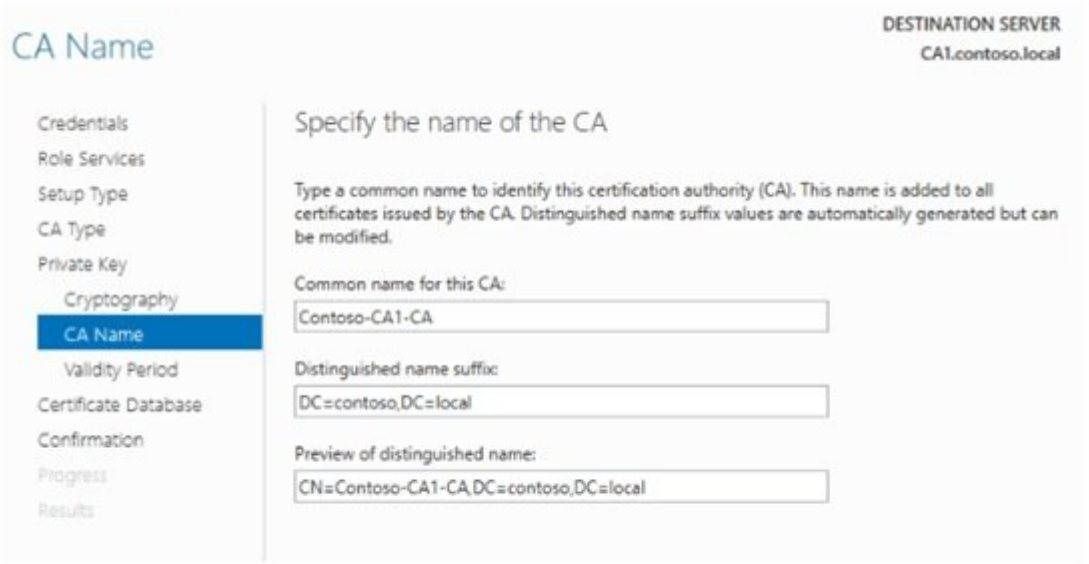
نحوه ساخت گواهی‌نامه‌ها و الگوها در ویندوز سرور 2019 و انتشار آن‌ها

ایجاد گواهی‌نامه‌ها و الگوها یکی از وظایف اصلی مدیران شبکه است. اگر مهارت شما در زمینه ایجاد، مدیریت و کنترل بر نحوه تخصیص مجوزه‌ها به کامپیوترها و کاربران ضعیف باشد، در آینده با مشکلات عدیده‌ای همچون دسترسی‌های غیرمجاز یا عدم اتصال درست کامپیوترها و کاربران به ابزارها و فناوری‌ها روبرو خواهید شد.

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

نام‌گذاری سرور مرجع صدور گواهینامه

اکنون که نقش فوق را نصب کردید در مرحله بعد باید نام میزبان سرور را انتخاب کنید. زمانی‌که برای اولین بار از ویزارد برای پیکربندی CA خود استفاده می‌کنید با صفحه‌ای به‌نام مشخص کردن نام CA روبرو می‌شوید. تعجب کرده‌اید؟ ما قبلا نام میزبان را مشخص کرده‌ایم؟ بله درست است، اما با کمی تفاوت! ما نام میزبان نهایی خود را داریم و نام سرور را با یکپارچه کردن سرور با دامنه و اکتیو دایرکتوری مشخص کردیم، اما تعیین نام CA Name موضوع دیگری است. این نامی است که درون خاصیت‌های هر گواهی‌نامه‌ای که CA صادر می‌کند، ظاهر خواهد شد. این نام در بخش‌های مختلف درون اکتیو دایرکتوری پیکربندی می‌شود، زیرا ما در حال ساخت یک Enterprise CA هستیم. ویزارد به شکل خود تعریفی نامی که قادر به استفاده از آن هستید را مشخص می‌کند که بسیاری از مدیران شبکه به سادگی از آن استفاده می‌کنند. اگر می‌خواهید نام موردنظر خود را پیکربندی کنید، باید آن‌را مشخص کنید. نام ثابت CA به صورت زیر تعریف می‌شود.



