بسم الله الرحمن الرحیم

عنوان تحقیق

Installing From Media (IFM)

Read Only Domain Controller (RODC)

استاد محترم: جناب آقای مهندس منصوری

نگارنده: یوسف رشیدی

جهت درس: MCSA 2016

مجتمع فنی تهران

هدف کلی تحقیق

آشنایی کامل با RODC

اهداف جزئی

۱. علت استفاده از RODC

۲. آشنایی با RODC Cache

۳. امنیت در RODC

۴. آشنایی با گروه Allow و Denied

۵. آشنایی با Authenticate و Authentication در RODC

۶. آشنایی با عملکرد RODC

۷. آشنایی با ویژگیهای RODC

۸. آشنایی با محدودیتها در یک RODC

۹. آشنایی با نصب یک IFM

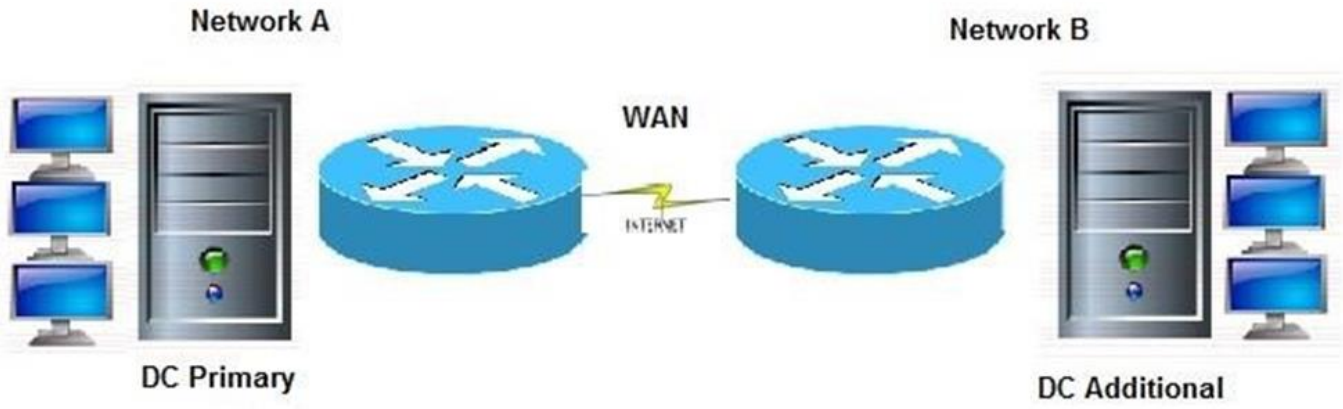
هدف کاربردی

هندل نمودن موضوع RODC و نحوه عملکرد این رول

Microsoft RODC

مقدمه :

شکل زیر را در نظر بگیرید.



ابتدا فرض میکنیم شبکه ی B، admin ندارد، در این صورت:

تمام اطلاعات بین DC ها Replicate می شود. حال اگر کسی بتواند DC Additional را سرقت کند، می تواند به تمامی اطلاعات دست پیدا کند، که این موضوع از نظر امنیتی مشکل ایجاد می کند.

حال فرض می کنیم که شبکهی B، آدمین دارد، اسم یوزر Admin B بوده و عضو گروه Domain users می باشد.

در اینصورت دو وظیفه برای این admin وجود دارد:

۱. رسیدگی به مسائل مربوط به کلاینتهای سایت B

۲. مسائل مربوط به نگهداری DC در سایت B (نصب برنامه، آنتی ویروس و ...)

برای انجام امور مربوط به کلاینتها (مثلا ساخت یوزر، تغییر پسورد و ...)، می توان برای یوزر Admin B، Delegation تعریف کرد. بدین ترتیب که یک OU برای تمامی کاربران سایت B ایجاد می کنیم و بر روی این OU به یوزر Admin B از طریق Delegation حق ساخت یوزر و ریست کردن پسورد می دهیم. برای انجام امور مربوط به نگهداری DC ، چندین راه وجود دارد:

۱. یوزر Admin B را عضو گروه Domain Admins کنیم. در این صورت قدرت خیلی زیادی پیدا می کند و می تواند در تمام کامپیوترهای عضو دامین Login کند که اصلا از لحاظ امنیتی صحیح نیست .پس این راه حل رد می شود.

۲. یوزر Admin B را عضو گروه Administrators در DC Additional کنیم تا فقط بر روی کامپیوتر مربوط به DC Additional دسترسی admin داشته باشد. این راه حل هم از لحاظ امنیتی منطقی و صحیح نیست، زیرا DC ها با هم Replicate می کنند و در اصل یوزر Admin B ، عضو گروه Administrators در DC Primary نیز می شود و می تواند بر روی DC Primary هم Login کند. پس باز هم یوزر قدرت زیادی پیدا می کند .پس این راه حل هم رد میشود.

پس نتیجه میگیریم که بهترین راه، استفاده از DC بصورت RODC باشد. یعنی (Read Only DC) ، چون هر تغییری که در یک DC صورت بگیرد، به علت Replicate در DC دیگر نیز اعمال می شود، پس نمیتوان از گزینه های موجود در Active Directory استفاده کرد.

حال به بررسی مسائل مربوط به این راه حل می پردازیم:

DC به سرقت برود. در این حالت می توانیم تنظیم کنیم که پسوردهای مربوط به یوزرهای مهم و حیاتی در RODC به هیچ وجه Cache نشود. البته دقت شود که به طور پیش فرض هیچ پسوردی در سمت RODC، Cache نمی شود.

زمانی که DC به صورت RODC نصب می شود، دو گروه به Active Directory اضافه می شود.

اگر یوزری در گروه Allow قرار بگیرد، پسوردش در سمت Cache RODC می شود.

اگر یوزری در گروه Denied قرار بگیرد، پسوردش در سمت Cache RODC نمی شود.

علت استفاده از این گروه ها این است که اگر قرار باشد تمام درخواستهای مربوط به Authentication به سمت DC مرکزی ارسال شود، پس انگار در سایت B هیچ DC ای وجود ندارد و در صورت قطعی ارتباط خط WAN دچار مشکل می شویم.

در اینحالت RODC در پشت صحنه، هر از چند گاهی به DC مرکزی مراجعه و پسوردهای یوزرهای موجود در گروه Allow را می پرسد و Cache میکند. با این توضیحات اگر DC دزدیده شود، پسوردهای مربوط به یوزرهای کم اهمیت از دست میرود که از لحاظ امنیتی مشکل زیادی ایجاد نمی کند.

علت استفاده از RODC

اطلاعات مربوط به DC Primary به تمام DC های Additional ارسال میشود و اگر Database مربوط به DC Additional دزدیده شود، باعث لو رفتن یوزر و پسوردهای موجود در Active Directory میشود که از لحاظ امنیتی اصلا مناسب نیست. پس به سمت ایجاد RODC در سایتهای مرتبط با دفتر مرکزی میرویم.

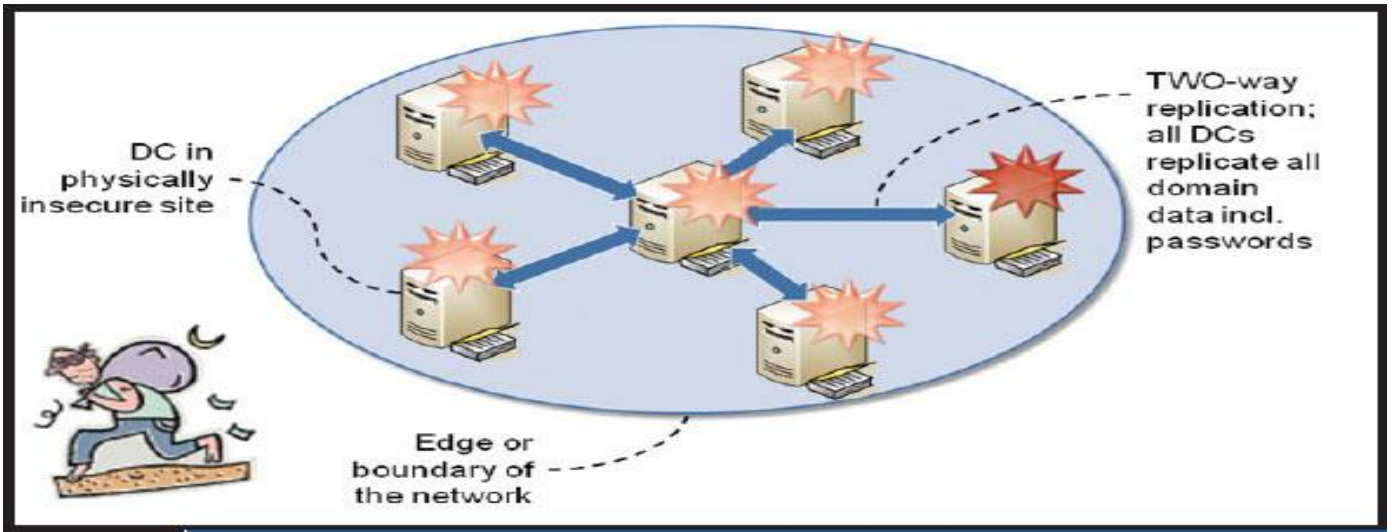


Figure 1: Windows 2000/2003 branch-office DCs can negatively impact the whole AD forest

