Overview of offline backup best practice

V1.0

LOCAL DIGITAL Cyber

Objective

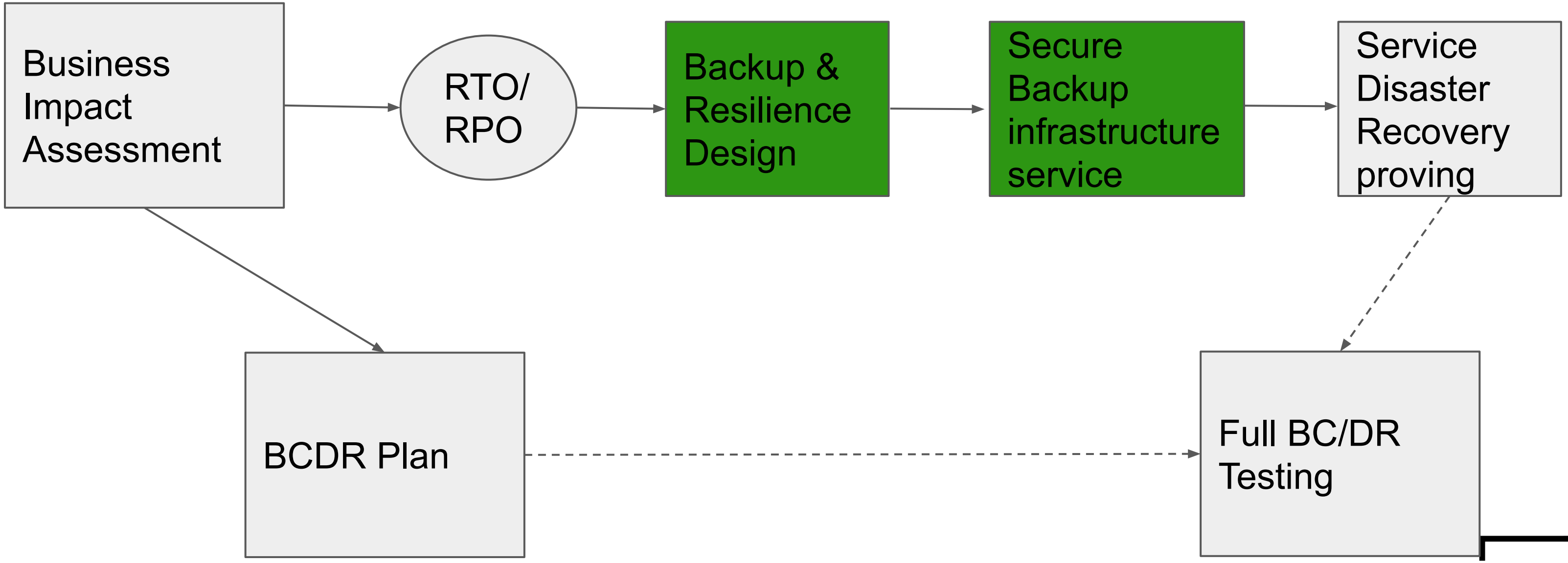
Outline guidance and approach for the best practice implementation of offline backup and immutable backup options for all Local Authority Virtualised Council Information Systems.

As a general observation, you would either implement offline or immutable backups, as there is no need for both in the same organisation.

Both of these technologies are covered in this presentation pack.

CTP connections

Mission critical service resilience and recovery.


Business Impact Assessment
RTO/ RPO
Backup & Resilience Design
Secure Backup infrastructure service
Service Disaster Recovery proving
BCDR Plan
Full BC/DR Testing

LOCAL DIGITAL Cyber

Why do I need offline backups?

