SnapServer and RDX QuikStor Architecture Tech Brief

March 2017

Why Do You Need It?

Companies large and small rely on digital information to conduct business. Financial applications, human resource systems, customer relationship management software, and supply chain management solutions are the backbone of most organizations. The accelerating pace of data creation, accumulation, and diffusion is becoming an increasingly common phenomenon among companies throughout the world today. Data is growing exponentially due to widespread use of the Internet, email, and media-rich software.

Data protection – arguably the most important aspect of data center management applies to any system whether it is physical, partitioned, or virtual.

Backup and recovery remains the pain point among most storage management organizations. Coping with failed backups and finding a solution for diminishing backup windows has been a top priority. Not having an efficient backup process means you're not backing up and protecting all your data until the backup window opens or is large enough to do the backups and complete them in a timely manner.

What if a server crashes, or a file gets modified, or a database gets corrupted just before the backup window?

Backup and recovery is an inherently challenging process that becomes more difficult as a company's data grows and the demands on its online availability increases, further limiting the time available for backup and recovery operations.

How Can We Help?

Disk-based backup is gaining market momentum as an economical and highly effective way to reduce backup windows and boost recovery time frames while ensuring compliance with regulations and corporate governance requirements. As part of an effort to continually improve our product line, Overland Storage SnapServer has a new backup and recovery feature that allows it to integrate an RDX QuikStor as a backup target to deliver an ideal nearline backup and near instantaneous recovery that meets the requirement of always being protected.

The RDX can easily be attached to one or more USB 3.0 ports on the SnapServer XSR or XSD products. Once attached, SnapServer quickly and automatically discovers the device as well as the removable media.

Since the SnapServer has more than one USB 3.0 port, connecting multiple RDX devices can be used for best performance. Performance can easily increase when two RDX QuikStor devices are attached to both ports which can provide simultaneously backup or recovery and could double the overall performance.



Overview

The SnapServer has many methods of protecting digital data on its local volumes. This includes replication and synchronization features as Snap ECR (Encrypted Continuous Replication), Snap EDR (Enterprise Data Replicator) and SnapSync. In this paper, we'll cover in detail the new backup and recovery option with the SnapServer and RDX QuikStor. This section outlines terminologies used in backup and recovery along with common deployment scenarios for backup and recovery with SnapServer.

Contents

SnapServer Overview	3
RDX Overview	
Deployment with SnapServer and RDX	3
Backup and Recovery Terminology	4
Backup and Recovery with SnapServer and RDX	4
RDX QuikStor Feature	7
Scheduling an RDX Backup	8
Fast Recovery from an RDX cartridge	10
Portability and Disaster Recovery	13
Portable Protected Data	13
SnapSync and Protecting File-sync Data	14
Proven Disaster Recovery with Snap ECR and RDX	17
Best Practices	19
Conclusion	21
References	22

SnapServer Overview

Built upon the award winning GuardianOS, the SnapServer offers enterprise class management and data protection features. SnapServer is a Unified, Secure, Expandable storage NAS. It provides advanced security and a variety of replication and file synchronization options. SnapServer architecture along with all its features provides significant benefits including availability, scalability, performance and flexibility in deployment.

The SnapServer family includes the following products: XSR120, XSR40 and XSD40.

More information on SnapServer products can be found here.

http://www.overlandstorage.com/products/snapserver/index.aspx

RDX Overview

RDX is a removable disk-based technology providing lightning fast backup and restore. The RDX product family is designed to deliver cost efficiency to small and medium-sized businesses (SMB) with growing data storage needs. The RDX QuikStor outlined in this document is a media-based removable storage system that is rugged, reliable and convenient storage for backup, archive, data interchange and disaster recovery. Some of the benefits include high capacity removable cartridges (4TB, 3TB, 2TB etc.). It also has USB 3.0 high speed interface for fast and reliable performance.

More information on RDX products can be found here.

http://www.tandbergdata.com/emea/index.cfm/products/removable-disk/

Deployment with SnapServer and RDX

Deploying an RDX QuikStor to a SnapServer is as simple as just attaching it to one of the USB 3.0 ports located on the back of each appliance.

