چگونه یک گواهی SSL را دریافت کرده و آن‌را روی ویندوز سرور 2019 نصب کنیم؟

ارسال درخواست برای دریافت یک گواهی SSL فرآیند پیچیده‌ای نیست و شاید با چند کلیک ساده و پرداخت وجه مربوطه این‌کار انجام شود. اما پیش از ارسال درخواست لازم است به یکسری نکات مهم دقت کنید.

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

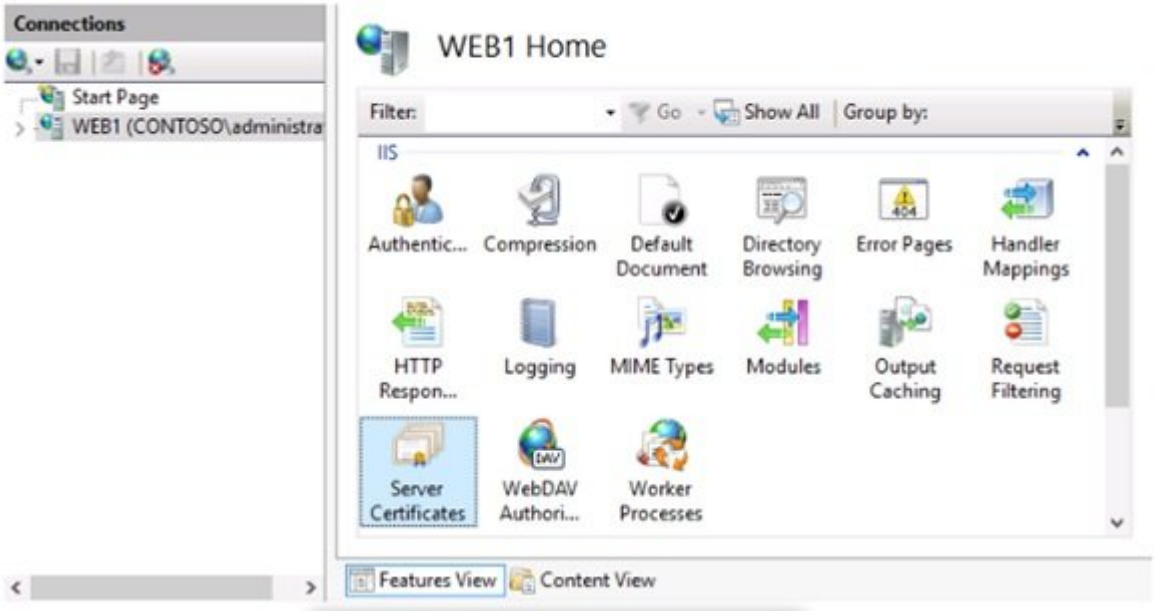
ایجاد یک درخواست امضای گواهی

اگر اولین قدم شما برای به‌دست آوردن یک گواهینامه SSL از مراجع صدور گواهی عمومی ورود به وب‌سایت آن‌ها، خرید یک گواهی و بلافاصله دانلود گواهی است، شما یک کار مهم را انجام نداده‌اید. در چنین شرایطی هیچ راهی وجود ندارد تا درباره کلید خصوصی که ممکن است در سرور وب خود قرار داده‌اید اطلاعاتی به دست آورید و در نتیجه چنین گواهی در هر مکانی که نصب شود، بدون استفاده است.

هنگامی‌که یک گواهینامه SSL را روی یک سرور وب نصب می‌کنید، لازم است درباره کلید خصوصی گواهی اطلاعات کافی داشته باشد. چگونه اطمینان حاصل کنیم که چنین اطلاعاتی را به دست می‌آوریم؟ برای این منظور لازم است با اصطلاح به‌نام درخواست ثبت گواهی (CSR) آشنا باشید. اولین قدم برای دریافت اصولی یک گواهینامه SSL، ایجاد CSR است. هنگامی که این فایل را ایجاد می‌کنید، بستر وب‌سرور کلید خصوصی مورد نیاز را ایجاد می‌کند و آن‌را روی سرور شما مخفی می‌کند. CSR به گونه‌ای ایجاد می‌شود که می‌داند چگونه باید با کلید خصوصی ارتباط برقرار کند. شما از CSR هنگام ورود به وب‌سایت مرجع صدور CA برای ارائه درخواست گواهی استفاده می‌کنید.

