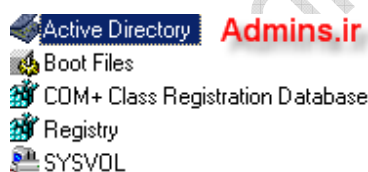


به نام خداوند ایران زمین

امروزه تهیه پشتیبان از فایل ها ، اسناد و دیتاها در هر شبکه و سیستمی ، خواه شبکه کوچک یا بزرگ باشد ضروری به نظر می رسد ؛ حتی تهیه پشتیبان بر روی رایانه های شخصی هم گاهی واجب می باشد. در همین راستا پشتیبان گیری از Active Directory هم در جهت نگهداری و پشتیبانی از آن یکی از اصول پایه و مهم به شمار می آید.

تهیه پشتیبان از Active Directory را به ۲ صورت گرافیکی و توسط خط فرمان می توان انجام داد که در این آموزش هر دو صورت بررسی خواهد شد. پشتیبان گیری مرتب و طبق زمانبندی مناسب سبب می شود تا در مواقع بحرانی از دست دادن دیتا و اطلاعات شانس بیشتری در جهت برگرداندن آنها داشته باشید. برای تهیه پشتیبان از Active Directory می بایست از **Systemstate** پشتیبان تهیه کنید ، پشتیبان گیری از Active Directory هیچ گونه خللی در کار Domain Controller و شبکه ایجاد نمی کند. SystemState دارای اجزای مختلفی می باشد ، که این اجزا بر روی سیستمی که نقش Domain Controller ایفا می کند متفاوت از دیگر سیستم ها می باشد. در این جا اجزای تشکیل دهنده آن در یک DC مورد بررسی قرار می دهیم :



۱. Active Directory
۲. Boot Files
۳. COM+ Class Registration Database
۴. Registry
۵. **SYSVOL**
۶. Certificate Service Database

نکته :

موارد ۱ و ۵ فقط بر روی Domain Controller جزئی از SystemState هستند. مورد ۶ فقط بر روی سیستمی که CA سرور باشد وجود خواهد داشت.

اکثر اجزای در بالا ذکر شده را می توان از اسمشان به کارایشان پی برد و فقط به توضیحی کوتاه در مورد SYSVOL می پردازیم :
SYSVOL یک فولدر به اشتراک گذاشته شده می باشد که حاوی تمپلت های GroupPolicy و اسکریپت های Logon می باشد.

هر چند SystemState در بردارنده اکثر تنظیمات سیستم می باشد ولی الزاما حاوی تمام فایل ها و اطلاعات مورد نیاز برای برگرداندن کامل سیستم به قبل از خرابی و مشکل

نمی باشد . البته برای برگرداندن اطلاعات Active Directory تهیه پشتیبان از آن کافی است ؛ برای تهیه پشتیبان کامل از سیستم می توان از ابزارهایی نظیر NortonGhost بهره جست.

نکته مهم :

در هنگام تهیه پشتیبان از Active Directory باید به زمان مشخص شده برای **Tombstone** (سنگ قبر) توجه داشته باشیم از آن رو که نمی توان آن را از پشتیبان گرفته شده قبل مدت زمان مشخص شده برای Tombstone بازگرداند ؛ زمان پیش فرض ۶۰ روز می باشد که اگر ویندوز بروز رسانی شده باشد تا ۱۸۰ روز هم قابل افزایش می باشد. پس سعی کنید در بازه های زمانی کوتاه پشتیبان گیری صورت گیرد و حداقل ۲ پشتیبان در زمان Tombstone داشته باشید.

Tombstone چیست ؟

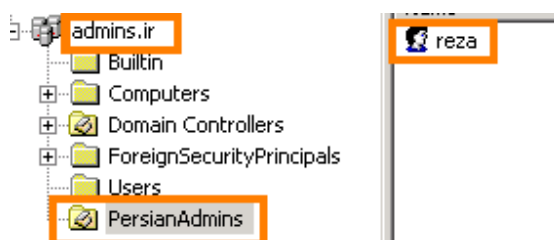
وقتی یک Object را از Active Directory پاک می کنیم در مرحله اول بطور فیزیکی از پایگاه داده حذف نمی شود بلکه Active Directory مشخصه **isDeleted** (attribute) را True می کند و آن را به یک container خاص به نام **CM Deleted** انتقال می دهد ,حالا این Object یک Tombstone می باشد که با استفاده از ابزارهای معمول قابل مشاهده نمی باشد.

می توان با استفاده از این خاصیت Objectهایی که اشتباه پاک شده اند را حتی بدون استفاده از Backup&Restore بازیابی کرد. یکی از ابزارهایی که می تواند Tombstoneها را بازگرداند **Adrestore** می باشد.

شرکت مایکروسافت داشتن حداقل ۲ سرور Domain Controller را توصیه کرده است , چنانکه در صورت خرابی سرور اصلی , سرور پشتیبان وظایف آن را بعهده می گیرد و خللی در کار شبکه به وجود نمی آید ؛ البته فقط یک سرور می تواند در بردارنده **Operations master role** ها باشد و در صورت از دست دادن کامل DC اصلی این ها را به DC دیگر انتقال می دهیم. DC های پشتیبان را Additional Domian Controller می نامند و هنگام نصب Active Directory در پنجره Active Directory Type باید Additional Domain Controller for existing domain را انتخاب کرد. هر چند داشتن Additional DC بسیار ریسک از دست دادن اطلاعات را کاهش می دهد ولی برای بازگردانی اطلاعات بصورت **Auhoritative** (در ادامه بررسی می شود) به پشتیبان SystemState نیاز خواهید داشت.

ایجاد تغییراتی برای آزمایش :

برای اینکه پشتیبان گیری و بازگرداندن آن فایل لمس باشد , یک OU به نام PersianAdmins و یک کاربر با نام Reza ایجاد کنید.



پشتیبان گیری از **Active Directory** :

همان طور که اشاره شد برای پشتیبان گیری از ActiveDirectory باید از Systemstate پشتیبان تهیه کنیم , برای این منظور کابری که قصد گرفتن پشتیبان دارد باید عضو گروه **Domain Admins** باشد تا بتواند این عملیات را انجام دهد. توجه داشته باشید که برای تهیه پشتیبان باید حتما بصورت Local از ابزار Backup Utility استفاده کنید , از آنجاییکه پشتیبان SystemState را نمی توان از راه دور تهیه کرد , البته می توان از Remote Desktop جهت اجرای این ابزار بصورت Local بهره جست.

