Windows İşletim Sistemleri Yerel Gruplar ve Kullanıcıların İncelenmesi / Güvenlik Ayarları

Bilişim sektöründe birçok kişi yönetimsel işlemleri gerçekleştirirken ya da bir kaynağa erişim hakkı tanımlarken yerel kullanıcıları kullanır ya da yerel gruplara üye eklemesi yapar. Çoğu zaman bilinçsiz yapılan bu işlemler yüksek güvenlik riskleri oluşturmaktadır. Grupların özellikleri, güvenlik ayarları ve bu gruplara üye kişilerin yapabilecekleri ile ilgili bilgileri içermektedir bu çalışma.

Varsayılan yerel gruplar

Yerel Kullanıcılar ve Gruplar Microsoft Yönetim Konsolu'nda (MMC) bulunan Groups klasörü, varsayılan yerel grupların yanı sıra oluşturduğunuz yerel grupları da görüntüler. Windows Server 2003 çalıştıran bir sunucu veya üye sunucu yüklediğinizde, varsayılan yerel gruplar otomatik olarak oluşturulur. Bir yerel gruba ait olmak, kullanıcıya yerel bilgisayarda çeşitli görevleri gerçekleştirme hakları ve becerileri verir.

Yerel gruplara yerel kullanıcı hesapları, etki alanı kullanıcı hesapları, bilgisayar hesapları ve grup hesapları ekleyebilirsiniz. Bununla birlikte, etki alanı grup hesaplarına yerel kullanıcı hesapları ve yerel grup hesapları ekleyemezsiniz.

- **“Administrators” Grubu**

Bu grubun üyeleri sunucu üzerinde tam denetim hakkına sahiptir ve kullanıcılara gereken kullanıcı haklarını ve erişim denetimi izinlerini atayabilir. “Administrator” hesabı aynı zamanda bir varsayılan üyedir. Bu sunucu bir etki alanına katıldığında, Domain Admins grubu otomatik olarak bu gruba eklenir. Bu grup sunucu üzerinde tam denetim hakkına sahip olduğundan, kullanıcı eklerken dikkatli olmanız gerekir.

- **“Administrators” Grubu Kullanıcı Hakları**

Bu bilgisayara ağdan erişme; Bir işlem için bellek kotaları ayarlama; Yerel olarak oturum açmaya izin verme; Terminal Hizmetleri aracılığıyla oturum açmaya izin verme; Dosya ve dizinleri yedekleme; Çapraz geçiş denetimini atlama; Sistem saatini değiştirme; Disk belleği dosyası oluşturma; Program hatalarını ayıklama; Uzaktaki sistemden kapatmayı zorlama; Zamanlama önceliğini artırma; Aygıt sürücüleri yükleme ve kaldırma; Denetim ve güvenlik günlüğünü yönetme; Üretici yazılımı ortam değişkenlerini değiştirme; Birim bakım görevlerini gerçekleştirme; Tek işlem için profil oluşturma; Sistem performansı için profil oluşturma; Bilgisayarı takma biriminden çıkarma; Dosya ve dizinleri geri yükleme; Sistemi kapatma; Dosyaların veya diğer nesnelerin sahipliğini alma.

- **“Backup Operators” Grubu**

Bu grubun üyeleri, dosyaları koruyan izinlerden bağımsız olarak, bu sunucudaki dosyaları yedekleyebilir ve bilgisayara geri yükleyebilir. Bunun nedeni, bir dosyayı yedekleme hakkının, tüm dosya izinlerinden önce gelmesidir. Güvenlik ayarlarını değiştiremezler.

- **“Backup Operators” Grubu Kullanıcı Hakları**

Bu bilgisayara ağdan erişme; Yerel olarak oturum açmaya izin verme; Dosya ve dizinleri yedekleme; Çapraz geçiş denetimini atlama; Dosya ve dizinleri geri yükleme; Sistemi kapatma.

