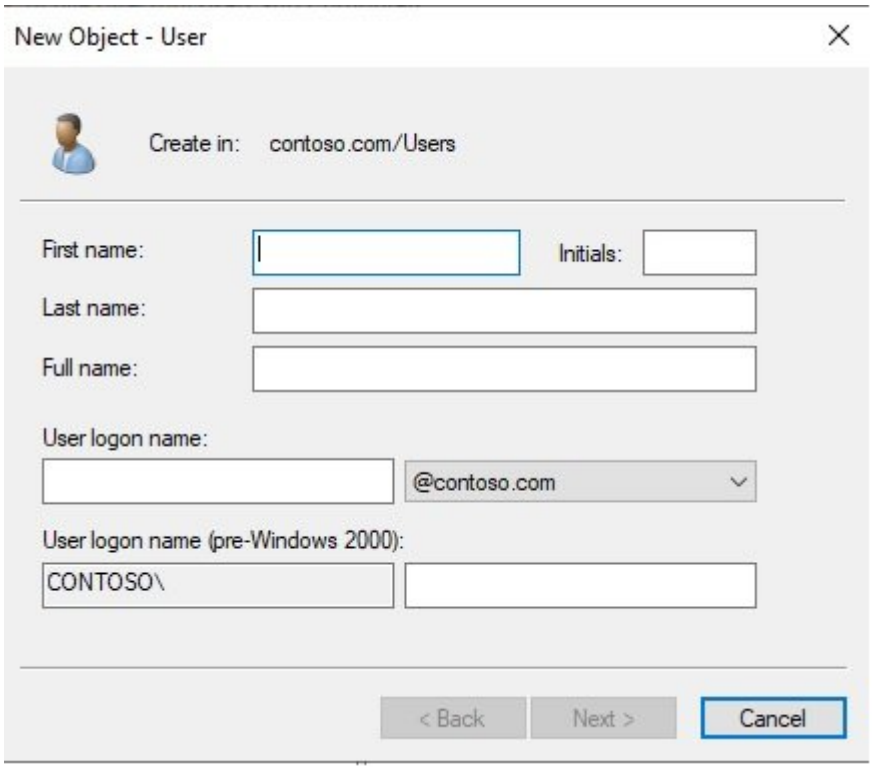
آموزش ویندوز سرور: با User Accounts و Security Groups در ویندوز سرور 2019

ایجاد حساب‌های کاربری، گروه‌های امنیتی و اعتبارسازی حساب‌های کامپیوتری از جمله فرآیندهای مهمی هستند که اجازه می‌دهند، کاربران به شبکه و سرور دسترسی داشته، کاربران درستی به منابع و فایل‌های حساس دسترسی داشته باشند و کامپیوترها به شکل پیش‌فرض به واحدهای سازمانی (OU) عمومی درون اکتیو دایرکتوری اضافه نشوند. در این بخش از آموزش رایگان ویندوز سرور 2019 اجازه دهید به‌طور مختصر و سریع به عملکرد این مولفه‌ها نگاهی داشته باشیم. در آینده به شکل مفصل‌تر هر یک از این ابزارها را بررسی خواهیم کرد.

