چگونه از ماشین‌های مجازی به شکل ایمن در ویندوز سرور 2019 استفاده کنیم؟

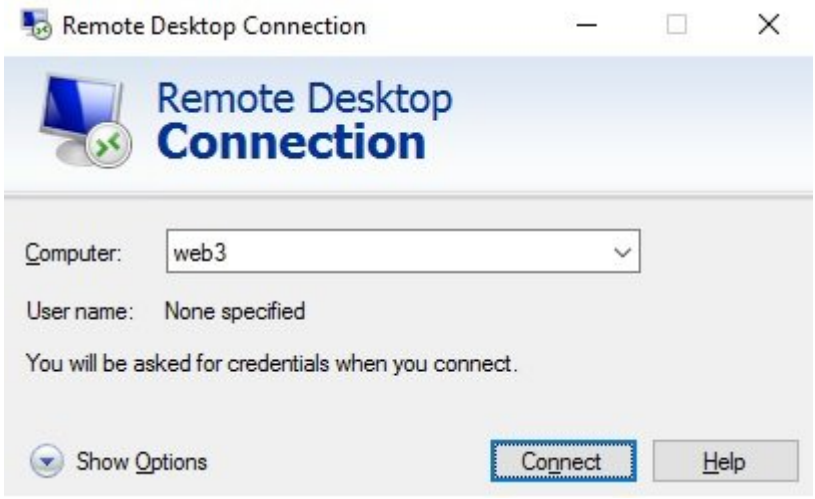
در آخرین شماره از آموزش ویندوز سرور 2019 به سراغ مباحث تکمیلی مجازی‌سازی، ماشین‌های مجازی محافظت شده، میزبان‌های محافظت شده و محصول Hyper-V 2019 خواهیم رفت.

بخش پایانی - برای مطالعه قسمت قبل آموزش رایگان **ویندوز سرور 2019 اینجا** کلیک کنید.

کنسول Hyper-V، پروتکل دسکتاپ از راه دور (RDP) و پاورشل

در حالی که تنظیمات سخت‌افزاری ماشین‌های مجازی باید از طریق Hyper-V Manager پیکربندی شود، اما تعامل روزانه شما با این ماشین‌های مجازی به عنوان سرورهای در حال اجرا در محیط واقعی انجام می‌شود و ضرورتی ندارد به سرور Hyper-V مراجعه کنید. با این حال، Hyper-V Manager ابزای به‌نام Hyper-V Console دارد که گزینه‌ای به‌نام Connect در اختیار کاربر قرار می‌دهد. گزینه فوق اجازه می‌دهد به سرعت و سادگی با کنسول سرورها ارتباط برقرار کنید. دسترسی به سرورها به روش فوق زمانی مفید است که بخواهید موضوعاتی را در بایوس یا اطلاعاتی که خارج از سیستم‌عامل ویندوز قرار دارند و روی ماشین مجازی در حال اجرا هستند را مشاهده کنید. در چنین شرایطی به این سطح از دسترسی به کنسول نیاز دارید.

هنگامی که سرورهای ویندوز را به عنوان ماشین‌های مجازی به خدمت می‌گیرید، تعامل با این سرورها به همان روشی انجام می‌شود که با سرورهای فیزیکی در شبکه ارتباط برقرار می‌کنید و از پروتکل RDP برای برقراری ارتباط با سرور استفاده کنید. اگر سرور خود را روی ماشین مجازی نصب کرده‌اید (در این‌جا سرور مجازی من WEB3 نام دارد و ویژگی RDP را روی آن فعال کرده‌ام)، دلیلی وجود ندارد که MSTSC را باز نکنید و به سرور مجازی از طریق دسکتاپ خود وارد نشوید.



همین قاعده در ارتباط با پاورشل یا هر روش سنتی دیگری که برای اتصال از راه دور به سرور از آن استفاده می‌کنید صدق می‌کند. از آن‌جایی که ماشین مجازی کاملاً آنلاین است و سیستم‌عامل سرور روی آن نصب شده، می‌توانم از PowerShell Remoting برای اعمال تغییرات روی سرور مجازی (WEB3) خود استفاده کنم یا از یک سرور یا کامپیوتر شخصی دیگری برای این‌کار استفاده کنم. پس از آن‌که سخت‌افزار خود را آماده و سیستم‌عامل را روی ماشین مجازی نصب کردید، به ندرت احتیاج پیدا می‌کنید به کنسول Hyper-V به منظور تعامل با سرور وارد شوید. دلایل اصلی باز کردن Hyper-V Manager برای دستیابی به ماشین مجازی این است که تغییراتی در سطح سخت‌افزار روی سرور اعمال کنید، مواردی همچون اضافه کردن هارد دیسک، تنظیم حافظه اصلی یا انتقال اتصال شبکه از یک سوئیچ به دیگری از جمله این موارد است.

