How to Configure Samba Server in Redhat Linux

This tutorial explains how to configure Samba server in Linux and Samba client in Windows and Linux including how to create IPTABLES rules and configure SELinux Booleans to allow Samba traffic step by step with practical examples. Learn how to share resources and access shared resources in Samba network.

* Microsoft window use Common Internet File System (CIFS) protocol for networking.
* CIFS was developed from Server Message Block (SMB) protocol.
* Samba is a open source software.
* Samba uses TCP/IP protocol.
* Samba is Linux implementation of SMB/CIFS protocols.
* Samba allows interoperability between Linux and Window.
* Samba provide file and print sharing service between Linux and Window system.
* Samba allows Linux to interact with Window client, Server, member of Active Directory, Primary domain controller, or member server.
* Samba support Microsoft Access Control Lists.
* Main configuration file of Samba server is **/etc/samba/smb.conf**
* Samba Web Administration tool (SWAT) is a GUI base configuration tool for Samba Serveravailable from RHEL 6
* In Linux SAMBA provides the following services:
  + User Authentication and authorization
  + File and printer sharing
  + Name resolution
  + Browsing

**RHCE Exam topic covered in this article**

* Provide network shares to specific clients.
* Provide network shares suitable for group collaboration.

During the RHCE exam you will not have access to Microsoft window so you must know how to test Samba configuration with Linux system.

In this tutorial I will use two systems **Server** and **linuxclient** from our LAB environment. I will configure Samba Server on **Server**system and samba client on **linuxclient** system. If you want to check the network topology used in this article please check following article.[Lab set up for RHEL practice](https://www.computernetworkingnotes.com/rhce-study-guide/rhel-7-lab-setup-for-rhce-practice.html).

**RPM required for Samba Server**

|  |  |
| --- | --- |
| RPM | Description |
| samba | Base RPM for Samba Server |
| samba-client | Base RPM for Samba Client |
| samba-common | Include commands those required by Samba Server and client |
| samba-doc | provide Samba documentation |
| samba-swat | GUI interface for Samba configuration |
| samba-winbind | Allow interoperability between Linux and Window |
| samba-domainjoin-gui | Allow linux user to connect with windows workgroups and domains. |

**LAB tasks**

* Configure Samba on Server system. Configure iptables firewall and SELinux Booleans to allow Samba connection on server.
* Create 5 users on Server system. Make a group of two users. Add all users in Samba user database.
* Check connectivity form linuxclient and windowclient system. Verify by login from one user.
* Create a sharedata folder on server. Grant read and write access to public on sharedata folder. Share publicly this folder. Test form linux and window client.

Configure Samba Server

On samba server following RPM are required

* samba
* samba-common
* samba-winbind

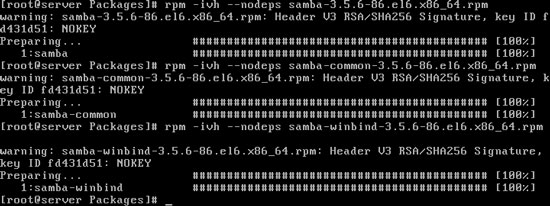
Check necessary rpm

rpm-qa-samba

You can install RPM from several sources including YUM repository, dump of RPM, FTP, etc. In this article I am installing RPM form RHEL 6 disk. Mount RHEL 6 disk in media folder and change directory to Package folder

cd-media-package

Install necessary RPM.

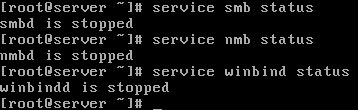


Samba Daemons

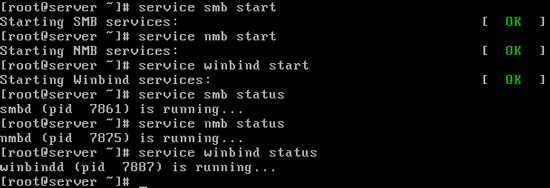
For Samba we need three services to run, one optional and two required

|  |  |  |  |
| --- | --- | --- | --- |
|  | Service | Daemons | Description |
| Required | smb | smbd | (SMB/CIFS Server) main samba service which provide user authentication and authorization and file and printer sharing |
| Required | nmb | nmbd | (NetBIOS name server) Resources browsing |
| Optional | winbind | winbindd | For host and user name resolution |

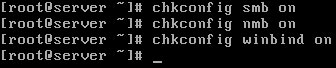
If you have just installed RPM than these service would be stopped.



