



پودمان ۴

مدیریت متمرکز منابع شبکه

با اتصال رایانه‌ها به یکدیگر و برقراری ارتباط بین آنها می‌توان علاوه بر مدیریت منابع شبکه، دسترسی سریع‌تری را برای کاربران مهیا کرد. اما از آنجایی که داده‌ها روی رایانه‌های مختلف در شبکه قرار دارند و کاربران نیز برای کار با آنها باید از رایانه‌های مختلف استفاده کنند، مدیریت آنها کمی دشوار به نظر می‌رسد. با افزایش تعداد کاربران و رایانه‌ها نگرانی برای امنیت افزایش یافته است. برای این منظور سیستم‌عامل‌های سرویس‌دهنده، طراحی شدند تا علاوه بر قابلیت‌های متداول شبکه مانند اشتراک داده‌ها و مجوز دسترسی، امکان مدیریت متمرکز داده‌ها و کاربران را برای مدیران مهیا کنند. سیستم‌عامل‌های سرویس‌دهنده با داشتن قابلیت‌هایی که به آنها سرویس می‌گویند، مشخصات کاربران را در بانک اطلاعاتی به نام Active Directory به صورت متمرکز جمع‌آوری و مدیریت می‌کنند و یا داده‌ها را در یک فضای نامی مشترک برای همه سرویس‌دهنده‌های پرونده، به اشتراک می‌گذارند. در این پودمان هنرجو با اتکا بر دانش و مهارت قادر خواهد بود نصب و پیکربندی سرویس‌های ADDS، پرونده و چاپگر را به همراه تنظیم سیاست روی منابع در محیط ویندوز سرور انجام دهد.

واحد یادگیری ۵

شایستگی مدیریت متمرکز منابع شبکه

آیا تا به حال پی برده‌اید

- چگونه مدیر یک کافی‌نت می‌تواند همه رایانه‌های شبکه و کاربران را مدیریت کند؟
- برای محدود کردن دسترسی موقت یک کارمند به اسناد شبکه چه باید کرد؟
- مدیر یک فروشگاه زنجیره‌ای چگونه می‌تواند اسناد مالی و فهرست‌های فروش را به صورت متمرکز مدیریت کند؟
- چگونه می‌توان چاپگرهای یک دفتر کار را در اختیار همه کارمندان قرار داد؟
- در یک کافی‌نت چگونه می‌توان دسترسی به چاپگر را برای برخی کاربران فعال کرد؟

هدف از این واحد شایستگی، مدیریت متمرکز منابع به اشتراک گذاشته شده با استفاده از سیستم عامل سرور است.

استاندارد عملکرد

اشتراک منابع شبکه و مدیریت متمرکز آنها با استفاده از سیستم عامل سرور

شبکه‌های Domain

در کارگاه هنرستان ماهر ۸ رایانه وجود دارد که به صورت گروه کاری (Workgroup) شبکه شده‌اند و تعداد هنرجویان کلاس ۱۶ نفر است. هنرآموز کلاس از ماهر خواسته است که برای هم‌کلاسی‌های خود حساب کاربری ایجاد کند و مطالب درسی را برای آنها به اشتراک بگذارد. ماهر با چه مشکلاتی روبه‌رو خواهد شد؟ اگر تعداد رایانه‌ها به ۲۵ و هنرجویان به ۳۲ نفر افزایش یابد، باز هم می‌تواند از همین نوع شبکه استفاده کند؟ آیا با شبکه کردن رایانه‌ها به صورت Domain مشکلات برطرف می‌شود؟

پاسختان را یادداشت کرده، با هم کلاسی‌های خود بحث و گفت‌وگو کنید، سپس نتیجه را در جدول زیر خلاصه کنید.

...	مورد ۲	مورد ۱	
		تعریف حساب کاربری روی هر رایانه	مشکلات Workgroup
	پشتیبانی از تعداد زیاد رایانه		مزایای Domain

شبکه Domain به نوع و پیکربندی شبکه وابسته نیست و می‌تواند در هر نوع شبکه‌ای مثل یک شبکه LAN کوچک در هر جایی از دنیا پیاده‌سازی شود.

یادداشت



سرویس ADDS

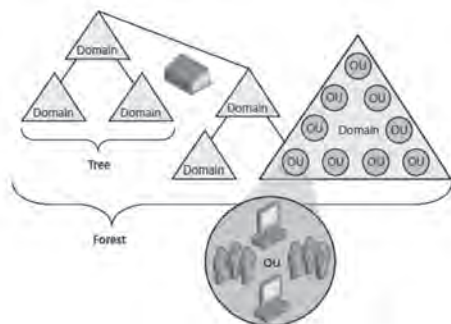
سرویس ADDS (Active Directory Domain Services) این امکان را برای مدیران فراهم می‌کند تا بتوانند شبکه سازمانی خود را به بخش‌هایی به نام Domain تقسیم کنند و برای هر Domain یک بانک اطلاعاتی مرکزی به نام Active Directory ایجاد کنند. AD یک بانک اطلاعاتی از منابع مختلف مثل سخت‌افزار، نرم‌افزار و کاربران است که برای رایانه‌های شبکه به اشتراک گذاشته می‌شود.

AD همانند یک دفترچه تلفن است. همان‌طور که شما به‌وسیله دفترچه تلفن می‌توانید به نشانی و شماره تلفن دوستان، آشنایان و سازمان‌های مختلف دسترسی پیدا کنید، رایانه‌ها، برنامه‌ها و کاربران شبکه به‌وسیله AD می‌توانند اهداف مختلف مثل شناسایی کاربران را انجام دهند. در شکل‌گیری AD اجزای مختلفی به‌صورت منطقی و فیزیکی تعریف می‌شوند. برای کاربران و رایانه‌ها از شیء (Object) استفاده می‌کنیم و برای دسته‌بندی اشیا

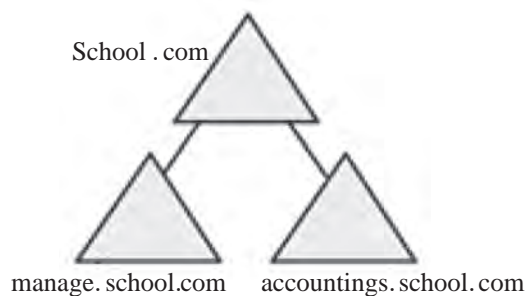
در Domain واحد سازمانی (Organizational Unit) تعریف می‌کنیم.

دامنه (Domain): به گروه منطقی از رایانه‌ها و سایر اجزای شبکه مثل کاربران و گروه‌ها دامنه می‌گویند.

Root Domain: به اولین Domain که در یک شبکه نصب می‌شود Root Domain می‌گویند.



شکل ۱- ساختار AD



شکل ۲- Domain Tree

درخت (Domain Tree): بیشتر سازمان‌ها نیاز به یک Domain دارند. اما در سازمان‌های بزرگ براساس محدوده جغرافیایی چندین بخش ایجاد می‌کنند و برای هر بخش یک Domain تعریف می‌کنند. به این مجموعه Domain Tree می‌گویند. برای مثال اگر شبکه Domain یک هنرستان با نام school.com تعریف شده باشد. در صورتی که بخواهیم بخش مدیریت و حسابداری هنرستان را به آن اضافه کنیم، باید برای هر کدام در school.com یک Sub Domain تعریف کنیم.

Domain Tree دارای یک Root Domain و چندین Domain زیر مجموعه است که به آنها Sub Domain می‌گویند.

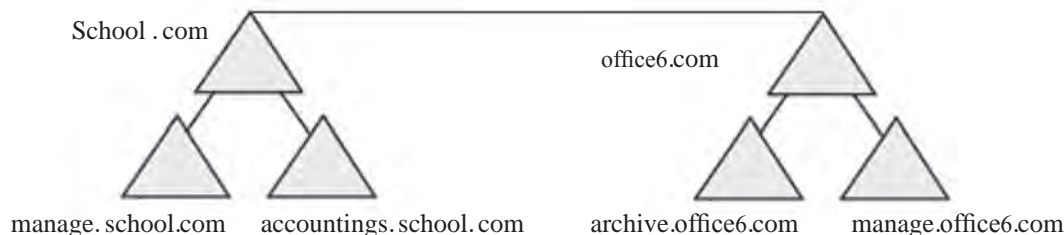
Sub Domain و Root Domain شکل ۲ را در جدول زیر بنویسید.

Root Domain	
Sub Domain	

فعالیت
کارگاهی



جنگل (Forest): مجموعه‌ای از یک یا چند Domain Tree است. برای مثال اگر بخواهیم شبکه هنرستان school.com را گسترش دهیم به طوری که با شبکه اداره ناحیه آموزش و پرورش مربوطه به صورت متمرکز مدیریت شود، باید آنها را به صورت Forest پیاده‌سازی کنیم (شکل ۳).



شکل ۳- Forest

DC (Domain Controller): به رایانه سرویس دهنده‌ای که سرویس ADDS روی آن نصب و پیکربندی شده است، DC می‌گویند. وظیفه DC شناسایی و مدیریت دسترسی‌ها در شبکه است.

سیستم عامل DC باید از نوع سرور مانند Windows server 2012 باشد.

یادداشت



پیاده‌سازی شبکه Domain

برای ایجاد یک شبکه Domain ابتدا باید سرویس دهنده DC را پیکربندی کرده، سپس رایانه‌های سرویس گیرنده (Client) را عضو آن کنیم.

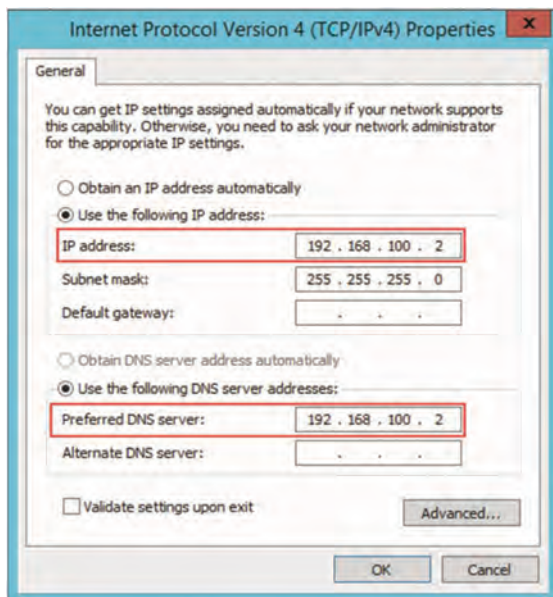
کارگاه ۱ نصب سرویس ADDS

۱ با حساب کاربری Administrator وارد ویندوز سرور شوید.

۲ آدرس IP را به صورت استاتیک تنظیم کنید.

در مورد دلیل ثابت بودن آدرس IP رایانه‌های سرویس‌دهنده تحقیق کنید و درباره نتیجه تحقیق با هم کلاسی‌هایتان بحث و گفت‌وگو کنید.

فعالیت
منزل

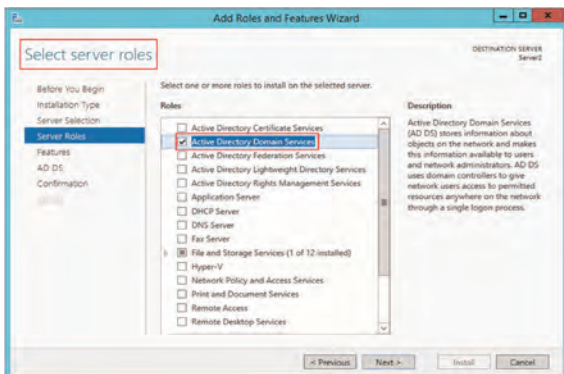


شکل ۴- تنظیمات IP

۳ آدرس Preferred DNS server را تعیین کنید.

آدرس IP تنظیم شده در مرحله ۲ را در کادر Preferred DNS server تایپ کنید (شکل ۴).

در صورتی که آدرس DNS را قبل از نصب سرویس ADDS تنظیم نکنید، به صورت پیش فرض آدرس 127.0.0.1 را به عنوان آدرس DNS در نظر می‌گیرد.



۴ سرویس Active Directory Domain Services را به سرور اضافه کنید.

سرویس Active Directory Domain Services را از پنجره Server Roles انتخاب کنید (شکل ۵).

با انتخاب این سرویس، پنجره نصب ویژگی‌های آن باز می‌شود. دکمه Add Features و سپس دکمه Next را کلیک کنید.

شکل ۵- پنجره انتخاب سرویس‌ها

۵ سرویس ADDS را نصب کنید.

در پنجره Confirm Installation Selections با کلیک روی دکمه Install سرویس ADDS را نصب کنید.

۶ سرویس ADDS را پیکربندی کنید.

پس از کامل شدن مراحل نصب سرویس ADDS برای ایجاد سرویس‌دهنده DC باید سرویس ADDS را پیکربندی کنیم.

فیلم شماره ۱۲۱۱۸: پیکربندی سرویس ADDS

فیلم



فیلم را مشاهده کنید و سپس یک Domain با نام schoolN.com ایجاد کنید. به جای حرف N شماره رایانه خود را بنویسید زیرا در یک شبکه نمی‌توانیم Domain‌های همانم داشته باشیم.

فعالیت کارگاهی



جدول ارزشیابی شایستگی‌های غیر فنی، ایمنی، بهداشت و توجهات زیست محیطی

شایستگی‌ها	شرایط عملکرد (ابزار، مواد، تجهیزات، زمان، مکان و...)	نتایج ممکن	استاندارد (شاخص‌ها/داوری/نمره دهی)	نمره
شایستگی‌های غیر فنی	مسئولیت‌پذیری، توجه به جزئیات کار - زبان فنی	قابل قبول	توجه به مسئولیت کاربر برای عضویت او در گروه‌ها و تعیین مجوزها و سیاست‌ها و اعطای مجوز استفاده از چاپگر - بازگرداندن تنظیمات به حالت اولیه پس از انجام عملیات	۲
ایمنی و بهداشت	توجه به سطح دسترسی مورد نیاز کاربران و گروه‌ها			
توجهات زیست محیطی	کاهش مصرف کاغذ با اشتراک گذاری منبع	غیر قابل قبول	توجه به ایمنی و بهداشت محیط کارگاه	۱
نگرش	دقت در اختصاص مجوزها			

* این شایستگی‌ها در ارزشیابی پایانی واحد یادگیری باید مورد توجه قرار گیرند.



ارزشیابی مرحله ۱

مراحل کار	شرایط عملکرد (ابزار، مواد، تجهیزات، زمان، مکان و...)	نتایج ممکن	استاندارد (شاخص‌ها/داوری/نمره دهی)	نمره
پیاده‌سازی Domain Controllers	مکان: کارگاه استاندارد رایانه تجهیزات: شبکه‌ای از رایانه‌ها که حداقل یکی از آنها دارای سیستم عامل سرور باشد. زمان: ۳۵ دقیقه	بالاتر از حد انتظار	نصب کامل سرویس AD - پیکربندی سرویس AD - تعیین گذرواژه باز یابی مطابق استاندارد	۳
		در حد انتظار	نصب سرویس AD - پیکربندی سرویس AD	۲
		پایین تر از حد انتظار	نصب سرویس AD	۱



انواع حساب‌ها در AD (Accounts)

به منابع شبکه مثل کاربر و رایانه شیء (Object) می‌گویند که با مجموعه‌ای از صفات توصیف می‌شوند. برای مثال صفات‌های یک کاربر ممکن است شامل نام، نام خانوادگی و رایانه باشد. از جمله اشیای مهم قابل تعریف در AD می‌توان به انواع حساب‌ها اشاره کرد که عبارت‌اند از:

- **User Accounts:** از حساب کاربری برای شناسایی کاربران (authentication) هنگام ورود به Domain و دسترسی به منابع استفاده می‌شود.

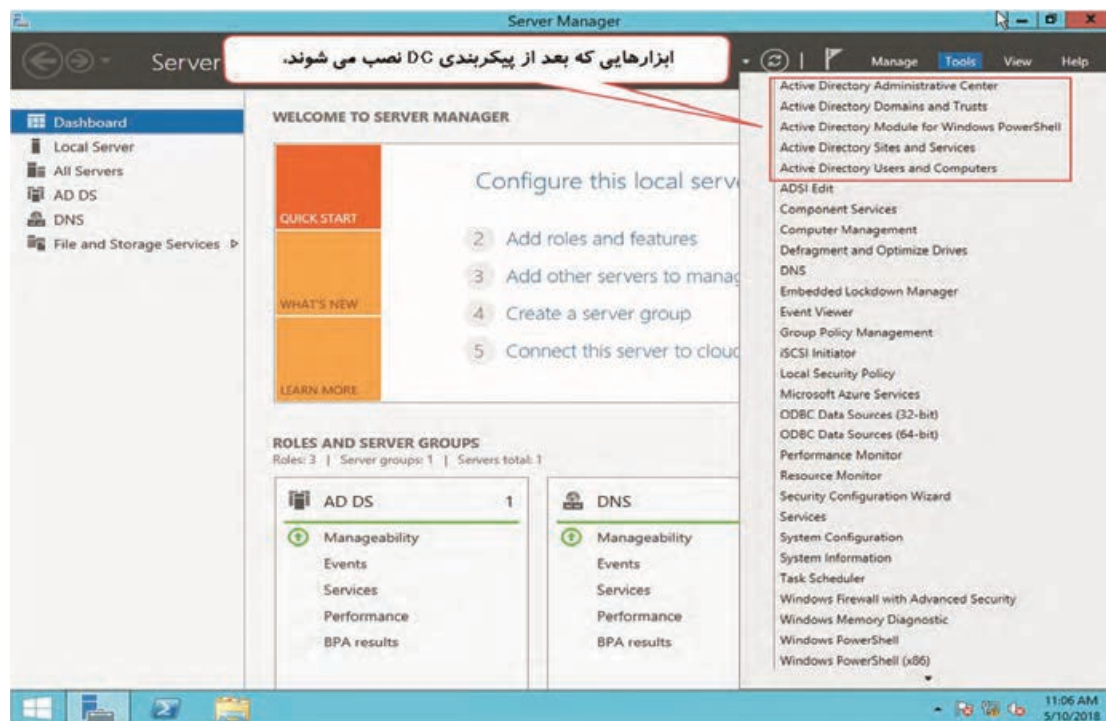
- **Group Accounts:** از حساب‌های گروهی برای گروه‌بندی حساب‌ها استفاده می‌شود، تا بتوان آنها را آسان‌تر مدیریت کرد.