- It is generally considered best practice within the field of backups to keep at least one copy of data in an 'offline' storage location. This is becoming increasingly important now that Cryptolocker Attacks are commonplace.
- The NCSC has seen numerous incidents where ransomware has not only encrypted the original data on-disk, but also the connected USB and network storage drives holding data backups. Incidents involving ransomware have also compromised connected cloud storage locations containing backups.
- The impact that this will have will mean your backups are effectively of no real use so a system recovery will be a lengthy process and expensive in terms of resource and lack of ability to function as a Local Authority.

Why do I need offline backups? (cont.)

- The purpose of an 'offline backup' (sometimes called a 'cold backup') is to remain unaffected should any incident impact your live environment. You can do this by:
  - Only connecting the backup to live systems when absolutely necessary
  - Never having all backups connected at the same time (by ensuring at least one of your media locations is on removable devices or in an immutable location on your systems).

Why do I need offline backups? (cont.)

- The **3-2-1** rule is one to follow:

  3 Backups, 2 Locations, 1 Offline Copy

  Example - local backup at primary location, replica or 2nd backup location at DR Location and one offline backup

- With at least one backup offline at any given time, an incident cannot affect all of your backups simultaneously.

Why do I need offline backups? (cont.)

- It must be realised that restoration from an offline backup will take longer than normal but in that it will be happening because of a ransomware or crypto attack this additional time should be an accepted part of your disaster recovery procedure.
- Having a set of backups on Offline Media Storage will effectively act as an immutable copy of backup data (especially if you make the Tape Read Only (RO)). This will give you the ability to restore with confidence from a recent point in time backup.
- Having Backups completely offline will mean that an attack on your systems will not be able to corrupt the backups on this media.

https://www.ncsc.gov.uk/blog-post/offline-backups-in-an-online-world

Offline backup options

There are three main offline backup technologies open to us.

- The primary type is **Tape**. Capacities per tape currently can go up to 30TB with typical compression rates. Autoloaders with multiple drives can vastly increase capacity and reduce time to backup. Tapes should be regularly removed and securely stored, ideally in a different location.
- **Virtual Tape Libraries (VTL)** are increasing in popularity but rely on reliable disk storage behind them, but these cannot be removed from site.
- **Removable Disks**. If your storage requirements for backups is at the lower end of the scale you may be able to use removable storage based on Hard Drives.
- The technology to select will be dependent on the current infrastructure and also the availability of personnel to change the removable media where required. There is no “one size fits all” solution.

Tape

With Physical tape there are multiple things to consider before deciding on a specific route to take.

Design considerations:

- Size of data to be written to tape on each job.
    - If you are breaking down tape jobs per logical group of servers you may be able to use a single tape drive. With typical compression capacities per tape can go up to 30TB (Native maximum capacities of tapes are illustrated on a following slide).
    - Autoloaders with multiple drives can vastly increase capacity and reduce time to backup.

Tape (cont.)

With Physical tape there are multiple things to consider before deciding on a specific route to take.

- Location of the Tape System
    - The ideal location would be at the DR location linked to a physical backup server which is not domain joined

Tape (cont.)

- Tapes should be regularly removed and securely stored, ideally in a different location. Tapes should also be made Read Only (RO) before storage so they are not accidentally used.
- Regular tests of file and server restoration needs to happen to prove the backups are in a usable state.
- For critical server restoration, consider the recovery speed of the LTO technology that you are selecting. For example, LTO-8 can recovery faster than a LTO-7.

Tape (cont.)

