

# Oracle Secure Backup 10.2 Policy-Based Backup Management

*An Oracle White Paper  
December 2007*

# Oracle Secure Backup 10.2 Policy-Based Backup Management

## Product Highlights

- Fastest, most efficient Oracle database backups to tape
- Heterogeneous file system protection
- Backup encryption to tape
- Automated tape vaulting
- Automated or on demand tape duplication
- Automated migration from VTL to physical tape
- Backup and restore locally or over the network
- Dynamic tape drive sharing for maximum tape resource utilization
- ACSLs support
- Integrated with Oracle Recovery Manager (RMAN) and Enterprise Manager (EM)
- Low-cost, per tape drive pricing

## SECURE ENTERPRISE DATA PROTECTION

Reliable data protection in the enterprise extends beyond simple tape backup to multi-tiered data protection strategies based on criticality of data, recovery time objectives (RTO) and retention meeting business and regulatory requirements. Tape media remains the cornerstone of enterprise data protection providing the most affordable, reliable media for long-term backup storage. Enterprise environments consistently manage 1000s of backup tapes with differing retention periods, multiple tape storage locations and security requirements making effective tape backup management critical to the IT infrastructure.

## ORACLE SECURE BACKUP

Oracle Secure Backup is a centralized tape backup management solution providing performant, 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.

Optimized integration between Recovery Manager (RMAN) and Oracle Secure Backup (OSB) provides the fastest most efficient tape backup for the Oracle database. OSB provides the media management layer for RMAN supporting Oracle9i through Oracle Database 11g.

With a highly scalable client / server architecture, Oracle Secure Backup provides local and remote data protection leveraging SSL for secure intra-domain communication and two-way server authentication. The OSB backup environment (domain) is centrally managed from the OSB Administrative Server which houses backup metadata, configuration files, policies, schedules and is the certificate authority (CA) facilitating two-way server authentication.

## NEW IN ORACLE SECURE BACKUP 10.2

The next generation, Oracle Secure Backup 10.2, provides a broad set of new features, optimizations and enhancements. The key new features are listed below by category. While this isn't a complete list of enhancements, this paper discusses how these features meet enterprise tape backup requirements.



### **Encryption**

- Backup encryption to tape for file systems and Oracle9i forward

### **Policy-Based Tape Backup Management**

- Vaulting – Automated tape rotation between multiple locations
- Policy based or OnDemand tape duplication
- Migration from Virtual Tape Library (VTL) to physical tape

### **Device Support**

- ACSLS support for StorageTek/Sun enterprise libraries

### **Manageability**

- Enhanced OSB catalog backup with pre-defined policies

### **Performance**

- Oracle Secure Backup 10.2 and Oracle Database 11g performance optimizations

The individual merit of each new feature is significant in addressing data protection security and tape management complexities. Oracle Secure Backup 10.2 combines the new features with existing functionality delivering comprehensive policy based tape backup management for the enterprise. Increasingly datacenters are standardizing data protection operations achieving greater consistency for backup security and tape handling. With OSB 10.2, data protection can be streamlined through user-defined policies for servers, tape devices and media.

### **Backup Encryption to Tape**

The recent rash of lost backup tapes has catapulted backup encryption to the forefront. Addressing the new security paradigm, OSB 10.2 provides AES128, AES192 or AES256 backup encryption for supported file systems and Oracle database. With OSB 10.1, backup encryption to tape was limited to the database available for Oracle Database 10gR2 forward leveraging RMAN backup encryption technology. Oracle Secure Backup 10.2 backup encryption may be automated through user-defined policies or at the backup level for one-time backup encryption requirements with all encryption keys being stored and managed by the OSB Administrative Server.

It's long been said, "encryption is easy; it's the key management that's hard". OSB 10.2 addresses key management changes head on with multiple key generation options, key regeneration policies and central key storage on the Administrative Server. The implementation necessary for utilizing backup encryption is determination of key management options and procedures. Three key generation methods are available:

**Transparent mode** – The most secure method, keys are randomly generated based on the selected encryption algorithm AES128 to AES 256.

**Passphrase mode** – Keys are generated using a user-defined passphrase. If the encryption keys are no longer available, backups could be decrypted and restored using the passphrase.

**Transient mode** – Keys are generated using a user-defined passphrase. By default, transient keys are not stored on the Administrative Server since these are considered one-off backups. When restored, presumably at second site, which doesn't have access to original Administrative Server catalog, the user must input the correct passphrase to decrypt and restore.