- **Computer Accounts:** برای رایانه‌هایی که عضو دامنه می‌شوند حساب رایانه‌ای ایجاد می‌شود که برای برقراری ارتباط امن بین رایانه و شبکه استفاده می‌شود.

برای سازماندهی اشیاء در محدوده یک دامنه، واحد سازمانی (Organizational Unit) ایجاد می‌کنند که یک گروه مدیریتی است و می‌تواند شامل اشیایی از قبیل حساب کاربری، رایانه، چاپگر و... باشد. به واحد سازمانی به اختصار OU می‌گویند

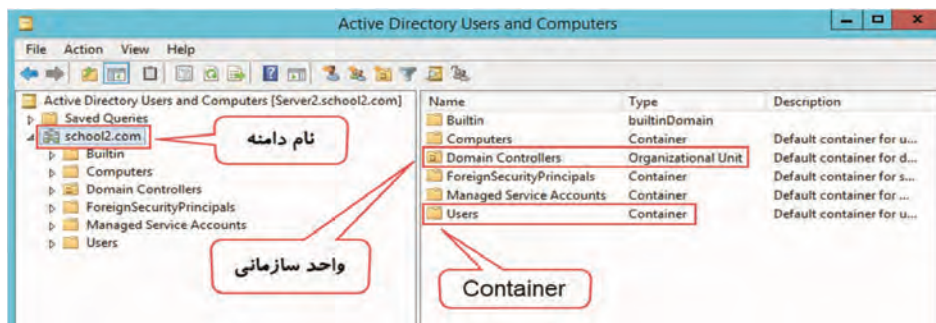
ابزار مدیریت حساب‌ها

بعد از پیکربندی DC ابزارهایی برای مدیریت Domain و اشیاء آن نصب می‌شوند. از جمله این ابزارها، ابزار مدیریتی Active Directory Users and Computers است که برای مدیریت اشیاء و حساب‌ها به کار می‌رود. این ابزار را از فهرست منوی Tools برنامه Server Manager اجرا کنید (شکل ۶).



شکل ۶- فهرست ابزارهای مدیریت AD

با کلیک روی نام دامنه، پوشه‌هایی نمایش داده می‌شود که به‌طور پیش‌فرض هنگام پیکربندی ADDS ایجاد شده‌اند، به این پوشه‌ها Container می‌گویند (شکل ۷).



شکل ۷- محیط Active Directory Users and Computers

OU نوع خاصی از Container است که به‌وسیله کاربران ایجاد می‌شود. تنها واحد سازمانی که به‌وسیله ADDS ایجاد می‌شود، واحد سازمانی Domain Controllers است.

یادداشت

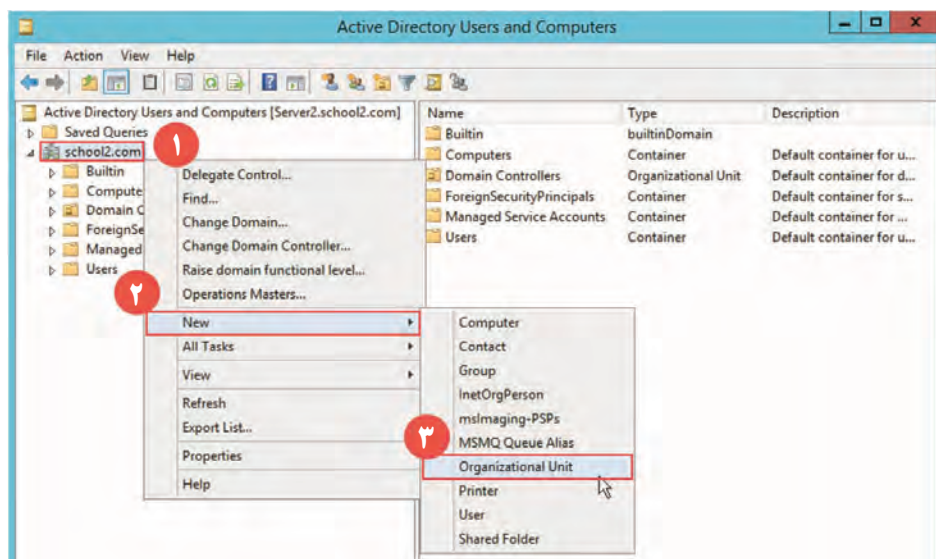


کارگاه ۲ ایجاد OU و حساب کاربری

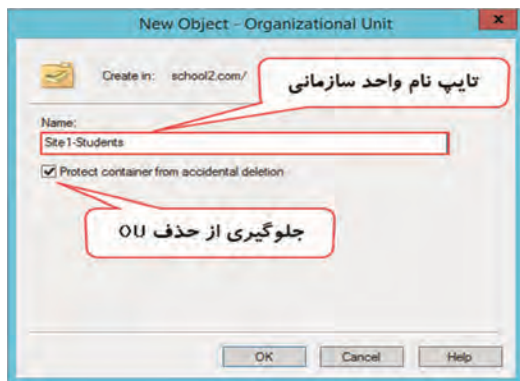
در هر سازمان برای مدیریت ساختاریافته و ساده‌تر از یک مجموعه OU استفاده می‌شود. برای مثال استفاده از OUهایی نظیر کارگزینی، امور اداری، حسابداری، آموزش، روابط عمومی، IT... در بسیاری از شرکت‌ها و سازمان‌ها مرسوم است. در یک Domain می‌توانید تعدادی OU ایجاد کرده، و منابع و کاربران را بر اساس نوع شغل یا موقعیت جغرافیایی در آنها تعریف کنید. بنابراین در هر OU می‌توانید یک مدیر و تعدادی کارمند و منابع مانند رایانه، چاپگر و... قرار دهید.

۱ کادر محاوره‌ای ایجاد Organizational Unit را باز کنید.

ابزار Active Directory Users and Computers را باز کنید و روی نام دامنه (school2.com) راست کلیک کرده (۱)، گزینه New (۲) و سپس Organizational Unit (۳) را انتخاب کنید (شکل ۸).



شکل ۸- مسیر دسترسی به کادر محاوره‌ای ایجاد OU



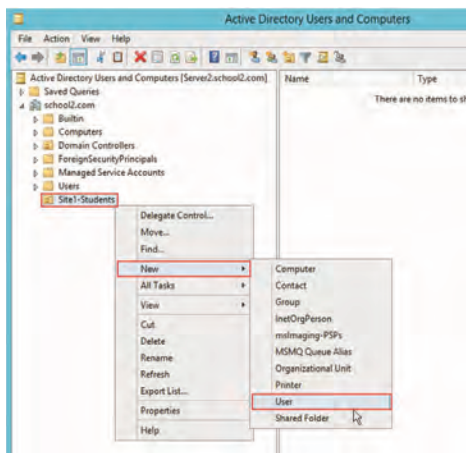
شکل ۹- ایجاد OU

۲ برای ایجاد OU نام آن را وارد کنید.

Site1-Students را به عنوان نام OU تایپ کنید (شکل ۹). اگر گزینه Protect container from accidental deletion فعال باشد، AD بعد از ایجاد OU اجازه حذف آن را نمی‌دهد. پس از ایجاد OU جدید می‌توان کاربران و سایر حساب‌های دیگر را درون آن تعریف کرد.

تحقیق کنید چگونه می‌توان یک OU را حذف کرد.

پژوهش



۳ یک حساب کاربری در واحد سازمانی Site1-Students ایجاد کنید.

کادر محاوره‌ای New Object - User را باز کنید. روی واحد سازمانی Site1-Students راست کلیک کرده، گزینه New و سپس User را انتخاب کنید (شکل ۱۰). برای کاربری با نام ماهر بینا کادرهای مربوط به صفات را تکمیل کنید (شکل ۱۱).

شکل ۱۰- مسیر دسترسی به کادر محاوره‌ای ایجاد حساب کاربری



شکل ۱۱- کادر محاوره‌ای ایجاد حساب کاربری

Full name شناسه کاربر در Domain و User logon name شناسه کاربر برای ورود به محیط Domain است. بنابراین هر دو باید منحصر به فرد باشند. از نام (pre-Windows 2000) User Logon name برای ورود به Domain از طریق سیستم عامل های قبل از 2000 مثل Win95 و Win98 و NT4.0 استفاده می شود که این نام هم باید منحصر به فرد باشد. به ترکیب User logon name با نام دامنه که در مثال ما، m.bina@school2.com است، UPN (User Principal names) می گویند.

چرا Full name و User logon name بهتر است متفاوت تعریف شوند؟

کنجکاوی



۴ گذرواژه و سیاست های امنیتی حساب کاربری را تعیین کنید.

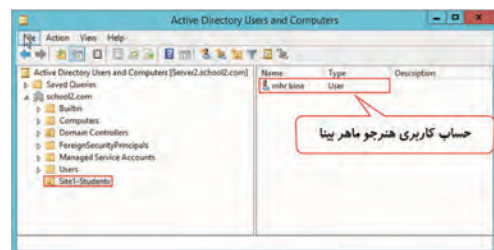
دکمه Next را کلیک کنید. کادر محاوره ای تعریف گذرواژه و تنظیم سیاست های پیش فرض باز می شود (شکل ۱۲). سیاست های امنیتی مربوط به حساب کاربران، در ویندوز سرور ۲۰۱۲ شما را ملزم به استفاده از گذرواژه پیچیده (Complex) می کند. طبق این سیاست ها طول گذرواژه حداقل ۷ نویسه است و در نویسه ها باید حداقل ۳ مورد از ۴ مورد زیر وجود داشته باشد:

- ۱- حروف بزرگ
- ۲- حروف کوچک
- ۳- اعداد
- ۴- نشانه های خاص

شکل ۱۲- کادر محاوره ای تعیین گذرواژه و سیاست های پیش فرض

- سیاست های امنیتی تعریف شده در پایین شکل ۱۲ را ترجمه کرده، توضیح دهید.
- چرا سیاست User must... به صورت پیش فرض فعال است؟

فعالیت گروهی

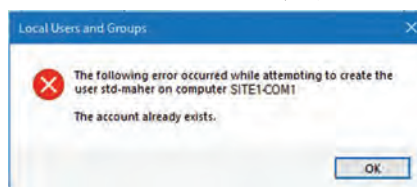


۵ صحت مشخصات کاربر را بررسی کنید.

در پنجره خلاصه مشخصات کاربر، پس از اطمینان از صحت اطلاعات وارد شده دکمه Finish را کلیک کنید. حساب کاربری با نام کامل mhr.bina در واحد سازمانی Site1-Students ایجاد می شود (شکل ۱۳).

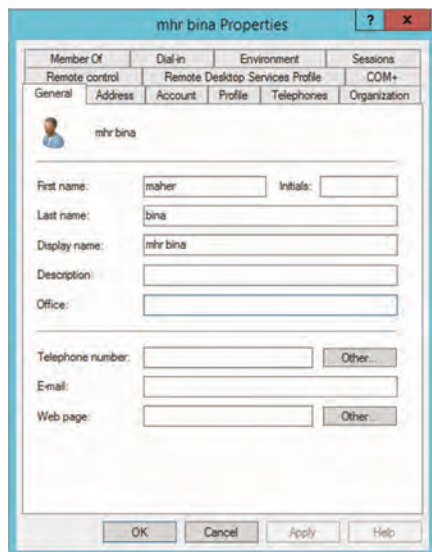
شکل ۱۳- نمایش حساب کاربری در AD

دلیل نمایش پیام شکل های ۱۴ را بیان کرده، آن را ترجمه کنید.



شکل ۱۴- پیام های خطا هنگام ایجاد حساب کاربری

فعالیت گروهی



شکل ۱۵- کادر محاوره‌ای مشخصات کاربر

تغییر مشخصات کاربران

روی حساب کاربری mhr bina راست کلیک کرده، گزینه Properties را انتخاب کنید. مشخصات کامل کاربر به وسیله برگه‌های این پنجره قابل نمایش و تغییر است (شکل ۱۵).
برای نمایش تمام مشخصات حساب کاربری باید از منوی View پنجره Active Directory Users and Computers گزینه Advanced Features را فعال کنید.

فیلم شماره ۱۲۱۱۹: تنظیم مشخصات حساب کاربری

فیلم



فیلم را مشاهده کنید و فعالیت را انجام دهید.

فعالیت
کارگاهی



برای اعضای گروه خود حساب کاربری ایجاد کنید به طوری که:

- کاربر ۱ از ساعت ۸ تا ۱۲ صبح و کاربر ۲ از ساعت ۱ تا ۵ بعد از ظهر اجازه ورود به شبکه را داشته باشند.
- هر دو هنگام اولین ورود به شبکه مجبور به تغییر گذرواژه خود شوند.
- کاربر ۱ بتواند به وسیله تمام رایانه‌های عضو شبکه وارد شبکه شود؛ اما کاربر ۲ فقط از رایانه شماره ۱ بتواند وارد شود.

کارگاه ۳ ایجاد حساب کاربری با استفاده از الگو

ساخت حساب کاربری و تنظیم مشخصات آن برای چندین کاربر وقت گیر است. از آن جایی که کاربران در Domain بر اساس نوع شغل و محل کار دسته‌بندی می‌شوند، دارای مشخصات مشابه هستند مثلاً هنجرویان رشته شبکه و نرم‌افزار رایانه دارای ساعت کارگاهی یکسان برای استفاده از رایانه‌ها هستند و گروه‌بندی‌های مشابه دارند. بنابراین برای سرعت بخشیدن به این امر می‌توانید یک حساب کاربری الگو (User Template) ایجاد کنید و سپس تنظیمات الگو را برای حساب کاربری جدید کپی کنید.

۱ واحد سازمانی به نام std-computer برای هنجرویان رشته رایانه ایجاد کنید.

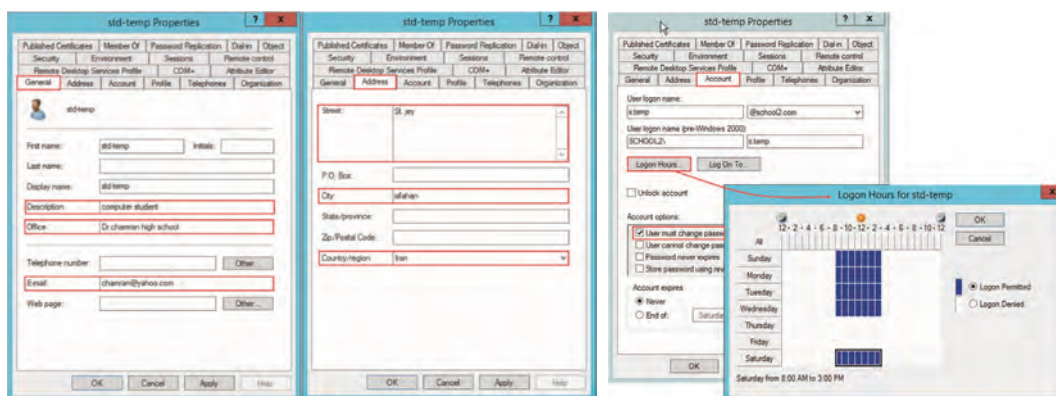
۲ در واحد سازمانی std-computer، یک حساب کاربری با نام std-temp ایجاد کنید.

سیاست User must change password at next logon را غیرفعال و سیاست Account is disabled را فعال کنید.

چرا سیاست تغییر گذرواژه را برای حساب کاربری الگو غیر فعال و سیاست Account is disabled را فعال کردیم؟

۳ صفات حساب کاربری را تنظیم کنید.

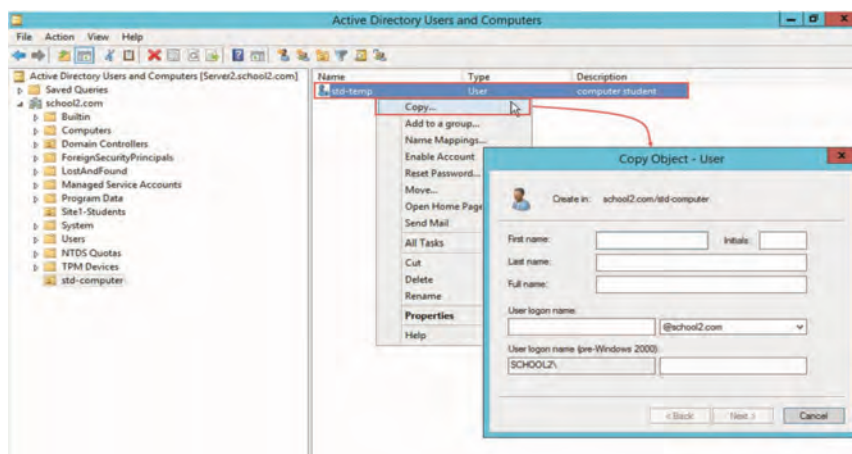
کادر محاوره‌ای Properties حساب کاربری std-temp را باز کرده، برخی از صفات را در برگه‌های General، Address و Account تغییر دهید (شکل ۱۶).



