راهنمای جامع

MCSE 70-742

مدیریت هویت در ویندوز سرور ۲۰۱۶

Identity in Windows Server 2016

Andrew Warren

Microsoft Press

ترجمه: مهندس مهران تاجبخش

انتشارات پندارپارس

سرشناسه : وارن، اندرو
Warren, Andrew
عنوان و نام پدیدآور : راهنمای جامع MCSE 70-742: مدیریت هویت در ویندوز سرور ۲۰۱۶/ [اندرو وارن]؛ ترجمه مهران تاجبخش.
مشخصات نشر : تهران : پندار پارس،۱۳۹۶.
مشخصات ظاهری : ۳۸۲ ص.: مصور،جدول.
شابک : 978-600-8201-45-8: ۲۷۰۰۰۰ ریال
وضعیت فهرست نویسی : فیپا
یادداشت : عنوان اصلی: ...Identity in Windows Server 2016
موضوع : ویندوز مایکروسافت، سرور
موضوع : Microsoft windows sever
موضوع : نرم‌افزار مایکروسافت
موضوع : Microsoft software
موضوع : سیستم‌های عامل (کامپیوتر)
موضوع : (Operating systems (Computers
موضوع : داده‌پردازی -- کارمندان -- گواهی و گواهی‌نامه‌ها
موضوع : Electronic data processing personnel -- Certification
موضوع : شبکه‌های کامپیوتری
موضوع : Computer networks
شناسه افزوده : تاجبخش، مهران، ۱۳۴۷ -، مترجم
رده بندی کنگره : QA۷۶/۷۷۴ ۱۳۹۶ ۲و۹و/
رده بندی دیویی : ۰۰۵/۴۳۲
شماره کتابشناسی ملی : ۴۸۴۷۰۵۷

انتشارات پندارپارس

دفتر فروش: انقلاب، ابتدای کارگرجنوبی، کوی رشتچی، شماره ۱۴، واحد ۱۶

تلفن: ۶۶۵۷۲۳۳۵ – تلفکس: ۶۶۹۲۶۵۷۸ همراه: ۰۹۲۱۴۳۷۱۹۶۴

www.pendarepars.com **info@pendarepars.com**

نام کتاب : **راهنمای جامع MCSE 70-742، مدیریت هویت در ویندوز سرور ۲۰۱۶**

ناشر : **انتشارات پندار پارس**

تألیف : **اندرو وارن**

برگردان : **مهران تاجبخش**

چاپ نخست : **شهریور ۹۶**

شمارگان : **۵۰۰ نسخه**

طرح جلد : **رامین شکرالهی**

چاپ، صحافی : **روز**

قیمت : **۲۷۰۰۰ تومان** **شابک : ۸-۴۵-۸۲۰۱-۶۰۰-۹۷۸**

تقدیم به رامتین، پسر عزیزم.

ارزشمندترین سرمایه زندگی من.

تلاش و پشتکار تو، به طور حتم آینده‌ای درخشان را برایت نوید می دهد.

تقدیم به دانشجویان عزیزم،

امیدوارم همواره در مراحل تحصیل و زندگی پایدار و سرافراز باشید.

سخنی با خواننده

این کتاب ترجمه کتاب ارائه شده توسط مایکروسافت در حوزه مدیریت هویت در ویندوز سرور ۲۰۱۶ با عنوان "Identity in Windows Server 2016"و برای کسب مدرک بین المللی مایکروسافت در این حوزه (70-742) است. بی‌تردید مطالب این کتاب می‌تواند مرجع و راهنمای مناسبی برای راهبران و متخصصان فناوری اطلاعات، مراکز داده و فضاهای ابری که بخواهند از سیستم عامل ویندوز سرور ۲۰۱۶ در پیکربندی سیستم‌های خود استفاده کنند و همچنین کسانی که بخواهند مسیر حرکت برای دریافت مدرک بین المللی MCSE ویرایش سال ۲۰۱۶ را طی کنند، باشد.

در حین مطالعه کتاب شما هم تأیید خواهید کرد که مطالب به صورت کامل و جامع به همراه تمامی جزئیات موجود ارائه شده است. در تألیف کتاب، نویسنده با درج تصاویر در هر مرحله برای شرح فناوری‌های مختلف به خواننده کمک کرده تا بتواند موضوعات مورد بحث را با استفاده از تصاویر ارائه شده به صورت کامل و دقیق دنبال کند.

برای ارائه هر چه بهتر و دقیق‌تر موضوعات مطرح شده در این کتاب، در طول هر بخش افزون بر تمرین‌های موردی، از یک سناریوی واقعی برای مطرح کردن موارد و مشکلات موجود در فضای کار استفاده شده است که مراحل اجرای آن به صورت مجموعه‌ای آزمایشگاهی با ذکر همه جزئیات و مراحل، آورده شده است.

این کتاب با توجه به موضوعات و نحوه ارائه محتوا، می‌تواند برای کسانی که به صورت عملیاتی با شبکه‌ها، مراکز داده و فضای ابری ویندوز سرور ۲۰۱۶ در ارتباط هستند و همچنین کسانی که متقاضی دریافت مدارک بین‌المللی مایکروسافت می‌باشند، به عنوان بهترین مرجع مد نظر قرار گیرد.

گفتنی است که متقاضیان دریافت مدرک بین المللی MCSE ابتدا باید با گذراندن سه دوره آموزشی به شرح زیر، مدرک مهندسی پایه مایکروسافت (MCSA) را دریافت کنند.

- 70-740: Installation, Upgrade and Computer with Windows Server 2016
- 70-741: Networking with Windows Server 2016
- 70-742: Identity Management with Windows Server 2016

پس از آن با توجه به گرایش مورد علاقه و یا نیاز فرد متقاضی، می‌تواند یکی از مدارک مهندسی مایکروسافت (MCSE) را که در زیر فهرست آنها آورده شده است دریافت کند:

- MCSE: Business Application
- **MCSE: Cloud Platform and Infrastructure**
- MCSE: Data Management and Analytics
- MCSE: Mobility
- MCSE: Productivity

در صورتی‌که فرد بخواهد مدرک مهندسی مایکروسافت را در حوزه نصب، راه اندازی، پیکربندی و مدیریت مراکز داده و فضای ابری کسب کند، باید دوره مشخص شده فوق را بگذراند. دوطلبانی که دارای مدرک MCSA باشند، با گذراندن حداقل یک دوره از مجموعه دوره‌های ارائه شده در بخش تخصصی سیستم عامل ویندوز سرور، می‌توانند مدرک مهندسی مایکروسافت (MCSE) را کسب کنند.

منتظر نظرها و پیشنهادهای سازنده همه سروران عزیز می‌باشم تا در انتشار کتاب‌های بعدی از همین سری مد نظر قرار دهم. پیشاپیش از عنایت و توجه‌تان کمال تشکر و سپاس را دارم.

در باره مترجم

با بیش از ۲۶ سال سابقه تدریس در حوزه فناوری اطلاعات و شبکه، در حدود ۱۰ سال است که به طور تخصصی در حوزه آموزش، مشاوره و اجرای پروژه‌های مربوط به امنیت شبکه و فضای مجازی و تست نفوذ و ادله الکترونیک و ارائه خدمات آموزش و مشاوره در حوزه پیاده‌سازی سیستم مدیریت امنیت اطلاعات (ISO27001) فعالیت دارم که حاصل آن مدارک بین المللی متعدد در حوزه شبکه، امنیت شبکه و تست نفوذ به شرح زیر می‌باشد:

Network+, CCNA, CCNP, CCNA Security, CCNP Security, Security+, CIW Security Professional, ISO27001 Lead Auditor.

MCSE– Cloud Platform and Infrastructure (in written)

MCE – Microsoft Certified Educator (in written)

در صورت نیاز به برقراری ارتباط با من می‌توانید از طریق رایانامه زیر اقدام نمایید:

info@mehrantajbakhsh.com

فهرست

فصل نخست

نصب و پیکربندی سرویس دامنه اکتیودایرکتوری (AD DS)

یکی از راه‌حل‌های جامع برای مدیریت هویت و دسترسی در سیستم‌عامل ویندوز سرور ۲۰۱۶، سرویس دامنه اکتیودایرکتوری (AD DS)[1] می‌باشد. بنابراین برای رفع نیازهای سازمان در ارتباط با مدیریت هویت، پیاده‌سازی و پیکربندی این سرویس از اهمیت زیادی برخودار می‌باشد.

در این فصل، با چگونگی نصب و پیکربندی کنترل کننده‌های دامنه آشنا خواهیم شد و افزون بر آن با چگونگی تعریف کاربران، گروه‌های کاری و رایانه‌ها و واحدهای سازمانی در آن‌ها آشنا می‌شویم. فراگیری موارد ذکر شده در پیاده‌سازی سرویس دامنه اکتودایرکتوری نقش اساسی دارند.

مهارت‌های این فصل:

- نصب و پیکربندی کنترل کننده‌های دامنه
- ایجاد و مدیریت کاربران و رایانه‌ها در اکتیودایرکتوری
- ایجاد و مدیریت گروه‌ها و واحدهای سازمانی (OU)[2] در اکتیودایرکتوری

---

[1] Active Directory Domain Services
[2] Organizational Unit

مهارت ۱/۱: نصب و پیکربندی کنترل کننده‌های دامنه

کنترل کننده‌های دامنه، نقش میزبان سرور AD DS را در ویندوز سرور ۲۰۱۶ برای مدیریت هویت و خدمات مرتبط با آن در شبکه سازمان و تجهیزات موجود در آن ایفا می‌کنند. پیش از اینکه با موارد کاربرد و استفاده از این سرویس آشنا شویم، باید با اصول و مبانی موجود در این سرویس آشنا شویم، که از جمله آنها می‌توانیم به فارست‌ها(جنگل‌ها) و درخت‌ها و دامنه‌ها و سایت‌ها و واحدهای سازمانی اشاره کنیم.

در این بخش مطالب زیر ارائه می‌شوند

- مبانی AD DS
- نصب یک فارست جدید
- افزودن و حفظ کنترل‌کننده دامنه
- نصب سرور AD DS بر روی Server Core
- نصب کنترل‌کننده دامنه با استفاده از قابلیت Install from Media
- نصب و پیکربندی کنترل‌کننده دامنه فقط خواندنی
- پیکربندی global catalog server
- پیکربندی کپی‌برداری از کنترل‌کننده دامنه (cloning)
- ارتقای کنترل‌کننده دامنه
- انتقال و توقف عملیات سرویس‌های اصلی
- رفع موارد و مشکلات مربوط به ثبت رکورد DNS SRV

مبانی سرویس دامنه اکتیودایرکتوری (AD DS)

AD DS شامل اجزای فیزیکی و منطقی می‌باشد. اجزای فیزیکی آن، مواردی ملموس نظیر کنترل‌کننده دامنه می‌باشد و موارد منطقی در آن شامل فارست می‌باشد.

