Microsoft Exchange Server 2010

پژوهش و نگارش: وحید نصیری
Vahid_Nasiri@Yahoo.Com
زمستان ۱۳۸۸

فهرست مطالب

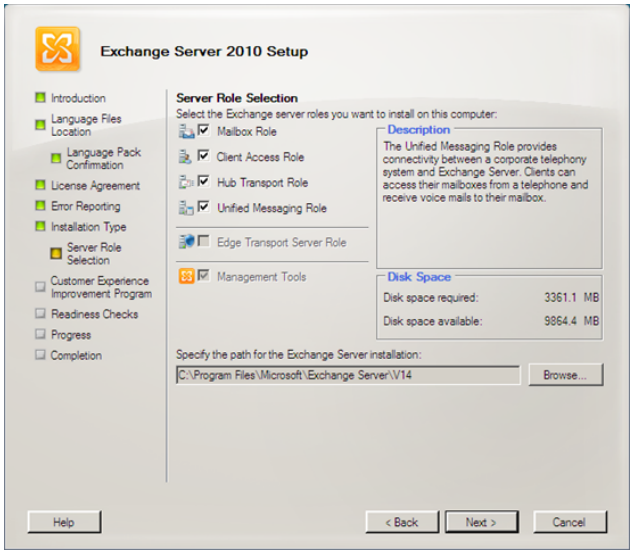
مقدمه

برنامه‌ی Exchanger server ، نرم افزار ارسال و دریافت ایمیل سازمانی مایکروسافت است که در رده‌ی محصولات سرور آن شرکت قرار می‌گیرد. اولین نگارش Exchanger server در سال ۱۹۹۳ ارائه شد و به صورت محدود در اختیار حدود ۵۰۰ شرکت قرار گرفت. در سال ۱۹۹۶ اولین نگارش عمومی آن به نام Exchange server 4.0 به عموم ارائه گشت و در سال ۱۹۹۷ با ارائه‌ی Exchange server 5.0 آمار مشتریان این محصول به ۳۲ هزار کاربر رسید. به همراه این نگارش، اولین نسخه‌ی برنامه Outlook web access نیز ارائه گردید. با افزایش استقبال از این محصول، در همان سال نگارش 5.5 آن نیز ارائه شد و ظرفیت بانک‌های اطلاعاتی آن تا 16TB در نگارش سازمانی آن افزایش یافت. در سال ۲۰۰۰، اولین نگارش یکپارچه‌ی آن با Active directory ارائه شد. بزرگترین مشکل این محصول در سال ۲۰۰۰، کوچ از نگارش‌های قدیمی به نگارش جدید بودند که این مشکل در سال ۲۰۰۳ با ارائه Exchange server 2003 برطرف گردید. در اواخر سال ۲۰۰۶ ، Exchange server 2007 ارائه گشت که مهمترین تفاوت آن با نگارش‌های قبلی، ارائه‌ی آن تنها برای سکوهای ۶۴ بیتی بود به همراه بهبودهایی در اندازه‌ی صندوق‌های پستی تا ۲ گیگابایت، تضمین فعالیت بی‌وقفه بهبود یافته ، شروع به کنار گذاری Public folders و تمهیداتی جهت ارسال و دریافت پیغام‌های صوتی. در اواخر سال ۲۰۰۹ نگارش ۲۰۱۰ این محصول ارائه گشت که تنها با ویندوز سرور ۲۰۰۸ سازگار می‌باشد و در آن عمده‌ی مشکلات به همراه نگارش ۲۰۰۷ آن برطرف شده است همانند Outlook web access سازگار با تمامی مرورگرهای امروزی، امکان مدیریت تحت وب صندوق‌های پستی کاربران، بازنگری در گزینه‌های تضمین فعالیت بی‌وقفه و ساده سازی آن‌ها، افزایش تعداد بانک‌های اطلاعاتی قابل تعریف در یک سرور و بسیاری از موارد دیگر که در طی چندین فصل به بررسی آن‌ها خواهیم پرداخت.

وحید نصیری
زمستان ۸۸

فصل ۱- آشنایی با نقش‌های Exchange Server 2010

در فصل آتی حین نصب بسته‌ی نرم افزاری Exchange server 2010 باید نقش‌هایی مانند Hub Transport server ، Mailbox server و غیره را انتخاب نمائیم (شکل ۱). در فصل جاری قصد داریم با جزئیات این نقش‌ها آشنا شویم.



شکل ۱- انتخاب نقش‌های مختلف Exchange server 2010 در حین نصب اولیه آن.

نقش‌ها در Exchange server 2010

نقش‌ها در Exchange server 2010 گروه بندی منطقی ویژگی‌ها و اجزایی هستند که کار مشخصی را در این مجموعه‌ی اطلاع رسانی بر عهده دارند. تمام نقش‌های موجود را منهای نقش Edge Transport server می‌توان بر روی یک سرور نصب نمود. در یک شرکت بزرگ می‌توان هر نقش را بر روی یک سرور مجزا نیز نصب نمود و یا در شرکتی با تعداد کاربر کمتر می‌توان تمامی نقش‌های موجود را (با توجه به استثنای ذکر شده) به یک سرور واگذار نمود.

مزایای وجود نقش‌ها در Exchange server 2010 به شرح زیر هستند:

- توزیع ساده‌تر. نقش‌های متفاوت را می‌توان به سادگی بر روی سرورهای مختلف نصب کرد.

- کنترل مدیریتی بهتر. با توجه به امکان نصب نقش‌های متفاوت بر روی سرورهای مختلف، می‌توان افراد مختلفی را با مسؤولیت‌های متفاوت جهت مدیریت این سرورها مشغول به کار نمود.
- مقیاس پذیری. به جای نصب تمامی نقش‌ها بر روی یک سرور، با نصب نقش‌های متفاوت در سرورهای مختلف، بار کاری مجموعه‌ی Exchange server بین این سرورها توزیع خواهد شد.
- بهبود امنیتی. با نصب نقش‌های متفاوت بر روی سرورهای مختلف، سطح حمله نیز به همان اندازه کاهش خواهد یافت.
- سادگی پروسه‌ی نصب. اگر نیاز به نصب Mailbox server role وجود داشته باشد، تنها کافی است این گزینه‌ی ساده را به جای انتخاب چندین ویژگی که این نقش را تشکیل خواهند داد، انتخاب کرد.

آشنایی با نقش Hub Transport server

کار نقش Hub Transport server ، ارسال پیام‌ها است. این نقش پیام‌های دریافتی را طبقه بندی، مدیریت و ارسال می‌کند. در هر Active directory باید حداقل یک نقش Hub Transport server نصب گردد و سروری که این نقش بر روی آن نصب خواهد شد باید عضو دامنه‌ی Active directory ما نیز باشد.

پروتکل SMTP جهت ارسال و مدیریت پیام‌های کاربران بسیار غیر بهینه عمل می‌نماید. توسط این پروتکل اگر پیغامی حاوی یک پیوست ۵ مگابایتی باشد، به هر گیرنده یک نسخه‌ی ۵ مگابایتی ارسال خواهد شد (حتی اگر تمامی آن‌ها بر روی یک سرور قرار داشته باشند). در حالیکه توسط فناوری Hub Transport server بهینه ترین روش ارسال پیغام در شبکه محاسبه شده و در صورتیکه تمام دریافت کنندگان بر روی یک سرور راه دور قرار داشته باشند، تنها یک نسخه از این ایمیل ۵ مگابایتی به سرور راه دور ارسال می‌گردد و در همان سرور تنها کپی‌های این ایمیل به صندوق‌های پستی کاربران هدایت خواهد شد. به این صورت بار و ترافیک شبکه در یک محیط پرکاربر به شدت کاهش خواهد یافت.

همچنین توسط Hub Transport server امکان اعمال سیاست‌های ارسال ایمیل نیز درون یک سازمان وجود دارد که در طی فصول آتی در مورد آن بیشتر توضیح داده خواهد شد. برای مثال اعمال سیاست رمزنگاری بر روی محتوای ایمیل‌هایی حاوی اطلاعات محرمانه یک سازمان (شبیه به Rules تعریف شده در Outlook اما این‌بار در سطح سرور و برای تمامی کاربران و یا کاربرانی مشخص).

لازم به ذکر است که امکان استفاده مستقیم از Hub Transport server برای ارسال ایمیل به خارج از سازمان نیز وجود دارد، اما توصیه‌ی اکید امنیتی است که این نقش را به Edge Transport server محافظت شده واگذار نمائید.

اگر علاقمند باشید که جزئیات معماری این نقش را مشاهده نمائید، می‌توان دیاگرام آن‌را از آدرس ذیل دریافت نمود:
http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=6eb8c09a-6ea4-442a-9faa-de33265ceb84

آشنایی با نقش Mailbox server

کار نقش Mailbox server مدیریت صندوق‌های پستی و بانک‌های اطلاعاتی public folders است. سرورهای صندوق پستی جهت مباحث مقیاس پذیری و اطمینان بالای عملکرد از مفاهیم clustering و replication پشتیبانی می‌کنند. سروری که این نقش بر روی آن نصب می‌گردد نیز باید عضو دامنه‌ی Active directory ما بوده و همچنین پیشنهاد می‌شود که هیچگونه دسترسی به آن از اینترنت وجود نداشته باشد.

این نقش تنها کار ذخیره سازی ایمیل‌ها را به عهده دارد و همچنین اطلاع رسانی به نقش Hub Transport در مورد مدیریت آن‌ها را انجام می‌دهد.

با توجه به امکان نصب این نقش به صورت مجزا بر روی یک سرور اختصاصی، امکان بهره گیری از امکانات SAN و امثال آن به شکلی بهینه وجود خواهد داشت.

در طی آشنایی با مراحل نصب برنامه در فصل بعدی، یکی از گزینه‌ها آن، نصب public folders برای کاربرانی است که هنوز از Outlook 2003 استفاده می‌کنند. توصیه مایکروسافت در نگارش‌های جدید این محصولات، استفاده از SharePoint جهت ارائه محیطی تعاملی است بجای استفاده از public folders با معماری قدیمی آن.

آشنایی با نقش Edge Transport server

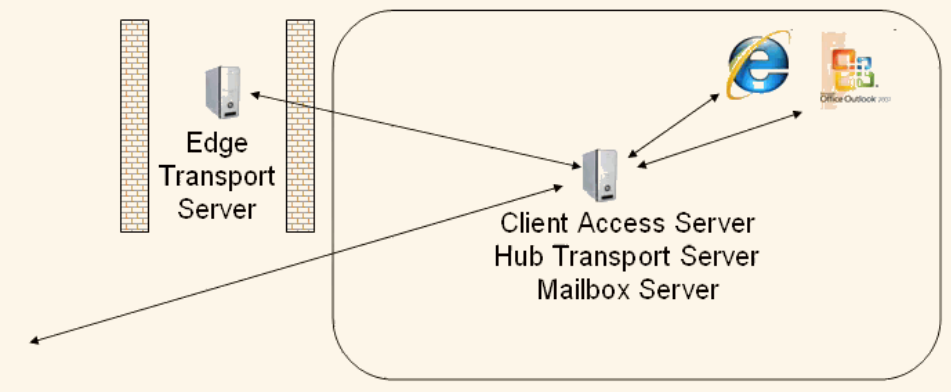
کار نقش Edge Transport server ایجاد دروازه‌ای جهت پشتیبانی از پروتکل SMTP (Simple Mail Transport Protocol) بین ارگان شما و خارج از آن، برای مثال اینترنت است. این نقش ایمیل‌ها را از دنیای خارج به Hub Transport server هدایت می‌کند و برعکس. جهت رعایت مباحث امنیتی این نقش باید بر روی سروری نصب گردد که عضو دامنه‌ی Active directory شما نیست و همچنین توصیه شده است که بر روی این سرور جهت کاهش سطح حمله، هیچ برنامه و سرویس دیگری بجز فایروال نیز نصب نگردد (شکل ۲). این نقش امور زیر را مدیریت می‌کند:

- مدیریت ارسال‌ها و دریافت‌ها
- بررسی اعتبار ارسال کننده‌های ایمیل
- بررسی ضمایم ایمیل‌های دریافتی و ارسالی
- ویروس یابی ایمیل‌های ارسالی و دریافتی با کمک نرم افزارهای جانبی نصب شده

از آنجائیکه نقش Edge Transport server جزو Active directory شبکه شما نخواهد بود، از Active Directory Application Mode یا ADAM جهت دسترسی به اطلاعات کاربران شبکه و دریافت کنندگان ایمیل‌های رسیده استفاده خواهد کرد.

امکان نصب چندین Edge Transport server جهت بهره گیری از مباحث load balancing نیز میسر است.

بنابراین مطابق توضیحات ارائه شده، امکان ترکیب نقش Edge Transport server با سایر نقش‌های مهیای Exchange server 2010 وجود ندارد.



شکل ۲– نحوه‌ی قرار گیری Edge Transport server در خارج از یک شبکه و محافظت آن با فایروال و نحوه‌ی تعامل آن با سایر نقش‌های نصب شده. هر چند مطابق تصویر، Hub Transport server نیز امکان تعامل با دنیای خارج را دارد اما توصیه اکید امنیتی است که از Edge Transport server استفاده شود.

آشنایی با نقش Client Access server یا CAS

کار نقش Client Access server پشتیبانی از انواع و اقسام پروتکل‌های دریافت و ارسال ایمیل است. در هر Active directory که یک نقش Mailbox server نصب شده است، حداقل یک نقش Client Access server نیز باید نصب گردد.

این نقش از پروتکل‌ها و روش‌های دریافت و ارسال ایمیل ذیل پشتیبانی به عمل می‌آورد:

- کلاینت‌های OWA (outlook web access)
- POP (پروتکل post office) و IMAP (پروتکل Internet Message Access)
- Outlook Anywhere (روش RPC over HTTP که از Exchange Server 2003 متداول گردید)
- کلاینت‌های EAS
- پروتکل MAPI (Messaging Application Programming Interface) که جهت اتصال مستقیم به صندوق‌های پستی قابل استفاده است (همانند برنامه Outlook)

در یک شبکه که نقش‌های CAS و Mailbox server بر روی سرورهای مجزایی نصب شده‌اند، CAS برای یافتن Mailbox servers از Global catalog server موجود در Domain استفاده خواهد کرد. همچنین توصیه می‌شود که پیوند ارتباطی بین CAS و Mailbox server را از نوع پرسرعت انتخاب کنید.

از ویژگی‌های دیگر CAS می‌توان به موارد ذیل اشاره کرد:

- Autodiscovery : امکان یافتن کاربران در Domain و ایجاد خودکار پروفایل برای آن‌ها.
- Web Services : امکان دسترسی به امکانات Exchange server به کمک برنامه نویسی.

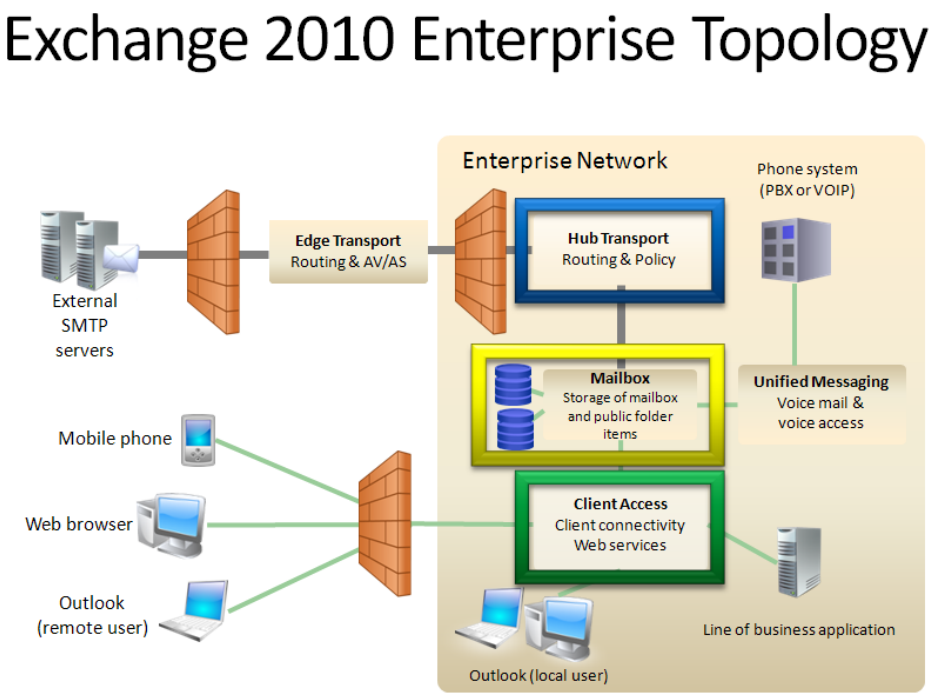
آشنایی با نقش Unified Messaging server

کار نقش Unified Messaging server یکپارچه سازی خدمات و پیام‌های Fax و Voice با سیستم ارسال و دریافت ایمیل‌های ارگان شما است. برای نصب این نقش در یک شبکه داخلی، نیاز به نصب سه نقش Hub Transport، Client Access و Mailbox نیز می‌باشد. همچنین باید به Global catalog server موجود در Domain نیز دسترسی داشته باشد. توصیه شده است برای نصب این نقش از یک سرور مجزا و اختصاصی با دسترسی به وسایل IP/PBX و یا VoIP ، استفاده شود.

پیغام‌های صوتی شامل موارد زیر می‌توانند باشند:

- پاسخ دهی توسط پیغام‌های صوتی از پیش ذخیره شده
- گوش فرادادن به پیغام‌های صوتی رسیده و پاسخ دهی به آن‌ها
- گوش فرا دادن به پیغام‌های ذخیره شده در تقویم
- برقراری تماس تلفنی با توجه به اطلاعات اشخاص ذخیره شده اشخاص در سازمان
- پذیرفتن و یا رد درخواست‌های جلسات

اکنون با توجه به این توضیحات، جانمایی نقش‌های مختلف Exchange server 2010 را بهتر می‌توان درک کرد (شکل ۳).



شکل ۳– تصویری از جانمایی نقش‌های مختلف Exchange server 2010 .

نحوه‌ی دریافت یک ایمیل از اینترنت و ورود آن به Exchange server 2010

جزئیات جریان کاری دریافت یک ایمیل از اینترنت و هدایت و مدیریت آن توسط Exchange server 2010 مطابق مراحل زیر است:

۱- ایمیل رسیده از اینترنت در ابتدا به Edge Transport server خواهد رسید.

۲- توسط Edge Transport server کارهای فیلتر کردن spam ها، بکارگیری آنتی ویروس و امثال آن صورت خواهد گرفت. سپس پیغام‌های رسیده به Hub Transport server ارسال می‌شوند.

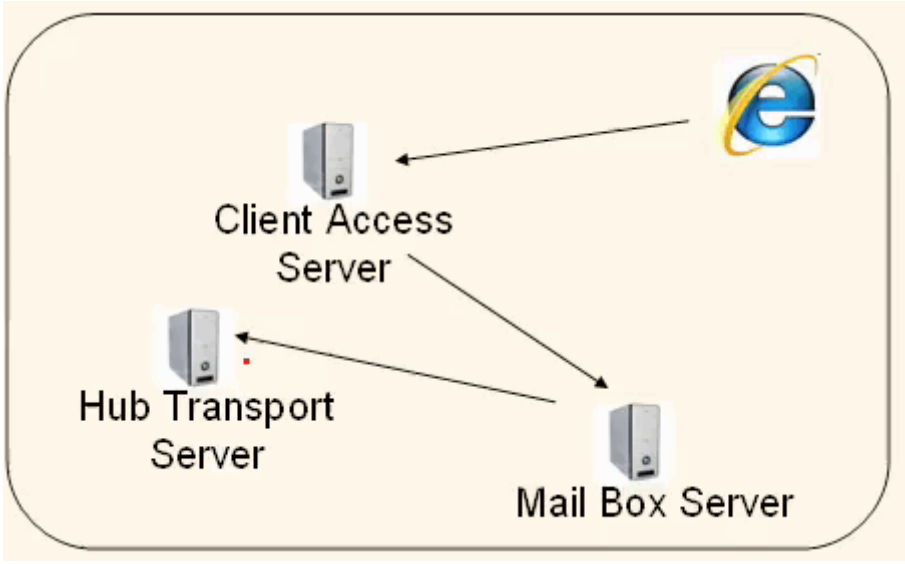
۳- توسط Hub Transport server کار بررسی محتوا، اعمال سیاست‌های کاری شرکت و همچنین یافتن بهینه‌ترین مسیر ارسال ایمیل‌ها به دریافت کنندگان صورت گرفته و در نهایت ایمیل‌ها را به Mailbox server هدایت می‌کند.

۴- Mailbox server ایمیل‌ها را در صندوق پستی کاربران قرار داده و سپس آن‌ها را مطلع می‌سازد.

۵- کاربران برای مشاهده ایمیل‌های رسیده از برنامه‌های مختلفی مانند Outlook ، OWA ، وسایل ویندوز موبایل و امثال آن جهت اتصال به client access server بهره خواهند جست.

۶- همچنین اگر در این بین پیام voice mail خاصی نیز برای کاربران رسیده باشد، Unified Messaging server کار مدیریت و قرار دادن آن‌ها را در صندوق پستی کاربران به عهده خواهد گرفت.

نحوه‌ی ارسال و مدیریت ایمیل‌ها در یک شبکه داخلی Exchange server 2010 که به اینترنت نیز راهی ندارد همانند مراحل ذکر شده است با این تفاوت که مرحله Edge Transport server آن حذف شده و کار دریافت اولیه پیغام‌ها از client access server شروع می‌شود. سپس پیغام‌ها در Mailbox server ذخیره شده و توسط Hub Transport server مدیریت نهایی بر روی آن‌ها صورت خواهد گرفت (شکل ۴).



شکل ۴- نحوه مدیریت ایمیل‌ها در یک شبکه داخلی با کمک سه سرور که نقش‌های متفاوتی بر روی آن‌ها نصب شده است.

توصیه‌هایی جهت نصب بهینه نقش‌های Exchange server 2010

تا اینجا با جزئیات نقش‌های مختلف Exchange server 2010 آشنا شدیم و همچنین نکته‌ی بارز تمامی آن‌ها امکان نصب هر کدام بر روی سرورهای اختصاصی است. با این تفاسیر بهترین توصیه جهت نصب بهینه این نقش‌ها چیست؟

اگر سازمان شما کمتر از ۷۵ نفر کارمند دارد که مطابق اصطلاحات رایج به آن small business هم گفته می‌شود، تمامی نقش‌ها را بر روی یک سرور اختصاصی نصب کنید. بدیهی است که برای نقش Edge Transport server نیاز به سروری مجزا خواهید داشت.

اگر سازمان شما بیش از ۷۵ نفر کارمند دارد (medium-sized business) توصیه مایکروسافت به استفاده از دو domain controller جهت افزونگی (redundancy)، یک سرور اختصاصی برای نصب دو نقش Hub Transport، Client Access و یک سرور مجزا برای نصب نقش Mailbox می‌باشد. همچنین از سرور مجزای دیگری برای نصب نقش Edge Transport server استفاده کنید. با افزایش تدریجی کارکنان سازمان می‌توان هر کدام از نقش‌های یاد شده را بر روی سرورهای اختصاصی نیز نصب نمود.

در سازمان‌های بزرگ (large business) توصیه‌های سازمان‌های متوسط تجاری در حال رشد نیز کاربرد دارد با این تفاوت که نقش mailbox server را می‌توان بر روی چندین سرور اختصاصی نیز نصب نمود. در کل جهت نصب نقش‌های مختلف بر روی چندین سرور اختصاصی مختلف می‌توان به ترتیب ذیل عمل کرد:

۱- نصب نقش CAS
۲- نصب نقش Hub Transport server
۳- نصب نقش Mailbox server
۴- نصب نقش Edge Transport server (اختیاری)
۵- نصب نقش Unified Messaging server (اختیاری)

در تمام این حالت‌ها بهتر است نصب نقش اختیاری Unified Messaging بر روی یک سرور اختصاصی و مجزا از سایر نقش‌ها با توجه به ترافیک بالای آن صورت گیرد.

فصل ۲ – نصب و راه اندازی Microsoft Exchange Server 2010

پیش‌نیازهای اجباری نصب Microsoft Exchange Server 2010

برخلاف نگارش‌های قبلی این محصول، Microsoft Exchange Server 2010 تنها در نسخه‌ی ۶۴ بیتی ارائه شده است و فقط بر روی ویندوزهای سرور ۲۰۰۸ به بعد قابل نصب و راه اندازی می‌باشد. بنابراین نگارش ۲۰۱۰ آن بر روی ویندوز سرور ۲۰۰۳ نصب نخواهد شد. همچنین Management Tools آن نیز بر روی ویندوزهای ویستا ۶۴ بیتی به بعد و یا ویندوز سرور ۲۰۰۸ شصت و چهاربیتی قابل نصب است.

به علاوه اگر در سازمان خود دارای نگارش‌های قبلی Exchange Server هستید، تنها کوچ از نگارش‌های SP2 مربوط به Exchange Server 2007 و یا Exchange Server 2003 پشتیبانی می‌شود.

Exchange Server 2010 برای عملکرد صحیح، نیاز به وجود Active directory در شبکه داشته و همچنین فرض بر این است که این Global Catalogs و Domain Controllers دارای آخرین به روز رسانی‌های ارائه شده نیز هستند. بدیهی است بدون وجود Active directory موفق به نصب آن نخواهید شد.

علاوه بر آن، نیاز به نصب موارد ذیل نیز می‌باشد:

بسته‌ی نرم افزاری مورد نیاز	آدرس دریافت
Microsoft .NET Framework 3.5	به همراه اجزای ویندوز قابل نصب است
Windows Remote Management (WinRM)	http://go.microsoft.com/fwlink/?LinkID=160491
Windows PowerShell	http://support.microsoft.com/kb/968929
Update for the Microsoft Management Console (MMC)	http://go.microsoft.com/fwlink/?LinkId=3052&kbid=951725
Extensions for ASP.NET AJAX	http://go.microsoft.com/fwlink/?LinkId=137040
Microsoft Filter Pack	http://go.microsoft.com/fwlink/?LinkId=137042

اگر از نگارش R2 ویندوز سرور ۲۰۰۸ استفاده نمائید، آخرین نگارش اکثر موارد فوق را نیز به همراه دارد (.NET Framework 3.5 ، Windows Remote Management 2.0 و PowerShell v2) و نیازی جهت مراجعه به سایت مایکروسافت برای دریافت و نصب آن‌ها نمی‌باشد.

همچنین نگران این پیش نیازها نیز نباشید. در حین نصب برنامه، هرجایی که پیش نیازی موجود نبود، برنامه نصاب با یک خطا متوقف شده و در ذیل پیغام خطا، لینک دریافت بسته نرم افزاری مورد نظر را نیز ارائه می‌دهد. پس از نصب کمبودهای گوشزد شده، مجددا برنامه نصاب را اجرا نمائید تا از ادامه عملیات نصب شروع به کار نماید.

با توجه به پیش نیازهای ذکر شده، امکان نصب Exchange server 2010 بر روی Windows 2008 Server Core نمی‌باشد (برای مثال این سرور از دات نت فریم پشتیبانی نمی‌کند).

پیش نیازهای Active directory جهت نصب Exchange server 2010

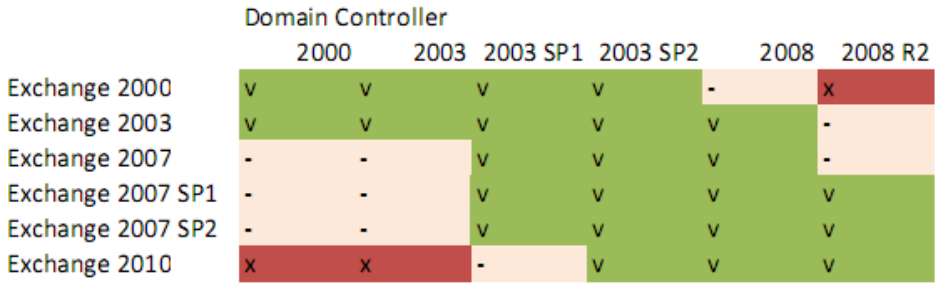
در تصاویر ذیل به صورت خلاصه پیش‌نیازهای لازم Active directory مورد نیاز جهت نصب Exchange server 2010 را در مقایسه با سایر نگارش‌های قبلی ملاحظه می‌نمائید.

Exchange server 2010 را تنها بر روی ویندوز سرور ۲۰۰۸ نسخه ۶۴ بیتی می‌توان نصب نمود، اما این برنامه می‌تواند از یک Domain ویندوز سرور ۲۰۰۳ با آخرین سرویس پک‌های موجود و یا ویندوز سرور ۲۰۰۸ استفاده نماید (شکل ۱).

Global catalog server مورد نیاز نیز می‌تواند ویندوز سرور ۲۰۰۳ با آخرین به روز رسانی‌های موجود و یا ویندوز سرور ۲۰۰۸ باشد (شکل ۲).

سایر موارد مورد نیاز مانند domain functional level، Schema master و امثال آن نیز می‌توانند بر اساس آخرین نگارش‌های ویندوز سرور ۲۰۰۳ و یا ویندوز سرور ۲۰۰۸ باشند (شکل‌های ۳ تا ۵).

در این تصاویر هر جایی علامت X را مشاهده می‌نمائید به معنای عدم پشتیبانی آن نگارش است.



شکل ۱- Domain controllers مورد پشتیبانی توسط Exchange server 2010

Global Catalog

	2000	2003	2003 SP1	2003 SP2	2008
Exchange 2000	v	v	v	v	-
Exchange 2003	v	v	v	v	v
Exchange 2007	-	-	v	v	v
Exchange 2007 SP1	-	-	v	v	v
Exchange 2007 SP2	-	-	v	v	v
Exchange 2010	x	x	x	v	v

شکل ۲– Global catalog servers مورد پشتیبانی توسط Exchange server 2010

Schema Master

	2000	2003	2003 SP1	2003 SP2	2008	2008 R2
Exchange 2000	v	v	v	v	x	x
Exchange 2003	v	v	v	v	v	x
Exchange 2007	x	x	v	v	v	x
Exchange 2007 SP1	x	x	v	v	v	v
Exchange 2007 SP2	x	x	v	v	v	v
Exchange 2010	x	x	v	v	v	v

شکل ۳– Schema masters مورد پشتیبانی توسط Exchange server 2010

Domain Functional level

	2000 Mixed	2000 Native	2003 Interim	2003 (Native)	2008 RTM
Exchange 2000	v	v	v	v	x
Exchange 2003	v	v	v	v	x
Exchange 2007	x	v	x	v	v
Exchange 2007 SP1	x	v	x	v	v
Exchange 2007 SP2	x	v	x	v	v
Exchange 2010	x	x	x	v	v

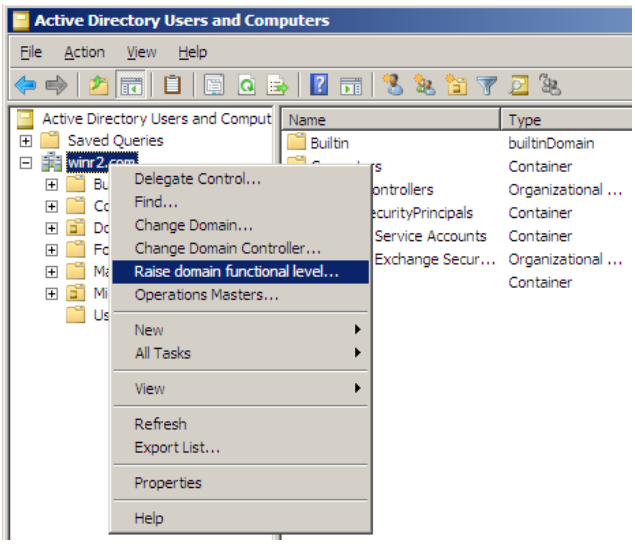
شکل ۴– Domain functional levels مورد پشتیبانی توسط Exchange server 2010

Forest Functional level

	2000 Native	2003 Interim	2003 (Native)	2008 RTM
Exchange 2000	v	v	v	x
Exchange 2003	v	v	v	x
Exchange 2007	v	x	v	v
Exchange 2007 SP1	v	x	v	v
Exchange 2007 SP2	v	x	v	v
Exchange 2010	x	x	v	v

شکل ۵– Forest functional levels مورد پشتیبانی توسط Exchange server 2010

برای تغییر domain functional level مطابق تصویر ۶ می‌توان عمل کرد:



شکل ۶- نحوه تغییر domain functional level جهت نصب exchange server 2010

البته اگر domain controller شما نیز از نوع ویندوز سرور ۲۰۰۸ باشد، نیازی به تغییر خاصی نخواهید داشت و این مورد در آن به حداکثر مقدار ممکن تنظیم شده است. اگر domain controller شما از نوع ویندوز سرور ۲۰۰۳ است باید این سطح کارآیی حداقل به Windows 2003 native تنظیم شود در غیر اینصورت عملیات نصب Exchange server 2010 با موفقیت به پایان نخواهد رسید.

نصب اجزاء ویندوز سرور ۲۰۰۸ پیش از شروع عملیات نصب

پیش از شروع به نصب Microsoft Exchange Server 2010 نیاز است تا یک سری از اجزاء ضروری مورد نیاز آن‌را در ویندوز سرور ۲۰۰۸ نصب نمود. بسته به نقش‌هایی که به این سرور انتساب خواهیم داد، اجزای متفاوتی را باید نصب نمود. این نقش‌ها را در جدول ۱ می‌توانید مشاهده نمائید.

جدول ۱– اجزاء متفاوت مورد نیاز از ویندوز سرور ۲۰۰۸ جهت نصب نقش‌های گوناگون Exchange Server 2010.

Role Services/Role	Mailbox	Client Access Server	Hub	Unified Messaging	Typical CAS, HUB and Mailbox	Edge
RSAT-ADDS	X	X	X		X	
RSAT-ADLDS						X
Web-Server	X	X	X	X		
Web-Metabase	X	X	X	X		
Web-Lgcy-Mgmt-Console	X	X	X	X		
Web-ISAPI-Ext		X				
Net-http-Activation		X				
Web-Basic-Auth	X	X	X	X		
Web-Digest-Auth		X				
Web-Windows-Auth	X	X	X	X		
Web-Dyn-Compression		X				
RPC-over-HTTP-proxy		X				
Web-net-ext	X	X	X	X		
Desktop-Experience				X		

برای نصب هر یک از نقش‌های ذکر شده راه‌حل‌های متفاوتی وجود دارد برای مثال استفاده از رابط کاربری ویندوز سرور ۲۰۰۸ جهت نصب آن‌ها و یا استفاده از برنامه کمکی استاندارد خط فرمان ServerManagerCMD که جهت انجام این‌گونه امور و یا حتی اتوماسیون آن‌ها امروزه بیشتر بکار گرفته می‌شود. روش کلی استفاده از برنامه خط فرمان ServerManagerCMD به شکل زیر است:

```
ServerManagerCmd –i <role>
```

برای مثال برای نصب اولین نقش ذکر شده در جدول یک از دستور خط فرمان زیر نیز می‌توان کمک گرفت:

```
ServerManagerCMD –i RSAT-ADDS
```

و در حالت کلی پیش از شروع به نصب گزینه‌های متداول Exchange Server 2010، یکبار دستورات زیر را در خط فرمان ویندوز سرور ۲۰۰۸ اجرا نمائید:

```
sc config NetTcpPortSharing start= auto
ServerManagerCmd -i RSAT-ADDS
ServerManagerCmd -i Web-Server
ServerManagerCmd -i Web-ISAPI-Ext
ServerManagerCmd -i Web-Metabase
ServerManagerCmd -i Web-Lgcy-Mgmt-Console
ServerManagerCmd -i Web-Basic-Auth
ServerManagerCmd -i Web-Digest-Auth
ServerManagerCmd -i Web-Windows-Auth
ServerManagerCmd -i Web-Dyn-Compression
ServerManagerCmd -i NET-HTTP-Activation
ServerManagerCmd -I RPC-over-HTTP-proxy
```

لازم به ذکر است که در صورت وجود هر یک از نقش‌های فوق، از دستور اجرا شده صرفنظر می‌گردد و اجرای مجدد آن‌ها مشکلی را برای سرور به وجود نخواهند آورد.

نکته ۱ – امکان ترکیب دستورات نصب

امکان ترکیب این دستورات به شکل یک دستور نیز وجود دارد و حالت کلی آن به صورت زیر است:

```
ServerManagerCMD –i <component-1> <component-2> .. <component-N>
```

برای مثال:

```
ServerManagerCmd -i RSAT-ADDS Web-Server Web-ISAPI-Ext Web-Metabase Web-Lgcy-Mgmt-Console Web-Basic-Auth Web-Digest-Auth Web-Windows-Auth Web-Dyn-Compression NET-HTTP-Activation RPC-over-HTTP-proxy
```

به صورت خلاصه جهت نصب هر یک از نقش‌های ذیل از بسته‌ی نرم افزاری Microsoft Exchange Server 2010 نیاز به اجرای فرامین ذکر شده می‌باشد:

Client Access Role

```
ServerManagerCmd -i Web-Server Web-Metabase Web-Lgcy-Mgmt-Console Web-Basic-Auth Web-Windows-Auth Web-Net-Ext Web-Digest-Auth Web-Dyn-Compression NET-HTTP-Activation Web-ISAPI-Ext RPC-over-HTTP-proxy RSAT-ADDS
```

Transport Role

```
ServerManagerCmd -i Web-Server Web-Metabase Web-Lgcy-Mgmt-Console Web-Basic-Auth Web-Windows-Auth Web-Net-Ext RSAT-ADDS
```

Mailbox Role

```
ServerManagerCmd -i Web-Server Web-Metabase Web-Lgcy-Mgmt-Console Web-
Basic-Auth Web-Windows-Auth Web-Net-Ext RSAT-ADDS
```

و اگر هر سه مورد را با هم بخواهیم نصب کنیم تنها کافی است پیش نیاز آن‌را به صورت ذیل در طی یک دستور مهیا نمائیم:

```
ServerManagerCmd -i Web-Server Web-Metabase Web-Lgcy-Mgmt-Console Web-
Basic-Auth Web-Windows-Auth Web-Net-Ext Web-Digest-Auth Web-Dyn-
Compression NET-HTTP-Activation Web-ISAPI-Ext RPC-over-HTTP-proxy RSAT-
ADDS
```

همانطور که در ابتدای فصل نیز ذکر شد، یک سری بسته‌ی نرم افزاری نیز باید پیش از فعال سازی این نقش‌ها نصب شود. برای مثال جهت نصب نقش Mailbox ، نصب MSFilter Pack یاد شده ضروری است.

پس از نصب نقش‌های ضروری ذکر شده، نیاز است تا سرور را یکبار راه اندازی مجدد نمائید.

نکته ۲ – استفاده از فایل‌های XML جهت نصب ساده‌ی نقش‌ها

اگر به DVD نصب Exchange Server 2010 مراجعه نمائید پوشه‌ی scripts آن‌را خواهید یافت. مواردی که در مورد نقش‌های مورد نیاز سرور به آن‌ها اشاره شد، به صورت یک سری فایل xml نیز در این پوشه قابل ملاحظه هستند. برای استفاده از آن‌ها باید به شکل زیر عمل کرد:

```
ServerManagerCMD –ip <XML file Name>
```

برای مثال اگر حالت متداول نصب Exchange Server 2010 را بخواهیم دنبال نمائیم تنها کافی است دستور زیر را در خط فرمان اجرا نمائیم (البته بدیهی است که مسیر صحیح فایل نیز باید وارد شود):

```
ServerManagerCMD –ip Exchange-typical.xml
```

جهت تکمیل این بخش، خلاصه نقش‌های متفاوتی که به این روش می‌توان نصب نمود به شرح ذیل است (ابتدا گزینه‌های مورد نظر ذکر شده و سپس خطوط فرمان مرتبط جهت نصب پیش‌نیازهای ضروری هر گزینه ارائه شده‌اند):

Client Access, Hub Transport, and the Mailbox role:

```
sc config NetTcpPortSharing start= auto
ServerManagerCmd -ip Exchange-Typical.xml -Restart
```

Client Access, Hub Transport, Mailbox, and Unified Messaging server roles:
```
sc config NetTcpPortSharing start= auto
ServerManagerCmd -i Desktop-Experience
ServerManagerCmd -ip Exchange-Typical.xml -Restart
```

Client Access and Hub Transport server roles:
```
sc config NetTcpPortSharing start= auto
ServerManagerCmd -ip Exchange-Typical.xml -Restart
```

Hub Transport and Mailbox server roles:
```
ServerManagerCmd -ip Exchange-Typical.xml -Restart
```

Client Access and Mailbox server roles:
```
sc config NetTcpPortSharing start= auto
ServerManagerCmd -ip Exchange-Typical.xml -Restart
```

Client Access role:
```
sc config NetTcpPortSharing start= auto
ServerManagerCmd -ip Exchange-CAS.xml -Restart
```

Hub Transport role:
```
ServerManagerCmd -ip Exchange-Hub.xml -Restart
```

Mailbox role:
```
ServerManagerCmd -ip Exchange-MBX.xml -Restart
```

Unified Messaging role:
```
ServerManagerCmd -ip Exchange-UM.xml -Restart
```

Edge Transport role:
```
ServerManagerCmd -ip Exchange-Edge.xml -Restart
```

نکته ۳ – استفاده از امکانات پاورشل

هر چند برنامه خط فرمان ServerManagerCMD بدون مشکل در تمامی نگارش‌های ویندوز سرور ۲۰۰۸ کار می‌کند، اما هر بار که آن‌را اجرا نمائیم در ابتدا با پیغام زیر مواجه خواهیم شد:

```
Servermanagercmd.exe is deprecated, and is not guaranteed to be supported
in future releases of Windows. We recommend that you use the Windows
PowerShell cmdlets that are available for Server Manager.
```

مطابق پیغام ارائه شده، احتمالا این برنامه خط فرمان در نگارش‌های بعدی ویندوز سرور پشتیبانی نشده و حذف خواهد شد. روش پیشنهادی مایکروسافت استفاده از دستورات PowerShell برای افزودن نقش‌های مورد نظر به ویندوز سرور می‌باشد. برای استفاده از PowerShell ویندوز، ابتدا پس از اجرای آن، باید دستور زیر را اجرا نمود:

```
Import-Module ServerManager
```

سپس بسته به گزینه‌های مورد نظر از بسته نرم افزاری Exchange Server 2010 یکی از دستورات ترکیبی زیر را باید اجرا نمود (حالت متداول، اولین دستور ترکیبی ذکر شده است):

Client Access, Hub Transport, and the Mailbox role:

```
Add-WindowsFeature NET-Framework,RSAT-ADDS,Web-Server,Web-Basic-Auth,Web-
Windows-Auth,Web-Metabase,Web-Net-Ext,Web-Lgcy-Mgmt-Console,WAS-Process-
Model,RSAT-Web-Server,Web-ISAPI-Ext,Web-Digest-Auth,Web-Dyn-
Compression,NET-HTTP-Activation,RPC-Over-HTTP-Proxy -Restart
```

Client Access, Hub Transport, Mailbox, and Unified Messaging server roles:

```
Add-WindowsFeature NET-Framework,RSAT-ADDS,Web-Server,Web-Basic-Auth,Web-
Windows-Auth,Web-Metabase,Web-Net-Ext,Web-Lgcy-Mgmt-Console,WAS-Process-
Model,RSAT-Web-Server,Web-ISAPI-Ext,Web-Digest-Auth,Web-Dyn-
Compression,NET-HTTP-Activation,RPC-Over-HTTP-Proxy,Desktop-Experience -
Restart
```

Client Access and Hub Transport server roles:

```
Add-WindowsFeature NET-Framework,RSAT-ADDS,Web-Server,Web-Basic-Auth,Web-
Windows-Auth,Web-Metabase,Web-Net-Ext,Web-Lgcy-Mgmt-Console,WAS-Process-
Model,RSAT-Web-Server,Web-ISAPI-Ext,Web-Digest-Auth,Web-Dyn-
Compression,NET-HTTP-Activation,RPC-Over-HTTP-Proxy -Restart
```

Hub Transport and Mailbox server roles:

```
Add-WindowsFeature NET-Framework,RSAT-ADDS,Web-Server,Web-Basic-Auth,Web-
Windows-Auth,Web-Metabase,Web-Net-Ext,Web-Lgcy-Mgmt-Console,WAS-Process-
Model,RSAT-Web-Server -Restart
```

Client Access and Mailbox server roles:

```
Add-WindowsFeature NET-Framework,RSAT-ADDS,Web-Server,Web-Basic-Auth,Web-
Windows-Auth,Web-Metabase,Web-Net-Ext,Web-Lgcy-Mgmt-Console,WAS-Process-
Model,RSAT-Web-Server,Web-ISAPI-Ext,Web-Digest-Auth,Web-Dyn-
Compression,NET-HTTP-Activation,RPC-Over-HTTP-Proxy -Restart
```

Client Access role:

```
Add-WindowsFeature NET-Framework,RSAT-ADDS,Web-Server,Web-Basic-Auth,Web-
Windows-Auth,Web-Metabase,Web-Net-Ext,Web-Lgcy-Mgmt-Console,WAS-Process-
Model,RSAT-Web-Server,Web-ISAPI-Ext,Web-Digest-Auth,Web-Dyn-
Compression,NET-HTTP-Activation,RPC-Over-HTTP-Proxy -Restart
```

Hub Transport or the Mailbox role:
```
Add-WindowsFeature NET-Framework,RSAT-ADDS,Web-Server,Web-Basic-Auth,Web-Windows-Auth,Web-Metabase,Web-Net-Ext,Web-Lgcy-Mgmt-Console,WAS-Process-Model,RSAT-Web-Server -Restart
```

Unified Messaging role:
```
Add-WindowsFeature NET-Framework,RSAT-ADDS,Web-Server,Web-Basic-Auth,Web-Windows-Auth,Web-Metabase,Web-Net-Ext,Web-Lgcy-Mgmt-Console,WAS-Process-Model,RSAT-Web-Server,Desktop-Experience -Restart
```

Edge Transport role:
```
Add-WindowsFeature NET-Framework,RSAT-ADDS,ADLDS -Restart
```

پس از نصب نقش‌های مورد نظر و راه اندازی مجدد سرور، دستور زیر را نیز در PowerShell اجرا نمائید تا Net.Tcp Port Sharing Service در حالت اجرای خودکار در هر بار راه اندازی مجدد سرور قرار گیرد:

```
Set-Service NetTcpPortSharing -StartupType Automatic
```

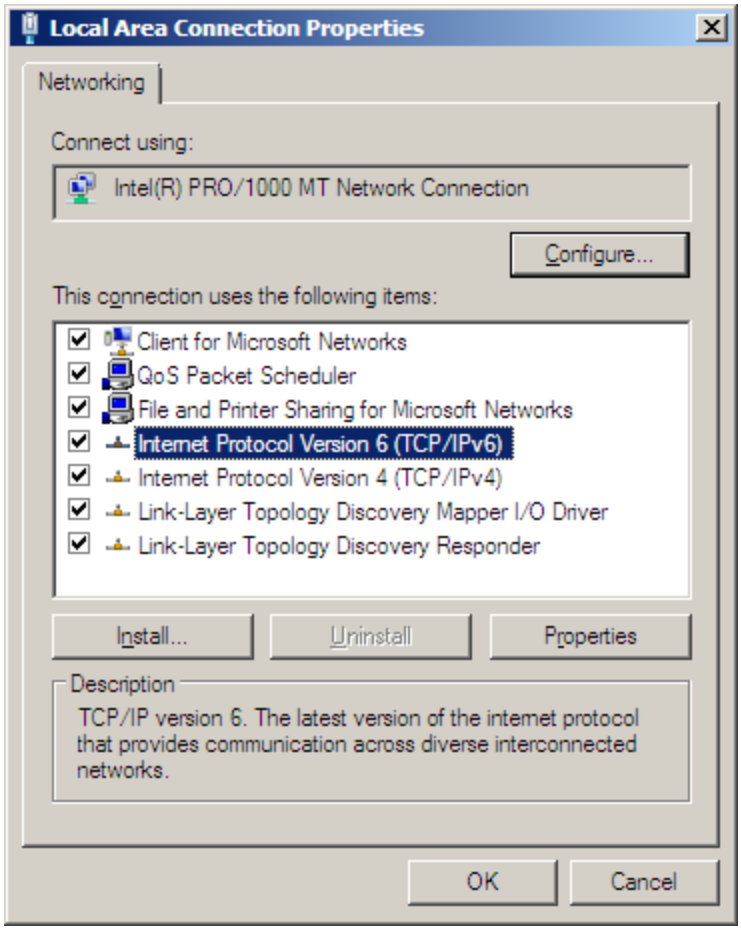
همچنین نصب نقش Windows Server Backup نیز توصیه می‌شود:
```
Add-WindowsFeature Backup-Features
```

غیرفعال سازی IPv6

احتمالا هنگام انجام تنظیمات شبکه ویندوز سرور خود، IPv6 را نیز غیرفعال کرده‌اید. لازم به ذکر است که IPv6 جزو الزامات نصب Exchange Server 2010 است و اگر آن‌را غیرفعال کرده باشید در حین نصب با خطای زیر متوقف خواهید شد:

```
Error:
The following error was generated when "$error.Clear(); if ($RoleStartTransportService) { start-SetupService -ServiceName MSExchangeTransport }" was run: "Service 'MSExchangeTransport' failed to reach status 'Running' on this server.".
Service 'MSExchangeTransport' failed to reach status 'Running' on this server.
```

برای رفع این مشکل مهم، ابتدا IPv6 را در قسمت Control Panel\Network and Internet\Network Connections فعال کنید (مطابق شکل بعد).



