HP 3PAR OS 3.2.1 MU2 Patch 08
Release Notes

This release notes document is for Patch 08 and intended for HP 3PAR Operating System Software 3.2.1.200 (MU2) Patch 08 (P08).

Acknowledgments

Intel®, Itanium®, Pentium®, Intel Inside®, and the Intel Inside logo are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Microsoft®, Windows®, Windows® XP, and Windows NT® are U.S. registered trademarks of Microsoft Corporation.

Adobe® and Acrobat® are trademarks of Adobe Systems Incorporated.

Java and Oracle are registered trademarks of Oracle and/or its affiliates.

UNIX® is a registered trademark of The Open Group.

Documentation

For the latest version of this document, go to http://www.hp.com/go/3par/, navigate to your product page, click **Support for your product**, and then click **Manuals**.

Contents

1 Overview of HP 3PAR OS

This release notes document describes the modifications and known issues for Patch 08. The application of this patch is intended for HP 3PAR OS 3.2.1.200 (MU2). This patch is intended to be installed on an as required basis.

Supported platforms

The HP 3PAR Configuration Matrix for HP 3PAR OS 3.2.1 contains information about supported hardware and software platforms. For additional information, go to the Single Point of Connectivity Knowledge for HP Storage Products (SPOCK) website: http://www.hp.com/storage/spock.

NOTE: If you attempt to install this patch on hardware platforms which are not supported, it will result in the following error:

```
Performing pre-update checks...This File Persona update is not intended
for this system class.Update failed.
```

Patch Details

- Patch Name: HP 3PAR OS 3.2.1 MU2 P08
- Prerequisite: The Service Processor must be at release level SP-4.3.0.GA-24 plus the latest SP patch
- This patch applies to: HP 3PAR OS Release 3.2.1.200 (MU2)

NOTE: This patch is not revertible.

NOTE: Applying this patch to the HP 3PAR OS will restart some of the affected OS components. With these restarts, events and alerts might be generated and this is an expected behavior. The system continues to serve data, but existing CLI or IMC sessions might be interrupted.

Included in this patch

HP 3PAR OS 3.2.1 MU2 P08 includes:

- Issue ID: None
- Description: Enable File Persona.
- Affected Packages: tpd-cli, tpd-fs, tpd-vmmgr, tpd-update, tpd-prerevert
- Obsoletes: None
- Requires: OS-3.2.1.200-MU2
- Build Version: 3.2.1.222

NOTE: HP recommends installing patches in the same sequence as they are released, unless instructed otherwise.

Affected components

Component	Version
CLI Server	3.2.1.222 (P08)
Software Updater	3.2.1.222 (P08)
File Persona	1.0.0.32-20150129 (P08)

NOTE: Remote CLI clients earlier than version 3.1.2 will not be able to connect to the HP 3PAR OS 3.2.1 MU2 or later.

Modifications to the HP 3PAR OS

The purpose of this patch is to enable File Persona feature of HP 3PAR OS.

As a licensed feature of the HP 3PAR OS, the File Persona enables a rich set of file protocols and core file data services on an HP 3PAR StoreServ system. It inherits 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 also include client workloads such as home directory consolidation, group/department shares, and corporate shares via the File Persona – all with truly Converged Controllers, truly agile capacity, and truly unified management.

The File Persona is supported on the HP 3PAR StoreServ 7200c, 7400c, 7440c, and 7450c systems. It provides the following features:

- Rich file protocols including SMB 3.0, 2.1, 2.0, and 1.0 plus NFSv4.0, and v3.0

- Object Access API via a REST API for cloud applications

- Transparent failover for clients via SMB 3.0 and NFS

- Performance acceleration leveraging Adaptive Flash Cache

- Data compaction via Thin Provisioning

- Data optimization via the separately licensed Adaptive Optimization and Dynamic Optimization

- Point-in-time File Store snapshots

- Support for third party antivirus software, network share and NDMP-based backup/restore

- Disaster recovery replication via the separately licensed Remote Copy

- Security of FIPS 140-2 validated Data At Rest Encryption when using self encrypting drives

- Active Directory, Folder Redirection, Offline Files, Roaming User Profiles, DFS-Namespace, and Microsoft Management Console for Microsoft-based IT infrastructure

