

۷ کارنیل، بزرگترین شبکه موفقیت ایرانیان می باشد، که افرادی زیادی توانسته اند با آن به موفقیت برسند، فاطمه رتبه ۱۱ کنکور کارشناسی، محمد حسین رتبه ۶۸ کنکور کارشناسی، سپیده رتبه ۳ کنکور ارشد، مریم و همسرش راه اندازی تولیدی مانتو، امیر راه اندازی فروشگاه اینترنتی، کیوان پیوستن به تیم تراکتور سازی تبریز، میلاد پیوستن به تیم صبا، مهسا تحصیل در ایتالیا، و.... این موارد گوشه از افرادی بودند که با کارنیل به موفقیت رسیده اند، شما هم می توانید موفقیت خود را با کارنیل شروع کنید.

برای پیوستن به تیم کارنیلی های موفق روی لینک زیر کلیک کنید.

[www.karnil.com](http://www.karnil.com)

همچنین برای ورود به کانال تلگرام کارنیل روی لینک زیر کلیک کنید.

<https://telegram.me/karnil>

# **Windows 2003 Server**

## **Beta Version**

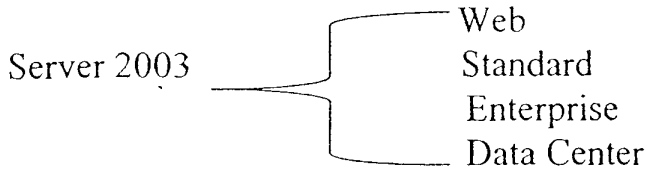
70-290

e-mail : [Niazkhani@yahoo.com](mailto:Niazkhani@yahoo.com)



# Server 2003(Beta)

انواع نسخه های Server2003:



## ۱- Server2003 Web

این نسخه در پلات فورم ۲۰۰۳ نسخه جدیدی میباشد در حالت کلی این نسخه تا ۲ Gb Ram را پشتیبانی میکند و در حالت کلی در صورت پشتیبانی سخت افزار تا ۲ عدد Cpu را بصورت متقارن پشتیبانی میکند و در صورتی که بخواهیم در شبکه Web Server یا Application Server داشته باشیم از نسخه فوق استفاده میکنیم قابل ذکر است این نسخه نمی تواند به عنوان Gateway و یا DHCP سرور و یا Fax سرور در نظر گرفته شود ولی میتواند از طریق امکان RemoteDesktop مدیریت شود. نسخه فوق میتواند عضو Domain شود ولی نمیتواند به عنوان DC در شبکه فعالیت کند. یعنی بعنوان Router نمیتوان از آن استفاده کرد (حالت Router نرم افزارها)

برای کارهای مثل راه اندازی یک web عملکرد بهتری از مدل سرور ۲ دارد چون تعدادی از سرورس ها را ندارد در حدات web بهتر است

نکته:

تعداد کانکشنهای Inbound در یک شبکه توسط این نسخه ۱۰ کانکشن است ولی تعداد کانکشنهای ایجاد شده از طریق Web محدودیتی ندارد. در ارتباط dial up هم بیروت شود؟

## ۲- Server2003 Standard

این نسخه میتواند به عنوان Web Server و Application Server و Mail Server در شبکه فعالیت بکنند در حالت کلی تا ۴ Gb Ram و تا ۴ عدد Cpu را بصورت متقارن بر روی این پلات فورم میتواند وجود داشته باشد. در صورتی که بخواهیم میتوانیم از این نسخه به عنوان DC در شبکه استفاده بکنیم معمولاً از این نسخه در شبکه های محلی استفاده میشود.

- اگر محدودیت سخت افزار من را هم Enterprise بهتر است.

## ۳- Server2003 Enterprise

این نسخه معمولاً در شبکه های Wan استفاده می شود در حالت کلی تا ۲۲ Gb Ram و تا ۸ عدد Cpu را پشتیبانی میکند. قدرت پردازش این پلات فورم در حالت کلی بیشتر از نسخه Standard میباشد.

قابلیت x64 دارد که سرورس در دو نسخه Application و Server دارد که هر کدام هم برای سرورس های ۶۴ بیتی و ۳۲ بیتی کاربرد دارند.

## ۴- Server2003 Data Center

این نسخه در دو ورژن ۳۲ بیتی و ۶۴ بیتی موجود میباشد. نسخه ۳۲ بیتی این پلات فورم در حالت کلی تا ۶۴ Gb Ram و تا ۳۲ عدد Cpu را به صورت متقارن پشتیبانی میکند. اما نسخه ۶۴ بیتی این پلات فورم تا ۲۵۶ Gb Ram و تا ۱۲۸ عدد Cpu را به صورت متقارن پشتیبانی میکند.

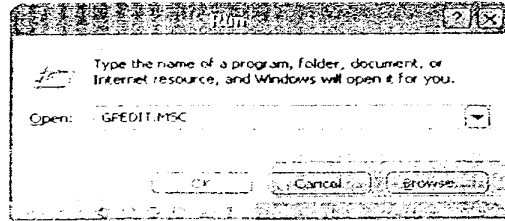
# MICROSOFT Windows

Ram Gb و تا ۱۲۸ عدد-Cpu را به صورت متقارن پشتیبانی میکند. جاهنایی که خواهیم حجم سنگینی از اطلاعات را جایجا بکنیم از این نسخه استفاده میشود.

نکته: `caul computer policy \ Computer Configuration \ Admin... \ system`  
برای پاک کردن صفحه پرسوجوی شات دان بر روی MemberServer باید در Run تایپ کنیم

gpedit.msc مطابق شکل ۱

شکل شماره (۱)

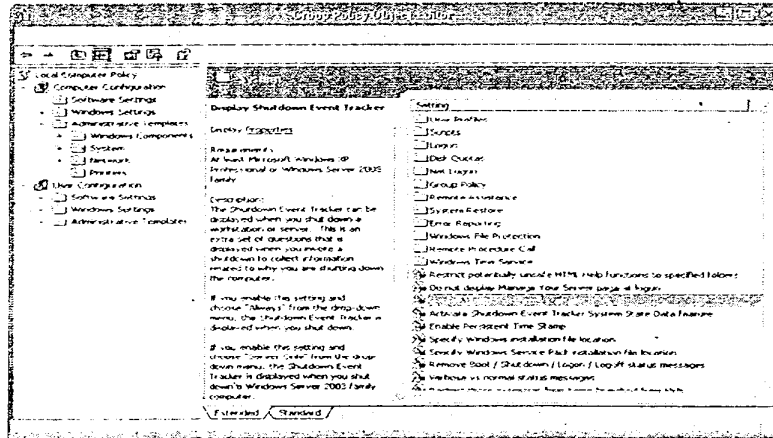


بعد از این کار پنجره ای باز میشود که به آدرس زیر مطابق شکل شماره ۲ رفته و این گزینه را غیر فعال کنید:

`computer configuration \ administrative templates \ system \ display shutdown event tracker`

در properties آنرا Disable میکنیم

شکل شماره ۲



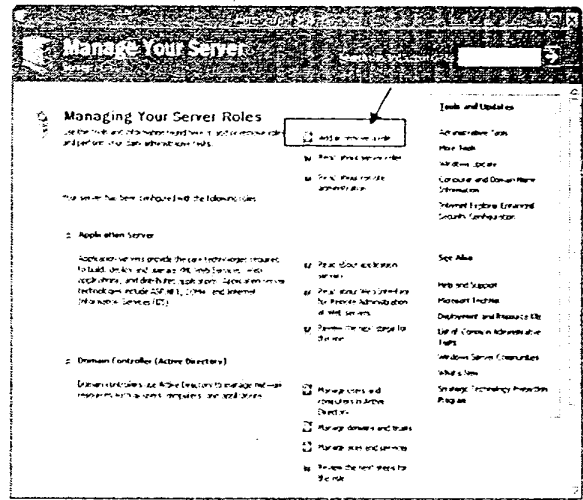
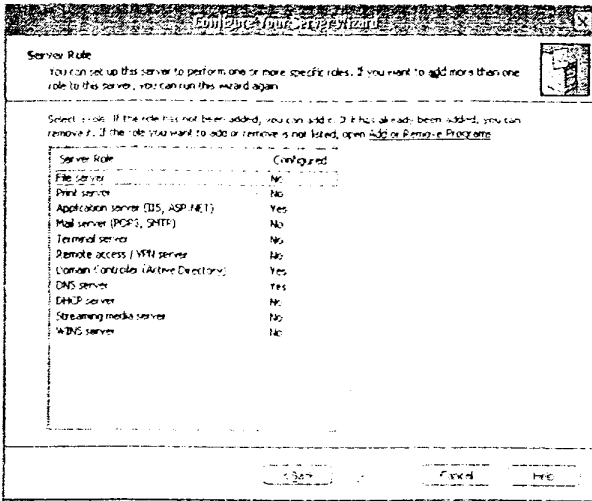
## : File Server

یک سروری است که از طریق آن میتوان امکانی بزای مدیریت فایلها و دسترسی کاربران در درایوهای مختلف را بصورت متمرکز بر روی یک Server برای شبکه خود اعمال بکنیم. برای راه اندازی این قابلیت از طریق Manage your server option در منوی Administrative tools به صورت زیر عمل میکنیم.

Admin...Tools \ Configure your server wizard *File server*

دکمه فولدر را share کرده و از Quota بر حجم آن استفاده میکنیم که این کار File server را برسد

# MICROSOFT Windows



## : Print Server

سیستم عاملی که بر روی آن پرینتر نصب شده و پرینتر مربوطه Share شده باشد میتواند نقش Print Server را برای ما اجراء کند.

توسط پروتکل IPP میتوان به یک پرینتر در اینترنت پرینت فرستاد.

## : Application Server

سروری میباشد که بر روی آن برنامه های تحت Web قرار میگیرد و از طریق سرویس IIS این برنامه در اختیار کامپیوترهای دیگر قرار میگیرد. (Internet Information Service=IIS)

## : Terminal Server

توسط این سرویس میتوان بصورت Remote به یک سرور وصل شده و مدیریت سرور مربوطه را بر عهده بگیریم و یا میتوانیم برنامه ای که تحت شبکه میباشد را از طریق این سرویس اجراء کنیم.

→ درج

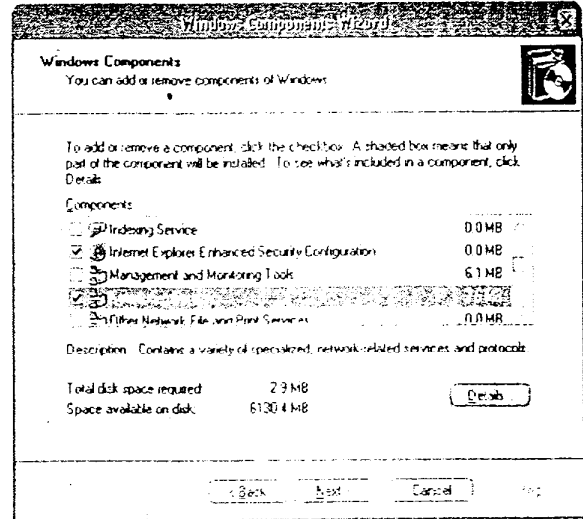
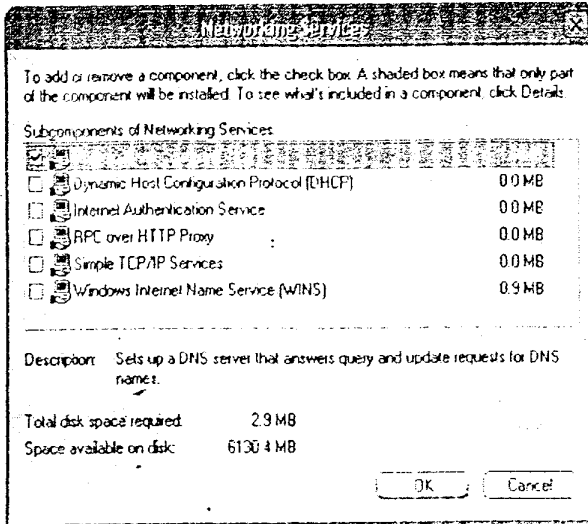
## VPN SERVER \ REMOTE ACCESS (RAS server)

توسط این امکانات میتوانیم بصورت Remote به کاربران مختلف مجوز وصل شدن به شبکه داخلی خود را از خارج بدهیم و یا از طریق VPN ارتباطات امن بین دو نقطه برقرار بکنیم.

