1 Permisos básicos de ficheiros e carpetas

Moitas veces precísase restrinxir o acceso a unha carpeta ou ficheiro a unha serie de usuarios ou grupos. Nesta sección veremos como facelo.

1.1 Sumario

- 1 Introdución aos permisos
  - 1.1 Usuario e grupo propietario
  - 1.2 Permisos básicos
- 2 Modificar os permisos
  - 2.1 Abrir como administrador (*root*)
- 3 Afinar permisos nunha estrutura de carpetas
  - 3.1 Introdución: *pensar*
  - 3.2 Crear a estrutura de carpetas: *facer*
  - 3.3 Afinar permisos das carpetas home dos usuarios: *facer*
  - 3.4 Conclusión
- 4 Listas de control de acceso: ACL
  - 4.1 Instalar Eiciel e activar as ACLs
  - 4.2 Afinar os permisos con ACL
- 5 Comandos para a configuración dos permisos
- 6 Permisos dunha unidade Windows

1.2 Introdución aos permisos

Lémbrense os usuarios creados en pasos previos.

```
Nome           Nome real              Grupo primario  Grupo secundario        Perfil

administrador  administrador          administrador   sudo, ...               Administrador
carlos         Carlos Carrión         g-profes        g-usuarios, ...         Estándar (Usuario de escritorio)
noa            Profe- Noa Pin Pin     g-profes        g-usuarios, sudo, ...   Administrador
roi            Roi Paz Paz            g-alum          g-usuarios, ...         Estándar (Usuario de escritorio)
```

Con respecto ao que se fixo en pasos previos, modificouse o usuario *carlos*: establecendo como grupo primario **g-profes**, e como grupo secundario **g-usuarios**.

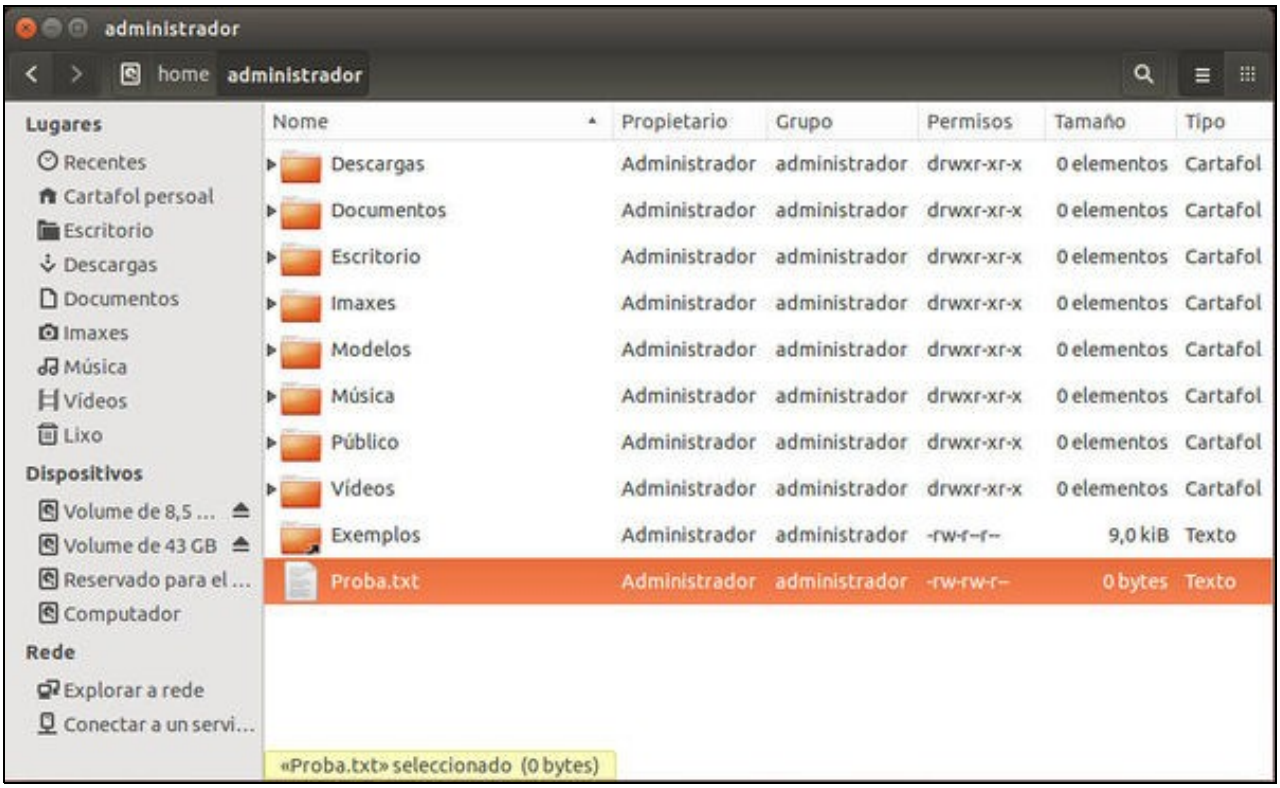
Noa e *Carlos* parécense en que pertencen ao grupo *g-profes*, pero *noa* pode administrar o sistema e *carlos* non. Nese senso o usuario profesor *carlos* e o usuario alumno *roi*, teñen os mesmos poucos privilexios.

A usuaria *noa* pode administrar o sistema ao igual que o usuario chamado *administrador*, pero este último non pertence nin ao grupo *g-profes* nin *g-usuarios*.

Ao grupo *g-usuarios* só pertencen os usuarios: *carlos*, *noa* e *roi*.

1.2.1 Usuario e grupo propietario

Toda carpeta e todo ficheiro teñen un **usuario propietario** e un **grupo propietario** do mesmo:



Entrouse no sistema como a usuaria *noa*. Esta usuaria accedeu á carpeta do usuario *administrador*. Usa a visualización en formato lista, engade as columnas: propietario, grupo e permisos e súbeos para enriba na lista. (véxase unha sección anterior para mirar como configurar *nautilus* con esta visualización).

Na imaxe obsérvase que o **usuario propietario** de cada carpeta e arquivo é o usuario *administrador*.

O **grupo propietario** é o grupo chamado *administrador*.

Cando un usuario crea unha carpeta/ficheiro:

- Quen é o **usuario propietario**?: O usuario que a creou
- Quen é o **grupo propietario**?: O *grupo principal* ao que pertence ese usuario.

Aínda así, o **grupo propietario** pódese cambiar despois a calquera outro grupo, aínda que o usuario non teña nada que ver con el.

1.2.2 Permisos básicos

Os **permisos básicos** en GNU/Linux son moi sinxelos, e por tanto presentan como veremos algunhas limitacións. Nesta sección estudarase o xusto para que se entenda o seu funcionamento.

A unha carpeta ou ficheiro pódenselle adxudicar permisos a tres tipos de usuarios:

- **Usuario propietario** (U).
- **Grupo propietario** (G), que non ten porque ser grupo principal do usuario propietario.
- **Outros** (O), que non sexa o *usuario propietario* nin ningún usuario que pertenza ao *grupo propietario*.

Os permisos seguen un patrón coñecido como **UGO**: usuario, grupo e outros.

Existen tres permisos independentes:

```
Permiso              Ficheiro                  Carpeta
r  (Read)            Ver contido               Ver o contido
w (Write)            Escribir/modificar        Crear/modificar obxectos
x  (eXecute)         Executar                  Acceder á carpeta (sen ver  o contido).
```

A cada tipo de usuario pódeselle asignar unha combinación dos tres permisos anteriores. Por exemplo para o usuario propietario, sobre un ficheiro, poderíanse asignar calquera das combinacións seguintes:

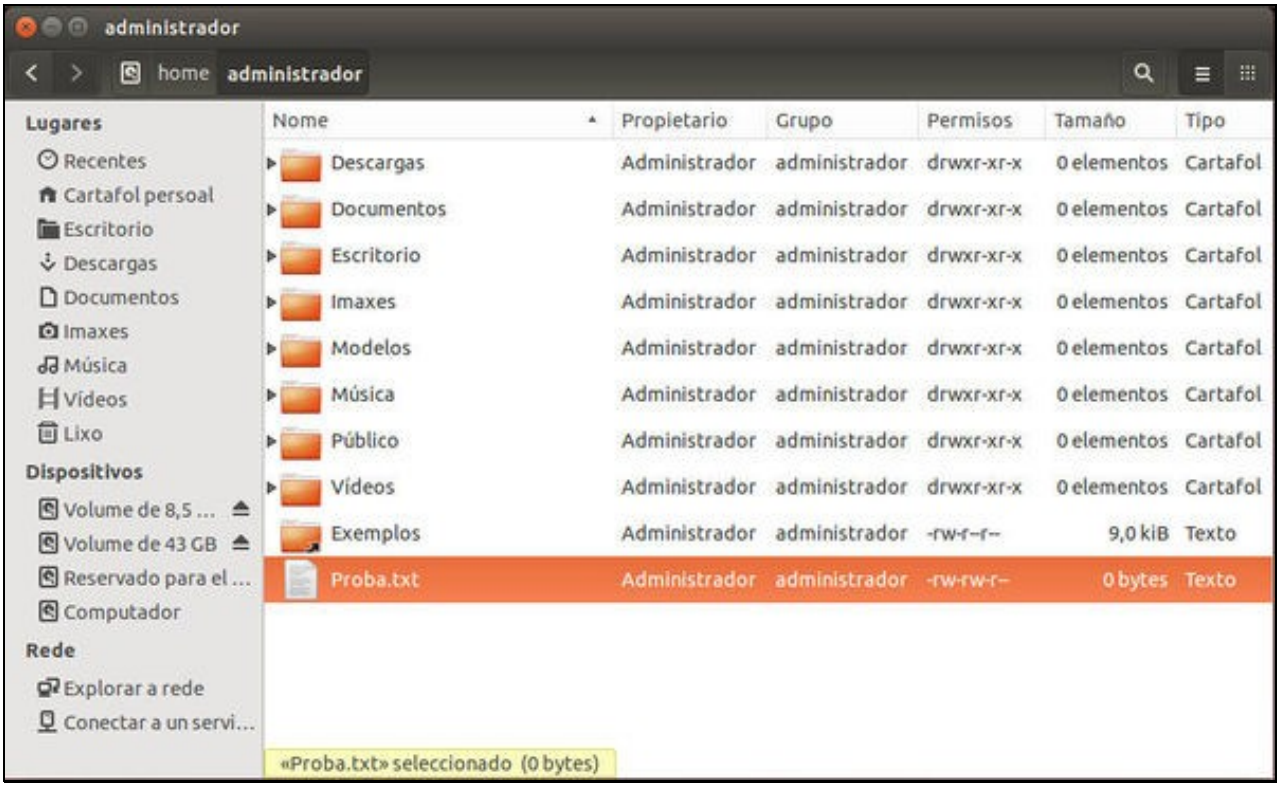
```
- - -   Ningún permiso. O usuario non pode facer nada co arquivo.
- - x   Pode executar o ficheiro, se é executable. Non pode modificalo nin ver o seu contido.
- w -   Pode modificar o arquivo (engadirlle/extraerlle contido). Non pode executalo nin velo.
- w x   Pode executar e modificar o ficheiro pero non pode velo.
r - -   Pode ver o contido do ficheiro, pero non modificalo nin executalo.
r ? x   Pode ver o contido e executar o ficheiro. Non pode modificalo.
r w -   Pode ver o contido e modificalo ficheiro. Non pode executalo.
r w x   O usuario pode, ver o contido do ficheiro, modificalo e executalo se é un arquivo executable.
```

A alguén asaltaralle a dúbida de como poder modificar un ficheiro sen poder ver o seu contido. Pois si se pode, existen comandos para iso, pero escápanse aos obxectivos que se perseguen neste material.

TAMÉN PODES VER...

Neste enlace podes afondar máis no coñecemento dos permisos básicos en GNU/Linux

Volvamos sobre a imaxe anterior:



Na columna permisos vese que a secuencia comeza cunha *letra* ou un *guión*:

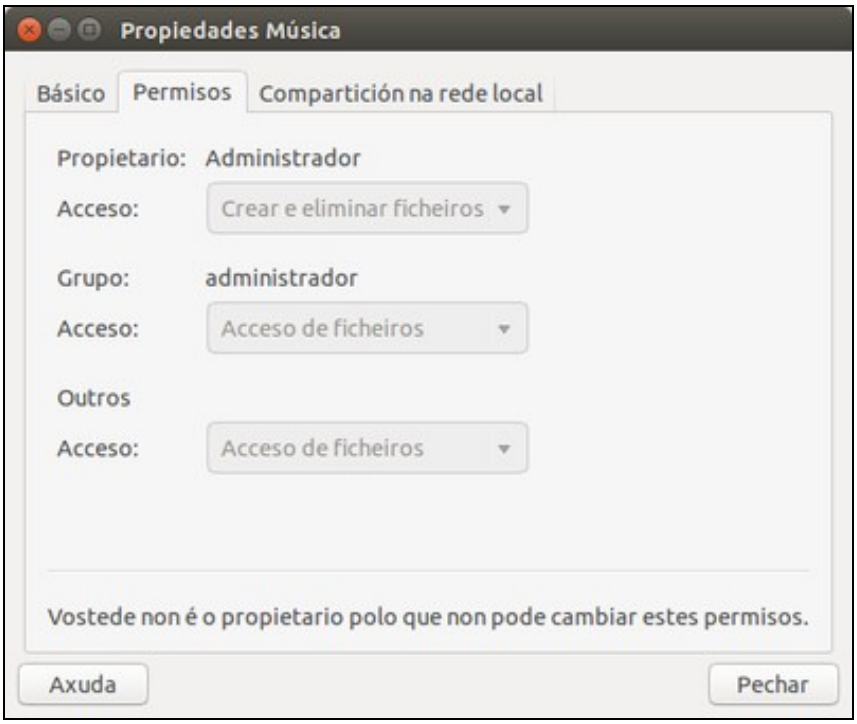
- **l**:*link*, enlace, acceso a un directorio
- **d**:*directory*, directorio, carpeta
- **-**: arquivo, ficheiro

A continuación séguelle tres grupos de permisos. Véxase por exemplo a carpeta *Música*:

- **drwxr-xr-x**:
    - **d**:indica que é unha carpeta (directorio).
    - **rwx**: os 3 primeiros permisos corresponden ao *usuario propietario* (**U**) (administrador). Este pode facer de todo.
    - **r-x**: os 3 segundos permisos corresponden ao *grupo propietario* (**G**) (administrador). Calquera usuario que pertenza a este grupo pode ver o contido e acceder á carpeta *Música*.
    - **r-x**: os 3 últimos permisos corresponden a todos os demais usuarios, outros (O): (roi, noa, carlos). Neste exemplo en *Música* poden ver o seu contido e acceder a ela.

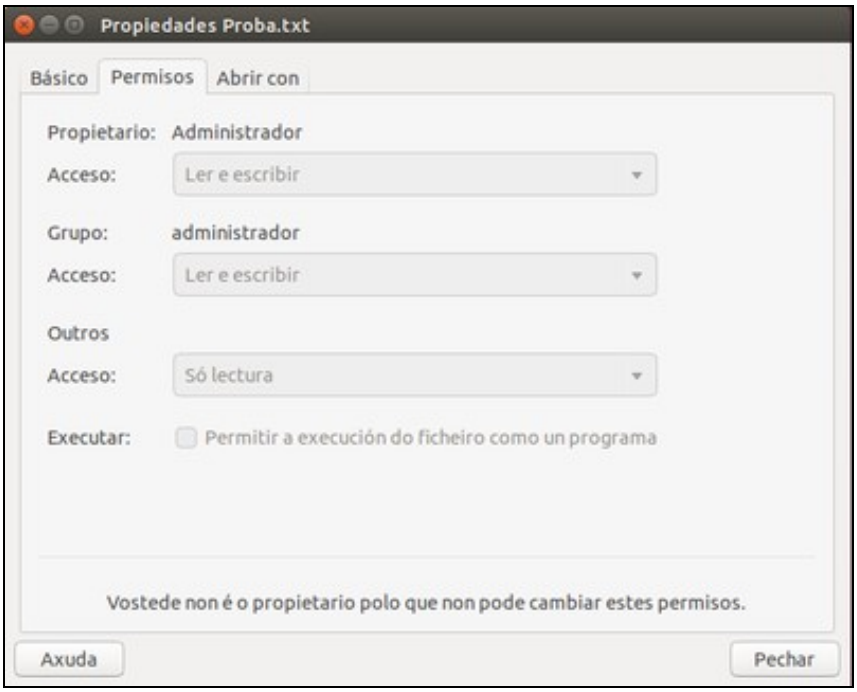
Por hoxe, xa está ben de texto e comecemos co modo gráfico.

