Hewlett Packard
Enterprise

Replication and disaster recovery guide for File Persona

HPE 3PAR OS 3.3.1 MU1

Technical white paper

Contents

Introduction to disaster tolerance for the HPE 3PAR File Persona Software

As organizations increasingly depend on business-critical file data services, data protection and recovery are essential for everyday business operations, especially during major failures or disasters. Customers consider various technologies and strategies for protecting, and reliably recovering their business-critical data in a timely manner. The main factors for selecting technologies are cost of downtime, backup windows, maturity of technology and many more.

HPE 3PAR StoreServ as a unified storage offering provides fast, efficient and reliable block storage for application workloads and with its File Persona Software feature, rich file data services for user home directories, collaboration and data governance use cases. Using the same robust data protection technologies used for block data services, File Persona file shares are securely stored and protected against file system corruption, accidental deletion of files and folders, and disasters.

One of the key technologies used to enable disaster tolerance for block volumes and file shares is the HPE 3PAR Remote Copy feature. It can be used with the HPE 3PAR File Persona Software to replicate File Provisioning Groups (FPGs) to another HPE 3PAR running File Persona. Additional technologies with autonomous high-availability, client-accessible file system snapshots, NDMP and share backups, and HPE Recovery Manager Central integration complete the data protection feature set to enable highest availability levels for File Persona file shares.

While there are multiple aspects to protecting File Persona file shares, this technical white paper provides an overview of how the HPE 3PAR software features Remote Copy and Virtual Copy can be used with File Persona to enable disaster tolerance and disaster recovery.

Audience for this paper

A technical audience will gather an understanding of the data replication options for File Persona file shares using the Remote Copy software features. This paper assumes familiarity with the concepts and the deployment of file storage solutions and HPE 3PAR Remote Copy. Contact your HPE representative for more information on how to apply the information presented in this paper in your environment.

HPE 3PAR File Persona architectural overview

The HPE 3PAR File Persona Software is built upon the resilient Mesh-Active architecture of HPE 3PAR StoreServ and benefits from the HPE 3PAR storage foundation of wide-striped logical disks and autonomic Common Provisioning Groups (CPGs). A single CPG can be shared between file and block to create file shares or logical unit numbers (LUNs) to provide true convergence without dedicated or stranded pools of capacity for block or file.

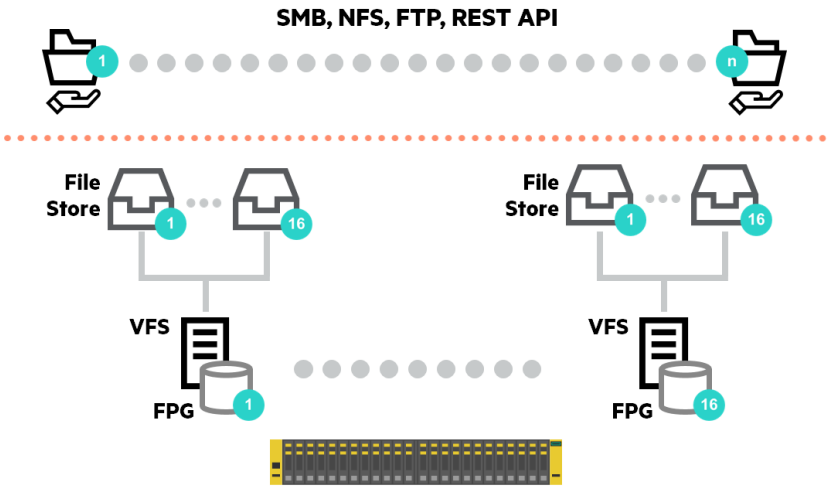

Figure 1. HPE 3PAR File Persona architecture

Figure 1 highlights File Persona's core architecture, which consists of the following components:

- **File Provisioning Groups (FPGs):** An FPG is an instance of the HPE intellectual property Adaptive File System. It controls how files are stored and retrieved. Each FPG is transparently constructed from one or multiple Virtual Volumes (VVs) and is the unit for high-availability, replication and disaster recovery for File Persona file shares. A node pair of HPE 3PAR StoreServ supports up to 16 FPGs.
- **Virtual File Servers (VFSs):** A VFS is conceptually like a server. As such, it presents up to four virtual IP addresses to clients, participates in user authentication, and can hold policies for user and group quotas or virus scanning policies. There is a one-to-one relationship between FPGs and VFSs, which means up to 16 VFSs can be created on an HPE 3PAR StoreServ node pair.
- **File Stores:** A File Store is a slice of a VFS and FPG that allows defining different snapshot policies, capacity quotas, customized virus scanning policies, and File Lock policies, in addition to enforced ACLs and their inheritance with NTFS or Legacy security modes to customize a file system for a particular use case.
- **File shares:** A file share provides data access to clients through the SMB, NFS and FTP protocol, as well as the Object Access REST API. Multiple file shares can be created for a File Store and at different directory levels within a File Store.

As highlighted in the architecture description, the foundation for FPGs is one or multiple Virtual Volumes. Therefore, most block data services provided for Virtual Volumes are available for FPGs as well. These data services include Virtual Copy snapshots for local recovery of entire FPGs and Remote Copy for enabling disaster tolerance through replication, which are the subject of this technical white paper.

Important
While Remote Copy replication provides a secondary copy of the data, it does not alleviate the need to perform regular backups.

Planning for replication

Configuration of Remote Copy and its associated features is performed using the HPE 3PAR StoreServ Management Console (SSMC) and the HPE 3PAR Command Line Interface (CLI). While most replication related commands are available through SSMC, there are some specific File Persona related operations that require the use of the CLI. A comprehensive explanation of Remote Copy in general is provided in the technical white paper Disaster-tolerant solutions with HPE 3PAR Remote Copy.

Although most examples provided in this technical white paper provide sufficient information to configure replication for File Persona file shares, refer to the latest HPE 3PAR documentation for details.

Authentication considerations

File Persona authentication requires the local user authentication provider to be present in the authentication provider stack to allow administrator access to file shares if external authentication are unavailable. The local user database is not automatically synchronized with Remote Copy and requires manual intervention. Any modifications in the local user database on either a primary storage system (system1) or its backup storage system (system2) need to be manually synchronized to ensure user access after a failover.

Recommended practice is to use an external authentication provider, Lightweight Directory Access Protocol (LDAP) or Active Directory Domain Services (AD DS), for user access wherever possible. Only default administrative users and groups in the local authentication provider are then used as a safety measure. This eliminates the need of manual synchronization of local users and groups in a replicated environment and ensures continued access for users to files and folders stored on File Persona.

Note
Configuring authentication with AD DS, LDAP and local users on the backup storage system (system2) is ideally performed before the actual failover, to minimize downtime during disaster recovery.

Replication mode

Remote Copy, the replication technology used by File Persona, supports both asynchronous periodic—a snapshot based replication mechanism—as well as synchronous replication modes in a unidirectional or bidirectional configuration. Selection of replication mode mainly depends on intended recovery point objective (RPO) and available network infrastructure, specifically latency is a determining variable. Please refer to the HPE 3PAR Remote Copy Software User Guide for details on selecting an appropriate replication mode.

Networking considerations

In environments with differing IP addressing schemas in the primary and backup data center, Virtual File Servers (VFS) can be preconfigured to support both the primary data center addressing schema and the backup data center IP addressing schema. It is highly recommended to preconfigure the VFSs with the IP addresses of both the primary and the backup data center IP addresses initially. This expedites the failover process significantly and reduces downtime. An example scenario is depicted in Figure 2, where an example VFS "VFS 1" is configured with two IP addresses. IP 1 is online in the primary data center and IP 2 is not connected. After a failover to the backup data center IP 2, which is configured to comply with the backup data center IP addressing schema, becomes online and IP 1 remains offline.

Alternatively, IP addresses can also be modified and adjusted to the backup data center IP addressing schema after a failover. Please refer to Adjusting VFS IP addressing on backup storage system for details on the manual process.