Start necessary services



Make sure the services are running at the next time Linux is booted



How to allow samba through firewall

During the RHCE 6 exam we will have both firewall (iptables) and SELinux protection.

To make Samba to communicate outside the server we have to configure iptables and SELinux.

How to allow Samba in iptables

SAMBA uses ports 137,138,139 and 445

|  |  |
| --- | --- |
| Port 137 | UDP NetBIOS name service (WINS) |
| Port 138 | UDP NetBIOS datagram |
| Port 139 | TCP NetBIOS Session (TCP), Windows File and Printer Sharing |
| Port 445 | Microsoft-DS Active Directory, Windows shares (TCP) |
| Port 445 | Microsoft-DS SMB file sharing (UDP) |

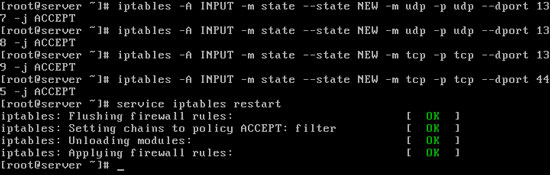
To open firewall for Samba adds the following rules and restart the iptables

#iptables -A INPUT -m state --state NEW -m udp -p udp --dport 137 -j ACCEPT

#iptables -A INPUT -m state --state NEW -m udp -p udp --dport 138 -j ACCEPT

#iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 139 -j ACCEPT

#iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 445 -j ACCEPT



How to allow Samba server from SELinux firewall

SELinux as a security feature prevents any viewing of a share automatically. SELinux is the complex security features of Linux. For RHCE 6 exam you should know following SELinux booleans

|  |  |
| --- | --- |
| samba\_enable\_home\_dirs | Enables the sharing of home directories |
| samba\_export\_all\_ro | Enable read-only access to any directory |
| samba\_export\_all\_rw | Sets up read/write access to any directory |
| samba\_share\_t Default file | which Samba can share |

You can enables samba\_export\_all\_ro or samba\_export\_all\_rw Booleans in lab environment but it in real life that would be a security risk. Its good habit to set a file types for file and directories which need to be share via Samba. You can do that with following command

# chcon -R -t samba\_share\_t /sharedata

In this example we enable /sharedata directory. Now Samba can share this directory.

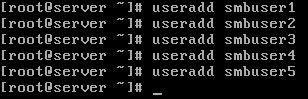
To share the default home directory run following command:

setsebool -P samba\_enable\_home\_dirs on

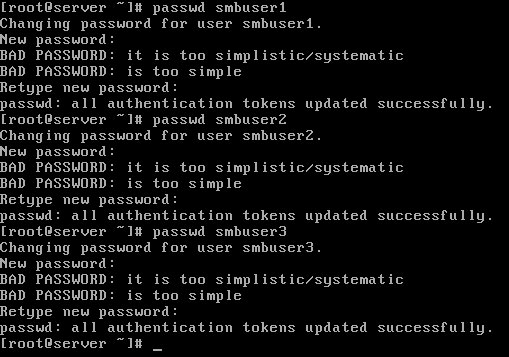
-P makes sure the change preserve after reboot.

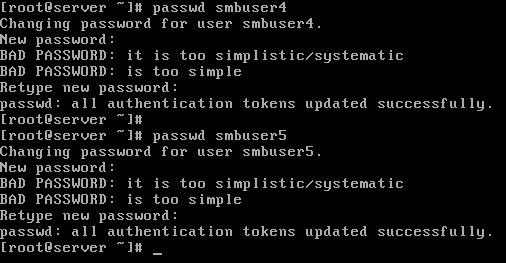
setbool

You can create a new Samba user only from valid accounts on a Linux computer so create 5 users

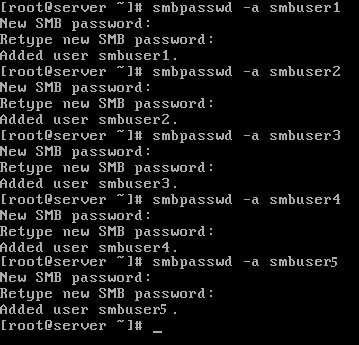


Set password for all users. Avoid setting password for local system if you only creating these users for Samba service and do not want to grant them local system access.