- **“DHCP Administrators” Grubu**

DHCP Sunucusu hizmetiyle yüklenir. Bu grubun üyeleri, Dinamik Ana Bilgisayar Yapılandırma Protokolü (DHCP) Sunucusu hizmetine, yönetim erişimine sahiptir. Bu grup, yalnızca DHCP sunucusuna sınırlı yönetim erişimi verilmesini sağlar, ancak sunucuya tam erişim sağlamaz. Bu grubun üyeleri, DHCP konsolunu veya Netsh komutunu kullanarak sunucudaki bir DHCP'yi yönetebilir, ancak sunucuda bunun dışında bir yönetim eylemi gerçekleştiremezler.

- **“DHCP Administrators” Grubu Kullanıcı Hakları**

Varsayılan kullanıcı hakları yoktur.

- **“DHCP Users” Grubu**

DHCP Sunucusu hizmetiyle yüklenir. Bu grubun üyelerinin, DHCP Sunucusu hizmetine salt okunur erişimi vardır. Böylece üyeler, belirli bir DHCP sunucusunda depolanan bilgi ve özellikleri görüntüleyebilir. Bu bilgiler, DHCP durum raporlarına gereksinim duyan personele destek vermek için yararlıdır.

- **“DHCP Users” Grubu Kullanıcı Hakları**

Varsayılan kullanıcı hakları yoktur.

- **“Guest” Grubu**

Bu grubun üyeleri için oturum açılırken geçici bir profil oluşturulur ve üye oturumu kapattığında profil silinir. Guest hesabı (varsayılan olarak devre dışıdır) aynı zamanda bu grubun varsayılan bir üyesidir.

- **“Guest” Grubu Kullanıcı Hakları**

Varsayılan kullanıcı hakları yoktur.

- **“HelpServicesGroup” Grubu**

Bu grup, yöneticilerin tüm destek uygulamaları için ortak haklar belirlemelerine olanak verir. Varsayılan olarak grubun tek üyesi, Uzaktan Yardım gibi Microsoft destek uygulamalarıyla ilişkilendirilmiş hesaptır. Bu gruba kullanıcı eklemeyin.

- **“HelpServicesGroup” Grubu Kullanıcı Hakları**

Varsayılan kullanıcı hakları yoktur.

- **“Network Configuration Operators” Grubu**

Bu grubun üyeleri, TCP/IP ayarlarında değişiklik yapabilir ve TCP/IP adreslerini yenileyip bırakabilir. Bu grubun varsayılan üyesi yoktur.

- **“Network Configuration Operators” Grubu Kullanıcı Hakları**

Varsayılan kullanıcı hakları yoktur.

- **“Performance Monitor Users” Grubu**

Bu grubun üyeleri, Administrators veya Performance Log Users gruplarına üye olmaksızın, sunucudaki performans sayaçlarını yerel olarak veya uzaktaki istemcilerden izleyebilir.

- **“Performance Monitor Users” Grubu Kullanıcı Hakları**

Varsayılan kullanıcı hakları yoktur.

- **“Performance Log Users” Grubu**

Bu grubun üyeleri, Administrators grubuna üye olmaksızın, sunucudaki performans sayaçlarını, günlükleri ve uyarıları yerel olarak veya uzaktaki istemcilerden yönetebilir.

- **“Performance Log Users” Grubu Kullanıcı Hakları**

Varsayılan kullanıcı hakları yoktur.

- **“Power Users” Grubu**

Bu grubun üyeleri, kullanıcı hesapları oluşturabilir, oluşturdukları hesapları değiştirebilir ve silebilirler. Yerel gruplar oluşturabilir, oluşturdukları bu yerel gruplara kullanıcı ekleyebilir veya bu gruplardan kullanıcı kaldırabilirler. Ayrıca Power Users, Users ve Guests adlı gruplara kullanıcı ekleyebilir veya bu gruplardan kullanıcı kaldırabilirler. Üyeler paylaşılan kaynaklar oluşturabilir ve oluşturdukları paylaşılan kaynakları yönetebilir. Üyeler dosyaların sahipliğini alamaz, dizinleri yedekleyip geri yükleyemez, aygıt sürücüleri yükleyip kaldıramaz ve güvenlik ve denetim günlüklerini yönetemez.

- **“Power Users” Grubu Kullanıcı Hakları**

Bu bilgisayara ağdan erişme; Yerel olarak oturum açmaya izin verme; Çapraz geçiş denetimini atlama; Sistem saatini değiştirme; Tek işlem için profil oluşturma; Bilgisayarı takma biriminden çıkarma; Sistemi kapatma.

