Linux - Samba Setup Rocky 9

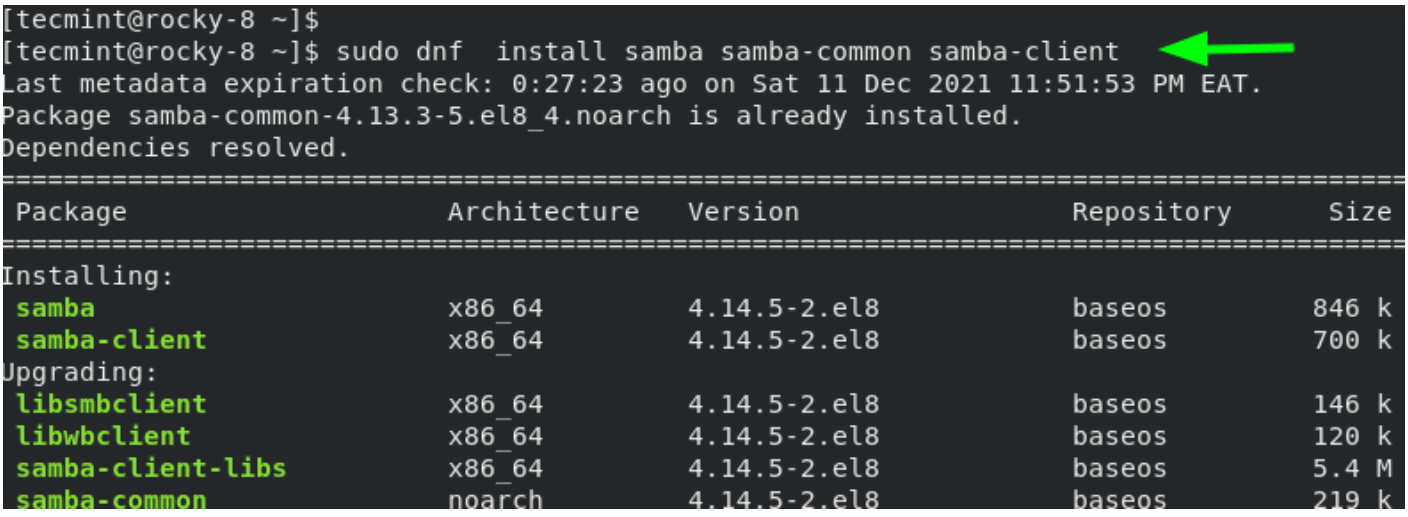
> Last verified: October 2026 for RHEL / Rocky Linux 9 against the Red Hat Samba guide, the smb.conf manual and Microsoft's SMB guest access documentation.

Step 1: Install Samba on Linux

To get started out with **Samba**, install the **Samba** core packages including the client package:

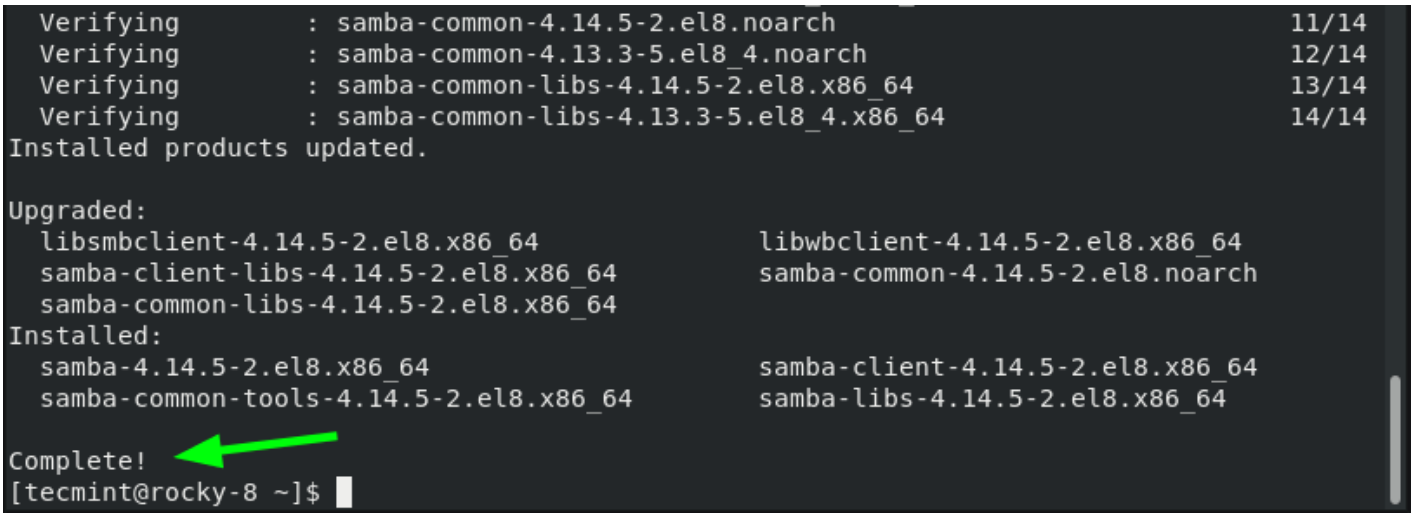
```
dnf install -y samba samba-common samba-client
```

