TECHNICAL BRIEF: SYMANTEC NETBACKUP™ 7.5 TECHNICAL BRIEF

Symantec NetBackup™ 7.5 Technical Brief

Who should read this paper

This document is intended for backup administrators and other IT professionals responsible for backup architecture and strategy. It is a technical overview of the top new features available with NetBackup 7.5 and includes an overview of the business value and key underlying principles of each new feature.

Content

Overview

While backup may take many forms, recovery should not. Over the years organizations have looked to a variety of point products and technologies to address their IT SLAs. Whether it's snapshots, deduplication, replication, virtual machine protection, or the private cloud. The benefit is that for every pain point, there is a solution out there to address it. Unfortunately cost and complexity can get in the way of achieving the perfect data protection strategy. In the real world, the balancing act is between meeting recovery time and recovery point objectives, yet still keeping Capital Expenditure (CapEx) and Operational Expenditure (OpEx) costs down.

Symantec NetBackup™ 7.5 is the single backup solution when recovery is needed, whether from tape, disk, snapshot, cloud–physical or virtual. Only Symantec NetBackup™ 7.5 with V-Ray technology can unify backup, deduplication, replication, snapshots, and appliances with support for VMware® and Microsoft Hyper-V® in a single product helping to reduce complexity and cost.

This document overviews the top seven new features available in NetBackup 7.5 and outlines the business value and underlying principles of each feature.

NetBackup Replication Director

Feature description

Replication Director integrates the power of array-based snapshot technologies with traditional backup data management. Replication Director is designed to be the single integration point between primary storage and storage array hardware and backup operations.

Array-based backups have traditionally introduced limitations in the backup process. Long-term retention can be costly. Individual files or objects are commonly not cataloged and therefore difficult to find. Integration with other backup targets has been problematic at best and sometimes not even possible. Moving data from short-term array snapshot storage to longer-term storage (e.g. tape) requires manual intervention or custom scripts.

Replication Director solves all of these issues by managing array snapshots and automating replication to any supported secondary and tertiary storage as well as tape creation. Provisioning of replicas, cataloging, and granular file recovery are all controlled by NetBackup.

Replication Director uses the proven NetBackup proven OpenStorage Technology (OST) API to interface with the storage arrays of Symantec's partners. With the NetBackup 7.5 release, Replication Director provides support for NetApp® storage systems. Subsequent NetBackup releases will extend this support to additional primary storage and storage array hardware array vendors and Symantec storage management solutions.

For details of the hardware supported by Replication Director please check the NetBackup 7.x Hardware Compatibility List.

Business value

In this joint solution, NetBackup creates, catalogs, and manages NetApp Snapshot copies and replication to deliver a future-ready backup strategy. Management is centralized enabling administrators to leverage their existing NetBackup skills and expertise to manage traditional backup processes as well as high speed snapshot and replication processes. Administrator defined NetBackup scheduling and retention policies are used to control when NetApp Snapshot copies are automatically created, maintained, and expired. This removes the barriers between processes; significantly reducing the time spent managing data protection and making it easier for administrators to easily gain access to powerful data protection tools within the NetApp array. The integrated solution provides the speed of snapshots and the recoverability of backup in one solution.

Replication Director leverages new OST feature sets to automatically control array-based snapshots and replication as part of a comprehensive data protection strategy. The scheduling, cataloging, and subsequent migration of snapshot data and images is completely controlled by Replication Director. This integration across many levels of backup hardware allows backup administrators to take advantage of the relative strengths of any tiered backup medium by automatically migrating data from array snapshots to other arrays, VTL's, deduplication targets, the cloud, tape, or any combination of these technologies. All of this capability is powered by Symantec's OST.

Benefits of using NetBackup Replication Director include:

- **Centralized data protection management—**The storage administrator no longer has to be tasked with managing snapshots and replication. These can now be completely controlled by the backup administrator from within a single console across the NetBackup global data protection environment. Subsequent backup data migration scheduling and retention is automatically controlled within the NetBackup policy-driven framework.
- **Automatic snapshot management—**Replication Director eliminates the need for separate array snapshot management, point solutions, or scripts. Replication Director controls the entire snapshot process for both backup and restore operations. Using the NetBackup scheduling process, array snapshots are automatically created, maintained, and expired per a backup administrator defined retention schedule.
- **Snapshot copy monitoring—**NetBackup OpsCenter can be used to monitor the snapshot copy process from start to finish. After the original snapshot has been created, OpsCenter monitors and reports the status of each subsequent data migration event.
- **Powerful global search and granular restore—**As part of backup processing, data within the snapshot can be indexed into the NetBackup catalog as a one of the processing steps. Data that exists across multiple snapshots can instantly be found and restored. Backed up data can exist on one or multiple destinations. Because this data is cataloged and controlled by NetBackup, granular file or entire volume restores can be processed from any backup destination, regardless of whether the data exists on a snapshot, in the cloud, or any other supported backup target. This global search and granular restore capability is available through the OpsCenter Operational Restore feature. For more details, see the "Operational Restores with OpsCenter" section.
- **Off-host processing—**Backup impact on production systems is minimized by aligning storage tiers with data protection activities such as backup generation and data cataloging.
- **Enhanced recovery—**Backups based on array snapshots can be executed as often as necessary to meet aggressive restore requirements. Restores can be processed instantly from ultra fast storage array snapshots or from any backup data copy that has been created via the Storage Lifecycle feature. In this way, restores can be processed from the backup copy that can provide the fastest possible restore.

Underlying principles

NetApp arrays feature two replication engines for protecting data on a secondary system: SnapVault and SnapMirror. SnapVault is designed for high speed disk-to-disk backup, enabling an administrator to keep a few Snapshot copies on primary storage for near term recovery and replicate snapshot copies to a secondary system for longer term, high speed recovery. SnapMirror is designed for disaster recovery and makes an exact replica of all application data as well as Snapshot copies on a secondary system providing multiple recovery points to failover to in the event of an outage.

SnapVault and SnapMirror offer powerful data protection options, but have been traditionally managed from an independent interface. This means that backups administered from the traditional backup application and array snapshots (used as part of a backup strategy) are administered and monitored separately.

This is where the NetBackup OST API comes into play. The OST API is designed to allow intelligent disk devices to integrate with NetBackup. The NetBackup and NetApp engineering groups have collaborated to integrate the NetBackup OST API with a plug-in created and maintained by NetApp. This plug-in to API integration delivers seamless connectivity and management between NetApp FAS and NetBackup. NetBackup administrators can now manage, control, and schedule the entire NetApp Snapshot copy process from within NetBackup. The result of this effort is called NetBackup Replication Director.

