

An Oracle White Paper
November 2011

Oracle Secure Backup 10.4 – High-Performance Tape Backup for Oracle Environments

Table of Contents

Tape Backup Management	1
Oracle Secure Backup	2
Centralized Tape Backup Management	2
Network Load Balancing	3
Most Optimized Backup and Recovery for Oracle	4
Oracle Secure Backup Management Interfaces	5
Policy-Based Management Infrastructure	6
Strict Security Controls for Backup Data and Domain.....	6
Backup Encryption and Key Management	7
User-level Access Control	8
Host Authentication and Secure Network Communications.....	8
Automated Media Lifecycle Management	9
Retention	9
Tape Duplication	11
Tape Vaulting	12
Using Media Lifecycle Policies	12
Managing Volumes	13
Oracle Database Backup and Restore.....	15
Oracle-Recommended Tape Backup for Oracle Exadata Database Machine .	17
File System Backup and Restore	18
Managing OSB Jobs	19
Broad Tape Device Support.....	20
Summary	21

Tape Backup Management

For decades, businesses have depended on tape for all or an integral part of their data protection infrastructure. Tape remains the lowest-cost per GB of storage, is inherently portable and ideally suited for long-term storage. Keeping pace with increasing amounts of data, tape technology has evolved with dramatic increases in capacity and data transfer rates. Withstanding the test of time, tape media remains the cornerstone of most enterprise backup and recovery architectures.

Backup tapes in active use or storage at any one company can number in the tens of thousands. Some tapes may be used for short-term storage, others for long-term. Data protection requirements may dictate that some or all backups be encrypted, tapes duplicated and/or tapes stored at various locations throughout its retention period. Most importantly, backup tapes must be readily available for restoration when needed.

This paper discusses how Oracle Secure Backup 10.4 delivers comprehensive tape backup management for the enterprise.

Oracle Secure Backup

Oracle Secure Backup (OSB) delivers unified data protection for heterogeneous environments with a common management interface across the spectrum of servers. Protecting both Oracle databases and unstructured data, Oracle Secure Backup provides centralized tape backup management for your entire IT environment:

- Oracle database via built-in integration with Recovery Manager (RMAN) supporting Oracle Database 11g, Oracle Database 10g and Oracle9i
- File system data protection: UNIX / Windows / Linux servers
- Network Attached Storage (NAS) data protection leveraging the Network Data Management Protocol (NDMP)

The Oracle Secure Backup environment may be managed using command line, OSB web tool and/or Oracle Enterprise Manager (EM).

Centralized Tape Backup Management

Oracle Secure Backup offers centralized backup management of distributed servers, NAS devices and tape devices through a single point of administration called the OSB Administrative Server. The configured hosts and tape devices managed by an Administrative Server comprise an OSB domain. With a highly scalable client/server architecture, Oracle Secure Backup domains may consist of one to hundreds of hosts (servers and/or NAS devices).

All hosts within the backup domain will have one or more Oracle Secure Backup roles:

- **Administrative Server** houses the backup catalog, configuration data and is the certificate authority for server authentication.
- **Media Server(s)** transfer data to and from direct or Storage Area Network (SAN) attached tape devices.
- **Client(s)** are hosts which are backed up. All hosts within the domain will be assigned the client role during installation along with additional role(s) as defined by the user: media server and/or Administrative Server. A backup domain will include only one Administrative Server.

Oracle Secure Backup communicates directly with the host to backup mounted file systems or storage. An Oracle database may be located on any host regardless of the host's configured Oracle Secure Backup role. Figure 1 below shows an example of an OSB domain:

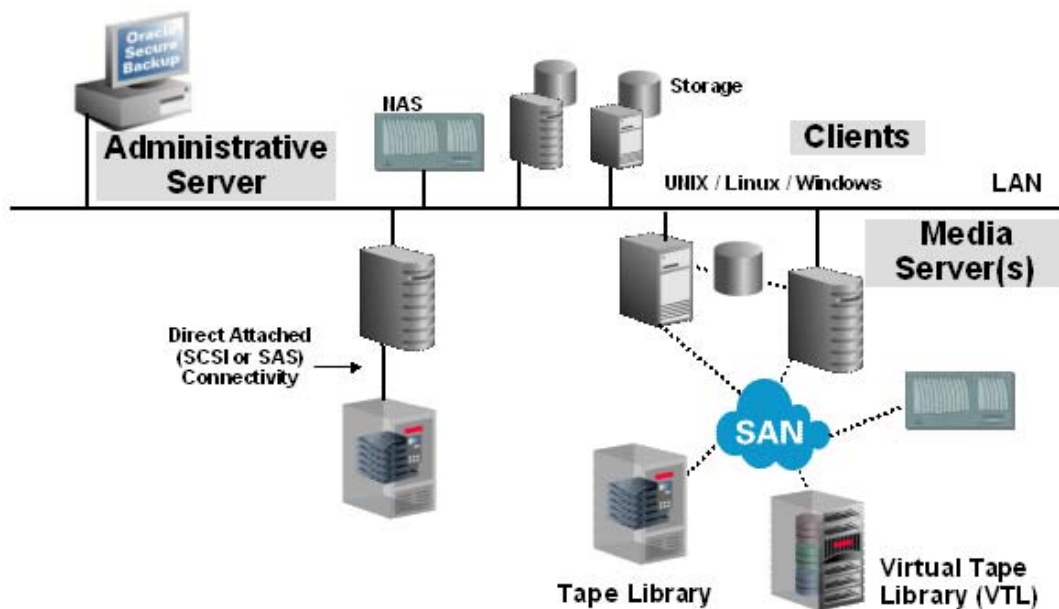


Figure 1: Example of an Oracle Secure Backup domain.

