Avoiding data loss in virtual environments.

WE RECOVER FROM DATA LOSS IN SERVER HARDWARE AND STORAGE. Data loss is still prevalent in virtualised platforms and this type of data loss is often more destructive as multiple virtualised systems are affected by the loss of a single physical server or storage device.

What can you do if you experience data loss?

Virtualisation brings an extra layer of complexity to a host system and when data loss occurs within a virtual machine, it is critical to select a data recovery provider that is experienced in data recovery for virtualised systems.

At Kroll Ontrack, by utilising the industry's largest team of data recovery engineers and an unmatched suite of custom data recovery tools, your virtualised data loss situation can be evaluated and, in many cases, recovered in a matter of hours via our in-lab, on-site or remote data recovery services.

Common causes of data loss in virtualised environments

Through our extensive experience in handling data recovery cases from virtualised environments as well as direct feedback we have received from clients, we have been able to establish a pattern of the common causes of data loss:

- File system corruption
- Deleted virtual machines
- Internal virtual disk corruption
- RAID and other storage/server hardware failures
- Deleted or corrupt files contained within virtualised storage systems

"Over the next twelve months, we will see virtual environments adopted by an increasing number of organisations. It is essential that water-tight disaster recovery plans are in place before we enter this new and exciting technology era".

— Robin England,
Senior Research and Development Engineer

How to avoid data loss in virtual environments

If you start to experience problems with either your virtual environment, hypervisor or RAID storage array, then there are five key steps to remember in order to best preserve your data:

- Restore backups to a different volume
- If there is a RAID problem, test the backup by restoring it to a different location or image each drive from the RAID before attempting a rebuild
- Do not create any new files on the disk needing recovery or continue to run virtual machines until the important data is recovered
- Do not run FSCK or CHKDSK file system repair tools on a virtual disk unless a good backup has been validated by restoring it to a different volume
- Always have a disaster recovery plan in place to ensure that, should a moment of crisis arise, you are able to quickly respond while giving yourself the best chance possible of recovering your data and minimising downtime. That plan should include the contact details of a reliable data recovery provider – a key piece of information which is often overlooked when developing the plan.

Technical considerations to avoid data loss when using Cloud storage solutions

- Interruptions to power supply and electrical spikes can cause data loss, data corruption and data availability issues. Does your cloud provider have a record of technical reliability to cope with your needs?
- What type of storage is used? Is a form of RAID used that has redundancy? What hypervisor is used? What certifications does the provider's employees/data centre have?
- Are backup systems and protocols in place? Do these systems and protocols meet your own in-house backup standards?
- Does your cloud vendor have a data recovery provider identified in its business continuity/disaster recovery plan? In instances of data loss, it is imperative that a rapid response procedure is adhered to.
- What are the service level agreements with regard to data recovery, liability for loss, remediation and business outcomes?
- Can you share data between cloud services? If you terminate a cloud relationship can you get your data back? If so, what format will it be in? How can you be sure all other copies are destroyed?
- What measures does the provider take to secure your data? Is end-of-life data erased? Who certifies that it has been deleted? Do you still own your data once it is cloud-based?

Legal considerations to avoid data loss when using Cloud storage solutions

- Can the cloud provider retain data in accordance with your company's corporate document retention policy?
- Will the cloud provider offer assurances that it will comply with data protection regulations?
- In case of litigation or an investigation, will you or your external e-discovery provider be able to access and either extract or preserve all electronically stored information? If so, how quickly is access provided?
- Where exactly is your data stored? Where is the data centre located geographically?

CONTACT

For more information, call or visit us online:
+44 (0)20 3627 2118 | krollontrack.co.uk
+353 (0)1 960 9265 | ontrackdatarecovery.ie

Kroll Ontrack®