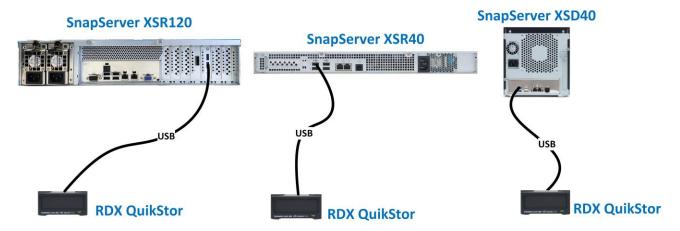


Figure 1 SnapServer (XSR120, XSR40 and XSD40) and RDX QuikStor USB attached.

As illustrated in Figure 1, simply attach a QuikStor to the USB port of the SnapServer.

Backup and Recovery Terminology

The following information is the most commonly used terminology related to data backup and recovery.

- Source Data This is the primary data set that is copied or protected.
- Target This is the location where a copy of source data is routed to which is typically another disk or tape medium.
- File-level Backup A type of backup that is defined at the level of files and folders.
- Full Backup A method of backup which copies the entire data set (Files/Folders).
- Restore Recovery of partial or entire source data set.
- Input / Output Transfer Rates- This is the performance throughput of a backup or recovery measured in MB per second.
- Backup Client An application agent that is installed on a client, in this case a SnapServer. The agent communicates to the Backup Server and the source data is pushed to it for backup or pulled from it for restore.
- Backup Server An application on a dedicated server class system that writes data, pushed by the backup client over the network, to a backup medium (disk or tape).
- Scheduler A major software component of the Backup Server that allows you to schedule regular automated backup jobs and coordinates their execution. Backups can be scheduled at periodic intervals, or individual files can be automatically backed up immediately after they have been updated.

Backup and Recovery with SnapServer and RDX

When traditional backup solutions fail, enterprises are exposed to windows of potential data loss. There are several ways to protect the data on a SnapServer. In this section, we will describe the most common methods of data protection including the new RDX feature integrated with SnapServer.

- Traditional Backup and Restore method: you deploy a backup client agent (Veritas Backup Exec, NetBackup, and NetWorker) on a SnapServer that requires backup services. With this approach, the backup agent scans the file system for changes and sends the changed information across the network to a backup server that writes the data to a backup medium, such as local disk attached to the backup server or a magnetic tape device. The drawbacks of this method are:
 - o Tedious and can be complex to install and configure the Backup Client Agent on each SnapServer.
 - o Maintaining proper versions of the Backup Client Agent software on the SnapServer is required.
 - o Performance can vary depending on network contention or usage. It can also be hindered with an under resourced backup server.
 - o Constant communication between the Backup client agent and Backup Server is required to achieve successful backups and restores.
 - The primary component is the Backup Server; it is the brains of this method. Without a Backup Server running backups and restores are not possible.

As illustrated in Figure 2, the environment shown is a typical backup environment leveraging a Backup Server and its targets. Data is copied over the network from the SnapServer to the Backup Server.

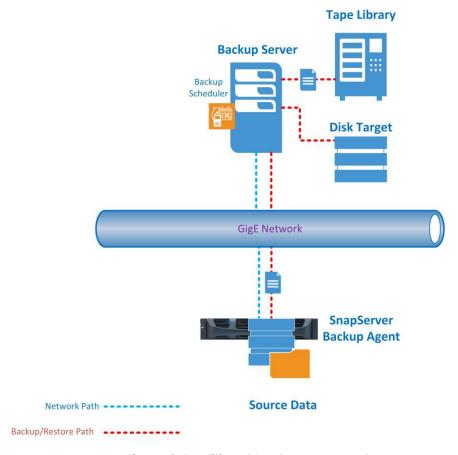


Figure 2: Traditional Backup Approach

- RDX QuikStor Integration with SnapServer: This added feature enables the local SnapServer volume to back up the data to a removable cartridge allowing for the best performance for backup and recovery. The local backup to RDX eliminates the contention of running a backup over a network. The following lists the benefits of using this method:
 - Extremely Fast Deployment (Three easy steps).
 - Upgrade GuardianOS on SnapServer to GOS 7.7.220
 - Attach RDX QuikStor to the SnapServer
 - Create a Scheduled Backup Job using the Snap Web Management Interface
 - Cost Effective Solution
 - Does not require additional Backup Software/Application nor Client Agents
 - Does not require additional expensive hardware; Tape Drive, Tape Library, Fibre Channel SAN, SAS Host Bus Adapter etc.
 - Simplified Backup Scheduler Configuration and Options.
 - Easy access to RDX QuikStor option with Snap Web Management.
 - Extremely Fast Backup using USB 3.0. With two RDX you can double your performance!