As depicted in Figure 1, the OSB Administrative Server may be a single purpose host but that's not a requirement. Any host within the domain (except NAS devices) may act as the Administrative Server. In practice, it's very common to co-locate the RMAN catalog and Enterprise Manager repository on the OSB Administrative Server.

Network Load Balancing

Today's servers commonly have multiple network interfaces to increase throughput and connectivity for a range of network types such as Infiniband (IB), 10 GB and/or 1 GB Ethernet. If a server has two IB ports, do you want backup/restore traffic only using one? No, you would want to distribute the workload over available networks.

Oracle Secure Backup 10.4 balances the load across like network interfaces thereby increasing performance and avoiding over / under use of any one interface. If a host contains more than one network interface of a particular type, OSB uses all the available interfaces of that type for the data connections between the client host and the media server host. The type of network interface will be selected by OSB in priority order of RDS / RDMA (Reliable Datagram Socket over Remote Direct Memory Access) over Infiniband, IPv6 and then IPv4.

The connection type must be supported on both the client and the media server for it to be selected by OSB. If RDS / RDMA over Infiniband isn't supported on both hosts, Oracle Secure Backup will automatically use TCP/IP over Infiniband. If an OSB Preferred Network Interface (PNI) is configured, then load balancing on the media server will be disabled in favor of the user-defined PNI setting.

Most Optimized Backup and Recovery for Oracle

Oracle Secure Backup provides the most optimized tape backup for the Oracle database while reducing the complexity and cost of secure, high performance backup and recovery.

Data protection for your entire Oracle environment is simplified when using an Oracle integrated solution – not to mention the advantages of having a single technical resource. When installing Oracle Secure Backup, the SBT (System Backup to Tape) library for RMAN tape backups is automatically linked. Using Oracle Enterprise Manager, you can manage the OSB backup domain from tape vaulting to backup / restore operations.

As part of the Oracle product family, OSB has built-in integration with the Oracle database achieving performance advantages resulting in 25 – 40% faster tape backup than comparable 3rd party products. Key performance and tape vaulting optimizations between OSB and RMAN are discussed in the *Oracle Database Backup and Restore* section of this paper.

Oracle Exadata Database Machine, Oracle Database Appliance and Oracle SuperCluster are engineered to deliver extreme performance. These systems may be connected via Ethernet or Infiniband to media servers for tape backup. The best backup/restore performance can be achieved using Infiniband connectivity and is the most common deployment strategy.

Oracle Secure Backup 10.3, along with most other media manager products, transports data over Infiniband (IB) using TCP/IP. While TCP/IP over IB works, the performance is as much as 50% faster when using RDS / RDMA over IB! So, Oracle Secure Backup 10.4 supports RDS / RDMA over IB for the fastest Oracle database backup to tape in these environments. This OSB optimization is discussed further in the *Oracle-Recommended Tape Backup for Oracle Exadata Database Machine* section of this paper.

Oracle Secure Backup delivers comprehensive tape backup management with enterprise-class features and Oracle database integration in one, complete solution. Comparable products separately license advance features; OSB does not. Advanced capabilities are inclusive in the Oracle Secure Backup low-cost, per tape drive license simplifying license management without compromising functionality.

Oracle Secure Backup provides a low-cost alternative for reliable data protection further increasing return on your Oracle investment (ROI).

Oracle Secure Backup Management Interfaces

If your preference is command line, the entire backup domain may be managed through obtool, OSB command line interface, and RMAN for Oracle database protection. If your preference is a Graphical User Interface (GUI), the OSB web tool and Oracle EM provide a comprehensive management infrastructure.

Oracle Secure Backup is the only media management software integrated with EM Database and Grid Control as shown in Figure 2. Beginning with EM Database Control 11.2.0.1 and EM Grid Control 10.2.0.5, the OSB domain, file system backup/restore operations and of course the Oracle database may all be managed using EM. While the backup domain and file system backup /restore operations can be easily managed using the OSB web tool, EM provides some additional capabilities such as:

- Monitoring / alerting
- Remote host browsing allows easy selection of file system directories or files to select for backup operations
 - EM agent must be installed on the host to utilize remote host browsing

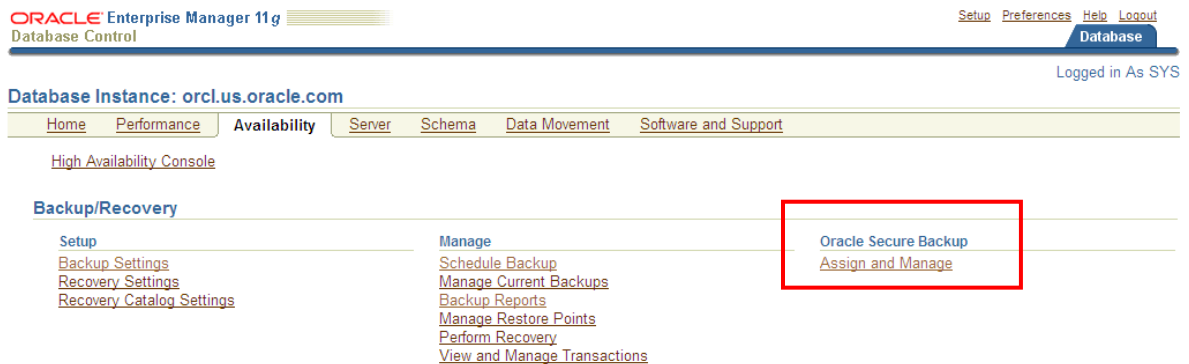


Figure 2: Availability tab in Enterprise Manager 11g Release 2 Database Control.

