DIGITAL CONTINUITY BY DATASTOR™

Best Practices
DATASTOR Enterprise Protection Server Deployment

This document describes several deployment options for the DATASTOR Enterprise Protection Server (EPS) and Scalable Protection Server (SPS) data protection solutions. These solutions have been designed to provide digital continuity for businesses of all sizes and as such are flexible and allow the client to select the most appropriate deployment option for their IT infrastructure. State-of-the-art tools for backup, archive and replication to facilitate Disaster Recovery (DR) are integral in DATASTOR Enterprise level solutions. All the deployment options include the initial backup to a local disk device (Internal, DAS, SAN, RDX, NAS storage target) followed by a copy and/or vaulting process for reliable off-site data protection to complete the DR solution. There are several factors that influence the decision for optimal deployment.

- Size of the IT infrastructure (number of servers to be protected)
- Number of physical locations in the organization
- Distance between physical locations
- Anticipated natural disasters at the specific geographical location
- WAN infrastructure
- Client preference for DR method
- Cost

One Office/Location

Smaller organizations with one location or multiple locations without a WAN[MM1] or VPN between locations should plan for a deployment as shown in Figure 1 below. All the backup data will initially be stored on the disk media of choice. The data is stored on disk in logical storage units called “Stores”. This backup data is the primary data source for fast recovery that will be required due to an isolated issue such as accidental deletion of files, disk failure, server/workstation failure, etc. Detailed planning is required for the optimal DR process.

There is no perfect DR process but it is always preferable to have a copy of the backup data off site as all locations are subject to local disasters such as a fire that can destroy the client’s place of business. When determining where the copy of backup should be kept geographical location requires consideration. For example, locations prone to widespread natural disasters like earthquakes, floods and hurricanes need to plan for possible destruction of a large area around the client’s business. In cases such as this having a copy of the backup data in close proximity to the business increases the risk of DR failure because the copy may also be damaged or destroyed. An option in this scenario is vaulting the backup data to cloud storage. This solution is not a failsafe option for fast recovery as local infrastructure damage may delay access to the backup data, but the potential for damaged or destroyed data will be minimized. DR planning applies to all the deployment options discussed in this document.

Below are some of the off-site storage options for DR you can apply to your deployment:[MM2]

- Copy data to a portable hard drive or a removable ruggedized hard drive (RDX cartridge) that will be kept at an off-site location. EPS and SPS have built-in tools (Store Groups) that facilitate the rotation of multiple disk media devices.
- Vault data to a tape library for off-site storage.
- Vault data to cloud storage
- Combination of above options to further minimize the risk of DR failure.

