ITB721/ITN721
Unix Network Administration

Lecture 3
File System Administration and Data Management

Lecture Content

- Local Data Storage Devices
- Local File Systems
- Networked File Systems
- Data Management

Local Data Storage Devices

Include

- Hard disk drives
- Removable disk storage media
- Portable storage devices

Hard Disk Drives

- Normally physically built into computer
  - Not user removable
- Typical capacities today around 80-750GB (1 Gigabyte = 10^9 bytes)
- Operating system usually installed on hard disk drive

Hard Disk Drive Partitions

- Hard disk drive may be split into several independent partitions
- Each partition
  - functions as a separate hard disk drive
  - can be formatted with a different file system type
  - can have a different operating system
- Primary or extended
- Partitioning
  - managed using the partition table

Partition Table

- Essential part of every hard disk drive
- Stores information about the partitions including
  - sizes
  - start/end location on hard disk
  - file system type
- Can use "fdisk" command to display/edit

Partitions

- Primary Partitions
  - Maximum of four primary partitions, then one extended
  - Kernel should be stored on a primary partition
  - One primary partition marked as bootable (active)
- Extended and Logical Partitions
  - Necessary if more than four partitions required
  - Extended partition consists of logical partitions
  - Logical partitions behave like primary partitions

Removable Disk Storage Media

- Include floppy disks (largely obsolete), CDs, DVDs
- Can be removed and exchanged or transported
- Requires hardware drive, usually installed in computer
- Formatted for particular file system type

Removable Disk Storage Media Capacity

- CD (Compact Disc)
  - Stores ≈ 700MB of data
- DVD (Digital Versatile Disc)
  - Stores almost 5GB of data (on 1 surface)
  - can get up to 4 surfaces available
- BD (Blu-ray Disc)
  - Stores 25GB of data (on 1 surface)
  - Can get up to 2 surfaces available

Portable Storage Devices

- Include USB flash drives, mobile phones, digital cameras
- Typically plug into USB port
- Formatted for particular file system type

Local File Systems

- Used to organize, store and manage data files and their attributes
- Each file system of a particular type
- Each file system type has own standard scheme for representing files, directories and file information
- Each local data storage device formatted with appropriate file system type

File System Types for Hard Disk Drives

- One file system per partition
- Each partition formatted with appropriate file system type
- Possible to have same file system type on multiple partitions

Native File System Types for Linux Hard Disk Partitions

- ext2: earlier file system type
- ext3: newer file system type
  - includes journalling support
- Swap file system type
  - swap partition formatted for temporary swap space

Structure of Linux Hard Disk Partitions

- Minimum is root "/" partition
- /boot partition often also required
- Usually also has swap partition
- If large system, common to also have, eg,
  - /home partition
  - /var partition
  - /tmp partition

Linux Hard Disk Partitions

- Each formatted with ext2 or ext3 file system type (other than for the swap partition)
- Normally partition is read-write
- Partition device files are named
  - for IDE, EIDE hard disk drives, eg
    - /dev/hda1 – first partition on first drive
    - /dev/hdb3 – third partition on second drive
  - for SCSI, SATA hard disk drives, eg
    - /dev/sda1 – first partition on first drive
    - /dev/sdc2 – second partition on third drive

File System Types for Removable Disk Storage Media

- Particular file system uses appropriate block sizes
- Commonly supported types allow media to be used on different operating systems
- Media must not be removed while system still reading from or writing to it

File System Types for CDs and DVDs

- ISO9660
  - Can only be used on CDs
  - Read only file system type
- UDF (Universal Disk Format)
  - Used on DVDs and BDs (can be used on CDs also)
  - Read only file system type

File System Types for Portable Storage Devices

- Particular file system uses appropriate block sizes
- Designed to handle device attachment and removal while computer is running
  - but unmount before removing

File System Types for USB Flash Drives

- Typically FAT/VFAT file system
- Can be mounted as read-write or read only file system
- Most newer USB flash drives permit multiple partitions

Accessing Local Data Storage Devices in Linux

- Must be mounted in order to access
- Device mounted onto an existing local subdirectory
  - Known as a "mount point"
- Files and directories which are accessible start from that mount point

Mount Point

- A directory on your local system (but should be carefully chosen)
- Mount points for temporary mounts usually in /media
  - eg /media/disk, /media/cdrecorder
- Hard disk drive partitions (eg /, /home, /var, /tmp) are usually automatically mounted

