# چگونه از گواهی‌نامه‌ها در DirectAccess مبتنی بر ویندوز سرور 2019 استفاده کنیم؟


فارغ از نحوه تعامل و برقراری ارتباط میان DirectAccess با IPv6 موضوع مهم دیگری که مدیران باید درباره آن اطلاع داشته باشند، گواهی‌نامه‌هایی که توسط DirectAccess استفاده می‌شوند. زمانی که تصمیم می‌گیرید درباره نحوه عملکرد DA اطلاعات کسب کنید، به سرعت متوجه خواهید شد که در مکان‌های مختلف باید از گواهینامه‌ها استفاده کنید.

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

## گواهینامه‌های استفاده شده با DirectAccess

فارغ از نحوه تعامل و برقراری ارتباط میان DirectAccess با IPv6 موضوع مهم دیگری که مدیران باید درباره آن اطلاع داشته باشند، گواهی‌نامه‌هایی که توسط DirectAccess استفاده می‌شوند. زمانی که تصمیم می‌گیرید درباره نحوه عملکرد DA اطلاعات کسب کنید، به سرعت متوجه خواهید شد که در مکان‌های مختلف باید از گواهینامه‌ها استفاده کنید. در حالی که شبکه خصوصی مجازی نیازمند استفاده از گواهینامه‌ها است، تشخیص این‌که کدام گواهینامه‌ها باید در چه مکانی استفاده شوند بر عهده مدیران شبکه است که درک درست این مسئله به کمی مطالعه زیاد و بررسی مستندات مایکروسافت نیاز دارد. اکنون قصد داریم نکاتی که شاید ممکن است برای شما در زمینه گواهینامه‌های DirectAccess مبهم باشند را برای شما روشن کنیم.

شرط اصلی درک درست این مطلب این است که یک سرور ویندوزی CA در شبکه خود داشته باشید. دقت کنید در این مرحله وجود یک زیرساخت کلید عمومی برای DirectAccess موضوع مهمی نیست. در این مرحله باید به فکر انتشار گواهی‌نامه‌ها برای سرور DA و کلاینت‌های خود باشیم. فقط سه مکان وجود دارد که گواهینامه‌ها در DirectAccess استفاده می‌شود و دو مورد از این گواهی‌نامه‌ها نیز SSL هستند.

## گواهی SSL در وب سرور NLS

همان‌گونه که قبلا اشاره شد، وب سایت NLS برای اجرا به پروتکل HTTPS نیاز دارد. به عبارت دقیق‌تر باید یک گواهینامه SSL را روی سروری که قرار است وب‌سایت NLS را میزبانی کند نصب کنید. با فرض این‌که یک سرور CA داخلی دارید این گواهینامه را می‌توانید از سرور فوق تهیه کنید و ضرورتی ندارد گواهی‌نامه‌ای از یک CA عمومی خریداری کنید، زیرا این گواهینامه قرار است تنها از طریق ماشین‌های متصل به دامنه و کلاینت‌های DirectAccess استفاده شود. از آن‌جایی که کامپیوترهای متصل به دامنه به‌طور خودکار به سرورهای CA در شبکه اعتماد دارند این گواهینامه به سادگی از CA داخلی صادر می‌شود و دقیقاً همان کاری را انجام می‌دهد که برای به‌کارگیری در

DirectAccess به دنبال آن هستیم.

## گواهینامه SSL در سرور DirectAccess

یک گواهینامه SSL باید روی سرور DirectAccess نصب شود، اما این گواهی‌نامه باید از مرجع صدور گواهینامه عمومی خریداری شود. این گواهینامه برای اعتبارسنجی استریم‌های ترافیکی پروتکل IP-HTTPS که از سمت کامپیوترهای کلاینت می‌آیند استفاده خواهد شد، به دلیل این‌که ترافیک فوق از نوع SSL است در نتیجه برای تأیید اعتبار به یک گواهی SSL نیاز داریم. از آن‌جایی که شنونده IP-HTTPS از طریق اینترنت وارد می‌شود، توصیه می‌شود به جای اینکه سعی کنید از گواهی‌نامه زیرساخت کلید عمومی داخلی خود استفاده کنید از یک گواهینامه صادر شده از طریق یک مرکز عمومی استفاده کنید. اگر شرکت شما قبلا یک wildcard SSL دارد بهتر است برای صرفه‌جویی در هزینه‌ها از آن استفاده کنید.

