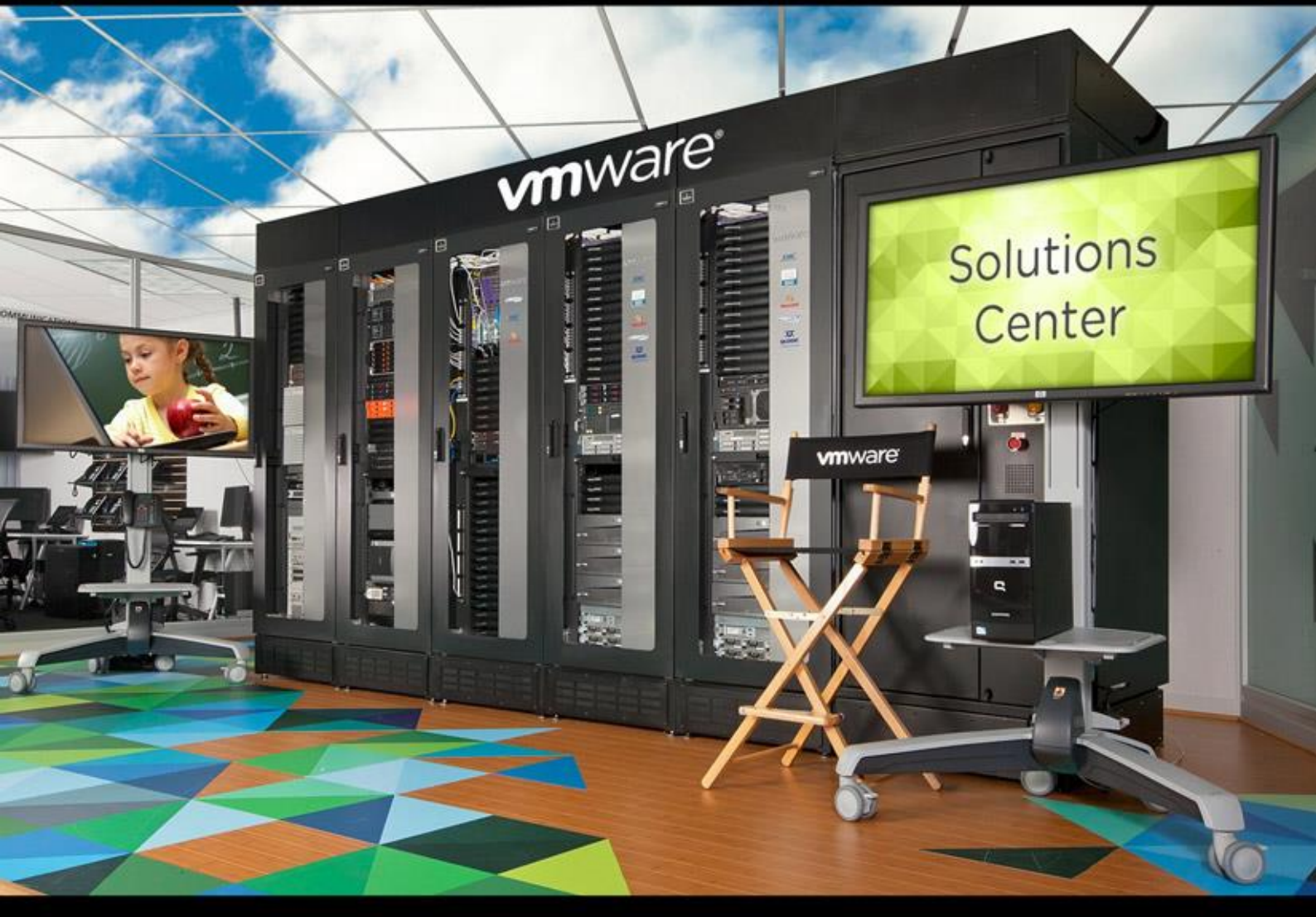




# VMware vSphere 5.0

آموزش نصب، پیکربندی و مدیریت زیر ساخت مجازی



ترجمه و تالیف: احسان علیمحمدی

[www.yepco.ir](http://www.yepco.ir)

بِسْمِ اللَّهِ  
الرَّحْمَنِ  
الرَّحِيمِ

تقدیم به آنان که وجودم جز هدیه وجودشان نیست

پدر و مادر عزیزم

و

تقدیم به مهدی آذربایجانی که با صبرش در تمامی لحظات رفیق راه بود

این کتاب رایگان است و حق فروش آن تنها برای نویسنده و شرکت یگانه ارتباطات پیشرو محفوظ می باشد اما اگر احساس کردید که برای شما مفید بوده، خوشحال می شویم مبلغی را برای حمایت از کودکان سرطانی در وب سایت [موسسه خیریه محک](#) پرداخت نمایید، واریز اینترنتی آن بیش از ۲ دقیقه زمان نخواهد برد. پیشاپیش از شما سپاسگزاریم.

## فهرست مطالب

۱۴	مقدمه
۱۵	فصل اول: مجازی سازی چیست؟
۱۶	بخش اول: معرفی مجازی سازی
۱۷	زیر ساخت فیزیکی
۱۸	زیر ساخت مجازی
۱۹	معماری فیزیکی و مجازی
۲۰	چرا از ماشین مجازی (VM) استفاده می کنیم؟
۲۲	منابع اشتراکی
۲۳	مجازی سازی CPU
۲۴	استفاده از حافظه فیزیکی و مجازی هاست
۲۵	شبکه فیزیکی و مجازی
۲۷	فایل سیستم های فیزیکی و VMware vSphere VMFS
۲۹	کپسوله سازی
۳۰	ساختار فایل سیستم
۳۱	فایل های ماشین مجازی (vm)
۳۳	بخش دوم: واسط کاربری VMware vSphere
۳۴	واسط کاربری
۳۵	دانلود کردن vSphere Client
۳۶	استفاده از vSphere Client
۳۷	vSphere Client: سربرگ پیکربندی
۳۸	مشاهده پیکربندی حافظه و پردازنده
۳۹	مشاهده Log های سیستم ESXi
۴۱	مشاهده قابلیت های دارای لایسنس
۴۲	مدیریت ESXi از طریق خط فرمان
۴۴	کارگاه شما ره یک:
۴۵	بخش سوم: بررسی اجمالی ESXi
۴۶	VMware ESXi
۴۸	معماری ESXi



۵۰.....	پیکربندی ESXi
۵۱.....	پیکربندی ESXi : دسترسی root
۵۲.....	پیکربندی ESXi : مدیریت شبکه
۵۳.....	پیکربندی ESXi : سایر تنظیمات
۵۴.....	ESXi به عنوان یک کلاینت NTP
۵۵.....	تنظیمات شبکه: DNS & Routing
۵۶.....	تنظیمات دسترسی از راه دور : پروفایل امنیتی
۵۷.....	بهترین روش مدیریت کا ربران ESXi
۵۸.....	کارگاه شماره دو:
۵۹.....	فصل دوم: ماشین های مجازی
۶۰.....	بخش اول: مفاهیم ماشین مجازی
۶۱.....	ماشین مجازی چیست؟
۶۲.....	فایل های که یک ماشین مجازی ایجاد می کند
۶۴.....	مشاهده فایل های ماشین مجازی
۶۵.....	استفاده از سربرگ Storage Views برای نمایش فایل ها
۶۷.....	سخت افزار ماشین مجازی
۶۹.....	CPU و حافظه
۷۰.....	دیسک مجازی
۷۲.....	کارت شبکه مجازی
۷۴.....	سایر دستگاه ها
۷۶.....	کنسول ماشین مجازی
۷۸.....	بخش دوم: ایجاد ماشین مجازی
۷۹.....	ویزا رد ایجاد ماشین مجازی
۸۰.....	انتخاب پیکربندی Typical
۸۲.....	امکان Thin Provisioning در دیسک مجازی
۸۳.....	انتخاب پیکربندی Custom
۸۵.....	Raw Device Mapping
۸۶.....	نصب سیستم عامل
۸۷.....	VMware Tools

۸۹.....	Virtual Appliance
۹۰.....	نصب یک قالب OVF
۹۱.....	کارگاه شماره سه:
۹۲.....	فصل سوم: VMware vCenter Server
۹۳.....	بخش اول: نصب ESXi
۹۴.....	پیش نیازهای سخت افزاری ESXi
۹۶.....	نصب ESXi 5.0
۹۸.....	نصب ESXi
۹۹.....	بوت شدن ESXi از SAN Storage
۱۰۱.....	بخش دوم: معماری vCenter Server
۱۰۲.....	vCenter Server به عنوان یک پلتفرم مدیریتی
۱۰۳.....	معماری vCenter
۱۰۴.....	ارتباط ESXi و vCenter Server
۱۰۵.....	کامپوننت های vCenter Server
۱۰۶.....	ماژول های vCenter Server
۱۰۷.....	ماژول های پیش فرض vCenter Server
۱۰۹.....	بخش سوم: نصب vCenter Server - نسخه ویندوز
۱۱۰.....	گزینه های پیاده سازی vCenter Server
۱۱۱.....	نیازمندیهای سخت افزار و نرم افزار vCenter Server
۱۱۳.....	نیازمندیهای دیتابیس vCenter
۱۱۴.....	محاسبه اندازه دیتابیس
۱۱۵.....	پیش از نصب vCenter Server
۱۱۶.....	نصب vCenter Server و کامپوننت های آن
۱۱۷.....	نصب vCenter Server در حالت Standalone Instance و یا Linked Mode Group
۱۱۸.....	ویژارد نصب vCenter Server
۱۲۰.....	سرویس های vCenter Server
۱۲۱.....	کارگاه شماره چهار:
۱۲۲.....	بخش چهارم: نصب و توسعه vCenter Virtual Appliance
۱۲۳.....	قابلیت های vCenter Server Appliance

۱۲۵.....	vCenter Server Appliance	مزیت های
۱۲۶.....	vCenter Server Appliance	نیازمندیهای
۱۲۷.....	Appliance	وارد کردن
۱۲۸.....	Appliance	شروع به کار کردن
۱۲۹.....	vCenter Server Appliance	پیکربندی شبکه
۱۳۰.....	vCenter Server Appliance	پیکربندی منطقه زمانی
۱۳۱.....		اتصال به واسط کاربری تحت وب
۱۳۲.....	vCenter Server	پیکربندی
۱۳۴.....	vCenter Server Services	مدیریت
۱۳۵.....	vCenter Server	سایر پیکربندهای
۱۳۶.....		کارگاه شما ره پنج:
۱۳۷.....	vCenter Server	بخش پنجم: مدیریت
۱۳۸.....		آبجکت های دیتاستر
۱۳۹.....		سازماندهی آبجکت ها درون پوشه ها
۱۴۰.....	vSphere Client	راهنمای
۱۴۱.....	vCenter Server	نمای Host ها و کلاستر ها و vm و Template ها
۱۴۲.....	vCenter Server	نمای Datastores & Networks
۱۴۳.....	vCenter Server	افزودن یک هاست به
۱۴۴.....	vCenter	نگاه اجمالی به لایسنس
۱۴۵.....	vCenter Server	رویدادهای
۱۴۶.....	vCenter Server System Logs	
۱۴۷.....		کارگاه شما ره شش:
۱۴۸.....		فصل چهارم: پیکربندی و مدیریت شبکه مجازی
۱۴۹.....	vNetwork Standard Switch	بخش اول: معرفی
۱۵۰.....		شبکه مجازی و سوئیچ مجازی چیست؟
۱۵۱.....		انواع اتصالات سوئیچ مجازی
۱۵۲.....		مثال هایی از اتصالات سوئیچ مجازی
۱۵۳.....		انواع سوئیچ های مجازی
۱۵۴.....		کامپوننت های سوئیچ مجازی استاندارد

۱۵۶	..... پیکربندی سوئیچ مجازی استاندارد
۱۵۷	..... پورت های سوئیچ مجازی استاندارد
۱۵۸	..... خصوصیات آداپتور شبکه
۱۵۹	..... VLANs
۱۶۰	..... ملاحظات شبکه فیزیکی
۱۶۱	..... کارگاه شمار هفت:
۱۶۲	..... بخش دوم: پیکربندی پالیسی های Standard Virtual Switch
۱۶۳	..... پالیسی های شبکه
۱۶۴	..... پالیسی امنیت
۱۶۶	..... پالیسی Traffic Shapping
۱۶۷	..... پیکربندی Traffic Shapping
۱۶۸	..... پالیسی NIC Teaming
۱۷۰	..... متد Load Balancing: مبتنی بر Port ID
۱۷۱	..... متد Load Balancing: مبتنی بر Source MAC Hash
۱۷۲	..... متد Load Balancing: مبتنی بر IP Hash
۱۷۴	..... تشخیص و مدیریت خرابی شبکه
۱۷۶	..... فصل پنجم: پیکربندی و مدیریت Storage مجازی
۱۷۷	..... بخش اول: مفاهیم Storage
۱۷۸	..... نگاه اجمالی به Storage
۱۸۰	..... نگاه اجمالی به پروتکل های Storage
۱۸۲	..... Datastore
۱۸۳	..... VMFS نسخه 5.0
۱۸۵	..... NFS
۱۸۶	..... قرارداد های نامگذاری Storage
۱۸۸	..... نمای نقشه ای Storage
۱۸۹	..... ملاحظات که در Storage های فیزیکی باید مورد توجه قرار گیرد
۱۹۰	..... بخش دوم: پیکربندی iSCSI Storage
۱۹۱	..... کامپوننت های iSCSI
۱۹۲	..... آدرس دهی و نام گذاری iSCSI Node

۱۹۳	.....	iSCSI Initiator – iSCSI	آغاز کننده
۱۹۵	.....	Software iSCSI	پیکربندی
۱۹۶	.....	IP Storage	پیکربندی شبکه برای ESXi
۱۹۷	.....	iSCSI Target	روش های شناسایی و جستجوی
۱۹۸	.....	CHAP	امنیت در iSCSI :
۲۰۰	.....	iSCSI	سخت افزاری
۲۰۱	.....	iSCSI Storage	چند مسیر سازی با
۲۰۲	.....	NAS/NFS Storage	بخش سوم: پیکربندی
۲۰۳	.....	NFS	کامپوننت های
۲۰۴	.....	NFS	پیکربندی برای کنترل دسترسی
۲۰۶	.....	NFS	آدرس دهی و کنترل دسترسی
۲۰۷	.....	NFS Datastore	پیکربندی یک
۲۰۹	.....	IP Storage	نمای اطلاعات
۲۱۰	.....	NFS Datastore	Unmount کردن و حذف کردن یک
۲۱۱	.....	NFS Storage	چند مسیر سازی و
۲۱۳	.....		کارگاه شماره هشت:
۲۱۳	.....		کارگاه شماره نه:

## مقدمه

در این کتاب سعی شده است تا مفاهیم پایه ای مجازی سازی و VMware vSphere به شکلی تصویری و با نثری نسبتاً روان برای شما عزیزان ارائه گردد. توصیه می شود که پیش از مطالعه هر صفحه ابتدا اسلاید های تصویری آن را با دقت مطالعه و سپس به متن ترجمه شده آن مراجعه نمایید. بدین ترتیب می توانید درک بهتری از مسائل داشته باشید. به نظر بنده درک این کتاب برای کسانی که هیچ گونه آشنایی با مجازی سازی و ابزار VMware vSphere ندارند آسان می باشد البته اگر این کتاب را مطالعه نمودید و اشکالاتی را در آن یافتید، ممنون می شوم تا انتقاد خود را برای بنده ارسال نمایید تا در نسخه های بعدی آن را اصلاح نمائیم. لازم به ذکر است که کارگاه های آموزشی که در این کتاب مطرح شده در حال حاضر آماده ارائه نیست و تلاش ما بر این است که این کارگاه ها را در قالب فایل های ویدئویی رایگان عرضه نمائیم. منتظر انتقادات و پیشنهادات شما عزیزان هستیم.

احسان علیمحمدی

[Alimohamadi@Yepco.ir](mailto:Alimohamadi@Yepco.ir)

۱۳۹۲/۰۷/۳۰



## فصل اول: مجازی سازی چیست؟



این فصل شامل بخش های زیر می گردد:

۱. معرفی مجازی سازی
۲. رابط کاربری VMware vSphere
۳. بررسی اجمالی ESXi

اهمیت این فصل:

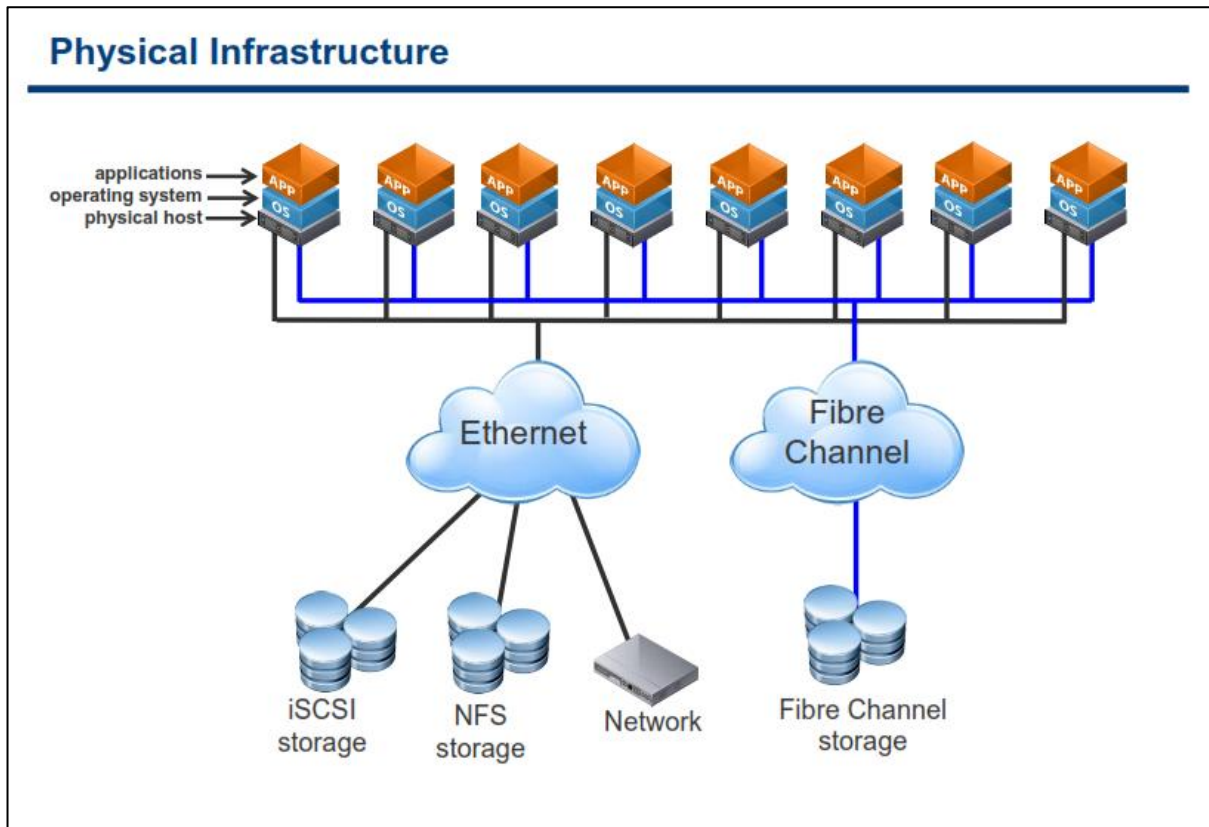
VMware vSphere بر مبنای اجزا و کامپوننت های متعددی پیاده سازی شده است که شما می بایست به عنوان یک vSphere Administrator با آنها آشنا باشید. در این فصل مفاهیم کلی مجازی سازی، ماشین مجازی، ESXi و همچنین اجزای اصلی vSphere تشریح می گردد. در ادامه شما به این نکته پی خواهید برد که vSphere چگونه می تواند در دیتاستر ها به کمک شما بیاید.

## بخش اول: معرفی مجازی سازی

بعد از به اتمام رساندن این بخش شما قادر خواهید بود:

- تفاوت میان معماری مجازی و فیزیکی را درک و تشریح نمایید
- یک ماشین مجازی (VM) را تعریف نمایید
- مزیت های استفاده از ماشین مجازی را تشریح نمایید
- نحوه برخورد VMware vSphere با پردازنده ها (CPU)، حافظه (Memory)، شبکه (Network) و دیسک ها (Disk) را تشریح نمایید
- فایل های یک ماشین مجازی را شناسایی و تشریح نمایید
- معماری ESXi را تشریح نمایید

## زیرساخت فیزیکی

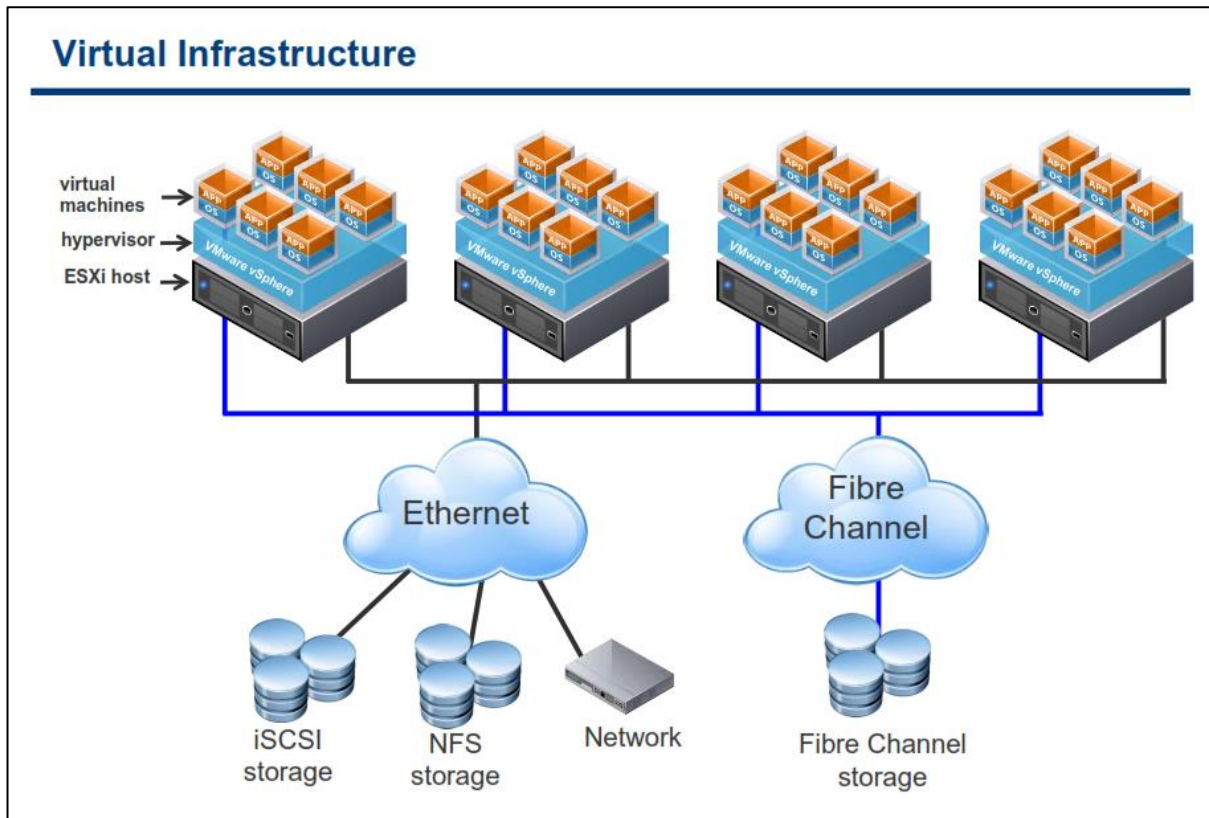


به صورت سنتی، سیستم عامل ها و نرم افزارها بروی کامپیوترهای فیزیکی اجرا می شوند که همین امر باعث بوجود آمدن چالش های متعددی در اجرای تعداد زیادی از سرورهای فیزیکی در یک دیتاسنتر شده است. این مدل از انعطاف پذیری و کارآمدی بالایی برخوردار نیست. البته برنامه ریزی و هزینه ای که برای زیرساخت های یک دیتاسنتر از قبیل فضای رک، برق اضطراری، کابل کشی، تامین سرور و غیره انجام می شود بسیار مهم هستند اما بخش کمی از مشکلات مربوط به این موارد می گردد.

در حالت استاندارد هر یک از نرم افزارها در یک دیتاسنتر می بایست بروی یک سیستم عامل به اجرا در بیایند که در این صورت شما می بایست از تعداد زیادی سرور فیزیکی استفاده نمایید که این مسئله در بسیاری موارد به سود سازمان نخواهد بود، چراکه در این حالت شما تنها از ۵ الی ۱۰ درصد ظرفیت و توان سرورهای فیزیکی خود استفاده می نمایید و همچنین می بایست از فضای دیتاسنتر بزرگتری برخوردار باشید و در کنار آن از سیستم های تامین برق و خنک کننده قدرتمندتری استفاده نمایید که این عوامل خود نیز هزینه های شما افزایش خواهند داد.

همچنین تهیه سرور نیز در چنین محیط هایی زمان بر می باشد و می بایست زمان زیادی صرف تهیه سخت افزار، نصب و راه اندازی سیستم عامل، آنتی ویروس، سرویس پک و غیره شود و از طرفی زمان زیادی باید صرف نمایند تا سرورها را با محیط دیتاسنتر خود یکپارچه کنید به عنوان مثال: باز کردن پورت، پیکربندی Rule فایروال، اتصال به Storage و غیره.

## زیرساخت مجازی

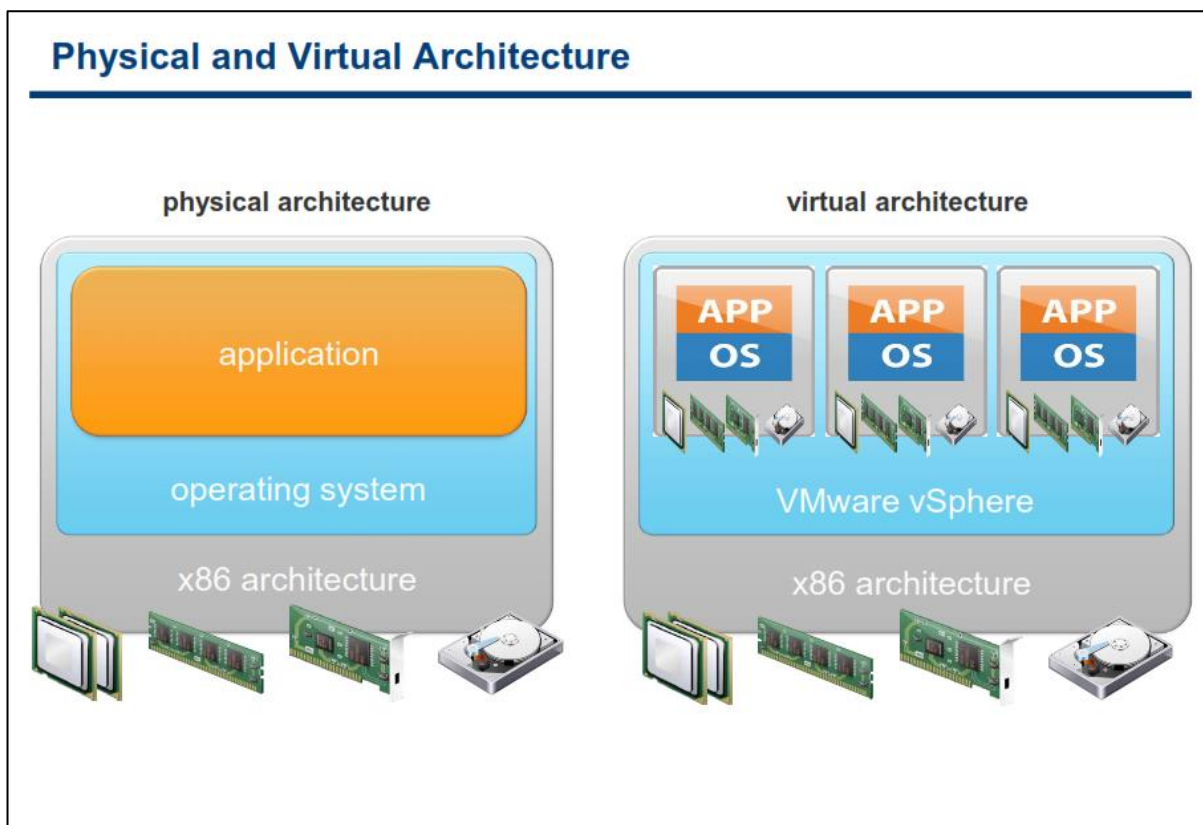


مجازی سازی این قابلیت را برای شما فراهم می کند تا بتوانید چندین ماشین مجازی (ماشین مجازی شامل یک سیستم عامل و یک برنامه می باشد) را بروی یک سرور به صورت مجازی به اجرا در بیاورید. توجه داشته باشید که هر یک از برنامه ها به صورت مستقل بروی یک سیستم عامل به اجرا در می آیند. تبدیل یک دیتاسنتر فیزیکی به یک دیتاسنتر مجازی باعث کاهش موارد مورد نیاز یک دیتاسنتر از قبیل سیستم تامین برق، سیستم خنک کنندگی، کابل کشی، فضای مصرفی در داخل رک، تجهیزات شبکه، منابع ذخیره سازی و غیره می شود چراکه شما با این کار تعداد سرور های فیزیکی خود را کاهش داده اید.

این کاهش دادن با تبدیل شدن چندین سرور فیزیکی به ماشین های مجازی و در نهایت یکی کردن آنها در یک Host امکان پذیر می شود. Host کامپیوتر میزبانی می باشد که چندین ماشین مجازی بروی آن به اجرا در می آیند.

در محیط های مجازی، تهیه و راه اندازی سرورهای جدید همانند حالت قبل سخت و پیچیده نیست و شما دیگر نیازی به صبر کردن برای تهیه سخت افزار، نصب سیستم عامل، سرویس پک، کابل کشی و سیستم خنک کننده (Cooling) ندارید. بدین ترتیب شما به سادگی می توانید از طریق یک رابط کاربری گرافیکی (GUI) این کار را عرض چند دقیقه انجام دهید.

## معماری فیزیکی و مجازی



مجازی سازی، راه حلی برای بسیاری از مشکلات است که توسط کارکنان بخش IT مشاهده می شود. مجازی سازی تکنولوژی است که در واقع سخت افزار فیزیکی را از سیستم عامل کامپیوتر جدا می کند. مجازی سازی برای شما این قابلیت را فراهم می کند تا بتوانید حجم زیادی از پردازش ها را از طریق ماشین های مجازی و با قراردادن آنها بروی یک کامپیوتر به اجرا در آورید.

یک ماشین مجازی (vm) یک کامپیوتری است که به صورت نرم افزاری ایجاد می شود و شبیه یک کامپیوتر فیزیکی، سیستم عامل و برنامه ها می توانند بروی آن نصب و اجرا گردند. هر vm شامل سخت افزارهای مجازی خود از قبیل CPU, Memory, Network Adapter, Hard Disk و همچنین سیستم عامل و برنامه های کاربردی می باشد.

در تصویر بالا تفاوت بین معماری فیزیکی و مجازی مشخص شده است. در ساختار فیزیکی سیستم عامل بطور مستقیم با سخت افزار نصب شده در ارتباط می باشد و پردازش ها را اجرا و تخصیص حافظه و ... را انجام می دهد.

اما در مقابل یک هاست مجازی شده با سخت افزار از طریق یک لایه نرم افزاری که لایه مجازی سازی یا همان Hypervisor در ارتباط می باشد. Hypervisor منابع سخت افزاری را بصورت دینامیکی و پویا برای ماشین مجازی فراهم می کند. همچنین Hypervisor این قابلیت را برای vm فراهم می کند که بتواند بدون وابستگی به سخت افزار لایه پائین به فعالیت خود ادامه دهد و در واقع به سخت افزار Hypervisor وابسته نباشد. بطور مثال یک vm می تواند از یک هاست مجازی شده به هاست دیگر منتقل شود بدون اینکه مشکلی بوجود آید یا همچنین Hard Disk های مجازی یک ماشین مجازی می توانند از یک نوع منبع ذخیره سازی (Storage) به یک نوع دیگر منتقل شوند.

## چرا از ماشین مجازی (VM) استفاده می‌کنیم؟

## Why Use Virtual Machines?

**Physical machine****Difficult to move or copy****Bound to a specific set of hardware components****Often has a short lifecycle****Requires personal contact to upgrade hardware****Virtual machine****Easy to move and copy:**

- Encapsulated into files
- Independent of physical hardware

**Easy to manage:**

- Isolated from other virtual machines
- Insulated from hardware changes

**Provides the ability to support legacy applications****Allows servers to be consolidated**

بروی یک ماشین فیزیکی شما می‌توانید مستقیماً یک سیستم عامل یا OS را نصب کنید، اما می‌بایست برای هر سخت افزار درایور مخصوص به خودش را نصب کنید و در صورت ارتقاء مجدد باید این کار را دوباره انجام دهید و بدین ترتیب همیشه نیاز است تا تکنسین‌ها این کار را پس از ارتقاء سخت افزار و یا OS انجام دهند.

اما **vm** ۱۰۰٪ نرم افزاری است و در واقع مجموعه‌ای از فایل‌ها می‌باشد. **vm** ها از درایورهای استاندارد دستگاه‌ها استفاده می‌کنند و بدین ترتیب سخت افزارها می‌تواند بدون اینکه نیاز به تغییر درایور و یا بخش دیگری از **vm** باشند، ارتقاء پیدا کنند.

ماشین‌های مجازی که بروی یک هاست قرار می‌گیرند کاملاً از همدیگر مجزا هستند و هیچ تداخل نرم افزاری با یکدیگر ندارند. بدین معنی که شما می‌توانید یک **Database Server** را به همراه یک **Email Server** بروی یک سرور فیزیکی و بروی دو ماشین مجازی و بدون هیچ گونه تداخلی نصب و راه‌اندازی نمایید.

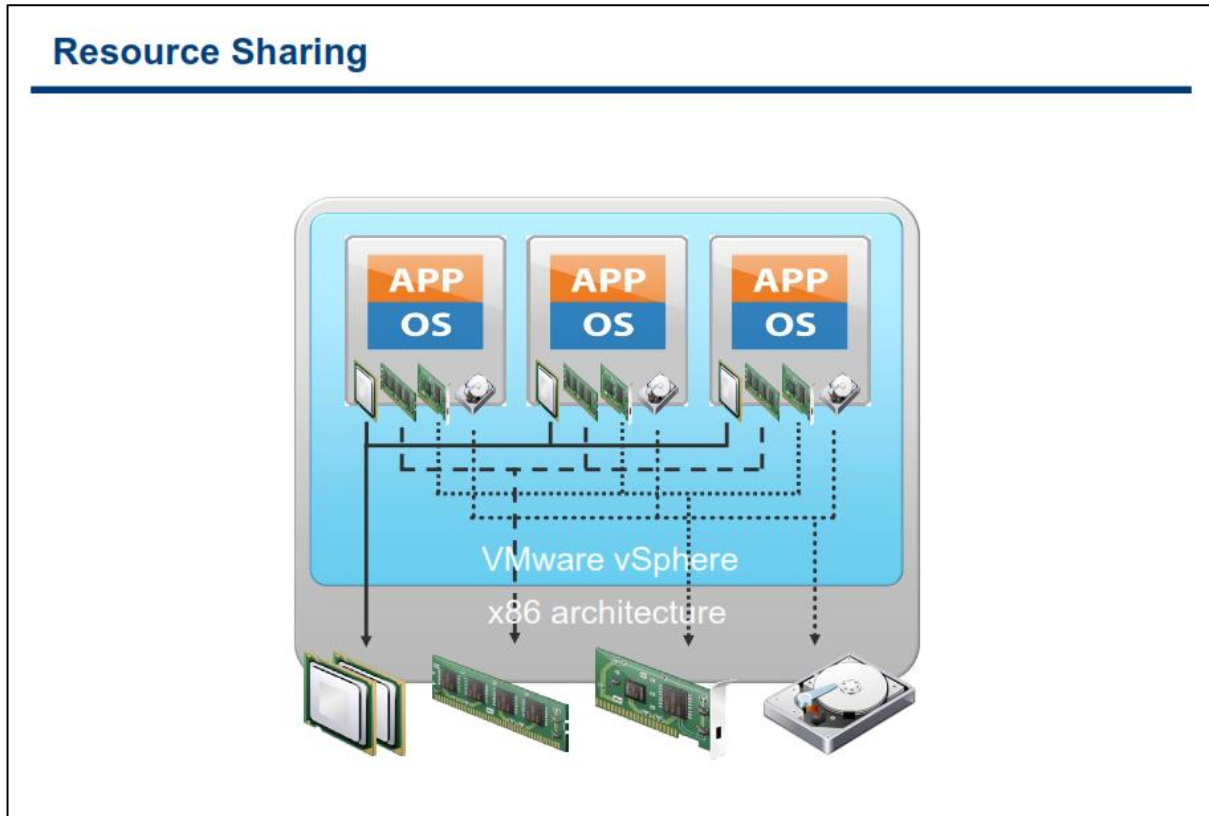
اگر در یک ماشین‌های مجازی کاربری دارای سطح دسترسی **Administrator** در سیستم عامل خود باشد، به هیچ وجه امکان دسترسی به سایر ماشین‌های مجازی را بدون تأیید مدیر سیستم ندارد. بدین ترتیب اگر سیستم عامل یکی از ماشین‌های مجازی دچار مشکل شود، سایر ماشین‌های مجازی موجود بروی هاست به فعالیت خود ادامه می‌دهند. در صورتیکه یک سیستم عامل در یک ماشین مجازی دچار مشکل شود، بروی دسترسی کاربران به سایر ماشین‌های مجازی خللی وارد نمی‌کند و همچنین در عملکرد سایر ماشین‌های مجازی نیز تاثیری نخواهد داشت.



با استفاده از ماشین مجازی (vm) شما می توانید سرورهای فیزیکی خود را یکپارچه کنید و از حداکثر توان سرور های فیزیکی استفاده نمائید. چراکه vm ها مجموعه ای از فایل ها هستند که قابلیت های زیادی را می توان برای آنها فراهم آورد که در هیچ معماری فیزیکی قابل پیاده سازی نیست. به عنوان مثال:

- قابلیت vShield امکانی را فراهم می کند که بتوانید دسترسی vm ها به یکدیگر را در محیط مجازی کنترل کنید. این قابلیت در هیچ زیرساخت فیزیکی وجود ندارد.
- با استفاده از قابلیت هایی همچون **High Availability, Fault Tolerant, Live Migration** شما می توانید زمان سرویس دهی (Up Time) را افزایش داده و زمان Recovery را در مواقع بحرانی و مورد نیاز کاهش دهید.

نکته دیگری که در این رابطه می توان بیان کرد این است که شما می توانید از نرم افزارهای قدیمی و سیستم عامل های قدیمی نیز بروی این پلتفرم مجازی استفاده کنید حتی اگر سخت افزارهای جدید موجود بروی سرور فیزیکی شما، سیستم عامل های قدیمی را پشتیبانی نکنند. به عنوان مثال شما می توانید برای یک سرور فیزیکی HP Proliant DL380 یک ماشین مجازی ایجاد و بروی آن ویندوز ۹۸ نصب نمائید.

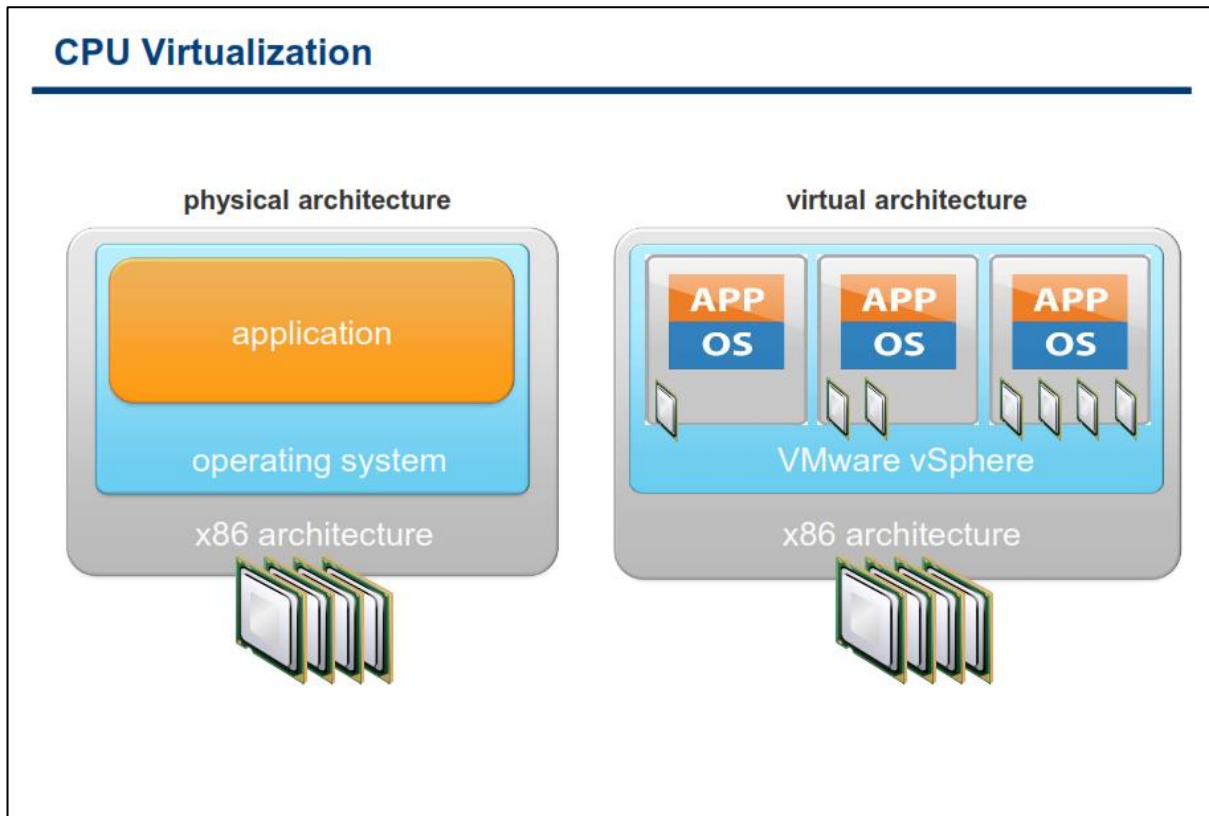


نکته کلیدی که در مجازی سازی وجود دارد این است که منابع فیزیکی به اشتراک گذاشته می شوند. مجازی سازی این امکان را به شما می دهد تا بتوانید چندین **vm** را بروی یک سرور فیزیکی به اجرا در آورید، در واقع هر ماشین مجازی از بخشی از منابع به اشتراک گذاشته شده یک ماشین فیزیکی استفاده می کند. هر **vm** از **CPU** ها بصورت اشتراکی استفاده می کند که البته زمانبندی آنها توسط **Hypervisor** کنترل می شود و همین طور به ماشین های مجازی فضایی از حافظه فیزیکی تخصیص داده شده است که بتوانند از آن استفاده نمایند. سایر منابع نیز بدین صورت کار می کنند یعنی از منابع به اشتراک گذاشته شده استفاده می کنند اما زمانبندی و مدیریت آن به عهده **Hypervisor** می باشد.

زمانیکه چند **vm** بروی **ESXi** اجرا می شوند هر **vm** بخشی از منابع سخت افزاری را به خود اختصاص می دهد. **Hypervisor** مشابه **OS** های سنتی **vm** ها را زمانبندی کرده و حافظه را به آنها تخصیص می دهد. در سیستم عامل های معمولی برنامه ها زمانیکه که اجرا می شوند سیستم عامل به آنها فضایی از حافظه را تخصیص می دهد و همچنین استفاده برنامه ها از **CPU** را زمانبندی می کند. در **Hypervisor** نیز چنین می باشد، در واقع **Hypervisor** به **vm** ها به مانند برنامه های کاربردی نگاه می کند و همانگونه که برنامه ها برای ادامه کار خود نیاز به منابع دارند و سیستم عامل های معمولی آنها را در اختیار برنامه ها قرار می دهند، **Hypervisor** نیز منابع را در اختیار **vm** ها قرار می دهد. این کارها با مکانیزم های کنترلی پیچیده و ماهرانه ای مدیریت می شوند.

با تنظیمات پیش فرض **ESXi**، همه **vm** ها از منابع به اشتراک گذاشته شده به صورت برابر استفاده می کنند بدین معنی که در حالت پیش فرض همه **vm** ها در استفاده از منابع از اولویت یکسانی برخوردار هستند.

## مجازی سازی CPU

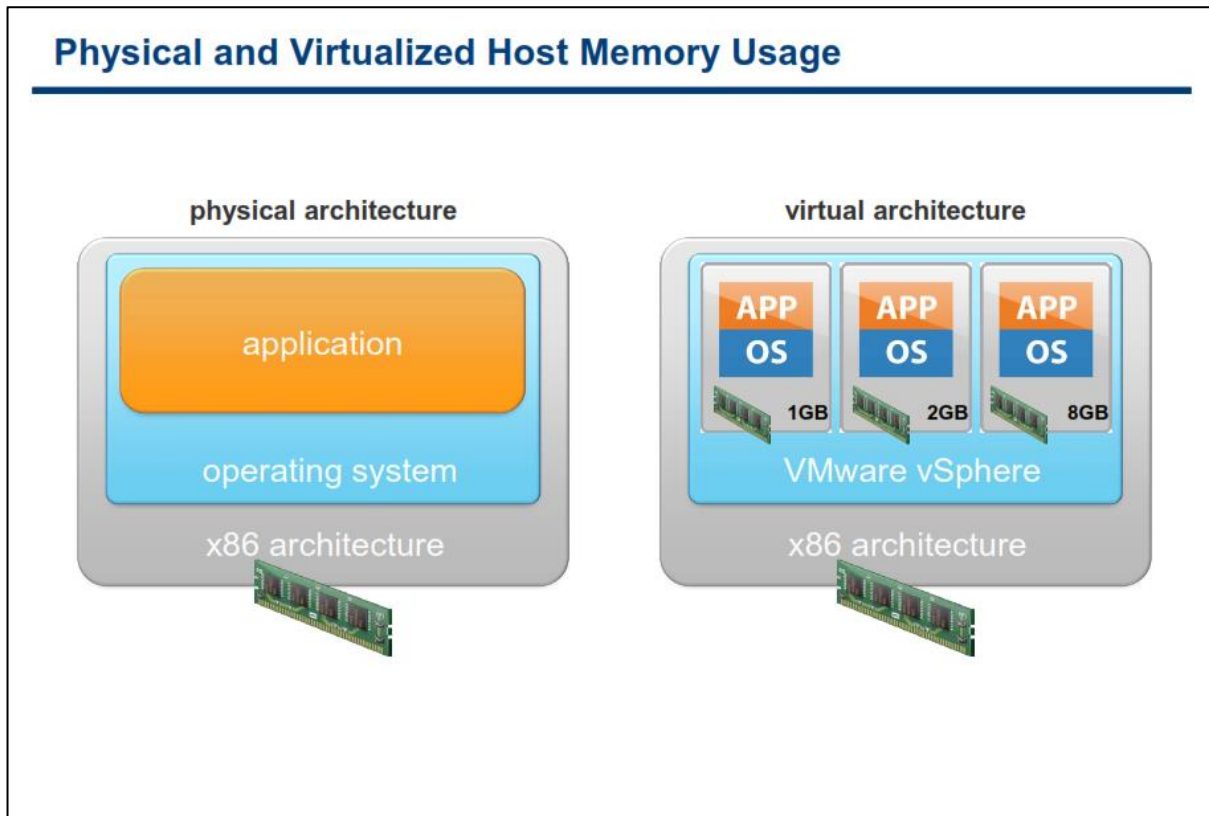


مجازی سازی CPU یک Emulation نیست و شما نباید Emulation را با virtualization اشتباه بگیرید. در Emulation همه کار توسط نرم افزار Emulator انجام می پذیرد. در این حالت سخت افزار ماشین مجازی به صورت کامل شبیه سازی می شود و ماشین های مجازی به صورت کامل می توانند روی (هرنوع معماری) نصب و اجرا گردند. بطور مثال می توان از Cisco Packet Tracer در شبیه سازی روترهای سیسکو نام برد. این نرم افزار بطور کامل عملکرد روترها و سوئیچ های سیسکو را شبیه سازی می کند ولی در مقابل نرم افزار GNS3 ابزاری است که امکان اجرای سیستم عامل IOS سیسکو را بروی معماری x86 فراهم می آورد.

از آنجائیکه مجازی سازی CPU در کارایی بسیار تاثیر دارد لذا دسترسی ماشین های مجازی به CPU به صورت مستقیم انجام می پذیرد و در واقع virtualization یا همان Simulation رخ می دهد. Hypervisor تنها در زمان ایجاد vm دستورات را از طرف vm و با واسطه اجرا می کند.

اما زمانیکه vm ها در ESXi اجرا می شوند ممکن است vm ها برای دریافت منابع CPU با هم رقابت نمایند و زمانیکه مجادله بر سر CPU رخ دهد هاست ESXi پردازنده های فیزیکی را برای تمام vm ها برش زمانی می دهد و همه ماشین های مجازی براساس برش زمانی که ESXi برای آنها در نظر گرفته است می توانند به CPU دسترسی داشته باشند. نکته قابل توجه اینجاست که هر vm از حداکثر تعداد CPU مشخص شده خود می تواند استفاده کند.

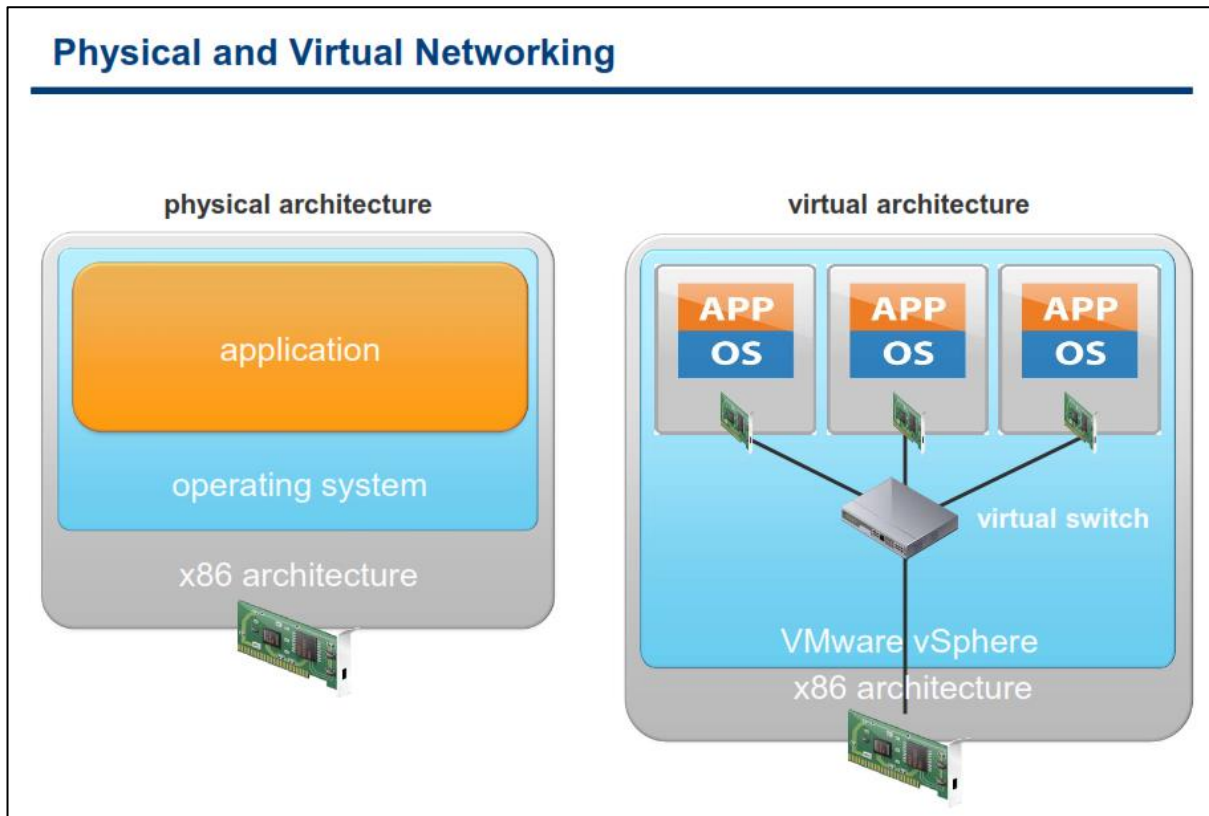
## استفاده از حافظه فیزیکی و مجازی هاست



در محیط های غیر مجازی، OS یا همان سیستم عامل تمام حافظه فیزیکی را به خود اختصاص می دهد. زمانیکه برنامه ای شروع به اجرا شدن می کند از یک واسطی که توسط OS فراهم شده است، برای تخصیص و یا آزادسازی حافظه مجازی در حین اجرا استفاده می کند. حافظه مجازی (Virtual Memory) یک تکنیک مفیدی می باشد که اکثر OS ها از آن بهره می برند و تقریباً همه CPU های مدرن دارای سخت افزاری برای پشتیبانی از حافظه مجازی می باشند. حافظه مجازی یک فضای آدرس دهی مجازی یکپارچه ای را برای نرم افزار ایجاد می کند. در واقع با استفاده از تکنیک لزومی ندارد داده ها به صورت فیزیکی در کنار یکدیگر قرار گیرند و می توان آنها را بروی سطح حافظه توزیع نمود. این تکنیک برای Swap, File Mapping, Process Protection در کامپیوترهای پیشرفته مورد استفاده قرار می گیرد.

اما در محیط مجازی، VMware Hypervisor یک فضای آدرس دهی پشت سر هم و پیوسته را برای vm، زمانیکه شروع بکار می کند ایجاد می کند. این فضای حافظه در زمان ایجاد vm پیکربندی می شود و دارای خصوصیات شبیه به حافظه مجازی می باشد. این پیکربندی به Hypervisor این اجازه را می دهد که چندین vm را بطور همزمان اجرا و از دسترسی حافظه یک vm توسط vm دیگر جلوگیری و حفاظت کند.

## شبکه فیزیکی و مجازی



کامپوننت های شبکه در vmware شامل دو قسمت کلی می باشد: **Virtual Network Adapter** یا کارت شبکه مجازی که هر **vm** می تواند چندین کارت شبکه مجازی داشته باشد و بعدی **Virtual Switch** و یا همان سوئیچ مجازی می باشد که برای برقرار کردن ارتباط **vm** ها با یکدیگر بروی یک **ESXi** و بدون هیچ سخت افزار اضافی استفاده می شود. سوئیچ مجازی همچنین از قابلیت **VLAN** طبق استاندارد های سازگار با تولیدکنندگانی همچون سیسکو پشتیبانی می کند.

تکنولوژی **VMware** این امکان را به شما میدهد که بتوانید از طریق سوئیچ مجازی، **vm** ها را به یکدیگر و یا شبکه های خارجی متصل نمائید. سوئیچ مجازی همانند سایر سوئیچ های حقیقی **Frame** ها را در لایه **Data Link** ارسال می کنند. یک هاست **ESXi** ممکن است شامل چندین سوئیچ مجازی باشد. سوئیچ مجازی از طریق کارت شبکه **Outbound** هاست به شبکه خارجی متصل می شود. سوئیچ مجازی قابلیت یکی کردن چندین کارت شبکه مجازی (**vmnic**) را دارا می باشد و این بسیار شبیه **NIC Teaming** در سرورهای سنتی می باشد که باعث افزایش پهنای باند و ایجاد **Fault Tolerant** و تحمل پذیری خطا می شود. این امکانات در سوئیچ مجازی تعبیه شده است.

سوئیچ مجازی از بسیاری از موارد شبیه سوئیچ فیزیکی مدرن می باشد. همانند یک سوئیچ فیزیکی هر سوئیچ مجازی مجزا می باشد و **IP Table** خودش را دارا می باشد. هر مقصدی که در سوئیچ مجازی در نظر گرفته می شود فقط با پورت هایی در همان سوئیچ مجازی، که فریم متعلق به آنجاست تطابق داده می شود. بدین ترتیب این قابلیت امنیت را در سطح سوئیچ مجازی افزایش داده و کار را برای هکر ها مشکل خواهد کرد.

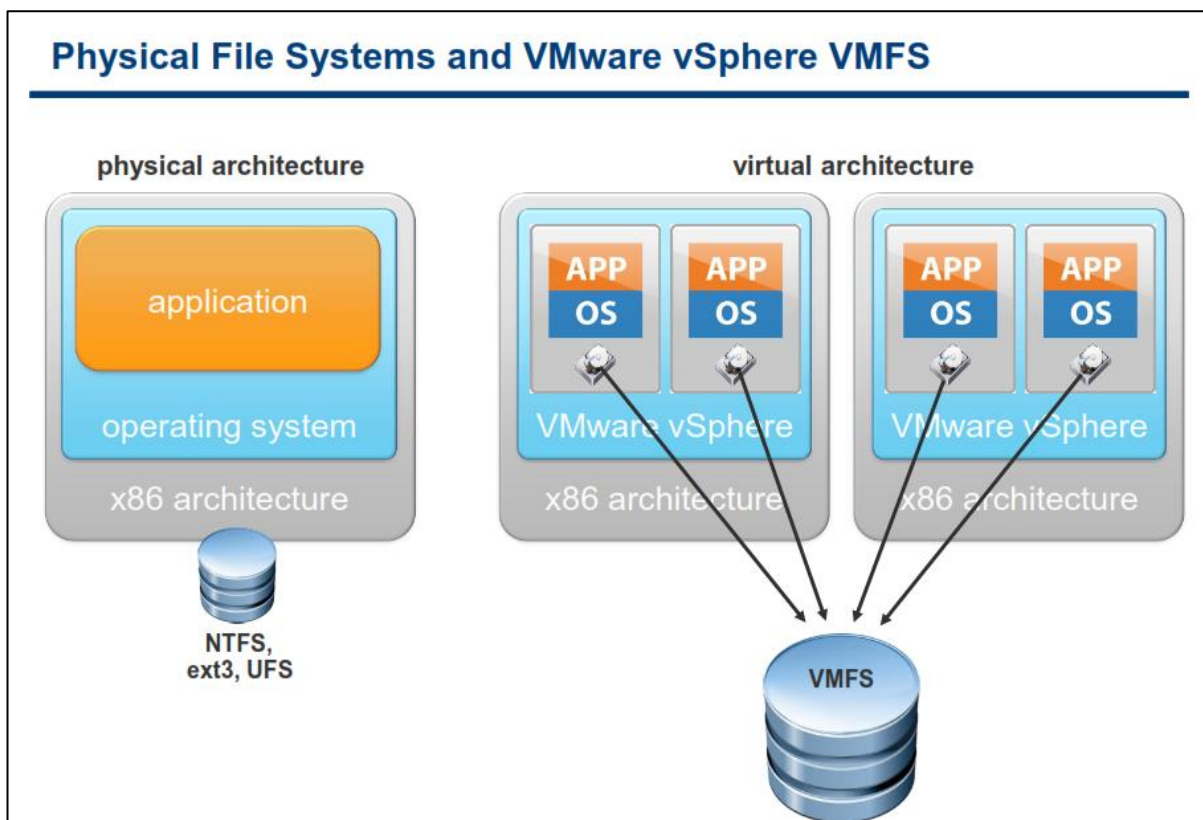
سوئیچ ها همچنین از VLAN در سطح پورت سوئیچ پشتیبانی می کنند و هر پورت می تواند به عنوان Access و یا Trunk پیکربندی شود و دسترسی را برای یک و یا چندین VLAN فراهم نماید.

چندین سوئیچ مجازی نمی توانند بطور داخلی به هم متصل شوند و ترافیک شبکه نمی تواند بطور مستقیم از یک سوئیچ مجازی به سوئیچ مجازی دیگر در همان هاست حرکت کند و منتقل شود. برخلاف سوئیچ فیزیکی سوئیچ مجازی نیاز به قابلیت Spanning Tree Protocol ندارند چراکه در یک توپولوژی شبکه تک سطحی محصور شده اند.

سوئیچ مجازی همه پورت هایی را که شما نیاز دارید را برای شما فراهم می آورند. سوئیچ مجازی به حالت آبخاری نیاز ندارند چراکه سوئیچ مجازی، کارت شبکه فیزیکی را به اشتراک نمی گذارند و بدین ترتیب تاخیر در رسیدن پکت در میان سوئیچ های مجازی رخ نمی دهد.



