چگونه یک گواهی SSL را برای سرور دیگری در ویندوز سرور 2019 ارسال کنیم؟

بحث ارسال گواهی‌ها برای سرور دوم، در دنیای شبکه یک کار عادی است. اما اگر این‌کار را به درستی انجام ندهید، دردسرهای متعددی را متحمل خواهید شد. ارسال درست گواهی‌ها تنها زمانی کامل می‌شود که کلید خصوصی نیز به درستی ارسال شده باشد. همچنین در برخی موارد مجبور هستید یک گواهی به روش‌های خاصی ارسال کنید. اکنون با دو روش ارسال گواهی از طریق کنسول MMC و کنسول IIS آشنا خواهید شد.

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

ارسال گواهی از طریق کنسول MMC

به فروشگاه Local Computer Certificate در MMC و سپس به مسیر Personal | Certificate بروید. اکنون می‌توانید گواهی **SSL** فهرست شده در این بخش را مشاهده می‌کنید. روی گواهی کلیک راست کرده و سپس به All Tasks | Export... بروید. اولین کاری که باید انجام دهید ارسال کلید خصوصی است. دقت کنید کلید خصوصی را باید پنهان نگه دارید و به گواهی اجازه می‌دهید تا به‌طور صحیح با سروری که روی آن نصب شده ارتباط برقرار کند. اگر گواهی را بدون کلید خصوصی صادر کنید، گواهینامه روی سرور دیگری کار نخواهد کرد. بنابراین در اینجا حائز اهمیت است که اگر این گواهینامه را به قصد نصب وی وب سرور دوم صادر می‌کنید و از گواهی برای اعتبارسنجی ترافیک SSL استفاده می‌کنید، گزینه Yes, export the private key را انتخاب کنید.

در زمان انجام این‌کار، ویزارد به شما هشدار می‌دهد، هنگامی که قصد ارسال گواهی‌نامه را دارید که حاوی اطلاعات مربوط به کلید خصوصی است باید یک گذرواژه مناسب را تهیه کنید که از فایل PFX که قرار است صادر و استفاده شود محافظت کند. اگر فراموش کنید چنین کاری را انجام دهید، فایل صادر شده کاملا بی استفاده خواهد بود. اگر گذرواژه‌ای که تعیین کرده‌اید بیش از اندازه ساده یا حدس زدن آن آسان است، هر شخصی که فایل PFX را دریافت می‌کند ممکن است بتواند از گواهینامه و کلید خصوصی روی وب‌سرورهای‌تان استفاده کند که این‌کار خوب نیست.

ارسال از طریق IIS

درون اپلت Server Certificate در IIS، کافی است روی گواهی کلیک راست کرده و Export را انتخاب کنید. با این‌کار صفحه‌ای ظاهر می‌شود که در آن باید گذرواژه مربوطه را تعیین کنید

ما گزینه‌های بیشتری داشتیم که هنگام ارسال از طریق MMC قادر به انتخاب یا رد آن‌ها هستیم، پس چرا گزینه‌ها در IIS این‌قدر محدود هستند؟ IIS برای سرعت بخشیدن به فرآیند صادر کردن گواهی، سایر تنظیمات را روی حالت پیش‌فرض قرار می‌دهد. هنگام صادر کردن گواهینامه SSL، احتمال این‌که کلید خصوصی را صادر کنید زیاد است. بنابراین، IIS فرض را بر این مبنا قرار می‌دهد و از نشان دادن سایر گزینه‌ها به شما صرف‌نظر می‌کند. شما مجبور هستید گذرواژه را وارد کنید، زیرا در مورد کلید خصوصی انتخابی ندارید. ارسال گواهی به‌صورت خودکار انجام خواهد شد. بنابراین، اگر دلیلی برای ارسال گواهی وجود داشت که نباید حاوی اطلاعات مربوط به کلید خصوصی شود، بهتر است از کنسول IIS برای این‌کار استفاده نکنید. در این حالت باید MMC را باز کرده و از طریق جادوگر که قابلیت‌های بیشتری در اختیارتان قرار می‌دهد استفاده کنید.

