Shares with Windows ACLs

From SambaWiki

Contents

Introduction

On every Samba host you can, as on any MS Windows OS, share a folder to make it accessible for other users. There's no difference if this host is a Samba Active Directory Domain Controller, a Domain Member or a standalone server. File shares can be setup in two ways: Set completely via smb.conf parameters and POSIX ACLs or to be managed using Windows tools and ACLs. The latter is described in this documentation.

Important note: Samba Active Directory Domain Controllers have extended ACL support enabled globally, to enable management of share permissions and ACLs via Windows!

Preparatory work

File system support

Check that the filesystem, the share will reside on, supports the "user" and "system" xattr name spaces. It also requires ACL and XATTR support. See File system support for further details.

Samba ACL support

Make sure, Samba was compiled with ACL support. Check with the following command:

```
# smbd -b | grep HAVE_LIBACL
   HAVE_LIBACL
```

If "HAVE_LIBACL" is not found, then Samba was compiled without extended ACL support. See Dependencies - Libraries and programs if you compiled Samba yourself.

Enable extended ACL support in smb.conf

The following is only required on Domain Members and not on Domain Controllers, where this setting is hard coded enabled.

Add the following to your [global] section of your smb.conf:

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

See the smb.conf man page for further details on the parameters.

SeDiskOperatorPrivilege

Accounts that should be able to configure share permissions, require the privilege "SeDiskOperatorPrivilege". To view the current privilege list on a host, run

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

In the following, we will grant the privilege to the group "Domain Admins", but before doing this, make sure that the group is available to the local OS by NSS; usually via Winbindd:

```
# getent group "Domain Admins"
domain admins:x:10001:
```

If you don't get an output showing the queried name and its ID, there may be something wrong in your NSS configuration or if you are using Winbindd with RFC2307 (idmap_ad), you might not have an ID assigned (see User and group management for how to administer Unix Attributes in an AD). If the "Domain Admins" group is available to the OS, you can grant the SeDiskOperatorPrivilege privilege to:

```
# net rpc rights grant 'SAMDOM\Domain Admins' SeDiskOperatorPrivilege -U'SAMDOM\administrator'
Enter SAMDOM\administrator's password:
Successfully granted rights.
```

Adding a new share

- Create the new shared folder, if it doesn't already exist

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

- In order to allow a user or group to modify permissions, "Full control" is required. If you haven't modified it, the default value of "acl map full control" is "yes", this defines that "rwx" (read-write-execute) is mapped to "Full control". Accordingly to allow members of the "Domain Admins" group to edit permissions via Windows, we need to set the following:

```
# chmod g=rwx /srv/samba/Demo/
# chgrp "Domain Admins" /srv/samba/Demo/
```

- Add the new share to your smb.conf. No further parameters other than the following are required or suggested (e. g. "force user/group" is not compatible with the vfs objects "acl_xattr" and can cause "Access denied" errors)!

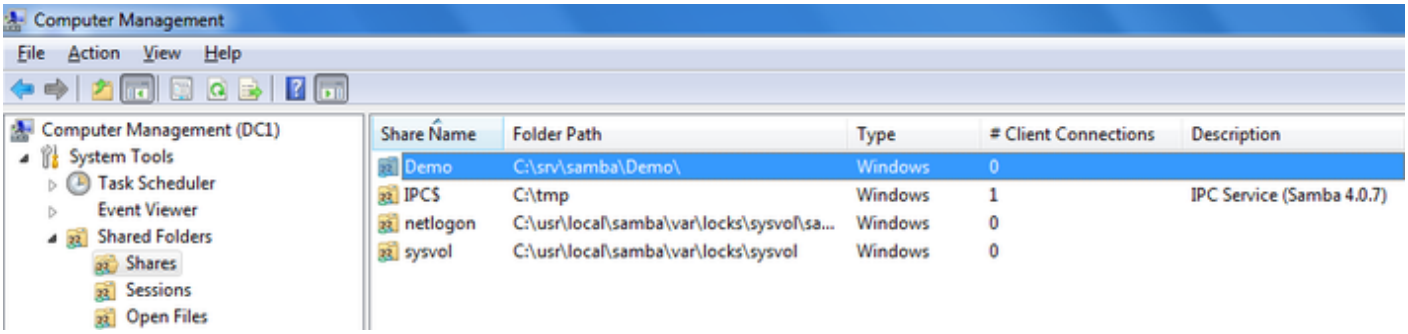
```
[Demo]
       path = /srv/samba/Demo/
       read only = no
```

