

مجازی سازی Virtualization

ویرایش اول
بهمن ۱۳۹۱



با دانشی کافی و دیدی روشن می توانید دست به کار پیاده سازی تکنولوژی مجازی سازی در سازمان خود شوید. در این مجموعه بسیاری از ویژگی های کاربردی مجازی سازی تشریح و خواننده به سادگی و بدون صرف وقت در سمینار های طولانی، از مفاهیم علمی و ساختارهای مجازی سازی آگاه می شود و در بخش اصطلاحات راجع به ابزار های معروف VMware و وظایف آنها می آموزد.



گردآوری و ترجمه: مریم ثقفی

ویرایش: عباس عظیمی

به سفارش: شرکت فنی و مهندسی ایمن افزار وایا

تاریخ انتشار: بهمن ۱۳۹۱

کلیه حقوق مادی و معنوی این مجموعه برای شرکت فنی و مهندسی ایمن افزار وایا محفوظ و هر گونه کپی برداری، چاپ و تکثیر مستلزم اجازه کتبی است.



تقدیم به پرسنل پر تلاش،

مشتریان و مخاطبین عزیز شرکت ایمن افزار وایا

و همه کارشناسان ایرانی که با رویاهایشان واقعیت را می سازند.

فهرست مطالب

مقدمه	۰۱
مجازی سازی چیست؟	۰۲
مزایای مجازی سازی	۰۳
مجازی سازی مناسب چه سازمان هایی است؟	۰۵
مجازی سازی چگونه کار می کند؟	۰۵
معرفی محصولات مجازی سازی کمپانی VMware	۰۷
- VMware Workstation	
- VMware Fusion	
- VMware Player	
- VMware vSphere	
Desktop Virtualization چیست؟	۱۰
مقایسه Hyper-V، VMware و Citrix	۱۲
آشنایی با برخی از اصطلاحات رایج مجازی سازی و کاربرد آنها	۱۸
- ESX و ESXi	
- Hypervisor	
- vSphere Client	
- vCenter Server	
- vSphere Update Manager	
- vMotion چیست؟	
- Storage vMotion چیست؟	
- Distributed Resource Scheduler (DRS)	
- Distributed Power Manager (DPM)	
- قابلیت دسترسی مستمر (High Availability)	
- سیستم تحمل خطا (Fault Tolerance)	
نمونه هایی از موارد موفق در مجازی سازی (Success Stories)	۳۱
سوالات متداول (FAQ)	۳۴

منابع



vmware
vSphere 5

دوره آموزشی و
کارگاه کاملاً عملی
مجازی سازی
مطابق با سیلابس
vmware
به همراه
تجهیزات مورد نیاز
در شهر و سازمان شما



با ما در تماس باشید:
www.vaya.ir/newsletter
newsletter@vaya.ir
(021) 442 311 47



VAYA CO.
Information Security Solutions
www.vaya.ir

مقدمه

برایان تریسی در کتاب "قدرت برنامه ریزی" می گوید: ما در عصری فوق العاده زندگی می کنیم. هرگز در طول تاریخ، رسیدن شمار زیادی از مردم به اهدافشان تا این حد امکان پذیر نبوده است. وظیفه شما این است که در آنچه اقتصاددانان "عصر طلایی" نامیده اند، به بهترین نحو مشارکت داشته و برای داشتن یک زندگی متفاوت، در هر حوزه فردی متفاوت باشید. باید یاد بگیرید، رشد کنید و تجربیاتی را که تحمل و بینش رسیدن به یک زندگی برتر را به شما می دهند، بدست آورید.

در عصر طلایی، کامپیوتر یکی از برترین اختراعات بشری محسوب می شود و دانش این حوزه هر ۳ سال تقریباً ۲ برابر می گردد، پس متخصصان این فن آوری باید با شیوه ای هوشمندانه و با صرف کمترین زمان و هزینه خود را به روز نگه دارند و آمادگی پذیرش تغییرات بنیادی را در خود پرورش دهند. جالب است که این تغییرات کم و کوچک نیستند، سیستم عامل Dos با آمدن ویندوز بازنشسته شد، Usenet جای خود را به وب داد، فایل سرورهای قدرتمند Novell به سرورهای ویندوزی تعظیم کردند و نرم افزارهای مبتنی بر سیستم عامل جای خود را به Web Application ها می دهند و وقت آن است که بپذیریم مجازی سازی به راحتی وارد عمل شده و شیوه های سابق مدیریت منابع سخت افزاری، سرورها و دیتا سنترها را متحول کرده است و به خاطر داشته باشیم اگر ۱۰ سال پیش به توانایی نصب ویندوز و سرویس هایی کاربردی نظیر Active Directory افتخار می کردیم، اکنون آنها تبدیل به توانایی های اولیه برای کارشناسان شبکه شده اند.

در این نوشتار با ما همراه شوید و خود را برای روزی نه چندان دور آماده کنید که در آن توانایی طراحی، نصب، نگهداری و پشتیبانی از سیستم ها و دیتاسنترهای مجازی وظیفه اولیه و مهارت پایه شما محسوب می گردد.

ویرایش حاضر این نوشتار با حمایت مادی و معنوی شرکت ایمن افزار وایا بصورت رایگان منتشر و تقدیم شما می گردد و به یقین بهتر شدن ویرایش های بعدی و انتشار موضوعات دیگر مستلزم همراهی و دریافت نظرات شماست، بنابراین ما را با نظرات خود همراهی نمایید.

عباس عظیم

azimi@vaya.ir

مجازی سازی چیست؟

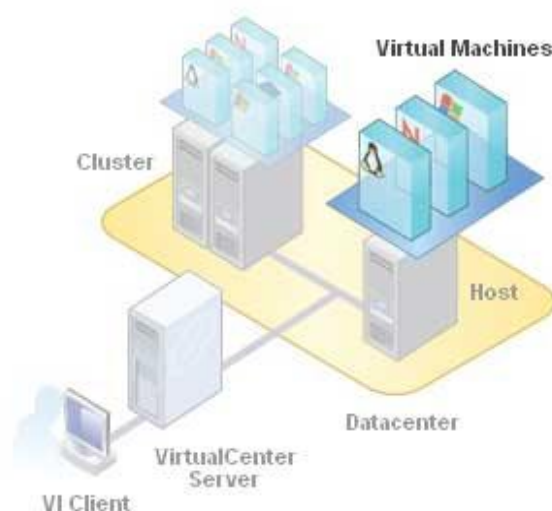
مجازی سازی اولین بار برای استفاده بهینه تر از سخت افزارهای Mainframe، در دهه ۱۹۶۰ توسعه یافت. ولی امروزه کامپیوترها با معماری های x86 نیز با مشکلات مشابه آبر کامپیوترها در آن دهه مواجه شده اند. کمپانی VMware، مجازی سازی برای معماری های x86 را در دهه ۱۹۹۰ اختراع کرد تا راهی نوین در جهت استفاده بهینه از منابع سخت افزاری ایجاد کند.

مجازی سازی برای اولین بار توسط شرکت IBM در حدود ۳۰ سال پیش اجرا شد، تا بتوان آبر کامپیوترها را با پارتیشن های منطقی به ماشین های مجازی از هم جدا، تقسیم کرد.

این پارتیشن ها Mainframe ها را قادر می ساخت تا بتوانند به صورت Multitask کار کنند، Application های متعدد را اجرا و پردازش کنند. از آنجا که منابع آبر کامپیوترها در آن زمان بسیار گران قیمت بودند، لذا آنها را بطور کامل برای این نوع پارتیشن بندی طراحی و پیاده سازی می کردند.

مجازی سازی به شکلی در طول سالهای ۱۹۸۰ تا ۱۹۹۰ رها شده بود، زیرا مشتریان ترجیح میدادند تا از نرم افزارهای Client-Server و از سرویس دهنده های x86 روی میزی (Desktop) استفاده کنند. کم کم با تکثیر نسخه های گسترده ای از لینوکس و ظهور ویندوز به عنوان سیستم عامل سرور ها در دهه ۱۹۹۰، سرورهای x86 به عنوان استاندارد معرفی شدند.

رشد سرورهای x86 و استقرار کامپیوترهای روی میزی منجر به چالشهای عملیاتی جدید در زیرساخت IT شد. در سال ۱۹۹۹ شرکت VMware، x86 را یک هدف کلی قرار داد و مجازی سازی برای x86 را معرفی کرد تا راهی باشد برای حل اکثر این چالشها. امروزه سخت افزار دستگاه های x86 برای کار با یک سیستم عامل طراحی شده اند، به نوعی به معنای واقعی هدر دادن منابع!





مجازی سازی یا به اصطلاح Virtualization تکنولوژی است که بوسیله آن می توان اجرای همزمان دو یا چند سیستم عامل بر روی یک سرور را داشته باشیم. این تکنولوژی نرم افزاری موجبات دگرگونی در چشم انداز فناوری اطلاعات و همچنین تغییرات اساسی در زیرساخت IT سازمان را فراهم می کند.

به بیان دیگر، مجازی سازی پیوند دهنده میان سخت افزار و سیستم عامل است و به شما اجازه اجرای چند نرم افزار کاربردی و سیستم عامل را بر روی یک سیستم فیزیکی می دهد، به نحوی که باعث بهره وری در هزینه های سخت افزار و نرم افزار و همچنین استفاده بهینه از تمامی منابع سیستمی، کاهش هزینه و کاهش مصرف انرژی می شود.

مزایای مجازی سازی

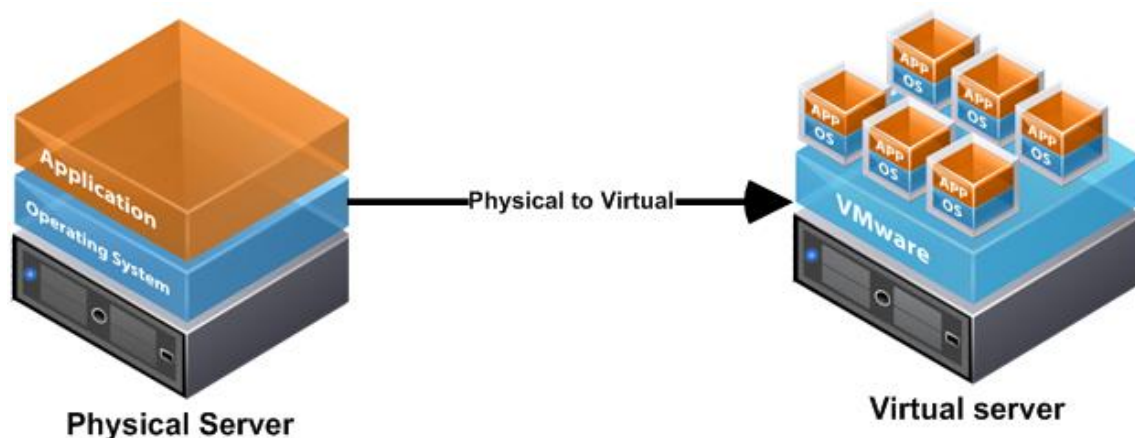
چه راهکاری را می توان به منظور حداقل سازی هزینه ها به کار برد؟ چه راهکاری را می توان به منظور سرمایه گذاری مفید در دوران رکود اقتصادی جهان به کار گرفت؟ چگونه می توان با سرمایه گذاری درست، ریسک بحران شدید اقتصادی را که کشورمان را نیز تهدید می کند، کاهش داد؟

مجازی سازی می تواند راهکاری بسیار مناسب باشد. تصور کنید به جای آنکه ۱۰ سرور فیزیکی داشته باشید که ۱۰ سیستم عامل مختلف بر روی آنها نصب است و هر کدام سرویس خاصی را به کاربران ارائه می دهند، می توانید تنها سه یا چهار سرور فیزیکی به همراه یک Storage مناسب داشته باشید و در عین حال ۱۰ سیستم عامل مجزا بر روی این چهار سرور فیزیکی (Host) به صورت همزمان و با پایداری بسیار بالاتر به کاربران سرویس دهی می نمایند.

جالبتر از آن، اگر بدانیم این راهکار در عین حال که کارایی شبکه را افزایش می دهد و زمان از کار افتادگی سرویس ها را چه به صورت سخت افزاری و چه نرم افزاری به میزانی قابل توجه کاهش می دهد و کاربران نهایی هرگز متوجه هیچ گونه اختلالی نمی شوند، آن وقت با اطمینان خاطر می توان برای پیاده سازی این راهکار اقدام نمود.