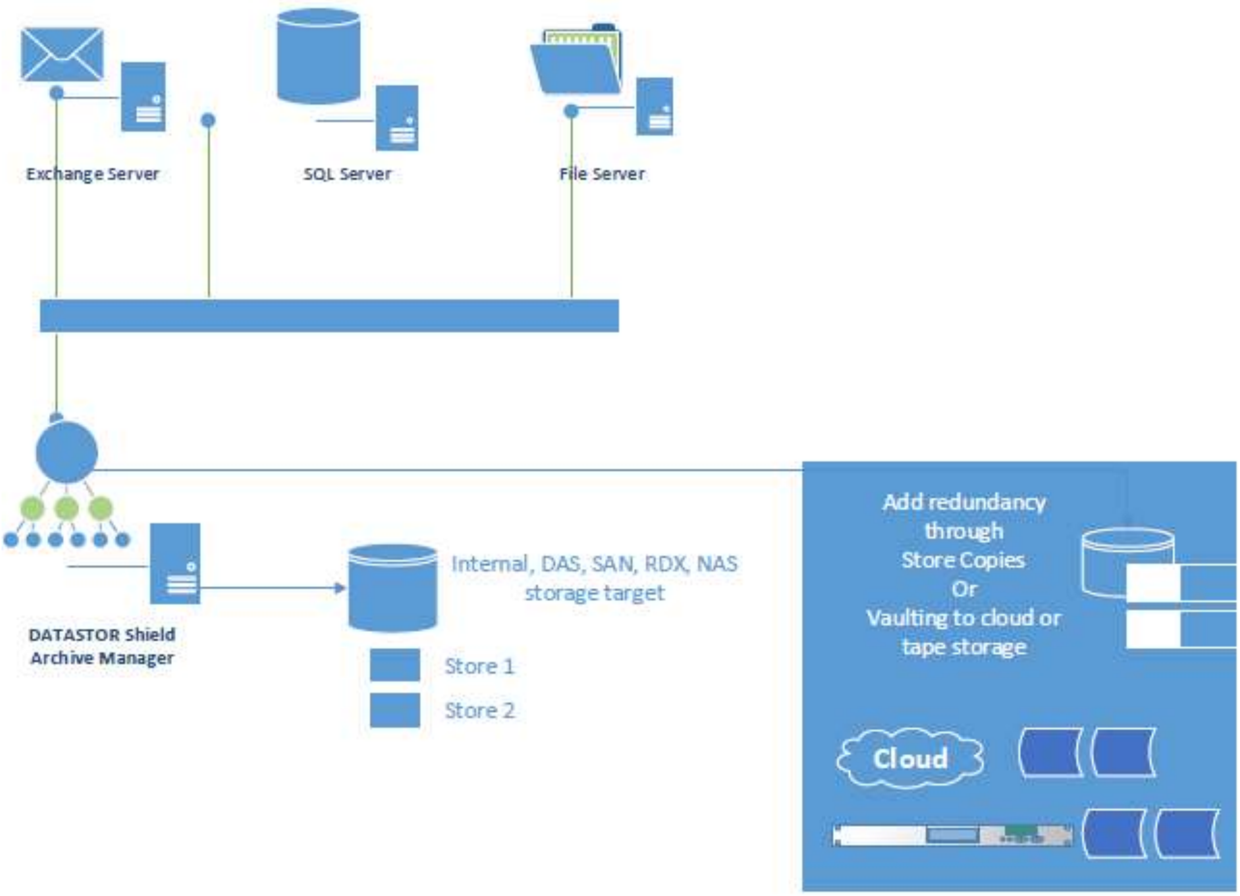
Exchange Server
SQL Server
File Server
DATASTOR Shield Archive Manager
Internal, DAS, SAN, RDX, NAS storage target
Store 1
Store 2
Add redundancy through Store Copies Or Vaulting to cloud or tape storage
Cloud

Figure 1

Two Office Locations

The deployment shown in figure 2 requires a private line (WAN) or VPN for implementation. In general the faster the connection between locations the more efficient the replication process will be. An important benefit of global deduplication is the compounding efficiency on network bandwidth utilization when transferring between locations.

In this deployment there is an Archive Manager installed at each location. An Archive Manager centrally manages the protection plans for all servers and workstations at a site. Backup data is stored to local storage and then replicated to storage at another location. Backup data at Site 1 is replicated to Site 2 and data from Site 2 is replicated to Site 1. Depending on geographical considerations this may be sufficient but the DR options described earlier would add another level of redundancy and reduce the risk of DR failure.

