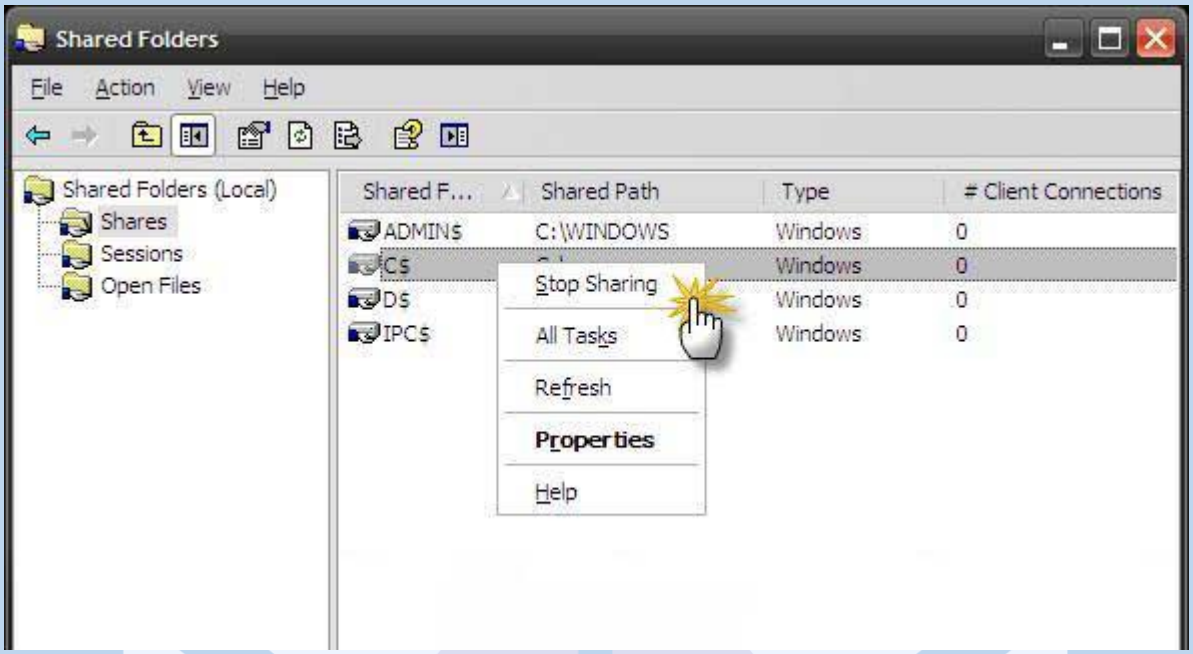
معرفی Share های پیشفرض ویندوز یا Administrative Shares و روش غیرفعال کردن آنها



Administrative Shareها در واقع Share های پیشفرض سیستم عامل ویندوز هستند که توسط بیشتر ویندوزهای مبتنی بر پایه NT مانند (NT, 2000,XP,2003, Vista, Windows 7 Windows 8) به وجود می آیند. این Share های پیشفرض هر پارتیشن موجود در سیستم را به اشتراک می گذارند. این Share ها به هر کسی که به عنوان عضو گروهAdministrator احراز هویت کرده باشد، اجازه دسترسی به دایرکتوری اصلی هر هارد درایو موجود روی سیستم را می دهند. این Share ها عموما در خارج از محیط Enterprise استفاده نمی شوند و به صورت پیشفرض روی نسخه های خانگیXP ، Vista ، Windows 7وWindows 8 قابل دسترسی نمی باشند. در اصل وجود این Shareها برای اهداف مدیریتی می باشد. این Share ها به منظور پشتیبانی از راه دور توسط مدیرهای شبکه به وجود آمده اند .

نام های Share ها

Administrative Shares عبارتی است که توسط Microsoft برای مجموعه ای از منابع به صورت پیش فرض به اشتراک گذاشته شده تعیین شد که به شرح زیر هستند :

- هر Drive Letter به اضافه علامت $ (فقط پارتیشن های مربوط به همان کامپیوتر، نه هر دستگاه جداشدنی از سیستم مانند CD/DVD، درایو های ذخیره USB
- $admin : برای به اشتراک گذاری دسترسی به %SYSTEMROOT% که معمولا C:\WINDOWS یا C:\WINNT می باشد

علامت $ اضافه شده به انتهای این اسم ها به معنی مخفی بودن این Share ها می باشد. ویندوز این چنین Share هایی را در میان Share هایی که در طی پرس و جو های عادی (Typical Queries) توسط کاربران انجام می شود را لیست نمی کند .این بدان معنا است که برای دسترسی به Administrative Share، باید نام آن Share را بدانیم.عموما بر این عقیده هستند که هر Share که اسم آن به $ خاتمه یابد، یک Administrative Shareمی باشد. به موجب تعریف مایکروسافت از عبارتAdministrative Share ، این برداشت اشتباه می باشد. با وجود این که هر Share حتی (Non-Administrative Shares) می توانند $ در انتهای اسم خود داشته باشند، اما فقط آن Share های پیش فرض که توسط ویندوز به وجود آمده و دارای $ در انتهای اسم خود هستند، به عنوان Administrative Share در نظر گرفته می شوند.آدرس UNC کلی برای یک Administrative Share به صورت زیر است :

```
1\\NetworkComputerName\(Drive letter)$
```