Install-Samba in Linux



The command installs the packages specified along with the dependencies as displayed on the output. After the installation is complete, you will get a summary of all the packages that have been installed.

Samba Installation Completes



Step 2: Create and Configure Samba Shares

Once all the **samba** packages have been installed, the next step is to configure the **samba shares** . A samba share is simply a directory that is going to be shared across client systems in the network.

Here, we are going to create a samba share called **/data** in the **/srv/tecmint/** directory path.

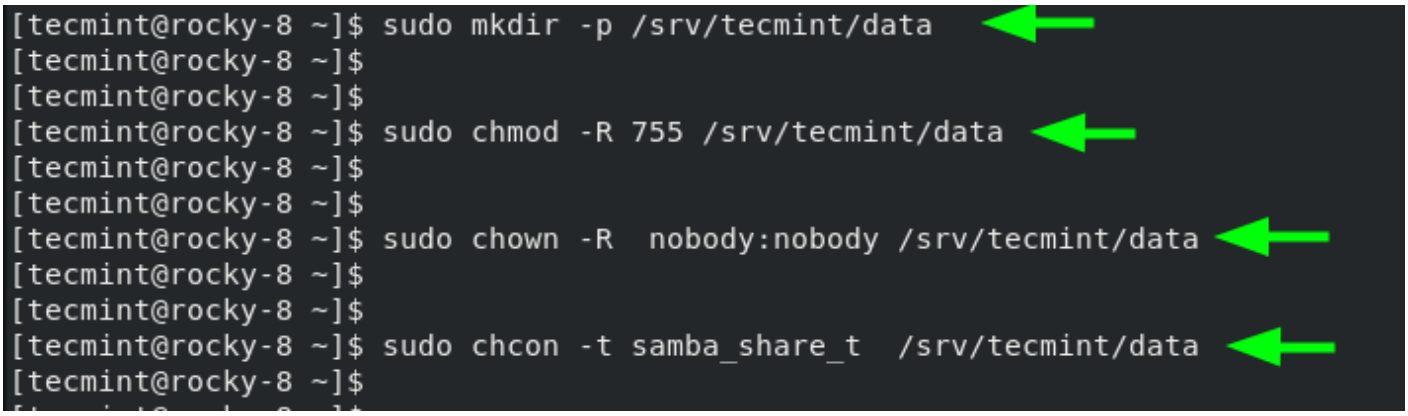
```
mkdir -p /srv/tecmint/data
```

Next, we will assign permissions and ownership as follows.

```
chmod -R 755 /srv/tecmint/data
chown -R  nobody:nobody /srv/tecmint/data
semanage fcontext -a -t samba_share_t "/srv/tecmint/data(/.*)?"
restorecon -Rv /srv/tecmint/data
```

The semanage + restorecon pair sets the SELinux label permanently, so it survives a file system relabel (chcon does not). If semanage is missing, install it with `dnf install policycoreutils-python-utils`.