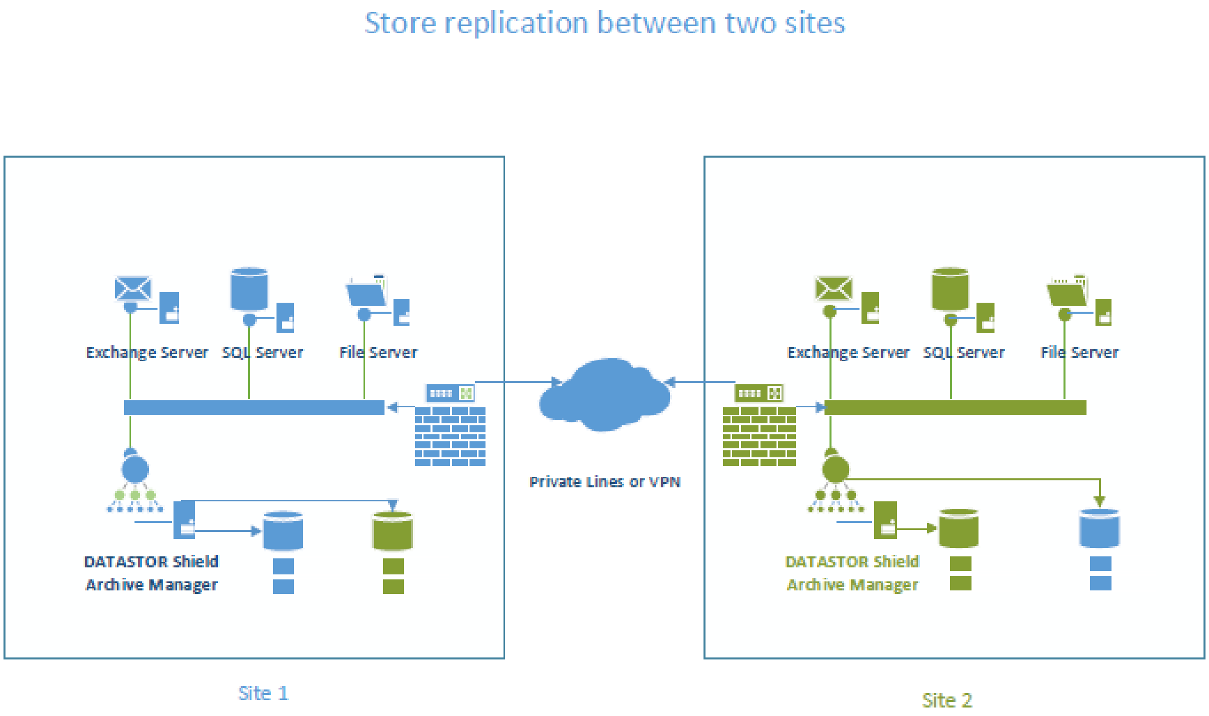

Figure 2

Multiple Locations with local backup

This deployment is very similar to the two location deployment. Each site has an Archive Manager. Protection plans can be managed centrally or locally. Backup data is replicated over a WAN or VPN to a data center or main site. This is commonly referred to as a “Hub and Spoke” deployment. Depending on the security of the data center site, additional redundancy options such as removable disk, tape or cloud should be considered. See Figure 3.

The case study linked here http://www.datastor.com/site/wp-content/uploads/2012/10/FirstOnsiteCSFinal5.pdf is an example of this implementation. With over 40 locations firstonsite Restoration had a significant data protection challenge. Their solution combined the hub and spoke architecture with RDX removable disk technology. Protection plans for all locations are managed centrally with data stored locally on the RDX ruggedized removable disks. This solution facilitated seeding the centralized storage by initially shipping RDX media with subsequent backups taking place over the WAN.