مرکز مدیریت ویندوز (WAC)

ما WAC را در سراسر این آموزش به صورت پراکنده استفاده کردیم. WAC ابزاری فوق‌العاده جدید است که مایکروسافت می‌خواهد مدیران سرور برای تعامل و مدیریت هر جنبه از سرورهای خود از آن استفاده کنند. سرورهای ماشین مجازی میزبانی شده در Hyper-V از این قاعده مستثنا نیستند. شما می‌توانید از ابزارهای WAC برای مدیریت سرورهای مجازی و واقعی به یک شکل استفاده کنید.

ماشین‌های مجازی محافظت شده

اگر شغل روزانه شما ارتباطی با Hyper-V ندارد، ممکن است هیچ‌گاه اصطلاح ماشین‌های مجازی محافظت شده به گوش‌تان نخورده باشد. این اصطلاح به خوبی عملکرد این ماشین‌های را شرح می‌دهد. یک ماشین مجازی محافظت شده به نوع خاصی از ماشین‌های اشاره دارد که توسط الگوریتم‌ها رمزگذاری شده‌اند و تنها فایل دیسک سخت (VHDX) با استفاده از BitLocker رمزگذاری نشده است. به نظر می‌رسد به‌کارگیری راه‌کار فوق ساده است، اما راهکار فوق تنها زمانی که برخی از پیش‌نیازها وجود داشته باشد تحقق می‌یابد. برای اینکه رمزگذاری BitLocker به درستی کار کند، ماشین مجازی به یک تراشه مجازی (Platform Trusted Platform (TPM نیاز دارد.. TPMها به سرعت به یکی از مولفه‌های سخت‌افزاری دنیای فناوری تبدیل شده‌اند، اما به‌کارگیری آن‌ها توسط بیشتر مدیران شبیه به یک فناوری عجیب‌وغریب است. ماشین‌های مجازی محافظت شده می‌توانند قفل شوند تا فقط در محیط‌های سالم استفاده شوند. راهکار فوق به میزان قابل توجهی امنیت را بهبود می‌بخشد.

برای آن‌که با عملکرد ماشین مجازی محافظت شده بهتر آشنا شویم، اجازه دهید به بررسی وضعیتی بپردازیم که یک ماشین مجازی محافظت نشده استفاده می‌شود. ایده به‌کارگیری ماشین‌های مجازی محافظت شده مهم است، به ویژه زمانی که میزبان در ابر مستقر شده و شما نمی‌توانید از امنیت شرکت ارائه‌دهنده خدمات مطمئن باشید. در چنین شرایطی ممکن است شرکت ارائه‌دهنده خدمات یا حتا دپارتمان فناوری‌اطلاعات که یک ابر خصوصی راه‌اندازی کرده به محتویات درون ماشین مجازی دسترسی پیدا کند.

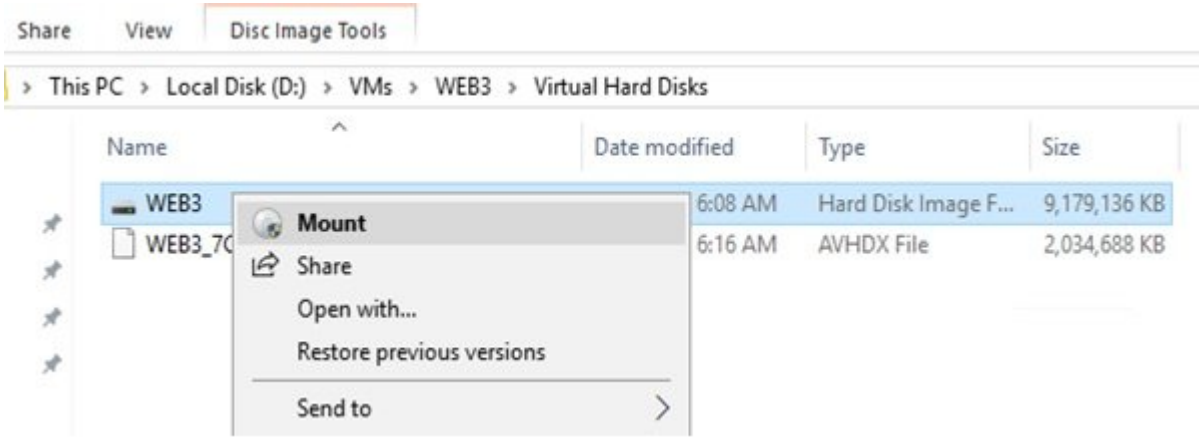
ما یک سرور میزبان Hyper-V را اجرا کردیم و در آن میزبان یک ماشین مجازی به‌نام WEB3 ایجاد کردیم. اجازه دهید حالتی را تصور کنیم که من یک ارائه‌دهنده میزبان ابری هستم و WEB3 وب سرور متعلق به یکی از مشتریان

