BEST PRACTICES GUIDE

Nimble Storage Best Practices for Microsoft Windows File Sharing

Table of Contents

3 Introduction

4 Benefits of Native Windows File Sharing Functionality

4 SMB

4 Distributed File System (including DFS-R)

4 File Classification Infrastructure (FCI)

5 File Server Resource Management Tools (FRSM)

5 Native Disk Management Utility

5 Shadow Copies (previous versions) of Shared Folders

5 Offline Folders / Files and Folder Redirection

6 Security

6 Additional Microsoft File Services Features

7 Configuring Nimble Volumes

7 Volume Creation

10 Configuring Windows with Nimble Storage

10 Configure Roles and Features

10 Configure Failover Clustering

11 Connect Volume

11 Test the Volume

11 Configure Clustered File Sharing

11 Enable Continuous Availability

13 Data Protection

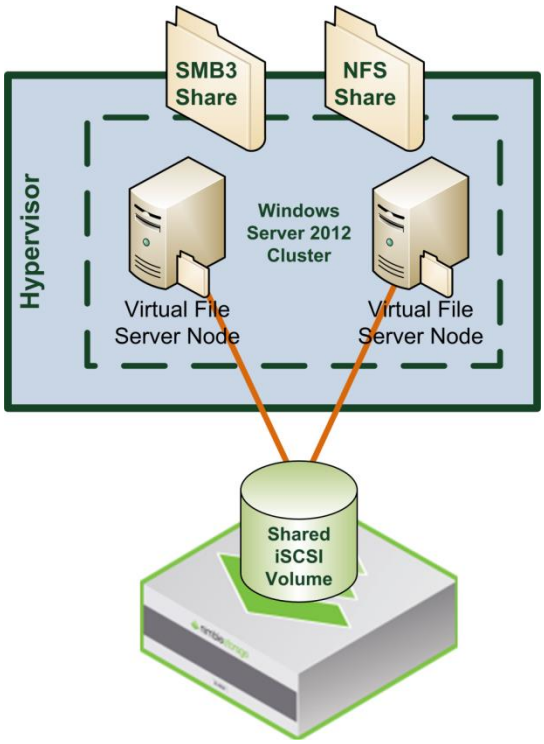
14 Data Restoration

14 Summary

Introduction

Nimble Storage provides a revolutionary block-level storage platform that simultaneously improves storage performance and capacity. Block-level storage is perfect for application servers; however users typically share their work using File-level storage or Network Attached Storage (NAS). When considering NAS solutions, customers can either choose specialized NAS solutions or leverage more general purpose operating systems such as Microsoft Windows or Linux.

This best practices guide provides a multi-protocol file sharing NAS solution for both Windows and Linux systems that still leverages the power of Nimble Storage performance and scalability. This document leverages Windows Server 2012 native enterprise file services role to provide the NAS functionality with the most complete coverage for the SMB/CIFS and NFS protocols that are most common in data center environments. Microsoft has a tremendous number of capabilities that have been requested over the years by IT organizations. Such organizations can leverage the extensive file-serving and data management capabilities found natively in Microsoft Windows Servers while leveraging the economics and performance of converged storage using Nimble CS Array technology.



This solution also leverages Microsoft Failover Clustering features to provide high availability in the event of a Windows operating system failure. Windows Server 2012 Failover Clusters require shared storage accessible to each participating node in the cluster. The storage must also permit the use of SCSI-3 Reservation Protocol to ensure that only one node of the cluster controls the storage at a time to avoid conflicts. This means that the virtual cluster nodes must avoid using virtual disks for the data storage and connect directly to the Nimble Storage array as shown in the architectural diagram.

Benefits of Native Windows File Sharing Functionality

SMB

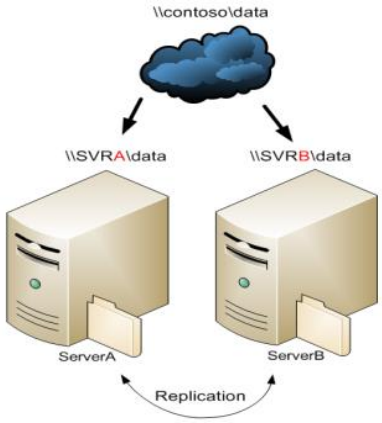
SMB 3.0 is the new Microsoft CIFS implementation. It's an improved version of the Server Message Block protocol that ships with Windows Server 2012 and Windows 8. SMB 3.0 further enhances the SMB protocol offering:

- SMB Transparent Failover
- SMB Scale Out
- SMB Multichannel
- SMB Direct
- SMB Encryption
- VSS for SMB File Shares
- SMB Directory Leasing
- SMB PowerShell

Many non-Microsoft CIFS implementations do not support CIFS SMB 3.0 and the ones which do have weak interoperability and integration. This can compromise the performance and overall stability of your CIFS file serving environment.