شکل ۷ – فعال سازی مجدد IPv6 در صورت غیرفعال بودن آن.

در ادامه برای غیرفعال سازی واقعی IPv6 باید کمی رجیستری ویندوز را تغییر داد. با کمک برنامه استاندارد RegEdit ویندوز به مسیر ذیل مراجعه کنید:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters

سپس در صفحه‌ی جزئیات آن کلیک راست کرده و مدخلی از نوع DWord سی و دو بیتی را به نام DisabledComponents ایجاد نمائید. بر روی آن دوبار کلیک کرده و مقدار آن‌را در حالت decimal مساوی ۴۲۹۴۹۶۷۲۹۵ وارد کنید (و یا FFFFFFFF در حالت Hexadecimal). سپس یکبار سرور را راه اندازی مجدد نمائید.

روش دیگر غیرفعال سازی صحیح IPv6 کمک گرفتن از برنامه Microsoft Fix It است که در آدرس ذیل قابل تهیه می‌باشد:

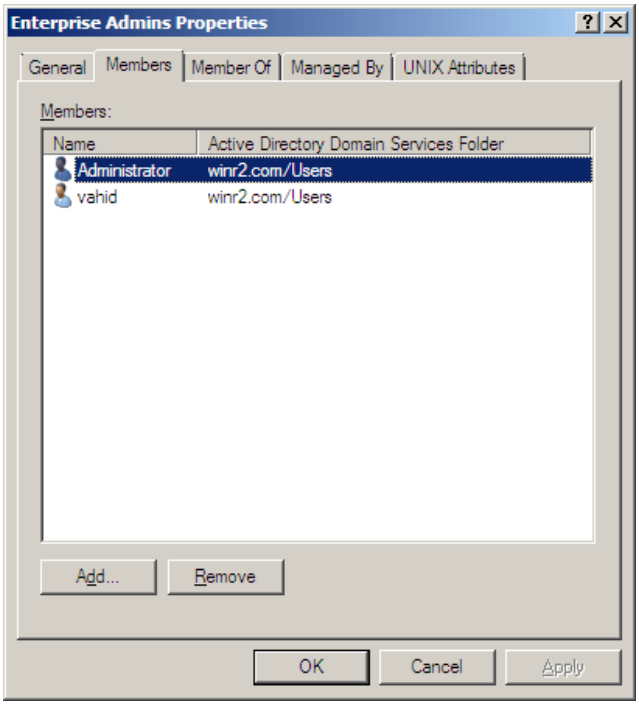
http://support.microsoft.com/kb/952842

نصب Exchange Server 2010 از طریق رابط گرافیکی

در ادامه‌ی این فصل دو روش را در مورد نصب Exchange Server 2010 از طریق رابط گرافیکی و سپس از طریق خط فرمان بررسی خواهیم کرد. هر دو روش به یک نتیجه منتهی شده و عموما روش‌های خط فرمان جهت اتوماسیون عملیات نصب مفید هستند.

تا اینجا فرض بر این است که بسته‌های پیش‌نیاز را نصب کرده‌اید و همچنین نقش‌های یاد شده را نیز به ویندوز سرور خود افزوده‌اید. علاوه بر آن، نکته‌ی مربوط به IPv6 را نیز باید رعایت نمائید. برای شروع به نصب بسته‌ی نرم افزاری Exchange Server 2010، کاربر وارد شده به سیستم باید جزو گروه Enterprise Admins یا Schema Admins باشد. اگر اینطور نیست، ابتدا کاربر مورد نظر خود را به این گروه‌ها افزوده (شکل ۸) و سپس یکبار Log off و Log in را نیز فراموش نکنید.

به صورت خلاصه جهت به روز رسانی Active directory ، برنامه نصاب باید تحت مجوز کاربری با حداقل سطح دسترسی Schema Administrators group به سیستم وارد شده باشد. همچنین جهت نصب Exchange server 2010 در یک Organization باید کاربر وارد شده به سیستم دارای حداقل دسترسی Enterprise Administrators نیز باشد.



شکل ۸– برنامه نصاب بسته نرم افزاری Exchange Server 2010 باید تحت مجوز یکی از کاربران گروه Enterprise Admins اجرا شود.

اکنون DVD بسته نرم افزاری Exchange Server 2010 را گشوده و فایل setup آن‌را اجرا نمائید. مراحل نصب با کمک رابط گرافیکی به شرح زیر هستند (شکل‌های ۹ تا ۲۳):

۱- در صفحه‌ی خوش آمد گویی اولیه بر روی دکمه Next کلیک نمائید تا به صفحه‌ی انتخاب زبان رهنمون شوید. در این صفحه یا می‌توانید گزینه دریافت و نصب آخرین فایل‌های زبان تهیه شده از اینترنت و سایت مایکروسافت را انتخاب کنید و یا گزینه‌ی آخر را انتخاب نموده و به زبان‌های موجود در DVD نصب بسنده نمائید. سپس بر روی دکمه Next کلیک کنید.

۲- در صفحه بعدی، توافقنامه ارائه شده را پذیرفته و بر روی دکمه Next کلیک نمائید.

۳- برنامه‌ی نصاب در ادامه از شما در مورد امکان گزارش خطاها به مایکروسافت سؤال خواهد نمود. بسته به نظر خود یکی از گزینه‌های بلی یا خیر را انتخاب کنید و سپس بر روی دکمه Next کلیک کنید.

۴- اکنون به مهمترین صفحه‌ی انتخاب نوع نصب برنامه رسیده‌ایم. اگر حالت معمول را انتخاب کنید نقش‌های Hub Transport، Client Access و Mailbox Server نصب خواهند شد. اگر حالت سفارشی نصب را انتخاب کنید، می‌توان بسته به نیاز، نقش‌های متفاوتی را انتخاب نمود. در حالت پیش فرض معمول، امکان انتخاب نقش Unified Messaging Server که جهت فعال سازی Voice mail کاربرد دارد، وجود ندارد و این نقش را تنها در حالت سفارشی می‌توان انتخاب نمود. حالت پیش فرض را پذیرفته و بر روی دکمه Next کلیک کنید. هر زمانیکه نیاز به نصب نقش دیگری نیز وجود داشت می‌توان مجددا برنامه نصاب را اجرا کرده و در حالت سفارشی نقش مورد نظر را افزود و از این لحاظ محدودیتی وجود ندارد. سپس بر روی دکمه Next کلیک کنید.

۵- در صفحه‌ی بعدی ارائه شده، نام organization مورد نظر پرسیده می‌شود. این نام محدودیت‌های ذیل را دارد:

- باید از حروف A تا Z (کوچک یا بزرگ) تشکیل شده باشد.
- می‌تواند شامل اعداد هم باشد.
- اگر از فاصله جهت معرفی کلمات کمک گرفتید باید آن‌ها را بین علائم نقل قول قرار دهید.
- امکان بکارگیری خط تیره (dash) نیز وجود دارد.

۶- در صفحه بعدی در مورد کاربرانی که به این میل سرور متصل خواهند شد سؤال پرسیده می‌شود. آیا در شبکه خود کاربری را دارید که هنوز از Outlook 2003 استفاده می‌کند؟ اگر پاسخ بلی است باید در اینجا گزینه Yes را انتخاب نمائید تا public folder database مخصوص این کاربران در Exchange server ساخته شود (در غیر اینصورت این کاربران امکان استفاده از میل سرور را نخواهند داشت). هر چند این بانک اطلاعاتی را پس از نصب نیز می‌توان افزود.

۷- اگر نقش Client Access server را انتخاب کرده باشید، اکنون در مورد اینکه آیا این سرور بر روی اینترنت نیز قرار خواهد گرفت یا خیر سؤال پرسیده می‌شود. در صورتی که قصد استفاده از این میل سرور را در

اینترنت نیز داشته باشید، نام domain مورد نظر خود را در اینجا وارد نمائید (برای مثال mail.mysite.com).

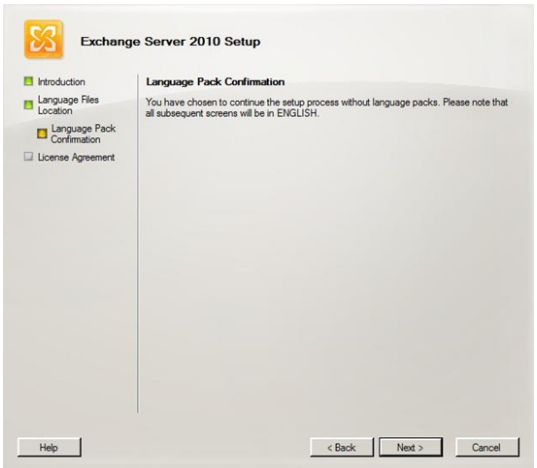
۸- در ادامه یک سری سؤال عمومی در مورد نوع شرکت شما و امکان به اشتراک گذاری اطلاعاتی از این دست سؤال پرسیده می‌شود.

۹- اکنون بر روی دکمه ادامه کلیک کنید. در ابتدا پیش نیازهای نصب بررسی می‌شوند. اگر هر موردی را رعایت نکرده باشید ابتدا به شما پیغام لازم جهت رفع آن‌ها داده خواهد شد. سپس عملیات نصب صورت خواهد گرفت.

شکل ۹- صفحه‌ی آغازین نصب

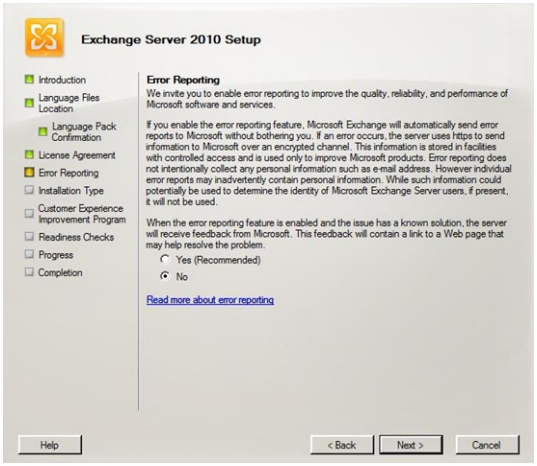
شکل ۱۰ – صفحه‌ی معرفی محصول

شکل ۱۱ – صفحه‌ی انتخاب زبان‌ها



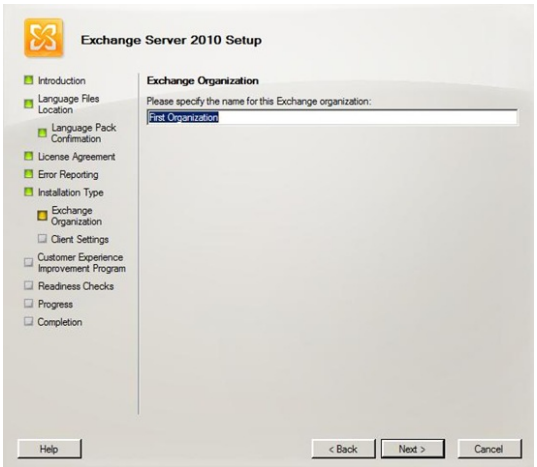
شکل۱۲- صفحه‌ی نصب زبان‌ها

شکل ۱۳– صفحه‌ی پذیرش توافقنامه

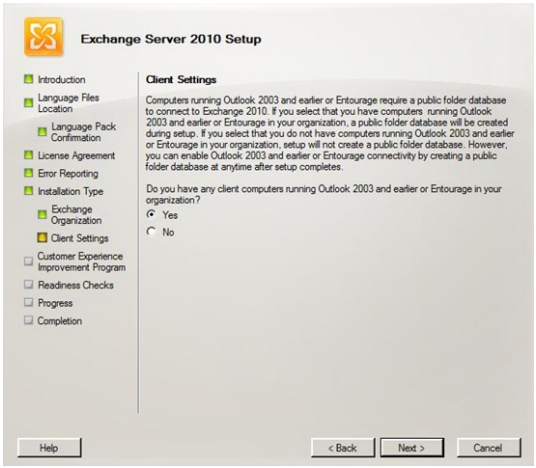


شکل ۱۴– صفحه‌ی پذیرش گزارش خطاها به مایکروسافت

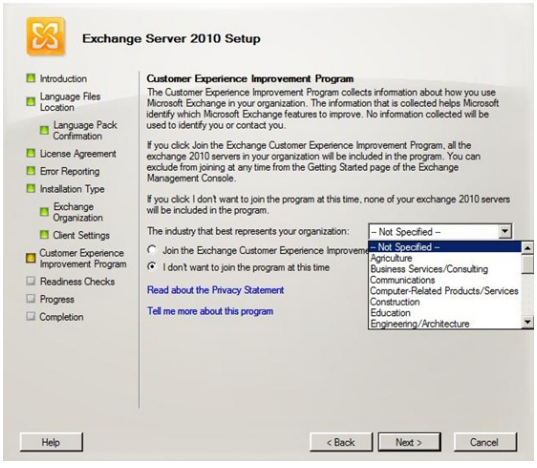
شکل ۱۵ – صفحه‌ی انتخاب نقش‌ها برای نصب



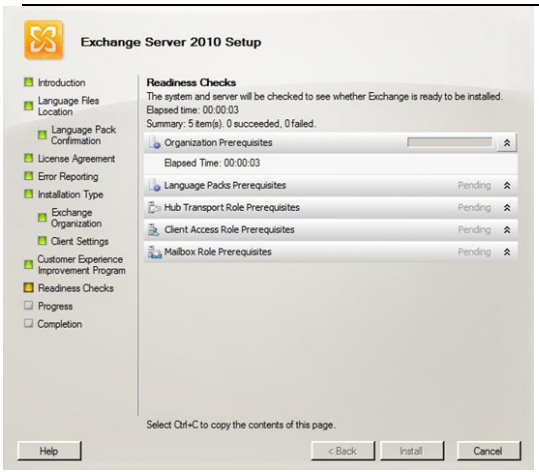
شکل ۱۶ – صفحه‌ی ورود نام ارگان



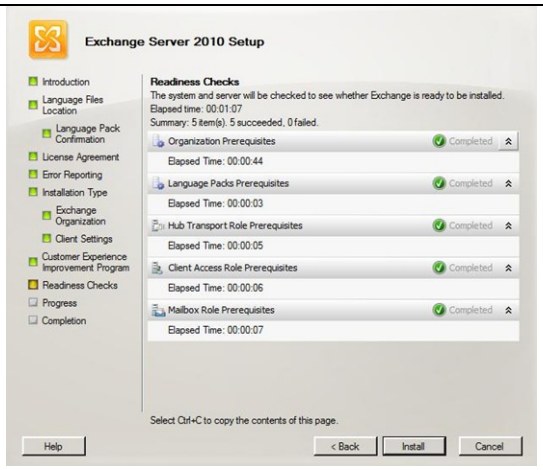
شکل ۱۷ – مخصوص کاربران Outlook 2003



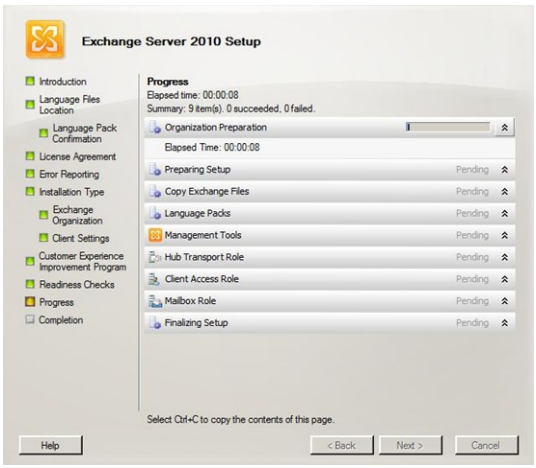
شکل ۱۸ – انتخاب نوع سازمان شما



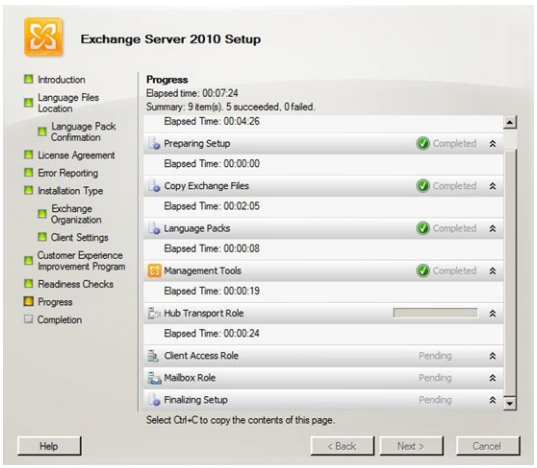
شکل ۱۹ – بررسی پیش نیازهای نصب



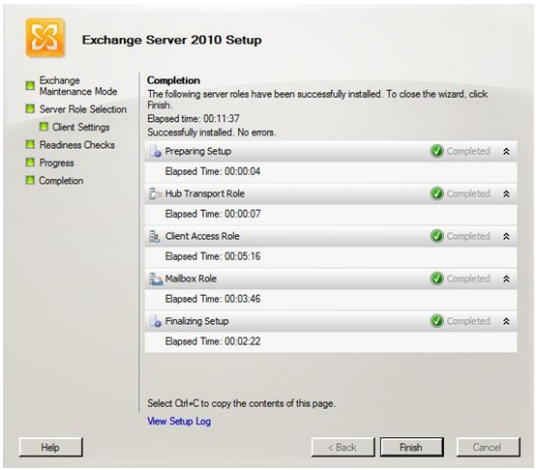
شکل ۲۰ – پایان بررسی پیش نیازهای نصب



شکل ۲۱ – شروع به نصب نقش‌های انتخابی



شکل ۲۲ – مراحل نصب نقش‌های انتخابی



شکل ۲۳ – پایان عملیات نصب

نصب Exchange Server 2010 از طریق خط فرمان

در این قسمت نیز فرض بر آن است که پیش‌نیازهای نصب را رعایت کرده‌اید. اکنون نصب بسته نرم افزاری Exchange Server 2010 از طریق خط فرمان به سادگی اجرای چند فرمان ذیل می‌باشد:

الف) آماده سازی Active directory

فایل setup بسته نرم افزاری را بر روی DVD این محصول یافته و سپس از طریق آن یکی از دو دستور زیر را که معادل می‌باشند اجرا نمائید:

```
Setup /PrepareSchema
Setup /ps
```

به این صورت کار آماده سازی Schema مربوط به Active directory جهت نصب Exchange Server 2010 انجام خواهد شد.

ب) آماده سازی Domain و Organization

در ادامه یکی از دو دستور معادل زیر را جهت آماده سازی domain خود اجرا نمائید:

```
Setup /p /on:myOrganizationName
Setup /PrepareAD /OrganizationName:myOrganizationName
```

myOrganizationName دلخواه ذکر شده در این خط فرمان (همانند قسمت ۵ روش استفاده از رابط گرافیکی نصب)، به بانک اطلاعاتی Active directory شما اضافه خواهد شد.

ج) نصب نهایی بسته نرم افزاری Exchange Server 2010

```
setup /m:install /r:H C M
setup /mode:install /roles:ht,ca,mb
```

دستور خط فرمان فوق (دو سطر ذکر شده در حقیقت یک دستور هستند و صرفا جهت تکمیل بحث ارائه شدند)، کار نصب سه نقش transport ، client access و mailbox را به صورت خودکار انجام خواهد داد که توضیحات پارامترهای آن به شرح زیر است:

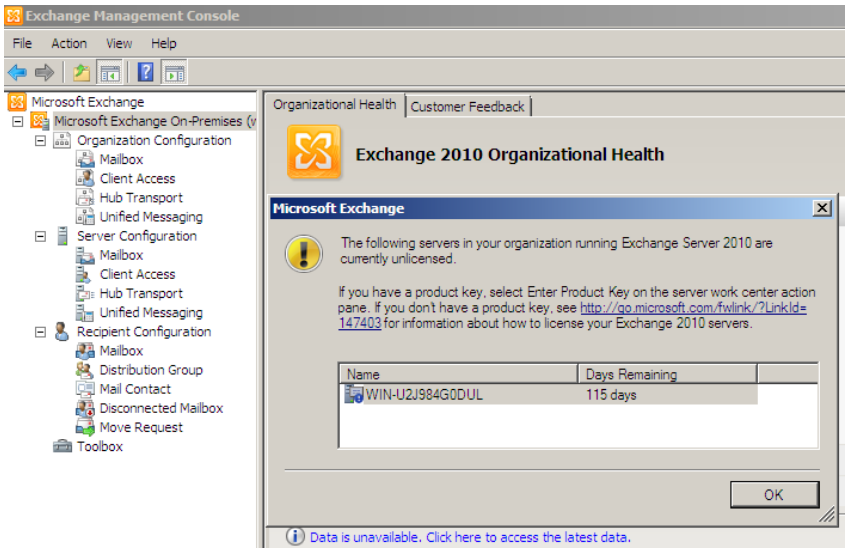
```
/m = /mode
/r = /role, /roles
H = Transport
C = Client Access
M = Mailbox
```

سپس مدتی منتظر بمانید تا عملیات نصب پایان یابد.

همانطور که ملاحظه می‌کنید از خلاصه فرامین خط فرمان ذکر شده در این فصل می‌توان یک `.bat` فایل تهیه کرد و سپس کار نصب این مجموعه را با سهولت هر چه تمامتر انجام داد.

بررسی صحت عملیات نصب `Exchange server 2010`

پس از پایان عملیات نصب، `Exchange management console` را اجرا نمائید (شکل ۲۴). در اولین بار اجرای این `console` ، پیغام وارد کردن کلید معتبر برنامه را دریافت خواهید کرد.



شکل ۲۴– تصویری از اولین اجرای `Exchange management console` .

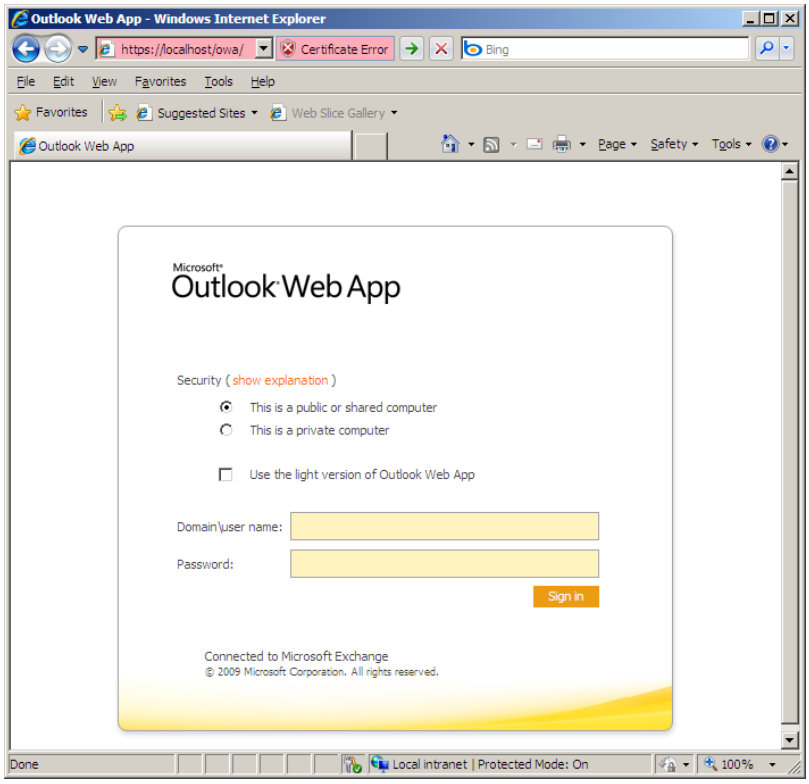
جهت اطلاع، قیمت‌های نگارش‌های مختلف این برنامه به شرح زیر است:

Exchange Servers	Prices
Exchange Server 2010 Standard Edition	$699 US
Exchange Server 2010 Enterprise Edition	$3,999 US

مهم‌ترین تفاوت نگارش‌های `standard` و `enterprise` در تعداد دیتابیس‌هایی است که پشتیبانی می‌کنند. نگارش `standard` از یک تا ۵ دیتابیس و نگارش سازمانی از یک تا ۱۰۰ دیتابیس را پشتیبانی می‌کنند. همچنین این محصول بر اساس نوع کلید معتبری که وارد خواهید کرد به صورت استاندارد و یا نگارش سازمانی شناخته خواهد شد.

علاوه بر این می‌توان جهت بررسی صحت نصب، در مرورگر خود برای گشودن برنامه Outlook web access آدرس زیر را وارد نمود (شکل ۲۵):

https://localhost/owa



شکل ۲۵– نمایی از Outlook web access پس از نصب اولیه Exchange Server 2010 .

همانطور که مشاهده می‌کنید، به همراه این بسته نرم افزاری، امکان مرور کردن ایمیل‌های دریافتی از طریق یک برنامه‌ی تحت وب به نام Outlook web access نیز میسر است و در این حالت کاربران شما در شبکه نیاز به نصب هیچگونه برنامه خاصی جهت دریافت و یا ارسال ایمیل‌ها نخواهند داشت؛ هر چند بهترین کارآیی را با برنامه Outlook 2007 و یا نگارش‌های بالاتر آن مشاهده خواهید کرد.

Outlook web access برنامه‌ی تهیه شده‌ای با کمک ASP.Net است (به همین جهت نیاز به نصب نقش وب سرور IIS وجود داشت) که اعتبار سنجی آن از نوع Windows Authentication یکپارچه با Active directory می‌باشد.

نحوه‌ی ورود کلید معتبر Exchange server 2010

پس از تهیه کلید معتبر خود، جهت ورود آن به برنامه به یکی از دو طریق زیر می‌توانید عمل کنید:

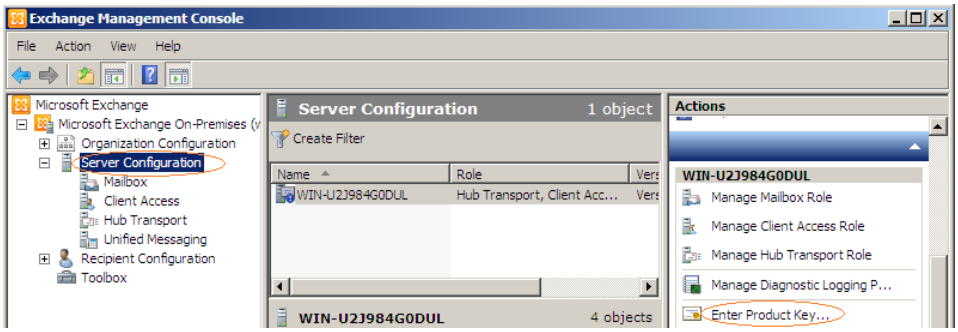
الف) استفاده از دستورات خط فرمان PowerShell به صورت زیر:

```
Set-ExchangeServer -Identity ExServer01 -ProductKey aaaaa-aaaaa-aaaaa-aaaaa-aaaaa
```

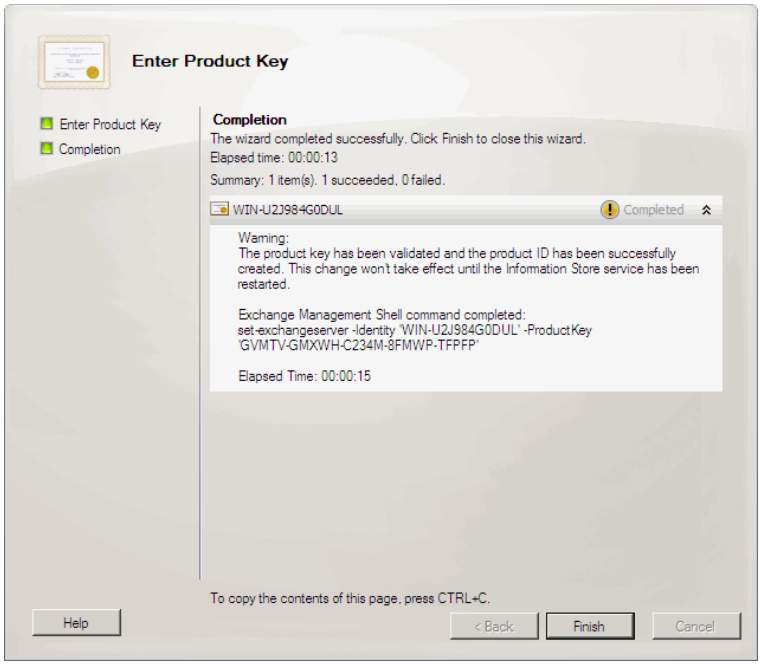
ب) استفاده از Exchange management console به ترتیب ذیل:

۱- به قسمت Server Configuration مراجعه نمائید.

۲- در قسمت actions سمت راست صفحه، بر روی Enter Product Key Group کلیک کنید (شکل ۲۶) تا صفحه ورود کلید معتبر برنامه ظاهر شود.



شکل ۲۶- نحوه‌ی ورود کلید معتبر محصول با استفاده از رابط گرافیکی.



شکل ۲۷- پیغام راه اندازی مجدد سرویس Information store پس از ورود سریال محصول.

مطابق شکل ۲۷، پس از ورود کلید معتبر خود، یکبار باید سرویس Information store را راه اندازی مجدد نمود (مراجعه به کنسول سرویس‌های ویندوز، یافتن سرویس Microsoft Exchange Information Store و راه اندازی مجدد آن).

مشکلاتی که ممکن است حین نصب Exchange server 2010 با آن مواجه شوید

شایع‌ترین مشکلات نصب Exchange server 2010 به شرح زیر هستند:

- کمبود فضای کافی بر روی دیسک سخت جهت نصب برنامه
- عدم رعایت پیش‌نیازهای لازم ذکر شده در ابتدای فصل
- غیرفعال کردن IPv6 بر روی ویندوز سرور ۲۰۰۸ به صورت نادرست
- مشکلات تنظیمات DNS در شبکه
- تنظیم نبودن Domain functional level به صورت صحیح (که در قسمت پیش نیازهای Active directory در ابتدای فصل توضیح داده شد)
- اجرای برنامه‌ی نصاب تحت مجوز کاربری که دسترسی لازم را برای انجام تغییرات ندارد (این کاربر باید جزو گروه‌های domain admins ، schema admins و enterprise admins باشد)

فصل ۳ – مدیریت و تنظیمات Mailbox servers

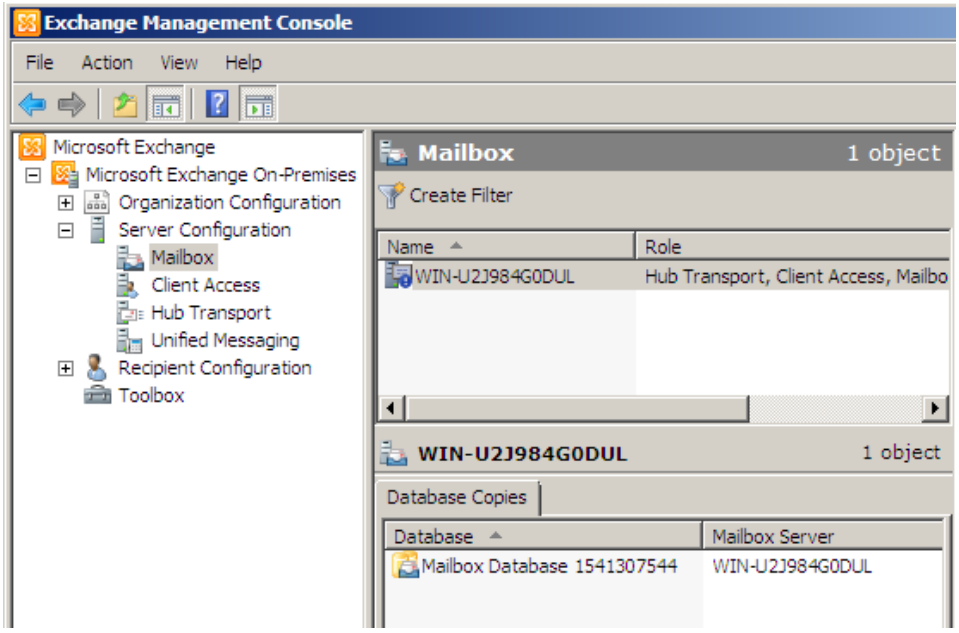
پس از انجام عملیات ابتدایی نصب Microsoft Exchange server ، نیاز به انجام تنظیمات Mailbox servers می‌باشد. این تنظیمات شامل موارد ذیل هستند:

- ایجاد و تنظیم گروه‌های ذخیره سازی اطلاعات (storage groups)
- تنظیم نمودن public folders
- تنظیمات امنیتی Mailbox server
- تنظیم کردن صندوق‌های پستی کاربران
- انجام تنظیمات دفترچه آدرس‌های آفلاین (offline address book)

در ادامه به بررسی هر کدام از این موارد خواهیم پرداخت.

گروه‌های ذخیره سازی اطلاعات

در Exchange server ، اطلاعات ایمیل‌های کاربران در سروری که نقش Mailbox server بر روی آن نصب شده است ذخیره می‌گردد (شکل ۱).



شکل ۱– بانک اطلاعاتی پیش فرض ذخیره سازی اطلاعات Mailbox server.

Mailbox server از بانک‌های اطلاعاتی جهت مدیریت موارد زیر کمک می‌گیرد:

- اطلاعات صندوق‌های پستی کاربران
- اطلاعات پوشه‌های عمومی (public folders)
  - پوشه‌های عمومی برای کاربران Outlook 2003 و قبل از آن ضروری است (ترکیب Outlook 2007 به بعد و Exchange 2010 نیازی به این نوع پوشه‌ها ندارند). در این پوشه‌های عمومی موارد ذیل ذخیره می‌شوند:
    - اطلاعات دفترچه آدرس‌های آفلاین (offline address book)
    - اطلاعات تعریف شده در تقویم‌های مربوط به زمان‌های آزاد و بسته‌ی کاربران

تمام این اطلاعات در فایلی با پسوند edb ذخیره می‌گردد. پیشنهاد مایکروسافت به عنوان جایگزین پوشه‌های عمومی در هنگام ترکیب Outlook 2007 به بعد و Exchange 2010 ، استفاده از SharePoint می‌باشد. توسط SharePoint، به اشتراک گذاری اطلاعاتی همانند اسناد، اطلاعات و رخ دادهای تعریف شده در تقویم‌ها، وظایف و غیره به شکل سازمان یافته‌تری میسر است و همچنین این محصول قابلیت یکپارچگی کاملی را با محصولات مجموعه آفیس مایکروسافت منجمله Outlook دارد.

در هنگام نصب اولیه Exchange server ، اولین گروه ذخیره سازی اطلاعات به صورت خودکار ایجاد می‌گردد. اگر از این بانک اطلاعاتی جهت مدیریت صدها کاربر استفاده شود، به زودی با بانک اطلاعاتی بسیار حجیمی مواجه خواهید شد.

اگر از نگارش استاندارد Exchange server استفاده نمائید، حداکثر تا ۵ گروه ذخیره سازی اطلاعات را می‌توان تعریف نمود و حداکثر ۵ بانک اطلاعاتی قابل ایجاد هستند. این مورد در نگارش سازمانی به ۱۰۰ بانک اطلاعاتی افزایش یافته است (در Exchange server 2007 سازمانی این مورد حداکثر تا ۵۰ بانک اطلاعاتی قابل تنظیم بود). در هر دو نگارش سازمانی و استاندارد محدودیتی در مورد حجم بانک‌های اطلاعاتی وجود ندارد.

با ایجاد گروه‌های مختلف ذخیره سازی اطلاعات، با توجه به امکان تعریف صندوق‌های پستی مجزا برای هر کاربر بر روی هر کدام از آن‌ها، دیگر با یک بانک اطلاعاتی عظیم اولیه مواجه نبوده و تهیه پشتیبان و همچنین بازیابی اطلاعات مربوطه نیز بسیار ساده‌تر خواهد شد. همچنین اگر یکی از این بانک‌های اطلاعاتی از کار بیفتد تنها قسمتی از سازمان شما متاثر خواهند شد و نه تمامی افراد دارای صندوق پستی در Exchange server .

فایل‌های تشکیل دهنده‌ی یک گروه ذخیره سازی اطلاعات

جهت مشاهده‌ی محل قرارگیری بانک اطلاعاتی پیش فرض ایجاد شده می‌توان به مسیر زیر مراجعه کرد:

```
C:\Program Files\Microsoft\Exchange Server\V14\Mailbox\Mailbox Database (number)
```

در این پوشه می‌توان فایل edb بانک اطلاعاتی مورد نظر را یافت؛ همچنین فایل‌های log تراکنش‌های صورت گرفته در سرور را نیز می‌توان در این پوشه مشاهده کرد. علاوه بر آن فایلی با پسوند chk که معرف checkpoint file است را مشاهده خواهید کرد. فایل‌های دیگر موجود در این پوشه با پسوند jrs از نوع reserved transaction logs هستند. اگر بر روی درایو جاری، دیگر فضای خالی باقی نمانده باشد، می‌توان این دو فایل را که صرفا مقداری فضای خالی را رزرو کرده‌اند، حذف نمود.

فایل temp.edb موجود در پوشه بانک اطلاعاتی صندوق‌های پستی، فضایی است موقتی جهت ثبت تراکنش‌های صورت گرفته و هر بار هنگام از سرگیری مجدد Exchange server حذف شده و مجددا ایجاد خواهد شد.

توصیه‌هایی جهت عملکرد بهینه گروه‌های ذخیره سازی اطلاعات

- فایل‌های لاگ مربوط به تراکنش‌ها بهتر است بر روی دیسک سختی دیگر و یا حتی درایوی دیگر قرار گیرند. این مورد جهت بهینه سازی سرعت خواندن و نوشتن اطلاعات بر روی دیسک سخت ضروری است.
- فایل‌های بانک اطلاعاتی برنامه و سیستم عامل بهتر است بر روی درایوهای مجزایی قرار داشته باشند.
- سیاست صحیحی را در مورد پیاده سازی مباحث RAID اعمال نمائید.
  - RAID 0 با توجه به نوشتن و خواندن اطلاعات بر روی دو سخت دیسک مجزا (قسمتی از یک اطلاعات مشخص بر روی دیسک اول و قسمتی دیگر از همان اطلاعات بر روی دیسک دوم قرار می‌گیرد)، سرعت بالایی را از لحاظ مباحث IO به همراه خواهد آورد؛ اما اگر یکی از سخت دیسک‌ها دچار مشکل شود، اطلاعات دیسک دیگر نیز قابل استفاده نخواهد بود.
  - RAID 1 یک فایل را بر روی دو دیسک سخت خواهد نوشت. این روش بهبود سرعتی را در خواندن و نوشتن اطلاعات به همراه نخواهد داشت اما با از دست دادن یکی از دیسک‌های سخت، دیسک دوم بدون مشکل قادر به ادامه کار و نجات سازمان خواهد شد.
  - RAID 5 حداقل به سه دیسک سخت نیاز خواهد داشت. در این حالت در صورت از دست دادن یکی از دیسک‌های سخت، دو دیسک دیگر قادر به بازسازی اطلاعات بر اساس اطلاعات ویژه‌ای که از یکدیگر دارند خواهند شد.

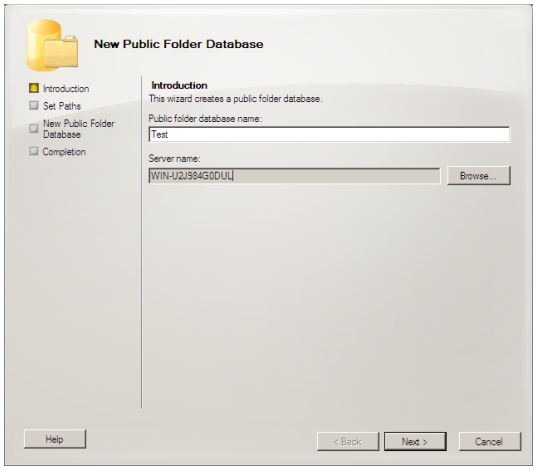
- همچنین امکان ترکیب این موارد نیز وجود دارد برای مثال RAID 0+1 ، RAID 5+1 و RAID 1+0.

- توصیه مایکروسافت، استفاده از SAN (storage area networks) جهت ذخیره سازی اطلاعات بانک‌های اطلاعاتی Exchange server می‌باشد.

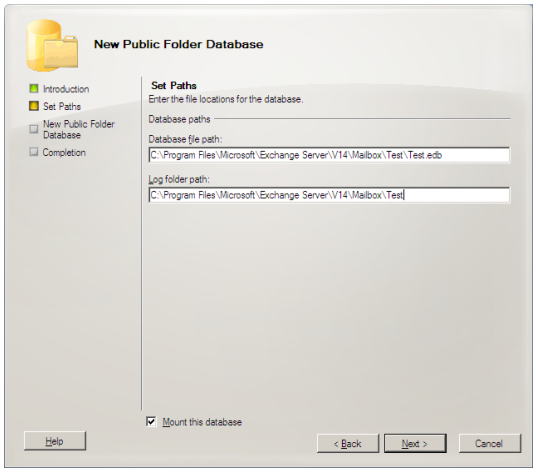
مدیریت پوشه‌های عمومی در Exchange 2010

اگر در حین نصب، به سؤال آیا در سازمان شما هنوز از Outlook 2003 استفاده می‌شود پاسخ منفی داده باشید، پوشه عمومی (public folder) پیش فرض ایجاد نخواهد شد. هر چند این پوشه عمومی را پس از نصب نیز می‌توان ایجاد کرد.