## گواهی‌های ماشینی که روی سرور DA و تمامی کلاینت‌های DA استفاده می‌شوند

آخرین و پیچیده‌ترین قسمت پازل گواهینامه DirectAccess گواهی‌های ماشین است. زمانی‌که به درستی درباره مواردی که به آن‌ها نیاز دارید اطلاعات کافی دارید، کار چندان سختی پیش‌رو ندارید. در این حالت فقط نیاز داریم که یک گواهی Computer یا Machine را روی سرور DirectAccess و هر یک از دستگاه‌های کلاینت DirectAccess نصب کنیم. این گواهی ماشین به عنوان بخشی از فرآیند تأیید هویت تونل‌های IPsec استفاده می‌شود. این بخش بزرگی از روشی است که در آن DirectAccess تأیید می‌کند کامپیوتر شما قصد برقراری ارتباط با DA را دارد شما واقعا همان شخصی هستید که ادعا می‌کنید.

بهترین راه برای صدور گواهی‌نامه‌های ماشین وارد شدن به سرور CA و ساخت یک الگوی گواهی جدید است که در اصل یک نسخه تکثیر شده از یک الگوی کامپیوتری از پیش ساخته شده است. هنگامی که الگوی گواهی جدید خود را تنظیم می‌کنید، مطمئن شوید فاکتورهای زیر در گواهی‌نامه لحاظ شده است.

نام مشترک (Common Name) گواهی باید با FQDN کامپیوتر مطابقت داشته باشد.

نام موضوع پیشنهادی (SAN) گواهی‌نامه هم‌طراز با نام DNS کامپیوتر برابر باشد.

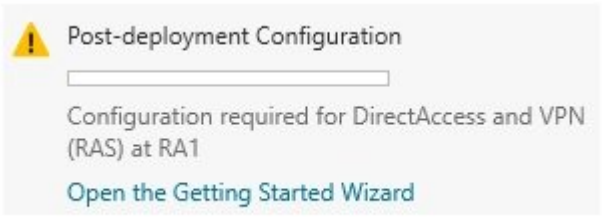
این گواهینامه باید برای موارد داخلی (Enhanced Key Usage) برای احراز هویت کلاینت و احراز هویت سرور استفاده شود.

در اینجا لازم است به این نکته اشاره کنیم که ما واقعا نمی‌خواهیم این‌کار را انجام دهیم، زیرا صدور این گواهینامه‌ها برای آن‌که DirectAccess کار کند ضرورتی ندارد. اگر در سمت کلاینت از ویندوز 8 یا نسخه‌های جدیدتر استفاده می‌کنید، شما می‌توانید از DA بدون گواهی‌های ماشین استفاده کنید. در هنگام ساخت تونل‌های IPsec کامپیوترهای موجود در شبکه می‌توانند از رویکردی به‌نام Kerberos Proxy برای احراز هویت استفاده کنند، اما اکیدا توصیه می‌کنم موضوع گواهی‌نامه‌ها را جدی بگیرید. به‌کارگیری گواهینامه‌ها به عنوان بخشی از فرآیند تأیید اعتبار، اتصال را پایدارتر و ایمن‌تر می‌کند. علاوه بر این، همانند قرار دادن NLS اگر به دنبال کارکرهای پیشرفته DirectAccess همچون تعادل بار یا multisite هستید یا حتی اگر می‌خواهید برخی از کامپیوترهای مجهز به ویندوز 7 را از طریق DA متصل کنید به گواهی‌نامه‌ها نیاز خواهید داشت. بنابراین ، در وهله اول بهتر است قبل از آن‌که به‌طور رسمی کار با DirectAccess را آغاز کرده و گواهینامه‌ها را صادر کنید، کمی در این زمینه تمرین کنید.

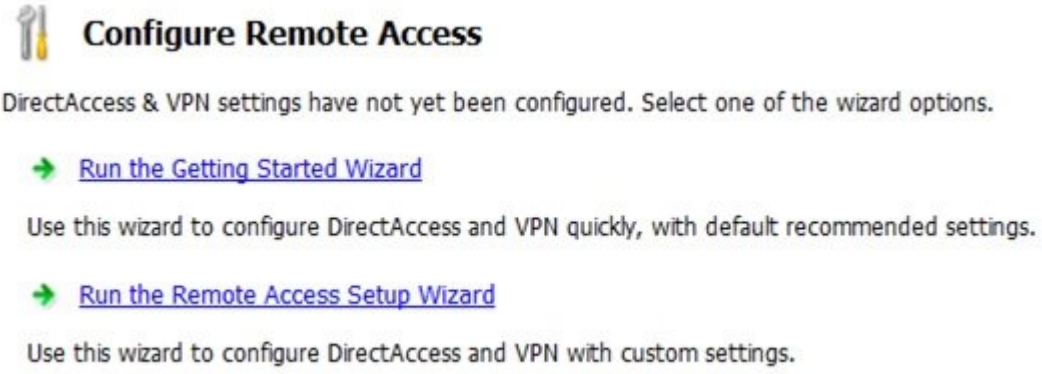
## از Wizard Getting Started استفاده نکنید!