(DFS) Distributed File System (including DFS-R)

DFS simplifies the management of multiple file servers by aggregating file shares located in different file servers under a single logical folder. DFS provides location transparency and redundancy to improve data availability during failure or heavy load scenarios by allowing shares in multiple different locations to be logically grouped under one folder. DFS-R offers file replication capabilities that support remote differential compression to minimize network bandwidth.



Ensure the non-Microsoft CIFS implementation you're evaluating has full support and integration for DFS and DFS-R. DFS-R is Microsoft proprietary and it is not available in non-Microsoft implementations.

File Classification Infrastructure (FCI)

Windows Server File Classification Infrastructure (FCI) provides insight into your data to help you manage your file data more effectively, reduce costs, and mitigate risks by providing a built-in

solution for file classification that allows administrators to automate manual processes with predefined policies based on the business value of the data.

🚫**Non-Microsoft CIFS implementations cannot integrate with FCI functionality.**

File Server Resource Management Tools (FSRM)

Windows Servers also includes a set of tools that offer quota, file screen and report management. These tools can generate a variety of reports on utilized storage, such as the number of duplicate files that are stored and a report of large files. There is also support quota management and real-time file screening to halt the storage of illegal content.

🚫**The FSRM tools are proprietary to Microsoft file servers and thus are not available on non-Microsoft CIFS implementations.**

Native Disk Management Utility

The Disk Management utility is used for managing hard disks and the volumes or partitions that they contain. With Disk Management, you can initialize *Nimble CSArray disks* and format volumes with the FAT, FAT32, or NTFS file systems. Disk Management enables you to perform most disk-related tasks without restarting the system or interrupting users.

Shadow Copies (previous versions) of Shared Folders

Shadow Copies of Shared Folders provides point-in-time copies of files that are located on shared file server resources that are attached to the *Nimble CSArray*. With Shadow Copies of Shared Folders, users can view shared files and folders as they existed at points of time in the past. Accessing previous versions of files, or shadow copies, is useful because users can:

- Recover files that were accidentally deleted.
- Recover from accidentally overwriting a file.
- Compare versions of a file while working.

🚫**Ensure the non-Microsoft CIFS implementation you're evaluating has full support and integration with Microsoft's Shadow Copies.**

Offline Folders/Files and Folder Redirection

Windows offline folder and file redirection provides a cached online mode, whereby read operations go to the local cache and write operations go to the cache and the server endpoint. Other changes include better handling of per-user encryption and synchronization, support for differential transfers of large files such as PSTs, and seamless offline and online transitions.

🚫**Ensure the non-Microsoft CIFS implementation you're evaluating has full support and integration with Microsoft's Offline Folders/Files and Folder Redirection.**

Security

NTFS Folder/File Security: Windows supports all the NTFS security types for files/folders (ACLs, DACLs, SACLs) which are necessary for user / group permissions as well as file auditing purposes.

🚫**Non-MS CIFS implementations may not support the full spectrum of NTFS ACLs, DACLs and SACLs. This can often lead to incompatibilities with applications and security vulnerabilities within your organization.**

Active Directory Domain Support: This is the primary and critical means most organizations control and enforce user authentication and authorization within their file serving environments.

🚫**Failure to have full and proper AD integration and support of all domain types (W2K, W2K3, W2K8, native-mode, mixed mode, etc.) can cause security, integration and support headaches.**

Additional Microsoft File Services Features

Many non-Microsoft 3rd party NAS CIFS implementations do not offer the same, "exact" level of specific integration and interoperability when compared to Microsoft. Often times these specific "under-the-cover" details are overlooked at first, but can become major issues later on. These incompatibilities and integration gaps are viewed by Microsoft as non-supported and non-qualified configurations, leaving the organization in a precarious situation.