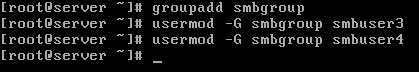




Command smbpasswd -a can be used to add a user to the password database under /etc/samba/ for SAMBA authentication. Set up Samba users with the smbpasswd command.



Create a smbgroup and add smbuser3 and smbuser4 users



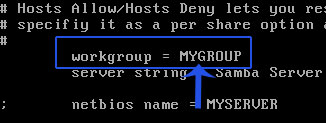
Now open main configuration file of Samba

vi-smb-conf

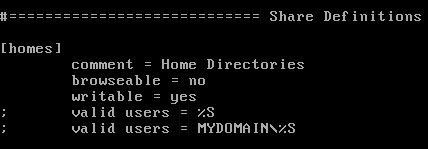
The smb.conf file includes two types of comment lines.

* The hash symbol (#) is used describes a feature
* The semicolon (;), used to comment out feature (Add ; to disable the feature, remove ; to enable the feature)

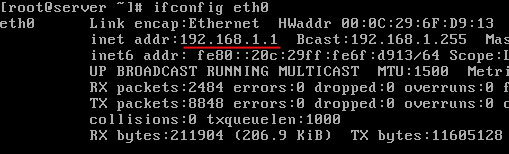
Note down the value of workgroup directory



It would be same on network for seamless connectivity

Now navigate to **Share Definitions** section By default Samba automatically share the home directory of the logged-in user which is define in the first four lines of this section.   
**browseable = no** limit user to his own home directory. Samba reads home directory information from **/etc/passwd** file so you need not to specify the home directories path.  


Close the **smb.conf** file now and Note down the IP address of server



That's all configurations which we need right now on server.

Configure Samba client on Linux system

On Samba client following RPM are required

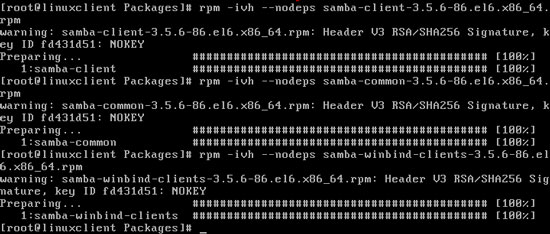
* samba-client
* samba-common
* samba-winbind-client

rpm-qa-samba-client

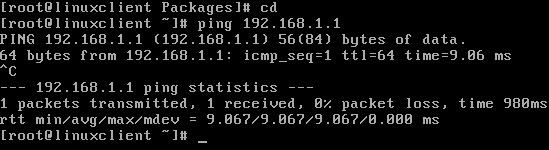
Mount RHEL 6 disk in media folder and move to Package directory



Install RPM if required.



Check connectivity from Samba Server.



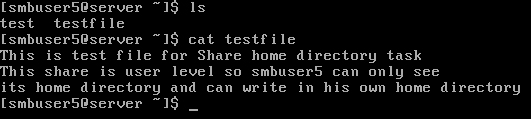
Try to list share from Samba server with smbuser1



To verify "Share user home directory" [lab task], list the share from smbuser5 and create a sambatmp folder. Logged in from smbuser5 and mount his home directory in sambatmp folder. To make sure user have writeable permission also create a test file.



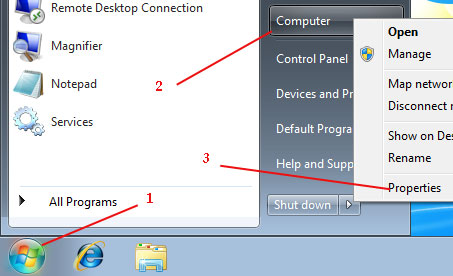
Go on server system and logged in from smbuser5 and verify the testing.



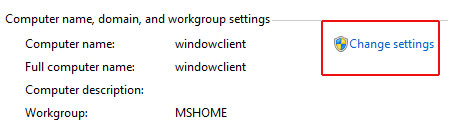
We have successfully configured Samba client on Linux client system.