حتما در خصوص RODC مطالعاتی داشته اید و ممکن است هر کس از شما سئوال بکند بگویید که RODC مخفف کلمه های Read Only Domain Controller یا Domain Controller فقط خواندنی است و معمولا این برداشت می شود که این یک کپی کامل ولی خواندنی از پایگاه داده اکتیودایرکتوری شما است که در سایت های مختلف شبکه خودتان قرار می دهید. طبیعتا زمانیکه صحبت از RODC می شود شما از آن در شعبه ها یا نمایندگی های شرکت یا سازمان خود می خواهید استفاده کنید تا کاربران آن شبکه بتوانند به راحتی به سیستم ها و سرویس های مورد نیاز شبکه Login کنند. اما آیا تا به حال به این موضوع فکر کرده اید که چه فرآیندی بر روی RODC انجام می شود که باعث احراز هویت شدن یا Authenticate شدن کاربران می شود ؟ این خیلی مهم است که در زمان استفاده از RODC درست متوجه بشویم که Authentication چگونه انجام می شود.

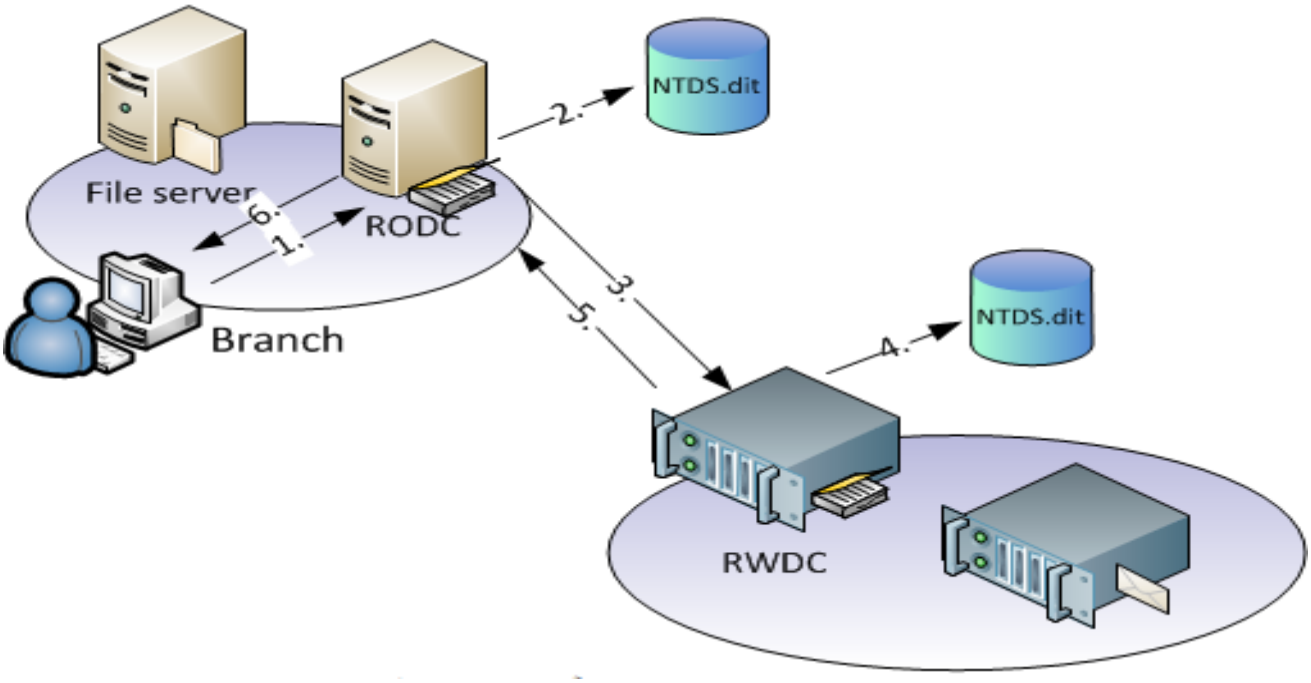
اول از همه یک نکته را در نظر داشته باشید که در RODC هیچ پسوردی بصورت پیشفرض ذخیره نشده است و به همین خاطر نباید نگران به سرقت رفتن اطلاعات موجود در آن باشید ، البته این یک فرضیه است. قبل از هرگونه توضیحی این موضوع را هم فراموش نکنید که تمام نیاز کاربران شما در شعبه ها و نمایندگی های شما فقط Login کردن داخل سیستم نیست و شما باید بدانید که احراز هویت توسط پروتکل Kerberos انجام می شود که پروتکل احراز هویت پیشفرض اکتیودایرکتوری است. در دنیای Kerberos چند قانون اصلی وجود دارد ، مهمترین قانون در Kerberos این است که اگر شما Ticket احراز هویت نداشته باشید ، بنابراین احراز هویت هم نمی شوید و دسترسی ها برای شما باز نخواهند شد.شما از Kerberos برای همه سرویس های دامین استفاده می کنید ، برای انجام برخی کارها حتی کامپیوترها نیز در اکتیودایرکتوری بایستی احراز هویت شوند چه برسد به کاربران ، بنابراین بسیار ضروری و الزامی است که شما سیستم احراز هویتی خودتان را که در دفتر مرکزی دارید در شعبه ها و نمایندگی ها هم داشته باشید و از همه مهمتر شما باید سیستمی داشته باشید که حتی در صورت از بین رفتن لینک و ارتباط بین دفتر اصلی و شعبه یا نمایندگی ، همچنان بتواند احراز هویت کاربران را نیز انجام بدهد.

طبیعی است که شما هیچوقت ریسک قرار دادن کل Domain Controller خودتان به عنوان یک DC خواندنی نوشتنی در شعبه ای که بعضا کارشناس فنی هم ندارد را انجام نمی دهد. در اینجاست که شما از مکانیزمی باید استفاده کنید که ضمن اینکه احراز هویت را بتواند بصورت Offline و از طریق نام کاربری و رمز عبور Cache شده انجام دهد بتواند ریسک امنیتی شما را نیز به حداقل برساند. شما در چنین مواردی از RODC استفاده می کنید.

احراز هویت ماشین ها و کاربران در RODC چگونه انجام می شود ؟

مکانیزم احراز هویت ماشین ها و کاربران در اکتیودایرکتوری تا حدود زیادی شبیه به هم و یکسان است. کلاینت ها از طریق DNS سرور و فرآیند DC Locator متوجه می شود که که سرور RODC ای که در همان سایت وجود دارد عملیات احراز هویت را باید انجام دهد و در اصطلاح فنی تر DC Locator تشخیص می دهد که RODC وظیفه Authoritative Authentication را بر عهده دارد. همانطور که در تصویر زیر مشاهده می کنید در اولین گام کلاینت درخواست احراز هویت خودش را به سمت سرور RODC ارسال می کند. در گام دوم سرور RODC به پایگاه داده خود که فایلی به نام NTDS.DIT است نگاه می کند تا ببیند آیا نام کاربری و رمز عبور کلاینت مورد نظر را بصورت ذخیره شده در پایگاه داده موجود دارد یا خیر ؟ با توجه به اینکه اطلاعات احراز هویت این کلاینت در پایگاه داده فعلی RODC قرار ندارد بنابراین RODC گام سوم را شروع می کند. در مرحله سوم RODC درخواست احراز هویت کلاینت را از طریق لینک شبکه WAN به سمت سرور DC اصلی هدایت می کند و طبیعتا می داند که در آنجا باید اطلاعات در پایگاه داده وجود داشته باشد. در گام چهارم RWDC ما از پایگاه داده خود اطلاعات مربوط به احراز هویت را بررسی می کند و با توجه به اینکه در این قسمت اطلاعات در پایگاه داده وجود دارد در گام پنجم پاسخ را به سمت سرور RODC هدایت می کند که حاکی از صحت اطلاعات درخواستی احراز هویت می باشد. در گام ششم که مرحله بعدی است درخواست کلاینت سرویس دهی شده است و کلاینت می تواند در فایل سرور احراز هویت و Login کند اما طبیعتا از این موضوع خوشحال نیست که چرا خودش احراز هویت را انجام نداده است . برای اینکه مجددا شرمنده کلاینت ها نشود اینبار اطلاعات احراز هویتی کلاینت که کامپیوتر یا کاربر است در پایگاه داده RODC

بصورت Cache شده نگهداری می شود تا در درخواست های احراز هویت بعدی کلاینت به جای سئوال کردن از سرور RWDC از اطلاعات خودش برای احراز هویت استفاده کند. برای اینکار ابتدا RWDC بررسی می کند که آیا Password Replication Policy خودش قابلیت Cache کردن پسوردها به RODC را داده است یا خیر ، اگر این اجازه داده شده بود ، اطلاعات احراز هویت آن کاربر در پایگاه داده RODC از این به بعد وجود خواهد داشت.