🚫**Some of the more common integration and feature gaps found in 3rd party non-Microsoft CIFS implementations that should be tested and verified include:**

- Support for Microsoft reparse points
- Support for Alternate Data Streams (aka. named streams)
- Support for CIFS Opportunistic locking (better performance.)
- Support for NTFS ChangeNotify operations
- Support for Roaming User Profiles
- Support for NTFS Extended Attributes
- Support for NTFS Sparse Files
- Support for Symbolic links via SMB 2.1
- Support for full use of Local Users and Local Groups
- Support for Microsoft Encryption

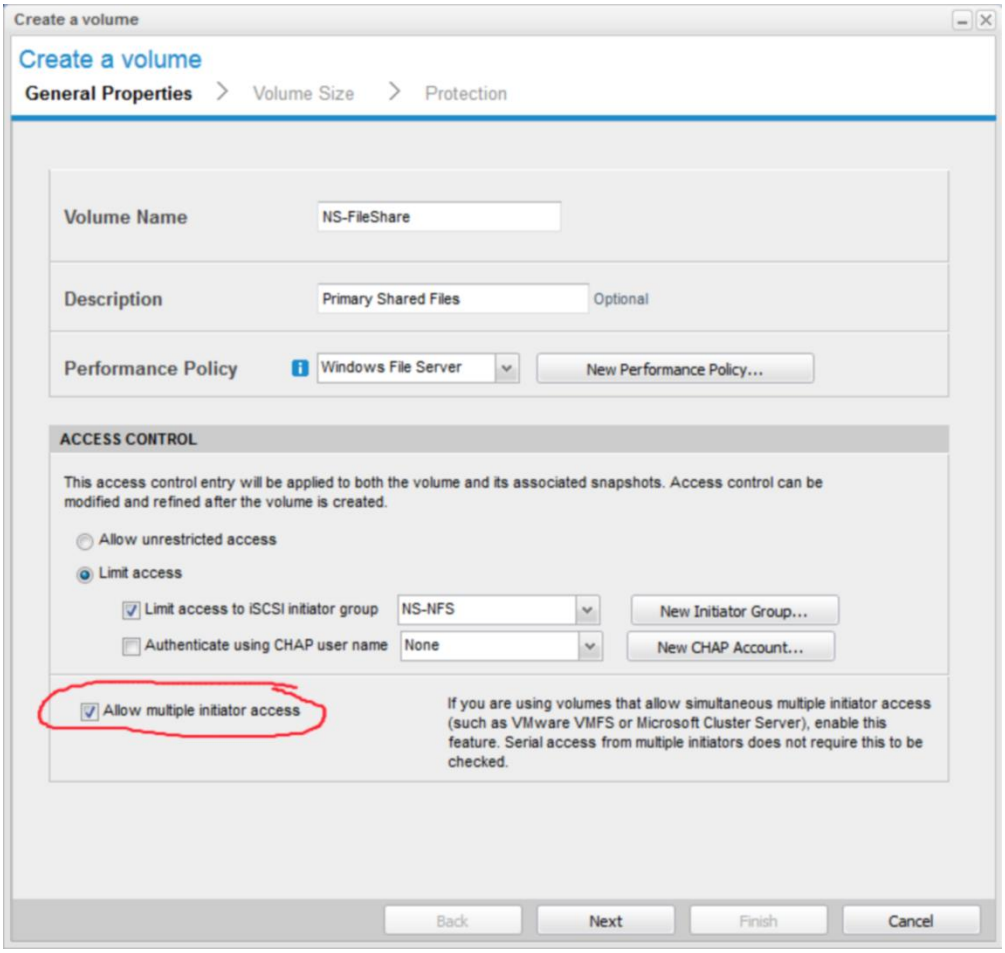
- MMC support for user, group and directory quotas
- Support for all security levels for CIFS connections (hisec.inf)
- Support for Secure LDAP (LDAP over SSL)
- Server & client side SMB signing
- Support for Access Based Enumeration (ABE)
- Support for Microsoft Group Policy Objects
- Support for LDAP signing and sealing
- Support for Local account policies
- Support for file System Access & Logon Auditing via EventViewer
- On-board, on-access and on-demand Antivirus protection
- Support for Microsoft WebDAV
- Support for IPv6 with CIFS
- Support for Granular file blocking
- MMC Support for Local Users/groups

Configuring Nimble Volumes

Volume Creation

Login to your Nimble Storage array, select Manage -> Volumes, then click the “New Volume” button. Enter a Name that will be used to form the iSCSI target volume name and optionally a description. Next select the Performance Policy “Windows File Server” which will help the Nimble array to better understand the characteristics of the data stored on the volume. The Windows File Server Performance Policy uses a block size of 4 KB and enables both Compression and Caching which is suitable for most file server applications.