شکل ۱۶- تغییر صفات حساب کاربری

۴ از حساب کاربری الگو نسخه مشابه ایجاد کنید.

روی حساب کاربری std-temp راست کلیک کرده، گزینه Copy را انتخاب کنید (شکل ۱۷).



شکل ۱۷- مسیر دسترسی به کادر محاوره‌ای Copy

۵ حساب کاربری جدید را برای کاربر مورد نظر تنظیم کنید.

اطلاعات کاربر موردنظر را تایپ کرده، سیاست Account is disabled را غیرفعال کنید. بدین ترتیب حساب کاربری برای کاربر موردنظر، با صفات مشترک با الگو ایجاد می‌شود.

۶ صفات حساب کاربری ایجاد شده را با حساب کاربری الگو مقایسه کنید.

کدام صفات‌ها از حساب کاربری الگو کپی نشده‌اند؟

کارگاه ۴ مدیریت کاربران

در این کارگاه به بررسی عمومی‌ترین وظایف مدیریتی می‌پردازیم که روی حساب کاربری انجام می‌شود.

۱ گذرواژه حساب کاربری را تغییر دهید.

یکی از اشتباهات کاربران، فراموش کردن گذرواژه است. بنابراین مدیر باید گذرواژه کاربران را Reset کند. برای این منظور روی حساب کاربر مورد نظر در AD راست کلیک کرده، گزینه Reset Password را انتخاب کنید. گذرواژه جدید را تایپ کرده، گزینه User must change password at next logon را فعال کنید تا کاربر در اولین ورود با گذرواژه جدید بتواند آن را تغییر دهد. در این حالت گذرواژه کاربر فقط در اختیار خودش خواهد بود.

۲ حساب کاربری را غیر فعال کنید.

از آنجایی که حساب کاربری اجازه دسترسی به منابع و رایانه‌های شبکه را برای کاربران فراهم می‌کند، باید مطمئن باشید که حساب کاربری به وسیله خود کاربر استفاده می‌شود. از این رو اگر کاربری به هر دلیلی مانند غیبت یا اخراج از آن استفاده نمی‌کند، آن را غیرفعال کنید تا دیگران از آن سوء استفاده نکنند. برای غیرفعال کردن حساب کاربری، روی حساب کاربری مورد نظر در AD راست کلیک کرده، گزینه Disable Account را انتخاب کنید.

حساب کاربری غیرفعال شده در مرحله ۲ را فعال کنید.

فعالیت
کارگاهی



۳ حساب کاربری را حذف کنید.

در صورتی که به یک حساب کاربری نیاز نداشته باشید، بهتر است آن را حذف کنید. روی حساب کاربر مورد نظر در AD راست کلیک کرده، گزینه Delete را انتخاب کنید.

با حذف حساب کاربری تمام مشخصات، مجوزها و عضویت آن در گروه‌ها از بین می‌رود؛ بنابراین در صورت حذف سهوی، حساب کاربری قابل بازیابی نیست. به همین دلیل توصیه می‌شود ابتدا آن را غیرفعال کنید و بعد از اطمینان به عدم نیاز، آن را حذف کنید.

یادداشت



انواع گروه‌ها و حوزه عملکرد آنها

گروه‌ها اشیایی هستند که می‌توانند برای دسته‌بندی اشیای دیگر مثل کاربر، رایانه و گروه‌های دیگر استفاده شوند. زمانی که مجوزهای امنیتی برای یک گروه روی یک منبع تعریف می‌شوند تمام اعضای درون گروه، این مجوزها را دریافت می‌کنند.

در ویندوز سرور ۲۰۱۲ دو نوع گروه (Group type) تعریف می‌شود:

- **گروه‌های امنیتی (Security Group)** که برای اعطای مجوز دسترسی به منابع شبکه استفاده می‌شود.
- **گروه‌های توزیعی (Distribution Group)** که برای فراهم کردن فهرست نامه‌های الکترونیکی کاربران به کار می‌روند.

حوزه عملکرد گروه‌ها (Group Scope) چگونگی تخصیص مجوزها به اعضای درون آنها را مشخص می‌سازد. هر دو گروه امنیتی و توزیع‌کننده می‌توانند در یکی از ۳ نوع حوزه عملکرد زیر قرار گیرند:

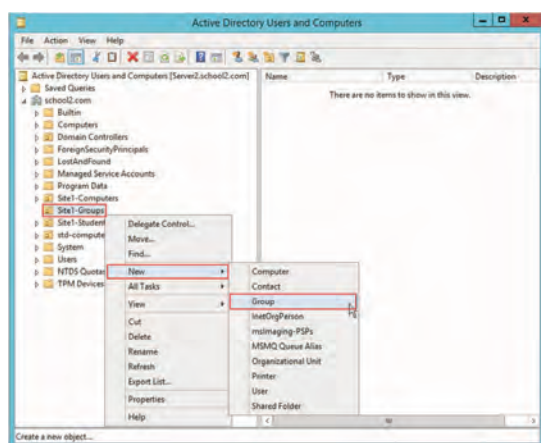
- Domain Local Groups: از این گروه برای مدیریت مجوزها روی منابع استفاده می‌شود.
- Global Groups: از این گروه برای گروه‌بندی اشیای مختلف بر اساس نوع کار استفاده می‌شود.
- Universal Groups: از این گروه برای مدیریت مجوزها روی منابع در بیش از یک Domain استفاده می‌شود.

کارگاه ۵ ایجاد حساب گروهی و عضو کردن کاربر در آن

۱ یک OU به نام Site1-Groups ایجاد کنید.

۲ یک حساب گروهی در واحد سازمانی Site1-Groups ایجاد کنید.

روی واحد سازمانی Site1-Groups راست کلیک کرده، گزینه New و سپس گزینه Group را انتخاب کنید (شکل ۱۸) و صفات حساب گروهی به نام G-teacher را تعیین کنید (شکل ۱۹).



شکل ۱۸-مسیر دسترسی به کادر محاوره‌ای ایجاد حساب گروهی



شکل ۱۹- کادر محاوره‌ای ایجاد حساب گروهی

۳ گروه دیگری به نام G-mail از نوع Distribution ایجاد کنید.

هر دو گروه را در واحد سازمانی Site1-Groups مشاهده می‌کنید.

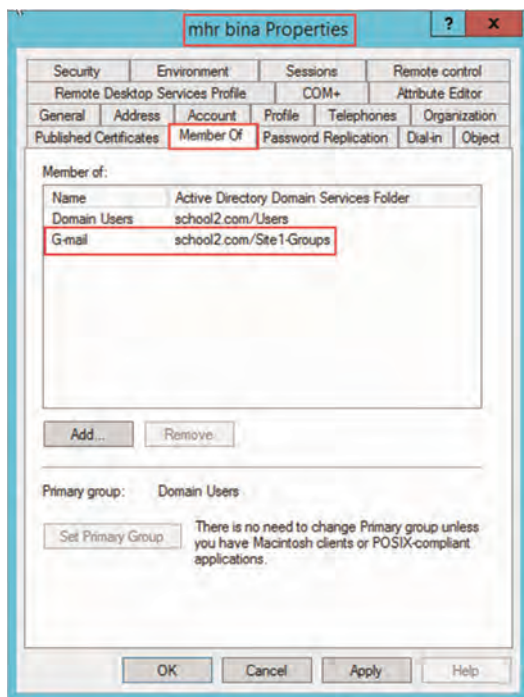
۴ کاربرد گروه‌های Security و Distribution را بررسی کنید.

در یکی از درایوها پوشه‌ای ایجاد کرده، سپس کادر محاوره‌ای انتخاب نام کاربر یا گروه مربوط به مجوزهای این پوشه را باز کنید.

در فهرست نمایش داده شده، نام کدام یک از گروه‌های G-mail و G-teacher نمایش داده می‌شود؟

کنجکاوی





شکل ۲۰- برگه Member of

۵ حساب کاربری را در گروه عضو کنید.

روی حساب کاربری mhr bina راست کلیک کرده، سربرگ Member Of را از کادر محاوره‌ای مشخصات کاربر انتخاب کنید. با استفاده از دکمه Add گروه G-mail را انتخاب کنید تا کاربر mhr bina عضو گروه G-mail شود (شکل ۲۰).

گروهی با نام G-student ایجاد کنید و سپس با استفاده از زبانه Members پنجره مشخصات آن، حساب کاربری خودتان را عضو گروه کنید.

فعالیت
کارگاهی



ارزشیابی مرحله ۲

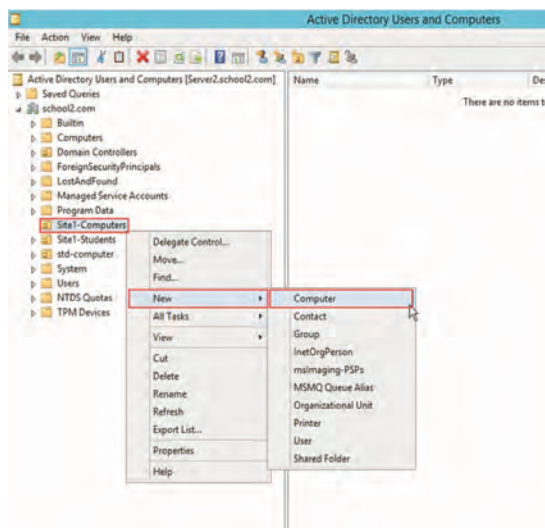
نمره	استاندارد (شاخص‌ها/دآوری/نمره دهی)	نتایج ممکن	شرایط عملکرد (ابزار، مواد، تجهیزات، زمان، مکان و...)	مراحل کار
۳	ایجاد OU، حساب کاربری و حساب گروهی - انجام تنظیمات حساب کاربری - عضو کردن کاربر در گروه باتوجه به مسئولیت کاربر	بالاتر از حد انتظار	مکان: کارگاه استاندارد رایانه تجهیزات: شبکه‌ای از رایانه‌ها که حداقل یکی از آنها دارای سیستم عامل سرور باشد. زمان: ۳۵ دقیقه	مدیریت کاربران
۲	ایجاد OU، حساب کاربری و حساب گروهی - انجام تنظیمات حساب کاربری - عضو کردن کاربر در گروه	در حد انتظار		
۱	ایجاد OU، حساب کاربری و حساب گروهی	پایین تر از حد انتظار		



مدیریت رایانه‌های سرویس گیرنده

رایانه‌ها نیز همانند کاربران که با حساب کاربری خود شناسایی می‌شوند، دارای یک حساب رایانه‌ای هستند.

کارگاه ۶ ایجاد حساب رایانه‌ای



وقتی رایانه‌ای را عضو Domain می‌کنیم، به صورت خودکار AD بر اساس نام آن (Computer Name) یک حساب رایانه‌ای برای آن در پوشه Computers ایجاد می‌کند. چون این رایانه عضو پوشه پیش فرض می‌شود، قابل مدیریت برای تنظیم سیاست نیست. به همین دلیل بهتر است قبل از عضو کردن آن، ابتدا یک OU بسازیم و سپس یک حساب رایانه‌ای بر اساس نام آن، درون OU ایجاد کنیم.

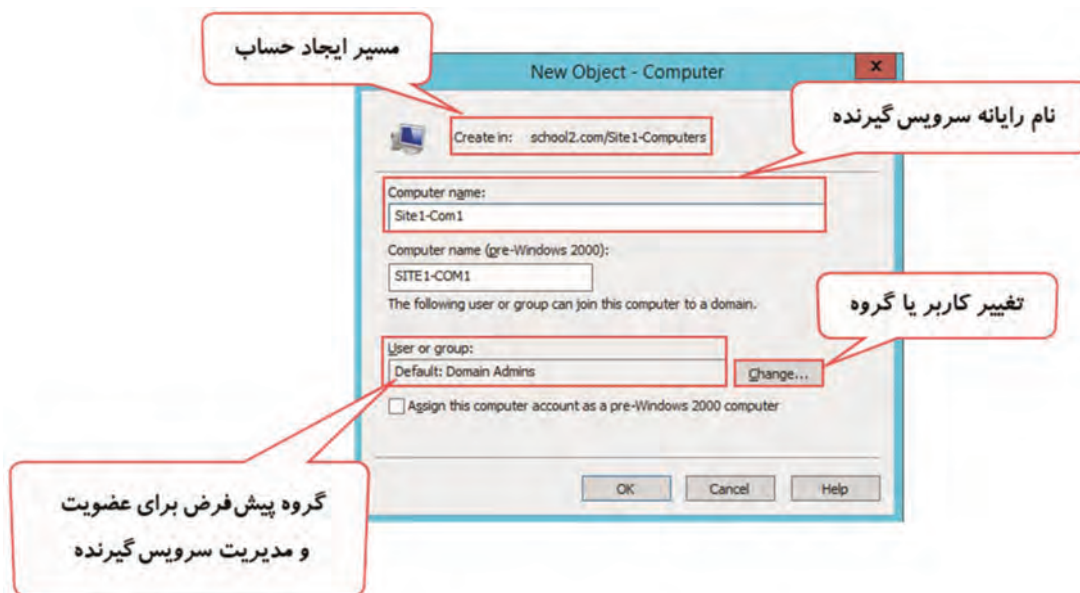
۱ یک OU به نام Site1-Computers ایجاد کنید.

۲ یک حساب رایانه‌ای ایجاد کنید.

شکل ۲۱- مسیر دسترسی به کادر محاوره‌ای ایجاد حساب رایانه‌ای

پنجره New Object - Computer را باز کنید.

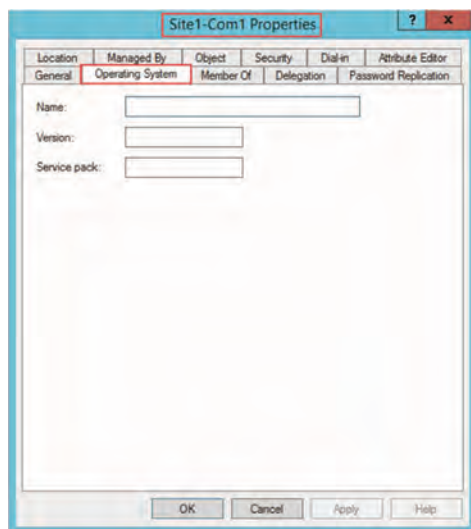
روی واحد سازمانی Site1-Computers راست کلیک کرده، گزینه New و سپس گزینه Computer را انتخاب کنید (شکل ۲۱). در کادر محاوره‌ای باز شده، صفات حساب رایانه‌ای را تعیین کنید (شکل ۲۲).



شکل ۲۲- کادر محاوره‌ای ایجاد حساب رایانه‌ای



شکل ۲۳- تطبیق نام رایانه با نام حساب رایانه‌ای



شکل ۲۴- برگه مشخصات سیستم عامل حساب رایانه‌ای

نام رایانه‌ای که در حساب رایانه‌ای تایپ می‌کنید باید دقیقاً با نام رایانه در برگه Computer Name کادرمحاوره‌ای System Properties رایانه سرویس گیرنده یکسان باشد. در غیر این صورت در زمان عضویت رایانه، AD بر اساس نام آن رایانه یک حساب رایانه‌ای در پوشه پیش فرض می‌سازد (شکل ۲۳).

با تأیید پنجره New Object-Computer حساب رایانه‌ای با نام Site1-Com1 ایجاد می‌شود.

۲۳ مشخصات حساب رایانه‌ای را مشاهده کنید.

کادرمحاوره‌ای Properties حساب رایانه را باز کرده، برگه Operating System را انتخاب کنید. چون هنوز سرویس گیرنده عضو DC نشده است مشخصات سیستم عامل خالی است (شکل ۲۴).

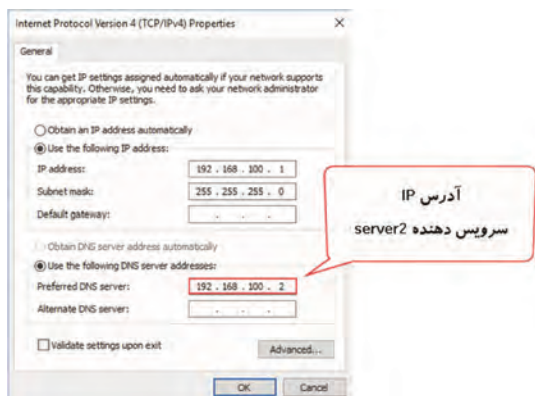
به طور پیش فرض فقط اعضای گروه Domain Admins مانند کاربر Administrator می‌توانند رایانه‌ای را که برایش حساب رایانه‌ای ساخته‌اید عضو Domain کنند، مگر آنکه هنگام ایجاد حساب رایانه‌ای، در کادر User or group کاربر یا گروهی را برای انجام این کار تعیین کرده باشید (شکل ۲۲).