RODC چگونه کار می کند؟

خوب تا اینجای کار اگر مجددا کاربر یا کامپیوتر ما درخواست احراز هویت را به سمت RODC بفرستد ، فرآیند احراز هویت حتی با قطع شدن ارتباط شبکه WAN نیز انجام می شود و کاربر قادر به Login خواهد بود. اگر فرآیند Password Replication ای که عنوان کردیم در مرحله قبل انجام نمی شد RODC در صورت بروز مشکل برای لینک شبکه WAN دیگر قادر به احراز هویت نبود و درخواست کلاینت ما بی نتیجه می ماند. در مرحله بعدی می خواهیم در خصوص فرآیند دریافت Ticket و همچنین چگونگی دسترسی به سرویس مورد نظر صحبت کنیم.

مایکروسافت با RODC یک قابلیت دیگر جدید به ویندوز سرور ۲۰۰۸ و یا بهتر بگویم به دومین کنترولر (DC) اضافه کرد. اساس انجام این کار توسط مایکروسافت به خاطر نداشتن یا نبودن امنیت در مکانهایی خارج از دفتر مرکزی بود تا دومین کنترولرها بهتر محافظت شوند. همانطور که میدانیم در اینگونه مکانها امنیت فیزیکی یا خیلی کم است و یا اصلا نیست، همچنین در این مکانها کسانی که دارای دانش فنی کافی باشند، وجود ندارند و اصولا تعدادی یوزر (User) هستند که در حال انجام کار روزانه خود و استفاده از یک خط اینترنت یا WAN می باشند. پس مشاهده میکنیم که این دومین کنترولرها به مانند دومین کنترولرهای واقع در دفتر مرکزی یا سنترال از امنییتهای فیزیکی و دانش فنی برخوردار نیستند .

تا قبل از ویندوز سرور ۲۰۰۸ به خاطر این مشکلات گفته شده تا حد امکان تلاش می شد که در این مکانها دومین کنترولر وجود نداشته باشد و به همین علت یوزرها برای عملیات Authentication از خط WAN که به دومین کنترولر سنترال متصل بود استفاده میکردند و در صورتی که برای این خط WAN مشکلی پیش میامد یوزرها نمی توانستند عمل Authentication انجام داده و به دومین وارد شوند (Logon) و نهایت میتوانستند از قابلیت (cached credentials) استفاده کرده و به صورت لوکال وارد شوند (Logon) که آن هم مشکلی را حل نمیکرد، زیرا به منابعی که در دومین به اشتراک گذاشته شده (Shared Resource) بود دیگر دسترسی نداشتند. دقیقا به همین علت مایکروسافت RODC را وارد صحنه کرد .

ویژگیهای یک دومین کنترولر RODC

یک RODC دارای یک کپی یا المثنی از بانک اطلاعتی اکتیو دایرکتوری (NTDS.DIT) است (همه اشیاء Objects و خواص Attributes)، که همانند آن بر روی یک دومین کنترولر معمولی موجود است. تنها چیزی که در مقایسه بین این دو دومین کنترولر فرق می کند این است که اجازه ندارد این بانک اطلاعتی اکتیو دایرکتوری (NTDS.DIT) را تغییر دهد و فقط اجازه خواندن آن را دارد و تمام تغییرات را دومین کنترولر معمولی از طریق عملیات Replication بر روی آن اعمال میکند .

این قابلیت وجود دارد که روی RODC سرور DNS اینستال شود، ولی باز هم فقط اجازه خواندن دارد. میتواند در خود همه نرم افزارهای پارتیشن دایرکتوری Application Directory Partitions به مانند Domain DNS Zones یا Forest DNS Zones داشته باشد. کامپیوترها می توانند از آن برای پیدا کردن اسم (Name Resolution) استفاده کنند و یوزرهایی که در آن مکان هستند می توانند به صورت نرمال Logon کنند. اما اجازه ندارد که اسامی را به روز رسانی کند (Name Updates) یا اینکه رکورد جدید NS ایجاد کند (منظور خودش به صورت مستقل).

بر روی یک RODC میتوان مشخص کرد که کدام اکانت یوزر، کامپیوتر یا سرویس اجازه ذخیره شدن یا نشدن دارد (credential caching).به صورت استاندارد اکانتهای ادمینها به مانند Domain Administrator در RODC ذخیره نمی شوند. دو گروه دومین امنیت محلی (Domain Local Security Groups) وجود دارد که یکی Denied RODC Password Replication Group و دیگری Allowed RODC Password Replication Group می باشد که برای مدیریت ذخیره سازی اکانتها می باشند. شما همچنین می توانید از گروههایی که خودتان ساختید استفاده کنید. اگر یک یوزر همزمان در هر دو گروه باشد، گروه Denied RODC Password Replication Group حق تقدم دارد. اگر اکانت یک یوزر فقط یکبار ذخیره شود، بار دیگر آن یوزر می تواند حتی با وجود نداشتن ارتباط با دومین کنترولر سنترال Logon کند بدون نیاز به خط .WAN در صورتی که RODC دزدیده شود، فقط در آن اکانتهای ذخیره شده می باشد و اگر اکانت کامپیوتر RODC را از اکتیو دایرکتوری پاک کنیم، به صورت اتوماتیک تمام اکانتهایی که در ذخیره شده بود، ریست (Reset) می شوند تا پسوردهای دزدیده شده غیر قابل استفاده باشند .

عملیات Replication فقط به صورت یک طرفه (One-Way) است. چون RODC اجازه هیچ تغییری به صورت مستقل ندارد بنا بر این دومین کنترولرهای معمولی, احتیاجی به گرفتن اطلاعات در عملیات Replication از RODC ندارند. عملیاتReplication فقط به صورت ورودی (Inbound) هستند و نه به صورت خروجی (Outbound) ، به همین علت سرورهای Bridgehead کمتر می شوند .

میتوان یک یوزر دومین یا گروه دومین (Domain User or Group) را به صورت ادمین برای RODC ایجاد کرد, توسط قابلیت.Delegation در این صورت آن یوزر یا گروه به صورت ادمین لوکال می شوند بدون اینکه مانند ادمینهای دومین اجازه دسترسیهای گوناگون به دومین کنترولهای دیگر یا دومین را داشته باشند. به طور مثال آنها میتوانند Update ها یا Driver ها را اینستال کنند .

به صورت پیش فرض (Default) در یک RODC اطلاعات اکانت یوزر یا کامپیوتر ذخیره نمی شود، به غیر از اکانت کامپیوتر خودش و یک اکانت ویژه krbtgt برای خود RODC. RODC یک مرکز توزیع کلید (Key Distribution Center – KDC) در اکتیو دایرکتوری در آن محل یا سایت (Site) است .RODC از اکانت برای رمزنگاری (encrypted) اعطای بلیط (ticket-granting tickets – TGT) استفاده میکند و این در مقایسه با یک دومین کنترولر معمولی فرق میکند.

این رفتاری که RODC در عملیات Replication یک کپی کامل از Schema دریافت میکند در بعضی از شرایط ممکن است مطلوب نباشد. به طور مثال ممکن است که از یک برنامه استفاده شود که اطلاعات مهمی را در اکتیو دایرکتوری ذخیره میکند و ما نمیخواهیم که این اطلاعات در RODC باشد.برای همین RODC یک انتخاب را عرضه میکند و نامشRead-only partial attribute set – ROPAS می باشد که همچنین به نام (RODC filtered attribute set – ROFAS) نیز معروف است. این فانکشن اجازه میدهد که که مشخص کنیم کدام خواص (attributes) متفاوت به RODC در عملیات Replication ارسال شوند.اگر بخواهیم از این قابلیت ذکر شده استفاده کنیم، باید توجه کنیم که سطح در حال کار جنگل یا کل ساختار (forest functional level) باید روی Windows Server 2003 یا بالاتر باشد .

RODC را میتوان در محل مورد نظر با این نسخه های ویندوز استفاده کرد:

الف- دومین کنترولر ۲۰۰۳/۲۰۰۳R2در همان دومین یا در دومین دیگر

ب- دومین کنترولر۲۰۰۸/۲۰۰۸R2 در همان دومین یا در دومین دیگر

پ- RODC دومین کنترولر ۲۰۰۸/۲۰۰۸R2 در همان دومین یا در دومین دیگر

برای این که بتوان از RODC استفاده کرد، خواص (attributes) زیر به ویندوز ۲۰۰۸ اضافه می شود

ms-DS-Reveal-OnDemand-group

ms-DS-Never-reveal-group

ms-DS-Revealed-list

ms-DS-AuthenticatedTo-account list

چه محدودیتهایی در یک RODC وجود دارد

به علت این که یک RODC فقط میتواند دیتابیس اکتیو دایرکتوری را بخواند، نمیتواند در خود FSMO ها را داشته باشد. به همین منظور برای داشتن FSMO باید دومین کنترولر بتواند روی دیتابیس اکتیو دایرکتوری تغییر ایجاد کند یا بنویسد .