- **“Print Operators” Grubu**

Bu grubun üyeleri, yazıcıları ve yazdırma sıralarını yönetebilir.

- **“Print Operators” Grubu Kullanıcı Hakları**

Varsayılan kullanıcı hakları yoktur.

- **“Remote Desktop Users” Grubu**

Bu grubun üyeleri, sunucuda uzaktan oturum açabilir.

- **“Remote Desktop Users” Grubu Kullanıcı Hakları**

Terminal Hizmetleri'nden oturum açmaya izni verme.

- **“Replicator” Grubu**

Replicator grubu, çoğaltma işlevlerini destekler. Replicator grubunun tek üyesi, etki alanı denetleyicisinin Replicator hizmetlerinde oturum açmak için kullanılan etki alanı kullanıcı hesabı olmalıdır. Bu gruba gerçek kullanıcıların kullanıcı hesaplarını eklemeyin.

- **“Replicator” Grubu Kullanıcı Hakları**

Varsayılan kullanıcı hakları yoktur.

- **“Terminal Server Users” Grubu**

Bu grup, Terminal Server kullanarak sistemde oturum açmış durumdaki tüm kullanıcıları içerir. Kullanıcıların Windows NT 4.0'da çalıştırabildiği herhangi bir program, Terminal Server User grubunun üyeleri için de çalışır. Bu gruba atanan varsayılan izinler, üyelerin daha önceki programların çoğunu çalıştırmasına olanak verir.

- **“Terminal Server Users” Grubu Kullanıcı Hakları**

Varsayılan kullanıcı hakları yoktur.

- **“Users” Grubu**

Bu grubun üyeleri, uygulamaları çalıştırma, yerel ve ağ yazıcılarını kullanma ve sunucuyu kapatma gibi genel görevleri gerçekleştirebilir. Kullanıcılar dizinleri paylaşamaz veya yerel yazıcılar oluşturamaz. Varsayılan olarak Domain Users, Authenticated Users ve Interactive grupları, bu grubun üyesidir. Bu nedenle, etki alanında oluşturulan herhangi bir kullanıcı hesabı, bu grubun üyesi olur.

- **“Users” Grubu Kullanıcı Hakları**

Bu bilgisayara ağdan erişme; Yerel olarak oturum açmaya izin verme; Çapraz geçiş denetimini atlama.

- **“WINS Users” Grubu**

WINS hizmetiyle yüklenir. Bu grubun üyeleri, Windows Internet Ad Hizmeti'ne (WINS) salt okunur erişim hakkına sahiptir. Böylece üyeler, belirli bir WINS sunucusunda depolanan bilgi ve özellikleri görüntüleyebilir. Bu bilgiler, WINS durum raporlarına gereksinim duyan personele destek vermek için yararlıdır.

- **“WINS Users” Grubu Kullanıcı Hakları**

Varsayılan kullanıcı hakları yoktur.

Gruplar için varsayılan güvenlik ayarları

Kullanıcılara üç temel güvenlik düzeyi atanabilir. Bu izinler, Administrators, Power Users veya Users grubunun üyesi olan son kullanıcılara verilir.

- **“Administrators”**

Administrators grubu, bilgisayar bakım görevlerini gerçekleştirmek için sağlanmıştır. Bu gruba verilen varsayılan izinler, sistemin tümü üzerinde tam denetim kurulmasına olanak sağlar. Sonuç olarak, yalnızca güvenilen çalışanlar bu grubun üyesi olabilir.

- **“Power Users”**

Power Users grubunun üyeleri Users grubunun üyelerinden daha çok, Administrators grubunun üyelerinden daha az izne sahiptir. İleri düzeydeki kullanıcılar, yöneticiler grubu için ayrılan görevlerin dışındaki herhangi bir işletim sistemi görevini gerçekleştirebilirler. Power Users grubuna verilen varsayılan izinler, grup üyelerinin bilgisayar ile ilgili bütün ayarları değiştirmesine olanak sağlar.