Create Samba Share Directory



Next, we are going to make some configurations in the **smb.conf** configuration file which is Samba's main configuration file. But before we do so, we will back up the file by renaming it with a different file extension.

```
mv /etc/samba/smb.conf /etc/samba/smb.conf.bak
```

Next, we are going to create a new configuration file.

```
vim /etc/samba/smb.conf
```

We will define policies on who can access the samba share by adding the lines shown in the configuration file.

```
[global]
workgroup = WORKGROUP
server string = Samba Server %v
netbios name = samba-server
security = user
map to guest = bad user
dns proxy = no



[Public]
path =  /srv/tecmint/data
browsable =yes
writable = yes
guest ok = yes
read only = no
```

Save and exit the configuration file.

> Do not add `ntlm auth = true` (older guides include it). It is an alias for `ntlmv1-permitted` and re-enables insecure NTLMv1. The default, `ntlmv2-only`, works with all modern clients.

To verify the configurations made, run the command:

```
testparm
```

Verify Samba Configuration

```
[tecmint@rocky-8 ~]$
[tecmint@rocky-8 ~]$ sudo testparm
Load smb config files from /etc/samba/smb.conf
Loaded services file OK.
Weak crypto is allowed

Server role: ROLE_STANDALONE

Press enter to see a dump of your service definitions

# Global parameters
[global]
        dns proxy = No
        map to guest = Bad User
        security = USER
        server string = Samba Server %v
        idmap config * : backend = tdb


[Public]
        guest ok = Yes
        path = /srv/tecmint/data
        read only = No
```

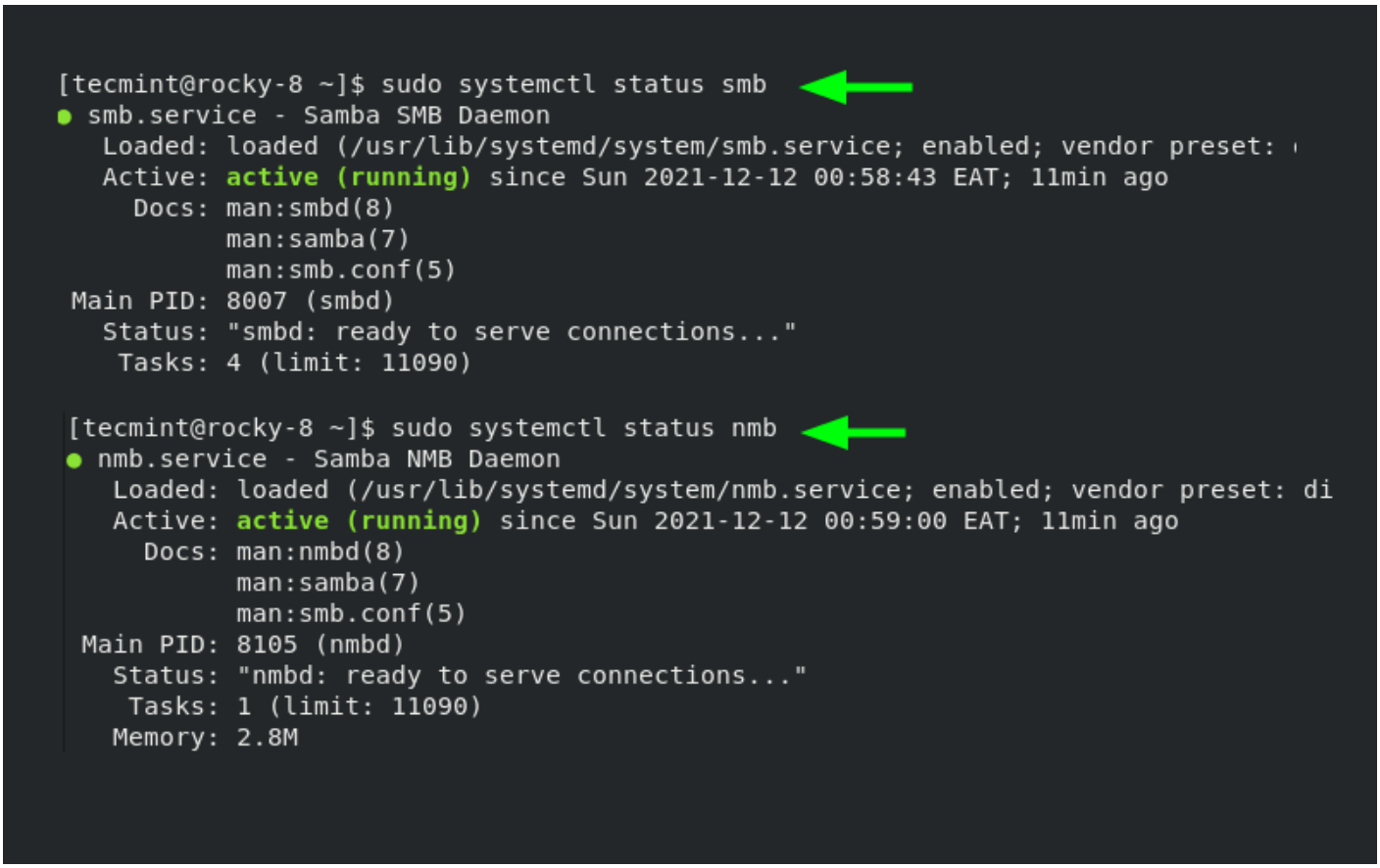
Next, start and enable Samba daemons as shown.

```
systemctl enable --now smb;systemctl enable --now nmb
```

