پیکربندی Active Directory

این PDF به صورت تصویری و مرحله به مرحله توضیح داده شده است.

www.NetworkBooks.ir
www.TejaratServer.ir

برگرفته از پروژه های عملی شرکت

فصل سوم

پیکربندی Active Directory

NetworkBooks.ir

داشتن یک مدیریت متمرکز برروی تمامی منابع شبکه از جمله: کاربران، گروه‌ها، اعضای هر گروه، پرینترها و سایر اشیائی که در شبکه دخیل هستند امری مهم و حائز اهمیت می‌باشد. یکی از موارد مهم در مدیریت اشیاء شبکه، داشتن کنترل دقیق بر نحوه و نوع عملکرد اشیاء است.
Active Directory ابزاری است که ویندوزسرور با استفاده از آن به کنترل و مدیریت اشیاء موجود در شبکه می‌پردازد. هرشئ که بخواهد در شبکه با سایر اشیاء تعامل داشته باشد ابتدا باید در Active Directory ثبت شده باشد. درواقع با ثبت اشیاء در Active Directory عملیات احراز هویت برای شئ صورت می‌پذیرد.
در ابتدای این فصل بهتراست تا با انواع حالاتی که می‌توان یک شبکه را در سازمان پیاده کرد آشنا شده و سپس به بررسی بیشتر Active Directory بپردازیم.

انواع شبکه‌های سازمانی

انواع شبکه‌ها ازنظر سطح عملکرد در ویندوز به دو دسته Workgroup و Domain تقسیم می‌شوند که در ادامه این موارد توضیح داده خواهد شد.

Workgroup

معمولاً در شبکه‌هایی که کمتر از 50 کامپیوتر وجود دارد، از این نوع شبکه استفاده می‌شود. در این نوع شبکه سروری وجود نداشته و تمامی کامپیوترها می‌توانند هم سرور و هم کلاینت باشند (درواقع یک شبکه نظیربه‌نظیر است). دراین نوع از شبکه‌ها هرکامپیوتر به‌صورت کاملاً مستقل عمل کرده و با کامپیوترهای دیگر در ارتباط است. هرکاربر تنها می‌تواند از کامپیوتری استفاده کند که نام‌کاربری‌اش درآن ثبت شده باشد. به‌عنوان مثال اگر که نام‌کاربری X در PC1 وجود داشته باشد، کاربر نمی‌تواند در PC2 با استفاده از همان نام‌کاربری به سیستم وارد شود و درواقع اطلاعات کاربری و اشیاء شبکه به‌صورت محلی درهر کامپیوتر ذخیره شده‌است.
☑ در شبکه Workgroup برای ترجمه نام به IP از پروتکل NetBIOS استفاده می‌شود (در فصل 2 با نحوه کارکرد پروتکل NetBIOS آشنا شدید).
مشکلی که در این شبکه وجود دارد این‌است که اگر در شبکه تعداد کامپیوترها افزایش پیدا کند، شبکه در کارآیی دچار اختلال خواهد شد. به‌عنوان مثال فرض کنید در یک شبکه 500 کامپیوتر وجود دارد، حال اگر 100 کامپیوتر به‌صورت همزمان بخواهند باهم ارتباط داشته باشند باید از پروتکل NetBIOS استفاده کرده و اقدام به ارسال Broadcast کنند. بنابراین مجموعاً 100×499 بسته بیهوده در شبکه ارسال خواهد شد که دراین‌حالت، شبکه کارایی خودرا ازدست می‌دهد و بسیار کند می‌شود و در بعضی مواقع شبکه از کار می‌افتد. راه‌حلی که برای رفع این مشکل

NetworkBooks.ir

پیشنهاد شده است استفاده از Domain بوده که باعث می‌شود تا کارآیی شبکه تا حد زیادی افزایش یابد.

درحالت کلی توصیه می‌شود تا در شبکه‌هایی که بیش از 20 کامپیوتر وجود دارد، از Domain بجای Workgroup استفاده شود تا بتوان بار ترافیکی که پروتکل NetBIOS به شبکه تحمیل می‌کند را کاملاً حذف کرد. البته تکنیک‌های دیگری برای کاهش Broadcastهای تولید شده توسط پروتکل NetBIOS در شبکه مانند پیاده‌سازی سرور WINS وجود دارد.

دامین Domain

همان‌گونه که گفته شد در هنگامی که از حالت Workgroup استفاده می‌شود تعداد کاربران محدود است اما در هنگام استفاده از Domain هیچ‌گونه محدودیتی وجود ندارد. درواقع در هنگام استفاده از Domain یک سرور به‌صورت اختصاصی تعیین می‌شود تا در آن کلیه نام‌های کاربری و اشیا تعریف و ثبت شود. در این حالت کلیه اشیاء موجود در شبکه وابسته به سرور خواهند بود چراکه تمامی اطلاعات اشیاء در سرور ذخیره می‌شود. باتوجه به این‌که کلیه اطلاعات کاربران در سرور مرکزی نگهداری می‌شود پس درنتیجه دریک سازمان، کاربر محدودبه استفاده از یک کامپیوتر نبوده و می‌تواند با نام‌کاربری خودش ازهر کامپیوتری وارد شده و به امور خود بپردازد. از آنجایی‌که تمامی امور توسط سرور انجام می‌گیرد، مشکل Broadcast درشبکه حل شده و بار اضافی به شبکه تحمیل نخواهد شد. استفاده ازاین روش دارای مزایای خاصی بوده که در ادامه به بررسی آن‌ها خواهیم پرداخت.

مزیت‌های Domain

- هرکاربر که در سرور Domain معتبر باشد، می‌تواند ازپشت هرکامپیوتر عضو دامنه به سیستم وارد شده و به سرویس‌های موردنیاز خود دسترسی داشته باشد.
- به‌دلیل وجود مدیریت متمرکز امنیت تامین شده بیشتر خواهد بود.
- به‌دلیل وجود سرور DNS دیگر خبری از ترافیک‌های Broadcast که ناشی از NetBIOS می‌باشد نبوده و مشکل عدم کارایی و کندی سرعت شبکه حل‌شده است.
- استفاده از ساختار نام‌گذاری سلسله مراتبی که به آن FQDN یا Fully Qualify Domain Name گفته می‌شود.