## فایل سیستم های فیزیکی و VMware vSphere VMFS



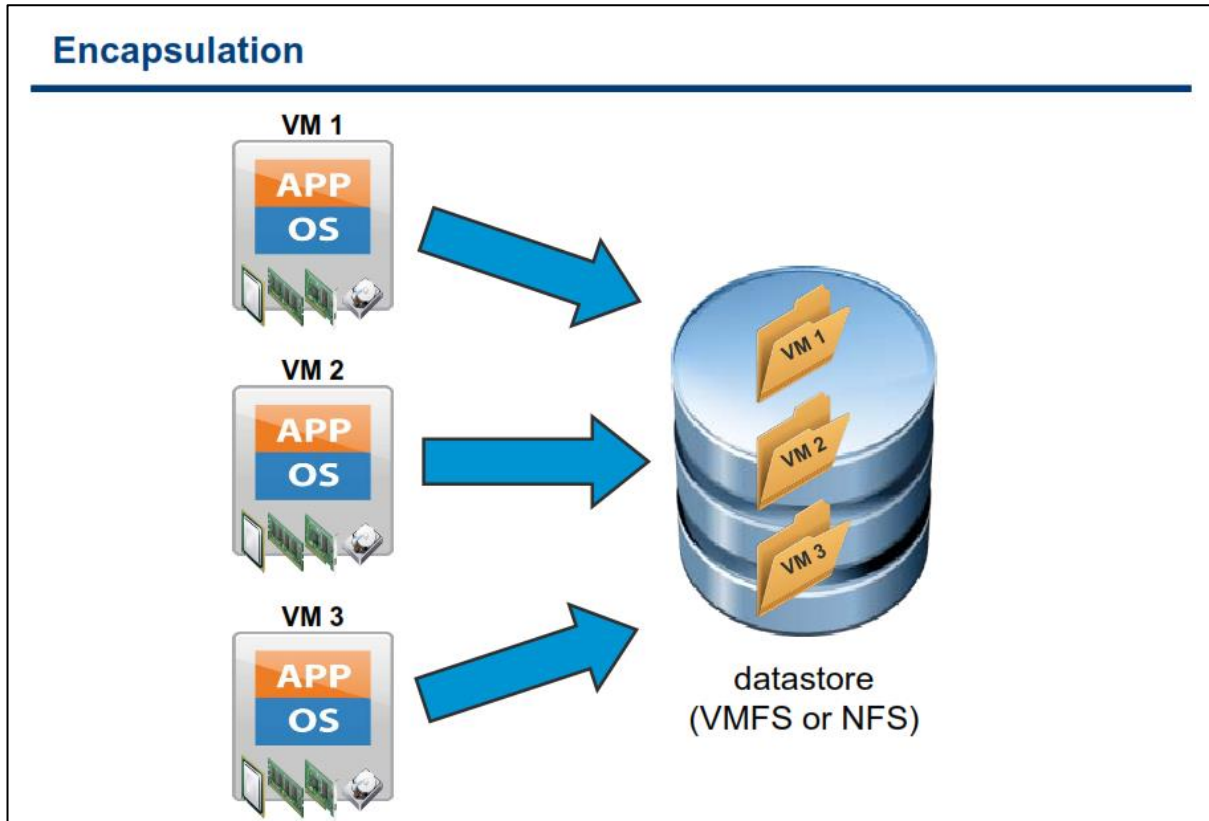
فایل سیستم های معمول تنها به یک سرور اجازه می دهند تا در یک زمان خاص بروی یک فایل عملیات خواندن و نوشتن را انجام دهند. در مقابل فایل سیستم VMware vSphere VMFS یک ساختار توزیع شده از منبع ذخیره سازی را برای شما فراهم می کند و این اجازه را برای شما فراهم می کند که چندین هاست ESXi بتوانند بطور همزمان بروی یک منبع ذخیره سازی و به اشتراک گذاشته شده (Shared Storage) عملیات نوشتن و خواندن را انجام دهند. VMFS برای محیط مجازی ایجاد، طراحی و بهبود یافته است. VMFS یک فایل سیستم کلاستری با کارایی بالا برای vm ها می باشد. VMFS در زمان مشکلات سخت افزاری خیلی سریع و انعطاف پذیر می تواند عمل کند.

VMFS میزان استفاده از یک منبع ذخیره سازی را با چندین vm که دسترسی های به اشتراک گذاشته شده (Shared Access) دارند افزایش می دهد. VMFS همچنین زمینه لازم برای سرویس های زیرساختی توزیع شده را همانند انتقال در حین اجرا vm ها (Live Migration VM), بالانس دینامیک حجم کار از طریق محاسبه منابع در دسترس و راه اندازی خودکار vm ها (Auto Restart) و Fault Tolerant را فراهم می آورد.

VMFS یک واسط (Interface) را برای منابع ذخیره سازی فراهم می کند. بنابراین با استفاده از این واسط پروتکل هایی همچون NAS, iSCSI, Fibre Channel پشتیبانی می شوند و می توان از آنها به عنوان منبع ذخیره سازی برای vm ها استفاده نمود.

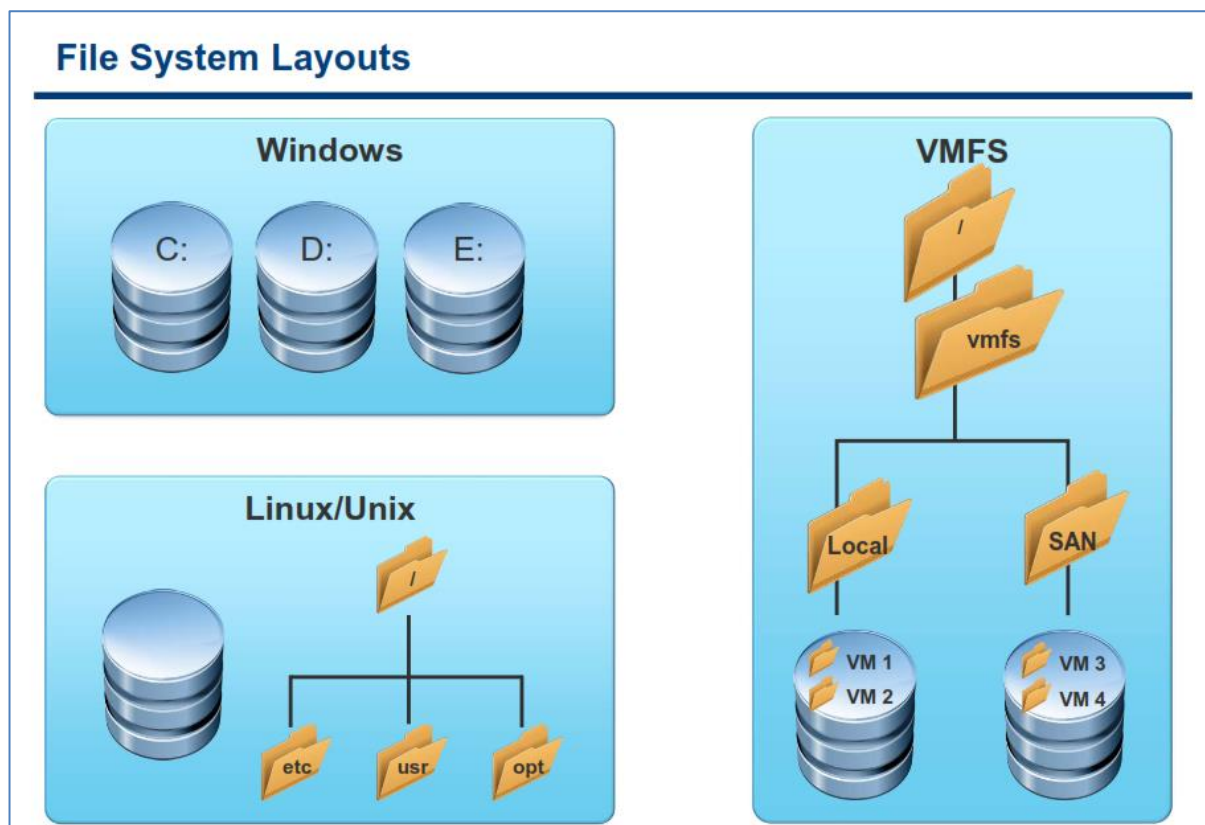
از دیگر امکانات جالب VMFS امکان رشد و توسعه دینامیک و پویای VMFS Datestore با استفاده از متد VMFS Volume Grow می باشد که این قابلیت این امکان را برای شما فراهم می آورد که بتوانید حجم datastore Storage را بدون توقف (DownTime) افزایش دهید.

در مجموع میتوان گفت که VMFS یک فایل سیستم توزیع شده است که قابلیت های منحصر به فردی را فراهم می آورد که هیچ فایل سیستم دیگری چنین قابلیتی را ندارد. VMFS متدهای File Locking توزیع شده ای را برای ارتباط میان vm ها و منبع ذخیره سازی فراهم می کند که شاید نتوان در هیچ فایل سیستم توزیع شده ای آن را یافت. امکان منحصر به فرد دیگری که VMFS فراهم می کند این است که شما می توانید vm ها به راحتی به منبع ذخیره سازی که در حال کار است، متصل نمائید،



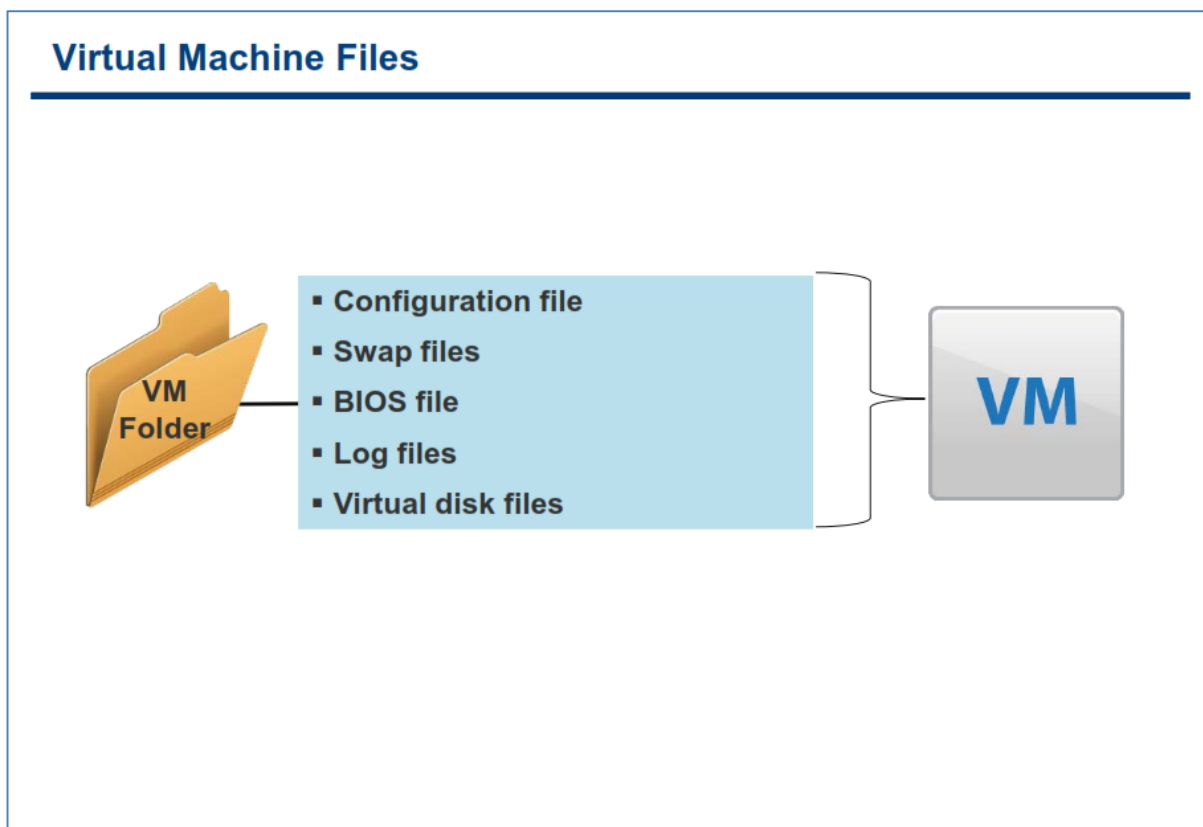
VMFS همه فایل های یک vm را در داخل یک پوشه و یا دایرکتوری کپسوله می کند. همین امر باعث تداوم سرویس دهی و بهبود بازیابی داده ها در مواقع مورد نیاز می شود. این امکان در بسیاری از موارد می تواند راه گشا باشد.

## ساختار فایل سیستم



VMFS برای پشتیبانی از فایل های بزرگ و اجرای دستورات کوتاه (به صورت همزمان) بهینه شده است. یک VMFS datastore از یک ساختاری شبیه به سیستم عامل لینوکس یا یونیکس بهره می برد. هر datastore به یک پوشه و یا دایرکتوری Mount می شود (همانند پوشه Local و SAN در اسلاید بالا) که خود آن نیز شامل تعدادی زیر پوشه و فایل دیگر می باشد. فایل های مربوط به هر vm در یکی از این زیر پوشه ها قرار می گیرد (همانند vm1 , vm2).

## فایل های ماشین مجازی (vm)



**vmx**: فایل پیکربندی ماشین مجازی با پسوند **vmx** شناخته می شود. در این فایل متنی اطلاعاتی همچون **Hardware Configuration , Advanced Power and Resource Settings , VMware Tools Options, Power Management Options** وجود دارد. شما می توانید این فایل را با ویرایشگرهای متنی ساده باز کرده و به صورت دستی تغییرات مورد نظر خود را در آن اعمال نمائید.

**vswp**: فایل **swap** که با پسوند **vswp** شناخته می شود، فقط زمانی ایجاد می شود که هاست تمام حافظه خود را از دست داده باشد (**Out of Memory**). برای مثال شما یک **vm** با **2.0 GB** حافظه ایجاد می کنید ولی در یک زمان تمام حافظه فیزیکی موجود در هاست به اتمام می رسد و شرایطی پیش می آید که تنها **1.5 GB** آن به **vm** اختصاص داده می شود و در نتیجه برای **512** مگابایت **Overflow** رخ می دهد. در این شرایط یک فایل **swap** با حجم **512 MB** ایجاد می شود (در واقع زمانیکه استفاده از **RAM** های تعریف شده بروی هاست بالا می رود و از حد موجود آن می گذرد برای آن مقدار از حافظه ای که وجود ندارد فایل **swap** ایجاد می شود).

**nvram**: فایل **BIOS** که با پسوند **nvram** شناخته می شود برای نگهداری تنظیمات **BIOS** از آن استفاده می شود فرمت این فایل باینری می باشد و اگر پاک شود بصورت خودکار در زمان روشن شدن **vm** با تنظیمات پیش فرض ایجاد می شود.

**log**: فایل **log** که با پسوند **log** شناخته می شود کلیه **log** های مربوط به **vm** در آنها ذخیره می شود و برای عیب یابی از آنها می توان استفاده نمود. این فایل در پوشه **vm** ذخیره می شود و به ازای هر سیکل روشن و خاموش شدن **vm** یک فایل **log** ایجاد می شود. این فایل ها با نام **vmware.log** ذخیره می شوند و در صورتیکه بیش از یک فایل **log** وجود داشته

باشد **log** فایل ها نیز بصورت **vmware-#.log** ذخیره می شوند (# به نشانه عدد می باشد). همیشه ۶ فایل **log** آخر **vm** نگهداری می شود و در صورت خاموش و روشن کردن **vm** قدیمی ترین فایل **log** حذف خواهد شد و فایل **log** جدید ایجاد می شود.

**vmdk**: فایل هارد دیسک مجازی **vm** با پسوند **vmdk** شناخته می شود. همه هارد دیسک های مجازی (**Virtual Disk**) از دو بخش تشکیل شده اند: یکی از آنها که حاوی تمامی اطلاعاتی می باشد که بروی هارد دیسک **vm** شما قرار دارد و اندازه آن برابر با حجم دیسک شما می باشد و دیگری یک فایل متنی کوچک به عنوان توصیف کننده دیسک یا همان **Descriptor File** می باشد. **Descriptor File** حاوی اطلاعاتی در مورد سکتور، سیلندر و نوع آداپتور دیسک می باشد. در برخی از موارد این دو بخش در دو فایل جداگانه قرار می گیرند و در برخی موارد دیگر فایل **Descriptor File** به صورت **embedded** در فایل داده **vmdk** قرار می گیرد. فایل **vmdk** ممکن است در چندین قالب مختلف ایجاد شود:

۱. **vmname.vmdk**: بخش **Descriptor File** و بخش داده دیسک مجازی هر دو می توانند بصورت **embeded** در یک فایل جای گیرند. در این صورت قالب فایل بصورت **vmname.vmdk** می باشد ولی در صورتیکه که **Descriptor File** در یک فایل ایجاد شود این قالب یعنی **vmname.vmdk** را به خود اختصاص می دهد و بخش داده نیز در سایر قالب های زیر قرار می گیرد.
۲. **vmname-flat.vmdk**: در صورتیکه **Descriptor File** در یک فایل جداگانه و در قالب **vmname.vmdk** ایجاد شود دیسک مجازی پیش فرضی که برای **vm** ایجاد می شود با این قالب ایجاد خواهد شد.
۳. **vmname-delta.vmdk**: این نوع قالب **Virtual Disk** در واقع همان **redo-log** می باشد که از زمان ایجاد **Snapshot** ایجاد می شود و تغییرات پس از **Snapshot** بروی این قالب از فایل نوشته می شود.
۴. **vmname-rdm.vmdk**: زمانی که یک **vm** از **Raw Device Mapping** استفاده می کند این قالب از فایل ایجاد می شود که این فایل به عنوان فایل نگاشت برای **RDM-Disk** استفاده می شود.
۵. **diskname-####.vmdk**: همانند قالب **vmname-delta.vmdk** این قالب بصورت اتوماتیک زمانی که شما یک یا چندین **Snapshot** تهیه می کنید ایجاد می شود. این فایل تغییرات ایجاد شده بروی **Virtual Disk** را در حین اجرای **vm** ذخیره می کند. این قالب ممکن است بیش از یک فایل باشد که با پسوند های منحصر به فرد ##### که بصورت اتوماتیک تولید می شود از هم جدا می شوند.
۶. **vmname-s####.vmdk**: در صورتیکه در حین ایجاد **vm** اینگونه تعیین کرده باشید که **Virtual Disk** در چندین فایل با حجم حداکثر ۲ GB قرار گیرد فایل **vmdk** شما با این فرمت ایجاد می شوند. البته در برخی موارد ممکن است این قالب بصورت **vmname-f####.vmdk** نیز وجود داشته باشد.

نکته اینکه در برخی از محصولات قدیمی **vmware** برای ذخیره سازی فایل هارد دیسک مجازی از پسوند **dsk** استفاده می شود.

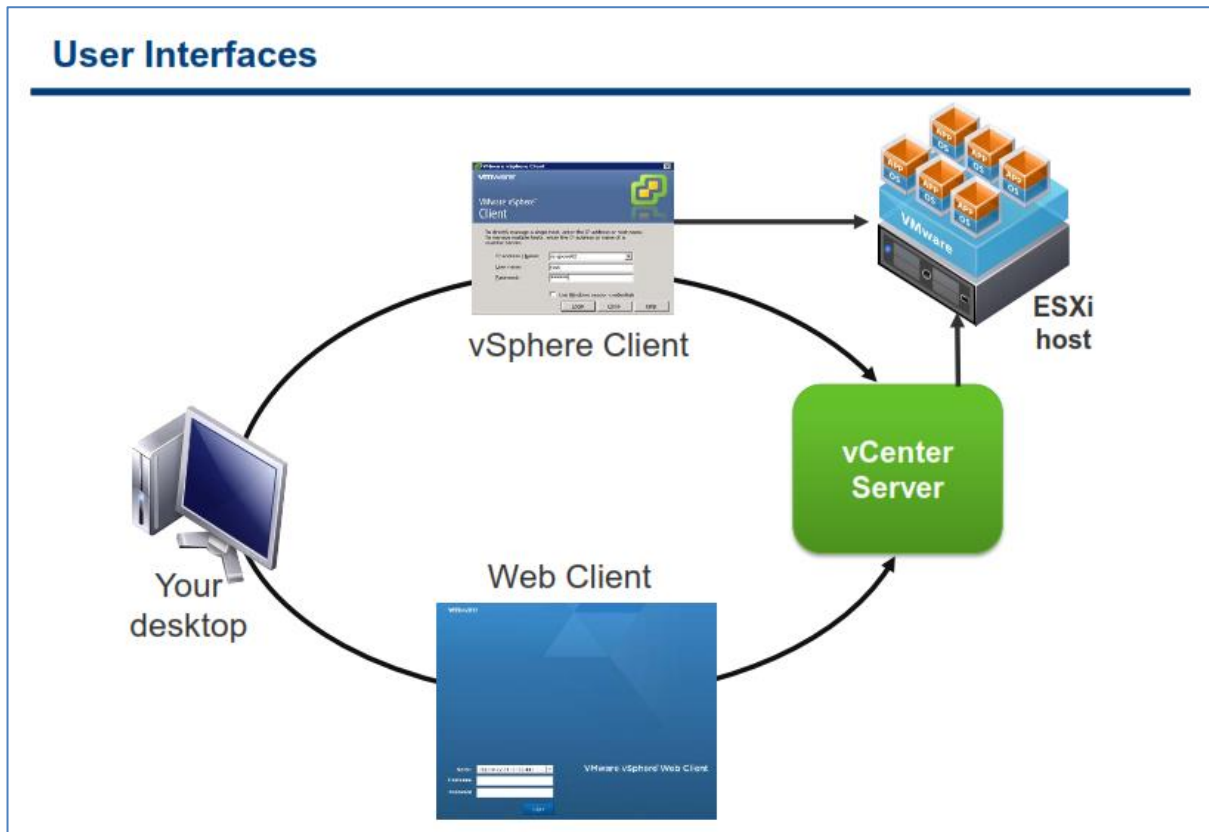


## بخش دوم: واسط کاربری VMware vSphere

بعد از به اتمام رساندن این بخش شما قادر خواهید بود:

- VMware vSphere Client را دانلود و نصب نمائید
- با استفاده از vSphere Client بصورت remote به هاست ESXi متصل شوید
- تنظیمات ESXi را پیکربندی و مشاهده نمائید:
  - پیکربندی حافظه و پردازنده
  - سیستم ESXi logs
  - لایسنس نرم افزار
- مدیریت ESXi از طریق خط فرمان

## واسط کاربری



در vSphere 5.0 دو واسط کاربری وجود دارد که می توانید برای ارتباط با محیط vSphere از آن استفاده نمایید. یکی از این واسط های کاربری vSphere Client نام دارد که برای اتصال به هاست ESXi و vCenter استفاده می شود. واسط کاربری vSphere Client تمامی امکانات مورد نیاز برای پیکربندی و مشاهده تنظیمات یک دیتاسنتر را برای شما فراهم می آورد. نکته جالب اینکه در صورتیکه از طریق نرم افزار vSphere Client به vCenter متصل شوید از امکانات بالاتری برخوردار خواهید بود.

اما واسط کاربری دوم که با نام vSphere Web Client شناخته می شود و با استفاده از Adobe Flex به زیبایی و به صورت تحت وب طراحی شده است و به همین دلیل برای اجرای آن نیازمند نصب پلاگین Adobe Flash بروی مرورگر خود می باشید. نسخه Web Client دارای قابلیت های پائین تری نسبت به نسخه ویندوزی آن یعنی vSphere Client می باشد. نسخه تحت وب این برنامه تنها دارای قابلیت هایی همچون Inventory, VM Deployment و Configuration می باشد که البته این امکانات در نسخه vSphere 5.1 افزایش یافته است. شما می توانید از هر یک از این واسط های کاربری استفاده و یا در صورت لزوم به صورت همزمان از آنها استفاده نمایید.

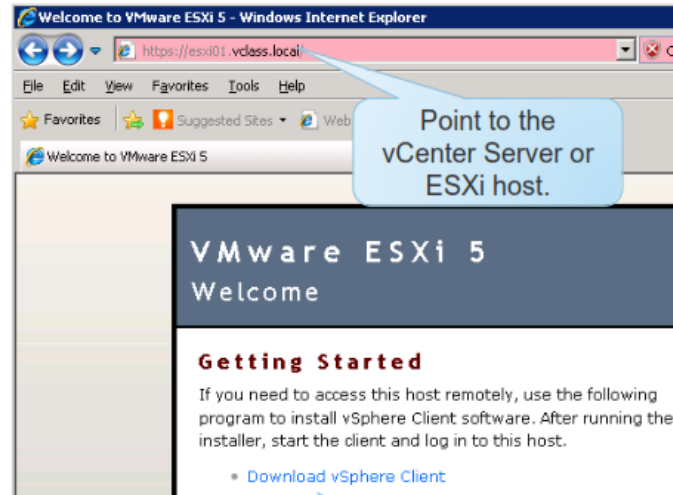
## دانلود کردن vSphere Client

## Downloading the vSphere Client

vSphere Client is an interface used to connect remotely to VMware vCenter Server™ from a Windows system.

You can download the vSphere Client in two ways :

- Use the VMware Infrastructure™ Management Installer.
- Download the client from the vCenter Server system or an ESXi host.



واسط کاربری vSphere Client واسط کاربری کامل تری برای اتصال به vCenter و ESXi می باشد چراکه اکثر امکانات گرافیکی مربوط به برنامه در آن موجود می باشد. علاوه بر آن، vSphere Client کنسولی را برای مدیریت و دسترسی به ماشین مجازی فراهم می آورد.

vSphere Client را به سادگی می توانید از طریق VMware vCenter Installer که بروی DVD این برنامه وجود دارد نصب نمایید. vSphere Client تنها بروی سیستم عامل های ویندوزی نصب می شود. برای آگاهی از اینکه vSphere Client بروی چه نسخه هایی از ویندوز نصب می شود می توانید به مقاله vSphere Compatibility Matrixes در وب سایت <http://www.vmware.com/support/pubs> مراجعه نمایید.

همچنین شما می توانید پس از نصب ESXi و یا vCenter از طریق مرورگر وب به یکی از این دو متصل شوید و از طریق تصویری که اسلاید بالا ملاحظه می کنید برنامه vSphere Client را دانلود و بروی سیستم خود نصب نمایید.

## استفاده از vSphere Client

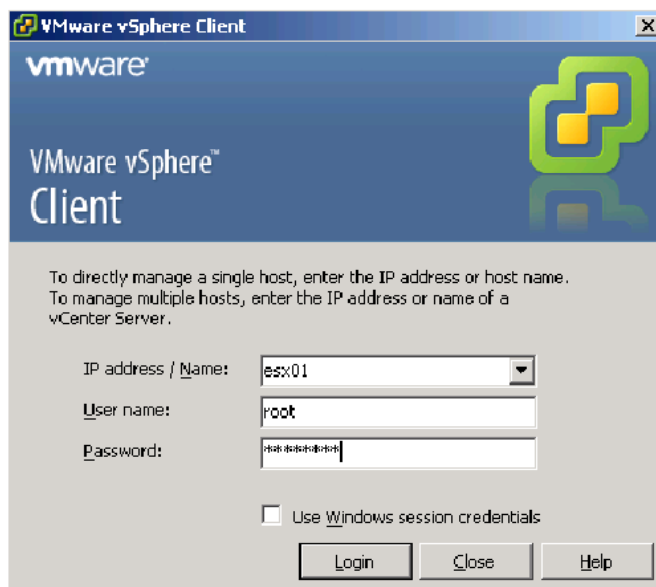
## Using the vSphere Client

The vSphere Client is an interface used to remotely connect to an ESXi host or a vCenter Server from a Windows PC.

On the vSphere Client login screen, enter:

- Host name or IP address of ESXi host or vCenter Server
- User name
- Password for that user

(Optional) Use your Windows session credentials.

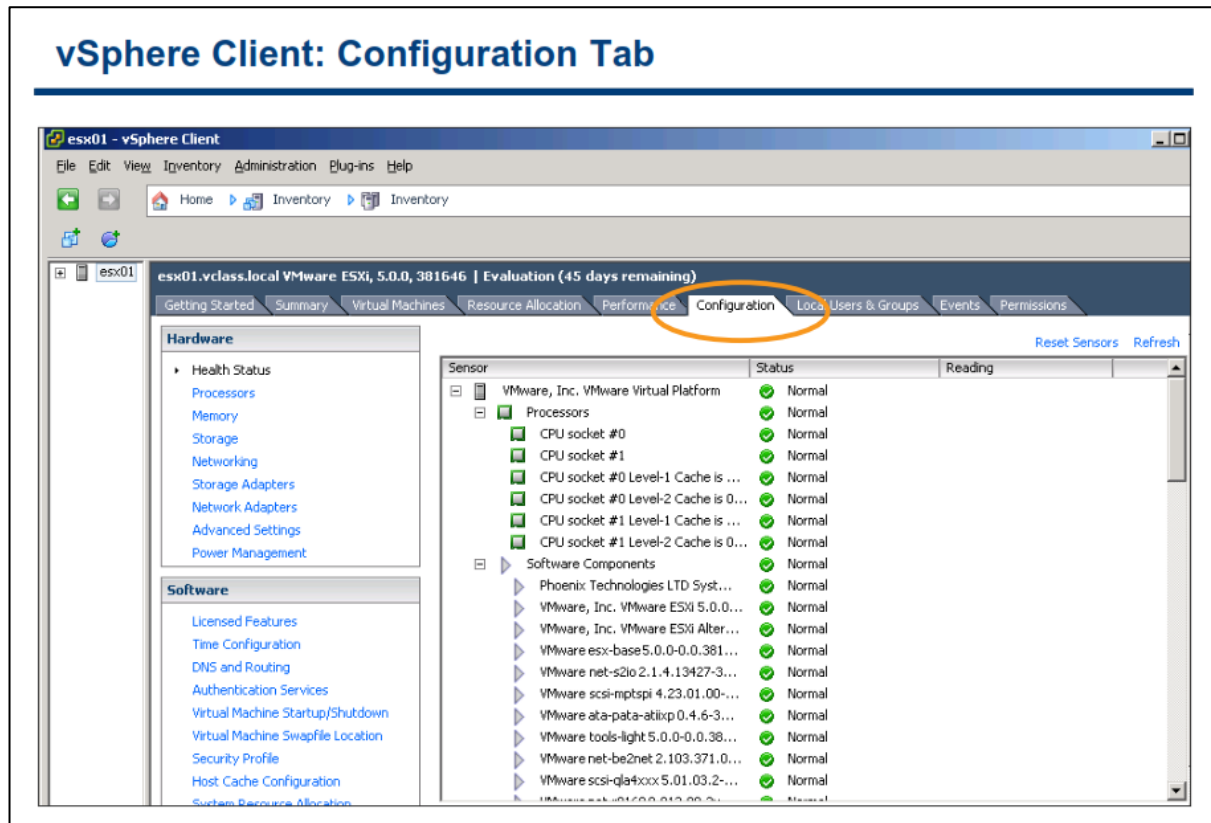


به منظور استفاده از برنامه vSphere Client بروی آیکن آن در دسکتاپ خود کلیک کنید و در پنجره Login نام DNS Host و یا IP سرور ESXi و یا vCenter Server را وارد نمایید و سپس Username , Password دسترسی به آن را وارد نمایید در صورتیکه می خواهید به vCenter متصل شوید شما می توانید از حساب کاربری Local و یا Domain سرور vCenter برای اتصال به آن استفاده نمایید.

همچنین در صورتیکه vSphere Client را بروی سرور vCenter نصب کرده اید می توانید بجای IP و Host name از "localhost" استفاده نمایید و یا اگر می خواهید از Username , Password که با آن Login نموده اید استفاده نمایید گزینه Use Windows Session Credentials را انتخاب کنید تا بدون نیاز به وارد کردن Credential به vCenter و ESXi متصل شوید. مثلا اگر با نام کاربری Administrator وارد سیستم شده اید و می خواهید از همان اطلاعات برای Login کردن استفاده نمایید، این گزینه را انتخاب نمایید.

برای آگاهی از نیازمندیهای سخت افزاری و نرم افزاری vSphere Client می توانید به مقاله ESXi and vCenter Server Setup Guide در وب سایت <http://www.vmware.com/support/pubs> مراجعه نمایید.

## vSphere Client: سربرگ پیکربندی



زمانیکه از طریق vSphere Client به ESXi متصل می شوید در پنل سمت چپ بروی سربرگ Configuration کلیک نمائید بدین ترتیب می توانید تنظیمات سخت افزاری و نرم افزاری هاست ESXi را ببینید.

در این سربرگ شما می توانید پیکربندی Processor, Memory و همچنین پیکربندی Network, Storage مربوط به هاست ESXi را مشاهده و تغییر دهید. علاوه بر موارد فوق اقدامات زیر را نیز می توانید مشاهده و تغییر دهید:

- سریال لایسنس را وارد نمائید
- NTP را پیکربندی نمائید
- DNS Primary, Secondary را پیکربندی نمائید
- Security Profile را پیکربندی نمائید

شما همچنین همانند اسلاید بالا می توانید در این بخش از سلامت هاست خود از طریق Health Status اطلاع پیدا کنید. اگر عملکرد یک کامپوننت به صورت عادی و نرمال باشد، Status آن سبز می شود و در صورتیکه وضعیت آن در آستانه خطر باشد و یا بدرستی کار نکند، آیکن آن به رنگ زرد و یا قرمز نشان داده می شود. معمولاً رنگ زرد به نشانه کاهش کارایی و یا Performance می باشد و رنگ قرمز به نشانه Stop شدن کامپوننت ها و یا اجرا شدن تا سر حد Maximum می باشد (بطور مثال حافظه به میزان ۹۵٪ مورد استفاده قرار گرفته باشد). ولی اگر Status خالی باشد بدین معنی است که سرویس مانیتورینگ نتوانسته وضعیت کامپوننت را تشخیص دهد.

## مشاهده پیکربندی حافظه و پردازنده

## Viewing Processor and Memory Configuration

The image shows two screenshots of the VMware vSphere Configuration console for a virtual machine named 'esx01'. The top screenshot shows the 'Processors' configuration page, and the bottom screenshot shows the 'Memory' configuration page. In both screenshots, the 'Processors' and 'Memory' options in the left-hand navigation pane are circled in orange.

**Processors Configuration:**

General		
Model	Intel(R) Xeon(R) CPU	X5650 @ 2.67GHz
Processor Speed	2.7 GHz	
Processor Sockets	2	
Processor Cores per Socket	1	
Logical Processors	2	
Hyperthreading	N/A	

**System Information:**

Manufacturer	VMware, Inc.	
Model	VMware Virtual Platform	
BIOS Version	6.00	
Release Date	5/5/2009 12:00:00 AM	
Service Tag	VMware-42 3b da 79 49 0a 9c e6-a7 d2 f9 b7 49 2b 16 43	
Asset Tag	No Asset Tag	

**Memory Configuration:**

Physical	
Total	2559.5 MB
System	9.5 MB
Virtual Machines	2550.0 MB

در سربرگ **Configuration** و در بخش **Hardware** شما می توانید بروی **Processors** کلیک نمائید و از مدل پردازنده ، سرعت پردازنده و همچنین تعداد سوکت ها ، هسته ها (Core) و Logical Processor آن اطلاع پیدا نمائید.

همچنین با کلیک بروی **Memory** می توانید اطلاعاتی را درباره حافظه فیزیکی همانند اندازه کل حافظه ، میزان استفاده از حافظه برای کل سیستم و میزان استفاده از حافظه برای vm ها بدست آورید.

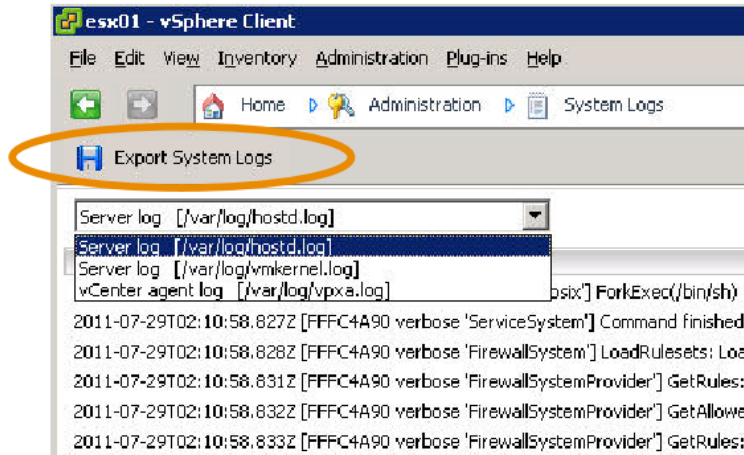
## مشاهده Log های سیستم ESXi

## Viewing ESXi System Logs

Use the vSphere Client to view logs.

Export system logs to an archive file.

- Send to VMware Support.



Log گزارشی است از رویدادها و اتفاقاتی که بروی یک سیستم روی می دهد. برای مشاهده Log های سیستم ESXi می بایست در منوی vSphere Client به بخش View->Administration->System Logs مراجعه نمائید.

ESXi دارای فایل های Log با نام های hostd.log و vmkernal.log می باشد. این Log ها شامل کلیه رویدادها و رخدادها از زمانیکه سیستم ESXi روشن می شود می باشد. این Log ها برای بخش پشتیبانی VMware و همچنین متخصصانی که قصد عیب یابی سیستم را دارند بسیار مفید می باشند. زمانیکه شما بروی یک مشکل با تیم پشتیبانی صحبت می کنید، شما می بایست فایل های Log هاست ESXi را برای تیم پشتیبانی فراهم نمائید.

vSphere Client به شما اجازه می دهد که بتوانید Log های سیستم را فشرده و و بروی دسکتاپ خود ذخیره نمائید. شما می توانید این فایل های Log را برای عیب یابی به بخش پشتیبانی VMware ارسال نمائید. برای ذخیره کردن Log ها بروی دسکتاپ خود می توانید همانند اسلاید بالا بروی Export System Logs کلیک نمائید.

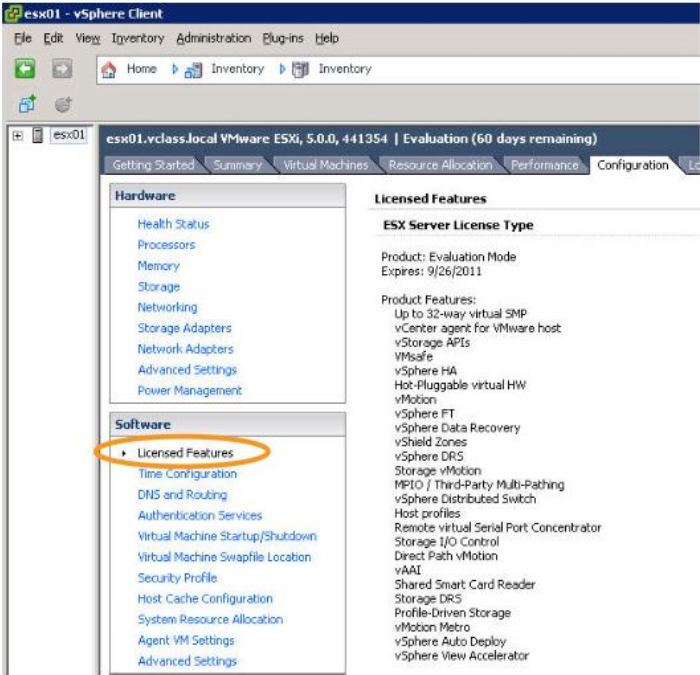
در vSphere 5.0 چندین بهبود برای Log گیری در سیستم ESXi افزوده شده است. همه Log ها از پروتکل Syslog پشتیبانی می نمایند. Syslog پروتکلی است که به یک دستگاه اجازه ارسال Log های خود را میدهد. بدین ترتیب Log ها می توانند بروی سیستم ESXi و یا بروی یک سرور دیگر در شبکه (Remote Server) ذخیره شوند و یا اینکه از هر دو قابلیت استفاده شود. شما بروی Remote Server می توانید Log های چندین هاست ESXi را ذخیره نمائید. پیام های Log را می توان با استفاده از پروتکل های امنی همچون SSL به Remote Server های دیگری انتقال داد.

vSphere Syslog Listener به عنوان یک plug-in اختیاری بروی vCenter Server ویندوزی قرار می گیرد و از آن می توان برای Log گیری از این برنامه استفاده نمود و از طرف دیگر در vCenter Virtual Appliance عملیات Log گیری با استفاده از Syslog داخلی این Appliance انجام می شود. با استفاده از vSphere 5.0 می توانید پیام های Log را از منابع مختلف به مکان دیگری انتقال دهید که البته این نیز می بایست پیکربندی شود. همچنین شما می توانید از طریق خط فرمان (CLI) هاست ESXi عملیات Log گیری را پیکربندی نمائید.



## مشاهده قابلیت های دارای لایسنس

## Viewing Licensed Features



**Before purchasing licenses, you can install ESXi in evaluation mode:**

- Intended for demonstration and evaluation purposes
- Allows software to be completely operational immediately after installation
- Does not require any licensing configuration
- Provides full functionality for 60 days

برای وارد کردن لایسنس هاست ESXi می بایست بروی لینک **Licensed Features** در سربرگ **Configuration** کلیک نمائید. در پنجره **Licensed Features** شما می توانید لایسنس های نرم افزار را مشاهده و از قابلیت هایی که برای این نرم افزار فعال شده است مطلع شوید.

قبل از خرید و فعال سازی لایسنس های ESXi، شما می توانید نرم افزار را در حالت آزمایشی نصب نمائید. بطور پیش فرض نرم افزار پس از نصب در حالت آزمایشی قرار می گیرد. در طول دوره آزمایشی شما می توانید از تمامی قابلیت های این نرم افزار که در پنجره **Licensed Features** نمایش داده شده است استفاده نمائید.

مدت زمان استفاده آزمایشی از نرم افزار، از تاریخی که آن را نصب می نمائید به مدت ۶۰ روز می باشد. در طول این مدت، مکرراً زمان انقضای حالت آزمایشی به شما اطلاع رسانی می شود. این مدت زمان ۶۰ روزه قابل تمدید نیست و امکان متوقف کردن آن نیز وجود ندارد. بعد از انقضای حالت آزمایشی، شما دیگر قادر به انجام بسیاری از کارها در **vCenter** و **ESXi** و **Server** نمی باشید. برای مثال شما دیگر قادر نخواهید بود یک ماشین مجازی را روشن و یا خاموش نمائید. همچنین تمامی هاست های ESXi از **vCenter Server** جدا و قطع می شوند. برای ادامه استفاده از تمامی قابلیت های ESXi و **vCenter Server** شما می بایست یک لایسنس تهیه نمائید.

همان طور که در اسلاید بالا نمایش داده شده است، هاست ESXi در حالت آزمایشی به اجرا در آمده است. اما در صورتیکه می خواهید لایسنس نرم افزار را وارد نمائید بروی گزینه **Edit** که در قسمت بالای سمت راست پنجره **Licensed Features** وجود دارد، کلیک نمائید. سپس گزینه **Assign License** را انتخاب و لایسنس جدید را وارد نمائید.

## مدیریت ESXi از طریق خط فرمان

**Managing ESXi from the Command Prompt**

To perform management tasks from a remote command prompt, use:

- VMware vSphere Command-Line Interface (vCLI):
  - Set of commands run from a remote Linux or Windows system and executed on an ESXi host
  - Packaged as an application
- VMware vSphere Management Assistant (vMA):
  - Platform for running a variety of toolkits:
    - vCLI
    - vSphere SDK for Perl
    - vSphere API
  - Packaged as a virtual appliance based on Linux
- VMware vSphere PowerCLI:
  - Automation tool for administering a vSphere environment
  - Distributed as a snap-in to Windows PowerShell

برای مدیریت هاست ESXi از طریق خط فرمان می توانید از ابزارهای (vSphere Command Line Interface) vCLI ، (vSphere Management Assistant) vMA و vSphere PowerCLI استفاده نمایید.

ابزار vCLI مجموعه ای از دستورات را در قالب یک نرم افزار کاربردی برای شما فراهم می آورد که می توانید با استفاده از آن هاست ESXi را مدیریت کنید. این ابزار می تواند مستقیماً به ESXi و یا vCenter متصل شود و برای اتصال به vCenter از User ها ، Role های تعریف شده در vCenter استفاده می نماید. شما با استفاده از vCLI می توانید از طریق سیستم عامل لینوکس و یا ویندوز دستورات خود را بروی ESXi به صورت remote اجرا نمایید.

vMA نیز یک پلتفرمی برای اجرای دستورات و اسکریپت های می باشد که شما آن توسعه داده اید. vMA باید بروی یک هاست که از ماشین مجازی ۶۴ بیتی پشتیبانی می کند اجرا گردد. vMA به عنوان یک Virtual Appliance و به صورت built-in و بروی Redhat Linux توسعه داده شده است. (یک Virtual Appliance مجموعه ای از ماشین های مجازی می باشد که در داخل یک پکیج قرار گرفته اند و به صورت یکپارچه مدیریت و بروزرسانی می شوند). این پلتفرم ابزارهایی همچون vCLI ، vSphere SDK for Perl و vSphere API را فراهم می کند. vSphere SDK for Perl یک واسط اسکریپت نویسی ساده ای را برای vSphere API فراهم می آورد. توسعه دهندگان و اسکریپت نویسان می توانند با آپجکت های vSphere API از طریق vSphere SDK ارتباط برقرار کنند. برای کسب اطلاعات بیشتر می توانید به سایت [develop.vmware.com](http://develop.vmware.com) مراجعه کنید.

شما می توانید با استفاده از یک مرورگر به هاست ESXi متصل شده و ابزارهای vCLI و vMA را از طریق لینک هایی که در این صفحه قرار گرفته است، دانلود نمایید.

PowerCLI نیز ابزاری برای خودکار سازی کار ها در یک محیط vSphere می باشد. این ابزار به عنوان یک Snap-in به Windows Powershell افزوده شده است. PowerCLI یک ابزار خط فرمانی قدرتمند می باشد که با استفاده از آن می توانید همه ویژگی های vSphere Management شامل vm, Storage, Networking را خودکار نمایید. PowerCLI شامل بیش از ۲۰۰ دستور و صفحه راهنما می باشد. برای دانلود PowerCLI می توانید به وب سایت <http://www.vmware.com/go/powercli> مراجعه نمایید.

## کارگاه شماره یک:

در این کارگاه آموزشی، شما نحوه نصب و راه اندازی نرم افزارهای vSphere Client و vSphere Web Client را خواهید آموخت که شامل موارد زیر می باشد:

۱. نصب نرم افزار vSphere Client
۲. نصب نرم افزار vSphere Web Client

## بخش سوم: بررسی اجمالی ESXi

بعد از به اتمام رساندن این بخش شما قادر خواهید بود:

- معماری ESXi را تشریح نمایید
- تنظیمات ESXi را همچون موارد زیر پیکربندی نمایید:
  - شبکه
  - لایسنس
  - کلاینت NTP
  - DNS & Routing
  - پروفایل امنیتی
- بهترین روش را برای مدیریت کاربران ESXi تشریح نمایید

## VMware ESXi

## VMware ESXi

- Available for purchase with vSphere 5 or a free version can be downloaded
- High-security
  - Memory Hardening
  - Kernel Module Integrity
  - Trusted Platform Module
- Small disk footprint
- Can be installed on hard disks, SAN LUNs, USB devices, SD cards, or directly into memory

شما می توانید نسخه رایگان ESXi که vSphere Hypervisor نامیده می شود را از وب سایت [www.vmware.com](http://www.vmware.com) دانلود و یا از نسخه لایسنس دار آن استفاده نمایید. ESXi را می توانید بروی Flash ,CD-ROM , Hard Disk ,SD Card نصب و یا حتی آن را را بروی هاست های بدون دیسک نصب نمایید (مستقیماً بروی حافظه از طریق امکانی بنام Auto Deploy نصب می گردد).

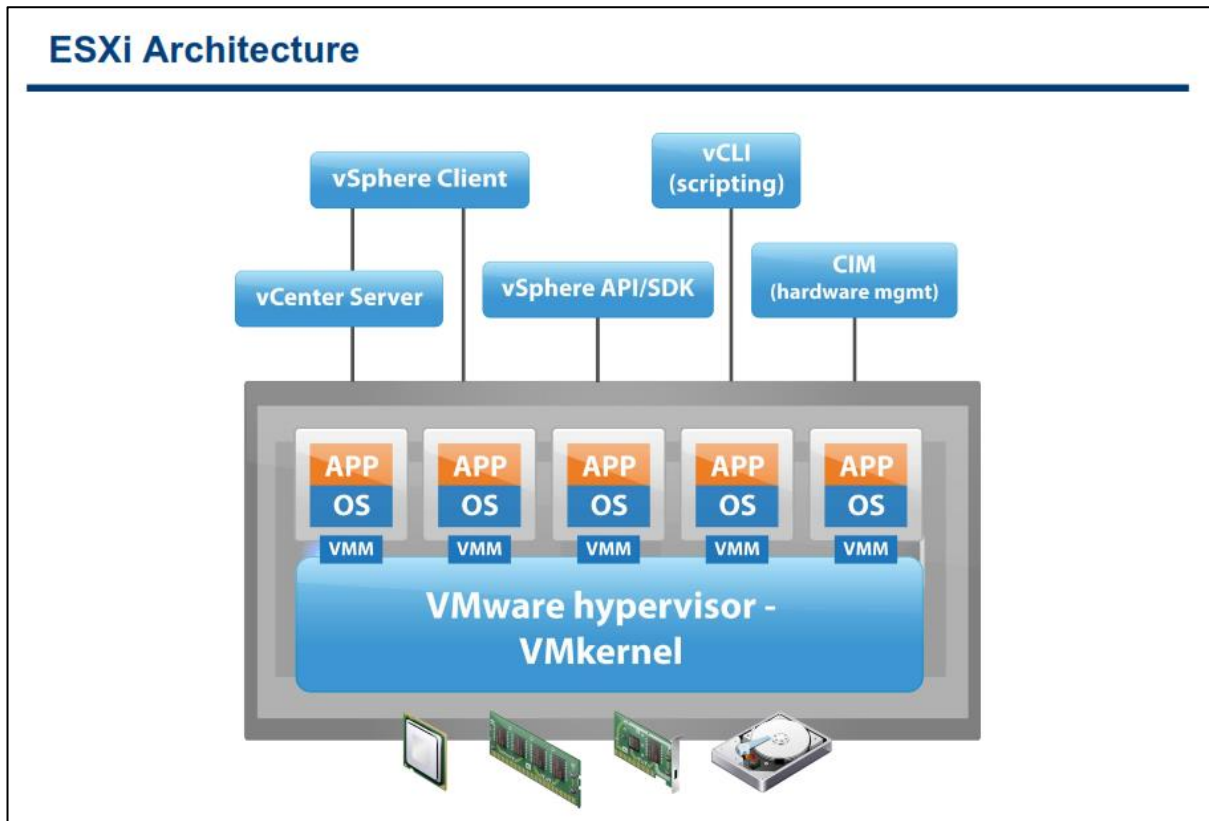
ESXi فضایی کمتر از ۷۰ مگابایت را اشغال می کند که همین مسئله باعث افزایش امنیت و ضریب اطمینان آن شده است.

بعضی از بهبود های که در ESXi 5.0 به وجود آمده عبارتند از :

- پشتیبانی از حداکثر ۵۱۲ ماشین مجازی و تعداد CPU ۲۰۴۸ مجازی به ازای هر هاست
- پشتیبانی از سرورهای فیزیکی با ۱۶۰ CPU Logical و ۲ ترابایت حافظه (RAM)
- پشتیبانی ESXi از هاست هایی که دارای UEFI Boot می باشند. (UEFI یک واسط نرم افزاری بین سیستم عامل و میان افزار (Firmware) سخت افزار است که قبل از بوت سیستم قرار می گیرد. UEFI در سیستم های امروزی جایگزین BIOS شده است).

علاوه بر موارد ذکر شده، ESXi از قابلیت های امنیتی بیشتری بهره برده که از جمله آن می توان به موارد زیر اشاره نمود:

۱. **Memory Hardening**: کرنل ESXi، برنامه های کاربردی کاربر و همچنین کامپوننت های اجرایی (همانند درایور ها و فایل های کتابخانه ای) را در یک آدرس تصادفی و غیر قابل پیش بینی قرار می دهد. بدین ترتیب آدرس دهی حافظه را دشوار می کند تا توسط هکر ها قابل دسترسی و پیش بینی نباشد.
۲. **Kernel Module Integrity**: با استفاده از امضای دیجیتال این اطمینان را در یکپارچه سازی و احراز هویت ماژول ها، درایور ها و برنامه هایی که بوسیله VMKernel بارگذاری شده اند، را ایجاد می کند.
۳. **Trusted Platform Module**: یک قطعه سخت افزاری می باشد که فرایند بوت شدن و لود شدن درایور ها را از لحاظ معتبر بودن چک و بررسی می کند. بدین ترتیب اگر فایل های مخربی جایگزین فایل های بوت سیستم عامل شوند از بوت شدن آن سیستم عامل با فایل های مخرب جلوگیری و به مدیر سیستم اعلام می گردد.



ESXi یک لایه مجازی سازی را برای به اشتراک گذاری منابع سیستم (همچون حافظه، CPU، کارت شبکه و هارد دیسک) به ماشین های مجازی فراهم می کند. ESXi صرفاً یک Hypervisor (مدیر ماشین های مجازی) است که یک بستری را برای دینامیک کردن و اتوماتیک کردن دیتاسنتر شما ایجاد می کند.

ساختار ESXi بدین گونه می باشد که تمامی نرم افزارهای موجود بروی یک vm، بدون دسترسی مستقیم به سخت افزار فیزیکی و یا اصلی اجرا می شوند. ESXi Hypervisor بنام VMkernel نیز شناخته می شود. VMkernel درخواست ها را از ماشین مجازی برای دریافت منبع (Network, Disk, Memory, ...) از Virtual Machine Monitor (VMM) دریافت می کند و پس از آن به سخت افزار اصلی ارائه می دهد و در نهایت دوباره از طریق همین VMM به ماشین مجازی پاسخ می دهد. VMM در هر vm به منظور ارائه Virtual Hardware به vm و دریافت و ارسال درخواست ها فعالیت می کند.

به هاست ESXi می توانید از طریق چندین رابط کاربری دسترسی پیدا کنید:

۱. vSphere Client
۲. vCLI
۳. vSphere API
۴. (CIM) Common Information Model



CIM یک استاندارد مدیریتی است که توسط DMTF یا Distributed Management Task Force ارائه می شود. اکثر اطلاعاتی که از طریق CIM دریافت می شود را می توانید از طریق vSphere API نیز بدست آورید. اما با این حال برخی از اطلاعات فقط از طریق CIM دریافت می شود بطور مثال وضعیت سلامت (Status Health) سخت افزار هاست ESXi.

ESXi از پردازنده اینتل Xeon و بالاتر و همچنین پردازنده AMD پشتیبانی می کند. ESXi شامل یک VMKernel که با ساختار ۶۴ بیتی است. هاست هایی که دارای پردازنده ۳۲ بیتی هستند از طریق ESXi پشتیبانی نمی شود. ولی ESXi از Guest ها و یا همان ماشین های مجازی با سیستم عامل ۳۲ و ۶۴ بیتی پشتیبانی می کند.

برای اطلاعات بیشتر در مورد سخت افزارهای و Guest OS پشتیبانی شده توسط ESXi به سایت [www.vmware.com](http://www.vmware.com) مراجعه کنید (Hardware Compatibility List).

## Configuring ESXi

The Direct Console User Interface (DCUI) is similar to the BIOS of a computer with a keyboard-only user interface.

```

VMware ESXi 5.0.0 (VMKernel Release Build 381646)
VMware, Inc. VMware Virtual Platform
2 x Intel(R) Xeon(R) CPU X5570 @ 2.93GHz
2.5 GiB Memory

Download tools to manage this host from:
http://esx01/
http://172.20.10.51/ (STATIC)

<F2> Customize System/View Logs
<F12> Shut Down/Restart
  
```

شما می توانید از طریق رابط کاربری مستقیم هاست ESXi که بنام DCUI (Direct Console User Interface) شناخته می شود تنظیمات اولیه ESXi را پیکربندی نمایید. برای وارد شدن به تنظیمات می بایست کلید F2 را بزیند. شما از طریق این کنسول تنها می توانید تنظیمات و پیکربندی های سطح پائین را بروی ESXi انجام دهید.

## پیکربندی ESXi: دسترسی root

## Configuring ESXi: root Access

The DCUI allows an administrator to:

- Set a root password (complex passwords only)
- Enable or disable lockdown mode (to prevent user access to host as root)



نام کاربری مدیر سیستم هاست ESXi کلمه "root" می باشد و به صورت پیش فرض کلمه عبور آن null و یا خالی می باشد. اگر شما هیچ کلمه عبوری را برای نام کاربری root تعیین ننمائید، نمی توانید از طریق رابط های کاربری vSphere Client به هاست متصل شوید. برای تعیین کلمه عبور گزینه Configuration Password را انتخاب و سپس کلمه عبور خود را وارد نمائید. در این بخش توجه داشته باشید که می بایست کلمه عبور خود را به صورت Complex (یعنی در کلمه عبور خود می بایست حداقل یک حرف بزرگ و حداقل یک حرف کوچک و حداقل یک عدد وجود داشته باشد) و با حداقل ۸ کاراکتر وارد نمائید.

اگر گزینه LockDown Mode را فعال نمائید تمام دسترسی های راه دور (Remote) با نام کاربری root به هاست ESXi مسدود می شود و تنها از طریق vSphere vCenter و یا DCUI می توانید به ESXi دسترسی داشته باشید. یعنی دیگر از طریق ابزارهای vSphere Client, vSphere API, vCLI, PowerCLI نمی توان به هاست ESXi بطور مستقیم متصل شد.

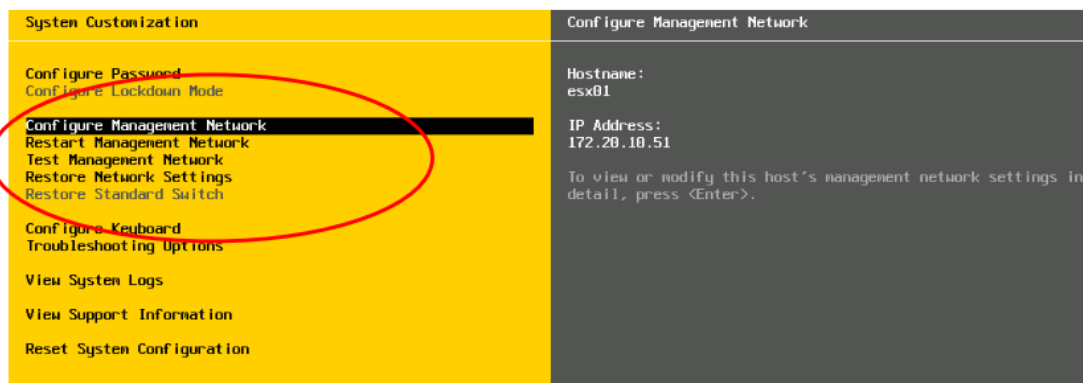
نکته: در صورتی که هر دو گزینه Support Mode و Lockdown Mode را فعال نمائید امکان دسترسی تیم پشتیبانی فراهم نخواهد بود چراکه گزینه Lockdown Mode دارای اولویت بالاتری می باشد.

## پیکربندی ESXi: مدیریت شبکه

## Configuring ESXi: Management Network

The DCUI allows you to modify network settings:

- Host name
- IP configuration (IP address, subnet mask, default gateway)
- DNS servers



شما می بایست IP Address هاست ESXi را پیش از هر کار دیگری پیکربندی نمایید. بطور پیش فرض هاست ESXi بر روی حالت DHCP Client قرار دارد و IP Address را از DHCP Server دریافت می کند. برای تغییر و پیکربندی تنظیمات اولیه شبکه شما می توانید هم از DCUI و هم از vSphere Client استفاده نمایید.

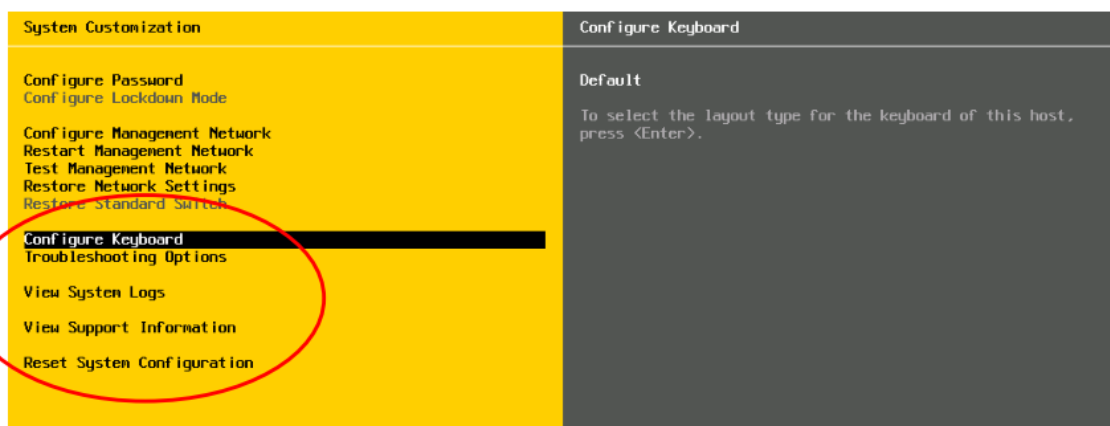
از طریق کنسول DCUI همانند اسلاید بالا شما می توانید Host Name و IP Address (شامل Subnet و IP Address و Mask, Default Gateway می باشد) و DNS Server را پیکربندی نمایید. همچنین شما می توانید آن کارت شبکه فیزیکی هاست را که برای مدیریت و اتصال به ESXi استفاده می شود را تغییر دهید و یا اینکه تنظیمات مربوط به VLAN را انجام دهید. از دیگر اقداماتی که در این بخش می توانید انجام دهید استفاده از تنظیمات IP v.6 و همچنین پیکربندی DNS Suffix شبکه محلی می باشد (بطور مثال yepco.local).

## پیکربندی ESXi: سایر تنظیمات

## Configuring ESXi: Other Settings

The DCUI allows an administrator to:

- Configure keyboard layout
- View support information
- View system logs
- Enable troubleshooting services, when required



با استفاده از DCUI شما می توانید Keyboard Layout را که بصورت پیش فرض بروی English تنظیم شده است را تغییر دهید. همچنین می توانید اطلاعات مربوط به بخش پشتیبانی vmware را در منوی View Support Information (همانند شماره سریال لایسنس ESXi) مشاهده نمایید و یا اینکه Log های مربوط به هاست را در منوی View System Logs مشاهده نمایید.

گزینه Troubleshooting Options نیز سرویس عیب یابی را فعال و غیر فعال می کند. به صورت پیش فرض این گزینه غیر فعال است. سرویس عیب یابی شامل موارد زیر می باشد:

۱. Local Tech Support Mode: این گزینه برای عیب یابی مشکلات به صورت محلی و مستقیم می باشد.
۲. Remote Tech Support Mode Service: این گزینه نیز برای عیب یابی مشکلات از راه دور و به صورت Remote می باشد. یعنی با استفاده از پروتکل SSH و نرم افزاری همچون Putty، کارشناسان vmware می توانند به هاست شما متصل شده و اقدام به عیب یابی نمایند.

توصیه می شود Troubleshooting Options را تنها در مواردی که نیاز به پشتیبانی است فعال نمایید و در غیر این صورت به دلایل امنیتی آن را غیر فعال نمایید.

گزینه Reset System Configuration نیز به شما اجازه می دهد تنظیمات سیستم را به حالت پیش فرض برگردانید و همه Package ها و Extension هایی که بروی این هاست نصب شده است را حذف نماید.

