ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 8, Issue 3, pp: (242-245), Month: July - September 2020, Available at: www.researchpublish.com

Toward a Secured and Optimized Infrastructure for File Sharing

Moyed Ahmed Alsadiq

Saudi Arabia

***Abstract*: File sharing is an integral part of computing infrastructure and at the same time has many known vulnerabilities that can be exploited by attackers. Enforcing highest security standards can reduce risks related to file share infrastructure through reducing risks probabilities and impact. To build a notable file share infrastructure, multiple best practices can be implemented to ensure highly available, secure, optimized, auditable and customer-oriented infrastructure.**

***Keywords*: Network Attached Storage (NAS), Antivirus Scanning, Microsoft Distributed File System (DFS) and Integrated Solutions.**

1. INTRODUCTION

The best practices to create a secured and optimized File Share should consider many elements and all of them should be combined with each other to provide the stability of data access and the required protection for organization data.

In IT market, there are many technologies to host the file shares and each one has its own features and the proper infrastructure should be selected to meet organization needs.

In this article, I will select **Network-attached storage (NAS)** as the hosting infrastructure for the File Shares that it is the best to accommodate large organization requirements.

The article will start by describing NAS and its benefits followed by best practices to secure access, enhance virus scanning, deploy high availability solutions, optimize resources and enforce accountability.

Network Attached Storage

Network-attached storage (NAS) is dedicated file storage that enables a huge number of users and client devices to retrieve data from centralized disk capacity. Users on a local area network (LAN) access the shared storage via a standard Ethernet connection. Each NAS resides on the LAN as an independent network node, defined by its own unique Internet Protocol (IP) address.

Below are some benefits of network-attached storage,

- The NAS storages can host mixed of file shares (Windows & Linux) as NAS support CIFS and NFS protocols
- The NAS storages are accessible from anywhere from your network or outside the network
- The NAS storages are very stable environment for hosting file shares, the operating system update is online for Linux without interruption and within seconds for Windows
- The NAS storages are easy to setup and manage
- The NAS storages can provide large capacity of space and excellent performance
- The NAS storages provide high availability of the data access as NAS provide the data replication and easy restore the data from the backup
- The prices for the NAS storages are reasonable

2. MANAGING ACCOUNTS & DATA ACCESS

For better managing and securing the NAS storage to host File Shares, the built-in local account on each storage must be renamed as well as to use domain accounts to manage and configure the NAS storage and data hosted on it. It is a recommended to change these domain accounts' passwords on each two months with complex password with a mixed of 32 characters and must be saved encrypted in a secured repository.

Also, the responsibilities for managing the storages should be distributed between IT administrators such as one IT administrator to configure the storage and create the shares and another IT administrator to manage the shares and backup the shares. This will enforce segregation of duties principle and hence to protect the availability of the data and avoid any intended or unintended human errors.

Also, to secure the data access on each file share, the file share that has confidential data must be encrypted and the Everyone Group or Domain Users Group should not be used or added on the file share. A specific security groups must be used to manage the NTFS & Share Permissions

File Protection Using Virus Scanning

To increase the security and to protect data, the NAS storages must be integrated with another infrastructure managed by a different IT team to deploy **antivirus Scanning** activities

On each NAS storage, the antivirus servers must be connected to scan all data (in and out) and no one can save or open a files without scanning them.

To stabilize the scanning of antivirus servers, the antivirus servers should be mixed between virtual servers and physical servers as in case the virtual environment is down the physical servers will continue scanning the data to be available for the users.

The antivirus servers must be configured to rescan the files after any update for the antivirus software and the NAS storage should be configured with no access for the files in case all antivirus servers are down.

Microsoft Distributed File System (DFS)

After creating the File Share, it is highly recommended to integrate the file shares on the NAS storages with **Microsoft Distributed File System (DFS),** to enable the users to access the file share easily as the users will use user-friendly naming convention instead of using the server name and share name.

Distributed File System or DFS is the process to logically group a huge number of shares saved on multiple servers and to transparently link shares into a single hierarchical namespace. This is organized in a treelike structure. DFS supports multiple modes including both stand-alone and domain-based DFS services.