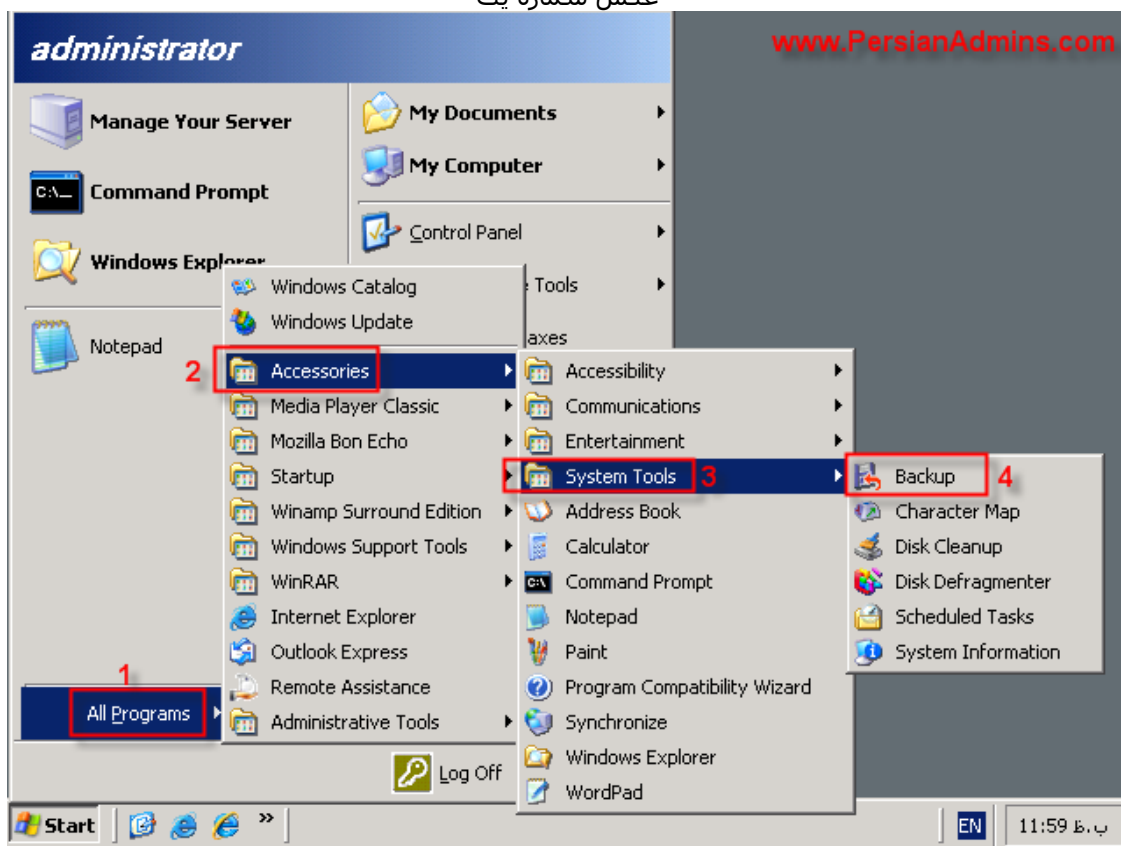
پشتیبان گیری توسط رابط گرافیکی :

برای تهیه پشتیبان مراحل زیر را طی می کنیم :

۱ - از منوی شروع آدرس زیر را جهت اجرای Backup Utility طی می کنیم :

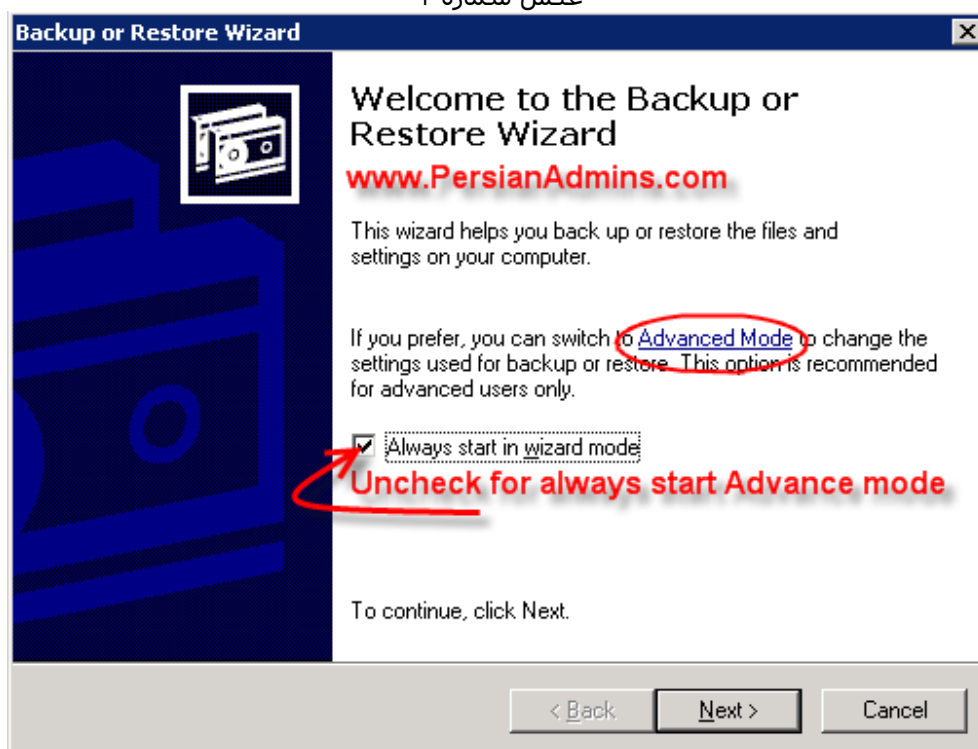
Start Menu → All Programs → Accessories → System Tools → Backup

عکس شماره یک



۲ - در پنجره Backup or Restore Wizard طبق عکس بر روی Advance mode کلیک کنید. (عکس شماره ۲)
اگر می خواهید همیشه در حالت پیشرفته اجرا شود ، تیک Always start in wizard mode را بردارید.