از اساسی ترین دغدغه های مدیران IT می توان به کاهش هزینه های نگهداری شبکه اشاره داشت. هزینه هایی که روز به روز در حال افزایش هستند مانند:

- هزینه خرید و تعویض سخت افزار مورد نیاز سرورها
- هزینه تجهیز اتاق سرور (هر چه تعداد سرور ها بیشتر، راه اندازی اتاق های سرور مبتنی بر استاندارد پر هزینه تر)
- هزینه برق مصرفی
- هزینه نیروی فنی مورد نیاز به منظور نگهداری سیستم ها
- هزینه سرمایه گذاری اتاق سرور
- هزینه ناشی از عدم کارکرد صحیح شبکه و از کار افتادن آن و ...
- هزینه خرید نرم افزارهایی با لایسنس معتبر مانند آنتی ویروس ها
- هزینه بکاپ گیری و پیاده سازی شیوه های مدیریت بحران



می توان این لیست را تا مدت ها ادامه داد و فهرست بلند بالایی از این هزینه های سنگین تهیه کرد. بدین جهت با استفاده از مجازی سازی و بهره مندی از کاربردهای بی شمار آن می توان به اصلی ترین مزایای زیر اشاره نمود:

- امکان ایجاد محیطهای Test & Development به صورت بسیار مقرون به صرفه
- سهولت و اطمینان خاطر بیشتر در پشتیبان گیری و بازیابی سرورها (Disaster Recovery & Backup)
- امنیت بسیار بالاتر سرورها

- کاهش شدید هزینه تجهیزات شبکه
- مدیریت بهتر و آسانتر سرورها و سرویس ها و کاهش هزینه های مدیریتی
- استفاده هر چه بهتر از فضای موجود در Data Center و کاهش هزینه های آن
- صرفه جویی در تهیه سخت افزار
- استقلال سیستم عاملها از سخت افزار و افزایش قابلیت حمل و جابجایی
- بهره وری هر چه بیشتر از سخت افزار و کاهش هزینه ها
- استفاده بهینه از فضای فیزیکی در مراکز داده و کاهش هزینه ها
- کاهش شدید در مصرف انرژی الکتریسیته مصرفی در مراکز داده و کاهش هزینه ها
- کاهش هزینه نگهداری و مدیریت سرور و سرویس ها

مجازی سازی مناسب چه سازمان هایی است؟

برخی از افراد به اشتباه گمان می کنند مجازی سازی تنها مختص مراکز داده یا دیتا سنتر های بزرگ می باشد. در صورتی که این تصویری کاملاً اشتباه است. شرکت های پیشرو در زمینه مجازی سازی این تکنولوژی را جهت استفاده برای رده ی وسیعی از شبکه ها طراحی کرده اند. از شبکه های کوچکی با یک سرور گرفته تا دیتا سنتر های بزرگ با دهها یا صدها سرور و سرویس دهنده مختلف. همان طور که پیشتر نیز اشاره شد مجازی سازی با مزایای خود طیف گسترده ای از نیازهای سازمان ها و افراد را در جهت استفاده بهینه تر از منابع، صرفه جویی و پایداری سرویس ها مرتفع می سازد.

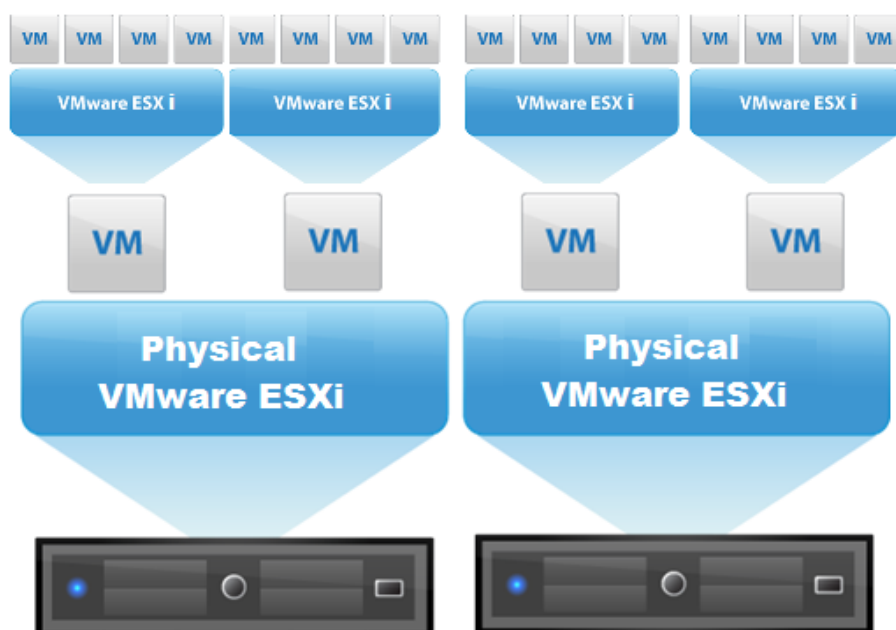
مجازی سازی چگونه کار می کند؟

در این فن آوری یک لایه نرم افزاری به نام Hypervisor* بین ماشین های مجازی و سخت افزار قرار می گیرد. قلب مجازی سازی همان ماشین های مجازی است که یک سیستم عامل به همراه سرویس ها و برنامه کاربردی داخل آن را شامل می شود.

ماشین های مجازی کاملاً از هم تفکیک شده اند و به یکدیگر وابستگی ندارند. وظیفه Hypervisor تخصیص دینامیکی منابع سخت افزاری به ماشین های مجازی در هنگام نیاز آنها و آزاد سازی آنها است. به

این شکل که در ابتدا نرم افزار مجازی ساز یا همان Hypervisor بر روی سخت افزار سرور نصب می گردد و سپس در درون آن به تعداد مورد نیاز ماشین مجازی تعریف می گردد.

پس از این مرحله هر ماشین مجازی مانند یک سخت افزار مستقل عمل می کند که می توان بر روی آن سیستم عامل دلخواه را نصب کرده و سپس سرویسها را راه اندازی نمود. در حالت پیشرفته تر می توان سخت افزار چندین سرور مختلف را به صورت منطقی با یکدیگر جهت مجازی سازی تجمیع نمود و کل منابع را به صورت تجمیعی در اختیار یک Hypervisor قرار داد.



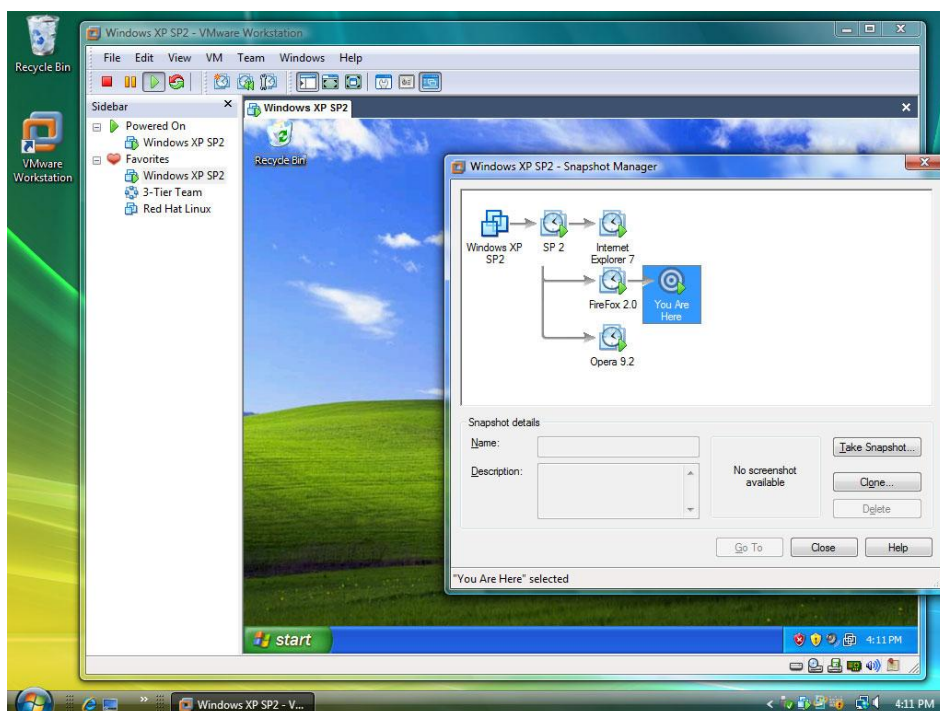
* برای مثال Hypervisor در ابزار کمپانی VMware با نام ESXi ارائه می شود.

معرفی محصولات مجازی سازی کمپانی VMware

۱- VMware Workstation:

این ابزار نرم افزار بسیار مشهوری از خانواده Virtual ها با قدمتی بیش از ۱۵ سال می باشد این نرم افزار مبتنی بر سیستم عامل با کسب جوایز متعدد بین المللی و هدف اجرای پلت فرم ها یا سیستم عامل های متعدد بر روی تنها یک سخت افزار طراحی شده است. این نرم افزار کاربران را قادر می سازد پیچیده ترین برنامه های تحت شبکه که در ویندوزهای مایکروسافت، Linux، Novell و غیره اجرا می شوند را تنها روی یک رایانه ی Desktop اجرا کنند.

VMware Workstation بر روی یک سیستم عامل نصب می شود و به عنوان یک نرم افزار جانبی به فعالیت می پردازد. با توجه به وسعت و انعطاف پذیری VMware Workstation، کاربران آن طیف نامحدودی از قبیل کاربران خانگی تا مدیران شبکه که هریک اهداف خاص خود را دنبال می کنند در بر می گیرد.

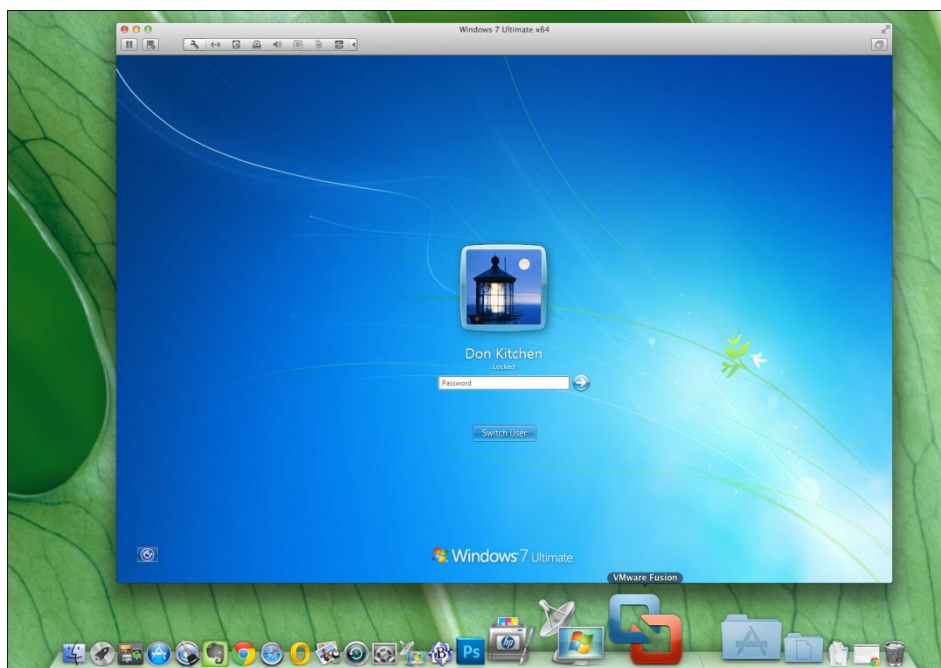


گوشه ای از موارد استفاده VMware workstation

- شبکه بندی مجازی (Virtual Networking) که تمام قابلیت های یک شبکه حقیقی را داراست.
- بررسی نرم افزار های مختلف
- بررسی ویروس ها و آنتی ویروس های مختلف به طوری که به سیستم اصلی هیچ آسیبی نرسد.
- بررسی سیستم عامل های مختلف
- و زمینه های آموزشی از قبیل
 - آموزش و یادگیری مفاهیم شبکه، شبیه سازی شبکه
 - آموزش و یادگیری سیستم عامل های گوناگون

۲- VMware Fusion:

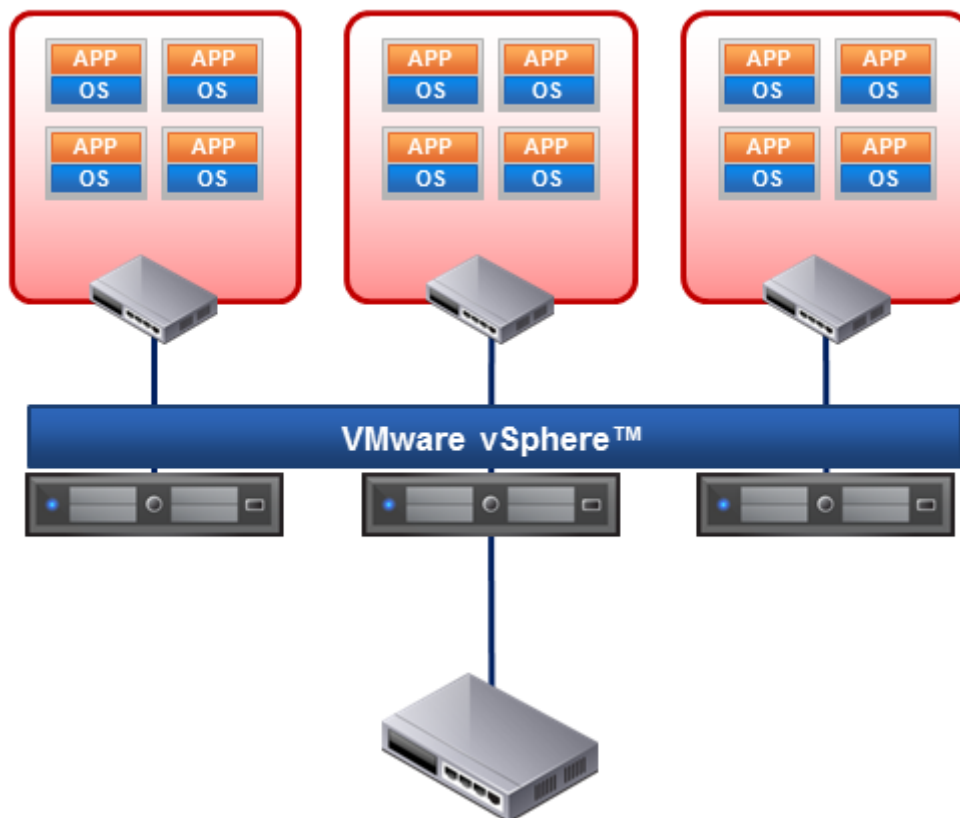
این نرم افزار مانند همان VMware Workstation برای سیستم عامل های "مکینتاش" می باشد.



۳- VMware Player:

سیستم کاری اش تقریباً مشابه Workstation است و همانطور که از نامش پیداست صرفاً برای اجرای فایل ماشین های مجازی ساخته شده است و کاملاً رایگان می باشد و بسیاری از قابلیت های VMware Workstation را ندارد.

۴- VMware vSphere: این محصول را می توان کاملترین مجموعه نرم افزاری شرکت VMware در سالهای اخیر نامید و در واقع مجموعه ای کامل از انواع ابزاری های مختلف VMware می باشد که در یکجا جمع شده و تقریباً کلیه امکاناتی که از یک سیستم مجازی سازی انتظار می رود را دارا است. این ابزار بهترین بستر مجازی سازی در سطح دیتاسنتر و سرور های سازمان را فراهم آورده و شامل تمامی قابلیت های مجازی سازی است که توسط ابزارهای vCenter، ESXi و vSphere Client پیاده سازی و مدیریت می شود. در بخش های بعدی به بررسی دقیق تر این ابزار می پردازیم.



جدا سازی

راه حل های جدا سازی
LAN و شبکه اطلاعاتی
سازمان از اینترنت

www.vaya.ir

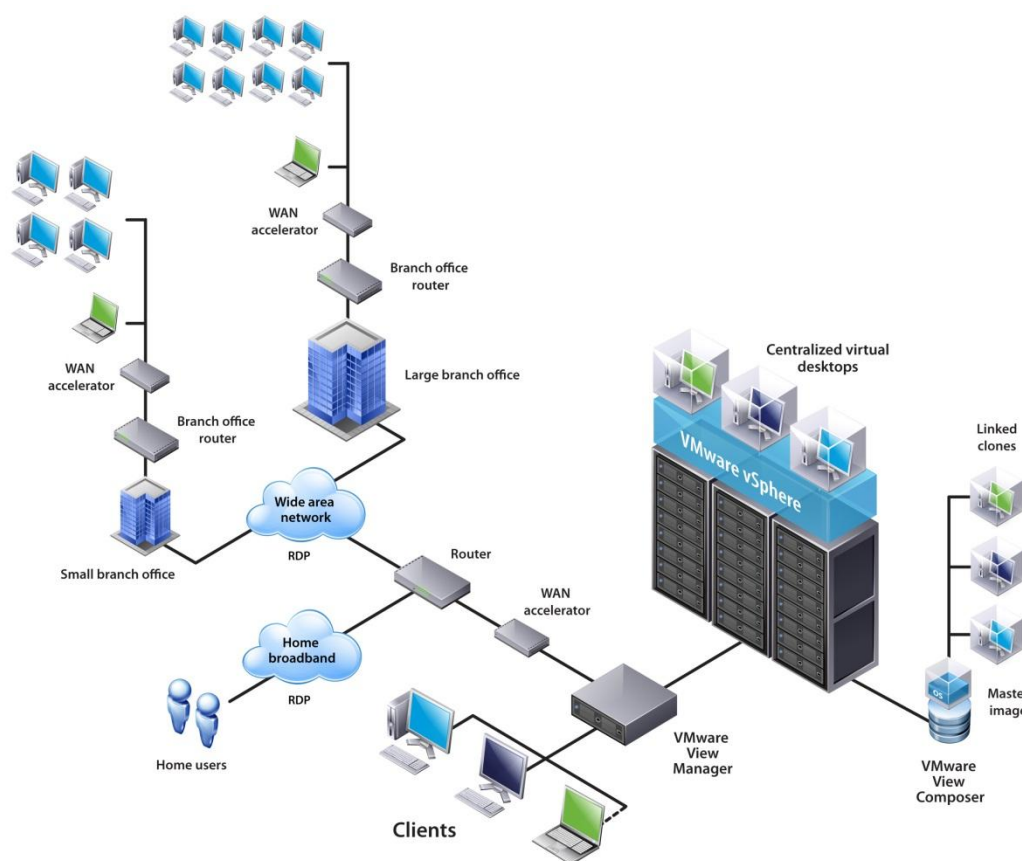
۰۲۱) ۴۴۲ ۳۱۱ ۴۷

۰۲۸۱) ۳۳۵ ۹۶ ۷۰



Desktop Virtualization چیست؟

منظور از مجازی سازی دسکتاپ (Desktop Virtualization)، اجرای سیستم عامل و نرم افزارها در ماشین های مجازی (Virtual Machine) است که بر روی دیتا سنتر در سرور نصب شده اند و برای استفاده کاربران در اختیار آنها قرار می گیرد. به نحوی که هر کاربر دسکتاپ کاملاً مستقل خود را دارد و به فعالیت بر روی دسکتاپی خارج از لپ تاپ، PC، یا Thin Client خود می پردازد. مجازی سازی دسکتاپ یعنی انتقال دسکتاپ کاربران نهایی از کامپیوتر شخصی به "فضای ابری". در این حالت سیستم عامل مورد استفاده از سخت افزار مستقل می شود و از این پس می توان بر روی هر کدام از کامپیوترهای شخصی و یا تین کلاینت ها، هر نوع سیستم عامل و هر نوع نرم افزاری داشته باشید.

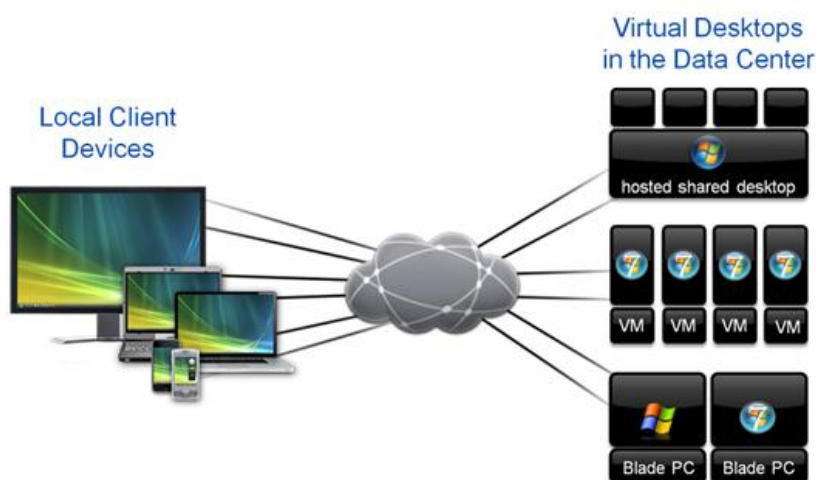


در این روش کاربران می توانند تحت شبکه و با استفاده از هر کامپیوتری به دسکتاپ خود دسترسی داشته باشد. تکنولوژی مجازی سازی دسکتاپ، با استفاده از مدل پردازشی مبتنی بر سرور، میزکار کاربر را از محل فیزیکی سخت افزار مستقل می کند. در این مدل، میزکار کاربر بجای اینکه روی حافظه محلی رایانه کاربر ذخیره شود، روی سرور ذخیره می شود. بنابراین زمانی که کاربر در حال کار است، تمامی برنامه ها، پردازش ها و داده ها روی سرور در حال اجرا و نگهداری هستند.

بهتر است این سیستم را با مثالی کاربردی شفاف کنیم.

بر اساس اصول امنیتی همگی نیاز داریم تا کاربران سازمان در ۲ محیط مجزا به فعالیت بپردازند؛ یکی شبکه LAN یا شبکه اطلاعاتی سازمان است و دیگری شبکه اینترنت. این در حالی است که کاربران فقط یک PC، Laptop یا تین کلاینت دارند و خرید دستگاهی مستقل و ایجاد شبکه ای مستقل برای استفاده از اینترنت به قدری هزینه بردار است که غیر ممکن تلقی می شود. اما این نیاز با استفاده از Virtual Desktop به صورت بسیار ارزان و بسیار ایمن و ایزوله کاملاً عملی است. کاربران با یک دستگاه به دسکتاپ مجازی خود متصل شده و بصورت کاملاً ایمن تمام کارهای اینترنتی را بر روی Virtual Desktop که خارج از شبکه اطلاعاتی سازمان تعبیه شده است انجام می دهند.

اگر هم Virtual Desktop دچار آلودگی یا حمله شود هیچ تأثیری بر روی اطلاعات سازمان یا دستگاه های کاربران نخواهد گذاشت.



به طور کلی مجازی سازی دسکتاپ دارای مزایای زیر است:

- امنیت بالای اطلاعات سازمان
- استفاده بیشتر از منابع سخت افزاری موجود
- پایداری و تحمل خطا
- کاهش هزینه ها با تغییر در زیر ساخت سخت افزاری
- کاهش هزینه های مدیریتی و نگهداری
- عدم نیاز به ارتقاء تک تک رایانه ها
- نصب و بروز رسانی متمرکز نرم افزار های سازمانی
- دفع خطر ویروس ها و دیگر بد افزارها
- دسترسی همیشگی میزکار کاربران مستقل از هر مکان در هر زمان
- Load Balancing
- High Availability (HA)
- Redundancy
- Zero Downtime

مقایسه نسخه های Corporate محصولات VMware، Hyper-V و Citrix

نرم افزار VMware ESXi/ESX اولین، سریع ترین و پایدار ترین شبیه ساز مقیم بر سخت افزار تاریخ کامپیوتر می باشد که در سال ۲۰۰۱ پا به عرصه دنیای شبکه گذاشته است و تا به امروز که ۵ نسل از این نرم افزار طراحی و ارائه شده است، VMware ESXi/ESX در ده ها هزار شبکه مختلف در حال سرویس دهی می باشد. تولید کنندگان دیگر زیر ساخت های مجازی سازی هنوز به دوران بلوغ و کمال نرسیده اند و برای اینکه بتوانند ثبات و اطمینان را به دیتا سنتر ها هدیه دهند کار های بسیاری برای انجام در پیش رو دارند.

با توجه به شکاف عمیقی که بین VMware و باقی رقبای از جمله Microsoft، Oracle و Citrix بوجود آمده، طبیعی است که هرگاه تلاش های رقبای آنان را به نسل موجود VMware نزدیک کنند ESX برای ارائه نسل بعدی و تمدید این شکاف آماده خواهد بود. به بیان بهتر این فاصله بوجود آمده موجب گردیده است تا VMware همیشه برگ برنده ای داشته باشد و بتواند تمایز خود را به همگان اثبات کند.

در این بخش سعی بر آن شده که به صورت اجمالی قیاسی داشته باشیم بر امکانات و توانایی های VMware در برابر شرکت های قدرتمندی همچون Microsoft و Citrix.



Hyper-v
Microsoft



فضای مورد نیاز برای استقرار نرم افزار

• **VMware:**

در صورتی که از نسخه رایگان ESXi استفاده شود تنها به ۷۰ مگابایت فضا نیاز دارد.