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

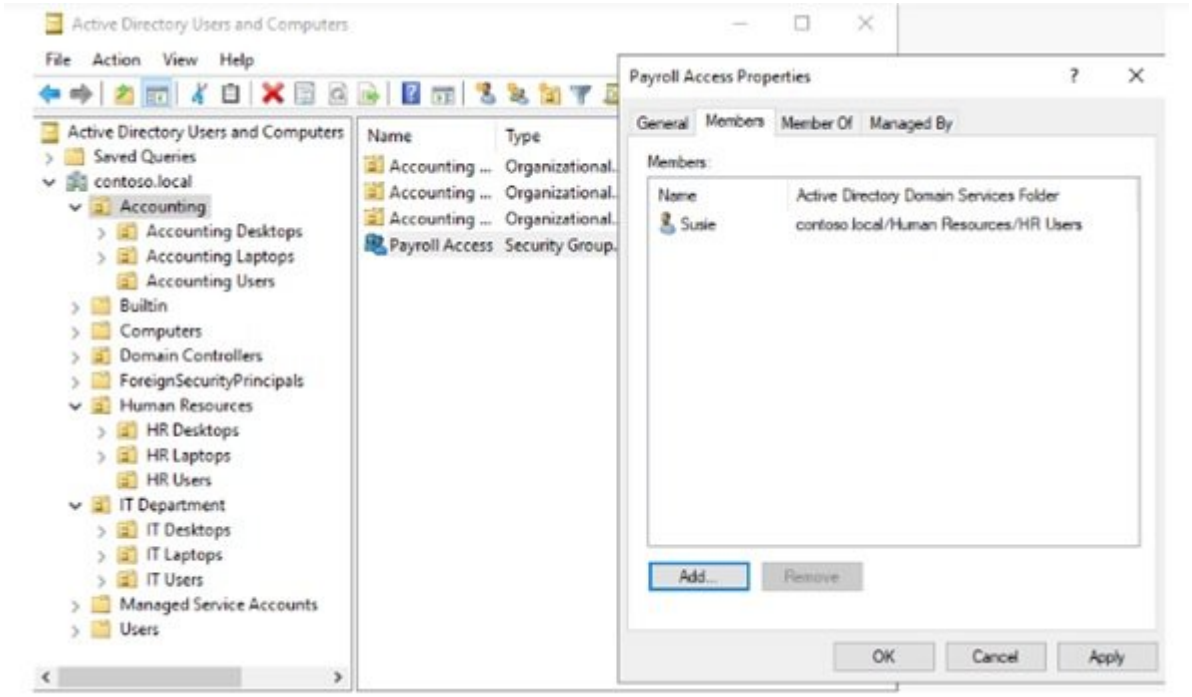
حساب‌های کاربری

زمانی که واحد سازمانی (OU) که قرار است اشیا در آن قرار گیرند را انتخاب کردید، در مرحله باید یک کاربر جدید ایجاد کنید. فرض کنید، یک حساب کاربری Server Administrator داریم و قصد داریم به این حساب کاربری برای ورود به اکتیور دایرکتوری و انجام کارهای خودش مجوزهای لازم را تخصیص دهیم. برای انجام این‌کار ابتدا باید OU مناسب برای این حساب را پیدا کرده، روی OU موردنظر کلیک راست کرده و به بخش User رفته، روی New و سپس User کلیک می‌کنیم. در ادامه پنجره جمع‌آوری اطلاعات درباره همه ملزوماتی که اکتیودایرکتوری برای ساخت یک حساب جدید به آن‌ها نیاز دارد نشان داده می‌شود. بیشتر این اطلاعات حالت خود تعریفی دارند، اما اگر با دنیای اکتیودایرکتوری آشنایی ندارید، باید بدانید که اولین فیلد به نام کاربری واردشونده اشاره دارد. هر اطلاعاتی که در این فیلد قرار داده شود به عنوان نام کاربری رسمی کاربر در شبکه شناخته می‌شود. هر زمان کاربری قصد ورود به یک کامپیوتر یا سرور را داشته باشد، این نام کاربری برای ورود در نظر گرفته می‌شود. زمانی که پیکربندی به پایان رسید، مدیر جدید قادر است از نام کاربری و گذرواژه جدید برای ورود به کامپیوترها و سرورهایی که درون شبکه قرار دارند استفاده کند. پس از اتمام فرآیند فوق، مدیر جدید قادر خواهد بود از نام کاربری و گذرواژه خود برای ورود به کامپیوترها و سرورها در شبکه در محدوده کرانه‌های مرزهای امنیتی که ما روی دستگاه‌ها نصب کرده ایم، استفاده کند.



