CA ARCserve® Backup: Protecting heterogeneous NAS environments with NDMP

FEBRUARY 2012

Phil Maynard
DATA MANAGEMENT CUSTOMER SOLUTIONS UNIT
Introduction

Everywhere you look, the amount of business critical applications and data in the corporate world is skyrocketing, and there are no signs of slowing down. This growth creates nightmares for IT in terms of storing information along with keeping the infrastructure and its associated applications available for the business at all times. In order to take advantage of best practices, meet business demands and provide a more scalable means of sharing and accessing user data, IT began looking for ways of separating this data from the application servers.

In the early 1990’s, NetApp delivered its NetApp Filer, supporting both Windows CIFS and UNIX NFS protocols, and thus was born the proprietary Network Attached Storage, NAS, market. NAS devices have gained tremendous popularity over the years – according to Global Industry Analysts, Inc., the NAS device market is forecast to reach over USD$7B by the year 2017 - due to their ease of deployment, manageability and for businesses of all sizes dealing with data growth issues, their ease of expandability.

With any hot market, many companies were quick to join and now offer their own NAS devices, with different benefits and selling propositions that make environments of heterogeneous NAS devices commonplace nowadays. A consequence of all these new devices was the inability to protect all of the data stored within them in a consistent way, without running multiple backup products, storing data in multiple storage pools or spending money to reconfigure an existing data protection environment.

In response to these issues, a group of storage companies in the late 1990’s, led by NetApp, introduced the Network Data Management Protocol (NDMP) – a standard protocol designed to allow NAS devices to be backed up and recovered by data protection products, like CA ARCserve Backup. In this white paper, we will look at the ARCserve Backup NDMP NAS Option and how its capabilities align with the needs of IT organizations of all sizes looking to protect their heterogeneous NAS environments.
Quick NDMP Primer

NDMP is an open protocol resulting from an initiative by several storage companies to create an open means of protecting NAS storage devices. The main objective of the protocol is addressing issues faced by backup vendors when attempting to backup networks of heterogeneous NAS devices, sometimes called NAS filers. NDMP benefits NAS vendors by allowing them to focus on maintaining compatibility with a single protocol instead of maintaining support for the many backup products on the market. Likewise, NDMP benefits the backup vendors by allowing them to only worry about providing support for the protocol in general and not every individual NAS device on the market. This flexibility allows backup vendors to provide special services to specific NAS devices if they so choose.

The NDMP specification, found at http://www.ndmp.org, defines the protocol in great detail if you would like to know more, however a quick overview shows that it is essentially made up of two main services:

- **Data Service:** Either reads data from disk and produces an NDMP data stream (in a specific format from the backup product) or it reads an NDMP data stream from a NAS device and writes the stream to disk – depending on whether a backup or restore is requested.

- **Tape Service:** Either reads an NDMP data stream from a NAS device and writes it directly to tape or it reads data from tape and writes an NDMP data stream to a NAS device, depending on whether a backup or restore was requested. When the tape drive/library is hooked directly to the NAS Device, all tape-handling functions are also managed by this service.

NDMP removes many of the technical barriers and business issues that exist with ensuring data are protected properly on these devices, regardless of how many exist or who manufactured them. NDMP provides many benefits to the business, among them are things such as:

- Reduced complexity
- Interoperability of systems from different vendors
- Lower administrative costs
- Better performing backups
- Allows NAS Devices to be “backup product ready” when they ship
Introducing CA ARCserve Backup NDMP NAS Option

CA ARCserve Backup is a comprehensive storage solution for applications, databases, distributed servers, and file systems. It provides backup and restore capabilities for databases, critical applications and network clients. The CA ARCserve Backup NDMP NAS Option provides IT with the ability to backup and recover data on NAS devices utilizing NDMP.

The CA ARCserve Backup NDMP NAS Option resides on the same server as CA ARCserve Backup and handles all communication between ARCserve and the NAS devices. The ARCserve Backup NDMP NAS Option provides maximum flexibility in protecting heterogeneous NAS ecosystems by enabling IT to configure various methodologies to protect them, allowing CA ARCserve Backup to be added seamlessly into existing SAN/NAS environments. The CA ARCserve Backup NDMP NAS Option also is integrated tightly with CA ARCserve Backup’s many features, including its built-in deduplication, to provide organizations with a very cost-effective solution for protecting all NAS devices in an environment.