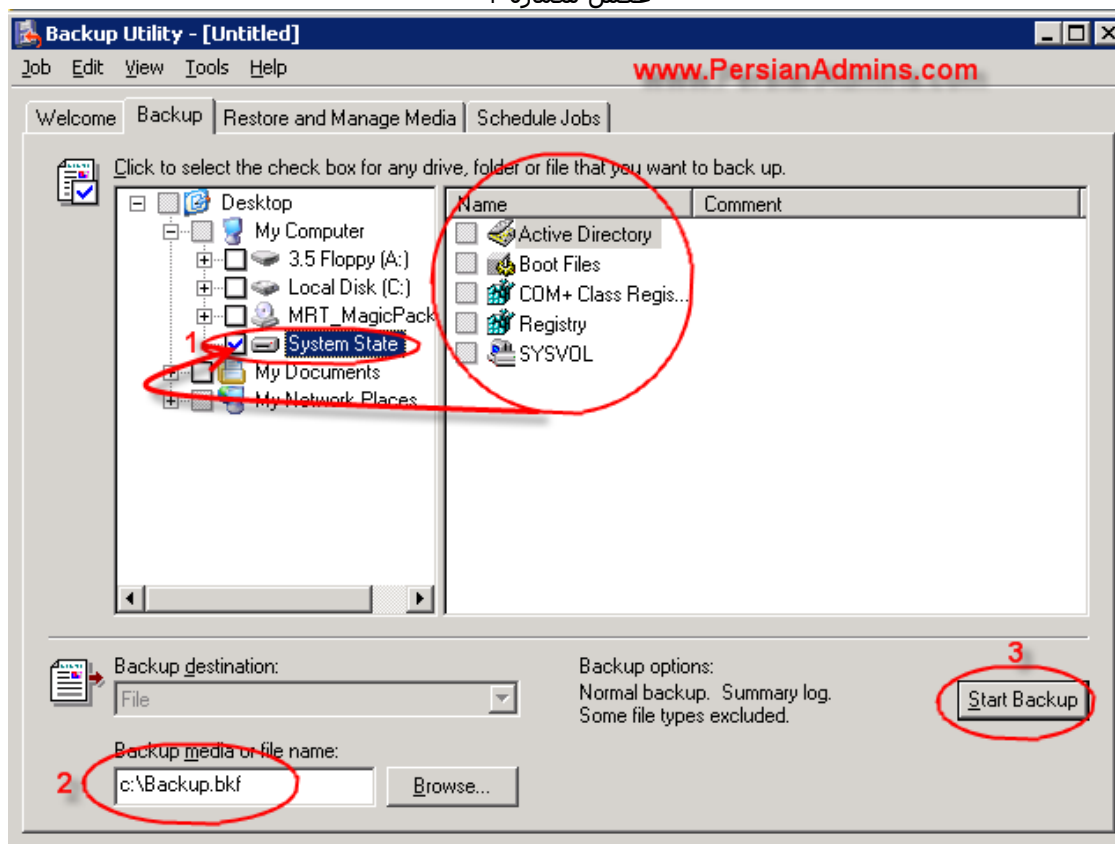
عکس شماره ۲



۲ - در تب Backup , طبق عکس شماره ۲ SystemState را انتخاب و تیک آن را بزنید.

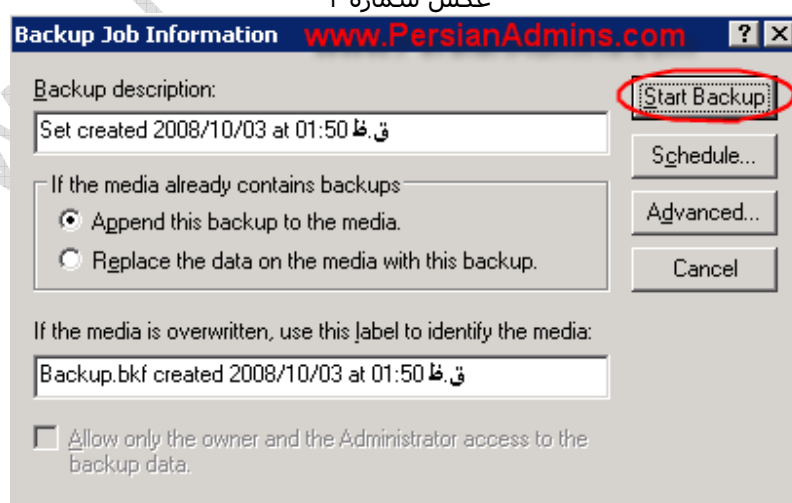
۴ - از دکمه Browse محلی که می خواهید پشتیبان در آنجا ذخیره شود را مشخص و نامی متناسب برای آن انتخاب کنید , سپس بر روی Start Backup کلیک کنید.

عکس شماره ۲



۵ - در پنجره Backup Job Information بر روی Start Backup کلیک کنید. همچنین می توانید برای یک پشتیبان گیری مرتب در همین مرحله بر روی Schedule کلیک کنید و زمانبندی مناسب را انجام دهید.

عکس شماره ۴



۶ - در این مرحله پشتیبان گیری شروع و پایان می پذیرد , در آخر بر روی Close کلیک کنید.

عکس شماره ۵



توجه :

توصیه می شود پشتیبان را حتما در حالت Normal انجام دهید و از انواع دیگر پشتیبان گیری مانند Incremental یا Differential خودداری کنید. (توضیح در مورد انواع حالت های پشتیبان گیری به کتاب ۲۷۰-۷۰ یا ۲۹۰-۷۰ مراجعه کنید.)

پشتیبان گیری توسط خط فرمان :

برای تهیه پشتیبان توسط خط فرمان (Command Line) مراحل زیر را طی کنید :

۱ - از منوی Start برنامه CMD را از آدرس زیر اجرا کنید.
Start → Run → Enter 'CMD' → OK

۲ - در خط فرمان با استفاده از دستور ntbakup به صورت زیر می توان پشتیبان تهیه کرد :

```
Ntbackup backup systemstate /J 'Backup Job' /F 'c:/systemstate.bak'
```

ntbackup : ابزار پشتیبان گیری از طریق خط فرمان می باشد.
Backup : مشخص کننده این است که عملیات پشتیبان گیری صورت می پذیرد.
Systemstate : مشخص کننده این است که از Systemstate پشتیبان گرفته می شود.
/F : نام فایل پشتیبان و محل آن را مشخص می کند.

ایجاد تغییراتی برای آزمایش :

اکنون برای آزمایش بازگردانی اطلاعات ، OU ، PersianAdmins ، و کاربر Reza که ایجاد کرده بودید را حذف کنید.

بازگرداندن اطلاعات Restore Active Directory :

در ویندوز سرور ۲۰۰۳ برای بازگرداندن پایگاه داده Active directory در صورت تنظیمات اشتباه ، خرابی یا از دست دادن اطلاعات بدلیل مشکلات سخت افزاری و نرم افزاری شیوه های مختلفی وجود دارد ، در ساده ترین حالت در صورت وجود چندین DC می توان DC دیگری را نصب و سپس به واسطه Replication بین DC ها تمامی اطلاعات به DC جدید منتقل خواهد شد ؛ راه دیگر استفاده از ابزار پشتیبان گیری برای بازگرداندن اطلاعات می باشد.

توجه داشته باشید که وقتی از یک Domain Controller پشتیبان تهیه می کنید ، از تمامی دیتاهای Active Directory به همراه فولدر SYSVOL و Registry بر روی سرور پشتیبان گرفته می شود پس در موقع بازگرداندن آن ، هر آنچه پشتیبان گرفته شده همچون تنظیمات Group policy و رجستری هم به حالت قبل باز می گردد.

شیوه های بازگرداندن پشتیبان :

برای بازگرداندن پشتیبان Active Directory ۳ روش وجود دارد :

۱ - Primary

۲ - Normal (NonAuthoritative)

۳ - Authoritative

۱ - Primary : این شیوه اولین Domain Controller را مجدداً ایجاد می کند وقتی هیچ راه دیگری برای ایجاد دوباره دومین وجود ندارد. این شیوه زمانی کاربرد دارد که هیچ DC دیگری در شبکه وجود ندارد و می خواهید DC اصلی را توسط پشتیبان مجدد ایجاد کنید.

۲ - Normal : این شیوه دوباره Active Directory را به حالت قبل از پشتیبان گیری برمی گرداند و سپس به واسطه Replicate بین DC ها بروز می شود. این شیوه زمانی استفاده می شود که چندین DC در شبکه وجود دارد و می خواهید یک DC را به آخرین وضعیت مناسب آن برگردانید.