Through unified command line or GUI, the Oracle Secure Backup domain may be intuitively managed and customized to meet your specific requirements. Screenshots from the OSB web tool and EM are dispersed throughout this paper.

Policy-Based Management Infrastructure

Oracle Secure Backup includes a set of pre-configured defaults and policies defining operational behavior within the OSB backup domain from amount of time OSB logs should be maintained to minimum password length required for OSB users. You may leave the existing default settings or modify as appropriate for your specific requirements.

Policy	Description
backup encryption	policies for backup encryption operations
daemons	daemon and service control policies
devices	device management policies
duplication	duplication-related policies
index	index catalog generation and management policies
logs	log and history management policies
media	general media management policies
naming	WINS host name resolution server identification
ndmp	
operations	
scheduler	
security	
testing	
vaulting	

Name	Current Value
Login token duration	15 minutes
Web inactivity timeout	15 minutes
Establish SSL communications	<input checked="" type="radio"/> Yes <input type="radio"/> No
Transmit X.509 certificates	<input checked="" type="radio"/> Yes <input type="radio"/> No
Encrypt backup data before transmission	<input type="radio"/> Yes <input checked="" type="radio"/> No
Public and private key sizes (in bits)	<input type="radio"/> 512 <input type="radio"/> 768 <input checked="" type="radio"/> 1024 <input type="radio"/> 2048 <input type="radio"/> 3072 <input type="radio"/> 4096
Trusted hosts	<input checked="" type="radio"/> Yes <input type="radio"/> No
Minimum user password length	0

Figure 3: OSB web tool screenshot of the "Defaults and Policies" page.

In addition to the “Defaults and Policies” infrastructure, Oracle Secure Backup provides policy-based management for backup operations, media lifecycle management and backup encryption to tape each of which is discussed in more detail within this paper.

Strict Security Controls for Backup Data and Domain

Data is the life-blood of business and must be guarded against malicious intent while in active state on production servers or preserved state on tape. Data center security procedures are key in restricting physical access to servers, data, and company networks. As data is preserved onto tape, Oracle Secure Backup works in parallel providing strict security controls for protecting backup data and guarding access to the backup domain.

Unfortunately in today’s world, no software can claim complete protection against malicious intent. However, Oracle Secure Backup offers multiple security options when combined with security-based operational policies provides maximum security for the backup infrastructure. Oracle Secure Backup security controls can be categorized into three areas:

- Backup Encryption and Key Management
- User-Level Access Control
- Host Authentication and Secure Network Communications

Securing backup data is of critical importance. Oracle Secure Backup meets this requirement head-on with strong, user-definable controls for guarding access to the backup domain and securing backup data on tape. Oracle’s commitment to delivering reliable, secure software is evident in Oracle Secure Backup.

Backup Encryption and Key Management

Oracle Secure Backup provides policy-based encryption key management for OSB native (host-based) and hardware (LTO-4, LTO-5, T10000B and T10000C tape drives) backup encryption. Oracle Secure Backup encryption policies provide a consistent infrastructure allowing users to exercise fine-grained control over encryption requirements and key management across the backup domain.

Encryption key management is identical whether host-based or tape drive backup encryption is utilized. You may define backup encryption policies on a global (domain level) or by host. Figure 4 shows host backup encryption options:

Encryption:	<input type="radio"/> required <input checked="" type="radio"/> allowed
Algorithm:	<input type="radio"/> aes128 <input checked="" type="radio"/> aes192 <input type="radio"/> aes256
Rekey frequency:	<input checked="" type="radio"/> duration <input type="text" value="1"/> <input type="text" value="month"/> <input type="button" value="v"/> <input type="radio"/> never <input type="radio"/> system default <input type="radio"/> per backup
Key type:	<input checked="" type="radio"/> transparent <input type="radio"/> use passphrase <input type="text"/> verify passphrase <input type="text"/>

Figure 4: OSB web tool screenshot of host encryption options.

If host encryption is set to “required”, then all OSB backups on the host whether file system or Oracle database will be encrypted. Conversely, encryption “allowed” means that backups from the host may be encrypted as configured at the backup level. The rekey frequency determines how often encryption keys for host backups should be changed. If the user-defined key type is

transparent (randomly generated keys), then the encryption keys will be updated automatically per rekey frequency schedule. With a passphrase key type, OSB will send an email to the administrator requesting a new passphrase be entered to meet the rekey policy.

Encryption keys are centrally stored on the OSB Administrative Server in host specific key stores. When restoration of encrypted backups occurs within the same OSB domain, Oracle Secure Backup will automatically decrypt the backup regardless of defined key type.

User-level Access Control

Oracle Secure Backup offers user-level access control based on configured OSB users, associated backup privileges (OSB classes) and operating system user privileges. During installation, the OSB admin user is automatically created with user-defined password and is assigned to the pre-defined OSB “admin” class which is analogous to a super user.

Additional OSB users may be configured by the admin user and assigned to one of six pre-defined classes or a new class may be created. While a user may be associated with only one OSB class, a class may be associated with multiple users.

The identifying user data and associated rights are cataloged and managed by Oracle Secure Backup. This provides a consistent user identity throughout the backup domain.

Host Authentication and Secure Network Communications

Secure communication between distributed hosts within the backup infrastructure is essential. Oracle Secure Backup has embedded Secure Socket Layer (SSL) technology to guard against unauthorized access to the backup domain as follows:

- Two-way server authentication between UNIX / Linux / Windows hosts
- Encryption as part of SSL transport for secure transmission of OSB control messages and/or backup and restore data

During installation, an X.509 host identity certificate is automatically created and stored in an embedded Oracle wallet, which is exclusively used for storing host identity certificates. As certificate authority, the OSB Administrative Server digitally signs all host certificates automatically during installation.