سرویس‌دهنده AD DS دارای اجزای منطقی زیر می‌باشد:

- **فارست (Forest)** به مجموعه‌ای از کنترل کننده‌های دامنه AD DS گفته می‌شود که دارای الگوی مشترک (Schma) بوده و با استفاده از یک مسیر دوطرفه قابل اعتماد به یکدیگر مرتبط شده باشند. در بسیاری از سازمان‌ها، کنترل کننده‌های دامنه را در یک فارست پیاده‌سازی می‌کنند، دلایل موجود برای پیاده‌سازی چندین فارست در سازمان، به شرح زیر می‌باشند:
  - نیاز به راهبری جداگانه و تفکیک شده در بخش‌های مختلف سازمان
  - استفاده از انواع مختلف و الگوهای متفاوت کنترل کننده‌های دامنه موجود در بخش‌های مختلف سازمان

- **دامنه (Domain)** دامنه به یک واحد منطقی راهبری متشکل از کاربران، گروه‌ها، رایانه‌ها و سایر اجزای دیگر در شبکه سازمان گفته می‌شود. بر اساس نیاز سازمان، چندین دامنه می‌توانند بخش‌های تشکیل دهنده یک یا چند فارست در سازمان باشند. ساختار دامنه‌ها بر اساس ارتباط پدر و فرزندی و ارتباط‌های قابل اعتماد شکل می‌گیرند.

نکته آزمون

از دامنه‌ها برای تفکیک عملیات راهبری استفاده نمی‌شود، زیرا همه دامنه‌های موجود در یک فارست، توسط راهبر آن مدیریت و راهبری می‌شوند که این افراد معمولا در یک گروه راهبران امنیتی فراگیر در سازمان تعریف می‌شوند. برای تفکیک کامل عملیات راهبری، باید فارست‌های AD DS جداگانه تعریف شوند.

- **درخت (Tree)** درخت به مجموعه‌ای از دامنه‌های AD DS گفته می‌شود که در یک دامنه ریشه با یکدیگر مشترک می‌باشند و همگی از یک ساختار نام‌گذاری (محدوده اسامی Namespaces) استفاده می‌کنند. به عنوان مثال، sales.adatum.com و marketing.adatum.com هر دو در دامنه ریشه adatum.com مشترک می‌باشند و هر دو از نام‌گذاری مشترک adatum.com نیز استفاده می‌کنند. با استفاده از یک درخت می‌توان یک فارست AD DS ایجاد کرد و یا می‌توان در ایجاد آن از چندین درخت استفاده کرد. یکی از دلایل استفاده از چندین درخت برای ایجاد فارست AD DS سازمان، نیاز به استفاده از چندین محدوده نام‌گذاری می‌باشد، که بر اساس ادغام و خریداری سازمان‌های دیگر به وجود می‌آید.
- **الگو (Schema)** الگوی AD DS، به مجموعه مشخصات و ویژگی‌های اجزایی که در فارست AD DS ایجاد شده و نگهداری و مدیریت می‌شوند، گفته می‌شود. به عنوان مثال، کاربر یک نوع منطقی از اجزای موجود در فارست می‌باشد که دارای مشخصات و ویژگی‌های مخصوص به‌خود می‌باشد، که از جمله آنها می‌توان به نام کامل، دپارتمان و رمزعبور اشاره کرد. ارتباط بین اجزا و مشخصات مربوط به آن، توسط الگو (Schema) تعریف می‌شود و در همه کنترل‌کننده‌های دامنه موجود در فارست، یک نسخه از این الگو نگهداری می‌شود.
- **واحد سازمانی (Organitaional Unit – OU)** واحد سازمانی در داخل دامنه، محفظه‌ای شامل کاربران، گروه‌ها و رایانه‌ها و سایر واحدهای سازمانی می‌باشد. از واحد سازمانی برای سهولت در امر راهبری استفاده می‌شود. با توجه به قراردادن کاربران، گروه‌ها و اجزای مورد نظر در یک واحد، امکان تخصیص مجوزهای دسترسی به آنها ساده‌تر انجام می‌شود. با استفاده از GPOها می‌توانیم، آیین‌نامه‌های مربوط به حدود دسترسی و مجوزهای استفاده از منابع مختلف موجود در دامنه را تعریف کنیم و آنها را به واحدهای سازمانی مورد نظر مرتبط کنیم. در زمان ایجاد کنترل‌کننده دامنه، به‌طور پیش‌فرض در آن یک واحد سازمانی با نام Domain Controllers ایجاد می‌شود.
- **محفظه (Container)** افزون بر واحدهای سازمانی، برای گروه‌بندی اجزای موجود در دامنه می‌توانیم از محفظه استفاده کنیم. در کنترل‌کننده دامنه محفظه‌های پیش‌فرض Computers و Builtin و Managed Service Accounts وجود دارند. امکان برقراری ارتباط بین محفظه‌ها و GPOها وجود ندارد.

- **سایت (Site)** یک سایت، نمایشی منطقی از موقعیت فیزیکی در سازمان می‌باشد. سایت می‌تواند بخش بزرگی از یک سازمان را در برگیرد (نظیر یک شهر) و یا تعدادی از زیر شبکه‌های موجود در یکی از بخش‌های موجود در سازمان را شامل شود. با استفاده از سایت‌ها امکان تفکیک و مدیریت ارائه خدمات در شبکه سازمان، به‌صورت راحت‌تر امکان‌پذیر می‌باشد. به‌طور مثال در زمان راه‌اندازی رایانه حاوی سیستم‌عامل ویندوز ۱۰، باید مکان کنترل‌کننده دامنه در شبکه سازمان مشخص شود، تا با استفاده از آن، ورود به شبکه و تأیید هویت کاربر انجام شود. با استفاده از سایت می‌توانیم عملیات کپی‌برداری از محتویات کنترل‌کننده‌های دامنه را زمان‌بندی و مدیریت کنیم.
- **زیرشبکه (Subnet)** زیرشبکه، نمایش منطقی از زیر شبکه‌های فیزیکی موجود در شبکه سازمان می‌باشد.

نکته آزمون

سایت پیش‌فرض Default-First-Site-Name در زمان نصب سرویس‌دهنده AD DS و فارست، ایجاد می‌شود. همه کنترل کننده‌های دامنه، تا زمانی‌که برای آنها سایت جدیدی ایجاد شوند، در این سایت قرار داده می‌شوند. در صورتی‌که قصد افزودن اجزای جدیدی به سایت مورد نظر را دارید، باید نام آن را تغییر دهید.

با استفاده از زیر شبکه‌ها، می‌توانیم مکان فیزیکی رایانه‌های موجود در فارست AD DS را بر اساس خدمات مورد استفاده در آنها، در شبکه سازمان، مشخص کنیم. به‌طور پیش‌فرض در ابتدا زیرشبکه ایجاد نمی‌شود، پس از ایجاد هر زیرشبکه باید آن را در یک سایت قرار دهیم. هر سایت می‌تواند شامل چندین زیرشبکه باشد.

- **بخش (Partition)** اطلاعات مربوط به سرویس‌دهنده AD DS به‌طور فیزیکی در یک بانک‌اطلاعاتی و در همه کنترل‌کننده‌های دامنه ذخیره می‌شود. با توجه به اینکه بخش‌هایی از کنترل‌کننده‌های دامنه به‌طور پی‌درپی تغییر می‌کنند و به‌روز رسانی می‌شوند، و برخی دیگر به ندرت تغییر می‌کنند، می‌توانیم آنها را در بخش‌های جداگانه نگهداری کنیم.

نکته **رونوشت AD DS**

زمانی‌که در AD DS تغییراتی را ایجاد می‌کنیم، سایر بخش‌های مرتبط با آن نیز باید به‌روز رسانده شوند. این عملیات با عنوان رونوشت AD DS نامیده می‌شوند. با تفکیک بانک‌اطلاعات به بخش‌های کوچک‌تر، محدوده رونوشت‌برداری کوچک‌تر خواهد شد.

بخش‌های مختلفی که در بانک‌اطلاعات ایجاد می‌شوند، عبارتند از:

- **الگو** این بخش در سطح فارست می‌باشد و به ندرت تغییر می‌کند. در این بخش الگوی مورد استفاده در فارست ذخیره می‌شود.
- **پیکربندی** این بخش در سطح فارست می‌باشد و تغییرات در آن به ندرت انجام می‌شود. در این داده‌های پیکربندی فارست نگهداری می‌شود.

- **دامنه** این بخش در سطح دامنه می‌باشد. اطلاعات موجود در این بخش، به تکرار تغییر می‌کنند و در همه کنترل‌کننده‌های دامنه نیز نگهداری می‌شود. در این بخش اطلاعات مربوط به اجزای موجود در دامنه که شامل کاربران و رایانه‌های موجود در فارست می‌باشند، نگهداری می‌شود.
- **ارتباط‌های مطمئن (Trus relationships)** ارتباط مطمئن که اغلب با عنوان trust نیز نامیده می‌شود،

نکته **بخش برنامه‌های کار با فهرست‌ها**
امکان ایجاد بخش‌های خاص برای برنامه‌های کاربردی کار با فهرست‌ها در داخل فارست وجود دارد. به عنوان مثال، می‌توانیم سرویس‌دهنده DNS را برای عملیات کپی‌برداری اکتیودایرکتوری مربوط به آن پیکربندی کنیم.

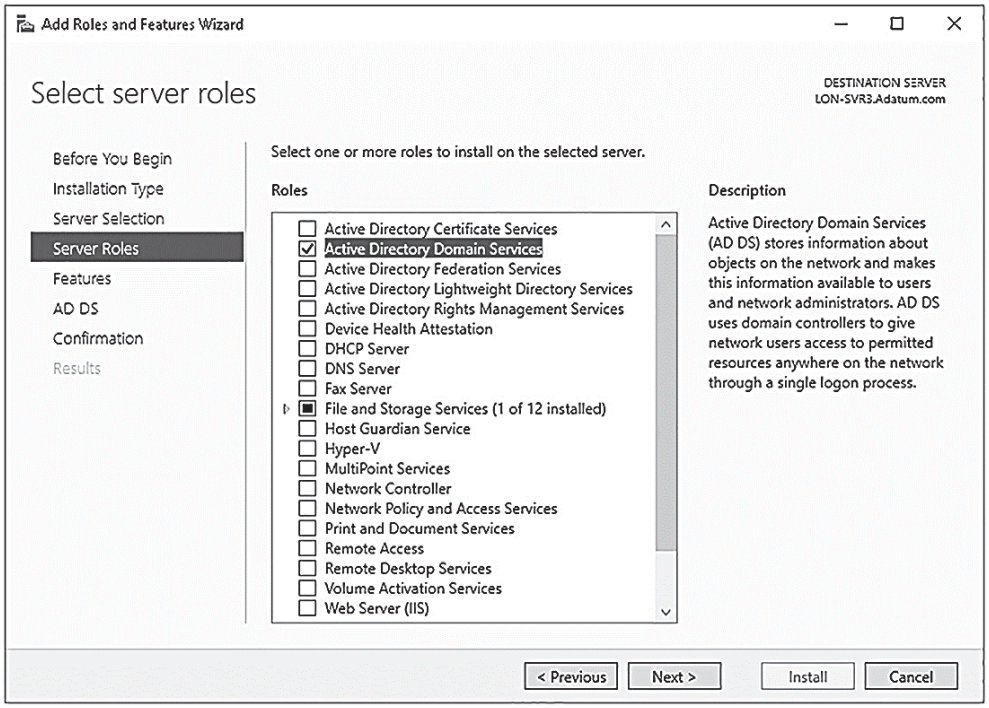
یک توافق امنیتی بین دو دامنه موجود در یک فارست و یا یک فارست و شبکه خارج از آن می‌باشد. با استفاده از این نوع ارتباط، امکان برقراری ارتباط کاربران یک طرف به منابع موجود در طرف دیگر فراهم می‌شود. در این نوع ارتباط یک طرف اعتمادکننده (trusting) و طرف دیگر اعتمادشونده (trusted) نامیده می‌شوند. طرفی که در آن منابع قرار دارد، اعتمادکننده و طرفی که در آن کاربران قرار دارند، اعتمادشونده نامیده می‌شوند.

