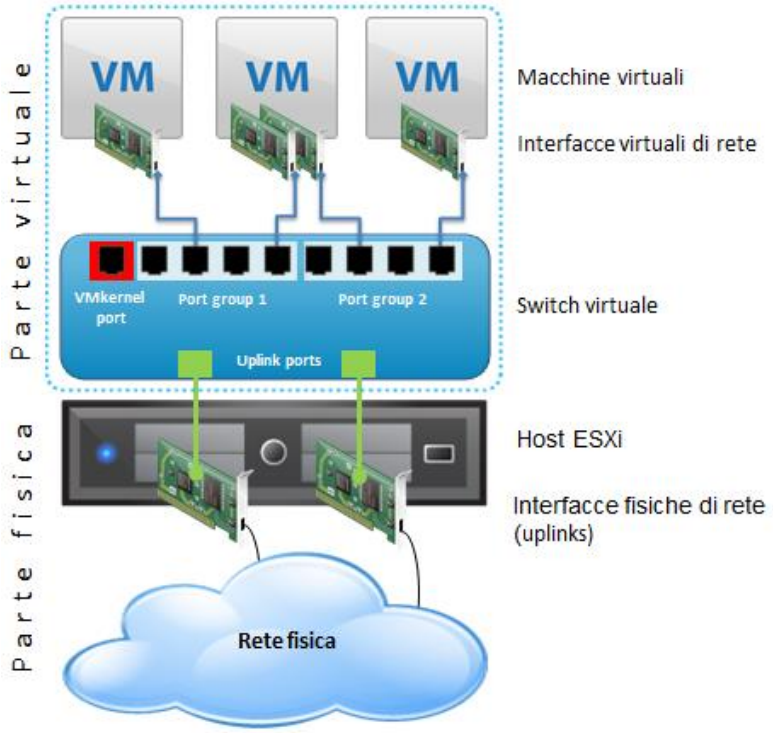


Riepilogo - configurazione delle VLAN in un port group.

- VLAN ID da 1 a 4094 – intervallo degli ID da utilizzare per le singole VLAN.
- VLAN ID 0 (Zero) – utilizzato per disattivare il VLAN tagging. È il valore predefinito, da utilizzare se non si desidera alcuna VLAN.
- VLAN ID 4095 – è un valore che corrisponde a tutte le VLAN, in pratica abilita il funzionamento del trunk nel port group.

Capitolo 7
Virtual networking con switch standard

Uno switch virtuale standard, nell'ambiente di VMware vSphere, consente alle macchine virtuali di comunicare tra loro con gli stessi protocolli utilizzati negli switch fisici, senza la necessità di hardware di rete aggiuntivo. In generale, gli switch virtuali possono essere interfacciati alla rete fisica semplicemente associandoli a una o più interfacce fisiche disponibili negli host. Nello schema qui sotto viene schematizzato il virtual networking di VMware vSphere con l'impiego di uno switch standard, o **Standard vSwitch**.

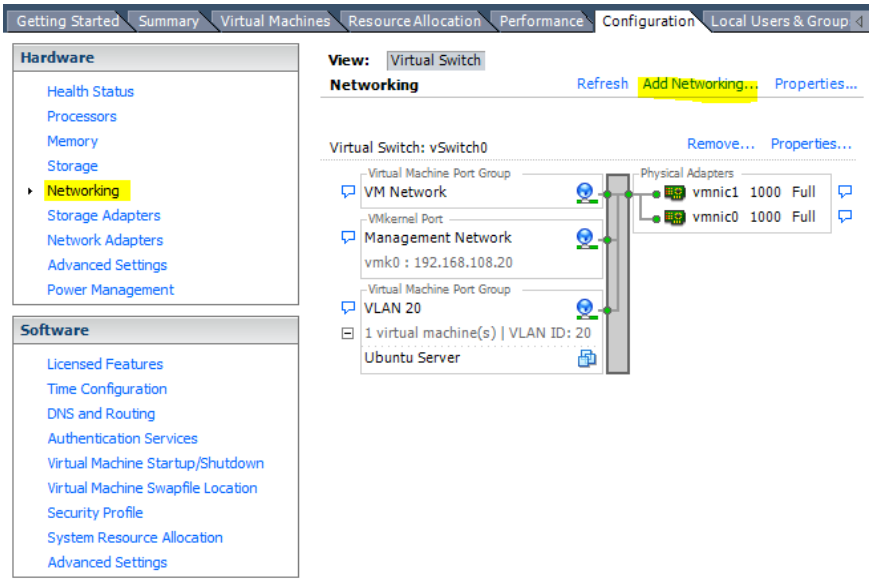


Possiamo osservare, partendo dall'alto, delle macchine virtuali dotate di interfacce virtuali, queste ultime connesse alle porte di uno switch virtuale standard, o Standard vSwitch. Lo switch virtuale è suddiviso in diversi Port Group, ed è collegato alle interfacce fisiche del server fisico tramite le porte di uplink. Esiste una porta di uplink per ogni interfaccia fisica collegata allo switch virtuale.

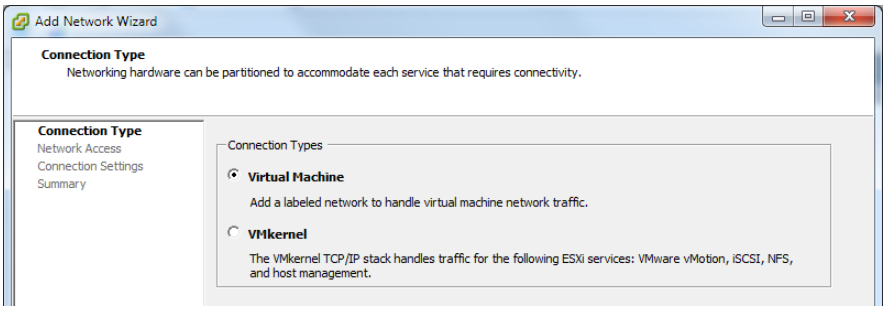
7.1 Creazione di uno switch standard

Procedura tramite vSphere Client

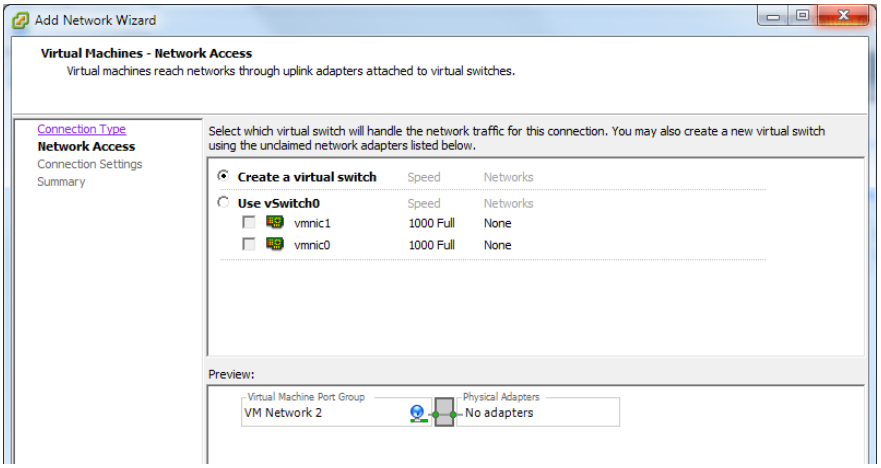
1) All'interno del tab **Configuration** dell'host selezionato, andare nella sezione **Networking**, quindi selezionare la voce **Add Networking**.



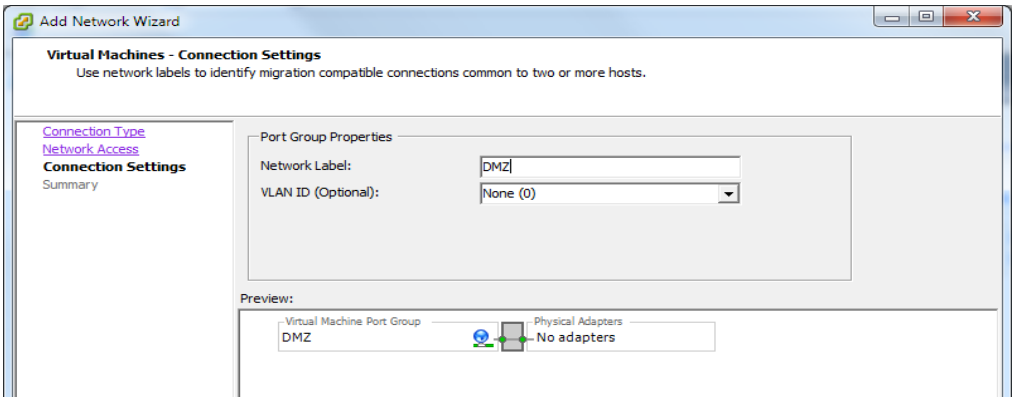
2) Selezionare il tipo di connessione necessaria. Le connessioni di tipo **Virtual Machine** consentono di creare un nuovo switch standard, oppure un nuovo port group all'interno di uno switch esistente.



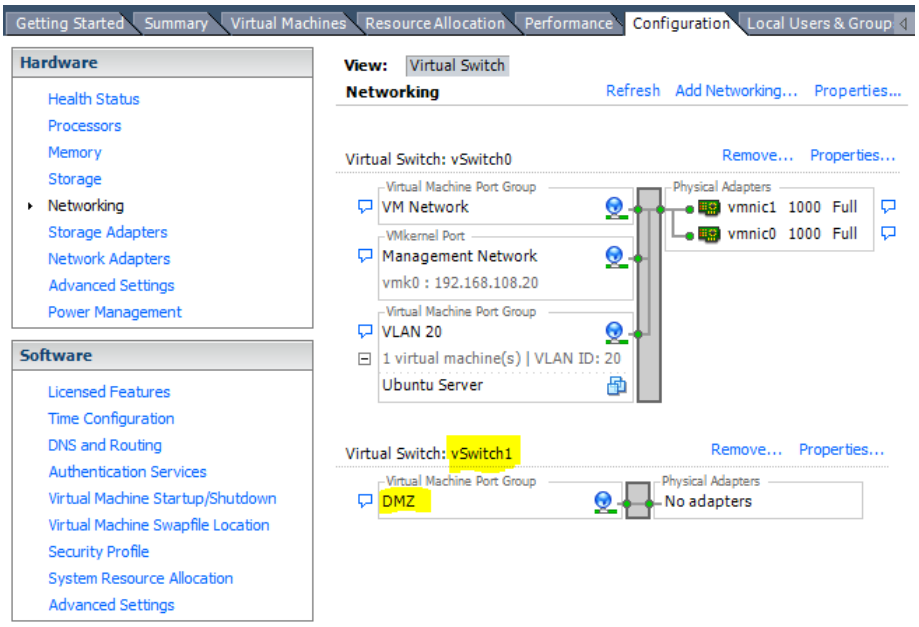
3) Creare un nuovo virtual switch. In maniera predefinita, un nuovo switch virtuale standard sarà dotato di 120 porte: ogni interfaccia di rete virtuale connessa occupa una porta. Si tenga conto del fatto che anche ogni uplink collegato occupa una porta. Si possono configurare sino a un massimo di 4.088 porte per ogni switch standard, con un limite complessivo di 4.096 porte per tutti gli switch virtuali standard all'interno di un singolo host ESXi.



4) La creazione di un nuovo switch prevede, in maniera implicita, la creazione di un primo port group. Assegnare un nome al gruppo e un VLAN ID se necessario. Il port group dell'esempio mostrato raccoglierà macchine da proteggere in DMZ dietro un firewall; lo switch sarà privo di uplink, perché deve semplicemente fornire connessione a macchine virtuali protette dal firewall (anch'esso installato su una macchina virtuale). In tal caso il firewall avrà più interfacce virtuali, e almeno una di esse sarà collegata allo switch appena creato.

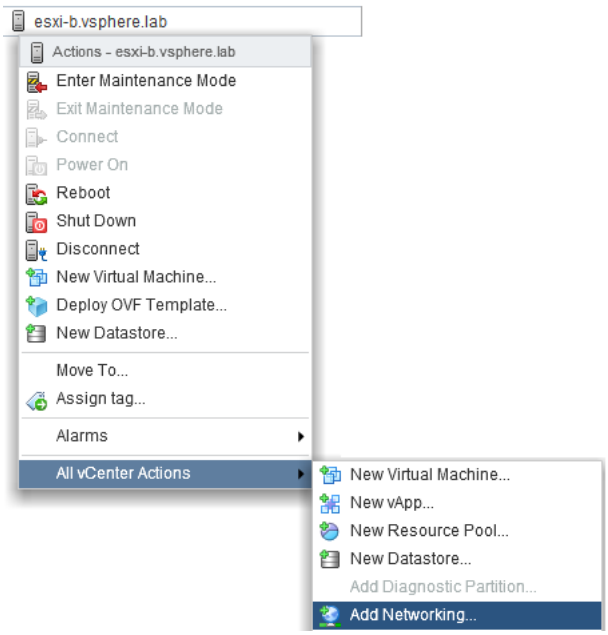


5) Dopo aver terminato la procedura, si può vedere il riepilogo di quanto configurato.

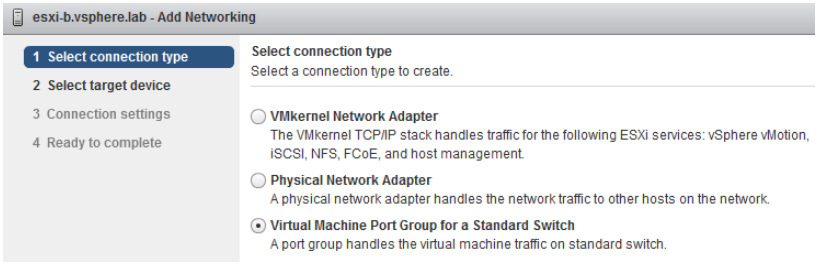


Procedura tramite vSphere Web Client

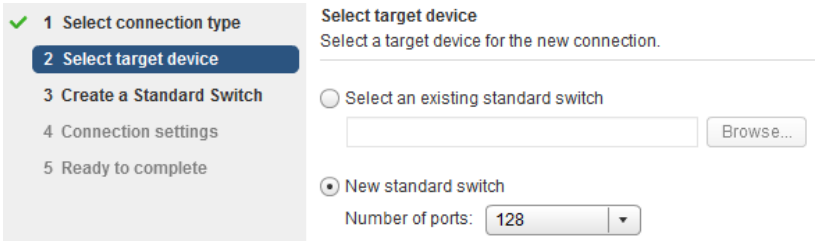
1) Tramite il pannello di navigazione a sinistra, individuare l'host desiderato, fare clic con il tasto destro su di esso e selezionare **All vCenter Actions** > **Add Networking**.



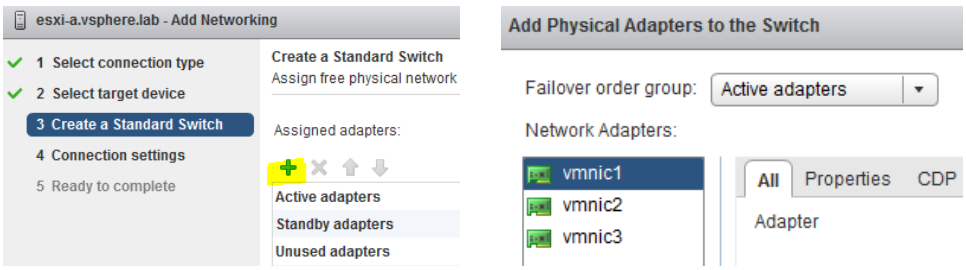
2) Su **Select connection type**, selezionare la voce **Virtual Machine Port Group for a Standard Switch** e fare clic su Next.



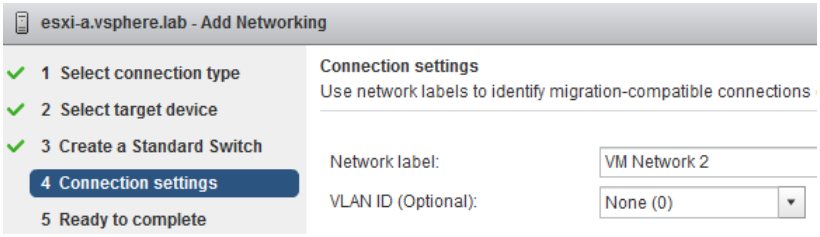
3) Su **Select target device**, creare un nuovo switch standard, specificando il numero di porte desiderate.



4) Su **Create a Standard Switch**, assegnare le interfacce di rete fisiche al nuovo switch virtuale, facendo clic sul simbolo "**+**". Le interfacce possono essere assegnate ad uno dei gruppi di failover seguenti: Active Adapters, Standy Adapters, Unused Adapters. È comunque possibile creare il nuovo switch senza interfacce.



5) Su **Connection settings**, assegnare un nome al port group, oppure accettare quello generato dal sistema.

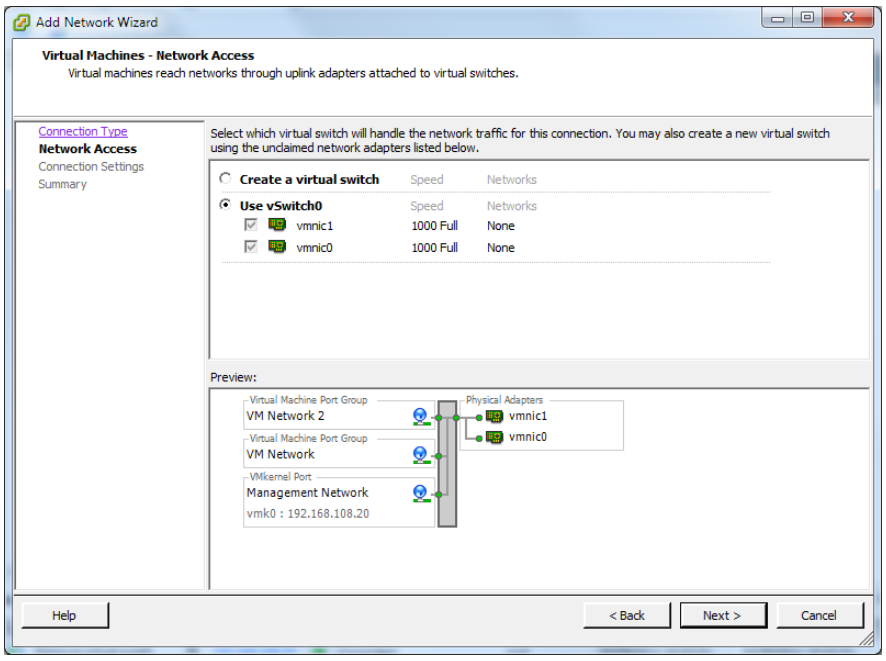


6) Andando avanti, sarà possibile rivedere le impostazioni assegnate. Fare clic su Back per eseguire le modifiche necessarie, oppure fare clic su Finish per terminare.

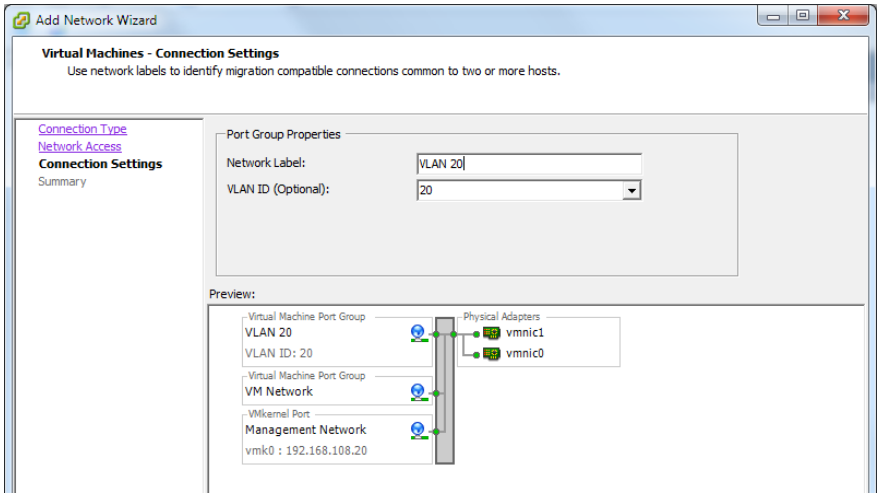
7.2 Creazione di un port group

Procedura con vSphere Client

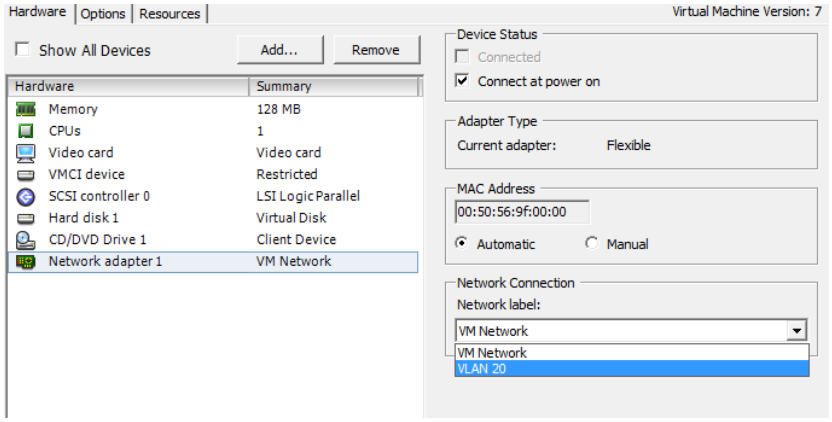
1) All'interno del tab **Configuration** dell'host selezionato, andare nella sezione **Networking**, quindi selezionare la voce **Add Networking**.
2) Selezionare il tipo di connessione necessaria. Le connessioni di tipo **Virtual Machine** consentono di creare un nuovo switch standard, oppure un nuovo port group all'interno di uno switch esistente.
3) Utilizzare uno switch esistente per creare un nuovo gruppo di porte al suo interno.

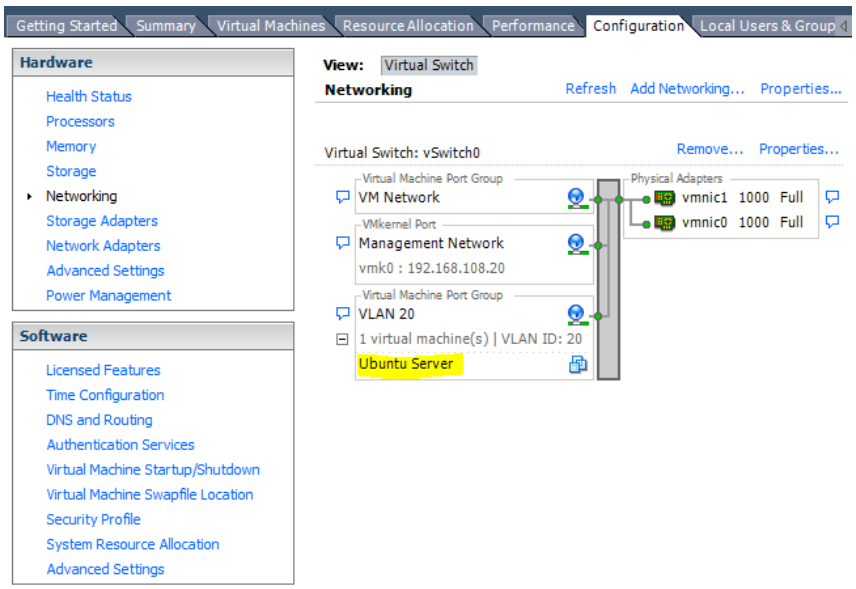


4) Un Port Group può essere visto come insieme di caratteristiche ben precise che accomuna tutte le porte appartenenti al gruppo stesso. Al port group può essere assegnato un VLAN ID. Se non si vogliono utilizzare VLAN, lasciare il valore predefinito (0).



5) Per collegare una macchina virtuale (o meglio una o più interfacce virtuali) ad un port group, è sufficiente specificare il nome del port group a cui collegare l'interfaccia. Qui sotto vediamo un esempio con una macchina virtuale denominata "Ubuntu Server".

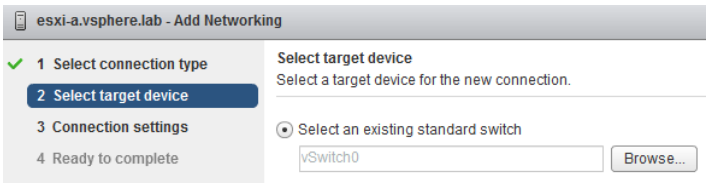




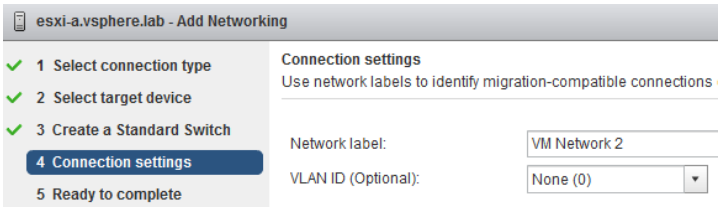
Procedura con vSphere Web Client

1) Tramite il pannello di navigazione a sinistra, individuare l'host desiderato, fare clic con il tasto destro su di esso e selezionare **All vCenter Actions** > **Add Networking**.

2) Su **Select connection type**, selezionare la voce **Virtual Machine Port Group for a Standard Switch** e fare clic su Next.
3) Su **Select target device**, selezionare uno switch esistente per creare al suo interno un nuovo port group.



4) Su **Connection settings**, assegnare un nome al port group, oppure accettare quello generato dal sistema.



5) Andando avanti, sarà possibile rivedere le impostazioni assegnate. Fare clic su Back per eseguire le modifiche necessarie, oppure fare clic su Finish per terminare.

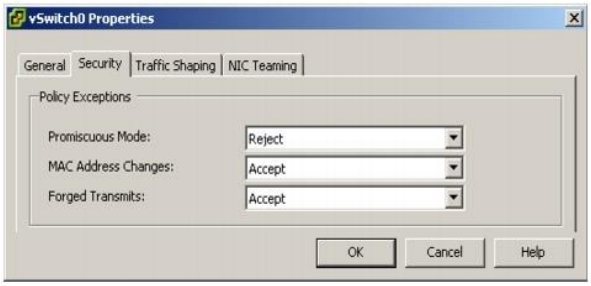
7.3 Impostazioni di sicurezza

Le impostazioni di sicurezza della rete virtuale (**network security policies**) sono configurabili sia a livello di switch sia di port group. Se vengono definite impostazioni specifiche per un port group, allora queste prevalgono sulle impostazioni assegnate a livello di switch. I parametri si configurano nelle proprietà dello switch o del port group, tramite vSphere Client o vSphere Web Client. Come già indicato in più occasioni, solo se si utilizza vSphere Client ci si può collegare direttamente all'host ESXi che contiene lo switch da modificare.

- **Promiscuous Mode**: impostazione della modalità promiscua per le interfacce di rete virtuali. È definita in modalità promiscua una scheda di rete che rimane in ascolto su tutto il traffico che passa sul cavo attestato ad essa. In maniera predefinita, in una rete Ethernet ogni interfaccia di rete rimane in ascolto dei soli pacchetti il cui MAC-address di destinazione corrisponde al proprio. È chiamata sniffing l'attività di ascolto di tutto il traffico passante; lo sniffing prevede appunto di impostare la scheda di rete in modalità promiscua. Con l'impostazione **Reject**, le interfacce virtuali non saranno in grado di intercettare il traffico non indirizzato ad esse, anche se impostate in modalità promiscua. Con l'impostazione **Accept**, è possibile compiere attività di sniffing in rete (di default è su Reject).
- **MAC Address Changes**: rende possibile la modifica del mac-address nelle macchine virtuali. Se impostato su **Reject**, nel momento in cui una macchina virtuale utilizza un mac-address differente da quello assegnato alla sua interfaccia virtuale, non sarà più in grado di ricevere pacchetti: tecnicamente viene disabilitata la relativa porta sullo switch virtuale, finché non si ripristina l'indirizzo MAC corretto. Di default l'impostazione è su Accept.
- **Forged Transmits**: specifica se devono essere accettati pacchetti con mac address modificato. Se l'impostazione corrisponde a **Reject**, saranno bloccati tutti i pacchetti in uscita con mac-address sorgente diverso da quello assegnato all'interfaccia virtuale (di default è su Accept).

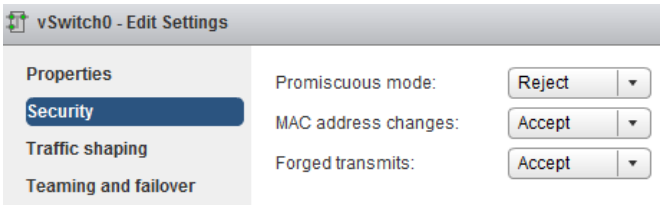
Procedura tramite vSphere Client

1) All'interno del tab **Configuration** dell'host selezionato, andare nella sezione **Networking**, selezionare uno switch standard e fare clic su **Properties**.
2) Nel tab **Ports**, selezionare lo switch o un port group, quindi fare clic su **Edit**. Le impostazioni assegnate a livello di port group sovrascrivono quelle assegnate a livello di switch.
3) Fare clic sul tab **Security** e impostare i parametri come desiderato.



Procedura tramite vSphere Web Client

1) Nel pannello di navigazione a sinistra, individuare l'host desiderato, fare clic sul tab **Manage**, quindi su **Networking** > **Virtual Switches**.
2) Selezionare lo switch dalla lista e fare clic su **Edit settings**. Se le impostazioni devono essere assegnate ad un port group, selezionarlo nello schema di rete che appare più sotto e fare clic su Edit Settings.
3) Fare clic su **Security** e impostare i parametri desiderati. Nel caso di un port group, abilitare la voce **Override** per sovrascrivere i parametri impostati a livello di switch.



7.4 Gestione del traffico

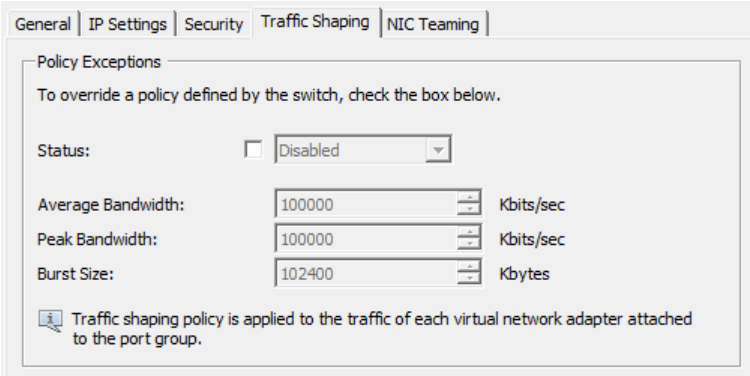
Le impostazioni del **Traffic Shaping**, disponibili sia a livello di switch che di port group, consentono di ottimizzare e garantire le prestazioni del traffico di rete, riducendo i tempi di latenza e sfruttando al meglio la banda disponibile grazie a meccanismi che prevedono l'accodamento e il ritardo dei pacchetti in uscita (**outbound traffic**). Le impostazioni, indicate qui sotto, valgono per tutte le porte virtuali connesse allo switch o al port group.

- **Average Bandwidth**: valore di traffico medio (bit per secondo) che lo switch cerca di far rispettare.
- **Peak Bandwidth**: larghezza di banda extra disponibile per brevi istanti.
- **Burst Size**: quantità di traffico che può essere trasmesso o ricevuto alla velocità di picco.

Procedura tramite vSphere Client

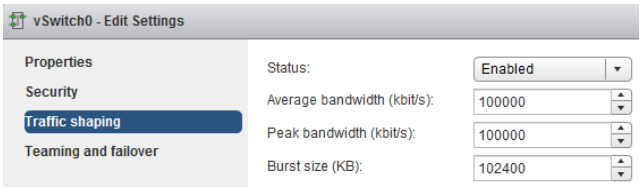
1) All'interno del tab **Configuration** dell'host selezionato, andare nella sezione **Networking** e selezionare uno switch standard, quindi fare clic su **Properties**.

2) Nel tab **Ports**, selezionare lo switch o un port group, quindi fare clic su **Edit**. Le impostazioni assegnate a livello di port group sovrascrivono quelle assegnate a livello di switch.
3) Fare clic sul tab **Traffic Shaping**.
4) Selezionare la voce **Enabled** dal menu **Status** per abilitare le politiche di gestione sotto indicate.



Procedura tramite vSphere Web Client

1) Nel pannello di navigazione a sinistra, individuare l'host desiderato, fare clic sul tab **Manage**, quindi su **Networking** > **Virtual Switches**.
2) Selezionare lo switch dalla lista e fare clic su **Edit settings**. Se le impostazioni devono essere assegnate ad un port group, selezionarlo nello schema di rete che appare più sotto e fare clic su Edit Settings.
3) Fare clic su Traffic shaping e selezionare la voce **Enabled** dal menu **Status** per abilitare le politiche di gestione. Nel caso di un port group, abilitare la voce **Override** per sovrascrivere le impostazioni assegnate a livello di switch.



4) Per ogni policy (Average Bandwidth, Peak Bandwidth, Burst Size), inserire il valore desiderato.
5) Fare clic su OK per terminare la procedura.

7.5 Bilanciamento del carico di rete e tecniche di failover

Uno switch virtuale può essere connesso a più interfacce di rete fisiche (quelle dell'host ESXi) e sfruttare più uplink per il collegamento alla rete fisica; la funzionalità che permette l'uso contemporaneo di più uplink è chiamata **NIC Teaming**.

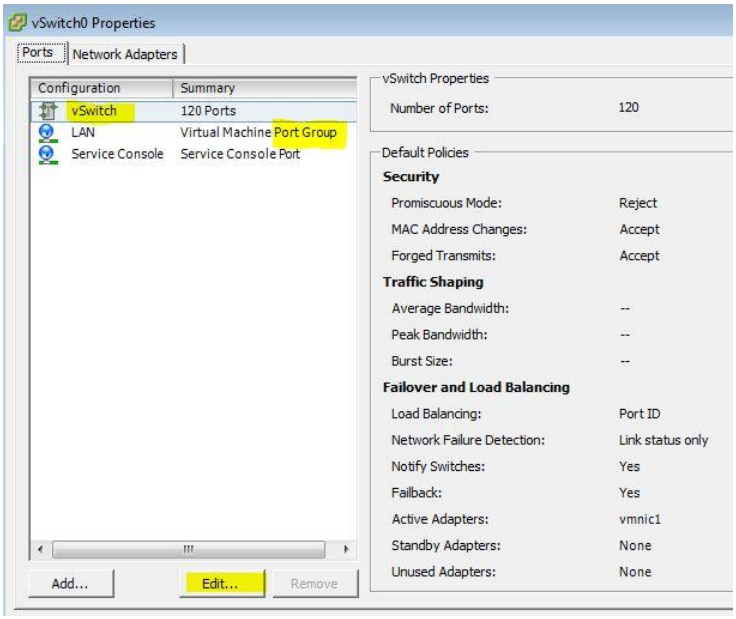
Le interfacce fisiche di uno stesso team devono trovarsi nello stesso dominio di broadcast. Per intenderci, non devono essere attestate su porte appartenenti a VLAN diverse. Il NIC Teaming è configurabile sia a livello di switch virtuale che di port group. Se per un port group non vengono specificate impostazioni, allora vengono ereditate le impostazioni dello switch virtuale. Le impostazioni possibili riguardano principalmente due aspetti: il bilanciamento del carico e il failover.

- Il bilanciamento del carico (**Load Balancing**) permette di distribuire il traffico tra macchine virtuali e rete fisica attraverso due o più uplink. In pratica si ottiene un throughput più alto, e la quantità di dati trasmessi nell'unità di tempo sarà superiore a quella disponibile con un solo uplink.
- Il **failover** è il meccanismo con cui il traffico di rete viene instradato su un'altra interfaccia di rete fisica quando la prima non è più operativa.

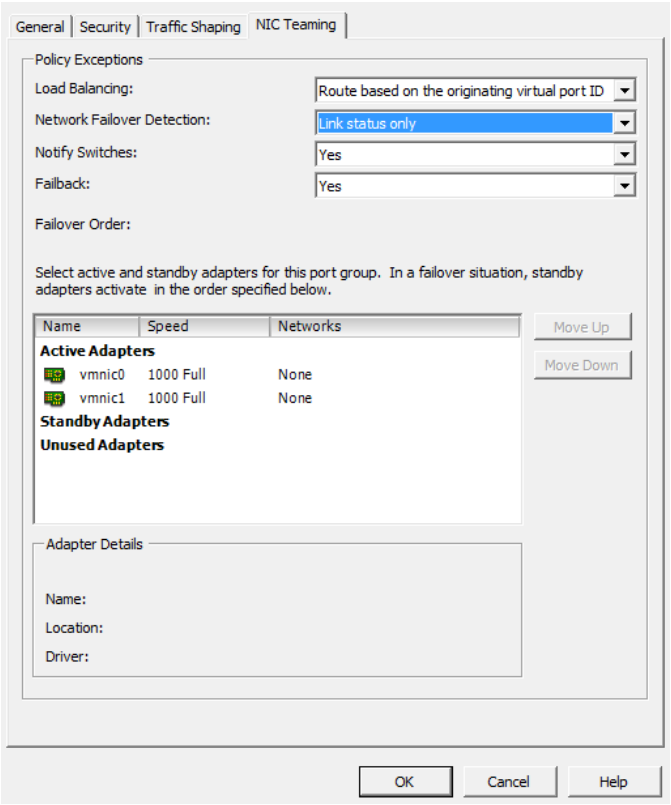
7.5.1 Configurazione del Teaming e del Failover

Procedura con vSphere Client

1) All'interno del tab **Configuration** dell'host selezionato, andare nella sezione **Networking** e fare clic sulla voce **Properties** relativa allo switch da modificare.
2) Selezionare lo switch virtuale o un port group, quindi fare clic su **Edit**.

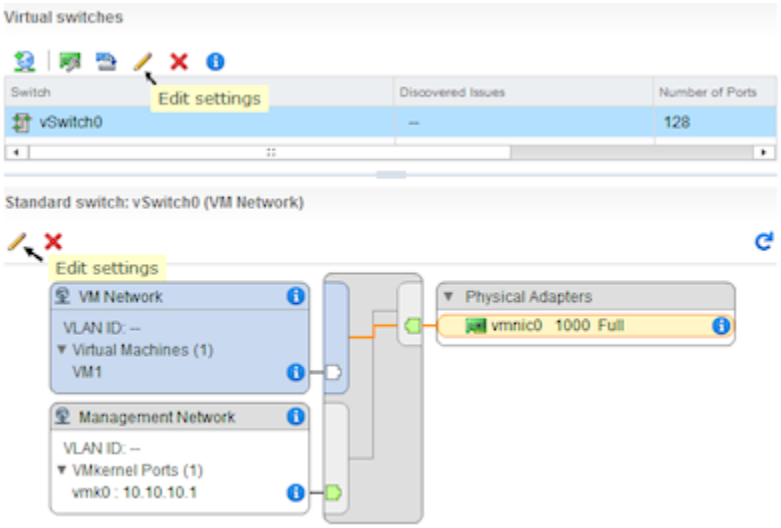


3) Per modificare le impostazioni di Failover e Load Balancing, selezionare il tab **NIC Teaming**.

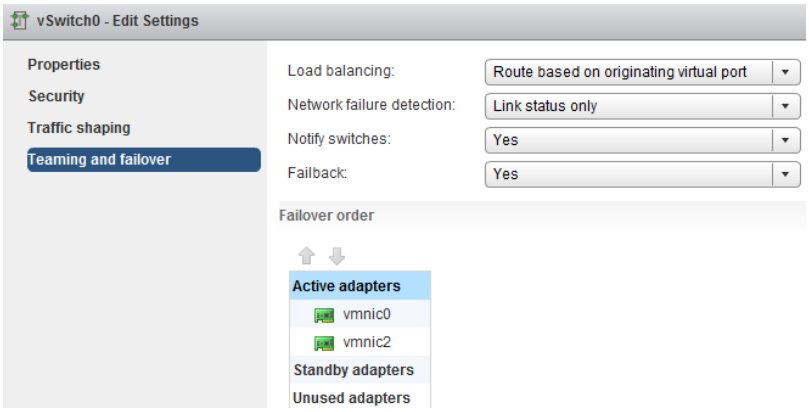


Procedura con vSphere Web Client

1) Nel pannello di navigazione a sinistra, individuare l'host desiderato, fare clic sul tab **Manage**, quindi su **Networking** > **Virtual Switches**.
2) Selezionare lo switch dalla lista e fare clic su **Edit settings**. Se le impostazioni devono essere assegnate ad un port group, selezionarlo nello schema di rete che appare più sotto e fare clic su **Edit Settings**.



3) Fare clic su **Teaming and failover** e impostare i parametri come desiderato.



7.5.2 I parametri di Teaming e Failover

Load Balancing

- **Route based on the originating port ID** - con questo metodo il traffico in uscita dalla rete virtuale viene mappato ad una specifica interfaccia fisica. L'algoritmo utilizzato prevede che l'interfaccia fisica sia scelta in base all'ID della porta virtuale su cui è collegata la VM. Per capire meglio, ogni macchina virtuale ha un port-ID che identifica la sua associazione allo switch virtuale: il carico è bilanciato in base all'ID e nient'altro. È un meccanismo che abbraccia tutti i protocolli. Quando si utilizza questa impostazione, il traffico in uscita da un'interfaccia virtuale è inviato sempre allo stesso uplink, purché non avvenga un failover verso un'altra interfaccia fisica. Anche le risposte sono ricevute sulla stessa interfaccia fisica, perché lo switch fisico esterno memorizza l'associazione con essa (associazione porta - indirizzo MAC). Questa impostazione fornisce una distribuzione uniforme del traffico se il numero di interfacce di rete virtuali è superiore al numero di uplink fisici.

  Con l'instradamento basato sul **port ID**, il traffico in uscita da una macchina virtuale è mappato in modo statico a un'interfaccia fisica: non importa quanto sia occupata la scheda di rete, il traffico continuerà a transitare per la stessa scheda e non sarà mai inoltrato verso un'interfaccia inattiva o più scarica (a meno di failover). Tuttavia, poiché il calcolo per la scelta della scheda di rete è eseguito solo una volta, questo metodo impegna pochissimo la CPU. Inoltre, poiché ci si basa sulle porte, se una macchina virtuale è stata configurata con più interfacce di rete virtuali, si ha la certezza che per ognuna di queste saranno utilizzati uplink diversi.

- **Route based on source MAC hash** - con questo metodo l'instradamento è basato sull'hash dell'indirizzo MAC sorgente. In pratica il traffico in uscita da una VM è indirizzato ad uno specifico uplink in base all'indirizzo MAC dell'interfaccia virtuale. Valgono le stesse considerazioni del punto precedente: il traffico proveniente da un'interfaccia di rete virtuale è inviato sempre alla stessa scheda fisica dell'host ESXi ed anche le risposte vengono ricevute sulla stessa scheda fisica, in quanto lo switch fisico esterno memorizza l'associazione con essa (associazione porta - indirizzo MAC). Una macchina virtuale non può utilizzare più di un uplink a meno che non utilizzi più indirizzi MAC sorgenti (e quindi più interfacce virtuali) per il traffico in uscita.

  Con il metodo basato su MAC sorgente, il traffico in uscita da ogni macchina virtuale è associato a una specifica scheda di rete fisica, in base all'indirizzo MAC dell'interfaccia virtuale. Questo comportamento è quasi identico al precedente, ma per macchine con più

interfacce virtuali non è garantito l'uso di uplink differenti; per questo motivo il metodo in oggetto non è quasi mai consigliato.

- **Route based on IP hash** - l'instradamento è basato sull'hash degli indirizzi IP (sorgente e destinazione) di ogni pacchetto. Affinché questo metodo possa funzionare, è necessario che lo switch fisico esterno aggreghi le porte tramite protocollo **EtherChannel** o secondo standard **802.3ad** (in particolare il protocollo LACP che rappresenta una parte delle specifiche 802.3ad). Il bilanciamento viene eseguito per il traffico in uscita: si utilizza un uplink differente per ogni sessione "IP-sorgente/IP-destinazione". Ad esempio, se una VM con un determinato IP comunica con due destinazioni IP differenti (esterne all'host ESXi), impegna due interfacce fisiche (uplink) distinte.

  L'instradamento basato su IP è l'unico metodo che permette, a una macchina virtuale dotata di una sola vNIC, di utilizzare la larghezza di banda complessiva di più interfacce di rete fisiche. Richiede tuttavia una modifica sulla configurazione dello switch fisico esterno, con l'attivazione di funzioni (EtherChannel) che non tutti gli switch supportano.

- **Use explicit failover order** - con questa impostazione non c'è bilanciamento del carico ma solo failover, in base alle impostazioni di failover specificate nel riquadro "Failover order". Quando accade un evento di failover, la scelta del nuovo uplink da utilizzare ricade su quello in linea da più tempo, in base al valore di **reported uptime**.

Failover

- **Link Status only** - si basa esclusivamente sullo stato del collegamento (link status) fornito dall'interfaccia fisica dell'host ESXi. Possono essere rilevati guasti dovuti a un cavo di rete staccato o allo switch fisico con problemi di alimentazione. Non è possibile tuttavia rilevare errori di configurazione, come ad esempio una porta dello switch fisico bloccata dal protocollo spanning tree, o configurata in modo errato a livello di VLAN.

- **Beacon Probing** – vengono inviati dei **beacon packets** (pacchetti per il rilevamento di errori sulla rete) e si rimane in ascolto di essi. I pacchetti beacon sono inviati in broadcast da tutti gli uplink del team. Lo switch fisico esterno inoltra (per sua natura) i pacchetti su tutte le porte appartenenti allo stesso dominio di broadcast. Ogni uplink rimane in attesa di ricevere i pacchetti dagli altri uplink dello stesso team; se un uplink non riceve pacchetti per tre volte consecutive, è marcato come "failed". In tal caso la caduta del link può essere dovuta sia a problemi sull'interfaccia fisica connessa allo switch esterno, sia a problemi a valle che non permettono ai pacchetti beacon di raggiungere l'uplink. Questo metodo permette di rilevare problemi sui collegamenti in maniera più precisa della semplice modalità "Link Status only".

Notify switch

L'opzione Notify Switch, quando attiva, permette all'host ESXi di notificare immediatamente, allo switch fisico esterno, i cambiamenti avvenuti a seguito di failover. Le notifiche avvengono anche quando un'interfaccia virtuale di una qualsiasi VM viene collegata allo switch virtuale, nell'ottica di diminuire i tempi di latenza.

Failback

Per impostazione predefinita, le interfacce fisiche dello stesso team lavorano secondo una logica di Failback: se una scheda fisica in stato "failed" torna in linea, riprende servizio immediatamente, rimpiazzando l'interfaccia che aveva assunto il suo ruolo. Di default, la modalità Failback è impostata su Yes. Al contrario, impostando il Failback su No, l'interfaccia di rete è tenuta inattiva

anche dopo il suo ritorno in linea (ovviamente finché l'altra interfaccia non va in errore e si riattiva una nuova procedura di failover).

Failover order

L'opzione Failover Order specifica come distribuire il carico di lavoro sulle interfacce di rete fisiche.

- **Active Uplinks** - le interfacce in questo gruppo sono tutte parte attiva del team.
- **Stanby Uplinks** - le interfacce in questo gruppo rimangono in standby per entrare in funzione nelle situazioni di failover, in cui prendono il posto di quelle andate in down.
- **Unused Uplinks** - le interfacce in questo gruppo semplicemente non sono utilizzate.

7.6 Inserimento di una nuova interfaccia di uplink

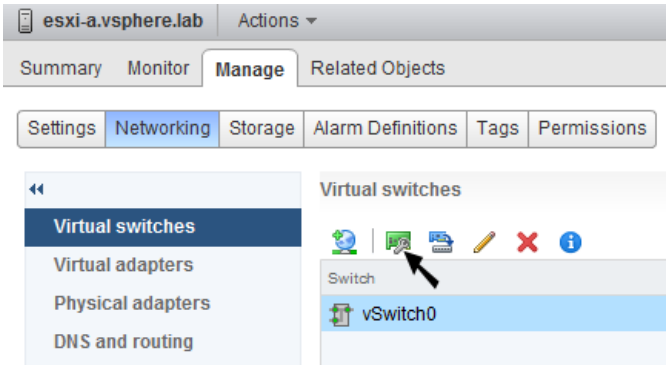
Per sfruttare i vantaggi offerti dal NIC Teaming, è necessario associare ad un singolo switch virtuale un minimo di due interfacce fisiche di rete. Lo switch virtuale sarà dotato di tanti uplink quante sono le interfacce fisiche associate.

Procedura con vSphere Client

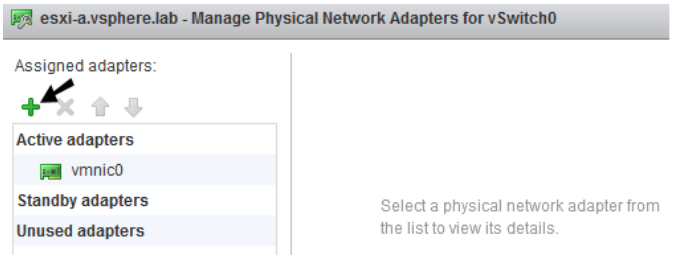
1) All'interno del tab **Configuration** dell'host selezionato, andare nella sezione **Networking** e fare clic sulla voce **Properties** relativa allo switch da modificare.
2) Selezionare il tab **Network Adapters**.
3) Fare clic su **Add** per avviare la procedura guidata di aggiunta di un'interfaccia. Selezionare una o più interfacce dalla lista e fare clic su Next.
4) (Opzionale) Per riordinare le interfacce rispetto alle due categorie Active Adapters e Standby Adapters, fare clic su **Move Up** o **Move Down**.
5) Fare clic su Next, quindi su Finish.

Procedura con vSphere Web Client

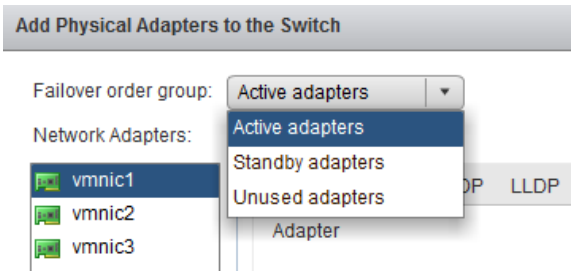
1) Nel pannello di navigazione a sinistra, individuare l'host desiderato, fare clic sul tab **Manage**, quindi su **Networking** > **Virtual Switches**.
2) Selezionare lo switch a cui aggiungere un uplink e fare clic su **Manage the physical network adapters**.



3) Fare clic su **Add adapters**.



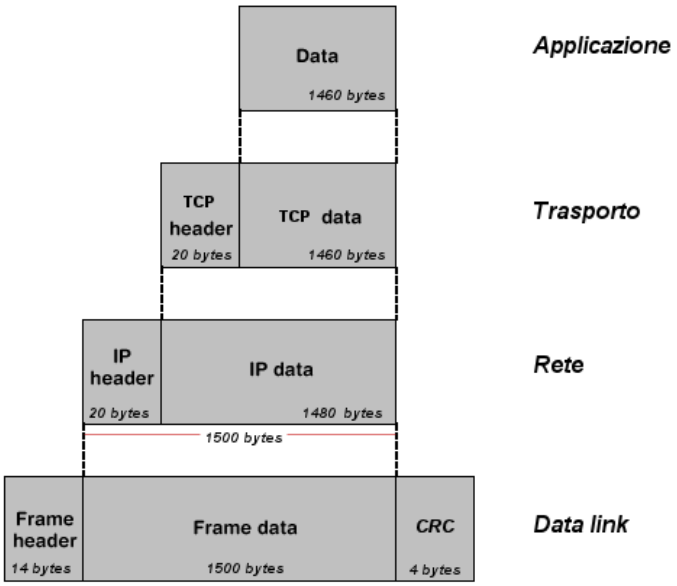
4) Selezionare un'interfaccia dalla lista e impostare il **Failover order group** dal menu a tendina in alto. Quindi fare clic su OK.



5) L'interfaccia aggiunta apparirà nella lista sotto la voce **Assigned Adapters**.
6) Fare clic su **OK** per concludere la procedura.

7.7 Impostazione dell'MTU

MTU, **Maximum Transmission Unit**, è la grandezza massima che può avere un pacchetto di livello 3 della pila ISO OSI, o livello rete nella pila TCP/IP (immagine sotto). In condizioni normali, tale dimensione è di **1500 byte**.

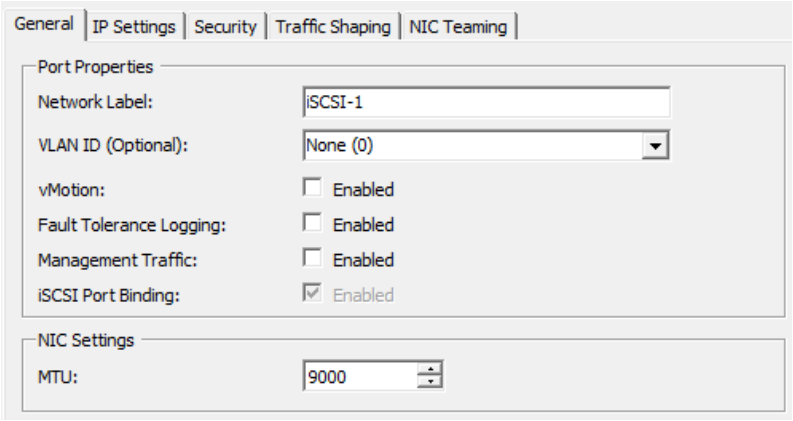


È possibile migliorare il rendimento della rete e ridurre l'utilizzo della CPU durante il trasferimento di file di grandi dimensioni, abilitando carichi maggiori e più efficienti per ogni pacchetto trasmesso. Per fare questo si utilizzano i **Jumbo frame**, ossia frame Ethernet di dimensioni superiori a 1500 byte. Se un dispositivo utilizza i Jumbo Frame, anche gli altri dispositivi della stessa rete devono avere la funzione Jumbo Frame abilitata, ed in particolare devono utilizzare lo

stesso valore MTU. Gli host ESXi supportano Jumbo frame con MTU sino a **9000 byte**. È possibile impostare il parametro per ogni switch virtuale e per ogni interfaccia VMkernel.

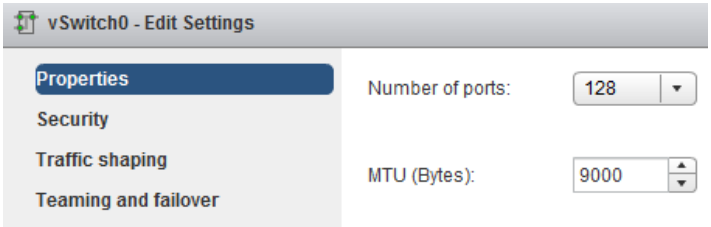
Procedura tramite vSphere Client

1. Nel tab **Configuration**, fare clic su **Networking**.
2. Fare clic sulle proprietà dello switch che si vuole modificare.
3. Nel tab **Ports**, selezionare il virtual switch o l'interfaccia VMkernel da modificare e fare clic su **Edit**;
4. Su **NIC Settings**, impostare il valore di **MTU** e fare clic su OK.



Procedura tramite vSphere Web Client

1) Nel pannello di navigazione a sinistra, individuare l'host desiderato, fare clic con il tasto destro su di esso, fare clic sul tab **Manage**, quindi su **Networking** > **Virtual Switches**.
2) Selezionare lo switch da modificare e fare clic su **Edit settings**.
3) Nella pagina **Properties**, impostare il valore di **MTU** come desiderato.



Procedura da riga di comando

Collegandosi alla console dell'host ESXi, è possibile impostare i Jumbo Frame da riga di comando, rispettando la sintassi seguente:

```
# esxcli network vswitch standard set -m MTU -v vSwitch#
```

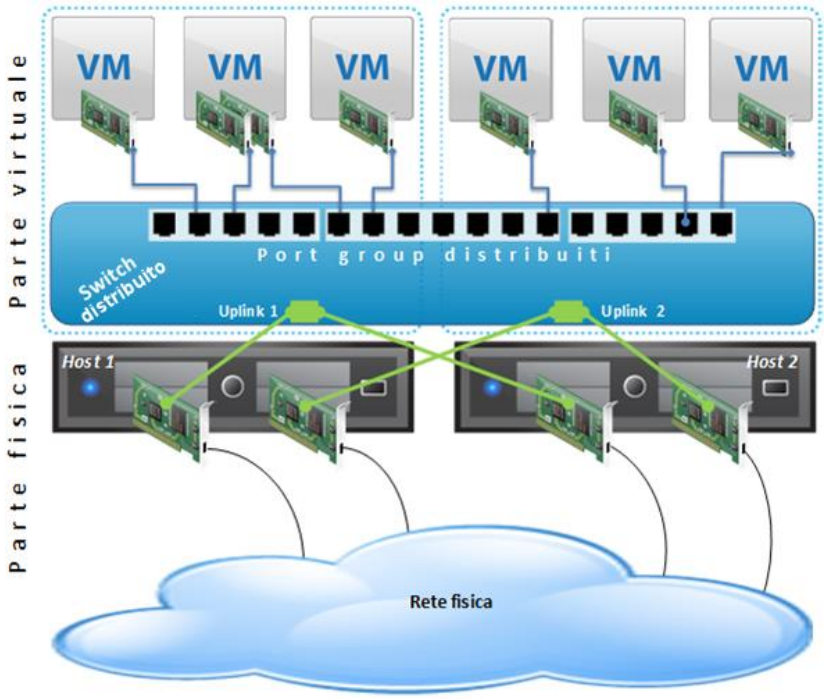
Il comando imposta l'MTU per tutti gli uplink dello switch virtuale. Se invece si vuole visualizzare la lista di tutti gli switch dell'host, con i relativi parametri di configurazione, si utilizza il comando seguente:

```
# esxcli network vswitch standard list
```

Capitolo 8
Virtual networking distribuito

Il networking virtuale distribuito si basa sull'impiego di switch virtuali distribuiti, tecnicamente chiamati **vSphere Distributed Switch (VDS)**. Si tratta di oggetti gestiti dal vCenter Server, creati per avere una configurazione del networking che si mantiene uguale su tutti gli host dell'infrastruttura virtuale. Il vantaggio di uno switch distribuito è che le impostazioni assegnate a una porta, o a un gruppo di porte, rimangono sempre uguali da un host all'altro, con evidenti vantaggi nella gestione delle macchine virtuali durante la loro migrazione fra host diversi. Le impostazioni assegnate ad uno switch distribuito vengono salvate nel database del vCenter Server.

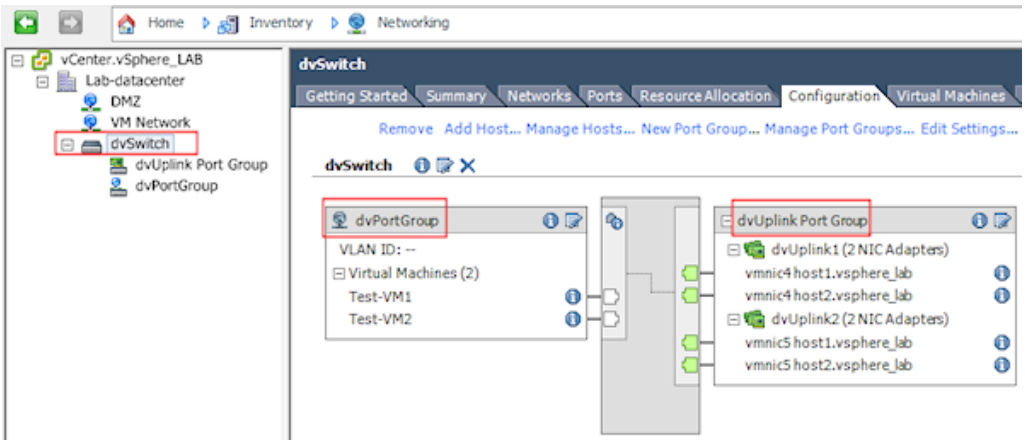
Abbiamo già visto che uno switch standard è dotato di porte e gruppi di porte; allo stesso modo uno switch distribuito è dotato di porte e gruppi di porte distribuiti, rispettivamente chiamati **Distributed Ports** (**DV Ports**) e **Distributed Port Groups** (**DV Ports Groups**). Proseguendo con lo stesso parallelismo, una porta distribuita è semplicemente una porta di uno switch distribuito che permette il collegamento al VMkernel o all'interfaccia di rete di una macchina virtuale. Un gruppo di porte distribuite definisce le opzioni di configurazione di un insieme di porte distribuite. In maniera predefinita la configurazione di una porta distribuita è determinata dalle impostazioni assegnate al port group di appartenenza, ma è possibile assegnare impostazioni specifiche per ogni singola porta.



Una porta di uplink di uno switch distribuito è chiamata **Uplink Port** (**dvUplink**); permette l'astrazione fisica dello switch distribuito rispetto ad ogni singolo host. Ad ogni porta di uplink possono essere associate una o più interfacce fisiche messe a disposizione dai vari host. Le porte di uplink sono organizzate in un unico gruppo, chiamato **Uplink Port Group** e gestito dal vCenter Server. Tutte le politiche di rete e le regole per gli uplink sono impostate a livello di gruppo.

Nell'immagine qui sotto possiamo vedere un esempio di Distributed Switch, con un solo Port Group configurato, dotato di due Uplink: Uplink1 e Uplink2. Ognuno dei due Uplink è interfacciato a due

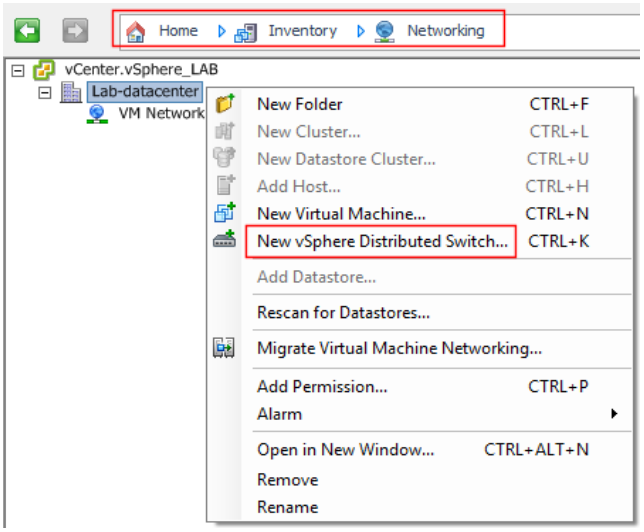
NIC fisiche appartenenti a host differenti. Come si può notare, gli uplink sono organizzati in un unico Uplink Port Group.



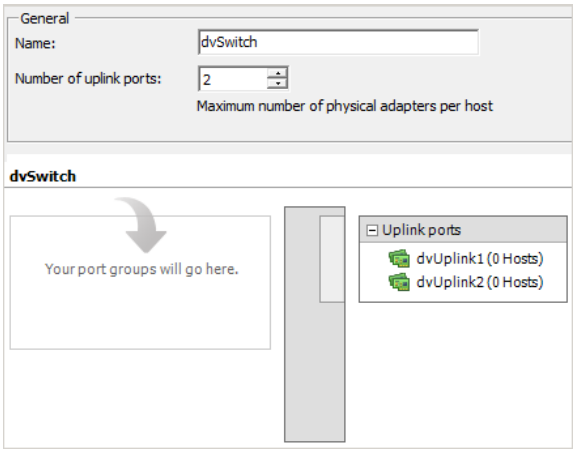
8.1 Creazione di uno switch distribuito

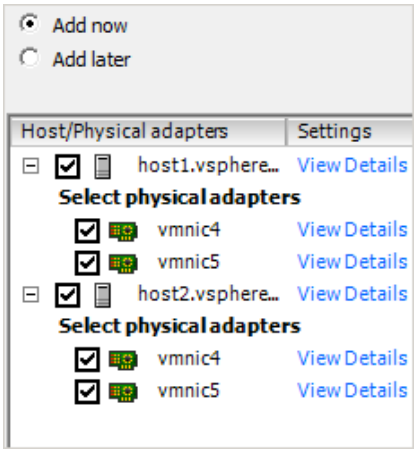
Procedura tramite vSphere Client

1. Dal percorso **Inventory > Networking**, fare clic con il tasto destro sul **Datacenter** e selezionare la voce **New vSphere Distributed Switch**. Nella procedura guidata, scegliere la versione desiderata di switch distribuito.

