متوازن‌سازی بار ترافیک شبکه در ویندوز سرور 2019 چیست و چه کاربردی دارد؟

هنگامی که در حال استفاده از سرورهای خودمان در یک سازمان هستیم، چگونه می‌توانیم برخی ویژگی‌های شگفت‌انگیزی که باعث پایدار شبکه می‌شوند را به زیرساخت خود اضافه کنیم؟ برای پاسخ‌گویی به این پرسش باید با مفاهیم متعادل‌سازی بار شبکه (NLB)، پیکربندی یک وب سایت متعادل شده، Clustering ،Failover clustering tires، تنظیم یک failover clustering و S2D سرنام Storage Spaces Direct آشنا شویم.

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

افزونگی در Windows Server 2019

هر زمان تصمیم می‌گیرید از فناوری جدیدی استفاده کنید، سعی می‌کنید در قالب یک برنامه‌ریزی دقیق آن‌را یا بگیرد و در عمل برای بهبود راندمان کسب‌وکار از آن استفاده کنید. در دنیای سرورها به دنبال آن هستید تا بفهمید به چه سرورهایی نیاز دارید، در کجا باید آن‌ها را قرار دهید و چگونه باید شبکه را برای کارمندان و کاربران پیکربندی کنید. ما در عصری زندگی می‌کنیم که فناوری همیشه در دسترس قرار دارد و عدم دسترسی به فناوری به هیچ عنوان قابل قبول نیست، به ویژه اگر سرویس‌های ابری را میزبانی می‌کنیم. ما باید به هر برنامه یا سرویسی که کاربران ما برای انجام کار خود به آن وابسته هستند حساس باشیم و مطمئن شویم که سرویس ما به شکل تمام وقت در دسترس آن‌ها قرار دارد. برای آن‌که بتوانیم چنین سطحی از دسترسی را ارائه کنیم به قابلیتی به‌نام افزونگی نیاز داریم. جالب است که صحبت کردن درباره افزونگی خیلی ساده‌تر از فکر کردن درباره آن است! ما باید در مورد فناوری‌هایی که از آن‌ها استفاده می‌کنیم بررسی کنیم تا ببینیم آیا فناوری‌ها ویژگی افزونگی را در اختیار ما قرار می‌دهند یا خیر. این آموزش بر مبنای ویندوز سرور 2019 پایه‌ریزی شده، بنابراین فناوری‌هایی که در مورد آن‌ها بحث می‌کنیم، همان‌هایی هستند که می‌توانید در مراکز داده محلی خود، روی سرورهای واقعی (فیزیکی یا مجازی) که وظیفه ساخت و پیکربندی مراکز داده را عهده‌دار دارند استفاده کنید. ابر می‌تواند برخی از گزینه‌های گسترش‌پذیری جادویی و افزونگی را در اختیار ما قرار دهد، بدون آن‌که نیازی به دانستن جزییات داشته باشیم. هنگامی که در حال استفاده از سرورهای خودمان در یک سازمان هستیم، چگونه می‌توانیم برخی ویژگی‌های شگفت‌انگیزی که باعث پایدار شبکه می‌شوند را به زیرساخت خود اضافه کنیم؟ برای پاسخ‌گویی به این پرسش باید با مفاهیم متعادل‌سازی بار شبکه (NLB)، پیکربندی یک وب سایت متعادل شده، Clustering tires ،Failover clustering، تنظیم یک failover clustering و S2D سرنام Storage Spaces Direct آشنا شویم.

متعادل‌سازی بار شبکه (Network Load Balancing)

غالباً ، وقتی به صحبت‌های مردم گوش می‌دهم که درباره سرور خود صحبت می‌کنند، گفت‌وگوها پیرامون یک کلمه

