



مجازی‌سازی یکی از روش‌های عملی، به نسبت جدید و محبوب برای مدیریت مراکز داده است. برپایی مراکز داده مجازی در قلب نمونه‌های فیزیکی، مزایای متعددی دارد. می‌توان چندین سرور مجازی را روی یک سخت‌افزار پیاده کرد که در این صورت، هزینه‌های مربوط به سخت‌افزار به‌طور قابل‌توجهی کاهش می‌یابند. در صورت از کار افتادن یک سرور، کافی است ماشین مجازی را دوباره پیاده‌سازی کنیم و به پیکربندی سخت‌افزاری نیازی نخواهد بود. در نتیجه زمان از دست رفتن سرویس بسیار کوتاه می‌شود. از دیگر مزایای این روش امکان پیاده‌سازی ماشین‌های مجازی با وظایف مختلف و مهاجرت آن‌ها به ابر است. در ادامه گفت‌وگویی انجام‌شده از نظریه‌های دو تن از کارشناسان این حوزه را می‌خوانید. به‌منظور پیوستگی مطالب و ساده‌تر شدن مطالعه، متن اصلی اندکی تغییر داده‌شده و از حالت گفت‌وگو در آمده است.

تفاوت‌ها با گذشته

از حدود بیست سال پیش که شرکت VMware محصول ایستگاه‌کاری خود و ابزار **مجازی‌سازی ESX** را معرفی کرد تا به امروز، اصول اولیه **مجازی‌سازی** تغییر چندانی نکرده است. امروزه، شاهد افزایش کارایی، به‌ویژه افزایش تقاضا برای ذخیره‌سازی هستیم. شاید از مهم‌ترین تحولات این حوزه بتوان به تحول در نحوه مدیریت مجازی‌سازی، شبکه‌ها و مهاجرت **ماشین‌های مجازی** اشاره کرد. در روزهای آغازین پیدایش ماشین‌های مجازی، این ماشین‌ها در یک سرور فیزیکی محصور بودند. یک سرور فیزیکی را مجازی‌سازی می‌کردید و چندین **ماشین مجازی** داشتید که فقط روی همان سرور کار می‌کردند و امکان انتقال آن‌ها به سرورهای دیگر وجود نداشت. در نتیجه اگر سرور فیزیکی با نقصی روبه‌رو می‌شد، عملکرد همه ماشین‌های مجازی روی آن سرور هم با مشکل مواجه می‌شدند و شما راهی برای نجات دادن خدمات خود نداشتید. با معرفی محصولات نظیر vMotion این امکان فراهم شد که در مواقع لزوم، ماشین‌های مجازی به‌سادگی بین سرورهای فیزیکی مهاجرت کنند. با کمک vMotion شرکت VMware یا ابزار Replica در Hyper-V می‌توان ماشین‌های مجازی را تقریباً به‌طور آبی به کلاسترهای مجزا در مکان‌هایی که به‌طور فیزیکی از هم جدا هستند، منتقل کرد.

نگرانی‌ها و امنیت

امنیت **مجازی‌سازی** و خطرات اجرای هم‌زمان چندین **ماشین مجازی** در یک زیرساخت فیزیکی مشترک شاید مهم‌ترین چالش‌هایی هستند که در آغاز پیدایش روش‌های **مجازی‌سازی** به آن‌ها توجهی نشده یا کمتر توجه شده بود. اگرچه، امروزه آسیب‌پذیری‌های امنیتی برای مثال در معماری پردازنده‌های مرکزی وجود دارد، با این حال بسته‌های الحاقی برای رفع این نقایص سخت‌افزاری به‌سرعت عرضه می‌شوند. در نتیجه مهاجمان به‌راحتی نمی‌توانند از این آسیب‌پذیری‌ها سوءاستفاده کنند و برای انجام حملات مؤثر به **ماشین‌های مجازی**، نیازمند دسترسی سطح بالا به خود سامانه‌ها هستند. به‌طورکلی این‌زوله‌کردن منابع و **ماشین مجازی**، سطح ایمنی را بسیار بالا می‌برد اما

مشکلات از جایی آغاز می‌شود که این ایزوله‌سازی به‌طور نامناسبی پیاده شده باشد. یک محیط مجازی که به‌درستی طراحی شده و با ایزوله کردن شبکه و ایزوله کردن فضای ذخیره‌سازی (در صورت نیاز) همراه باشد، از ایمنی بالایی در حملات برخوردار است.