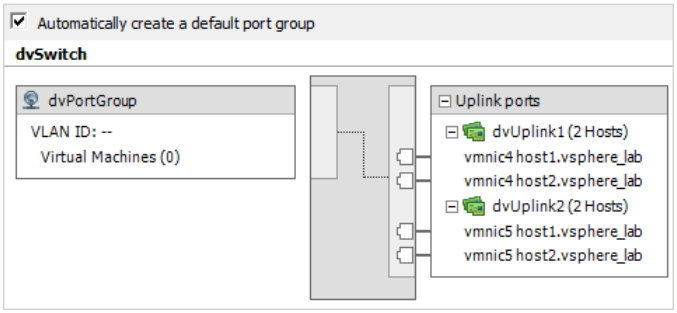


2. Nella finestra successiva, scegliere un nome per lo switch e specificare il **numero di porte di uplink**, ossia il **numero massimo di interfacce fisiche per ogni host** che faranno parte del dvSwitch. Gli host e le interfacce fisiche possono essere inseriti subito o successivamente; nel primo caso è sufficiente selezionare gli host desiderati e le rispettive interfacce libere e poi fare su **Add now**.



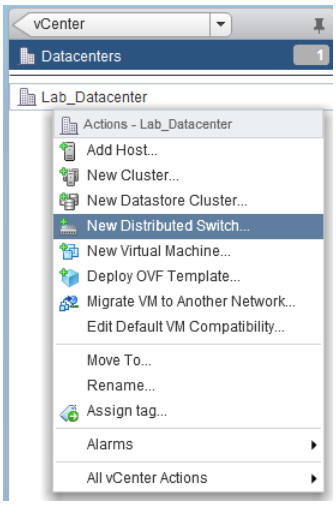


3. Infine l'ultima schermata propone un riepilogo delle impostazioni, con la possibilità di creare automaticamente un port group predefinito (**Automatically create a default port group**).



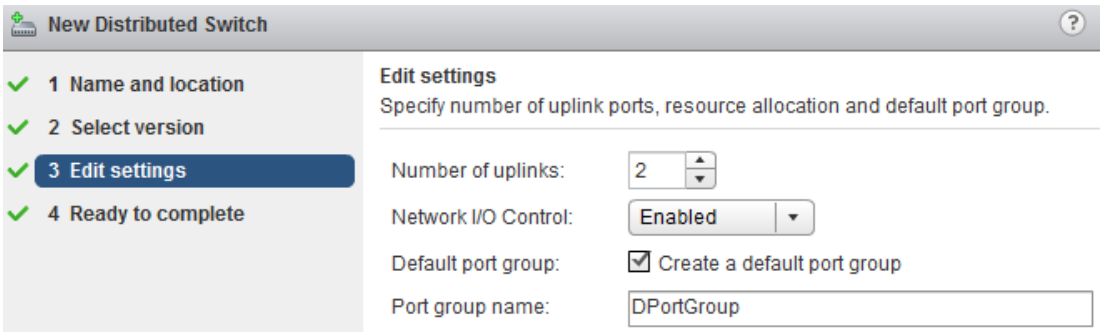
8.1.2 Procedura tramite vSphere Web Client

1. Nel pannello di navigazione a sinistra, individuare il data center desiderato, fare clic con il tasto destro su di esso e selezionare la voce **New Distributed Switch**.



2. Su **Name and Location**, digitare un nome per il nuovo switch distribuito, oppure accettare il nome proposto dal sistema, e fare clic su **Next**.
3. Su **Select version**, scegliere la versione desiderata di switch distribuito e fare clic su **Next**.

4. Su **Edit Settings**, specificare il **numero di uplink**, ossia il **numero massimo di interfacce fisiche per ogni host** che faranno parte dello switch distribuito. È inoltre possibile abilitare o disabilitare la funzione di **Network I/O control**, creare automaticamente un port group predefinito (**Create a default port group**) e assegnare un nome al port group predefinito.



5. Nella schermata successiva viene proposto un riepilogo delle impostazioni. Fare clic su **Finish** per terminare la procedura.

8.2 Inserimento e gestione degli host in uno switch distribuito

È possibile associare gli host ESXi e le interfacce di rete ad uno switch distribuito anche dopo la creazione dello switch stesso. Con vSphere Client, gli host e le interfacce sono associabili allo switch distribuito sia durante la creazione dello switch stesso, sia successivamente, mentre con vSphere Web Client sono necessari dei passaggi da eseguire successivamente alla creazione dello switch.

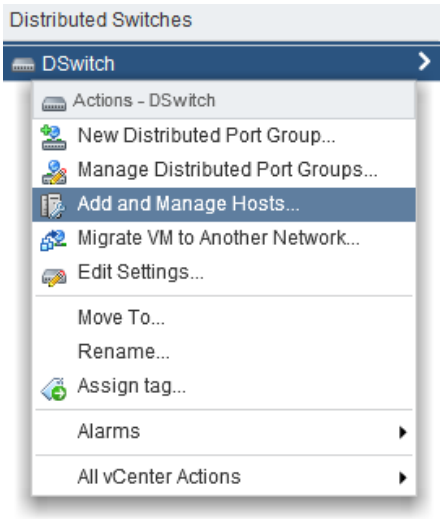
Procedura tramite vSphere Client

Per aggiungere un nuovo host ad uno switch distribuito, i passaggi sono indicati di seguito.

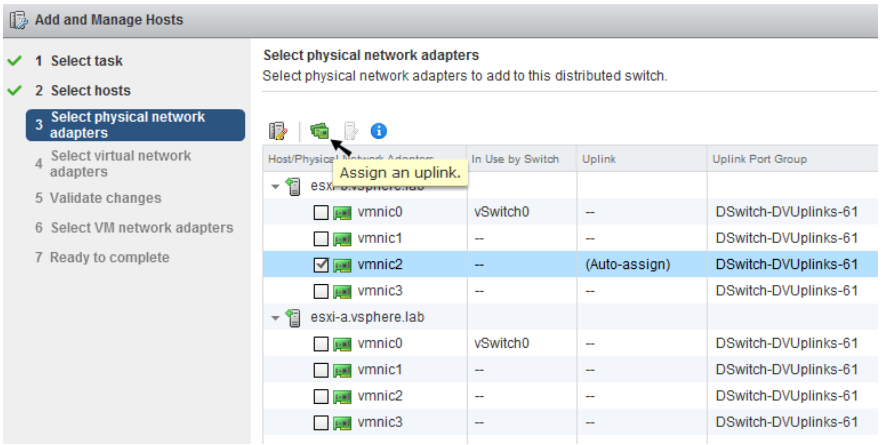
1. Nella modalità di visualizzazione **Networking**, fare clic con il tasto destro sullo switch distribuito. Selezionare la voce **Add Host** per aggiungere un nuovo host, oppure **Manage Host** per gestire un host già associato allo switch.
2. Selezionare gli host.
3. Selezionare le interfacce fisiche da aggiungere e/o deselezionare quelle da rimuovere, quindi fare clic su **Next**.
4. È possibile migrare le interfacce VMkernel su un port group distribuito, da selezionare nel menu a tendina nella colonna a destra. Per non effettuare alcuna migrazione, selezionare la voce **Do not migrate**. Fare clic su **Next**.
5. Opzionalmente, è possibile spostare le macchine virtuali nello switch distribuito. In tal caso, selezionare la voce **Migrate virtual machine networking** e impostare i port group di destinazione per la macchina virtuale.
6. Fare clic su **Next**, quindi su **Finish** per terminare la procedura.

Procedura tramite vSphere Web Client

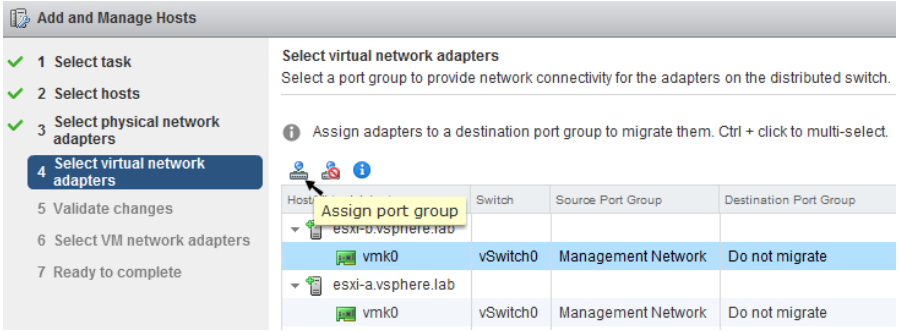
1. Nel pannello di navigazione a sinistra, individuare lo switch distribuito di proprio interesse, fare clic con il tasto destro su di esso e selezionare **Add and Manage Hosts**.



2. Su **Select Task**, selezionare l'opzione **Add Hosts** e fare clic su Next.
3. Fare clic su **Add new hosts** (simbolo "**+**") e selezionare gli host desiderati, quindi fare clic su OK e andare avanti.
4. Nella pagina **Select physical network adapters**:
    a. Per ogni interfaccia che si vuole inserire, selezionare il check box relativo e fare clic su **Assign an uplink**.



    b. Selezionare una porta di uplink dalla lista e fare clic su **OK**.
    c. La porta selezionata apparirà nella colonna **Uplink**. Se non si seleziona manualmente un uplink, quest'ultimo sarà assegnato automaticamente (**Auto-assign**).
    d. Fare clic su Next.
5. Nella pagina **Select virtual network adapters**:
    a. Selezionare le interfacce dalla lista e fare clic su **Assign port group**.



b. Nel box che si apre, selezionare un port group e fare clic su OK.

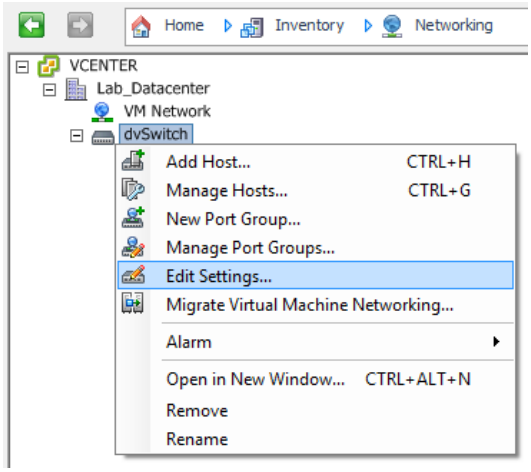
6. (Opzionale) Nella pagina **Select VM network adapters**, selezionare le macchine virtuali o le interfacce da migrare nello switch distribuito.
7. Fare clic su **Finish** per terminare la procedura.

8.3 Impostazioni di uno switch distribuito

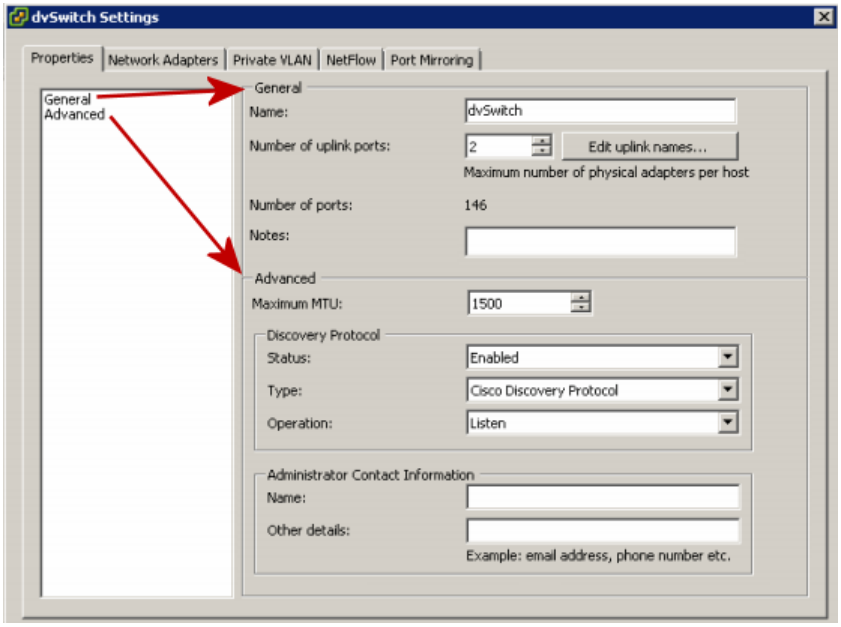
8.3.1 Proprietà generali di uno switch distribuito

Gestione tramite vSphere Client

1. Seguire il percorso **Inventory > Networking**, quindi fare clic con il tasto destro sullo switch distribuito e selezionare la voce **Edit Settings**.



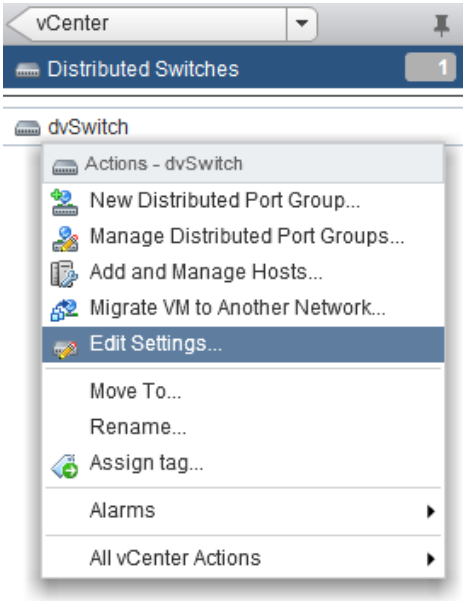
2. Nella finestra delle impostazioni, il primo tab **Properties** permette la modifica dei valori di tipo **General** e quelli di tipo **Advanced**.



3. I valori modificabili sono:
   - nome dello switch;
   - numero di porte di uplink;
   - dimensione massima MTU;
   - attivazione del protocollo Cisco Discovery Protocol;
   - informazioni sull'amministratore.

Gestione tramite vSphere Web Client

1. Nel pannello di navigazione a sinistra, individuare lo switch distribuito di proprio interesse, fare clic con il tasto destro su di esso e selezionare la voce **Edit Settings**.



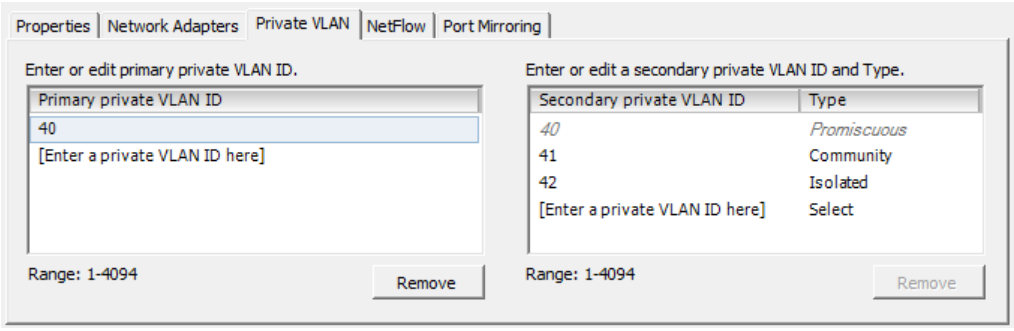
2. Nella finestra delle impostazioni, sono presenti le pagine **General** e **Advanced**.
3. I valori modificabili sono:
   - nome dello switch;
   - numero di porte di uplink;
   - attivazione del Network I/O control;
   - dimensione massima MTU;
   - attivazione del protocollo Cisco Discovery Protocol;
   - informazioni sull'amministratore.

8.3.2 VLAN di tipo privato

Le VLAN private sono utilizzate per risolvere i limiti del VLAN ID e il problema dello spreco di indirizzi in alcune configurazioni di rete. Una VLAN privata è identificata da un ID primario, ma può avere più ID secondari associati ad essa. Nel primo caso la VLAN prende il nome di **VLAN privata primaria**, nel secondo caso **VLAN privata secondaria**. La VLAN primaria è di tipo promiscuo, ossia le sue porte possono comunicare con tutte le porte configurate con l'ID primario. Le porte della VLAN secondaria possono essere di tipo **Isolated**, ossia comunicano solo con porte promiscue, o **Community**, ossia comunicano sia con porte promiscue sia con le altre porte della stessa VLAN secondaria. Affinché ci sia comunicazione tra una VLAN privata e la rete fisica, lo switch fisico esterno deve supportare la funzione di "Private VLAN".

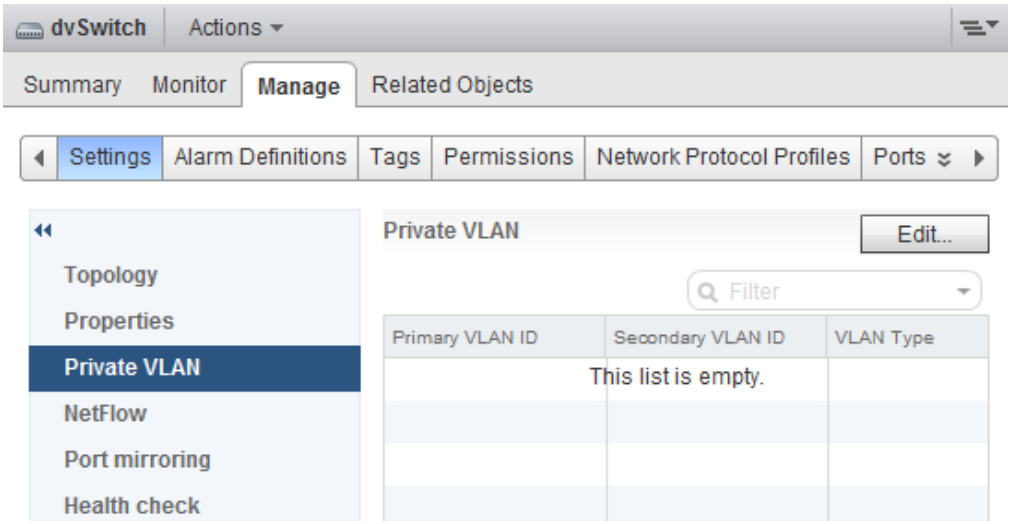
Gestione tramite vSphere Client

- Fare clic con il tasto destro sullo switch distribuito e selezionare la voce **Edit Settings**. Nella finestra delle impostazioni, andare sul tab **Private VLAN**.



Gestione tramite vSphere Client

- Individuare e selezionare lo switch distribuito nel pannello di navigazione a sinistra, fare clic sul tab **Manage**, fare clic su **Settings**, selezionare la voce **Private VLAN**, infine fare clic su **Edit.**

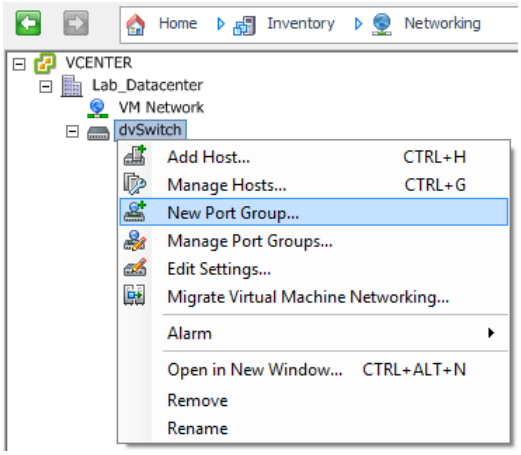


8.4 Creazione e modifica di un port group distribuito

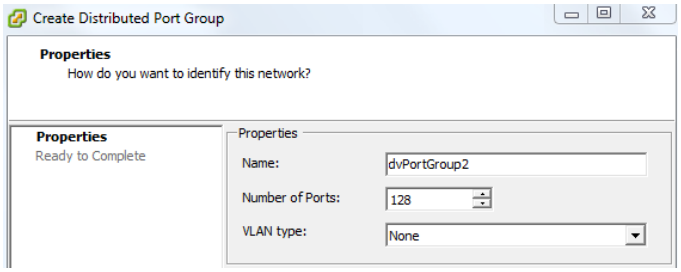
Con un port group distribuito (**Distributed Port Group**) si definiscono le opzioni di configurazione dell'insieme di porte che gli appartengono. In maniera predefinita, infatti, la configurazione di una porta distribuita è determinata dalle impostazioni assegnate al port group di appartenenza. Tuttavia, nei paragrafi successivi, vedremo come sia possibile assegnare impostazioni specifiche per ogni singola porta.

Procedura tramite vSphere Client

1. Andare su **Inventory** > **Networking**, fare clic con il tasto destro sullo switch distribuito e selezionare la voce **New Port Group**.



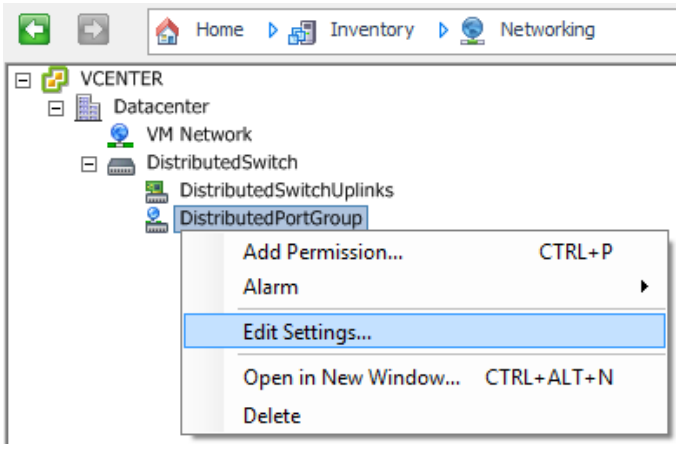
2. Inserire il nome, il numero di porte, ed eventualmente il tipo di VLAN.



Per quanto riguarda il tipo di VLAN, sono possibili diverse opzioni.

- **None** - per non utilizzare alcuna VLAN.
- **VLAN** - scegliendo questa voce, più sotto appare il campo VLAN ID in cui inserire l'ID della VLAN (tra 1 e 4094).
- **VLAN Trunking** - inserire l'intervallo di VLAN.
- **Private VLAN** - selezionare la VLAN privata precedentemente configurata a livello di switch.

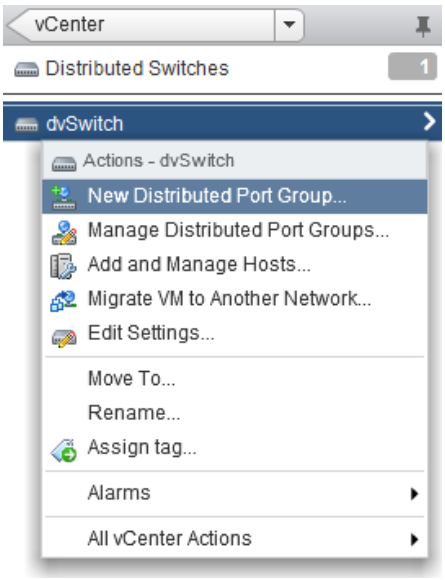
3. Dopo avere creato il nuovo port group distribuito, per modificarne le impostazioni fare clic con il tasto destro su di esso e selezionare la voce **Edit Settings**.



Per quanto riguarda le possibili impostazioni, far riferimento al paragrafo "Impostazioni di un port group distribuito" più avanti.

Procedura tramite vSphere Web Client

1. Individuare lo switch distribuito di proprio interesse nel pannello di navigazione a sinistra, fare clic con il tasto destro su di esso e selezionare la voce **New distributed port group**.



2. Nella pagina **Select name and location**, digitare il nome del nuovo port group distribuito, oppure accettare il nome generato automaticamente, quindi fare clic su **Next**.
   Nella pagina **Configure settings**, impostare le proprietà generali. Per quanto riguarda le possibili impostazioni, far riferimento al paragrafo "Impostazioni di un port group distribuito" più avanti.
3. Fare clic su **Next**, quindi su **Finish** per terminare la procedura.

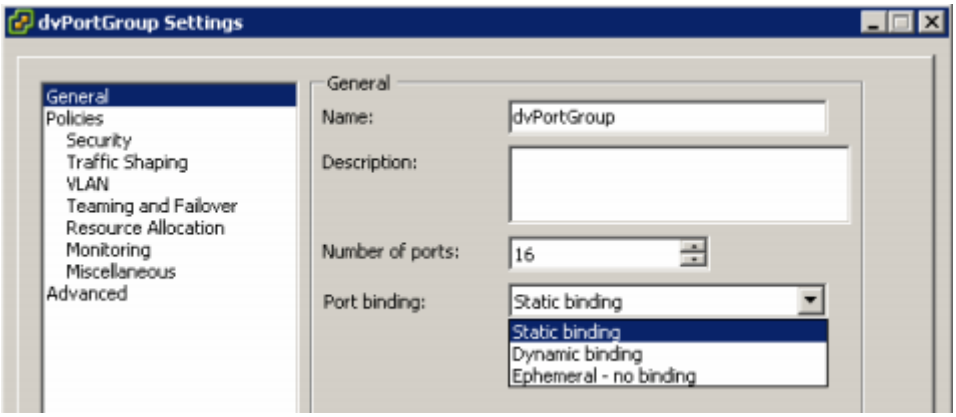
8.5 Impostazioni di un port group distribuito

8.5.1 Port binding

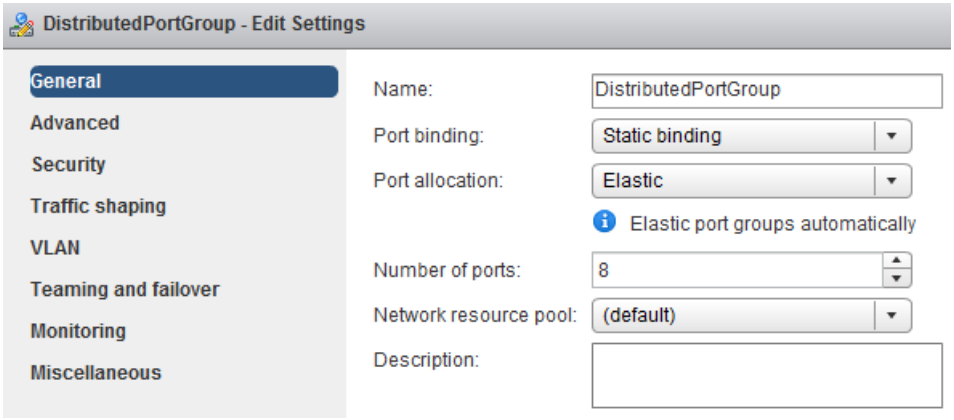
Con il port binding si configura l'associazione tra le porte del port group distribuito e le macchine virtuali.

- **Static binding** - assegnazione statica di una porta ad una VM, appena quest'ultima viene connessa al dvPort Group. L'assegnazione delle porte in modalità statica può essere realizzata solo tramite il vCenter Server.
- **Dynamic binding** - assegnazione dinamica di una porta a una VM, a partire dall'accensione di quest'ultima e comunque dopo la connessione al dvPort Group. L'associazione è persa allo spegnimento delle VM. La modalità dinamica non è più supportata in vSphere 5, tuttavia viene mantenuta per questioni di compatibilità.
- **Ephemeral - no binding** - con questa configurazione, l'associazione di una VM con una porta si stabilisce quando la VM è accesa e la sua interfaccia di rete risulta connessa. L'associazione è persa allo spegnimento della VM, oppure quando l'interfaccia di rete virtuale della VM risulta disconnessa. L'assegnazione delle porte in modalità ephemeral può essere realizzata sia in modo diretto, attraverso gli host ESX/ESXi, sia tramite il vCenter Server, con la possibilità quindi di gestire la connessione delle VM attraverso gli host nel momento in cui il vCenter non fosse in linea.

Gestione tramite vSphere Client



Gestione tramite vSphere Web Client

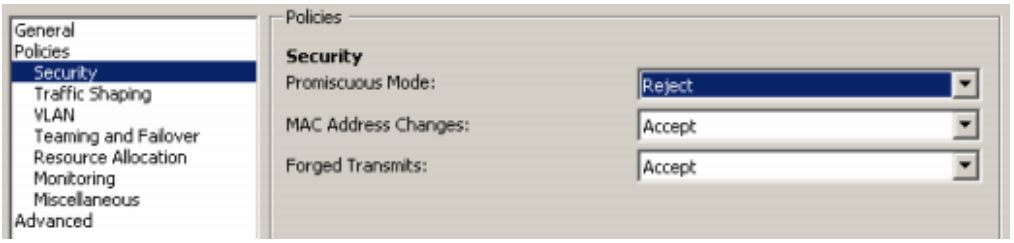


8.5.2 Security

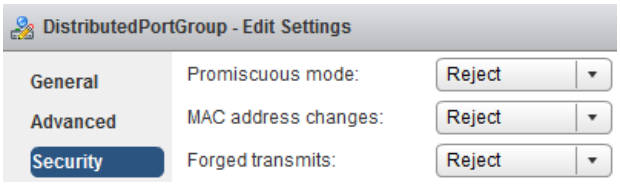
Le impostazioni di sicurezza sono valide per l'intero port group distribuito, con concetti simili a quanto già visto per gli switch standard.

- **Promiscuous Mode**: impostazione della modalità promiscua per le interfacce di rete virtuali. Se si sceglie Reject (impostazione di default), le interfacce virtuali non saranno in grado di intercettare il traffico non indirizzato ad esse, anche se impostate in modalità promiscua. Con l'impostazione Accept, è possibile eseguire attività di sniffing in rete.
- **MAC Address Changes**: rende possibile la modifica del mac-address nelle macchine virtuali. Se impostato su Reject, nel momento in cui una macchina virtuale utilizza un mac-address differente da quello assegnato alla sua interfaccia virtuale, non sarà più in grado di ricevere pacchetti. Di default l'impostazione è su Accept.
- **Forged Transmits**: specifica se una VM può inviare pacchetti con mac address diverso da quello impostato nell'interfaccia virtuale (di default è su Accept). Se l'impostazione è su **Reject**, verranno bloccati tutti i pacchetti in uscita con mac-address sorgente diverso da quello assegnato.

Gestione tramite vSphere Client



Gestione tramite vSphere Web Client

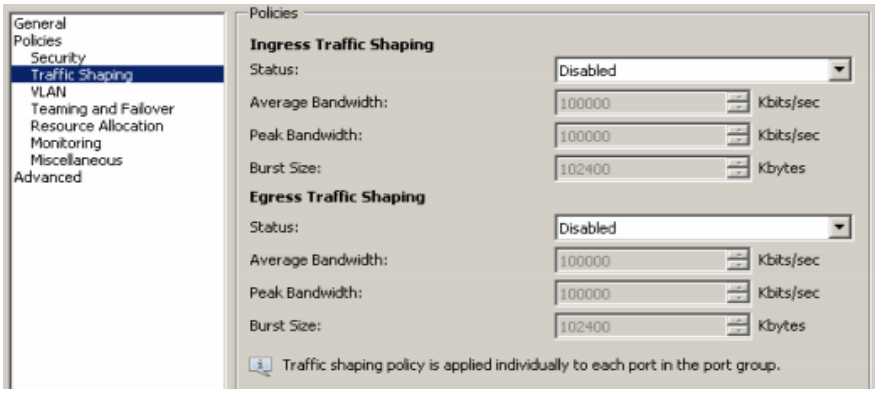


8.5.3 Traffic Shaping

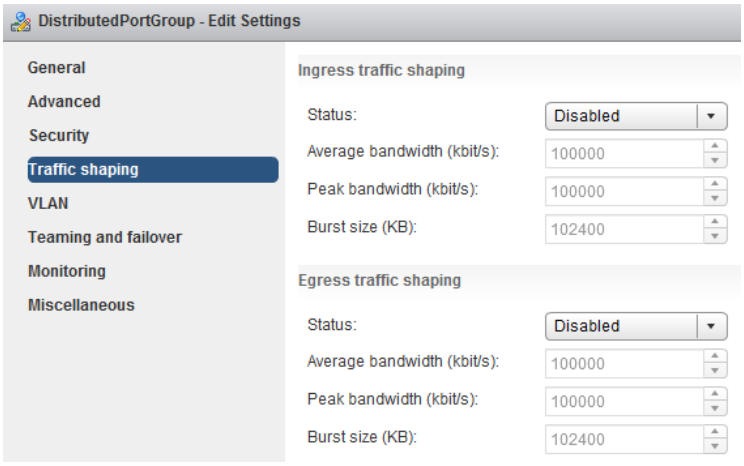
Le impostazioni di **Traffic Shaping** sono finalizzate a ottimizzare e garantire le prestazioni per il traffico di rete, a ridurre o controllare i tempi di latenza e a sfruttare al meglio la banda disponibile, tramite l'accodamento e il ritardo dei pacchetti in ingresso (**ingress**) ed in uscita (**egress**).

- **Average Bandwidth**: valore di traffico medio che lo switch cerca di far rispettare.
- **Peak Bandwidth**: larghezza di banda extra disponibile per brevi istanti.
- **Burst Size**: quantità di traffico che può essere trasmesso o ricevuto alla velocità di picco.

Gestione tramite vSphere Client



Gestione tramite vSphere Web Client

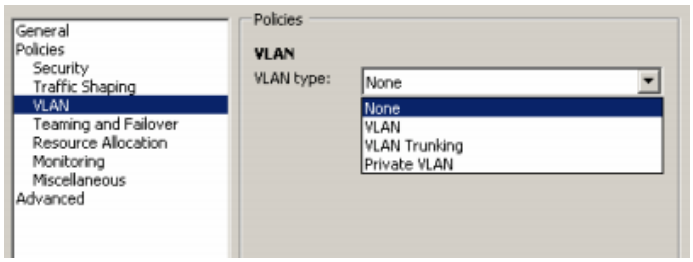


8.5.4 VLAN

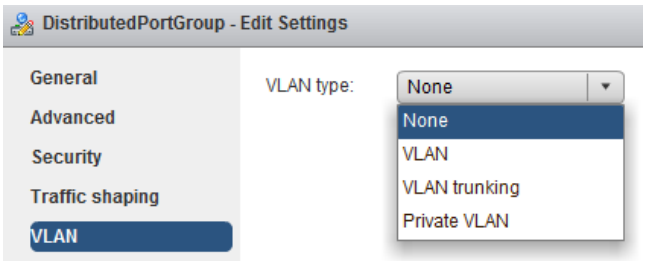
La finestra **VLAN** permette di definire le impostazioni relative al tipo di VLAN da utilizzare nel port group distribuito.

- **None** - nessuna VLAN da utilizzare
- **VLAN** - inserire l'ID della VLAN da utilizzare, da 1 a 4094
- **VLAN Trunking** - inserire il range del trunk, all'interno dell'intervallo 1 - 4094
- **Private VLAN** - selezionare una VLAN privata configurata in precedenza.

Gestione tramite vSphere Client



Gestione tramite vSphere Web Client



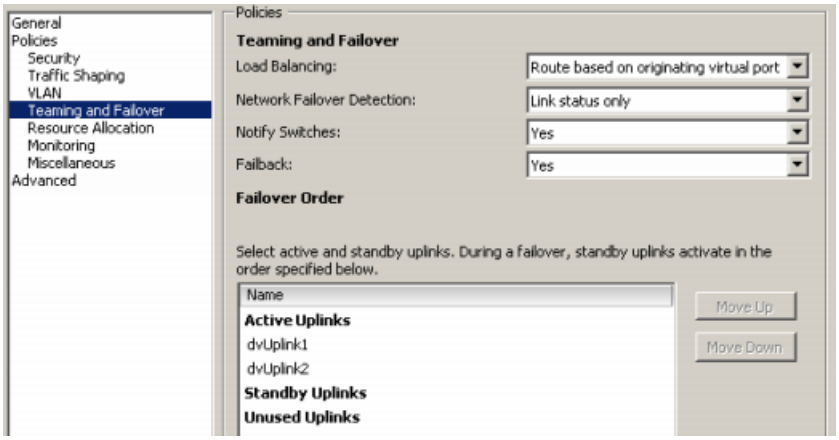
8.5.5 Teaming and Failover

La finestra **Teaming and Failover** permette di impostare il bilanciamento del carico (Load Balancing) e le politiche di failover che determinano in che modo il traffico di rete è distribuito tra gli uplink e in che modo deve essere reindirizzato in caso di errori sulle interfacce fisiche.

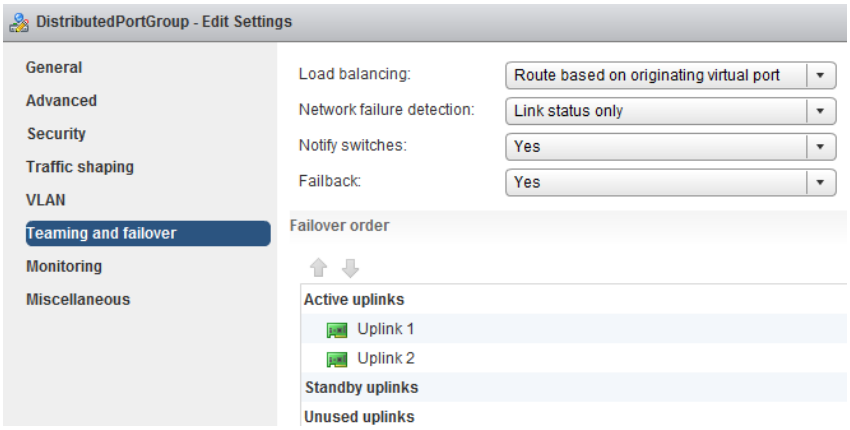
- **Load Balancing**.
  - **Route based on originating virtual port** - l'uplink è scelto in base alla porta virtuale dalla quale il traffico entra nello switch distribuito.

  - **Route based on IP hash** - l'instradamento è basato sull'hash degli indirizzi IP (sorgente e destinazione) di ogni pacchetto.
  - **Route based on source MAC hash** - con questo metodo l'instradamento è basato sull'hash dell'indirizzo MAC sorgente.
  - **Route based on physical NIC load** - l'instradamento è basato sul carico corrente delle interfacce fisiche.
  - **Use explicit failover order** - uplink scelto in ordine a partire dall'alto della lista Active Uplinks.
- **Network Failover Detection** - la configurazione del failover, e quindi del metodo che permette di rilevare l'assenza di connettività su un'interfaccia e di trovarne un'altra in sostituzione, prevede la scelta fra due metodi.
  - **Link Status only** - si basa esclusivamente sullo stato del collegamento (link status) fornito dall'interfaccia fisica dell'host ESXi.
  - **Beacon Probing** - vengono inviano dei **beacon packets** (pacchetti sonda per il rilevamento di errori sulla rete) e si rimane in ascolto di essi. Se un uplink non riceve pacchetti per tre volte consecutive, viene marcato come "failed".
- **Notify switch** - permette la notifica del failover allo switch fisico esterno.
- **Failback** - per impostazione predefinita, le interfacce fisiche dello stesso team lavorano secondo una logica di Failback: se una scheda fisica in stato "failed" ritorna in linea, riprenderà servizio immediatamente rimpiazzando l'interfaccia che aveva assunto il suo ruolo. Di default, la modalità Failback è impostata su Yes. Al contrario, impostando il Failback su No, l'interfaccia di rete viene tenuta inattiva anche dopo il suo ritorno in linea, ovviamente finché un'altra interfaccia non va in errore e si riattiva una nuova procedura di failover.
- **Failover order** - l'opzione Failover Order permette di specificare come distribuire il carico di lavoro sulle interfacce di rete fisiche. Le opzioni sono:
  - **Active Uplinks**: le interfacce in questo gruppo sono tutte up e parte attiva del team.
  - **Stanby Uplinks**: le interfacce in questo gruppo rimangono in standby per entrare in funzione in situazioni di failover.
  - **Unused Uplinks**: le interfacce in questo gruppo semplicemente non vengono utilizzate.

Gestione del Teaming e del Failover tramite vSphere Client



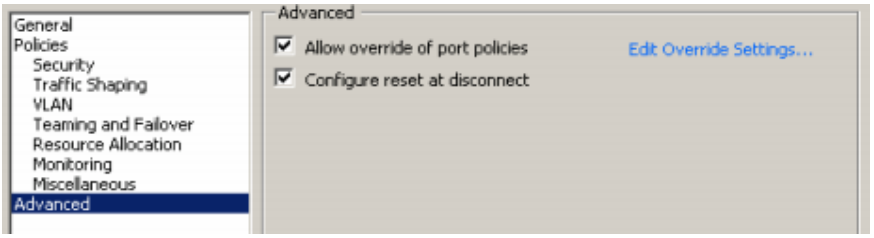
Gestione del Teaming e del Failover tramite vSphere Web Client



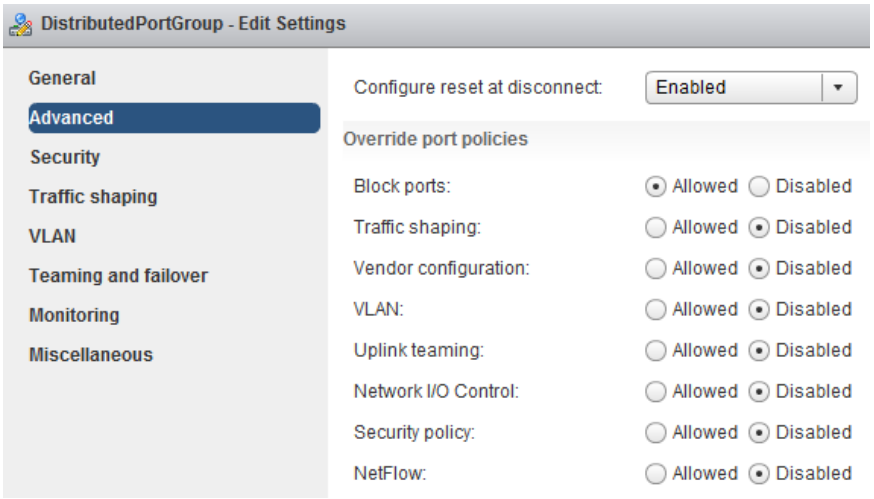
8.5.6 Advanced

La sezione **Advanced** consente, per ogni singola porta, di sovrascrivere le impostazioni assegnate al port group distribuito.

Gestione tramite vSphere Client



Gestione tramite vSphere Web Client



8.5.7 Altre politiche di gestione

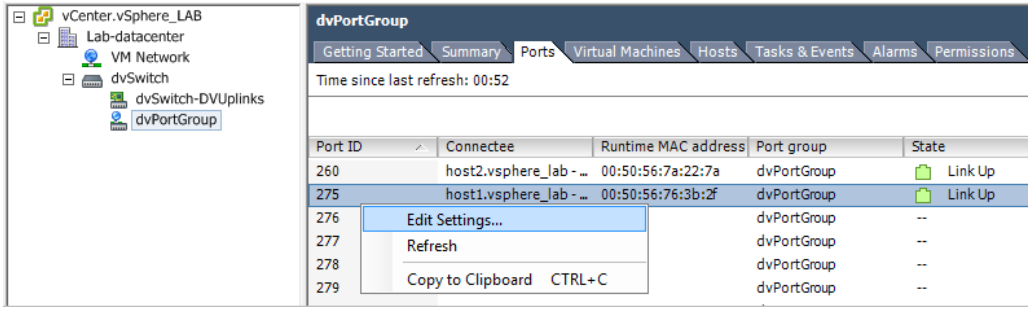
- **Resource Allocation** - permette di definire il Network Resource Pool da associare al dvPortgroup.
- **Monitoring**: permette di abilitare il protocollo **NetFlow** per il dvPortGroup.
- **Miscellaneous** - la funzione **Block all ports** permette il blocco di tutte le porte del dvPortgroup.

8.6 Porte di uno switch distribuito

Una porta distribuita (Distributed Port) è semplicemente una porta che appartiene ad uno switch distribuito e che permette il collegamento in rete del VMkernel o delle macchine virtuali. In maniera predefinita, la configurazione di una porta distribuita è determinata dalle impostazioni del port group cui appartiene. È comunque possibile assegnare impostazioni specifiche per ogni singola porta.

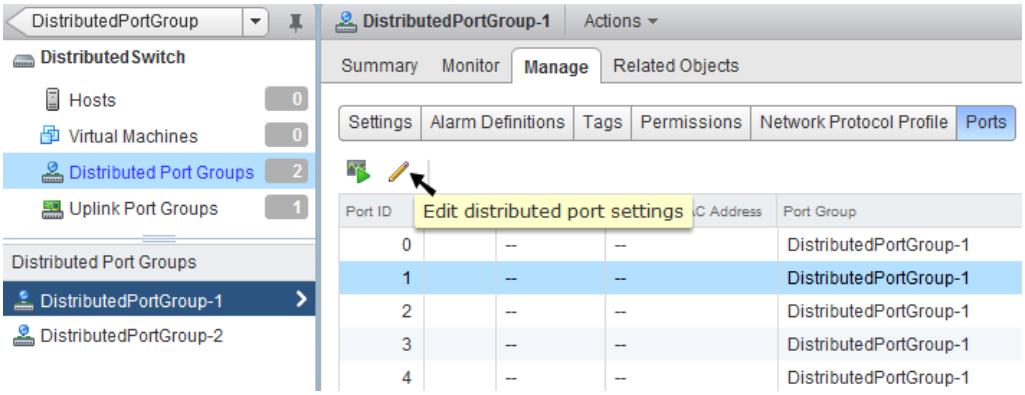
Procedura tramite vSphere Client

- Partendo dal tab **Ports** dello switch distribuito o del port group distribuito, si fa clic su **Edit Settings** nel menu contestuale della porta.



Procedura tramite vSphere Web Client

1. Nel pannello di navigazione a sinistra, individuare lo switch distribuito di proprio interesse, quindi selezionare un port group distribuito.
2. Fare clic sul tab **Manage**, poi su **Ports**, quindi selezionare una porta distribuita dalla tabella.
3. Fare clic su **Edit distributed port settings**.



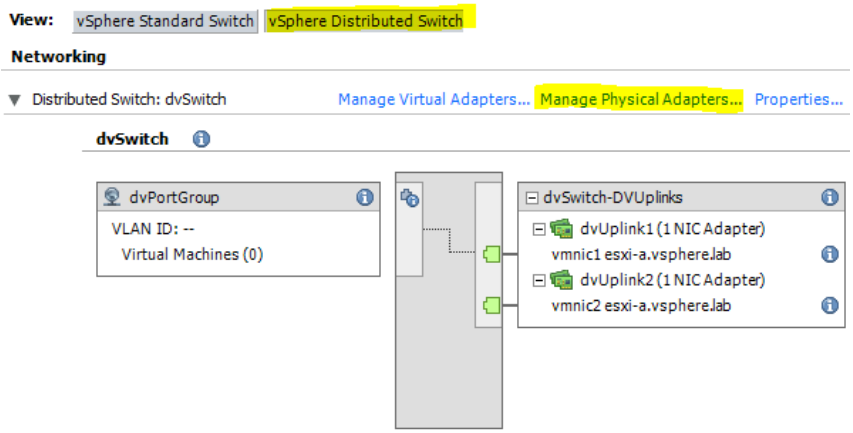
8.7 Gestione delle interfacce di rete negli switch distribuiti

Per ogni host associato ad uno switch distribuito, è necessario dedicare almeno un'**interfaccia fisica** (ossia un **uplink**) allo switch distribuito; è possibile assegnare nuove interfacce fisiche in qualsiasi momento. Per ogni host, si può dedicare una sola interfaccia fisica per ogni porta di uplink dello switch distribuito.

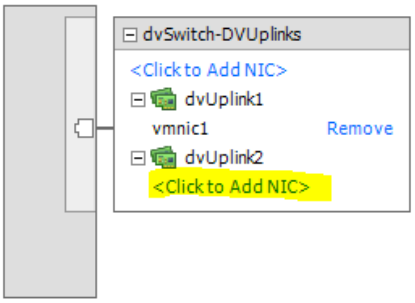
Le **interfacce virtuali** sono invece utilizzate per fornire servizi di rete (ad esempio vMotion o IP storage) attraverso lo switch distribuito. Le interfacce virtuali di uno switch distribuito sono di tipo **VMkernel**. Per ogni host associato allo switch distribuito, si possono creare nuove interfacce VMkernel o migrare quelle esistenti.

Gestione delle interfacce fisiche tramite vSphere Client

1. Nella modalità di visualizzazione **Hosts and Clusters**, selezionare l'host desiderato.
2. Nel tab **Configuration**, fare clic su **Networking**.
3. Selezionare la modalità di visualizzazione **vSphere Distributed Switch** e fare clic su **Manage Physical Adapters**.



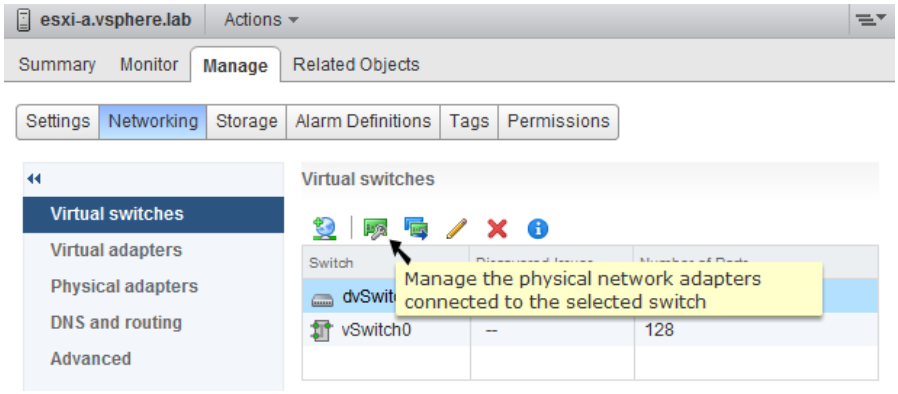
4. Fare clic su **Add NIC** e selezionare l'interfaccia fisica da aggiungere. Se si seleziona un'interfaccia già impegnata su un altro switch, questa sarà rimossa da quello switch e riassegnata allo switch corrente. Per rimuovere un'interfaccia, fare clic su **Remove**.



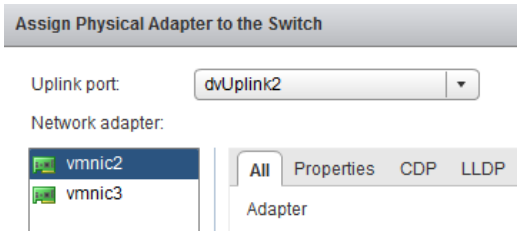
5. Fare clic su **OK** per terminare la procedura

Gestione delle interfacce fisiche tramite vSphere Web Client

1. Nel pannello di navigazione a sinistra, individuare un host, fare clic sul tab **Manage** e selezionare **Networking** > **Virtual Switches**.
2. Selezionare lo switch distribuito desiderato e fare clic su **Manage the physical network adapters**.



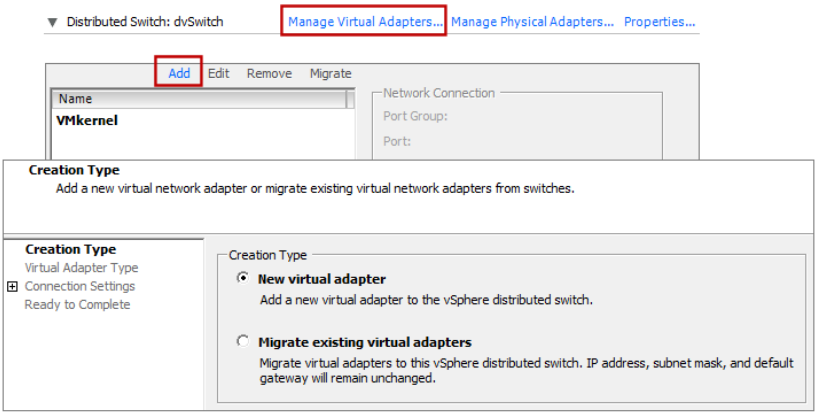
3. Fare clic su **Add adapters** (simbolo "**+**") per aggiungere un'interfaccia fisica (uplink), oppure fare clic su **Remove** (simbolo "**x**") per la rimozione.
4. Se si sta aggiungendo un'interfaccia, selezionarla dalla lista che appare, impostando la porta di uplink di destinazione.



Gestione delle interfacce virtuali tramite vSphere Client

La procedura per creare una nuova interfaccia VMkernel è indicata di seguito.

1. Selezionare un host nella modalità di visualizzazione **Hosts and Clusters**.
2. Nel tab **Configuration**, fare clic su **Networking**.
3. Selezionare la modalità di visualizzazione **vSphere Distributed Switch**.
4. Fare clic su **Manage Virtual Adapters** e fare clic su **Add.**
5. Selezionare la voce **New virtual adapter**.



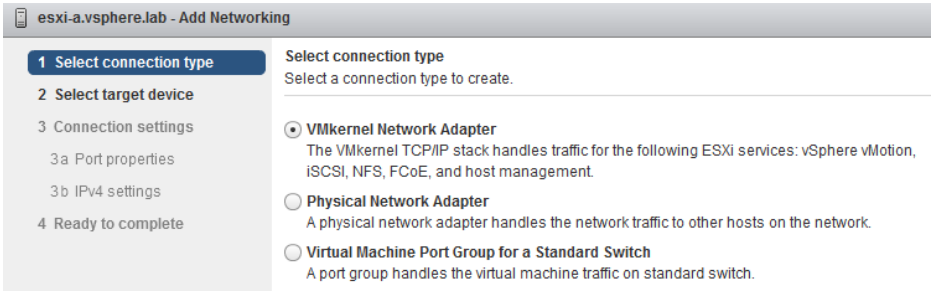
6. Selezionare la voce **VMkernel**, quindi scegliere il port group distribuito o l'ID della porta a cui connettere la nuova interfaccia.
7. Selezionare i servizi che devono essere forniti dall'interfaccia VMkernel: **vMotion**, **Fault Tolerance**, **Management.**
8. Configurare i parametri di rete, andare avanti e fare clic su **Finish**.

Procedura per migrare un'interfaccia già esistente.

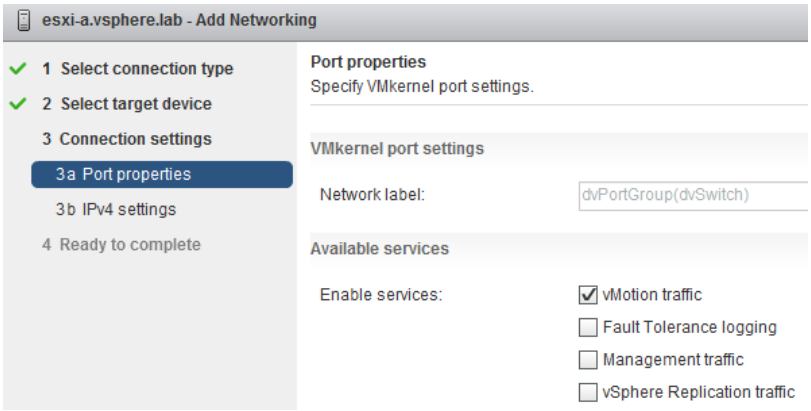
1. Ripetere i passaggi precedenti sino al punto 4.
2. Selezionare la voce **Migrate existing virtual network adapters**.
3. Selezionare una o più interfacce di rete da migrare.
4. Per ogni interfaccia selezionata, specificare il port group di destinazione dal menu a tendina.
5. Andare avanti e fare clic su **Finish**.

Gestione delle interfacce virtuali tramite vSphere Web Client

1. Nel pannello di navigazione a sinistra, selezionare l'host desiderato e fare clic con il tasto destro su di esso.
2. Selezionare le voci **All vCenter Actions** > **Add Networking**.
3. Nella pagina **Select connection type**, selezionare **VMkernel Network Adapter** e fare clic su **Next**.



4. Nella pagina **Select target device**, selezionare un **distributed port group** esistente e fare click **Next**.
5. Nella pagina **Port properties**, selezionare i servizi che devono essere forniti dall'interfaccia VMkernel, e fare clic su **Next**.



6. Configurare i parametri di rete, andare avanti e fare clic su **Finish**

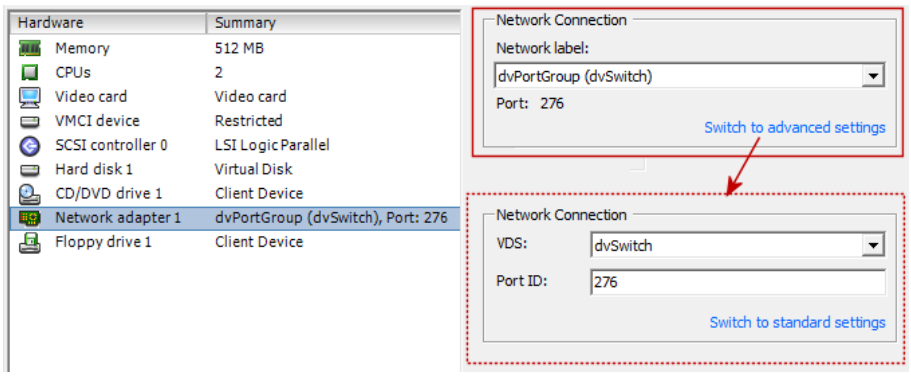
8.8 Connessione di una macchina virtuale ad uno switch distribuito

La connessione di una macchina virtuale ad uno switch distribuito può essere eseguita sia configurando le sue interfacce di rete, sia spostando gruppi di macchine da uno switch standard ad uno distribuito.

Procedura tramite vSphere Client

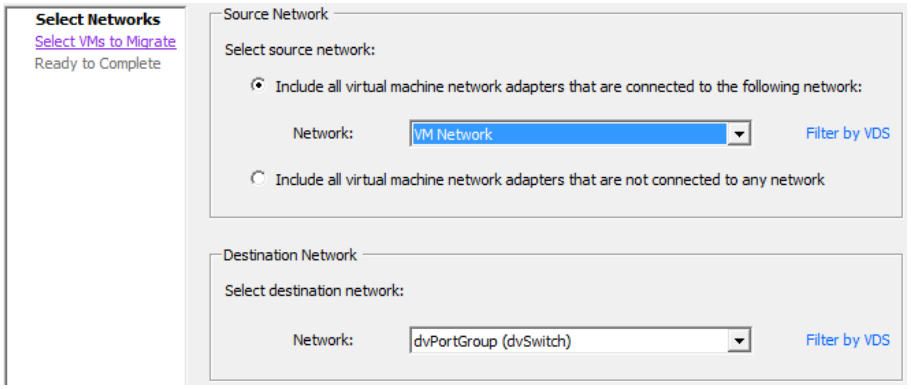
Se si sceglie di configurare le interfacce di rete della macchina virtuale, è sufficiente specificare il port group distribuito oppure l'ID della porta di destinazione per ogni interfaccia.

1. Selezionare la macchina virtuale dall'inventario, fare clic con il tasto destro su di essa e selezionare la voce **Edit Settings**.
2. Nel tab **Hardware**, selezionare un'interfaccia di rete.
3. Selezionare il port group distribuito a cui associare l'interfaccia di rete e fare clic su OK.



Se invece si sceglie di spostare un intero gruppo di macchine virtuali da uno switch standard ad uno distribuito, o viceversa, seguire i passaggi indicati di seguito.

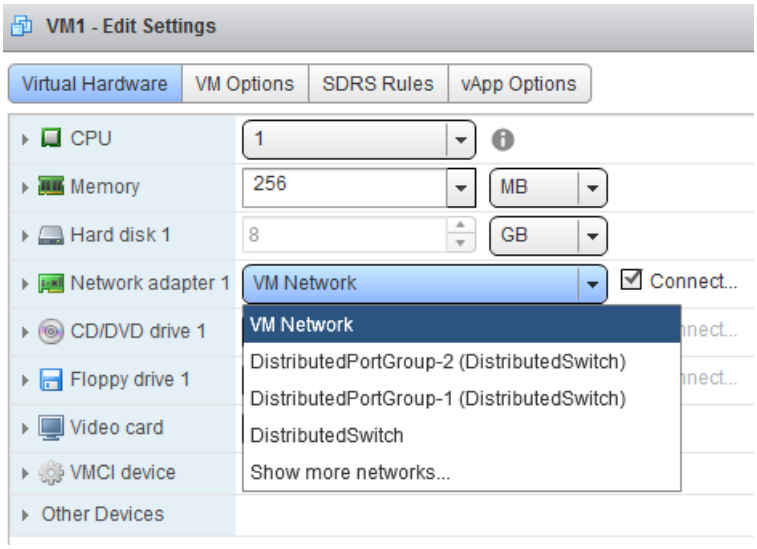
1. Dal percorso **Inventory > Networking**, fare clic con il tasto destro sul Datacenter e selezionare la voce **Migrate Virtual Machine Networking**.
2. Nella procedura di migrazione guidata, selezionare le reti di origine e destinazione, quindi selezionare le macchine virtuali da migrare.



Procedura tramite vSphere Web Client

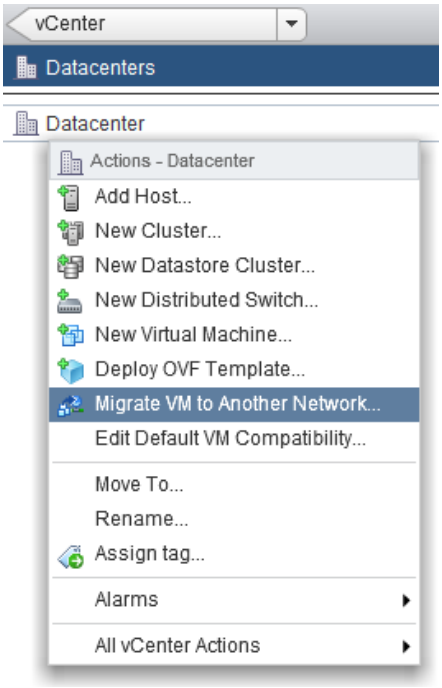
Per configurare le interfacce di rete della macchina virtuale, seguire i passaggi indicati di seguito.

1. Tramite il pannello di navigazione a sinistra, individuare e selezionare la macchina virtuale desiderata e fare clic con il tasto destro su di essa.
1. Fare clic su **Edit Settings** e selezionare un'interfaccia di rete.
2. Selezionare il port group distribuito a cui associare l'interfaccia e fare clic su **OK**.



Per spostare un intero gruppo di macchine virtuali da uno switch standard ad uno distribuito, o viceversa, i passaggi sono indicati di seguito.

1. Nel pannello di navigazione a sinistra, selezionare il datacenter desiderato e fare clic con il tasto destro su di esso.
2. Selezionare la voce **Migrate VM to Another Network**.



3. Nella procedura di migrazione guidata, selezionare le reti di origine e destinazione, quindi selezionare le macchine virtuali da migrare.

Capitolo 9
Lo storage virtuale

9.1 Tecnologie di storage

VMware vSphere supporta diverse tecnologie di storage.

