گواهی‌نامه‌ها چه نقشی در ویندوز سرور 2019 دارند؟

یاد گرفتیم که ابزار عمومی مدیریت در ویندوز سرور 2019 از طریق MMC و MSC در دسترس قرار دارند. بیشتر مدیران شبکه ترجیح می‌دهند از میان‌برهای MSC برای دسترسی سریع‌تر به ابزارهای مدیریت استفاده کنند. شما نیز می‌توانید این میان‌برها را از طریق خط فرمان یا محیط پاورشل اجرا کرده و به ساده‌ترین شکل به ابزارهای مدیریتی دسترسی داشته باشید. در کنار ابزارهای مدیریتی که نقش مهمی در ویندوز سرور 2019 دارند، گواهی‌نامه‌ها نیز نقش بسیار مهمی در مدیریت هرچه دقیق‌تر سرور دارند. گواهی‌نامه‌ها چه مولفه‌هایی هستند؟

میان‌برهای MSC مختلفی وجود دارند که اجازه می‌دهند در کوتاه‌ترین زمان به ابزارهای مدیریتی دسترسی داشته باشید. از مهم‌ترین ابزارهایی که برای مدیریت سرور به آن‌ها نیاز دارید و با استفاده از میان‌برهای MSC به سریع‌ترین شکل در دسترس‌تان خواهد بود به موارد زیر می‌توان اشاره کرد:

- DSA.MSC: Active Directory Users and Computers
- WF.MSC: Windows Defender Firewall with Advanced Security
- DSSITE.MSC: Active Directory Sites and Services
- DNSMGMT.MSC: DNS Manager
- GPEDIT.MSC: Local Group Policy Editor
- GPMC.MSC: Group Policy Management Console
- CERTSRV.MSC: Certification Authority Management
- CERTTMPL.MSC: Certificate Template Management
- CERTLM.MSC: Local Computer Certificates Store
- CERTMGR.MSC: Current User Certificates Store
- COMPMGMT.MSC: Computer Management
- DEVMGMT.MSC: Device Manager
- DHCPMGMT.MSC: DHCP Manager
- DISKMGMT.MSC: Disk Management
- EVENTVWR.MSC: Event Viewer
- PERFMON.MSC: Performance Monitor
- SECPOL.MSC: Local Security Policy Console
- FSMGMT.MSC: Shared Folders

گواهی‌نامه‌ها در ویندوز سرور 2019

به دلایل مختلفی، استفاده از گواهینامه‌ها برای بسیاری از مدیران شبکه حتا آن‌هایی که برای سال‌ها در حوزه فناوری‌اطلاعات مشغول به کار هستند، فرآیند دلهره‌آوری به نظر می‌رسد، زیرا گزینه‌های مختلف زیادی در ارتباط با گواهی‌نامه‌های سرور وجود دارد، اما یک کنسول مدیریتی کاربرپسند از پیش ساخته شده برای کار با انواع مختلفی از گواهی‌نامه‌ها وجود ندارد. همچنین مسائل عمومی دیگری نیز در ارتباط با گواهی‌نامه‌های سرور وجود دارد که امکان پرداختن به آن‌ها در این آموزش وجود ندارد. برخی از مدیران شبکه عادت دارند از فناوری‌هایی استفاده می‌کنند که از گواهی‌نامه‌های سازمانی استفاده می‌کنند و اغلب روی هر ایستگاه کاری در شبکه نصب می‌شوند. اگر هیچ تجربه‌ای در ارتباط با این فرآیند ندارید، ممکن است به‌کارگیری گواهینامه روی یک وب‌سرور تجاری کار ترسناکی به نظر برسد، چه رسد به این‌که مجبور شوید به صدها یا هزاران گواهی‌نامه در یک زمان رسیدگی کنید. سناریوی متداول دیگر حالتی است که در آن یک شرکت، گواهی‌نامه‌های خاص خود را تعیین می‌کند، در حالی که کارمندان قادر به استفاده از آن نیستند، در این حالت سازمان شخص ثالثی را استخدام می‌کند تا گواهی‌نامه‌ها را درون شبکه سازمانی پیاده‌سازی کند. البته این رویکرد به تدریج در حال محو خواهد شد، زیرا شکاف دانشی به وجود می‌آورد که هیچ‌گاه این شکاف پر نخواهد شد، زیرا شما ممکن است از یک گواهی‌نامه روی سرور استفاده کنید، اما هیچ‌گاه در زمان کار با گواهی‌نامه یا ویرایش آن احساس راحتی نکنید.

اصطلاحی که به شکل گسترده برای گواهی‌نامه‌ها استفاده می‌شود، زیرساخت کلید عمومی (PKI) سرنام **Public Key Infrastructure** است. PKI توسط سرورها در شبکه ارائه می‌شود، اما پیکربندی سرورها برای به‌کارگیری و ارائه گواهینامه‌ها فرآیندی است که شما باید آن‌را مدیریت کنید. سرورهایی که تعیین می‌کنید که سرور گواهینامه باشند به عنوان سرورهای صدور گواهینامه (CA) شناخته می‌شوند و ما نیز در آموزش‌های آتی از اصلاح سرورهای CA برای اشاره به آن‌ها استفاده خواهیم کرد.

