Technical white paper

Technical overview of HP 3PAR File Persona Software Suite

Truly converged file and object access for HP 3PAR StoreServ Storage

Table of contents

Introduction

The modern IT needs for their data centers to deploy, serve, manage and report on different tiers of business applications, databases, virtual workloads, home directories and file sharing all at the same time, co-locate multiple systems, and share power and energy. This is true for large as well as small environments. Modern IT would like to consolidate as much as possible to minimize cost and maximize efficiency of their data centers and branch offices. HP 3PAR StoreServ is highly efficient, flash-optimized storage engineered for the true convergence of block, file, and object access to help consolidate diverse workloads efficiently. HP 3PAR OS and converged controllers incorporate multiprotocol support into the heart of the system architecture.

Audience

This white paper provides an overview of the HP 3PAR File Persona Software Suite and the technical details about the features and core file data services included in the software suite. It is intended to assist the System Administrators, Solution Architects, Pre-sales engineers, and Professional Services Consultants who design, deploy, and administer the HP 3PAR StoreServ storage system in a home directory or corporate/group share environment.

Overview

HP 3PAR File Persona Software Suite is a licensed feature of HP 3PAR OS that enables a rich set of file protocols and core file data services on an HP 3PAR StoreServ system. As a feature of HP 3PAR OS, File Persona Software Suite inherits one of the industry-leading architecture and Block Persona benefits of HP 3PAR StoreServ. It extends the spectrum of primary storage workloads natively addressed by HP 3PAR StoreServ from virtualization, databases, and applications via the Block Persona to include client workloads such as home directory consolidation, group and department shares, and corporate shares via the File Persona—all with truly Converged Controllers, truly agile capacity, and truly unified management.

HP 3PAR File Persona Software Suite tightly integrates into the data center by supporting the standard industry NAS protocols, file services ecosystem such as authentication and authorization methods, antivirus servers, and variety of client OSs while managing it all with a single streamlined interface.

Product highlights

- Rich file protocols including Server Message Block (SMB) 3.0, 2.1, 2.0, and 1.0, and NFSv4.0 and v3.0 to support a broad range of client OSs.
- Object access application-programming interface (API) that enables programmatic data access via a representational state transfer (REST) API for cloud applications from virtually any device anywhere.
- Transparent Failover for clients via SMB 3.0 and NFS to allow for non-disruptive HP 3PAR OS upgrades or in the event of a controller failure.
- Performance acceleration leveraging HP 3PAR Adaptive Flash Cache for read intensive workloads.
- Data compaction via thin built-in zero detect and HP 3PAR Thin Provisioning, plus data optimization via the separately licensed HP 3PAR Adaptive Optimization and HP 3PAR Dynamic Optimization.
- Comprehensive data protection with point-in-time File Store snapshots for user-driven file recovery, support for third-party antivirus software, network share and Network Data Management Protocol (NDMP)-based backup/restore, and disaster recovery replication via the separately licensed HP 3PAR Remote Copy.
- Security of Federal Information Processing Standard (FIPS) 140-2 validated Data-at-Rest (DAR) Encryption as an optional additional measure to prevent unauthorized data access.
- Seamless integration with a broad range of IT infrastructure. This includes Active Directory for Microsoft®-based IT infrastructure including core Microsoft data services, such as Folder Redirection, Offline Files, Roaming User Profiles, distributed file system (DFS)-Namespace, and Microsoft Management Console. It also includes Lightweight Directory Access Protocol (LDAP) and local user authentication for Linux®-based IT infrastructure.
- Single management interface for file and block through HP 3PAR StoreServ Management Console (SSMC) GUI with a performance dashboard, custom reports capability, and HP 3PAR OS CLI.

Licensing

HP 3PAR File Persona Software Suite title uses a capacity-based licensing approach, hence there is a 1 TB software LTU for each HP 3PAR StoreServ 7000c series models (7200c, 7400c, 7440c, and 7450c). The 1 TB software LTU for a particular platform is a single stock-keeping unit (SKU) irrespective of the drive type or drive capacity, which includes all file protocols SMB, NFS, and Object Access API and core file data services. Specific number of 1 TB LTUs need to be purchased for every TB of usable file capacity on these 7000c converged controllers.

The only additional hardware required for HP 3PAR File Persona Software Suite is the NICs in the HP 3PAR StoreServ array: the 4-port 1GbE NIC or the 2-port 10GbE NIC.

Architecture

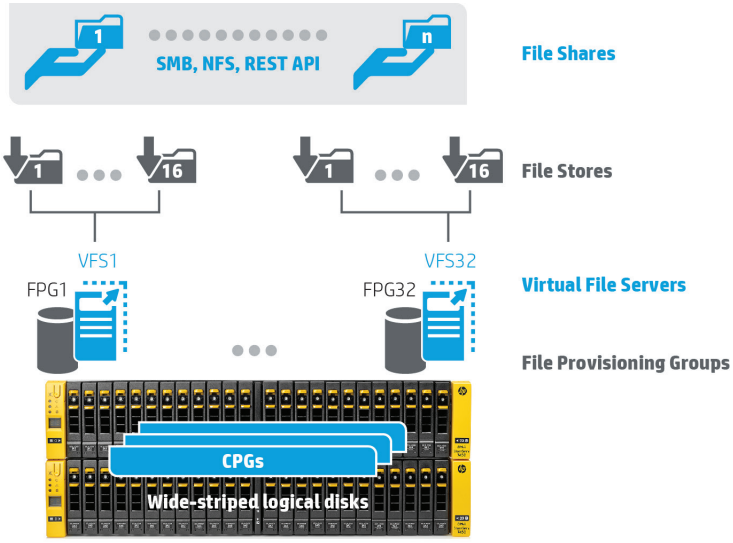
HP 3PAR File Persona Software Suite concepts and terminology

HP 3PAR StoreServ File Persona Software Suite is comprised of the following managed objects:

- File Provisioning Groups (FPGs)
- Virtual File Servers (VFSs)
- File Stores
- File Shares

The File Persona Software Suite is built upon the resilient mesh-active architecture of HP 3PAR StoreServ and benefits from HP 3PAR storage foundation of wide-striped logical disks and autonomic Common Provisioning Groups (CPGs). A CPG can be shared between file and block to create the File Shares or the logical unit numbers (LUNs) to provide the true convergence. Figure 1 represents the four managed objects for HP 3PAR File Persona Software Suite within HP 3PAR OS.

Figure 1. HP 3PAR File Persona logical view



A File Provisioning Group (FPG) is an instance of the HP intellectual property Adaptive File System. It controls how files are stored and retrieved. Each File Provisioning Group is transparently constructed from one or multiple Virtual Volumes (VVs) and is the unit for replication and disaster recovery for File Persona Software Suite. There are up to 16 FPGs supported on a node pair.

