WHITE PAPER: TECHNICAL OVERVIEW

symantec.
Confidence in the connected world.

NetBackup Desktop Laptop Option

Technical Product Overview

Mayur Dewaikar, Sr. Technical Product Manager
NetBackup Platform

Symantec Technical Network White Paper

Executive Summary

Data Protection Challenges for Desktops & Laptops

When it comes to protecting data on desktops and laptops, today's IT administrators are faced with a daunting challenge. An increasing amount of important corporate data resides on desktops and laptops that are not backed up on a regular basis. And an increasing number of workers use laptops on multiple desktops making schedule backups less reliable. Providing centralized protection for desktop and laptop systems can consume valuable network bandwidth and storage resources. These resource issues have led companies to resort to ad-hoc solutions. The most popular method for protecting desktop and laptop data relies on manual, user-initiate backups through the use of shared folders on a corporate network (i.e., a personal "z" drive or some other arbitrary letter). Obviously this puts data at risk because many users fail to configure and regularly run these backups.

Many system administrators will readily admit that most users fail to copy their data to these shares frequently enough to provide effective data protection. The result is lost data and worker productivity. The cost to recreate lost data can be surprisingly high. Laptops pose the greatest challenge because their users are typically on the road, have infrequent connections to the network and rarely take the time to manually protect their data. Finally, there is also a growing population of users that want to keep files synchronized between their desktop and laptop machines. Individual backup applications that reside on corporate PCs do not provide the automation and centralization necessary to deliver reliable data recovery and efficient use of existing IT resources.

An Efficient Solution using NetBackup™

To meet the needs of corporations with valuable data on desktop and laptop computers, Symantec offers the Veritas NetBackup™ Desktop Laptop Option. It offers the following key benefits:

- Provides continuous disk based backup protection whether in the office or on the road
- Synchronizes files between multiple desktops and laptops
- Integrates into existing IT infrastructure and policies lowering total cost of ownership
- Allows users to quickly restore files without assistance
- Lightweight design eliminates the need for a dedicated application server

The NetBackup Desktop Laptop Option offers ***continuous disk-based protection*** for customers regardless of physical location or connectivity to a network. It not only enables customers to restore their own files, but also enables them to synchronize work files between multiple desktops and laptops. The product easily integrates into existing IT infrastructures because it leverages both local and network-based storage for backups, simplifying automation and centralization of backups. Customers can work and travel with peace of mind, knowing that their business data can be recovered in the event of loss.

Customers who have multiple desktops can use the NetBackup Desktop Laptop Option to automatically synchronize data between their computers via a network share so they have the most up-to-date versions of files no matter which computer they use. An intuitive user interface allows customers to easily retrieve their own data or files whether in the office or on the road.

The architecture of the NetBackup Desktop Laptop Option eliminates the need for a separate dedicated application server to process and store backup data. Administrators can choose local and/or network-based storage for this data. This enables the solution to easily fit into the existing infrastructures and offer consistent data protection policies with minimal investments in hardware or additional training.

How the Desktop Laptop Option Works

Centralized Administration

IT administrator's have the ability to customize the backup environment through the use of Profiles. Profiles provide an easy way to logically group users by department or function and tailor specific parameters to meet each group's needs. Within each profile the administrator can:

- Set backup schedules –manual, periodic, scheduled, and continuous
- Specify the number of file versions retained
- Specify the bandwidth for the backup
- Include or exclude drives, folders or files from backup
- Set the maximum amount of storage each user is allocated
- Determine the extent to which the desktop user can modify settings.

When a customer's computer connects to their corporate network, their files will be copied to their Network User Data Folder based on their assigned profile. The profile also determines when backups should be performed – continuously, periodically, on a schedule, or manually.

When using the continuous protection mode, backups occur regardless of whether the user is online or offline. When not connected to the network, the program copies backs up files to a local folder on a customer's machine. When the computer reconnects to the network, the files will be automatically moved from the local folder to their assigned network folder. The same sequence occurs when users are online. Files will be backed up to both local and network folders as defined in their profiles. To manage the amount of data stored on local machines, system administrators can specify different retention periods for backup data on local and network folders. Finally, all of these settings can be controlled centrally by a system administrator or control of these settings can be given to end-users.

Delta File Transfer

The delta file transfer feature enables a more efficient incremental backup process that reduces storage consumption. When this option is enabled, the initial backup requires transfer of the entire file. Subsequent backups require only the transfer of changed file segments, reducing the bandwidth required, improving backup speed, and reducing storage costs.

Restore Files Anytime

Customers can restore a previous version of a file without being connected to the network. Local revisions are maintained on a customer's machine. If a user overwrites a specific document while on an airplane or in a hotel room and needs a past version, they can restore a previous version without IT assistance.