- **Storage locale,** o **Direct-attached storage**, ossia il disco o l'insieme di dischi collegati direttamente (non via rete) a un host ESXi. Lo storage di tipo locale non può essere condiviso fra più host, ed i dati in esso memorizzati sono accessibili solo dall'host che lo detiene. Poiché non prevede la condivisione in rete, non permette di sfruttare alcune importanti tecnologie di alta affidabilità e di bilanciamento automatico dei carichi.
- **Fibre Channel** - è una tecnologia usata nelle Storage Area Network e consente di convogliare i segnali su cavi in fibra ottica. Il protocollo principale di questa tecnologia è il Fibre Channel Protocol (FCP), impiegato per il trasporto dei comandi SCSI sulla rete Fibre Channel.
- **FCoE** - Fibre Channel over Ethernet, standard che permette l'incapsulamento del protocollo Fibre Channel sulla rete Ethernet.
- **iSCSI** - è un protocollo che consente l'impacchettamento dei comandi SCSI su TCP/IP. Il server che vuole utilizzare lo spazio storage offerto da una SAN iSCSI utilizza un client, detto "initiator", che consente di inviare al target (il dispositivo iSCSI) i comandi che consentono di leggere e scrivere sui dischi.
- **NAS** - dispositivo di storage condiviso che rende disponibile in rete lo spazio di memorizzazione tramite protocollo NFS. È importante ricordare che NFS non supporta dischi RDM, poiché non prevede il supporto ai comandi SCSI inviati dal VMkernel in modo diretto tramite mappatura RDM.

Nella tabella seguente vediamo un confronto fra le tecnologie di storage rispetto alle funzionalità supportate.

Funzionalità	Fibre Channel	FCoE	iSCSI	NFS
ESX Boot	Si	Si	Solo se l'Initiator è di tipo Hardware	No
VM Boot	Si	Si	Si	Si
RDM	Si	Si	Si	No
vSphere VMotion	Si	Si	Si	Si
Storage VMotion	Si	Si	Si	Si
vSphere HA	Si	Si	Si	Si
Fault Tolerance	Si	Si	Si	Si

9.1.1 Convenzioni nei nomi dei dispositivi di storage

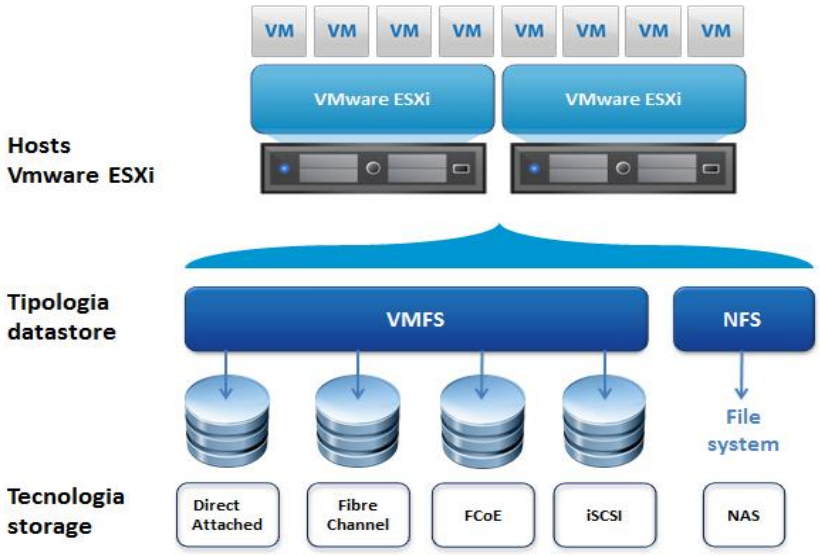
I dispositivi di storage seguono diverse convenzioni per l'identificazione tramite nome.

- **SCSI ID**, ossia l'indirizzo univoco dei dispositivi SCSI.

- **Canonical name**, nelle forme naa.number (Network Address Authority ID), t10.number (secondo specifiche IETF), eui.number (Extended Unique Identifier secondo specifiche IEEE). Se non si ottengono nomi validi dalle unità logiche, viene utilizzato uno spazio dei nomi con prefisso "mpx" seguito dal runtime name.
- **Runtime name**, rappresenta il percorso hardware del dispositivo (es. vmhba1:C0:T1:L3).

9.2 I datastore

Per la memorizzazione delle macchine virtuali, vSphere utilizza unità di memorizzazione chiamate **datastore**. Un datastore è un contenitore logico che si mostra agli host come storage generico, con struttura di memorizzazione sempre uguale, indipendentemente dalla reale tecnologia di storage impiegata. I datastore possono utilizzare due tipi di file system: VMFS e NFS.



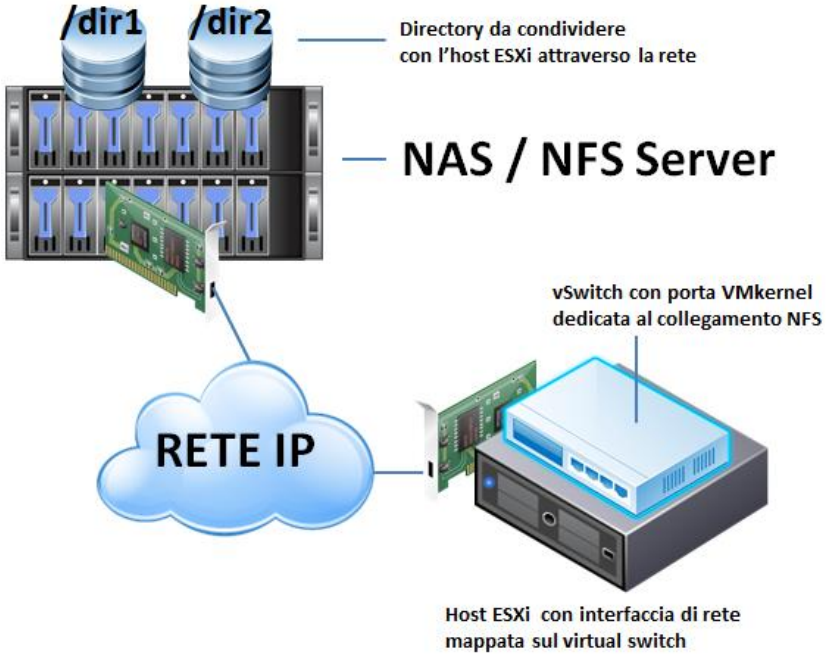
9.2.1 VMFS

VMFS, ora giunto alla **versione 5**, è un file system di tipo "cluster", permette cioè la lettura e la scrittura sullo storage a più host contemporaneamente. Su un singolo datastore VMFS-5 possono essere connessi sino a 64 host ESXi. La precedente versione VMFS-3 permetteva l'impiego di unità non superiori a 2Tb; con VMFS-5 questo limite è stato portato a 64Tb, grazie all'impiego di tabelle di partizione **GPT** (**GUID Partition Table**) in sostituzione del formato **MBR** (**Master Boot Record**). VMFS-5 utilizza una dimensione dei blocchi fissa di **1Mb**, ideale per la memorizzazione di file di grandi dimensioni (come i file dei dischi virtuali), mentre utilizza un indirizzamento per sotto-blocchi (**subblock addressing**) con file di piccole dimensioni, ottimizzando così l'uso dello spazio. Per assicurarsi che una stessa macchina virtuale non sia utilizzata contemporaneamente da più host ESXi, si adotta un meccanismo di blocco distribuito (**block-level distributed locking**). Se un host va in down, il blocco viene rilasciato affinché le macchine virtuali possano essere riavviate su un altro host. Sia chiaro che VMFS è trasparente per le macchine virtuali, nel senso che al loro interno sarà presente il file system del sistema operativo utilizzato.

9.2.2 NFS

NFS è un file system che permette di utilizzare la rete per accedere a dischi remoti come se fossero locali. È reso disponibile da dispositivi NAS, dotati solitamente di un sistema operativo di tipo Unix e di diversi hard disk destinati all'immagazzinamento dei dati. Un sistema di questo tipo è identificabile anche come NFS server.

Un host ESXi accede ad un NFS server tramite porte VMkernel, che permettono di sfruttare il protocollo NFS. La porta VMkernel, configurata con un suo indirizzo IP, deve essere connessa alla stessa rete (logica e fisica) del NAS. Si raccomanda di utilizzare switch virtuali e interfacce di rete dedicate esclusivamente al collegamento NFS, su reti distinte in cui passa solo traffico NFS.



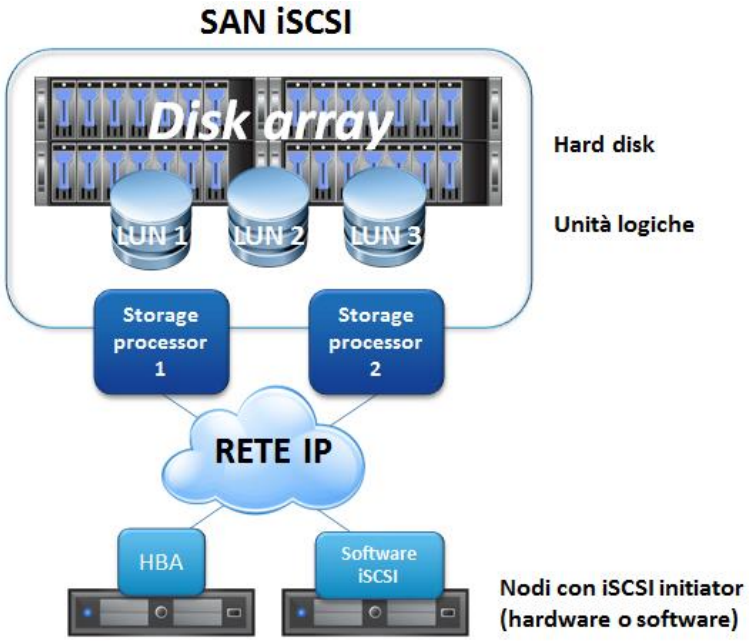
Nell'host ESXi, i privilegi di accesso NFS sono tipicamente assegnati all'utente root; tuttavia, questa impostazione potrebbe risultare problematica con alcuni NAS. Per proteggere i volumi NFS, infatti, in alcune configurazioni è attiva l'opzione "root_squash", con cui il server NFS considera gli accessi root come accessi di utenti senza privilegi. In questo modo un host ESXi sarebbe bloccato nel tentativo di accedere ai file memorizzati nei volumi NFS. Per aggirare il problema, l'amministratore del NAS dovrebbe utilizzare l'opzione "no_root_squash" al posto di "root_squash", insieme ai privilegi di lettura e scrittura, permettendo all'host ESXi di avere accesso completo ai volumi NFS.

9.3 Storage iSCSI

Un sistema di storage basato su iSCSI lavora come una SAN (Storage Area Network), in modo che lo spazio storage sia disponibile a qualsiasi server della rete LAN. Una SAN iSCSI utilizza il protocollo iSCSI (Internet SCSI) per collegarsi alla rete dei nodi che intende servire. Il protocollo iSCSI impacchetta i comandi SCSI su TCP/IP rendendo così possibile l'utilizzo dell'infrastruttura di rete esistente.

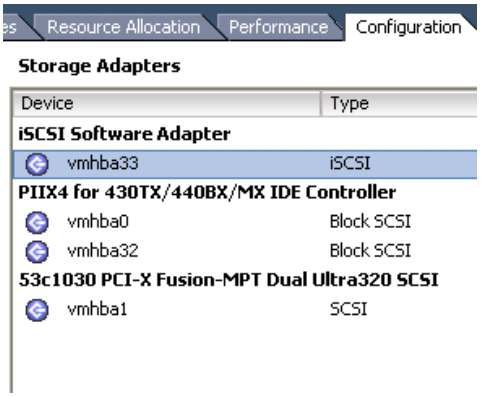
Un host ESXi che vuole utilizzare lo spazio storage offerto da una SAN iSCSI deve utilizzare un client o driver iSCSI, detto **initiator**, implementabile a livello software oppure a livello hardware con interfacce HBA. L'initiator consente di inviare al **target** (il dispositivo iSCSI, nel nostro caso la SAN) i comandi che consentono di leggere e scrivere sui dischi. Sia l'initiator che il target sono definiti **nodi iSCSI**, e sono identificabili tramite un nome univoco, detto **IQN** (**iSCSI Qualified Name**). L'IQN può essere lungo sino a 255 caratteri: prevede il prefisso "iqn", un codice che indica l'anno e il mese in cui il fornitore ha registrato il suo "naming authority string", seguito dallo stesso "naming authority string", infine una stringa opzionale, scelta dal fornitore, preceduta da "**:**".

Un esempio di IQN è il seguente (relativo all'adattatore iSCSI software di un host ESXi):
iqn.1998-01.com.vmware:esx-host1-38114a04



9.3.1 Adattatore iSCSI software

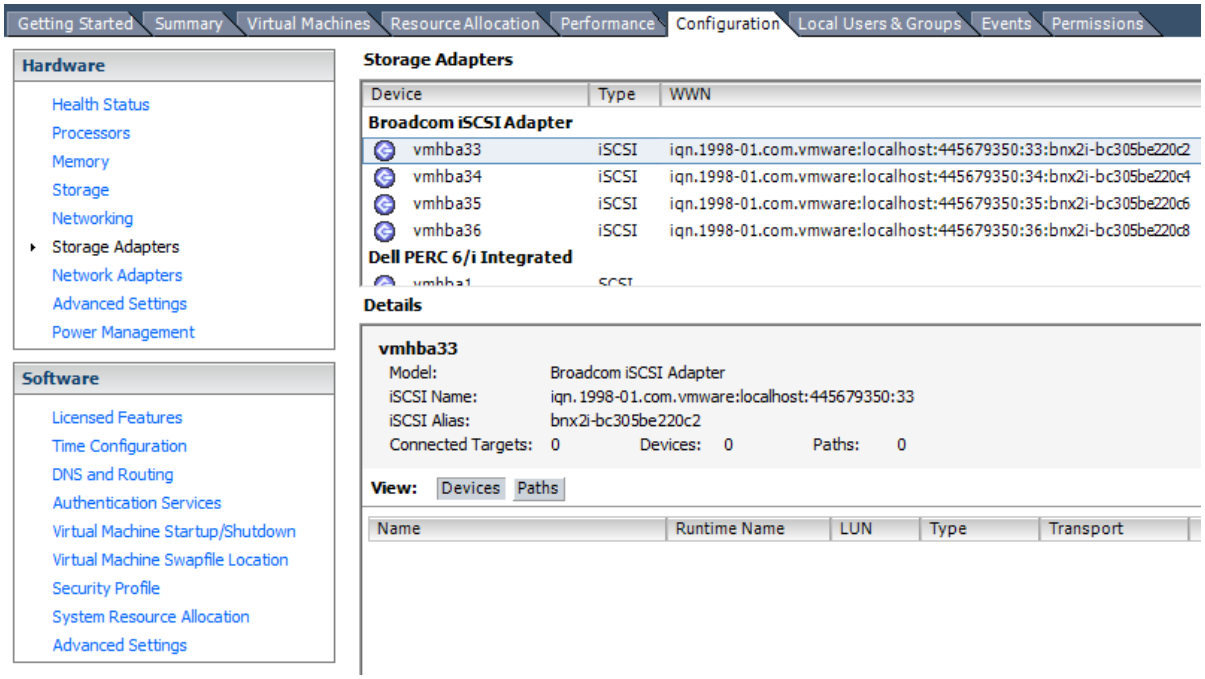
È indicato da VMware come **Software iSCSI adapter** e corrisponde all'**initiator** implementato direttamente nel kernel di vSphere ESXi. Permette all'host di collegarsi ad uno storage iSCSI tramite normali interfacce di rete, consentendo di sfruttare questa tecnologia senza la necessità di acquistare interfacce hardware dedicate. Nell'immagine sotto, possiamo vedere l'adattatore iSCSI software, raggiungibile nel tab **Configuration**, sezione **Storage Adapter**.



9.3.2 Adattatori iSCSI hardware dipendenti

Vengono indicati da VMware come **Dependent Hardware iSCSI Adapter**. Sono interfacce di rete dove parte dello stack iSCSI è implementata in hardware (utilizzando le risorse hardware dell'adattatore), consentendo all'host di risparmiare risorse relative a CPU e memoria. La loro gestione a livello di configurazione di rete dipende da ESXi: indirizzo IP e parametri per instaurare le sessioni iSCSI vanno configurati nella gestione del Networking.

Qui sotto possiamo vedere una scheda Broadcom NetXtreme II 5709 a 4 porte con funzionalità di offload iSCSI: l'host ESXi in questo caso vede quattro adattatori **Dependent Hardware**. Nella sezione **Networking** questa scheda mette a disposizione quattro interfacce di rete.



9.3.3 Adattatori iSCSI hardware indipendenti

Vengono indicati da VMware come **Independent Hardware iSCSI Adapter**, e sono anche chiamati **iSCSI HBA**. Si tratta di interfacce dove tutto lo stack iSCSI è implementato in hardware (utilizzando le risorse hardware dell'adattatore), consentendo all'host ESXi di risparmiare risorse relative a CPU e memoria. L'interfaccia di gestione, necessaria per configurare la parte di networking e lo stack iSCSI, è implementata direttamente sul firmware. Un esempio di adattatore di questo tipo è il QLogic QLA4052.

9.3.4 Considerazioni sugli adattatori iSCSI

Gli adattatori con funzionalità di accelerazione hardware iSCSI (iSCSI Offload Engine), siano essi di tipo **dependent** che **independent**, liberano le risorse del server che sarebbero impiegate nelle operazioni ad alta intensità sui dati, ottimizzando così le prestazioni di I/O sia del server sia dello storage.

In molti casi, specialmente per la piccola e media impresa, l'initiator software integrato nel kernel di vSphere ESXi sarà sufficiente, ma nelle situazioni "importanti" sarà utile utilizzare iSCSI su schede accelerate, che hanno tuttavia costi superiori rispetto alle normali interfacce di rete Ethernet. C'è comunque da rilevare che le prestazioni non dipendono solo dalle interfacce utilizzate, ma anche e soprattutto dalla SAN e dalla rete che collega la SAN agli host. Altri elementi importanti sono il supporto ai Jumbo Frame e il numero di interfacce che si utilizzano per il collegamento alla SAN: sfruttando il multipathing si hanno a disposizione percorsi fisici diversi da utilizzare contemporaneamente per il collegamento tra host e SAN, con notevole miglioramento delle prestazioni.

9.3.5 Configurazione dell'adattatore iSCSI software

Per creare un collegamento iSCSI è necessario predisporre prima il networking, al fine di poter associare le porte VMkernel alle interfacce fisiche. Chiameremo **porte iSCSI** le interfacce VMkernel impiegate per il collegamento iSCSI. In caso di impiego di una sola interfaccia di rete, è necessario creare una porta iSCSI nello switch virtuale connesso all'interfaccia stessa. Nel caso di più interfacce fisiche dedicate al collegamento iSCSI, si dovranno creare tante porte iSCSI quante sono le interfacce fisiche utilizzate (mapping 1 a 1). Si raccomanda di utilizzare sempre switch virtuali e

interfacce di rete dedicate esclusivamente al collegamento iSCSI, e su reti distinte in cui passa solo traffico iSCSI.

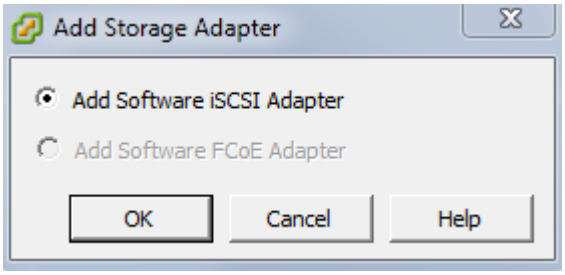
Procedura tramite vSphere Client

Creazione di una porta VMkernel iSCSI

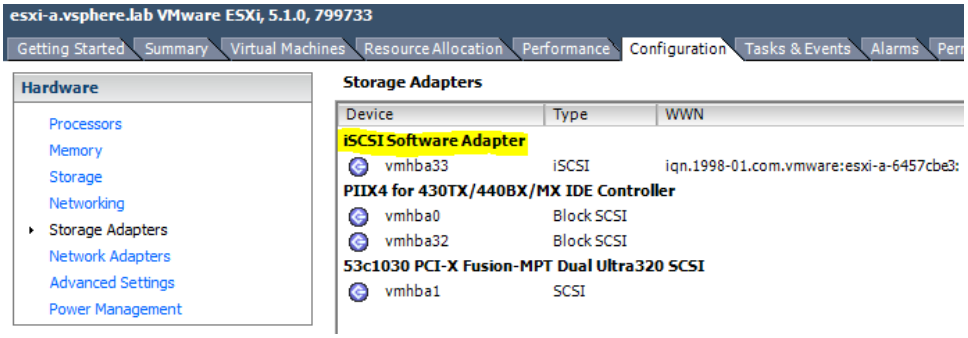
1. Selezionare un host ESXi, andare nel tab **Configuration**, quindi sulle impostazioni del **Networking**.
2. Fare clic su **Add Networking**, selezionare **VMkernel** per il tipo di connessione e andare avanti.
3. Creare un nuovo switch, selezionare l'interfaccia di rete da utilizzare per il traffico iSCSI e andare avanti.
4. Inserire un nome per la porta VMkernel che si sta creando e andare avanti.
5. Specificare le impostazioni IP, andare avanti e fare clic su Finish.

Attivazione dell'adattatore iSCSI software

1. Sempre nel tab **Configuration** dell'host ESXi, fare clic a sinistra su **Storage Adapters**.
2. Fare clic su **Add** in alto a destra, selezionare la voce **Add Software iSCSI Adapter** e fare clic su OK.

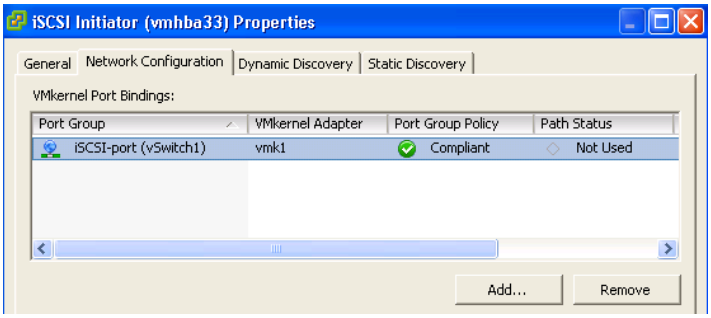


3. L'adattatore iSCSI software (vmhba##) sarà visibile nella lista degli **Storage Adapters**.



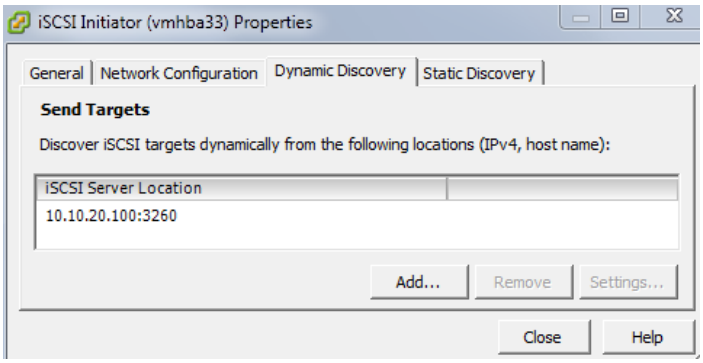
Port binding

1. Fare clic con il tasto destro sull'adattatore iSCSI software e selezionare la voce **Properties**.
2. Nelle opzioni dell'adattatore iSCSI, andare sul tab **Network Configuration**, fare clic su **Add**, selezionare la porta iSCSI creata precedentemente e fare clic su **OK**. Questo passaggio realizza il **binding** (associazione) tra l'adattatore iSCSI software e la porta VMkernel creata precedentemente.

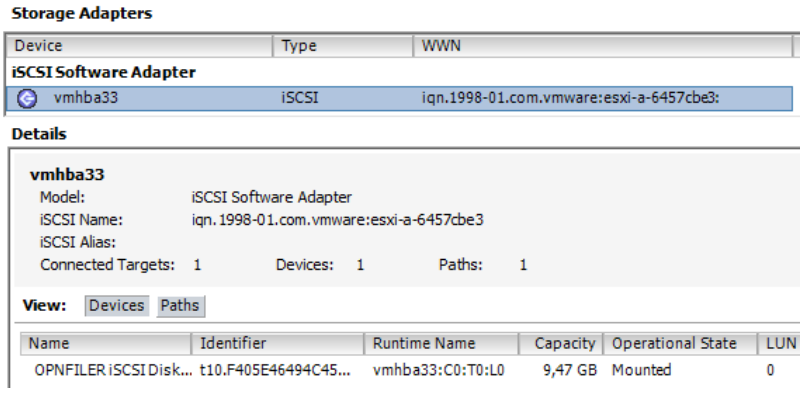


Discovery

1. Sempre all'interno delle proprietà dell'adattatore iSCSI software, andare sul tab **Dynamic Discovery.**
2. Fare clic su **Add** e inserire l'indirizzo IP del target iSCSI, di norma corrispondente allo Storage Processor della SAN iSCSI, quindi fare clic su **OK**.



3. Fare clic su **Close** per terminare la procedura. A questo punto il sistema propone un rescan dell'HBA iSCSI per rilevare le nuove modifiche: al termine della scansione, dovrebbero essere già visibili le LUN configurate sulla SAN.



In generale, la ricerca del target iSCSI prevede due possibili metodi (il primo è quello visto sopra).

- **Dynamic discovery** - modalità chiamata anche "**SendTargets discovery**", ossia l'host contatta lo storage processor della SAN su un preciso indirizzo IP, e la SAN risponde inviando la lista di tutti i target presenti al suo interno.
- **Static discovery** - si utilizza se sono già noti tutti i target.

Terminata la fase di configurazione dell'adattatore, sarà possibile creare un datastore VMFS all'interno di una LUN della SAN iSCSI. Per la procedura, far riferimento più avanti al capitolo "Gestione dei datastore".

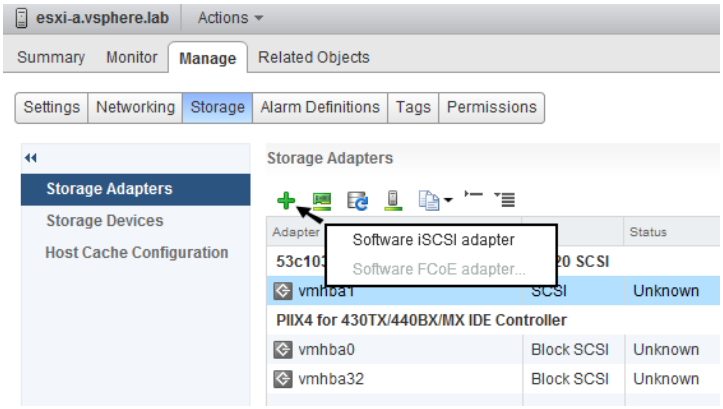
Procedura tramite vSphere Web Client

Creazione di una porta VMkernel iSCSI

1. Nel pannello di navigazione a sinistra, selezionare l'host desiderato e fare clic con il tasto destro su di esso.
2. Selezionare le voci **All vCenter Actions > Add Networking**.
3. Selezionare **VMkernel Network Adapter** per il tipo di connessione e andare avanti.
4. Creare un nuovo switch, selezionare l'interfaccia di rete da utilizzare per il traffico iSCSI e andare avanti.
5. Inserire un nome per la porta VMkernel che si sta creando e andare avanti.
6. Specificare le impostazioni IP, andare avanti e fare clic su **Finish**.

Attivazione dell'adattatore iSCSI software

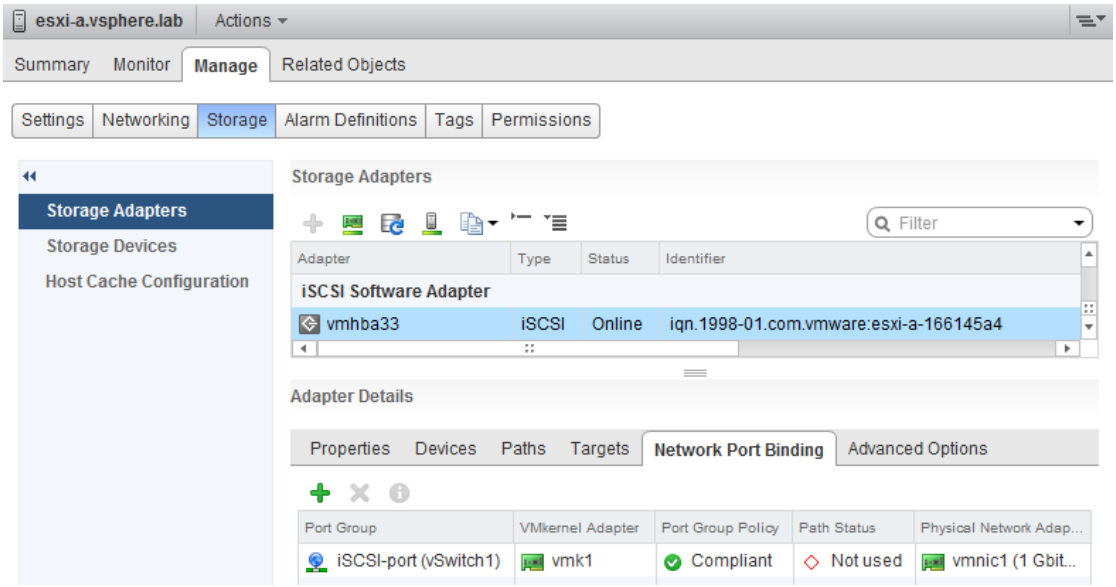
1. Andare nel tab **Manage** dell'host ESXi e fare clic su **Storage**.
2. Selezionare la voce **Storage Adapters** e fare clic su **Add new storage adapter** (simbolo "**+**").
3. Selezionare **Software iSCSI Adapter** e confermare facendo clic su **OK**.



4. L'adattatore iSCSI software (vmhba#) sarà visibile nella lista degli **Storage Adapters**.

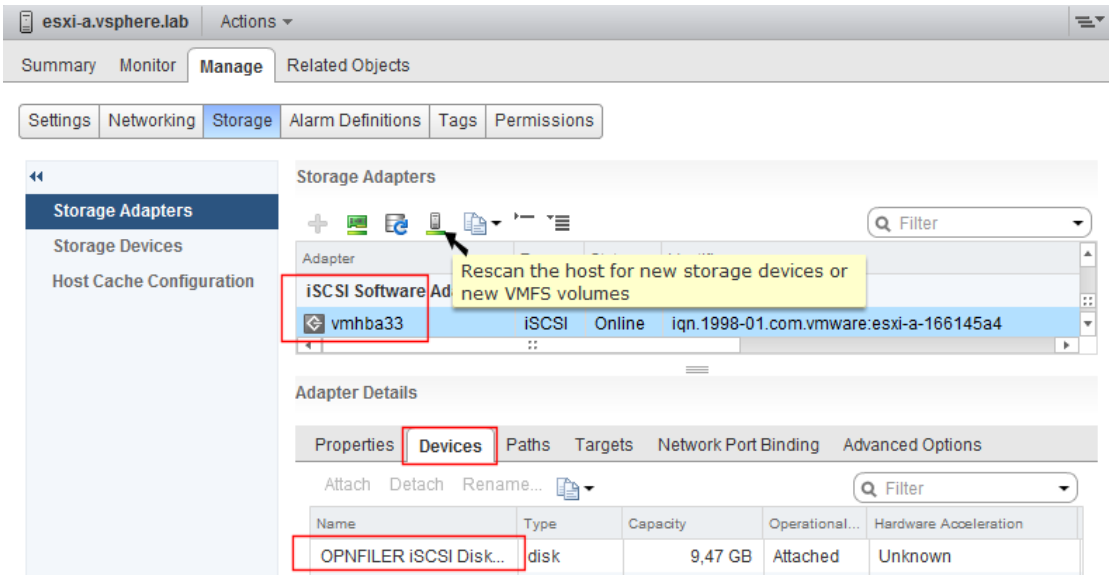
Port binding

1. Nella lista degli **Storage Adapters**, selezionare l'adattatore iSCSI software.
2. Nel riquadro inferiore **Adapter Details**, selezionare il tab **Network Port Binding** e fare clic su **Add**.
3. Selezionare la porta VMkernel iSCSI creata precedentemente e fare clic su **OK**. Questo passaggio realizza il **binding** (associazione) tra l'adattatore iSCSI software e la porta VMkernel creata precedentemente.



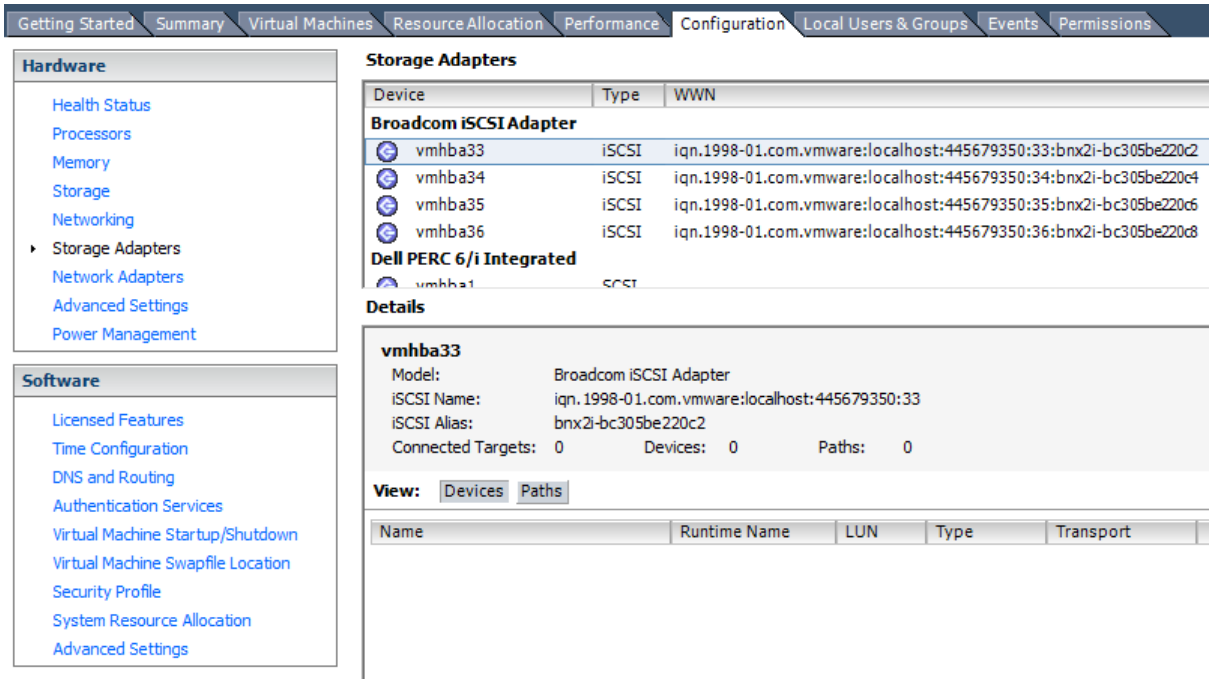
Discovery

1. Sempre all'interno del riquadro **Adapter Details**, spostarsi sul tab **Targets**
2. Selezionare la voce **Dynamic Discovery** e fare clic su **Add**.
3. Inserire l'indirizzo IP del target iSCSI, di norma corrispondente allo Storage Processor della SAN iSCSI, quindi fare clic su **OK**.
4. Eseguire un rescan dell'HBA iSCSI per rilevare le nuove modifiche: al termine della scansione, sotto il tab **Devices** dovrebbero essere già visibili le LUN configurate sulla SAN.



9.3.6 Configurazione di un adattatore iSCSI hardware

Prima di configurare un adattatore iSCSI hardware, bisogna assicurarsi che sia visibile nella lista **Storage Adapters**. Nell'immagine sotto, ad esempio, appare una scheda Broadcom NetXtreme II 5709 a 4 porte con funzionalità di offload iSCSI: in questo caso si tratta di un adattatore "Dependent Hardware" con 4 interfacce di rete.



Successivamente si procede con la creazione di una porta VMkernel iSCSI, con le stesse modalità viste per l'adattatore iSCSI software. Per quanto riguarda il port binding tra un adattatore iSCSI hardware e la porta VMkernel iSCSI, l'aspetto più importante è quello di determinare in modo esatto il nome dell'interfaccia di rete fisica associata all'adattatore iSCSI hardware, affinché l'associazione sia eseguita correttamente.

Per determinare la corretta associazione, nelle proprietà dell'iSCSI Initiator fare clic sul tab **Network Configuration** (con vSphere Client) o **Network Port Binding** (con vSphere Web Client) e fare clic su **Add**. Saranno mostrate le sole interfacce fisiche corrispondenti agli adattatori iSCSI hardware.

Sarà poi necessario configurare uno o più indirizzi per il target discovery (come già visto per gli adattatori software), in modo che l'initiator iSCSI possa individuare le risorse storage disponibili sulla rete.

Terminato la fase di configurazione dell'adattatore hardware, sarà possibile creare un datastore VMFS all'interno di una LUN della SAN iSCSI. Per la procedura di creazione di un nuovo datastore, far riferimento al capitolo "Gestione dei datastore" più avanti.

9.3.7 Multipathing iSCSI

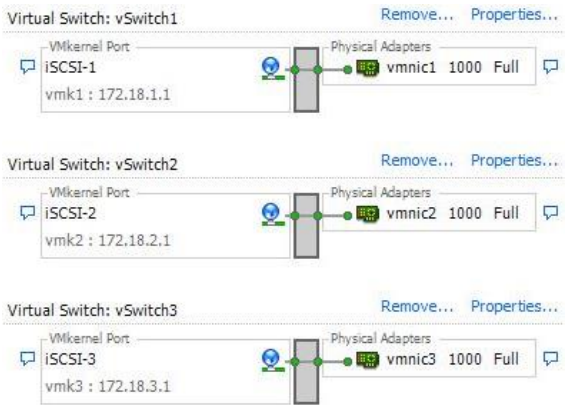
Il multipathing permette di impiegare più percorsi fisici per trasferire i dati tra un host e lo storage, garantendo failover e bilanciamento del carico. Per sfruttarlo, è necessario configurare più interfacce per il collegamento iSCSI e creare tante porte VMkernel iSCSI quante sono le interfacce fisiche utilizzate per la connessione iSCSI. Per ogni porta VMkernel iSCSI, dovrà essere rispettata un'associazione 1:1 tra la stessa interfaccia VMkernel e la corrispondente interfaccia di rete fisica. In sostanza si realizza ciò che viene definito **mapping 1:1**.

Le possibilità sono due:

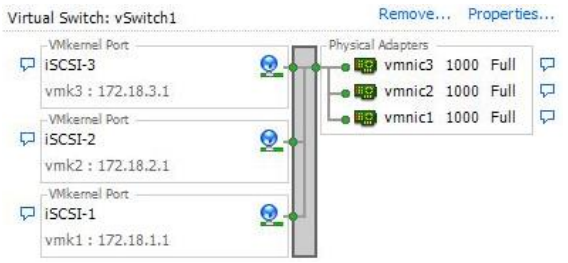
1. creare uno switch standard per ogni porta iSCSI;
2. aggiungere tutte le porte iSCSI in un unico switch standard.

Nel primo caso l'associazione è implicita. Nel secondo caso si dovrà configurare il networking affinché sia attiva una sola interfaccia fisica per ogni porta VMkernel. In maniera predefinita, infatti, per ogni porta VMkernel tutte le interfacce fisiche sono attive contemporaneamente.

1) Collegamento iSCSI su più interfacce di rete con switch multipli.

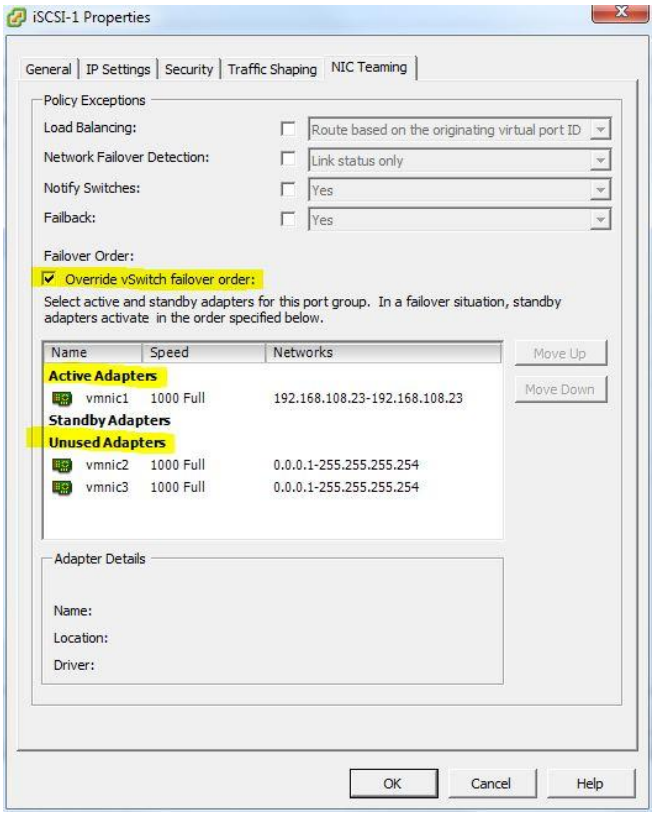


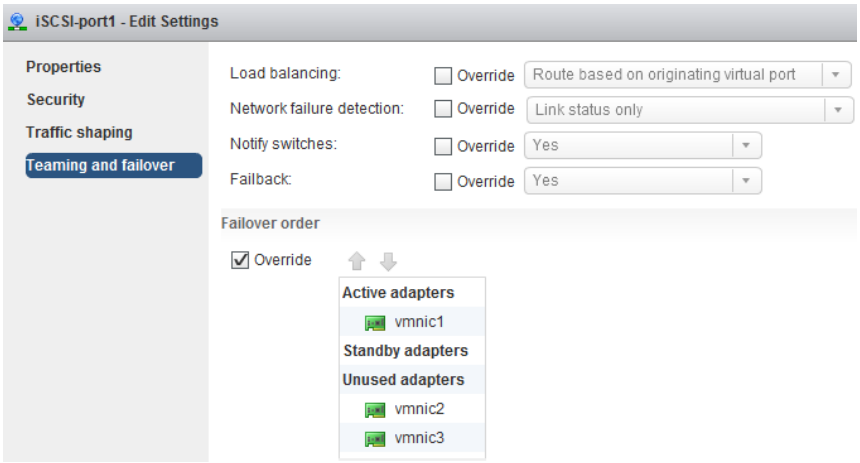
2) Collegamento iSCSI su più interfacce di rete con singolo switch.



Nel secondo caso, sarà necessario mappare ed associare ognuna delle porte iSCSI-1, iSCSI-2, iSCSI-3, alle rispettive interfacce di rete vmnic1, vmnic2, vmnic3. Pertanto, nelle proprietà di ogni porta VMkernel iSCSI, nelle impostazioni di **Teaming** si seleziona la voce **Override vSwitch failover order** e si imposta una sola interfaccia attiva, spostando le altre nel gruppo **Unused Adapters**. Il passaggio appena descritto deve essere ripetuto per ognuna delle tre porte VMkernel.

Qui sotto due immagini di esempio, riferite alla porta iSCSI-1, la prima ottenuta con vSphere Client, la seconda con vSphere Web Client.





9.3.8 Sicurezza iSCSI

Nella rete IP, i dati concernenti il traffico iSCSI non sono cifrati, pertanto è consigliabile adottare un metodo, da applicare a tutti i nodi iSCSI, che renda sicure le connessioni. Un ottimo metodo è quello di implementare il **protocollo di autenticazione CHAP**. Il CHAP verifica periodicamente l'identità dei nodi tramite un processo di handshake a tre vie; la verifica si basa su un segreto condiviso. ESXi supporta l'autenticazione CHAP a livello di **storage adapters**. Sono supportati due metodi CHAP principali:

- **one-way CHAP**, cioè autenticazione unidirezionale, dove il target autentica l'initiator dell'host ESXi e non viceversa;
- **mutual CHAP**, cioè autenticazione bidirezionale, chiamata anche "mutual CHAP", dove si aggiunge un secondo livello di autenticazione in cui **l'initiator autentica il target**.

L'autenticazione one-way CHAP è supportata con tutti i tipi di adattatori iSCSI, mentre l'autenticazione mutual CHAP è supportata solo con gli adattatori iSCSI software e "dependent hardware". Per questi due tipi di adattatori, è prevista inoltre l'autenticazione **per-target CHAP**, che permette di configurare diverse credenziali per ogni target.

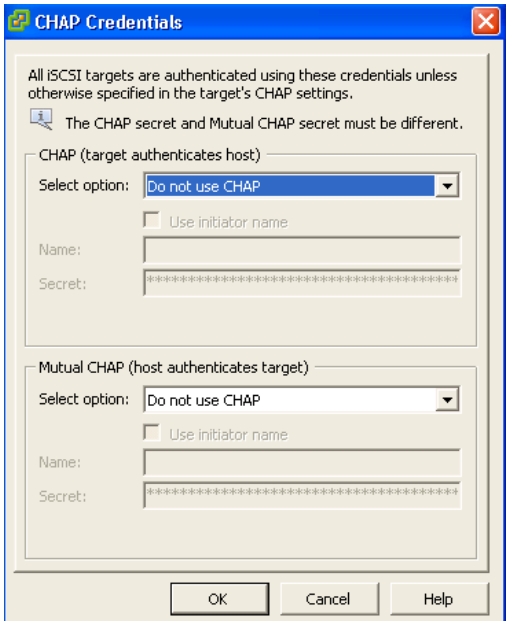
Nell'impostare i parametri del protocollo CHAP, sono possibili le opzioni indicate di seguito.

- **None - Do not use CHAP** - l'autenticazione CHAP non viene utilizzata.
- **Do not use CHAP unless required by target** - l'host non utilizza l'autenticazione CHAP, a meno che non sia richiesta dal target (la SAN iSCSI).
- **Use CHAP unless prohibited by target** - l'host preferisce l'autenticazione CHAP, ma utilizza una connessione non autenticata se il target rifiuta o non supporta CHAP.
- **Use CHAP** - l'autenticazione CHAP deve essere configurata su entrambi i nodi iSCSI.

L'autenticazione CHAP avviene nel solo momento in cui l'host si connette alla SAN. Per tutto il tempo in cui la connessione è attiva, non vi sono nuove autenticazioni, e l'accesso dell'host alla SAN è sempre permesso. Vi è una nuova autenticazione e riconnessione solo a seguito di connessione chiusa da parte dell'host o della SAN.

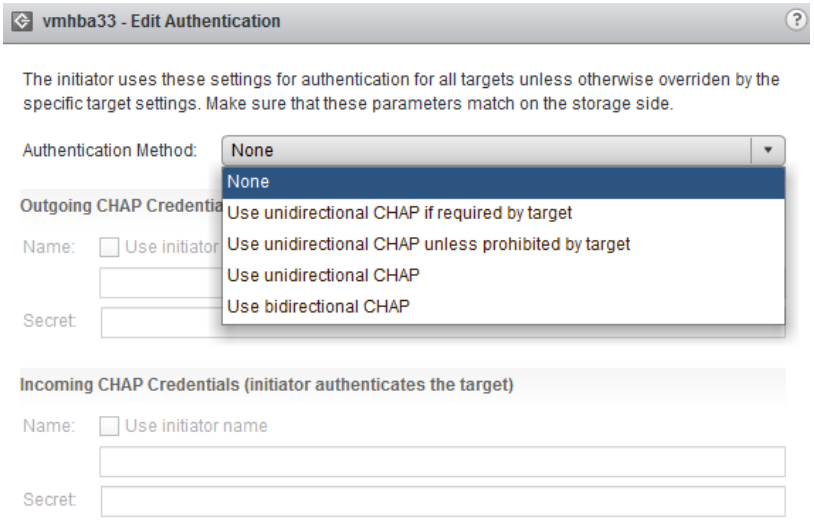
Impostazioni CHAP con vSphere Client

Nella lista degli Storage Adapters, fare clic con il tasto destro sull'adattatore iSCSI. All'interno del tab **General** fare clic sul pulsante **CHAP**.



Impostazioni CHAP con vSphere Web Client

Selezionare l'adattatore iSCSI dalla lista degli Storage Adapters. Nel riquadro **Adapter Details** in basso, selezionare il tab **Properties** e fare clic su **Edit** nella sezione **Authentication**.



9.4 Storage Fibre Channel

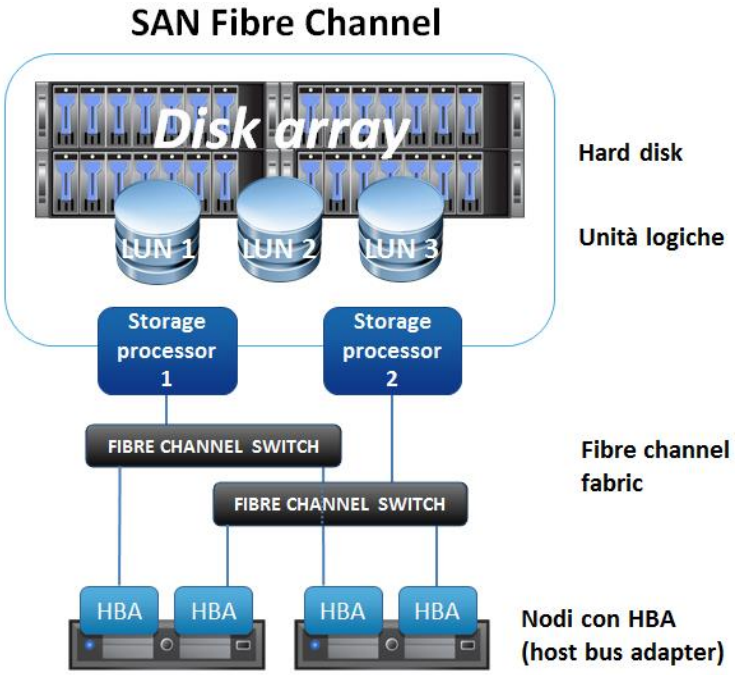
Gli host ESXi supportano sistemi Fibre Channel e sistemi Fibre Channel over Ethernet (FCoE).

Una SAN Fibre Channel si compone degli elementi indicatidi seguito.

- La **SAN** intesa come hardware o sistema si storage - composta da hard disk e uno o più controller (storage processor)
- **LUN** - Logical Unit Numbers, unità logiche identificate da indirizzi numerici. Le unità logiche possono essere dei JBOD, ossia un gruppo di dischi accessibili singolarmente o visibili in modo concatenato, oppure dei set RAID.
- **Storage Processor** – s'interpone tra gli host e i dischi fisici, garantendo connettività front-end ai primi, che in tal modo possono utilizzare lo spazio storage. Dispone di un certo

quantitativo di memoria, divisa in memoria cache di lettura e memoria cache di scrittura: la prima è utilizzata per rispondere alle richieste inoltrate dai server, la seconda per agevolare la scrittura dei server sullo storage.

- **HBA** - l'**host bus adapter**, detto anche host controller o host adapter, è una scheda d'espansione che consente di connettere un host ad una Storage Area Network. Nella rete Fibre Channel è identificato da un **World Wide Name** (**WWN**), simile a un indirizzo MAC Ethernet, in quanto usa un OUI assegnato dall'IEEE. Esistono due tipi di WWN: un WWN nodo, condiviso da tutte le porte dell'adattatore, ed un WWN porta, unico per ciascuna porta. A livello di host ESXi, un HBA viene mostrato nell'elenco degli "storage adapters".
- **Fibre Channel fabric** - è l'insieme di uno o più switch Fibre Channel. Uno switch Fibre Channel permette la connessione degli **HBA** alle unità di storage; ha funzionalità simili a quelle di uno switch ethernet, ma opera sul protocollo Fibre Channel.



Per garantire la disponibilità dei collegamenti allo storage, ESXi supporta il multipathing, per cui in caso di blocco di uno o più elementi quali HBA o switch, sarà possibile raggiungere lo storage attraverso percorsi fisici differenti. Per garantire il multipathing ogni host deve avere due o più HBA, meglio se collegati a due o più switch e due storage processor. Perché il multipathing possa funzionare correttamente, ci si deve assicurare che ogni LUN si presenti con lo stesso ID a tutti gli host.

Tra i requisiti di compatibilità tra SAN Fibre Channel e host ESXi, vi è quello di avere un solo datastore VMFS configurato per ogni LUN della SAN.

9.4.1 Indirizzamento e controllo accessi

Per il controllo degli accessi degli host alle LUN esistono diversi metodi di controllo.

- **Soft zoning** - implementato a livello di switch Fibre Channel, permette il controllo degli accessi alle LUN basandosi sugli identificativi WWN;
- **Hard zoning** - implementato a livello di switch Fibre Channel, permette il controllo degli accessi agli storage processor basandosi sulle porte degli switch;

- **LUN masking** - il controllo accessi si basa sul concedere visibilità di una LUN ad un host. Il LUN masking può essere implementato sia a livello di host ESXi sia a livello di storage processor.

Gli switch Fibre Channel implementano lo **zoning** per impedire il traffico non voluto fra i dispositivi e gli HBA. Lo zoning consente di:

- impedire ad un server non-ESXi di accedere allo storage, e quindi di modificare i dati presenti nelle partizioni VMFS;
- ridurre il numero di LUN e target mostrati ad un host;
- controllare ed isolare determinati percorsi verso lo storage.

9.4.2 Fibre Channel over Ethernet

Per l'accesso a una SAN Fibre Channel attraverso una rete Ethernet si sfrutta il protocollo FCoE, che permette di incapsulare il traffico Fibre Channel all'interno di frame Ethernet.

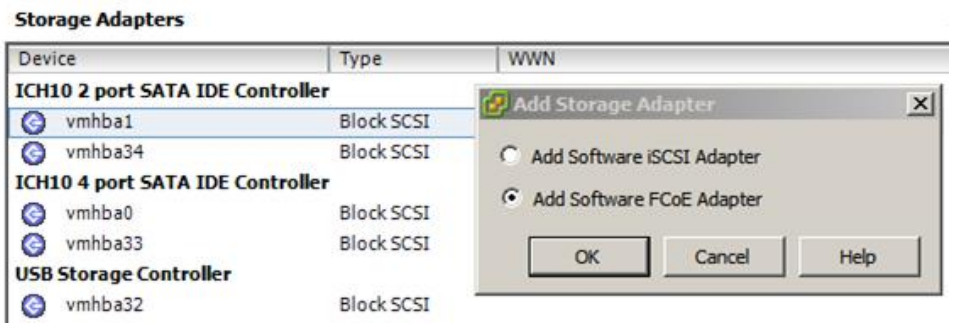
Gli adattatori FCoE utilizzati dall'host ESXi possono essere hardware o software.

- Gli **adattatori hardware** sono chiamati **CNA**, **Converged Network Adapter**, e contengono nella stessa interfaccia sia la componente Ethernet sia quella Fibre Channel. Queste due parti, all'interno di ESXi, appaiono entrambe, ossia la parte Ethernet sarà mostrata nell'elenco "network adapters" (vmnic), la parte Fibre Channel nell'elenco "storage adapters". Nessuna configurazione è richiesta per far funzionare la parte Fibre Channel.
- Gli **adattatori software** sono invece interfacce di rete con supporto hardware ai processi FCoE.

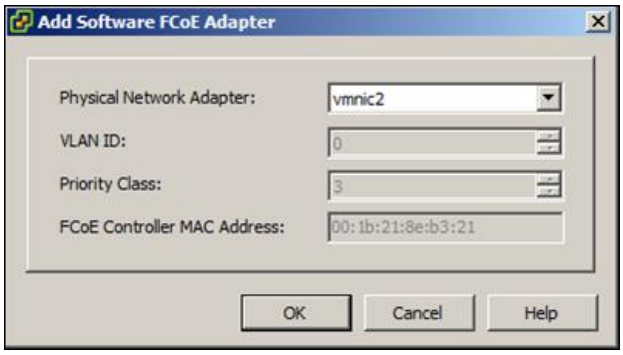
Dopo aver terminato la fase di configurazione degli adattatori FCoE (nei paragrafi successivi l'esempio con l'adattatore FCoE software di ESXi), sarà possibile creare un datastore VMFS all'interno della SAN Fibre Channel. Per la procedura di creazione di un datastore, far riferimento al capitolo "Gestione dei datastore" più avanti.

Configurazione dell'adattatore FCoE software con vSphere Client

1. Selezionare un host ESXi, andare nel tab **Configuration**, quindi sulle impostazioni del **Networking**.
2. Fare clic su **Add Networking**, selezionare **VMkernel** per il tipo di connessione e andare avanti.
3. Creare un nuovo switch, selezionare l'interfaccia di rete (vmnic#) con supporto FCoE e andare avanti.
4. Inserire un nome per la porta VMkernel che si sta creando e andare avanti.
5. Specificare le impostazioni IP, andare avanti e fare clic su **Finish**.
6. Andare nella lista degli **Storage Adapters** ed aggiungere l'adattatore FCoE software (procedura uguale a quella che permette di attivare l'adattatore iSCSI software).



7. Selezionare l'interfaccia fisica da associare all'adattatore FCoE software (nell'esempio sottostante, la vmnic2 è quella con supporto al FCoE).



8. Dopo aver attivato l'adattatore FCoE software, sarà creato automaticamente un nuovo adattatore **vmhba** visibile nella lista degli **Storage Adapters**. A questo punto sarà possibile aggiungere un datastore FCoE dalla sezione Storage.

Configurazione dell'adattatore FCoE software con vSphere Web Client

1. Nel pannello di navigazione a sinistra, selezionare l'host desiderato e fare clic con il tasto destro su di esso.
2. Selezionare le voci **All vCenter Actions > Add Networking**.
3. Selezionare **VMkernel Network Adapter** per il tipo di connessione e andare avanti.
4. Creare un nuovo switch, selezionare l'interfaccia di rete (vmnic#) con supporto FCoE e andare avanti.
5. Inserire un nome per la porta VMkernel che si sta creando e andare avanti.
6. Specificare le impostazioni IP, andare avanti e fare clic su **Finish**.
7. Andare sul tab **Manage** dell'host ESXi e fare clic su **Storage**.
8. Selezionare la voce **Storage Adapters**, fare clic su **Add new storage adapter** (simbolo "**+**") e selezionare l'adattatore FCoE software.
9. Selezionare l'interfaccia fisica da associare all'adattatore FCoE software.
10. Dopo aver attivato l'adattatore FCoE software, sarà creato automaticamente un nuovo adattatore **vmhba** visibile nella lista degli **Storage Adapters**. A questo punto sarà possibile aggiungere un datastore FCoE dalla sezione Storage.

9.4.3 NPIV

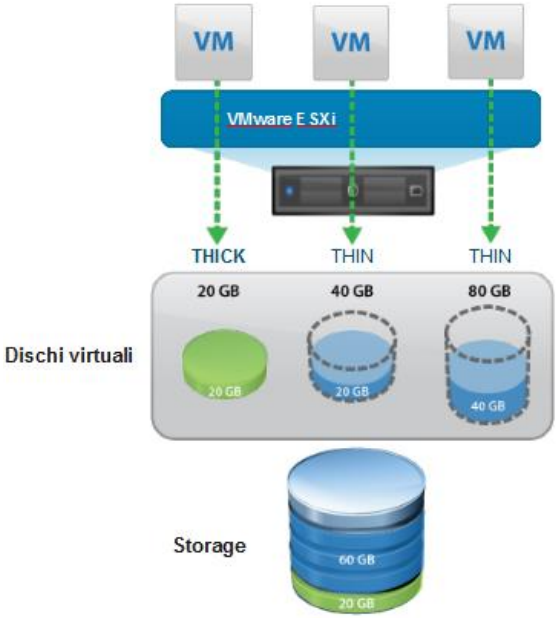
N-Port ID Virtualization (**NPIV**) è uno standard ANSI T11 che descrive come un singolo HBA possa registrarsi in una **Fibre Channel fabric** utilizzando diversi nomi (WWPN). Questo permette a più porte virtuali di condividere una singola porta fisica grazie all'uso di più indirizzi, ognuno dei quali apparirà come entità distinta. Un utilizzo tipico di NPIV è associato all'uso di dischi RDM. Per creare un nuovo NPIV, è necessario modificare alcune impostazioni delle macchine virtuali, nella scheda "Options": infatti l'uso di un RDM in ambiente Fiber Channel non prevede la creazione di un nuovo Fiber Channel NPIV in maniera predefinita. La creazione degli NPIV è possibile solo sugli host collegati a sistemi Fiber Channel che supportano questa funzionalità.

NPIV supporta il vMotion ma non lo Storage vMotion.

9.5 Thin provisioning

VMware vStorage Thin Provisioning consente un utilizzo dinamico dello storage da parte delle macchine virtuali, tramite un'allocazione dello spazio "intelligente" e vantaggiosa per quanto

riguarda i costi di gestione. In sostanza, nel momento in cui si crea un disco virtuale in modalità thin per una VM, lo spazio occupato sullo storage sarà quello effettivamente occupato dai dati della VM, indipendentemente dalla dimensione assegnata al disco virtuale. La dimensione massima del disco non viene allocata interamente sullo storage e il disco crescerà nelle dimensioni in base allo spazio che verrà via via richiesto dalla VM durante il suo ciclo produttivo. Nell'esempio sottostante, la prima VM utilizza un'allocazione completa di tipo THICK, mentre le altre 2 utilizzano un'allocazione dinamica di tipo THIN. Il sistema operativo della prima VM vedrà un disco da 20Gb; all'interno dello storage fisico, il file corrispondente a quel disco sarà grande esattamente 20Gb. I sistemi operativi delle altre 2 VM vedranno rispettivamente un disco da 40Gb ed uno da 80Gb; tuttavia, all'interno dello storage fisico, i file corrispondenti a quei dischi virtuali occuperanno solo 60Gb, ossia la quantità di dati effettivamente necessaria in quel momento alle 2 macchine virtuali.



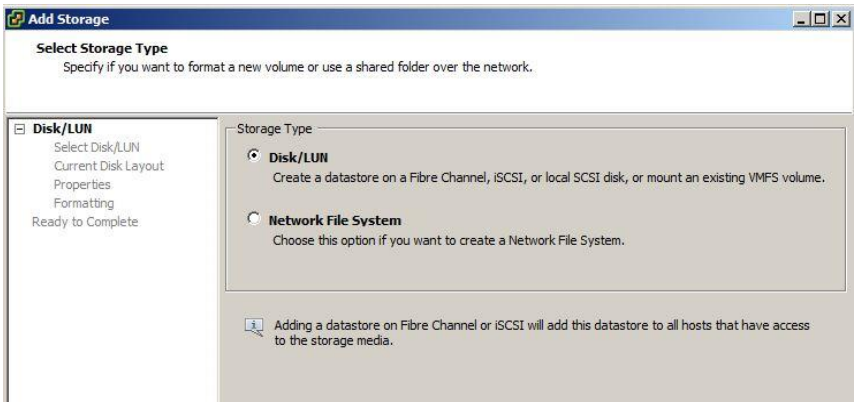
9.6 Gestione dei datastore

9.6.1 Creazione di un datastore VMFS

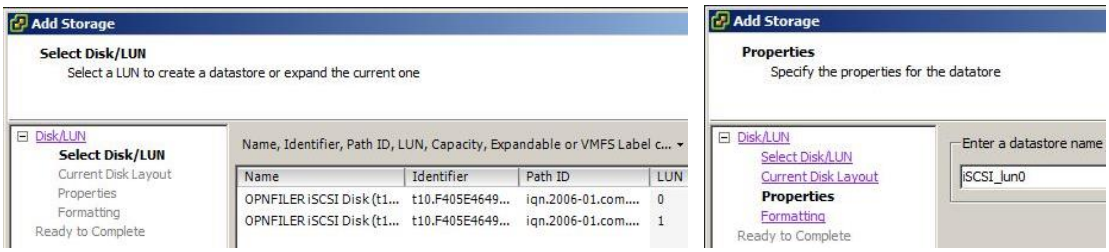
Procedura tramite vSphere Client

Nell'esempio che segue, collegheremo la LUN_0 di uno storage iSCSI ad un host ESXi.

