IT2775 Operations Security

Backup and Recovery

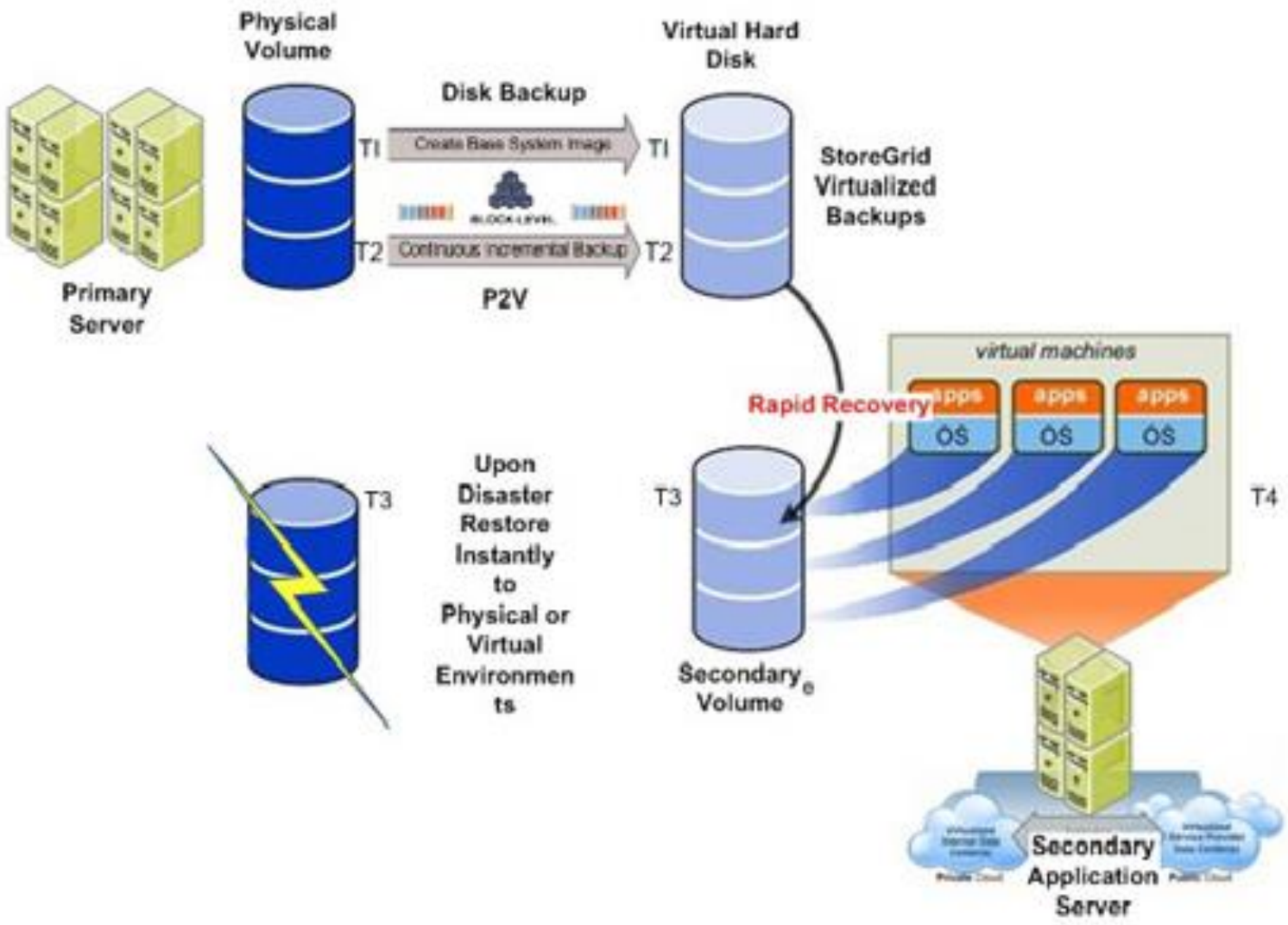
NANYANG POLYTECHNIC

Objectives

- Backup and Recovery
- Backup Media
- Backup Storage
- Backup Integrity
- Backup Encryption

Backup and Recovery

- Backup
  - Process of creating a copy of production data into reliable media for future recovery when needed.
  - Restore production data when it is lost or corrupted.
- Archives
  - Stored data when not required in production.
  - Standards or laws and regulations on data retention
  - Kept only as long as required
    - not to be kept beyond their required and useful life.


Physical Volume
Virtual Hard Disk
Disk Backup
T1
Create Base System Image
T1
StoreGrid Virtualized Backups
BLOCK-LEVEL
T2
Continuous Incremental Backup
T2
Primary Server
P2V
virtual machines
Rapid Recovery
apps
OS
apps
OS
apps
OS
T3
Upon Disaster Restore Instantly to Physical or Virtual Environments
T3
T4
Secondary Volume
Secondary Application Server

Backup and Recovery

- Recovery
  - Process of utilizing the backup media to create a copy of the production data into operational media
  - Effectiveness depend on ability to recover data, when needed.
- Policies
  - Proper authorization is given to restore the data.
- Procedures
  - Recovery done correctly, quickly and efficiently.
  - Estimate actual time needed to recover a system.