- o RDX has compatible high capacity removable drives and SSD cartridges
 - 500GB, 1TB, 2TB, 3TB, 4TB
 - SSD: 128GB, 256GB
- Quick and non-complex Recovery method
 - Restore is local and not over a congested network

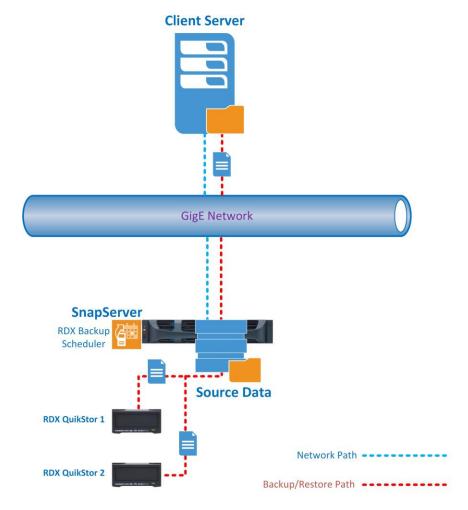


Figure 3 RDX Integration with SnapServer

As illustrated in Figure 3, with GuardianOS 7.7.220 and above, the integration of RDX QuikStor is possible. This method bypasses network contention and not to mention expensive and complex backup applications.

RDX QuikStor Feature

The RDX QuikStor integration is available only with GuardianOS 7.7.220 and above, which is available here.

http://support.overlandstorage.com/support/snapserver-nas.htm

Once upgraded, the Storage | RDX QuikStor tab is an available option in the Snap Web Management Interface. When an RDX QuikStor is attached, it is discovered and displayed as shown in Figure 4. The following features are available within the RDX QuikStor tab:

- View the status of the RDX cartridge
- o Display free space and Size of the RDX cartridge
- Display the serial number of the RDX dock and cartridge
- o Display the Filesystem for the current loaded cartridge
- o Media Management tools as: Format, Copy Eject and Rename Volume
- Create, View, Edit, Clone and Suspend Backup Schedules

Figure 4: Snap Web Management and RDX QuikStor feature



Scheduling an RDX Backup

RDX scheduled backups allow the backup or storage administrator to schedule backups. The Backup Scheduler copies all files, directories in the selectable volumes within the SnapServer. Configuring the backup schedule is very easy to do. For additional information on configuring a rotational daily backup, refer to the section 'Best Practices'.

As illustrated in Figure 5, shows the typical backup of user data on the SnapServer.

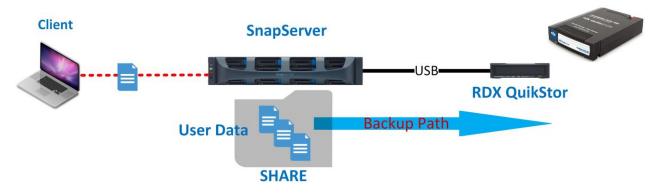
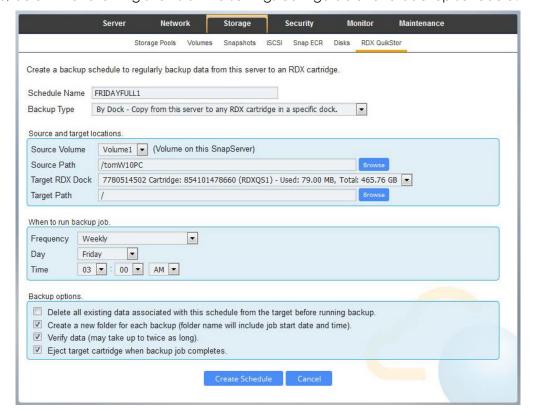


Figure 5 the following is the data flow during the backup.