پس از اتخاذ تصمیمات لازم در زمینه طراحی و اجرای پیش‌نیازهایی که تاکنون در مورد آن‌ها صحبت کردیم در نهایت زمان آن رسیده که نقش Remote Access را روی سرور DirectAccess جدید نصب کنید! پس از اتمام نصب نقش، مشابه با سایر نقش‌هایی که روی ویندوز سرور 2019 نصب کردیم، پیامی مشاهده می‌کنید که اعلام می‌دارد نقش مربوطه را باید پیکربندی کنید. در حقیقت اگر علامت تعجب زرد در داخل Server Manager را مشاهده کردید گزینه‌ای به‌نام Getting Started Wizard در اختیار دارید، اما گزینه فوق چیزی نیست که علاقه‌مند به کلیک کردن روی آن باشید.

مکانی که در آن باید تنظیمات DirectAccess را تنظیم کنید، همان کنسول Remote Access Management است که از طریق منوی Tools از ویزاد Server Manager در اختیار شما قرار دارد. ابزاری که در زمان نصب نقش Remote Access به ویندوز اضافه شد. اگر ابزار فوق را اجرا کنید پنجره‌ای همانند شکل زیر مشاهده می‌کنید که دو گزینه در اختیار ما قرار می‌دهد.




روی گزینه Run the Getting Started Wizard کلیک نکنید! GSW یک روش میان‌بر برای پیاده‌سازی DirectAccess است که تنها برای نصب و اجرای سریع DA طراحی شده است. توصیه می‌کنم تحت هیچ شرایطی از GSW در ارتباط با پیکربندی DA استفاده نکنید، زیرا یک پیکربندی سریع و آسان در اختیارتان قرار می‌دهد و اجازه نمی‌دهد روی بسیاری از فاکتورهای پیکربندی تغییری اعمال کنید.




زمانی که کنسول فوق را مشاهده کردید روی گزینه Run Remote Access Setup Wizard را کلیک کنید تا صفحه مربوط به پیکربندی DirectAccess را همراه با تمامی تنظیمات آن مشاهده کنید. صفحه پیکربندی DA شامل مجموعه‌ای از چهار مرحله مختلف است که دسترسی به گزینه‌های پیکربندی دقیق را امکان‌پذیر می‌کند. تنظیمات و نکات ریز جالب توجهی در این صفحات قرار دارد که هرکدام از آن‌ها معنا و مفهوم خاص خود را دارند. اگر قبلا DirectAccess را پیکربندی کرده‌اید و از Wizard Getting Started استفاده کرده‌اید، DA ممکن است برای شما کار کند، اما به شکل کارآمد و ایمنی اجرا نمی‌شود. اما چرا نباید از ویزارد Getting Started Wizard استفاده کنیم؟ در پاسخ به این پرسش به موارد زیر می‌توانیم اشاره کنیم:

GSW وب‌سایت NLS را در سرور DA میزبانی می‌کند که جالب نیست.

GSW تنظیمات GPO کلاینت DA را روی Domain Computers اعمال می‌کند که ایده وحشتناکی است.