• **Microsoft Hyper-V:**

در صورتی که به صورت Server Core Only استفاده شود به ۲ گیگابایت و در صورتی که از Full Windows Installation استفاده شود به ۱۰ گیگابایت فضا نیاز است.

• **Citrix Xen Server:**

فضای مورد نیاز این نرم افزار به طور ثابت ۱,۸ گیگابایت می باشد.

سیستم عامل مورد نیاز برای اجرا

• **VMware:**

نسخه رایگان ESXi بدون نیاز به سیستم عامل پایه عمل نموده و مستقیماً با سخت افزار ارتباط برقرار می کند.

• **Microsoft Hyper-V:**

این نرم افزار بر پایه سیستم عامل Microsoft Windows Server 2008 سرویس دهی می کند.

• **Citrix Xen Server:**

این نرم افزار بر پایه سیستم عامل Linux NetBSD سرویس دهی می کند.

دراپور های سخت افزاری

• **VMware:**

دراپورها بر اساس حجم انبوهی از تولید کنندگان در این نرم افزار قرار داده شده اند.

• **Microsoft Hyper-V:**

دراپور های استاندارد Windows.

• **Citrix Xen Server:**

دراپور های استاندارد Linux.

مدیریت پیشرفته حافظه RAM

• **VMware:**

قابلیت استفاده از حافظه بلا استفاده یک ماشین برای یک ماشین دیگر.

• **Microsoft Hyper-V:**

این قابلیت وجود ندارد.

• **Citrix Xen Server:**

این قابلیت وجود ندارد.

مدیریت پیشرفته فضای مورد استفاده

- **VMware:**

امکانات پیشرفته ای از قبیل Storage vMotion به شما این امکان را می دهد که سرور مجازی را به صورت زنده و در حال سرویس دهی از یک SAN Storage به مکان دیگری انتقال دهید.

- **Microsoft Hyper-V:**

چنین گزینه ای در این نرم افزار وجود ندارد.

- **Citrix Xen Server:**

چنین گزینه ای در این نرم افزار وجود ندارد.

سرعت انتقال اطلاعات هارد دیسک مجازی I/O

- **VMware:**

بر اساس تکنولوژی سخت افزاری مورد استفاده محاسبه میگردد و عملاً برابر با توان سخت افزاری می باشد.

- **Microsoft Hyper-V:**

حداکثر برابر با گلوگاه (Bottleneck) سیستم عامل Windows Server می باشد.

- **Citrix Xen Server:**

حداکثر برابر با گلوگاه (Bottleneck) سیستم عامل میزبان.

انعطاف پذیری در اضافه نمودن منابع سخت افزاری

- **VMware:** امکان اضافه نمودن RAM و CPU در حالت فعال، بدون نیاز به توقف سرور

مجازی وجود دارد البته به شرطی که سیستم عامل میهمان پشتیبانی کند. همچنین امکان افزودن حجم هارد دیسک و یا یک هارد دیسک جدید در حالت فعال، امکان اضافه نمودن کارت شبکه در حالت فعال و . . . موجود است.

- **Microsoft Hyper-V:**

امکان اضافه نمودن هارد دیسک جدید در حالت فعال.

- **Citrix Xen Server:**

امکاناتی در این زمینه وجود ندارد.

برای بررسی دقیق تر به جدول صفحه بعد مراجعه فرمایید

جدول مقایسه بین VMware، Hyper-V و Citrix

Hypervisor Attributes	VMware vSphere 5.1	Windows Server 2012 with Hyper-V (beta)	Citrix XenServer 6
Small Disk Footprint	✓ 144 MB disk footprint	✗ >5GB with Server Core installation ~10GB with full Windows Server installation	✗ >1GB
OS Independence	✓ No reliance on general purpose operating system	✗ Relies on Windows 2012 in Parent Partition	✗ Relies on Linux in Dom0 management Partition
Hardened Drivers	✓ Optimized with hardware vendors	✗ Generic Windows drivers	✗ Generic Linux Drivers
Advanced Memory Management	✓ Ability to reclaim unused memory, de-duplicate memory pages, compress memory pages, swap to disk/SSD	✗ Only uses ballooning, requires special drivers—no Linux, no NUMA.	✗ Only uses ballooning.
Advanced CPU Management	✓ Tuned to support Intel SMT hyper-threading; Supports 3D graphics accelerators	✗ No reliable performance advantage when using hyper-threading	✗ No reliable performance advantage when using hyper-threading
Advanced Storage Management	✓ VMware vStorage VMFS	✗ Lacks an integrated cluster file system	✗ Lacks an integrated cluster file system, storage features support very few arrays
Virtual Security Technology	✓ VMware vShield Endpoint Enables hypervisor level security introspection	✗ Nothing comparable	✗ Nothing comparable
Flexible Resource Allocation	✓ Hot add VM vCPUs and memory, VMFS volume grow, hot extend virtual disks, hot add virtual disks	✗ Nothing comparable	✗ Nothing comparable
Simplified Patching	✓ No unrelated patching; Image-based patching with rollback capabilities provide clean and simple host patching	✗ Subject to unrelated patching; Complex patching architecture requires additional effort and complexity	✗ Subject to unrelated patching; Requires manual updates

BACKUP

۳۶۴ روز پایداری، اما فقط یک روز سیاه و بحرانی
مکانیزم پشتیبان گیری آن روز باید در کنار شما باشد
راه حل های پشتیبان گیری و مدیریت بحران

www.vaya.ir

(۰۲۱) ۴۴۲ ۳۱۱ ۴۷

(۰۲۸۱) ۳۳۵ ۹۶ ۷۰



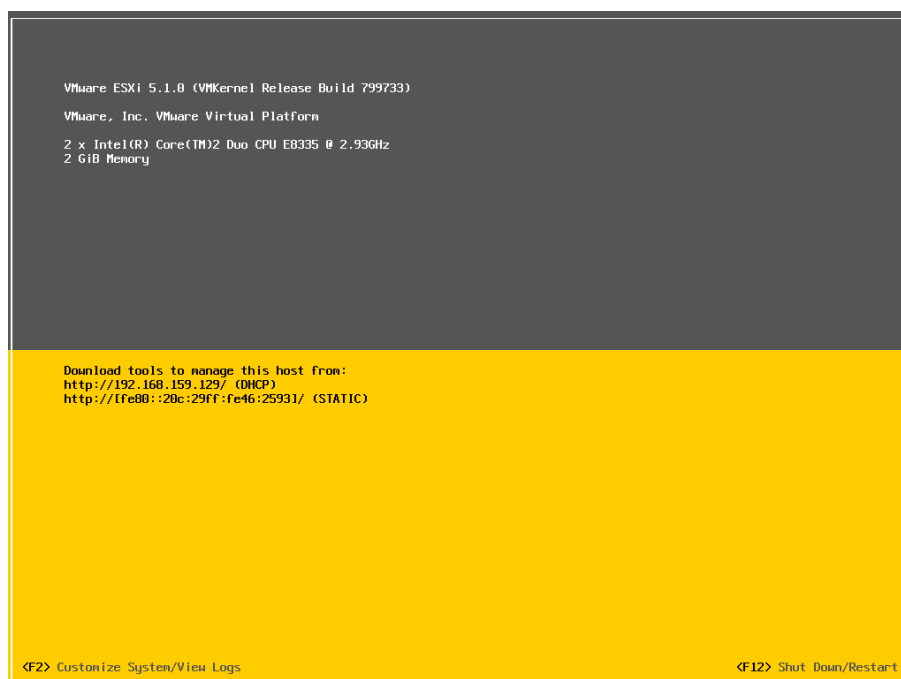
آشنایی با برخی از اصطلاحات رایج مجازی سازی و کاربرد آنها

از آنجا که نرم افزار مجازی سازی VMware نسبت به سایر رقبا رایج تر و کاربردی تر می باشد، به معرفی برخی از اصطلاحات رایج در این پلت فرم می پردازیم. بدیهی است با درک کارایی هریک و آگاهی از نحوه عملکرد آن قابلیت، در تشخیص و به کار گیری محصولات کمپانی های دیگر نیز تسلط خواهید یافت.

VMware ESXi و VMware ESX

این نرم افزارها در حقیقت خود به نوعی سیستم عامل محسوب می شوند، زیرا در هنگام نصب مستقیماً بر روی سخت افزار نصب می شوند و نیازی به سیستم عامل میزبان یا به اصطلاح Host ندارند و از مجموعه نرم افزارهای Hostless محسوب می شوند. ESXi آخرین ورژن از سری نرم افزاری VMware Hypervisor است. تکنولوژی استفاده شده از نوع Bare Metal و مستقل از سیستم عامل می باشد.

این پلت فرم همچنین مدیریت کاملی بر روی سخت افزار و منابع سیستم اعمال می کند. شرکت VMware بعد از ارائه نسخه 4.1 به دلایلی که در ادامه ارائه شده است به کاربران خود توصیه کرد تا از ESXi استفاده کنند.



چند تفاوت اصلی بین ESX و ESXi:

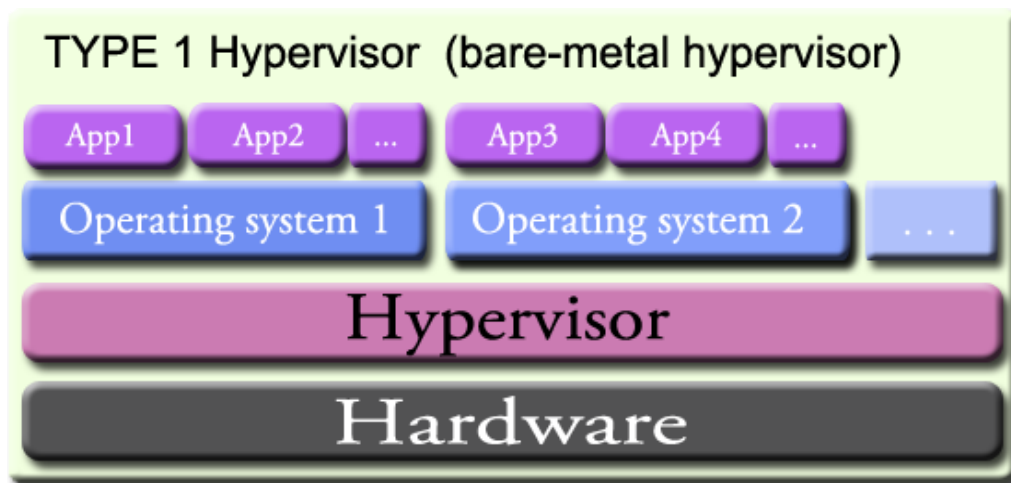
- ۱- حذف Service Console برای همگان:
قبلا Service Console فقط برای کسانی که ESXi را خریداری می کردند حذف شده بود ولی در ESXi 5.0 برای تمامی افرادی که این محصول را نصب می کنند (چه خریداری کرده باشند و چه نکرده باشند) حذف شده است.
- ۲- فایل سیستم VMFS 5:
VMFS در واقع فایل سیستم مربوط به VMware است، مانند NTFS که فایل سیستم مربوط به Windows است. VMFS 5 دیگر MBR-Base نیست، بلکه GPT-Bsae می باشد که این امر محدودیت DataStore را از 2TB به 64TB افزایش داده است و همچنین دیگر مجبور به مشخص کردن Block Size که قبلا باعث محدودیت در حجم Virtual Disk می شد نیستند.
- ۳- پشتیبانی از طیف وسیعتری از سخت افزارهای مختلف:
ESXi 5.0 طیف وسیعتری از SATA Controller ها را پشتیبانی می کند و این امر سبب سهولت در نصب ESXi 5.0 روی سخت افزارهای ارزانتر می شود.
- ۴- ESXi سبک تر و دارای سرعت بوت و نصب بالاتری می باشد.
- ۵- ESXi دارای دیواره آتش بهتر، با مدیریت و پیکربندی پیشرفته تری است.
- ۶- در ESXi، قسمت Health Status نهاده شده است. (وضعیت CPU، RAM، فضای ذخیره سازی، دمای سرور، وضعیت fan ها و ...)
- ۷- بعضی از خصوصیات شبکه در ESXi، به واسطه سرویس ها پیکربندی می شود در نتیجه خطای کمتری به وجود می آید.
- ۸- به دلیل امنیت بالا، ESXi به وصله های امنیتی کمتری نیاز دارد و در نتیجه ریسک کمتری برای تغییرات وجود دارد.

Hypervisor چیست؟

Hypervisor لایه ای است که در سیستم های مجازی سازی وظیفه کنترل منابع سخت افزاری را بر عهده دارد و به طور مستقیم یا بهتر بگوییم بدون واسطه سخت افزار را کنترل می کند.

