Permissions and users management

The Windows NTFS permissions system is an excellent resource for managing user privileges over file resources, allowing you to adjust options for what a user can do and what they can access.

Currently the NTFS protocol is well designed, no serious security problems have been reported and the default configurations are not excessively relaxed, but it is necessary to understand Windows user groups.

Windows users

- Administrator: Has absolute control of the system, it cannot be deleted, it is disabled by default, although if it is started in safe mode, it will be enabled.
- Guest: Allows access to the computer over the network, if there are shared resources, without the need for a username and password, although with restricted privileges, it is disabled by default.
- Initial User: This is the user that is created during the operating system installation process and is assigned to the administrators group.

There are other special operating system accounts that Microsoft Windows uses to run services.

Windows users

Special Microsoft Windows accounts are:

- System: Belongs to the administrators group and has all privileges on the system. An administrator could execute with system privileges through the at command, a task will be created that runs as system. Nothing running under system is shown on the screen, you would have to use psexec from sysinternals: **psexec –i –s cmd.exe**
- LocalService: Presents anonymous credentials on the network, has low privileges and has presentation permission on the system.
- NetworkService: Acts as the system on the network.

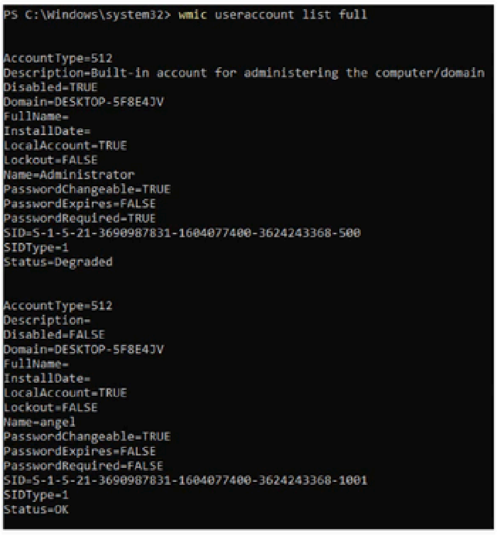
It is possible to list user accounts in Windows with the following command: **wmic useraccount list full**

Demo

These commands allow you to verify characteristics of users and groups.