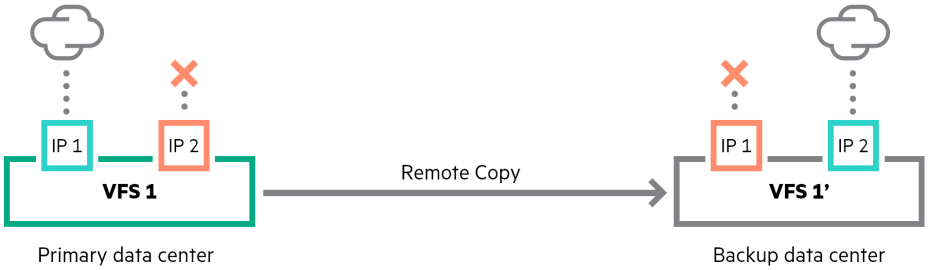

Figure 2. VFS configuration with different IP addressing schemas in the primary and backup data center.

Another factor to consider for replication is the use of fully qualified domain names (FQDNs). If the environment is set up that clients use FQDNs to connect to VFS IP addresses, three options can be considered for ensuring continued access to file shares hosted on a replicated VFS:

1. Adding VFS IP addresses and new FQDNs for the backup storage system (system2) to the Domain Name System (DNS) and inform clients to connect to the new FQDNs. Configuration of the VFS IP addresses and FQDNs with DNS for the backup storage system (system2) can be done prior to a planned or unplanned failover. Clients will however need to be notified after the failover to use the new FQDNs of the backup storage system (system2) which is disruptive.
2. Modification of original DNS entries for the primary storage systems VFS IP addresses (system1) to resolve to the VFS IP addresses of the backup storage system (system2) after a planned or unplanned failover. Clients will be able to mount file shares using the same FQDN.
3. Providing the VFS IP addresses on the backup storage system (system2) to clients. Clients will need to be notified to use IP addresses instead of FQDNs, however no alteration of FQDNs in DNS is required.

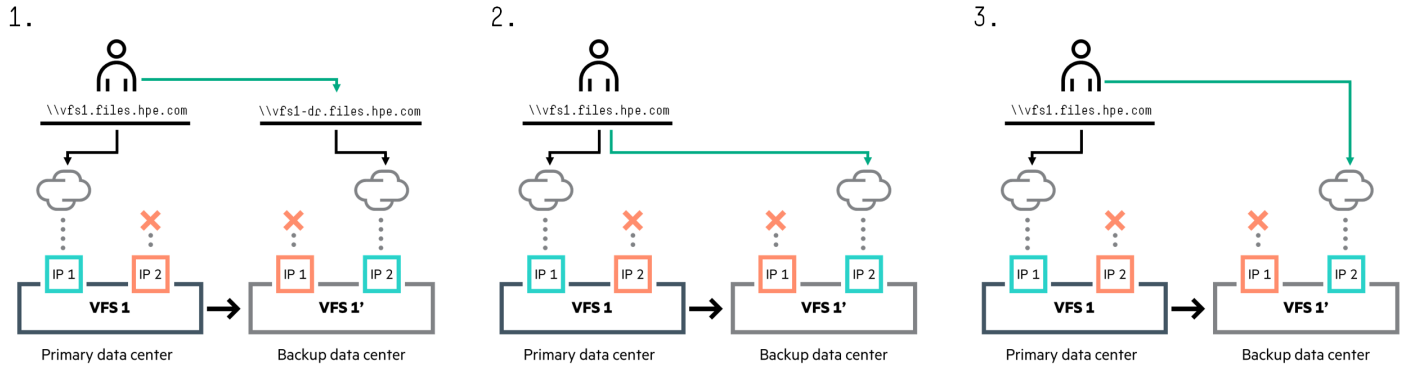

Figure 3. FQDN adjustment scenarios in DNS.

Each option is a valid solution to ensure clients are able to connect to file shares for replicated VFSs in a failover scenario. Consider each option and its associated procedure before implementing a solution to ensure that business availability and uptime requirements are met.

Note
This procedure is only required where the IP addressing schema in the primary data center differs from the schema in the backup data center.

File Provisioning Group name collisions

Replication using Remote Copy is done on the Virtual Volume level. One or more Virtual Volumes are used to build an FPG that contains a VFS, multiple File Stores, file shares and user data. There are no checks in-place to verify if the backup storage system (system2) contains FPGs that have conflicting names with the primary storage system (system1). In case of a name collision, i.e., the backup storage array (system2) contains an FPG with the same name as a replicated FPG on the primary storage system (system1), the replicated FPG cannot be mounted for disaster recovery purposes and SMB or NFS shares are not available on the backup storage system (system2) after a failover as depicted in Figure 4.

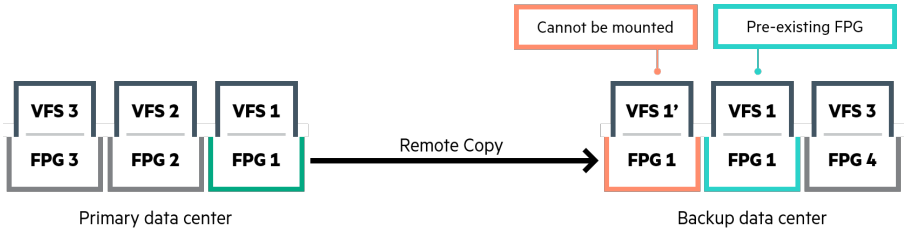

Figure 4. Example FPG name collision in a replicated environment.

Carefully name your FPGs on the primary storage system (system1) and verify there are no conflicting FPG names defined on the backup storage system (system2).

Configure Remote Copy

The backup storage system (system2) should be configured with similar settings as the source storage system (system1) prior to setting up Remote Copy. Table 1 lists File Persona configuration items that must match on both systems to ensure proper operation after a failover.

Table 1. File Persona configuration items that require manual adjustments on the backup storage system.

Configuration item	Comments
Authentication • Active Directory • LDAP • Local	If local users or groups have been modified, the altered accounts on the source system (system1) must be synchronized with the backup system (system2). This is because local user and group accounts are not replicated using Remote Copy. Use the CLI command `createfsuser` or the SSMC to create the local accounts on the backup storage system (system2).
Authentication Provider Stacking	Although not mandatory, best practices suggest to use the same authentication provider stacking order on both the primary and backup storage system.
Identity mapping settings • RFC2307 • Local user mapping • NFSv4 ID Mapping	To ensure proper authentication and authorization when cross-protocol access is in use, the same user mapping settings are to be used in both the primary and the backup storage system.
NDMP	NDMP and backup ISV settings are not replicated and need to be manually configured on the backup storage system (system2) if required.
Antivirus	Antivirus settings are not replicated and need to be manually configured on the backup storage system (system2) if required.
Snapshot schedules	Snapshot schedules are not replicated and need to be manually configured on the backup storage system (system2) if required.

Remote Copy using RCIP

File Persona can use either Fibre Channel or IP as the transport for replication. For this technical white paper, Remote Copy over IP (RCIP) is used and only a high-level summary of the configuration steps is provided. Therefore, the ports 0:3:1 and 1:3:1 are used in this paper. For details on cabling and configuration for other configuration options, please refer to the HPE 3PAR Remote Copy Software User Guide.

Configuration of replication ports

Use the SSMC to assign IP addresses to selected Remote Copy ports on both the primary storage system (system1) and the backup storage system (system2). In the SSMC, select **3PAR StoreServ** > **Ports** > **Port ID** > **0:3:1** > **System {primary/backup storage system}** > **Actions** > **Edit** and complete the port dialog box as depicted in Figure 5. For the IP address, chose a unique value on a single subnet. Repeat this procedure for port 1:3:1 on both storage systems.

