

# WINDOWS NT PERMISSIONS

By Pat Bloodwell

## ADMINISTRATOR GROUP

I will begin with my focus on the Administrator group, the most powerful group in the operating system.

The following is an actual example of a typical situation that we have seen on a number of occasions. It involves a user account that has local administrator access when the user logs on to the local computer name, but does not have local administrator access when the user logs on to the domain name.

The main difference between logging in the local machine name or logging into the domain name is where the login is authenticated. When the user logs in to the local machine, his login is authenticated by the local directory database, created and modified by the local User Manager application. When a user logs into the domain, his login is authenticated either by the global directory database on the PDC (Primary Domain Controller) or a copy of that same global directory database on a BDC (Backup Domain Controller). This centralized directory database is created and modified by User Manager for Domains from any domain controller or other Windows NT system that has User Manager for Domains on the local system. Which way the user chooses to login will determine which of the two separate accounts the user is actually using.

In this case, the account "workstation/joe" is a member of the local administrator group and can perform all functions locally as an administrator. The account "domain/joe" is NOT a member of the local administrator group. Thus the "domain/joe" account is not an administrator on this local system. There are several options you can use to set up this account as an administrator; here are two that I believe are the simplest solutions:

1. If you want **domain/joe** to be an administrator on THIS WORKSTATION ONLY, add his global account name, "domain/joe," to the administrator group in this specific workstation's User Manager. The local User Manager controls access to the local system.
2. If you want "domain/joe" to be an administrator on ALL GLOBAL SYSTEMS, add the group Domain Admins to his account in User Manager for Domains. User Manager for Domains controls the global user database for the domain. By default, Domain Admins are members of the local administrator group on any system that is running Windows NT, making "domain/joe" a local administrator on all Windows NT systems. I will be discussing this powerful group in a later article. To add the account "domain/joe" to the Administrator group on this local system only:
  - Open User Manager on the local system from this menu location: Start / Programs/Administrative Tools.
  - Within the User Manager Window, highlight and double click Administrators in the Groups column of the lower sub window.
  - Within the Local Group Properties Window, select the Add button.
  - Within the Add Users and Groups Window, make sure that the correct domain name is displayed in the List Names From pull down list and highlight the account name joe, select the Add and OK buttons.
  - Within the Local Group Properties Window, select the OK button and close User Manager.

To add the account **domain/joe** to the domain admin group:

Revised December 29, 2008

Page 1 of 6

# WINDOWS NT PERMISSIONS

By Pat Bloodwell

- Open User Manager for Domains on any domain controller or other Windows NT system that has the User Manager for Domains application installed from this menu location: Start / Programs / Administrative Tools.
- Within the User Manager for Domains Window, highlight and double click Domain Admins in the Groups column of the lower sub window.
- Within the Global Group Properties Window, highlight joe and select the Add and OK buttons.
- Close User Manager for Domains.

In this article, I was working with the administrator group but this general procedure applies to any local or global group. My next article will include data on the differences between local and global groups. If you have any further data or comments on my article please contact me at the attached e-mail address.

## GLOBAL AND LOCAL GROUPS

In the first article on the subject we discussed a default global group called Domain Admins. As you may recall, any user who is a member of the Domain Admins is by default a member of the local Administrator group on any system running Windows NT. I repeat this data because I think the relationship between the Domain Admins groups and the Administrator group is the clearest way to illustrate the layout and power of global and local groups.

Global groups are used to administrate users at the domain level. If you have a user on your domain that you wish to have the same access as another user, you put that user into the same global group as the other user and he will have that same access. If you want a user to have administrator rights on all Windows NT systems on your domain, add them to the global Domain Admins group and they will have the access and rights by default.

The actual access and rights exist on the local system level, not on the Domain level. Being a member of the Domain Admins itself is only powerful because of the default that every system running Windows NT has the group Domain Admins as a member of the local Administrator group. It is the local Administrator group that actually has the access and rights. This is the key to domain user administration: The access and rights exist on the local system, and the global group has the same access and rights because it is linked to the local group.

It's really that simple, but how does this look in the two interfaces: **User Manager and User Manager for Domains?** Let's start with User Manager for Domains. User Manager for Domains controls the directory database for the domain along with the local directory database on all domain controllers:

- Open User Manager for Domains on any domain controller or other Windows NT system that has User Manager for Domains application installed from this menu location: Start / Programs / Administrative Tools.
- Within the lower subwindow within the User Manager for Domains window, you will see two different icons. The icons with the two users and the Earth are global groups while the icons with the two users and the CRT (the monitor) are local groups. Highlight and double click the global group icon for Domain Admins in the Groups column of the lower subwindow.

# WINDOWS NT PERMISSIONS

By Pat Bloodwell

- Within the right hand subwindow of Global Group Properties window, you will see ONLY domain users and NOTHING ELSE. This is key to what I mentioned above about global groups being used to administrate users on the domain level. You can add or remove domain users ONLY to global groups. No global groups, local groups or local users may be added.

Next, we'll use User Manager to see how local groups function. User Manager manages only the local directory database.

- Open User Manager on the local system from this menu location: Start / Programs / Administrative Tools.
- Within the lower subwindow within the User Manager window, you will see only one type of icon. The icons with the two users and the CRT are local groups. You do not have access to global groups from User Manager, only your local directory database. Highlight and double click Administrators in the Groups column of the lower subwindow.
- Within the Local Group Properties window, select the Add button.
- Within the Add Users and Groups window, you will see either your local system name or a domain name displayed in the List Names From pull down list. If you see your local system name in the pull down list, you will see all of the user accounts in your local system's directory database ONLY. If you see a domain name displayed in the pull down list, you will see both all the user accounts on the domain and all of the global groups. You would use this interface to add global groups our domain users to your local group.

