



By Scott Sinclair

# ADVANCED FILE SHARING AND MANAGEMENT IN THE DELL NX4

The Dell™ NX4 network attached storage (NAS) device goes beyond simple file servers to provide advanced features ranging from point-in-time snapshots and replication to deduplication, file-level retention, and tiered storage access. Combined with support for both Internet SCSI (iSCSI) and Fibre Channel, this system can help meet enterprise-class requirements, simplify data management, and reduce costs.

The Dell NX4 network attached storage (NAS) device is designed to provide flexible, enterprise-class file storage for Microsoft® Windows®, Linux®, and UNIX® environments. Advanced EMC® features such as point-in-time snapshots, replication, and deduplication enable the Dell NX4 to provide functionality well beyond simple file servers to help save administrative time and reduce costs, while support for both Internet SCSI (iSCSI) and Fibre Channel helps maximize flexibility in multi-protocol environments. File and block storage can be consolidated into a single Dell NX4 system to help simplify management.

The Dell NX4 uses the Data Access in Real Time (DART) OS for multi-protocol network file and block access. DART supports concurrent use of the Common Internet File System (CIFS) and Network File System (NFS) protocols and supports sophisticated locking and access-control mechanisms, enabling seamless file sharing across Windows-, Linux-, and UNIX-based client systems without compromising data integrity and without requiring performance-reducing emulation.

Providing capabilities designed for organizations that require functionality well beyond that of a simple file server, the Dell NX4 helps share files efficiently across both CIFS and NFS systems, protect critical file data with high availability, save wasted disk space where data growth has led to a proliferation of duplicate

files, comply with data retention regulations, and implement efficient backup and recovery processes.

## HIGH-AVAILABILITY ARCHITECTURE

Because file data can be as vital as application data, the Dell NX4 is designed to provide high availability without compromise—enabling organizations to continue operating at the same performance and service levels even in the event of a failure. The primary/standby architecture supports automatic failover and is designed to eliminate single points of failure from the network to the disk drive. The system is designed for high levels of fault tolerance, while the DART and EMC FLARE® operating environments offer advanced fault detection and isolation capabilities. Administrators can take advantage of hot-pluggable and standby components for transparent high availability and rapid recovery.

## POINT-IN-TIME SNAPSHOTS

EMC Celerra® SnapSure™ software enables administrators to create logical point-in-time read-only or read/write copies of file systems and iSCSI logical units (LUNs) to support online backups and quick recovery of deleted files. End users can quickly and easily restore previous versions of a file without administrator involvement. SnapSure also helps save disk space and time by

### Related Categories:

Data consolidation and management

Dell NX4

Network attached storage (NAS)  
Storage

Visit [DELL.COM/PowerSolutions](http://DELL.COM/PowerSolutions) for the complete category index.

supporting multiple snapshot versions of a file system or iSCSI LUN.

SnapSure is designed for excellent read performance. It operates on the copy-on-first-write principle: when a block within a production file system is modified, SnapSure saves a copy containing the block's original contents to a separate volume, referred to as the SavVol. Subsequent changes to the same block are not copied to this volume. SnapSure reads the original blocks in the SavVol and the unchanged blocks remaining in the production file system to provide a complete point-in-time image called a checkpoint.

Checkpoints can be read-only or read/write, and can serve as a direct data source for applications that require point-in-time data. Administrators can use checkpoints to restore a production file system or part of a file system to a previous state. Additionally, they can use writable checkpoints to create a test environment for databases and files where, after testing, changes can be applied nondestructively to the production file system. SnapSure also supports online checkpoint access, helping eliminate the need for administrator involvement when a client system needs to list, view, or copy a point-in-time file or directory in a read-only checkpoint

or use it to restore information from a previous point in time.

## ASYNCHRONOUS REPLICATION

As an option to the Dell NX4 NAS device, EMC Celerra Replicator™ software provides a powerful, simplified tool for asynchronous replication (see Figure 1). This tool uses standard IP-based local area networks (LANs) and wide area networks (WANs) to maintain consistent read-only or read/write replicas across sites, helping simplify configuration and management and enabling deployment of remote replication using familiar IP networking—which can result in significant savings in both staff time and budget. Administrators can easily define policies such as recovery point objectives (RPOs), and the software includes an adaptive scheduler that can determine the size and frequency of updates necessary to meet a given RPO, taking into account available bandwidth, data load, and data transfer concurrency.

Organizations can take advantage of Celerra Replicator in a number of ways:



The Dell NX4 NAS device is designed to provide flexible, enterprise-class file storage in heterogeneous mixed-protocol environments

- **Disaster recovery:** Administrators can replicate a duplicate copy of production data to a remote site, where it can be brought online with little downtime in case of a disaster.
- **Content distribution:** One-to-many replication can push content to remote sites—for example, when new engineering or software builds need to be distributed to multiple locations.
- **Backup:** Performing backups with a copy of the production data helps avoid the need to take the production applications offline. The backup can occur locally or at the remote location.
- **Decision support:** File systems and iSCSI LUNs can be replicated to make a copy of a database to be used for data mining and decision support without affecting production applications.
- **Software testing:** Before upgrading software on production systems, administrators can create a duplicate copy of the data and test the upgrade. Writable checkpoints allow administrators to test software with a modifiable copy of the production data.
- **Data center migrations:** When relocating to a new data center, administrators can copy data to the new system and force a failover, helping ensure that the migration is carried out without data loss.