- LDAP and local user authentication for Linux-based IT infrastructure

- 3PAR StoreServ Management Console (SSMC) GUI with a performance dashboard, custom reports capability and the 3PAR OS CLI

Known issues with the OS

Issue ID	Description
116147	If a non-standard MTU size is configured, it must be configured again after enabling File Persona on additional nodes in the system.
122094	When HP 3PAR OS is upgraded to version 3.2.1 MU2 P08 and File Persona is configured, you cannot revert to previous HP 3PAR OS version.
123354	If a controlmag operation is used to bring PDs offline, it might impact FPG (File provisioning Group) VVs and in turn affect FPG availability. Such controlmag operations must be done carefully. Identify any impact to FPGs and deactivate those FPGs before any PDs are brought offline. Failure to do so might cause commands such as `showvfs` and `showfstore` to fail even after the PDs are brought online.
123570	An FPG is allowed to be activated even when shortage of disk space may deactivate it shortly thereafter. If the free disk space in a CPG associated with an FPG falls below 60 GB, the FPG is automatically deactivated. The `setfpg -activate` CLI command allows the FPG to be reactivated even if there is less than 60 GB of free space in the CPG. That can result in the FPG getting deactivated shortly

Issue ID	Description
	thereafter. To prevent this, additional storage must be provided before reactivating an FPG that was deactivated due to space shortage.
125281	When patches are required to be included in the "all nodes down"/"SP-to-Node" rescue image, do not perform SP-to-Node rescue from spmaint. Call HP Support for assistance in rescuing the system. Specifically, if File Persona was active and the system needs to have an "all nodes down" rescue, call HP Support.

Known issues with the File Persona package

The following issues are related to File Persona.

Issue ID	Description
35971, 53639, 53718	The '^' character is not supported in File Persona 1.0 for HP-SMB user and group names. When HP-SMB name searches are performed on names containing this character, the character is replaced with a space character internally. For example, `user^name` is changed to `user name` in HP-SMB. HP-SMB recommends not to use the '^' character as a legal Windows name character because it is interpreted as a space character causing name searches to fail unexpectedly or be resolved to an unintended name. HP-SMB does not provide an exported configuration interface to change the space replacement character to a different value for File Persona.
37406, 37422	SMB and FPG read and write statistics reported in the `statfs` command do not account for the data transferred via ODX.
37975	Restarting HP SMB server multiple times in quick succession causes daemon to get stuck, if Active Directory cache contains large number of entries. This occurs when the HP SMB server is stopped while the Active Directory cache is still being loaded. Workaround: To resolve the issue, call HP support.
38232	When a VSE (Virus Scan Engine) goes down, an attempt to connect to the VSE might cause a delay of a minute or more before returning with failure message. All the reads or scans triggered during the period wait before being served according to VSE unavailable policy.
38407	The HP-SMB Active Directory (AD) cache caches user/group names and associated IDs. LDAP and local provider names are not cached by File Persona. HP recommends that administrators perform membership changes at non peak hours or ask impacted users to exit and login again after the cache is updated.
43723	Setting hard storage usage limit for a roaming profile user, and then exceeding the quota might lead to a loss of data synchronization between the Windows client and the SMB share.
48667,	NFS clients can enumerate exports from all Virtual File Servers through any of the Virtual File Server IPs active on a given node. Connect to the exports through the IP address specifically associated with a given export's Virtual File Server. Otherwise, it will lead to failures in migration of FPGs using the `setfpg -primarynode` and `setfpg -failover` commands.
49563	Concurrent operations to update and query local user or group information need to ensure automatic transactions. Avoid modification to local user or group during the local authentication. Retry the authentication if it fails during parallel administrative operations.
50592	When reaching a maximum limit, the behavior for the last written file hitting the limit varies by protocol.
51034	LDAP lookup failures might not provide correct file owner when looking up file owners. Workaround: To resolve this, clear the keying with the `nfsidmap -c` command on the client.
51653	All exports from the NFS server perspective are per node, not per Virtual File Server (VFS). The administrator must configure the client properly for VFS separation. Do not use the Linux `showmount -e` command but use the output of the 3PAR admin tools. For NFS clients, do not use automount with a host map.

