South Colonie Central School District

Server Virtualization
and
Disaster Recovery Plan

Prepared by Lucid Solutions Group

Table of Contents

Executive Summary

In 2007 South Colonie Central School District sought out an affordable and reliable disaster recovery solution. At the same time several servers were approaching end of life and had fallen out warranty. In addition, with the cost and capacity of new server hardware, many of the servers would have been severely underutilized. These appeared to be different problems requiring different solutions. However, Lucid Solutions Group (formerly SystemsEng), introduced the school district to server virtualization as a means of solving both problems.

Server virtualization converts physical servers into virtual servers, allowing several servers to operate on a single physical server. Instead having 10 different physical servers (along with the space and power requirements), and IT staff can have 10 virtual servers running on 1 physical server. This reduces the need to replace purchase new physical server to replace old ones.

Virtual servers are represented by flat files that reside on a physical server hard drive. Because they are flat files, virtual servers can be easily moved between physical servers as well as separate geographic locations. This makes disaster recovery easier, less expensive and quicker. Disaster recovery plans based solely on hardware require identical hardware for each physical server in the organization to exist in at a recovery site. This hardware typically sits unutilized until a disaster occurs. This is a very costly and wasteful solution, which is why many organizations choose not to implement it. With server virtualization technology, the recovery site simply needs enough hard drive space to store replicas the virtual machines.

After consultation with Lucid Solutions Group (formerly SystemsEng), the school district chose VMware as the virtualization platform to address the above stated problems. During this project Lucid Solutions Group (formerly SystemsEng) virtualized several physical servers and reallocated a couple of those physical servers to replacement even older servers. Lucid also set up a disaster recovery site at the Roessleville Elementary School. However, the disaster recovery plan is an in-depth one with several layers of protection. An overview of the plan follows.

Disaster Recovery Overview

The following sections are an overview of the virtualization approach and disaster recovery plan. Configuration drawings are also included to better explain the design.

Data Corruption, Accidental Deletion and Prevention

Traditional Tape Backup

Although most of the servers are now virtualized the data that resides on those virtual servers looks no different to staff as they did when running on physical servers. These virtual servers run the Symantec Remote Backup Agent. This agent allows the Symantec Central Backup server to connect to the virtual servers and back up the data to tape on a daily basis. The Symantec Central Backup server connects to a tape backup autoloader, which holds several tapes at one time. The autoloader automatically switches between tapes during the backup process, reducing the amount of time server administrators spend changing out tapes.

In this case if a data file or group of files become corrupt or are accidentally deleted, IT staff can recover the file with ease by restoring it from tape. This is a relatively quick and simple process. Most people familiar with data center operations will quickly notice that this procedure does not differ from that employed with physical servers. The difference with the current solution is that it does not stop here. This is only the first tier of the in-depth disaster recovery solution.

Virtual Machine Snapshots

It is not unusual for data to become corrupt as the result of software patches and configuration changes. With physical servers the only solution is restoring the data from tape. However, snapshots allow the server administrator to make a “point in time” copy of the virtual machine prior to software patching and configuration changes. If at any time during the patch update or configuration change data is corrupted, or worse, the server becomes unresponsive, the server administrator simply reverts to the previous snapshot with a mouse click. Within seconds, the virtual machine returns to the same state it was in when the snapshot was taken. There is no need to go to tape in order to restore files. This is part of the standard operating procedure in a virtualized environment.

Physical Servers

Although it would be ideal to virtualize all physical servers, there are some servers that could not be permanently virtualized for a variety of reasons. It was critical that these servers also benefit from the data protection offered by virtualization. The solution to this problem was to virtualize those physical servers strictly as a means of recovery. A virtual copy of these servers are created on a regular schedule and taken offline. If at any time the physical server suffers a hardware failure, the virtual version can be brought online within minutes and made current by restoring data files from the most

recent backup. Take the following simple example for a server called Physical Server A. Remember, all servers are backed up to tape on a daily basis.

