An Oracle White Paper
June 2009

Oracle Secure Backup 10.3 – New Features

Table of Contents

Enterprise Data Protection

The amount of data in small and enterprise environments has and is continuing to grow exponentially from one year to the next. The complexity of managing large and growing amounts of production data can be daunting. Securing and protecting that data in rapidly changing, 24x7 environments can be challenging requiring the right combination of software, hardware and short/long-term planning.

An overall data protection strategy begins with the determination of backup and recovery requirements. Based on those requirements, backup storage policies for onsite and offsite requirements should be defined. Finally, management and operational considerations turn a data protection strategy in a plan such as:

- Accessibility of backup data to meet Recovery Time Objectives (RTO)
- Management of tape vaulting between multiple locations
- Security of backup data regardless of storage location

This paper discusses how the Oracle Secure Backup 10.3 new features can be leveraged to address these enterprise data protection requirements.

Oracle Secure Backup (OSB) – Overview

Oracle Secure Backup is a centralized tape backup management solution providing high-performance, heterogeneous data protection in distributed UNIX, Linux, Windows and Network Attached Storage (NAS) environments. Protecting file system and Oracle database data, Oracle Secure Backup provides a complete tape backup solution for enterprise environments, with the following capabilities:

- Oracle Database backup to tape through integration with Recovery Manager (RMAN) supporting versions Oracle9*i* to Oracle Database 11g.
    - Optimized tape backup for the Oracle database, backing up only currently used blocks and eliminating backup of committed undo – both of which help increase backup performance by 25 – 40% over comparable products.
- Heterogeneous file system support in distributed environments to locally or remote (over network) attached tape devices.
- NAS data protection leveraging the Network Data Management Protocol (NDMP)
- Policy-based backup management:
    - Backup encryption and key management
    - Tape vaulting: Automated management of tape rotation between multiple locations
    - Tape duplication: Automated duplication per policy or on demand with same or different retention and rotation schedule as that of the original tape(s)
- Broad tape device support for new and legacy devices
    - Dynamic drive sharing provides increased tape drive utilization in Storage Area Network (SAN) environments

With a highly scalable client / server architecture, Oracle Secure Backup provides local and remote data protection leveraging Secure Socket Layer (SSL) technology for secure intra-domain communication and two-way server authentication.

New Features in OSB 10.3

Building upon the management foundation of previous releases, Oracle Secure Backup 10.3 delivers increased manageability and device utilization addressing data protection complexities in very large environments. A brief list of OSB 10.3 enhancements follows with more detailed descriptions discussed in the remainder of this paper.

- Manageability
    - Enhanced tape vaulting automation, scheduling and location reporting
    - Improved reporting of backup and volume metadata
    - Enhanced flexibility for system administrative domain management
    - Improved web browser interface
- Security
    - Expanded Backup Encryption Options
        - Native or hardware (LTO-4) encryption options with seamless encryption key management between the two
- Device Management
    - Server-less tape duplication
    - Verification checks for accurate device configuration
- Infrastructure
    - IPv6 Support
    - Improved catalog indexing and maintenance performance

Manageability

Data protection plans layout the backup infrastructure defining backup/restore requirements including retention, onsite/offsite storage, and backup redundancy. A plan is just a plan until it is implemented and optimized for ongoing operational management.

Oracle Secure Backup provides policy-based media and backup management for standardization across the backup domain. Defining OSB policies or performing daily operational tasks is easily accomplished utilizing the OSB web tool, command line interface (obtool) or Oracle Enterprise Manager.

Tapes are managed through their lifecycle from first write to finally reuse by defining one or more Oracle Secure Backup media management components:

- Media families – Foundation for tape management, establishes retention methodology
- Storage locations – Defines "passive" locations where tapes will reside through the media lifecycle such as an onsite media cabinet or an offsite location such as an alternate data center or Iron Mountain etc.

    - Active storage locations (tape devices) are automatically defined for each configured tape device

- Rotation Policy(s) – Defines the ordered tape locations and when the tapes should move from one to next location
- Duplication policy(s) – Defines when tapes should be duplicated, how many duplicates should be made and the media family to be used for duplicate tapes (same or alternate media family as original set of tapes)
- Vaulting and volume duplication scan schedules – Defines when OSB generates tape movement or duplication jobs per respective policies

A rotation and/or duplication policy may be associated with one or more media families. A media family may be associated with only one rotation and/or duplication policy however a rotation and duplication policy may be associated with multiple media families.