Replication Director uses OST to access NetApp volumes via the NetApp OnCommand Server (formerly known as Data Fabric Manager or DFM). Using the OST API to plug-in integration, NetBackup instructs the array to create and, if desired, replicate the snapshot from primary to secondary storage. Additionally the NetApp Snapshot copies can be replicated to multiple array volumes or duplicated to any supported tertiary storage such as a deduplication target, cloud-based storage, or a tape drive.

The instructions to create the initial snapshot are based on a NetBackup policy. If the snapshot is to be replicated, these instructions are controlled through a NetBackup Storage Lifecycle Policy. Once scheduled, this entire process is completely automated. No backup image can be moved, expired, or deleted from any of these volumes unless NetBackup initiates this action.

With the initial release of NetBackup 7.5, Replication Director will support file level cataloging and restores with NFS and CIFS based NetApp storage.

Storage Lifecycle Policies are used to provide an intuitive interface that controls the entire data lifecycle.

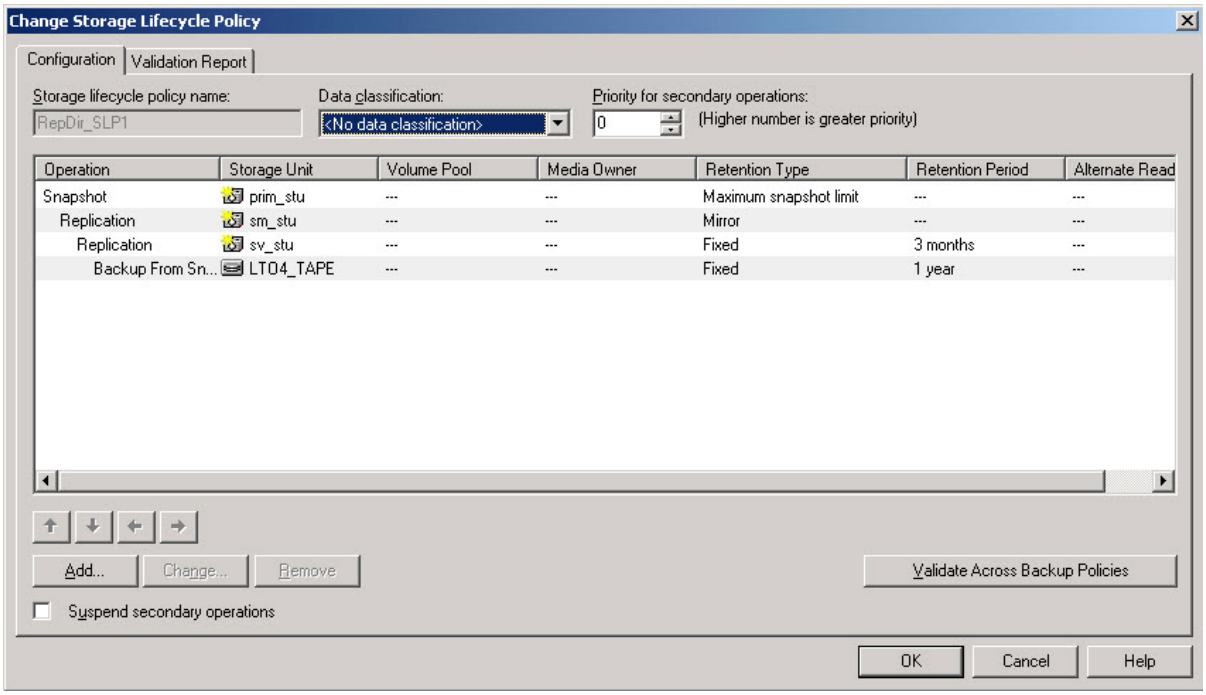

Figure 1. Storage Lifecyle Policy Interface

Figure 1 shows a snapshot that is replicated to SnapMirror and SnapVault before being backed up to disk storage.

Restoring files from NetApp snapshots is completely integrated into NetBackup using the new OpsCenter Operational Restore interface shown in Figure 2.