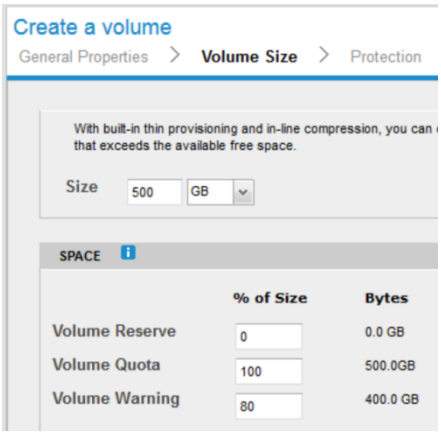
However, if your file server will hold a majority of data that is already compressed, such as a video file share, then you should create a customer Performance Policy that disables Compression and possibly Caching if there will not be a likelihood of random access patterns. If you are at all unsure about using the custom Performance Policy features for your data then use the “Windows File Server” performance profile or contact Nimble Storage Technical Support for additional guidance.



You should limit access to the volume at a minimum by using iSCSI Initiator Groups. You can create a new Initiator Group and add each cluster server's IQN that is available in the Microsoft iSCSI Initiator tool on each clustered server. You should avoid using the cluster node's IP address which can change and is also unique to a single NIC port, which would require you to add every potential server data IP versus using the single IQN per server.

Another key consideration for sharing the iSCSI volume between Windows 2012 cluster nodes is to enable "Allow multiple initiator access". This enables support for SCSI-3 Reservation Protocol which is required by clustered servers to arbitrate cluster resource ownership.

The next step is to define the size and optionally the space characteristics of the volume. Nimble Storage provides thin provisioning of volumes by default which means that storage is not immediately reserved until it is actually used. This feature can allow you to overprovision a storage array but may prove beneficial to reduce manual effort to grow data volumes in the future or in environments where the full data store is seldom used such as development and testing environments. You can pre-allocate storage space ahead of time by using the Volume Reserve function.



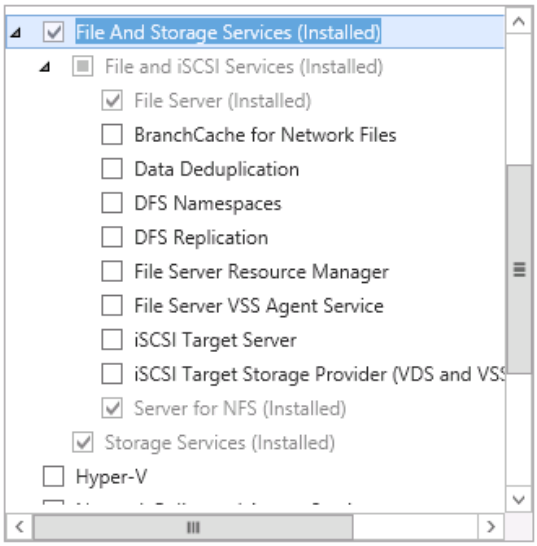
Data protection will be covered later in this document with more detail, for now you can select the radio button marked “None”. We will fully configure the clustered file shares and then come back to enable automated snapshot protection.

Configuring Windows with Nimble Storage

This section assumes that you have two newly installed Windows 2012 Server edition machines, either virtual or physical, that will be configured to host clustered file shares for high-availability.

Configure Roles and Features

The first step is to install the necessary Roles and Features that we will use to build the clustered NAS solution. Use the Server Manager Dashboard and select Manager -> Install Roles and Features. Select the following features within “File and Storage Services”. You may want to install other components for additional data management and monitoring functionality such as the Data Deduplication and File Server Resource Manager, however these are not required. Also, note that Server for NFS is selected by default, but can be ignored if you will not be sharing data with Unix/Linux systems using this protocol.



Install the Failover Clustering and MPIO Features, which enables high-availability and permits load balancing of data I/O across multiple network connections between server nodes and the Nimble Storage array. This provides resiliency in the event of a network path failure as well as additional performance when multiple connections are available.