کارگاه ۷ عضویت رایانه‌های سرویس گیرنده در DC

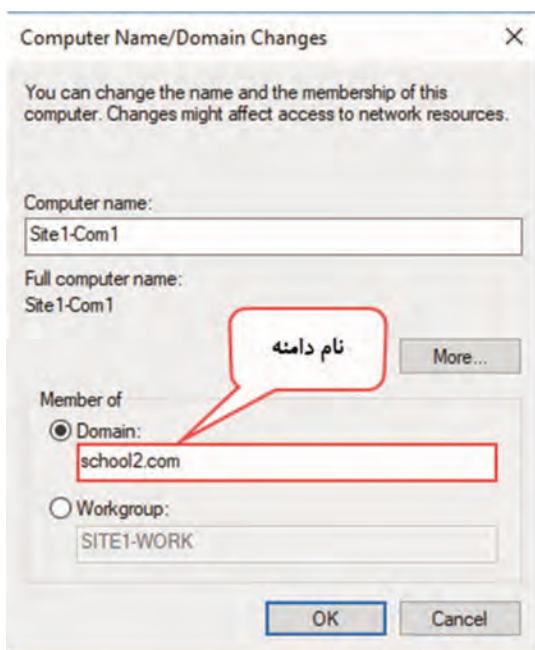
برای کنترل رایانه‌های شبکه به وسیله سرویس دهنده DC و ایجاد شبکه Domain باید آنها را عضو DC کنیم. برای انجام این کارگاه و فعالیت‌های آن، به سه رایانه یکی به عنوان سرویس دهنده DC و دو رایانه دیگر به عنوان سرویس گیرنده با سیستم عامل ویندوز ۱۰ برای هر گروه نیاز داریم. رایانه سرویس دهنده DC را server2 و سرویس گیرنده‌ها را Site1-Com1 و Site1-Com3 می‌نامیم (شکل ۲۵).



شکل ۲۵- نام رایانه‌های کارگاه ۷ و سیستم عامل آنها



شکل ۲۶- کادر محاوره‌ای تنظیمات کارت شبکه IP



شکل ۲۷- کادر محاوره‌ای تغییر عضویت



شکل ۲۸- کادر دریافت نام کاربری و گذرواژه کاربر مجاز به عضو کردن رایانه

در کارگاه ۶ برای رایانه Site1-Com1 حساب رایانه‌ای ایجاد کردیم.

۱ با حساب کاربری Administrator وارد DC (server2) شوید.

۲ با حساب کاربری عضو گروه Administrators به ویندوز ۱۰ رایانه Site1-Com1 وارد شوید.

۳ DNS server سرویس گیرنده Site1-Com1 را تعیین کنید.

کادر محاوره‌ای تنظیم آدرس IP رایانه Site1-Com1 را باز کنید و در کادر Preferred DNS server آدرس IP سرویس دهنده (server2) را تایپ کنید (شکل ۲۶).

۴ سرویس گیرنده Site1-Com1 را عضو DC کنید.

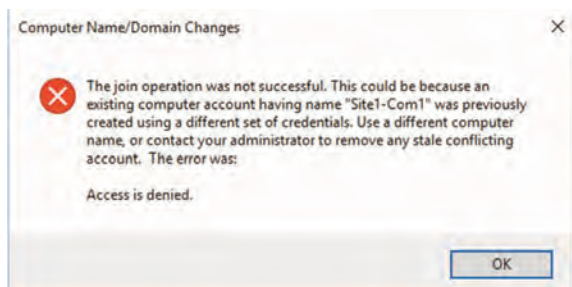
کادر محاوره‌ای تغییر نام رایانه سرویس گیرنده را باز کنید. رایانه سرویس گیرنده روی حالت Workgroup است. برای تغییر عضویت آن، گزینه Domain را انتخاب کرده، نام دامنه server2 (school2.com) را تایپ کنید (شکل ۲۷).

۵ تغییر عضویت را تأیید کنید.

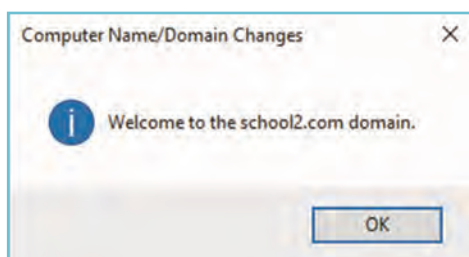
با انتخاب دکمه OK، کادر دریافت نام کاربری و گذرواژه کاربر مجاز به عضو کردن رایانه، نمایش داده می‌شود (شکل ۲۸).

نام و گذرواژه حساب کاربری که برای شما در دامنه ایجاد شده را تایپ کنید. نتیجه چه خواهد شد؟

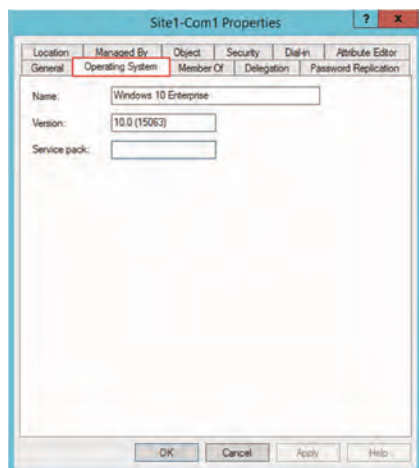
پیام خطای شکل ۲۹ را ترجمه کرده، دلیل نمایش آن را توضیح دهید.



شکل ۲۹- پیام خطا هنگام عضویت در Domain



شکل ۳۰- پیام خوش آمدگویی ورود به دامنه



شکل ۳۱- مشخصات سیستم عامل حساب رایانه‌ای

دکمه OK کادر پیام را کلیک کنید تا کادر دریافت نام کاربری و گذرواژه نمایش یابد. این بار مشخصات حساب کاربری Administrator رایانه DC را تایپ کنید. پیام خوش آمدگویی ورود به دامنه را تأیید کنید (شکل ۳۰).

بدین ترتیب رایانه سرویس گیرنده عضو سرویس دهنده DC می شود.

۶ رایانه را راه اندازی مجدد کنید.

۷ مشخصات سیستم عامل رایانه سرویس گیرنده را مشاهده کنید.

پس از عضو شدن رایانه سرویس گیرنده، ابزار Active Directory Users and Computers را در رایانه DC (server2) باز کنید. روی حساب رایانه‌ای Site1-Com1 راست کلیک کرده و گزینه Properties را انتخاب کنید. در برگه Operating System می توانید مشخصات سیستم عامل رایانه سرویس گیرنده را مشاهده کنید (شکل ۳۱).

رایانه Site1-Com3 را بدون تعریف حساب رایانه‌ای برای آن، عضو server2 کنید. در کادر ورود مشخصات حساب کاربری برای عضویت کاربر، نام و گذرواژه حساب کاربری خودتان در دامنه را تایپ کنید. نتیجه چه خواهد شد؟ حساب رایانه‌ای سرویس گیرنده Site1-Com3 در کدام پوشه ایجاد می شود؟

اگر برای رایانه‌ای حساب رایانه‌ای تعریف نکنید، همه کاربران تعریف شده در AD می توانند آن را عضو Domain کنند. هر کاربر می تواند حداکثر ۱۰ رایانه را عضو کند.



شکل ۳۲- صفحه ورود به محیط ویندوز

Log On به سرویس گیرنده عضو DC

با عضو شدن سرویس گیرنده در Domain صفحه ورود به ویندوز تغییر می کند. بدین ترتیب دو حالت برای ورود داریم (شکل ۳۲).

- ورود به Domain با استفاده از حساب کاربری تعریف شده در AD
- ورود به رایانه با استفاده از حساب کاربری محلی

با استفاده از مشخصات حساب کاربری mhr bina به رایانه Site1-Com1 وارد شوید.

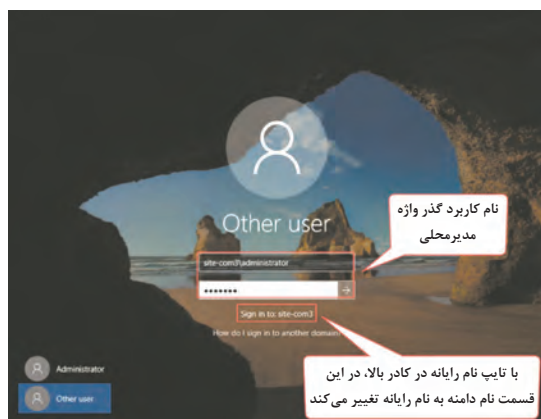
فعالیت
کارگاهی



کنجکاوی



آیا می توانیم از Full name برای ورود به Domain استفاده کنیم؟ چرا؟



شکل ۳۳- ورود به محیط ویندوز برای رایانه عضو DC

برای وارد شدن محلی به سیستم عامل سرویس گیرنده ای که عضو DC شده است باید در کادر محاوره ای دریافت نام کاربر، از قالب زیر استفاده کنیم.
Computer name\user name

برای سرویس گیرنده Site1-Com3 باید: Site1-Com3\administrator را تایپ کرده و سپس گذرواژه را وارد کنید (شکل ۳۳).

کارگاه ۸ حذف ابزارهای AD و سرویس ADDS

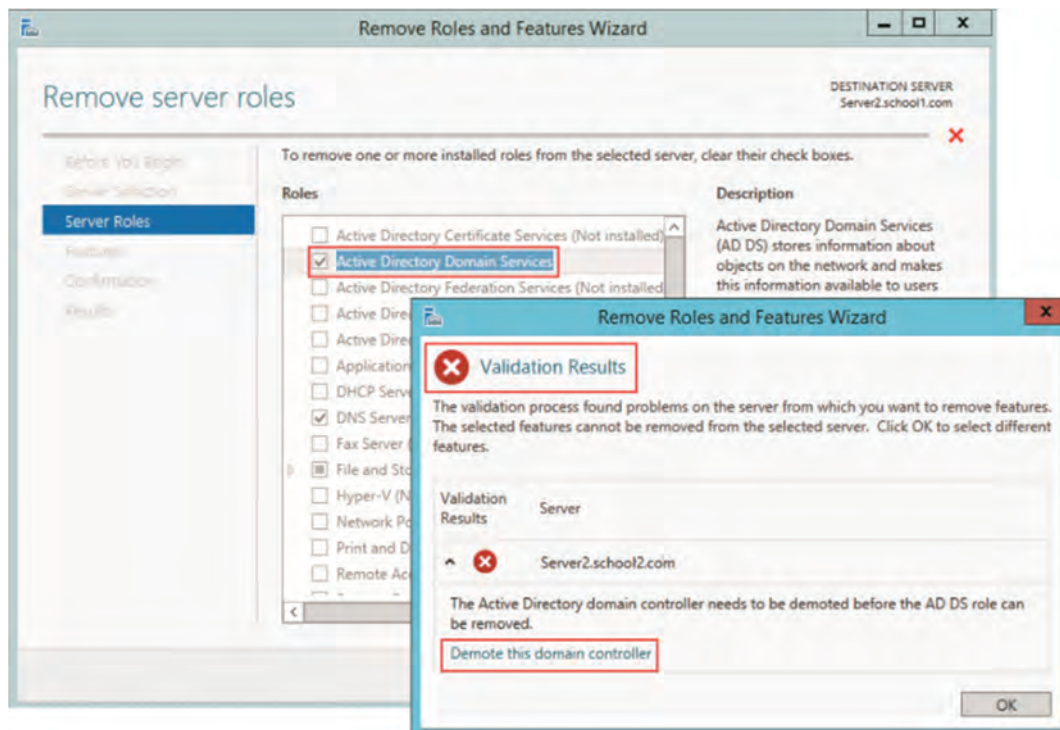
برای حذف DC، باید ابتدا ابزارهای AD و سپس سرویس ADDS را حذف کنیم.

۱ با حساب کاربری Administrator وارد ویندوز سرور شوید.

۲ برنامه Server Manager را باز کنید.

۳ برای حذف سرویس ADDS اقدام کنید.

از منوی Manage گزینه Remove Roles And Features را انتخاب کرده، روی گزینه Active Directory Domain Services کلیک کنید. پنجره حذف ویژگی‌های آن باز می‌شود. دکمه Remove Features را کلیک کنید. در کادر باز شده روی گزینه Demote this domain controller کلیک کنید (شکل ۳۴).



شکل ۳۴- کادر محاوره‌ای حذف DC

۴ مراحل ویزارد را برای حذف DC دنبال کنید.

- گزینه Force the removal of this domain controller را انتخاب کرده، دکمه Next را کلیک کنید.
- برای دریافت تأیید عمل حذف، کادر محاوره‌ای هشدار نمایش داده می‌شود، گزینه Proceed with removal را انتخاب کنید و دکمه Next را کلیک کنید.
- در کادر محاوره‌ای New Administrator Password گذرواژه جدیدی تعریف کنید و دکمه Next را کلیک کنید. با این کار، گذرواژه حساب کاربری Administrator به گذرواژه جدید تغییر می‌کند.
- دکمه Demote را کلیک کنید.
- با اتمام مراحل، رایانه راه‌اندازی مجدد می‌شود و ابزارهای AD حذف می‌شوند اما هنوز سرویس ADDS فعال است.

۵ با حساب کاربری Administrator و با گذرواژه جدید، به ویندوز وارد شوید.

۶ مراحل ۲ تا ۴ را مجدداً انجام دهید.

- با اتمام مراحل، رایانه را راه‌اندازی مجدد کنید. پس از ورود به ویندوز با کمی تأخیر، کادر محاوره‌ای برای تأیید حذف سرویس ADDS ظاهر می‌شود. دکمه Close را کلیک کنید. بدین ترتیب سرویس ADDS حذف می‌شود.



مراحل کار	شرایط عملکرد (ابزار، مواد، تجهیزات، زمان، مکان و...)	نتایج ممکن	استاندارد (شاخص‌ها/دآوری/نمره دهی)	نمره
اتصال به DC	مکان: کارگاه استاندارد رایانه تجهیزات: شبکه‌ای از رایانه‌ها که حداقل یکی از آنها دارای سیستم عامل سرور باشد. زمان: ۳۵ دقیقه	بالاتر از حد انتظار	ایجاد حساب رایانه‌ای و مشاهده مشخصات آن - عضویت رایانه‌های Log On - DC سرویس گیرنده در به سرویس گیرنده عضو DC - حذف ابزارهای AD و سرویس ADDS	۳
		در حد انتظار	ایجاد حساب رایانه‌ای و مشاهده مشخصات آن - عضویت رایانه‌های سرویس گیرنده در Log On - DC به سرویس گیرنده عضو DC	۲
		پایین تر از حد انتظار	ایجاد حساب رایانه‌ای و مشاهده مشخصات آن	۱

Group Policy

سیاست‌ها (Policies) یکی از قابلیت‌های مهم سیستم‌عامل‌ها هستند که به شما امکان مدیریت و کنترل کاربران و رایانه‌ها را به صورت متمرکز می‌دهند تا بتوانید محیطی امن برای آنها ایجاد کنید. برای مثال سیاستی وجود دارد که از دسترسی کاربر به محیط ویرایش رجیستری جلوگیری می‌کند. رجیستری بانک اطلاعاتی است که سیستم‌عامل اطلاعات پیکربندی خود را درون آن نگهداری می‌کند. اگر سیاست جلوگیری از ویرایش رجیستری را تنظیم و اعمال کنید، کاربران نمی‌توانند به محیط رجیستری دسترسی پیدا کنند و پیکربندی سیستم‌عامل را تغییر دهند. سیاست دیگری که برای امنیت رایانه استفاده می‌شود، غیرفعال کردن کاربر Administrator است. این دو مثال به نکته مهمی اشاره می‌کنند. برخی از سیاست‌ها مانند عدم دسترسی به محیط رجیستری روی کاربران اعمال می‌شوند، صرف نظر از رایانه‌ای که کاربر به آن وارد می‌شود. به چنین سیاست‌هایی تنظیمات کاربر (User Configuration) می‌گویند. تنظیمات کاربر از زمان ورود کاربر به سیستم‌عامل، روی حساب کاربری اعمال می‌شوند.

گروه دیگری از سیاست‌ها مانند غیرفعال کردن کاربر Administrator روی رایانه اعمال می‌شوند، صرف نظر از اینکه کدام کاربر به رایانه وارد می‌شود. به چنین سیاست‌هایی تنظیمات رایانه (Computer Configuration) می‌گویند. تنظیمات رایانه از زمان روشن کردن رایانه و قبل از ورود کاربر به سیستم‌عامل، روی رایانه اعمال می‌شوند.

ابزارهای پیکربندی Group Policy

مدیران IT در سازمان‌ها برای پیکربندی سیاست‌ها در Domain از ابزار Group Policy Management و برای شبکه‌های گروه کاری از ابزار جایگزینی به نام Local Group Policy Editor استفاده می‌کنند. ابزار Local Security Policy که برای پیکربندی سیاست‌های امنیتی روی رایانه‌های شخصی استفاده می‌شود، زیرمجموعه‌ای از Local Group Policy Editor است.

به یک یا چند سیاست که برای کاربران و رایانه‌ها پیکربندی می‌شوند، GPO (Group Policy Object) می‌گویند. اگر GPOها با Local Group Policy Editor ایجاد شوند، به صورت محلی در رایانه ذخیره می‌شوند. به همین دلیل به آنها LGPO (Local GPO) می‌گویند. سیاست‌های LGPO فقط روی رایانه‌هایی اعمال می‌شوند که در آن ذخیره شده‌اند؛ بنابراین بهتر است از آنها برای رایانه‌های شخصی یا رایانه‌های عضو شبکه گروه کاری استفاده کنیم. برای پیکربندی LGPOها می‌توان از دو ابزار Local Group Policy Editor و Local Security Policy استفاده کرد.