A imaxe seguinte amosa os permisos da carpeta *Música* en modo gráfico (botón dereito sobre ela e seleccionar *Propiedades*):



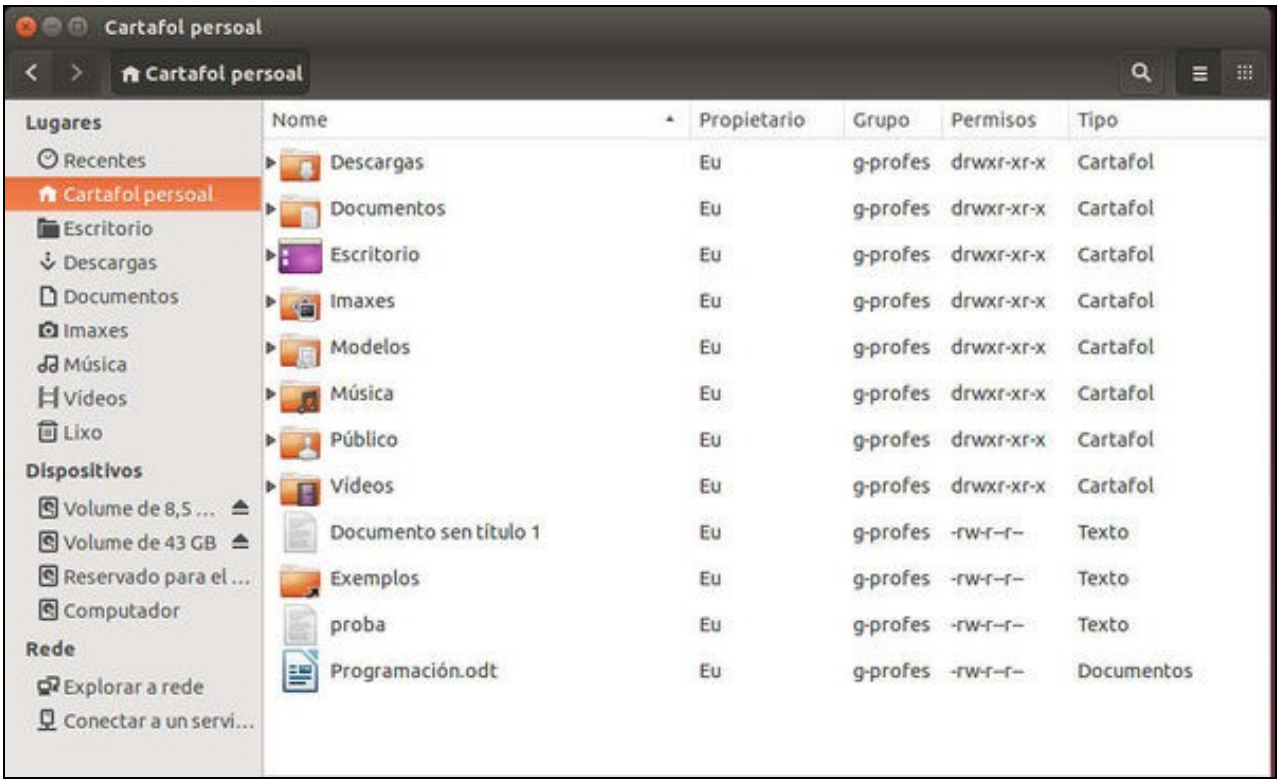
Como se pode observar, *noa* (lémbrese que é noa quen está fozando nas intimidades do usuario *administrador*), non pode realizar ningún cambio, pois ela non é a dona da carpeta. Só dous usuarios poden cambiar os permisos dunha carpeta/ficheiro: o *creador* e o usuario *root*, como se verá máis adiante.

Finalmente, observar os permisos dun arquivo. *Noa* segue sen poder facer nada, pois non é a dona do arquivo.



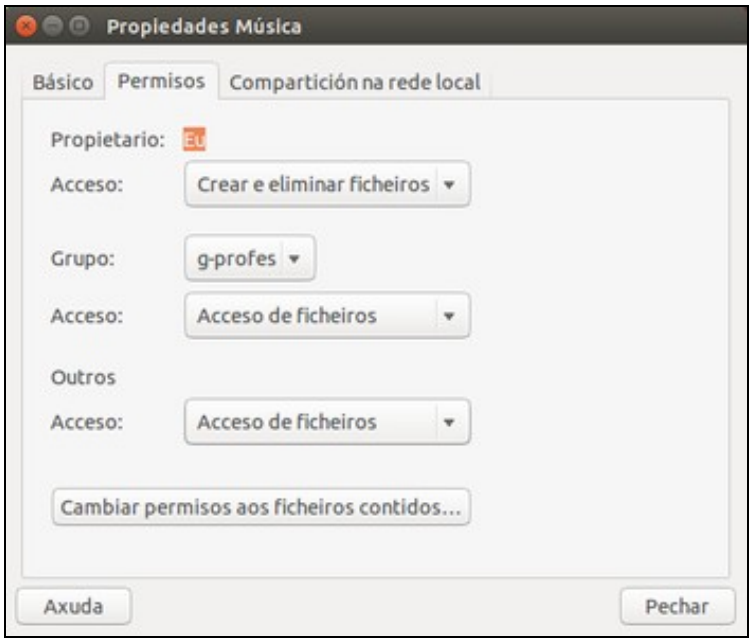
1.3 Modificar os permisos

Noa volve á súa carpeta.

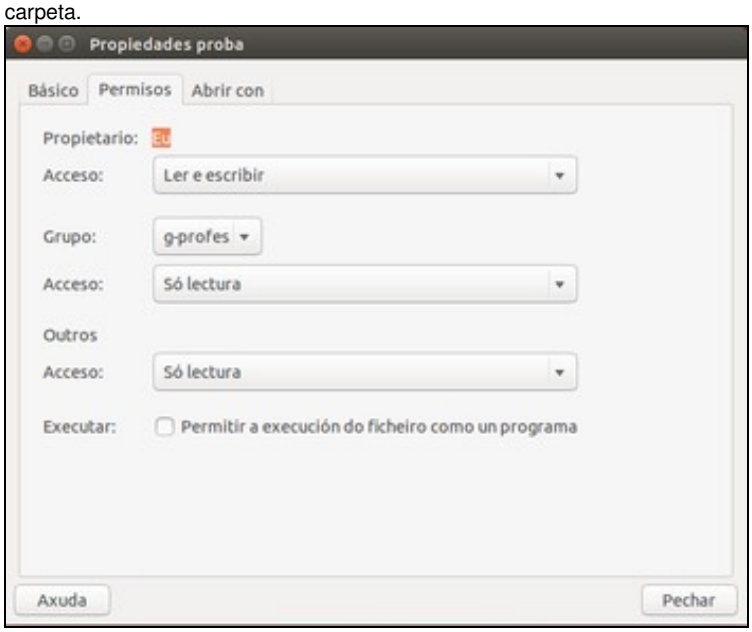


Notar que o **grupo propietario** en cada un dos obxectos é *g-profes*, e o usuario *carlos* tamén pertence a el.

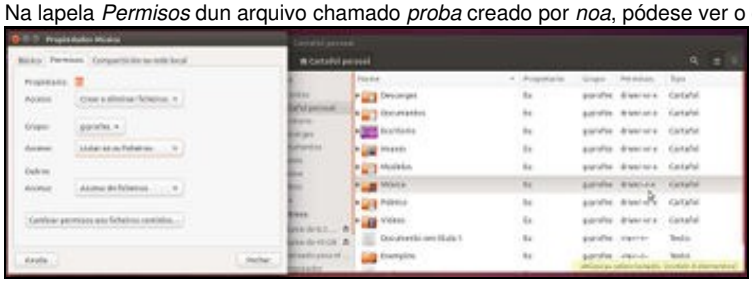
- Cambiar permisos

- 

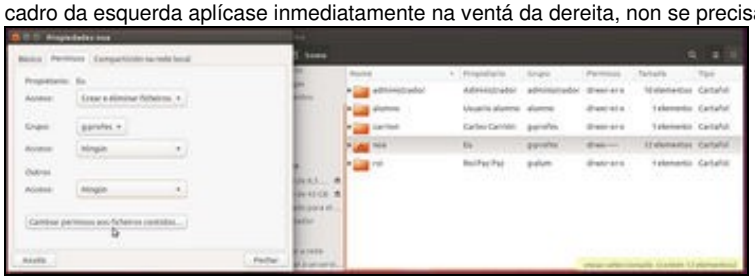
Na lapela *Permisos* da carpeta *Música* da usuaria *noa*, pódese observar que o *usuario propietario* é ela mesma. Nese cartafol, noa ten ós máximos permisos (*crear e eliminar ficheiros*, *rwx*). O *grupo propietario* é *g-profes*. Calquera que pertenza a ese grupo (por exemplo *carlos*) pode acceder ós ficheiros contidos nesa carpeta. Calquera *outro usuario* distinto dos anteriores tamén pode acceder aos ficheiros desa carpeta.

- 

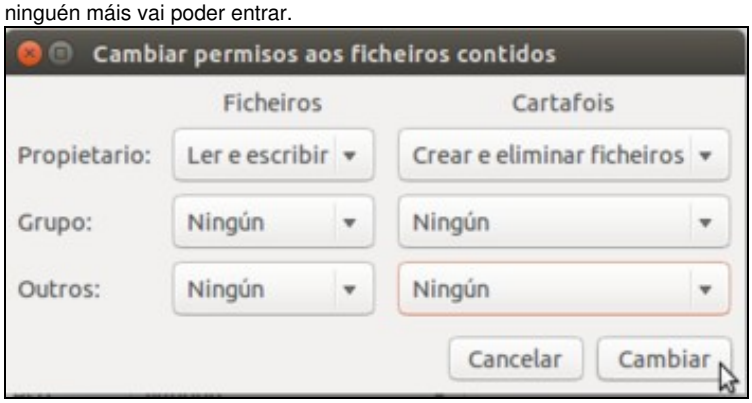
Na lapela *Permisos* dun arquivo chamado *proba* creado por *noa*, pódese ver o que pode facer todo o mundo, por defecto, con ese arquivo.