آیا می‌توانیم نقش CA را روی یک کنترل‌کننده دامنه نصب کنم؟

با توجه به این‌که این نقش به‌طور رسمی یکی از نقش‌های Active Directory Certificate Service است، این امکان وجود دارد که آن‌را روی یکی از سرورهای کنترل دامنه خود نصب کنیم؟ متأسفانه پاسخ منفی است. بسیاری از مشاغل کوچک و متوسط این‌کار را انجام می‌دهند و برخی از آن‌هایی که خوش شانس هستند با انجام این‌کار به مشکلات جدی برخورد نمی‌کنند، به عبارت دقیق‌تر به لحاظ فنی این امکان وجود دارد، اما مایکروسافت این موضوع را تایید نمی‌کند و پیشنهاد می‌کند CA را روی سرورهای خودتان بسازید. سعی کنید تا جایی که امکان دارد این نقش را با سایر نقش‌ها روی سرور یکسان میزبانی نکنید.

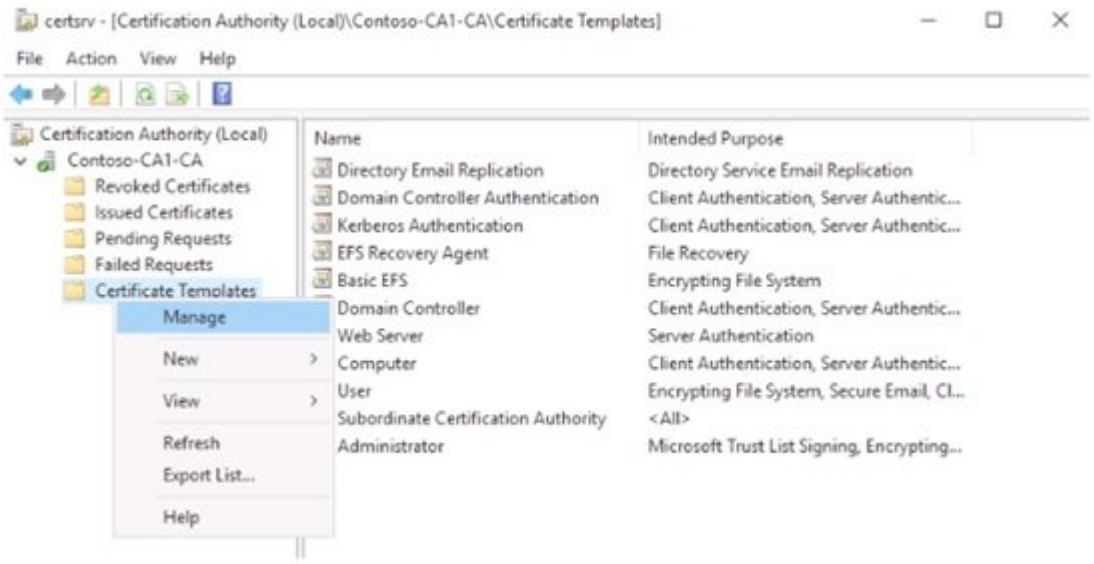
ایجاد یک الگوی گواهی جدید

وقت آن رسیده تا یکسری کارهای عملی انجام دهیم. حالا که نقش CA نصب شده است، بگذارید کمی آن‌را ویرایش کنیم. هدف از سرور گواهینامه صدور گواهینامه است، بنابراین ، باید کاری انجام دهیم؟ اما عجله نکنید. زمانی‌که تصمیم می‌گیرید گواهینامه‌ای از سرور CA را به یك دستگاه یا کاربر اختصاص دهید، شما این موضوع را انتخاب نمی‌کنید که کدام گواهینامه را مستقر کنید، بلکه الگوی گواهی که در نظر دارید مستقر کنید را مشخص می‌کنید تا در ادامه بتوانید از یک گواهی که بر اساس تنظیمات الگو پیکربندی شده استفاده کنید. الگوهای گواهینامه عملکردی شبیه به دستورالعمل طبخ غذا دارند. شما در سرور CA، الگوهای خود را ایجاد می‌کنید و کلیه ملزومات یا تنظیمات خاص را که می‌خواهید در گواهی نهایی درج شوند را مشخص می‌کنید. در ادامه، وقتی کاربران یا کامپیوترها درخواست یک گواهینامه از سرور CA را ارائه می‌دهند، آن‌ها گواهی‌نامه را بر مبنای دستورالعملی که از پیش تدوین شده روی ماشین‌ها نصب می‌کنند و به سرور CA اعلام می‌کنند کدامیک از دستورالعمل‌های الگو را باید برای ساخت گواهی موردنیازشان به کار ببرد.