واحد به‌نام خوشه است. به‌طور مثال، اگر ما یک خوشه تنظیم کنیم تا افزونگی را برای سرورها فراهم کند... یا وب‌سایت اصلی ما روی یک خوشه در حال اجرا است..... این سوال به ذهن خطور می‌کند که آیا خوشه‌بندی باید در هر مکانی استفاده شود یا تعریف خاصی برای استفاده از خوشه‌بندی وجود دارد؟ وقتی از جزئیات مربوط به نحوه پیکربندی یک چنین سیستم‌هایی صرفنظر می‌کنیم، متوجه می‌شویم که متعادسازی بار (NLB) روی این سیستم‌ها در حال انجام است. NLB ترافیک را در سطح TCP / IP توزیع می‌کند به این معنی که سیستم‌عامل‌های سرور ممکن است به یکدیگر متکی باشند. این رویکرد باعث به وجود آمدن افزونگی در لایه شبکه می‌شود. متعادل‌سازی بار شبکه در ظاهر کمی گیج‌کننده است، زیرا متعادسازی بار ترافیکی شبکه در مقابل خوشه‌بندی قرار دارد و مایکروسافت گاهی اوقات مفاهیم را در قالب یک خوشه ارائه می‌کند، یک نمونه روشن در این زمینه DirectAccess است. مستندات TechNet می‌گویند، هنگامی که دو یا چند سرور DA با هم در یک آرایه قرار می‌گیرند یک خوشه ایجاد شده است، اما یک failover clustering در جریان نیست. فناوری که در پس‌زمینه در حال اجرا است و اجازه می‌دهد دو گره با یکدیگر ارتباط برقرار کنند Windows NLB است. احتمالاً در بازار سخت‌افزارهای متعادل‌کننده بار ترافیکی نام‌هایی همچونKemp، Cisco، F5 و Barracuda را شنیده‌اید. این شرکت‌ها محصولات سخت‌افزاری اختصاصی را ارائه می‌دهند که می‌توانند ترافیک را به سمت یک نام یا مقصد خاص سوق دهند و ترافیک را میان دو یا چند برنامه سرور تقسیم می‌کنند. درست است که تجهیزات فوق بهترین مکانیزم متعادل‌سازی بار ترافیکی شبکه را ارائه می‌کنند، اما هزینه‌بر هستند و زیرساخت شبکه را پیچیده‌تر می‌کنند. یکی از قابلیت‌های شاخصی که این محصولات ارائه می‌کنند، اما ویژگی از پیش ساخته شده NLB ارائه نمی‌کند در ارتباط با SSL است. این تجهیزات سخت‌افزاری ترافیک وب‌سایت را از کامپیوترهای کلاینت دریافت که اطلاعات را بر مبنای SSL ارسال می‌کنند دریافت کرده و بسته‌ها را رمزگشایی می‌کنند. به این ترتیب وب سرور کار کمتری انجام می‌دهد، زیرا لازم نیست چرخه‌های کاری پردازنده مرکزی را برای رمزگذاری و رمزگشایی اختصاص دهد.

چه نقش‌هایی می‌توانند از NLB استفاده کنند؟

NLB برای برنامه‌های بدون حالت (statless) طراحی شده، به عبارت دیگر برنامه‌هایی که به ارتباطات بلندمدت یا حافظه بلندمدت نیازی ندارند. سرویس‌های وب (IIS) بیشترین منفعت را از افزونگی ارائه شده توسط NLB به دست می‌آورند. پیکربندی NLB آسان است و افزونگی کامل برای وب‌سایت‌هایی که روی ویندوز سرور اجرا می‌شوند ارائه می‌کند، بدون آن‌که هزینه‌های اضافی به وجود آورد. علاوه بر این، NLB می‌تواند برای بهبود عملکرد سرورهای FTP، دیوارهای آتش و پروکسی استفاده شود.

نقش دیگری که قادر است به خوبی با NLB ارتباط برقرار کند، دسترسی از راه دور است. به‌طور خاص، DirectAccess می‌تواند از مولفه NLB ویندوز استفاده کند تا یک مکانیزم دسترسی از راه دور با سرورهای ورودی اضافی را فراهم کند. زمانی که DirectAccess را تنظیم می‌کنید تا از توازن بار استفاده کند، این موضوع به سرعت آشکار نمی‌شود که شما از ویژگی NLB سیستم‌عامل استفاده برای متعادل‌سازی بار استفاده کرده‌اید، زیرا تنظیمات توازن بار از داخل کنسول Remote Access Management و نه کنسول NLB پیکربندی می‌شوند. هنگامی که برای ایجاد تعادل بار از Remote Access Management استفاده می‌کنید، کنسول Remote Access به مکانیسم NLB سیستم‌عامل متصل شده و آن‌را پیکربندی می‌کند به گونه‌ای که الگوریتم‌ها و مکانیزم‌های انتقال بسته‌هایی که توسط DirectAccess استفاده می‌شود، به بهترین شکل ترافیک را میان چند سرور تقسیم می‌کنند.