نصب فارست جدید

برای نصب یک فارست AD DS جدید، ابتدا باید نخستین کنترل‌کننده دامنه را در فارست ایجاد کنیم. این بدان معنا است که در یکی از سرورهای ویندوز سرور ۲۰۱۶، سرویس‌دهنده AD DS را نصب کنیم و سپس سرور مورد نظر را به عنوان کنترل‌کننده دامنه پیکربندی کنیم و سپس در آن گزینه Add A New Forest را انتخاب کنیم.

برای ایجاد فارست جدید، ابتدا با استفاده از مراحل زیر سرویس‌دهنده AD DS را در سرور مورد نظر نصب می‌کنیم:

۱- با استفاده از حساب کاری راهبر محلی وارد ویندوز سرور ۲۰۱۶ می‌شویم.
۲- برنامه Server Manager را باز می‌کنیم. در پیشخوان بر روی عبارت Add Roles and Fetures کلیک می‌کنیم.
۳- در پنجره Add Roles and Features Wizard جلو می‌رویم و همانند شکل زیر، در صفحه Server Role، گزینه Active Directory Domain Services را انتخاب می‌کنیم و سپس بر روی کلید Add Features کلیک و بر روی کلید Next کلیک می‌کنیم.



۴- تا انتهای پنجره نصب می‌رویم و بر روی کلید Install کلیک می‌کنیم.

۵- پس از اتمام عملیات نصب، بر روی کلید Close کلیک می‌کنیم.

نکته آزمون

برای نصب سرویس‌دهنده مورد نظر می‌توانیم از دستورات خط فرمان پاورشل نیز استفاده کنیم. برای این‌کار کافی است که پنجره خط فرمان پاورشل را در سطح راهبر باز کنیم و سپس دستور زیر را در آن وارد کنیم:

```
Install-WindowsFeature AD-Domain-Services
```

پس از اینکه فایل‌های مربوط به سرویس‌دهنده AD DS را بر روی سرور مورد نظر نصب کردیم، نوبت به پیکربندی نخستین کنترل‌کننده دامنه در فارست مورد نظر می‌رسد. برای این‌کار از مراحل زیر استفاده می‌کنیم:

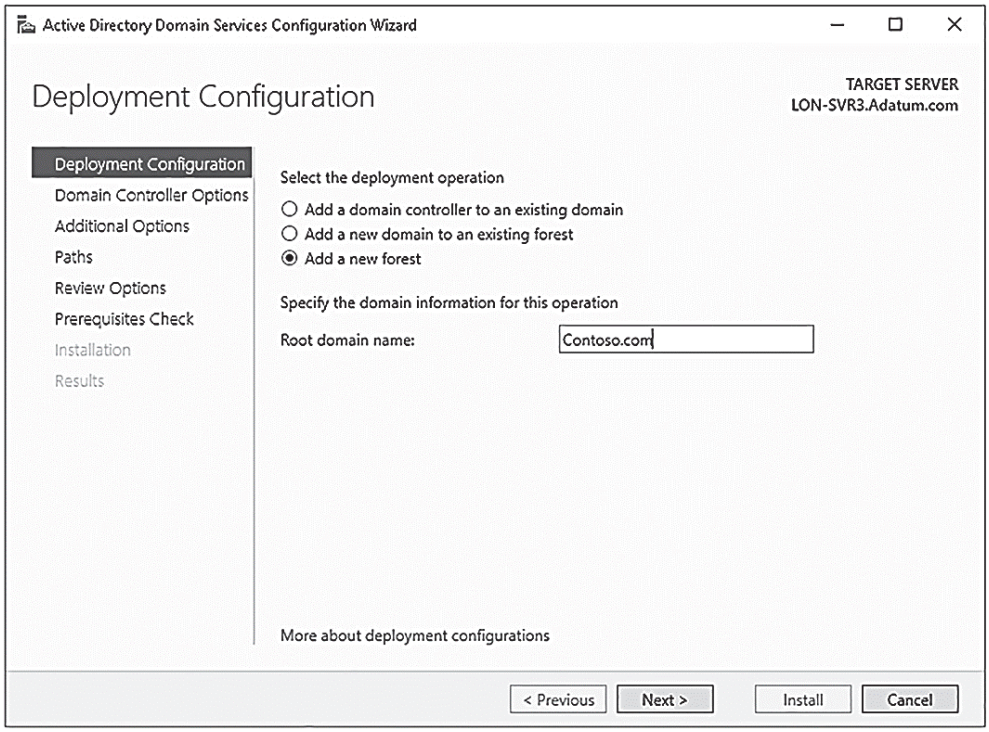
۱- در برنامه Server Manager، بر روی کلید Notifications کلیک می‌کنیم (مثلث زرد)، سپس بر روی عبارت Promote To A Domain Controller کلیک می‌کنیم.

نکته آزمون

برای تبدیل سرور مورد نظر به کنترل‌کننده دامنه می‌توانیم از دستورات خط فرمان پاورشل نیز استفاده کنیم. به عنوان مثال می‌توانیم با استفاده از دستور زیر، سرور مورد نظر را به کنترل‌کننده دامنه با نام Adatum.com تبدیل کنیم و همچنین در آن سرویس‌دهنده DNS را نیز فعال کنیم.

```
Install-ADDSDomainController -InstallDns -DomainName adatum.com
```

۲- در پنجره Active Directory Domain Services Configuration Wizard، در صفحه Deployment Configuration، در بخش Select The Deployment Operation، بر روی کلید Add A New Forest کلیک و سپس نام دامنه ریشه را وارد می‌کنیم (شکل زیر). سپس بر روی کلید Next کلیک می‌کنیم.



۳- در صفحه Domain Controller Options (شکل زیر)، گزینه‌های زیر را پیکربندی می‌کنیم و سپس بر روی کلید Next کلیک می‌کنیم.

- **Forest Functional Level** در این بخش قابلیت‌های مورد نظر در فارست را مشخص می‌کنیم. در این بخش حداقل سطح عملیات دامنه‌های موجود در فارست را مشخص می‌کنیم. به عنوان مثال، با انتخاب گزینه Windows Server 2012 مشخص می‌کنیم که دامنه‌های مورد نظر در فارست در سطح ویندوز سرور ۲۰۱۲ می‌باشند. گزینه‌های قابل انتخاب در این بخش عبارتند از :

- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016

- **Domain Functional Level** در این بخش قابلیت‌های مورد نظر در سطح دامنه را مشخص می‌کنیم. گزینه‌های این بخش عبارتند از:

- Windows Server 2008
- Windows Server 2008 R2

- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016

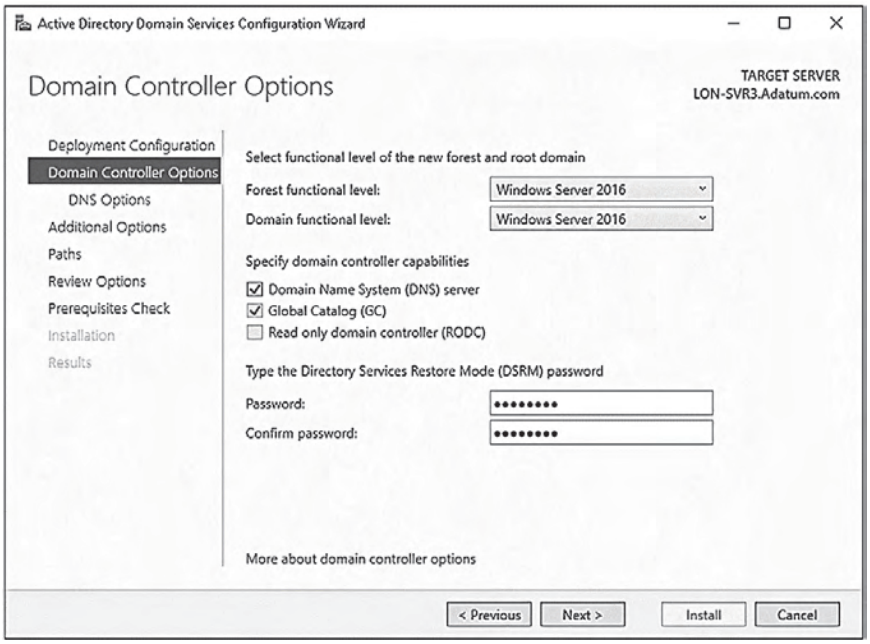
نیاز به مطالعه بیشتر دارید؟ **سطوح عملیاتی در ویندوز سرور ۲۰۱۶**
برای دسترسی به اطلاعات بیشتر در مورد سطوح عملیاتی فارست در سیستم‌عامل ویندوز سرور ۲۰۱۶، به تارنمای Microsoft Texchnet در آدرس زیر مراجعه کنید:
https://technet.microsoft.com/windows-server-docs/identity/ad-ds/windows-server-2016-functional-levels

- **Domain Name System (DNS) Server** سرویس DNS برای تفکیک اسامی مورد استفاده می‌گیرد و وجود آن در سرویس‌دهنده AD DS ضروری می‌باشد. این گزینه به‌طور پیش‌فرض انتخاب شده‌است، در صورتی‌که در ساختار شبکه، سرویس‌دهنده DNS دیگری را پیکربندی کرده‌ایم، می‌توانیم این گزینه را غیرفعال کنیم.
- **Global Catalog (GC)** از این سرور برای ارائه خدمات در سطح فارست استفاده می‌شود. این گزینه به‌طور پیش‌فرض انتخاب شده‌است و نمی‌توان آن را غیرفعال کرد، زیرا نخستین کنترل‌کننده دامنه باید نخستین و تنها سرور Global Catalog باشد. پس از اینکه کنترل کننده‌های دامنه دیگری را در فارست مورد نظر اضافه کنیم، می‌توانیم این گزینه را غیرفعال کنیم.
- **Read Only Domain Controller (RODC)** این گزینه تعیین می‌کند که اطلاعات کنترل‌کننده دامنه فقط خواندنی می‌باشند. این گزینه به‌طور پیش‌فرض انتخاب نشده‌است و برای نخستین و تنها کنترل‌کننده دامنه فعال نمی‌باشد.
- **Directory Services Restore Mode (DSRM) Password** این گزینه زمانی استفاده می‌شود که کنترل‌کننده دامنه را در وضعیت بازیابی (Restore) راه‌اندازی می‌کنیم.

۴- در صفحه Additional Options، نام دامنه NetBIOS را تعیین می‌کنیم. پروتکل NetBIOS امروزه زیاد مورد استفاده قرار نمی‌گیرد، در این پروتکل برای نام‌گذاری‌های دامنه از ساختار سلسله مراتبی استفاده نمی‌شود. به‌طور پیش‌فرض، نام این دامنه، نخستین بخش از نام فارست AD DS می‌باشد. به عنوان مثال، در صورتی‌که نام فارست مورد نظر Contoso.com باشد، نام دامنه NetBIOS، CONTOSO در نظر گرفته می‌شود. به‌طور معمول نیازی به تغییر این نام نمی‌باشد، سپس بر روی کلید Next کلیک می‌کنیم.