Be sure to confirm that both the **smb** and **nmb** daemons are running. (nmb only provides NetBIOS name resolution and network browsing; it is optional if your clients connect by DNS name or IP.)

```
systemctl status smb;systemctl status nmb
```

Verify Samba Status



To enable access to samba share from remote Windows systems, you need to open the samba protocol on the firewall.

```
firewall-cmd --permanent --add-service=samba
firewall-cmd --reload
firewall-cmd --list-services
```

Step 3: Accessing Samba Share from Windows

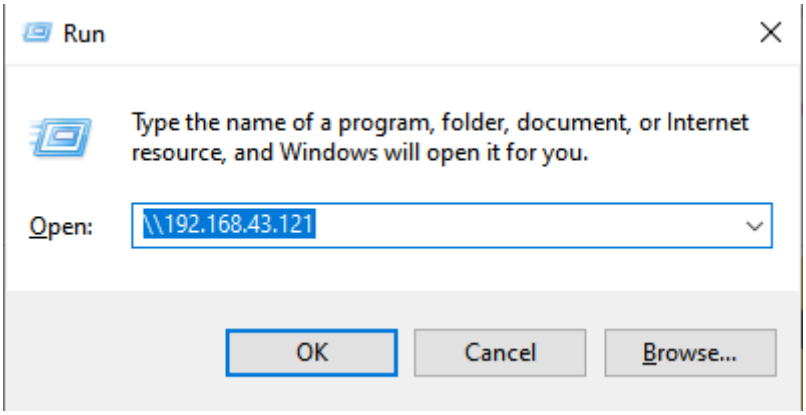
Thus far, we have installed **samba** and configured our **samba share**. We are now ready to access it remotely. To do this on a Windows client, press the Windows logo `key + R` to launch the **Run** dialog.

> Current Windows versions block guest (no password) access to SMB shares by default: Windows 10 1709+ and Windows Server 2019+ disable insecure guest logons, and Windows 11 24H2 / Windows Server 2025 also require SMB signing, which guest sessions cannot do. If the **Public** share will not open, use the authenticated share from Step 4 rather than weakening the client security settings.

In the textfield provided, enter the samba server's IP address as shown:

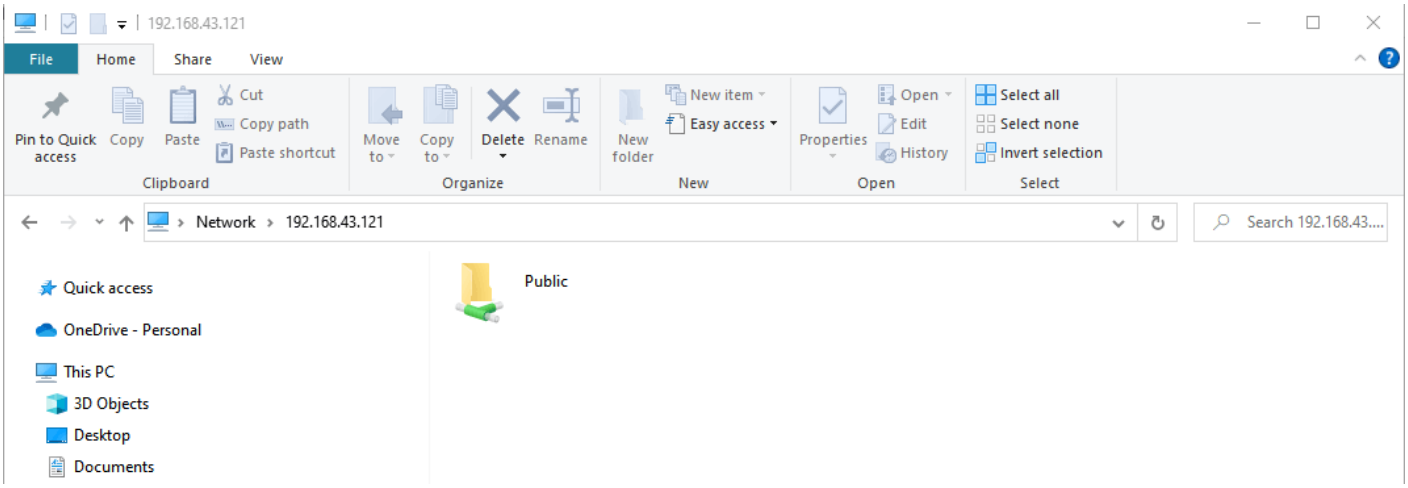
```
\\server-ip
```

Access Samba Share from Windows



The following window labeled '**Public**' will pop up. Remember, this is the directory that points to our samba share in the **/srv/tecmint/data** directory.

Access Samba Share Directory on Windows

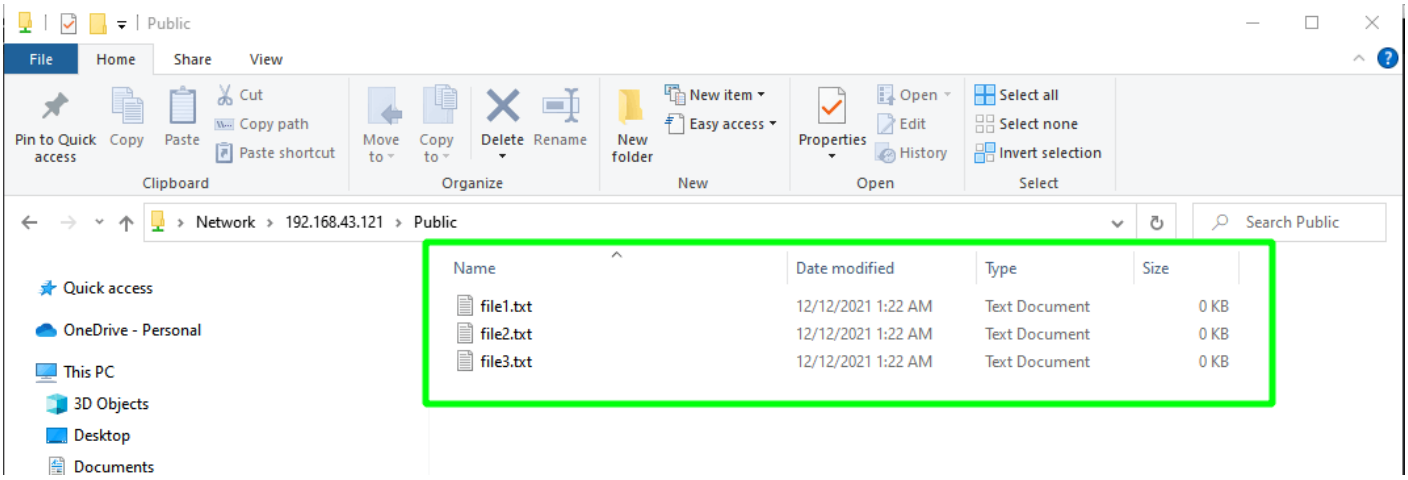


Currently, our directory is empty as we have not created any files. So, we will head back to our terminal and create a few files in the samba share directory.

```
cd /srv/tecmint/data
touch file{1..3}.txt
```

Now, we will navigate to the '**Public**' folder where the files we created earlier will be displayed.