من است. من برای مشتریان خود یک سوئیچ مجازی خصوصی مستقل برای اتصال به شبکه ایجاد کردم تا آن‌ها بتوانند سرور و شبکه خود را مدیریت کنند. در این حالت من در سطح شبکه به ماشین مجازی مشتریان خود دسترسی ندارم. نکته‌ای که لازم است به آن دقت کنید این است که سرور WEB3 به دامنه و شبکه مستاجران من متصل شده و به عنوان میزبان ابر به اعتبارنامه مربوط به دامنه مشتریان دسترسی ندارم و نمی‌توانم به سرور آن‌ها وارد شوم.

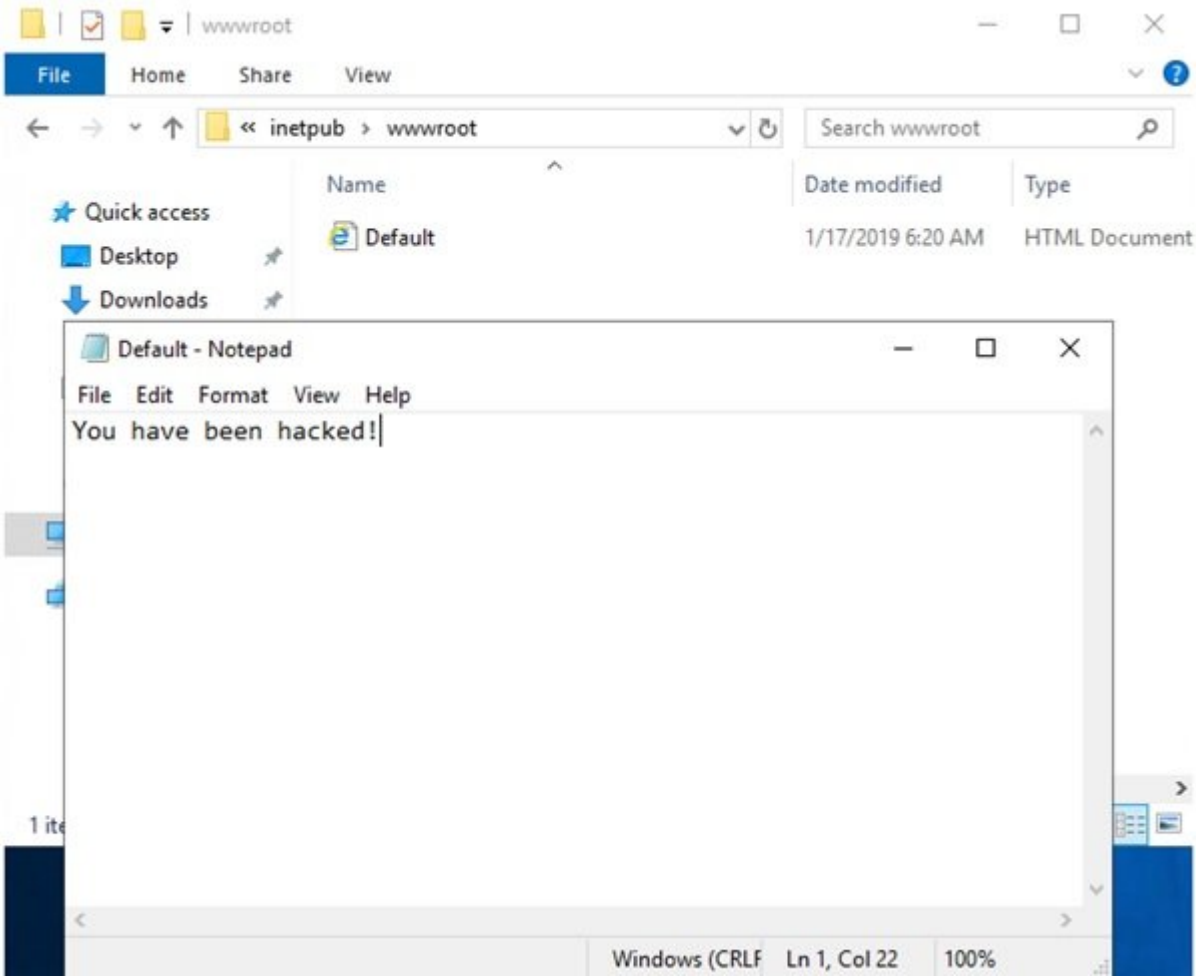
به نظر می‌رسد همه چیز در حالت مطلوب قرار دارد. شما به عنوان مشتری نمی‌خواهید که ارائه‌دهنده ابر بتواند درون ماشینه‌ای مجازی شما که ابر میزبانی می‌شوند را مشاهده کند. شما همچنین نمی‌خواهید مشتریان دیگری که ممکن است ماشین‌های مجازی در همان ابر داشته باشند محتویات سرورهای شما را مشاهده کنند. همین موضوع در ارتباط با ابرهای خصوصی نیز صادق است. اگر شما میزبان یک ابر خصوصی هستید و به شرکت‌های مختلف یا بخش‌های مختلف یک شرکت اجازه می‌دهید ماشین‌های مجازی ایزوله شده را روی فضای ابری شما قرار دهند باید اطمینان حاصل کنید که لایه‌های امنیتی واقعی میان ماشین‌های مجازی مختلف و میان ماشین‌های مجازی و میزبان وجود دارد.