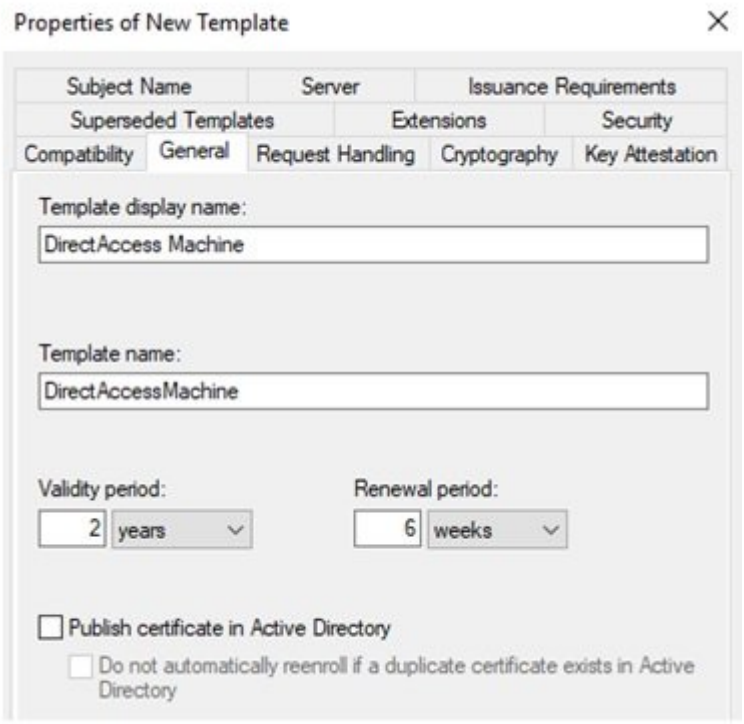
در مدت زمان پیکربندی اولین سرور CA یکسری الگوهای گواهی از پیش ساخته در کنسول را مشاهده می‌کنید. یکی از این قالب‌های از پیش ساخته شده Computer نام دارد که به‌طور معمول از پیش تنظیم شده است تا اگر یک کامپیوتر کلاینت یک گواهی کامپیوتر را از CA جدید درخواست کرد سرور بتواند با موفقیت گواهینامه فوق را صادر کند. با این حال، الگوها و گواهی‌نامه‌های از پیش ساخته شده در همه موارد راهگشا نیستند. برخی موارد مجبور می‌شوید الگوی خود را ایجاد کنید تا بتوانید تنظیمات و پیکربندی خاصی را روی یک الگو اعمال کنید. در این حالت شما دقیقا می‌دانید چه تنظیماتی در گواهینامه‌ها وجود دارد و با آسودگی خیال می‌توانید از گواهی‌نامه که ایجاد کرده‌اید برای کامپیوترهای تحت شبکه استفاده کنید.

برای این منظور، باید یکبار دیگر به کنسول مدیریتی وارد شویم تا بتوانیم چنین کاری را انجام دهیم. در منوی Tools از ابزار Server Manager، روی گزینه Certification Authority کلیک کنید. پس از ورود به این بخش، می‌توانید