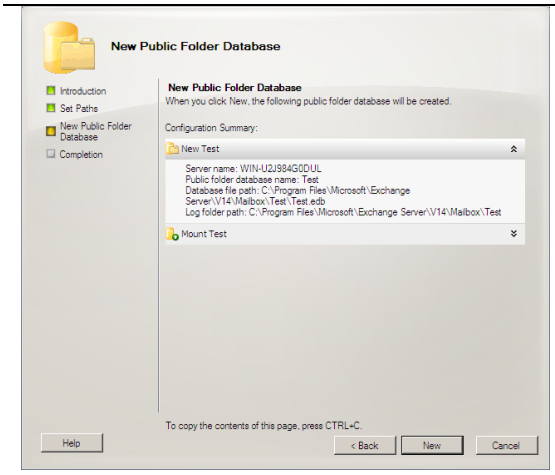
برای ایجاد بانک اطلاعاتی پوشه عمومی به Organization Configuration > Mailbox مراجعه کنید. سپس در برگه‌ی actions در سمت راست صفحه، بر روی گزینه New Public Folder Database کلیک نمائید. در صفحه‌ی ظاهر شده، نامی دلخواه را وارد کرده، سپس بر روی دکمه browse کلیک نمائید تا سرور mailbox را بتوان انتخاب نمود. در ادامه مسیر قرار گیری بانک اطلاعات و فایل‌های لاگ آن پرسیده می‌شود. همانطور که پیشتر نیز ذکر شد، جهت کارآیی بیشتر سیستم بهتر است این دو مسیر حداقل بر روی دو درایو مجزا از هم تعریف شوند. در صفحه بعد بر روی دکمه New کلیک کرده تا بانک اطلاعاتی پوشه‌های عمومی ایجاد گردد (شکل‌های ۲ تا ۴).



شکل ۲– ایجاد یک پوشه عمومی جدید

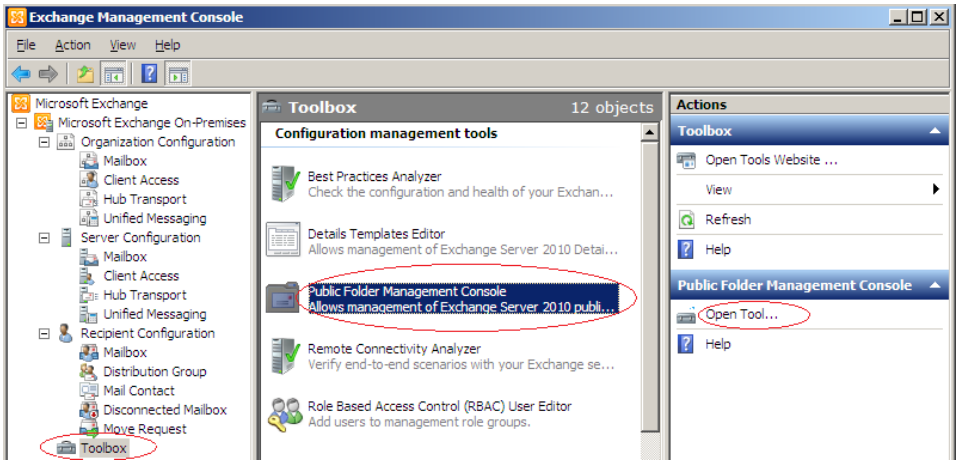


شکل ۳– تعیین مسیرهای فایل‌های مورد نیاز



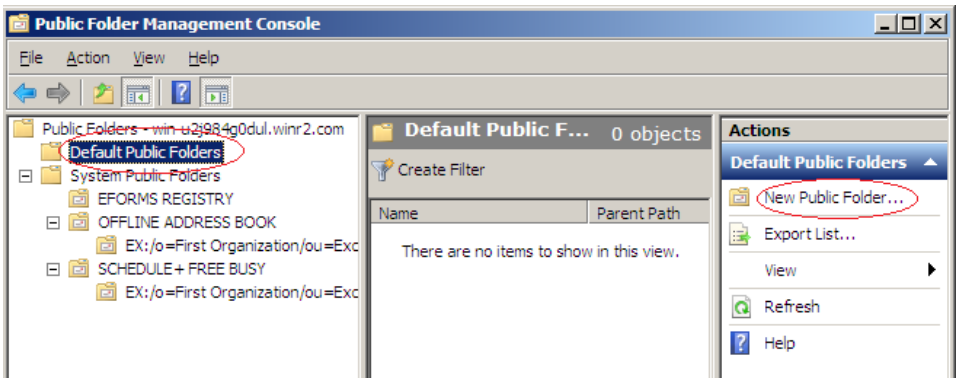
شکل ۴– کلیک بر روی new جهت ایجاد بانک اطلاعاتی پوشه‌های عمومی

برای مدیریت public folders باید در management console به قسمت toolbox آن مراجعه کرده و سپس در قسمت management tools گزینه configuration public folder management console را یافته و بر روی آن کلیک راست کرده و گزینه open tool را انتخاب کنید. یا همین گزینه در برگه actions سمت راست صفحه نیز قابل مشاهده و دسترسی است (شکل ۵).



شکل ۵– نحوه دسترسی به کنسول مدیریتی پوشه‌های عمومی.

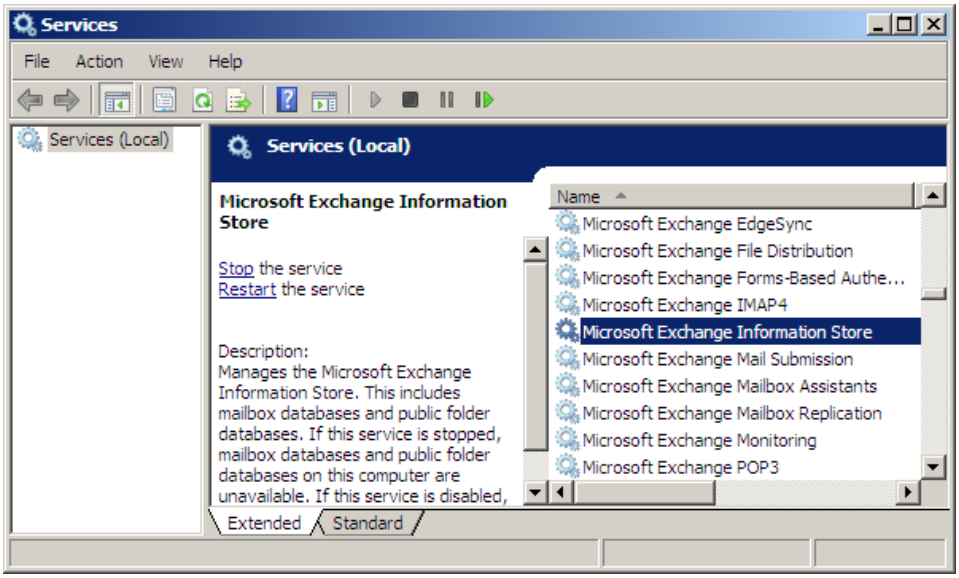
اکنون کنسول مدیریتی پوشه‌های عمومی ظاهر خواهد شد (شکل ۶) که در آن قسمت دفترچه‌ی آدرس‌های آفلاین و تنظیمات تقویم‌ها در مورد ساعات آزاد و مشغول پرسنل تنظیم شده در Outlook مشخص است.



شکل ۶– کنسول مدیریتی پوشه‌های عمومی.

در این کنسول، default public folder را انتخاب کرده و سپس از برگه‌ی actions در سمت راست صفحه، گزینه‌ی new public folder را انتخاب کنید. در صفحه‌ی ظاهر شده نام دلخواهی را وارد کرده و بر روی دکمه new کلیک نمائید تا پوشه‌ی عمومی جدیدی ایجاد گردد. پس از ایجاد این پوشه جدید، با کلیک بر روی آن و انتخاب گزینه‌ی خواص، می‌توان مباحثی مانند حد مجاز استفاده، replication و غیره را تنظیم نمود.

لازم به ذکر می‌باشد که پس از طی مراحل فوق نیاز است تا سرویس Microsoft Exchange Information Store را یکبار متوقف و سپس راه اندازی مجدد نمود (شکل ۷).



شکل ۷– راه اندازی مجدد سرویس Microsoft Exchange Information Store پس از انجام تنظیمات پوشه‌های عمومی

مدیریت صندوق‌های پستی کاربران در Exchange 2010

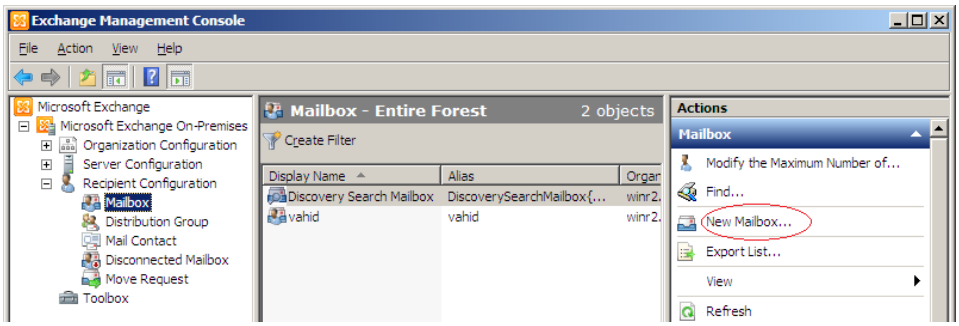
ارسال و دریافت کنندگان ایمیل در Exchange server به گروه‌های زیر تقسیم می‌شوند:

- Mailbox users : کاربرانی هستند که دارای یک حساب کاربری در Active directory می‌باشند و یک صندوق پستی Exchange برای آن‌ها تعریف شده است و آدرس ایمیل آن‌ها نیز داخلی است.
- Mail-Enabled users : این نوع کاربران نیز دارای یک حساب کاربری در Active directory هستند اما آدرس ایمیل آن‌ها متعلق است به خارج از مجموعه. عموما کاربران بخش امور مالی نیازمند اینگونه تنظیمات هستند.
- Resource mailbox : این نوع صندوق‌های پستی برای منابعی مانند اطاق‌های کنفرانس و امثال آن طراحی شده‌اند.
- Mail contacts : بر اساس اشیاء Contact تعریف شده در Active directory کار می‌کنند که می‌توانند دارای ایمیل‌هایی متعلق به خارج از سازمان نیز باشند.
- Distribution groups : مجموعه‌ای از کاربران، گروه‌ها و ارتباطات را تشکیل می‌دهند. به عبارت دیگر هنگامیکه که ایمیلی به این گروه ارسال می‌شود، این ایمیل به تمامی اعضای گروه به صورت خودکار هدایت خواهد شد.
- Linked mailbox : ممکن است تعدادی از کاربران شما در یک Active directory forest مجزا قرار داشته باشند که به این صورت می‌توان با آنان ارتباط برقرار ساخت.

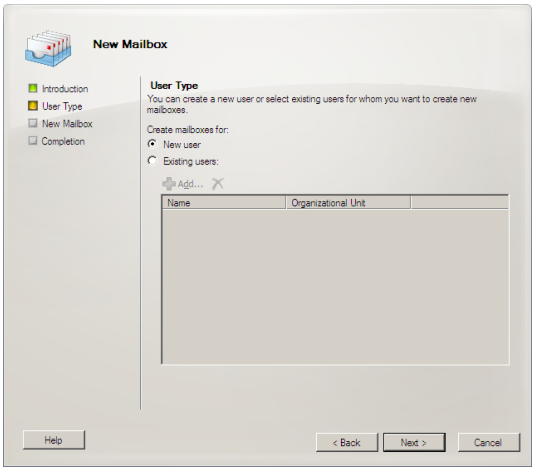
نحوه‌ی ایجاد و حذف صندوق‌های پستی در Exchange 2010

برای ایجاد و حذف صندوق‌های پستی در Exchange 2010 روش‌های گوناگونی وجود دارد که ساده‌ترین آن‌ها مراجعه به Management console قسمت recipients configuration گزینه mailbox می‌باشد (شکل ۸).

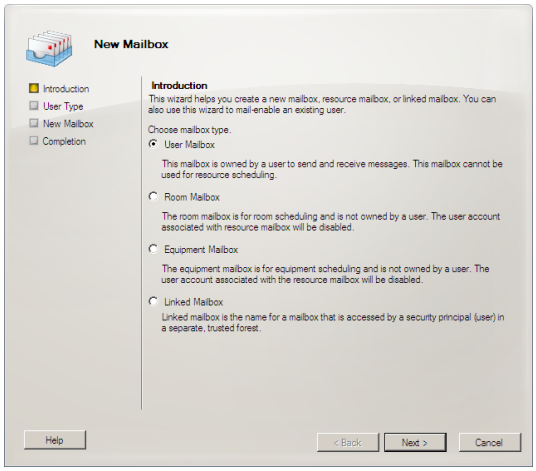
پس از ورود به قسمت مدیریت صندوق‌های پستی ارسال و دریافت کنندگان ایمیل، جهت ایجاد یک صندوق پستی جدید، بر روی لینک New mailbox در برگه actions سمت راست صفحه کلیک نمائید. در این برگه می‌توان کاربری جدید را در Active directory تعریف و یا برای کاربری موجود صندوق پستی تعریف نمود.



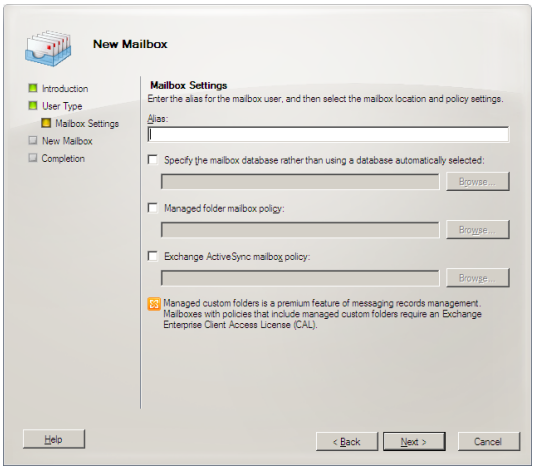
شکل ۸– کنسول مدیریتی Exchange 2010 و ایجاد یک صندوق پستی جدید



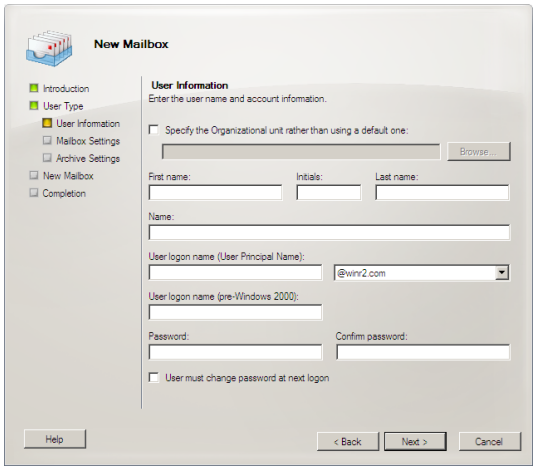
شکل ۱۰– ایجاد صندوق پستی برای کاربری موجود و یا ایجاد یک کاربر جدید و سپس ایجاد صندوق پستی برای او



شکل ۹– شروع به ایجاد یک صندوق پستی جدید



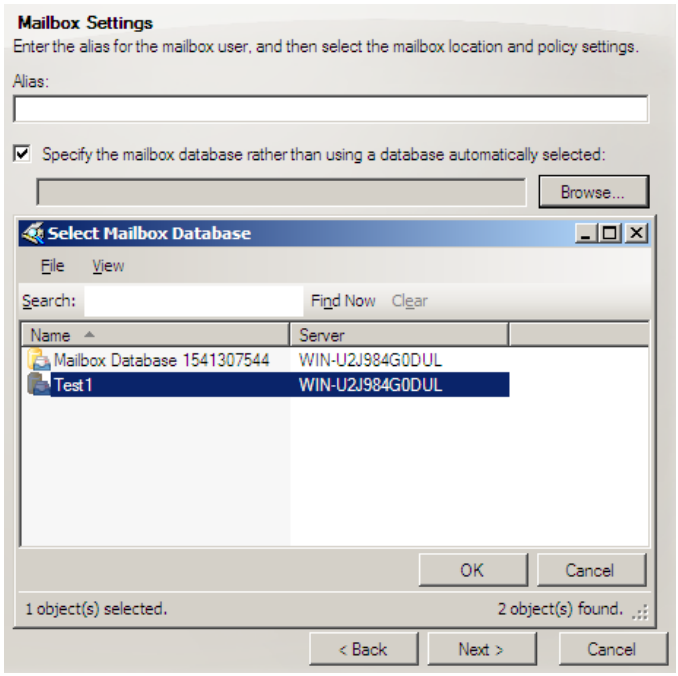
شکل ۱۲– انتخاب نام مستعار (همان logon name) و همچنین بانک اطلاعاتی قرارگیری اطلاعات کاربر



شکل ۱۱– تکمیل مشخصات کاربر در حالت ایجاد یک کاربر جدید

مراحل ایجاد یک صندوق پستی جدید در شکل‌های ۹ تا ۱۲ نمایش داده شده‌اند. در صفحه‌ی اول پس از کلیک بر روی لینک New mailbox ، گزینه user mailbox انتخاب شده و سپس در صفحه‌ی بعدی می‌توان ابتدا یک کاربر جدید را در شبکه تعریف و در ادامه برای او صندوق پستی ایجاد کرد و یا یکی از کاربرانی را که دارای صندوق پستی نیست انتخاب نمود (گزینه existing users) و سپس برای او صندوق پستی تعریف کرد (در این حالت به صورت هوشمند فقط لیست کاربران بدون صندوق پستی نمایش داده می‌شود و نه لیست کلیه کاربران تعریف شده در Active directory).

تنها نکته جالب این مراحل، امکان انتخاب دیتابیس ذخیره سازی اطلاعات این صندوق پستی جدید است (شکل ۱۳) که در مورد آن پیشتر بحث شد. می‌توان جهت مدیریت بهینه اطلاعات، چندین دیتابیس اصلی را تعریف کرد (که البته این مورد محدود است به نوع نگارش Exchange server) و سپس کاربران را در دیتابیس‌های متفاوتی قرار داد. برای ایجاد یک بانک اطلاعاتی جدید هم می‌توان همانند ایجاد بانک اطلاعاتی پوشه‌های عمومی به قسمت Organization Configuration > Mailbox رجوع کرده و گزینه New mail database را انتخاب کرد (و در اینجا می‌توان مدیریت بهتری را بر روی محل قرارگیری دیتابیس و لاگ فایل‌های آن مطابق توصیه‌های ارائه شده اعمال نمود).



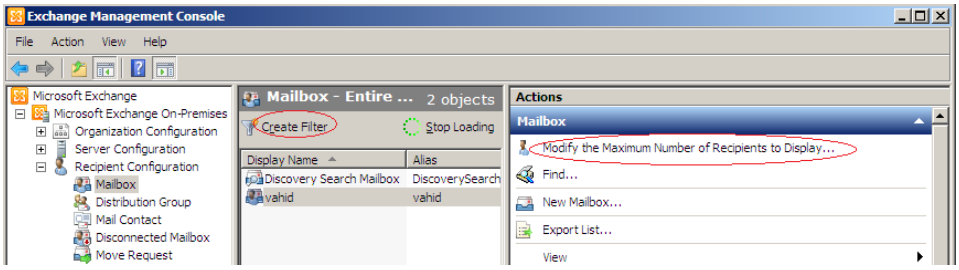
شکل ۱۳– انتخاب بانک اطلاعاتی محل قرارگیری داده‌های صندوق پستی کاربر

برای حذف صندوق پستی کاربران دو گزینه در برگه‌ی actions سمت راست صفحه قرار گرفته است با اسامی remove و disable. اگر از گزینه remove استفاده شود، کاربر از Active directory نیز حذف خواهد شد.

بنابراین اگر قصد حذف کاربر مورد نظر را از شبکه ندارید، از گزینه disable جهت غیرفعال کردن صندوق پستی او استفاده نمائید.

نکته – امکانات جستجوی کاربران

ممکن است در یک شبکه بزرگ، یافتن کاربران در لیست مدیریتی صندوق‌های پستی کار مشکلی باشد. به همین منظور دو گزینه در management console برای این امر در نظر گرفته شده است (شکل ۱۴).



شکل ۱۴– امکان جستجو و فیلتر بر روی صندوق‌های پستی تعریف شده

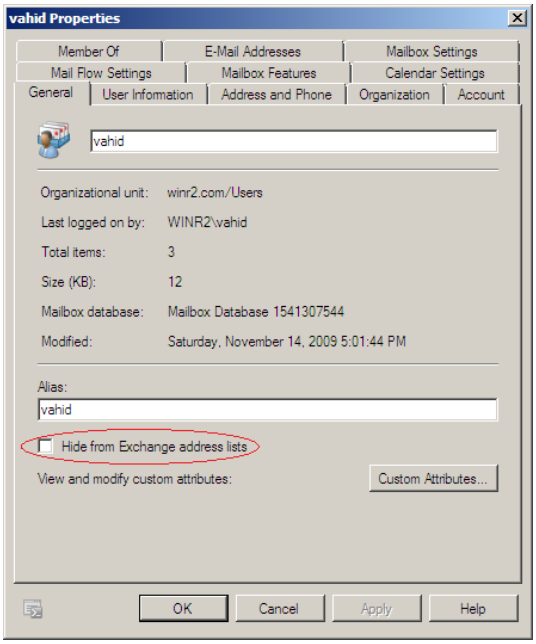
همانطور که در شکل ۱۴ نیز مشخص شده است، یا می‌توان از گزینه Create filter استفاده نمود و سپس برای مثال کاربران را بر اساس نام خانوادگی تعریف شده در Active directory جستجو نمود و یا می‌توان با استفاده از گزینه modify the max number of recipients display… ، لیست نمایشی را به تعدادی که مشخص می‌نمائیم، محدود کرد.

آشنایی با تنظیمات مهم صندوق‌های پستی در Exchange 2010

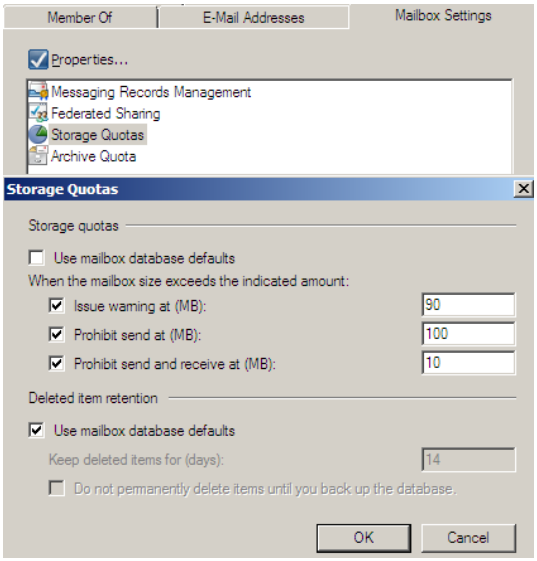
با کلیک راست بر روی هر صندوق پستی تعریف شده و انتخاب گزینه‌ی properties می‌توان تنظیمات مربوطه را تغییر داد. در صفحه‌ی خواص صندوق پستی یک کاربر، چند نکته‌ی مهم ذیل وجود دارند که در ادامه به صورت سؤال و جواب‌های متداول مرور خواهند شد:

- آیا می‌خواهید یک کاربر در لیست آدرس‌های ایمیل برای مثال در Outlook ظاهر نشود؟ در این حالت گزینه Hide from exchange address list را انتخاب کنید (شکل ۱۵).
- آیا می‌خواهید به یکی از کاربران بیشتر یا حتی کمتر از سهمیه بندی پیش فرض مقرر شده برای کلیه اعضای سازمان، اختیاراتی را نسبت دهید؟ برای انجام اینکار می‌توان تنظیمات storage quotas را ویرایش کرد (شکل ۱۶).

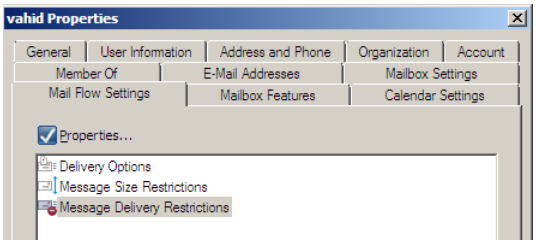
- آیا می‌خواهید تحرکات مشکوک یکی از کاربران را تحت نظر قرار دهید؟ آیا شخصی در سازمان شما به مسافرت رفته است و می‌خواهید کلیه ایمیل‌های دریافتی او به صورت موقت به شخص دیگری (برای مثال جانشین او) نیز رونوشت شوند؟ برای این منظور به گزینه delivery options برگه mail flow settings مراجعه کنید (شکل‌های ۱۷ و ۱۸) و تنظیمات مربوط به قسمت forward to را تکمیل نمائید.
- آیا نیاز است تا منشی بخش شما از طرف مدیر بخش ایمیل‌های خاصی را ارسال کند؟ برای این منظور در گزینه delivery options برگه mail flow settings صندوق پست الکترونیکی مدیر بخش، نام کاربری او را اضافه نمائید و این مجوز را به او اعطا کنید.
- آیا یکی از کاربران سازمان شما علاقه وافری به ارسال ایمیل به کل افراد سازمان دارد؟ برای این منظور در گزینه‌ی delivery options برگه mail flow settings ، حداکثر تعداد افراد مجازی را که این شخص می‌تواند در هر بار ارسال ایمیل انتخاب نماید توسط قسمت Recipients limits محدود و مشخص نمائید.
- آیا نیاز است تا کاربری را در شبکه به ارسال ایمیل به عده‌ای خاص محدود کرد؟ برای اعمال این سیاست به گزینه message delivery restrictions برگه mail flow settings مراجعه نمائید (شکل ۱۹).
- آیا نیاز است تا دسترسی Outlook web access از شخصی گرفته شود؟ برای این منظور به برگه Mailbox features مراجعه کنید (شکل ۲۰).
- آیا نیاز است تا آدرس SMTP خاصی را برای یکی از کاربران مطابق ایمیل‌های تعریف شده در برنامه‌های اتوماسیون اداری، تعریف کرد؟ برای اعمال این تغییر به برگه E-mail addresses رجوع نمائید (شکل ۲۱). حتی اگر آدرس ایمیل دومی در اینجا اضافه شود، ایمیل‌های ارسالی به هر کدام از دو آدرس SMTP تنظیم شده، به کاربر مورد نظر ارسال خواهند شد.



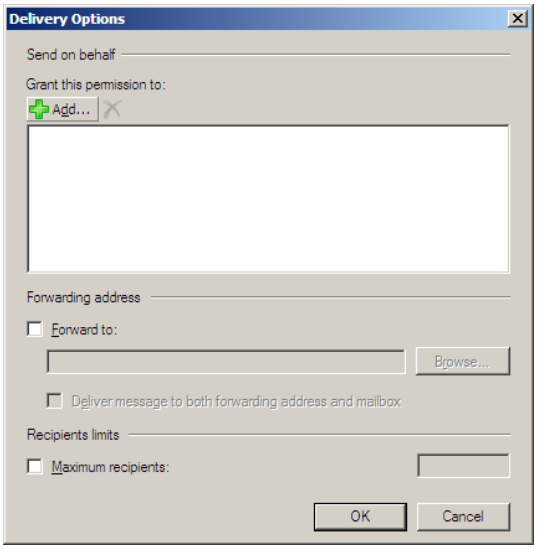
شکل ۱۵– امکان مخفی کردن آدرس کاربر از لیست آدرس‌ها



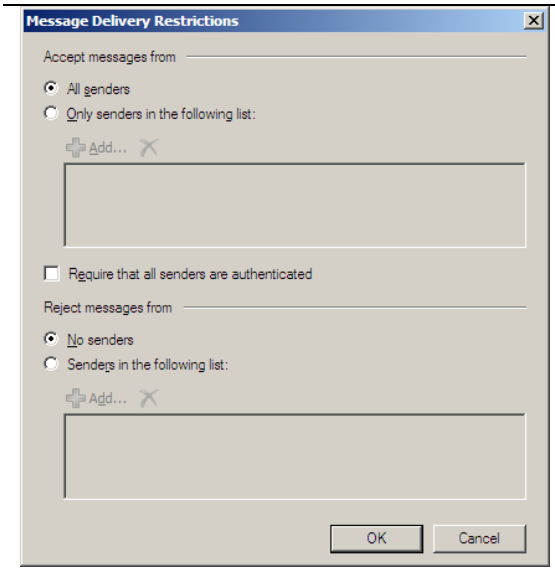
شکل ۱۶– امکان تعریف سهمیه بندی یک کاربر به صورت ویژه و مجزا از تنظیمات پیش فرض سازمانی



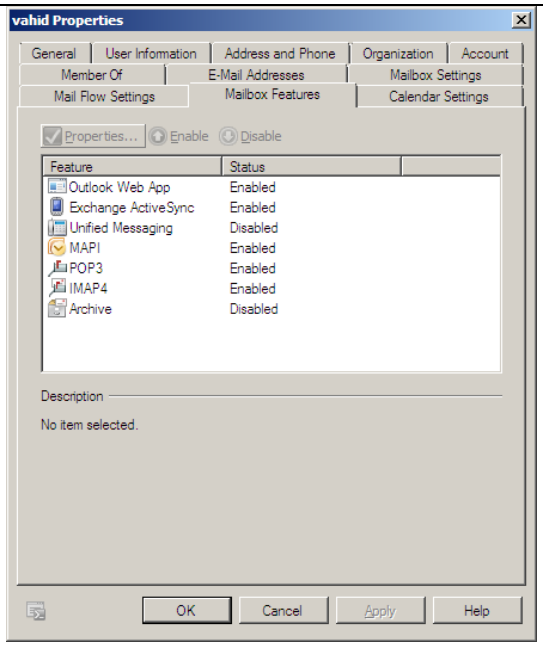
شکل ۱۷– تنظیمات نحوه‌ی ارسال و دریافت ایمیل‌های یک کاربر خاص



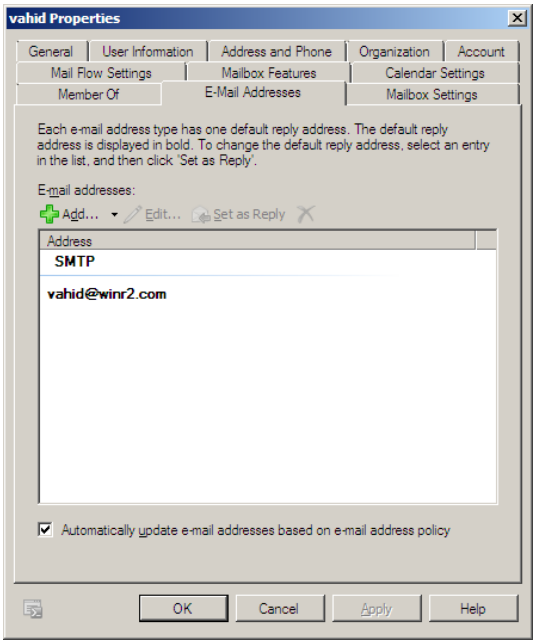
شکل ۱۸– امکان ارسال رونوشت ایمیل‌های یک شخص به اشخاصی خاص در شبکه



شکل ۱۹– امکان محدود کردن ارسال و دریافت یک صندوق پستی به و از اشخاصی خاص



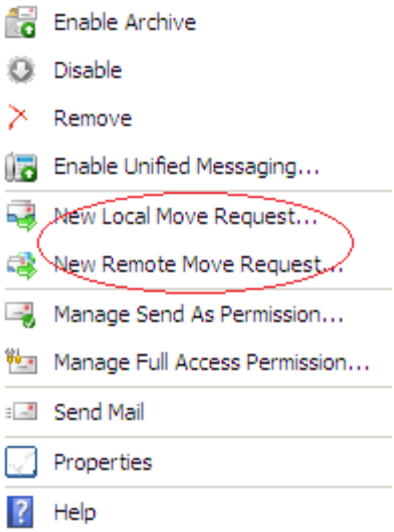
شکل ۲۰– امکان فعال و غیر فعال کردن ویژگی‌های قابل دسترسی یک صندوق پستی



شکل ۲۱– امکان تعریف آدرس SMTP سفارشی برای یک کاربر

نحوه‌ی انتقال یک صندوق پستی در Exchange 2010

همانطور که پیشتر نیز ذکر شد بهتر است جهت مدیریت بهینه‌ی بانک‌های اطلاعاتی صندوق‌های پستی کاربران، به ازای گروه‌های مختلف کاری در سازمان، یک بانک اطلاعاتی جدید را ایجاد کرد (رجوع به قسمت Organization Configuration > Mailbox و انتخاب گزینه New mail database). اکنون جهت انتقال یک کاربر از یک بانک اطلاعاتی موجود به بانک اطلاعاتی دیگر، دو گزینه انتقال به بانک اطلاعاتی محلی و راه دور در برگه actions قسمت مدیریت صندوق‌های پستی کاربران قابل مشاهده است (شکل ۲۲).



شکل ۲۲– امکان انتقال یک صندوق پستی به بانک اطلاعاتی دیگر.

پس از انتخاب گزینه‌ی New local move request ، امکان انتخاب بانک اطلاعاتی محلی مقصد، جهت انتقال میسر است؛ سپس مشخص ساختن اینکه اگر ایمیل‌های تخریب شده‌ای در این صندوق پستی وجود داشتند آیا کار انتقال صورت گیرد یا خیر یا اینکه از موارد معیوب صرفنظر گردد، صورت خواهد گرفت و در پایان با کلیک بر روی دکمه‌ی New، کار انتقال آغاز می‌گردد.

در حالت New remote move request امکان انتقال صندوق پستی از یک Active directory به نمونه‌ای دیگر وجود دارد (که جزو تازه‌های Exchange server 2010 است).

ایجاد و مدیریت گروه‌های توزیعی (distribution groups) در Exchange 2010

گروه‌های توزیعی بسیار پرکاربرد و رایج هستند. برای مثال تعریف گروه مدیریت منابع انسانی (HR) با یک آدرس ایمیل مشخص و سپس هنگامیکه به این آدرس، ایمیلی ارسال گردد، کلیه اعضای آن گروه ایمیل مربوطه را دریافت خواهند کرد.

در Active directory دو گروه وجود دارند که جهت تعریف گروه‌های توزیعی در Exchange قابل استفاده می‌باشند:

- Security groups : که جهت مدیریت دسترسی‌های کاربران قابل تعریف هستند.
- Distribution groups : تنها جهت مدیریت ایمیل‌ها بکار می‌روند و قابلیت‌های امنیتی ذکر شده را ندارند.

هر دو گروه security و یا distribution در یک active directory را می‌توان اصطلاحا Mail enabled کرد. تنها تفاوت اصلی در اینجا است که اگر گروهی را درون یک گروه security قرار دهید، این گروه زیر مجموعه نیز ایمیل‌های گروه اصلی را دریافت خواهد کرد (که گاهی از اوقات از دیدگاه امنیتی این مورد مطابق سیاست‌های سازمان نمی‌باشد) که در مورد یک distribution group به این صورت نیست.

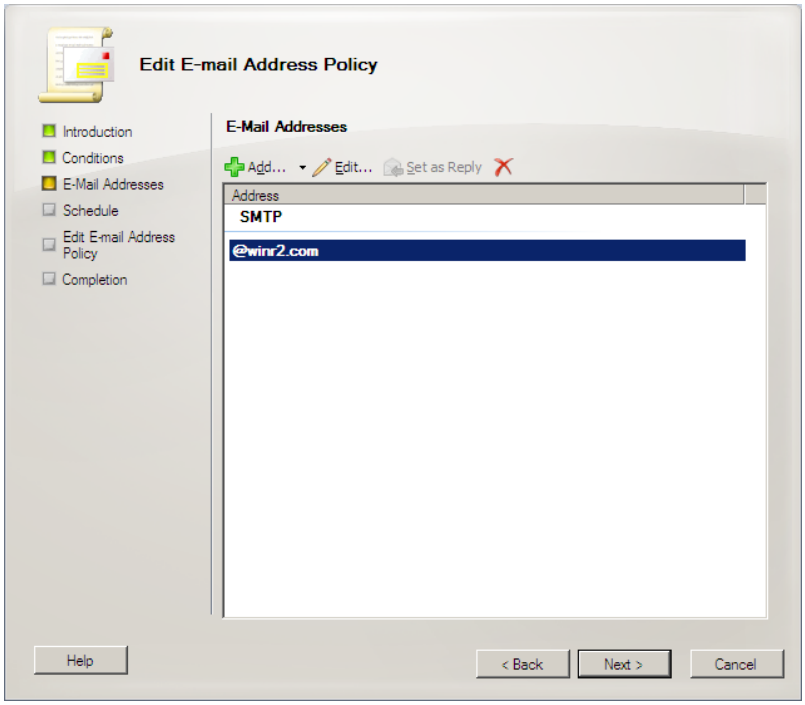
گروه سومی نیز قابل تعریف است که به صورت پویا بر اساس کاربران و یا گروه‌های توزیعی ایجاد می‌شود:

- Dynamic distribution groups : این گروه‌ها بر اساس کوئری‌ها و فیلترهای صورت گرفته بر روی گروه‌ها و کاربران تعریف شده در Active directory به صورت پویا تولید می‌شوند (مباحث LDAP queries)؛ برای مثال تعریف یک گروه پویا بر اساس کاربرانی که کد پستی خاص یک منطقه را دارند و این اطلاعات از global catalog server دریافت می‌شود. این گروه‌ها بر اساس یک سری کاربر ثابت تهیه نشده و هر بار که فراخوانی می‌شوند ابتدا بر اساس کوئری تعریف شده، اطلاعات لازم را از Active directory اخذ کرده، گروه مورد نظر را تشکیل داده و سپس نسبت به ارسال ایمیل به اعضای پویای یافت شده اقدام خواهد شد.

جهت مدیریت این گروه‌ها تنها کافی است به قسمت recipient configuration و گزینه‌ی distribution groups مراجعه کرد. در اینجا می‌توان گروهی جدید را ایجاد نمود و یا گروهی موجود را افزود. اگر گروهی را از این طریق تعریف نمائیم، علاوه بر اضافه شدن به تعاریف Active directory به صورت خودکار Mail enabled نیز خواهد بود؛ اما اگر در ابتدا گروهی را به Active directory اضافه نمائیم، این گروه‌ها در لیست distribution groups کنسول مدیریتی Exchange server ظاهر نخواهند شد، زیرا هنوز امکان ارسال و دریافت ایمیل برای آن‌ها فعال نشده است. در این حالت تنها کافی است گزینه New distribution group انتخاب شده و یکی از گروه‌های موجود انتخاب گردد.

نحوه‌ی تغییر SMTP Domain پیش فرض سازمان

اگر دقت کرده باشید آدرس SMTP تمامی کاربران به صورت پیش فرض به نام Domain ما ختم شده است. اگر به هر دلیلی نیاز به تغییر این تنظیم پیش فرض برای تمامی کاربران یا حتی عده‌ای از آن‌ها وجود داشت باید به قسمت Organization configuration > Hub transport و سپس برگه E-Mail address policies آن مراجعه نمود. با ویرایش Default policy موجود (گزینه Edit را از برگه actions سمت راست صفحه انتخاب نمائید) و سپس دوبار کلیک بر روی دکمه Next و رسیدن به صفحه E-mail Addresses آن می‌توان این مقدار پیش فرض را ویرایش نمود (شکل ۲۳).



شکل ۲۳– امکان تغییر نام Domain آدرس‌های ایمیل سازمان برای کلیه کاربران.

برای تغییر SMTP Domain یک کاربر تنها کافی است به خواص صندوق پستی الکترونیک او مراجعه کرده و سپس مقدار موجود در برگه‌ی E-Mail Addresses را ویرایش کرد (شکل ۲۱).

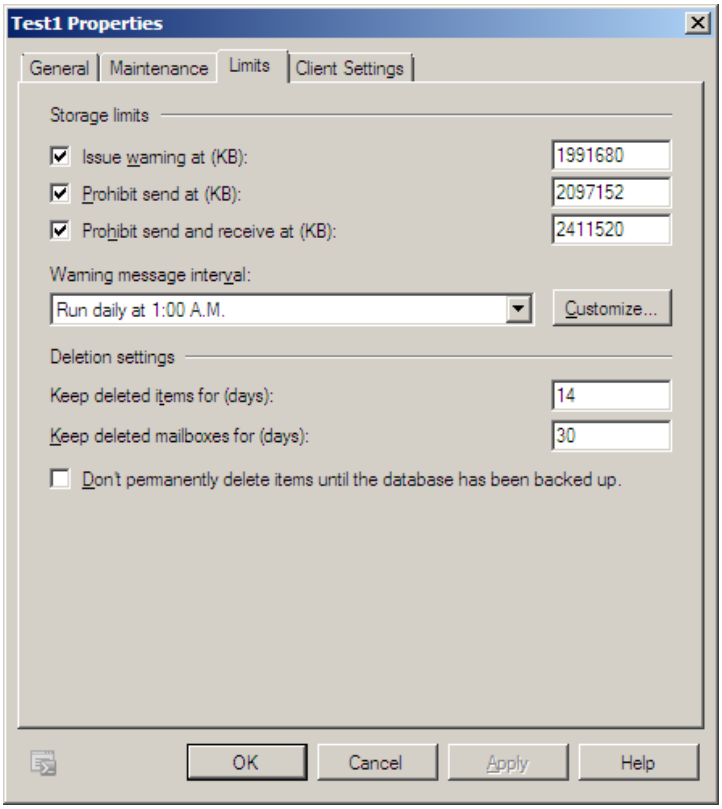
اگر نیاز بود تا تنها عده‌ی خاصی از اعضای سازمان برای مثال ساکنین منطقه‌ای خاص دارای SMTP Domain ویژه‌ای باشند، می‌توان یک گزینه New E-mail address policy را از برگه actions سمت راست صفحه انتخاب کرده و سپس همانند تعریف یک Rule جدید در Outlook می‌توان سیاست جدیدی مبتنی بر تعریف فیلتر بر روی منطقه‌ی افراد ایجاد نمود.

نحوه‌ی تنظیم سهمیه بندی عمومی صندوق‌های پست الکترونیکی

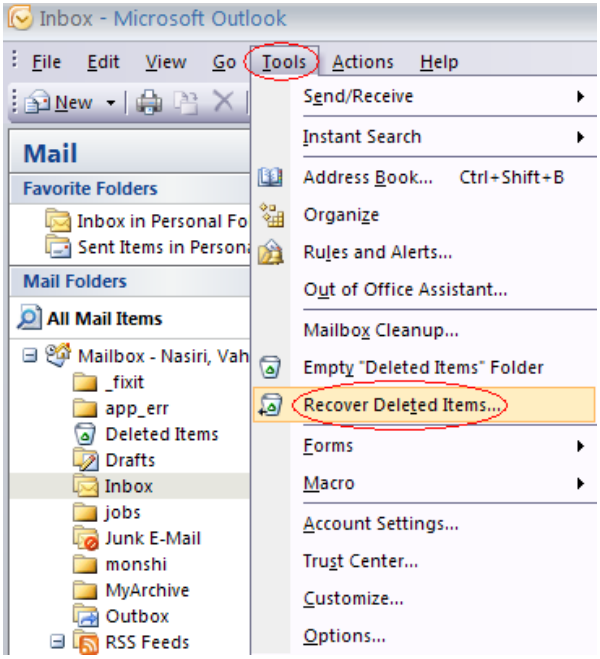
پیش فرض‌های سهمیه بندی هر صندوق پست الکترونیکی، از تنظیمات بانک اطلاعاتی که آن صندوق پستی بر روی آن قرار گرفته است خوانده می‌شود و حالت پیش فرض آن‌را در شکل ۲۴ ملاحظه می‌نمائید (قسمت `Organization configuration > Mailbox` ، سپس برگه `Database management` آن و کلیک راست و مراجعه به خواص دیتابیس مورد نظر).

به همین جهت می‌توان برای بخش‌های مختلف یک سازمان بسته به حجم کاری آن‌ها دیتابیس‌های مختلف با سهیمه بندی‌های مختلفی ایجاد کرده و سپس صندوق‌های پستی کاربران را به آن دیتابیس‌ها انتقال داد.

همچنین در این برگه می‌توان مشخص ساخت که ایمیل‌های حذف شده کاربران تا چه مدتی در سرور نگهداری شوند (در قسمت `deletion settings` خواص دیتابیس). به این صورت اگر کاربری به اشتباه ایمیلی را حذف کرده باشد امکان بازیابی آن‌را در `Outlook` (منوی `tools` گزینه `Recover deleted items`) خواهد داشت (شکل ۲۵). علاوه بر آن مطابق تنظیمات این برگه اگر به اشتباه یا مطابق سیاست‌های سازمان، صندوق پست الکترونیکی شخصی نیز حذف گردد، قابل بازیابی خواهد بود.



شکل ۲۴– سهمیه بندی صندوق‌های پست الکترونیکی کاربران به ازای یک بانک اطلاعاتی مشخص.



شکل ۲۵– امکان بازیابی ایمیل‌های حذف شده کاربران در Outlook بر اساس تنظیمات بانک اطلاعاتی صندوق‌های پست الکترونیکی کاربران.

فصل ۴ – مباحث تکمیلی تنظیمات ارسال و دریافت کنندگان ایمیل

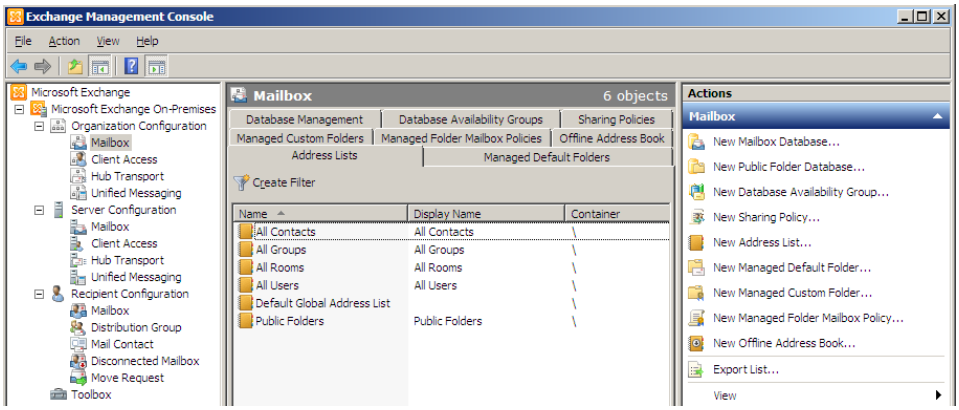
مدیریت و تنظیم لیست‌های آدرس‌ها

زمانیکه کار تعاریف صندوق‌های پستی سازمان به پایان رسید، اکنون نوبت به تهیه لیست آدرس‌های ایمیل تعریف شده و ارائه خودکار آن‌ها به برنامه‌هایی مانند Outlook است تا کاربران بتوانند به سادگی آدرس‌های ایمیل موجود را یافته و از آن‌ها استفاده کنند.