Configuring iSCSI and MPIO

Follow the Nimble Storage Best Practices for Networking to properly configure both iSCSI and MPIO on each server node. It is available on the Nimble support site.

Configure Failover Clustering

Create a new cluster by adding each of the server nodes to the cluster. You should give the cluster a unique name on the network, this name will be used to manage the clustered roles and resources but will not be used by normal user traffic. For example, FSCluster.domain.com.

Connect Volume

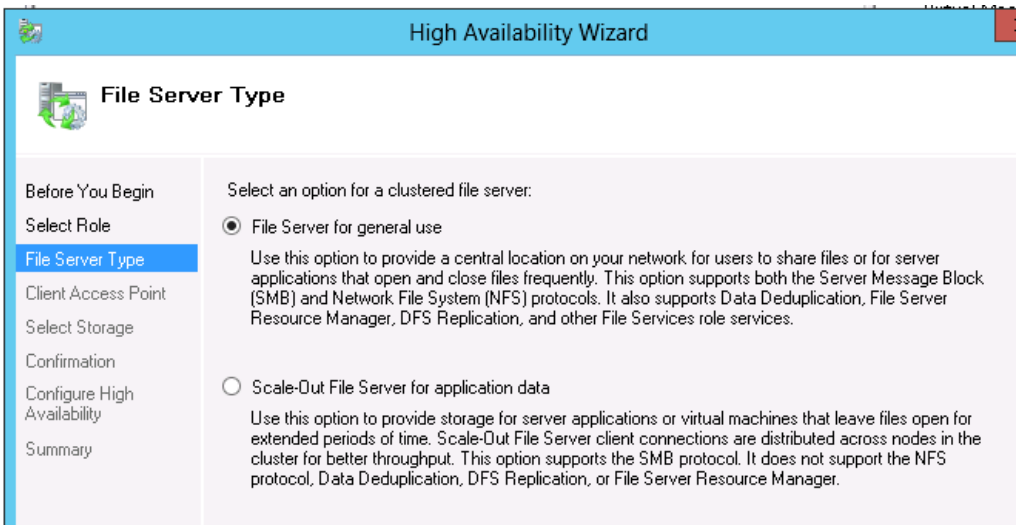
Use the iSCSI Management tools on each cluster node to connect to the Nimble Volume that you want to use as a file share. Use the Disk Management tools provided in the Computer Management tool to bring the volume on-line and initialize it with a GPT partition table. You can format it using Windows NTFS best practices (http://support.microsoft.com/kb/314878) which will normally be "default".

Test the Volume

Testing volume performance is a quick way to determine if there are any problems between the Windows file server and the storage. A simple method uses the Windows Explorer to copy many files from the file server to the volume used as a file share.

Configure Clustered File Sharing

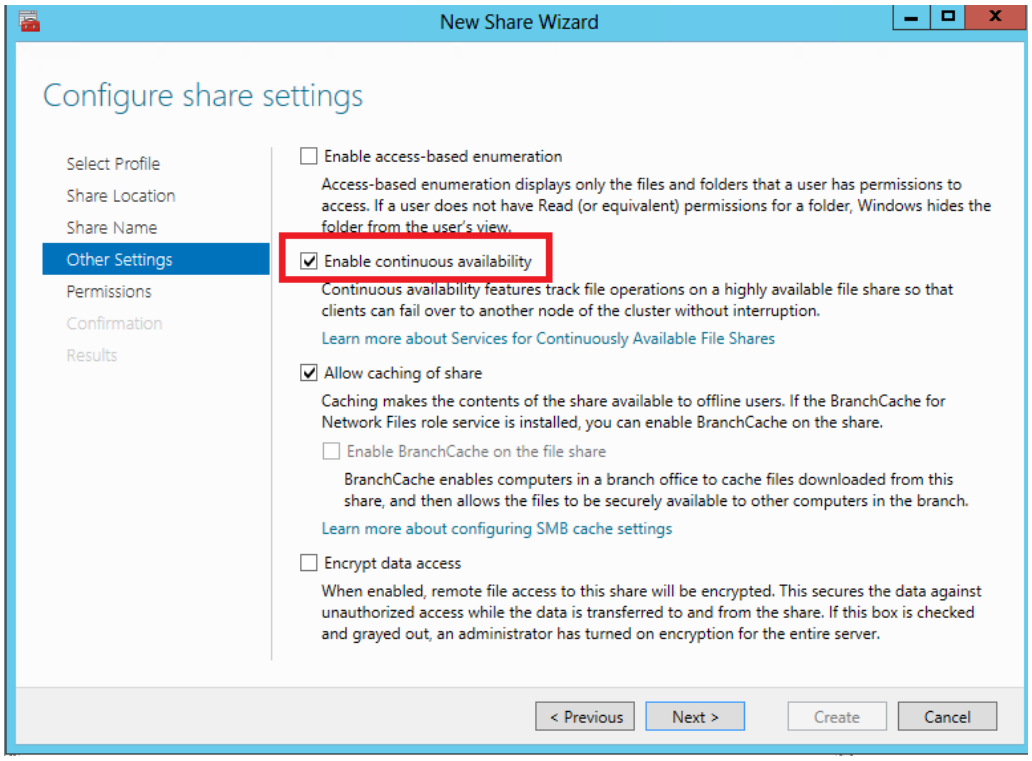
There are two types of clustered file shares that you can create with Windows 2012 Failover Clustering, General Use and Scale-Out File Server. The Scale-Out File Server is a new addition with Windows Server 2012 and leverages Clustered Shared Volumes to distribute load between cluster nodes in an Active/Active methodology. Scale-Out File Servers are designed to support server applications like databases or virtual disk files in Hyper-V implementations. Note: using a Scale-Out File Server role has limitations that do not permit the use of certain Windows-native tools such as Deduplication; see the Microsoft Tech Note for further information: http://technet.microsoft.com/en-us/library/hh831349.aspx.



