SAMBA

Sharing files with Windows hosts

What is SAMBA?

- A number of open source protocols that enable Linux machines to exchange files and share printers with Windows as well as other systems like MAC and DOS.
- SAMBA uses TCP/IP for communication. It uses NetBIOS and TCP/IP for the naming services.
- For file sharing, the CIFS (Common Internet File System) is used. This is an open-source implementation of the SMB (Server Message Block) protocol.
- With SAMBA you can enjoy the security and stability of Linux as a file server while continuing to use you Window clients.
- When a filesystem or a directory is shared through SAMBA, it appears in Windows Network Places just like any normal Windows share

Installation

- SAMBA has a number of packages, each of which provides a different functionality. They can be installed through the package manager (yum or apt-get). They can be listed as follows:
  - samba: this includes the service daemon (smbd) and the NetBIOS service daemon (nmbd)
  - samba-common: contains the configuration files (like smb.conf)
  - samba-client: contains client tools that are used to connect and query remote SMB hosts like `smbclient`
  - samba-windbind: contains tools that allow a Linux machine to join a Windows Active Directory domain and use Windows users and groups for authentication
- Once done, you can launch the daemons using `service smb start`

Querying shares

- You can query shares on your local machine as well as on other SAMBA based or Windows machines using the smbclient command
- The syntax is as follows: `smblcient -L host`
- Press ENTER when prompted for a password
- If a name server is not available on the domain, you can start the SAMBA name server by issuing service nmb start, which will provide NETBIOS names for the hosts.
- The output of this command shows the available directories and printers offered by the queried host

Allowing access through iptables

- If you are using the firewall, the following ports must be enabled on the firewall:
  - 445 (TCP): this is the port on which smbd daemon listens
  - 139 (TCP): used for the NetBIOS hostname resolving
  - 137 and 138 (UDP): used by the nmbd daemon. Open them only if you intend to use nmbd for incoming requests
  - By default, ESTABLISHED and RELATED packets should be enabled

Configuring shares

- Shares can be configured by editing the /etc/smb.conf file. Lines starting with semicolon (;) are commented out.
- The file already has three defined sections:
  - [global]: contains settings that apply to the whole server. You can configure the workgroup name, log file location, type of security, among other settings
  - [homes]: by default users on a SAMBA server are able to access their home directories remotely. This section defines whether they can only browse their directories or they can write and modify files as well.
  - [printers]: configures whether or not printers are shared (through CUPS)

The [global] section

- The most important options can be listed as follows:
  - `workgroup:` this is the domain name that appears to the client when connecting to the server.
  - `netbios` name: this is the name of the server as it appears to clients. If commented out, the hostname is displayed
  - `log file:` specifies the location of the log file. The %m corresponds to the hostname or the IP address of the machines connecting to the SAMBA share.
  - `max log size:` specifies the maximum log file size after which it gets rotated. That is, the file is renamed to have .old appended to it while new data gets written to a new file. The default is 50k.
  - `interfaces:` it can be used to lockdown SAMBA to listen only only specific network interfaces or IP address
  - `hosts allow:` can be used to restrict access to only specific hosts. No asterisks used here, you just enter the first part of the address and to match the whole subnet. For example 192.168.0. will match all hosts that have IP address from 192.168.0.1 to 192.168.0.254 this can be followed by a netmask like /255.255.255.0

The [homes] section

- This section is used to give the system users access to their own home directories via SAMBA. The following are the most important options:
  - browseable: hides SAMBA servers from being discovered (like from Network Places in Windows).
  - writable: if set to yes, users can add and delete files in their home directories
  - valid users: if this value is commented out, any valid user on the system can log on. However, if it is uncommented and set to %s this will restrict access to users of the service (SAMBA users). It can be also preceded by a domain name like MYDOMAIN\%s to restrict access to users of a specific domain.

The [printers] section

- Printers that are configured using the CUPS protocol is available for network printing by the SAMBA services if printable = yes.
- If cups options = raw that means that SAMBA will let Windows clients use their own drivers for printing. The shared printer will be just a raw one
- Other options can be set like writeable and browseable, which provide the same functionality as shared directories.

LAB: creating and using a SAMBA share

- Target: create a shared directory that can be accessed by Windows hosts.
- Create a directory that will be used as a SAMBA share /samba
  mkdir /samba
- Create a local user that will be the owner of this share
  useradd joe
  passwd joe
  chown joe:joe /samba
- Add this user to SAMBA users to be able to access the share:
  smbapasswd –a joe
- Add an entry to /etc/samba/smb.conf to configure the shared directory:
  [Windows share]
  comment = This is a test Windows share
  path = /samba
  read only = no
  browseable = yes
  valid users = joe
- Restart the service to apply the changes
  service smb restart
- Try to access the shared directory from a Windows machine and ensure that you can read and write files.