کارگاه ۹ پیکربندی LGPO

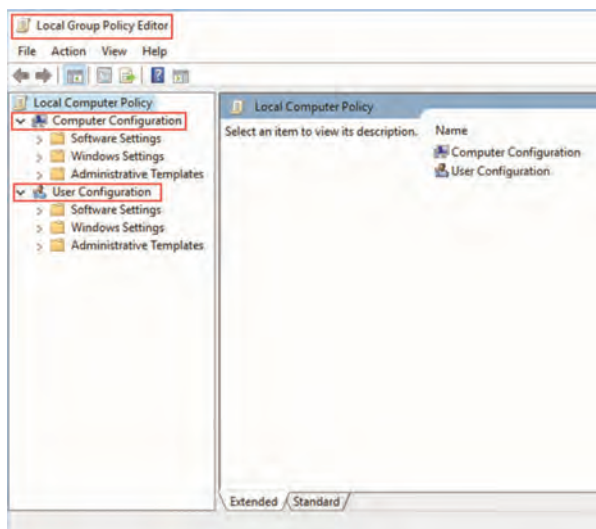
این کارگاه را روی سرویس‌دهنده DC انجام ندهید.

۱ با کاربر Administrator به محیط ویندوز وارد شوید.

۲ پنجره رجیستری را باز کنید.

دستور regedit را به وسیله کادر محاوره‌ای Run اجرا کنید. پنجره رجیستری باز می‌شود. آن را ببندید.

۳ پنجره Local Group Policy Editor را باز کنید (شکل ۳۵).

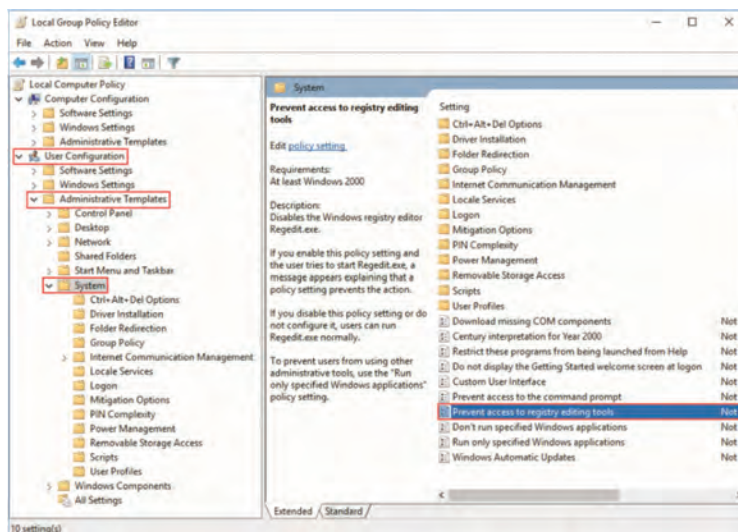


شکل ۳۵- پنجره Local Group Policy Editor

در کادر جست‌وجوی نوار وظیفه عبارت Edit group policy را تایپ و آن را انتخاب کنید. می‌توانید از دستور gpedit.msc در کادر محاوره‌ای Run نیز برای ورود به این ابزار استفاده کنید.

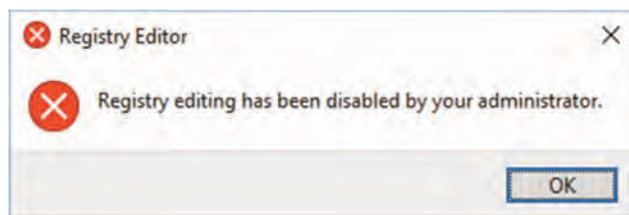
۴ سیاست جلوگیری از ویرایش رجیستری را فعال کنید.

از بخش User Configuration مسیر Administrative Templates/system را انتخاب کرده، سیاست Prevent access to registry editing tools را فعال کنید (شکل ۳۶).



شکل ۳۶- دسترسی به تنظیمات سیاست Prevent access to registry editing tools

روی سیاست Prevent access to registry editing tools دابل کلیک کنید. در کادر باز شده گزینه Enabled را فعال کرده، دکمه OK را کلیک کنید. برخی از سیاست‌ها بلافاصله پس از تنظیم اعمال می‌شوند. اما بیشتر آنها هر ۹۰ تا ۱۲۰ دقیقه یک‌بار refresh می‌شوند. در صورتی که بخواهید زودتر اعمال شوند از دستور gpupdate در کادر محاوره‌ای Run استفاده کنید. پنجره رجیستری را باز کنید (شکل ۳۷).



شکل ۳۷- پیام غیرفعال بودن ویرایش رجیستری

- پیام شکل ۳۷ را ترجمه کنید.
- سیاستی تنظیم کنید که به روزرسانی خودکار ویندوز (Windows Update) غیرفعال شود.

فعالیت
کارگاهی



اگر GPOها با Group Policy Management ایجاد شوند، روی اشیا Domain اعمال می‌شوند و در DC ذخیره می‌شوند به همین دلیل به آنها Domain Base GPO می‌گویند. Domain Base GPOها روی اشیای تعریف شده در AD تنظیم می‌شوند و از آنها برای مدیریت متمرکز کاربران و رایانه‌ها در شبکه Domain استفاده می‌شود.

فیلم شماره ۱۲۱۲۰: ایجاد Domain Base GPO

فیلم



فعالیت
کارگاهی



- پس از مشاهده فیلم روی رایانه خود، سرویس ADDS را نصب و پیکربندی کنید.
- OU به نام std-electronic ایجاد کرده، در آن برای هم گروهی های خود حساب کاربری ایجاد کنید.
- یک GPO تعریف کنید که هیچ یک از کاربران std-electronic نتوانند به محیط ویرایش رجیستری دسترسی داشته باشند.

چون Containerها به وسیله AD ایجاد و مدیریت می شوند، نمی توانیم روی آنها سیاست تعریف کنیم به همین دلیل نام آنها را در پنجره Group Policy Management مشاهده نمی کنید.

یادداشت



سیاست های حساب کاربری (Account Policies)

سیاست های تعریف شده برای حساب کاربری شامل دو بخش Password Policy و Account Lockout Policy هستند. Password Policy با کنترل نحوه تعریف و مدیریت گذرواژه، امنیت رایانه شما را افزایش می دهد.

فیلم شماره ۱۲۱۲۱: ایجاد Password Policy

فیلم



فعالیت
کارگاهی



- پس از مشاهده فیلم GPO تعریف کنید که همه کاربران std-electronic در هنگام تعیین و یا تغییر گذرواژه خود مجبور شوند آن را به صورت پیچیده و با حداقل طول ۱۰ نویسه تعریف کنند و نتوانند از ۵ گذرواژه قبلی خود استفاده کنند.

Account Lockout Policy

یک هکر می تواند نام کاربری یا گذرواژه شما را بر اساس اطلاعات ذخیره شده در رایانه مثل نشانی E-mail، نام و نام خانوادگی و شماره کارمندی و... حدس بزند. هکر پس از پیدا کردن نام کاربری، سعی می کند گذرواژه صحیح را با ترکیب کردن اطلاعات به دست آمده حدس بزند و برای بررسی درستی گذرواژه ای که حدس زده، برای ورود به محیط کاربری از آن استفاده می کند. این حملات را می توانید با کم کردن تعداد logon ها خنثی کنید. این رفتار را در دستگاه های ATM مشاهده کرده اید. با ۳ بار اشتباه وارد کردن گذرواژه، کارت عابر بانک به وسیله دستگاه ضبط می شود. این رفتارها به وسیله سیاست های Account Lockout Policy مدیریت می شوند. سیاست های این بخش به مدیر شبکه اجازه می دهد که بتواند حداکثر تعداد دفعات logon ناموفق یک کاربر را مشخص کند و در صورت رخ دادن این تعداد ورود ناموفق، از دسترسی کاربر برای مدت زمان مشخص به رایانه جلوگیری کند. وقتی نام یا گذرواژه کاربری اشتباه تایپ شود، رایانه به کمک سیاست های امنیتی تعریف شده، آن حساب کاربری را قفل (lock) می کند تا از ورود افراد ناشناس با حساب کاربری دیگران جلوگیری کند.

کارگاه ۱۰ پیکربندی Account Lockout Policy

این کارگاه را روی سرویس دهنده DC یا سرویس گیرنده عضو آن انجام ندهید.

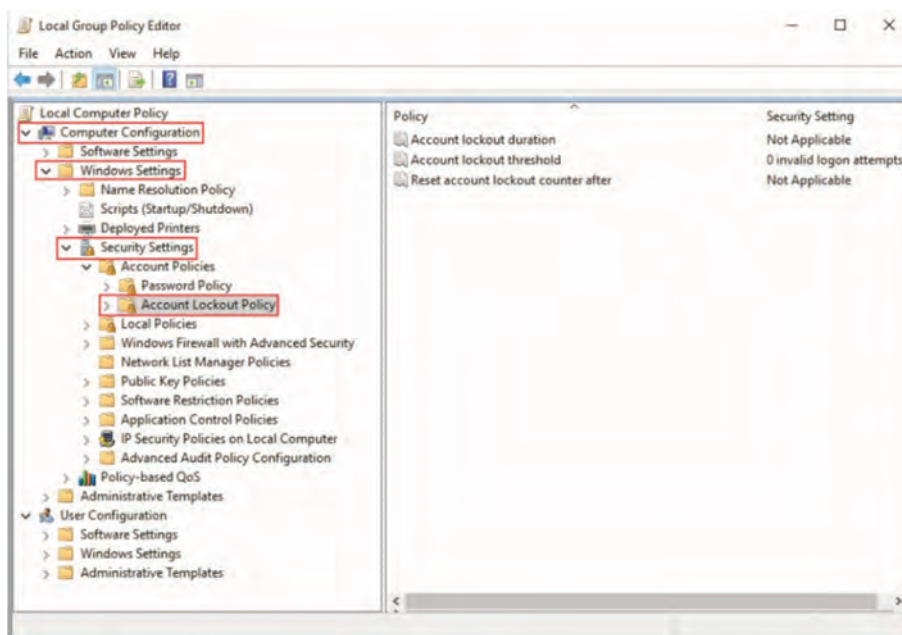
۱ با کاربر عضو گروه Administrators به محیط ویندوز وارد شوید.

۲ پنجره Local Group Policy Editor را باز کنید.

۳ به بخش تنظیم سیاست های Account Lockout Policy بروید.

از بخش Computer Configuration مسیر Windows Settings/Security Settings را انتخاب کرده،

گزینه Account Policies را باز کنید و سپس روی Account Lockout Policy دابل کلیک کنید (شکل ۳۸).



شکل ۳۸- دسترسی به سیاست های Account Lockout Policy

۴ حداکثر تعداد دفعات ورود اشتباه گذرواژه را که منجر به قفل شدن حساب کاربری می شود، تعیین کنید.

روی سیاست Account lockout threshold دابل کلیک کرده، عدد ۳ را تنظیم کنید.

۵ مدت زمان قفل شدن حساب کاربری را تعیین کنید.

روی سیاست Account lockout duration دابل کلیک کرده، زمان ۵ دقیقه را تنظیم کنید.

۶ تنظیمات انجام شده را اعمال کنید.

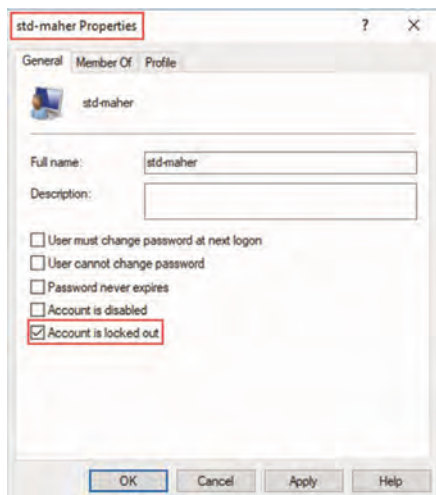
برای اعمال تنظیمات باید سیاست ها به روزرسانی شود. در کادر محاوره ای Run دستور gpupdate را تایپ کرده، دکمه OK را کلیک کنید.

۷ صحت عملکرد سیاست تعیین شده را بررسی کنید.

از محیط کاربری Administrator خارج شوید و با حساب کاربری خود، ۳ مرتبه گذرواژه را اشتباه تایپ کنید. سپس سعی کنید برای بار چهارم با گذرواژه صحیح وارد ویندوز شوید. چه اتفاقی می افتد؟

Unlocking a User Account

یکی دیگر از وظایف مدیریتی روی حساب کاربری، خارج کردن حساب کاربری از حالت Lock است. برای خارج کردن حساب کاربری از حالت lock دو راه وجود دارد:



- مدت زمان مشخص شده در سیاست مربوطه برای lock سپری شود. (برای مثال ما ۵ دقیقه)

- مدیر در پنجره مشخصات کاربر در بخش Computer Management، گزینه Account is locked out را غیرفعال کند (شکل ۳۹).

شکل ۳۹- خارج کردن حساب کاربری از حالت lock

در AD چگونه می توان حساب کاربری را از حالت Lock خارج کرد؟

کنجکاوی



در مورد سیاست Reset account lockout counter after تحقیق کنید.

پژوهش



ارزشیابی مرحله ۴

مرحله کار	شرایط عملکرد (ابزار، مواد، تجهیزات، زمان، مکان و ...)	نتایج ممکن	استاندارد (شاخص ها/داوری /نمره دهی)	نمره
تنظیم سیاست های امنیتی کاربران	مکان: کارگاه استاندارد رایانه تجهیزات: شبکه ای از رایانه ها که حداقل یکی از آنها دارای سیستم عامل سرور باشد. زمان: ۲۵ دقیقه	بالاتر از حد انتظار	ایجاد و تنظیم user policy و group policy - پیکربندی سیاست های گذرواژه و حساب کاربری	۳
		در حد انتظار	ایجاد و تنظیم user policy و group policy	۲
		پایین تر از حد انتظار	انجام ۱ مورد از ۳ مورد ایجاد و تنظیم user policy	۱

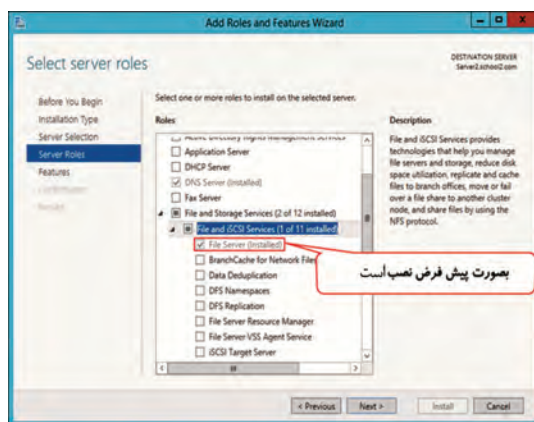


مدیریت پرونده‌ها

داده‌های مختلف مثل اسناد مالی، طرح‌های توسعه و فهرست‌های فروش سازمان‌ها و شرکت‌ها در پرونده‌ها و پوشه‌ها ذخیره می‌شوند. بنابراین مدیران برای اینکه بتوانند این منابع را مدیریت کنند و در اختیار کاربران شبکه قرار دهند، باید آنها را به اشتراک بگذارند. اشتراک گذاری با متمرکز کردن اسناد در یک پوشه، به مدیریت راحت‌تر آنها کمک می‌کند و به کاربران اجازه می‌دهد تا با استفاده از مجوز مناسب و دسترسی به شبکه به پرونده‌ها دسترسی پیدا کنند. ویندوز سرور دارای سرویسی به نام File Services یا سرویس‌های پرونده است که با استفاده از ویژگی‌های مختلف، پوشه‌ها و پرونده‌ها را به اشتراک می‌گذارد و آنها را مدیریت می‌کند. برای انجام کارگاه‌ها و فعالیت‌های این بخش برای هر گروه، به دو رایانه سرویس‌دهنده و یک رایانه

سرویس‌گیرنده نیاز داریم. یکی از سرویس‌دهنده‌ها را به عنوان سرویس‌دهنده DC پیکربندی کنید و دیگری را به همراه سرویس‌گیرنده عضو DC کنید. رایانه سرویس‌دهنده DC را server2، سرویس‌دهنده عضو را server1 و سرویس‌گیرنده ویندوز ۱۰ را Site-Com3 می‌نامیم.

با نصب سیستم‌عامل سرور ۲۰۱۲، File Services به صورت پیش فرض نصب می‌شود (شکل ۴۰). به کمک هنرآموز خود، این سرویس را Uninstall کنید، سپس کارگاه ۱۱ را انجام دهید.



شکل ۴۰ - File Services

کارگاه ۱۱ نصب File Services

- ۱ با حساب کاربری Administrator وارد ویندوز سرور رایانه DC (server2) شوید.
- ۲ File Services را انتخاب کنید.

این سرویس را از مسیر File And Storage Services/File And iSCSI Services در پنجره Server Roles انتخاب کرده، دکمه Next را کلیک کنید.