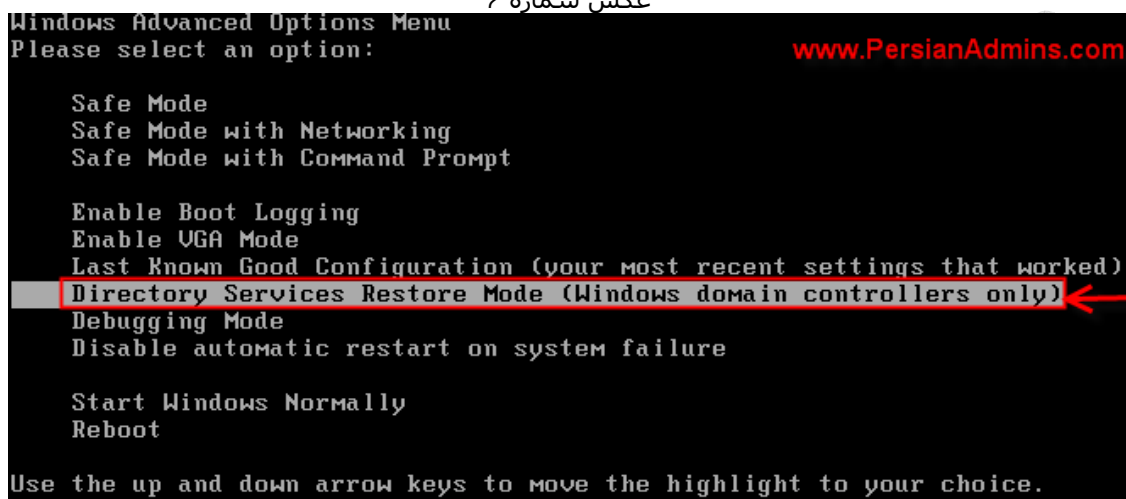
۳ - Authoritative : این شیوه پشت سر Normal استفاده می شود بدین معنی که مراحل همانند Normal صورت می پذیرد منتها در آخر یک سری دیتای مشخص را نشانه دار می کنید تا در Replicate بین DC ها برعکس Normal بازنویسی نشوند . فرض کنید اشتباهی یک OU را حذف کرده اید و در Replicate بین دومین ها این OU در تمام DC های دیگر هم حذف شده است ، هم اکنون برای بازگرداندن آن فقط می توانید از شیوه Authoritative استفاده کنید ، زیرا به علت وجود DC از شیوه Primary نمی توان استفاده کرد ، در صورت استفاده از Primary کلیه اطلاعات بعد از پشتیبان گیری از بین می رود ؛ در صورت استفاده از شیوه Normal به خاطر Replicate بین DC ها ، OU که در DC های دیگر پاک شده است در DC جدید هم پاک می شود پس باید با مشخص کردن آن بصورت Authoritative از بازنویسی آن جلوگیری کرد.

نحوه بازگرداندن بصورت Primary :

برای بازگرداندن پشتیبان مراحل زیر را طی کنید :

۱ - Domain Controller را در حالت **Directory Services Restore Mode** شروع مجدد کنید.

عکس شماره ۶



۲ - از منوی شروع آدرس زیر را جهت اجرای Backup Utility طی می کنیم :

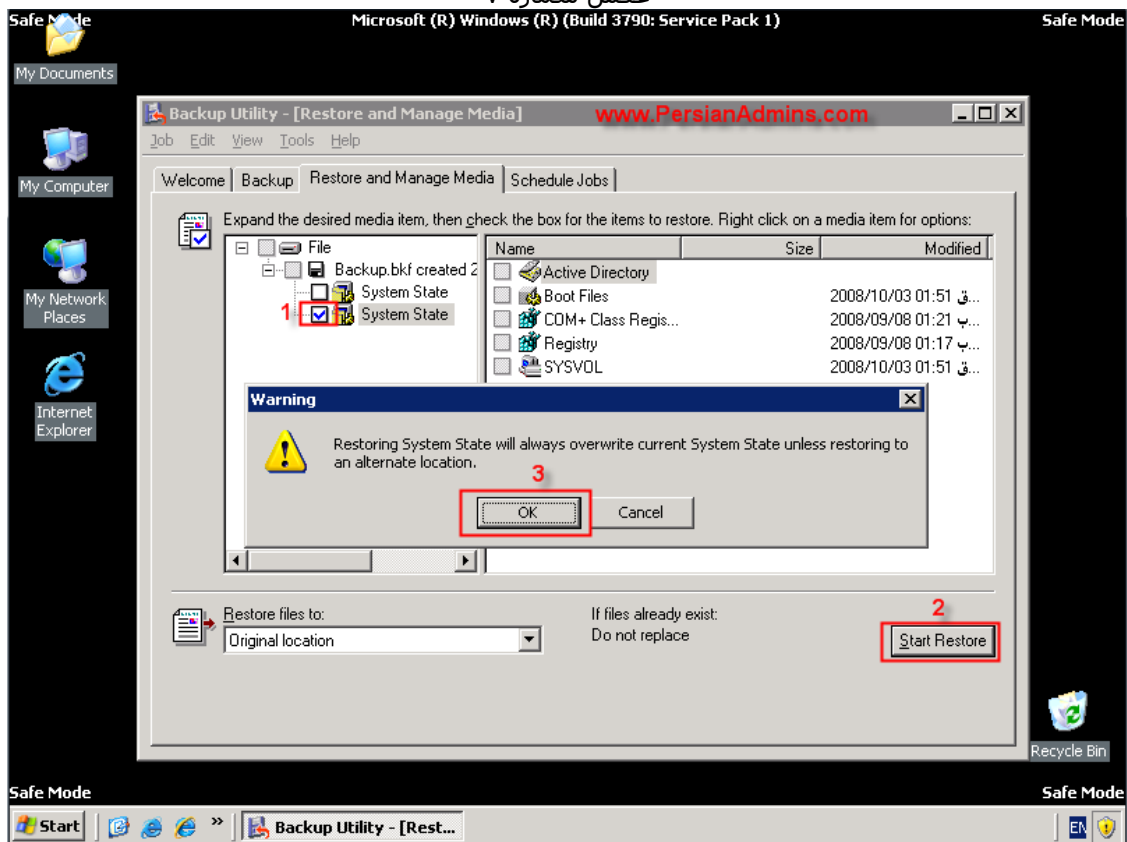
Start Menu → All Programs → Accessories → Sytem Tools → Backup

۳ - در پنجره Backup or Restore Wizard بر روی Advance mode کلیک کنید.(عکس شماره ۲)

۴ - در تب Restore and Manage Media هر آنچه که می خواهید بازگردانید که در اینجا SystemState می باشد را انتخاب و سپس بر روی Start Restore کلیک کنید ؛ یک صفحه هشدار دهنده باز می شود که OK را می بایست انتخاب کنید.

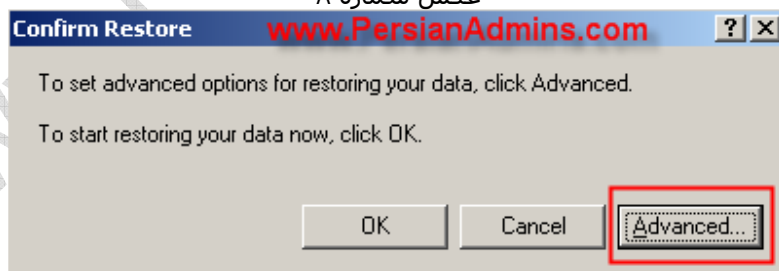
آموزش پشتیبان گیری از **Active Directory**

عکس شماره ۷



۵ - در Confirm Restore بر روی Advanced کلیک کنید.