## ESXi به عنوان یک کلاینت NTP

## ESXi as an NTP Client

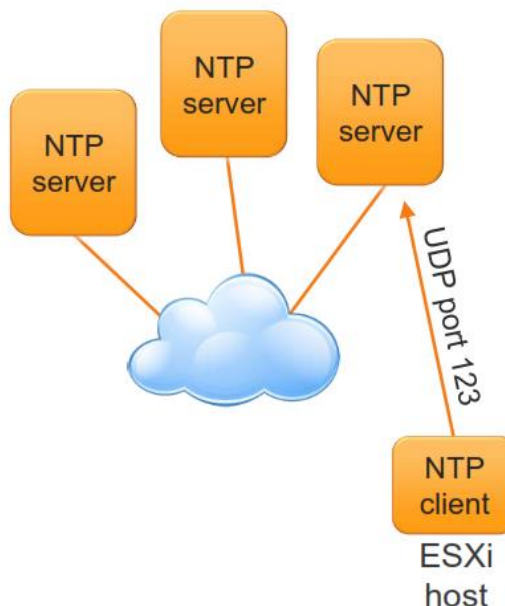
Network Time Protocol (NTP) is a client-server protocol used to synchronize a computer's clock to a time reference.

## NTP is important:

- For accurate performance graphs
- For accurate time stamps in log messages
- So that virtual machines have a source to synchronize with

## An ESXi host can be configured as an NTP client.

- It can synchronize time with an NTP server on the Internet or your corporate NTP server.



NTP یک پروتکل استاندارد اینترنت می باشد که از آن برای یکسان سازی ساعت در شبکه استفاده می شود. استفاده از NTP به دلایل زیر از اهمیت بالایی برخوردار است:

۱. اطلاعات مرتبط با کارایی و Performance سرور ها می بایست بدرستی تفسیر و نمایش داده شوند.
۲. زمان دقیق رخداد ها و رویداد ها می بایست به درستی در پیام های Log نمایش داده شود.
۳. vm ها می تواند زمان خود را با هاست ESXi یکسان سازی نماید. یکسان سازی زمان برای سرویس ها و برنامه هایی که بروی vm اجرا می شوند بسیار مهم و مفید می باشد. مانند Database هایی که بروی vm ها در حال اجرا می باشد.

NTP یک پروتکل کلاینت - سروری می باشد و زمانی که شما ESXi را به عنوان یک کلاینت NTP پیکربندی می کنید، هاست ESXi زمان و ساعت خود را با NTP Server یکسان می کند. NTP سرور می تواند در شبکه داخلی شما باشد و یا اینکه بروی اینترنت باشد. پورت NTP Server به صورت پیش فرض ۱۲۳ UDP می باشد. ESXi از نسخه ۳ و ۴ NTP پشتیبانی می کند.

برای کسب اطلاعات بیشتر درباره NTP می توانید به [www.ntp.org](http://www.ntp.org) مراجعه نمایید.

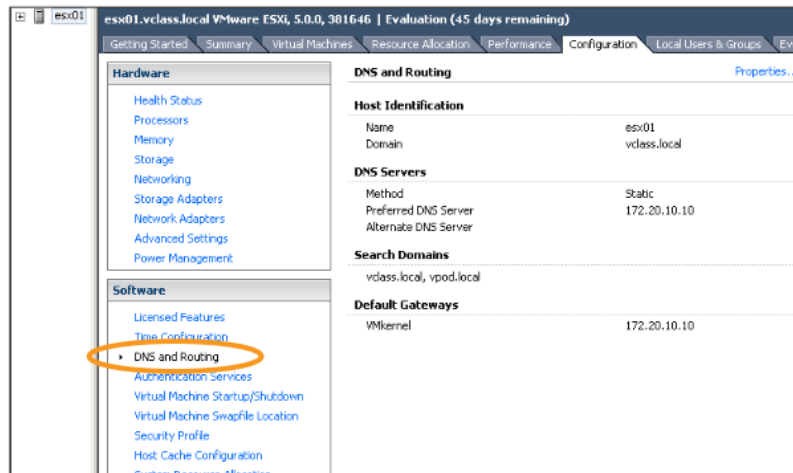
برای تنظیم کردن NTP می بایست با ابزار vSphere Client به ESXi متصل شوید و در بخش Configuration گزینه Time Configuration را انتخاب و NTP سرور خود را وارد نمایید و آدرسی همانند [ir.pool.ntp.org](http://ir.pool.ntp.org) را وارد نمایید. این آدرس معتبر است و از همین آدرس می توانید برای دیتاسنتر خود استفاده نمایید.

## تنظیمات شبکه: DNS &amp; Routing

## Network Settings: DNS and Routing

The DNS and Routing link allows you to change:

- Host name and domain
- DNS server addresses and search domains
- Default VMkernel gateway



در بخش DNS and Routing هاست ESXi شما می توانید تغییرات زیر را اعمال نمایید:

- نام هاست و دامنه را تنظیم نمایید
- DNS Primary and Secondary را تنظیم نمایید
- Default Gateway که همان VMKernel را تنظیم نمایید

برای انجام این پیکربندی می بایست بروی سربرگ Configuration هاست ESXi کلیک نمایید و سپس گزینه DNS and Routing را انتخاب و بروی لینک Properties کلیک نمایید.

## تنظیمات دسترسی از راه دور: پروفایل امنیتی

**Remote Access Settings: Security Profile****On ESXi hosts:**

- Remote clients are prevented from accessing services on the host.
- Local clients are prevented from accessing services on remote hosts.
- Unless configured otherwise, daemons will start and stop with the ESXi host:
  - For example, DCUI or NTP

به صورت پیش فرض ESXi از دسترسی Remote User ها به سرویس های هاست جلوگیری می کند و از طرف دیگر نیز از دسترسی Local User به سرویس های راه دور جلوگیری می کند. ولی با این حال برخی از پورت های هاست باز می باشد. ESXi دارای یک Firewall داخلی ضعیف می باشد که شما می توانید از طریق سربرگ Configuration هاست، گزینه Security Profile را انتخاب و این فایروال را پیکربندی نمائید و برخی از دسترسی ها را ایجاد و یا حذف نمائید.

برای ایجاد دسترسی به یک کلاینت و یا سرویس شما می بایست CheckBox مورد نظر را انتخاب و یا برای حذف دسترسی به یک کلاینت و یا سرویس، CheckBox مورد نظر را از حالت انتخاب خارج نمائید.



## بهترین روش مدیریت کاربران ESXi

**ESXi User Account Best Practices**

**You should implement the following user account best practices:**

- Strictly control root privileges to the ESXi host.
- Use the vSphere Client to manage the ESXi host.
- Ideally, use vCenter Server – and thus vCenter Server user accounts – to manage hosts.

بروی هاست ESXi، کاربر root قدرتمندترین و نامحدودترین کاربر بروی سیستم می باشد و قادر به اجرای همه دستورات و فایل ها می باشد. ایمن نگه داشتن این حساب کاربری از مهم ترین گام های برقراری امنیت به شمار می رود.

زمانیکه شما از vCenter Server برای مدیریت هاست ها استفاده می کنید، می بایست از طریق واسط کاربری vSphere Client به vCenter Server وارد شوید و از آنجا هاست ها را مدیریت نمایید. اتصال مستقیم به هاست ESXi از طریق vSphere Client می بایست صرفاً در موارد اجباری صورت پذیرد. برای مثال زمانیکه vCenter Server دچار مشکل شده است، این امکان می بایست وجود داشته باشد تا شما بتوانید به هاست ESXi از طریق vCLI و یا vSphere Client متصل شوید.

شما می توانید تمامی هاست های خود را از طریق vCenter Server و به صورت متمرکز مدیریت نمایید. این کار باعث مدیریت بهتر دسترسی ها و کاربران می گردد. برای اتصال به vCenter شما می توانید هم از Local Account و هم از Domain Account استفاده نمایید. توصیه می شود از Domain Account برای مدیریت هاست ESXi استفاده نمایید.

## کارگاه شماره دو:

در این کارگاه شما خواهید توانست هاست ESXi خود را پیکربندی نمائید که شامل موارد زیر می باشد:

۱. اتصال به هاست ESXi با vSphere Client
۲. مشاهده Hardware Configuration هاست
۳. پیکربندی DNS and Routing بروی یک هاست
۴. پیکربندی هاست ESXi به عنوان یک NTP Client

## فصل دوم: ماشین های مجازی



این فصل شامل بخش های زیر می گردد:

۱. مفاهیم ماشین مجازی
۲. ایجاد یک ماشین مجازی

اهمیت این فصل:

یک ماشین مجازی مجموعه ای از سخت افزارهای مجازی می باشد که بروی آن سیستم عامل های پشتیبانی شده به همراه نرم افزارهای آن در حال اجرا هستند. شما می توانید ماشین مجازی را به چندین روش ایجاد نمائید. انتخاب یک روش صحیح می تواند به شما در کاهش زمان و بهبود فرایند راه اندازی مدیریت شده ماشین های مجازی کمک می کند.

## بخش اول: مفاهیم ماشین مجازی

بعد از به اتمام رساندن این بخش شما قادر خواهید بود:

- مفهوم ماشین مجازی را تشریح نمائید
- فایل های یک ماشین مجازی را مشاهده و تشریح کنید
- سخت افزارهای یک ماشین مجازی را لیست نمائید

## ماشین مجازی چیست؟

### What Is a Virtual Machine?

#### A virtual machine is:

- A set of virtual hardware on which a supported guest operating system and its applications run
- A set of discrete files



virtual machine

#### A virtual machine's configuration file describes the virtual machine's configuration, including its virtual hardware.

- Avoid using special characters and spaces in the virtual machine's name.

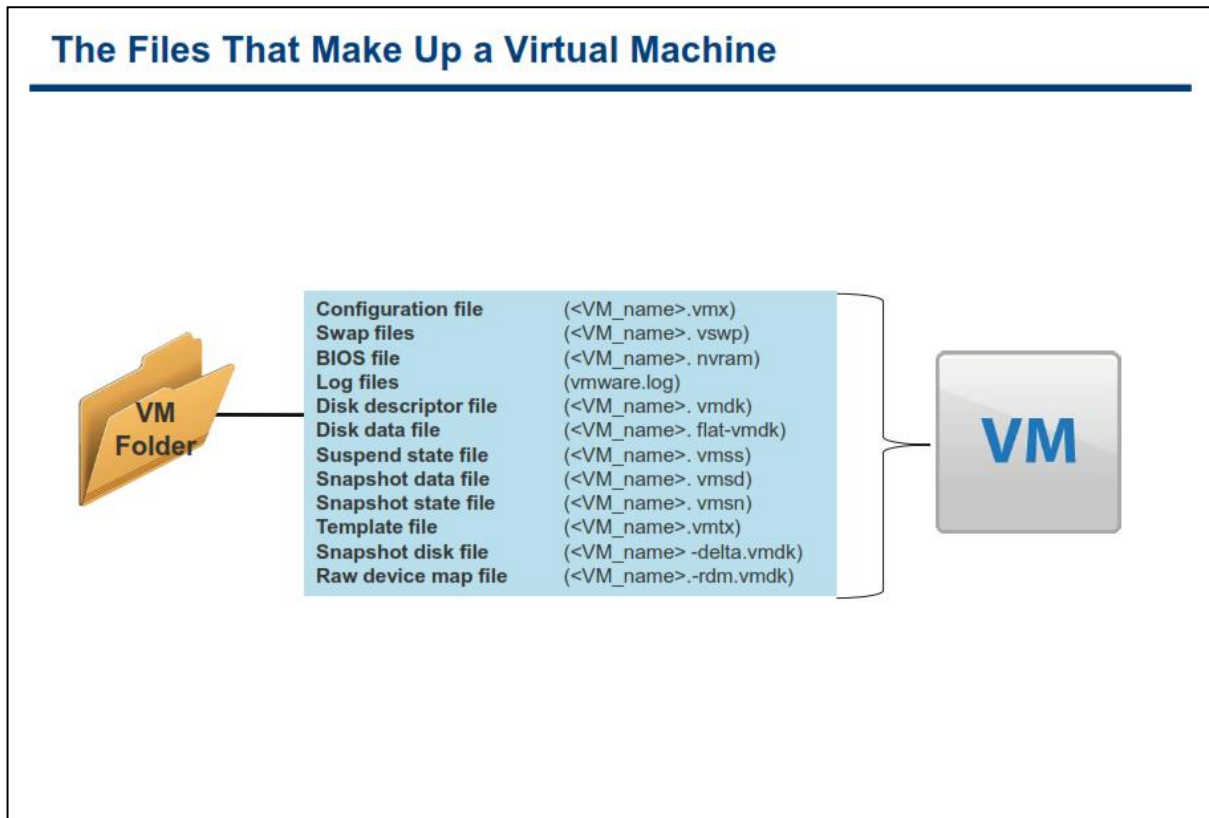
#### MyVM.vmx

```
...
guestOS = "winnetstandard"
...
displayName = "MyVM"
(etc.)
```

یک ماشین مجازی مجموعه ای از سخت افزارهای مجازی می باشد که بروی آن سیستم عامل های پشتیبانی شده به همراه نرم افزارهای کاربردی آن در حال اجرا هستند. در واقع ماشین مجازی مجموعه ای از فایل های ناپیوسته می باشند. فایل پیکربندی هر ماشین مجازی، تنظیمات و پیکربندی های آن را تشریح می کنند که این پیکربندی ها و تنظیمات شامل مواردی همچون تعداد CPU و میزان حافظه، هارد دیسک، کارت شبکه و غیره می باشد. تمامی این پیکربندی ها درون یک فایل متنی با پسوند vmx تعریف می شود.

زمانیکه قصد دارید یک vm را نام گذاری نمایید، توصیه می شود از کارکترهای خاص (همانند @#!%&\* و فاصله (Space)) در نام گذاری vm ها استفاده نکنید و از آن پرهیز کنید چراکه از نام vm برای ساخت سایر فایل های یک vm استفاده می شود و احتمال بروز مشکل در مواردی وجود دارد.

## فایل های که یک ماشین مجازی ایجاد می کند



در اسلاید بالا برخی از فایل های سازنده یک ماشین مجازی نمایش داده شده است. بجز فایل های Log، نام هر یک از فایل ها با نامی که برای ماشین مجازی تعیین کرده اید (<VM\_name>) شروع می شوند. یک vm و یا ماشین مجازی شامل فایل های زیر می باشد (البته این موارد در فصل قبلی بیان شد اما بدلیل اهمیت آن دوباره آن می پردازیم):

- یک فایل پیکربندی با پسوند vmx
- یک یا چندین فایل دیسک مجازی (Virtual Disk files). اولین دیسک مجازی بنام <VM\_name.vmdk> و پس از آن <VM\_name>-flat.vmdk نام گذاری می گردد.
- یک فایل حاوی تنظیمات BIOS ماشین مجازی با پسوند nvram
- فایل Log جاری ماشین مجازی که با پسوند و نام (vmware.log) شناخته می شود و مجموعه ای از فایل هایی که برای نگهداری فایل های Log قدیمی تر استفاده می شود با پسوند و نام (vmware-#.log) شناخته می شوند. بدین ترتیب در صورتیکه بیش از یک فایل log وجود داشته باشد log فایل ها نیز به صورت vmware-#.log ذخیره می شوند (# به نشانه عدد می باشد). همیشه شش Log فایل آخر vm نگهداری می شود و در صورت خاموش شدن و روشن کردن vm قدیمی ترین log فایل حذف خواهد شد و فایل log جدید ایجاد می شود.
- فایل swap که با پسوند vswp شناخته می شود برای نگهداری حافظه swap در زمانیکه حافظه تعیین شده برای ماشین مجازی به اتمام میرسد و پس از سرریز حافظه بخشی از اطلاعات حافظه به این فایل انتقال داده می شود.
- فایل تشریح کننده Snapshot که با پسوند vmsd شناخته می شود. اگر ماشین مجازی دارای Snapshot نباشد محتوای این فایل خالی خواهد بود.

اگر ماشین مجازی به یک **Template** و یا قالب تبدیل شود (این مبحث در فصل های بعدی تشریح میشود)، فایل پیکربندی **Template** ماشین مجازی با پسوند (vmtx) جایگزین فایل پیکربندی **vm** با پسوند **vmx** می شود.

اگر ماشین مجازی بیش یک دیسک مجازی داشته باشد، فایل های بعدی آن با نام های **<vm\_name>\_#.vmdk** و یا **<vm\_name>\_#-flat.vmdk** نام گذاری می گردد. اگر **disk** ها بیش از یک فایل باشند به ترتیب دارای شماره (#) می شوند همانند **vm\_name\_#.vmdk** و یا **vm\_name\_#-flat.vmdk**. بطور مثال اگر نام یک ماشین مجازی **Test01** باشد و دارای دو دیسک مجازی باشد، این ماشین مجازی دارای فایل هایی با نام های **Test01.vmdk** , **Test01-flat.vmdk** , **Test01\_1.vmdk** , **Test01\_1-flat.vmdk** می باشد.

همچنین ماشین های مجازی می توانند دارای فایل های دیگری نیز باشند، برای مثال اگر یک ماشین مجازی دارای یک یا چندین **Snapshot** باشد و یا دارای **RDM (Raw Device Mapping)** باشد فایل های دیگری نیز به آن اضافه خواهد شد. از طرفی دیگر هر ماشین مجازی دارای فایل های **Lock** با پسوند **lck** می باشند. همچنین اگر شما از ابزارهایی همچون **VMware Data Recovery** برای تهیه نسخه پشتیبان از **vm** ها استفاده نمائید فایل های برای پیگیری تغییرات در فایل ها ایجاد می شوند.

## مشاهده فایل های ماشین مجازی

### Displaying a Virtual Machine's Files

Click on a VM. On the Summary tab, right-click the datastore on the Resources pane.

Click Browse Datastore to browse its files.

Storage	Status	Drive Type
VMFS-02	Normal	Non-SSD

Name	Size	Provisioned Size	Type	Path
Greg-01-1.vmx	2.69 KB		Virtual Machine	[datastore1] Greg-01-1
Greg-01-1.vmdk	1,154,048.00 KB	2,097,152.00 KB	Virtual Disk	[datastore1] Greg-01-1
vmware.log	141.75 KB		Virtual Machine ...	[datastore1] Greg-01-1
Greg-01-1.nvram	8.48 KB		Non-volatile me...	[datastore1] Greg-01-1
Greg-01-1.vmx	0.26 KB		File	[datastore1] Greg-01-1
Greg-01-1.vmsd	0.00 KB		File	[datastore1] Greg-01-1
vmx-Greg-01-1-2191458621-1...	46,080.00 KB		File	[datastore1] Greg-01-1
Greg-01-1-829f013d.vswp	393,216.00 KB		File	[datastore1] Greg-01-1

فایل های ماشین مجازی یا بروی **VMware VMFS Datastore** و یا بروی **NFS Datastore** ذخیره می گردند. شما با استفاده از واسط کاربری **VMware vSphere Client** می توانید فایل های ماشین مجازی را مشاهده نمائید البته در صورتیکه بدانید ماشین مجازی بروی کدام **Datastore** قرار گرفته است. (**Datastore**: محلی انتزاعی برای ذخیره سازی ماشین های مجازی می باشد)

برای یافتن **Datastore** که ماشین مجازی بروی آن ذخیره شده است شما می بایست **vm** خود را در بخش **Inventory and view** انتخاب و سپس به سربرگ **Summary** بروید. سپس در پنل **resource** شما می توانید لیستی از **Datastore** هایی که توسط این ماشین مجازی استفاده می شوند را ببینید. بروی یکی از **Datastore** ها راست کلیک نمائید و گزینه **Browse Datastore** را انتخاب نمائید. بدین ترتیب محتوای **Datastore** به شما نمایش داده می شود و شما می توانید بروی پوشه ماشین مجازی خود کلیک نمائید و فایل های مربوط به آن ماشین مجازی را مشاهده و حتی در صورت لزوم فایلی را آپلود و یا دانلود نمائید.

در پنجره **Datastore Browser** دیسک های مجازی تنها شامل یک فایل با پسوند **vmdk** هستند. ولی در واقع یک دیسک مجازی شامل دو فایل می باشد:

- فایل **vmdk** که در واقع تشریح کننده خصوصیات و ویژگی های دیسک مجازی است
- فایل **flat.vmdk** - (این فایل **Hidden** می باشد) که حاوی داده ها و اطلاعاتی است که بروی دیسک مجازی ذخیره شده است



## استفاده از سربرگ Storage Views برای نمایش فایل ها

## Using the Storage Views Tab to Display Files

Click the Storage Views tab.

Select Show All Virtual Machine Files from the menu.

View: Reports Maps

Show all Virtual Machine Files

Name	Path	File type	Datastore	Size
Andrew02-1.nvram	[VMFS-02] Andrew02-1/Andrew02-1.nvram	NVRAM	VMFS-02	8.48 KB
Andrew02-1.vmdk	[VMFS-02] Andrew02-1/Andrew02-1.vmdk	Disk Descriptor	VMFS-02	0.00 B
Andrew02-1.vmsd	[VMFS-02] Andrew02-1/Andrew02-1.vmsd	Snapshot List	VMFS-02	0.00 B
Andrew02-1.vmx	[VMFS-02] Andrew02-1/Andrew02-1.vmx	Configuration	VMFS-02	2.92 KB
Andrew02-1.vmx	[VMFS-02] Andrew02-1/Andrew02-1.vmx	Extended Configuration	VMFS-02	2.67 KB
Andrew02-1-7a27e5f9.vswp	[VMFS-02] Andrew02-1/Andrew02-1-7a27e5f9.vswp	Swap	VMFS-02	384.00 M
Andrew02-1-aux.xml	[VMFS-02] Andrew02-1/Andrew02-1-aux.xml		VMFS-02	0.00 B
Andrew02-1-flat.vmdk	[VMFS-02] Andrew02-1/Andrew02-1-flat.vmdk	Disk Extent	VMFS-02	1.10 GB
vmware.log	[VMFS-02] Andrew02-1/vmware.log	Log	VMFS-02	73.90 KB
vmware-0.log	[VMFS-02] Andrew02-1/vmware-0.log	Log	VMFS-02	202.84 K
vmware-1.log	[VMFS-02] Andrew02-1/vmware-1.log	Log	VMFS-02	174.31 K
vmware-2.log	[VMFS-02] Andrew02-1/vmware-2.log	Log	VMFS-02	94.32 KB
vmx-Andrew02-1-2049435129-2.vswp	[VMFS-02] Andrew02-1/vmx-Andrew02-1-2049435129-2.vswp		VMFS-02	45.00 MB

همانطور که در اسلاید بالا مشاهده می نمائید، شما می توانید به صورت گرافیکی تمام فایل های ماشین مجازی را در سربرگ Storage View مربوط به آن ماشین مجازی مشاهده نمائید. برای دسترسی به سربرگ Storage View ماشین مجازی، شما می بایست ماشین مجازی خود را در بخش Inventory و در زمانیکه به vCenter Server متصل هستید انتخاب نمائید و سپس بروی سربرگ Storage View کلیک نمائید. همان طور که در اسلاید بالا مشاهده می نمائید شما دارای دو نما و یا همان View هستید: Reports و Maps. اگر بروی Reports کلیک نمائید یک منوی کشویی در زیر آن ظاهر می شود و بدین ترتیب گزینه های مختلفی را برای گزارش گیری در اختیار شما قرار می دهد. برای مثال علاوه بر این مشاهده همه فایل های ماشین مجازی، می توانید این موارد را نیز مشاهده نمائید:

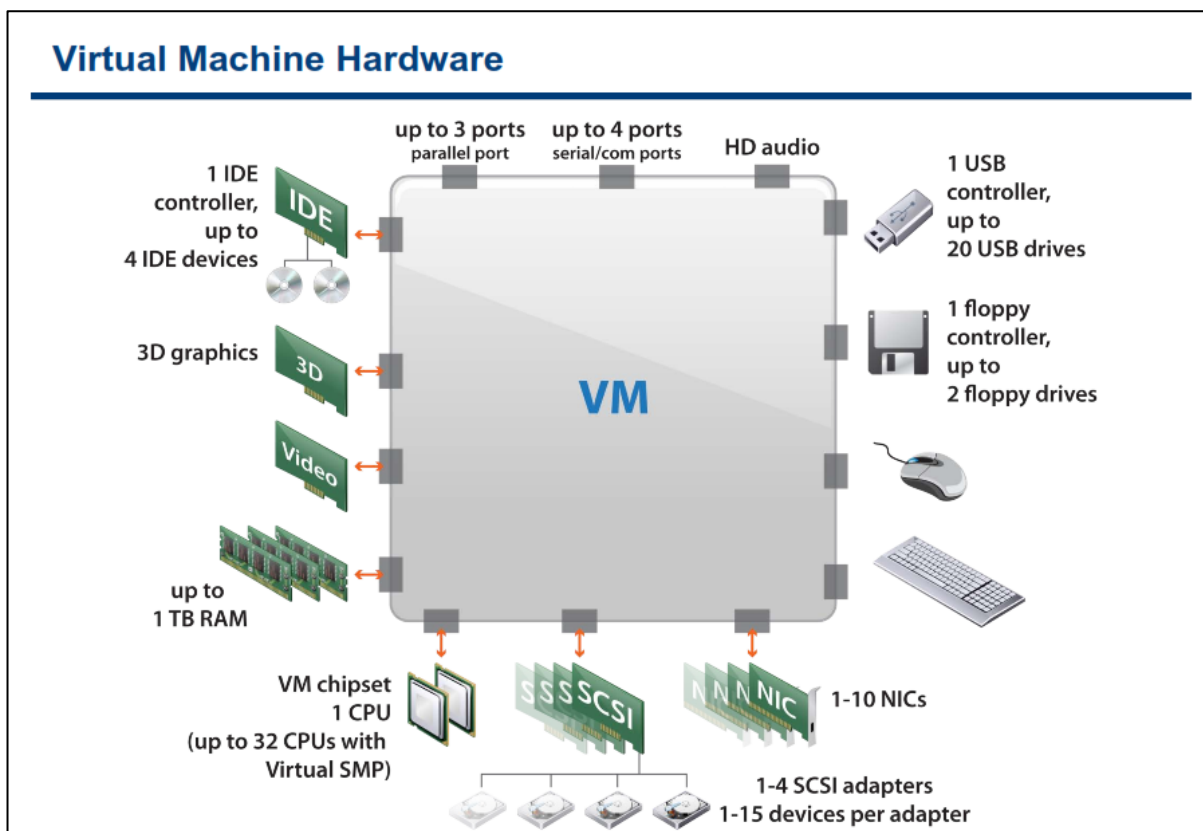
- Datastore ها
- LUN ها
- آداپتورهای SCSI , Path, Array Port
- NAS Mount

توجه داشته باشید موارد فوق در فصل های بعدی به تفصیل تشریح خواهد شد. همچنین شما می توانید از سربرگ Configuration هاست ESXi نیز اقدام به مشاهده فایل های ماشین مجازی نمائید. برای اینکار می بایست مراحل زیر را دنبال کنید:

- هاست VMware ESXi مورد نظر را در بخش Inventory انتخاب کنید و سپس بروی سربرگ Configuration کلیک نمائید.

- در مرحله بعدی بروی لینک Storage کلیک نمائید.
- در این مرحله بروی Datastore که حاوی فایل های ماشین مجازی می باشد راست کلیک نمائید و گزینه Browse Datastore را انتخاب کنید.
- در نهایت وارد پوشه هم نام ماشین مجازی مورد نظر شوید.

## سخت افزار ماشین مجازی



یک ماشین مجازی از سخت افزار مجازی استفاده می نماید. هر سیستم عامل که بروی ماشین مجازی نصب می گردد، دستگاه های سخت افزاری را به صورت عادی می بیند. این بدین معنی است که تفاوت میان سخت افزار واقعی و سخت افزاری مجازی را متوجه نمی شود. در واقع سیستم عامل متوجه نمی شود که این دستگاه مجازی می باشد. تمامی ماشین های مجازی دارای سخت افزارهای یک شکل می باشند (البته بجز مواردی که یک Administrator می تواند یک سخت افزار متفاوت اعمال نماید). سخت افزارهای یک شکل این امکان را برای ماشین مجازی فراهم می آورد که بتواند به صورت Portable و یا قابل حمل در میان پلتفرم های VMware Virtualization جابجا شود بدون اینکه اختلالی در اجرای این ماشین مجازی ایجاد شود.

شما می توانید مواردی همچون CPU ماشین مجازی و حافظه را پیکربندی نمایید و همچنین دیسک های مجازی و کارت های شبکه مجازی (NIC) را نیز اضافه نمایید. شما همچنین قادر خواهید بود تا سخت افزارهای مجازی دیگر همچون Floppy Drive، CD/DVD Drive، SCSI Drive را نیز اضافه و پیکربندی نمایید. البته لازم به ذکر است که شما نمی توانید تمامی دستگاه ها را پیکربندی و اضافه نمایید. برای مثال شما نمی توانید یک Video Card را اضافه نمایید ولی می توانید Video Card ها را در داخل سیستم عامل پیکربندی نمایید.

شما همچنین می توانید چندین USB Device را همانند قفل های USB نرم افزارها و Flash Memory ها به یک ماشین مجازی که بروی هاست ESXi قرار گرفته و این USB Device ها به صورت فیزیکی به آن هاست متصل هستند، اضافه نمایید. زمانیکه شما یک USB Device را به هاست ESXi متصل می نمایید، این USB Device تنها برای vm هایی که بروی آن هاست قرار گرفته اند قابل دسترسی می باشد. این vm ها نمی توانند به USB Device هایی که بروی سایر هاست ها

قرار گرفته اند متصل شوند. هر USB Device در هر لحظه فقط توسط یک ماشین مجازی مورد استفاده قرار می گیرد. زمانیکه که شما یک USB Device را از یک vm جدا می کنید، این USB Device برای سایر vm هایی که بروی آن هاست هستند در دسترس قرار می گیرد.

نکته:

شما می توانید تا شش دستگاه PCI vSphere DirectPath را به یک vm اضافه نمایید. این دستگاه ها می بایست برای استفاده از گذرگاه PCI بروی هاستی که vm بروی آن اجرا می شود رزرو گردد. توجه نمایید که در این حالت شما نمی توانید از قابلیت Snapshot استفاده نمایید.

برای کسب اطلاعات بیشتر در خصوص سخت افزار ماشین مجازی می توانید به سایت <http://www.vmware.com> مراجعه نمایید و مقاله vSphere Virtual Machine Configuration Guide را مطالعه کنید. همچنین برای مشاهده لیست کاملی از حداکثر پیکربندی های ماشین مجازی می توانید به مقاله Configuration Maximum در وب سایت <http://www.vmware.com> مراجعه نمایید.

## CPU و حافظه

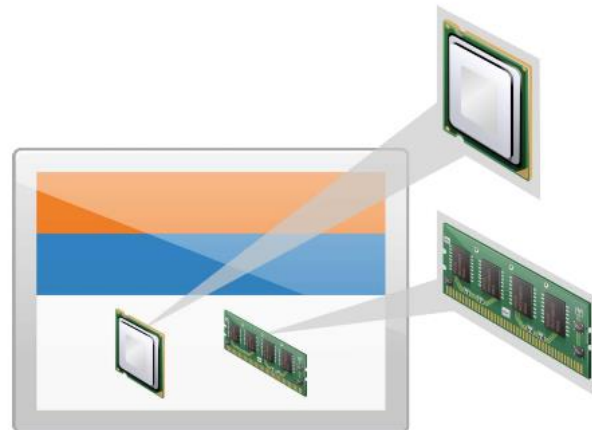
## CPU and Memory

## Up to 32 virtual CPUs (vCPUs):

- Depends on the number of licensed CPUs on a host and the number of processors supported by a guest operating system

## Up to 1TB maximum memory size:

- Depends on the amount the guest operating system will be told that it has



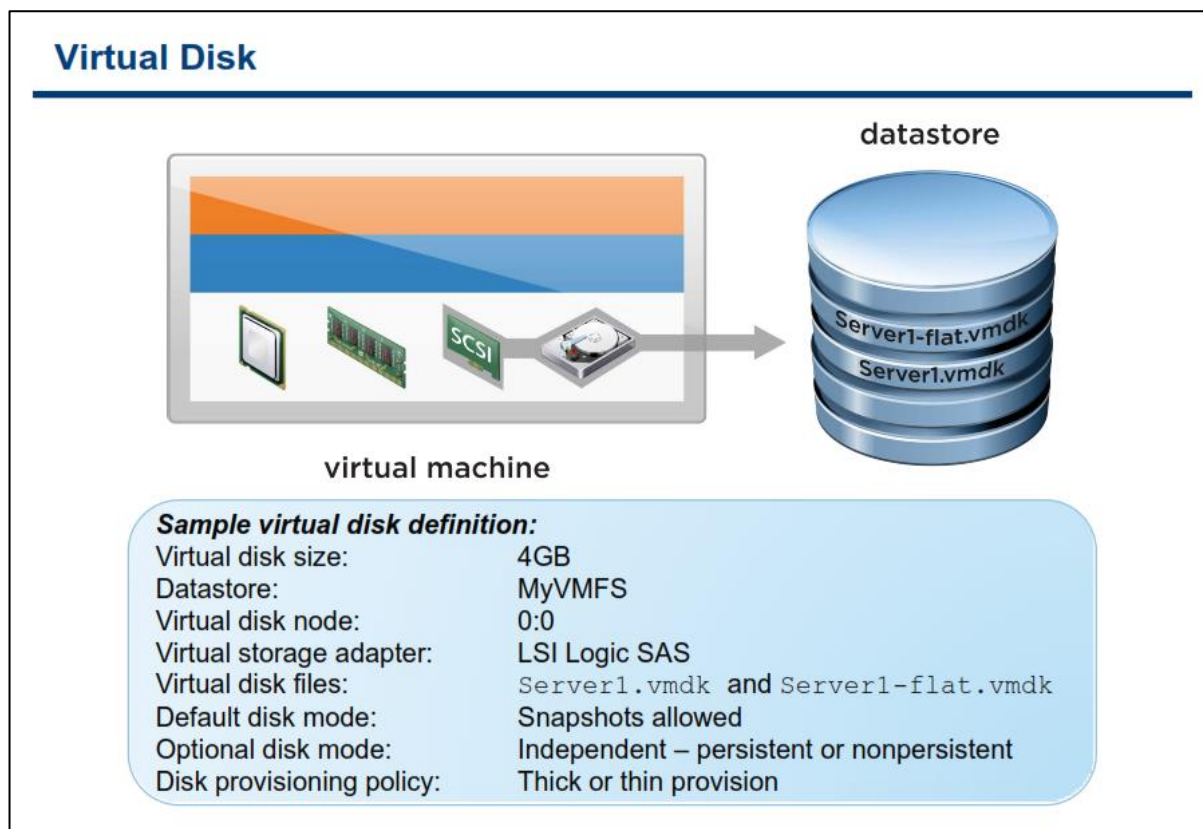
virtual machine

ابزار **VMware vSphere Client** می تواند اندازه پیش فرض حافظه (RAM) را برای ماشین ها مجازی در زمان ایجاد آنها تعیین نماید. اما با این وجود شما می بایست از اندازه حافظه مورد نیاز خود برای نرم افزارها و سیستم عاملی که بروی **vm** نصب شده اطلاع حاصل نمائید. حداکثر اندازه حافظه ای که شما می توانید برای یک **vm** در نظر بگیرید یک ترابایت می باشد. میزان حافظه ای که شما در نظر می گیرید حداکثر میزان حافظه ای است که **vm** می تواند از آن استفاده نماید.

با استفاده از قابلیت **VMware vSphere Virtual Symmetric Multiprocessing** شما می توانید ماشین های مجازی با حداکثر ۳۲ پردازنده تعریف نمائید و بتوانید پردازش های سنگینی که در ارتباط مستقیم با **CPU** هستند را بروی هاست **ESXi** به اجرا در آورید.

این در حالی است که بسیاری از سیستم عامل ها و یا نرم افزارها برای استفاده از چندین **CPU** طراحی و بهبود داده نشده اند. البته هر هاستی نیز نمی تواند دارای ماشین های مجازی با چندین **CPU** باشد. چرا که در بسیاری از موارد **CPU** ها فیزیکی محدود هستند.

## دیسک مجازی



هر vm می تواند حداقل یک Virtual Disk و یا دیسک مجازی داشته باشد . افزودن اولین Virtual Disk باعث می شود که یک Virtual SCSI Adapter بصورت مجازی به vm اضافه گردد. ESXi چهار نوع آداپتور را برای Virtual Disk ارائه می دهد: BusLogic Parallel , LSI Logic Parallel , LSI Logic SAS , VMware Paravirtual SCSI

تفاوت BusLogic Parallel , LSI Logic Parallel , LSI Logic SAS تنها به سیستم عامل آن ماشین مجازی وابسته است که از آن آداپتور پشتیبانی نماید. در صورتیکه شما از سیستم عامل های جدید استفاده می کنید پیشنهاد می شود از SAS استفاده نمائید. حال اگر میزان I/O شما در یک vm بیش از ۲۰۰۰ I/O در ثانیه می باشد پیشنهاد می شود از VMware Paravirtual SCSI استفاده نمائید و در غیر این صورت اگر کمتر از این مقدار I/O وجود داشت همان SAS را انتخاب کنید چرا که در مواردی مفید نخواهد بود.

فایل Virtual Disk در پوشه ای که فایل پیکربندی vm قرار دارد بروی VMFS datastore ذخیره می شود. این فایل همنام ماشین مجازی می باشد. شما می توانید تعیین کنید که Virtual Disk در یک SCSI Target ID خاص و یا در یک LUN مجزا بروی SAN Storage قرار گیرد. از طرفی دیگر شما می توانید تعیین کنید که Virtual Disk شما منبع ذخیره سازی را اشغال کند و یا نکند. این امکان را Disk Provisioning می نامند. Disk Provisioning دارای دو حالت thick ,thin می باشد. بصورت استاتیک در ابتدا تمام فضای تعیین شده دیسک را بروی datastore به خود اختصاص می دهد و آن را اشغال می کند ولی در حالت thin به نسبت فضایی که بروی دیسک مجازی ذخیره شده است این حجم اشغال می شود که البته این موضوع در بعضی از مواقع ممکن است دردسر ساز شود چراکه ممکن است شما بیش از اندازه فضا به vm ها اختصاص دهید و این به مرور برای شما مشکل آفرین شود.

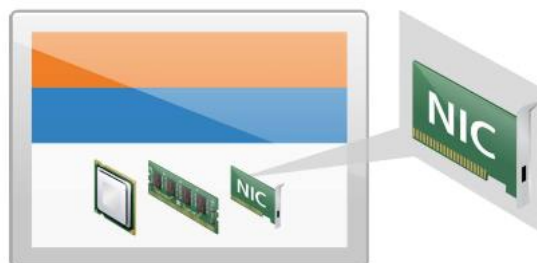
حالت های خاصی دیگری نیز برای دیسک مجازی وجود دارد که بنام **independent** شناخته می شود. حالت **independent** دارای دو گزینه **Persistent, non-Persistent** می باشد که البته در بخش های بعدی بطور کامل تشریح خواهد شد.

## کارت شبکه مجازی

### Virtual Network Interface Card

#### Network adapters that might be available for your virtual machine:

- Flexible – Can function as either a vlnance or vmxnet adapter:
  - vlnance – Also called PCNet32, supported by most 32-bit guest operating systems
  - vmxnet – Provides significantly better performance than vlnance
- e1000 – e1000e
  - High-performance adapter available for only some guest operating systems
- vmxnet, vmxnet2, and vmxnet3 are VMware® drivers and are only available with VMware Tools
  - vmxnet2 (Enhanced vmxnet) – vmxnet adapter with enhanced performance
  - vmxnet3 – Builds on the vmxnet2 adapter



virtual machine

Whenever possible, choose vmxnet3.

آداپتور های شبکه و یا همان کارت های شبکه مجازی دارای سه نوع اصلی هستند:

۱-Flexible: در این حالت اگر ابزار VMware Tools بروی سیستم عامل vm نصب نباشد عملکرد آن شبیه به vlnance adapter می باشد و اگر VMware Tools نصب باشد عملکرد آن به صورت vmxnet خواهد بود.

- vlnance : همان نسخه شبیه سازی شده کارت شبکه AMD PCNet32 Lance NIC که در اکثر سیستم عامل های ۳۲ بیتی بصورت built-in پشتیبانی می شود. نکته قابل توجه این است که بجز ویندوز ویستا و بالاتر از آن، سرعت این کارت شبکه در حدود 10 Mbps می باشد.
- vmxnet: این نوع NIC دارای کارایی بهتری نسبت به vlnance می باشد و برای vm ها بهبود داده شده است و نوع فیزیکی آن وجود ندارد و توسط vmware تولید و درایور آن عرضه می شود.

۲-e1000: یک نسخه شبیه سازی شده کارت شبکه Intel 82545EM Gigabit Ethernet NIC می باشد و درایور آن بصورت built-in در سیستم عامل های جدید شامل XP , Linux Kernel 2.4 و بالاتر وجود دارد. این نوع NIC به صورت پیش فرض بروی سیستم عامل های ۶۴ بیتی تنظیم می شود. البته توجه داشته باشید که پهنای باند و کارایی این نوع NIC به کارت شبکه هاست فیزیکی بستگی دارد.

۳-e1000e: یک نسخه شبیه سازی شده Intel 82574 Gigabit Ethernet NIC می باشد که در ماشین های مجازی با hardware version 8 به بالا پشتیبانی می شود و هم اکنون صرفاً در vm هایی با سیستم عامل های ویندوزی پشتیبانی می شود و متأسفانه در لینوکس پشتیبانی نمی شود.



۴-vmxnet2: این NIC نوع بهبود یافته vmxnet می باشد که دارای قابلیت ها و امکانات پیشرفته ای از جمله **jumbo frames** و **hardware off-loads** می باشد.

۵-vmxnet3: نسل جدید vmxnet می باشد که بطور مستقیم هیچ ارتباطی به vmxnet2 , vmxnet ندارد ولی شامل تمامی قابلیت های آنها به همراه چندین قابلیت جدید دیگر می باشد که شامل **MSI/MSI-X** , **IPv.6 off-loads** , **Interrupt Delivery** , **Multiqueue or Receive-Side Scaling** می باشد. این نسل در سیستم عامل های محدودی پشتیبانی می شود و فقط با vm هایی با **hardware version 7.0** به بالا پشتیبانی می شود. تقریبا در همه سیستم عامل هایی همچون **7, 2008R2, 2008, xp, 2003, 2003R2** و **Redhat 5** و به بالا پشتیبانی می گردد.

## سایر دستگاه‌ها

### Other Devices

---

**CD/DVD drive:**

- Connect to CD-ROM, DVD, or ISO image.

**USB 3.0:**

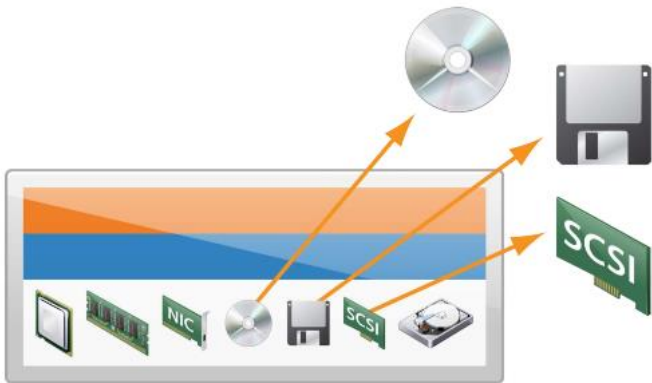
- Smart card readers.

**Floppy drive:**

- Connect to floppy or floppy image.

**Generic SCSI devices (such as tape libraries):**

- Can be connected to additional SCSI adapters



virtual machine

CPU مجازی و حافظه مجازی حداقل نیازمندیهای یک سخت افزار مجازی می باشد اما داشتن یک دیسک مجازی و کارت شبکه مجازی یک vm را مفید تر از قبل می سازد. سایر سخت افزارهای مجازی برای vm شامل: CD/DVD Drive مجازی ، Floppy Drive مجازی و SCSI Drive های مجازی می باشد. CD/DVD Drive و یا Floppy Drive می توانند از موارد زیر برای ماشین مجازی مسپردهی شوند:

- CD/DVD Drive و یا Floppy Drive موجود بروی هاست فیزیکی ESXi
- فایل ISO Image با پسوند .iso و Floppy Image با پسوند .flp
- CD/DVD Drive و یا Floppy Drive موجود بروی سیستم Local (همان سیستمی که شما از طریق آن به هاست ESXi متصل می شوید)

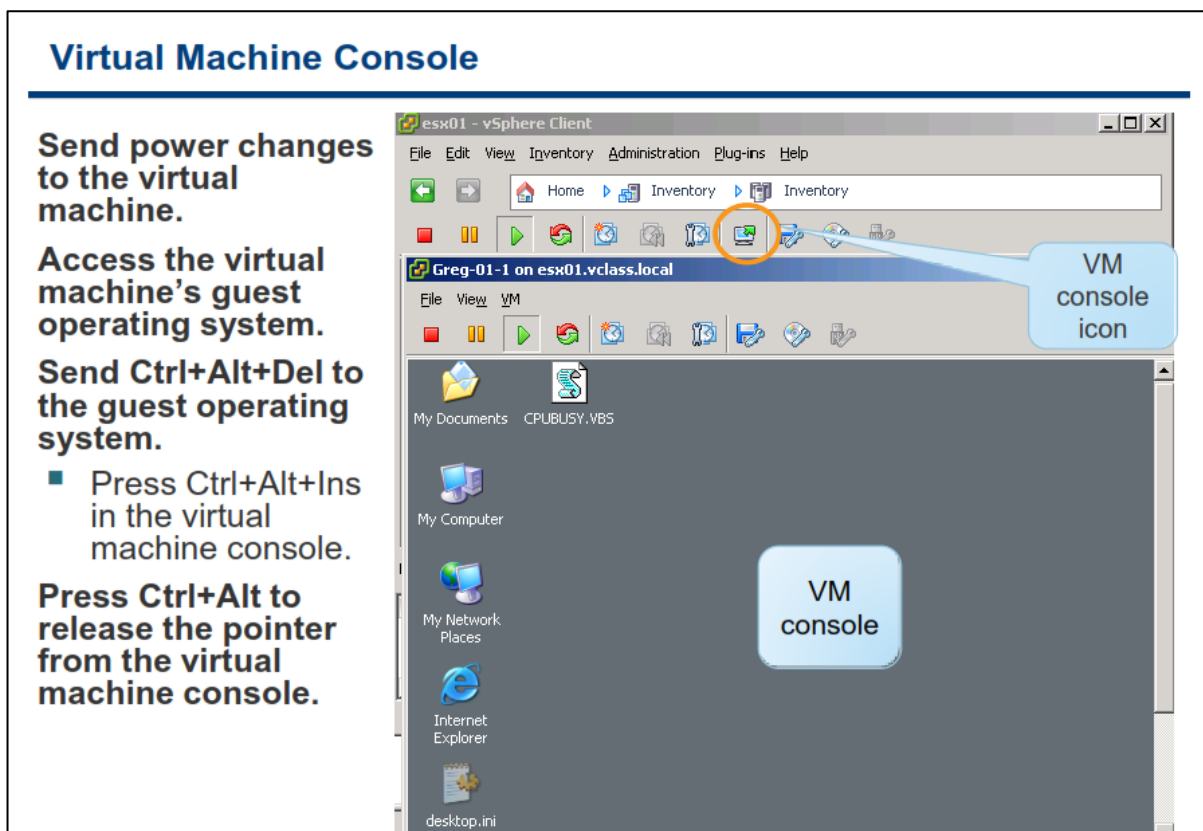
شما می توانید CD/DVD Drive ماشین مجازی را به یک Drive فیزیکی و یا یک فایل .iso نگاشت (Map) نمائید. یک فایل iso فایلی است که به صورت بایت به بایت از روی CD\DVD کپی شده است و Ripped می باشد. Ripped یک فایل سیستم است که بصورت بایت به بایت بروی سطح دیسک کپی شده است. بدین ترتیب شما می توانید به CD\DVD های مجازی با پسوند iso از راه دور دسترسی داشته باشید و البته در صورت استفاده از این راهکار از سرعت دسترسی بالاتری نسبت به داریو های فیزیکی برخوردار خواهید شد.

شما همچنین می توانید دستگاه های SCSI معمول را همانند Tap Library به vm های خود متصل نمائید. این دستگاه ها می توانند به Virtual SCSI Adapter های یک ماشین مجازی متصل شوند.

در نسخه vSphere 5.0 از دستگاه هایی با پورت USB 3.0 در ماشین های مجازی دارای سیستم عامل لینوکس نیز پشتیبانی می گردد. شما همچنین می توانید دستگاه های USB 3.0 را به کامپیوتری که بروی آن نرم افزار vSphere Client و یا vSphere Web Client نصب شده است، متصل نمائید و سپس دستگاه USB موجود بروی این سیستم ها را به ماشین مجازی متصل نمائید. بدین ترتیب لزومی ندارد شما حتما دستگاه USB را به هاست فیزیکی ESXi متصل نمائید تا از آن در ماشین مجازی استفاده نمائید. البته توجه نمائید که در vSphere 5.0 امکان اتصال مستقیم دستگاه های USB 3.0 به هاست ESXi وجود ندارد و پشتیبانی نمی شود.

برای کسب اطلاعات بیشتر در خصوص ایجاد یک ماشین مجازی می توانید به مقاله vSphere Virtual Machine Administration Guide در وب سایت <http://www.vmware.com> مراجعه نمائید.

## کنسول ماشین مجازی



امکان Remote Console ماشین مجازی در نرم افزار vSphere Client به همراه قابلیت دسترسی به صفحه نمایش ، موس و کیبورد فراهم شده است. بدین ترتیب برای نصب سیستم عامل بروی vm می توانید از این امکان استفاده نمائید. Remote Console این امکان را به شما می دهد تا بتوانید به BIOS یک ماشین مجازی دسترسی داشته باشید. همچنین از طریق این کنسول شما می توانید ماشین مجازی را روشن ، خاموش و یا حتی مجدداً آن را راه اندازی نمائید (Restart). Remote Console، از اتصال Smart Card Reader به چندین ماشین مجازی پشتیبانی می کند که بدین ترتیب می توان از این قابلیت برای احراز هویت به ماشین مجازی استفاده نمود.

توصیه نمی شود از Remote Console برای اتصال به vm برای کارهای روزانه و عادی استفاده شود اما برای اینگونه فعالیت ها و ارتباط با دسکتاپ vm می توان از ابزارهایی همچون VMware View ، Remote Desktop Connection ، Virtual Network Connection و یا ابزارهای مشابه استفاده نمود. در حقیقت از این کنسول می بایست برای خاموش و روشن کردن vm ، پیکربندی سخت افزار، عیب یابی مشکلات شبکه و مسائلی از این دست استفاده نمود.

این کنسول به شما این امکان را می دهد که بتوانید Ctrl+Alt+Del را برای vm ارسال نمائید. برای اینکار می توانید از کلید ترکیبی Ctrl+Alt+Insert استفاده نمائید و یا اینکه در این کنسول از منوی VM->Guest گزینه Send Ctrl+Alt+Del را انتخاب نمائید. همچنین شما می توانید از کلید ترکیبی Ctrl+Alt برای برگرداندن کنترل اشاره گر موس به سیستم خودتان استفاده نمائید.

برای مشاهده Remote Console یک ماشین مجازی ، بروی ماشین مجازی مورد نظر در بخش Inventory راست کلیک نمائید و گزینه Open Console را انتخاب نمائید.

## بخش دوم: ایجاد ماشین مجازی

بعد از به اتمام رساندن این بخش شما قادر خواهید بود:

- یک ماشین مجازی را ایجاد نمائید
- Option های ماشین مجازی را پیکربندی نمائید
- یک سیستم عامل بروی ماشین مجازی نصب نمائید
- VMware Tools را در داخل سیستم عامل نمائید
- نحوه وارد کردن Virtual Appliance را به داخل ESXi تشریح نمائید

## ویژارد ایجاد ماشین مجازی

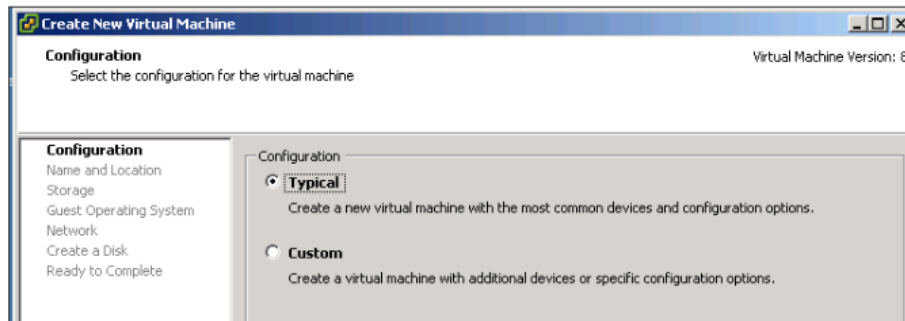
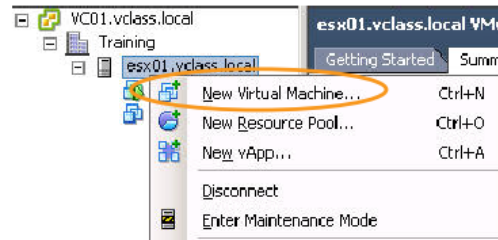
### Create New Virtual Machine Wizard

#### Create a new virtual machine in the VMware vCenter Server inventory.

- In the Inventory view, select a datacenter, cluster, or host.

#### Start the Create New Virtual Machine wizard.

- Perform a "typical" or "custom" configuration.



چندین روش برای ایجاد و گسترش یک ماشین مجازی وجود دارد. در این بخش شما فرا می گیرید که چگونه یک ماشین مجازی را به صورت دستی و Manully ایجاد نمایید و یا اینکه چگونه یک فایل Virtual Appliance (فایلی با فرمت Open Virtualization Format) را به درون محیط مجازی وارد نمایید.

شما می توانید از ویژارد Create New Virtual Machine در برنامه vSphere Client برای ایجاد ماشین مجازی استفاده نمایید. برای اینکار شما می بایست به نمای Host and Cluster و یا نمای VM and Template مراجعه نمایید.

در نمای Host and Cluster بروی نام Datacenter، Cluster و یا نام Host راست کلیک نمایید و گزینه New Virtual Machine را انتخاب نمایید. بدین ترتیب ویژارد Create New Virtual Machine ظاهر می شود. در این ویژارد از شما پرسیده می شود آیا شما می خواهید vm جدید را به صورت عادی (Typical) و یا سفارشی (Custom) پیکربندی نمایید. مسیر پیکربندی Typical دارای فرایند کوتاه تری می باشد چراکه در این حالت گزینه هایی که به ندرت نیاز به تغییر پیدا می کنند نمایش داده نمی شود. اما مسیر پیکربندی Custom دارای فرایندی طولانی تری می باشد و همچنین گزینه متعددی را نیز به شما نمایش می دهد.

## انتخاب پیکربندی Typical

## Choosing the Typical Configuration

## Information needed for a typical configuration:

- Virtual machine name and inventory location
- Location in which to place the virtual machine (cluster, host, resource pool)
- Datastore on which to store the virtual machine's files
- Guest operating system and version
- Disk parameters for creating a new virtual disk:
  - Disk size
  - Disk-provisioning settings:
    - **Allocate and commit space on demand (Thin Provisioning)**
    - **Support clustering features such as Fault Tolerance**

اگر شما پیکربندی Typical را انتخاب نمائید، ویزارد Create New Virtual Machine اطلاعاتی از قبیل موارد زیر را به شما نمایش می دهد:

- مشخص کردن نام ماشین مجازی
- مشخص کردن مکانی از vCenter Server Inventory که vm در آنجا قرار می گیرد
- مشخص کردن datastore که فایل های vm بروی آن قرار می گیرند
- مشخص کردن سیستم عاملی که می بایست بروی ماشین مجازی نصب گردد

همچنین شما می بایست اندازه و فضایی که می خواهید برای دیسک مجازی vm در نظر بگیرید را مشخص نمائید. و سپس می بایست یکی از گزینه های زیر را برای ذخیره سازی دیسک مجازی انتخاب نمائید:

- **Thick Provision Lazy Zeroed**: این نوع دیسک مجازی در ابتدا تمام ظرفیت مورد نظر را در حین ایجاد vm و یا دیسک مجازی اشغال میکند. Lazy Zeroed نیز بدین معنی است که در زمانیکه دیسک مجازی ایجاد می شود تمامی بلوک های دیسک مجازی با صفر پر نمی شوند و در زمانیکه ماشین مجازی اقدام به نوشتن بروی دیسک مجازی می کند عملیات صفر کردن بلوک های دیسک مجازی انجام می شود.
- **Thick Provision Eager Zeroed**: این نوع دیسک نیز همانند حالت قبلی در ابتدا تمام ظرفیت مورد نظر را به خود اختصاص می دهد فقط با این تفاوت که در لحظه ایجاد دیسک مجازی تمام بلوک ها را صفر می کند که این کار باعث افزایش مدت زمان ایجاد vm و یا دیسک می شود. برای استفاده از قابلیت های همچون Fault



**Tolerance** می بایست از این نوع دیسک استفاده نمائید. در غیر این صورت می بایست **Virtual Disk** ها را **convert** نمائید که البته اینکار نیز توصیه نمی گردد.

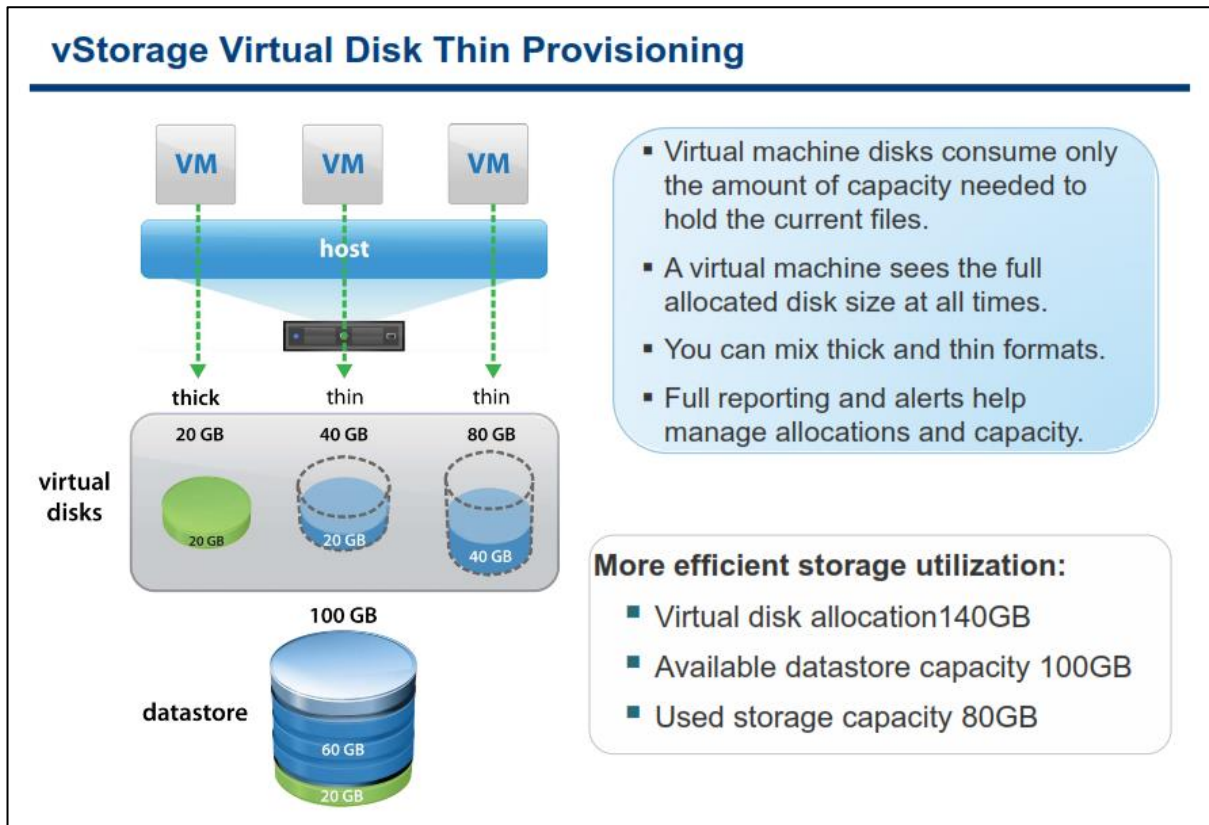
- **Thin Provision**: در این حالت شما یک ظرفیتی را برای **Virtual Disk** در نظر می گیرید که این ظرفیت بطور کامل در ابتدا توسط دیسک مجازی اشغال نمی شود. این گزینه به شما در صرفه جویی دیسک فیزیکی و همچنین کاهش زمان ایجاد دیسک مجازی کمک فراوانی می کند.

مثال: اگر شما دارای یک **datastore** با ظرفیت ۵۰۰ گیگابایت داشته باشید. همچنین یک ماشین مجازی از نوع **Thick** با ظرفیت ۱۰۰ گیگابایت بسازید، در همان ابتدا ۱۰۰ گیگابایت از فضای ۵۰۰ گیگابایتی سرور شما از دست میرود و مورد استفاده قرار می گیرد. اما اگر دیسک مجازی خود را از نوع **Thin** بسازید و بطور مثال یک سیستم عامل با حجم ۲ گیگابایت بروی آن **vm** نصب نمائید، همین دو گیگابایت از سرور اصلی (۵۰۰) کم می شود و البته شما می توانید تا حداکثر ۱۰۰ گیگابایت نیز اطلاعات بروی این دیسک مجازی ذخیره نمائید.

جدول زیر نشان دهنده تفاوت میان انواع دیسک های مجازی می باشد. این تفاوت ها شامل مدت زمان ایجاد یک نوع دیسک مجازی، نحوه تخصیص بلوک های دیسک و صفر کردن آنها و همچنین نحوه قالب بندی (**Layout**) انواع دیسک ها می باشد.

