راهنمای جامع

MCSE 70-741

فنآوری شبکه با استفاده از ویندوز سرور ۲۰۱۶

Networking in Windows Server 2016

Andrew Warren

Microsoft Press

ترجمه: مهندس مهران تاجبخش

انتشارات پندارپارس

انتشارات پندارپارس

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

تلفن: ۶۶۵۷۲۳۳۵ - تلفکس: ۶۶۹۲۶۵۷۸ همراه: ۰۹۲۱۴۳۷۱۹۶۴

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

نام کتاب : **راهنمای جامع MCSE 70-740، فنآوری شبکه با استفاده از 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 : **۲۵۰۰۰ تومان** **شابک : ۵-۳۳-۸۲۰۱-۶۰۰-۹۷۸**

تقدیم به رامتین، پسر عزیزم.

ارزشمندترین سرمایه زندگی من.

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

تقدیم به دوست گرامی دکتر حسینی عزیز،

بی شک دوستان خوب همانند ستارگان در زندگی‌مان می‌درخشند.

سخنی با خواننده

این کتاب ترجمه کتاب ارائه شده توسط مایکروسافت در حوزه فناوری شبکه در ویندوز سرور ۲۰۱۶ با عنوان "Networking in Windows Server 2016" می‌باشد. کتاب با محتوای تخصصی در زمینه شبکه ویندوز سرور و برای کسب مدرک بین‌المللی در این حوزه (70-741) توسط شرکت مایکروسافت ارائه شده 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. نگارنده در تالیف کتاب، از درج تصاویر در هر مرحله برای شرح فناوری‌های مختلف استفاده کرده است تا خواننده 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 بین المللی 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

چنانچه 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، می توانند مدرک مهندسی مایکروسافت (MCSE) را کسب کنند.

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

درباره 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 دارد 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 ایشان می‌توانید از طریق رایانامه زیر اقدام نمایید:

info@mehrantajbakhsh.com

فهرست

فصل نخست

پیاده‌سازی سیستم نام دامنه (DNS)

معمولا، کاربران و رایانه‌ها از نام میزبان به جای آدرس IPv4 و IPv6 برای برقراری ارتباط با سایر ایستگاه‌ها و سرویس‌های شبکه استفاده می‌کنند. سرویس نام دامنه [1](DNS) در ویندوز سرور ۲۰۱۶ وظیفه تبدیل نام دامنه به آدرس‌های IPv4 و IPv6 را بر عهده دارد.

ازآنجایی‌که بسیاری از برنامه‌های کاربردی و سرویس‌های مهم در سرور از سرویس نام دامنه استفاده می‌کنند، آشنایی با این سرویس و چگونگی نصب و پیکربندی آن در ویندوز سرور ۲۰۱۶ از اهمیت زیادی برخوردار می‌باشد. به همین دلیل یکی از مباحث موجود در آزمون ۷۰-۷۴۱ (شبکه با ویندوز سرور ۲۰۱۶) نصب و پیکربندی و مدیریت سرویس‌دهنده نام دامنه (DNS) می‌باشد.

علاوه بر موارد فوق در آزمون 741-70 مباحثی نظیر پیاده‌سازی مناطق (DNS Zones) و رکوردهای سیستم نام دامنه، نیز از مواردی هستند که به آن پرداخته می‌شود. پیاده‌سازی، پیکربندی و مدیریت مناطق نام دامنه و همچنین ایجاد و مدیریت میزبان‌ها و رکوردهای مرتبط با سرویس‌ها در مناطق، از موارد مهمی هستند که باید در ویندوز سرور ۲۰۱۶ فراگرفته شوند.

مهارت‌های این فصل:

- نصب و پیکربندی سرورهای DNS
- ایجاد و پیکربندی مناطق و رکوردها در سرویس‌دهنده DNS

[1] Domain Name System

مهارت ۱/۱: نصب و پیکربندی سرورهای DNS

در ویندوز سرور ۲۰۱۶ سرویس‌دهنده DNS قابلیت ارائه سرویس تخصیص Domain Name (نام دامنه) برای رایانه‌ها و تجهیزات موجود در ساختار شبکه سازمان را دارد. اولین قدم برای استفاده از این سرویس، پیاده‌سازی سرویس‌دهنده DNS در ویندوز سرور ۲۰۱۶ می‌باشد.

مروری بر تعیین نام دامنه

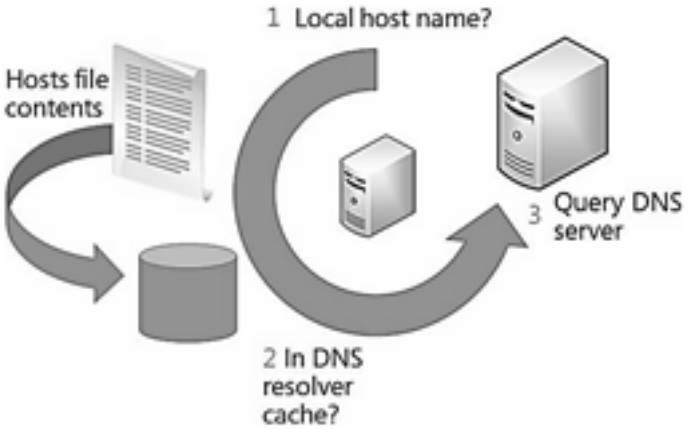
هرچند، استفاده از پروتکل آدرس‌دهیIP کاری دشوار و پیچیده نمی‌باشد، اما استفاده از نام ایستگاه به جای استفاده از آدرس‌های IPv4 و IPv6 بسیار ساده‌تر می‌باشد. همانند زمانی‌که با استفاده از نام تارنما قصد برقراری ارتباط با آن را دارید.

زمانی‌که از یک محصول، به‌طور مثال Microsoft Edge، برای دسترسی به یک تارنما از طریق نام آن اقدام می‌کنید، نخست نام تارنمای مورد نظر، با استفاده از سرویس نام دامنه به آدرس IPv4 و یا IPv6 متناظر با آن در لایه پایین‌تر تبدیل می‌گردد. در ویندوز ۱۰ و ویندوز سرور ۲۰۱۶ از دو نوع نام به شرح زیر استفاده می‌شود:

- **نام‌های میزبان (Host names):** یک نام میزبان می‌تواند حداکثر دارای ۲۵۶ حرف باشد، و تنها دارای حروف و اعداد و نقطه و خط تیره می‌باشد. نام میزبان در واقع نام مستعاری است که با نام دامنه در سرور DNS ادغام می‌شود. به‌عنوان مثال، نام مستعار computer1، به‌عنوان پیشوند نام دامنه‌ی Contoso.com در نظر گرفته می‌شود و با استفاده از آن، نام میزبان یا نام دامنه کامل[1](FQDN) به صورت computer1.contoso.com ایجاد می‌شود.
- **نام‌های NetBIOS:** این نام‌ها امروزه کاربرد چندانی ندارند، این اسامی از ساختار سلسه مراتبی (دارای پیشوند همانند نام دامنه) استفاده نمی‌کنند و تنها می‌توانند یک عبارت ۱۶ حرفی باشند. از حرف شانزدهم به‌عنوان مشخص کننده نام سرویس مورد نظر توسط ۱۵ حرف قبلی استفاده می‌شود. بنابراین، عبارت LON-SVR1[20h] برای مشخص کردن سرویس‌دهنده NetBIOS بر روی رایانه‌ای با نام LON-SVR1 استفاده می‌شود.

چگونگی تبدیل نام‌ها در ویندوز ۱۰ و ویندوز سرور ۲۰۱۶ به چگونگی پیکربندی آنها بستگی دارد. اما به‌طور معمول چگونگی عملکرد آنها همانند آن چیزی است که در شکل زیر نشان داده شده است:

[1] Fully Qualified Domain Name



مراحل زیر روند تخصیص نام میزبان در ویندوز ۱۰ و ویندوز سرور ۲۰۱۶ را نشان می‌دهند.

۱- تشخیص داده می‌شود، آیا نام میزبان درخواستی با نام میزبان محلی یکسان است.
۲- در حافظه محلی میزبان، مربوط به سرویس‌دهنده DNS، به دنبال نام دامنه درخواستی جست‌وجو می‌کند. محتویات این حافظه با توجه به اینکه نام میربان درخواستی یافت شود، به‌روز رسانده می‌شود. افزون بر آن محتویات فایل محلی Hosts، به این حافظه افزوده می‌شود.
۳- درخواست سرویس‌دهنده DNS برای نام میزبان درخواستی.