حالا اجازه دهید به سناریو فوق از منظر امنیتی نگاه کنیم. من یک کارمند ارائه‌دهنده خدمات ابری متخلف هستم و تصمیم می‌گیرم پیش از ترک محل کار آسیب‌هایی به سازمان وارد کنم. پاک کردن سرور WEB3 کاملاً راحت است، زیرا من به کنسول مدیریتی میزبان دسترسی دارم. با این حال، حذف ماشین فوق مشکل خاصی به وجود نمی‌آورد، زیرا مشتری ممکن است سرور را دومرتبه ایجاد کند یا سرور را دوباره از نسخه پشتیبان بازگرداند. در سناریو دیگر این کارمند متخلف ممکن است برای خراب کردن ماشین مجازی به سراغ تغییر محتوای سایت‌ها و اطلاعاتی برود که درون ماشین مجازی قرار دارد. کارمند متخلف برای دستکاری وب‌سایت مشتری که روی سرور WEB3 در حال اجرا است نیازی به دسترسی واقعی به ماشین مجازی ندارد، زیرا دسترسی مستقیم به فایل هارد دیسک مجازی دارد. تنها کاری که این فرد باید انجام دهد این است که به آن فایل VHD آسیب وارد کند، وب‌سایت را تغییر دهد و وب‌سایت را با اطلاعاتی که دوست دارد نشان دهد ویرایش کند.

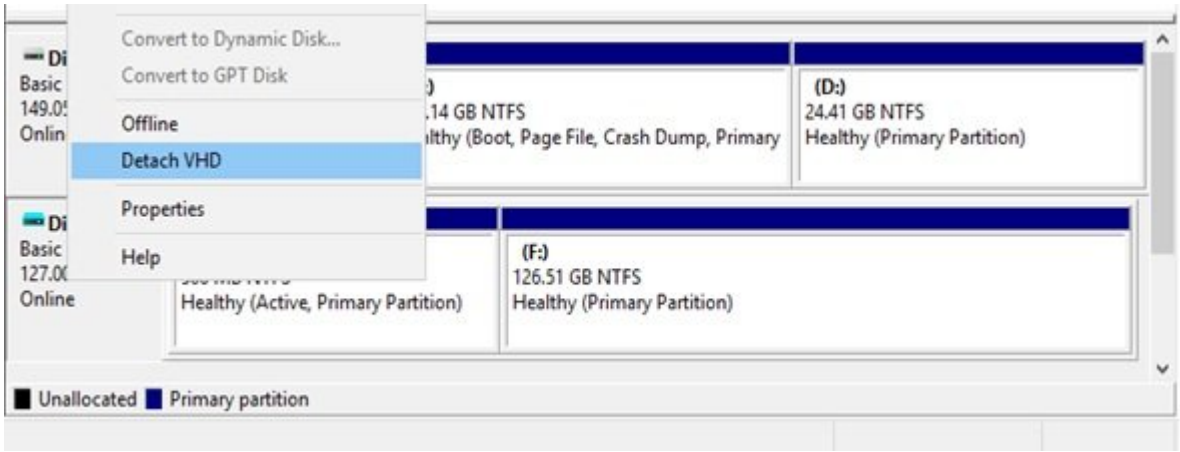
برای این منظور کارمند متخلف ابتدا باید به Hyper-V Server وارد شود و به پوشه‌ای مراجعه کند که فایل VHD مربوط به WEB3 در آن مکان نگه‌داری می‌شود. در این حالت نیازی به اعتبارنامه مشتری نیست. علاوه بر این، مشتری هیچ‌گاه متوجه نخواهد شد که تغییری روی ماشین مجازی او انجام گرفته است. کاربر متخلف به سادگی روی فایل VHD راست‌کلیک کرده و گزینه Mount را انتخاب می‌کند.