## : DNS Server

سروری است که وظیفه آن تبدیل IP به اسم و یا برعکس میباشد.

Mail server = هم به پرینتر از خاص آن را نصب کنیم مثل Exchange


**MICROSOFT  
Windows**


Control Panel – Add \ Remove – Windows Components

### (Dynamic Host Configuration Protocol) : DHCP Server

سروری میباشد که از طریق رنج IP که بر روی آن تعریف میشود به صورت اتوماتیک به کلاینتها IP میدهد ضمناً این سرویس حتماً باید بر روی کامپیوتری که نسخه سرور دارد نصب شود.

Domain Controller

: Active Directory (AD)

هدف AD : (مدیریت مرکزی)

یک ساختار و مجموعه میباشد که بصورت Logical در داخل یک Forest قرار می گیرد. در داخل Forest یکسری Tree (شاخه) وجود دارد و در داخل هر Tree می توانیم یک Domain نصب بکنیم. که از طریق این مجموعه میتوانیم شبکه خود را به قسمتهای مختلف و Domainهای مختلف تقسیم بندی کنیم قابل ذکر است کلیه قوانین موجود در داخل شبکه ما باید در داخل ساختار AD تعریف بشود. در داخل هر Tree یک Domain تعریف می شود، به اولین Domainی که در داخل Forest ما تعریف می شود RootDomain گفته می شود. به Domainهای بعدی که در داخل Treeها ایجاد می شود Child Domain گفته میشود.

: Domain

یک مجموعه Logical میباشد که در داخل آن منابعی از قبیل کامپیوترها و کاربران و پرینترها تعریف می شود.

سه اصل مهم برای نصب AD و تبدیل کامپیوتر به DC: Server

۱- IP کامپیوتر بصورت استاتیک و دستی وارد شود.



my computer \ properties \ computer name \ change

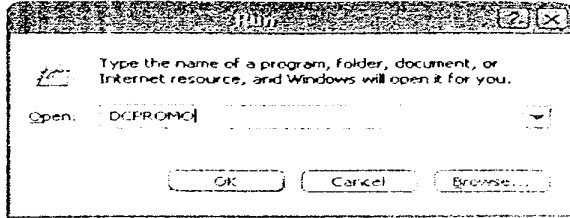
۲- اسم کامپیوتر مشخص و با معنی باشد که خودمان وارد کرده باشیم. در این قسمت روحت wg است.

۳- برای نصب AD وجود سرویس DNS الزامی است. و IP تحت server DNS preferred را دارد تا اسم که در هنگام نصب AD عرض شد را کند که آیا میفرهید DNS راهم لقب کنیم؟ -

آدرس IP مربوط به DNS راهم می دهیم در اینجا.  
IP همان server: ۱۷۲.۱۶.۰.۱

مراحل تبدیل کامپیوتر به DC:

در Run تایپ کنید Depromo و پنجره ای باز میشود برای نصب AD.



دو گزینه New Domain و Additional داده میشود که اولی برای نصب AD و تبدیل کامپیوتر به DC است و دومی برای زمانی که بخواهیم از DC موجود خود یک DC پشتیبان ایجاد بکنیم. (روزها سیتر اینگر)  
بعد از انتخاب نصب DC گزینه Domain in a new forest را زده و صفحه بعدی اسم DNS را برای Domain باید انتخاب کنیم به عنوان مثال Microsoft.com

### NET BIOSE NAME

فورمت نام گذاری قدیمی ماکروسافت است که این اسم از ۱۶ کاراکتر تشکیل میشود که ۱۵ تای آن را کاربر انتخاب میکند و آخرین کاراکتر را خود سیستم اضافه می کند.

Sysvol: این فولدر share و رانج DC ها استفاده می کنند و نه client ها.

به هنگام نصب AD فولدری بر روی کامپیوتر DC ایجاد میشود که این فولدر بصورت پیشفرض Share میباشد و قابل ذکر است محل این فولدر باید حتماً در پارتیشن NTFS5 باشد. این فایل حاوی سیاستهای کلی تعریف شده در داخل ساختار AD می باشد، DCها برای اینکه بتوانند با یکدیگر Replication انجام دهند از این فولدر استفاده میکنند.

مرحله بعد نصب کردن سرویس DNS است در این مرحله به دو صورت میتوان عمل کرد حالت اول از سیستم بخواهیم به صورت اتوماتیک این کار را انجام دهد حالت دوم قبل از نصب AD سرویس فوق را به صورت دستی بر روی کامپیوتر نصب بکنیم. ولی وجود DNS برای نصب AD الزامی است.  
مرحله بعدی انتخاب کلاینتهایی که با Server ما ارتباط برقرار میکنند است که گزینه اول برای پلاتفرم های قبل ۲۰۰۰ و دومی برای پلاتفرم های ۲۰۰۰ و ۲۰۰۳ را ساپورت می کند.



در مرحله بعد کاربر باید Password ی را وارد بکند که در زمان Backup گیری و Restore کردن مورد استفاده قرار می گیرد.

**نکته Depromo :** حذف AD

این فرمان بصورت یک کلید دو حالتی عمل می کند یعنی در صورتی که سرویس AD بر روی کامپیوتر نصب نباشد سرویس فوق را نصب میکند و در صورت نصب بودن سرویس فوق را پاک می کند.

**Gpupdate** : فرمانی است که برای Refresh کردن تمامی اعمالی که در داخل Domain,DC انجام شده به کار می رود. *policy را Refresh می کند (مراد از جریبها نمیکنیم)*  
Gpupdate /force

**Ou** : یک مجموعه مدیریتی و مستقل و کوچکتر از Domain می باشد که می توان مدیریت آن را به یک و یا چند نفر واگذار کرد و حدود و اختیارات خاصی را برای آن در نظر گرفت و می توان در داخل آن کاربران, پرینترها و کامپیوترهای مختلف تعریف بکنیم.

**Site** : یک مجموعه ای از Subnet ها می باشد و در حالت کلی هر Subnet توسط یک Router از همدیگر جدا میشوند. هدف تعریف سایت برای راحتتر و سریعتر Replicate کردن اطلاعات می باشد.

**Domain controller**

به هنگام نصب AD یک Ou یی به این نام در داخل کنسول بصورت پیش فرض ایجاد می شود, در صورتی که بخواهیم قوانین موجود بر روی DC خود را تعریف بکنیم با رایت کلیک کردن و Properties گرفتن از این Ou در قسمت Group Policy سیاستهای خود را تعریف می کنیم.

**Group policy**

قسمتی است که در آن قوانین موجود بر روی کامپیوترها و کاربران خود را تعریف میکنیم این کار هم بر روی Domain و هم بر روی Ou و هم بر روی Site قابل تعریف می باشد یک Group Policy در حالت کلی از دو قسمت تشکیل شده است :

۱- Computer Configuration

۲- User Configuration

Site : قسمت های سایت را از هم جدا میکند و محدودیت بر این است که یک user فقط در DC احوال در ضمن خود در  
Active Directory  
Add کردن site در MMC



نکته: در صورتیکه یک policy مستعمل بر روی Domain, Site و OU تعریف شده باشد. بنا بر این policy که در قسمت OU تعریف می گردد بر موارد قبلی override خواهد کرد اما در صورتیکه به طور مثال بر روی سایت و policy تعریف گردد و بر روی Domain و OU NOT Configured انتخاب گردد و policy که بر روی Site تعریف شده است اعمال خواهد شد.

↓  
 در حالتی که OU و Site  
 در حالتی که OU و Site

□ Block policy inheritance

با انتخاب گزینه فوق بر روی Domain و OU موارد تعریف شده بر روی Parent بالا دست به ارث نمی برد.

با انتخاب گزینه -- no override: prevent از option در Group policy بر روی Domain, Site و یا OU موارد تنظیم شده بر روی پاترن دست حاصل خواهد شد حتی اگر Level 3 پاترن دست گزینه Block policy inheritance را انتخاب کرده باشند.

\* در تعریف policy ها اعتبارات صید و منابع مختلف ایجاد و بنا را دست بندی نمودند. Application یا security -- در ادامه در مدیریت آنها بتوان هرگونه را به تنهایی Disable و یا no override نمود.

\* برای اعمال تغییرات در policy حتما باید gpupdate را در Run اجرا نمود در بعضی مواقع که با این دستور policy اعمال نشدند / Force نیز می توان اجزای مختلف را به وسیله gpupdate /target:Computer می توان فقط قسمت Computer را اعمال و user را اعمال نکرد.

\* نکته: در صورتیکه بخواهیم یک policy برای کاربران مختلف اعمال گردد باید کاربر مربوطه مجوز Read و Apply group Policy را داشته باشد.

به تمام user هایی که در شبکه Domain وارد می شوند Authenticated users گفته می شود.

اگر بخواهیم به یک user این Group Policy ها اعمال شود در قسمت Security Properties Group Policy در Add, user شده و Apply Group Policy یا Deny می کنیم.

\* با استفاده از Group Policy management Console می توان effective policy ها را بر روی user یا ...

# Windows

گزینه شماره ۱ قوانین مربوط به کامپیوتر را میتوان اعمال کرد و در گزینه شماره ۲ قوانین مربوط به کاربران را ریف میکنیم ، بعد از تعریف کردن قوانین مختلف در این مرحله با فرمان Gpupdate قوانین تعریف شده بر روی کامپیوتر ها و Domain ها و یا DC ها اعمال میشود.

نکته: استثنا ، کدی موارد تعریف شده در باره Account policy فقط بر روی Domain

قابل تعریف می باشد (برای کاربر ما هم قابل تعریف است ولی عمل نمیکند)   
 user configure   
 computer configuration

\* اگر بر روی Properties ، policy در سمت چپ General tab آن دو گزینه وجود

دارد که برای این است که اگر در Computer صلاحیت جج اعمالی صورت نگیرد آنرا Disable کنیم و بالعکس که باین کار سرعت کامپیوتر بیشتر می شود.