- Reload Samba

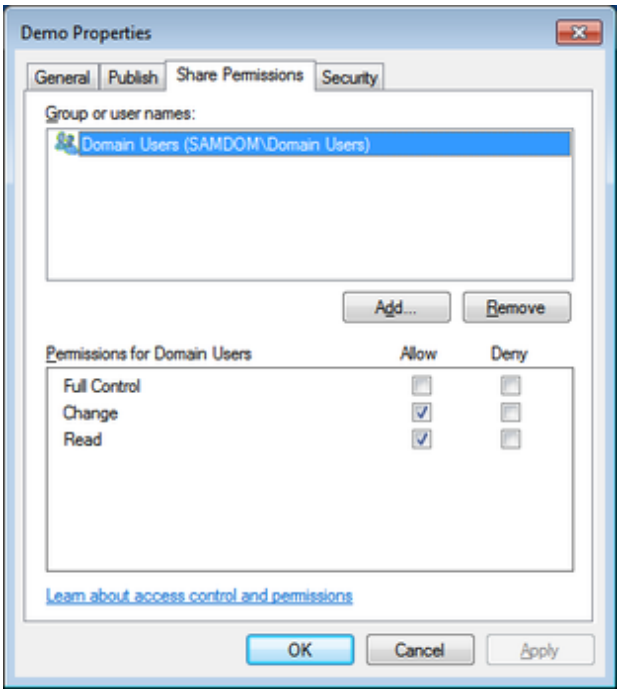
```
# smbcontrol all reload-config
```

Setup share permissions (optional)

- Log on to a Windows machine, using an account that is a member of the "Domain Admins" group
- Open the Start Menu, search for "Computer Management" and open the program
- In the menu bar go to "Action" / "Connect to another computer"
- Enter the name of the Samba host on which you want to edit the share permissions
- Navigate to "System Tools" / "Shared Folders" / "Shares" and select the desired share



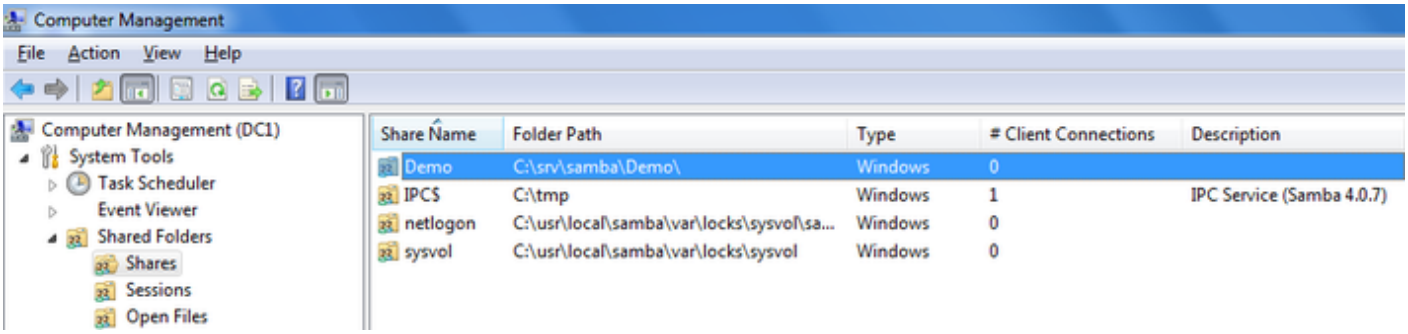
- Right-click to the share name and choose "Properties"
- Go to the "Share Permissions" tab and define who is allowed to connect to the share