Before performing any backup and restore operations, server identity is two-way authenticated using the X.509 host certificates; commonly referred to as an SSL handshake. A host identity certificate is used for securing communication between hosts within the backup domain and is not associated with the backup itself. If a host ID certificate were updated or eliminated, it would have NO effect on the ability to restore backup data to that or another host.

OSB control messages and/or backup data may be encrypted while in transit over the network utilizing SSL encryption. Upon reaching its destination, messages and backup data are automatically

decrypted by SSL and are not encrypted when written to tape. As shown in Figure 3, security controls such as use of SSL is configurable.

Note: Backups which were encrypted by OSB on the host will not be re-encrypted via SSL for transport over the network.

Automated Media Lifecycle Management

Once backup data stored on tape is no longer needed, its lifecycle is complete and the tape media reused. Management requirements during a tape's lifecycle (retention period) may include duplication and/or vaulting across multiple storage locations. Oracle Secure Backup provides effective media lifecycle management through user-defined media policies:

- Retention
- Tape duplication
- Vaulting - rotation of tapes between multiple locations

Media lifecycle management may be as simple as defining appropriate retention settings or more complex to include tape duplication with the original and duplicate(s) having different retention periods and vaulting requirements. Oracle Secure Backup media families, often referred to as tape pools, provide the media lifecycle management foundation.

At its simplest level, a media family defines the retention methodology to be utilized for all tapes belonging to that media family. A duplication and/or rotation policy may then be associated with the media family thereby establishing how the tapes are managed throughout their lifecycle.

In Oracle Secure Backup, a volume is a single unit of media such as an LTO tape. Volume and tape nomenclature are used interchangeably. One backup operation may be contained on a single volume or span multiple volumes (referred to as a volume set).

Retention

There are two types of Oracle Secure Backup media families with differing retention methodologies as described below:

- **Time-managed** which leverages a user-defined retention ("keep volume set") associated with the media family to determine tape expiration.
 - File system data or Oracle database backups may be written to time-managed media families.
- **Content-managed** utilizes defined RMAN retention parameters associated with the database to determine when the tape may be reused (effectively an expired tape).
 - Only Oracle database backups may be written to content-managed tapes.

Beyond content or time-managed retention, you can define how long tapes may be written to, or if they may be appended at all after the first backup operation via the media family. In practice, tape pools are rarely configured to disallow additional writes. However, it's very common to limit how long a tape may be appended as defined by the media family's write window setting (optional).

Every tape will be associated with a media family. When Oracle Secure Backup first writes to a tape, the media family associated with that backup operation will be assigned. Only backups of the same media family will later be appended to the tape. When a backup operation is performed, OSB will automatically select an appropriate backup tape for use whether appending to an existing volume or writing to a new volume via overwriting an expired tape or an unlabeled one.

If a backup spans volumes, OSB will automatically swap tapes during the backup operation. A volume set will continue expanding until either the write window closes or expiration date reached (time-managed tapes only) at which point a new volume set will be created for the impending backup job.

Time-Managed Media Families

With time-managed media families, the retention period is associated with the tape as a whole, and not a particular backup housed on the tape. Upon first tape write, OSB will calculate a specific expiration date for the tape(s).

The date and time of the first backup operation written to a tape is always the starting point for calculating expiration. If a write window has not been defined, then tape expiration is calculated based on the media family's "keep volume set" duration. If a write window is defined, tape expiration will be the sum of both duration settings:

$$\text{Tape expiration date} = \text{Write window} + \text{Keep Volume Set duration}$$

File system or Oracle database backups may be written to time-managed media families.

Defining a write window is optional but recommended especially for time-managed tapes. Without one, the volume set will continue expanding up to date of expiration. All members of the volume set will have the same expiration date as was calculated at time of volume set creation.

Content-Managed Tapes

A specific expiration date is not associated with content-managed tapes as is done with time-managed. The expiration or recycling of these tapes is based on the attribute associated with the backup images on the tape. All backup images written to content-managed tapes will automatically have an associated "content-manages reuse" attribute. Since the recycling of content-managed tapes adheres to user-defined RMAN retention settings, RMAN instructs OSB when to change the backup image attribute to "deleted".

The RMAN DELETE OBSOLETE command communicates which backup pieces (images) are no longer required to meet the user-defined RMAN retention periods. Once OSB receives this

communication, the backup image attribute will be changed to “deleted”. The actual backup image isn’t deleted but the attribute is updated within the OSB catalog. Once all backup images on tape have a deleted attribute, Oracle Secure Backup will consider the tape eligible for re-use similar to that of an expired time-managed tape.

Tape Duplication

Many organizations have service level agreements requiring backup tapes be duplicated for redundancy and/or offsite storage purposes. With Oracle Secure Backup, tapes may be duplicated per user-defined policy or on demand for one-time duplication needs. Duplicate tapes may have the same or different retention and rotation schedules as that of the original tape.

Oracle Secure Backup 10.4 supports both traditional and server-less tape duplication. 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. Server-less tape duplication leverages Virtual Tape Library (VTL) capabilities to perform copy operations between virtual and physical tapes eliminating the transport of data through the media server. With server-less duplication, only OSB control messages and metadata regarding the duplication process are transported through the media server.

Server-less tape duplication is faster with reduced overhead on the media server than is traditional tape duplication. Figure 5 shows the data transport between the two duplication methodologies.