A Virtual File Server (VFS) is conceptually like a server. As such, it presents virtual IP addresses to clients, participates in user authentication services, and can have properties for such things as user/group quota management and antivirus policies. There are up to 16 VFSs supported on a node pair, one per FPG.

File Stores are the slice of a Virtual File Server and File Provisioning Group at which snapshots are taken, capacity quota management can be performed, and antivirus scan service policies customized. There are up to 256 File Stores supported on a node pair, 16 File Stores per VFS.

File Shares are what provide data access to clients via SMB, NFS, and the Object Access API, subject to the share permissions applied to them. Multiple File Shares can be created for a File Store and at different directory levels within a File Store.

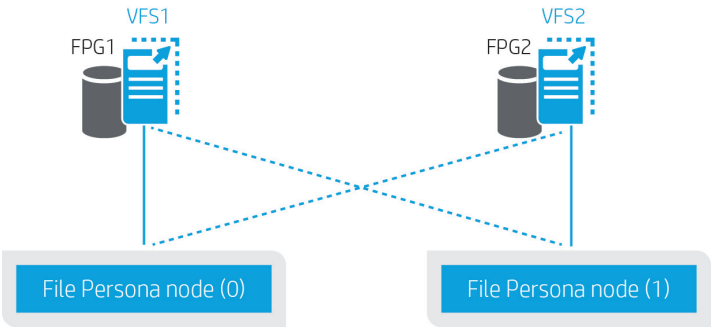
File Shares and VFSs are managed as normal operations via StoreServ Management Console. File Stores and FPGs are typically managed explicitly for advanced operations only.

Resiliency and high availability

HP 3PAR File Persona Software Suite uses a mission-critical proven HP intellectual property-based 64-bit journaling file system that has been optimized for high metadata-driven workloads such as home directory consolidation and corporate/group shares.

HP 3PAR File Persona Software Suite benefits from the inherited HP 3PAR StoreServ resiliency, in case of an event requiring node-failover, the File Persona Software Suite will failover to the other node in the node pair. The VFS ownership changes to the other node. Depending on the protocol, the failovers are transparent to the users.

Figure 2. HP 3PAR File Persona high availability



Name services and authentication

Name services refers to user account name and group name resolution/lookups from user and group databases like Active Directory, LDAP, or local user database. Name resolution refers to user, group, or host name lookup in the respective Name Services databases. Authentication and authorization are essential components of home directories consolidation and corporate/group shares in the data center. Any user trying to access his home directory over the network needs to be identified as himself with his associated credentials. The process of identifying an individual usually based on a username and password is called authentication. HP 3PAR File Persona Software Suite supports three types of Name Services—Active Directory, LDAP, and local database. It supports Kerberos, NT LAN Manager version 2 (NTLMv2), and NTLM types of authentication for Active Directory and LDAP users along with support for authentication for local users and groups.

The File Persona Software Suite uses the local user authentication method as the default, but Active Directory and LDAP services can be added to the authentication stack for the user and group name lookup. Picking the correct order optimizes the performance of account name lookups. The stacked authentication lookup order is persistent during the failover.

Note
Authentication should generally be configured before starting to write data to the system, to avoid any implications of changes to the authentication scheme.

Active Directory

Active Directory is a directory service primarily used in Windows® environments, where Kerberos, NTLMv2, and NTLM are primary types of authentications. HP 3PAR File Persona Software Suite supports the user credential authentication using Kerberos, NTLMv2, or NTLM authentication in Active Directory based on the authentication stack order defined within File Persona Software Suite. Active Directory performs name lookups and authentications for user accounts and groups and all user name lookups are stored in Active Directory name cache on the File Persona node. This cache is referenced or populated for every user name request and will be cleared when the File Persona is restarted.

The File Persona node joins the Windows Active Directory domain where it creates the computer account for the File Persona node. The computer name created in the AD domain is in the format of HP 3PAR StoreServ system name plus the node number (e.g., deptserver-0.sales.hp.com[1]). Use `showfs -ad` command at the HP 3PAR OS CLI to check if the node has joined the Active Directory domain properly.

Note

- Networking node IP addresses, gateway, and Domain Name System (DNS) should be configured on the File Persona node before attempting to associate to LDAP or Active Directory.
- NTP should be configured for HP 3PAR StoreServ system such that the array and the domain controller are relatively in sync before attempting an Active Directory-join, or the join may fail.

Lightweight Directory Access Protocol (LDAP)

LDAP is most commonly used in Linux/UNIX® environments, where customers have users that connect to SMB or NFS shares on HP 3PAR StoreServ system running File Persona Software Suite. The LDAP provider uses ldapsearch requests to lookup users and groups by name or security identifier (SID). SIDs are formulated based on an SID prefix and user ID (UID)/group ID (GID) when the POSIX schema template is configured. It also provides NTLM or NTLMv2 authentication by matching a user-supplied password with a Windows-encrypted password stored in LDAP. The LDAP schema attribute it uses, depends on the schema template used. The File Persona SMB server can be configured to use either Samba or POSIX schema, but only one schema at a time. Use `showfs -ldap` command at the CLI to check the status of LDAP authentication.

The LDAP connection for File Persona Software Suite can be using three categories:

- Simple connection—The authentication is done through plain text.
- Secure Sockets Layer (SSL)—The authentication is done through NTLM and uses the LDAP server's fully qualified domain name (FQDN) name to connect. The communication will be established on port 636 by default.
- Transport Layer Security (TLS)—The authentication is done through NTLM and uses the LDAP server FQDN name to connect. The communication will be established on port 389 by default.

Local authentication

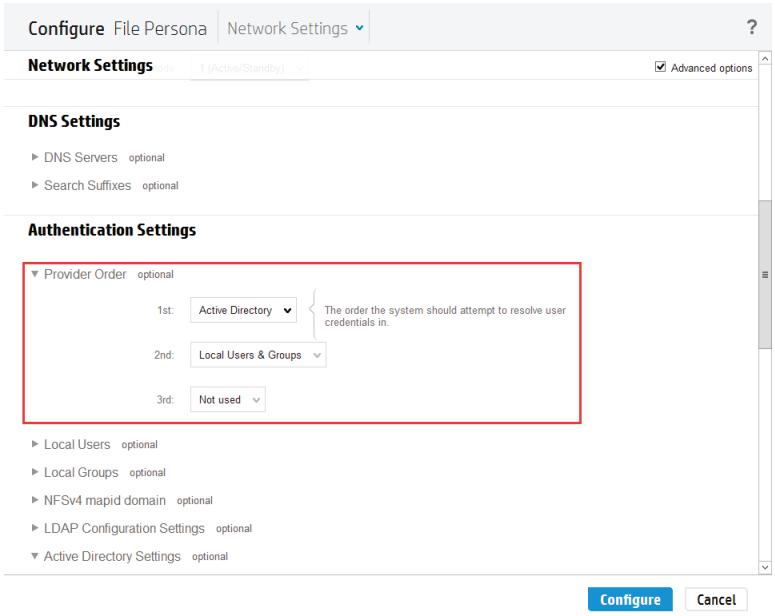
Local authentication will often be used in smaller Windows or Linux/UNIX environments. Each node has a copy of the local user database. All changes to the local accounts database are replicated to all File Persona nodes in a system. Local users are authenticated using NTLMv2 authentication by default. The password is stored in encrypted form in the local user database. UIDs and GIDs are assigned automatically if not specified during their creation. The Storage Administrator should make sure that IDs are unique across the name services.