Thin Provision	Thick Provision Eager Zeroed	Thick Provision Lazy Zeroed	
خیلی سریع	آهسته و به میزان اندازه دیسک مجازی بستگی دارد	سریع	زمان ایجاد
صفر کردن و تخصیص دادن در زمان نوشتن بروی دیسک صورت می پذیرد	بطور کامل از ابتدا تخصیص داده می شود	بطور کامل از ابتدا تخصیص داده می شود	تخصیص بلوک ها
قالب ها براساس وضعیت دینامیک درایو ها در زمان تخصیص بلوک متفاوت می باشند و احتمال پشت سر هم قرار گرفتن بلوک های فایل به شدت کاهش می یابد	شانس بسیار زیادی وجود دارد که بلوک های فایل پشت سر هم قرار گیرند	شانس زیادی وجود دارد که بلوک های فایل پشت سر هم قرار گیرند	قالب بندی دیسک مجازی
بلوک های فایل در زمانیکه بلوک ها تخصیص پیدا می کنند صفر می شوند	بلوک های فایل در زمان ایجاد دیسک صفر می شوند	بلوک های فایل در زمان اولین نوشتن بروی دیسک صفر می شوند	صفر کردن بلوک فایل های ذخیره شده

## امکان Thin Provisioning در دیسک مجازی



با استفاده از امکان **Thin Provisioning** در دیسک مجازی شما می توانید از فضای ذخیره سازی (**Storage**) خود به صورت بهینه و به همان اندازه ای که نیاز دارید استفاده نمایید. این امکان در صرف جویی فضای دیسک فیزیکی تاثیر به سزایی دارد. این امکان این اجازه را به شما می دهد که بتوانید بیش از فضای در دسترس خود دیسک مجازی تعریف نمایید. امکان **Thin Provisioning** گزارشات و هشدار هایی را برای استفاده و تخصیص فضا فراهم می کند که با استفاده از آن می توانید فضای ذخیره سازی را بهتر مدیریت نمایید.

امکان **Thin Provisioning** در اغلب اوقات با امکانی بنام **Storage Array Deduplication** در منابع ذخیره سازی مورد استفاده قرار می گیرد که همین امر باعث بهبود استفاده از دیسک می شود و در موارد بسیاری برای پشتیبان گیری از **vm** ها مورد استفاده قرار می گیرد.

البته توجه داشته باشید که همیشه امکان **Thin Provisioning** مناسب نیست و برای استفاده از این امکان باید ارزیابی هایی اولیه ای صورت پذیرد. بطور مثال در زمان بازیابی (**Recovery**) یک دیسک مجازی، دیسک هایی از نوع **Thick** راحت تر و بهتر مورد بازیابی قرار می گیرند و همین مسئله باعث می شود بروی برخی از ماشین های مجازی حساس از نوع **Thin** استفاده نکنیم.

## انتخاب پیکربندی Custom

## Choosing the Custom Configuration

## Other information needed for a custom configuration:

- Virtual machine version (version 8 is the latest)
- Number of CPUs, number of cores per CPU and size of memory
- Number of NICs, network to connect to, and network adapter type
- SCSI controller type
- Whether to create a new disk, use an existing disk, use an RDM, or use no disk
- Other disk-provisioning settings:
  - Whether to store the virtual disk with the virtual machine or in a different datastore
  - Virtual device node (for example, SCSI(0:0))
  - Mode-independent (persistent and nonpersistent)

## For both the typical and the custom configurations:

- You can edit virtual machine settings before completing the task.
  - For example, attach an ISO image to the virtual CD/DVD drive.

اگر شما پیکربندی Custom را انتخاب نمائید، در ویزارد Create New Virtual Machine تنظیمات بیشتری را می‌بایست پیکربندی نمائید، همانند نسخه ماشین مجازی.

آخرین نسخه ماشین مجازی نسخه ۸.۰ می‌باشد که البته این نسخه با ESXi 5.0 و بالاتر از آن سازگاری کامل دارد (البته به تازگی نیز نسخه ۹ و ۱۰ ماشین مجازی برای سازگاری با ESXi 5.1 و ESXi 5.5 عرضه شده است). نسخه ۸.۰ ماشین مجازی از امکانات بالاتری به نسبت نسخه‌های قبلی برخوردار است.

همچنین در ویزارد Custom علاوه بر موارد بالا گزینه‌هایی همانند موارد زیر را به شما ارائه می‌دهد:

- ساختن یک دیسک مجازی جدید
- استفاده از دیسک مجازی موجود
- ساختن یک Raw Device Mapping (RDM) - در اسلاید بعدی به این موضوع می‌پردازیم
- ایجاد vm بدون دیسک مجازی

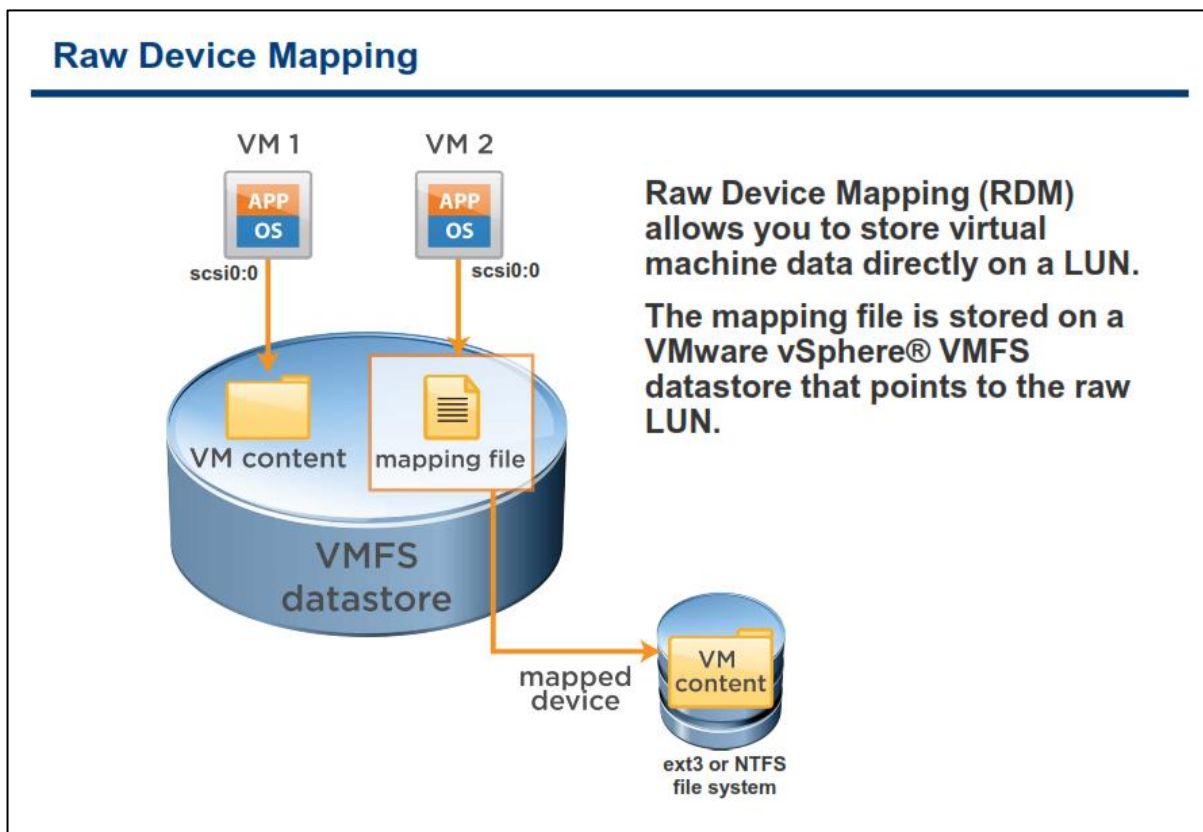
برای ساخت vm در حالت Custom شما می‌توانید همچنین datastore و ISO و SCSI Controller Type و RAW Disk، تعداد CPU ها و هسته‌های آن، میزان ظرفیت حافظه، تعداد کارت‌های شبکه یک ماشین مجازی به همراه تعیین نوع آنها، را برای یک vm را مشخص کنید. همچنین شما می‌توانید Virtual Device node و حالت Independent (مستقل) را برای دیسک مجازی مشخص کنید. پیکربندی حالت مستقل یا Independent را برای Virtual Disk شامل گزینه‌های زیر می‌باشد:

**persistent** یا پایدار: در این حالت تغییرات بلافاصله و به صورت دائمی بروی دیسک اعمال و نوشته می شود اما در این نوع دیسک دیگر از **Snapshot** پشتیبانی نمی شود. این حالت بسیار شبیه همان دیسک های فیزیکی می باشد چراکه تغییرات بلافاصله اعمال می شود و هیچ مکانیزی نیز همانند **Snapshot** برای بازیابی اطلاعات قبلی وجود ندارد.

**nonpersistent** و یا ناپایدار: در این حالت تغییراتی که بروی دیسک ایجاد می شود صرفاً تا زمانیکه که **vm** روشن می باشد پایدار است و زمانیکه **vm** خاموش و یا **Restart** می شود این تغییرات از بین می رود. در این حالت حتی اگر **Snapshot** نیز بازیابی شود، تغییرات از بین می رود. البته شما در اکثر مواقع نیاز به تغییر این حالت برای **Virtual Disk** ندارید.

توجه داشته باشید که در هر دو حالت **Typical** و **Custom** پس از ایجاد ماشین مجازی نیز شما می توانید این موارد را تغییر دهید. بطور مثال شما می توانید فایل **ISO** را بعداً به **vm** متصل نمایید.

## Raw Device Mapping



یک RAW Device Map یا همان فایل RDM یک فایل ذخیره شده بروی منبع ذخیره سازی فیزیکی (Physical Storage) یا همان VMFS Volume می باشد. RDM به شما این اجازه را می دهد که بتوانید داده های vm را مستقیماً بروی یک Storage فیزیکی ذخیره نمایید. بدین ترتیب تمامی اطلاعات شما بروی یک دیسک مجازی نوشته نمی شوند و هر آن چیزی که در داخل یک ماشین مجازی وجود دارد بروی منبع ذخیره سازی فیزیکی نوشته می شود.

بجای ذخیره داده vm در یک Virtual Disk در VMFS datastore شما می توانید داده های vm را مستقیماً بروی raw LUN (به شماره بندی منطقی که بروی یک SAN Storage تخصیص داده می شود اطلاق می شود) یک منبع ذخیره سازی ذخیره نمایید. در صورتیکه از نرم افزاری بروی یک vm استفاده می کنید که نیاز به شناخت برخی از ویژگی های فیزیکی Storage دارد، ذخیره سازی داده ها بدین صورت می تواند بسیار مفید و کاربردی باشد.

استفاده از این امکان به شما اجازه می دهد که از برخی از دستورات SAN Storage برای مدیریت آن استفاده نمایید.

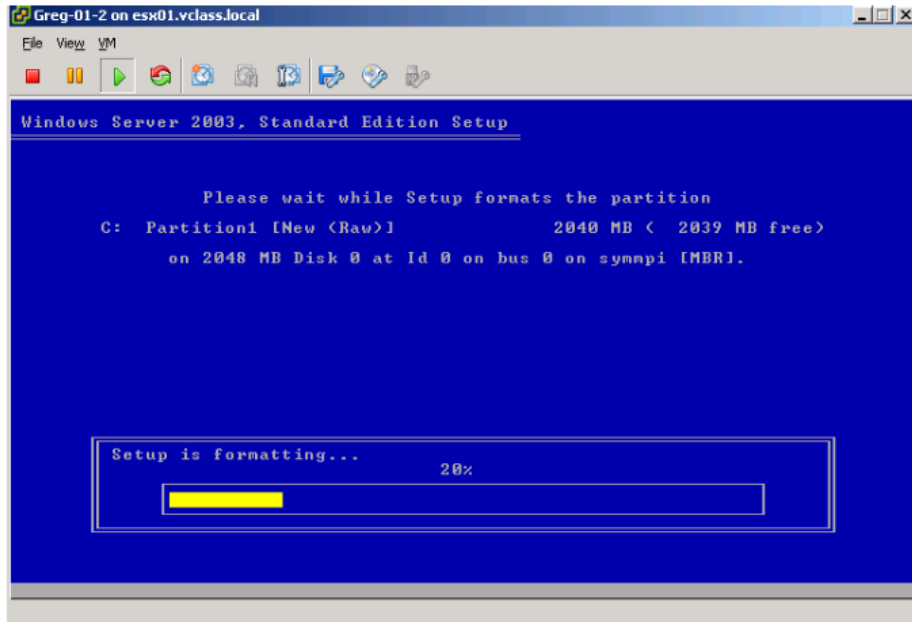
RDM برای vm هایی که می خواهند بصورت مستقیم با دیسک های واقعی SAN در تعامل باشند توصیه می شود. همچنین اگر داده های شما بسیار حجیم هستند و همچنین اگر نمی خواهید این داده ها بروی یک Virtual Disk قرار گیرند می توانید از این قابلیت استفاده کنید.

همانطور که در اسلاید بالا می بینید، Mapping File در واقع یک فایل اشاره گر می باشد که به یک raw LUN (LUN خام) اشاره می کند.

## نصب سیستم عامل

## Installing the Guest Operating System

Install the guest operating system into the virtual machine.



نصب سیستم عامل بروی ماشین مجازی دقیقاً شبیه به نصب آن بروی یک کامپیوتر فیزیکی می باشد. برای نصب یک سیستم عامل بروی ماشین مجازی می بایست از طریق کنسول vm و ابزار vSphere Client که در بخش های قبلی بیان شد با ماشین مجازی ارتباط برقرار کنید. vSphere Client به شما امکان می دهد تا یک CD-ROM , DVD و یا فایل ISO را که حاوی فایل های نصب سیستم عامل می باشد را به یک Virtual CD\DVD Drive متصل نمایید.

همانطور که در اسلاید بالا می بینید یک سیستم عامل Windows Server 2003 در حال نصب بروی ماشین مجازی می باشد. همچنین برای کسب اطلاعات بیشتر در خصوص سیستم عامل هایی که بروی یک ماشین مجازی نصب می شوند می توانید به مقاله [http://www.vmware.com/pdf/GuestOS\\_guide.pdf](http://www.vmware.com/pdf/GuestOS_guide.pdf) مراجعه نمایید.

## VMware Tools

## VMware Tools

**Features of VMware Tools include:**

- Device drivers:
  - SVGA display
  - vmxnet/vmxnet3
  - Balloon driver for memory management
  - Sync driver for quiescing I/O
  - Improved mouse
- Virtual machine heartbeat
- Time synchronization
- Ability to shut down virtual machine
- Adds additional choices to Perfmon DLL.

VMware Tools مجموعه ای از ابزارهای مفید برای بهبود کارایی یک vm می باشد. VMware Tools مدیریت vm ها و عملکرد سخت افزارهای مجازی را با جایگزین کردن درایور های VMware بجای درایورهای سیستم عامل، هماهنگ و تنظیم می نماید. با وجود اینکه شما می توانید VMware Tools را بروی سیستم عامل ماشین مجازی نصب نکنید اما توصیه می شود که VMware Tools را حتما نصب نمایید. VMware Tools قابلیت هایی را از قبیل موارد زیر برای شما فراهم می آورد:

- یکسان سازی زمان vm با زمان HOST ESXi
- مجموعه ای از درایورهای سخت افزارهای VMware
  - SVGA Display Driver
  - vmxnet/vmxnet3 Network برای برخی از سیستم عامل ها
  - BusLogic SCSI برای برخی از سیستم عامل ها
  - Memory Control Driver برای تخصیص حافظه در میان vm ها و یا همان Balloon driver برای مدیریت حافظه
  - بهبود عملکرد موس و کیبورد و همچنین VMware Mouse Driver
  - قابلیت ShutDown کردن نرم افزاری vm با استفاده از دکمه Power off کنسول vm
  - Virtual Machine Heartbeat (به منظور مانیتورینگ و بررسی لحظه به لحظه در مکانیزم High Availability مورد استفاده قرار می گیرد)

- با استفاده از **VMware Tools** می توانید اقدام به توسعه اسکریپت هایی نمائید که به شما در اجرای اتوماتیک عملیات در یک سیستم عامل کمک خواهد کرد. این اسکریپت ها می توانند به گونه ای پیکربندی شوند که در حین تغییر وضعیت روشن و یا خاموش شدن ماشین مجازی اجرا گردند.
- **VMware User Process** امکانی است که با استفاده از آن می توانید متن و یا فایل را از یک **vm** به سیستم عاملی که **vSphere Client** در آن نصب است کپی نمائید.
- درایور یکسان سازی برای **quiesce I/O**



## Virtual Appliance

## Virtual Appliances

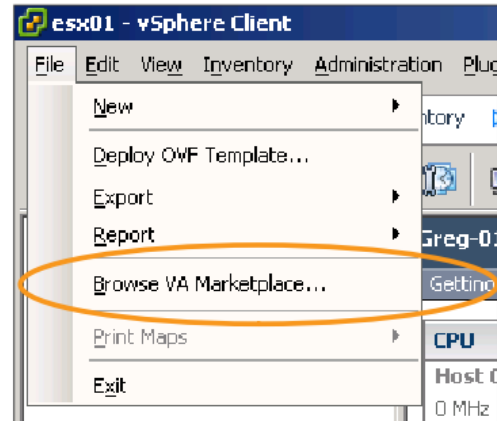
## Preconfigured virtual machines:

- Usually designed for a single purpose (for example, a safe browser or firewall)
- Deployed as an OVF template

## Available from the VMware Virtual Appliance Marketplace:

- <http://www.vmware.com/appliances>

Use the VMware vSphere® Client™ to upload appliances into VMware vCenter Server™ or an VMware ESXi™ host.



یک **Virtual Appliance** یک ماشین مجازی از پیش پیکربندی شده می باشد که سیستم عامل و نرم افزار های آن از پیش بروی آن نصب شده اند. یک **Virtual Appliance** برای اهداف خاصی همچون ابزارهای **Backup & Recovery** و ابزارهای فایروال طراحی می شوند.

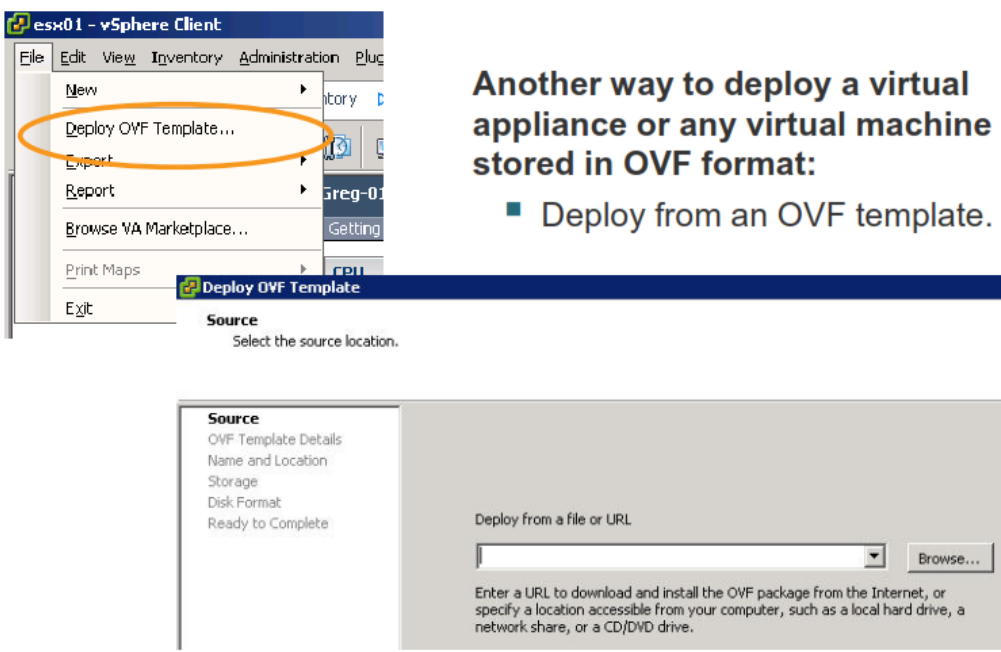
یک **Virtual Appliance** را می توانید با استفاده از **vSphere Client** و با فرمت **OVF** وارد نمائید (**Import**) و یا خروجی بگیرید (**Export**). **Virtual Appliance** ها را می توانید از وب سایت هایی همچون **VA Marketplace** دریافت و **Import** نمائید.

برای اینکار شما می توانید با استفاده از برنامه **vSphere Client** به هاست و یا **vCenter Server** متصل شوید و از منوی **File->Browse VA Marketplace** را انتخاب کنید.

**Virtual Appliance** ها به عنوان **Open Virtualization Format** یا همان **OVF** منتشر می شوند. **OVF** یک پلتفرم مستقل ، کارآمد ، توسعه پذیر و توزیع شده برای **vm** ها می باشد. **OVF** یک فایل فشرده شده می باشد و به همین خاطر راحتتر آن را می توان دانلود و یا جابجا کرد. توجه داشته باشید که در هنگام **Import** کردن می بایست از سازگاری آن با سرور مقصد اطمینان حاصل نمائید چراکه **VA** های ناسازگار **Import** نخواهند شد.

## نصب یک قالب OVF

## Deploying an OVF Template



Another way to deploy a virtual appliance or any virtual machine stored in OVF format:

- Deploy from an OVF template.

**Source**  
Select the source location.

**Source**  
OVF Template Details  
Name and Location  
Storage  
Disk Format  
Ready to Complete

Deploy from a file or URL

Enter a URL to download and install the OVF package from the Internet, or specify a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

با استفاده از vSphere Client شما می توانید Virtual Appliance را وارد نمائید (Import) و یا خروجی بگیرید (Export).

برای وارد کردن Virtual Appliance می بایست هاست و یا کلاستری را که می خواهید Virtual Appliance در آنجا اجرا گردد را انتخاب نمائید و سپس منوی File->Deploy OVF Template را انتخاب و فایل OVF را وارد نمائید. شما همچنین می توانید در wizard وارد کردن Virtual Appliance از یک آدرس URL نیز استفاده نمائید، بدین ترتیب فایل OVF از اینترنت دانلود شده و بروی سرور Deploy می گردد.

با خروجی گرفتن از یک ماشین مجازی در واقع شما از آن یک Virtual Appliance ایجاد می نمائید که قابلیت جابجایی و وارد شدن در سایر زیر ساخت های مجازی را دارا می باشد. برای Export کردن یک vm نیز شما می بایست آن vm را خاموش و دستگاه هایی شبیه به CD/DVD را از آن قطع کنید و سپس از گزینه File->Export->Export OVF Template استفاده نمائید.

## کارگاه شماره سه:

در این کارگاه آموزشی، شما نحوه ایجاد، وارد کردن و آماده سازی ماشین مجازی را خواهید آموخت که شامل موارد زیر می باشد:

۱. ایجاد ماشین مجازی
۲. نصب یک سیستم عامل بروی ماشین مجازی
۳. شناختن یک **Disk Format** برای ماشین مجازی و میزان استفاده آن از دیسک فیزیکی
۴. نصب **VMware Tools** بروی یک ماشین مجازی
۵. فعال کردن یکسان سازی زمان و تاریخ بین ماشین مجازی و هاست **ESXi**
۶. کپی کردن برنامه ها از **CD-ROM** به ماشین مجازی

## فصل سوم: VMware vCenter Server



این فصل شامل بخش های زیر می گردد:

۱. نصب ESXi
۲. معماری vCenter Server
۳. نصب vCenter Server - نسخه ویندوز
۴. نصب و توسعه vCenter Virtual Appliance
۵. مدیریت آیتم های موجود در vCenter Server

اهمیت این فصل:

از آنجائیکه هاست ESXi منابع فیزیکی را برای ماشین های مجازی فراهم می آورد و همچنین از آنجائیکه VMware vCenter Server به شما کمک می کند تا چندین هاست ESXi را به همراه ماشین های مجازی آنها به صورت یکپارچه مدیریت نمایید، اشکال در نصب، پیکربندی و مدیریت vCenter Server و ESXi می تواند باعث کاهش کارایی مدیریتی و یا بوجود آمدن DownTime در زیر ساخت مجازی شود.

## بخش اول: نصب ESXi

بعد از به اتمام رساندن این بخش شما قادر خواهید بود:

- چگونگی نصب ESXi را تشریح نمائید
- از حداقل نیازمندی ها برای پیکربندی Boot From SAN آگاه شوید

## پیش نیازهای سخت افزاری ESXi

**ESXi Hardware Prerequisites****Processor – 64-bit x86 CPU:**

- All AMD Opteron processors
- All Intel Xeon 3000/3200, 3100/3300, 5100/5300, 5200/5400, 5500/5600, 7100/7300, 7200/7400, and 7500 processors
- Up to 160 logical CPUs (cores or hyperthreads)

**Memory – 2GB RAM minimum****One or more Ethernet controllers:**

- Gigabit or 10Gb Ethernet controllers are supported.
- For best performance and security, use separate Ethernet controllers for the management network and the virtual machine networks.

**Disk storage:**

- A SCSI adapter, Fibre Channel adapter, converged network adapter, iSCSI adapter, or internal RAID controller
- A SCSI disk, Fibre Channel LUN, iSCSI disk, or RAID LUN with unpartitioned space: SATA, SCSI, SAS

VMware ESXi نیازمند یک سرور ۶۴ بیتی می باشد (برای مثال Intel Xeon , AMD Opteron, Intel Nehalem). سرور ها می توانند تا ۱۲۸ CPU Logical (Core & Hyperthreads) داشته باشند و همچنین هر هاست می تواند از حداکثر ۵۱۲ Virtual CPU پشتیبانی نماید. همچنین هر سرور نیازمند حداقل ۲ GB حافظه (RAM) می باشد. یک هاست ESXi تا حداکثر 1.0 TB حافظه (RAM) را به صورت سخت افزاری پشتیبانی می کند. هاست ESXi می بایست حتما دارای موارد زیر باشد:

- یک یا چند کارت شبکه فیزیکی
- یک SCSI Controller
- یک RAID Controller
- یک SCSI Disk و یا یک Local RAID LUN

شما می توانید ESXi را بروی SATA Disk Drive , SCSI Drive Disk , SAS Disk Drive نصب و boot نمائید. برای تهیه سخت افزار هاست ESXi، سخت افزار شما می بایست از VMware ESXi پشتیبانی نماید و یا اصطلاحاً VMware Ready باشد.

برای کسب اطلاعات بیشتر در خصوص نصب ESXi می توانید به مقاله ESXi and vCenter Server Setup Guide و مقاله ESXi Embedded and vCenter Server Setup Guide در وب سایت <http://www.vmware.com/> مراجعه نمائید. همچنین برای کسب اطلاعات بیشتر در خصوص حداکثر میزان پیکربندی سخت افزاری و یا نرم افزاری که از طریق

vmware پشتیبانی می گردد می توانید به مقاله Configuration Maximum به نشانی <http://www.vmware.com/support/pubs> مراجعه نمائید.

Installing ESXi 5.0			
Install Option	Required/Optional	Default Selection	Comments
Host name	Required	None	
Install Location	Required	None	Must be at least 5GB if you install the components on a single disk.
Keyboard Language	Optional	U.S. English	
VLAN ID	Optional	None	VLAN ID Range: 0 through 4094
IP Address	Optional	DHCP	Configure a static IP address or use DHCP to configure the network.
Subnet Mask	Optional	Calculated based on IP address	IP address, subnet mask, gateway, and DNS network settings can be changed after installation.
Gateway	Optional	Based on IP address and subnet mask	
Primary DNS	Optional	Based on IP address and subnet mask	Secondary DNS server can also be defined.
Root Password	Optional	None	Must contain between 6 and 64 characters.

در نصب عادی ESXi شما می بایست Bootable CD مربوط به ESXi را در داخل سرور قرار داده و از طریق آن boot نمائید و به سوالات که در حین نصب از شما پرسیده می شود پاسخ دهید و در نهایت ESXi بروی Local Disk نصب نمائید. با استفاده از این روش Target Disk، فرمت شده و پارتیشن بندی می شود و بروی آن ESXi boot image نصب می گردد. اگر شما قبلاً بروی دیسک های سرور، ESXi را نصب نکرده باشید، همه داده هایی که بروی دیسک وجود دارند حذف خواهند شد. این داده ها شامل پارتیشن بندی، سیستم عامل ها و همچنین تمامی فایل های مرتبط با آن می باشد که حذف خواهند شد.

پیش از نصب ESXi، می بایست موارد زیر را در نظر بگیرید:

- در نصب عادی ESXi، Installer به شما در خصوص نیازمندیهای سیستم پیغام می دهد.
- مطمئن شوید که ساعت سیستم بروی UTC تنظیم شده باشد. این تنظیم را می بایست در BIOS سرور انجام شود.
- به قطع بودن Network Storage های خود دقت نمائید. این کار باعث کاهش زمان جستجوی فضای خالی بروی دیسک های موجود می گردد. زمانیکه شما Network Storage را قطع می نمائید، فایل های موجود بروی آن دیگر در دسترس نخواهند بود.

نکته: توجه نمائید نباید LUN های یک SAN Storage را که شامل فایل های نصبی ESXi می باشد را قطع نمائید و همچنین نباید VMware vSphere VMFS Datastore که حاوی فایل های نصبی ESXi دیگری می باشد را قطع نمائید.



اگر شما شروع به نصب ESXi بروی دیسکی که حاوی نصب قبلی از یک ESXi و یا ESX و یا حتی یک VMFS datastore باشد، نمائید، ESXi Installer گزینه هایی را برای Upgrade کردن و Migrate و یا مهاجرت کردن از ESX به ESXi نمایش می دهد و از شما برای نگه داشتن و تغییر ندادن VMFS datastore سوال می نماید.

برای شروع نصب ESXi می بایست مراحل زیر را دنبال نمائید:

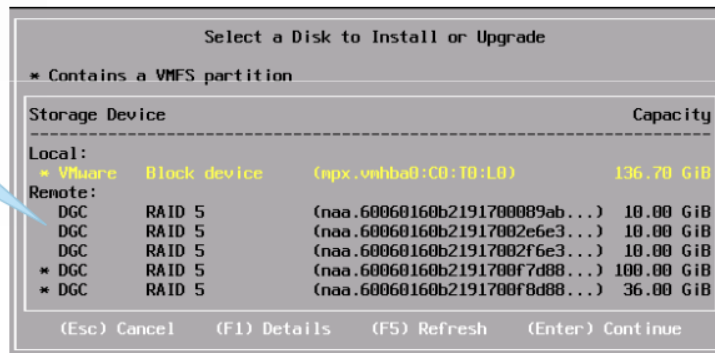
- CD نصب ESXi را در داخل CD\DVD-ROM هاست خود قرار دهید و سپس دستگاه را Restart نمائید.
- BIOS را برای بوت شدن از طریق CD\DVD-ROM تنظیم نمائید.
- سپس مراحل نصب را براساس موارد بالا ادامه دهید.

## Installing ESXi

You must have the ESXi 5.0 ISO file on CD or DVD media.  
Boot from the CD or DVD to start the ESXi installer.

Make sure that you select a disk that is not formatted with VMware vSphere® VMFS.

Choose a volume that has not been formatted with VMFS.



در صفحه انتخاب دیسک، درایوی را که می خواهید ESXi را بروی آن نصب نمایید را انتخاب نمایید و سپس کلید Enter را بزنید. همچنین می توانید با فشار دادن کلید F1 اطلاعاتی را در خصوص دیسک انتخاب شده مشاهده نمایید.

در هنگام انتخاب دیسک دقت نمایید و به ترتیب دیسک ها در لیست نمایش داده شده اعتنا نکنید چراکه ممکن است دیسک دیگری را انتخاب نمایید و اطلاعات قبلی آن در حین نصب پاک گردد. این ترتیب دیسک توسط BIOS تعیین می شود و ممکن است آن ترتیب بندی مورد نظر شما نباشد. برای مثال، زمانیکه شما ESXi را بروی Local Disk نصب می نمایید، Local Disk ممکن است اولین دیسک در لیست نباشد. این مشکل ممکن است بروی سیستم هایی که دارای درایو هایی هستند که بصورت Hot-Swap به دستگاه متصل و یا قطع می شوند رخ دهد. البته اگر دیسکی که انتخاب کرده اید حاوی اطلاعات باشد، صفحه تائید انتخاب دیسک برای شما ظاهر خواهد شد.

همه هاست هایی که ESXi بروی آنها نصب می گردد از فرمت GPT (GUID Partition Table) بجای فرمت MSDOS-Style Partition استفاده می نمایند. با استفاده از این تغییر شما می توانید ESXi را بروی دیسک هایی با حجم بیش از 2.0 TB نیز نصب نمایید.

Partition Table بروی بخشی از ESXi Installer Image قرار دارد و در زمانیکه ESXi نصب می گردد بروی دیسک نوشته می شود. لازم به ذکر است دیسک ها با فرمت VMFS-5 پارتیشن بندی می شوند. ESXi زمانیکه برای اولین بار پس از نصب و یا Upgrade بوت می شود یک Scratch Partition و یک VMFS Partition ها را بصورت خالی ایجاد می نماید. Scratch Partition فضایی در حدود 4.0 GB می باشد و در آن اطلاعاتی در خصوص vm-support output ذخیره می گردد. باقی مانده دیسک نیز با فرمت VMFS-5 فرمت می گردد.

## بوت شدن ESXi از SAN Storage

## Boot from SAN

- ESXi may be booted from SAN.
  - Supported for Fibre Channel SAN
  - Supported for iSCSI and FCoE for certain qualified storage adapters
- SAN connections must be made through a switched topology unless the array is certified for direct-connect.
- The ESXi host must have exclusive access to its own boot LUN.
- Use different LUNs for VMFS datastores and boot partitions.



شما می توانید از **Boot From SAN** در مواقع زیر استفاده نمائید:

- اگر نمی خواهید از **Local Storage** برای نصب ESXi استفاده نمائید.
- اگر می خواهید از سیستم های بدون دیسک همانند **Blade Server** ها استفاده نمائید.

از جمله مزایای **Boot From SAN** می توان به موارد زیر اشاره نمود:

- شما می توانید از سرورهای بدون **Storage** داخلی در تراکم بالا استفاده نمائید چراکه سرور های بدون **Local Disk** اغلب فضای محیطی کمتری را اشغال می کنند.
- شما می توانید سرورهای جدید را از محل قبلی **Boot**، جایگزین و بارگذاری نمائید.
- در صورتیکه **Storage** شما از قابلیت **Array** و یا **Snapshot** بهره مند باشد، می توانید از بوت شدن ESXi در **SAN** پشتیبان تهیه نمائید.
- همچنین شما می توانید از چندین مسیر به **Boot Disk** سرور ESXi دسترسی داشته باشید که بدین ترتیب از دیسک ها در برابر خرابی در یک مسیر محافظت می شود.

توجه: چند مسیر سازی (**Multipathing**) در یک **Boot LUN** تنها برای **Active-Active Arrays** پشتیبانی می شود. در بخش های بعدی این متد را تشریح خواهیم کرد.

برای فعال کردن **Boot from SAN** شما می بایست چندین کار را به صورت صحیح انجام دهید. تفاوت این کارها در پروتکل **Storage** ای است که از آن استفاده می نمائید. **Boot from SAN** از پروتکل های **Storage** زیر پشتیبانی می نماید:

- (Fibre Channel and Fibre Channel over Ethernet)- FCoE
- Hardware iSCSI
- Software and dependent hardware iSCSI

شما می بایست بروی یک SAN LUN به اشتراک گذاشته شده یک Diagnostic Partition پیکربندی نمائید. یک Diagnostic Partition، پارتیشنی است که از چندین هاست، قابل دسترسی است و می تواند اطلاعاتی را در خصوص خطاهای سیستم در آنجا ذخیره نماید.

- اگر بیش از یک هاست ESXi، از یک LUN به عنوان Diagnostic Partition استفاده نماید، آن LUN می بایست در Zone ی قرار گیرد که همه سرورها بتوانند به آن دسترسی داشته باشند. Zone همانند VLAN است و البته در مورد سوئیچینگ Storage ها مطرح می شود.
- هر سرور نیازمند ۱۰۰ مگابایت فضا در Diagnostic Partition می باشد، بدین ترتیب اندازه LUN تعیین می نماید که چه تعداد سرور می تواند از آن استفاده نمایند. هر هاست ESXi به یک Slot قابل شناسایی نگاشت می شود. VMware توصیه می کند اگر سرورها از یک Diagnostic Partition به اشتراک گذاشته شده استفاده می کنند، حداقل شانزده Slot (معادل ۱۶۰۰ مگابایت) از فضای دیسک را باید به آن اختصاص دهید.
- اگر دستگاه ها تنها دارای یک Slot قابل شناسایی باشند، همه هاست های ESXi، اطلاعات خود را در یک Slot به اشتراک می گذارند. این پیکربندی به راحتی می تواند مشکلاتی را بوجود آورد. اگر دو سیستم ESXi یک Core Dump را در یک زمان یکسان اجرا نمایند، Core Dump ها بروی یکدیگر در Diagnostic Partition رونویسی می شوند.
- در زمانیکه شما از iBFT (iSCSI Boot Firmware Table) برای بوت شدن یک هاست ESXi از SAN استفاده می نمائید، شما نمی توانید یک Diagnostic Partition را بروی یک SAN LUN تنظیم نمائید. در عوض، شما می توانید از ابزار vMA (vSphere Management Assistant) برای جمع آوری اطلاعات و Log از هاست ها و ذخیره آنها برای تجزیه و تحلیل استفاده نمائید.

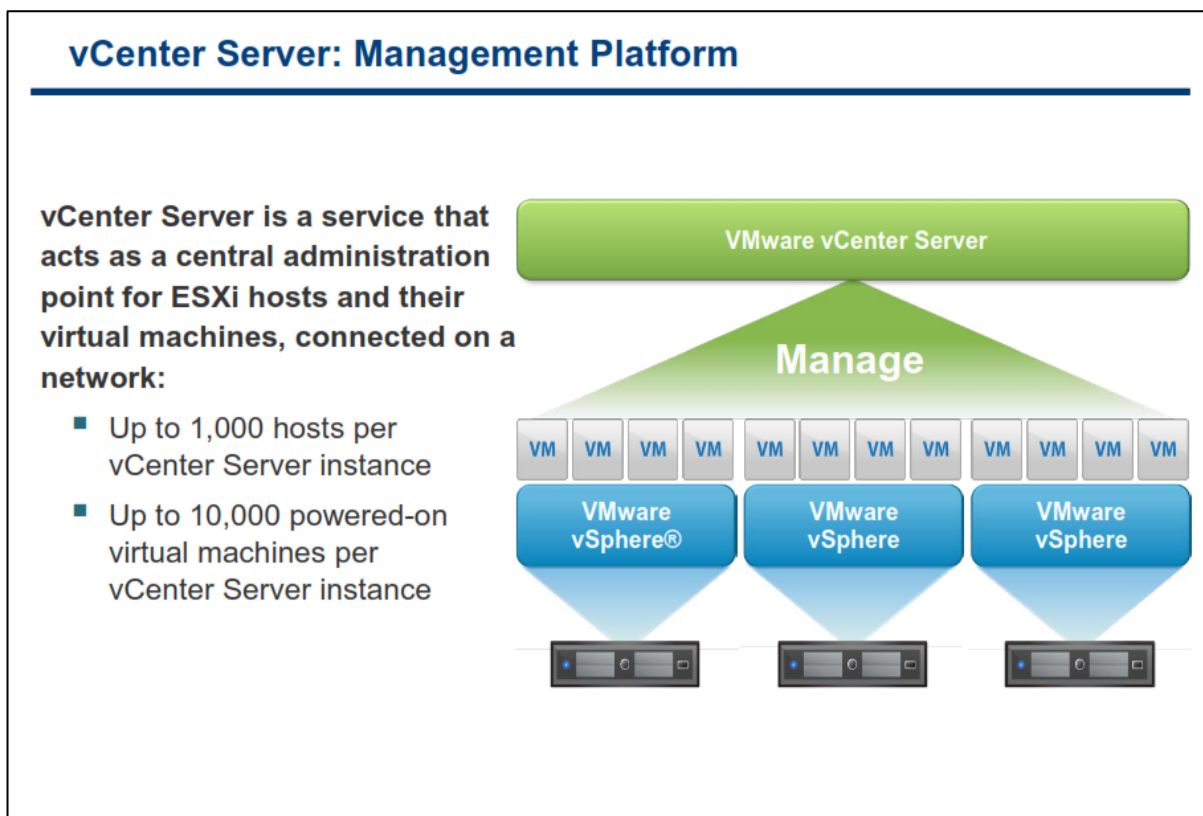
برای کسب اطلاعات بیشتر در خصوص پیکربندی Boot From SAN با استفاده از FC, FCoE, iSCSI می توانید به مقالاتی در این موضوع به آدرس <http://www.vmware.com/support/pubs> استفاده نمائید.

## بخش دوم: معماری vCenter Server

بعد از به اتمام رساندن این بخش شما قادر خواهید بود:

- معماری vCenter Server را تشریح نمایید
- نحوه برقراری هاست های ESXi با vCenter Server را تشریح نمایید
- ماژول ها و کامپوننت های vCenter Server را شناسایی نمایید

## vCenter Server به عنوان یک پلتفرم مدیریت

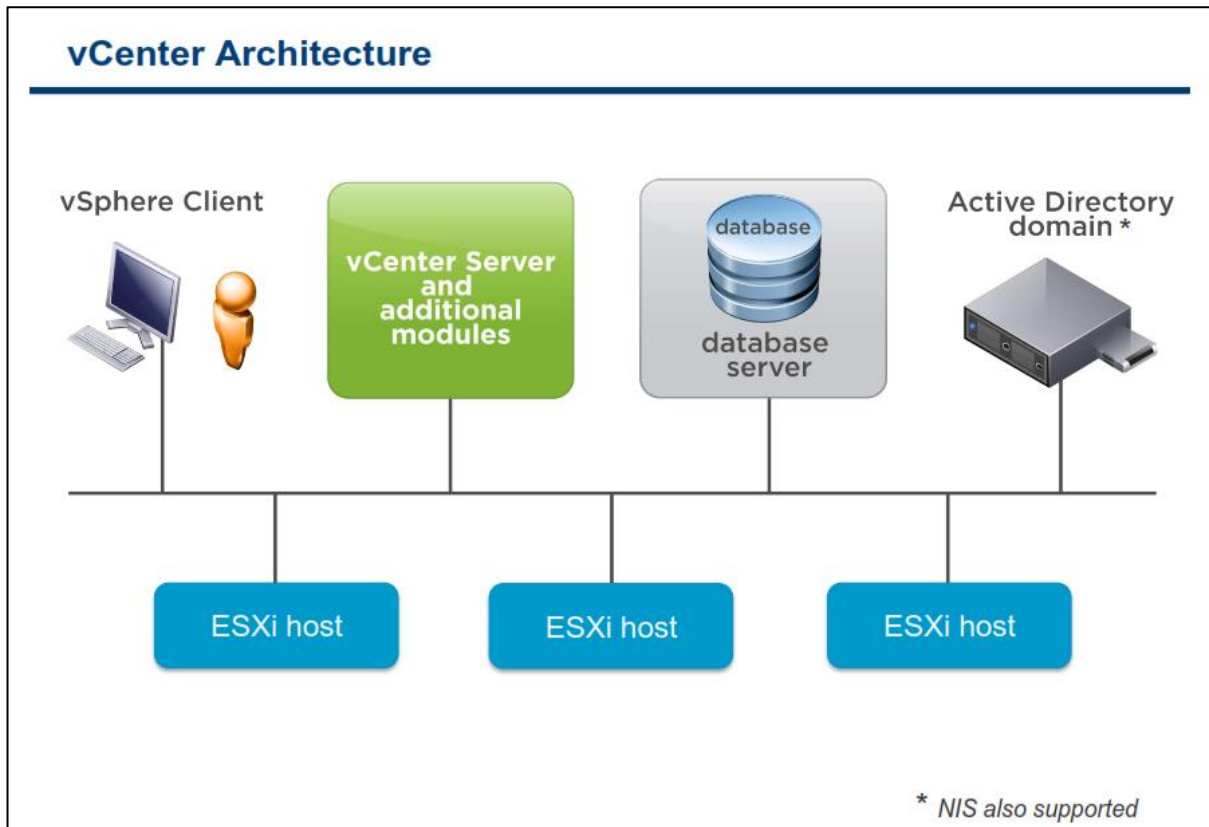


vCenter سرویسی است که از آن برای مدیریت مرکزی هاست های ESXi و vm های آنها در صورتیکه این هاست ها به شبکه متصل باشند، استفاده می گردد. با استفاده از این سرویس شما می توانید اقدامات مورد نیاز خود را بروی vm و هاست بصورت مستقیم انجام دهید. vCenter شامل ماژول ها و سرویس های متعددی می باشد که شما می توانید از آنها بهرمنند شوید. شما می توانید vCenter را هم بروی سیستم عامل های ویندوزی پشتیبانی شده نصب نمائید و هم از Appliance مبتنی بر سیستم عامل لینوکس که شرکت VMware برای شما تدارک دیده است استفاده نمائید. vCenter قابلیت های متعددی را برای شما فراهم می آورد که از جمله آن می توان به قابلیت Distributed Resource Scheduler (DRS) و یا زمانبند منابع توزیع شده، قابلیت High Availability(HA) و یا همان حداکثر دسترسی، قابلیت Fault Tolerance(FT) و قابلیت vMotion اشاره نمود.

هر سرویس vCenter Server می تواند تا حداکثر ۱۰۰۰ هاست ESXi را پشتیبانی و مدیریت نماید. از طرف دیگر vCenter Server می تواند از حداکثر ۱۰۰۰۰۰ vm بصورت و روشن پشتیبانی و همچنین از حداکثر ۱۵۰۰۰۰ vm بصورت ریجستر شده و خاموش پشتیبانی نماید.

شما می توانید چندین vCenter را با استفاده از قابلیت Linked Mode Group به یکدیگر متصل نمائید. بدین ترتیب شما می توانید با ورود به یک vCenter از سایر اطلاعاتی که در vCenter های دیگر وجود دارد اطلاع حاصل نمائید و آنها را مدیریت نمائید. در نتیجه شما می توانید از هاست ها و vm های بیشتری نیز بدین ترتیب استفاده نمائید.

## معماری vCenter



معماری و یا ساختار vCenter متکی به موارد زیر می باشد:

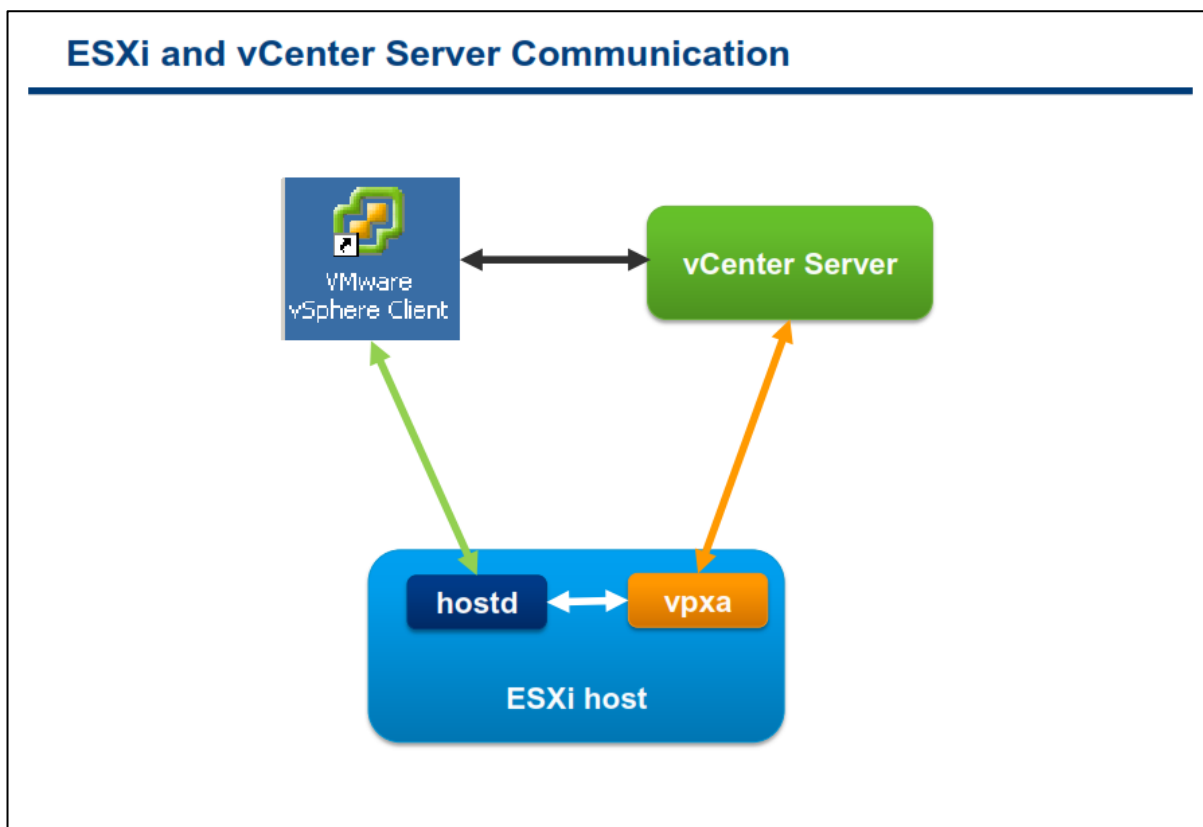
**vSphere Client:** شما از ابزار vSphere Client علاوه بر مدیریت هاست ESXi برای مدیریت vCenter نیز می توانید استفاده نمائید و به آن متصل شوید. اگر هاست ESXi را در داخل vCenter بصورت مدیریت شده وارد نمائید، از آن پس مدیران می بایست همیشه از vCenter برای مدیریت هاست ها استفاده نمایند.

**vCenter Server Database:** حیاتی ترین کامپوننت vCenter پایگاه داده (Database) آن می باشد. در Database اطلاعاتی از قبیل Inventory Items , Security Role , Resource Pool, Performance Data و سایر اطلاعات حیاتی برای vCenter نگهداری می شود.

**Active Directory Domain:** امنیت در vCenter براساس Windows Security تعیین شده است. در حالت عادی vCenter به Active Directory نیازی ندارد ولی در صورتیکه سرور vCenter عضوی از Domain باشد، کاربران و گروه های Active Directory در دسترس vCenter قرار خواهد داشت و می تواند از آنها استفاده نماید. ولی اگر vCenter عضوی از Domain نباشد vCenter از Local Windows Users & Group استفاده می نماید. و یا در صورتیکه از Virtual Appliance استفاده می نمائید می بایست از نام کاربری که در لینوکس تعریف می شود همانند root استفاده نمائید.

**Managed Hosts:** نرم افزار vCenter به شما این اجازه را میدهد که ESXi را به خوبی VM هایی که بروی آن در حال اجرا هستند مدیریت کنید.

## ارتباط ESXi و vCenter Server



همانطور که در اسلاید بالا مشاهده می‌نمائید، vCenter از طریق یک Agent (که بروی ESXi قرار دارد) بنام vpxa به هاست ESXi دسترسی و با آن ارتباط برقرار می‌کند. زمانیکه هاست به vCenter اضافه می‌شود vpxa بروی ESXi شروع به کار می‌کند. vpxa با سرویس هاست که بنام hostd شناخته می‌شود ارتباط برقرار می‌کند و بدین ترتیب دستورات و فرامین را برای هاست ESXi ارسال می‌کند.

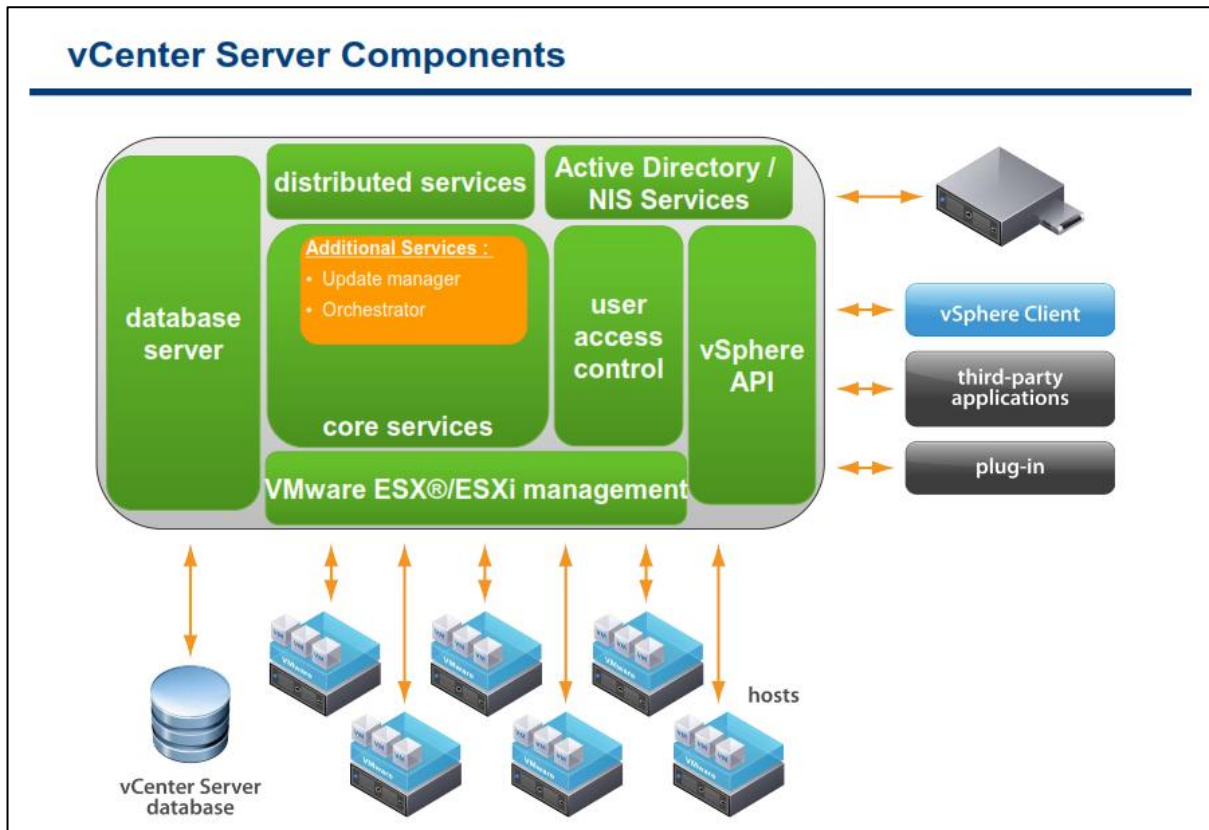
hostd به صورت مستقیم بروی ESXi اجرا می‌شود و مسئول مدیریت اکثر عملیات ها بروی هاست ESXi می‌باشد. این سرویس از وضعیت همه vm ها و منابع ذخیره سازی که برای ESXi مشخص شده اند، آگاه است. اکثر دستورات و پیام ها از طریق vCenter به hostd انتقال پیدا می‌کنند که از جمله آن می‌توان به ایجاد، انتقال و یا روشن کردن vm و غیره اشاره نمود.

vpxa به عنوان یک واسطه میان vpxd که بروی vCenter اجرا می‌شود و hostd که بروی ESXi قرار دارد عمل می‌کند و برای رله کردن و یا روانه کردن دستورات و کارها بروی ESXi استفاده می‌شود.

زمانیکه شما به vCenter Server با استفاده از vSphere Client متصل می‌شوید، دستورات را از طریق vpxa به هاست ESXi انتقال می‌دهد و vCenter Database نیز بروز رسانی می‌شود و اطلاعاتی نیز در آن نوشته می‌شود ولی اگر شما مستقیماً از طریق vSphere Client به ESXi متصل شوید این ارتباط مستقیماً به hostd متصل می‌شود و vCenter Database بروز رسانی نمی‌شود و اطلاعات و Log ها نیز در آن نوشته نمی‌شود.



## کامپوننت های vCenter Server



vCenter Server شامل سرویس ها و کامپوننت های زیر می باشد:

**Core Service:** این سرویس شامل مدیریت منابع، مدیریت vm ها، زمانبندی کارها، Log های آماری، مدیریت آلام و رخدادها (Event)، ایجاد vm و همچنین و پیکربندی vm و هاست می باشد.

**Distributed Service:** این سرویس نیز شامل قابلیت های HA, DRS, vMotion که همراه با vCenter Server نصب می گردند.

**Additional Service:** شامل پکیج های مجزایی هستند که نیاز به نصب جداگانه ای بروی vCenter Server دارند اما نیاز به لایسنس جداگانه ای ندارند. همانند vCenter Converter که برای تبدیل ماشین های فیزیکی به مجازی استفاده می شود و یا همچنین vCenter Update که برای به روز رسانی بخش های متعدد VMware vSphere استفاده می گردد.

**Database Interface:** این سرویس نیز دسترسی به vCenter Database را فراهم می کند.

**Active Directory Interface:** این سرویس دسترسی به کاربران و گروه های Active Directory را فراهم می کند.

**VMware vSphere API:** این سرویس نیز با vSphere SDK ترکیب می شود و یک واسط را برای نوشتن برنامه های سفارشی برای دسترسی به vCenter فراهم می کند.

## Additional vCenter Server Modules

Optional vCenter Server modules (plug-ins) provide additional features to vCenter Server.

### Examples:

- VMware vSphere Update Manager
- VMware Site Recovery Manager™ Plug-In
- VMware Data Recovery

These modules include a server component and a client component:

- The client component is a plug-in available for download and installation to the VMware vSphere® Client™ after the server component is installed in vCenter Server.
- The client component alters the interface by adding items related to the enhanced functionality.

ماژول های vCenter Server یا همان Plug-ins برنامه هایی هستند که قابلیت های متعددی را فراهم می آورند.

معمولا ماژول ها شامل یک بخش سرور و یک بخش کلاینت می باشند. بعد از اینکه بخش سرور یک ماژول نصب گردید و در vCenter Server ریجستر گردید بخش کلاینت آن نیز برای دانلود و نصب بروی vSphere Client در دسترس قرار خواهد گرفت. بدین معنی که شما می توانید آن را بطور جداگانه بروی کامپیوتری که vSphere Client را نصب نموده اید دانلود و نصب نمایید و از قابلیت هایی که این ماژول در اختیار شما قرار می دهد استفاده نمایید. زمانیکه که ماژول را بطور کامل نصب می نمایید بسته به قابلیت هایی که برای شما فراهم می آورد ممکن است یک سربرگ (tab) و یا نما (view) و یا منویی به نرم افزار vSphere Client اضافه گردد.

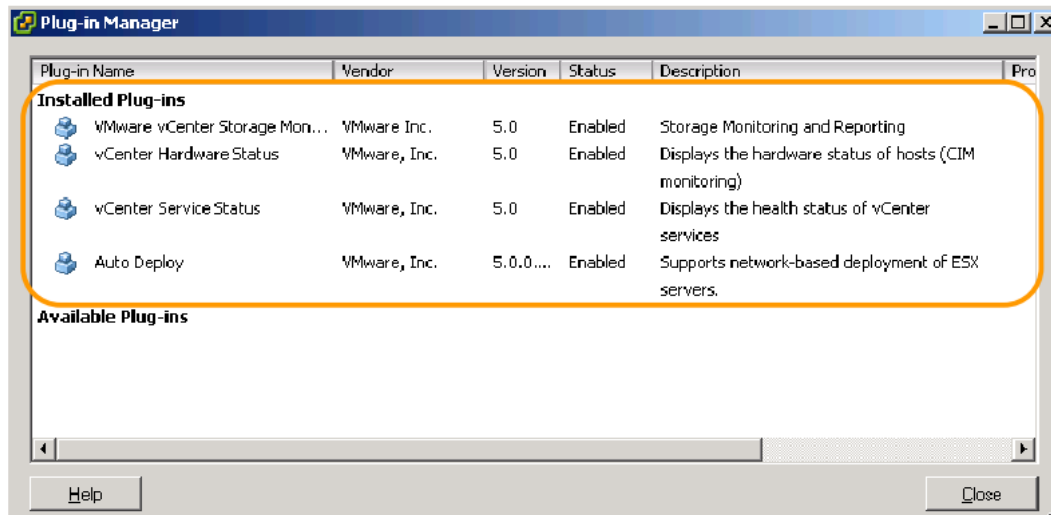
این ماژول ها از قابلیت های Core vCenter همانند احراز هویت و مدیریت دسترسی ها و غیره استفاده می کنند اما با این وجود می توانند دسترسی ها، وظایف، رخدادهای خودشان را داشته باشند. برای استفاده از ماژول ها حتما می بایست vCenter Server را نصب نمایید. توجه داشته باشید که ماژول ها و vCenter می توانند به صورت جداگانه بروزرسانی گردند.

## ماژول های پیش فرض vCenter Server

## Default vCenter Server Plug-Ins

vCenter Server is installed with a set of default plug-ins.

To install a new plug-in, use the Plug-in Manager in the vSphere Client.



vCenter Server دارای سه ماژول می باشد که بطور پیش فرض نصب و فعال گردیده اند:

- **vCenter Storage Monitoring**: این ماژول به vCenter Server اجازه می دهد که از منابع ذخیره سازی (Storage) گزارش گیری و آنها را مانیتور نماید. این ماژول سربرگ **Storage View** مربوط به هاست را در vSphere Client ایجاد می کند.
- **vCenter Service Status**: این ماژول یک آیکن **vCenter Service Status** را به پنل **Administration** در vSphere Client اضافه می کند. برای مشاهده وضعیت صحت عملکرد (Health) می توانید به مسیر **Home - Administration -> vCenter Service Status** مراجعه نمایید.
- **vCenter Hardware Status**: این ماژول در vCenter به شما وضعیت سخت افزاری هاست را نمایش می دهند. این ماژول سربرگ **Hardware Status** را به vSphere Client هاست اضافه می کند.

در بخش **plug-ins** همچنین شما می توانید ماژول های نصب شده را مشاهده نمایید. برای دیدن آنها می توانید به مسیر **plug-in->Manage Plug-ins** در vSphere Client مراجعه نمایید.

بعد از اینکه بخش سرور یک ماژول را بروی vCenter Server نصب کردید می توانید بخش کلاینت آن را از بخش **Plug-ins Manager** دانلود و نصب نمایید.

اما برخی از ماژول هایی که ممکن است نیازمند خرید لایسنس باشند عبارتند از:

- Site Recovery
- Data Recovery
- vCenter CapacityIQ
- AppSpeed Server
- Update Manager
- vCenter Orchestrator

این لیست شامل ماژول هایی که توسط سایر شرکت ها طراحی شده اند نمی باشد. شما می توانید سایر ماژول هایی که توسط شرکت های ثالث طراحی شده اند را طریق وب سایت [www.vmware.com](http://www.vmware.com) بررسی نمائید و در صورتیکه در مدیریت هرچه بهتر محیط مجازی به شما کمک کند آن را خریداری و نصب نمائید.