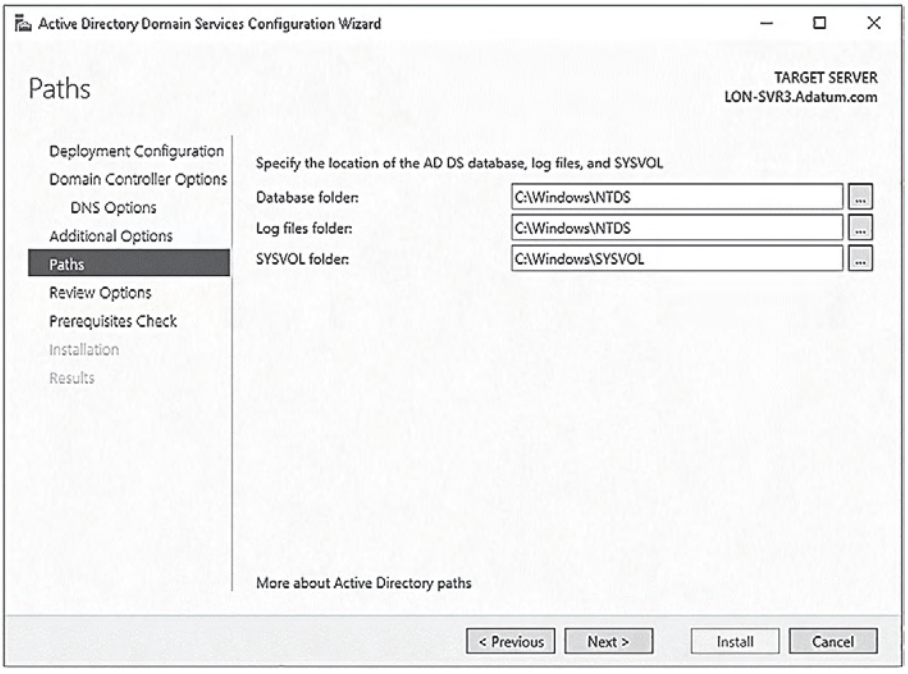
۵- همان‌گونه که در شکل زیر نشان داده شده‌است، مسیر قرارگیری بانک‌اطلاعات AD DS و فایل‌های لاگ و محتوای SYSVOL را تعیین می‌کنیم. سپس بر روی کلید Next کلیک می‌کنیم. به‌طور پیش‌فرض مسیرهای زیر در نظر گرفته شده‌اند:

- Database folder: C:\Windows\NTDS
- Log files folder: C:\Windows\NTDS
- SYSVOL folder: C:\Windows\SYSVOL



نکته آزمون

در تعیین مسیرها در صورتی‌که از مسیرهای مختلف بر روی دیسک‌های موجود در سرورهای مختلف استفاده کنیم، کارآیی و سرعت دسترسی به اطلاعات مورد نظر افزایش خواهند یافت.



۶- گزینه‌های پیکربندی را مرور و سپس بر روی کلید Next کلیک می‌کنیم تا کنترل‌های پیش از نصب انجام شوند.
۷- سپس بر روی کلید Install کلیک می‌کنیم، در حین انجام عملیات نصب، سرور مورد نظر راه‌اندازی می‌شود.
۸- با استفاده از حساب کاری راهبر (admin) دامنه، وارد سرویس‌دهنده مورد نظر می‌شویم.

نیاز به مطالعه بیشتر دارید؟ **نصب سرویس‌دهنده AD DS**
برای دسترسی به اطلاعات بیشتر در مورد پیاده‌سازی و نصب سرویس‌دهنده AD DS، به تارنمای Microsoft Texchnet در آدرس زیر مراجعه کنید:
https://technet.microsoft.com/en-us/windows-server-docs/identity/ad-ds/deploy/install-active-directory-domain-services--level-100-

افزودن و حذف کنترل‌کننده دامنه

پس از اینکه اولویت کنترل‌کننده دامنه را در فارست AD DS مورد نظر مشخص کردیم، برای اینکه قابلیت انعطاف‌پذیری و کارآیی آن را افزایش دهیم، می‌توانیم کنترل‌کننده دامنه بیشتری را در فارست مورد نظر ایجاد کنیم. عملیات افزودن کنترل‌کننده دامنه جدید، تا حد زیادی شبیه به عملیات مربوط به کنترل‌کننده دامنه اول می‌باشد، ابتدا سرویس‌دهنده AD DS را نصب می‌کنیم (با استفاده از Server Manager و یا خط فرمان پاورشل)، سپس سرور مورد نظر را به عنوان کنترل‌کننده دامنه در نظر می‌گیریم.

گزینه‌های مورد نیاز در زمان نصب بر اساس جزئیات می‌توانند تغییر کنند، به عنوان مثال، افزودن یک کنترل‌کننده دامنه در شرایطی که کنترل‌کننده دامنه پیشین در فارست وجود داشته باشد، با افزودن کنترل‌کننده دامنه جدید در دامنه جدید اندکی متفاوت می‌باشد.

در زمان نصب کنترل‌کننده دامنه جدید دو حالت مختلف می‌تواند در نظر گرفته شود:

- **افزودن کنترل‌کننده دامنه جدید در دامنه موجود** برای انجام عملیات نصب در این شرایط باید ابتدا با استفاده از حساب کاری راهبر عضو در گروه راهبری، وارد دامنه مورد نظر شویم.
- **افزودن کنترل‌کننده دامنه جدید در دامنه جدید** در این شرایط باید با استفاده از حساب کار عضو گروه راهبری، در فارست مورد نظر که دامنه جدید در آن ایجاد خواهد شد، وارد شویم. در این شرایط سطح دسترسی و مجوزهای لازم برای تعریف دامنه در ساختار درختی دامنه‌های موجود در فارست را خواهیم داشت.

یکی از دلایلی که کنترل کننده‌های جدید در فارست ایجاد می‌کنیم، افزودن نسخه‌های متعدد از اطلاعات آن در بخش‌های مختلف فارست می‌باشد. زیرا بیشترین ترافیک در فارست مربوط به تغییراتی است که در سطح دامنه انجام می‌شود. با تقسیم فارست به دامنه‌های کوچکتر، می‌توانیم سطح تغییرات را محدودتر و ترافیک مربوط به آن را در کنترل کننده‌های دامنه توزیع کنیم. به عنوان مثال، شرکت A. Datum دارای شبکه‌ای گسترده در اروپا و کانادا می‌باشد. در این شرایط دو دامنه جداگانه برای شبکه اروپا و کانادا ایجاد می‌کنیم، Europe.Adatum.com و Canada.Adatum.com. به این ترتیب تغییرات انجام شده در هر یک از دامنه‌ها، در دیگری تکرار نخواهد شد.

افزودن کنترل‌کننده دامنه جدید در دامنه موجود

برای این‌کار باید ابتدا با حساب کار راهبر دامنه مورد نظر وارد شویم و سپس عملیات را مطابق با مراحل زیر انجام دهیم:

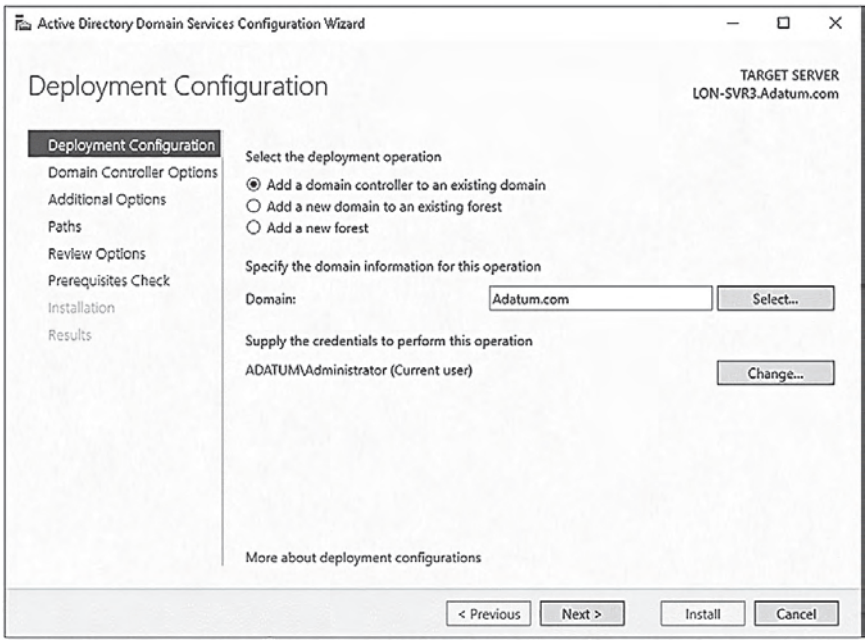
نکته آزمون

فرض بر این است که سرور مورد نظر، که سرویس کنترل‌کننده دامنه در آن نصب خواهد شد، عضوی از دامنه مورد نظر می‌باشد، وگرنه بهتر است که برای سهولت کار، ابتدا سرور مورد نظر را به دامنه مورد نظر وارد کنیم و سپس عملیات تبدیل آن به کنترل‌کننده دامنه را انجام دهیم. اگر نمی‌خواهیم کنترل‌کننده دامنه جدید در دامنه موجود قرار داشته باشد، باید در مراحل نصب، برای آن حساب کاری راهبر برای کنترل‌کننده دامنه مورد نظر تعریف کنیم. در انتهای نصب نیز باید سرویس‌دهنده DNS مربوط به آن را به گونه‌ای پیکربندی کنیم که امکان دسترسی به اسامی و ساختار نام‌گذاری‌های انجام شده در فارست موجود در سازمان را داشته باشد.

۱- ابتدا در سرور مورد نظر، سرویس‌دهنده AD DS را نصب می‌کنیم.

۲- در برنامه Server Manager، بر روی گزینه Notifications کلیک می‌کنیم، سپس بر روی عبارت Promote This Server To A Domain Controller کلیک می‌کنیم.

۳- در پنجره Active Directory Domain Services Configuration Wizard، و در صفحه Deployment Configurations، بر روی گزینه Add A Domain Controller To An Existing Domain کلیک می‌کنیم (شکل زیر).