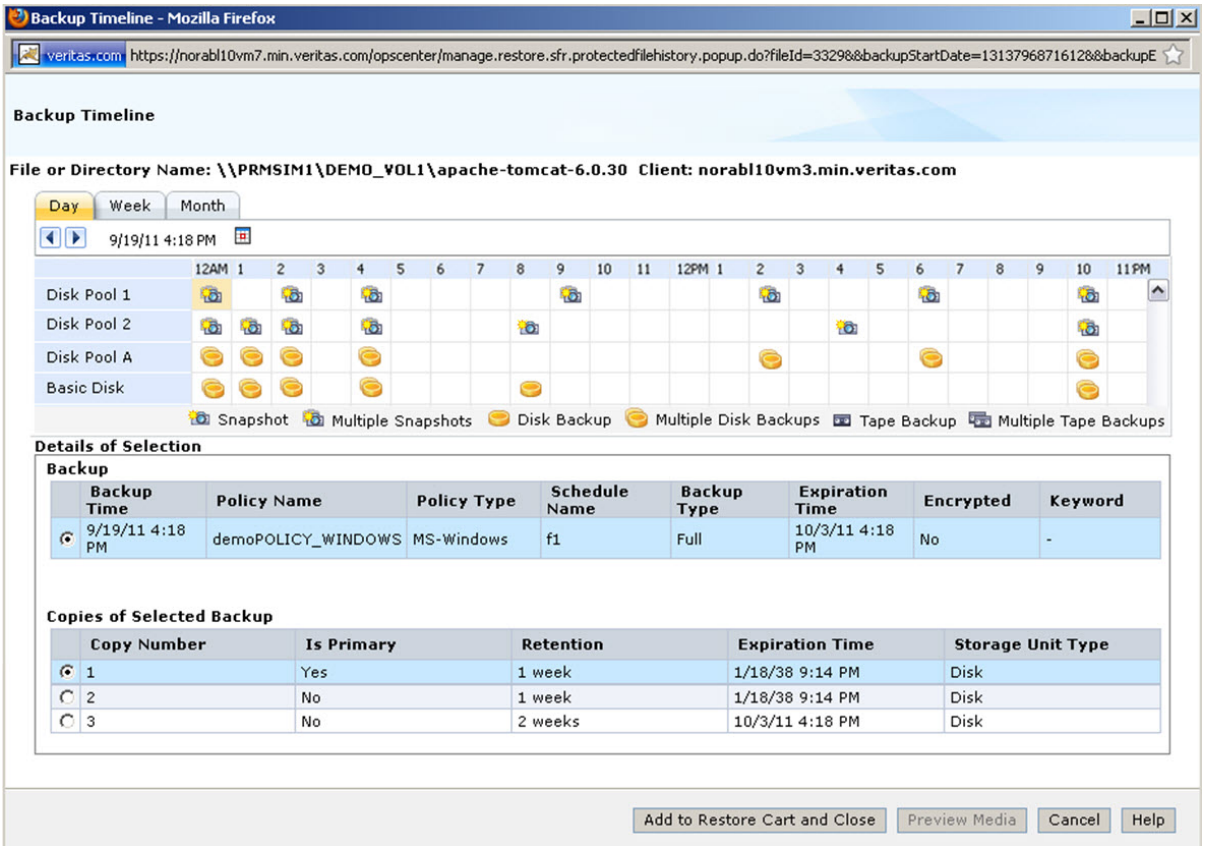

Figure 2. OpsCenter Operational Restore Interface

NetBackup Accelerator

Feature description

NetBackup Accelerator facilitates intelligent, streamlined backups to disk by increasing the speed of full backups. The increase in speed is made possible by change detection techniques on the client. The client uses the change detection techniques and the client's current file system to identify changes that occurred since the last backup. The client sends the changed data to the media server in a more efficient backup stream. The media server combines the changed data with the rest of the client's data that is stored in previous backups to create a new full backup image without needing to transfer all the client data. In other words, NetBackup Accelerator provides a full backup, but at the cost and speed of an incremental backup.

NetBackup Accelerator addresses the issues of increasing data volumes requiring protection and shrinking windows available to backup those data volumes. It provides a unique solution to the problem by identifying reading and transferring only changed files or blocks. NetBackup Accelerator significantly reduces the amount of resource (time, network, and storage) that a full backup requires. Using NetBackup Accelerator, a very large file system can be fully backed up in the amount of time previously taken by an incremental backup.

NetBackup Accelerator supports the following storage unit types:

- NetBackup appliances, Media Server Deduplication Option (MSDP), and PureDisk plug-in

- Cloud storage plug-ins
- OpenStorage Technology (OST) devices that have qualified support for NetBackup Accelerator

Please refer to the NetBackup 7.x Hardware Compatibility List for information about which OST devices are supported with NetBackup Accelerator.

Business value

Using NetBackup Accelerator benefits customers by providing:

- Significantly faster backups
- Reduced CPU overhead on the client
- Reduced utilization of network resources
- Reduced utilization of storage resources
- Faster recovery (restores) from a single source rather than multiple backups

These benefits combine to deliver lower OpEx and CapEx.

Typical use cases for NetBackup 7.5 Accelerator include:

- Backing up file systems where completing a full backup within the backup window is an issue
- Using NFS or CIFS (vs. remote NDMP) to backup NAS filers because only changed files are backed up for Accelerator full backups
- Improvement of remote office data protection by decreasing amount of backed up data to transfer over the network
- Improved cloud support by reducing amount of redundant data sent to cloud storage

Underlying principles

NetBackup Accelerator combines three mechanisms to reduce processing time and network traffic when creating a full backup image:

1. Change journaling/change logging is used to rapidly identify the files and blocks which have changed since the last backup.
2. The backup sends only those changed files or blocks to the backup storage device, minimizing the network traffic. Where available, client side deduplication can be used in combination with NetBackup Accelerator to further reduce the amount of data sent over the network.
3. Once the changed data is received by the backup storage an optimized synthetic full backup is automatically created.

In the 7.5 release NetBackup Accelerator delivers file system support for Microsoft Windows®, UNIX®, Linux® platforms as well as a complete framework that will be leveraged in future releases to deliver coverage for VMware and applications/databases.

NetBackup Accelerator uses track logs on the client and reconciles these to the current file system state to determine the changes since the last backup. In NetBackup 7.5 it can also utilize the Windows NTFS Change Journaling to track changes on NTFS file systems. Using change journaling further enhances the speed of the backup by reducing the time required to identify the changes to the file system.

NetBackup Accelerator should be regarded as a complimentary technology of client deduplication, not a replacement for it:

- When used together, client deduplication can further reduce the amount of data NetBackup Accelerator sends over the network to the media server during a full backup while NetBackup Accelerator also reduces the time required to determine what data needs to be sent.

- NetBackup Accelerator also reduced network chatter during a full backup with client deduplication as only the changed files need to be check for pre-existing segments rather than all files in the file system being backed up.
- The combination of NetBackup Accelerator and client deduplication gives a powerful advantage over other backup technologies in remote office data protection environments with low bandwidth networks.

Search and Hold

Feature description

NetBackup 7.5 introduces new functionality which allows an administrator to place backups on "Hold" to prevent them expiring on the due expiration date or being manually expired by an administrator. This is accomplished with a new binary that runs on a schedule which will "Index" the existing NetBackup catalog and store the information in a database on a specified media server. This database can then be "Searched" using OpsCenter. When the data is found, and a Hold is placed, the Search process modifies the NetBackup catalog and EMM database and puts a hook in the files to prevent the data from being expired until the Hold is removed.

In this release, file system backups can be indexed. This can include VMware backups using the VMware vStorage™ API's for Data Protection (VADP) and the new Replication Director backups. The indexing is based on file metadata only.

This new feature will benefit customers who may have legal litigation who need to retain data that has been protected by NetBackup.

The Index process is turned off by default and is configured in three places—at the Policy Attribute level, at the Schedule level and at the Client level.

Business value

For customers who experience legal issues that require them to save data for litigation, this new feature will prove invaluable. While currently limited in scope to simple "Search and Hold" functionality this new feature will provide the ability to quickly change the retention of data that has been previously backed up (legacy data) and to Index new data after it is backed up. In previous releases, searching for specific data and then changing the retention of that data can be very be very time consuming, and even then, difficult to determine if all the images associated with that data found. In addition, once the data is no longer needed, releasing it would be just as difficult.

By combining these features into an automated process and providing the Search/Hold capability within OpsCenter makes it very easy to accomplish this same process. Something that literally could take days or weeks and hundreds of "man-hours" now takes seconds.

