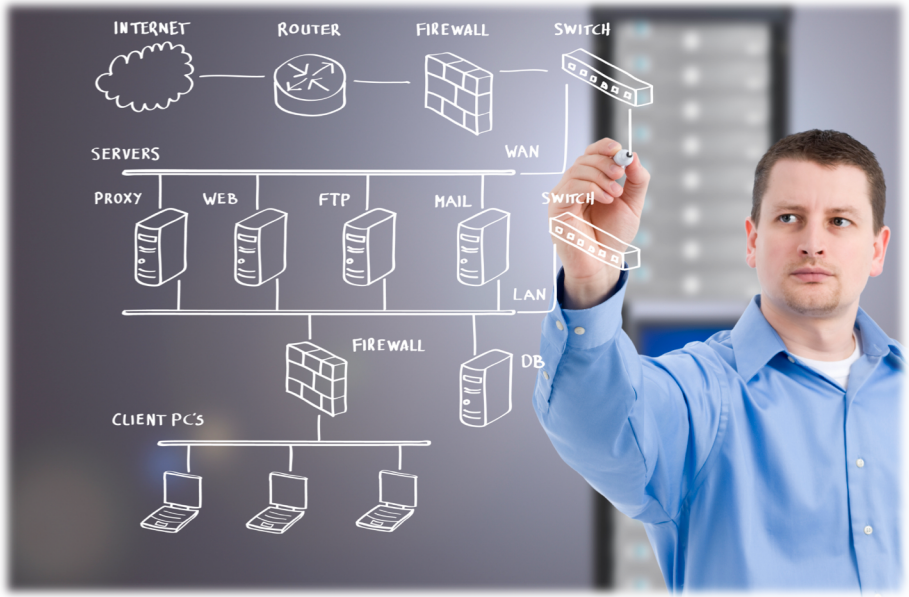
As an alternative to expensive cloud storage, Storage Networks can host a cost-effective NAS from Synology, QNAP, TrueNAS, and others to serve as an offsite backup repository for Veeam, Nakivo, Arcserve, and Unitrends.

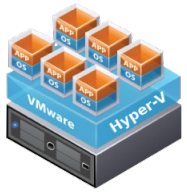
The device will be fully monitored and maintained in an SOC Certified Colocation Facility so no travel is required by your IT team, regardless of where you are in the world.

For most customers, the advantage to a hosted NAS is cost savings observed from not having a monthly bill that grows as you store more backups.

For smaller environments, Storage Networks does offer traditional “per TB” pricing for backups where data is stored on our SAN.



Customer Server Room



Customer Firewall

Virtual pfSense / Barracuda / Fortinet Firewall OR OpenVPN

Storage Networks

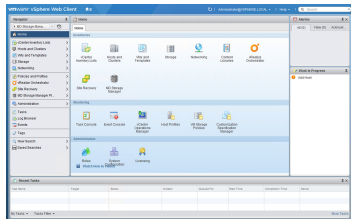
Backup proxy

Remote Hosted Veeam / Nakivo / ArcServe Proxy / RPS

1

2

Writes Data to Hosted Synology Server



Restores Data to vCenter (vSphere), Hyper-V, or KVM servers for testing or DR

3

- QNAP, FreeNAS, TrueNAS work too
- Site to Site VPN is preferred, but a simple OpenVPN agent can be deployed on the local backup server if a Site-to-Site VPN is not possible.

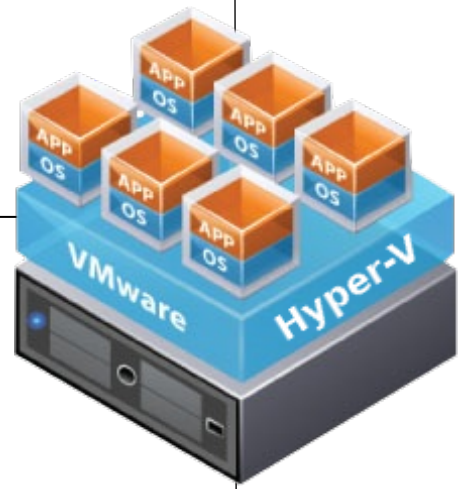
DRaaS Environment Access

OPTION 1: Assign public IPs to VMs (IIS, Exchange, etc.) and NAT via virtual pfSense, Fortinet, or Barracuda Firewall

