VERITAS The truth in information.

Veritas Backup Exec.

Protecting Network Attached Storage (NAS) devices.

OVERVIEW

Veritas Backup Exec™ is the backup solution without barriers, delivered your way. You choose what to back up, where to store it and how to pay for it. Your data remains secure and available at every stage—whether backing up on-premises to the cloud, protecting workloads within the cloud, recovering from the cloud or connecting to on-prem storage. With Backup Exec you can connect with an ever-expanding family of solutions to help you to run your business confidently.

Backup Exec is available for purchase in either perpetual or term subscription licensing, with the level of functionality you require—Bronze, Silver or Gold. Bronze edition offers the most economic option. Silver edition offers the most-used features. Gold edition includes all features and functionality available in Backup Exec. Your purchase is based on the amount of front-end data you need to back up. Your chosen license-set is available in whatever quantities you require.

Backup Exec gives you comprehensive protection against external threats. So if the unthinkable happens, your critical data is backed up and ready to be recovered, quickly and easily.

Key benefits

- Flexible methods of backup and restore.
- Significantly reduced recovery time with Direct Access Restore.
- Reduced backup management.
- Greatly expanded NDMP device support.
- Automated NDMP filer data duplication to tape.
- NDMP device support increases the number of disk targets that can be selected for disk-based data protection.
- Automatically move backup data through different storage tiers, including cost-effective cloud storage, as it ages.
- Use deduplication and compression where it makes sense to improve bandwidth and storage use.
- Embrace unified data protection to make backup simple again, something point products can't achieve.

INTRODUCTION AND OVERVIEW

The network data management protocol (NDMP) is an industry-standard programming interface that provides best practice backup and recovery for NAS systems. A NDMP-approach enables a backup server to communicate directly with a NAS filer and to transmit data to the specified backup storage device. NDMP eliminates the need for backup vendors to write device-specific code for NAS devices to facilitate backup.

The Challenge of Protecting NDMP Filers NDMP Filers, or NAS devices, reside on the network with the primary purpose of providing file services. NAS devices that use standard operating systems (for example, Windows-powered NAS devices) support the installation of backup agents, and can be backed up like any other file server. However, some NAS devices use a custom operating system that does not support third party backup agents. A standard backup interface for NAS devices exists in the form of the network data management protocol (NDMP)—which is a backup standard for NAS devices that do not support installation of a backup agent.

Many customers are faced with a confusing number of options and configurations when it comes to backing up and restoring their network attached storage (NAS) servers. Most NAS vendors and data protection providers have multiple options for protecting your NAS environment. This solution brief will help you make sense of the options available to you for NAS backup and restore in Backup Exec.

BACKUP EXEC AND NDMP

Backup Exec provides a comprehensive data protection solution that supports a wide range of platforms and applications found in today's data centers. It includes centralized administration and reporting, media management, automated backups and restores.

Feature	Description	Benefit
Multiple Backup/Restore Methods	Provides full and varying levels of incremental backups: Backup at the directory level and restore at the file level.	Flexible methods ensure that backups occur during the backup window and reduce tape and disk resources.
Backup/Restore Access Control Lists	Allows backup of the access control lists during the backup, which contain the user's or group's access rights to each share.	Ensures that security rights can be retained during a restore.
Verify Backup/Restore	Allows Backup Exec to verify the integrity of the data without actually restoring the data.	Helps ensure that your NDMP data is truly protected and recoverable.
Direct Access Restore	Uses Direct Access Restore (DAR) during the restore job. With DAR-enabled recovery, Backup Exec can specify the exact location of a file in a backup data stream. This allows the NDMP server to read the data applicable to the file being restored.	Significantly reduces the recovery time by decreasing the amount of information that is processed.
File History Control	Prevents the generation of file history data; backup times are not unnecessarily increased. By enabling file history, recovery is optimized for selected subsets of data in the backup image. If the file history is unavailable and you must later restore data, you can restore the entire backup image.	Improve backup time. Improve granular recovery of files.