While this functionality is mainly focused on customers who need to respond to legal inquiries, other users may find this feature useful for its search capability. It is not able or intended to change retention periods on the fly. This is primarily focused on "Hold" functionality for legal purposes.

Underlying principles

The NetBackup Catalog consists of a number of databases and flat files that work together to allow data on a tape or disk to be cross referenced in the event of a restore request. This new functionality will scan the catalog and create a database that can be searched based on settings in the Policy about what to Index. By creating a database the Search functionality performance is greatly improved.

Once the data is found, a Hold can be placed on the data which will change a flag on the backup image to mark it as held and from being expired. This Hold will also make it so that these images cannot be deleted or changed using the CLI. For example, an error will be displayed if

a command (bpexpdate) is run against a held image. This allows a legal team the ability to provide information to a NetBackup admin about what information needs to be kept from expiring during an investigation phase.

Once the data is Held, and the changes are made to the NetBackup catalog to prevent expiration, the data can then be manually restored and/or manually ingested into Symantec Enterprise Vault™.

Operational Restores with OpsCenter (ORO)

Feature description

While restores have been available through the BAR (Backup, Archive, and Restore) GUI, it only allows for Folder searching and can only search a single Client and single Master. It also requires the help of the Backup Administrator.

Operational Restores using OpsCenter (ORO) is functionality that allows other key stakeholders within the organization to recover their own files. These stakeholders may include the Help Desk, Application owners or the VM Administrator. This feature enables searching for files across any Master and/or Client that is configured with OpsCenter and includes wildcard searches, specific file type searches as well as filtering by a number of different methods. It also includes a "Restore Cart" that allows the restores to be placed in the cart for batch restores.

Operational Restore is also used with Replication Director to choose which copy of the data to recover.

Business value

The ability to quickly search for files across multiple Clients will save the backup/restore admin a great deal of time. Typically when a restore is needed the person requesting the restore may only know the name of the file they need, or a partial name. They may not know the Client it was on or the date/time it was backed up. The new functionality of Operational Restores will make it much easier for the backup admin to find the files even if limited information about them is available.

In addition to this functionality, the files can be searched based on filtering on a number of different levels (policy, schedule, etc.) to reduce the change of providing too many results. Basically the restore search can be as broad or as narrow as the situation dictates.

This functionality can be further enhanced using OpsCenter's View Based Access Control where access to a Client or Master can be granted to a specific user without them having to have access to all of the Masters or all of the Clients.

By spending less time on restores the backup admin will have time for other backup related duties.

Underlying principles

The concept for Operational Restores is very simple. When a restore is needed, the GUI walks the NetBackup Catalog. Additional hooks were put into the Catalog in NetBackup 7.5 to make this work, therefore only Masters at NetBackup 7.5 (either new installs or upgrades) will work with Operational Restores. The restore is the same as with the BAR GUI—the NetBackup catalog is consulted, the media that the image is on is found and the data is restored. If tapes are not in the library they may need to be procured before the restore can take place. There is a Preview Media button to determine if the Media is in the robot or not.

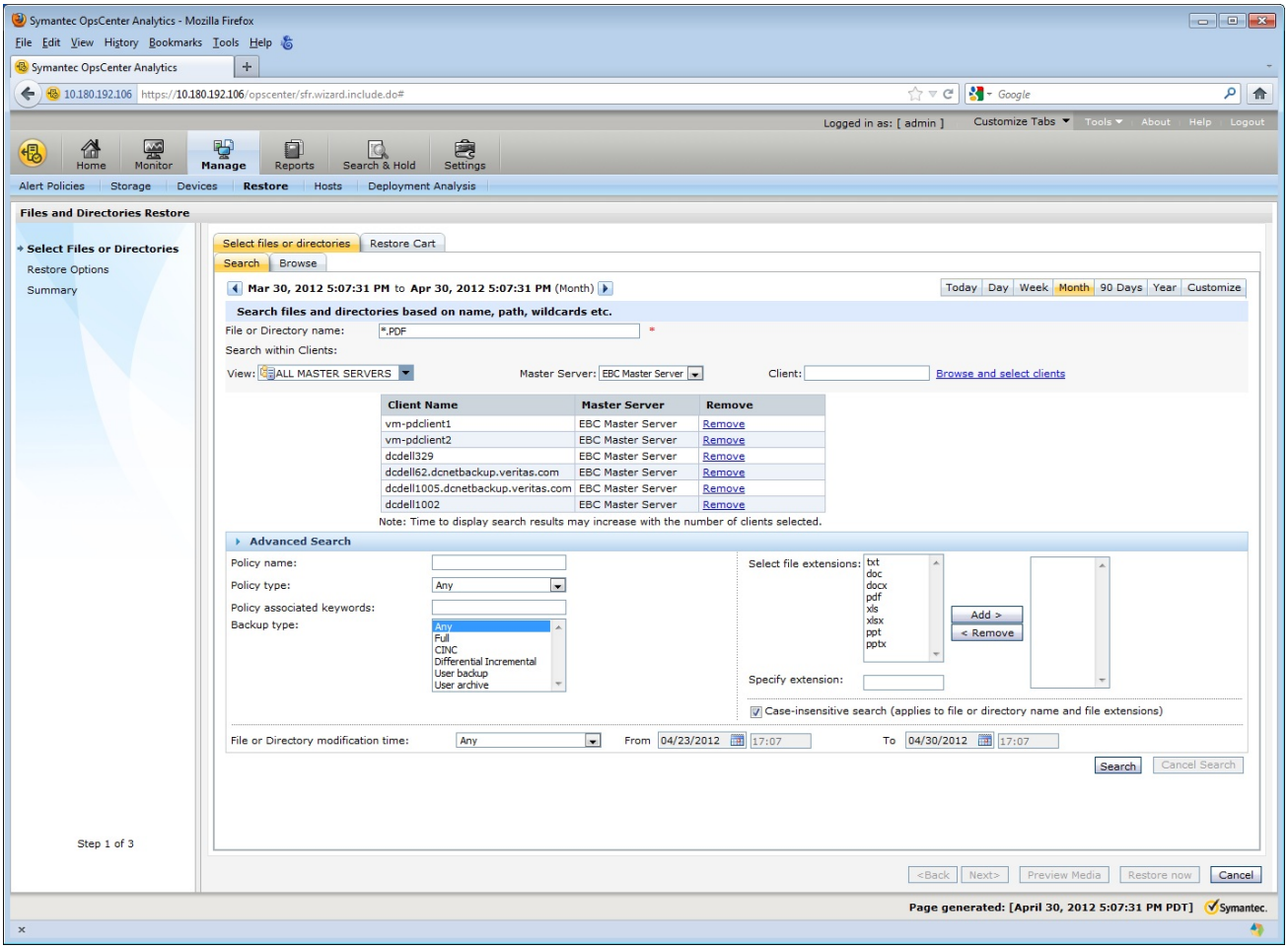

Figure 3. Advanced Search Dropdown

Once the data has been found, it is listed in a column format as seen in Figure 3. At this point, the files could be chosen for restore by selecting them on the left hand side and simply clicking “Restore Now,” however, this is only part of what this new tool can do.