اکنون که VHD به شکل مستقیم روی سیستم‌عامل سرور میزبان قرار گرفته، کارمند متخلف می‌تواند هارد دیسک ماشین مجازی را به شکل یکی از درایورهای اصلی سیستم مشاهده کند. این کارمند برای پیدا کردن فایل‌های وب‌سایت به پوشه wwwroot مراجعه می‌کند و صفحه پیش‌فرض را تغییر می‌دهد تا محتوایی که مدنظر قرار دارد نشان داده شود.



وقتی دستکاری فایل‌های سایت به پایان رسید، ابزار Disk Management را باز می‌کند و روی گزینه mounted disk راست‌کلیک کرده و گزینه Detach VHD را انتخاب می‌کند.



در انتها فایل به مکان اصلی باز گردانده می‌شود و تمام. البته می‌توان یک کپی از فایل VHD را روی یک حافظه فلش کپی کرد. با این سناریو مخرب هنوز هم فکر می‌کنید میزبانی ماشین‌های مجازی در ابر به شکل محافظت نشده ایمن است؟ نمونه ذکر شده یک مثال واقعی است که ممکن است در دنیای واقی رخ دهد و به همین دلیل است که برخی از سازمان‌ها تمایلی ندارند تا فعالیت‌های تجاری مهم خود را به فضای ابری متعلق به سازمان‌های مختلف انتقال دهند. خوشبختانه، مایکروسافت با ارائه فناوری جدیدی به‌نام shielded VM این مشکل امنیتی را برطرف کرده است.

رمزگذاری VHDها

مایکروسافت از قبل یک فناوری رمزگذاری عالی درایو به‌نام بیت‌لاکر ارائه کرده است. ماشین‌های مجازی محافظت شده ماشین‌های مجازی Hyper-V هستند که ویژگی رمزگذاری درایو بیت‌لاکر روی آن‌ها فعال شده است. هنگامی که کل فایل VHD با بیت‌لاکر محافظت و رمزگذاری شود، هیچ‌کس نمی‌تواند یک درب پشتی برای دسترسی به درایو ایجاد کند. در این حالت تلاش برای نصب فایل VHD باعث بروز خطای زیر می‌شود:

زیرساخت‌های لازم برای ماشین‌های مجازی محافظت شده

برای دستیابی به ماشین‌های مجازی محافظت به یکسری پیش‌نیازهای لازم نیاز است. یکی از این ملزومات میزبان‌های محافظت شده است. برای ارائه ماشین‌های مجازی محافظت شده به سرورهای میزبانی محافظت شده نیاز دارید. میزبان‌های محافظت شده در حقیقت سرورهای Hyper-V در پوسته هستند. آن‌ها ماشین‌های مجازی را شبیه به سرور Hyper-V میزبانی می‌کنند با این تفاوت که به شکل رمزگذاری شده از ماشین‌های مجازی محافظت شده میزبانی می‌کنند. میزبان‌های مجازی محافظت شده باید روی نسخه ویندوز سرور 2016 یا 2019 اجرا شوند و باید بر مبنای مکانیزم UEFI که شامل تراشه TPM 2.0 است اجرا شوند. البته TPM 2.0 یک الزام نیست، اما پیشنهاد می‌شود. در ادامه به سرویس HGS سرنام Host Guardian Service که روی یک سرور یا یک خوشه از سرورها (حداقل سه سرور) اجرا می‌شود برای تایید اعتبار سرورها نیاز است. زمانی که یک ماشین مجازی محافظت شده روی یک سرور میزبانی محافظت شده اجرا می‌شود، در ادامه سرویس HGS ایمن و مطمئن بودن همه چیز را تضمین می‌کند. سرویس فوق باید روی سرور 2016 یا 2019 اجرا شود. HGS cache قابلیت جدیدی است که مایکروسافت به ویندوز سرور 2019 اضافه کرده است. نسخه قبلی دارای محدودیت‌هایی در ارتباط با ماشین‌های مجازی محافظت شده بود که محدودیت‌های فوق برداشته شده است.

ادغام‌سازی با لینوکس

بسیاری از شرکت‌ها از لینوکس برای انجام برخی از کارها استفاده می‌کنند. برای بهره‌مندی از لینوکس در کنار ویندوز سرور 2019 راهکارهایی به شرح زیر وجود دارد:

اجرای لینوکس در Hyper-V: در گذشته ماشین‌های مجازی روی یک سرور Hyper-V محدود به سیستم‌عامل مبتنی بر ویندوز هستند، اما دیگر این‌گونه نیست. مجازی‌سازی Hyper-V اجازه می‌دهد از ماشین‌های مجازی مبتنی بر لینوکس در Hyper-V Manager استفاده کنید.