نیاز به مطالعه بیشتر دارید ؟ **تفکیک نام IPv4**

برای دسترسی به اطلاعات بیشتر در مورد تفکیک نام در پروتکل IPv4، به تارنمای Microsoft TechNet، در آدرس زیر مراجعه کنید:

https://technet.microsoft.com/library/dd379505(v=ws.0).aspx

البته سرویس DNS در ویندوز سرور ۲۰۱۶ قادر است تا فعالیت‌های بیشتری را از تبدیل نام میزبان به آدرس IPv4 و برعکس انجام دهد. رایانه‌ها با استفاده از این سرویس‌دهنده می‌توانند مکان سرویس‌های مورد نظر خود را در ساختار شبکه سازمان مشخص کنند. به‌عنوان مثال، زمانی‌که یک رایانه راه‌اندازی می‌شود، باید کاربر با استفاده از اطلاعات هویتی خود به اکتیودایرکتوری سرویس‌های دامنه (AD DS)[1] وارد شود و احتمالا می‌خواهد که نرم‌افزار Microsoft Outlook را اجرا کند. این بدان معنا است، که رایانه مورد نظر باید مکان سرویس‌دهنده اکتیودایرکتوری در دامنه محلی مورد نظر را پیدا کند، و پس از آن باید مکان قرارگیری سرویس‌دهنده، ایمیل و صندوق پستی مورد نیاز را مشخص کند. برای انجام این‌کارها از سرویس‌دهنده DNS استفاده می‌شود.

[1] Active Directory Domain Services

تعیین نیازها برای نصب سرویس‌دهنده DNS

پیش از اقدام به نصب سرویس DNS باید از وجود شرایط مورد نیاز در سرور مطمئن شویم. نیازهای سرویس DNS برای نصب عبارتند از:

- **امنیت،** باید پیش از اقدام به نصب به‌عنوان عضوی از گروه راهبران دامنه در سرور مورد نظر وارد شده باشیم.
- **پیکربندی IP،** در سرور مورد نظر، باید به‌طور ثابت پیکربندی‌های مورد نیاز برای آدرس‌های IPv4 و IPv6 را انجام داده باشیم. انجام این‌کار تضمین می‌کند که کاربران بتوانند در هر شرایطی مکان سرویس‌دهنده DNS مورد نظر را در ساختار شبکه پیدا کنند.

افزون بر موارد بالا، باید برای پاسخگویی به سوالات مربوط به ساختار و پیکربندی شبکه سازمان، آماده باشیم. این سوالات مربوط به شرایط ارتباط با اینترنت و شناسایی منابع سازمان با استفاده از اسامی ثبت شده نام دامنه، برای معرفی عمومی سازمان می‌باشند. البته در زمان نصب سرویس‌دهنده DNS نیازی به تعریف اسامی نام دامنه ذکر شده نیست، و آنها را پس از نصب و در زمان پیکربندی سرویس‌دهنده DNS در آن، تعریف می‌کنیم.

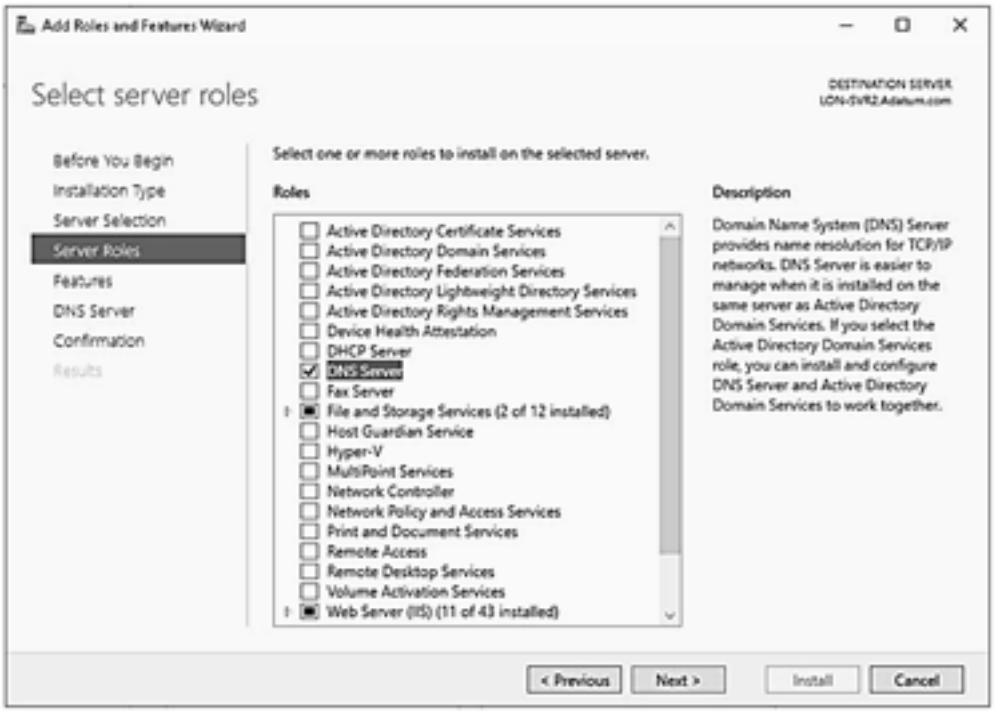
نصب سرویس‌دهنده DNS

برای نصب سرویس DNS، می‌توانیم از برنامه Server Manager و یا خط‌فرمان پاورشل استفاده کنیم.

نصب سرویس‌دهنده DNS با استفاده از Server Manager

برای نصب سرویس‌دهنده DNS با استفاده از Server Manager باید مراحل زیر را انجام دهیم:

۱- در سرور مورد نظر با حساب کاربری راهبر محلی، وارد می‌شویم.
۲- برنامه Server Manager را باز می‌کنیم.
۳- در برنامه Server Manager، بر روی گزینه Manage کلیک می‌کنیم و سپس گزینه Add Role & Features را انتخاب می‌کنیم.
۴- در پنجره نصب خودکار Add Role & Features، نخست در صفحه Before you begin، بر روی کلید Next کلیک می‌کنیم.
۵- در صفحه انتخاب نوع نصب (Select Installation Type)، گزینه Role-Based or Feature-Based Installation را انتخاب می‌کنیم، سپس بر روی کلید Next کلیک می‌کنیم.
۶- در صفحه انتخاب سرور مقصد (Select Destination Server) از بخش Server Pool، سرور مورد نظر را انتخاب می‌کنیم، سپس بر روی کلید Next کلیک می‌کنیم.
۷- در فهرست سرویس‌ها (Roles list) در صفحه انتخاب نقش و سرویس (Select Server Role)، گزینه DNS Server را انتخاب می‌کنیم، سپس بر روی کلید Next کلیک می‌کنیم (شکل زیر).



۸- در پنجره Add Role & Features، بر روی کلید Add Features کلیک می‌کنیم و سپس بر روی کلید Next کلیک می‌کنیم.

۹- درصفحه Select feature page، بر روی کلید Next کلیک می‌کنیم.

۱۰- در صفحه DNS Server page، بر روی کلید Next کلیک می‌کنیم.

۱۱- در صفحه Confirm Installation Selection، بر روی کلید Install کلیک می‌کنیم. پس از اینکه عملیات نصب خاتمه یافت، بر روی کلید Close کلیک می‌کنیم.

نصب با استفاده از خط‌فرمان پاورشل ویندوز

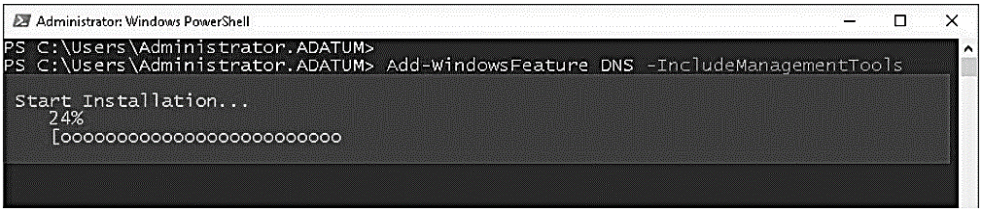
با توجه به اینکه نصب سرویس، در سرور مورد نظر با استفاده از برنامه Server Manager بسیار ساده می‌باشد، اما همیشه سریع‌ترین راه ممکن نیست. برای نصب سرویس‌دهنده DNS و ابزارهای مرتبط با آن با استفاده از خط‌فرمان پاورشل ویندوز، باید مراحل زیر را انجام دهیم:

۱- در سرور مقصد با استفاده از حساب کاربری Local Administrator، وارد می‌شویم.

۲- پنجره خط‌فرمان پاروشل را در سطح راهبر باز می‌کنیم.

۳- در خط‌فرمان فرمان پاورشل، همانند شکل زیر دستور زیر را وارد می‌کنیم و سپس کلید Enter را فشار می‌دهیم:

```
Add-WindowsFeature  DNS -Include ManagementTools
```



معرفی سناریوهای پیاده‌سازی سرویس DNS پشتیبانی شده بر روی نانو سرور

نانو سرور یکی از گزینه‌های جدید در نصب ویندوز سرور ۲۰۱۶ می‌باشد. این نسخه همانند نسخه Core می‌باشد، اما به منابع سخت‌افزاری بسیار کمتری نیاز دارد. این ویرایش از ویندوز سرور دارای قابلیت‌های بسیار محدودی در عملیات مربوط به راهبر محلی می‌باشد، و می‌تواند برنامه‌های کاربردی ۶۴ بیتی و نرم‌افزارهای مامور (Agent) و ابزارها را پشتیبانی کند.

در انتخاب نانو سرور، به جای سایر نسخه‌های ویندوز سرور، باید شرایط مختلفی را در نظر گرفت. به‌عنوان مثال، نانو سرور گزینه مناسبی برای ایجاد سرویس‌دهنده وب با استفاده از نرم‌افزار IIS[1] می‌باشد. افزون بر آن، این سرور برای ایجاد سرویس‌دهنده DNS نیز ایده‌آل می‌باشد.