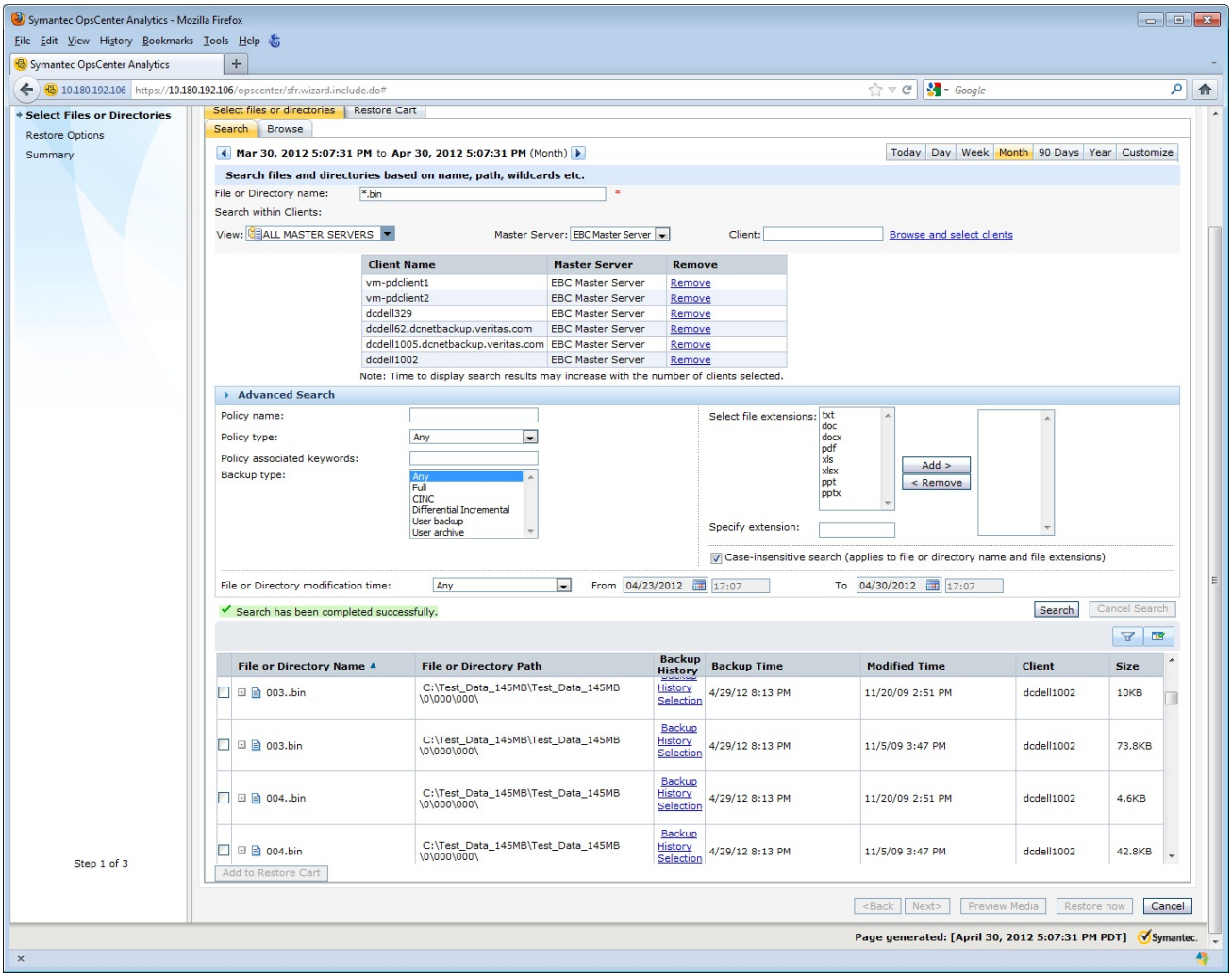

Figure 4. Output of the file search

To get more information about the files, and where the data is located, a Backup History link is provided. Clicking on it for the individual file will open a screen that indicates not only where the file resides (disk or tape) but also, in the case of Replication Director—which version of the file to restore (Figure 4).

Application Protection for VMware Virtual Machines

Feature description

The last few versions of NetBackup offered extensive features for protecting VMware virtual machines, as well as application agents for Microsoft® Exchange, SharePoint®, and SQL® Server databases. However, databases could only be protected by installing the NetBackup client on the VMware virtual machine running as a database server, and backing it up as if it were a physical machine.

This has changed in NetBackup 7.5. It is now possible to use the NetBackup award-winning VMware backup technology while retaining the ability to recover databases using database agents.[1] This includes restoring entire databases for disaster recovery purposes as well as

1-Symantec NetBackup 7 for VMware, Best of VMworld 2010.

individual database objects such as Exchange mail messages and SharePoint documents using the NetBackup patent-pending Granular Recovery Technology (GRT).

Business value

The new NetBackup VMware application backup features will result in considerable savings on time, training, and equipment costs:

- The ability to combine advanced VMware backups with application protection will result in dramatically faster backup of database servers, as well as making it unnecessary to perform two different types of backup for the same virtual machines.
- In many configurations data will flow over a SAN rather than a local area network, reducing network load, and contention, and the CPU load on virtual servers is substantially reduced.
- Less disk space is required on NetBackup storage units since there are no longer multiple backup images.
- Recovery is performed with the same database agent user interfaces that are currently used, eliminating the need to retrain operators and administrators, and data can be recovered to both virtual and physical machines.

