

Setting Up Your Infrastructure:

Disaster Recovery & Business Continuity Best Practices

Disaster Recovery Overview

Data Loss & Employee Downtime is an Inevitable Event. The question is: *What Will You Do?*

Tomorrow, next week, six months, next year—it will happen. Your organization will experience data loss from a server or from an individual's computer. Are you prepared for that event? Some points to consider:

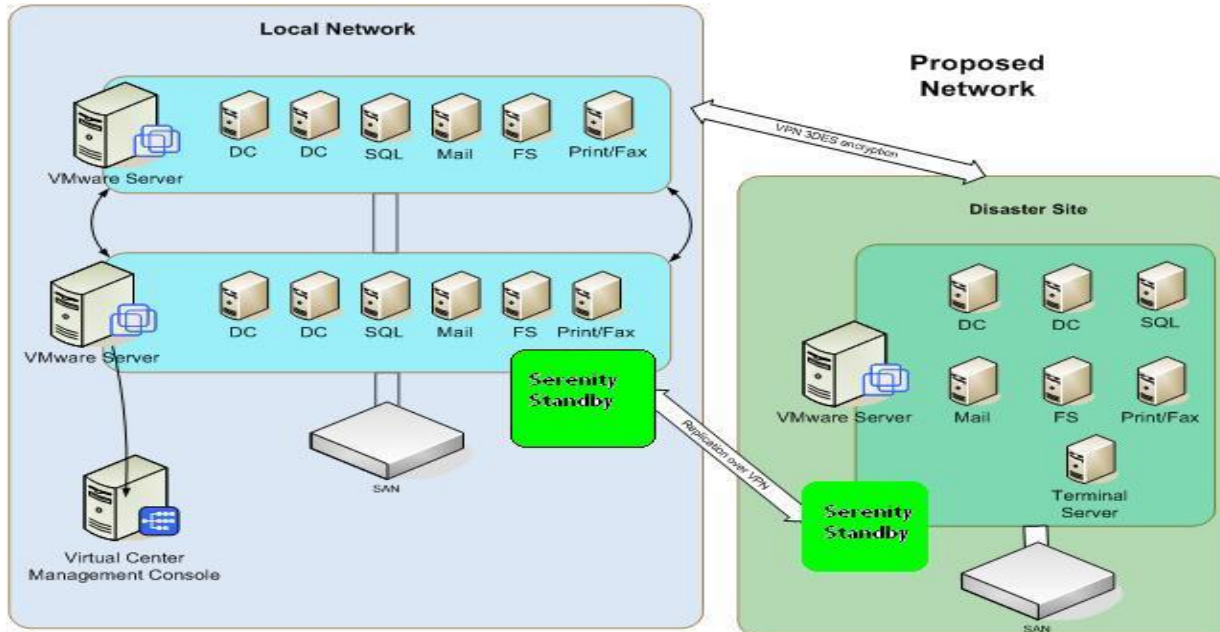
- U.S. small businesses lose over \$10 billion per year because of data loss. - American Data Recovery Association
- Hardware or system failure accounts for 78% of all data loss. - American Data Recovery Association
- Human error accounts for 11% of all data loss. - American Data Recovery Association
- 60% of companies that lose their data will shut down within 6 months of the disaster. American Data Recovery Association
- 40% of small business will go out of business if they cannot get to their data in the first 24 hours after a crisis. -- Gartner
- 43% of companies never resume business following a major fire. Another 35% are out of business within 3 years. -- U.S. National Fire Protection Agency
- 93% of companies that had trouble restoring their data after a data disaster are out of business within 18 months. -- HP

Technology crashes can have a devastating and sometimes lasting effect on business efficiency. Hurricanes, tornadoes, floods, malicious acts, or simple mistakes: unfortunately, unplanned outages do happen. From natural disasters to human error like kicking a power cord loose, every business is susceptible to some form of business stoppage. No business can afford to just be down for days or even hours without suffering a loss of some sort. At best, your company could expect to incur minor financial losses and have to smooth things over with unhappy customers. At worst, a business would be unable to recover and resort to closing.

Executive Summary

If data and employee uptime is critical setting up a virtual environment for disaster recovery should be explored and the cost-benefits weighed accordingly.