[1] Windows 2000 and above DNS domain name support up to 24 characters in the hostname. Make sure to follow Microsoft guidelines for the hostname character length.

Authentication stack order

The authentication stack order can be configured from the SSMC after enabling **Advanced options** in the **Configure** File Persona menu. The **Local Users & Groups** must be included in the **Provider Order**, while LDAP and Active Directory are optional. Active Directory and **Local Users & Groups** are the default stacking orders (see figure 3), and as a best practice, there should not be a value in the stacking order that is not configured. To show the configured stacking order on the CLI use `showfs -auth`. Note that the stacking order is configured separately from the authentication methods, and if a method is not in the stack, users will not be able to authenticate using that method.

Figure 3. Configuring the authentication stack order



Note

The authentication and authorization method used for HP 3PAR File Persona Software Suite is separate from the security method used for management of the HP 3PAR StoreServ array (Management Console and CLI). For instance, management array access can be using local authentication and authorization method (on the HP 3PAR StoreServ nodes), while HP 3PAR File Persona is using Active Directory for authentication and authorization.

Authorization and permissions

Authorization is a process used to verify what effective permissions a user (or group) has on files or folders. Authorization is performed by comparing user account or member names of a group with the permissions on file storage resources such as files or directories. Only authorized users (or groups) are allowed to access any file or folder, while the rest are denied access. For shared folder access, the user has to go through the share permissions first to check if the user is authorized to access that share. An ACL is a list of access control entries (ACEs). Each ACE in an ACL identifies a trustee and specifies the access rights allowed, denied, or audited for that trustee. SMB users are granted access based on the advanced access rights allowed through NTFS ACLs permissions set on files and directories. NFS users are granted access based on the POSIX or NFSv4 ACLs set on file or directories. The user's name or UID and all group memberships/GIDs are evaluated in determining access to files and directories. The most restrictive user rights are honored when granting access to files and folders.

Converged ACL

HP 3PAR File Persona Software Suite uses the advanced HP Adaptive File System that is designed for storing the converged ACLs on the disk in the NFSv4.1 ACL format for all files and directories and converts the ACLs to each protocol specific ACL for SMB, NFS, or HTTP clients, as described in table 1. The Adaptive File System also performs the name resolution for the username from the protocol specific username format to user principal name (UPN) format to store on the disk.

Table 1. Converged ACLs

Converged ACL stack	SMB	NFSv3	NFSv4	Object Access API over HTTP
ACLs enforcer	SMB server	FPG (file system)	FPG (file system)	FPG (file system)
ACLs enforced by File Persona	NTFS ACLs	POSIX ACLs	POSIX ACLs	POSIX ACLs
On-disk ACLs stored	NFSv4.1 ACLs	NFSv4.1 ACLs	NFSv4.1 ACLs	NFSv4.1 ACLs
Name resolution	Domain\username → user@domainname	UID/GID → user@domainname	user@domainname → user@domainname	Domain\username → user@domainname

Note

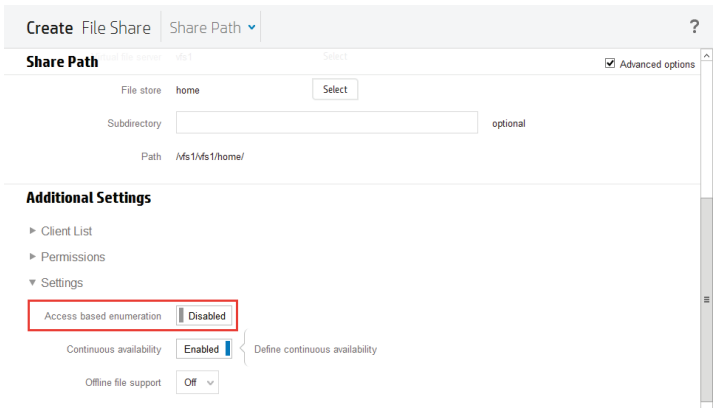
HP 3PAR File Persona Software Suite supports file locking within a protocol but not across protocols, so accessing the same file simultaneously from different file protocols is not supported. This restriction does not preclude the access of the directory or files by any file protocol at different times e.g., all locks held by SMB clients are honored by other SMB clients.

Access-based Enumeration (ABE)

HP 3PAR File Persona Software Suite supports Access-based Enumeration, which is a very useful feature in the home directories consolidation scenario. Access-based Enumeration is a Microsoft Windows feature which when applied on an SMB share, allows users to list only the files and folders to which they have access when browsing content on the file share. This avoids user confusion that can be caused when users connect to a file share and encounter a large number of files and folders that they cannot access. This feature allows administrators to control the display of files and folders according to a user's access rights. Therefore, when applied on a shared folder that contains many home directories, users who access the shared folder can see only their personal home directories; other users' folders are hidden from view. This can also be used on group shares with common set of the files or application data, accessed by a group of users.

In addition to protecting sensitive information at your workplace, ABE enables administrators to simplify the display of large directory structures for the benefit of users who do not need access to the full range of content. End users see only the files and folders that they are responsible for, rather than looking through a busy folder structure with hundreds of users folders in it. . Administrators can be more productive because they don't have to help less-skilled users navigate through dense shared folders. Enabling ABE in File Persona is done by specifying the `-abe true` option when creating the File Share `createfs smb -abe true <vfs> <sharename>`. The SSMC can also be used to enable this when creating or modifying the **File Share**, (see figure 4 [enable the **Advanced options**]).

