بسم الله الرحمن الرحیم

آشنایی با User ها و Permission

سیستم عامل ها دارای کاربر یا User هستند که می تواند با سیستم کار کند.هر User بنا بر خواست مدیر یا Administrator می تواند تا سطح مشخصی به سیستم دسترسی داشته باشد.این دسترسی همواره ثابت است و تا زمانی که مدیر سیستم نخواهد بالا و پایین تر ببرد ، تغییر نخواهد کرد.در این مقاله سعی داریم تا شما را با انواع User های موجود در سیستم عامل Windows آشنا کنیم.

اجازه داشتن یا Permission چیست؟

هر کاربر در حد مشخصی اجازه دسترسی به سیستم را دارد.به این حد مشخص دسترسی به سیستم ، Permission می گویند که تمام تنظیمات آن در اختیار مدیر اصلی است.

گروه کاربری یا User Group:

هر گروه کاربری ، میزان دسترسی مشخصی از User های عضو در آن به سیستم را مشخص می کند.در واقع هر گروه ، سطح اختیارات و وظایف هر کاربر را شامل می شود.گروه های کاربری توسط مدیر اصلی ایجاد شده و سطح اختیارات و دسترسی هر یک از گروه ها را او مشخص می کند.اگر در یک شبکه با چندین نفر کاربر بخواهید به طور جداگانه سطح اختیارات هر کاربر را مشخص کنید ، باید زمانی زیادی را صرف این کار کنید اما گروه های کاربری این کار را برای شما آسان تر کرده و شما می توانید هر User را در گروه خاص خودش قرار دهید و طبق تنظیمات آن گروه ، سطح اختیارات او را تعیین کنید.

گروه های کاربری به چند دسته تقسیم می شوند؟

در سیستم عامل ویندور ، 2 گروه کاربری کلی وجود دارند:

1) Global Group
2) Local Group

گروه Global Group:

این گروه از دو گروه اصلی Domain Administrators و Domain User تشکیل شده است.این گروه ها مخصوص شبکه هستند و هر یک از آن ها می توانند به شبکه و دامنه دسترسی داشته باشند.این گروه ها در Server ها بیشتر وجود دارند.

گروه Local Group:

این گروه به طور پیش فرض از 9 گروه اصلی تشکیل شده است.در ادامه هر یک از گروه ها را توضیح خواهیم داد.

User ها در ویندوز:
در سیستم عامل ویندوز به طور از قبل طراحی شده ، تعداد 9 گروه کاربری یا User Group داریم که بنا بر نسخه ی ویندوز کمی بیشتر یا کم تر است.در سیستم عامل ویندوز می توان با دستور net localgroup تمامی گروه های کاربری را مشاهده نمود البته در صورتی که دسترسی لازم را برای انجام این کار داشته باشید.

گروه Administrators:

User هایی که در این گروه قرار دارند ، می توانند به کل سیستم دسترسی کامل داشته باشند.کاربرانی را اضافه و یا حذف کرده و سطح اختیارات آن ها را کنترل کنند.User هایی که در این گروه قرار دارند مانند Administrator نمی توانند حذف شوند و برای حذف هر یک باید یک Account مدیریتی دیگر در این گروه کاربری وجود داشته باشد.Password این کاربران تنها با اختیار کاربر مدیر دیگری می تواند تغییر کند.همه ی User ها ، تحت نظر کاربران این گروه قرار دارند.

گروه Server Operators یا Network Configuration Operators:

User هایی که در این گروه قرار دارند ، می توانند تنظیمات شبکه و Server را انجام دهند.سطح اختیارات آن ها در حد مدیر سیستم است.نمی توانند به Account مدیران دسترسی داشته باشند.این کاربران می توانند ، سرویس های شبکه را به سیستم اضافه و یا کم کنند.

گروه Backup Operators:

User های این گروه تنها قادر هستند تا به فایل ها دسترس داشته و آن ها را ویرایش کرده و یا بخوانند. در واقع آن ها می توانند از سیستم پشتیبان تهیه کنند.اجازه دسترسی به Account کاربران دیگر را به طور کامل ندارند.

گروه Help Services Group:

User های این گروه می توانند در صورت بروز مشکل در یکی از سرویس های در حال اجرای سیستم و غیاب کاربران گروه های دیگر مانند Server Operators ، به صورت موقت سرویس را درست کنند.در واقع سطح اختیاری در حد مدیرسیستم دارند.

گروه Power Users:

User هایی این گروه می توانند به تمامی Account ها دسترسی داشته باشند.همچنین آن ها می توانند سرویس های در حال اجرا را کنترل کنند.سطح اختیارات آن ها در حد مدیر است.

گروه Remote Desktop Users:

User های این گروه می توانند از شبکه به داخل سیستم به وسیله ی برنامه ی Remote Desktop Connection وارد شوند و اختیارات در حد خواندن و نوشتن فایل ها دارند.

گروه Guests:

User های این گروه دارای پایین تر سطح اختیارات هستند.حتی برای وصل شدن به اینترنت نیز ، باید موافقت و اجازه ی مدیر اصلی را داشته باشند.اجازه ی اجرای هر برنامه ای را ندارند.تنها می توانند فایل ها را بخوانند و اجازه ویرایش آن ها را ندارند.

گروه Replicator:

User های این گروه در حد معمولی به سیستم دسترسی دارند و می توانند فایل ها بخوانند و یا ویرایش کنند.