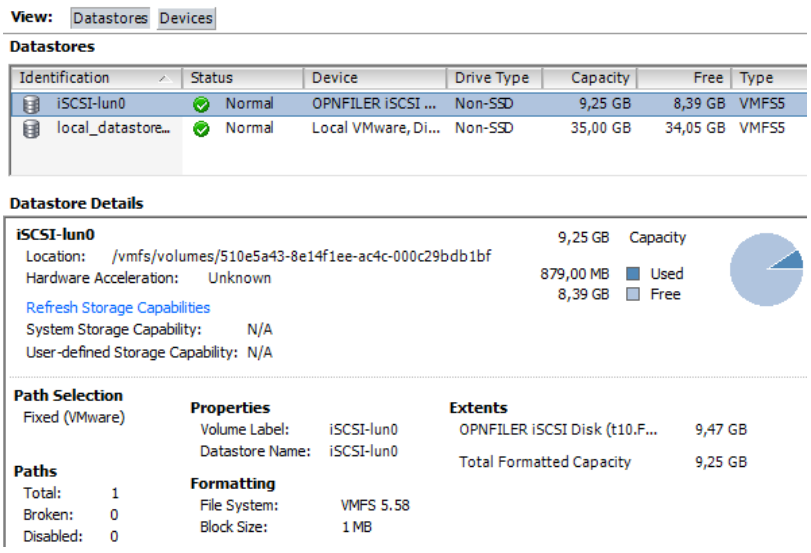
1. All'interno del tab **Configuration** dell'host ESXi, selezioniamo la voce **Storage**, quindi **Add storage** in alto a destra. Per aggiungere un datastore VMFS, selezionare **Disk/LUN**.



2. Selezioniamo la LUN 0 e andiamo avanti.
3. Scegliere la versione del file system, **VMFS3** o **VMFS5**, e andare avanti.
4. Una volta creata la nuova partizione, possiamo assegnarle un nome.

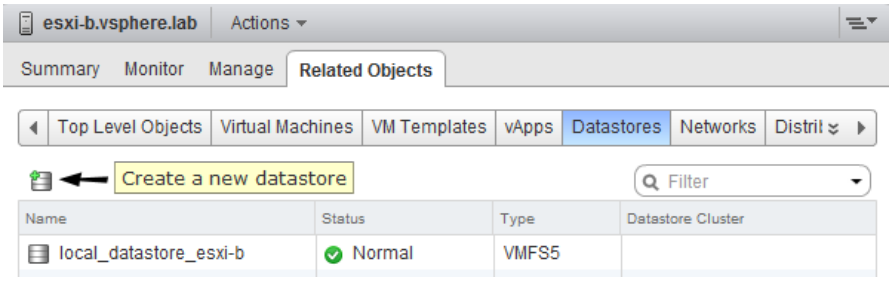


5. Si procede infine con l'impostazione delle dimensioni del datastore.
6. Una volta che il datastore è stato creato, le sue proprietà saranno visibili facendo clic su di esso nella lista dei datastore.

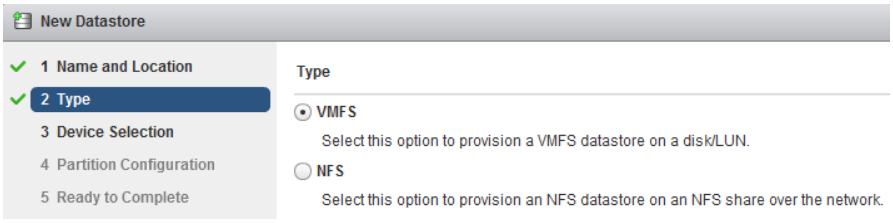


Procedura tramite vSphere Web Client

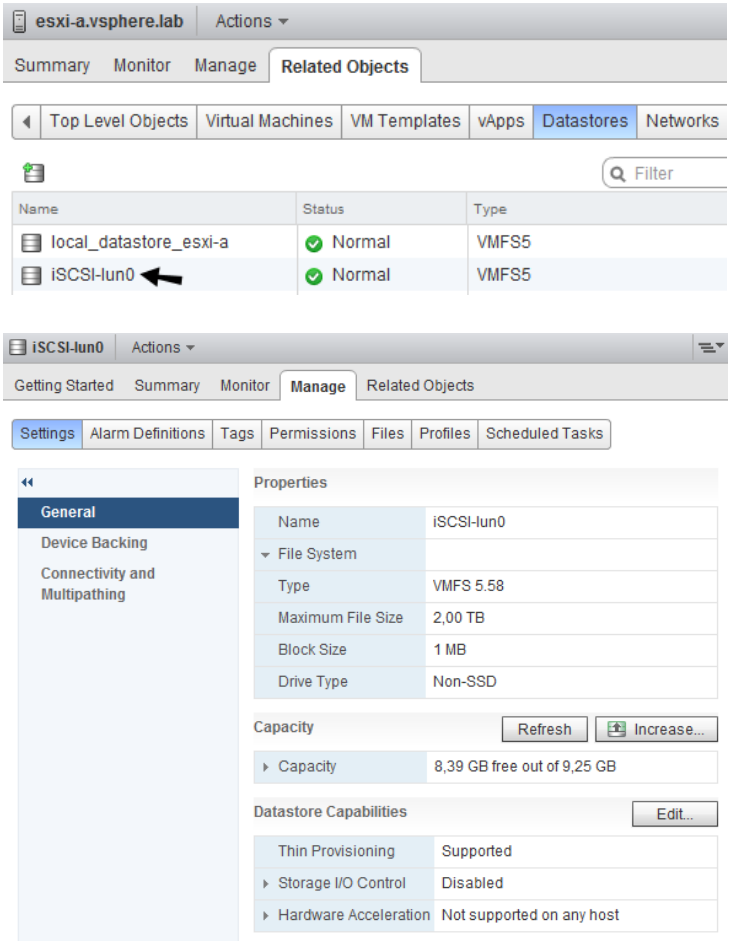
1. Nel pannello di navigazione a sinistra, individuare e selezionare l'host desiderato.
2. Selezionare il tab **Related Objects** e posizionarsi su **Datastores**.
3. Fare clic su **Create a new datastore**.



4. Inserire un nome per il nuovo datastore, andare avanti e selezionare **VMFS** come tipo di datastore.



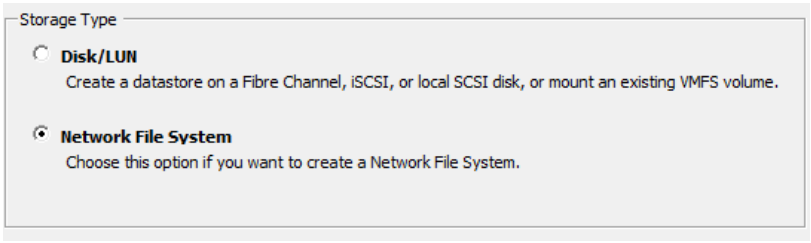
5. Selezionare la LUN desiderata e andare avanti.
6. Scegliere la versione del file system, **VMFS3** o **VMFS5**, e andare avanti.
7. Impostare le dimensioni del datastore, andare avanti e terminare l'operazione.
8. Una volta che il datastore è stato creato, sarà possibile vedere le sue proprietà ed i dettagli facendo clic su di esso nella lista dei datastore.



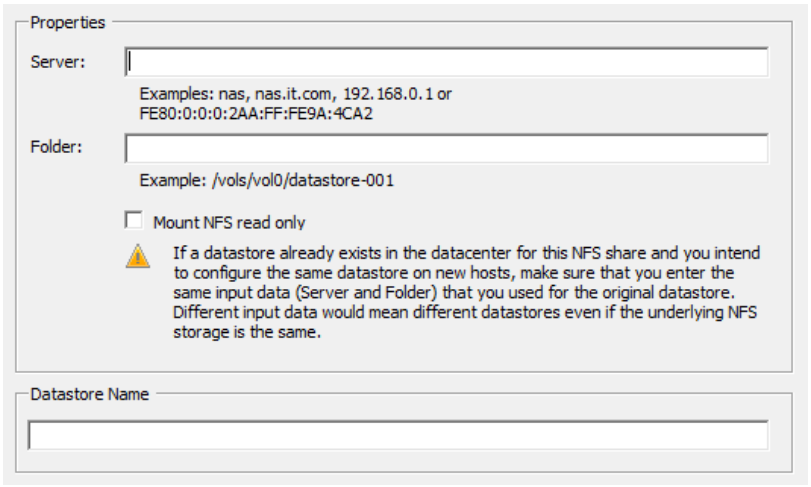
9.6.2 Creazione di un datastore NFS

Procedura tramite vSphere Client

1. Selezionare l'host ESXi dall'inventario, andare nel tab **Configuration**, quindi sulla voce **Storage** presente nella colonna a sinistra.
2. Fare clic su **Add Storage** e selezionare **Network File System**.



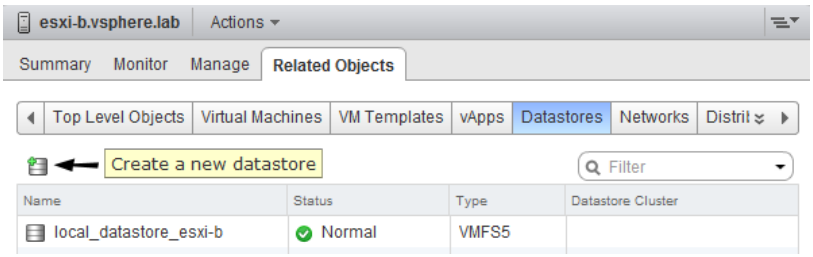
3. Compilare i campi **Server**, **Folder** e **Datastore Name** con gli opportuni valori.



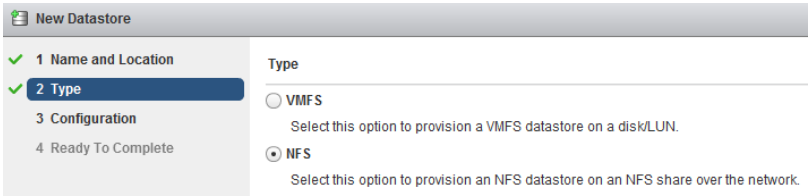
4. Cliccare su **Finish**.

Procedura tramite vSphere Web Client

1. Nel pannello di navigazione a sinistra, individuare e selezionare l'host desiderato.
2. Selezionare il tab **Related Objects** e posizionarsi su **Datastores**.
3. Fare clic su **Create a new datastore**.



4. Inserire un nome per il nuovo datastore.
5. Selezionare **NFS** per il tipo di datastore.



6. Compilare i campi **Server** e **Folder** con gli opportuni valori.

9.6.3 Esplorazione di un datastore

Con vSphere Client, selezionare un host ESXi dall'inventario, andare nel tab **Configuration** e fare clic su **Storage**. Nel riquadro **Datastores**, fare clic con il tasto destro del mouse su un datastore e selezionare la voce **Browse datastore**.

Con vSphere Web Client, individuare e selezionare l'host desiderato dal pannello di navigazione a sinistra. Fare clic sul tab **Related Objects** e selezionare la voce **Datastores**. Fare clic con il tasto destro del mouse su un datastore e selezionare la voce **File Browser**.

9.6.4 Eliminazione di un datastore

Un datastore può essere eliminato o "smontato". L'eliminazione di un datastore comporta:

- la sua rimozione da tutti gli host collegati;
- la sua rimozione dal dispositivo di storage;
- l'eliminazione di tutti i file contenuti al suo interno.

Per eliminare un datastore, fare clic con il tasto destro su di esso, quindi selezionare **Delete** (nel caso di vSphere Web Client , selezionare **All vCenter Actions> Delete Datastore**).

Se si vuole semplicemente scollegare un datastore da uno specifico host, è necessario procedere con l'operazione di **Unmount**: in tal caso il datastore è rimosso, rimanendo tuttavia intatto e visibile a tutti gli altri host collegati ad esso. Per riutilizzarlo sull'host da cui è stato rimosso, si esegue l'operazione inversa di **Mount**.

9.6.5 Datastore overcommitted

Un datastore è definito "overcommitted" quando i dischi in modalità thin-provisioning crescono sino ad allocare una quantità di spazio che va oltre le reali capacità del datastore. In questa situazione, il client vSphere evidenzia il datastore che presenta questo problema. La situazione può essere prevenuta con un attento monitoraggio, impiegando il sistema di allarmi e gli strumenti di reportistica di vSphere. Per risolvere una situazione di datastore overcommited, è possibile impiegare lo Storage vMotion per spostare alcune macchine virtuali su un altro datastore, oppure è possibile aumentare le dimensioni del datastore in uso.

Le dimensioni possono essere aumentate sfruttando una nuova LUN su cui estendere lo spazio del datastore, o espandendo il datastore sino ai limiti della LUN su cui è configurato, ovviamente se è rimasto spazio libero a disposizione nella LUN stessa.

9.7 Accelerazione hardware nello storage virtuale

In ottica di flessibilità, a partire da ESX/ESXi 4.1, VMware ha introdotto l'interfaccia **vStorage APIs for Array Integration** (**VAAI**), che fornisce funzionalità di accelerazione hardware tramite dispositivi di storage con supporto VAAI. L'interfaccia consente di eseguire alcune specifiche operazioni, come la **clonazione di macchine virtuali** o la **migrazione tramite Storage vMotion**, direttamente dalle unità storage, consentendo agli host un risparmio di risorse CPU, memoria e rete.

VAAI prevede il supporto a diverse operazioni fondamentali, dette **primitive**.

- **Atomic Test & Set (ATS)** - funzione eseguita durante la creazione e il blocco di file nei volumi VMFS.
- **Clone Blocks/Full Copy/XCOPY** - funzione utilizzata per copiare o migrare dati all'interno dello stesso storage fisico.
- **Zero Blocks/Write Same** – funzione utilizzata per le operazioni di azzeramento, che consente all'array storage di azzerare quantità elevate di blocchi.
- **Thin Provisioning** - permette agli host ESXi di informare lo storage fisico perché possa reimpiegare in altre LUN lo spazio precedentemente occupato da una VM (cancellata o spostata su un altro datastore).
- **Block Delete** – permette di richiamare spazio sfruttando la funzionalità SCSI UNMAP.

Per ogni datastore e ogni dispositivo di storage, è possibile verificare il supporto all'accelerazione hardware:

- tramite vSphere Client, nella colonna **Hardware Acceleration** (tab Configuration, menu Storage);
- tramite vSphere Web Client, nel blocco **Datastore Capabilities** all'interno delle impostazioni del datastore (entrare nel datastore, fare clic sul tab Manage e selezionare la voce Settings).

Lo stato del supporto può essere **Unknown**, **Supported** o **Not Supported**. Il valore iniziale è Unknown. Lo stato diventa Supported dopo che l'host esegue con successo un'operazione di offload. Se invece l'operazione fallisce, lo stato diventa Not Supported. Tuttavia, se lo storage fornisce un supporto all'accelerazione hardware solo parziale, lo stato rimane Unknown.

9.7.1 Accelerazione hardware per il thin provisioning

L'interfaccia VAAI fornisce supporto negli ambienti che utilizzano il thin provisioning con funzionalità integrate negli array storage, facilitando i meccanismi per il recupero dello spazio inutilizzato e semplificando le attività riguardanti il monitoraggio dello spazio disco.

VAAI Thin Provisioning informa l'array dello spazio che viene liberato, in seguito a operazioni di eliminazione o rimozione di file dal datastore mediante Storage vMotion, o in seguito all'eliminazione o alla migrazione in un altro datastore di un disco virtuale, ad esempio tramite Storage DRS. L'array può quindi recuperare i blocchi di spazio liberati. Inoltre, controlla l'utilizzo dello spazio sulle LUN con thin provisioning per evitare l'esaurimento dello spazio fisico.

9.7.2 La funzione di recupero dello spazio inutilizzato

Da sempre, in occasione della migrazione di macchine virtuali da un datastore, i blocchi utilizzati dalle macchine virtuali stesse prima della migrazione venivano ancora segnalati come "in uso" da parte dell'array. Questo significava che le statistiche di utilizzo dall'array di storage potevano essere fuorvianti e che in tali occasioni poteva verificarsi un notevole spreco di spazio su disco. Grazie alle nuove primitive VAAI, il dispositivo di storage viene informato quando i blocchi non sono più in uso, con conseguente miglioramento della segnalazione del consumo di spazio su disco e possibilità di recupero dei blocchi inutilizzati.

9.7.3 Accelerazione hardware nei dispositivi di storage a blocchi

Se si utilizzano dispositivi di storage a blocchi (Fibre Channel o iSCSI) con supporto all'accelerazione hardware, gli host ESXi sono agevolati in specifiche operazioni.

- **Full copy**, chiamata anche **clone blocks** o **copy offload**. In questo caso lo storage esegue direttamente le operazioni di copia dei dati senza che vi siano attività di lettura e scrittura da parte degli host. L'operazione consente di ridurre il tempo e il carico di rete

durante la clonazione delle macchine virtuali, il provisioning da un template, oppure la migrazione con vMotion.

- **Block zeroing**, chiamata anche **Zero blocks** o **Write Same**. Consente all'array storage di azzerare quantità elevate di blocchi, per allocare nuovo spazio storage, sia esso libero o precedentemente occupato da dati. Permette di ridurre i tempi e i carichi di rete durante la creazione di nuove macchine virtuali e nella formattazione di dischi virtuali.
- **Hardware assisted locking**, chiamata anche **Atomic Test & Set (ATS)**. Permette il locking delle macchine virtuali senza la necessità di impiegare meccanismi di "SCSI reservations". Permette il blocco dei dischi per settore, evitando di bloccare un'intera LUN utilizzando le prenotazioni SCSI.

9.7.4 Accelerazione hardware nei dispositivi NAS

L'accelerazione hardware nei dispositivi NAS è stata introdotta a partire da vSphere 5. Può essere abilitata con l'impiego di plug-in (pacchetti VIB) messi a disposizione dai produttori. Consente agli host ESXi di demandare ai dispositivi NAS diverse operazioni.

- **Full file clone** - operazione simile al **VMFS block cloning**. La differenza sta nel fatto che il NAS clona interi file anziché segmenti di file.
- **Reserve space** – consente allo storage di allocare lo spazio per dischi virtuali in formato thick.
- **Lazy file clone** – consente a VMware View di demandare allo storage la creazione dei "linked clones".
- **Extended file statistics** – consente di demandare allo storage l'elaborazione di accurati report sull'utilizzo dello spazio.

9.7.5 Considerazioni sull'accelerazione hardware

Se si sfrutta l'accelerazione hardware nei dispositivi di storage, è necessario tener conto di alcune condizioni che potrebbero portare ad errori nelle operazioni. I dispositivi di storage restituiscono un errore per ogni funzione non implementata nel loro hardware. Questi errori obbligano l'host ESXi ad utilizzare i suoi metodi nativi per portare a termine le operazioni.

In particolare, il **VMFS data mover** interviene a livello software in queste situazioni:

- datastore sorgente e di destinazione hanno differente dimensione dei blocchi;
- il file sorgente corrisponde ad un disco RDM, mentre il file di destinazione è di tipo standard (non-RDM);
- il disco sorgente VMDK è "eagerzeroed thick", mentre quello di destinazione è di tipo thin;
- il disco sorgente (o di destinazione) VMDK è in un formato "sparse" oppure "hosted";
- la macchina virtuale sorgente ha delle snapshot.

9.7.6 vSphere Storage I/O Control

vSphere Storage I/O Control (**SIOC)** fornisce un meccanismo di controllo dinamico per la gestione dell'accesso alle risorse I/O da parte delle macchine virtuali all'interno di un cluster. Rispetto alle versioni precedenti, dove il supporto era solo per storage FC e iSCSI, a partire da vSphere 5 la funzionalità SIOC è stata estesa anche ad NFS, e in generale ai NAS (Network-Attached Storage).

I benefici più rilevanti sono:

- accesso contemporaneo di più VM allo storage regolato dinamicamente in base alle share, assegnate su disco a livello di VM;
- prestazioni migliori per le applicazioni sensibili alla latenza, che utilizzano molti I/O di piccole dimensioni (minori di 8KB);

- distribuzione di risorse non utilizzate alle VM che ne hanno bisogno, in base alle share assegnate su disco a livello di VM;
- prestazioni migliori per le VM con carichi di lavoro critici, in particolare durante i momenti di congestione sull' I/O.

Lo Storage I/O Control consente di controllare le code di accesso a un datastore condiviso per i dischi di ogni macchina virtuale; tramite la configurazione delle share permette di mantenere gli SLA corretti per le VM business-critical rispetto alle altre VM residenti nel medesimo volume. I valori di share sono gestiti a livello di datastore, con le informazioni condivise tra tutti gli host. Ciò significa che nessuna macchina virtuale deve essere in grado di creare da sola un collo di bottiglia in qualsiasi ambiente, indipendentemente dal tipo di storage condiviso utilizzato. Storage I/O Control riduce automaticamente la velocità di una macchina virtuale che consuma una grande quantità di larghezza di banda I/O quando viene superata la soglia di latenza configurata.

Vi sono tuttavia alcune limitazioni:

- i datastore con SIOC abilitato devono essere gestiti da un solo vCenter Server;
- SIOC non supporta dischi Raw Device Mapping (RDM);
- SIOC non supporta datastore con estensioni multiple (multiple extents);
- lo storage utilizzato deve essere certificato e compatibile con la funzione di Storage I/O Control.

9.7.7 Integrazione dello storage con vCenter Server

Le **vSphere Storage APIs for Storage Awareness** (**VASA**) sono delle API che permettono ai dispositivi di storage di integrarsi con le funzionalità di gestione del vCenter. Con esse è possibile verificare e gestire caratteristiche e funzionalità dello storage direttamente dal vCenter Server. Il sistema VASA può agevolare, ad esempio, il processo di risoluzione dei problemi o le comunicazioni tra vSphere e gli amministratori di storage. Le caratteristiche di storage, come i livelli RAID, thin o thick provisioning, oppure gli stati di replica, possono essere visualizzate nel vCenter Server attraverso funzionalità definite in base al sistema (descrittori per datastore), oppure attraverso attributi esposti tramite Storage Views e SMS API.

L'integrazione tra VASA e gli array di storage è possibile grazie a plug-in creati dai produttori dello storage stesso. I plug-in si integrano nel vCenter Server, riportando tutti i dati degli array nell'interfaccia grafica di vCenter. I dati riguardano il funzionamento dello storage, la configurazione fisica dei datastore e le informazioni sull'utilizzo degli spazi nelle LUN.

9.8 Percorsi multipli per lo storage

Per garantire affidabilità e disponibilità, i sistemi storage di classe enterprise sono generalmente dotati di storage processor doppi, configurabili in modalità **active-active** o **active-passive**. In una configurazione active-active, l'accesso alle LUN è consentito simultaneamente attraverso tutti gli storage processor disponibili. Tutti i percorsi sono attivi contemporaneamente (finché un percorso non è più disponibile). In una configurazione active-passive, solo uno storage processor rimane attivo e fornisce l'accesso alle LUN, mentre l'altro attende in modalità passiva (diventa attivo solo in caso di errore del primo).

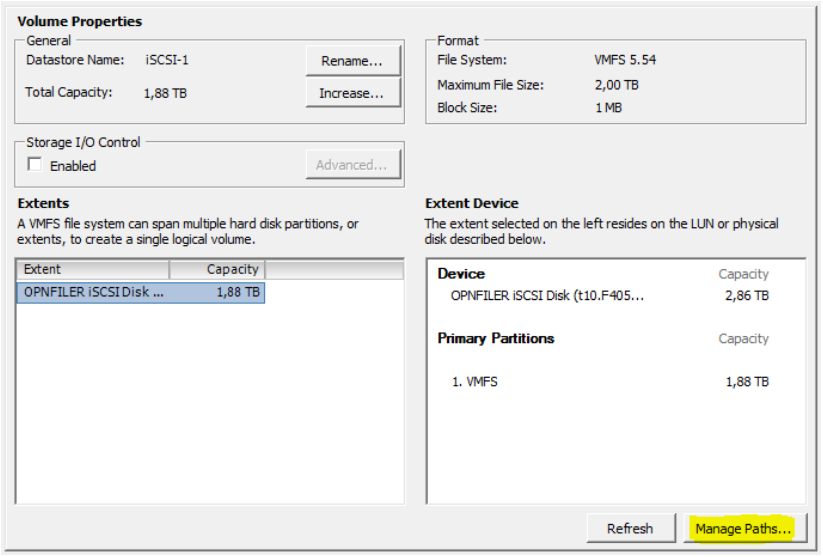
VMware offre bilanciamento dei carichi e meccanismi di failover nativi, con possibilità di impostare diverse politiche di gestione dei percorsi.

- **Fixed** - l'host usa sempre il percorso preferito, finché questo è disponibile, diversamente prova con percorsi alternativi. È la politica predefinita nelle configurazioni active-active.

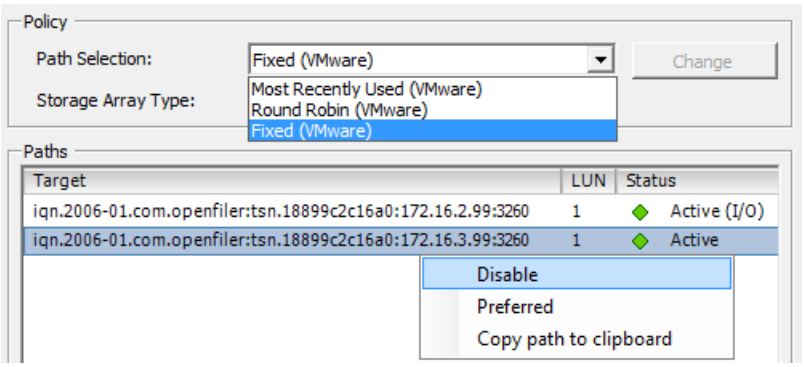
- **Most Recently Used** (**MRU**) - l'host segue il percorso utilizzato più recentemente, finché questo non è più disponibile. In questo caso si utilizza un nuovo percorso, e fino a quando sarà disponibile il nuovo percorso non ne verranno presi in considerazione altri, neanche quello di origine quando dovesse tornare disponibile.
- **Round Robin** - l'host impiega un algoritmo con cui seleziona a rotazione tutti i percorsi disponibili. Oltre al failover del percorso, la politica di Round Robin prevede il bilanciamento dei carichi su tutti i percorsi. L'algoritmo di Round Robin deve essere supportato dallo storage.

Gestione dei percorsi con vSphere Client

1. Aprire la finestra delle proprietà del datastore di proprio interesse e fare clic su **Manage Paths**.

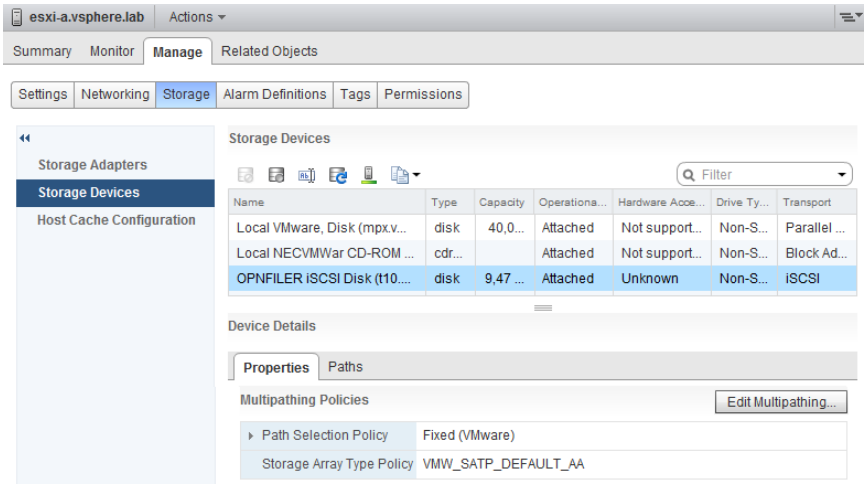


2. Dal menu **Path Selection**, scegliere la politica di gestione dei percorsi. Se è stata scelta una politica di gestione di tipo Fixed, sarà possibile impostare manualmente un percorso preferito; questa possibilità non è prevista con MRU e Round Robin. In tutti i casi è possibile disabilitare un percorso, ad esempio per esigenze di manutenzione sullo storage.

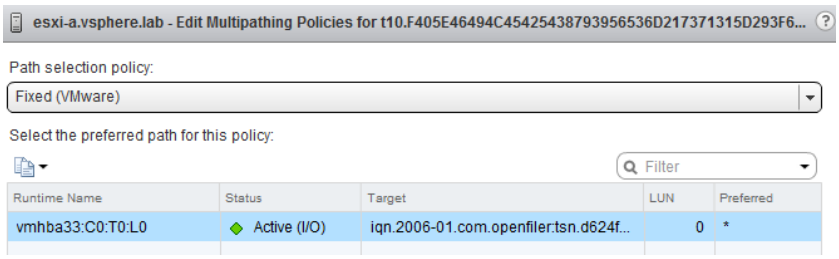


Gestione dei percorsi con vSphere Web Client

1. Nel pannello di navigazione a sinistra, individuare e selezionare l'host desiderato.
2. Selezionare il tab **Manage** e fare clic su **Storage**.
3. Fare clic su **Storage Devices** e selezionare il dispositivo per il quale gestire i percorsi.
4. Fare clic su **Edit Multipathing** nel riquadro più in basso.



5. Dal menu **Path Selection**, scegliere la politica di gestione dei percorsi.



9.8.2 Path failover

Il Path Failover si verifica quando il percorso attivo verso una LUN cambia, di solito a causa di un guasto di un elemento della SAN lungo quel percorso. Quando il percorso attivo non è più disponibile, **le operazioni di I/O dello storage possono interrompersi per un intervallo compreso tra 30 e 60 secondi**, fino a quando l'host determina che il collegamento non è più disponibile e porta a termine la procedura di failover, con la scelta di un altro percorso. In quella fase, se si tenta di visualizzare l'host, oppure i suoi dispositivi di storage, o le sue interfacce di rete, le operazioni potrebbero apparire in stallo, e le macchine virtuali potrebbero non rispondere. Completata la procedura di path failover, le operazioni di I/O dello storage e le macchine virtuali riprenderanno il loro normale funzionamento.

Capitolo 10
Le macchine virtuali

10.1 Hardware di una macchina virtuale

La virtualizzazione permette di ospitare più sistemi operativi all'interno di una stessa macchina fisica, razionalizzando e ottimizzando l'hardware grazie a meccanismi di distribuzione delle risorse disponibili. La virtualizzazione rende possibile astrarre gli elementi hardware (hard disk, ram, CPU, interfacce di rete) e renderli disponibili sotto forma di risorse virtuali. L'insieme di queste risorse virtuali prende il nome di **macchina virtuale**, o **Virtual Machine** (**VM**). Su una macchina virtuale può essere installato un sistema operativo e le relative applicazioni; più macchine virtuali possono girare contemporaneamente su una stessa macchina fisica.

Tutte le macchine virtuali hanno una certa uniformità per quanto riguarda il tipo di hardware, aspetto che rende possibile il loro spostamento attraverso le diverse piattaforme di virtualizzazione VMware. L'elenco che segue descrive nel dettaglio gli elementi hardware che caratterizzano una VM.

10.1.1 CPU

Una VM in esecuzione su VMware ESXi può essere configurata con una o più CPU virtuali. Tuttavia non possono essere assegnate più CPU di quelle presenti nell'host ESXi (CPU logiche, ossia il prodotto tra numero di socket e numero di core). Se l'host e la licenza in uso lo consentono, è possibile avere sino a un massimo di 64 CPU per VM (ESXi 5.1).

10.1.2 Hard Disk

Una VM ha di norma almeno un disco. Durante la creazione del primo disco, viene aggiunto implicitamente anche un controller SCSI per la connessione del disco virtuale. L'adattatore SCSI può essere di diversi tipi:

- BusLogic Parallel;
- LSI Logic Parallel;
- LSI Logic SAS;
- VMware Paravirtual.

La scelta dell'adattatore viene effettuata automaticamente e si basa sul tipo di sistema operativo indicato per la VM durante la sua creazione.

10.1.3 Interfacce di rete

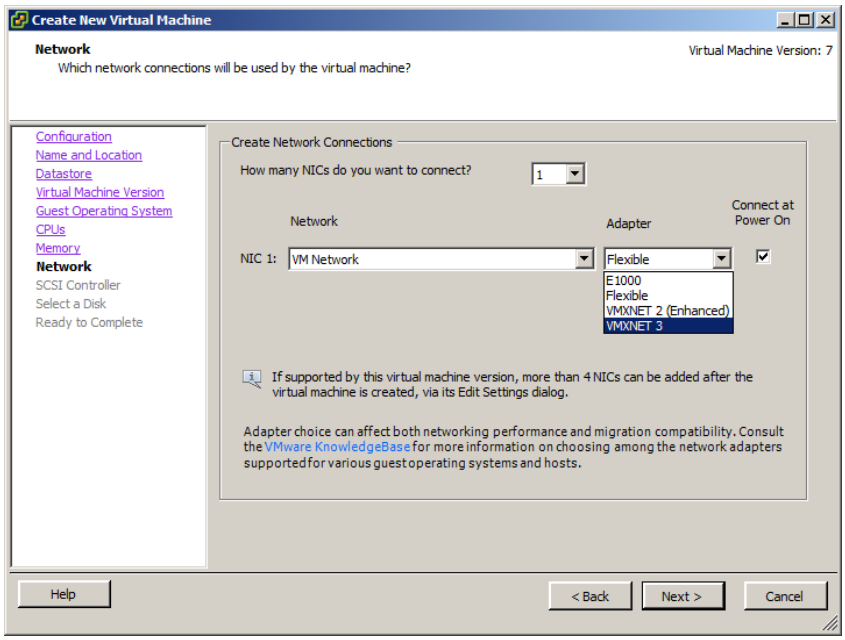
Di seguito l'elenco dei diversi tipi di interfacce di rete virtuali.

- **Flexible -** quando, durante la creazione di una VM, si seleziona l'adattatore di rete in modalità "flessibile" (Flexible Adapter), la macchina virtuale utilizzerà un'interfaccia **vlance** se i VMwaree Tools non sono installati, mentre utilizzerà un'interfaccia **vmxnet** dopo l'installazione degli stessi.
    - **vlance -** è un dispositivo virtuale che fornisce l'emulazione delle interfacce Ethernet Lance AMD pcnet32. È compatibile con la maggior parte dei sistemi guest a 32-bit.
    - **vmxnet -** è un dispositivo paravirtualizzato, progettato specificatamente per operare in un ambiente virtuale. I suoi driver non sono presenti nativamente nei

sistemi operativi guest, per questo è necessaria l'installazione dei VMware Tools. Supporta sistemi sia a 32bit che a 64bit, e supporta funzioni avanzate come TCP Segmentation Offload (TSO) e Jumbo Frames.

- **E1000** - è un dispositivo virtuale che fornisce l'emulazione dell'adattatore di rete Intel 82545EM Gigabit Ethernet (E1000). I driver di questo adattatore sono presenti nella maggior parte dei sistemi operativi. Viene scelto automaticamente da vSphere se durante la creazione della VM si specifica un sistema operativo a 64 bit.
- **VMXNET 2** (Enhanced vmxnet) - si basa sull'interfaccia vmxnet, ma presenta funzioni aggiuntive come il supporto ai jumbo frame e all'hardware off-load. Così come l'interfaccia vmxnet, anche la vmxnet2 necessita dei VMware Tools.
- **VMXNET 3** - rappresenta l'ultima versione di interfacce di rete paravirtualizzate. A livello di progettazione non ha riferimenti con le interfacce vmxnet e vmxnet2. Offre comunque le stesse funzionalità disponibili nella vmxnet2, con in più il supporto al multiqueue (conosciuto in Windows come Receive-Side Scaling), all'offload su IPv6, ed all' MSI/MSI-X interrupt delivery. Quest'interfaccia è supportata da un limitato numero di sistemi operativi, ed è disponibile solo su VM con **hardware versione 7** o superiore. VMware consiglia l'uso dell'adattatore VMXNET3 ogni qualvolta sia possibile il suo impiego, perché garantisce le migliori prestazioni fra tutte le interfacce di rete virtuali.

Nell'immagine qui sotto, possiamo vedere la fase di creazione di una VM (in modalità avanzata) in cui viene chiesto che tipo di interfaccia di rete utilizzare.



In generale, per tutte le interfacce di rete virtuali, funzioni tipiche delle reti fisiche come velocità e impostazioni duplex non hanno rilevanza, perché tutto il processo di trasferimento dei dati avviene nella RAM dell'host ESXi, istantaneamente e senza possibilità di collisioni.

Importante: la velocità di rete riportata dai sistemi operativi delle macchine virtuali non riflette necessariamente la reale velocità sull'interfaccia di rete fisica. Ad esempio, può succedere di impiegare un'interfaccia **vlance** e rilevare che il sistema operativo riporti una velocità di 10Mbps, nonostante l'interfaccia fisica di appoggio sia a 1Gbps. Il problema è dato dall'emulazione, tuttavia ESXi non sarà limitato a una velocità di soli 10Mbps, ma trasferirà i pacchetti alla massima velocità concessa dall'adattatore di rete fisica, nel nostro esempio a 1Gbps.

10.1.4 Memoria RAM

La quantità massima di memoria RAM assegnabile a una VM è di 1Tb (ESXi 5.1).

10.1.5 Altri dispositivi e interfacce

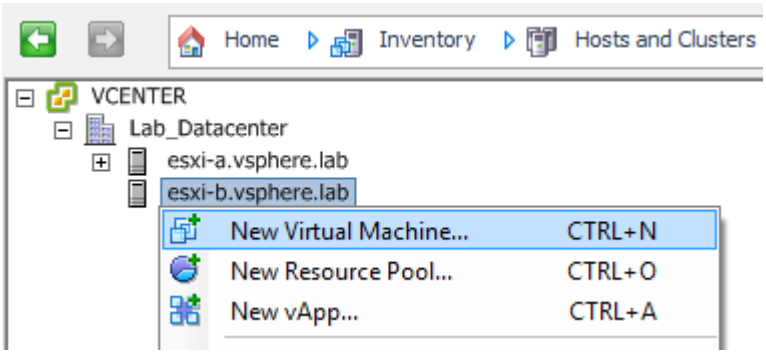
- **Chipset** - la scheda madre di una VM usa un chipset proprietario basato sulle seguenti architetture:
  - Intel 440BX AGPset 82443BX Host Bridge/Controller;
  - Intel 82371AB (PIIX4) PCI ISA IDE Xcelerator;
  - National Semiconductor PC87338 ACPI 1.0 and PC98/99 Compliant SuperI/O;
  - Intel 82093AA I/O Advanced Programmable Interrupt Controller.
- **DVD/CD-ROM** - Il lettore CD/DVD è installato di default durante la creazione di una VM. Può essere utilizzato per connettere in maniera remota un DVD/CD-ROM dalla macchina che esegue il vSphere Client o Web Client, oppure può essere interfacciato al lettore fisico dell'host ESXi, o ancora può essere sfruttato per montare un'immagine ISO.
- **Floppy Drive** - Installato di default durante la creazione di una VM. Può essere utilizzato per connettere in maniera remota il floppy drive dalla macchina che esegue il vSphere Client o Web Client, oppure può essere interfacciato al floppy drive dell'host ESXi, o ancora può essere sfruttato per montare un'immagine floppy (file con estensione .flp).
- **Interfacce IDE** - Le due interfacce di tipo IDE (Integrated Drive Electronics) presenti in modo nativo su ogni VM permettono di avere sino a un massimo di 4 dispositivi IDE (hard disk IDE e lettori CD-ROM).
- **Porta parallela -** permette l'interfacciamento con la porta parallela dell'host ESXi. Può inoltre essere connessa ad un file di output.
- **Controller PCI -** in una VM è presente un solo controller PCI che non può essere né rimosso né configurato.
- **Dispositivi PCI -** si possono aggiungere sino a 6 dispositivi di tipo vSphere DirectPath. I dispositivi devono essere riservati per il PCI passthrough nell'host ESXi.
- **Dispositivo di puntamento -** necessario per l'interfacciamento tra il mouse connesso alla console (tramite vSphere Client) e quello della VM.
- **Porta seriale -** una VM può utilizzare sino a 4 porte seriali, interfacciabili alle porte fisiche dell'host ESXi, a un file presente nell'host ESXi, oppure a un percorso di rete.
- **Dispositivi SCSI -** hard disk o cd/dvd scsi collegabili grazie all'interfaccia scsi installata di default sulla VM.
- **Controller SIO -** un controller SIO è disponibile in maniera predefinita su ogni VM. Permette di avere porte parallele e seriali, ma non può essere né rimosso né configurato.
- **Tastiera** - Necessaria per l'interfacciamento tra la tastiera connessa via console (tramite vSphere Client) e quella della VM.
- **Controller USB -** corrisponde al chip hardware che permette la connessione di dispositivi USB. vSphere 5 include il supporto ai dispositivi USB 3.0 all'interno delle macchine virtuali con sistema Linux. Il controller consente inoltre l'interfacciamento di dispositivi USB 3.0 collegati nel computer che esegue vSphere Client o Web Client.
- **Dispositivi USB -** i dispositivi USB possono essere connessi all'host ESXi o al computer che esegue vSphere Client.
- **VMCI -** Virtual Machine Communication Interface device. Fornisce un canale di comunicazione ad alta velocità tra la VM e l'hypervisor. Non può essere né rimosso né configurato.

10.2 Creazione di una macchina virtuale

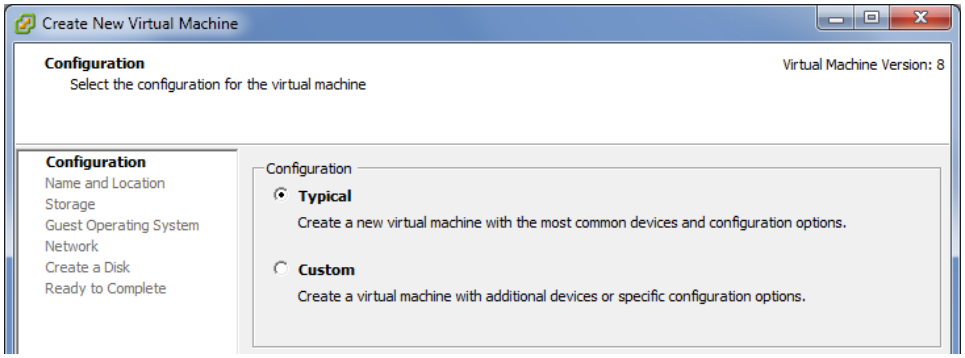
Procedura tramite vSphere Client

Per la creazione di una VM, è necessario collegarsi al vCenter o direttamente ad un host ESXi. Il secondo metodo è consigliabile solo se l'host ESXi non fa parte di un'infrastruttura vSphere. È il caso, ad esempio, di vSphere ESXi in versione gratuita, che permette di creare e gestire una o più macchine virtuali all'interno di un unico host.

In ogni caso, dopo aver eseguito il login, è sufficiente fare clic con il tasto destro su un qualsiasi oggetto dell'inventario contenitore di VM (datacenter, cartella, cluster, resource pool, host) e selezionare la voce **New Virtual Machine**.

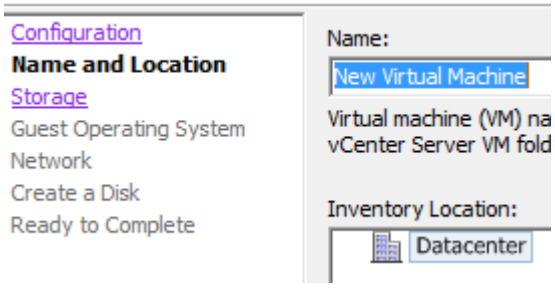


La procedura guidata ci permette di scegliere tra una configurazione tipica (**Typical**) e una configurazione avanzata (**Custom**). Nel primo caso non saranno richiesti parametri avanzati, mentre nel secondo si possono configurare tutti gli aspetti riguardanti la macchina virtuale.

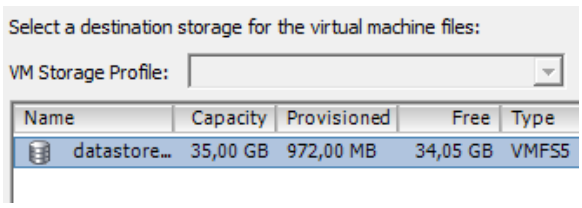


Di seguito i passi di una configurazione tipica.

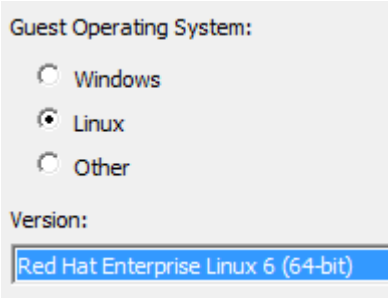
1. Inserire il nome della VM e specificarne la posizione rispetto all'inventario.



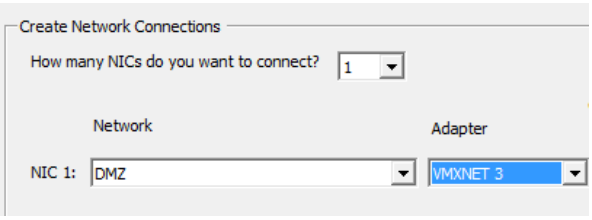
2. Scegliere il datastore in cui salvare la VM.



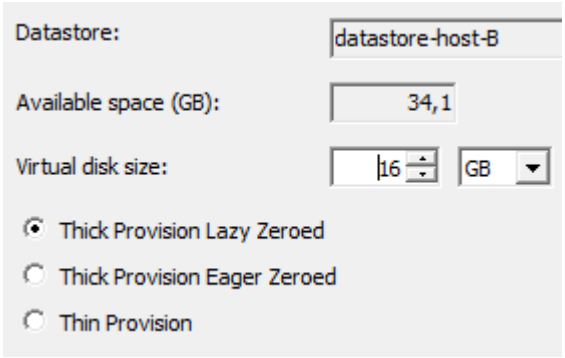
3. Scegliere il tipo di sistema operativo che verrà installato.



4. Scegliere il tipo di interfaccia di rete. Per quanto riguarda la scelta tra le diverse interfacce disponibili, vedere la sezione "Hardware di una macchina virtuale".



5. Impostare il disco virtuale (tipo e dimensione).



Thick Provision Lazy Zeroed. Con quest'opzione lo spazio verrà interamente allocato durante la creazione della VM. All'interno dello spazio allocato, i blocchi verranno azzerati solo a partire dalla prima scrittura effettuata dalla VM.
Thick Provision Eager Zeroed. Con quest'opzione lo spazio verrà interamente allocato durante la creazione. All'interno dello spazio allocato, i blocchi saranno azzerati immediatamente durante la creazione del disco. In questo caso la creazione del disco richiederà tempi più lunghi, proporzionalmente alla grandezza del disco stesso.
Thin Provision. Con quest'opzione lo spazio sarà allocato dinamicamente su richiesta. In sostanza la dimensione massima del disco non viene allocata interamente sullo storage. Il disco crescerà nelle dimensioni in base allo spazio richiesto dalla VM durante il suo ciclo produttivo.

Con **vSphere Client**, la configurazione "Custom" prevede, rispetto alla "Typical", alcuni parametri aggiuntivi.

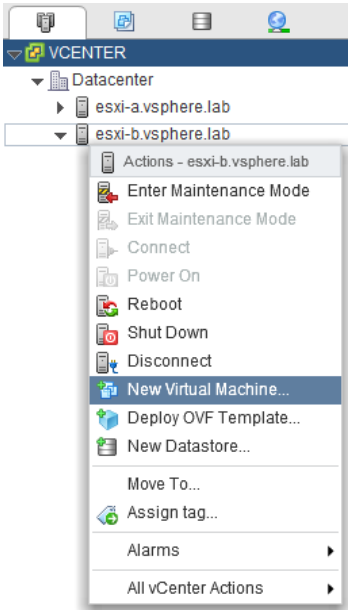
- **Virtual Machine Version**, in altre parole versione dell'hardware della VM. La versione 9 è l'ultima disponibile per gli host ESXi 5.1. Se si vuole mantenere la compatibilità con ESXi 5.0, selezionare la versione 8. Se si vuole mantenere la compatibilità con ESX/ESXi 4.x, selezionare la versione 7. È possibile eseguire l'upgrade (ma non il downgrade) della versione hardware di una VM in qualsiasi momento; tuttavia, l'operazione può essere portata a termine solo a VM spenta.
- **Numero di virtual socket e numero di core per socket**. La scelta è legata al numero di CPU presenti nell'host ESXi e dal numero di CPU supportate dal sistema operativo guest. Alcuni sistemi operativi sono infatti limitati per girare su un numero massimo di CPU definito dalle licenze in uso. Ad esempio, Windows Server 2003 Standard Edition è limitato a un massimo di 4 CPU, dove ogni CPU è intesa come socket. Se le CPU sono di tipo multi-core, utilizzando CPU dual-core il sistema operativo potrebbe sfruttare sino a 8 core. Nelle macchine virtuali VMware, nelle versioni precedenti a vSphere 4.0, le CPU virtuali apparivano esclusivamente come CPU single core; pertanto, creando una macchina virtuale con 8 CPU, un qualsiasi sistema operativo avrebbe "visto" 8 CPU single core. In questa situazione, se il sistema operativo è Windows 2003 SE (limitato a 4 CPU), sono sfruttate solo 4 CPU virtuali. La limitazione descritta è stata superata a partire da vSphere 4, in cui sono state introdotte le impostazioni "**number of virtual sockets"** e "**number of cores per virtual socket"**, consentendo di controllare il numero di core per CPU in una macchina virtuale.
- **Memoria RAM**. La configurazione personalizzata permette di specificare da subito questo valore.

- **Controller SCSI**. La selezione può essere fatta tra BusLogic Parallel, LSI Logic Parallel, LSI Logic SAS, VMware Paravirtual.
- **Tipo di disco**. È possibile scegliere se creare un nuovo disco, utilizzare un disco esistente, o utilizzare un disco **Raw Device Mapping** (**RDM**), ovvero consentire alla macchina virtuale di scrivere in modo diretto su una LUN dello storage. Vedremo la funzione RDM in modo dettagliato più avanti. Se si seleziona un nuovo disco, è possibile impostare lo stesso in modalità indipendente, detta **Independent Mode**. In questa modalità il disco non viene incluso in alcuna snapshot eseguita per la macchina virtuale. La modalità Independent prevede dischi di tipo **Persistent**, che si comportano come i dischi convenzionali in cui tutti i dati sono scritti in modo permanente, e dischi **Non Persistent**, in cui le modifiche vengono perse quando si spegne o si riavvia la macchina virtuale.

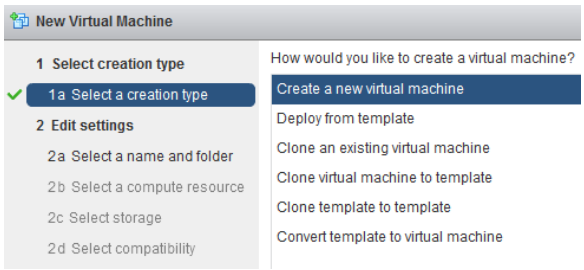
Procedura tramite vSphere Web Client

1. Nel pannello di navigazione a sinistra, fare clic con il tasto destro su un qualsiasi oggetto dell'inventario che possa essere un contenitore per la VM che si vuole creare (datacenter, cartelle, cluster, resource pool, host).

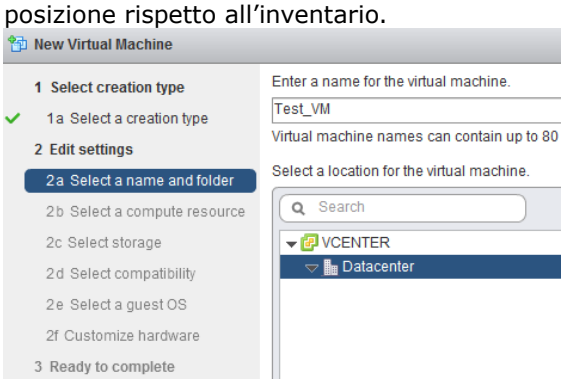
2. Selezionare **New Virtual Machine**.



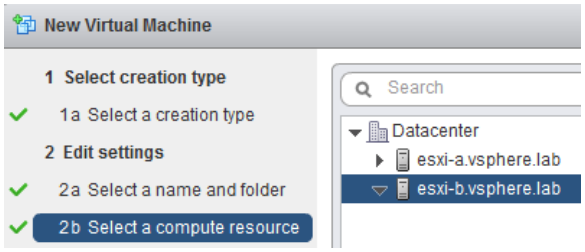
3. Selezionare la voce **Create a new virtual machine** e fare clic su **Next**.



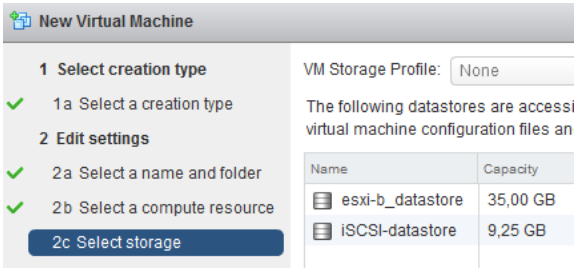
4. Inserire il nome della VM e specificarne la posizione rispetto all'inventario.



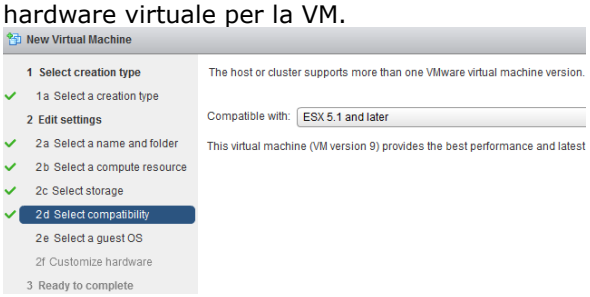
5. Scegliere un host che fornirà le risorse di calcolo.



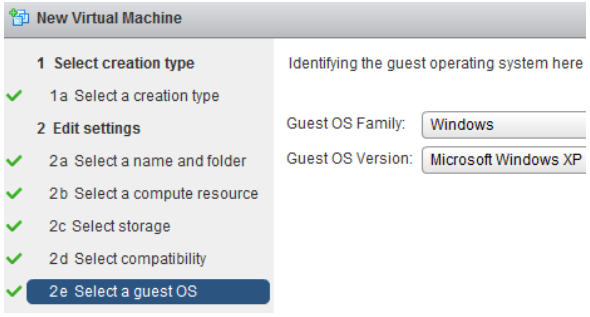
7. Scegliere il datastore in cui salvare la VM.



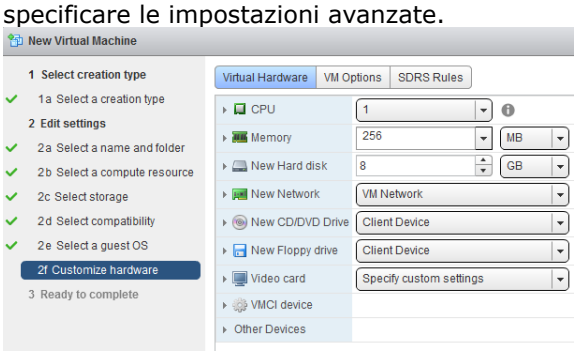
8. Scegliere il livello di compatibilità con le diverse versioni di ESXi, ovvero la versione di hardware virtuale per la VM.



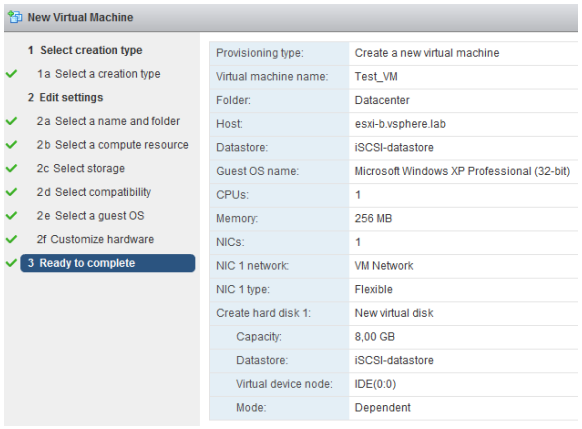
9. Scegliere il tipo di sistema operativo da installare.



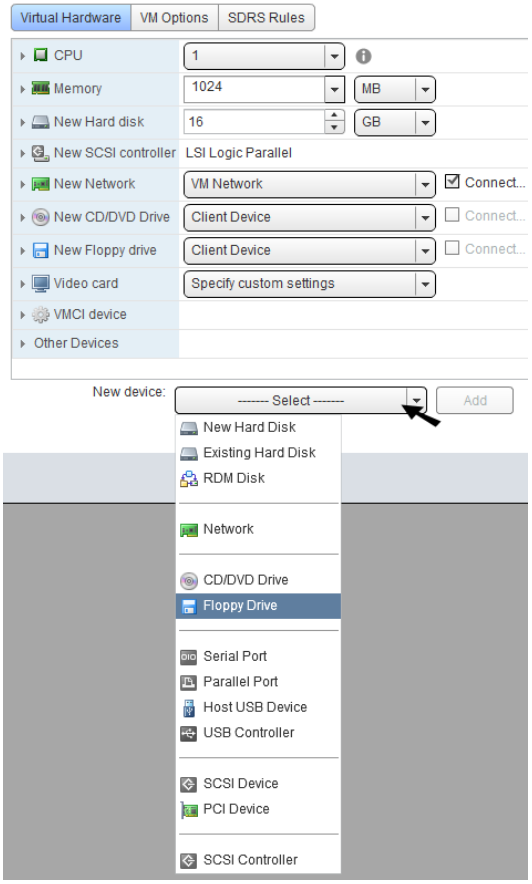
10. Impostare l'hardware e le opzioni per la VM. In questo passaggio si impostano CPU, disco virtuale (tipo e dimensione) e interfacce di rete. Fare clic su ogni elemento hardware per specificare le impostazioni avanzate.



11. La procedura termina con il riepilogo delle impostazioni assegnate.



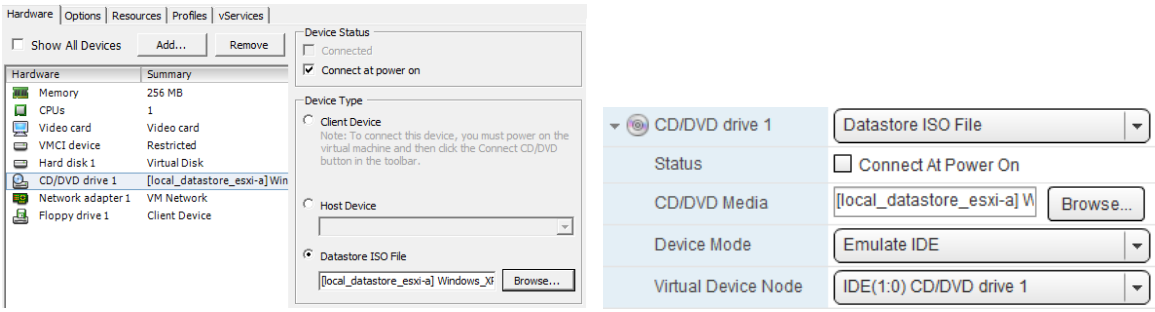
Con vSphere Client abbiamo visto che esiste la possibilità di configurare diversi parametri avanzati, utilizzando la procedura "Custom". Gli stessi parametri sono configurabili con vSphere Web Client, durante la fase di creazione guidata della VM, nella pagina **Customize hardware**. La creazione guidata prevede che un primo disco virtuale sia aggiunto automaticamente. È possibile utilizzare il menu **New device** per aggiungere un nuovo disco, selezionarne uno esistente, o aggiungere un disco RDM. Lo stesso menu consente l'inserimento di nuovi dispositivi. Per configurare nel dettaglio ogni dispositivo, è sufficiente fare clic su di esso e modificare i campi di proprio interesse. Per rimuovere un dispositivo, è necessario posizionare il puntatore su di esso e fare clic sull'icona **Remove**.



10.2.2 Installazione del sistema operativo guest

L'installazione del sistema operativo all'interno di una macchina virtuale prevede gli stessi passaggi necessari su una macchina fisica. Utilizzando vSphere Client o vSphere Web Client, all'interno delle periferiche hardware della VM è possibile associare alla periferica **CD/DVD drive** un'immagine ISO presente in un datastore, oppure il lettore CD dell'host ESXi, o ancora il lettore CD della macchina da cui si eseguono vSphere Client o Web Client. Le immagini ISO montate saranno viste dalla VM come supporti CD/DVD. La VM potrà quindi effettuare il boot da CD/DVD e si potrà procedere all'installazione del sistema operativo.

Qui sotto, l'esempio di un'immagine ISO montata nella VM. A sinistra la configurazione del drive CD/DVD con vSphere Client, a destra con vSphere Web Client.



10.2.3 VMware Tools

I VMware Tools sono un insieme di utilità che migliorano le prestazioni dei sistemi operativi guest. Il miglioramento è principalmente dovuto alla sostituzione dei driver generici dei sistemi guest con

driver specifici progettati per l'hardware virtuale. È consigliato installare sempre e comunque i VMware Tools. L'installazione comprende anche gli elementi sotto indicati:

- un driver video SVGA;
- il driver vmxnet per le interfacce di rete;
- il driver SCSI BusLogic;
- un driver di controllo per l'allocazione efficiente della memoria tra macchine virtuali;
- il pannello di controllo dei VMware Tools.

L'installazione dei VMware Tools nelle macchine **Windows** richiede i passaggi seguenti:

- con vSphere Client - tasto destro sulla VM e selezionare **Guest > Install/Upgrade VMware Tools**;
- con vSphere Web Client - tasto destro sulla VM e selezionare **All vCenter Actions > Guest OS > Install/Upgrade VMware Tools**.

Per le macchine **Linux**, i passaggi di sopra eseguono solo il mount dell'immagine contenente i VMware Tools per Linux. L'installazione deve essere completata manualmente, dalla riga di comando del sistema Linux.

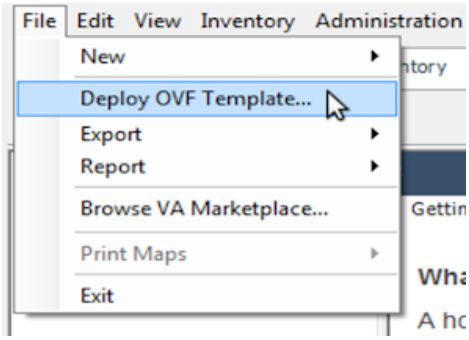
a) Creare un punto di mount:
   mkdir /mnt/cdrom
b) Montare il CD-ROM:
   mount /dev/cdrom /mnt/cdrom
c) Posizionarsi in una directory temporanea (ad esempio, /tmp):
   cd /tmp
d) Estrarre i file presenti nell'installer nel CD:
   tar zxpf /mnt/cdrom/VMwareTools-x.x.x-yyyy.tar.gz
e) Eseguire l'installer e configurare i VMware Tools:
   cd vmware-tools-distrib
   ./vmware-install.pl
f) Rispondere alle domande proposte, premendo il tasto Enter per accettare i valori predefiniti proposti di volta in volta.

10.2.4 Le virtual appliance

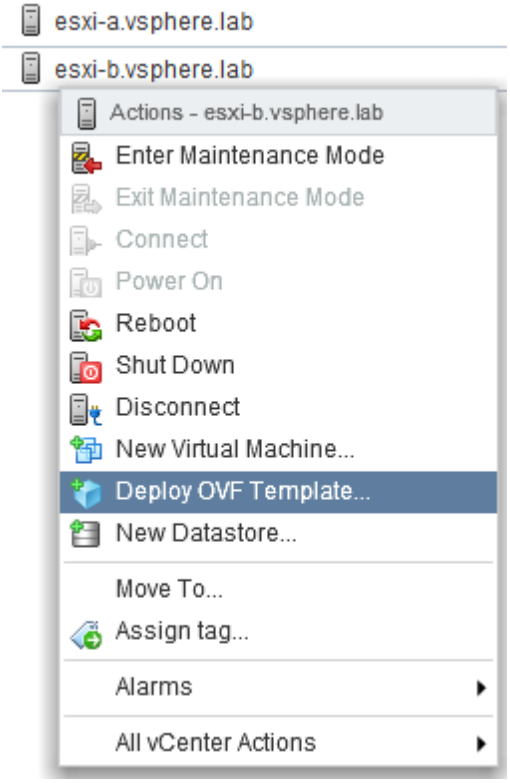
Una virtual appliance è una VM preconfigurata che include il sistema operativo guest e altri software già installati. Può essere importata nell'inventario del vCenter Server o direttamente su un host ESXi tramite vSphere Client. Le virtual appliance sono distribuite nel formato OVF (Open Virtualization Format), un formato aperto per la distribuzione di macchine virtuali.