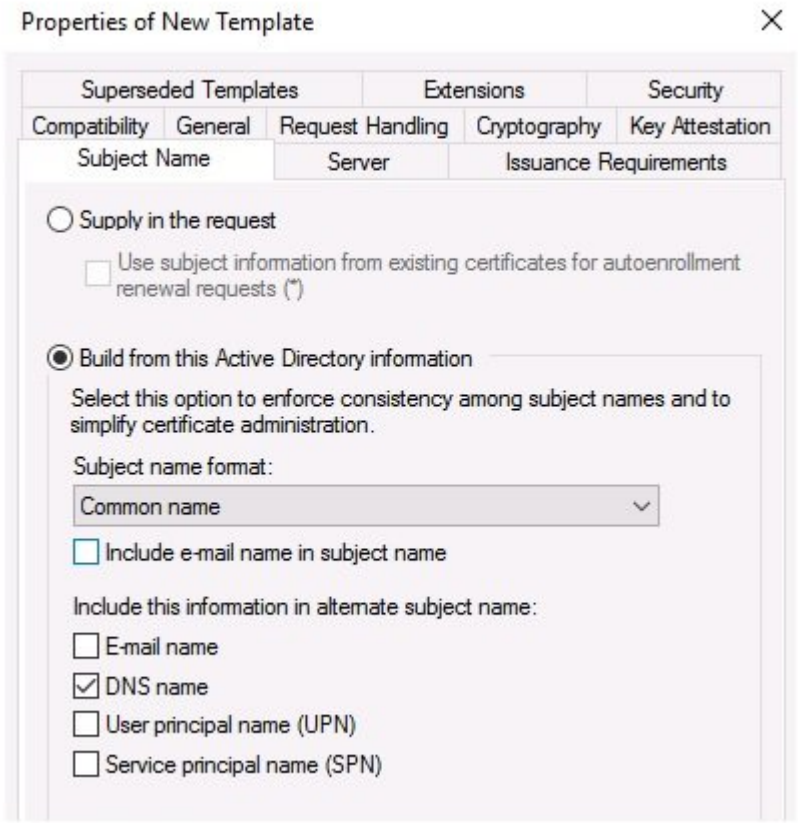
نام مرجع صدور گواهی‌نامه را باز کنید تا یکسری از پوشه‌ها ظاهر شوند. یکی از پوشه‌های درون این قسمت Certificate Templates نام دارد. اگر روی این پوشه کلیک کنید، فهرستی از قالب‌هایی را مشاهده می‌کنید که در حال حاضر در سرور CA ما ساخته شده‌اند. از آن‌جایی که نمی‌خواهیم این قالب‌های از پیش ساخته شده را استفاده کنیم، بهتر است در این بخش کلیک راست کرده و یک الگوی جدید ایجاد کنیم، اما کلیک راست در این بخش مکان صحیحی برای ساخت یک الگوی جدید نیست. زیرا قالب‌های گواهی‌نامه‌ها در این مکان به درستی ایجاد نمی‌شوند و باید در زمان ایجاد درجه بالایی داشته باشند، به همین دلیل به صفحه دوم می‌رویم، جایی که قادر هستیم یک مدیریت و ویرایش دقیق روی الگوها اعمال کنیم. بنابراین روی پوشه Certificate Templates کلیک راست کرده و سپس گزینه Manage را انتخاب کنید.



اکنون فهرست جامع‌تری از قالب‌ها را مشاهده می‌کنید که برخی از آن‌ها در صفحه اول قابل مشاهده نبودند. برای ساخت یک الگوی جدید، کاری که می‌خواهیم انجام دهیم این است که یک الگوی از پیش ساخته شده با عملکردی مشابه با هدف‌مان را پیدا کرده و الگوی گواهی جدید خود را بر مبنای آن ایجاد کنیم. قالب‌های Computer رایج‌تر هستند، زیر اغلب سازمان‌ها روزبه‌روز از فناوری‌های بیشتر و بیشتری استفاده می‌کنند که به این گواهینامه‌ها نیاز دارند. البته همان‌گونه که گفتیم در نظر نداریم، الگوی از پیش آماده شده را استفاده کنیم، زیرا می‌خواهیم از یک نام خاص‌تر استفاده کرده و همچنین مدت اعتبار گواهی‌نامه نیز بیشتر از مقدار پیش‌فرض باشد. روی الگوی Computer کلیک راست کرده و سپس Duplicate Template را انتخاب می‌کنیم. با این‌کار پنجره Properties برای ایجاد الگوی جدید باز می‌شود. پنجره‌ای که اجازه می‌دهد یک نام منحصر به فرد را درون زبانه General وارد کنیم. در آموزش‌های آتی درباره DirectAccess، فناوری دسترسی از راه دور که در بیشتر محیط‌های امروزی استفاده می‌شود صحبت خواهیم کرد. پیاده‌سازی درست DirectAccess شامل صدور گواهینامه‌های ماشین برای کلیه ایستگاه‌های کاری همراه کلاینت‌ها می‌شود، بنابراین قصد داریم از این الگوی جدید برای این منظور استفاده کنیم. برگه General همچنین فیلدی برای تعیین مدت اعتبار گواهینامه دارد که آن‌را 2 سال مشخص می‌کنیم.