از جمله مزایای Hypervisor می توان به امکان دسترسی مستقیم به سخت افزار که سبب افزایش سرعت عملکرد لایه مجازی سازی می شود اشاره کرد. همچنین این روش، امکان اجرای پروسه های نرم افزاری بدون ارسال درخواست ها به واسطه یا سیستم عامل میزبان را فراهم می کند.

Hypervisor ها کاملاً وابسته به سخت افزار نیستند و امکان ارسال پروسه های یک Hypervisor به سخت افزاری دیگر و اجرای آن وجود دارد. امکان کنترل منابع در یک Hypervisor به طور کامل قابل اعمال است.

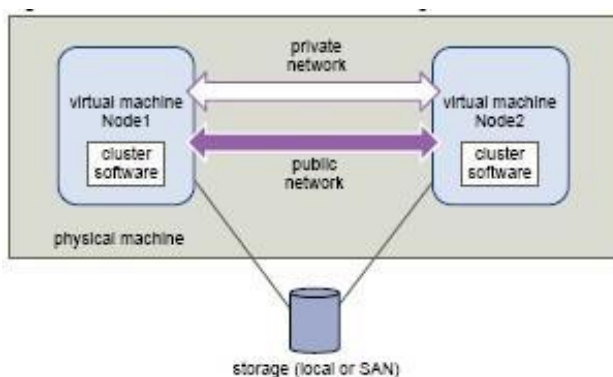


Clustering چیست؟

(a) **Clustering ماشین های مجازی بر روی یک سرور فیزیکی (ESX/ESXi Host)**

یک کلاستر بر روی یک سرور فیزیکی، از ماشین های مجازی کلاستر شده بر روی یک سرور ESX/ESXi تشکیل شده است که اصطلاحاً این نوع از Cluster را حالت جزیره نیز می نامند. ماشین های مجازی به یک حافظه اشتراکی متصل هستند. این نوع از

پیکربندی پایداری سرویس های ما را در برابر مشکلات احتمالی که برای سیستم های عامل پیش می آید بالا می برد، ولی به دلیل عدم وجود سرور فیزیکی دیگر، توانایی پایدار نگاه داشتن سرویس ها را در برابر مشکلات سخت افزاری ندارد.



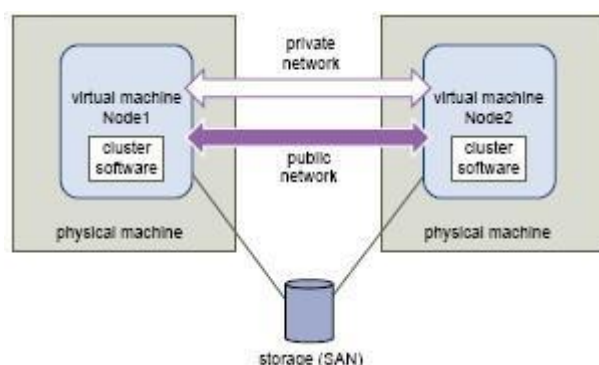
همانطور که در شکل بالا می بینید

- دو ماشین مجازی بر روی یک سرور (Host) سخت افزاری (ESX/ESXi Host) کلاستر شده اند.
- ماشین های مجازی با یک لینک اختصاصی به یکدیگر متصل شده اند که ارتباط لحظه به لحظه را برای آنها فراهم می کند.
- هر ماشین مجازی به حافظه اشتراکی واحدی متصل است که می تواند SAN یا Local Disk باشد.

(b) Clustering ماشین های مجازی بر روی چند سرور فیزیکی (ESX/ESXi Hosts)

در این نوع از Clustering، ماشین های مجازی بر روی سرور های فیزیکی مختلف به صورت کلاستر در می آیند و علاوه بر پایداری در برابر مشکلات نرم افزاری و سیستم عامل ها، در برابر مشکلات سخت افزاری نیز پایداری سرویس ها را حفظ می کنند.

این معماری حتماً به حافظه اشتراکی و ترجیحاً بر پایه فیبر نوری (SAN FC) احتیاج دارد.

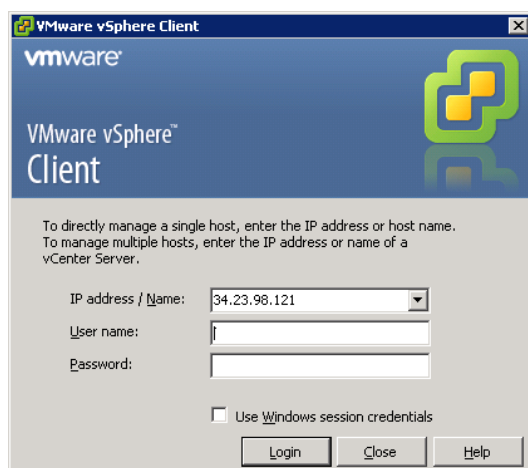


همانطور که در شکل بالا می بینید

- دو ماشین مجازی بر روی دو سرور فیزیکی به صورت کلاستر در آمده اند.
- ماشین های مجازی به وسیله لینک اختصاصی جهت ارتباط لحظه به لحظه (Heartbeat) و لینک عمومی به یکدیگر متصل هستند.
- هر ماشین مجازی به حافظه اشتراکی که باید بر روی SAN باشد متصل هستند.

vSphere Client چیست؟

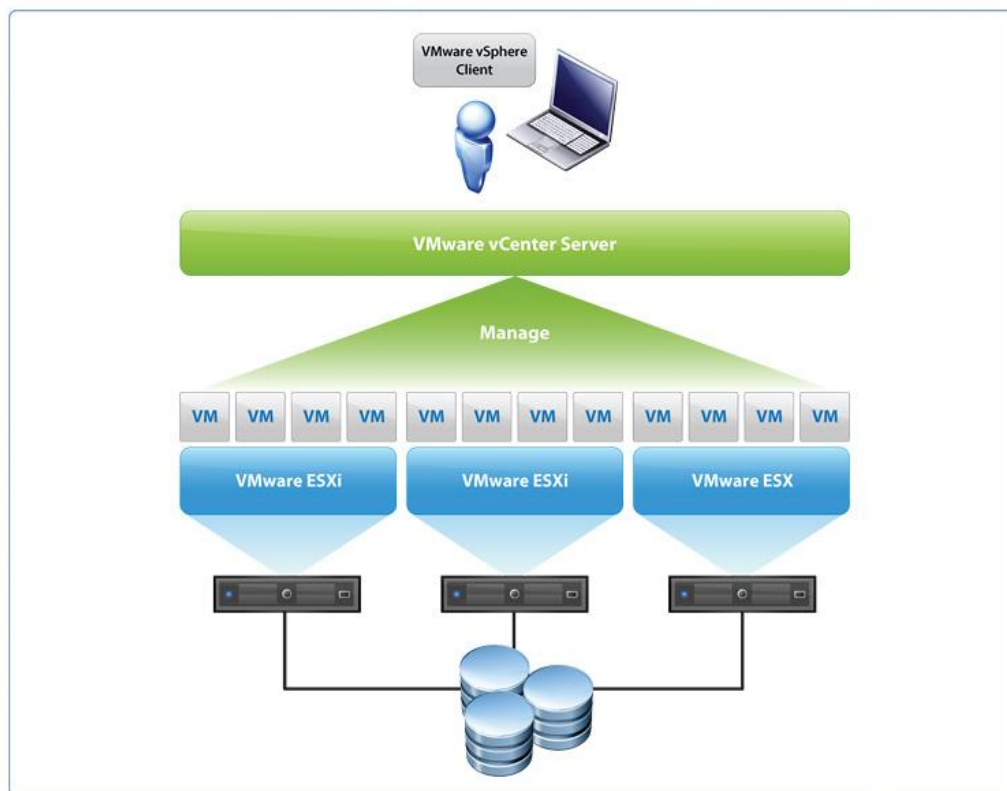
همانگونه که می دانید ESX به صورت CLI است. بنابراین برای مدیریت ماشین های مجازی از نرم افزار vSphere Client استفاده می گردد.



vCenter Server چیست؟

vCenter نرم افزاری برای مدیریت vSphere و کلاستر کردن هاست ها می باشد. vCenter Server ابزار است برای مدیریت متمرکز تمام ماشین های ESXi و تمامی متعلقات و ماشین مجازی ساخته شده بر روی آنها. همچنین برای کمک به توسعه پذیری محیط Server vCenter یک پایگاه داده Back-End برای نگهداری اطلاعات مربوط به میزبان ها و ماشین مجازی بکار می گیرد، که این بانک اطلاعاتی می تواند Microsoft SQL و یا Oracle باشد. در نسخه های قبلی vSphere، vCenter Server فقط می توانست بر روی ویندوز اجرا شود ولی در نسخه ۵ یک Appliance پایه لینوکس همراه با مجموعه ارائه شده است.

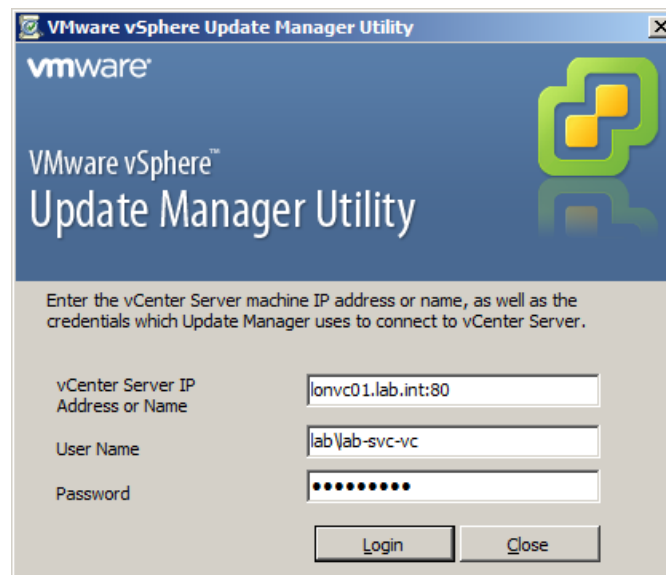
البته بدون استفاده از vCenter Server هم می توان سرورهای ESXi را بصورت منفرد مدیریت کرد، ولی برای استفاده از قابلیت های بسیار ارزشمند مجموعه مجازی سازی VMware vSphere نظیر، vMotion، زمان بندی منابع توزیع شده (DRS)، قابلیت دسترسی مستمر (High Availability)، سیستم تحمل خطا (Fault Tolerance) و بسیاری از قابلیت های دیگر که در ادامه توضیح داده خواهد شد، استفاده از vCenter لازم است.



vSphere Update Manager

Update Manager پلاگینی است برای vCenter Server که به کمک آن می توان سرورهای ESXi و ماشین های مجازی انتخاب شده را با آخرین Update ها و Patch ها به روز رسانی کرد. Update Manager امکانات زیر را فراهم می آورد:

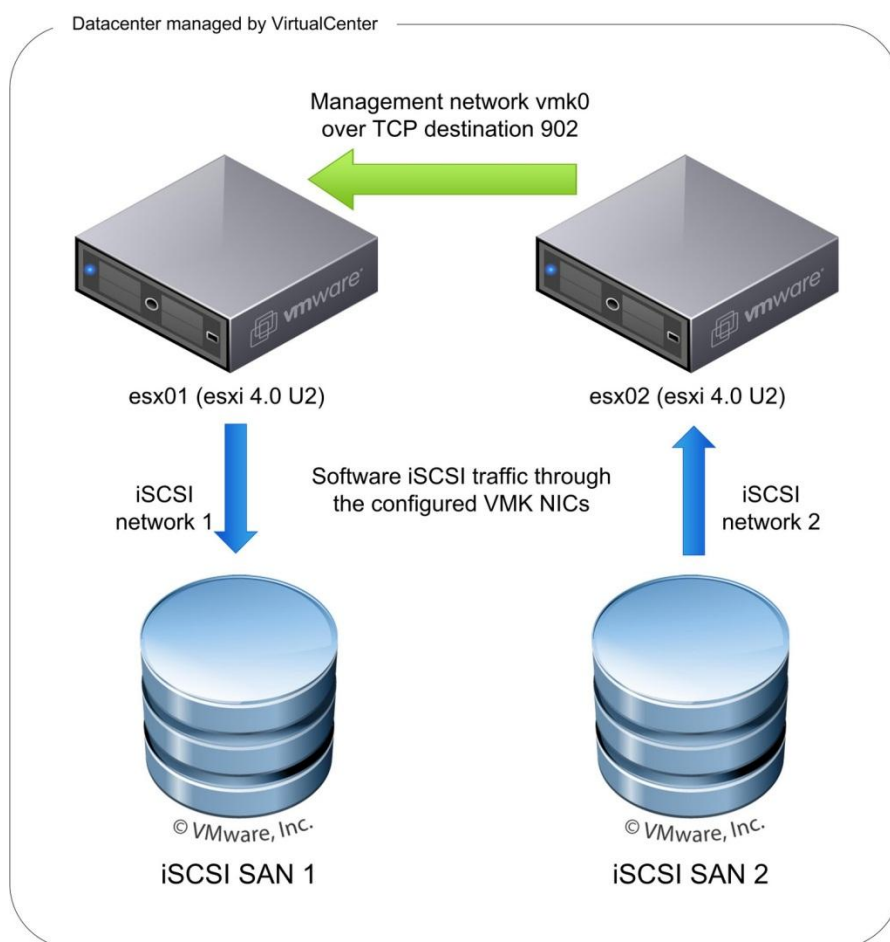
- بررسی و تشخیص سیستم هایی که نیاز به بروز شدن دارند.
- نصب خودکار آپدیت ها
- یکپارچگی کامل با دیگر قابلیت های vSphere مثل سیستم زمان بندی منابع توزیع شده



vMotion چیست؟

ابزار vMotion که Live Migration نیز خوانده می شود، یکی از بهترین و جذاب ترین قابلیت هایی است که vSphere در اختیار ما قرار می دهد و آن انتقال ماشین های مجازی در حال اجرا از یک میزبان فیزیکی به میزبان دیگر، بدون حتی لحظه ای خاموش شدن ماشین مجازی و قطع شدن اتصال ماشین مجازی به شبکه می باشد. vMotion محتویات در حال اجرا (حافظه اصلی)