برای آنکه برای یک user خاصیت وارد شدن به server داشته باشد باید ابتدا user در Domain

در Domain Controller و پنجره properties گرفته در تب Group policy ، Group Edit

گرفته در تب Local policies > security settings > windows settings > Computer Config > user rights Assignment > Allow log on locally > Add user: Distinguished Name

سطح این فرمت آدرس دهی می توانیم به Object های داخل AD اشاره بکنیم. برای استفاده از این نوع آدرس می از پارامترهای DC و OU و CN استفاده میشود. در این فرمت اسم و قسمت دوم Domain را با DC و

OU را با پارامتر OU و بقیه Object ها را با Cn مشخص می کنیم. به طور مثال کاربری به اسم Ali در داخل Microsoft.com در MCSE

در صورت زیر مطرح میشود.   
 CN = Ali   
 OU = MCSE   
 DC = Microsoft, DC = COM

و یا   
 CN = Test, OU = MCSE , DC = Microsoft, DC = COM

توابع فرمان های موجود در سرور ۲۰۰۳:

فرمان dsadd   
 D:\> dsadd /?

سطح این فرمان می توانیم در داخل Ad پارامتر و یا Object ی را اضافه و ایجاد نماییم.

/? Help   
 dsadd user /?

dsadd user Cn = xxxxx , Ou = MCSE , dc = Microsoft, DE = COM

Dsadd OU ou = IT, DC = Microsoft, DC = COM

مانند Dsget   
 > netdom



## فرمان Dsget

توسط این فرمان می توانیم مشخصات و خواص یک object را مشاهده نماییم.

### فرمان Dsmod:

توسط این فرمان مشخصات obj ها قابل تغییر می باشد.

### فرمان Ds move:

این فرمان می تواند obj را از یک محل در داخل ساختار Ad به محل دیگر در ساختار AD با فرمت آدرس دهی DN (Distinguished Name) منتقل کرد.

### فرمان Dsrm:

این فرمان obj ها را می تواند در یک ساختار درختی از یک محل به محل دیگر منتقل نماید. (برای منتقل کردن)

### فرمان Dsquery:

توسط این فرمان می توانیم لیست obj های موجود در داخل AD را مشاهده کرده و گزارشی از obj های مربوطه تهیه بکنیم.

```
dsquery user dc = Microsoft, dc = com
dsquery user ou = It, dc = Microsoft, dc = com
dsquery ou dc = Microsoft, dc = com
```

```
user CN=user,dc=bbc,dc=com
```

### فرمان Csvde:

توسط این فرمان می توانیم کلیه obj های خود را در داخل یک فایل text ، Export کرده و در مواقع ضروری obj های خود را در داخل ساختار AD ، import نماییم . نحوه Export کردن به صورت زیر میباشد:

```
Csvde -f d:\filename.txt
```

این فرمان در داخل Excel براحتی قابل ویرایش می باشد.

نحوه Import کردن این فایل به صورت زیر می باشد:

```
Csvde -i -f d:\filename.txt
```

```
DN, object class, name, User Account Control,
Sam Account Name, Display Name, User principal name
"CN = user 12, Ou = MCSE, DC = Microsoft, DC = com"
user, user 12, 514, user 12, a12 b12 c12, user 12@ Microsoft.com
```

### فرمان Ldifde:

این فرمان همانند فرمان csvde می باشد. توسط این فرمان می توانیم کلیه obj های خود را در داخل یک فایل متنی export کرده و در مواقع خاص می توانیم فایل مورد نظر را در داخل AD ، import نماییم. قابل ذکر است که این فایل در داخل word براحتی قابل ویرایش می باشد.



```

ldifde -f C:\lmcse.txt ←
dn:CN = user 14, ou, mcse, Dc = Microsoft, DC = com
object class : user
display name: a14 b2 c2
name: user 114
user Account control: 514
Sam Account Name: user 114
User principal name: user 114@ Microsoft
و به صورت زیر قابل Import شدن می باشد:
ldifde -i -f C:\name.txt

```

با این فرمان متن بصورت فایل word می باشد.

فرمت آدرس دهی **user principle name** :

این فرمت آدرس دهی همانند فرمت آدرس دهی استفاده شده در Email می باشد و معمولاً در داخل یک forest برای مشخص کردن اینکه کاربران مربوطه قصد login کردن به کدام domain را دارد استفاده می شود.

Corlos @ Microsoft.com

user principlename: name@domain nam

براصل فرلدر sysvol Replicate کلترس DC ها.

### FRS: (File Replication Services)

این سرویس وظیفه Replication بین DC های مختلف در شبکه را به عهده دارد. این سرویس بصورت اتوماتیک بر روی ویندوز سرور نصب می باشد. بر روی member سرورها و standalone سرور ها بصورت دستی باید سرویس فوق start نماییم.

عملیات Replication بین DC ها توسط تکنولوژی انجام می گیرد که اصطلاحاً به این تکنولوژی kcc یا (KnowledgeConsistencyChecker) گفته می شود. در این نوع تکنولوژی از ساختار Ring برای Rep بین DC ها استفاده می شود. قابل ذکر است که در این ساختار دو مسیر مختلف برای فرستادن اطلاعات بین DC ها را انجام دهد.

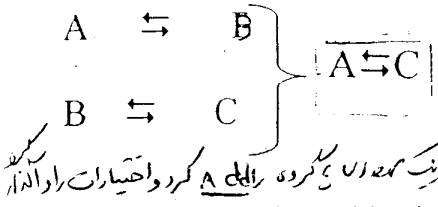
program\Admin-- Tools\Domain and Trust

Trust (اعتماد) :

اطمینان سازی بین دو گروه کاری را گفته می شود توسط این امکان می توانیم با اعتماد سازی بین Domain ها مختلف مجوز استفاده از Domain های مختلف را از منابع یکدیگر فراهم نماییم در صورتیکه Domain مانند x به Domain مانند y ، Trust نماید. کاربران Domainy می توانند از منابع موجود بر روی DomainX

# MICROSOFT Windows

استفاده نمایند. قابل ذکر است با ایجاد Trust بین Domain های مختلف امکان ارتباط بین Domain های مختلف فراهم می شد که در پلات فرمهای 2000 به بعد بصورت اتوماتیک بین Domain های یک forest یک Trust دوطرفه ایجاد می شود ولی در NT4 مجبور بودیم بصورت دستی این کار را انجام دهیم در پلات فرمهای 2000 به بعد در صورتی که Domain A با B Trust ، ایجاد نماید B با C Trust ، ایجاد بکند بصورت پیش فرض A با C Trust ایجاد می کند به این قابلیت ، قابلیت Transitive گفته می شود.



را از آن کردن

## Delegation: روی او کلیک راست را زده و در Delegation Control و سران نت هم روی او کلیک کرده و گزینه را در اختیار او گذار

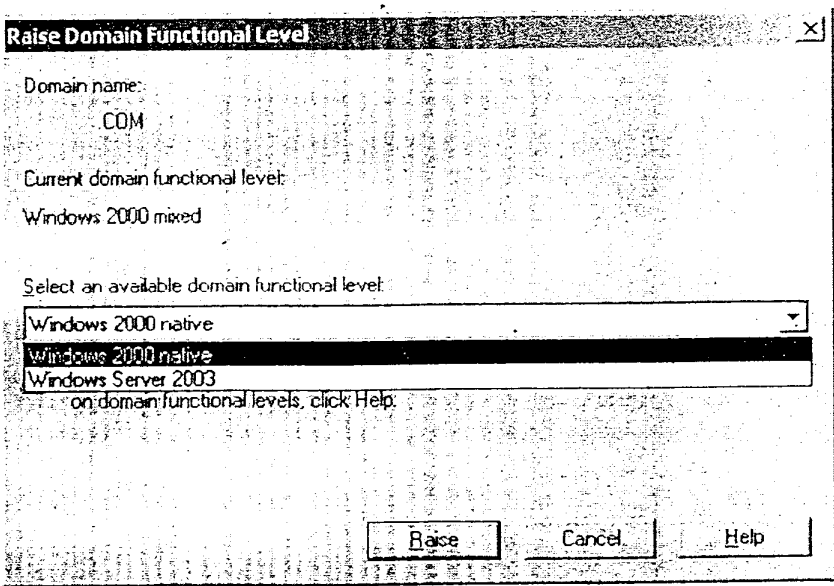
توسط این امکان می توانیم مسئولیت موجود بر روی یک Domain و یا یک ou را به کاربر های مختلف واگذار نماییم. برای این کار کافیست که بر روی او و یا Domain مختلف رفته و با راست کلیک کردن و انتخاب گزینه Delegate control مجوزهای لازم را به کاربران مختلف برای مدیریت قسمتهای تعیین شده مشخص نماییم.

## GUID (Globally unique ID): که ۱۲۸ بیتی است

Object های موجود در داخل ساختار AD و یا به عبارت دیگر obj های موجود در داخل یک Domain از یک کد منحصر بفرد استفاده می کند قابل ذکر است که قسمت اول هر GUID در داخل یک Domain یکسان می باشد ولی نسبت به یک Domain دیگر متفاوت می باشد این قضیه در کامپیوترهای local توسط پارامتری به نام SID مشخص می شود.

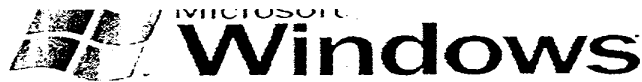
## Site

در صورتی که بخواهیم بصورت فیزیکی شبکه خود را از قسمتهای مختلف جدا نماییم از این امکان استفاده می نماییم. در حالت کلی یک سایت مجموعه ای از subnet ها می باشد و هر subnet توسط یک رنج IP و یا یک Router از یکدیگر جدا می شود. معمولاً هدف از تعریف site برای راحت و سریعتر Replicate کردن اطلاعات می باشد.



## انواع Domain Functional Level

به هنگام نصب AD بر روی پلات فرمهای ۲۰۰۳ می توانیم چهار Level برای Domain های 2003 در نظر بگیریم.



۱- Windows 2000 mixed

در صورتی که Domain ما بر روی این مد قرار گرفته باشد در شبکه میتوانیم DC های NT4 ، 2000 ، 2003 داشته باشیم بصورت پیش فرض Domain های 2003 بر روی این مد قرار دارند.

۲- Win 2000 Native

در صورتی که Domain 2003 ما بر روی این مد قرار گرفته باشد در شبکه فقط DC های 2000 و 2003 می توانید داشته باشید.

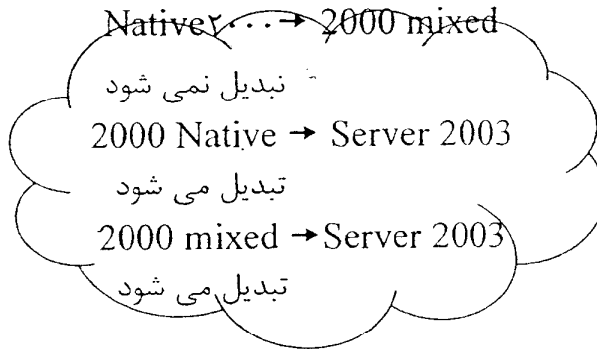
نکته :

در این حالت کلاینت های NT4 می توانند عضو Domain باشد ولی نمی تواند DC باشد.

۳- Server 2003: بهترین در زمینه این Level است و در صورتی که در این حالت عملکرد و قابلیت ها بهتر است در این مد فقط DC های 2003 می توانند در شبکه فعالیت نمایند.

۴- Windows server 2003 Interim

در صورتی که بخواهیم در شبکه فقط DC های NT4 ، 2003 وجود داشته باشند از این مد استفاده می کنیم.