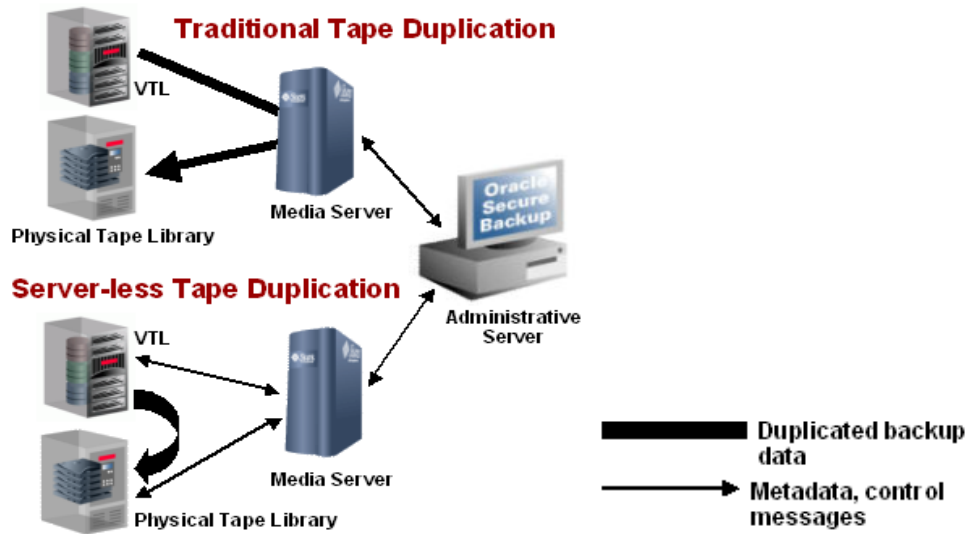


Figure 5: Graphical depiction of data transport differences between traditional and server-less duplication.

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 Device Support Matrix¹.

Tape Vaulting

Backup tapes are highly portable and often stored in offsite locations for disaster recovery purposes. These tapes are first created from within a tape device but usually don't remain within the device for long periods of time. Once removed from a hardware device, tapes may be stored in an onsite or offsite location. You can effectively manage tape movement between multiple locations using Oracle Secure Backup rotation policies.

A rotation policy defines when a tape should be moved, to which user-defined location and for how long. Within a rotation policy, you define rules for tape vaulting such as 1 hour after close of write window or 6 months after arriving at the storage location. The rotation policy is then associated with one or more OSB media families.

Oracle Secure Backup determines which tapes are eligible to move per rotation policy by performing a scan of the OSB catalog. This catalog scan can be evoked on a recurring "Vaulting Scan Schedule" or as a "Vault Now" operation. Tremendously flexible, vaulting scans may be scheduled by location or by media family within a location. Based on the vaulting scan results, OSB will automatically create a media movement job for the tapes to be moved along with an associated pick and distribution list.

In addition to pick and distribution lists, vaulting reports may be generated to effectively manage tapes between multiple locations. Report types include location, schedule, exception, missing or in transit.

Using Media Lifecycle Policies

The first step in creating an effective media management strategy is to define media requirements based on groups/tiers of backup data. Grouping backups with similar management requirements is especially important when using tape media. It wouldn't be an effective use of tape storage capacity to include backup images needed for 1 month on the same tapes as that requiring 7-year retention. Oracle Secure Backup media families and associated policies provide a consistent, automated solution for managing tapes.

¹ Tape Device Support Matrix: <http://www.oracle.com/technetwork/database/secure-backup/learnmore/osb-tapedevicematrix-520156.pdf>

Once your tape handling requirements have been established by group/tier, configure OSB media management policies:

- 1) Create a media family per “group” of backup data
- 2) Define storage location(s) where tapes may reside once removed from tape devices
 - a. These can be onsite or offsite locations
 - b. OSB will automatically create a storage location for each configured tape device, referred to as an active location
- 3) Create a rotation policy for each storage movement strategy
 - a. Examples of storage movement strategies:
 - i. Tape remains in library for 1 week, then moves to location XYZ for six months at which point it is then returned to the tape library for reuse
 - ii. Tape remains within originating device for 2 days, then moves to storage location 123 for 1 month, then moves to location XYZ until tape expiration date and then returned to the tape library for reuse
 - b. If all tapes moving between multiple locations utilize the same storage movement strategy, then only one rotation policy needs to be created and can be associated with one or more media families
- 4) Create a duplication policy per duplication strategy
 - a. Examples of duplication strategies:
 - i. Make two duplicates of tapes associated with media family A; One duplicate to same media family and second to media family B
 - ii. Make one duplicate of tapes associated with media family C to same media family
- 5) Associate rotation and/or duplication policy to appropriate media family(s)
- 6) Schedule vaulting and duplication scan schedules

Managing Volumes

The number of backup tapes managed by IT environments can be staggering ranging from a few hundred to many thousands. These tapes could be originals, duplicates, stored onsite or offsite or currently in transit between locations. Backup administrators need to know where tapes are located, what backups are on what tapes, and how to effectively handle exceptions for out-of-band situations. Even the most organized administrator can’t accomplish this without a solid underlying management system. Oracle Secure Backup puts information regarding volume content, location, movement schedule, duplicates (if any) at your fingertips.