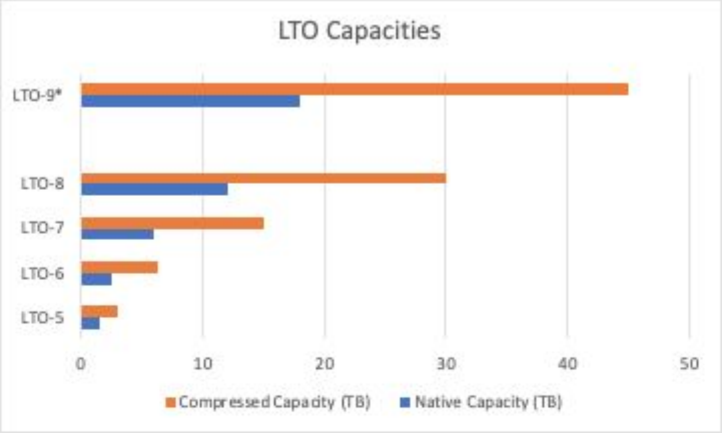
- Leading vendors for tape systems:
  - Quantum https://www.quantum.com/en/products/tape-storage/lto-tape-drives/
  - HPE https://www.hpe.com/uk/en/storage/storeever-tape-storage.html
  - Dell https://www.dell.com/mk/business/p/tape-backup-products
  - Lenovo https://www.lenovo.com/gb/en/data-center/enterprise-storage/-tape-storage/c/storage-tape

** Other Tape System Vendors are available.*

Tape capacities

Currently LTO-8 is the largest capacity tape. LTO-9* currently is due to release in 2021.
These are single tape capacities.

Technology	Native Capacity (TB)	Compressed Capacity (TB)
LTO-5	1.5	3
LTO-6	2.5	6.25
LTO-7	6	15
LTO-8	12	30
LTO-9*	18	45

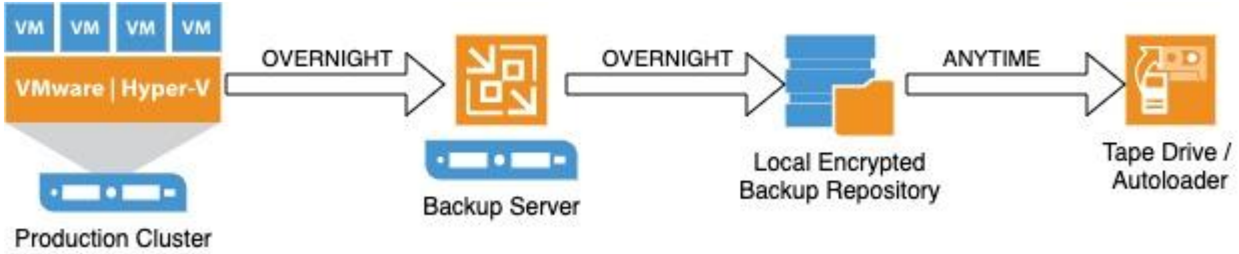


*For further information on LTO-9 refer to : https://www.quantum.com/en/products/tape-storage/lto-9/

Tape backup techniques

Utilising Autoloaders will allow for a larger amount of data to be stored per backup job. The job time can be almost halved with dual drives.

Backup to tape in a virtualised environment is usually made from the primary disk backup which is taken from the live system overnight, and the writing of the backup to tape(s) will happen during the day, and not impact on the live production environment. This technique is referred to as Disk to Disk to Tape.



LOCAL DIGITAL Cyber

Virtual Tape Library

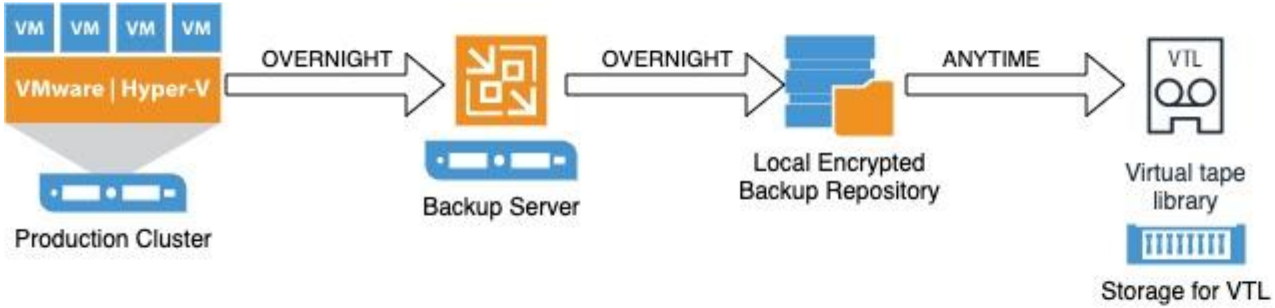
With Virtual Tape Libraries (VTL) consideration should be given to the following points before deciding on whether this technology is a good fit for your organisation