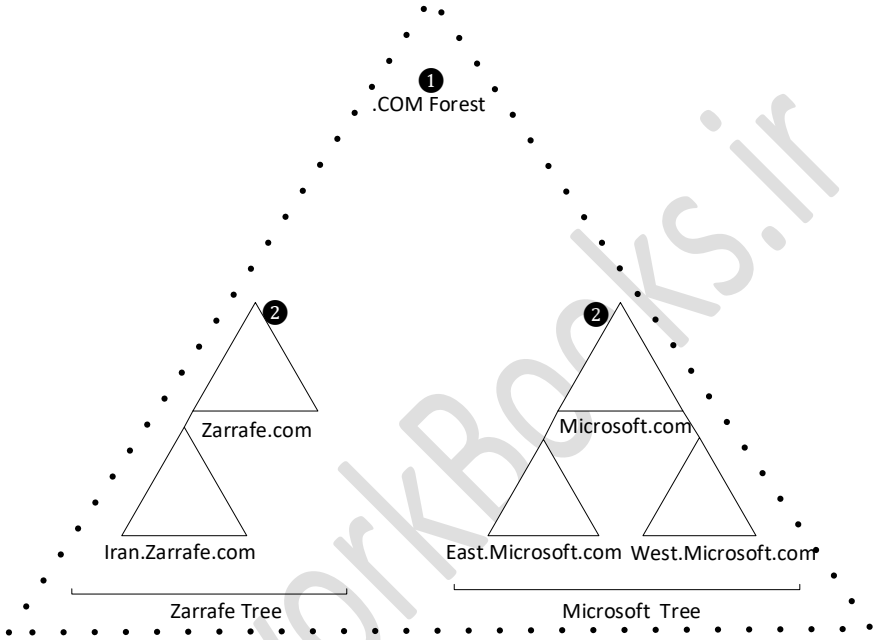
ساختار سلسله‌مراتبی در دامنه

درواقع ماهیت اصلی Active Directory سلسله مراتبی بودن آن در پیاده‌سازی است، به‌این صورت که در بالاترین سطح از ساختار سلسله‌مراتبی Forest وجود دارد و در داخل یک Forest می‌تواند

NetworkBooks.ir

یک یا چند Domain وجود داشته باشد که هرکدام از Domainها شامل یک‌سری بخش‌های کوچکتر بانام OU (Organization Unit) است که اشیا موجود در شبکه در این OUها قرار خواهند گرفت.

برای درک بهتر مفاهیم Forest، Domain بهتر است تا به شکل 3- 1 کنید:



شکل 3- 1

❶ **Forest**: اولین شئ که در هنگام پیاده‌سازی Active Directory می‌بایستی ایجاد شود Forest بوده و در برگیرنده سایر اشیاء خواهد بود. به‌عنوان مثال در یک Forest بانام COM. وجود دارد.

در Forest مفهومی به‌نام Schema وجود دارد که در آن اطلاعات مربوط به اشیاء و ویژگی‌های اشیاء ذخیره می‌شود.

☑ **ویژگی (Attribute)**: هر شئ در Active Directory دارای یک‌سری ویژگی است. به‌عنوان‌مثال شئ کاربر شامل نام، نام‌خانوادگی، آدرس ایمیل و... می‌باشد.

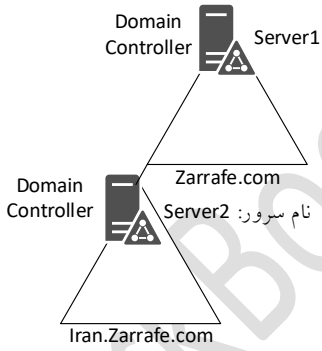
❷ **Domain**: دامنه یک شئ بوده که تحت Forest ایجاد می‌شود و درواقع یک ساختار جامع در شبکه است که تمامی نام‌های کاربری، کامپیوترها، پرینترها و سایر سیستم‌های تحت شبکه را به‌صورت متمرکز مدیریت می‌کند. باتوجه به شکل 3- 1دو دامنه با نام‌های Zarrafe.com و Microsoft.com وجود دارد که در Forestی با نام COM. قرار دارند. توجه داشته باشید در هر دامنه می‌توان یک یا چند زیر دامنه ایجاد کرد که مطابق با شکل 3- 1 در دامنه Zarrafe.com یک

NetworkBooks.ir

زیردامنه و در دامنه Microsoft.com دو زیردامنه وجود دارد.

به هر دامنه اصطلاحاً یک درخت گفته می‌شود. به‌عنوان‌مثال در شکل 3-1 دو درخت با نام‌های Zarrafe.com و Microsoft.com وجود دارد که در راس هردرخت ریشه دامنه یا اصطلاحاً Root Domain قرار دارد.

هر دامنه و هر زیردامنه‌ای که ایجاد می‌شود باید دارای یک کنترل کننده باشد به‌این معنی‌که هر دامنه باید برروی یک سرور پیاده‌سازی و نصب گردد. به‌عنوان‌مثال به شکل 3- 2 توجه کنید که دامنه Zarrafe.com و زیردامنه Iran.Zarrafe.com هرکدام دارای یک کنترل‌کننده یا Domain Controller هستند.



شکل 3- 2

تا اینجا با مفاهیم پایه و ابتدایی از ADDS تا حدودی آشنا شدید. بهتراست قبل‌از پرداختن به جنبه‌های پیاده‌سازی این Role و بررسی بیشتر جزئیات، با چند مفهموم که در ADDS کارآیی دارد آشنا شوید.

آشنایی با سطوح عملیاتی در Forest و Domain

با پیشرفت ویندوزسرور یک‌سری ویژگی و قابلیت‌های جدیدی به ADDS اضافه شده‌است. به‌عنوان مثال در ویندوزسرور2016 قابلیت‌های جدیدی به ADDS اضافه شده است که ویندوزسرور2003 از پشتیبانی آن‌ها عاجز می‌باشد. به‌همین دلیل شرکت مایکروسافت به‌ازاء هر ویندوزسرور یک سطح‌عملیاتی تعریف کرده‌است تا بتواند بین نسل‌های متفاوت سازگاری به‌جود آورد.

در ویندوزسرور سطوح عملیاتی که پشتیبانی می‌شود در زیر نوشته شده است.

NetworkBooks.ir

سطوح پشتیبانی شده در ویندوزسرور2016:

- Windows Server 2016
- Windows Server 2012
- Windows Server 2008
- Windows Server 2003

سطوح پشتیبانی شده در ویندوزسرور2012:

- Windows Server 2012
- Windows Server 2008
- Windows Server 2003

سطوح پشتیبانی شده در ویندوزسرور2008:

- Windows Server 2008
- Windows Server 2003

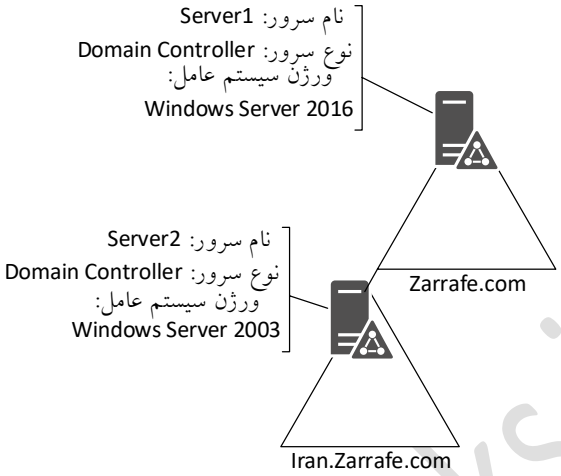
سطوح پشتیبانی شده در ویندوزسرور2003:

- Windows Server 2003

سطح عملیاتی دامنه (Domain Functional Domain)

همان‌گونه که گفته شد هردامنه می‌تواند دارای یک یا چند زیردامنه باشد. سرورهایی که برروی آن‌ها دامنه و یا زیردامنه نصب و پیاده‌سازی می‌شود ممکن است نسخه‌های متفاوتی از ویندوزسرور برروی آن‌ها نصب شده باشد. به‌همین دلیل باید برای عملکرد صحیح دامنه و زیردامنه‌ها سطوح عملیاتی یکسانی را انتخاب کرد. برای درک بهتر این موضوع به شکل 3-3 توجه کنید. دامنه‌ای با نام Zarrafe.com و زیردامنه‌ای با نام Iran.zarrafe.com وجود دارد که به‌ترتیب برروی Server1 و Server2 نصب شده‌اند. برای این‌که هردو سرور بتوانند در دامنه به‌درستی با یکدیگر ارتباط برقرار کنند بایستی در یک سطح عملیاتی قرار گیرند. حال باتوجه به شرایط موجود هردو سرور باید در سطح عملیاتی Windows Server 2003 قرار گیرند.