Enable Continuous Availability

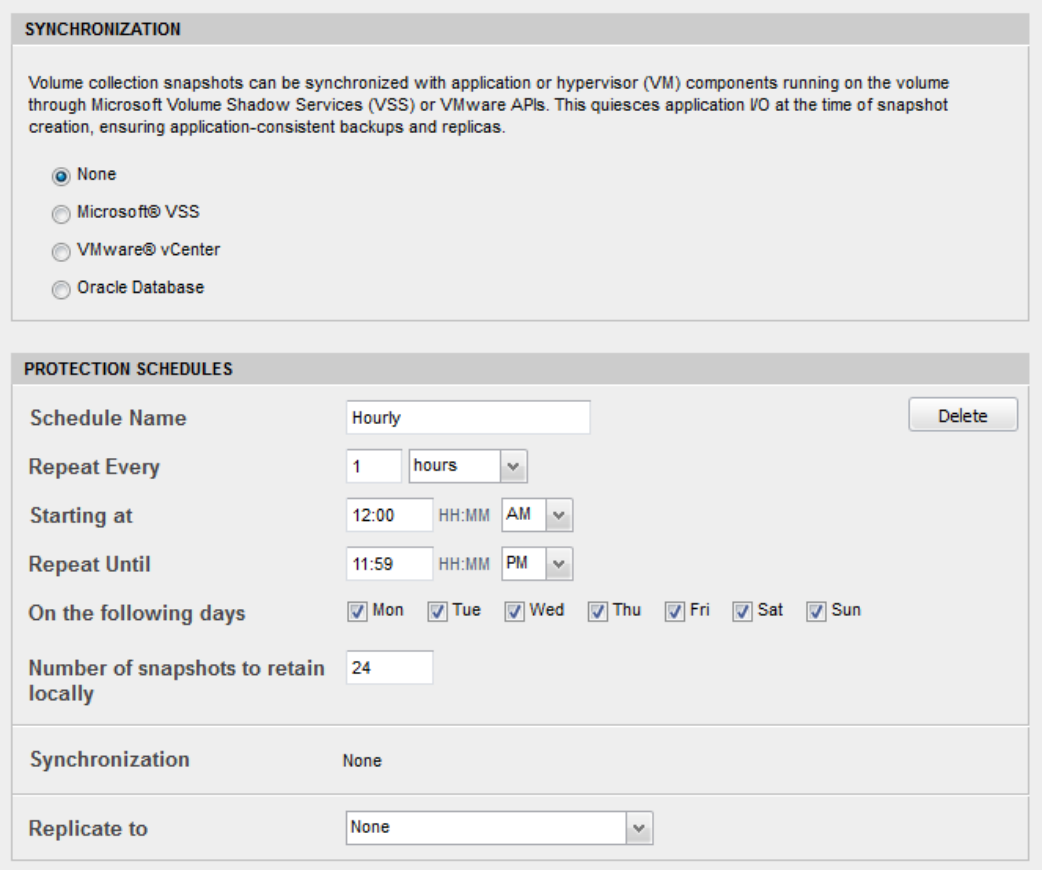
SMB3 includes a powerful feature called "Continuous Availability" which provides transparent failover of shares between cluster nodes without impacting the client. This feature is only available in Windows 2012, Windows 8 and newer operating systems. The feature essentially shares client state between cluster nodes to enable file share failover without service downtime. You can

enable the feature easily when creating your file shares or modifying the existing file shares as follows.