- Design Considerations:
  - Compatibility of a VTL option for your SAN Storage with your backup software. Not all SAN's are suitable for VTL technologies.
  - Available local storage space on which to 'back the VTL onto' as VTL's use disk space to emulate tape cartridges.
  - Is the VTL Storage connected to, or part of, your main SAN ? This is not ideal as if you lose your SAN you also lose your backups.
  - Ability to ship the VTL Destination files offsite in a usable format, especially if a second location for your backup data is part of your DR plan.

Virtual tape backup techniques

VTL's essentially act as autoloaders, therefore as with tape drives they will allow for a larger amount of data to be stored per backup job.

Backup to VTL is very similar to regular tape in that it is usually made from the primary disk backup which is taken from the live system overnight, and the writing of the backup to VTL will happen during the day, and not impact on the live production environment. Despite the destination being virtual, this technique can also be referred to as Disk to Disk to (Virtual) Tape.



LOCAL DIGITAL Cyber

Removable disk

When considering utilising removable disks, there are specific items to review before deciding on whether this technology is a good fit for your organisation.

Design donsiderations:

- Size of data to be written to disk

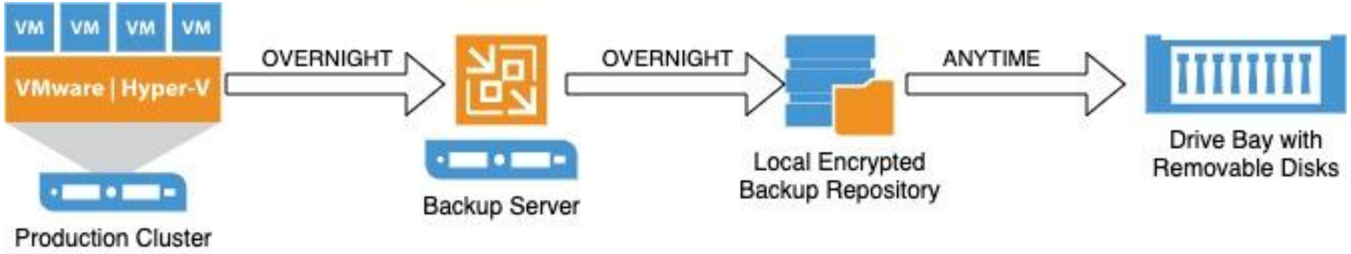
- If you are backing up and retaining large amounts of data then you need the storage which provides the removable drive option to be able to handle large volumes of data. You may have to break your jobs down to manageable chunks and send to multiple drives for removal.

– How will you store the disks while they are offline ?

– How will you handle encrypting the drives so they are readable in the event of a disaster ?

Removable disc backup techniques

Backup to Removable Disks is very similar to Regular Tape in that it is usually made from the primary disk backup which is taken from the live system overnight, and the writing of the backup to Removable Disks will happen during the day, and not impact on the live production environment. Despite the destination being virtual, this technique can also be referred to as Disk to Disk to Disk.



LOCAL DIGITAL Cyber

Immutable storage

An **immutable** backup or **storage** means that your data is fixed, unchangeable and can never be deleted easily. This is particularly important when it comes to malware or ransomware. Also, if you need to retain records for a period of time and don't want them accidentally deleted or changed (such as financial records), immutable storage ensures that.