The NDMP specification provides several options for architecting NDMP protection of NAS devices, the most popular ones that are all supported by CA ARCserve Backup NDMP NAS Option are:

1. **Local NAS Protection**: If a NAS Device has a locally attached tape device, CA ARCserve Backup triggers a server-less backup of the NAS devices’ data, directly to the tape device.

   ![Diagram showing NDMP Commands Issued By ARCserve](image)

   Restoring data in a Local NAS Protection environment works similarly to backing up the data. To restore data from tape to the NAS device is completed through CA ARCserve’s Restore Manager to configure and submit the job.

   - **Dynamic Device Sharing (DDS)**: In an environment composed of fiber-attached storage devices with one or more CA ARCserve Backup servers, complications can arise when
exposing devices that reside uniquely on the fiber. When separate fiber adapters exist to enumerate devices on a fiber loop, DDS dynamically manages all duplicate references to a device, giving you more flexibility in choosing how you design your storage topology.

DDS allows you to do the following:

- Share drives and tape libraries seamlessly between the local CA ARCserve Backup Server and the NAS Device as well as between multiple NAS Devices.
- Backup NAS data to the same tape that you backed up the non-NAS data to.
- Multi-stream the NAS and non-NAS jobs and package them up as a single job.

2. **NAS 3-Way Protection:** In a 3-way NAS protection architecture, an attached tape drive or library is shared and provides storage of backups for multiple NAS devices across the network.

In instances such as the above example, some NAS devices do not have tape devices attached to them. In a 3-Way Protection scenario with CA ARCserve Backup NDMP NAS Option, as long as one NAS device has an attached tape device, all heterogeneous NAS devices on the network can be backed up to the tape device attached to one of the NAS devices, controlled by CA ARCserve Backup.

Restoring data in a 3-Way Protection environment works similarly to the Local NAS Protection – utilizing CA ARCserve’s Restore Manager to configure and submit the job to restore the desired data from the tape library to the specified NAS device.
3. **NAS Device/Filer to Server Protection:** In Filer to Server Protection, all NAS backup data is sent directly to the CA ARCserve Backup media server and is stored in its attached media.

Filer to Server Protection is one of the most popular architectures utilized with NDMP as it allows IT to store all NAS data to any media – tape, disk, cloud, deduplicated disk, etc. – that is attached to the backup server. Along with the NAS data, this methodology allows all data for the rest of the file servers and applications on the network to be under management by CA ARCserve Backup, allowing IT to maximize media usage by appending the NAS backup data onto normal backup media.

Similar to the other NDMP methodologies, restores are managed through the Restore Manager interface within ARCserve Backup.

CA ARCserve Backup’s NDMP NAS Option is integrated with CA ARCserve’s other data protection technologies, such as replication, deduplication as well as supporting CA ARCserve’s native media format to tape or disk.
Use Cases / Benefits of CA ARCserve Backup NDMP NAS Option

The benefits of the CA ARCserve Backup NDMP NAS Option extend to several critical constituencies, including cost reduction and consolidation of storage, remote office protection and cloud data protection.

Use Case #1: Cost Reduction and Consolidation of Storage

As organizations continue to grow, so too does the amount and importance of data that needs to be protected. Business needs are demanding cost-effective solutions to minimize overhead, consolidate storage and enable the business to focus on its core growth.

Data deduplication is one of the fastest growing technologies in the data protection industry today. Deduplication, like that which is integrated into CA ARCserve Backup, is a method of reducing storage needs by reducing redundant data – across multiple servers or within a single one - while only requiring one instance of data to actually be retained on the storage media. The redundant data is replaced with pointers to the unique data copy to allow entire data sets to be rebuilt / recovered. CA ARCserve Backup’s deduplication provides many benefits to businesses such as saving money on storage media since less is required, as well as providing for longer disk retention periods of data, which results in better recovery time objectives (RTO’s) for a longer time.

Figure 1. Combining CA ARCserve Backup’s built-in deduplication with its NDMP NAS Option allows IT to build solutions integrating NDMP backups with deduplication.