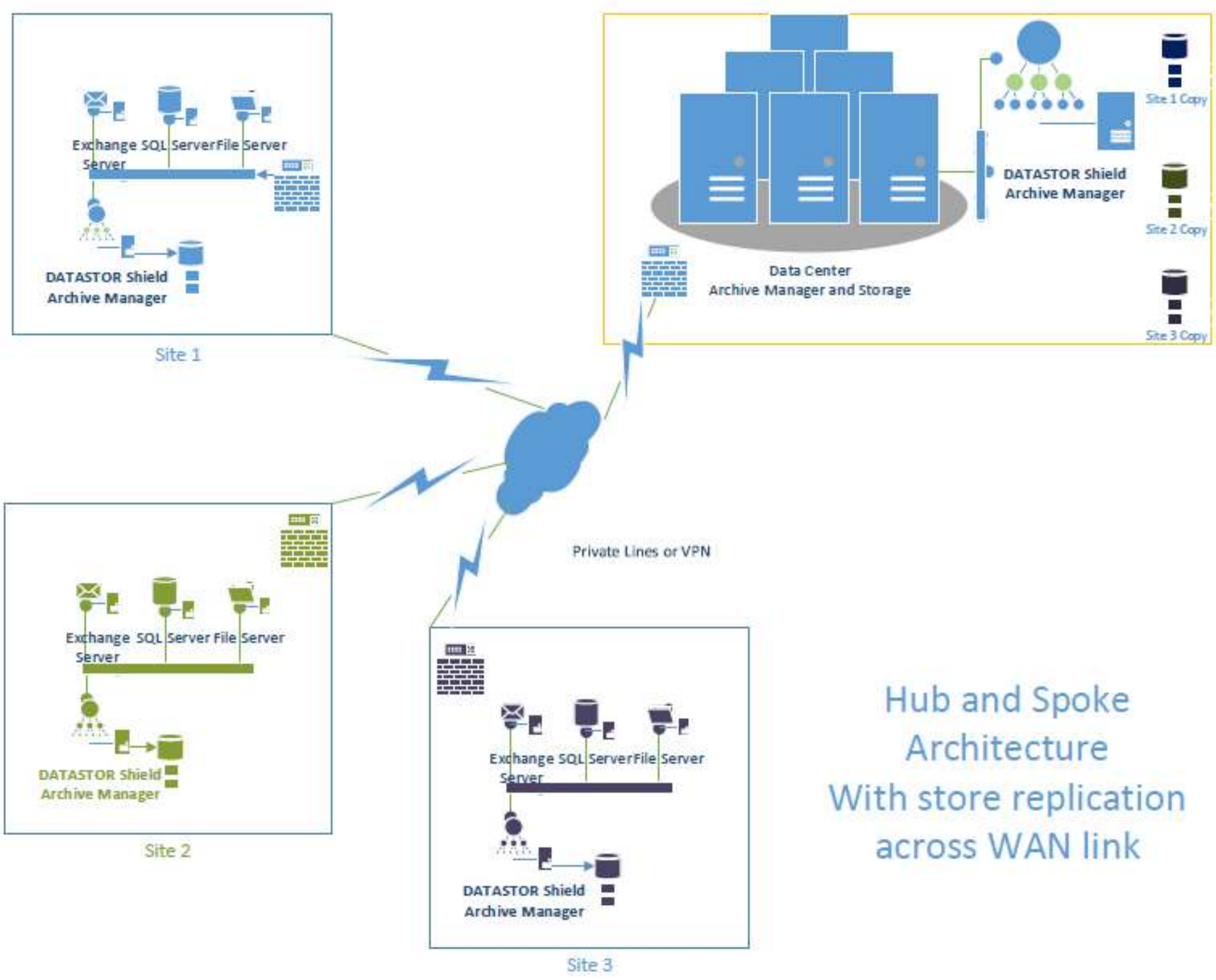
Exchange Server
SQL Server
File Server
DATASTOR Shield Archive Manager
Site 1
Exchange Server
SQL Server
File Server
DATASTOR Shield Archive Manager
Site 2
Exchange Server
SQL Server
File Server
DATASTOR Shield Archive Manager
Site 3
DATASTOR Shield Archive Manager
Site 1 Copy
Site 2 Copy
Site 3 Copy
Data Center
Archive Manager and Storage
Private Lines or VPN
Hub and Spoke Architecture
With store replication across WAN link

Figure 3

Multiple locations – Central backup

This deployment option (Figure 4) is a good option for businesses that have the infrastructure to support the data recovery needs of the business. Because there isn't a local copy of the backup data at remote locations, network bandwidth must be sufficient to provide a reasonable recovery window. For single file recovery this is generally not an issue. An alternate recovery solution for larger recovery scenarios would be to transport a copy of the backup data via removable disk to the recovery site. Ideally the recovery site is in close proximity to the central location.

When executing protection plans on servers at remote sites, plan runtime can be reduced by utilizing cached content on the remote server. While the plan executes, the Remote Accelerator process can access the cached content locally, generate the difference file, and then just send the difference file across the WAN, reducing network communication and reducing the backup window.

This case study http://www.datastor.com/site/wp-content/uploads/2012/10/SVVSD_CaseStudy_v2.pdf details the implementation at the St. Vrain Valley School District. Backup data is stored at a central location and then replicated offsite.