Configure window 7 as Samba client system

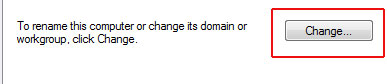
Open computer properties



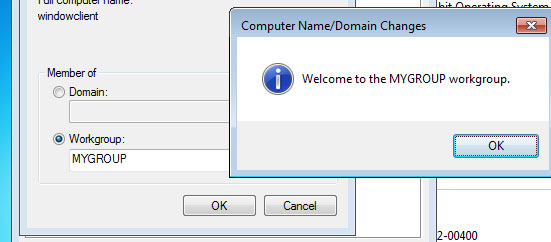
Click on change setting



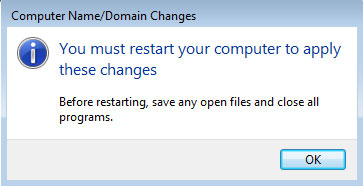
Click on change



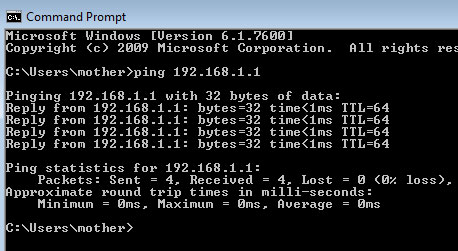
Change workgroup name to MYGROUP



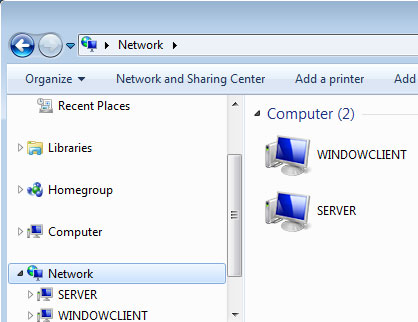
System restart is required, confirm restart



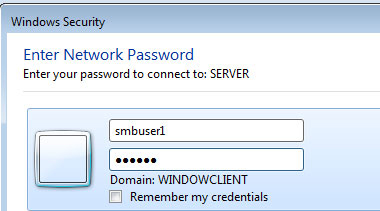
After system restart Check connectivity form Server



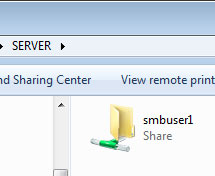
Open Network and click on server system



Login from smbuser1



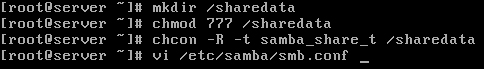
User will be logged in his home directory



We have successfully configured window 7 as a client system of Samba.

Create a sharedata folder on server. Grant read and write access to public on sharedata folder. Share publicly this folder. Test form linux and window client.

On Server create a **/sharedata** folder. This folder is created from root user so our users will not be able to write in this folder. Change its permission 777. Configure SELinux Boolean . Now open the **smb.conf** file



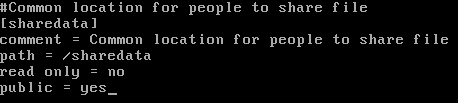
This share of **/sharedata** will share a common location where user can download / upload / read the files. In this end of file add following stanza and save the file

# Common location for people to share files [sharedata]

comment = common location file sharing

path = /sharedata

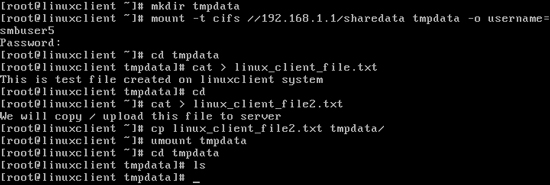
read only = no public = yes



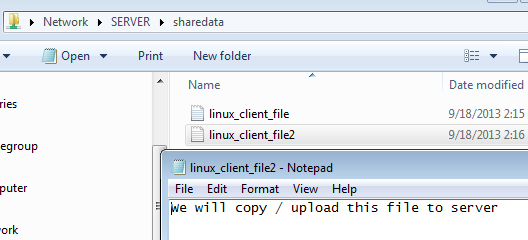
Restart the **smb** service

restart-smb

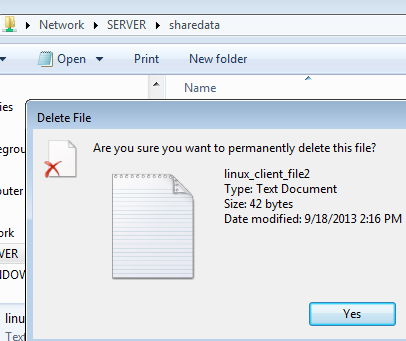
On linuxclient create a **tmpdata** directory and mount the **sharedata** folder in it. Create test files.