Importazione di una virtual appliance

Tramite **vSphere Client**, selezionare la voce **Deploy OVF Template** dal menu File.



Tramite **vSphere Web Client**, selezionare dall'inventario un oggetto che faccia da contenitore (cartella, datacenter, host, ecc.) e scegliere la voce **Deploy OVF Template**.



Nella procedura guidata viene chiesto di specificare il nome e la posizione del file OVF relativo all'appliance da importare. I file OVF possono essere scaricati direttamente da internet; in tal caso è sufficiente specificare l'URL che punta a quei file.

Se invece si vuole esportare una VM sotto forma di appliance virtuale:

- con vSphere Client, selezionare la VM e fare clic sulla voce di menu **File > Export > Export OVF Template**;
- con vSphere Web Client, selezionare la VM, fare clic con il tasto destro su di essa e selezionare la voce **All vCenter Actions > Export OVF Template**.

10.3 File di una macchina virtuale

Una macchina virtuale, all'interno dell'hypervisor ESXi, è costituita da un insieme di file, ognuno con un importante ruolo. Ogni macchina virtuale viene salvata all'interno di una cartella che normalmente ha il nome della VM stessa; i file che la compongono sono elencati di seguito:

- Un file di configurazione con estensione .**vmx**. Se una VM è convertita in template, il file di configurazione .vmx è sostituito dal file di template .vmtx.
- Eventuali file addizionali di configurazione con estensione .**vmxf**.
- Uno o più file corrispondenti ai dischi virtuali della VM. Per ogni disco virtuale, esistono un file con estensione **.vmdk** ed uno con suffisso ed estensione **-flat.vmdk**. Il primo è solo un descrittore delle caratteristiche del disco virtuale, il secondo è il vero e proprio contenitore dei dati. Nel caso in cui la VM sia dotata di più dischi virtuali, la seconda coppia di file presenta un suffisso aggiuntivo corrispondente alla sequenza dischi, partendo da 1.

Ad esempio, se la macchina virtuale UbuntuServer avesse due dischi virtuali, la prima coppia di file sarebbe costituita da UbuntuServer.vmdk e UbuntuServer-flat.vmdk, mentre la seconda coppia sarebbe costituita da UbuntuServer_1.vmdk e UbuntuServer_1-flat.vmdk.

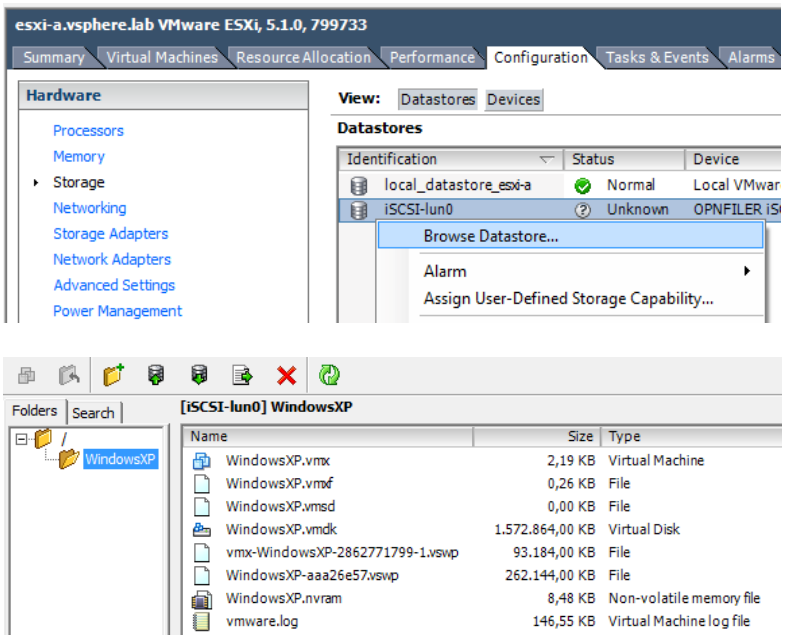
- Un file con estensione **.nvram** contentente il BIOS della macchina virtuale.
- Uno o più file di log con estensione **.log**.
- Un file di swap, con estensione **.vswp**, utilizzato per recuperare memoria durante i periodi di contesa (non ha niente a che vedere con il file di swap utilizzato dal sistema operativo presente nella VM).
- File di snapshot con estensione **.vmsd** e **.vmsn**, vuoti nel caso in cui la VM non abbia alcuna snapshot.

A livello di funzionamento, la macchina virtuale è un insieme di componenti hardware virtuali che permettono il funzionamento di un sistema operativo e delle applicazioni installate su di esso: il fatto che la macchina sia di tipo virtuale è trasparente per il sistema operativo e le applicazioni installate su di essa.

10.3.1 Visualizzare i file di una macchina virtuale

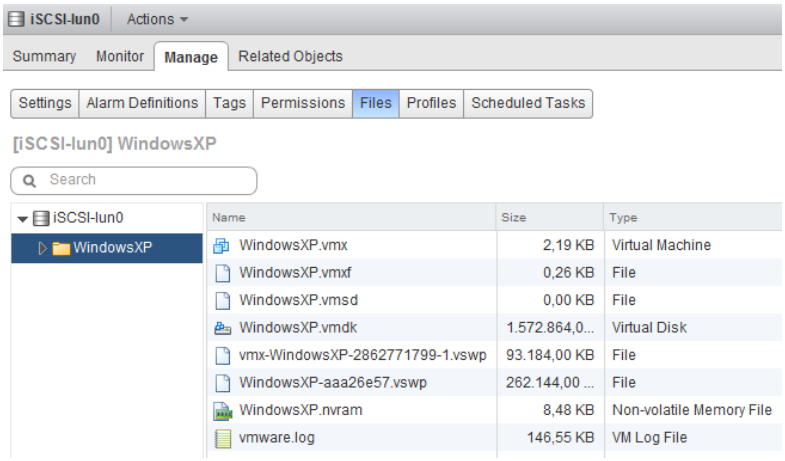
Procedura tramite vSphere Client

- Fare clic con il tasto destro sul datastore che ospita la VM e scegliere la voce **Browse Datastore**.



Procedura tramite vSphere Web Client

- Entrare nel datastore che ospita la VM, fare clic sul tab **Manage** e selezionare la voce **Files**.



Procedura tramite console

Tramite i due client grafici, ogni disco virtuale è rappresentato dal solo file .vmdk e viene omessa la visualizzazione della controparte -flat.vmdk. Per visualizzare tutti i file bisogna utilizzare la command line accedendo in console sull'host ESXi.

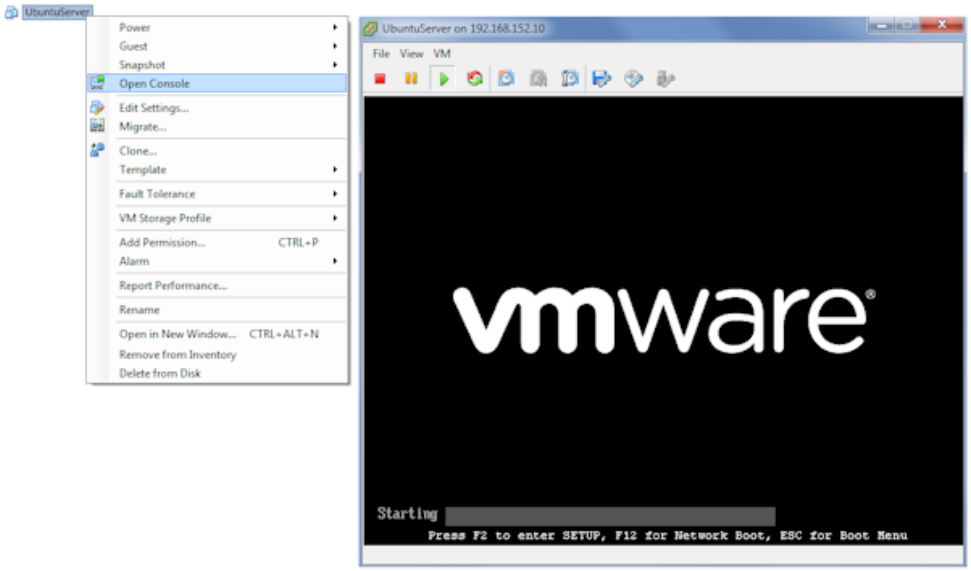
Nell'esempio qui sotto è infatti visibile il file –flat.vmdk.

```
~ # ls /vmfs/volumes/iSCSI-lun0/WindowsXP/
WindowsXP-aaa26e57.vswp    WindowsXP.vmdk      WindowsXP.vmxf
WindowsXP-flat.vmdk        WindowsXP.vmsd      vmware.log
WindowsXP.nvram            WindowsXP.vmx       vmx-WindowsXP-2862771799-1.vswp
```

10.4 Console di una macchina virtuale

La console di una VM permette l'accesso diretto al sistema operativo della VM stessa. Si utilizza in particolare durante per la fase di installazione del sistema operativo e per l'accesso al BIOS della VM. Consente di operare sull'alimentazione della VM, grazie alle funzioni di accensione, spegnimento e reset, e di inviare la sequenza di tasti Ctrl+Alt+Canc alla VM (tramite la combinazione Ctrl+Alt+Ins all'interno della console).

La console è disponibile con vSphere Client e con vSphere Web Client. Per aprire la console di una VM, fare clic con il tasto destro su di essa e selezionare la voce **Open Console**.


UbuntuServer
Power
Guest
Snapshot
Open Console
Edit Settings...
Migrate...
Clone...
Template
Fault Tolerance
VM Storage Profile
Add Permission... CTRL+P
Alarm
Report Performance...
Rename
Open in New Window... CTRL+ALT+N
Remove from Inventory
Delete from Disk
UbuntuServer on 192.168.152.10
File View VM
vmware
Starting
Press F2 to enter SETUP, F12 for Network Boot, ESC for Boot Menu

Capitolo 11
Gestione delle macchine virtuali

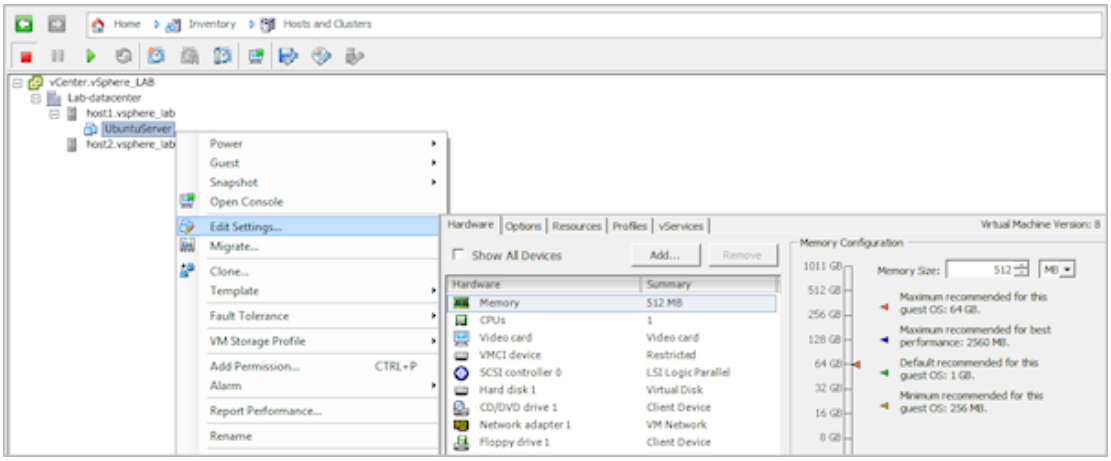
11.1 Modificare le caratteristiche di una macchina virtuale

Le caratteristiche di una VM possono essere modificate dalla finestra delle sue proprietà. Si può avere la necessità di modificare una VM per diversi motivi, così come accade per le macchine fisiche: inserimento di un'interfaccia di rete, upgrade di memoria RAM, aggiunta di nuovi dischi, ecc., oppure rimozione degli stessi elementi appena indicati. Alcuni elementi possono essere aggiunti o rimossi anche a caldo, e sono definiti come **hot-pluggable devices**. Altri, come CPU e memoria, possono diventare hot-plug solo se:

- il sistema operativo guest supporta questa funzione;
- sono installati i VMware Tools;
- l'hardware della macchina virtuale è versione 7 o superiore;
- l'opzione hot-plug è abilitata nelle opzioni della VM.

Procedura con vSphere Client

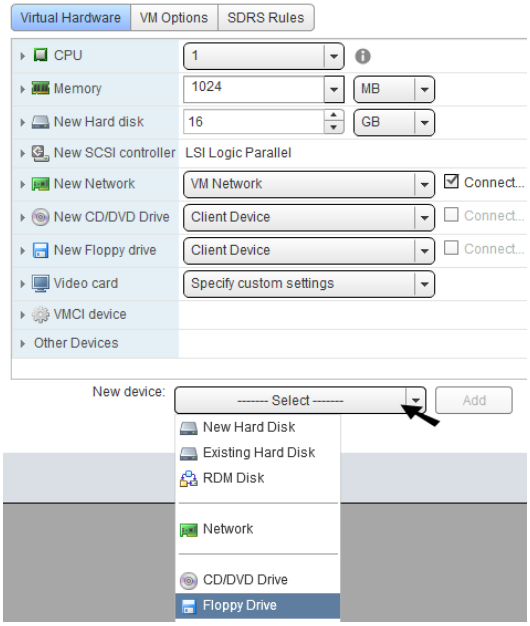
- Fare clic con il tasto destro sulla VM e selezionare la voce **Edit Settings**.



- Per aggiungere o rimuovere un elemento hardware dalla VM, utilizzare rispettivamente i bottoni **Add** e **Remove**.

Procedura con vSphere Web Client

- Fare clic con il tasto destro sulla VM e selezionare la voce **Edit Settings**.
- Per aggiungere un nuovo dispositivo, utilizzare il menu **New device**.



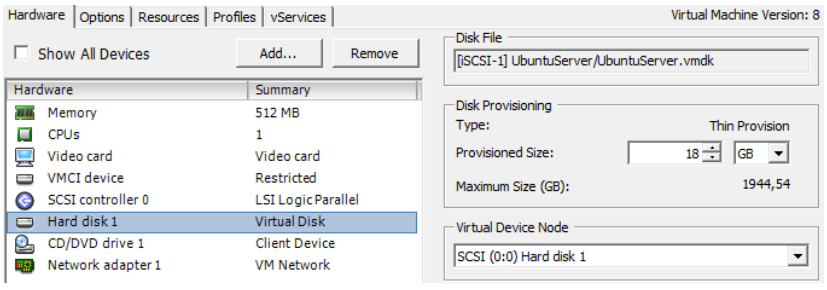
- Per configurare nel dettaglio ogni dispositivo, è sufficiente fare clic su di esso e modificare i campi di proprio interesse.
- Per rimuovere un dispositivo, è necessario posizionare il puntatore su di esso e fare clic sull'icona **Remove**.

11.1.2 Incrementare le dimensioni di un disco virtuale

L'operazione è possibile anche a macchina accesa, a patto di aver installato i VMware Tools. Non si può incrementare la dimensione di un disco se la VM ha delle snapshot. Dopo aver incrementato le dimensioni di un disco virtuale, saranno necessari appositi tool (in dotazione nel sistema guest o forniti da terze parti) per la modifica delle partizioni, affinché possa essere sfruttato il nuovo spazio libero non partizionato.

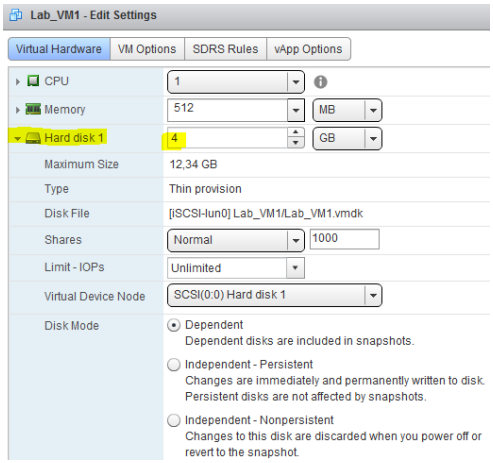
Procedura con vSphere Client

1. Fare clic con il tasto destro sulla macchina virtuale e selezionare la voce **Edit Settings**.
2. Selezionare l'hard disk virtuale.
3. Inserire la nuova dimensione.



Con vSphere Web Client

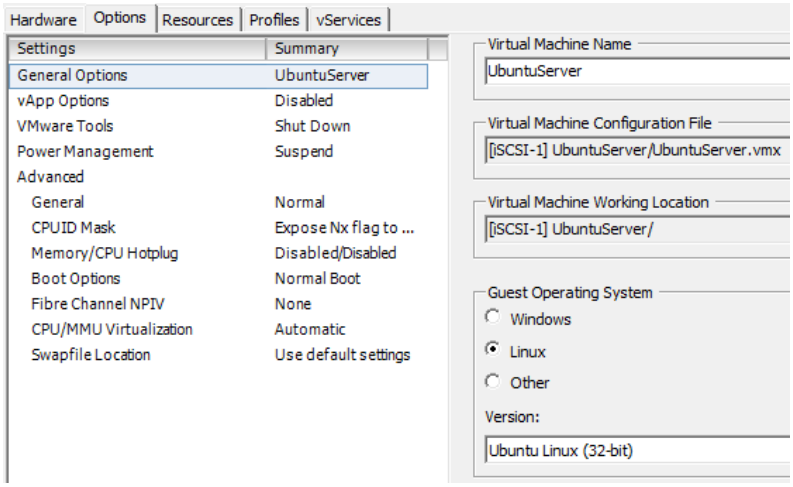
1. Fare clic con il tasto destro sulla macchina virtuale e selezionare la voce **Edit Settings**.
2. Selezionare l'hard disk virtuale.
3. Inserire la nuova dimensione.



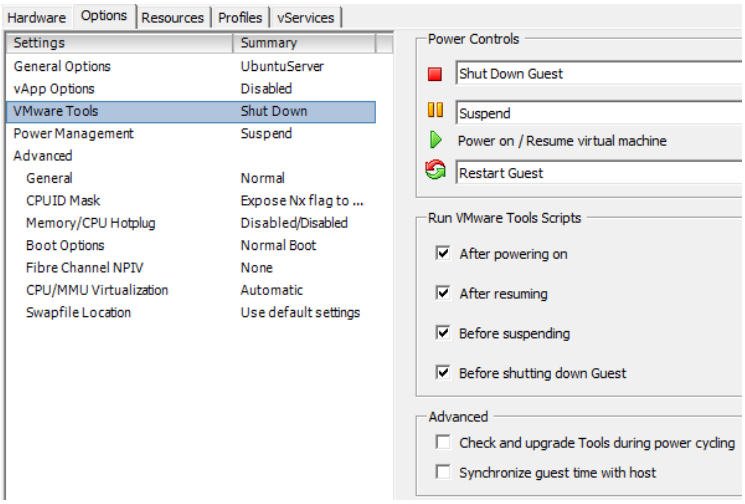
11.1.3 Opzioni di una macchina virtuale

Il tab **Options**, presente nella finestra delle impostazioni di una VM, permette la modifica di diverse opzioni.

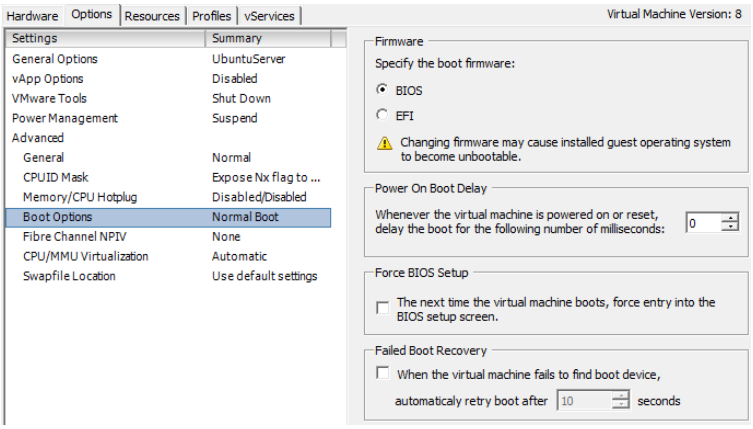
- **Nome della VM** - modificabile alla voce **General Options**. Il cambio del nome non modifica il nome dei file della macchina virtuale.



- **Comportamento dei VMware Tools** - si può impostare l'effetto dei pulsanti di alimentazione della macchina virtuale e l'esecuzione di determinati script in base ad alcuni eventi. Gli script possono essere impostati all'interno della VM, nella finestra di dialogo dei VMware Tools. Infine si può decidere di rendere automatico l'aggiornamento dei VMware Tools non appena una nuova versione risulta disponibile, e rendere automatico l'aggiornamento dell'orologio della macchina virtuale con l'host ESXi.



- **Opzioni di boot** - si può impostare il tipo di firmware della VM, **BIOS** o **EFI**, e il tempo di attesa tra la fase di BOOT e quella di start-up del sistema operativo. Esiste la possibilità di forzare la VM ad accedere al BIOS al prossimo avvio (Force Bios Setup), ad esempio per impostare il boot da CDROM, o impostare un riavvio dopo un certo numero di secondi nel caso in cui non fossero presenti dispositivi di boot (Failed Boot Recovery).



11.1.4 Allocazione di risorse

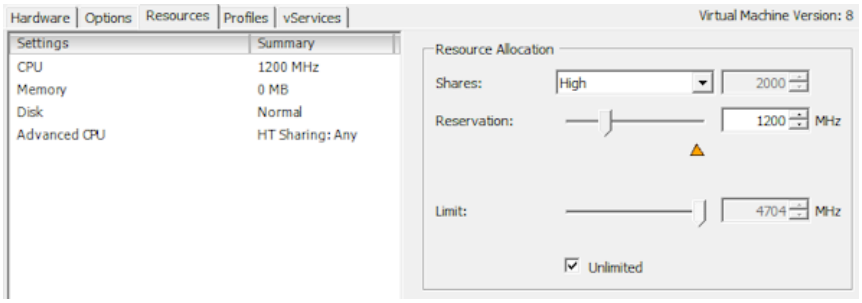
Per ogni VM, è possibile gestire l'allocazione delle risorse. I valori impostabili per gli elementi CPU, memoria e disco sono indicati di seguito.

- **Shares** - priorità sull'accesso della VM alle risorse condivise.
- **Reservation** - valore minimo di risorse garantite e preallocate per la VM dall'host ESXi. Questo valore rappresenta allo stesso tempo le risorse fisiche garantite al VMkernel per l'avvio della VM stessa.
- **Limit** - valore massimo di risorse che non può mai essere superato. Nel caso della CPU il valore è espresso in cicli (MHz), nel caso della memoria è espresso in Mb.

I concetti di allocazione delle risorse saranno trattati in maniera approfondita nel capitolo "Gestione e controllo delle risorse".

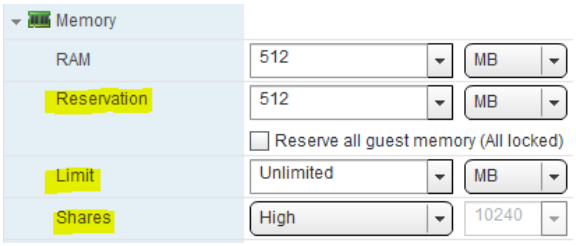
Procedura tramite vSphere Client

- Con vSphere Client, la gestione delle risorse di una VM si esegue dal tab **Resources**, nelle proprietà della VM stessa.



Procedura tramite vSphere Web Client

- Con vSphere Web Client, la gestione delle risorse si esegue dal pannello di gestione hardware, nelle impostazioni della VM, espandendo le opzioni disponibili per CPU, memoria e dischi.



11.2 Dischi RDM

VMware vSphere supporta la modalità di accesso **Raw Device Mapping** (**RDM**) per le macchine virtuali. Si tratta di una funzione che consente l'accesso diretto a una LUN presente sullo storage fisico (tipicamente SAN fibre channel o iSCSI). Quando si aggiunge un disco RDM ad una VM, l'hypervisor crea un file "puntatore" che fa riferimento alla LUN della SAN. Di fatto un RDM è un file con estensione *.vmdk* che contiene solo le informazioni di puntamento; i dati risiedono esclusivamente nella LUN.

La mappatura tramite il file puntatore (o file di mapping) consente alle LUN di apparire come facenti parte di un volume VMFS: il file di mapping si presenta come file .vmdk tipico dei dischi virtuali ed è referenziato nella configurazione della macchina virtuale. Quando devono essere eseguite operazioni di lettura o scrittura, la LUN viene aperta per l'accesso e il file di mapping permette di ottenere i puntamenti. Successivamente, le operazioni di lettura e scrittura utilizzano direttamente la LUN senza più passare attraverso il file di mapping. La macchina virtuale vede il dispositivo RDM come un disco SCSI virtuale.

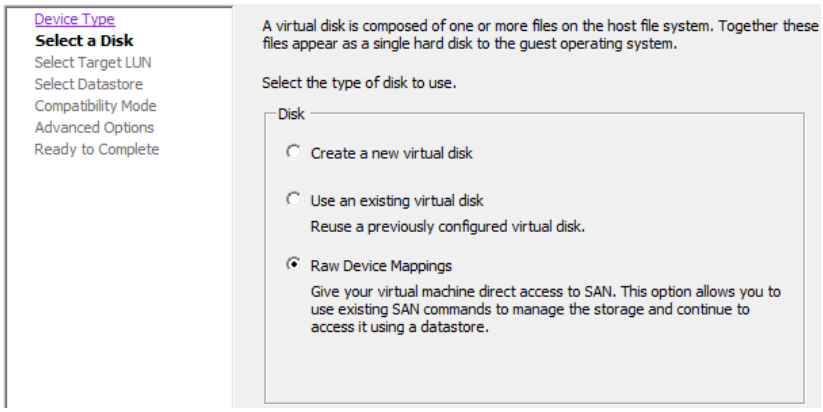
Gli host ESXi supportano 2 modalità RDM.

- **Phisical compatibility mode** - in questa modalità il sistema operativo guest accede in modo diretto allo storage. Il VMkernel passa tutti i comandi SCSI al dispositivo e tutte le caratteristiche fisiche della LUN sono visibili. Si consiglia questa modalità per interagire direttamente con l'hardware della SAN, soprattutto se nella macchina virtuale sono installate applicazioni orientate alla gestione della SAN stessa. La modalità fisica non permette la clonazione di una LUN, la trasformazione della LUN in template, oppure la migrazione nel caso in cui sia prevista la copia del disco della VM.
- **Virtual compatibility mode** - in questa modalità il VMkernel invia solo i comandi di lettura/scrittura al dispositivo mappato. Questo appare al sistema operativo guest esattamente come un disco virtuale in un volume VMFS, e le caratteristiche fisiche della

LUN sono nascoste. Se si utilizza un disco raw in modalità virtuale sono possibili funzionalità avanzate come l'uso delle snapshot, la clonazione del disco e la creazione di template.

Nuovo disco RDM con vSphere Client

- Creare un nuovo disco per la VM e, nella finestra di scelta del tipo di dispositivo, scegliere **Raw Device Mappings**.
- Fare clic sulla LUN da collegare e specificare la compatibilità fisica o virtuale.



Nuovo disco RDM con vSphere Web Client

- Per collegare una LUN ad una macchina virtuale in modalità RDM, aggiungere un dispositivo RDM alla VM stessa.
- Fare poi clic sul nuovo dispositivo per specificare la compatibilità fisica o virtuale.

11.3 Utilizzo dei template

Un template, o modello, è la versione "master" di una macchina virtuale da cui è possibile creare e distribuire nuove macchine virtuali con caratteristiche predeterminate, quali:

- sistema operativo guest;
- set di applicazioni installate;
- configurazioni legate alle risorse computazionali (hardware).

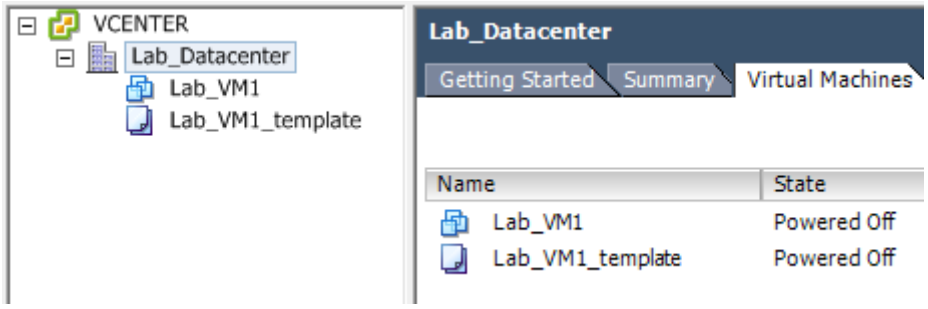
È uno strumento molto comodo per realizzare quello che si chiama provisioning delle VM; consente di evitare azioni ripetitive nel momento in cui si vogliono realizzare più macchine con caratteristiche comuni.

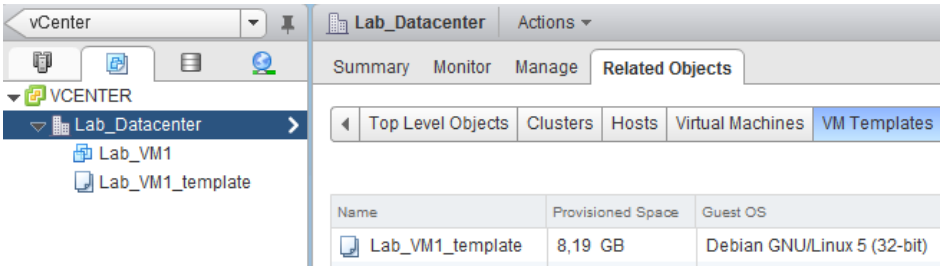
Una VM può essere clonata da un template, oppure convertita in template. Nel primo caso l'operazione è chiamata **Clone to Template**; la macchina virtuale da cui si parte per la realizzazione del template è mantenuta in esecuzione. Il risultato sono due macchine virtuali, la prima che rimane in produzione, la seconda che diventa un template. L'altra operazione possibile è chiamata **Convert to Template**; la macchina virtuale di origine si trasforma in template e non potrà più andare in produzione, fermo restando che, da quel template, possiamo generare una nuova macchina virtuale.

Le operazioni sui template sono possibili solo collegandosi al vCenter e non direttamente agli host. Con **vSphere Client**, fare clic con il tasto destro sulla VM e selezionare la voce **Template**. Con **vSphere Web Client**, fare clic con il tasto destro sulla VM e selezionare la voce **All vCenter Actions > Template**.

La clonazione su template prevede la possibilità di scegliere il formato dei dischi che verranno generati: si può scegliere se mantenere lo stesso formato della macchina di origine, oppure scegliere i formati thick o thin. La conversione in template lascia invece intatti i file corrispondenti ai dischi e non prevede possibilità di scelta.

Per vedere tutti i template disponibili, da vSphere Client o Web Client, si deve scegliere la modalità di visualizzazione **VMs and Template**, oppure si seleziona l'oggetto contenitore (datacenter, cluster, host o cartella) nella vista **Hosts and Clusters** e si va sul tab **Virtual Machines**.





Per distribuire una macchina virtuale da un template, è sufficiente fare clic con il tasto destro sul template e selezionare la voce **Deploy Virtual Machine from this Template**.

A livello di file su datastore, se una VM è convertita in template avrà il file **.vmx** sostituito da un nuovo file con estensione **.vmtx**.

11.4 Clonazione di una macchina virtuale

Clonare una macchina virtuale vuol dire creare una copia esatta della macchina virtuale stessa. La clonazione è possibile solo eseguendo l'accesso al vCenter Server. Non è possibile clonare una VM collegandosi direttamente a un host ESXi. La clonazione può essere eseguita sia a caldo (macchina accesa) sia a freddo (macchina spenta). Tuttavia, nel primo caso, gli applicativi non vanno in quiescenza (stato di sospensione). Pertanto, in caso di applicativi con elevato numero di richieste,

come i motori di database, o comunque con elevati carichi operativi, si consiglia la clonazione a freddo.

Per eseguire la clonazione di una macchina virtuale, semplicemente fare clic con il tasto destro su di essa e selezionare la voce **Clone**.

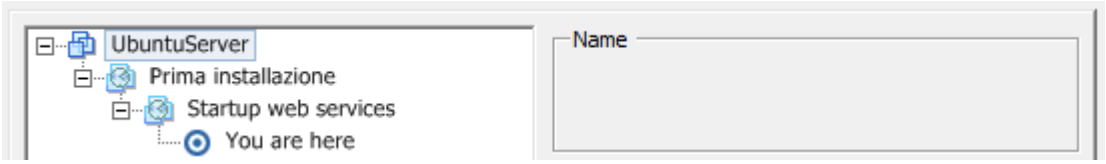
Si raccomanda di personalizzare le macchine clonate per evitare conflitti in rete. I parametri di hostname, l'indirizzo IP, il SSID delle macchine Windows in dominio, sono tutti elementi che dovrebbero essere modificati per non ritrovarsi in rete con due macchine identiche, che andrebbero reciprocamente in conflitto. Per questo scopo può essere utilizzata la funzione **Guest customization** che si presenta durante le operazioni di clonazione o distribuzione a partire da un template. Questa funzione sfrutta i VMware Tools, che devono essere presenti nella macchina virtuale sorgente.

Per la personalizzazione guidata di sistemi Windows precedenti a Windows 2008 e Vista, è necessario installare Microsoft Sysprep Tools nel vCenter server, mentre sui sistemi Linux deve essere presente Perl ed il volume root deve essere formattato con file system ext2, ext3 o ReiserFS.

11.5 Snapshot di una macchina virtuale

La snapshot di una VM corrisponde ad una sua istantanea registrata su disco (sullo storage fisico). L'istantanea può essere utilizzata in qualsiasi momento per riportare la macchina virtuale allo stato dell'istantanea stessa.

Una snapshot è utile quando vi è la necessità di compiere modifiche sul software della VM, ad esempio aggiornamenti del sistema operativo o modifiche sugli applicativi che vi girano sopra, garantendo la possibilità di ripristinare la VM ad uno stato precedente ed annullando eventuali problemi dovuti alle modifiche effettuate.



Possono essere create più snapshot per VM, e la relazione tra le diverse snapshot è di tipo parent-child (genitore-figlio), con organizzazione ad albero. Ogni snapshot ha un genitore ed un figlio, tranne l'ultima snapshot che non ha figli.

Una snapshot mantiene le informazioni riguardanti:

- impostazioni della VM (incluse nei file .vmx e .nvram) e stato di alimentazione;
- stato dei dischi;
- stato della memoria nel momento di creazione della snapshot.

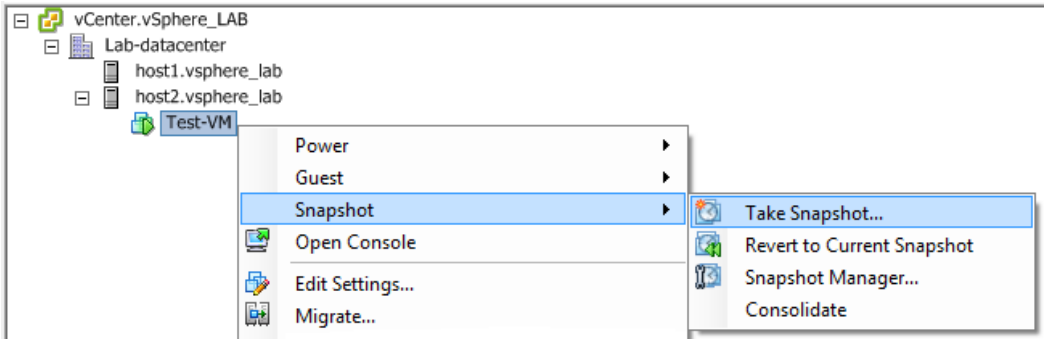
È importante rilevare che **le snapshot non possono e non devono essere considerate come un metodo di backup delle macchine virtuali**.

11.5.1 Creazione delle snapshot

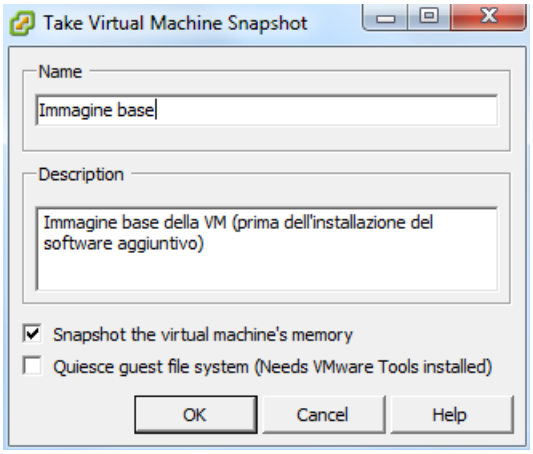
Procedura tramite vSphere Client

- Fare clic con il tasto destro sulla macchina virtuale.

- Dal menu **Snapshot**, selezionare la voce **Take snapshot**.

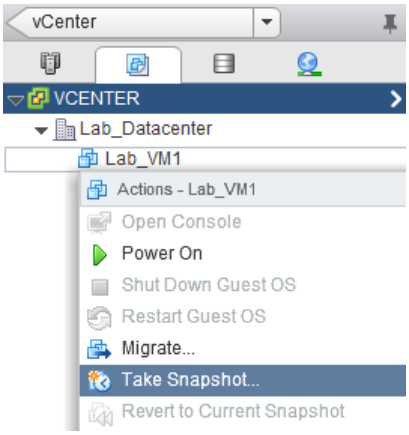


- Nel box di dialogo, bisogna specificare un nome per la snapshot e (opzionalmente) inserire una descrizione. Se si spunta l'opzione **Snapshot the virtual machine's memory**, disponibile solo per le macchine accese, il contenuto della memoria sarà salvato insieme alla snapshot. Se nel sistema operativo guest sono installati i VMware Tools, è consentito mettere in quiescenza il file system, spuntando la relativa casella.



Procedura tramite vSphere Web Client

- Fare clic con il tasto destro sulla macchina virtuale e selezionare la voce **Take snapshot**.



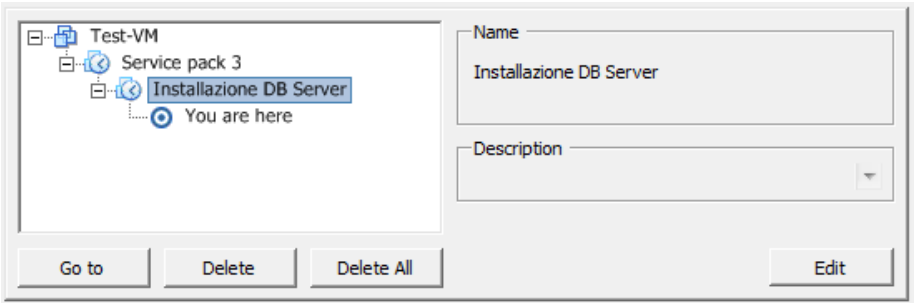
11.5.2 Gestione delle snapshot

Le snapshot possono arrivare a occupare molto spazio all'interno dello storage. L'indicazione generale è di non lasciare attive le snapshot create, perché generano un overhead nei tempi di

accesso ai dati della VM e possono crescere sullo storage fino alla dimensione del disco padre. Nel caso in cui si arrivasse ad avere il datastore con lo spazio in esaurimento a causa della crescita di una o più snapshot, sarà necessario procedere a una migrazione della VM o al consolidamento delle snapshot. L'operazione con cui si eliminano tutte le snapshot è chiamata **consolidation**. Un'altra possibilità è quella di clonare la VM su un altro datastore, perché il cloning di una macchina virtuale prevede implicitamente il consolidamento delle sue snapshot.

Gestione tramite vSphere Client

- Fare clic con il tasto destro sulla macchina virtuale.
- Dal menu **Snapshot**, selezionare la voce **Snapshot manager**.
- All'interno dello Snapshot Manager, sono possibili le operazioni indicate di seguito.
  - **Delete** - consolida le modifiche della snapshot selezionata sulla snapshot superiore (parent disk). La snapshot selezionata viene poi eliminata.
  - **Delete All** - consolida le modifiche delle snapshot precedenti allo stato corrente, quello indicato dalla voce **You are here**. Le snapshot precedenti saranno eliminate.
  - **Go to** - permette di ripristinare la VM allo stato della snapshot selezionata.



Gestione tramite vSphere Web Client

- Fare clic con il tasto destro sulla macchina virtuale e selezionare la voce **Manage Snapshots**.
- All'interno dello Snapshot Manager, sono possibili le stesse operazioni possibili indicate con vSphere Client.

11.5.3 File di una snapshot

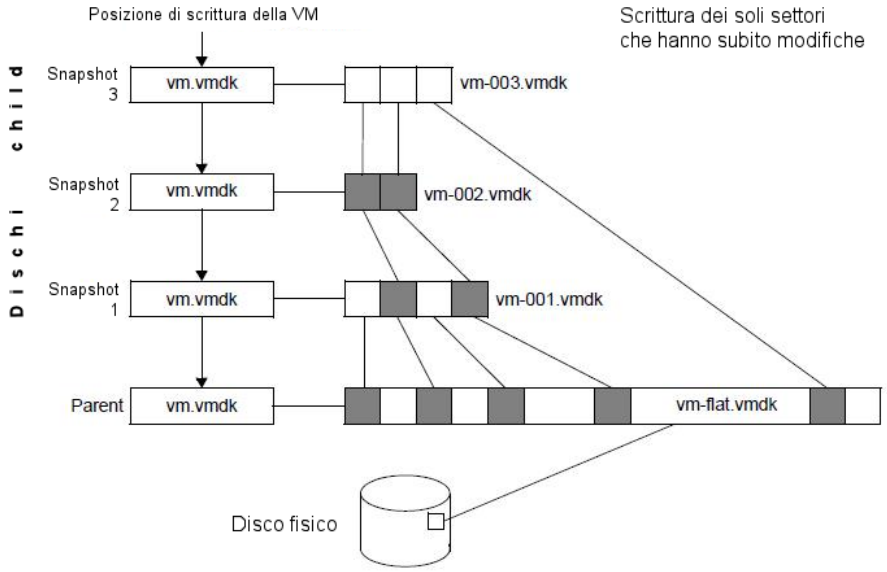
Ogni snapshot è costituita da diversi file.

- **Memory state file**, con suffisso ed estensione del tipo *nome_vm-Snapshot#**.vmsn***, rappresenta lo stato della memoria; il simbolo # è il numero di sequenza (a partire da 1). Viene creato un nuovo file per ogni nuova snapshot, poi cancellato se la relativa snapshot viene cancellata. Se, durante la creazione della snapshot, si sceglie di includere anche il contenuto di memoria della VM, questo file sarà grande quanto la dimensione della memoria, diversamente sarà di dimensioni molto ridotte.
- **Snapshot description file**, con suffisso ed estensione del tipo *nome_vm-00000#**.vmdk***, contiene informazioni sulla snapshot.
- **Snapshot delta file**, con suffisso ed estensione del tipo *nome_vm-00000#**-delta.vmdk***, contiene le modifiche effettuate sul disco della VM. Quando viene creata una snapshot, la macchina virtuale non utilizza più il suo file .vmdk per le operazioni di scrittura, ma impiega il delta disk file che conterrà tutte le modifiche successive alla creazione della snapshot.
- **Snapshot list file**, con suffisso ed estensione del tipo *nome_vm**.vmsd***, mantiene le informazioni riguardanti tutte le snapshot della macchina virtuale, ovvero i riferimenti ai

file .vmsn e .vmdk. È creato insieme alla macchina virtuale e ne esiste uno solo indipendentemente dalla presenza e dal numero di snapshot.

11.5.4 Funzionamento del processo di snapshot

Alla creazione di una snapshot, viene creato un "child disk", corrispondente al file *nome_vm-00000#-delta**.vmdk***. I dischi derivanti da una snapshot utilizzano un meccanismo di copy-on-write (copia su scrittura), ossia i blocchi dei dati modificati sono copiati dal parenti disk solo quando vi è un'operazione di scrittura. Gli incrementi sono di 16mb. Il primo disco child viene creato a partire dall'immagine base della VM (il disco originale), e le snapshot successive vengono generate a partire dal disco precedente rispetto alla struttura ad albero.



11.5.5 Esclusione di dischi dal processo di snapshot

Si possono escludere uno o più dischi dal processo di snapshot impostandoli come dischi indipendenti (**independent disk**). Quest'impostazione si effettua normalmente durante la creazione del disco, ma può essere applicata anche successivamente, a macchina virtuale spenta.

Un disco indipendente può essere di tipo **persistent** o **nonpersistent**. Nel primo caso, alla creazione di una snapshot, per questo disco non vengono generati file "delta", e le successive scritture su disco sono mantenute anche in caso di eliminazione della snapshot.
Nel secondo caso, viene impiegato un meccanismo di log (**redo log**) per tracciare le modifiche effettuate su disco dopo la creazione della snapshot. Il redo log e le scritture su disco vengono perse con lo spegnimento o il riavvio della macchina virtuale.

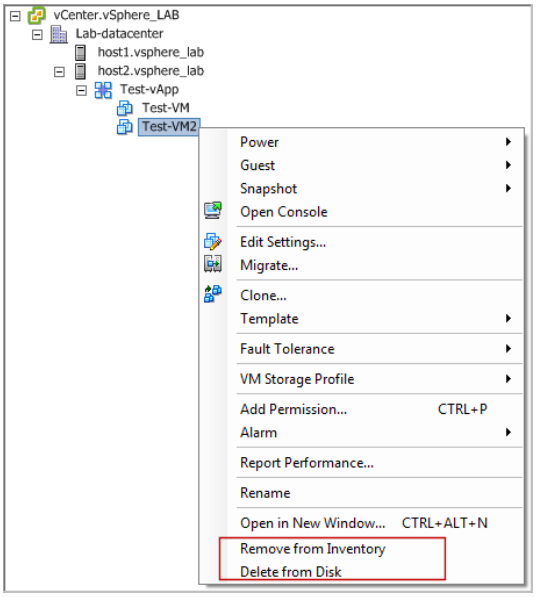
11.6 Rimozione di una macchina virtuale

Le macchine virtuali possono essere rimosse dall'inventario o dal disco. Nel primo caso la macchina virtuale viene rimossa dal database del vCenter Server e dall'host che la ospitava, ma non vengono rimossi i suoi file presenti nello storage. Nel secondo caso vengono invece eliminati tutti i file della VM presenti nel datastore (non si può recuperare la VM se non da un backup).

Procedura con vSphere Client

- Fare clic con il tasto destro sulla VM.

- Selezionare una delle due voci **Remove from Inventory** o **Delete from Disk**.



Procedura con vSphere Web Client

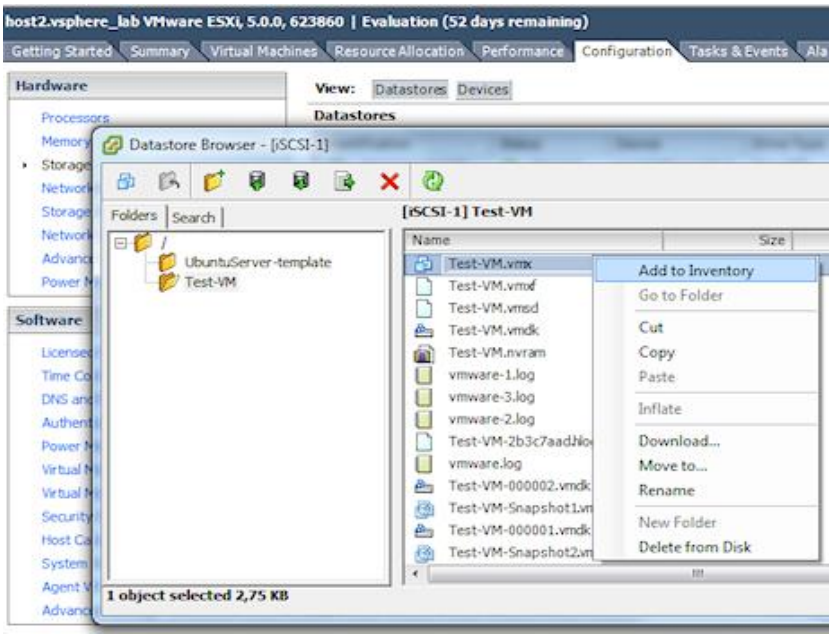
- Fare clic con il tasto destro sulla VM.
- Fare clic su **All vCenter Actions**.
- Selezionare una delle due voci **Remove from Inventory** o **Delete from Disk**.

11.7 Registrazione di una macchina virtuale

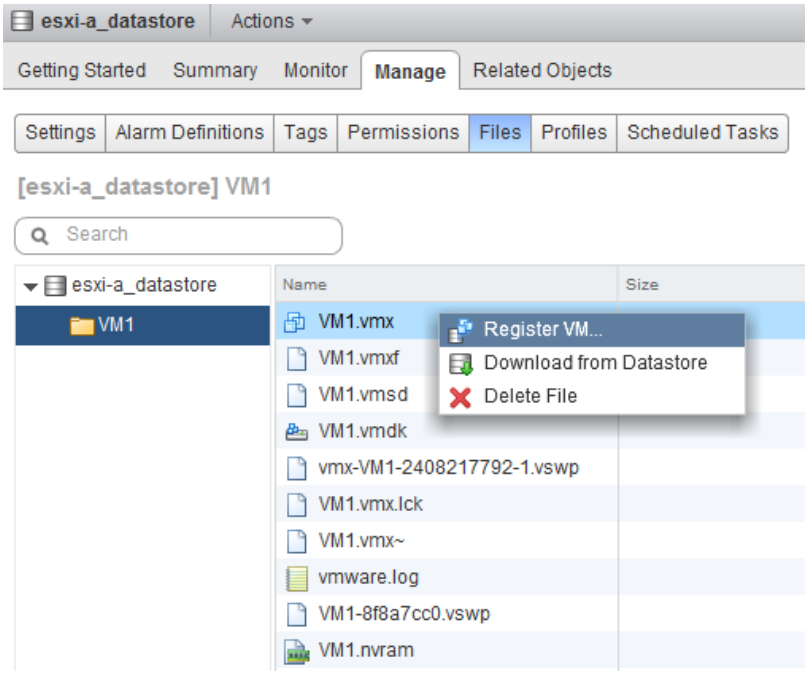
È possibile registrare ed aggiungere all'inventario una VM rimossa precedentemente (ma non cancellata dal disco), oppure una VM copiata o spostata da diverso host/datastore.

Per procedere con la registrazione di una VM, individuare il file **.vmx** della macchina virtuale, fare clic con il tasto destro su di esso e selezionare la voce **Add to inventory** (**Register VM** su vSphere Web Client).

Procedura con vSphere Client



Procedura con vSphere Web Client



11.8 VMware vApp

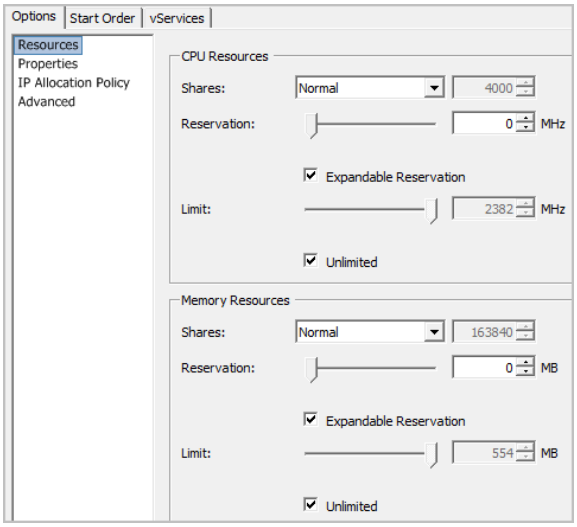
Una vApp è principalmente un **contenitore di macchine virtuali**. Permette di ridurre le operazioni di manutenzione eseguite quotidianamente dagli amministratori: le azioni eseguite su una vApp, infatti, si riflettono su tutti gli oggetti contenuti al suo interno. Tramite vApp, ad esempio, possiamo spegnere, accendere o clonare tutte le VM presenti all'interno della vApp stessa. Una vApp è non solo un contenitore di macchine virtuali, ma allo stesso tempo un **resource pool** per quelle macchine virtuali. Se ci si collega direttamente a un host ESXi tramite vSphere Client, la vApp è rappresentata come Resource Pool; per visualizzare una vApp in quanto tale, è necessario collegarsi al vCenter Server.

È possibile creare una nuova vApp selezionando un singolo host ESXi o un cluster DRS dall'inventario. Con vSphere Web Client, fare clic con il tasto destro su un host o un cluster DRS e selezionare le voci **All vCenter Actions** > **New vApp**. Con vSphere Client, fare clic con il tasto destro su un host o un cluster DRS e selezionare la voce **New vApp**.

Le impostazioni di una vApp possono essere specificate sia in fase di creazione, sia successivamente, facendo clic con il tasto destro su di essa e selezionando la voce **Edit Settings**.

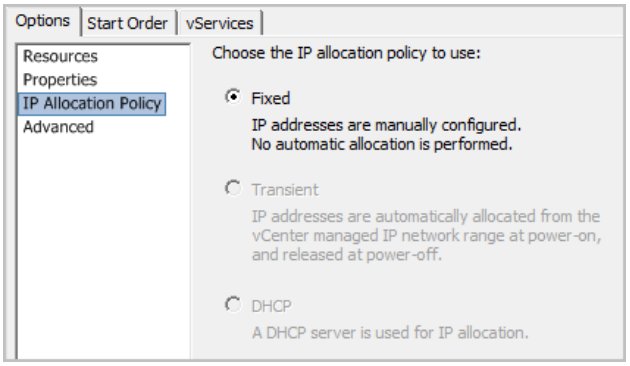
Le impostazioni possibili sono indicate di seguito.

- **Allocazione delle risorse di memoria e di CPU**.
  - **Shares** - priorità sull'accesso della vApp alle risorse condivise.
  - **Reservation** - valore minimo di risorse garantite e preallocate per la vApp.
  - **Limit** - valore massimo di risorse che non può mai essere superato. Nel caso della CPU il valore è espresso in cicli (MHz), nel caso della memoria è espresso in Mb.

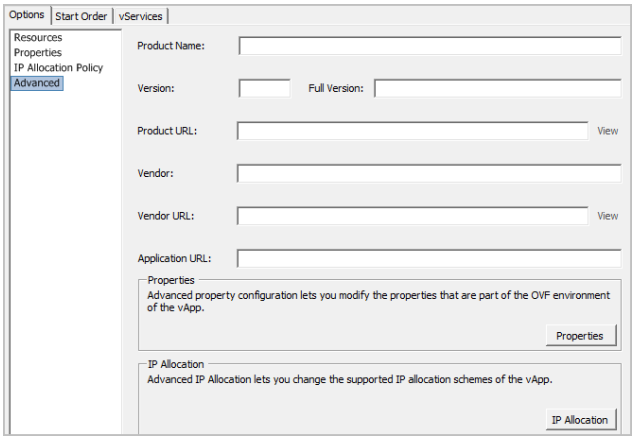


  I concetti di allocazione delle risorse saranno trattati in maniera approfondita nel capitolo "Gestione e controllo delle risorse".

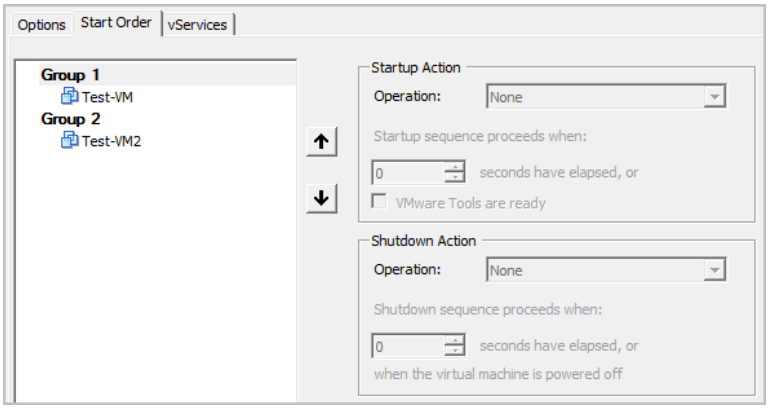
- **Politica di allocazione IP** – permette di specificare come devono essere allocati gli indirizzi IP all'interno della vApp. Esistono la modalità manuale (**Fixed**), automatica con **DHCP**, oppure allocazione tramite un pool che si attiva nel momento in cui la vApp viene accesa (**Transient**).



- **Impostazioni avanzate** – permettono di specificare informazioni riguardanti il vendor, le proprietà specifiche della vApp e l'allocazione degli IP.



- **Start Order** - permette di impostare l'ordine di accensione e spegnimento delle VM, con una procedura che prevede la creazione di gruppi di VM.



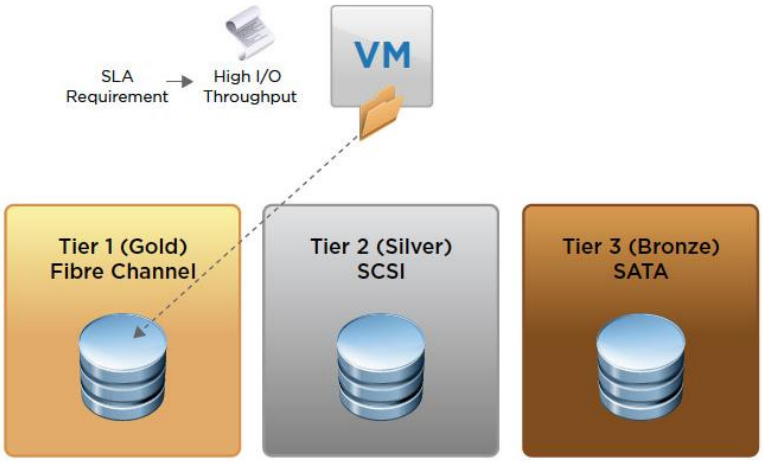
Capitolo 12
Profili storage per le macchine virtuali

L'ambiente vSphere consente di mettere in relazione le diverse tipologie di datastore con le macchine virtuali attraverso la funzionalità **Profile-Driven Storage**, che consente il posizionamento rapido e intelligente delle macchine virtuali in base a SLA, disponibilità, prestazioni e in base alle funzionalità di storage fornite.

Le diverse caratteristiche dello storage, definite **Storage Capabilities**, possono essere collegate ad un profilo storage, e quest'ultimo associato ad una macchina virtuale. I profili sono impiegati durante il provisioning, la duplicazione e l'uso di Storage vMotion, e permettono a una VM l'utilizzo di uno storage che garantisca determinati livelli di qualità, disponibilità e prestazioni.

Profile-Driven Storage comprende diversi funzionalità.

- Integrazione completa con **vSphere Storage API for Storage Awareness** (VASA) - lo storage con supporto VASA comunica al vCenter Server l'insieme di funzionalità che può garantire. Il vCenter riconosce tali capacità, e le inserisce nella lista delle **Storage Capabilities**.
- Supporto per lo Storage NFS, iSCSI e Fibre Channel (FC), e per tutti gli array di Storage inclusi nell'elenco di compatibilità hardware per VMware vSphere.
- Possibilità di creare regole di posizionamento per le macchine virtuali sotto forma di profili storage.
- Possibilità di verificare facilmente la conformità di una macchina virtuale con tali regole.



12.1 Storage capabilities

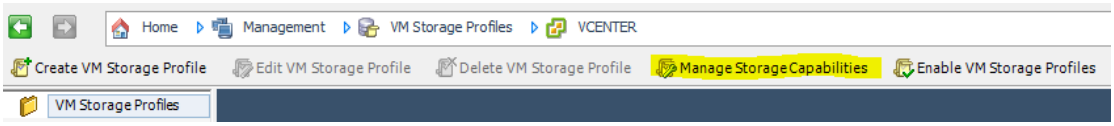
12.1.1 Verifica delle capacità dello Storage

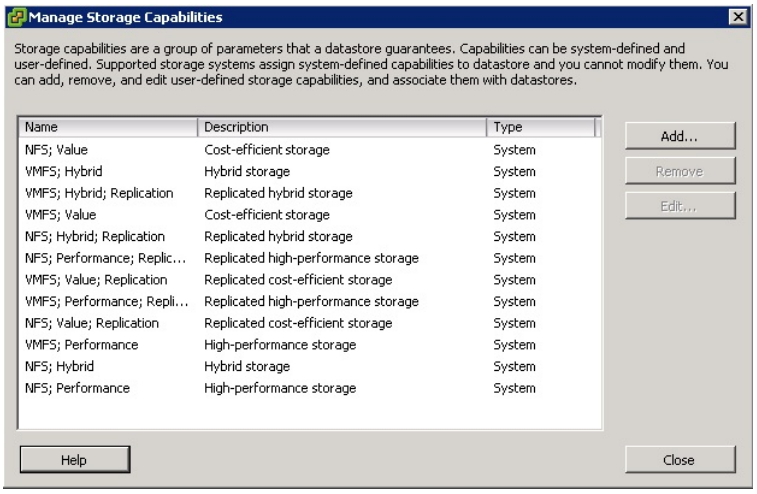
Se un sistema storage supporta l'interfaccia VASA, è possibile verificare le sue capacità definite a livello di sistema.

Procedura tramite vSphere Client

- Andare su **Management > VM Storage Profiles**.

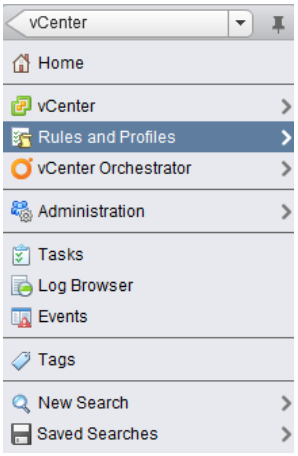
- Fare clic su **Manage Storage Capabilities**.

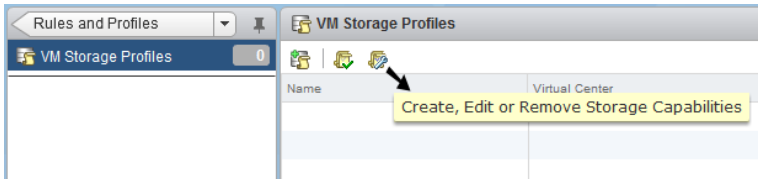




Procedura tramite vSphere Web Client

- Dalla home page fare clic su **Rules and Profiles > VM Storage Profiles**.



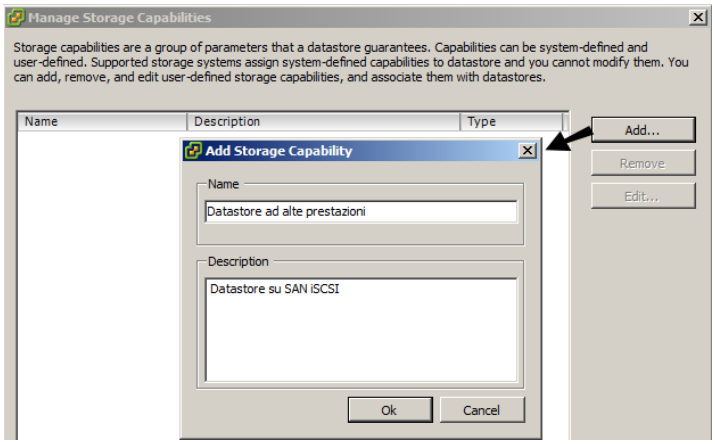


12.1.2 Creazione di una storage capability personalizzata

Se un sistema storage non supporta l'interfaccia VASA, è possibile creare una Storage Capability e assegnarla ad un datastore di quel sistema, così da definirne le capacità che può garantire.