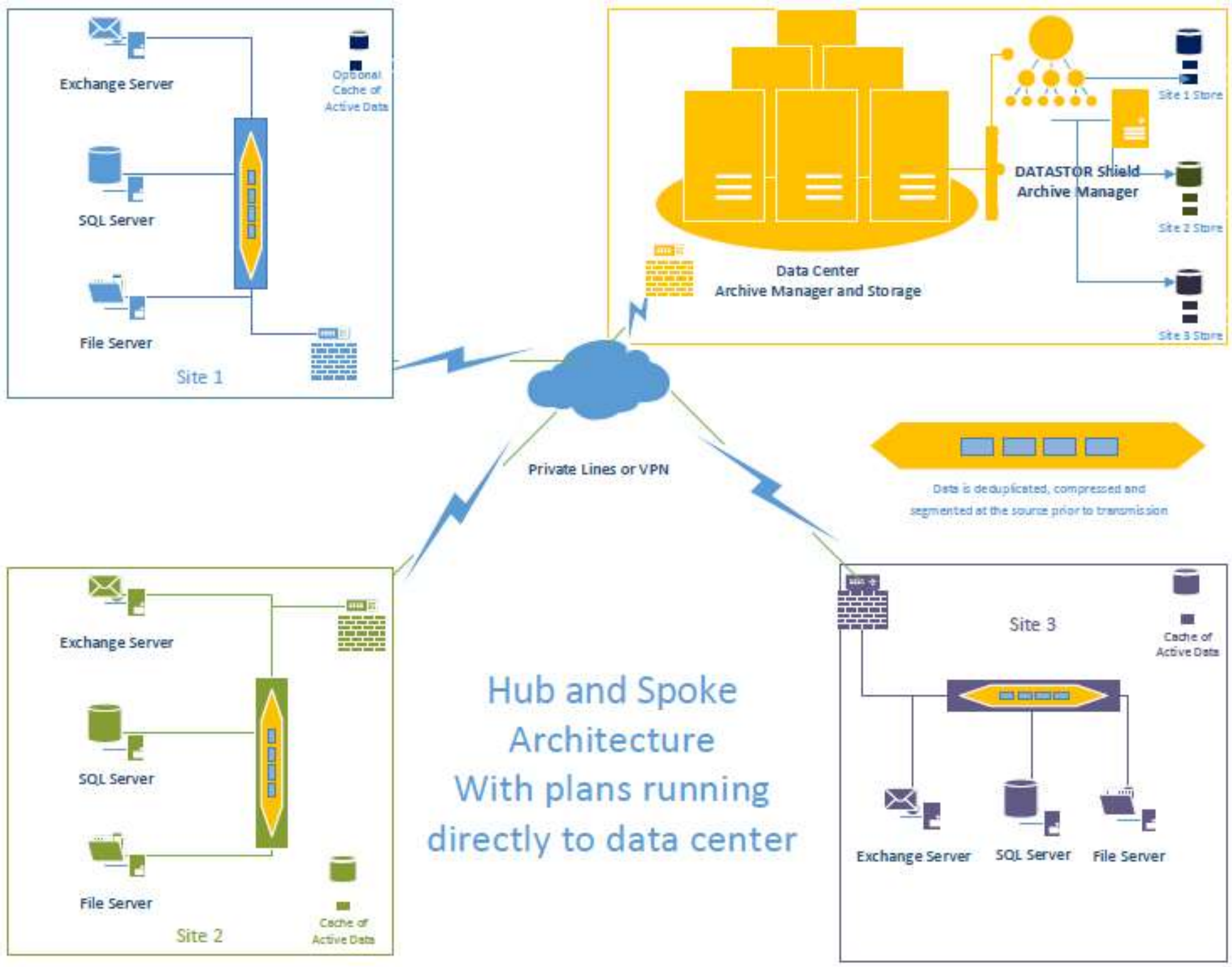
Exchange Server
Optional Cache of Active Data
SQL Server
File Server
Site 1
Site 1 Store
DATASTOR Shield Archive Manager
Site 2 Store
Data Center
Archive Manager and Storage
Site 3 Store
Private Lines or VPN
Data is deduplicated, compressed and segmented at the source prior to transmission
Exchange Server
SQL Server
File Server
Site 2
Cache of Active Data
Hub and Spoke Architecture With plans running directly to data center
Site 3
Cache of Active Data
Exchange Server
SQL Server
File Server

Figure 4

Summary

The numerous tools that are integral to DATASTOR enterprise protection solutions provide the flexibility for architecting a data protection plan to meet the needs of businesses large and small. Contact DATASTOR for consultation services on specific configuration needs.