Install Samba on CentOS 7

Samba is a free and open-source re-implementation of the SMB/CIFS network file sharing protocol that allows end users to access files, printers, and other shared resources.

In this tutorial, we will show how to install Samba on CentOS 7 and configure it as a standalone server to provide file sharing across different operating systems over a network.

We'll create the following Samba shares and users.

Users:

- **sadmin** - An administrative user with read and write access to all shares.
- **josh** - A regular user with its own private file share.

Shares:

- **users** - This share will be accessible with read/write permissions by all users.
- **josh** - This share will be accessible with read/write permissions only by users josh and sadmin.

The file shares will be accessible from all devices on your network. Later in the tutorial, we will also provide detailed instructions on how to connect to the Samba server from Linux, Windows and macOS clients.

Prerequisites

Before you begin, make sure you are logged in to your CentOS 7 system as a user with sudo privileges.

Installing Samba on CentOS

Samba is available from the standard CentOS repositories. To install it on your CentOS system run the following command:

sudo yum install samba samba-client

Once the installation is completed, start the Samba services and enable them to start automatically on system boot:

sudo systemctl start smb.service
sudo systemctl start nmb.service

sudo systemctl enable smb.service
sudo systemctl enable nmb.service

SELinux Configuration

vim /etc/sysconfig/selinux

Set SELinux value to disabled.

The smbd service provides file sharing and printing services and listens on **TCP ports 139** and **445**. The nmbd service provides NetBIOS over IP naming services to clients and listens on **UDP port 137**.

Configuring Firewall

Now that Samba is installed and running on your CentOS machine, you'll need to [configure your firewall](https://linuxize.com/post/how-to-setup-a-firewall-with-firewalld-on-centos-7/ and open the necessary ports.
To do so, run the following commands:

firewall-cmd --permanent --zone=public --add-service=samba
firewall-cmd --zone=public --add-service=samba

firewall-cmd --reload

Creating Samba Users and Directory Structure

For easier maintainability and flexibility instead of using the standard home directories (/home/user) all Samba directories and data will be located in the /samba directory.

Start by creating the /samba directory:

sudo mkdir /samba

Create a new group named sambashare. Later we will add all Samba users to this group.

sudo groupadd sambashare

Set the /samba directory group ownership to sambashare:

sudo chgrp sambashare /samba

Samba uses Linux users and group permission system but it has its own authentication mechanism separate from the standard Linux authentication. We will create the users using the standard Linux useradd tool and then set the user password with the smbpasswd utility.

As we mentioned in the introduction, we'll create a regular user that will have access to its private file share and one administrative account with read and write access to all shares on the Samba server.

Creating Samba Users

To create a new user named josh, use the following command:

sudo useradd -M -d /samba/josh -s /usr/sbin/nologin -G sambashare josh

The useradd options have the following meanings:

- -M -do not create the user's home directory. We'll manually create this directory.
- -d /samba/josh - set the user's home directory to /samba/josh.
- -s /usr/sbin/nologin - disable shell access for this user.
- -G sambashare - add the user to the sambashare group.

Create the user's home directory and set the directory ownership to user josh and group sambashare:

sudo mkdir /samba/joshsudo chown josh:sambashare /samba/josh

The following command will add the setgid bit to the /samba/josh directory so the newly created files in this directory will inherit the group of the parent directory. This way, no matter which user creates a new file, the file will have group-owner of sambashare. For example, if you don't set the directory's permissions to 2770 and the sadmin user creates a new file the user josh will not be able to read/write to this file.

sudo chmod 2770 /samba/josh

Add the josh user account to the Samba database by setting the user password:

sudo smbpasswd -a josh

You will be prompted to enter and confirm the user password.

New SMB password:
Retype new SMB password:
Added user josh.

Once the password is set, enable the Samba account by typing:

sudo smbpasswd -e josh

Enabled user josh.

To create another user repeat the same process as when creating the user josh.

Next, let’s create a user and group sadmin. All members of this group will have administrative permissions. Later if you want to grant administrative permissions to another user simply add that user to the sadmin group.

Create the administrative user by typing:

sudo useradd -M -d /samba/users -s /usr/sbin/nologin -G sambashare sadmin

The command above will also create a group sadmin and add the user to both sadmin and sambashare groups.

Set a password and enable the user:

sudo smbpasswd -a sadmin
sudo smbpasswd -e sadmin

Next, create the Users share directory:

sudo mkdir /samba/users

Set the directory ownership to user sadmin and group sambashare:

sudo chown sadmin:sambashare /samba/users

This directory will be accessible by all authenticated users. The following command configures write/read access to members of the sambashare group in the /samba/users directory:

sudo chmod 2770 /samba/users

Configuring Samba Shares

Open the Samba configuration file and append the sections:

sudo vim /etc/samba/smb.conf

/etc/samba/smb.conf

[users]
path = /samba/users
browseable = yes
read only = no
force create mode = 0660
force directory mode = 2770
valid users = @sambashare @sadmin

[josh]
path = /samba/josh
browseable = no
read only = no
force create mode = 0660
force directory mode = 2770
valid users = josh @sadmin

The options have the following meanings:
[users] and **[josh]** - The names of the shares that you will use when logging in.
path - The path to the share.
browseable - Whether the share should be listed in the available shares list. By setting to no other users will not be able to see the share.
read only - Whether the users specified in the valid users list are able to write to this share.
force create mode - Sets the permissions for the newly created files in this share.
force directory mode - Sets the permissions for the newly created directories in this share.
valid users - A list of users and groups that are allowed to access the share. Groups are prefixed with the @ symbol.

For more information about available options see the Samba configuration file documentation page.

Once done, restart the Samba services with:

sudo systemctl restart smb.service
sudo systemctl restart nmb.service

Korte versie

create dir public

chmod 777 public

yum install samba

cd /etc/samba

vim /etc/samba/smb.conf

[RestrictedAdmin]
comment = Restricted access directory
path = /public
read only = No
guest ok = No
valid users = admin
browseable = Yes

host allow = ip subnet invullen

chcon -R -t samba_share_t /public
semanage fcontext -a -t samba_share_t " /public(/.*)?"

systemctl start smb

systemctl enable smb

systemctl status smb

smbpasswd -a admin

testparm

Unieke FAQ ID: #1035
Auteur: diode
Laatst bijgewerkt:11-03-2021 16:52