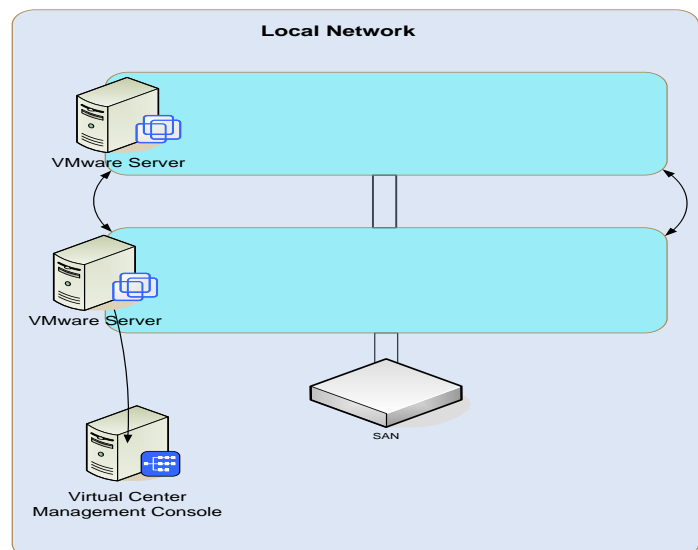
Step One: Map Your Local Network



Step Two: Setup Virtual Infrastructure

Scope includes but is not limited to:

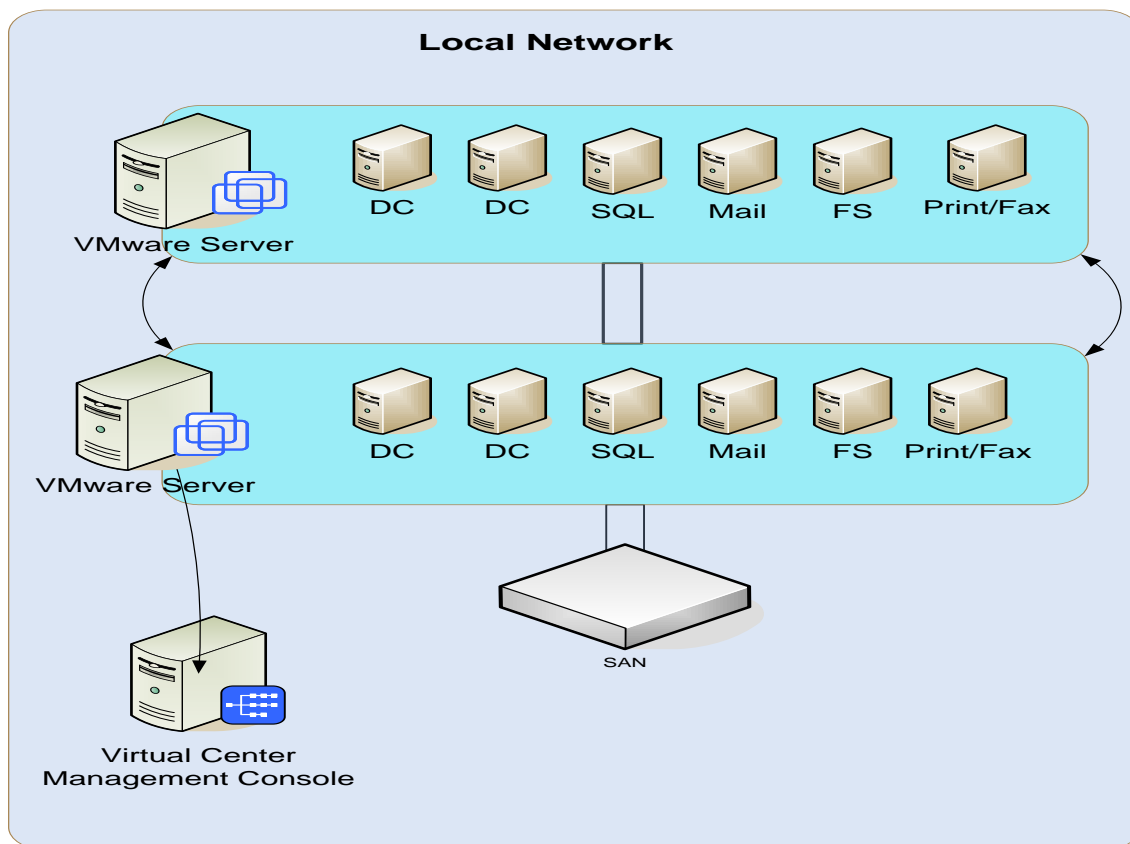
- Physically setup servers and SAN infrastructure
- Setup Virtual Machines
- Configure SAN software and setup LUNs on both SANs
- Create license server for VMware licensing
- Setup Virtual center server
- Enable load balancing and high availability functions