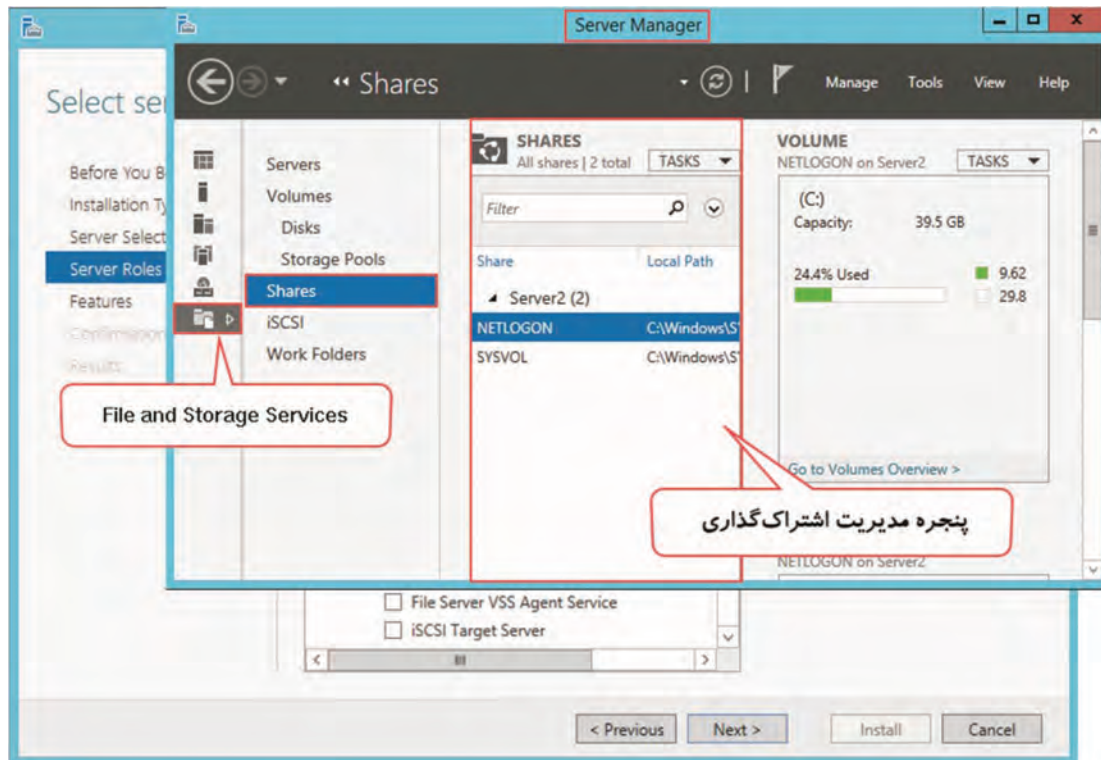
- ۳ سرویس را نصب کنید.

دکمه Install را کلیک کنید.

کارگاه ۱۲ اشتراک پوشه با استفاده از ابزار File And Storage Services

- در شبکه‌های گروه‌کاری و کوچک از گزینه Share With و در شبکه‌های توسعه یافته، از زبانه Sharing پنجره Properties برای اشتراک گذاری استفاده می‌کنیم. اما در شبکه‌های بزرگ برای کنترل متمرکز منابع اشتراکی روی همه دیسک‌ها در سرورهای مختلف، از ابزار File And Storage Services استفاده می‌کنیم.
- ۱ با حساب کاربری Administrator وارد ویندوز سرویس‌دهنده پرونده (server2) شوید.

۲ در پنجره Server Manager نماد File And Storage Services را انتخاب کنید (شکل ۴۱).



شکل ۴۱- پنجره مدیریت اشتراک گذاری

۳ پروفایل اشتراک گذاری را انتخاب کنید.

ویندوز سرور ۲۰۱۲ از دو پروتکل برای اشتراک گذاری استفاده می کند: (Server Message Blocks) SMB: پروتکل استاندارد است که برای اشتراک گذاری پرونده ها در همه نسخه های ویندوز استفاده می شود. (Network File System) NFS: پروتکل استاندارد است که برای اشتراک گذاری پرونده ها در سیستم عامل های Linux و UNIX استفاده می شود. گزینه shares را کلیک کرده، از منوی TASKS گزینه New Share را کلیک کنید. از فهرست File share profile گزینه SMB Share-Quick را انتخاب کنید.

۴ پوشه ای را با نام Program-C و مجوز Change به اشتراک بگذارید.

برای انجام این کار در کادرهای محاوره ای بعدی، نشانی پوشه، نام اشتراکی و مجوز را مشخص کنید.

با استفاده از آدرس UNC به پوشه های اشتراکی رایانه های شبکه متصل شوید.

فعالیت
گروهی



Distribute File System

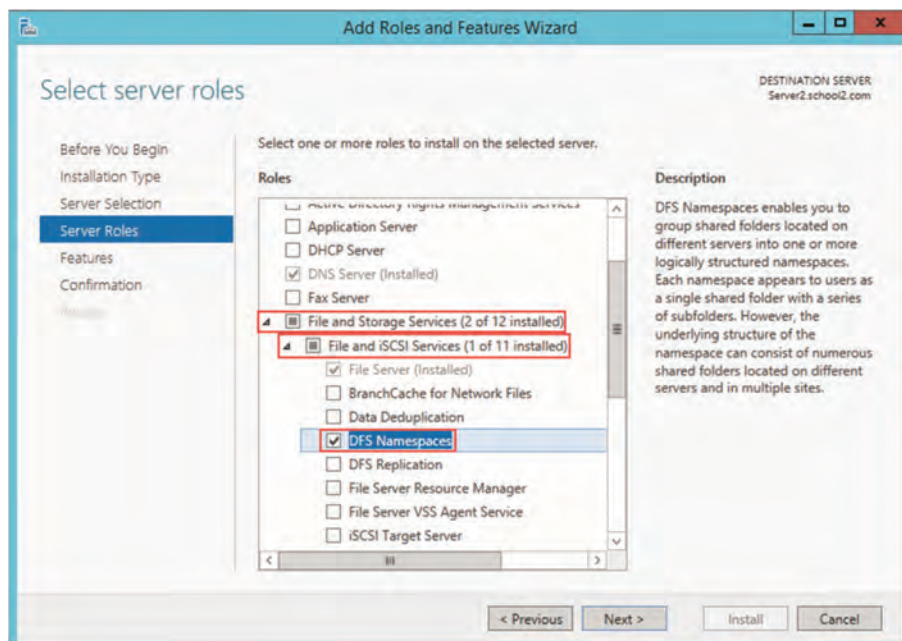
رشته شبکه و نرم افزار رایانه یک هنرستان دو کلاس دارد. هنرجویان کلاس ۱ تمرینات زبان C# را در پوشه‌ای به نام Program-C ذخیره می‌کنند که در رایانه server2 به اشتراک گذاشته شده است. اما هنرجویان کلاس ۲ تمرینات خود را در پوشه اشتراکی Program-C در رایانه server1 قرار می‌دهند. اگر همه هنرجویان بخواهند به این گزارشات دسترسی پیدا کنند باید آدرس پوشه‌های اشتراکی را به طور کامل تایپ کنند. به یاد آوردن نام سرویس دهنده پرونده‌ای که پرونده مورد نظر کاربر در آن ذخیره شده، برای هنرجو دشوار است. DFS یک فضای نامی (namespace) واحد ایجاد می‌کند تا کاربران بتوانند به وسیله آن به هر پوشه اشتراکی در هر سرویس دهنده پرونده در سازمان دسترسی داشته باشند.

کارگاه ۱۳ نصب سرویس DFS

۱ با حساب کاربری Administrator وارد ویندوز سرویس دهنده پرونده (server2) شوید.

۲ سرویس DFS Namespaces را انتخاب کنید.

از مسیر File And Storage Services/File And iSCSI Services در پنجره Server Roles این سرویس را انتخاب کنید (شکل ۴۲). کادر محاوره‌ای نصب ویژگی‌های آن باز می‌شود. دکمه Add Features و سپس Next را کلیک کنید.



شکل ۴۲- مسیر دسترسی به سرویس DFS Namespaces

۳ سرویس DFS Namespaces را نصب کنید.

دکمه Install را کلیک کنید. پس از نصب، ابزار DFS Management به فهرست برنامه‌ها در Server Manager اضافه می‌شود.

در رایانه server1 پوشه‌ای را با نام Program-C و مجوز Change به اشتراک بگذارید. سپس سرویس‌های DFS Namespaces و DFS Replication را نصب کنید. سرویس DFS Replication زیرمجموعه سرویس DFS Namespaces است.

فعالیت
گروهی

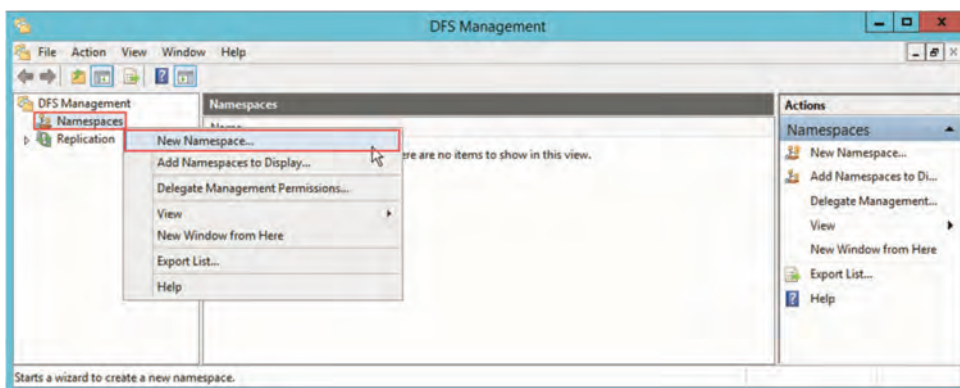


کارگاه ۱۴ ایجاد فضای نامی DFS

۱ ابزار DFS Management را در server2 باز کنید.

۲ برای server2 یک فضای نامی ایجاد کنید.

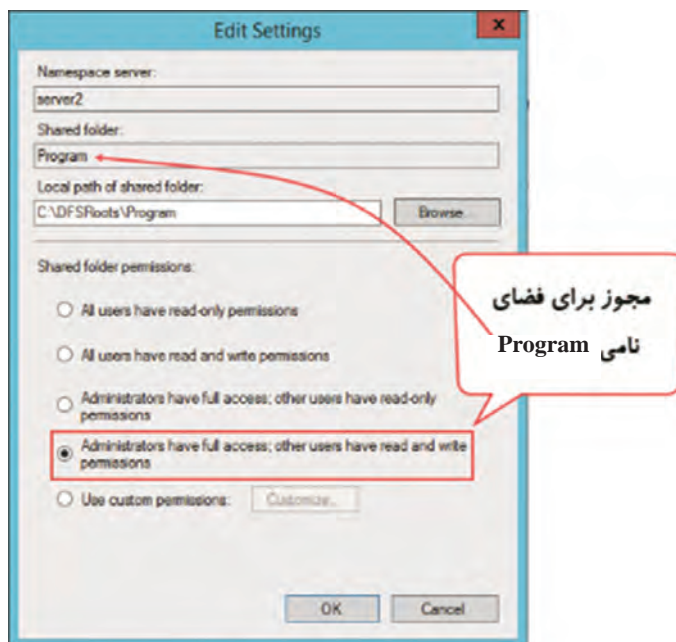
روی گزینه Namespaces راست کلیک کرده، گزینه New Namespaces را انتخاب کنید (شکل ۴۳).
server2 را در پنجره Namespace Server انتخاب کنید و دکمه Next را کلیک کنید.



شکل ۴۳- مسیر دسترسی به پنجره ایجاد فضای نامی

۳ نام و مجوز فضای نامی را تعریف کنید.

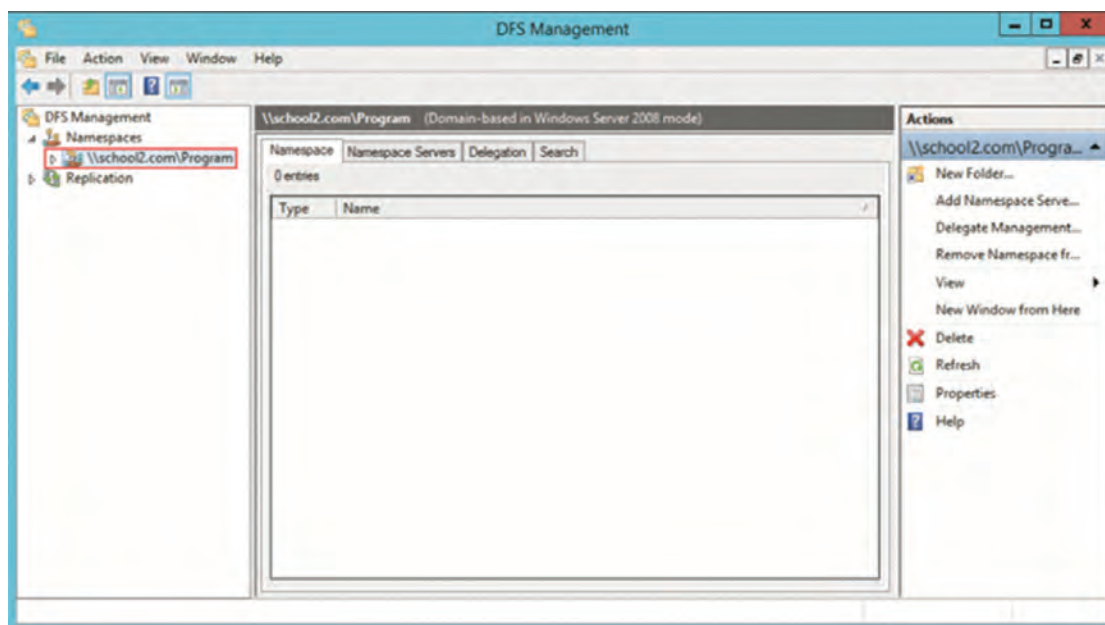
در پنجره Namespace Name and Settings نام Program را تایپ کرده، به کمک دکمه Edit Settings مجوز لازم را انتخاب کنید (شکل ۴۴).



شکل ۴۴- تعیین نام و مجوز فضای نامی

۴ نوع فضای نامی را تعیین کنید.

نوع فضای نامی را Domain-based انتخاب کنید. برای شبکه‌های گروه کاری گزینه Stand-alone انتخاب می‌شود. دکمه Create را کلیک کنید. فضای نامی Program به آدرس \\school2.com\Program ایجاد می‌شود (شکل ۴۵).



شکل ۴۵- فضای نامی اضافه شده به پنجره DFS Management

فیلم شماره ۱۲۱۲۲: افزودن پوشه به DFS Namespace

فیلم

فیلم را مشاهده کنید و فعالیت زیر را انجام دهید.



- برای کارگاه رایانه خود یک سرویس دهنده DC پیکربندی کنید. سپس دو رایانه دیگر با سیستم عامل Server 2012 را عضو DC کنید.

فعالیت
کارگاهی

- هر سه رایانه را به عنوان سرویس دهنده پرونده پیکربندی کنید. سپس در هر سه رایانه پوشه‌هایی را به اشتراک بگذارید و یک فضای نامی در سرویس دهنده DC ایجاد کنید و پوشه‌های اشتراکی هر سه سرویس دهنده را به آن اضافه کنید.



- سایر رایانه‌های شبکه را به عنوان سرویس گیرنده عضو DC کنید.

- در نرم‌افزارهای مختلف اسنادی را ایجاد کنید و آنها را در پوشه‌های اشتراکی ذخیره کنید.

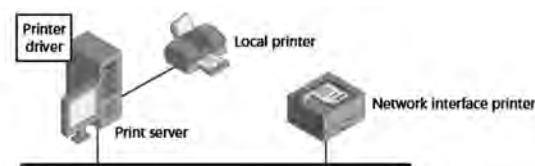
ارزشیابی مرحله ۵



مرحله کار	شرایط عملکرد (ابزار، مواد، تجهیزات، زمان، مکان و ...)	نتایج ممکن	استاندارد (شاخص‌ها/داوری/نمره دهی)	نمره
پایاده سازی File Server	مکان: کارگاه استاندارد رایانه تجهیزات: شبکه‌ای از رایانه‌ها که حداقل یکی از آنها دارای سیستم عامل سرور باشد. زمان: ۲۰ دقیقه	بالاتر از حد انتظار	نصب File Service و اشتراک گذاری منابع در آن - تنظیم مجوزهای مربوطه - نصب سرویس DFS و ایجاد فضای نامی و اشتراک گذاری منابع در آن	۳
		در حد انتظار	نصب File Service و اشتراک گذاری منابع در آن - تنظیم مجوزهای مربوطه	۲
		پایین تر از حد انتظار	نصب File Service	۱

مدیریت چاپگرها

چاپگرها از دستگاه‌هایی هستند که تقریباً همه کاربران در طول روز با آنها سر و کار دارند. بنابراین نیاز است که هر کاربر یک چاپگر در اختیارش باشد؛ اما خرید تعداد زیاد چاپگر برای سازمان‌ها نیاز به هزینه زیادی دارد و از طرفی مدیریت آنها را مشکل می‌کند. با قرار دادن چاپگرها در شبکه می‌توان هم تعداد آنها را کاهش داد و هم مدیریتشان را متمرکز کرد. به همین دلیل نیاز است که مدیران شبکه به نصب، پیکربندی و مدیریت چاپگرها آشنا باشند.



شکل ۴۶- چاپگر در شبکه

اصطلاحات مهم چاپ

Logical printer: نرم‌افزاری برای انجام تنظیمات و

مدیریت چاپگر است. در واقع رابط بین سیستم‌عامل و چاپگر است و نماد آن در قسمت Devices and Printers کنترل پنل نمایش داده می‌شود.