- 

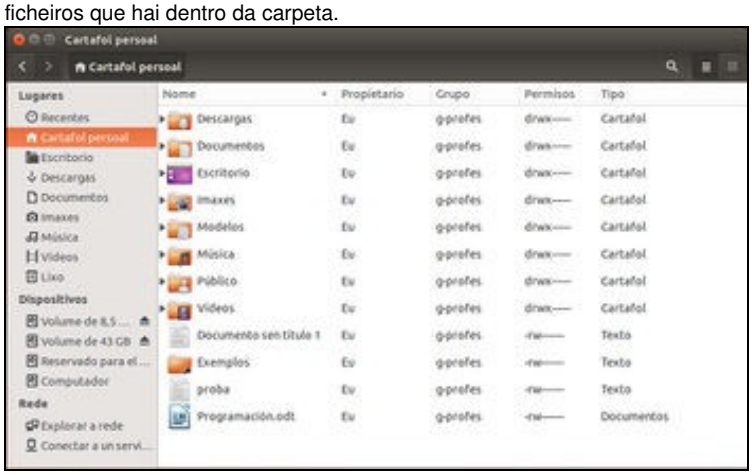
Na imaxe, pódese ver o resultado de aplicar os permisos *Listar só os ficheiros* para g-profes. (rwx r-- r-x). Calquera cambio que se faga no cadro da esquerda aplícase inmediatamente na ventá da dereita, non se precisa pechar para ver o resultado.

- 

Na ventá da dereita fixarse, que permisos hai, por defecto, sobre cada carpeta de usuario. Calquera pode entrar a fisgar na carpeta de calquera usuario. Para solucionar iso, noa decide que só ela vai ter acceso á súa carpeta. Pero ademais tamén configura os permisos que deben ter todos os ficheiros que hai dentro da carpeta, e propaga eses permisos a todo ficheiro e carpeta que haxa dentro de *noa*. Isto último non sería preciso se só se quere que ninguén máis para acceda a carpeta de *noa*, con configurar a carpeta raíz *noa*, xa é suficiente, xa ninguén máis vai poder entrar.

- 

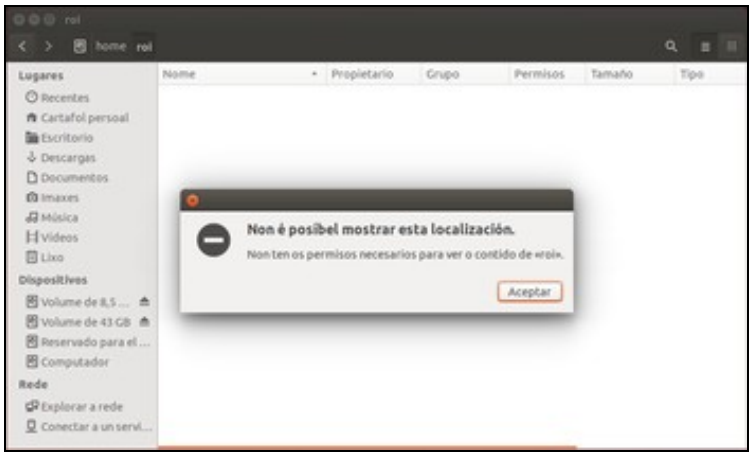
Ao picar no botón para cambiar os permisos dos contidos, teremos que indicar os permisos que queremos establecer para as carpetas e ficheiros que hai dentro da carpeta.

- 

O resultado da acción anterior produciu que os permisos da carpeta *nai noa* se propagaran ás carpetas/ficheiros *fillos*. Observar que noa non pode cambiar o propietario da carpeta (isto ten lóxica, se *noa* ten unha carpeta, por exemplo, con contido *comprometido* non sería xusto que lle pasase a propiedade (*o problema*) a outro usuario), aínda que si pode cambiarlle o *grupo propietario* para un grupo ao que ela pertenza, como por exemplo *g-usuarios*. **CONCLUSIÓN:** *noa* pode cambiar os permisos, pero non a propiedade das carpetas/ficheiros das que é dona.

-

A imaxe, amosa que *roi* tamén cambiou os permisos. Roi entrou no sistema e cambiou os permisos só da carpeta *roi*, sen propagar.

- 

Noa entra no sistema. Non pode entrar na carpeta de *roi*. Nin pode abrir a carpeta, nin en propiedades pode cambiar os permisos. Pero como podería facer *noa* iso sobre carpetas nas que non é dona?.

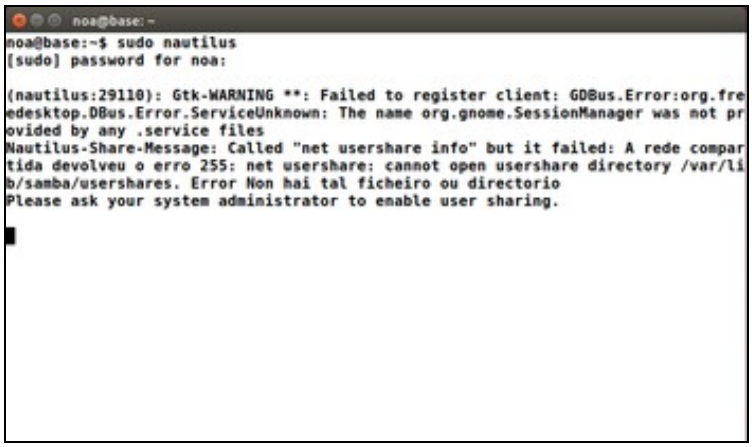
1.3.1 Abrir como administrador (*root*)

Ós únicos que poden cambiar os permisos dun ficheiro/carpeta son o seu dono e o usuario *root*. E o único que pode cambiar as propiedades dun ficheiro/carpeta é o usuario *root*.

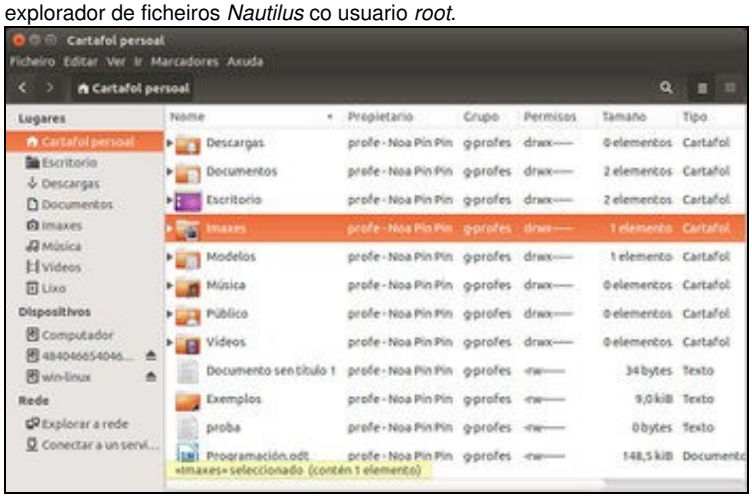
Así que se *noa* quere cambiar os permisos de ficheiros ou carpetas das que non é dona, o que pode facer é iniciar o explorador de ficheiros *Nautilus* como usuario *root* (Lémbrese que nun apartado anterior explicamos como executar comandos como *root* usando o comando *sudo*)

- Abrir como *root*
-

Iniciamos a aplicación **Terminal**.

- 

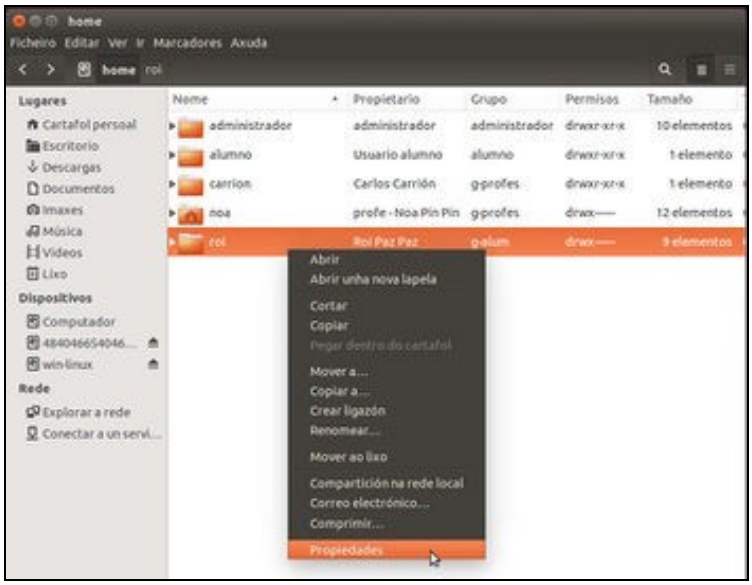
Introducimos o comando **sudo nautilus**. Teremos que introducir de novo o contrasinal de *noa*, e desta forma estamos executando o explorador de ficheiros *Nautilus* co usuario *root*.