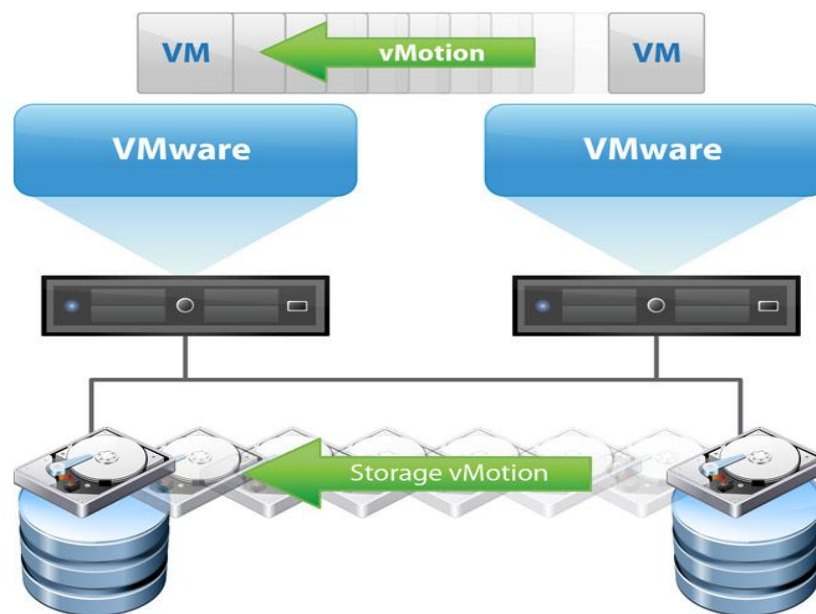
را از یک سیستم به سیستم دیگر منتقل می کند اما محتویات سیستم ذخیره سازی دست ناخورده در جای خود باقی می ماند.



Storage vMotion چیست؟

یکی دیگر از امکانات جالب vSphere این است که شما را قادر می سازد یک ماشین مجازی را در حالیکه روشن و در حال سرویس دهی است از روی یک Storage (جایی که محل قرارگیری ماشین های مجازی است) بر روی یک Storage دیگر انتقال دهید.

Storage vMotion امکانی است برای انتقال محتویات دیسک مجازی یک سیستم مجازی خاموش و یا در حال اجرا از یک واحد ذخیره سازی به یک واحد ذخیره سازی دیگر، بدون جابجایی ماشین پردازش. یعنی محل اجرای ماشین مجازی تغییر نمی کند و این در حالی اتفاق می افتد که ماشین مجازی روشن بوده و طی زمان انتقال واحد ذخیره سازی خللی در کار آن ایجاد نمی شود.



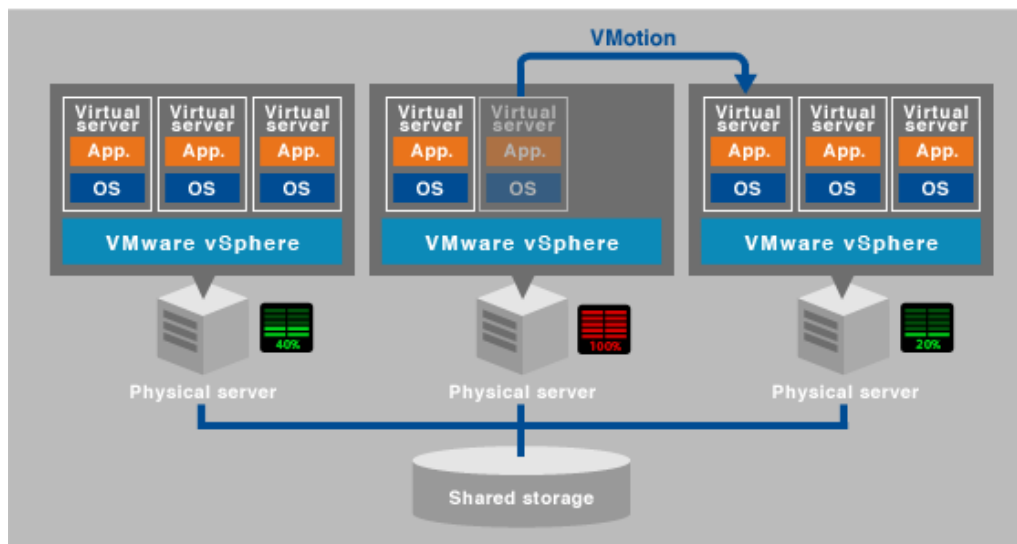
Distributed Resource Scheduler (DRS) چیست؟

vMotion یک عمل دستی است. یعنی مدیر سیستم باید به طور دستی عمل vMotion را انجام دهد. اگر بخواهیم با توجه به نیاز مثلاً برای تنظیم بار میزبان های ESXi عمل vMotion بطور خودکار انجام شود، اینجاست که پای زمان بندی منابع توزیع شده و یا به اختصار DRS وسط می آید.

پیشتر با مفهوم کلاستر آشنا شدید نیازی به تکرار دوباره نیست. در مجموعه vSphere، کلاستر، مجموعه ای از میزبان های ESXi است که منابع خود را در یک استخر منابع (Resource Pool) به اشتراک می گذارند. به عبارت دیگر کلاستر ESXi، یک تجمع توان پردازشی و حجم حافظه های تمام میزبان های عضو کلاستر است.

VMware Distributed Resource Scheduler (DRS)

Automatic resource allocation based on CPU and memory load status



حال بر می گردیم به موضوع DRS، اهداف و وظایف DRS در دو بند خلاصه می شود:

- در هنگام شروع (روشن شدن ماشین مجازی)، DRS سعی می کند ماشین های مجازی را در میزبانی اجرا کند که دارای بار پردازشی کمتری باشد.
- هنگامی که ماشین مجازی در حال اجرا است، DRS مدام (هر ۵ دقیقه یکبار) در حال جستجو و اندازه گیری است تا ماشین های مجازی را به میزبانی انتقال دهد که برای منابع مورد نیازشان، کمترین رقابت وجود داشته باشد.

مورد اول که معمولاً Intelligent Placement نیز خوانده می شود اشاره به این مفهوم دارد که در هنگام روشن شدن ماشین مجازی که در داخل یک کلاستر قرار دارد، ماشین مجازی برای اجرا به میزبانی منتقل می شود که از لحاظ منابع آزاد موجود بهترین باشد. بند دوم هم این موضوع را بیان می کند که حتی وقتی ماشین های مجازی روشن هم هستند DRS دائماً سعی می کند بهترین میزبان ESXi را از نظر منابع آزاد موجود که در داخل همان کلاستر قرار دارد، برای انتقال ماشین مجازی انتخاب کند.

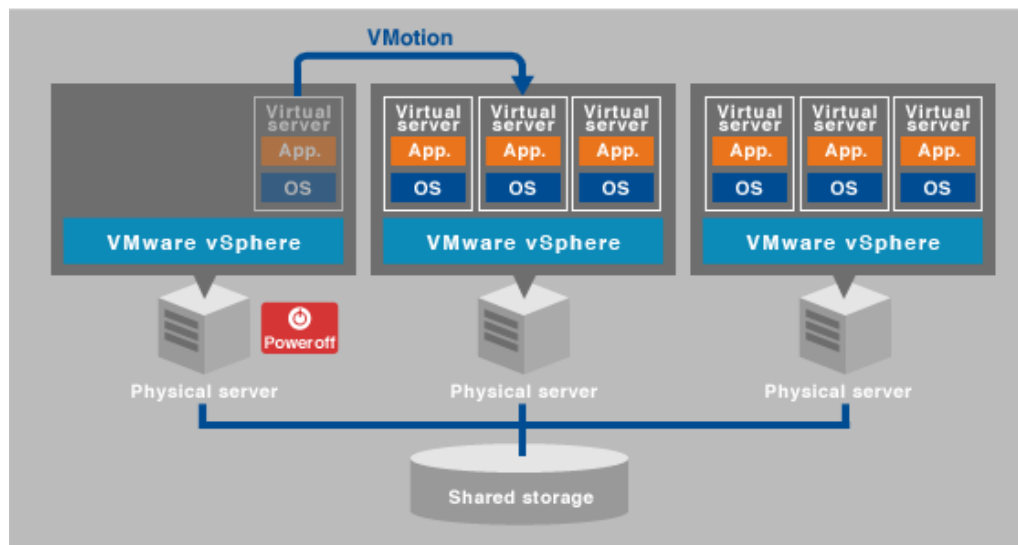
مثلا وقتی در هنگام روشن بودن چندین ماشین مجازی عضو کلاستر، اگر یک یا چند ماشین مجازی بار پردازش بالایی را به سیستم تحمیل کنند، DRS به طور خودکار یک یا چند عدد از آنها را به ESXi های عضو همان کلاستر که منابع پردازشی آزاد بیشتری دارند، منتقل می کند.

Distributed Power Manager (DPM) چیست؟

با توجه به وضع کنونی و اهمیت و صرفه جویی در برق مصرفی، این تکنولوژی بسیار می تواند کارآمد باشد. اساس کار این تکنولوژی به این صورت است که پس از پایان ساعات کاری که بار بر روی سرورها کم می شود، به شکل اتوماتیک آنها را به یک یا چند ESX Server مشخص منتقل می نماید و بقیه ESX ها را تا زمانی که دوباره بار کاری زیاد شود (برای مثال صبح روز کاری بعد) به صورت Stand by نگه می دارد. این کار تاثیر زیادی در میزان برق مصرفی خواهد گذاشت همچنین عمر سرورها را هم افزایش خواهد داد.

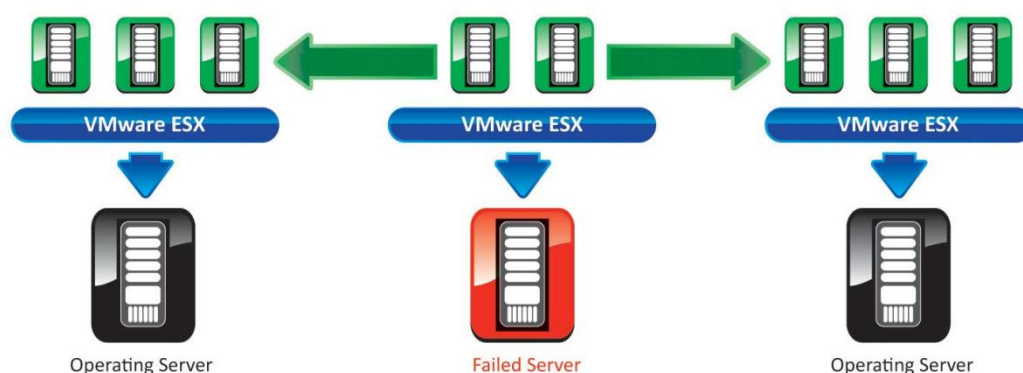
VMware Distributed Power Management (DPM)

Power reduction by enabling shutdown of underutilized servers



قابلیت دسترسی مستمر (High Availability)

نگرانی که ممکن است پیش آید این است که اگر چندین سرور مجازی بر روی یک سرور فیزیکی اجرا شوند، در صورت خراب شدن سرور فیزیکی تمام سرور های مجازی از کار خواهد افتاد! دسترسی مستمر پاسخی به این مشکل است. عملکرد این تکنولوژی بدین صورت است که ابتدا دو یا چند سرور فیزیکی در قالب یک کلاستر قرار می گیرند و ماشین های مجازی بر روی سرور های فیزیکی کلاستر توزیع می شوند. اگر یکی از سرور ها (Hostها) خراب شود، ماشین های مجازی آن Host به Host های دیگر عضو آن کلاستر منتقل می شوند. در این بین ماشین های مجازی اجرا شده بر روی سرور خراب شده قبل از انتقال Reset می شوند. تمام این اعمال بطور کاملاً اتوماتیک انجام می شوند. شکل زیر این مساله را به تصویر کشیده است.