Issue ID	Description
52014	For systems with a large number of FPGs, VFS IP addresses, and shares; changing the current owner of a set of FPGs to a new node can involve shutdown, relocation, and bring up and initialization of a lot of pieces and a large amount of state. For SMB3 clients using persistent handles, persistent handle file state is maintained for seamless failover so they can continue from their previous state. The timeout for how long the client will keep trying to reconnect to a persistent handle and how long the server maintains state waiting for a client reconnect is 5 minutes. Heavily loaded and heavily configured systems whose FPGs take more than 5 minutes to complete failover operations causes loss of persistent handle state on the SMB3 clients.
52387, 55268	Under scenarios where a significant block workload exists, FPGs (File Provisioning Group) for a node may be automatically migrated to the partner node. This can lead to a temporary disruption in client access, depending on the protocols in use. The load on the system must be reduced either through the addition of more hardware (disks/nodes) or by the reduction of client workload. The FPGs must be returned to their primary node using the `setfpg -failover` command. For the purposes of this issue, significant block workload is defined as either of the following: • Service times of greater than 150 ms, as reported by the `statvlun` command • Occurrences of delayed acks (DelAck), as reported by the `statcmp` command
52463	An internal cache in one of the system processes gets full after creating 16 FPGs. The process is automatically restarted and no manual corrective action is required.
52602	Adding Local user and group names that match with known SID (Security Identifier) names might lead to unexpected results. Well-known names are checked and resolved before Local names regardless of the provider load order. Well-known SID names are not reported in user and group enumeration reports.
52603, 54198	When an VFS (Virtual File Server) does not have any VFS IP address assigned to it, none of the SMB shares on it are accessible by clients. However, the enumeration of shares by the 3PAR management GUI can see inconsistent lists of shares in cases where VFS exists but has no IP address associated with it. You can use the 3PAR management GUI to add a new SMB share on VFS with no IP address on it. This newly added SMB share is seen in the enumeration, but other shares are invisible until an IP address is added to the VFS. If HP-SMB is restarted or rebooted, VFS shares without IP addresses are seen. SMB never presents anything inconsistent to SMB clients since they can only access the shares by an IP address. The inconsistent share list is only visible to the 3PAR management GUI, and it becomes fully consistent again when an IP address is added to the VFS.
52686	To rename a file where the characters in the file name only differ in case (for example, file.txt to FILE.txt): 1. rename file.txt temp 2. rename temp FILE.txt NOTE: SMB is not case sensitive but it preserves case so the file `file.txt` is the same as `File.TXT`.
52700	If the external network link is down on the backup node for an FPG when the current node has a failure, the FPG will still be failed over. This scenario can occur if the nodes are attached to only a single switch and the switch goes down or when all network links on a backup node are down at the time a failover is being processed. Workaround: After the network links are operational again, to bring the FPG command back to its proper owner, issue the `setfpg -failover` command .
52920	If the external network link is down during FPG activation, VFS IPs are not automatically activated when the link gets operational. This condition might likely occur either during boot time or during failover time. Workaround: After the link is operational, if you can not ping the VFS IP, deactivate the FPGs and activate them again using following commands: • `setfpg -deactivate` • `setfpg -activate` To fail over to the partner node, use the `setfpg -failover` command. If the link is operational, the network activation is successful now.

