Feature Description – NetBackup Vault Extension

Vault Extension is an additional feature to NetBackup that automates selection and duplication of backup images and ejection of media for transfer to and from a separate, off-site storage facility. NetBackup Vault also generates reports to track the location and content of the media. Vault functionality does not have to be used only for disaster recovery – you can use Vault to manage the data and the media that you store off-site for regulatory archival purposes.

NetBackup Vault uses existing NetBackup functions for all operations, such as duplication of images, media control, reporting, and ejecting and injecting of tapes. Information from Vault is integrated with other NetBackup components and appears in the NetBackup Activity Monitor.

NetBackup Vault Extension should not be confused with Symantec Enterprise Vault which is Symantec's Enterprise level archiving product.

NetBackup Overview

The NetBackup Platform is a complete backup and recovery solution that is optimised for virtually any workload, whether physical, virtual, arrays, or big data, and delivers truly flexible target storage options, whether tape, 3rd party disk, appliances, including the NetBackup Deduplication Appliances and Integrated Backup Appliances, or cloud. Symantec NetBackup 7.6 with V-Ray Technology delivers the performance, automation, and manageability necessary to protect virtualised deployments at scale – where thousands of Virtual Machines and petabytes of data are the norm today, and where software-defined data centres and IT-as-a-service become the norm tomorrow. Enterprises trust Symantec.

Key Benefits
• Provides additional backup protection by duplicating backup images.
• Support of multiple media types for both backup and duplication media to provide for optimal cost-effective configurations.
• Provides batch duplication to maximise resource utilisation.
• Maintains file operating system level information and security.
• Utilises NetBackup three-tier architecture to create a scalable, distributed and heterogeneous design.
• Controls tape storage within tape silo versus tapes ejected from silo for transport to offsite vault.
• Automatic assignment of vault slot identifiers when required for use by vault vendor.
• Generation of various reports including media usage, pick lists and vault inventory.
• Usage of existing NetBackup capabilities for key features to ensure compatibility and robustness.

- *Comprehensive* – As a single solution to protect all of your data assets, NetBackup provides support for virtually every popular server, storage, hypervisor, database, and application platform used in the enterprise today.

- *Scalable* – High performance, elastic automation, and centralised management based on a flexible, multitier architecture enables NetBackup to adapt to the growing needs of a fast-paced, modern enterprise data centre.

- *Integrated* – From backup appliances to big data platforms, NetBackup integrates at every point in the technology stack to improve reliability and performance. OpenStorage Technology (OST) provides even tighter integration with third-party storage and snapshot solutions.

- *Innovative* – With hundreds of patents awarded in areas including backup, recovery, virtualisation, deduplication, and snapshot management, NetBackup continues a long tradition of bringing advanced technologies to market first.

- *Proven* – For over a decade, NetBackup has led the industry as the most popular enterprise data protection software by market share and is used by many of the largest enterprises on the planet. When you need your data back, you can trust NetBackup.

Key Features

- One platform, one console unifies virtual and physical global data protection
- Unified global management of snapshots, replicated snapshots, backup, and recovery
- Scalable, global deduplication across virtual and physical infrastructures
- V-Ray one pass backup, instant image and single file restore for virtual and physical
- Automated virtual data protection and load balanced backup performance

Key Benefits

- Unified, enterprise-class virtual and physical data protection eliminates point products, offers better visibility, leverages resources, and reduces cost, complexity, and risk when virtualising mission-critical applications

- V-Ray technology lets you search and recover a single file from an image backup in minutes instead of a manual mount, search, and restore that can take hours or even days

- Simplified management and faster recovery of snapshots and replicated snapshots from anywhere in the backup environment

- "Always on" protection of new, moved, or cloned VMs eliminates uncertainty and overloading of hosts during backups
- NetBackup intelligent deduplication reduces storage costs with deduplication rates as high as 98% while optimising backup performance and resources with flexible "end-to-end" deployment options

Business Value

Off-site data protection, or vaulting, is the strategy of sending critical data out of the main location (off the main site) as part of a disaster recovery plan. Data is usually transported off-site using removable storage tape in this instance. Sending backups off-site ensures systems and servers can be reloaded with the latest data in the event of a disaster, accidental error, or system crash. Sending backups off-site also ensures that there is a copy of pertinent data that isn't stored on-site.

