Is Your Filer Safe? the Implementation Challenges in NAS as a File Server

Mr. Vikas T V
Student, 4th Sem, M.tech(CNE), Dept. of CSE
AIT Tumkur, India

Mr. Rakesh S
Asst. Professor, Dept of CSE
AIT Tumkur, India

***Abstract*— The focus on best practices to overcome defined challenges while consolidating of data across servers and LAN users in a Corporate Network. This paper will explore in detail the need for data consolidation, challenges in security. There is a continuous need for data consolidation across different servers and LAN users in corporate networks as on demand information access and sharing is critical to ensure informed decision. Thus organizations invest on central IP storage system (NAS) to ensure data consolidation and effective sharing. But there is a need for effective information security and data protection in these kind of consolidated storage infrastructure approach. Identify the challenges related to Security on a central network storage system i.e. NAS. The outcome of this paper can be used as a guideline document by the IT professionals in any Small scale and Enterprise organization as they prepare for effective central file server or NAS deployment and effective management.**

Keywords—SAN, NAS, DAS, File Server, Authentication, Access control, Backup

I. INTRODUCTION

In computing, a file server is a computer attached to a network that has the primary purpose of providing a location for shared disk access, i.e. shared storage of computer files (such as documents, sound files, photographs, movies, images, databases, etc.) that can be accessed by the workstations that are attached to the same computer network. The term server highlights the role of the machine in the client–server scheme, where the clients are the workstations using the storage. A file server is not intended to perform computational tasks, and does not run programs on behalf of its clients. It is designed primarily to enable the storage and retrieval of data while the computation is carried out by the workstations.

A file server may be dedicated or non-dedicated. A dedicated server is designed specifically for use as a file server, with workstations attached for reading and writing files. File servers may also be categorized by the method of access: Internet file servers are frequently accessed by File Transfer Protocol (FTP) or by HTTP (but are different from web servers that often provide dynamic web content in addition to static files). Servers on a LAN are usually accessed by SMB/CIFS protocol (Windows and UNIX-like) or NFS protocol (Unix-like systems).

II. ARCHITECTURES OF STORAGE SYSTEMS

A. *DAS (Direct Attach System)*

Having storage directly attached to the workstations and application servers makes management of this data intractable and an administration, compliance and maintenance nightmare. If more storage needs to be added, changes are to be made directly to the hardware where the applications are running, causing downtime. It also introduces data responsibility to the application administrators, which is not an optimal responsibility model. Furthermore, pockets of these direct attached storage cannot be used in a globally optimal manner, where storage space can be consolidated over lesser storage media. Finally, DAS introduces too much management overhead when tasks such as backups and compliance are involved. The below figure shows the architecture of DAS

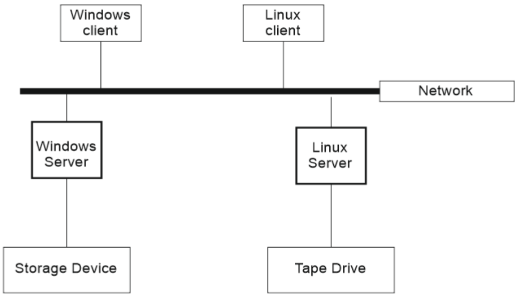


Fig 2.1 Direct Attached Storage

Backup and compliance software and hardware need reach all the way into the application and workstation infrastructure to be able to perform their tasks, which typically crosses IT boundaries in enterprises as well as introduces complexity due to the lack of consolidation for these tasks.

B. SAN (Storage Area Network)

In a SAN, the separation of the application servers and workstations from their storage medium is done at the lowest level possible in the communication stack, namely at the block IO level. Here, the raw storage commands to store and retrieve atoms of the storage (such as disk blocks) are extended from local bus access to a Fiber Channel or IP network based access (such as with iSCSI). Furthermore, SAN technologies offer a degree of virtualization such that the actual physical location and parameters of the disk are abstracted (virtualized) from the actual file system logic which runs on the application servers and workstations. However, the actual file system logic still does reside on the application servers and workstations and the file system is thus managed by them. The below figure shows the san architecture