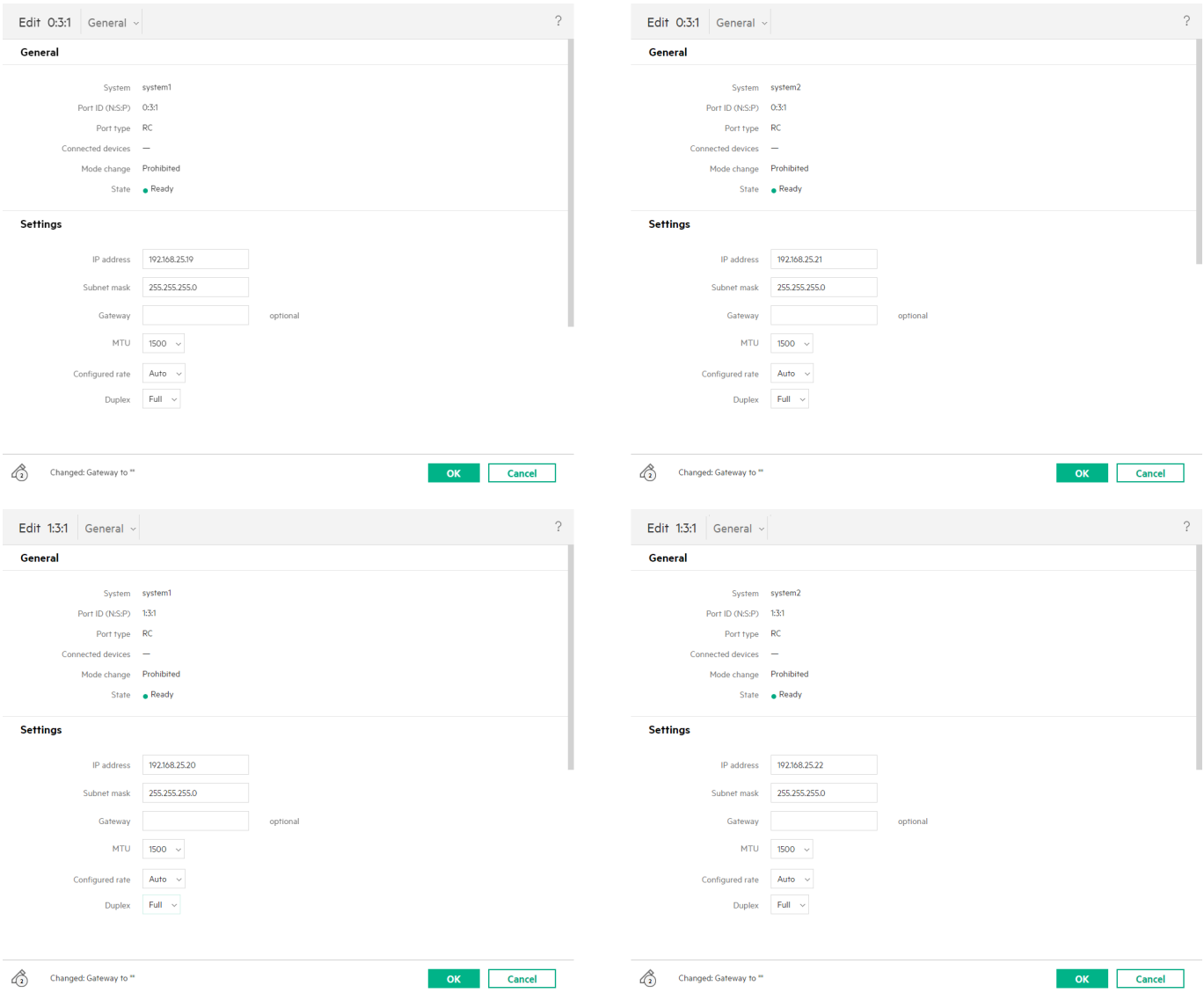

Figure 5. Example port configuration on primary storage system (system1) and backup storage system (system2).

Enable Remote Copy

In the SSMC, open the main menu and select **Show all** to display the Remote Copy configuration section. Select **Remote Copy Configurations** > **+ Create Configuration** and complete the dialog box to enable Remote Copy between the two storage systems.

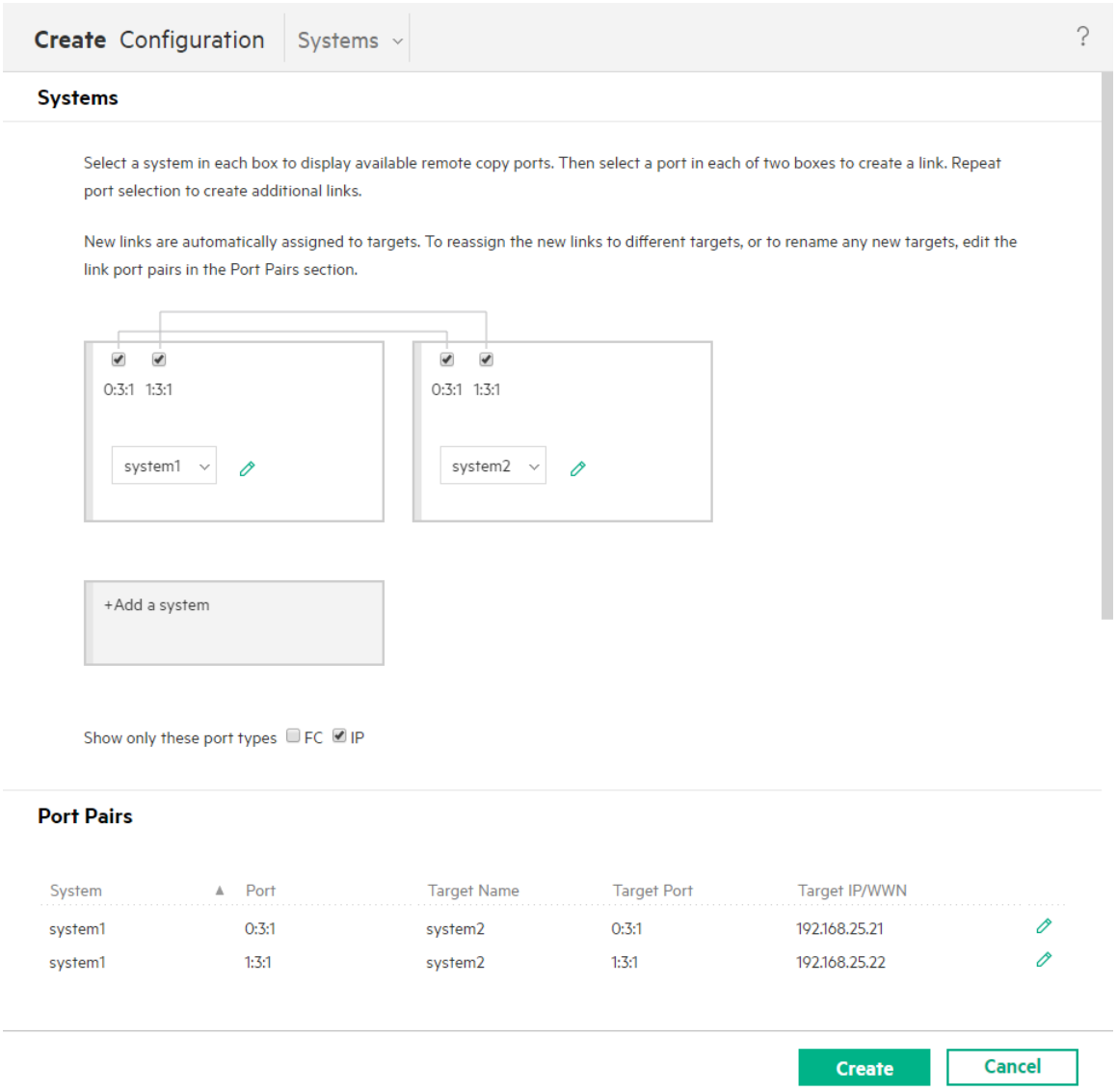

Figure 6. Create Remote Copy configuration example dialog.

Note

Verify the Remote Copy status of both the primary storage system (system1) and the backup storage system (system2). Ensure that the link status is up on all ports. Verify using the SSMC by navigating to **3PAR StoreServ** > **Remote Copy Configurations** > **Links.**

Create Remote Copy Group

A Remote Copy Group defines the replication relationship of one or more Virtual Volumes between the storage arrays and their mapping from source volumes to target volumes. It is recommended that a separate Remote Copy Group is created for every FPG that will be replicated in order to failover and failback the FPGs individually.