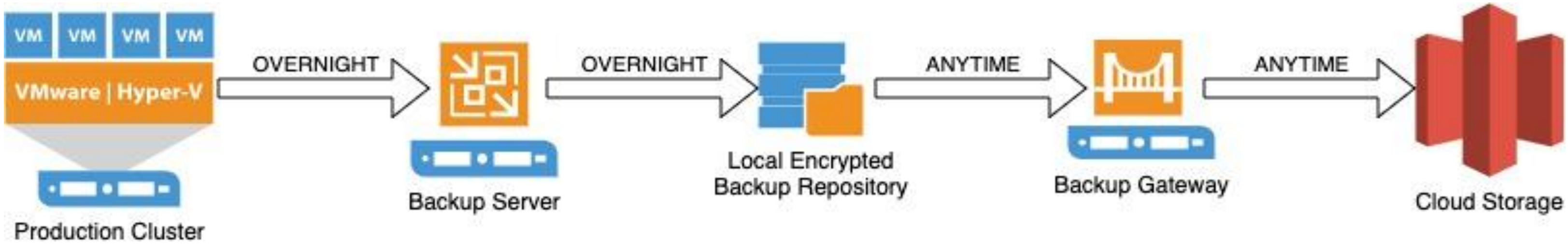
- Immutable Storage technologies can be connected live which makes them an attractive option since they are online to recover from.

Immutable storage options

- Primary Immutable options include:
  - **Cloud Based** Immutable Storage
    This technology is increasing in popularity but costs will be variable as you will pay for storage of the backups, along with transfers in/out.
  - **SAN Based** Immutable Storage
    This is a technology whose features are dependant on the Vendor of your SANs. For instance NetApp have the ‘Snap Suite’ - where you can backup entire LUNs between NetApp Devices with SnapMirror, then ‘Vault’ off recovery points on the target SAN and make them immutable.

Cloud based storage example

- Cloud Based Targets
  - Such as Amazon Web Services S3 / Glacier / Deep Glacier
  - By introducing this tech via an on-premise gateway you can send also immutable copies of data into offsite storage with long term retention periods. This does have data transit costs, along with storage costs at each layer.
  - Veeam and other backup software providers have ‘Gateway’ products to interface with AWS / MS-Azure for backup storage technologies.