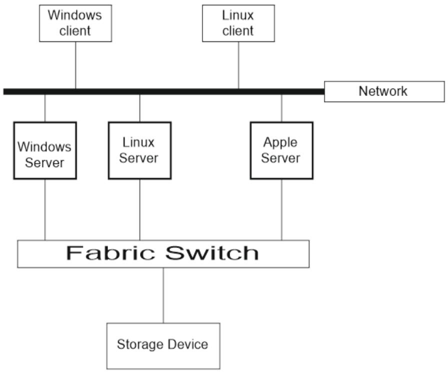


Fig 2.2 Storage Area Network

SAN allows storage administrators to consolidate storage and manage the data centrally, administering such tasks such as compliance, security, backup and capacity extension in one centralized location. However, the consolidation typically can extend as granular as a volume. Each volume is then managed by the storage client directly. While volumes can be virtualized, different volumes remain independent and somewhat restrict the flexibility for adds, moves and changes by the storage administrator without involving application server and workstation IT architects. The most common reason for using a SAN is where the application required direct control over the file system for reasons such as manageability and performance.

C. NAS (Network Attach Storage)

Network-attached storage (NAS) is file-level computer data storage[1] server connected to a computer network providing data access to a heterogeneous group of clients. NAS not only operates as a file server[2], but is specialized for this task either by its hardware, software, or configuration of those elements. NAS is often manufactured as a computer appliance a specialized computer built from the ground up for storing and serving files rather than simply a general purpose computer being used for the role. The below figure shows the architecture of NAS.

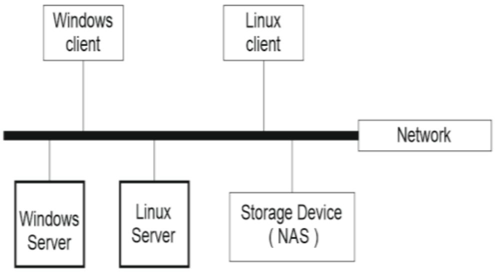


Fig 2.3 Network Attach Storage

As of 2010 NAS devices began gaining popularity as a convenient method of sharing files among multiple computers Potential benefits of dedicated network-attached storage, compared to general-purpose servers also serving files, include faster data access, easier administration, and simple configuration[3]. NAS systems are networked appliances which contain one or more hard drives, often arranged into logical, redundant storage containers or RAID. NAS uses file-based protocols such as NFS (popular on UNIX systems), SMB/CIFS (Server Message Block/Common Internet File System) (used with MS Windows systems), AFP (used with Apple Macintosh computers), or NCP (used with OES and Novell NetWare). NAS units rarely limit clients to a single protocol. Note that hard drives with "NAS" in their name are functionally similar to other drives but may have different firmware, vibration tolerance, or power dissipation to make them more suitable for use in RAID arrays, which are sometimes used in NAS implementations.

D. Evolution of NAS

In the early 1980s, the "Newcastle Connection" by Brian Randell and his colleagues at Newcastle University demonstrated and developed remote file access across a set of UNIX machines. Novell's NetWare server operating system and NCP protocol was released in 1983. Following the Newcastle Connection, Sun Microsystems' 1984 release of NFS allowed network servers to share their storage space with networked clients. 3Com and Microsoft would develop the LAN Manager Software and protocol to further this new market. 3Com's 3Server and 3+Share software was the first purpose-built server (including proprietary hardware, software, and multiple disks) for open systems servers.

Inspired by the success of file servers from Novell, IBM, and Sun, several firms developed dedicated file servers. While 3Com was among the first firms to build a dedicated NAS for desktop operating systems, Auspex Systems was one of the first to develop a dedicated NFS server for use in the UNIX market. A group of Auspex engineers split away in the early 1990s to create the integrated NetApp filer, which supported both the Windows CIFS and the UNIX NFS protocols, and had superior scalability and ease of deployment. This started the market for proprietary NAS devices now led by NetApp and EMC Celerra.