## بخش سوم: نصب vCenter Server - نسخه ویندوز


بعد از به اتمام رساندن این بخش شما قادر خواهید بود:

- حداقل نیازمندی ها برای نصب VMware vCenter Server را بشناسید
- vCenter Server را بروی سیستم عامل های ویندوزی پشتیبانی شده نصب نمایید


## گزینه های پیاده سازی vCenter Server

### vCenter Server Deployment options

physical host




-OR-



virtual machine

---



Linux based

- Deployed on physical host or virtual machine and installed with a supported version of Windows.
- Reasons to use Windows-based vCenter Server instead of the vCenter Server virtual appliance
  - Support staff trained only on Windows operating systems
  - Applications that depend on a specific Windows version
  - Prefer to use a physical host

---

- Deployed as a virtual appliance that runs the SuSE Linux operating system
  - No operating system license required
  - Simple configuration using web browser
  - Offers same user experience as Windows based version

vCenter Server می تواند بروی یک ماشین فیزیکی و یا بروی یک ماشین مجازی اجرا شود. زمانیکه vCenter Server را بروی یک ماشین فیزیکی به اجرا در می آورید:

- به یک سرور فیزیکی مستقل نیاز دارید.
- vCenter Server در معرض از کار افتادن خواهد بود. چراکه تنها بروی یک سیستم فیزیکی به اجرا در می آید.
- کارایی vCenter Server تنها محدود به سیستم سخت افزاری می شود.

اما زمانیکه vCenter Server را بروی یک ماشین مجازی به اجرا در می آورید:

- نیازی به یک سرور فیزیکی مستقل نیست.
- vCenter Server در معرض از کار افتادن نخواهد بود.
- یک نمونه از vCenter Server می تواند در حین تعمیر و نگهداری از یک هاست به هاست دیگری مهاجرت کند.
- vCenter Server می بایست برای دریافت منابع با سایر ماشین های مجازی رقابت کند.

## نیازمندیهای سخت افزار و نرم افزار vCenter Server

**vCenter Server Hardware and Software Requirements****Hardware requirements (physical or virtual machine):**

- Number of CPUs – Two 64-bit CPUs or one 64-bit dual-core processor
- Processor – 2.0GHz or higher Intel or AMD processor\*
- Memory – 4GB RAM minimum\*
- Disk storage – 4GB minimum\*
- Networking – Gigabit connection recommended
- \* Higher if database runs on the same machine

**Software requirements:**

- 64-bit operating system is required.
- See “vSphere Compatibility Matrixes.”

سخت افزار vCenter Server می بایست دارای حداقل نیازمندی های زیر باشد:

- تعداد CPU : دو CPU 64-bit و یا یک CPU Dual-Core 64-bit
- پردازنده: یک پردازنده Intel و یا AMD با فرکانس 2.0 Ghz و یا بالاتر
- حافظه (RAM): 4.0 GB
- حداقل فضای دیسک فیزیکی: 4.0 GB
- شبکه : یک اتصال یک Gigabit و یا حداقل ۱۰۰ Megabit

اگر دیتابیس vCenter Server نیز بروی همان ماشین نصب شود، نیازمندی های پردازنده ، حافظه و دیسک نیز می بایست افزایش پیدا کند. همچنین این نیازمندی ها بسته به تعداد ماشین های مجازی و هاست هایی که مدیریت می شوند می بایست افزایش پیدا کند. برای مثال برای مدیریت بیش از هزار هاست و ده هزار ماشین مجازی روشن، vCenter Server می بایست دارای ۸ هسته و 16.0 GB حافظه و 10.0 GB فضای دیسک باشد.

مطمئن شوید که vCenter Server از سیستم عامل شما پشتیبانی می کند. vCenter Server نیازمند یک سیستم عامل 64-bit و همچنین یک 64-bit Database Source Name (DSN) برای اتصال vCenter Server به دیتابیس می باشد.

vCenter Server نیازمند Microsoft .NET 3.5 Framework می باشد. اگر این ابزار بروی سیستم شما نصب نشده است، با استفاده از DVD نصب برنامه vCenter Server می توانید آن را نصب نمایید. توجه داشته باشید که برای نصب .NET 3.5 SP1 ممکن است به اینترنت نیاز داشته باشید تا فایل دیگری را برای نصب دانلود نماید.

اگر شما می خواهید از دیتابیس Microsoft SQL Server 2008 R2 Express برای vCenter Server استفاده نمائید، می بایست Microsoft Windows Installer version 4.5 یا همان MSI 4.5 بروی سیستم نصب گردد. شما می توانید MSI 4.5 را از سایت مایکروسافت دانلود نمائید. همچنین شما می توانید MSI 4.5 را مستقیماً از DVD برنامه نصب vCenter Server و از طریق Autorun آن نصب نمائید.

vCenter Server و IIS هر دو از پورت ۸۰ به عنوان پورت پیش فرض برای اتصالات HTTP استفاده می کنند. این تداخل می تواند باعث ایجاد مشکل در سرویس vCenter Server بعد از نصب سرویس vSphere Authentication Proxy گردد. برای حل این تداخل میان IIS و vCenter Server می بایست این اقدامات را انجام دهید:

- اگر IIS قبل از نصب vCenter Server نصب شده باشد:
  - پورت vCenter Server را از پورت ۸۰ به پورت دیگری تغییر دهید.
- اما اگر vCenter Server قبل از نصب IIS نصب شده باشد:
  - قبل از Restart و یا راه اندازی مجدد vCenter Server پورت پیش فرض IIS را به پورت دیگری تغییر دهید.



## نیازمندیهای دیتابیس vCenter

**vCenter Database Requirements**

Each vCenter Server instance must have a connection to a database to organize all the configuration data.

**Supported databases:**

- Microsoft SQL Server 2005 SP3 (required)
  - SP4 recommended
- Microsoft SQL Server 2008 R2 Express
  - Microsoft SQL Server 2008
- Oracle 10g R2 and 11g
- IBM DB2 9.5 and 9.7

**Default database – Microsoft SQL Server 2008 Express:**

- Bundled with vCenter Server
- Used for product evaluations and demos
- Also used for small deployments (up to five hosts and 50 virtual machines)

vCenter Server برای ذخیره و سازماندهی سرور ها نیازمند یک دیتابیس است. vCenter Server از دیتابیس SQL Server و Oracle و IBM BD2 پشتیبانی می نماید. شما می بایست دارای یک دسترسی Administration Credential برای Login به این دیتابیس ها باشید.

همچنین شما می توانید از دیتابیس نهادینه شده Microsoft SQL Server 2008 R2 Express که در برنامه Installer vCenter Server است، استفاده نمائید. از این دیتابیس می توانید برای پیاده سازی vSphere در سطح کوچک و برای حداکثر ۵ هاست و ۵۰ ماشین مجازی استفاده نمائید.

VMware Update Manager نیز نیازمند یک دیتابیس می باشد. Update Manager می تواند از دیتابیس vCenter Server استفاده نماید. اما VMware توصیه می نماید که از یک دیتابیس برای vCenter Server و از یک دیتابیس دیگر برای Update Manager استفاده نمائید. البته برای پیاده سازی های کوچک نیاز به یک دیتابیس مجزا برای Update Manager نیست.

## محاسبه اندازه دیتابیس

### Considerations for Calculating the Database Size

Number of hosts	50	<p><b>Use the vCenter Server 5.x Database Sizing Calculator:</b></p> <ul style="list-style-type: none"> <li>■ For Microsoft SQL Server and Oracle</li> </ul> <p><b>Or use the what-if calculator built into vCenter Server.</b></p>	
Number of virtual machines	300		
Number of clusters	10		
Number of resource pools	50		
Number of datastores	50		
Number of datacenters	8		
Number of root folders	1		
Average number of network devices per host			2
Average number of network devices per virtual machine			1
Average number of disk devices per host			10
Average number of disk devices per virtual machine			4
Average number of CPUs per host			4
Average number of virtual CPUs (vCPUs) per virtual machine			2
Number of device types per virtual machine for datastore statistics			4
Average number of debugging statistics or devices			1000

	Number of Samples Collected Every 5 Minutes	Potential DB Size in Gigabytes at the End of 1 Year	+15%	-15%	Space Required for Temporary DB
Statistics Collection Level 1	8992	2.5	2.9	2.2	2.5
Statistics Collection Level 2	18972	5.4	6.2	4.6	5.4
Statistics Collection Level 3	44072	12.5	14.4	10.6	12.5
Statistics Collection Level 4	70432	20.0	22.9	17.0	20.0

اندازه دیتابیس بسته به تعداد ماشین های مجازی، هاست و داده هایی که می بایست ذخیره شوند متغیر می باشد. VMware برای شما ابزاری را فراهم کرده است که با استفاده از آن می توانید اندازه دیتابیس خود را تخمین بزنید.

VMware vCenter Server 5.x Database Sizing Calculator یک فایل اکسل می باشد که با استفاده از آن می توانید اندازه دیتابیس vCenter Server را تخمین بزنید. البته این تخمین را می توانید برای دیتابیس های همچون Oracle و Microsoft SQL Server انجام دهید. این تخمین اندازه، براساس اطلاعاتی که شما وارد می نمائید (همچون تعداد هاست و ماشین های مجازی) محاسبه می شود.

vCenter Server همچنین دارای امکانی می باشد که شما با استفاده از آن می توانید بصورت Built-in اندازه دیتابیس خود را براساس تعداد ماشین های مجازی و هاست ها و همچنین بازه زمانی که اطلاعات و گزارشات ذخیره می شوند، تخمین و محاسبه نمائید. این بازه های زمانی مشخص می کند که شما به چه صورت اطلاعات را (Statistics Level) و برای چه مدتی (Keep for) و هر چند مدت (Interval Duration) می خواهید ذخیره نمائید. برای مشاهده این بخش می بایست به بخش vCenter Server Setting -> Administration رفته و گزینه Statistics را از پنل سمت چپ انتخاب نمائید. توجه نمائید که با تغییر دادن این پارامتر ها هیچ تغییری در اندازه دیتابیس شما ایجاد نخواهد شد.

برای دریافت فایل اکسل Database-Sizing Spreadsheet به منظور محاسبه اندازه دیتابیس Oracle و Microsoft SQL Server می بایست به آدرس <http://www.vmware.com/support/pubs> مراجعه نمائید.

## پیش از نصب vCenter Server

**Before Installing vCenter Server**

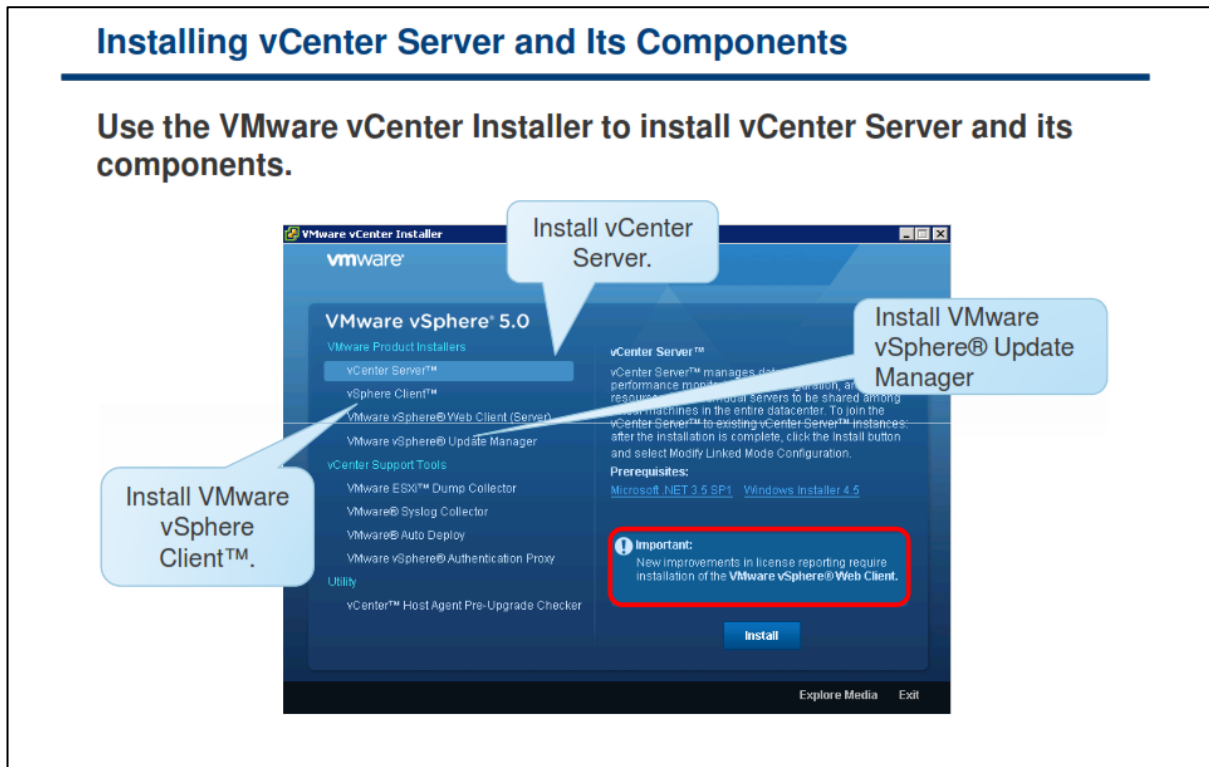
**Before beginning the vCenter Server installation, make sure that the following prerequisites are met:**

- Ensure that vCenter Server hardware and software requirements are met.
- Ensure that the vCenter Server system belongs to a domain rather than a workgroup.
- Create a vCenter Server database, unless you are using the default database.
- Obtain and assign static IP address and host name to the vCenter Server system.

پیش از شروع فرایند نصب vCenter Server شما می بایست از فراهم آوردن پیش نیازهای آن اطمینان حاصل نمائید:

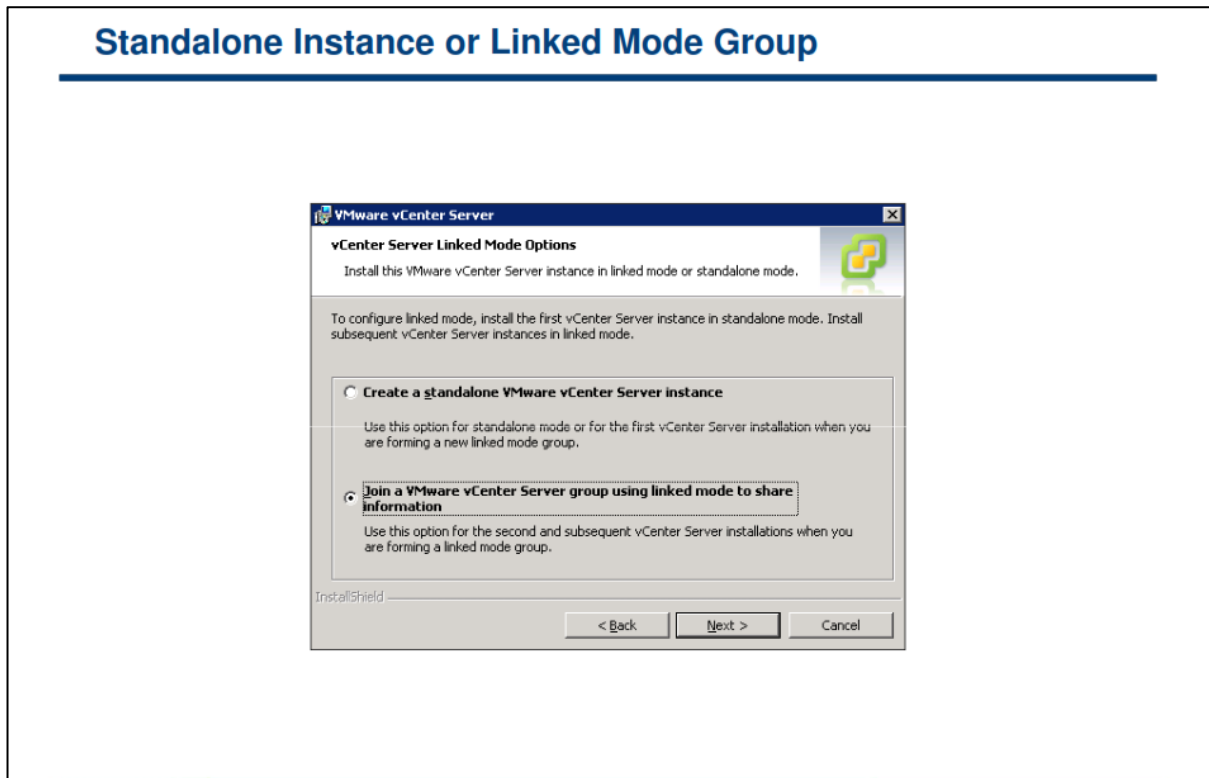
- سیستم شما می بایست حداقل نیازمندی های سخت افزاری و نرم افزاری را دارا باشد.
- سیستم می بایست به Domain سازمان Join گردد. در صورتیکه این سیستم بصورت Workgroup استفاده می شود، vCenter Server شما قادر به مشاهده سایر سیستم های موجود در Domain در زمانیکه از قابلیت Guided Consolidation استفاده می کند، نخواهد بود. (Guided Consolidation ابزاری است که با استفاده از آن می توانید عملیات تبدیل ماشین های فیزیکی به مجازی را براساس توصیه ها و تحلیل های VMware انجام دهید)
- یک دیتابیس برای vCenter Server ایجاد نمائید. در صورتیکه می خواهید از SQL Server 2008 Express استفاده نمائید نیازی به این کار نیست.
- برای Windows Server که قرار است بروی آن vCenter Server نصب نمائید می بایست Host Name و IP Address و FQDN Name مناسبی در نظر بگیرید تا از طریق DNS Server داخلی امکان دستیابی هاست های ESXi به آن وجود داشته باشد.
- شما می توانید از یک Firewall بروی vCenter Server استفاده نمائید اما پیش از آن می بایست از دسترسی هاست های ESXi به vCenter Server اطمینان حاصل نمائید.

## نصب vCenter Server و کامپوننت های آن



برای نصب vCenter Server و کامپوننت های آن می بایست از VMware vCenter Installer استفاده نمائید. VMware vCenter Installer به شما امکان می دهد که نرم افزارهای vCenter Server، vSphere Client و کامپوننت های vCenter Server را نصب نمائید. برای اجرای Installer می بایست فایل autorun.exe را از CD\DVD آن اجرا نمائید.

## نصب vCenter Server در حالت Standalone Instance و یا Linked Mode Group



در یک گروه Linked Mode، هر کاربر vCenter Server می تواند سایر نمونه های vCenter Server را که به آنها دسترسی دارد را مشاهده نماید.

زمانیکه برای اولین بار گروه vCenter Server Linked Mode را تنظیم می نمائید، شما می بایست اولین vCenter Server را بصورت Standalone نصب نمائید چراکه هنوز هیچ vCenter Server دیگری برای Join وجود ندارد. نمونه های ثانویه vCenter Server می تواند به اولین vCenter Server و یا دیگر نمونه های vCenter Server که به گروه Linked Mode متصل و یا Join شده اند Join شوند. (همانند اسلاید بالا)

برای اتصال یک vCenter Server به یک گروه Linked Mode حتما می بایست vCenter Server ها عضوی از Domain باشند. البته User Domain های این سرورها می بایست به عنوان Administrator در Domain تعریف شوند.

نمونه های vCenter Server در یک گروه Linked Mode نیازی به داشتن یک User Domain یکسان ندارند. نمونه ها می توانند با Domain Account مختلف اجرا شوند. بطور پیش فرض این نمونه ها با System Account داخلی سیستمی که vCenter Server بروی آن نصب شده است اجرا می شوند.

در حین نصب vCenter Server اگر شما IP Address یک نمونه دیگری از vCenter Server را وارد نمائید، Installer آن IP Address را به FQDN تبدیل می کند.

نکته: برای اینکه Linked Mode Replication آماده کار باشد، DNS می بایست در شبکه شما عملیاتی شده باشد.

## vCenter Server Installation Wizard

The vCenter Server Installation wizard asks for the following data.

Parameter	Description
User name and organization	User identification
License key	Evaluation or valid license key
Database information	Default database or remote database connection information
SYSTEM account information	User for running the vCenter Server service
Destination folder	Software location
Standalone or join a Linked Mode group	Standalone instance or enable two or more vCenter Server inventories to be visible from the vSphere Client
Ports	Ports used for communicating with client interfaces and managed hosts
JVM memory	JVM memory configuration for the vCenter Server Web service
Ephemeral port configuration	Select if vCenter Server will manage hosts that power on more than 2000 virtual machines simultaneously

برای آغاز نصب vCenter Server، می بایست بروی لینک vCenter Server در پنجره اصلی VMware vCenter Installer کلیک نمائید. ویژارد نصب vCenter Server اطلاعات زیر را از شما درخواست می کند:

- **User name** و **Organization Name** و **کلید لایسنس**: اگر کلید لایسنس را در این ویژارد وارد نکنید، vCenter Server در حالت آزمایشی نصب می گردد. بعد از نصب، شما می توانید با استفاده از vSphere Client لایسنس vCenter Server را وارد نمائید.
- **اطلاعات دیتابیس**: صفحه گزینه های دیتابیس vCenter Server Installer این امکان را برای شما فراهم می آورد که یا دیتابیس پیش فرض را انتخاب نمائید و یا دیتابیس های پشتیبانی شده ای را که قبلا در مورد آن بحث نموده ایم را انتخاب کنید. اگر انتخاب شما، استفاده از یک دیتابیس SQL Server می باشد، شما می بایست یک **Data Source Name** یا **DSN** ایجاد نمائید. **DSN** حاوی اطلاعات خاصی در خصوص دیتابیس هایی است که برای اتصال به آن نیاز به **ODBC Driver** است. اگر از دیتابیس های پشتیبانی شده موجود استفاده نمائید، شما می بایست **Username** و **Password** ورود به این دیتابیس ها را وارد نمائید.
- **حساب کاربری SYSTEM Account** و **یا برخی از حساب های کاربری**: صفحه **vCenter Server Service** اطلاعاتی را در خصوص **Windows SYSTEM Account** یا یک حساب کاربری خاص برای اجرای سرویس vCenter Server از شما دریافت می کند. این اطلاعات همان **Username** و **Password** یک حساب کاربری می باشند. دلیل اصلی استفاده از حساب های کاربری خاص در واقع استفاده از احراز هویت **Windows** برای **SQL Server** می باشد. البته امنیت نیز دلیل دیگری برای این موضوع می باشد. **Built-in SYSTEM Account** دارای حق دسترسی بیشتری برای نیازهای vCenter Server بروی سیستم می باشد که می توان از آن برای



برطرف کردن مشکلات امنیتی استفاده نمود. حتی اگر شما نمی خواهید از Windows Authentication برای SQL Server استفاده نمائید و یا اگر شما می خواهید از دیتابیس Oracle استفاده نمائید، شما می توانید از Local Account برای vCenter Server استفاده نمائید. تنها شرطی که Local Account می بایست داشته باشد این است که باید عضوی از گروه Local Administrator آن سیستم باشد.

- تعیین مسیر نصب نرم افزار: شما می توانید مسیر نصب نرم افزار را در این بخش تغییر دهید.
- نصب یک نمونه Standalone vCenter Server و یا Join نمودن آن به یک گروه Linked Mode: اگر نمونه ای از vCenter Server را برای اولین بار در محیط مجازی خود نصب می نمائید می بایست آن را به صورت Standalone vCenter Server نصب نمائید. یک گروه Linked Mode به شما این امکان را می دهد تا بتوانید آبجکت های موجود در چندین نمونه vCenter Server را مدیریت و مشاهده نمائید.
- vCenter Port: سرور vCenter می بایست قادر به به ارسال داده به هر هاست مدیریت شده و دریافت داده از هر رابط های کاربری باشد. VMware از پورت های زیر برای برقراری ارتباط استفاده می کند: پورت ۴۴۳ (HTTPS) ، پورت ۸۰ (HTTP) ، پورت ۹۰۲ (UDP Heartbeat) ، پورت ۸۰۸۰ (Web Service HTTP) ، پورت ۸۴۴۳ (Web Service HTTPS) ، پورت ۶۰۰۹۹ (Web Service Change Service Notification) ، پورت ۳۸۹ (LDAP) و پورت ۶۳۶ (SSL). در صورتیکه دلیل دیگری برای تغییر پورت ها وجود نداشته باشد، پیشنهاد می شود از پورت های پیش فرض استفاده نمائید.
- حافظه JVM: سرور vCenter حاوی سرویسی بنام VMware VirtualCenter Management Webservices می باشد. این سرویس نیازمند یک الی چهار گیگابایت فضای اضافی بروی RAM است. برای پیکربندی اختیاری WebService، شما می توانید در حین نصب، حداکثر حافظه JVM را براساس تعداد آبجکت ها برای WebService تعیین نمائید. برای مثال اگر شما دارای آبجکت های کمی باشید (کمتر از ۱۰۰ هاست)، اندازه حافظه JVM را می بایست ۱۰۲۴ مگابایت انتخاب نمائید و اگر شما دارای آبجکت های بیشتری باشید (بیش از ۴۰۰ هاست)، اندازه حافظه JVM را می بایست ۴۰۹۶ مگابایت انتخاب نمائید.
- پیکربندی پورت های موقت (Ephemeral Port): با استفاده از این قابلیت پورت های موقتی در یک محدود خاص و در زمان مورد نیاز برای مدیریت هاست هایی که دارای ماشین های مجازی زیادی می باشند ایجاد می گردد. بدین ترتیب از ارسال و دریافت انبوهی از اطلاعات به یک پورت خاص جلوگیری به عمل می آید و برای هر ارتباط یک پورت دینامیک ایجاد و پس از خاتمه آن پورت بسته می شود.

برای کسب اطلاعات بیشتر در خصوص نصب vCenter Server، به مقاله ESXi and vCenter Server Setup Guide در وب سایت <http://www.vmware.com/support/pubs> مراجعه نمائید.

## vCenter Server Services

Instead of using the vCenter Server appliance, you can install vCenter Server on a Windows system.

After vCenter Server is installed, a number of services start upon reboot and can be managed from the Windows Control Panel (Administrative Tools > Services).

Name	Description
VMwareVCMSDS	Provides VMware VirtualCenter Server LDAP directory services.
VMware vSphere Profile-Driven Storage Service	VMware vSphere Profile-Driven Storage Service
VMware VirtualCenter Server	Provides centralized management of VMware virtual machines.
VMware VirtualCenter Management Webservice	Allows configuration of VMware VirtualCenter Management services.
* VMware vCenter Orchestrator Configuration	VMware vCenter Orchestrator Server Web Configuration
VMware USB Arbitration Service	
VMware Upgrade Helper	Virtual hardware upgrade helper service
VMware Tools Service	Provides support for synchronizing objects between the host and guest operating systems.
VMware Snapshot Provider	VMware Snapshot Provider
VMware Physical Disk Helper Service	Enables support for running virtual machines from a physical disk partition
* Virtual Disk Service	Provides software volume and hardware volume management service.
vCenter Inventory Service	vCenter Inventory Service

\* Do not start automatically

بعد از نصب vCenter Server بروی ویندوز چندین سرویس جدید در Windows Service ایجاد می گردد:

- **VMware vCenter Orchestrator Configuration**: این ابزار یک موتور گردش کار است که می تواند به مدیران در اتوماتیک کردن کارهای دستی موجود کمک نماید.
- **VMware VirtualCenter Management Webservice**: این سرویس این امکان را به شما می دهد سرویس های مدیریت vCenter را پیکربندی نماید.
- **VMware VirtualCenter Server**: این سرویس قلب vCenter Server به شمار می رود و مدیریت متمرکز ماشین های مجازی و هاست های ESXi را انجام می دهد.
- **VMware VCMSDS**: سرویس LDAP را برای vCenter Server فراهم می آورد.

**VMware Tools Service** (همانند اسلاید بالا) در حین نصب vCenter Server نصب نمی شود. این سرویس زمانیکه **VMware Tools** بروی سیستم عامل ماشین مجازی نصب می شود، نصب می گردد. **VMware Upgrade Helper** نیز در حین نصب vCenter Server نصب نمی گردد. **VMware Tools** از این سرویس هرگاه سخت افزار یک ماشین مجازی به یک نسخه جدیدتر ارتقاء پیدا می کند استفاده می کند.



## کارگاه شماره چهار:

در این کارگاه آموزشی، شما نحوه نصب و راه اندازی کامپوننت های vCenter Server را خواهید آموخت که شامل موارد زیر می باشد:

۱. اتصال به vCenter Server
۲. پیکربندی SQL Server ODBC Connection برای یک Remote Database (در صورت لزوم)
۳. نصب vCenter Server

## بخش چهارم: نصب و توسعه vCenter Virtual Appliance

بعد از به اتمام رساندن این بخش شما قادر خواهید بود:

- یک vCenter Virtual Appliance در یک زیرساخت مجازی وارد (Import) نمائید
- vCenter Virtual Appliance نصب و پیکربندی نمائید

## قابلیت های vCenter Server Appliance

### vCenter Server Appliance Features

The vCenter Server appliance features include the following:

- Pre-packaged 64-bit application running on SUSE Linux Enterprise Server 11
- Embedded database available for:
  - Evaluating the appliance
  - Running less than 5 ESXi servers or less than 50 virtual machines
- Support for external Oracle and IBM DB2 databases when running in an enterprise
- vCenter Server appliance configuration performed through a web-based interface
- Support for the vSphere Web Client application
- The vCenter Server virtual appliance, which can authenticate with either Active Directory (AD) or Network Information Service (NIS)

شما می توانید به دو صورت از vCenter Server در دیتاسنتر خود استفاده نمایید:

- استفاده از یک **Linux-based Appliance** که در درون آن vCenter به صورت پیش فرض نصب گردیده است.
- نصب نرم افزار vCenter بروی نسخه های ویندوزی که از جانب VMware پشتیبانی می شوند.

هر دو روش بالا تفاوت چندانی با یکدیگر ندارند و قابلیت هایی همچون **HA, FT, DRS, vm Migration, Performance** را برای مدیران فراهم می آورد. شما با استفاده از **vSphere Client** می توانید به هریک از vCenter های بالا متصل شوید. در نتیجه شما هیچگونه تفاوتی در مشاهده امکانات و غیره مشاهده نخواهید کرد و استفاده از هریک از این روش ها از چشم کاربر پنهان خواهد بود.

اما استفاده از نسخه **Appliance** زمان مورد نیاز برای نصب و پیکربندی vCenter را کاهش می دهد و هزینه های شما را در خصوص خرید لایسنس ویندوز و غیر نیز کاهش خواهد داد. در واقع نسخه **Appliance** این نرم افزار بروی سیستم عامل لینوکس و به صورت یک پکیج آماده توزیع و منتشر شده است. **vCenter Server Appliance** یا به اختصار **vCSA** یک برنامه از پیش پکیج شده است که بروی **SUSE Linux Enterprise 11** توسعه داده شده است.

توجه داشته باشید که در برخی قابلیت ها **vCSA** از میزان و توان کمتری پشتیبانی می کند. در داخل **vCSA** بصورت **Embedded** دیتابیس **BD2** وجود دارد و شما تنها برای کمتر از ۵ سرور **ESXi** و کمتر از ۵۰ **vm** در محیط دیتاسنتر خود می

توانید از آن استفاده نمائید که البته در صورتیکه شما از نسخه ویندوزی vCenter به همراه Microsoft SQL Express استفاده نمائید همین محدودیت ها را خواهید داشت. در دیتاستر های بزرگ امکان استفاده از دیتابیس های بیرونی همچون Oracle در vCSA وجود دارد. از سایر ویژگی های vCSA می توان به موارد زیر اشاره نمود:

- در vCSA از vSphere Web Client برای اتصال و پیکربندی پشتیبانی می شود.
- از Active Directory ، NIS و کاربران و گروه های Local برای احراز هویت کاربران پشتیبانی می شود.
- می توانید از NFS Mount برای ذخیره کردن Log ها و Core vCSA استفاده نمائید.
- می توانید از پیکربندی سایر vCSA ها خروجی (Export) بگیرید و در یک vCSA دیگر وارد (Import) نمائید.
- می توانید وصله های امنیتی (Patch) از طریق واسط کاربری تحت وب vCSA نصب نمائید.

در مجموع vCSA تقریبا تمام قابلیت های Windows vCenter Server را بجز موارد زیر دارا می باشد:

- امکان اتصال به دیتابیس SQL Server Enterprise وجود ندارد.
- امکان vCenter Server Linked Mode برای اتصال vCenter ها به یکدیگر وجود ندارد.
- امکان vCenter Server Heartbeat برای ایجاد Fault Tolerance در میان vCenter ها وجود ندارد.

توصیه می شود پیکربندی زیر برای vCSA در نظر گرفته شود:

- حداقل تعداد دو vCPU
- 8Gb Memory
- LSI Logic Parallel
- VMXNET نسخه ۳
- حداقل 15Gb و حداکثر 60Gb برای VMDKs
- VMware Tools

## مزیت های vCenter Server Appliance

**vCenter Server Appliance Benefits**

The benefits of using the vCenter Server appliance include the following:

- Simplified deployment and configuration:
  - Import appliance to an ESXi server
  - Configure the network and time zone settings
  - Use the web interface to configure the appliance
- Lower total cost of ownership by eliminating the Windows operating system dependency and associated licensing costs
- No change to user experience when connecting to vCenter Server with the VMware vSphere Client

به راحتی شما می توانید vCSA را بروی یکی از هاست های ESXi وارد و یا Import می شود و سپس تنظیمات شبکه و Time Zone را پیکربندی نمائید و در نهایت می توانید از طریق Web Browser به آن متصل و اقدام به پیکربندی سایر بخش های آن نمائید. این پیکربندی ها شامل Host Name, IP Address, Subnet Mask, Time Zone, Directory Services و غیره می شود. شما همچنین می توانید سرویس vCenter Server Service را stop و یا start نمائید.

## نیازمندیهای vCenter Server Appliance

vCenter Server Appliance Requirements	
vCenter Server Appliance Hardware	Requirements
Disk space needed on the host machine	Minimum = 7GB Maximum = 82GB
vCenter Server Appliance memory allocation	For 1-10 hosts or 1-100 virtual machines, allocate <b>4GB</b> .
	For 10-100 hosts or 100-1000 virtual machines, allocate <b>8GB</b> .
	For 100-400 hosts or 1000-4000 virtual machines, allocate <b>13GB</b> .
	For more than 400 hosts or 4000 virtual machines, allocate <b>17GB</b> .
Processor	2 vCPU (default)

در حین نصب Windows Based vCenter Server از شما برای پیکربندی حافظه آزاد Java Virtual Machine سوال می شود. vCSA نیز دارای چنین گزینه ای می باشد که البته حافظه آزاد آن نیز از قبل پیکربندی شده است. جدول زیر به شما کمک می کند تا حافظه اصلی را براساس حافظه آزادی که از قبل پیکربندی شده است برای vCSA پیکربندی نمایید.

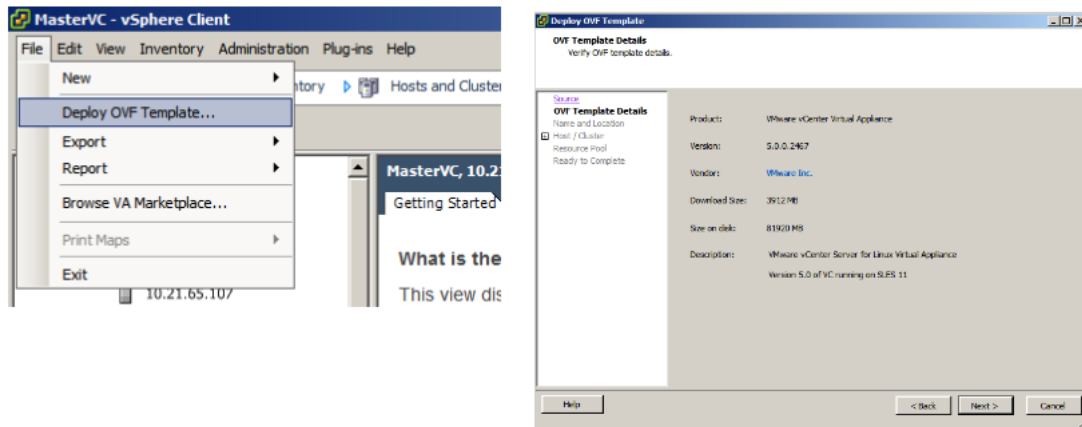
جمع کل	Policy Based Storage Management	Inventory Service	Tomcat Web Server	vCenter Server Inventory Size
3.5 GB	512 MB	2 GB	1 GB	ESXi ۱۰۰-۱ هاست یا ۱۰۰۰-۱ ماشین مجازی
7.0 GB	1 GB	4 GB	2 GB	ESXi ۴۰۰-۱۰۰ هاست یا ۱۰۰-۱۰۰۰ ماشین مجازی
11.0 GB	2 GB	6 GB	3 GB	بیش از ۴۰۰ هاست ESXi یا ۴۰۰۰ ماشین مجازی

## وارد کردن Appliance

## Importing the Appliance

To import the appliance, select File > Deploy OVF Template.

The appliance is imported on an ESXi host that is part of the virtual infrastructure.



برای وارد کردن و یا Import کردن vCSA شما می بایست گزینه File->Deploy OVF Template را در vSphere Client انتخاب نمائید و محل فایل vCSA را که دارای پسوند OVF می باشد را تعیین نمائید. برای مثال شما می توانید آدرس URL این فایل و یا آدرس محلی آن را بروی هارد دیسک Local خود معرفی و انتخاب نمائید.

## شروع به کار کردن Appliance

## Starting the Appliance

Once the appliance boots up, the network settings and time zone need to be configured.

Network settings can be configured from the console or using a web interface.

```

VMware vCenter Server Appliance 5.0.0.3247 Build 434158
To manage your appliance please browse to https://172.20.10.94:5480/
Welcome to VMware vCenter Server Appliance

Quickstart Guide: (How to get vCenter Server running quickly)
1 - Open a browser to: https://172.20.10.94:5480/
2 - Accept the EULA
3 - Select the 'Database' section
4 - Enter your database connection information
5 - Select the 'Status' section
6 - Click on the 'Start vCenter' button

*Login
Configure Network
Set Timezone (Current:UTC)

Use Arrow Keys to navigate
and <ENTER> to select your choice.

To release the cursor from the console, press Ctrl-Alt

```

پس از وارد کردن vCSA شما می بایست ماشین مجازی آن را روشن نمائید و پس از بوت شدن کامل آن شما می توانید همانند اسلاید بالا از طریق Console ماشین مجازی دستور العمل هایی که شما می بایست آن را انجام دهید را مشاهده می نمائید. در ابتدا شما می بایست تنظیمات مربوط به شبکه و Time Zone (گزینه Configure Network و Set Timezone) را پیکربندی نمائید و پس از آن از طریق یک Web Browser به IP Address آن متصل شوید و اقدام به انجام سایر پیکربندی ها نمائید.



## پیکربندی شبکه vCenter Server Appliance

## Configuring the vCenter Server Appliance Network

Access the appliance console

Select Configure Network, then enter the network settings.

Reboot the appliance after the network is configured.

```

Login
*Configure Network
Set Timezone (Current:UTC)
Use Arrow Keys to navigate
and <ENTER> to select your choice.

```

```

Please enter the desired network parameters.
To exit, type q at any prompt.

This machine may receive an IPv6 SLAAC address when the network provides one.
Configure an additional IPv6 address? y/n [n]:
Use a DHCPv4 Server instead of a static IPv4 Address? y/n [y]: n
IPv4 Address [1]: 192.168.0.60
Netmask [1]: 255.255.255.0
Gateway [1]: 192.168.0.254
DNS Server 1 [1]: 192.168.0.57
DNS Server 2 [192.168.0.57]:
Hostname [localhost.localdomain]: UCVA50.ad.srt.local
Is an IPv4 proxy server necessary to reach the Internet? y/n [n]:
IPv4 Address: 192.168.0.60
Netmask: 255.255.255.0
Gateway: 192.168.0.254
Proxy Server:
DNS Servers: 192.168.0.57, 192.168.0.57
Hostname: UCVA50.ad.srt.local
Is this correct? y/n [y]: _

```

زمانیکه شما vCSA را به صورت کامل بروی محیط مجازی خود Deploy می نمائید می بایست شبکه آن را نیز پیکربندی نمائید تا با سایر بخش ها ارتباط برقرار کند. همانند اسلاید بالا برای انجام تنظیمات شبکه می بایست از طریق Console ماشین مجازی vCSA گزینه Configure Network را انتخاب نمائید و IP Address , Subnet Mask, Default Gateway, DNS Server, Hostname را تنظیم و در نهایت کلید y را به معنی ذخیره کردن تنظیمات وارد می نمائید. توجه نمائید که پس از انجام تنظیمات می بایست vCSA را Restart نمائید.

## پیکربندی منطقه زمانه vCenter Server Appliance

## Configuring the vCenter Server Appliance Time Zone

Access the appliance console

Select Set Timezone and set the time zone to the appropriate location.

```

Login
Configure Network
*Set Timezone (Current:UTC)
Use Arrow Keys to navigate
and <ENTER> to select your choice.

```

```

Please identify a location so that time zone rules can be set correctly.
Please select a continent or ocean.
1) Africa
2) Americas
3) Antarctica
4) Arctic Ocean
5) Asia
6) Atlantic Ocean
7) Australia
8) Europe
9) Indian Ocean
0) Pacific Ocean
1) none - I want to specify the time zone using the Posix TZ format.
? -

```

زمان و ساعت در دیتاسنترها از اهمیت بالایی برخوردار می باشد لذا شما می بایست حتما TimeZone یا همان منطقه زمانی را به درستی برای vCSA تنظیم نمائید. vCSA به صورت پیش فرض زمان را با هاست ESXi یکسان سازی می کند. بدین ترتیب اگر شما منطقه زمانی را به درستی برای vCSA تعیین نمائید vCSA به صورت خودکار زمان صحیح را دریافت خواهد کرد.

همانند اسلاید بالا شما می بایست گزینه Set Timezone را انتخاب کنید و سپس بطور مثال می توانید منطقه زمانی Tehran - Iran را از بخش Asia انتخاب نمائید.

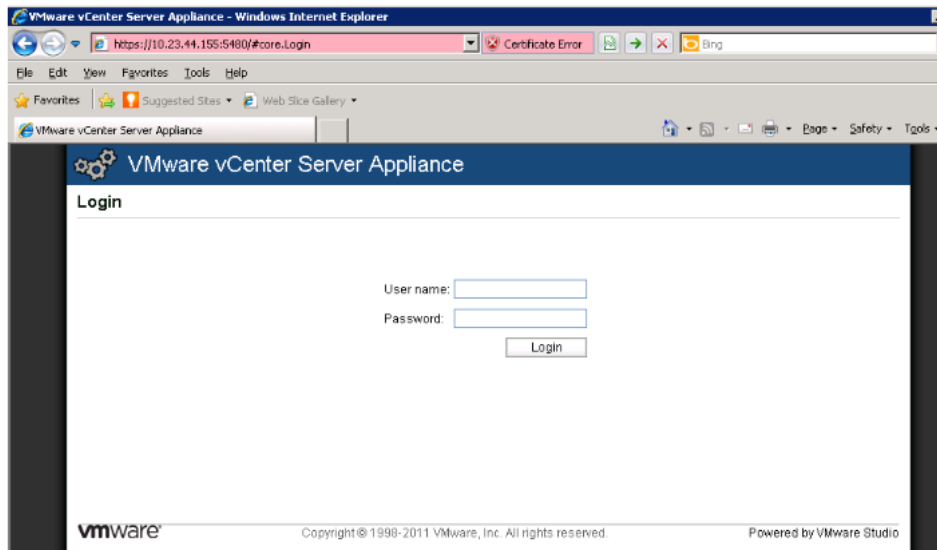
## اتصال به واسط کاربری تحت وب

## Connecting to the Web Interface

Open a web browser and type:

[https://\[appliance name|ip address\]:5480](https://[appliance name|ip address]:5480)

Log in and configure the appliance.



برای انجام سایر پیکربندی های vCSA شما می بایست یک مرورگر وب (Web Browser) را باز نمائید سپس IP Address و یا Hostname آن vCSA را به همراه پورت ۵۴۸۰ وارد نمائید و بخش تنظیمات پیشرفته این نرم افزار وارد شوید. توجه نمائید که می بایست برای این URL از https استفاده نمائید. بطور مثال شما می بایست این آدرس را وارد نمائید.

<https://192.168.1.200:5480>

## پیکربندی vCenter Server

## Configuring vCenter Server

Accept the enterprise-user license agreement and configure the database.

- Click **Accept EULA** to accept the end-user license agreement (EULA), which displays upon first login.
- Select **embedded** or **Oracle** for database type.
- Enter connection information if required.
- Click **Test Settings** or **Save Settings**.

The image shows two screenshots of the VMware vCenter Server Appliance configuration interface. The top screenshot displays the 'vCenter Server' tab with the 'EULA' sub-tab selected. The 'VMware vCenter Server End User License' section shows 'EULA Status: Accepted'. The 'Accept EULA' button is highlighted with an orange circle. The bottom screenshot shows the 'Database' sub-tab selected. The 'Database Settings' section shows 'Operation was successful.' and 'Any change in database configuration will require a STOP/START of the vCenter Server to take effect.' The 'vCenter Database Settings' section has 'Database Type' set to 'embedded'. The 'Test Settings', 'Save Settings', and 'Reset DB Contents' buttons are highlighted with orange circles.

پس از باز کردن کنسول مدیریتی vCSA از طریق مرورگر وب شما می توانید با نام کاربری پیش فرض root و کلمه عبور vmware به تنظیمات پیشرفته vCSA وارد شوید. پس از وارد شدن به vCSA در اولین بار شما باید مراحل زیر را همانند اسلاید بالا انجام دهید:

- از سربرگ vCenter Server گزینه EULA را انتخاب و بروی Accept EULA به نشانه پذیرفتن License Agreement کلیک نمائید.
- سپس می بایست به سربرگ Database مراجعه نموده و نوع دیتابیس را embedded DB2 و یا Oracle انتخاب نمائید. در صورتیکه که دیتاسنتر شما بیش از 5 هاست ESXi دارد و تعداد vm های آن از مرز 50 دستگاه عبور می کند می بایست از یک دیتابیس خارجی Oracle برای vCSA استفاده نمائید و باید مشخصات یک دیتابیس خارجی Oracle را برای آن وارد نمائید و در غیر این صورت می توانید از همان نوع embedded استفاده نمائید.
- سپس بروی گزینه Test Setting کلیک کرده و در صورتیکه تست اتصال به دیتابیس با موفقیت انجام شده باشد می بایست گزینه Save Setting را به نشانه تأیید نهایی انتخاب نمائید.
- در نهایت شما می بایست همانند اسلاید بعدی به سربرگ Status رفته و سرویس های vCenter Service را با استفاده از گزینه Start vCenter Service آماده به کار نمائید

با استفاده از این کنسول vCSA می توانید تنظیمات متعددی را انجام دهید که از جمله آنها می توان به موارد زیر اشاره کرد:

- تغییر تنظیمات شبکه
- **Start** و **Stop** کردن سرویس های **vCenter Server**
- پیکربندی پورت ها در فایروال
- فعال کردن **Directory Service** به منظور استفاده از یک سرویس های همچون **Active Directory** و **LDAP**
- تغییر **Host Name**
- خاموش و یا **Restart** کردن **vCSA**
- بروزرسانی و **Upgrade** کردن (ارتقاء) **vCSA**

توجه داشته باشید هر سربرگ دارای یکسری **Action** ها می باشد که در سمت چپ به نمایش درآمده و قابلیت هایی را که برای شما فراهم می آورد را به شما نمایش می دهد.

## مدیریت vCenter Server Services

## Manage vCenter Server Services

Turn on the vCenter Server service and manage additional vCenter Server services.

- Click **Start vCenter**.
- Click the **Services** tab.
- Start and stop services for the vSphere Web Client and ESXi hosts.

VMware vCenter Server Appliance

vCenter Server | **Services** | Authentication | Network | System | Update | Upgrade | Help | Logout user root

Status | Database | Settings | Administration | Storage

**VMware vCenter Server Status**

Service Version: 5.0.0-413592  
Service Status: Stopped

Database Type: not configured  
Database Server:

**Actions**

Start vCenter  
Stop vCenter  
Refresh

vCenter Server | **Services** | Authentication | Network | System | Update | Upgrade | Help | Logout user root

Status | Syslog | NetDump | AutoDeploy

**vCenter Services Status**

ESXi Syslog Status: Running  
ESXi Network CoreDump Status: Running  
ESXi AutoDeploy Status: Stopped  
ESXi Syslog Collector Server Port: 614  
ESXi Syslog Collector Server SSL Port: 1614  
ESXi Network CoreDump Server Port: 6500  
ESXi AutoDeploy Server Port: 6502  
vSphere Web Client Status: Running

**Actions**

Start ESXi Services  
Stop ESXi Services  
Start vSphere Web Client  
Stop vSphere Web Client  
Refresh

همان طور که در بخش قبلی توضیح داده شد شما می توانید از سربرگ **Services** اقدام به **Start** و **Stop** کردن سرویس های **vCenter Server** نمائید. توجه داشته باشید که فعالیت و اجرای **vCenter Server** نیازمند معرفی یک دیتابیس می باشد و تا زمانیکه شما دیتابیس را به آن معرفی ننمائید، سرویس آن **Start** نخواهد شد.

علاوه بر **Start** کردن سرویس **vCenter Server** شما می توانید سرویس **vSphere Web Client** را نیز در سربرگ **Services** به منظور استفاده از آن **Start** و یا **Stop** نمائید.

## سایر پیکربندهای vCenter Server

## Additional vCenter Server Configuration Options

There are many other configuration options that are beyond the scope of this discussion.



The other tabs offer various configuration options. For example:

- Configure HTTP/HTTPS ports
- Change appliance password
- Reboot or shutdown the appliance
- Configure logging and core file storage
- Modify IP address, DNS, and hostname

در سربرگ **Services** گزینه های زیادی برای **Start** و **Stop** کردن سرویس ها، پیکربندی پورت های شبکه و فضای **Core Dump** وجود دارد. فضای **Core Dump** سرویس هایی را برای هاست های **ESXi** از جمله **System Logging**، **Core Dump Capture** و **AutoDeploy** فراهم می کند.

در سربرگ **Authentication** شما می توانید **Network Information Service** و یا **Active Directory Service** را پیکربندی نمایید.

در سربرگ **Network** شما می توانید تنظیماتی از جمله **IP.v6** و **IP.v4**، **DNS Server**، **Gateway**، **Host Name**، **Netmask** را پیکربندی نمایید. همچنین شما می توانید گزینه هایی را برای دسترسی به **vCSA** از طریق **Proxy Server** پیکربندی نمایید.

در سربرگ **System** نیز به شما گزینه هایی برای **Shutdown** و **Reboot** کردن **vCSA** نمایش داده می شود.

در سربرگ **Update** نیز به شما نسخه **vCSA** نمایش داده می شود و به شما اجازه داده می شود تا تنظیمات **Automatic Update** را پیکربندی نمایید. در سربرگ **Upgrade** نیز به شما گزینه هایی برای ارتقاء **vCSA** از نسخه فعلی به نسخه جدید نمایش داده می شود.

## کارگاه شماره پنج:

در این کارگاه آموزشی، شما اقدامات اولیه vCenter Server را خواهید آموخت که شامل موارد زیر می باشد:

۱. پیکربندی vCenter Server Appliance را با یک مرورگر وب
۲. پیکربندی vCenter Server Appliance با استفاده از Directory Service
۳. ریجستر کردن VMware vSphere Web Client با vCenter Server Appliance
۴. اتصال به یک vCenter Server Appliance با استفاده از vSphere Client

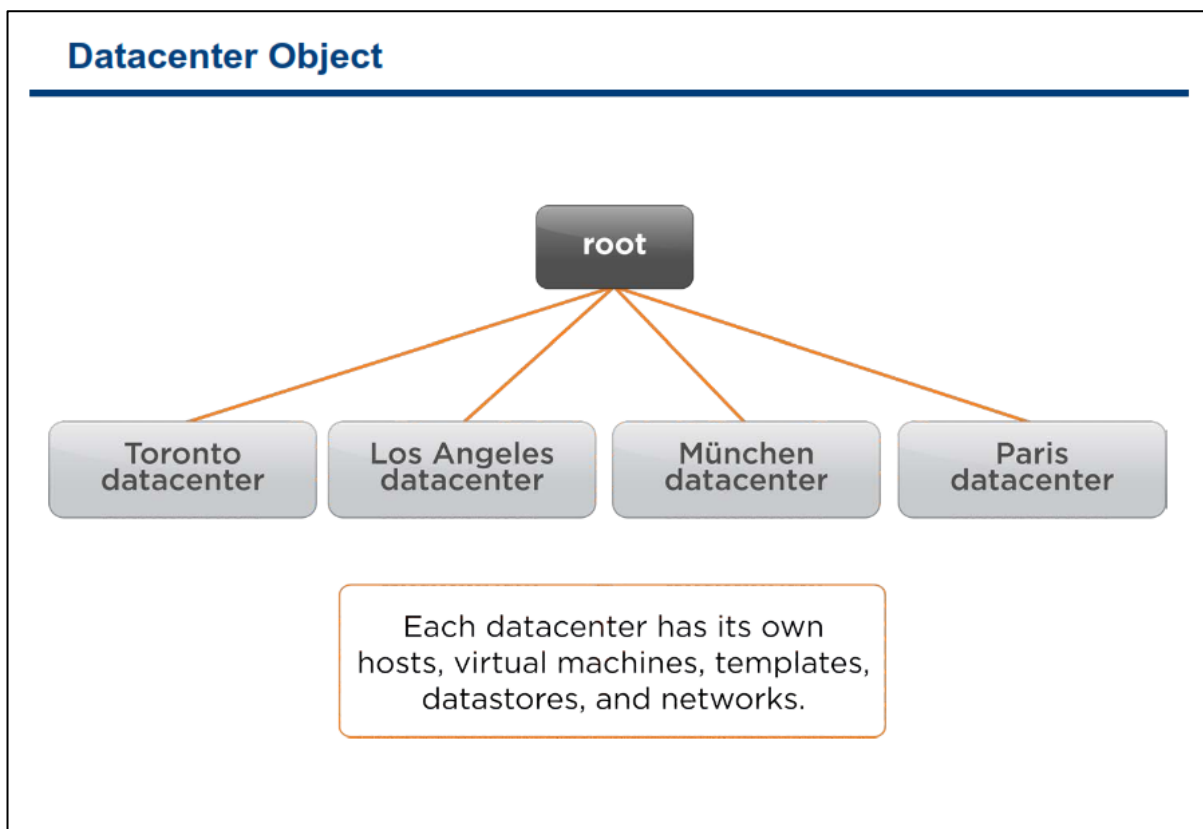


## بخش پنجم: مدیریت vCenter Server

بعد از به اتمام رساندن این بخش شما قادر خواهید بود:

- آپجکت های vCenter Server ایجاد و سازماندهی کنید
- vCenter Server با استفاده از vSphere Client راهبری کنید
- لایسنس جدید به vCenter Server اضافه کنید
- رخداد ها و Log های vCenter Server مشاهده نمائید
- یک مدیر برای vCenter Server ایجاد نمائید

## آبجکت های دیتاستر

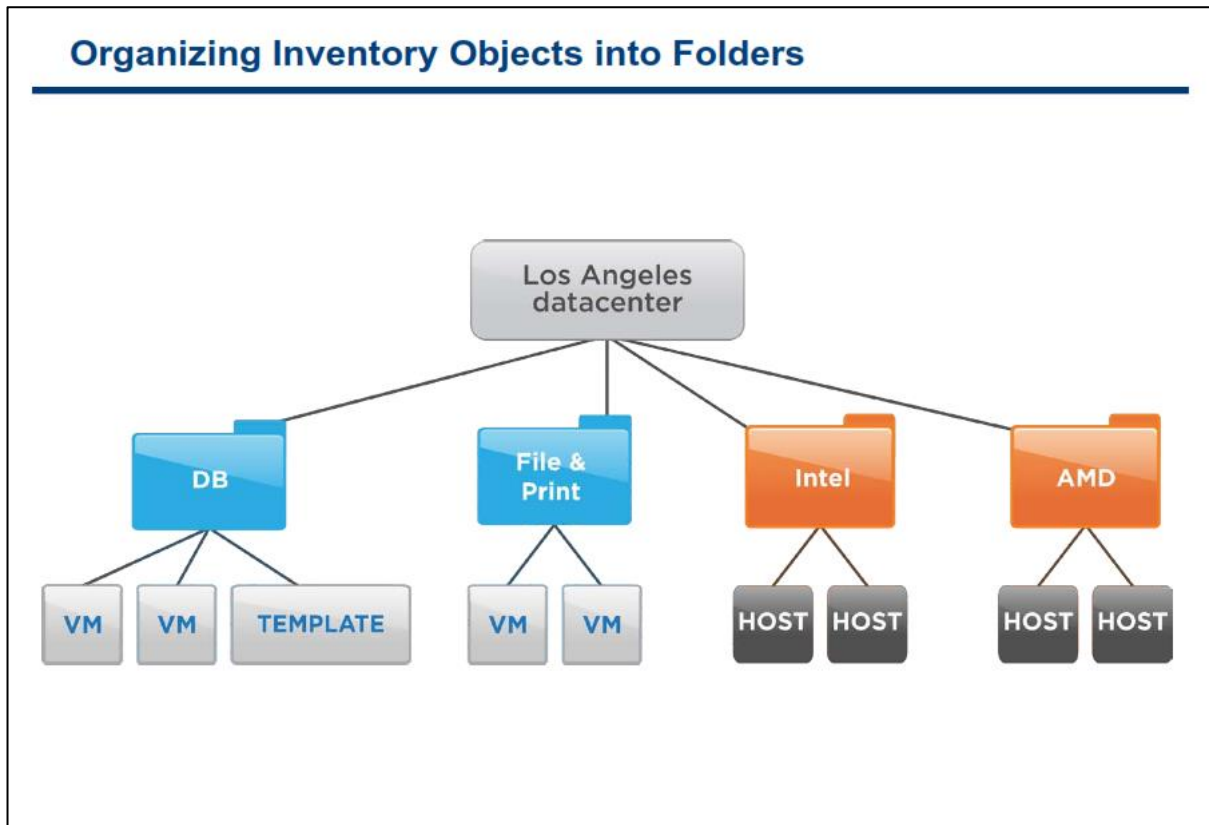


آبجکت ها و تمامی اجزای vCenter Server از یک ساختار درختی تشکیل شده اند. این آبجکت ها یا دربرگیرنده سایر آبجکت ها می باشند همانند پوشه ها و یا آبجکت هایی هستند که شما می توانید آنها را مدیریت نمایید. هاست ها ، vm ها ، Template ، کلاستر ها، datastore ها و یا شبکه ها از دسته دوم آبجکت ها به شمار می آیند. از این ساختار درختی برای گروه بندی آبجکت ها به یک روش معناداری استفاده می گردد بطوریکه شما می توانید براساس آن حق دسترسی ها را تعیین نمایید. شما می توانید از vCenter Server برای مدیریت یک یا چندین دیتاستر استفاده نمایید. شرکت های بزرگ ممکن است از چندین دیتاستر برای کسب و کار خود استفاده نمایند. آبجکت ها در داخل هر دیتاستر می توانند با هم در تعامل باشند ولی در خارج از دیتاستر با هم در تعامل نیستند و دارای محدودیت می باشند. برای مثال شما می توانید یک ماشین مجازی را با استفاده از vMotion از امکان یک هاست به هاست دیگر در همان دیتاستر منتقل نمایید اما نمی توانید همان ماشین مجازی را به یک هاست دیگر در یک دیتاستر دیگر منتقل نمایید. اما شما می توانید از یک ماشین مجازی کپی برداری نمایید و آن را در یک دیتاستر دیگر به اجرا در آورید.

همان طور که در اسلاید بالا مشاهده می نمایید، دیتاسترها براساس محل جغرافیای و شهرهایی که در آنجا قرار دارند ایجاد می گردد. بدین معنی که شما می بایست دیتاستر را صرفا براساس محل جغرافیایی آن ایجاد نمایید. در واقع هر محل جغرافیایی Administrator ها ، مسئولین و مجموعه مشتریان خود را دارد و همچنین مجموعه سرور های ESXi ، vm ، datastore و شبکه مخصوص به خود را دارد.

بالاترین آبجکت در vCenter Server Inventory آبجکت root نامیده می شود. آبجکت root خود vCenter Server System می باشد. آبجکت root را نمی توانید از آبجکت ها حذف نمایید.

