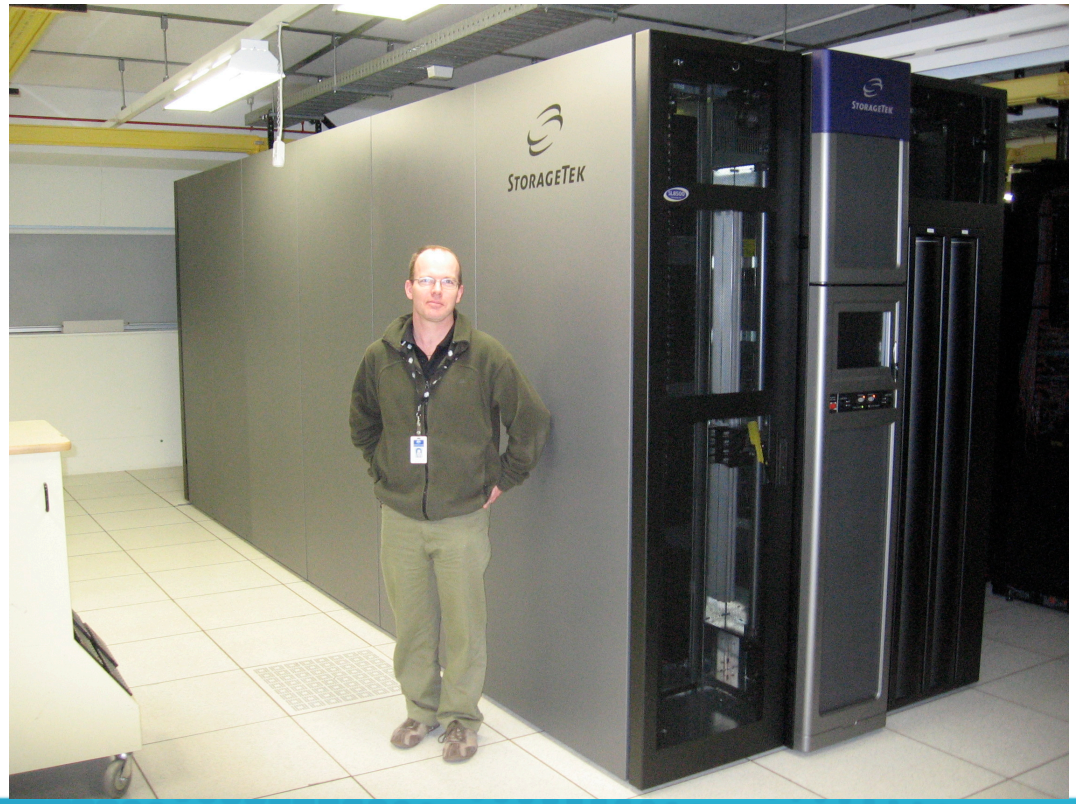

Ways to Lose Data

Robert C Bell

CSIRO Advanced Scientific Computing & RDSI

www.csiro.au

CSIRO

News in May 2011

*** Bad Moon Rises Over Cloud Perceptions ***

It's a glorious day for those with backup and recovery services to pitch, not to mention for those who are nipping at the heels of Amazon Web Service's cloud empire. On the flip side, for those who just got word that their data is unrecoverable via a short letter, not to mention those who have been proclaiming cloud computing as the safe bet for mission critical applications--it's been quite a bleak morning.

Read More: http://www.hpcinthecloud.com/ct/uz5613109Biz11013583

HPC in the Cloud Weekly Update

e-mail from Amazon

Hello,

A few days ago we sent you an email letting you know that we were working on recovering an inconsistent data snapshot of one or more of your Amazon EBS volumes. We are very sorry, but ultimately our efforts to manually recover your volume were unsuccessful. The hardware failed in such a way that we could not forensically restore the data.

What we were able to recover has been made available via a snapshot, although the data is in such a state that it may have little to no utility...

If you have no need for this snapshot, please delete it to avoid incurring storage charges.

We apologize for this volume loss and any impact to your business.

