Replacing File Servers With a Network Attached Storage Solution In All Remote Offices of the S.C. Vocational Rehabilitation

Chris S. South

S.C. Vocational Rehabilitation department

January 24, 2011

Problem Statement

The S.C. Vocational Rehabilitation Department for several years has utilized servers in each field office to allow employees to store files such as Word, Excel, PowerPoint and Outlook archive documents. Servers are provided for each office so that files may be accessed on a 'local area network' at faster speeds than if they were accessed remotely from a server in the State Office data center in Columbia. Although these are not high-end servers they cost approximately $3,300.00 each if you include software licenses that must be purchased for their operating systems. The agency currently operates 33 of these servers. When a server stops working in an office it must be replaced as quickly as possible if information technology staff cannot successfully talk field staff through steps to make the server operational again. Each server's files are backed up to a server in Columbia each night and before taking a replacement server to an office the files for that office must be restored to the new file server for that office. Once restored the server is driven to the remote location which can be up to 3 hours for some locations in South Carolina. Therefore, sometimes an office can be without their files for 24 hours or more if the replacement cannot be delivered by close of business at 5:00 p.m. There is also a chance that recently created files could be lost.

Network Attached Storage (NAS) devices have been developed over the past years to serve as storage solutions for Information technology. A typical NAS device costs a fraction of a server to purchase, has more than double the storage capacity of a typical server, does not require any software licenses and is approximately 75% smaller in size and weight than a server.

Purchasing two NAS devices that store over one terabyte (1 trillion bytes) each worth of data cost less money than purchasing one file server with one terabyte of storage space. If each

office had two NAS devices that successfully utilized the built in automatic NAS-to-NAS synchronization function that comes with the device then, the time employees are without file access can be reduced to a few minutes and file loss would be almost nonexistent. When a 'primary' NAS device stopped working in an office I.T. staff would be able to remotely activate the 'secondary' NAS device as the new primary. Because these two devices' files stay synchronized all files would be ready for access within minutes with no file restore or technician-travel time necessary at that moment. Files from the primary NAS device in each office would continue to be backed up to the State Office each night in the event of a disaster that would damage both primary and backup NAS devices at an office. Although not a huge savings, using the NAS solution to replace aging file servers would actually allow the agency to spend less money while making extraordinary advances in customer service.

Data Collection

Data was collected from internal helpdesk tickets to evaluate the frequency in which file servers have problems and how many offices have been affected during the evaluated time frame. This data is to help decide how much of a problem the agency has with its file servers. Data was also collected by interviewing technicians who work to resolve files server problems and documenting the time it takes to complete the steps of repairing or replacing a file server. This data is used to compare the results with the time and effort that would be needed to correct a problem with a NAS device to see if down time could be reduced for field staff if a NAS solution is used. Data was then collected from vendors who manufacture and/or sale files servers and NAS devices to perform a cost evaluation as well as to possibly understand the marketing trend of NAS devices. This data is used to decide if the agency can actually save money while taking advantage of the latest technology available. Finally, I contacted agency staff in remote offices to

get their feedback on experiences with the current file server system. This data was collected to determine if internal customers are complacent or dissatisfied with the service provided for file storage.

Data Analysis

To determine the frequency in which outages and other problems with file servers occur all helpdesk ticket records were downloaded to a spreadsheet and then all tickets pertaining to file servers were separated. There were 9,233 tickets in the database when I downloaded them. These tickets span from July of 2009 to December 2010, or approximately 1 ½ years. Of the 9,233 tickets there were only 150 tickets related to file server problems. This is only a little over 1.5 percent of all helpdesk calls and lower than I expected. File servers generate an average of 2.6 calls per month. However, considering the wide variety of problem calls we receive, the finding is still significant because the majority of helpdesk calls are for one person having a problem but when a file server is down it affects an entire office. Of the 150 file server tickets I found 48 of them resulted from a file server being inaccessible to anyone at the corresponding office. (There was actually 52 tickets but 3 of them were duplicate calls for the same outage.) Therefore, in the past 1 ½ years over 32 percent of helpdesk calls concerning file servers are due to a file servers being inaccessible. It appears that problems with file servers that are inaccessible are most frequently resolved by rebooting the server and then the server becomes accessible within a few minutes. (A deeper look into why a file servers become inaccessible but resolved by just rebooting is needed but not necessarily the goal of my data collection.) When rebooting does not fix an inaccessible file server it is then top priority to replace the down server. I found ten