سیستم تحمل خطا (Fault Tolerance)

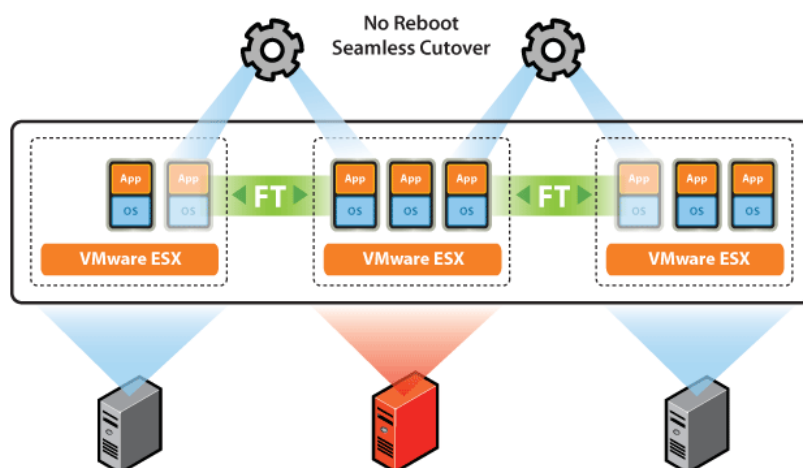
در یک کلاستر که HA در آن فعال است چنانچه یکی از سرورهای فیزیکی به هر دلیلی از کار بیافتد ماشین های مجازی آن، قبل از انتقال به سرور فیزیکی دوم Reset می شوند و برای مدت کوتاهی که ممکن است تا ۳ دقیقه طول بکشد، خارج از سرویس خواهند بود و قاعدتاً تمام داده های ذخیره نشده داخل حافظه RAM از بین خواهند رفت. FT تکنولوژی است که حتی این مساله را نیز حل کرده است.

عملکرد این تکنولوژی بدین صورت است که در کلاسترهایی که FT فعال است یک کپی از ماشین های مجازی در حال اجرا، بر روی یک سرور دومی نیز اجرا می شوند و در صورت بروز

اختلال در یکی از سرور های فیزیکی بلافاصله و بدون کوچکترین وقفه ای ماشین های مجازی جایگزین شده و کاربر نهایی متوجه این موضوع نخواهد شد.

بعد از جایگزینی یک کپی از ماشین مجازی بر روی سرور سوم ایجاد خواهد شد. تمامی این اعمال بطور اتوماتیک توسط vSphere انجام می شود. شکل زیر این موضوع را به تصویر کشیده است.

اگر هر دو سرور اصلی و سرور آینه ای خراب شوند ماشین مجازی، Reset می شود و یک کپی از آن بر روی سرور در دسترس، دوباره اجرا خواهد شد.



نمونه های از موارد موفق در مجازی سازی (Success Stories)

۱- یک دانشگاه بزرگ آمریکایی

به دنبال مدرن کردن تجهیزات، یک دانشگاه بزرگ آمریکایی اقدام به رسیدگی به تجهیزات IT خود کرد در این باره رییس مرکز IT میگوید: "ما سخت افزارهایی داشتیم که به آخر عمر خود رسیده بودند و به سختی در دسترس قرار میگرفتند. ما دریافتیم که مجازی سازی راهی ساده و موثر در زمینه ی مدرن شدن است."

دانشگاه مزایای خرید لایسنس VMware را برای قسمت شبکه ی دانشگاه Ohio بررسی و تهیه نمود. به گفته ی CIO خرید VMware این اجازه را به ما داد که اهداف IT خود را سریعتر پیش ببریم.

داشتن راهکار VMware در دانشگاه مزایای فراوانی از جمله مقیاس پذیری (Scalability) و کارایی مناسب و از همه مهمتر کاهش هزینه ها داشت. همچنین CIO میگوید با داشتن VMware در مقابل نیازهای مشتری، محیط IT انعطاف پذیر و مناسبی فراهم می آید.

نتایج:

- ذخیره ۴۰۰,۰۰۰ دلار برای راه اندازی سیستم های قدیمی در یک سال مالی
- کاهش هزینه های اصلی به میزان ۵۰ درصد (CIO می گوید اگر به جای VMware سیستم های فیزیکی می خریدم، هزینه های من دوبرابر می شد).
- افزایش کارایی IT
- کار کردن کمتر با داشتن بیشترین سرور (CIO می گوید می تواند با یک سرور ۶۰۰ سرور دیگر را مدیریت کند)

۲- شرکت بزرگ نفتی Sand Mining

در شرکت بزرگ نفتی Sand Mining تمام پروژه های IT با تحلیل بر ارزش آن آغاز میشود. همیشه و بدون استثنا این نتایج و تحلیل ها نشان داده است که مجازی سازی با تکنولوژی VMware بهترین انتخاب است.

شرکت نفتی Sand Mining در Calgary واقع شده است. این مجموعه جزء بزرگترین شرکت استخراجی نفت و گاز محسوب می شود و روز به روز به ارقام استخراج خود، فضاهای موجود و بخش شبکه سازمان می افزاید.

وضعیت سیستمی این شرکت از خیلی جهات شبیه ساختار IT دیگر محیط های بزرگ تجاری است. ۴۵۰ سرور در ۳ دیتاسنتر که Oracle های نصب شده بر روی لینوکس ویرایش Red Hat و Solaris و SQL های نصب شده بر روی Windows وظیفه ذخیره سازی و حمایت از اطلاعات آنرا بر عهده دارند.

به علاوه شرکت از ۱۴۰۰ نرم افزار استفاده می نمود که استراتژیک بودند و نمی شد آنها را در نظر نگرفت. این حجم نرم افزاری و اطلاعاتی، فشاری بر روی دیتاسنترهای Calgary ایجاد کرده بود که نیاز به منابع بیشتری برای ذخیره سازی داشتند.

ذخیره سازی ۲ میلیون دلاری

مسئول سرویس دهی شرکت میگوید: "یکی از دلایل اجرا کردن راه کار VMware، کم کردن هزینه ها بود. او میگوید محاسبات ما نشان میدهد که هزینه راه اندازی سرورهای VMware در ۴ سال معادل ۴,۵۰۰ دلار است. این در حالی است که هزینه خرید یک سرور با ۲ عدد CPU فیزیکی در طی این مدت ۳۵,۹۰۰ دلار می شود.

ماشین های مجازی با توجه به High Availability که دارند نسبت به سیستم های فیزیکی قدیمی کارایی بیشتری ارائه می دهند. با اجرای این پروژه شرکت از هزینه ۱.۷ میلیون دلاری خرید تجهیزات سخت افزاری و ۱.۴ میلیون دلاری هزینه انرژی و ۴۹۰,۰۰۰ دلاری خرید نرم افزار که جمعاً باعث صرفه جویی با رقمی بیش از ۳ میلیون دلار می شود، سود بزرگی کسب نمود.

مدیریت سیستم های مجازی هم راحت تر از حالت فیزیکی آن است. برای مثال قبلاً ۱۴ کارمند برای مدیریت ۱۹۶ سرور فیزیکی مورد نیاز بود و اکنون ۱۱ کارشناس به خوبی ۴۸۵ سرور مجازی را مدیریت می کنند.

تکنولوژی VMware برای ذخیره سازی

مجازی سازی فقط شروع کار برای سازمان بود و بلوغ کامل آن در محیط های ذخیره سازی آشکار شد. به علت حجم وسیع کار، اطلاعات به صورت تصاعدی افزایش می یافت. شرکت تصمیم گرفت ساختار قدیمی ذخیره سازی اطلاعات را با SAN Storage های مبتنی بر فیبر نوری جایگزین نماید. این تصمیم هم باعث کاهش هزینه ها و هم کاهش حجم درخواستی سرورها به میزان ۷ ترابایت شد.

با تکنولوژی vStorage VMware ما دیگر برای اضافه کردن سرور نیاز به فراخوانی تیم ذخیره سازی نداریم زیرا این ساختار کاملاً خودکار می باشد.

با VMware vSphere شرکت دید بهتری بر روی منابع ذخیره سازی و سرورهای خود پیدا کرد. تا جایی که اخیراً نیز با قرار دادن Cisco Nexus 1000v در مدار شبکه مجازی شده شبکه قویتری را در اختیار ماشین های مجازی قرار داده است.

سوالات متداول (FAQ)

- چه سخت افزاری برای اجرا کردن vSphere با ساختار ESXi لازم است؟
ساختار ESXi Hypervisor بر روی هزاران سیستم سروری تصدیق شده است و می تواند روی بعضی USB KEY های خاص هم اجرا گردد. به طور کلی سخت افزارهایی که با ESX سازگار بودند نیز میتوانند ESXi را پشتیبانی کنند. اما برای اطلاعات بیشتر درباره سازگاری سیستم خود بهتر است به HCL سایت VMware مراجعه کنید.
- چه سیستم عاملی را میتوانیم بر روی vSphere با ساختار ESXi نصب کنیم؟
VMware مانند تمامی ارائه دهندگان مجازی سازی از طیف وسیعی از سیستم عامل ها پشتیبانی می کند.
- آیا میتوان ماشین هایی که توسط Microsoft Virtual Server ، Microsoft Virtual PC یا VMware Server تعریف شده اند را بر روی vSphere اجرا کرد؟
بله شما میتوانید از ابزار رایگان شرکت به نام VMware vCenter Converter برای وارد کردن سیستمهای ساخته شده توسط Microsoft Virtual Server و غیره به vSphere بهره بجویید. VMware vCenter Converter حتی میتواند از منابعی مانند سیستم های فیزیکی نیز برای تبدیل به سیستم مجازی استفاده کند.
- آیا vCLI و Power CLI در ESX و ESXi یکسان کار میکنند؟
اکثر دستورات vCLI و Power CLI بر روی هر دو ساختار یکسان کار می کنند. دستورات کمی از vCLI موجود است که با ESX سازگاری ندارد و این موارد در جدول توضیحات vCLI آمده است. همچنین تفاوت های خاص ساختاری بین دستورات vCLI و COS وجود دارد که در KB1008194 به آن اشاره شده است.
- ESXi Shell چیست؟

ESXi Shell حالت دستوری برای تحلیل و ترمیم سیستم های اجرا شده vSphere بر روی ESXi می باشد. ESXi Sell می تواند از طریق DCUI یا vCenter Server فعال و غیر فعال شود و حتی میتوان به صورت Remote از طریق SSH به آن دسترسی داشت.

- آیا SSH برای ESXi حمایت می شود؟

بله، دسترسی SSH به ESXi Shell از ورژن ۴.۱ به بعد قابل پشتیبانی است.

- چه سرور هایی با VMware vSphere 5 سازگارند؟

VMWare لیستی از سخت افزار های سازگار با vSphere ارائه داده است که می توان آن را در صفحه HCL سایت مشاهده نمود.

- آیا با ابزار هایی مانند iPad می توان به ESX/ESXi متصل شد و آنرا مدیریت کرد؟

ابزار های مربوطه برای iOS و Android وجود دارد، اما بصورت مستقیم نمی توانید به Host های ESX یا ESXi متصل شوید. برای مدیریت سرور های مجازی چنانچه از vSphere استفاده می کنید و vCenter دارید، می توانید پلاگین vCMA را بر روی vCenter نصب و فعال نمایید و به راحتی با آن ارتباط برقرار نمایید.

در دنیای مجازی امروز

اعین، سریع و پایدار

به حرکت ادامه دهید.

www.vaya.ir
021-44231147



هفت پات ایرا
خود را از ما بخواهید

هانی پات چیست؟ | HONEYPOT

هانی پات یا طعمه و دام برای هکر ها

Honeypot ها یک تکنولوژی تقریباً جدید و شدیداً پویا هستند. همین ماهیت پویا باعث می شود که به راحتی نتوان آنها را تعریف کرد. Honeypot ها به خودی خود یک راه حل به شمار نرفته و هیچ مشکل امنیتی خاصی را حل نمی کنند، بلکه ابزارهای بسیار انعطاف پذیری هستند که کارهای مختلفی برای امنیت اطلاعات انجام می دهند و تأثیر شگرفی بر امنیت سازمان می گذارند.