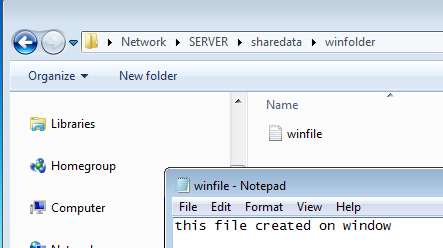
sharedata is a temporary folder and we have shared it with full permission for everyone. It means other user should be able to read / write the file made from smbuser5. To test it go on window system and open server system from network. Open sharedata folder and read the file



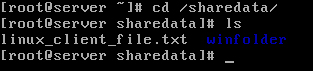
Now delete this file.



Make a folder and create file in it



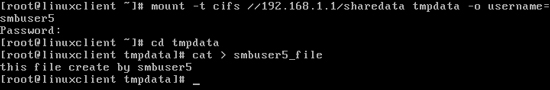
Check these on Server system.



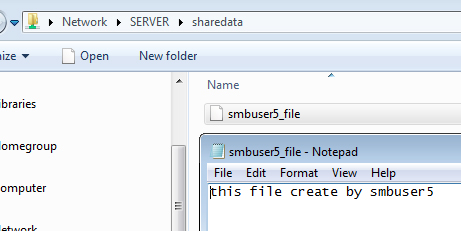
In above example we shared a folder in insure way where any user can delete others file and folder. Now make it little bit secure. Go server and change permission to 1777

set-stickybit-sharedata

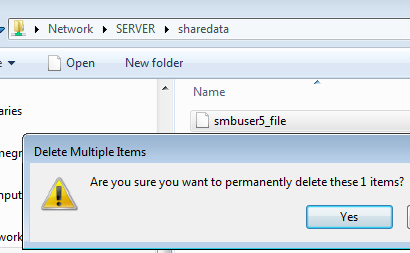
On linuxclient logged in from smbuser5 and create a file



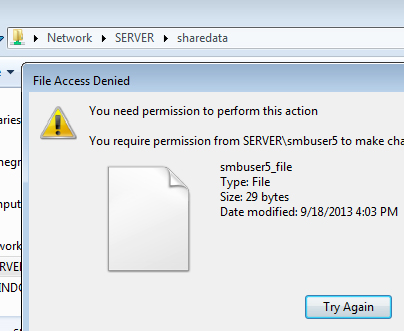
On window we are logged from smbuser1, try to read the file.



Now try to delete this file.

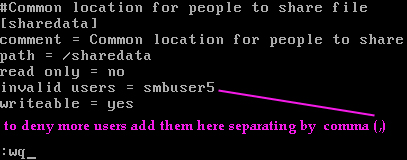


It will be denied



How to deny users in Samba

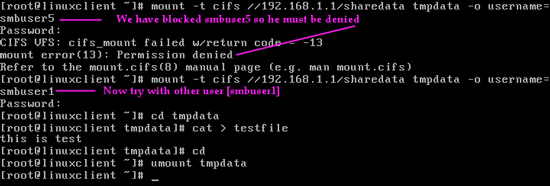
Samba allows you to deny user / users from shared resources. To deny **smbuser5** from **sharedata** open **/etc/samba/smb.conf** and change configuration value to following and save the file



Reload the smb service

reload-smb

On linuxclient system first try to mount sharedata from smbuser5 and than from smbuser1



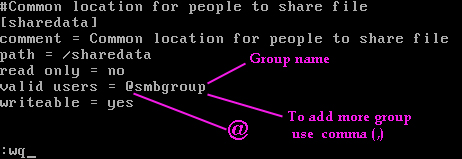
How to limit samba to group

We have created a group smbgroup above in this tutorial. Now configure Samba to allow access only to this group.

