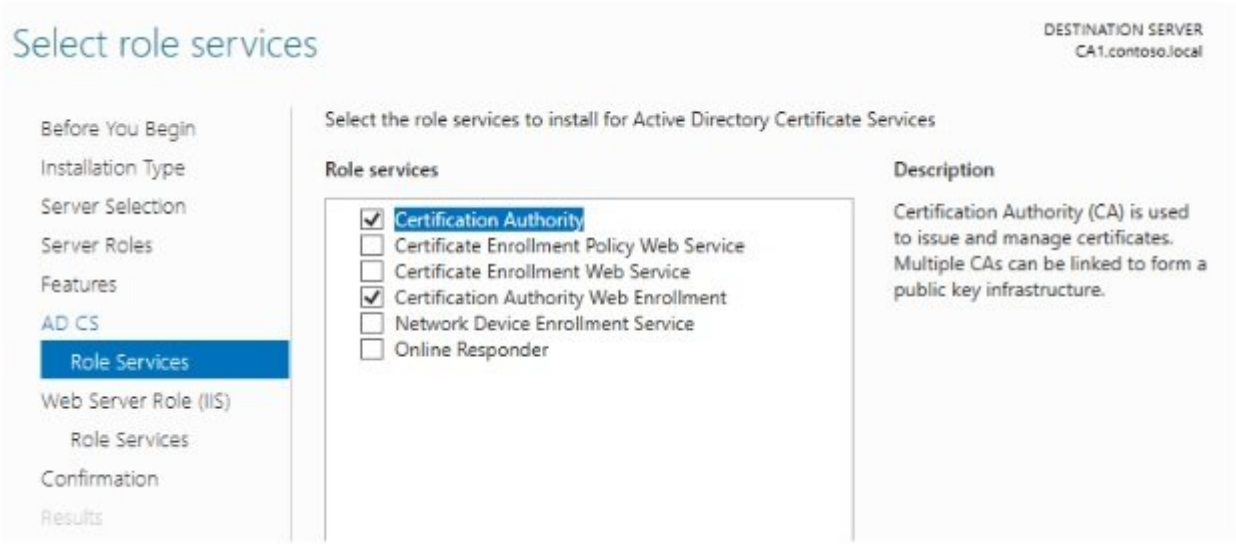
آشنایی با انواع مختلف مراجع صدور گواهی‌نامه سازمانی و مستقل در ویندوز سرور 2019

برای آن‌که زیرساخت کلید مجازی خود را پیاده‌سازی کنید، در اولین گام باید نقش خدمات صدور گواهی‌نامه اکتیودایرکتوری را روی ویندوز سرور نصب کرده و نوع آن را مشخص کنید.

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

زیرساخت کلید مجازی خود را برنامه‌ریزی کنید

از آن‌جایی که آموزش ما حول محور **ویندوز سرور 2019** است، در نتیجه سرور CA شما باید به جدیدترین نسخه از سیستم‌عامل ویندوز سرور تجهیز شده باشد. همانند سایر نقش‌هایی که در **سرور 2019** وجود دارد و با نحوه نصب برخی از آن‌ها آشنا شدید، ساخت سرور صدور گواهی‌نامه در شبکه‌ای که در اختیار دارید به سادگی نصب نقش‌ها در ویندوز است. زمانی‌که تصمیم دارید نقشی را به یک سرور جدید اضافه کنید، اولین نقشی که در این زمینه باید نصب کنید، نقش خدمات صدور گواهینامه اکتیو دایرکتوری (AD CS) سرنام Active Directory Certificate Services است. هنگام نصب این نقش باید به دو نکته مهم پیش از ایجاد یک محیط زیرساخت کلید عمومی پایدار دقت کنید. زمانی که در حال نصب نقش AD CS هستید، اولین تصمیمی که باید اتخاذ کنید انتخاب سرویس‌هایی است که برای انجام کارهای خود باید آن‌ها را نصب کنید. تصویر زیر این موضوع را نشان می‌دهد.



با کلیک روی هر گزینه، توضیحی در مورد قابلیت‌های هر سرویس نشان داده می‌شود که به شما در انتخاب نقشی که به آن نیاز دارید کمک می‌کند. اجازه دهید توضیح مختصری در مورد این گزینه‌ها ارائه کنیم، زیرا ممکن است در آینده به آن‌ها نیاز پیدا کنید.

Certification Authority: سرویس فوق موتور گواهی اولیه است که برای آن‌که یک سرور به یک سرور مرجع صدور گواهی‌نامه رسمی تبدیل شود باید آن‌را نصب کنید.