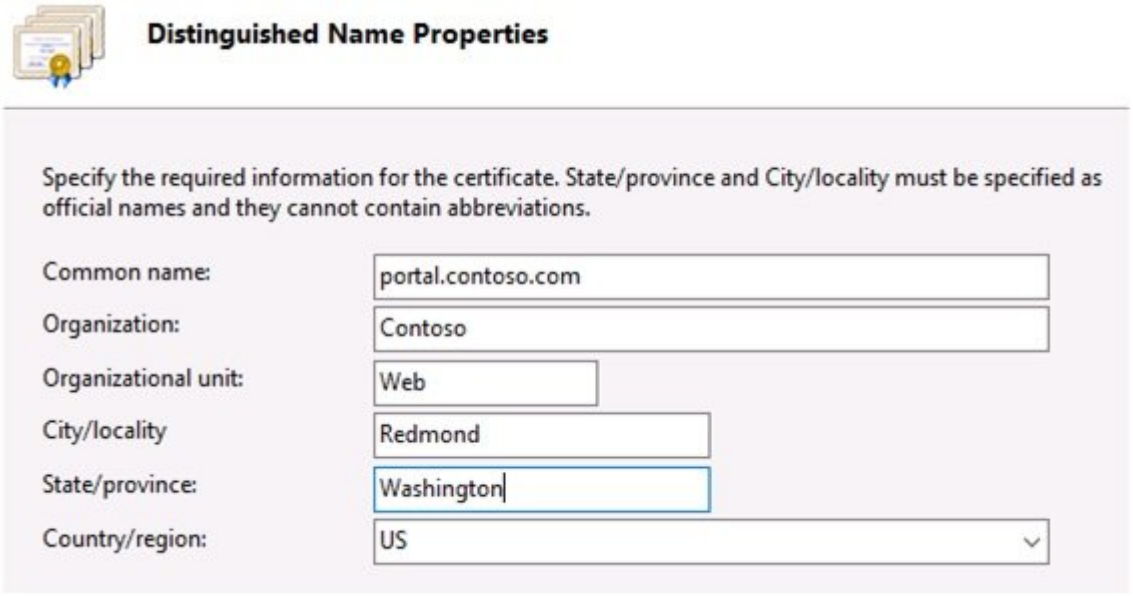
دقت کنید که کلید خصوصی درون CSR قرار ندارد و مرجع صادر کننده گواهی هرگز نمی‌داند کلید خصوصی شما چیست. این کلید اهمیت بالایی دارد و فقط در وب‌سرور سازمانی شما ذخیره می‌شود.

برای ایجادIIS ، CSR را از منوی Tools درون Server Manager انتخاب کرده و از درخت ناوبری سمت چپ صفحه روی نام وب‌سرور کلیک کنید. با این‌کار یکسری از اپلت‌های مختلف در مرکز کنسول نشان داده می‌شوند. اپلتی که قصد کار با آن‌را داریم Certificate Server نام دارد. روی آن دوبار کلیک کنید.

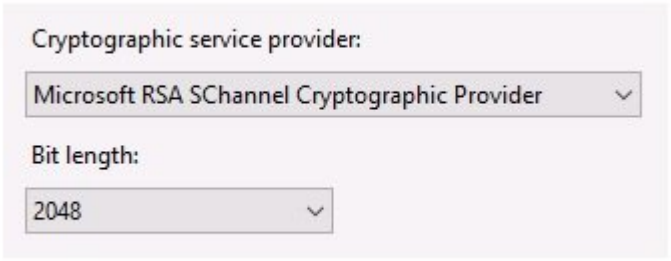


درون صفحه Certificates Server می‌توانید گواهی‌های موجود در سرور را به شکل فهرست شده مشاهده کنید. این همان مکانی است که گواهی SSL را درون آن مشاهده خواهیم کرد. گواهی که در نظر داریم درون ویژگی‌های سایت قرار داده و زمانی که به سمت پروتکل HTTPS رفتیم از آن استفاده کنیم. اولین قدم برای به‌دست آوردن گواهی جدید ایجاد درخواست گواهی از طریق مرجع صدور است. اگر به سمت راست صفحه نگاه کنید، بخش Actions را مشاهده می‌کنید که در پایین آن فهرست ایجاد درخواست گواهی (Create Certificate Request) وجود دارد. روی Action کلیک کنید.