helpdesk tickets that documented replacing down file servers. However, there are occasions where a file server is replaced and not documented with a helpdesk ticket so an exact number was not possible. There are technicians that begin work at 7:30 a.m. that will notice if a server is down and begin the process and notify the office as well. Also, there are times when the office that is down actually contacts a technician directly instead of calling helpdesk and again, a ticket is never created. Of the ten documented outages a total of seven of the tickets were from different offices where the remaining three tickets were from two of those offices having more than one documented outage. Interviewing four network technicians, two database administrators and documenting file server procedures helped to collect data that shows the time and resources used to correct file server problems. Normally an office calls the information technology helpdesk to report problems accessing file servers and a helpdesk ticket is created. Helpdesk staff try to resolve any simple issues by having the caller verify that the server's power cord is plugged in to an electrical outlet, the network cable is plugged into a network jack and making sure it's not simply powered off. If the issue needs more attention the helpdesk ticket is then routed electronically to a "Network Support" technician. Network technicians will attempt to access the server remotely and view error logs and error messages provided from the operating system as well as verify that all necessary software is in a "running" state. If the server is accessible and the problem cannot be determined within a few minutes then technicians reboot the server to try and restore file access to the office. As found in the helpdesk ticket data rebooting usually restores file access and the ticket is closed and normally not looked into anymore unless the server keeps having to be rebooted periodically. Servers that continue to have problems or cannot be fixed remotely are replaced as a high priority. Spare servers are preloaded with common software and are available at all times. A network technician must

connect a spare server to the agency's network and request a file restore from a Database Administrator. A Database administrator locates the latest backup of the server and restores the files to the new server. One year ago the backup files from these servers were only stored on magnetic tape and a restore could take a couple of hours. However, today the backup files are stored on disk drives which complete restores in minutes. Once verified that the new server is working and all files have been restored it is driven to the necessary location by a Hardware Service technician and put in place of the old server. Staff that are logged on to the network at the time must log off and back on to restore access to their files on the new server. It occurred to me that helpdesk tickets are documented and closed differently by each technician. Some technicians close the ticket after the file restore was successful and some will wait until the day after the server has been replaced to ensure the new server stayed working for 24 hours. Therefore, to get a true document on how long the process takes I went through the steps of preparing and restoring an actual server.

The following was tested and documented using the backed up files one of our largest offices in Greenville, S.C which is also approximately a two and a half hour drive from Columbia:

Action	Approximate time
1) Connect new server to mouse, keyboard & monitor & power up	2 minutes
2) Logon, name server, introduce server to network & reboot again	4 minutes
3) Have database administrator create and run restore process	20 minutes
4) Verify files have been restored	2 minutes
5) Power off server, disconnect wires & load on hardware van	5 minutes
6) Drive to location	2 hours, 30 minutes
7) Replace old server with new (connect mouse, monitor & keyboard)	3 minutes
8) Power up server and verify network connection	4 minutes
9) Have office staff log off and back on – verify file access	10 minutes
Approximate time to regain file access	**3 hours, 20 minutes**

Using 2 NAS devices that we currently own I tested switching from one NAS device to another by disconnecting the primary NAS and then changing the name and I.P. address of the backup NAS. The backup NAS was now the primary and the actions took approximately 20 minutes to complete.

1) Locate and disconnect network cable from primary NAS	1 minute
3) Remove DNS entry on network for primary NAS	2 minutes
3) Logon to Backup and change name & I.P. address	5 minutes

4) Reboot new primary NAS	2 minutes
4) (office staff would log off and log on & verify files)	10 minutes
Approximate time to regain file access	**20 minutes**

Therefore, if the Greenville office that I used as a server replacement test had a primary and backup NAS solution, file access for the office would have been achieved 3 hours sooner or 90% quicker. A new backup NAS can be shipped to the remote office with the configuration setup being completed remotely. The old primary NAS that went down can be shipped back to Columbia to be repaired, if possible, then recycled. In talking to network technicians I learned that there have been occasions where files are missing from a new and restored server because a server malfunctions late in the day before a backup of that days work is performed that night. Also, there was an incident where a server was replaced in an office that takes three hours to drive to and the wrong backup file was used to restore files. Nobody discovered the error until workers at the remote office complained. A file restore was then performed again but this time over the network from Columbia to the remote office using the correct backup file which ran several hours due to the slower network link. This resulted in workers in that office not having file access for almost forty-eight hours. The feeling seems mutual with all technicians that a better file access solution is needed.