Figure 4. Enable ABE on file share



Protocol support

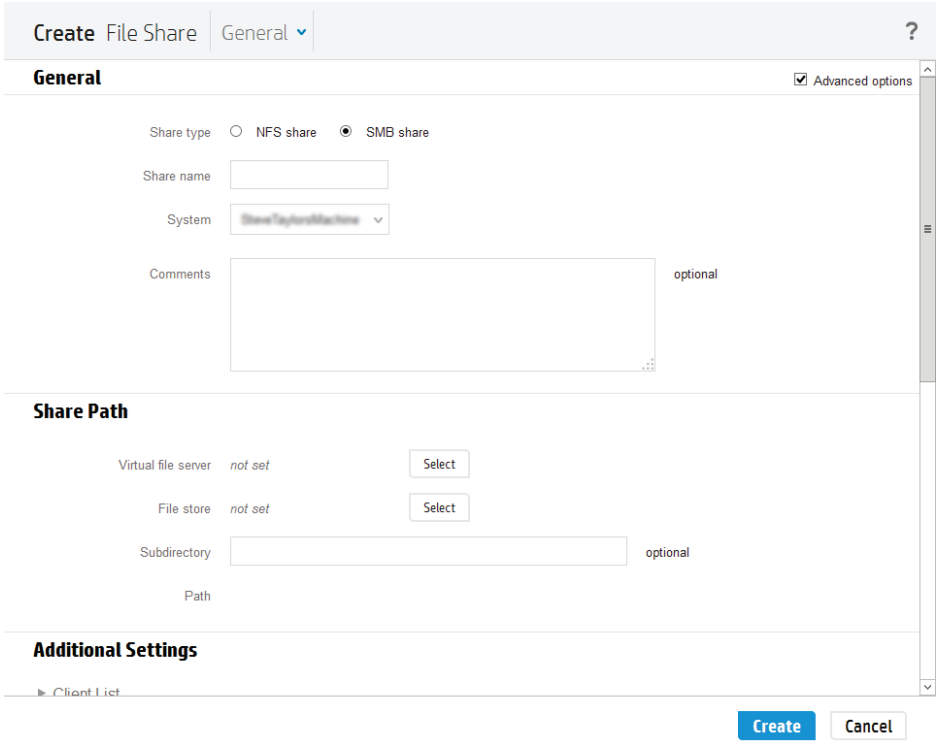
SMB protocol

The SMB protocol is the most widely used protocol for home directory access and brings a robust feature set for enterprise file sharing. File sharing protocols provide central management of data that uses client/server method, reduces administrative overhead, and provides granular access control to the files.

The SMB protocol is the default protocol used by the Windows clients, but there are also Mac Linux, and Samba clients, which use the SMB protocol to connect to an SMB file server. It brings a variety of security, performance, resiliency, and efficiency features that help customers to offer home directories, group/department shares, and corporate shares to their clients.

The SMB File Share can be created using `createfshare smb [options <arg>] <vfs> <sharename>` instructing the File Share to use the SMB protocol.

Figure 5. Creating SMB file share



HP 3PAR File Persona Software Suite supports SMB 3.0, 2.1, 2.0, and 1.0. This includes advanced SMB 3.0 protocol feature of Transparent Failover, SMB opportunistic locks (oplocks) and leases (file and directory) for all SMB versions; crediting and large maximum transmission unit (MTU) size for SMB 2.x and beyond versions. In addition to these SMB protocol features, File Persona Software Suite also supports Offloaded Data Transfer (ODX) features of Microsoft Windows 2012.

Table 2. SMB protocol version supported with various operating systems

OS	SMB 3.0	SMB 2.1	SMB 2.0	SMB 1.0
Windows® 8/8.1, Windows Server® 2012 R2	✓	✓	✓	✓
Windows® 7, Windows Server 2008 R2		✓	✓	✓
Windows Vista®, Windows Server 2008			✓	✓
Windows® XP, Windows Server 2003 R2				✓
Mac OS 10.8, 10.9		✓		

Transparent Failover

SMB Transparent Failover is one of the key features in the feature set introduced in SMB 3.0 with Windows Server 2012 and Windows 8 OSs. SMB Transparent Failover enables administrators to configure Windows File Shares to be continuously available. Using continuously available File Shares, administrators can perform hardware or software maintenance on any cluster node without interrupting the client connections that store their data files on these File Shares. Also, in case of a hardware or software failure, the clients will transparently reconnect to another cluster node without any disruption to the user connections. To benefit from SMB Transparent Failover, both the SMB client computer and the SMB server computer must support SMB 3.0 at a minimum. Computers running down-rev SMB versions, such as 1.0, 2.0, or 2.1 can connect and access data on a file share that has the continuously available property set, but will not be able to leverage the benefits of the SMB Transparent Failover feature.

SMB Oplocks and Leases

Opportunistic locks or oplocks is a client caching mechanism that allows SMB/SMB 2.0 clients to decide the client-side buffering strategy dynamically, so the network traffic can be minimized to improve performance. In SMB 2.1, client oplock lease model allows oplocks to be held by a client for enhanced file and handle caching opportunities for the SMB client. This feature brings performance improvement by reducing network bandwidth consumption, greater file server scalability, and better response time when accessing the files over a network. The only disadvantage of the file level oplocks or leases is that if there are any changes in the files and folders on the file server, clients with the cached listing of that directory would not be aware of the changes when directory listing is refreshed locally. In SMB 3.0, the directory-leasing feature improves this behavior, by allowing the SMB client to cache the directory and file metadata together in a consistent manner for longer duration. Clients are notified when directory information on the server changes and the data resynchronizes and updates the cache. This feature is designed to work with user's home folders (read/write with no sharing) and published shares (read-only with sharing). This results in improved network performance and faster response time.

SMB Crediting

SMB 2.0 and above protocol uses a credit-based flow control, which allows the server to control a client's behavior. The server will start with a small number of credits and automatically scale up as needed. With this, the protocol can keep more data "in flight" and better utilize the available bandwidth. It makes it easy for clients to send a number of outstanding requests to a server. This allows the client to build a pipeline of requests instead of waiting for a response before sending the next request. This is especially relevant when using a high-latency network.

Large MTU size

The MTU of a communications protocol of a layer is the size (in bytes) of the largest protocol data unit that the layer can pass on. HP 3PAR File Persona Software Suite supports large MTU size, which has been introduced in SMB 2.1 to achieve better performance for 10GbE (high-speed, low-latency) networks. In SMB 2.1, this maximum MTU size is increased from 64 KB to 1 MB. At the SMB client computers, the large MTU option must be enabled in the registry; by default, it is enabled on Windows 2012 and 2012 R2. HP 3PAR File Persona Software Suite adapts to what the SMB client computer is using for its MTU size.