1. As a means of data protection for physical servers Physical Server A is virtualized every Friday and Tuesday evening.
2. Physical Server A suffers a hardware failure on Thursday.
3. Server administrators start Physical Server A's virtualized version within a matter of minutes, which was taken on Tuesday evening.
4. Server administrators then restore data files from Wednesday evening's tape backup.
5. While data is being served from the virtual server, server administrators repair the hardware failure on the physical server.
6. Once the physical is repaired and ready to come back online, server administrators backup the data files on the virtual server to tape and shutdown the virtual server.
7. Finally, server administrators bring the physical server back online and restore the data files.

The above procedure makes the server (virtualized version) and its data available in less than 20 minutes, depending on the amount of files to restore, instead of hours or days. This solution also gives server administrators breathing room while repairing the physical server. Without the virtualized version of the physical server one of the following would have to occur:

1. The server and its data would be unavailable until the hardware failure is fixed, which could take hours/days depending the time it takes to receive and replace the failed part.
2. Server administrators would have to locate an identical physical server, install the base operating system and perform a full server restore from tape. If an identical server is available, which usually is not the case, the recovery could still take hours/days to complete.

Catastrophic Data Center Failure

A catastrophic failure is any event that results in serious or permanent physical damage to the main network hub, the high school, rendering operations inoperable.