Step Three: Virtualize Existing Physical Servers

Scope includes but is not limited to:

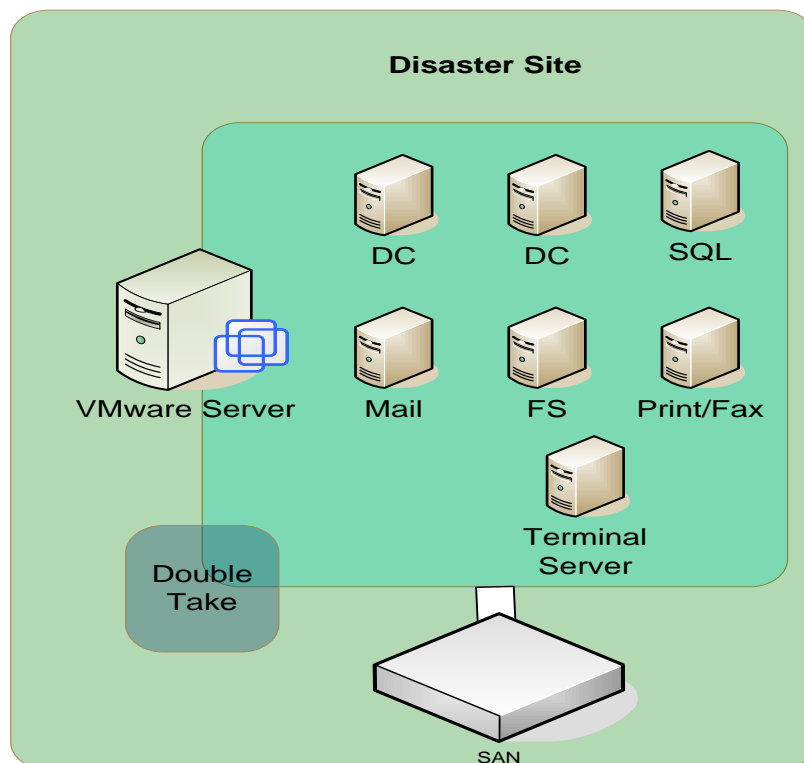
- Virtualize domain controllers
- Virtualize SQL server
- Virtualize mail server
- Virtualize File server
- Virtualize Print and Fax server
- Migrate virtual images to new VI environment
- Bring up all new VM's in new environment
- Move SQL database to SAN
- Move Exchange Information store to the SAN
- Move files and folders to the SAN
- Test high availability functionality



Step Four: Setup Disaster Recovery site

Scope includes but is not limited to:

- Cut over the network functions to new VI environment
- Post cutover support
- Physically setup servers and SAN infrastructure
- Migrate virtual machine to Disaster recovery VM server for initial seed
- Setup terminal server Virtual machine
- Install line of business applications on the terminal server
- Ship disaster recover site hardware to new data center



Step Five: Connect Disaster recovery site and start replication

Scope includes but is not limited to:

- Verify the link to the disaster recovery site
- Install local virtual infrastructure
- Initiate replication

Step Six: Test and Documentation

Scope includes but is not limited to:

- Test the High availability on local LAN
- Test replication
- Test disaster recovery processes
- Document new environment and train employees and managers

Disaster Recovery Provider Criteria:

1. Cost
 1. Amount of data
 2. Number of applications
2. Accessibility / Reliability
 1. Connectivity SLA (Service Level Agreements guaranteeing performance and uptime)
 2. Confidentiality - only those who need access to certain information have it.
 3. Ensures that resources will not be deleted or be made inaccessible. The inability to access a required resource at Personable by attack, intentional tampering, or even catastrophic events has been minimized by careful attention to physical site security, redundancy, fail-over planning and comprehensive disaster recovery strategies.
 4. Pipe and bandwidth speeds
 5. Redundancy
3. Backup Solution
 1. Preventive monitoring
 2. Workflow
 3. Devices: Network, Server, PC, Laptops, PDAs, Applications, Databases.
 4. Rolling backup frequency - Go back to any previous version from 15 minutes up to one year before.
 5. Anytime, Anywhere Access. While any provider can give you access to your QuickBooks from any computer with an internet connection, our system is robust and built to be used every day. The virtual desktop makes it easy to move files and interact with your programs from any computer.