Samba – разные права доступа к субдиректориям

Возникла задача дать всем доступ к корневой папке и выборочный к субдиректориям. Схема такая:

dir – folder1, folder2

Дописываем в /etc/samba/smb.conf такие настройки:

```
[dir]
  comment = dir
  path = /home/dir
  read only = no
  valid users = @sambagroup
  force group = +sambagroup
  create mask = 0660
  force create mode = 0110
  directory mask = 0770
  writable = yes
  browseable = yes

[folder1]
  comment = folder1
  path = /home/dir/folder1
  read only = no
  valid users = @user_folder1
  force group = +user_folder1
  browseable = no

[folder2]
  comment = folder2
  path = /home/dir/folder2
  read only = no
  valid users = @user_folder2
  force group = +user_folder2
  browseable = no
```

У нас есть три группы пользователей: **sambagroup**, **users_folder1** и **users_folder2**.

Пользователям, например, **user1** и **user2** разрешено пользоваться только директорией **users_folder1**, а пользователям **user3, user4** – только **users_folder2**. Пути в эти субдиректории лежат через **dir** (/home/dir), поэтому все пользователи включены в отдельную группу **sambagroup**.

Создаем эти группы и пользователей:

```
useradd -M -s /sbin/nologin user1
groupadd users_folder1
usermod -aG users_folder1 user1
usermod -aG sambagroup user1

useradd -M -s /sbin/nologin user2
groupadd users_folder1
usermod -aG users_folder1 user2
usermod -aG sambagroup user2

useradd -M -s /sbin/nologin user3
groupadd users_folder2
usermod -aG users_folder2 user3
usermod -aG sambagroup user3

useradd -M -s /sbin/nologin user4
groupadd users_folder2
usermod -aG users_folder2 user4
usermod -aG sambagroup user4
```

Проверяем и перезапускаем сервис:

```
# testparm
# systemctl restart smbd
# systemctl restart nmbd
```

Создаем директории и выставляем права:

```
# chown root:everybody /home/dir
# chmod 770 /home/dir
# chown root:users_folder1 /home/dir/folder1
# chmod 2770 /home/dir/folder1
# chown root:users_folder2 /home/dir/folder2
# chmod 2770 /home/dir/folder2
```

Права при создании файлов и субдиректорий во внутренних папках **folder1** и **folder2** наследуются из прав, прописанных в секции **[dir]** для родительской папки. Более того, их уже не обязательно явно указывать в подсекциях **[folder1]** и **[folder2]** – они просто игнорируются.

Права 2770, выставленные на папки **folder1** и **folder2** гарантируют, что все файлы и подпапки, находящиеся в них, будут всегда создаваться с соответствующими подгруппами этих родительских папок, что предоставляет пользователям подгрупп полный доступ к любым документам и подпапкам, даже если они созданы другими пользователями.

Директива **force create mode = 0110** необходима для того, чтобы дополнительно выставить на вновь создаваемые файлы executable бит для владельца и группы, который не выставляется директивой **create mask**. Директива **force create mode** действует по принципу **ИЛИ** с основной маской доступа, и выставляет бит в том случае, если он не выставлен директивой **create mask**.

Директива **force group = +подгруппа** запрещает доступ к папкам всем, кто не входит в эту подгруппу.

Директива **writable = yes** в главной секции разрешает запись в основную папку **dir**, но в то же время жёстко задаёт права записи и в подпапки этой папки, которые невозможно переопределить во внутренних секциях. Это странное наследование правил записи разрешает запись в подпапках **folder1** и **folder2** только в том случае, если вы пришли к ним через родительскую папку **dir**. Если же попытаться обратиться к подпапкам напрямую, то они окажутся доступными только для чтения и даже уполномоченные пользователи подгрупп ничего не смогут сделать с содержимым этих подпапок.