Local Mounting in Linux

- Use "mount" command
- "-t" option specifies file system type (eg ext2, ext3, msdos, vfat, nfs, iso9660, udf)
- General format of command line

  # mount -t <file system type> <device> <mount point>

- Example Mount Command Lines

  # mount -t iso9660 /dev/hdc1 /media/cdrecorder

  # mount -t ext3 -o rw /dev/hda2 /home/staff

Automatic Mount at Boot

- Devices listed in /etc/fstab are automatically mounted at boot
  - Unless "noauto" option is listed
- Specified mount points, file system types, options etc for each device are stored in /etc/fstab
  - Possible to specify local and remote mounts

Active Mounts

- Important to keep track of active mounts
- Information on active mounts stored in /etc/mtab
- Lists both local and remote mounts
- Includes temporary mounts as well as boot time mounts
- Can use “df” command to list and monitor size and usage of mounted file systems (also available space)

Unmounting

- Always unmount temporarily mounted file systems
  - Completes writing of data from cache to device
  - Enables safe removal
- Failure to unmount can cause loss of data

umount <mount point>

Networked File Systems

- Enables files to be accessed within and between networks
- Commonly used to access file servers
- Centralizes file storage
- Client mounts exported shares on server
- Requires careful security consideration

Principles of Networked File Systems

- Typically local directory (share) on server, exported by server
  - client workstation mounts exported share
- Standard protocols for mounting remote file systems include
  - NFS (Network File System)
  - CIFS (Common Internet File System)

NFS: Network File System

- Developed for Unix
- Fully implemented in Linux
- Windows versions exist
- Exports directories to particular systems or networks
- Uses Client/Server model

NFS: Server

- Entries for exported directories in /etc/exports file
- Checks incoming mount for authorization
  - Based on requested directory, IP address of requesting system etc
  - No user level access control

Sharing Files in NFS

- /etc/exports lists exported paths, authorized clients, access rights eg

```
/home/user1/share    s622-81.fit.qut.edu.au(rw)
/home/user2/project   *.qut.edu.au(ro)
/home/user3/pub       131.181.116.81(ro)
```

- After any changes, restart the nfs service by typing in

```
# service nfs restart
```

(More on services in Lectures 4 and 5)

NFS: Client

- "mount" command supports NFS file system type
- Mount point must be existing local directory
- Only root can NFS mount (unless users are given access by root)

showmount -e <nfs server>

  - Lists directories (shares) exported by server

mount -t nfs <share> <mount point>

- share is
  - <hostname>:<path>
  - eg files.fit.qut.edu.au:/home/n1234567/task

CIFS: Common Internet File System

- For accessing remote file systems
- Includes remote printer access capability
- Not specific to particular operating system
  - Available for Unix, Windows etc
- Based on SMB (Server Message Block)

CIFS Configuration on Linux

- Configuration file is /etc/samba/smb.conf
  - Exported shares listed as sections
  - Specifies access control to shares
- Access to exported shares can be restricted, eg
  - Username/password
  - IP address
- Restart “smb” service

Mounting CIFS Shares

- “mount” command line with “cifs” file system type
- Specify share as //<hostname>/<sharename>
- Can use "smbclient" command line
  - to list exported shares
  - for interactive access

Data Management

- Aspects include
  - Quotas
  - Current Data Storage
  - Backups
  - Data Transfer

Quotas

- Limit on disk space used by user (or group of users)
- Allows hard disk drive partition to be shared reasonably and fairly
- Prevents extensive resource consumption by particular user/s
- Normally applied to partition containing home directories and other data directories
- Not normally applied to system only partitions
- Can be set up for individual users and/or groups of users

Quota Limits

- Most common limit is total number of blocks used
  - sum of sizes of all files owned by user/group
- Can also limit total number of inodes used
- Soft and hard limits
  - Hard limit cannot be exceeded
  - Soft limit can be exceeded for grace period
  - Grace period resets once soft limit no longer exceeded
  - Example of block limits
    - Soft limit: 600000 blocks, Grace period: 7 days, Hard limit: 900000 blocks

Actions on Limit Breach

- Display warning message on console
- Possible to
  - Email user when limit is approaching
  - Email user and/or System Administrator
- Once hard limit reached, cannot write further data to disk

Preparing File System for Quotas

- /etc/fstab requires additional option/s
  - "usrquota" for user level quotas
  - "grpquota" for group level quotas
  - reboot to activate changes in /etc/fstab
- “quotacheck” command creates a quota management file
- Other relevant commands for quota management include edquota, quotaon, quotaoff, repquota, warnquota, quota