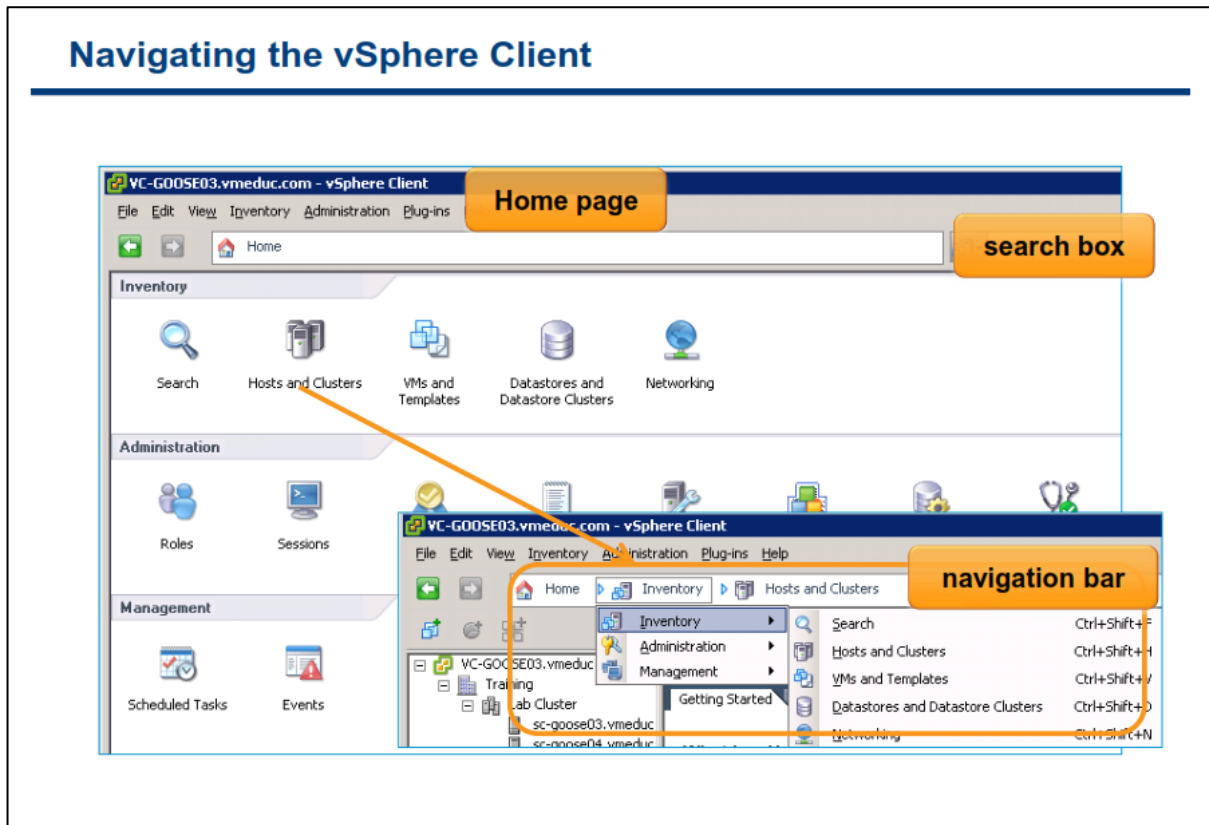
## سازماندهی آبجکت‌ها درون پوشه‌ها



هر یک آیت‌ها را در یک دیتاستر می‌توانید در داخل یک پوشه (Folder) و زیر پوشه (Sub Folder) قرار دهید. این کار باعث سازماندهی بیشتر آیت‌ها می‌گردد. همچنین یکی دیگر از مزایای دسته بندی آبجکت‌ها در داخل پوشه‌ها این است که می‌توانید دسترسی مناسبی را برای مدیران برحسب دسته بندی که مشخص کرده اید تعیین نمایید.

همانطور که در اسلاید بالا مشاهده می‌نمائید، VM‌ها و Template‌ها براساس نقش و فعالیت در پوشه مخصوص به خود قرار گرفته‌اند. همچنین هاست‌ها براساس خانواده CPU‌ها در پوشه‌های مخصوص به خود قرار گرفته‌اند.

البته ایجاد دسته بندی و پوشه‌های مختلف ممکن است مدیریت آن را نیز مشکل کند که باید این نکته را نیز مد نظر داشته باشید و دسته بندی‌ها را با دقت و آینده نگری تعیین نمایید.

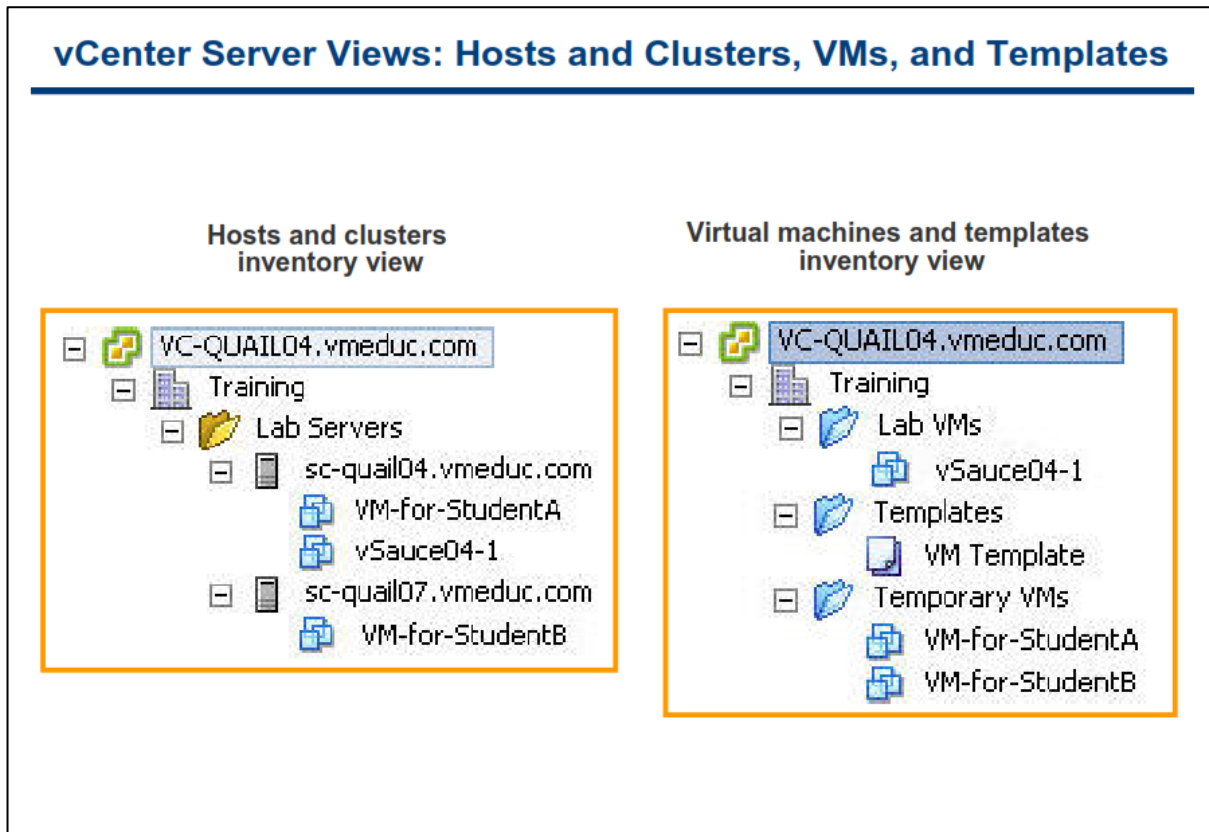


در vSphere Client این امکان برای شما فراهم می گردد تا آجکت ها را مدیریت نمائید. زمانیکه شما با استفاده از vSphere Client به vCenter Server وارد و یا Login می نمائید در ابتدا صفحه Home Page آن را مشاهده می نمائید. قالب پیش فرض صفحه Home دارای نوار Menu ، نوار Navigation ، پنل ها و همچنین بخش Search می گردد. این صفحه دارای آیکن هایی برای فعالیت های اصلی vSphere Client می گردد که شامل : Inventory ، Administration ، Management و Soution and Application (در اسلاید بالا دیده نمی شود) می گردد. برای بازگشت به صفحه Home نیز شما می توانید بروی گزینه Home در نوار Navigation کلیک نمائید.

نوار Navigation مسیر ساختار یافته ای را برای نمای فعلی vSphere Client نمایش می دهد. برای مثال زمانیکه شما در نمای Hosts and Clusters قرار دارید نوار Navigation مسیر Home->Inventory->Hosts and Clusters را به شما نمایش می دهد. شما می توانید بروی یک آیتم در نوار Navigation کلیک نمائید و بدین ترتیب سایر گزینه های مربوط به آن سطح از ساختار درختی را مشاهده نمائید.

همچنین vSphere Client دارای یک بخش جستجو می باشد که در تمام نماها در دسترس شما است. به صورت پیش فرض vSphere Client در میان تمامی آجکت ها جستجو انجام می دهد ولی با این وجود شما می توانید بروی آیکن مورد نظر کلیک نمائید و جستجو خود را محدود نمائید. نتایج جستجو نیز در زیر کادر جستجو نمایش داده می شوند.

## نمای vCenter Server : Host ها و کلاسترها و vm و Template ها



در نمای **Host and Clusters Inventory** شما می توانید تمامی کلاسترها و هاست ها را در یک دیتاسنتر مشاهده نمایید.

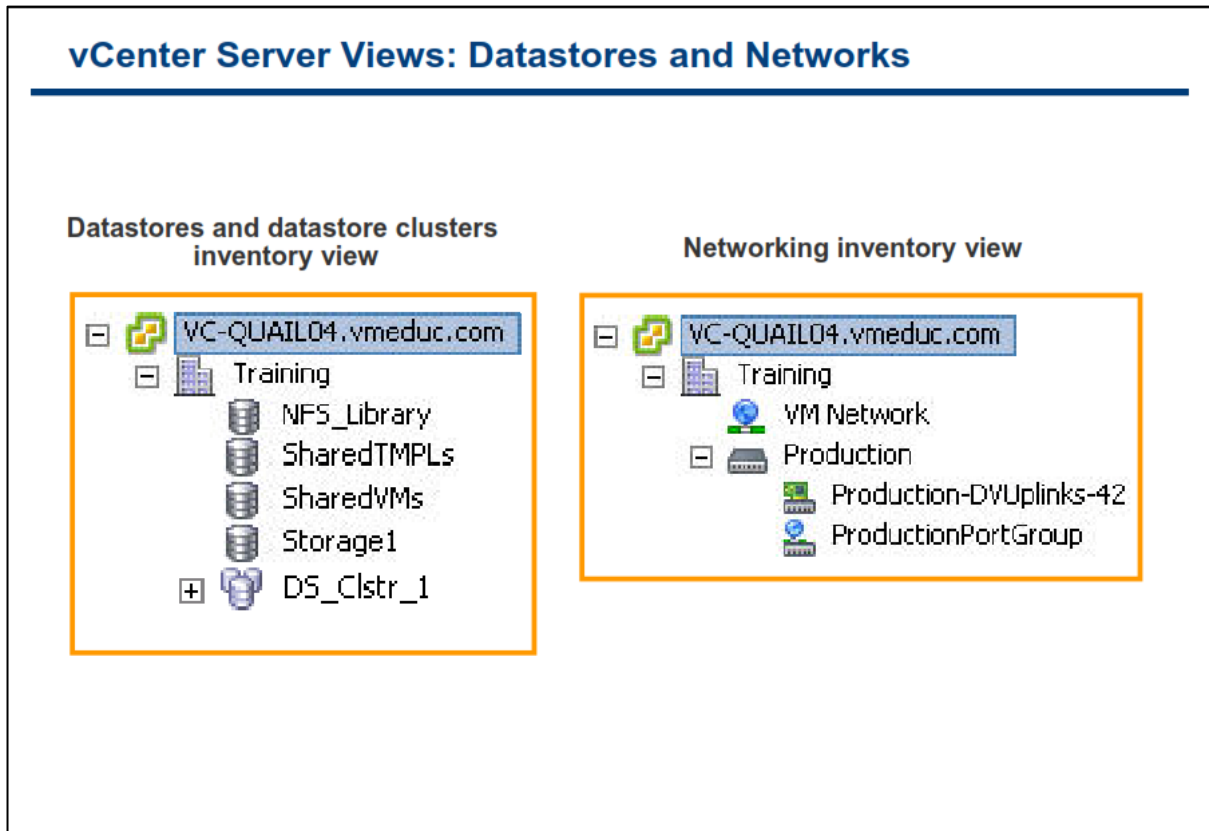
در نمای **VMs and Templates Inventory** نیز شما می توانید تمامی **Template** ها و **vm** ها را در دیتاسنتر مشاهده نمایید. در اسلاید بالا، نام دیتاسنتر **Training** می باشد. نام آبجکت **root** همان نام **vCenter Server** می باشد که در اینجا **VC-QUAIL04.vmeduc.com** نام گذاری شده است.

هر نما دارای مدیریت و پوشه های مخصوص به خودش می باشد و ایجاد تغییرات در سازماندهی یک نما در دیگر تاثیر نمی گذارد. همانطور که در اسلاید مشاهده می نمایید، پوشه **Lab Server** در نمای **Host and Clusters Inventory** در نمای **VMs and Templates Inventory** نمایش داده نمی شود. به همین ترتیب پوشه **Lab VMs** ، **Template** و **Temporary VMs** در نمای **VMs and Templates Inventory** در نمای **Host and Clusters Inventory** نمایش داده نمی شود.

به صورت پیش فرض شما نمی توانید اطلاعات مربوط به **Templates** را در نمای **Host and Clusters Inventory** ببینید. برای مشاهده **Templates** در این نما، شما می بایست دیتاسنتر خود را انتخاب و سپس به سربرگ **Virtual Machines** مراجعه نمایید.

همچنین به صورت پیش فرض شما نمی توانید اطلاعات مربوط به **Host** و **Cluster** را در نمای **VMs and Templates Inventory** مشاهده نمایید. برای مشاهده **Host** ها در این نما، شما می بایست دیتاسنتر خود را انتخاب و سپس به سربرگ **Hosts** مراجعه نمایید.

## نمای vCenter Server :Datastores &amp; Networks



نمای Datastore and datastore clusters inventory تمامی Datastore ها و Datastore clusters را در یک دیتاستر نمایش می دهد.

نمای Networking inventory نیز تمامی Port Group و Distributed virtual switch را نمایش می دهد (Port Group و Distributed virtual switch در فصل های بعدی تشریح خواهد شد).

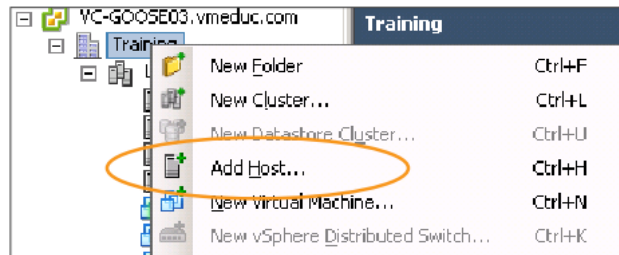
همانند سایر نما ها شما می توانید در این نما ها نیز آبجکت های خود را در داخل پوشه ها سازماندهی نمائید.

## افزودن یک هاست به vCenter Server

## Adding a Host to the vCenter Server Inventory

To add an ESXi host to the vCenter Server inventory, use the Add Host wizard and specify:

- Fully qualified domain name
- User name and password
- Lockdown mode enabled



برای افزودن هاست به vCenter شما می بایست به نمای **Hosts & Cluster Inventory** مراجعه نمائید و بروی دیتاستر خود راست کلیک و گزینه **Add Host** را انتخاب کنید. سپس می بایست **FQDN Name** و یا **IP Address** هاست ESXi را در ویزارد **Add Host** وارد نمائید. در مرحله بعدی می بایست نام کاربری **root** و کلمه عبور هاست ESXi را وارد نمائید. از vCenter Server حساب کاربری **root** برای **Login** کردن اولیه به هاست ESXi و ایجاد حساب کاربری اختصاصی **vpuser** استفاده می کند. از حساب کاربری **vpuser** برای احراز هویت های آتی خود استفاده می کند و با تغییر حساب کاربری **root** خللی در فعالیت های بعدی که vCenter با هاست ESXi دارد، بوجود نمی آید.

و در نهایت شما می توانید گزینه **Lockdown Mode** را فعال نمائید. **Lockdown Mode** امکان دسترسی از راه دور را به هاست ESXi به صورت مستقیم مسدود می نماید(البته با استفاده از حساب کاربری **root**). با استفاده از این حالت شما تنها از طریق **vCenter Server** می توانید هاست ESXi را از راه دور مدیریت نمائید. این کار در افزایش ضریب امنیتی محیط مجازی به شما کمک می کند.

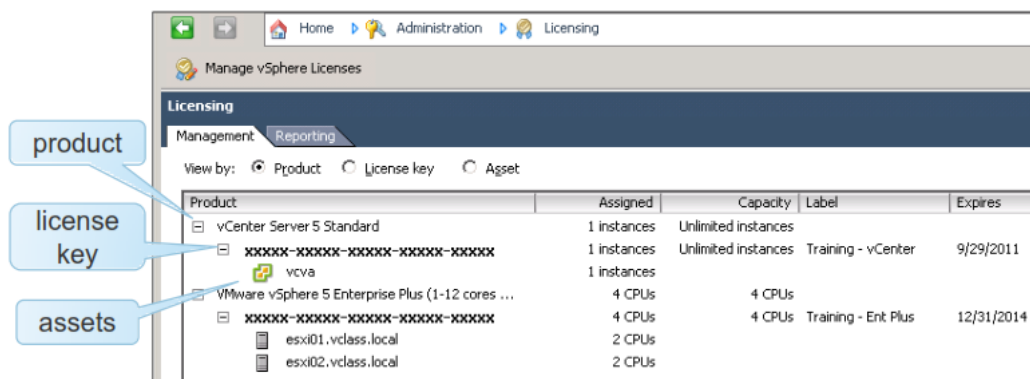
## نگاه اجمالی به لایسنس vCenter

## vCenter License Overview

Licenses are managed and monitored from vCenter Server.

Licensing consists of:

- Product – License to use a vSphere software component or feature
- License key – 25-character string that corresponds to a product
- Asset – Machine on which a product is installed



در محیط vSphere شما می توانید لایسنس نرم افزار را به صورت متمرکز در vCenter Server مدیریت نمایید. تمامی قابلیت های نرم افزار در ۲۵ کاراکتر کلید لایسنس کپسوله می گردد.

اطلاعات لایسنس را می توانید براساس محصول (Product)، کلید لایسنس (License Key) و دارایی (Asset) مشاهده نمایید:

- محصول: یک لایسنس است که برای امکانات و کامپوننت های vSphere استفاده می شود. برای مثال حالت آزمایشی و یا vSphere 5 Enterprise Plus
- کلید لایسنس: یک شماره سریال است که به محصول مرتبط می باشد.
- دارایی: یک ماشین است که محصول بروی آن نصب گردیده است. برای اینکه نرم افزار به صورت قانونی اجرا شود می بایست دارایی دارای لایسنس باشد.

برای کسب اطلاعات بیشتر در خصوص لایسنس VMware vSphere می توانید به مقاله ESXi and vCenter Server Setup Guide در سایت <http://www.vmware.com/support/pubs> مراجعه نمایید.



## رویدادهای vCenter Server

**vCenter Server Events**

VC-GOOSE03.vmeduc.com VMware vCenter Server, 5.0.0, 380461

Getting Started | Datacenters | Virtual Machines | Hosts | Tasks & Events | Alarms | Permissions | Maps | Scheduled Task

View: Tasks | Events

Description, Type or Target contains:  Clear

Description	Type	Date Time	Task	Target	User
Configured storage DRS on datastore cluster DS_Clstr_1	info	5/18/2011 11:12...	Configure Stora...	DS_Clstr_1	Administrator
Reconfigured Storage I/O Control on datastore SAN (1)	info	5/18/2011 11:12...		SAN (1)	
Enabled storage DRS on datastore cluster DS_Clstr_1 with automation level Manual	info	5/18/2011 11:12...	Configure Stora...	DS_Clstr_1	Administrator
Alarm 'Datastore cluster is out of space' on DS_Clstr_1 changed from Gray to Green	info	5/18/2011 11:12...		Training	
Task: Configure Storage DRS	info	5/18/2011 11:12...	Configure Stora...		Administrator

details of selected event

رویداد و یا Event در vCenter Server نتیجه و یا خروجی Task ها و فعالیت های تولید شده می باشد. برای مثال تغییر دادن پیکربندی یک ماشین مجازی.

برای مشاهده رویداد و یا Event ها می بایست به نمای Inventory مراجعه نمائید و سپس یک آبجکت را انتخاب و همانند اسلاید به سربرگ Task & Events مراجعه نمائید. در سربرگ Task & Events شما می توانید تمامی رویدادهای مرتبط با آن آبجکت را مشاهده نمائید.

همچنین شما می توانید از کادر جستجو برای جستجو در میان Event ها براساس توضیحات، نوع و غیره نیز استفاده نمائید.

شما می توانید از نوار Menu به View->Management->Events مراجعه نمائید و رویدادهای سیستمی vCenter Server را مشاهده نمائید. رویدادهای سیستمی vCenter Server می توانند در عیب یابی مشکلات بسیار مفید باشند.

## vCenter Server System Logs

The screenshot shows the vSphere Client interface for a vCenter server. The breadcrumb navigation path is Home > Administration > System Logs > vc-goose02.vmeduc.com. The 'Export System Logs' button is highlighted with an orange circle. Below the navigation, there is a list of log files with a search field and a 'log search' callout box pointing to it. The log entries include:

```

vCenter server log [vpxd-6.log]
vCenter server log [vpxd-alert-6.log]
vCenter server log [vpxd-profiler-2.log]
vpxd-profiler [vpxd-profiler-2.log]
[2010-04-08 10:50:18.582 02012 info 'App'] Log path: C:\ProgramData\VMware\VMware VirtualCenter\Logs
[2010-04-08 10:50:18.582 02012 info 'App'] Initializing SSL
[2010-04-08 10:50:18.582 02012 info 'Libs'] Using system libcrypto, version 9080BF
[2010-04-08 10:50:21.770 02012 info 'App'] Vmactore::InitSSL: doVersionCheck = true, handshakeTimeoutUs = 120000000
[2010-04-08 10:50:21.911 02012 info 'App'] Starting VMware VirtualCenter 4.1.0 build-233726
[2010-04-08 10:50:21.973 02012 info 'App'] Log directory: C:\Windows\system32\config\systemprofile\AppData\Local\VMware\
  
```

برای مشاهده لیستی از Log های vCenter Server شما می توانید به Home->Administration->System Logs مراجعه نمایید. همانند Event ها شما می توانید در میان Log ها جستجو نمایید و یا حتی از آن خروجی بگیرید و حتی برای عیب یابی به صورت یک فایل فشرده برای شرکت VMware ارسال نمایید. همانند Event ها، Log ها نیز برای عیب یابی یک مشکل بسیار مفید خواهند بود.

## کارگاه شماره شش:

در این کارگاه آموزشی، شما اقدامات اولیه vCenter Server را خواهید آموخت که شامل موارد زیر می باشد:

۱. نصب لایسنس vSphere
۲. ایجاد یک آبجکت دیتاسنتر در vCenter Server
۳. ایجاد یک آبجکت پوشه در vCenter Server
۴. اضافه کردن هاست ESXi به vCenter Server

## فصل چهارم: پیکربندی و مدیریت شبکه مجازی



این فصل شامل بخش های زیر می گردد:

۱. معرفی vNetwork Standard Switch
۲. پیکربندی پالیسی های Standard Virtual Switch

اهمیت این فصل:

قابلیت های شبکه مجازی VMware vSphere به ماشین مجازی این امکان را می دهد که بتوانند با سایر ماشین های مجازی و یا فیزیکی ارتباط برقرار کنند. بدین ترتیب مدیران می توانند هاست ESXi را مدیریت نمایند و از طرف دیگر از منابع ذخیره سازی (Storage) مبتنی بر IP در محیط مجازی استفاده نمایند و از قابلیتی همچون vSphere vMotion Migration بهره مند شوند. اشتباه و یا پیکربندی نادرست شبکه در ESXi می تواند تاثیرات منفی را بروی عملکرد Storage ها و مدیریت ماشین های مجازی بوجود آورد.

## بخش اول: معرفی vNetwork Standard Switch

بعد از به اتمام رساندن این بخش شما قادر خواهید بود:

- شبکه مجازی، سوئیچ مجازی و انواع اتصالات سوئیچ مجازی را تشریح نمایید
- کامپوننت های یک vNetwork Standard Switch را تشریح نمایید
- یک vNetwork Standard Switch ایجاد نمایید

## شبکه مجازی و سوئیچ مجازی چیست؟

### What Is a Virtual Network? What Is a Virtual Switch?

**A virtual network provides the networking for hosts and virtual machines that use virtual switches.**

**A virtual switch:**

- Directs network traffic between virtual machines and links to external networks.
- Combines the bandwidth of multiple network adapters and balances traffic among them. It can also handle physical network interface card (NIC) failover.
- Models a physical Ethernet switch:
  - A virtual machine's NIC can connect to a port.
  - Each uplink adapter uses one port.

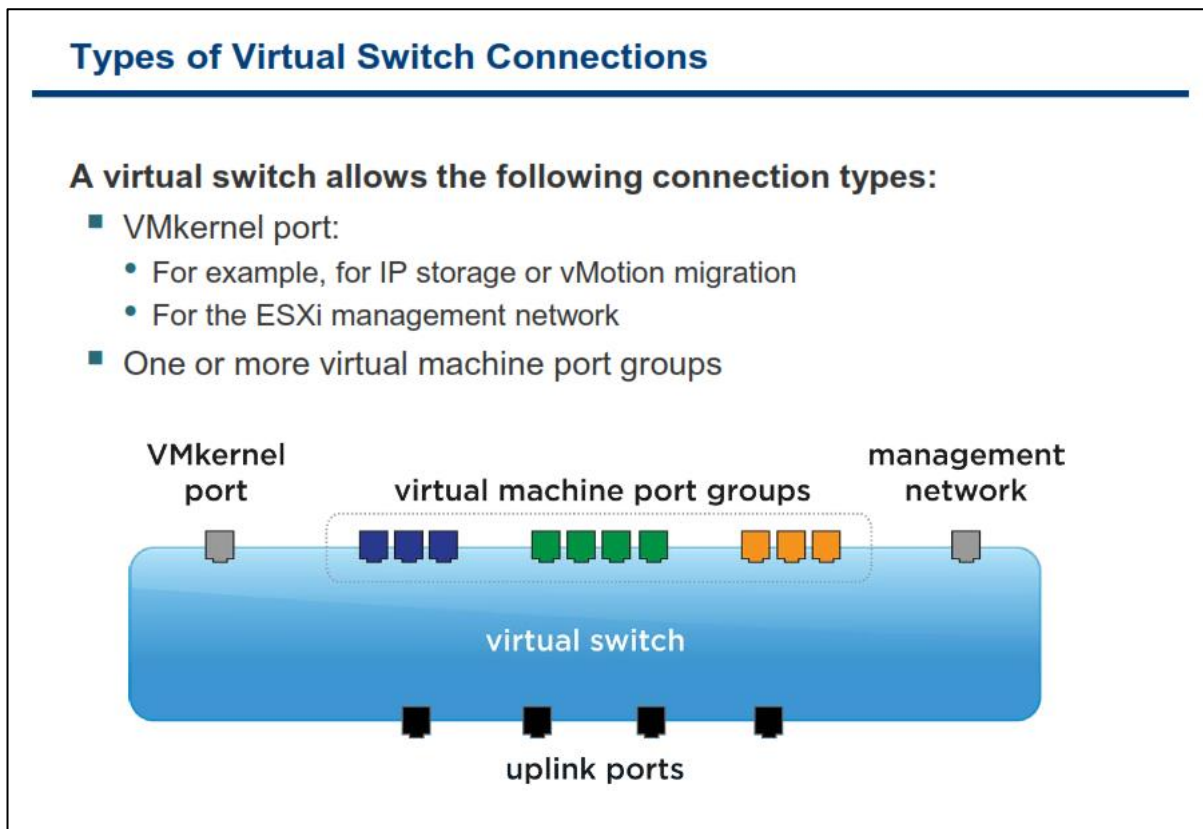
یک **Virtual Network** یا همان شبکه مجازی، ارتباطات شبکه ای را برای **vm** هایی که بروی **VMware ESXi** قرار دارند، ایجاد می کند. یکی از کامپوننت های اصلی شبکه مجازی **Virtual Switch** می باشد. یک **Virtual Switch** یک نرم افزار توسعه داده شده در **VMkernel** می باشد که ارتباطات شبکه ای را برای **vm** هایی که بروی **ESXi** وجود دارند، فراهم می کند.

**VMkernel** در حقیقت چندین نقش را در محیط مجازی ایفا می کند: ۱- ارتباطات شبکه ای را برای مدیریت هاست ها فراهم می کند ۲- سرویس هایی از قبیل **NFS**, **vMotion**, **iSCSI** را فراهم می کند ۳- سوئیچ های مجازی به **VMkernel** متصل می شوند و از طریق آن با دنیای بیرون ارتباط برقرار می کنند.

همه ارتباطات شبکه توسط یک یا چند **Virtual Switch** بروی هاست انجام می شوند. یک **Virtual Switch** بستر را برای ارتباط **vm** ها با یکدیگر فراهم می کند. هرچند اگر آنها بروی یک یا چندین هاست مختلف در حال اجرا باشند. **Virtual Switch** ها در لایه ۲ **OSI** کار می کنند. شما نمی توانید دو **Virtual Switch** را به یک کارت شبکه (**NIC**) فیزیکی هاست **Map** و یا نگاشت نمائید. اما شما می توانید دو یا چند **Physical NIC** را به یک **Virtual Switch** متصل و یا **Map** نمائید.

با استفاده از **Virtual Switch** شما می توانید پهنای باند چندین **Network Adapter** را با هم ترکیب نمائید و حجم ترافیک ارتباطی آنها را بالانس نمائید. همچنین می توانید **NIC** های فیزیکی هاست را برای **Failover** شدن پیکربندی نمائید. اگر **Uplink Adapter** یا همان **NIC** فیزیکی هاست به یک **Virtual Switch** متصل شود، هر **vm** می تواند به شبکه خارجی نیز متصل شود.

## انواع اتصالات سویچ مجازی



یک Virtual Switch دو نوع connection را برای هاست ها و vm ها فراهم می کند:

- اتصال vm به یک شبکه فیزیکی
- اتصال سرویس VMKernel به یک شبکه فیزیکی

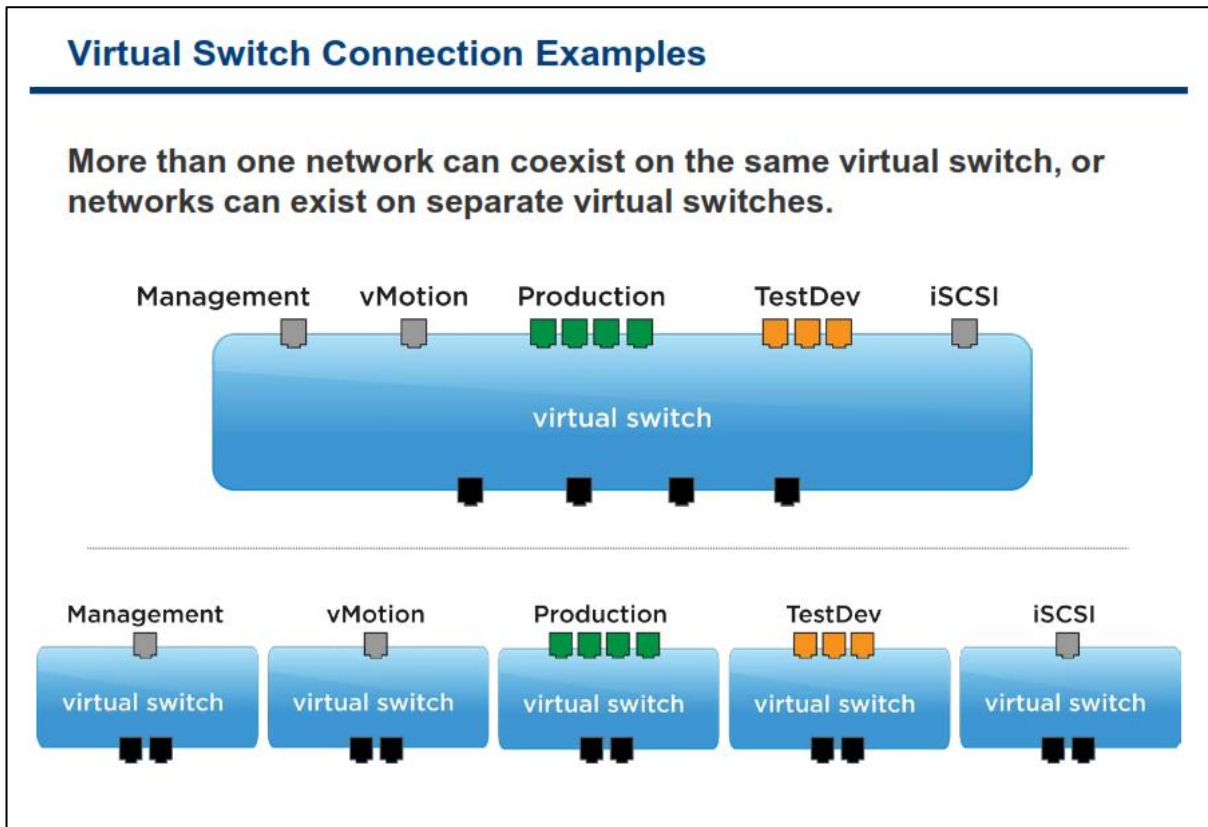
VMKernel در واقع سرویسی می باشد که هسته مرکزی vSphere را به سرویس های دیگر متصل می نماید و بطور مثال برای دسترسی به IP storage (مانند iSCSI, NFS)، مهاجرت و یا vMotion Migration و دسترسی به Management هاست استفاده می شود.

از پورت Network Management هاست ESXi برای اتصال به شبکه و یا سرویس راه دور همانند vSphere Client استفاده می شود. بدین معنی که نرم افزار vSphere Client صرفاً به پورت Network Management می تواند متصل گردد و در صورتیکه این پورت وجود نداشته باشد، امکان مدیریت هاست از طریق vSphere Client غیر ممکن می شود.

هر پورت Network Management و هر پورت VMKernel می بایست با IP address, Subnet Mask, Gateway خودش پیکربندی شوند. بدین معنی که شما نمی توانید از سایر IP Address های محیط مجازی برای اتصال به Network Management استفاده نمائید.

همانطور که در اسلاید بالا ملاحظه می نمائید، vm Port Group و VMkernel Port از طریق NIC فیزیکی هاست که آن نیز به پورت Uplink Virtual Switch متصل است، به دنیای خارج متصل می شوند.

## مثال هایی از اتصالات سوئیچ مجازی



در طراحی محیط شبکه مجازی شما می توانید همه شبکه ها را بروی یک سوئیچ مجازی قرار دهید و یا اینکه برای هر شبکه از یک سوئیچ مجازی استفاده نمائید. این تصمیم گیری تا حد زیادی به طراحی شبکه فیزیکی شما بستگی دارد. برای مثال ممکن است بروی هاست به تعداد Virtual Switch ها، NIC فیزیکی وجود نداشته باشد و یا اینکه ممکن است شما بروی پورت های سوئیچ فیزیکی VLAN های خاصی را تعریف کرده باشید.

نکته کلیدی اینجاست که همه NIC های فیزیکی به Virtual Switch ها انتساب داده می شوند، بنابراین همه پورت ها و Port Group ها بروی همان NIC های فیزیکی به اشتراک گذاشته می شوند. باید توجه داشته باشید که تعریف چندین vm بروی یک شبکه مجازی که تنها به تعداد محدودی Physical Uplink ختم می شوند باعث کاهش پهنای باند vm های شما می گردد.



## انواع سوئیچ های مجازی

**Types of Virtual Switches**

**A virtual network supports two types of virtual switches:**

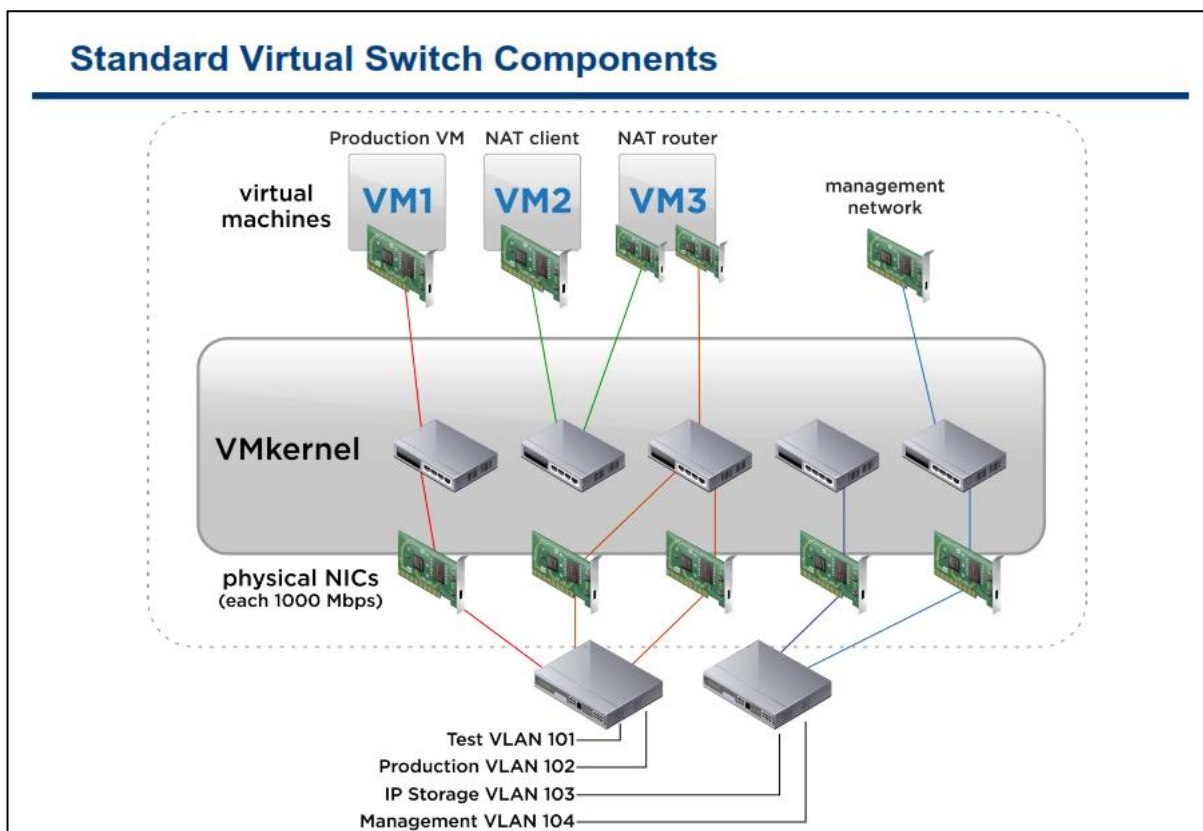
- vNetwork standard switches:
  - Virtual switch configuration for a single host
  - Discussed in this module
- vNetwork distributed switches:
  - Virtual switches that provide a consistent network configuration for virtual machines as they migrate across multiple hosts

یک Virtual Network از دو نوع Virtual Switch پشتیبانی می کند:

۱. **vNetwork Standard Switch**: یک **Standard Switch** برای یک هاست و در سطح هاست پیکربندی می شود. شما می توانید تا حداکثر ۴۰۸۸ پورت در هر **Standard Switch** و ۴۰۹۶ پورت در هر هاست تعریف نمایید.

۲. **vNetwork Distributed Switch**: همانند **Standard Switch** می باشد با این تفاوت که این **Switch** در سطح **vCenter** پیکربندی می شود. این امکان باعث می شود که شما صرفاً از یک سوئیچ مجازی برای کل محیط مجازی خود استفاده نمایید. این بدین معنی است تمام پورت های **Distributed Switch** برای تمامی هاست ها شناخته شده است. با استفاده از **Distributed Switch** شما می توانید بدون قطع شدن در اتصالات شبکه ماشین های مجازی خود را در میان هاست ها جابجا نمایید.

## کامپوننت های سوئیچ مجازی استاندارد



یک vSwitch Standard بستر را برای ارتباط vm ها در یک هاست فراهم می کند. در این اسلاید برای درک بیشتر پنج نمونه متفاوت از vSwitch Standard بیان شده است که به ترتیب از سمت چپ به راست تشریح خواهد شد:

- ۱- در این نمونه یک vSwitch Standard با یک NIC فیزیکی مرتبط شده است و با دنیای بیرون در ارتباط می باشد. این سوئیچ صرفاً برای vm1 مورد استفاده قرار می گیرد.
- ۲- صرفاً یک vSwitch Standard داخلی می باشد و با دنیای بیرون در ارتباط نیست. بدین ترتیب vm ها در یک هاست ESXi بطور مستقیم به vm های دیگر در همان vSwitch Standard ارتباط برقرار کنند. vm2 , vm3 از این سوئیچ برای ارتباط با یکدیگر استفاده کنند.
- ۳- یک vSwitch Standard می باشد که از قابلیت NIC teaming بهره مند می باشد. یعنی توزیع خودکار پکت ها را در میان چندین NIC فیزیکی و فراهم آوردن Failover برای vm ها. vm3 دارای NIC مجازی می باشد که به این سوئیچ متصل می باشد.
- ۴- این vSwitch Standard به هیچ یک از vm ها متصل نیست و صرفاً به VMKernel متصل می باشد. همانطور که در بخش قبلی بیان شد از VMKernel برای استفاده از قابلیت هایی همچون iSCSI و NAS-Based Storage استفاده می شود.
- ۵- یک vSwitch Standard که توسط VMKernel استفاده می شود و از طریق آن می توان به قابلیت Remote Management دسترسی داشت. در صورتیکه این vSwitch Standard برای اتصال به Remote

**Management** وجود نداشته باشد، شما امکان اتصال به هاست **ESXi** خود از طریق ابزارهایی همچون **vSphere Client** از دست خواهید داد.

نکته ۱: یک **vSwitch Standard** نمی تواند بطور مستقیم با یک **vSwitch Standard** دیگر در ارتباط باشد برای این کار شما باید از یک **vm** در میان دو **vSwitch Standard** استفاده نمائید. در واقع آن **vm** نقش **Gateway, Router, Firewall** به خود می گیرید که البته این کار باعث پیچیده تر شدن شبکه شما می شود. توصیه می شود تا حد امکان از این حالت بپرهیزید.

نکته ۲: همانطور که در بخش های گذشته بیان شد از سرویس **VMKernel** به منظور دسترسی به **Remote Management** و همچنین استفاده از این سرویس برای راه اندازی **NAS-Based Storage** و **iSCSI** استفاده می شود.

## پیکربندی سوئیچ مجازی استاندارد

### Default Standard Virtual Switch Configuration

The screenshot shows the configuration page for a Standard Switch (vSwitch0). Key elements include:

- View:** vSphere Standard Switch (selected) and vSphere Distributed Switch.
- Networking:** A tab with buttons for Refresh, Add Networking..., Properties..., and Delete the virtual switch.
- Standard Switch: vSwitch0:**
  - Virtual Machine Port Group:** Includes VM Network and VMkernel Port Management Network (vmk0: 172.20.10.51).
  - Physical Adapters:** Includes vmnic0 (1000 Full).
- Callouts:**
  - "Display standard virtual switches." points to the View dropdown.
  - "Delete the virtual switch." points to the Delete button.
  - "Enable IPv6 on ESXi host." points to the Networking tab.
  - "Display virtual switch properties." points to the Properties button.
  - "Display Cisco Discovery Protocol information." points to the vmnic0 adapter.
  - "Display port group properties." points to the VM Network port group.

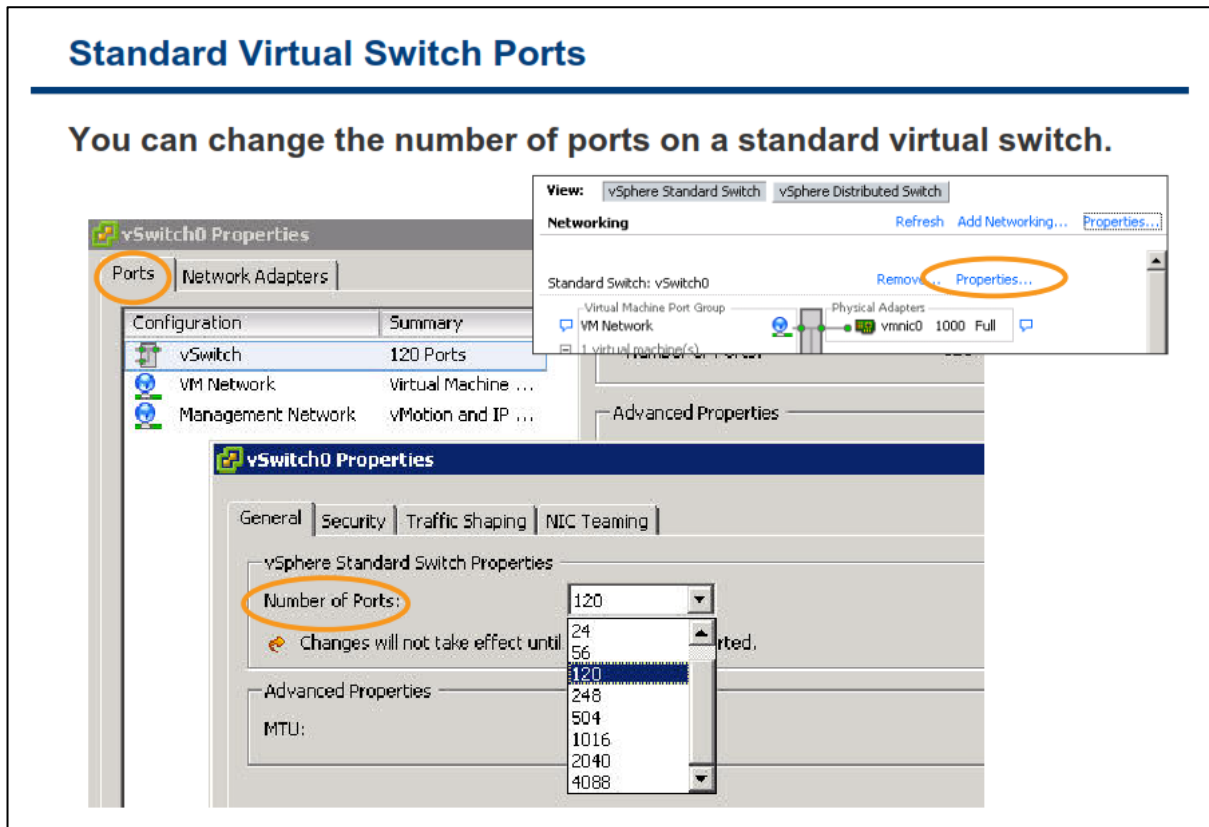
شما برای مشاهده پیکربندی vSwitch Standard هاست می توانید از سربرگ Configuration هاست ESXi بروی لینک **Networking** کلیک نمائید.

همانطور که در اسلاید بالا نمایش داده شده است، سوئیچ استاندارد vSwitch0 بروی هاست ESXi تعریف شده است. بطور پیش فرض در نصب هاست ESXi یک **Port Group** بنام **VM Network** و یک پورت **VMkernel** بنام **Management Network** ایجاد شده است. به عنوان بهترین تجربه به شما توصیه می شود که **VM Network** را از **Management Network** جدا نمائید و هر کدام از موارد بالا را حداقل بروی یک سوئیچ مجازی و بطور جداگانه قرار دهید. این کار باعث افزایش کارایی و امنیت می شود.

برای حذف یک vSwitch Standard بروی لینک **Remove** و برای دیدن مشخصات آن بروی **Properties** کلیک نمائید. برای مشاهده توضیحات پورت و **Port Group** می توانید بروی آیکن آبی رنگ راهنما کلیک کنید و یا در صورتیکه **Cisco Discovery Protocol** بروی سوئیچ فیزیکی شما فعال باشد می توانید مشخصات پورت فیزیکی سوئیچ سیسکو را نیز مشاهده نمائید.

**Cisco Discovery Protocol (CDP)** به مدیران این امکان را می دهد تا متوجه شوند که کدام پورت سوئیچ سیسکو به سوئیچ مجازی متصل شده است. زمانیکه **CDP** برای یک سوئیچ مجازی فعال می شود، شما می توانید مشخصات یک سوئیچ سیسکو را از طریق **vSphere Client** مشاهده نمائید. این مشخصات شامل **Device ID, Software Version, Timeout** می باشد.

## پورت های سوئیچ مجازی استاندارد

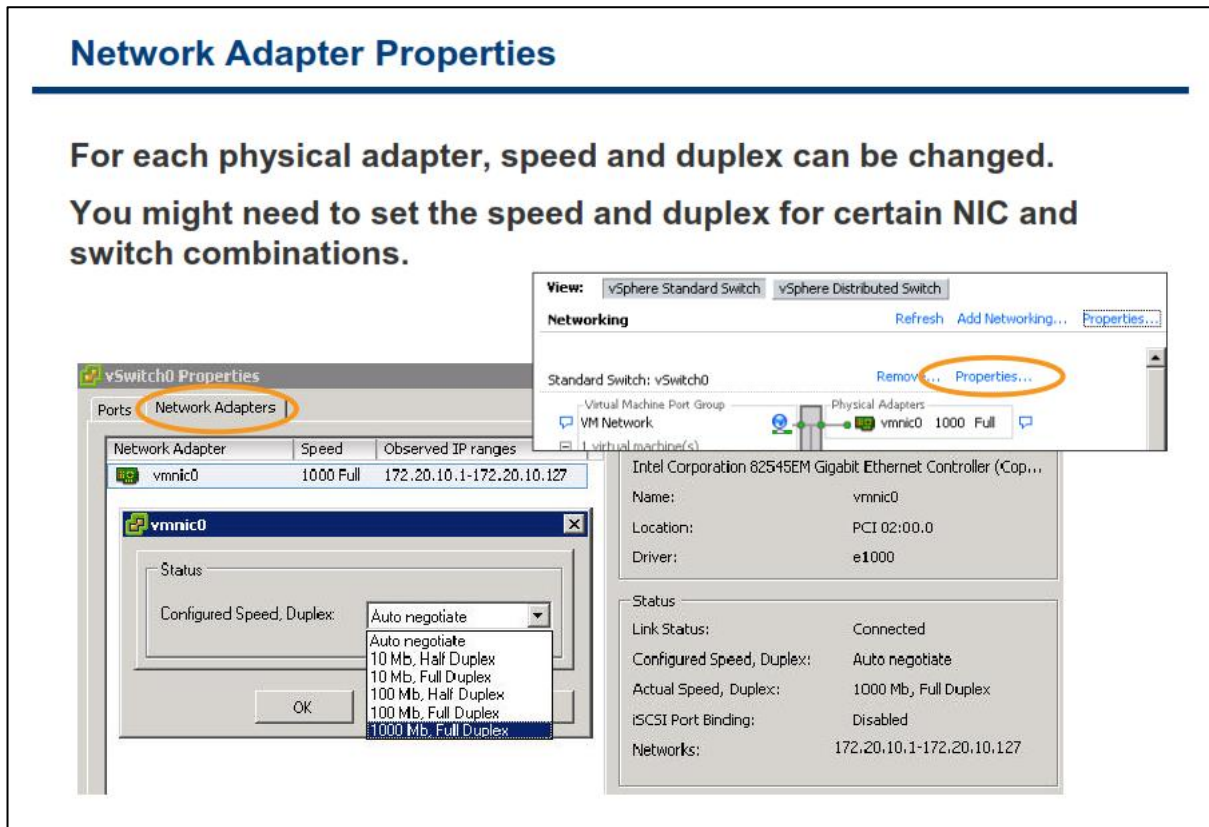


زمانیکه بروی گزینه **Properties** مربوط به سوئیچ استاندارد مجازی خود کلیک می نمائید، شما می توانید تعداد پورت های یک سوئیچ استاندارد مجازی را در سربرگ **General** تعیین نمائید.

زمانیکه یک **vSwitch Standard** ساخته می شود، بصورت پیش فرض ۱۲۰ پورت برای آن ایجاد می گردد. شما می توانید تعداد این پورت ها را تا ۴۰۸۸ پورت ارتقاء دهید. این پورت ها در ارتباطات میان ماشین های مجازی و **NIC** های فیزیکی هاست (**Uplink**) مورد استفاده قرار می گیرد. البته برخی از پورت ها توسط **VMKernel** مورد استفاده قرار می گیرد.

برای تغییر تعداد پورت ها مراحل زیر را می بایست انجام دهید:

۱. با استفاده از نرم افزار **vSphere Client** بروی هاست **ESXi** خود کلیک نمائید و به سربرگ **Configuration** مراجعه نمائید.
۲. بروی **Networking** کلیک نمائید.
۳. سپس بروی لینک **Properties** مربوط به سوئیچ مجازی خود کلیک نمائید و همانند اسلاید بالا تعداد پورت ها را تغییر دهید.



برای تغییر سرعت و همچنین Duplex بودن یک Virtual Network Adapter در vSwitch Standard می توانید مراحل زیر را دنبال کنید:

۱. با استفاده از نرم افزار vSphere Client هاست ESXi مورد نظر را انتخاب و به سربرگ Configuration مراجعه نمایید.
۲. بروی Networking کلیک نمایید.
۳. سپس در بخش Properties مربوط به vSwitch Standard مورد نظر به سربرگ Network Adapter مراجعه نمایید.
۴. در نهایت برای تغییر سرعت و Duplex بودن بروی دکمه Edit کلیک نمایید.

نکته: اگر شما از آداپتورهای شبکه 1 Gbps استفاده می کنید، تنظیمات مربوط به سرعت و Duplex را بروی Auto Negotiate قرار دهید چراکه حالت Auto Negotiate براساس استاندارد Gigabit Ethernet طراحی شده است. در سایر موارد توصیه می شود که بسته به NIC و پورت سوئیچ فیزیکی، سرعت و نوع آن را براساس نظیر آن انتخاب نمایید. برای مثال پورت 100Mbps را برای NIC فیزیکی 100Mbps انتخاب نمایید. اما برای پورت های 10 Gbps استفاده از Auto Negotiate پشتیبانی و توصیه نمی شود.

## VLANs

**ESXi supports 802.1Q VLAN tagging.**  
**Virtual switch tagging is one of three tagging policies supported.**

- Packets from a virtual machine are tagged as they exit the virtual switch.
- Packets are untagged as they return to the virtual machine.
- Affect on performance is minimal.

**ESXi provides VLAN support by giving a port group a VLAN ID**

**VLAN** یک گروه بندی منطقی میان پورت های سوئیچ است که به ماشین های مجازی و یا پورت هایی که در یک **VLAN** قرار دارند اجازه ارتباط می دهد. یک **VLAN** یک پیکربندی نرم افزاری برای **Broadcast Domain** می باشد. مزایای استفاده از **VLAN** شامل :

- ایجاد گروه بندی منطقی شبکه ها (براساس توپولوژی فیزیکی نمی باشد)
- بهبود کارایی بوسیله پیکربندی ترافیک **Broadcast** برای یک مجموعه ای از پورت های سوئیچ
- صرفه جویی در هزینه ها بوسیله جداسازی شبکه بدون استفاده از روتر های جدید

**VLAN** ها می توانند بروی مجموعه ای از پورت ها (**Port Group**) پیکربندی شوند. **ESXi** از **VLAN** ها، از طریق **Virtual Switch Tagging** پشتیبانی می کند. بدین ترتیب به **Port Group** یک **VLAN ID** تخصیص می دهد. (البته استفاده از **VLAN ID** اختیاری می باشد). **VMKernel** همه پکت های **Tag** شده و **Tag** نشده را از طریق **Virtual Switch** کنترل می کند. یک پورت سوئیچ فیزیکی می بایست بروی **ESXi** به عنوان یک **Static Trunk Port** تعریف شود. یک **Trunk Port** یک پورت بروی سوئیچ فیزیکی شبکه می باشد که در آن پکت ها **Tag** شده با یک **VLAN ID** دریافت و ارسال می شوند. الزاما برای یک **vm** نیازی به پیکربندی **VLAN** نیست. در واقع **vm** از اینکه به یک **VLAN** متصل شده و یا نشده آگاه نیست.

برای کسب اطلاعات بیشتر در خصوص پیاده سازی **VLAN** می توانید به مقاله **VMware ESX Server 3 802.1Q VLAN Solutions** در وب سایت [http://www.vmware.com/pdf/esx3\\_vlan\\_wp.pdf](http://www.vmware.com/pdf/esx3_vlan_wp.pdf) مراجعه نمائید.



## ملاحظات شبکه فیزیکی

## Physical Network Considerations

Discuss VMware vSphere® networking needs with your network administration team. Discuss the following issues:

- Number of physical switches
- Network bandwidth required
- Physical switch support for 802.3AD (for NIC teaming)
- Physical switch support for 802.1Q (for VLAN trunking)
- Network port security
- Cisco Discovery Protocol (CDP) and its operational modes: listen, broadcast, listen and broadcast, and disabled.

بدلیل اینکه محیط شبکه مجازی شما در نهایت متکی به شبکه فیزیکی می باشد، لذا یک vSphere Administrator باید در مورد نیاز های شبکه vSphere با تیم شبکه سازمان مشورت نماید. در اسلاید بالا لیستی از نیازها شبکه برای vSphere فراهم شده است که با استفاده از آنها می توانید به تحلیل نیازها و اقداماتی که باید صورت بپذیرید دست یابید. البته این لیست کامل نیست و تنها موارد پایه ای در آن مورد توجه قرار گرفته است.

- تعداد سوئیچ های فیزیکی
- سوئیچ های فیزیکی که از 802.3AD (برای NIC Teaming) پشتیبانی می کند
- سوئیچ های فیزیکی که از 802.1Q (برای VLAN Trunking) پشتیبانی می کند
- امکان CDP برای سوئیچ های Cisco
- پهنای باند مورد نیاز شبکه
- پورت های امنیتی شبکه

پارامترهای متعددی در طراحی یک شبکه مجازی دخیل هستند که علاوه بر موارد بالا آنها را نیز باید در نظر بگیرید. از جمله آنها می توان به مواردی همچون میزان تجهیزات شبکه ای که در دسترس قرار دارند، میزان پهنای باندی که نرم افزارهای کاربردی شما به آن نیاز دارند و قابلیت هایی که می خواهید از آنها استفاده نمائید (همچون NIC Teaming و VLAN و غیره) را در نظر بگیرید.



## کارگاه شماره هفت:

در این کارگاه آموزشی، شما یک سوئیچ مجازی شبکه و Port Group آن را ایجاد خواهید کرد که شامل موارد زیر می باشد:

۱. مشاهده پیکربندی سوئیچ مجازی استاندارد
۲. ایجاد یک سوئیچ مجازی استاندارد به همراه Port Group ماشین مجازی
۳. اتصال ماشین مجازی به یک Port Group سوئیچ مجازی

## بخش دوم: پیکربندی پالیسی های Standard Virtual Switch

بعد از به اتمام رساندن این بخش شما قادر خواهید بود:

- خصوصیات امنیتی یک Port Group سوئیچ مجازی استاندارد را تشریح نمائید که شامل موارد زیر می باشد:
  - VLANs
  - پالیسی های Security, Traffic Shaping, NIC Teaming

## پالیسی های شبکه

**Network Policies****Three network policies:**

- Security
- Traffic shaping
- NIC teaming

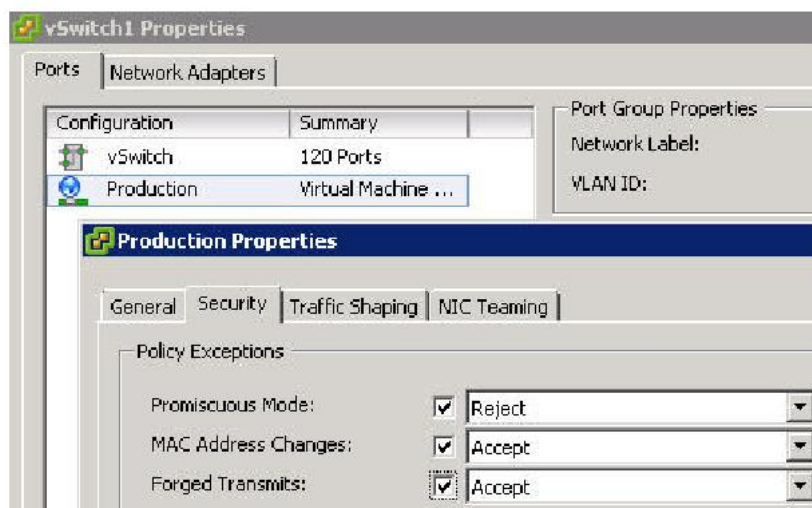
**Policies are defined:**

- At the standard virtual switch level:
  - Default policies for all the ports on the standard virtual switch
- At the port or port group level:
  - Effective policies: Policies defined at this level override the default policies set at the standard virtual switch level.

سه نوع پالیسی در شبکه مجازی وجود دارد که شامل Security، NIC Teaming، Traffic Shaping می باشد. این پالیسی ها را می توان برای کل vSwitch Standard تعریف نمود و یا همچنین می توانید آنها را بروی VMKernel Port و یا یک Port Group ماشین مجازی تعریف نمائید. بدین ترتیب زمانیکه شما یک پالیسی را بروی پورت های مجزا و Port Group تعریف می نمائید، آن پالیسی بروی پالیسی های پیش فرض قبلی جایگزین و Override می شود.

## Security Policy

Administrators can configure layer 2 Ethernet security options at the standard virtual switch and at the port groups.



پالیسی های امنیتی در **Virtual Switch** و **Port Group** تعریف می شوند. در واقع این پالیسی ها تعریف می شوند تا فریم های خروجی و ورودی را فیلتر نماید. (در سطح لایه ۲ OSI انجام می پذیرید). این پالیسی های امنیتی شامل استثنائات زیر می باشند:

- **Promiscuous Mode**: زمانیکه این گزینه به صورت **Reject** تعیین می شود **Virtual Network Adapter** ماشین مجازی هیچ فریمی را به غیر از فریمی که حاوی **MAC Address** خودش است را دریافت نمی کند. ولی زمانیکه به صورت **Accept** تعیین می شود، **Virtual Network Adapter** تمامی فریم هایی که بروی **vSwitch Standard** شناسایی می شوند و براساس **VLAN Policy** به آن پورت اجازه دسترسی به فریم داده می شود را دریافت می کند. برای مثال زمانیکه شما می خواهید از یک ماشین مجازی برای مانیتور کردن شبکه مجازی خود استفاده نمائید می توانید از گزینه **Accept** استفاده نمائید چراکه در این حالت به فریم های سایر ماشین های مجازی نیز دسترسی دارید. (گزینه پیش فرض **Reject** می باشد).
- **MAC Address Change**: زمانیکه این گزینه را به عنوان **Reject** انتخاب می کنید، اگر از طریق **Guest OS** ماشین مجازی، **MAC Address** ماشین مجازی تغییر کند و با **MAC Address** که در فایل **vmx** وجود دارد تطابق نداشته باشد همه فریم های ورودی **Drop** و یا رد خواهند شد و در صورتیکه **MAC Address** با **MAC Address** که در فایل **vmx** است مطابقت داشته باشد همه فریم ها دریافت خواهند شد. (گزینه پیش فرض **Accept** می باشد).