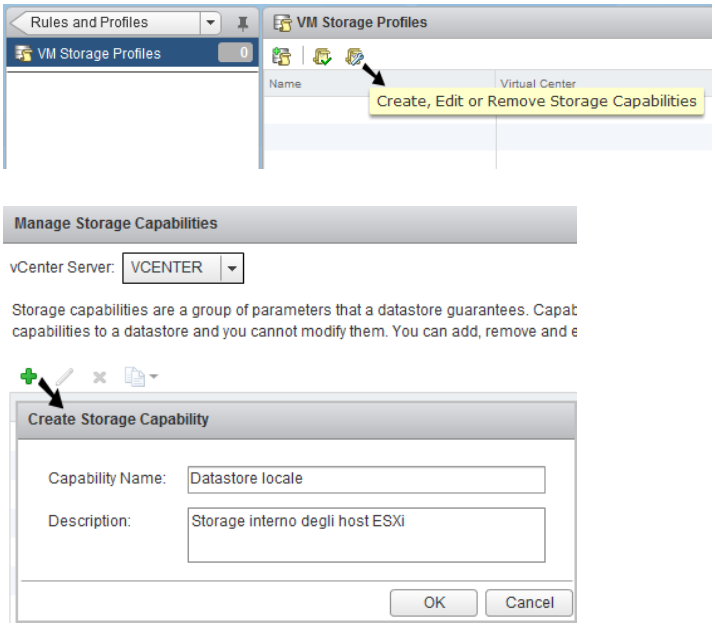
Procedura tramite vSphere Client

- Andare su **Management > VM Storage Profiles** e fare clic su **Manage Storage Capabilities**.
- Nella finestra di gestione delle Storage Capabilities, fare clic su **Add** ed inserire un nome ed una descrizione per la capability.



Procedura tramite vSphere Web Client

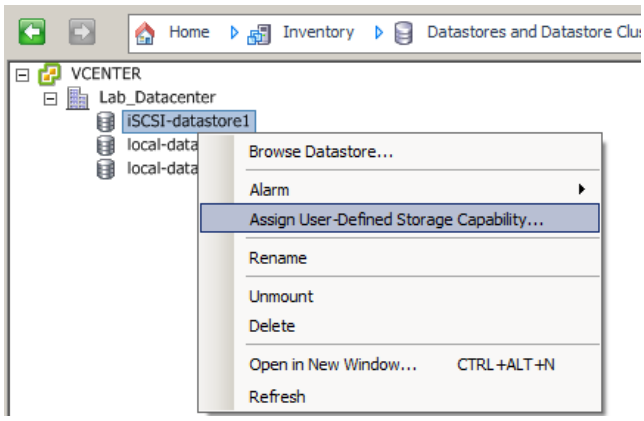
- Dalla home page fare clic su **Rules and Profiles > VM Storage Profiles**.
- Fare clic sull'icona **Create, Edit or Remove Storage Capabilities.**
- Nella finestra di gestione delle Storage Capabilities, fare clic su **Add** ed inserire un nome ed una descrizione per la capability.



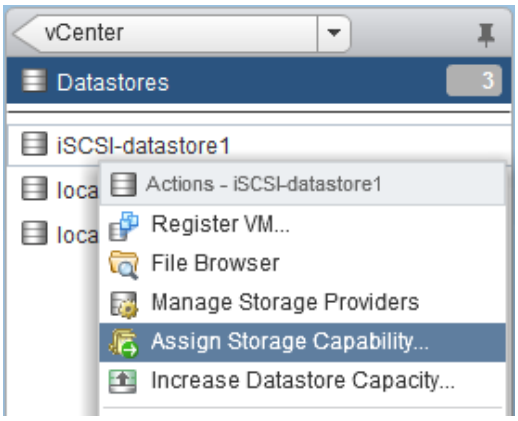
12.1.3 Assegnazione di una storage capability ad un datastore

Dopo aver definito una capability, è necessario assegnarla al datastore che possiede le caratteristiche in essa indicate. Sia con **vSphere Client** che con **vSphere Web Client**, è sufficiente selezionare il datastore da modificare, fare clic con il tasto destro su di esso e selezionare la voce **Assign Storage Capability**.

Procedura tramite vSphere Client



Procedura tramite vSphere Web Client



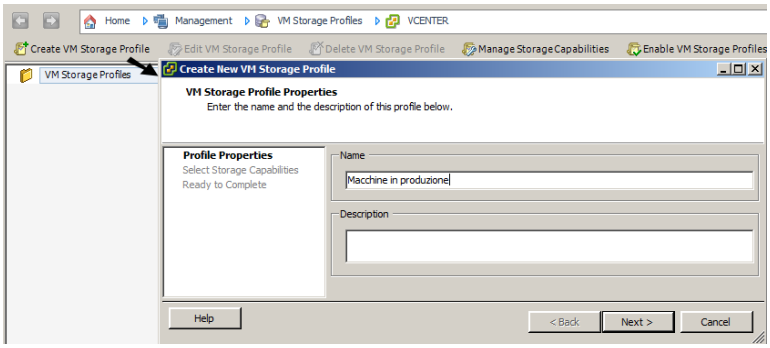
12.2 Creazione di un profilo storage

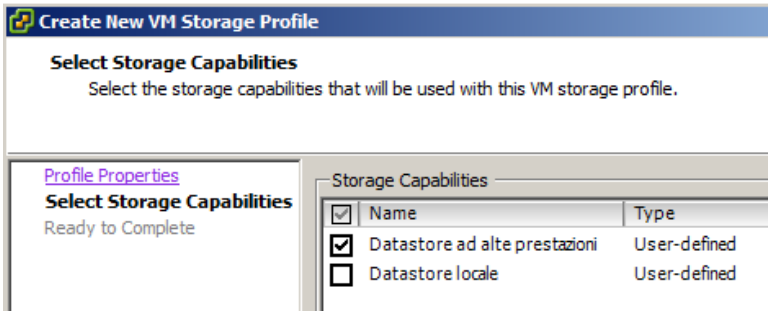
Un profilo storage contiene le informazioni su caratteristiche e capacità dello storage. Abbiamo visto come tali capacità siano definibili a livello utente, oppure possono emergere direttamente dagli storage con supporto VASA. Un profilo viene associato ad una VM durante il provisioning, la creazione di dischi VMDK, la migrazione, la duplicazione e così via. Durante queste operazioni, il client vSphere mostra i datastore che garantiscono le capacità indicate nel profilo storage. In questo modo il provisioning di una VM viene sempre effettuato su un datastore conforme, contenente le caratteristiche di storage corrette per la VM. Una volta che la VM è posizionata su un datastore conforme, la VM stessa viene dichiarata conforme.

È possibile creare un elenco di profili storage, riferiti a diversi livelli di caratteristiche storage.

Procedura con vSphere Client

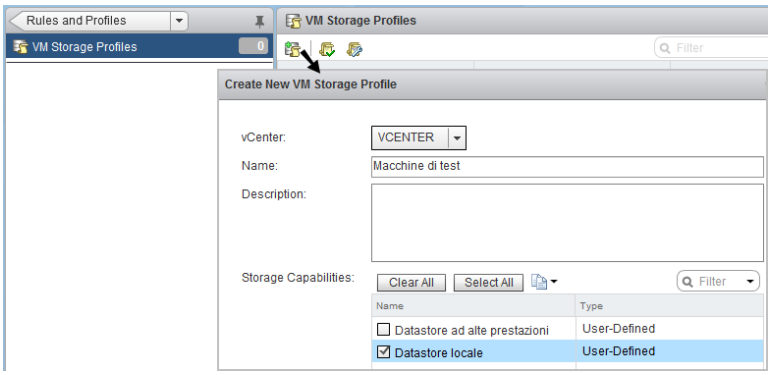
- Andare su **Management > VM Storage Profiles** e fare clic su **Create VM Storage Profile**.
- Nella finestra che si aprirà, inserire un nome ed una descrizione per il profilo, quindi selezionare le Storage Capabilities da associare al profilo.





Procedura con vSphere Web Client

- Dalla home page fare clic su **Rules and Profiles > VM Storage Profiles**.
- Fare clic sull'icona **Create a new VM Storage Profile**.
- Nella finestra che si aprirà, inserire un nome ed una descrizione per il profilo, quindi selezionare le Storage Capabilities da associare al profilo.

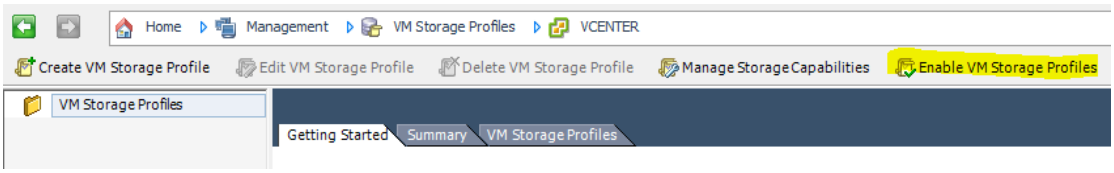


12.3 Attivazione dei profili storage

Prima di poter utilizzare i profili storage, è necessario attivarli a livello di host o di cluster.

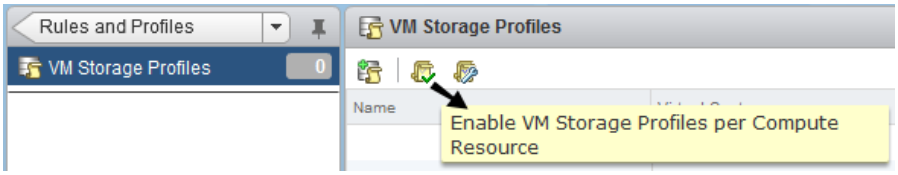
Procedura tramite vSphere Client

- Andare su **Management > VM Storage Profiles** e fare clic su **Enable VM Storage Profiles**.
- Nella finestra che si aprirà, selezionare l'host o il cluster per cui abilitare i profili storage e fare clic su **Enable**.



Procedura tramite vSphere Web Client

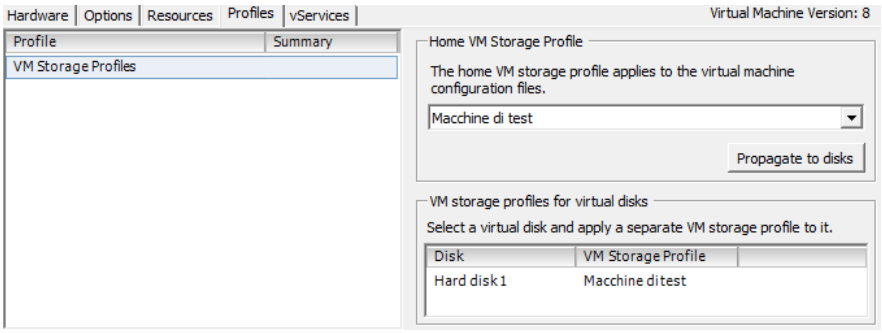
- Dalla home page fare clic su **Rules and Profiles > VM Storage Profiles**.
- Fare clic sull'icona **Enable VM Storage Profiles**. Nella finestra che si aprirà, selezionare l'host o il cluster per cui abilitare i profili storage e fare clic su **Enable**.



12.4 Applicare un profilo storage a una macchina virtuale

Procedura con vSphere Client

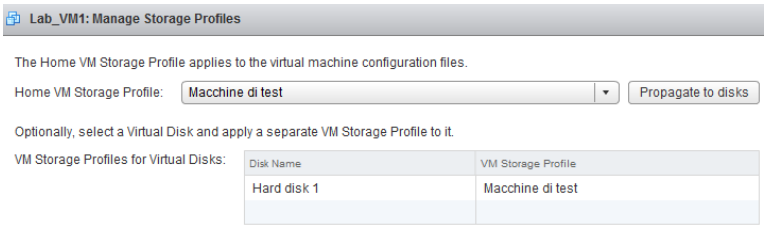
- Fare clic con il tasto destro sulla VM a cui applicare il profilo storage e selezionare le voci **VM Storage Profile > Manage Profiles**.
- In alternativa, entrare nelle impostazioni della VM e fare clic sul tab **Profiles**.
- Nel riquadro a destra **Home VM Storage Profile**, selezionare il profilo storage desiderato. Il profilo sarà applicato ai cosiddetti "virtual machine home files", ossia i vari file della VM con estensione .vmx, .vmsd, .nvram, ecc., ad esclusione dei dischi virtuali.
- Per propagare il profilo ai dischi, fare clic su **Propagate to disks**. È comunque possibile selezionare un profilo specifico per ogni disco, tramite il menu a tendina nella colonna **VM Storage Profile**.



- Una volta assegnato, il profilo storage apparirà sul pannello **VM Storage Profiles**, nel tab **Summary** della VM.

Procedura con vSphere Web Client

- Fare clic con il tasto destro sulla VM a cui applicare il profilo storage e selezionare le voci **All vCenter Actions > Storage Profiles > Manage Storage Profiles**.
- In alternativa, entrare nelle impostazioni della VM, fare clic sul tab **Manage**, andare su **Profiles** e fare clic su **Manage Storage Profiles.**
- Nel riquadro che si aprirà, dal menu **Home VM Storage Profile** selezionare il profilo storage desiderato. Per propagare il profilo ai dischi, fare clic su **Propagate to disks**. È comunque possibile selezionare un profilo specifico per ogni disco, tramite il menu a tendina nella colonna **VM Storage Profile**.



- Una volta assegnato, il profilo storage apparirà sul pannello **VM Storage Profiles**, nel tab **Summary** della VM.

12.5 Verifica della conformità di un profilo

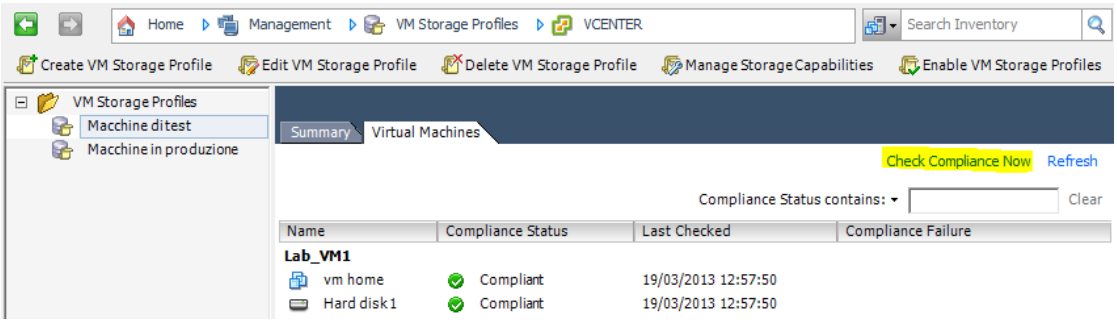
Quando si associa un profilo storage ad una macchina virtuale, e si selezionano i datastore per dischi e file relativi alla macchina stessa, è possibile verificare se i datastore utilizzati sono conformi con il profilo storage. In pratica si esegue la verifica della conformità (**compliance**).

La verifica può portare a 2 risultati.

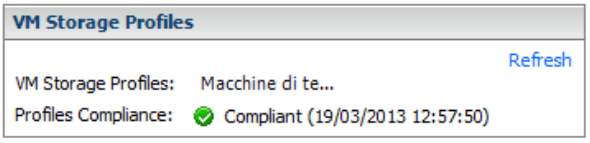
- Conforme (compliant) - i datastore utilizzati per la VM hanno caratteristiche e capacità in linea con quanto indicato nel profilo storage utilizzato.
- Non conforme (non-compliant) - i datastore utilizzati per la VM non hanno le caratteristiche e le capacità previste dal profilo storage utilizzato. In tal caso sarà possibile migrare file e dischi virtuali su un datastore conforme.

Procedura con vSphere Client

- Andare su **Management > VM Storage Profiles** e selezionare un profilo storage dall'inventario.
- Selezionare il tab **Virtual Machines**. Il tab mostra le macchine virtuali e i dischi virtuali che utilizzano il profilo storage selezionato.
- Fare clic su **Check Compliance Now**. Nella colonna **Compliance Status** apparirà il risultato della verifica.

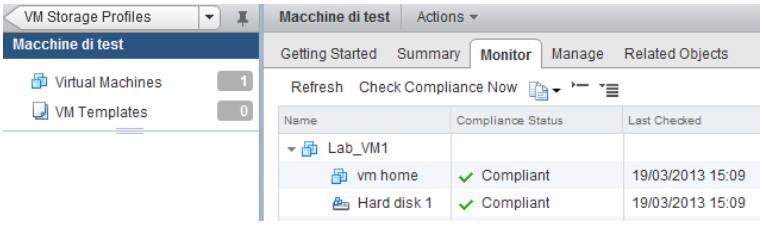


- In alternativa, fare clic con il tasto destro su una VM e selezionare le voci **VM Storage Profile > Check Profiles Compliance**. Andare quindi sul tab **Summary**: le informazioni sulla conformità sono visibili nel pannello **VM Storage Profiles**.

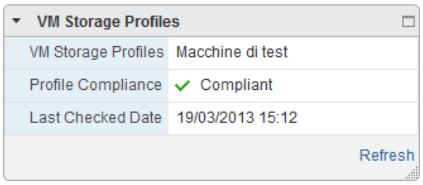


Procedura con vSphere Web Client

- Dalla pagina Home, fare clic sulle voci **Rules and Profiles > VM Storage Profiles**.
- Nella lista **VM Storage Profiles**, fare doppio clic su un profilo storage esistente.
- Fare clic sul tab **Monitor** e clic su **Check Compliance Now**. Nella colonna **Compliance Status** apparirà il risultato della verifica.



- In alternativa, fare clic con il tasto destro su una VM e selezionare le voci **All vCenter Actions > Storage Profiles > Check Storage Profile Compliance**.
- Andare quindi sul tab **Summary**: le informazioni sulla conformità sono visibili nel pannello **VM Storage Profiles**.



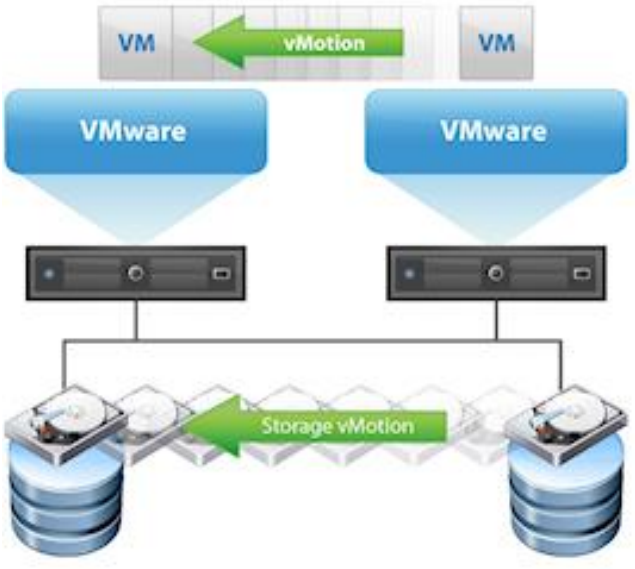
Capitolo 13
Migrazione delle macchine virtuali

13.1 Tipi di migrazione possibili

VMware vSphere prevede diverse possibilità per la migrazione delle macchine virtuali tra host e tra storage diversi.

- Migrazione di tipo **Cold** (a freddo), ossia migrazione della VM spenta, utilizzabile per lo spostamento su diverso host o diverso datastore.
- Migrazione di tipo **Suspended**, in altre parole migrazione della VM messa in pausa, utilizzabile per lo spostamento su diverso host o diverso datastore.
- Migrazione tramite **vMotion**, ovvero migrazione della **VM accesa**, utilizzabile per lo spostamento tra host diversi.
- Migrazione tramite **Storage vMotion**, ovvero migrazione della **VM accesa** su diverso datastore.

Entrambi i servizi vMotion e Storage vMotion consentono di migrare macchine virtuali mantenendole accese, senza causare interruzioni per gli utenti o perdite di dati. Prima di vSphere 5.1, per sfruttare il servizio di vMotion era richiesto che le macchine virtuali fossero residenti su uno storage condiviso, all'interno di partizioni VMFS. Con vSphere 5.1 la migrazione non richiede uno storage condiviso, ed è resa possibile anche con VM posizionate all'interno di datastore locali. In sostanza è possibile il cambio simultaneo di storage e host, ossia è permessa una combinazione di vMotion e Storage vMotion in un unico passaggio. Da evidenziare il fatto che tale migrazione combinata è possibile solo utilizzando vSphere Web Client, ed è disponibile in tutte le edizioni di vSphere che abbiamo la licenza per l'uso del vMotion.



Le migrazioni cold e suspended possono essere utilizzate per lo spostamento di una VM su datacenter diverso, operazione non possibile con il vMotion.

Per quanto riguarda i dispositivi RDM:

- la migrazione vMotion non modifica i dischi RDM; questi rimangono tali anche dopo la registrazione della VM su un altro host;

- la migrazione Storage vMotion consente lo spostamento dei dischi RDM sul datastore di destinazione (viene spostato il file di mappatura .vmdk).

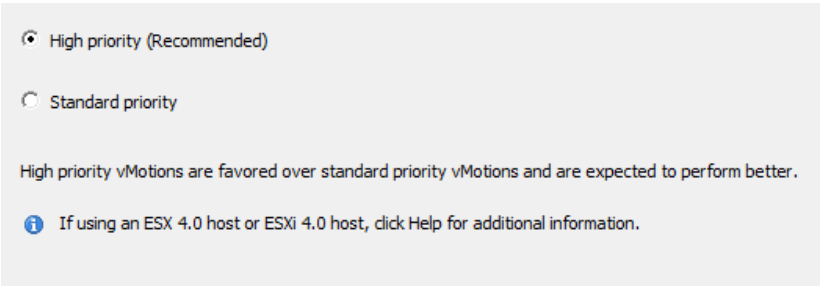
13.2 vSphere vMotion

13.2.1 Migrazione di una macchina virtuale con vSphere vMotion

Con il vMotion, l'intero stato di una macchina virtuale viene traslato da un host ad un altro. Per stato di una VM si intende il contenuto della sua memoria e tutte le informazioni relative all'hardware, quali BIOS, elenco dispositivi, CPU, interfacce di rete e relativi MAC-address. Prima di iniziare la migrazione della VM, il vCenter Server esegue una pre-verifica dei requisiti: gli avvisi appariranno in giallo, e consentiranno di proseguire, mentre gli errori appariranno in rosso, e non consentiranno la migrazione.

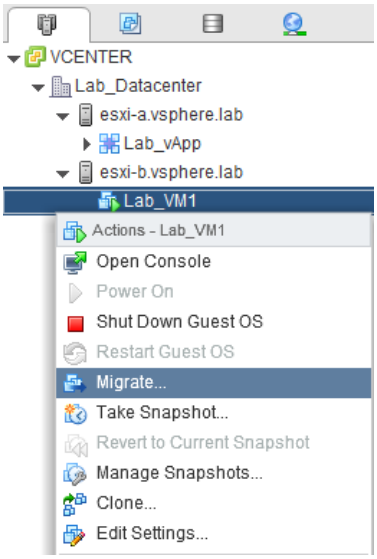
Procedura tramite vSphere Client

- Fare clic con il tasto destro sulla macchina accesa e selezionare la voce **Migrate**.
- In caso di storage condiviso, nella procedura guidata selezionare la voce **Change host**. In tal caso, dopo la migrazione, i file della VM saranno sempre nello stesso storage. Se invece la VM risiede su un datastore locale, sarà necessario procedere a un cambio simultaneo di host e datastore, selezionando la voce **Change both host and datastore**.
- È possibile impostare la priorità del vMotion utilizzando le opzioni High Priority e Standard Priority.
  - **High Priority** – negli host con ESX/ESXi versioni 4.1 e successive, vCenter Server cerca di riservare le risorse ad entrambi gli host di origine e di destinazione, affinché siano disponibili per tutte le migrazioni simultanee. Il vCenter Server garantisce una quota maggiore di risorse CPU alle migrazioni ad alta priorità rispetto alle migrazioni a priorità standard. In ogni caso le migrazioni saranno portate a termine indipendentemente dalle risorse riservate.
  - **Standard Priority** – negli host con ESX/ESXi versioni 4.1 e successive, vCenter Server riserva le risorse ad entrambi gli host di origine e di destinazione, affinché siano rese disponibili per tutte le migrazioni simultanee. Il vCenter Server concede una quota minore di risorse CPU alle migrazioni a priorità standard rispetto alle migrazioni ad alta priorità. In ogni caso le migrazioni saranno portate a termine indipendentemente dalle risorse riservate.

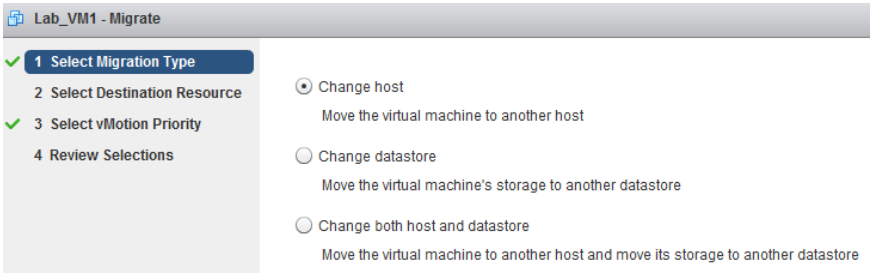


Procedura tramite vSphere Web Client

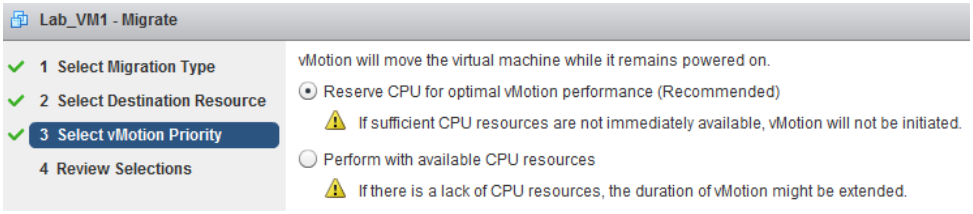
- Fare clic con il tasto destro sulla macchina accesa e selezionare la voce **Migrate**.



- In caso di storage condiviso, nella procedura guidata selezionare la voce **Change host**. Così facendo, dopo la migrazione i file della VM saranno sempre nello stesso storage. Se invece la VM risiede su un datastore locale, sarà necessario procedere con un cambio simultaneo di host e datastore, selezionando la voce **Change both host and datastore**.



- È possibile impostare la priorità del vMotion in base a due opzioni.
  - **Reserve CPU for optimal VMotion performance** - il vCenter Server cerca di riservare risorse ad entrambi gli host di origine e di destinazione, affinché queste siano disponibili per tutte le migrazioni eseguite contemporaneamente. Sono garantite elevate risorse CPU. Se tali risorse non sono disponibili, l'operazione di vMotion non viene avviata.
  - **Perform with available CPU resources** - il vCenter Server cerca di riservare risorse ad entrambi gli host di origine e di destinazione, affinché queste siano disponibili per tutte le migrazioni eseguite contemporaneamente. Per l'operazione, sono assegnate risorse CPU limitate. Se non c'è disponibilità di risorse, la durata del vMotion può essere estesa.



13.2.2 Requisiti per le migrazioni con vSphere vMotion

La migrazione di una VM richiede una corretta configurazione della rete sia per l'host sorgente, sia per quello di destinazione.

In particolare si consiglia quanto di seguito indicato.

- Su ogni host, configurare un'interfaccia VMkernel per il vMotion.
- Utilizzare interfacce fisiche Gigabit per il vMotion; è preferibile che gli host abilitati al vMotion siano attestati su una rete Gigabit Ethernet.
- Se nell'host sono disponibili solo due interfacce di rete:
    - dedicare l'interfaccia gigabit al vMotion, e nell'altra interfaccia utilizzare le VLAN per dividere il traffico delle VM dal traffico di management;
    - in alternativa, per una miglior disponibilità, combinare entrambe le interfacce in teaming, e utilizzare le VLAN per la separazione del traffico: una o più VLAN per il traffico delle VM e una per il vMotion;
- Assicurarsi che la rete virtuale su cui è attestata una VM sia presente anche nell'host di destinazione; durante la migrazione il vCenter Server assegna le macchine virtuali ad un determinato virtual switch sulla base del nome assegnato al port group, nome che deve avere corrispondenza tra host sorgente e host di destinazione.
- Perché la migrazione con vMotion possa andare avanti, la VM non deve trovarsi su switch privi di uplink (virtual intranet).

Per quanto riguarda gli host, i requisiti per una migrazione vMotion sono indicati di seguito.

- Se si esegue il vMotion classico, con cambio del solo host, è richiesta la visibilità dello stesso datastore da entrambi gli host (sorgente e destinazione).
- Compatibilità tra host a livello di CPU; ad esempio, se la CPU dell'host sorgente supporta le estensioni SSE4.1 e questo supporto non esiste nella CPU di destinazione, la migrazione vMotion fallisce.
- Se la VM ha dischi RDM, questi devono essere visibili e accessibili anche dall'host di destinazione; inoltre i file di mapping dei dischi RDM devono trovarsi nello stesso datastore.
- La VM da migrare non può avere immagini CDROM e floppy montate.

13.2.3 Funzionamento di vSphere vMotion

- Appena avviata l'operazione di vMotion (Change Host), la memoria della macchina virtuale viene copiata dall'host sorgente a quello di destinazione, attraverso la rete, con gli utenti che possono continuare ad accedere alla VM. Di conseguenza è possibile una modifica di pagine di memoria anche durante il vMotion; il meccanismo prevede che di queste modifiche sia tenuta traccia nell'host sorgente, su una **memory bitmap**.
- Prima che sia completamente trasferita sull'host di destinazione, la VM è portata in uno stato di quiescenza, dove non sono più possibili modifiche. Nella fase di quiescenza sono trasferiti sull'host di destinazione lo stato dei dispositivi e la memory bitmap.
- Non appena entra in quiescenza, la VM viene avviata nell'host di destinazione; la rete è informata del cambio di switch tramite protocollo RARP (Reverse ARP) e, terminata la fase di sincronizzazione del punto precedente, gli utenti potranno accedere alla macchina ospitata sul nuovo host.

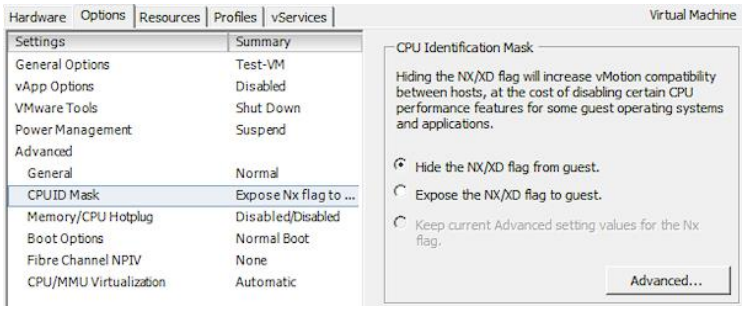
13.2.4 Flag NX/DX

Nelle impostazioni di una macchina virtuale, alla voce **CPUID Mask** è possibile impostare le funzioni **AMD No eXecute (NX)** e **Intel eXecute Disable (XD)**. Si tratta di due tecnologie di sicurezza, implementate a livello di CPU, che seguono lo stesso obiettivo: marcare le pagine di memoria come "data-only" per evitare l'esecuzione di codice dannoso o attacchi di buffer overflow. Il meccanismo prevede l'isolamento delle aree di memoria da dedicare alle istruzioni della CPU oppure ai dati. Se un'area di memoria è contrassegnata con il flag NX o XD, non vi possono risiedere istruzioni, ma solo dati.

Se la tecnologia è abilitata su un host sorgente, vMotion richiede che sia abilitata anche sull'host di destinazione. Sulle macchine virtuali il flag NX/DX è esposto in maniera predefinita, pertanto se l'host utilizza questa tecnologia, anche i sistemi operativi guest possono utilizzarla. Disattivare l'esposizione del flag sulle macchine virtuali aumenta la compatibilità tra host per le operazioni di vMotion, al costo di disattivare le relative funzioni di sicurezza.

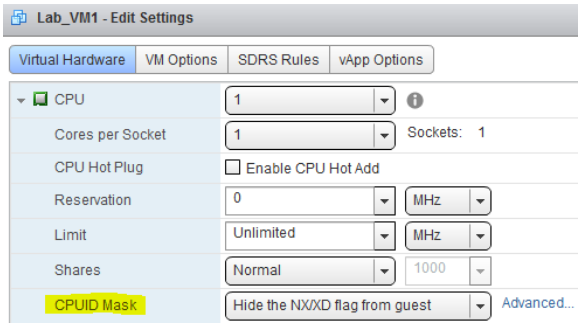
Nascondere l'esposizione del flag NX/XD con vSphere Client

- Entrare nelle impostazioni della VM e andare nel tab **Options**.
- Selezionare la voce **CPUID Mask** e impostare l'opzione **Hide the NX/DX flag from guest**. La modifica non può essere eseguita a caldo (con la macchina in esecuzione).



Nascondere l'esposizione del flag NX/XD con vSphere Web Client

- Entrare nelle impostazioni della VM.
- Selezionare la CPU e impostare l'opzione **Hide the NX/DX flag from guest** nel relativo campo **CPUID Mask.** La modifica non può essere eseguita a caldo (con la macchina in esecuzione).

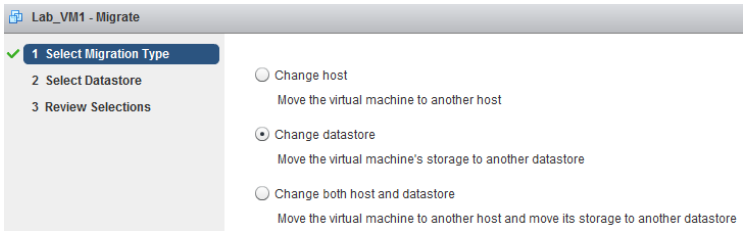


13.3 vSphere Storage vMotion

Lo storage vMotion impiega la stessa tecnologia del vMotion, applicata però ai file delle macchine virtuali, che possono essere spostati da un datastore ad un altro mantenendo le VM accese. La tecnologia è indipendente dal tipo di storage utilizzato, e può lavorare indifferentemente attraverso datastore NFS o datastore VMFS su iSCSI, Fibre Channel o storage locale.

13.3.1 Migrazione di una macchina virtuale con vSphere Storage vMotion

Per migrare una VM utilizzando Storage vMotion, sia con vSphere Client che con vSphere Web Client, fare clic con il tasto destro sulla macchina accesa e selezionare la voce **Migrate**. Nella procedura guidata, selezionare la voce **Change datastore**.



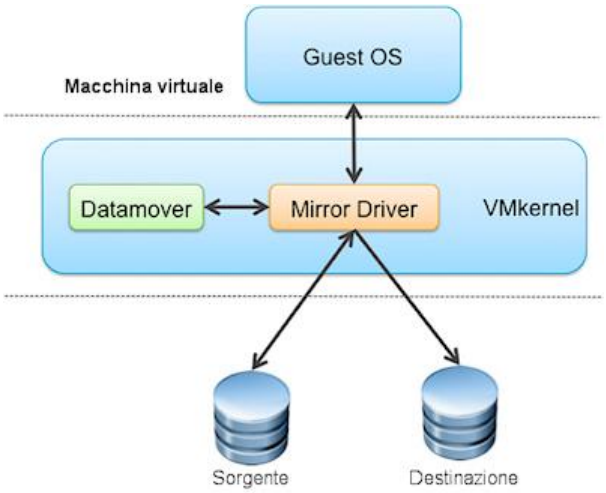
13.3.2 Funzionamento di vSphere Storage vMotion

Una migrazione con Storage vMotion prevede l'utilizzo di un'architettura di tipo mirroring, con copia di blocchi disco tra datastore sorgente e datastore di destinazione.

1. Il processo di migrazione esegue un primo passaggio nel datastore sorgente, copiando tutti i blocchi necessari sul datastore di destinazione.
2. Se alcuni blocchi subiscono modifiche durante il processo di copia, saranno sincronizzati tramite un driver chiamato **Mirror Driver**, che evita inutili passaggi ricorsivi su tutti i blocchi.

Nelle versione 4.x di vSphere il componente che si occupava del controllo della migrazione storage si chiamava **Change Block Tracking** (**CBT**). CBT segna i blocchi già copiati che sono stati modificati durante il processo di migrazione, e alla fine del processo si dedica alla sincronizzazione delle modifiche di cui si è tenuta traccia. La nuova tecnologia del Mirror Driver di vSphere 5 permette la migrazione del disco con un singolo passaggio, migliorando i tempi di migrazione e aumentando l'efficienza.

Il Mirror Driver fa parte del VMkernel e viene attivato per ogni macchina virtuale. Quando il processo di migrazione è avviato e avviene una modifica sul disco della VM in fase di spostamento, il Mirror Driver copia su entrambi i dischi (sorgente e destinazione) le modifiche e attende il consenso di entrambi i dischi virtuali prima di inviare l'informazione di modifica al sistema operativo Guest. Questa funzione non solo aumenta l'efficienza di Storage vMotion, ma anche la prevedibilità dei tempi di migrazione, semplificando così la pianificazione delle migrazioni e riducendo il tempo di esecuzione per ciascuna migrazione.



Perché la migrazione di una VM con storage vMotion possa essere portata avanti, i dischi della VM **non possono essere in modalità non-persistent**. Ricordiamo che con vSphere 5.1 è stata introdotta la possibilità di eseguire contemporaneamente una migrazione host e storage anche su macchine virtuali accese. Tuttavia, la migrazione di macchine virtuali durante l'installazione dei VMware Tools non è supportata.

Lo storage vMotion supporta la migrazione di dischi RDM, alle seguenti condizioni:

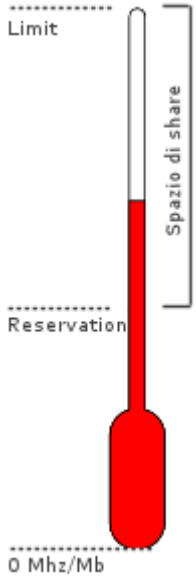
- per la copia di dischi RDM impostati in compatibilità virtuale, è consentito migrare il file di mapping oppure effettuare una conversione del disco RDM nel formato thick o thin durante la migrazione (se la destinazione non è NFS);
- per la copia di dischi RDM impostati in compatibilità fisica, è consentito migrare solo il file di mapping.

Capitolo 14
Gestione e controllo delle risorse

In questa sezione vedremo come monitorare l'occupazione di risorse tramite il vCenter Server, con l'obiettivo di massimizzare le prestazioni dell'ambiente vSphere. Vedremo inoltre come tenere traccia degli allarmi per evitare problemi sulla nostra infrastruttura.

14.1 Allocazione e distribuzione delle risorse

VMware vSphere impiega un meccanismo di distribuzione delle risorse basato sui concetti descritti di seguito.



- **Limit** - valore massimo di cicli CPU (in MHz) o quantitativo di memoria che non può essere superato da una VM o da un pool di risorse.
- **Reservation** - valore minimo di cicli CPU o quantitativo di memoria garantito e pre-allocato per una VM o per un pool di risorse.
- **Shares** - a livello concettuale, rappresenta lo spazio di risorse che il VMkernel mette in condivisione tra le VM. Ogni VM utilizza queste risorse condivise per raggiungere la quota "limit". Ovviamente possono verificarsi situazioni in cui più VM cercano di recuperare risorse dallo spazio condiviso, per arrivare ognuna al proprio "limit", con la possibilità che l'insieme delle risorse richieste sia superiore al valore totale di quelle disponibili sull'host (situazione di **overcommitment**). In questi casi il VMkernel gestirà tutte le situazioni di contesa delle risorse, con tecniche diverse che vedremo più avanti. Per impostazione predefinita, quando si crea una macchina virtuale, le sue risorse riservate sono impostate a zero, pertanto il 100% di risorse della VM vengono recuperate, quando necessario, dallo spazio di risorse condiviso. A livello di configurazione, nelle impostazioni di una VM o di un pool, vedremo come il valore di share rappresenti la **priorità di accesso alle risorse condivise**.

Quando si accende una macchina virtuale, il sistema controlla le quantità di risorse di CPU e memoria non ancora allocate. Sulla base delle risorse disponibili, il sistema determina se possono essere garantite le risorse riservate per la macchina virtuale. Questo processo è chiamato **admission control**. Se le risorse di CPU e memoria (non ancora riservate) sono sufficienti, la macchina virtuale può essere accesa. In caso contrario, comparirà un avviso di risorse insufficienti.

14.2 Concetti sulla memoria virtuale

Nell'architettura vSphere, ci sono 3 livelli di memoria.

1. Il VMkernel crea uno spazio di indirizzamento contiguo all'interno della memoria fisica dell'host ESXi, ripartito fra le varie VM in esecuzione.
2. La memoria RAM assegnata alle VM è resa disponibile dal VMkernel, a partire dallo spazio di indirizzamento descritto al punto 1. Il VMkernel consente di effettuare un'associazione 1:1 tra porzioni di memoria fisica e memoria utilizzata dalle VM, facendo in modo che le porzioni utilizzate da una VM non possano essere utilizzate da altre VM.
3. Ogni sistema operativo guest utilizza la memoria assegnata alla VM per metterla a disposizione delle applicazioni, come accade nelle installazioni fisiche.

La memoria fisica utilizzata da una VM rispetta la regola seguente:
VM's host memory usage = VM's guest memory size + VM's overhead memory

In pratica la memoria fisica utilizzata corrisponde alla memoria assegnata alla VM più un certo carico di memoria richiesto dall'host ESXi per le funzioni di virtualizzazione. Questo carico aggiuntivo è detto **overhead memory**. La memoria di overhead è legata al numero di CPU virtuali della VM e alla quantità di RAM assegnata alla VM.

14.2.1 RAM overcommitment e gestione delle contese di memoria

Si ha una situazione di RAM overcommitment (sovrautilizzo della RAM) quando la memoria RAM totale presente nell'host ESXi è inferiore a quella complessivamente allocata per tutte le macchine virtuali.

Una situazione di RAM overcommitment si verifica sia quando le risorse totali non sono sufficienti, sia quando una macchina virtuale richiede ulteriore RAM rispetto a quella già allocata. Sia chiaro però che per una VM non viene mai allocata più memoria di quella specificata per essa, ovvero se ad una VM abbiamo assegnato 1Gb di memoria RAM, questo sarà il limite massimo di memoria allocabile. Il VMkernel cerca di ottimizzare la distribuzione della memoria fisica, prendendo in prestito parte della RAM assegnata alle VM quando queste non sono sotto carico, e riassegnandola ad altre VM quando queste richiedono più risorse. Con questa tecnica è possibile, ad esempio, utilizzare un host con 2Gb di memoria fisica ed eseguire su di esso quattro VM con 1Gb di RAM ognuna.

Quando la memoria fisica è "overcommited", **per ogni macchina virtuale viene allocato un quantitativo di memoria fisica compreso tra il valore di Reservation e il valore di Limit**. La RAM allocata oltre il valore di Reservation è determinata dall'host ESXi in base alla priorità di **Shares** e in base ad una stima del recente carico di lavoro per quella VM.

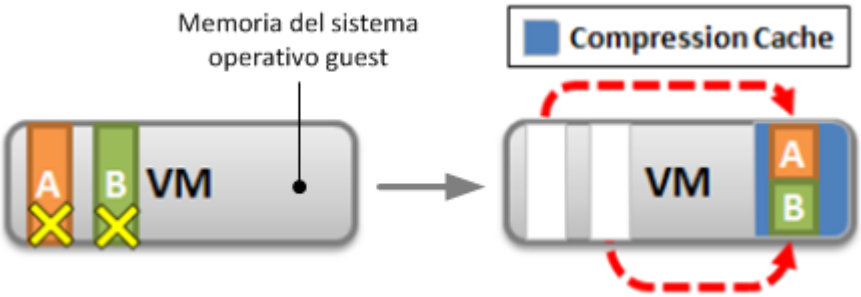
Per consentire i meccanismi di RAM overcommitment, il VMkernel utilizza un file di swap (**.vswp**), creato per ogni VM alla sua accensione ed eliminato allo spegnimento. Il file .vswp ha una dimensione pari alla quantità di memoria assegnata alla VM meno la memoria riservata. Per impostazione predefinita, quando si crea una macchina virtuale, la sua memoria riservata è impostata a zero, ossia il 100% di RAM della VM può essere sfruttata dal VMkernel per ridistribuire le risorse. Secondo queste specifiche, una VM configurata con 2Gb di RAM, in maniera predefinita avrà un file di swap di 2Gb. Se però si imposta per essa 1Gb di memoria riservata, allora il file di swap sarà di 1Gb. Se la memoria riservata fosse di 2Gb, il file di swap sarebbe pari a zero. Quando per una VM si specifica una certa quantità di memoria riservata, tale quantità sarà disponibile esclusivamente per quella VM e non per le altre. Una VM non userà il file di swap finché ci sarà RAM fisica a sua disposizione. Nel momento in cui tutta la RAM fisica dell'host ESXi è utilizzata, ha inizio il meccanismo di RAM overcommitment e le macchine virtuali inizieranno a utilizzare il file di swap. Poiché il file di swap si trova sullo storage, le operazioni su di esso saranno più lente rispetto alle operazioni effettuate in RAM. Se per una VM si specifica un certo valore di memoria riservata, ma l'host ESXi non ha abbastanza memoria fisica a disposizione, la VM non potrà essere accesa.

L'ottimizzazione della memoria può essere implementata con diverse tecniche.

- **Transparent Page Sharing** (**TTS**) – consente di evitare la replica di pagine di memoria identiche, allocandole una sola volta. Alle macchine virtuali che richiedono uno stesso contenuto informativo viene fornita la stessa ed unica pagina di memoria, con il risultato che più VM consumano meno memoria di quella che occorrerebbe nelle installazioni fisiche.
- **Memory ballon driver** – è un driver che consente il trasferimento di memoria dalle VM poco impegnate ad altre VM. È installato insieme ai VMware Tools ed è tecnicamente chiamato detto **vmmemctl**.

- **Memory compression** – tecnica impiegata nei periodi di contesa di memoria. Prevede la compressione delle pagine di memoria meno utilizzate, quelle che un sistema operativo guest posiziona nel file di swap su disco. Quelle pagine di memoria saranno compresse in RAM, pertanto la loro compressione e decompressione sarà più veloce rispetto alla lettura/scrittura su disco. La tecnica è trasparente rispetto ai sistemi operativi ospitati nelle macchine virtuali. Il risultato è un'occupazione di RAM fisica inferiore rispetto a quella necessaria in condizioni standard. ESXi tenta sempre di comprimere quelle pagine di memoria che possono essere ridotte a una dimensione di 2Kb. Di default, la cache di compressione ha una dimensione pari al 10% della memoria allocata alle VM, ma questi valori possono essere modificati tramite le impostazioni avanzate di ESXi. I parametri modificabili (nei menu **Configuration** > **Advanced Settings** su vSphere Client, **Manage** > **Settings** > **Advanced System Settings** su vSphere Web Client) sono i seguenti:

    - **Mem.MemZipEnable** = "1" abilita la memory compression; "0" disabilita la memory compression;
    - **Mem.MemZipMaxPct** = dimensione della cache di compressione, valore impostabile tra 5 e 100.



14.3 Virtual SMP

Il **Virtual Symmetric Multi-Processing** (**SMP**) consente a un'unica macchina virtuale l'utilizzo simultaneo di più processori (CPU virtuali o vCPU). Ogni VM può avere sino a 8 vCPU se l'ambiente vSphere ha una licenza di tipo standard, sino a 32 se la licenza è di tipo Enterprise, sino a 64 se la licenza è di tipo Enterprise Plus. Il VMkernel, tramite un meccanismo chiamato **CPU scheduler**, assegna dinamicamente le vCPU alla CPU fisica dell'host ESXi.

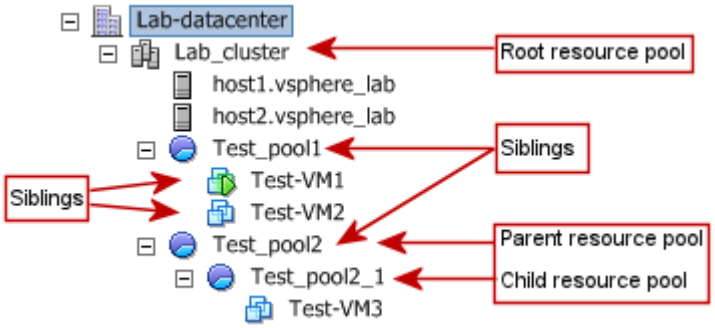
Prima di spiegare come il VMkernel effettua la mappatura tra le CPU virtuali associate alle VM e le CPU fisiche presenti nell'host ESXi, è necessario introdurre alcuni concetti sulle CPU multi-core. I processori oggi in commercio sono dotati di più **core** all'interno di uno stesso circuito integrato, chiamato **socket** (zoccolo). Ogni core deve essere visto come un singolo processore: ad esempio, possiamo considerare una CPU quad core come 4 CPU a singolo core. Ognuno di questi core è capace di eseguire un processo per volta. In questo caso ogni core prende il nome di **Logical Processor**. Se la CPU in uso supporta l'**hyperthreading**, ogni core sarà capace di eseguire due processi per volta; in questo caso ogni core corrisponde a due **Logical Processor**. L'hyperthreading deve essere abilitato nel BIOS dell'host ESXi; a livello di configurazione di ESXi, l'hyperthreading è abilitato di default.

Ogni vCPU assegnata alle VM è vista, lato host, come un processo indipendente dagli altri, ovvero un thread. Il compito del VMkernel è quello di mappare una vCPU ad un Logical Processor, nel momento in cui quest'ultimo risulta disponibile. Per ogni istante vi è quindi un'associazione vCPU-LogicalProcessor. Per la distribuzione del carico CPU, il VMkernel divide la CPU fisica in porzioni di tempo (da 2 a 40 millisecondi) da distribuire a tutte le VM, in modo che ogni VM esegua i suoi processi come se disponesse sempre delle vCPU che le sono state assegnate.

14.4 Pool di risorse

Un **Resource Pool** (pool di risorse) è un raggruppamento gerarchico di risorse di CPU e di memoria. Può contenere sia macchine virtuali sia ulteriori resource pool. Le risorse possono essere prelevate da un singolo host oppure da un Cluster dove sia abilitata la funzionalità vSphere Distributed Resource Scheduler. I resource pool danno diversi vantaggi, descritti di seguito.

- **Controllo accessi e delega delle autorizzazioni**.
- **Separazione di risorse**.
- **Gestione di insiemi di macchine virtuali che eseguono servizi multilivello**.
- **Organizzazione gerarchica e flessibile delle risorse** - gerarchicamente, esiste un **root resource pool** corrispondente alla somma dei megahertz di tutte le CPU e alla somma dei megabyte di RAM disponibili su un host ESXi o su un cluster. Ad eccezione del root pool, gli altri resource pool hanno un riferimento superiore, ossia un **parent resource pool**. Un pool figlio, o **child pool**, viene utilizzato per allocare risorse dal pool padre. Resource pool e macchine virtuali sullo stesso livello sono detti **siblings** (fratelli). Un resource pool può contenere macchine virtuali, ulteriori child resource pools, o entrambe le entità.



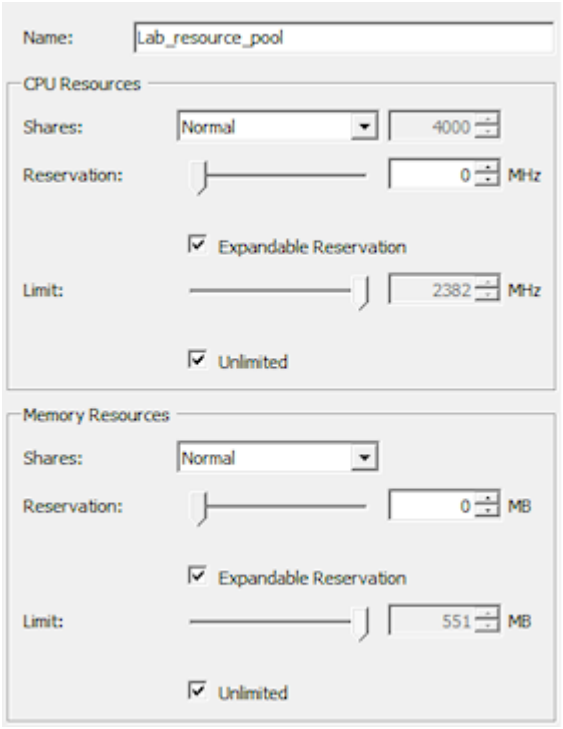
- **Isolamento tra pool diversi o condivisione di risorse tra pool** - gli amministratori di livello superiore possono assegnare e rendere disponibile un pool di risorse ad amministratori di livello inferiore.

14.4.1 Creazione di un resource pool

Un pool di risorse può essere creato all'interno di un singolo host ESXi, di un cluster DRS, o nidificato all'interno di un altro pool. Con vSphere Client, è sufficiente fare clic con il tasto destro su uno di questi oggetti e selezionare la voce **New Resource Pool**. Con vSphere Web Client, selezionare le voci **All vCenter Actions** > **New Resource Pool**.

Così come per le macchine virtuali, anche per i pool esistono gli attributi di reservation, limit e shares; hanno però effetto sull'intero pool e non sulle singole macchine virtuali.

- **Limit** - valore massimo di cicli CPU (in MHz) o quantitativo di memoria che non può essere superato dal pool.
- **Reservation** - valore minimo di cicli CPU o quantitativo di memoria garantito e pre-allocato per il pool. Non può superare il valore di reservation del pool superiore.
- **Shares** - priorità sull'accesso del pool alle risorse condivise. Ad esempio, se un pool ha un valore doppio di shares CPU rispetto ad un altro pool, rispetto a questo sarà autorizzato ad utilizzare il doppio delle risorse.
- **Expandable reservation** - quando non sono disponibili le risorse indicate dal parametro reservation, questo parametro consente al resource pool di cercare risorse inutilizzate nei livelli superiori, permettendo di soddisfare le richieste.



È necessario prestare particolare attenzione quando si abilita il parametro "expandable reservation": un resource pool di livello inferiore potrebbe utilizzare tutte le risorse messe a disposizione dai pool di livello superiore, con potenziali problemi per gli altri pool nello stesso livello.

14.4.2 Inserimento di una VM in un resource pool

Una VM può essere inserita all'interno di un pool di risorse sin dalla sua fase di creazione: la procedura guidata permette infatti di specificare un pool di risorse di destinazione. Se la VM è già esistente, le procedure possibili sono queste:

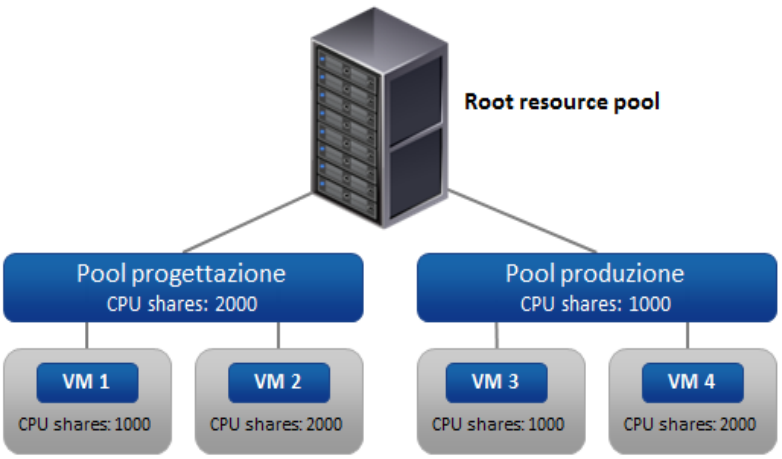
- tramite **vSphere Client**, selezionare la VM dall'inventario e trascinarla all'interno del pool di risorse desiderato;
- tramite **vSphere Web Client**, selezionare la VM dall'inventario, fare clic con il tasto destro su di essa, selezionare la voce **Move to** e specificare il pool di destinazione.

Lo spostamento di una VM all'interno di un pool di risorse segue queste regole:

- i parametri di **Reservation** e **Limit** impostati per la VM non vengono modificati;
- se il parametro **Shares** è impostato sui valori predefiniti **High**, **Medium**, **Low**, la percentuale di share della VM sarà adattata al numero totale di share in uso nel resource pool;
- se il parametro **Shares** è impostato su un valore personalizzato, il valore rimarrà invariato all'interno del resource pool.

14.4.3 Esempi di utilizzo dei resource pool

Per quanto riguarda il concetto di share, vediamo un esempio pratico con due pool di pari livello.



- Il pool di progettazione ha un valore di **CPU Shares** doppio rispetto al pool di produzione, pertanto rispetto a quest'ultimo sarà autorizzato ad utilizzare il doppio delle risorse CPU.
- In una situazione di contesa delle risorse, il pool di progettazione potrà impegnare il 66% di risorse del root pool, mentre il pool di produzione potrà utilizzarne il 33%.
- Lo stesso discorso si estende alle VM di ogni pool: la VM 2 potrà impegnare il 66% di risorse del pool di progettazione, mentre la VM 1 potrà utilizzarne il 33%. La VM 4 potrà impegnare il 66% di risorse del pool di produzione, mentre la VM 1 potrà utilizzarne il 33%.

14.5 Monitorare l'uso delle risorse

Per garantire l'efficienza e l'affidabilità di un sistema, sia in ambiente virtuale, sia negli ambienti tradizionali, è necessario monitorare le prestazioni di tutte le parti che compongono l'infrastruttura: server fisici, macchine virtuali, storage, rete. In linea generale, le prestazioni indicano il grado di rapidità con cui si completano le attività di sistema e delle applicazioni, rapidità che potrebbe essere frenata da un lento accesso allo storage, da un'insufficiente potenza di calcolo, da un'insufficiente quantità di memoria disponibile per le VM, oppure dalla velocità effettiva delle interfacce di rete. Il monitoraggio permette di ottimizzare o mantenere efficiente un sistema.

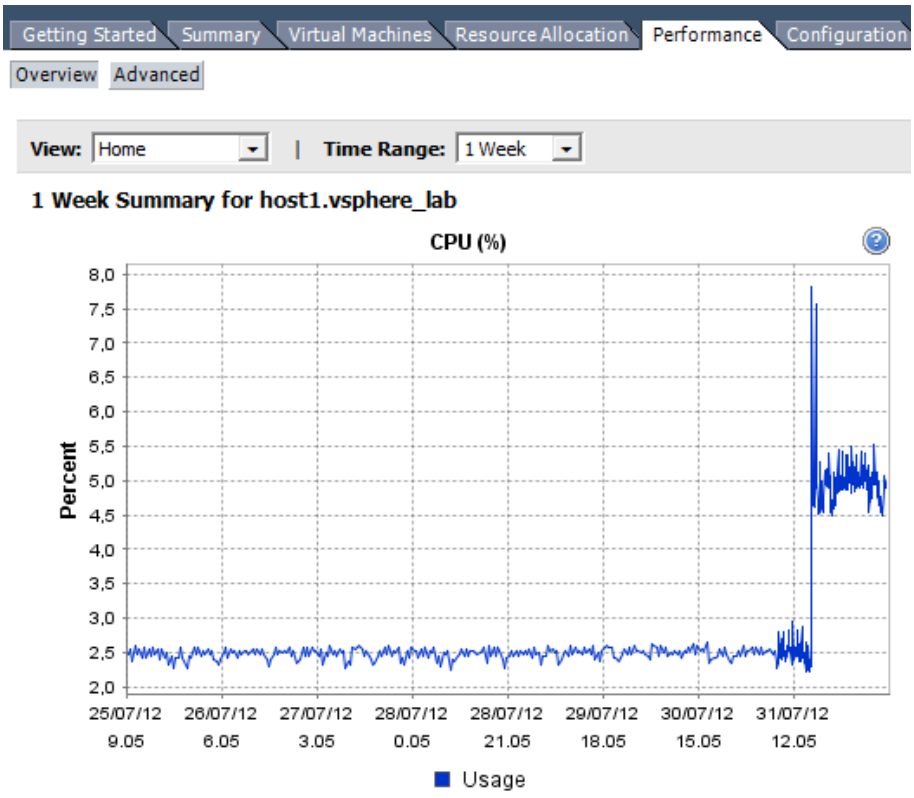
14.5.1 Monitorare i sistemi guest

Per il monitoraggio delle prestazioni nei sistemi operativi guest, oltre agli strumenti di analisi forniti dagli stessi sistemi (su Windows, ad esempio, si utilizza **Task Manager** per il controllo di CPU e memoria), esistono strumenti di terze parti e funzionalità integrate nei **VMware Tools**. Per quanto riguarda gli strumenti di terze parti, segnaliamo **Iometer**, utile strumento per l'analisi delle richieste I/O sui dischi, disponibile sotto forma di immagine ISO avviabile, da montare su una VM. Per quanto riguarda i VMware Tools, essi includono una libreria di funzioni chiamata **Perfmon DLL**, che consente l'accesso alle statistiche generate da CPU e memoria all'interno delle VM. Sui sistemi Windows, la libreria Perfmon DLL può essere sfruttata dallo strumento di analisi delle prestazioni **Performance Monitor**. È possibile utilizzare Performance Monitor di Windows per esaminare l'effetto sulle prestazioni di una VM prodotto dai programmi in esecuzione, sia in tempo reale e sia raccogliendo i dati di registro per un'analisi successiva.

14.5.2 Analisi delle performance tramite il vCenter Server

Il vCenter Server mette a disposizione diversi strumenti di verifica delle performance. Con **vSphere Client**, i dati di performance sono localizzabili sull'omonimo tab ai vari livelli di

datacenter, host e macchine virtuali. Con **vSphere Web Client**, fare clic su **Monitor > Performance** sui diversi oggetti datacenter, host, macchine virtuali, ecc.



Le informazioni sono mostrate con dei grafici. Sono inoltre presenti due viste: **Overview** e **Advanced**. Con la prima vengono mostrati i valori relativi a CPU, dischi, memoria e rete. Con la seconda sono disponibili più contatori, le viste sono personalizzabili ed è possibile sia esportare sia stampare i dati.

14.5.3 Analisi delle prestazioni tramite riga di comando

A livello di host ESXi, è disponibile uno strumento a riga di comando per verificare in tempo reale l'utilizzo delle risorse. Lo strumento, chiamato **esxtop**, è l'equivalente VMware del noto comando **TOP** dei sistemi Unix, con il vantaggio di poter gestire parametri legati all'infrastruttura virtuale. Può essere avviato in tre modalità differenti:

- interattiva - i dati sono stampati a schermo in tempo reale;
- batch capture - è possibile registrare l'output verso un file, che può essere esportato ed analizzato successivamente anche con strumenti di terze parti;
- replay - vengono visualizzati i parametri campionati durante una sessione di vm-support.

La sintassi di utilizzo di **esxtop** è la seguente:

esxtop [-] [h] [v] [b] [s] [a] [c filename] [R vm-support_dir_path] [d delay] [n iter]

14.5.4 Verifica della CPU

Per verificare se una VM è limitata da poche risorse CPU, è necessario prima di tutto un controllo all'interno del sistema operativo guest, con strumenti che consentano la verifica delle prestazioni della CPU. Si procede poi al controllo dal punto di vista dell'host ESXi: se l'utilizzo della CPU rimane

elevato per lunghi periodi di tempo, significa che la VM è limitata da insufficienti risorse CPU assegnate.