نکته:

در حالت کلی کاربران از پشت DC نمی توانند به صورت Local به DC login نمایند برای اینکه به کاربران چنین مجوزی بدهیم باید در قسمت GP موجود بر روی DC مجوز لازم را به کاربر مربوطه بدهیم.  
Group policy

Global catalog

در داخل هر forest پایگاه داده ای می باشد که در داخل آن همه object های موجود به همراه مشخصات آن در داخل این پایگاه داده قرار می گیرد به طور مثال در صورت ایجاد کاربری بنام test همه مشخصات کاربر فوق در داخل این پایگاه داده قرار می گیرد. اصطلاحاً به سروری که این پایگاه داده بر روی آن قرار می گیرد GlobalCatalog سرور گفته می شود. قابل ذکر است که تعداد این سرور ها در داخل یک forest متغیر می باشد.

- Active Directory site and service
- + Sites
- + Default first - site - name
- + Servers
- + www1
- + NTDS settings \ properties

- اولین DC پسوان Global catalog است که می توان یک سرور داشت

- محل این پایگاه داده در سرور ویندوز NTDS است

- اگر عمل DC ها با هم فاصله زیاد دارد بهتر است که در هر محل یک Global catalog داشته باشیم تا سرعت عملکرد بالاتر برود.

# Windows

## Profile های نرم افزاری

### ۱- Local Profile

بهنگام ایجاد کاربر در صورتی که برای کاربران در قسمت پروفایل مسیری تعیین نشده باشد در داخل پارتیشن که ویندوز ما قرار دارد در فولدر Documents And Settings به اسم کاربر یک فولدر ایجاد میشود که در داخل این فولدر پروفایل کاربر وجود دارد که به این پروفایل LocalProfile گفته می شود. قابل ذکر است کاربرانی که بصورت Local بر روی کامپیوتر Login می کنند پروفایل آنها از داخل فولدر مربوطه Download شده و در اختیار کاربر قرار می گیرد و به هنگام Shutdown کردن تغییرات ایجاد شده در داخل این فولدر Upload می گردد.

نکته:

در داخل فولدر Documents And Settings فولدري وجود دارد تحت عنوان All Users مواردی که در داخل این فولدر ذخیره می گردد برای همه کاربران اعمال می گردد در صورتی که بر روی این فولدر گروههای مختلف را محدود بکنیم گروههای فوق از موارد Default تعریف شده در این قسمت نمی توانند استفاده بکنند.

### ۲- Roaming Profile

در این نوع پروفایل در قسمت Properties کاربر مسیر مشخص شده ای برای Download کردن پروفایل کاربر در شبکه مشخص می گردد قابل ذکر است پروفایل کاربر مربوطه از محل مورد نظر در شبکه Download شده و در اختیار کاربر قرار می گیرد. در این حالت یک مدیریت مرکزی برای کلیه پروفایل های کاربران ایجاد می گردد و کاربران از هر جای شبکه بخواهند وارد شبکه شوند مسیر مشخص شده ای برای پروفایل های کاربران در نظر گرفته می شود.

نکته:

به هنگام تعریف Roaming پروفایل در پلاتفرم های ۲۰۰۳ فقط تغییرات انجام شده را بر روی پروفایل کاربر به محل اصلی Upload می شود این عمل از بالا بردن ترافیک شبکه جلوگیری می کند.

## طریقه ساخت یک Roaming Profile

یک کاربر ایجاد می کنیم بعد قبل از آنکه با آن کاربر Login کنیم یک فولدر میسازیم و آن را Share میکنیم. در قسمت User Profile در محل Profile Path آدرس فولدري که Share شده را می دهیم و بعد از این کار Login کرده و پروفال در فولدر مربوطه ایجاد می شود.

### ۳- Mandatory Profile

وقتی دار user میزنیم از این بابت تعریف میکنیم  
shot down

۱۲

windows setting security setting \local policy\user right  
shot down the system  
برای دارن مجب shot Down بهر کسی که خراب سیستم را کرده است  
در آن client اجبار میکنیم  
G-pupdate / Force

**Table 4-1 Group Scope and Allowed Objects**

Group Scope	Allowed Objects
<b>Windows 2000 native or Windows Server 2003 functional level domain</b>	
Domain Local	Computer accounts, users, global groups, and universal groups from any forest or trusted domain. <i>Members</i> Domain local groups from the same domain. <i>Members اول دریا</i> Nested domain local groups in the same domain. <i>Member of</i> <i>دسته Nested دریا</i>
Global	Users, computers and global groups from same domain. Nested global (in same domain), domain local, or universal groups. <i>Members of</i>
Universal	Universal groups, global groups, users and computers from any domain in the forest. Nested global, domain local, or universal groups.
<b>Windows 2000 mixed or Windows Server 2003 interim functional level domain</b>	
Domain Local	Computer accounts, users, global groups from any domain. <i>Member of</i> <i>دسته</i> <i>Member</i> <i>دسته</i> Cannot be nested. <i>نمی تواند</i>
Global	Only users and computers from same domain. Cannot be nested.
Universal	Not available.

### Special Identities

There are also some special groups called *special identities*, that are managed by the operating system. Special identities cannot be created or deleted; nor can their membership be modified by administrators. Special identities do not appear in the Active Directory Users And Computers snap-in or in any other computer management tool, but can be assigned permissions in an ACL. Table 4-2 details some of the special identities in Windows Server 2003.

**Table 4-2 Special Identities and Their Representation**

Identity	Representation
Everyone	Represents all current network users, including guests and users from other domains. Whenever a user logs on to the network, that user is automatically added to the Everyone group.
Network	Represents users currently accessing a given resource over the network (as opposed to users who access a resource by logging on locally at the computer where the resource is located). Whenever a user accesses a given resource over the network, the user is automatically added to the Network group.
Interactive	Represents all users currently logged on to a particular computer and accessing a given resource located on that computer (as opposed to users who access the resource over the network). Whenever a user accesses a given resource on the computer to which they are logged on, the user is automatically added to the Interactive group.





# Windows

## انواع Built-in Global Group

- 1- **Domain Users** : کاربرانی که بر روی Domain ایجاد می شوند به صورت پیش فرض عضو این گروه خواهند بود. *نویس users در xp است که وقتی ایماکس کنیم عضو این گروه هستند.*
  - 2- **Domain Admins** : کاربرانی که عضو این گروه می باشند می توانند Admin یک Domain باشند. *Global*
  - 3- **Enterprise Admins** : یک گروه Universal می باشد، زمانی که Domain ما در حالت Mixed2000 و یا Interine باشد این گروه عضو Global می باشد. زمانی که Domain ما به 2000 Native و یا Server2003 تبدیل می شود این گروه از Global تبدیل به Universal می شود. زمانی که بخواهیم به یک Administrator به بیش از یک Domain برای مدیریت منابع Domainها مجوز دهیم از این گروه استفاده می کنیم. *سی سریت hald ها های زیر مجوز را هم بدست گیرد.*
- معمولاً در یک Forest اولین Domainی که ایجاد می شود چنین گروهی بر روی Domain ما ایجاد میشود.

Name	Type	Description
Administrator	User	Built-in account for admini...
Cert Publishers	Security Group ...	Members of this group are...
DnsAdmins	Security Group ...	DNS Administrators Group
DnsUpdateProxy	Security Group ...	DNS clients who are perm...
Domain Admins	Security Group ...	Designated administrators...
Domain Computers	Security Group ...	All workstations and serve...
Domain Controllers	Security Group ...	All domain controllers in th...
Domain Guests	Security Group ...	All domain guests
Domain Users	Security Group ...	All domain users
Enterprise Admins	Security Group ...	Designated administrators...
Group Policy Creator Owners	Security Group ...	Members in this group can...
Guest	User	Built-in account for guest ...
HelpServicesGroup	Security Group ...	Group for the Help and Su...
IIS_WPG	Security Group ...	IIS Worker Process Group
IUSR_	User	Built-in account for anony...
IWAM_	User	Built-in account for Intern...
RAS and IAS Servers	Security Group ...	Servers in this group can ...
Schema Admins	Security Group ...	Designated administrators...
SUPPORT_388945ad	User	This is a vendor's account ...
TelnetClients	Security Group ...	Members of this group ha...

یعنی اگر بخواهیم که Domain به منابع client دسترسی نداشته باشد؟  
 به Domain Admins دسترسی داریم. Admin با سیدت local یا client را حذف کنیم و user ها client را تغییر دهیم.  
 نکته:

گروه های ذکر شده در بالا به صورت پیش فرض هیچ مجوزی را ندارند این گروهها با عضویت در گروههای Local دیگر مجوز می گیرند، به طور مثال Domain Admin عضو گروه Local Administrator یک گروه می شود، قابل ذکر است زمانی که یک ویندوز XP را عضو Domain میکنیم Adminهای Domain به عنوان Administrator ماشین XP می تواند عمل بکند.

### Computer Account ✓

زمانی که کامپیوترها عضو Domain می شوند در داخل کنسول Add users and computers در داخل این کنسول فولدری به نام Computers وجود دارد به اسامی کامپیوترهای عضو Domain شده یک Account به اسم کامپیوتر مربوطه ایجاد می شود. برای ایجاد یک ComputerAccount در داخل DC حتماً باید عضو دو

- گروه Administrator و یا Account Operators باشیم.
- هر user که می خواهد در DC متصل شود، *از یک کامپیوتر* Computer Account می خواهد. *بخودش* *9x*
- برای اینکه یک کامپیوتر به Domain وصل شود باید در client در دست *Change* *My computer \ properties \ computer name*
- نام کامپیوتر در *Domain* را بزنیم.
- user می تواند در client سرانبراین کار را کند.

# Windows

در حالت عادی در صورتی که عضو دو گروه فوق باشیم ، می توانیم computerAccount های دلخواه خود را در داخل DC ایجاد نماییم. قابل ذکر است در صورتی که از پشت کلاینتهای win 9x به یک <sup>Domain</sup> login نماییم کامپیوتر Account برای این پلاتفرم ها در داخل AD ایجاد نمی شود.

\* از طریق فرمانهای dsadd و Netdom می توانیم computer Account در داخل Ad ایجاد نماییم.

در حالت کلی برای اجرای فرمان Netdom باید از روی CD 2003 در داخل support \ tools \ suptools. ms<sub>i</sub> را بر روی کامپیوتر اجرا بکنیم.

> DSADOL computer cn=kk,ou=it,dc=bbe,dc=com

\* برای اجرای فرمانهایی از قبیل Netdom و فرمانهای دیگر باید فایل suptools.msi بر روی DC نصب گردد.

> Netdom ADD computerName /domain:DomainName /user:Administrator /password:userpassword[/ou:OUDN]

نکته:

**computer Account** می توانند برای نصب RIS : Remote Installation Services در شبکه مورد استفاده قرار گیرد.

نکته : فقط در کامپیوتر DC در باکس ACL علاوه بر ADD کردن گروهها و کاربران می توانیم ComputerAccount نیز اضافه کرده و محدودیتهای خاصی را برای computerAccount های شبکه خود ایجاد نماییم. این امکان در پلاتفرم NT موجود نمی باشد.

## نکته های Computer Account

- 1- در صورتی که یکی از computer Account های ما در صورت وجود نتواند به DC ، login نماید، باید Account مربوطه در داخل AD یکبار Reset شود.
- 2- در صورتی که کلاینت عضو Domain شود و کامپیوتر Accounty در داخل AD به اسم computer مربوطه ایجاد شود در صورت Disable کردن این Account ، Account مربوطه بصورت موقت غیرفعال می شود.
- 3- در صورتی که کامپیوتری قبلاً عضو Domain شده باشد و Accounty در داخل AD به اسم computer مربوطه ایجاد شده باشد در صورتی که بخواهیم کامپیوتر مربوطه را از عضویت Domain خارج کنیم و بعد از خارج کردن Account مربوطه از داخل AD پاک نشود باید بصورت دستی این کار انجام گیرد.