• **Forged Transmits**: (ارسال جعلی): زمانیکه این گزینه را به عنوان **Reject** انتخاب می کنید، اگر از طریق **Guest OS** ماشین مجازی، **MAC Address** ماشین مجازی تغییر کند و با **MAC Address** که در فایل **vmx** وجود دارد تطابق نداشته باشد همه فریم های خارجی و یا ارسالی رد خواهد شد و امکان ارسال آنها وجود نخواهد شد. اما زمانیکه **Accept** را انتخاب می کنید، فریم ها ارسال می گردد (گزینه پیش فرض **Accept** می باشد).

استفاده از حالت هایی بجز حالت های پیش فرض در برخی موارد لازم است مثلا زمانیکه شما از یک نرم افزار برای **Sniff** و آنالیز کردن شبکه خود استفاده می کنید. در غیر این صورت استفاده از موارد بالا امنیت سرور ها را تهدید خواهد کرد. برای مثال یک هکر می تواند از قابلیت **Promiscuous Mode** برای دریافت ترافیک شبکه به منظور انجام کارهای خرابکارانه استفاده نماید و یا برخی از افراد ممکن است با استفاده از **Spoofing MAC Address** به دسترسی های غیرمجازی دست یابند.

انتخاب گزینه **Reject** برای **Forged Transmits** و **MAC Address Change** به شما کمک می کند تا از حملات مشخصی که ممکن است از طریق ماشین های مجازی بوجود آید پیشگیری نمائید.

اما اگر ماشین های مجازی شما **MAC Address** را تغییر می دهد همانند برخی از **OS-based Firewall** ها شما می بایست برای **Forged Transmits** و **MAC Address Change** گزینه **Accept** را انتخاب نمائید.

برای تنظیم پالیسی های امنیتی باید مسیر زیر را دنبال کنید:

۱. از سربرگ **Configuration** هاست مورد نظر بروی لینک **Networking** کلیک نمائید.
۲. سپس بروی گزینه **Properties** مربوط به سوئیچ مجازی که می خواهید پالیسی آن را تغییر دهید کلیک نمائید.
۳. در کادر **vSwitch Properties** آن **Port Group** را که می خواهید تغییر دهید را انتخاب و بروی گزینه **Edit** کلیک نمائید.
۴. در نهایت به سربرگ **Security** بروید و تنظیمات خود را اعمال نمائید.

## Traffic-Shaping Policy

Network traffic shaping is a mechanism for controlling a virtual machine's network bandwidth.

Average rate, peak rate, and burst size are configurable.



Traffic Shaping می تواند در جایی که می خواهید محدودیت ترافیک را از یک vm به vm دیگر و یا از یک vm به گروهی از vm ها اعمال نمائید بسیار کاربردی باشد. اما به هر ترتیب شما می توانید از Traffic Shaping برای محافظت از vm و یا برای سایر ترافیک ها در شبکه های پر ازدحام نیز استفاده نمائید.

Network Traffic Shapping مکانیزمی برای کنترل پهنای باند شبکه ماشین مجازی می باشد و بروی vSwitch Standard و فقط بروی ترافیک خروجی شبکه اعمال می شود. برای کنترل ترافیک داخلی می بایست از Load-Balancing استفاده و یا از قابلیت rate-limiting روترهای فیزیکی خودتان استفاده نمائید.

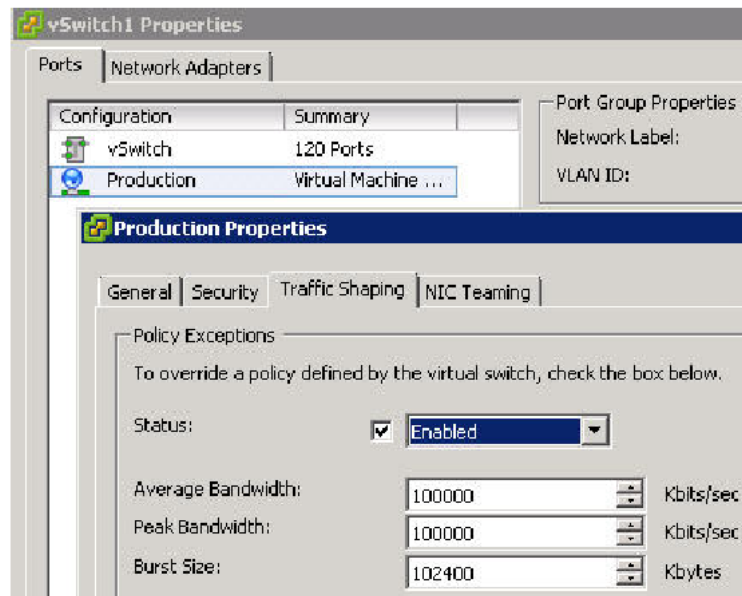
Traffic Shapping برحسب پارامترهای Average ، Peak Bandwidth و Burst Size پیکربندی می شود که در اسلاید بعدی تشریح خواهد شد.

## Configuring Traffic Shaping

Traffic shaping is disabled by default.

Parameters apply to each virtual NIC in the standard virtual switch.

On a standard switch, traffic shaping controls outbound traffic only.



Network Traffic shaping به صورت پیش فرض غیر فعال می باشد و در vSwitch Standard صرفاً بروی ترافیک خروجی فعال می شود. این امکان دارای پارامترهای متغیری می باشد که هم در سطح سوئیچ مجازی و هم در سطح Port Group تعریف می شوند. این پارامترها شامل:

- **Average Bandwidth:** متوسط پهنای باند (خروجی) مورد استفاده و مجاز که بر حسب کیلوبیت در ثانیه انتخاب می شود.
- **Peak Bandwidth:** حداکثر پهنای باند (خروجی) مورد استفاده و مجاز بر حسب کیلوبیت در ثانیه انتخاب می شود.
- **Burst Size:** اگر سایر پورت های سوئیچ از میزان پهنای باند خود استفاده نکنند، دیگر پورت ها می توانند بر حسب میزانی که شما تعیین می کنید از پهنای باند سایر پورت ها و تا حداکثر سرعت تعیین شده در **Peak Bandwidth** استفاده نمایند. برای مثال شما یک سوئیچ مجازی دارید که دارای ۵ پورت می باشد. در صورتیکه ۳ پورت این سوئیچ مجازی از پهنای باند تخصیص داده شده خود استفاده نکنند، ۲ پورت دیگر می توانند از پهنای باند آنها یا به اصطلاح از سرعت **Burst** تا حداکثر سرعت تعیین شده در **Peak Bandwidth** استفاده نمایند. حال اینکه این دو پورت چه میزان می توانند از این پهنای باند آزاد استفاده نمایند، مقداری است که شما می بایست آن را بر حسب کیلوبایت در کادر **Burst Size** وارد نمایید. میزان **Burst Size** از حاصل ضرب **Peak Bandwidth** در زمان (ثانیه) بدست می آید.

## NIC Teaming Policy

**NIC Teaming settings:**

- Load Balancing (outbound only)
- Network Failure Detection
- Notify Switches
- Failback
- Failover Order

Name	Speed	Networks
<b>Active Adapters</b>		
vmnic1	1000 Full	172.17.32.112-172.17.32.115
vmnic2	1000 Full	172.17.32.112-172.17.32.115
<b>Standby Adapters</b>		
<b>Unused Adapters</b>		

NIC Teaming Policy به شما اجازه می دهد تا ترافیک شبکه را بروی چندین NIC فیزیکی توزیع نمائید و یا در زمان Failure شدن، ترافیک را به سایر NIC ها مسیردهی نمائید. NIC Teaming شامل تنظیمات Load Balancing و Failure می باشد. NIC Teaming در حالت پیش فرض بروی کل vSwitch Standard تنظیم شده است. این تنظیمات می توانند در سطح Port Group اعمال و Override شوند یعنی شما در سطح Port Group یکسری استثنائات را برای سوئیچ مجازی مشخص نمائید.

برای تغییر NIC Teaming یک Port Group می بایست مسیر زیر را دنبال نمائید:

- به سربرگ Configuration هاست ESXi خود مراجعه نمائید و لینک Networking را انتخاب کنید.
- بروی گزینه Properties سوئیچ مورد نظر که Port Group در آنجا قرار دارد کلیک کنید.
- Port Group مورد نظر را از لیست پورت ها انتخاب کرده و بروی گزینه Edit کلیک نمائید.
- سپس به سربرگ NIC Teaming مراجعه نمائید و در آنجا تنظیمات را پیکربندی نمائید.

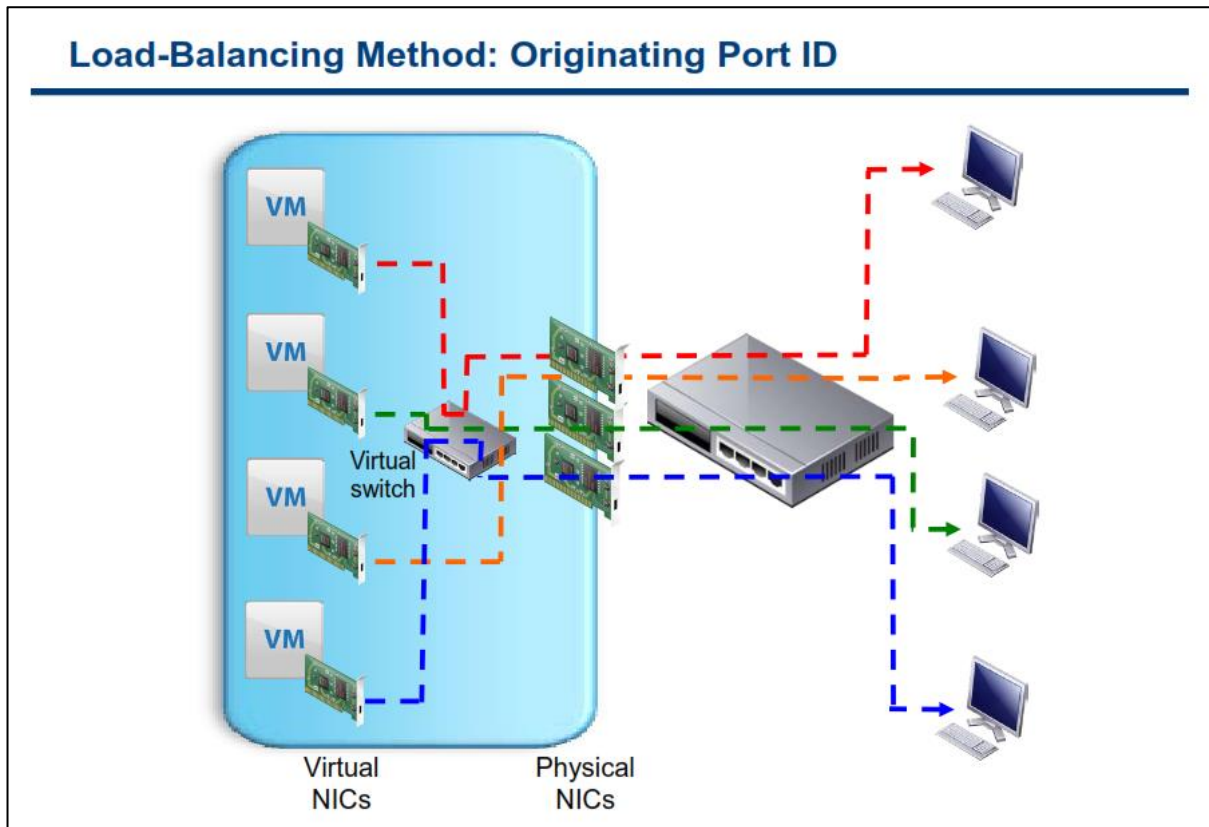
NIC Teaming شامل پیکربندی های زیر می باشد:

- Load Balancing (فقط برای ترافیک خروجی): با استفاده از این گزینه می توانید تعیین کنید که ترافیک خروجی چگونه و با چه متدی در میان آداپتورهای فیزیکی متصل به سوئیچ مجازی یا Port Group توزیع شود. Load Balancing ترافیک ورودی از طریق سوئیچ فیزیکی قابل کنترل است و در vmware تمهیداتی برای آن اندیشیده نشده است.



- **Network Failure Detection**: با استفاده از این گزینه می توانید مکانیزم تشخیص قطع و یا متصل بودن لینک شبکه را انتخاب نمایید. ESXi براساس این مکانیزم اقدام به انجام Failover می کند. این امکان بروی Guest VLAN Tagging پشتیبانی نمی شود.
- **Notify Switches**: اگر این گزینه را بروی Yes قرار دهید، هر گاه یک ترافیک یک NIC مجازی بخواهد از یک NIC فیزیکی متفاوتی (در صورتیکه NIC فیزیکی اصلی دچار مشکل شده باشد و حالت Failover رخ داده است) که در NIC Teaming قرار دارد عبور کند، یک پکت اطلاع رسانی بروی شبکه و به منظور بروز رسانی IP Table سوئیچ فیزیکی ارسال می گردد. در اکثر موارد این فرایند در کسری از ثانیه رخ می دهد و برای کاربر محسوس نخواهد بود. توجه داشته باشید که نباید از این گزینه در Microsoft Network Load Balancing و در حالت unicast استفاده نمایید. اما در حالت multicast انتخاب این گزینه مشکلی را بوجود نمی آورد.
- **Failback**: گزینه Failback نحوه برگشت یک NIC فیزیکی را به حالت active پس از Recovey مشخص می کند. اگر Failback برابر با NO باشد NIC فیزیکی که قبلا Fail شده و هم اکنون Recovey شده در لیست Adapter های Inactive باقی می ماند تا زمانیکه یک Active Adapter دچار مشکل و Fail شود و آنوقت این Adapter غیر فعال، وارد مدار شود و به حالت اکتیو در می آید، اما اگر Failback برابر با YES باشد هر زمان که Adapter - Fail شده Recovey شود بلافاصله وارد مدار می شود و با Standby Adapter که در زمان Failure جایگزین شده بود جابجا می شود.
- **Failover order**: این گزینه نیز شامل موارد زیر می گردد:
  ۱. **Active Adapter**: آداپتورهایی که در NIC Teaming مورد استفاده قرار می گیرند
  ۲. **Standby Adapter**: آداپتورهایی هستند که اگر یک یا چند Active Adapter دچار مشکل شوند و یا Fail شوند فعال و وارد مدار می گردند
  ۳. **Unused Adapter**: آداپتورهایی که در NIC Teaming مورد استفاده قرار نمی گیرند

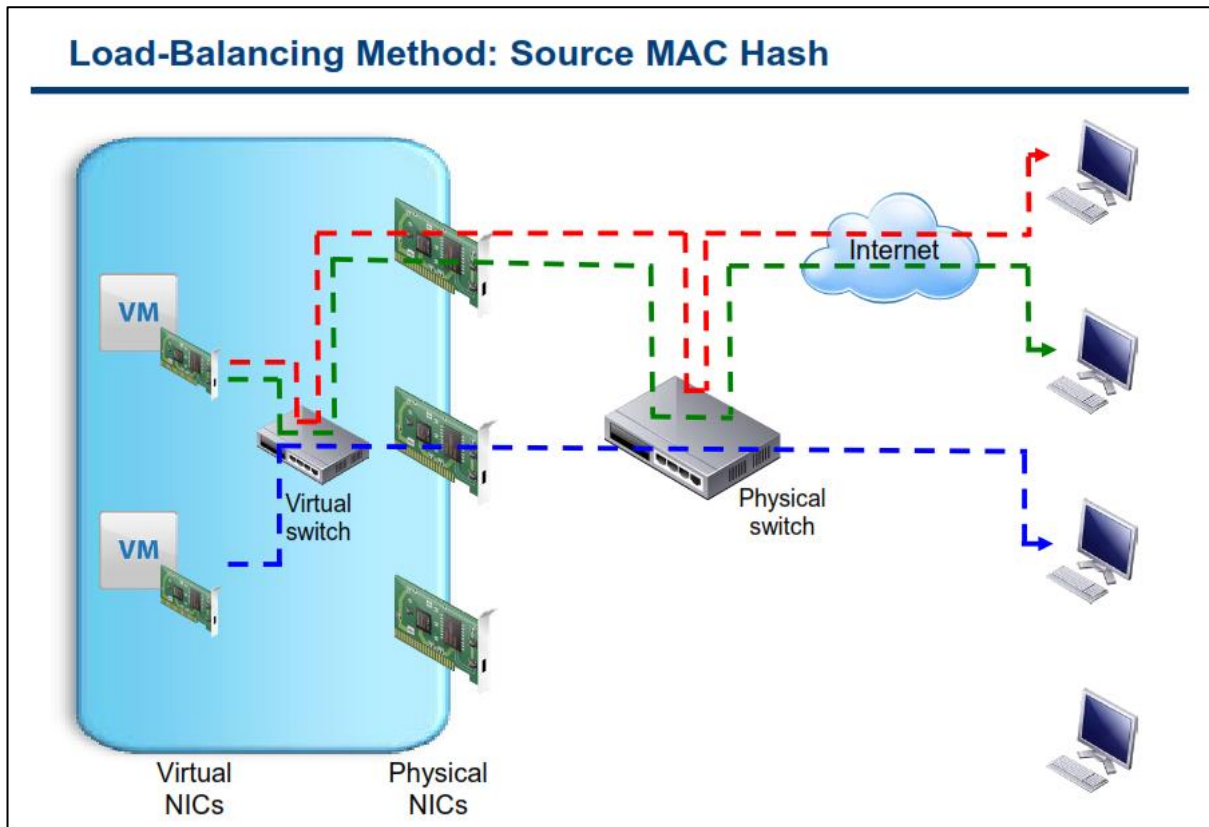
## متد Load Balancing: مبتنی بر Port ID



در این متد ترافیک خروجی هر یک از VM ها براساس شماره پورت آنها در سوئیچ مجازی از یک NIC فیزیکی به بیرون ارسال می شود. بطور مثال شما فرض نمائید از یک سوئیچ مجازی که دارای سه Uplink می باشد استفاده می نمائید. زمانیکه شما از متد Originating ID استفاده می نمائید، اولین VM که روشن می گردد ترافیک آن از طریق NIC-1 منتقل می شود سپس زمانیکه دومین VM روشن می گردد، ترافیک آن از طریق NIC-2 منتقل می شود. زمانیکه سومین VM روشن می گردد، ترافیک آن از طریق NIC-3 منتقل می شود و در نهایت زمانیکه چهارمین VM روشن می گردد، ترافیک آن از طریق NIC-1 منتقل می شود. این روش همانند روش Round Robin می باشد که در بسیاری از مسائل برنامه نویسی از آن استفاده می گردد. این روش ساده و سریع و بدون اینکه VMkernel درگیر شود انجام می پذیرد.

زمانیکه شما از این روش استفاده می کنید هر VM حداکثر از تمام پهنای باند فراهم شده توسط یک NIC فیزیکی استفاده می کند و نمی تواند از پهنای باند دو NIC و یا بیشتر برای یک VM استفاده نمود. این متد در تمامی سوئیچ های فیزیکی پشتیبانی می شود و قابل پیاده سازی نیز می باشد.

## متد Load Balancing مبتنی بر Source MAC Hash

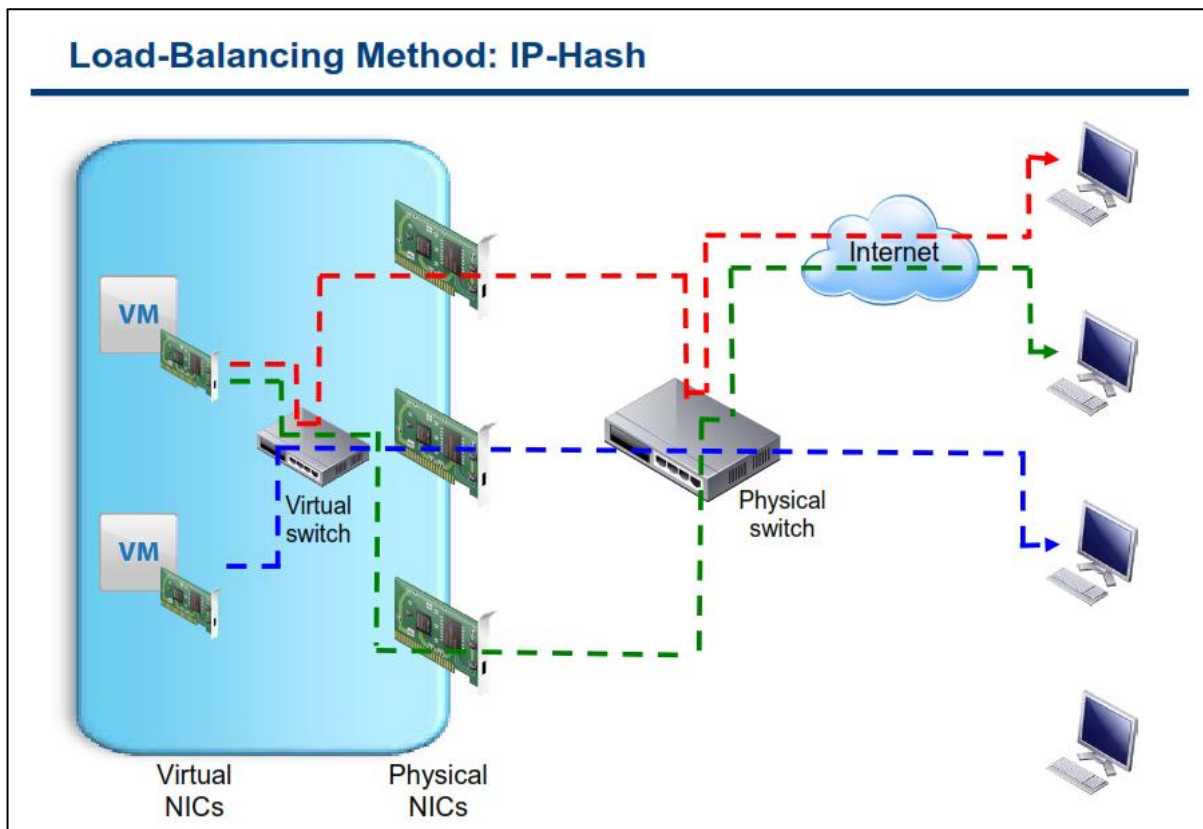


این متد نیز شبیه به متد Originated ID می باشد، با این تفاوت که بالانس نمودن ترافیک براساس MAC Address صورت می پذیرد. بطور مثال فرض نمائید در یک شبکه مجازی از یک سوئیچ مجازی با سه Uplink استفاده می نمائید و همچنین در شبکه خود از دو VM استفاده می نمائید. یکی از این VM ها دارای دو کارت شبکه مجازی می باشد. زمانیکه شما از متد Source MAC Address استفاده می نمائید، ترافیک اولین VM شما که دارای یک کارت شبکه مجازی می باشد از NIC-1 فیزیکی عبور می کند سپس دومین VM شما که دارای دو کارت شبکه می باشد، ترافیک کارت شبکه اول آن از NIC-2 آن عبور می کند و ترافیک کارت شبکه دوم آن از NIC-3 فیزیکی عبور می کند. در واقع هر کارت شبکه مجازی به یک کارت شبکه فیزیکی نگاشت (Map) می شود.

این متد با همه سوئیچ های فیزیکی سازگار می باشد و سربار کمتری نیز دارد ولی ممکن است ترافیک را در میان همه NIC های فیزیکی همانند شکل بالا منتقل نکند.

همانند متد Originated ID زمانیکه شما از این روش استفاده می کنید هر VM حداکثر از تمام پهنای باند فراهم شده توسط یک NIC فیزیکی استفاده می کند و نمی تواند از پهنای باند دو NIC و یا بیشتر برای یک VM استفاده نماید. این متد در تمامی سوئیچ های فیزیکی پشتیبانی می شود و قابل پیاده سازی نیز می باشد.

متد Load Balancing: مبتنی بر IP Hash



در متد IP Hash، هر NIC فیزیکی برای هر پکت و براساس IP Address مبداء و مقصد انتخاب می شود. بدین معنی که اولاً بالانس ترافیک براساس پکت صورت می پذیرد و ثانیاً انتخاب مسیر خروجی (NIC فیزیکی) بر مبنای IP Address مبداء و مقصد آن پکت صورت می پذیرد. این متد دارای سربار CPU بیشتری نسبت به حالت های قبلی می باشد اما دارای توزیع بهتری بروی همه NIC های فیزیکی می باشد.

متد IP Hash نیازمند آن است که سوئیچ فیزیکی شما از استاندارد 802.3ad یا همان EtherChannel پشتیبانی نماید. پروتکل LACP (Link Aggregation Control Protocol) متدی برای کنترل و مجتمع کردن چندین پورت فیزیکی به یک کانل واحد (به صورت Logical) می باشد. (LACP بخشی از IEEE 802.3ad می باشد) EtherChannel و 802.3ad هر دو شبیه به هم هستند و یک هدف را دنبال می کنند با این تفاوت که EtherChannel اساساً بروی سوئیچ های سیسکو و به منظور پورت ترانکینگ استفاده می شود. این تکنولوژی به شما امکان می دهد تا چندین پورت فیزیکی سوئیچ را به یک پورت مجازی تبدیل نمائید. از این روش برای Fault Tolerance و همچنین افزایش پهنای باند میان سوئیچ ها، روترها و سرور ها استفاده می شود.

زمانیکه شما از این متد IP hash استفاده می نمائید، یک NIC ماشین مجازی می تواند از پهنای باند چندین NIC فیزیکی استفاده نماید که بدین ترتیب شما می توانید از پهنای باند چندین Uplink برای یک VM استفاده نمائید.

زمانیکه یک vm با چندین Client متفاوت ارتباط برقرار می کند آن ترافیک ها از روی چندین NIC فیزیکی منتقل می شوند. همچنین ممکن است پکت ها از طریق چندین مسیر و چندین NIC فیزیکی مختلف به مقصد برسند که در این صورت می بایست بروی سوئیچ فیزیکی LACP پشتیبانی گردد.

توجه داشته باشید که قابلیت های vSphere تنها برای ترافیک خروجی می باشد و بروی ترافیک ورودی نمی تواند Load Balance را با قابلیت های vSphere پیاده سازی نماید.

برای مشاهده نیازمندیهای هاست ESXi برای Link Aggregation می توانید به مقاله <http://kb.vmware.com/kb/1001938> مراجعه نمایید.

## تشخیص و مدیریت خرابی شبکه

### Detecting and Handling Network Failure

Network failure is detected by the VMkernel, which monitors:

- Link state only
- Link state plus beaconing

Switches can be notified whenever:

- There is a failover event
- A new virtual NIC is connected to the virtual switch

Failover implemented by the VMkernel based on configurable parameters:

- Failback: How a physical adapter is returned to active duty after recovering from a failure
- Load-balancing option: Use explicit failover order. Always use the highest order uplink from the list of active adapters that pass failover detection criteria.



VMkernel می تواند از وضعیت لینک (Link Status) یا سیگنال Beacon و یا هر دوی آنها برای تشخیص قطع بودن شبکه استفاده نماید. وضعیت لینک (Link Status) مشکلات شبکه را از قبیل بیرون کشیدن کابل و مشکلات برقی سوئیچ فیزیکی شناسایی و مانیتور می کند. این مانیتورینگ، خطاهای پیکربندی و همچنین VLAN های اشتباه و ... را تشخیص نمی دهد و از طرفی دیگر بیرون کشیدن کابل و یا قطع شدن لینک بروی بخش دیگری از سوئیچ فیزیکی را شناسایی نمی کند. اما سیگنال Beacon وضعیت شبکه را از طریق یک پکت ۶۲ بایتی که هر ۱۰ ثانیه ارسال می شود بررسی می نماید.

زمانیکه سیگنال Beacon فعال است، VMkernel پکت های Beacon را برای همه NIC های فیزیکی در یک NIC Team ارسال می کند و سپس منتظر جواب می ماند. این تکنیک به مراتب کامل تر از تکنیک Link Status عمل می کند.

زمانیکه یک NIC مجازی به Switch مجازی متصل می شود VMkernel می تواند به سوئیچ فیزیکی اطلاع رسانی (Notify) نماید. همچنین هرگاه یک مشکلی در ارسال ترافیک NIC مجازی به یک NIC فیزیکی رخ دهد، یک سوئیچ فیزیکی می تواند آگاه شود. این اطلاع رسانی برای بروز رسانی IP Table سوئیچ های فیزیکی بروی شبکه ارسال می گردد.

در اکثر موارد این اطلاع رسانی مطلوب تر از مکانیزم های دیگر می باشد چراکه در غیر این صورت vm ها زمان تاخیر بیشتری را بعد از Failure و یا vMotion تجربه خواهد کرد. اما نمی توانید از این گزینه زمانیکه vm به Port Group که بروی آن Microsoft Network Load Balancing unicast-mode در حال اجرا هست، استفاده نمائید. (البته NLB در multicast-mode مشکلی ندارد و می توانید از این گزینه استفاده نمائید)

زمانیکه از **Failure Order** به صورت واضح استفاده می شود همیشه از بالاترین **NIC** فیزیکی در لیست **Active Adapter** برای شرایط **Failure-Detection** استفاده می شود.

گزینه **Failback** هم نحوه برگشت یک **NIC** فیزیکی را به حالت **Active** پس از **Recovery** مشخص می کند. اگر **Failback** برابر با **NO** باشد **Adapter** که قبلاً **Fail** شده و هم اکنون **Recovery** شده در لیست **Adapter** های **Inactive** باقی می ماند اما زمانیکه یک **Adapter Active** دچار مشکل و **Fail** شود و آنوقت این **Adapter** غیر فعال وارد مدار می شود و به حالت فعال در می آید.

ولی اگر **Failback** برابر با **YES** باشد هر زمان که **Adapter - Fail** شده **Recovery** شود، بلافاصله وارد مدار می شود و با **Standby Adapter** که در زمان **Failure** جایگزین شده بود جابجا می شود.



## فصل پنجم: پیکربندی و مدیریت Storage مجازی



این فصل شامل بخش های زیر می گردد:

۱. مفاهیم Storage
۲. پیکربندی iSCSI Storage
۳. پیکربندی NAS/NFS Storage
۴. Fiber Channel SAN Storage (به زودی)
۵. VMware vSphere VMFS Datastore (به زودی)
۶. VMware vSphere Storage Appliance (به زودی)

اهمیت این فصل:

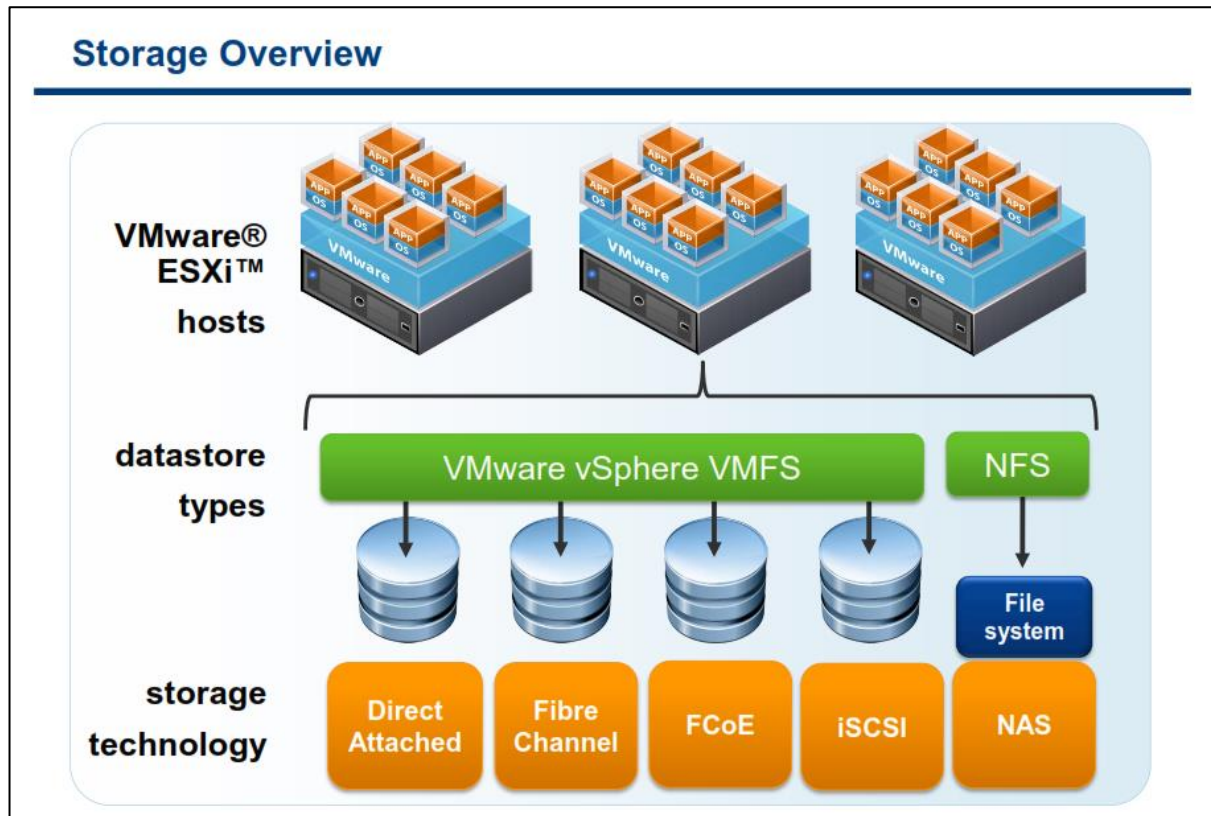
قابلیت های Storage در VMware این امکان را در اختیار شما می دهند تا براساس هزینه ، کارایی و نیازمندی های مدیریتی Storage خود، آن را پیکربندی نمائید. استفاده از یک Storage برای پشتیبان گیری، بازیابی و همچنین فعال نمودن قابلیت High Availability و انتقال VM ها میان هاست ها الزامی می باشد.



## بخش اول: مفاهیم Storage

بعد از به اتمام رساندن این بخش شما قادر خواهید بود:

- تکنولوژی ها و Datastore های VMware vSphere Storage را تشریح نمائید
- قراردادهای نام گذاری Storage ها را تشریح نمائید



هاست ESXi باید بگونه ای پیکربندی شود که از یک datastore به اشتراک گذاشته شده استفاده نماید. datastore مدل های منحصر بفردی را برای ذخیره سازی فایل های vm فراهم می کنند. بسته به نوع Storage، شما باید آن را با File System هایی همچون VMFS و یا یک File System Native و یا Storage Device هایی که از پروتکل NFS (Network File System) پشتیبانی می کنند فرمت و پیکربندی نمائید.

چندین تکنولوژی Storage توسط VMware ESXi پشتیبانی می شود که شامل موارد زیر می باشند:

- **DAS (Direct-Attached Storage):** در این تکنولوژی هارد دیسک های Internal, External بصورت Array و بطور مستقیم به هاست متصل می شوند. (در این تکنولوژی از اتصال مستقیم بجای ارتباطات شبکه ای استفاده می شود)
- **Fibre Channel:** یک پروتکل انتقال سریع داده که برای Storage Area Network یا همان SAN استفاده می شود. در تکنولوژی Fibre Channel دستورات بصورت پکت های SCSI و در میان نود های Fibre Channel انتقال پیدا می کند. عموماً نودهای یک Fibre Channel می تواند شامل سرور و Storage System و Tap Drive باشد. همچنین در مواردی از Fibre Channel Switch برای تبادل اطلاعات میان چندین Storage استفاده می شود. این فرم از Fiber Channel Network نام Fabric شناخته می شود. تجهیزات و پروتکل های این تکنولوژی با شبکه های مبتنی بر TCP/IP کاملاً متفاوت می باشند که از جمله آن می توان به آداپتورهای HBA اشاره کرد که همانند آداپتورهای NIC در شبکه TCP/IP عمل می کنند.

- **FCoE**: در این روش ترافیک **Fibre Channel** بروی قالب فریم های **Ethernet** و یا **Fibre Channel over Ethernet** پک و بسته بندی می شوند. بدین وسیله شما می توانید از یک لینک ارتباطی **TCP/IP** برای انتقال **Fibre Channel** و هم برای انتقال ترافیک و داده عادی شبکه استفاده کنید. **FCoE** باعث افزایش بهروری در استفاده از تجهیزات فیزیکی و همچنین باعث کاهش تعداد پورت های شبکه مورد نیاز و کابل کشی می شود. معمولاً پهنای باند این لینک ها در حدود **۱۰ Gbps** می باشد.
  - **iSCSI**: یک پروتکل انتقال **SCSI** می باشد با این تفاوت که دسترسی به **Storage** را از طریق **TCP/IP** استاندارد شبکه فراهم می کند. این متد **SCSI block-Oriented** را بروی **TCP/IP** نگاشت (**Map**) می کند. آغاز کننده ها یا همان **initiator** ها (همانند کارت سخت افزاری **iSCSI HBA** هستند که بروی هاست **ESXi** نصب شده اند) که دستورات **SCSI** را برای **Storage** ارسال و در **iSCSI Storage System** قرار می دهند.
  - **NAS (Network Attached Storage)**: یک **Storage** به اشتراک گذاشته شده می باشد که بروی شبکه استاندارد **TCP/IP** قرار دارد و در سطح **File System** می باشد. **NAS Storage** برای **NFS datastore** استفاده می شود. پروتکل **NFS** از دستورات **SCSI** پشتیبانی نمی کنند.
- در نتیجه **FCoE**, **NAS**, **iSCSI** می توانند بروی لینک **۱ Gbps** و یا **۱۰ Gbps** اجرا شوند. پورت **۱۰ Gbps** سطح کارایی **Storage** را افزایش می دهد و پهنای باند لازم را برای چندین نوع ترافیک در اختیار شما قرار می دهد.

## نگاه اجمالی به پروتکل های Storage

### Storage Protocol Overview

Storage Protocol	Supports boot from SAN	Supports VMware vSphere® vMotion®	Supports vSphere High Availability	Supports vSphere DRS	Supports Raw Device Mapping
Fibre Channel	•	•	•	•	•
FCoE	•	•	•	•	•
iSCSI	•	•	•	•	•
NFS		•	•	•	
DAS		(for virtual machine swap files)			•

از تکنولوژی Local Storage یا همان DAS خیلی از مدیران برای نصب ESXi استفاده می کنند. (DAS نقطه مقابل SAN می باشد). Local Storage برای محیط های کوچک ایده آل می باشد چراکه در هزینه های خرید و مدیریت SAN صرف جویی می کنند. اما استفاده نکردن از SAN باعث می شود تا شما بیشتر قابلیت های مجازی سازی را از دست بدهید برای مثال بالانس حجم کاری و همچنین Live Migration را در میان هاست های خود نخواهید داشت. همچنین DAS می تواند برای ذخیره داده های غیر حیاتی از جمله ISO CD\DVD ، VM Template و VM های غیر ضروری و آزمایشگاهی مورد استفاده قرار گیرد.

استفاده از SAN باعث فعال شدن قابلیت هایی همچون vMotion، HA و DRS می شود. همچنین امکانات قدرتمندی را برای شما فراهم میکند که از جمله آن می توان به موارد زیر اشاره نمود:

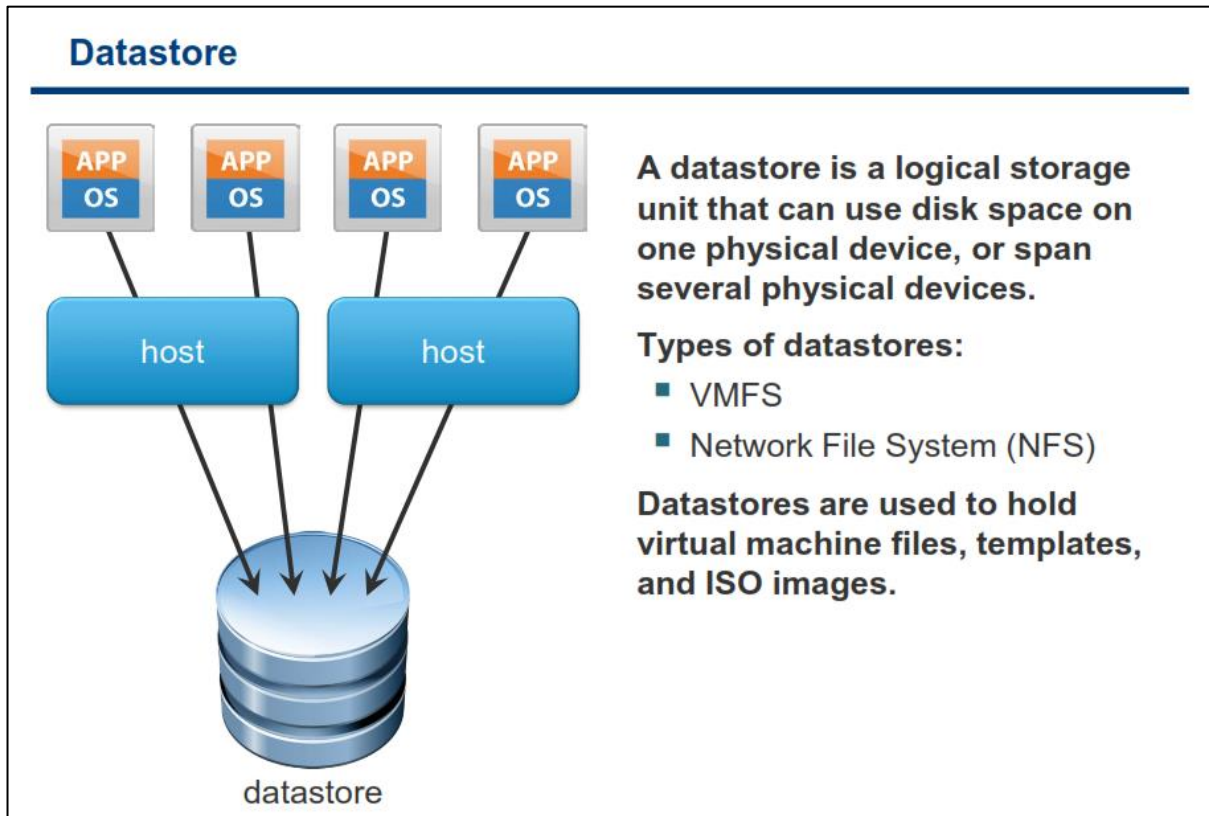
- VM Clustering در میان هاست های ESXi
- تخصیص فضای بسیار زیاد در حد ترابایت برای هاست های ESXi
- مخزن مرکزی برای ذخیره فایل های vm و template ها

ESXi همچنین از متدهای مختلفی برای بوت شدن از SAN پشتیبانی می کند. این امکان باعث می شود که در حین تعمیر و نگهداری (Maintenance) نیاز به Additional Local Storage و یا سرورهایی همچون Blade System که هارد دیسک ندارند نباشد. زمانیکه که شما هاست خود را برای بوت شدن از روی SAN پیکربندی می کنید Boot Image هاست بروی یک یا چندین LUN (یک شماره منطقی برای بخش های Storage می باشد که از آن برای آدرس دهی در دستگاه های

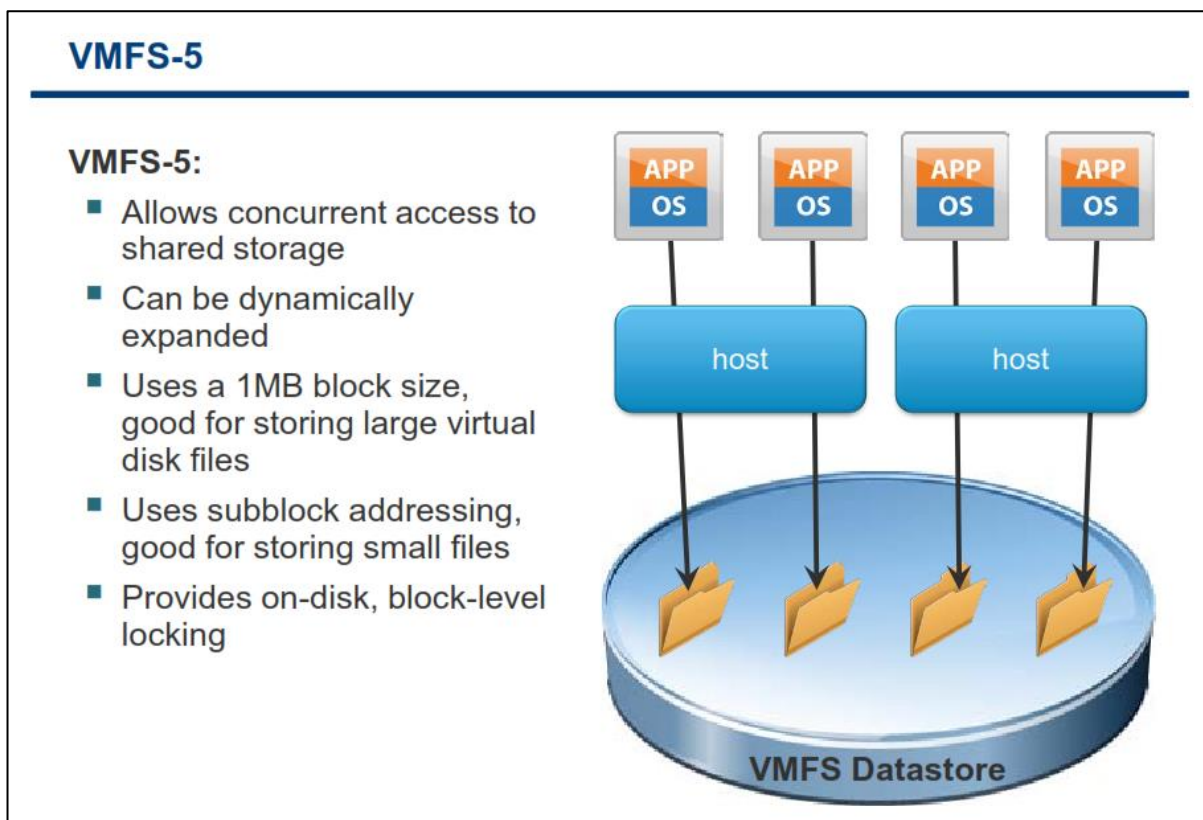
مبتهی بر پروتکل SCSI استفاده می شود) ذخیره می شود و زمانیکه هاست روشن می شود هاست از روی LUN های SAN که ارجهتر از Local Disk آن سرور می باشد بوت می شود. هاست های ESXi فقط از یک سخت افزار iSCSI Adapter مستقل برای بوت شدن پشتیبانی می کند.

هاست های ESXi از Software iSCSI Adapter و Hardware iSCSI Adapter برای بوت شدن پشتیبانی می کند. نکته ای که در این خصوص وجود دارد این است که کارت شبکه و یا همان Network adapter باید فقط از فرمت iSCSI Boot Firmware Table (iBFT) پشتیبانی نماید. iBFT متد ارتباطی برای بوت شدن دستگاه ها از روی iSCSI می باشد.

## Datastore



**Datastore** نیز یک واژه مفهومی و عمومی برای محل ذخیره سازی فایل ها می باشد. یک **Datastore** می تواند در دو فرمت **VMFS** و **NFS** باشد. با هر یک از این دو فرمت **Datastore** می تواند در میان چندین هاست **ESXi** به اشتراک گذاشته شود. شما همچنین می توانید از **Datastore** ها برای ذخیره کردن **Image CD\DVD** , **Floppy Image** , **Template** استفاده نمائید.



VMFS یک File System توزیعی و کلاستری می باشد که به چندین سرور اجازه می دهد که بطور همزمان بروی آن بنویسند و یا از آن بخوانند. VMFS یکسری سرویس های منحصر بفرد برای مجازی سازی فراهم می کند که شامل:

- Migration ماشین های مجازی از یک سرور فیزیکی به سرور فیزیکی دیگر بدون Downtime
- Restart خودکار ماشین های مجازی Fail شده بروی یک سرور فیزیکی مجزا
- Clustering ماشین های مجازی بروی چندین سرور فیزیکی

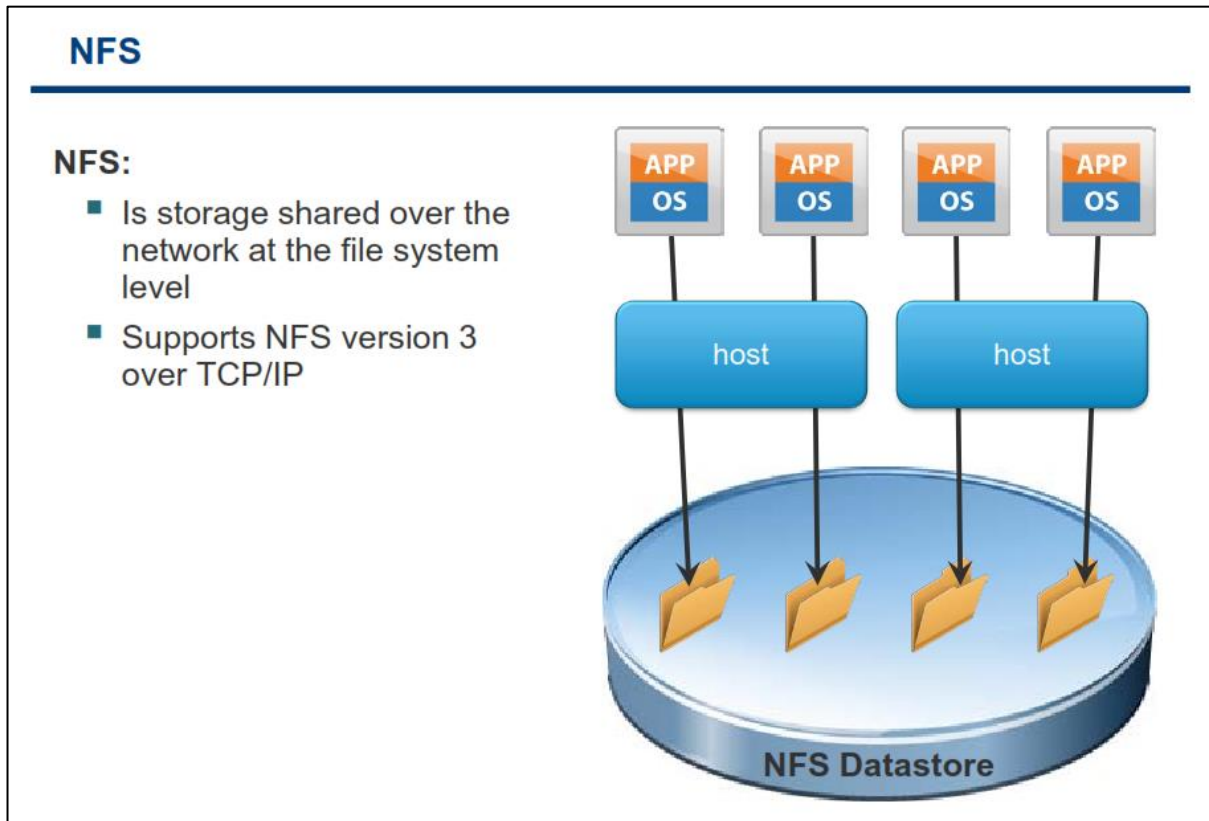
VMFS به چندین ESXi اجازه می دهد بطور همزمان به VM Storage به اشتراک گذاشته شده دسترسی داشته باشند. اندازه یک VMFS Datastore در حین اجرای vm و روشن بودن آن می تواند بصورت دینامیکی افزایش پیدا می کند. یک VMFS Datastore می تواند بصورت کارآمد داده های بزرگ و کوچک مربوط به vm را ذخیره کند. VMFS Datastore می تواند از فایل های vmdk با حجمی بیش از 2.0 TB نیز پشتیبانی نماید. همچنین VMFS می تواند از Subblock Addressing برای استفاده کارآمدتر از Storage در ذخیره و بازیابی فایل هایی با حجم کم مورد استفاده قرار گیرد.

از آنجائیکه اجرای همزمان یک vm بروی دو هاست باعث خراب شدن فایل های vm می شود، VMFS از یک متد بنام Block-level Distributed Locking برای حصول اطمینان از اینکه یک vm در یک زمان بروی چندین سرور فیزیکی روشن نباشد استفاده می کند. اگر یک سرور فیزیکی Fail شود on-Disk Lock برای vm منتشر می شود و vm می تواند بروی سرور فیزیکی دیگر restart شود. بدین ترتیب پس از Fail شدن هاست یک VM، آن VM بروی سرور دیگر مجددا روشن می گردد.

VMFS datastore از یک یا چندین LUN تشکیل شده است. Virtual Disk هایی که بروی VMFS datastore ذخیره می شوند همیشه به عنوان SCSI device برای vm شناخته می شوند.

VMFS می تواند بروی چندین SCSI-base Storage همچون iSCSI , FC Storage , DAS توسعه پیدا کند. VMFS توسط vm دیده نمی شود و ماشین های مجازی تنها File System خودشان را و یا به اصطلاح native خود را می بیند.





NFS یک پروتکل اشتراک فایل می باشد که ESXi با استفاده از آن می تواند با NAS ارتباط برقرار کند. NAS یک دستگاه خاصی است که به شبکه متصل می شود و می تواند سرویس اشتراک فایل را برای هاست ESXi فراهم نماید.

NFS شبیه به VMFS می باشد و برای ذخیره فایل های vm , Template و ISO می توان از آنها استفاده نمود بعلاوه اینکه از NFS می توان برای Migration با استفاده از امکان vMotion استفاده نمود. نکته اینکه ESXi از NFS نسخه ۳ پشتیبانی می کند.

ESXi از پروتکل Network Lock Manager استفاده نمی کند(از این پروتکل استاندارد برای پشتیبانی فایل Locking در NFS استفاده می شود) اما در عوض vmware از پروتکل Locking خودش استفاده می کند. NFS برای Lock کردن، فایل lock را با نام lck-fileid بروی NFS server ایجاد می کند. زمانیکه که فایل Lock ایجاد می شود یک update بصورت دوره ای برای سایر هاست های ESXi ارسال می شود تا به آنها اطلاع دهد که هنوز Lock فعال می باشد.

جهت کسب اطلاعات بیشتر در خصوص NFS Locking شما می توانید به مقاله موجود در لینک زیر مراجعه نمایید:

<http://kb.vmware.com/kb/1007909>

## Storage Device Naming Conventions

Storage devices are identified in several ways:

- SCSI ID – Unique SCSI identifier
- Canonical name – The Network Address Authority (NAA) ID is a unique LUN identifier, guaranteed to be persistent across reboots.
  - In addition to NAA IDs, devices can also be identified with mpx or t10 identifiers.
- Runtime name – Uses the convention vmhbaN:C:T:L. This name is not persistent through reboots.

SCSI ID	Canonical Name	Runtime Name	Lun
010001000020204573785...	t10.94544500000000000000000001000000...	vmhba34:CO:T0:L1	1
020003000060060160eb7...	naa.60060160eb7026007ef7a4b3a50adf11	vmhba0:CO:T1:L3	3
020019000060060160eb7...	naa.60060160eb7026002666a802a60adf11	vmhba0:CO:T1:L25	25
0200030000600805f3001...	naa.600805f30016be8000000000131700d6	vmhba0:CO:T0:L3	3

اگر ما بخواهیم در یک بستر مجازی از Storage ها استفاده نمائیم قطعاً نیازمند شناسه هر Storage هستیم چرا که برای آدرس دهی یک Storage در شبکه نمی توان از روش هایی همچون IP و غیره استفاده کرد و لذا می بایست از قراردادهای نام گذاری این تجهیزات اطلاع داشت و از آن استفاده نمود. در ESXi دستگاه های SCSI یا Storage ها با استفاده از شناسه های متفاوتی شناخته می شوند که هر شناسه یک هدف مشخصی دارد. برای مثال VMKernel نیازمند یک شناسه می باشد که توسط Storage تولید شده است. اگر یک شناسه منحصر به فرد نمی تواند توسط Storage تعیین شود، VMkernel باید یک شناسه منحصر به فرد دیگری را برای هر LUN و یا Disk تولید کند. بسته به نوع Storage هاست ESXi این شناسه ها را براساس الگوریتم های و قراردادهای متفاوتی ایجاد می کند. این شناسه ها شامل:

۱. SCSI ID: یک آدرس منحصر به فردی از دستگاه SCSI می باشد.
۲. Canonical name: این شناسه شبیه به MAC Address در کامپیوتر ها می باشد و شناسه ای است که اکثر Storage ها از آن بهره می برند و هاست ESXi صرفاً آن را با استفاده از دستوراتی از Storage می خواند. این شناسه دائمی (بعد از هر Reboot تغییر پیدا نمی کند) است و در میان تمامی Storage ها منحصر به فرد می باشد. این شناسه در یکی از قالب های زیر نمایش داده می شود.
  - **naa.number**: نام دیگر آن Network Address Authority ID -NNA ID که شناسه های جهانی و بین المللی هستند که پس از reboot نیز تغییر پیدا نمی کنند

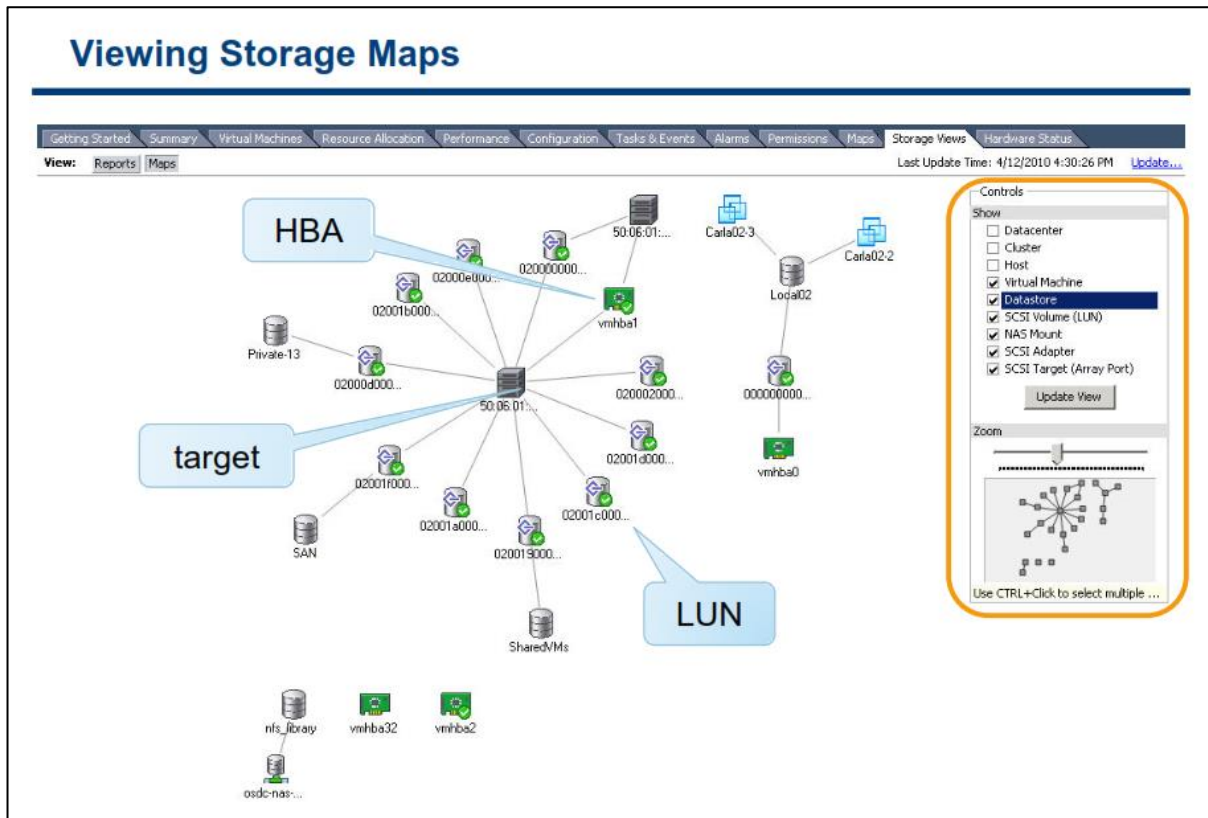
- **t10.number**: شناسه ۱۰T نیز یک شناسه منحصر به فرد دیگر است که می تواند روی هر SCSI Device ارائه شود. شبیه NNA ID و شناسه MAC، این شناسه توسط موسسه IETF برای شناسایی vendor ها انتساب داده می شود. این شناسه همیشه با رشته "۱۰t" شروع می شود.
- **eui.number**: پیشوند "eui" که یک نام ۱۶ کاراکتری می باشد. این نام شامل ۲۴ بیت برای نام شرکت می باشد که آن توسط IEEE انتساب داده میشود و ۴۰ بیت آن برای یک ID منحصر به فرد می باشد.

نکته: در صورتیکه هیچکدام از شناسه های بالا توسط هاست دریافت نشود خود ESXi شناسه ای با قالب `mpx.path` تولید می کند. برای مثال ، `mpx.vmhba1:C0:T1:L3` . این شناسه دائمی نبوده و حتی منحصر به فرد نیز نمی باشد.

۳. **Runtime Name**: این شناسه نام اولین مسیر به Storage می باشد که توسط هاست تولید می شود. این شناسه برای دستگاه قابل اعتماد نمی باشد چراکه دائمی نیست و ممکن است زمانیکه شما یک کارت HBA را به هاست اضافه می کنید این آدرس تغییر پیدا کند.

شاید از خودتان سوال کنید که چرا **vmware** از این همه شناسه برای شناسایی Storage ها استفاده می کند. جواب این سوال در این نکته خلاصه شده است که Storage ها جزو تکنولوژی ها نوین می باشند و هنوز استاندارد یکسانی برای آنها در دنیا فراهم نشده است و هر سازنده ای از یک شناسه بروی محصول خود استفاده می کند. به همین دلیل **vmware** تلاش کرده تا از تمامی استانداردها پشتیبانی نماید.

نمای نقشه‌ای Storage



با استفاده از ابزار Storage Map شما می‌توانید نقشه و وضعیت Storage های خود را مشاهده نمایید و از آن برای عیب‌یابی استفاده نمایید. برای مثال شما می‌توانید از این بخش رابطه و تعداد مسیرهای میان vm، Storage، هاست و HBA Adapter را مشاهده نمایید.