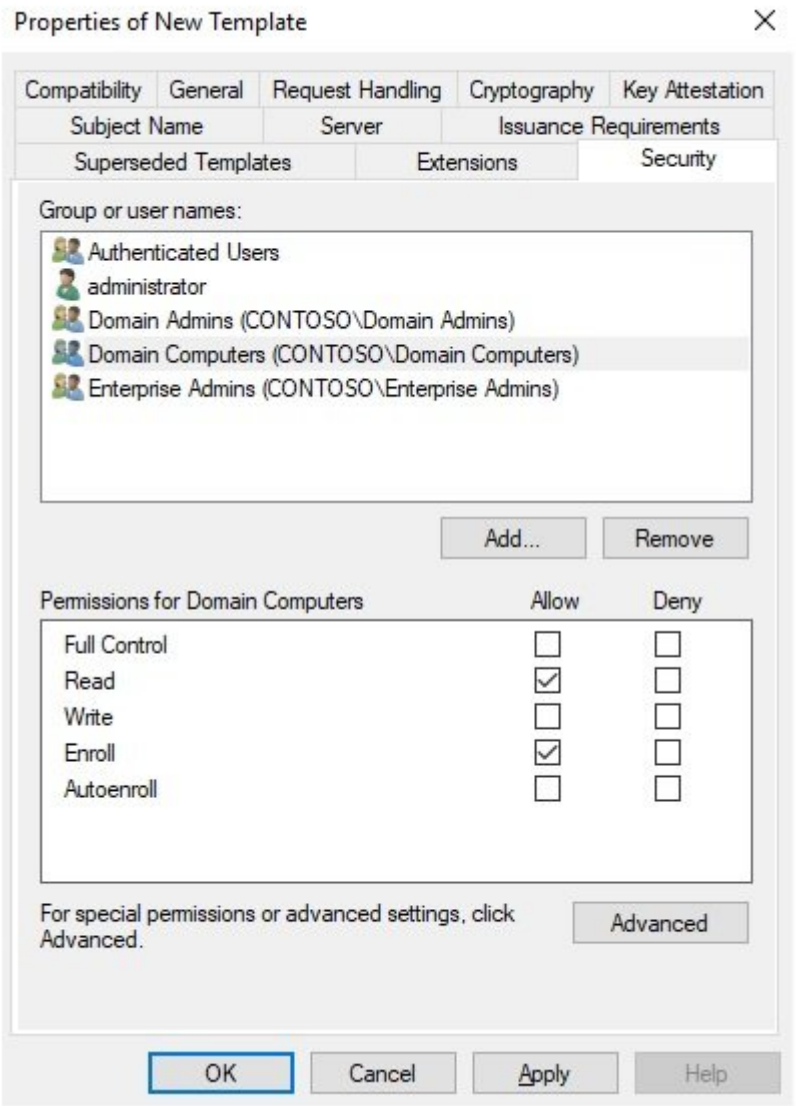


اگر گواهینامه‌هایی را که می‌خواهید صادر کنید نیاز به تغییر تنظیمات بیشتری دارد، باید به زبانه‌های دیگر مراجعه کنید. به‌طور مثال، پارامتر دیگری که قصد تغییر آن‌را داریم در زبانه Subject Name قرار دارد. در نظر دارم گواهینامه‌های جدید من دارای یک نام موضوعی باشند که هماهنگ با نام کامپیوترهایی باشند که گواهی‌نامه برای آن‌ها صادر می‌شود. بنابراین از منوی بازشونده گزینه Common name را انتخاب می‌کنم.