یک RODC نمیتواند سرور Bridgehead باشد. یک سرور Bridgehead مسئولیت عملیات Replication را دارد. این سرور تمام تغییرات در سایت (Site) خود را جمع آوری میکند و با سرورهای Bridgehead دیگر سایتها مبادله میکند که خودش مستلزم عملیات Replication دو طرفه است. ولی همانطور که در بالا فهمیدیم RODC دارای عملیات Replication یکطرفه است .

باید همیشه قبل از اینستال کردن اولین RODC یک دومین کنترولر۲۰۰۸/R۲۰۰۸ در شبکه وجود داشته باشد .

RODC – ها نمیتوانند با هم عملیات Replication را انجام دهند.

سرور اکسچنج (Exchange) روی RODC ساپورت نمی شود .

اگر به هر علتی دومین کنترولر نرمال از از مدار خارج شود و دیگر نتوان آن را وارد کرد و فقط در شبکه RODC باقی مانده باشد، هیچ راهی وجود ندارد که RODC را به یک دومین کنترولر معمولی تبدیل کرد و باید کل دومین خود را از اول درست کنید .در جایی خواندم که گفته شده بود RODC را میتوان به عنوان پشتیبان دومین کنترولر استفاده کرد که این کاملا اشتباه است و همانطور که خواندید، RODC نمیتواند پشتیبان باشد چون نمیتواند FSMO را داشته باشد و نمیتوان آن را تبدیل به دومین

کنترولر معمولی کرد . پس همیشه اگر از RODC استفاده میکنید حداقل ۲ دومین کنترولر معمولی داشته باشید و به صورت منظم از دومین کنترولرها بک آپ بگیرید.

آیا می توان چندین RODC را در یک سایت راه اندازی نمود؟ در صورت مثبت بودن پاسخ، مزایا و معایب انجام این کار چیست؟

در خصوص این سناریو می بایست خدمت علاقمندان عرض کنم که بله، می توان هر تعداد که مایل باشیم در سایت مورد نظر خود RODC راه اندازی کنیم. از مزایای انجام این کار آنست که اگر یکی از RODC ها از دور خارج شود، RODC دیگر می تواند پاسخگوی درخواست کلاینت ها باشد (Fault Tolerance). اما این سناریو معایبی هم دارد که با دانستن آن ممکن است قبل از پیاده سازی این سناریو، کمی بیشتر فکر کنید.

به طور کلی یکی از سناریوهای مفید جهت راه اندازی دامین کنترلرهایی از نوع RODC، استفاده از آنها در Branch Office ها می باشد. معمولا Branch Office ها با سایت های مرکزی، از ارتباط مناسبی برخوردار نبوده و به عبارت دیگر ارتباط میان آنها با سایت مرکزی reliable نمی باشد. در این حالت بکارگیری از چندین RODC در یک سایت (فرض بر آنست که در سایت مورد نظر، دامین کنترلری از نوع Writable وجود ندارد)، باعث بالا رفتن قابل توجه ترافیک خواهد شد. به مثال زیر توجه کنید:

فرض کنید که شبکه سازمان شما از دو سایت به نام های Site1 و Site2 تشکل شده است. Site2 شامل تنها دو RODC به نام های RODC1 و RODC2 می باشد. در Site2 قرار است کاربری به نام User A با استفاده از یک لپتاپ به نام Laptop A به دامین لاگین نماید. همچنین فرض کنید که تنظیمات مرتبط با Password Replication Policy به گونه ای پیکربندی شده است که با اولین لاگین User A از طریق Laptop A، اطلاعات مرتبط با عملیات احراز هویت آنها در هر دو RODC موجود cache گردد. حال با داشتن این مفروضات می خواهیم بدانیم که عملیات لاگین کاربر مورد نظر چه تاثیرات منفی بر روی لینک میان Site1 و Site2 خواهد داشت ، همانطور که می دانید، عملیات لاگین به دامین، ابتدا از Laptop A آغاز شده و در نهایت به کاربر User A ختم می گردد. با توجه به این مطلب و در نظر گرفتن مفروضات فوق، رخدادهای زیر به وقوع می پیوندد:

۱. Laptop A درخواستی مبنی بر آغاز عملیات احراز هویت را به سوی RODC1 گسیل می دارد.

۲. بدان علت که هنوز RODC1 اطلاعات مرتبط با عملیات احراز هویت Laptop A را در خود ذخیره ننموده است، این درخواست از سوی Laptop A به سوی یک دامین کنترلر از نوع writable که در Site1 واقع شده است، از طریق RODC1 ارسال می گردد.

۳. دامین کنترلر مورد نظر در Site1، عملیات احراز هویت کلاینت مذکور را به انجام رسانیده و نتیجه این عملیات را به سوی RODC1 ارسال می نماید.

۴. در این مرحله، پاسخ دریافت شده از سوی دامین کنترلر مورد نظر، توسط RODC1 به سوی کلاینت مورد نظر ارسال می گردد. سپس RODC1 در خواستی به سوی دامین کنترلر مورد نظر به منظور مجوز ذخیره سازی اطلاعات مرتبط با عملیات احراز هویت کلاینت را، ارسال می کند.

۵. دامین کنترلر مورد نظر، تنظیمات انجام گرفته در Password Replication Policy را مورد بررسی قرار داده و در نهایت، اطلاعات مرتبط با احراز هویت کلاینت مورد نظر را به سوی RODC1 ارسال می نماید تا بدین ترتیب RODC1 بتواند این اطلاعات را در خود ذخیره نماید.

۶. حال اگر کلاینت مذکور ری استارت گردد، هیچ تظمینی وجود ندارد که به منظور احراز هویت دوباره به سراغ RODC1 رود. اگر چنانچه جهت انجام عملیات احراز هویت به سراغ RODC2 رود، مراحل فوق مجددا برای RODC2 تکرار می گردد.

با توجه به سناریوی فوق، می توان براحتی فهمید که همواره وجود دو یا چند RODC در یک سایت مفید واقع نخواهد شد.

نصب یک RODC :

برای نصب یک RODC مراحل زیر را طی کنید:

۱. اطمینان پیدا کنید که Forest Functional Level حداقل Windows Server 2003 است.

۲. اگر در سراسر جنگل دامین کنترلری ویندوز سرور ۲۰۰۳ دارد adprep /rodcprep را اجرا کنید.

۳. اطمینان پیدا کنید حداقل یک DC ویندوز سرور ۲۰۰۸ دارد.

۴. نصب RODC

اگر یک Forest موجود را به روز رسانی می کنید تا شامل دامین کنترلر های ویندوز سرور ۲۰۰۸ باشد و قصد نصب RODC را دارید باید دستور adprep /rodcprep را اجرا کنید. این دستور باعث می شود تا مجوز های لازم جهت Replicate شدن Application Partition مربوط به DNS با RODC را ایجاد می کند.

اگر تمامی دامین کنترلرها ویندوز سرور ۲۰۰۸ دارند نیازی به اجرای این دستور نیست. فایل ها مربوطه در دی وی دی ویندوز سرور ۲۰۰۸ در پوشه Sources در پوشه Adprep قرار دارد و این پوشه را در دامین کنترلری که رول Schema Master را دارد کپی کنید و در CMD به محلی که فایل ها را کپی کرده اید بروید و سپس دستور را اجرا کنید. توجه داشته باشید که برای اجرای این دستور باید مجوز های مدیریتی لازم را داشته باشید در واقع باید عضو گروه Enterprise Admins باشید چرا که قرار است Schema تغییر کند.

حداقل باید یک DC با ویندوز سرور ۲۰۰۸ وجود داشته باشد (در دامین) به صورت ایده آل این دامین کنترلر باید در نزدیک ترین سایت یا به عبارت دیگر با کوتاه ترین لینک از محل قرار گیری RODC باشد. اگر می خواهید که RODC به عنوان DNS Server نیز عمل کند باید دامین کنترلر ویندوز سرور ۲۰۰۸ نیز شامل Zone های مربوطه باشد. نصب RODC مشابه نصب Additional Domain Controller است با این تفاوت که در انجام مراحل ویزارد باید چک باکس Read-Only Domain Controller را چک بزنید.

Installing From Media (IFM) – Active Directory

بیایید سناریوی زیر را فرض کنیم.