Certification Authority Web Enrollment: غالباً این سرویس نصب می‌شود، به ویژه در محیط‌هایی که به اندازه کافی کوچک هستند که یک سرور CA تکی به تنهایی بتواند کل محیط را پشتیبانی کند. بخش web-enrollment قابلیت‌های IIS (وب‌سرور) را روی سرور مدنظر نصب می‌کند و وب‌سایت کوچکی که برای مدیریت درخواست گواهینامه‌ها از آن استفاده می‌شود را راه‌اندازی می‌کند.

Certificate Enrollment Web Service and Certificate Enrollment Policy Web Service: در بیشتر مواقع، تنها دغدغه ما صدور گواهینامه‌هایی برای سامانه‌های متصل به دامنه و خود شرکت است. در نتیجه سرویس فوق زمانی نیاز است که قصد دارید از این سرور CA برای صدور گواهینامه برای کامپیوترهایی که عضو دامنه نیستند استفاده کنید. در این حالت باید سرویس فوق روی سرور نصب شود.

Network Device Enrollment Service: همان‌گونه که از نام این سرویس مشخص است، این بخش از CA امکان انتشار گواهینامه برای روترها و انواع دیگر دستگاه‌های شبکه را ارائه می‌کند.

Online Responder: کاربرد این سرویس در ارتباط با محیط‌های سازمانی بزرگ است. درون هر گواهینامه ویژگی‌هایی در ارتباط با فهرست ابطال مجوز (CRL) وجود دارد. هنگامی که یک کامپیوتر کلاینت از یک گواهی‌نامه استفاده می‌کند، قادر است از ویژگی CRL استفاده کند تا مطمئن شود گواهی‌نامه‌ای که از آن استفاده می‌کند ابطال نشده است. CRL نقش کلیدی در بحث امنیت گواهینامه‌ها دارد. در محیطی با هزاران کلاینت، CRL ممکن است برای پاسخ‌گویی به حجم بسیار بالایی از پاسخ‌ها همواره مشغول باشد. شما می‌توانید سرورهای CA اضافی را اجرا کنید تا سرویس Online Responder را برای کمک به بارکاری استفاده کنند.

با توجه به هدفی که در آموزش ویندوز سرور 2019 داریم، قصد داریم دو گزینه نشان داده شده در تصویر قبلی را نصب کرده و از آن استفاده کنیم. در اغلب موارد بیشتر مشاغل کوچک و متوسط از دو سرویس Certification Authority و Certification Authority Web Enrollment استفاده می‌کنند.

سازمانی در مقابل مستقل

پس از آن‌که نقش AD CS را نصب کردید، مدیر سرور به شما اطلاع می‌دهد که خدمات گواهی به پیکربندی اضافی نیاز دارند، درست همانند بیشتر نقش‌هایی که روی سرور نصب می‌کنید. هنگامی که برای اولین بار نقش CA خود را

پیکربندی می‌کنید، باید تصمیم بزرگی اتخاذ کنید. سرور CA باید به صورت مرجع صدور گواهی‌نامه سازمانی (Enterprise CA) پیکربندی شود یا باید به صورت مرجع صدور گواهی‌نامه مستقل (Standalone CA) پیکربندی شود.

اجازه دهید کار را با مرجع صدور سازمانی آغاز کنیم. همان‌گونه که ویزارد به شما می‌گوید، یک سرور CA سازمانی باید عضو دامنه شما باشد و این سرورهای گواهی‌نامه به‌طور معمول باید آنلاین باشند تا بتوانند برای کامپیوترها و کاربرانی که نیاز به گواهینامه دارند، گواهی‌نامه مربوطه را در اختیارشان قرار دهند. اگر قصد دارید از این سرور CA برای صدور گواهینامه استفاده کنید، بدیهی است که باید سرور همواره روشن باشد. بیشتر سرورهای CA در یک محیط دامنه، CAهای سازمانی هستند. در هنگام ایجاد یک سرور CA سازمانی، الگوها و برخی اطلاعات خاص گواهی‌نامه درون خود اکتیو دایرکتوری ذخیره می‌شوند که یکپارچگی میان گواهی‌نامه و دامنه را منسجم‌تر می‌کند. اگر این اولین تعامل شما با نقش CA است، توصیه می‌کنم کار را با گواهی‌نامه CA سازمانی آغاز کنید، زیرا در آینده به نیازهای سازمانی به درستی پاسخ خواهد داد.