آشنایی با مفاهیم لیست‌های آدرس‌ها (Address lists)

هر لیست آدرس، مجموعه‌ای از آدرس‌های ایمیل است که حاصل یک LDAP query از Active directory می‌باشد.

به صورت پیش فرض یک سری لیست آدرس از پیش تعریف شده در Exchange server وجود دارند که لیست آن‌ها را در تصویر ذیل می‌توان مشاهده نمود (مراجعه به Organization configuration قسمت Mailbox و سپس مشاهده‌ی برگه Address lists):

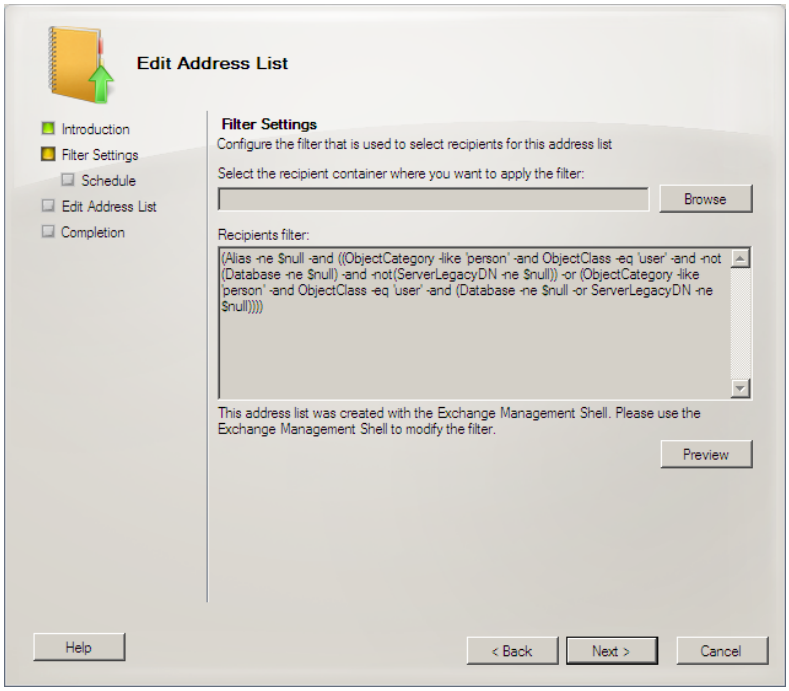


شکل ۱– لیست‌های آدرس‌های پیش فرض Exchange server 2010 .

- All contacts : شامل تمامی اطلاعات تماس با قابلیت ارسال و دریافت ایمیل است.
- All groups : شامل کلیه Distribution groups تعریف شده می‌باشد.

- `All rooms` : شامل آدرس‌های پست الکترونیکی تمام منابعی است که به آن‌ها آدرس ایمیلی اختصاص داده شده است.
- `All users` : شامل لیست تمامی کاربرانی است در سازمان که دارای صندوق پست الکترونیکی می‌باشند.
- `Global address list` و یا `GAL` : شامل لیست تمام افراد و منابعی است که در سازمان برای آن‌ها ایمیل تعریف شده است. امکان تعریف چندین `GAL` وجود دارد اما هر بار تنها یکی از آن‌ها برای کاربران قابل مشاهده خواهد بود.

برای مثال اگر `All users` را انتخاب کرده و از برگه‌ی `Actions` سمت راست صفحه گزینه‌ی `edit` را انتخاب کنیم می‌توان `LDAP Query` مربوطه را در قسمت `Recipients filter` مشاهده نمود (شکل ۲).



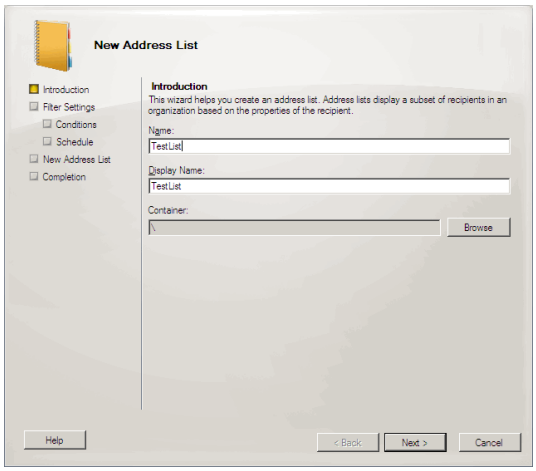
شکل ۲– `LDAP query` متناظر با گروه `All users`.

نحوه‌ی ایجاد یک لیست آدرس سفارشی

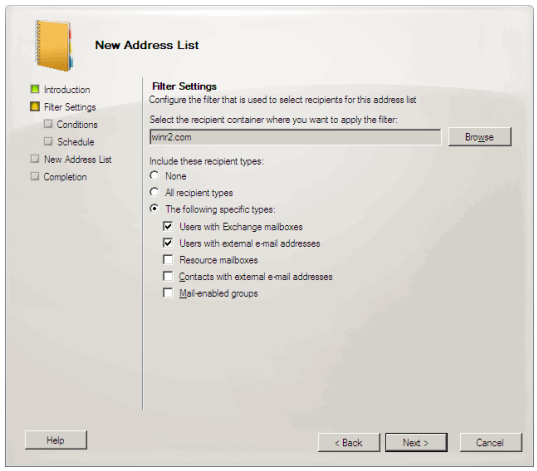
اگر به شکل ۱ دقت نمائید، یکی از گزینه‌های برگه `Actions` سمت راست صفحه، `New address list` است. بر روی این گزینه کلیک نمائید تا صفحات انجام مراحل مختلف آن ظاهر شوند (شکل‌های ۳ تا ۷).

در این مراحل در ابتدا نام لیست آدرس‌ها پرسیده می‌شود. سپس محل قرارگیری آن و نحوه اعمال به اشخاص مورد نظر سؤال پرسیده خواهد شد که می‌تواند تمامی حالات و یا یک سری موارد مشخص باشند. سپس شبیه به ایجاد یک

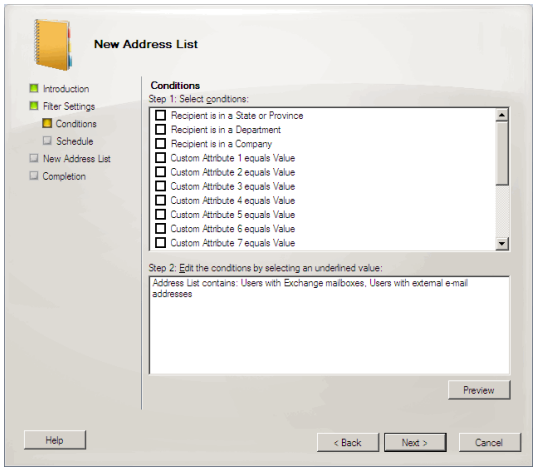
Rule جدید Outlook ، اینجا نیز می‌توان نحوه‌ی تهیه لیست را فیلتر کرد. سپس زمان اعمال این لیست به کل مجموعه باید مشخص گردد. در صفحه بعدی که کار انجام افزودن این لیست سفارشی فیلتر شده را بر عهده دارد، می‌توان LDAP Query حاصل از این مراحل را نیز مشاهده نمود.



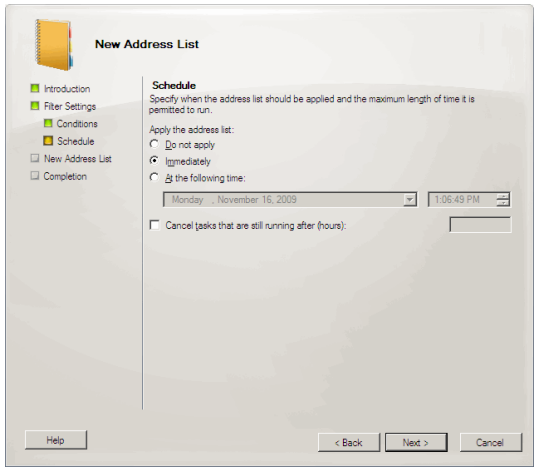
شکل ۳– مشخص ساختن نام لیست



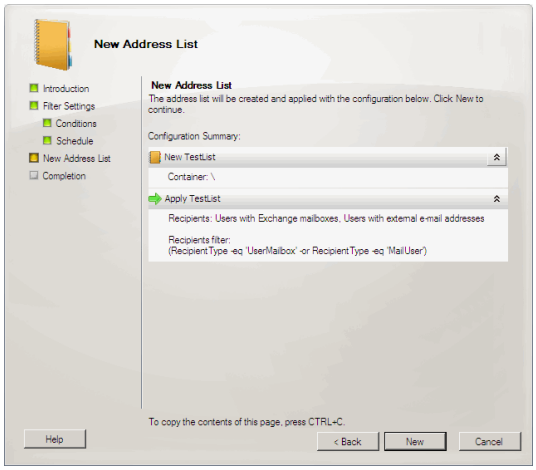
شکل ۴– مشخص سازی محل قرارگیری و نحوه اعمال لیست



شکل ۵– ساخت فیلتر بر اساس آیتم‌های موجود یا سفارشی



شکل ۶– مشخص سازی زمان اعمال لیست



شکل ۷– پایان کار ساخت یک لیست جدید

تعریف اطلاعات تماس‌های کاربران

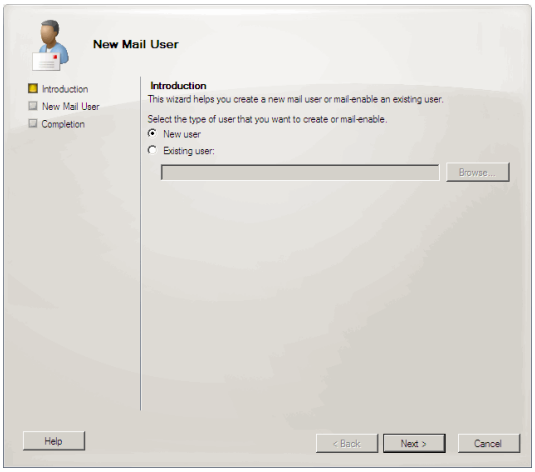
در فصل قبل با نحوه‌ی ایجاد یک صندوق پستی جدید برای کاربران شبکه آشنا شدیم. در این قسمت قصد داریم برای کاربرانی که از خارج از سازمان با ما در حال همکاری هستند و برای آن‌ها در شبکه حساب کاربری ایجاد شده است اما قصد دارند ایمیل‌های خود را در صندوق پستی خارج از سازمان مطالعه کنند، تنظیمات ویژه‌ای را تدارک ببینیم. به کاربران فصل قبل در اصطلاح Mailbox users گفته می‌شوند و حساب‌های کاربری که شرح آن‌ها رفت (Mailbox آن‌ها در Exchange server ما قرار نخواهد گرفت) Mail-Enabled Accounts نامیده خواهند شد.

برای این منظور باید به قسمت recipients configuration گزینه Mail contact مراجعه کرده و سپس در برگه Actions سمت راست صفحه بر روی گزینه ...New Mail user کلیک نمود (شکل‌های ۸ تا ۱۰).

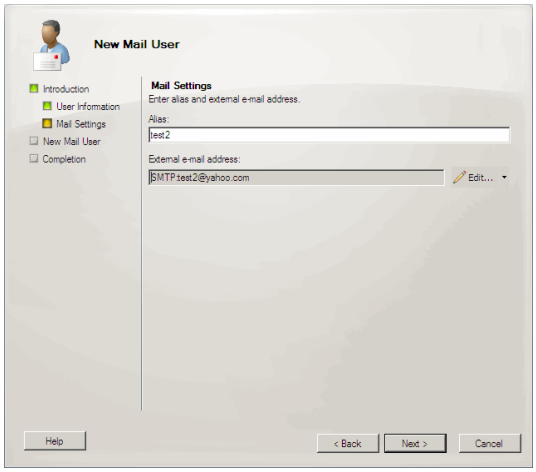
در این مراحل امکان ایجاد یک کاربر جدید در Active directory وجود داشته و یا می‌توان از یکی از کاربران موجود استفاده کرد. سپس باید نام مستعاری را وارد کرده و آدرس ایمیل خارجی شخص مورد نظر را وارد کرد. در پایان با کلیک بر روی دکمه New عملیات ساخت حساب کاربری شخص با ویژگی Mail user صورت می‌گیرد. این نوع حساب‌های کاربری نیز در GAL ظاهر می‌شوند اما آیکون آن‌ها اندکی متفاوت است.

نکته – افزودن اطلاعات تماس کاربری که حساب کاربری ندارد

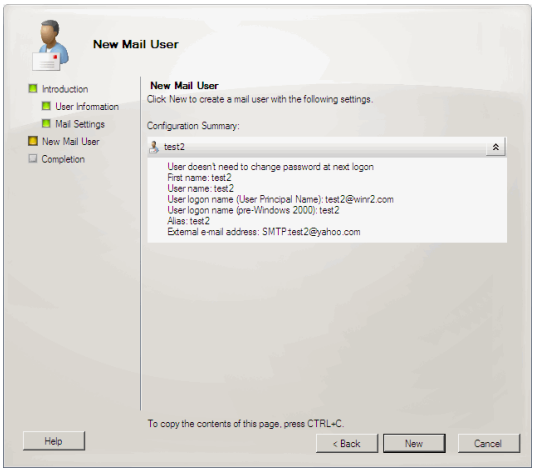
اگر قصد نداشته باشیم برای این کاربر خاص حساب کاربری جدیدی در Active directory ایجاد کنیم می‌توان از گزینه New mail contact در همان قسمت استفاده کرد. به این صورت اطلاعات این کاربر به همراه ایمیل خارجی آن نیز جهت ارسال ایمیل به او در GAL ظاهر شده و در اختیار کلیه کاربران سازمان خواهد بود.



شکل ۸– ایجاد یک Mail user جدید یا استفاده از یکی از کاربران موجود



شکل ۹– تنظیم نام مستعار و همچنین ایمیل خارجی شخص



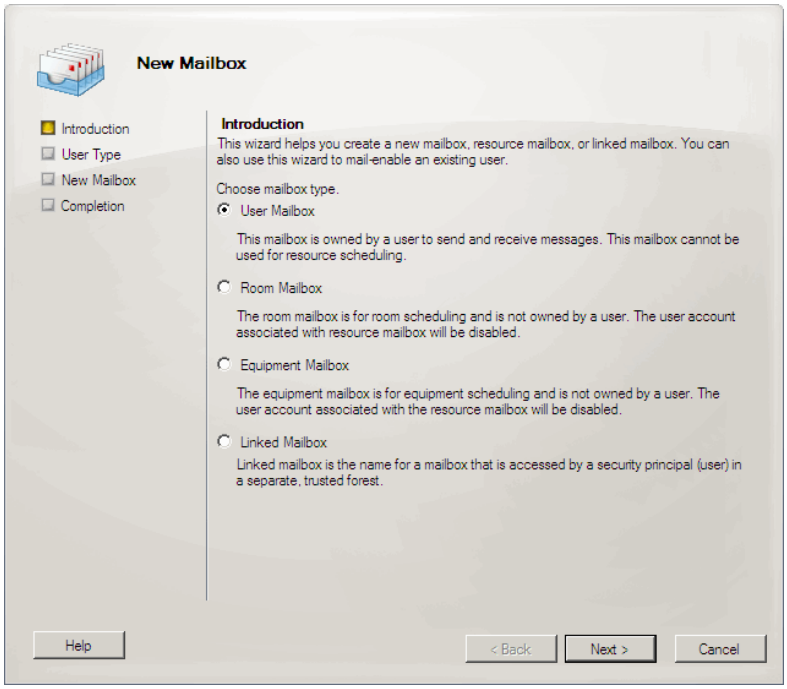
شکل ۱۰– مرور و پایان کار ایجاد Mail user جدید

تعریف صندوق پستی الکترونیکی برای منابع و تجهیزات

اگر مجددا به گزینه new mailbox همانند فصل قبل رجوع کنیم موارد دیگری را نیز می‌توان مشاهده کرد (شکل ۱۱)؛ امکان ایجاد ایمیل برای منابع و تجهیزات و غیره.

برای مثال اگر گزینه‌ی Room mailbox را انتخاب کنیم، مراحل کار همانند مراحلی است که تاکنون مرور شده‌اند؛ اما با یک تفاوت. در اینجا کاربری که جهت Room mailbox انتخاب می‌شود باید در Active directory غیرفعال شده باشد. در غیر اینصورت در لیست انتخاب کاربران ظاهر نخواهد شد.

عموما هدف از ایجاد صندوق پستی برای تجهیزات یا منابع استفاده از آن‌ها در تقویم Outlook و زمانبندی استفاده از آن‌ها می‌باشد.



شکل ۱۱– گزینه‌های مختلف امکان ایجاد یک صندوق پست الکترونیکی جدید.

گزینه‌ی ایجاد Linked mailbox برای ایجاد صندوق پست الکترونیکی یک Active directory forest دیگر موجود در سازمان، در Exchange server تحت مدیریت شما در خارج از Active directory forest آن می‌تواند مورد استفاده قرار گیرد (بین این دو Active directory forest نیز باید رابطه اطمینان برقرار شده باشد).

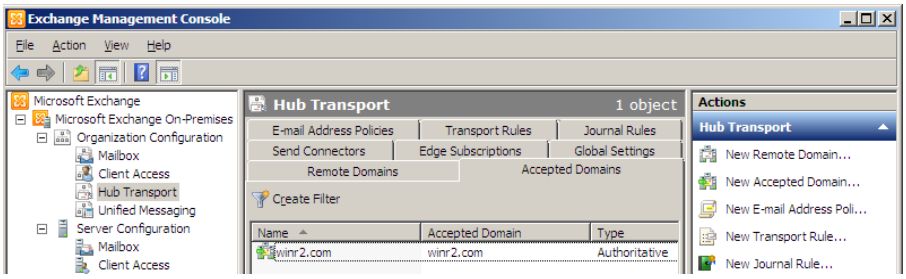
مدیریت دومین‌های پذیرفته شده (Accepted domains)

در یک Domain مفروض تنها امکان تعریف یک ارگان Exchange server وجود دارد؛ اما در همین Domain می‌توان بیش از یک SMTP Domain را تعریف و استفاده نمود.

هر Domain، دریافت کننده‌ی ایمیل اصطلاحا Authoritative domain نامیده می‌شود (که جهت ارسال ایمیل به کارکنان داخلی سازمان کاربرد دارد). اگر بنابر تشخیص یک Edge transport server و یا حتی یک Authoritative domain ، نیاز به ارسال ایمیل به سروری دیگر وجود داشت، به آن سرور ثانویه Relay domain گفته می‌شوند (که این عملیات رله می‌تواند داخلی (به یک Active directory forest دیگر) و یا خارجی باشد).

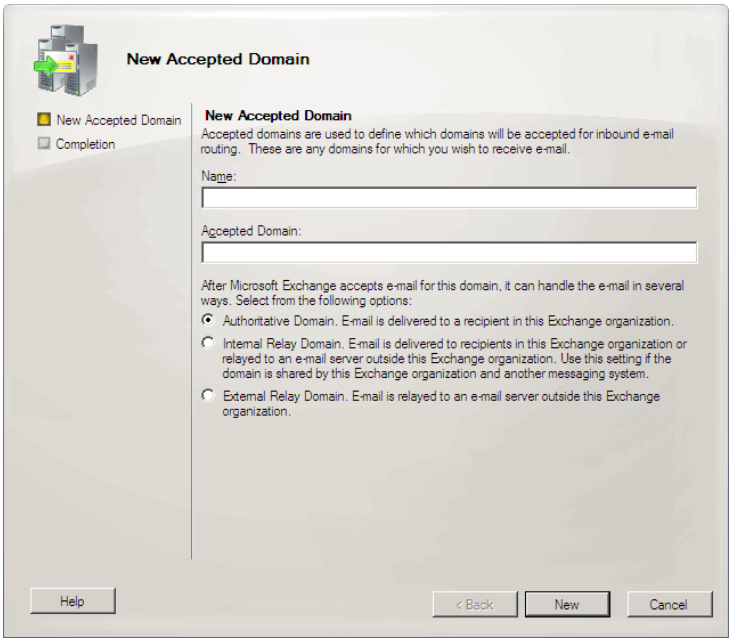
برای تنظیم دومین‌های پذیرفته شده باید به قسمت Organization configuration گزینه Hub transport، برگه‌ی Accepted domains مراجعه کرد (شکل ۱۲).

همانطور که در شکل ۱۳ نیز مشخص است، دومین پذیرفته شده پیش فرض همان Active directory domain ما است و از نوع Authoritative نیز می‌باشد.



شکل ۱۲– تنظیمات دومین‌های پذیرفته شده

اگر در همین قسمت بر روی گزینه New accepted domains برگه actions سمت راست صفحه کلیک کنیم، صفحه ایجاد یک دومین پذیرفته شده جدید نمایان خواهد شد و در این صفحه مطابق توضیحاتی که پیشتر ارائه شد، انواع ارائه شده را بهتر می‌توان درک نمود.



شکل ۱۳– تعریف یک دومین پذیرفته شده جدید

تنظیمات مرتبط با برنامه‌های اتوماسیون اداری جهت ارسال ایمیل از طریق Exchange server

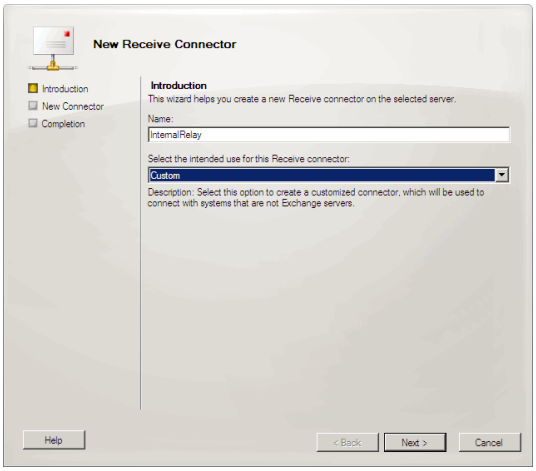
از Exchange server 2007 به بعد نحوه‌ی مدیریت برنامه‌هایی که می‌توانند در شبکه ایمیل ارسال کنند تغییر کرده است. پیش از این تنها کافی بود تا یک شخص، برنامه‌ی مورد نظر ارسال ایمیل خود را اجرا کرده و نسبت به ارسال ایمیل ناشناس به کلیه پرسنل سازمان اقدام نماید. اما اکنون به دلایل امنیتی این مورد ممنوع شده است و باید سرورهای مجاز ارسال ایمیل (برای مثال سرورهایی که برنامه‌های اتوماسیون اداری یک شرکت بر روی آن نصب هستند) را به عنوان سرور امن ارسال ایمیل تعریف نمود و مابقی کامپیوترهای موجود در شبکه امکان ارسال ایمیل از طریق سایر برنامه‌ها را ندارند و خطای زیر را دریافت خواهند کرد:

```
Error: 530 5.7.1 Client was not authenticated
```

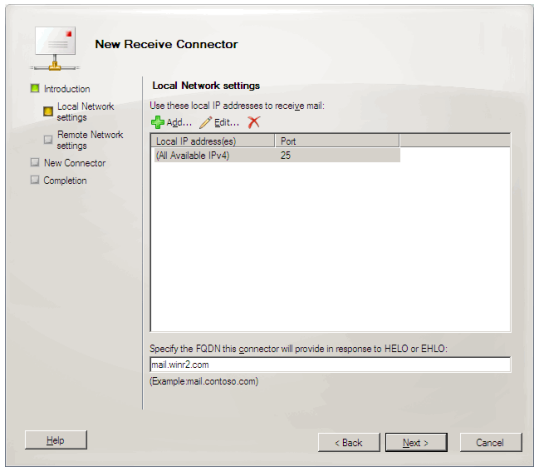
بدیهی است از آنجائیکه اشخاص هنگام استفاده از Outlook ابتدا باید در شبکه اعتبارسنجی شوند و برنامه Outlook تحت مجوز شخصی اعتبار سنجی شده (login به دومین) و دارای صندوق پست الکترونیکی در Exchange server اجرا می‌شود، مشکلی از لحاظ ارسال ایمیل نخواهند داشت. اما سایر برنامه‌ها، بدون انجام اعتبار سنجی امکان ارسال ایمیل ناشناس در شبکه را ندارند. همچنین باید درنظر داشت که عموما برنامه‌های برای مثال اتوماسیون اداری تحت مجوز یک کاربر محلی با سطح دسترسی بسیار پایین اجرا می‌شوند. به همین جهت برای رفع این مشکل باید یک Receive Connector ویژه را تعریف نمود که مراحل آن به شرح ذیل هستند. در این مراحل فرض بر این است که سرور برنامه‌های اتوماسیون اداری ما با IP ثابت مساوی ۱۰.۱۰.۱۰.۱۳۱ در شبکه قرار گرفته است:

- ابتدا به قسمت Server Configuration گزینه Hub Transport مراجعه کنید. در اینجا با قسمت Receive Connectors سروکار خواهیم داشت و کار آن تعریف دروازه‌ای است منطقی که تمامی ایمیل‌های ارسالی از طریق آن دریافت می‌شوند.
- در این قسمت از برگه Actions سمت راست بر روی گزینه New Receive Connector کلیک نمائید.
- در صفحه باز شده یک نام دلخواه را وارد کرده و سپس بر روی دکمه Next کلیک کنید (شکل ۱۴).
- در ادامه FQDN مورد استفاده در این متصل کننده را مشخص کنید (همان FQDN سرور Exchange است) برای مثال mail.domain.com (شکل ۱۵). سپس بر روی دکمه Next کلیک نمائید.
- در صفحه‌ی بعدی تعاریف پیش فرض را حذف کرده و IP سرور برنامه‌های خود را وارد نمائید (شکل ۱۶). سپس بر روی دکمه‌های New و Finish کلیک نمائید تا کار تعریف این اتصال دهنده سفارشی به پایان رسد.
- پس از اضافه شدن این اتصال دهنده سفارشی، بر روی آن کلیک راست کرده و در صفحه خواص آن به برگه Permission groups مراجعه نمائید و گزینه Anonymous users را انتخاب کنید (شکل

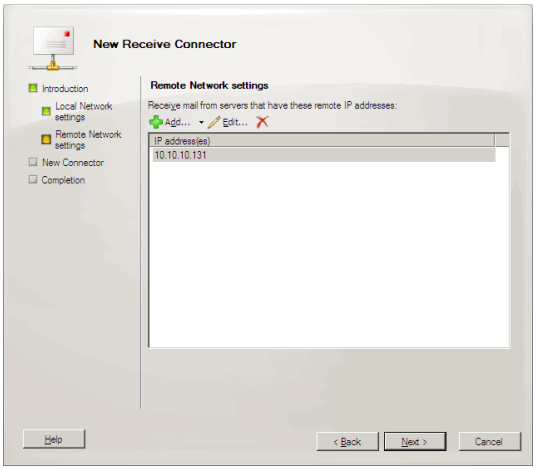
۱۷). به این صورت برنامه‌های واقع شده در سرور مشخص اتوماسیون اداری ما قادر خواهند بود تا بدون نیاز به اعتبارسنجی خاصی نسبت به انجام امور روزمره و ارسال ایمیل‌های خود اقدام کنند.



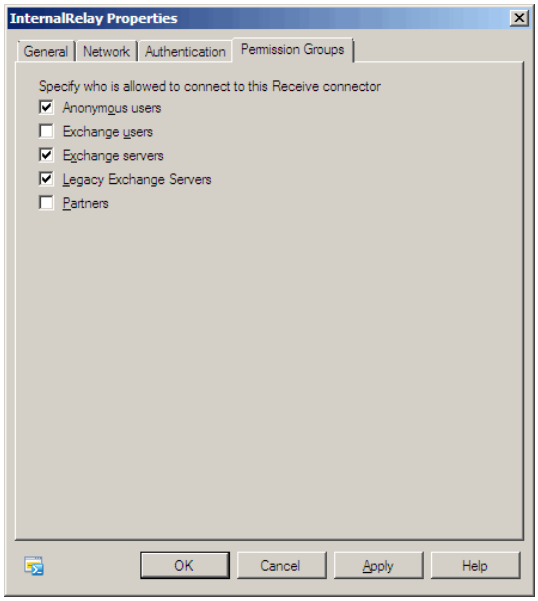
شکل ۱۴– ایجاد یک اتصال دهنده‌ی سفارشی



شکل ۱۵– تعریف FQDN مناسب



شکل ۱۶– مشخص ساختن IP سرور مجاز

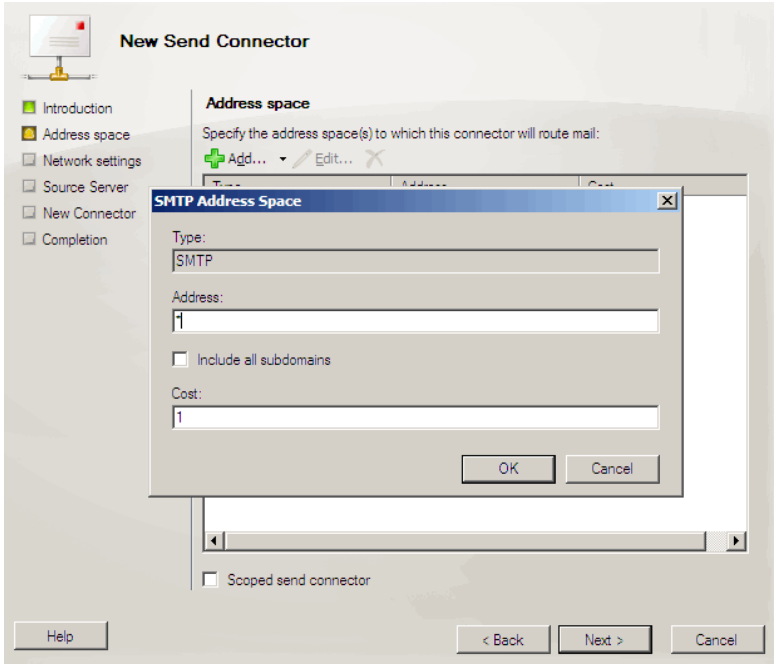


شکل ۱۷– تنظیمات لازم جهت ارسال ایمیل به صورت ناشناس

تنظیمات ارسال و دریافت ایمیل از اینترنت

همانطور که در فصل‌های قبل نیز ذکر شد، روش صحیح و امن برقراری ارتباط با اینترنت استفاده از یک سرور مجزا به نام Edge transport server و نصب نقش مربوطه بر روی آن است. اگر این سرور نصب نگردد، باید به قسمت Server Configuration گزینه Hub Transport مراجعه نمود. سپس در قسمت Receive Connectors بر روی Default receive connector کلیک راست کرده و درصفحه خواص آن به برگه Permission groups مراجعه نموده و گزینه Anonymous users را انتخاب کرد. به این صورت از دنیای خارج می‌توانند به Hub transport server ما ایمیل ارسال کنند.

اکنون برای تنظیم امکان ارسال ایمیل به دنیای خارج باید به قسمت Organization Configuration > Hub Transport مراجعه کرد. در اینجا گزینه‌ی New Send Connector در برگه‌ی Actions سمت راست صفحه باید انتخاب گردد و مراحل ایجاد آن طی شود. تنها نکته‌ی مهم آن وارد کردن علامت ستاره در صفحه‌ی Address space آن است (شکل ۱۸). به این معنا که ارسال ایمیل به تمامی آدرس‌های ایمیل اینترنتی مجاز خواهد بود.



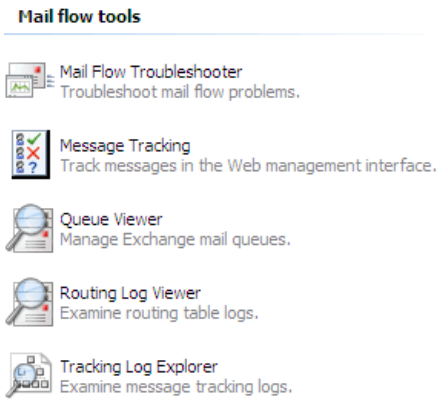
شکل ۱۸– تنظیمات ارسال ایمیل به خارج از سازمان.

خطایابی مشکلات ارسال و دریافت ایمیل

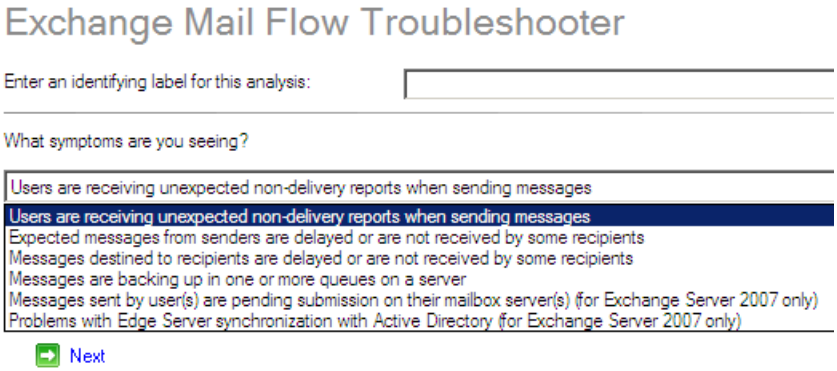
اگر به گزینه‌ی Toolbox در کنسول مدیریتی Exchange server مراجعه کنیم، ابزارهای مختلفی برای خطایابی مشکلات احتمالی پیش بینی شده‌اند (شکل ۱۹).

با انتخاب گزینه‌ی Mail flow troubleshooter می‌توان گزینه‌های مختلفی را جهت خطایابی انتخاب نمود (شکل ۲۰). برای مثال تعدادی از کاربران گلایه دارند که ایمیل‌های آن‌ها ارسال نشده یا پیغام‌های خطایی را پس از ارسال ایمیل دریافت می‌کنند. توسط این ابزار می‌توان مشکلات موجود را یافته و خطایابی کرد. برای نمونه اگر سرویسی متوقف شده باشد یا تعریف آدرس ایمیلی دچار اشتباه باشد، اگر مشکلات DNS در شبکه موجود باشند و امثال آن‌را دقیقا گزارش داده و بر اساس آن‌ها می‌توان کار رفع اشکال از سیستم را آغاز نمود.

انتخاب گزینه‌ی Message tracking ما را به کنسول مدیریتی تحت وب ارائه شده در Exchange server 2010 هدایت می‌کند که در آن می‌توان وضعیت ارسال و دریافت‌های اشخاص را دقیقا بررسی و خطایابی کرد (شکل ۲۱).



شکل ۱۹– ابزارهای خطایابی مشکلات احتمالی در حین ارسال و دریافت ایمیل



شکل ۲۰– گزینه‌های متفاوت خطایابی ارسال و دریافت ایمیل

همچنین با انتخاب گزینه‌ی Queue Viewer می‌توان وضعیت ایمیل‌های ارسالی و ایمیل‌های قرار گرفته در صف ارسال، آخرین خطاهای سیستم و مشکلات احتمالی موجود را مشاهده نمود. یکی از کاربردهای مهم آن تشخیص حملات Spam از اینترنت، فیلتر کردن و حذف کلی پیغام‌های ناخواسته می‌باشد.

شکل ۲۱– بررسی وضعیت ارسال و دریافت اشخاص از طریق برنامه OWA .

فصل ۵ – بررسی تنظیمات Client Access Server

تمام کلاینت‌هایی که از پروتکل MAPI استفاده نمی‌کنند (یعنی کلیه برنامه‌ها منهای Outlook)، جهت دسترسی به اطلاعات صندوق‌های پستی الکترونیکی از Client Access Server استفاده خواهند کرد. به همین جهت در یک Active directory domain که داری Mailbox Server می‌باشد، وجود یک سرور با نقش Client Access نیز الزامی است. کلاینت‌هایی که به CAS نیاز دارند شامل موارد زیر می‌باشند:

- Outlook web access (برنامه‌ی مخصوص تحت وب مرور ایمیل‌ها)
- ActiveSync (جهت دسترسی کاربرانی که از موبایل خود جهت مرور ایمیل‌ها استفاده می‌کنند. به صورت پیش فرض فعال است.)
- Outlook anywhere
- POP3 و یا IMAP4
- CAS Services

معرفی Outlook web access

Outlook web access برنامه‌ی تحت وب نوشته شده با ASP.Net است که حین نصب نقش CAS بر روی سرور مورد نظر نصب خواهد گردید. کاربران توسط این برنامه می‌توانند بدون نیاز به نصب برنامه‌ی خاصی بر روی رایانه خود، ایمیل‌های خود را از طریق یک مرورگر وب مرور نمایند. مهم‌ترین تغییر OWA در Exchange server 2010 سازگاری آن با اکثر مرورگرهای امروزی است که در نگارش قبلی آن که به همراه Exchange server 2010 ارائه می‌شد اینگونه نبود و سایر مرورگرها بجز IE ، تنها قسمتی از توانایی‌های OWA را می‌توانستند مشاهده نمایند. مزیت دیگر استفاده از OWA ، امکان دسترسی به صندوق‌های پستی Exchange server 2010 از طریق سایر سیستم عامل‌های موجود در دنیا است.

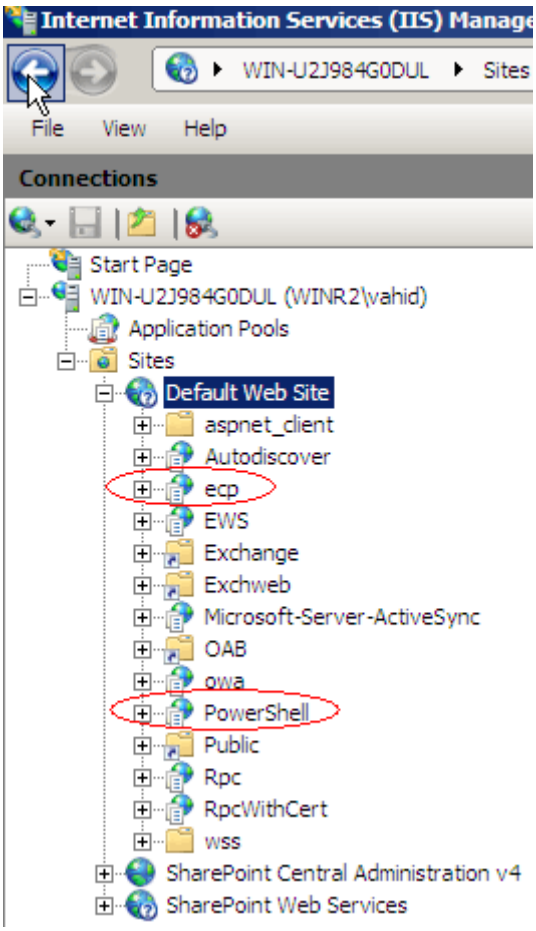
بهترین پشتیبانی از Exchange server 2010 از طریق نرم افزار Outlook انجام می‌شود و برای مثال دسترسی آفلاین به ایمیل‌ها از طریق OWA میسر نیست.

کاربران جهت مشاهده‌ی OWA تنها کافی است مسیر ذیل را در مرورگر خود وارد نمایند:

https://servername/owa

جهت مدیریت دایرکتورهای مجازی OWA می‌توان از کنسول مدیریتی IIS7 استفاده نمود (شکل ۱). همانطور که در تصویر نیز مشخص است دو مورد جدید و مهمی که به OWA اضافه شده‌اند ECP و PowerShell می‌باشند. ECP اکثر امکانات مدیریتی روزمره Exchange server 2010 را از طریق یک برنامه تحت وب در اختیار شما قرار خواهد داد

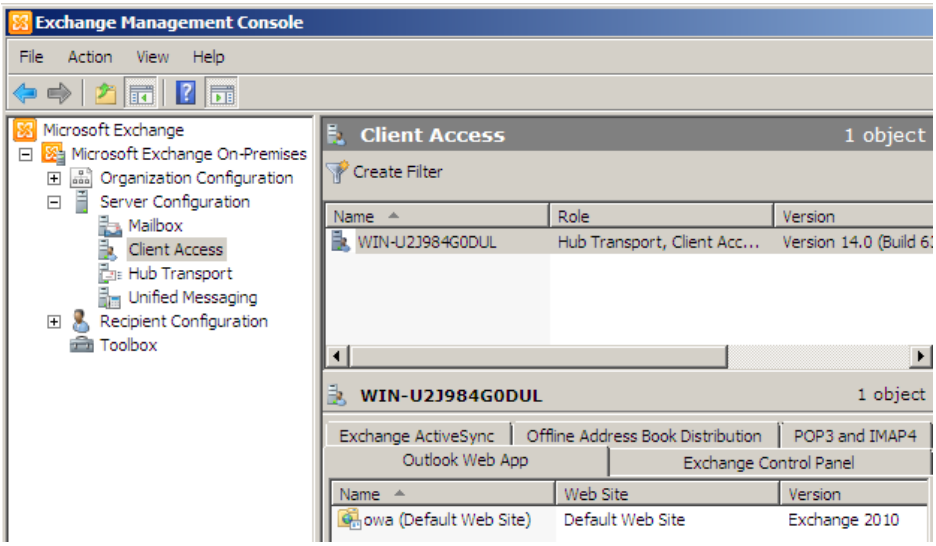
و همچنین پوشه مجازی PowerShell آن امکان اجرای دستورات PowerShell را از راه دور نیز میسر می‌سازد که این مورد از قابلیت‌های جدید PowerShell 2.0 می‌باشد.



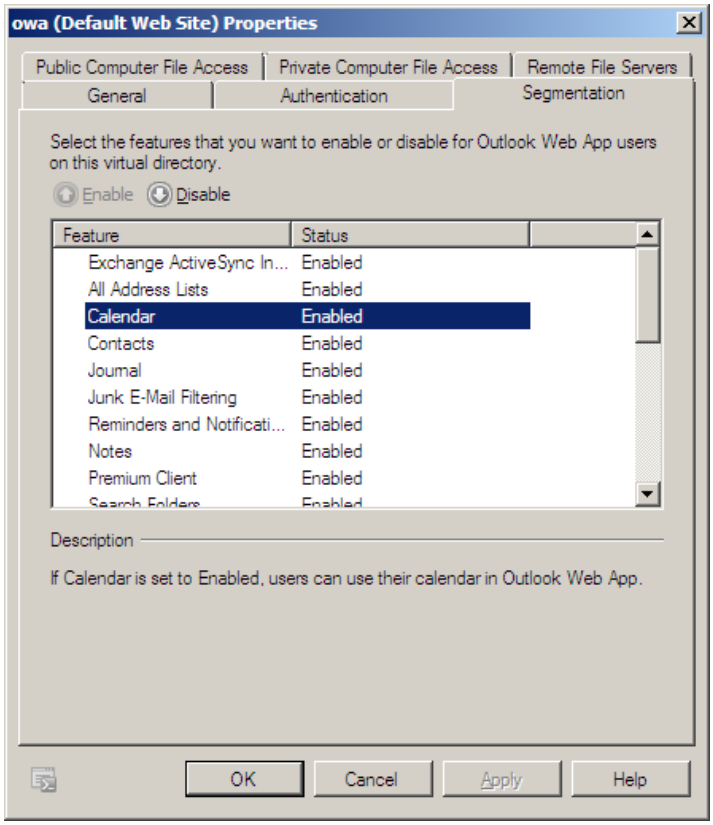
شکل ۱– کنسول مدیریتی IIS7 و پوشه‌های مجازی OWA .

همچنین از طریق کنسول مدیریتی Exchange server نیز می‌توان مواردی مانند تغییر آدرس و سطوح دسترسی و غیره را نیز مدیریت نمود. برای این منظور باید به قسمت Server configuration گزینه Client access مراجعه کرد (شکل ۲). در اینجا امکانات مدیریتی پوشه‌های مجازی OWA به شکل واضح‌تری وجود دارند. یک برگه به OWA اختصاص یافته و برگه‌های دیگر جهت مدیریت تنظیمات ECP یا Exchange control panel ، Exchange ActiveSync و OAB یا Offline address book بکار می‌روند. تمام این موارد تنظیمات مشابهی را ارائه می‌دهند که شامل مشخص سازی نحوه‌ی اعتبار سنجی جهت دسترسی به آن‌ها، آدرس داخلی و خارجی مرور آن‌ها و همچنین فعال و غیرفعال سازی ویژگی‌های آن می‌باشند. برای مثال اگر نیاز بود تا قابلیت تقویم OWA از آن حذف شود تنها کافی است به برگه‌ی Segmentation خواص OWA مراجعه کرده (شکل ۳) و این قابلیت را غیرفعال نمود. به صورت پیش فرض تمامی قابلیت‌های این برنامه فعال هستند.

اگر مطالب فصل‌های قبل را به خاطر داشته باشید، امکان تنظیم این ویژگی‌ها به ازای یک فرد نیز میسر است (تنظیمات فوق بر روی کل سازمان اثر گذار خواهند شد). برای این منظور باید به خواص صندوق پستی یک کاربر مراجعه کرده و در برگه‌ی Mailbox features آن برای مثال OWA را غیرفعال نمود.