Issue ID	Description
53581, 40025	Cross protocol access to file stores is not supported, although it is permitted by the HP 3PAR OS software. Avoid cross protocol access to file stores to prevent unexpected behavior.
53617	When using Symantec VSEs, attempting to scan files larger than 2 GB may cause the scan engine to be reported as DOWN. To avoid this issue, set a policy to exclude scanning of files larger than 2 GB using the `excludesize` option of the `setfsav pol` command.
53648	Unexpected failover of FPGs may occur while running a maximum intensity benchmark workload. If this occurs, an alert is generated. The FPGs must be failed back to their original node with the `setfpg -failover` command.
53711	During failover/failback, on few occasions, some client applications which do not have any IO retries might disconnect due to a transient stale handle condition. This might require the client application to reconnect even though the failover/failback completes successfully. Any new client applications connecting to the mount point does not face any problem accessing the mount point as the mount point is restored upon failover/failback with no issues.
53736	File create/delete operations on NFSv4 take approximately twice as long as on NFSv3.
54357	When a group name in LDAP matches a built-in group name, the fully qualified name of the built-in group is required to modify members from the GUI and CLI when Local is stacked after Ldap in the provider stacking. This is because the name services resolve the name in Ldap before Local, causing the member change to fail if the domain portion of the name is not included.
54480	After a power failure, some FPGs might not be activated automatically. After the VVs supporting the FPG are in a normal state, manually request activation of the FPG through SSMC or by using `setfpg -activate <fpgname>` command.
54549	Depending on the network infrastructure, synchronous network I/O connections might reset in the event of failover before completing the failover operation.
54903	The configured LDAP server for use by File Persona may become unreachable from a subset of the nodes. If this occurs, and users are unable to authenticate to shares exported from a FPG activated on such a node, this may be recovered by issuing a `stopfs <node>` request followed by a `startfs -enable <node>` request to restart File Persona services for that node. After restarting the File Persona services, the affected FPGs must be moved back to their assigned node with the `setfpg -failover` command.
54946	Changing a VFS IP to an address which is already in use on the network (failing duplicate address detection) results in an error claiming that the address is already in use in the cluster, and an inconsistent state for that address. The recovery is to remove that address and add it again with the correct value.
55554	When a large VFS configuration containing many shares, quotas, or other configuration elements is restored with the `restorefsconf` command, the command will timeout if the restore takes more than 90 seconds to complete. The restore operation continues in the background and might still complete successfully. Confirm that the restore has completed successfully using various `show*` commands such as `showfshare`.
55669	Deactivation of an FPG containing Object Access API shares results in a short disruption to all Object Access API shares for that node. This can be triggered by the use of the deactivate, failover, or primarynode options to the `setfpg` command. Retry any data transfers that are temporarily disrupted during this operation.
55757	Reducing the number of enabled File Persona nodes from 4 to 2 and then increasing the number of enabled nodes back to 4 results in failures in the `createvfs` command and InSplore collections. To resolve this issue, contact your service provider. Alternatively, disabling File Persona for all nodes, and then enabling File Persona again resolves this issue. This option requires reconfiguration of global File Persona settings.
55760	Use of the Object Access API with LDAP authentication can lead to instability, and is not currently supported.

Addendum to User Documentation

The following items are meant as a supplement to the other available user documentation to provide clarifications to the behavior of the File Persona.

Issue ID	Description
43509	If an user runs ROBOCOPY on a shared SMB folder containing child objects with inherited ACLs, the user must be a share admin. To add a user as a share admin, add the user to BUILTIN\\Administrators group by using the following command: `setfsgroup -memberlist +<MyDomain>\\john1 Administrators`
47144	HP's storage platform has high-availability features such as shared storage accessible from both failover partners and a reliable network connection between the partners. These features, along with HP SMB server software, make it capable of hosting shares which are classified as Continuously Available, and therefore it can support the SMB 3.0 specified share property called Continuous Availability (CA). Windows MMC (Microsoft Management Console) does not know about the HP storage platform CA support. When MMC creates shares, it does not mark the new share as a CA share. SMB3 Clients accessing the share check for the CA property, and if it is not found then the SMB3 Persistent Handles feature is not used. Workaround: To support SMB3 Persistent Handles on a share created by MMC, go to the product's 3PAR SSMC or CLI and turn on the "Continuous Availability" property of the share.
47659	FPG names are limited to containing alphanumeric characters and underscores.
50125	A directory created by the `createfshare nfs` command has Administrators as the group owner by default. Solaris does not have Administrators group by default. Therefore, the user can change the group owner to root, by mounting the NFS share in NFS version 3, and executing the `chown root:root mydirectory` command.
50650	When using HP-SMB, set appropriate permissions for each individual users if desired. When running FSCT (File Server Capacity Tool) , appropriate permissions are required or FSCT prepare server step will fail with following error "Error setting permissions.
51218	When using the Object Access API, the `chmod`, `chown`, `chgrp`, and `ls` commands have super user privileges with the local Administrator account. To perform other operations like `rmdir` on files where the administrator does not have sufficient access, a `chmod`, `chown`, or `chgrp` command must be issued first for the object and then operate on it.
52444	Privileges are not utilized from Active Directory users of SMB. Privileges like Bypass-Traverse are not preserved. Workaround: If privileges are needed for backups, HP recommends to use an Administrative account placed in the built-in Administrators or Backup Operators group on the SMB server.
52707	UID and GID assignment must begin at 1,000.
52933	NFSv4 ACL attributes do not enumerate in the same order as they are set.
52969	The automatically created `.admin` file store is for use by functions such as configuration backup, antivirus quarantine management, and quota import/export. Create shares only for these specific uses within the `.admin` file store, and not for general file storage.
53437	Files and folders might become stranded if they are owned by an unmappable GID. When this happens, the ACLs for such folders and files might need modification to allow an admin or other user to clean up the files. However, when the Linux GID for the file's group is not resolvable, the ACL setting GUI in Windows clients encounters errors trying to modify the ACL on the file/folder. Workaround: An SMB share administrator can change the file's group to a legal group. This can be done by overwriting the entire ACL with one that has a good group. To do this: 1. Make a directory or file with a good GID and ACL. This can be done in explorer, CMD, or powershell. `PS C:\> mkdir z:\new_good_dir` 2. Set the ACL of the stranded directory to be a copy of the ACL from the good directory:`PS C:\> get-acl -path Z:\new_good_dir	set-acl -path <stranded directory parh>`