File Synchronization

Customers can access their data from multiple desktops at multiple locations using the synchronization feature. By selecting this option, customers can access files or folders across protected machines where and when they need it, regardless of the file's original location.

Administration of User Storage Policies

The NetBackup Desktop Laptop Option offers a flexible approach to the assignment and management of storage for backup data. System administrators can import users and assign them to existing network storage shares as Network User Data Folders, or they can automate the creation of network-based folders for each user when the first backup occurs. The following key features simplify the assignment and management of storage for backup data

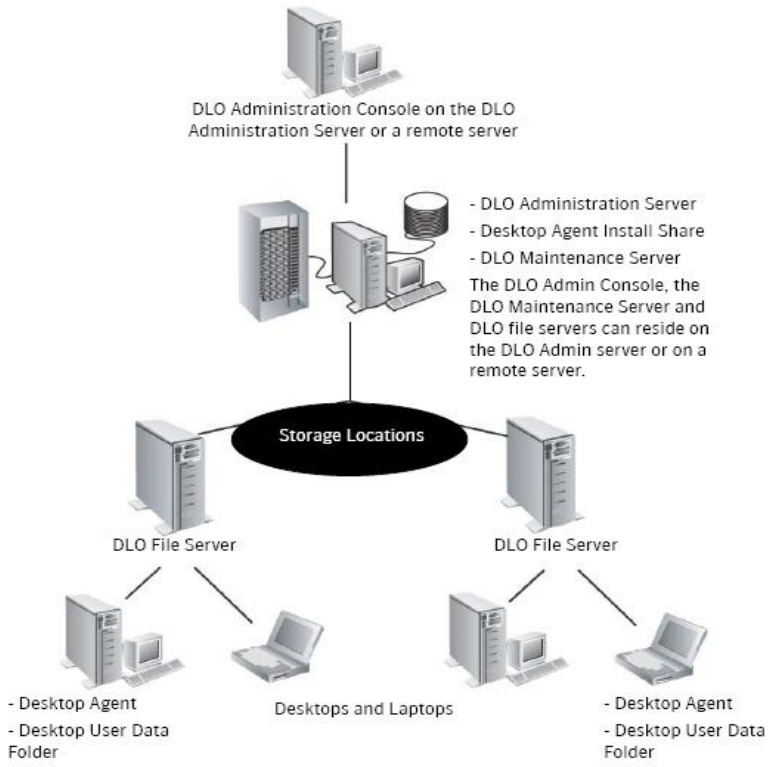
Automate network storage assignments– When the Desktop Agent is first run on a desktop or laptop it will automatically assign the user a profile that includes both a local and network storage location (network user data folder).

Customize backup version control– Administrators or users can determine the number of file versions retained and the amount of storage space allowed for both network and local storage. This enables end-users the flexibility to specify storage for local revisions and system administrators to manage network storage usage.

Enable different recovery points for local and network data– Each backup selection can be configured to store a specified number of revisions in a local data folder. Road warriors and executives who don't connect as frequently may want to maintain a large number of local copies for all data, whereas those customers with desktops and network connectivity may have very little need to store local revisions.

Architecture Overview

The NetBackup Desktop Laptop Option environment consists of four main components - the administration console, a network file server, the desktop laptop agent, and an optional maintenance server (used for delta file transfer option).



The Desktop Laptop Option Administration Console

All administration functions can be performed from the main console. These include profile management, status and alert monitoring, storage management, and the initiation of restore jobs for individual user machines. The console also provides a quick summary view of tasks and latest status.

Administration and profile settings are stored in a single MSDE (Microsoft Data Exchange) database on the local server. Information such as profiles, user specific settings, machine names, storage designations and alert events are kept here. The desktop agents use this database to obtain configuration information. A local copy of this configuration data is used when a computer is not connected to the network.

File Servers

Network storage locations for are hosted on file servers. The NetBackup Desktop Laptop Option supports network-attached storage (NAS), storage-area networks (SAN), and direct-attached storage (DAS) as storage devices. It also supports NTFS, FAT, and FAT32 partitions as storage locations, but FAT and FAT32 are not recommended.

Desktop Agent

The desktop agent is the component that resides on the individual user's desktop or laptop computer. It initiates backups and provides customers with an easy interface by which they can recover their data. It protects customer data by backing up designated files to the local user folder (i.e., Desktop User Data Folder) and their assigned network folder (i.e., Network User Data Folder). This data can be restored at any time by the administrator or by the user. If a user has multiple machines, the backup data that is stored can be made available to the user on all of their computers by synchronizing their data. Synchronization is initiated by the user and ensures that the most recent file version is available to them when and where they need it. Synchronization is quick and easy to set up, and uses domain level security. Once synchronization is established, files are readily available and easy to restore from each of the user's synchronized computers.