Starting in the early 2000s, a series of startups emerged offering alternative solutions to single filer solutions in the form of clustered NAS – Spinnaker Networks (acquired by NetApp in February 2004), Exanet (acquired by Dell in February 2010), Gluster (acquired by RedHat in 2011), ONStor (acquired by LSI in 2009), IBRIX (acquired by HP), Isilon, (Comanter), (acquired by EMC - November 2010), PolyServe (acquired by HP in 2007), and Panasas, to name a few. In 2009, NAS vendors (notably CTERA Networks and NETGEAR) began to introduce online backup solutions integrated in their NAS appliances, for online disaster recovery.

III. Challenges In NAS As a Fileservers

NAS challenges the traditional file server approach by creating systems designed specifically for data storage. Instead of starting with a general-purpose computer and configuring or removing features from that base, NAS designs begin with the bare-bones components necessary to support file transfers and add features "from the bottom up." Like traditional file servers, NAS follows a client/server design. A single hardware device, often called the NAS box or NAS head, acts as the interface between the NAS and network clients. These NAS devices require no monitor, keyboard or mouse. They generally run an embedded operating system rather than a full-featured NOS. One or more disk (and possibly tape) drives can be attached to many NAS systems to increase total capacity. Clients always connect to the NAS head, however, rather than to the individual storage devices. Clients generally access a NAS over an Ethernet connection. The NAS appears on the network as a single "node" that is the IP address of the head device. A NAS can store any data that appears in the form of files, such as email boxes, Web content, remote system backups, and so on. Overall, the uses of a NAS parallel those of traditional file servers. The challenges in central IP storage as a file servers are Performance, security, scalability, capacity etc... Over all of this this paper gives an approach for the security challenges.

IV. SECURITY CHALLENGES

Security challenges includes Authentication, Access controls, Data Protection.

A. *Authentication*

Authentication is a process of validating the user for the shares created in the NAS i.e. storage to stores and access the files from the NAS over network.

B. *Access controls*

Access control are the permissions to the shares created in the NAS to share the files in it. By creating the groups and the users we can give the permissions for that share to the groups or to the particular users whom are going to use that share.

C. *Data protection*

Data protection is a process of protecting the data which are present in the storage. Data loss may occur due to file system corruption or by the disk failure or accidental or malicious deletion or site or server crash or by any natural disasters etc. for these reasons we need to protect the data over loss. There are too many techniques to protect the data they are Snapshot, RAID, Backup and archive, replication. Snapshot will ensure instart recovery or roll back to an active file system. RAID ensures Redundancy against disk failures. Replication is the technique used to maintain off-site online copies of data. Backup is a process of copying multiple versions of live data on the defined target media. If we take backup using disk then it is D2D, if we use Tape then it is D2T. Backup is the common method of data protection. There are 3 types of backup they are Full back up: Complete copy of data selection to target with no dependency, Incremental: Backup data selection with reference to previous backup either full are incremental, Differential: backup data selection with reference to previous full backup.

V. TECHNICAL SPECIFICATIONS

Sl. NO.	Backup server	Client system	Tape system
1	**OS:** Windows Server 2008 R2 Standard	**OS:** Windows vista	**Drive Technology:** LTO
2	**Hostname:** Backup Server	**Hostname:** Development_Section	**Physical drive:** LTO-3
3	**IP Address:** 192.168.0.X	**IP Address:** 192.168.0.X	**No. of tapes slot:** 08 nos
4	**Backup Application:** Netvault Server Edn. Version 9.2	**Backup Application:** Netvault CLient Edn. Version 9.2	**Interface:** SCSI MD68 pin
5	**HBA:** SCSI HBA for tape system Connect		**Interconnect:** External SCSI

VI . REQUIREMENTS

1) *Hardware*
   - *Backup server*
   - *Tape system (secondary storage),*
   - *Client*
   - *Network switch*
2) *Software*
   - *Netvault server edition,*
   - *Netvault client edition,*
   - *Windows Server 2008 R2 Standard*
   - *Linux OS.*

VII. LOGICAL STEPS FOR SETUP

A. At Backup Server

- Assign IP address and connect to network
- Connect and configure the external tape system
- Install and configure backup software server edition.
- Discover the tape system and management
- Label the data tapes for backup and data archive storage

B. At Backup Client

- Assign IP address and connect to network
- Install and configure backup software client edition.
- Understand the data partitions and backup requirements
- Establish network connection with backup server

C. Add Backup client to Server

- Discover the backup client across network
- Add to the client management for data backup approach.