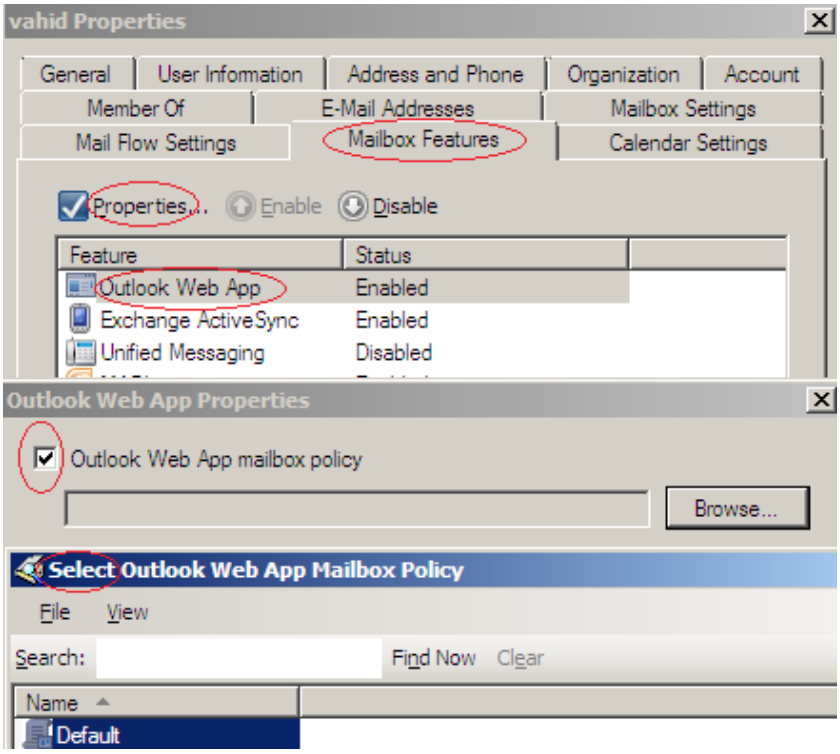


شکل ۲– مدیریت CAS از طریق کنسول مدیریتی Exchange server .



شکل ۳– فعال و یا غیرفعال سازی ویژگی‌های مختلف OWA .

اگر به برگه‌ی Mailbox features یک صندوق پستی مراجعه کنیم، در نگاه اول امکان تنظیمات ریز ویژگی‌ها وجود ندارد. به عبارت دیگر یا OWA را می‌توان برای یک کاربر غیرفعال ساخت و یا برعکس. اگر نیاز به اعمال تنظیمات ریزتری وجود داشت می‌توان به قسمت Organization configuration و گزینه‌ی Client Access آن مراجعه کرد. در اینجا می‌توان برای ActiveSync (کاربران موبایل) و یا OWA یک سیاست جدید را تعریف نمود (برای مثال فقط تقویم غیرفعال شود). سپس امکان اعمال این سیاست به یک صندوق پستی خاص وجود دارد (شکل ۴).



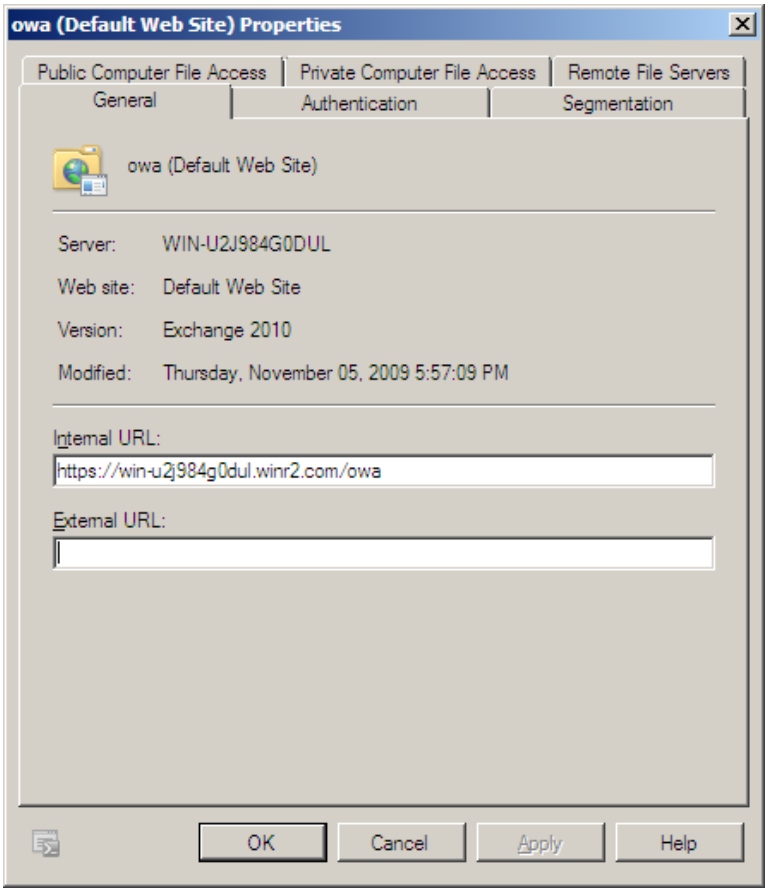
شکل ۴– امکان اعمال سیاستی مشخص به یک صندوق پستی.

تصحیح تنظیمات SSL مربوط به Outlook web access

برای مشاهده‌ی صفحه تنظیمات OWA یا می‌توان به IIS مراجعه نمود و یا از کنسول مدیریتی Exchange server 2010 استفاده کرد. برای این منظور به قسمت Server configuration گزینه Client Access و سپس برگه‌ی Outlook web app مراجعه کنید. در اینجا تنظیمات OWA را در برگه‌ی خواص آن می‌توان مشاهده‌نمود (شکل ۵).

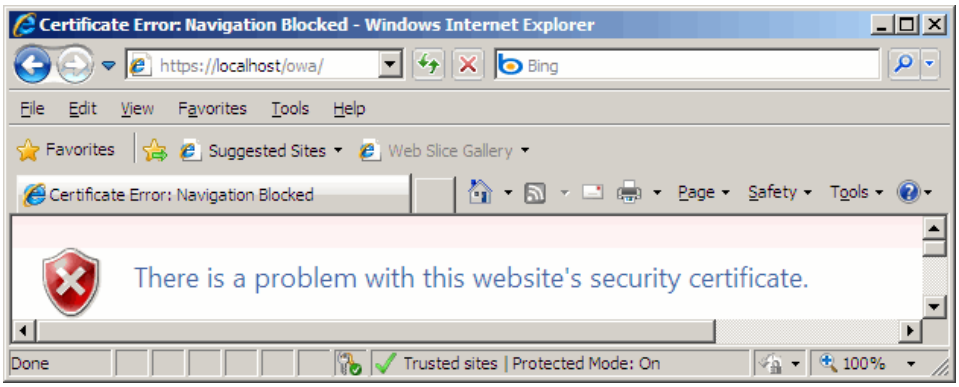
برای مثال در برگه General آن آدرس دسترسی به آن در شبکه داخلی مشخص شده است. همچنین اگر این برنامه قرار است از اینترنت نیز مورد استفاده قرار گیرد، امکان مشخص سازی آدرس آن نیز بر اساس نام DNS تهیه شده، میسر است.

برخلاف نسخه قبلی OWA مربوط به Exchange server 2007 که تنها هنگام استفاده از مرورگر IE مایکروسافت امکان استفاده از تمامی قابلیت‌های آن وجود داشت، نسخه جدید OWA با تمامی مرورگرهای جدید نیز بدون مشکل و در حالت کامل کار می‌کند.



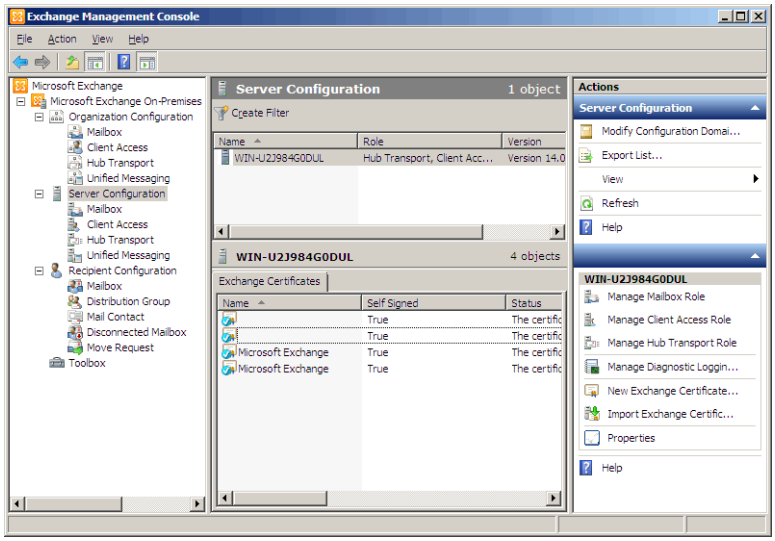
شکل ۵– برگه تنظیمات OWA .

جهت امنیت بیشتر Outlook web access ، این سایت باید از طریق آدرس‌های https مورد استفاده قرار گیرد. اولین مشکلی که کاربران حین استفاده از این سایت با آن مواجه خواهند شد، خطای غیرمعتبر بودن مجوز SSL سایت است (شکل ۶).



شکل ۶– مجوز پیش فرض SSL سایت OWA معتبر نیست و باید اصلاح شود.

هنگام نصب اولیه Exchange server 2010 یک سری مجوز SSL نیز بر روی سرور نصب می‌شوند که در قسمت Server configuration کنسول مدیریتی Exchange server قابل مشاهده هستند (شکل ۷). به صورت پیش فرض نیز یکی از این تنظیمات جهت سایت OWA مورد استفاده قرار می‌گیرد؛ اما از آنجائیکه گزینه‌ی Issued to آن در IIS دقیقا به نام کامپیوتر جاری سرور تنظیم شده است، هنگام استفاده از آن توسط آدرس صحیح DNS مربوط به سایت OWA ، خطای غیرمعتبر بودن مجوز SSL را دریافت خواهیم کرد (گزینه Issued to نیز باید دقیقا با آدرس DNS تنظیم شده هماهنگ باشد).



شکل ۷– مجوزهای پیش فرض نصب شده توسط Exchange server 2010 .

جهت تولید یک مجوز SSL جدید با استفاده از قابلیت تولید self-signed certificates ارائه شده در IIS7 و سپس استفاده از آن باید به ترتیب زیر عمل کرد:

۱– به کنسول مدیریتی IIS7 مراجعه نمائید (شکل ۸).

۲– نام سرور را انتخاب نموده و سپس به گزینه‌ی Server certificates آن مراجعه نمائید (شکل ۹).

۳- در قسمت Server certificates تمامی مجوزهای نصب شده توسط Exchange server 2010 را می‌توان مشاهده نمود. به صورت پیش فرض مجوز WMSvc-ServerName به عنوان مجوز پیش فرض سایت OWA استفاده شده است. همانطور که در شکل نیز مشاهده می‌کنید Issued to آن مطابق با نام DNS سرور جاری نیست و به همین جهت کاربران خطای معتبر نبودن مجوز SSL مورد استفاده را دریافت می‌کنند.

۴- اکنون در همین قسمت بر روی لینک Create self-signed certificate در برگه actions سمت راست صفحه کلیک نمائید.

۵- در صفحه باز شده، Friendly name را به صورت ComputerName.domain.com وارد نمائید (فرض بر این است که DNS مربوط به OWA نیز به همین صورت (بر اساس نام صحیح کامپیوتر و دومین جاری) تنظیم شده است) (شکل ۱۰).

۶- پس از ایجاد این مجوز SSL جدید، اکنون نوبت به معرفی آن به صورت یک مجوز امن می‌باشد در غیراینصورت باز هم کاربران همان صفحه‌ی نمایش خطای غیرمعتبر بودن مجوز SSL را دریافت خواهند کرد. برای این منظور ابتدا باید این مجوز تولیدی را Export کرد. ابتدا مجوز را انتخاب نموده و سپس بر روی لینک Export در برگه Actions سمت راست صفحه کلیک نمائید (شکل ۱۱).

۷- سپس در صفحه ظاهر شده باید مسیری را جهت ذخیره شدن این مجوز به همراه یک کلمه عبور دلخواه مشخص نمود (شکل ۱۲).

۸- پس از تهیه خروجی از آن، درRun منوی Start ویندوز تایپ کنید : certmgr.msc تا Certificate Manager ویندوز ظاهر شود (شکل ۱۳).

۹- در کنسول Certificate Manager ، بر روی Trusted Root Certification Authorities > Certificates کلیک راست نموده و از منوی ظاهر شده گزینه All Tasks > Import را انتخاب نمائید تا بتوانیم فایل pfx. تولیدی در قسمت قبل را به عنوان یک مجوز امن معرفی کنیم.

۱۰- اکنون صفحات مراحل مختلف معرفی فایل pfx.ظاهر می‌شوند. ابتدا باید مسیر فایل مربوطه را مشخص کرد (شکل ۱۴).

۱۱-سپس کلمه عبور فایل pfx. را وارد نمائید (شکل ۱۵).

۱۲-در ادامه بر روی دکمه browse کلیک کرده و در صفحه ظاهر شده ابتدا گزینه Show physical stores را انتخاب کنید. اکنون مطابق شکل گزینه Trusted Root Certification Authorities > Local Computer باید انتخاب شود (شکل‌های ۱۶ و ۱۷).

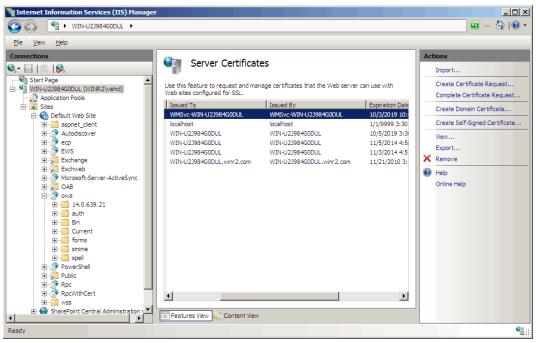
۱۳-سپس صفحه پایان مراحل معرفی نمایان خواهد شد (شکل ۱۸).

۱۴-تا اینجا مراحل معرفی این مجوز جدید به صورت یک مجوز امن به پایان رسید. اکنون نوبت به تغییر تنظیمات پیش فرض IIS است. مجددا به کنسول مدیریتی IIS7 مراجعه نمائید. در قسمت Sites ، گزینه Default web sites را انتخاب کرده و در برگه Actions سمت راست صفحه بر روی لینک bindings کلیک نمائید (شکل ۱۹).

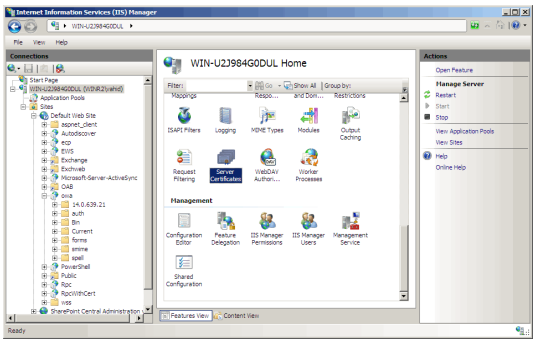
۱۵–در صفحه ظاهر شده گزینه https را یافته و سپس بر روی دکمه Edit کلیک نمائید (شکل ۲۰).

۱۶–در صفحه ویرایش تنظیمات مجوزهای SSL، مجوز جدیدی را که ساخته‌ایم معرفی خواهیم کرد (شکل ۲۱).

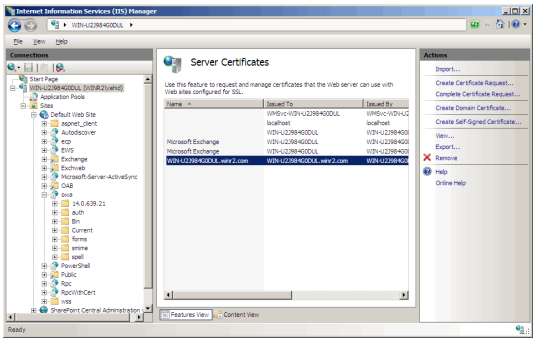
۱۷– اکنون اگر OWA را از طریق آدرس : https://compuetrName.domain.com/owa مرور نمائیم، سایت مذکور را بدون هیچگونه مشکل و خطایی مشاهده خواهیم کرد (شکل ۲۲).



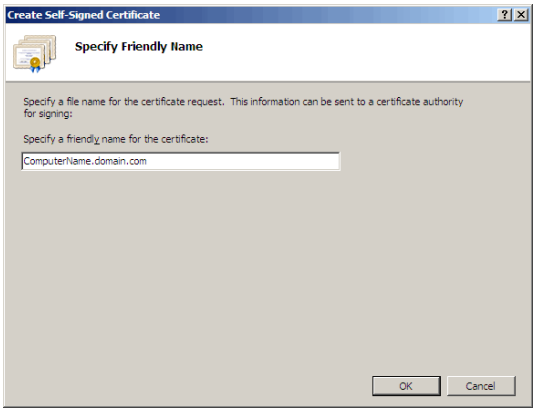
شکل ۹– مجوزهای SSL نصب شده بر روی وب سرور ویندوز ۲۰۰۸



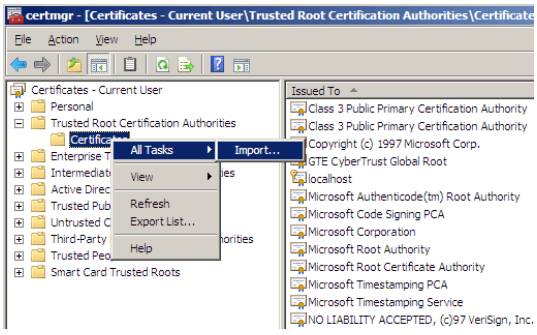
شکل ۸– کنسول مدیریتی IIS7 و قسمت Server certificates آن



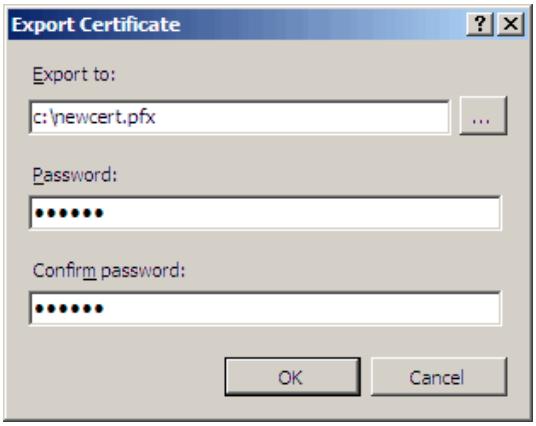
شکل ۱۱– نمایی از مجوز جدید اضافه شده



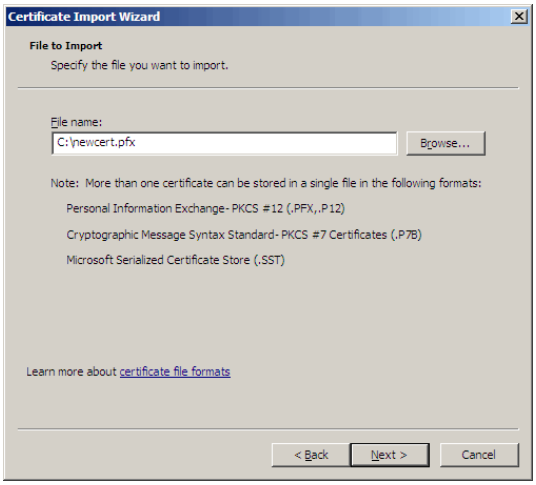
شکل ۱۰– ایجاد یک مجوز جدید



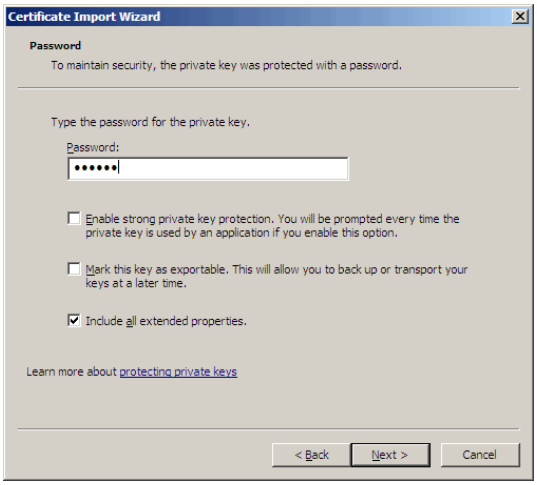
شکل ۱۳– معرفی مجوز تهیه شده به صورت یک مجوز امن



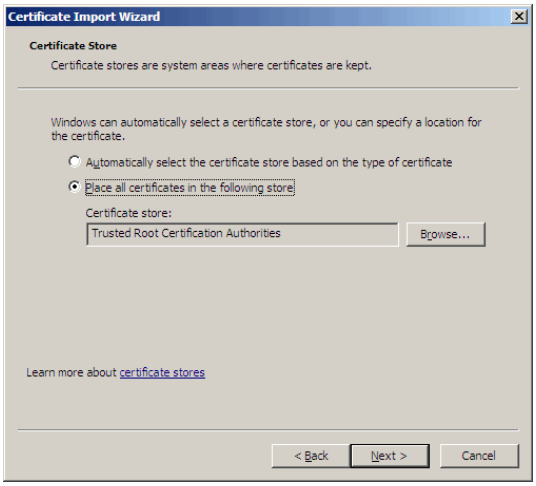
شکل ۱۲– تهیه یک خروجی از مجوز نصب شده



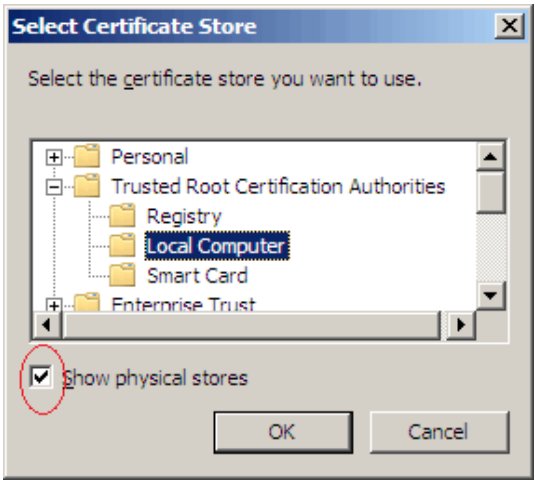
شکل ۱۴– مشخص سازی محل مجوز



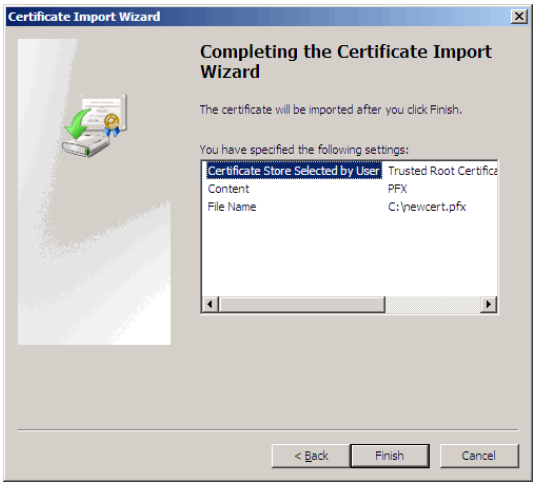
شکل ۱۵– ورود کلمه عبور متناظر با مجوز



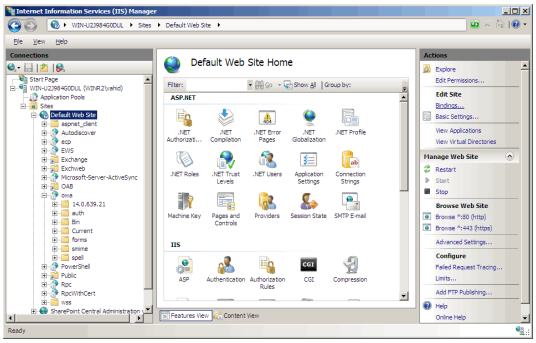
شکل ۱۶– مشخص سازی محل قرار گیری مجوز



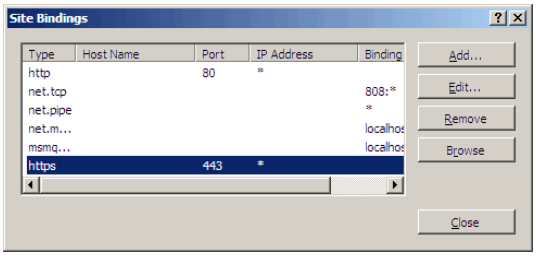
شکل ۱۷– مشخص سازی محل دقیق قرارگیری مجوز دریافت شده



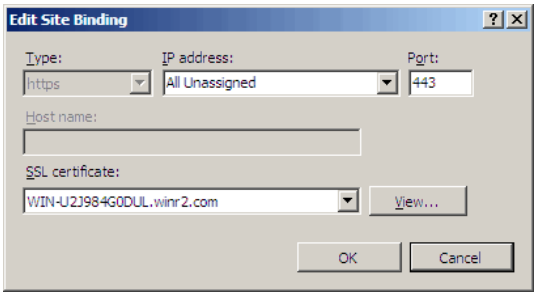
شکل ۱۸– پایان مراحل معرفی مجوز به صورت امن



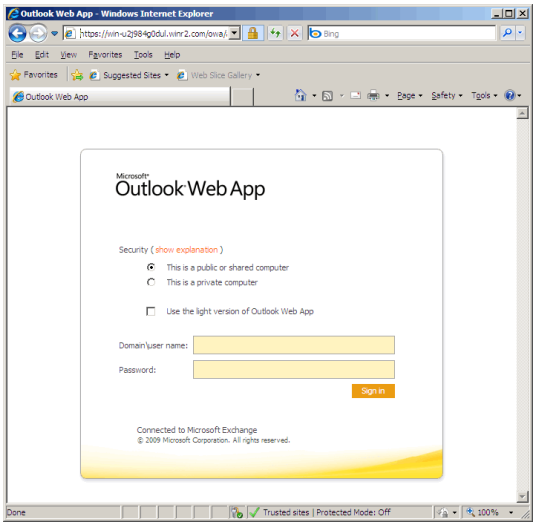
شکل ۱۹– تغییر تنظیمات binding سایت در کنسول مدیریتی IIS



شکل ۲۰– انتخاب گزینه Https



شکل ۲۱– ویرایش مشخصات مجوز SSL سایت



شکل ۲۲– مشاهده OWA بدون بروز خطا

استفاده از برنامه‌ی SelfSSL جهت تولید مجوزهای SSL

اگر نام DNS انتخاب شده برای سایت OWA با نام سرور جاری هماهنگی نداشته باشد، روش تولید مجوز SSL توسط IIS7 پاسخگو نبوده (زیرا توسط روش Self-signed certificate مربوط به IIS7 ، قسمت Issued to آن همواره به computerName.domain.com ختم خواهد شد) و تفاوتی مشاهده نخواهد شد (باز هم همان خطای غیرمعتبر بودن مجوز SSL را در مرورگر مشاهده خواهیم کرد). برای این منظور باید به روش زیر عمل کرد:

۱– دریافت مجموعه IIS6 Resource Kit و سپس مراجعه به برنامه SelfSSL.exe آن (این برنامه خط فرمان، امکان تنظیم دقیق قسمت Issued to را میسر می‌سازد). برنامه‌ی SelfSSL از آدرس زیر قابل دریافت است:

http://www.microsoft.com/downloads/details.aspx?FamilyID=56fc92ee-a71a-4c73-b628-ade629c89499&displaylang=en

۲– سپس روش استفاده از آن جهت تولید یک مجوز SSL به صورت زیر است:

```
SelfSSL /N:CN=<your web site address (no http://)> /V:<how many days
the certificate should be valid> /S:<site ID from above> [/P:<port, if not
443>]
```

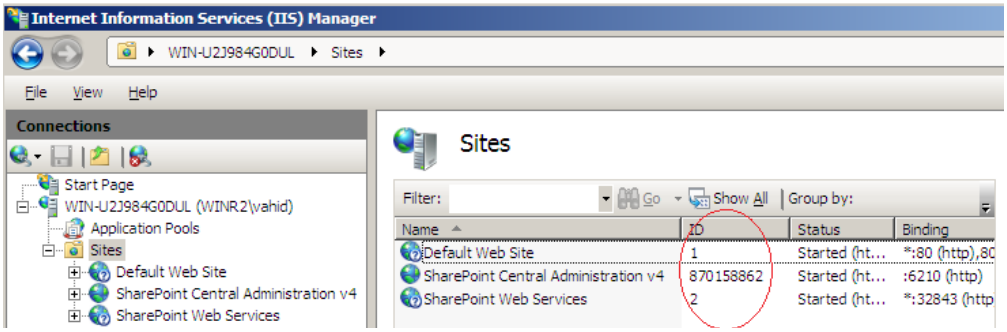
توسط روش IIS7 ، مجوز تولید شده تنها یکسال اعتبار خواهد داشت؛ اما در اینجا تعداد روز اعتبار را نیز دقیقا می‌توان مشخص کرد.

برای مثال اگر نام DNS تنظیمی ما جهت سایت OWA به صورت www.testssl.com باشد و قصد داشته باشیم به مدت هزار روز مجوز SSL ایی را برای آن صادر نمائیم، تنها کافی است در خط فرمان بنویسیم:

```
SelfSSL /N:CN=www.testssl.com /V:1000 /S:1
```

عددی که پس از پارامتر S می‌آید شماره ID سایت مورد نظر است (شکل ۲۳).

۳- اکنون سایر مراحل جهت معرفی این مجوز SSL به صورت یک مجوز امن و همچنین تغییر binding پیش فرض سایت مانند مراحل قبل است و تفاوتی ندارد.



شکل ۲۳– نحوه‌ی مشخص سازی اعداد مورد استفاده در پارامتر S برنامه SelfSSL.

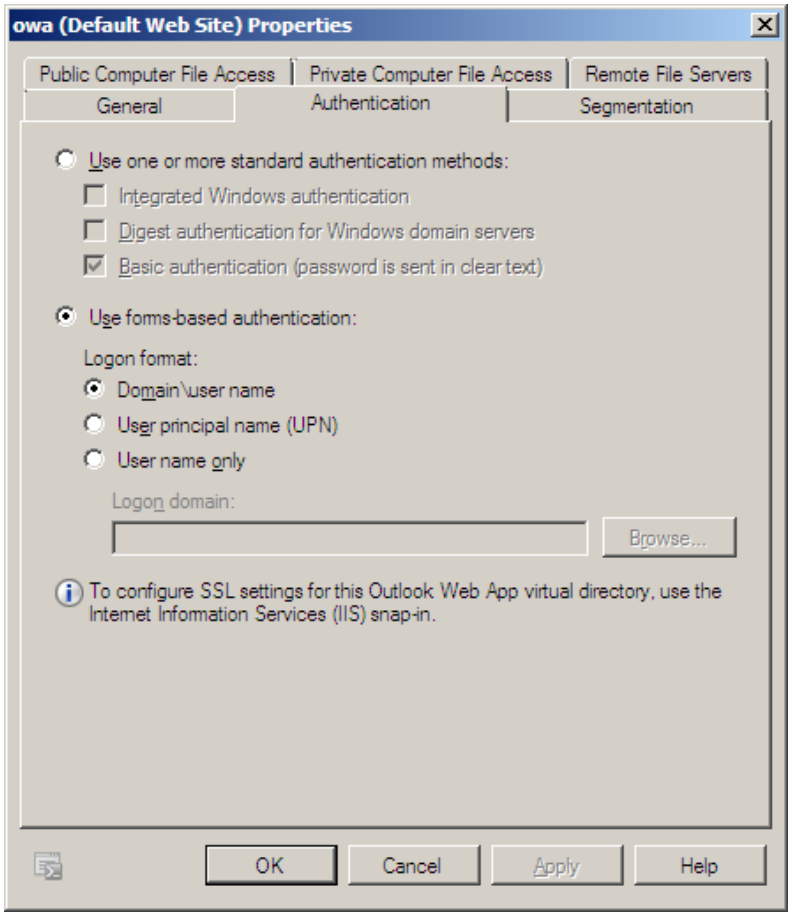
حذف صفحه‌ی ورود نام کاربری و کلمه‌ی عبور OWA و یکپارچه سازی آن با Active directory

برنامه‌ی OWA، حالت‌های مختلفی از اعتبار سنجی را پشتیبانی می‌کند که آن‌ها را در شکل ۲۴ مشاهده می‌نمائید. حالت پیش فرض نصب شده، Form-based authentication است که امکان استفاده از نام کاربری شخص در شبکه و سپس کلمه عبور آن‌را در هر بار مراجعه به برنامه میسر می‌سازد. این روش تنها در حالت استفاده از SSL، امن می‌باشد.

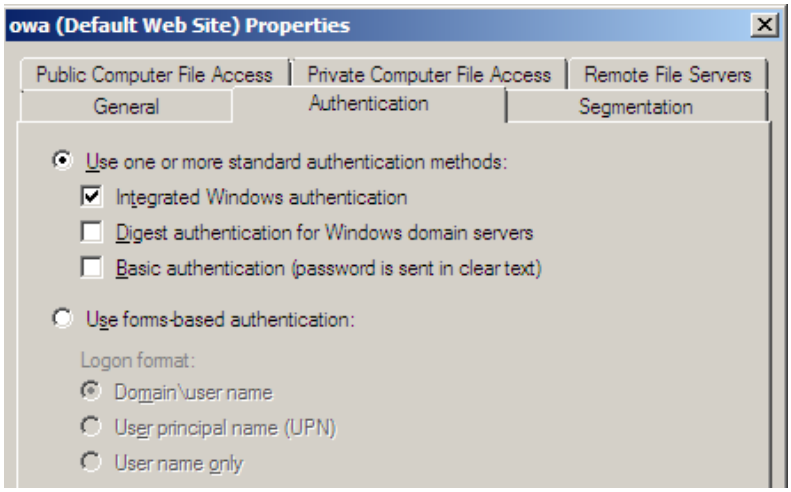
همیشه امن‌ترین حالت اعتبار سنجی کاربران در شبکه‌های ویندوزی و اینترانت داخلی، استفاده از حالت Integrated windows authentication می‌باشد. در این حالت از اعتبار حساب کاربری شخص وارد شده به سیستم بدون درخواست ورود نام کاربری و کلمه‌ی عبور او استفاده می‌گردد. همچنین در این حالت کلیه مراحل اعتبار سنجی به صورت رمزنگاری شده صورت خواهد گرفت.

برای تنظیم این مورد کافی است همانند شکل ۲۵ عمل شود و گزینه مربوطه انتخاب گردد. سپس مطابق اخطار شکل ۲۶، وب سرور ما نیز باید راه اندازی مجدد شود. برای این منظور دستور `iisreset /noforce` باید با سطح دسترسی مدیریتی در خط فرمان اجرا گردد.

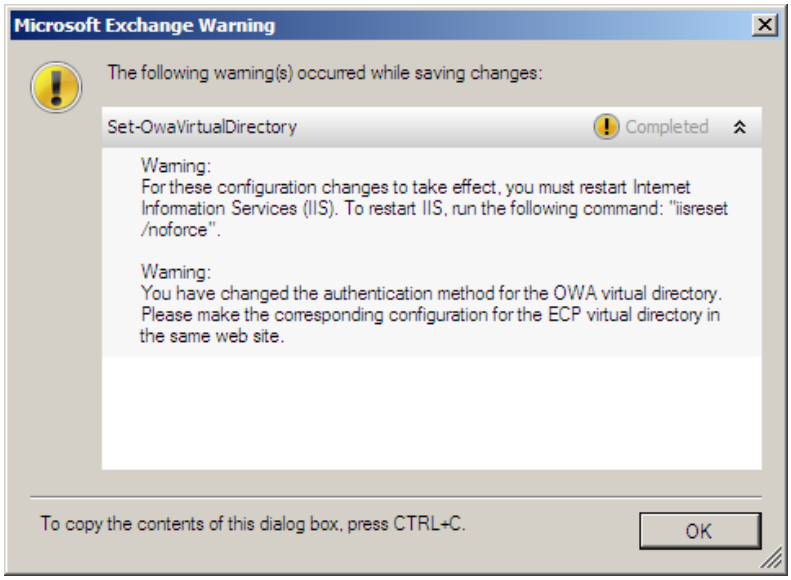
پس از این‌کار به کنسول مدیریتی IIS مراجعه کرده و دایرکتوری مجازی ECP را نیز انتخاب کنید. در قسمت Authentication آن، همانند شکل ۲۷ حالت `Windows authentication` را فعال نمائید. یا روش دیگر انجام این عملیات مراجعه به برگه‌ی `Exchange control panel` در قسمت `Server configuration` گزینه‌ی `Client Access` می‌باشد. ECP را یافته و سپس به خواص آن مراجعه نمائید. در اینجا نیز باید در برگه‌ی اعتبار سنجی صفحه‌ی باز شده، تغییرات مشابهی را اعمال نمود.



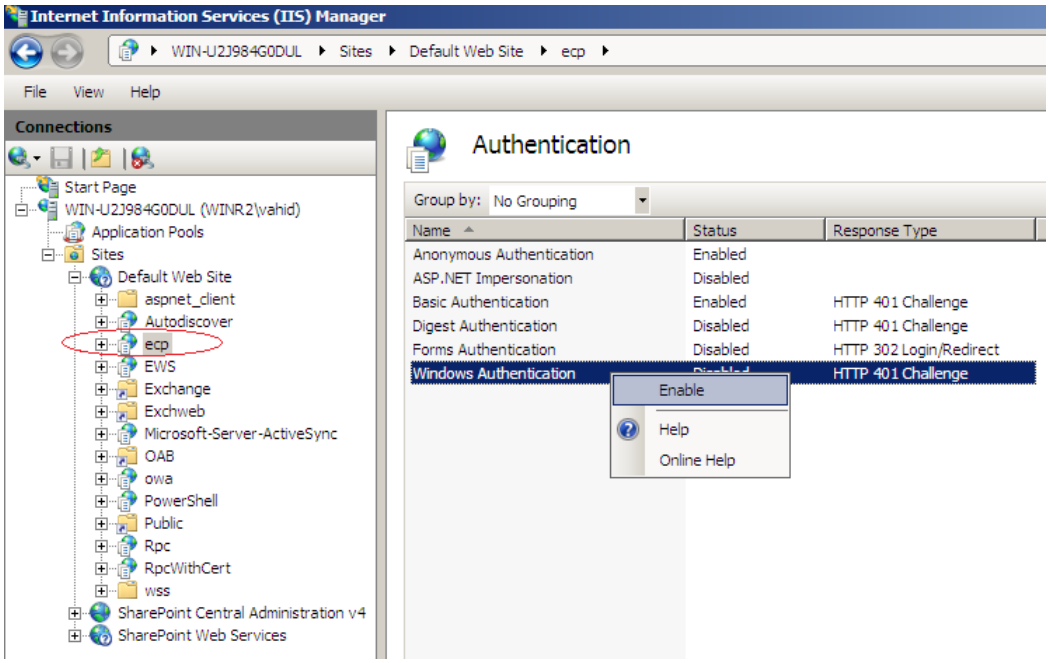
شکل ۲۴– حالت‌های مختلف اعتبار سنجی پشتیبانی شده توسط OWA .



شکل ۲۵– تغییر حالت اعتبار سنجی پیش فرض برنامه OWA .



شکل ۲۶– پس از تغییر نحوه اعتبار سنجی برنامه OWA نیاز به راه اندازی مجدد IIS می‌باشد.



شکل ۲۷– تغییر اعتبار سنجی دایرکتوری مجازی ECP .

لازم به ذکر است که جهت اعمال این تغییرات، نقش CAS باید بر روی سروری مجزا و اختصاصی نصب گردد. در غیراینصورت (اگر CAS به همراه سایر نقش‌ها بر روی یک سرور نصب شده) این تغییرات به درستی کار نخواهند کرد.

سایر مواردی که می‌توان در حین اعتبار سنجی مشخص ساخت به صورت زیر هستند:

- Basic Authentication : در این حالت کلمه عبور به صورت معمولی و رمزنگاری نشده در شبکه انتقال داده می‌شود. در صورت استفاده از این روش استفاده اجباری از SSL توصیه می‌شود.
- Digest Authentication : در این حالت کلمه‌ی عبور به صورت هش شده در طول شبکه انتقال داده می‌شود و با هش موجود در سرور مقایسه خواهد شد. این حالت نیاز به یک حساب کاربری در Active directory دارد.

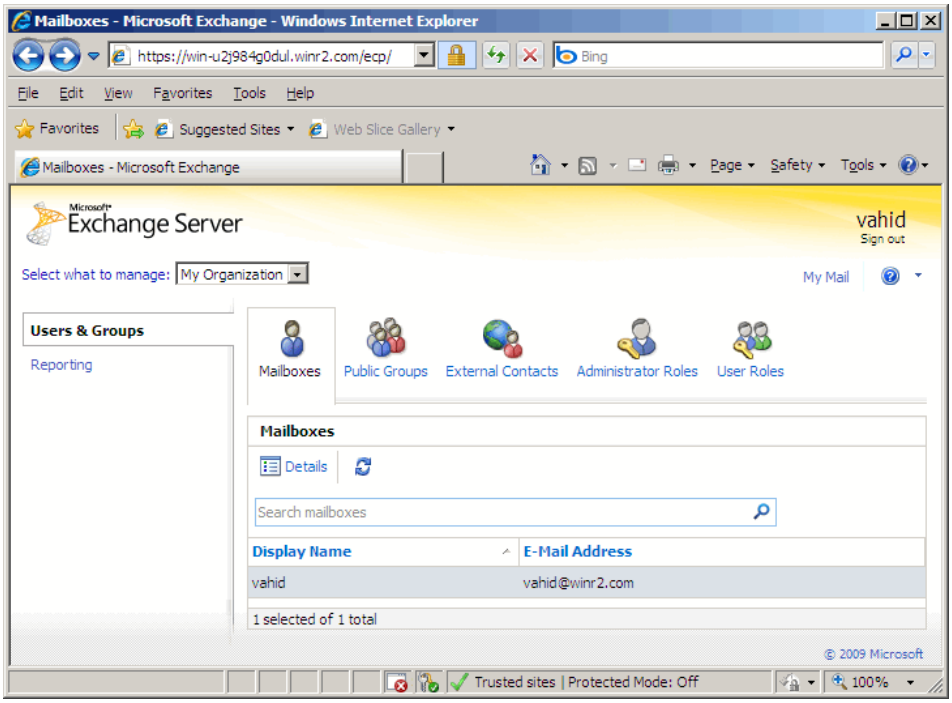
آشنایی با ECP یا Exchange control panel

یکی از قابلیت‌های جدید PowerShell ویندوز سرور ۲۰۰۸ ، PowerShell Remoting است که امکان مدیریت Exchange server را از راه دور مهیا می‌سازد. از همین قابلیت در برنامه‌ی تحت وب جدیدی به نام ECP در Exchange server 2010 جهت مدیریت کاربران، صندوق‌های پستی و امثال آن می‌توان استفاده کرد (شکل ۲۸). جهت دسترسی به آن باید به صورت زیر عمل نمود:

https://localhost/ecp/

بدیهی است همانطور که پیشتر نیز ذکر شد، جهت عدم مواجه شدن با خطای غیرمعتبر بودن مجوز SSL ، باید بجای localhost از نام DNS صحیح تنظیم شده در IIS استفاده کرد.

به همین جهت OWA دیگر مخفف Outlook web access نبوده و در این نگارش جدید، Outlook web application نامیده می‌شود و متشکل است از چندین برنامه‌ی مدیریتی و ملاحظه‌ی ایمیل‌های رسیده.



شکل ۲۸– نمایی از ECP در حالت استفاده از حساب کاربری با دسترسی پائین.

برنامه‌ی تحت وب ECP بر اساس مجوزهای کاربر وارد شده، امکانات مختلفی را ارائه خواهد داد. در حالت ورود با دسترسی یک کاربر معمولی (مانند شکل ۲۸)، تنها امکان تغییر و به روز رسانی مشخصات شخصی، وجود خواهد داشت. مزیت مهم این روش امکان تقسیم وظایف بین پرسنل مدیریتی شبکه است. به این ترتیب می‌توان بدون مراجعه به کنسول مدیریتی کامل Exchange server، بر اساس سطوح دسترسی تعریف شده، عملیات مدیریتی خاصی را انجام داد که اصطلاحا به آن Role Based Authentication Control یا RBAC گفته می‌شود.

برای مشاهده لیست این نقش‌های مدیریتی دستور زیر را در خط فرمان PowerShell وارد نمائید:

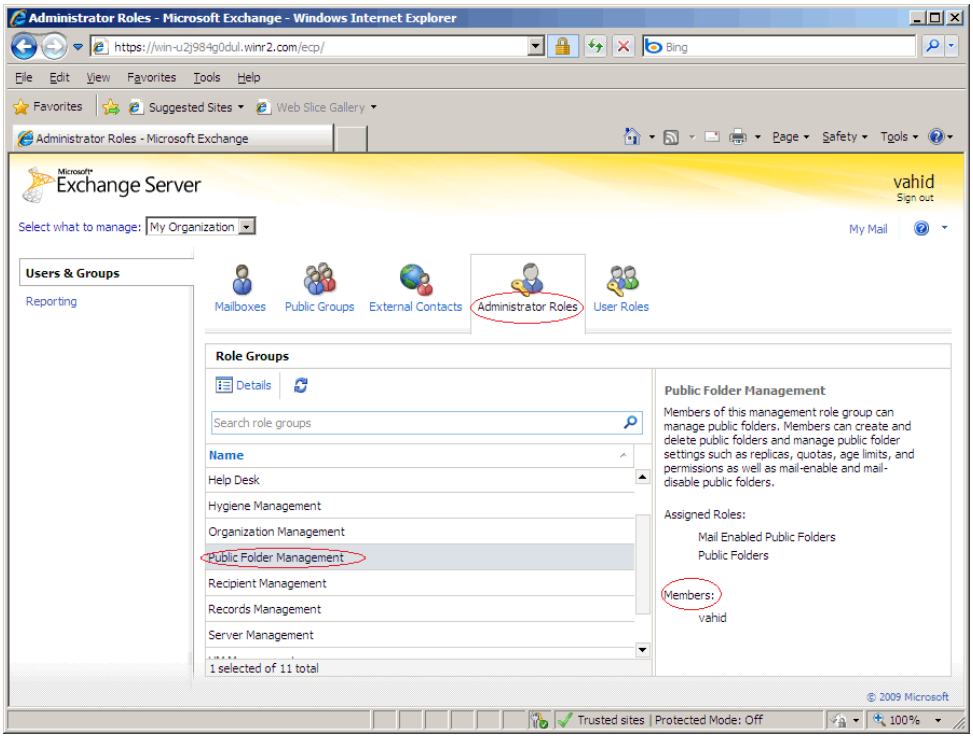
```
Get-ManagementRole
```

و یا جهت مشاهده تمامی نقش‌های انتساب داده شده می‌توان از دستور زیر استفاده نمود:

```
Get-ManagementRoleAssignment
```

برای افزودن افراد به این گروه‌ها و نقش‌های مدیریتی کافی است در برنامه‌ی تحت وب ECP به قسمت Administrator Roles مراجعه نموده، نقش مورد نظر را انتخاب کرده و کاربران دلخواهی را به کمک دکمه‌ی

Details به هر نقش افزود. همچنین هنگام انتخاب هر گروه در این قسمت، در پایان راهنمای سمت راست صفحه، اعضای گروه نیز لیست خواهند شد (شکل ۲۹).



