ITB721/ITN721 Unix Network Administration

Practical 3

The new commands you will need for this practical include "ln", "quotacheck", "edquota", "repquota", "tar". Browse these **and other** relevant man pages immediately before using the commands.

Exercise 1: Mounting Remote CIFS Shares

This exercise must be done in the laboratories. In this exercise, you will be connecting to the student file server, nas.fit.qut.edu.au (IP address 131.181.70.16). nas.fit.qut.edu.au uses CIFS to export student home directories to certain computers.

1. Display a list of all exported directories from nas.fit.qut.edu.au which are available for mounting.
2. Create a mount point /mnt/nas on your computer.
3. Mount the share HOME (read write) from nas.fit.qut.edu.au (in this case you must use the IP address) onto the mount point /mnt/nas on your computer, also being sure to specify the workgroup "qutad" on port 139.
4. View the contents of the /etc/mtab file and write down the relevant entry from that file.
5. View the contents of your nas.fit.qut.edu.au directory from your mount point.
6. Copy a file (eg prac3file) from your home directory on your local machine to your directory on nas.fit.qut.edu.au.
7. Unmount the mount point. (First perform all necessary steps in order to be able to unmount.)
8. Confirm that you are no longer mounted to nas.fit.qut.edu.au by again viewing the contents of the /etc/mtab file.

Exercise 2: Mounting Remote NFS Shares

This exercise must be done in the laboratories. In this exercise, you will be connecting to the laboratory Linux server, athena.fit.qut.edu.au (IP address 131.181.116.21). Athena uses NFS to export certain directories to the computers in the laboratories.

1. Display a list of all exported directories from athena which are available for mounting.
2. Create a mount point /mnt/athena on your computer.
3. Mount the directory /pub/721 (read only) from athena onto the mount point /mnt/athena on your computer.
4. View the contents of the /etc/mtab file and write down the relevant entry from that file.
5. View the contents of the shared directory from your mount point.
6. Unmount the mount point (carefully).
7. Confirm that you are no longer mounted to athena by again viewing the contents of the /etc/mtab file.

Exercise 3: Exporting NFS Shares

1. Start up two Xen virtual machines, virtpc1 and virtpc2.
2. On virtpc1, configure the eth0 interface with the IP address 192.168.20.1, netmask 255.255.255.0 and broadcast 192.168.20.255. Activate this interface.
3. On virtpc2, configure the eth0 interface with the IP address 192.168.20.2, netmask 255.255.255.0 and broadcast 192.168.20.255. Activate this interface.
4. Test the connectivity between virtpc1 and virtpc2.
5. On virtpc1, create a new user account and password for Mr W Brown.
6. As "wbrown", create a directory within his home directory called "pub-wb". Check that the permissions on "pub-wb" give other users read and execute access to this directory.
7. Following on from Question 6, as wbrown, **use a single command line** for "find" to locate all files in the /etc directory with a filename beginning with the string "hosts" and copy these files to this "pub-wb" directory. **Note that the copying should be performed as a part of the single command line for "find".**
8. On virtpc1, as the root user, export wbrown's "pub-wb" directory to all users on virtpc2 allowing them to have read only access to that directory. Then, on virtpc1, execute the command line "service nfs restart". (Services will be discussed in Lectures 4 and 5.)
9. On virtpc2, list all the shares that have been exported from virtpc1. Ensure that wbrown's "pub-wb" directory has been successfully exported.
10. On virtpc2, as user vmuser, create a mount point in your home directory called /home/vmuser/mnt.
11. On virtpc2, as the root user, mount wbrown's "pub-wb" directory in read only mode from virtpc1 onto the mount point, /home/vmuser/mnt, to allow the user vmuser to share wbrown's pub-wb directory.
12. View the /etc/mtab file on virtpc2 and write down the relevant entry.
13. On virtpc2, as the user vmuser, change into the /home/vmuser/mnt directory and list the files within it to verify that they are the same as those in /home/wbrown/pub-wb on virtpc1. Also, verify that you cannot create files within the /home/vmuser/mnt directory, and that you cannot modify any files in this directory.
14. On virtpc2, as the root user, unmount the mount point (carefully).
15. Poweroff virtpc2.
16. Poweroff virtpc1.