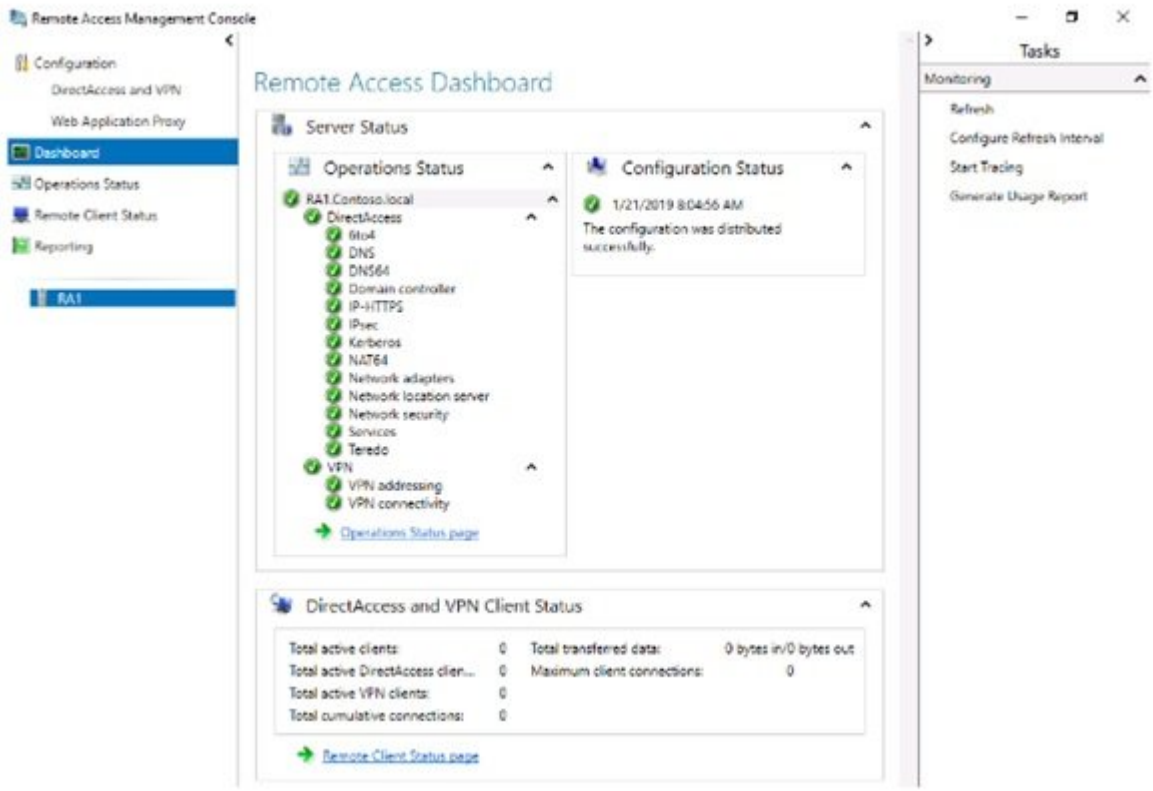
GSW از گواهی‌های خود امضا شده استفاده می‌کند که سطح امنیتی 101 را ارائه می‌کند که به هیچ عنوان مناسب نیست.

GSW به‌طور خودکار Teredo را غیرفعال می‌کند که محدودیت‌هایی به وجود می‌آورد.

GSW به شما اجازه نمی‌دهد به گزینه‌های پیشرفته DirectAccess دسترسی داشته باشید، احتمالا به این دلیل که خودش همه چیز را تنظیم می‌کند و در نتیجه توانایی شما برای به‌کارگیری قابلیت‌های پیشرفته این فناوری را محدود می‌کند.

## کنسول مدیریت دسترسی از راه دور

شما به خوبی می‌دانید که چگونه به کاربران امکان دسترسی از راه دور به سرور جدید را بدهید. همانند بسیاری از دستگاه‌های شبکه، هنگامی که تمامی تنظیمات خود را روی Remote Access Server اعمال می‌کنید، در مرحله بعد اجازه می‌دهد تا فرآیندها کار عادی خود را آغاز کنند. اگر همه چیز را به دسترس پیکربندی کرده و ویرایش کرده باشید، نیازی نیست در حالت عادی دومرتبه اقدام به ویرایش تنظیمات کنید. با این حال، کنسول Remote Access Management در ویندوز سرور 2019 نه فقط برای پیکربندی بخش‌ها و مولفه‌های دسترسی از راه دور، بلکه برای نظارت و گزارش‌گیری نیز مفید است. هنگامی که DirectAccess کار می‌کنید، ابزار فوق همان چیزی است که برای پیکربندی، مدیریت و نظارت به آن نیاز دارید. در بخش VPN / AOVPN مجموعه ابزارهای دسترسی از راه دور قرار دارد که اجازه می‌دهند از داخل RRAS به پیکربندی شبکه خصوصی مجازی بپردازید، اما RAMC مکانی است که اجازه نظارت بر سمت سرور، نظارت بر ارتباط کلاینت‌ها و گزارش‌گیری آماری را می‌دهد. مهم نیست از VPN ، DA یا ترکیبی از هر دو مورد استفاده کنید، RAMC ابزاری است که آسودگی خیال را برای شما به همراه می‌آورد. اجازه دهید به درون این کنسول نگاهی داشته باشیم و صفحات مختلف آن‌را مرور کنیم.




در شماره آینده آموزش رایگان ویندوز سرور 2019 مبحث فوق را ادامه خواهیم رفت.

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

**آموزش رایگان ویندوز سرور 2019**

**تاریخ انتشار:**

04 آبان 1398

---

**نشانی منبع:**
https://www.shabakeh-mag.com/networking-technology/16213/%DA%86%DA%AF%D9%88%D9%86%D9%87-%D8%A7%D8%B2-%DA%AF%D9%88%D8%A7%D9%87%DB%8C%E2%80%8C%D9%86%D8%A7%D9%85%D9%87%E2%80%8C%D9%87%D8%A7-%D8%AF%D8%B1-directaccess-%D9%85%D8%A8%D8%AA%D9%86%DB%8C-%D8%A8%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