شکل ۲۹– افزودن و یا حذف نقش‌های مدیریتی در ECP .

معرفی Outlook Anywhere

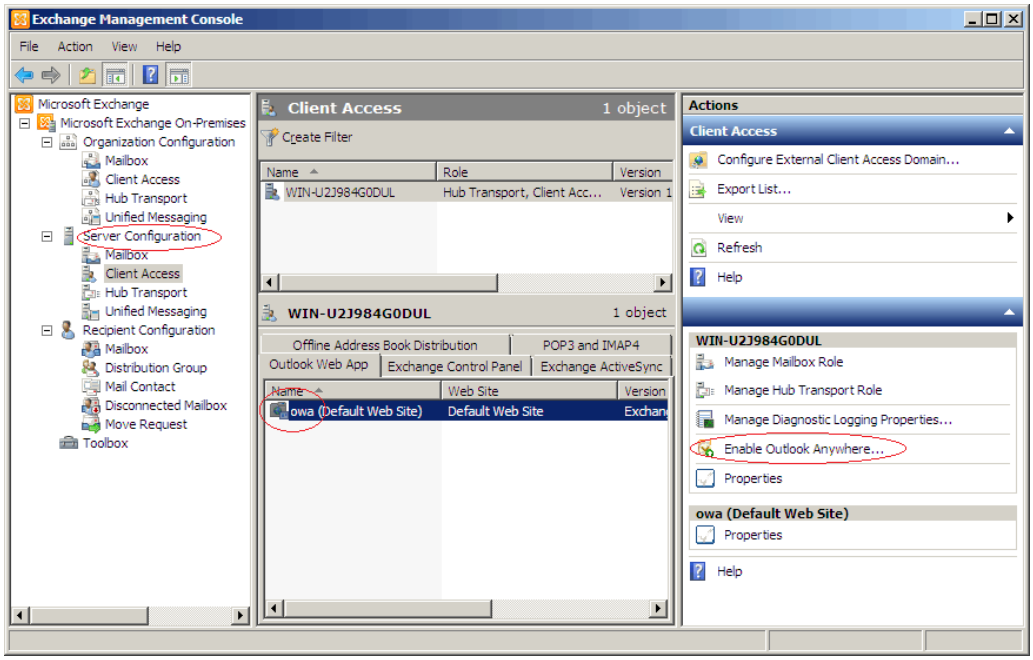
به Outlook Anywhere در نگارش‌های قبلی Exchange server ، RPC over HTTP نیز گفته می‌شد. از این حالت جهت استفاده از برنامه Outlook در خارج از سازمان برای برقراری ارتباط با داخل سازمان از طریق اینترنت استفاده می‌شود. در Exchange server 2003 برای برقراری این نوع ارتباطات می‌بایستی از VPN استفاده می‌شد. اما با بهبودهای حاصل شده در نگارش‌های پس از آن دیگر نیازی به استفاده از VPN جهت استفاده از Outlook در خارج از سازمان نیست.

برای استفاده از Outlook Anywhere ابتدا باید این قابلیت را در کنسول مدیریتی Exchange server 2010 فعال نمود. سپس جهت برقراری ارتباطات امن نیاز به یک مجوز SSL خواهد بود و در آخر باید کلاینت‌هایی که از این قابلیت استفاده می‌کنند نیز تنظیم شوند.

در فصل نصب اولیه Exchange server 2010 بر روی ویندوز سرور ۲۰۰۸ ، ویژگی RPC-over-HTTP-proxy را به کمک دستور خط فرمان ذیل نصب نمودیم:

```
ServerManagerCmd -I RPC-over-HTTP-proxy
```

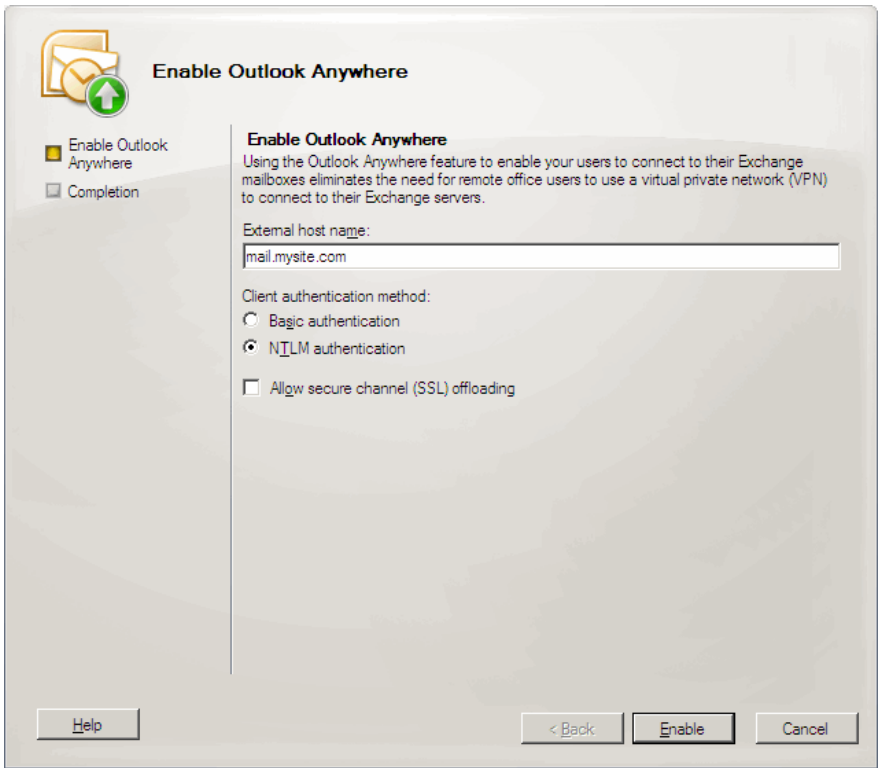
سپس به قسمت Server configuration گزینه Client access مراجعه کرده و در برگه Actions سمت راست صفحه، بر روی لینک Enable Outlook anywhere کلیک کنید (شکل ۳۰).



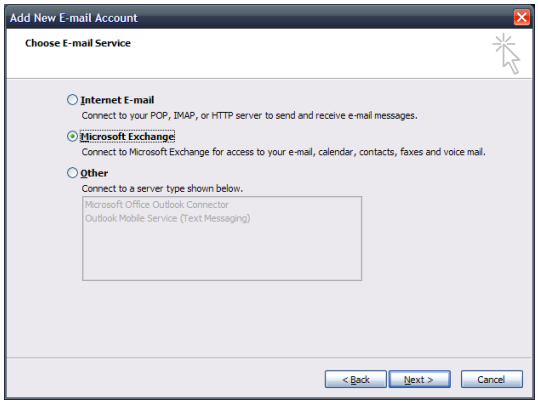
شکل ۳۰– فعال سازی Outlook anywhere از طریق کنسول مدیریتی Exchanger server 2010.

در صفحه‌ی باز شده (شکل ۳۱)، نام DNS خارجی میل سرور خود را وارد نمائید. NTLM authentication کلمات عبور را به صورت هش شده انتقال می‌دهد بنابراین امنیت بیشتری از روش Basic authentication خواهد داشت و همچنین سازگاری خوبی نیز با ISA Server دارد. اگر از یک شتاب دهنده‌ی SSL در سازمان خود استفاده نمی‌کنید، گزینه مربوط به SSL ارائه شده را انتخاب ننمائید. سپس بر روی دکمه‌ی Enable در پایین صفحه کلیک نمائید. این ویژگی پس از فعال سازی، حدود ۱۵ دقیقه طول خواهید کشید تا قابل استفاده نهایی شود. در این حالت تمام کاربران می‌توانند از این قابلیت استفاده نمایند.

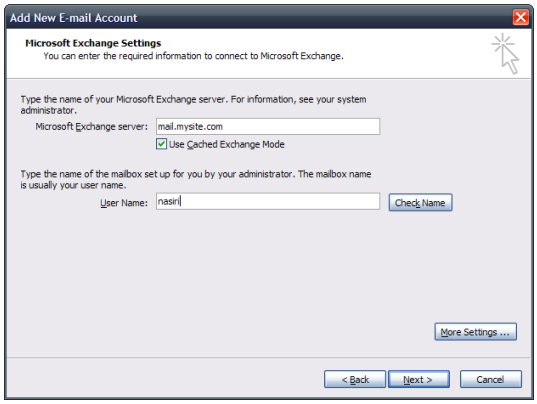
اکنون تمام کلاینت‌های Outlook خارج از سازمان شما باید همانند قبل به Control panel ویندوز خود مراجعه نموده، بر روی آیکون Mail کلیک نمایند. هر چند اکنون خارج از سازمان بوده و از طریق اینترنت قرار است ایمیل‌های خود را بررسی کنند، در اینجا نیز نوع اتصال را باید از نوع Exchange server انتخاب کنند (شکل ۳۲). در صفحه‌ی بعدی تنظیمات، باید مشخصات سرور و همچنین حساب کاربری وارد شود (شکل ۳۳). نکته‌ی مهم حین انجام تنظیمات این صفحه، مراجعه به قسمت More settings در پایین صفحه‌ی تنظیمات مشخصات سرور و سپس در صفحه‌ی باز شده، در برگه‌ی Connection آن باید گزینه‌ی مربوط به Outlook Anywhere را انتخاب نمود (شکل ۳۴). در ادامه بر روی دکمه‌ی تنظیمات Exchange server باید کلیک نموده و مشخصات دقیق سرور و نوع اعتبار سنجی را مشخص کرد (شکل ۳۵).



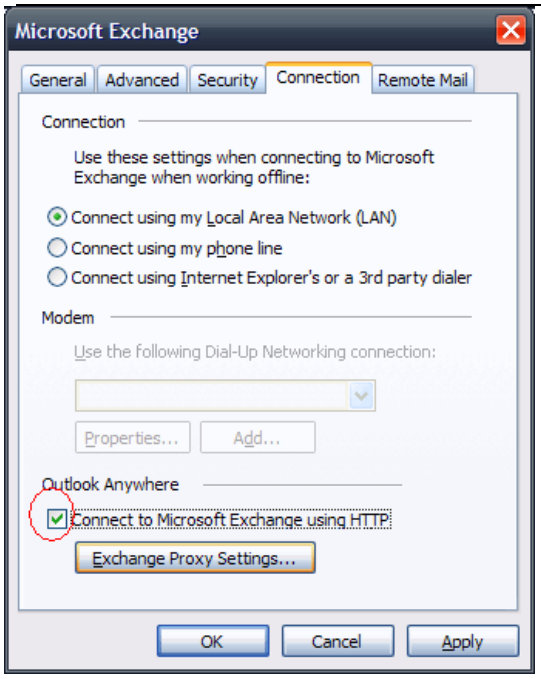
شکل ۳۱– وارد کردن نام DNS عمومی Exchange Server جهت فعال سازی Outlook Anywhere.



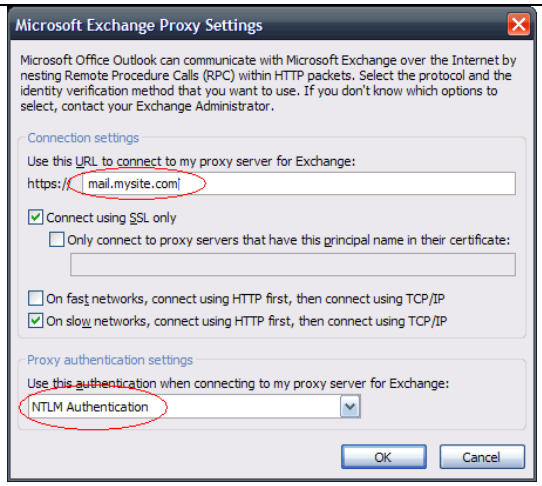
شکل ۳۲– اتصال به Exchange server



شکل ۳۳– وارد کردن مشخصات سرور و نام کاربری



شکل ۳۴– انتخاب گزینه Outlook anywhere



شکل ۳۵– تنظیمات Outlook anywhere

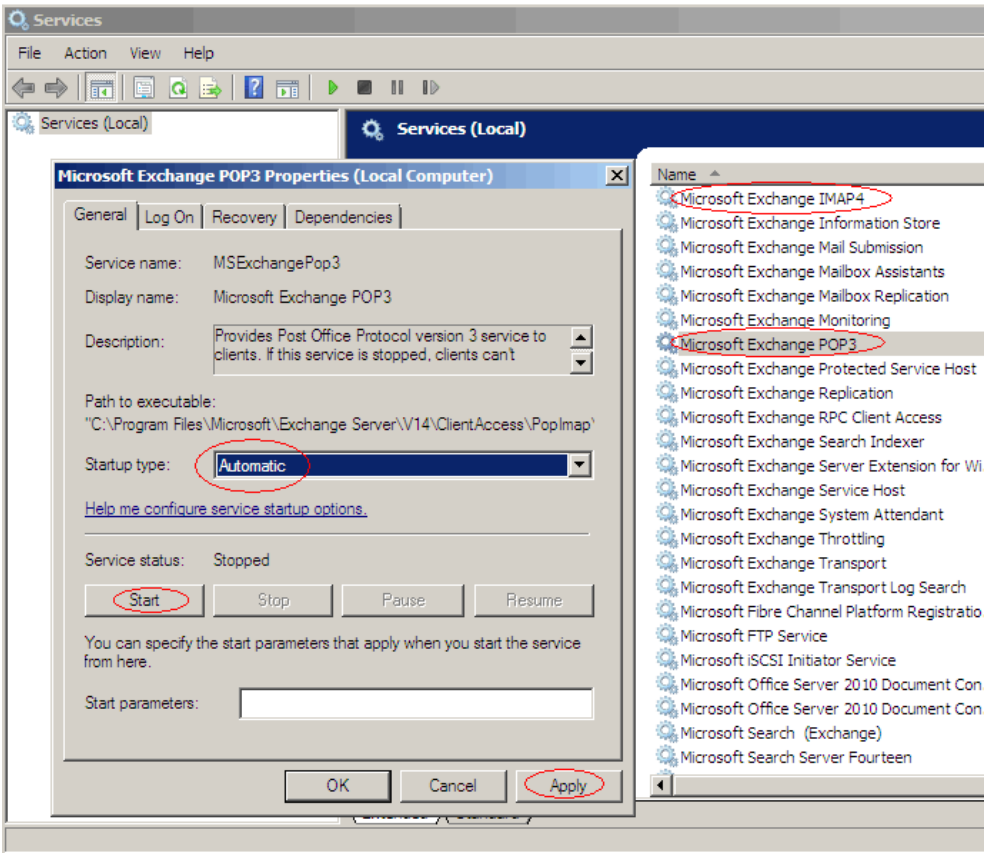
اگر از Outlook 2007 استفاده می‌کنید حتما باید آخرین به روز رسانی‌های آن‌را نیز نصب نمائید؛ زیرا تا پیش از سرویس پک ۲ آن، با این نوع ارتباطات RPC over HTTP مشکل وجود داشت و نیاز به تغییراتی در رجیستری ویندوز کلاینت‌ها ضروری بود (فایلی با پسوند reg. با محتوای زیر باید بر روی کلاینت‌ها اجرا می‌شد):

```
Windows Registry Editor Version 5.00
[HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Outlook\RPC]
"DefConnectOpts"=dword:00000000
```

فعال سازی سایر پروتکل‌ها

اگر به هر دلیلی قصد استفاده از سایر پروتکل‌های ارسال و دریافت ایمیل را داشته باشید باید به صورت زیر عمل نمود:

کنسول مدیریتی سرویس‌های ویندوز را اجرا نموده (شکل ۳۶) و سپس سرویس‌های Microsoft Exchange POP3 و Microsoft Exchange IMAP4 را یافته، فعال و آغاز نمائید.

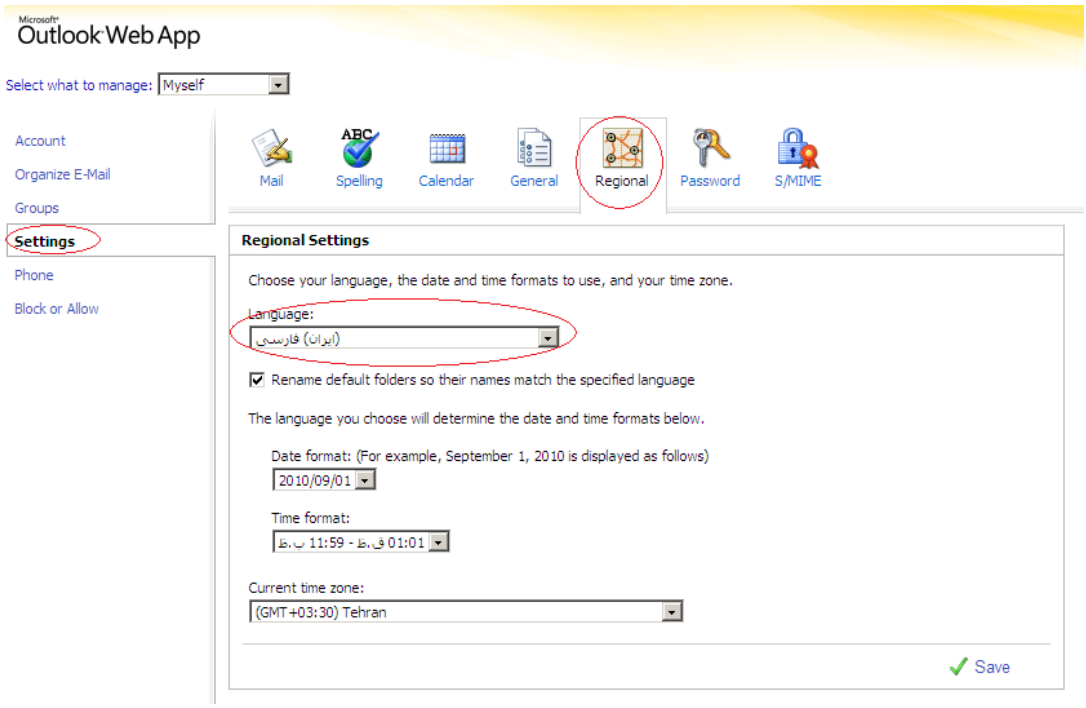


شکل ۳۶– فعال سازی سرویس‌های POP3 و IMAP4 .

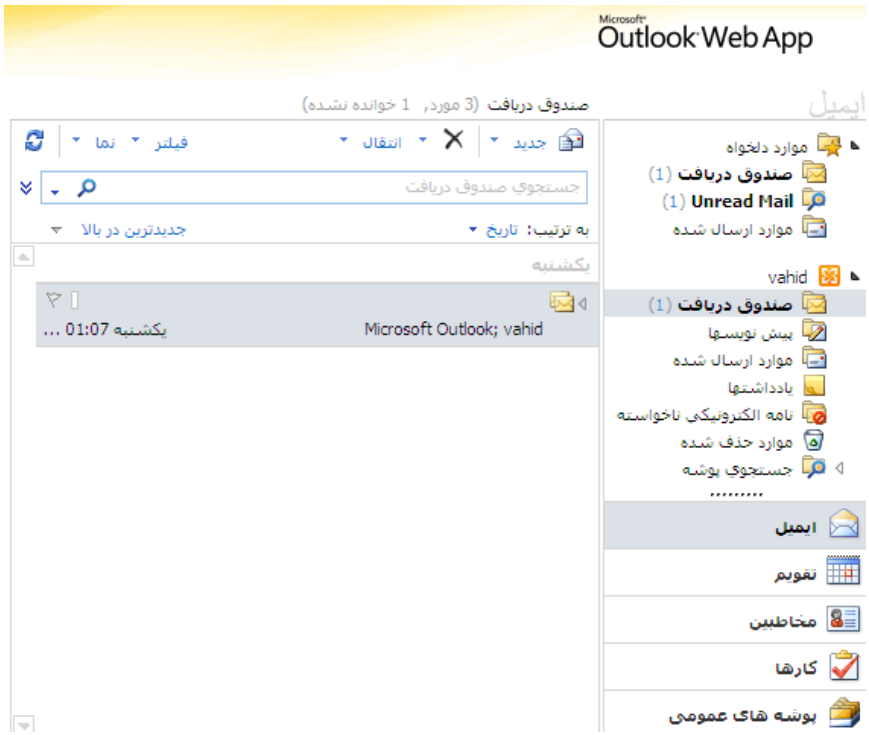
نصب و فعال سازی زبان فارسی برنامه‌ی OWA

برنامه‌ی Outlook web access همراه نگارش RTM مجموعه‌ی Exchange server 2010 شامل زبان فارسی نیست. اما با دریافت آخرین بسته‌ی به روز شده‌ی زبان‌های آن، زبان فارسی نیز به این مجموعه اضافه خواهد شد. برای دریافت این بسته به آدرس ذیل مراجعه نمائید:
http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=4ba91cf8-dafa-4328-9edc-2052fe8347fc

نصب آن نکته‌ی خاصی نداشته و صرفا با چندبار کلیک بر روی دکمه‌ی Next به پایان می‌رسد.
اکنون کاربران در قسمت Options برنامه‌ی OWA با مراجعه به گزینه‌ی Settings و برگه‌ی Regional آن می‌توانند زبان فارسی را انتخاب نمایند (شکل ۳۷). لازم به ذکر است که در لیست زبان‌های آن به دنبال کلمات Farsi و یا Persian نباید گشت. دقیقا عبارت <<(ایران) فارسی>> ذکر شده است. نمایی از برنامه OWA را پس از نصب و انتخاب زبان فارسی به عنوان زبان پیش فرض برنامه، در شکل ۳۸ ملاحظه می‌فرمائید.



شکل ۳۷– انتخاب زبان فارسی برای برنامه‌ی OWA .



شکل ۳۸– نمایی از برنامه OWA پس از انتخاب زبان فارسی به عنوان زبان پیش فرض برنامه.

فصل ۶ – تهیه‌ی پشتیبان و آشنایی با نحوه‌ی بازیابی اطلاعات

هنگامیکه سیستم ارسال و دریافت ایمیل در یک سازمان راه اندازی می‌شود و پس از مدتی پرسنل جهت انجام بسیاری از کارها و هماهنگی‌ها از آن استفاده کرده و به آن خو می‌گیرند، تحمل چند دقیقه از کار افتادن سیستم و قطع این پل ارتباطی برای آن‌ها بسیار مشکل و غیر قابل تحمل خواهد شد. به همین جهت تهیه‌ی پشتیبان‌های منظم و آشنایی با نحوه‌ی بازیابی آن‌ها یکی از موارد اساسی مدیریت Exchange server 2010 می‌باشد.

سیاست‌های مختلف تهیه پشتیبان از Exchange server 2010

- Full backup:
  - شامل تهیه پشتیبان آنلاین کامل (زمانیکه Exchange server در حال کار است) از فایل‌های بانک اطلاعاتی Exchange server و لاگ‌های تراکنش‌های آن است. در این حین، تراکنش‌های کامل و اعمال شده از مجموعه لاگ‌ها حذف می‌شوند.
- Incremental backup:
  - تهیه Full back پایه تمامی انواع مختلف پشتیبان‌ها است. بنابراین قبل از هر کاری و استفاده از هر روشی نیاز است تا ابتدا یک پشتیبان کامل تهیه شود. اگر بانک‌های اطلاعاتی ما حجیم باشند، تهیه پشتیبان کامل، زمانبر و نیاز به فضای قابل توجهی خواهد داشت. برای این منظور می‌توان از روش Incremental backup استفاده کرد. در این حالت تنها از اطلاعاتی که پس از تهیه یک پشتیبان کامل و یا پس از تهیه آخرین Incremental backup به سیستم اضافه شده‌اند، پشتیبان تهیه خواهد شد. در این حالت نیز تراکنش‌های کامل و اعمال شده از مجموعه لاگ‌ها حذف می‌شوند.
- Differential backup:
  - در این حالت از آخرین اطلاعات تغییر کرده پس از تهیه آخرین پشتیبان کامل از سیستم، پشتیبان تهیه می‌شود. این روش تاثیری بر روی فایل‌های تراکنش‌های سیستم ندارد.
- Copy backup:
  - پشتیبان ساده‌ای است شبیه به Full backup از فایل‌های اصلی بانک اطلاعاتی سیستم. این روش نیز تاثیری بر روی فایل‌های تراکنش‌های سیستم نداشته و هیچ اثری از آن در سیستم ثبت و نگهداری نمی‌شود. توصیه می‌شود ماهی یکبار این نوع پشتیبان نیز تهیه شود.
- Brick-level backup:

- در این حالت از تک تک پیغام‌های موجود در صندوق‌های پستی کاربران پشتیبان تهیه خواهد شد. به فضای بیشتری نیاز داشته (نسبت به پشتیبان کامل) و همچنین طولانی‌تر است. در حالت پشتیبان کامل از پیغام‌های تکراری صرفنظر می‌شود. برای مثال اگر یک شخص، پیغامی را برای ۵۰ نفر ارسال کرده باشد در حالت Brick-level backup از هر ۵۰ پیغام ارسالی پشتیبان مجزایی تهیه خواهد شد؛ به همین جهت حجم بیشتری را نیز اشغال می‌کند. برای تهیه این نوع پشتیبان باید از ابزارهای جانبی شرکت‌های نرم افزاری مرتبط استفاده کرد و به صورت استاندارد پشتیبانی نمی‌شود. تهیه این نوع پشتیبان تنها برای افراد کلیدی سازمان توصیه می‌شود.

برای مثال اگر پشتیبان کاملی در پایان روز یک شنبه تهیه شده باشد، Incremental backup روز دوشنبه، تنها از اطلاعات اضافه شده در طی روز دوشنبه پشتیبان تهیه خواهد کرد. در ادامه اگر در روز سه شنبه یک Incremental backup دیگر تهیه شود، این پشتیبان تنها حاوی اطلاعات روز سه شنبه خواهد بود. بنابراین برای بازیابی این مجموعه نیاز است ابتدا پشتیبان کامل بازیابی شود و سپس به ترتیب، هر یک از Incremental backups تهیه شده باید بازیابی شوند.

در حالت Differential backup، اگر پشتیبان کامل در پایان روز یک شنبه تهیه شده باشد، Differential backup روز دوشنبه، تنها از اطلاعات اضافه شده در طی روز دوشنبه، پشتیبان تهیه خواهد کرد. در ادامه اگر در روز سه شنبه یک Differential backup دیگر تهیه شود، کار تهیه پشتیبان از روز دوشنبه شروع خواهد شد و شامل اطلاعات هر دو روز دوشنبه و سه شنبه خواهد بود. بنابراین در این حالت برای بازیابی اطلاعات تنها به اطلاعات پشتیبان کامل و آخرین Differential backup تهیه شده نیاز می‌باشد و سایر Differential backups موجود اهمیتی نخواهند داشت.

نکته – وضعیت لاگ‌های سیستم در حالت circular logging

در حالتی که Exchange server به circular logging تنظیم شود، لاگ‌های تراکنش‌های سیستم پس از کامل شدن، بازنویسی خواهند شد. به همین جهت در این حالت امکان تهیه Incremental backup و یا Differential backup وجود نخواهد داشت.

روش‌های مختلف تهیه پشتیبان از Exchange server 2010

دو روش کلی برای تهیه پشتیبان از Exchange server 2010 وجود دارد:

- Streaming backups:
  - روش استفاده از ابزار استاندارد Windows backup که سال‌ها است به همراه ویندوز ارائه شده و مورد استفاده قرار می‌گیرد (این روش در ویندوز سرور ۲۰۰۸ منسوخ شده است).

- Volume shadow copy service یا VSS :
  - برای اولین بار به همراه Exchange server 2003 ارائه شد. از روش Streaming backups بسیار سریعتر است و همچنین تقریبا تمامی ابزارهای جانبی که جهت تهیه پشتیبان از Exchange server توسط سایر شرکت‌های نرم افزاری ارائه شده‌اند از این روش استفاده می‌کنند. با استفاده از این روش Copy مخصوص، بدون نیاز به متوقف سازی سرویس‌های Exchange server می‌توان از اطلاعات بانک‌های اطلاعاتی آن پشتیبان تهیه کرد. همچنین در این حالت، برنامه نیز از تهیه این نوع پشتیبان مطلع می‌گردد. بنابراین فرصت خواهد داشت تا اطلاعات لازم را تهیه کرده و همچنین سیستم کش خود را تخلیه نماید تا دراین حین، اطلاعاتی از دست نرود.

از چه اطلاعاتی باید پشتیبان تهیه کرد؟

- بانک‌های اطلاعاتی :
  - از تمام بانک‌های اطلاعاتی Mailbox servers (همان فایل edb.) باید پشتیبان تهیه کرد. در حالت استفاده از نگارش سازمانی Exchange server تا ۱۰۰ بانک اطلاعاتی را می‌توان تعریف و استفاده نمود.
- لاگ‌های تراکنش‌های سیستم
- اطلاعات Active directory :
  - بدیهی است این مورد خارج از محیط Exchange server قرار می‌گیرد، اما باید دقت داشت که Exchange server بدون Active directory کار نخواهد کرد.
- تنظیمات Client access و Hub transport و سایر نقش‌های موجود

سیاست‌های مختلف بازیابی اطلاعات

- بازیابی ایمیلی حذف شده :
  - در این مورد و نحوه‌ی بازیابی یک ایمیل مهم حذف شده از طریق برنامه‌ی Outlook در طی فصل‌های قبل بحث شد (پایان فصل مدیریت و تنظیمات Mailbox servers). ایمیل‌های حذف شده تا ۱۴ روز قابل بازیابی هستند (این مورد از طریق برگه تنظیمات یک بانک اطلاعاتی Mailbox server قابل تغییر است).
- بازیابی صندوق پست الکترونیکی حذف شده:

- صندوق‌های پست الکترونیکی حذف شده به صورت پیش فرض تا ۳۰ روز نگهداری می‌شوند (این مورد نیز از طریق برگه تنظیمات یک بانک اطلاعاتی Mailbox server قابل تغییر است) و از طریق بازیابی پشتیبان‌های تهیه شده، قابل بازیابی خواهند بود که در ادامه در مورد جزئیات آن توضیحات لازم ارائه خواهد شد.

- بانک اطلاعاتی تخریب شده :
  - این مشکل از طریق بازیابی پشتیبان‌های تهیه شده قابل برطرف شدن است یا استفاده از گزینه‌های High availability که در طی فصول آتی در مورد آن‌ها بحث خواهد شد.
- Exchange server تخریب شده:
  - اگر به هر علتی یکی از نقش‌های سرور شما تخریب شده باشد برای بازیابی آن می‌توان دستور زیر را در خط فرمان PowerShell وارد نمود:

```
Setup /m:RecoverServer
```

لازم به ذکر است که بازیابی یک بانک اطلاعاتی بر روی اطلاعات کلیه افرادی که صندوق پستی‌اشان در آنجا قرار دارد تاثیر گذار خواهد بود. بنابراین بهتر است که کاربران را به گروه‌های کوچکتری تقسیم نمود و از تعداد بیشتری بانک اطلاعاتی جهت مدیریت مجموعه‌های مختلف کاربران استفاده کرد.

تهیه‌ی پشتیبان و بازیابی اطلاعات با استفاده از ابزار Windows Server backup

جهت اجرای این برنامه باید به All Programs گزینه‌ی Accessories و سپس قسمت System Tools آن و برنامه‌ی Windows Server backup (WSB) مراجعه نمود. به صورت پیش فرض این نقش بر روی ویندوز سرور ۲۰۰۸ نصب نیست و باید آن‌را افزود. برای این منظور دو دستور زیر را در خط فرمان PowerShell ویندوز با سطح دسترسی مدیریتی وارد نمائید:

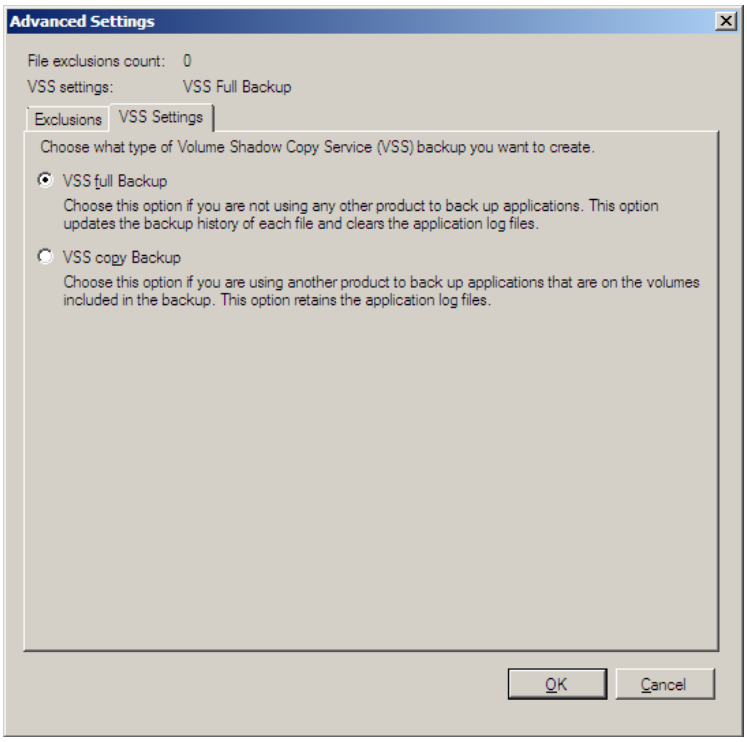
```
import-module servermanager
Add-WindowsFeature Backup-Features
```

برنامه‌ی جدید Windows Server backup (WSB) ویندوز سرور ۲۰۰۸ با برنامه قدیمی NT backup نگارش‌های قبلی ویندوز سرور، کاملا متفاوت بوده و از نو بازنویسی شده است. این برنامه امکان تهیه پشتیبان‌هایی از نوع VSS را دارا است و streaming backups قدیمی را دیگر پشتیبانی نمی‌کند. به همین جهت دیگر گزینه‌ی مخصوص و مجزای Exchange server را در این برنامه (همانند NT backup قدیمی) مشاهده نخواهید کرد. اما تیم برنامه نویسی Exchange server افزونه‌ای را به نام volume snapshot (VSS) plug-in برای یکپارچگی با برنامه Windows server backup ارائه داده است که در هنگام نصب Exchange server 2010 به WSB اضافه می‌شود (حتی اگر WSB در حین نصب اولیه Exchange server 2010 بر روی سیستم نصب نباشد. این افزونه تنها از سرویس پک ۲ مربوط به Exchange server 2007 به بعد در دسترس است).

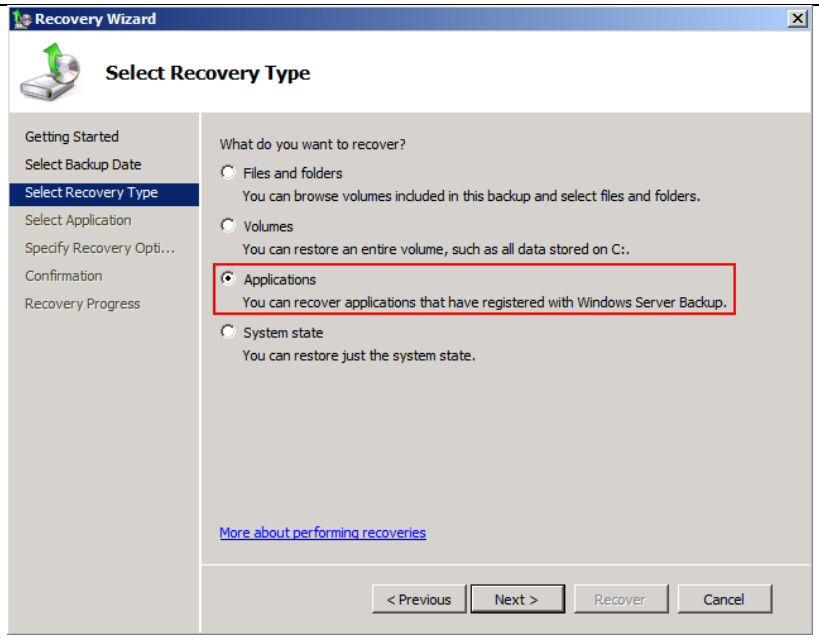
در این حالت، تهیه‌ی پشتیبان از درایوهای مخصوص Exchange server، به صورت خودکار پشتیبان VSS مربوط به Exchange server را نیز تهیه می‌کند (کل درایوهای مرتبط را باید انتخاب نمود که این مورد یکی از محدودیت‌های WSB است).

پس از پایان تهیه VSS backup ، WSB برنامه Exchange server را مطلع ساخته و سپس لاگ‌های تراکنش‌ها همانطور که در مبحث Full backups نیز عنوان شد، از سیستم حذف می‌شوند (برای بررسی این موضوع می‌توان به پوشه‌ی بانک‌های اطلاعاتی Exchange server مراجعه کرد و یا به خواص بانک‌های اطلاعاتی برنامه در کنسول مدیریتی Exchange server مراجعه نمائید. در اینجا تاریخ last full backup را می‌توان ملاحظه نمود).

لازم به ذکر است که حالت پیش فرض این برنامه، VSS Copy Backup است و نه حالت VSS Full Backup که سبب حذف لاگ‌های تراکنش‌ها می‌شود. برای انتخاب حالت VSS Full Backup ، باید حالت Custom backup را انتخاب نموده، درایوهایی را که شامل اطلاعات Exchange server هستند، انتخاب نمود، سپس در قسمت Advanced Settings آن، گزینه‌ی VSS Full Backup را برگزید (شکل ۱).



شکل ۱– انتخاب حالت VSS Full Backup.



شکل ۲– هنگام بازیابی اطلاعات، امکان انتخاب برنامه‌ی Exchange server نیز هست.

در حالت بازیابی اطلاعات (مراجعه به برگه Actions سمت راست صفحه برنامه WSB و انتخاب گزینه‌ی Recover)، نیازی به بازیابی کل اطلاعات موجود در پشتیبان نیست. در اینجا مطابق شکل ۲ می‌توان برنامه‌ی Exchange server را انتخاب کرده و تنها اطلاعات مرتبط با آن‌را بازیابی نمود. در حالت بازیابی می‌توان مکان اصلی (recover to original location) و یا مکان دیگری را برای بازیابی اطلاعات در نظر گرفت.

در حالت انتخاب مکان اصلی، اطلاعات موجود بازنویسی خواهند شد (ابتدا بانک‌های اطلاعاتی موجود dismount و سپس بر اساس داده‌های بانک‌های اطلاعاتی ارائه شده، mount خواهند شد).

اما اگر مکان دیگری انتخاب شود (Recover to another location)، تنها فایل‌های مربوطه کپی شده و تغییری در Exchange server حاصل نخواهد شد. مهم‌ترین استفاده از این حالت، بازیابی ایمیل‌های حذف شده‌ی چند نفر از پرسنل سازمان می‌باشد و قصد بازیابی کلیه ایمیل‌های تمامی پرسنل را همانند حالت قبل نداریم. همانطور که پیشتر نیز عنوان شد، ایمیل‌های حذف شده‌ی اشخاص تا مدت معینی از پشتیبان‌های تهیه شده قابل بازیابی هستند.

برای استفاده از فایل‌های بازیابی شده در حالت انتخاب مکانی دیگر، باید ابتدا یک recovery database (RDB) را ایجاد کرده و سپس بانک اطلاعاتی بازیابی شده مورد نظر را به آن mount نمود که روش انجام آن به صورت ذیل است:

در خط فرمان ویندوز پس از ورود به پوشه‌ی بازیابی شده، دستور زیر را صادر نمائید (توسط برنامه کمکی Eseutil می‌توان وضعیت بانک اطلاعاتی را که قرار است بازیابی شود (MailboxDatabaseName.edb) بررسی نمود):

```
Eseutil.exe /MH "MailboxDatabaseName.edb"
```

در خروجی این برنامه، سطر مربوط به state را یافته و مقدار آن‌را بررسی نمائید. اگر در حالت dirty shutdown قرار داشت، امکان mount آن به یک RDB (recovery database) وجود نداشته و ابتدا باید این مورد را اصلاح نمود. برای تغییر حالت به وضعیت clean shutdown ، دستور زیر را در خط فرمان صادر نمائید:

```
Eseutil /R E00 /I /d
```

هر دو دستور فوق باید در مسیر فایل‌های بازیابی شده اجرا شوند. اکنون مجددا دستور اول را اجرا نموده و وضعیت جدید را بررسی نمائید (باید به وضعیت clean shutdown تغییر کرده باشد).

برای تعریف یک RDB جدید در Exchange 2010 تنها از طریق خط فرمان PowerShell به صورت ذیل می‌توان عمل نمود:

```
New-MailboxDatabase -Name "Recovery Database" -Server srv01 -EDBFilePath
"C:\Restore\Mailbox\MDB01\MDB01.edb" -Logfolderpath
C:\Restore\Mailbox\MDB01\ –Recovery
```

پس از اجرای این دستور، بانک اطلاعاتی بازیابی شده جدید در Exchange Management Console در کنار سایر بانک‌های اطلاعاتی برنامه قابل مشاهده خواهد بود. برای استفاده از آن تنها کافی است دستور زیر را صادر نمائیم:

```
Mount-Database "Recovery Database"
```

اکنون نیاز است بدانیم صندوق‌های پستی کدامیک از پرسنل در این بانک اطلاعاتی بازیابی شده قرار دارند. برای این منظور دستور زیر را در خط فرمان PowerShell ویندوز وارد نمائید:

```
Get-MailboxStatistics –Database "Recovery Database"
```

با توجه به لیست مشخص شده پرسنل، برای بازیابی اطلاعات صندوق پستی وحید نصیری به بانک اطلاعاتی کاری برنامه باید مطابق دستور زیر عمل نمود:

```
Restore-Mailbox –Identity "Vahid Nasiri" –RecoveryDatabase "Recovery
Database"
```

اگر علاقمند باشیم که اطلاعات بازیابی شده یک کاربر مشخص در پوشه‌ای دلخواه (TargetFolder) ذخیره شوند باید دستور زیر را اجرا کرد:

```
Restore-Mailbox –Identity "Vahid Nasiri" –RecoveryDatabase "Recovery
Database" –RecoveryMailbox "Vahid Nasiri" –TargetFolder "Restored content"
```

برنامه‌های جانبی تهیه پشتیبان از Exchange server

گزینه‌ی دیگری که مایکروسافت جهت تهیه پشتیبان‌ها و حافظت از اطلاعات مشغول به کار بر روی آن است، برنامه‌ی System Center Data Protection Manager 2010 می‌باشد که به عنوان گزینه‌ی اول تهیه پشتیبان و بازیابی اطلاعات در اینجا نیز مطرح می‌شود:
http://edge.technet.com/Media/System-Center-Data-Protection-Manager-2010-and-Microsoft-Exchange/

همچنین شرکت Symantec نیز برنامه مخصوصی را جهت تهیه پشتیبان از Exchange server ارائه داده است:
http://shop.symantecstore.com/store/symnasmb/en_US/DisplayProductDetailsSmbPage/productID.107505800/ThemeID.106400/pgm.13399900?resid=s-nxzwoHAkEAAGnVekMAAAAI&rests=1259570894964

سایر برنامه‌های دیگر از این دست به قرار زیر هستند:

- Handy backup: http://www.handybackup.net/
- BackupAssist : http://www.backupassist.com/
- IBackup: http://www.ibackup.com/

به علاوه محصولات شرکت GFI نیز مانند GFI MailArchiver و سایر محصولات امنیتی آن، بسیار مورد توجه هستند:

http://www.gfi.com/mailarchiver

برنامه نویسی ابزارهای پشتیبان گیری از Exchange server 2010 SDK

برنامه نویس‌ها نیز می‌توانند جهت تهیه ابزارهای جانبی پشتیبان گیری از Exchange server 2010 با کمک SDK ارائه شده توسط مایکروسافت، اقدام نمایند. برای دریافت این SDK به آدرس‌های زیر مراجعه نمائید:
http://www.microsoft.com/downloads/details.aspx?FamilyID=6093ae54-525a-4d86-820c-31bc0c63a238&displayLang=en
http://msdn.microsoft.com/en-us/library/dd877010%28EXCHG.140%29.aspx

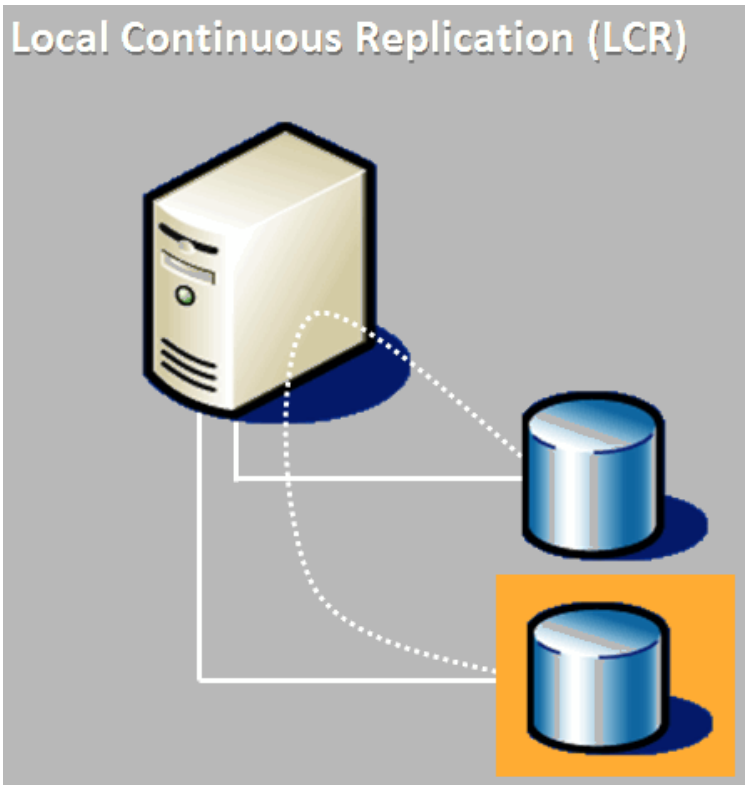
فصل ۷ – آشنایی با گزینه‌های تضمین فعالیت بی‌وقفه (High Availability)

تضمین فعالیت بی‌وقفه و یا High Availability (HA) یکی از مسایل مهم و کلیدی سازمانی است که اکثر امور ارتباطات داخلی و یا خارجی خود را بر این اساس بنا کرده است. در این سازمان تحمل از کار افتادن سرور ارسال و دریافت ایمیل‌ها و یا از دست دادن اطلاعات مرتبط با آن بسیار مشکل است و به محض بروز مشکلی در سیستم، باید پاسخگوی سیلی از شکایات پرسنل باشید. به همین منظور قابلیت‌های بسیاری در Exchange server جهت تضمین فعالیت بی‌وقفه پیش بینی شده است که در این فصل آن‌ها را مرور خواهیم کرد.