> نیاز به مطالعه بیشتر دارید ؟ **آغاز کار با نانو سرور**
> برای دسترسی به اطلاعات بیشتر در مورد چگونگی کار و استفاده از نانو سرور، به تارنمای Microsoft TechNet، در آدرس زیر مراجعه کنید:
> https://technet.microsoft.com/windows-server-docs/compute/nanoserver/getting-started-with-nano-server

برای نصب سرویس‌دهنده DNS بر روی نانو سرور، می‌توانیم یکی از روش‌های زیر را انتخاب کنیم:

- **نصب سرویس‌دهنده DNS به‌عنوان بخشی از مراحل نصب نانو سرور** در این حالت می‌توانیم در زمان نصب و پیاده‌سازی نانو سرور، با استفاده از دستور پاورشل New-NanoServerImage، از پارامتر –Packages Microsoft-NanoServer-DNS-Packageاستفاده کنیم تا در حین نصب نانو سرور، سرویس‌دهنده DNS نیز بر روی سرور نصب شود.
- **افزودن سرویس مورد نظر پس از نصب نانو سرور**، در این حالت پس از اینکه نانو سرور نصب شد، می‌توانیم سرویس‌دهنده DNS مورد نظر را با استفاده از برنامه Server Manager، و یا خط‌فرمان پاروشل ویندوز، نصب کنیم. البته با توجه به اینکه این سرور دارای حداقل امکانات مدیریتی و راهبری محلی می‌باشد، این‌کار را باید به صورت راه‌دور بر روی سرور انجام دهیم.

برای نصب سرویس DNS بر روی نانو سرور، می‌توانیم از یکی از روش‌های زیر استفاده کنیم:

[1] Internet Information Services

- **با استفاده از برنامه Server Manager**، با استفاده از گزینه Add Other Server To Manage، نانو سرور مورد نظر را به فهرست سرورهای قابل مدیریت در برنامه اضافه می‌کنیم. برای افزودن سرویس DNS در سرور مورد نظر، باید همان مراحلی که در بالاتر به آن اشاره شد را انجام دهیم.
- **ایجاد نشست راهبری راه‌دور در نانو سرور با استفاده از خط‌فرمان پاورشل ویندوز Enter-PSSession**. پس از انجام این‌کار می‌توانیم با استفاده از دستور پاورشلی که در قسمت پیش برای نصب سرویس‌دهنده DNS به آن اشاره کردیم، سرویس DNS را بر روی نانو سرور نصب کنیم. به‌عنوان مثال می‌توانیم از دستور زیر برای نصب سرویس‌دهنده DNS بر روی نانو سرور استفاده کنیم:

```
Enable-WindowsOptionalFeature -Online -FeatureName DNS-Server-Full-Role
```

نکته آزمون

اکتیودایرکتوری دارای سرویس‌دهنده DNS در نانو سرور پشتیبانی نمی‌شود، به عبارت دیگر تنها می‌توانیم سرویس‌دهنده DNS مبتنی بر فایل را بر روی نانو سرور پیاده‌سازی کنیم.

نیاز به مطالعه بیشتر دارید؟ **فعال سازی و استفاده از دستورات راه‌دور خط‌فرمان پاورشل**

برای دسترسی به اطلاعات بیشتر در مورد استفاده از خط‌فرمان پاورشل از راه‌دور به تارنمای Microsoft TechNet در آدرس زیر مراجعه کنید:

https://technet.microsoft.com/magazine/ff700227aspx

پیکربندی Forwarders، Root Hints، Recursion و Delegation

پس از نصب سرویس‌دهنده DNS بر روی سرور مورد نظر، نوبت به پیکربندی آن می‌رسد. پیکربندی سرویس‌دهنده DNS شامل تنظیم Forwarders، Root Hints، Resursion و Delegation می‌باشد.

پیکربندی Forwarders

با استفاده از این فناوری می‌توانیم واکنش سرویس‌دهنده DNS مورد نظر را در زمانی‌که نمی‌تواند به درخواست ارسالی، پاسخ دهد مشخص کنیم. به‌عنوان مثال، می‌توانیم با استفاده از این فناوری سرویس‌دهنده‌های DNS مشخصی را برای دریافت درخواست‌های دریافتی از اینترنت، و ارائه پاسخ به آنها تعیین کنیم.

با استفاده از فناوری DNS Forwarding می‌توانیم عملیات زیر را انجام دهیم:

- سرویس‌دهنده DNS تنها به درخواست‌هایی که مراجع تائید شده توسط مناطق محلی ارسال شده‌اند، پاسخ دهد. آنگاه همه درخواست‌های دیگر به سرویس‌دهنده‌های DNS دیگر ارسال خواهند شد.
- شرایط انتقال درخواست‌ها به سرویس‌دهنده DNS در دامنه‌های مورد نظر را با استفاده از انتقال مشروط (Conditional forwarding) تعریف می‌کنیم. در صورتی‌که در درخواست دریافتی، نام دامنه

مورد نظر وجود داشته باشد، به‌طور مثال، contoso.com، آنگاه به سرویس‌دهنده DNS تعیین شده ارسال می شود.

برای پیکربندی فناوری Forwarding در سرویس‌دهنده DNS باید مراحل زیر را انجام دهیم:

۱- در برنامه Server Manager، از منوی Tools گزینه DNS را انتخاب می‌کنیم.
۲- در پنجره DNS Manager بر روی سرویس‌دهنده DNS مورد نظر کلیک راست می‌کنیم، سپس از منوی ظاهر شده گزینه Properties را انتخاب می‌کنیم.
۳- در پنجره Server Properties، بخش Forwarders را انتخاب می‌کنیم، سپس بر روی کلید Edit کلیک می‌کنیم.
۴- در پنجره Edit Forwarders، در فهرست IP Address، IP آدرس سرور مورد نظر که می‌خواهیم همه درخواست‌های DNS به آن ارسال گردند را وارد می‌کنیم و سپس بر روی کلید OK کلیک می‌کنیم. در این بخش می‌توانیم سرورهای DNS دیگر را نیز پیکربندی کنیم. در این بخش اولویت سرویس‌دهنده‌های DNS نیز مشخص می‌شوند. در این بخش امکان تنظیم زمان مجاز برای پاسخگویی به درخواست‌ها (Timeout) بر حسب ثانیه نیز تعیین می‌شود.
۵- در پنجره Server Properties در بخش Forwarders، می‌توانیم فهرست سرویس‌دهنده‌های تنظیم شده را مشاهده، و ویرایش کنیم (شکل زیر). همچنین در این بخش می‌توانیم واکنش این فناوری، زمانی‌که هیچ سرویس‌دهنده‌ای برای انتقال درخواست یافت نشود را نیز مشخص کنیم. به‌طور پیش‌فرض، در این شرایط فناوری Root Hints انتخاب می‌شود. این فناوری در بخش بعد شرح داده می‌شود. پس از اتمام پیکربندی بر روی کلید OK کلیک می‌کنیم.

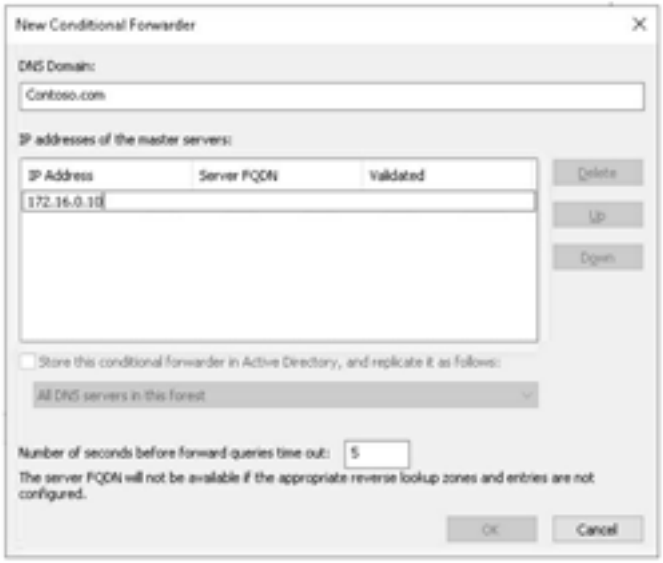
برای فعال‌سازی و پیکربندی انتقال مشروط (Conditional forwarding)، می‌توانیم از مراحل زیر استفاده کنیم:

۱- در بخش DNS Manager، بر روی عبارت Conditional Forwarding کلیک راست می‌کنیم، سپس گزینه New Conditional Forwarding را انتخاب می‌کنیم.

نکته آزمون

برای پیکربندی فناوری انتقال درخواست‌های سرویس‌دهنده DNS می‌توانیم از فرمان Add-DnsServerForwarder در خط‌فرمان پاورشل ویندوز نیز استفاده کنیم.

۲- در پنجره New Conditional Forwarding، همانند شکل زیر، در فیلد DNS Domain نام دامنه‌ای که برای آن شرط انتقال تعریف می‌شود، را وارد می‌کنیم. سپس در فیلد IP Address در بخش Master server list، آدرس سرویس‌دهنده برای انتقال را وارد می‌کنیم و سپس کلید Enter را فشار می‌دهیم.