انواع گواهی‌های رایج

انواع مختلفی از گواهینامه‌ها وجود دارند که ممکن است برای انجام کارهای خود مجبور به انتشار آن‌ها شوید. همان‌گونه که مشاهده خواهید کرد، هنگامی که به گواهینامه‌ای نیاز دارید که فهرستی از الزامات خاص را دارد، شما می‌توانید یک الگوی گواهی را برای هر نوع مشخصه‌ای که مدنظر دارید ایجاد کنید. در این حالت، نوع واقعا خاصی از یک گواهی‌نامه وجود ندارد، بلکه تنها الگوهای گواهی وجود دارند که شما اطلاعاتی که برای انجام فعالیت‌های خود به آن‌ها نیاز داشته‌اید را درون الگوها قرار داده‌اید. به‌طور کلی بهتر است گواهینامه‌ها در گروه‌های مختلف و تفکیک شده قرار گیرند تا مشخص شود هر گواهی‌نامه قرار است چه کاری انجام دهد.

گواهی‌های کاربری

همان‌گونه که از نامش پیدا است، یک گواهینامه کاربری برای یک حساب کاربری استفاده می‌شود. یکی از زیرساخت‌هایی که بیشترین استفاده از گواهی‌نامه‌ها را دارد، زیرساخت تایید اعتبار-شبکه است. شرکت‌هایی که به دنبال تأیید هویت قدرتمندتر در محیط‌های خود هستند، اغلب به عنوان بخشی از فرآیند احراز هویت به گواهینامه‌ها دقت نظر خاصی دارند. کارت‌های هوشمند یکی از مکانیسم‌های خاصی هستند که می‌توانند برای این منظور استفاده شوند. در برخی از سازمان‌ها کاربران برای دسترسی به کامپیوتر خود مجبور هستند کارت فیزیکی را به کامپیوتر متصل کنند.

کارت‌های هوشمند می‌توانند در مکانی خاص روی کامپیوترهای جدیدی که TPM نام دارد به صورت مجازی ذخیره شوند. دلیل این‌که ما در این‌جا به کارت‌های هوشمند اشاره کردیم این است که در بیشتر موارد فرآیند تایید کارت هوشمند از طریق یک گواهی کاربری که درون کارت هوشمند ذخیره شده انجام می‌شود. اگر در یک پروژه مجبور شدید کارت‌های هوشمند را در وضعیت عملیاتی قرار دهید، به احتمال زیاد به زیرساخت PKI احتیاج خواهید داشت.

گواهی‌های کامپیوتر

این گواهی‌ها اغلب به‌نام گواهی‌نامه‌های ماشین یا کامپیوتر شناخته می‌شوند و برای کمک به تعامل بهتر بین شبکه و کامپیوتر استفاده می‌شوند. فناوری‌هایی شبیه به SCCM بدون در نظر گرفتن اینکه چه کاربری به سامانه وارد شده و از گواهی‌نامه کامپیوتری استفاده می‌کند با کامپیوترها ارتباط برقرار کرده و آن‌ها را مدیریت می‌کنند. این نوع گواهینامه‌ها همچنین برای پردازش رمزگذاری بین سیستم‌های موجود در شبکه استفاده می‌شوند به‌عنوان مثال،

زمانی‌که نیاز دارید از IPsec برای رمزگذاری ارتباطات بین کلاینت‌ها و یک فایل سرور بسیار امن استفاده کنید. صدور گواهینامه‌های کامپیوتر یا ماشین برای نقاط انتهایی در این زنجیره ارتباطی برای درست کردن کار لازم است. سازمان‌ها غالبا به منظور احراز هویت تونل‌های DirectAccess، شکل دیگری از دسترسی از راه دور خودکار به دستگاه‌های سازمانی از گواهینامه کامپیوتر استفاده می‌کنند. دلایل و فناوری‌های مختلفی وجود دارند که ممکن است شما را مجبور کنند از این مدل گواهینامه‌ها برای ایستگاه‌ها در محیط سازمانی استفاده کنید.

گواهینامه‌های SSL

اگر خود را در وسط جاده گواهینامه‌ها مشاهده کردید، جایی که یک سرور CA واقعا نقشی در مدیریت گواهی‌نامه‌ها نداشته، اما گواهی‌نامه‌ای را صادر و نصب شده، به احتمال زیاد در حال کار با یک گواهی SSL هستید. SSL از رایج‌ترین گواهینامه‌هایی است که در زیرساخت‌های فناوری امروزی استفاده می‌شود و حتا اگر شما از وجود آن‌ها اطلاعی نداشته باشید و یک سرور CA مستقل هم نداشته باشید، شرکت شما بازهم از گواهینامه‌های SSL استفاده خواهد کرد.