Underlying principles

Basic architecture

The NetBackup Exchange, SharePoint, and SQL agents are capable of performing a backup by leveraging Microsoft's Volume Shadow Copy Service (VSS) to generate a snapshot of a database file, backing up the snapshot, and then releasing the snapshot. This capability has been modified and extended to allow the database agents to operate on an image generated by a NetBackup VMware vSphere™ backup. The result is the ability to recover data from a single backup image in as many as four different ways:

1. Full recovery of an entire virtual machine
2. File-level recovery of data in a virtual machine (V-Ray)
3. Recovery of an entire database using a database agent
4. Recovery of individual database objects using GRT

Application state capture

In order to accomplish this, NetBackup 7.5 introduces a new type of backup job—an Application State Capture (ASC). When a VMware policy that is enabled for application protection launches, NetBackup automatically executes an ASC job before any application data is actually transferred. The ASC job examines the virtual machine and determines whether all the prerequisites have been met, what type of database(s) are present, and any other metadata necessary to protect the application. If there are multiple databases running in the same VM (e.g., both Exchange and SQL Server), they will all be captured during a single ASC job if the policy is configured to do so.

Application State Capture runs immediately after the parent backup job is initiated and is clearly identified in the Activity Monitor. The ASC job runs quickly; when it finishes, the actual backup job will be initiated.

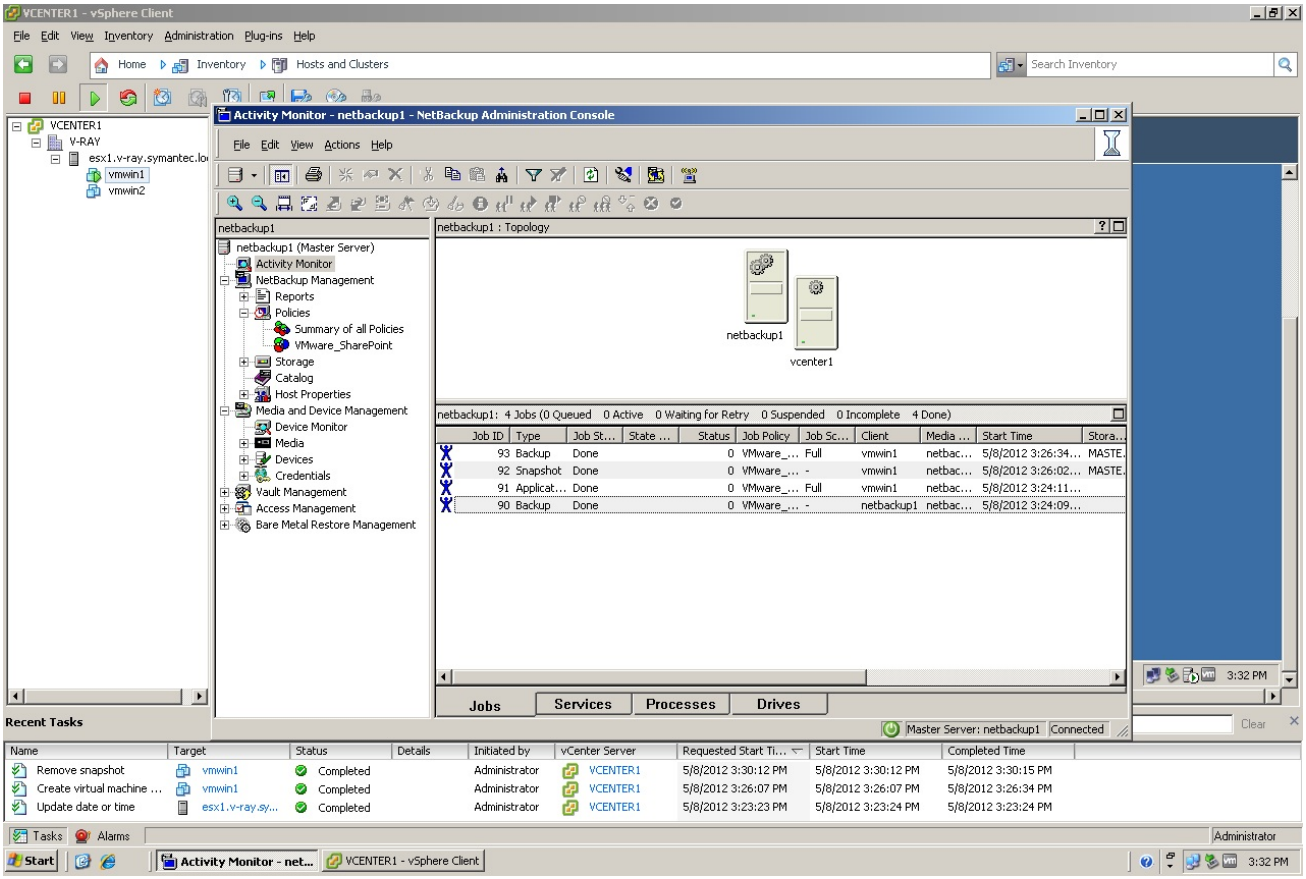

Figure 5. Application State Capture job in Activity Monitor

If an ASC job fails to detect a database or if a prerequisite is not met an error will be reported in the job log, but the parent job will not terminate. A conventional VMware snapshot and backup will be performed even if the applications residing within the VM cannot be protected using an agent, and the parent job will terminate with a Status 1. If there are no applications detected by the ASC job, the parent will terminate with Status 0.

All DB data must reside in VMware VMDK files. As with existing VMware backups, data on independent or raw device mapping (RDM) volumes will not be captured. The ASC job will detect this and skip any databases that have any component on an independent or RDM volume, and report it to the administrator in the job log.

VMware Policy Enhancements

Feature description

The design of the NetBackup policy has been refined and improved over many years of use. As backup technologies have evolved, minor changes to the NetBackup policy have been implemented as needed. This has worked very well for network based backups. Shared storage, SAN, and NDMP transfers have also been supported but these configurations are really just variations on client backups and typically require minimal changes to the NetBackup policy.

Virtual machine technologies have dramatically changed backup requirements. Standard backup agents are installed on and focus on protecting files that exist within a running operating system. Virtual machine backups can be configured this way as well. However, the

physical implementation of the virtual machine offers architectural differences that unlock compelling backup and restore options. Hypervisor vendors have recognized this and have created integration points or API's that provide backup software vendors access to advanced backup methods designed specifically for virtual machines.