Types of Backup Media

1. Tapes
   - ✓ Typically last longer than hard disk media.
   - ✓ Cheaper and higher capacity.
   - ✓ Reliable through integrity checks.
   - ✘ Slow I/O speed.

2. Optical Discs
   - ✓ Fast random and sequential access.
   - ▪ Write-once or re-writable media.
   - ▪ Higher per unit storage cost than tapes
   - ✘ Limited capacity for each disc.

Types of Backup Media

3. Hard Disks

- ✓ Faster I/O speed.
- ✓ Self correcting error checks.
- ✘ Expensive especially for higher capacity.
- ✘ Subjected to disk crash, mechanical faults.

4. Online/Cloud Storage (see additional references)

- ✓ Transfers media failure risks to vendor.
- Depends on network protocols to correct errors.
- Costs depend on vendor and leased bandwidth.
- Speed depends on bandwidth.

Control of Backup Media

- Backup data: Sensitive and critical
  - Malicious theft
  - Opportunistic stealing
  - Accidental misplacement

- Backup media: Weakest link in organisation
  - Tend to overlook their physical security
  - Serious security risk if not handled properly

Backup Storage

- Un-locatable backup = No backup!
  - Store in a secure location
  - Mark clearly to retrieve correct backup
    - Volume no
    - Name and Purpose
    - Media type
    - Date used/created
    - Location
  - Store in database and bar-coded on media.
  - Maintain logs of media movement.
  - Audit complete inventory of media.

Backup Storage

- Onsite storage: Local tape library, cabinets in server room
  - store at the location where backup was made.
  - immediate access for retrieval when required.
  - same physical risks as the server it is backing up
- Offsite storage: Media vaulting, online backups
  - store in an alternate site where backup was made.
  - access is not immediate, e.g. for disaster recovery
  - reduce same physical risk as the server.
  - secure media movement to remote location.

Backup Integrity

- Backups are kept for long periods of time.
  - When required, its failure is typically catastrophic.
  - *"Cannot read media", "Restore failed"*
- Integrity of the media
  - Check at creation time and regularly thereafter.
  - Media preserved with proper storage and handling.
  - More regular full backups to mitigate media failure.

    Plan 1: 10 incremental backups followed by full backup

    Plan 2: 5 incremental backups followed by full backup

    ➢ Plan 1 is more risky that Plan 2.

Backup Integrity

1. Verification as part of backup
   - Cause backup time to increase.
   - Selectively verify only critical backup points.
   - Fixing backup errors immediately after backup cost less than realizing it is corrupted at recovery time.
2. Restore backups to alternate server
   - Validates recoverability of the backup.
   - Verifies the physical integrity of backup media.
   - Provides a ready copy of the recovered data, reducing recovery time in the event of a disaster.
   - Establishes a last known good backup.

Backup Encryption

- Secure backups through encryption
  - Minimise data leakage when backups are lost or misplaced.
  - For intentional theft, difficult to retrieve data.

Backup Encryption Issues

1. Performance
   - Tradeoff between backup time and security.
2. Key Management
   - Encryption key is essential to access backup data.
   - Loss of key => loss of data, needs to be protected.
3. Error Tolerance
   - Encrypted data is less tolerable of errors.
   - Bit error in block can render the whole block useless.
   - Requires more stringent media integrity.

Backup Encryption Issues

4. Recovery Requirements
   - Additional software/hardware to decrypt.
   - Need to be available during emergencies.
   - Hardware-based encryption:
     - Hardware need to be present to access/recover data.
     - Compatibility and interface with production system.
   - Software-based encryption:
     - Software needs to be setup to access/recover the data.

Video on H/w Encryption

Summary

- Backup and Recovery
- Backup Media
  - Tapes, Optical Discs, Hard Disks, Online/Cloud
- Backup Storage
  - Onsite, Offsite
- Backup Integrity
  - Verify upon backup, Restore to alternate server
- Backup Encryption
  - Performance, Key management, Error tolerance, Recovery requirements

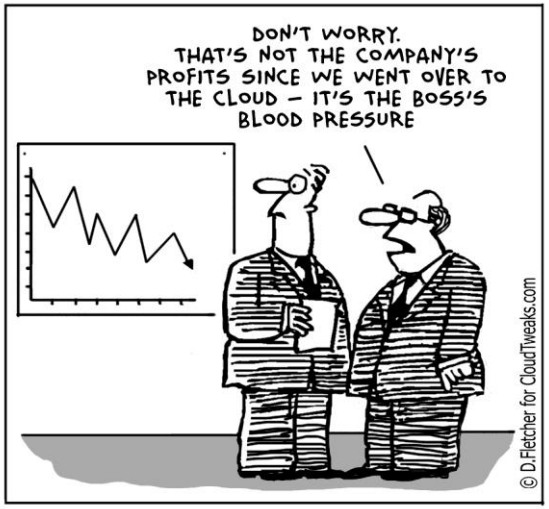
Additional References

Backup Storage

- Media vaulting
  - Remote location to hold physical tapes.
  - Mostly outsourced to third-party vendors.
  - Vendors' media handling procedures must satisfy requirements of its customers.