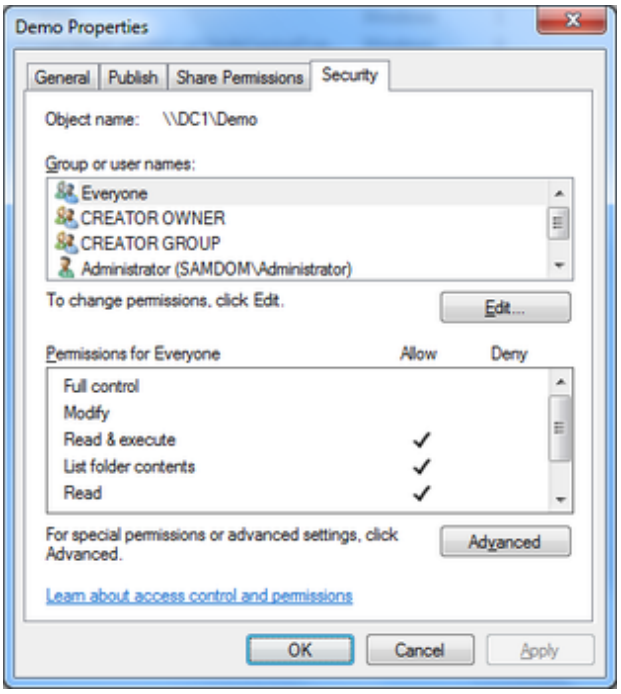
- Save the changes by closing the windows with "OK"

Set ACLs on the root of a share

- Log on to a Windows machine, using an account that is a member of the "Domain Admins" group
- Open the Start Menu, search for "Computer Management" and open the program
- In the menu bar go to "Action" / "Connect to another computer"
- Enter the name of the Samba host on which you want to edit the share permissions
- Navigate to "System Tools" / "Shared Folders" / "Shares" and select the desired share



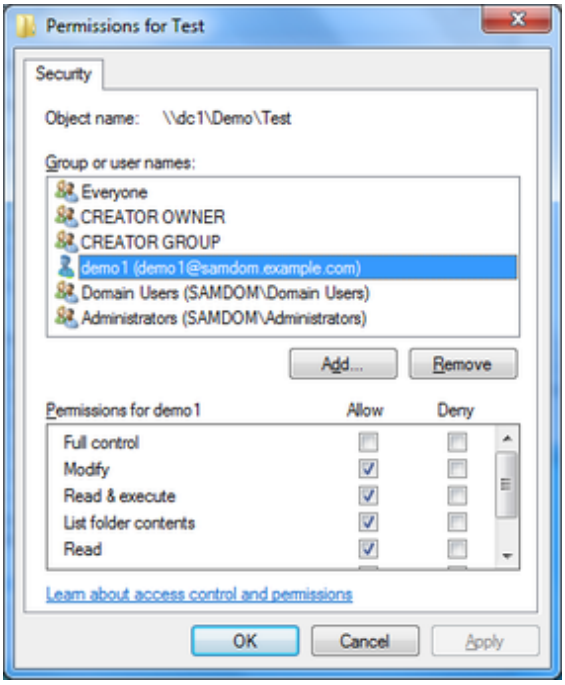
- Right-click to the share name and choose "Properties"
- Go to the "Security" tab, click the "Edit" button and configure the desired Windows ACLs



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

Set ACLs on subfolders of a share

- Log on to a Windows machine, using an account that is a member of the "Domain Admins" group
- 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"

Troubleshooting

In certain situations, configuration parameters which were commonly used on shares with POSIX ACLs, 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 (need to run as root):

```
# setfacl -R -b /srv/samba/Demo/
# setfacl -R -b /srv/samba/Demo/*
# setfacl -R -m default:group:"Domain Admins":rwx /srv/samba/Demo/
```

Related documentation

The following documentation discusses related topics:

- Setting up home drives
- Implementing Windows roaming profiles