Exercise 4: Quota Management

1. Find and read Sections 1.1, 3.5, 3.6, 4.1, 4.4, 4.5, 4.6, 5.2 and 5.3 of the Quota mini-HOWTO.

   The remaining questions in this exercise are to be done on the virtual machine, virtpc1.

2. Start up virtpc1. On virtpc1, prepare the / partition's file system for quotas pertaining to individual users. This involves editing the /etc/fstab file to enable user quota support. Then, activate this by powering off virtpc1 and then starting up virtpc1 again.
3. Log in to virtpc1 again. Create the quota file using the "quotacheck" command with appropriate options. This should create a file in the / directory. What is the name of this file?
4. Set the quota for the vmuser user to be a soft limit of 6000 blocks, and a hard limit of 8000 blocks. Write down the steps you took in order to do this.
5. Set the maximum time that the soft limit can be exceeded to 4 hours (grace period).

6. Turn quotas on, then generate a quota report showing the current utilization of disk space.
7. As the user vmuser, copy some large files into /home/vmuser until the soft limit is exceeded. Write down the message displayed on the screen. As the root user, how do you determine which users have exceeded quota?
8. As the user vmuser, copy more files into /home/vmuser until the hard limit is reached. What happens once the hard limit is reached?
9. Poweroff virtpc1.

Exercise 5: Backing Up

This exercise is to be done on the parent machine.

1.
    a. As the root user, create a backup of all the files in the /etc directory, including all its subdirectories and contents. This backup should be an uncompressed tar archive file. Record the size of this uncompressed tar archive file.
    b. Compress the archive in gz format. Check the size of the compressed archive file and compare it with the uncompressed archive file size. What percentage reduction was possible with the compression?
    c. Delete the compressed tar archive file.
2.
    a. As the root user, create a directory /archive.
    b. In the directory /archive, create a compressed tar archive file of the entire contents of the /home directory, including all its subdirectories and their contents.
    c. While still in the directory /archive, extract the contents of this compressed tar archive and check that the extracted files are the same as those originally archived.
    d. Delete only the contents of the /archive directory.
3. **This question of Exercise 5 is additionally required to be done by ITN721 students (but is optional for ITB721 students).** Following on from Question 2, write a shell script that creates in the /tmp directory, an incremental backup (a compressed tar archive file) of all files in the /etc/mail directory that have been modified in the last 72 hours. The script should specify this file to be created with the name HHMM-DD-MM-YYYY.tgz, that is, an incremental backup performed at 10:00pm on 14 March 2007 should be called 2200-14-03-2007.tgz (read about the "FORMAT" option in the man page for "date" for assistance with this). The shell script should then copy the compressed tar archive to the /archive directory and then remove it from the /tmp directory. Thoroughly test that this shell script is working correctly.

    Note that there are many ways to do this. One way, for example, could be to use an appropriate "find" command line, a "tar" command line, a "cp" command line and an "rm" command line within the shell script.

Exercise 6: More Searching

1. As the root user, use a single "find" command line to locate all the files on the system with a filename ending in the extension "conf", and simultaneously display the number of lines in each of those files.

2. Use a "sort" command line to display a sorted list of the entries in the /etc/passwd file in ascending numeric order of group ID.
3. Use a single "find" command line that finds all files in the /etc directory with a filename starting with the string "issue", and deletes the read permission for the owning group of these files.
4.
    a. As a normal user, use a "find" command line which displays all files on the system with the string "xinetd" in the filename.
    b. As a normal user, use a "find" command line which displays all files on the system with the string "xinetd" in the filename, and which directs any output errors to the pseudo device, null.