Access Samba Share Files on Windows



Perfect. We have successfully managed to access our s**amba share**. However, our directory is accessible to anyone and everybody can edit and delete files at will, which is not recommended especially if you plan to host sensitive files.

In the next step, we will demonstrate how you can create and configure a secure samba share directory.

Step 4: Secure Samba Share Directory

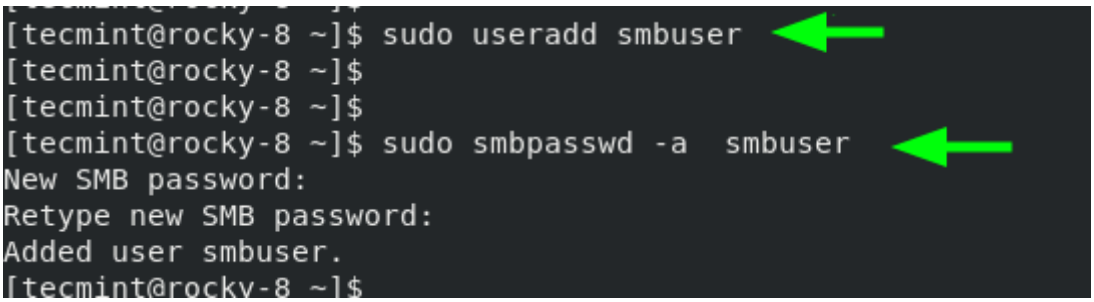
First, we will create a new samba user.

```
useradd smbuser
```

Next, we will configure a password for the samba user. This is the password that will be used during authentication.

```
smbpasswd -a smbuser
```

Create Samba User



Next, we will create a new group for our secure samba share and add the new samba user.

```
groupadd smb_group
usermod -aG smb_group smbuser
```

Thereafter, create yet another samba share which will be securely accessed. In our case, we have created another directory in the same path as the

```
mkdir -p  /srv/tecmint/private
```

Then configure the file permissions for the samba share

```
chmod -R 770 /srv/tecmint/private
semanage fcontext -a -t samba_share_t "/srv/tecmint/private(/.*)?"
restorecon -Rv /srv/tecmint/private
chown -R root:smb_group /srv/tecmint/private
```

Once again, access the Samba configuration file.

```
$ sudo vim /etc/samba/smb.conf
```

Add these lines to define to secure samba share.

```
[Private]
path = /srv/tecmint/private
valid users = @smb_group
guest ok = no
writable = no
browsable = yes
```