The below figure shows the logical representation of the backup server to client

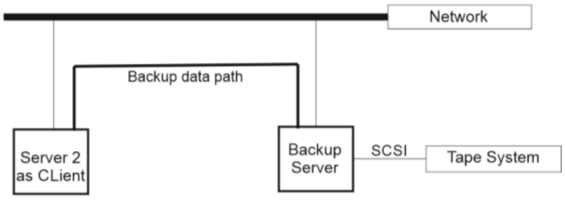
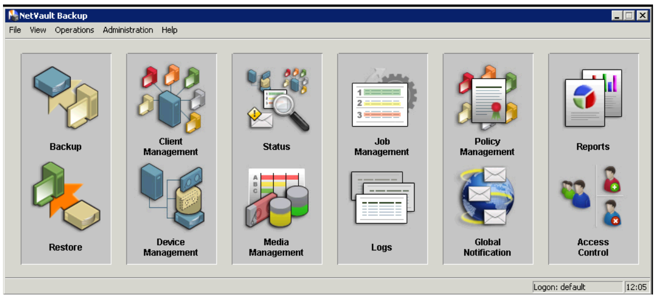


Figure 7.1 logical representation

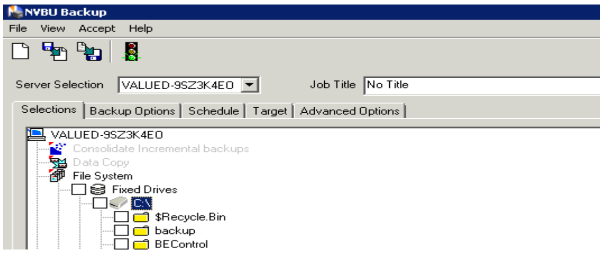
VIII. IMPLEMENTATION AND FIGURES

The below figure shows the Netvault Server edition which runs on the backup server.



A. Back up process

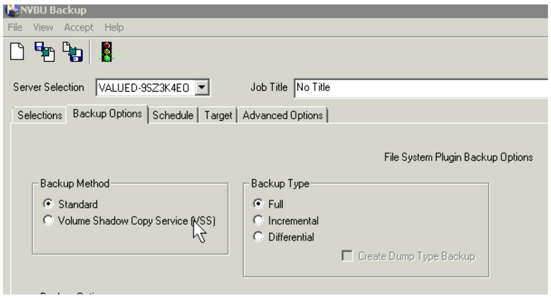
Click on the device management and click on the add menu then click on add library and select the tape library. Click on the client management and add the backup client.


NVBU Backup
File View Accept Help
Selections | Backup Options | Schedule | Target | Advanced Options

Server Selection VALUED-9SZ3K4EO Job Title No Title

VALUED-9SZ3K4EO
Consolidate Incremental backups
Data Copy
File System
□ Fixed Drives
□ C:\
□ $Recycle.Bin
□ backup
□ BEControl

Click on the backup in the netvault IDE. Select the backup client and select the data to be backup. Click on the Backup option.select Backup method as standard. And for taking backup first time select the full as backup type as shown in figure below, for further backup select the appropriate bacup types either full or incremental or diffrential