Tape Vaulting

In Oracle Secure Backup 10.3, vaulting has been enhanced providing additional flexibility, automation and tracking of tapes between locations. Specific Oracle Secure Backup 10.3 vaulting enhancements are listed below with more in-depth discussion to follow:

- Vaulting scan schedules may now be configured at the media family level in addition to location or domain level
- Media movement jobs created by vaulting scans may now be automatically run without user intervention to explicitly "run" the job
- Enhanced location status indicating when tapes are in transit between locations
- Ability to "Vault Now" which evokes a vaulting scan and corresponding media movement job
- Enhanced utilization of library ejection capabilities
- Improved exception handling for tapes providing ability to update location, mark the tape(s) missing or remove the tape from the OSB catalog (physical lost tape)
- Increased flexibility allowing a user to update the tape location without generation of a corresponding media movement job
- Ability to preview tape location prior to performing a file system restore operation
    - This new file system restore functionality is similar in concept to the existing RMAN **restore database preview** and **restore database preview recall** commands available with Oracle Database 10*g*R2 and OSB 10.2 forward

Vaulting Scan Schedules: Filtering by Media Family(s)

Vaulting scan schedule options have been expanded to include media family selections. This additional flexibility allows system administrators the ability to schedule volume rotation at the tape pool (media family) level. For example, an IT organization may want to vault tapes from media family "A" on Monday, Wednesday, Friday at 9:00am and tapes from media family "B" on Tuesdays and Thursdays at 1:00pm. Media family selections are easily configured as follows:

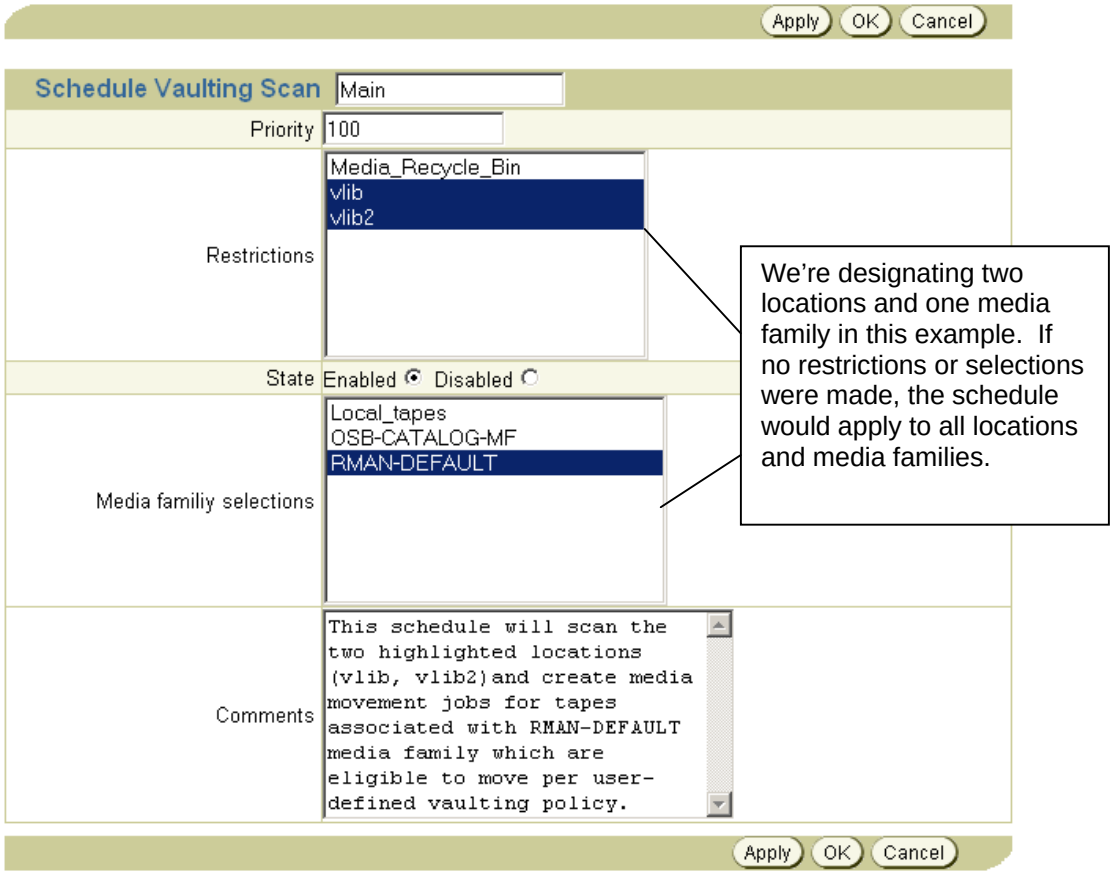

Figure 1: Defining a vaulting scan schedule using the OSB web tool.