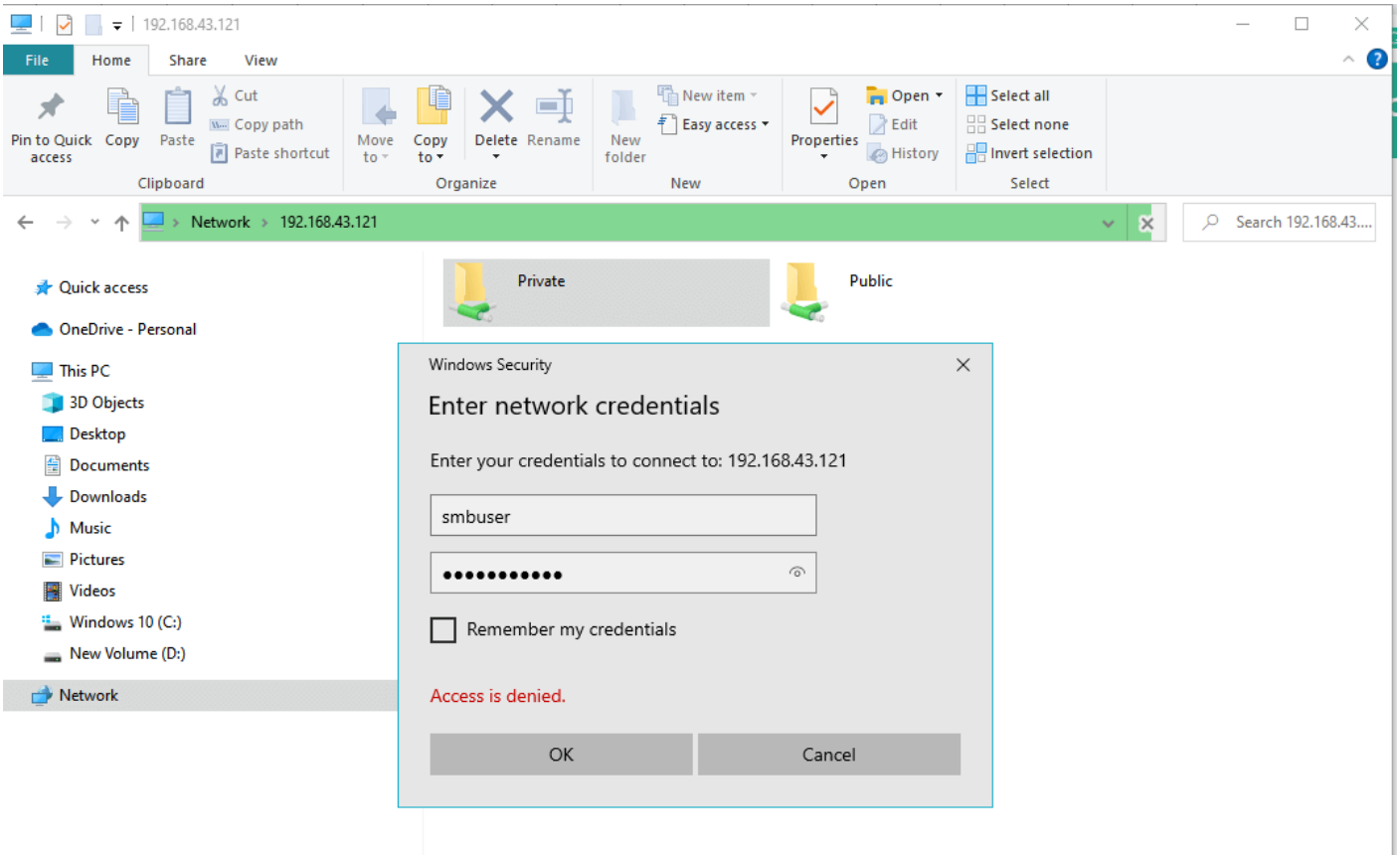
Save the changes and exit.

Finally, restart all the samba daemons as shown.

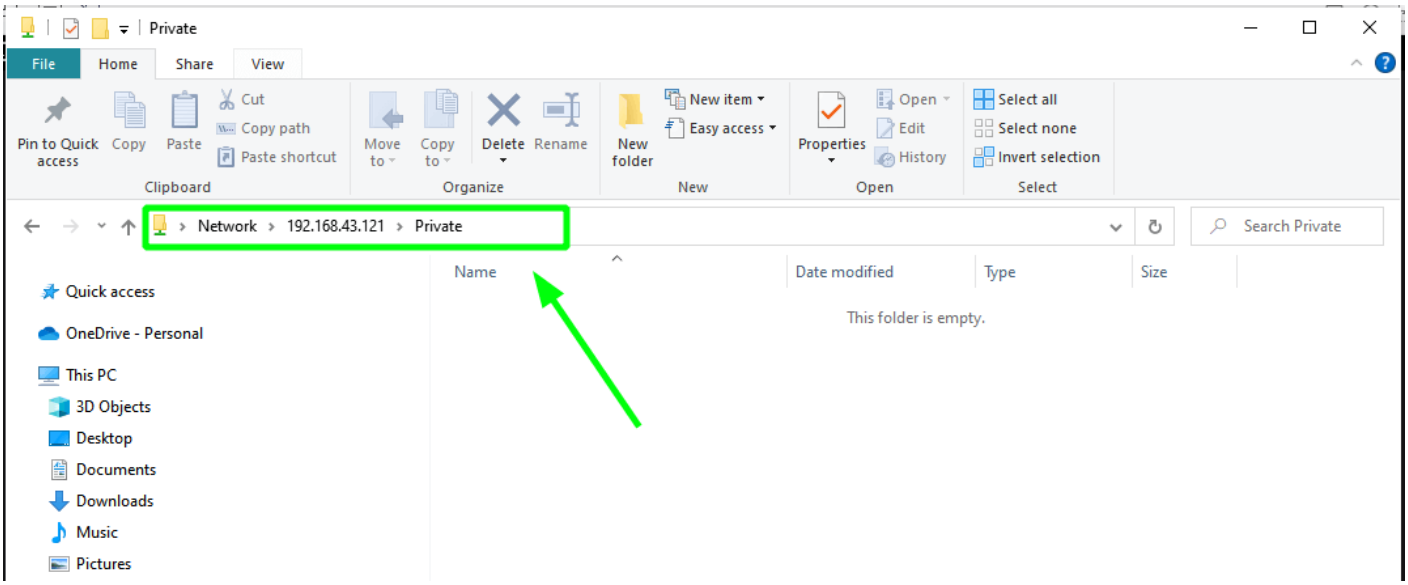
```
systemctl restart smb;systemctl restart nmb
```