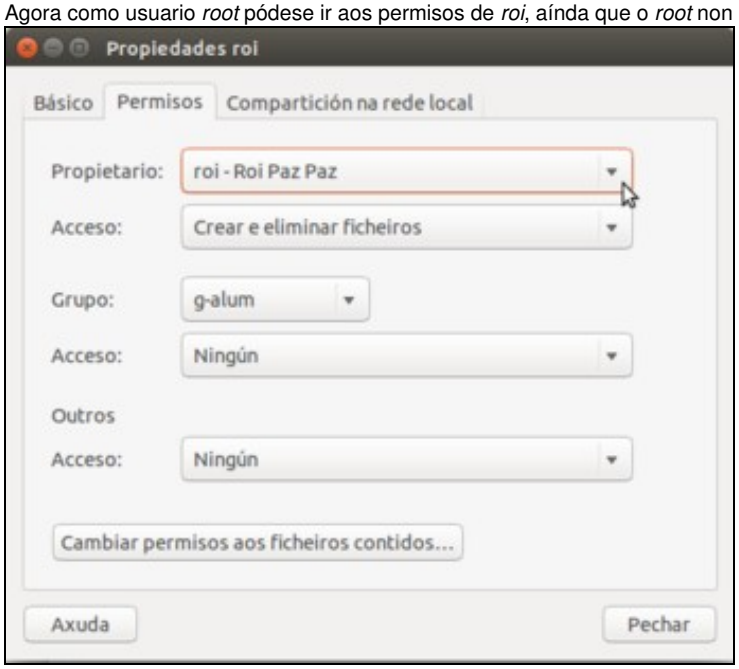
- 

Aínda que como carpeta persoal aparece a carpeta de *noa*, podemos comprobar que agora non estamos executando o navegador de ficheiros co usuario *noa*, xa que no propietario do ficheiro vemos *profe - Noa Pin Pin* en lugar de *Eu*.

-

O usuario *root* mirando a carpeta de *roi* (Lémbrese que co usuario *noa* non podíamos facelo).

- 

Agora como usuario *root* pódese ir aos permisos de *roi*, aínda que o *root* non pertenza a *g-alum* nin sexa o propietario da carpeta *roi*.
- 

Agora si que o usuario *root* pode cambiar de todo, permisos e propietarios.

1.4 Afinar permisos nunha estrutura de carpetas

Crear toda unha árbore de carpetas, nas que os profes poidan facer unhas cousas, os alumnos outras, etc, etc, é materia dun manual de administración. Pero aínda así, imos ver unha estrutura simple na que os profes poidan intercambiar información cos seus alumnos.

1.4.1 Introdución: *pensar*

Como sempre, aplicaremos a regra baseada no Principio de Pareto e moi usado polo americanos **80% think, 20% do** (80% pensar, 20% facer).

Preténdese:

- 1º.- Que ás carpetas *home* de cada alumno poidan entrar os profesores para ver o seu contido.
- 2º.- Que só o alumno en cuestión poida escribir/modificar na súa propia *home*.
- 3º.- Que á carpeta *home* de cada profesor só poida acceder o profesor en cuestión.
- 4º.- Que haxa un espazo comun nos que os profesores que accedan poidan crear *cousas propias de profes*. Que só poidan acceder os profes.
- 5º.- Que haxa un espazo común onde os profes poidan deixar material para o alumnado, e que este poida acceder e recollelo, pero non modificalo nin escribir.

Lémbrense os usuarios que existen e os grupos aos que pertencen

Nome	Nome real	Grupo primario	Grupo secundario	Perfil
administrador	administrador	administrador	sudo, ...	Administrador
carlos	Carlos Carrión	g-profes	g-usuarios, ...	Estándar (Usuario de escritorio)
noa	Profe- Noa Pin Pin	g-profes	g-usuarios, sudo, ...	Administrador
roi	Roi Paz Paz	g-alum	g-usuarios, ...	Estándar (Usuario de escritorio)

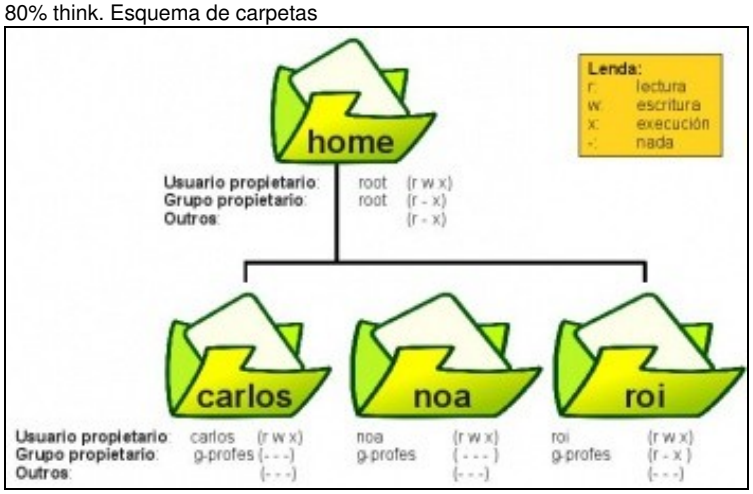
O grupo *g-usuarios* ten como membros a: *carlos, noa, roi*.

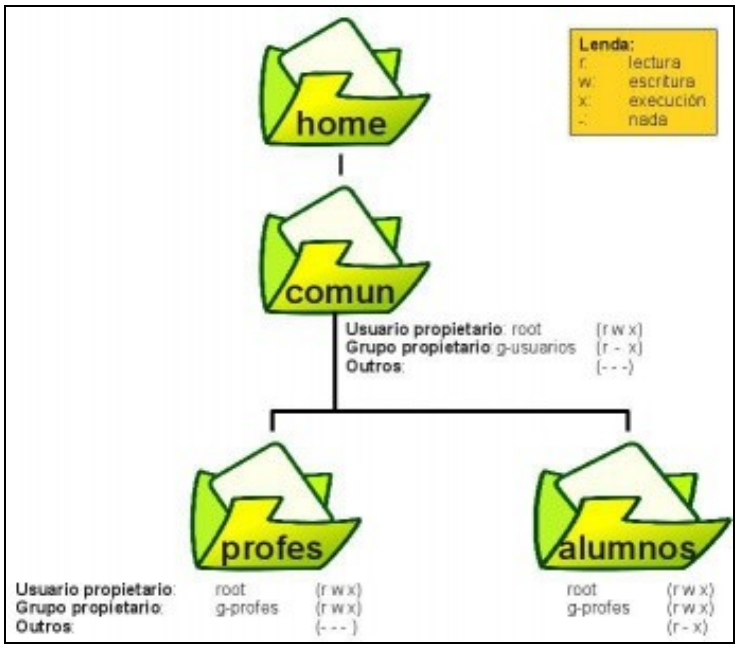
O grupo *g-profes* ten como membros a: *carlos, noa*.

O grupo *g-alum* ten como membros a: *roi*.

O usuario *administrador* non pertence a ningún dos tres grupos anteriores.

Véxase graficamente o que se pretende. Isto non ten moito senso se se trata de 20 ordenadores e en todos se realiza o mesmo. O bo sería que logo isto estivese compartido para usar dende outro equipo. Verase na seguinte sección.

- 80% think. Esquema de carpetas
- 

Na carpeta */home* todo **usuario profesor** terá a súa carpeta a que só el poderá acceder, e todo **usuario alumno** terá a súa carpeta á que só o alumno poderá acceder para realizar o que desexe. Interesa que ás carpetas dos usuarios alumnos os profesores poidan acceder en modo lectura e execución.
- 

Na carpeta */home* crearase unha carpeta chamada **comun**, á que poidan acceder todos os que pertenzan ao grupo *g-usuarios* en modo lectura/execución (o usuario *administrador* non vai poder acceder e os demais non van poder crear nada dentro de /**home**/**comun**). Na

carpeta **profes**, poderán acceder os usuarios que pertenzan ao grupo *g-profes* e realizar o que desexen. O mesmo sucederá na carpeta /**home**/**comun**/**alumnos**, pero ademais os **outros** (aqueles que pasaron o filtro de **g-usuarios** en /**home**/**comun**) poderán acceder para Ler/Executar. Os **outros**, neste caso que se está a ver, é o usuario alumno *roi*.