Windows NT 4.0'dan yükselttiğinizde, kuruluşunuzda yükseltme işleminden önce kullanılan uygulamalarla geriye dönük uyumluluk sorunları çıkmasını engellemek için, Restricted Users grubunun üyeleri otomatik olarak Power Users grubuna yerleştirilir. Windows NT 4.0'da çalışan birçok uygulamanın doğru çalışabilmesi için izinlerin yükseltilmesi gerekir. Power Users için varsayılan Windows 2000, Windows XP Professional ve Windows Server 2003 ailesi güvenlik ayarları, Windows NT 4.0'daki Users grubunun varsayılan güvenlik ayarlarına çok benzer. Windows NT 4.0'da Users grubundan birinin çalıştırabildiği tüm programları, Windows 2000,

Windows XP Professional veya Windows Server 2003 ailesinde Power Users grubu üyeleri de çalıştırabilir.

Son kullanıcıların yükseltilmiş Power Users grubu izinlerine sahip olmasını istemezseniz, bu kullanıcıları Users grubu üyesi yapabilir ve yalnızca Windows Logo Program for Software uygulamalarını çalıştırmalarını sağlayabilirsiniz. Windows Logo Program for Software grubundan olmayan uygulamaların desteklenmesi gerekiyorsa, son kullanıcıların Power Users grubunun bir parçası olması gerekecektir.

Power Users aşağıdakileri yapabilir:

- Windows Logo program for Software'e ait Windows 2000, Windows XP Professional veya Windows Server 2003 ailesi uygulamalarının yanı sıra eski uygulamaları da çalıştırma.
- İşletim sistemi dosyalarını değiştirmeyen veya sistem hizmetlerini yüklemeyen programlar yükleme.
- Yazıcılar, tarih ve saat, güç seçenekleri ve diğer Denetim Masası kaynaklarını içeren sistem çapında kaynakları özelleştirme.
- Yerel kullanıcı hesapları ve gruplarını oluşturma ve yönetme.
- Varsayılan olarak başlatılanların dışında kalan sistem hizmetlerini durdurma ve başlatma.

Power Users kendilerini Yöneticiler grubuna ekleme iznine sahip değildir. Power Users, kullanıcılar kendilerine izin vermediği sürece, başka kullanıcıların NTFS birimindeki verilerine erişemez.

Dikkat

- Windows 2000, Windows XP Professional, veya Windows Server 2003 ailesinin bir üyesinde eski programları çalıştırabilmek için çoğunlukla bazı sistem ayarlarına erişimi değiştirmeniz gerekir. Power Users'ın eski programları çalıştırmasına izin veren aynı varsayılan ayarlar, Power Users'ın sistem üzerinde ek ayrıcalıklar elde etmesine, hatta tam yönetim denetimi kazanmasına olanak sağlar. Bu nedenle, program işlevselliğinden ödün vermeden en yüksek güvenlik düzeyine ulaşmak için Windows Logo Program for Software uygulamalarının dağıtılması çok önemlidir. Bu programlar Users grubu tarafından sağlanan Güvenli yapılandırma altında başarılı bir şekilde çalışır.
- Power Users programları yükleyebileceği veya değiştirebileceğinden, Power Users olarak Internet'e bağlandığınızda, sisteminiz Truva atlarına ve diğer güvenlik risklerine açık duruma gelir.

- **“Users”**

Bu gruba ayrılan varsayılan izinler, üyelerin işletim sistemi ayarlarını veya diğer kullanıcıların verilerini değiştirmesine olanak tanımadığından, kullanıcılar grubu en güvenli seçenektir.

Kullanıcılar grubu, programların çalıştırılabileceği en güvenli ortamı sağlar. NTFS dosya sistemi ile biçimlendirilen bir birimde, yeni yüklenen sistemdeki (yükseltilen sistemde değil) varsayılan güvenlik ayarları, bu grubun üyelerinin işletim sisteminin ve yüklenen programların bütünlüğünü bozmasını önleyecek şekilde tasarlanmıştır. Kullanıcılar sistem çapında kayıt defteri ayarlarını, işletim sistemi dosyalarını veya program dosyalarını değiştiremez. Users grubu iş istasyonlarını

kapatabilir, ancak sunucuları kapatamaz. Kullanıcılar yerel gruplar oluşturabilirler, ancak yalnızca kendi oluşturdukları yerel grupları yönetebilirler. Yöneticiler tarafından yüklenmiş veya dağıtılmış olan Windows Logo program for Software'e ait Windows 2000, Windows XP Professional veya Windows Server 2003 ailesi üyelerinin programlarını çalıştırabilirler. Users grubu, kendi veri dosyalarının (%userprofile% dizininde depolanan dosyalar) tümü ve kayıt defterinin kendilerine ait bölümü (HKEY_CURRENT_USER bölümünde) üzerinde tam denetim sahibidir.