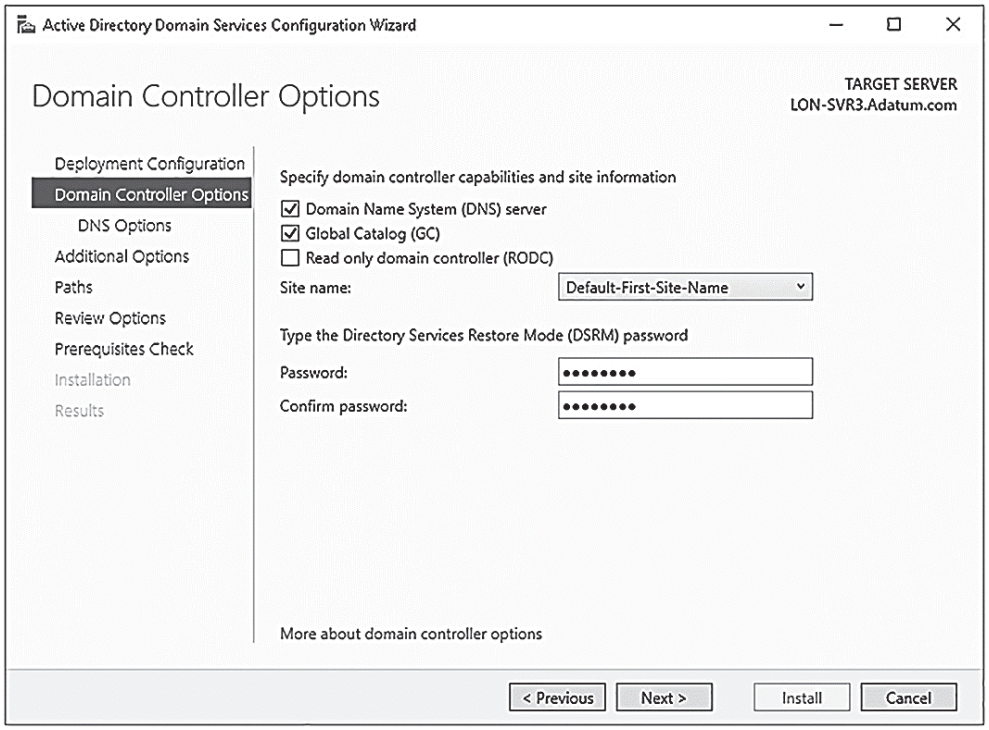


۴- نام دامنه را مشخص می‌کنیم. نام پیش‌فرض، نام دامنه‌ای در نظر گرفته می‌شود که سرور مورد نظر در آن قرار دارد. البته امکان انتخاب سایر دامنه‌های موجود در فارست نیز وجود دارد.

۵- برای انجام عملیات پیش‌رو، اطلاعات حساب کاری با سطح دسترسی مناسب را وارد می‌کنیم. به‌طور پیش‌فرض، اطلاعات حساب کاری کاربر جاری در نظر گرفته می‌شود.

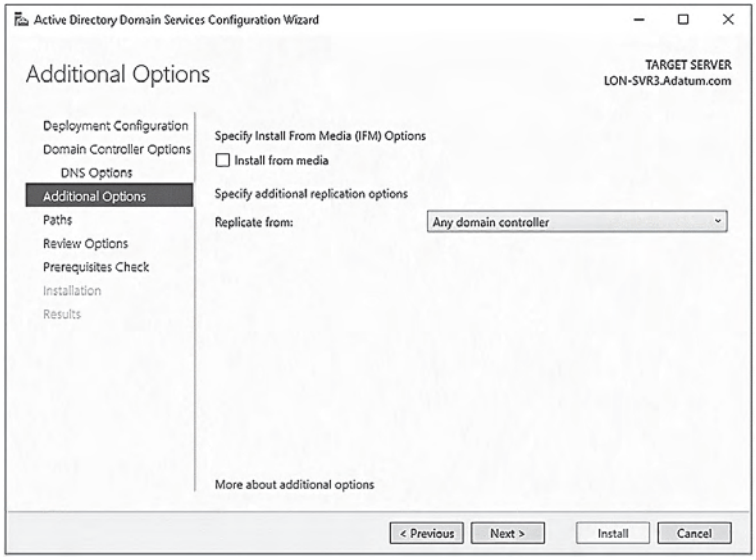
۶- در صفحه Domain Controller Options، اطلاعات سرور Domain Name System (DNS) و Global Catalog (GC) و Read Only Domain Controlole (RODC) (به‌طور پیش‌فرض فعال می‌باشند) را پیکربندی می‌کنیم. بر خلاف نخستین دامنه‌ای که در فارست ایجاد کردیم، می‌توانیم این دامنه را از نوع Read Only Domain Controller (RODC) تعریف کنیم.

۷- در فهرست Site name (شکل زیر)، نام سایتی که دامنه به‌طور فیزیکی در آن قرار دارد را مشخص می‌کنیم. به‌طور پیش‌فرض Default-First-Site-Name انتخاب شده‌است. تا زمانی‌که سایت‌های AD DS دیگری را ایجاد نکرده‌ایم، تنها سایت قابل انتخاب، این می‌باشد. پس از ایجاد سایت‌های جدید، امکان انتقال کنترل‌کننده دامنه به آنها نیز وجود دارد.



۸- رمزعبور Directory Services Restore Mode (DSRM) را وارد می‌کنیم و سپس بر روی کلید Next کلیک می‌کنیم.

۹- در صفحه Additional Oprions، باید چگونگی ثبت اطلاعات مربوط به کنترل‌کننده دامنه در بانک‌اطلاعات AD DS را مشخص کنیم. در این بخش، از اطلاعات موجود در کنترل‌کننده دامنه فعال استفاده می‌کنیم و یا اینکه گزینه Any Domain Controller را انتخاب می‌کنیم (شکل زیر) و یا کنترل‌کننده دامنه ویژه‌ای را انتخاب می‌کنیم. افزون بر آن می‌توانیم از گزینه Install From Media (IFM) استفاده کنیم. سپس بر روی کلید Next کلیک می‌کنیم.



۱۰- همانند کنترل‌کننده دامنه پیشین، فیلد Path را مقدارگذاری می‌کنیم و سپس بقیه مراحل نصب را ادامه می‌دهیم.

۱۱- در انتها بر روی کلید Install کلیک می‌کنیم. در حین نصب کنترل‌کننده دامنه، سرور مورد نظر راه‌اندازی خواهد شد.

پس از اتمام عملیات نصب می‌توانیم با استفاده از حساب کاری راهبر دامنه وارد می‌شویم.

افزودن کنترل‌کننده دامنه در یک دامنه جدید

برای افزودن کنترل‌کننده دامنه جدید در یک دامنه جدید در فارست موجود، باید با استفاده از حساب کاری کاربر عضو گروه راهبری فارست مورد نظر وارد شویم و سپس مراحل زیر را انجام دهیم.

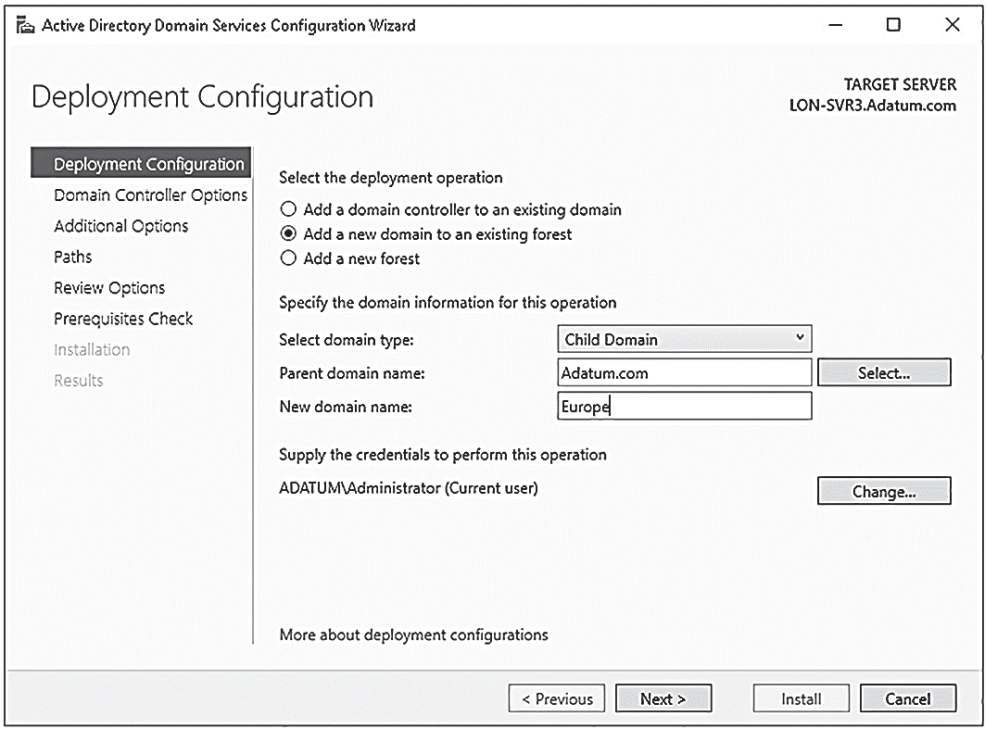
نکته آزمون

برای اینکه بتوانیم با استفاده از یک حساب کاری اعضای گروه راهبری در فارست مورد نظر وارد شویم، باید سرور مورد نظر پیش‌تر به عنوان عضو در یکی از دامنه‌های موجود در فارست AD DS مورد نظر، تعریف شده باشد. وگرنه، راحت‌ترین راه این است که سرور مورد نظر را به عنوان عضوی از ریشه فارست تعریف کنیم و سپس مراحل نصب را انجام دهیم. اگر نمی‌خواهیم این‌کار را انجام دهیم، باید با حساب کاری راهبر محلی وارد شویم و برای آن سطح دسترسی راهبری در شبکه سازمان را در نظر بگیریم و مراحل نصب را انجام دهیم. افزون بر آن لازم است که سرور مورد نظر به سرویس‌دهنده DNS موجود در فارست AD DS برای تفکیک اسامی مورد نیاز دسترسی داشته باشد.

۱- ابتدا سرویس‌دهنده Actice Directory Domain Services را بر روی سرور نصب می‌کنیم.

۲- در برنامه Server Manager، بر روی کلید Notifications کلیک و سپس عبارت Promote This Server To A Domain Controller را انتخاب می‌کنیم.

۳- در پنجره Active Directory Domain Services Configuration Wizard، در صفحه Deployment Configuration (شکل زیر)، گزینه Add A New Domain To An Existing Forest را انتخاب می‌کنیم.



۴- اکنون می‌توانیم چگونگی افزودن دامنه جدید را مشخص کنیم:

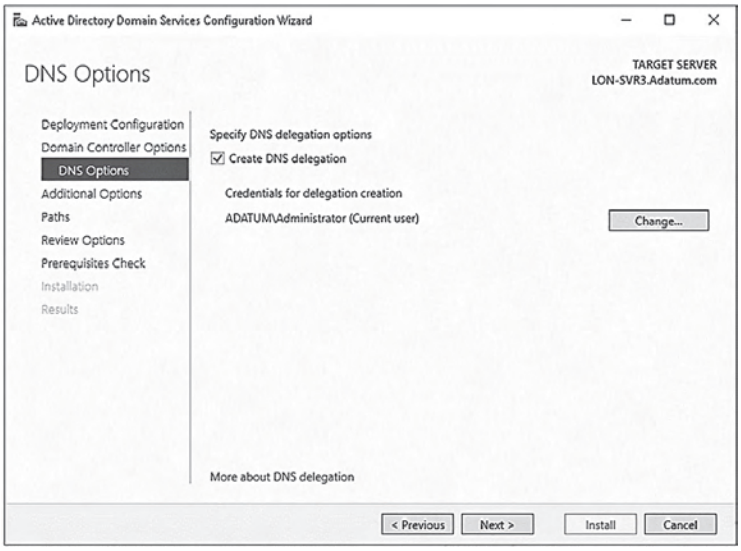
- **Child Domain** با استفاده از این گزینه یک دامنه فرعی در دامنه اصلی مورد نظر ایجاد می‌کنیم. به عبارت دیگر، دامنه جدید به عنوان یک شاخه در درخت موجود ایجاد خواهد شد.
- **Tree Domain** با استفاده از این گزینه، یک درخت جدید در فارست موجود ایجاد می‌کنیم. درخت جدید از همان الگوی فارست موجود استفاده می‌کند و ریشه آن هم دامنه ریشه مربوط به فارست می‌باشد، اما باید برای آن یک نام‌گذاری مستقل انجام دهیم. انجام این‌کار برای زمانی‌که در سرویس‌دهنده DNS چندین نام دامنه ایجاد می‌کنیم، بسیار مفید می‌باشد. اما لازم نیست که برای آن، عملیات راهبری جداگانه همانند یک فارست مستقل انجام دهیم. در صورتی‌که گزینه Tree Domain را انتخاب کنیم، باید فارستی را که می‌خواهیم درخت مورد نظر به آن اضافه شود، مشخص کنیم. به‌طور پیش‌فرض، فارستی که در آن وارد شده‌اید، انتخاب می‌شود.