اکنون باید به یک زبانه دیگری برویم، زبانه‌ای که شما برای هر الگوی گواهی که ایجاد می‌کنید باید به آن مراجعه

کنید. این زبانه جدید Security است. می‌خواهیم مطمئن شویم که مجوزهای امنیتی برای این الگو به گونه‌ای تنظیم شده‌اند که اجازه می‌دهند تا گواهی برای کاربران یا کامپیوترهایی که مورد نظر ما قرار دارند صادر شود و در عین حال مطمئن شویم که تنظیمات امنیتی بیش از اندازه ساده نیستند تا به هر شخصی که احتیاجی ندارد، مجوزی را دریافت کند. به‌طور مثال، قصد دارم این گواهینامه‌های DirectAccess را برای تمام کامپیوترهای موجود در دامنه صادر کنم، زیرا نوع گواهی ماشین که من ایجاد کردم قادر است برای احراز هویت عمومی IPsec نیز استفاده شود که ممکن است روزی آن‌را پیکربندی کنم. بنابراین، مطمئن می‌شوم Domain Computer در زبانه Security قید شده است و وضعیت مجوزهای آن به صورت Read and Enroll ، تنظیم شده است، به‌طوری که هر کامپیوتری که به دامنه ملحق می‌شود، امکان درخواست گواهی جدید را بر اساس الگوی جدید من داشته باشد.



از آن‌جایی که این چیزی است که من در گواهینامه جدید خود نیاز دارم، به سادگی روی OK کلیک می‌کنم تا الگوی گواهی جدید من در فهرست قالب‌های سرور CA قرار بگیرد.