Click the "Triggers" button to define when the vaulting scan schedule should run; one or more times daily, weekly or monthly.

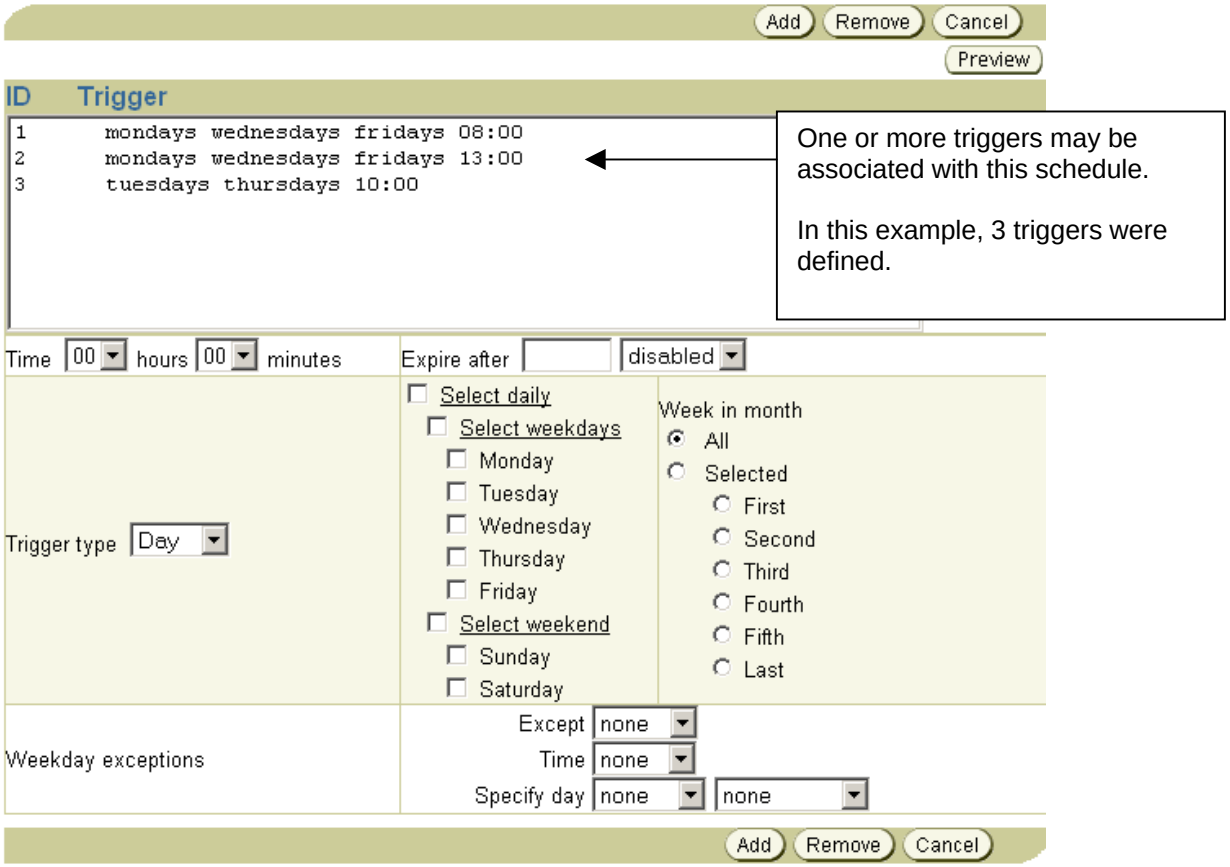

Figure 2: Creating a trigger for an OSB schedule.