If you are backing up even moderate amounts of data and shipping tapes off-site on a daily basis then keeping track of copies of backup tapes, where they are located, when the backup took place, for how long they need to be retained and when they need to be over written or deleted can be a messy job. Indeed, just the process of understanding tape rotation can be challenging.

So, most companies will be using some sort of off-site storage for tape. But different types of data often are retained for different lengths of time. For example, you may want to vault your finance data for seven years and your customer data for 20 years. To do this, the off-site copy of your backups will have different retentions based on the type of data. Vault can process different types of data individually if your backups are organised based on the type of data being protected.

So, one of your most important choices is whether to send original or duplicate images off site. Vault distinguishes between original images and duplicate images. NetBackup creates original images during a backup job, including all of the copies that are created concurrently by a backup policy. NetBackup can create up to four copies of an image concurrently during the backup process; all are considered originals.

Underlying Principles

Vaulting is the process of sending backup images off site to a protected storage location. There are a number of considerations you need to make, including a number of steps in the Vaulting process, these are:

- Choosing backup images
- Duplicating backup image
- Backing up the NetBackup catalog
- Ejecting media
- Generating reports

A Vault job must, at the very minimum, select images (Choose Backups). Other steps are optional per jobs so you can separate the Vault tasks into separate jobs if desired, in order to use different jobs to accomplish different tasks. For example, you can use one job to select and duplicate images daily, and another job to eject media and generate reports weekly. Although the process of injecting returned media back into the robot is a manual operation, the Vault reports include the media that should be recalled from the off-site location and injected into the robot.

Initially you need to choose the backup images that are candidates to be transferred off site. For every Vault job you must configure the image selection. Vault uses the criteria in a Vault profile to determine which backup images are candidates to send off site. (A Vault profile is a set of rules for selecting images, duplicating images, and ejecting media.)

If you create multiple original images concurrently during a backup job, Vault can send original images off site (depending on the profile rules). If you duplicate images, Vault uses the primary backup image as the source image for the duplication operation. However, Vault duplicates from a non-primary copy on disk, improving performance, if one exists.

The next step of the Vault process is to back up the images that are candidates to be transferred off site are duplicated. This is the image duplication step. Vault writes copies of the backup images on the media that you can eject and transfer off site.

If you send your only backup image off site or create multiple original backup images and send one or more of those images off site, you do not have to duplicate images in Vault and therefore do not have to configure the duplication step. However, you must write the original image to media in the off-site volume pool so it is ejected and transferred off site.

Following the duplication process you have the option to back up the NetBackup catalog. This would be advised as the NetBackup catalog consists of databases of information about the NetBackup configuration and any backups that have been performed. The information about backups includes records of the files and the media on which the files are stored, including information about media sent off-site. The catalogs also have information about the media and the storage devices that are under the control of Media Manager.

In the fourth step of the Vault process the media that you then transfer to secure storage is ejected, this can be at a separate facility. Vault reporting facilities can track the media that are ejected and are recalled from off-site storage for reuse after the images expire. Media can be ejected

automatically by a scheduled Vault job or manually after the job has completed. Media can be ejected for each job individually or can be consolidated into a single eject operation for multiple Vault jobs.

Finally reports can be generated; these reports track the media that Vault manages. You can use the reports to determine which media should be moved between your site and the off-site storage location and when this should happen. Reports can be generated individually or consolidated as part of the Vault job or manually after the job is finished.

Vault uses Volume groups to determine where a volume is located. Volumes in a robotic volume group reside in a robot. During a Vault job, Vault searches the robotic volume group for the media that matches a profile's criteria; if media are found, Vault ejects that media and then moves it logically to an off-site volume group. (A logical move means to change the volume attributes to show the new location.) When a volume in off-site storage expires and is injected back into the robot, Vault moves it back into the robotic volume group.