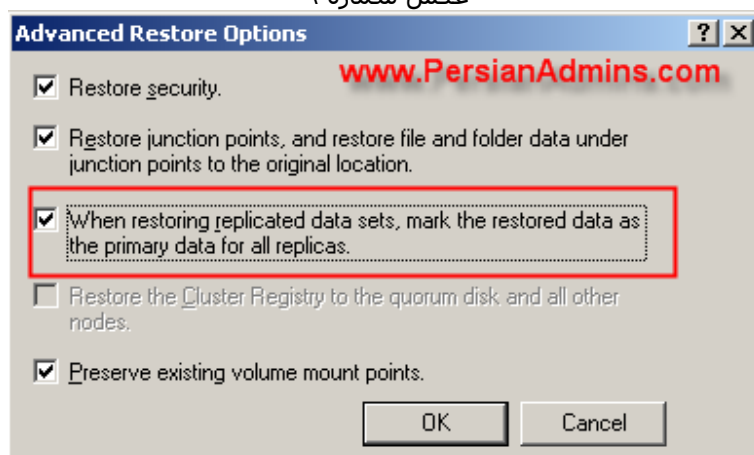
عکس شماره ۸



آموزش پشتیبان گیری از Backup and Restore **Active Directory**

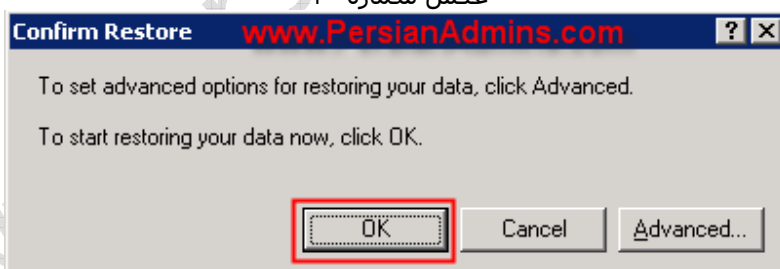
۶ - در پنجره Advanced Restore options ، When restoring replicated data sets, mark the restored data as the primary data for all replicas را انتخاب و بر روی ok کلیک کنید.

عکس شماره ۹



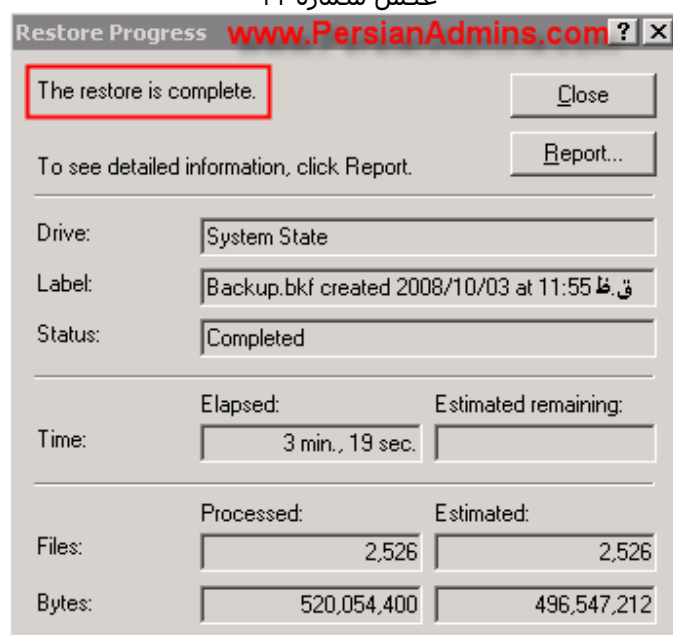
۷ - بر روی ok کلیک کنید.

عکس شماره ۱۰



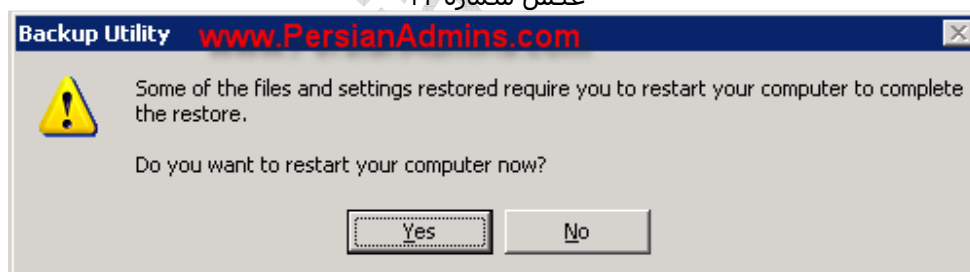
۸ - در این مرحله بازگردانی پشتیبان پایان می پذیرد. بر روی Close کلیک کنید.

عکس شماره ۱۱



۹ - در پنجره Backup Utility پیغامی مبنی بر شروع مجدد سیستم ظاهر می شود که شما Yes را انتخاب کنید.

عکس شماره ۱۲

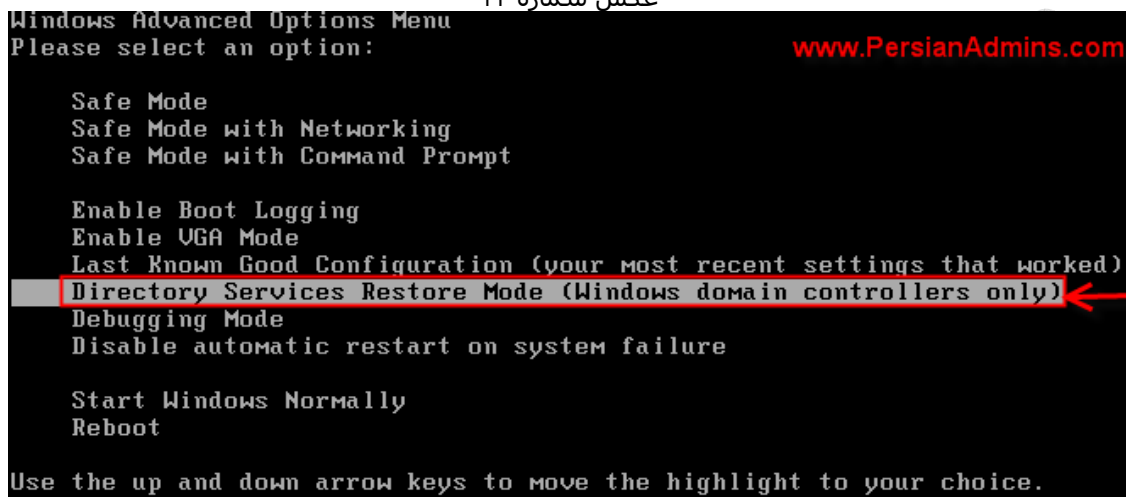


نحوه بازگرداندن بصورت Normal :

برای بازگرداندن پشتیبان مراحل زیر را طی کنید :

۱ - Domain Controller را در حالت **Directory Services Restore Mode** شروع مجدد کنید.