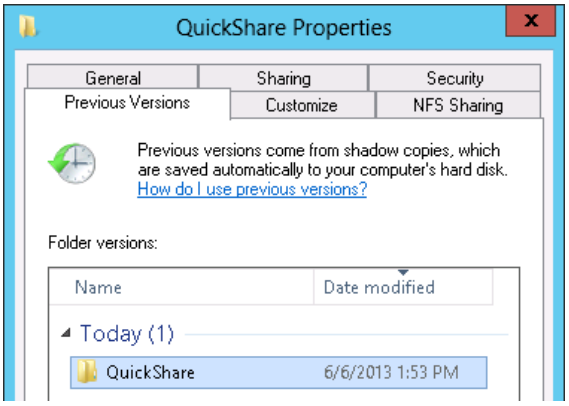
Data Protection

Nimble Storage provides a converged storage solution that enables you to perform snapshot backups of file share data near instantaneously. Typical file shares don't require quiesce prior to snapshot because they contain data such as Microsoft Office documents versus database applications like Microsoft SQL Server or Exchange which require quiesce prior to backup. This improves the Recovery Point in Time (RPO) by increasing the number of snapshots to as frequently as every minute. It is also important to note that Nimble snapshots are highly efficient and consume very little storage capacity.



When enabling protection on your Nimble volume, you can leave Synchronization at the default of "None" because shared office files don't require quiesce, also known as crash consistent. You can create one or more Protection Schedules based on your protection needs. For example, you might want frequent recovery intervals such as every 15 minutes; however the value of such fine grained snapshots diminishes over time. Thus, you might consider doing snapshots every minute for 2 hours and then keeping hourly snapshot for 3 days and finally keeping daily snapshots for 90 days retention. Another consideration when developing protection schedules is the replication schedule if you would like to protect your data off-site. Nimble Storage also allows you to keep standard protection schedules as templates that can be quickly used for other volumes.

Data Restoration



Recovery of data is the true measure of any backup solution, especially when measured in time. Traditional backup solutions require making copies of data to a different physical location and possibly moving that data off-site based upon age. Restoration using traditional backup tools also requires the time to copy data from the backup media back to a production server prior to making it available for application recovery. Microsoft Windows Server introduced the Previous Versions feature to file sharing to make the restoration process both quicker by eliminating the copy restore and also to permit user self-service for file restoration. Volume Shadow Copies and Previous Versions combine to provide an easy and valuable solution for file sharing solutions.

There are a few drawbacks to the Windows-native VSS/Previous Versions solution that Nimble Storage snapshot backups can provide a replacement for. Using Nimble snapshot backups alone loses the user self-service restoration functionality of Previous Versions until Microsoft updates the feature to leverage VSS hardware providers. The following are use cases where Nimble snapshot backups can help your file share implementation.

- Previous Versions requires a Windows client to take advantage of the user self-restoration functionality. NFS-based clients require administrator assistance to perform file restoration.
- Leverages VSS Software Provider which requires host CPU processing cycles. Nimble Storage arrays provide purpose built optimized storage processing capabilities that offload much of the processing burden from the host.
- Backups using third-party tools require host CPU, Storage I/O and Networking bandwidth. Nimble has partnered with backup software vendors such as CommVault to provide SAN-based backup directly from Nimble Storage arrays using Nimble snapshot. This greatly reduces the impact to production host systems.

Summary

Using Nimble Storage and Windows Server 2012 together provides a best-of-breed solution that matches Nimble's powerful storage solution with Windows file sharing compatibility and flexibility. The solution detailed in this best practice guide provides a highly available file sharing solution for both SMB/CIFS and NFS.

Nimble Storage, Inc.
2740 Zanker Road, San Jose, CA 95134
Tel: 408-432-9600; 877-364-6253) | www.nimblestorage.com | info@nimblestorage.com