When you access your server this time around, you will notice an additional ‘**Private**‘ folder. To access the folder, you will be required to authenticate with the Samba user’s credentials. Provide the username and password of the user you created in the previous step and click ‘**OK**’.

Samba User Authentication



Samba Private Share Directory



Step 5: Accessing Samba Share from Linux Client

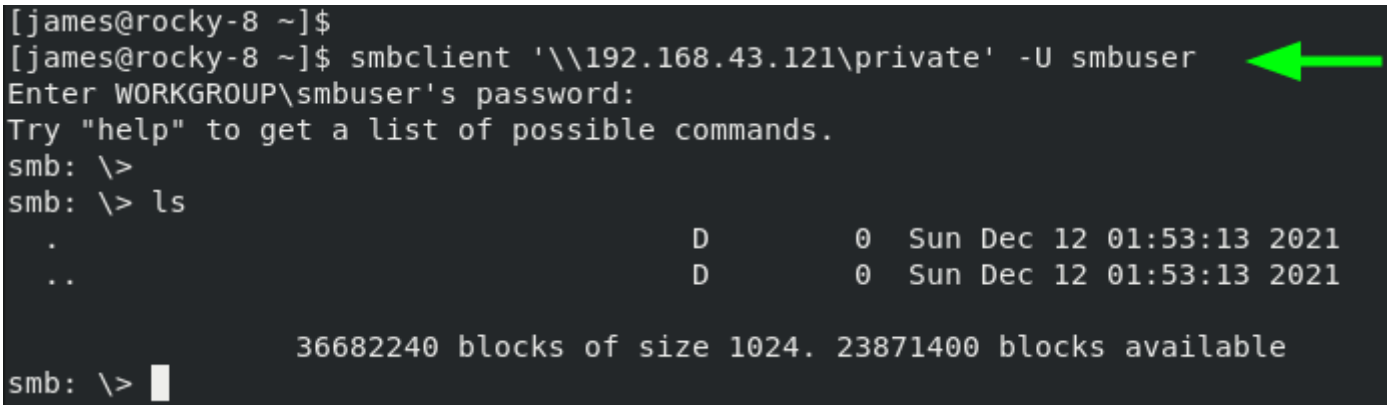
To access the share from a Linux client, first, ensure that the Samba client package is installed.

```
$ dnf install -y samba-client
```

Then use the **smbclient** command as follows

```
smbclient //server-ip/private -U smbuser
```

Access Samba Share from Linux



And this concludes this guide on setting up **Samba** on **RHEL**, **CentOS Stream**, **Rocky Linux,** and **AlmaLinux**. Your feedback on this guide will be highly appreciated.

Some taken from https://www.tecmint.com/install-samba-rhel-rocky-linux-and-almalinux/

Sources

- https://docs.redhat.com/en/documentation/red_hat_enterprise_linux/9/html/configuring_and_using_network_file_services/assembly_using-samba-as-a-server_configuring-and-using-network-file-services
- https://www.samba.org/samba/docs/current/man-html/smb.conf.5.html
- https://learn.microsoft.com/en-us/windows-server/storage/file-server/enable-insecure-guest-logons-smb2-and-smb3
- https://www.tecmint.com/install-samba-rhel-rocky-linux-and-almalinux/

Revision #1
Created 2 September 2024 22:40:52 by Admin
Updated 24 October 2026 14:10:46 by Admin