Backup and duplication schedules often run at non-peak times. A vaulting scan schedule may run in peak or non-peak times taking into account the physical aspect of removing tapes from the library to be vaulted. When run, vaulting scan schedules automatically generate media movement jobs with associated pick and distribution reports. Per user policy, media movement jobs may run immediately or be placed into pending status until explicitly run by the user. Your media movement policy should be considered when determining vaulting scan schedule triggers: As for example, if your media movement policy is such that:

- Media movement jobs are set to run automatically (new in OSB 10.3):
    - Schedule vaulting triggers during times when personnel are available to remove tapes from the library

- Media movement jobs are placed into pending status until run by user (default):
    - Vaulting triggers may be scheduled at any time of day or night
        - Explicitly run media movement jobs during times when personnel are available to remove tapes from library

In Oracle Secure Backup 10.3, you may configure media movement jobs to run automatically by changing "Auto run media movement jobs" setting to "yes" as shown in the screen shot below or through obtool with the autorunmmjobs policy command:

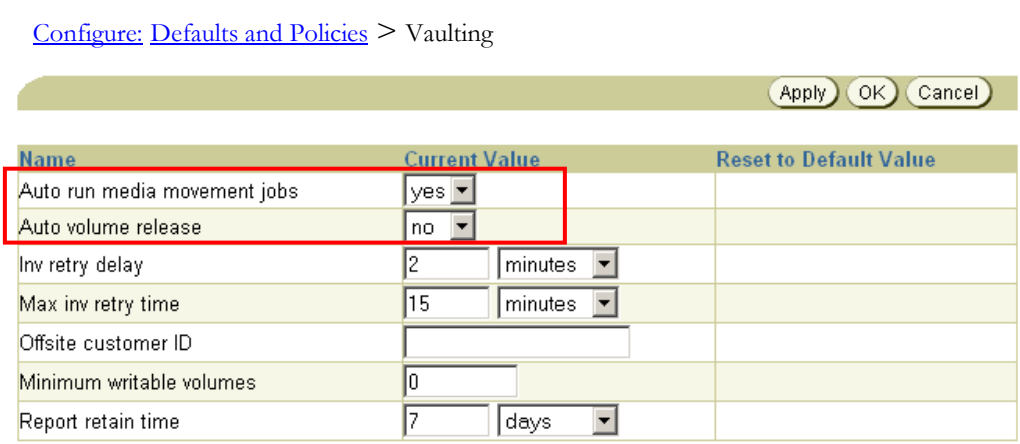

Figure 3: Domain-wide vaulting policy settings.

Vault Now

In addition to regularly scheduled vaulting scans, you may choose the "Vault Now" capability, which performs a vaulting scan and creates the corresponding media movement job. This new enhancement is very useful for adhoc vaulting needs. A vault now operation doesn't disrupt or replace defined vaulting scan schedules but instead adds a one-time scan to identify tapes eligible for movement per rotation policy.

Configuring a "Vault Now" operation is very similar to a vaulting scan schedule except it occur s immediately (or at configured time) versus on a repeating basis as defined using schedule triggers. The screenshot below shows how to schedule a "Vault Now" operation:

Manage: Vault Now

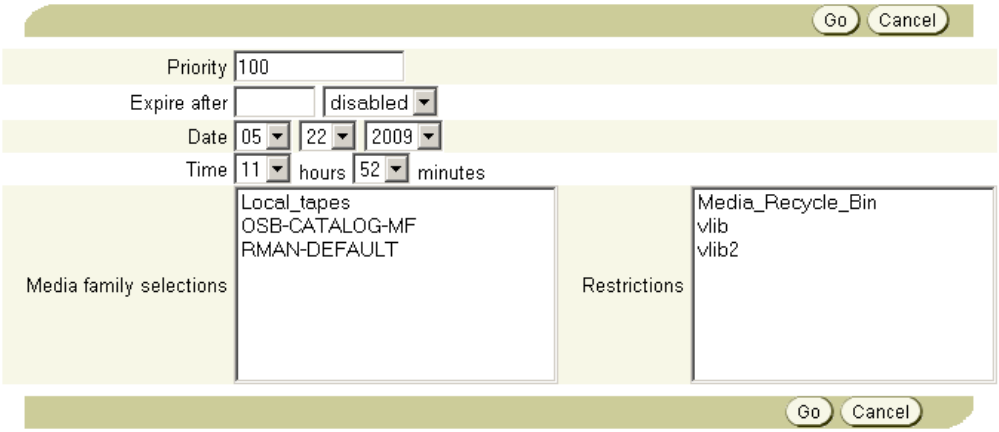

Figure 4: Vault Now screenshot from the OSB web tool.

In the above example, we have not selected any specific media families or limited the operation to select locations, so this "Vault Now" operation would be applicable to the entire domain regardless of media family. The current date and time is displayed by default, which would run the job immediately. The vaulting job may be performed at a scheduled time in the future by changing the date and time of the "Vault Now" operation.