۳- به‌طور اختیاری، می‌توانیم مقدار گزینه Number of Seconds Before Forward Queries Time Out را نیز مشخص کنیم. مقدار آن به صورت پیش‌فرض ۵ ثانیه می‌باشد.

۴- سپس بر روی کلید OK کلیک می‌کنیم.

نکته آزمون

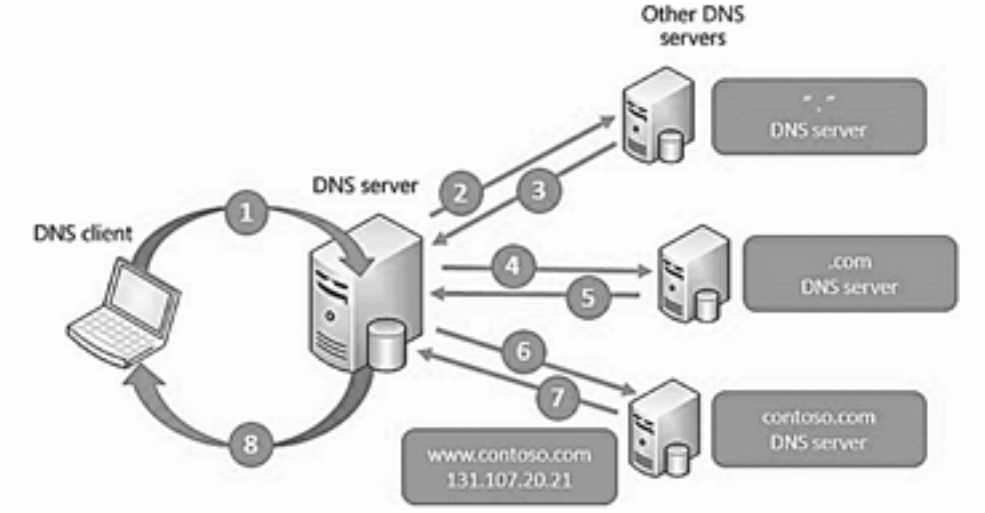
برای پیکربندی فناوری انتقال مشروط درخواست‌های سرویس‌دهنده DNS، می‌توانیم از فرمان Add-DnsServerConditionalForwarderZone در خط‌فرمان پاورشل ویندوز نیز استفاده کنیم.

پیکربندی Root Hints

اگر از فناوری DNS forwarding استفاده نکرده باشیم، در صورتی‌که سرویس‌دهنده DNS مورد نظر امکان پاسخ‌گویی به درخواست DNS دریافتی را نداشته باشد، از فناوری Root Hints برای ارائه پاسخ به آن استفاده می‌کند. پیش از پرداختن به فناوری Root Hints، بسیار مهم است که با چگونگی ارائه پاسخ به درخواست‌های DNS مربوط به اینترنت آشنا شویم.

درخواست‌های DNS اینترنت چگونه پردازش می‌شوند

برنامه کاربردی سمت کاربر، نظیر Microsoft Edge، درخواست تعیین IPv4 متناظر با نام دامنه مورد نظر (مثلا www.contoso.com) را دارد. به این برنامه کاربردی، سرویس‌گیرنده DNS گفته می‌شود. مراحلی که برای پردازش این نوع درخواست انجام می‌شود، در ادامه شرح داده شده است (شکل زیر).



۱- برای سرویس‌گیرنده DNS، پیکربندی سرویس‌دهنده DNS برای پاسخگویی به درخواست‌ها، (به‌طور مثال www.contoso.com)، به صورت بازگشتی انجام شده است.

نکته آزمون

زمانی‌که سرویس‌دهنده DNS درخواست بازگشتی دریافت می‌کند، یا نتیجه مربوط به آن را بازمی‌گرداند، و یا اینکه پیام خطا ارسال می‌کند، سرویس‌دهنده در این شرایط درخواست را به سرور دیگری انتقال نمی‌دهد.

- سرویس‌دهنده DNS کنترل می‌کند، در صورتی‌که صلاحیت ارسال پاسخ برای درخواست دریافتی را داشته باشد، آنگاه آن را به درخواست کننده ارسال می‌کند.
- در صورتی‌که صلاحیت آماده‌سازی پاسخ مناسب را نداشته باشد، در حافظه سرویس‌دهنده DNS در میزبان محلی، جست‌وجو می‌کند تا در صورت وجود، پاسخ مربوط به درخواست را در آن پیدا کند، و آن را به درخواست کننده ارسال کند.

۲- در صورتی‌که رکورد مورد نظر در حافظه پنهان سرور وجود نداشته باشد، آنگاه سرویس‌دهنده DNS با استفاده از درخواست‌های تکرار شونده، آن را به سرویس‌دهنده‌های DNS دیگر ارسال می‌کند. این‌کار را از سرویس‌دهنده ریشه (سرور سرشاخه) شروع می‌کند.

نکته آزمون

زمانی‌که سرویس‌دهنده DNS درخواست تکرارشونده دریافت کند، یا پاسخ مناسب برای آن را ارسال می‌کند و یا آن درخواست را به سایر سرویس‌دهنده دارای صلاحیت ارسال می‌کند.

۳- در صورتی‌که سرویس‌دهنده DNS ریشه بتواند به درخواست مورد نظر پاسخ دهد، آن را به درخواست کننده ارسال می‌کند، وگرنه IP آدرس سرویس‌دهنده بعدی دارای صلاحیت در یک سطح پایین‌تر را در همان شاخه (com.) باز می‌گرداند.
۴- سپس سرویس‌دهنده DNS اصلی با دریافت آدرس مورد نظر، درخواست تکرار شونده دیگری به سرویس‌دهنده مورد نظر ارسال می‌کند.
۵- در صورتی‌که سرویس‌دهنده DNSD در شاخه com. صلاحیت ارائه پاسخ مناسب برای درخواست دریافتی را نداشته باشد، آنگاه IP آدرس سرویس‌دهنده DNS مربوط به دامنه Contoso.com را باز می‌گرداند.
۶- سرویس‌دهنده DNS اصلی مربوط به دامنه Contoso.com، درخواست تکرارشونده دیگری را ارسال می‌کند.
۷- سرویس‌دهنده DNS مربوط به دامنه Contoso.com، صلاحیت ارائه پاسخ مناسب برای درخواست دریافت شده را دارد و در این مورد، پاسخ مناسب، آدرس IPv4 مربوط به دامنه Contoso.com می‌باشد.
۸- سرویس‌دهنده DNS اصلی، رکورد را در حافظه پنهان خود ذخیره می‌کند، و سپس آن را به درخواست کننده ارسال می‌کند.

فناوری Root Hints چگونه استفاده می‌شود

همان‌گونه که در توضیحات بالا و شکل پیش مشاهده کردید، در صورتی‌که سرویس‌دهنده DNS صلاحیت ارائه پاسخ را نداشته باشد، و اطلاعات مورد نیاز را در حافظه پنهان خود نداشته باشد، آنگاه از سرویس‌دهنده ریشه، برای یافتن سرویس‌دهنده DNS دارای صلاحیت برای ارسال پاسخ مناسب به درخواست دریافت شده، شروع می‌کند. البته باید توجه داشته باشیم، که بدون در اختیار داشتن IP آدرس سرویس‌دهنده DNS ریشه، انجام این عملیات امکان‌پذیر نمی‌باشد.

با استفاده از فناوری Root Hints، سرویس‌دهنده‌های DNS، می‌توانند در اینترنت به دنبال سرویس‌دهنده ریشه جست‌وجو کنند. سرویس‌دهنده DNS مایکروسافت، با استفاده از رکوردهای مربوط به فناوری Root Hints، از پیش پیکربندی شده‌اند. البته امکان ویرایش در این رکوردها، با استفاده از کنسول DNS Manager و با استفاده از خط‌فرمان پاورشل ویندوز نیز وجود دارد.

نکته آزمون

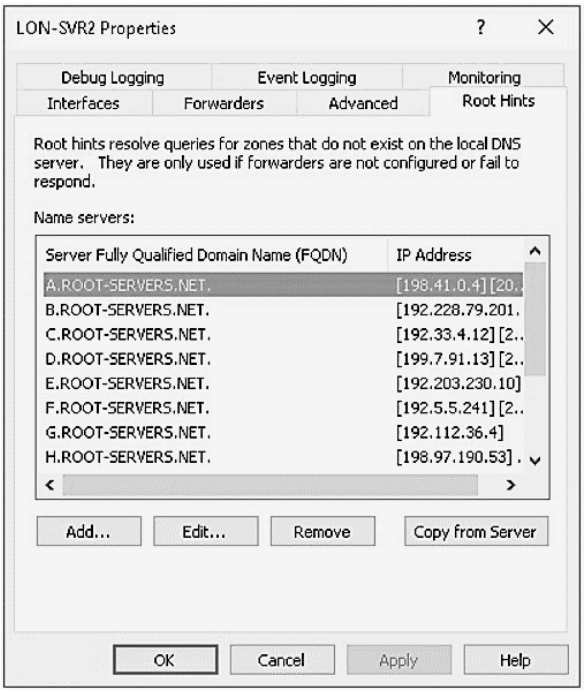
به‌طور پیش‌فرض، سرویس‌دهنده DNS فناوری Root Hints را با استفاده از یک فایل با نام CACHE.DNS که در مسیر %system root%\System32\dns قرار دارد، پیاده‌سازی می‌کند.