From the volumes management page of the web tool as depicted in Figure 6, users can view all volumes or filter by location(s), media family(s) or volume attributes by selecting desired “view options”:

Manage: Volumes

View Options Apply

Volume Attributes

Unexpired volumes Expired volumes Open volumes Closed volumes

Volumes with no barcodes Volumes with no volume IDs

Single Selection

Volume ID: Barcode: Locations: Media family:

Other

Group volume set members

Edit Duplicate Recall Release Show Backup Sections Remove

Show Properties Show Backup Pieces Show Volume Set Show Duplicates

Select All Clear (1-6 of 6) Prev Next

Select	Volume ID	Barcode	Seq	Rotation policy	Duplication Policy	Location	Media family	Created	Expires	Spa
<input type="checkbox"/>	FS_onsite-000001	d1892a3627231028129000c294af78b	1	Tier_1	Offsite_1	vlib2	FS_onsite	2009/05/19.14:35	2009/06/21.14:35	248.
<input type="checkbox"/>	OSB-CATALOG-MF-000001	d198705427231028129000c294af78b	1	Tier_1	Offsite_1	vlib2	OSB-CATALOG-MF	2009/05/19.14:36	2009/06/09.14:36	249.
<input type="checkbox"/>	obe11g_DB-000001	d1a7aa4c27231028129000c294af78b	1	Tier_2	not specified	vlib2	obe11g_DB	2009/05/19.16:33	never; content manages reuse	none
<input type="checkbox"/>	obe11g_DB-000002	d1b71bf827231028129000c294af78b	1	Tier_2	not specified	vlib2	obe11g_DB	2009/05/19.16:33	never; content manages reuse	none
<input type="checkbox"/>	obe11g_DB-000006	d1f5a22e27231028129000c294af78b	3	not specified	not specified	vlib2	obe11g_DB	2009/05/19.16:33	never; content manages reuse	none
<input type="checkbox"/>	obe11g_DB-000007	d204d47427231028129000c294af78b	4	not specified	not specified	vlib2	obe11g_DB	2009/05/19.16:33	never; content manages reuse	41.8

Edit Duplicate Recall Release Show Backup Sections Remove

Figure 6: OSB web tool screenshot of the volumes management page.

Based on the view options selected, the corresponding volumes are then displayed. Additional information regarding volume contents, properties or associated volumes (i.e. duplicates) may be obtained by selecting volume(s) and then appropriate “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. The screenshot below shows how to edit a volume’s status:

Options Reset

Expire date Tip: May not be specified when selecting a new location or policy

Retain time seconds

Set new duplication policy

Set new rotation policy

Set new location Override rotation policy Do not create movement job

Not in transit Tip: May not be specified when selecting a new location or policy

Missing Attribute Yes No Tip: May not set Missing attribute while specifying a new location or policy

Volume ID	Missing	Rotation Policy	Duplication Policy	Location	Created	Expire
Local_tapes-000009	no	not specified	not specified	vlib	2010/01/05.14:52	2010/01/13.14:52

Figure 7: OSB web tool screenshot of volume editing options.

Oracle Database Backup and Restore

For over ten years, RMAN has been and continues to be the recommended backup utility for the Oracle database. Oracle Secure Backup is integrated with RMAN providing the media management layer (MML) for Oracle database tape backup and restore operations. The tight integration between these two products delivers high-performance Oracle database tape backup.

Specific performance optimizations between RMAN and OSB which reduce tape consumption and improve backup performance are:

- **Unused block compression** – Eliminates the time and space usage needed to backup unused blocks.
- **Undo backup optimization** – Eliminates the time and space usage needed to backup undo that is not required to recover the current backup.

Oracle Secure Backup further enhances performance for Oracle database backup/restore to tape by intelligent sharing other Oracle processes:

- RMAN and OSB share the SBT buffer which reduces CPU overhead upwards of 10%. By sharing the SBT buffer, OSB eliminates the need to copy data from the SBT to tape buffer as is the process for most other media management products.
- The Oracle database shadow backup/restore process and OSB data service communicate via a shared memory area for data transfer between the processes. On NUMA (Non-Uniform Memory Access) machines, OSB 10.4 insures these corresponding processes run in the same NUMA region(s) to deliver the fastest performance. If Oracle database shadow processes are spread over multiple NUMA regions for load balancing, OSB piggy backs on this distribution to always align processes within the same NUMA regions.

Oracle Database backup and restores from tape are best managed using Oracle Enterprise Manager (EM) or RMAN command-line interface. Oracle Secure Backup's integration with these products provides a uniform, familiar experience for Oracle customers.

Oracle Secure Backup provides policy-based media management for RMAN backup operations via user-defined Database Backup Storage Selectors. One Database Backup Storage Selector (SSEL) may apply to multiple databases or multiple SSELs may be associated with a single database. For example, you would create two SSEL for a database when using RMAN duplexing and each copy should be written to a different media family. The SSEL contains the following information:

- Database name / ID or applicable to all databases
- Host name or applicable to all hosts
- Content: archive logs, full, incremental, autobackup or applicable to all
- RMAN copy number (applicable when RMAN duplexing is configured)

- Media family name
- Name(s) of devices to which operations are restricted (if no device restrictions are configured, OSB will use any available device)
- Wait time (duration) for available tape resources
- Encryption setting

Oracle Secure Backup will automatically use the storage selections defined within a SSEL without further user intervention. To override the storage selections for one time backup operations or other exceptions, define alternate media management parameters in the RMAN backup script.

The tight integration between RMAN, EM and OSB makes initial configuration a simple process. By performing four easy steps, you are ready to backup the database to tape:

1. Define your OSB Administrative Server in EM enabling the OSB domain to be managed via Enterprise Manager.
2. Pre-authorize an Oracle Secure Backup user for use with RMAN allowing the RMAN backup/restore be performed without having to explicitly login to OSB.
3. Set-up Database Backup Storage Selector(s) in Oracle Secure Backup defining which media family, tape devices and encryption settings are to be used for RMAN backups.
4. Establish RMAN backup setting such as parallelism or compression as in the EM screenshot shown in Figure 8, below:

Tape Settings

Tape drives must be mounted before performing a backup. You should verify that the tape settings are valid by clicking on 'Test Tape Backup', before saving them.