ما یک دفتر مرکزی شرکت و شعبه آن را داریم .در شعبه ، قصد داریم یک Domain Controller جدید را نصب کنیم. ارتباط بین دو نقطه کند است .پرونده Active Directory (ntds.dit) از حجم بسیاری تشکیل شده است. اگر از روش نصب کلاسیک Domain Controller در Active Directoryپیروی کنید ، می توانید تصور کنید چند ساعت یا چند روز زمان لازم است تا همگام سازی کامل DC جدید به پایان برسد.

به همین دلیل ، مایکروسافت ما را قادر می سازد با استفاده از روش Install From Media DC (IFM) به حل این مشکل بپردازیم. بنابراین ، ما می توانیم زمان لازم برای تکمیل فرایند را به میزان قابل توجهی کاهش دهیم. در واقع ، آنچه ما انجام می دهیم ایجاد یک پرونده با داده های Active Directory، چیزی مانند بک آپ ، از یک DC موجود و سپس وارد کردن آن به DC جدید شعبه است .بنابراین ، فقط زمان مورد نیاز برای هماهنگی تغییرات بین بک آپ و زمان ریستور نهایی آن با DC جدید است.

قبل از شروع روش نصب از روش (IFM) ، باید موارد اساسی را بدانید.

۱. **بدیهی است که روش IFM نمی تواند برای اولین DC یک Froot مورد استفاده قرار گیرد فقط برای اضافه کردن یک DC اضافی مورد استفاده قرار می گیرد.**
۲. **اطلاعات یا Media باید توسط یک DC از همان دامنه AD ایجاد شود.**
۳. **اگر DC جدید سرور (GC) باشد ، باید اطلاعات یا Media توسط یک DC ایجاد شود که یک سرور GC نیز باشد.**
۴. **اگر DC جدید سرور DNS باشد ، اطلاعات یا Media باید توسط یک DC با نقش DNS نصب شده ایجاد شود.**
۵. **اگر RODC را مستقر می کنید ، می توانید اطلاعات یا Media را از طریق یک DC قابل نوشتار یا RODC موجود ایجاد کنید.**

۶. روش IFM یک پایگاه داده موقت در پوشه٪ TMP٪ ایجاد می کند ، بنابراین مطمئن شوید که فضای کافی در محل پوشه وجود دارد.

با استفاده از ویندوز سرور ۲۰۱۶ و ابزار NTDSUtil.exe ، می توانید دو نوع اطلاعات یا Media را ایجاد کنید. Full (writable) Domain Controller یا RODC برای Windows Server 2008 R2 دو گزینه دیگر وجود دارد ، Full DC با SYSVOL و RODC با SYSVOL. که در انتهای همین بحث به آن می پردازیم.

باتوجه به اینکه در کلاس به نصب Active Directory با استفاده از روش Install From Media (IFM) در ویندوز سرور ۲۰۱۶ میپردازیم در این مقاله به استفاده از این روش در ویندوز سرور ۲۰۰۸ مراجعه کوتاهی انجام می دهیم.

نصب Installing From Media (IFM) در ویندوز سرور ۲۰۰۸

فرض کنید که در شبکه سازمان خود، سرویس Active Directory را بر روی یک دامین کنترلر راه اندازی نموده اید. حال بنا بر دلایلی می خواهید این سرویس را بر روی دامین کنترلر دیگری در حالت Additional Domain Controllerراه اندازی کنید. در این سناریو فرض بر آنست که دامین کنترلر دوم در مکانی دور از دامین کنترلر اول قرار گرفته و پهنای باند ارتباط میان آنها بسیار محدود بوده و یا از ثبات مورد نظر برخوردار نمی باشد. همچنین فرض کنید که پایگاه داده مربوط به سرویس Active Directoryدارای حجم قابل توجهی بوده و شما پالیسی های متعددی جهت مدیریت سیستم های موجود در سازمان وجوددارد را ایجاد نموده اید.

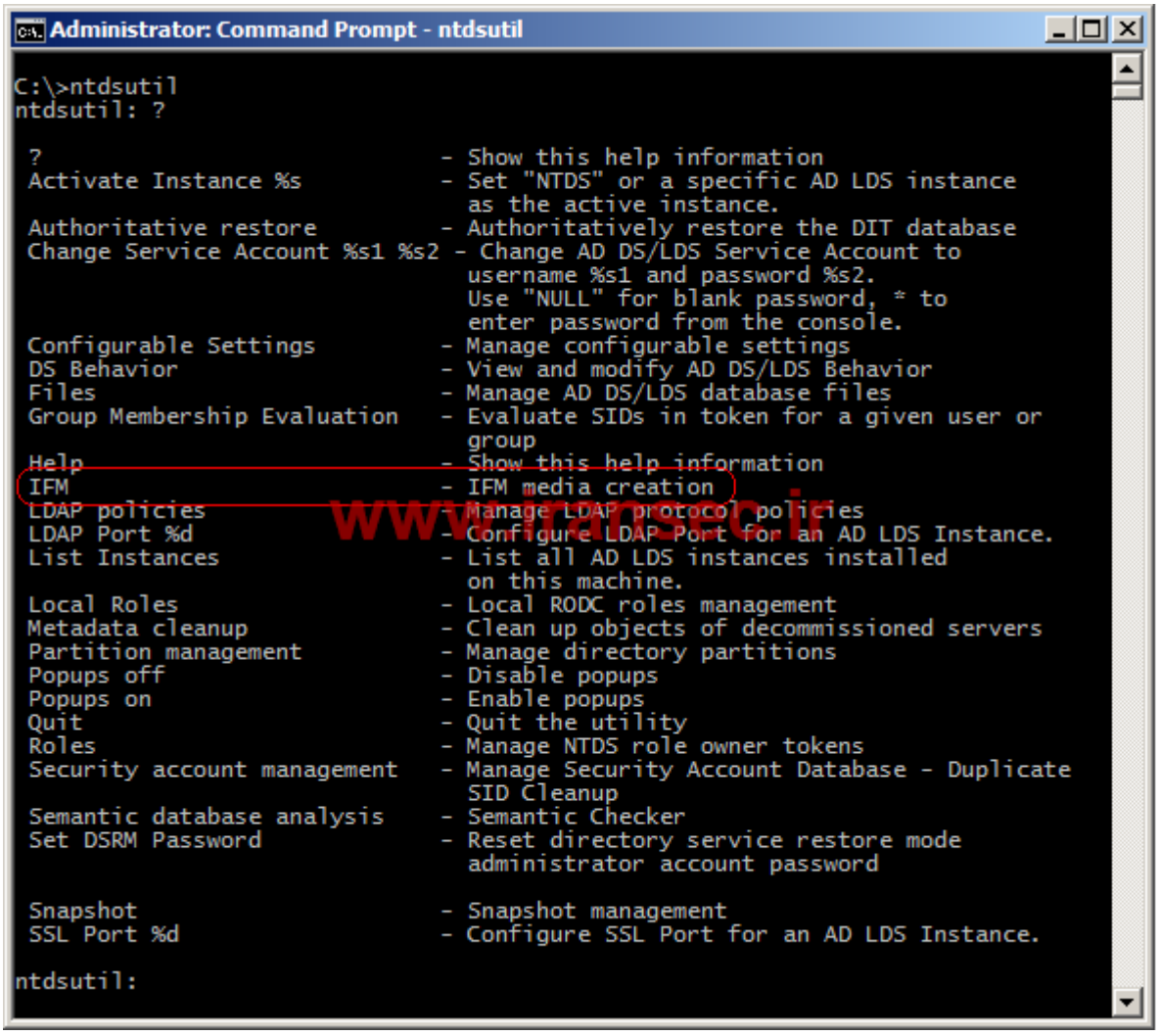
به صورت پیش فرض هنگامی که شما یک Additional Domain Controller ایجاد می نمایید، در عملیات نصب سرویس Active Directory بر روی آن، اطلاعات موجود در پایگاه داده مربوط به سرویس Active Directory موجود در دامین کنترلر اول به صورت خودکار به این دامین کنترلر انتقال می یابد. حال اگر پهنای باند میان این دو دامین کنترلر محدود باشد و یا از ثبات کافی برخوردار نباشد، ممکن است عملیات انتقال اطلاعات با مشکل دچار شده و در نهایت عملیات راه اندازی Additional Domain Controllerبا مشکل مواجه گردد.