Sincerely,

Amazon Web Services, EBS Support

This message was produced and distributed by Amazon Web Services LLC, 410 Terry Avenue North, Seattle, Washington 98109-5210

HPC in the Cloud Weekly Update

Outline

1. Introduction
2. Threats to data
3. Identifying risk
4. Risk mitigation
5. Other considerations
6. Mirroring, backup and HSM for file protection

1. Introduction

- **Sequel to poster at eResearch 2009: "Your Data, Our Responsibility"**
  - Those of us who manage/operate facilities which include storage have a responsibility
- **Paul Simon wrote the song *50 ways to leave your lover*, containing the lines *"There must be fifty ways / To leave your lover".***
  - I reckon there must be 50 ways to lose your data; we had better ensure that RDSI does not become 50 million dollar ways to lose your data.
- **This talk started as a paper for RDSI, addressing some issues in protecting data.**

1. Introduction

- **Can't guarantee "no loss of data", so must have measures to reduce the risk.**
- **This talk addresses threats that could result in data loss, and mitigation of the threats.**
- **For given expenditure, protection of data is at the expense of capacity (2nd copies).**
- **For the first time in our existence, humans can keep a 'complete' record of their life and work.**
  - Not possible with analogue and physical storage.
  - Growth in capacity of digital storage, and reduction in cost per byte have been extraordinary, and seem likely to continue for some time.

2. Threats to data

- **Examples of threats to the holdings of data which may lead to the loss of data.**
- **External**
  - Terrorism
  - Targeted terrorism (a terrorism attack that targets all copies of some data)
  - War
  - Natural disaster (storm, hail, lightning, flood, cyclone, tornado, earthquake, tsunami, fire, landslide, liquefaction, drought, meteorite, cosmic rays). Though natural disasters, many of these can be exacerbated by human activity.

UQ Flood (courtesy ABC)

2. Threats to data

- **External**
  - Nuclear accident, arson, fire, water damage, electrical fire.
  - Subsidence
  - Financial or organisational failure, insolvency, bankruptcy, breach of contract
  - Ram raid
  - Robbery
  - Political campaign, sabotage, riot, insurrection, civil war
  - Climate change

2. Threats to data

- **Facilities**
  - Building failure
  - Infrastructure failure, e.g. power supply, water supply, telecommunications, plant, floor collapse, fire suppression damage to equipment
- **Hardware**
  - CPU, Memory, Channels, Network, Switches, Controllers, Disc (bit rot), Tapes, Hardware/media obsolescence
- **Software**
  - In OS
  - In filesystem
  - In database
  - In firmware, e.g. RAID, storage arrays, discs, controllers
  - In middleware, e.g. HSM, iRods, transfer programs

2. Threats to data

- **Software**
  - In shells and scripting languages
  - In applications
  - In software rot
  - (Where although the data may be intact, the means to access and manipulate the data may be lost. For example, no current versions of Microsoft PowerPoint can read PowerPoint presentations from a decade ago.)
  - The Victorian Electronic Records Strategy (VERS) developed by CSIRO with the Public Records Office of Victoria was one of the first good examples of a successful implementation of a strategy to avoid this problem. The strategy involves storing information in two formats, both with open definitions: PDF, to preserve the look of a document, and XML to preserve the meaning through metadata.

2. Threats to data

- **Human**
  - Disgruntled employee, particularly systems administrator
  - Revenge
  - Human failure (wrong command, wrong machine, wrong window, wrong directory, wrong instructions; lack of procedures or failure to follow, faulty scripts)
  - Finger trouble (`rm * .o` instead of `rm *.o`)
  - Network intrusion, particularly if root is compromised
  - (In a paper from the 1990s, possibly from IDC, it was reported that 68% of incidences of data loss were due to human error. This is clearly the most common cause, and yet we are beguiled at times into strenuous efforts to protect our data from hardware errors.)

3. Identifying risk

- **Risk assessment is commonly done by considering the chances of a threat, and the impact of a threat.**
  - Events with a low chance and low impact are usually ignored.
  - Events with high chance and high impact must have mitigation.
- **A matrix for risk assessment is usually developed. Below is a simple example.**

3. Identifying risk

Risk Assessment	Low Chance	High Chance
Low Impact	Cosmic rays *(=> low risk)*	Disc failure *(=> medium risk)*
High Impact	Meteorite *(=> medium risk)*	Human error *(=> high risk)*

- **The higher the chance and the higher the impact, the greater is the threat to the data, which then requires more preventative action.**

4. Risk mitigation

- **Risk mitigation is the identification and implementation of controls that will lower the risk.**
- **Here is a sample risk mitigation strategy for each of the above hazards.**

4. Risk mitigation

- **Hazard: Cosmic rays**
  - (low-Chance, low-Impact)
- **Mitigation**
  - Since cosmic rays are likely to destroy only a few bits at a time, the usual parity checking is likely to safeguard against this. Regular checking of all storage media and the keeping of two physical copies mitigates any losses.