NetworkBooks.ir



شکل3- 3

به‌صورت پیش‌فرض در زمان نصب و راه‌اندازی ADDS در ویندوزسرور2016، اگر سطح عملیاتی دامنه برروی 2003 تنظیم شود، دامین تنها از ویژگی‌های 2003 پشتیبانی خواهد کرد.

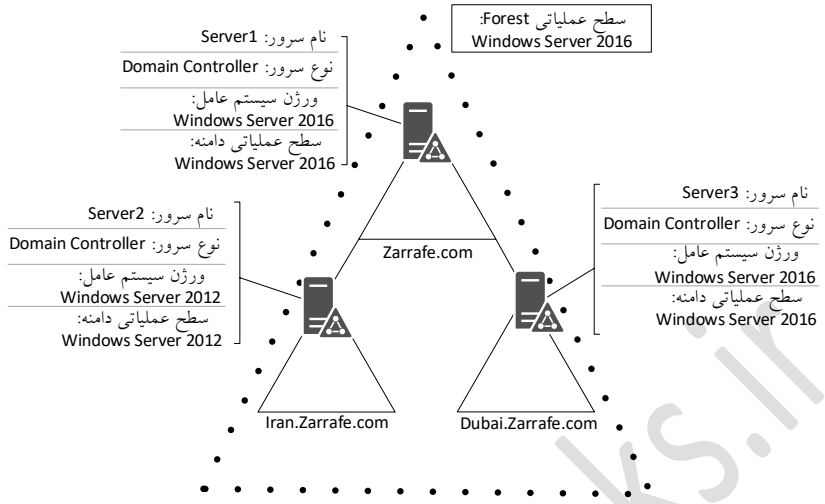
سطح عملیاتی Forest

باتوجه به مطالب گفته شده در Forest چندین دامنه را می‌توان تعریف کرد. سطح عملیاتی Forest توسط اولین DC درون اولین دامنه مشخص می‌شود. برای درک بهتر این موضوع به مثال زیر توجه کنید.

مثال:

در شکل3- 4 دامنه‌ای بانام Zarrafe.com در Forestی بانام com. ایجاد شده است. در دامنه Zarrafe.com دو زیردامنه با نام‌های Iran.Zarrafe.com و Dubai.Zarrafe.com وجود دارد. سطح عملیاتی Forest توسط Domain Controllerی که درون Zarrafe.com قرار دارد تعیین می‌شود چراکه اولین دامنه‌ای است که باعث ایجاد Forest می‌شود پس‌درنتیجه باتوجه‌به شکل3- 4 سطح عملیاتی Forest برابر با ۲۰16 تنظیم خواهد شد. هنگامی که سطح عملیاتی Forest مشخص شد تمامی دامنه و زیردامنه‌هایی که در Forest قرار می‌گیرند، باید در سطح-عملیاتی مشابه و یا کمتر نصب شوند. به‌عنوان مثال باتوجه به مثال گفته شده، دیگر نمی‌توان دامنه‌ای با سطح عملیاتی بالاتر از 2016 نصب کرد.

NetworkBooks.ir



شکل 3- 4

طراحی و پیاده‌سازی Domain

در هنگام پیاده‌سازی اولین دامنه (Domain) به موارد زیر توجه نمایید:

- آیا دامنه‌ای از قبل در سازمان وجود دارد؟
- نام دامنه چه چیزی باشد؟
- چه تعداد دامنه نیاز است؟
- آیا سرورDNS در دامنه وجود دارد؟
- سطح عملیاتی دامنه چه خواهد بود؟
- آیا سرورDNS دیگری در سطح شبکه وجود دارد؟

ارتقا ADDS از ویندوز2012 به 2016

ویژگی‌ها و Attributeهای ویندوزسرور2016 به‌نسبت ویندوزسرور2012 دارای یک‌سری افزایش یافته است . بنابراین قبل از ارتقا ویندوز سرور2012 به نسخه سرور2016 باید این Attributeها را یکسان‌سازی کنید و برای انجام این‌کار از دستور Adprep استفاده می‌شود.

زمانی که نیاز باشد تا یک DC با سطح عملیاتی Windows Server 2016 به Forestای با سطح-عملیاتی پایین‌تر اضافه شود باید ابتدا دستور Adperep /Forestprep را اجرا نمایید.

برای اضافه‌کردن DC به دامنه‌ای با سطح‌عملیاتی پایین‌تر نیاز است تا از دستور Adprep /Domainprep استفاده شود.

NetworkBooks.ir

جهت اضافه‌کردن RODC به Forestی با سطح‌عملیاتی پایین‌تر نیاز است تا از دستور Adprep/Rodcprep استفاده شود.

☑ توجه داشته باشید که دستور Adprep در طول نصب AD در ویندوزسرور2016 به‌صورت خودکار اجرا می‌گردد.

تا به‌اینجای کار مفاهیم تئوری مرتبط به ADDS را مورد بررسی قرار دادیم. حال بهتر است تا در اولین قدم از بخش عملی این Role را نصب و پیاده‌سازی کنید.

تمرین 3-1

عنوان: پیاده‌سازی ADDS در شبکه‌ای با تعداد 300 کامپیوتر

شرح: دراین تمرین قصد برآن است تا سرویس ADDS را برروی سرور نصب کرده و یک کامپیوتر را به دامنه Join کنید. در ادامه چندین نام‌کاربری به AD اضافه کرده و به دامنه Logon کنید.

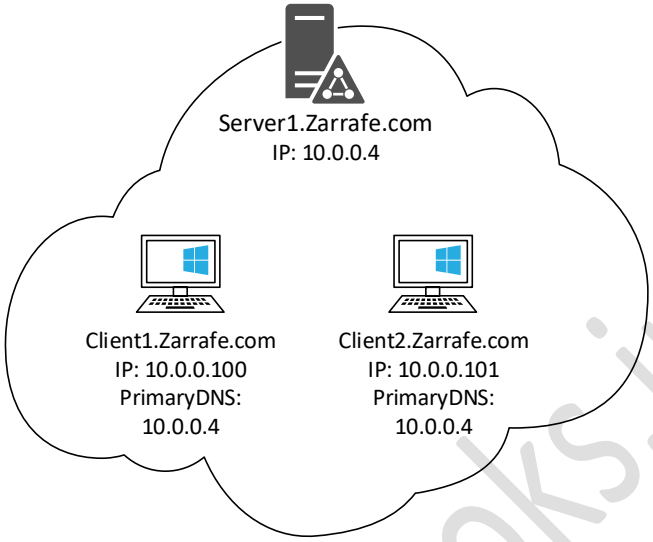
اهداف:

- آشنایی با نحوه نصب و پیکربندی ADDS
- آشنایی با نحوه Join کردن کلاینت به دامنه
- آشنایی با نحوه ساخت نام‌کاربری در ADDS
- نحوه وارد شدن به دامنه با استفاده از نام‌کاربری

تجهیزات و پیش‌نیازها:

- یک ویندوزسرور 2016 با آدرس IP: 10.0.0.4
- یک یا چند کلاینت ویندوز 8 با آدرس IP: 10.0.0.100 و آدرس PrimaryDNS: 10.0.0.4

NetworkBooks.ir



شکل 3-5

مراحل تمرین:

گام 1 نصب سرویسAD و Promoteکردن آن

گام2 عضو کردن کامپیوترهای کلاینت در دامنه (یا همان سرور AD)

گام3 ایجاد چند کاربر درون سرورAD

گام4 وارد شدن از طریق یکی از کاربران به کامپیوترهای کلاینت

گام 1 نصب سرویس AD و Promoteکردن آن

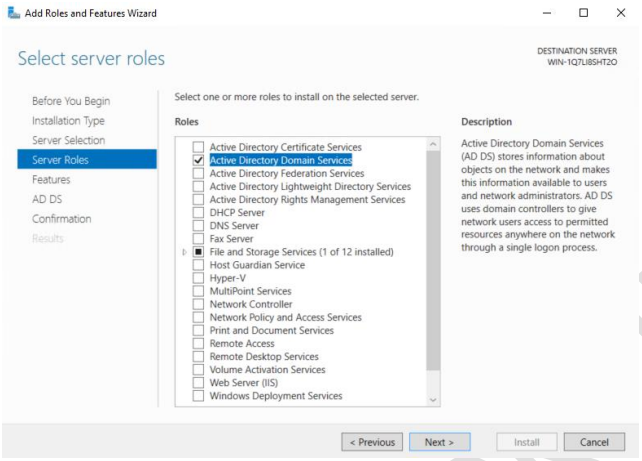
در اولین قدم به‌منظور نصب و راه‌اندازی AD، نصب Role و در ادامه Promote کردن سرور است. Promote کردن سرور عملیاتی است که بعد از نصب Role صورت پذیرفته و سرور را آماده به سرویس‌دهی می‌کند.

برای نصب Role مراحل زیر را انجام دهید.

1. Server Manager را بازکرده و برروی Add Roles and Features کلیک کنید.
2. در صفحه Before you begin برروی Next کلیک کنید.
3. در صفحه Select Installation Type دکمه رادیویی Role-Based را انتخاب کرده و برروی Next کلیک کنید.
4. در صفحه Select Destination Server دکمه رادیویی Local Machine را انتخاب کنید.

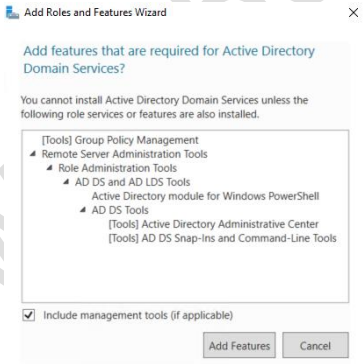
NetworkBooks.ir

5. در صفحه Select Server Roles گزینه Active Directory Domain Services را انتخاب کنید.



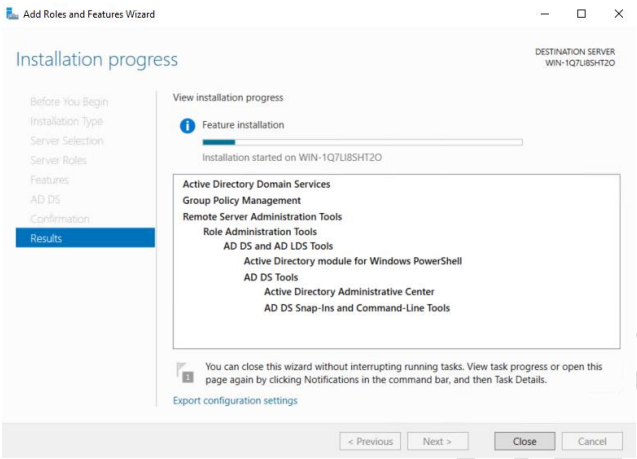
شکل 3-6

6. بعد از انتخاب این گزینه یک پنجره محاوره‌ای مبنی‌بر نصب Featureهای پیش‌نیاز که موردنیاز AD است درخواست می‌شود. برروی دکمه Add Features کلیک کنید.



شکل 3-7

7. برروی Next کلیک کنید.
8. در صفحه Select Features موارد پیش‌فرض را تغییر ندهید و برروی Next کلیک کنید.
9. در صفحه Information برروی دکمه Next کلیک کنید.
10. در صفحه Confirmation Installation برروی دکمه Install کلیک کنید.
11. صفحه Installation Screen مراحل نصب نمایش داده می‌شود.



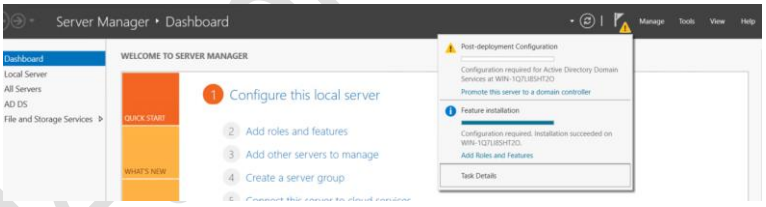
شکل 3-8

12. بعد از کامل شدن نصب برروی دکمه Close کلیک کنید.

13. Server Manager را بسته و سرور را Restart کنید.

14. بعد از Restart شدن با نام کاربری Administrator وارد شوید تا Server Manager به‌صورت اتوماتیک باز شود.

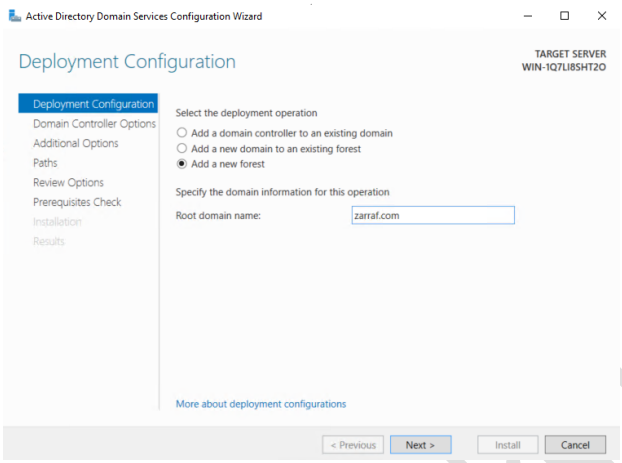
15. در قسمت Notification برروی لینک Promote this Server to Domain Controller کلیک کنید.



شکل 3-9

16. در این مرحله تنظیمات Domain Controller را انجام خواهید داد. قصد شما ایجاد یک Domain Controller برروی یک دامنه جدید و دریک Forest جدید است. در صفحه Deployment Configuration دکمه رادیویی Add a New Forest را انتخاب کنید. حال نیاز به واردکردن Root Domain Name است که ما در اینجا Zarrafe.com را وارد کردیم. برروی Next کلیک کنید.