یکی از برجسته‌ترین ویژگی‌هایی که NLB ارائه می‌کند این است که می‌توانید بدون اینکه روی عملکرد گره‌های موجود در شبکه تأثیر بگذارد تغییراتی در محیط ایجاد کنید. به دنبال اضافه کردن یک سرور جدید به یک آرایه NLB هستید؟ مشکلی نیست این‌کار بدون مشکل و بدون آن‌که مجبور به قطع سرویس‌دهی شوید امکان‌پذیر است. آیا سروری باید به شکل موقت از دسترس خارج شود؟ هیچ مشکلی وجود ندارد کافی است NLB روی یک گره خاص متوقف شود و گره دیگری در آرایه وظیفه گره متوقف شده را انجام دهد. در حقیقت NLB یک کارت شبکه خاص است که اجازه می‌دهد حالت‌های مختلف NLB را روی کارت‌های مختلف شبکه پیاده‌سازی کرد. شما می‌توانید NLB را روی یک کارت شبکه خاص متوقف کنید و سرور را از آرایه خارج کنید. حتا کار بهتری نیز می‌توان انجام داد، اگر کمی وقت دارید پیش از آن‌که سرور را به سرعت آفلاین کنید فرمان drastop را اجرا کنید. این فرمان اجازه می‌دهد تا نشست‌های شبکه موجود که در حال حاضر روی آن سرور قررا دارند به‌طور کامل بسته شوند.

آدرس‌های آی‌پی مجازی و اختصاصی

یک مدیر شبکه باید درباره روشی که NLB بر مبنای آن از آدرس‌های آی‌پی استفاده می‌کند اطلاعات کافی داشته

باشد. دقت کنید به هر کارت شبکه در یک سرور که بخشی از یک آرایه متعادل‌کننده بار است باید یک آدرس آی‌پی ایستا اختصاص داده شود. NLB با آدرس‌هایی که DHCP ارائه می‌کند کار نمی‌کند. در دنیای NLB یک آدرس آی‌پی ایستا در کارت شبکه به عنوان یک آی‌پی اختصاصی در نظر گرفته می‌شود. این آدرس‌های اختصاصی برای کارت‌های شبکه منحصر به‌فرد هستند، بدیهی است که هر سرور آدرس آی‌پی اختصاصی مخصوص به خود را دارد. به‌طور مثال، در مثال ما WEB1 روی آدرس آی‌پی اختصاصی خودش یعنی 10.10.10.40 کار می‌کند و سرور WEB2 نیز آدرس اختصاصی خود 10.10.10.41 را دارد.

دقت کنید هنگامی که میان دو سرور از NLB استفاده می‌کنید باید مراقب آدرس‌های آی‌پی اختصاصی باشید، البته این امکان وجود دارد که یک آدرس آی‌پی جدید ایجاد کنیم که میان دو سرور به‌اشتراک قرار گیرد، به این آی‌پی مشترک، آدرس آی‌پی مجازی (VIP) گفته می‌شود. به‌طور مثال، زمانی که به سراغ راه‌اندازی NLB می‌روید، در نظر داریم آدرس آی‌پی 10.10.10.42 به عنوان VIP استفاده کنیم. آدرسی که تاکنون در شبکه استفاده نشده است. برای روشن‌تر شدن بحث اجازه دهید نگاهی سریع به آدرس‌های آی‌پی داشته باشیم که هنگام راه‌اندازی وب‌سایت متعادل‌کننده باز استفاده می‌شوند.

WEB1 DIP = 10.10.10.40

WEB2 DIP = 10.10.10.41

Shared VIP = 10.10.10.42

هنگامی که رکورد DNS خود برای intranet.contoso.local را منتشر می‌کنیم، این نامی است که برای وب‌سایتمان در نظر می‌گیریم. من فقط یک رکورد میزبان A را ایجاد می‌کنم که این رکورد به آدرس آی‌پی مجازی 10.10.10.42 اشاره می‌کند.