برای مثال :

```
1\\ComputerName\C$
```

این نمایانگر Administrative Share مربوط به پارتیشن "C" روی کامپیوتر "MyComputer"می باشد. این ساختار برای هر درایو متعلق به کامپیوتر درست می باشد. مانند \\MyComputer\d ، \\MyComputer\e (با درنظر گرفتن اینکه D و E، درایو متعلق به کامپیوتر بوده و دستگاه جداشدنی نیستند)

```
1\\MyComputer\ADMIN$
```

این نمایانگر Administrative Share مربوط به %SYSTEMROOT% در کامپیوتر "MyComputer" می باشد .

طریقه Hide کردن Administrative Share ها

این Administrative Share ها می توانند توسط فردی با سطح دسترسی Administratorحذف شوند. ولی پس از Restart کردن کامپیوتر مجددا به صورت خودکار ایجاد خواهند شد. با اعمال تغییراتی در Registry که در زیر آمده اند، می توانید تمامی Administrative Share ها را مخفی (حذف) نمایید. اگر این تنظیمات موجود نیستند، آنها را باید ایجاد کنید :

برای Server ها

۱. ابتدا Run را بازکرده، Regeditرا تایپ کرده و Enter را فشار دهید.
۲. به شاخه HKEY__LOCAL__MACHINE بروید.
۳. به زیرشاخه SYSTEM\CurrentControlSet\Services\LanManServer\Parameters بروید.
۴. یک کلید از نوع REG__DWORD با نام AutoShareServer ایجاد کنید.
۵. برای مخفی کردن Administrative Share ها، مقدار کلید ایجاد شده را به ۰ و برای نمایان شدن آنها، مقدار کلید را به ۱ تغییر دهید.

برای Client ها

ابتدا Run را بازکرده، Regeditرا تایپ کرده و Enter را فشار دهید.

۱. به شاخه HKEY__LOCAL__MACHINE بروید.
۲. به زیرشاخه SYSTEM\CurrentControlSet\Services\LanManServer\Parameters بروید.
۳. یک کلید از نوع REG__DWORD با نام AutoShareWks ایجاد کنید.
۴. برای مخفی کردن Administrative Share ها، مقدار کلید ایجاد شده را به ۰ و برای نمایان شدن آنها، مقدار کلید را به ۱ تغییر دهید.

طریقه Disable کردن Administrative Share ها

مایکروسافت جزییات زیادی را در مورد شیوه Disable کردن Administrative Share ها بیان نکرده است. دستور :

```
NET SHARE C$ /delete
```

را می توان برای Disable کردن Root Share در یک کامپیوتر تحت شبکه اجرا کرد. مشکل اینجاست که پس از Restart کردن کامپیوتر، این Shareبه صورت خوذکار ایجاد خواهد شد.یک راه حل معمول، ایجاد یک Batch File است که حاوی دستورهایی برای غیر فعال کردن Administrative Shareها میباشد. (این Share ها توسط دستور "NET SHARE" قابل مشاهده می باشند) و سپس می بایست این فایل Batchرا توسط Windows Task Scheduler در بخش Startup قرارداد که با هر بار روشن شدن سیستم، اجرا شود. معمولا دستورات زیر در قالب یه فایل Batch می توانند Administrative Share های Windows XP یا Windows Vista را غیرفعال نمایند :

```
NET SHARE C$ /delete
NET SHARE D$ /delete
NET SHARE admin$ /delete
```

همچنین از طریق بخش Shared Folders در Computer Management نیز می توان نسبت به غیر فعال کردن این share ها اقدام کرد. بدین گونه که

۱. روی Icon مربوط به My Computer راست کلیک کرده و گزینه Manage را انتخاب کنید. (و یا درRun، عبارت compmgmt.msc را تایپ کرده و Enter را فشار دهید)
۲. در سمت چپ به قسمت Shared Folders و سپس به قسمت Shares بروید.
۳. همان گونه که مشاهده میکنید، تمامی Share ها (چه آنهایی که توسط کاربر ایجاد شده اند و چه Administrative Share ها) قابل مشاهده هستند. روی Administrative Shareمورد نظر راست کلیک کرده و گزینه Stop Sharing را انتخاب کنید.
۴. پنجره هشداری با مضمون اینکه "این Share برای اهداف مدیریتی ایجاد شده است و پس از Restart شدن سرویسServer ، مجددا ایجاد خواهد شد" ظاهر میگردد .روی Yes کلیک کنید.