Peter Rittwage، مهندس فنی ارشد شرکت IntelliSystems معتقد است: «همیشه از وپروس‌ها و بدافزارهایی سخن گفته می‌شود که می‌توانند به هاپیروایزر حمله کنند. من به‌شخصه تاکنون با چنین چیزی مواجه نشده‌ام. به نظر من برنامه‌ریزی چنین چیزی بسیار دشوار است.»

ابزارهای مجازی‌سازی

در بیشتر موارد برای **مجازی‌سازی**، نام ابزارهای Hyper-V و VMware یا KVM/Xen مطرح است. یکی از مهم‌ترین پارامترها برای انتخاب ابزار **مجازی‌سازی** علاوه بر کارایی، هزینه‌ای است که می‌خواهید صرف کنید. این طیف هزینه بازه‌ای متنوع را شامل می‌شود که یکسر آن KVM/Xen قرار دارد و بعد Hyper-V است و در نهایت VMware قرار گرفته که گران‌ترین گزینه محسوب می‌شود. VMware ابزارهای مدیریت فوق‌العاده‌ای دارد و یک شاهکار در عرصه **مجازی‌سازی** سخت‌افزاری محسوب می‌شود، اما استفاده از آن بسیار گران است. اگر از محیط ویندوزی استفاده می‌کنید و اغلب ماشین‌های مهمان، ویندوز سرور را اجرا می‌کنند در این صورت محیط Hyper-V انتخاب خوبی برای شما خواهد بود. KVM و Xen هر دو پلتفرم‌های هاپیروایزر اپن‌سورس فوق‌العاده‌ای محسوب می‌شوند، اما فاقد رابط‌های مدیریتی هستند. اگرچه برای رفع این مشکل راهکارهایی چون استفاده از محیط‌هایی نظیر OpenStack یا استفاده از ابزاری نظیر OnApp وجود دارد، اما با این وجود اگر تجربه کافی برای استفاده از این ابزارها و نرم‌افزارهای اپن‌سورس نداشته باشید، چنین راهکارهایی سبب پیچیدگی بیشتر طراحی می‌شوند و کمک چندانی به شما نخواهند کرد.

مطلب پیشنهادی



در مجازی‌سازی مایکروسافت موفق‌تر است یا VMware؟
مقایسه دو محصول مجازی‌ساز VSphere و Hyper-V

مجازی‌سازی در چه جاهایی مفید است؟

اگرچه امکان **مجازی‌سازی** اغلب در بارهای کاری وجود دارد اما اگر نرم‌افزارهایی دارید که به‌طور انحصاری از پردازنده مرکزی، رم یا I/O ذخیره‌سازی استفاده سنگینی می‌کنند، شاید بهترین راهکار این باشد که چنین نرم‌افزارهایی را در قالب سرورهای مستقل، درون یک محیط **مجازی‌سازی** شده بزرگ‌تر قرار دهید. همچنین می‌توانید یک سرور فیزیکی را به‌گونه‌ای پیکربندی کنید که فقط یک ماشین مجازی را اجرا کند و به این ترتیب علاوه بر این‌که مطمئن خواهید بود نرم‌افزار موردنظرتان از نظر دسترسی به منابع سخت‌افزاری در شرایط خوبی است، از مزایای یک محیط مجازی‌سازی شده نظیر امکانات مدیریتی و مهاجرت بارکاری بهره‌مند خواهید شد. با این اوصاف باید توجه داشت که همه نرم‌افزارها به‌راحتی با پردازنده‌های مجازی و NIC های مجازی کنار نمی‌آیند، زیرا به‌گونه‌ای طراحی شده‌اند که با سخت‌افزار فیزیکی ارتباط برقرار کنند. اما خبر خوب این است که با رشد بازار **مجازی‌سازی**، این نرم‌افزارها مسیر تکامل را طی می‌کنند و در آینده با مشکلات کمتری در این زمینه روبرو خواهیم شد. به‌طورکلی اگر قصد دارید از همه منابع خود برای یک عملکرد خاص (High-CPU Or High-IOP Function) نظیر پیاده‌سازی یک سرور SQL که بار زیادی را تحمل می‌کند، استفاده کنید به مجازی‌سازی نیاز چندانی ندارید. مجازی‌سازی در مواردی کمک می‌کند که بخواهیم سخت‌افزار را بین چندین مأموریت به اشتراک بگذاریم.

