

ΕΒΟΟΚ

Broadcast media

Avoiding the object storage performance pitfalls faced by media and broadcasting organizations ЕВООК

DIREC

BIG PICTURE

Is object storage the right choice?

Broadcast media



Easy scalability

Storage of large volumes of video, audio, image and unstructured files



Lower costs at scale

Object storage has cheaper disks than Storage Area Networks (SANs)



Simplified data retrieval

Metadata identifies properties of the object for easy retrieval



Compatibility

Compatible with DAM/MAM, and video asset management (VAM) applications

Pitfalls

11

1. Failing to optimize object storage	4-6	
2. Bolting object storage onto existing high availability architecture	7-9	
3. Assuming object storage data is always secure in public cloud	10-12	
		And the second
		No. C.

7 Failing to optimize object storage

Need to deliver the efficiencies promised

New media formats such as 4K, 360 degree, and 60 frame video introduce greater storage challenges which can be solved by object storage. In fact, object storage active archive solutions can be <u>100X faster, and 70% cheaper</u> than public cloud storage. However, these efficiencies can only be realized through optimization, ensuring maximum throughput for these high-performing applications.

Good or Great?

Reality

Object storage on its own is not a complete solution. It requires a high availability solution called load balancing to provide an uninterrupted end user experience, and consistent data access.

Data accessibility

Even though object storage nodes replicate across data centers, load balancers can identify the best data center to use for the end user, based on their location.

REMEDIES



Don't rely on round-robin Domain Name System

Object storage platforms use simple roundrobin DNS to direct user requests, but this form of load distribution doesn't guarantee high availability as there are no health checks, meaning requests can continue to be sent to failed or overloaded servers.





Immediate failover to an alternative server is needed in the event of a system failure, or for essential maintenance. So if a server fails or is taken offline, for whatever reason, user traffic is rerouted without any disruption to the end user.



Prevent bottlenecks to maximize performance

Ensure traffic can be intelligently shared across all available nodes and servers to prevent bottlenecks and performance degradation. Load balancers for example, have access to more information about the available infrastructure and can therefore make the best use of the available resources.

PITFALL

Bolting object storage onto existing high availability architecture

Need to avoid potential performance issues

With pre-existing high availability solutions already in place it can be tempting to bolt object storage onto existing architecture. However, this can result in resources being pulled by other applications, and resources that were intended to support the object storage application being drained. The end result is performance issues.



Noisy neighbor

լել

Available resources can be claimed by any or all of the other applications attached to a shared load balancer.

Unsatisfactory performance

Is likely to have nothing to do with the object storage provider.

Reality

A per app high availability approach is the only way of guaranteeing the performance of the object storage application, and easy scalability.

Heavy usage

Media companies will likely make high demands of their object storage applications, which they cannot afford to be compromised.

A dedicated HA solution

Storage vendors themselves advocate use of a <u>dedicated pair</u> of load balancers.

REMEDIES



Resilience

Protect object storage from server failure and congestion, leading to interrupted service and downtime. This ensures the application remains always-on and able to perform as intended.



Responsiveness

Make sure your object storage application remains available to the end user - regardless of load. With natural peaks and troughs traffic needs to be proactively managed to make the best use of available resources.



Scalability

Put dedicated infrastructure in place to future proof data demands and ensure unlimited scalability. With exponential growth in large data sets expected, a degree of redundancy needs to be inbuilt to ensure adequate ROI.

PITFALL

Object storage data is always secure in public cloud

Data security cannot be delegated

More and more organizations are opting for cloud native object storage. Roughly the same amount of data is now stored in the cloud as it is in the private cloud or on-premise — close to <u>80 PB per year</u>. But, while data is indeed encrypted and backed up in the public cloud, it does not necessarily follow that it is therefore 'safe' in the public cloud.

Security's on me

Icast media

Access control

Even in the public cloud, it remains the responsibility of media organizations to limit privileges and access as much as possible.

Encryption

Encryption keys remain the responsibility of the media organization.

Reality

Data loss and corruption can occur with all forms of data, and media organizations remain accountable for data security, regardless of where they choose to store it.

Data configuration

This cannot be outsourced to public cloud providers and must be done correctly to avoid introducing security vulnerabilities.

Lack of configurability

Due to the lack of control over shared resources designed for the many not the few, it can be hard to satisfy security standards for protected data in the public cloud.

REMEDIES



Data security

Conduct regular security checks and ensure the integrity of your data when it's moved or copied to different locations. Every cloud provider has different security and encryption protocols so it may be that while one vendor satisfies your compliance criteria, another does not.



Zero trust

Assign least privileged access to specific buckets and rotate encryption keys. Public cloud providers themselves are at pains to emphasize that they are only responsible for platform security measures, not data security.



Backups

Public cloud platforms do not replace the need for regular backups to ensure the protection and security of all stored data. Were someone with malicious intent to gain access to your cloud data, this would lead to irretrievable data loss. At the end of the day, data is still stored on servers in the cloud they just belong to someone else.

Summary

- A high availability solution is required for object storage applications to perform as intended.
- Object storage requires a dedicated high availability pair to avoid a noisy neighbor situation.
- The public cloud may not be a suitable place to store protected data.







Don't compromise the security of your applications. Have a hybrid environment you need to manage? We can make sure it stays resilient, and always-on.⁹⁹

Malcolm Turnbull, Co-Founder, Loadbalancer.org

About the company

Our mission is to ensure your business is never interrupted by downtime — using tailored, high availability solutions to optimize application delivery.

Bringing decades of experience to your deployment, we're here to get to the heart of what matters to you, delivering uptime you measure in years, not months.

Find out if our clever, not complex, Application Delivery Controllers (ADCs) and exceptional, personalized support are the right fit for your application stack.

www.loadbalancer.org



SMART • FLEXIBLE • UNBREAKABLE