Bununla birlikte, kullanıcı düzeyindeki izinler, kullanıcıların her zaman eski uygulamaları başarıyla çalıştırmasına olanak sağlamaz. Bu eski uygulamaları çalıştırmak için, Users grubu üyelerinin uygulamaları çalıştırmasına izin veren güvenlik düzeyini azaltabileceğinizi ya da Users grubu üyelerini Power Users grubu üyeliğine yükseltebileceğinizi unutmayın. Her iki seçenek de kuruluşunuzun güvenlik düzeyini indirecektir. Users grubu üyelerinin Windows Logo program for Software uygulamalarını çalıştırmaları garanti edildiğinden, en iyi yöntem yalnızca bu uygulamaları kullanmaktır.

Windows 2000, Windows XP Professional veya Windows Server 2003 ailesinin bir üyesini çalıştıran sistemlerin güvenliğini sağlamak için yönetici şunları yapmalıdır:

- Son kullanıcıların, yalnızca Kullanıcılar grubunun üyesi olmasına dikkat etmelidir.
- Windows Logo program for Software programları gibi Users grubu üyelerinin başarıyla çalıştırabileceği programları dağıtmalıdır.

Users grubu üyeleri Windows 2000'den önceki Windows sürümlerini çalıştıramazlar; bunun nedeni, bu programların dosya sistemini ve kayıt defteri güvenliğini desteklememesi (Windows 95 ve Windows 98 gibi) veya başka varsayılan güvenlik ayarlarıyla gönderilmiş olmasıdır (Windows NT). Yeni yüklenmiş NTFS sistemlerinde eski uygulamaları çalıştırmak konusunda sorunlarınız varsa, aşağıdakilerden birini yapın:

1. Windows Logo program for Software uygulamalarının yeni sürümlerini yükleyin.
2. Son kullanıcıları, Users grubundan Power Users grubuna taşıyın.
3. Kullanıcılar grubunun varsayılan güvenlik izinlerini azaltın. Bunun için Uyumlu güvenlik şablonunu kullanmanız gerekir.

Anonymous grubu artık Everyone grubunun üyesi değildir

Windows XP Professional ve Windows Server 2003 ailesinde, Anonymous grubu artık Everyone grubunun üyesi değildir.

Windows 2000 sistemi Windows XP Professional veya Windows Server 2003 ailesine yükseltildiğinde, Everyone grubu için izin girdileri olan (Anonymous Logon grubu için açık izni olmayan) kaynaklar, yükseltme işleminden sonra Anonymous grubundaki kullanıcılar tarafından kullanılamaz. Birçok durumda bu, anonim erişime getirilmiş uygun bir sınırlamadır. Anonim erişim gerektiren önceki uygulamaları desteklemek için adsız erişime izin vermeniz gerekebilir. Adsız oturum açma grubuna erişim izni vermeniz gerektiğinde, Adsız Oturum Açma güvenlik grubunu ve izinlerini belirgin olarak eklemeniz gerekir.

Diğer gruplar

- **Interactive**

Bu grup, o anda bilgisayarda oturum açmış kullanıcıyı içerir. Windows 2000, Windows XP Professional veya Windows Server 2003 ailesine yükseltme sırasında, eski uygulamaların yükseltme işleminden önceki gibi çalışmaya devam etmesini sağlamak için, Interactive grubunun üyeleri de Power Users grubuna eklenir.

- **Network**

  Bu grup, o anda sisteme ağ üzerinden erişen tüm kullanıcıları içerir.

- **Backup Operators**

  Backup Operators grubunun üyeleri, dosyaları koruyan izinlerden bağımsız olarak, onları yedekleyip bilgisayara geri yükleyebilirler. Ayrıca bilgisayarda oturum açıp kapatabilirler, ancak güvenlik ayarlarını değiştiremezler.

