

Disaster Recovery : Real Time DR

Real-time Disaster Recovery is more akin to a Business Continuity solution and when integrated with a Backup solution, the business is completely covered and protected for virtually all disaster and recovery requirements.

The key concept around the technical delivery of Real-time DR is stretching the live production environment to the remote data centre using native features of the hypervisor platform itself. For VMware this would be HA, Stretched Cluster type capability.

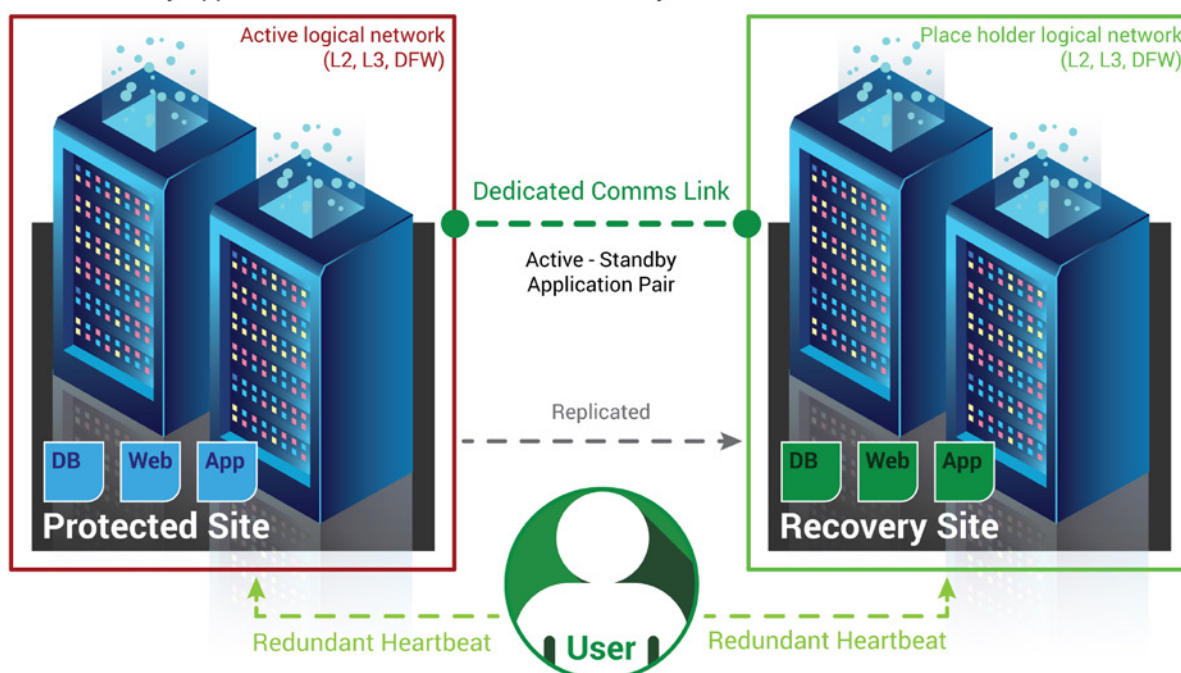
- Pros
 - Natively integrated with production hypervisor and network solutions
 - No management of replication middleware required
 - Real-time Recovery Point Objective (RPO)
 - Near real-time Recovery Time Objective (RTO)
 - Shortest recovery time – seconds to minutes
- Cons
 - Higher Cost
 - Need for storage solution/hardware capable of multi-site deployments
 - Little protection against ransomware / cryptolocker attacks + backup

Solutions components would include;

- Expanded / extended live hypervisor environment
- Backup including backup management
- Dedicated active server host/s to match on-site hardware
- Live SAN (~30TB)
- Cloud storage for backups (~30TB)
- Dark fibre / point to point link

Disaster Recovery with SRM + NSX

Active-Standby Application Pair, No Cross Site Connectivity, Traffic Directed to Active Site



Disaster Recovery : Replication

Traditional replication requires the implementation and ongoing and continued management and maintenance of third party middleware solutions such as Zerto or Veeam.