لینوکس در ماشین‌های محافظت شده: درباره اجرای ماشین‌های مجازی محافظت شده در Hyper-V به شما گفتیم، اکنون باید بدانید که ماشین‌های مجازی مبتنی بر لینوکس در Hyper-V پشتیبانی می‌شوند. به عبارت دیگر ترکیبی از ماشین‌های مجازی لینوکسی و ویندوزی در دسترس است.

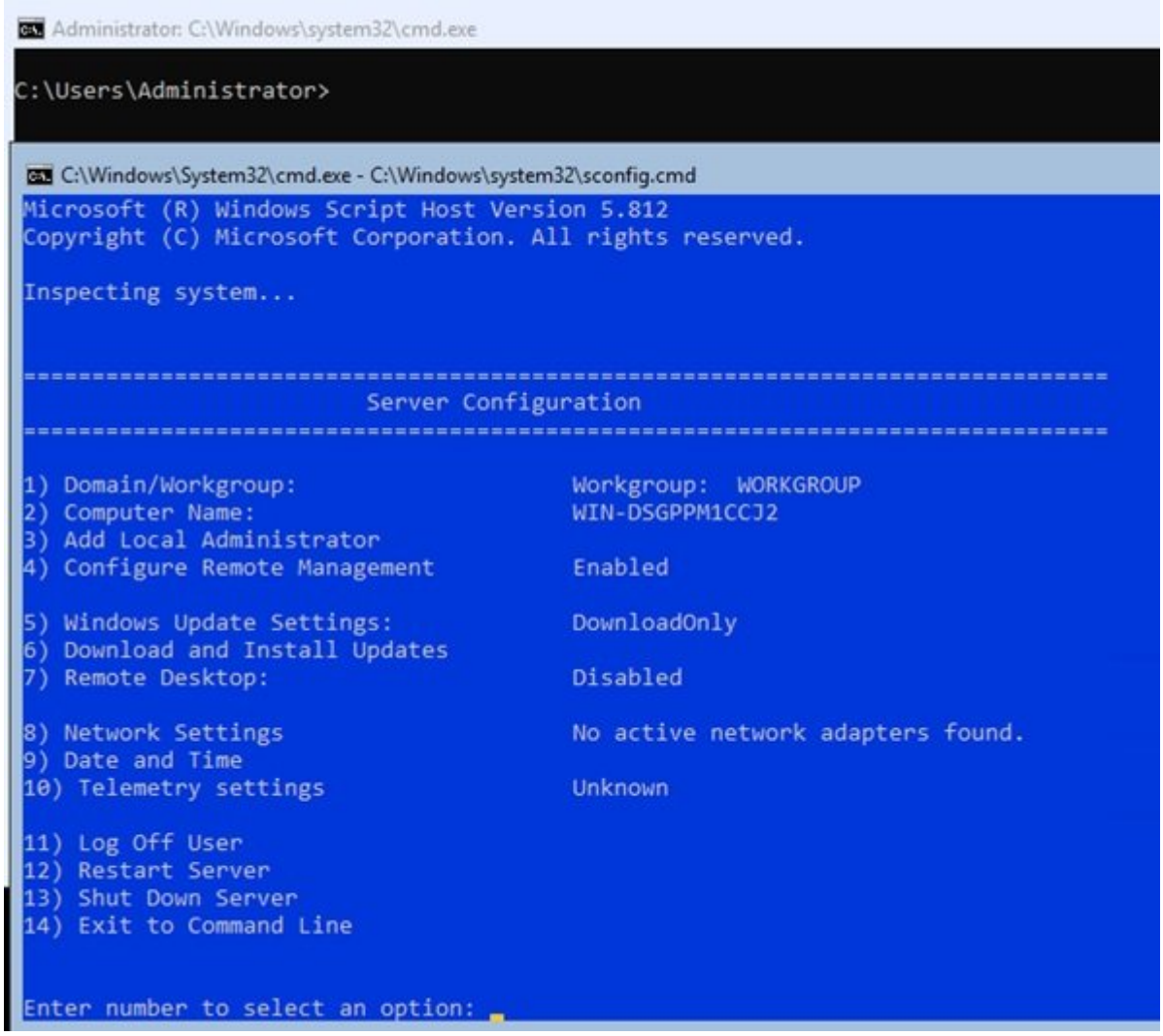
اجرا در کانتینرها: اجرای ظروف: بیشتر سرورها و مدیران Hyper-V برای نصب لینوکس روی سیستم‌های خود مشکلی ندارند، زیرا این فرآیند ساده است، اما دلیل برای انجام این‌کار ندارند. اما در برخی موارد به‌کارگیری لینوکسی به ویژه در بحث دوآپس مهم است. هنگام ساخت برنامه‌های کاربردی گسترش‌پذیر که برای ابر آماده می‌شوند، ما اغلب در مورد اجرای این برنامه‌ها در درون کانتینرها صحبت می‌کنیم. در گذشته، میزبانی کانتینرها روی ویندوز سرور به این معنی بود که خود کانتینر باید ویندوز را اجرا کند. اکنون می‌توانید کانتینر مستقر در لینوکس را بالای ویندوز سرور 2019 میزبانی کنید و به این شکل به انعطاف‌پذیری بالایی در فرآیند توسعه نرم‌افزار دست پیدا کنید.