4. Risk mitigation

- **Hazard: Meteorite**
  - (low-Chance, high-Impact)
- **Mitigation**
  - ?

4. Risk mitigation

- **Hazard: Disc failure**
  - (high-Chance, low-Impact)
- **Mitigation**
  - Since this is a common event, it must be guarded against. RAID is the usual solution, with RAID 6 now preferred because studies have shown that about 25% of RAID rebuilds on SATA disc encounter a second failure.

4. Risk mitigation

- **Hazard: Human error**
  - (high-Chance, high-Impact)
- **Mitigation**
  - Let us consider close to the worst case, where a human with root privileges types the wrong command at the wrong place at the wrong time, and wipes out the directory to information across an entire repository.
  - How do we mitigate the risks?

4. Risk mitigation

- **Hazard: Human error**
  1. Minimise the use of the highest level of privilege.
  2. Ensure that the controlling software for the repository will not allow the deletion of files and directory information.
  3. Learn from the aviation industry on safety – checklists, crew training, no single person operations.
  4. Hire people with the right personality types for systems administration – no cowboys.

4. Risk mitigation

- **Hazard: Human error**

5. Follow the idea of the (story of the) French legislation that was in place for hundreds of year, that makers of fireworks had to live, with their families, on the premises at which they made fireworks. Make the systems administrators store their own files in the same repository that they manage, using the same tools.
6. Remove write and modify privileges from files as a matter of course.
7. Do mirrors and backups, and use multiple sites.
8. Isolate the multiple copies at different sites, by not allowing cross-site system administrator privileges.

Note that the mitigation strategy for the human error can also go some way to guarding against malicious actions by humans.

5. Other considerations

- **Many other factors to consider to cover all of the hazards listed above. Some are:**
  - Physical protection, Network security, Safe working practices, Dealing with at-risk employees
  - RAID, Mirroring, Dual-site running, Backup, Multiple site storage
  - Checking processes, Verifying the data

6. Mirroring, backup and HSM for file protection

- **Having a mirror and/or backup or HSM of data at the same site, (or even better at a second site) provides a high level of protection against many hazards.**

6. Mirroring, backup and HSM for file protection

- **Mirroring is the taking of a copy of data onto another storage medium.**
- **This is often done almost continually, or at short intervals, and the target of the mirroring is the same place every time.**
- **Thus each mirror operation over-writes the last mirror.**
  - Great for fast restores – can even mount mirror

6. Mirroring, backup and HSM for file protection

- **Backup is the taking of a copy of data onto another storage medium.**
- **This is often done at short to medium intervals, e.g. hours to days.**
- **The target of the backup is a different place every time, so that each backup does not over-write the last backup.**

6. Mirroring, backup and HSM for file protection

- **Although mirroring guards against many risks, it does not completely protect: if I *butcher* a file, and the *butchered* file is mirrored everywhere almost instantaneously, then the mirroring is no protection at all, and gives a false sense of security.**
  - The issue is the time interval between the actual damaging event and the realisation that damage has been done, compared with the time-interval of the mirroring.

6. Mirroring, backup and HSM for file protection

- **Backup strategies recognise this issue, and keep multiple copies of files back in time, with the hope that the coverage will be sufficient so that the last good version of a file is in the backups, and hence able to be restored.**
  - Ideally, one would keep every instance of every file. Hardly any backup strategies do this, but are confined to keeping snapshots of the file system at particular instances in time.

6. Mirroring, backup and HSM for file protection

- **A backup management strategy is needed to decide how many and which backups are kept, as no one can afford the capacity to keep every backup.**
  - So the tendency is to keep all the recent backups, with sparser and sparser spacing as you go back in time. This fits in with the observation that recovery is less and less likely to be needed from backups as you go further back in time.