Volume "in transit" Location Status

When media movement jobs are run in OSB 10.2, the tapes' location is updated with the next scheduled location without taking into account time transfer time between locations. In Oracle Secure Backup 10.3, the location for tapes moved will be reported as "in transit" until the location is updated by the user or tape library inventory operation. For the first tape movement from an active location (tape device), the location will automatically report the next destination but subsequent tape moves will indicate an "in transit" location.

The tape's "in transit" location may be updated in one of two ways:

1) Insert the tape into a tape library. Once the library is inventoried, the tape's location is automatically updated from "*in transit*" to the library's name.

2) Update the tape's location to "*not in transit"* using the web tool or obtool. This will update the tapes location within OSB to the scheduled location per rotation policy.

Improved Web Browser Interface

The OSB web tool has been enhanced supporting new features as well as streamlining volume and job management activities. The volumes and jobs management pages now display significantly *more* information and increased filtering options than that of previous releases.

From the volumes management web page, users can view all volumes or filter by location(s), media family(s) or volume attributes by selecting desired "view options":

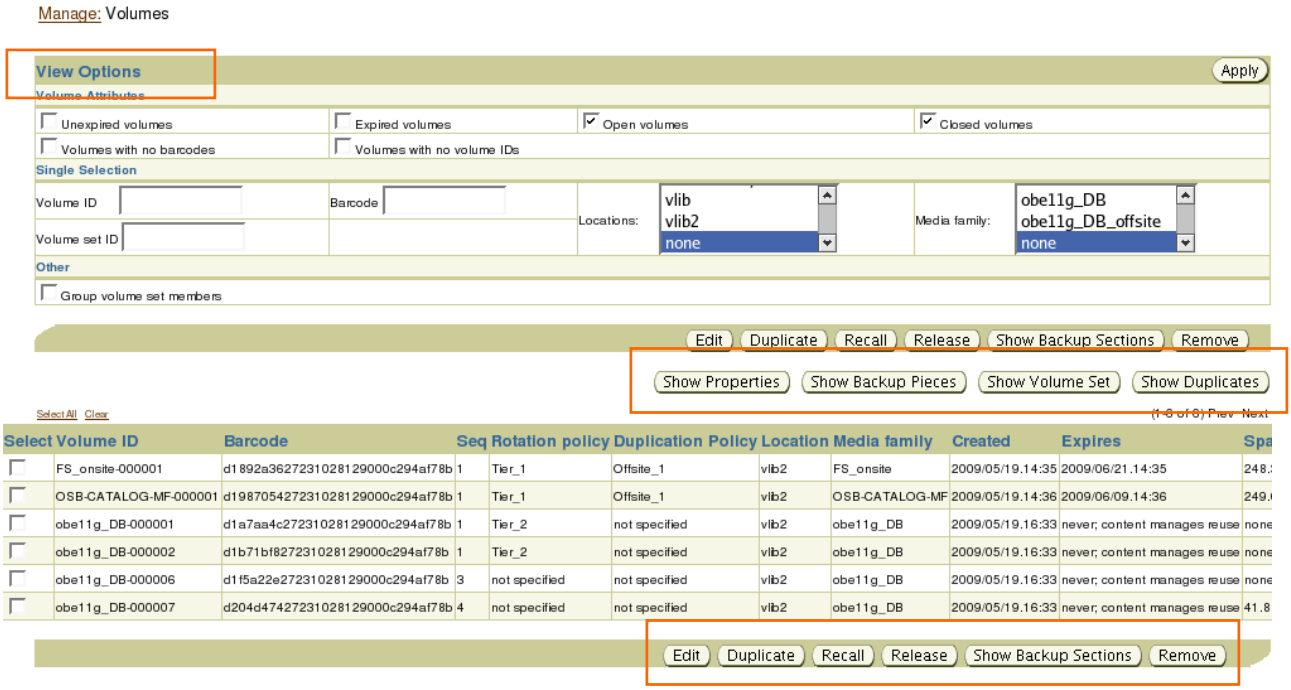

Figure 5: OSB web tool volumes management page.

Based on the view options, the corresponding volumes are then displayed. Obtain volume contents, properties or associated volumes (i.e. duplicates) by selecting volume(s) and then a "Show …" button. Volumes may be managed individually or as part of a group by selecting one or multiple volumes then choosing the desired operation such as edit, duplicate, recall or release.

Increased Information Reported: Backups and Volumes

The metadata output for backups and volumes has been expanded in OSB 10.3 providing more information, which may be useful for administrative management:

- The "*list host backup*" web tool page (included with restore pages) and lsbu obtool command now displays volume location for the associated backup.