NetworkBooks.ir



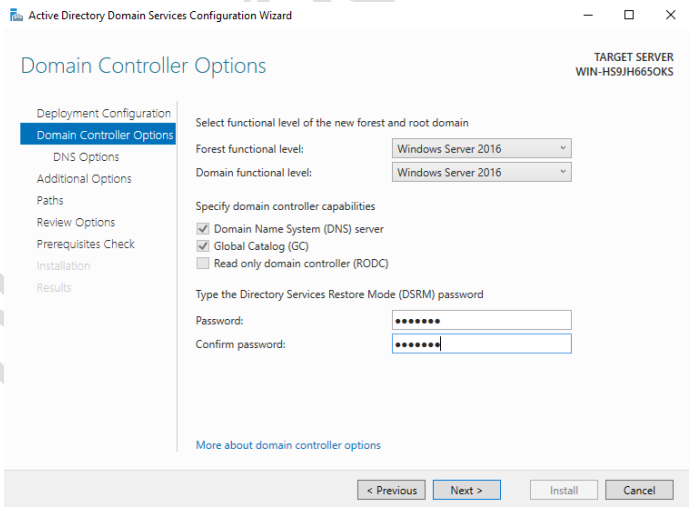
شکل 3- 10

17. در صفحه Domain Controller Options گزینه‌های زیر را تنظیم کنید.

– از دو قسمت Function Level گزینه Windows server 2016 انتخاب کنید.

– مطمئن شوید که گزینه‌های DNS و Global Catalog انتخاب شده باشند.

– دراین قسمت یک رمزعبور پیچیده درنظر گرفته (به‌عنوان مثال123@qwe)و سپس برروی Next کلیک کنید.



شکل 3- 11

18. در پنجره DNS Options برروی Next کلیک کنید.

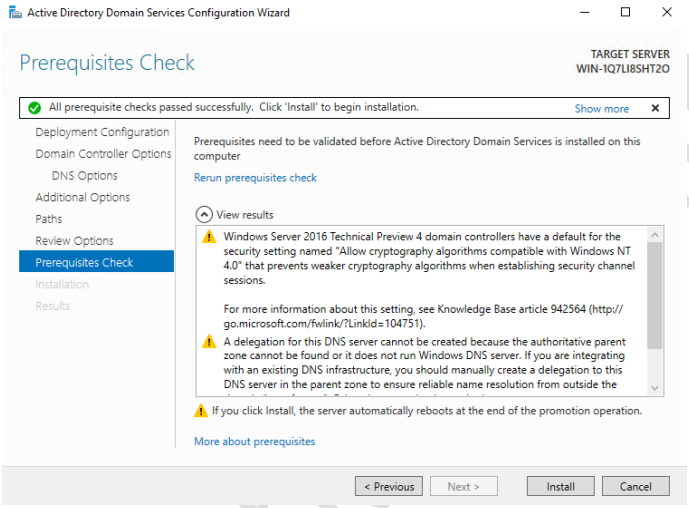
19. در پنجره Additional Options موارد پیش‌فرض NetBIOS Domain Name را پذیرفته و

برروی Next کلیک کنید.

20. در پنجره Paths مسیرهای پیش‌فرض را پذیرفته‌و برروی Next کلیک کنید.

21. در پنجره Review Options تنظیمات صورت گرفته را بررسی کرده و بـرروی Next کلیـک کنید.

22. در پنجره Prerequisites Check برروی دکمه Install کلیک کنید.

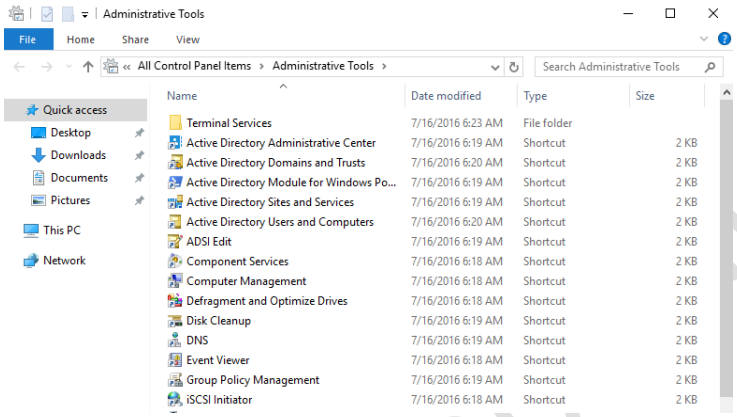


شکل 3- 12

23. بعداز اتمام مراحل نصب، سیسـتم بـه‌صـورت اتوماتیـک Reboot شـده و بـا نـام‌کـاربری Administrator وارد شوید.

شکل 3- 13

24. Server Manager را ببندید.
25. برروی منو Start کلیک کرده و Administrative Tools را انتخاب کنید.
26. حال باید موارد مربوط به Active Directory که در اینجا اضافه‌شده است را ببندید.



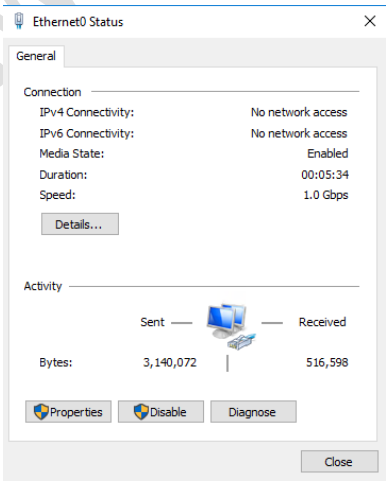
شکل 3- 14

27. پنجره Administrative Tools را ببندید.

گام2 Joinکردن یک کامپیوتر به AD (عضویت یک کامپیوتر در دامنه)

در قدم اول برای Joinکردن کامپیوتر به‌دامنه، ابتدا باید تنظیمات آدرسIP را برروی کلاینت انجام دهید.

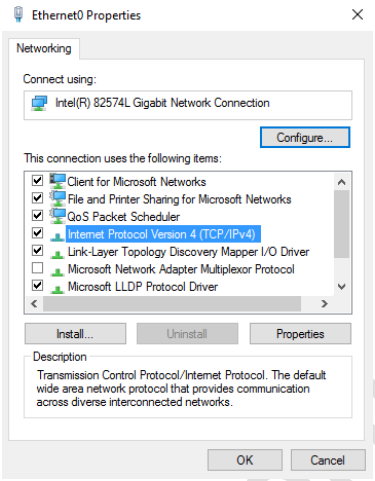
1. به Control Panel رفته و Network Sharing Center را اجرا کنید.
2. برروی نام کارت شبکه کلیک کرده تا قسمت تنظیمات مربوطه باز شود.



شکل 3- 15

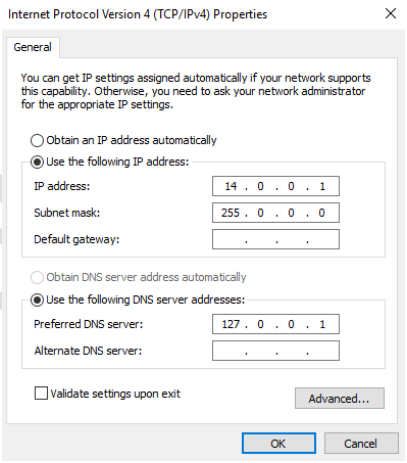
NetworkBook

3. برروی Properties کلیک کرده و در پنجره بازشده بـرروی Internet Protocol 4 دوبـارکلیـک کنید.