Share folder ها :

# Windows

۲- برای محدود کردن منابع موجود بر روی پارتیشن های FAT برای استفاده کاربران شبکه تنها راه استفاده از sharepermission ها می باشد ولی برای منابعی که بر روی پارتیشنهای NTFS قرار دارند می توانیم از اشتراک share permission و NTFS Permission استفاده نماییم.

۲- SharePermission ها فقط بر روی منابع شبکه و یا منابعی که از طریق clientforMicrosoftNetworks در محیط شبکه قرار می گیرد اعمال می شود از این مجوزها نمی توانیم برای منابعی که از طریق پروتکل Http برای web browser ها اتفاق می افتد اعمال بکنیم.

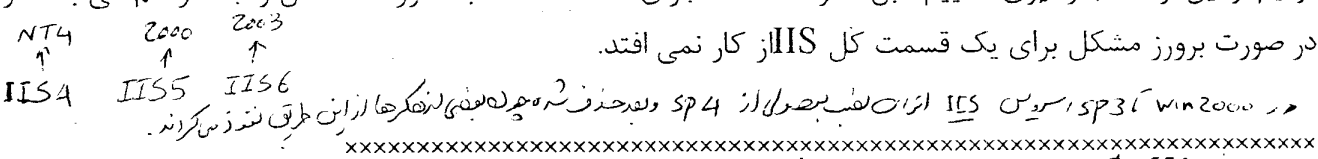
## Sharefolder ها:

بعد از به اشتراک گذاشتن منابع موجود در شبکه می توانیم از طریق computer management در قسمت sharefolder بر روی منابع خود properties گرفته و در تب publish منابع موجود را در داخل AD publish می نماییم. بعد از publish کردن منابع موجود در داخل AD قابل دسترسی می باشند.  
نکته: منابع share در publish کردن در AD در بک گراند در پنجره open file در شبکه را نشان می دهد.  
در پلاتفرم های ۲۰۰۰ و XP در صورتی که کاربر Object ی را بر روی کامپیوتر ایجاد بکند مالک آن می باشد و Administrator و یا کسی که مجوز Take Owner Ship داشته باشد می تواند مالکیت را از کاربر مربوطه گرفته (Take Owner Ship) ولی نمی تواند را به کاربر دیگری واگذار بکند اما در Server 2003 می توان مالکیت را از کاربری گرفت و به کاربر دیگر و یا بعد به خود کاربر داد اصطلاحا گفته می شود می توان عمل Give Owner Ship انجام داد.

publish منابع share در یک کامپیوتر local را در اختیار AD قرار می دهد.  
Server می تواند قابلیت Give ownership داشته باشد و در تب Admin می تواند Give ownership کند در صورتی که در تب take در آنجا باشد.  
\* وقتی پرینتر را نصب کنیم بصورت اجزای Publish است و اگر بخواهیم از Publish خارج کنیم روی لبه share تیک  list in the directory را برمی داریم. (پرینت صفحه ۱۵)

## IIS (Internet information service)

توسط این سرویس که بصورت پیش فرض در server 2003 نصب نمی باشد می توانیم در داخل شبکه خود web server و یا FTPserver راه اندازی نماییم. قابل ذکر است در صورتی که server 2000 خود را که بر روی آن سیستم IIS نصب می باشد (IIS5) را به سرور 2003 ارتقاء نماییم IIS5 به IIS6 ارتقاء پیدا می کند و ما نمی توانیم از این ارتقاء جلوگیری نماییم. قابل ذکر است که اجزای مختلف IIS6 به صورت مستقل و جدا از هم می باشند در صورت بروز مشکل برای یک قسمت کل IIS از کار نمی افتد.



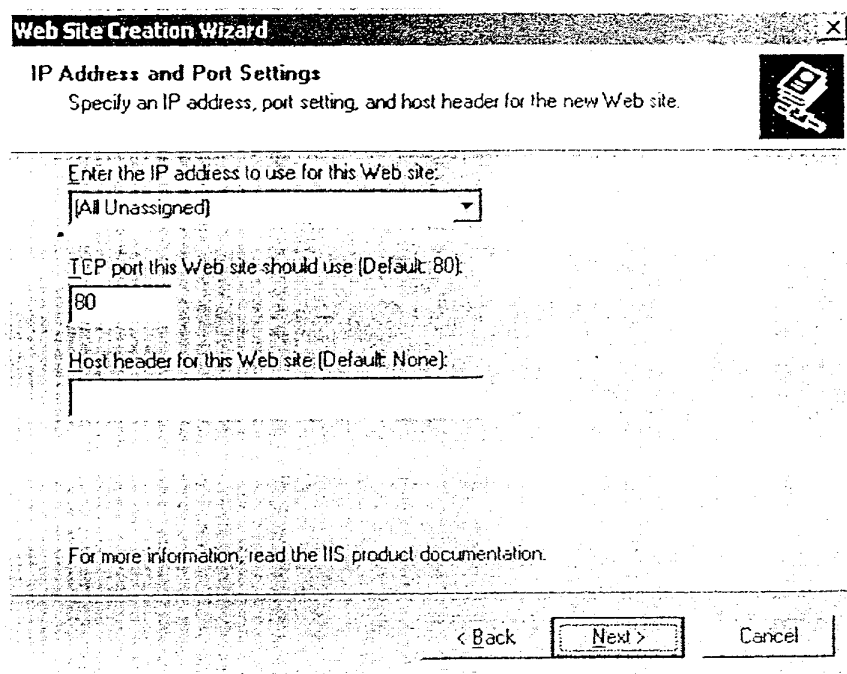
برای نصب IIS در Component Add/Remove در تب  FTP service  
 Internet Printing  
 IIS  
که اینها در Application server هستند در details هستند



# Windows

Website → New → website

بهنگام ایجاد website در داخل سیستم IIS در قسمت IP Address and port settings می توانیم IP سایت مورد نظر خود را به همراه port مربوطه و در صورت نیاز سایت مربوطه را مشخص کنیم معمولاً میتوانیم بر روی یک IIS چندین site داشته باشیم.



**Web Site Creation Wizard**

**IP Address and Port Settings**  
Specify an IP address, port setting, and host header for the new Web site.

Enter the IP address to use for this Web site:  
[All Unassigned]

TCP port this Web site should use (Default: 80):  
80

Host header for this Web site (Default: None):  
[ ]

For more information, read the IIS product documentation.

< Back    Next >    Cancel

برای اینکه بهنگام وصل شدن به web site های مختلف بر روی IIS مشکلی پیش نیاید می توانیم برای هر سایت یک IP منحصر بفرد اختصاص دهیم و یا از طریق port تعریف شده در صورتی که IP دو سایت یکی بود این تفکیک را قائل شویم در صورتی که برای دو سایت IP و Port های ما یکسان باشد میتوانیم از طریق Host header سایت های مختلف را از یکدیگر تفکیک نماییم.

## Web Site

در این قسمت IP سایت مورد نظر را به همراه Port و در صورت نیاز Host Header سایت مورد نظر خود را وارد می کنیم. معمولاً برای قرار دادن چند سایت بر روی یک IIS برای اینکه به هنگام برقراری ارتباط مشکلی پیش نیاید می توانیم به هر سایت یک IP منحصر به فرد اختصاص دهیم و یا به هر سایت یک پورت منحصر به فرد و یا در قسمت Host Header در صورتی که IP و پورت سایت های ما یکسان باشد سایت های خود را از همدیگر مجزا نمود.

## قابلیت های دیگر در IIS6

## Socket Pooling ✓

# Windows

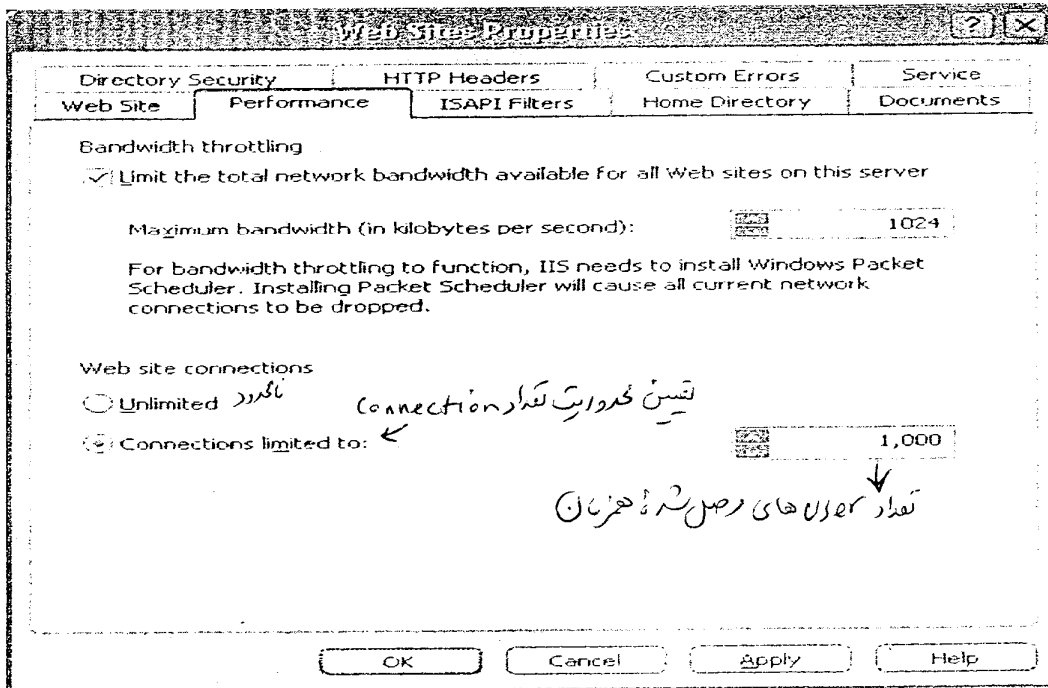
در صورتی که برای سایت های خود IP و اسم سایت یکی باشد می توانیم یک شماره پورت نیز برای آنها اختصاص داد و توسط آن که بیانگر یک سرویس خاص می باشد که اصطلاحاً به آن TCP پورت گفته می شود و این شماره پورت باید به هنگام Brows کردن سایت توسط کلاینت مشخص گردد.

## Multisite Hosting: تعریف چند website روی یک سرور

توسط این قابلیت می توانیم بر روی یک IIS چندین وب سایت داشته باشیم با این شرط که شماره پورت و یا IP سایت و یا Host Headerها با یکدیگر متفاوت باشد.