گروه Users:

User های این گروه هم در حد معمولی و کار با سیستم به آن دسترسی دارند و می توانند فایل های مختلف را بخوانند و ویرایش کنند اما دسترسی به Account سایر کاربران را ندارند.

این نکته را نباید فراموش کرد که اگر اختیارات همه ی گروه های بالا را جمع کنیم بازهم به سطح اختیارات مدیر اصلی یا Administrator نمی رسد. البته توضیحات داده شد ، بر اساس اختیارات پیش فرض گره های کاربری بوده و شما می توانید هر یک از این اختیارات را تنظیم کنید.

کاربر مخفی در ویندوز:

سیستم عامل ویندوز علاوه بر گروه و کاربران گفته شده ،کاربر مخفی دارد.این کاربرSYSTEM است که اختیارات بیشتر از Administrator را دارد؛اما نمی توان به آن وارد شد.همه ی اختیارات مدیر کل از SYSTEM است و این کاربر دز زمان فعال بودن کاربران دیگر نیز فعال است.

گروه های ویژه:
گروه های ویژه برای کنترل انواع خاصی از قابلیت های سیستم وجود دارند.شما نمی توانید کاربران را از گروه های ویژه حذف کنید و یا اضافه کنید و به این دلیل آن ها ویژه هستند.این گروه ها همیشه بر روی کامپیوتر شما فعال هستند و جزو Local Group قرار می گیرند.هر یک از این گروه ها وظایف خاصی دارند :

1) INTERAVTIVE: یک گروه متغیر است که از کاربرانی که در حال حاضر به صورت Local وارد شده اند ، تشکیل می شود.
2) NETWORK: یک گروه متغیر دیگر از کاربرانی تشکیل می شود که Session یا نشست های شبکه دارا می باشند.
3) CREATOR OWNER: که مالک یک شئ بخصوص است ، حتی اگر خود مالک این شئ ا ایجاد نکرده باشد.
4) EVERYONE: این گروه برای فراهم کردن اجازه دستیابی به پروسه های معمولی سیستم منظور شده است ، اگر چه این گروه می تواند برای دادن اجازه دست یابی به تقریبا همه چیز به کار برود.

چگونه می توان سطح اختیارات هر کاربر یا گروه کاربری را مشخص کرد؟

می توانید به Start-Control Panel- Administrative Tools – Local Security Policy – Local Policies- User Right Assignment رفته و هر کار خاصی را در اختیار کاربر مشخصی قرار دهید.برای این کار هم ، روی عمل مشخص شده در زیر ستون Policy یا سیاسیت ، دو بار کلیک کرده و در پنجره ی باز شده نام گروه کاربری مورد نظر را وارد کنید.اگر نام مورد نظر یا گروه کاربری شما نبود ، با کلیک بر روی Add User or Group ، در پنجره ی باز شده Object Types را کلیک کنید و گزینه ی Group را تیک بزنید.سپس به پنجره قبلی باز گشته و در قسمت Enter the objects names to select ، نام کاربری یا گروه مورد نشر خود را وارد کنید و بر روی Check Names کلیک کرده ودر صورت وجود کاربر یا گروه مورد نظر ، بر روی دکمه ی OK کلیک کنید.

راه های دیگر برای اعمال محدودیت و تعیین سطح اختیارات :

استفاده از فایل سیستم NTFS:این فایل سیستم همراه ویندوز NT معرفی شد و قابلیت های امنیتی زیادی دارد.برای استفاده از این قابلیت ها ابتدا باید فایل سیستم خود را به NTFS تبدیل کنید سپس به Start-Control Panel-Administrative Tools-Local Security Policy – Local Policies – Security Options رفته و از ستون Policy ، Network access : Sharing and security model for local accounts را انتخاب کنید و آن را به Classic – local .... تغییر دهید و یکبار سیستم را Restart کنید.سپس بر روی درایو مورد نظر خود کلیک راست کرده و زبانه ی Security را انتخاب کنید.در این قسمت می توانید با انتخاب نام هر کاربر یا گروه کاربری در قسمت Group or user names ، در قسمت .... Permission for دسترسی و سطح اختیارات او را تعیین کنید.این اختیارات شامل موارد زیر هستند :

1) Full Control:دسترسی کامل به فایل ها و سیستم
2) Modify:تنظیم کردن تنظیمات مختلف
3) Read & Execute:خواندن و یا اجرا کردن فایل
4) List Folder Content:دیدن محتویات یک پوشه
5) Read:خواندن یک فایل
6) Write:نوشتن یک فایلو یا در واقع ایجاد کردن آن
7) Special Permissions:اختیارات بیشتر و ویژه

شما می توانید با تیک زدن Allow این عمل را فعال و یا با تیک زدن Deny این عمل را برای کاربر یا گروه کاربری مشخص غیر فعال کنید.

راه دیگر این است که بر روی برنامه ی اجرایی مورد نظر کلیک راست کرده و ....Run as را انتخاب کنید.به این شکل یک کاربر و یا گروه کاربری خاصی می توانند یک برنامه ی خاص را اجرا کنند.

راه دیگر که کمتر پیشنهاد می شود ، استفاده از برنامه های رمز گذار بر روی پوشه ها و فایل ها است.این برنامه ها به دلیل برخی از تنظیمات غلط می توانند باعض از بین رفتن پوشه ی شما شوند.

Copyright© by Siahacker
2005-2006 All Rights Reserved
Email:Siahacker@gmail.com