Data was also collected from state contract vendors for NAS versus server price comparison. Seagate is one of the world's largest hard drive and storage solutions manufacturer and have been in business since the 1970's. It is important to have a reliable name brand to ensure quality and support. Therefore, I have chosen Seagate's " Blackarmor 420" NAS device to evaluate a NAS versus server cost-comparison. This unit comes with 2 hard drives that are

1-terabyte each and can hold up to four hard drives for future growth. However, having the two 1-terabyte drives will actually result in a little over 1-terabyte of storage space for files to be stored after setup is complete. The reason is that the unit would be configured to utilize a protocol known as "RAID level 5" which would merge the two drives together as one big drive and use an algorithm to write the data to the drives in such a way that if one of the hard drives ever fails then a new drive can be put in its place and the data from the failed drive can be recovered from the original drive that is still working by using its algorithm. The lowest quote for a Seagate Blackarmor 420 was $519.95 and advertises as being able to handle up to fifty computer connections, "B&H Photo". The five largest offices for the agency currently have an average of forty computers and the five smallest offices have an average of thirteen computers. The Blackarmor 420 is not currently on state contract but the quote was from vendor who does have state contract for items such as digital cameras and projectors. To compare costs of new file servers to that of a NAS device I used the S.C. Information Technology Management Office web site to access state contract vendors and their current contract prices. Following are quotes for low-end servers compatible to the existing file servers. All servers are quoted from S.C. state contracts under WSCA Solicitation Number: 5400001124. All servers quoted were based on a server with a single 1-terabyte hard drive and 2-gigabytes of system memory (RAM), comparable processors running a minimum speed of 2.4 gigahertz and a 3 year warranty.

Vendor	Model Server	Quote	State Contract Number
Howard Computers	Esteem I7408	$1,442.70	5000008958
Hewlett Packard	ProLiant ML330 G6	$1,571.84	5000008963
DELL	Poweredge T110	$1,625.55	5000008961
IBM	x3200 M3	$2,123.33	5000008965

I located purchase order number 06-12412 dated April 4, 2006 that was used to purchase 30 of the existing file servers and found the agency paid $1,630 for each server.

A software license for an operating system will be needed for each server but none are needed for a NAS device. Although the agency currently owns transferable licenses for these servers they are Windows Server 2003 licenses which is obviously outdated but usable. Windows Server 2008 enterprise license quotes for $1,861.97 from DELL using state contract number contract number: 4400000319 and quoted for $1,889.72 from CompuCom Systems under contract number: 4400000318. Adding the cost of an operating system license to the server cost puts the cheapest server at $3,279.40. To purchase two BlackArmor NAS devices would cost only $1,039.90. Cheaper, low-end NAS devices can be purchased for networks with five to ten computers and higher-end, more costly NAS devices can be purchased for networks with hundreds of computers. The BlackArmor 420 would be a mid-range NAS device.

Below is a comparison showing the cost of purchasing one file server versus purchasing two NAS devices for an office.

Quantity	System	Cost	Licensing Cost	Total cost
1	**Server**	**$1,442.70**	**$1,861.97***	**$3,304.67**
2	**NAS**	**$1,039.90**	**$0.00**	**$1,039.90**
				= $2,264.77 savings per office.
			Replacing the current 33 servers:	**= 74,737.50 savings for agency**

** The agency does have the choice of continuing to use Windows 2003 server which would reduce the total savings to $377.53 per office and total of $12,458.49 for the agency.*

To gain concept of marketing trends for NAS devices I searched the world wide web for information on the history and current state of NAS devices. NAS storage was first developed in the early 1980's but did not gain market popularity until the early 1990's. During the early 2000's more companies began manufacturing NAS and the amount of data they can hold continues to grow exponentially. Web site www.storagesearch.com lists one hundred and

seventy eight companies that manufacture NAS devices. It would be almost impossible to verify the companies were all still in business or will be in business much longer.

An article titled 'NAS Technology Is Ready For Prime Time" from 1999 by Computer Technology Review states the following:

> 'Network Attached Storage (NAS) is emerging as a powerful, proven technology for meeting an organization's unquenchable demand for storing data, regardless of its source on the network. Three factors are accelerating end user demand for NAS and for a new generation of storage appliance offerings:

*Cost benefit to IT.

*Administrative convenience.

*Network-based Unix and Microsoft NT integration.'

(Computer Technology Review, 1999, page 1).

Ten years later Gartner, Inc. reports:

> "Worldwide vendor revenue for the network-attached storage and unified storage market increased 4% in 2009 compared with 2008 to about $3.5 billion. The estimated pure NAS market grew 1.4% to $2.73 billion." (Gartner Inc., 2010, page 1).

The market for NAS devices continue to grow and based on market data the NAS solution is more than a trend but a solid foundation for file storage with several years of development.