وارد کردن گواهی به سرور دوم

زمانی‌که فایل PFX به شکل کامل در دسترس قرار گرفت، در مرحله بعد فرآیند وارد کردن گواهی به سرور دوم کار ساده‌ای است. از درون کنسول MMC یا IIS و با راست کلیک و انتخاب گزینه Import قادر به وارد کردن گواهی هستید. با دنبال کردن مراحلی که برای وارد کردن گواهی وجود دارد باید فایل PFX را انتخاب کرده و گذرواژه‌ای که برای محافظت از گواهی تعیین شده است را درون فیلد مربوطه وارد کنید. در این مرحله گواهی به سرور دوم وارد می‌شود. اگر روی خصوصیات گواهی کلیک کنید، یک آیکون کلید کوچک و پیام خصوصی کلید که پایین صفحه ویژگی‌های گواهی نمایش داده شده است را مشاهده می‌کنید. اگر پیام خصوصی را مشاهده نمی‌کنید، در طی فرآیند ارسال گواهی کاری را به اشتباه انجام داده‌اید. اکنون باید به عقب بازگشته و دومرتبه این‌کار را انجام دهید.

به جلو حرکت کرده و آن‌را امتحان کنید. سروری را با گواهی **SSL** پیدا کرده و فرآیند ارسال گواهی روی سرور را بدون آن‌که کاری در ارتباط با کلید خصوصی انجام دهید آزمایش کنید. زمانی‌که گواهی را به سرور جدید وارد می‌کنید مشاهده می‌کنید که فایل گواهی بدون کلید خصوصی وارد شده و هیچ‌گونه پیغامی در پایین صفحه خصوصیات نشان

داده نمی‌شود، اما فایلی که ارسال شده و حاوی کلید خصوصی است باعث نشان دادن پیغام درستی در این بخش می‌شود. برای آن‌که درک بهتری از هر دو حالت به دست آورید، یک گام به جلو برداشته و سعی کنید از هر دو گواهینامه روی یک وب سایت غیر مهم استفاده کنید تا ببینید چه اتفاقی می‌افتد. متوجه می‌شوید گواهی که فاقد کلید خصوصی است، نمی‌تواند ترافیک SSL را تأیید کند. اگر سعی در صدور گواهینامه SSL دارید و گزینه کلید خصوصی خاکستری است، بدان معنا است که وقتی مدیر اصلی این گواهینامه را روی وب‌سرور نصب کرده اما گزینه خاصی را انتخاب کرده که امکان ارسال کلید خصوصی در آن مسدود شده است. در این حالت، شما نمی‌توانید گواهینامه را با کلید خصوصی صادر کنید.

گواهی‌ها برای برخی از مدیران شبکه اوضاع پیچیده‌ای را رقم می‌زنند و به همین دلیل است که آن‌ها فکر می‌کنند گواهی‌ها تنها دردسرآفرین هستند. اگر در زمان کار با گواهی‌ها اطلاعی در مورد نحوه به‌کارگیری کنسول‌های مدیرتی که برای کار با زیرساخت گواهی‌ها در اختیارتان قرار دارند اطلاعی نداشته باشید، این فرآیند بیش از اندازه برای شما دشوار و پیچیده خواهد شد. اما اگر مطالبی که در ارتباط با گواهی‌ها ارائه کردیم را با دقت مطالعه کنید، حتا اگر با مشکل جدی روبرو شوید، بازهم پیدا کردن علت بروز مشکل کار چندان سختی نخواهد بود.

برای آن‌که سطح دانش خود در ارتباط با گواهی‌ها را محک بزنید، پیشنهاد می‌کنم به پرسش‌های زیر دقت کرده و به آن‌ها پاسخ دهید:

1. نام نقشی درون **ویندوز سرور 2019** چیست که به شما اجازه می‌دهد گواهی‌هایی را از سرور خود صادر کنید؟

2. چه نوع سرور مرجع صدور گواهی (CA) معمولا برای اولین بار در محیط دامنه نصب می‌شود؟

3. آیا باید نقش مرجع صدور گواهینامه را روی یک کنترل‌کننده دامنه نصب کنید؟

4. بعد از ایجاد یک قالب الگوی جدید گواهی، قبل از این‌که بتوانید الگوی جدید صدور گواهینامه برای کامپیوترها یا کاربران صادر کنید، چه کاری باید انجام دهید؟

5. نام کلی تنظیمات GPO چیست که گواهی‌ها را مجبور به صدور می‌کند، بدون آن‌که به مداخله دستی یک مدیر نیازی باشد؟

6. گواهینامه **SSL** فقط در صورتی قادر به اعتبارسنجی درست ترافیک است که اطلاعات کلید _____ را با وب‌سرور به‌اشتراک قرار داده باشد.

7. اطلاعات اولیه مورد نیاز یک مجوز عمومی برای تهیه گواهینامه **SSL** جدید (اشاره: شما این‌کار را از طریق وب‌سرور خود انجام دادید.) چیست؟

ما بحث گواهی‌ها در ویندوز سرور 2019 را در این‌جا به پایان می‌رسانیم و به سراغ مبحث شبکه‌سازی در ویندوز سرور 2019 می‌رویم.