شکل 3-16

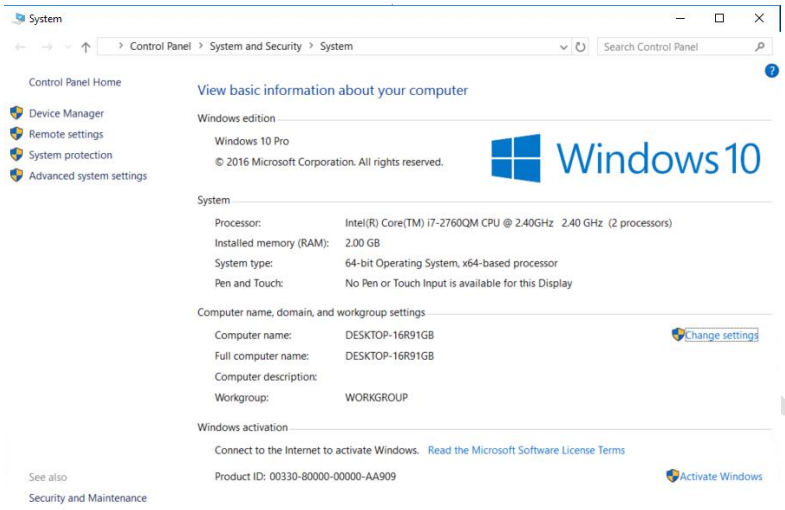
4. در پنجره بازشده تنظیمات را مطابق‌با شکل انجام داده و برروی OK کلیک کنید.



شکل 3-17

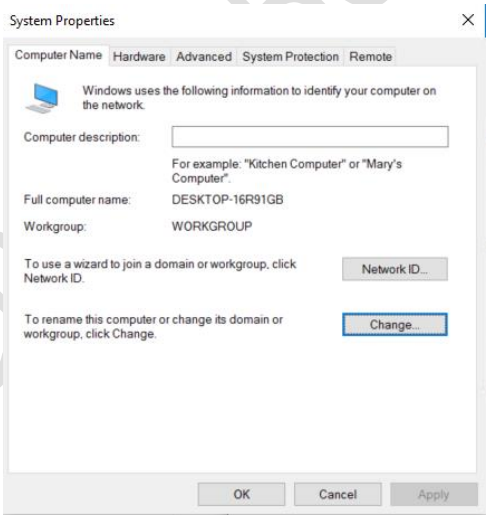
5. در کامپیوتر کلاینت که دارای ویندوز۷ یـا ۸ و یـا 10 اسـت بـرروی آیکـن My Computer راست‌کلیک کرده و Properties را انتخاب کنید.

6. در پنجره System برروی لینک Change Setting در قسمت Computer Name کلیک کنید.



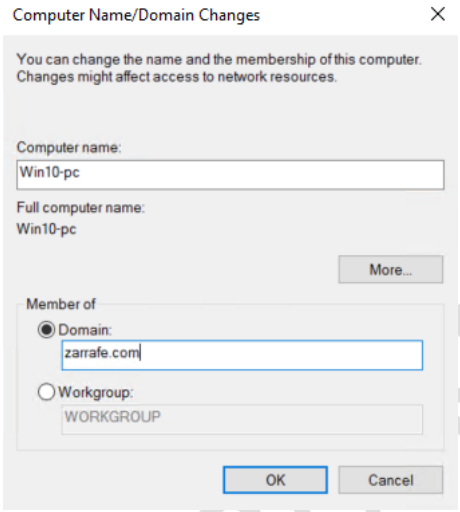
شکل 3- 18

7. بـرروی دکمـه Change کـه در کنـار To Rename This Computer or Change This Domain or Workgroup قرار دارد، کلیک کنید.



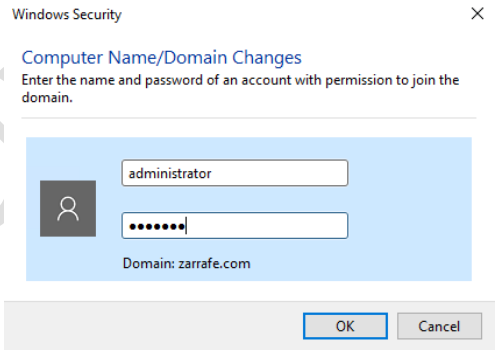
شکل 3- 19

8. در بخش Member of گزینه Domain را انتخاب کنید و نام دامنه zarrafe.com را وارد نمایید و برروی OK کلیک نمایید.



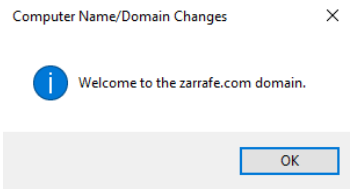
شکل 3- 20

9. در ادامه پنجره‌ای بازشده که نام‌کاربر و رمزعبور مدیر دامنه را درخواست می‌کند. نام‌کاربری و رمزعبور مدیر دامنه (نام‌کاربری: Administrator و رمزعبور: 123@qwe) را وارد کرده و سپس برروی دکمه OK کلیک کنید.



شکل 3- 21

10. درصورتی‌که با موفقیت به دامنه وصل شدید یک پنجره محاوره‌ای به شما پیام خوش‌آمدگویی خواهد داد.



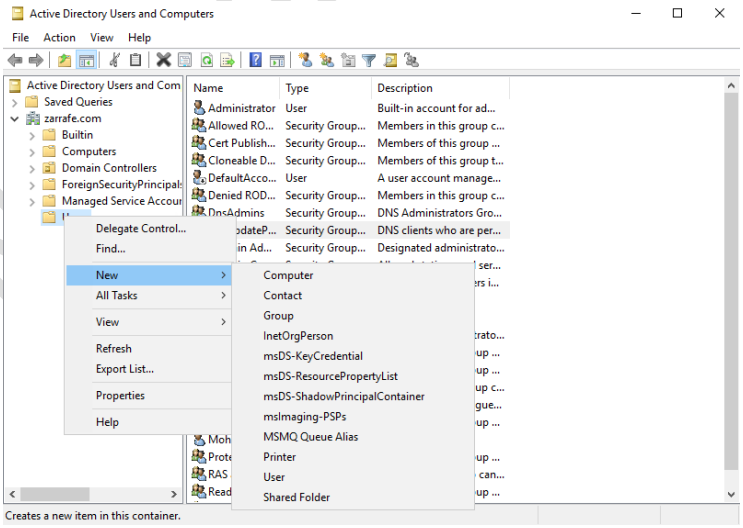
شکل 3- 22

11. درنهایت پیامی مبنی‌بر Rebootکردن سیستم جهت اعمال تغییرات به شما نشان داده خواهد شد، برروی Restart Now کلیک کنید.

گام3 ایجاد چند کاربر درون سرور AD

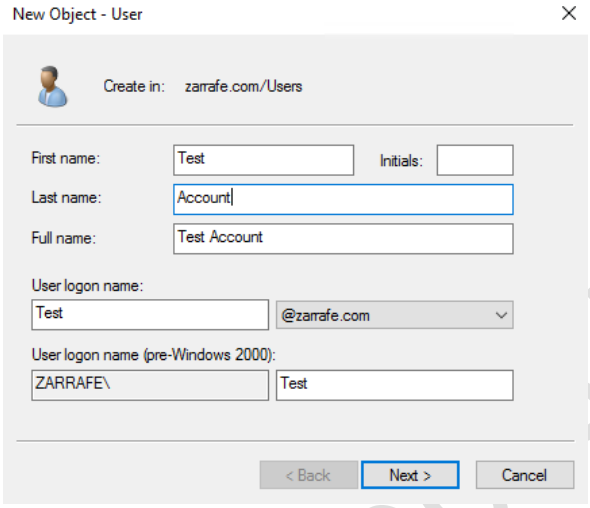
وارد سرور AD شوید و از Administrative Tools کنسول Active Directory Users and Computers (ADUC) را اجرا کنید.