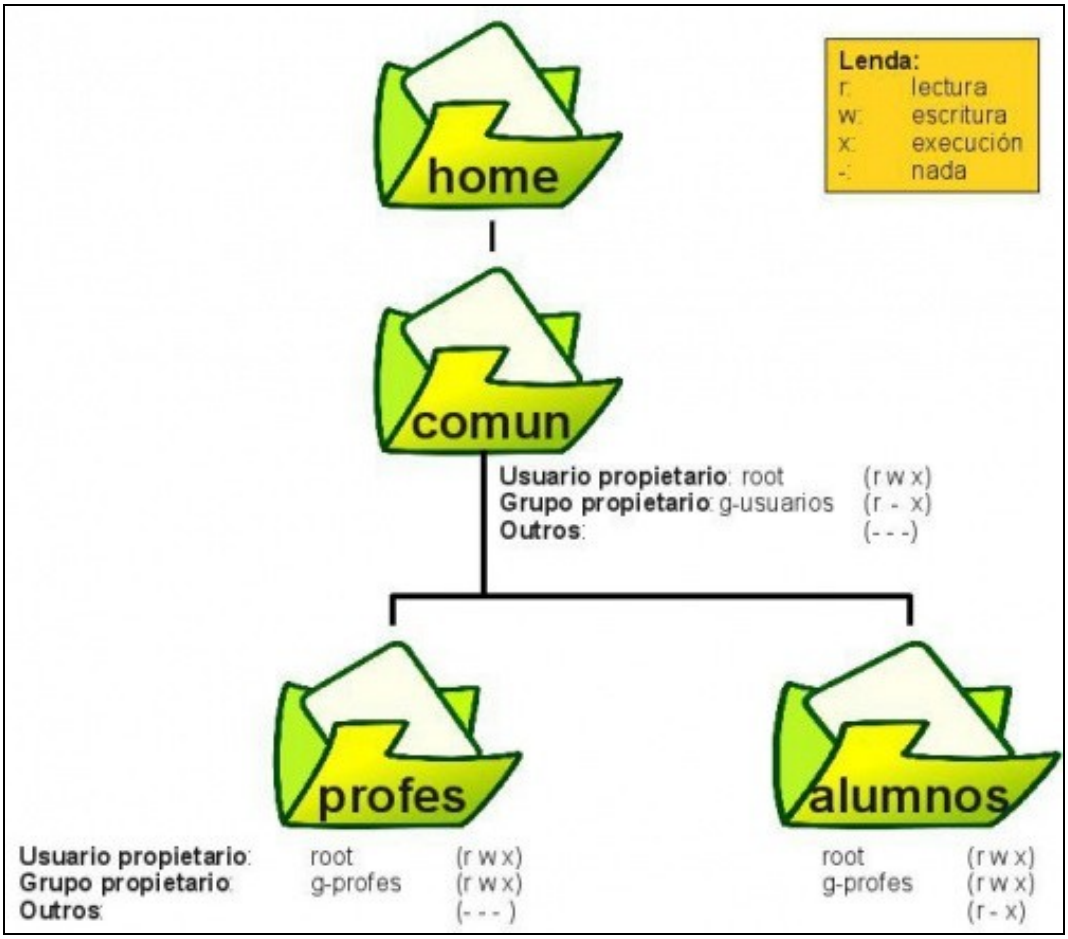
Un pouco enrevesado, verdade?. Pois si, porque estes son os permisos básicos, nun curso de administración poderíanse ver ferramentas de afine máis precisas como as ACL (Listas de Control de Acceso) e a súa flexibilidade, como se comentará despois.

Xa se fixo o 80% (*think*, pensar), pásese ó 20% (*do*, facer)

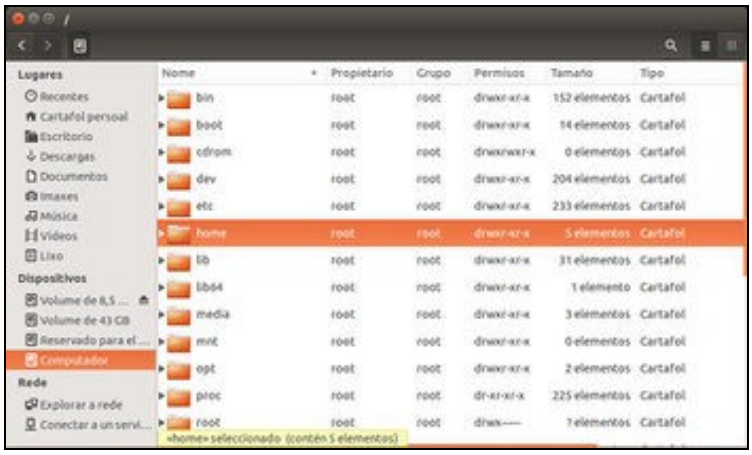
1.4.2 Crear a estrutura de carpetas: *facer*

Vaise comezar por crear /**home**/**comun** e súa estrutura.

A imaxe é unha *maqueta/plano* do que se pretende:



- 20% do. Carpetas de comun

- 

Mirar os permisos e os propietarios de */home*. A usuaria que iniciou a sesión é *noa*. **root** é o dono e pode (rwx), o grupo propietario é *root* e pode (r-x) e os outros *poden* (r-x)

-

Noa non pode crear nada directamente en /**home**. Revisar os permisos da imaxe anterior.

-

Pero non hai problema: executamos o *nautilus* como *root* con *sudo* e entramos na carpeta /**home**. Agora xa se pode crear cousas, pois abriuse a carpeta como *root*.

-

Como usuario *root*, crear en /**home** as carpetas: *comun*, *comun/alumnos* e *comun/profes*. A imaxe amosa os propietarios de cada carpeta e os seus permisos.

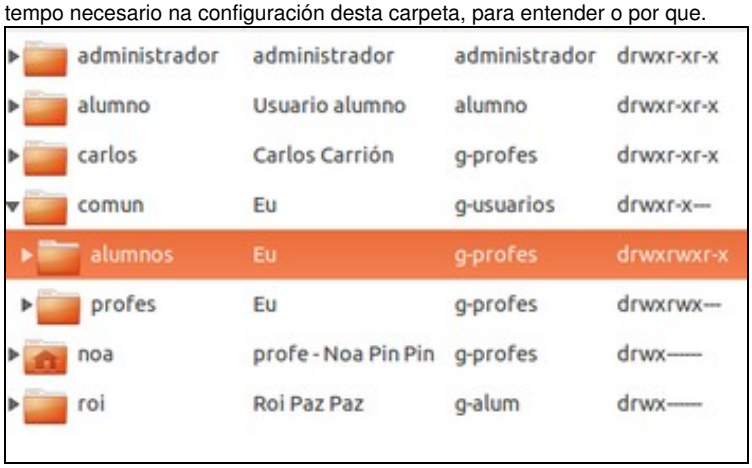
-

Na carpeta /**home**/**comun** débese: sacar os permisos a **outros**. Configurar como grupo propietario á **g-usuarios** e concederlle o *acceso a ficheiros*.

-

Na carpeta /**home**/**comun**/**profes**, igual que no caso anterior, só que o grupo propietario é *g-profes* e dáselle permiso de *crear e eliminar ficheiros*.

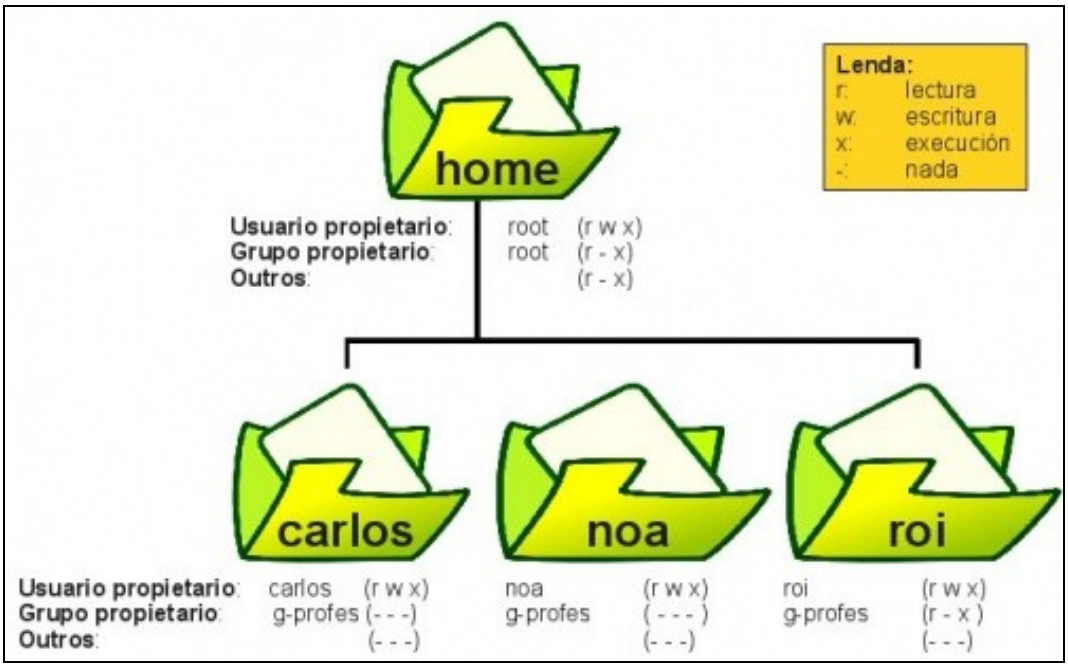
-

A carpeta /**home**/**comun**/**alumnos**, paradoxicamente igual a anterior, pero ademais a *outros* permíteselle acceder aos ficheiros. Repárese o tempo necesario na configuración desta carpeta, para entender o por que.
- 

Unha síntese de todo o realizado, observar donos, grupos donos e permisos concedidos.