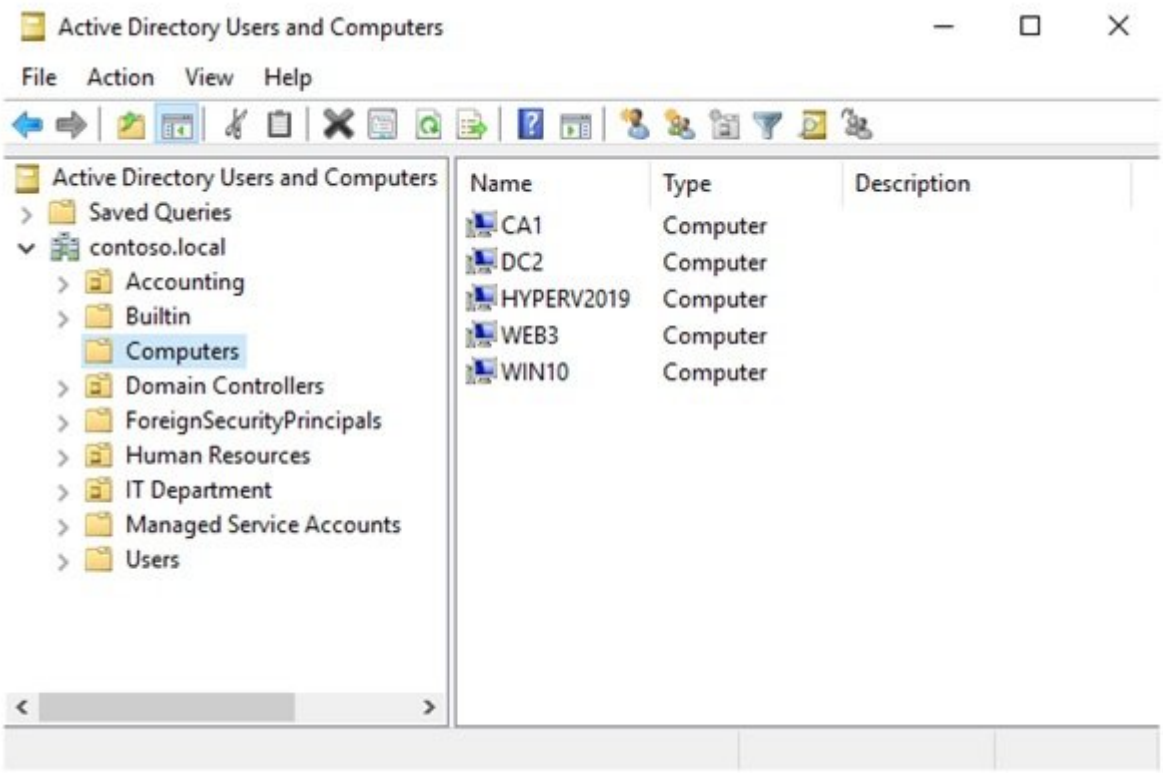
Security Groups

یکی دیگر از OUهای مفید در اکتیودایرکتوری، بخش گروه‌های امنیتی است. ما می‌توانیم با نگاه کردن به OU تمایز بین انواع مختلف حساب‌های کاربران و حساب‌های کامپیوتری را تشخیص دهیم، اما زمانی‌که به اطلاعات دقیق‌تری در ارتباط با ساختارها نیاز داریم باید چه کاری انجام دهیم؟ شاید کارمندی دارید که مسئولیت انجام یکسری کارهای بخش منابع انسانی و حسابداری با او است. در بیشتر موارد مجبور هستیم مجوز دسترسی به فایل‌سرورها را برای گروه‌های خاصی تعیین کنیم تا افراد شاغل در دپارتمان‌های مختلف بتوانند بر مبنای مجوزهای تخصیص داده شده قادر باشند در پوشه‌های خاصی فایل‌ها را خوانده یا محتوای آن‌ها را ویرایش کنند. فرض کنید، کارمندی به نام Susie از بخش منابع انسانی نیاز دارد به پوشه حقوق و دستمزد دسترسی داشته باشد، اما جیم از منابع انسانی نباید چنین دسترسی را داشته باشد. سوزی و جیم هر دو در OU یکسانی قرار دارند و در نتیجه سطح مجوزها و قابلیت‌های مشابهی در اختیار دارند، اما مجبور هستیم به صراحت مشخص کنیم که تنها سوزی است که اجازه دارد به اطلاعات حقوق و دستمزد دسترسی داشته باشد. با ایجاد گروه‌های امنیتی در اکتیو دایرکتوری می‌توانیم کاربران را به حساب‌های کاربری، حساب‌های کامپیوتری و حتا سایر گروه‌ها اضافه و حذف کرده و دسترسی به منابع را به شکل دقیق و روشن برای آن‌ها مشخص کنیم. برای این منظور شما باید گروه‌های جدید را مشابه با حساب‌های کاربری ایجاد کرده و OU مناسبی که قرار است گروه‌های جدید در آن وارد شوند را مشخص کرده و سپس روی OU موردنظر کلیک راست کرده و به بخش New | Group بروید. زمانی که گروه موردنظر را ایجاد کردید، روی آن کلیک راست کرده و به زبانه Properties بروید. در ادامه می‌توانید روی زبانه Members مکانی که همه کاربرانی که قرار است عضو گروه جدید شوند را اضافه کنید. شکل زیر این موضوع را نشان می‌دهد.