Hyper-V Server 2019

مجازی‌سازی یک فرآیند هیجان برانگیز است. آماده‌سازی سخت‌افزارها، نصب ویندوز سرور 2019 و اجرای Hyper-V تمام آن کاری است که باید انجام دهید تا صدها یا هزاران ماشین مجازی را میزبانی کنید و به کسب درآمد بپردازید. البته دقت کنید هر ماشین مجازی که ایجاد می‌کنید، مجوز سیستم‌عامل خاص خود را دارد که منطقی است. البته بسته به نوع SKU که برای سیستم‌عامل میزبان استفاده می‌کنید، محدودیتی در ارتباط با میزبان تعداد مشخصی از ماشین‌های مجازی روی Hyper-V Server وجود دارد. به‌طور مثال نسخه Windows Server 2019 Edition Standard به عنوان Hyper-V Server اجازه اجرای دو ماشین مجازی را می‌دهد. واضح است که نسخه Standard Edition SKU به گونه‌ای طراحی نشده که به عنوان Hyper-V Server استفاده شود. نسخه Windows Server 2019 Datacenter Edition محدودیت فوق را ندارد. نسخه Datacenter اجازه اجرای تعداد نامحدودی از ماشین‌های مجازی را می‌دهد.

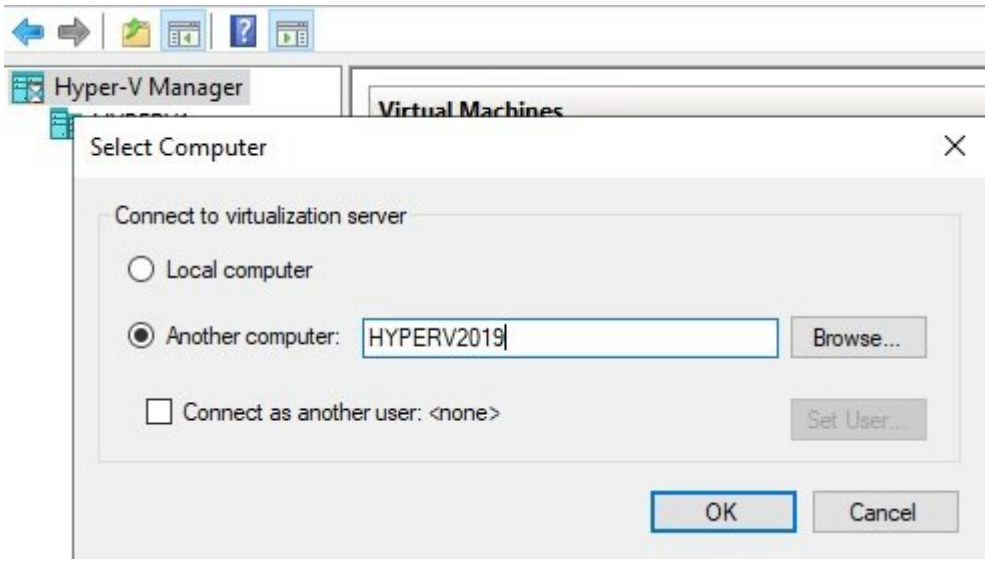
تمامی این صحبت باعث می‌شود تا به سراغ محصولی به‌نام Hyper-V Server 2019 برویم. دقت کنید Hyper-V Server 2019 متفاوت از نقشی است که روی ویندوز سرور 2019 نصب کردید. Hyper-V Server 2019 یک محصول دیگر مایکروسافت است. این نرم‌افزار نصب و راه‌اندازی خاص خود را دارد و یک رابط کاربری کاملاً متفاوت از یک سرور سنتی دارد. نصب Hyper-V Server 2019 روی یک محصول سخت‌افزاری باعث می‌شود تا یک سرور به دست آورید که قادر است تعداد نامحدودی ماشین مجازی Hyper-V را میزبانی کند و کار خاص دیگری انجام نمی‌دهد. شما نمی‌توانید از این محصول به عنوان سرور عمومی استفاده کنید تا سایر نقش‌ها یا خدمات را میزبانی کند. Hyper-V Server همچنین دارای رابط کاربری گرافیکی نیست. Hyper-V Server 2019 یک مزیت بزرگ دارد که رایگان است.