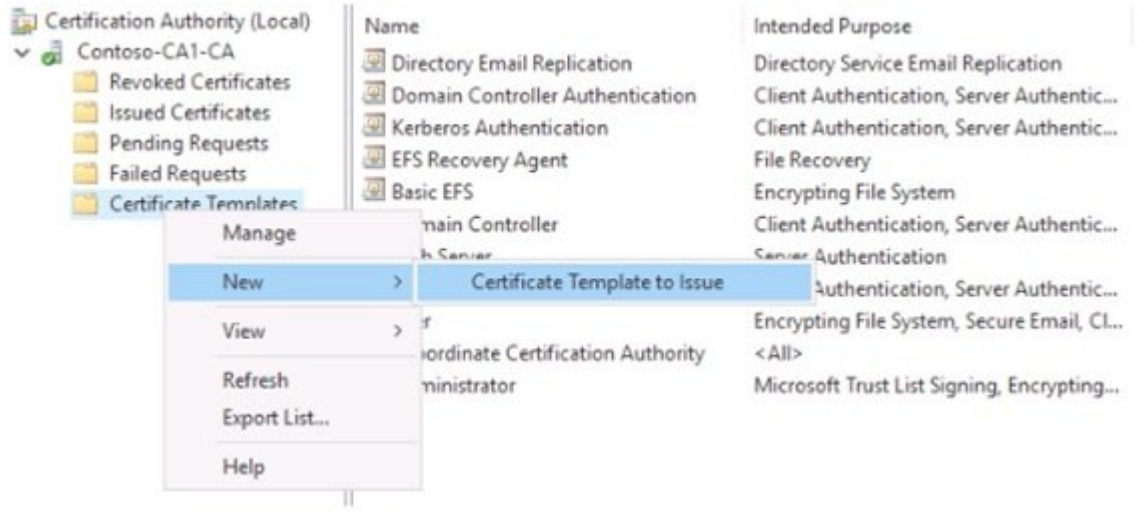
گواهینامه جدید خود را منتشر کنید

زمانی که گواهی‌نامه خود را ایجاد کردید، در مرحله بعد باید آن‌را منتشر کنید. در حال حاضر الگوی کاملا جدیدی برای صدور در اختیار دارید و اطمینان دارید که مجوزهای موجود در آن الگوی گواهی به درستی پیکربندی شده‌اند، به‌طوری که هر کامپیوتری که عضو دامنه است، این توانایی را داشته باشد تا برای بهره‌مندی از گواهی‌نامه فوق درخواستی را ارائه دهد. بنابراین در مرحله بعد باید به کامپیوتر کلاینت برویم و درخواست گواهینامه بدهیم، اما پیش از انجام این‌کار باید یک کار اضافی دیگر نیز انجام دهید تا مطمئن شوید همه چیز به درستی کار می‌کند.

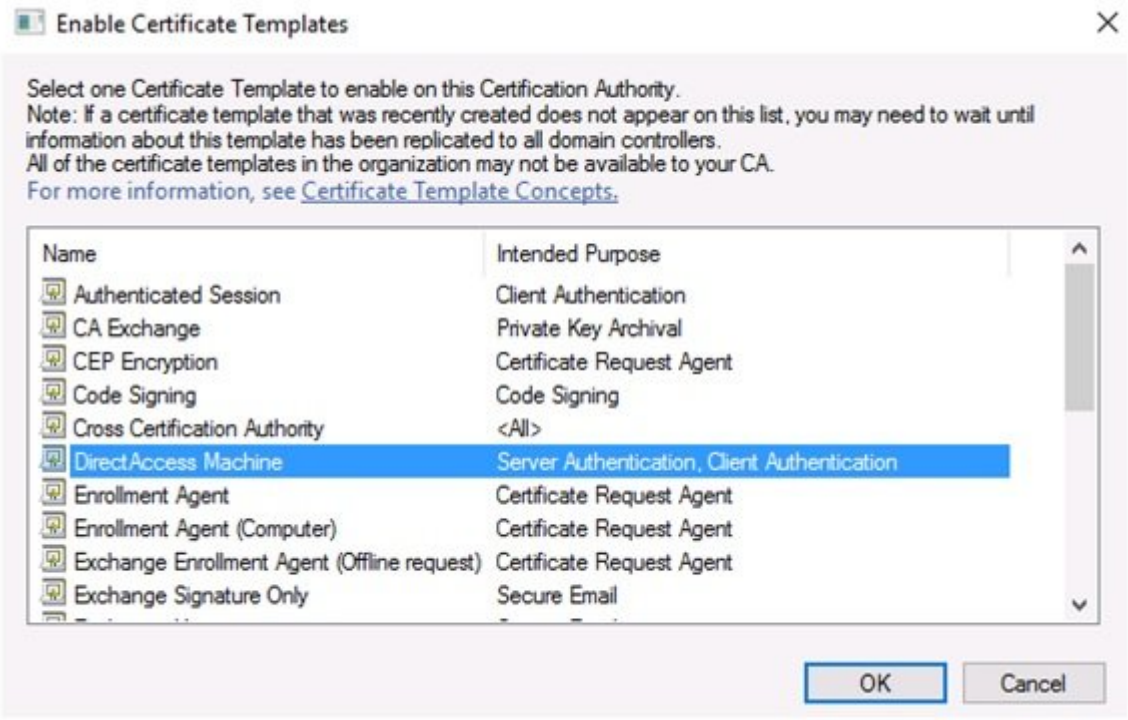
درست است که الگوی جدید ایجاد شده، اما هنوز منتشر نشده است. بنابراین در حال حاضر، سرور CA الگوی جدید ما را به عنوان گزینه‌ای در اختیار کلاینت‌ها قرار نمی‌دهد. حتی اگر مجوزهای امنیتی برای این کار پیکربندی شده باشند. روند انتشار یک گواهینامه بسیار سریع بوده و تنها به چند کلیک ماوس نیاز دارد.