این فن آوری با تکنولوژیهای مانند فایروالها و سیستمهای تشخیص نفوذ (IDS) متفاوت است، چرا که آنها مسائل امنیتی خاصی را حل کرده و به همین دلیل راحت تر تعریف می شوند. فایروالها یک تکنولوژی پیشگیرانه به شمار می آیند، آنها از ورود مهاجمان به شبکه یا سیستم های کامپیوتری جلوگیری می کنند. IDS ها یک تکنولوژی تشخیصی هستند. هدف آنها این است که فعالیتهای غیر مجاز یا خرابکارانه را شناسایی کرده و درباره آنها به متخصصان امنیت هشدار دهند. تعریف Honeypot کار سخت تری است، چرا که آنها در پیشگیری، تشخیص، جمع آوری اطلاعات و کارهای دیگری مورد استفاده قرار می گیرند، اما حالت دفاعی ندارند و به عبارتی کار امنیتی نمی کنند اما بر امنیت شبکه به شدت تأثیر گذارند.

شاید بتوان یک Honeypot را با عناوین زیر توصیف کرد:

- یک هانی پات با هویتی نفوذ پذیر به وظایف خود می پردازد.
- هانی پات یک ابزار امنیتی است و نقشی ضروری در امنیت سازمانها، بسیار بیش تر از Firewall و IPS ایفاء می کند.
- Honeypot یک سیستم اطلاعاتی است که ارزش آن به استفاده غیر مجاز و ممنوع دیگران از آن است.

این تعاریف به وسیله اعضای لیست ایمیل Honeypot انجام شده است. لیست ایمیل Honeypot یک انجمن متشکل از بیش از ۵۰۰۰ متخصص امنیت است. از آنجاییکه Honeypot ها در اشکال و اندازه های مختلفی وجود دارند، ارائه تعریف جامعی از آن کار بسیار سختی است. تعریف یک Honeypot نشان دهنده نحوه کار آن و یا حتی هدف آن نیست. این تعریف صرفاً ناظر به نحوه ارزش گذاری یک Honeypot است. به عبارت ساده تر، Honeypot ها تکنولوژی هستند که ارزش آنها به تعامل مجرمان با آنها بستگی دارد. تمامی Honeypot ها بر اساس یک ایده کار می کنند: هیچکس نباید از آنها استفاده کند و یا با آنها

تعامل برقرار نماید، هر تعاملی با Honeypot غیر مجاز شمرده شده و نشانه ای از یک حرکت خرابکارانه به شمار می رود.

یک Honeypot سیستمی است که در شبکه سازمان قرار می گیرد، اما برای کاربران آن شبکه هیچ کاربردی ندارد و در حقیقت هیچ یک از اعضای سازمان حق برقراری هیچگونه ارتباطی با این سیستم را ندارند. این سیستم دارای یک سری ضعفهای امنیتی عمدی است. از آنجاییکه مهاجمان برای نفوذ به یک شبکه همیشه به دنبال سیستمهای دارای ضعف می گردند، این سیستم توجه آنها را به خود جلب می کند و با توجه به اینکه هیچکس حق ارتباط با این سیستم را ندارد، پس هر تلاشی برای برقراری ارتباط با این سیستم، یک تلاش خرابکارانه از سوی مهاجمان محسوب می شود. در حقیقت این سیستم نوعی دام است که مهاجمان را فریب داده و به سوی خود جلب می کند و به این ترتیب علاوه بر امکان نظارت و کنترل کار مهاجمان، این فرصت را نیز به سازمان می دهد که فرد مهاجم را شناسایی کند و از سیستمهای اصلی شبکه خود دور نگه دارند.

یک Honeypot هیچ سرویس واقعی ارائه نمی دهد. هر تعاملی که انجام گیرد، هر تلاشی که برای ورود به این سیستم صورت گیرد، یا هر فایل داده ای که روی یک Honeypot مورد دسترسی قرار گیرد، با احتمال بسیار زیاد نشانه ای از یک فعالیت خرابکارانه و غیر مجاز است. برای مثال، یک سیستم Honeypot می تواند روی یک شبکه داخلی به کار گرفته شود. این Honeypot از هیچ ارزش خاصی برخوردار نیست و هیچکس در درون سازمان نیازی به استفاده از آن ندارد و نباید از آن استفاده کند. این سیستم می تواند به ظاهر یک فایل سرور، یک وب سرور، یا حتی یک ایستگاه کاری معمولی باشد. اگر کسی با این سیستم ارتباط برقرار نماید، به احتمال زیاد در حال انجام یک فعالیت غیر مجاز یا خرابکارانه است.

در حقیقت، یک Honeypot حتی لازم نیست که حتماً یک کامپیوتر باشد. این سیستم می تواند هر نوع نهاد دیجیتالی باشد (معمولاً از آن به Honeytokn یاد می شود) که هیچ ارزش واقعی ندارد. برای مثال، یک بیمارستان می تواند مجموعه ای نادرست از رکوردهای اطلاعاتی بیماران ایجاد نماید. از آنجا که این رکوردها Honeypot هستند، هیچکس نباید به آنها دسترسی پیدا کرده و یا با آنها تعامل برقرار کند. این رکوردها می توانند در داخل پایگاه داده بیماران این بیمارستان به عنوان یک جزء Honeypot قرار گیرند. اگر یک کارمند یا یک فرد مهاجم برای دسترسی به این رکوردها تلاش نمود، می توان اقدام وی را به عنوان نشانه ای از یک فعالیت غیر مجاز تلقی کرد، چرا که هیچکس نباید از این رکوردها استفاده کند. اگر شخصی

یا چیزی به این رکوردها دسترسی پیدا کند، یک پیغام هشدار صادر می شود. این ایده ی ساده پشت Honeypot هاست که آنها را ارزشمند می کند.

دو یا چند Honeypot که در یک شبکه قرار گرفته باشند، یک HoneyNet را تشکیل می دهند. نوعاً در شبکه های بزرگ تر و متنوع تر که یک Honeypot به تنهایی برای نظارت بر شبکه کافی نیست، از HoneyNet استفاده می کنند. HoneyNet ها معمولاً به عنوان بخشی از یک سیستم بزرگ تشخیص نفوذ پیاده سازی می شوند. در حقیقت HoneyNet یک شبکه از Honeypot های با تعامل بالاست که طوری تنظیم شده است که تمامی فعالیتها و تعاملها با این شبکه، کنترل و ثبت می شود.

مزایای استفاده از Honeypot

- Honeypot ها صرفاً مجموعه های کوچکی از داده ها را جمع آوری می کنند. Honeypot ها فقط زمانی که کسی یا چیزی با آنها ارتباط برقرار کند داده ها را جمع آوری می نمایند، در نتیجه صرفاً مجموعه های بسیار کوچکی از داده ها را جمع می کنند، که البته این داده ها بسیار ارزشمندند. سازمانهایی که هزاران پیغام هشدار را در هر روز ثبت می کنند، با استفاده از Honeypot ها ممکن است فقط صد پیغام هشدار را ثبت نمایند. این موضوع باعث می شود که مدیریت و تحلیل داده های جمع آوری شده توسط Honeypot ها بسیار ساده تر باشد.
- Honeypot ها موارد خطاهای تشخیص اشتباه را کاهش می دهند. یکی از مهمترین چالشهای اغلب سیستمهای تشخیصی این است که پیغامهای هشدار دهنده خطای زیادی تولید کرده و در موارد زیادی، این پیغامهای هشدار دهنده واقعاً نشان دهنده وقوع هیچ خطری نیستند. یعنی در حالی یک رویداد را تهدید تشخیص می دهند که در حقیقت تهدیدی در کار نیست. هر چه احتمال این تشخیص اشتباه بیشتر باشد، تکنولوژی تشخیص دهنده بی فایده تر می شود. Honeypot ها به طور قابل توجهی درصد این تشخیصهای اشتباه را کاهش می دهند، چرا که تقریباً هر فعالیت مرتبط با Honeypot ها به طور پیش فرض غیر مجاز تعریف شده است. به همین دلیل Honeypot ها در تشخیص حملات بسیار موثرند.

- Honeypot ها می توانند حملات ناشناخته را تشخیص دهند. چالش دیگری که در تکنولوژیهای تشخیصی معمول وجود دارد این است که آنها معمولا حملات ناشناخته را تشخیص نمی دهند. این یک تفاوت بسیار حیاتی و مهم بین Honeypot ها و تکنولوژیهای امنیت کامپیوتری معمولی است که بر اساس امضاهای شناخته شده یا داده های آماری تشخیص می دهند. تکنولوژیهای تشخیصی مبتنی بر امضا، در تعریف به این معنا هستند که ابتدا باید هر حمله ای حداقل یک بار انجام شده و امضای آن شناسایی گردد و سپس با استفاده از آن امضا، در موارد بعدی شناخته شود. تشخیص مبتنی بر داده های آماری نیز از خطاهای آماری رنج می برد. Honeypot ها طوری طراحی شده اند که حملات جدید را نیز شناسایی و کشف می کنند. چرا که هر فعالیتی در ارتباط با Honeypot ها غیر معمول شناخته شده و در نتیجه حملات جدید را نیز معرفی می کند.
- هانی پات ها فعالیتهای رمز شده را نیز کشف می کنند. حتی اگر یک حمله رمز شده باشد، Honeypot ها می توانند این فعالیت را کشف کنند. به تدریج که تعداد بیشتری از سازمانها از پروتکلهای رمزگذاری مانند SSH، IPsec و SSL استفاده می کنند، این مساله بیشتر خود را نشان می دهد. Honeypot ها می توانند این کار را انجام دهند، چرا که حملات رمز شده با Honeypot به عنوان یک نقطه انتهایی ارتباط، تعامل برقرار می کنند و این فعالیت توسط Honeypot رمز گشایی می شود.
- Honeypot با IPv6 کار می کند. اغلب Honeypot ها صرف نظر از پروتکل IP از جمله IPv6، در هر محیط IP کار می کنند. IPv6 یک استاندارد جدید پروتکل اینترنت (IP) است که بسیاری از سازمانها در بسیاری از کشورها از آن استفاده می کنند. بسیاری از تکنولوژیهای فعلی مانند فایروالها و سنسورهای سیستم تشخیص نفوذ به خوبی با IPv6 سازگار نشده اند.
- Honeypot ها بسیار انعطاف پذیرند. Honeypot ها بسیار انعطاف پذیرند و می توانند در محیطهای مختلفی مورد استفاده قرار گیرند. همین قابلیت انعطاف پذیر Honeypot هاست که به آنها اجازه می دهد کاری را انجام دهند که تعداد بسیار کمی از تکنولوژیها می توانند انجام دهند: جمع آوری اطلاعات ارزشمند به خصوص بر علیه حملات داخلی.

- Honeypot ها به حداقل منابع نیاز دارند. حتی در بزرگترین شبکه ها، Honeypot ها به حداقل منابع احتیاج دارند. یک کامپیوتر پنتیوم قدیمی و ساده می تواند میلیونها آدرس IP یا یک شبکه بسیار بزرگ را نظارت نماید.

برای اینکه خیال خود را راحت کنید و یک هانی پات مناسب داشته باشید با دوستان خود در وایا تماس بگیرید

هانی پات HONEYPOT

هانی پات یک ابزار امنیتی است و نقشی ضروری در امنیت سازمانها، بسیار بیشتر از Firewall و IPS ایفا می کند. هانی پات با هویتی نفوذپذیر به وظایف خود می پردازد.

برای مطالعه HoneyPot و بررسی تأثیر شگفت انگیز استفاده از آن در امنیت شبکه سازمان. به مقاله "HoneyPot چیست؟" مراجعه فرمایید.

دوستان شما در وایا آماده پاسخگویی و ارائه خدمت مشاوره در مورد بکارگیری و پیاده سازی

هانی پات می باشند.

دفتر مرکزی:
۰۲۱ ۴۴۲ ۳۱۱ ۴۷

دفتر قزوین:
۰۲۸۱ ۳۳۵ ۹۶ ۷۰

www.vaya.ir
info@vaya.ir



منابع:

- Mastering VMware vSphere 5-1
- VMware.vSphere.For.Dummies
- www.vaya.ir
- www.certcc.ir
- www.vmware.com
- www.wikipedia.com
- www.webhostingtalk.ir
- کتاب الکترونیکی مجازی سازی ترجمه محمد جواد اسماعیلی



با ما در تماس باشید:
www.vaya.ir/newsletter
newsletter@vaya.ir
(021) 442 311 47



VAYA CO.
Information Security Solutions
www.vaya.ir