A system administrator performs the initial configuration of the agent through the use of profiles. If desired, the administrator can give the user rights to change agent settings. Depending on the rights granted, the user my or may not be able to restore files, synchronize files, configure backup selections, set schedules, view history, and perform other tasks.

Maintenance Server

A maintenance server is required to enable the delta file transmission and storage feature. The maintenance server manages the deletion of previous delta revisions from storage locations. Although the maintenance server is used only for the Delta File Transfer feature, it is enabled and installed by default on the desktop laptop administration server. In large installations (greater than 5000 end-users) it may be more efficient to have one maintenance server for each storage location host (i.e. file server). If the administration server is also the Storage Location host, then no additional steps are required to configure the maintenance server.

From Continuous Data Protection to User-Initiated Backups

The NetBackup Desktop Laptop Option provides four different backups schedule modes: Continuous, Periodic, Scheduled or Manual. How often the backups occur and when depends greatly on how the backups are configured and what type of operating systems are in the organization. The following provides an overview of these four modes:

Continuous Mode – Continuous protection copies a file when it has been saved and closed. This allows for the greatest level of protection. With personal Microsoft Outlook files or .PST files as they are commonly referred to, protection can occur when the program is in use. Continuous protection is available on systems that support the Windows Change Journal (Windows 2000 +) and have data residing on a NT File System (NTFS) volume. File Allocation Table (FAT) volumes do not support continuous operation.

Periodic Mode – Periodic protection copies user files based on a pre-determined interval. The default interval is set to have a backup occur every 30 minutes, which should be sufficient for most users. If your system doesn't support continuous mode or the user data resides on a FAT volume, then the use of Periodic protection is recommended.

Scheduled Mode – Scheduled protection copies user files based on a frequency set by the administrator. This option can be used if the user data doesn't change often or if you prefer to have operations run on an hourly or daily basis.

Manual Mode – Manual protection copies the data when the user initiates it from the Desktop Agent or the administrator initiates a backup from the Administration Console. Because this option is not automatic and does not ensure that the data copies and saved for the user is current, it is recommended that you choose use this option only to supplement one of the preferred methods mentioned earlier.

Installation Overview

Administration Console Overview

The machine running the DLO administration console must be in a Windows Domain or Active Directory. Double click the setup.exe file to start the installation process. After installation of the Console the option to configure protection for desktops and laptops will be located under the Tools menu. During installation, a share is created for the Desktop Agent files.

Built-In Configuration Wizards

The Getting Started Wizard allows administrators to setup the Desktop Laptop Option easily and quickly. There are three basic steps to follow:

1) Create a Profile, to determine which files are backed up, when files are backed up, and the level of interaction the desktop user has the Desktop Agent.
2) Determine where user data will be stored on the network. The Desktop Laptop Option requires an individual user data folder on the network for each user. If Storage Locations are used, they will automatically create Network User Data Folders for each new Desktop Agent user. If network data storage folders already exist for each user, they can be added to the Desktop Laptop Option individually or imported in bulk.
3) Create an Automated User Assignment to automatically assign a Storage Location and Profile to new users, or configure new users manually.

Authentication and Communication

The administration console can be managed by any user who has full admin rights on the administration server. The user's account must be a domain account and must have rights to create network shares and manage permissions of network shares and directories on any remote server used for Storage Locations or network user data folders. This is commonly accomplished by using a domain administrator account, or can be accomplished by granting a standard domain account local administrative rights to the servers hosting the DLO resources.

DLO requires domain accounts. Every Desktop Agent user must log in to DLO using a domain account. If you have users who log in using local accounts, they can still use DLO, but they must have domain credentials to authenticate with DLO.

Flexible User Data Folder Options

User Data Folders are used by the NetBackup Desktop Laptop Option to store protected and synchronized data for each Desktop Agent user. As previously noted, there are two kinds of user data folders -Network User Data Folders, located on the network, and Desktop User Data Folders located the local machine of the user. These locations can be configured for use based on the frequency with which a user remains connected to the network. For example, users that do not travel or work on desktops could be configured to backup directly to their network share user data folder. By contrast, road warriors or users that have sporadic network connection should be configured to backup to their machine's user data folders first, to ensure that a copy of their backup has been made safely to at least one location.

Desktop Agent Installation Overview

The Desktop Agent is the software that runs on the individual user's desktop or laptop. The Desktop Agent can be installed by the administrator or the user very quickly. The administrator has the option of pushing out the Desktop Agent by silent installation or login scripts. Alternatively, users can access the software from a designated share: <\\DLO Administration Server\DLOAgent> for installation. The first backup runs as specified in the Profile after the software is installed and automatically configured.