As displayed in Figure 6, the backup schedule is simplified and can be modified and submitted at any given time.

Figure 6, below the following shows all the settings configurable for a backup schedule.

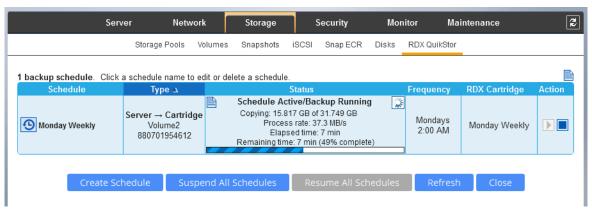


The backup schedule has very user friendly configurable options. The Table 1 below shows these options.

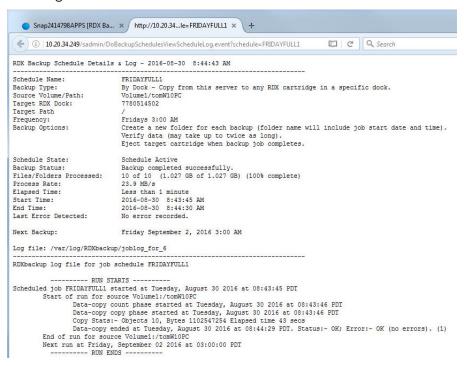
Table 1. Backup Schedule Options

Settings	Option/Details
Schedule Name	Name of the backup job
Backup Type	 By Dock – Copy from this server to any RDX cartridge in a specific dock. By Cartridge – Copy from this server to a specific RDX cartridge in any dock.
Source and Target Locations	
Source Volume	Volume on this SnapServer: Volume 1, Volume 2 etc.
Source Path	Browse (navigate the volume selected)
Target RDX Cartridge	Drop-down selection to choose the cartridge
Target Path	Browse (navigate the directory or root of RDX cartridge destination)
When to run backup job	
Frequency	The following options are available: 1. On Insert of Target Cartridge 2. Daily (Time) 3. Weekdays (Time) 4. Weekly (Day of week and Time) 5. Monthly (Day – Backup will be skipped if selected by days exceed days in month, Time) 6. End of Month (Time)
Backup Options	
	 Delete all existing data associated with this schedule from the target before running a backup. Create a new folder for each backup (folder name will include job start date and time). Preserve full source path at target. Verify Data (may take up to twice as long). Eject target cartridge when backup job completes.

Figure 7 below shows an active backup.



As illustrated in **Figure 8** below when the backup completes, a log is generated and can be viewed in the Snap Web Management.



Fast Recovery from an RDX cartridge

The most important part of backup is the restore task. Recovering data is done in reverse, where data is copied from the RDX QuikStor cartridge to the original location on the SnapServer or another volume on the SnapServer. SnapServer uses the 'Copy Data' feature in the RDX QuikStor option which can quickly retrieve files and directories without the need for any centralized index or database that can become a bottleneck to performance or scalability.

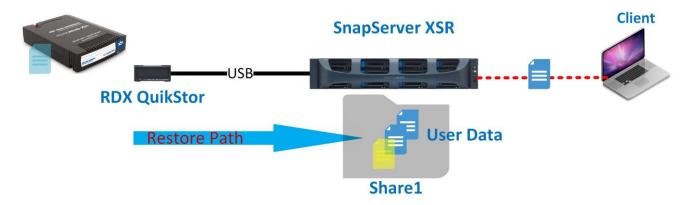
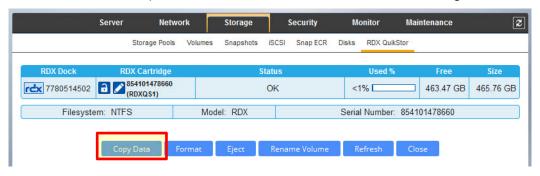


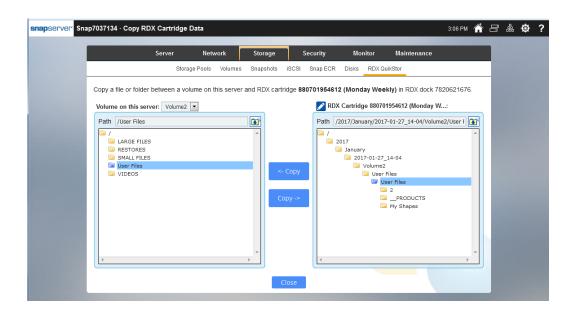
Figure 9: Shows a simplified data recovery flow between the RDX to the SnapServer.