لازم به ذکر است که در Exchange server 2010 تعدادی از مفاهیم قدیمی HA مانند Local Continuous Replication (LCR)، Single copy clusters (SCC) و Clustered mailbox servers که در نگارش‌های قبلی این محصول قابل تنظیم بوده‌اند با توجه به امکانات جدید آن و بازنگری‌های صورت گرفته جهت کاهش پیچیدگی محصول، حذف شده‌اند. اما جهت تکمیل مبحث، تئوری این موارد نیز توضیح داده خواهند شد.

آشنایی با روش Local continuous replication و یا LCR

توسط گزینه‌ی منسوخ شده‌ی LCR، یک کپی از بانک‌های اطلاعاتی صندوق‌های پستی کاربران بر روی دیسک سخت دیگری در همان سرور تهیه می‌شود. هدف آن نیز پشتیبانی از سازمان‌های کوچک و متوسط بود. جهت نگهداری و به روز رسانی این کپی تهیه شده از فناوری log shipping استفاده می‌شود که اولین بار در SQL Server 2000 معرفی گردید. لاگ‌های تراکنش‌ها در سرور، جزئیات تمام امور رخ داده در بانک‌های اطلاعاتی را در خود نگهداری می‌کنند. در روش LCR این لاگ فایل‌های تراکنش‌های سیستم به پوشه لاگ مربوط به LCR کپی شده و سپس اعمال می‌گردند (شکل ۱). پیاده سازی این روش تنها بر روی یک سرور میسر بود. در این حالت اگر بانک‌های اطلاعاتی اصلی سیستم دچار مشکل شوند، سیستم به سادگی به بانک‌های اطلاعاتی همانند سازی شده این روش رجوع کرده (باید به صورت دستی صورت گیرد) و تضمین فعالیت بی‌وقفه‌ای را ارائه خواهد داد.

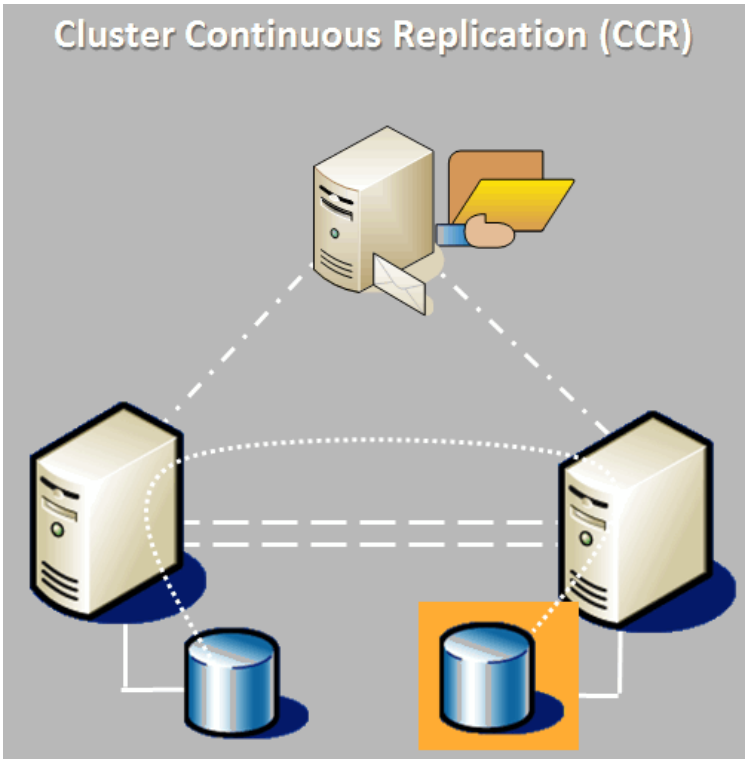


شکل ۱– نمایی از روش LCR و اعمال لاگ‌های تراکنش‌ها از یک بانک اطلاعاتی به بانک اطلاعاتی همانند سازی شده

آشنایی با روش Cluster Continuous replication و یا CCR

در این روش برخلاف روش LCR، کپی‌های بانک‌های اطلاعاتی بر روی سروری دیگر نگهداری می‌گردد. در اینجا کار همانند سازی این بانک‌های اطلاعاتی نیز توسط فناوری log shipping که در مورد آن توضیح داده شد، انجام می‌شود. ابتدا لاگ‌های تراکنش‌ها از سرور اصلی به پوشه لاگ‌های سرور LCR کپی شده و سپس به بانک‌های اطلاعاتی موجود در آن جهت انجام عملیات همانند سازی، اعمال می‌گردند (شکل ۲). در این روش با توجه به اینکه سرور دوم در یک Cluster قرار دارد، در صورت بروز مشکل دربانک‌های اطلاعاتی سرور اصلی، رجوع به سرور LCR به صورت خودکار صورت خواهد گرفت. در اینجا نیاز به نصب دو Exchange server می‌باشد. به سرور اصلی، Active و به سرور CCR ، Passive گفته می‌شود. همچنین به کامپیوتر سومی نیز نیاز خواهد بود. به این کامپیوتر، شاهد و یا Witness گفته می‌شود و مسؤول نظارت بر رجوع خودکار به کامپیوتر passive در صورت بروز مشکل است. بدیهی است جهت استفاده از این قابلیت‌ها نیاز به ویندوز سرور نگارش سازمانی نیز می‌باشد.

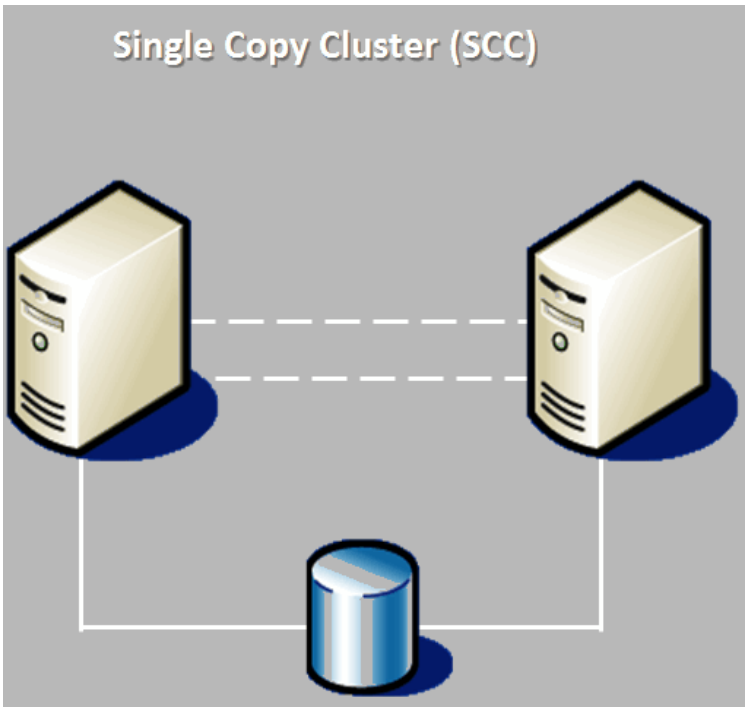
یکی از نقش‌هایی که از Exchange server 2010 حذف شده است (همان نقش‌هایی که در حین نصب می‌توان انتخاب نمود)، نقش Clustered mailbox servers است که در Exchange server 2007 برای راه اندازی روش CCR می‌بایست بر روی هر دو کامپیوتر Active و Passive نصب می‌شد.



شکل ۲– نمایی از روش CCR و انتقال و اعمال لاگ‌های تراکنش‌ها از یک سرور به سروری دیگر

آشنایی با روش Single copy cluster و یا SCC

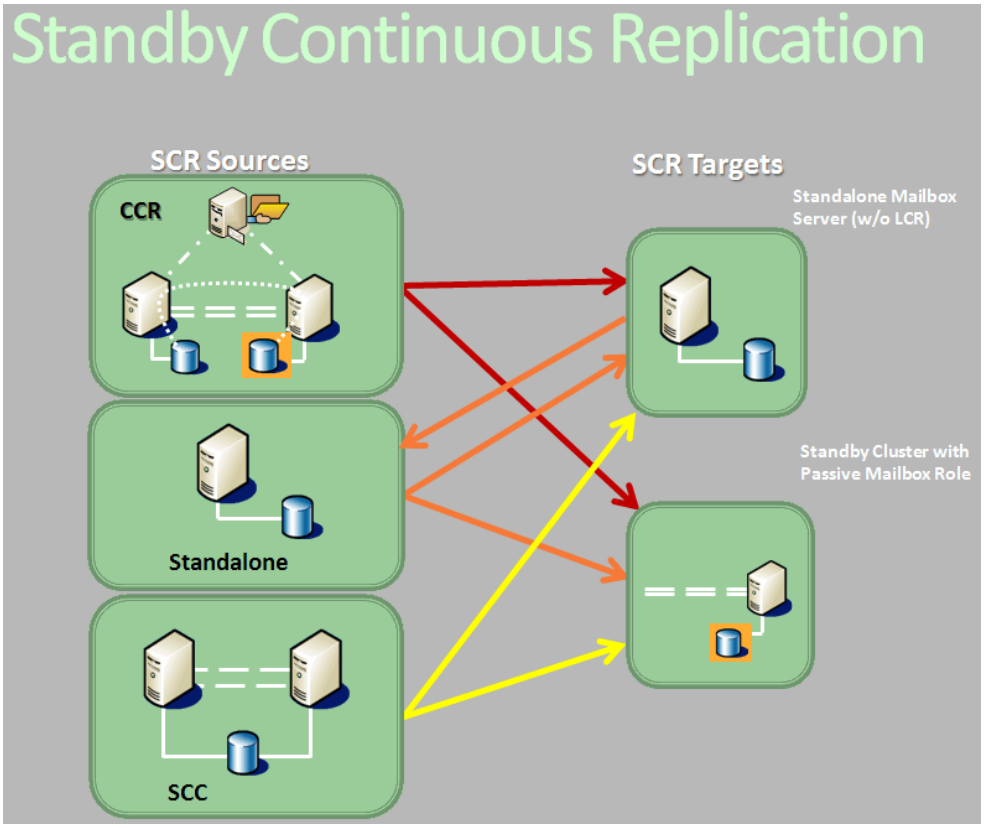
روش SCC نیز جزو منسوخ شده‌های Exchange server 2010 است (شکل ۳). این روش به همراه اولین نگارش‌های Exchange server ارائه گردید و بر اساس Clustering کار می‌کند و نیاز به یک محل ذخیره سازی اطلاعات به اشتراک گذاشته شده دارد (برای مثال یک SAN). باید دقت داشت که در این روش، یک محل به اشتراک گذاری اطلاعات ذخیره شده وجود داشته و در صورت از دست دادن آن، عملکرد سیستم مختل خواهد شد. به همین جهت استفاده از سایر روش‌های دیگر بجای این روش منسوخ شده توصیه می‌گردد.



شکل ۳– نمایی از روش SCC

آشنایی با روش Standby continuous replication و یا SCR

این روش از Exchanger server 2007 SP1 به بعد معرفی شده است و به روش‌ها LCR و CCR بسیار شبیه است (شکل ۴). در روش LCR لاگ فایل‌ها بر روی همان سرور بر روی دیسک سخت دیگری کپی می‌شدند، در روش CCR امکان کپی لاگ‌های تراکنش‌ها به سرور دیگری مهیا بود. اما روش جدید SCR امکان استفاده بیش از یک سرور را جهت کپی و اعمال لاگ‌های تراکنش‌های سیستم دارد. باید دقت داشت که از SCR نمی‌توان پشتیبان تهیه کرد و همچنین در این روش کامپیوترهای Active و Passive دیگر معنا ندارند. در این راه حل، SCR sources می‌توانند شامل بانک‌های اطلاعاتی فعال سیستم و یا حتی یک گروه CCR و یا SCC باشند. SCR targets می‌توانند متشکل از یک سرور با نقش Mailbox و یا یک گره Passive در Cluster باشند.



شکل ۴– نمایی از روش Standby continuous replication

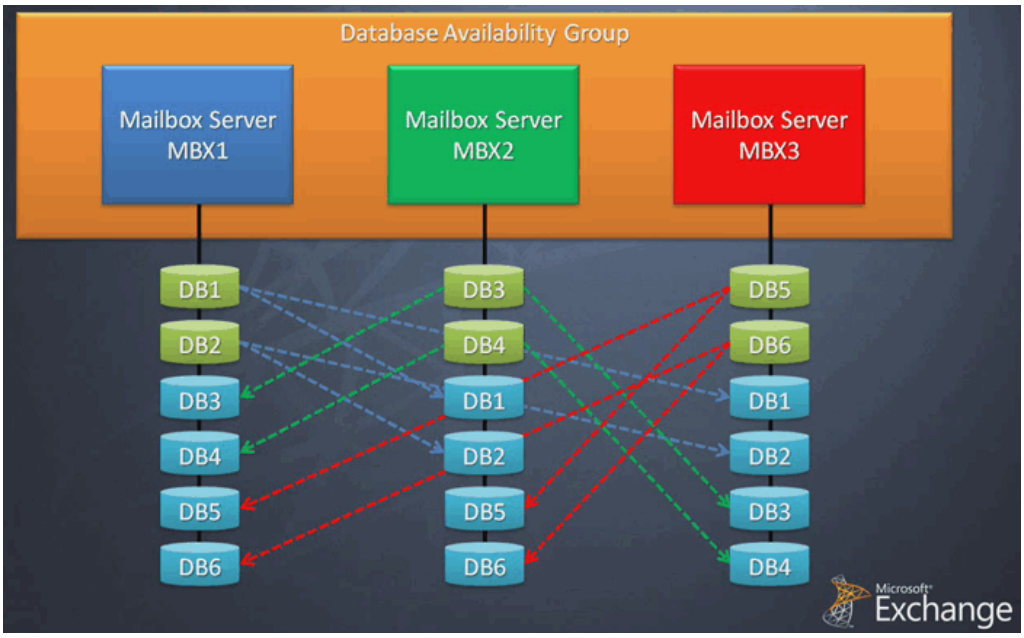
موارد عنوان شده تا اینجا، اصول تئوری بکار گرفته شده در انواع و اقسام روش‌های تضمین کارکرد بی‌وقفه‌ی Exchange server است. این روش‌ها در Exchange server 2010 جهت کاهش پیچیدگی‌های سیستم و پیاده سازی آن‌ها به صورت زیر تغییر کرده‌اند و ادغام شده‌اند.

آشنایی با Database mobility

با معرفی مکانیزم Database mobility امکان همانند سازی بانک‌های اطلاعاتی Exchange server 2010 در چندین سرور مهیا است. به این صورت بانک‌های اطلاعاتی یک Exchange server را می‌توان در سروری دیگر شبیه سازی و یا حتی در صورت بروز مشکل در سرور اصلی، mount و استفاده کرد. برای این منظور باید یک DAG و یا Database availability group را در Exchange server تعریف نمود. هر DAG می‌تواند متشکل از بانک‌های اطلاعاتی همانند سازی شده تا ۱۶ میل‌باکس سرور باشد. در این حالت پس از تعریف DAG ، میل‌باکس سرورهای موجود به آن اضافه شده و سپس می‌توان نسبت به همانند سازی بانک‌های اطلاعاتی بین

سرورهای این گروه اقدام نمود. DAG هر دو حالت بازیابی دستی و یا خودکار از وقفه‌های پیش آمده در سرورها را پشتیبانی می‌کند.

فرض کنید در یک سازمان سه میل باکس سرور مجزا نصب شده است. هر سرور نیز دارای ۲ بانک اطلاعاتی صندوق‌های پستی کاربران است. این بانک‌های اطلاعاتی باید با اسامی منحصربفردی نامگذاری شوند تا بتوان در یک DAG از آن‌ها استفاده نمود (برای مثال DB1 تا DB6). تا اینجا خبری از مفاهیم Service availability و یا Data availability نیست. پس از آن ابتدا یک DAG را تعریف کرده و این سه سرور را به آن اضافه خواهیم کرد. اکنون می‌توان مفاهیم Continuous replication را بین این سرورهای گروه DAG خود، پیاده سازی کرد (شکل ۵). Continuous replication در Exchange server 2010 به شدت بهبود یافته و حاوی گزینه‌های فشرده سازی و یا حتی رمزنگاری اطلاعات نیز می‌باشد.



شکل ۵– پیاده سازی تضمین فعالیت بی‌وقفه در Exchange server 2010

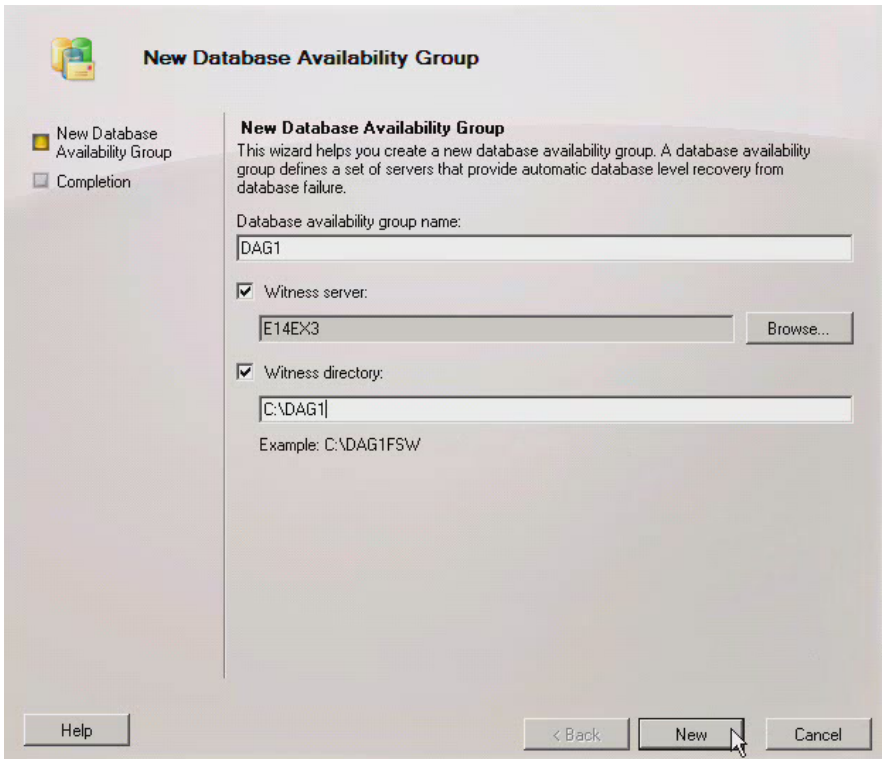
همانطور که در شکل ۵ نیز ملاحظه می‌نمائید، سه میل باکس سرور ما در یک DAG قرار گرفته‌اند و سپس بانک‌های اطلاعاتی فعال آن‌ها (که با رنگ سبز نمایش داده شده‌اند) بین سرورهای دیگر همانند سازی شده‌اند (این بانک‌های اطلاعاتی با رنگ آبی مشخص شده‌اند). اکنون اگر به دلایل مختلفی مانند عیوب سخت افزاری، مشکلات شبکه، مسایل نرم افزاری و غیره یکی از دیتابیس‌ها دچار مشکل شود (مثلا DB1 در MBX1 دچار مشکل شده)، بازیابی از وقفه‌ی پیش آمده در کمتر از۳۰ ثانیه به صورت خودکار صورت خواهد گرفت و بانک‌های اطلاعاتی همانند سازی شده که در حالت Passive قرار دارند، Active خواهند شد (برای مثال DB1 در MBX2 تبدیل به بانک اطلاعاتی فعال و قابل استفاده می‌گردد). همچنین اگر یک سرور به طور کامل از شبکه خارج شود، کپی‌های بانک‌های اطلاعاتی آن در

سرورهای دیگر به صورت خودکار در حالت فعال وارد شبکه شده و کاربران سازمان احساس بروز مشکل خاصی را نخواهند کرد.

پیاده سازی تضمین فعالیت بی‌وقفه در Exchange server 2010

در این قسمت فرض بر این است که حداقل دو سرور مجزا حاوی نقش‌های Mailbox سرور در شبکه شما موجود است. همچنین نیاز به یک سرور شاهد (Witness) مجزا از این گروه نیز می‌باشد.

برای پیاده سازی تضمین فعالیت بی وقفه در Exchange server 2010 در کنسول مدیریتی آن به قسمت Organization configuration و گزینه‌ی Mailbox آن مراجعه نمائید. اکنون از برگه‌ی Actions سمت راست صفحه، گزینه‌ی New database availability group را جهت ایجاد یک DAG جدید در مجموعه انتخاب نمائید. در برگه‌ی ظاهر شده (شکل ۶)، ابتدا نام منحصربفرد این گروه جدید تضمین فعالیت بی‌وقفه را باید وارد کرد (بهتر است همان نام کامپیوتر جاری باشد). سپس باید سرور شاهد را انتخاب نمود. این سرور خارج از گروه تضمین فعالیت ما قرار دارد و همچنین پوشه‌ای که قرار است بر روی آن ایجاد شود نیز به صورت خودکار پیکره بندی شده و نیازی به اقدام خاص دیگری نخواهد بود.



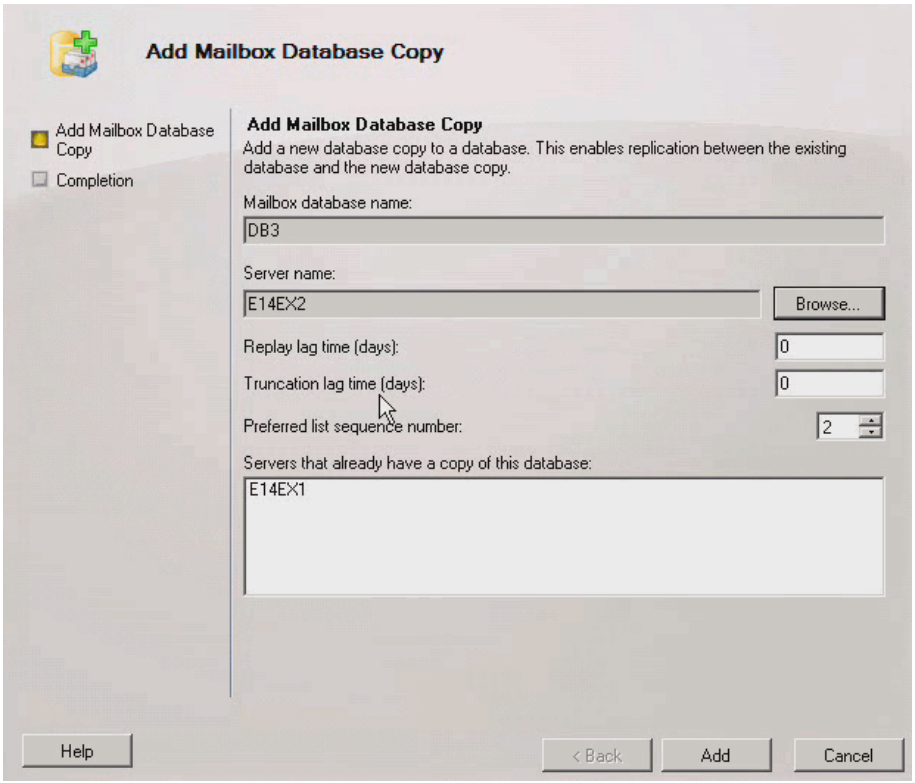
شکل ۶– ایجاد یک DAG جدید

پس از ایجاد DAG ، بر روی آن در برگه‌ی database availability group کلیک راست کرده و گزینه‌ی مدیریت اعضای DAG را انتخاب نمائید. در اینجا می‌توان میل باکس سرورهایی را که باید به این DAG اضافه نمود، انتخاب کرد و سپس تمام کارهای تنظیمات کلاسترها، ثبت بانک‌های اطلاعاتی در اطلاعات Clustering شبکه، ثبت در DNS و غیره به صورت خودکار صورت می‌گیرد. بنابراین این سرورها باید دارای گزینه‌ی نصب شده‌ی failover clustering ویندوز سرور ۲۰۰۸ نگارش سازمانی یا Datacenter باشند (دستور زیر را در خط فرمان اجرا نمائید).

```
ServerManagerCmd -i Failover-Clustering
```

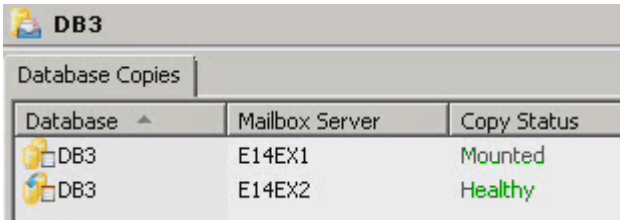
حتی اگر این گزینه را نصب نکرده باشید، این Wizard کار نصب آن‌را به صورت خودکار انجام خواهد داد (البته این نصب تنها در حالت اجرای این Wizard به صورت محلی بر روی همان سرور مورد نظر با موفقیت کامل خواهد شد).

اکنون که کار ایجاد DAG و همچنین افزودن سرورهای مورد نظر به این گروه و معرفی سرور شاهد پایان یافت، نوبت به انجام فرآیند همانند سازی بانک‌های اطلاعاتی این سرورها می‌رسد. برای این منظور به قسمت Organization Configuration و گزینه‌ی Mailbox آن مراجعه نمائید. سپس به برگه‌ی database management آن رجوع کرده و بر روی دیتابیس‌های مورد نظر خود کلیک راست نمائید و گزینه‌ی Add mailbox database copy را انتخاب کنید. در صفحه‌ی باز شده (شکل ۷)، بر روی دکمه‌ی Browse کلیک کرده و سروری را که باید کپی این بانک اطلاعاتی بر روی آن قرار گیرد انتخاب نمائید و سپس بر روی دکمه‌ی Add کلیک کنید.



شکل ۷– تعریف نحوه‌ی همانند سازی بانک‌های اطلاعاتی

پس از این عملیات، بانک اطلاعاتی فعال سیستم با وضعیت mounted و بانک اطلاعاتی Passive با وضعیت Healthy نمایش داده خواهد شد (شکل ۸).



شکل ۸– نمایی از وضعیت بانک‌های اطلاعاتی Active و Passive بر روی دو سرور مجزا.

جهت فعال سازی دستی بانک اطلاعاتی که در حالت passive قرار دارد، تنها کافی است بر روی آن در همین قسمت نمایش وضعیت‌ها کلیک راست کرده و سپس گزینه‌ی Activate database copy را انتخاب نمود.

فصل ۸ – آشنایی با تنظیمات ضد هرزنامه‌ها (Anti-Spams)

همانطور که در فصل‌های قبل نیز ذکر گردید، برای اتصال Exchange server به اینترنت بهتر است نقش Edge transport server را بر روی یک سرور مجزا نصب و راه اندازی نمود. به همراه این نقش انواع و اقسام گزینه‌های مقابله با هرز نامه‌های رسیده نیز وجود دارد.

این امکانات بر روی سروری با نقش Hub transport به صورت پیش فرض نصب نشده است زیرا فرض بر این است که از این سرور قرار است در یک شبکه‌ی داخلی با پرسنلی مشخص استفاده گردد و اگر شخصی اقدام به ارسال هرزنامه نمود به راحتی می‌توان صندوق پستی او را غیرفعال کرد. اما امکان اتصال مستقیم hub transport server نیز بدون استفاده از Edge transport server به اینترنت وجود دارد. بدیهی است تنها در این حالت نیاز به نصب ابزارهای مقابله با ضدهرزنامه‌ها در یک hub transport سرور می‌باشد و در سایر شرایط نیازی به انجام این عملیات نیست.

در فصل جاری ابتدا این گزینه را فعال ساخته و سپس به بررسی تنظیمات مختلف آن خواهیم پرداخت. امکانات مقابله با هرز نامه‌ها در Edge transport server نیز دقیقا همانند امکاناتی است که برای hub transport سرور توضیح داده خواهند شد.

فعال سازی امکانات مقابله با هرزنامه‌ها در Hub transport server

برای فعال سازی امکانات مقابله با هرز نامه‌ها در Hub transport server باید به پوشه‌ی زیر مراجعه کرده:

```
C:\Program Files\Microsoft\Exchange Server\V14\Scripts
```

و سپس اسکریپتی به نام install-AntispamAgents.ps1 را در کنسول پاورشل Exchange server با دسترسی مدیریتی اجرا نمود (exchange management shell)؛ که خلاصه‌ی این عملیات به شرح زیر است:

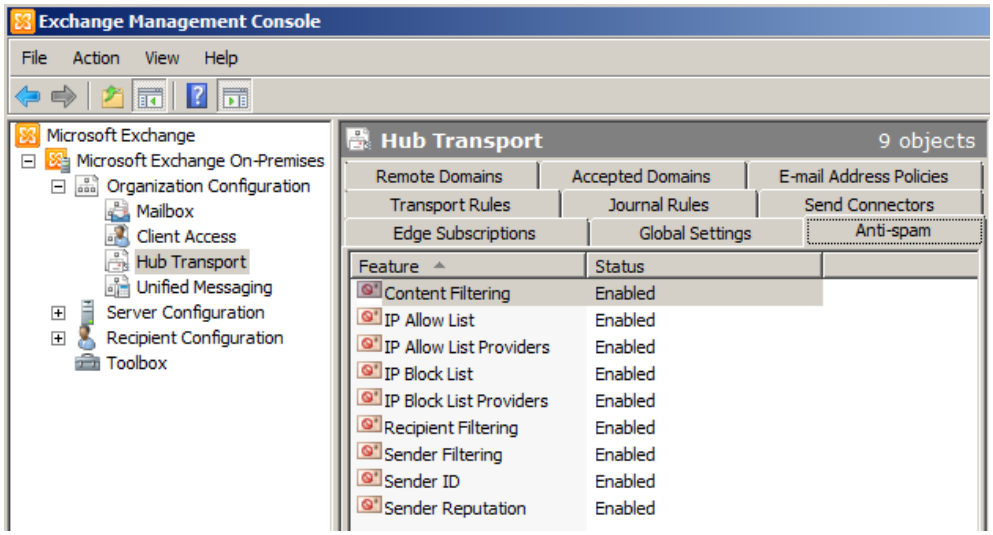
```
[PS] C:\Windows\system32>cd "C:\Program Files\Microsoft\Exchange
Server\V14\Scripts"
[PS] C:\Program Files\Microsoft\Exchange Server\V14\Scripts>.\install-
AntispamAgents.ps1

WARNING: The agents have been installed. Please restart Microsoft Exchange
Transport service for changes to take effect.
```

```
WARNING: You must enable Microsoft Update on your Exchange server to
receive anti-spam updates.
```

همانطور که ملاحظه می‌کنید پس از نصب امکانات مقابله با هرز نامه‌ها، باید سرویس Microsoft Exchange Transport را در کنسول مدیریتی سرویس‌های ویندوز یافته و سپس راه اندازی مجدد نمود. همچنین جهت دریافت آخرین بانک اطلاعاتی سرورهای ارسال کننده هرزنامه نیز باید امکانات به روز رسانی خودکار ویندوز را فعال نمود.

پس از نصب اسکریپت یاد شده و راه اندازی مجدد سرویس Microsoft Exchange Transport ، یکبار کنسول مدیریتی Exchange server را بسته و مجددا باز نمائید. اکنون اگر به قسمت Organization configuration و گزینه‌ی Hub transport آن مراجعه کنیم، برگه‌ی Anti-spam اضافه شده است (شکل ۹).



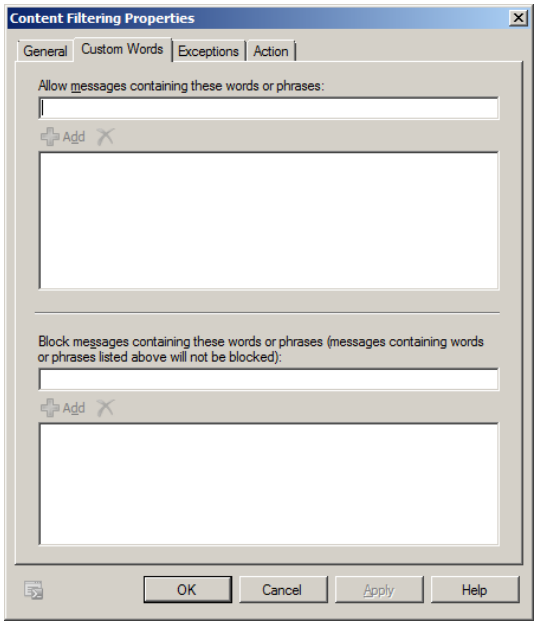
شکل ۹– فعال سازی گزینه‌های مقابله با هرزنامه‌ها در یک Hub transport server.

در این حالت پس از نصب گزینه‌ی Anti-spam ، هر کدام از ایمیل‌های دریافتی، ابتدا بر اساس فیلترهای تعریف شده در این قسمت بررسی شده و سپس به دریافت کننده رسانده خواهند شد.

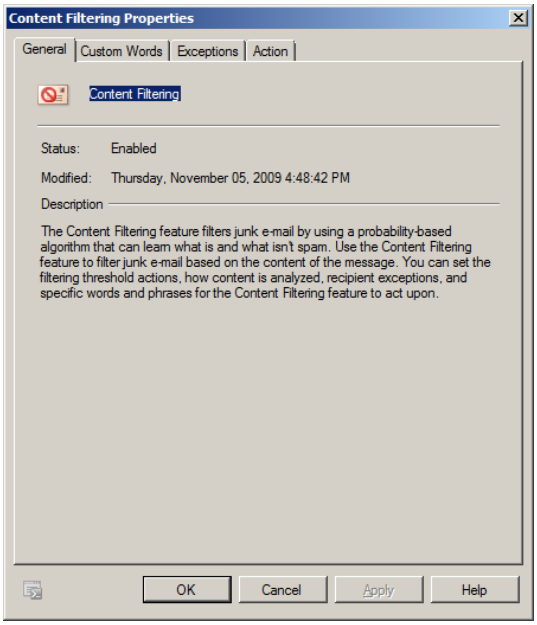
فیلتر کردن ایمیل‌های رسیده بر اساس محتوای آن‌ها

بر اساس قابلیت content filtering ، محتوای ایمیل‌های رسیده بررسی شده و یک عدد SCL به هر ایمیل نسبت داده می‌شود (SCL=Spam confidence level). بر این اساس احتمال هرزنامه بودن یک ایمیل مشخص شده و بر اساس تنظیمات این قسمت (شکل ۱۳)، اگر عدد حاصل بزرگتر یا مساوی ۷ بود، ایمیل رسیده به عنوان یک هرزنامه تشخیص داده می‌شود. این فیلتر به کمک به روز رسانی‌های ویندوز هر روز با اطلاعات جدیدتری به روز رسانی می‌شود. همچنین می‌توان دقیقا مشخص ساخت که با یک هرزنامه چگونه باید رفتار شود. آیا باید بلافاصله حذف شود، برگشت زده شود یا در قرنطینه قرار گیرد (شکل ۱۳). در اینجا منظور از قرنطینه، ایجاد یک صندوق پستی خاص و سپس ارسال تمام هرزنامه‌ها جهت بررسی بیشتر به آن صندوق پستی ویژه می‌باشد (با انتخاب این گزینه، یک جعبه‌ی متنی جهت ورود آدرس ایمیل این صندوق پستی ظاهر خواهد شد).

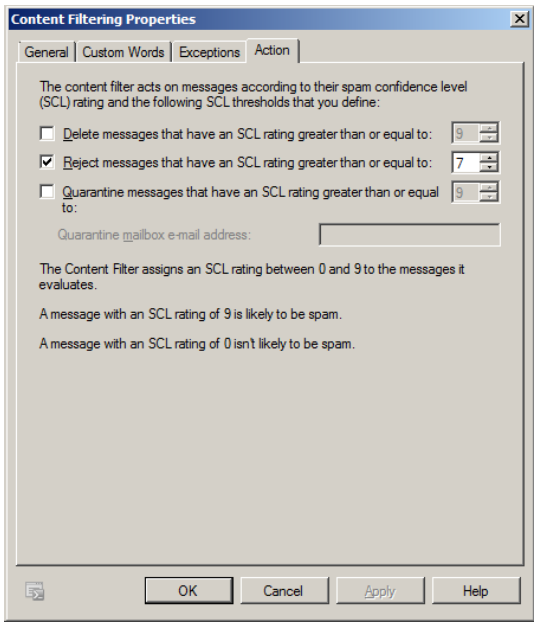
امکان تنظیم بانک اطلاعاتی سفارشی این قسمت نیز با استفاده از برگه‌ی Custom words آن وجود دارد. برای مثال اگر ایمیلی حاوی اطلاعات مشخصی بود، آن ایمیل به عنوان هرزنامه درنظر گرفته نشود (یا برعکس، با استفاده از قسمت block messages آن). در برگه‌ی Exceptions می‌توان آدرس‌های ایمیل اشخاصی را وارد کرد که نیاز است هیچگونه فیلتری بر روی ایمیل‌های آن‌ها صورت نگیرد.



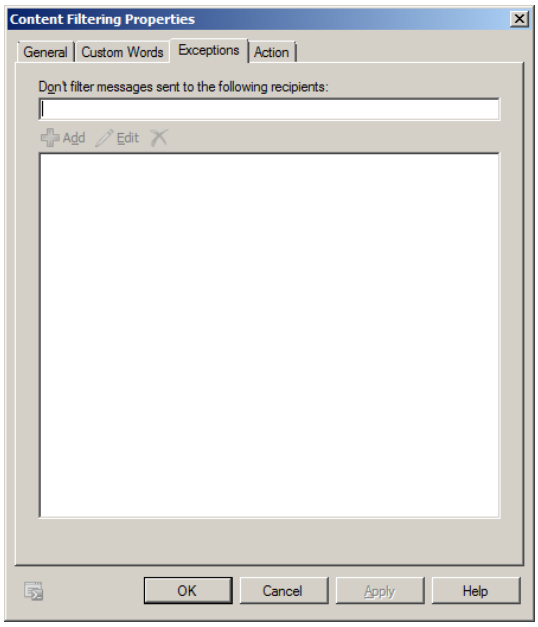
شکل ۱۱– تعریف کلمات و جملات سفارشی جهت مجاز دانستن و یا فیلتر کردن آن‌ها



شکل ۱۰– صفحه‌ی ابتدایی فیلتر بر اساس محتوا



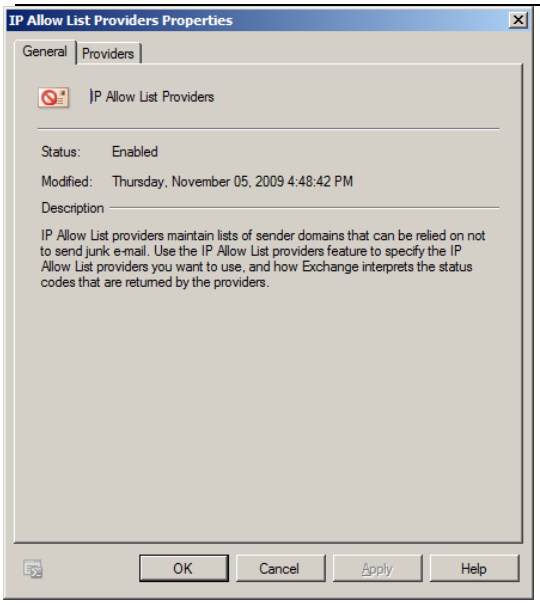
شکل ۱۳– نحوه‌ی اعمال SCL به ایمیل‌های دریافتی



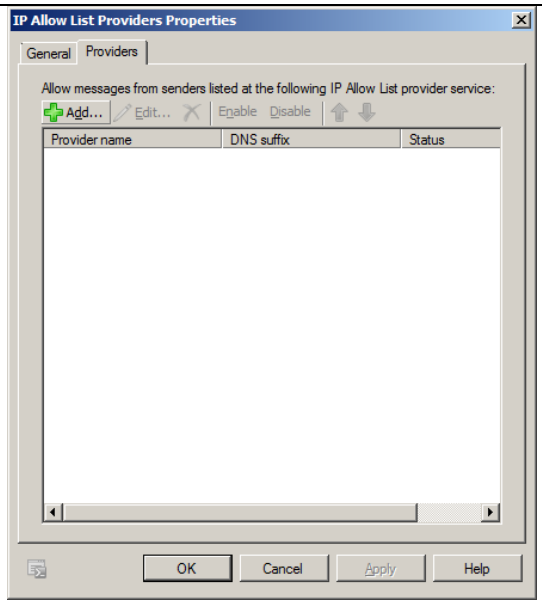
شکل ۱۲– امکان تعریف آدرس‌های ایمیلی که باید از فیلترهای اعمالی معاف باشند.

فیلتر کردن ایمیل‌های رسیده بر اساس IP های مجاز

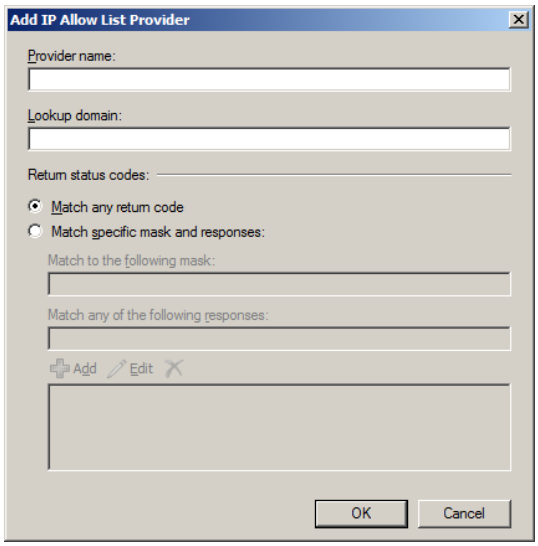
در قسمت امکانات Anti-spam مربوط به Exchange server ، Providers به معنای سایت‌های اینترنتی هستند که رکورد اطلاعات سایت‌ها و IP های ارسال کننده‌ی ایمیل را نگهداری کرده و آن‌ها را به شما به صورت رایگان یا بر اساس دریافت هزینه‌ای ارائه می‌دهند. در این قسمت می‌توان این نوع Providers را جهت به روز رسانی بانک اطلاعاتی Exchange server معرفی کرد.



شکل ۱۴– صفحه‌ی ابتدایی فیلتر بر اساس IPهای مجاز



شکل ۱۵– امکان تعریف Providers

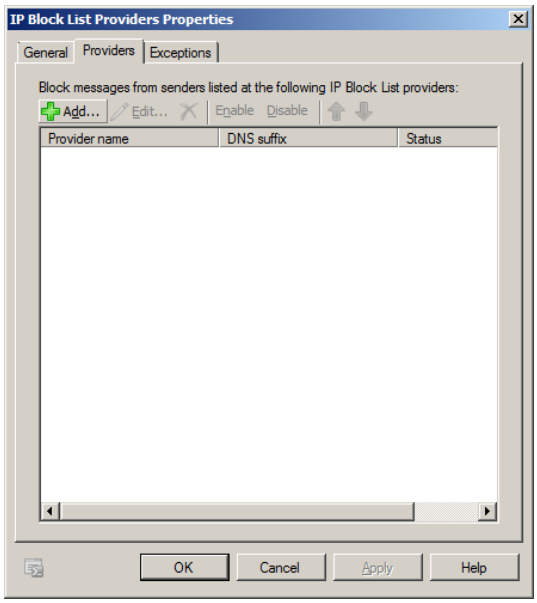


شکل ۱۶– صفحه‌ی ورود Provider مورد نظر

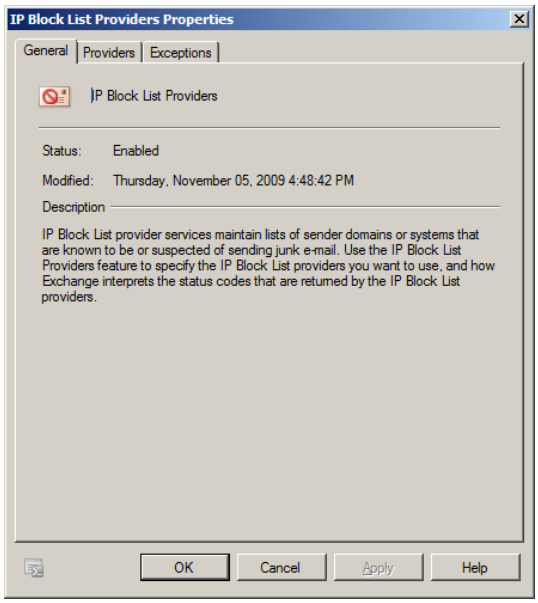
فیلتر کردن ایمیل‌های رسیده بر اساس IP های غیرمجاز

اگر پس از بررسی‌ها مشخص شده است که از یک IP خاص و یا حتی یک بازه‌ی IP ویژه، هرزنامه دریافت می‌کنید، می‌توان آن‌ها را در قسمت IP Block list providers وارد نمود. از این پس زمانیکه ایمیلی به سرور ارسال گردد، ابتدا IP منبع ارسال کننده مشخص شده و با لیست IP های غیرمجاز تعریف شده مطابقت داده می‌شود. اگر این IP در لیست سیاه IP های ما قرار داشت، ایمیل‌های آن برگشت زده خواهند شد.