Tape Drives

Concurrent streams to tape drives

Tape Backup Type Backup Set

An Oracle backup file format that allows for more efficient backups by interleaving multiple backup files into one output file.

Compressed Backup Set

An Oracle backup set in which the data is compressed to reduce its size.

Oracle Secure Backup Domain

Version on Database Server 10.3.0.2

Oracle Secure Backup Domain Target OSB

Backup Storage Selectors [Configure](#)

A backup storage selector is recommended when backing up the database to tape.

Figure 8: Enterprise Manager Database Control “Backup Settings” page.

For Oracle database restoration, a restore request is submitted from RMAN to OSB. If the tapes are within the library, the restore will begin immediately assuming device availability. However, if the tapes needed for restore could be offsite; you may want to confirm the location of tapes prior to issuing the restore command. With RMAN and OSB you can easily do so by issuing the following RMAN command(s):

- `RESTORE DATABASE PREVIEW` command provides a list of tapes needed for restoration which are offsite.
- `RESTORE DATABASE PREVIEW RECALL` command initiates a recall operation via OSB to return the tapes from offsite to the tape device for restoration. Once the tapes are onsite, you can begin the RMAN restore operation.

Oracle-Recommended Tape Backup for Oracle Exadata Database Machine

Oracle Secure Backup (OSB) delivers the fastest, best integrated, and most affordable tape backup for Exadata.

As an essential component of Oracle Maximum Availability Architecture (MAA), OSB has been tested and validated for Exadata by the MAA Development team. With an Oracle Exadata Database Machine Full Rack test configuration shown in Figure 9, OSB 10.3 demonstrated a backup rate of 8.6 TB/hour for full backups and an effective backup rate of 10 to 70 TB/hour for incremental backups². In these tests, available hardware throughput was saturated – faster backup rates could be achieved by increasing the number of tape drives.

How many more tape drives could have been effectively added to the environment? The MAA validation tested determined the effective maximum front-in throughput (Exadata to media server) using TCP/IP over Infiniband (IB) was about 2GB/sec per media server. The back-end hardware throughput could be increased (more HBA's/tape drives) improving performance until the front-end throughput of 2GB/sec is reached. Once front-end throughput is saturated, adding more tape drives would not increase performance without more media servers. What if front-end throughput were increased?

Oracle Secure Backup 10.4 leverages RDS / RDMA over Infiniband (IB), thereby increasing data transfer rates over the IB port on the media server providing two key advantages:

- 1) Potentially reduces the number of media servers required to meet performance goals as more front-end throughput allows more tape drives per media server to be effectively utilized. If throughput is around 50% higher using RDS / RDMA over IB, that would translate to about 3GB/sec instead of 2GB/sec per media server with one IB port.

² MAA White Paper: <http://www.oracle.com/technetwork/database/features/availability/maa-tech-wp-sundbm-backup-11202-183503.pdf>

- 2) Media server(s) could leverage multiple IB ports versus only one when using TCP/IP over Infiniband as adapter bonding does not support TCP/IP over IB at this time – only RDS / RDMA. Two IB RDMA ports per media server could effectively double the front-end throughput.

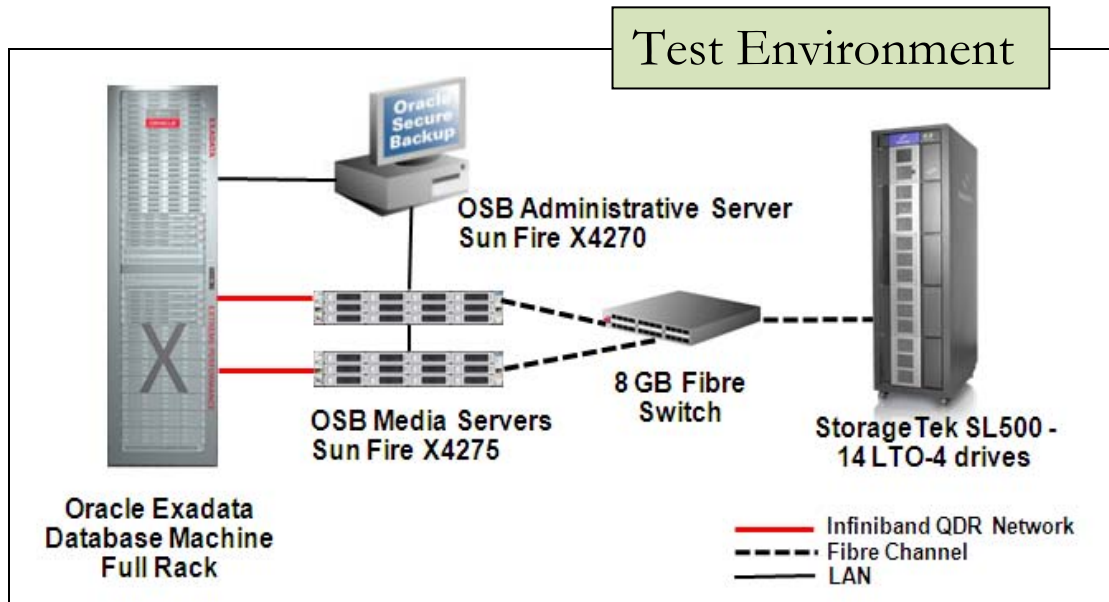


Figure 9: Exadata backup environment used in the MAA performance paper.