عکس شماره ۱۳



۲ - از منوی شروع آدرس زیر را جهت اجرای Backup Utility طی می کنیم :

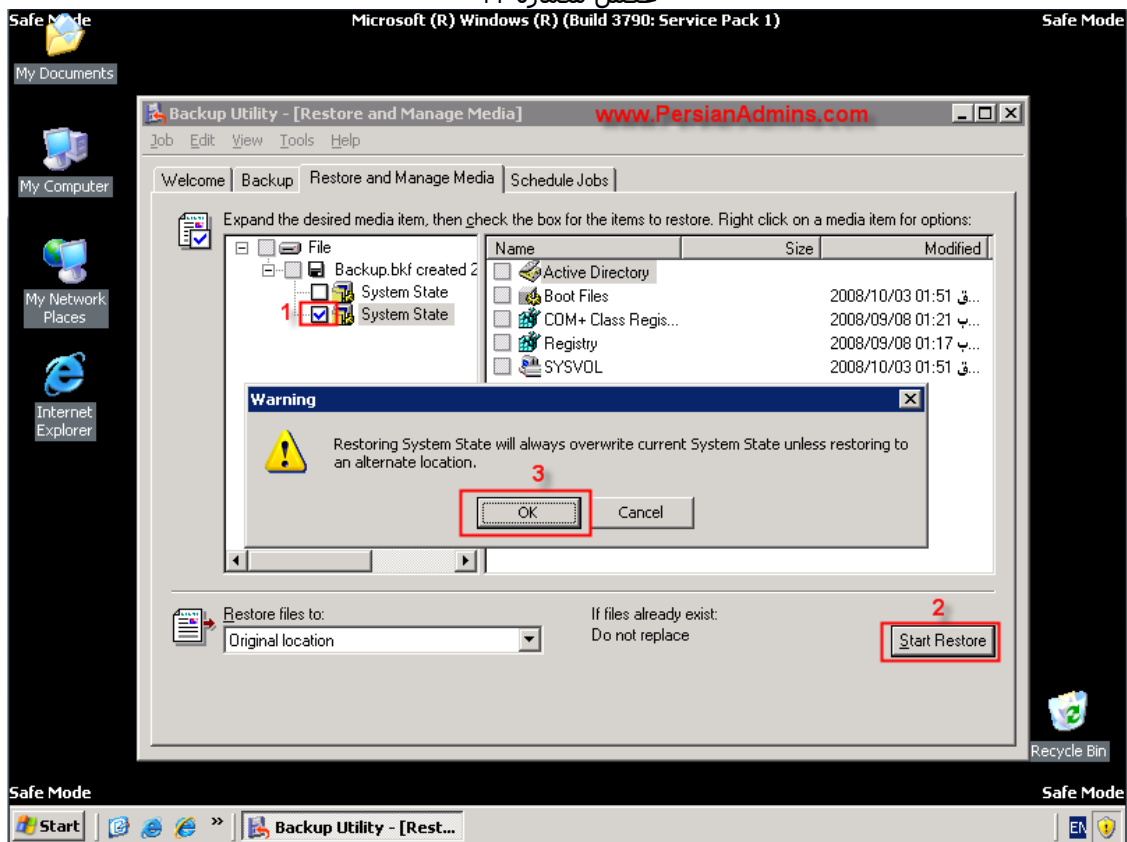
Start Menu → All Programs → Accessories → Sytem Tools → Backup

۳ - در پنجره Backup or Restore Wizard بر روی Advance mode کلیک کنید.(عکس شماره ۲)

۴ - در تب Restore and Manage Media هر آنچه که می خواهید بازگردانید که در اینجا SystemState می باشد را انتخاب و سپس بر روی Start Restore کلیک کنید ؛ یک صفحه هشدار دهنده باز می شود که OK را می بایست انتخاب کنید.

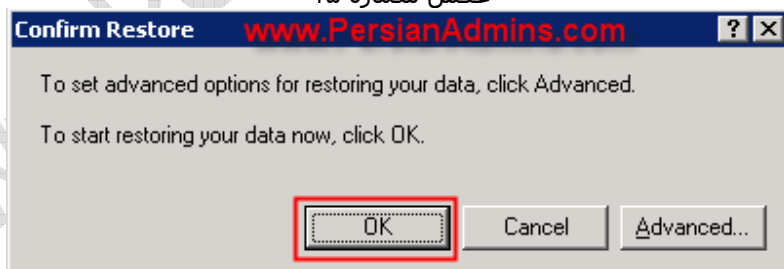
آموزش پشتیبان گیری از **Active Directory** Backup and Restore

عکس شماره ۱۴



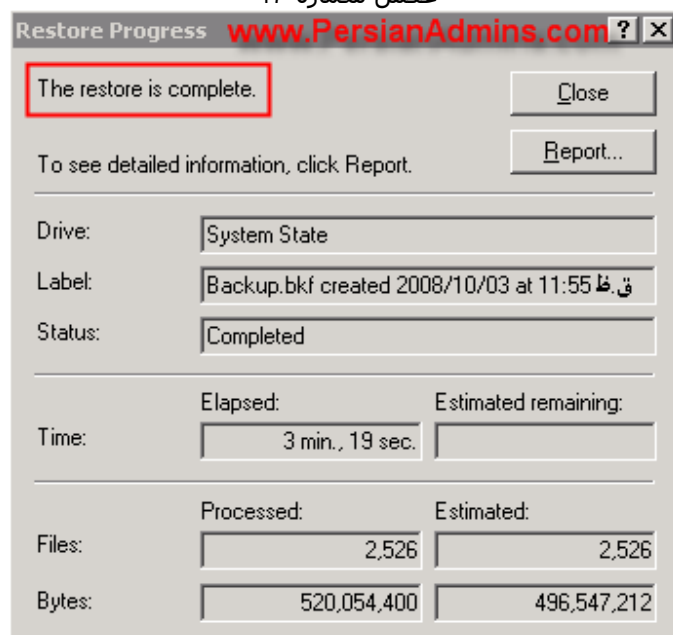
5 - بر روی ok کلیک کنید.

عکس شماره ۱۵



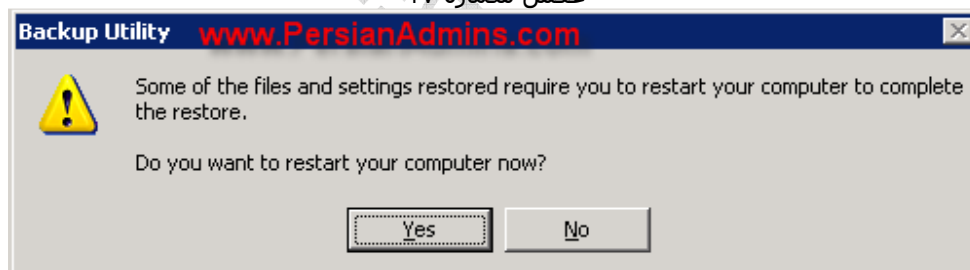
6 - در این مرحله بازگردانی پشتیبان پایان می پذیرد. بر روی Close کلیک کنید.

عکس شماره ۱۶



7 - در پنجره Backup Utility پیغامی مبنی بر شروع مجدد سیستم ظاهر می شود ,
Yes را انتخاب کنید.