- Backup section listings now include the section size.
- A volume or range of volumes may be queried to list backup sections or Oracle RMAN backup pieces contained on the volume(s) as depicted below:

Database Backup Pieces	
Backup piece OID	101
Database	orcl
Database ID	1158305843
Content	full
Copy number	0
Created	2009/05/19.16:33
Host	obe11g
Piece name	02kfe8tm_1_1
Encryption	off
Backup piece OID	103
Database	orcl
Database ID	1158305843
Content	full
Copy number	0
Created	2009/05/19.16:38
Host	obe11g
Piece name	04kfe96s_1_1
Encryption	off

Figure 6: Listing of backup pieces for a selected volume.

Increased Flexibility for System Administration Tasks

Oracle Secure Backup 10.3 provides several enhancements for increased flexibility and control of typical operational needs such as:

- Extend tape expiration date
- Enable or disable user-configured schedules
- Define name to display in the "from" line for OSB generated emails
- Inventory the full library or subset based on a user-specified range of storage elements

Security

The inherent portability of tape media addresses key backup, long-term storage and disaster recovery requirements. Securing backup data on tape when onsite, offsite and even lost requires backup encryption.

Oracle Secure Backup 10.3, provides both host-based and hardware backup encryption options. Backup encryption capabilities have been expanded from existing host-based encryption to support of hardware (LTO-4) encryption. Encryption key generation and management are identical whether host-based or LTO-4 tape drive encryption is utilized.

Backup encryption performed on the LTO-4 tape drive provides benefits such as:

- Eliminates overhead on the server associated with the encryption process.
- Encrypts NAS backups, which is not possible with OSB host-based encryption.

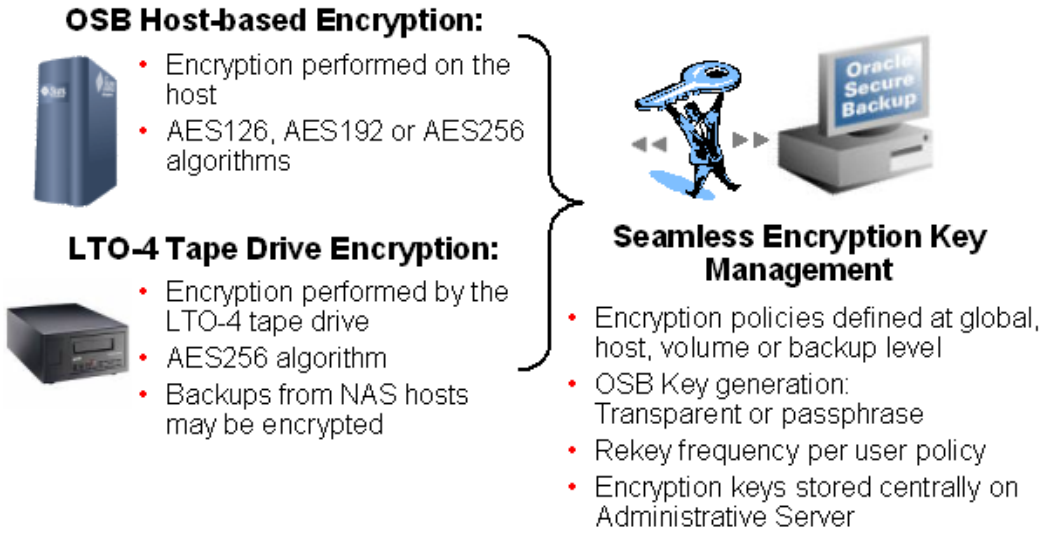

Figure 7: Host-based and hardware encryption options.

Oracle Secure Backup delivers policy-based backup encryption with backup encryption keys securely stored on the Administrative Server. Encryption keys may be generated transparently (randomly) or using a passphrase and regularly updated based on user-defined key regeneration schedule(s).

Device Management

Oracle Secure Backup qualifies new tape devices and connectivity on an ongoing with updates listed on the OSB tape device matrix available on OTN.

Server-less Tape Duplication

In addition to traditional tape duplication, Oracle Secure Backup 10.3 provides server-less tape duplication increasing performance and reducing overhead on the media server during the duplication process. This advanced duplication functionality leverages the hardware to perform copy operations between virtual and physical tapes eliminating the transport of data through the media server.