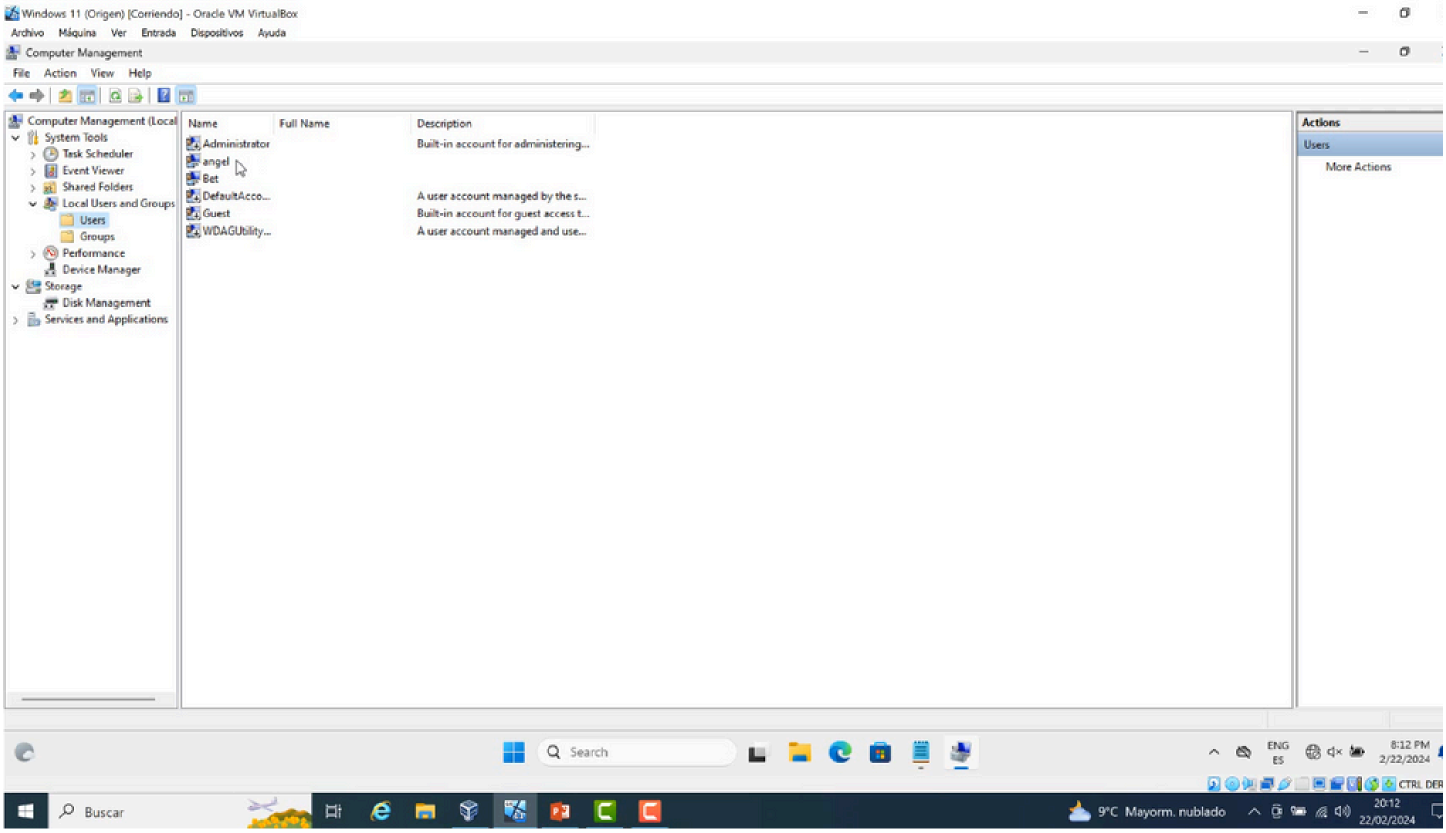
```
whoami /all
whoami /groups
wmic useraccount list full
```

From the **computer administrator** you can consult the groups or properties section of a specific user.