۵- نام دامنه جدید را وارد می‌کنیم، در صورتی‌که گزینه دامنه فرعی (Child Domain) را انتخاب کرده باشیم، باید از نام دامنه اصلی به عنوان پسوند در نام دامنه مورد نظر استفاده کنیم. به عنوان مثال، برای ایجاد یک دامنه فرعی به نام Europe در دامنه اصلی Adatum.com باید نام دامنه مورد نظر را به‌صورت Europe.adatum.com ایجاد کنیم. در صورتی‌که دامنه به عنوان یک درخت جدید در فارست مورد نظر ایجاد می‌شود، نیازی به ذکر نام دامنه اصلی برای آن نمی‌باشد و سپس بر روی کلید Next کلیک می‌کنیم.

۶- در صفحه Domain Controller Options، سطح عملیاتی دامنه مورد نظر را مشخص می‌کنیم و در آن سرویس‌های DNS، GC و RODC را پیکربندی می‌کنیم. نام سایت مربوط به دامنه را انتخاب و در انتها برای سرویس DSRM، رمزعبور مناسبی انتخاب و بر روی کلید Next کلیک می‌کنیم.

۷- در صفحه DNS Options (شکل زیر)، گزینه Create DNS Delegation را انتخاب می‌کنیم، با این‌کار برای زیردامنه مورد نظر، در سرویس‌دهنده DNS، محدوده نام‌گذاری مورد نیاز را ایجاد و سپس بر روی کلید Next کلیک می‌کنیم.

نیاز به مطالعه بیشتر دارید؟ **آشنایی با مفهوم Zone Delegation**
برای دسترسی به اطلاعات بیشتر در مورد Zone Delegation، می‌توانید به آدرس زیر در تارنمای TechNet مایکروسافت، مراجعه کنید:
https://technet.microsoft.com/library/cc771640(v=ws.11).aspx



۸- نام دامنه NetBIOS را نیز مشخص می‌کنیم و ادامه مراحل نصب را انجام می‌دهیم و در انتها بر روی کلید Install کلیک می‌کنیم.

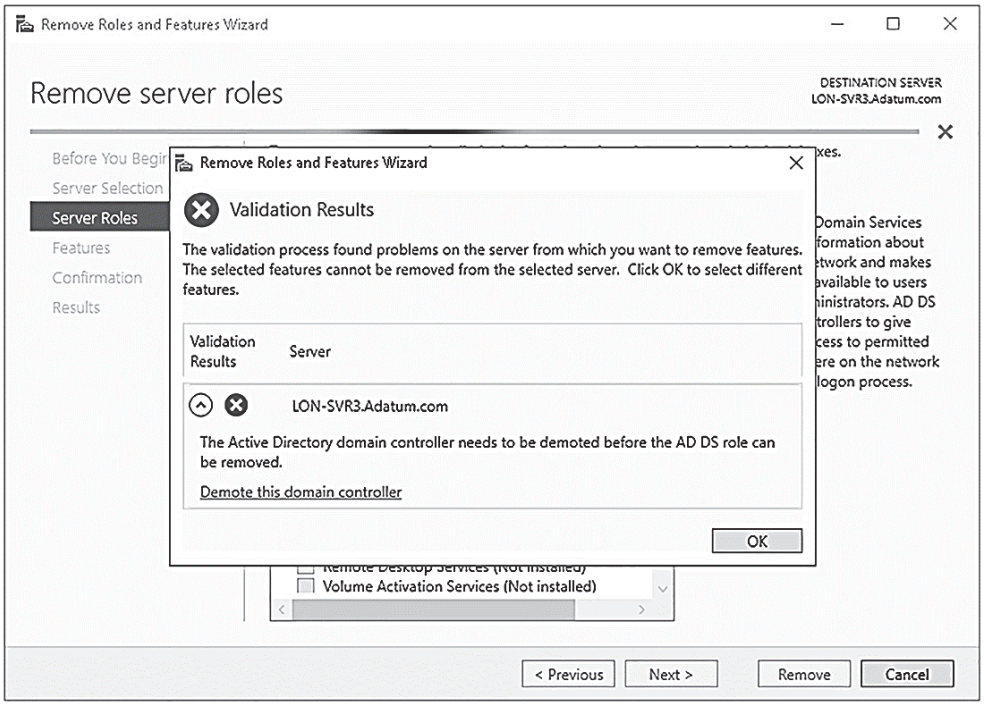
۹- در زمان نصب، سرور کنترل‌کننده دامنه یک‌بار راه‌اندازی مجدد می‌شود. پس از اتمام عملیات می‌توانیم با استفاده از حساب کاری راهبر دامنه وارد شویم.

حذف کنترل‌کننده‌های دامنه

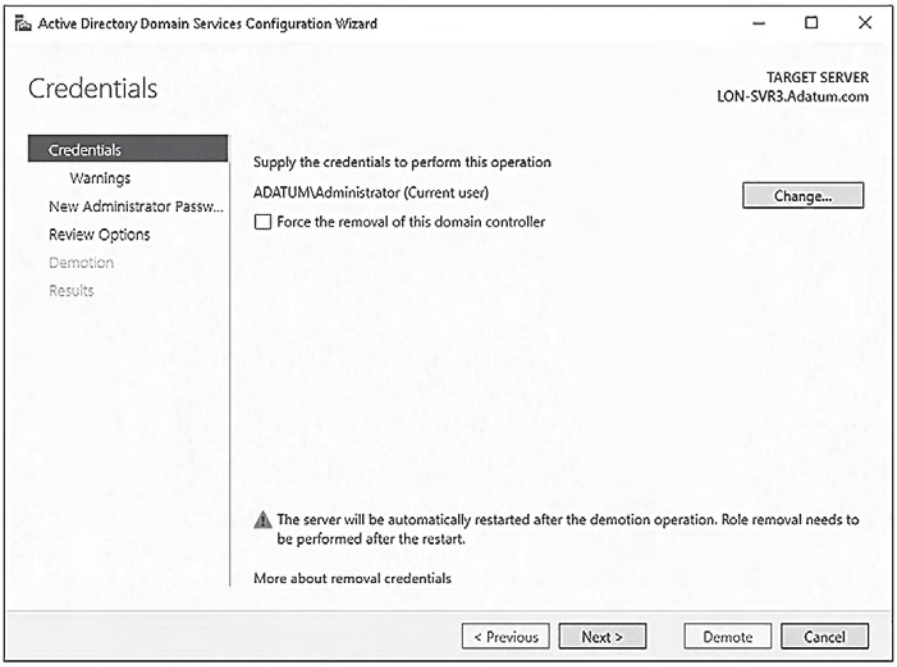
گاهی نیاز می‌باشد که کنترل‌کننده دامنه‌ای کنار گذاشته و حذف شود. انجام این‌کار، سرراست و ساده می‌باشد. برای انجام آن از برنامه Server Manager مطابق با مراحل زیر استفاده می‌کنیم:

۱- با استفاد از حساب کاری، با سطح دسترسی مناسب وارد می‌شویم. برای حذف کنترل‌کننده دامنه از یک دامنه، باید با حساب کاری راهبر دامنه وارد شویم و برای حذف تمام دامنه، باید با حساب کاری راهبر اصلی در شبکه سازمان وارد شویم.

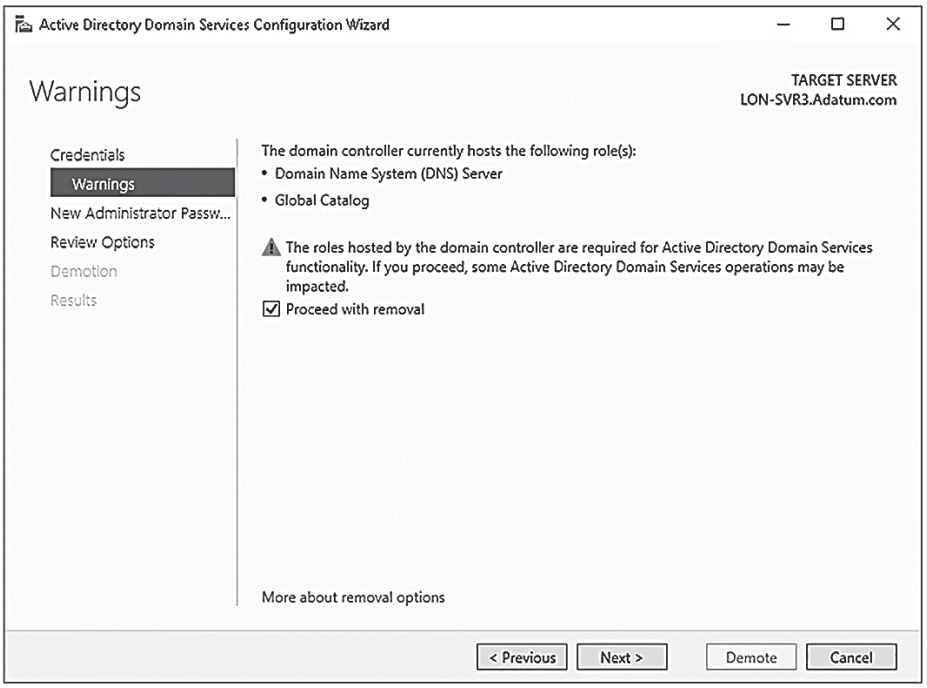
۲- برنامه Server Manager را باز می‌کنیم و از منوی Manage گزینه Remove Roles And Features را انتخاب می‌کنیم.
۳- در پنجره Remove Roles And Features Wizard، در صفحه Before you begin بر روی کلید Next کلیک می‌کنیم.
۴- در صفحه Select Destination Server، سرور مورد نظر را انتخاب و بر روی کلید Next کلیک می‌کنیم.
۵- در صفحه Remove Server Roles، گزینه Active Directory Domain Services را غیرفعال و سپس گزینه Remove Features را انتخاب و بر روی کلید Next کلیک می‌کنیم.
۶- در پنجره Validation Results (شکل زیر)، بر روی کلید Demote This Domain Controller کلیک می‌کنیم.



۷- پنجره Active Directory Domain Services Wizard باز می‌شود (شکل زیر)، در صفحه Credentials در صورت لزوم، اطلاعات حساب کاری کاربر مجاز برای حذف سرویس‌دهنده مورد نظر را وارد می‌کنیم. گزینه Force The Removal Of This Domain Controller را تا زمانی‌که دامنه دچار اشکال نشده باشد و یا اینکه قادر به پاسخی نباشد، انتخاب نمی‌کنیم. سپس بر روی کلید Next کلیک می‌کنیم.



۸- در صفحه Warnings (شکل زیر)، برای حفظ سرویس‌های DNS و GC سوال می‌شود. گزینه Proceed With Removal را انتخاب و سپس بر روی کلید Next کلیک می‌کنیم.