## Bandwidth Throttling: تقسیم پهنای باند

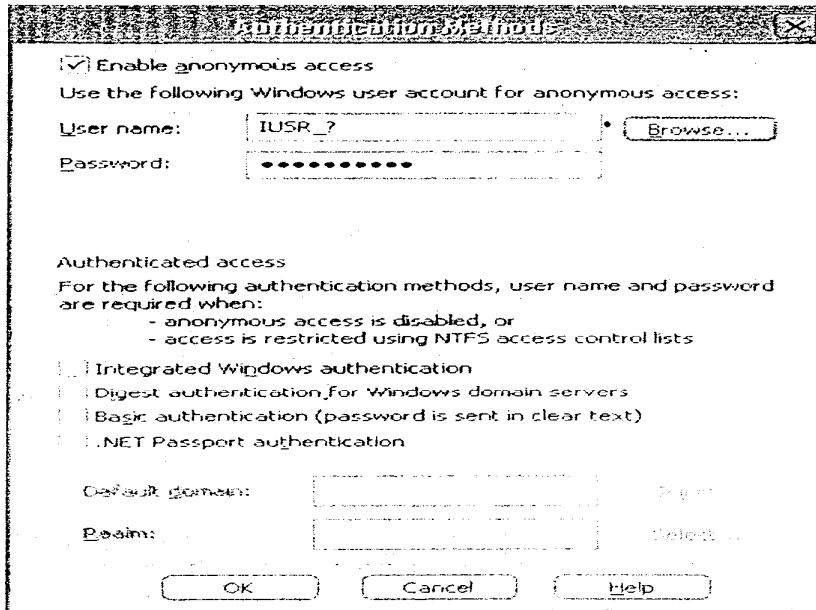
توسط این قابلیت می توانیم پهنای باند اشغال شده توسط وب سایت های مختلف خود را می توانیم محدود بکنیم. و تعداد کانکشن های که با Web سرور مربوطه میتواند ایجاد شود را محدود کنیم.



# Windows

## ✓ انواع روشهای Web Authentication :

در Directory Security - Edit - Authentication - Enable Anonymuos Access به هنگام ایجاد یک Web Site بر روی IIS به صورت پیش فرض گزینه Enable Anonymuos Access علامت خورده به این مفهوم است که همه کاربران بصورت ناشناس با استفاده از کاربری تحت عنوان اسم کامپیوتر - IUSER که عضو گروه Domain User می باشد همه کاربران می توانند از Web Site شما بازدید نمایند.



## انواع Anonymuos Access

### ۱- Integrated Windows Authentication :

توسط این Level کاربران بهنگام استفاده از وبسایت باید اسم کاربر و پسوردی که باید سرویس IIS بر روی آن قرار دارد را وارد نمایند.

### ۲- Digest Authentication For Windows Domain Servers :

(دارای امنیت در شبکه داخلی می باشد)

در صورت استفاده از این Level فقط کاربرانی که در داخل AD تعریف شده اند میتوانند با وب سایت ارتباط برقرار بکنند، قابل ذکر است این Level حالت امنیتی بین کلاینتها و Web سرورها به هنگام ایجاد ارتباط برقرار می کند.

### ۳- Basic Authentication (Password Is Send In Clear Text) :

• میتوان تک یک، چند، اینها را فصل کنیم اما ترکیب اینها عمل نمیکند بلکه بالاترین عمل برسد / البته به بررسی سرور که چه ارتباط دارند

# Windows

در صورت استفاده از این Level پسوردهای منتقل شده بین کلاینت و WebServer بصورت Clear رد و بدل می شود. (بدون حالت امنیتی)

قابل ذکر است در این Level در صورتی که پسورد ما مانیتور شود (یعنی با نرم افزار خاصی پسورد را کیچر کنیم) توسط نرم افزارهای مختلف قابل دسترسی می باشد، این Level حالت امنیتی برای کاربران ما ایجاد نمی کند، قابل ذکر است کاربران بهنگام دسترسی به وب سایت باید دارای یک Account Local و یا یک Domain Account باشند.

**۴-Net Passport Authentication**: (دارای امنیت در شبکه داخلی می باشد) *دو تا این تکت با ما داریم، ۳ تا می بقیه برضال می تونیم*  
این Level در سرور ۲۰۰۳ جدید می باشد. *روش بسیار خوبی است در این باره packaging خامی را در این مکترو بافت مخرم - نکته:*

در قسمت DirectorySecurity در IP Address قسمت Edit می توانیم IP های خاصی برای ورود به سایت خود تعیین کنیم.

## Home Directory

در این قسمت علاوه بر اینکه HomePage های ما می توانند بر روی کامپیوتر محلی ما قرار بگیرند می توانیم آدرس شبکه ای یک فولدر و یا آدرس URL یک وب سایت دیگری را مشخص بکنیم.

## FTP Site (File Transfer Protocol)

توسط این سرویس و راه اندازی FTP Server کاربران قادر خواهند بود برنامه ای را از روی FTP سرور Upload و یا Download بکنند. قابل ذکر است FTP سرور به صورت پیش فرض از TCP پورت ۲۱ استفاده می کند. برای راه اندازی چنین سرویسی ابتدا باید سرویس FTP را از مسیر زیر بر روی کامپیوتر نصب کنیم.

Windows Component – Application Server *redirection نام دارد، properties بزرگ لیمهای تگلی برای*  
*کدری Details رفته در سرور سرور نیاز را انتخاب می کنیم*

## Virtual Directory در قسمت Web Site

توسط این امکان می توانیم لینکهای مورد نیاز برای سایتهای خود را ایجاد نمائیم.

*رایت کلیک در new website، پس new و virtual... که نام سایت link پس میرا از همین می کنیم مثل*

<http://www.bbc.com/v7>

## Shadow Copies

توسط این امکان در Server2003 می توانیم از فایلهایی که در محیط شبکه موجود میباشند و در حال حاضر باز می باشند یک کپی بر روی کامپیوتر ایجاد می کند و در مواردی که کاربری بصورت اشتباهی فایل را پاک و یا



# Windows

تغییراتی در آن فایل ایجاد نمود سریع بتوانیم تغییرات موجود را به حالت عادی برگردانیم. در این حالت تغییرات در داخل درایوی که ویندوز نصب است داخل فولدر System Volum Information ذخیره می شود.

**نکته در مورد پرینترها :**

به هنگام نصب پرینتر بر روی DC بصورت اتوماتیکال پرینتر مربوطه در داخل AD , Publish می شود قابل ذکر است به هنگام نصب پرینتر نمی توانیم از Publish شدن پرینتر در داخل AD جلوگیری بکنیم ولی بعد از نصب میتوان چنین کاری را انجام داد.

نکته: در قسمت Sharing با انتخاب گزینه ListInTheDirectory می توان پرینتر را در داخل AD شناسایی نمود.

## Separator Page

برای جدا سازی اسناد پرینت گرفته شده می توانیم از الگو های جدا سازی تهیه شده توسط شرکت میکروسافت استفاده نمود.

کاربری که پرینت می فرستد توسط چهار الگو زیر می تواند اسناد خود را جدا بکند.

sysprtj.sep - sysprint.sep - pscript.sep - pcl.sep

**نکته:**

در پلاتفورم های ۲۰۰۰ به بعد می توان توسط پروتکل IPP به یک Web Server از طریق آدرس URL پرینت بفرستیم برای این کار ابتدا بر روی پرینت سرور سرویس InternetPrinting را نصب میکنیم با نصب این سرویس بر روی پرینت سرور در کنسول IIS در قسمت Web Site - Default Web Site فولدر Printers اضافه می گردد. سپس از پشت کلاینت با انتخاب NetworkPrinter و در مرحله بعد با انتخاب گزینه سوم آدرس Print سرور به صورت زیر داده می شود.

HTTP://Server/printers/Myprinter/.printer

**نکته:**

از طریق فرمانی در CMD میتوان سرویس Spooler را Restart نمود.



Net Start Spooler  
 Net Stop Spooler

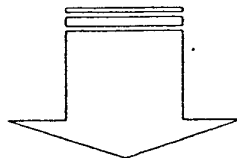
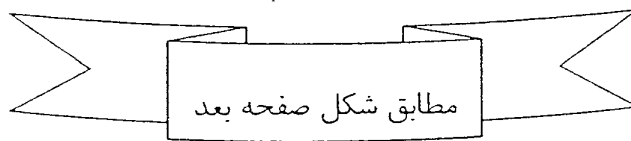
## SUS Server

توسط این سرویس در Server2003 می توانیم یک سرور مرکزی ایجاد کرده و سرور مرکزی خود را با سرور موجود در سایت Microsoft به روز کرده و کلاینتهای موجود در شبکه انواع Patch های موجود در سایت Microsoft را از روی SUS Server داخلی Download بکنند، قابل ذکر است این کار را بر روی پلات فورم های ۲۰۰۰ی که Service Pack2 به بعد روی آنها نصب است می توان اعمال نمود.

xxxxxxxxxxxxxxxxxxxx

برای راه اندازی SUS Server ابتدا باید سرویس IIS بر روی کامپیوتر نصب شود سپس نرم افزار SUS بر روی کامپیوتر موجود نصب گردد، بعد از نصب SUS در داخل کنسول IIS در قسمت Default Web Site فولدری به نام SUS Admin اضافه خواهد شد.

نکته: در داخل کنسول IIS در صورتی که فولدر SUS Admin را Browse کنیم وارد محیط SUS میشویم در این قسمت توسط گزینه Set Option می توانیم SUS سروری که قرار است سرور ما از آن سرور مربوطه خود را Update کند را مشخص نماییم.



# Windows

Internet Information Services (IIS) Manager

Microsoft Software Update Services

Version 1.0.370.552

### Set options

Set your Software Update Services options, and then click Apply.

**Select a proxy server configuration:**

Do not use a proxy server to access the Internet (در صورت نداشتن proxy انتخاب)

Use a proxy server to access the Internet

Automatically detect proxy server settings

Use the following proxy server to access the Internet:

Address:  Port: 80

Use the following user credentials to access the proxy server:

User:  Password:

Allow basic authentication when connecting to proxy server

---

**Specify the name your clients use to locate this update server:**

Server name:  (سرور واسطه)

If your clients cannot resolve a NetBIOS name (computername) you should change this to a DNS name (computername.domainname) or use the server's IP address.

---

**Select which server to synchronize content from:**

Synchronize directly from the Microsoft Windows Update servers

Synchronize from a local Software Update Services server:  (سرور واسطه انتخاب کرد)

Type the name of the server. Example: CorpWU1

Synchronize list of approved items updated from this location (replace mode)

---

**Select how you want to handle new versions of previously approved updates:**

Automatically approve new versions of previously approved updates (مورد تایید)

Do not automatically approve new versions of approved updates. I will manually approve these updates later.

© 2002 Microsoft Corporation. All rights reserved. Terms of Use Privacy Statement

رابطه کلید و کلمه:

معمولاً به پیغامی در مایکروسافت خودتون را update کند.

تمایش تعداد item های مربوط به هر برنامه که آورده است.

# Windows

نکته:

برای اینکه کلاینتها به SUS سرور داخلی وصل شده و خود را Update بکنند به دو طریق می توان عمل نمود، در صورتی که کلاینت مربوطه عضو Domain باشد می توانیم در قسمت GP.Domain موارد تنظیمی را انجام دهیم در صورتی که کلاینت مربوطه عضو Domain نباشد باید بر روی کلاینت به صورت زیر عمل بکنیم.

این دستور هم وارد استری یا این می شود  
سی در bbs.com سایت کلیک کرده در properties این group policy را انتخاب کرده و در قسمت edit در آنجا می توانیم تنظیمات را انجام دهیم.  
Computer Configuration – Administrative Templates – Windows Components – Windows Update





# Windows

نکته:

## Monitor server

در این قسمت می توانیم لیستی از موارد Download شده از SUS سرور مرکزی را ببینیم.

✓ برای تنظیم کردن نحوه وصل شدن کلاینت به sus serve به دو صورت می توانیم عمل نماییم.

### (۱) بر روی client :

برای این کار در قسمت Run کلاینت فرمان gpedit.msc را وارد کرده و در قسمت GP هر کلاینت برای تک تک کلاینتها تنظیمات خود را انجام می دهیم. (در صورتی که کلاینت ما عضو Domain نباشد).