اگر بخواهیم جریان ترافیک مربوط به درخواست‌های سرویس‌دهنده DNS را در شبکه داخلی سازمان پیکربندی کنیم، می‌توانیم محتویات این فایل را ویرایش کنیم. البته انجام این‌کار برای شبکه میانی نیز، که در بین شبکه داخلی و اینترنت قرار دارد، نیز مفید می‌باشد.

ویرایش Root Hints

برای تغییر در اطلاعات Root Hints، از منوی Tools و گزینه DNS Manager، به صورت زیر استفاده می‌کنیم:

۱- در برنامه Server Manager، منوی Tools را باز می‌کنیم و در آن گزینه DNS Manager را انتخاب می‌کنیم.
۲- در کنسول DNS Manager، سرویس‌دهنده DNS مورد نظر را مشخص می‌کنیم. بر روی آن کلیک راست و از منوی باز شده گزینه Properties را انتخاب می‌کنیم.
۳- در پنجره Server Properties، همانند شکل زیر بخش Root Hints را انتخاب می‌کنیم.



۴- در این بخش می‌توانیم رکورد جدید اضافه کنیم، و یا رکوردهای موجود را ویرایش و یا حذف کنیم. در این بخش می‌توانیم با کلیک بر روی کلید Copy From Server، اطلاعات مربوط به Root Hints را از سرویس‌دهنده DNS دیگر، درون‌ریزی (import) کنیم. پس از اینکه عملیات ویرایش Root Hints به پایان رسید، بر روی کلید OK کلیک می‌کنیم.

با استفاده از دستورات خط‌فرمان پاورشل ویندوز نیز، امکان ویرایش اطلاعات مربوط به Root Hints وجود دارد. برای مدیریت Root Hints، دستورات زیر در خط‌فرمان پاورشل ویندوز در نظر گرفته شده‌اند:

- **Add-DnsServerRootHints** امکان افزودن رکورد جدید در Root Hints را فراهم می‌سازد.
- **Remove-DnsServerRootHints** با استفاده از این دستور می‌توانیم، رکورد Root Hints را حذف کنیم.

- **Set-DnsServerRootHints** با استفاده از این دستور می‌توانیم، رکورد Root Hints موجود را ویرایش کنیم. همچنین با استفاده از Get-DnsServerRootHints امکان بازیابی اطلاعات رکورد مورد نظر برای ویرایش را داریم.
- **Import-DnsServerRootHints** امکان تهیه کپی از اطلاعات Root Hints موجود در سرویس‌دهنده DNS دیگر را فراهم می‌سازد.

به‌عنوان مثال، برای به‌روز رسانی مقدار تخصیص داده شده به H.Root-server.adatum.com، در Root Hints، در خط‌فرمان پاورشل از دو دستور زیر استفاده می‌کنیم:

```
$hint = (Get-DnsServerRootHint | Where-Object {$_.NameServer.RecordData.NameServer -eq
"H.Root-Servers.Adatum.com."} )
$hint.IPAddress[0].RecordData.Ipv4address = "10.24.60.254"
```

با استفاده از دستور نخست، اطلاعات مربوط به H.Root-servers.adatum.com بازیابی شده، و در متغیری به نام $hint قرار داده می‌شود. با استفاده از دستور Get-DnsServerRootHint می‌توانیم فهرستی از همه رکوردهای موجود در Root Hints را بازیابی کنیم، و با استفاده از پارامتر Where-Object نتیجه خروجی دستور را با مقدار مورد نظر فیلتر می‌کنیم (H.Root-servers.adatum.com).

پیکربندی Recursion

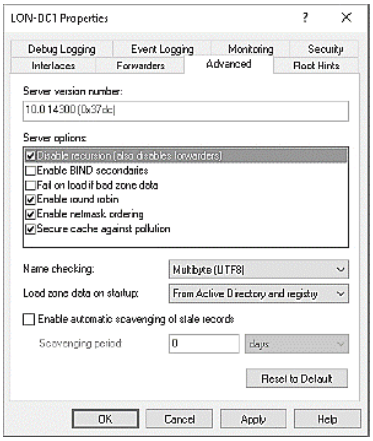
این فناوری به روند عملیاتی گفته می‌شود، که سرویس‌دهنده DNS اصلی دریافت کننده درخواست کاربر، برای دسترسی به پاسخ درخواست، از جانب درخواست کننده، درخواست او را به سرویس‌دهنده DNS دیگر، ارسال می‌کند. سپس پاسخ دریافتی را به درخواست کننده ارسال می‌کند. به‌طور پیش‌فرض، همه سرویس‌دهنده‌های DNS، درخواست‌های دریافتی را به این شکل، به سرویس‌دهنده‌های DNS دیگر ارسال می‌کنند، و آنها نیز پاسخ را به سرویس‌دهنده‌های اصلی، باز می‌گردانند، و از طریق آنها پاسخ‌ها به کاربران انتقال داده می‌شوند.

از آنجایی‌که کاربران خراب‌کار، می‌توانند با استفاده از این فناوری، حمله اختلال در سرویس (DoS)[2] را در سرویس‌دهنده‌های DNS اجرا کنند، بنابراین باید این فناوری را در سرویس‌دهنده‌های DNS موجود در شبکه داخلی سازمان، غیرفعال کنیم، تا درخواست‌های بازگشتی از این نوع را دریافت نکنند.

برای غیرفعال کردن فناوری درخواست‌های بازگشتی (Recursion)، باید از مراحل زیر استفاده کنیم:

۱- در برنامه Server Manager، از منوی Tools، گزینه DNS Manager را انتخاب می‌کنیم.
۲- در کنسول DNS Manager، بر روی سرور مورد نظر کلیک راست می‌کنیم، و از منوی باز شده گزینه Properties را انتخاب می‌کنیم.
۳- بخش مربوط به Advanced را انتخاب می‌کنیم (شکل زیر)، در بخش Server Options گزینه Disable Recursion (Also Disbale Forwarders) را انتخاب می‌کنیم و سپس بر روی کلید OK کلیک می‌کنیم.

[2] Denial of Service



Recursion Scopes

همان‌گونه که ممکن است به نظر برسد، غیرفعال کردن فناوری ارسال درخواست‌های بازگشتی، مفید و سودمند نیست، زیرا سرویس‌دهنده‌هایی نیز وجود دارند، که باید این فناوری در آنها فعال باشد. اما با توجه به اینکه همچنان ریسک تهدید و حمله در مورد آنها وجود دارد، در ویندوز سرور ۲۰۱۶، از فناوری Recursion Scopes استفاده می‌شود. با استفاده از این فناوری، می‌توانیم محدوده امکان دریافت درخواست‌های بازگشتی، در سرویس‌دهنده‌های DNS را کنترل کنیم. برای انجام این‌کار، باید از DNS Server Policies استفاده کنیم.

به‌عنوان مثال، فرض می‌کنیم که باید سرویس‌دهنده DNS در شبکه داخلی با امکان ارسال درخواست‌ها به صورت بازگشتی، برای کاربران موجود در دامنه Adatum.com وجود داشته باشد، اما این سرویس‌دهنده، نباید امکان دریافت درخواست‌های بازگشتی که دارای منبع اینترنتی هستند، را داشته باشد. برای پیکربندی این تنظیم در سرویس‌دهنده DNS مورد نظر، کافی است که خط‌فرمان پاورشل را باز کنیم و از دو دستور زیر استفاده کنیم:

```
Set-DnsServerRecursionScope -Name . -EnableRecursion $False
Add-DnsServerRecursionScope -Name "InternalAdatumClients" -EnableRecursion $True
```

با استفاد ه از دستور نخست، فناوری Recursion را برای محدوده پیش‌فرض در سرویس‌دهنده DNS غیرفعال می‌کنیم، که نتیجه آن غیرفعال شدن این فناوری در سرویس‌دهنده مورد نظر می‌باشد. محدوده پیش‌فرض برای این فناوری، همچنان‌که در بالاتر نیز به آن اشاره کردیم، مربوط به سرورهای بازگشتی، و انتقال دهنده‌ها (Server-lewvel resusion and forwarders) می‌باشد.

دستور دوم، محدوه جدیدی با نام InternalAdminClients ایجاد می‌کند، و فناوری Recursion برای کاربران موجود در این محدوده فعال می‌شود. در مرحله بعد باید مشخص کنیم، که کدام کاربر، در این محدوده جدید قرار دارد. با استفاده از دستور پاورشل زیر می‌توانیم این‌کار را انجام دهیم:

```
Add-DnsServerQueryResolutionPolicy -Name "RecursionControlPolicy" -Action ALLOW
-ApplyOnRecursion -RecursionScope "InternalAdatumClients" -ServerInterfaceIP
"EQ,10.24.60.254"
```

در این مثال، درخواست‌های کاربرانی که به سرویس‌دهنده DNS دارای IP آدرس 10.24.60.254 ارسال می‌شوند، به‌عنوان کاربران موجود در محدوده InternalAdminClients در نظر گرفته می‌شوند، و برای آنها فناوری Recursion فعال می‌باشد. برای درخواست‌های سایر کاربرانی که به درگاه‌های دیگر سرویس‌دهنده DNS ارسال می‌شوند، فناوری Recusrion غیرفعال در نظر گرفته می‌شود.