Printer: دستگاهی است که متن یا تصویر را روی کاغذ یا رسانه‌های دیگر چاپ می‌کند و شامل دو نوع زیر است:

- **Local printer:** چاپگری که به دستگاه‌های فیزیکی یک سرویس‌دهنده چاپ وصل می‌شود.
- **Network interface printer:** چاپگری که به وسیله کارت شبکه خود مستقیماً به شبکه وصل می‌شود.
- **Print server:** رایانه‌ای که چاپگرهای شبکه را مدیریت می‌کند. چاپگرهای شبکه اسناد را از سرویس‌گیرنده دریافت و برای چاپ پردازش می‌کنند.
- **Print job:** اسنادی که برای چاپ در صف چاپ قرار می‌گیرند.



پیاده‌سازی سرویس‌دهنده چاپ (Print server)

ویندوز سرور دارای سرویسی به نام Print server است که با استفاده از ابزار Print And Document Services Tools امکان مدیریت چاپگر را در شبکه فراهم می‌کند. برای پیاده‌سازی سرویس‌دهنده چاپ باید سرویس Print server به همراه ابزار Print And Document Services Tools و سرویس‌های وابسته به آن مثل Internet Printing نصب شوند.

سرویس Print server را در سرور DC (server2) نصب کنید. این سرویس، زیر مجموعه Print And Document Services Role است.

برای انجام کارگاه‌ها و فعالیت‌های این بخش، به دو رایانه برای هر گروه نیاز دارید. یکی را به عنوان سرویس‌دهنده DC پیکربندی کنید و دیگری را به عنوان سرویس گیرنده با سیستم عامل ویندوز ۱۰ عضو DC سرویس‌دهنده DC را server2 و سرویس گیرنده را Site1-Com1 می‌نامیم. همچنین در صورت داشتن چاپگر از آنها استفاده کنید در غیر این صورت می‌توانید از چاپگرهای پیش فرض ویندوز که در کارگاه‌ها نام برده شده، به صورت مجازی استفاده کنید.

کارگاه ۱۵ نصب چاپگر به وسیله ابزار Print Management

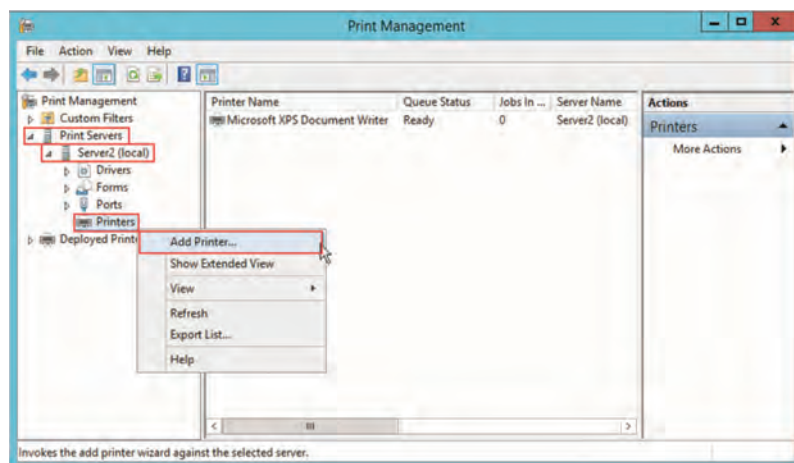
با نصب سرویس Print server ابزار Print Management به فهرست منوی Tools برنامه Server Manager اضافه می‌شود که به کمک آن می‌توانید سرویس‌دهنده‌های چاپ و چاپگرها را مدیریت کنید.

۱ با حساب کاربری Administrator وارد ویندوز سرویس‌دهنده چاپ (server2) شوید.

۲ پنجره Print Management را باز کنید.

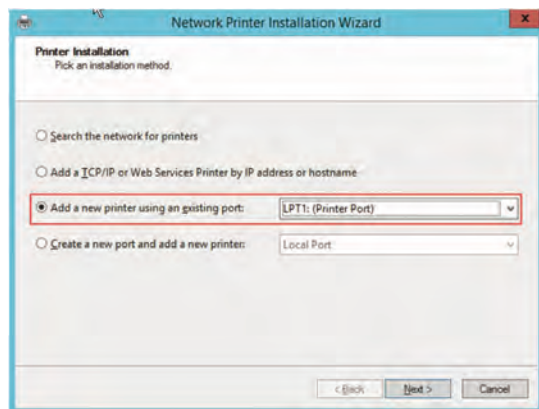
۳ یک چاپگر جدید برای نصب اضافه کنید.

روی گزینه Printers راست کلیک کرده، گزینه Add Printer را انتخاب کنید (شکل ۴۷).



شکل ۴۷- مسیر دسترسی به کادر محاوره‌ای Add Printer

در کادر محاوره‌ای Add Printer روی گزینه The printer that I want isn't listed کلیک کنید. سپس گزینه



شکل ۴۸- انتخاب درگاه چاپگر

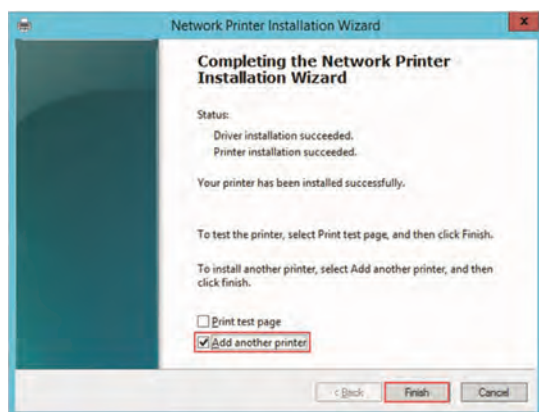
Add a new printer using an existing port را کلیک کرده، درگاه پیش فرض LPT1 را انتخاب کنید (شکل ۴۸).

۴ درایور چاپگر را نصب کنید.

در کادر محاوره‌ای نصب درایور، دکمه Install a new driver را انتخاب کرده، دکمه Next را کلیک کنید. مدل چاپگر خود را انتخاب کنید. برای مثال چاپگر HP LaserJet 1022 Class Driver را انتخاب کنید.

۵ چاپگر را به اشتراک بگذارید.

در کادر محاوره‌ای اشتراک گذاری، گزینه Share this printer را انتخاب کرده، دکمه Next را کلیک کنید.



شکل ۴۹- انتخاب نصب چاپگر دیگر در پایان نصب

۶ چاپگر دیگری برای نصب اضافه کنید.

در کادر محاوره‌ای پایان نصب، گزینه Add another printer را برای نصب چاپگر دوم انتخاب کنید (شکل ۴۹).

۷ چاپگر دوم را نصب کنید.

مجدداً همان چاپگر نصب شده در مرحله ۴ مجدداً (HP LaserJet 1022 Class Driver) را روی درگاه LPT2 نصب کنید اما به اشتراک نگذارید (شکل ۵۰).



شکل ۵۰- فهرست چاپگرهای نصب شده در پنجره Print Management

با استفاده از ابزار Devices and Printers کنترل پنل، چاپگر دیگری با نام دلخواه روی درگاه COM1 نصب کنید.



۱ با حساب کاربری Administrator وارد ویندوز سرویس دهنده چاپ (server2) شوید.

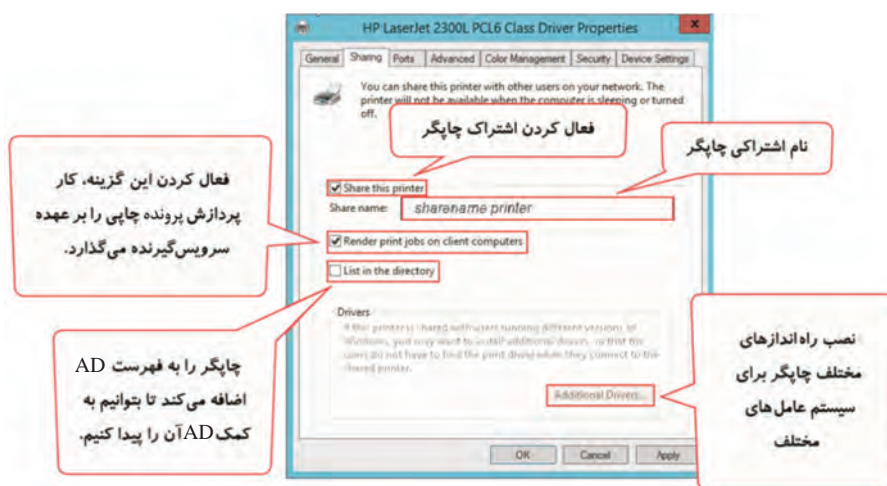
۲ چاپگر نصب شده را به اشتراک بگذارید.

بعد از نصب هم می توانید چاپگر را به اشتراک بگذارید. برای این منظور دو روش زیر وجود دارد:

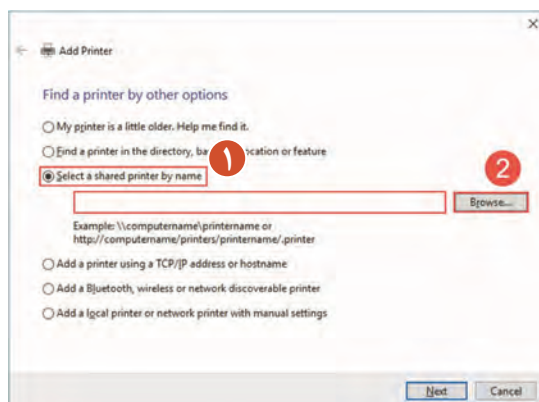
● استفاده از Control Panel: روی چاپگر راست کلیک کرده، گزینه Printer properties و سربرگ Sharing را انتخاب کنید.

● استفاده از ابزار Print Management: در ابزار Print Management روی چاپگر راست کلیک کرده، گزینه Manage Sharing را انتخاب کنید.

با یکی از دو روش به برگه Sharing چاپگر نصب شده در فعالیت کارگاهی وارد شوید (شکل ۵۱). گزینه Share this printer را فعال کنید و چاپگر را با نام پیش فرض به اشتراک بگذارید.



شکل ۵۱- برگه Sharing چاپگر

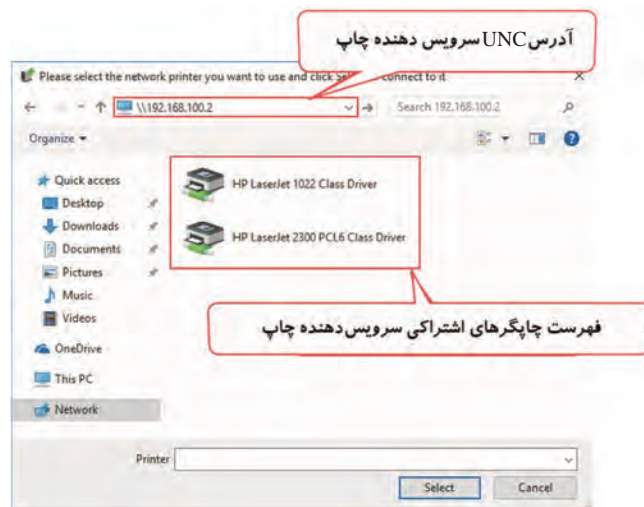


شکل ۵۲- انتخاب چاپگر به اشتراک گذاشته شده

۳ امکان استفاده از چاپگر به اشتراک گذاشته شده را برای حساب کاربری خود فراهم کنید.

با حساب کاربری تعریف شده برای خودتان در AD وارد رایانه Site1-Com1 شوید. گزینه Add a printer را از ابزار Devices and Printers انتخاب کنید. در کادر Select a shared printer by name دکمه Browse را کلیک کنید (شکل ۵۲).

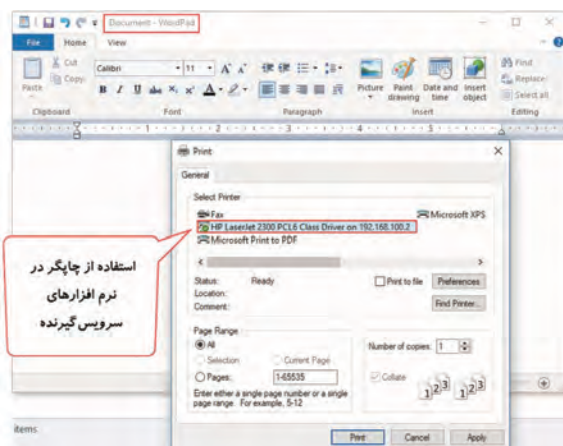
آدرس UNC سرویس دهنده چاپ را تایپ کنید تا فهرست چاپگرهای اشتراکی شبکه نمایش داده شود (شکل ۵۳). چاپگر به اشتراک گذاشته شده در مرحله ۲ را انتخاب کنید. دکمه Next را کلیک کنید تا نصب چاپگر تکمیل شود.



شکل ۵۳- فهرست چاپگرهای اشتراکی سرویس دهنده چاپ

۴ از نصب چاپگر روی سرویس گیرنده اطمینان حاصل کنید.

می توانید در نرم افزارهای مختلف از چاپگر اشتراکی سرویس دهنده چاپ برای چاپ اسناد خود استفاده کنید (شکل ۵۴).



شکل ۵۴- پنجره چاپ نرم افزار WordPad

پیکربندی مجوزهای چاپگر و سرور چاپ

به طور پیش فرض گروه everyone اجازه چاپ اسناد را دارند و می توانند سرویس دهنده های چاپ را مشاهده کنند. گروه Administrators می تواند اسناد همه کاربران را که در صف چاپ قرار دارند، مدیریت کند و چاپگر را پیکربندی کند؛ اما کاربران فقط می توانند اسناد خود را که در صف چاپ قرار دارند مدیریت کنند. در برگه Security چاپگر می توانید مجوزهای زیر را پیکربندی کنید (جدول ۱):

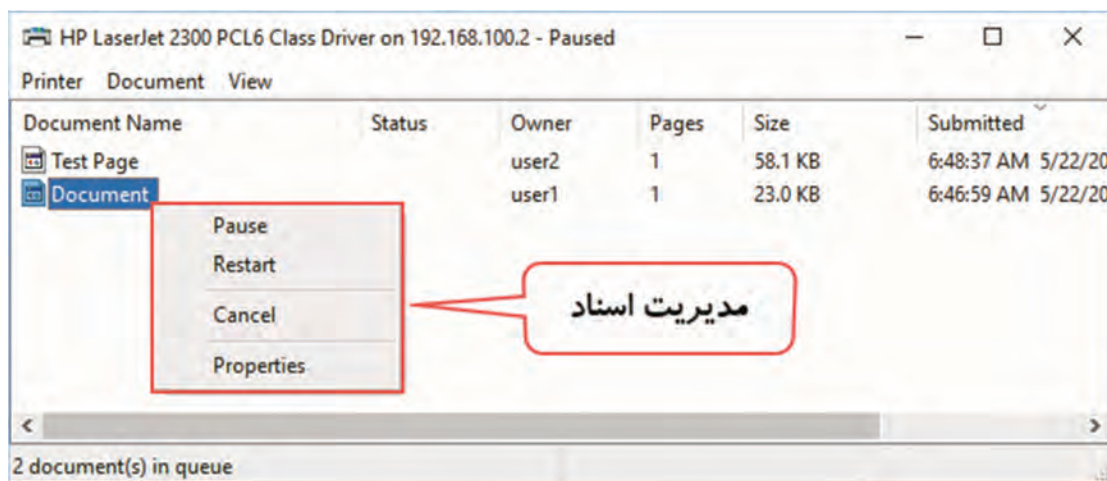
- **Print:** اجازه چاپ اسناد را به کاربر می دهد.
- **Manage this Printer:** اجازه پیکربندی تنظیمات چاپگر را به کاربر می دهد.
- **Manage Documents:** اجازه مدیریت همه اسناد ارسالی به چاپگر را به کاربر می دهد.

جدول ۱- قابلیت‌های مجوز چاپ

مجوزها			قابلیت ها
Manage Printer	Manage Documents	Print	
✓		✓	چاپ اسناد
✓	✓	✓	Pause, Resume, Restart, Cancel کردن اسناد خود کاربر
✓	✓	✓	اتصال به چاپگر
✓	✓		Pause, Resume, Restart, Cancel کردن همه اسناد کاربران
✓			اشتراک چاپگر
✓			تغییر خصوصیات چاپگر
✓			حذف چاپگر
✓			تغییر مجوزهای چاپ

مدیریت اسناد چاپی

با ارسال اسناد برای چاپ، چاپگر آنها را براساس ترتیب و اولویت در صف قرار می‌دهد. کاربر براساس مجوز تعریف شده می‌تواند روی آنها کارهایی مثل Pause, Resume, Restart و Cancel را انجام دهد (شکل ۵۵).



شکل ۵۵- پنجره صف چاپ

برای دسترسی به صف چاپ می‌توانید بعد از ارسال پرونده به چاپگر، روی نماد چاپگر در نوار وظیفه و یا نام چاپگر در Devices and Printers دابل کلیک کنید.

فعالیت
گروهی



در سرویس‌دهنده چاپ، چاپگری را نصب کرده، آن را به اشتراک بگذارید. برای دیدن صف چاپ روی آن راست کلیک کرده، گزینه Pause را انتخاب کنید. سپس کارهای زیر را انجام دهید:

- در AD گروه‌هایی با نام G-teacher و G-student تعریف کنید.

- کاربری با نام User1 ایجاد کنید و در گروه G-teacher عضو کنید.