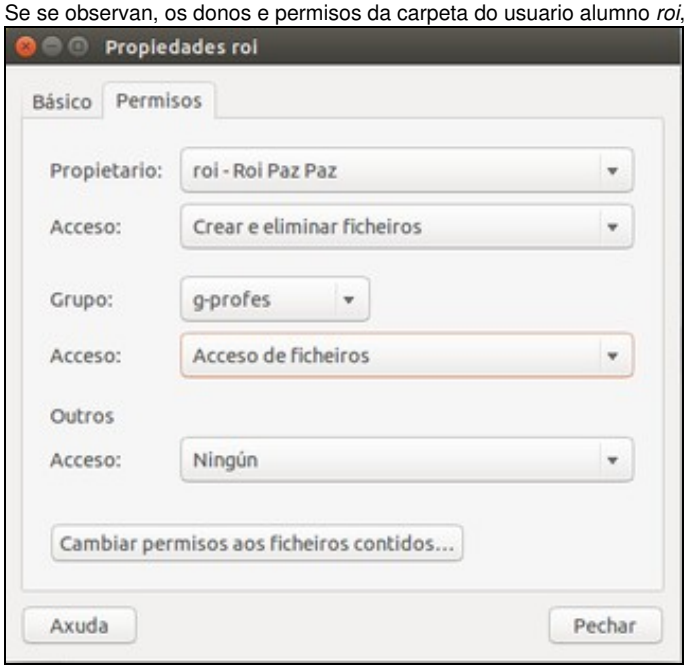
1.4.3 Afinar permisos das carpetas home dos usuarios: *facer*

Continúase coas carpetas *home* do alumnado.



- 20% do. Carpetas home dos alumnos
-

Se se observan, os donos e permisos da carpeta do usuario alumno *roi*, chegaráse á conclusión de que os profesores non poden entrar.

- 

Resólvese, cambiado o grupo propietario da carpeta *roi* a g-profes e permitíndolle *acceder a ficheiros*. Os demais usuarios (*outros*), ningún permiso.

-

  A carpeta de *roi* cos propietarios e permisos axeitados. Nesta imaxe só restaría configurar os permisos da carpeta do usuario *carlos*, sacándolle os permisos ao *grupo propietario* e a *outros*.

1.4.4 Conclusión

Os *permisos básicos* son moi simples, pero pola contra moi pouco flexibles. Problemas que presenta o anterior:

- Como *roi* é dono da súa carpeta pode cambiar os permisos e non deixar entrar aos profes, ou deixar entrar a todos os demais usuarios á súa carpeta. Home, sempre queda abrirlle un expediente ao alumno, pero cando un se dea conta ao mellor xa é tarde.

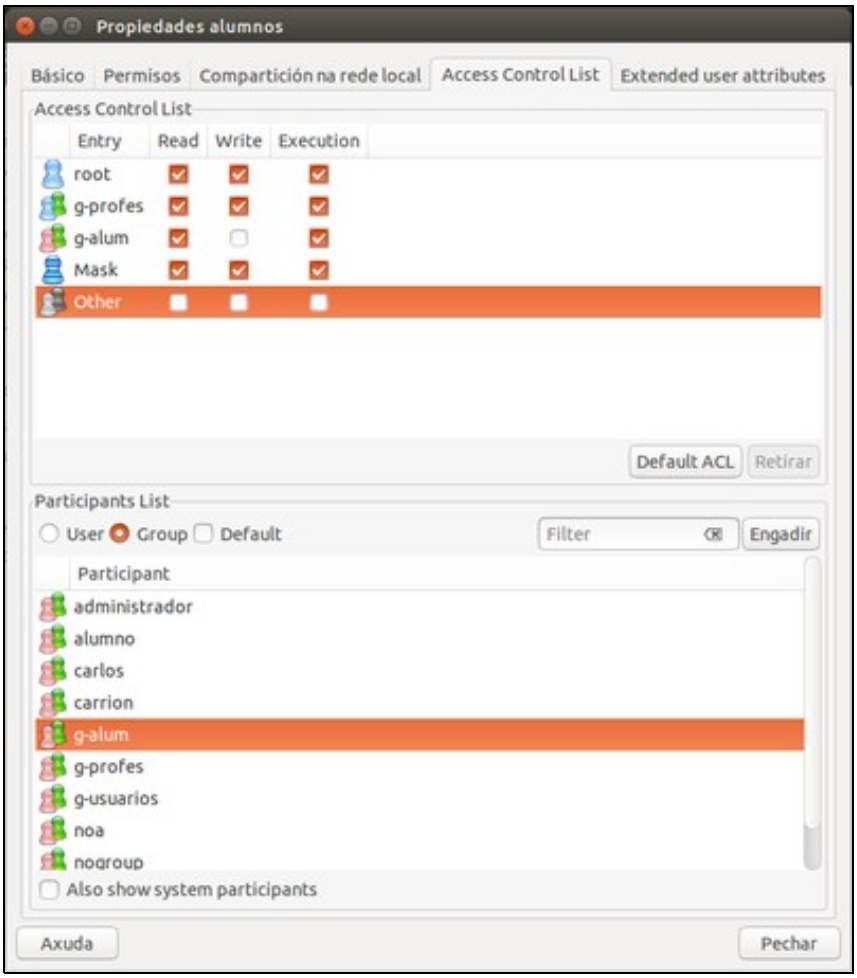
- Se mañá se dan de alta conserxes que pertenzan ao grupo *g-usuarios*, aínda que sexa como secundario, van poder entrar na carpeta */home/comun/alumnos*, cando aí non deberían entrar. Poden entrar porque *outros* poden acceder a esa carpeta.

Ao ter só tres tipos de usuarios, UGO (user, group, other) aos que asignarlle permisos a anterior configuración vese moi limitada. Sería interesante dispor de Listas de Control de Acceso (**ACL**, *Access Control List*), nas que poder afinar moito máis os permisos.

1.5 Listas de control de acceso: ACL

As *Listas de Control de Acceso (ACL: Access Control List)* veñen a suplir as eivas mencionadas anteriormente. Nunha ACL pódese especificar explicitamente quen pode facer que cousas e quen non non pode facer outras.

A imaxe amosa un exemplo de ACLs xestionadas co programa **Eiciel** feito por Roger Ferrer Ibáñez.

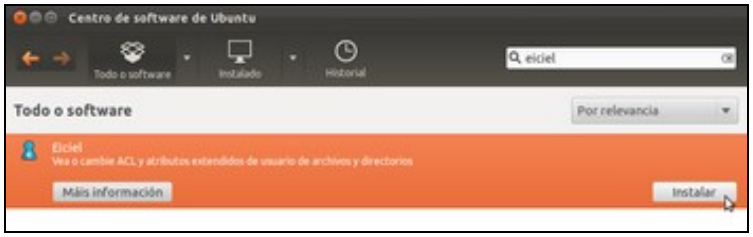


TAMÉN PODES VER...

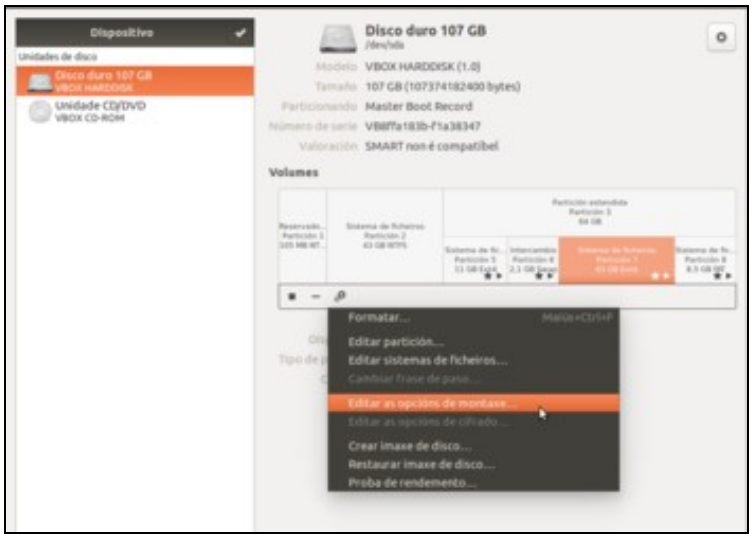
O uso de ACLs e a creación dunha estrutura máis complexa de carpetas que albergase os datos do alumnado, organizado por cursos e materias e do profesorado, dividido en departamentos, etc, que albergase a información de todos os usuarios dunha rede é algo complexo e escápase aos obxectivos deste manual, sería materia dun manual de administración de redes con Linux. Pódese seguir unha mostra do que se pode chegar a facer en: Servizos de rede e deseño dunha infraestrutura de dominio con GNU/Linux