در پنجره نتایج، باید اطلاعات ذخیره شده در گواهی SSL را جمع‌آوری کنید. فیلد نام Common اطلاعات بسیار مهمی دارد که نام DNS که قرار است گواهی از آن محافظت کند را خواهد داشت. در حالت کلی نام وب‌سایت خود را درون این فیلد وارد می‌کنید. در ادامه سایر فیلدها را با اطلاعات سازمان خود پر می‌کنید. سایر فیلدها می‌توانند یکسری یادداشت‌های ویژه داشته باشند که بیشتر مدیران شبکه برای اطلاعات تکمیلی از آن‌ها استفاده می‌کنند. به‌طور مثال، برای فیلد واحد سازمانی برخی از مدیران تنها واژه web را می‌نویسند. دقت کنید در فیلد State نام شهر را کامل وارد کرده و از نام کوتاه استفاده نکنید.



در صفحه Cryptographic Service Provider Properties، بیشتر در نظر دارید ارائه‌دهنده سرویس Cryptographic را به صورت پیش‌فرض تنظیم کنید، مگر این‌که یک کارت رمزنگاری تخصصی در سرور خود داشته باشید و قصد آن‌را داشته باشید تا برای پردازش و رمزگذاری درون سایت از آن استفاده کنید. در سرور IIS ، تقریبا همیشه Microsoft RSA SChannel Cryptographic Provider را مشاهده می‌کنید. آن‌چه که باید در این‌جا تغییر دهید، تغییر اندازه Bit است. طول بیت استاندارد برای سال‌های متمادی برابر با 1024 بود و در ویندوز سرور 2019 نیز به عنوان پیش‌فرض انتخاب شده است. کارشناسان سرانجام به این نتیجه‌گیری کلی رسیدند که که اندازه 1.024 خیلی ضعیف باشد و باید استاندارد جدید 2048 جایگزین آن شود. وقتی برای درخواست گواهی به وب‌سایت مرجع صدور گواهی می‌روید، مطمئن شوید که حداقل اندازه برابر با 2048 بیت باشد. منوی کشویی را باز کرده و اندازه را به سال 2048 تغییر دهید:



تنها کاری که باید برای CSR انجام دهیم این است که برای آن یک مکان و نام فایل مشخص کنیم. ذخیره‌سازی فایل csr در حالت متنی گزینه عاقلانه‌ای است، زیرا همه آن‌چه باید هنگام درخواست گواهی انجام دهیم این است که فایل را باز کنیم و سپس محتویات را انتخاب و کپی کنیم. اکنون فایل csr را ایجاد کرده‌اید و می‌توانید از این فایل برای درخواست گواهی از مرجع صدور عمومی گواهی استفاده کنید.

ارسال و ثبت درخواست گواهی

اکنون برای دریافت گواهی به سایت مرجع عمومی بروید. هر یک از شرکت‌هایی که اشاره کردیم شبیه به GoDaddy یا Verisign برای این منظور مناسب هستند. هر مرجعی رابط کاربری وب خاص خود را دارد، بنابراین نمی‌توانیم مراحل دقیقی را که باید برای این فرآیند پشت سر بگذارید را به شکل دقیق تشریح کنیم. پس از ایجاد یک حساب کاربری و ورود به سایت صادر کننده گواهی باید بتوانید گزینه خرید گواهی SSL را پیدا کنید. پس از خرید گواهی، یک

فرآیند برای درخواست و استقرار گواهی وجود خواهد داشت.

زمانی‌که وارد رابط کاربری سایت برای ساخت گواهینامه جدید خود می‌شوید، به‌طور کلی تنها اطلاعاتی که مرجع صادرکننده از شما درخواست می‌کند، محتوای فایل csr است. اگر فایل متنی را که قبلا ذخیره کردیم باز کنید، مجموعه‌ای عجیب و غریب از کاراکترها را مشاهده می‌کنید.