## ملاحظات که در Storage های فیزیکی باید مورد توجه قرار گیرد

### Physical Storage Considerations

Discuss vSphere storage needs with your storage administration team, such as:

- LUN sizes
- I/O bandwidth
- Disk cache parameters
- Zoning and masking
- Identical LUN presentation to each ESXi host
- Active-active or active-passive arrays
- Export properties for NFS datastores

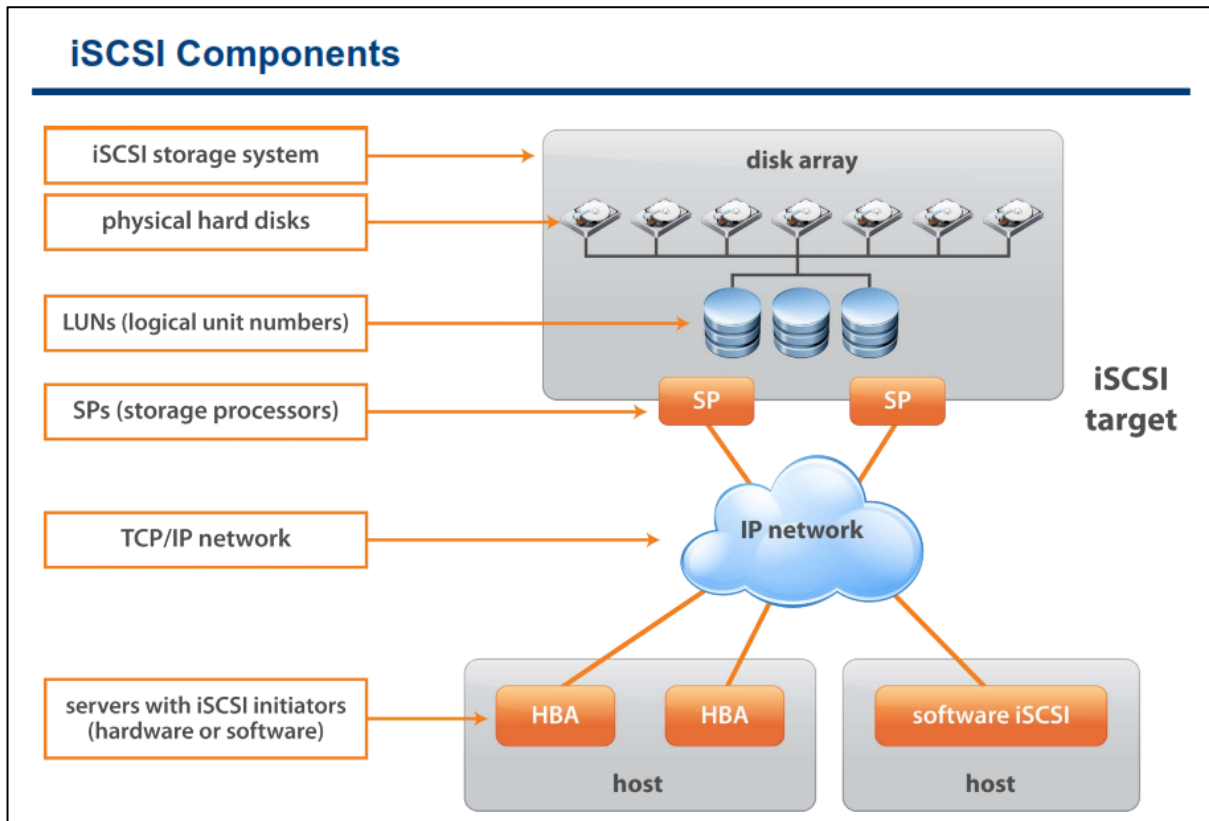
در صورتیکه شما می خواهید vSphere را در سازمان خود راه اندازی نمایید قبل از آن می بایست درباره نیازمندی های Storage با سرپرستان و تکنسین های آن مشورت نمایید. بطور مثال شما می بایست درباره مسائل زیر با آنها مشاوره نمایید و به یک تصمیم مشخص را اتخاذ نمایید.

- اندازه و حجم هر LUN
- I/O Bandwidth مورد نیاز برای برنامه ها
- پارامترهای Disk Cache, Zoning, Masking
- LUN های ارائه شده برای هر ESXi
- Multipathing Setting (Active-Active یا Active-Passive) برای Storage
- تنظیمات NFS

## بخش دوم: پیکربندی iSCSI Storage

بعد از به اتمام رساندن این بخش شما قادر خواهید بود:

- استفاده از IP Storage در ESXi تشریح کنید
- کامپوننت ها و آدرس دهی iSCSI را تشریح کنید
- iSCSI Initiator را پیکربندی نمائید

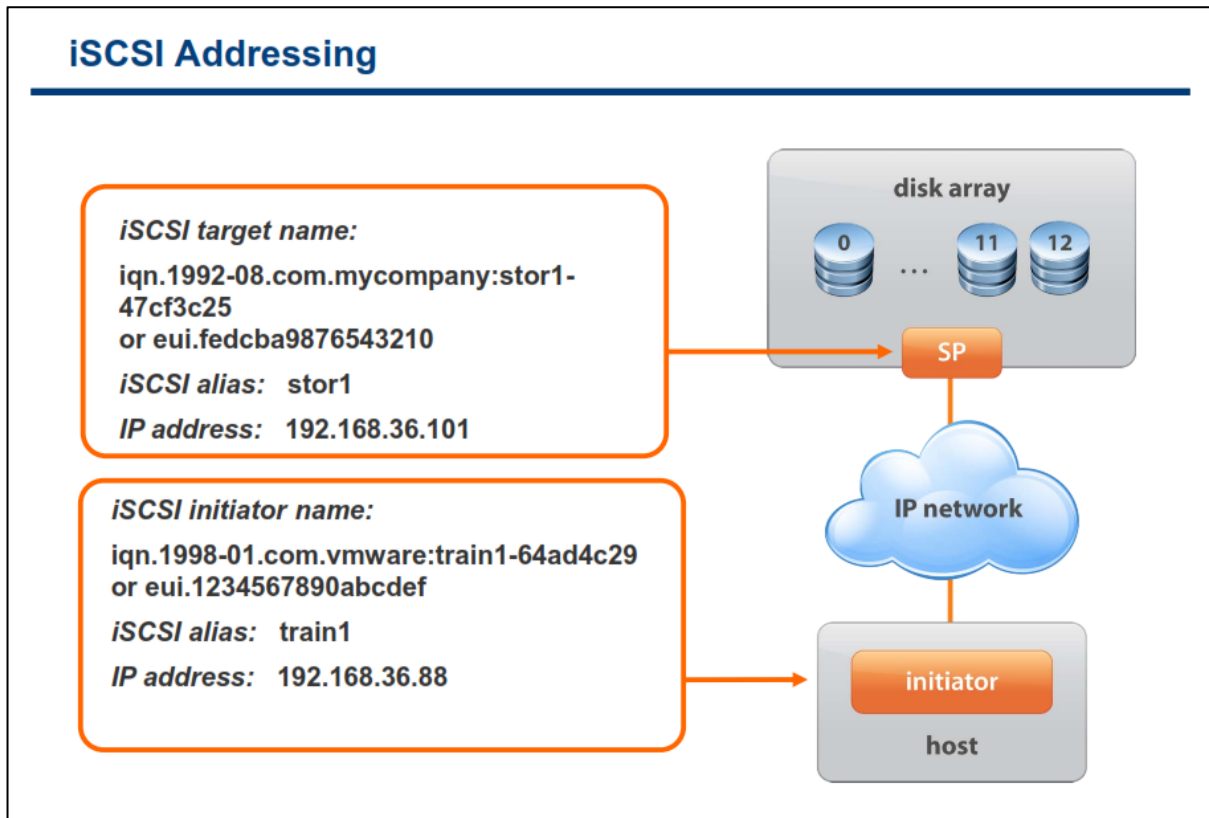


یک iSCSI SAN یک iSCSI Storage System می باشد که شامل یک یا چندین LUN و همچنین شامل یک یا چندین Storage Processor یا همان SP می باشد. ارتباط میان Storage و هاست بروی TCP/IP انجام می شود. هاست ESXi با یک iSCSI Initiator پیکربندی می شود. یک Initiator می تواند Hardware-base باشد همانند HBA و یا Software-base باشد که بنام iSCSI Software Initiator در vSphere شناخته می شود.

یک Initiator دستورات SCSI را به یک IP در شبکه ارسال می کند. یک Target نیز دستورات SCSI را از روی یک یا چند IP در شبکه دریافت می کند. شما می توانید چندین Initiator و Target در iSCSI network خود داشته باشید. iSCSI بصورت SAN عمل می کند چراکه Initiator یک یا چندین Target را پیدا می کند، یک Target تمام LUN ها را به Initiator ارائه می کند و از طرف دیگر Initiator دستورات SCSI را ارسال می کند. Initiator ها در هاست ESXi مقیم هستند و Target ها نیز در Storage قرار هستند.

iSCSI Array ها می توانند دسترسی هاست به Target را با استفاده از چندین مکانیزم همانند IP Address یا Subnet و یا Authentication محدود نمایند.

## آدرس دهی و نام گذاری iSCSI Node



مدخل های قابل آدرس دهی و قابل کشف شدن را **iSCSI node** می گویند. یک **iSCSI node** نیاز به یک نام دارد که براساس آن مدیریت شود. **iSCSI name** می تواند براساس فرمت های زیر باشد:

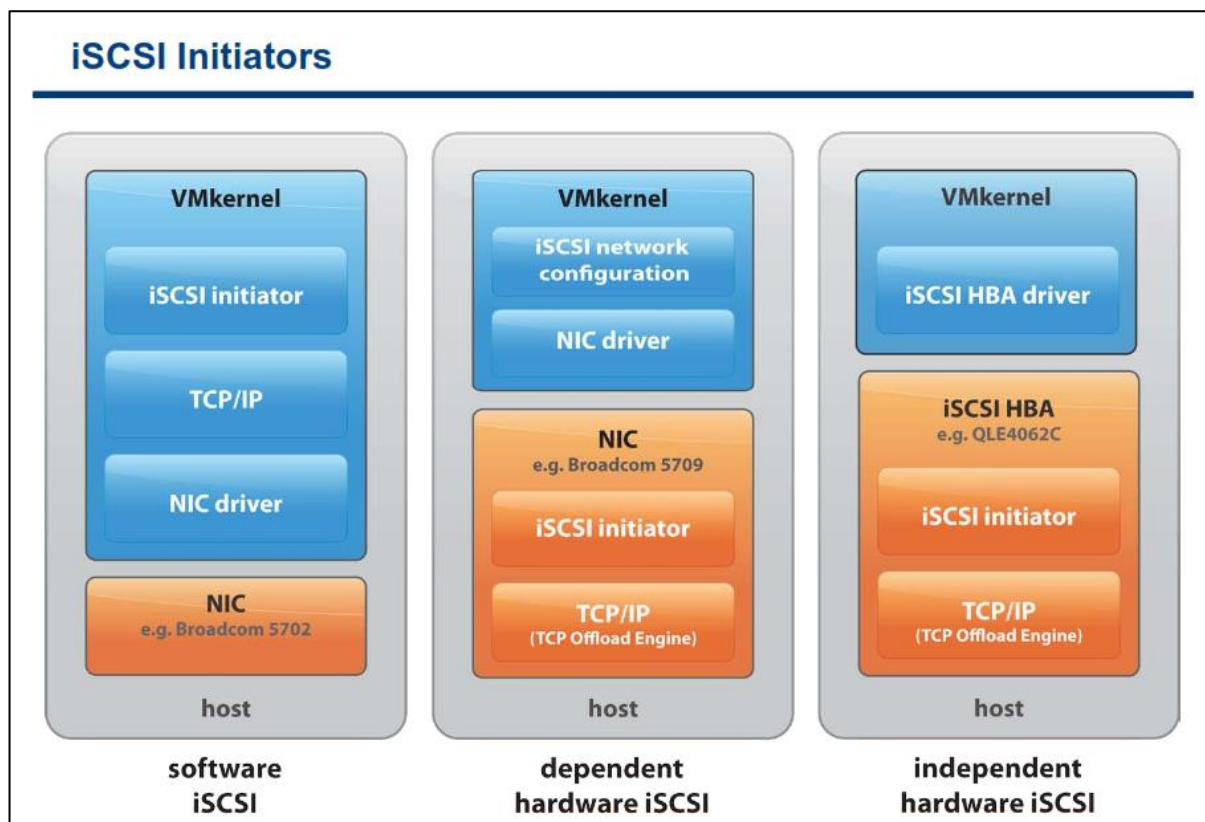
**iSCSI Qualified Name** یا **IQN: IQN** حداکثر ۲۵۵ کاراکتر می باشد که متشکل از این موارد می باشد:

- پیشوند **iqn**
- تاریخ که شامل تاریخ ماه و سالی است که **Domain** و **Sub Domain** در آن ثبت شده است.
- رشته نامی معتبر می باشد که معمولا شامل نام **Domain** و **Sub Domain** رزرو شده می باشد.
- علامت (**:**)
- نام منحصر به فردی که می بایست توسط شما انتخاب شود.

**EUI naming**: پیشوند **"eui"** که یک نام ۱۶ کاراکتری می باشد. این نام شامل ۲۴ بیت برای نام شرکت می باشد که توسط **IEEE** انتساب داده می شود و ۴۰ بیت دیگر آن نیز یک **ID** منحصر به فرد می باشد.



آغاز کننده iSCSI — iSCSI Initiator



برای دسترسی به iSCSI Target ها، هاست شما می بایست از Initiator ها استفاده کند. Initiator ها دستورات SCSI را بین هاست و iSCSI target در قالب پروتکل iSCSI کپسوله می کنند و سپس دریافت و ارسال می کنند. هاست ESXi از دو نوع Initiator پشتیبانی می کند: Software iSCSI initiator , Hardware iSCSI initiator

Software iSCSI Initiator یک کد built-in است که توسط vmware در داخل VMKernel ایجاد شده است و با استفاده از آن می توانید بدون نیاز به خرید سخت افزارهای خاص از تکنولوژی iSCSI استفاده نمایید. این نوع Initiator به شما اجازه می دهد که هاست خود را با استفاده از یک کارت شبکه استاندارد (Network Adapter) به iSCSI Storage متصل نمایید. Software iSCSI Initiator پردازش های لازم برای iSCSI را در حین ارتباط با Network Adapter انجام می دهد.

Hardware iSCSI Initiator یک کارت سخت افزاری می باشد که امکان دسترسی به iSCSI Storage را برای شما بر روی TCP/IP فراهم می آورد. Hardware iSCSI Initiator ها به دو دسته تقسیم می شوند: Hardware iSCSI initiator وابسته , Hardware iSCSI initiator مستقل

یک Hardware iSCSI Initiator وابسته، بدلیل اینکه یک کارت NIC می باشد به VMWare Networking و پیکربندی های آن و همچنین مدیریت iSCSI interface که توسط vmware فراهم شده است وابسته است. این نوع Adapter یک کارت شبکه (Standard Network Adapter) می باشد که دارای قابلیت iSCSI Offload Engine نیز می باشد.

ایجاد این نوع عملکرد در adapter شما می بایست Networking را برای iSCSI Traffic تنظیم نمائید و همچنین این Adapter و یک VMKernel iSCSI Port مناسب متصل نمائید.

اما یک Hardware iSCSI initiator مستقل، مدیریت و پردازش شبکه iSCSI را برای هاست ESXi بصورت مستقل انجام می دهد چراکه این سخت افزار برخلاف مدل قبلی یک iSCSI HBA می باشد.

برای تصمیم گیری در مورد خرید یک Storage Adapter شما می توانید براساس پارامترهای متعددی از جمله: هزینه ، امکان Failover و CPU Overhead و همچنین بوت شدن از روی SAN اقدام نمائید.

برای مشاهده لیست کامل I/O Adapter , iSCSI Storage Array پشتیبانی شده توسط vmware می توانید به لینک زیر مراجعه نمائید:

<http://www.vvmare.com/resources/compatibility>

## Configuring Software iSCSI

### To configure the iSCSI software initiator:

1. Configure a VMkernel port for accessing IP storage.
2. Enable the iSCSI software adapter.
3. Configure the iSCSI IQN name and alias (if required)
4. Configure iSCSI software adapter properties, such as static/dynamic discovery addresses and iSCSI port binding
5. Configure iSCSI security (Challenge Handshake Authentication Protocol (CHAP)).

برای پیکربندی Software iSCSI شما می بایست موارد زیر را انجام دهید:

۱- برای ایجاد دسترسی ESXi به iSCSI storage شما می بایست یک VMkernel Port ایجاد نمایید.

۲- سپس Software iSCSI Initiator را فعال نمایید تا هاست شما بتواند از آن استفاده کند. پس از فعال کردن Software iSCSI Initiator یک iSCSI Name پیش فرض براساس نام گذاری IQN برای شما انتخاب می شود.

۳- در این مرحله شما می بایست یک یا چند Storage Target Address را برای iSCSI Initiator پیکربندی نمایید. شما نمی توانید IP Address , iSCSI Name, Port Number یک Storage Target را تغییر دهید. برای تغییر دادن آن شما می بایست آن را حذف و مجدداً Storage Target را اضافه نمایید.

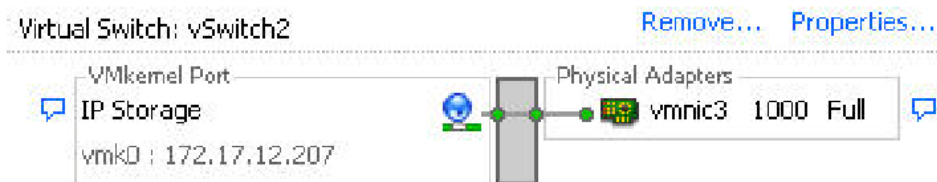
۴- در نهایت برای بالا بردن سطح امنیت ارتباطی می توانید Challenge Handshake Authentication Protocol یا CHAP را پیکربندی نمایید تا بدین وسیله صحت دسترسی یک Initiator به Target را از طریق شبکه بررسی نمایید.

هر یک از موارد فوق در ادامه تشریح خواهد شد.

## ESXi Network Configuration for IP Storage

**A VMkernel port must be created for ESXi to access software iSCSI.**

- The same port can be used to access NAS/NFS storage.



**To optimize your vSphere networking setup:**

- Separate iSCSI networks from NAS/NFS networks.
  - Physical separation is preferred.
  - If that is not possible, use VLANs.

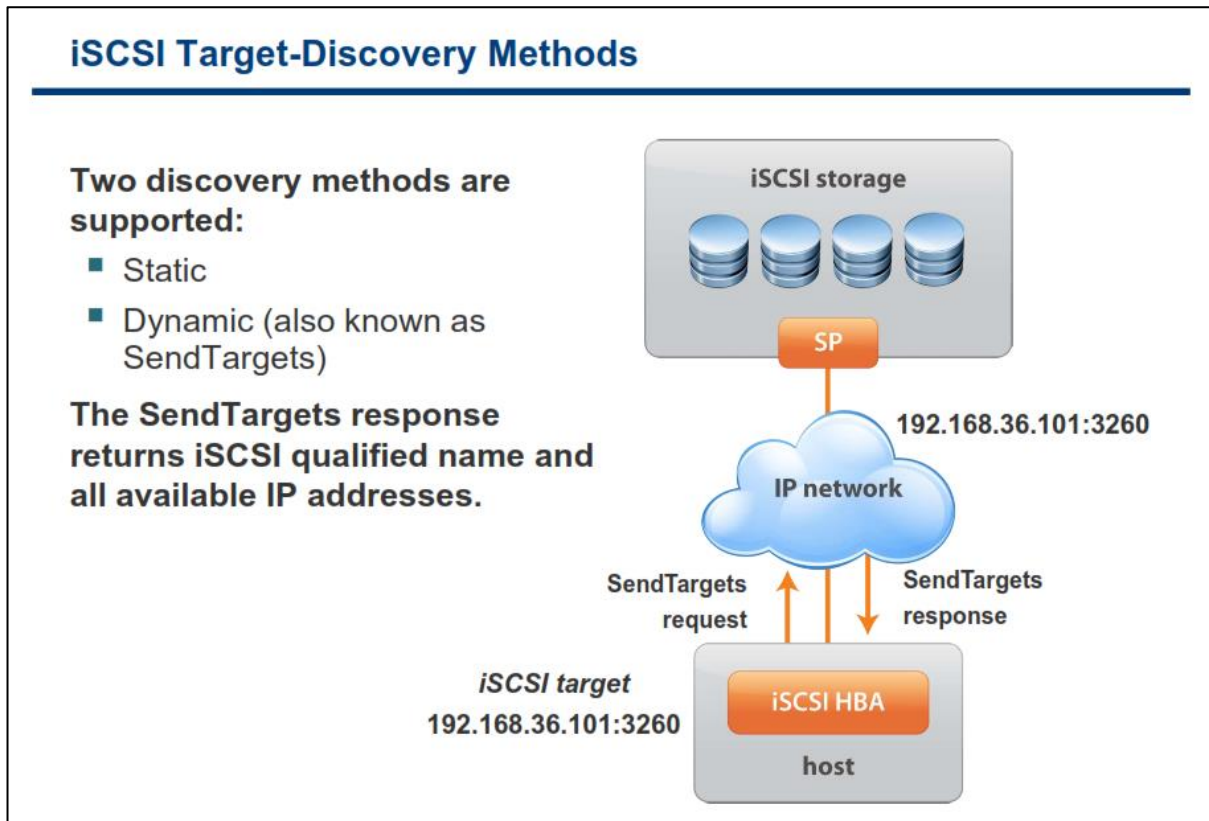
پیکربندی شبکه برای Software iSCSI شامل ایجاد VMKernel Port بروی Virtual Switch می باشد. بسته به تعداد Physical Adapter هایی که شما می خواهید به برای ترافیک iSCSI اختصاص دهید تنظیمات شبکه شما متفاوت خواهد بود:

- اگر شما یک Physical Adapter دارید، شما نیاز به یک VMKernel Port بروی Virtual Switch دارید.
- اگر شما دو یا بیشتر Physical Network Adapter برای iSCSI دارید ، شما می توانید از این Adapter ها برای Host-based Multipathing استفاده کنید. Multipathing در درس های بعدی تشریح خواهد شد.

برای اضافه کردن VMKernel Port به یک Virtual Switch از قسمت Configuration هاست خود به بخش Networking بروید و یک Port جدید اضافه نمایید.

برحسب تجربه توصیه می شود برای امنیت و کارایی بهتر، iSCSI Network را از شبکه های دیگر خود جدا کنید. اگر بصورت فیزیکی این کار صورت می گیرد بسیار خوب است و اگر اینگونه امکان پذیر نیست بصورت Logically و با استفاده از VLAN های جداگانه آن را جدا نمایید.

## روش های شناسایی و جستجوی iSCSI Target



ESXi از دو متد iSCSI Target Discovery پشتیبانی می کند:

۱- **Static Discovery**: در این حالت Initiator نیاز به انجام Discovery ندارد چراکه Initiator همه Storage Target ها را با استفاده از IP Address و یا DNS Name می شناسد و به آنها متصل می شود.

۲- **Dynamic Discovery**: این متد بنام SendTarget Discoverey نیز خوانده می شود. هر زمان که Initiator به یک iSCSI Server مشخص متصل می شود، درخواست SendTarget خود را برای سرور ارسال می کند. سرور با استفاده از یک لیست فراهم شده از Target های در دسترس به Initiator پاسخ می دهد. Name و IP Address این Storage Target ها به عنوان Static Target در vSphere Client ظاهر می شوند. اگر شما یک Static Target را بوسیله Dynamic Discovery حذف کنید، آن Storage Target ممکن است در زمان اسکن بعدی و یا HBA reset و یا reboot هاست دوباره به لیست اضافه گردد.

### iSCSI Security: CHAP

**iSCSI initiators use CHAP for authentication purposes.**

- By default, CHAP is not configured.

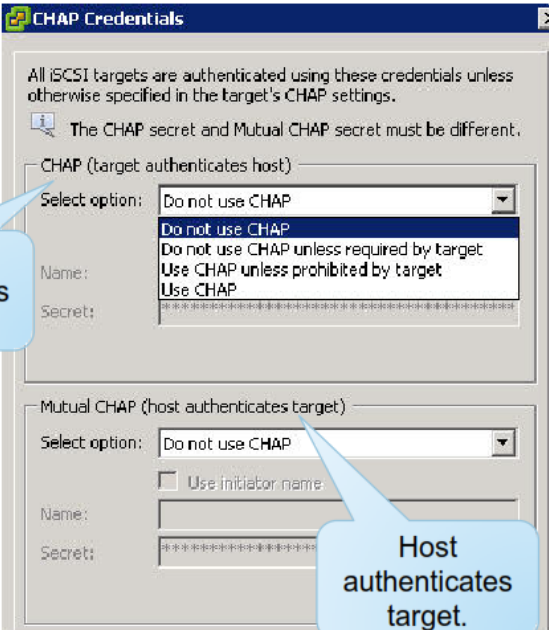
**ESXi supports two types of CHAP authentication:**

- Unidirectional
- Bidirectional
  - Software iSCSI only

**ESXi also supports per-target CHAP authentication.**

- Software iSCSI only
- Different credentials for each target

*Software iSCSI properties > General tab*



بدلیل اینکه در تکنولوژی iSCSI هاست به Remote Target متصل می شود و داده ها در هنگام انتقال Encrypt و یا رمزنگاری نمی شوند، به شما توصیه می شود که از CHAP برای ایمن سازی Storage Network خود استفاده نمائید. ESXi از دو متد CHAP Authentication پشتیبانی می کند:

- **Unidirectional:** این متد One-way CHAP نیز نامیده می شود که در این حالت Storage Target شما Initiator را Authenticate می کند اما Initiator شما Storage Target را Authenticate نمی کند. شما می بایست CHAP Secret یا همان CHAP Password را برای Initiator هایی که می خواهند به Storage Target ارتباط برقرار کنند، مشخص نمائید.
- **Bidirectional:** این متد Mutual CHAP نیز نامیده می شود و فقط برای Software iSCSI قابل اجرا می باشد. در این متد هم Initiator ها Storage Target را Authenticate می نمایند و هم بالعکس. شما می بایست Target Secret و Initiator Secret متفاوتی را تعیین نمائید.

CHAP از الگوریتم Three-way Handshake برای چک کردن هویت هاست و بالعکس استفاده می کند. چک کردن آن نیز براساس یک مقدار خصوصی از قبل تعیین شده و یا همان CHAP Secret می باشد که بین Initiator و Storage Target به اشتراک گذاشته شده است.

از ESXi CHAP Authentication در سطح Adapter پشتیبانی می کند. در این حالت همه Storage Target ها یک CHAP Secret را از iSCSI Initiator دریافت می کنند

نکته: بصورت پیش فرض CHAP پیکربندی نشده است.

برای پیکربندی CHAP بروی هاست ESXi در سطح Adapter در پنجره iSCSI Initiator Properties بروی سربرگ General کلیک و سپس بروی CHAP برای نمایش پنجره CHAP Credential کلیک کنید.

زمانیکه CHAP را انتخاب می کنید شما با گزینه های زیر روبرو می شوید:

- **Do not use CHAP**: با استفاده از این گزینه هاست از CHAP برای احراز هویت استفاده نمی کند. اگر این گزینه را انتخاب کنید احراز هویت غیر فعال می شود.
- **Do not use CHAP unless required by target**: با این گزینه هاست ترجیح می دهد که ارتباط بصورت non-CHAP باشد ولی اگر Storage Target به احراز هویت نیاز داشت به اتصالات CHAP اجازه اتصال می دهد (البته این امکان تنها برای iSCSI software initiator فعال می باشد)
- **Use CHAP unless prohibited by target**: با این گزینه هاست ترجیح می دهد که ارتباط بصورت CHAP باشد ولی اگر Storage Target احراز هویت را منع کند اتصالات بصورت Non-CHAP مورد استفاده قرار می گیرند.
- **use CHAP**: با این گزینه هاست به احراز هویت موفقیت آمیز CHAP نیاز دارد (البته این امکان تنها برای iSCSI Software initiator می باشد). همچنین شما باید Mutual CHAP را نیز پیکربندی نمایید.

قبل از پیکربندی CHAP می بایست هم فعال بودن CHAP را در iSCSI Storage و هم متد CHAP Authentication که سیستم پشتیبانی می کند را بررسی نمایید. اگر مشکلی در این زمینه وجود نداشت، شما می بایست آن را برای Initiator ها فعال نمایید. همچنین می بایست اطمینان حاصل کنید که CHAP Authentication Credentials هاست با Credential هایی که بروی iSCSI Storage پیکربندی شده اند، تطابق داشته باشند. همچنین vmware توصیه می کند که از CHAP با مشورت سازنده و فروشنده ایی که iSCSI SAN را از آن تهیه نموده اید اقدام به پیکربندی CHAP نمایید تا بهترین نتیجه حاصل گردد.



## پیکربندی iSCSI سخت افزاری

**Configuring Hardware iSCSI****To configure the iSCSI hardware initiator:**

1. Install the iSCSI hardware adapter.
  - For independent hardware iSCSI adapters
    - Verify properly formatted IP address and IQN names.
  - For dependent hardware iSCSI adapters
    - Determine the name of the physical NIC associated with adapter so that port binding is properly configured.
2. Modify the iSCSI name and configure the iSCSI alias.
3. Configure iSCSI target addresses.
4. Configure iSCSI security (CHAP).

## پیکربندی iSCSI Hardware Initiator:

۱- قبل از شروع پیکربندی iSCSI Hardware Initiator اطمینان حاصل کنید iSCSI HBA به درستی نصب شده و در لیست Storage Adapter های موجود برای پیکربندی نمایش داده می شود. برای اینکار در هاست خود بروی تب Configuration کلیک کرده و Storage Adapter را انتخاب نمایید. اگر Initiator بدرستی نصب شده باشد شما می توانید Properties آن را مشاهده نمایید.

۲- در صورتیکه ضرورت داشته باشد شما می توانید Alias Name و iSCSI Name را تغییر دهید. همچنین می بایست از فرمت درست iSCSI Name آن اطمینان حاصل نمایید. برخی از Storage ها ممکن است Hardware Initiator ها را شناسایی نکنند. اگر شما iSCSI Name را تغییر داده اید حتما می بایست Session خود را قطع نموده (Logout کرده و مجددا Login نمایید) و مجددا با iSCSI ارتباط برقرار نمایید تا در Session جدید Name بروزرسانی گردد.

۳- می بایست یک یا چند Target Discovery Address را برای در دسترس قراردادن Storage در شبکه پیکربندی نمایید.

۴- CHAP را پیکربندی نمایید تا بدین وسیله صحت دسترسی یک Initiator را به Target از طریق شبکه بررسی نمایید.. تنها قابلیت One-way CHAP برای Hardware Initiator ها فعال می باشد.



## چند مسیری سازی با iSCSI Storage

### Multipathing with iSCSI Storage

**Hardware iSCSI:**

- Use two or more hardware iSCSI adapters.

**Software or dependent hardware iSCSI:**

- Use multiple NICs.
- Connect each NIC to a separate VMkernel port.
- Associate VMkernel ports with iSCSI initiator.

The diagram illustrates a multipathing setup. At the top, 'iSCSI storage' is represented by four disks, each with an 'SP' (Storage Processor) label. These connect to an 'IP network' cloud. Below the network, there are two 'iSCSI independent hardware adapter' boxes and one 'iSCSI initiator (software or dependent hardware)' box. Two 'NIC' (Network Interface Card) boxes are connected to the network and the initiator. An arrow points from the NICs to the initiator, labeled 'VMkernel ports'.

**Configure port binding in the Properties window of the iSCSI adapter.**

Port Group	VMkernel Adapter	Port Group Policy	Path Status

زمانیکه شما ESXi را برای Multipathing و Failover تنظیم می کنید شما می توانید از چندین Hardware iSCSI Adapter و یا چندین Virtual NIC بسته به نوع iSCSI Initiator استفاده نمایید.

در این حالت هاست می تواند از ۲ یا بیشتر Hardware iSCSI Adapter استفاده نمایند و از طرفی دیگر نیز Storage ها می توانند با استفاده از یک یا چند سوئیچ مورد دسترسی قرار گیرند. پیکربندی می تواند بدین گونه باشد که هاست شامل یک Adapter و دو Storage Processor باشد که Adapter می تواند از چندین مسیر برای رسیدن به Storage استفاده نماید.

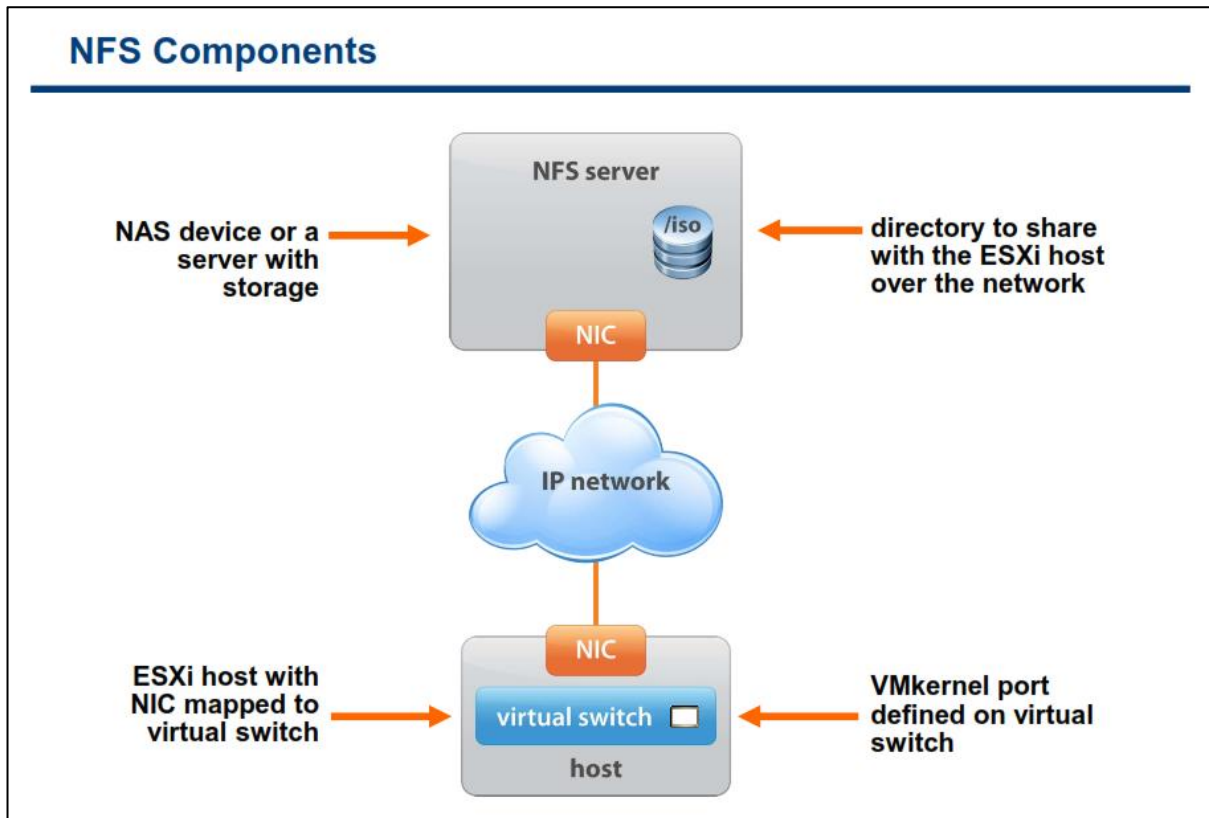
با Software iSCSI و یا Hardware iSCSI مستقل شما می توانید از چندین Virtual NIC برای برآوردن امکان Failover برای اتصال iSCSI بین هاست و iSCSI Storage استفاده نمایید. بدلیل اینکه پلاگین Multipathing در vSphere بصورت مستقیم به NIC فیزیکی بروی هاست دسترسی ندارد شما ابتدا باید هر NIC فیزیکی را به یک VMkernel مجزا متصل نمایید. همچنین می توانید از تکنیک Port-Binding برای ارتباط همه VMkernel Port ها به iSCSI Initiator استفاده نمایید. در نتیجه هر VMkernel Port می تواند به یک NIC فیزیکی مجزا متصل و یک مسیر متفاوت برای Storage فراهم نماید. بعد از پیاده سازی iSCSI Multipathing، هر پورت بروی ESXi، آدرس IP خودش را دارد اما همه آنها یک iSCSI Initiator IQN Name را به اشتراک می گذارند و از آن استفاده می کنند.

نکته: توصیه می شود که حداقل مقدر ترافیک iSCSI در میان روتر های شبکه مسیرهدهی نشوند.

## بخش سوم: پیکربندی NAS/NFS Storage

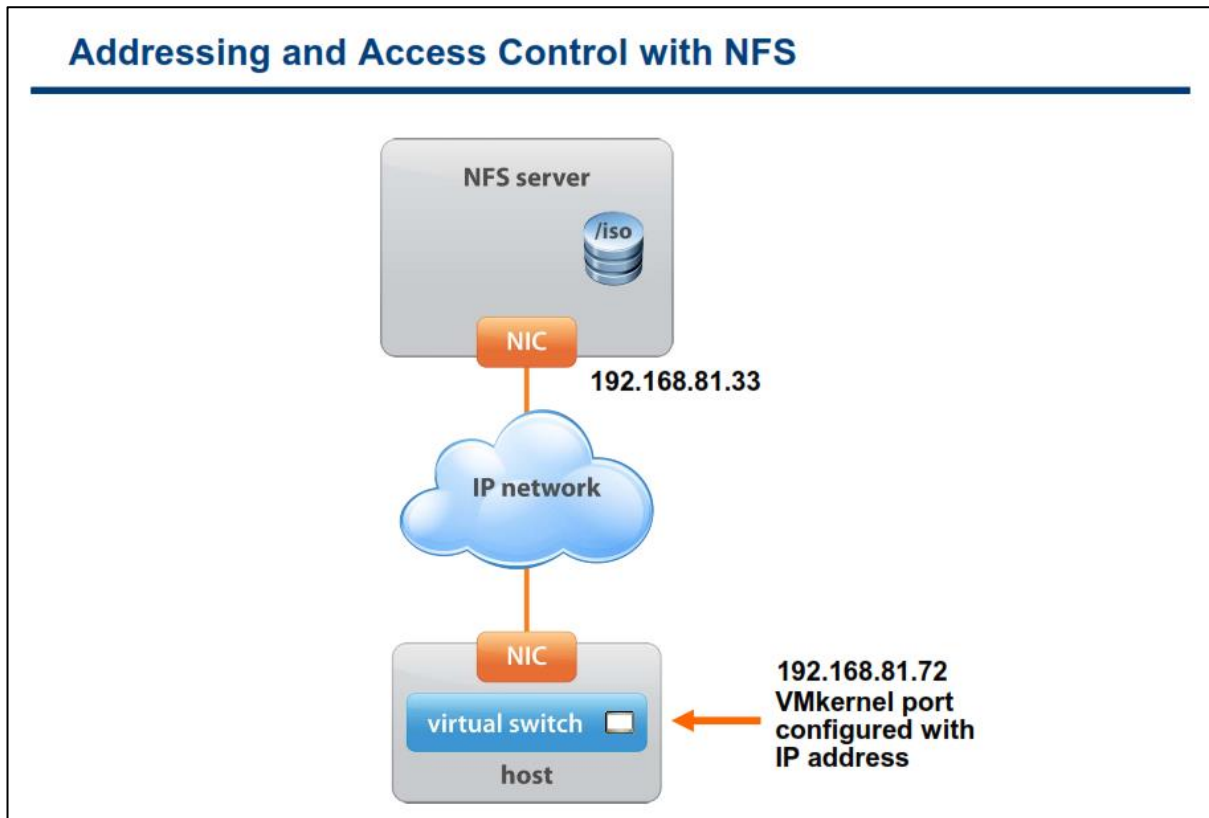
بعد از به اتمام رساندن این بخش شما قادر خواهید بود:

- کامپوننت های NFS و آدرس دهی آن را تشریح نمائید
- یک NFS Datastore جدید ایجاد نمائید



یک NFS File System بروی NAS Storage قرار می گیرد. این سیستم به عنوان NFS Server شناخته می شود. NFS Server شامل یک یا چندین دایرکتوری (Folder) می باشد که بروی شبکه TCP/IP برای هاست ESXi به اشتراک گذاشته است. یک هاست ESXi از طریق VMkernel Port ای که بروی یک Virtual Switch تعریف شده است به NFS Server دسترسی خواهد داشت.

## پیکربندی NFS برای کنترل دسترسی



اجازه بدهید قبل از اینکه درباره تنظیمات دسترسی مربوط به ESXi و NFS صحبت کنیم، کمی به پیکربندی NFS Server بپردازیم تا مسائل بعدی کمی واضح تر شوند:

بطور کلی برای پیکربندی NFS server شما نیاز دارید که سه فایل اصلی مربوط به NFS Server را بروی آن پیکربندی نمائید. این سه فایل شامل:

etc/exports

etc/hosts.allow

etc/hosts.deny

می باشد. اگر بخواهیم دقیق تر نگاه کنیم شما می توانید تنها با تنظیم فایل etc/exports در NFS Server آن را راه اندازی نمائید ولی تنظیم این فایل به تنهایی، امنیت NFS Server را تضمین نخواهد کرد و امنیت آن را به مخاطره می اندازد.

فایل exports حاوی لیست مدخل هایی هست که هر مدخل نشان دهنده volume هایی است که بروی NFS Server به اشتراک (Share) گذاشته شده است و همچنین نحوه به اشتراک گذاشته شدن آنها را نیز توصیف می کند. ساختار این مدخل ها به شکل زیر می باشد:

directory machine1 (option11,option12)

machine2 (option21,optio22)

**directory**: آدرس دایرکتوری هست که شما می خواهید آن را به اشتراک (Share) بگذارید. اگر شما دایرکتوری را **Share** نمائید تمام زیر دایرکتوری های آن نیز به تبع آن **Share** خواهند شد.

**machine**: آدرس IP و یا DNS کلاینت ای است که به این دایرکتوری **Share** شده، دسترسی دارد.

**optionXX**: در اینجا نیز گزینه های مربوط به نحوه دسترسی هر **machine** قرار داده می شود. این گزینه ها شامل موارد زیر می باشند:

۱- **ro**: کلاینت ها تنها اجازه خواندن از این دایرکتوری ها را دارند (**Read-only**)

۲- **rw**: کلاینت ها اجازه خواندن و نوشتن بروی دایرکتوری های **Share** شده را دارند (**Read/write**)

۳- **no\_root\_squash**: بصورت پیشفرض هر درخواست فایلی که توسط کاربر **root** یک ماشین کلاینت ایجاد می شود، بروی **NFS Server** به عنوان درخواستی از طرف **nobody** در نظر گرفته می شود. اما اگر گزینه **no\_root\_squash** انتخاب شده باشد کاربر **root** ماشین کلاینت، همان دسترسی را خواهد داشت که کاربر **root** مربوط به **NFS server** دارد. هر چند ممکن است این گزینه در بعضی مواقع لازم و ضروری باشد ولی انتخاب این گزینه می تواند پیامدهای جدی امنیتی زیادی را برای شما داشته باشد. در صورتیکه نیاز به این گزینه دارید شما باید محدودیت لازم را نیز در سطح های دیگر اعمال نمائید.

مثال:

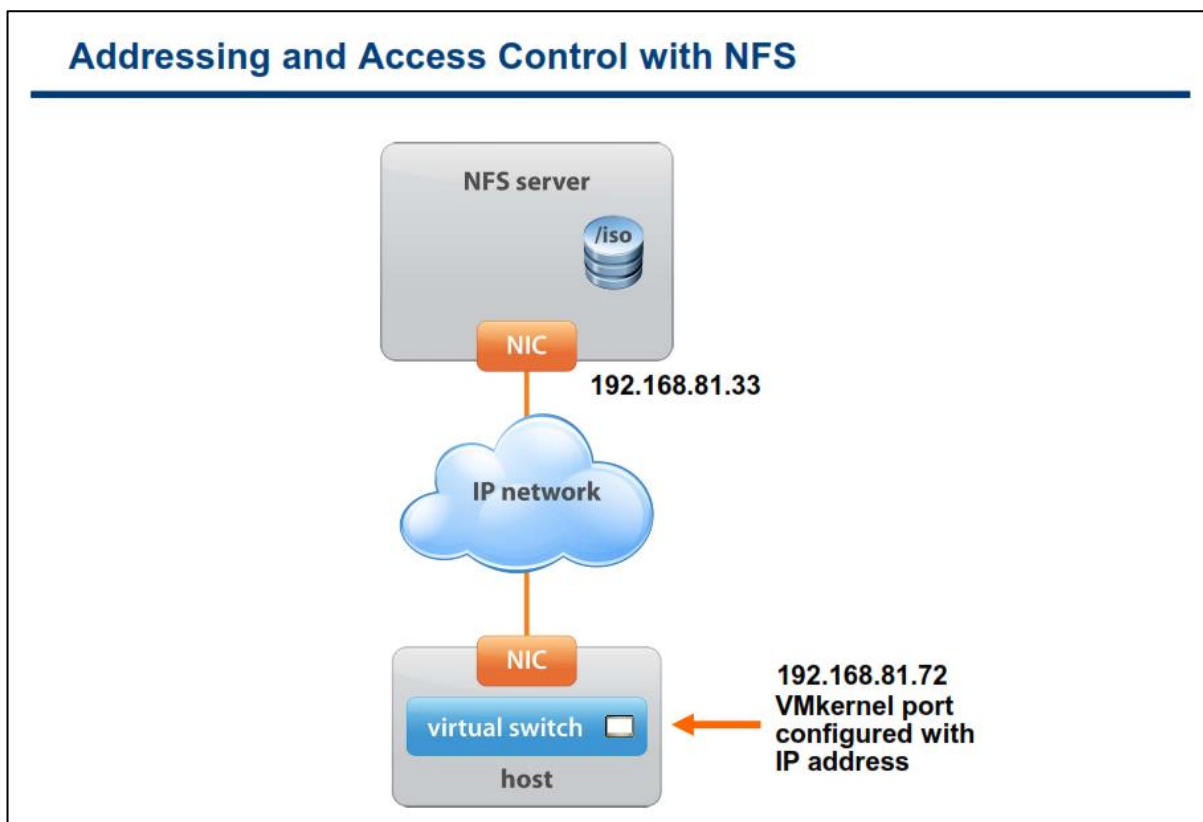
/usr/local 192.168.0.1(ro) 192.168.0.2(ro)

/home 192.168.0.1(rw,no\_root\_squash) 192.168.0.2(rw)

برای کسب اطلاعات بیشتر می توانید به لینک زیر مراجعه کنید:

<http://nfs.sourceforge.net/nfs-howto/ar۰۱s۰۳.html>

## آدرس دهی و کنترل دسترسی NFS



هاست ESXi بوسیله IP address و یا نام هاستی که بروی NFS server پیکربندی شده به سرور NFS متصل شده و دسترسی پیدا می کند. همچنین VMkernel Port نیز بوسیله یک IP address از رنج NFS Server پیکربندی می شود تا از طریق آن به NFS Server دسترسی داشته باشد.

بروی هاست ESXi اجازه دسترسی به NFS به کاربر root داده شده است. اما با داشتن اجازه کاربری root امکان دسترسی به همه NFS Volume ها نیست. معمولاً برای حفاظت از NFS volume ها از دسترسی غیر مجاز، مدیر NFS یا همان NFS Administrator امکانی بنام root\_squash را برای volume ها فعال می کند. زمانیکه root\_squash فعال هست NFS Server دسترسی بوسیله کاربر root را به عنوان یک کاربر غیر مجاز تلقی می کند و ممکن است درخواست های ESXi را برای دسترسی به فایل های VM موجود بروی NFS Server رد نماید.

NFS Administrator باید از امکان no\_root\_squash به جای root\_squash برای NFS volume ها استفاده نماید. گزینه no\_root\_squash به کاربر root هاست ESXi اجازه می دهد که به عنوان کاربر root بروی NFS Server شناخته شود. اگر شما VM ها را بروی NFS datastore قرار داده اید، NFS Administrator باید حق دسترسی read\write را به NFS datastore با گزینه no\_root\_squash بدهد.

نکته: فقط با این پیکربندی هاست ESXi می تواند vm ها بروی NFS Server مدیریت و Deploy نماید.

## پیکربندی یک NFS Datastore

**Configuring an NFS Datastore****Create a VMkernel port:**

- For better performance and security, separate it from the iSCSI network.

**Provide the following information:**

- NFS server name (or IP address)
- Folder on the NFS server, for example, /LUN1 and /LUN2
- Whether to mount the NFS file system read-only:
  - Default is to mount read/write
- NFS datastore name

برای دسترسی هاست ESXi به NFS datastore از طریق شبکه، باید یک VMkernel Port بروی Virtual Switch پیکربندی شود. بر حسب تجربه و برای افزایش امنیت و کارایی، توصیه می شود که شبکه NFS خود را از سایر شبکه ها جدا نمایید.

برای ایجاد NFS datastore مراحل زیر را باید طی نمایید:

۱- بروی لینک Storage موجود در تب Configuration هاست کلیک نمایید.

۲- در این مرحله بروی لینک Add Storage کلیک نموده و سپس Network File System را به عنوان نوع Storage خود انتخاب نمایید.

۳- سپس مشخصات مربوط به NFS datastore خود را در این بخش وارد نمایید. این مشخصات شامل:

- نام Host و یا IP Address مربوط به NFS Server
- مسیر پوشه بروی NFS Server که شما می خواهید این datastore به آن متصل (Map) شود.
- اگر می خواهید NFS را فقط به صورت Read-only استفاده و یا Mount نمایید، گزینه مربوط به آن را باید انتخاب کنید. (برای کاربردهایی همچون نگهداری فایل ISO Image)
- نام datastore

نکته: در صورتیکه می خواهید RDM (Raw Device Mapping) را به یک VM که بروی NFS datastore قرار دارد اضافه نمایید، شما حتما می بایست از یک VMFS datastore برای ذخیره کردن RDM Pointer استفاده نمایید. چراکه پروتکل NFS از دستورات SCSI بروی VMkernel پشتیبانی نمی کند.



## Viewing IP Storage Information

## Hosts and Clusters view &gt; Configuration tab &gt; Storage link

View: **Datstores** Devices

Refresh Delete Add Storage... Rescan All...

Identification	Status	Device	Drive Type	Capacity	Free	Type	Alarm Actio...	Hardware Acceleration
ISO Files (read on...	✓ Normal	172.20.10.12:/ISO5	Unknown	9.08 GB	3.89 GB	NFS	Enabled	Not supported
NFS-LUN2	✓ Normal	nfs.vclass.local:/lun2	Unknown	3.93 GB	3.86 GB	NFS	Enabled	Not supported
Local-ESXi02	✓ Normal	Local ATA Disk (t10.A...	Non-SSD	7.00 GB	5.13 GB	VMF55	Enabled	Unknown
VMFS-00	✓ Normal	LEFTHAND iSCSI Disk ...	Non-SSD	19.50 GB	13.22 G	VMF55	Enabled	Unknown
VMFS-02	✓ Normal	LEFTHAND iSCSI Disk ...	Non-SSD	19.50 GB	17.12 G	VMF55	Enabled	Unknown

## Datstores view &gt; Storage Views tab

vc-geese01.vmeduc.com

Training

- Local02
- nfs\_library
- SAN
- SharedVMs

nfs\_library

Getting Started Summary Virtual Machines Hosts Performance Configuration Tasks & Events Alarms Permissions Storage Views

View: Reports Maps

Show all NAS Mounts - Remote Host, Remote Path or

Remote Host	Remote Path	User name	Type	Datstore
osdc-nas-b	/vdcrepos/Classes/vSICM40A		NFS	nfs_library

پس از ساختن VMFS و یا NFS datstore شما می توانید datstore های خود را توسط لینک Storage در سربرگ Configuration مشاهده نمایید. این بخش همه datstore هایی را که به هاست متصل هستند را نمایش می دهد. همچنین از بخش Datstore Panel شما می توانید محتویات datstore ها را بوسیله راست کلیک کردن بروی هر datstore و انتخاب گزینه Browse Datstore مشاهده نمایید.

شما همچنین می توانید datstore های خودتان را از بخش Datstore View ببینید. برای مشاهده NFS datstore بروی سربرگ Storage View هاست خود کلیک نمایید و گزینه Show all NAS Mounts را انتخاب نمایید. این گزینه اطلاعاتی را درباره همه NFS datstore ها برای شما فراهم می کند که شامل NFS Server Name و Shared Folder Name , Datstore Type, Datstore Name می باشد.

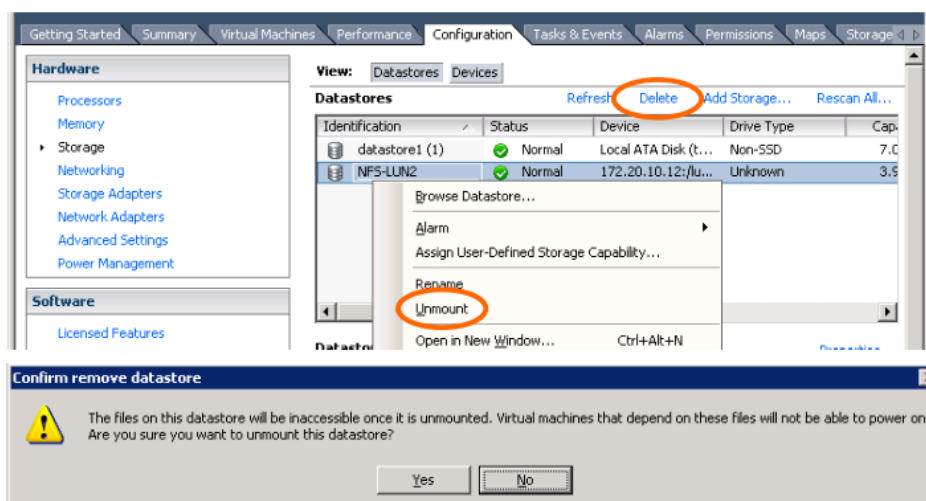
در نهایت شما می توانید از لینک Storage Adapter موجود در سربرگ Configuration، لیست تمامی Adapter ها را به همراه نوع آنها مانند Fibre Channel و iSCSI Adapter مشاهده نمایید.

## Unmount کردن و حذف کردن یک NFS Datastore

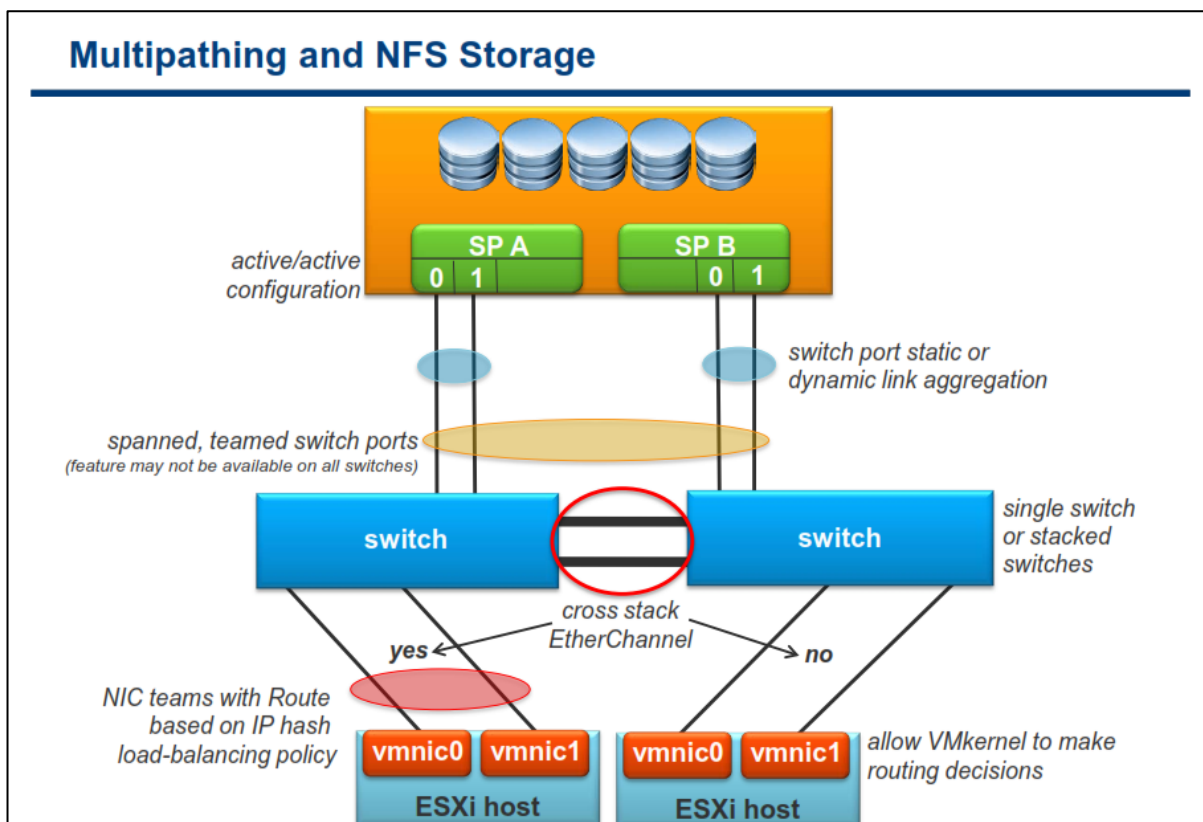
## Unmounting/Deleting an NFS Datastore

Click the Storage link in the Configuration tab to unmount an NFS datastore.

Unmounting an NFS datastore deletes that datastore.



Unmount کردن یک NFS datastore با Delete کردن NFS datastore فرقی ندارد. شما ابتدا باید همه vm هایی که بروی این datastore هستند را Stop نمائید. سپس برای پاک کردن و Unmount کردن NFS datastore بروی لینک Storage در سربرگ Configuration کلیک نموده و سپس بروی NFS datastore راست کلیک کرده و گزینه Unmount و یا Delete را انتخاب نمائید.



برای ایجاد یک ساختار High Availability در NAS، شما باید از نقاط تک کاناله و Single که احتمال قطع شدن و خرابی در آن وجود دارد (مانند NIC Card، کابل شبکه و سوئیچ) جلوگیری نمایید و در آنها افزونگی ایجاد نمایید. بدین ترتیب شما باید ESXi Host را با NIC Card های بیشتر (حداقل دو NIC) و سوئیچ های فیزیکی بیشتر (حداقل دو سوئیچ فیزیکی) پیکربندی نمایید.

زمانیکه از چندین NIC Adapter برای High Availability استفاده می نمایید، بهترین گزینه استفاده از NIC Teaming می باشد. بالانس کردن ترافیک (Load Balancing) به قابلیت های سوئیچ های فیزیکی خارجی (External) بستگی دارد چراکه سوئیچ خارجی می بایست از استاندارد 802.1d و یا EtherChannel Cisco Switch پشتیبانی نماید. NIC Teaming باید روی سوئیچ های خارجی بصورت جداگانه پیکربندی گردد.

در سطوح بالاتر برای کارایی و High Availability بیشتر می توان از قابلیت Cross Stack سوئیچ ها استفاده کرد (البته در صورتیکه سوئیچ ها از این قابلیت پشتیبانی نمایند). با سوئیچ های خاص شبکه، شما می توانید از طریق دو سوئیچ فیزیکی جداگانه که در حقیقت به صورت یک سوئیچ منطقی و Logical مدیریت می شوند، Team Port را به اجرا در آورید. استفاده از این قابلیت باعث ایجاد بهبودهایی در کارایی، در دسترس بودن بالا با تعداد NIC کمتر و داشتن مسیرهای بیشتر می شود، که در نهایت باعث توزیع ترافیک می گردد.

نکته قابل توجه اینجاست که فقط یک مسیر Active برای ارتباط میان ESXi Host و Single Storage Target وجود دارد. هرچند این امکان وجود دارد که شما ارتباط جایگزینی برای Failover فراهم کردن باشید اما پهنای باند میان یک

Storage و datastore به یک Single Connection محدود شده است. برای رفع این کمبود شما نیاز دارید که چندین اتصال (connection) از هاست ESXi به Target Storage داشته باشید. شما باید چندین datastore را پیکربندی کنید و در هر datastore از Connection جداگانه ای بین هاست ESXi و Storage استفاده نمائید.

پیکربندی توصیه شده برای چند مسیرسازی NFS با سوئیچ های متفاوت:

سوئیچ های خارجی که از Cross-Stack EtherChannel پشتیبانی می کنند	سوئیچ های خارجی که از Cross-Stack EtherChannel پشتیبانی نمی کنند
<ul style="list-style-type: none"> <li>• یک VMkernel Port تعریف نمائید</li> <li>• NIC Teaming را با استفاده از NIC های فیزیکی که به همان سوئیچ فیزیکی متصل شده اند پیکربندی نمائید.</li> <li>• NFS Server را با چندین IP Address پیکربندی نمائید (IP Address ها می توانند در یک Subnet باشند)</li> <li>• برای استفاده از چندین لینک ارتباطی NIC Teaming را با متد IP Hash Load-Balancing پیکربندی نمائید.</li> </ul>	<ul style="list-style-type: none"> <li>• دو یا بیشتر VMkernel Port را بروی سوئیچ های مجازی متفاوت و بروی Subnet های متفاوت پیکربندی نمائید.</li> <li>• NIC Teaming را با استفاده از NIC های فیزیکی متصل شده به همان سوئیچ فیزیکی پیکربندی نمائید.</li> <li>• NFS Server را با چندین IP Address پیکربندی نمائید (IP Address ها می توانند در یک Subnet باشند)</li> <li>• برای استفاده از چندین لینک ارتباطی، به جدول مسیریابی VMkernel اجازه دهید تا برای انتخاب لینک خودش تصمیم گیری نماید.</li> </ul>

## کارگاه شماره هشت:

در این کارگاه آموزشی، شما اتصال به NFS & iSCSI datastore را خواهید آموخت که شامل موارد زیر می باشد:

۱. افزودن یک VMkernel Port Group به یک سوئیچ مجازی استاندارد
۲. پیکربندی iSCSI Software Adapter
۳. پیکربندی اتصال به NFS datastore
۴. مشاهده اطلاعات مربوط به NFS & iSCSI datastore

## کارگاه شماره نه:

در این کارگاه آموزشی، شما پیکربندی شبکه را برای هاست ESXi براساس مجموعه ای از نیازمندیها خواهید آموخت که شامل موارد زیر می باشد:

۱. تحلیل نیازها
۲. طراحی سوئیچ مجازی و اتصالات فیزیکی

به یاری خداوند ادامه خواهد داشت ....