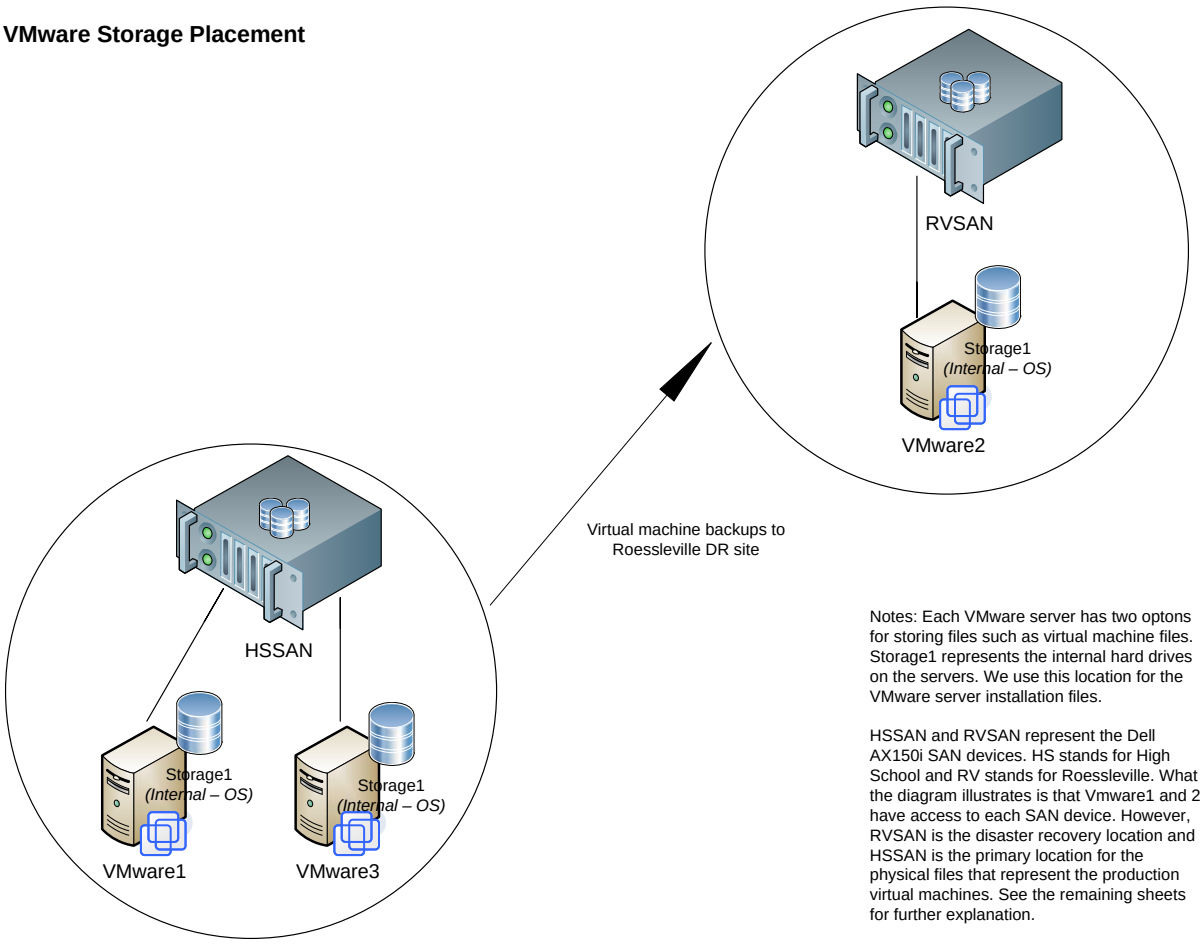
Disaster Recovery Site

A "hot site" describes a separate location that allows an organization to continue operations in the event of a catastrophic failure at the main networking hub. All data and work space is made available and ready for use with a short period of time.

Roessleville Elementary School acts as the school districts disaster recovery hot site by means of virtualization. Roessleville's server room has an identical VMware configuration as the high school, including the server and iSCSI SAN. The high school and Roessleville VMware servers communicate via the same VLAN, placing them on the same network. All production virtual servers exist on the high school SAN and are replicated to the Roessleville SAN on a regular schedule. The result is a complete replica of production virtual servers residing at the Roessleville site in a powered off state. In addition, a virtual server acting as an additional Active Directory Domain Controller resides on the Roessleville SAN. This is crucial because staff cannot access any network data without the availability of a domain controller, which is the entry point to the network. In the event of a catastrophic occurrence at the high school, virtual procuction servers can be powered on at the Roessleville site allowing access to critical data for as long as it is necessary.

Without virtualization this type of disaster recovery can be extremely costly. Consider the following. There are currently about a dozen production virtual servers running at the high school site. If these were physical servers identical hardware would have to exist at the Roessleville site, which would be extremely costly and wasteful. Implementing the virtualization solutions requires only one VMware server and one iSCSI SAN. See graphic on the next page.

VMware Storage Placement



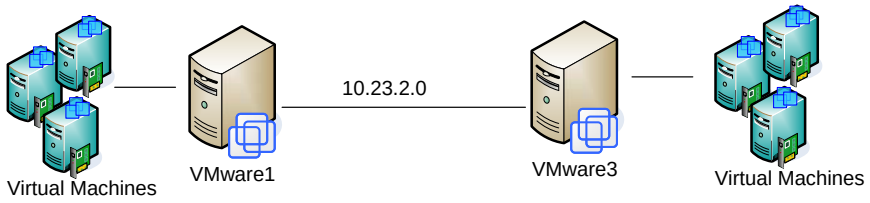
High Availability (HA)

Since the high school and Roessleville VMware sites exist on the same VLAN, despite them being in separate physical locations, the load of managing virtual servers is shared. The virtual servers themselves do not reside on the physical VMware servers. They reside on the iSCSI SAN that is attached to the VMware servers. The virtual servers are then managed by one VMware servers. Placing the virtual servers on the iSCSI SAN allows them to be managed by either VMware server with the use of VMware's HA and DRS features. However, virtual servers can only be managed by one VMware server at a time.

VMware HA continuously monitors each VMware server and in the event of physical VMware server failure, restarts the VMware server's virtual servers and hands over management of those virtual servers to the other running VMware server.

VMware HA also dynamically and without intervention move virtual servers between VMware servers based on current VMware server loads. This occurs without interruption to the virtual servers operations or access to virtual server data. See graphic on the next page.

VM Network – Vmotion, DRS, HA



Notes: Physical machines that were distributed throughout the school district are now virtual machine distributed across the 2 VMware servers. All servers now exist on the High School VLAN.

Placing the virtual servers on the same VLAN allows for increased uptime through the use of on the fly virtual machine migration, DRS and HA between the 2 primary VMware servers at the high school. If one server goes down or becomes over utilized the virtual machines are automatically migrated to the other VMware server. The virtual machines remain in the same physical location on the SAN but the other Vmware server takes over management of the virtual machines.