Create a Remote Copy Group to replicate the volumes for the FPG from the primary storage system (system1) to the backup storage system (system2) using the SSMC by navigating to **3PAR StoreServ** > **Remote Copy Configurations** > **+ Create Group**. Complete the dialog box as depicted in Figure 7.

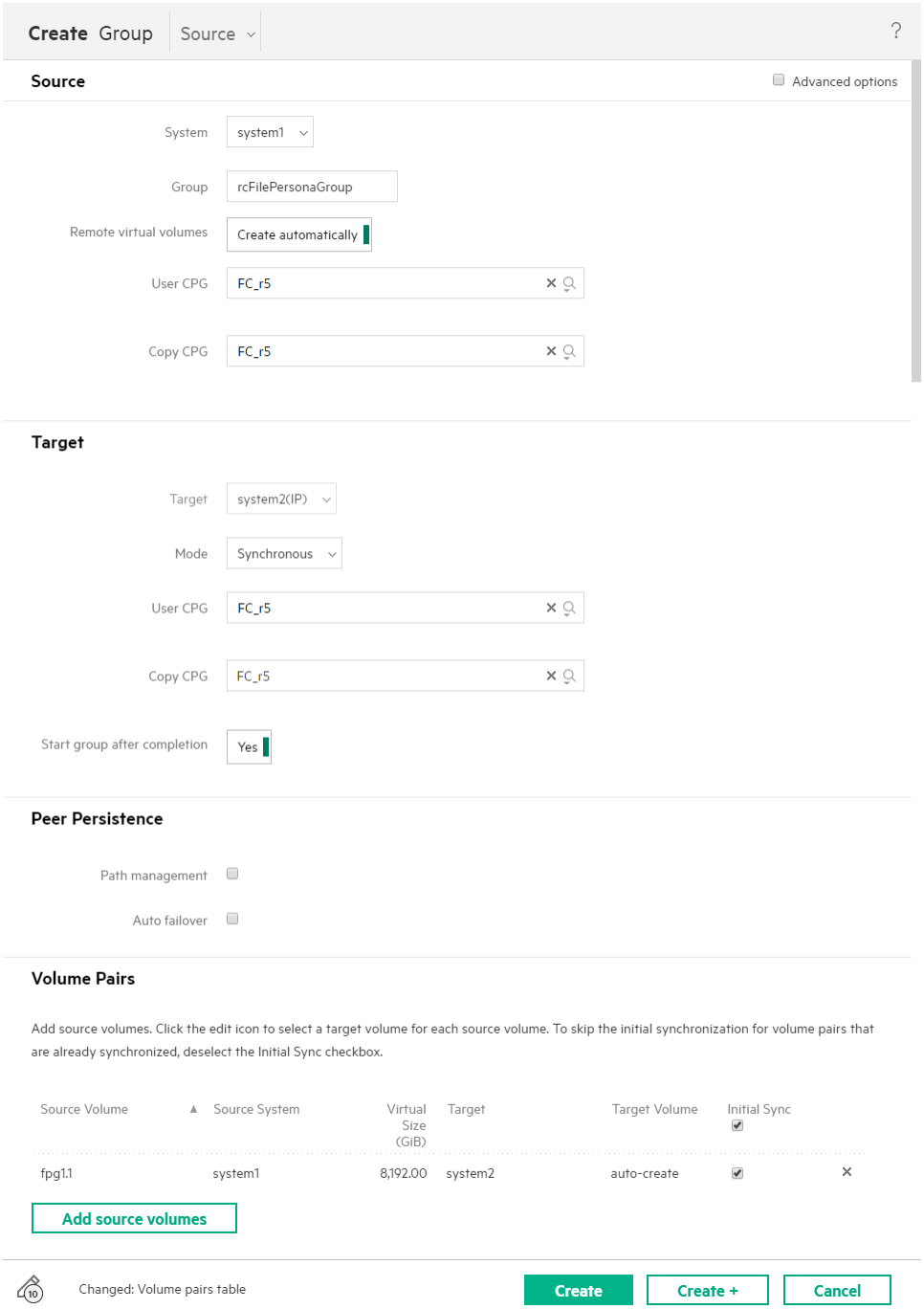

Figure 7. Create Remote Copy Group example dialog.

Important

If an FPG is comprised of more than one Virtual Volume, all Virtual Volumes of the FPG must be in the same Remote Copy group. This is the case if the FPG capacity exceeds 16 TiB and uses Thin Deduplicated Virtual Volumes.

Disaster recovery process

The following section discusses the disaster recovery process for FPGs replicated using Remote Copy, both for a planned and an unplanned failover scenario.

Planned failover process

A planned failover for replicated FPGs is a multistep process that deactivates an active FPG on the primary storage system (system1), reverses the replication direction, and finally recovers the FPG on the backup storage system (system2). Prior to a planned failover the Remote Copy synchronization state needs to report "Synced", otherwise there is a risk of data loss during the failover as not all changes to files and folders are available on the backup storage system.

Important

During the failover process, client access to file shares is disrupted. Please ensure that the failover is done during a maintenance window where users are minimally impacted.

Deactivate FPGs on primary storage system

On the primary storage system (system1), deactivate and detach all FPGs that are to be failed over to the backup storage system (system2) to ensure the FPGs and their VFSs are not active on both systems at the same time. This is best done using the CLI and the command `removefpg` with the `-forget` option.

```
system1 cli% showfpg
                ------(GB)-------
FPG  -Mountpath- -Size-- Available ActiveStates -DefaultCpg- -VVs-- State  Version
fpg1 /fpg1       8192.00   8191.32    ACTIVATED FC_r5        fpg1.1 normal 12.0
-------------------------------------------------------------------------------
   1 total       8192.00   8191.32

system1 cli% removefpg -forget fpg1
```

Repeat the above command for every FPG that should be failed over to the backup storage system (system2).

Stop Remote Copy Group

Once completed, stop the Remote Copy Group on the primary storage system (system1) using the SSMC. Navigate to **3PAR StoreServ** > **Remote Copy Groups** > **Actions** > **Stop** and complete the dialog box. Repeat this step for all Remote Copy Groups that will be failed over.

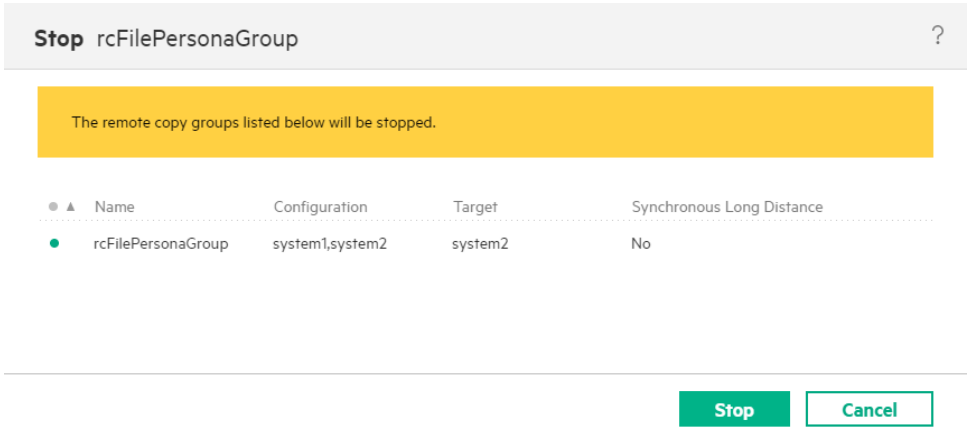

Figure 8. Stop Remote Copy Group example dialog.

Failover Remote Copy Group

Once the Remote Copy Groups are in a stopped state, failover the Remote Copy Group to the backup storage system (system2) using the SSMC. Select **3PAR StoreServ** > **Remote Copy Groups** > **Actions** > **Failover** for each Remote Copy Group and complete the dialog.