۹- در فیلد New Administrator Password، رمزعبوری را که برای راهبر محلی انتخاب کرده بودیم برای تأیید وارد می‌کنیم و سپس بر روی کلید Next کلیک می‌کنیم.

۱۰- گزینه‌های انتخاب شده را مرور و بر روی کلید Demote کلیک می‌کنیم.
۱۱- سرویس مورد نظر از سرور پاک خواهد شد و سرور یک‌بار راه‌اندازی مجدد می‌شود. سپس با استفاده از حساب کاری راهبر محلی می‌توانیم وارد شویم.

با استفاده از مراحل زیر می‌توانیم در کنترل‌کننده دامنه، حذف سرویس‌دهنده مورد نظر را کنترل کنیم:

۱- در کنترل‌کننده دامنه، بخش Active Directory Users And Computers را باز می‌کنیم و در فهرست Domain Controllers OU نباید نام کنترل‌کننده دامنه حذف شده را مشاهده کنیم.
۲- بر روی عبارت Computers container کلیک می‌کنیم، باید نام رایانه مورد نظر را در آن مشاهده کنیم.
۳- بخش Active Directory Sites And Services را باز می‌کنیم و در آن بخش Sites را انتخاب می‌کنیم و سپس بر روی عبارت Default-First-Site-Name کلیک می‌کنیم. در بخش Servers، نام سروری که کنترل‌کننده دامنه مورد نظر بر روی آن قرار داشت را حذف می‌کنیم.

نکته آزمون
اگر سرور غیرفعال شده، آخرین کنترل‌کننده دامنه در دامنه مورد نظر باشد، ابتدا باید همه رایانه‌های موجود در آن را حذف کنیم، البته باید آن‌ها را به دامنه دیگر در همان فارست منتقل کنیم. مراحل حذف در بالا اشاره شده است.

عملیات مربوط به حذف کنترل‌کننده دامنه را می‌توانیم با استفاده از دستورات خط فرمان پاورشل نیز انجام دهیم. برای این‌کار کافی است که دو دستور زیر را در خط فرمان پاورشل وارد کنیم:

```
Uninstall-addsdomaincontroller
Uninstall-windowsfeature AD-Domain_Services
```

نیاز به مطالعه بیشتر دارید؟ **حذف دامنه و کنترل‌کننده دامنه**
برای دسترسی به اطلاعات بیشتر در مورد حذف دامنه و کنترل‌کننده دامنه، می‌توانید به آدرس زیر در تارنمای TechNet مایکروسافت، مراجعه کنید:
https://technet.microsoft.com/en-us/windows-server-docs/identity/ad-ds/deploy/demoting-domain-controllers-and-domains--level-200-

نصب سرویس‌دهنده AD DS بر روی سرور Core

امکان پیاده‌سازی سرویس‌دهنده AD DS بر روی نسخه Core ویندوز سرور ۲۰۱۶ نیز وجود دارد. برای این‌کار باید از برنامه Server Manager و از راه دور و یا از دستور Install-WindowsFeatures AD-Domain-Services در خط فرمان پاورشل، استفاده کنیم.

پس از اینکه فایل‌های مورد نیاز را نصب کردیم، می‌توانیم با استفاده از برنامه Server Manager و از راه دور، پنجره Active Directory Domain Services Wizard را باز کنیم و سپس پیکربندی‌های مورد نیاز را در نسخه Core ویندوز سرور انجام دهیم، افزون بر آن می‌توانیم از دستور Install-ADDSDomainController در خط فرمان پاورشل نیز استفاده کنیم. ورای مراحل نصب فایل‌ها و باز کردن پنجره نصب سرویس‌دهنده AD DS، همه مراحل پیکربندی شبیه همان مراحلی است که در نسخه ویندوز سرور با رابط گرافیکی انجام دادیم (Desktop Experience).

نکته آزمون

امکان نصب سرویس‌دهنده AD DS در نسخه Nano Server وجود ندارد. بنابراین از نانو سرور نمی‌توانیم به عنوان کنترل‌کننده دامنه استفاده کنیم.

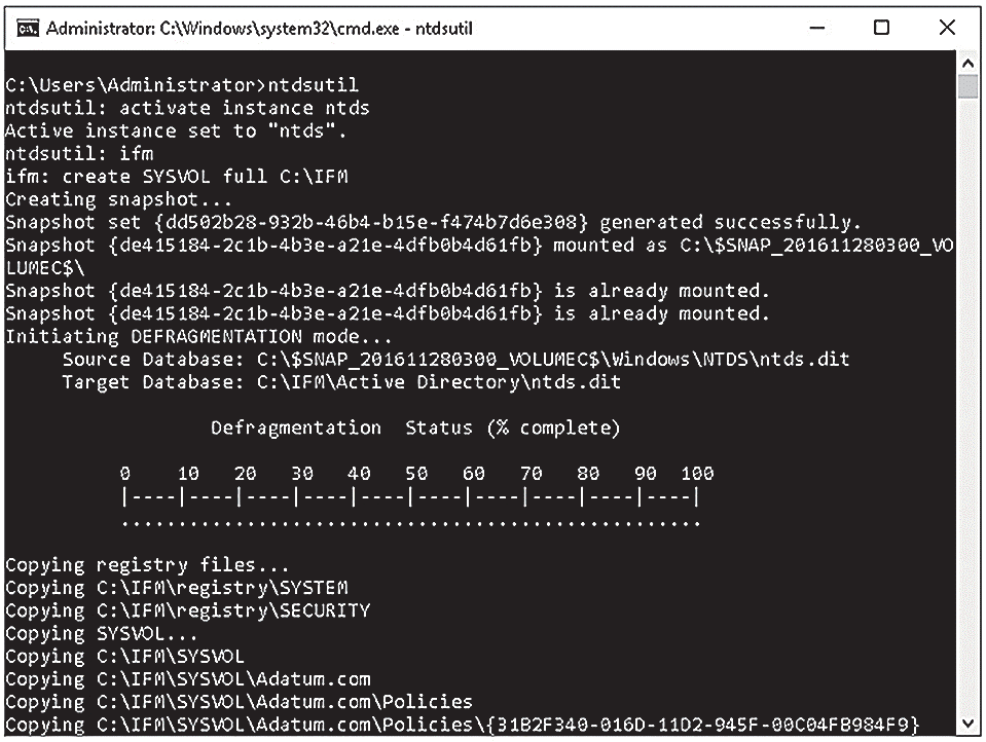
نصب کنترل‌کننده دامنه با استفاده از Media

در حین عملیات پیاده‌سازی کنترل‌کننده دامنه، محتویات بانک‌اطلاعات AD DS، در کنترل‌کننده دامنه جدید کپی می‌شود. این اطلاعات شامل الگو، پیکربندی‌های بخش‌های مختلف فارست و همچنین بخش مربوط به دامنه مورد نظر می‌باشند. پس از انجام همگام‌سازی اولیه، اطلاعات بین کنترل‌کننده‌های دامنه‌های موجود در فارست به روال عادی کپی‌برداری می‌شوند.

گاهی همگام‌سازی اولیه اطلاعات در کنترل‌کننده دامنه جدید با چالش‌هایی همراه می‌باشد. به عنوان مثال، زمانی‌که همگام‌سازی بین کنترل‌کننده‌هایی انجام می‌شود که در راه دور و با استفاده از خطوط ارتباطی با پهنای باند کم به‌یکدیگر متصل شده باشند، در این وضعیت، عملیات همگام‌سازی اولیه، زمان زیادی به درازا خواهد کشید و بخشی عمده از پهنای باند خطوط ارتباطی اشغال می‌شود.

برای رفع این چالش، عملیات همگام‌سازی کنترل‌کننده دامنه را با استفاده از کپی محتویات بانک‌اطلاعات AD DS در حافظه محلی انجام می‌دهیم. در این روش از گزینه پیاده‌سازی Install from Media (IFM) استفاده می‌کنیم و باید مراحل زیر را انجام دهیم:

۱- در کنترل‌کننده دامنه موجود، با استفاده از برنامه مرورگر فایل (File Explorer)، پوشه‌ای با نام دلخواه (C:\IFM) ایجاد می‌کنیم تا در آن یک نسخه کپی از محتویات بانک‌اطلاعات AD DS را ذخیره کنیم.
۲- پنجره خط فرمان را در سطح راهبر باز می‌کنیم و سپس در آن دستور ntdsutil.exe را اجرا می‌کنیم.
۳- در خط فرمان :ntdsutil، عبارت Activate instance ntds را وارد می‌کنیم و کلید Enter را فشار می‌دهیم.
۴- در خط فرمان :ntdsutil، عبارت ifm را وارد می‌کنیم و سپس کلید Enter را فشار می‌دهیم.
۵- در خط فرمان :ifm، عبارت create SYSVOL full C:\IFM را وارد می‌کنیم و سپس کلید Enter را فشار می‌دهیم (شکل زیر).

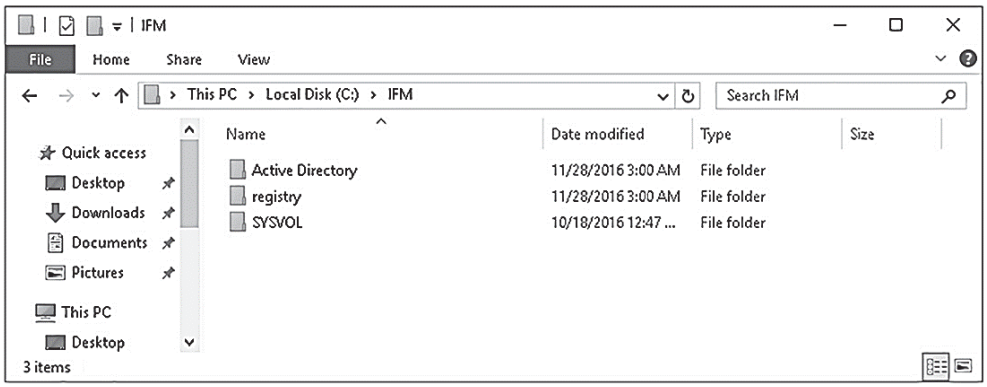


۶- در خط فرمان :ifm، عبارت quit را وارد می‌کنیم و کلید Enter را فشار می‌دهیم.

۷- در خط فرمان :ntdsutil، عبارت quit را وارد می‌کنیم و سپس کلید Enter را فشار می‌دهیم.

۸- پنجره خط فرمان را می‌بندیم.