OPTION 2: Use Windows Terminal Services (included in SPLA) so users can access non web-enabled applications via RDP

OPTION 3: Site to Site VPN so local users can access server resources if PCs are still available on premise (i.e. fire in server room leaves rest of office functional)

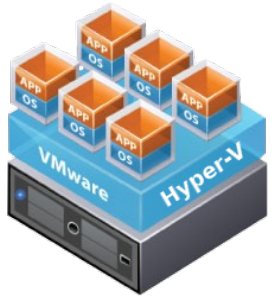
OPTION 4: Manage VMWare / HyperV via Complementary Windows 10 VM

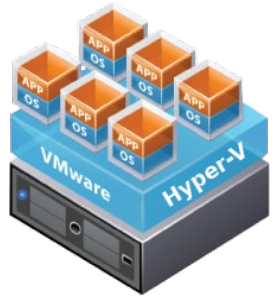


Storage Networks Virtual Infrastructure

REPLICA

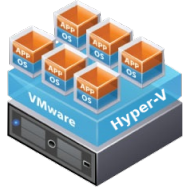
A Veeam or Nakivo Replica takes periodic snapshots on the source and copies to the destination. VMs can be spun up offsite quickly, but you are limited to 24 restore points. A hosted Synology NAS can be used to store targets with an ESXi / Hyper-V Server in front.

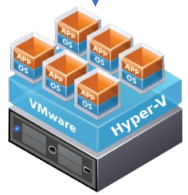




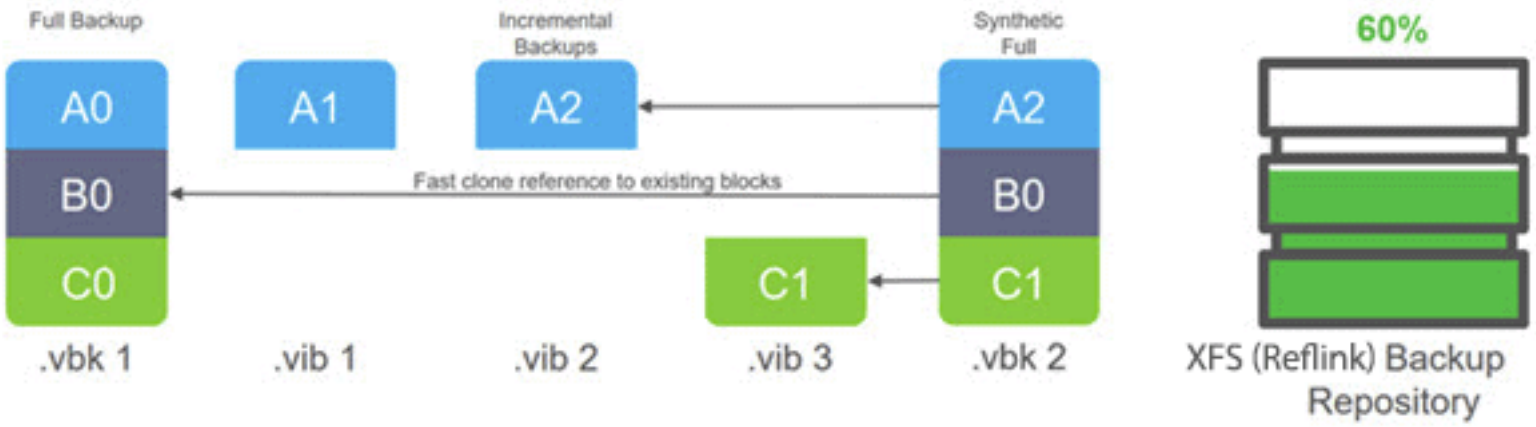
BACKUP COPY

A backup copy job just copies data from the customer storage system to the remote (hosted) storage system. No active running hypervisor is required at the cloud side. Recovery time (the time it takes to be up and running “in the cloud” is longer, however, as the backups need to be restored to a hypervisor.