Input from agency staff was collected as data to determine if the users of the current file servers are satisfied or not with the service provided. In general agency staff feel that the current file access provided is satisfactory and reliable until, of course, a server does have a problem.

Staff members reported losing files from server replacements and do not have much confidence that their files are being backed up properly to the state office each night. Staff that have lost files mostly stated they were missing old e-mails from e-mail archiving files and did not necessarily need the files but noticed they were missing. Staff are more concerned that they maintain access to the servers at the state office that contain the central data for client services. However, a staff member in one of the agency's work training centers that does business with private industry mentioned that they are now storing sales order templates for the SCEIS system and say losing access to the templates could temporarily halt business. When I explain the NAS backup/primary solution and the 90% faster recovery speed when a NAS device goes down to staff as compared to the current server method obviously staff agrees that would increase their level of satisfaction and confidence.

Implementation plan

In order to implement a NAS solution to replace the aging file servers in remote offices the purchase of two NAS devices for each office must be approved by administration. Upon approval, the hardware supervisor would purchase the devices and turn them over to the Network Support group for setup and configuration for each office which would be done at the remote office. This includes naming the devices, assigning I.P. addresses and choosing options such as setting the synchronization feature between primary and backup NAS devices. File access would then be terminated from the old file server while all files are copied from the server to the primary NAS device. Next, the synchronization from the primary to the backup NAS device would have to be verified to ensure it's working properly. Providing the primary NAS device is named the same name that the old file server, office staff would be able to log off and back to gain file access via the primary NAS. Targeting three offices per week should allow the project

to be completed in less than twelve weeks. Purchasing 66 NAS devices at the lowest quoted price to replace the current 33 file servers would be a total cost of $34,316.70. Of course, purchasing that many NAS devices with one purchase order I should be able to negotiate a better price to lower the total cost. Purchasing 33 new servers as well would warrant a price better than what I was quoted for purchasing one but to keep the data simple I based the cost projections on the price quotes from each vendor, quoted as if the purchase was for one server and the NAS purchase was for one device.

My biggest problem to overcome is that hard drive encryption is only available on higher-end NAS devices which is more power than is needed for the agency to efficiently provide storage for simple files. The agency works with sensitive data such as social security numbers and medical documents that must be protected from theft. NAS devices are so small that they are an easy theft target. However, given the technology for encryption on the higher-end NAS devices is already available it is foreseeable that lower-end NAS devices will provide disk encryption in the very near future. The BlackArmor 420 only offers encryption of the data while it is being transferred to and from a computer upon access but not while it is stored.

Evaluation Method

To further evaluate the NAS solution the agency will need to purchase two NAS devices for use by the Information Technology (I.T.) staff to store and access their files. There are currently 34 staff in the I.T. department which is comparable to one of the larger offices. Most I.T. staff constantly create, access and modify files all day. This would allow for maximum use of the primary NAS to test its ability to function properly and retrieve files in a timely manner. Testing the switch to the backup NAS device can easily be done by communicating and

scheduling the event with co-workers. To measure the results a comparison can be done where a file server is restored using the current method at the same time the scheduled test to switch to the backup NAS is performed. Any time differences can be measured and any glitches can be documented. Also, continuing to document the average frequency in which file servers become inaccessible and comparing it to how many times, if any, the test NAS device becomes inaccessible would show if the NAS devices are more reliable than traditional servers.

Summary and Recommendations

Based on data collected and the results of testing theories for replacing file servers with network attached storage (NAS) devices the South Carolina Vocational Rehabilitation Department can indeed gain advances in customer service and technology while lowering the cost of providing storage for the documents and various files that employees maintain at each office. Data shows that most remote offices experience brief file server outages that are resolved by rebooting servers while some offices have remained without file access for several hours or more while waiting on a new server to arrive. However, current file servers purchased five years ago will continue to fail as they age and grow obsolete. Therefore, a plan in place to replace these servers with a more reliable and cost effective solution is necessary to help the agency advance in the future. Current marketing and pricing shows that a redundant NAS solution can be achieved for less cost than a traditional server solution. Furthermore, this simple and cost effective solution will reduce down time for office staff when problems do occur. It is my recommendation that the agency continue to test using NAS devices for file storage and searching for the necessary encryption needs of the files stored on them.

References

NAS Technology Is Ready For Prime Time

Computer Technology Review, 1999 by Tim Williams, Sue Smith

http://findarticles.com/p/articles/mi_m0BRZ/is_8_19/ai_57603679/pg_2/?tag=content;col1

Market Share: Business Network-Attached Storage/Unified Storage, Worldwide, 2009,

Gartner Inc. http://www.gartner.com/DisplayDocument?id=1326621