شبکه‌سازی در ویندوز سرور 2019

همان‌گونه که تاکنون متوجه شده‌اید سرورها شبیه به درختی روبه‌رشد در شبکه‌ها هستند. آن‌ها زیرساخت ستون فقرات سازمان هستند و به ما اجازه می‌دهند تا کارهای خود را انجام دهیم. اگر سرورها را تنه یک درخت تصویر کنید، شبکه‌ها را باید ریشه درخت توصیف کنیم. شبکه شما بستری است که از زیرساخت شرکت پشتیبانی می‌کند و کانال‌هایی ایجاد می‌کند که همه دستگاه‌های داخل شرکت می‌توانند برای برقراری ارتباط با یکدیگر از آن استفاده کنند.

به‌طور سنتی، متخصصان سرور و متخصصان شبکه در صنعت فناوری‌اطلاعات و سایر صنایع به فعالیت اشتغال دارند. یک مدیر شبکه، فردی است که وظیفه اصلی او کار با سرورها است و به‌طور کلی در یک روز کاری فارغ از هر اندازه‌ای که سازمان دارد، فرصت کافی برای پشتیبانی از زیرساخت‌های شبکه را ندارو برعکس این قضیه نیز صادق است. سرپرستان شبکه به‌طور کلی تمرکزشان روی تجهیزات و ابزارهای مدیریتی است و علاقه‌ای ندارند به دنیای ویندوز سرور وارد شوند. با این حال، بسیاری از ما در شرکت‌های کوچکی کار می‌کنیم که در آن باید تخصص‌های

زیادی داشته باشیم. برخی روزها باید هم مسئولیت سرپرست شبکه و هم مسئولیت مدیری شبکه را عهده‌دار شویم یا در ارتباط با شبکه و ابزارهایی که برای عیب‌یابی ارتباطات به‌کار گرفته می‌شوند اطلاعات لازم را داشته باشیم. علاوه بر این، **ویندوز سرور 2019** یک دیدگاه جدید به دنیای شبکه‌ها وارد کرده که مجازی‌سازی شبکه‌ها را پیشنهاد داده است. یک شبکه فیزیکی همیشه وجود خواهد داشت و از سوئیچ‌های فیزیکی و روترها برای انتقال بسته‌ها بین اتاق‌ها و ساختمان‌های مختلف استفاده می‌کند. اما اکنون ما همچنین ایده شبکه‌های نرم‌افزار محور را درون سرورهای ویندوزی داریم که به ما امکان مجازی‌سازی برخی از پیکربندی‌ها و قابلیت‌ها را می‌دهد. نه تنها پیکربندی، بلکه در واقع ما در حال مجازی‌سازی ترافیک شبکه هستیم و سعی داریم شبکه‌های خود را از درون یک کنسول سرور ایجاد کنیم و به جای آن‌که از رابط‌های خط فرمان برای پیکربندی روترهای خود استفاده کنیم، این میراث گذشته را به تاریخ سپرده و به سراغ مفاهیم جدیدتر برویم.

اجازه دهید قبل از هر کاری به قابلیت‌ها و ویژگی‌های جدیدی که **ویندوز سرور 2019** در تعامل با شبکه‌های فیزیکی یا هر شبکه‌ای در اختیار ما قرار داده نگاهی داشته باشیم، زیرا این قابلیت‌ها برای هر سرپرستی در دنیای شبکه‌های امروزی مهم هستند. در ادامه به ویژگی‌های مجازی‌سازی شبکه خواهیم پرداخت. در ارتباط با شبکه‌سازی آشنایی با IPv6، ابزارهای شبکه‌سازی، ساخت یک جدول مسیریابی، شبکه‌های نرم‌افزارمحور و NIC Teaming نکات حائز اهمیت هستند.

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:

[□□□□□ □□□□□□ □□□□□□ □□□□ 2019]

تاریخ انتشار:

25 شهریور 1398

نشانی منبع:
https://www.shabakeh-mag.com/networking-technology/16028/%DA%86%DA%AF%D9%88%D9%86%D9%87-%DB%8C%DA%A9-%DA%AF%D9%88%D8%A7%D9%87%DB%8C-ssl-%D8%B1%D8%A7-%D8%A8%D8%B1%D8%A7%DB%8C-%D8%B3%D8%B1%D9%88%D8%B1-%D8%AF%DB%8C%DA%AF%D8%B1%DB%8C-%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%B1%D8%B3%D8%A7%D9%84-%DA%A9%D9%86%DB%8C%D9%85%D8%9F