### (۲) بر روی Domain :

برای این کار بر روی Gp Domain می توانیم موارد مورد نیاز خود را تنظیم کرده از این به بعد همه کلاینت هایی که عضو Domain هستند موارد تنظیمی بر روی Domain بر روی Client ها اعمال خواهد شد.

✓ نکته :

در صورتی که در قسمت window component در قسمت GP ، گزینه windows update وجود نداشت بر روی راست کلیک کرده و با انتخاب Add remove templates گزینه w\au را انتخاب می کنیم.

Administrative Templates

✓ نکته :

در حالت کلی یک sus server می تواند موارد Approve شده بر روی sus server را بر روی خود نصب نماید قابل ذکر است اگر sus server ما بر روی DC تنظیم شده باشد باید در قسمت GP موجود بر روی DC آدرس Sus server خود را وارد نماییم.

# Windows

نکته:

در صورتی که کلاینت ها نتوانستند به sus server وصل شوند و خود را Update نکنند مراحل زیر را انجام می دهیم:

- ۱) تاریخ و ساعت client ها با تاریخ و ساعت sus server یکی باشد.
- ۲) بعد از هرگونه تغییر در قسمت sus server در صورت جواب نگرفتن یکبار IIS را Restart می کنیم.
- ۳) یکبار سرویس Software update service synchronize را Restart می کنیم.
- ۴) در صورتی که موارد Download شده بر روی SUS سرور مشخص نباشد در داخل کنسول SUS در قسمت Monitor Server یکبار Refresh را انتخاب می کنیم.

نکته:

بعد از تنظیمات کلاینت ها برای استفاده از SUS سرور باید در قسمت رجستری کلاینت ها آدرس تعریف شده SUS سرور زیر اعمال شود.

**HKEY\_LOCAL\_MACHINE\software\policies\Microsoft\Windows\windowsUpdate**

آدرس: HWP\...  
WWW Status Server

نکته: Backup گیری از Sus:

بهنگام نصب IIS پوشه ای بنام Inetpub در داخل درایوی که ویندوز ما نصب می باشد ایجاد می شود. بصورت پیش فرض در صورت نصب IIS پوشه sus در داخل این پوشه ذخیره می گردد که این مسیر قابل تغییر می باشد برای Backup گیری از sus کلیه محتویات Inetpub در صورتی که sus در مسیر دیگری نصب شده باشد

- |                |     |   |   |
|----------------|-----|---|---|
| 1- Inetpub     | IIS | برای تهیه Backup کلاینت SUS باید مسیر فوق را گرفت | Backup از تنظیمات SUS در قسمت All task در IIS از بالاترین قسمت Backup/Restore Configuration |
| 2- sus فولدر   |     |   |   |
| 3- تنظیمات IIS |     |   |   |
- نکته:

با وارد شدن به کنسول IIS می توانیم از تنظیمات موجود بر روی IIS ، Backup گرفته و بهنگام Restart

کردن IIS تنظیمات Backup گرفته شده توسط IIS را Restore می نمایم.

- ۱- ابتدا IIS را نصب می کنیم و سپس در SUS را نصب می کنیم.
- ۲- سپس فولدر sus را در محل معینی که در خواست نصب می نمایم
- ۳- فولدر Inetpub را از تنظیمات Restore برای Backup جدید عمل خودش Restore (Alternate location)



نکته :

Backup Sus برای

%windir%\system32 \ inetsrv\ metaback

Backup این پوشه را برمی داریم.

**:Service pack**

شرکت Microsoft بعد از تولید سیستم عامل برای حل مجموعه از مشکلات و یا قابلیت های جدید در این سیستم عامل نرم افزاری تحت عنوان SP ارائه می کند. SP موجود در پلات فرمهای 2000 به بعد دو قابلیت اساسی نسبت به سرویسهای پگهای NT4 دارند.

**:Post Instalation**

در پلات فرمهای NT4 در صورتی که SP بر روی کامپیوتر سرور نصب باشد و بعداً سرویس خاصی بر روی کامپیوتر نصب شود دوباره مجبور به نصب SP می باشیم ولی در پلات فرمهای 2000 و 2003 این مشکل حل شد.

**:Slip Streaming** / تکرار در SP source ریندوز

در پلات فرمهای 2000 به بعد با فرمان update.exe می توانیم SP موجود را در داخل source ویندوز اعمال نماییم ولی در پلات فرمهای قبل از 2000 این امکان برای ما فراهم نبود.

برای اعمال کردن این قابلیت ابتدا SP موجود را با استفاده از سویچ (X) در مسیر مشخص شده Extract می نماییم. به طور مثال: در فرمهای NT4 برای استخراج از مسیر %windir%\system32\inetsrv\metaback\sp3.exe /x: folder name  
در فرمهای NT4 و 2000 و 2003 از مسیر %windir%\system32\inetsrv\metaback\sp3.exe /x: folder name استفاده می شود.

بعد از این مرحله در صورتی که بخواهیم ویندوزی که با آن بوت شده ایم را update نماییم از داخل پوشه service pack با وارد شده به پوشه I386 و انتخاب پوشه update و انتخاب فایل update.exe ویندوز موردنظر SP بر روی آن اعمال خواهد شد در صورتی که بخواهیم بر روی source ویندوز اعمال بکنیم باید از طریق cmd به مسیر فایل update.exe رفته و با این فرمان SP مربوطه در داخل Source ویندوز به صورت زیر قرار می گیرد. (مسیر ویندوز): /S:F:\SP(Extract)\I386\Update \Update.exe

**:Software licences** مدیریت

**:End User License Agreement (EULA)** تعریف

به قرارداد استفاده مجوز قانونی از نرم افزار گفته می شود. در حالت کلی مایکروسافت برای استفاده کاربران از محصولات خود دو نوع licences برای کاربران خود ارائه می دهد. این دو نوع licence عبارتند از :

**:per server**

# Windows

در این نوع licence بتعداد کانکشن های همزمان که قرار است از سرور استفاده نمایند licence خریداری می شود.

۲. **(Win 2000 Perseat) Per Device Or Per User** : یا *persita* ✓

در این نوع licence بتعداد کاربران و یا کلاینت ها باید licence خریداری شود. در صورتی که بخواهیم پلات فرم NT4 را به 2000 یا 2003، ارتقاء نماییم باید Licence Client Access (CAL) از شرکت مربوطه خریداری شود.

## : Terminal Server

در پلات فرمهای 2000 برای اینکه بتوانیم یک سرور 2000 را بصورت Remote کنترل نماییم باید بر روی server 2000 سرویس Terminal server نصب می کردیم این سرویس در پلات فرم 2000 در دو mode قابل دسترسی بود.

### ۱. Mode Administration :

در این Mode بصورت همزمان دو کانکشن بصورت Remot با server برای مدیریت server میتواند ایجاد شود این دو کانکشن ما محدودیت زمانی نداشتند.

### ۲. Mode Application :

در این Mode تعداد کانکشنها ها نامحدود ولی مدت زمان استفاده client ها از server ، ۹۰ روز میباشد در صورتی که بخواهیم محدودیت زمانی این Mode را برطرف نماییم باید Licence مربوطه از مایکروسافت خریداری شود.

در 2003 server توسط امکان Remot Desktop که معادل Mode Adminstration ترمینال سرور 2000 می باشد بصورت همزمان دو کانکشن بصورت نامحدود با server می توانیم ایجاد نماییم.

ترمینال سرور 2003 که در واقع همان Application Mode ، Terminal server 2000 می باشد بجای محدودیت ۹۰ روز از ۱۲۰ روز برای استفاده کاربران در نظر می گیرد.

Terminal server 2003 در دو سطح قابل دسترسی می باشد.

۱. Full Security: امنیت بیشتر است و با بعضی برنامه ها کار نمی کند

۲. relaxed security: امنیت پایین ولی با همه برنامه ها کار می کند





در صورتی که خواسته باشیم از طریق پلات فرمهای 9X و 2000 به یک Terminal Server 2003 وصل شویم باید بر از روی کامپیوتری که Terminal server بر روی آن نصب شده نرم افزار مربوطه را بر روی کلاینت نصب بکنیم.

windows\system32\client\tsclient\win32\setup

### : Roll Back Driver

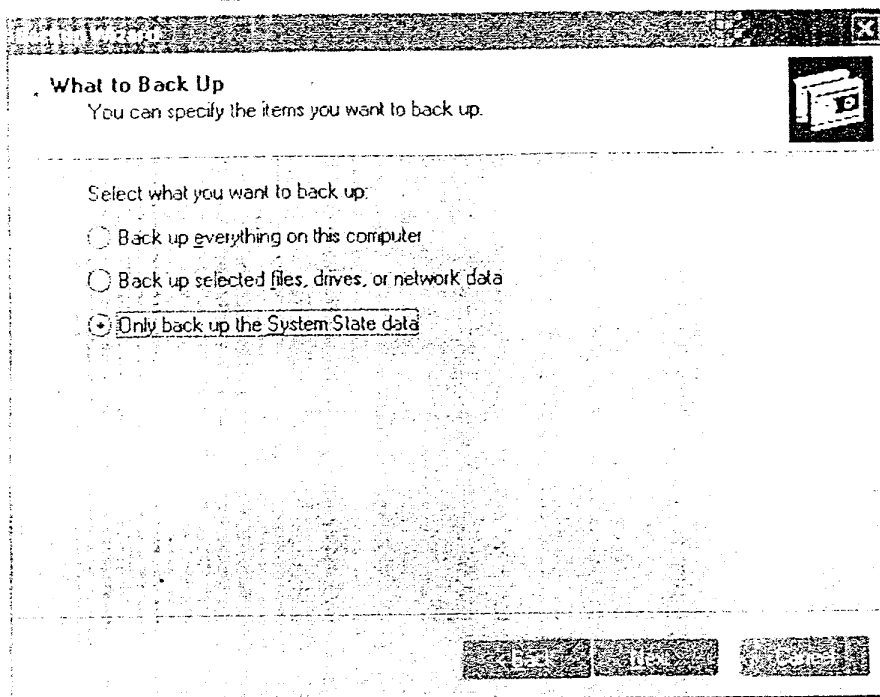
در قسمت Device Maneger بر روی یکی از قطعات رایت کلیک کرده برایتیز میگیریم. در سرور ۲۰۰۳ به صورت پیش فرض از این امکان می توانیم برای برگرداندن Driver به حالت قبل از نصب استفاده بکنیم , بصورت پیش فرض زمانی که بر روی سرور ۲۰۰۳ درایوی نصب میشود سرور ۲۰۰۳ اتوماتیک قبل از نصب درایور مربوطه Backup از درایور قبلی می گیرد در صورتی که خواسته باشیم میتوانیم از امکان Roll Back Driver برای برگرداندن درایور به حالت قبل استفاده بکنیم.

### : Backup از نوع System state data

با این امکان می توانیم بر روی DC از موارد زیر Backup بگیریم , قابل ذکر است این امکان بر روی پلات فورمهای ۲۰۰۰ و ۲۰۰۳ شامل موارد زیر می باشد.



# Windows



۱- Backup از System Registry .

۲- Backup از فایل‌های سیستمی و بوت فایل‌ها از قبیل Boot.ini , Ntldr , Ntdetect.com , Ntbootdd.sys , Bootsect.dos .

۳- Backup از فایل‌های سیستمی Protect شده ویندوز .

۴- Backup از Com+ .

۵- Backup از فولدر Sysvol .