NFS protocol

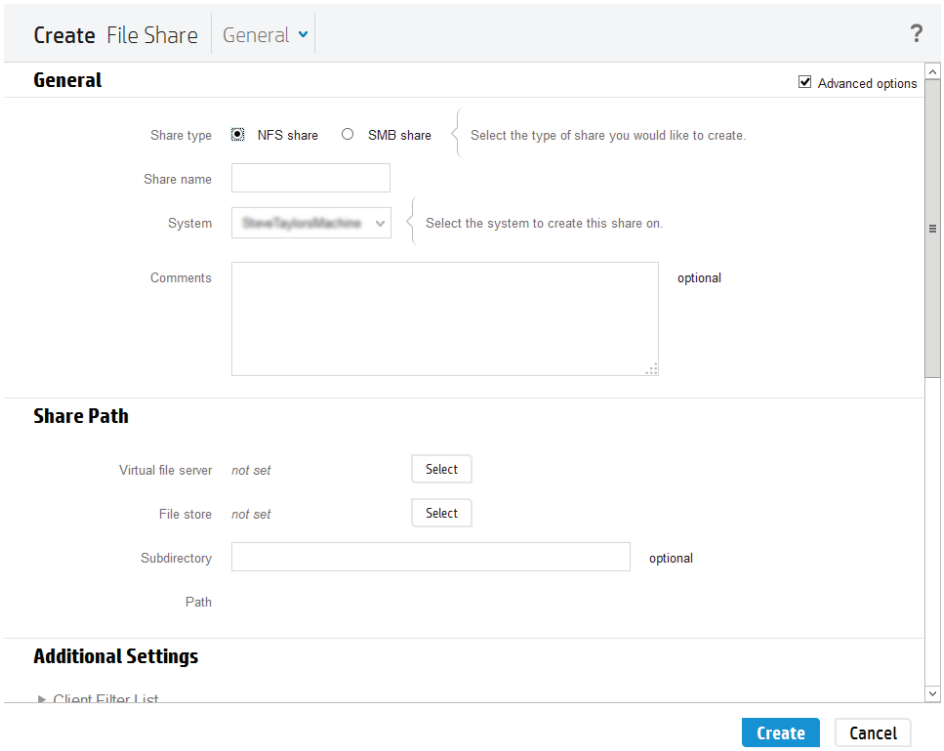
The NFS protocol is a versatile protocol for all Linux/UNIX clients, which provides high concurrency of the clients with central management of data using client/server method, reducing administrative overhead and provides granular access control on the files like SMB protocol.

The NFS protocol is the default protocol used by the Linux/UNIX clients designed to be independent of machine architecture, OS, network architecture, and transport protocol by using remote procedure call (RPC) calls.

HP 3PAR File Persona Software Suite supports NFSv4.0 and v3.0, and supports variety of Linux/UNIX client operating system. Refer to HP SPOCK site for interoperability matrix.

The NFS File Share can be created using `createfshare nfs [options <arg>] <vfs> <sharename>` instructing the File Share to use the NFS protocol.

Figure 6. Creating NFS file share



Object Access API

Web services can be considered as “RESTful” if they conform to the constraints described in the architectural constraints of REST. It changes the way programs interact with storage; complex file system semantics are compressed into a small number of commands. REST over HTTP is a simple way for applications to interact with the storage where, unlike SMB/NFS, HTTP access is available from nearly every device. This enables developers and customers to integrate direct file access into their applications. The Object Access API of HP 3PAR File Persona Software Suite is a rich set of file system semantics enabling RESTful applications to access files and folders on the File Share directly using REST API. The File Persona supports the operations listed in table 3.

Table 3. Object Access API supported operations

Operations	
Create/replace a file	Change permissions
Download file	Change owner
Delete file	Change group
Retrieve file information	Set extended attributes
Create directory	Get extended attributes
Retrieve directory content	Remove extended attributes
Delete directory	Commit data to disk
Get directory details	Rename file

The Object Access API-enabled File Share can be created using `createfshare obj [options <arg>] <vfs> <sharename>` instructing the File Share to use the Object Access API.

Object Access API command examples:

- Create file: `PUT http://10.33.19.94/v1/myObjShare/afile.txt`
- Download file: `GET http://10.33.19.94/v1/myObjShare/afile.txt`
- Delete file: `DELETE http://10.33.19.94/v1/myObjShare/afile.txt`
- List directory contents: `GET http://10.33.19.94/v1/myObjShare/?cmd=ls&type=true`

Integration with Microsoft environment

Home directory consolidation provides central management, security, efficiency for the users' home directory environment. The File Persona Software Suite supports several Microsoft features, which tightly integrate with the home directory consolidation and for the group/corporate shares. These features make it easier for a Storage Administrator to manage user data and enhance user experience at the same time, e.g., NTFS ACLs, Folder Redirection, Roaming User Profiles, Offline Files, DFS-Namespace, and management thru Microsoft Management Console (MMC).

User settings and user files are typically stored in the local user profile, under the **Users** folder on a local PC. The files in local user profiles can be accessed only from the current computer, which makes it difficult for users who regularly change workstations to work with their data and synchronize settings between multiple computers. Two technologies exist to address this problem: Roaming User Profiles and Folder Redirection. Both technologies have their advantages, and they can be used separately or together to create a seamless user experience from one computer to another. They also provide additional options for administrators managing user data.

Folder Redirection

HP 3PAR File Persona Software Suite support for Folder Redirection lets administrators redirect the path of a user local profile and application data folder to a new location. The location can be a folder on the local computer or a directory on a network file share typically the network home directory on the StoreServ system. The documents in the folder are available to the user from any computer on the network as if the documents were based on the local drive.

Roaming User Profiles

A roaming user profile is a concept in the Microsoft Windows OSs that allows users with a computer joined to a Windows Server domain to log on to any computer on the same network and access their documents and have a consistent desktop experience, such as applications remembering toolbar positions and preferences, or the desktop appearance staying the same. HP 3PAR File Persona Software Suite supports Roaming User Profiles to provide the same look and feel of the user desktop. This leverages easy replacement of a user's computer because all of the user's profile information is maintained separately on Active Directory, independent of the individual computer. When the user logs on to the new computer for the first time, the server copy of the user's profile is copied to the new computer and the home directory path continues to point to the network home directory stored on the HP 3PAR StoreServ system.

Offline Files

The Offline Files feature of Microsoft allows the users to access copies of their network files by making them available offline, even when the computer isn't connected to the corporate network. By supporting this feature, HP 3PAR File Persona Software Suite allows the home directory users to work with their network file offline by caching them on the local computer and automatically synchronizing their files when they connect to the network next time. To enable Offline Files when creating the File Share, specify the `–cache` option to be `off| manual|optimized|auto` where:

- Off: The client must not cache any files from this share. The share is configured to disallow caching.
- Manual: The client must allow only manual caching for the files open from this share. This is the default setting.
- Optimized: The client may cache every file that it opens from this share. Also, the client may satisfy the file requests from its local cache. The share is configured to allow automatic caching of programs and documents.
- Auto: The client may cache every file that it opens from this share. The share is configured to allow automatic caching of documents.

The command `createfshare smb –cache auto <vfs> <sharename>` creates a File Share <sharename> on the VFS <vfs> allowing automatic caching of documents.