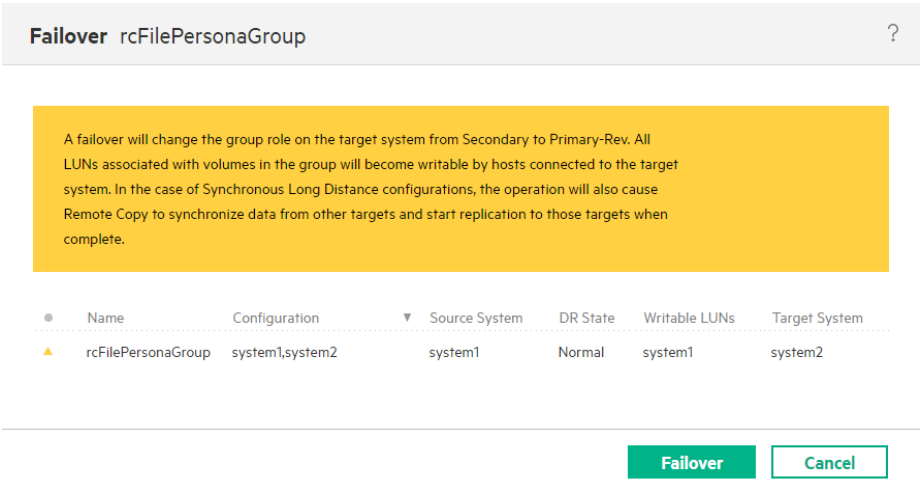

Figure 9. Failover Remote Copy Group example dialog.

Recover FPG on backup storage system

After the Remote Copy group was failed over to the backup storage system (system2) the FPG can be recovered using the replicated Virtual Volumes. Identify the Virtual Volume names on the backup storage system (system2) using the SSMC. Select **3PAR StoreServ** > **Remote Copy Groups** > **Target Volumes** for each Remote Copy Group. Note the Virtual Volume names in the Name column as displayed in Figure 10.

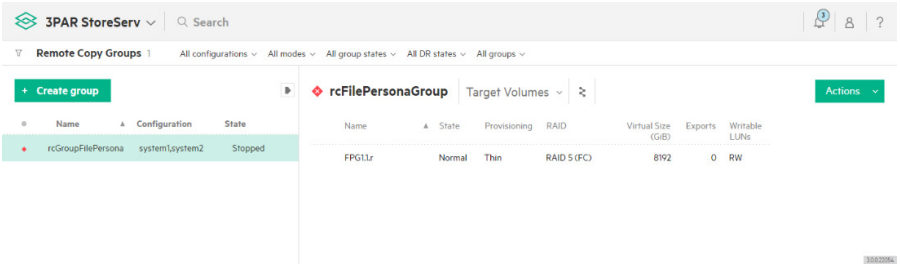

Figure 10. Display Target Volumes of Remote Copy Group.

Recover and activate the FPGs on the backup storage system using the CLI and the `createfpg` command. The `-recover` option indicates that an existing FPG is recovered from the specified Virtual Volumes. If the FPG is comprised of multiple Virtual Volumes, all of them need to be specified in the command as a space-separated list.

```
system1 cli% createfpg -recover fpg1.1.r
```

Repeat this command for all FPGs that need recovery on the backup storage system, specifying the Virtual Volume names for each FPG as a parameter.

Note

If the IP addresses for the VFSs were not configured for the backup storage system prior to the failover and the IP addressing schema in the backup data center differs from the primary data center, the clients will not be able to access the shares until the IP addresses for the backup storage system (system2) have been adjusted. This procedure is described in section Adjusting VFS IP addressing on backup storage system.

Reverse Remote Copy replication

Since clients can now modify files and folders on the backup storage system (system2), the replication direction of the Remote Copy Group needs to be reversed to synchronize changes back to the primary storage system (system1). This procedure is described in section Recover replication direction.

Unplanned failover process

The unplanned failover process assumes that the primary storage system (system1) is unavailable on the network due to a disaster in the site and a failover needs to be performed to activate the backup storage system. Figure 11 displays the Remote Copy Group status before and after the backup system was activated as described in this process.

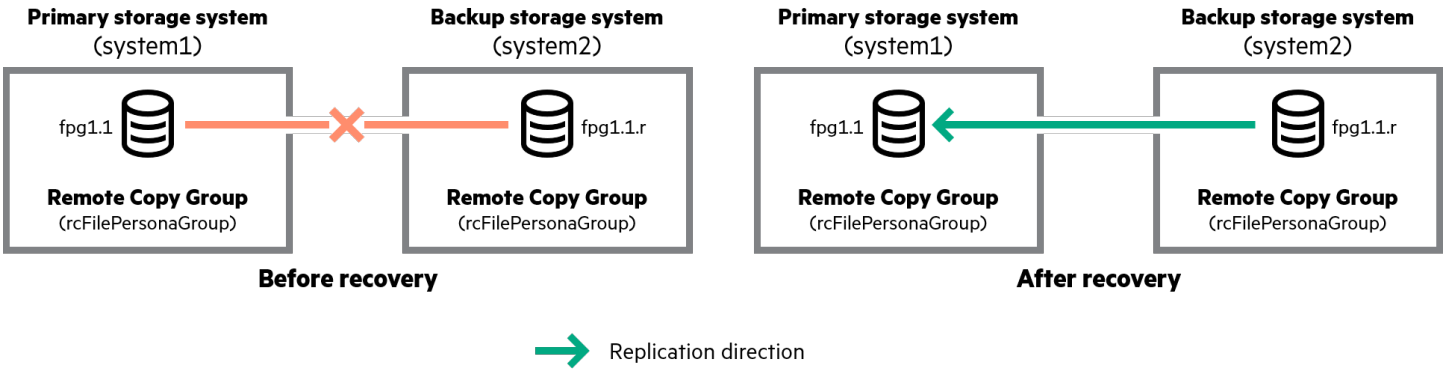

Figure 11. Remote Copy Group state before and after recovery.

Remote Copy Group state verification

After an unplanned failover the Remote Copy Group is in a stopped state, which can be reviewed using the SSMC by navigating to **3PAR StoreServ** > **Remote Copy Groups** and selecting the Remote Copy Group. The overview section will describe the active state of the Remote Copy Group as depicted in Figure 12, where the following information is to be reviewed:

Table 2. Remote Copy Group state information.

Property	Description
State	State should indicate "Warning", which specifies that replication between the primary storage system (system1) and the backup storage system (system2) has been interrupted due to the unplanned failure.
Role	Source Role should indicate "Primary" and the Backup Role should indicate "Secondary", which specifies that backup storage system (system2) is currently still the replication target for the Remote Copy Group and has not yet been promoted to represent the primary (active) version of the data.
Group state	Group State should indicate "Stopped", which specifies that replication between the primary storage system (system1) and the backup storage system (system2) has been interrupted due to the unplanned failure.

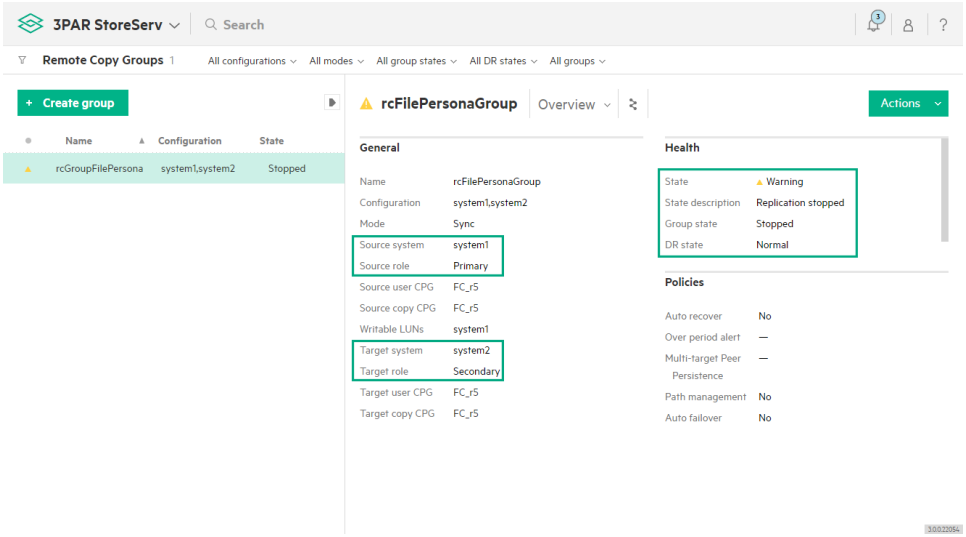

Figure 12. Display Remote Copy Group state example.