Oracle Secure Backup 10.4 achieves the fastest Oracle database backup to tape especially in engineered systems environments such as Exadata by leveraging RDS / RDMA over Infiniband. Oracle Secure Backup is pro-actively enhanced to deliver the best tape backup solution for the Oracle database – especially when using Oracle engineered systems.

File System Backup and Restore

From the enterprise data center to remote office, Oracle Secure Backup provides a scalable, data protection solution for your entire IT environment. Oracle Secure Backup delivers reliable data protection management with true “lights out” scheduling for heterogeneous, distributed environments.

Oracle Secure Backup offers multiple backups levels with full, cumulative and differential incrementals. In addition, a full offsite backup level may be scheduled without interfering with the regular full/incremental schedule. File system backups can be performed at the file, directory, file system or raw partition level meeting even the most stringent requirements within user-defined backup windows.

For file system backup operations, you define OSB “datasets” which describes what to backup. A dataset is a textual description employing a lightweight language to communicate how to build and organize files to be protected. Being Oracle Database aware, Oracle Secure Backup can skip database files during file system backups by using the “exclude oracle database files” directive within the dataset.

Dataset description files are hierarchically organized into a directory structure. Backups may be performed on a one-time basis as needed (Backup Now) or on a recurring schedule. Scheduling file system backups is an easy two-step process:

1. Create backup schedule identifying which dataset(s) to include, the priority level, encryption setting and device restrictions (if any).
2. Create backup trigger(s), which is a calendar-based time when the backup schedule will run along with backup level (i.e. full) and media family. A backup schedule often has multiple triggers but at least one trigger is required for the schedule to run.

File system restoration is equally easy to perform. Tree-style browsing of the OSB catalog offers multiple query options allowing browsing of all or a few backup versions. Data may be restored back to the original location or to alternative server as defined by the user.

When a file system restore is initiated and the necessary tape is offsite, Oracle Secure Backup will place the restore in a pending state and recall the tape. Once the tape is placed within the tape device, the restore operation will proceed.

Managing OSB Jobs

Operations that may occur on a recurring schedule or evoked immediately such as “Vault Now” are managed through Oracle Secure Backup scheduler. The OSB scheduler will automatically create a “job” with a unique identifier for each of these operations as listed below:

- File system backup or restore job
 - Backup of a dataset will generate a parent job then each host included in the dataset will have a corresponding subordinate job
- Oracle backup or restore job
 - Oracle database backup will generate a parent job then each backup piece will have a corresponding subordinate job
- Scan control job
 - Vaulting and duplication scans will each generate a scan control job
- Media movement job

- All tapes eligible to be moved as per a vaulting scan will be included within one media movement job.
- Duplication job
 - All tapes eligible to be duplicated as per a volume duplication scan will be included within one duplication job.

Large environments produce hundreds of operations daily and need an easy method of querying jobs. Oracle Secure Backup provides a streamlined jobs management page for quick filtering and access to jobs and associated information as shown in the Figure 8 below:

The screenshot shows the OSB web tool interface for job filtering. It features a 'View Options' header with an 'Apply' button. Below this are three main sections: 'Job Types', 'Job Statuses', and 'Filters'. The 'Job Types' section contains checkboxes for 'File system backup', 'File system restore', 'Dataset', 'Oracle backup', 'Oracle restore', 'Scan control', 'Media movement', and 'Duplication'. The 'Job Statuses' section contains checkboxes for 'Active', 'Failed', 'Complete', 'Pending', and 'Input pending'. The 'Filters' section includes dropdown menus for 'Hosts' (set to 'none'), 'User' (set to 'none'), and 'Dataset' (set to 'none'). Below these are date range selectors: 'Today', 'From' (02/19/2010), and 'To' (02/19/2010).

Figure 10: OSB web tool screenshot of job filtering options.

Each job will have a unique ID, properties and transcript. The job ID will include user name along with a sequential numeric number such as “admin/123”. Job properties describe high-level events such as the creation, dispatch, and completion times of the job. A transcript is created upon job dispatch and updates as the job progresses. The job transcript and properties are the best places to start when troubleshooting issues which may arise.

Oracle Secure Backup provides automatically generated reports of all or select jobs performed based on a user-defined schedule. These “Job Summary” reports may be generated by host, job type and distributed via email to selected users per user-defined schedule and date-range.

Broad Tape Device Support

Oracle Secure Backup supports over 200 new and legacy tape devices. New tape devices are qualified on an ongoing basis so please refer to the OSB compatibility matrix for the most current listing of supported devices.

Physical and virtual tape devices may be attached via SCSI, SAS or fibre as described on compatibility matrix. In SAN environments, Oracle Secure Backup dynamically shares tape devices between multiple hosts for maximum device utilization.

Summary

High-performant, secure data protection from server to tape is crucial for local and offsite storage of mission-critical data. Oracle Secure Backup delivers centralized tape backup management using a common management interface across all supported platforms. With an enterprise class feature set, Oracle Secure Backup easily scales from the smallest to largest IT environments delivering key advantages such as:

- Fastest Oracle database backup to tape
- Policy-based media lifecycle management
- Secure data protection with host-based or LTO and T10000 backup encryption options
- Dynamic tape drive sharing in SAN environments
- Heterogeneous file system data protection for UNIX / Linux / Windows and NAS devices

Oracle Secure Backup delivers data protection for the enterprise at over 75% less cost than comparable products. Unprecedented in the recent backup industry, OSB offers low-cost, single-component (per 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: Oracle Secure Backup 10.4:

High-Performance Tape Backup

November 2011

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

Copyright © 2009, Oracle and/or its affiliates. All rights reserved. This document is provided for information purposes only and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.