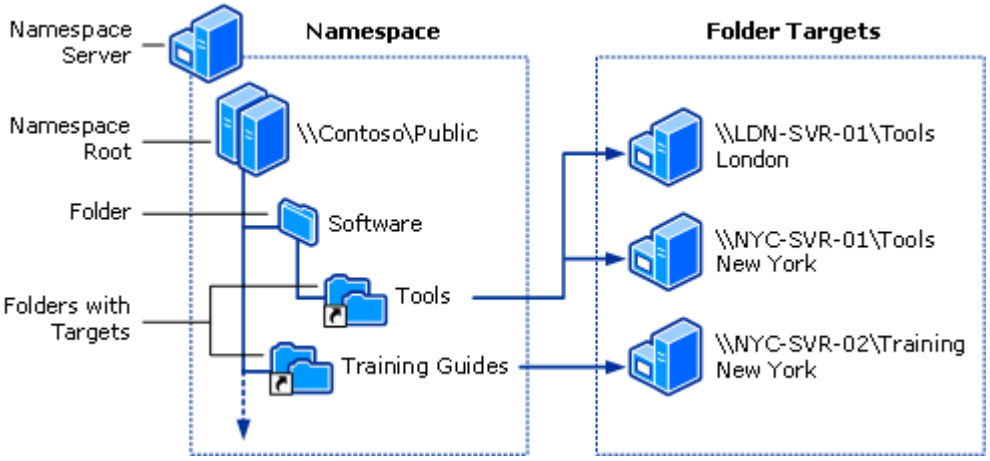
The DFS link should be configured for all users to be available for them once they login to their domain as they can see the DFS link mapped to any computer they use within the domain.

Below is a list of benefits for DFS.

- No need to change the link for the file share in case the server is changed as the DFS link can be redirected to the new target
- Easy for the users to access all shares as no need for the users to know the server name that hosting the data
- Fault tolerance (shares can be replicated, so if one server is down the users can access the shares from another server)
- Work load management (DFS allows administrators to distribute shared folders and workloads across several servers for more efficient network and server resources use)

To know more about the DFS, I will describe the components of the DFS

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 8, Issue 3, pp: (242-245), Month: July - September 2020, Available at: www.researchpublish.com



DFS namespace components (Image courtesy of Microsoft)

- **Namespace server** is the server that hosts the namespace, this server can be a member server or a domain controller.
- **Namespace root** is the starting point of the namespace and it is part of the domain. The namespace start with the Domain Name and this namespace will be replicated on all Active Directory Servers.
- **Folder t**here are two types of folders in the DFS namespace – folders without targets and folders with targets. The folders without targets are simply for the organization of the structure. Folders with targets link to servers that host the data
- **Folder targets** is the actual place of the data, this contains the server name and the share name and this should be associated with the folder in the namespace

3. DATA AVAILABILITY & RESOURCES OPTIMIZATION

To stabilize the availability of data access for the users, you must have a clear backup plan to back up the data on each NAS storage and DFS links as well.

Also, to minimize the down time for the data access especially for the critical shares, you should replicate the data on each NAS storage to another site as in case the primary site is down.

It is highly recommended that you enable the **Overprovisioning** and **Deduplication** on each share to save disk space

Overprovisioning is the process of creating the file share on the NAS storage with smaller size while the users view it with larger size, as an example you create the share with 400 GB while the users view the share size as 1000 GB, this will lead for saving a lot of spaces on each storage as many users request large size of shares and they do not use the requested space.

Data Deduplication is a process that eliminates many copies of the same file saved on the NAS storage and direct the users to one copy of the file, by enabling this process you will save a lot of spaces on the NAS storages.

More Solutions to Secure and Optimize

A log collection tool must be integrated to each NAS storage to collect the security events from each file share and save these events in different infrastructure and to be manage by different IT Team.

This tool will be used in case of any suspected violation such as deleting data or changes in the permissions for files or folders and it can be used to generate different types of reports related to data access. The Audit Log must be enabled on each File Share to enable this tool to collect the data from the NAS storage for each share.

A reporting tool must be available to generate different types of reports about the utilized space and remaining space on the NAS storages to make a clear plan of the required hardware of NAS storages, also to generate reports about the existing data such as file types, file sizes, duplications files, the life of files, to know the unused files and other reports.

A data migration tool must be available to migrate the data between NAS storages as well as between NAS storages, SAN or the user's computers as well. The tool should migrate the folders and files with their permissions, even the open files and it is must be fast enough to save time in the data migration.

4. CONCLUSION

The best practices to create secured and optimized File Share should consider many elements and all of them should be combined with each other to provide the stability of data access and the required protection for organization data

REFERENCES

[1] NetApp Website https://library.netapp.com/ecmdocs/ECMP1366831/html/GUID-8713AE4F-9454-4D04-985D-E4390CA9FCD2.html

[2] Microsoft Website https://docs.microsoft.com/en-us/windows-server/storage/dfs-namespaces/dfs-overview

[3] Dell Website https://www.delltechnologies.com/ar-sa/glossary/network-attached-storage.htm