Volume pools identify logical sets of volumes by usage. Vault uses them to determine if a volume should be ejected. Volume pools for images to be transferred off site are known as off-site volume pools. When you create the images that you want to send off site, write them to media in an off-site volume pool. During a Vault job, Vault searches a robot for the images that match the selection criteria. If the media the images reside on are in an off-site volume pool, Vault ejects that media.

NetBackup Vault interacts with the following NetBackup services and catalogs:

- Media Manager, which manages robots and media
- The NetBackup catalog and the Media Manager database record of the images that have been vaulted
- The Media Manager database information which determines when expired media can be returned to the robot for reuse
- The Activity Monitor which displays the status of the Vault job
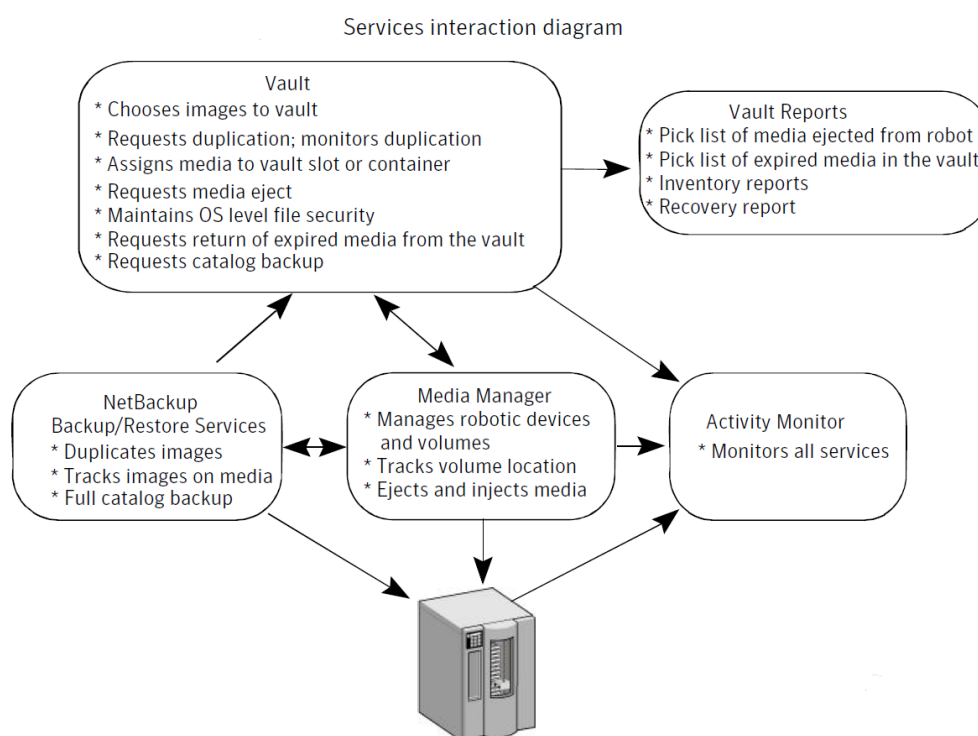

Figure 1 - NetBackup, Media Manager, and Vault relationships

Test Drive

Use the Choose Backups tab (shown in Figure 2) to configure the search for images to be vaulted. The most basic criterion you can set is the time frame. To refine the search for images to vault, you can select Attribute and Location to configure the advanced options. The default setting of these two criteria is for the check boxes to be unselected, which means all criteria in that particular field is included in the search for an image to vault. The criteria in the Attribute field are logical criteria to help you refine your search. The criteria in the Location field represent physical locations of the images to backup.