On server change the group of sharedata and update the permission to 1770. Open the **smb.conf** file

chgrp-sharedata

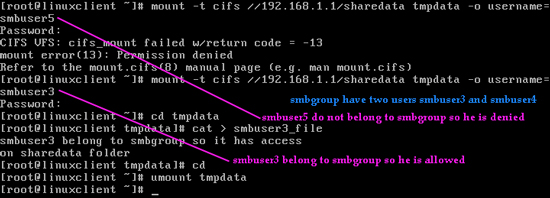
Update the stanza and save the file



reload the smb service

reload-smb

On linux client first try with smbuser5 which is not the member of smbgroup and later try with smbuser3 which is the member of smbgroup



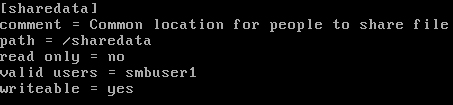
How to limit samba to users

Now we will share only for user/ users. Now configure Samba toallow only smbuser1 on sharedata folder.

On server make smbuser1 the owner of /sharedata folder and update the permission. Open the smb.conf

samba-user-share

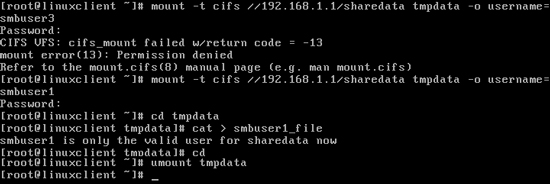
change the stanza and save the file



Reload the file

reload-smb

On linuxclient first try with other users and latter try with smbuser1

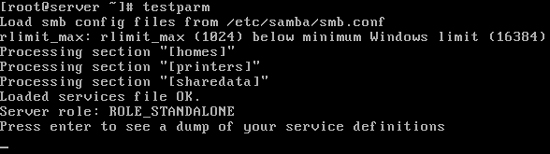


So far in this article we have configured different level of access for Samba share. For RHCE 6 exam always remember that file permissions, file system mount options, SELinux Booleans, ACL cannot be overridden by Samba. Its mean that if a directory does not have write permission and you have Samba setting writeable = yes, it will not allow to write. This is the reason why we first update the file system permission than we set Samba settings.

During the RHCE 6 exam following 2 commands can be very handy for you.

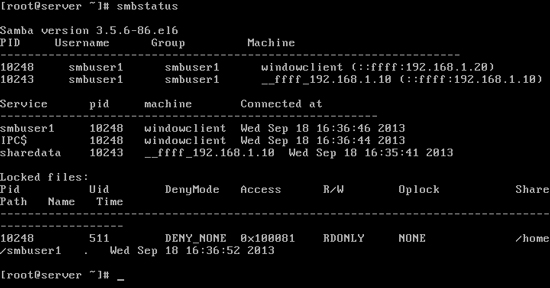
testparm

**testparm** command will check **smb.conf** file for internal errors. If output of this commands return without any errors, you use the configuration file.



smbstatus

This command will list the current Samba connection.



For RHCE 6 exam should also know following directives of smb.conf file

How to change samba server name [NetBIOS]

By default Samba hostname as a NetBIOS name. NetBIOS is name which other clients see in network browse lists such as those shown from a Microsoft net view command or a regular Linux smbclient command. To change the Samba server name uncomment and change the value of following directive.

; netbios name = MYSERVER

How to change samba workgroup name

Default workgroup name of Samba is MYGROUP. You can update it form smb.conf file. To change the default workgroup name update the value of following directive.

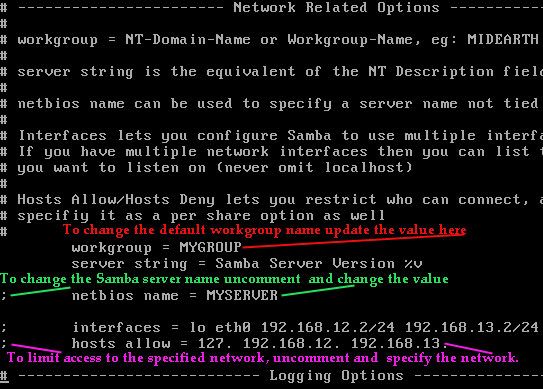
workgroup = MYGROUP

How restrict samba to local network

To limit access to the specified network, uncomment the following directive and give specify the network.

; hosts allow = 127. 192.168.12. 192.168.13.

If you uncomment without change the value it would limit access to the networks with the 192.168.12.0 and 192.168.13.0 network IP addresses, as well as the local computer (127.): You can also configure the hosts deny directive. Configure host allow/deny directives here only if you want to need make change globally. Individually shared directories can also be configured with hosts allow / deny. So if you are seeking for individually configurations do it in their own section.



That's all for this article.