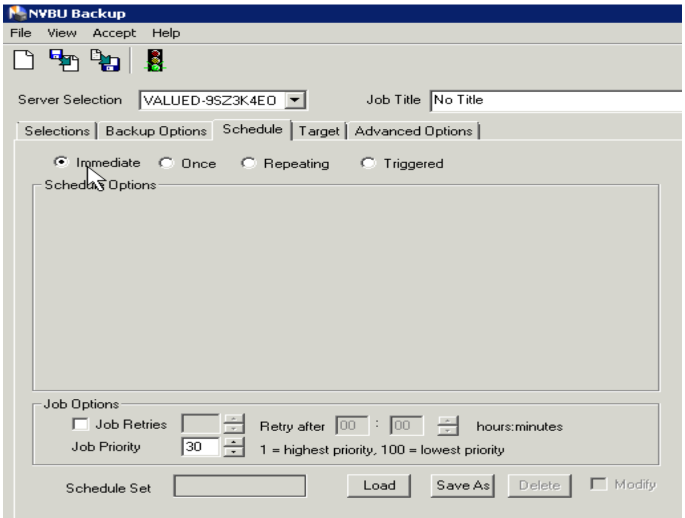

NVBU Backup
File View Accept Help
Selections | Backup Options | Schedule | Target | Advanced Options
File System Plugin Backup Options

Server Selection VALUED-9SZ3K4EO Job Title No Title

Backup Method
● Standard
○ Volume Shadow Copy Service (VSS)

Backup Type
● Full
○ Incremental
○ Differential
□ Create Dump Type Backup

Click on the Schedule tab, It consists of 4 option immediate: to take backup immediate, once: to take the backup only once, repeating: to take the back up repeatedly on the particular day or time or the day of the week or day of the month etc, Triggered: backup has to be taken when the backup is triggered


NVBU Backup
File View Accept Help
Selections | Backup Options | Schedule | Target | Advanced Options
Load
Save As
Delete

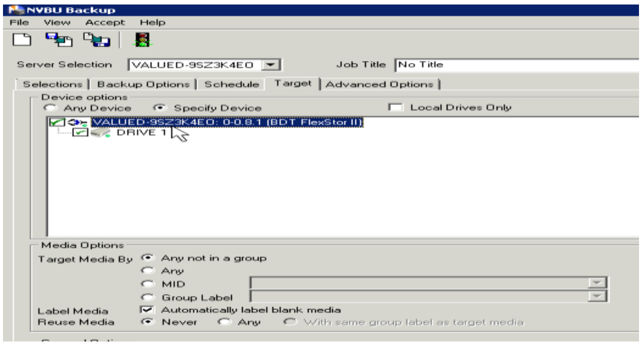
Server Selection VALUED-9SZ3K4EO Job Title No Title

● Immediate ○ Once ○ Repeating ○ Triggered

Schedule Options

Job Options
□ Job Retries Retry after 00 : 00 hours:minutes
Job Priority 30 1 = highest priority, 100 = lowest priority
Schedule Set □ Modify

Click on the target tab and select the target device connected to the backup server and even we can select the particular tape which is inserted into the tapesystem by selecting the MID in the target media by option.

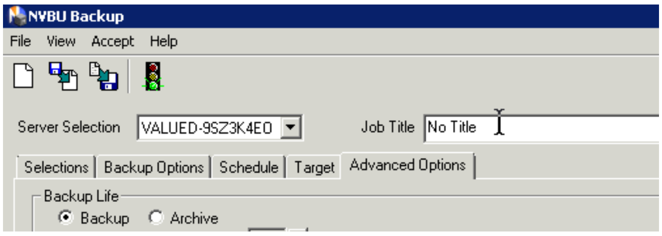

NVBU Backup
File View Accept Help
Selections | Backup Options | Schedule | Target | Advanced Options

Server Selection VALUED-9SZ3K4EO Job Title No Title

Device options
○ Any Device ● Specify Device □ Local Drives Only
☑ VALUED-9SZ3K4EO: 0-0.8.1 (BDT FlexStor II)
☑ DRIVE 1

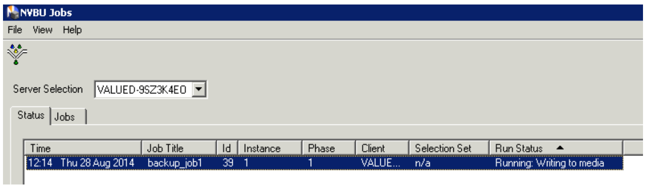
Media Options
Target Media By ● Any not in a group
○ Any
○ MID
○ Group Label
Label Media ☑ Automatically label blank media
Reuse Media ● Never ○ Any ○ With same group label as target media

Then click on the advance tab select backup or archive which ever required. Where backup selected then the backup will be write to media where we can re-write on it. If we select archive then the tape becomes WORM i.e. Write once Read More, so that the no media can be write on that media. After that name the jab title and save it and submit it.