حالت‌های NLB

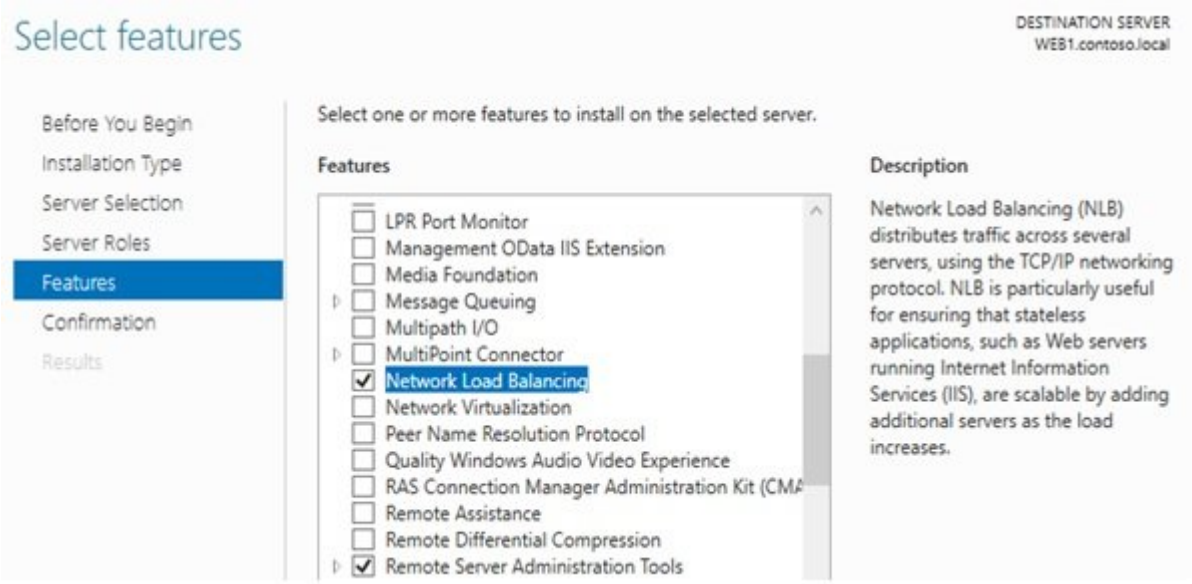
در پاراگراف بعد به سراغ پکیربندی مکانیزم متعادل‌کننده بار می‌رویم، اما پیش از انجام این‌کار باید به نکته مهمی دقت کنیم. یکی از تصمیمات مهم در این زمینه انتخاب حالت NLB است که قصد استفاده از آن‌را داریم. Unicast به‌صورت پیش‌فرض انتخاب شده و مکانیزیمی است که بیشتر شرکت‌ها NLB را بر مبنای آن راه‌اندازی می‌کنند، شاید به دلیل این‌که گزینه پیش‌فرض است، بیشتر شرکت‌ها از آن استفاده می‌کنند، اما باید بدانید گزینه‌های دیگری همچون Unicast، MutliCast، Multicast IGMP نیز وجود دارند که لازم است درباره آن‌ها اطلاعات کافی به دست آورید.

پیکربندی یک وب سایت متعادل با بار

صحبت کافی است؛ وقت آن است که این را برای خودمان تنظیم کنیم و امتحان کنیم. من دو سرور وب دارم که در شبکه آزمایشگاهی من ، WEB1 و WEB2 کار می کنند. هر دو از IIS برای میزبانی وب سایت Intranet استفاده می کنند. هدف من تهیه رکورد DNS منفرد برای کاربرانم است تا بتوانند با آنها ارتباط برقرار کنند ، اما اجازه دهید همه این ترافیک ها با برخی از توازن بار واقعی بین دو سرور تقسیم شود. برای انجام این کار مراحل بعدی را دنبال کنید.

فعال‌سازی NLB

قبل از هر کاری باید مطمئن شویم که سرورهای WEB1 و WEB2 برای به‌کارگیری NLB آماده هستند، زیرا ویژگی فوق به‌طور پیش‌فرض روی آن‌ها نصب نشده است. NLB یکی از ویژگی‌های موجود در ویندوز سرور 2019 است و شما شبیه به سایر ویژگی‌ها از طریق وزراد Add roles and features قادر به اضافه کردن آن هستید. پس در اولین گام باید ویژگی فوق را به تمامی سرورهایی که قرار است بخشی از آرایه NLB شوند اضافه کنید.