NetBackup 7.5 introduces two new policy types that exploit these new capabilities. These new policies are designed explicitly for VMware and Hyper-V. These new policy types offer a clean, straightforward interface that is implemented for each hypervisor. They are easier to configure, easier to maintain, and display all available backup options in an intuitive manner.

Business value

With the NetBackup 7.5 release, the policy enhancements provide many business benefits including:

- **Easier to use VMware and Hyper-V policy types—**When a VMware or Hyper-V policy is selected a separate tab appears which provides access to features that are explicitly designed for each respective hypervisor technology.
- **Microsoft application support (Exchange, SQL Server, SharePoint)—**NetBackup for VMware now supports database backups. Object level restores and transaction log truncation are easily configured.
- **Virtual machine disk exclusion—**VMware backups can now be defined to exclude specific VMDK's from backup processing. Either the boot disk or all data disks can be excluded. In this way, data that is considered redundant can be skipped. This means faster backups with decreased backup storage requirements.
- **Media server load balancing—**For years NetBackup has featured the ability to load balance across and failover backups to different media servers. Now VMware backups support this powerful capability.
- **VMware vCenter™ backup event posting—**VMware administrators can now be instantly notified of backup success and failures. No longer do they need to contact the busy backup administrator to determine the protection status of their VMware environment.
- **VMware Intelligent Policy vSphere 5 enhancements—**vSphere 5 provides new logical definitions of storage related to the new Datastore Cluster classification. NetBackup 7.5 now supports these new logical definitions and can automatically select and load balance any new or relocated Datastores configured as part of a Datastore Cluster. This capability also works with the new VMware vSphere™ 5 Storage DRS capability.

Underlying principles

VMware and Hyper-V have taken different approaches with data protection. VMware provides the vStorage API's for Data Protection (VADP). VADP offers a number of advanced backup capabilities that are not available from any other hypervisor vendor. Hyper-V's backup support is very VSS-centric and does not provide some of the features offered by VMware. Because each of these vendors have taken a very different data protection approach, a separate policy type for each was mandated. This not only eliminates confusion when configuring backups but it also provides flexibility to support new features from each vendor as they become available.

The following considerations were applied when designing these new policy types:

Separate VMware and Hyper-V policy types—Both VMware and Hyper-V virtualization technologies share many similarities but they approach data protection from a different perspective. These different backup perspectives provide capabilities that are in many cases not shared between the two. Providing a different policy type for each hypervisor allows the policy to be defined exactly for the hypervisor to be protected. No more confusing menus as only the features available from the specified vendor are listed in the policy type. For backward compatibility the standard Flash backup-Windows policy type still works for VMware or Hyper-V when upgrading to the 7.5 release. It is not

necessary to immediately modify all existing virtualization policies once an upgrade to 7.5 has been completed. NetBackup 7.5 also features a utility that can be used to automatically update existing VMware policies to this new policy format.

Microsoft Application Protection (VMware)—This is one area where the NetBackup client is utilized in concert with the VADP. Installed inside the virtual machine, the NetBackup client provides backups that are database aware for supported applications. The client ensures that the database is properly quiesced at backup time. The client also collects database metadata so that object level restores are cataloged. Optionally the client truncates database logs. Installing the NetBackup client provides flexible and powerful restore options while ensuring consistent database backups. The actual amount of metadata sent to the NetBackup server is very small. Backups are still processed using the VMware VADP backup infrastructure.

Virtual machine disk exclusion (VMware)—In certain instances it can be desirable to exclude specific virtual machine disks (VMDK's) from backups. For example, if many virtual machines have been configured from a standard template, the OS disk across many VM's will be essentially the same. There might be little reason to protect every OS disk across multiple VM's. The virtual machine disk exclusion option can automatically exclude the OS disk (VMDK), thereby improving overall backup performance by eliminating this redundant disk from backup processing. NetBackup uses V-Ray technology to accurately determine exactly which is the OS disk (VMDK). In this way, even disks with non-standard drive letters can automatically be selected for exclusion. Disk exclusion works with any VMware VM that is supported with the V-Ray file level recovery technology.

Media server load balancing (VMware and Hyper-V)—For some time NetBackup has supported a media server load balancing capability. When media server load balancing is enabled, backup processing can be balanced across multiple media servers. Backup processing can also be routed around failed media servers. NetBackup for VMware was not able to provide this ability as the communication between the Windows media server and the VMware vCenter server could only be statically defined. With the NetBackup 7.5 release, any Windows media server defined in a media server group can now be used.

vCenter backup event posting (VMware)—The VADP provides the ability to write specific events to the vCenter console. NetBackup 7.5 takes advantage of this to write either every backup event or just error backup events to the vCenter system. The status of NetBackup virtual machine protection can easily be monitored from the vSphere client. Virtual machine administrators are now empowered with immediate backup status information.

VMware Intelligent Policy vSphere 5 enhancements (VMware)—VMware introduced a number of new storage related enhancements to vSphere 5. These include Storage Dynamic Resource Scheduling (DRS). Storage DRS is similar to VMotion based DRS. Where VMware vMotion™ DRS moves VM's across VMware ESX®/ESXi™ servers based on resource availability, Storage DRS moves VMDK files based on storage resource availability. Storage resource definitions that can trigger a storage DRS event include storage capacity (lack thereof) and I/O load. When a Storage DRS event is triggered, Datastores within a Datastore Cluster are destination candidates for VMDK movement.

The VMware Intelligent Policy fully supports the Datastore Cluster definition. With NetBackup 7.5, any VM's located within a Datastore Cluster can automatically be selected for backup regardless of their location within that cluster. NetBackup 7.5 also supports the Datastore Cluster definition during restores. If the VM resided within a Datastore Cluster at backup time, that Datastore Cluster is automatically selected and targeted for restore. Alternate Datastore Clusters can optionally be selected for restore as well.

This policy also supports additional vCenter definitions and resource limits. VMware vCenter Custom Attributes can now be used to select VM's for protection. Additional resource limit definitions (vSphere 5) allow further refinement of backup processing balancing.

Cloud Enhancements

Feature description

The first integration between NetBackup and a cloud storage provider (the Nirvanix® cloud plug-in) was introduced in NetBackup 7.1. This integration, based on the OpenStorage Technology (OST) API allows customers with Nirvanix accounts to configure Nirvanix cloud storage as a storage target for NetBackup and define storage units that send backup data to the cloud storage. NetBackup 7.5 introduces a number of enhancements to the cloud integration offering including the following:

Support for three additional cloud storage providers—Support has been extended to three new cloud providers; Amazon S3, Rackspace Cloud Files, and AT&T Synaptic Storage.