Vault compares images in the NetBackup database with the criteria defined in the Choose Backups tab and generates a list of images that match the criteria. The image selection process chooses all images in the NetBackup catalog that match the criteria that you select under Attribute and Location, even images that are in a different vault. The criteria that you specify on the other tabs in the Profile dialog box determine whether Vault includes or excludes the selected images.
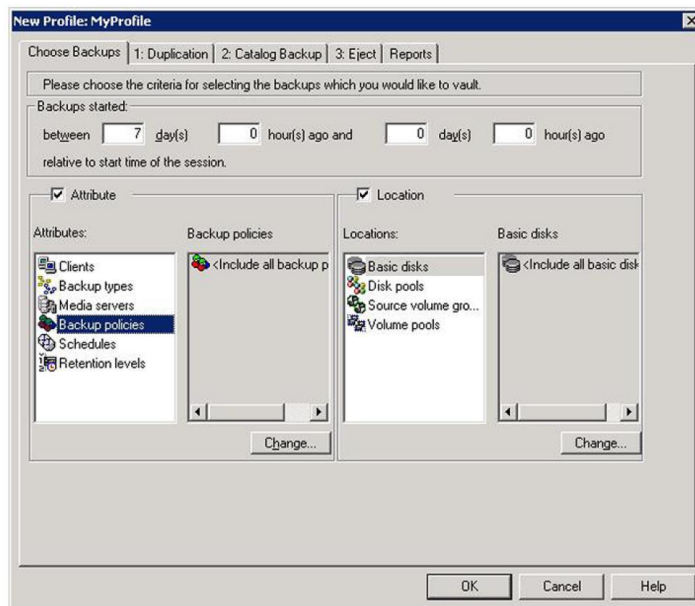

Figure 2 Backups tab on MyProfile

The Choose Backups tab enables you to quickly configure how you select criteria for your profile. For the broadest search coverage, you should leave the Attribute and Location check boxes empty and in their default state. This includes all criteria in your profile. Or, you can refine your search by using only criteria from the Attribute field, or search physical locations by using the criteria in the Location field. Finally, you can restrict your search to cover very specific areas by utilising various criteria in the Attribute and the Location fields.

The image selection process may select catalog backup images. However, if you are duplicating images, Vault does not duplicate existing catalog images. Vault ejects the media on which those images reside if that media is assigned to a volume pool that is listed in the Off-site Volume Pools list on the Eject tab.
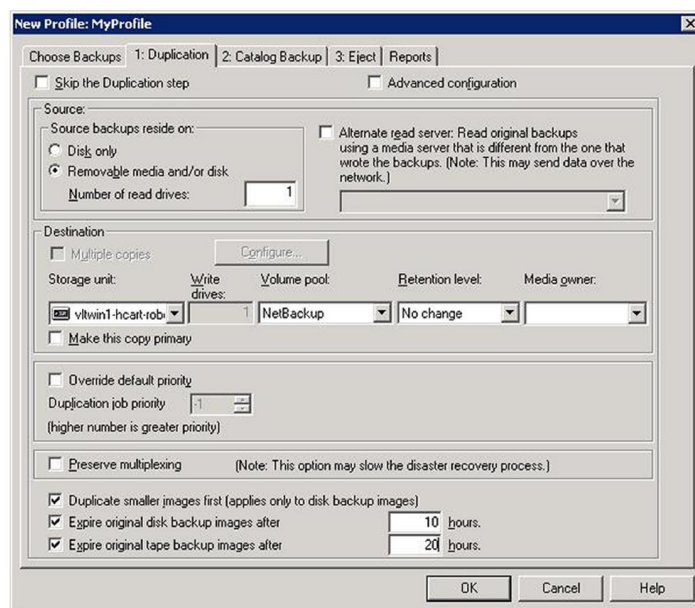