Offloaded Data Transfer

Offloaded Data Transfer (ODX) is a Microsoft Windows feature that enhances host performance by offloading copy and move operations by allowing them to be performed by the storage hardware rather than the OS. Support for ODX is introduced in SMB 3.0 and serves as a method to offload the copy of large files between SMB shares on the same controller. HP 3PAR File Persona Software Suite supports ODX natively in the SMB server in StoreServ system to improve the performance for large file transfers. By default, ODX is enabled Microsoft Windows Server 2012, Windows 8 and 8.1, when the pre-requisites are met, and can be verified by typing the following command in a PowerShell session:

Get-ItemProperty hklm:\system\currentcontrolset\control\filesystem -Name "FilterSupportedFeaturesMode"

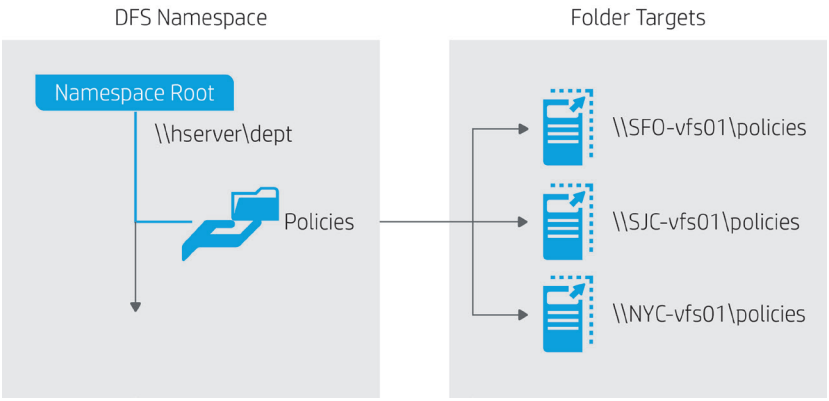
When ODX is enabled, the FilterSupportedFeaturesMode returns "0" as the value.

DFS-Namespace

HP 3PAR File Persona Software Suite supports the DFS Namespaces as a leaf node, so the shares can be distributed across the VFSs on the File Persona nodes easily for redundancy and load distribution.

A namespace is a virtual view of shared folders where the path to a namespace is similar to a Universal Naming Convention (UNC) path to a shared folder, but instead of referring to a server (like \\SFO-vfs01\policies) it is referring to the DFS-Namespace (like \\hserver\policies) allowing users a single place to locate data, but distributing data across different VFSs to enhance availability and performance.

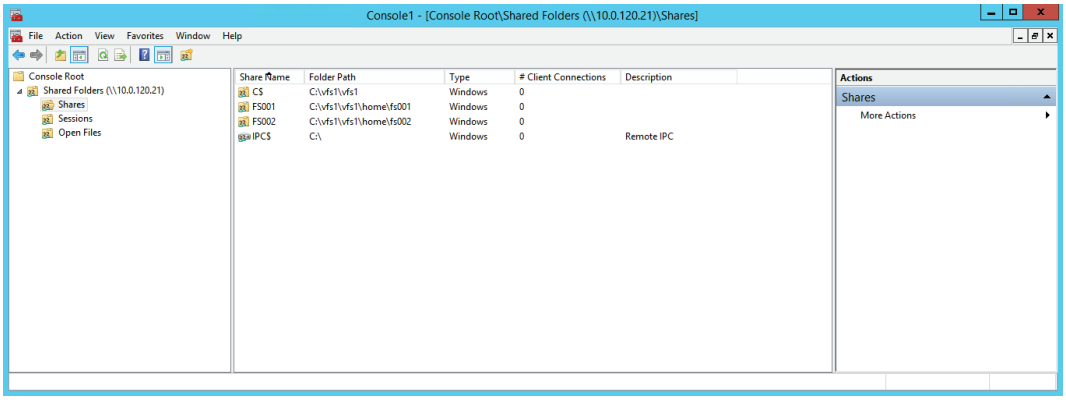
Figure 7. DFS-Namespace



Microsoft Management Console

HP 3PAR File Persona Software Suite offers seamless integration with the MMC to manage the shared folders on the HP 3PAR File Persona, see figure 8 (including creating new shares and deleting existing shares). For instance, to manage permissions for this share, right-click it, select properties, and select the permission tab. This will provide a well-known interface alternative to the SSMC for the File Share administrator.

Figure 8. Managing shared folders from MMC



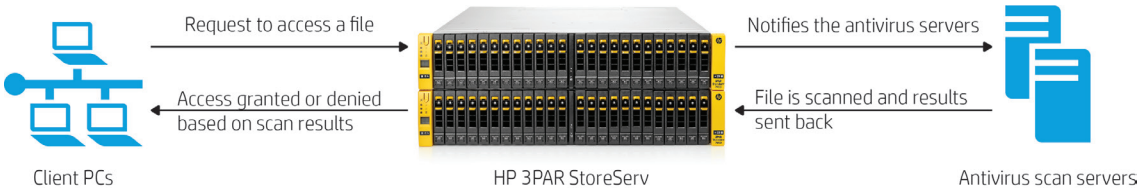
Antivirus scanning

HP 3PAR File Persona Software Suite supports antivirus scanning to provide data protection against the virus and malware. Antivirus scanning on a network share or home directory is critical for data protection as the incoming data is from multiple users and multiple PCs. It quarantines the infected files for an offline action to maintain the business continuity, thus preventing outages by a virus attack. The File Persona Software Suite seamlessly integrates with Internet Content Adaptation Protocol (ICAP)-based external third-party antivirus servers. Currently, File Persona Software Suite supports virus scan engines (VSEs) from Symantec Protection Engine 7.5, McAfee® VirusScan Enterprise version 8.8, and McAfee VirusScan Enterprise for Storage 1.0.2, but only single vendor at a time for the HP 3PAR StoreServ system.

HP 3PAR File Persona Software Suite supports antivirus scan policies to control scanning as well as on-access (real time) and on-demand scanning. For redundancy and improved throughput performance, the virus scanning can be configured with multiple antivirus scan servers. Scanned file information is persisted to avoid redundant scans and wasting valuable resources.

For more information on antivirus scanning, refer to Antivirus scanning best practices guide for HP 3PAR File Persona.