Wizard driven cloud storage configuration—A cloud storage configuration wizard simplifies the configuration process.

AES 256 bit cipher feedback mode encryption—The cloud plug-in leverages NetBackup's integrated key management system to provide key management for a 256 bit AES encryption module. Using this module encrypts the backup data before it is sent to the cloud storage ensuring the data is secure even in public cloud environments.

Bandwidth metering and throttling—Cloud utilization charges are based on both the data stored and the rate at which it is transferred to the cloud. Bandwidth metering allows the customer to monitor the rate at which data is being sent to the cloud. Associated bandwidth throttling allows the customer to limit the maximum bandwidth available for read and write operations and also to schedule periods during which data can and cannot be sent to the cloud storage.

Note: The cloud plug-in is not available for certain media server platforms. Please refer to the NetBackup 7.x Hardware Compatibility List for information about which platforms are supported with which cloud providers.

Business value

Cloud-based backup storage is an attractive proposition, particularly for SMB customers and remote sites of large enterprises, as it provides a way of storing backup data off site without the capital costs associated with a conventional backup infrastructure. The enhancements to cloud support in NetBackup 7.5 provide customers with a wider choice of cloud providers, more control over the way in which data is sent to the cloud and a simpler configuration process. For a quick and efficient way to back up to the cloud, NetBackup Accelerator can be leveraged.

Underlying principles

The Cloud Storage software stack is based on NetBackup's OST and uses interposing (layered) plug-ins to stack basic functions to create a complex storage component as shown in Figure 6 below. Note that the encryption plug-in is not engaged unless the encryption option is selected. The architecture is designed to allow other plug-ins to be added in future releases.

The cloud storage server wizard is selected from the main page of the administration GUI:

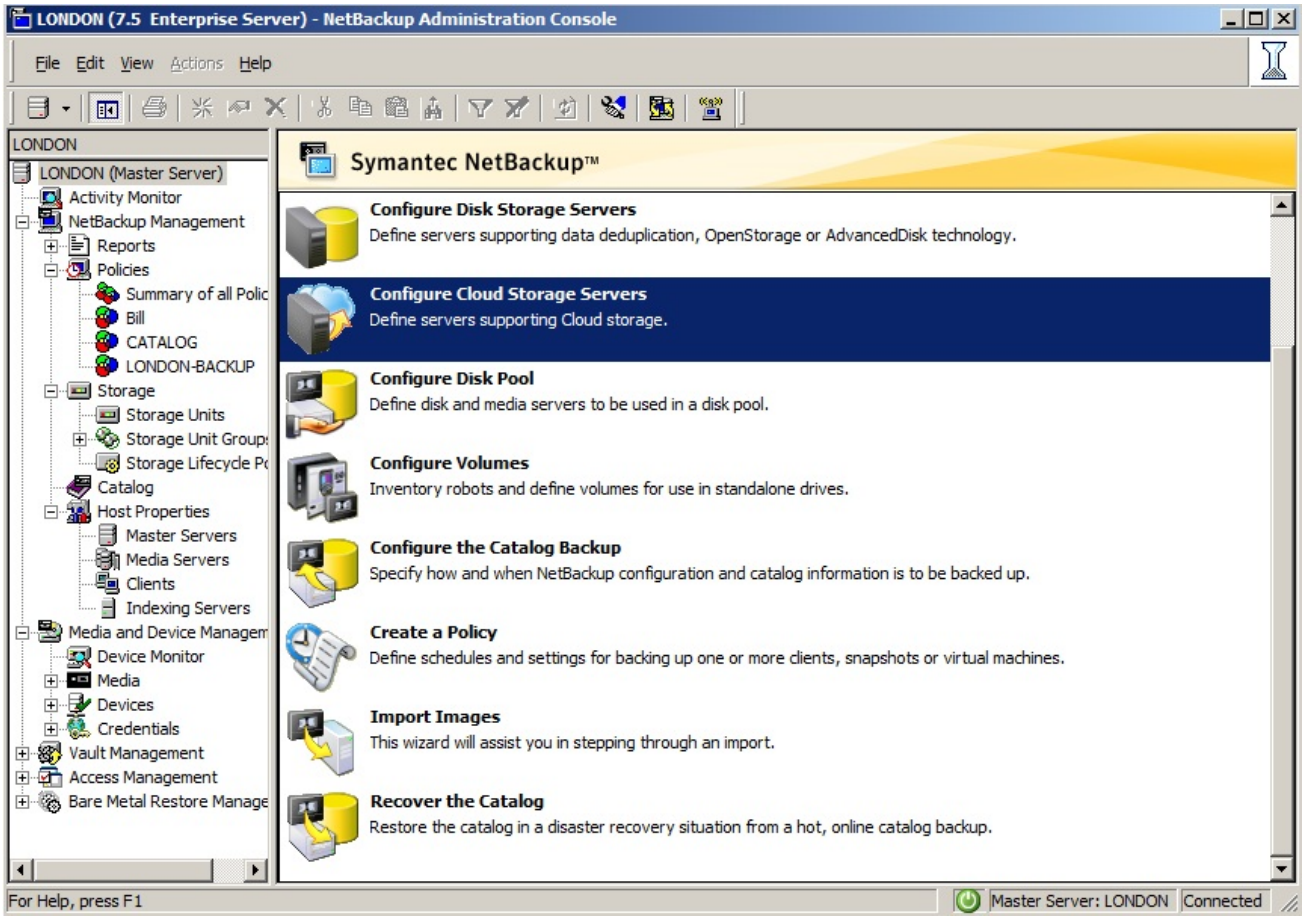

Figure 6. NetBackup Administration GUI

Summary

NetBackup 7.5 is the one backup and recovery solution that brings together multiple disparate solutions. Whether that is uniting NetApp snapshot and replication, physical and virtual, or the cloud. NetBackup 7.5 provides a variety of new features to help meet backup and recovery SLAs, reduce management overhead, and drive down storage costs.

For more information on NetBackup 7.5, please visit:

www.betterbackupforall.com

www.symantec.com/netbackup

www.netbackup.com

About Symantec

Symantec is a global leader in providing security, storage, and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored. Headquartered in Mountain View, 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 website.

Symantec World Headquarters
350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com

Symantec helps organizations secure and manage their information-driven world with **data backup and recovery software**.

8/2012 21264727