Failover Remote Copy Group

Failover the Remote Copy Group to the backup storage system (system2) using the SSMC. Select **3PAR StoreServ** > **Remote Copy Groups** > **Actions** > **Failover** for each Remote Copy Group and complete the dialog.

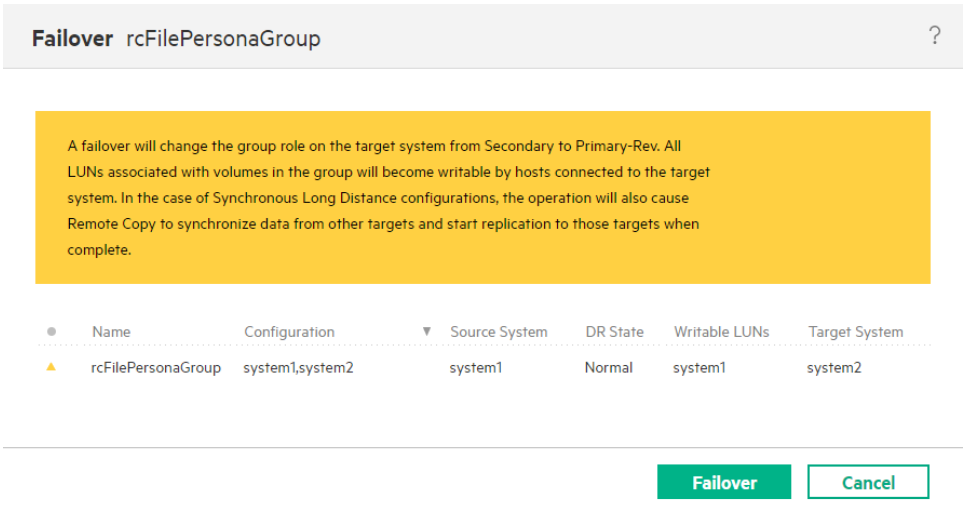

Figure 13. Failover Remote Copy Group example dialog.

Recover FPG on backup storage system

After the Remote Copy group was failed over to the backup storage system (system2) the FPG can be recovered using the replicated Virtual Volumes. Identify the Virtual Volume names on the backup storage system (system2) using the SSMC. Select **3PAR StoreServ** > **Remote Copy Groups** > **Target Volumes** for each Remote Copy Group. Note the Virtual Volume names in the **Name** column as displayed in Figure 14.

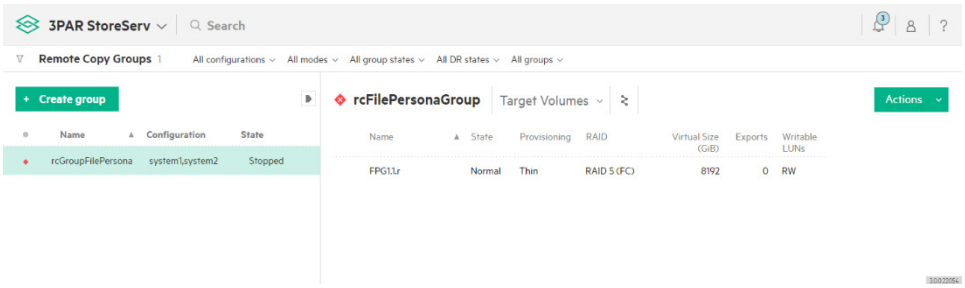

Figure 14. Display Target Volumes of Remote Copy Group.

Recover and activate the FPGs on the backup storage system using the CLI and the `createfpg` command. The `-recover` option indicates that an existing FPG is recovered from the specified Virtual Volumes.

```
system1 cli% createfpg -recover fpg1.1.r
```

Repeat this command for all FPGs that need recovery on the backup storage system, specifying the Virtual Volume names for each FPG as a parameter.

Note
If the IP addresses for the VFSs were not configured for the backup storage system prior to the failover and the IP addressing schema in the backup data center differs from the primary data center, the clients will not be able to access the shares until the IP addresses for the backup storage system (system2) have been adjusted. This procedure is described in section Adjusting VFS IP addressing on backup storage system.

Deactivate FPG on primary storage system

Once the primary storage system (system1) becomes available again, e.g., after the issues causing the disaster have been fixed, the FPGs on the system need to be deactivated in order to avoid any conflicts. This is done using the CLI and the command `removefpg` with the `-forget` option. As an example, to deactivate FPG "fpg1", execute the following command on the primary storage system (system1):

```
system1 cli% removefpg -forget fpg1
```

Repeat this step for every FPG that was failed over to the backup storage system (system2) as part of the disaster recovery process.

Reverse Remote Copy replication

Since clients can now modify files and folders on the backup storage system (system2), the replication direction of the Remote Copy Group needs to be reversed to synchronize changes back to the primary storage system (system1) once it is available again. This procedure is described in section Recover replication direction.

Planned failback process

After successful recovery of FPGs and Remote Copy Groups on the backup storage system (system2) as described in previous sections Remote Copy Groups can be recovered to the primary storage system (system1) once it is available again. The procedure is similar to a planned failover but requires some additional steps before recovery. Figure 15 displays the Remote Copy Group state before and after the failback process, which is described in this section.

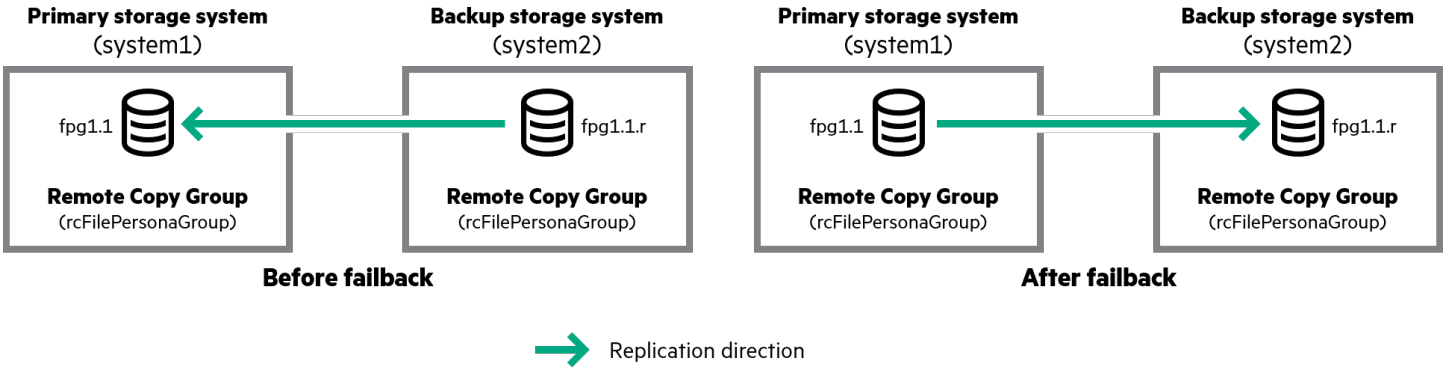

Figure 15. Remote Copy Group state before and after failback.

Recover replication direction

Once both storage systems are ready to resume normal operation, i.e., maintenance operations are completed, the natural replication direction needs to be restored and any pending changes need to be resynchronized.

Note

Figure 15 displays an environment where this operation has already been performed. If the replication direction has not yet been recovered as described in this section, the Remote Copy Group will report a stopped state.