In particolare, si consiglia la verifica del valore **CPU ready** (**%RDY**), ossia l'intervallo in cui una VM rimane in attesa di eseguire le istruzioni CPU. I valori ottimali sono sotto la soglia del 5%. L'attesa si verifica quando, all'interno dello stesso host, più VM sono in coda per l'accesso alle risorse CPU.

14.5.5 Verifica della memoria

I problemi di poca memoria disponibile devono essere verificati sia a livello di VM che di host. Nel primo caso, è necessario verificare che la VM non abbia un'**attività di ballooning** troppo frequente, situazione che si verifica quando il memory ballon driver richiede ulteriore memoria per la VM. Nel secondo caso, è necessario verificare i valori di **swap-in** e **swap-out** nei grafici di performance dell'host ESXi; questi valori sono ripetutamente alti se più VM sono limitate dalla memoria, e presentano tutte un'elevata attività di **ballooning** e di **paging**. Ricordiamo che il paging è il processo mediante il quale blocchi di codice vengono spostati dalla memoria RAM all'hard disk, su un file detto di paging o di swap. Il paging eccessivo, sia in ambiente virtuale che fisico, è sempre il primo indicatore di un quantitativo insufficiente di RAM.

I valori da verificare con particolare attenzione sono indicati di seguito.

- **Memctl** – mostra le attività del memory ballon driver. I valori sono alti quando il VMkernel ha bisogno di recuperare memoria già allocata. Il memory balloon driver, presente nelle VM con i VMware Tools installati, permette al VMkernel di trasferire memoria dalle VM poco impegnate ad altre VM che necessitano di ulteriore memoria, nelle situazioni di RAM overcommitment.
- **Swap** – mostra i valori dell'attività di paging.
- **Zip** – valori relativi all'attività di compressione della memoria da parte del VMkernel.

14.5.6 Latenza dei dischi

La latenza dei dischi è il primo dato da verificare quando si hanno problemi di prestazioni sullo storage. A livello host, è possibile monitorare il **throughput** (capacità di trasmissione) e la **latenza** (intervallo tra un input ed un output) per datastore e storage adapter. A livello di VM, è possibile monitorare throughput e latenza per specifici dischi virtuali. Il throughput si verificato tramite i valori di **Read rate** e **Write rate**, mentre la latenza con i valori di **Read latency** e **Write Latency.**

In particolare, è opportuno monitorare i valori indicati di seguito.

- **Kernel command latency** - tempo medio (espresso in millisecondi) che il VMkernel impiega per processare ogni comando SCSI. Dovrebbe essere compreso tra 0 e 1 millisecondo.
- **Phisical device command latency** - tempo medio (espresso in millisecondi) che lo storage fisico impiega per processare ogni comando SCSI. Se superiore a 15, significa che lo storage è stato sottodimensionato.

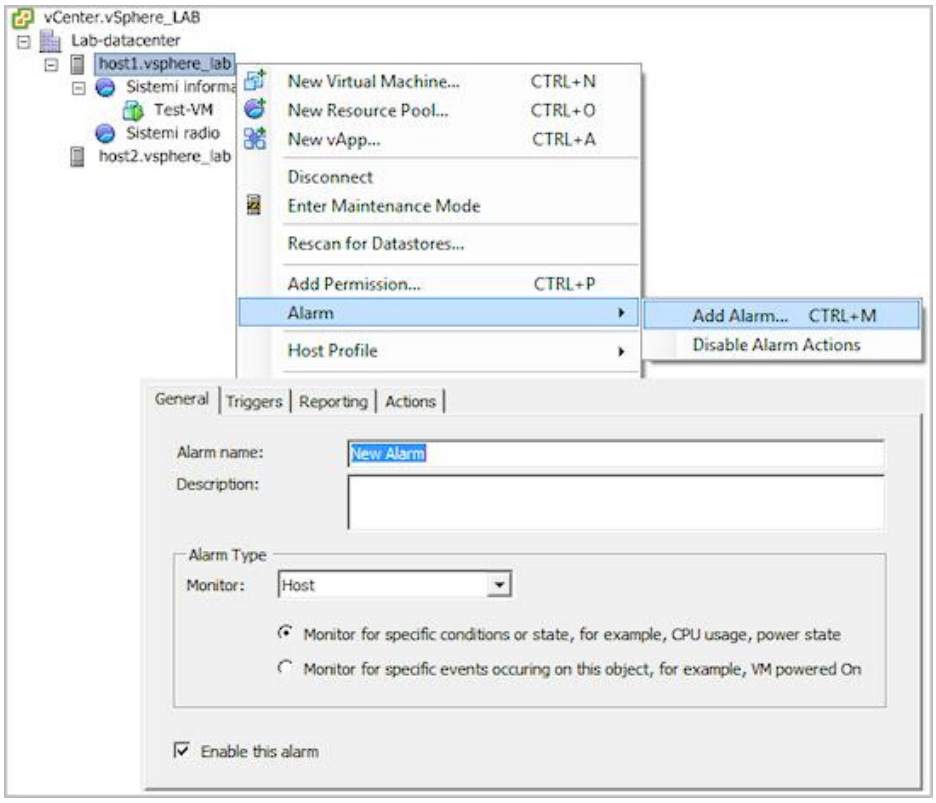
14.5.7 Lentezza della rete

I problemi sulle prestazioni della rete sono normalmente causati da saturazione della banda. La perdita di pacchetti di rete indica la presenza di colli di bottiglia, pertanto i principali contatori da monitorare per la verifica delle attività di rete sono quelli di **droppedTX** e **droppedRX**, relativamente alle VM.

14.6 Gestione degli allarmi

Quando si parla di allarmi, si deve distinguere tra l'evento che ha generato l'allarme e l'azione che si intraprende in risposta a quell'allarme. Nello specifico, un allarme è una notifica che arriva in risposta ad un evento o condizione precisa. Esistono degli allarmi predefiniti, ma se ne possono creare di nuovi e personalizzati per un grande insieme di oggetti presenti nell'inventario del nostro sistema virtuale.

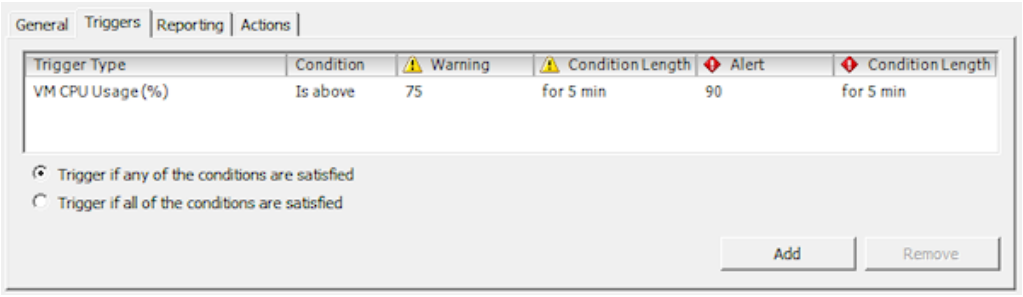
Per creare un allarme, fare clic con il tasto destro su un oggetto presente nell'inventario, quindi selezionare le voci **Alarm > Add alarm** (con vSphere Web Client le voci sono **Alarms > New alarm definition**).



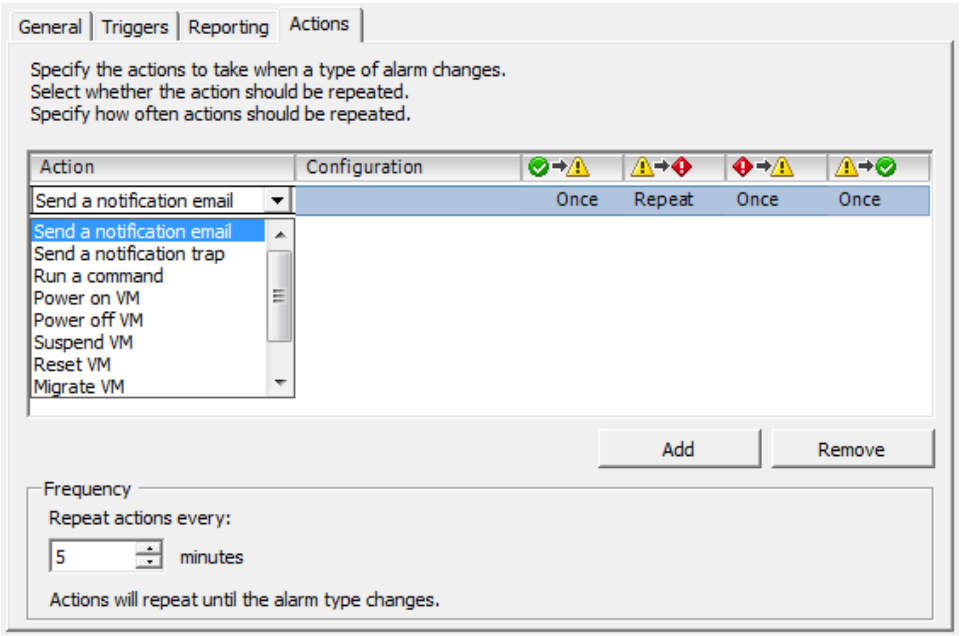
Nella procedura guidata, è possibile scegliere che tipo di allarmi impostare.

- **Monitor for specific conditions or state** - allarme basato su una condizione specifica in cui possono trovarsi CPU, VM, datastore, ecc.
- **Monitor for specific events occuring on this objec**t - allarme basato su un evento, ad esempio perdita di connettività, rimozione di un account, accensione di una VM, ecc.

Un allarme richiede un **trigger**, ossia una procedura automatica eseguita in coincidenza di un determinato evento. Nell'esempio sottostante è stato impostato un trigger che genera un avviso (**warning**) se la CPU supera il 75% di utilizzo per oltre 5 minuti di tempo e un allarme (**alert**) se la CPU supera il 75% di utilizzo per oltre 5 minuti di tempo.



Le azioni da intraprendere in risposta a un allarme sono configurabili su **Actions**. Le azioni possono essere ripetute una o più volte per ogni cambiamento di stato dell'allarme, da normale a warning, da warning ad alert, da alert a warning, da warning a normale.



Nel caso in cui si voglia inviare una notifica via mail, sarà necessario procedere con la configurazione dei parametri **Sender** e **SMTP** sulle impostazioni del vCenter Server, dove è possibile impostare anche i parametri relativi al protocollo SNMP.

Capitolo 15
Cluster DRS e bilanciamento tra host

Un **cluster** è un insieme di host ESXi e relative macchine virtuali, dove le risorse sono condivise e l'interfaccia di gestione è comune; un **cluster DRS** è semplicemente un cluster con il servizio **vSphere Distributed Resource Scheduler** (DRS) abilitato. Un cluster DRS permette di distribuire e bilanciare le risorse fisiche (CPU e memoria a sua disposizione) tra le varie VM.

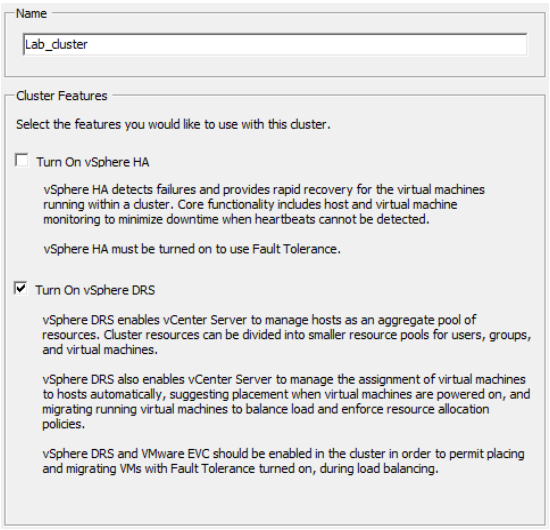
Quando si inserisce un host ESXi all'interno di un cluster DRS, le risorse dell'host diventano risorse del cluster. All'interno di un cluster DRS è possibile la gestione delle risorse nei termini descritti di seguito.

- **Initial placement** - nel momento in cui si accende una VM all'interno del cluster, il servizio DRS posiziona la VM in maniera ottimale all'interno di un host, applicando le impostazioni raccomandate.
- **Load balancing** - il servizio DRS monitora in modo continuo la distribuzione delle risorse di memoria e di CPU fra gli host e le macchine virtuali. I dati di carico vengono continuamente confrontati con un uso ideale delle risorse definito dal valore di **Migration Threshold**.
- **Power management** - tramite l'abilitazione di VMware Distributed Power Management (VMware DPM), funzionalità opzionale di VMware DRS, è possibile avere dei risparmi a livello di consumi energetici consolidando i carichi nei periodi di minor impegno delle risorse. In pratica vengono migrate le VM su un numero di host che garantiscono sufficienti risorse, permettendo di mettere in standby gli altri host che fornirebbero risorse in eccedenza.

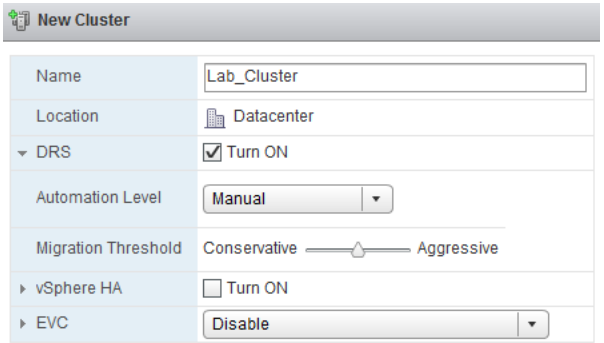
15.1 Creazione e gestione di un cluster DRS

Per creare un cluster DRS, fare clic con il tasto destro su un datacenter e selezionare la voce **New Cluster**. Nella schermata di creazione guidata del cluster, assegnare un nome e abilitare la voce **Turn on vSphere DRS**.

Finestra di creazione di un cluster con **vSphere Client**

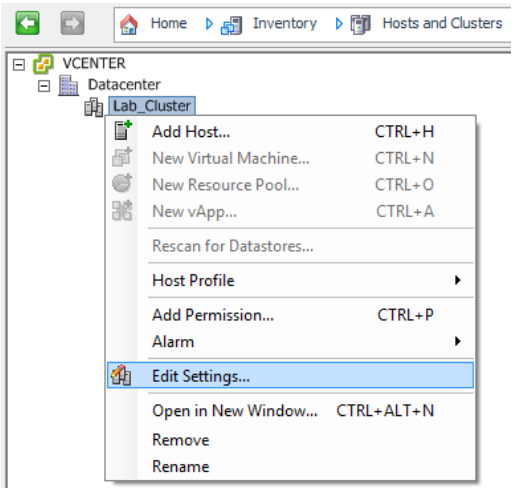


Finestra di creazione di un cluster con vSphere **Web Client**

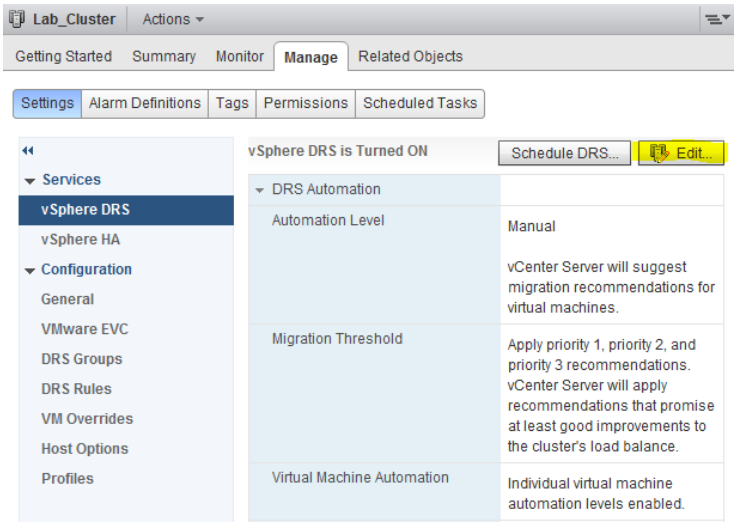


Alcuni parametri del cluster possono essere impostati durante la sua creazione. In ogni caso è possibile accedere a tutti i parametri successivamente.

- Con **vSphere Client**, fare clic con il tasto destro sul cluster e selezionare la voce **Edit Settings**.



- Con **vSphere Web Client**, selezionare il cluster, entrare nel relativo tab **Manage** e fare clic su **Settings**; per ogni servizio o impostazione in elenco, è presente il pulsante **Edit.**



15.1.1 Livelli di automazione

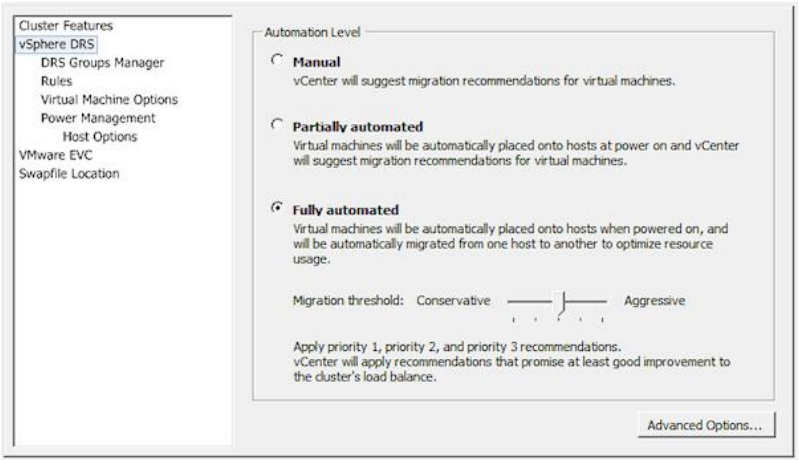
Durante la creazione di un cluster, oppure entrando nelle sue impostazioni successivamente, è possibile stabilire il livello di automazione di vSphere DRS, determinando se lo spostamento delle VM fra i vari host deve essere solamente suggerito oppure eseguito automaticamente dal sistema. Nel dettaglio, i livelli impostabili sono descritti di seguito.

- **Manual** - se il cluster diventa sbilanciato, il sistema mostra delle indicazioni per la migrazione delle macchine virtuali. Inoltre, all'accensione di una VM, viene mostrata una lista degli host nei quali posizionare la VM.
- **Partially automated** - l'automatismo è parziale, ovvero le VM, alla loro accensione, vengono posizionate nell'host meno utilizzato; tuttavia, se il cluster diventa sbilanciato successivamente, vengono solamente mostrate delle indicazioni per la migrazione delle macchine virtuali.

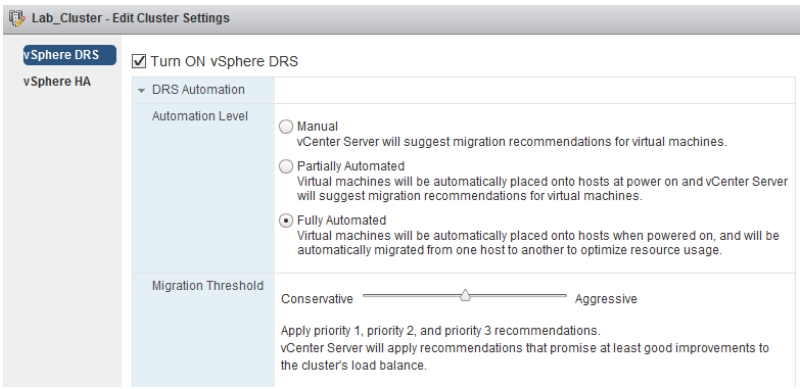
- **Fully automated** - l'automatismo è totale, pertanto le VM sono poste nell'host meno utilizzato fin dalla loro accensione e, se il cluster diventa sbilanciato, il sistema DRS interviene per spostare le VM su host più scarichi. Si deve utilizzare quest'opzione se si desidera che il vCenter Server sposti automaticamente le VM da un host impostato in maintenance mode.

È inoltre possibile impostare la velocità di migrazione delle macchine virtuali, tramite l'opzione **Migration threshold**. Si va da un livello 1 di tipo conservativo ad un livello 5 di tipo aggressivo: nel primo caso vengono applicate le priorità di livello 1, ossia le procedure da adottare per soddisfare i vincoli del cluster quali "affinity rules" e "host maintenance", nel secondo caso vengono adottate tutte le raccomandazioni che consentono anche solo un lieve miglioramento al bilanciamento del cluster.

- Impostazione del livello di automazione con **vSphere Client**



- Impostazione del livello di automazione con **vSphere Web Client**



15.1.2 Posizione del file di swap

L'impostazione **Swapfile Location** consente di specificare dove salvare i file di swap delle macchine virtuali. In maniera predefinita, questi file sono nella stessa cartella di ogni VM, ma si può scegliere di memorizzarli in un diverso datastore. La scelta consigliata è quella di lasciarli nella stessa cartella delle VM.

15.1.3 Gruppi DRS e regole

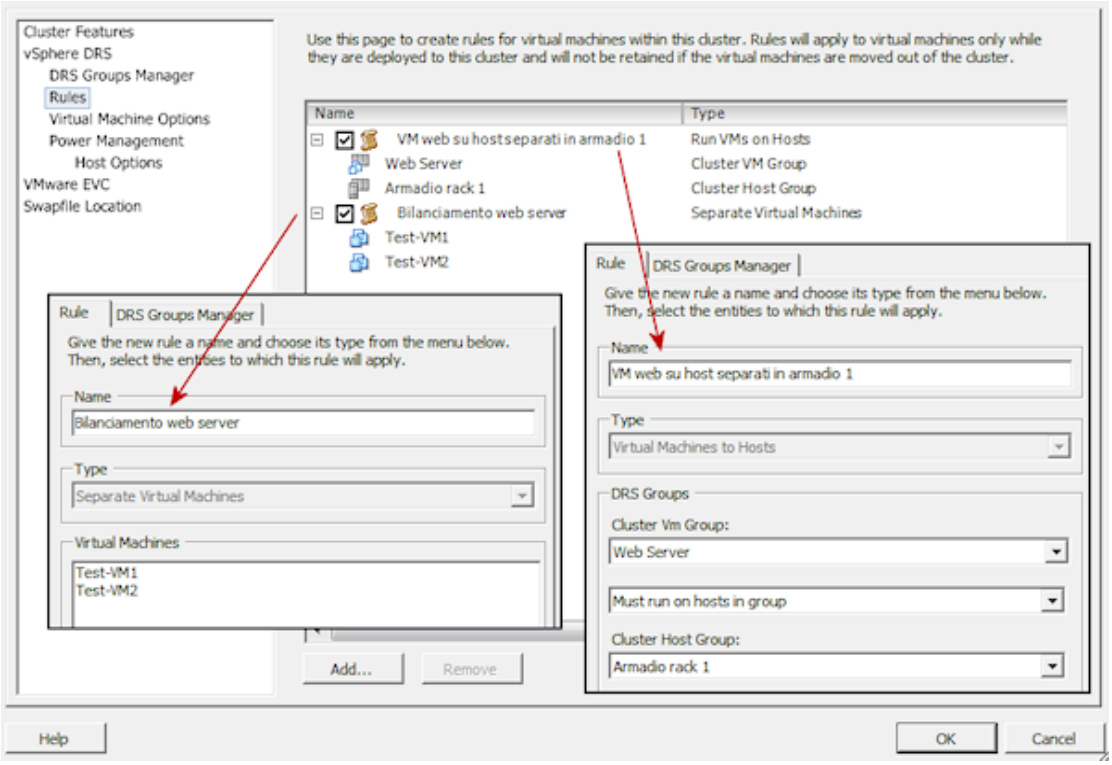
All'interno di un cluster DRS è possibile imporre al sistema l'osservazione di determinati criteri per quanto riguarda il posizionamento delle VM fra i vari host. Tali criteri sono rappresentati dalle **Affinity rules** (regole di affinità o più semplicemente regole DRS).

- **Keep virtual machines together** - regola di affinità (**Affinity rule**) con cui il DRS cerca di mantenere determinate macchine virtuali all'interno di uno stesso host;
- **Separate virtual machines** - regola di non affinità (**Anti-affinity rules**) con cui il DRS cerca di mantenere determinate macchine virtuali su host differenti, per ragioni di disponibilità.
- **Virtual machine to hosts** – regola che specifica condizioni e modalità di esecuzione di un gruppo DRS all'interno di uno specifico insieme di host. Diversamente dalle regole precedenti, riguardanti l'affinità tra VM, questa regola definisce l'affinità di un gruppo di VM rispetto a un gruppo di host.

All'interno di un cluster possono essere creati uno o più gruppi DRS. I gruppi costituiti da macchine virtuali sono chiamati **DRS Groups,** i gruppi costituiti da host sono chiamati **Host DRS groups**. Lo scopo di questi gruppi è di rendere più semplice la definizione delle regole di affinità di tipo "Virtual machine to host". È importante evidenziare che una VM può appartenere a più gruppi DRS.

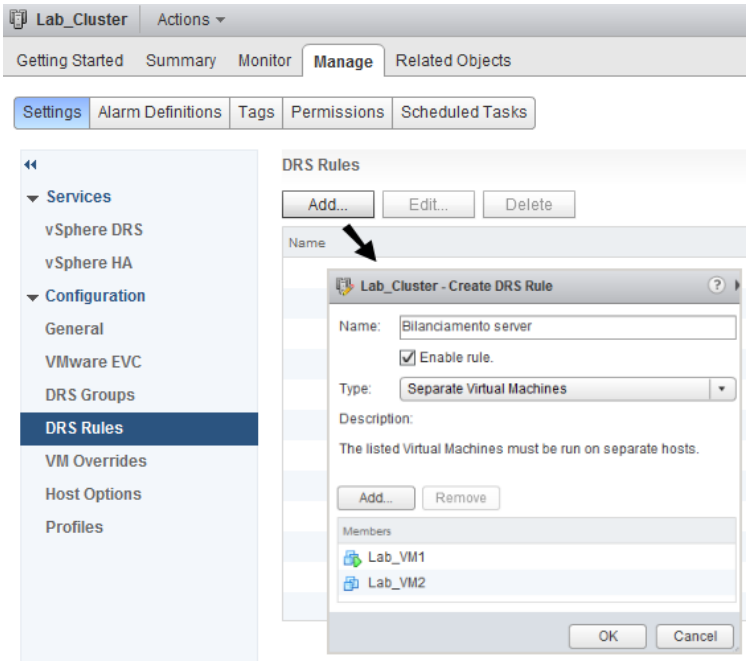
Creazione di una regola DRS con vSphere Client

- Entrare nelle impostazioni del cluster e fare clic su **Rules**.



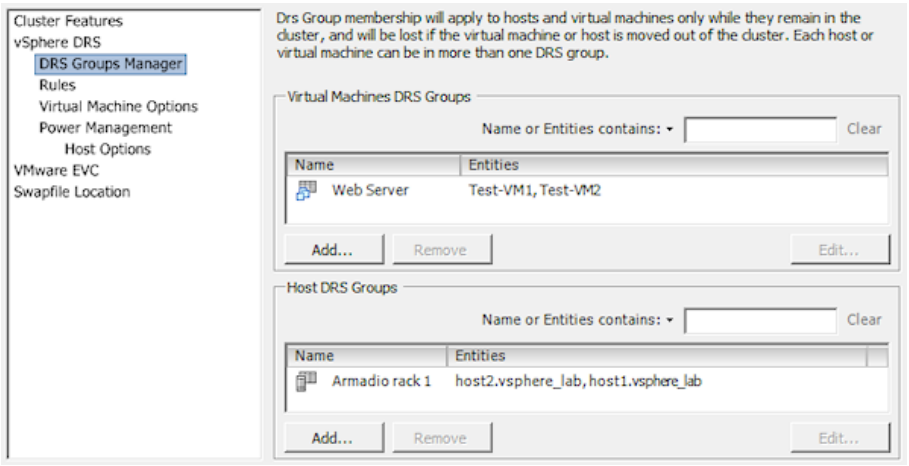
Creazione di una regola DRS con vSphere Web Client

- Selezionare il cluster, entrare nel relativo tab **Manage** e fare clic su **Settings**
- Selezionare la voce **DRS Rules** e fare clic su **Add**.



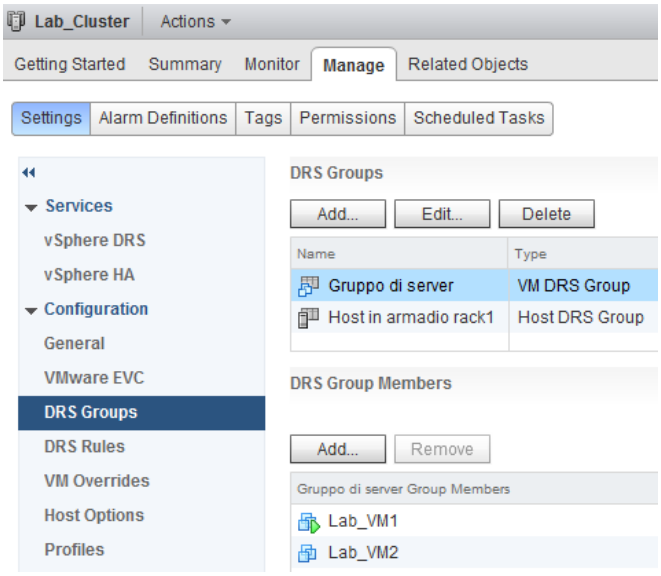
Creazione di un gruppo DRS con vSphere Client

- Entrare nelle impostazioni del cluster e fare clic su **DRS Groups Manager**.



Creazione di un gruppo DRS con vSphere Web Client

- Selezionare il cluster ed entrare nel relativo tab **Manage.**
- Fare clic su **Settings** e selezionare la voce **DRS Groups**.

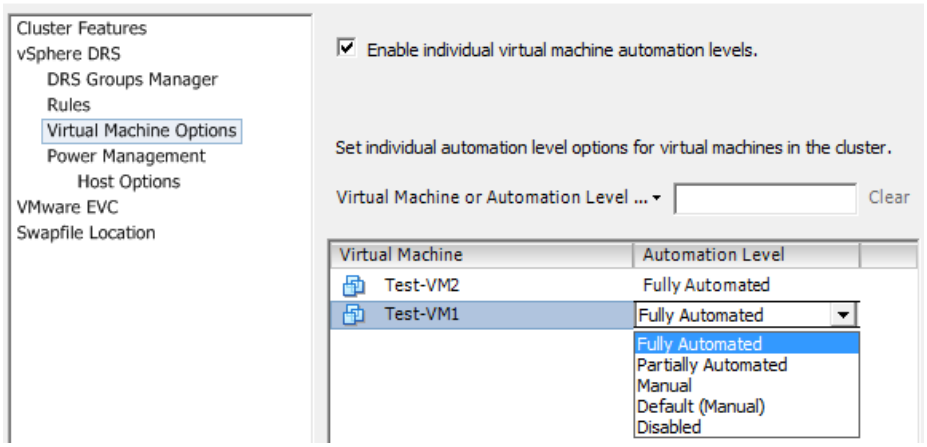


15.1.4 Livelli di automazione specifici per VM

All'interno di un cluster è possibile impostare, per ogni VM, livelli di automazione specifici che avranno precedenza rispetto ai livelli assegnati al cluster.

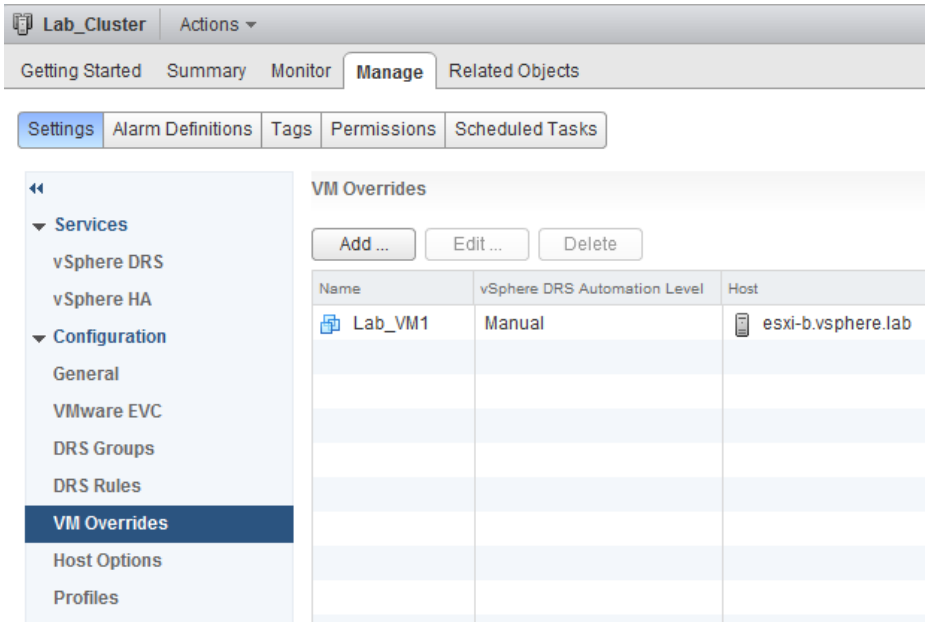
Livelli di automazione in vSphere Client

- Si trovano sotto la voce **Virtual Machine Options**.



Livelli di automazione in vSphere Web Client

- I livelli di automazione specifici per le VM si trovano sotto la voce **VM Overrides**.



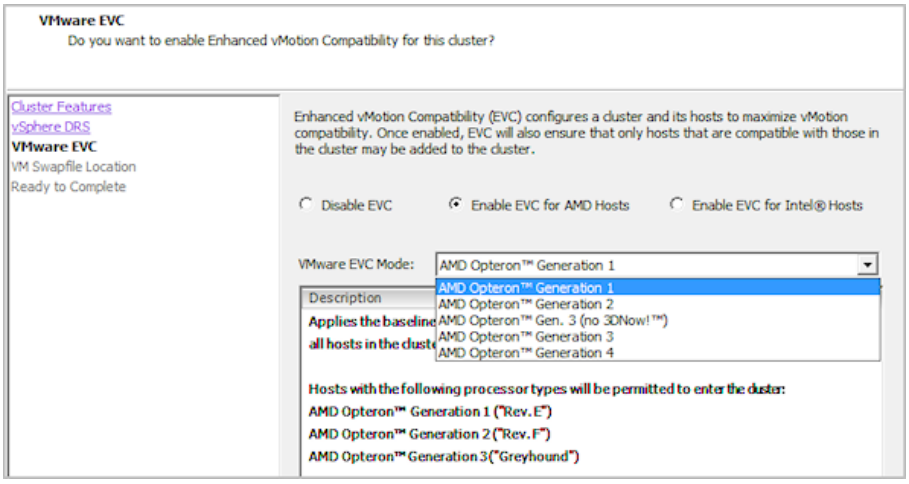
15.1.5 EVC e la compatibilità fra le CPU degli host

VMware Enhanced vMotion Compatibility (**EVC**) è un'importante funzionalità che permette di migliorare la compatibilità del vMotion fra gli host all'interno di un cluster, facendo sì che le CPU fisiche, anche nel caso in cui differissero tra loro, offrano alle VM lo stesso set di istruzioni. Utilizzando EVC si evitano errori di vMotion causati da possibili incompatibilità fra CPU. EVC è una funzionalità attivabile in un cluster, e non richiede che i servizi DRS e HA siano abilitati. Grazie all'EVC è più semplice aggiungere nuove CPU nel cluster, perché queste saranno configurate in modalità compatibile con quelle esistenti. Tuttavia la compatibilità è prevista solo fra CPU dello stesso produttore (AMD o Intel). Esistono diversi livelli di compatibilità, tecnicamente chiamati **baseline**; si parte dal più basso (**lowest baseline**), che permette la massima flessibilità e compatibilità grazie alla disattivazione di alcune funzioni CPU, sino al livello massimo (**highest baseline**), che espone le funzioni CPU più avanzate.

Con EVC abilitato, gli host devono supportare le funzionalità di **virtualizzazione a livello hardware** offerte da AMD-V o Intel VT. Tali funzionalità devono essere attive a livello di BIOS. Non è possibile aggiungere a un cluster DRS quegli host non allineabili al set di istruzioni CPU impostato con EVC.

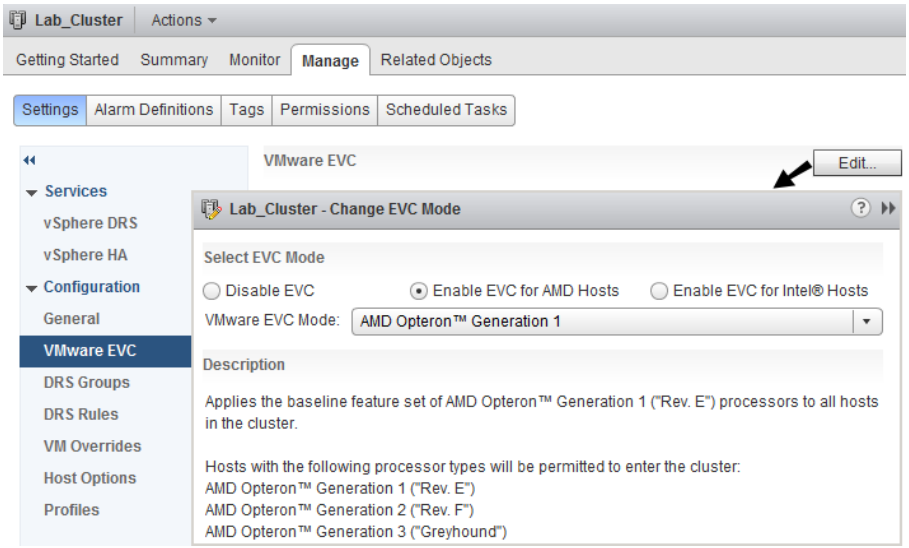
Configurazione di EVC con vSphere Client

- Entrare nelle impostazioni del cluster e fare clic su **VMware EVC**.



Configurazione di EVC con vSphere Web Client

- Selezionare il cluster e fare clic sul tab **Manage**.
- Fare clic su **Settings** e selezionare la voce **VMware EVC**.



15.2 Inserimento di un host nel cluster

Per inserire un host all'interno di un cluster con **vSphere Client**, è sufficiente trascinare l'host stesso all'interno dell'oggetto cluster. Con **vSphere Web Client**, fare clic con il tasto destro sull'host, selezionare la voce **Move to** e specificare il cluster di destinazione.

Per sfruttare il bilanciamento del carico offerto da VMware DRS, gli host devono soddisfare alcuni requisiti:

- devono far parte della stessa rete vMotion (vedere il capitolo dedicato al vMotion);
- devono aver accesso ad uno storage condiviso;
- le VM del cluster DRS devono avere i dischi virtuali memorizzati su un datastore accessibile sia dall'host sorgente che dall'host di destinazione.

15.3 Rimozione di un host dal cluster

Per rimuovere un host da un cluster, è necessario prima metterlo in "Maintenance Mode": per tale operazione, è sufficiente fare clic con il tasto destro sull'host e selezionare la voce **Enter Maintenance Mode**. A questo punto si può posizionare l'host fuori dal cluster.

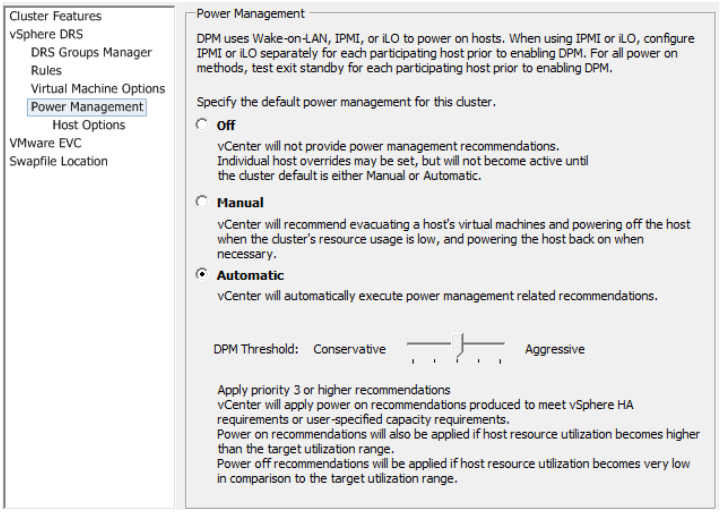
Per impostare un host in "Maintenance Mode", è necessario spegnere le macchine virtuali in esecuzione sull'host stesso, oppure migrarle tramite vMotion. Rimuovendo un host dal cluster, l'host perde la configurazione relativa ai resource pool, mantenendo tuttavia le impostazioni del root resource pool. Inoltre, rimuovendo l'host dal cluster, le risorse totali disponibili per il cluster diminuiscono: a quel punto, se le risorse riservate alle VM non sono tutte disponibili, una o più VM potrebbero non avere le risorse necessarie per il power-on.

15.4 Gestione dell'energia con VMware DPM

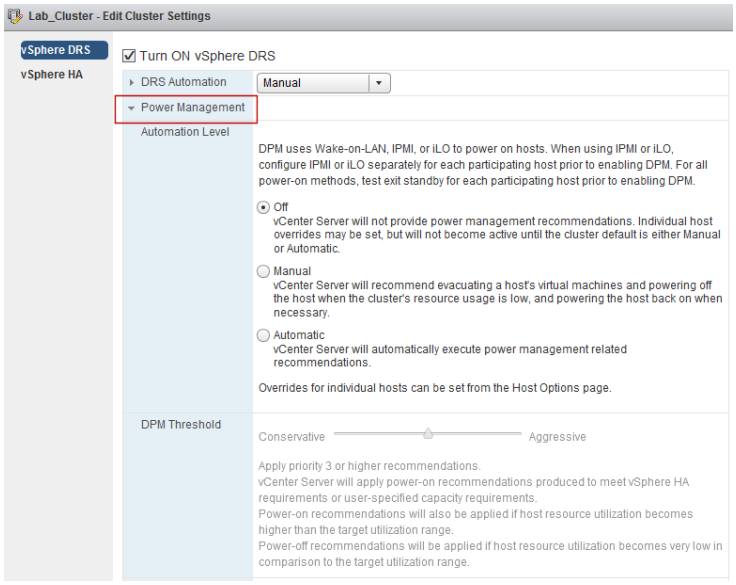
VMware DPM (Distributed Power Management) automatizza l'efficienza energetica nei cluster DRS, grazie alla costante ottimizzazione dei consumi. VMware DPM sfrutta VMware DRS per migrare automaticamente le macchine virtuali dagli host ESXi che possono essere spenti. Proprio perché sfrutta VMware DRS, VMware DPM può essere abilitato solo all'interno di un cluster DRS. Il risparmio di energia si ottiene dimensionando le capacità del cluster in base alle esigenze dei carichi di lavoro. Il servizio prevede lo spegnimento di host ESXi quando le risorse di CPU e memoria nel cluster sono utilizzate marginalmente; ovviamente vi è uno spostamento automatico delle relative VM su altri host. Nel momento in cui la richiesta di risorse cresce sino a rendere necessaria la presenza di più host, DPM provvede alla riaccensione degli host spenti, in base alle necessità. È importante indicare che la funzione DPM non prevede lo spegnimento di host che hanno in carico macchine virtuali con VMware Fault Tolerance attivo, semplicemente perché VMware DRS non è progettato per la migrazione di macchine con VMware FT abilitato.

15.4.1 Abilitare VMware DPM

VMware DPM è disabilitato per impostazione predefinita. Per abilitarlo con vSphere Client, selezionare la scheda **Power Management** all'interno delle opzioni del cluster, quindi selezionare una delle due voci **Manual** o **Automatic**.



Con vSphere Web Client, selezionare il cluster, entrare nel relativo tab **Manage**, fare clic su **Settings** e selezionare **vSphere DRS**. Nelle impostazioni di vSphere DRS è presente la sezione **Power Management**, dove è possibile abilitare VMware DPM.



Impostando la modalità manuale, è prevista l'esecuzione delle operazioni raccomandate a seguito di conferma da parte dell'utente. In modalità automatica, l'esecuzione delle operazioni raccomandate non prevede alcuna conferma. Infine, è possibile impostare la soglia DPM utilizzando la barra di scorrimento **DPM Threshold**. Esistono cinque livelli: dal più conservativo, con priorità 1, al più aggressivo, con priorità 5.

Per la gestione degli host, VMware DPM può utilizzare uno dei seguenti protocolli:

1. Intelligent Platform Management Interface (**IPMI**);
2. Hewlett-Packard Integrated Lights-Out (**iLO**);
3. Wake-On-LAN (**WOL**).

Ognuno di questi protocolli richiede il supporto a livello hardware da parte di un host, oltre ad una configurazione specifica.

Capitolo 16
Storage DRS e bilanciamento tra datastore

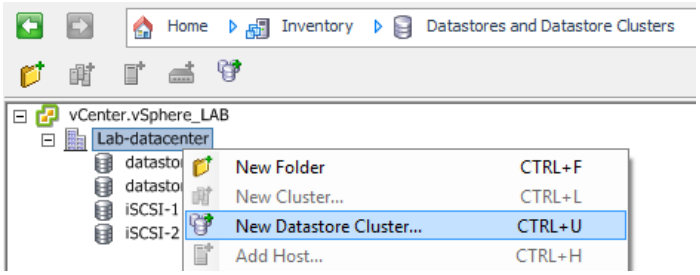
16.1 Cluster di datastore

Un **Datastore Cluster** è un insieme di datastore in cui le risorse storage sono condivise e l'interfaccia di gestione è in comune. Aggiungendo un datastore all'interno di un Datastore Cluster già esistente, le sue risorse diventeranno parte delle risorse globali del Datastore Cluster. Il servizio **vSphere Storage DRS**, che vedremo più avanti, viene erogato all'interno di un Datastore Cluster.

16.1.1 Creazione di un Datastore Cluster

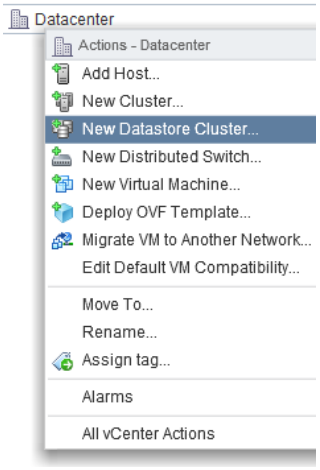
Procedura con vSphere Client

- Andare nella vista **Datastores and Datastore Clusters**.
- Fare clic con il tasto destro sul datacenter desiderato.
- Infine selezionare la voce **New Datastore Cluster**.
- Completare i passaggi richiesti tramite la procedura di creazione guidata.



Procedura con vSphere Web Client

- Nel pannello di navigazione a sinistra individuare e selezionare il datacenter desiderato.
- Fare clic con il tasto destro su di esso e selezionare la voce **New Datastore Cluster**.
- Completare la procedura di creazione guidata seguendo le indicazioni proposte.
- Al termine, fare clic su **Finish**.



Requisiti per la creazione di un Datastore Cluster

Un Datastore Cluster può contenere datastore con dimensioni e capacità I/O differenti, anche provenienti da array diversi, ma non permette le seguenti combinazioni:

- datastore NFS con datastore VMFS;
- datastore replicati (replicated datastores) insieme a datastore non replicati (non-replicated datastores);
- datastore condivisi tra differenti datacenter.

Si può aggiungere al cluster qualsiasi datastore già collegato ad un host, con le seguenti eccezioni:

- gli host collegati ai datastore devono avere VMware ESXi versione 5.0 o successive;
- un datastore non può trovarsi in più di un datacenter;
- quando si rimuove un datastore da un cluster, il datastore non viene scollegato dall'host e rimane presente nell'inventario;
- se un datastore collegato a un host ESX/ESXi versione 4.x (o precedenti) viene inserito in un Datastore Cluster, il servizio Storage DRS non potrà essere eseguito.

16.2 Storage DRS

Abilitando il servizio Storage DRS all'interno di un Datastore Cluster, si garantiscono le funzionalità descritte di seguito.

- **Initial placement** (posizionamento iniziale) - nel momento in cui si crea o si clona una VM, il servizio Storage DRS seleziona un datastore in cui posizionare i dischi della VM; lo stesso meccanismo si verifica quando si migra una VM su un altro Datastore Cluster, o quando si aggiunge un nuovo disco ad una VM. Il posizionamento è realizzato in conformità dei vincoli di spazio e in linea con gli obiettivi di bilanciamento I/O. Il sistema tende a ridurre al minimo il rischio di intense attività di I/O e di sovra-utilizzo di un datastore, che inciderebbero negativamente sulle prestazioni delle VM.
- **Ongoing balancing** (bilanciamento continuo) - il servizio Storage DRS monitora la distribuzione delle risorse storage, sia ad intervalli predefiniti di otto ore, sia quando uno o più datastore eccedono i limiti di spazio preconfigurati. Per quanto riguarda il calcolo dello spazio occupato, vengono considerate anche le macchine spente e le eventuali snapshot presenti. Storage DRS verifica anche il valore di latenza I/O, che non deve superare il 90% del valore massimo rilevato nel corso di un giorno.

16.2.1 Attivazione dello Storage DRS

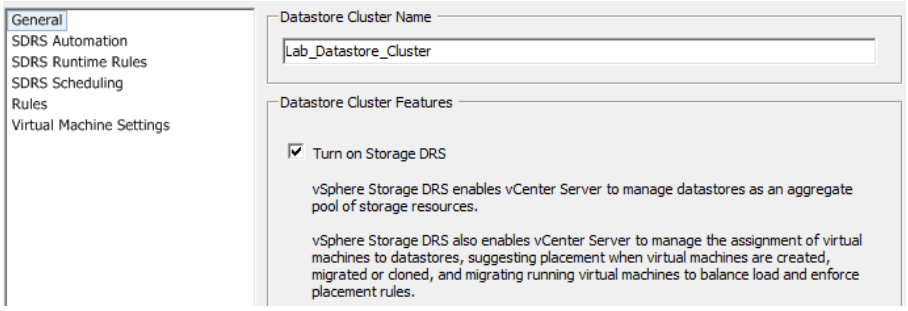
Storage DRS, anche se abilitato per un intero Datastore Cluster, non sarà attivo per i dischi delle VM configurate in uno dei modi seguenti:

- con servizio Fault Tolerance attivo;
- con file di swap posizionato nel datastore locale di un host ESXi;
- con uno o più dischi in modalità independent (sia persistent, sia non-persistent).

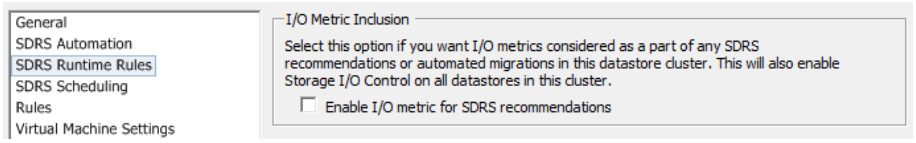
È possibile inserire insieme datastore VMFS3 e VMFS5, ma la raccomandazione è quella di utilizzare sempre datastore con le stesse caratteristiche.

Procedura con vSphere Client

- Fare clic con il tasto destro sul Datastore Cluster desiderato e selezionare la voce **Edit Settings**.
- Fare clic su **General.**
- Selezionare la voce **Turn on Storage DRS** e confermare facendo clic su **OK**.

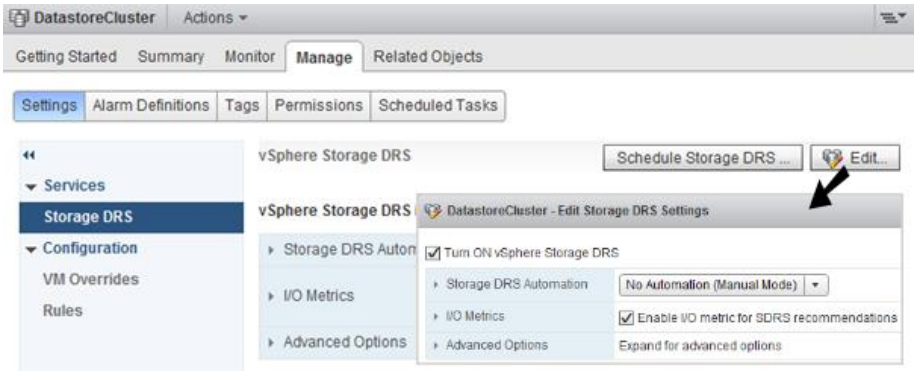


- Opzionalmente, è possibile disabilitare il controllo dei valori I/O, lasciando abilitati solo i controlli relativi allo spazio disco: per far questo, è sufficiente disabilitare la voce **Enable I/O metric for SDRS recommendations** nella finestra **SDRS Runtime Rules**.



Procedura con vSphere Web Client

- Selezionare il Datastore Cluster desiderato.
- Selezionare il tab **Manage** e fare clic su **Settings**.
- Su **Storage DRS**, fare clic su **Edit** e abilitare l'opzione **Turn ON vSphere Storage DRS**.



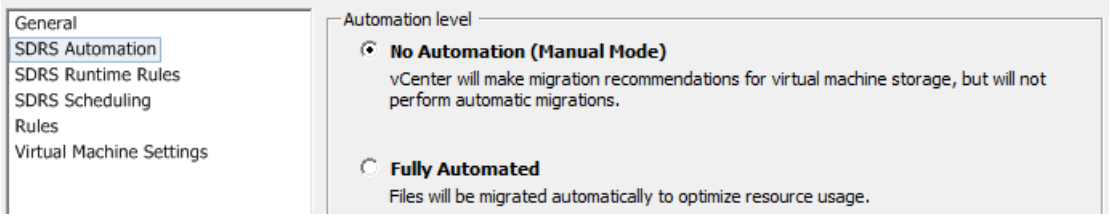
16.2.2 Livello di automazione dello Storage DRS

Il livello di automazione di un Datastore Cluster specifica se le azioni consigliate dallo Storage DRS debbano essere applicate automaticamente o manualmente. Le azioni consigliate sono tecnicamente chiamate **Recommendations** (raccomandazioni). L'automazione si configura nelle impostazioni del Datastore Cluster: sotto la voce **SDRS Automation** se si utilizza vSphere Client, su **Storage DRS Automation** se si utilizza vSphere Web Client. I valori possibili sono indicati di seguito.

- **No Automation** (**Manual Mode**) - le raccomandazioni di posizionamento e migrazione sono visualizzate nel tab **Storage DRS** (pagina **Recommendations**) del Datastore Cluster, ma devono essere applicate manualmente da un amministratore. Il sistema elenca tutte le raccomandazioni necessarie a bilanciare le risorse di spazio e di I/O del Datastore Cluster. Ogni indicazione include il nome della VM, il nome del disco virtuale, il nome del Datastore Cluster, i datastore di origine e destinazione, e una spiegazione delle raccomandazioni proposte. Alcune indicazioni costituiscono un obbligo, nelle situazioni di:
  - esaurimento dello spazio disco per un datastore;

- violazione di una regola di affinità;
- inserimento di un datastore in maintenance mode.

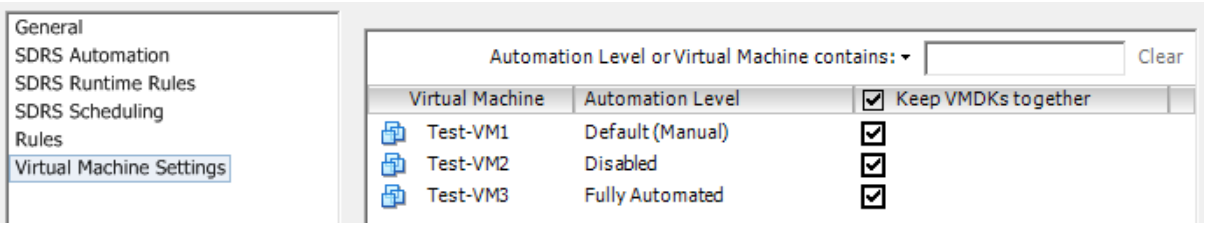
Nel momento in cui si applicano le raccomandazioni dello Storage DRS, il vCenter Server utilizza lo Storage vMotion per migrare i dischi delle VM su altri datastore all'interno del Datastore Cluster.



- **Fully Automated** - le raccomandazioni di posizionamento e migrazione sono applicate automaticamente.

16.2.3 Impostazioni specifiche dello Storage DRS per singole VM

È possibile impostare uno specifico livello di automazione, compresa la disattivazione dello Storage DRS, per ogni singola VM; in questo caso, l'impostazione assegnata a livello di VM prevale su quella assegnata al Datastore Cluster.

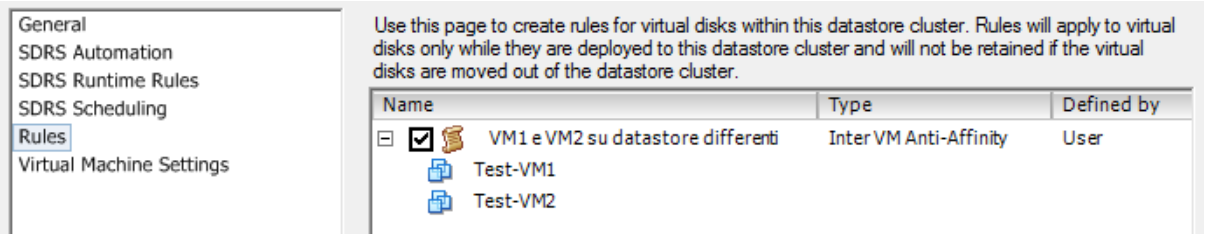


16.2.4 Regole di anti-affinità

In maniera predefinita i dischi virtuali di una macchina sono posizionati insieme nello stesso datastore, all'interno di un Datastore Cluster. Tuttavia è possibile impostare regole di anti-affinità, per posizionare dischi o VM in differenti datastore. Esistono due tipi di regole.

- **Inter-VM Anti-Affinity Rules** – con queste regole si specifica quali VM non devono mai stare nello stesso datastore.
- **Intra-VM Anti-Affinity Rules** - con queste regole si specifica quali dischi, associati a determinate VM, non devono mai stare nello stesso datastore.

Le regole si impostano sotto la voce **Rules**, nelle impostazioni del Datastore Cluster.



16.2.5 Impostare un datastore in Maintenance Mode

È possibile impostare un datastore in modalità Maintenance, con la possibilità di metterlo fuori servizio ed effettuare attività di manutenzione. Questa modalità è possibile solo se il datastore fa

parte di un Datastore Cluster con Storage DRS attivo; i datastore "stand-alone" infatti non possono essere impostati in Maintenance mode.

I dischi virtuali presenti nel datastore da impostare in Maintenance Mode devono essere migrati su un altro datastore. È possibile spostarli manualmente, tramite Storage vMotion, oppure automaticamente, sfruttando Storage DRS.

Per impostare un datastore in modalità Maintenance, fare clic con il tasto destro sul datastore stesso e selezionare la voce **Enter SDRS Maintenance Mode** (se si utilizza vSphere Web Client, selezionare **All vCenter Actions > Enter Storage DRS Maintenance Mode**). Apparirà quindi una lista di raccomandazioni, riguardanti le migrazioni necessarie; selezionare le raccomandazioni desiderate e fare clic su **Apply**. A questo punto il vCenter Server utilizzerà lo Storage vMotion per spostare i dischi dal datastore di origine a quello di destinazione; fatto ciò, il datastore di origine passerà in modalità Maintenance.

Capitolo 17
High Availability e Fault Tolerance

17.1 Alta disponibilità con vSphere HA

Il servizio vSphere HA, ovvero vSphere High Availability, attivabile all'interno di un cluster, può intervenire in caso di blocco di host, di sistemi operativi guest, di applicazioni in esecuzione sulle VM. In caso di blocco di un host, viene eseguito un riavvio automatico delle macchine virtuali su un altro host. In caso di blocco di un sistema guest, viene riavviata la relativa VM; in caso di blocco di un'applicazione, sfruttando software di terze parti (con un "agent" in ascolto), viene riavviata la relativa VM. Ovviamente non è detto che il riavvio di una VM risolva un problema sul sistema guest; sarà cura dell'amministratore configurare HA al meglio ed in base alle proprie esigenze.

Per il funzionamento di vSphere HA è necessario rispettare alcuni limiti.

- È necessario che il cluster non superi **32 host**.
- All'interno del cluster non si possono avere più di **4000 VM**.
- Ogni host non può avere più di **512 VM** (indipendentemente dal numero di host/cluster).

vSphere HA è integrato con vSphere DRS: infatti se un host subisce un blocco e le VM vengono spostate su un altro host, DRS può intervenire per bilanciare i carichi.

vSphere HA richiede il vCenter Server solo per la configurazione iniziale. In seguito il servizio funzionerà sugli host in maniera indipendente dal vCenter. Quest'aspetto è importante nel caso in cui si volesse proteggere un'istanza virtuale di vCenter Server con vSphere HA: se l'host che ospita il vCenter dovesse subire un improvviso blocco operativo (con la conseguenza di avere il vCenter non in linea), vSphere HA sposterebbe il vCenter su un altro host.

17.2 Architettura di vSphere HA

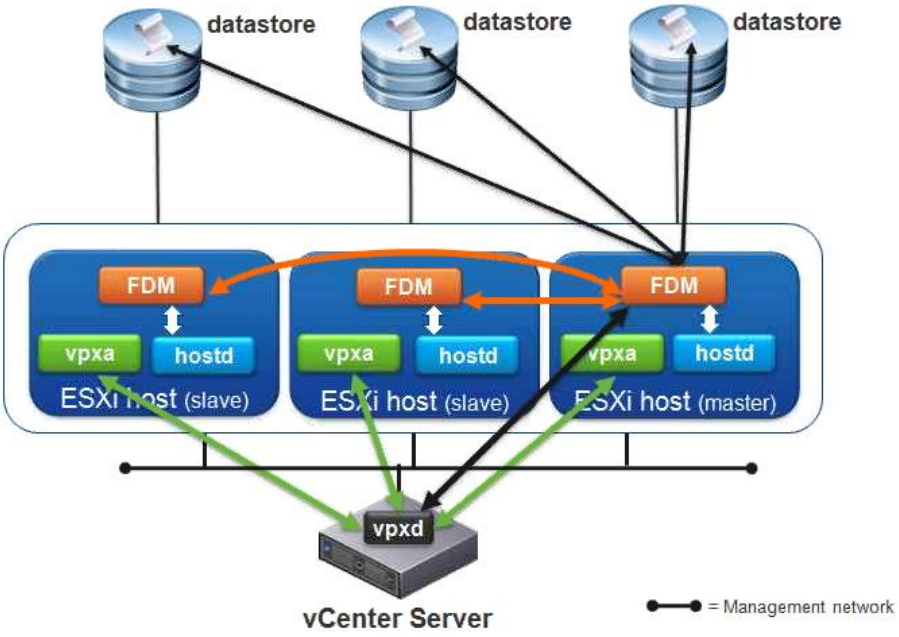
Il servizio HA si abilita all'interno di un cluster (vedere più avanti la sezione "Attivazione e configurazione di vSphere HA"). Appena il servizio HA viene abilitato, su ogni host entra in funzione il servizio **Fault Domain Manager** (**FDM**): grazie a questo servizio, ogni host ha "coscienza" di esser parte di un "fault domain". Affinché un host possa far parte di un fault domain, è necessario che siano rispettate 3 condizioni:

- l'host non deve essere disconnesso dal vCenter Server;
- l'host non deve trovarsi in maintainance mode;
- l'host non deve trovarsi in stand-by mode.

Il fault domain è gestito da un host "**master**"; tutti gli altri host sono definiti "**host slave**". L'elezione del master host avviene tramite un processo che premia **l'host che accede al numero più alto di datastore**. Se più host hanno lo stesso numero di datastore, la scelta si basa sul **MOID** (**Managed Object ID**), ossia un identificativo assegnato dal vCenter Server. L'elezione dura circa quindici secondi e occorre ogni volta che:

- si abilita il servizio HA;

- il master host presenta problemi dopo essere stato impostato in maintainance mode, standby mode o dopo la riconfigurazione di HA;
- gli host di tipo slave non comunicano più con il master per problemi di rete.



Durante il periodo di elezione la comunicazione avviene utilizzando il protocollo UDP (porta 8182). Terminata l'elezione, le comunicazioni tra master e slave viaggiano su protocollo TCP (porta 8182). Ogni slave mantiene una singola connessione TCP con il master.