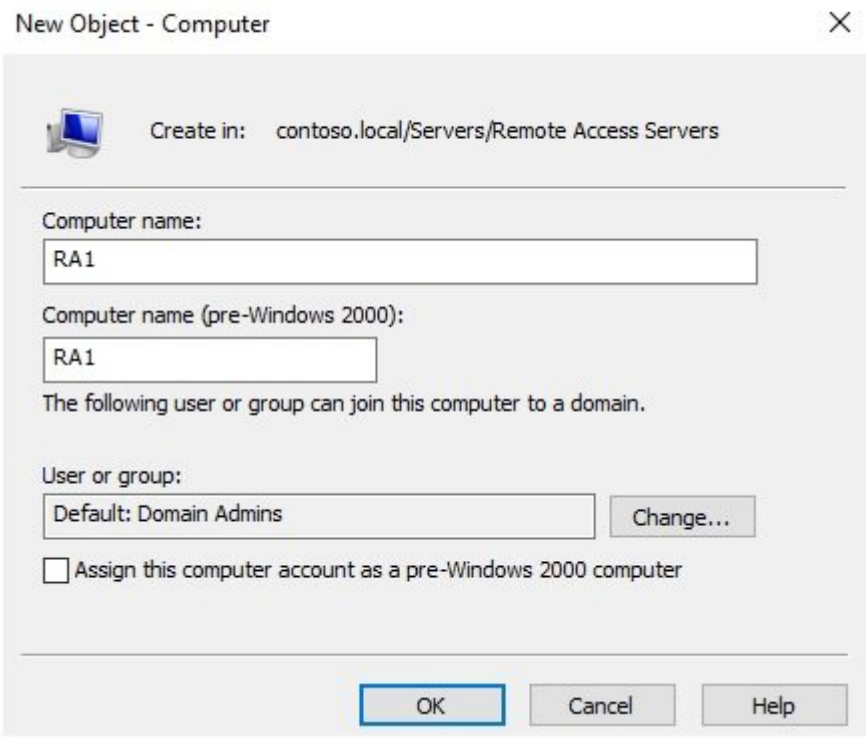
حساب‌های کامپیوتری

کاملا مرسوم است که از Active Directory Users and Computers برای ساخت حساب‌های کاربری جدید استفاده کنید. بدون ساخت یک حساب کاربری، یک کاربر نمی‌تواند به‌طور کامل به شبکه وارد شود. با این حال، کمی غیر عادی به نظر می‌رسد که ابزار فوق را برای متصل کردن کامپیوترها به دامنه استفاده کنید، زیرا بیشتر دامنه‌ها به گونه‌ای پیکربندی شده‌اند تا کامپیوترهای جدید بتوانند به دامنه متصل شده و فعالیت‌های خود را انجام دهند، بدون آن‌که نیازی به اضافه کردن آن‌ها به اکتیودایرکتوری ضرورتی داشته باشد. به عبارت دیگر، زمانی که شخصی نام کاربردی و گذرواژه‌ای که دارای مجوزهای مدیریتی است را در اختیار داشته باشد با نشستن پشت هر کامپیوتر متصل به شبکه، قادر است فرآیند اتصال به دامنه را روی یک کامپیوتر محلی انجام دهد. در این حالت اتصال با موفقیت انجام شده و اکتیو دایرکتوری شی جدیدی که بیان‌گر یک کامپیوتر است را به‌طور خودکار ایجاد می‌کند. اشیا کامپیوتری که به‌طور خودکار ایجاد می‌شوند، خودشان به‌طور پیش‌فرض به مخزن Computers اضافه می‌شوند، در بیشتر شبکه‌ها، اگر شما روی پوشه Computers کلیک کنید، فهرستی از ماشین‌های مختلف را مشاهده می‌کنید که برخی از آن‌ها ممکن است ترکیبی از هر دو مدل کامپیوترهای دسکتاپ و سرورهایی که باشند که به تازگی به یک دامنه متصل شده‌اند و به OU درست تخصیص داده نشده‌اند. به‌طور مثال شما می‌توانید یک تعداد ماشین را به دامنه خود متصل کنید، بدون آن‌که ابزار Ad Users and Computers را باز کنید. در این حالت اشیایی که به کامپیوترهای جدید تخصیص داده می‌شوند، به مخزن پیش‌فرض computers اضافه می‌شوند.