On the backup storage system (system2) use the SSMC to restore the direction of replication by selecting **3PAR StoreServ** > **Remote Copy Groups** > **Actions** > **Recover** and completing the dialog box.

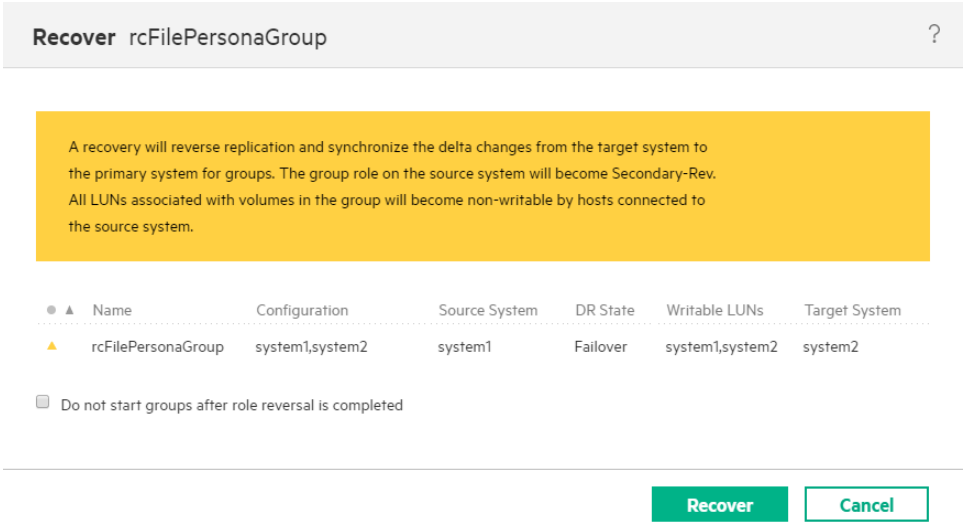

Figure 16. Recover Remote Copy Group example dialog.

Once recovered, verify that the Remote Copy Group DR state is “Recover” as displayed in Figure 17 and wait until the Remote Copy Group synchronization state reports “Synced” as indicated in Figure 18.

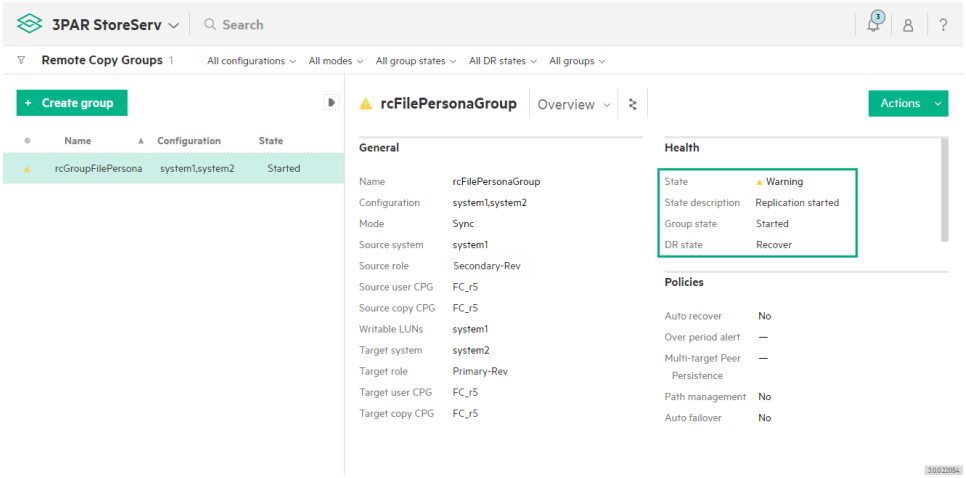

Figure 17. Remote Copy Group in Recover state.

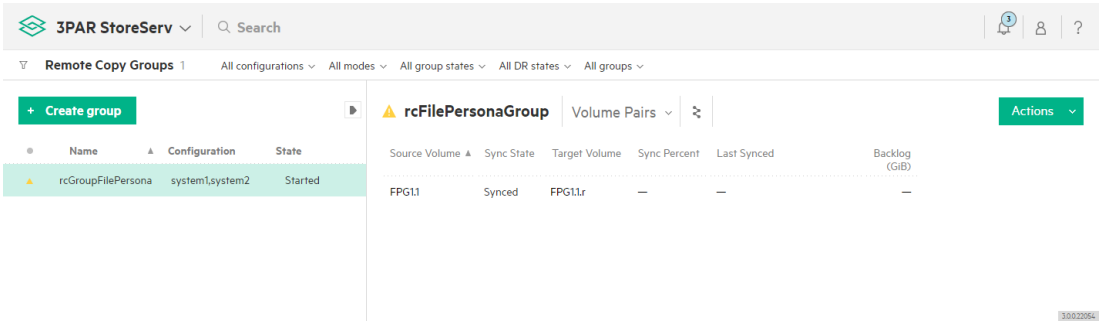

Figure 18. Remote Copy Group Volume Pairs in Synced state.

Revert natural replication direction

After the storage systems have completed data synchronization, identify the FPGs that will be failed over to the primary storage system (system1) and issue `removefpg` with the `-forget` option to detach and remove the FPGs on the backup storage system (system2):

```
system2 cli% removefpg -forget fpg1
```

Repeat this step for all FPGs that need to be failed back to the primary storage system (system1). Once all FPGs are removed from the backup storage system (system2), restore the natural direction of replication for the Remote Copy Groups using SSMC.

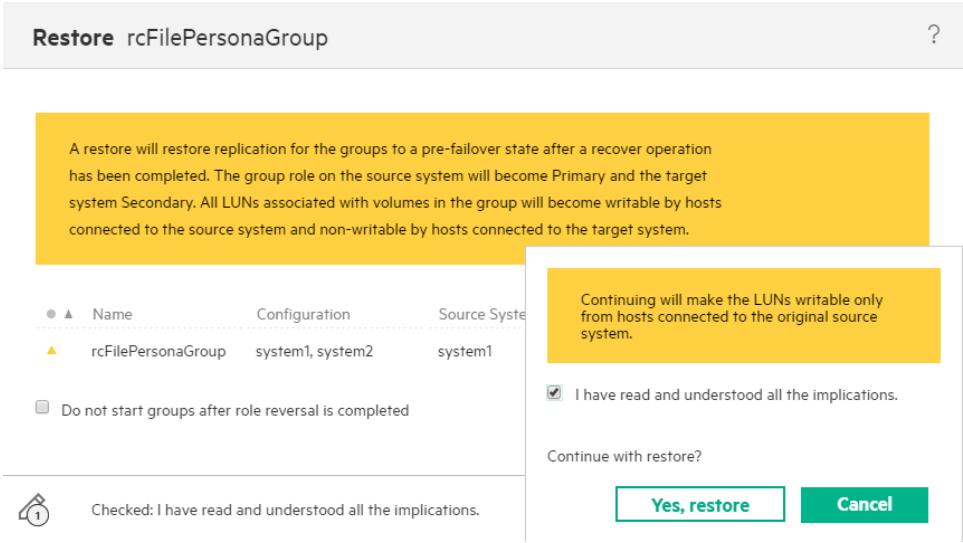

Figure 19. Restore Remote Copy Group example dialog.

After systems have been reversed to pre-failover configuration, verify the source role on the primary storage system (system1) is set to "primary" and the backup storage systems (system) target role is "secondary".