همان‌گونه که ممکن است از پاراگراف قبل متوجه شده باشید، مرجع صدور گواهی مستقل کمتر استفاده می‌شود. مستقل‌ها می‌توانند عضوی از دامنه باشند یا می‌توانند بخشی جدا از شبکه باشند و درون یک کارگروه محلی قرار بگیرند. اگر دغدغه‌های امنیتی دارید که سرور گواهینامه شما نباید به دامنه ملحق شود، گزینه مرجع صدور گواهی مستقل برای شما در نظر گرفته است. همچنین در برخی مواقع که اکتیو دایرکتوری به سادگی در محیط انتخابی در دسترس نیست شرکت‌ها از مرجع صدور گواهی مستقل استفاده می‌کنند. به اعتقاد من، شما به ندرت شبکه‌ای پیدا می‌کنید که شخصی سعی کرده باشد از ویندوز سرور 2019 به عنوان یک مرجع صدور گواهی‌نامه استفاده کند و در عین حال AD DS یا همان Active Directory Domain Services را نصب نکرده باشد، اگر در چنین شرایطی خود را گرفتار دیدید، باید گزینه Standalone را انتخاب کنید. سومین عاملی که باعث می‌شود گزینه فوق را انتخاب کنید، در شرایطی است که مجبور هستید سرور خود را خاموش کنید. ما یک چنین سناریویی را ریشه آفلاین می‌نامیم. ما هنوز درباره مرجع صدور ریشه صحبت نکرده‌ایم، اما صبور باشید. هنگامی که یک ریشه آفلاین را اجرا کرده و از آن استفاده می‌کنید سطح بالای سلسله مراتب زیرساخت کلید مجازی خود را به عنوان مرجع صدور ریشه مستقل ایجاد می‌کنید و سپس مراجع صدور پایین دستی را زیر آن ایجاد می‌کنید. مراجع صدور گواهی‌نامه تابعه یا همان پایین دستی مولفه‌هایی هستند که چندان ایمن نیستند و در نتیجه می‌توان در مواقع لازم با خیال راحت ریشه را خاموش کرد. اکثر شرکت‌ها چنین کاری را انجام نمی‌دهند، اما برخی از شرکت‌ها که خط‌مشی‌های امنیتی بسیار سطح بالایی دارند به یک چنین کاری نیاز دارند. اگر کلیه سرورهای مرجع صدور گواهی‌نامه یک شرکت به شکل Enterprise CA تنظیم شده و ارتباط گره خورده‌ای باهم داشته باشند به‌طوری که تمام اطلاعاتشان درون اکتیو دایرکتوری ذخیره شده باشد، این احتمال وجود دارد که در زمان حمله به یکی از مراجع صدور گواهی‌نامه پایین دستی کل زیرساخت کلید عمومی با یک فاجعه عظیم یا یک حمله هکری روبرو شود. تنها راه خلاصی از چنین حمله‌ای این است که کل محیط زیرساخت کلید عمومی و همه سرورهای مرجع صدور گواهی‌نامه را پاک کرده و دومرتبه آن‌ها را ایجاد کنید. اگر مجبور شدید چنین کاری را انجام دهید، نه تنها باید سرورها را دومرتبه ایجاد کنید، بلکه باید نسخه‌های جدیدی از همه گواهینامه‌های خود را دومرتبه منتشر کرده و در اختیار کاربران و دستگاه‌های مختلف قرار دهید.

در نقطه مقابل، اگر از یک مرجع صدور گواهی‌نامه ریشه مستقل استفاده کنید که در وضعیت آفلاین قرار داشته باشد، یک چنین حمله‌ای آن‌را آلوده نخواهد کرد. در این حالت، شما می‌توانید سرورهای صدور مجوز گواهی آلوده را خاموش کنید، در حالی که سرور ریشه مرکزی را با خیال آسوده پنهان نگه دارید. در ادامه می‌توانید این ریشه را به وضعیت آنلاین درآورده، ، مراجع صدور فرعی جدید را دومرتبه ایجاد کرده و از یک مسیر صد در صد ساده و راحت برای عملیاتی کردن آن‌ها استفاده کنید، زیرا کلیدهای ریشه شما که در CA ذخیره شده‌اند نیازی به بازنشر مجدد ندارند و هیچ‌گاه در معرض حمله قرار نگرفته‌اند.