برای استفاده از آن باید ایزو مربوطه به این محصول را دانلود کنید، روی یک دیسک رایت کنید و سپس روی سحت‌افزار نصب کنید. در ادامه فرآیند نصب سیستم‌عامل مشابه با آن چیزی است که ابتدای این آموزش به آن اشاره کردیم. پس از آن‌که کار نصب‌کننده به پایان رسید و به منوی بوت سیستم‌عامل در ویندوز سرور 2019 وارد شدیم، محیط همانند شکل زیر خواهد بود:



ما فقط با یک خطر فرمان همراه با یک ابزار پیکربندی به‌نام SConfig داریم که به‌طور خودکار راه‌اندازی شده است. با استفاده از صفحه‌کلید می‌توانیم کارهایی از قبیل تنظیم نام میزبان این سرور، الصاق به یک دامنه و تغییر تنظیمات شبکه را اعمال کنیم. پس از اتمام استفاده از این رابط متنی برای تنظیم نیازهای اساسی روی سرور و برقراری ارتباط آن با شبکه نیازی به دسترسی مجدد به کنسول Hyper-V Server نداریم، مگر اینکه به دنبال پشتیبان‌گیری یا بررسی مجدد تغییرات باشید. در عوض ، پس از پیکربندی سرور Hyper-V به سادگی از Hyper-V Manager یا PowerShell در یک سرور یا دسکتاپ دیگر متصل به شبکه و به شکل راه دور قادر به مدیریت ماشین‌های مجازی هستیند که درون سرور Hyper-V کار می‌کنند.

در تصویر زیر مشاهده می‌کنید که من Hyper-V Manager را راه‌اندازی کرده‌ام. در این‌جا یک نمونه از Hyper-V Manager را روی یک کامپیوتر مبتنی بر ویندوز 10 که نقش Hyper-V روی آن نصب شده اجرا کردم. در این مکان می‌توانم روی Hyper-V Manager راست‌کلیک کرده و گزینه Connect to Server را انتخاب کنم و نام سرور جدید Hyper-V را وارد کنم و یک کنسول اتصال از راه دور ایجاد کنم. از این اتصال راه دور، می‌توان بر تمامی عملکردهای موجود در Hyper-V Manager از طریق ویندوز 10 مدیریت اعمال کرد.



مشابه با روشی که پیش‌تر در ارتباط با Server Core و Nano Server به کار گرفتیم. Hyper-V Server مزایای زیادی همچون امنیت بالا، میزبانی تعداد نامحدودی ماشین مجازی و حتا کم کردن هزینه‌ها برای مشتریان را به همراه دارد.

کلام آخر

در این سری از آموزش **ویندوز سرور 2019** سعی کردیم، خوانندگان را با سیستم‌عامل تحت شبکه مایکروسافت که روی طیف گسترده‌ای از سرورها و مراکز داده استفاده می‌شود آشنا کنیم و نحوه ساخت و پیکربندی این سیستم‌عامل، الصاق آن به دامنه و مباحثی که هر کارشناس شبکه‌ای به آن نیاز دارید را بررسی کنیم. البته برای تبحر در ویندوز سرور به کار عملی زیاد و مراجعه به منابع مختلف نیاز است تا سطح مهارت‌های فنی بهبود پیدا کند. در این آموزش مجبور شدیم به برخی از عناوین به شکل فهرست‌وار اشاره کنیم تا مطالب کوتاه‌تر شود. امید است این مجموعه سطح دانش فنی خوانندگان را ارتقا داده باشد.

به زودی کتاب الکترونیکی **«آموزش ویندوز سرور 2019»** منتشر می‌شود.

برای مطالعه تمام بخش‌های آموزش **ویندوز سرور 2019** روی لینک زیر کلیک کنید:

آموزش رایگان ویندوز سرور 2019

تاریخ انتشار:
25 دی 1398

نشانی منبع:
https://www.shabakeh-mag.com/networking-technology/16457/%DA%86%DA%AF%D9%88%D9%86%D9%87-%D8%A7%D8%B2-%D9%85%D8%A7%D8%B4%DB%8C%D9%86%E2%80%8C%D9%87%D8%A7%DB%8C-%D9%85%D8%AC%D8%A7%D8%B2%DB%8C-%D8%A8%D9%87-%D8%B4%DA%A9%D9%84-%D8%A7%DB%8C%D9%85%D9%86-%D8%AF%D8%B1-%D9%88%DB%8C%D9%86%D8%AF%D9%88%D8%B2-%D8%B3%D8%B1%D9%88%D8%B1-2019-%D8%A7%D8%B3%D8%AA%D9%81%D8%A7%D8%AF%D9%87-%DA%A9%D9%86%DB%8C%D9%85%D8%9F