6. Mirroring, backup and HSM for file protection

- **However, the cost of multiple snapshots can be high**
  - ten snapshots take ten times as much storage
  - there is considerable i/o [and sometimes network traffic] as all files are copied to make every snapshot)
- **Use schemes which use hard-linking such as Apple's Time Machine, *lbackup* and the CSIRO ASC *rsync with hard-linking*.**
  - (See earlier DMF UG talk, but more progress since then).

6. Mirroring, backup and HSM for file protection

- **Log-structured file systems (write and never over-write), can help. But space hungry.**
- **HSMs can be set to never delete data. Provided a file exists in storage long enough to be captured by the HSM, then every copy is captured forever.**
  - CSIRO ASC experience suggests that this is likely to be about a 50% increase in the amount of storage needed and the number of files kept for a fairly active store.

6. Mirroring, backup and HSM for file protection

- **HSMs can obviate part of the backup problem, because they trickle data to secondary media continually.**
- **When a backup is done, only data not already trickled to the secondary media needs to be captured.**
- **This is typically the metadata for all files and files too small to bother the HSM with.**
- **HSMs can also be easily set up to make multiple copies, and for one of more copies to be taken off-site.**

Another Example

The Age. 2011-06-25.

"More than just data lost in cruel hack"

Adam Carey

June 25, 2011

http://www.theage.com.au/technology/security/more-than-just-data-lost-in-cruel-hack-20110624-1gjj4.html

Computer hackers have destroyed a Melbourne IT company. *Photo: Tanya Lake*

Another Example

SOME say it was an act of evil.

On the Queen's Birthday long weekend, a Melbourne IT company's hard drives were hacked and thousands of files and websites erased. Today that company, Distribute.IT, is dead - its business and reputation so trashed that its owners were forced this week to sell it to a competitor. Thousands of small Australian businesses whose websites it hosted are picking up the pieces.

The hacker obliterated 4800 websites in a lightning nighttime strike upon Distribute.IT on June 11, leaving a message on the company's home page: ....

7. The big one – malicious use of root

- **In the first version of the paper, I missed noting the potentially most dangerous risk, and that is an intrusion over the net which results in root compromise.**
  - In other words, an intruder gains access to a system, with every possible privilege.
- **See example above (company out of business), and recent NCI NF experience.**
- **Real possibility.**

7. The big one – malicious use of root

- **Every protection that is put in place using root (e.g. backups) can be undone by someone using root.**
- **An intruder with root access can find all the scheduled tasks (e.g. backup), read the scripts to look for targets for these, and over-write or destroy any protection of data.**
- **Worst case could be a root compromise which piggy-backed on backup processes to another host or site to root compromise the other hosts or sites. All copies of files, though widely distributed, could be wiped out.**

7. The big one – malicious use of root

- **Even tape copies of dumps would not be immune from this attack.**
- **The intruder could work from the crontab files, look at the scripts, uncover the tape records, and (if tape automation is in place) mount every tape, re-label it and write something, thus removing the entire contents (except for forensic recovery).**
- **So, some protection might be to ensure the dump (and DMF) tapes cannot be over-written without human intervention.**

7. The big one – malicious use of root

- Tape protection: write-once tapes, or removing the ‘write-ring’ from tapes.
- Each dump (and DMF) tape could be ejected from the tape library, the write protect invoked (by a human) and the tape re-inserted.
- For HSM, one entire pool of the two or more pools could be written to write-once tapes.
- Further protection: remove second copy tapes from the library so that operator or authorised staff would be needed to have them re-entered
- Storing the second-copy tapes at a site where there are no tape drives would help.

8. Conclusion

- **Do a risk assessment: biggest threats, biggest impact**
- **Communicate with users**
  - Tell them about policies, procedures, protection for file systems/storage (CSIRO ASC registration)
  - Education
- **Do backups (not just mirrors), and test restores!**

- **“It’s not that I’m paranoid: it’s just that they’re all out to get me!” mis-quote.**

CSIRO ASC
Dr Robert Bell

Phone: +61 3 9669 8102
Email: Robert.Bell@csiro.au
Web: http://hpsc.csiro.au/users/dmfug/Presentations_Oct09/DMF_as_a_target_for_backups/

Thank you

Contact Us
Phone: 1300 363 400 **or** +61 3 9545 2176
Email: Enquiries@csiro.au **Web:** www.csiro.au