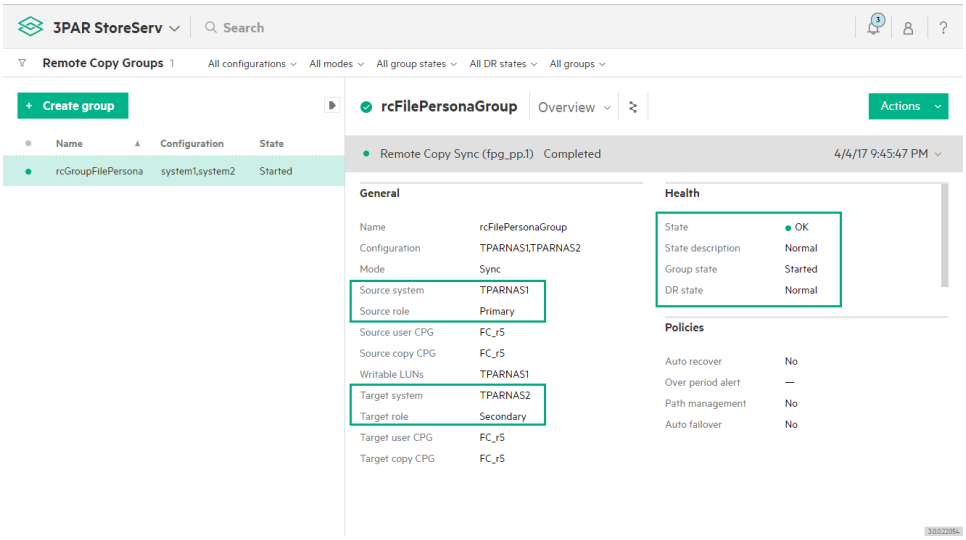

Figure 20. Restore Remote Copy Group example dialog.

Identify the Virtual Volumes associated with the FPG. Recover and activate the FPGs on the primary storage system using the CLI and the `createfpg` command. The `-recover` option indicates that an existing FPG is recovered from the specified Virtual Volumes.

```
system1 cli% createfpg -recover fpg1.1
```

Repeat this step for every FPG that was reverted as part of the disaster recovery process. Once the recovery completes, verify clients do have access to their shares.

Adjusting VFS IP addressing on backup storage system

In cases where differing IP addressing schemas are used in the primary and backup data center and where these IP address configurations have not been configured prior to the failover, IP addresses of Virtual File Servers need to be altered after a failover to the backup storage system (system2).

Note
The Virtual File Server must be recovered and active on the backup storage system (system2) before any alterations of its IP address configuration can be made.

Changing the IP address configuration of Virtual File Servers after recovery is best done using the HPE 3PAR CLI, but is also exposed through SSMC. First, the current IP address configuration of a recovered Virtual File Server can be obtained using the `showfsip` command.

```
system2 cli% showfsip vfs1
---------------ID--------------- VFS   FPG  IP_Address     Subnet        VLAN Type
4ef46afe27bd40949985ae3ad761fd92 vfs1  fpg1 192.168.10.100 255.255.255.0    0 user
-------------------------------------------------------------------------------
                                1 total
```

Use the `setfsip` command to change the IP address for the Virtual File Server.

```
system2 cli% setfsip -ip 192.168.20.100 -subnet 255.255.255.0 vfs1 4ef46afe27bd40949985ae3ad761fd92
Modify VFS IP: vfs1
select q=quit y=yes n=no: y
2181
system2 cli% showfsip vfs1
---------------ID--------------- VFS   FPG  IP_Address     Subnet        VLAN Type
4ef46afe27bd40949985ae3ad761fd92 vfs1  fpg1 192.168.20.100 255.255.255.0    0 user
-------------------------------------------------------------------------------
                                1 total
```

Once the IP address configuration is adjusted, DNS name resolution for the new IP address requires configuration. There are multiple options available to administrators, which have their own advantages and disadvantages as discussed earlier in this white paper.

- Add a new DNS entry for the new IP address and inform clients to connect to the new FQDN.
- Modify the original DNS entry with the altered IP address.

Volume recovery using Virtual Copy

In rare instances, entire FPGs may require recovery to an earlier state. Using point-in-time Virtual Copy snapshots of the Virtual Volumes of an FPG, file system corruption or major file system changes can easily be recovered.

Create Virtual Copy snapshot for recovery

By default, the Virtual Volumes that are associated with an FPG are created within a Virtual Volume Set, an HPE 3PAR Virtual Volume grouping mechanism. Using the Virtual Volume Sets to create Virtual Copy snapshots ensures that all Virtual Volumes associated with a single FPG are protected as a whole.

Identify the Virtual Volume Set of an FPG using the `showvvset` command.

```
system1 cli% showvvset fpg1
Id Name Members
11 fpg1 fpg1.1
----------------
 1 total 1
```

Before any Virtual Copy snapshot can be created, the Virtual Volumes require the assignment of a Common Provisioning Group used for snapshot space. For each volume in the Virtual Volume Set, use the `setvv` command to alter the Virtual Volumes in the set and assign a snapshot CPG.

```
system1 cli% setvv -snp_cgp FC_r5 fpg1.1
```

Create a new read-only Virtual Copy snapshot of the Virtual Volume set using the `creategroupsv` command, ensuring that all Virtual Volumes in the set are protected at the same point in time.

```
system1 cli% creategroupsv -ro fpg1.1
CopyOfVV SnapshotVV
  fpg1.1  fpg1.1.ro
system1 cli% showvv
                                                                                  ----Rsvd(MB)----- -(MB)--
Id Name                        Prov Type  CopyOf        BsId Rd -Detailed_State-  Adm   Snp    Usr   VSize
 1 .srdata                     full base  ---              1 RW normal              0     0  61440   61440
 0 admin                       full base  ---              0 RW normal              0     0  10240   10240
11 bootvv0fs                   full base  ---             33 RW normal              0     0 153600  153600
10 bootvv1fs                   full base  ---             32 RW normal              0     0 153600  153600
13 fpg1.1                      tpvv base  ---             76 RW normal            256  8704   8704 1048576
14  fpg1.1.ro                  snp  vcopy fpg1.1          76 RO normal             --    --     -- 1048576
12 FSQuorum                    full base  ---             34 RW normal              0     0   1024    1024
-------------------------------------------------------------------------------------------------------------
 7 total                                                                        256  8704 388608 2477056
```

Recover from Virtual Copy snapshot

Recovery from Virtual Copy snapshots is an offline recovery process and requires downtime. Clients will lose access to their shares hosted on the FPG that is recovered through this process. First, deactivate the FPG using the HPE 3PAR CLI command `removefpg` with the `-forget` option.

```
system1 cli% removefpg -f -forget fpg1
Removing fpg: fpg1
2185
```

Use the `showtask` command to display the status of the background operation and wait until the process completed before proceeding. Once completed, promote the Virtual Copy created earlier using the command `promotegroupsv` with the snapshot name as a parameter.

```
system1 cli% promotegroupsv fpg1.1.ro
Task 2186 has been started to promote virtual copy fpg1.1.ro to base
```

Once the Virtual Copy snapshot promotion completed, rediscover the FPG from the updated Virtual Volumes using the `createfpg` command and the `-recover` option.

```
system1 cli% createfpg -recover fpg1.1
```

Once the process completed, verify clients have access to their file shares that existed at the time the Virtual Copy was created.

Summary

As customers are looking for a robust unified storage solution for their business-critical application and user data, HPE 3PAR StoreServ with its Remote Copy feature presents a proven option to deliver disaster tolerance for both file and block workloads. File Persona file shares make use of the same robust replication technology as block volumes and benefit from its simplicity in management and efficiency in transport.

Enhanced by additional data protection technologies using share or NDMP backup and client-accessible file system snapshots, File Persona provides comprehensive capabilities to meet most customers recovery time and recovery point objectives with minimal management effort.

Additional resources

Refer to the following documents for additional information on HPE 3PAR File Persona Software and data protection strategies:

- Technical overview of HPE 3PAR File Persona Software
- Disaster-tolerant solutions with HPE 3PAR Remote Copy
- Protecting HPE 3PAR File Persona data
- Data protection for HPE 3PAR File Persona Software with HPE Recovery Manager Central
- Protecting HPE 3PAR File Persona data with share or NDMP backup using HPE Data Protector
- Protecting HPE 3PAR File Persona data with share or NDMP backup using Commvault
- Protecting HPE 3PAR File Persona data with share or NDMP backup using Veritas NetBackup

Learn more at

hpe.com/storage/3parfilepersona

4AA5-8027ENW, August 2017, Rev. 2

Hewlett Packard Enterprise