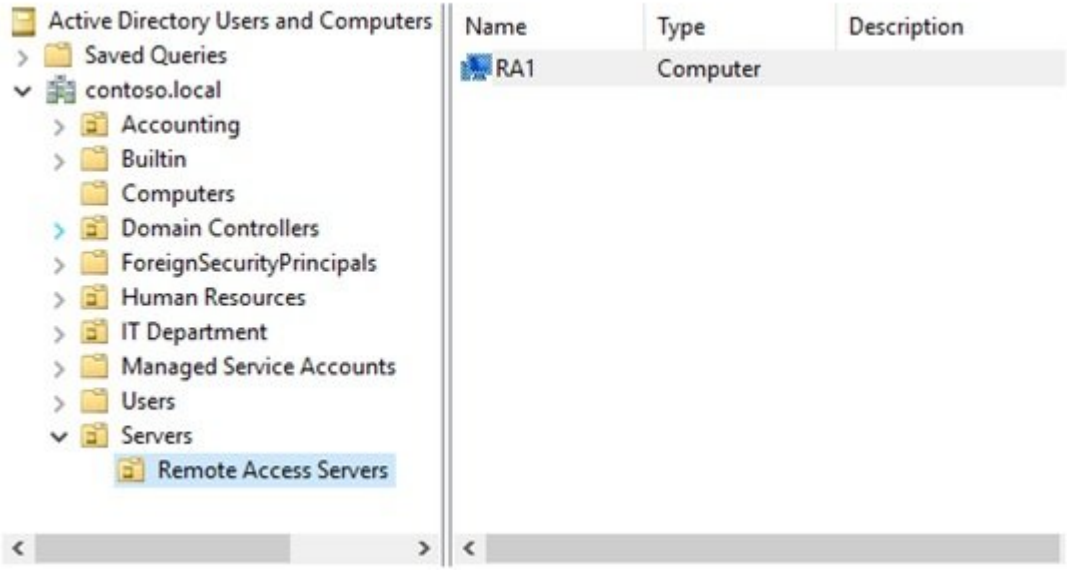


اگر حساب‌های کامپیوتری که به شکل خودکار به مخزن computers اضافه می‌شوند، همگی سامانه‌های کلاینتی هستند، مشکل خاصی ندارید، اما اگر کامپیوترهای فوق سرور باشند، آن‌گاه با مشکل بزرگی روبرو می‌شوید. بسیاری از شرکت‌ها خط‌مشی‌های امنیتی در شبکه خود تعریف می‌کنند و اغلب این خط‌مشی‌ها به گونه‌ای ایجاد می‌شوند که به‌طور خودکار به هر حساب کامپیوتری اجازه می‌دهند درون یکی از OUهای عمومی وارد شود. با استفاده از خط‌مشی‌های امنیتی می‌توانید یک راه عالی برای قفل کردن بخش‌هایی از ماشین‌های کلاینت که یک کاربر نیازی به دسترسی یا استفاده از آن‌ها ندارد را تعریف کنید، اما اگر به‌طور ناخواسته این خط‌مشی‌ها را برای محدودسازی یا قفل سرورهای جدید اعمال کنید، به محض اتصال به دامنه، متوجه خواهید شد که فرآیند پیکربندی سرور با مشکلاتی همراه خواهد بود و در برخی موارد پیکربندی‌ها اعمال نخواهند شد. به حرف من اعتماد کنید، زیرا این تجربه را در گذشته داشته‌ام. متاسفانه، حساب‌های جدید سرور که به اکتیودایرکتوری اضافه می‌کنید، شبیه به یک ایستگاه کاری که به یک دامنه اضافه شده‌اند، شناسایی و طبقه‌بندی می‌شوند، بنابراین شما نمی‌توانید مخازن پیش‌فرض مختلف را به سادگی برای سرورها مشخص کنید، زیرا آن‌ها یک سرور و نه یک ایستگاه کاری معمولی هستند.

برای حل این مشکل بالقوه چه کاری می‌توان انجام داد؟ پاسخ این است که برای حساب‌های دامنه متعلق به سرورهای جدید خود یک اعتبار تعریف کنید. شما حتا می‌توانید این اعتبار را برای همه حساب‌های کامپیوتری جدید اعمال کنید، هرچند اینکار عمدتا از سوی شرکت‌های بزرگ انجام می‌شود. اعتبارسازی برای یک حساب کامپیوتری شباهت خیلی زیادی به ساخت یک حساب کاربری دارد. قبل از اتصال کامپیوتر به دامنه، شما آن‌را داخل Active Directory ایجاد می‌کنید. ایجاد یک شی، قبل