1. از Administrative Tools کنسول مدیریتی ADUC را باز کنید.
2. در قسمت سمت چپ زیر شاخه Zarrafe.com را باز کنید.
3. برروی User راست‌کلیک و گزینه New و سپس User را انتخاب کنید.



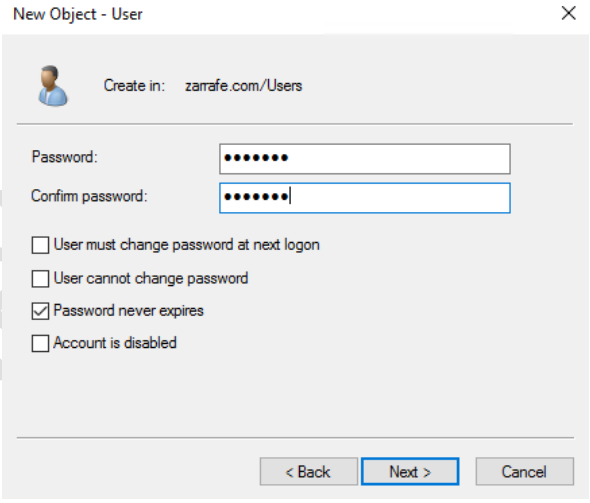
شکل 3- 23

4. مطابق با شکل 3- 24 اطلاعات را وارد کرده و برروی Next کلیک کنید.



شکل 3- 24

5. در قسمت بعد رمزعبور را وارد کرده و مطابق با عکس گزینه‌های مربوطه را تنظیم کنید.

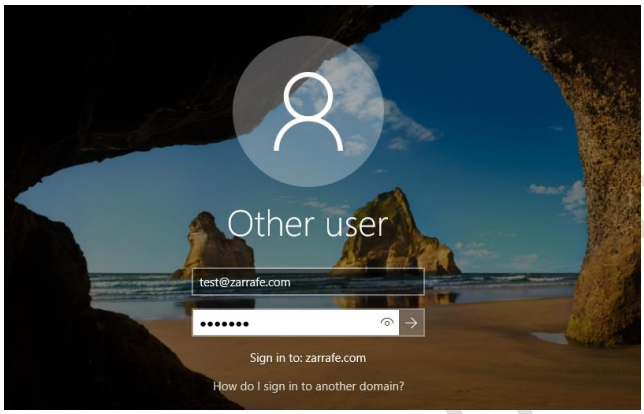


شکل 3- 25

5. در قسمت بعد برروی Finish کلیک کرده تا فرآیند ایجاد کاربر خاتمه یابد.

گام4 وارد شدن از طریق یکی از کاربران به کامپیوترهای کلاینت

حال که یک کامپیوتر را به دامنه Join کردید و نام‌کاربری را ایجاد کردید، از کامپیوتر کلاینت Logoff کرده و در صفحه Logon مطابق با شکل3- 26 نام‌کاربری و رمزعبور را وارد کنید.



شکل3- 26

استفاده از ابزارهای مدیریت Active Directory

بعد از نصب AD چندین ابزار در قسمت Administrative Tools اضافه خواهد شد که شامل:

- **Active Directory Administrative Center**: این قسمت به شما امکان انجام امور مربوط به Active Directory را از یک نقطه مرکزی می‌دهد. مواردی که دراین قسمت وجود دارد شامل:
  - Resetکردن رمزعبور کاربران
  - ساخت یا مدیریت حساب‌های کاربری
  - ساخت یا مدیریت گروه‌ها
  - مدیریت کامپیوترهای شبکه
  - ساخت یا مدیریت Organizational Units و Containers
  - اتصال به یک یا چندین دامنه
  - فیلتر کردن داده‌های Active directory
- **Active Directory Domain and Trust**: از این کنسول به‌منظور کنترل ارتباطات (Trust) بین دامنه‌ها، مشخص‌کردن سطوح عملیاتی Domain و Forest و تعیین UPN استفاده می‌شود.
- **Active Directory Sites and Services**: با استفاده از این کنسول می‌توان محدوده توزیع داده-های مربوط به AD در سطح Forest را مشخص کرد.

NetworkBook.ir

- **Active Directory User and Computers**: جهت مدیریت کامپیوترها و کاربران در محیط AD استفاده می‌شود.
- **Active Directory Module for Windows PowerShell**: مجموعه‌ای از دستورات برای مدیریت AD با استفاده از Power Shell است.

نحوه نصب AD در حالت Server Core

در ادامه به نحوه نصب AD برروی Server Core خواهیم پرداخت که برای‌این منظور بهتر است تمرین زیر را انجام دهید.

تمرین 3–2

عنوان: نحوه نصب AD برروی Server Core

شرح: در این تمرین قصد برآن است تا بتوان ADDS را برروی ویندوز Server Core نصب کنید. از آنجایی که حالت Server Core در برخی موارد استفاده می‌شود انجام این تمرین خارج از لطف نیست.

اهداف:

- تغییر نام سرور در Power Shell
- تغییر زمان در Power Shell
- تغییر رمزعبور مربوط به کاربر Administrator در Power Shell
- تغییر تنظیمات آدرس IP در Power Shell
- نصب ADDS در Power Shell

تجهیزات و پیش‌نیازها:

- ویندوزسرور 2016 با حالت نصب Server Core

مراحل تمرین:

گام 1 تنظیمات ساعت و اختصاص IP به سرور

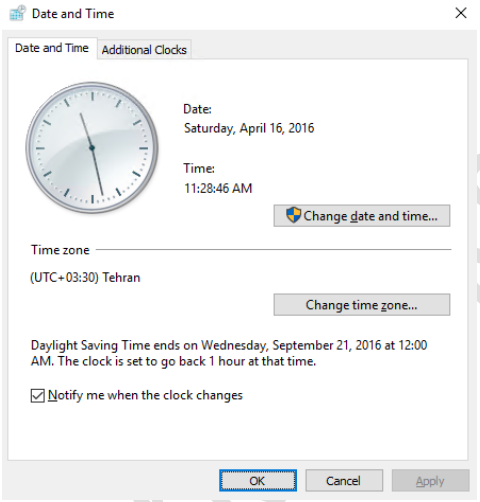
گام2 تنظیم رمزعبور روی سرور و تغییر نام سرور

گام3 نصب DNS و AD روی سرور

NetworkBooks.ir

گام 1 تنظیمات ساعت و اختصاص IP به سرور

1. در Command Prompt عبارت cd\windows\system32 را وارد کرده و دکمه Enter را فشار دهید.
2. timedate.cpl را تایپ کرده و تنظیمات مربوط به تاریخ، منطقه زمانی و زمان را انجام دهید، برروی OK کلیک کنید.



شکل 3-27

3. Netsh را تایپ کرده و دکمه Enter را فشار دهید.
4. Interface را نوشته و دکمه Enter را فشار دهید.
5. IPv4 را نوشته و دکمه Enter را فشار دهید.
6. برای دیدن آدرس IP و کارت شبکه‌ای که آدرس IP به آن اختصاص داده‌شده است، عبارت Show IP را نوشته و دکمه Enter را فشار دهید.