Figure 9. HP 3PAR File Persona antivirus architecture



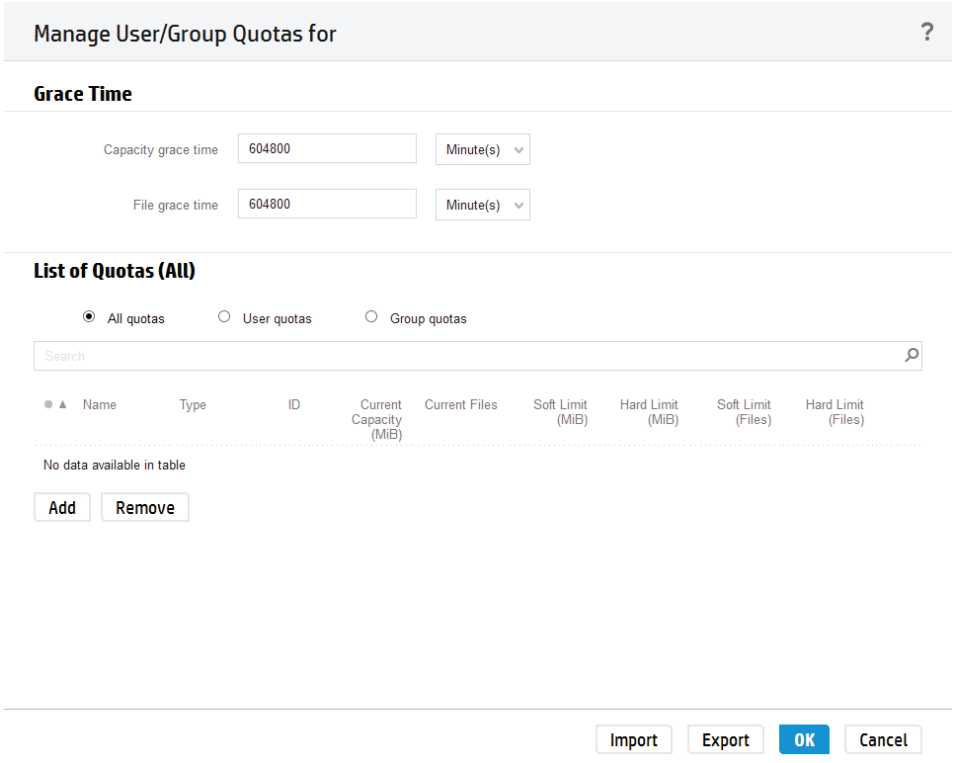
Quota management

Quota management is a method to provide better control and planning for data growth, thus reducing the business cost for backups and archival of the data. Furthermore, quotas help to have a fair allocation of the system resources and avoid undesired data being stored on the home directories. Quotas can be combined with alerts, logs, and reporting events for maintaining records and are essential for those organizations who implement a chargeback model in their environment.

HP 3PAR File Persona Software Suite enables quotas by default in the file system and supports native quota management for user/group quotas on a VFS and a capacity quota on File Stores. The user/group quotas allow for restriction on the total capacity or the number of files (or both) for a user or group within a VFS. The capacity quotas on the File Store enforce the quota policy to control the space usage and the number of files within that File Store independent of users and groups storing files in it.

Quotas used in File Persona can be configured with a hard threshold limit, which is immediately enforced after being exceeded (i.e., users cannot write any further once the hard limit is reached), or a soft threshold limit which when reached starts a grace period (seven days by default) in which continued writes are allowed. The File Persona Software Suite also supports quota reporting for current usage with alerts/events when a soft/hard threshold is reached and quotas are persistent through the local failover to the other node in the node pair. Quota management can be done from the SSMC by going to the details of the VFS, select **Manage User/Group Quotas** from the action menu, where quotas can be created or modified as well as all quotas can be exported or imported (see figure 10).

Figure 10. Manage User/Group Quotas



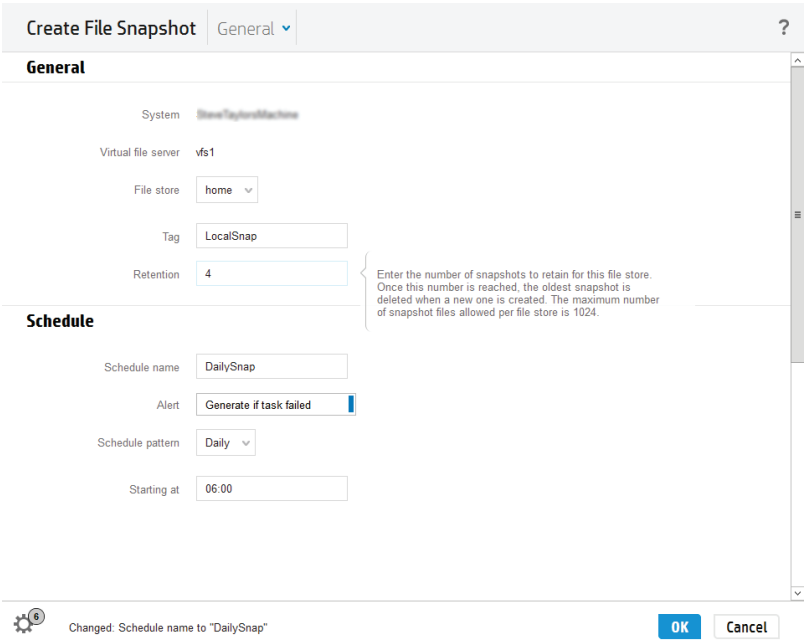
Data protection

User-driven local recovery

HP 3PAR File Persona Software Suite enables user-driven file recovery by using point-in-time File Store snapshots, which are different from block volume Virtual Copy snapshots. It is a versioning mechanism that allows a view of the present and past point-in-time states of the file system, while preserving previous states of files and folders. It allows users to perform the granular recovery of files or folders by themselves. The snapshots can be created on-demand or as per a schedule to create and delete expired snapshots. After snapshots are deleted, a snapshot reclamation process can be executed at the FPG level to reclaim any unused blocks.

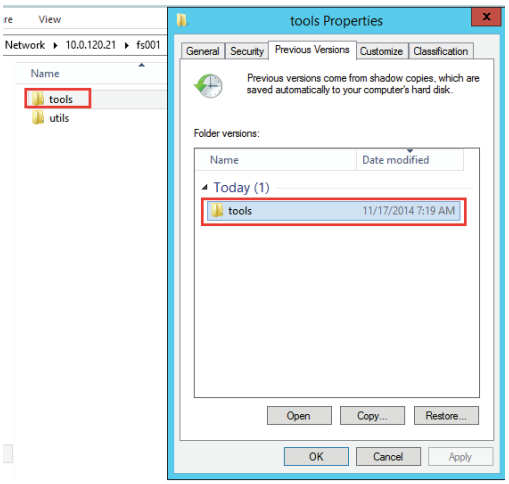
The snapshot can be created from the SSMC from the VFS view. From the action menu, select **Create File Snapshot** and fill out the required fields (see figure 11). The equivalent for the CLI is `createfsnap <vfs> <fstore> <tag>`.

Figure 11. Create File Store Snapshot



Restoring individual files from File Store snapshots is much more efficient than administrator-driven recovery. The user can restore their files on their own whenever they need to. For Windows clients, this recovery is facilitated by integrating the File Store snapshots with the **Previous Versions** tab in Windows Explorer (see figure 12). For Linux/UNIX clients, users can restore the previous versions of these files from the .snapshot directory.