از اتصال آن به دامنه به شما اجازه می‌دهد تا انتخاب کنید که کامپیوتر شما در هنگام اتصال به دامنه در چه OU وارد شود. با انجام این‌کار می‌توانید اطمینان حاصل کنید که OU انتخاب شده قادر است تنظیمات امنیتی و خط‌مشی‌هایی که در نظر دارید روی یک کامپیوتر جدید یا سرور اعمال شود را دریافت کند. به شدت توصیه می‌کنم فرآیند اعتبارسازی را برای تمام حساب‌های کامپیوتری در اکتیودایرکتوری و برای هر سرور جدیدی که قرار است آنلاین شود اعمال کنید. اگر این عمل را انجام دهید، حتا زمانی که احساس می‌کنید چنین کاری ضرورتی ندارد، در آینده مجبور نخواهید شد به دلیل برخی از مشکلات بازطراحی با مشکلات عدیده‌ای روبرو شوید. اعتبارسازی یک شی کامپیوتری به شکل مفرطی ساده و سریع است، در ابتدا باید OU خود را ایجاد کنید. پس از ساخت OU جدید روی آن کلیک راست کرده و گزینه New | computer را انتخاب کنید. در پنجره باز شده در فیلد Computer Name نام سرور را وارد کرده و کلید Ok را فشار دهید.



تنها به چند کلیک ساده کامپیوتر شما به OU که خود ایجاد کرده‌اید اضافه می‌شود. در تصویر زیر، یک واحد سازمانی (OU) به نام Servers را مشاهده می‌کنید که درون آن واحد سازمانی دیگری به نام Remote Access Servers قرار دارد که سرور جدید به نام RA1 به آن اضافه شده است.



در شماره آینده آموزش رایگان **ویندوز سرور 2019** سایر کنسول‌ها را بررسی خواهیم کرد.

برای مطالعه تمام بخش‌های **آموزش ویندوز سرور 2019** روی لینک زیر کلیک کنید:

آموزش رایگان ویندوز سرور 2019

تاریخ انتشار:
09 مرداد 1398

نشانی منبع:
https://www.shabakeh-mag.com/networking-technology/15832/%D8%A2%D9%85%D9%88%D8%B2%D8%B4-%D9%88%DB%8C%D9%86%D8%AF%D9%88%D8%B2-%D8%B3%D8%B1%D9%88%D8%B1-%D8%A8%D8%A7-user-accounts-%D9%88-security-groups-%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