همان‌گونه که در خروجی دستور Show IP مشاهده می‌کنید، اینترفیس Ethernet0 با شماره 7 شناخته‌می‌شود. بنابراین برای اعمال تغییرات روی این اینترفیس باید در دستور مرحله بعد از شماره اینترفیس استفاده کنید.

شکل 3- 28

Set address name = "7" source=static address=10.0.0.1 mask=255.0.0.0 gateway=10.0.0.10

شکل 3- 29

در اینجا از آدرس 10.0.0.x استفاده کرده‌ایم، حال شما می‌توانید بسته به تنظیمات محلی خودتان Address، Mask و Gateway را تغییر دهید.

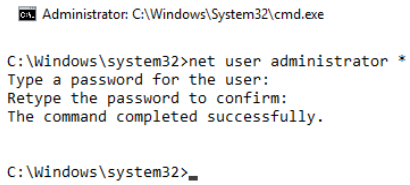
7. با استفاده از دستور Show IP می‌توانید تنظیمات صورت گرفته را مشاهده کنید.

8. Exit را وارد کرده و Enter را فشار دهید.

گام2 تنظیم رمزعبور برروی سرور و تغییر نام سرور

1. دستور Net User Administrator * را تایپ‌کرده و دکمه Enter را فشار دهید.

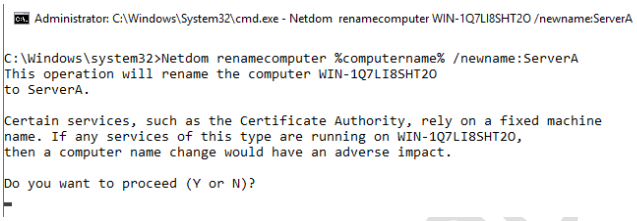
2. رمزعبور خود را وارد کرده و سپس آن را تأیید کنید (در اینجا ما از 123@qwe استفاده کرده‌ایم).



شکل 3- 30

3. برای تغییرنام کامپیوتر دستور زیررا وارد کرده و دکمه Enter را فشار دهید.

Netdom renamecomputer %computername% /newname:ServerA



شکل 3- 31

4. Y را وارد و دکمه Enter را فشار دهید.

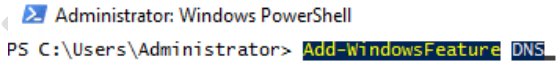
5. با دستور Shutdown /r /t 0 سیستم را Reboot کرده و بعد از بالا آمدن به سیستم وارد شوید.

گام3 نصب DNS و AD روی سرور

1. PowerShell را تایپ کرده و دکمه Enter را فشار دهید.

2. برای نصب DNS در محیط PowerShell دستور زیر را تایپ کرده و دکمه ENTER را فشار دهید.

Add-WindowsFeature DNS

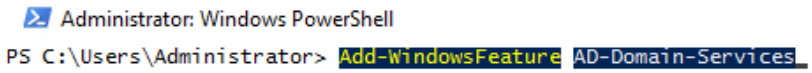


شکل 3- 32

3. در محیط PowerShell دستور زیر را تایپ کرده و دکمه Enter را فشار دهید.

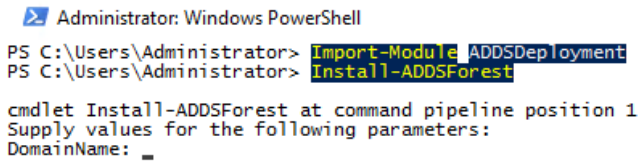
Add-WindowsFeature AD-Domain-Services

به‌وسیله این دستور Role مربوط به Active Directory Domain Service برروی سرور نصب می‌شود.



شکل 3- 33

4. پس از نصب ADDS دراین مرحله باید سرور دامنه را Promote کنید که برای انجام این‌کار در PowerShell دستور Import-Module ADDSDeployment را اجرا کنید و سپس دستور Install-ADDSForest را وارد کنید.



شکل 3- 34

5. نام دامنه خود را وارد کنید و دکمه ENTER را فشار دهید، در این تمرین zarrafe.com را وارد کرده‌ایم.
6. در مرحله بعد از شما رمزعبور Administrator برای حالت Safe Mode درخواست می‌شود.
7. رمزعبور را تایپ کرده و Enter را فشار دهید.
8. را نوشته و دکمه Enter را فشار دهید.
9. AD نصب‌شده و سیستم به‌صورت اتوماتیک Reboot خواهد شد.

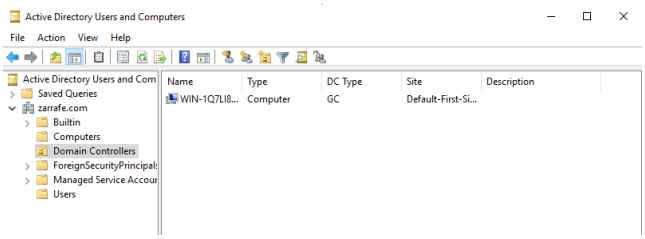
بررسی صحت نصب Active Directory

پس از نصب AD جهت اطمینان از صحت و درستی نصب می‌توانید از روش‌های زیر استفاده کنید:

استفاده از کنسول مدیریتی ADUC

یک روش خوب جهت اطمینان از کارکرد صحیح AD این‌است که از قسمت Administrative tools ابزار ADUC(Active Directory Users and Computers) را اجرا کنید تا محیطی مانند 3-35 باز شود. توجه داشته باشید نامی را که به‌عنوان نام دامنه انتخاب کرده‌اید در سمت چپ پنجره قابل‌مشاهده باشد؛ همچنین با کلیک برروی پوشه Domain Controllers باید نام سرور را در سمت‌راست ببینید و درصورتی‌که این دو مورد قابل‌مشاهده باشد AD بدون مشکل نصب و Promote شده است.

NetworkBooks.ir



شکل 3- 35

تست از طرف کلاینت‌ها

یکی از روش‌های تست AD این‌است که مطمئن شوید کلاینت‌ها می‌توانند منابع به اشتراک گذاشته‌شده را ببینند و از آن‌ها استفاده کنند. در برخی مواقع ممکن است که یکی‌از کلاینت‌ها نتواند به DC دسترسی پیدا کند دراین حالت باید تنظیمات آدرس IP مربوط به کلاینت بررسی شود و مشکل برطرف گردد. درصورتی که هیچ‌کدام از کامپیوترهای کلاینت نتوانند به DC دسترسی پیدا کنند باید در تنظیمات DNS، AD و آدرس‌های IP سرور به‌دنبال مشکل باشید.

اتصال به دامنه

Join شدن به معنی متصل‌کردن یک کلاینت به دامنه جهت بهره‌مندی از سرویس‌ها و مزایای دامنه است.

درصورتی‌که AD به‌درستی نصب و Promote شده باشد سایر سرورها و کلاینت‌ها باید بتوانند به دامنه Join شوند. هنگامی‌که کلاینت‌ها با موفقیت به‌دامنه Join شدند باید قادر به مشاهده منابع AD از طریق My Network Place باشند. با انجام این آزمایش می‌توانید از نحوه کارکرد صحیح Active Directory و اتصالات شبکه‌ای مطمئن شوید.

NetworkBooks.ir