بزرگ‌ترین چالش مجازی‌سازی

هنوز هم بزرگ‌ترین چالش **مجازی‌سازی**، توزیع و به اشتراک‌گذاری منابع بین زیرساخت و نرم‌افزارها است. در هر حالتی در زیرساخت شما مواردی وجود خواهند داشت که اولویت بیشتری نسبت به بقیه دارند. طراحی یک پلتفرم **مجازی‌سازی** شده در واقع ایجاد یک نوع تعادل و موازنه بین منابع پردازشی است که در اختیار دارید. در هر صورت شما ممکن است در بخش‌هایی از زیرساخت خود با گلوگاه‌هایی روبرو شوید که اثر منفی بر عملکرد آن داشته باشند، اما این امید وجود دارد که بتوانید در طراحی خود شرایطی را لحاظ کنید که این گلوگاه‌ها اثر منفی

کمتری بر عملکرد نرم‌افزارهایتان بگذارند. همیشه باید تخمینی از بارکاری آینده داشته باشید، چون نمی‌توانید به راحتی شبکه‌ای را که برپا کرده‌اید با یک محیط مجازی‌سازی شده جدید وفق دهید. در بخش ذخیره‌سازی هم باید به نکات مهمی توجه داشت. در اغلب پیاده‌سازی‌ها یک آرایه ذخیره‌سازی مرکزی برای محیط مجازی‌سازی شده در نظر گرفته می‌شود و در بیشتر موارد، یک گلوگاه را به سامانه مجازی‌سازی تحمیل می‌کند.



راهکارهای پیشنهادی

در حالی که راهکارهای فنی وجود دارد که می‌توانند به کاهش برخی از این مشکلات کمک کنند، نظیر SSD caching درون آرایه ذخیره‌سازی یا استفاده از ذخیره‌سازی خوشه‌ای (Clustered Storage) با این حال، هر یک از این راهکارها ایرادهای خود را دارند که باید به آن‌ها توجه داشت. یکی از بهترین راه‌ها برای کاهش مشکلات، ارزیابی (Benchmarking) دقیق سرورهای فیزیکی موجود و انتخاب درست روشی است که برای مجازی‌سازی زیرساخت خود در پیش خواهید گرفت. پیش از هرگونه تصمیم‌گیری در مورد سخت‌افزار یا مجازی‌سازی، باید از میزان پهنای باندی که هر سرور برای تبادل داده در WAN مصرف خواهد کرد، میزان درگیر شدن پردازنده مرکزی و حافظه در جریان بار کاری معمول و در پیک بار و همین‌طور از میزان disk I/O که هر سرور با آن مواجه است، آگاهی داشته باشید. با در اختیار داشتن چنین اطلاعاتی پیش از پیاده‌سازی، می‌توانید تصمیمات دقیق‌تری اتخاذ کنید. علاوه بر این قادر خواهید بود، خطاها و نقایص احتمالی را که ممکن است در محیط مجازی‌سازی شده رخ دهند، پیش‌بینی کنید و مطمئن باشید که در صورت بروز مشکل برای یک هایپروایزر فیزیکی، منابع پشتیبان کافی وجود دارد تا بتوانید ماشین‌های مجازی را به سلامت مهاجرت دهید.

مطلب پیشنهادی



ورود به دنیای مجازی‌سازی با سطح بالایی از مهارت‌ها
۵ گواهینامه برتر مجازی‌سازی

اشتباه‌های معمول در مجازی‌سازی

از جمله اشتباه‌های طراحی می‌توان به «تخصیص نامتوازن منابع» اشاره کرد. چیزی شبیه استفاده از ۲۴ هسته

پردازشی با ۶۴ گیگابایت حافظه. در یک محیط مجازی‌سازی شده، حافظه (RAM) بین ماشین‌های مجازی به اشتراک گذاشته نمی‌شود و در نتیجه ممکن است منابع حافظه زودتر از منابع پردازشی به پایان برسند. عدم تناسب توان ذخیره‌سازی با نیازها مورد دیگری است که باید به آن توجه کرد. برآورد دقیق ظرفیت ذخیره‌سازی شاید اهمیتی بیشتر از برآورد ظرفیت پردازشی داشته باشد زیرا هزینه‌های مربوط به ذخیره‌سازی در مقایسه با هزینه هسته‌های پردازشی با سرعت بیشتری افزایش می‌یابد. اگر شمار زیادی از پایگاه‌های داده را با تراکنش بالا دارید و می‌خواهید آن‌ها را مجازی‌سازی کنید، به disk I/O زیادی نیاز خواهید داشت و این یعنی نیاز به آرایه بزرگی از دیسک‌ها که مترادف است با تحمیل هزینه زیاد.