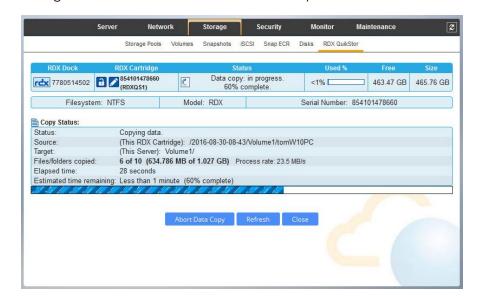
The steps to recover data from a backup are very simple. Use the following steps in the Snap Web Management under RDX QuikStor to recover data.

- Click the RDX Cartridge displayed
- Click Copy Data
- o Select the Volume and browse that target destination and select it
- o Browse the path of the source data and select it
- Verify both source and destination before you click Begin Copying

Figure 10 below shows the steps to take to recover data from the RDX cartridge.







The following shows the status of an active recovery

Figure 11 below shows a successful restore.

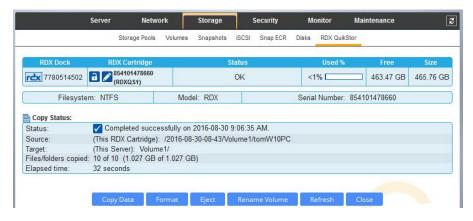


Figure 12 below shows a detail log of the restore job.



Portability and Disaster Recovery

Protecting your investment means having a good reliable copy of your data. The data must be readable and protected. This section covers the portability and disaster recovery capabilities with the RDX QuikStor and SnapServer solution. These sections cover in detail on SnapServer and RDX data interchange, SnapSync Filesync and Snap ECR.

Portable Protected Data

The following images show the portability capability the RDX provides.

As illustrated in Figure 13, the RDX cartridge is portable that it can easily be attached to Windows host system for data interchange. That is the Windows hosts at remote sites can insert an RDX NTFS formatted cartridge into its RDX dock to read the data. The data may be too large or sensitive to send over the network, thus physically sending the cartridge to the site is a great option.

The image shows an alternative option of exporting a cartridge to an offsite vault location like Iron Mountain for secure housing. The cartridge can be brought back as part of a media rotation or recovery.

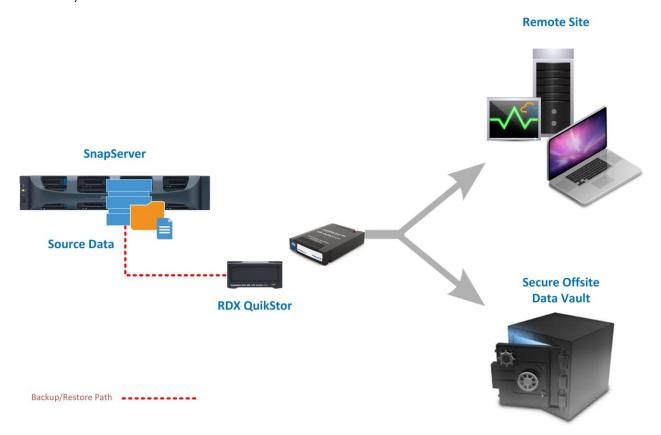


Figure 13 shows the portability capability the RDX provides

SnapSync and Protecting File-sync Data

As illustrated in Figure 14, SnapSync can be used as an easy way to file-synchronize data from site to site and with the collaborated data it can also be archived to locally attached RDX device. In the scenario, here, a file or directory is synchronized in a Windows environment located at Site B, and same data is file-synchronized to a Disaster Recovery Site C.