با توجه به سناریوی فوق چگونه می توان Additional Domain Controller مورد نظر را با موفقیت راه اندازی نمود؟ خوشبختانه Windows Server 2008 R2 دارای قابلیتیست که به واسطه

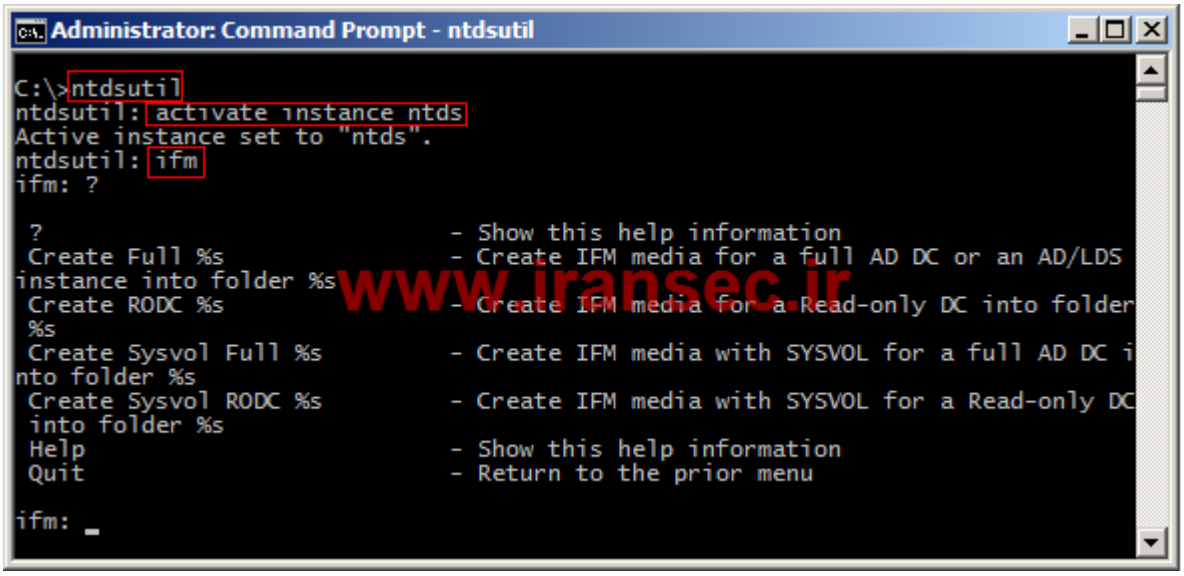
آن می توان اطلاعات مرتبط با سرویس Active Directory را در دامین کنترلر اول استخراج نموده و سپس آن را به سروری که قرار است نقش Additional Domain Controller را ایفا نماید، انتقال دهیم. سپس سرویس Active Directory را بر روی سرور مورد نظر بر اساس اطلاعات انتقال یافته راه اندازی نماییم.

نکته :قابلیت فوق اولین بار در Windows Server 2003 از سوی مایکروسافت معرفی شده است.

جهت انجام این سناریو ابتدا می بایست اطلاعات مرتبط با سرویس Active Directory را از دامین کنترلر اول استخراج نماییم. بدین منظور می بایست از ابزار ntdsutil به همراه سوئیچ ifm استفاده کنیم. به شکل زیر نگاه کنید:



نکته :ابزار ntdsutil می تواند در چهار حالت اقدام به استخراج اطلاعات مرتبط با سرویس Active Directoryنماید. به شکل زیر نگاه کنید:



این چهار حالت عبارتند از:

Full Domain Controller : از این روش زمانی استفاده کنید که می خواهید تمامی اطلاعات مرتبط با سرویس Active Directory بدون در نظر گرفتن اطلاعات موجود در فولدرSYSVOL ، را استخراج کنید. بدین منظور می بایست از دستور create full استفاده شود.

نکته : در صورت استفاده از این روش، بعد از نصب سرویس Active Directory بر روی Additional Domain Controller می بایست اطلاعات موجود در فولدر SYSVOL از دامین کنترلر اول به دامین کنترلر مذکور انتقال یابد. اگر چنانچه پالیسی های زیادی را جهت مدیریت کلاینت های موجود در سازمان خود ایجاد نموده اید، این عملیات ممکن است با در نظر گرفتن پهنای باند محدود و ناثبات، با مشکل مواجه شده و یا مدت زمانی طولانی به خود اختصاص دهد.

Full domain controller with SYSVOL: از این روش زمانی استفاده کنید که می خواهید تمامی اطلاعات مرتبط با سرویس Active Directory را به همراه محتویات فولدر SYSVOL استخراج نمایید. بدین منظور می بایست از دستور create sysvol full استفاده شود.

نکته :این روش تنها در Windows Server 2008 R2 امکان پذیر است.

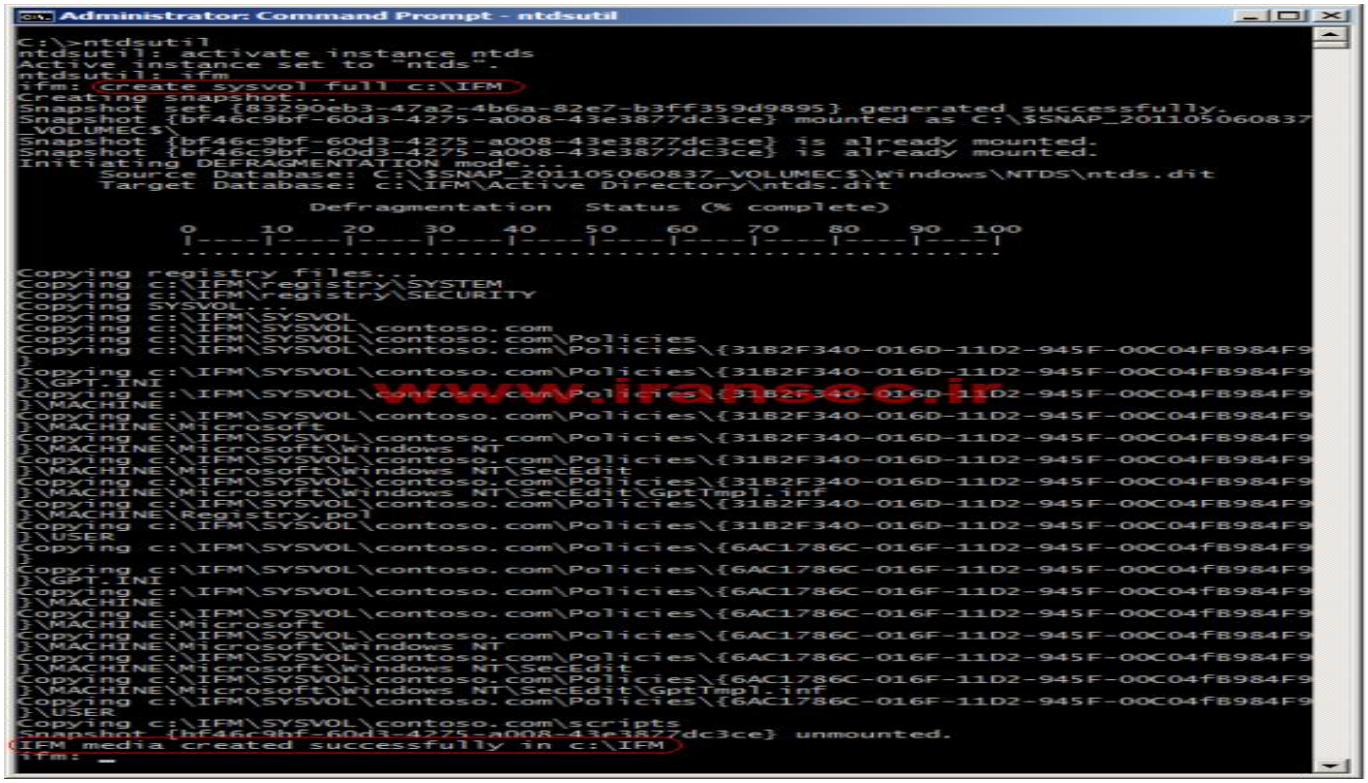
RODC: از این روش زمانی استفاده کنید که می خواهید یک Additional Domain Controller در حالت RODC و یا Read-Only Domain Controller ایجاد کنید. در این روش اطلاعات موجود در فولدر SYSVOL در نظر گرفته نمی شود. در این حالت می بایست از دستور create rodcاستفاده شود.

نکته ۱ :اطلاعات مورد نیاز جهت ایجاد یک Additional Domain Controller از نوع RODC با استفاده از این روش را می توان از روی یک Writable Domain Controller و یا یک RODC دیگر استخراج نمود.