The Backup Exec NDMP option extends the capabilities of Backup Exec to include native backup and restore of NAS appliances. Supported versions of software for these vendors' NAS appliances are listed on the Backup Exec Hardware Compatibility List (HCL). This allows you to create backups of data on an NAS without interrupting client access to the data. Backup Exec incorporates the protection of NDMP-enabled NAS into a single solution by enabling tape/VTL library sharing, drive sharing, direct access recovery and auto configuration. The following is an overview of the feature set provided by the NDMP option in Backup Exec:

HOW IT WORKS

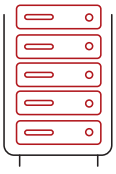
The Network Data Management Protocol is a standardized protocol for controlling backup and recovery data between primary and secondary storage devices like filers and tape libraries. By enabling NDMP protocol support on a NetApp Filer, the filer can carry out communications with NDMP-enabled backup applications (data management applications, or DMAs) such as Backup Exec.

NDMP BACKUP ARCHITECTURE

NDMP architecture consists of three entities:

Data management application
Backup Exec in our case is the DMA, which controls the NDMP session

NDMP data server
Transfers data between primary storage (e.g. s) and the data connection



NDMP tape server
Transfers data between secondary storage (e.g. tape) and the data connection

The Backup Exec NDMP Option supports the following NDMP backup topologies: A tape device directly attached to a NAS device (direct-attached), a tape device directly attached to another NAS device of the same brand (NAS device-to-NAS device) and a tape device attached to a backup server (NAS device-to-server).

DIRECT NDMP (TAPE DEVICE DIRECTLY ATTACHED TO A NAS DEVICE)

Direct NDMP backup is identical in practice to local NDMP backup, but differs in the implementation with sharing of SAN tape drives in a library with a Backup Exec server. With the Enterprise Server Option Shared Storage Option (SSO), Backup Exec can share tape resources between the Backup Exec servers and NAS. This requires the NDMP host to be SAN-attached and zoned to see the tape library. The Backup Exec server controls access to the tape device.

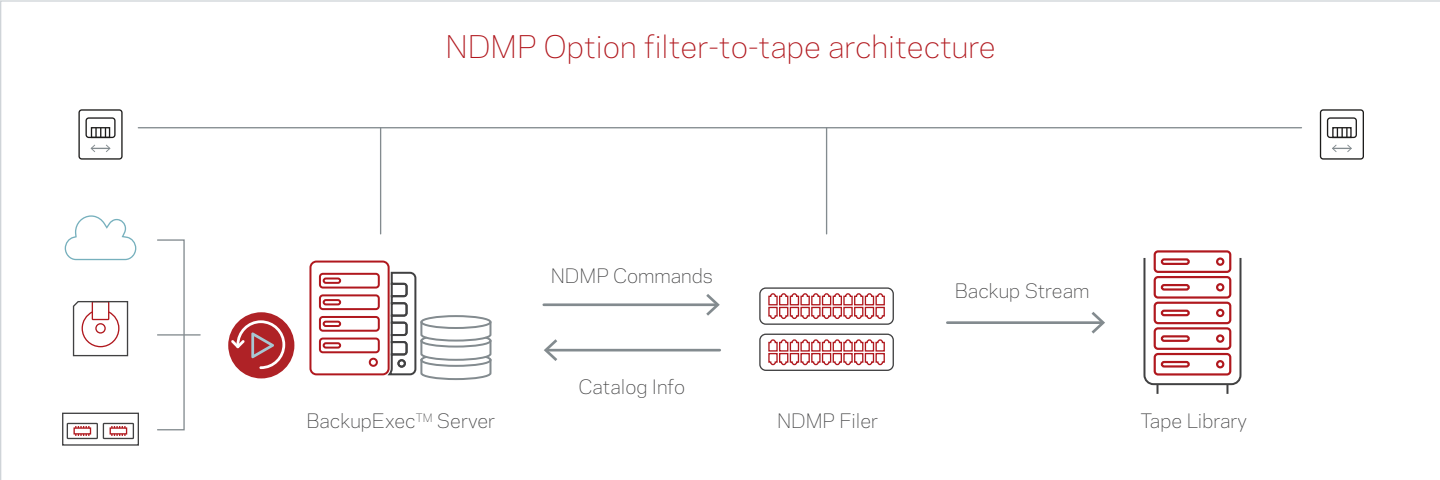


Figure 1: NDMP – Direct Attached

REMOTE NDMP

Remote NDMP backup incorporates the same tape device support as direct backup, but sends the data stream over the network and through a Backup Exec server. This can provide a few advantages, including support for writing backup data to disk with the introduction of Backup Exec. This can also result in some disadvantages, including slower network transfer speeds.