The underlying hardware requirements are very similar as that required by Real-time DR however with significant added cost for the middleware and human element in the ongoing management and maintenance of the solution.

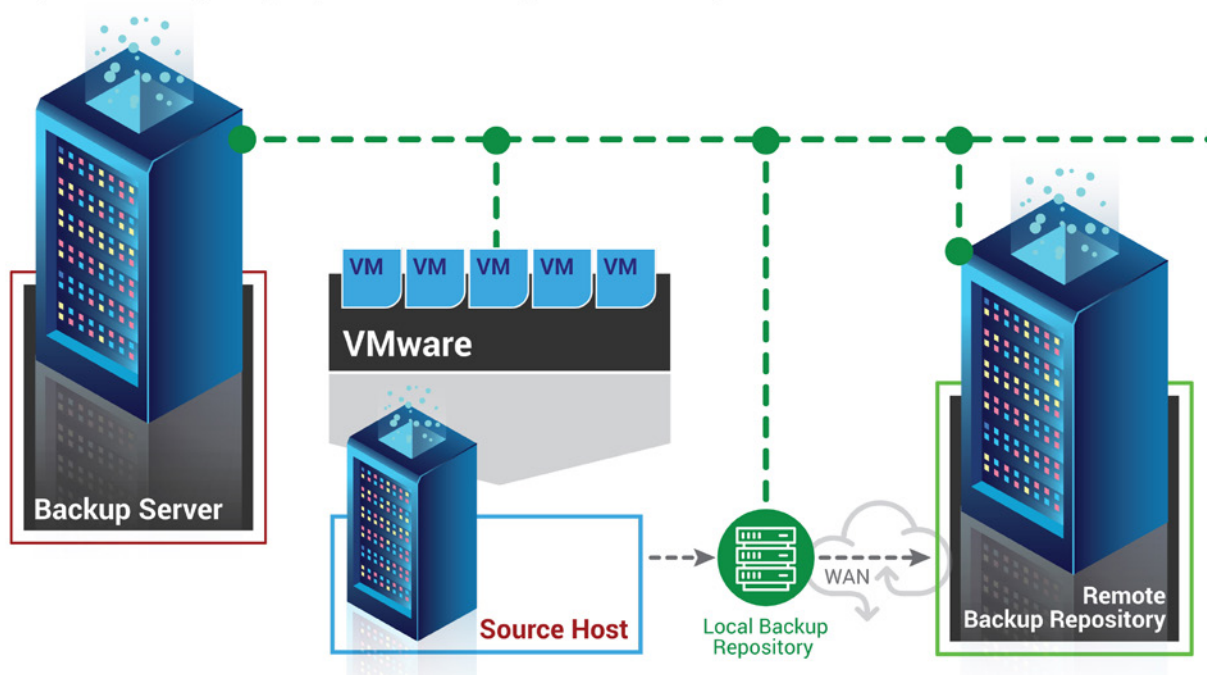
- Pros
 - Low or real-time Recovery Point Objective (RPO)
 - Recovery Time Objective (RTO) – minutes to hours
- Cons
 - Management and operation of replication middleware – often problematic
 - Higher cost
 - Little protection against ransomware / cryptolocker attacks + backup

Solutions components would include;

- Replication software including replication management
- Backup including backup management
- Dedicated active server host/s
- Live SAN (~30TB)
- Cloud storage for backups (~30TB)
- Dark fibre / point to point link

Replication / Backup for Disaster Recovery

Replication using third party software or next generation backups



Disaster Recovery : Hybrid DR

A Hybrid DR solution can incorporate parts of each recovery type, enabling the customer to gain an outcome which is optimised for price, RTO and RPO.