Each site has their own means of copying the synchronized data to their local RDX QuikStor. This solution provides simple but a secure enterprise class files sync and share.

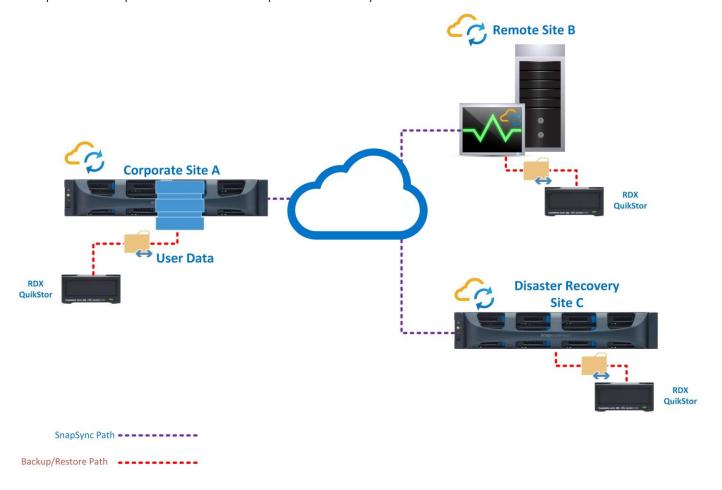


Figure 14 the following images shows SnapSync leveraged as a complementary solution for a site to site file-synchronization.

Figure 15 SnapSync can be used between two SnapServer appliances. Given the example here, the Engineering folder is synchronized from one SnapServer to another. The SnapServer with the RDX attached is configured to do weekly backups of the synchronized Engineering folder.

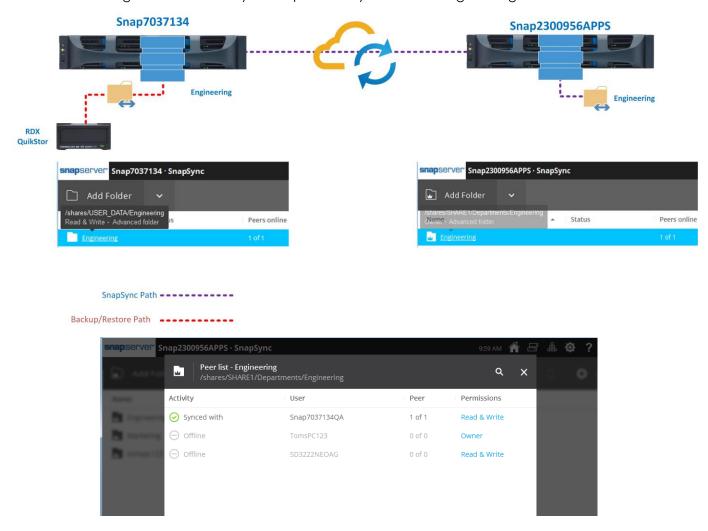


Figure 16 below shows the Engineering folder at the destination SnapServer. This data will be archived to a locally attached RDX QuikStor.

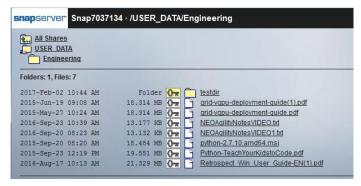


Figure 17 below shows the creation of an RDX backup schedule. Simply browse the volume to which the synchronize SnapSync folder is located and select it. Continue configuring the backup schedule options and create the schedule.

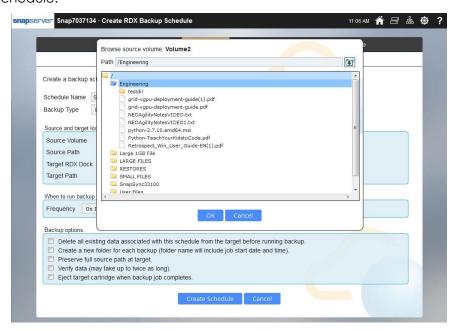
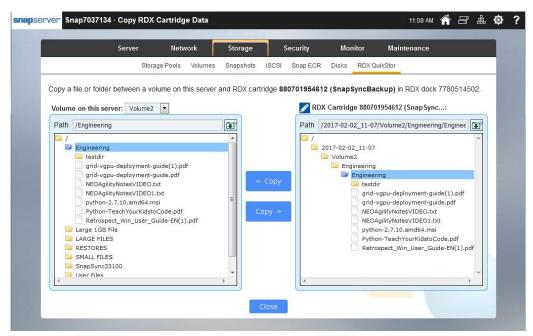




Figure 18 recovering the data from the RDX cartridge is like any restore job using the RDX QuikStor feature.