عکس شماره ۱۷

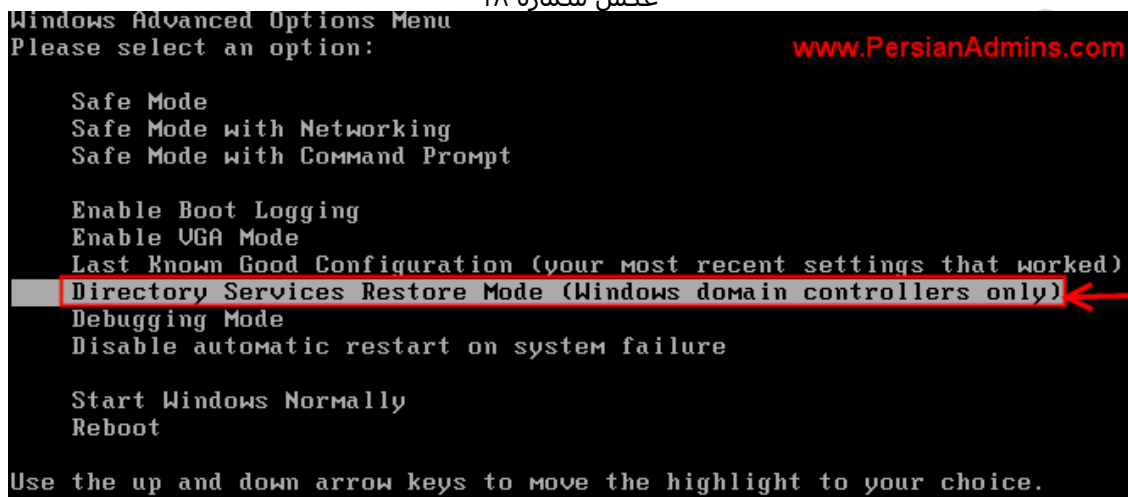


نحوه بازگرداندن بصورت **Authoritative** :

برای بازگرداندن پشتیبان مراحل زیر را طی کنید :

۱ - Domain Controller را در حالت **Directory Services Restore Mode** شروع مجدد کنید.

عکس شماره ۱۸



۲ - از منوی شروع آدرس زیر را جهت اجرای Backup Utility طی می کنیم :

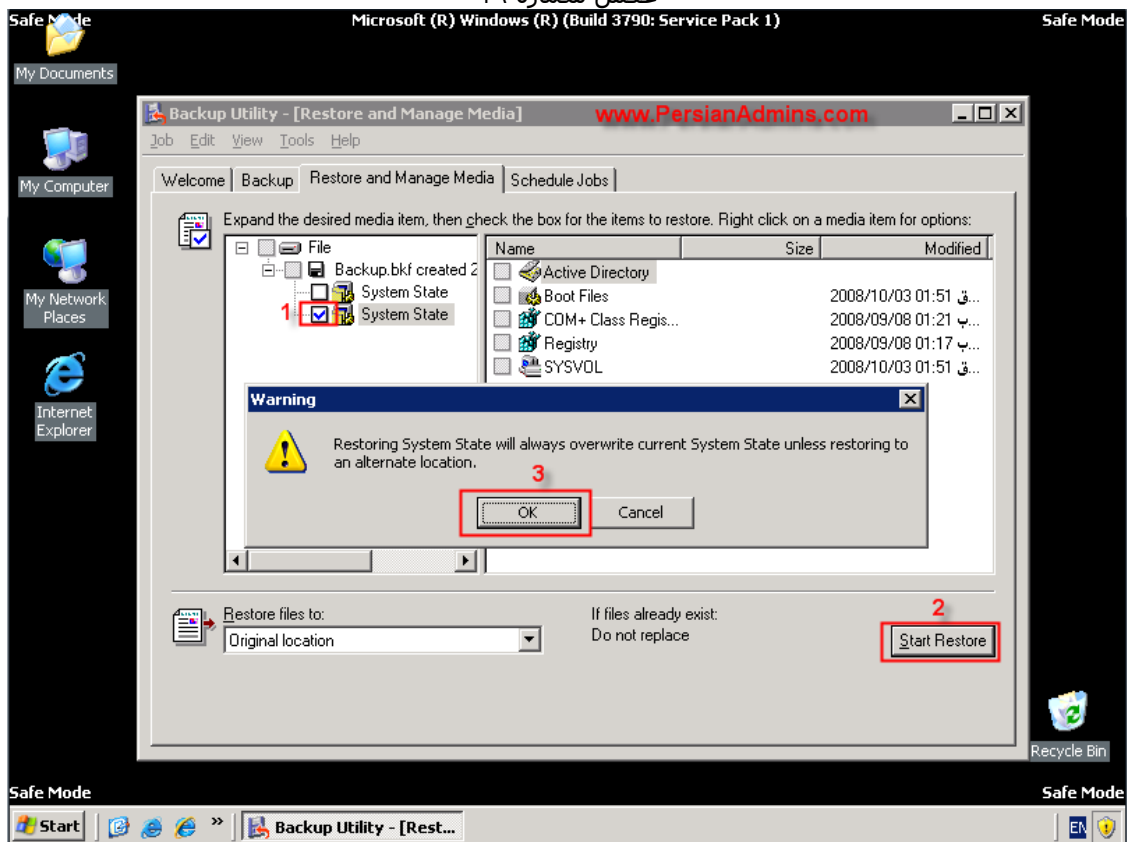
Start Menu → All Programs → Accessories → Sytem Tools → Backup

۳ - در پنجره Backup or Restore Wizard بر روی Advance mode کلیک کنید.(عکس شماره ۲)

4 - در تب Restore and Manage Media هر آنچه که می خواهید بازگردانید که در اینجا SystemState می باشد را انتخاب و سپس بر روی Start Restore کلیک کنید ؛ یک صفحه هشدار دهنده باز می شود که OK را می بایست انتخاب کنید.

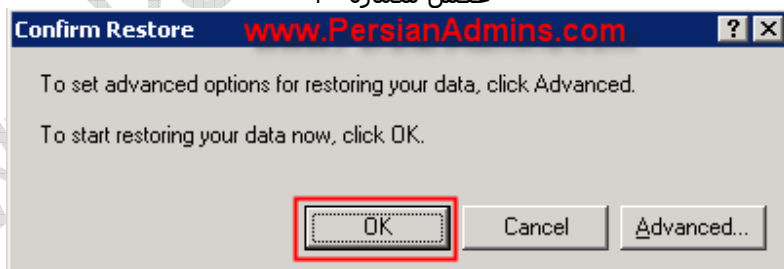
آموزش پشتیبان گیری از **Active Directory** Backup and Restore

عکس شماره ۱۹



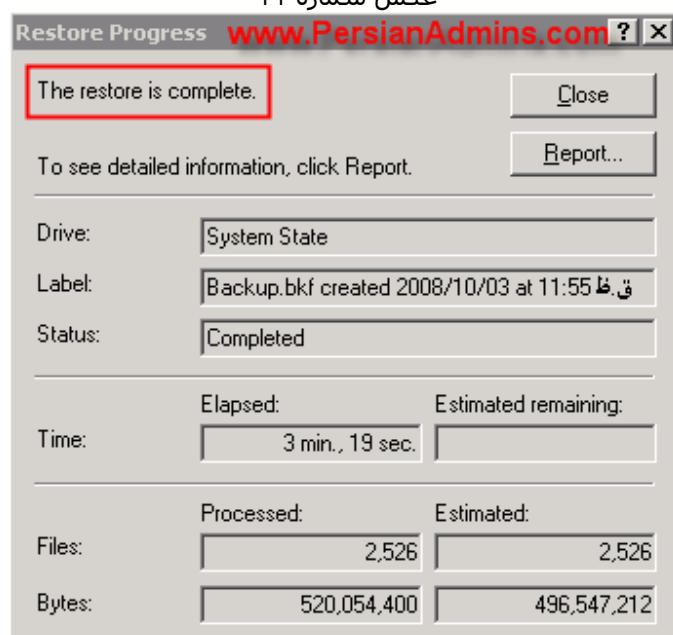
5 - بر روی OK کلیک کنید.