نیاز به مطالعه بیشتر دارید؟ **Add -Dnsserverqueryresolutionpolicy**
برای دسترسی به اطلاعات بیشتر در مورد پیکربندی محدوده درخواست‌های بازگشتی در خط‌فرمان پاورشل، به تارنمای Microsoft TechNet، در آدرس زیر مراجعه کنید:
https://technet.microsoft.com/library/mt126273.aspx

پیکربندی Delegation

این مبحث در ادامه این فصل شرح داده خواهد شد.

پیکربندی تنظیمات پیشرفته DNS

با استفاده از فناوری‌های Forwarding و Recursion و Root Hints می‌توانیم، مبانی عملکرد سرویس‌دهنده‌های DNS، را در قبال درخواست‌های دریافتی در ساختار شبکه سازمان، پیکربندی و کنترل کنیم. پس از تنظیم و پیکربندی فناوری‌های فوق، نوبت به تنظیم‌های پیشرفته در سرویس‌دهنده DNS می‌رسد.

پیکربندی DNSSEC

فناوری DNSSEC، برای حفاظت از سرویس‌دهنده DNS، مورد استفاده قرار می‌گیرد. این فناوری همه رکوردهای موجود در محدوده DNS را امضای دیجیتال می‌کند، به این ترتیب، کاربران سرویس‌دهنده، می‌توانند با استفاده از آن، اعتبار و مشمولیت اطلاعات موجود در اطلاعات دریافتی از سرویس‌دهنده DNS را کنترل کنند. با استفاده از این فناوری، کاربران می‌توانند مطمئن شوند که با سرویس‌دهنده DNS اصلی در ارتباط هستند.

نکته **DNS Zones**
ایجاد و مدیریت مناطق DNS در بخش "ایجاد مناطق DNS" شرح داده خواهد شد.

زمانی‌که کاربر، درخواستی را به سرویس‌دهنده DNS، که در آن فناوری DNSSEC فعال شده است، ارسال می‌کند، سرویس‌دهنده همه پاسخ‌های ارسالی به کاربر را امضای دیجیتال می‌کند. برای اینکه با استفاده از امضای دیجیتال، کاربر بتواند مشمولیت و اعتبار اطلاعات دریافتی را کنترل کند، باید کلید عمومی مربوط به زوج کلید عمومی/خصوصی امضای دیجیتال مورد نظر را، از مرجع قابل اعتماد صادر کننده کلیدها دریافت کند. برای این منظور، کاربران برای ارتباط به سرویس‌دهنده DNS، باید به‌طور مناسب پیکربندی شوند.

صادر کننده‌های زوج کلید قابل اعتماد (Trust Anchors)

برای پیاده‌سازی فناوری DNSSEC، باید نخست فضای TrustAnchors را ایجاد کنیم. از این فضا برای نگهداری کلیدهای عمومی مناطق مورد نظر در سرویس‌دهنده DNS استفاده می‌شود. نخست باید برای هر یک سرویس‌دهنده DNS که میزبان منطقه‌ای می‌باشند، از طریق منطقه امن، صادر کننده امن یا Trust Anchor ایجاد کنیم.

جدول آیین‌نامه تفکیک اسامی (Name Resulotion)

افزون بر آن، باید جدول آیین‌نامه تفکیک اسامی (NRPT) را ایجاد و منتشر کنیم. آیین‌نامه DNSSEC که در جدول NRPT درج می‌شود، برای تعیین شرایط کاربران سرویس دهنده DNS و ارسال دستورالعمل‌های مورد نیاز کاربران برای استفاده از فناوری امضای دیجیتال و برای اعتبارسنجی درخواست‌ها و پاسخ‌های دریافتی از سرویس‌دهنده مورد نظر می‌باشند.

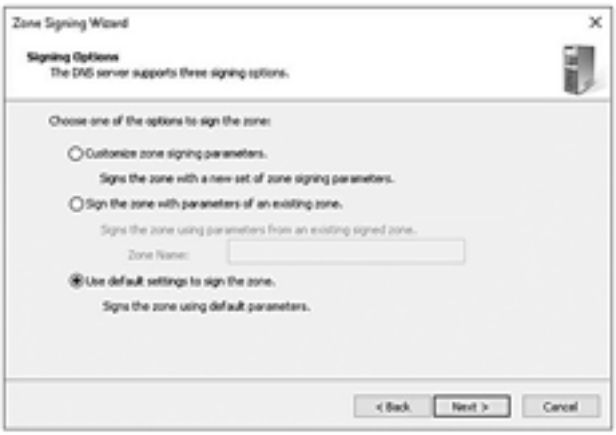
نکته آزمون

به‌طور معمول در محیط سرویس دامنه اکتیودایرکتوری (AD DS) از GPO برای انتشار جدول NRPT استفاده می‌شود.

پیاده‌سازی فناوری DNSSEC

پس از نصب ویندوز سرور ۲۰۱۶ و پیاده‌سازی سرویس‌دهنده DNS در آن، با استفاده از مراحل زیر می‌توانیم فناوری DNSSEC را در آن فعال کنیم:

۱- در کنسول DNS Manager پنجره DNSSEC Configuration Wizard را باز می‌کنیم، تا با استفاده از آن به منطقه DNS مورد نظر وارد شویم. بر روی منطقه مورد نظر کلیک راست می‌کنیم، از منوی باز شده گزینه DNSSEC را انتخاب و بر روی گزینه Sign The Zone کلیک می‌کنیم. پس از اینکه به منطقه موردنظر وارد شدیم (همانند شکل زیر)، امکان انتخاب سه گزینه مختلف را خواهیم داشت.



- **Customize Zone Signing Parameters** با استفاده از این گزینه امکان پیکربندی همه مقادیر مربوط به Key Signing Key (KSK) و Zone Signing Key (ZSK) را خواهیم داشت.
- **Sign The Zone With Parameters Of An Existing Zone** امکان استفاده از همان پارامترها و مقادیر موجود در دامنه وارد شده داده می‌شود.
- **Use Default Settings To Sign The Zone** با استفاده از مقادیر پیش‌فرض امکان ورود به منطقه مورد نظر را می‌دهد.

۲- در بخش بعد گزینه Configure Trust Anchor Distribution Points را انتخاب می‌کنیم. این گزینه وقتی انتخاب می‌شود که در بخش پیشین، گزینه Customize Zone Settings Parameters انتخاب شده باشد؛ وگرنه پس از ورود به منطقه مورد نظر، با استفاده از مراحل زیر می‌توانیم صادر کننده و توزیع کننده قابل اعتماد کلیدهای عمومی را پیکربندی کنیم:

- در DNS Manager، بر روی منطقه دلخواه کلیک راست می‌کنیم، از منوی باز شده گزینه DNSSEC را انتخاب می‌کنیم، سپس بر روی عبارت Properties کلیک می‌کنیم.
- در پنجره DNSSEC Properties مربوط به منطقه مورد نظر، در بخش Trust Anchor (همانند شکل زیر)، گزینه Enable The Distribution Of Trust Ancors For This Zone را فعال می‌کنیم، سپس بر روی کلید OK کلیک می‌کنیم. پس از اینکه پیام بر روی صفحه ظاهر شد، بر روی کلید Yes کلیک می‌کنیم و سپس بر روی کلید OK کلیک می‌کنیم.

- نقطه صادر کننده قابل اعتماد (Trust Anchor Points) را بررسی می‌کنیم و وجود رکوردهای DNS KEY (DNSKEY) را در آن کنترل می‌کنیم. برای انجام این‌کار در برنامه DNS Manager، در بخش Server عبارت Trust Points را انتخاب می‌کنیم. در این بخش باید اسامی مناطق مورد نظر که حاوی دو رکورد DNS KEY می‌باشند، مشاهده گردند.

۳- در مرحله بعد نوبت به پیکربندی جدول NRPT در سیستم‌های کاربران می‌رسد. برای این منظور باید جدول NRPT پیکربندی شده را به تمامی ایستگاه‌های کاربران منتشر کنیم، تا آنها نیز مراحل اعتبارسنجی درخواست‌ها را در سرویس‌دهنده DNSSEC بدانند. ساده‌ترین راه برای این‌کار استفاده از فناوری GPO می‌باشد:

- نخست پنجره Group Policy Management را باز می‌کنیم و در آن Default Domain Policy را انتخاب می‌کنیم.
- این آیین‌نامه را برای ویرایش باز می‌کنیم و در آن مسیر زیر را انتخاب می‌کنیم (همانند شکل زیر):

Computer Configuration / Policies / Windows Settings / Name Resolution Policy

- در بخش Create Rules، نام دامنه مورد نظر خود را در فیلد پسوندی وارد می کنیم (به‌طور مثال www.Adatum.com).
- گزینه Enable DNSSEC را برای آیین‌نامه مورد نظر انتخاب می‌کنیم. گزینه Require DNS Clients To Check That The Name And Address Data Has Been Validated By The DNS Server را نیز انتخاب می‌کنیم، سپس بر روی کلید Create کلیک می‌کنیم.