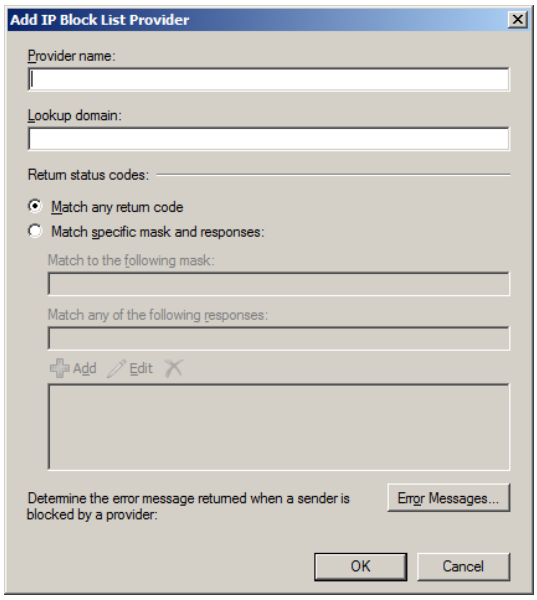
همانطور که عنوان شد منظور از Providers ، سایت‌های اینترنتی هستند که خدمات مربوطه را ارائه می‌دهند. با معرفی آن‌ها، بانک اطلاعاتی Exchange server به صورت متناوب بر اساس آخرین لیست IP های ارسال کننده هرزنامه به روز خواهد شد (شکل ۱۸). همچنین اگر نیاز است تا یکی از آدرس‌های ایمیل مشخص همکار سازمان، صرفنظر از بازخوردهای جمع آوری شده از اینترنت، در لیست سفید ارسال کنندگان ایمیل قرار گیرند، می‌توان آدرس ایمیل او را در برگه‌ی Exceptions وارد نمود (شکل ۱۹).



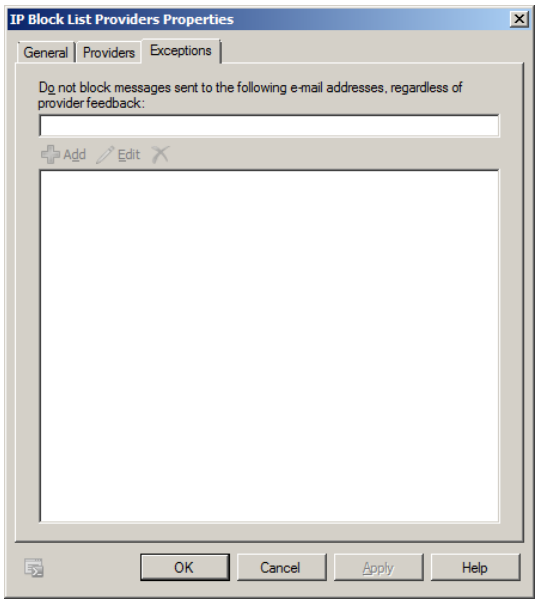
شکل ۱۸– امکان افزودن providers



شکل ۱۷– صفحه‌ی آغازین فیلتر بر اساس IPهای غیرمجاز



شکل ۲۰– صفحه افزودن یک provider جدید



شکل ۱۹– امکان تعریف استثناءها

تعدادی از این نوع Providers به شرح زیر هستند:

```
http://www.spamhaus.org/faq/answers.lasso?section=Spamhaus%20SBL
http://dnsbl.sorbs.net
http://bl.spamcop.net
https://toolbox.webhotel.net/cgi-bin/rbl.cgi
```

و یا از اسکریپت زیر نیز می‌توان جهت افزودن خودکار ۱۰ سایت برتر ارائه کننده خدمات اطلاعاتی جهت مقابله با هرزنامه ارسال کنندگان استفاده کرد:

ابتدا با استفاده از PowerShell به مسیر زیر وارد شوید:

```
C:\Program Files\Microsoft\Exchange Server\V14\Scripts
```

سپس دستور زیر را وارد نمائید:

```
.\get-antispamtoprblproviders.ps1
```

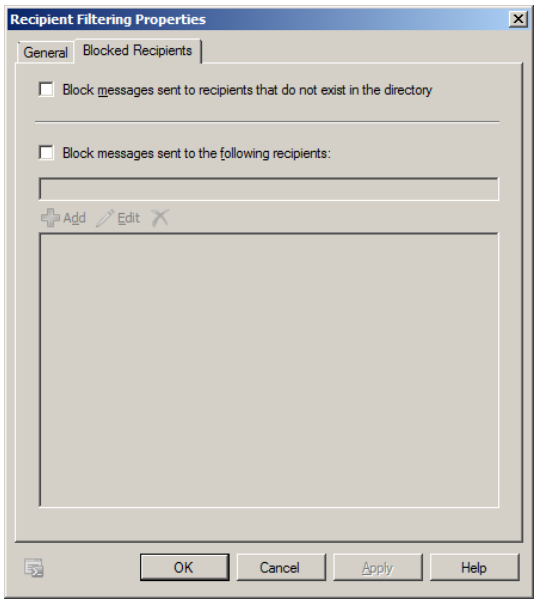
اسکریپت‌های افزودن این نوع Providers جهت سایر قسمت‌هایی که در این فصل توضیح داده می‌شوند نیز در همان پوشه Scripts موجود است. برای مثال:

Get-AntispamTopBlockedSenderDomains.ps1
Get-AntispamTopBlockedSenderIPs.ps1
Get-AntispamTopBlockedSenders.ps1
Get-AntispamTopRecipients.ps1

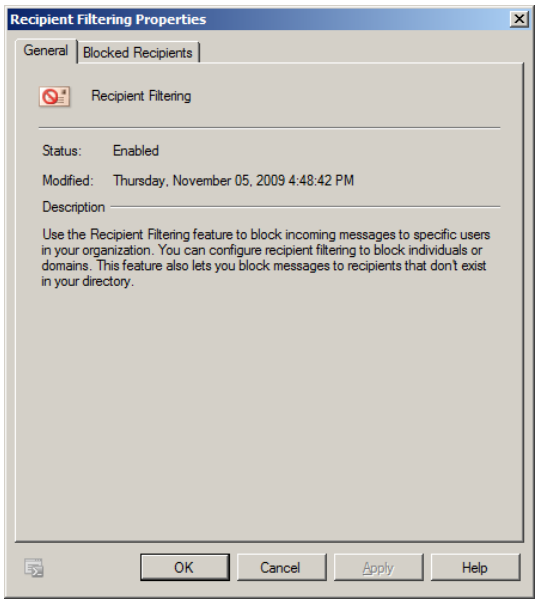
فیلتر کردن ایمیل‌های رسیده بر اساس دریافت کننده‌ها

در این قسمت اگر امکانات بررسی هرزنامه‌ها بر روی hub transport server نصب شده باشد، انتخاب گزینه‌ی اول برگه‌ی blocked recipients جهت فیلتر کردن ایمیل‌هایی که به هیچ یک از اعضای سازمان ما ارسال نشده است مفید می‌باشد. اگر از edge transport server برای این منظور استفاده می‌شود باید از همزمانی آن با hub transport server اطمینان حاصل نمود.

همچنین اگر مرتبا هرزنامه‌هایی برای یک یا چند آدرس ایمیل داخلی ارسال می‌شود، می‌توان آن‌ها را از دریافت هرزنامه‌ها با استفاده افزودن آن‌ها به قسمت پایین برگه‌ی blocked recipients، معاف کرد (شکل ۲۲).



شکل ۲۲– تنظیمات و مشخص سازی عدم ارسال هرزنامه‌ها به ایمیل‌های سازمان

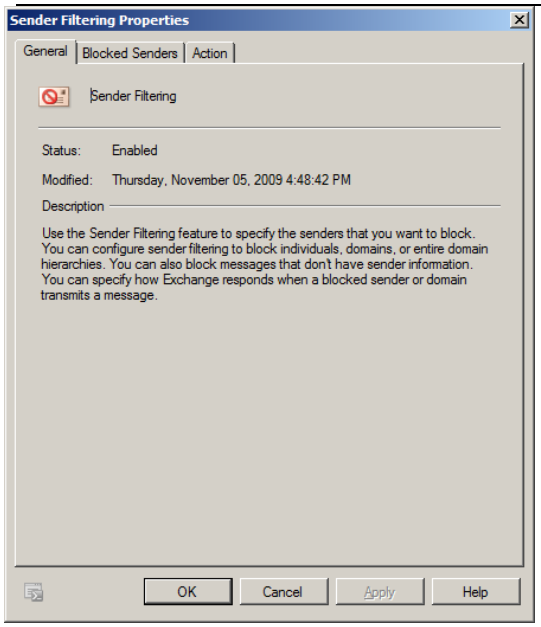


شکل ۲۱– صفحه‌ی آغازین فیلتر بر اساس دریافت کننده‌ها

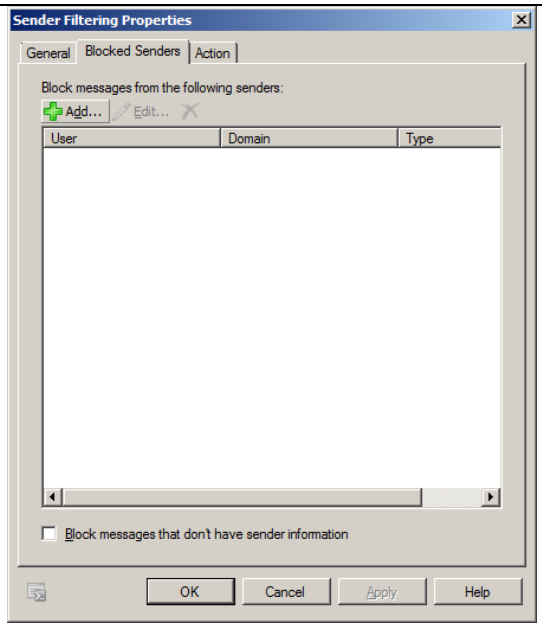
فیلتر کردن ایمیل‌های رسیده بر اساس ارسال کننده‌ها

اگر از آدرس‌های ایمیل مشخصی به صورت روزانه هرزنامه برای شما ارسال می‌شود، می‌توان آن‌ها را در قسمت `Blocked senders` مربوط به `Sender filtering` وارد کرد (شکل ۲۴)؛ یا حتی می‌توان کل `domain` مربوطه را نیز وارد نمود و تمام ایمیل‌های مربوط به آن `domain` مورد نظر را فیلتر کرد. در همین برگه با انتخاب گزینه‌ی `block messages that don’t have sender information` می‌توان کلیه ایمیل‌هایی را که اطلاعات ارسال کننده‌ی آن‌ها خالی است نیز فیلتر نمود.

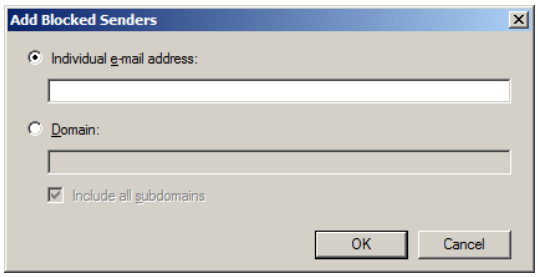
در اینجا بر اساس برگه‌ی `Action` یا می‌توان این نوع ایمیل‌های مشخص را برگشت زد و یا ممهور به علامت هرزنامه نمود (شکل ۲۶).



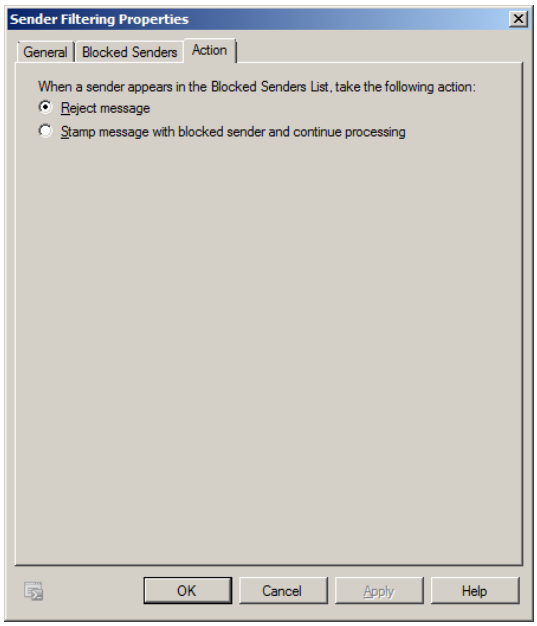
شکل ۲۳– صفحه‌ی آغازین فیلتر بر اساس ارسال کننده‌ها



شکل ۲۴– امکان تعریف ارسال کننده‌های غیرمجاز



شکل ۲۵– صفحه‌ی افزودن یک ایمیل ویژه و یا حتی یک domain مشخص به لیست سیاه ارسال کننده‌ها



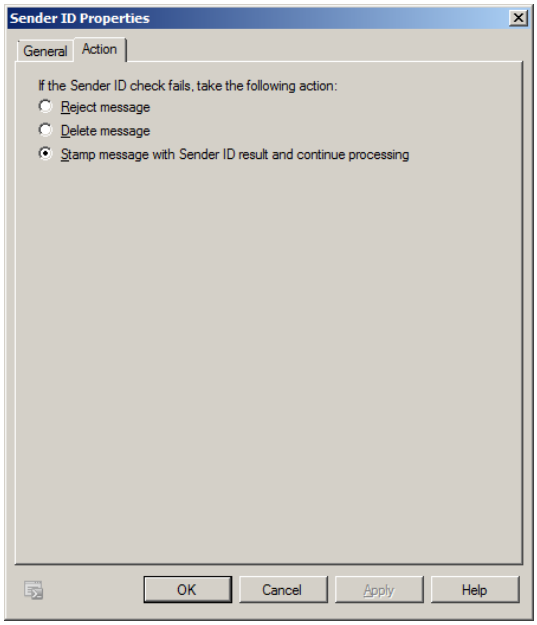
شکل ۲۶– صفحه‌ی تنظیم نحوه‌ی رفتار با ایمیل‌های فیلتر شده

فیلتر کردن ایمیل‌های رسیده بر اساس سایت‌های متقلب

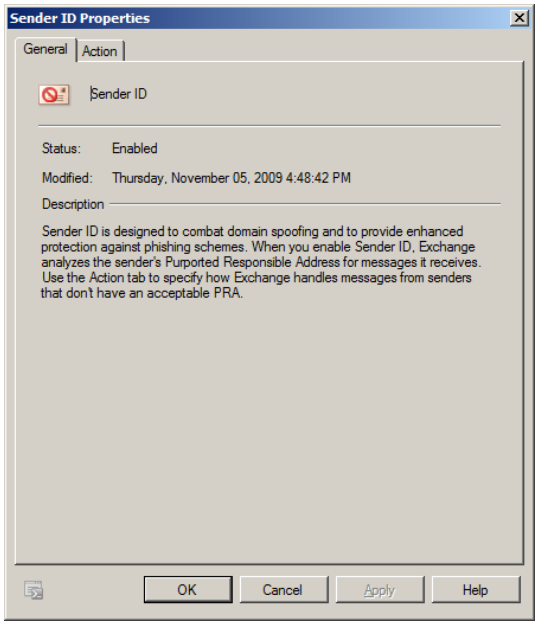
این قسمت از امکانات مبارزه با هرزنامه‌ها، جهت فیلتر کردن آدرس‌های ارسال کننده‌ی ایمیل‌های جعلی به کار می‌رود. برای مثال ارسال ایمیل از یک شرکت معروف در حالیکه IP ارسال کننده یا سایر مشخصات ویژه‌ی آن تطابقی با domain اصلی آن شرکت ندارد و در حقیقت یک نوع جعل هویت صورت گرفته است.

در اینجا نیز مطابق برگه‌ی Action می‌توان این نوع ایمیل‌ها را بلافاصله حذف کرد یا برگشت زد و یا ممهور به مهر جعلی بودن نمود.

بهتر است گزینه‌ی پیش فرض موجود را پذیرفت. زیرا گاهی از اوقات ممکن است DNS server یا سایر موارد مرتبط به درستی تنظیم نشده باشند و در این حالت حذف بلافاصله‌ی ایمیل‌های رسیده برای سازمان نامطلوب خواهد بود.



شکل ۲۸– صفحه‌ی تنظیم نحوه‌ی رفتار با ایمیل‌های فیلتر شده

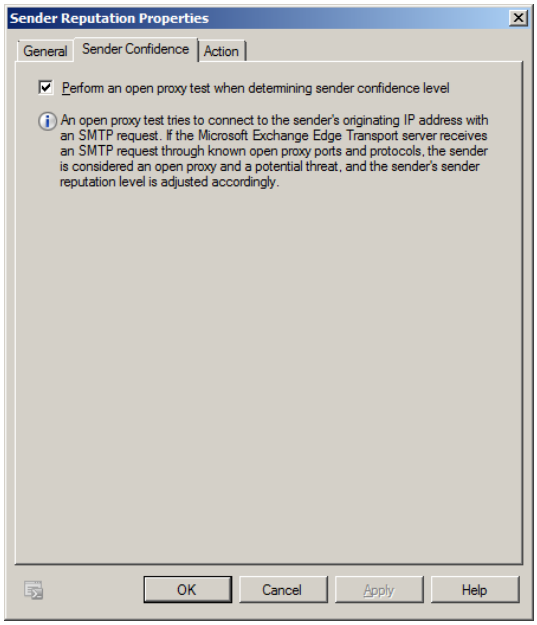


شکل ۲۷– صفحه‌ی آغازین فیلتر بر اساس سایت‌های متقلب

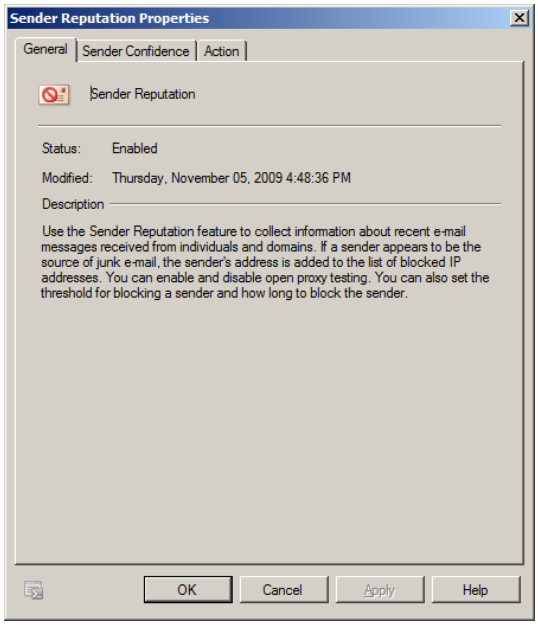
فیلتر کردن ایمیل‌ها بر اساس میزان اطمینان به ارسال کننده

Exchange server ایمیل‌های دریافتی در طول شبانه روز را تحت کنترل قرار می‌دهد. اگر بر اساس محاسبات خود به این نتیجه به برسد که شخصی یا IP خاصی مشغول به ارسال هرزنامه است، IP او را به مدت ۲۴ ساعت

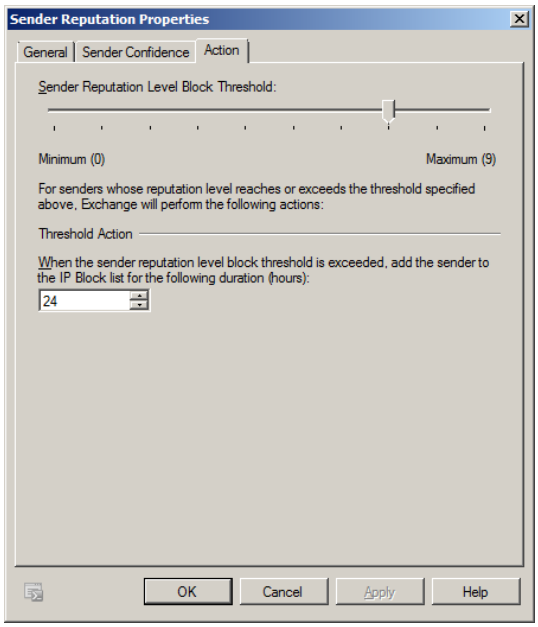
(عددی پیش فرض که در برگه‌ی action قابل تنظیم است)، در لیست سیاه قرار خواهد داد. جهت تشخیص این میزان اعتبار، از آزمون Open proxy نیز استفاده می‌شود (شکل ۳۰).



شکل ۳۰– امکان استفاده از آزمون Open proxy جهت تشخیص میزان اعتبار فرستنده



شکل ۲۹– صفحه‌ی آغازین فیلتر بر اساس میزان اطمینان به ارسال کننده‌ها



شکل ۳۱– صفحه‌ی تنظیم نحوه‌ی رفتار با ایمیل‌های فیلتر شده

فیلتر کردن ایمیل‌های رسیده بر اساس پیوست‌های مشکوک

امکان فیلتر کردن ایمیل‌ها بر اساس پیوست‌های آن‌ها نیز موجود است اما این قابلیت را باید با استفاده از دستورات خط فرمان PowerShell مربوط به Exchange server تنظیم نمود. برای بدست آوردن لیست دستورات موجود جهت انجام این تنظیمات، دستور get-help *attach* را در خط فرمان PowerShell وارد نمائید.

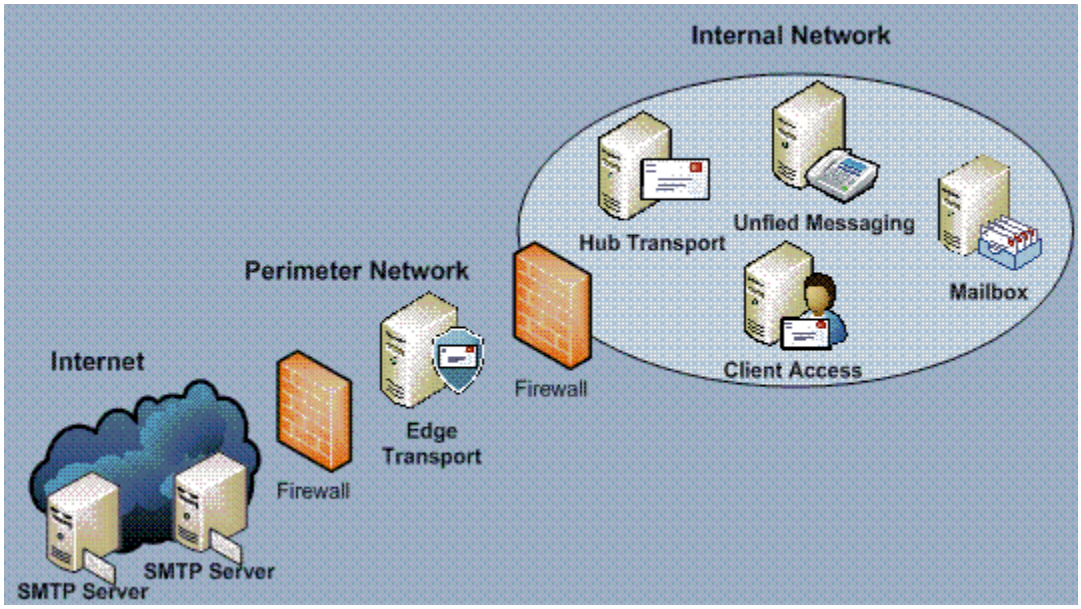
برای مثال امروز مشخص شده است که اگر ایمیلی به همراه پیوستی با پسوند vrs دریافت شد، این نوع ایمیل‌ها دارای ویروس بوده و سازمان را آلوده خواهند کرد. برای فیلتر کردن آن‌ها تنها کافی است دستور زیر را در خط فرمان PowerShell وارد نمود:

```
Add-AttachmentFilterEntry -Name *.vrs -Type FileName
```

فصل ۹- نصب و راه اندازی Edge Transport Server

در Exchange server 2010، نقش Edge transport server برای قرار گرفتن در محیطی محافظت شده توسط فایروال و سایر تمهیدات امنیتی و همچنین مجزا از Active directory جهت ارتباط با اینترنت طراحی شده است (شکل ۱). به علاوه از این نقش جهت بررسی هرزنامه‌ها و ویروس یابی ایمیل‌های رسیده نیز استفاده می‌شود. با توجه به اینکه این نقش خارج از Active directory جهت کاهش سطح حمله به آن نصب خواهد شد، برای دریافت اطلاعات صندوق‌های پستی کاربران از Active Directory Lightweight Directory Services یا AD LDS استفاده می‌کند. در اینجا برای هماهنگ سازی اطلاعات از EdgeSync نصب شده در Hub transport سرور کمک گرفته می‌شود که یک نوع replication رمزنگاری شده‌ی یک طرفه اطلاعات صندوق‌های پستی کاربران را با AD LDS نصب شده بر روی Edge transport server صورت می‌دهد. لازم به ذکر است که این اطلاعات همانند سازی شده تنها در حدی است که بتوان عملیات بررسی هرزنامه‌ها و همچنین جریان ارسال ایمیل‌ها را مشخص نمود. پس از دریافت ایمیل‌ها از اینترنت توسط نقش Edge transport server، آن‌ها به Hub transport سرور هدایت می‌شوند و برعکس.

در این فصل نحوه‌ی نصب و تنظیمات نقش Edge transport server را بررسی خواهیم کرد. مباحث مربوط به مبارزه با هرزنامه‌های آن همانند اطلاعات ذکر شده در فصل قبل است و از تکرار مجدد آن‌ها صرفنظر می‌شود.



شکل ۱– نحوه‌ی قرار گیری نقش Edge transport server در یک سازمان

نصب نقش Edge transport server

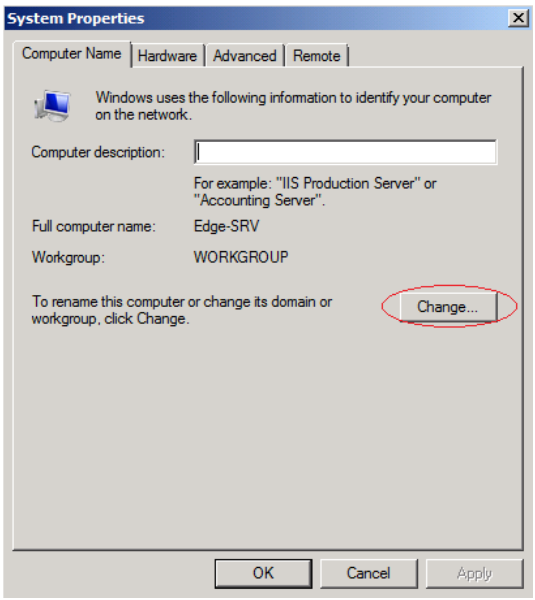
نقش Edge transport server را نمی‌توان به همراه سایر نقش‌های دیگر Exchange server بر روی یک سرور نصب نمود و حتما نیاز است تا آن‌را بر روی سروری مجزا و همچنین خارج از Active directory نصب کرد. پیش‌نیازهای نصب آن همانند سایر مواردی است که در فصل ۲ به آن‌ها اشاره شد (نصب دات نت فریم ورک ۳ و نیم سرویس پک یک، نصب آخرین نگارش‌های WinRM و همچنین PowerShell. به علاوه آخرین به روز رسانی‌های ویندوز نیز باید نصب شوند) و اگر به جدول ۱ فصل ۲ در مورد نقش Edge transport server دقت نمائیم، وجود ویژگی RSAT-ADLDS بر روی این سرور با اجرای دستور خط فرمان زیر ضروری است (یا همان Active Directory Lightweight Directory Services).

```
ServerManagerCmd -i ADLDS
```

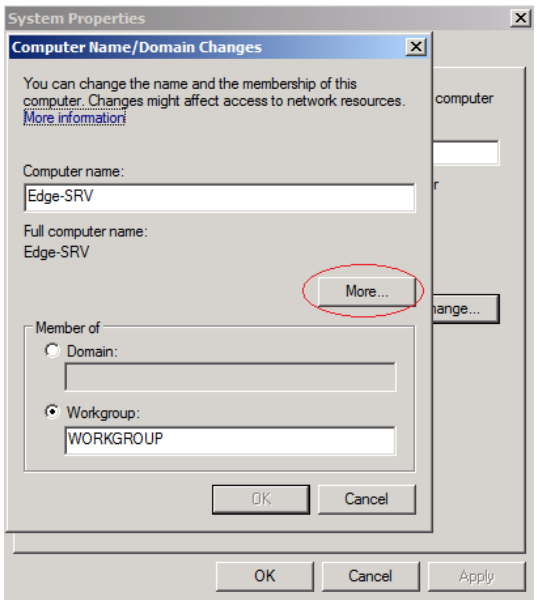
برای این منظور و نصب خودکار پیش‌نیازهای لازم، دستور زیر را در خط فرمان صادر نمائید (فایل xml ذکر شده در پوشه اسکریپت‌های DVD نصب Exchange server 2010 موجود است):

```
ServerManagerCmd -ip Exchange-Edge.xml -Restart
```

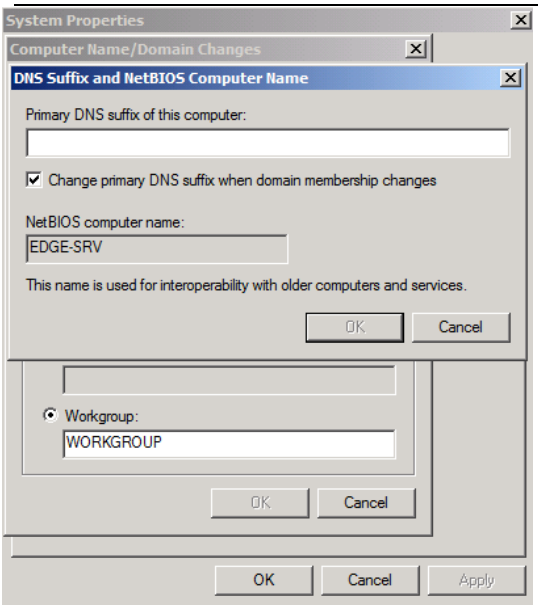
مطلب مهم دیگری که در این سرور حتما باید رعایت شود، تصحیح DNS suffix آن مطابق شکل‌های ۲ تا ۴ است (در غیر اینصورت موفق به نصب این نقش نخواهید شد).



شکل ۲- مراجعه به برگه‌ی خواص سیستم ویندوز



شکل ۳- کلیک بر روی دکمه‌ی More صفحه‌ی تعویض نام کامپیوتر جاری



شکل ۴– برگه‌ی وارد کردن DNS suffix صحیح

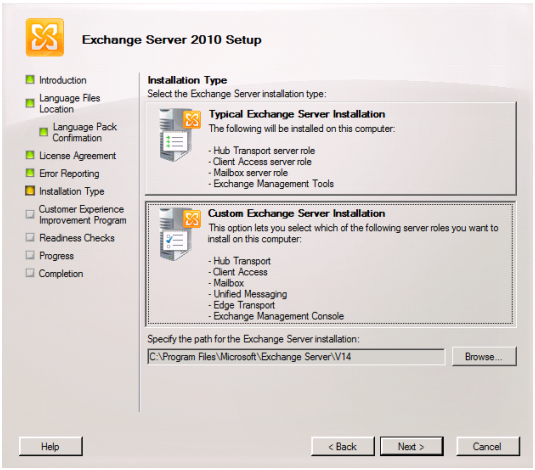
همچنین اطمینان حاصل کردن از اینکه دو سرور Edge transport server و Hub transport server بدون مشکل می‌توانند در شبکه به یکدیگر دسترسی داشته باشند نیز بسیار مهم است، در غیر اینصورت عملیات همانند سازی اطلاعات صندوق‌های پستی کاربران و همچنین انتقال ایمیل‌ها با شکست مواجه خواهند شد. برای این منظور باید FQDN سرور Hub transport در فایل hosts سرور Edge transport ذکر گردد و برعکس (فایل hosts در مسیر زیر قرار دارد):

%Systemroot%\System32\Drivers\Etc folder

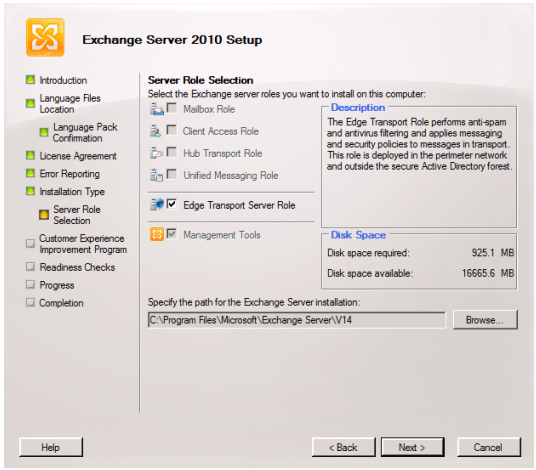
هر چند روش بهتر، استفاده از DNS server و ثبت یک static A record از سرورهای یاد شده در forward lookup zone آن می‌باشد.

به علاوه در فایروال‌های خود باید پورت ۲۵ سرور Edge transport به اینترنت و پورت‌های ۲۵ و ۵۰۶۳۶ جهت ارتباط با شبکه داخلی (Hub Transport server) باز شوند.

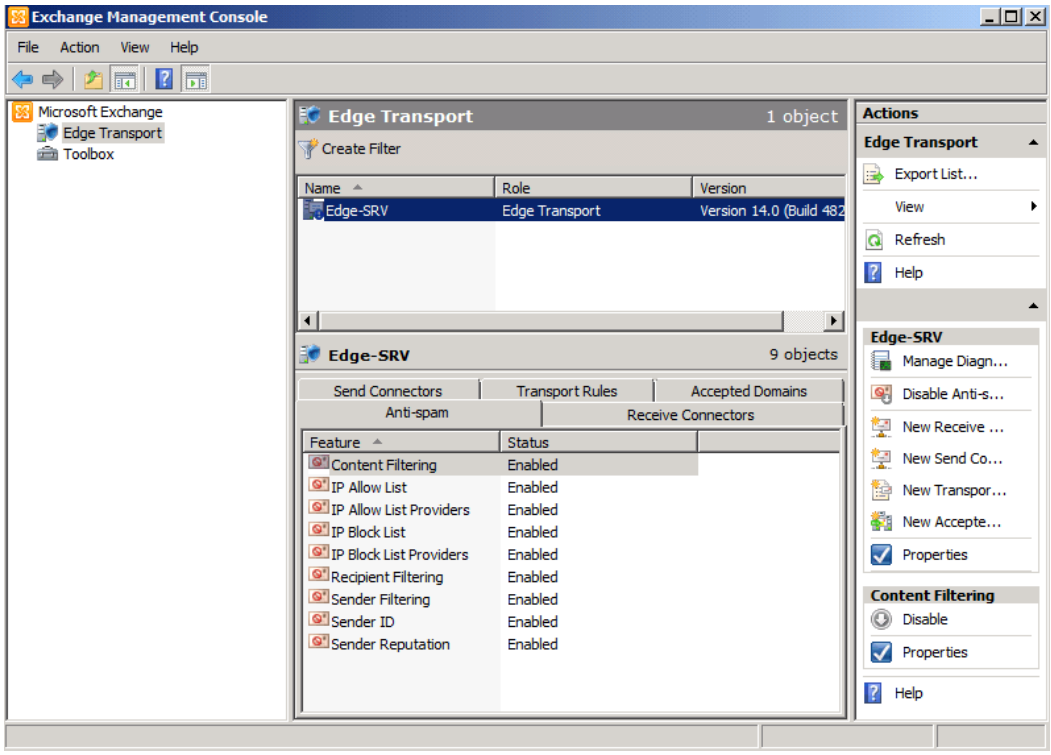
نصب نقش Edge transport server همانند روش‌های ذکر شده در فصل ۲ می‌باشد. ابتدا setup بسته‌ی نرم افزاری Exchange server را اجرا نمائید. تمامی مراحل نصب همانند مراحل ذکر شده است با دو تفاوت عمده که شامل انتخاب گزینه‌ی نصب سفارشی (شکل ۵) و سپس انتخاب نصب نقش Edge transport server می‌باشد (شکل ۶).



شکل ۵- انتخاب گزینه‌ی نصب سفارشی، جهت نصب نقش Edge transport server



شکل ۶- انتخاب گزینه‌ی Edge transport server



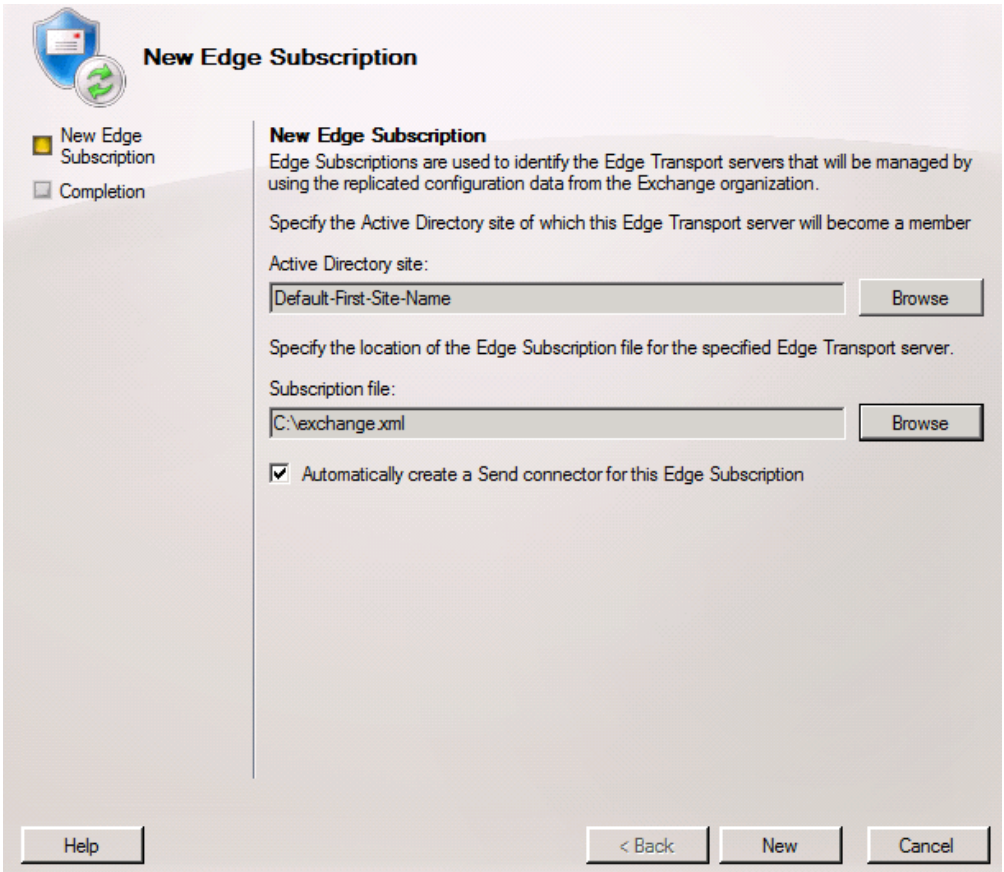
شکل ۷- نمایی از کنسول مدیریتی Edge transport server پس از نصب

انجام تنظیمات نقش Edge transport server

در ادامه باید کار شناسایی Edge transport server به Hub transport server صورت گیرد. برای این منظور در سرور Edge transport در خط فرمان PoweShell آن دستور زیرا صادر نمائید تا فایل تنظیمات مربوطه جهت معرفی آن سرور به Hub transport server تولید شود:

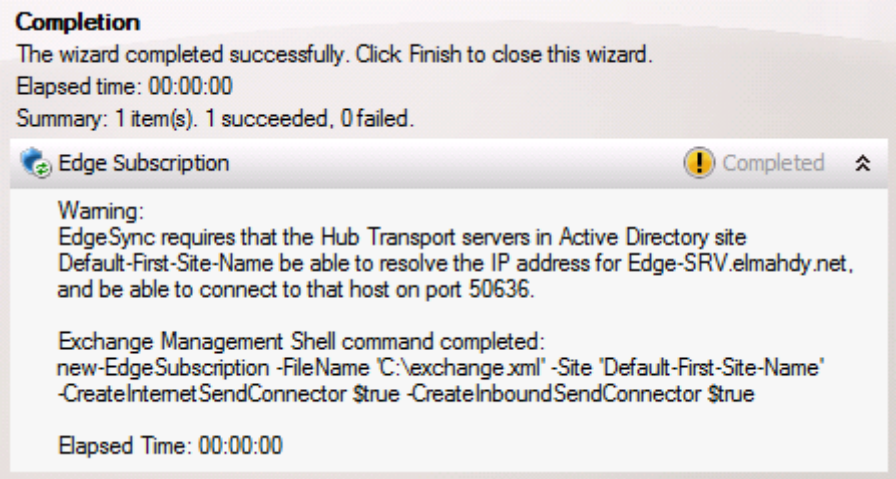
```
new-EdgeSubscription -file "c:\exchange.xml"
```

سپس فایل exchange.xml تولیدی را به سرور Hub transport منتقل نمائید. در این سرور پس از مراجعه به کنسول مدیریتی Exchange server ، در قسمت Organization configuration و گزینه‌ی Hub transport آن، به برگه‌ی Edge subscriptions مراجعه کنید. اکنون در برگه‌ی actions سمت راست صفحه بر روی لینک new edge subscription کلیک نمائید تا صفحه‌ی معرفی فایل xml ذکر شده باز شود (شکل ۸). پس از معرفی Active directory site و مسیر فایل xml تولید شده، بر روی دکمه‌ی New کلیک نمائید تا کار اشتراک به پایان رسد.



شکل ۸– معرفی Edge transport server نصب شده به Hub transport server موجود.

پس از پایان کار اشتراک، یک صفحه‌ی اخطار در مورد یادآوری الزام باز بودن پورت شماره ۵۰۶۳۶ جهت برقراری ارتباطات بین این دو سرور و همچنین اهمیت تنظیمات صحیح DNS ارائه می‌شود (شکل ۹).



شکل ۹– صفحه‌ی اخطار پس از ایجاد اشتراک Edge transport server.

به صورت خلاصه باید پورت‌های زیر در فایروال‌های موجود معرفی شوند:

- جهت ترافیک داخلی
  - SMTP – TCP port 25 از اینترنت
  - SMTP – TCP port 25 از Edge Transport server به Hub Transport server
  - DNS – UDP port 53 از Edge Transport server به Hub Transport server
- جهت ترافیک خارجی
  - SMTP – TCP/UDP port 25 از Edge Transport server به internet
  - SMTP – TCP/UDP port 25 از Hub Transport server به Edge Transport server
  - TCP port 50389 از Hub Transport server به Edge Transport server جهت ارتباطات LDAP for EdgeSync
  - TCP port 50636 از server به Edge Transport server جهت ارتباطات امن LDAP for EdgeSync
  - DNS – UDP port 53 از Edge Transport server به internet

پس از این مرحله باید تنظیمات مربوط به هماهنگ سازی این دو سرور صورت گیرد. برای پیاده سازی آن ابتدا در Edge Transport Server و کنسول مدیریتی Exchange server آن، به برگه‌ی زیر مراجعه کنید:

Organization configuration > Edge Transport Server > Receive connectors

در اینجا باید یک Receive Connector جدید را با استفاده از برگه‌ی actions سمت راست صفحه ایجاد کرد. نوع اتصال دهند را internal انتخاب کرده در صفحه‌ی بعد آدرس IP سرور Hub transport را وارد نمائید. پس از طی این مراحل امکان دریافت اطلاعات هماهنگ سازی از Hub transport میسر خواهد شد. سپس در خط فرمان PowerShell دستور زیر را وارد نمائید:

```
Start-EdgeSubscription
```

اکنون مجددا به Hub transport server مراجعه کرده و دستور زیر را در خط فرمان PowerShell وارد کنید تا کار هماهنگ سازی شروع شود:

```
Start-EdgeSynchronization
```

و برای اطمینان حاصل نمودن از عملیات انجام شده دستور زیر را در خط فرمان PowerShell وارد کنید:

```
Test-EdgeSynchronization
```

اگر در اینجا پیغام Failed را مشاهده کردید، به قسمت Failure details خروجی حاصل دقت نمائید. احتمالا در قسمت تعریف Receive Connector جدید در Edge transport server مشکلی وجود دارد. همچنین برگه‌ی Accepted domains آن‌را نیز باید بررسی نمود. هر چند پس از اجرای دستور Start-EdgeSubscription ، قسمت Accepted domains به صورت خودکار تنظیم شده و دو Receive Connector جدید نیز اضافه خواهند شد. این دو Receive Connector جدید در سرور Hub transport نیز ایجاد خواهند شد. کار آن‌ها ارسال ایمیل به اینترنت و دریافت ایمیل از اینترنت می‌باشد.

منابع و مآخذ

1- Morimoto R., Noel M., Amaris C., Abbate A., Weinhardt M., "Microsoft® Exchange Server 2010 Unleashed", Sams pub., 2010.
2- http://smtp25.blogspot.com
3- http://johanveldhuis.nl
4- http://blog.elmahdy.net
5- http://unifiedit.wordpress.com
6- http://exchangepedia.com
7- http://www.expta.com
8- http://mostlyexchange.blogspot.com