  Dikkat

  Veri dosyalarını ve sistem dosyalarını yedekleyip geri yükleyebilmek için, bu dosyalar üzerinde okuma ve yazma izinlerine sahip olmanız gerekir. Backup Operators grubunun dosyaları yedeklemesini ve geri yüklemesini sağlayan aynı varsayılan izinler, bu kullanıcıların grup izinlerini başka kullanıcıların dosyalarını okumak veya Truva atı programları yüklemek gibi, başka amaçlar için de kullanmasına olanak sağlar. Yalnızca Backup Operators tarafından yedekleme programının çalıştırabileceği bir ortam oluşturmak için Grup İlkesi ayarları kullanılabilir.

Yerel kullanıcı hesapları

Yerel Kullanıcılar ve Gruplar Microsoft Yönetim Konsolu'nda (MMC) bulunan Users klasörü, varsayılan kullanıcı hesaplarının yanı sıra oluşturduğunuz kullanıcı hesaplarını da görüntüler. Windows Server 2003 çalıştıran tek bir sunucu veya üye sunucu yüklediğinizde, bu varsayılan kullanıcı hesapları otomatik olarak oluşturulur. Aşağıdaki tabloda, Windows Server 2003 çalıştıran sunuculardaki varsayılan kullanıcı hesapları açıklanmaktadır.

- **“Administrator” Hesabı**

Administrator hesabı, sunucu üzerinde tam denetime sahiptir ve kullanıcılara gereken kullanıcı haklarını ve erişim denetimi izinlerini atayabilir. Bu hesap, yalnızca yönetici kimlik bilgileri gerektiren görevler için kullanılmalıdır. Bu hesabı kesinlikle sağlam bir parola kullanacak şekilde ayarlamanız önerilir. Administrator hesabı, sunucudaki Administrators grubunun üyesidir.

Administrator hesabı, Administrators grubundan silinemez veya kaldırılamaz, ancak yeniden adlandırılabilir veya devre dışı bırakılabilir. Administrator hesabının Windows'un pek çok sürümünde bulunduğu bilindiğinden, bu hesabı yeniden adlandırmak veya devre dışı bırakmak, kötü amaçlı kullanıcıların bu hesaba erişmelerini güçleştirir. Administrator hesabı, sunucuyu ilk kurduğunuzda kullandığınız hesaptır. Bu hesabı kendiniz için bir hesap oluşturmadan önce kullanın.

Önemli

Administrator hesabı devre dışı bırakılsa da, Güvenli Mod ile bir bilgisayara erişmek için kullanılabilir.

- **“Guest” Hesabı**

Guest hesabı, bilgisayarda gerçek hesapları olmayan kişiler tarafından kullanılır. Hesabı devre dışı bırakılmış, ancak silinmemiş bir kullanıcı da Guest hesabını kullanabilir. Guest hesabı parola gerektirmez. Guest hesabı varsayılan olarak devre dışı bırakılır, ancak onu etkinleştirebilirsiniz.

Guest hesabının haklarını ve izinlerini herhangi bir kullanıcı hesabında olduğu gibi ayarlayabilirsiniz. Varsayılan olarak Guest hesabı, bir kullanıcının sunucuda oturum açmasına olanak veren varsayılan Guests grubunun bir üyesidir. Herhangi bir izinle birlikte ek hakların, Administrators grubunun üyesi tarafından Guests grubuna verilmesi gerekir. Guest hesabı varsayılan olarak devre dışı bırakılır ve devre dışı olarak kalması önerilir.

- **“Help Assistant” Hesabı**

Uzaktan yardım oturumuyla yüklenir. Uzaktan Yardım oturumunu açmak için kullanılan birincil hesap. Bu hesap, Uzaktan Yardım oturumu istediğinizde otomatik olarak oluşturulur ve bilgisayara erişimi sınırlıdır. HelpAssistant hesabı Uzak Masaüstü Yardım Oturumu Yöneticisi hizmeti tarafından yönetilir ve bekleyen bir Uzaktan Yardım isteği yoksa, otomatik olarak silinir.