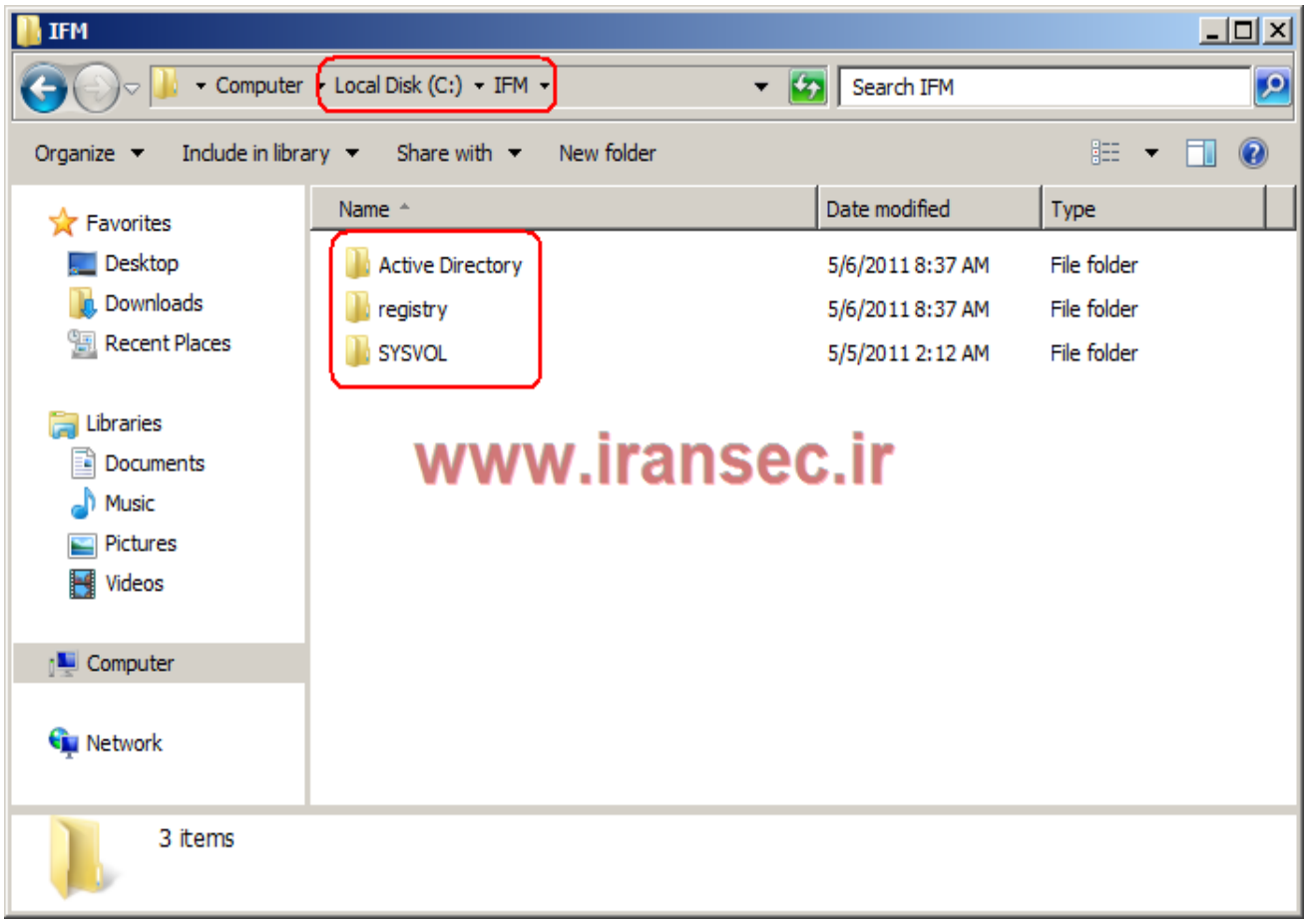
نکته ۲ :در صورت استفاده از این روش، بعد از نصب سرویس Active Directory بر روی Additional Domain Controllerمی بایست اطلاعات موجود در فولدر SYSVOL از دامین کنترلر اول به دامین کنترلر مذکور انتقال یابد. اگر چنانچه پالیسی های زیادی را جهت مدیریت کلاینت های موجود در سازمان خود ایجاد نموده اید، این عملیات ممکن است با در نظر گرفتن پهنای باند محدود و ناثبات، با مشکل مواجه شده و یا مدت زمانی طولانی به خود اختصاص دهد.

RODC with SYSVOL : تفاوت این روش با روش فوق در این است که در این روش اطلاعات موجود در فولدر SYSVOL نیز در نظر گرفته می شود. بدین منظور می بایست از دستور create sysvol rodc استفاده کنید.

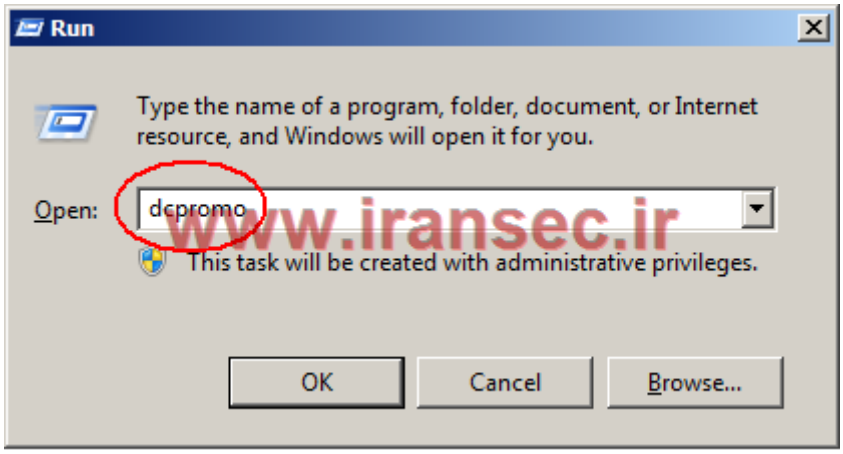
نکته :این روش تنها در Windows Server 2008 R2 امکان پذیر می باشد. در مثال زیر فرض بر آن شده است که می خواهیم یک Additional Domain Controller با استفاده از روش Full domain controller with SYSVOLایجاد نماییم. بدین منظور کافیست طبق شکل زیر عمل کنید:

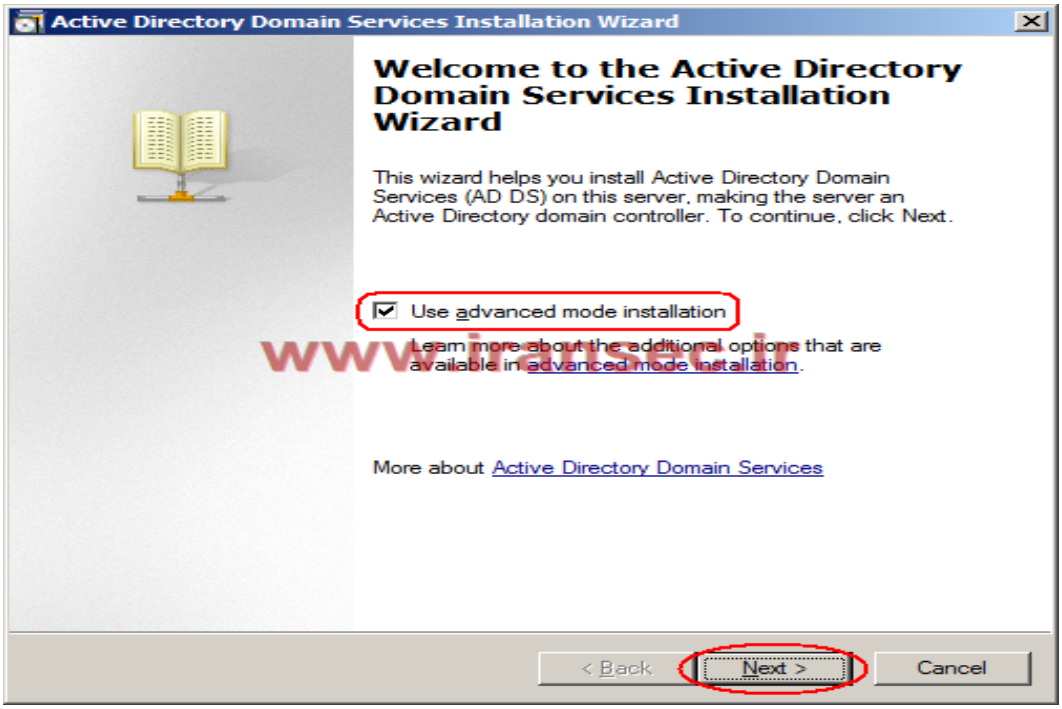


با انجام موفقیت آمیز عملیات فوق، محتویات پایگاه داده سرویس Active Directory به همراه محتویات فولدر SYSVOL در دامین کنترلر اول به فولدری با نام ifm که در ریشه درایو C قرار گرفته است، استخراج می گردد. به شکل زیر نگاه کنید:



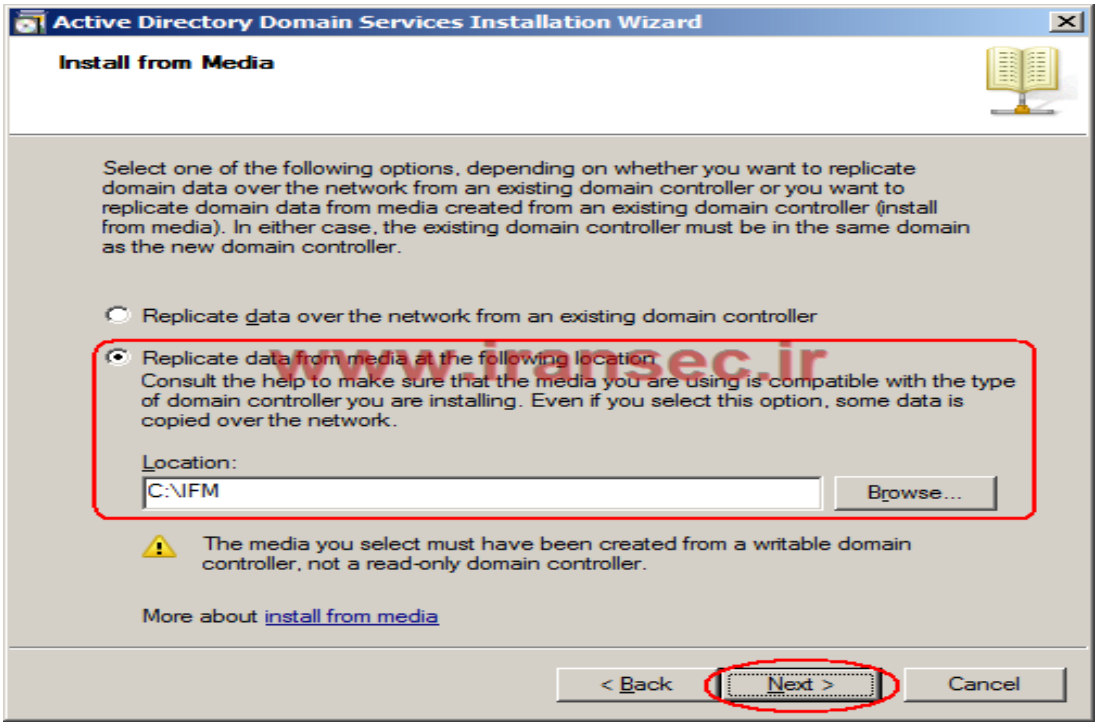
حال کافیست محتویات این فولدر را به سروری که مایل به نصب سرویس Active Directory در حالت Additional را داریم انتقال داده و سپس بر روی سرور مذکور طبق تصاویر زیر عمل کنیم:



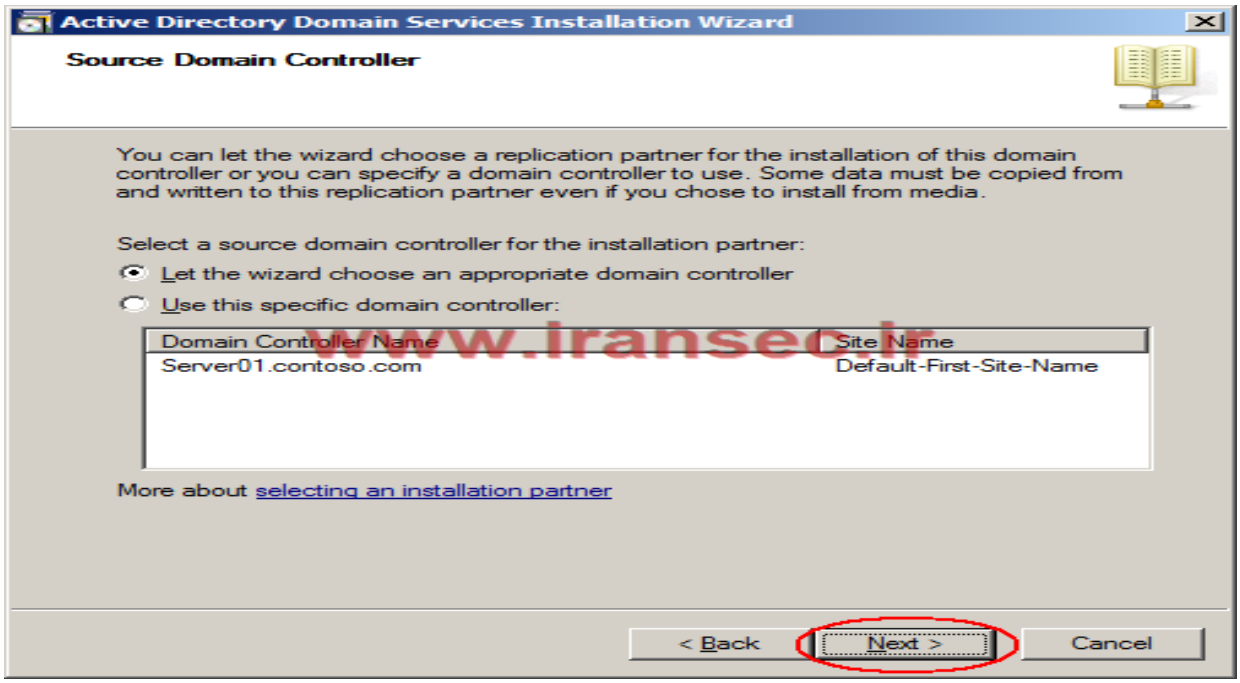


نکته :همچنین می توانید از دستور dcpromo /adv نیز استفاده کنید. با اجرای این دستور مشاهده خواهید نمود که ویزارد عملیات نصب به صورت پیش فرض گزینه Use Advanced Mode Installation را در حالت فعال قرار داده است.

عملیات نصب را بر اساس نیاز خود ادامه دهید. در این حالت بعد از مرحله Additional Domain Controller Options، انجام تنظیمات مورد نیاز جهت مشخص نمودن مکان اطلاعات انتقالی از دامین کنترلر اول برای شما به نمایش گذاشته می شود. به شکل زیر نگاه کنید:



بعد از انتخاب مسیر قرار گرفتن فولدر انتقالی از دامین کنترلر اول به دامین کنترلر مورد نظر، بر روی دگمه Next کلیک کرده و بدین ترتیب می توانید وارد تنظیمات مربوط به مرحله Source Domain Controller شوید. بر اساس نیاز خود یکی از گزینه های نمایش داده شده را انتخاب کرده و سپس بر روی دگمه Next کلیک کنید. به شکل زیر نگاه کنید:



در این مرحله عملیات نصب را با توجه به سیاست های سازمان خود به پایان برسانید.

نکته ۱ :با استفاده از روش فوق نمی توان به کلی عملیات replication اولیه را متوقف نمود. ممکن است از زمان اجرای ابزار ntdsutil تا زمان انتقال اطلاعات استخراجی و سپس ایجاد یک Additional Domain Controller، تغییراتی در پایگاه داده سرویس Active Directory به وقوع پیوسته باشند که در این شرایط این تغییرات می بایست به دامین کنترلر مورد نظر با استفاده از عملیات replication انتقال یابند. با توجه به این مطلب می توان نتیجه گرفت که هر چه زمان ایجاد اطلاعات استخراجی، انتقال آنها به دامین کنترلر مقصد و سپس نصب سرویس Active Directory زمان بیشتری به خود اختصاص دهد، شانس افزایش عملیات replication اولیه نیز افزایش می یابد.

نکته ۲ :استخراج اطلاعات مرتبط با سرویس Active Directory تنها از یک Writable Domain Controllerامکان پذیر است. این در حالیست که شما نمی توانید از یک RODC جهت استخراج اطلاعات مورد نظر استفاده کنید. همچنین می توانید از اطلاعات استخراج شده از یک Writable Domain Controllerجهت ایجاد یک Additional Domain Controller در حالت های Writable و RODC از طریق روش فوق استفاده کنید.

نکته ۳ :نمی توان از اطلاعات استخراجی جهت ایجاد یک Additional Domain Controller با سیستم عاملی متفاوت از دامین کنترلر اول، استفاده نمود. به عنوان مثال اگر چنانچه دامین کنترلر اول دارای سیستم عامل Windows Server 2008 باشد، نمی توان از اطلاعات استخراجی از آن برای ایجاد یک Additional Domain Controller با سیستم عامل Windows Server 2008 R2 استفاده کرد.

نکته ۴ 32 :بیتی و یا ۶۴ بیتی بودن دامین کنترلر مورد استفاده در انجام عملیات استخراج اطلاعات تاثیری بر ۳۲ بیتی و یا ۶۴ بیتی بودن سیستم عامل Additional Domain Controller مورد نظر ندارد.

نکته ۵ :فرض کنید که اطلاعات مرتبط با سرویس Active Directory را از یک دامین کنترلر با سیستم عامل Windows Server 2008 R2 استخراج نموده اید. حال قبل از انتقال اطلاعات استخراجی به سرور دوم و انجام عملیات نصب سرویسActive Directory ، اقدام به فعال نمودن قابلیت Active Directory Recycle Bin بر روی سرور اول می نمایید. در این حالت می بایست توجه داشته باشید که اطلاعات استخراجی دیگر فاقد ارزش بوده و نمی توان از آن برای ایجاد یک Additional Domain Controller استفاده کرد. در این حالت می بایست بار دیگر عملیات استخراج اطلاعات مرتبط با سرویس Active Directory را به انجام برسانید.

باتشکر فراوان از توجه شما استاد عزیز