این اطلاعات عجیب‌وغریب دقیقا همان چیزی است که مرجع صادرکننده برای ایجاد گواهینامه SSL جدید از شما درخواست می‌کند تا بداند چگونه می‌تواند با کلید خصوصی وب‌سرور شما ارتباط برقرار کند. فقط سرورهایی که CSR تولید کرده‌اند قادر هستند به شکل درست گواهینامه SSL را دریافت کرده و آن‌را پردازش کنند. به‌طور معمول، تمام کاری که باید انجام دهید این است که کل محتوای فایل csr را کپی کرده و آن‌را در وب سایت CA قرار دهید.

گواهینامه خود را دانلود و نصب کنید

اکنون باید صبر کنید. بسته به این‌که از چه مرجع صادرکننده گواهی استفاده می‌کنید، این فرآیند ممکن است زمان‌بر باشد، اما در حالت کلی گواهی شما ممکن است به سرعت آماده و قابل دانلود باشد. دلیل طولانی شدن زمان انتظار برای دریافت گواهی این است که بسیاری از مراجع صدور گواهی از کارشناسان انسانی برای تایید اطلاعات استفاده می‌کنند و کارشناس مربوطه اطلاعات را بررسی می‌کند تا مطمئن شود شرکت شما همان شرکتی است که ادعا می‌کند و شما واقعا مالک دامنه هستید. به یاد داشته باشید، مزیت واقعی یک گواهینامه SSL عمومی این است که CA تضمین می‌کند که کاربر این گواهی، شخص واقعی است و بنابراین آن‌ها اطمینان می‌دهند گواهی برای portal.contoso.com و مالک دامنه صادر شده و به اشتباه برای سازمان یا شخصی دیگری صادر نشده است.

هنگامی که موفق شدید گواهی را از وب‌سایت صادرکننده گواهی دانلود کنید، آن‌را روی وب‌سروری که فایل CSR روی آن ساخته شده است کپی کنید. مهم است که این گواهی جدید را روی همان سرور نصب کنید. اگر می‌خواهید این گواهی جدید را روی وب‌سرور دیگری نصب کنید که فایل CSR را تولید نکرده، اما در نظر دارد از گواهی ساخته شده استفاده کند ، باید بدانید که فرآیند وارد کردن گواهی با موفقیت انجام می‌شود، عملیاتی نخواهد شد. به یاد داشته باشید کلید خصوصی که گواهی قصد تعامل با آن را دارد، روی سایر سرورها وجود ندارد.

اکنون در کنسول مدیریتی IIS می‌توانیم گام بعدی را اجرا کنیم. در پنل Action روی گزینه Complete Certificate Request... کلیک کنید. با این‌کار پنجره کوچکی ظاهر می‌شود که در آن گواهی جدیدی که تازه دانلود کرده و به سرور وارد کرده‌اید را مشاهده می‌کنید. اکنون که گواهی در سرور به درستی مستقر شده است، وب‌سایت شما آماده استفاده از آن است.

اما یک کار دیگر هم باید انجام شود که همیشه بعد از نصب یا وارد کردن یک گواهی SSL باید انجام دهید. اکنون می‌توانید گواهی جدید خود را درون IIS مشاهده کنید، اگر روی گواهی جدید خود دوبار کلیک کنید، صفحه خاصیت‌های گواهی را مشاهده خواهید کرد. در زبانه General این خصوصیات به بخش پایین پنجره نگاه کنید. گواهی شما باید یک نماد کوچک و کلید خصوصی را همراه با متن گواهی نشان می‌دهد. اگر قادر به مشاهده این پیام هستید، فرآیند وارد کردن گواهی با موفقیت انجام شده و فایل گواهینامه جدید کاملا با CSR مطابقت دارد. اکنون سرور و گواهی، اطلاعات کلیدی خصوصی را به اشتراک می‌گذارند و گواهی SSL می‌تواند به درستی کار کرده و از وب‌سایت شما محافظت کند. اگر این پیام را مشاهده نمی‌کنید در فرآیند درخواست و دانلود گواهینامه مشکلی پیش آمده است. اگر پیام را در این‌جا مشاهده نمی‌کنید باید با تولید یک CSR جدید کار خود را شروع کنید، زیرا فایل گواهی که دریافت کرده‌اید هماهنگ با CSR نیست یا تنظیمی به درستی پیکربندی نشده است. بدون داشتن یک متن کلید خصوصی در انتهای این صفحه گواهی شما ترافیک را به درستی اعتبارسنجی نمی‌کند. در اینجا نمونه‌ای از یک روند درست دریافت، نصب و عملیاتی کردن گواهی را مشاهده می‌کنید.