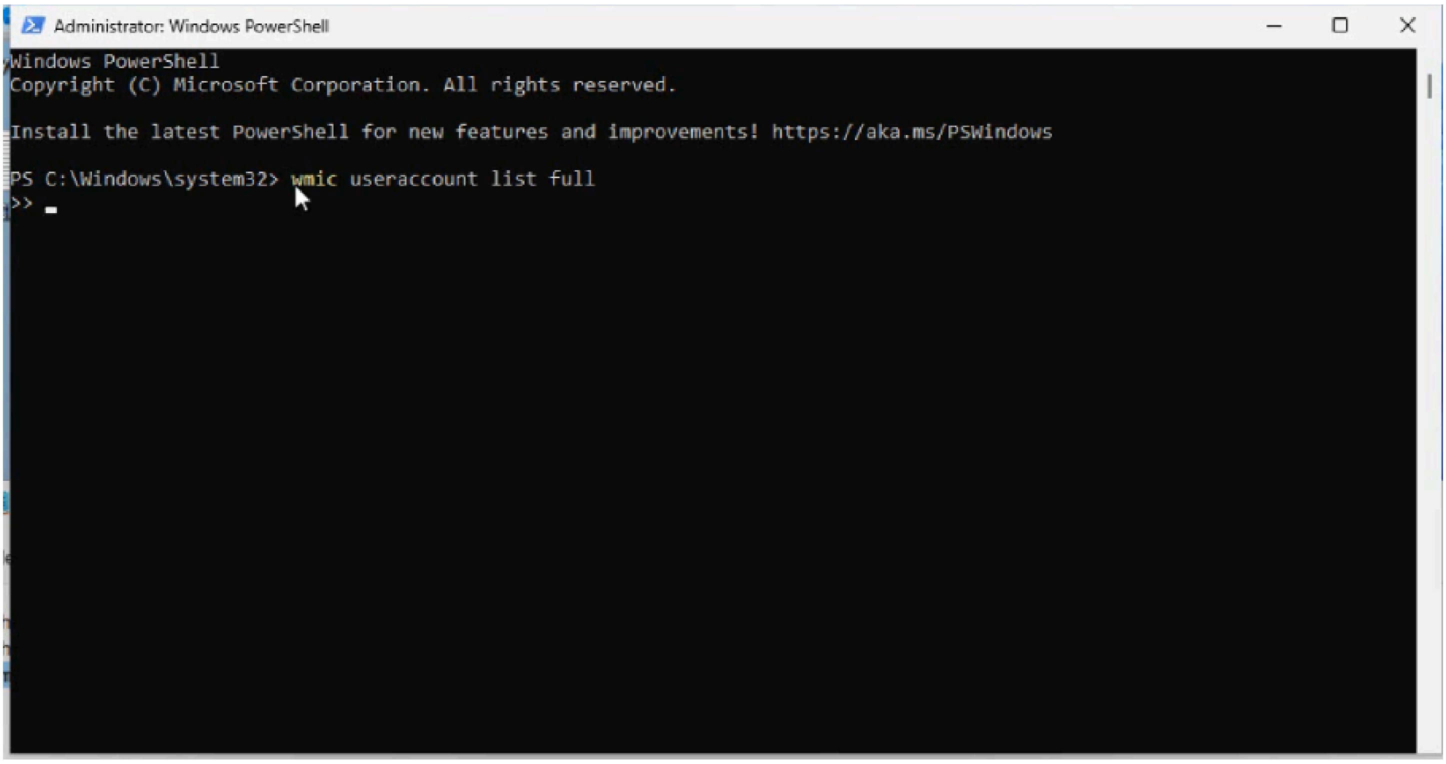


```
PS C:\Windows\system32> wmic useraccount list full


AccountType=512
Description=Built-in account for administering the computer/domain
Disabled=TRUE
Domain=DESKTOP-5F8E4JV
FullName=
InstallDate=
LocalAccount=TRUE
Lockout=FALSE
Name=Administrator
PasswordChangeable=TRUE
PasswordExpires=FALSE
PasswordRequired=TRUE
SID=S-1-5-21-3690987831-1604077400-3624243368-500
SIDType=1
Status=Degraded


AccountType=512
Description=
Disabled=FALSE
Domain=DESKTOP-5F8E4JV
FullName=
InstallDate=
LocalAccount=TRUE
Lockout=FALSE
Name=angel
PasswordChangeable=TRUE
PasswordExpires=FALSE
PasswordRequired=FALSE
SID=S-1-5-21-3690987831-1604077400-3624243368-1001
SIDType=1
Status=OK
```

