

Setup and configure file shares

Introduction

Samba allows you, since version 4, to do most share configuration via windows. In particular, the permission management with real Windows ACLs and multiple entries is much easier when done on Windows. The following Howto will give you an overview of how to manage shares.

To use the advanced features of Samba, it has to be compiled with ACL support. Also you need a filesystem that supports the “user” and “system” xattr namespaces. It also needs to have ACL and XATTR support.

You can see [Samba4 File System support](#) to complete the requirements.

ACL support on member server

The following is only required on Domain Member Servers and not on Domain Controllers! Add the following to your [global] section of your smb.conf if you don't did this early:

```
vfs objects = acl_xattr
map acl inherit = Yes
store dos attributes = Yes
```

This options are required on Member Servers, to enable the possibility for real windows ACLs. On Domain Controllers, ACL support is automatically enabled.

SeDiskOperatorPrivilege

To configure share permissions, you need an account with “*SeDiskOperatorPrivilege*”. To see existing privileges can be reviewed by:

```
# net rpc rights list accounts -U'YOURDOMAIN\administrator'
```

In case the 'administrator' account don't have this privilege, you can grant this privilege, e. g. to the “Domain Admin” group, run the following command on your server:

```
# net rpc rights grant 'YOURDOMAIN\Domain Admins' SeDiskOperatorPrivilege -
U'YOURDOMAIN\administrator'
```

Adding a new share

- Create a folder that you want to share

```
# mkdir -p /srv/samba/Demo/
```

- Add a new share to your smb.conf:

```
[Demo]
  path = /srv/samba/Demo/
  read only = no
```

- Reload Samba:

```
# smbcontrol all reload-config
```

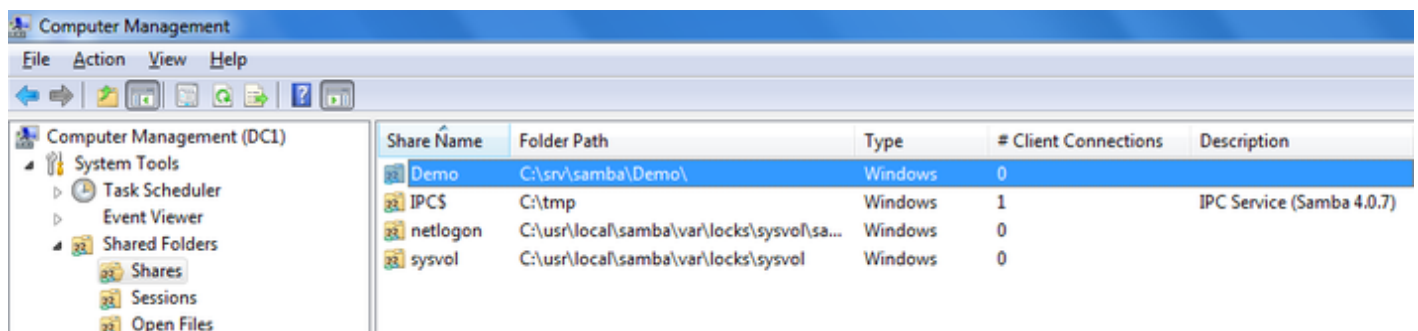
Setup share permissions

First you need to have access to your domain user administrator (or your currently domain user) in file system:

```
chown -R administrator:'domain users' /srv/samba/Demo
```

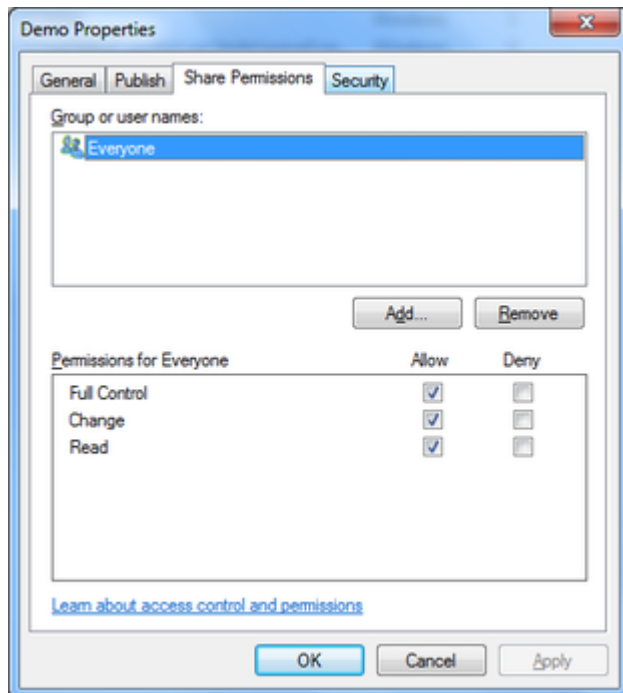
Then:

- Log on to a Windows machine using an account, to which the “*SeDiskOperatorPrivilege*” was granted to or an account in a group with granted privilege.
- Open the Start Menu and search for “Computer Management”.
- In the menu bar go to “Action” → “Connect to another computer”.
- Enter the name of your Samba server, you've create the new share on.
- Navigate to “System Tools” → “Shared Folders” → “Shares” and select the new added share.