علاوه بر این، معمولاً همیشه محیط‌های مجازی را خواهید دید که در آن‌ها برای هر ماشین مجازی مهمان، VLAN با مدیریت آدرس IP گره‌های پروایزر برای هر کدام در نظر گرفته شده است. به‌طور کلی چنین کاری لزومی ندارد و فقط بر میزان پیچیدگی مدیریت پلتفرم می‌افزاید. به‌جز در موارد خیلی خاص تا جای ممکن از حجم شبکه بکاهد و برای مدیریت جداسازی

(Separation) ماشین‌های مجازی روی شبکه از فهرست‌های دسترسی یا قوانین دیواره‌آتش (Firewall) استفاده کنید. همین‌طور در مجازی‌سازی‌ها شاهد استفاده زیاد از سویچ‌های مجازی هستیم که شاید لزومی به استفاده از این تعداد سویچ نباشد. اگر محیط به تعداد زیادی VLAN نیاز دارد، معمولاً برای هر VLAN به سویچ مجازی مجزا نیاز ندارید و در بیشتر موارد یک طراحی مناسب VLAN و سویچ‌های مجازی، میزان کافی از ایزولاسیون شبکه را در اختیاران قرار می‌دهد. پیکربندی نامناسب پردازنده مجازی، حافظه و فضای ذخیره‌سازی از جمله اشتباه‌های رایج در مجازی‌سازی است.

نگاهی به آینده

در آینده شاهد مجازی‌سازی شبکه روی سخت‌افزار شبکه خواهیم بود و در نتیجه زیرساخت فیزیکی شبکه که باید از زیرساخت مجازی که برپا کرده‌اید پشتیبانی کند، به‌طور مناسب‌تری با SDN و Scripting و vxLAN هماهنگ خواهد شد. مورد دیگر افزایش استفاده از Containerization درون ماشین‌های مجازی است. محصولات نظیر Docker و Kubernetes مجازی‌سازی سیستم‌عامل و نرم‌افزار را در درون خود ماشین مجازی فراهم می‌کنند. استفاده درست از چنین امکانی مزایای زیادی نظیر پیاده‌سازی سریع‌تر، در اختیار داشتن محیطی با ثبات‌تر و توانایی انتقال بی‌درنگ بارکاری نرم‌افزارها بین ماشین‌های مجازی دارد. پیشنهادها، برای افرادی که قصد پیاده‌سازی و نگهداری از پروژه‌های مجازی‌سازی سرور را دارند، برنامه‌ریزی برای رشد باشد. در طول مرحله طراحی، پس از ارزیابی محیط فعلی، مطمئن شوید که برنامه‌های مناسب برای توسعه پلتفرم یا هایپروایزرهای جدید یا زیرساخت ذخیره‌سازی اضافی دارید، به‌گونه‌ای که تأثیر این تغییرات را روی محیط مجازی‌سازی شده فعلی تا حد امکان کاهش دهید. در محیط‌های مجازی، تقاضای زیادی به دسترسی بالا وجود دارد، پس باید بتوانید برای پاسخ به این تقاضا، بدون این‌که مجبور به بازتعریف معماری کل پلتفرم شوید، ظرفیت ذخیره‌سازی یا شمار هایپروایزرها را افزایش دهید. علاوه بر این، باید یک استراتژی پشتیبان‌گیری خوب در چنته داشته باشید. اگر چه با مجازی‌سازی همه‌چیز، در مقابل خطا و نقص یک جزء فیزیکی زیرساخت، به انعطاف‌پذیری بهتری دست خواهیم یافت با این حال همیشه باید در انتظار بروز مشکل بود.

منبع:

نشانی منبع:

<https://www.shabakeh-mag.com/cover-story/15718/%D9%85%D8%AC%D8%A7%D8%B2%DB%8C%E2%80%8C%D8%B3%D8%A7%D8%B2%DB%8C-%D8%B3%D8%B1%D9%88%D8%B1%D8%8C-%D8%A8%D9%87%D8%AA%D8%B1%DB%8C%D9%86-%D8%A7%D9%84%DA%AF%D9%88%D9%87%D8%A7-%D9%88-%D8%A8%D8%AF%D8%AA%D8%B1%DB%8C%D9%86-%D8%A7%D8%B4%D8%AA%D8%A8%D8%A7%D9%87%E2%80%8C%E2%80%8C%D9%87%D8%A>