انتشار الگو

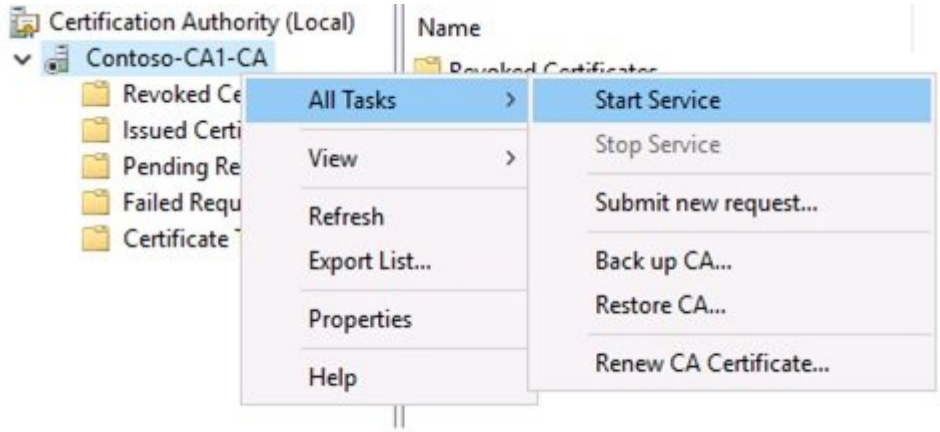
اگر کنسول Certificate Templates هنوز باز است(همان مکانی که ما در آن الگوهای خود را مدیریت کردیم)، آن‌را ببندید تا به کنسول مدیریت مرجع صدور گواهی‌نامه اصلی بروید. متوجه شده‌اید فهرست الگوهای موجود در گواهی‌نامه‌های این بخش کوتاه‌تر از قبل شده است، دلیل این امر این است که فقط الگوهای گواهینامه انتشار یافته و آماده برای انتشار در این بخش نشان داده می‌شود. برای اضافه کردن قالب‌های اضافی به فهرست انتشار از جمله مورد جدید ما، به سادگی روی پوشه Certificate Templates کلیک راست کرده و New |Certificate Template to Issue را انتخاب کنید.



اکنون فهرستی از الگوهای موجود که هنوز منتشر نشده‌اند نشان داده می‌شود. تنها کاری که باید انجام دهید این است که از فهرست موجود الگوی جدید خود انتخاب کرده و روی OK کلیک کنید. الگوی جدید در فهرست الگوهای صدور گواهینامه منتشر شده قرار می‌گیرد. اکنون می‌توانیم از یکی از کامپیوترهای کلاینت درخواستی را ارائه دهیم:



اگر این فهرست را جست‌وجو کردید و الگوی تازه ایجاد شده را مشاهده نکردید، باید یک قدم دیگر بردارید. گاهی اوقات دلیل عدم نمایش الگوی جدید در فهرست این دلیل است که باید منتظر شوید تا کنترل‌های دامنه فرآیند تکثیر را به پایان برسانند. در برخی مواقع متوجه خواهید شد که حتی پس از مدتی انتظار، الگوی جدید شما هنوز در این فهرست نیست. در این حالت، فقط باید سرویس مرجع صدور گواهی‌نامه را ملزم کنید تا اطلاعات الگوی جدید را قید کند. برای راه‌اندازی مجدد سرویس CA، روی نام CA در نزدیکی بالای کنسول مدیریت صدور گواهینامه (Certification Authority) کلیک راست کرده و به All Tasks|Stop بروید. فرآیند توقف سرویس به‌طور معمول فقط یک یا دو ثانیه طول می‌کشد و بلافاصله می‌توانید روی نام CA کلیک راست کنید و این بار به | All Tasks Start Service بروید. حالا سعی کنید دوباره الگوی جدید خود را منتشر کنید. اکنون باید آن‌را در این فهرست مشاهده کنید:



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:

09 شهریور 1398

نشانی منبع:
https://www.shabakeh-mag.com/networking-technology/15990/%D9%86%D8%AD%D9%88%D9%87-%D8%B3%D8%A7%D8%AE%D8%AA-%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-%D9%88-%D8%A7%D9%84%DA%AF%D9%88%D9%87%D8%A7-%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-%D9%88-%D8%A7%D9%86%D8%AA%D8%B4%D8%A7%D8%B1-%D8%A2%D9%86%E2%80%8C%D9%87%D8%A7