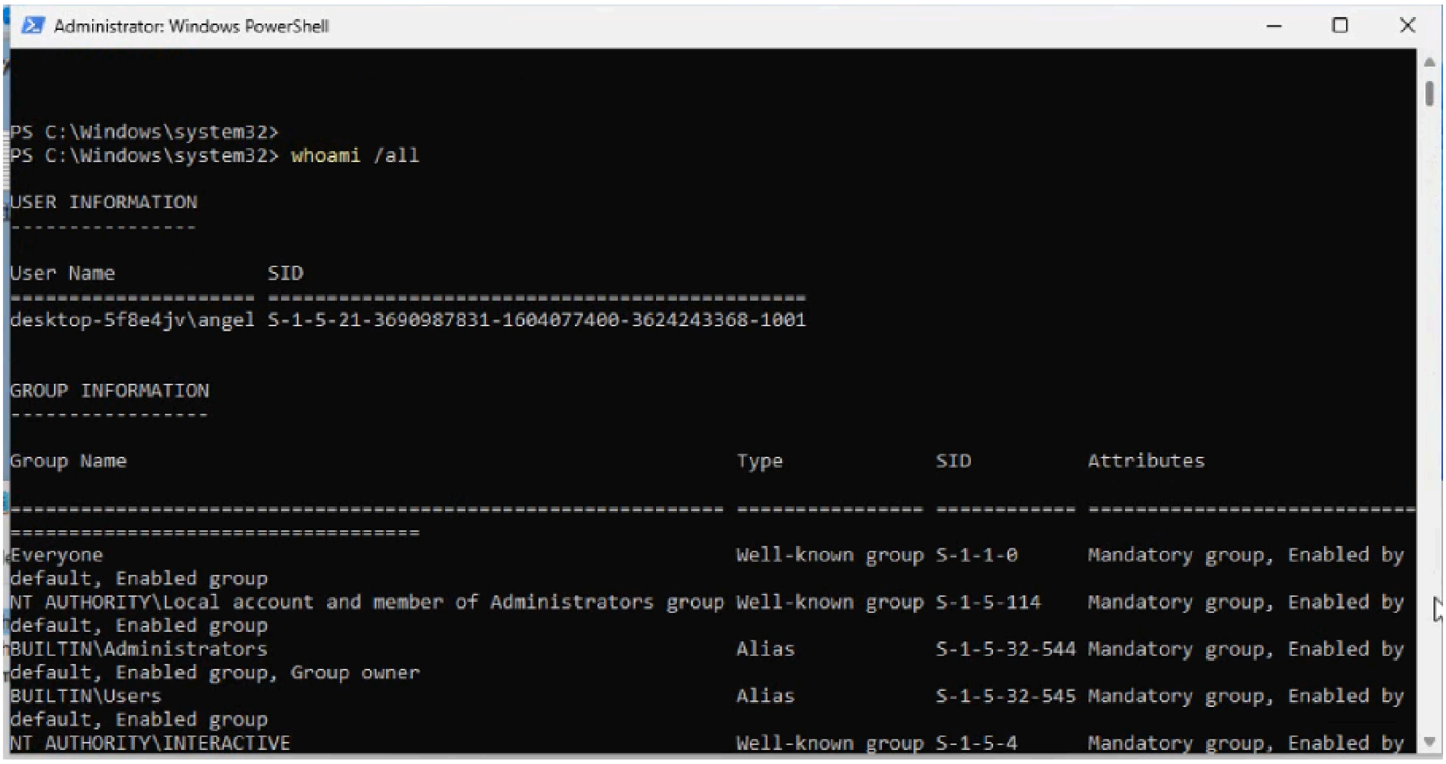
Pictures own elaboration



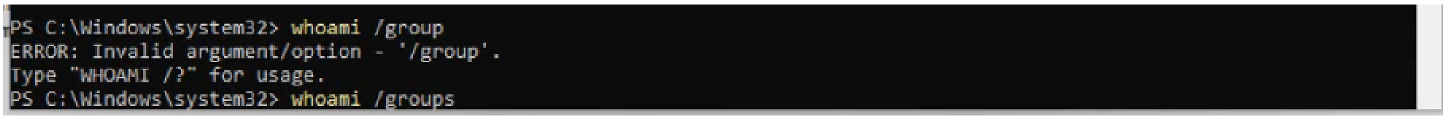
Name	Full Name	Description
Administrator		Built-in account for administering...
angel		
Bet		
DefaultAcco...		A user account managed by the s...
Guest		Built-in account for guest access t...
WDAGUtility...		A user account managed and use...



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Windows\system32> wmic useraccount list full
>>
```



```
PS C:\Windows\system32>
PS C:\Windows\system32> whoami /all

USER INFORMATION
----------------

User Name            SID
==================== ==============================================
desktop-5f8e4jv\angel S-1-5-21-3690987831-1604077400-3624243368-1001


GROUP INFORMATION
-----------------

Group Name                                                    Type             SID          Attributes

============================================================= ================ ============ ==============================
==================================
Everyone                                                      Well-known group S-1-1-0      Mandatory group, Enabled by
default, Enabled group
NT AUTHORITY\Local account and member of Administrators group Well-known group S-1-5-114    Mandatory group, Enabled by
default, Enabled group
BUILTIN\Administrators                                        Alias            S-1-5-32-544 Mandatory group, Enabled by
default, Enabled group, Group owner
BUILTIN\Users                                                 Alias            S-1-5-32-545 Mandatory group, Enabled by
default, Enabled group
NT AUTHORITY\INTERACTIVE                                      Well-known group S-1-5-4      Mandatory group, Enabled by
```