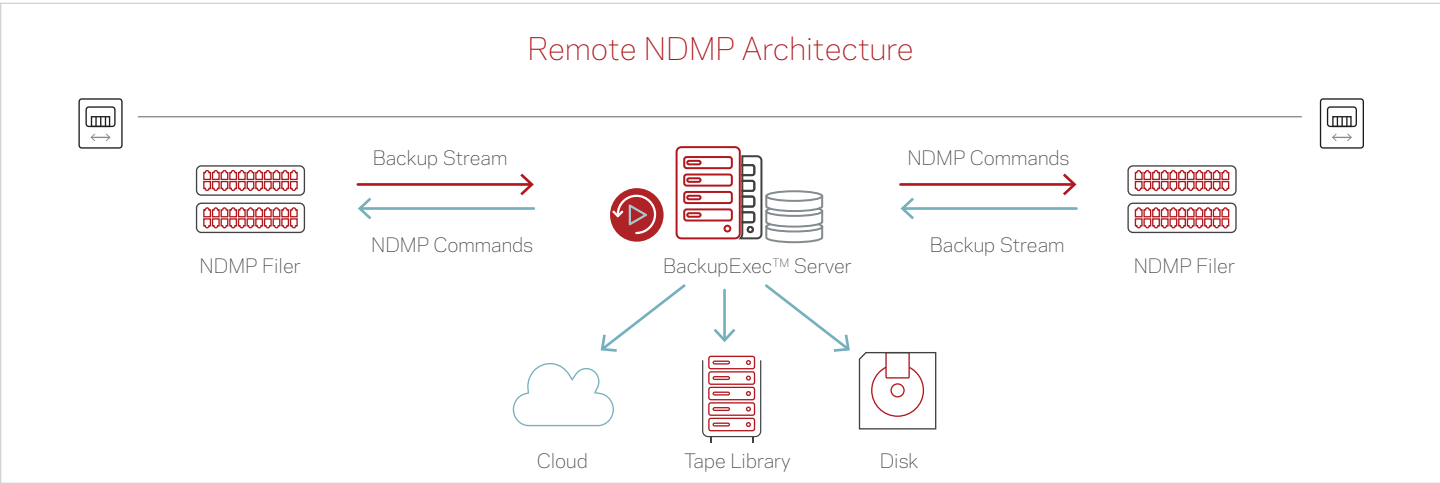


Figure 2: Remote NDMP

3-WAY NDMP (FILER-TO-FILER-TO-TAPE BACKUP TOPOLOGY)

In a three-way backup or restore, data is sent from an NDMP host over a LAN to a storage device that is attached to another NDMP host. This backup contrasts with local NDMP backup or restore where the data is sent directly to a storage device attached to the NDMP host. An additional option for protecting NAS devices is to utilize file sharing protocols such as CIFS or NFS and "walking" the file system to back

it up. While this may be an effective architecture for smaller NAS environments, it typically is not appropriate for most enterprise-class NAS devices and therefore is not discussed in this document.

Note: Backup Exec requires that both the participating NDMP servers must be from the same vendor.