نیاز به مطالعه بیشتر دارید؟ **نمایش گام به گام فناوری Dnssec در فضای آزمایشگاهی**
برای دسترسی به اطلاعات بیشتر در مورد پیکربندی فناوری DNSSEC، به تارنمای Microsoft TechNet، در آدرس زیر مراجعه کنید:
https://technet.microsoft.com/library/hh831411(v=ws.11).aspx

پیکربندی DNS socket pool

با استفاده از این فناوری می‌توانیم سرویس‌دهنده DNS را به شکلی پیکربندی کنیم که برای دریافت درخواست‌ها، از گذرگاه‌های تصادفی استفاده کند. در صورتی‌که این فناوری در سرویس‌دهنده DNS مورد نظر فعال شده باشد، در زمان راه‌اندازی آن برای دریافت درخواست، گذرگاهی را از میان گذرگاه‌های موجود (Socket pool) و آزاد، به صورت تصادفی انتخاب می‌کند. این بدان معنا است که سرویس‌دهنده از گذرگاه‌های پیش‌فرض و شناخته شده استفاده نمی‌کند. این‌کار تا حد زیادی از حملات مهاجمانی که قصد ارسال ترافیک مخرب از طریق گذرگاه‌های شناخته شده سرویس‌دهنده DNS را دارند، جلوگیری می‌کند. برای پیکربندی اندازه DNS socket pool، می‌توانیم از دستور خط‌فرمان DNSCMD.exe استفاده کنیم. برای این‌کار کافی است که در خط فرمان در سطح راهبر، دستور زیر را وارد کنیم:

dnscmd /Config /SocketPoolSize <value>

البته باید پس از اجرای این فرمان، سرویس‌دهنده DNS را یک‌بار راه‌اندازی کنیم. امکان تنظیم اندازه socket pool بین ۰ تا ۱۰/۰۰۰ وجود دارد. اندازه پیش‌فرض آن ۲۵۰۰ می‌باشد.

پیکربندی cache locking

وقتی که کاربری درخواست بازگشتی را به سرویس‌دهنده DNS ارسال می‌کند، سرویس‌دهنده پاسخ مربوط به آن را در حافظه پنهان خود (cache) نگهداری می‌کند، بنابراین می‌تواند به سایر کاربرانی که همان درخواست را دارند، سریعتر پاسخ دهد. مدت زمانی‌که این اطلاعات می‌توانند در حافظه پنهان (cache) باقی بمانند، با استفاده از مقدار TTL (Time To Live) تعیین می‌شود.

در مدت زمان TTL، در صورتی‌که اطلاعات تازه‌تر از رکورد موجود در حافظه cache دریافت شود، رکورد مورد نظر به‌روز رسانده خواهد شد. البته این‌کار می‌تواند یک تهدید امنیتی جدی ایجاد کند. با استفاده از این قابلیت، مهاجم و خراب‌کار می‌تواند اطلاعات موجود در این فضا را با داده‌های مخرب بازنویسی کند و به این ترتیب کاربر را به تارنمایی با محتوای مخرب هدایت کند.

برای کاهش این تهدید و خطر در ویندوز سرور ۲۰۱۶، می‌توانیم با استفاده از فناوری cache locking، زمانی‌که داده‌های موجود در حافظه cache، می‌توانند به‌روز رسانی شوند، را مشخص کنیم. در صورتی‌که این فناوری در سرویس‌دهنده DNS مورد نظر فعال شده باشد، تا وقتی که زمان TTL به‌اتمام نرسد، امکان به‌روز رسانی محتوای رکورد وجود ندارد.

برای پیکربندی فناوری cache locking در سرویس‌دهنده DNS، باید فرمان زیر را در خط‌فرمان پاورشل اجرا کنیم:

Set -DnsServerCache –LockingPercent <value>

مقدار <value> درصدی از محتوای TTL می‌باشد. به‌عنوان مثال، در صورتی‌که عدد ۷۵ را در آن قرار دهیم، آنگاه سرویس‌دهنده DNS تا زمانی‌که دست‌کم ۷۵ درصد از زمان TTL سپری نشده باشد، امکان به‌روز رسانی محتوای رکورد مورد نظر را نمی‌دهد.

نکته آزمون

به‌طور پیش‌فرض مقدار درصد در cache locking عدد ۱۰۰ در نظر گرفته می‌شود. این بدان معنا است که تا اتمام کامل TTL اجازه به‌روز رسانی محتوای رکورد مورد نظر داده نمی‌شود.

فعال‌سازی Response Rate Limiting

یکی دیگر از قابلیت‌های امنیتی در ویندوز سرور ۲۰۱۶، استفاده از فناوری response rate limiting می‌باشد. این فناوری برای مقابله با حمله DoS[3] (اختلال در سرویس) پیش‌بینی شده است. یکی از روش‌های اجرایی این نوع حمله در سرویس‌دهنده‌های DNS، ارسال ترافیک بیش از حد ظرفیت پاسخ‌گویی، به سرور مورد نظر می‌باشد.

در صورتی‌که در سرویس‌دهنده DNS، فناوری respone rate limiting فعال شده باشد، با دریافت ترافیک مخرب و با حجم زیاد، به جای انتشار آن به سایر سرویس‌دهنده‌های دیگر، آن را نادیده می‌گیرد. تشخیص ترافیک مخرب توسط سرویس‌دهنده، با مشاهده درخواست مشابه به تعداد زیاد و در فواصل زمانی کوتاه از یک منبع، انجام می‌شود.

به‌طور پیش‌فرض، این فناوری در سرویس‌دهنده DNS غیرفعال می‌باشد. برای فعال‌سازی این فناوری در سرویس‌دهنده DNS، باید دستور زیر را در خط فرمان پاورشل و در سطح راهبر اجرا کنیم:

Set DnsServerRespon seRateLimiting

این فرمان، فناوری response rate limiting را با مقدار پیش‌فرض فعال می‌کند. در این فرمان، با استفاده از پارامتر موجود، نرخ ترافیک مورد نظر را مشخص می‌کنیم.

نیاز به مطالعه بیشتر دارید؟ **Set-Dnsserverresponseratelimiting**
برای دسترسی به اطلاعات بیشتر در مورد پیکربندی فناوری response rate limiting، به تارنمای Microsoft TechNet، در آدرس زیر مراجعه کنید:
https://technet.microsoft.com/library/mt422603.aspx

پیکربندی DNS-based authentication of named entities

ویندوز سرور ۲۰۱۶ از فناوری جدیدی با عنوان DNS-Based Authentication of Named Entioties (DANE) در سرویس‌دهنده DNS پشتیبانی می‌کند. این فناوری با استفاده از پروتکل Transport Layer Security Authentication (TSLA) کار می‌کند و می‌تواند برای جلوگیری از حملات مرد میانی (MiTM)[4] در سرویس‌دهنده DNS در شبکه کمک کند.

فناوری DANE با استفاده از اینکه کاربران سرویس‌دهنده DNS باید اطلاعات مورد نیاز خود را از دامنه‌هایی درخواست کنند که مرجع قابل اعتماد صادر کننده گواهینامه دیجیتال (CA)[5]برای آنها گواهینامه اعتبار سنجی صادر کرده باشد، کار می‌کند؛ به‌عنوان مثال، فرض کنید که کاربری درخواست دریافت آدرس IPv4 مربوط به تارنمای https://www.adatum.com را از سرویس‌دهنده DNS داشته باشد. سرویس‌دهنده DNS افزون

[3] Denial of Service

[4] Man In the Middle Attack

[5] Certificate Authority

بر اینکه پاسخ درخواست مورد نظر را به کاربر ارسال می‌کند، اطلاعات مربوط به گواهینامه اعتبارسنجی سرویس‌دهنده وب، که دامنه www.adatum.com در آن قرار دارد و توسط صادر کننده قابل اعتماد (CA) ارائه شده است، را نیز به کاربر ارسال می‌کند.

راهبری DNS

آشنایی با چگونگی راهبری سرویس‌دهنده DNS از اهمیت زیادی برخوردار می‌باشد. با استفاده از ابزارهایی نظیر برنامه DNS Manager و خط‌فرمان پاورشل، راهبر سازمان می‌تواند، با سرویس‌دهنده DNS تبادل اطلاعات و محاوره لازم برای مدیریت و راهبری آن، انجام دهد. در سازمان‌های بزرگ، عملیات راهبری این سرویس مهم و پرکاربرد، کاری دشوار و حساس می‌باشد. در چنین مواردی معمولا با استفاده از آیین‌نامه‌های DNS، راهبری آن را به گروه‌های ویژه‌ای در شبکه واگذار می‌کنیم. در این شرایط ورود به سرویس‌دهنده DNS و استفاده از فناوری DNS logging یکی از مشکلات بالقوه در این مسیر می‌باشد.