```
PS C:\Windows\system32> whoami /group
ERROR: Invalid argument/option - '/group'.
Type "WHOAMI /?" for usage.
PS C:\Windows\system32> whoami /groups
```

NTFS and ACLs

In the NTFS file system, Access Control Lists define the permissions that users, groups, or programs have on objects.

There are three types of access control lists:

- DACL: They are discretionary, defined by the administrator or owner of the object.
- MACL: Mandatory, predefined by the system and not under the control of the user or owner of an object, there is no graphical way to establish or manage them.
- SACL: System rules, allow auditing access to objects.

NTFS permissions

The permission system can be managed graphically with the properties of the objects in the security tab, by command line with icacls.

The correct way to work with security permissions is to configure allow permissions, if something is not allowed it has an implicit deny, deny permissions are only assigned in very specific situations, because they take precedence over allowed permissions.

The recommendation is to assign permissions to groups, rather than users, and to folders instead of files, allowing for more efficient administration.

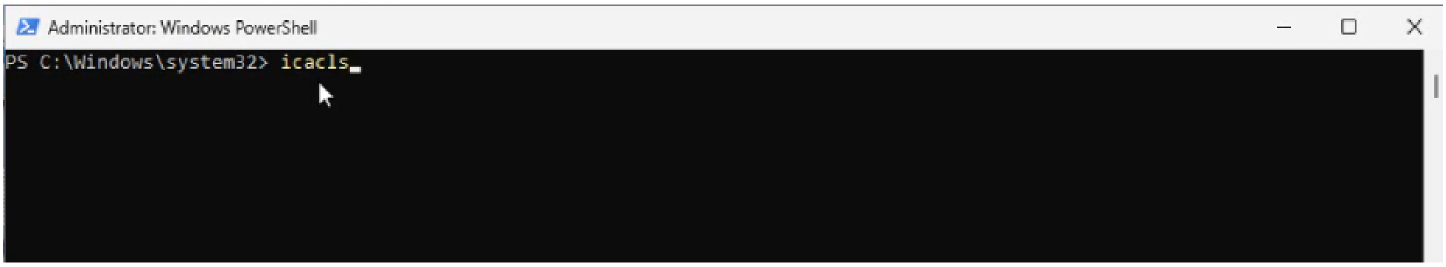
NTFS permissions

Moving or copying files between volumes with NTFS systems allows you to preserve the object's own permissions, although not the inherited permissions. You can also modify or configure the inheritance of permissions for a certain object.

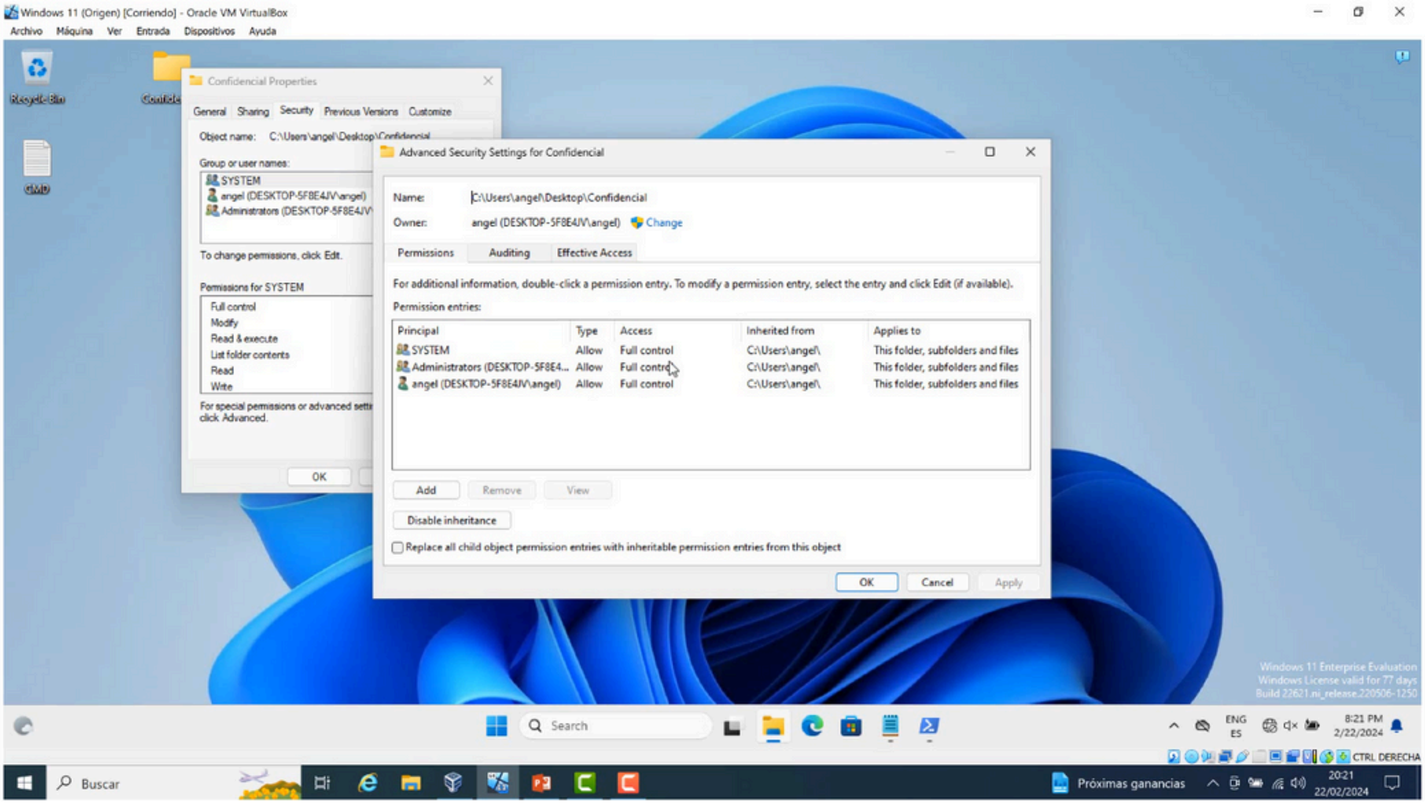
Additionally, the effective permissions or effective access tab offers the possibility of auditing the access of a specific user, depending on the groups to which they belong and the different permissions assigned.

Demo

- Check permissions from the graphical environment
- Revise icacls options