Proven Disaster Recovery with Snap ECR and RDX

The following image shows Snap Encrypted Continuous Replication (Snap ECR) as solution for a fast enterprise Disaster Recovery scenario leveraging the RDX as an archive device. Snap ECR integrates and enables Business Continuity with near zero data loss (RPO). It can replicate data at wire speed between SnapStorage environments. During a disaster Snap ECR can continue to provide reliable data protection and access, even if one of the SnapServers fails. Snap ECR with RDX provides significant benefits including availability, performance and ease of deployment.

As illustrated in Figure 19 below, we have two SnapServers using ECR as a disaster recovery solution to replicate a volume using ECR built policies and synchronize data from site-2-site. The target or DR site also has an RDX QuikStor attached to archive the replicated data.

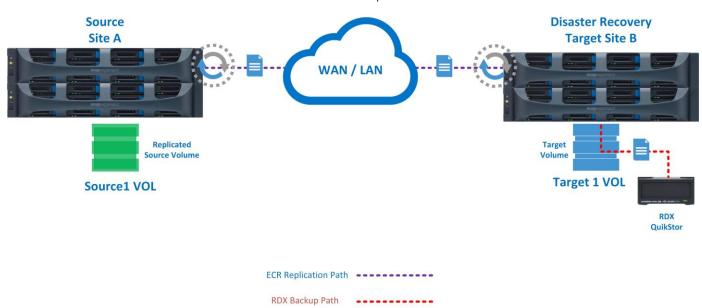


Figure 20 below shows a sample of the Snap ECR configuration on replicating the source volume to a target volume located in a remote SnapServer.

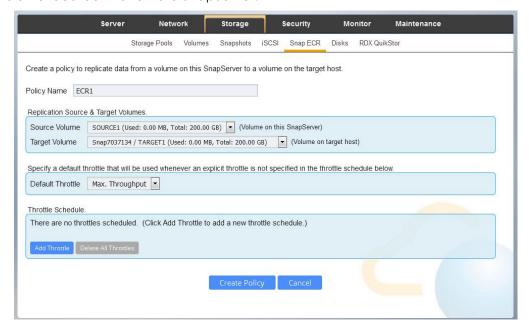


Figure 21 below shows the RDX QuikStor feature copy utility. **Note**, although a Scheduled backup policy is allowable to a Snap ECR volume, recovering data (Copy back) from the RDX is not possible and this is by design. It is restricted to copy from an RDX cartridge to an ECR enabled volume. The ECR enabled volume is distinguished with a (T) to show it is a currently used ECR Target volume. There are two options to recover ECR volume data from an RDX; first use an alternative volume (Non **(T)**) to recover the files. Second option is a brute force ECR change and that is to 'Remove Target Host' configuration.

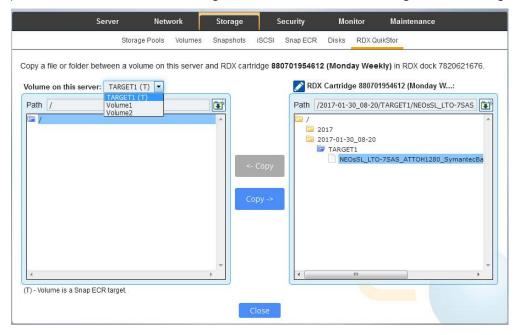
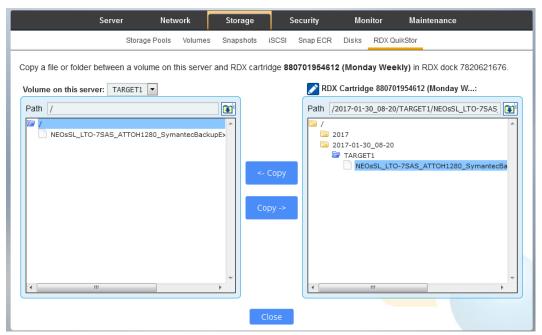


Figure 22 below shows that once the ECR Target host has been removed, RDX recovery to the once replicated volume can now be used as a restore volume.