پیاده‌سازی آیین‌نامه‌های DNS

آیین‌نامه‌های DNS قابلیت جدیدی است که در ویندوز سرور ۲۰۱۶ برای تنظیم عملکرد و رفتار سرویس‌دهنده DNS در شرایط مختلف در نظر گرفته شده است. به‌عنوان مثال، پیش‌تر دیدیم، که چگونه با استفاده از محدوده‌های بازگشتی توانستیم رفتار سرویس‌دهنده DNS را در هنگام دریافت درخواست‌های بازگشتی کاربران، تعریف و پیکربندی کنیم. این مورد یک نمونه کاربردی از به‌کارگیری آیین‌نامه‌های DNS می‌باشد.

در سازمان، بر حسب نیاز می‌توانیم یک یا چند آیین‌نامه DNS را تنظیم و پیکربندی کنیم. مواردی که می‌توانند منجر به تنظیم آیین‌نامه‌های DNS شوند، عبارتند از:

- **دسترسی مناسب به برنامه‌های کاربردی** سرویس‌دهنده DNS، کاربران را به سالم‌ترین نقطه ارتباطی برنامه کاربردی هدایت می‌کند. به‌عنوان مثال، در زمان نیاز به سودمندی بالا (High Availibility)، به گروه سرورهای مقابله با خرابی (Failiover Cluster) هدایت خواهند شد.
- **مدیریت ترافیک** سرویس‌دهنده DNS می‌تواند کاربر را به نزدیکترین سرور و یا مرکزداده هدایت کند.
- **تقسیم مرکز پاسخگوی سرویس‌دهنده DNS (Split-brain)** سرویس‌دهنده DNS بر حسب اینکه کاربران در داخل و یا خارج از شبکه قرار دارند، درخواست‌های آنها را، پردازش و ارسال می کند.
- **فیلترینگ** سرویس‌دهنده DNS قادر است تا در صورت تشخیص مخرب بودن میزبان ارسال کننده درخواست، ترافیک مربوط به آن را مسدود کند.
- **عملکردهای قانونی (Forensics)** سرویس‌دهنده DNS قادر است تا در صورت تشخیص درخواست مخرب، به جای هدایت آن به نقطه مورد درخواست، آن را به نقطه مشخص و ایزوله شده هدایت کند.
- **انتقال بر حسب زمان‌های روز** سرویس‌دهنده DNS می‌تواند بر حسب زمان‌بندی‌های تعیین شده در روز، کاربران را به سرورها و مراکز داده مشخص، هدایت کند.

برای پیاده‌سازی آیین‌نامه DNS، باید از دستورات خط‌فرمان پاورشل استفاده کنیم. برای این‌کار نخست باید رکوردهای موجود در مناطق تعریف شده در سرویس‌دهنده DNS را طبقه‌بندی کنیم، سپس کاربران

سرویس‌دهنده DNS در شبکه‌های مشخص را انتخاب کنیم، و یا از سایر مواردی که می‌تواند در تفکیک کاربران در سرویس‌دهنده DNS کمک کنند، استفاده کنیم. با استفاده از مشخصات زیر می‌توانیم کاربران سرویس‌دهنده DNS را تفکیک کنیم:

- **زیرشبکه کاربران (Client subnet)** آدرس‌های IPv4 یا IPv6 مربوط به زیرشبکه کاربران.
- **محدوده بازگشتی (Recursion scope)** نسخه منحصر به‌فرد از تنظیمات گروهی که پیکربندی محدوده بازگشتی را در سرویس‌دهنده DNS کنترل می‌کند.
- **محدوده‌های منطقه (Zone Scopes)** در این بخش مجموعه‌ای از رکوردهای منابع موجود در منطقه مورد نظر قرار دارد. یک رکورد می‌تواند در محدوده‌های مختلفی قرار داشته باشد، که با توجه به محدوده‌ها می‌تواند دارای IP آدرس متفاوت نیز باشد. مناطق DNS، می‌توانند دارای چندین محدوده DNS باشند.

برای پیاده‌سازی آیین‌نامه‌های DNS، نخست باید از یک یا چند مورد از ویژگی‌های که در بالا به آن اشاره شد، استفاده کنیم، و کاربران مورد نظر را طبقه‌بندی کرده و در محدوده‌های مشخص، قرار دهیم.

۱- به‌عنوان مثال، برای ایجاد یک زیرشبکه برای کاربران سرویس‌دهنده DNS در نیویورک، می‌توانیم از دستور زیر استفاده کنیم:

```
Add-DnsServerClientSubnet -Name "NYCSubnet" -IPv4Subnet "172.16.0.0/24"
```

۲- با استفاده از آدرس‌های IPv4 و یا IPv6 می‌بایست زیرشبکه‌های مختلفی را برای کاربران سرویس‌دهنده DNS ایجاد کنیم.

۳- سپس با استفاده از دستور زیر می‌توانیم، برای کاربران زیرشبکه نیوریورک سرویس‌دهنده DNS، محدوده DNS (Zone Scope) ایجاد کنیم:

```
Add-DnsServerZoneScope -ZoneName "Adatum.com" -Name "NYCZoneScope"
```

۴- مجددا، بر اساس نیاز می‌توانیم محدوده‌های مختلف از مناطق را ایجاد کنیم.

۵- سپس، برای ایجاد یک رکورد مشخص از IP آدرس، برای کاربران واقع در محدوده نیویورک، باید دستور زیر را در خط‌فرمان پاورشل اجرا کنیم:

```
Add-DnsServerResourceRecord -ZoneName "Adatum.com" -A -Name "www" -IPv4Address
"172.16.0.41" -ZoneScope "NYCZoneScope"
```

۶- در انتها، باید آیین‌نامه مورد نظر برای تعیین چگونگی پاسخ‌دهی به کاربرانی که با استفاده از فاکتورهای فوق، تعریف کردیم، را تنظیم کنیم:

```
Add-DnsServerQueryResolutionPolicy -Name "NYCPolicy" -Action ALLOW -ClientSubnet
"eq,NYCSubnet" -ZoneScope "NYCZoneScope,1" -ZoneName "Adatum.com"
```

اکنون، اگر کاربری که در محدوده تعیین شده در نیویورک قرار داشته باشد، درخواستی را به سرویس‌دهنده DNS با استفاده از آدرس IPv4 تارنمای www.adatum.com، ارسال کند، پاسخ او آدرس 172.16.0.41 می‌باشد. در صورتی‌که مناطق و محدوده‌های دیگر برای مکان‌های مختلف ایجاد کنیم، می‌توانیم سرویس‌دهنده DNS را به‌گونه‌ای پیکربندی کنیم که بر اساس مکآن‌های مختلف، آدرس‌های مورد نظر را، در پاسخ کاربران، به آنها ارسال کنند.

نیاز به مطالعه بیشتر دارید؟ **مروری بر آیین‌نامه‌های DNS**
برای دسترسی به اطلاعات بیشتر در مورد پیکربندی آیین‌نامه‌های DNS، به تارنمای Microsoft TechNet، در آدرس زیر مراجعه کنید:
https://technet.microsoft.com/windows-serverdocs/networking/dns/deploy/dns-pol icies-overview

پیکربندی راهبری انتصابی (Delegated Administration)

به‌طور پیش‌فرض، گروه‌های زیر قابلیت راهبری سرویس‌دهنده DNS سازمان را دارند:

- **راهبران دامنه (Domain Admins)** دارای مجوز دسترسی کامل به همه امکانات و قابلیت‌های موجود در سرویس‌دهنده DNS در همان دامنه می‌باشند.
- **راهبران سازمان (Enterprise Admins)** دارای مجوز دسترسی کامل به همه امکانات و قابلیت‌های موجود در سرویس‌دهنده‌های DNS، واقع در همه دامنه‌ها در فارست سرویس دامنه اکتیودایرکتوری (AD DS) می‌باشند.
- **راهبران DNS (Dns Admins)** امکان مشاهده و ویرایش داده‌های موجود در سرویس‌دهنده، تنظیمات و پیکربندی سرویس‌دهنده‌های DNS در دامنه‌های مربوط به خود را دارند.

در شبکه‌های کوچک تا متوسط، استفاده از این راهبران پیش‌فرض قابل قبول می‌باشد، اما در شبکه‌های بزرگ سازمانی، بهتر است که جنبه‌های مختلف مدیریتی در سرویس‌دهنده‌های DNS را به گروه‌های مشخص منتصب کنیم.

در صورتی‌که بخواهیم عملیات راهبری سرویس‌دهنده DNS را به کاربر و یا گروهی خاص منتصب کنیم، باید کاربر و یا گروه مورد نظر را به گروه راهبران سرویس‌دهنده DNS، در دامنه موجود در فارست، اضافه کنیم. برای تغییر عضویت گروه مورد نظر، باید از بخش Computers and Users، در اکتیودایرکتوری و یا از دستور Add-ADGroupMember در خط‌فرمان پاورشل، استفاده کنیم.

برای پیکربندی مجوزهای دسترسی راهبری در سرویس‌دهنده DNS، باید بر روی نام سرویس‌دهنده DNS مورد نظر، و یا منطقه مورد نظر در کنسول DNS Manager کلیک راست کنیم، سپس از منوی باز شده، گزینه Properties را انتخاب کنیم. در پنجره Server Properties و یا Zone Properties، بخش Security را انتخاب کنیم و در این بخش می‌توانیم، مجوزهای دسترسی را مشاهده و آنها را تغییر دهیم (همانند شکل زیر):