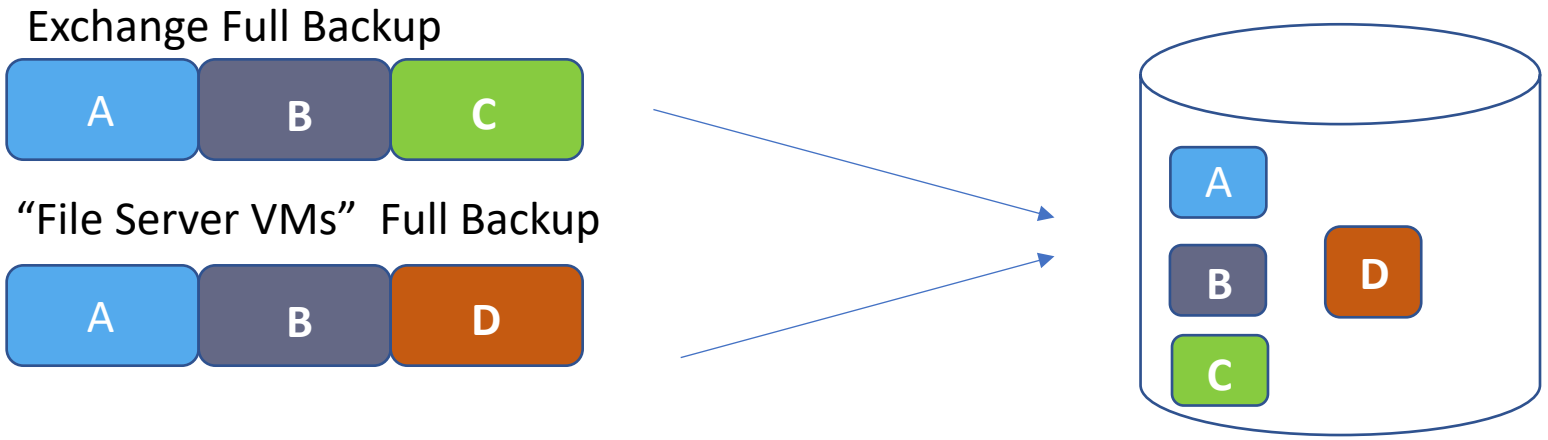


Newer Versions of Veeam and Nakivo support XFS Fast Clone:



XFS Fast Clone Repository

+ Supported with Immutable Repository
+ Should Dedupe Well with Synthetic Fulls
- Won't Dedupe with regular fulls or across backup jobs.
  - Ex: Common Blocks in the Exchange Backup won't dedupe with a file server.



RedHat VDO Repository

+ Best Data Reduction across all jobs
- Not Supported with Immutable Repo
- Synthetic Operations can be a bit slow, but this taxes SN, not Lexington

- ✓ Backups to a DR site should be tested regularly. Any time you use WAN optimized backup (Veeam, Unitrends, doesn't matter) there is a chance that an incremental backup corrupts the chain resulting in unusable backups.
- ✓ Restore procedures should also be documented. The first restore for all our customers, whether on premise or in the cloud, takes longer than expected due to unforeseen issues.
- ✓ **Frequently Observed Roadblocks During Disaster Spinup:**
  - Forgotten Passwords
  - Missing Active Directory Infrastructure
  - Unrealized services that must be manually brought online because the application / database is in a "failsafe" state
  - Missing Firewall Entries at the DR Site

Encryption in Transit

256-Bit AES Encryption with Nakivo / Veeam (native) and IKEv2/Ipsec Site-to-Site for backup applications that do not have native in flight encryption.

Data at Rest Encryption

Data is stored encrypted on disk drives.

Secure Facility

SSAE 18 standards for both SOC 1 Type II and SOC 2 Type II secure datacenter.

Secure Disaster Recovery Environment

In addition to Storage Networks' own firewalls protecting our infrastructure, your private DR environment will be protected by a virtual Cisco / Barracuda / pfSense virtual firewall that can be fully configured to your IT security standards (NATing, malware protection, IP restrictions, etc.)

Contact us for a free estimate and proof-of-concept.

Typical costs include the market rate for a rack mount Synology / QNAP / Other NAS, disk drives, and a monthly hosting fee for the equipment that does not increase as your dataset grows. You may need to purchase an extra disk drive if you run out of space, but this will not affect the monthly hosting fees.

Phone: 855-638-7867 (Extension 1)

E-Mail: projectcoordinator@storagenetworks.com