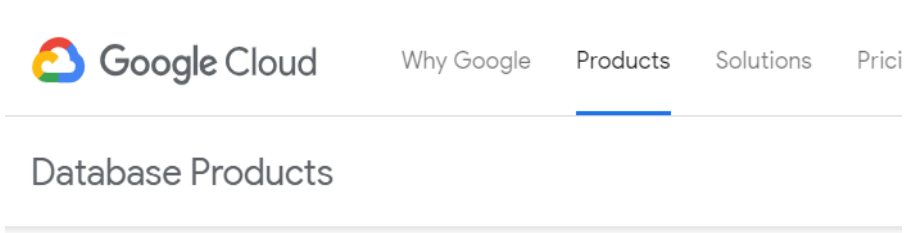
Backup Storage

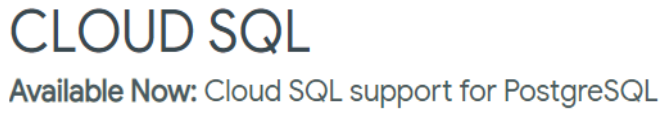
- Online Backup
  - Use of telecommunications infrastructure to send backup data electronically to a remote site.
  - Can be near instantaneous backup but will be costly.
  - Backup and recovery depends on the bandwidth.
  - Able to provide backup intervals of less than a day.

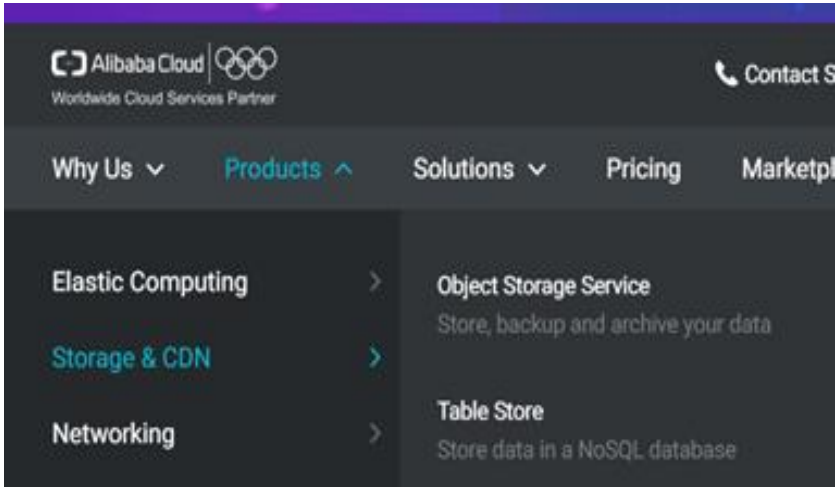


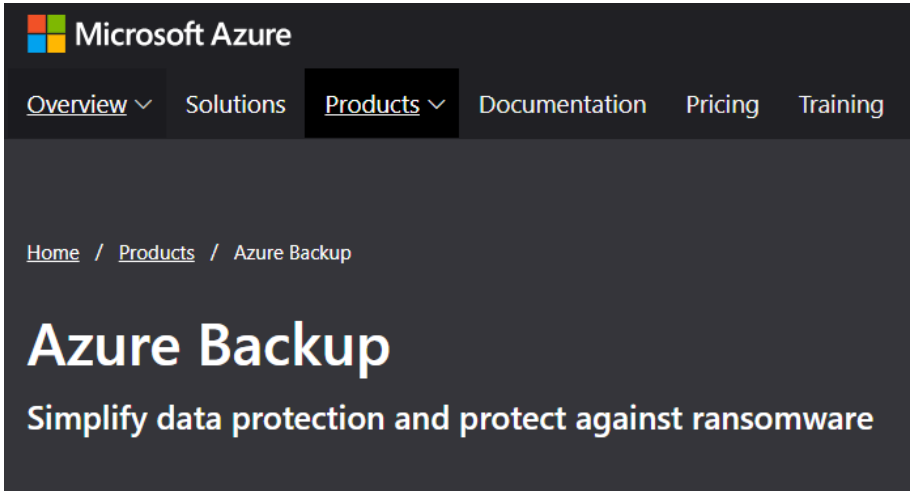
Cloud Backup

IDrive | Acronis True Image | SpiderOak ONE | SOS Online Backup | Backblaze | Livedrive | Carbonite | OpenDrive | Norton Online Backup | MozyHome









Online Backup