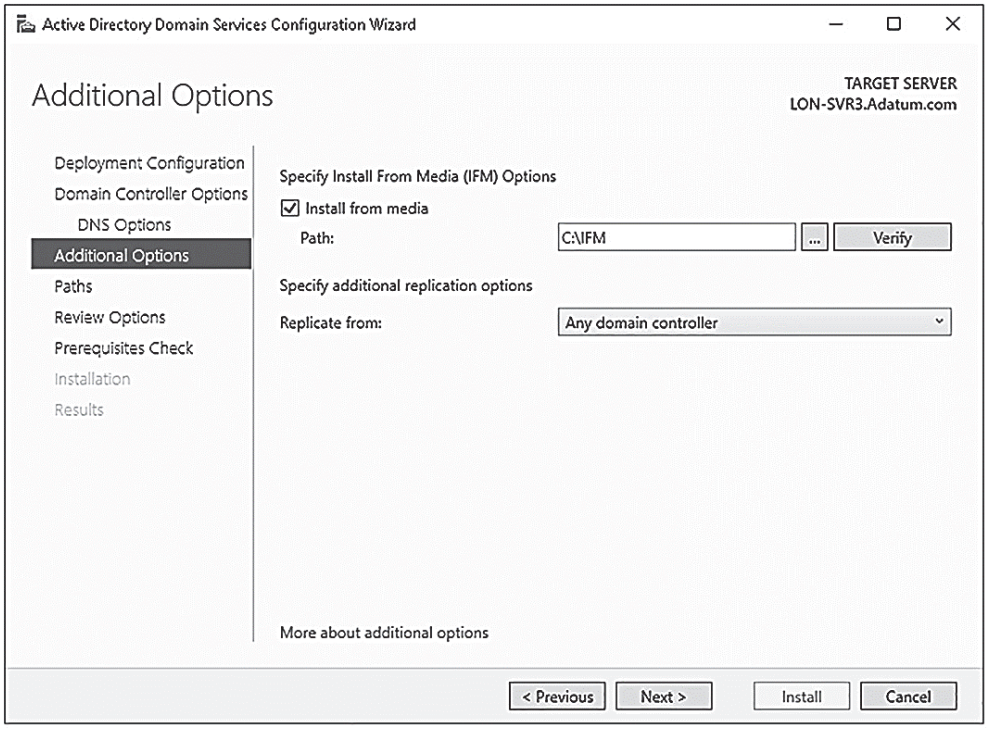
۹- در مروگر فایل، محتویات پوشه C:\IFM را در حافظه فلش کپی می‌کنیم (شکل زیر).



۱۰- در سرور کنترل‌کننده دامنه جدید، سرویس‌دهنده AD DS را مطابق با مراحل معمول نصب می‌کنیم، این‌کار را با استفاده از برنامه Server Manager و یا خط فرمان پاورشل انجام می‌دهیم.

۱۱- حافظه فلش موجود اطلاعات بانک‌اطلاعات AD DS را داخل سرور قرار می‌دهیم، سپس پنجره Active Directory Domain Services Wizard را از طریق برنامه Server Manager باز می‌کنیم و مراحل نصب را جلو می‌بریم.

۱۲- در صفحه Additional Options (شکل زیر)، گزینه Install From Media را انتخاب می‌کنیم. در فیلد Path، مسیر دسترسی به پوشه مورد نظر در حافظه فلش را مشخص و بر روی کلید Verify کلیک و سپس بر روی کلید Next کلیک می‌کنیم.



۱۳- مراحل نصب را ادامه می‌دهیم، در بخش آخر، تنظیمات انجام شده را مرور می‌کنیم و سپس بر روی کلید Install کلیک می‌کنیم. سرویس‌دهنده مورد نظر در حین عملیات نصب، یک‌بار راه‌اندازی مجدد می‌شود.

۱۴- پس از اتمام عملیات، می‌توانیم با حساب کاری راهبر وارد شویم.

اکنون در کنترل‌کننده دامنه جدید، محتویات کنترل‌کننده‌های دامنه موجود در فارست مورد نظر، قرار دارد. اینک می‌توانیم نام سایتی را که کنترل‌کننده دامنه مورد نظر در آن قرار دارد مشخص کنیم و سپس زمان‌بندی کپی‌برداری از اطلاعات در سایت مورد نظر را نیز تعیین کنیم. این عملیات در فصل دوم (مدیریت و نگهداری AD DS) و در بخش (مهارت ۲-۳: پیکربندی اکتیودایرکتوری در شبکه‌های سازمانی پیچیده) شرح داده می‌شوند.

نکته آزمون

برای انجام عملیات نصب و پیاده‌سازی کنترل‌کننده دامنه جدید می‌توانیم از دستور ADDSDomainController –InstallationMediaPath x:\ifm در خط فرمان پاورشل، در همان سرور نیز استفاده کنیم.

نصب و پیکربندی کنترل‌کننده دامنه فقط خواندنی (RODC)

در کنترل‌کننده فقط خواندنی (RODC)، محتویات موجود در سرویس‌دهنده AD DS با قابلیت خواندن از آن قرار داده می‌شود. از این نوع کنترل‌کننده‌های دامنه در بخش‌هایی از شبکه سازمان که در آن امنیت تضمین نشده است، استفاده می‌کنیم. به عنوان مثال، در شبکه شعب سازمان که در آن اتاق خاص و حفاظت شده برای سرور در نظر گرفته نشده است، می‌توانیم از این سرور به عنوان کنترل‌کننده دامنه محلی استفاده کنیم.

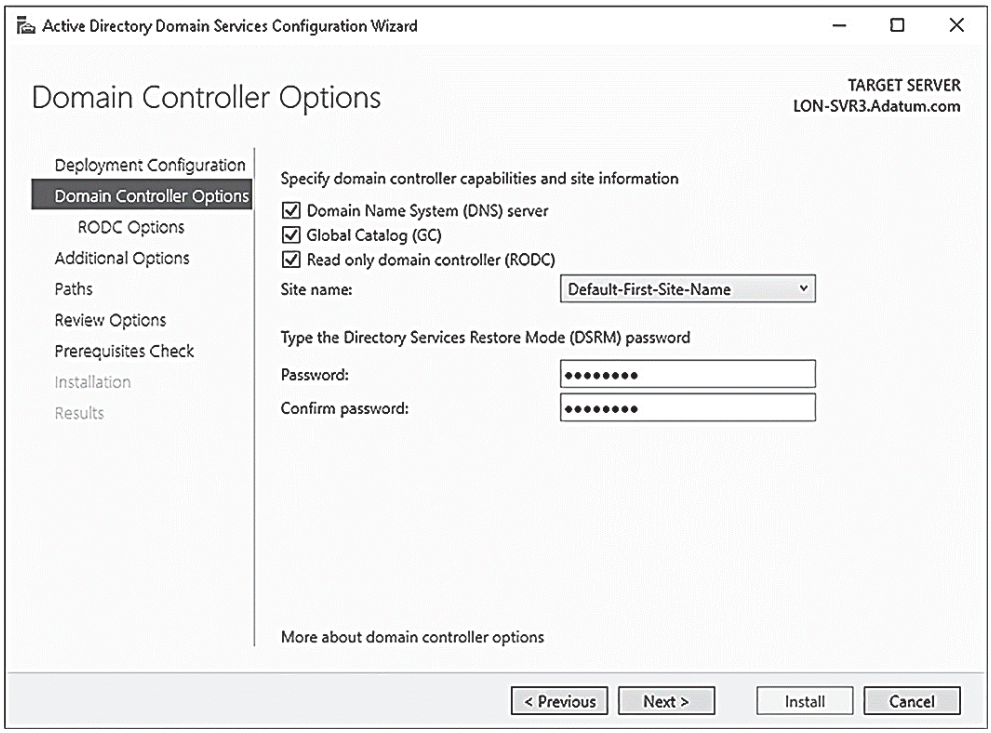
افزون بر آن این نوع کنترل‌کننده‌های دامنه به لحاظ راهبری دارای ویژگی‌های دیگری نیز می‌باشند که در زیر به آنها اشاره می‌کنیم:

- در هر دامنه و سایت، باید تنها یک عدد از این نوع کنترل‌کننده دامنه (RODC) داشته باشیم، زیرا تعدد آنها و عدم تطابق محتویات موجود در حافظه cache آنها باعث خواهد شد که کاربران و رایانه‌ها در هنگام ورود به دامنه با مشکل روبرو شوند.
- در سرویس‌دهنده RODC می‌توانیم سرویس‌دهنده DNS را نیز نصب کنیم. کاربران دامنه مورد نظر می‌توانند از این سرویس‌دهنده DNS همانند سرور دهنده DNS اصلی سازمان استفاده کنند و تنها در آن یک تفاوت وجود دارد، به‌روز رسانی پویا. با توجه به اینکه اطلاعات در این سرویس‌دهنده، فقط خواندنی می‌باشند، کاربران نمی‌توانند در محتویات آن، به‌روزرسانی پویا انجام دهند. در چنین شرایطی، برای کاربران باید نام کنترل‌کننده دامنه‌ای که می‌توانند اطلاعات موجود در آن را به‌طور پویا به‌روز رسانی کنند، مشخص شود.
- کنترل‌کننده دامنه RODC عملیات زیر را نمی‌تواند انجام دهد:
  - Operation master roles این عملیات نیازمند ثبت اطلاعات در بانک‌اطلاعات AD DS می‌باشند. به همین دلیل کنترل‌کننده RODC نمی‌تواند هیچیک از سرویس‌های پنج گانه این بخش را انجام دهد. این سرویس‌ها در ادامه این بخش شرح داده خواهند شد.
  - AD DS replication bridgeheads با توجه به اینکه این فناوری، وظیفه کپی‌برداری از محتویات بانک‌اطلاعات AD DS را بر عهده دارد، در این فناوری باید امکان ورود و خروج اطلاعات وجود داشته باشد. با توجه به اینکه کنترل‌کننده RODC تنها می‌تواند درخواست‌های ورودی را بپذیرد، بنابراین امکان استفاده از آن برای این نوع فناوری وجود ندارد.
- RODC نمی‌تواند:
  - در شبکه‌های راه دور (WAN) که خط ارتباطی قابل اعتماد وجود نداشته باشد، تأیید هویت انجام دهد. در صورتی‌که در شبکه شعبه سازمان، کاربران از کنترل‌کننده‌های دامنه متعدد استفاده کنند، کاربران غیر عضو در RODC نمی‌توانند عملیات تأیید هویت را در غیاب ارتباط راه دور انجام دهند. زیرا تأیید هویت کاربران غیر عضو بر اساس محتویات موجود در حافظه cache در کنترل‌کننده دامنه RODC انجام نمی‌شود.
  - امکان پشتیبانی از برنامه‌های کاربردی نیازمند ارتباط ثابت با سرویس‌دهنده AD DS. برخی از برنامه‌های کاربردی، نظیر مایکروسافت Exchange، نیاز به ارتباط دوطرفه با AD DS دارند. بنابراین با توجه به اینکه RODC این قابلیت را پشتیبانی نمی‌کند، در دامنه‌هایی که در آنها از این نوع برنامه‌های کاربردی استفاده می‌شود، باید از کنترل‌کننده‌هایی که امکان به‌روز رسانی اطلاعات در آنها وجود دارد، استفاده کنیم.

پیاده‌سازی RODC

پیش از پیاده‌سازی RODC، باید از وجود دست‌کم یک کنترل‌کننده دامنه قابل به‌روز رسانی اطلاعات در شبکه سازمان مطمئن شویم. پیاده‌سازی کنترل‌کننده دامنه RODC بسیار شبیه به مراحل ایجاد کنترل‌کننده‌های عادی در شبکه سازمان انجام می‌شود:

۱- ابتدا در سرور مورد نظر، سرویس‌دهنده Active Directory Domain Services را نصب می‌کنیم.
۲- پنجره Active Directory Domain Services Wizard را با استفاده از برنامه Server Manager باز می‌کنیم.
۳- در صفحه Domain Controller Options (شکل زیر)، گزینه Read Only Domain Controller (RODC) را انتخاب و در صورت نیاز گزینه‌های دیگر را نیز تنظیم و سپس بر روی کلید Next کلیک می‌کنیم.



۴- در صفحه RODC Options (شکل زیر)، گزینه‌های زیر را پیکربندی و سپس بر روی کلید Next کلیک می‌کنیم.