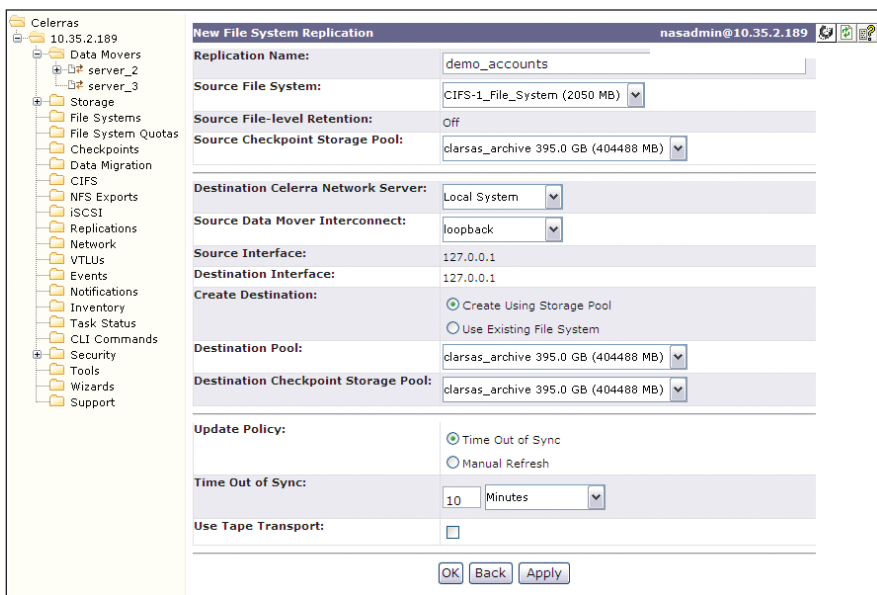


Figure 1. Celerra Replicator provides a powerful, simplified tool for asynchronous replication

the testing and execution of disaster recovery processes.

### VERSATILE BACKUP AND RESTORE

The Dell NX4 offers several options for backup and restore functionality to help meet the needs of common backup environments and maximize flexibility:

- **Network backups:** Network backups entail mounting CIFS or NFS file systems across a network and backing up to the backup server.
- **Network Data Management Protocol (NDMP) backups:** NDMP backups transfer data to a local backup device and use the LAN only for control information. This approach is typically employed for high-capacity backups and in environments requiring multi-protocol support.
- **Storage area network (SAN) backups:** SAN backups use the LAN for control information and do not involve the server in the data path from the SAN backup server.
- **NDMP volume-based backups (NVBs):** NVBs are an NDMP block-based backup option that can offer significant performance advantages for file systems with large numbers of small files (less than 16 MB). Using NVB in these environments can help significantly reduce backup windows.

### DATA DEDUPLICATION AND COMPRESSION

The Dell NX4 was designed to help organizations effectively handle the proliferation of unstructured data, combining file-level deduplication and compression to help intelligently reduce storage requirements with minimal performance impact. A built-in policy engine works in the background, transparently monitoring file activity and file attributes to intelligently identify candidate files. Files that meet certain criteria, such as low access frequency, are both compressed and deduplicated so that only a single instance of those files are retained.

Administrators can define specific filters to avoid processing files for which deduplication could result in an undesirable performance impact or only minimal storage savings.

### FILE-LEVEL RETENTION

The Celerra file-level retention (FLR) feature in the Dell NX4 enables administrators to protect files from modification or deletion until a specific retention date, helping organizations comply with enterprise, industry, or government requirements. FLR enables administrators, using CIFS or NFS operations, to meet write-once, read-many (WORM) requirements by creating a permanent, unalterable set of files and directories and offering an audit trail that logs user activity in that file system. The Dell NX4 offers this feature as a U.S. Securities and Exchange Commission (SEC) Rule 17a-4(f)-compliant option and as a non-compliant option.

### ANTIVIRUS PROTECTION


The optional Celerra Event Enabler (CEE) framework contains the Celerra Anti-Virus Agent (CAVA), which provides an antivirus solution for client systems using Celerra Network Server software. The agent uses CIFS in Microsoft Windows Server® 2003 or Windows 2000 Server domains, and uses third-party antivirus software from companies such as Symantec, McAfee, Computer Associates, Trend Micro, and Sophos to help identify and eliminate known viruses before they infect files on the storage system.

### COST-EFFECTIVE TIERED STORAGE ACCESS


The Dell NX4 features the open Celerra FileMover application programming interface (API) for tiered storage access. Administrators can migrate information stored on the Dell NX4 to secondary storage as well as to purpose-built archiving solutions with comprehensive transparency to users and third-party applications. The API requires a third-party policy engine to specify migration policies.

After a migration, file metadata remains on the Dell NX4 in an offline stub file. To a client system or application, the migrated files appear as though they have not moved, enabling the Dell NX4 to remain the primary interface for clients and applications. When file access is requested, the Dell NX4 automatically and transparently retrieves the file from the secondary storage. Using this approach to store critical data on the highly available Dell NX4 and infrequently used data on cost-effective secondary storage can help reduce costs for backup hardware, software, and tape media; increase efficiency through accelerated backups, consistent protection, and increased storage utilization; and enhance service levels through increased performance, high availability, and rapid recovery.

### FLEXIBLE, ENTERPRISE-CLASS FILE STORAGE

The Dell NX4 offers a variety of advanced features that can help organizations increase storage efficiency and reduce total cost of ownership. These advanced features, combined with the flexibility of file management for Microsoft Windows, Linux, and UNIX environments and support for both iSCSI and Fibre Channel, make the Dell NX4 well suited to help meet enterprise-class requirements while also helping to simplify management and reduce costs. 

**Scott Sinclair** is a product manager and strategist for Dell storage solutions.

MORE  
  
DELL.COM/PowerSolutions

QUICK LINKS

**Full white paper:**  
[DELL.COM/NX4FileFeatureWP](http://DELL.COM/NX4FileFeatureWP)

**Dell NX4:**  
[DELL.COM/NX4](http://DELL.COM/NX4)