Issue ID	Description
53688	If both the client and the array are not in a domain, a Windows 8 or Server 2012 client will not be able to successfully modify folder security on shared folders. Workaround: Use a client running another OS such as Server 2003 or Server 2008 to modify the folder security.
53713	The account with full control permissions can manage the share permissions and the NTFS file permissions. Administrators are not given a special bypass of `allowperms` on a share. Only users/groups which have share `allowperm` permissions will be able to access the share.
53715	By default, LDAP users are unable to access NFS exports. Workaround: After creating a share directory, create an export with no_root_squash. Mount it as root and use chmod/chown/chgrp to modify permissions. This no_root_squash export can be created with an allowed IP list of a single client to reduce any security impact.
53721	The default load order (provider stacking order) is set to AD, Local. This is expected to be the primary order for the vast majority of the customers. HP recommends using the default load order to minimize issues. To enable LDAP authentication: 1. Configure Ldap 2. Add Ldap to the provider stacking order To disable LDAP authentication, do one of the following: • Delete Ldap configuration • Remove Ldap from the provider stacking order However, not removing Ldap from the load order might cause unintended behavior. For efficient name resolutions, include only those providers in the load order that are expected to resolve names. The Local provider is always required since BUILTIN names are resolved by the Local provider. Configure the load order based on the expected usage of the name services included in the load order. Configure highly used services first to optimize the performance of name resolutions.
53724	There is a difference in behavior between NFSv4 and NFSv3 client mounts while mounting from clients that are not in the allowed list for the exports. NFSv3 prevents the mount from going through, NFSv4 clients is allowed to mount as the top level Pseudo Root has mount permissions for every one to allow them to browse the exports available like an auto mounter. But while trying to access the exports from those clients, the attempt to access the export is denied.
53727	NULLDACL not supported. Workaround: A NULLDACL means that the file is open to everyone. To do this, create an Everyone ACE and give Everyone full permissions.
53730	File Persona settings outside of the Virtual File Server need to be manually restored in a bare metal scenario. The configuration backup/restore process covers the preservation of the virtual file server data. However, the feature does not cover any of the system level configurations made with `setfs` or the virus scan engines configured with `setfsav vse [+|-]`. These need to be reconfigured manually in a bare metal restore scenario or when setting up a DR site. The information to be set with these commands can be obtained through the corresponding `showfs` commands. The AV (Anti-Virus) information can be obtained via the `showfsav` command.
53733	Duplicate users in multiple configured authentication providers are not supported.
53896	Shares cannot be MMC managed from array computer account. Use the VFS IP address or its corresponding DNS name.
54116, 55210	While using upload file API feature, the maximum upload file size is 35 MB.