وارد و خارج کردن گواهی

من اغلب خودم را ملزم می‌کنم که گواهی SSL یکسانی را روی چند سرور استفاده کنم. این‌کار ممکن است در شرایطی اتفاق بیفتد که بیش از یک سرور IIS سرویس‌دهی به سایت یکسانی را عهده‌دار هستند و از نوعی متعادل‌سازی بار برای تقسیم ترافیک بین آن‌ها استفاده می‌شود. این فرآیند همچنین ممکن است با هدف متعادل‌سازی بار سخت‌افزاری اجرا شود، مثال دیگر در این زمینه، زمانی‌که است که از گواهی‌های wildcard استفاده می‌کنید و یک گواهی wildcard را خریداری کرده‌اید که قرار است روی چند سرور نصب شود.

آیا حرف به معنای آن است که ما مجبور هستیم یک CSR جدید برای هر سرور داشته باشیم و برای یک کپی جدید از گواهی‌نامه یکسانی چند مرتبه درخواست دهیم؟ قطعا این‌گونه نیست و در حقیقت انجام این‌کار می‌تواند مشکلات دیگری برای شما ایجاد کند: وقتی یک مرجع صادرکننده کلید دومرتبه فرآیند کلیدسازی برای یک گواهی را انجام می‌دهد و شما درخواست یک گواهی با یک نام خاص برای گواهی که قبلا ایجاد شده است را ارسال می‌کنید، مرجع صادرکننده ممکن است گواهی اولی را ابطال کرده و کپی ثانوی را صادر کند. این موضوع همیشه و به سرعت قابل مشاهده نیست، به دلیل این‌که مدت زمانی برای از درجه اعتبار ساقط کردن گواهینامه اول تنظیم شده است. اگر دوباره رابط وب مرجع صادر کننده را مشاهده کنید و یک نسخه جدید از همان گواهی را با استفاده از CSR جدید برای سرور دوم وب خود درخواست کنید، ممکن است متوجه شوید که همه چیز برای چند روز خوب است، اما بعد ناگهان سرور اصلی وب اعتبارسنجی ترافیک را متوقف می‌کند زیرا گواهی SSL منقضی شده است.

چه کاری باید انجام دهیم؟ هنگامی که شما نیاز به استفاده مجدد از گواهی SSL یکسانی روی چند سرور دارید، شما می‌توانید به راحتی آن‌را خارج (export) کرده و به سرور مورد نظر وارد کنید. در این حالت نیازی نیست با مرجع صادرکننده تماس برقرار کنید. این فرآیند کاملا ساده است و دو گزینه برای انجام این‌کار وجود دارد. از MMC استفاده کرده یا به سراغ IIS رفته و از آن استفاده کنید. بسته به گزینه‌ای که انتخاب می‌کنید، مراحلی که باید پشت سر بگذارید متفاوت است. در هر دو حالت باید مواظب باشید که چه اتفاقی برای کلید خصوصی رخ می‌دهد.

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

:□□□□ □□□□ □□□□□□ □□□□□ □□□□□□ □□□□□□ □□□□ □□□□□□ □□□□□ 2019 □□□ □□□□ □□□□□ □□□ □□□□□

[□□□□□ □□□□□□ □□□□□□ □□□□ 2019](#)

تاریخ انتشار:
20 شهریور 1398

نشانی منبع:
https://www.shabakeh-mag.com/networking-technology/16013/%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%AF%D8%B1%DB%8C%D8%A7%D9%81%D8%AA-%DA%A9%D8%B1%D8%AF%D9%87-%D9%88-%D8%A2%D9%86%E2%80%8C%D8%B1%D8%A7-%D8%B1%D9%88%DB%8C-%D9%88%DB%8C%D9%86%D8%AF%D9%88%D8%B2-%D8%B3%D8%B1%D9%88%D8%B1-2019-%D9%86%D8%B5%D8%A8-%DA%A9%D9%86%DB%8C%D9%85%D8%9F