



Cloud storage - Due diligence

Data held in our hosted cloud storage is secured and backed up every 15 minutes across geographically separate locations underpinned by Microsoft's Azure platform.

Access your data across the Internet using a locally installed copy of the Volume™ software or via the web client and business portals.

Limitation

Due diligence is limited wholly to the database and its prescribed data held within, known as the Meta data, and the document's data repository.

Operating Requirements

In addition to the standard Volume application for data access to operate successfully adequate internet bandwidth is required along with an encryption key supplied by WLT's support team.

All other operations and functionality remain the same as the locally installed application. There are no requirements for Terminal Services, Citrix or VPNs.

Backups

Backup Frequencies

- Remote MS SQL Server databases operate with the following standard schedule, unless special requirements occur;
 1. Full backups—weekly
 2. Differential backups—nightly
 3. Transactional backups—every 15 minutes
- Documents are replicated within 10 minutes, after being added, to multiple geographical locations allowing multiple redundancies.
- All databases and documents are copied to multiple geographical independent locations at all levels of backup.

Scope

Data storage is limited to Volume and its users.

Security & Encryption

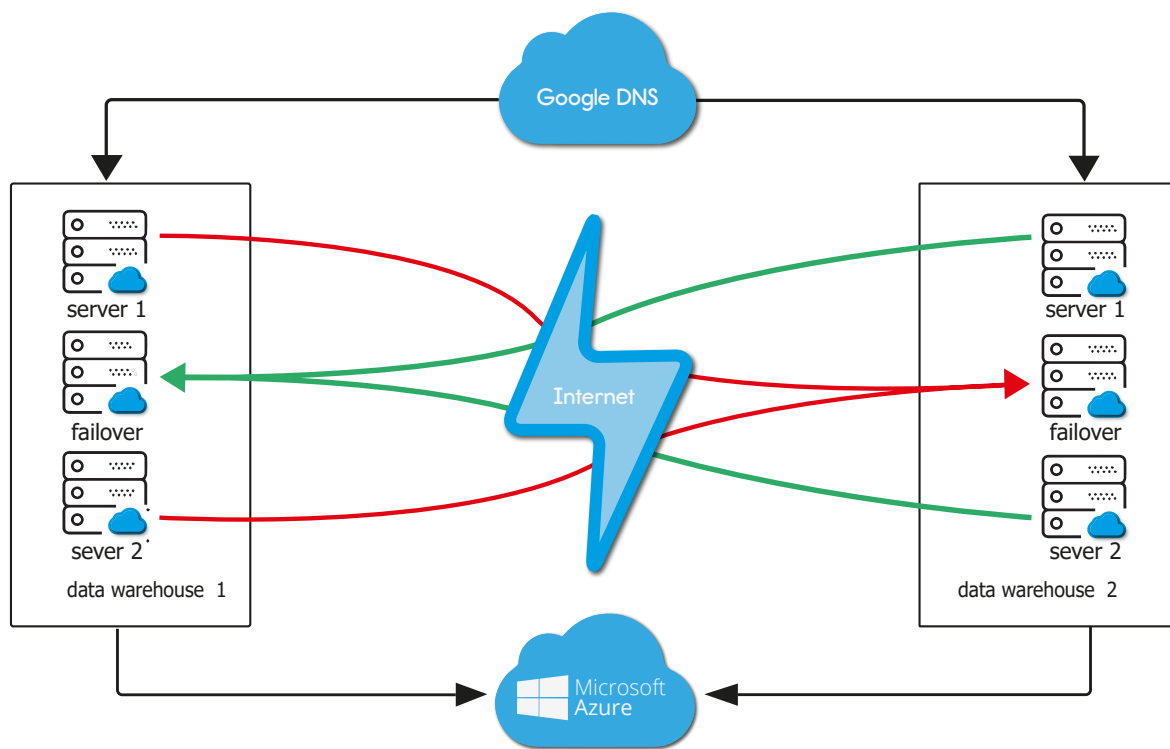
Prevention of unauthorised access.

- Logon is made via a User name and strong password combination specific to each user.
 - Site specific encryption keys are required on each client (that can be instantly switched to disable access if for example a laptop is stolen).
 - SSL.
 - TLS1.2 encryptions.
 - Data is stored in a proprietary format.
 - Time based authentication on every packet.
-

Disaster Recovery

There are a number of plans in place for specific disasters, including keeping spare server capacity to allow loads to be moved, standby virtual servers at other locations and backups in multiple locations.

The Volume™ servers are able to automatically restore paperwork from backup as required, removing the need to perform a complete restoration to new servers.



Fail-over

Each database is replicated to a separate physical location. Fail-over is established to the remote site in the event of a server failure. Google DNS is employed to allow instant DNS switching. Transactional backups are taken at 15 minutes intervals.

Physical Server Locations & Service Providers

Fasthosts

Gloucester

Watermark Technoloies

ShIPLEY

UK Servers

Coventry

Microsoft's Azure

Dublin

Amsterdam

Support

WTL operate during normal office hours 9am-5pm Monday-Friday excluding public holidays UK local time.

Microsoft Azure

Utilising Geo-Redundant Storage (GRS) maintains six copies of the data. With GRS, the data is replicated three times within the primary region, and is also replicated three times in a secondary region hundreds of miles away from the primary region, providing the highest level of durability.

In the event of a failure at the primary region, Azure Storage will failover to the secondary region. GRS ensures that the data is durable in two separate regions. All data is held within the European Union to abide by FCA regulations on document storage.



ISO 9001
Certificate No. GB2004726



ISO / IEC 27001
Certificate No. ISM7799246