17.2.1 Verifica del disservizio

Il master host invia periodicamente degli heartbeat sulle reti di management (tutte quelle configurate), per informare gli host slave della sua presenza. Gli host slave utilizzano una sola rete di management per le comunicazioni con l'host master; nel caso in cui la rete utilizzata non fosse più disponibile, proverebbero a comunicare su un'interfaccia di management alternativa (per la configurazione di una rete di management ridondata, far riferimento al paragrafo successivo).

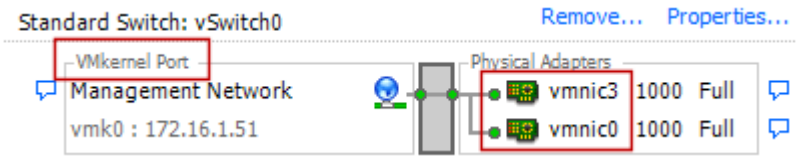
Per capire se un host non è più funzionante, ad esempio per un crash improvviso, o più semplicemente è isolato a livello di rete, vSphere HA utilizza i datastore, che fungono quindi da canale di comunicazione alternativo per la rilevazione degli heartbeat. Quando un host slave non risponde sulle reti di management, vSphere HA effettua una verifica degli heartbeat tramite datastore, per capire se l'host è comunque funzionante, nonostante sia isolato a livello di rete. Il datastore utilizzato per la verifica del disservizio tramite heartbeat è **quello con il più alto numero di host ESXi connessi** ad esso.

Una volta che il master host considera l'host slave non raggiungibile, lo etichetta come "**agent unreachable**". Se l'host non è più funzionante è previsto l'avvio automatico delle VM su altri nodi ESXi. Nel caso in cui l'host fosse isolato a livello di rete, sarebbe necessario l'intervento di un amministratore, oppure si dovrebbe impostare un trigger per il riavvio automatico delle VM su altri host.

17.3 Ridondanza per la rete di management

La rete di management è utilizzata da vSphere HA per l'invio delle comunicazioni di heartbeat fra tutti gli host del cluster. VMware raccomanda di adottare una rete ridondata per il management, per non avere punti deboli (single point of failure) nel networking.

Su ogni host del cluster, si dovrebbero avere due interfacce di rete in teaming, come mostrato nell'immagine sotto. Per il bilanciamento del carico fra le due NIC si consiglia di adottare la modalità predefinita "Route based on the originating Port ID", già descritta nel paragrafo "Bilanciamento del carico di rete e tecniche di failover", nella sezione del virtual networking.

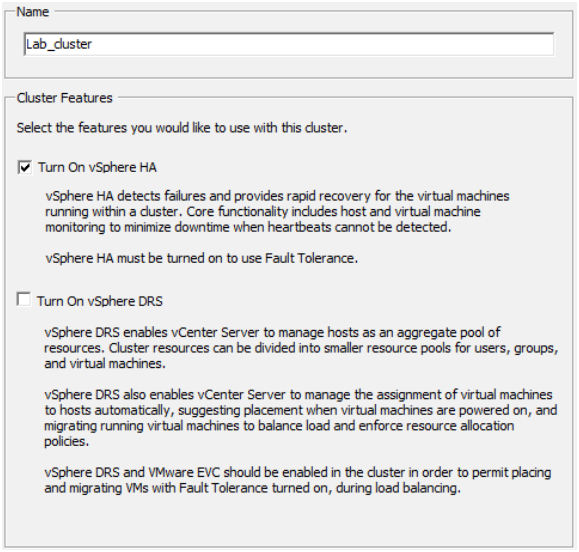


17.4 Attivazione e configurazione di vSphere HA

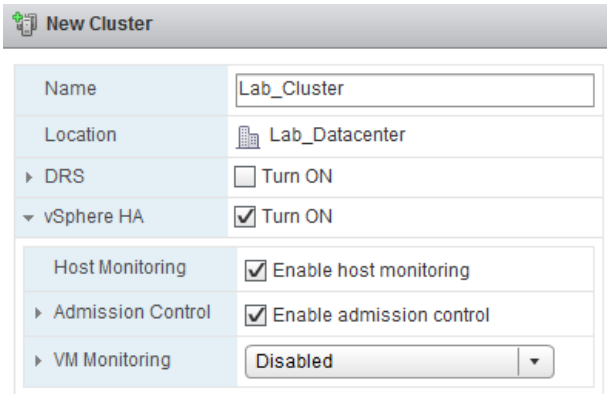
Nel paragrafo precedente abbiamo detto che il servizio HA si abilita all'interno di un cluster. Come già visto per vSphere DRS, un cluster è un insieme di host ESXi e delle relative macchine virtuali, dove le risorse sono condivise.

Per creare un cluster, fare clic con il tasto destro del mouse su un datacenter e selezionare la voce **New Cluster**. Nella schermata di creazione guidata del cluster, assegnare un nome e abilitare la voce "**Turn on vSphere HA**".

Finestra di creazione di un cluster con **vSphere Client**

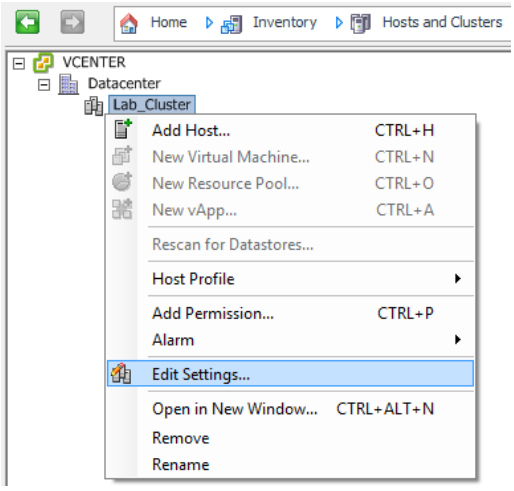


Finestra di creazione di un cluster con vSphere **Web Client**

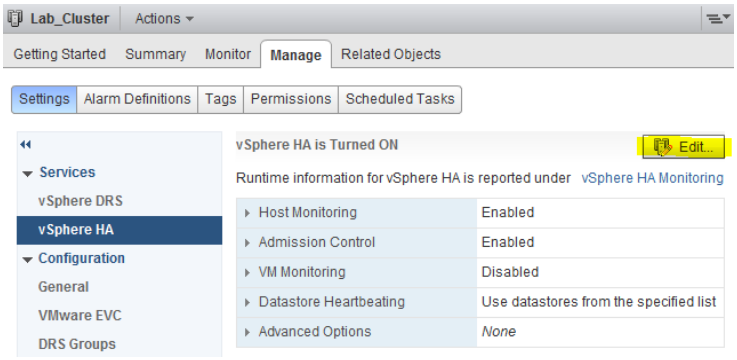


Alcuni parametri del cluster possono essere impostati durante la sua creazione. In ogni caso è possibile accedere a tutti i parametri successivamente, in questo modo:

- con **vSphere Client**, fare clic con il tasto destro sul cluster e selezionare la voce **Edit Settings**;



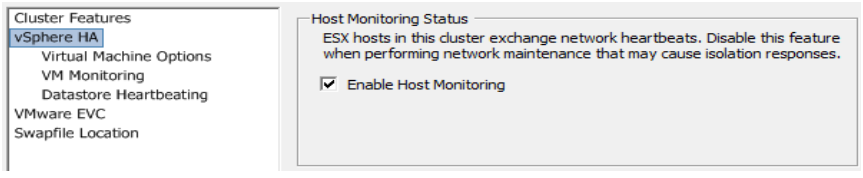
- con **vSphere Web Client**, selezionare il cluster, entrare nel relativo tab **Manage** e fare clic su **Settings**; per ogni servizio o impostazione in elenco, è presente il pulsante **Edit.**



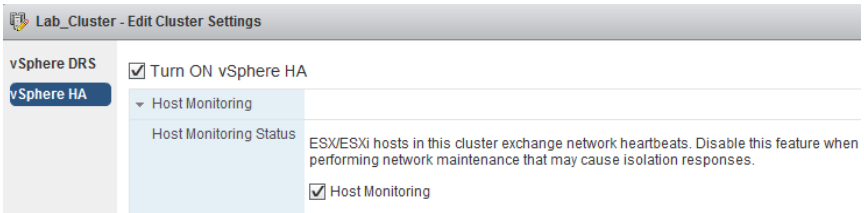
17.4.1 Host monitoring status

Nelle impostazioni del cluster, la pagina vSphere HA presenta come prima opzione la voce "**Enable Host Monitoring**". Disabilitando quest'opzione, il sistema non intraprende alcuna azione al verificarsi di un qualsiasi errore sugli host; è utile in quelle situazioni in cui devono essere portate a termine attività di modifica sulla rete che porterebbero ad un isolamento degli host.

Impostazione tramite vSphere Client



Impostazione tramite vSphere Web Client

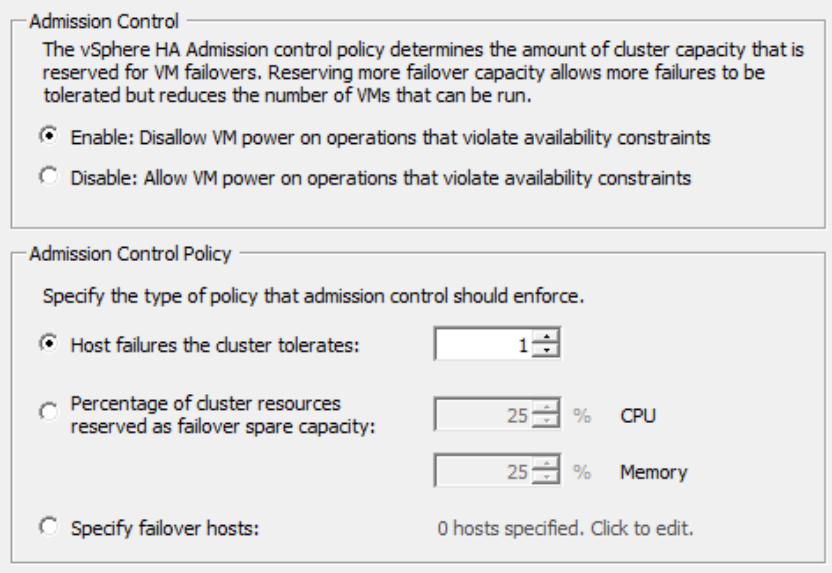


17.4.2 Admission control

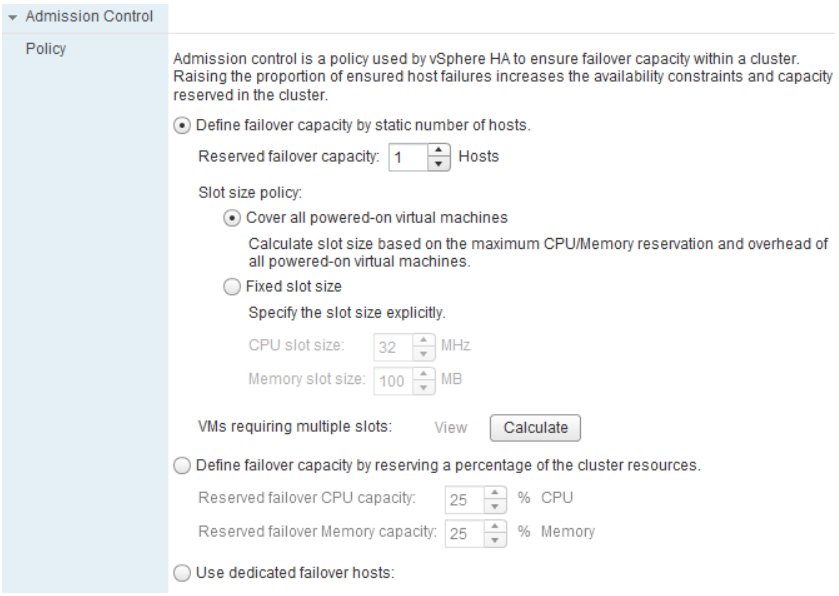
Il meccanismo Admission control controlla la quantità di risorse disponibili per una VM. Nel caso di vSphere HA, il sistema determina se possono essere garantite le risorse sufficienti per il failover di una macchina virtuale: se si, la macchina virtuale può essere accesa. In caso contrario, comparirà un avviso di risorse insufficienti. Se l'Admission control è disabilitato, vSphere HA non può garantire che tutte le VM di un host in errore possano essere riavviate. Con l'Admission control abilitato, è possibile impostare le politiche di funzionamento indicate di seguito.

- **Host Failures the cluster tolerates** (su vSphere Web Client la voce diventa **Define failover capacity by static number of hosts**) – con questa scelta, l'Admission Control calcola le risorse rimanenti nel cluster con un algoritmo basato sul concetto di **HA Slot**, e assegna ulteriori slot per tollerare il fallimento del numero di host specificato. Uno slot è una rappresentazione logica delle risorse di memoria e CPU che soddisfano le richieste di ogni VM in esecuzione nel cluster. Il numero massimo di host che possono fallire è illimitato.
- **Percentage of cluster resources reserved** (su vSphere Web Client la voce diventa **Define failover capacity by reserving a percentage of the cluster reources**) - la percentuale indica le risorse del cluster che devono rimanere inutilizzate, a disposizione di vSphere HA.
- **Specify a Failover Host** (su vSphere Web Client la voce diventa **Use dedicated failover hosts**) - con quest'opzione, se un host fallisce, le VM vengono riavviate in uno degli host specificati.

Abilitazione dell'Admission Control tramite vSphere Client

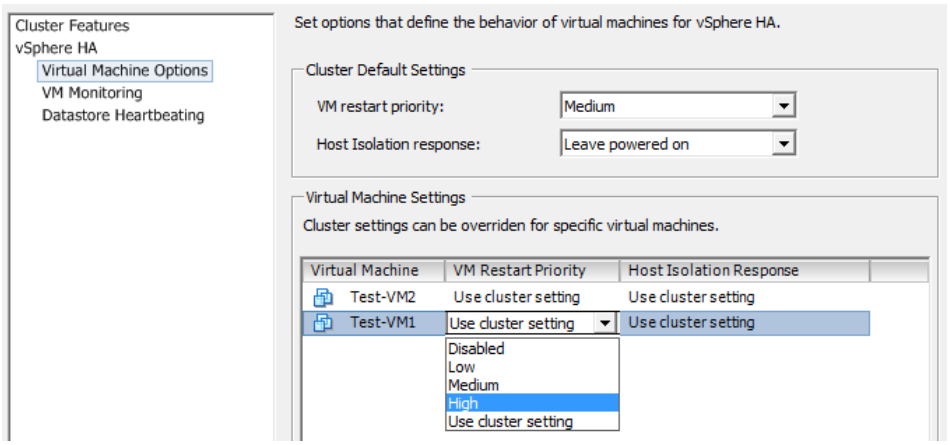


Abilitazione dell'Admission Control tramite vSphere Web Client



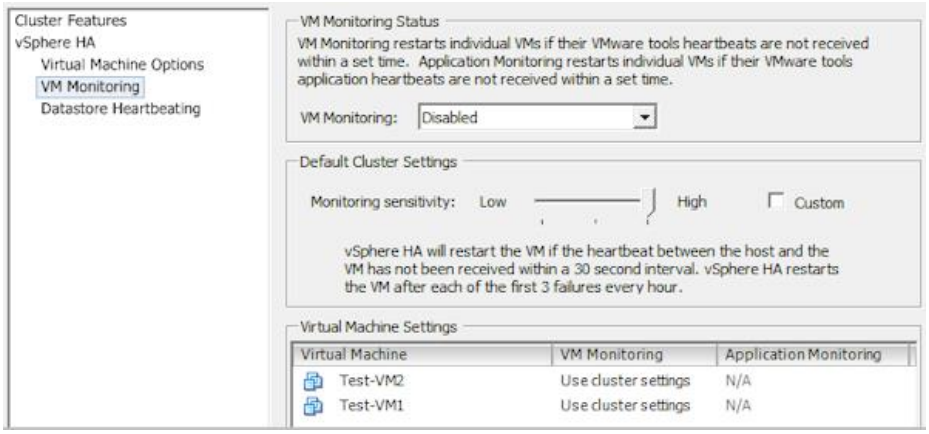
17.4.3 Virtual Machine Options

Il riavvio delle VM su altri host segue una precisa gerarchia: sono avviate prima le VM protette dal servizio di Fault Tolerance, poi le macchine che hanno priorità più alta. La priorità di una VM è ereditata dalle impostazioni del cluster, tuttavia può essere configurata manualmente nella pagina delle impostazioni di vSphere HA, alla voce **Virtual Machine Options** (su vSphere Web Client la voce è **VM Overrides**). In questa pagina è anche possibile decidere cosa fare delle VM in caso di intervento del servizio HA, anche per la situazione di host isolato a livello rete: si può decidere se lasciarle accese, fare uno shutdown delle stesse, o spegnerle con un power off. Se si desidera **disabilitare HA per una VM**, è sufficiente impostare la voce **Disabled** nella colonna **VM Restart Priority**.



17.4.4 Virtual Machine Monitoring

L'opzione VM Monitoring permette di riavviare specifiche VM quando la comunicazione heartbeat generata dai VMware Tools non viene ricevuta entro uno specifico periodo di tempo (di default è 2 minuti). Questa funzione è disabilitata in maniera predefinita.



17.5 Continuità del servizio con Fault Tolerance

Il servizio **Fault Tolerance** assicura la disponibilità continua delle VM, senza causare downtime o perdite di dati in caso di guasti su un host. Fault Tolerance può essere abilitato solo all'interno di un cluster vSphere HA. Abilitando Fault Tolerance per una VM, vSphere duplicherà quella VM su un altro host, tenendo accese entrambe le copie. La macchina di backup è chiamata "secondary virtual machine". In caso di crash dell'host che ospita la VM principale, la secondaria (già accesa e funzionante) viene promossa a primaria.

In condizioni normali, Fault Tolerance mantiene attiva la macchina virtuale secondaria in modalità "**virtual lockstep**" (blocco virtuale temporaneo). La tecnologia **VMware vLockstep** permette alla macchina virtuale secondaria di eseguire le stesse sequenze di istruzioni virtuali e ricevere gli stessi input previsti per la primaria; la VM secondaria è quindi pronta a subentrare in qualsiasi momento senza alcuna perdita di dati o interruzione di servizi. Entrambe le macchine virtuali sono viste e gestite come una singola unità, pur essendo poste su host fisici diversi; anche a livello di rete le macchine virtuali appaiono come una sola, con un solo indirizzo IP e un solo MAC address. Nel momento in cui una delle due VM, primaria o secondaria, dovesse risultare non più in linea, il servizio Fault Tolerance ne creerebbe una nuova copia su un altro host nello stesso cluster.

Il servizio Fault Tolerance impegna notevolmente lo storage e le risorse di rete; per questo motivo VMware raccomanda di non mantenere più di quattro VM con FT attivo per ogni host.

> Fault Tolerance richiede il vCenter Server solo per la configurazione iniziale. In seguito il servizio funzionerà sugli host in maniera indipendente dal vCenter.

17.5.1 Requisiti per l'attivazione del servizio di Fault Tolerance

Per quanto riguarda gli **host**:

- devono essere compatibili FT a livello di CPU;
- devono avere la licenza per l'uso di FT;
- devono essere certificati FT;
- devono avere le funzionalità di Hardware Virtualization (HV) abilitate a livello di BIOS.

Per quanto riguarda le **macchine virtuali**:

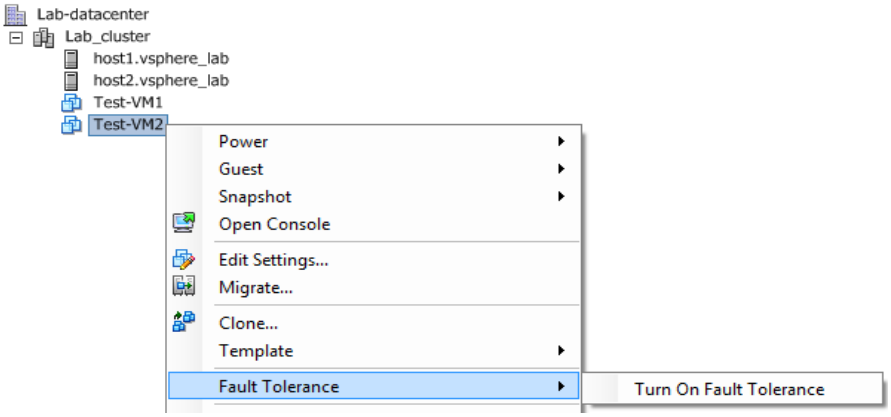
- non possono avere più di una vCPU; di conseguenza le VM con FT abilitato non possono utilizzare la tecnologia Virtual SMP che consente loro l'utilizzo di più vCPU;
- devono essere memorizzate in dischi VMDK in modalità thick o RDM in modalità virtuale; se si cerca di abilitare il servizio FT su una VM con dischi in modalità thin, un avviso indicherà che il disco dovrà essere convertito (a macchina spenta);
- devono avere in esecuzione un sistema operativo supportato;
- i file devono essere memorizzati in uno storage condiviso fra gli host.

17.5.2 Funzioni di vSphere non compatibili con Fault Tolerance

- **Snapshot** - per l'attivazione di FT su una VM, **tutte le snapshot devono essere rimosse**. Inoltre non possono essere generate snapshot per una VM con FT abilitato.
- **Storage vMotion** - non può essere utilizzato su una VM con FT abilitato. Per eseguire l'azione, disattivare FT per la VM e riabilitarlo al termine dello spostamento.
- **Linked clone** – non è possibile abilitare FT su una VM linked clone.
- **Virtual Machine Backup** - non possono essere utilizzate funzioni di backup che prevedono l'uso di snapshot.

17.5.3 Attivazione del Fault Tolerance su una macchina virtuale

Per proteggere una macchina virtuale con il servizio Fault Tolerance, fare clic con il tasto destro sulla VM desiderata all'interno del cluster, selezionare la voce Fault Tolerance e fare clic su **Turn on Fault Tolerance**. Con vSphere Web Client, selezionare le voci **All vCenter Actions > Fault Tolerance > Turn On Fault Tolerance**.



Capitolo 18
Protezione e backup dei dati

I metodi di backup tradizionali prevedono l'esistenza di un server di backup, collegato a dispositivi a nastro o array di dischi, ed un numero di agent software installati su ogni sistema operativo. Nelle architetture tradizionali, il rapporto tra sistemi operativi e server è di 1:1. Applicando questi metodi al mondo virtuale, ed estendendo questo impegno a tutte le VM presenti su un host, il carico potrebbe essere eccessivo, poichè gli agent impegnerebbero le risorse di ogni VM in maniera consistente durante le operazioni di backup. Non dimentichiamo poi che all'interno di un host virtualizzato più VM condividono le stesse interfacce di rete fisiche e lo stesso storage, elementi che potrebbero rivelarsi dei colli di bottiglia durante le procedure di backup con metodo tradizionale.

Le architetture virtuali offrono diversi vantaggi per le procedure di backup, con meccanismi che si differenziano dalla procedure tradizionali per una maggiore flessibilità e velocità. In particolare, indichiamo di seguito alcuni elementi chiave nelle procedure di backup in ambiente virtuale:

- possibilità di accesso diretto ai datastore che contengono le VM, con nessun carico sulle loro risorse durante il prelievo dei file dal datastore;
- nessuna necessità di agent software sulle VM;
- necessità di un solo livello di backup sia per il ripristino di un'intera VM che dei file in essa contenuti;
- il fatto che le VM vedano sempre lo stesso hardware rende agevole il ripristino su qualsiasi host.

Quando si avvia un'operazione di backup da una sorgente ad una destinazione, vi è un notevole impegno di risorse, non limitato alla rete su cui transitano i dati. La CPU infatti viene impegnata per le operazioni necessarie a individuare, decuplicare e comprimere i file oggetto del backup.

In ottica di flessibilità, VMware ha inoltre introdotto l'interfaccia **vSphere APIs for Data Protection** per permettere a software di terze parti l'interfacciamento con il sistema di backup di vSphere. L'interfaccia è integrata nativamente all'interno degli host ESXi.

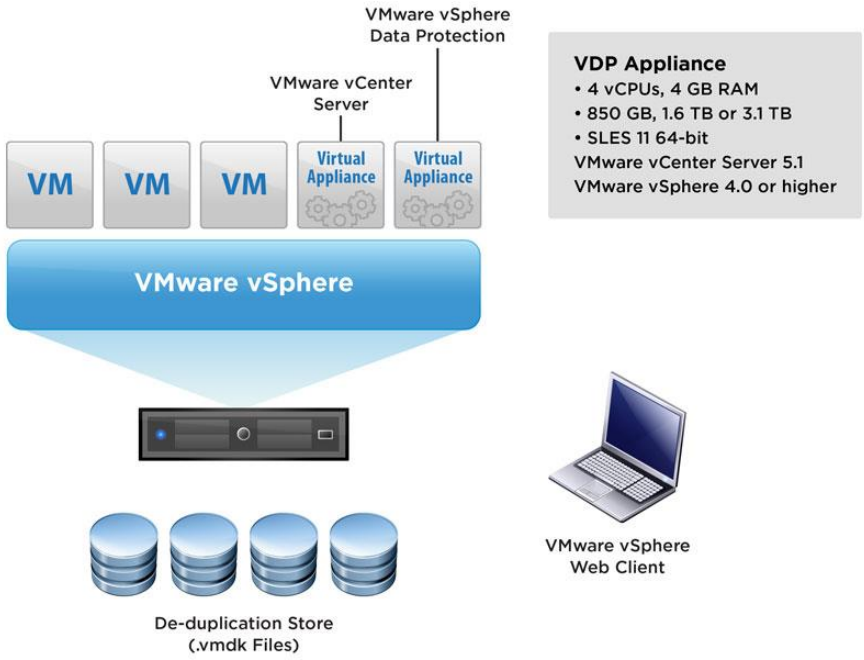
18.1 vSphere Data Protection

vSphere Data Protection (VDP) è una soluzione di backup su disco dedicata agli ambienti vSphere medio-piccoli. È rappresentata da un'appliance virtuale integrata con il vCenter Server e con la tecnologia **vSphere APIs for Data Protection**.

I punti che caratterizzano la soluzione VDP sono indicati di seguito.

- Backup disk-based per consentire un ripristino rapido delle macchine virtuali. I backup possono essere di tipo completo o incrementale.
- Backup di tipo image-level, con cui fornire backup completi delle VM, indipendentemente dal sistema operativo guest.
- Facile da distribuire, in quanto costituita da una macchina virtuale che gira su vSphere ESXi.
- Possibilità di ripristinare singoli file o intere immagini, in base alle necessità.
- Deduplica dei dati eseguita automaticamente per ogni operazione di backup.

- Impiego della funzionalità CBT (Changed Block Tracking) per tener traccia dei cambiamenti sui blocchi dei dischi virtuali.
- Inclusa a partire dalle edizioni vSphere Standard e vSphere Essentials Plus.

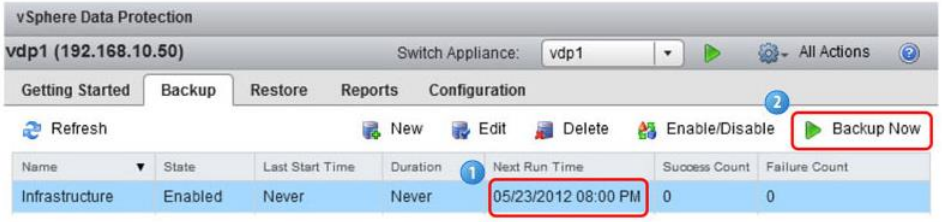


Ogni istanza di vCenter Server è in grado di supportare sino a 10 appliance VDP. Una virtual appliance VPD è costituita da 4 processori (vCPU) e 4GB di RAM. Ogni appliance può proteggere sino a 100 VM ed eseguire sino ad 8 operazioni di backup contemporanee; tuttavia le diverse appliance non condividono le informazioni sui loro backup. Per quanto riguarda la capacità di memorizzazione dei backup, sono disponibili tre diverse configurazioni:

- 0.5Tb (850Gb occupati su disco);
- 1Tb (1300Gb occupati su disco);
- 2Tb (3100Gb occupati su disco);

Lo spazio dedicato ai backup prende il nome di **deduplication store**. Lo spazio addizionale richiesto, che va oltre le dimensioni dedicate al backup, è necessario per la creazione e la gestione dei "checkpoints". Una volta implementata l'appliance, le sue dimensioni non possono essere più modificate.

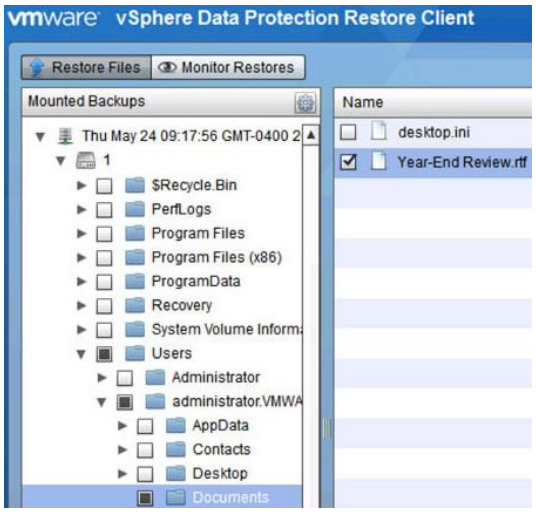
VDP fornisce un'interfaccia di gestione centralizzata, integrata nel vCenter Server, fruibile tramite vSphere Web Client. La creazione e la modifica delle attività di backup sono permesse a partire dal tab **Backup** presente nell'interfaccia di gestione, come mostrato nell'immagine sotto.



Per procedere con le operazioni di backup, è possibile selezionare le singole VM, oppure si può agire su contenitori quali datacenter, cluster e resource pool. Se si seleziona uno di questi

contenitori, il backup sarà eseguito per tutte le VM al suo interno. Ovviamente le attività possono essere programmate giornalmente, settimanalmente e mensilmente.

Per quanto riguarda le operazioni di recupero, è possibile ripristinare una VM in una posizione differente rispetto a quella originale. È possibile inoltre ripristinare singoli file o directory. Il recupero a livello file è possibile grazie a un tool chiamato **vSphere Data Protection Restore Client**.



18.1.1 Deduplicazione dei dati

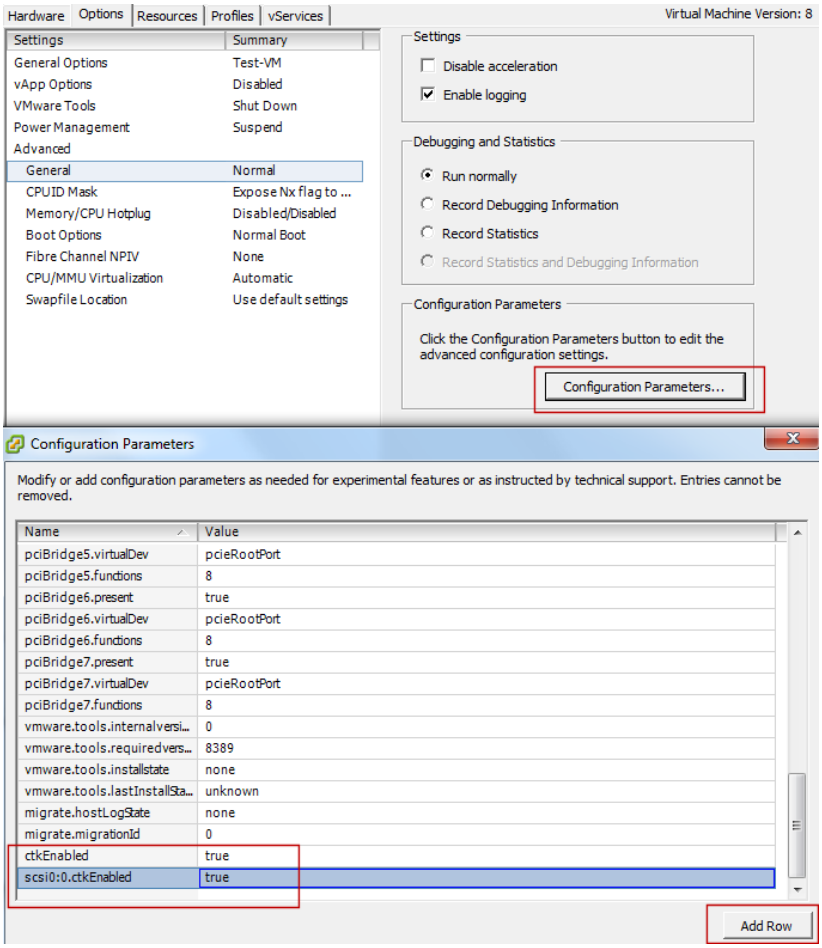
Nei punti sopra è stato indicato il supporto alla deduplicazione. Questa tecnologia prevede un meccanismo di backup a blocchi, differente dai meccanismi di backup tradizionali che invece agiscono per singoli file. In concreto, la deduplicazione è un processo in cui ogni blocco di dati viene confrontato con i blocchi precedentemente archiviati, per identificare una possibile ripetizione o ridondanza. Un blocco duplicato, ovvero ogni blocco contenente le stesse informazioni presenti nel backup precedente, non viene salvato una seconda volta. VDP utilizza la tecnologia **EMC Avamar** per la deduplicazione dei dati.

18.1.2 Changed Block Tracking

CBT, acronimo di Changed Block Tracking, è una funzionalità che si occupa, a livello di VMkernel, di tener traccia dei cambiamenti ai blocchi di un disco virtuale. È molto utile quando si devono gestire backup incrementali successivi ad un full backup. In quanto parte di vSphere APIs for Data Protection, la funzionalità può essere sfruttata da software di terze parti.

Le informazioni sui blocchi che hanno subito modifiche vengono fornite dal VMkernel alle applicazioni che ne fanno richiesta, senza che le applicazioni stesse debbano ricavare tali informazioni in maniera proprietaria, con conseguenti rallentamenti. Si consiglia tuttavia di non attivare CBT se non devono essere utilizzate applicazioni di backup che possano sfruttare le sue funzionalità.

Per l'utilizzo di CBT, l'hardware delle macchine virtuali deve essere almeno nella versione 7. La funzione di CBT è disabilitata per impostazione predefinita. Va attivata (tramite client vSphere o utilizzando l'SDK) su ogni macchina virtuale che vuole sfruttare questa funzione. Se si utilizza il client vSphere, è necessario aggiungere i parametri *ctkEnabled=true* e *scsi#:#.CtkEnabled=true* nella configurazione di ogni macchina virtuale. I simboli # fanno riferimento rispettivamente al controller e al disco della VM.



CBT memorizza le informazioni sui blocchi modificati in un file con suffisso "-ctk.vmdk", creato nella directory di ogni VM. Sarà presente un file "-ctk.vmdk" per ogni disco virtuale con CBT attivato. All'interno di questo file, lo stato di ciascun blocco viene monitorato e memorizzato con numeri di sequenza che permettono alle applicazioni di backup di sapere se un blocco ha subito modifiche.

Capitolo 19
La gestione degli aggiornamenti

19.1 Update Manager

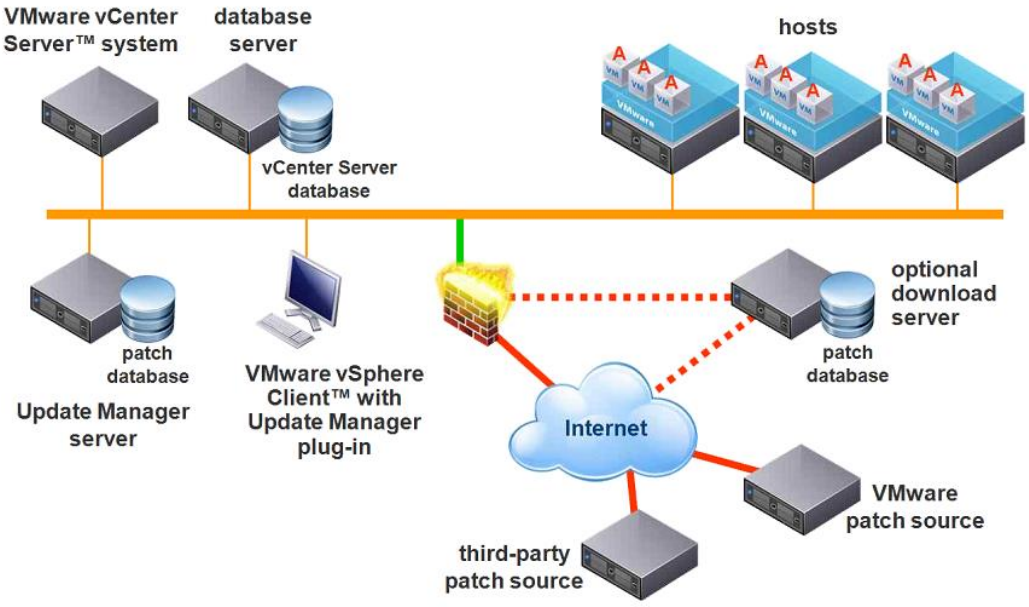
VMware vSphere Update Manager permette la gestione centralizzata degli aggiornamenti per i seguenti elementi:

- host ESX/ESXi;
- VMware Tools sulle macchine virtuali;
- hardware delle macchine virtuali;
- upgrade di appliance virtuali.

L'Update Manager permette inoltre l'upgrade a ESXi 5.1 per gli host ESX/ESXi 4.x e ESXi 5.0.

VMware vCenter Update Manager si compone di diversi elementi.

- **Update Manager Server** - installabile direttamente sul vCenter Server o su macchina separata (sia fisica che virtuale).
- **Patch database** - può essere installato sullo stesso motore DB utilizzato dal vCenter, oppure su un DB stand-alone.
- **Update manager plug-in** - viene eseguito nello stesso sistema su cui è stato installato il vSphere Client.
- **Guest agents** - sono gli agenti software installati all'interno delle macchine virtuali tramite l'Update Manager server.
- **Download Server** (opzionale) - utile se l'Update Manager non è connesso a Internet. Il download server è pertanto posizionato fuori dalla rete interna (ad esempio una DMZ), ed effettua il download delle patch da questa posizione. Il download viene eseguito dal servizio UMDS, che consente il download da URL multipli e permette di restringere il download a determinate versioni di prodotto.
- **Content Server** - rileva la disponibilità delle patch relative alle applicazioni più conosciute ed ai sistemi operativi. Si appoggia sul servizio internet Shavlik.

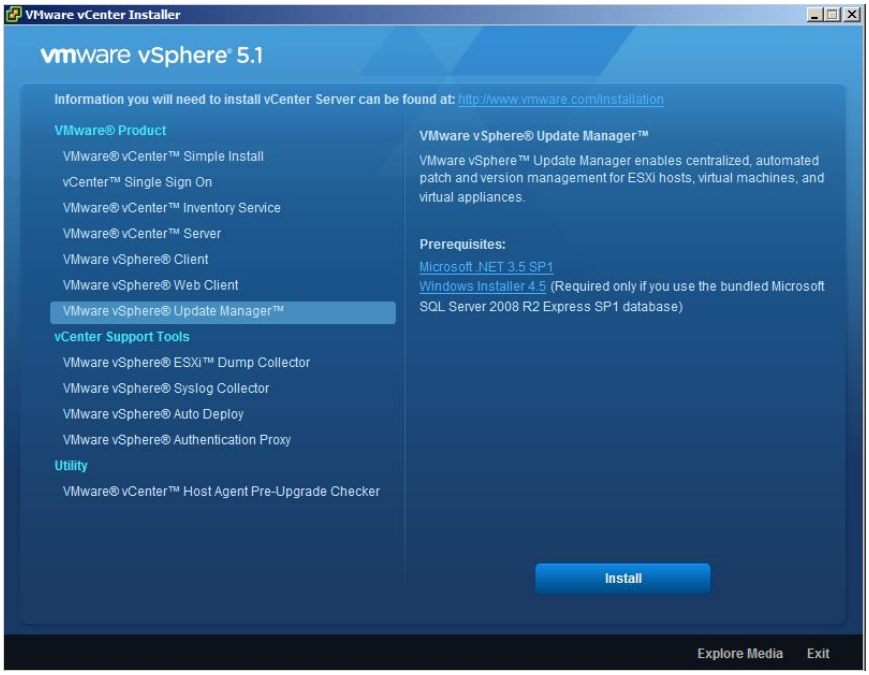


19.1.1 Installazione di Update Manager

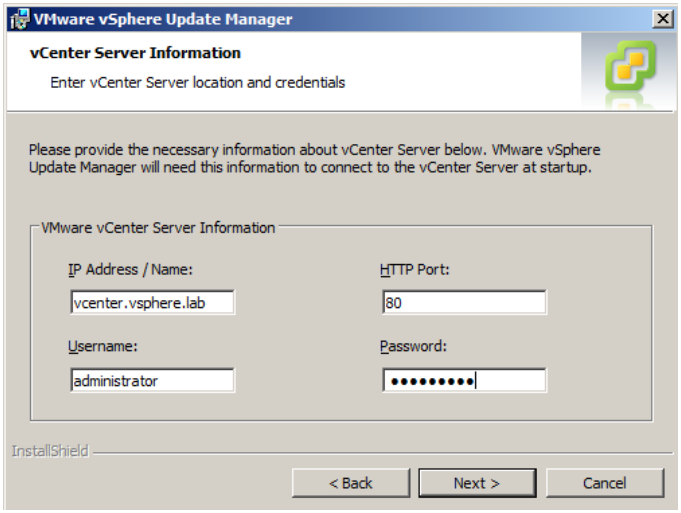
L'Update Manager può essere installato nella stessa macchina del vCenter Server o su macchina separata, sempre e solo su sistemi Windows Server 2003 e 2008 a 64 bit.

Per installare l'Update Manager ed i suoi componenti è necessario eseguire l'installer di VMware vCenter (esecuzione del file autorun.exe dal DVD di installazione).

- Dall'installer di VMware vCenter, selezionare la voce VMware vSphere Update Manager e fare clic su Install.

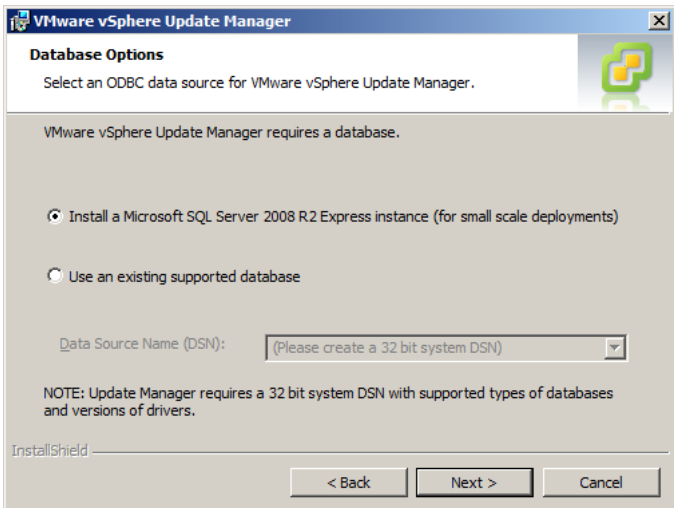


- Andare avanti sino alla finestra in cui fornire le informazioni del vCenter Server. Inserire quindi il nome o l'indirizzo IP del vCenter Server e le credenziali di accesso.

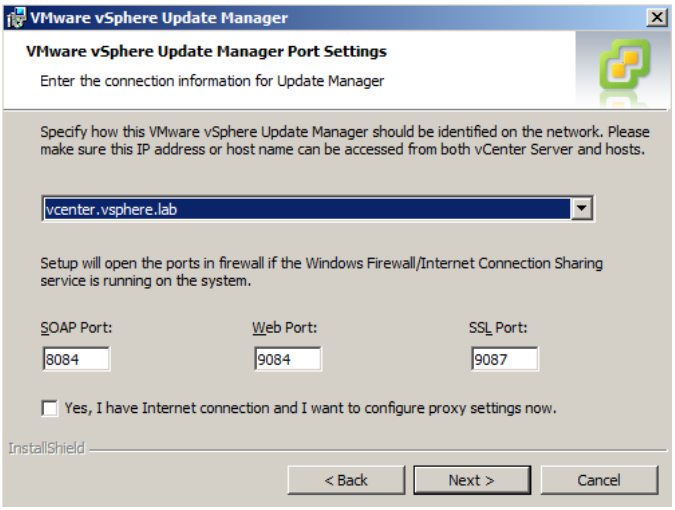


- Scegliere il database da utilizzare. Il database dell'Update Manager può risiedere nella stessa macchina in cui viene installato. Può essere di tipo integrato, basato su SQL Server

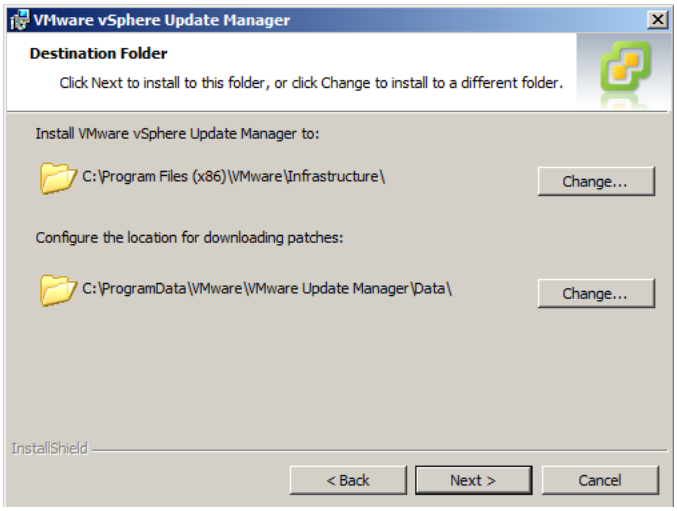
2008 R2 Express, sufficiente per un massimo di 5 host e 50 VM, oppure esterno (Oracle o SQL Server), per installazioni più grandi. Se si sceglie Microsoft SQL Server 2008 R2 Express, questo verrà installato e configurato automaticamente. Non sono richieste ulteriori configurazioni per il suo utilizzo.



- Andare avanti e modificare le porte di comunicazione solo se necessario. Se si utilizza un proxy per la navigazione, abilitare la voce "…I want to configure proxy settings now".



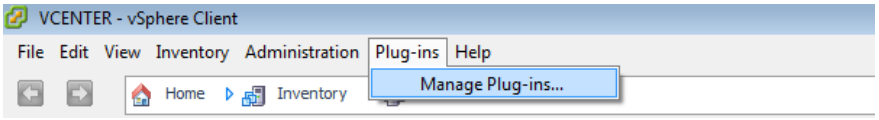
- Scegliere le cartelle di installazione e di download delle patch, andare avanti e fare clic su Finish per ultimare la procedura.



19.1.2 Installazione dell'interfaccia di gestione

L'interfaccia di gestione di Update Manager è integrata su vSphere Client tramite un plugin, chiamato **Update Manager Client Plug-In**; al momento (vSphere 5.1) non è possibile gestire l'Update Manager tramite vSphere Web Client. Per installare il plugin, seguire i passi indicati di seguito.

- Collegarsi al vCenter tramite vSphere Client.
- Andare su **Plug-ins > Manage Plug-ins.**

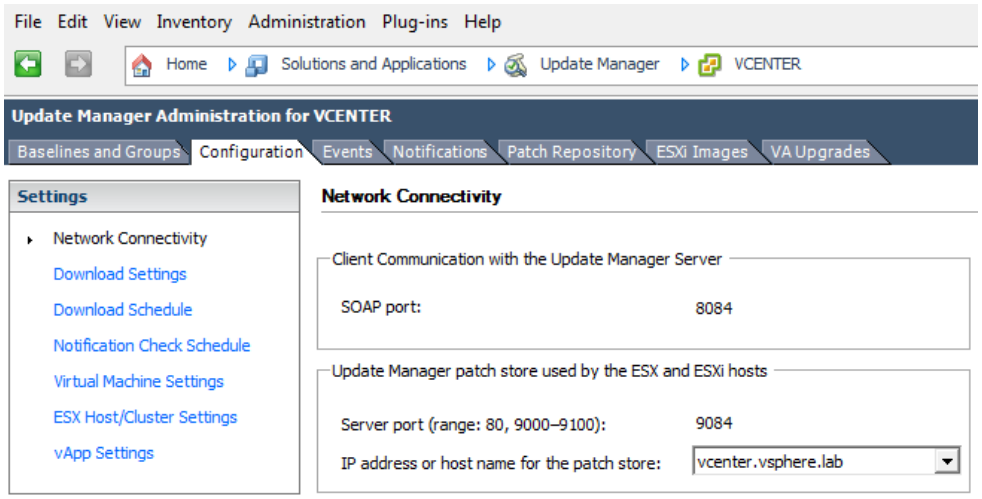


- Nella finestra di gestione plugin, selezionare la voce **Download and install** relativa al plugin **VMware vSphere Update Manager Extension**.

- Procedere con l'installazione di **vSphere Update Manager Client**.

19.2 Gestione e configurazione di Update Manager

Terminata l'installazione del plugin, l'interfaccia di gestione di Update Manager sarà raggiungibile da **Home > Solutions and Applications > Update Manager**. Per la configurazione delle impostazioni si va sul tab **Configuration**.



Le impostazioni configurabili sono indicate qui sotto.

- **Network Connectivity** – impostazione di indirizzo IP, nome host e porte di ascolto della macchina in cui è stato installato Update Manager.
- **Download Settings** - impostazioni su proxy e sulle patch da scaricare.
- **Download Schedule** - impostazioni sul download e sulla frequenza di verifica delle nuove patch.
- **Notification Check Schedule** - impostazioni sulla frequenza delle notifiche.
- **Virtual Machine Settings** - impostazione delle snapshot delle VM per garantire il ripristino in caso di problemi dovuti agli aggiornamenti.
- **ESX Host/Cluster Settings** - azioni che l'Update Manager deve intraprendere in caso di problemi su un host impostato in maintenance mode per necessità di aggiornamento.
- **vApp Settings** - impostazione dello smart reboot per le vApp.

19.2.1 Creazione di una baseline

Una baseline rappresenta un punto di riferimento per verificare il livello di aggiornamento di host, appliance e macchine virtuali. In pratica, una baseline è un insieme di patch e aggiornamenti, che possono riguardare host, macchine virtuali e virtual appliance.

Una baseline riguardante gli host può essere classificata in uno dei seguenti tipi:

- **host patch** - aggiornamenti di sicurezza riguardanti gli host ESX/ESXi;
- **host extension** - aggiornamenti per software e moduli addizionali riguardanti gli host ESX/ESXi;
- **host upgrade** - immagini ISO dell'hypervisor ESXi per l'aggiornamento dell'host da una versione precedente.

Una baseline riguardante le macchine virtuali permette di creare un riferimento per:

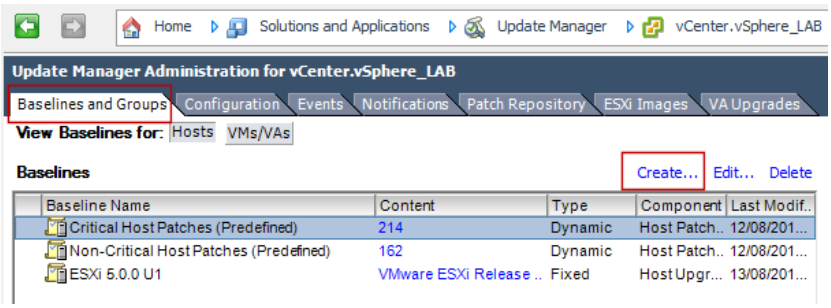
- versioni dei VMware Tools;
- versione dell'hardware delle macchine virtuali;
- versioni delle virtual appliance di terze parti.

Update Manager non supporta la creazione di baseline relative alle patch delle macchine virtuali: non è possibile, ad esempio, aggiornare una macchina Windows con le ultime patch rilasciate da Microsoft.

Una baseline può essere fissa o dinamica (**Fixed or Dynamic**): nel primo caso rimane identica a se stessa anche quando vengono scaricate nuove patch, nel secondo caso viene aggiornata con le nuove patch appena queste sono disponibili nell'Update Manager. I vari tipi di baseline possono essere raggruppati in una baseline di gruppo (**baseline group**), che consente il confronto di un oggetto con più baseline attraverso un solo passaggio. Esistono delle baseline predefinite, ma se ne possono creare delle nuove personalizzate.

Creazione di una nuova baseline

- Andare su **Home > Solutions and Applications > Update Manager**, selezionare il tab **Baseline and Groups** e fare clic sul link **Create**.

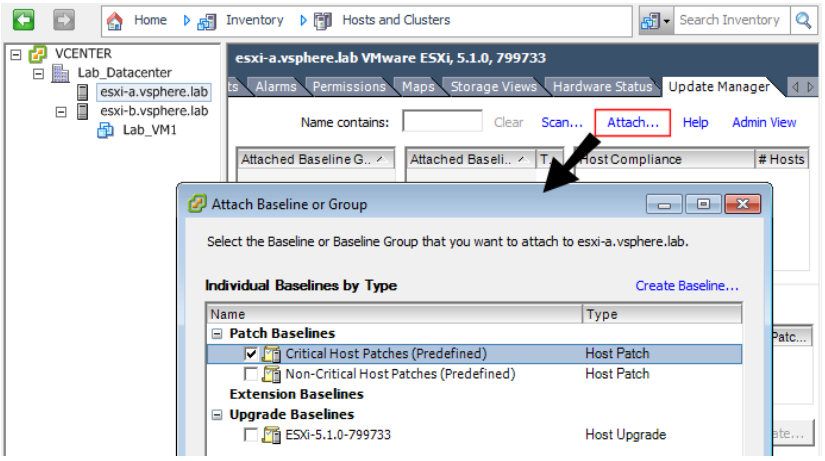


19.2.2 Collegamento di una baseline

Per verificare il livello di aggiornamento di un oggetto rispetto ad una baseline, è necessario collegare quest'ultima all'oggetto. Se l'oggetto contiene degli oggetti figlio, questi ultimi utilizzeranno la stessa baseline.

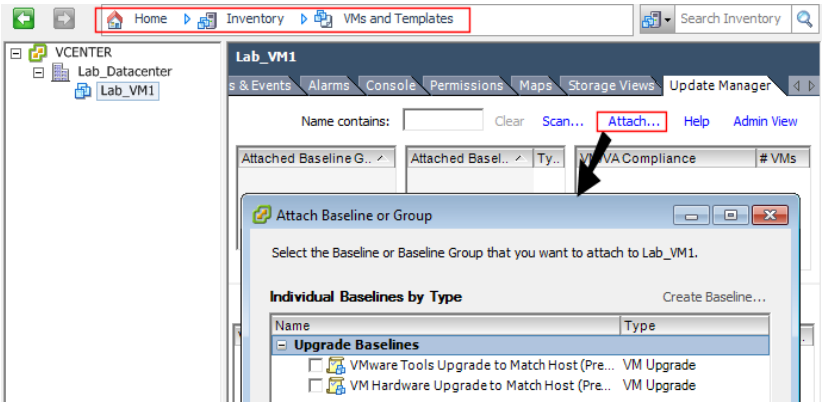
Collegare una baseline a un host

- Selezionare l'host dall'inventario.
- Entrare nel tab **Update Manager**, fare clic su **Attach** e selezionare la baseline o la baseline group da collegare.



Collegare una baseline a una macchina virtuale

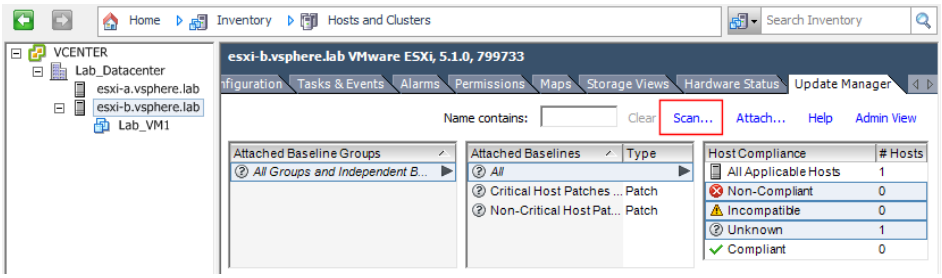
- Utilizzare la modalità di visualizzazione **VMs and Templates** (Home > Inventory > VMs and Templates).
- Selezionare una macchina virtuale, un template o un'appliance.
- Entrare nel tab **Update Manager**, fare clic su **Attach** e selezionare la baseline o la baseline group da collegare.



19.2.3 Esecuzione degli aggiornamenti

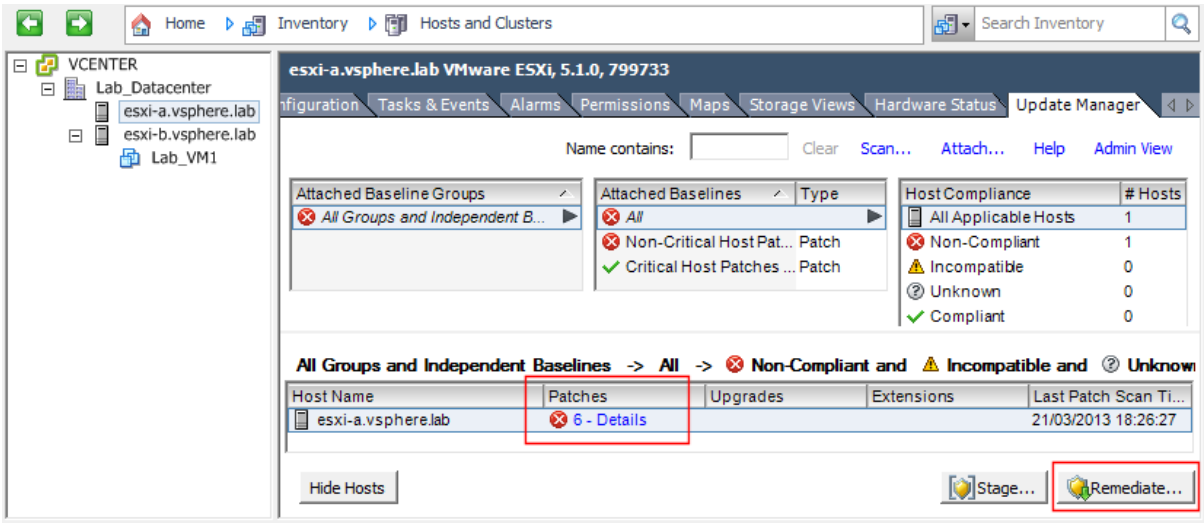
Per valutare il livello di sicurezza di un oggetto (host o VM) rispetto a una baseline, è necessario portare a termine una scansione per la verifica degli aggiornamenti necessari. Questa scansione può essere manuale o programmata. Se l'oggetto su cui viene eseguita la scansione ha degli oggetti figlio, anche questi ultimi saranno sottoposti a scansione.

Per eseguire una scansione manuale, selezionare l'oggetto, selezionare il tab Update Manager e fare clic su **Scan**.

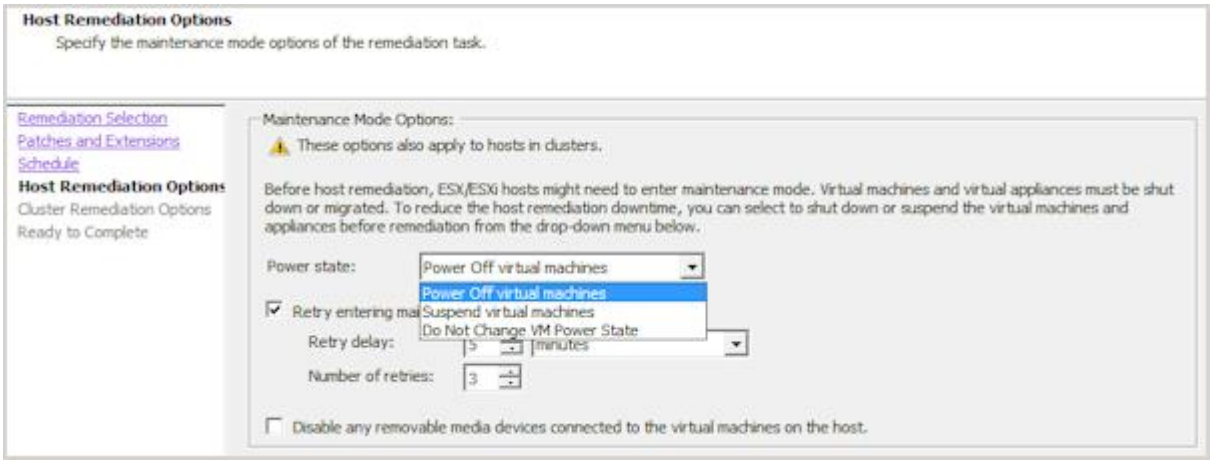


La stessa funzione è presente come voce nel menu contestuale dell'oggetto: tasto destro > **Scan for Updates**. Resta inteso che l'oggetto deve essere già collegato ad una baseline. Se invece si vuole programmare una scansione, andare su **Home > Management > Scheduled Tasks** e creare una nuova operazione programmata di tipo **Scan for Updates**.

I risultati della scansione sono visibili nel tab Update Manager relativo all'oggetto. Se l'oggetto è una VM, è necessario utilizzare la modalità di visualizzazione VMs and Templates. I dati forniti evidenziano il livello di conformità degli oggetti rispetto alle baseline collegate. Il livello di conformità si definisce **compliance**: un oggetto può essere **compliant** (conforme) o **non-compliant** (non-conforme). In caso di non conformità, per porre rimedio sarà necessario eseguire gli aggiornamenti indicati nelle baseline collegate all'oggetto. Per eseguire gli aggiornamenti, fare clic sulla funzione **Remediate**, disponibile come bottone nella parte inferiore del tab **Update Manager**, o selezionabile come voce nel menu contestuale dell'oggetto. Update Manager non prevede la funzione di remediate per l'appliance VMware vCenter Server.



L'operazione di remediation può richiedere che gli host siano in Maintenance Mode; in tal caso, è possibile scegliere a priori (nella procedura guidata di remediation) se spegnere le macchine virtuali, metterle in sospensione, oppure lasciarle nello stato in cui si trovano. In quest'ultimo caso, se le macchine sono accese, saranno spostate su altri host tramite vMotion.



Per limitare il downtime durante l'operazione di **remediation**, è possibile utilizzare la funzione **Stage**, che prevede il trasferimento di patch e aggiornamenti sugli host selezionati; in tal modo, quando si eseguirà il processo di remediation, i tempi di esecuzione risulteranno notevolmente ridotti, perché i file necessari si troveranno già negli host.

Bibliografia

Documentazione tecnica VMware vSphere 5.1 - http://www.vmware.com/support/pubs

- What's New in VMware vSphere 5.1
- vSphere Installation and Setup Guide
- vSphere Upgrade Guide
- vCenter Server and Host Management Guide
- vSphere Virtual Machine Administration Guide
- vSphere Host Profiles Guide
- vSphere Networking Guide
- vSphere Storage Guide
- vSphere Security Guide
- vSphere Resource Management Guide
- vSphere Availability Guide
- vSphere Monitoring and Performance Guide
- vSphere Data Protection Administration Guide

Documentazione di Marketing tecnico

- Novità di VMware vSphere 5.0 – Storage / MAGGIO 2011 (VMware Inc.)
- Novità di VMware vSphere 5.0 – Rete / APRILE 2011 (VMware Inc.)
- VMware vCenter Server – Datasheet IT – "Infrastruttura virtuale gestita dal centro e distribuita in tutta sicurezza" (VMware Inc.)
- VMware vSphere Essentials and Essentials Plus - Datasheet IT (VMware Inc.)

Manuali del corso di certificazione

- VMware vSphere ESXi 5.0 and vCenter Server 5.0 Student Manual: Install, Configure, Manage - Volumi 1 e 2 (VMware Inc.)