Figure 3 The Duplication tab of the Profile dialog box

Use the Duplication tab of the Profile dialog box to configure the rules that are used to duplicate images and to configure other duplication attributes. A duplication rule specifies the number of copies to create, a storage unit, off-site volume pool, retention period, media server (advanced configuration only), and what to do if an image copy fails (multiple copies only).
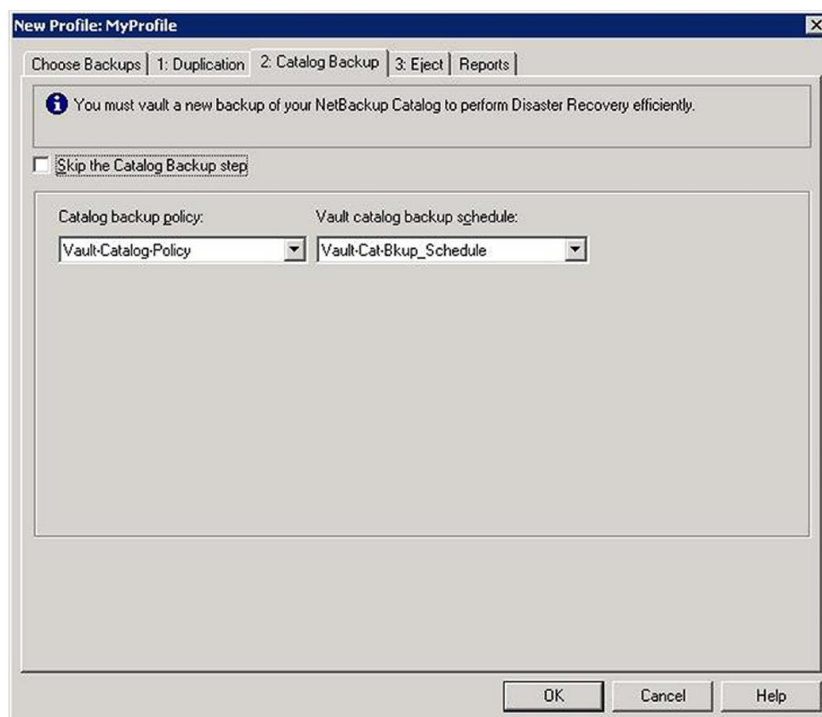

Figure 4 Profile dialog box Catalog Backup tab

Use the Profile dialog box Catalog Backup tab to specify the catalog backup policy and schedule that performs the Vault catalog backup. At least one NBU-Catalog policy that includes a Vault Catalog Backup schedule must exist so you can specify them on the Catalog Backup tab.

Vault uses the online, hot catalog backup method, which can back up the catalogs even when other NetBackup or Vault activity is occurring. (NetBackup provides two types of catalog backup; the other type is an offline, cold catalog backup that cannot occur when regular backup activity is occurring.) You must add the Vault catalog backup volume pool to the eject list on the Eject tab.

Licensing and Support Considerations

NetBackup Vault is installed on a NetBackup master server and requires a separate key. Once the license key has been added, either during the initial installation of Vault Extension or by using the **Help > License Keys** option of the NetBackup Administration Console, the option to perform vault management is then unlocked in the NetBackup Administration Console. There is not a separate GUI for controlling Vault Extension. You simply use the NetBackup Administration Console to configure and manage Vault.

Alternatively, you can manage Vault by using the following methods:

- Menu-based user interfaces
- Command line utilities

To license NetBackup Vault on a UNIX or Linux system, the NetBackup master server must be installed and running on the UNIX or Linux computer. In addition, you must have a valid NetBackup Vault license key. Make sure a valid license key for NetBackup Vault is registered on the master server. If you add the NetBackup Vault key after the NetBackup master server installation is complete, you must start the NetBackup Vault daemon. Then start the NetBackup-Java Administration Console and configure Vault.

When preparing to license NetBackup Vault on a Windows system, the NetBackup master server must be installed and running on the Windows computer. Vault runs on the NetBackup Master and cannot be installed on a NetBackup media server or on a NetBackup client.

Summary

NetBackup Vault Extension provides both backup duplication and offsite storage and retrieval of media. The system duplicates backup images onto tape or other media and simplifies restoring the duplicated files when the original backup image media is damaged or unavailable. NetBackup Vault Extension takes advantage of the NetBackup master-slave implementation that extends storage to other machines by centrally controlling duplication for multiple backup servers simultaneously. The system also ejects the duplicated media from any robotic storage units, assigns offsite

vault slot numbers and requests these tapes to be returned from the offsite location after a specified period of time, e.g. when the backup is no longer needed.

For More Information

Link	Description
http://www.netbackup.com/	NetBackup Home Page
http://www.symantec.com/docs/TECH59978	NetBackup Compatibility Information
http://www.symantec.com/docs/DOC6488	NetBackup Documentation
http://www.symantec.com/support	Symantec Support Portal
http://www.symantec.com/connect/backup-and-recovery	Symantec Connect Forum
http://techcenter.symantec.com/ecampus/enterprise?siteName=sena&courseNo=AT0900	Free E-Learning Library