For a Hybrid DR solution, the Real-time components would be deployed using native in-built technologies (such as AD, Exchange DAG, SQL Replication) to ensure the business/mission critical items operate active/active between on-site and off-site with less critical components protected via low cost backup, however with the newer backup technologies (such as Veeam), recoveries can be undertaken within hours, as required.

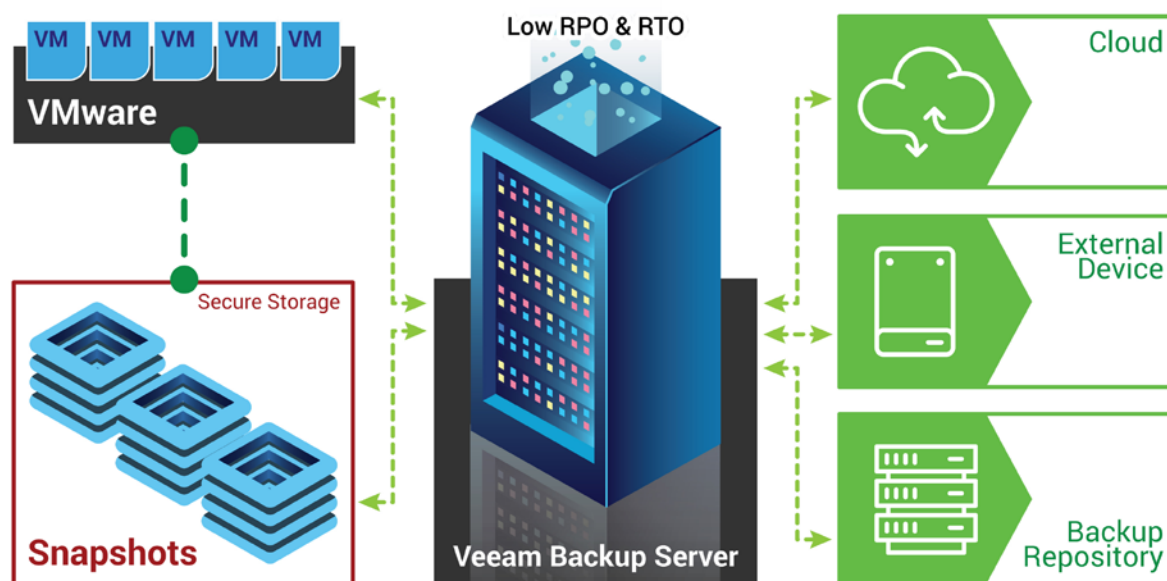
- Pros
 - Lower cost than replication
 - Combination of management requirements
 - Some protection against ransomware / cryptolocker attacks + backups
- Cons
 - Increased complexity of solution and design
 - Longest recovery time

Solutions components would include;

- Backup including backup management
- Dedicated active server host/s
- Smaller amount of live SAN (~3TB)
- Higher amount of cloud storage (~30TB)
- Dark fibre / point to point link

Hybrid Disaster Recovery

Combination of VMware, Veeam, Cloud, Tape or External Device Backup



Disaster Recovery : Backup

Providing the lowest cost solution for disaster recovery plans, backup systems are not what they used to be with modern backup technologies (such as Veeam) providing capabilities that only a true modern backup platform can deliver allowing DC Two to perform data and virtual machine restores quickly and efficiently.

With DC Two's cloud storage directly connected into our hosting platforms, we are able to bring online around 6 to 10 VMs per hour (in emergency situations) using tools such as Veeam's Instant Recovery. Whilst the servers themselves will be online, their performance will be limited while disks and datasets are live migrated to higher performance production storage.

- Pros
 - Lowest cost
 - Simple management
 - Best protection against ransomware / cryptolocker attacks
- Cons
 - Longest recovery time

Solutions components would include;

- Backup including backup management
- Cloud storage (~30TB)
- Internet connectivity

Replication / Backup for Disaster Recovery

Replication using third party software or next generation backups