۶- از تنظیمات IIS و Meta Data یی که حاوی اطلاعات IIS می باشد هم Backup می گیرد.

۷- Backup از Certificate Services :

با استفاده از این سرویس می توانیم مسایل امنیتی برای شبکه خود را در نظر گرفت از هک کردن شبکه شما توسط هکرها جلوگیری میکند.

۸- Backup از Clustering Services . با این سرویس می توان به نحوی این امکان را برای کامپیوتر خود بوجود آورد تا سرعت ذخیره سازی اطلاعات را بالاتر ببریم.

نکته :

به هنگام Backup گیری از طریق System State Data همه موارد بالا با یکدیگر انجام میگیرد و ما نمیتوانیم برای موارد بالا حالت انتخاب داشته باشیم.

# Windows

نحوه برگرداندن System State :

برای Restore کردن باید کامپیوتر خود را Restart کرده و با مد Dirctory Services کامپیوتر DC خود را راه اندازی می کنیم , در این حالت کلمه عبور برای Administrator همان رمزی خواهد بود که به هنگام نصب AD از ما سؤال میکند.

پیاده سازی انواع Raid ها :

در حالت کلی ۲ نوع Raid برای ذخیره سازی اطلاعات وجود دارد.

۱- Raid های نرم افزاری :

این نوع Raid ها با وجود دیسکهای Dynamic ایجاد می شوند, انواع Raid های نرم افزاری عبارتند از (Raid0 یا Strip) و (Raid1 یا Mirror) و (Raid5 یا Strip With Parity).

۲- Raid های سخت افزاری :

این نوع Raid ها توسط کنترلرهایی که بر روی مادربرد و امکانات موجود بر روی هارد دیسک قابل پیاده سازی می باشد کارایی و یا Performance این نوع Raid ها از Raid های نرم افزاری بیشتر می باشد.

## فرمان ←→ Diskpart

توسط این فرمان می توانیم برای مدیریت دیسکها و اطلاعاتی در مورد انواع دیسکها و Volume ها و ایجاد آنها از طریق این فرمان میوان اقدام نمود

دیسکهای Basic :

این نوع دیسکها محصولات ماکروسافت را پشتیبانی می کنند دیسکهایی که بر این اساس می باشند در ویندوز ۲۰۰۰ و ۲۰۰۳ می توانند دارای ۴ پارتیشن باشند.

1-(4) Primary

2-(3) Primary (1) Extended

3-(2) Primary (1) Extended

4-(1) Primary (1) Extended

Primary را برای Active partition کرده و هم تقسیم کردی  
extended را نه تران

دیسکهای Dynamic :

بطور کلی در دیسکهای Dynamic از نظر تعداد محدودیت پارتیشن محدودیتی وجود ندارد در دیسکهای Dynamic بجای اصطلاح پارتیشن Volume استفاده می شود , قابل ذکر است تحت شرایط خاص با توجه به اینکه Volume مورد نظر با NTFS فرمت شده باشد می توانیم فضای Volume خود را افزایش دهیم.

نکته :

۱- در کامپیوترهای Lab Tab دیسک Dynamic نمی تواند باشد.

۲- دیسک Dynamic را فقط Win 2000,XP,Server2003 Family پشتیبانی میکند.

# Windows

- ۳- دیسک Dynamic از تبدیل دیسک Basic بوجود می آید برای این کار حداقل یک مگابایت فضای خالی بر روی دیسک Basic باید وجود داشته باشد. قابل ذکر است اگر یک دیسک Basic را توسط ویندوز ۲۰۰۳ پارتیشن بندی کنیم این ویندوز بصورت اتوماتیک یک مگابایت فضای خالی کنار میگذارد.
- ۴- اگر یک دیسک Basic را به Dynamic تبدیل بکنیم پارتیشنها به Volume تبدیل می گردد.
- ۵- یک هارد دیسک در آن واحد می تواند یکی از نوعهای Basic , Dynamic باشد.
- ۶- برای تبدیل دیسک Dynamic به Basic ابتدا باید هم والیوم ها را پاک کرده و سپس با فرمان Convert To Basic Disk هم اطلاعات هارد دیسک خود را به Basic تبدیل میکنیم در این حالت هم اطلاعات ما از دست خواهد رفت.

## انواع Volume در Dynamic

۱- **Simple Volume**: این نوع از فضای موجود بر روی یک دیسک استفاده می کند در مقابل Simple Volume گزینه ای تحت عنوان Logical Volume می توانیم عرضه کنیم که در این حالت از فضای فیزیکی چند دیسک می توانیم استفاده بکنیم.

۲- **Spanned Volume**: این نوع از فضای موجود بر روی ۲ هارد داشته باشیم) این والیوم از فضای موجود بر روی ۲ الی ۳۲ دیسک استفاده می کند و نحوه ذخیره شدن اطلاعات در این نوع والیوم به صورت سری می باشد یعنی تا هارد دیسک اول ما پر نشود اطلاعات در هارد دیسک دوم ذخیره نمی شود. در این والیوم اگر یکی از هاردهای ما فیل شود همه اطلاعات از دست خواهد رفت در این نوع والیوم جنس هارد دیسک می تواند متفاوت باشد. فضای استفاده شده از دیسکها در این والیوم می تواند متفاوت باشد.

۳- **Striped Volume**: این نوع از فضای موجود بر روی ۲ الی ۳۲ دیسک استفاده می کند برخلاف spanned سایز Free Space های دیسکها باید برابر باشند در این والیوم نوع جنس هارد دیسک برای ما مهم نیست در این نوع والیوم اطلاعات بصورت بلوکهای ۶۴ کیلوبایتی ذخیره می شود بطور مثال ؛ اگر ما سه هارد دیسک داشته باشیم و اطلاعات ما به صورت سه بلوک ۶۴ کیلوبایتی تقسیم شده باشد همزمان اطلاعات بصورت سه گروه ۶۴ کیلوبایتی به صورت همزمان در روی سه هارد دیسک ذخیره می شود.

نکته: extend ندارد یعنی خود

# Windows

زمانیکه بخواهیم سرعت خواندن و نوشتن اطلاعات بالا باشد از Volume Striped اصطلاحاً گفته می شود این Volume, IO/Performance بالایی دارد.

نکته :

ویندوز Professional XP حالت FaultTolerance ندارد. ویندوز Server نسبت Professional XP دو نوع والیوم بیشتر پشتیبانی می کند.

نکته :

در ویندوز NT می توانیم بر روی یک دیسک بیسک والیوم های Striped, Sppaned را اعمال بکنیم ولی در ۲۰۰۰ یا ۲۰۰۳ بر روی دیسک Basic نمی توانیم والیوم Sppaned یا Striped را ایجاد بکنیم. حال اگر ویندوز NT4.0 خود را به ۲۰۰۳ Upgrade بکنیم ( بدون اینکه دیسک Basic خود را به Dynamic تبدیل بکنیم همچنان می توانیم از پارتیشنهای Sppaned یا Striped در ۲۰۰۳ استفاده بکنیم ولی مجوز ایجاد چنین پارتیشنهایی را نخواهیم داشت.

نکته :

والیومی که به عنوان Sppaned یا Striped ایجاد شده است نمی تواند SystemVolume یا BootVolume باشد.

## Mirrored (Raid1) : system and boot partition

این نوع والیوم فقط بر روی Server اعمال می شود، در این نوع والیوم اطلاعات بصورت همزمان بر روی دو هارد دیسک ذخیره می شود و در صورتیکه یکی از هارد دیسکهای ما فیل شود از هارد دیسک بعدی میتوانیم برای استفاده خود بهره ببریم. قابل ذکر است که در این نوع والیوم اطلاعات بصورت فیزیکی عیناً بر روی دو دیسک ذخیره می شود این نوع والیوم می تواند هم ، Boot Volume وهم System Volume باشد.

نکته :

به هنگام ایجاد Miroored در صورت وجود خطا اگر به هنگام بوت شدن مشکلی برای یکی از دیسکها پیش آید دو حالت زیر را می توانیم بررسی کنیم :

- ۱- دیسک دوم در واقع دیسکی که به هنگام بوت شدن از آن استفاده نمی شود Fail شود در این حالت مشکلی برای سیستم رخ نمی دهد.
- ۲- زمانیکه دیسک اول یعنی دیسکی که سیستم از آن بوت می شود Fail شود سیستم راه اندازی نخواهد شد معمولاً پیشنهاد می شود قبل از Fail شدن یک فلاپی که محتویات فایل Boot.ini و فایل های سیستمی از قبیل Ntldr , Ntdetect را در داخل فلاپی کپی کرده و مسیر Arc Path فایل Boot.ini را به دیسک دوم که سالم می باشد را تغییر نمائید.

تفاوت Boot Volume و system and boot partition :  
در Boot Volume می توانیم یک یا دو دیسک را در یک volume قرار دهیم.  
در system and boot partition می توانیم یک یا دو دیسک را در یک partition قرار دهیم.

در حالت simple می توانیم یک یا دو دیسک را در یک volume قرار دهیم.  
در حالت mirrored می توانیم یک یا دو دیسک را در یک volume قرار دهیم.



# Windows

نکته :

اگر به هنگام ایجاد Mirrored هر کدام از هارد دیسکهای ما بر روی کنترلر جداگانه ای باشد می توانیم یک حالت Full Fault Tolerance برای سیستم خود ایجاد بکنیم این در صورتی است که اگر یکی از کنترلرهای ما از کار بیافتد با کنترلر بعدی می توان هارد دیسک خود را Recovery (برگرداند) به این قابلیت Disk Duplexing گفته می شود.

**Mount کردن :**

در صورتی که به هنگام ایجاد والیوم از لحاظ تخصیص درایور با کمبود درایو مواجه شویم یا بخواهیم فضای یک والیوم را به صورت مجازی افزایش دهیم می توانیم یک فولدر را بر روی پارتیشن NTFS ایجاد کرده و سپس بر روی هارد دیسک خود یک والیوم ایجاد کرده و به جای تخصیص درایو Option Mount را انتخاب بکنیم به این ترتیب هر بار فایل یا شاخه ای را در والیوم فایلی ایجاد بکنیم آن فایل به صورت فیزیکی بر روی والیوم مورد نظر ایجاد خواهد شد. قابل ذکر است در داخل فولدر Mount شده نباید فولدر دیگری باشد.

**RAID 5**

در این والیوم از فضای ۳ الی ۳۲ دیسک استفاده می شود و به هنگام ذخیره شدن اطلاعات همانند Raid 0 اطلاعات به صورت بلوکهای ۶۴ کیلوبایتی بر روی دیسکها ذخیره می شود با این تفاوت که علاوه بر فایلهای ۶۴ کیلوبایتی یک کد اضافی به عنوان Parity بر روی دیسکها ذخیره می شود.

نکته :

فقط زمانی که یکی از دیسکهای ما Fail شود می توانیم حالت Fault Tolerance داشته باشیم و اگر بیش از یک دیسک Fail شود نمی توان حالت Fault Tolerance داشته باشیم.

نکته :

Raid 5 نمی تواند حالت System Volume , Boot Volume شود.

نکته :

Raid 5 از لحاظ Write سرعت پایین و از لحاظ Read سرعت بالایی دارد.

نکته :

به هنگام ایجاد والیوم Raid5 مقداری فضای اشغال شده توسط کد Parity یک سوم فضای کل هارد دیسک می باشد.



در کانال تلگرام کارنیل هر روز انگیزه خود را شارژ کنید 😊

<https://telegram.me/karnil>