Current Data Storage

- Include aspects of
  - local data storage
  - file servers
  - live mirrors
  - storage area networks

Local Data Storage

- Storage of data on local data storage devices
- Access to data requires appropriate account rights
- System failure impacts users on that system only
- Backup responsibility typically belongs to each user

File Servers

- Typically machines dedicated to remote data storage
- Typically only networked file system services/protocols available
  - Configured to use, eg, NFS, CIFS
- Security of all data stored depends on security of file server
- Enable central backups to be performed

File Server Deployment

- On dedicated machine
  - appropriate operating system is installed
  - all necessary storage and backup devices are installed/attached
  - connect machine to the network
  - configure machine with required services
  - set up accounts and quotas for users
  - export shares appropriately

Instruct users how to mount file system on file server

Live Mirrors

- Keeps second (or multiple) copy of data with changes updated on-the-fly
- Enables quick recovery if one drive fails
- Often used in highly critical situations where high uptime is required
- Various types of live mirrors, eg RAID

RAID (Redundant Array of Inexpensive/Independent Disks)

- Consists of multiple hard disk drives under control of RAID controller
- Multiple copies of data written onto separate hard disk drives
- Various RAID levels
- Not a replacement for backups

Storage Area Network (SAN)

- Used to store and make accessible huge amounts of corporate data
  - Hundreds of GBs to Terabytes
- Provides large storage repository for systems on the organization's LANs/networks
- Comprised of SAN storage devices, SAN file servers, client computer systems
- Administration very specific to particular SAN product (network)

SAN Architecture

- SAN storage devices connect to SAN file servers
- SAN file servers interact with
  - SAN storage devices; and
  - LAN systems
- Clients on LAN use eg NFS, CIFS to access SAN file servers

Backups

- Essential part of system and network administration
- Protect against loss of data which may be caused by
  - System crash
  - Hard disk drive failure
  - Users deleting files accidentally or maliciously

Backup Media

- CDs: about 700 MB
  - Commonly write once
  - Small capacity: not useful for full unattended backup
  - Possible to get cheap media, but is it worth the quality risk?
- DVDs: about 4-5 GB
  - Also commonly write once
  - Larger capacity than CDs

Backup Media

- Tape drives: up to hundreds of GB
  - Most common form of backup media for medium to large size organizations
- Network: depending on file server capacity
  - Common for workstations to backup to file server
- Storage Area Network (SAN)
  - High speed network connected collection of storage devices and servers

What to Backup

- Data
  - On a regular basis
- System and Configuration
  - Whenever changes are made

Types of Backup

- Full - Entire system
- Differential or delta - Changed or new files since last full backup
- Incremental - Only changed or new files since last full or differential or incremental backup
- Incremental and Differential Backups
  - Quicker to backup
  - Use less storage space
  - Slower to restore (ie need to use full backup and latest differential, or full backup and all differentials and incrementals)

Scheduling Backups

- Must develop backup routine
  - Many possible schedules eg for a Monday-Friday business
    - Monday: Incremental or differential
    - Tuesday: Incremental or differential
    - Wednesday: Incremental or differential
    - Thursday: Incremental or differential
    - Friday: Full backup
- Essential to adhere to the routine
- Full backups are infrequently performed
- Regular incremental backups are common

Testing Backups

- Once backup is complete, must be tested
- Ensure files can be successfully restored
  - Common problem: many administrators do not test
- Backups need to be reliable

Backup Guidelines

- Once backup plan is developed, follow it closely
- Label backup media carefully
- Verify every backup
- Periodically check backups by restoring all files to an empty system or partition
- Secure backups

Security of Backups

- Backup media must be secured
  - Anyone can restore backups
- Consider encrypted backups
  - Must store copy of encryption key safely
- Should have off-site storage of some backups

Using “tar” to backup

- “tar” command line

tar <options> <tar filename> <target>

- Some useful options

  -t list contents of tar archive

  -c create new tar archive

  -x extract files from tar archive

  -z compress/uncompress files

  -f required before tar filename

Data Transfer

- Data always transferred within network or between different networks
- Data on untrusted network must be protected in transit
  - Method varies depending on how data is required to be accessed
  - Must insist on a secure connection

Common Administrator Tasks

- Configuring and managing local data storage devices
- Mounting local and networked file systems
- Managing quotas
- Performing backups
  - Restoring files if lost or deleted

General Ethical Considerations

Topics relevant to this lecture include

- Exporting shares
- Quota management
- Backup management