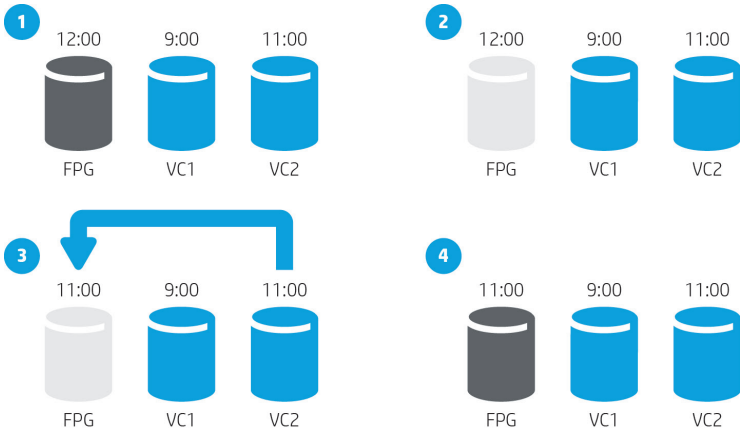
Figure 12. User driven file recovery



Administrator-driven recovery

Apart from user-driven recovery, HP 3PAR File Persona Software Suite also allows the Storage Administrator to recover the entire FPG using the HP 3PAR Virtual Copy technology, which is a crash consistent point-in-time snapshot of the entire FPG. This is useful for recovery of the FPG, in the event of a problem with the file system. The FPG will be rolled back to the previous point in time at which the Virtual Copy was created. This recovery will be an offline recovery, as the FPG has to be unmounted before the recovery starts. Figure 13 illustrates the process for an administrator-driven recovery for an FPG.

Figure 13. Administrator-driven recovery



Step 1: FPG corruption detected
Step 2: Forget (unmount) the FPG
Step 3: Promote the group Virtual Copy for the group of VVs making up the FPG to be recovered
Step 4: Recover (mount) the FPG to show up as active FPG and enable client access

Replication and disaster recovery

For the replication for File Persona Software Suite, HP 3PAR Remote Copy software is used in the same way for VVs for the File Persona as it is for VVs for the Block Persona, supporting Synchronous, Asynchronous Periodic and Synchronous Long Distance modes of HP 3PAR Remote Copy. All VVs in an FPG must be in a single Remote Copy group. The File Persona Software Suite supports 1:1, M:1 (many-to-one), 1:N (one-to-many), and M:N replication topologies for failover purpose only—not for distribution purpose as a read-only target.

For more information on how to configure Remote Copy, refer to the HP 3PAR OS Remote Copy software user guide and for disaster recovery process for File Persona Software Suite, refer to Replication and disaster recovery guide for HP 3PAR File Persona.

As a pre-requisite for disaster recovery configuration for File Persona Software Suite, the node networking, DNS configuration, Active Directory configuration, antivirus integration, scheduled tasks, etc. has to be set up manually on the remote array.

Backup and restore

HP 3PAR File Persona Software Suite supports network share-based backup over SMB or NFS protocol and NDMP over iSCSI-based backup. It supports the following software vendors for the backup and restore functions:

- HP Data Protector
- Symantec NetBackup
- CommVault Simpana
- IBM Tivoli Storage Manager

Note
For verifying the supported backup software versions compatibility and supported target backup devices, refer to the Single Point of Connectivity Knowledge (SPOCK) website at h20272.www2.hp.com.

System configuration backup
Each VFS keeps the configuration information of all File Stores and File Shares within it. This system configuration backup can be done at the VFS level in order to restore that configuration on another system to recreate the same VFS structure. The backup and restore process varies, based on the backup software being used. For more information on the backup and restore process, refer to the HP 3PAR Command Line Interface Administrator's Manual.

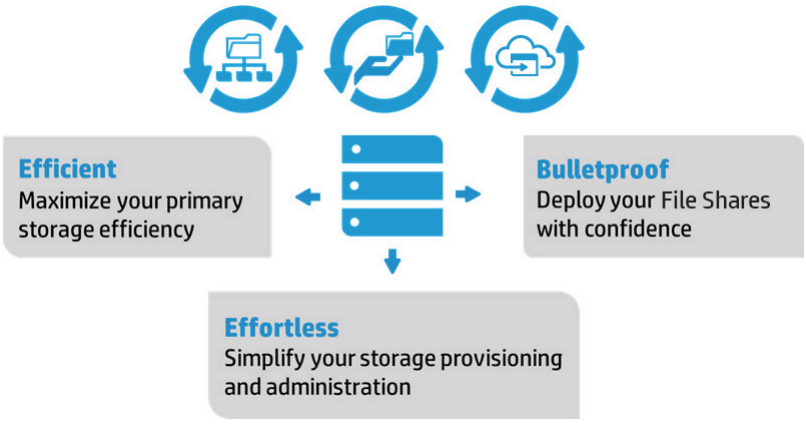
Support for the HP 3PAR data services

HP 3PAR File Persona Software Suite leverages data compaction technologies like HP 3PAR thin built-in zero detect and HP 3PAR Thin Provisioning to enable the efficient utilization of the storage resources. Built on the industry-proven autonomic disk foundation of HP 3PAR storage and to facilitate the right place for the right file data at the right time, it takes advantage of Adaptive Optimization and Dynamic Optimization. It leverages Adaptive Flash Cache for performance acceleration for the read-intensive workloads of the file sharing. It enables space and cost-efficient array-based snapshots (based on the FPG) by inheriting the Virtual Copy technology of the HP 3PAR StoreServ. HP 3PAR File Persona Software Suite health status is included in the HP 3PAR call home process to enhance support experience.

Conclusion

HP 3PAR File Persona Software Suite is a feature of HP 3PAR OS, which introduces native file services to the HP 3PAR StoreServ Storage system making it a truly converged block, file, and object access system, enabled by HP 3PAR OS and converged controllers. HP 3PAR File Persona Software Suite extends the workload reach of HP 3PAR StoreServ arrays to natively address client workloads in converged block and file opportunities. In other words, it is designed to address storage opportunities where customers are seeking to provide storage for both server workloads and client workloads from a single converged platform. Just as the default Block Persona is optimized for server workloads such as virtualization, database, and applications, the optional File Persona is optimized for client workloads such as home directory consolidation, group and department shares, corporate shares, and select custom cloud applications via the Object Access API.

Figure 14. Truly converged file and object access for the only primary storage you will ever need



Related documentation

HP 3PAR Command Line Interface reference guide

HP 3PAR StoreServ concepts guide

HP 3PAR StoreServ Management Console 2.0 Administrator Guide

HP 3PAR StoreServ Management Console Technical White Paper

HP 3PAR StoreServ Command Line Interface Administrator's manual

Antivirus scanning best practices guide for HP 3PAR File Persona

Replication and disaster recovery guide for HP 3PAR File Persona

For identifying storage system configuration specifications and compatibility information, go to the SPOCK website at h20272.www2.hp.com.

Learn more at
hp.com/go/3PAR/FilePersona

Sign up for updates
hp.com/go/getupdated

Share with colleagues

Rate this document

4AA5-6078ENW, December 2014, Rev. 1