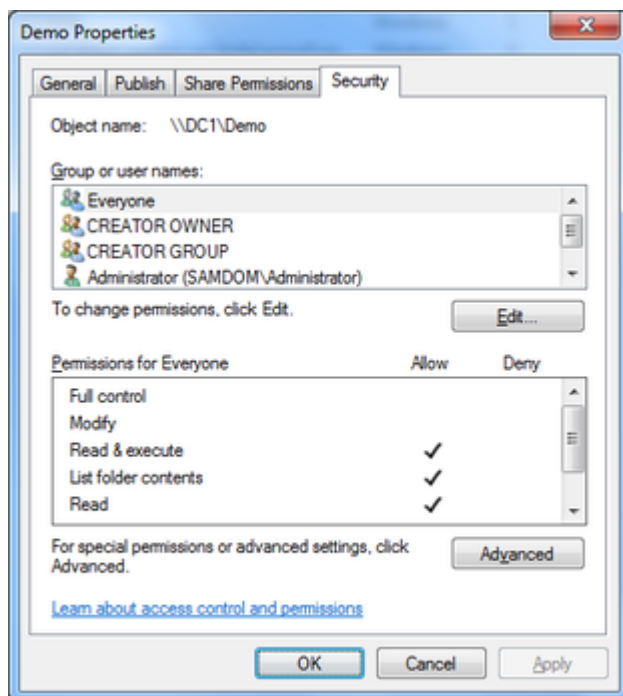


- Right-click to the share name, choose “Properties”.
- Go to the “Share Permissions” tab. Here you can configure who can access the share and the

appropriate permissions.



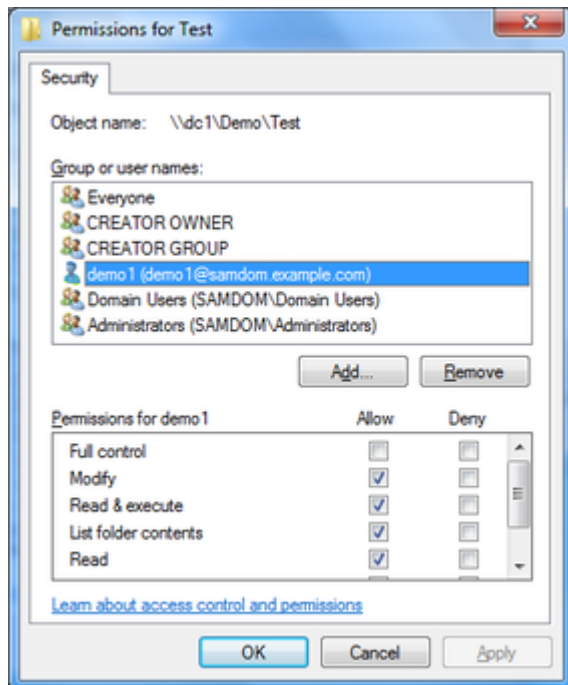
- Go to the "Security" tab, click the „Edit“ button and configure the file system permissions.



- Save the changes by closing the windows with "OK".

Change permissions on folders of a share

- Log on to a Windows machine as *Domain Administrator*.
- Navigate to the folder of which you want to change the permissions.
- Right-click to the folder and choose “Properties”.
- Go to the “Security” tab and click the “Edit” button.
- Change the permissions to your needs.



- Save the changes by closing the windows with “OK”.

Managing extended ACLs in Linux

To see extended ACLs:

```
# cd /srv && getfacl samba/Demo
# file: samba/Demo/
# owner: cbustillo
# group: domain\040users
user::rwx
group::r-x
other::r-x
```

To set extended ACLs for others users:

```
# setfacl -R -m default:other::r-x ServicePacks/
```

To remove all extended ACLs:

```
# setfacl -b /srv/samba/Demo
# setfacl -b /srv/samba/Demo/*
```

More info about extended ACLs in:

```
# man setfacl
# man getfacl
```

Troubleshooting

In certain situations, share configuration parameters which were commonly used with NT-style domains such as “force group” or “force user” may lead to “Access Denied” errors when trying to set permissions on a new share, or other complications, such as losing the ability to even see the Security tab. You may find even after correcting the issues that the problems may persist even after removing and re-adding the share properly. In such cases, it may be helpful to manually wipe out all ACLs on the share and recursively re-grant full control to the Domain Admins group with the setfacl command as follows (may need to run as root):

```
# setfacl -b /path/to/share
# setfacl -b /path/to/share/*
# setfacl -R -m default:group:domain\ admins:rwx /path/to/share
```

Related HowTos

The following HowTos treat topics, related on setting up file shares with special permissions or purposes:

- [Setting up a home share](#)
- [Samba and Windows Profiles](#)

From:

<https://redtic.uclv.cu/dokuwiki/> - **ICT Network Project**

Permanent link:

https://redtic.uclv.cu/dokuwiki/setup_config_file_shares

Last update: **2015/06/29 12:10**