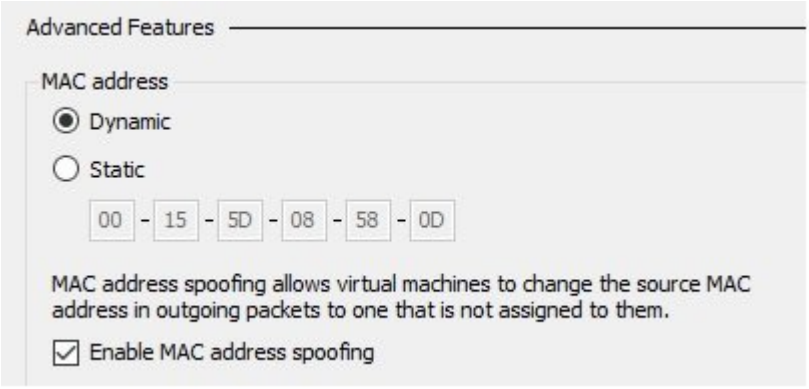
جعل مک آدرس روی ماشین‌های مجازی

بسیاری از سرپرستان شبکه وب‌سرورها را روی ماشین‌های مجازی اجرا می‌کنند. مهم نیست از Hyper-V، VMware یا سایر فناوری‌های مجازی برای میزبانی وب‌سرور استفاده کنید، در تمامی موارد یک گزینه خارجی در پیکربندی خود ماشین مجازی وجود دارد که اجازه می‌دهد ماشین مجازی از تغییر مک‌آدرس پشتیبانی کند.

این گزینه جدید Enable MAC spoofing نام دارد. گزینه فوق یک تیک ساده است که باید آن‌را فعال کنید تا فرآیند جعل مک‌آدرس به درستی انجام شود. دقت کنید این‌کار باید برای تمامی کارت‌های شبکه مجازی که قصد استفاده از NLB را دارند انجام شود. به خاطر داشته باشید، گزینه فوق تنظیمی برای کارت شبکه و نه برای ماشین مجازی است. اگر چند کارت شبکه در ماشین مجازی دارید و قصد متوازن‌سازی بار روی آن‌ها را دارید باید تیک فوق را روی تمامی کارت‌های شبکه فعال کنید.

برای اعمال این تغییر باید ماشین مجازی خاموش شود، بنابراین سرورهای WEB1 و WEB2 را خاموش می‌کنیم. در مرحله بعد باید کادر فوق را باز کرده و این گزینه را فعال کنیم. در ماشین مجازی Hyper-V باید روی نام سرور (WEB1) راست کلیک کنید و به تنظیمات ماشین مجازی بروید و سپس روی آداپتور شبکه کلیک کنید تا گزینه‌های مربوط به کارت شبکه مجازی مربوط به سرور خود (WEB1) را مشاهده کنید. در نسخه‌های جدید Hyper-V این تنظیمات در زیر مجموعه خصوصیات کارت شبکه و در بخش Advanced Features قرار دارند. در این بخش گزینه‌ای به‌نام Enable MAC address spoofing وجود دارد که برای جعل مک‌آدرس باید آن‌را فعال کنید.

اگر گزینه فوق خاکستری است به معنای آن است که ماشین مجازی روشن است و باید خاموش شود.



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

آموزش رایگان ویندوز سرور 2019

تاریخ انتشار:

13 آذر 1398

نشانی منبع:
https://www.shabakeh-mag.com/networking-technology/16349/%D9%85%D8%AA%D9%88%D8%A7%D8%B2%D9%86%E2%80%8C%D8%B3%D8%A7%D8%B2%DB%8C-%D8%A8%D8%A7%D8%B1-%D8%AA%D8%B1%D8%A7%D9%81%DB%8C%DA%A9-%D8%B4%D8%A8%DA%A9%D9%87-%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-%DA%86%DB%8C%D8%B3%D8%AA-%D9%88-%DA%86%D9%87-%DA%A9%D8%A7%D8%B1%D8%A8%D8%B1%D8%AF%DB%8C-%D8%AF%D8%A7%D8%B1%D8%AF%D8%9F