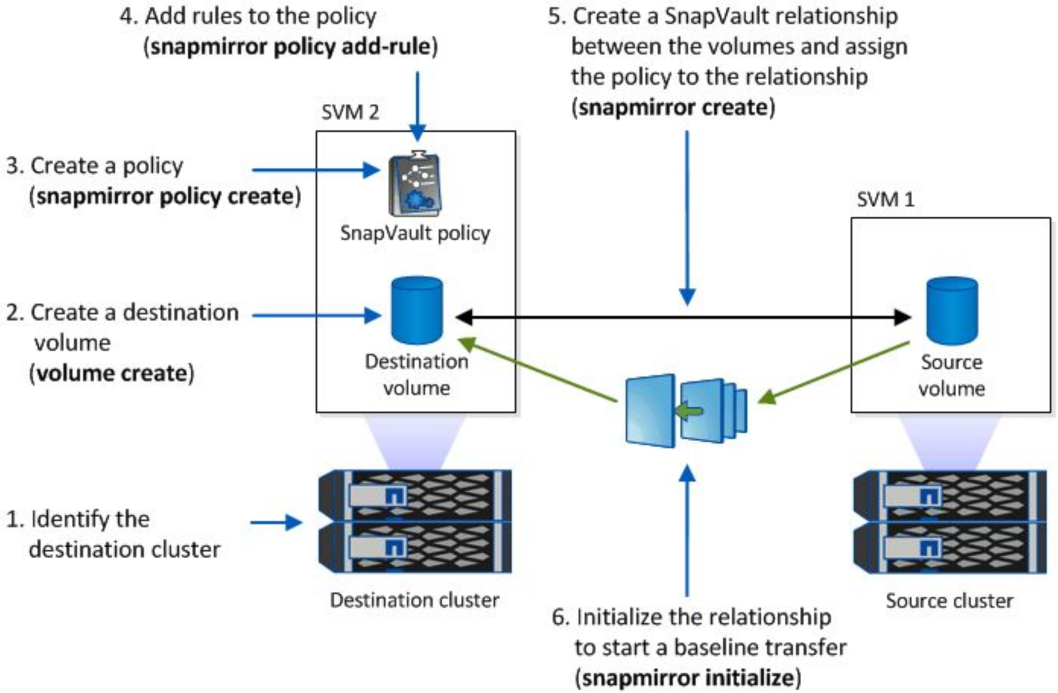
SAN based storage example

- SAN Based Replication (Example is NetApp SnapVault)

This technology allows for SAN based replication to have immutable copies at the DR site (Vaulted).

It’s not offline as such but it is unchangeable (but will be removed as part of an ‘ageing out’ of the ‘Snaps’).

Additional licensing over standard NetApp ones will be required.


4. Add rules to the policy (**snapmirror policy add-rule**)
5. Create a SnapVault relationship between the volumes and assign the policy to the relationship (**snapmirror create**)
SVM 2
3. Create a policy (**snapmirror policy create**)
SnapVault policy
SVM 1
2. Create a destination volume (**volume create**)
Destination volume
Source volume
1. Identify the destination cluster
Destination cluster
Source cluster
6. Initialize the relationship to start a baseline transfer (**snapmirror initialize**)

LOCAL DIGITAL Cyber

Implementation

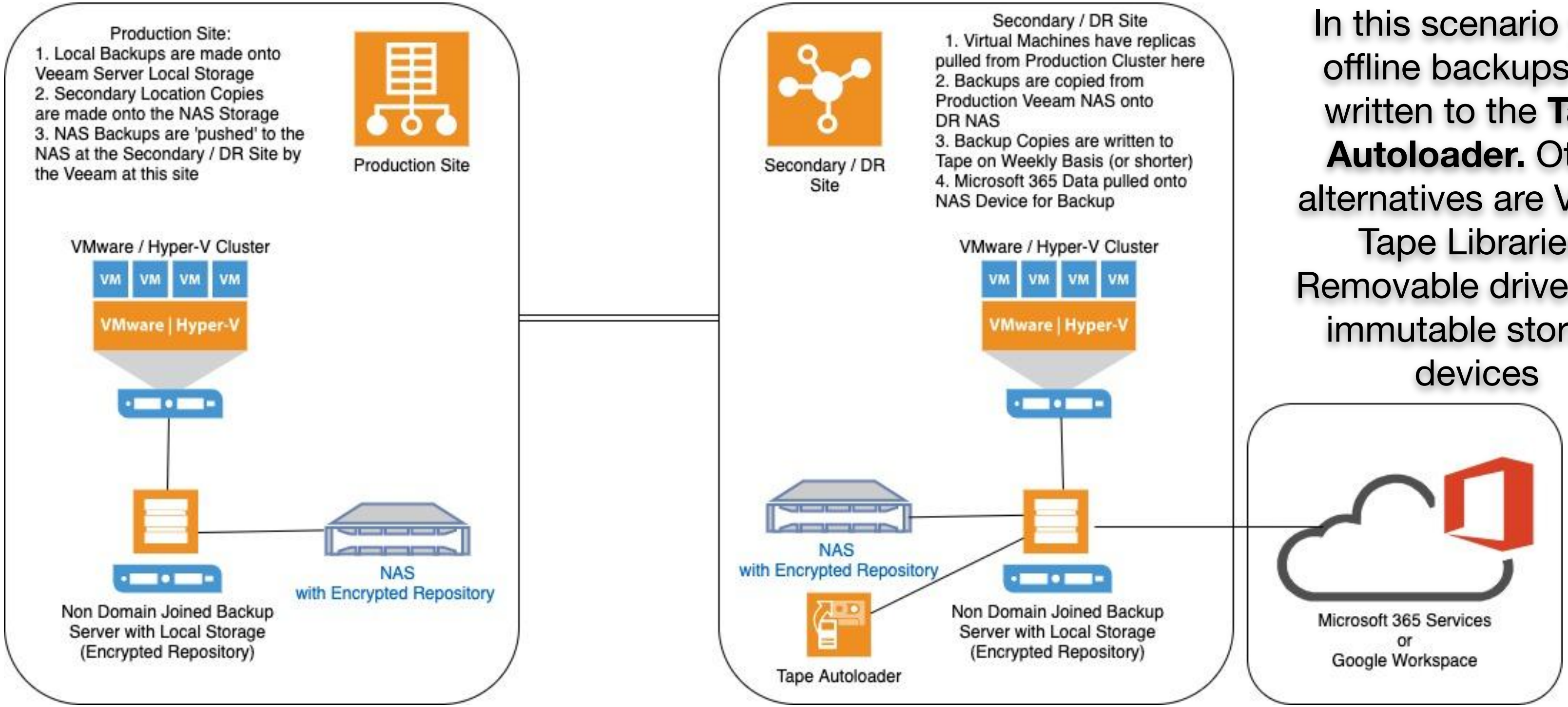
How can I implement offline media?

