RHCE
BOOT CAMP

File Sharing Services

redhat®

CERTIFIED
ENGINEER

NFS

- The Network File Service, or NFS, is used to share data with other servers.
- For this service to work properly, `portmap` and `nfs-utils` rpms must be installed, and `portmap` and `nfs` must be running.
- The command `rpcinfo` can be run to confirm that these services are running on a remote server:
  - `rpcinfo -p server1`
- The directories to be shared are listed in `/etc/exports`

/ETC/EXPORTS

- The directories to be shared are listed in `/etc/exports`
- `/etc/exports` should be configured as follows:
  - `<shared directory> <who>(<how>)`
- Note the **lack** of space between the who and the parenthesis for how. Be very careful about this!
- Example:
  - `/to/be/shared  station*.example.com(rw)`

EXPORTS NETWORK SPECIFICATIONS

- The host/network to be shared to can be specified in a number of convenient ways:
  - **Host** — Just a single host (given by name/ip)
  - **Netgroup** — NIS netgroup, expressed as `@group`
  - **Wildcards** — Using the asterisk, match based off hostnames plus wildcards, as `*.example.com`
  - **IP Networks** — Specify with IP/netmask or CIDR notation:

    `192.168.1.0/24`

    `192.168.1.0/255.255.255.0`

EXPORTFS

- **`exportfs –r`** refreshes the server share list
- **`exportfs –a`** exports all shares in /etc/exports
- **`exportfs –u`** un-exports a share name
- **`showmount -e server1`** shows shares on server1

NFS PERSISTENCE

- NFS mounts can be made persistent across reboots by adding the following to `/etc/fstab`:
  - `server1:/share  /server1/share  nfs  defaults 0 0`

LAB

1. Create a new user.

2. Configure your anonymous NFS user to use this new UID.

3. Grant read/write access to a directory this user owns to our class network, except for server1, who should get read-only access. (Bonus: Does the user name matter?)

4. Mount the NFS share from your neighbour, and add it to their `fstab`.

VSFTPD

- VSFTPd is the default ftp server
- The primary configuration file is `/etc/vsftpd/vsftpd.conf`
- Provides two levels of user access:
  - **Anonymous:** by default these users are chrooted to `/var/ftp` for security
  - **User:** these users authenticate with a username/password and can download any file they can read and can upload into any directory in which they have write access
- Individual users can be denied by placing their names in:
  - `/etc/vsftpd/ftpusers`

LAB

1. Configure VSFTPd to only allow the user `richard` to ftp to your server.

2. Make sure that `richard` is chrooted to his home directory upon login.

3. Configure your FTP server to allow anonymous access, chrooted to `/srv`

SAMBA

- SAMBA is an open source implementation of Windows networking protocols. With SAMBA, it is possible to:
  - Provide file and print services for various Microsoft Windows clients
  - Integrate with a Windows Server domain as a Primary Domain Controller (PDC) or as a Domain Member.
  - Be part of an Active Directory domain.

SAMBA

- SAMBA provides the following services in Linux:
  - Authentication and authorization of users (Active Directory)
  - File and printer sharing
  - Name resolution
  - Browsing (Wins or NetBios)

GETTING SAMBA GOING

- Four packages must be installed for SAMBA to work as desired:
  - **`samba`** provides basic software for sharing files and printers
  - **`samba-client`** allows server to connect to windows shares (also includes the smbclient command, which functions like a command-line ftp client)
  - **`system-config-samba`** GUI configuration tool
  - **`samba-common`** contains samba configuration files

GETTING SAMBA GOING

- For SAMBA to work properly, the following services must be running:

  - `smbd` (SMB/CIFS Server) for authentication and authorization and file and printer sharing

  - `nmbd` (NetBIOS name server) for resource browsing and possibly as a wins server

CONFIGURING SAMBA

- The main configuration file for SAMBA is:
  - `/etc/samba/smb.conf`
- This file is **very** well commented and has examples for just about anything that you need to do.
- Once you have made a configuration change, you can test it with the `testparm` command.

SAMBA USERS

- To have a SAMBA user, that user must first be created in `/etc/passwd`
- The command `smbpasswd -a` can then be used to add a user to `/etc/samba/smbpasswd` for SAMBA authentication.

SAMBA SHARES

- To see the SAMBA shares a user has access to, you use `smbclient` as follows:
  - `smbclient -L <server> -U <user>%<passwd>`
- To mount a share, you use the UNC path:
  - `mount.cifs //server/share /mount/point -o username=<user>`
- To configure this mount to happen at boot, add the following to `fstab`:
  - `//server/share /mount/point cifs  credentials=/etc/samba/pub.cred 0 0`
- (where `/etc/samba/pub.cred` is a file that only root can read which contains usernames and passwords)

LAB

1. Configure SAMBA to share your `/srv` directory only to one neighbor who must log in with the SAMBA username of `richard`.

2. Make this share read-only for the SAMBA user `guido`.

3. Mount the share from your neighbor. Configure it to mount automatically at boot time. Use a credentials file to store the account information securely.

```
slideshow.end();
```