VMware2, located at Roessleville, is not part of the Vmotion, DRS or HA. Roessleville is strictly a DR site.

SAN Hard Drive Protection

As part of the disaster recovery plan it is critically important that the iSCSI SANs mentioned above be protected against hard drive failure. While it is not possible to completely protect a system from hard drive failure, it is possible to have a failsafe in place to eliminate downtime. The SANs utilize RAID-5 and hot spare hard drives for this purpose.

The RAID 5 system takes a group of individual hard drives and configures them as a single drive. If one of the individual hard drives in the RAID set fails, the system continues to function normally. The hot spare kicks in during the failure to automatically take over for the failed hard drive. The only way for the SAN to be brought down by a

hard drive failure is if two or more of the drives fail at the same time, which is highly unlikely. However, if this does occur, the “Hot Site” scenario comes into play.

Additional Benefits to This Approach

Reduced Hardware Costs and Server Sprawl

Before the virtualization project, the school district was faced with having to replace several servers that were five or more years old and out of warranty. These servers were scattered throughout the school district at several schools. The virtualization project allowed the servers to be virtualized and consolidated on the iSCSI SAN at the high school site.

In addition, the foreign language program was installed on separate servers in different school. That program has now been consolidated on a single virtual server also running on the iSCSI SAN. As new needs arise for servers, instead of purchasing new hardware to run one or two applications, the school district can simply create a virtual server on the iSCSI SAN. The standard procedure is to create new virtual servers instead of buying new physical servers unless there is a specific and compelling need for new physical servers.

Reduced Server Administration Overhead

Prior to consolidating physical servers into virtual servers, server administrators had to drive to different schools in order to address physical server problems. This often resulted in increased downtime. All virtualized servers are now available via a single console application running on each server administrator’s computer. In addition, the time it takes to provision a new server can be hours or days depending on the amount of software to install. New virtual servers are created using pre-configured templates. These templates are virtual machines that have already been installed and configured with the base operating system configuration. To create a new virtual server, administrators simply create the server based on an existing virtual server template. This is an operation that literally takes minutes to complete.

Additional Infrastructure Changes

The server virtualization and disaster recovery project allowed space for several infrastructure improvements. These improvements resulted in increased uptime, less network administration overhead and better protection of data.

Active Directory Domain Structure

Prior to Lucid's involvement there were physical servers performing the domain controller role scattered throughout the district. This was a good solution years ago when the different locations were connected via slow WAN links. Since then the school district has installed fiber optic cable throughout, allowing for increased network speeds and reducing the need to place servers in all schools. Lucid consolidated Active Directory from about 8 domain controllers down to just 3. In addition, 1 of the 3 domain controllers are virtual servers.

Exchange Email Server

Prior to the virtualization project the Exchange email server experienced several issues as a result of hardware and software issues that occurred over time. The server itself was five+ years old and showing its age. Email outages and interruptions were a regular occurrence.

Several newer servers replaced by the virtualization project have been used to replace older servers Lucid assisted the server administrators in moving the Exchange application off of an older server to one of these newer servers freed up as a result of the virtualization project. This opportunity was also used to install a new version of Exchange Server software. Since the change email outages have been reduced significantly.

Web Server

The web server was in a similar situation as the Exchange server, running on older hardware. As with the Exchange server, the web administrator was able to reuse one of these newer servers freed up during the virtualization project that for the web server application.

Windows 2003 Shadow Copies

Windows 2003 shadow copies provides yet another layer of data protection by its own version of file snapshots twice per day, once in the morning and once in the afternoon. Windows 2003 stores a copy of the all shared files on the server and stores them in a hidden location on the server. At anytime a server administrator can restore a "previous version" of a file or folder dating as far back as several weeks. This is a simple file copy from the hidden location on the server to any location the server administrators chooses. Being a simple file copy makes the operation much quicker than restoring from tape. This is one of the many reasons why Windows 2003 is the recommended operating for newly configured virtual machines.