- Tape Autoloaders or Removable Disks can be added to backup servers as additional backup locations.
- VTL products will require sufficient additional storage to back the VTL software. They will be presented to the backups servers as additional backup locations.
- Cloud Storage Gateways can be added to backup servers to connect your on premise backup server to cloud storage providers (Amazon AWS Storage, Microsoft Azure Storage, etc).
- SAN Based Storage will require at the least additional licensing and will be dependent on the hardware vendor and the backup solution that is in place.

Implementation (cont.)

- But what if I already replicate my fileshares as CIFS shares direct from my SAN?
  - By having an offline copy of the data will allow a restore if your data is compromised by an attack.
  - Mapping CIFS shares within some Virtual Machines will facilitate a backup of these areas.
  - Use technologies such as NetApp SnapVault to give you immutable copies or multiple read/write points away from your primary snapshot.

Overview schematic of an ideal configuration



Production Site:
1. Local Backups are made onto Veeam Server Local Storage
2. Secondary Location Copies are made onto the NAS Storage
3. NAS Backups are 'pushed' to the NAS at the Secondary / DR Site by the Veeam at this site

Secondary / DR Site
1. Virtual Machines have replicas pulled from Production Cluster here
2. Backups are copied from Production Veeam NAS onto DR NAS
3. Backup Copies are written to Tape on Weekly Basis (or shorter)
4. Microsoft 365 Data pulled onto NAS Device for Backup

Production Site
VMware / Hyper-V Cluster
VM
VM
VM
VM
VMware | Hyper-V
Non Domain Joined Backup Server with Local Storage (Encrypted Repository)
NAS with Encrypted Repository
Secondary / DR Site
VMware / Hyper-V Cluster
VM
VM
VM
VM
VMware | Hyper-V
NAS with Encrypted Repository
Tape Autoloader
Non Domain Joined Backup Server with Local Storage (Encrypted Repository)
Microsoft 365 Services or Google Workspace

In this scenario your offline backups are written to the **Tape Autoloader.** Other alternatives are Virtual Tape Libraries, Removable drives and immutable storage devices

Veeam has been used in this example as it is the most prevalent technology in use amongst the 29 Councils reviewed. Arcserve UDP would work in effectively the same manner. SAN Based Snapshot systems (NetApp, Nimble etc) would be different from the technologies illustrated here

LOCAL DIGITAL Cyber

Ministry of Housing,
Communities &
Local Government

Thank you

We welcome feedback on our cyber support service

@LDgovUK

www.localdigital.gov.uk

#LocalDigital #FixThePlumbing

LOCAL DIGITAL Cyber