Many competitive backup solutions charge separately for deduplication - which can be quite expensive to implement due to capacity licensing – CA ARCserve Backup’s deduplication is tightly integrated with the backup product and operates in conjunction with its NDMP NAS Option. Integrating deduplication
with the CA ARCserve Backup NDMP NAS Option allows for businesses to perform global deduplication on all of the data on the network, including that from heterogeneous NAS devices, allowing the business to dramatically reduce costs and consolidate storage, regardless of how much data is to be protected.

**Use Case #2: Remote Office Backup & Recovery**

Data used to be housed solely in corporate datacenters, making protection of that data very clean and simple. However, like all things that change in the world of IT, new enhanced and lower-cost technologies, business acquisitions and the general emergence of PC’s over the years have made distributed computing models commonplace in many organizations. These distributed environments create new challenges for IT, as the demands of the business now require that all corporate data, regardless of where it resides, be properly protected.

The CA ARCserve Backup NDMP NAS Option allows architecting solutions based around best practices. Using a combination of CA ARCserve data protection technologies, IT can incorporate local backup and deduplication stores in its remote offices, and then utilize CA ARCserve Replication to centralize and consolidate remote deduplication stores to a centralized site.

![Remote Sites Diagram](image)

**Figure 2.** Utilizing a Filer to Server methodology in the remote sites allows IT to dedupe data in the remote office locations before sending it across the wire, dramatically reducing costs for protecting remote locations.

Utilizing CA ARCserve’s built-in deduplication and optional replication solution dramatically reduces data protection costs for remote office environments by minimizing the amount of data being sent across the wire and curtailing the need for expensive WAN optimization technologies that add complexity and costs.
Use Case #3: Cloud Data Protection Environments

Many businesses are recognizing the benefits of integrating cloud computing into their infrastructure and in particular, wrapping their data protection story around the cloud. The cost benefits for companies of all size are definitely apparent, and CA ARCserve Backup NDMP NAS Option is an ideal solution to integrate into these environments, whether integrating into a public, private or hybrid cloud ecosystem.

CA ARCserve Backup provides several means for backing up your data to the cloud:

- **CA ARCserve Backup** offers a cloud connector to Amazon Web Services storage or integration with private clouds. Backups are run locally to disk and then migrated into a private or public cloud for off-site data protection.

- **CA ARCserve D2D** also includes cloud connectors that enable you to copy, migrate and archive important files to a private or public cloud. CA ARCserve D2D performs incremental snapshots to local disk first, then uses CA ARCserve Backup’s file copy/archive feature to copy files to the cloud, thus only file changes since the last copy are sent to the cloud, providing unlimited version control whether utilizing the cloud for off-site disaster recovery or storage reduction.

- **CA ARCserve Replication** provides the ability to replicate data to a hosting service provider or an MSP facility. Allows replication of Windows, Linux or UNIX files and data directly to the cloud and includes a variety of WAN optimization features. CA ARCserve Replication copies CA ARCserve Backup and CA ARCserve D2D backups to any remote site or cloud location and is integrated tightly with CA ARCserve Backup to ease management.

- **CA ARCserve High Availability** provides continuous replication for Windows, Linux and UNIX (physical and virtual environments) to any private and public cloud server and storage resource and then performs real-time continuous system and application monitoring with automatic and push-button failover to protect critical servers and applications and minimize business disruptions during planned and unplanned outages. The Full System Protection feature allows replication of an entire physical and virtual system (including application and data) to an offline virtual server, eliminating the need for additional software licenses. Then you can use automatic and push-button failover to recover.

The CA ARCserve Backup NDMP NAS Option integrates with these different CA ARCserve products to allow maximum flexibility when protecting heterogeneous NAS environments.
Conclusions

A key element of deploying any new storage solution is ensuring it is easily integrated into the existing environment and strategies in place. Having to switch or re-architect an existing backup infrastructure to ensure new NAS devices on the network get protected is counter-productive to the nature of NAS and is an expenditure that many businesses cannot afford.

CA ARCserve Backup’s NDMP NAS Option provides a straightforward and flexible solution that provides IT the ability to add new devices while having them integrated into existing backup policies and strategies. CA ARCserve Backup also extends its powerful functionality of deduplication, cloud computing, replication and many others to the heterogeneous NAS environment through the use of the CA ARCserve Backup NDMP NAS Option.