- کاربر دیگری با نام User2 ایجاد کنید و در گروه G-student عضو کنید.

- در برگه Security چاپگر نصب کرده، به گروه G-teacher مجوز Manage Documents و به گروه G-student مجوز Print را اختصاص دهید.

- در رایانه Site1-Com1 با کاربر User1 وارد ویندوز شده، چاپگر را نصب کنید و در نرم‌افزار Word سندی ایجاد کرده، آن را برای چاپ به چاپگر مورد نظر ارسال کنید. برای کاربر User2 نیز این عمل را تکرار کنید.

- با کاربر User1 پنجره صف چاپ چاپگر را باز کنید. چه کارهایی را می‌توانید روی پرونده کاربر User1 و پرونده کاربر User2 در صف چاپ انجام دهید؟ نتیجه را در جدول زیر بنویسید.

نام پرونده	pause	Resume	Restart	Cancel
User1				
User2				

- با کاربر User2 پنجره صف چاپ چاپگر را باز کنید. چه کارهایی را می‌توانید روی پرونده کاربر User1 و پرونده کاربر User2 در صف چاپ انجام دهید؟ نتیجه را در جدول زیر بنویسید.

نام پرونده	pause	Resume	Restart	Cancel
User1				
User2				

- دو جدول را با هم مقایسه کنید و در مورد نتایج آن با هم کلاسی‌های خود بحث و گفت‌وگو کنید.

Printer pool

Printer pool شامل دو یا چند چاپگر مانند هم است که کاربران می‌توانند از آنها به عنوان یک چاپگر برای چاپ استفاده کنند. داشتن چندین چاپگر باعث کاهش زمان انتظار برای چاپ اسناد می‌شود.

چاپگرها در یک Printer pool از یک راه‌انداز استفاده می‌کنند.

یادداشت



کارگاه ۱۷ ایجاد Printer pool

در این کارگاه قصد داریم برای دو چاپگری که در کارگاه ۱۵ روی درگاه‌های LPT1 و LPT2 نصب کردید و یکی از آنها را به اشتراک گذاشتید، یک Printer pool ایجاد کنیم. برای ایجاد printer pool روی چند چاپگر فقط کافی است، یکی از آنها به اشتراک گذاشته شود و قابلیت Printer pooling را روی آن فعال کرد. اسناد ارسالی برای چاپ، به اولین چاپگر قابل دسترس در printer pool داده می‌شوند. در صورت اشتراک همه چاپگرهای printer pool کاربران می‌توانند مستقیماً از هر چاپگری برای چاپ استفاده کنند.

۱ با حساب کاربری Administrator وارد ویندوز سرویس‌دهنده چاپ (server2) شوید.

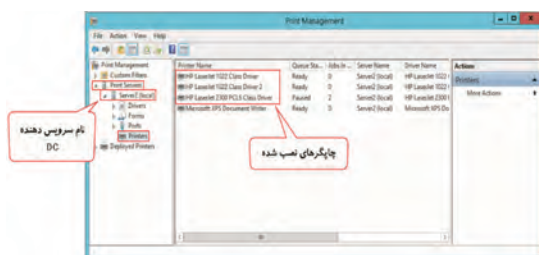
۲ ابزار Print Management را باز کنید.

۳ رایانه سرویس‌دهنده چاپ را انتخاب کنید.

روی نام رایانه سرویس‌دهنده چاپ در بخش Print Servers کلیک کنید.

۴ فهرست چاپگرهای نصب شده در سرویس‌دهنده چاپ را باز کنید.

روی گزینه Printers دابل کلیک کنید (شکل ۵۶).

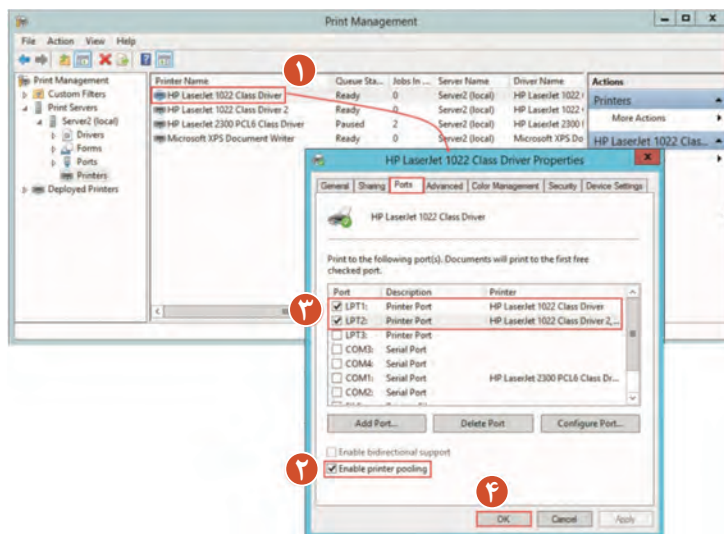


شکل ۵۶- فهرست چاپگرهای نصب شده در سرویس‌دهنده چاپ

۵ printer pooling را برای چاپگرهای درگاه LPT1 و LPT2 فعال کنید.

روی چاپگر HP LaserJet 1022 Class Driver راست کلیک کرده، گزینه Properties را انتخاب کنید. در برگه Ports گزینه Enable printer pooling را انتخاب کرده، سپس از فهرست، درگاه LPT1 و LPT2 را انتخاب کنید (شکل ۵۷).

بدین ترتیب اسناد چاپی ارسالی به سرویس‌دهنده چاپ، به هریک از این دو چاپگر که در دسترس باشند، فرستاده می‌شوند.



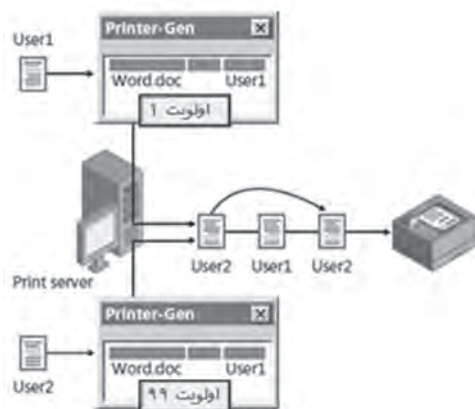
شکل ۵۷- فعال کردن printer pooling روی چاپگرهای درگاه LPT1 و LPT2



چاپگرهای جدیدی نصب کرده، printer pool ایجاد کنید، سپس اسنادی را برای چاپ به آنها بفرستید.

کارگاه ۱۸ پیکربندی Printer Priorities

وقتی چندین سند در صف چاپ قرار می گیرند، شما می توانید با اولویت بندی آنها اسناد مهم تر را زودتر چاپ کنید. برای مثال اسناد گروه G-student زودتر از گروه G-teacher چاپ شوند (شکل ۵۸).



شکل ۵۸- اولویت بندی اسناد صف چاپ

۱ با حساب کاربری Administrator وارد ویندوز سرویس دهنده چاپ (server2) شوید.

۲ چاپگری برای تعریف چندین اولویت روی آن نصب کنید.

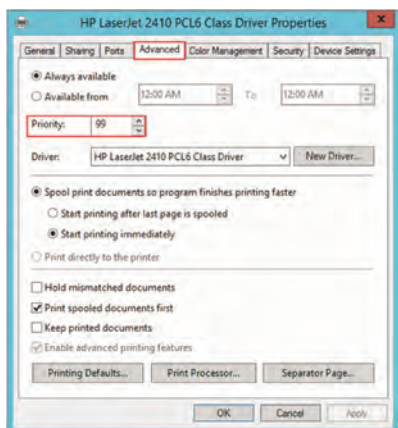
۳ همان چاپگر را مجدداً روی همان درگاه نصب کنید و هر دو چاپگر را به اشتراک بگذارید.

برای هر اولیوی که می خواهید تعریف کنید باید یک Logical printer نصب کنید، حتی اگر فقط یک دستگاه چاپگر داشته باشید. برای مثال اگر سه سطح دسترسی برای کاربران خود روی یک چاپگر نیاز دارید، باید آن چاپگر را سه بار با درگاه مشابه نصب کنید.

۴ اولویت و مجوزهای چاپ را تعیین کنید.

در Print Management روی چاپگر اول راست کلیک کرده، گزینه Properties را انتخاب کنید. در برگه Advanced اولویت ۹۹ را انتخاب کنید (شکل ۵۹). به گروه G-student مجوز چاپ را اختصاص دهید.

عدد ۹۹ بالاترین و عدد ۱ کمترین اولویت را دارد.



شکل ۵۹- تعیین اولویت چاپگر

۵ مرحله ۳ و ۴ را برای چاپگر دوم با اولویت ۱ برای گروه G-teacher تکرار کنید.

۶ هر چاپگر را برای یک کاربر نصب کنید.

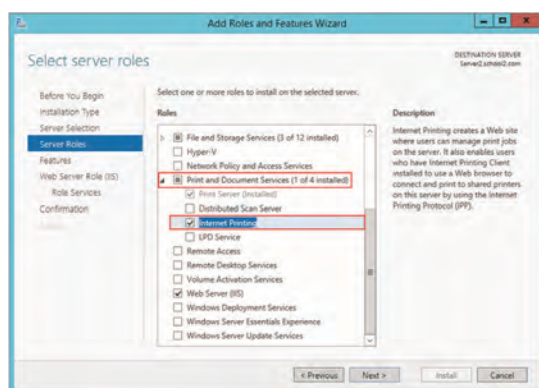
با user1 وارد ویندوز سرویس گیرنده شوید و چاپگر اول را نصب کنید. چاپگر دوم را برای user2 نصب کنید.

۷ ترتیب چاپ اسناد کاربران را بررسی کنید.

۸ با کاربران User1 و User2 چندین سند را برای چاپ ارسال کنید و ترتیب چاپ آنها را مشاهده کنید.

کارگاه ۱۹ مدیریت Internet Printing

سرویس Internet Printing امکان مدیریت چاپگرها را از طریق اینترنت به وسیله مرورگر فراهم می کند. برای دسترسی به سرویس دهنده چاپ از نشانی URL به صورت <http://<ServerName>/printers> استفاده می کنیم.



۱ با حساب کاربری Administrator وارد

ویندوز سرویس دهنده چاپ (server2) شوید.

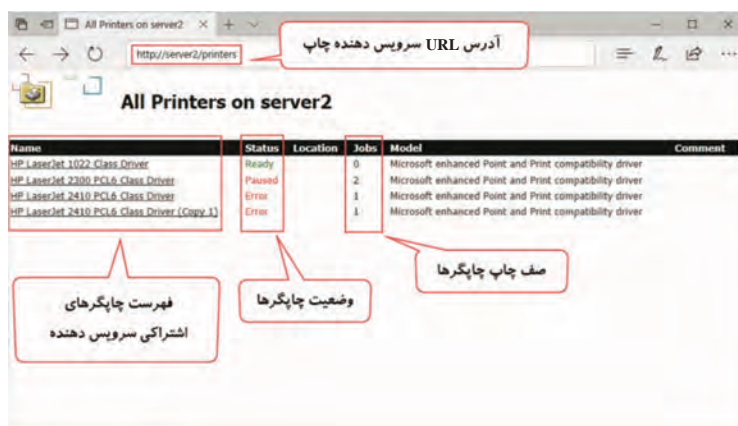
۲ سرویس Internet Printing را نصب کنید.

این سرویس را از زیر مجموعه Print And Document Services role انتخاب کرده، دکمه Next را کلیک کنید. پنجره نصب ویژگی های آن باز می شود. دکمه Add Features را کلیک کنید و سپس بقیه مراحل نصب را انجام دهید (شکل ۶۰).

شکل ۶۰- انتخاب سرویس Internet Printing برای نصب

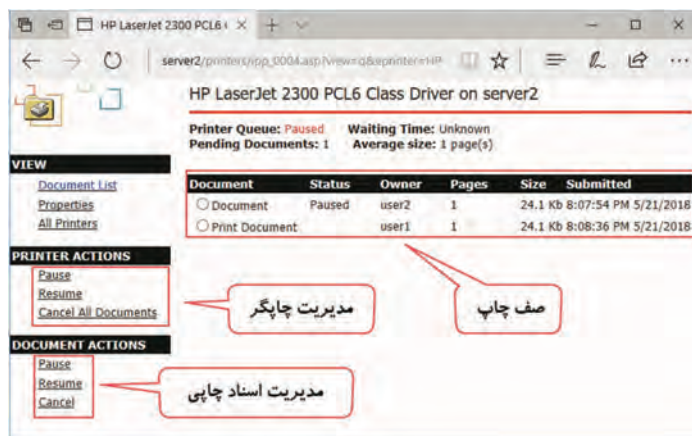
۳ اطلاعات چاپگرهای سرویس دهنده چاپ را مشاهده کنید.

در رایانه سرویس گیرنده در مرورگر، آدرس URL مربوط به سرویس دهنده چاپ (<http://server2/printers>) را تایپ کنید (شکل ۶۱).



شکل ۶۱- دسترسی به سرویس دهنده چاپ با استفاده از آدرس URL

فهرست چاپگرهای نصب شده و اشتراکی سرویس دهنده چاپ به همراه وضعیت جاری آنها نمایش داده می شود. با کلیک روی هر کدام می توانید اطلاعات بیشتری در مورد آن چاپگر مانند تعداد اسناد چاپ را مشاهده کنید (شکل ۶۲).



شکل ۶۲- پنجره مدیریت چاپگرهای سرویس دهنده چاپ

ارزشیابی مرحله ۶



نمره	استاندارد (شاخص ها/ داوری/ نمره دهی)	نتایج ممکن	شرایط عملکرد (ابزار، مواد، تجهیزات، زمان، مکان و...)	مراحل کار
۳	به اشتراک گذاشتن چاپگر و اعطای مجوز دسترسی - نصب چاپگر به اشتراک گذاشته شده روی سرویس گیرنده و استفاده از آن - مدیریت صف کارهای چاپی - ایجاد Printer Pool - مدیریت چاپگر از طریق اینترنت	بالاتر از حد انتظار	مکان: کارگاه استاندارد رایانه تجهیزات: شبکه ای از رایانه ها که حداقل یکی از آنها دارای سیستم عامل سرور باشد و حداقل یک چاپگر به یکی از رایانه ها متصل باشد. زمان: ۲۰ دقیقه	پایاده سازی Print Server
۲	به اشتراک گذاشتن چاپگر و اعطای مجوز دسترسی - نصب چاپگر به اشتراک گذاشته شده روی سرویس گیرنده و استفاده از آن	در حد انتظار		
۱	به اشتراک گذاشتن چاپگر	پایین تر از حد انتظار		

معیار شایستگی انجام کار:

کسب حداقل نمره ۲ از مراحل پایاده سازی Domain Controllers، مدیریت کاربران و اتصال به DC
کسب حداقل نمره ۲ از بخش شایستگی های غیر فنی، ایمنی، بهداشت، توجهات زیست محیطی و نگرش
کسب حداقل میانگین ۲ از مراحل کار

شرح کار:

- ۱- پیاده سازی Domain Controllers
- ۲- مدیریت کاربران
- ۳- اتصال به DC
- ۴- تنظیم سیاست های امنیتی کاربران
- ۵- پیاده سازی File Server
- ۶- پیاده سازی Print Server

استاندارد عملکرد:

اشتراک منابع شبکه و مدیریت متمرکز آنها با استفاده از سیستم عامل سرور
شاخص ها:

شماره مرحله کار	شاخص های مرحله کار
۱	پیاده سازی Domain Controllers
۲	ایجاد OU، حساب کاربری و حساب گروهی و مدیریت کاربران
۳	عضویت clientها در DC و Log On کردن با آنها
۴	تنظیمات Account Policies - ایجاد GPO و اعمال آن به OU
۵	نصب و راه اندازی File Service - اشتراک گذاری منابع بر حسب نیاز
۶	نصب و راه اندازی Print Server - مدیریت صف چاپ

شرایط انجام کار و ابزار و تجهیزات:

مکان: کارگاه رایانه مطابق استاندارد تجهیزات هنرستان ها

تجهیزات: شبکه ای از رایانه ها که حداقل یکی از آنها دارای سیستم عامل سرور باشد و حداقل یک چاپگر به یکی از رایانه ها متصل باشد.

زمان: ۱۷۰ دقیقه (پیاده سازی Domain Controllers ۳۵ دقیقه، مدیریت کاربران ۳۵ دقیقه - اتصال به DC ۳۵ دقیقه - تنظیم سیاست های امنیتی کاربران ۲۵ دقیقه - پیاده سازی File Server ۲۰ دقیقه - پیاده سازی Print Server ۲۰ دقیقه)

معیار شایستگی:

ردیف	مرحله کار	حداقل نمره قبولی از ۳	نمره هنرجو
۱	پیاده سازی Domain Controllers	۲	
۲	مدیریت کاربران	۲	
۳	اتصال به DC	۲	
۴	تنظیم سیاست های امنیتی کاربران	۱	
۵	پیاده سازی File Server	۱	
۶	پیاده سازی print Server	۱	
	شایستگی های غیر فنی، ایمنی، بهداشت، توجهات زیست محیطی و نگرش: مسئولیت پذیری، توجه به جزئیات کار - زبان فنی - توجه به سطح دسترسی مورد نیاز کاربران و گروه ها - کاهش مصرف کاغذ با اشتراک گذاری منابع - دقت در اختصاص مجوزها	۲	
میانگین نمرات			
			*

* حداقل میانگین نمرات هنرجو برای قبولی و کسب شایستگی، ۲ است.