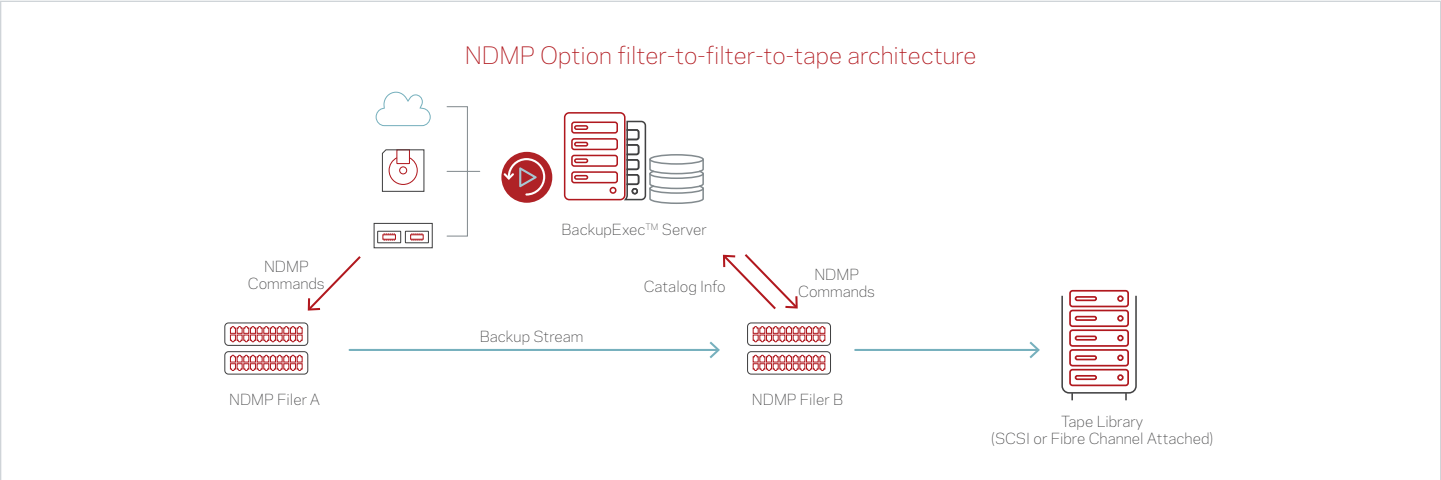


Figure 3: 3-way NDMP

SYSTEM REQUIREMENTS

To use the NDMP Option, the Backup Exec server must have the following:

- Backup Exec must be installed on a server running Windows Server 2003 R2/2008/ 2008 R2/2012/2012 R2 operating systems.
- The network-attached storage NDMP server must run version 4 of the Network Data Management Protocol.
- The NDMP server with the Network Data Management Protocol enabled.

You can find a list of compatible types of storage at www.backupexec.com/compatibility

Note: The NDMP Option is installed locally on the Backup Exec server as a separate add-on component of Backup Exec. No files are copied to the NDMP server.

SUPPORTED NDMP PLATFORMS

The NDMP platform support information is listed below. This information is organized by vendor manufacturer/model(s). Refer to the Backup Exec Hardware Compatibility List for minimum software required method of connection, and any other important notes or information relevant to the hardware and its compatibility.

LICENSING

The NDMP Option is included in Gold subscription editions.

SUMMARY

Backup Exec protection for NDMP Filers is designed to be flexible and easy-to-use. With Backup Exec NDMP Option, NDMP Filer data can be protected for immediate recovery or long-term storage. IT Administrators can leverage their investment in Backup Exec to protect NetApp Filers, centralizing management and reducing overall administration costs. The NDMP Option not only helps ensure the quality of backups, but it significantly reduces backup and recovery time with its Direct Access Restore and:

- Supports the backup and restore of NDMP NAS servers including NDMP NetApp, Dell EMC Isilon, Dell EMC VNX series, IBM N-Series storage configurations with tape devices attached.
- Protection for NDMP devices residing in remote locations including in a Storage Area Network (SAN) configurations.
- Automated NDMP filer data duplication to tape.
- Overall support for NDMP devices that greatly expands the number of disk targets that can be selected for disk-based data protection.

By combining NDMP platform with Backup Exec, businesses will have confidence that their critical data is harnessing the gold standard in Windows data recovery.

FOR MORE INFORMATION

Backup Exec web page http://www.backupexec.com
Backup Exec admin guide http://www.backupexec.com/admin
Backup Exec resources http://www.backupexec.com/resources
Backup Exec compatibility http://www.backupexec.com/compatibility
Backup Exec support http://www.backupexec.com/support
Backup Exec training www.backupexec.com/training
Backup Exec user forum http://www.backupexec.com/forum
Backup Exec blogs www.backupexec.com/blogs
60-day trialware for Backup Exec http://www.backupexec.com/trybe
Backup Exec promotions http://www.backupexec.com/save
Backup Exec subscription www.backupexec.com/subscription
PartnerNet https://partnernet.veritas.com/
Find a Backup Exec Partner http://veritas.force.com/public

ABOUT VERITAS TECHNOLOGIES LLC

Veritas Technologies empowers businesses of all sizes to discover the truth in information—their most important digital asset. Using the Veritas platform, customers can accelerate their digital transformation and solve pressing IT and business challenges including multi-cloud data management, data protection, storage optimization, compliance readiness and workload portability—with no cloud vendor lock-in. Eighty-six percent of Fortune 500 companies rely on Veritas today to reveal data insights that drive competitive advantage. Learn more at www.veritas.com or follow us on Twitter at @veritastechllc.

Veritas Technologies LLC
500 East Middlefield Road
Mountain View, CA 94043 USA
+1 (866) 837 4827
veritas.com

For specific country offices and contact numbers, please visit our website.
veritas.com/about/contact

VERITAS™
The truth in information.

V0665 4/18