Best Practices

Use the following guide lines to help configure your backup and recovery using the RDX and SnapServer built in backup.

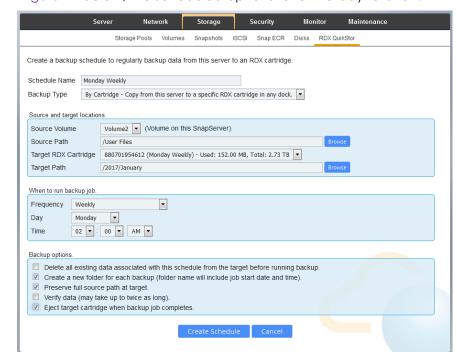
The following best practice information guides you in management of RDX media and how to help increase performance for both backup and recovery.

- o Run multiple streams using two RDX QuikStor devices.
- o If possible split the backups to two RDX, by sourcing large files to one RDX and smaller files to another. This helps isolate degraded performance to one schedule and to increase the other.
- Always make sure the RAID set is neither degraded nor initializing. Degraded raid set can dramatically slow performance during backup and restore.
- Always use the correct USB 3.0 ports on the SnapServer.
- When restoring data from the RDX cartridge to a different volume it was backed up from, always make sure that target volume has enough free space.
- Schedule backup jobs when SnapServer utilization is low. Usually in the evenings and weekends!
- Add additional memory resources, by default the XSR120 is 8GB but is can expandable up to 32GB.
- o Verifying the backup is always recommended. However, to increase performance on very small files and to meet the backup window, disable the verify option at the end of the backup.
- o If additional RDX media are available, use the Backup Method Type of "By Cartridge". This will allow for a five-day rotation configuration of different media. This method is best for staying organized, less wear on a single media and quick restores by identifying the day of the week media to recovering from. Use the following steps. Figure 24 is an example for this setup.
 - Use a five-day weekly rotation of media.

- Physically label each RDX media the day of the week if they are daily backups.
- Format the media with the day of the week for the Volume Name i.e.; Monday Weekly
- Create a Schedule for each day of the week "Monday, Tuesday", using the Frequency option of Weekly.
- It is best to create target directories with the Year and the Months. For example, create a root directory of 2017 and in that directory, a subdirectory January.
- Enable the option to "Eject target cartridge when backup job completes".

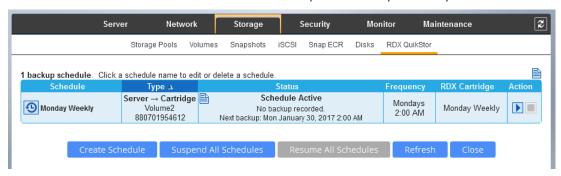
As illustrated in Figure 23 below, with two RDX QuikStor devices attached, simultaneous backups are possible. This increases performance which in turn meets the shrinking backup window. Running a backup and restore with an additional RDX is also possible.





As illustrated in Figure 24 below, the scheduled options for a five-day rotation.

Figure 25 below shows a scheduled rotational backup for the day Monday.



Conclusion

Ensuring that backup and recovery works fast and predictable is a key goal for many organizations. SnapServer with its new backup scheduler and integration with RDX QuikStor combines best of breed, optimized to deliver the absolute best combination of speed and protection for all data. It also provides flexible deployment options leveraging synchronized solutions such as SnapSync and Snap ECR.

References

For more information on Overland Storage Snap Server refer to the following link.

http://www.overlandstorage.com/products/snapserver/index.aspx

For more information on Tandberg RDX refer to the following link.

http://www.tandbergdata.com/emea/index.cfm/products/removable-disk/

For the latest versions of SnapServer or SnapCLOUD Guardian OS (GOS) please refer to the following link.

http://support.overlandstorage.com/support/snapserver-nas.htm