همان‌گونه که اشاره کردم، ما یک چنین وضعیتی را زیاد مشاهده نمی‌کنیم، اما احتمال وجود آن همواره وجود دارد. اگر علاقمند به یادگیری بیشتر در مورد مراجع صدور گواهی‌نامه ریشه آفلاین و کاربردهای آن‌ها هستید، پیشنهاد می‌کنم به مقاله سایت TechNet به نشانی زیر مراجعه کنید.

http://social.technet.microsoft.com/wiki/contents/articles/2900.offline-root-certification-authority-ca.aspx

اگر فکر می‌کنید که مهاجرت به مرجع صدور گواهی‌نامه آفلاین به دلیل ایمن بودن آن کار درستی است، اما دلیل خاصی برای این کار ندارید، توصیه می‌کنم صبر کنید و از یک ریشه آنلاین CA استفاده کنید. درست است که یکسری مزایای امنیتی در ارتباط با ریشه آفلاین وجود دارد، اما اکثر شرکت‌ها حاضر نیستند به دلیل کار مضاعفی که برای استفاده از یک مرجع صدور گواهی‌نامه آفلاین باید متحمل شوند از آن استفاده کنند. در بیشتر موارد شما از مرجع صدور گواهی سازمانی استفاده خواهید کرد، کاری که ما در این مقاله انجام می‌دهیم.

ریشه در مقابل پایین دستی (Root versus Subordinate)

این دومین انتخاب بزرگی است که باید هنگام ساخت یک مرجع صدور گواهی‌نامه جدید اتخاذ کنید. در نظر دارید سرور جدید شما یک مرجع صدور گواهی‌نامه ریشه (CA Root) باشد یا باید یک مرجع صدور گواهی‌نامه پایین دستی (Subordinate CA) باشد؟ در برخی موارد، حتا در بسیاری از مستندات مایکروسافت آمده است که یک CA پایین دستی اغلب به عنوان CA صادر کننده شناخته می‌شود. به‌طور کلی، در زیرساخت‌های کلید عمومی چند لایه، مرجع صدور پایین دستی/انتشاردهنده هر دو موجودیت واحدی هستند که فرآیند صدور گواهینامه به کاربران و دستگاه‌های شبکه را مدیریت می‌کنند.

تفاوت در واقع تنها مربوط به سلسله مراتب CA می‌شود که به آن نیاز دارید. در یک درخت زیرساخت کلید عمومی، یک گواهی سطح بالا وجود دارد که توسط خود ریشه CA امضا شده و همه چیز به آن متصل شده است. در طرف دیگر، یک مرجع صدور گواهی‌نامه پایین دستی در زیرمجموعه مرجع صدور گواهی‌نامه ریشه قرار دارد و گواهی‌نامه خاص خود را از ریشه بالای خود صادر می‌کند.

اگر به دنبال آن هستید که تنها یک سرور صدور گواهی‌نامه تکی ایجاد کنید باید آن‌را به صورت ریشه ایجاد کنید. اگر استراتژی شما بر مبنای صدور مرتب گواهی‌نامه‌ها است، اولین CA در محیط شما باید ریشه باشد و در ادامه CA پایین‌دستی دیگر قرار بگیرند. شما می‌توانید ریشه‌های متعدد و در نتیجه چندین درخت در یک شبکه داشته باشید. در این حالت نیز می‌توانید یک زیرساخت کلید عمومی ساخت یافته داشته باشید. در شرکت‌های کوچک‌تر، شما تنها یک سرور CA که یک ریشه سازمانی است را مشاهده می‌کنید، زیرا به دنبال سهولت در مدیریت هستند، این شرکت‌ها حاضرند ریسک کرده و این خطر را بپذیرند که اگر اتفاقی برای آن سرور افتاد، ساخت یک سرور جدید و بازنشر دومرتبه گواهی‌نامه‌ها کار چندان سختی نخواهد بود. برای شبکه‌های بزرگ‌تر، شما یک ریشه تکی را با مجموعه‌ای از پایین‌دستی‌ها مشاهده می‌کنید. به‌طور معمول ، در این حالت، CAهای پایین دستی هستند که کار واقعی یعنی صدور گواهینامه به کلاینت‌ها را انجام می‌دهند. در بیشتر موارد ، شما می خواهید Enterprise CA را انتخاب کنید و از آنجا ادامه دهید.

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:
06 شهریور 1398

نشانی منبع:
https://www.shabakeh-mag.com/networking-technology/15979/%D8%A2%D8%B4%D9%86%D8%A7%DB%8C%DB%8C-%D8%A8%D8%A7-%D8%A7%D9%86%D9%88%D8%A7%D8%B9-%D9%85%D8%AE%D8%AA%D9%84%D9%81-%D9%85%D8%B1%D8%A7%D8%AC%D8%B9-%D8%B5%D8%AF%D9%88%D8%B1-%DA%AF%D9%88%D8%A7%D9%87%DB%8C%E2%80%8C%D9%86%D8%A7%D9%85%D9%87-%D8%B3%D8%A7%D8%B2%D9%85%D8%A7%D9%86%DB%8C-%D9%88-

%D9%85%D8%B3%D8%AA%D9%82%D9%84-%D8%AF%D8%B1-
%D9%88%DB%8C%D9%86%D8%AF%D9%88%D8%B2