Server Selection: VALUED-9SZ3K4EO
Job Title: No Title
Backup Life: ● Backup ○ Archive

After submitting the backup of the data can be writing to the media we can see that in the job management option

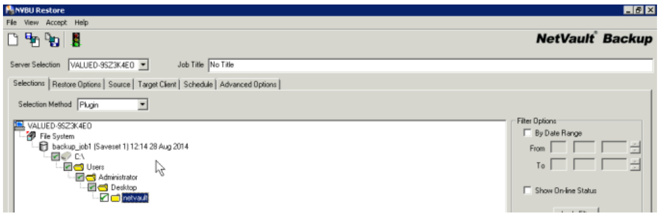


Server Selection: VALUED-9SZ3K4EO

Time	Job Title	Id	Instance	Phase	Client	Selection Set	Run Status
12:14 Thu 28 Aug 2014	backup_job1	39	1	1	VALUE...	n/a	Running: Writing to media

B. Restore Process

Click on the restore button to restore the backup took if in case of any data loss. Select the selection tab and select the files to be restored

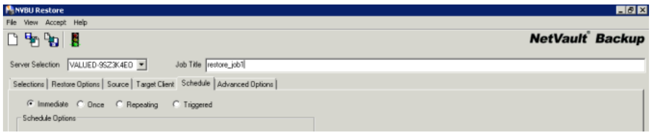


Server Selection: VALUED-9SZ3K4EO
Job Title: No Title
Selection Method: Plugin

VALUED-9SZ3K4EO
File System
backup_job1 (Saveset 1) 12:14 28 Aug 2014
☑ C:\
☑ Users
☑ Administrator
☑ Desktop
☑ netvault

□ By Date Range
□ Show On-line Status

Click on the source tab if there are more than one backup devices and select the appropriate backup device. Click on the target client tab and select the target system on which the restorsation of files has to be done.Click on the Schedule tab, It consists of 4 option Immediate: to restore immediate, Once: to restore only once, Repeating: to restore repeatedly on the particular day or time or the day of the week or day of the month etc, Triggered: restore has to be do when it is triggered. Name the job in the job title space and save it and submitt the job.



Server Selection: VALUED-9SZ3K4EO
Job Title: restore_job1
● Immediate ○ Once ○ Repeating ○ Triggered

After submitting the restore of the data can be writing to the target system. we can see that in the job management option.

IX . CONCLUSION

File servers are so important in current IT environments that they have developed into an independent product group in recent years. Network attach system is the name for pre-configured file servers. They consists of one or more internal servers, preconfigured disk capacity and usually stripped down or separate or special operating system. In Corporate network there is a more requirement of data consolidation. Usually in corporate may consists of many servers LAN and different operating system. So making the data consolidation is required across those different heterogeneous environment. This paper will explore in detail the challenges like Security issue like Authentication, Access controls, Data protection and recovery. The outcome of this paper can be used as a guideline document by the IT professionals in any Small scale and Enterprise organization as they prepare for effective central file server or NAS deployment and effective management.

REFERENCES

[1] http://en.wikipedia.org/wiki/Computer_data_storage
[2] http://en.wikipedia.org/wiki/File_server
[3] InfoStor. NAS Advantages: A VARs View, April 01, 1998. By Ron Levine
[4] http://en.wikipedia.org/wiki/Storage_area_network.
[5] http://en.wikipedia.org/wiki/File_server.
[6] http://en.wikipedia.org/wiki/Network-attached_storage.
[7] Information Storage Management, Second Edition, EMC Education Services

ABOUT AUTHORS

Mr.Vikas.T.V, presently pursuing M.Tech in Computer Network and Engineering, in Akshaya Institute of Technology, Tumkur, India. Affiliated to VTU, Belguam, India.

Mr.Rakesh.S, Received the M.Tech In Computer Science and Engineering. Presently he is working as Assistant Professor, Dept. of CSE at Akshaya Institute of Technology, Tumkur,India.