Issue ID	Description
54280	You can make an NFSv3 mount of a file system that contains NFSv4 ACLs. This combination exhibits the following behavior: • The NFS server grants or denies data access based on the NFSv4 ACLs • The NFS client cannot view or manipulate the ACLs directly. • If the mount is made with the acl option (noacl is the default), the NFS client can manipulate AIXC (AIX Classic) ACLs, but cannot manipulate NFSv4 ACLs.
54342	The File Persona represents file streams internally as independent files, which require some overhead to manage. When the antivirus is enabled, the performance of stream based operations might reduce further.
54671	When running an on demand or scheduled virus scan of a large set of files, the expected processing rate is no greater than 2 million files per day, depending on load.
54867	NFSv4 supports browsable pseudo root file system to support the use case of browsing the file system to find the exports to mount and mount. The pseudo root file system is exported "ro" so all the exports underneath can be browsed and mounted. If there are unexported directories underneath the psuedo root file system, the clients will be able to mount "ro" as the pseudo root file system is mounted "ro" to allow every one to browse. However if the client tries to access the unexported file system, the client will not be allowed to access as expected.
55517	For use with NDMP, each node in the cluster has a separate IQN. Listing of cluster IQNs list IQNs for all the nodes with their node name and per node IPs. Create and assign VTLs per node. For restoring data, modify/update the initiator IQN in VTL after FPG failover and failback.

Client OS Behaviors and Limitations

The following items are meant to capture issues seen on clients communicating to File Persona shares.

Issue ID	Description
52465	The RHEL 6.5 operating system does not support mounting of NFSv4 over UDP.
53241	Minimum version of VDU kernel to be used is version 2.6.32-504 when using Anti-virus software.
53494	When mounting in NFS version 4, the commands `ls -l` and `ls -v` in Solaris 10u10 give the error : Permission denied. To read the ACL of a file in NFS share, execute the `getfacl`command.
53621	The NFS Version 4 protocol supports NFSv4 style ACLs. 3PAR File Persona uses its own underlying file system to support NFSv4 ACL functionality. Solaris NFSv4 full featured capability however requires that ZFS be used as the underlying file system on the NFSv4 server. Consequently, the Solaris 11 NFSv4 ACL manipulation is supported with restrictions on 3PAR File Persona. Solaris NFSv4 chmod/ls commands are used to manipulate NFSv4 ACL's. Please refer to the 3PAR Solaris Implementation Guide for specific details.
53683	In NFS client version 2.6.32, create file fails with "Input/Output Error" if the size is more than quota limit. For other Linux versions such as RHEL 5.8 2.6.18 and CentOS 6.5 2.6.32, error message "Disk quota exceeded" is displayed when the file size exceeds allowed quota size.
54176	NFSv4 ACL commands are not supported by 3PAR File Persona for Solaris 10.
54201	Solaris does not support use of POSIX ACL commands from Solaris clients to manipulate NFSv4 ACLs.
54218	SuSE SLES 10 client does not support NFS4 ACL.
54219	HP-UX 11iv3 (11.31) is the only version of the HP UNIX Operating System that supports NFSv4. HP-UX NFSv4 clients only support POSIX ACLs and do not provide the necessary tools for NFSv4

Issue ID	Description
	ACL manipulation. When users need to manipulate ACLs, HP recommends mounting the 3PAR File Persona NFS shares with NFS version 3 and using the native HP-UX POSIX ACL commands.
54274	During manual fail over of StoreServ controller node FPG ownership by using setfpg command, NFS connection renewal is observed occasionally at failover on both Solaris 10 and 11 clients. Manual failover actually goes through and the clients stay connected to the NFS shares

Verifying the patch installation

The installation of Patch 08 can be verified from an interactive CLI session. Issue the CLI command `showversion -a -b` to verify that Patch 08 is listed.

```
cli% showversion -a -b
Release version 3.2.1.200 (MU2)
Patches:  P08

Component Name                  Version
CLI Server                      3.2.1.222 (P08)
CLI Client                      3.2.1.200
System Manager                  3.2.1.200 (MU2)
Kernel                          3.2.1.200 (MU2)
TPD Kernel Code                 3.2.1.200 (MU2)
TPD Kernel Patch                3.2.1.200 (MU2)
CIM Server                      3.2.1.200 (MU2)
.
.
.
Software Updater                3.2.1.222 (P08)
.
.
File Persona                    1.0.0.32-20150129 (P08)
```

NOTE: When displaying the `showversion` command output from the Service Processor, the CLI Client version is fixed in the SP code, and might differ from the output displayed from any other system.