گواهینامه‌های SSL بیشتر برای برقراری امنیت ترافیک وب‌سایت استفاده می‌شوند. هر بار که به یک وب‌سایت می‌روید و HTTPS را در نوار آدرس مشاهده می‌کنید، مرورگر شما با استفاده از یک استریم بسته SSL اطلاعات را بین کامپیوتر و وب‌سروری که در حال بازدید از آن هستید ارسال می‌کند. وب سرور دارای گواهینامه SSL است و مرورگر شما قبل از ورود به صفحه وب، آن گواهی را بررسی می‌کند تا مطمئن شود که گواهی معتبر است و اینکه وب‌سایت واقعاً همان ماهیتی است که به آن اشاره دارد. اگر از گواهینامه‌های SSL در وب‌سایت‌ها استفاده نمی‌کردیم، هر کسی می‌توانست سایت ما را جعل کرده و اطلاعات را به سایت خودش انتقال دهد.

اجازه دهید یک مثال ساده را بررسی کنیم. فرض کنید یکی از کاربران شما از وای‌فای عمومی در یک کافی‌شاپ استفاده می‌کند. یک مهاجم راهی برای دستکاری DNS در آن شبکه وای‌فای پیدا کرده است. زمانی که کاربر سعی می‌کند به آدرس mail.contoso.com مراجعه کند تا از طریق Outlook Web Access ایمیل‌های خود را بررسی کند، مهاجم ترافیک را روبایش کرده و کاربر را به وب‌سایتی که ظاهرا متعلق به پورتال شرکت است هدایت می‌کند، در حالی که کاربر به وب‌سایتی که توسط مهاجم میزبانی می‌شود وارد شده است. قربانی نام کاربری و گذرواژه را وارد می‌کند، اکنون هکر گواهی کاربر را داشته و می‌تواند برای دسترسی واقعی به شبکه از آن استفاده کند. چه عاملی مانع بروز این اتفاق در دنیای واقعی می‌شود؟ گواهینامه‌های SSL. هنگامی که وب‌سایت‌ها و صفحات مهمی همچون ورود به ایمیل به پروتکل HTTPS تجهیز می‌شوند، در این حالت مرورگر کاربران مجبور است تا گواهی SSL که سایت ارائه کرده را بررسی کند. این گواهینامه SSL شامل اطلاعاتی است که فقط شما به عنوان یک شرکت در اختیار دارید و این امکان وجود ندارد تا این اطلاعات را جعل کرد. به این ترتیب، هنگامی که کاربر شما به صفحه ورود به سیستم واقعی دسترسی پیدا می‌کند، مرورگر گواهی SSL را بررسی می‌کند و اگر معتبر بود، اجازه ادامه روند کار را می‌دهد. در بیشتر موارد کاربر حتا به جز نماد قفل کوچکی که در نزدیکی نوار آدرس مرورگر نشان داده می‌شود از وجود این گواهی اطلاعی پیدا نخواهد کرد. از طرف دیگر، اگر ترافیک میان کاربر و سایت در حال رهگیری و هدایت مجدد به وب‌سایت جعلی باشد، وضعیت بررسی گواهینامه SSL خراب گزارش داده شده (زیرا مهاجمان گواهی SSL معتبری برای نام وب‌سایت شرکت شما ندارند) و رهگیری کاربر متوقف می‌شود. در این حالت صفحه هشداری در ارتباط با گواهینامه به کاربر نشان داده می‌شود.

در این مرحله، کاربر باید کار را متوقف و بررسی کند که اشتباهی رخ نداده و با کارمندان IT سازمان تماس گرفته تا موضوع را بررسی کنند. گواهینامه‌های SSL که توسط وب‌سایت‌ها در اینترنت استفاده می‌شوند، متفاوت از گواهی‌نامه‌هایی هستند که سرور CA داخلی یک سازمان از آن استفاده می‌کند. شاید در مورد شرکت‌هایی همچون DigiCert ، Entrust ، Verisign و GoDaddy مطالبی دیده باشید. بیشتر سازمان‌ها از این شرکت‌های مطرح گواهینامه‌های SSL را خریداری می‌کنند، زیرا گواهی‌نامه‌های SSL معتبر و قابل اعتمادی را ارائه می‌کنند. هنگامی که به وب‌سایتی که گواهینامه SSL آن توسط یکی از فروشندگان عمومی ارائه شده مراجعه می‌کنید، کامپیوتر شما به آن گواهی‌نامه اعتماد می‌کند. مراجع صدور گواهی‌نامه‌های عمومی نهادهای شناخته شده هستند که به خاطر توانایی‌شان در صدور ایمن گواهینامه‌های SSL معروف هستند.

تاریخ انتشار:

02 شهریور 1398

نشانی منبع:
https://www.shabakeh-mag.com/networking-technology/15948/%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-%DA%86%D9%87-%D9%86%D9%82%D8%B4%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%AF%D8%A7%D8%B1%D9%86%D8%AF%D8%9F