Many VTL devices have hardware duplication capabilities for performing tape copy outside of media management software avoiding transport through a server. This type of out-of-band duplication gets the job done but is counterproductive to centralized tape management strategies,

as the backup software has no knowledge of the duplicated tapes. Server-less duplication provides the best of both worlds; hardware leveraged for the duplication process itself based on OSB directives with metadata regarding the duplicates maintained within OSB's catalog.

With traditional tape duplication, the backup data to be duplicated is transported from the tape device through the media server then back out to the tape device. With server-less duplication, only OSB control messages and metadata regarding the duplication process are transported through the media server. The following diagram graphically shows duplication data transport:

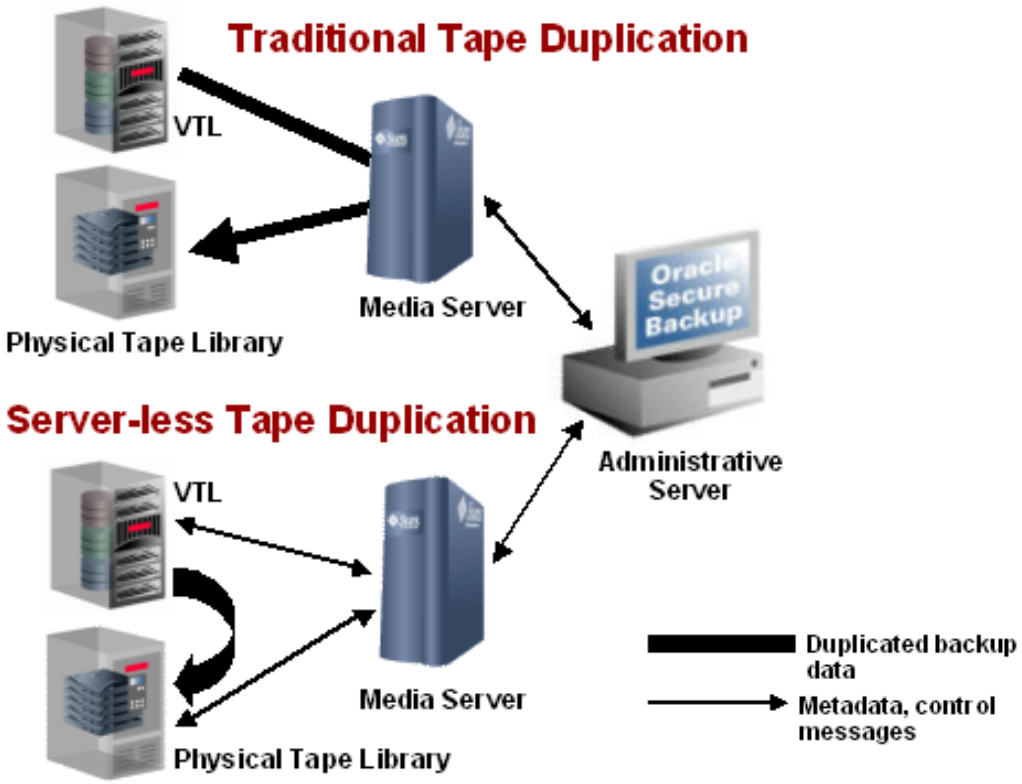

Figure 8: Traditional and Server-less Tape Duplication.

The physical tape drives used for server-less duplication from virtual to physical tape may be shared drives (as in Storage Area Networks - SAN) or dedicated to the VTL for duplication.

NOTE: The Virtual Tape Library must support NDMP Direct Copy, which enables server-less tape duplication. For a list of qualified devices supporting NDMP Direct Copy, please refer to the OSB Tape Support Matrix.

Improved Verification of Accurate Device Configuration

In Oracle Secure Backup 10.3, two new device configuration directives are available through obtool:

1) Verification Utility, `vfylibs`, scans environments reporting device configuration issues
2) Device serial number policy, `checkserialnumbers`, proactively identifies drive changes

The new device verification utility, `vfylibs`, verifies that the OSB configuration matches that of how the device represents itself via SCSI inquiries. By issuing the `vfylibs` command (via obtool), OSB sends SCSI inquires requesting device specific information to all configured tape libraries and drives. The resulting information is then compared with user-defined configuration settings within OSB reporting the following configuration errors:

- Tape drive wasn't configured or is not in service for a given library and Data Transfer Element (DTE)
- Attach point hasn't been configured for tape drive corresponding to a library and DTE within the domain
- Host associated with a configured attach point is not in service or could not be resolved (host not found).
- Device ID (constructed by OSB using SCSI Inquiry commands) associated with an attach point does not match the ID reported by the given library's DTE
    i. If mismatch occurs, OSB searches the ID of all drives to determine if the ID matches the DTE of a different library

Since the `vfylibs` utility identifies device configuration problems, best practice would be to run `vfylibs` after initial configuration and periodically as new devices are added or when troubleshooting potential device configuration issues.