```
PS C:\Windows\system32> icacls
```


Windows 11 (Origen) [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Recycle Bin
CMD
Confidencial Properties
General Sharing Security Previous Versions Customize
Advanced Security Settings for Confidencial
Permissions Auditing Effective Access
Add Remove View
Disable inheritance
OK Cancel Apply
Search
Buscar
Próximas ganancias

Object name: C:\Users\angel\Desktop\Confidencial

Group or user names:
- SYSTEM
- angel (DESKTOP-5F8E4JV\angel)
- Administrators (DESKTOP-5F8E4JV\

To change permissions, click Edit.

Permissions for SYSTEM
- Full control
- Modify
- Read & execute
- List folder contents
- Read
- Write

For special permissions or advanced setti click Advanced.

Name: C:\Users\angel\Desktop\Confidencial

Owner: angel (DESKTOP-5F8E4JV\angel) Change

For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).

Permission entries:

Principal	Type	Access	Inherited from	Applies to
SYSTEM	Allow	Full control	C:\Users\angel\	This folder, subfolders and files
Administrators (DESKTOP-5F8E4...	Allow	Full control	C:\Users\angel\	This folder, subfolders and files
angel (DESKTOP-5F8E4JV\angel)	Allow	Full control	C:\Users\angel\	This folder, subfolders and files

☐ Replace all child object permission entries with inheritable permission entries from this object

Windows 11 Enterprise Evaluation
Windows License valid for 77 days
Build 22621.ni_release.220506-1250

8:21 PM 2/22/2024

20:21 22/02/2024

Conclusions

- Identity management and a good knowledge of the groups assigned to users, together with permission administration on system objects, offer us an efficient mechanism to correctly manage access to data, services and devices.
- It is essential to understand the characteristics and details of all these elements to maintain levels of security in the NTFS file system and Windows objects.