طریقه فعال کردن Administrative Share در Windows Vista و Windows 7

به صورت پیش فرض، Windows Vistaو نسخه های جدیدتر ویندوز مانع از دسترسی حساب های کاربری Local به Administrative Shareها تحت شبکه می شوند .

برای فعال کردن Administrative Share ها، می بایست تغییری در Registry اعمال کنید. برای این منظور، وارد Registry شوید :

۱. به شاخه HKEY__LOCAL__MACHINE بروید.
۲. به زیرشاخه Software\Microsoft\Windows\CurrentVersion\Policies\System بروید.
۳. یک کلید از نوع REG__DWORD با نام LocalAccountTokenFilterPolicy ایجاد نمایید.
۴. مقدار آن را به ۱ تغییر دهید.

پس ازRestart ، Hidden Share از کامپیوترهای دیگر قابل دسترسی می باشد .توجه کنید که این تغییر درRegistry ، محدودیت های ویندوز روی User Account Control از راه دور را حذف می کند ، به جای Restart کردن ، شما احتمالا قادر به اجرای 'net stop server' و 'net start server'از یک Command Prompt با دسترسی مدیر هستید .

طریقه فعال کردن Administrative Share در Windows XP Service Pack 1,2,3

به صورت پیش فرض، Windows XP SP3مانع از دسترسی به Administrative Share تحت شبکه می شود.برای فعال کردن Administrative Share شما می بایست :

- Explorerرا باز کرده و به منوی Tools رفته و Folder Options را انتخاب کنید.
- به تب View رفته و تا پایین صفحه تا آخر قسمت Advanced Settings بروید.
- اطمینان حاصل کنید که "User simple file sharing (Recommended)" انتخاب نشده است.

این راه می بایست بدون نیاز بهRestart ، کار کند. توجه نمایید که نسخه Windows XP Homeاین گزینه را نداشته و بنابراین نمی تواند Administrative Shareرا نشان دهد .

امنیت و ممانعت از دسترسی

غیر فعال کردن Administrative Share ها خیلی از خطرهای امنیتی شناخته شده را خنثی می کند. برای مثال، ویروسی مانند کرم Conficker، حمله هایی موسوم به Dictionary Attack را روی Administrative Share انجام می دهد.روش های گوناگون برای ممانعت از دسترسی از راه دور روی محتویات کامپیوترعبارتند از :

- "Administrators"را از تب Security مربوط به پارتیشن مذکور حذف نمایید. این باعث ممانعت از دسترسی Administrator های خارج از کامپیوتر به پارتیشن مذکور می شود، در عین حال Administrator های داخلی کامپیوتر کماکان میتوانند به پارتیشن دسترسی داشته باشند.
- سرویس File and Printer Sharing را متوقف کنید) و یا پروتوکل NetBT را غیر فعال کنید.سرویس Workstation را متوقف و یا غیر فعال کنید.
- قوانینی روی IPSec برای ممانعت از ارتباطات داخلی (Inbound Connections) روی ۴۴۵ *tcp*و ۴۴۵ udpوضع نمایید.
- آن دسته از افرادی که نمی خواهید دسترسی داشته باشند را از گروه Administrators حذف نمایید.
- فایل های محرمانه خود را از طریق فناوری هایی مانند EFS وRMS ، کد گذاری (Encrypt) کنید.

امن کردن Share ها

DACL های موجود روی Administrative Share ها حتی توسط مدیر داخلی کامپیوتر نیز قابل ویرایش نیست. با شروع Windows XP Home Editionو نسخه های ویندوزی کلاینتی پس از آن، ویندوز ویژگی "ForceGuest" را وقتی که مدیر داخلی بدون گذرواژه باشد، استفاده می کند. وقتی یک کاربر از راه دور به کامپیوتر(Windows XP و ویندوزهای پس از آن) که دارای حساب کاربری مدیر بدون Password میباشد، احراز هویت (Authenticate)می کند مثل Map کردن به یکی از Administrative Share ها(ویندوز به Session آنها یک ژتون دسترسی مهمان (Guest Access Token) اعمال می کند (و نه ژتون دسترسی مدیر). این کار به طور قابل بحث دارای امنیت بیشتری در مقابل حمله های از راه دور میباشد (در مقایسه با Password های ضعیف یا Password هایی که حدس زدنشان راحت میباشد).

- $Print : این Share برای مدیریت Printer ها به صورت Remote استفاده میشود .
- $Fax : این Share توسط کلاینت ها برای ارسال Fax استفاده میشود .
- $IPC : این هم یکی از Hidden Share ها یا همون Administrative Share ها می باشد که توسط سرویس Server کنترل میشود. با متوقف کردن این سرویس $IPCهم پاک میشود $IPC که مخفف Inter-Process Communication است، با استفاده از سرویس RPC یا همونRemote Procedure Call ، به Client اجازه میدهد که دستورها را به Server بفرستد. دستورهایی مانند:
- لیست کردن همه Share ها
- لیست کردن همه کاربران
- لیست کردن فایل های داخل یکShare
- Stopو Start کردن سرویس ها