When the device policy `checkserialnumbers` is enabled (default), Oracle Secure Backup flags potential configuration issues that may occur after device changes, such as when a tape drive is replaced or recabled. Upon first use of a tape drive, OSB obtains and stores its serial number. With each subsequent use, the original serial number obtained is checked against the current serial number being reported by the drive.

If a mismatch occurs, OSB provides an error message and takes the drive out of service. This ongoing device checking is important to uncover potentially problematic mis-configurations. For example, a typical library maintenance operation could have resulted in two drives being mis-cabled: drive A was accidentally cabled to the location configured/associated with drive B. In this scenario, OSB would attempt to communicate with drive A (library DTE 1) when in fact the drive now associated with that attach point is actually DTE 2. This situation can cause an immediate backup/restore failure or intermittent problems, which are difficult to diagnose root cause.

In the event a tape drive is broken or replaced, the new drive will have a different serial number than that of the original configured drive. You would update the serial number within OSB to avoid a mismatch upon first use of the new/replaced tape drive by using the `chdev <device name> --updateserialnumber` command.

Infrastructure

Oracle Secure Backup 10.3 supports Internet Protocol version 6 (IPv6), the next-generation Internet Layer protocol for packet-switched network communication. Expanding IP support from version 4 (IPv4) to IPv6, Oracle Secure Backup delivers a comprehensive infrastructure seamlessly communicating with hardware using IPv4 or IPv6.

Catalog Index Performance Enhancements

A single backup operation may contain millions of directories, sub-directories and files for which the corresponding backup metadata is indexed within the Oracle Secure Backup catalog. Indexing performance has been significantly improved in Oracle Secure Backup 10.3 resulting in faster metadata importing for the backup operations. The indexing performance for a typical backup now achieves an average of 50,000+ files per second for UNIX, Linux, and Windows backups.

For backup of Network Attached Storage (NAS) appliances, Oracle Secure Backup utilizes NDMP, which requires a post-processing step to transform NDMP metadata into an appropriate format for indexing within the Oracle Secure Backup catalog. The NDMP post-processing has been further streamlined in Oracle Secure Backup 10.3 resulting in significantly improved indexing performance particularly advantageous for backups containing millions of small files.

Improved Catalog Maintenance Performance

The Oracle Secure Backup catalog is automatically "pruned" of obsolete metadata based on the index policy, `indexcleanupfrequency`, which by default occurs every 21 days. The catalog cleanup operation removes backup metadata associated with backups, which are no longer available on tape along with volume metadata associated with overwritten tapes. In Oracle Secure Backup 10.3, catalog "cleanup" has been enhanced to minimize overhead

associated with pruning of the catalog, substantially increasing performance for catalog maintenance operations.

Summary

Oracle Secure Backup 10.3 is centralized tape backup management software delivering enterprise class data protection for your entire IT environment. Data protection management for distributed servers, NAS devices and tape devices is streamlined with the OSB administrative server, central management console. With an enterprise feature set, Oracle Secure Backup easily scales from the smallest to largest IT environments.

Building upon a reliable infrastructure, Oracle Secure Backup 10.3 delivers enhanced manageability, new features and integration with the latest technologies:

- Increased tape vaulting automation and management
- Improved flexibility and control for common operational day-to-day tasks
- Enhanced reporting of in-process backups and volume locations
- Hardware and native backup encryption options
- Server-less or traditional tape duplication capabilities
- Device configuration accuracy checks
- Support of networking technologies: IPv6 and IPv4
- Improved performance for catalog indexing and clean-up operations

Oracle Secure Backup delivers data protection for the enterprise for over 75% less cost than comparable products. Unprecedented in the recent backup industry, OSB offers low-cost, single-component (tape drive) licensing making affordable, reliable data protection within reach of both small and large IT organizations. With Oracle Secure Backup, you can reduce IT costs without sacrificing functionality.

White Paper Title
June 2009
Author: Donna Cooksey
Contributing Authors:

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

Worldwide Inquiries:
Phone: +1.650.506.7000
Fax: +1.650.506.7200
oracle.com

Oracle is committed to developing practices and products that help protect the environment

0109