File server Disaster Recovery with Tiger Bridge

Microsoft Azure

In the event of system failure or malware attacks, organizations must be prepared to quickly recover and resume operations with the shortest downtime. Critical business data, including VM backups, must be immediately accessible, in its native format, from multiple high-availability points and restored with respect for ACLs.

Disaster Recovery Goals

Maintain operations
Reduce RPO and RTO
Prevent ransomware outages

Disaster Recovery Requirements

High availability (nines)
Active Directory ACL restoration
Partial restore
VM backup support

Typical DR approaches

Common DR approaches often include a third-party backup application that locks data to a specific vendor, in many cases requiring its own server and storage. These applications perform multiple full backups whether data has been changed or not, increasing write time and storage costs.

To ensure redundancy, data is also written to on-premises disk and tape. For safety, these tapes are often stored off-site. This duplication of data increases capital expense for storage hardware, takes time, and incurs human and other resource expenses.

In case of failure, data must first be restored from the backup with the proprietary software it was created with. This two-step process further delays access to the data. Packaging data inside another container makes restoration more vulnerable to corruption, locks data to the vendor, and usually requires full restores before data is available.

Pain points

- Buy and use non-native 3rd party software
- Vendor lock
- Data duplication in multiple full backups
- Full restore required before accessing data
- Long RPO and RTO
- Hardware expense
- Ransomware vulnerability

The Tiger Bridge approach

An ideal DR solution guards against ransomware attacks, supports VM backups, provides maximum availability, data redundancy, and allows mission-critical processes to resume immediately. Recovery Point Objective (RPO) and Recovery Time Objective (RTO) should be counted in minutes.

Tiger Bridge is a kernel-level software-only file system filter native to Windows that is compatible with DFS, VSS, and typical anti-virus services and provides intelligent ransomware monitoring. To defend against local failure, data is replicated to multiple high-availability Azure buckets as well as hot/cool/archive tiers for redundancy and cost flexibility. All data and files are stored in native formats with no 3rd-party backup application required to write or read data. Tiger Bridge is fully compatible with Veeam Backup & Replication when using backup and instant recovery and supports local tape and disk targets.

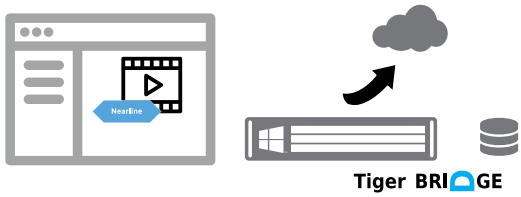
New data is replicated as it is created, so RPO is as short as the transfer time of the last modified file. This continuous replication removes the need for regular full backups, reducing transmission times and storage costs. RTO is short and recovery from any server failure is easy with Tiger Bridge. In case of partial data loss users simply access cloud data on demand and resume operations. In case of a complete site failure, cloud data can be restored to a virgin recovery server and users can immediately begin working with critical files. Data can be fully or partially restored to any number of new or repaired servers. In all cases, data is replicated and synchronized across sources and targets.

© 2020 Tiger Technology | www.tiger-technology.com | Subject to change without notice |

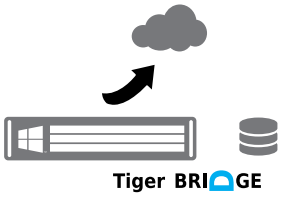
Shorten RTO and RPO
Defend against ransomware

Infinitely scale
Reduce capital expense

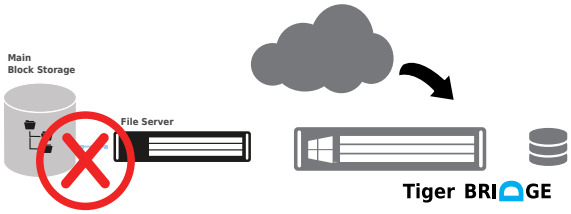
Backup VMs
Avoid vendor lock



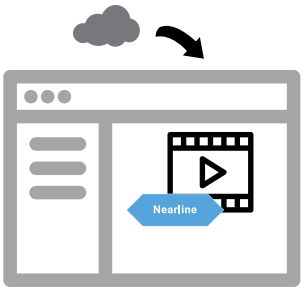
1. **Tiger Bridge replicates** the file system and data to Azure.



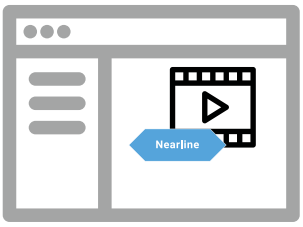
2. **New data** is replicated as it is created. RPO is reduced to the time it takes for files to be written to Azure.



3. **After a failure**, Tiger Bridge writes the file system, including ACLs, to the new server.



4. **Required files** are retrieved on-demand by users and applications. RTO is reduced to the time it takes to retrieve the files from Azure.



5. **Non-critical files** are automatically restored in the background.

Summary

Tiger Bridge is an ideal solution for Disaster Recovery. Tiger Bridge is transparent to users and applications, avoids vendor lock by preserving data in its native format, supports VM backups and supports Windows services such as DFS, VSS, and anti-virus, and defends against ransomware. It shortens RPO and RTO and allows mission critical operations to resume immediately after a failure.

Tiger Bridge is the only non-proprietary, software-defined data and storage management system to blend on-premises and multi-tier, multi-cloud storage into a single space. This human-friendly, transparent, and seamless file and application server extension enables millions of Windows server users to benefit from cloud scale and services, while securely preserving legacy applications and workflows. Native, kernel-level, and highly-tuned low-latency bi-directional integration into the file system enables unique, AI meta workflows and brings cloud scale, power, and services directly to users' current operations without disruption.

© 2020 Tiger Technology | www.tiger-technology.com | Subject to change without notice |