## WORKGROUPS VS DOMAINS

What we are talking about here really boils down to a workgroup. In a workgroup, you can have seamless access to another system if there is an account on that remote system that has the same username and password as the local account that you are using. Any access and permissions granted on that remote system to this account are available to you when you connect to that system using this account, which is exactly what is described about the domain account in the above question. The disadvantage is that you must maintain both accounts, as opposed to a single domain account. This can be useful to solve some issues, but in the long run it can get more complex do to the same issues you have in workgroups, i.e., the need to maintain the same username and password on both sides of the connection.

## CACLS

On another topic, CACLS (Change ACLs, as described in our 22 March 1999 article), I found a potentially dangerous issue. Fortunately, the solution is quite simple.

I was working on a computer which had the Group SYSTEM with READ access to all of the files on the partition and used CACLS to set the group SYSTEM to FULL CONTROL. Here is what happened.

When originally looking at the partition's permissions at the Command Prompt, the command:

```
X:\>CACLS EXECISOFT
```

displayed the following data:

Revised December 29, 2008

# WINDOWS NT PERMISSIONS

By Pat Bloodwell

```
X:\ExecSoft BUILTIN\Administrators:(OI)(IO)F
      BUILTIN\Administrators:(CI)F
      NT AUTHORITY\SYSTEM:(OI)(IO)(special access:)
            GENERIC_READ
            GENERIC_EXECUTE

      NT AUTHORITY\SYSTEM:(CI)R
```

SYSTEM was then changed from READ to FULL CONTROL by this command:

```
X:\>CACLS * /e /t /c /g SYSTEM:F
```

After this, the command:

```
X:\>CACLS EXECISOFT
```

Displayed the following:

```
X:\ExecSoft NT AUTHORITY\SYSTEM:(OI)(IO)(special access:)
      STANDARD_RIGHTS_ALL
      DELETE
      READ_CONTROL
      WRITE_DAC
      WRITE_OWNER
      SYNCHRONIZE
      STANDARD_RIGHTS_REQUIRED
      GENERIC_READ
      GENERIC_EXECUTE
      FILE_GENERIC_READ
      FILE_GENERIC_WRITE
      FILE_GENERIC_EXECUTE
      FILE_READ_DATA
      FILE_WRITE_DATA
      FILE_APPEND_DATA
      FILE_READ_EA
      FILE_WRITE_EA
      FILE_EXECUTE
      FILE_DELETE_CHILD
      FILE_READ_ATTRIBUTES
      FILE_WRITE_ATTRIBUTES

      NT AUTHORITY\SYSTEM:(CI)F
      BUILTIN\Administrators:(OI)(IO)F
      BUILTIN\Administrators:(CI)F
```

# WINDOWS NT PERMISSIONS

By Pat Bloodwell

Attempting to display the permissions from Windows NT Explorer (by right-clicking the root folder, then selecting Properties, Security, Permissions) resulted in an error message "The parameter is incorrect".

The issue appears to be altering the group SYSTEM from READ access to FULL CONTROL causes an over-saturation of data. Not only do you see "The parameter is incorrect" but all NTFS access restrictions are completely removed, allowing any local user or network share essentially FULL CONTROL access.

The way to fix this, and also the way to prevent it from occurring in the first place, is to remove the group SYSTEM using CACLS:

```
X:\>CACLS * /e /t /c /r SYSTEM
```

then re-add the group SYSTEM with FULL CONTROL:

```
X:\>CACLS * /e /t /c /g SYSTEM:F
```

It is possible you may get similar results when you use CACLS to modify any existing user. If you ever make a change using CACLS and begin to see unusual or unexpected behavior on your system, try going to CACLS and removing then re-adding that user.

## DOMAIN ADMINS GROUP

From User Manager for Domains, when you create an account, you can not create a domain account that is not a member of the Domain Users group. Select the Groups button; from within the Group Memberships window, you can just add Domain Admins and you are done. You can then remove Domain Users by highlighting the Domain Admins group in that same Group Memberships window and select the Set button next to Primary Group. You can then Remove the group Domain Users making the account a member of only one group. Simple and clean.

By default, any system running Windows NT includes the Domain Admins group of its domain as a member of its local Administrators group. Here are the rules in regards to Domain Admins. These rules are common to all Windows NT domains, once again keeping them simple:

1. If you DON'T want a specific global account to have Administrator rights on all systems within the domain, DON'T put them into the Domain Admins group.
2. By the same token, you do not need to add other groups to an account that is a member of the Domain Admins group, the power is already there. If you feel a need to do so, you have just made your Windows NT domain more complicated.

If you look at your Domain Administrator and find that it is a member of several other groups you may wish to ask yourself, "why?" Does the local Administrator group have the power to do anything or has there been other complexity added so that the Administrator group is really not as powerful as it was designed to be? Do you have areas of your domain where the local Administrator group does not have access? Have you restricted access to any files or folders, and neglected to include "System Full

# WINDOWS NT PERMISSIONS

By Pat Bloodwell

Control” and “Administrators Full Control”? Any “ifs”, “ands”, or “buts”? The key is to keep this part of the equation simple; the Administrator can do everything.