عکس شماره ۲۰



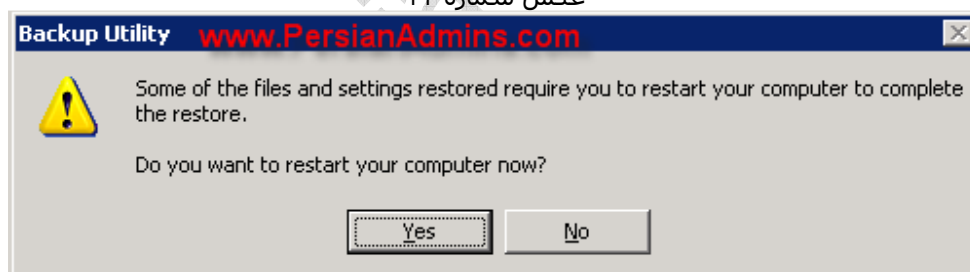
6 - در این مرحله بازگردانی پشتیبان پایان می پذیرد. بر روی Close کلیک کنید.

عکس شماره ۲۱



7 - در پنجره Backup Utility پیغامی مبنی بر شروع مجدد سیستم ظاهر می شود ، که بر عکس شیوه Normal می بایست No را انتخاب کنید.

عکس شماره ۲۲



تفاوت شیوه Normal با Authoritative از همین مرحله آغاز می شود که یک سری دیتا را برای جلوگیری از بازنویسی در Replicate بین DCها نشانه دار می کنید.

8 - از منوی Start برنامه CMD را از آدرس زیر اجرا کنید.
Start → Run → Enter `CMD` → OK

9 - در خط فرمان **Ntdsutil** را اجرا کنید.(عکس شماره ۲۳)

10 -در اعلان Ntdsutil , **authoritative restore** را تایپ و اجرا کنید.(عکس شماره ۲۳)

11 - در اعلان authoritative restore برای نشانه گذاری بدین ترتیب عمل کنید :

Restore subtree distinguished_name_of_object

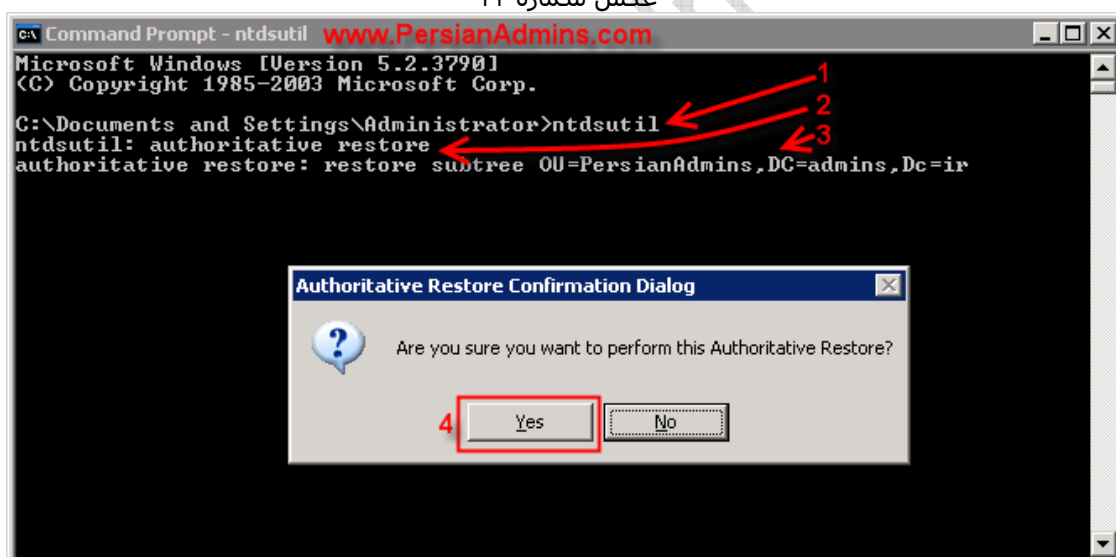
(Distinguished Name آدرس آیجکت در Active Directory می باشد , [اطلاعات بیشتر](#))

برای مثال برای نشانه گذاری OU , PersianAdmins , که در برای آزمایش حذف کرده بودید , بدین ترتیب عمل می کنیم :

Restore subtree OU=PersianAdmins,DC=Admins,DC=ir

سپس در پنجره ظاهر شده Yes را انتخاب کنید.

عکس شماره ۲۳



نکته :

نشانه گذاری کل پایگاه داده و تنظیمات بصورت Authoritative به این نحو انجام می شود :
Restore database

12 - Object مورد نظر با موفقیت نشانه گذاری شد , حال دو مرتبه quit را تایپ و اجرا کنید تا از اعلان ntdsutil خارج شوید.

آموزش پشتیبان گیری از Backup and Restore **Active Directory**

توجه داشته باشید که Object ی همانند OU به همراه تمامی Object های دیگری که در بر دارد مانند گروه ها و کاربرهایش نشانه گذاری می شود.

عکس شماره ۲۴

```
C:\Documents and Settings\Administrator>ntdsutil
ntdsutil: authoritative restore
authoritative restore: restore subtree OU=PersianAdmins,DC=admins,DC=ir

Opening DIT database... Done.

The current time is 10-03-08 12:29.03.
Most recent database update occurred at 10-03-08 11:54.25.
Increasing attribute version numbers by 100000.

Counting records that need updating...
Records found: 0000000002
Done.

Found 2 records to update.

Updating records...
Records remaining: 0000000000
Done.

Successfully updated 2 records.

The following text file with a list of authoritatively restored objects has been
created in the current working directory:
ar_20081003-122903_objects.txt
None of the specified objects have back-links in this domain. No link restore fi
le has been created.

Authoritative Restore completed successfully.

authoritative restore: quit
ntdsutil: quit
C:\Documents and Settings\Administrator>_
```

13 - Domain Controller را شروع مجدد کنید و در حالت عادی اجرا کنید.

در این آموزش با شیوه های مختلف پشتیبان گیری و بازگرداندن آن در Active Directory آشنا شدید , امید است که این آموزش کمک کوچکی برای دوستان و همکاران باشد.

منابع :

Microsoft Technet

کتاب 70-294

کتاب 2279B