Data Encryption

The NetBackup Desktop Laptop Option utilizes 128-bit AES encryption at the file level. The encrypted files are copied up to the file server using normal Windows networking protocols. The file content is transferred and stored encrypted, but directory names, file names and attributes are not encrypted.

Each user is assigned a unique encryption key that is stored in the Desktop Laptop Option database. When the Desktop Agent connects to the database for the first time, it transmits a key over the network. With subsequent connections a locally cached copy of the key is used. Administrators can restore encrypted data from the Administration Console.

Microsoft Outlook Personal Folders (i.e., .PST files)

The Desktop Laptop Option protects Outlook personal mail data files (hereafter referred to as .PST) by using the Microsoft Mail API (MAPI). These files can be backed up while Outlook is open and in use by the user. As a backup is performed, only mail messages that have changed or are new from the last backup are copied. This helps to lower storage overhead and bandwidth usage. An initial full backup is performed for the entire .PST file. Subsequent changes are made incrementally and added on a daily basis.

- It is important to make sure that the .PST files are listed in the default mail profile and selected for backup in a backup selection.
- If you need to restore a .PST file, the entire file is restored from the last backup. It is not possible to restore individual messages.

Lotus Notes Protection (i.e., .nsf files)

The Desktop Laptop Option protects Lotus Notes personal mail data files (hereafter referred to as .NSF) by using the Lotus Notes "C API" (CAPI). These files can be backed up while Lotus Notes is open and in use by the user. As a backup is performed, only mail messages that have changed or are new in the archive as compared to the last backup are copied. This helps to lower storage overhead and bandwidth usage. In addition to the mail archive file, DLO can backup BOOKMARK.NSF and NAMES.NSF incrementally.

Open File Protection for Other Files & Applications

There are backup limitations on files that are always opened or locked. The Desktop Laptop Option will attempt to back up files when they are closed or saved. If a file cannot be backed up because it is open, it will be added to the Desktop Agent's pending list and attempt to back up the file during the next backup. Some files will not be backed up because they never close.

Restoring Open Files

If the restore process encounters a file that is in use, the user will be asked if they want to restore the file or skip the file. If the user selects to restore the open file it will be replaced when the next reboot occurs.

Data Synchronization Feature

The Desktop Laptop Option synchronization feature allows for users who have multiple machines to have access to their data when they need it. Synchronization is configured by the user. Use of this feature can be enabled or disabled by the administrator. Any of the user's data residing on any of the machines will be accessible from the current machine once the data has been synchronized between them. The Synchronized Selections View lets the user manage which folders are synchronized across their machines.

Conflict Detection and Resolution

If a synchronized file is modified on more than one computer without updating the file with the Desktop Agent, a conflict will occur. You will be notified of the conflict and the Desktop Laptop Option will automatically select the most recently modified file, but will retain both revisions. For example, a conflict will occur when the same file is modified on both the desktop and laptop and the laptop is disconnected from the network. When the laptop is subsequently connected to the network, synchronization will detect a conflict.

Protecting the Environment and User Data with NetBackup

While the Desktop Laptop Option provides superior data protection for both desktop and laptop computers, NetBackup can further protect and ensure recovery of this end-user data in aggregate by performing a backup of the network-based storage used to store the data for each individual. A policy can be created in NetBackup easily accomplished by placing the desktop and laptop backup data in the regular NetBackup backup rotation.

Summary

All organizations have critical data on desktops and laptops that should be protected and many IT managers will acknowledge that this data is not adequately protected today. The NetBackup Desktop Laptop Option can address this gap in an efficient and reliable manner. In addition to providing continuous data protection and user-driven recovery, it also offers a synchronization feature which enables customers to access to data from multiple machines. IT managers now have an effective desktop and laptop data protection solution that deploys quickly, eliminates the overhead associated with end-user data recovery requests, and improves their customer satisfaction.

For more information about the NetBackup™ Desktop Laptop Option, please visit: **www.symantec.com/netbackup**

About Symantec

Symantec is a global leader in infrastructure software, enabling businesses and consumers to have confidence in a connected world. The company helps customers protect their infrastructure, information, and interactions by delivering software and services that address risks to security, availability, compliance, and performance. Headquartered in Cupertino, Calif., Symantec has operations in 40 countries. More information is available at www.symantec.com.

For specific country offices and contact numbers, please visit our Web site. For product information in the U.S., call toll-free 1 (800) 745 6054.

Symantec Corporation
World Headquarters
20330 Stevens Creek Boulevard
Cupertino, CA 95014 USA
+1 (408) 517 8000
1 (800) 721 3934
www.symantec.com

12/07 13583305