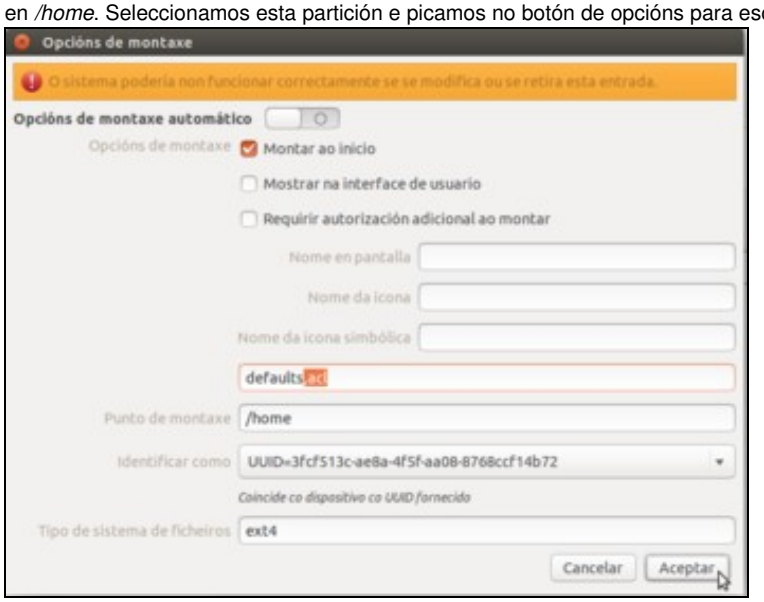
1.5.1 Instalar Eiciel e activar as ACLs

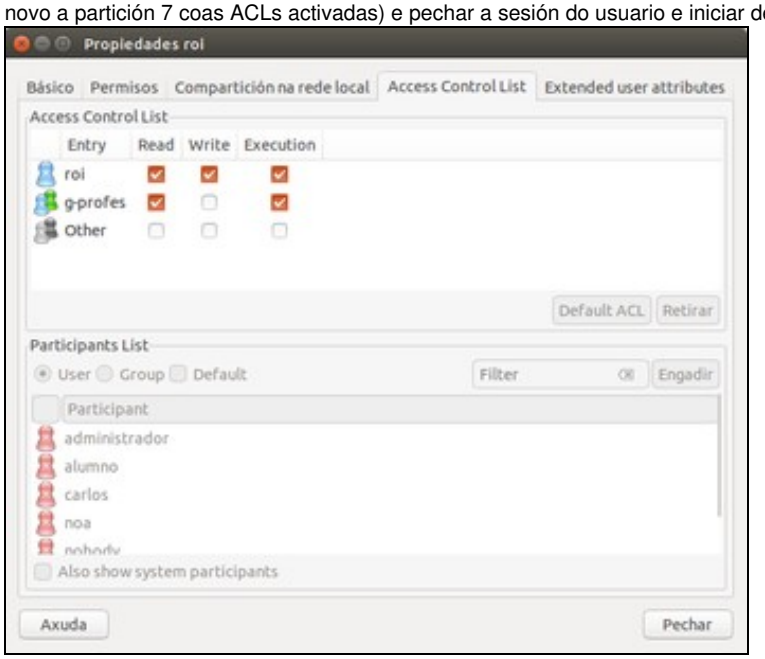
ACL é un paquete, que en Ubuntu xa ben instalado por defecto, pero hai que indicar sobre que partición (teñen que ter formato *ext3* ou *ext4*) se desexa aplicar.

- Instalar Eiciel e activar as ACLs
- 

Instalamos o paquete **Eiciel** usando o *Centro de Software de Ubuntu*.

- 

E utilizamos a ferramenta de *Discos* para activar as ACLs na partición 7 que almacena as carpetas persoais dos usuarios, que está montada en */home*. Seleccionamos esta partición e picamos no botón de opcións para escoller a opción de **Editar as opcións de montaxe...**
- 

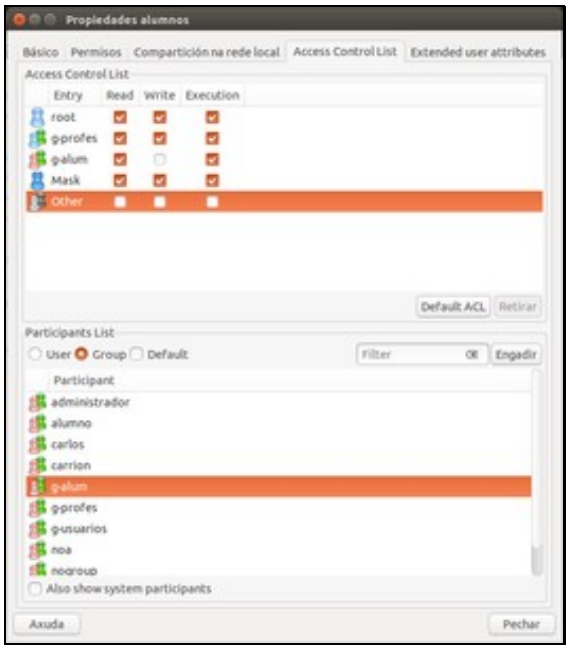
Para que se fagan efectivos os cambios podemos reiniciar o equipo ou executar o comando *sudo mount -o remount /home* (para montar de novo a partición 7 coas ACLs activadas) e pechar a sesión do usuario e iniciar de novo para que *nautilus* cargue as opcións do paquete *Eiciel*
- 

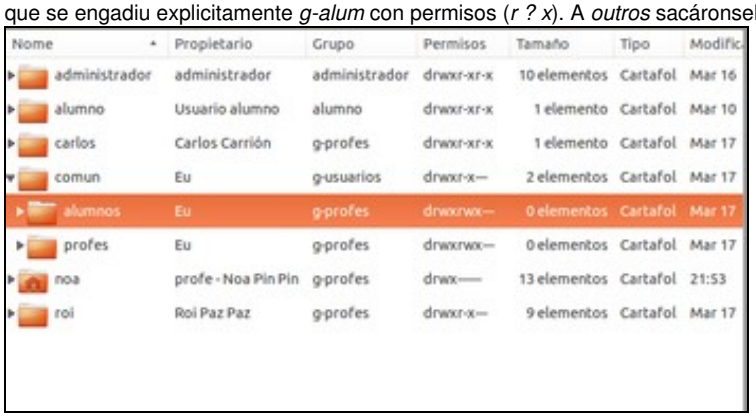
Feito isto, co usuario *noa* miramos as propiedades de */home/roi*. Vemos que aparece a lapela de *Lista de Control de Acceso*. Obviamente *noa* non pode modificar nada aí pois non é a dona.

1.5.2 Afinar os permisos con ACL

Neste exemplo vaise poñer explicitamente que na carpeta */home/comun/alumnos* os membros de *g-alumnos* poidan entrar e ver o seu contido pero non *outros*.

As ACL só poden ser editadas/cambiadas polo dono da carpeta/ficheiro ou polo usuario *root*. O mesmo que sucedía cos permisos básicos.

- Permisos de /home/comun/alumnos
- 

Para poder editar a ACL de **/home/comun/alumnos** é preciso iniciar *nautilus* como *root* e ir ás propiedades da carpeta en cuestión. Observar que se engadiu explicitamente *g-alum* con permisos (*r ? x*). A *outros* sacáronselle os permisos.
- 

Neste formato de visualización non se ven as ACLs, só os permisos básicos. Pero se nos fixamos, podemos ver que o usuario *carlos* aínda non ten ben postos con respecto ao que queríamos. Que despiste....

1.6 Comandos para a configuración dos permisos

Como xa se pode imaxinar, este método de configuración dos permisos antóllase pouco práctico para sistemas con moitos usuarios e moitas carpetas. Pódensenos quedar usuarios atrás (como o caso de *carlos*), ou confundirse nun permiso dunha carpeta. Hai que ser moi sistemático e revisalo con moita tranquilidade. Isto pódese realizar en modo gráfico se o número de usuarios é manexable (20 ? 40).

Cando se está falando de moitos usuarios o aconsellable é usar **scripts** ou *guións* (programas pequenos) que conteñan comandos que cambian propietarios e permisos en carpetas e ficheiros. Deste xeito o administrador pode realizar un programiña que faga todo ese traballo por el, se se equivoca o programa equivócase en todos, haberá que corrixilo para que o faga ben en todos os casos. Os comandos a usar en cada caso son:

- **chown**: (*change owner*, cambiar propietario). Para cambiar o usuario e grupo propietario.
- **chmod**: (*change mode*, cambiar modo). Para cambiar os permisos.

1.7 Permisos dunha unidade Windows

Se se editan os permisos dalgunha carpeta dentro de *win-linux*, carpeta na que está montada unha partición formatada en *fat*, non se pode cambiar ningún permiso. Os permisos anteriores non son aplicables para unidades FAT / NTFS de MS Windows.

Como se pode ver na imaxe, pódese probar a facer cambios nos propietarios e permisos dentro da carpeta *win-linux*... Non deixa facer ningún cambio.

-- Antonio de Andrés Lema e Carlos Carrión Álvarez