Since transparent mode encryption keys are randomly generated, if the encryption keys are destroyed then the encrypted backups are useless since they can't be decrypted. This is the most secure encryption methodology and makes protection of the encryption keys of critical importance. The encryption keys can be protected by regularly backing up the OSB Administrative Server, which is pre-figured in OSB 10.2. With passphrase encryption keys, protection of encryption keys is critical from the perspective of guarding access to keys from unauthorized personnel and of course, remembering the passphrase. However, if the passphrase encryption keys were destroyed, the backup(s) could be decrypted and restored by inputting the correct passphrase.

All backup encryption keys are stored on the OSB Administrative Server in a key store directory. Upon OSB installation, users will define a password used to encrypt this key store securing the keys in the event the Administrative Server is compromised. Each host within the backup domain has a separate key store for encryption keys stored within the domain key store on the Administrative Server. During restoration of an encrypted backup, the Administrative Server passes the necessary encryption key via SSL to the client host for decryption but the key is not permanently stored on the client host.

Oracle Secure Backup 10.2 provides user-defined policy based backup encryption at the global, host or backup level. While most environments don't encrypt all backup data within the domain, users can enforce encryption of all backups by global policy. If a host or global policy requires encryption, OSB will automatically encrypt the backups per policy regardless of the encryption settings at a lower level such as backup job. By using global or host encryption policies, users can meet encryption requirements without exception or concern that a specific scheduled or one-off backup wasn't properly configured. In the event of an exception to policy, users can override the global/host policy by explicitly turning off encryption for that backup.

Host and global encryption policies effect both file system and Oracle database backups. For example, if the host encryption policy mandates all host backup jobs be encrypted, then OSB will automatically encrypt RMAN and file system backup

jobs from that host assuming RMAN had not encrypted the backup. If RMAN backup encryption had been utilized, OSB would not re-encrypt. Either RMAN backup encryption or OSB backup encryption can be utilized to satisfy the host encryption requirement.

Generally critical backup data is located on one or more servers so the most common use case will be encryption policies defined at the host or backup level. The screen shot below shows how to configure host encryption policies:

Apply OK Cancel Preferred Network Interfaces

**Host obe11g**

IP interface name(s):	obe11g.us.oracle.com
Status:	in service
Roles:	client admin mediaserver
Access method:	ob
Encryption:	<input checked="" type="radio"/> required <input type="radio"/> allowed
Algorithm:	<input type="radio"/> aes128 <input checked="" type="radio"/> aes192 <input type="radio"/> aes256
Rekey frequency:	<input checked="" type="radio"/> duration 30 day <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"/>
TCP/IP buffer size:	bytes
Key store:	<input type="radio"/> Add a key to the keystore without making it active
Certificate key size (in bits):	1024
	<input type="checkbox"/> Suppress communication with host

Apply OK Cancel Preferred Network Interfaces

Certificate keys define level of security for host authentication and are NOT related to backup encryption.

Select required encryption if all backups from this host must be encrypted and allowed if select host backups may be encrypted. By default, the backup encryption algorithm is aes192 but is user-configurable.

Define how often encryption keys are rekeyed. The system default can be defined using "Defaults and Policies".

Select desired method of key generation either random (transparent) or based on a passphrase.

Once the host encryption policies are defined, backup encryption will automatically be performed based on these settings. If host backup encryption is "allowed" and select backups need to be encrypted, backup encryption would be defined in the backup schedule. In the backup schedule, users may choose to encrypt the backup, which would then utilize encryption settings of algorithm, rekey frequency and key type defined for the host. For RMAN backups to be encrypted using Oracle Secure Backup, the OSB host (database server) must have encryption setting of "required".

For maximum security, encryption keys should be periodically regenerated limiting exposure to malicious attack if an encryption key were compromised. For example, if all host backups were encrypted using one key for January, another key for February and so on, then a single "compromised" key could effect only one month of backups not the last 5 years.

Key regeneration policies are defined at the host level by time duration or per backup. For example, a host could use one encryption key for all backups with a new key being regenerated every 30 days. Conversely, the host encryption policy could generate a new, separate key for every backup operation. For transparent encryption keys, key regeneration will occur automatically based on user-defined policies. For passphrase encryption keys, the user will be notified via email that a new passphrase should be defined to meet regeneration policies.

With OSB 10.2, users may choose to deploy RMAN backup encryption (Oracle Database 10gR2 forward) or OSB native backup encryption. While both utilize the Oracle encryption library, some distinct differences should be considered when deciding which method to deploy:

- RMAN backup encryption occurs within the Oracle database and requires Oracle database EE. The encryption keys are managed by the database and not by OSB.
- OSB backup encryption occurs on the database server but outside of the database similar to other 3<sup>rd</sup> party media management utilities. The encryption keys for file system and database backup are stored on the OSB administrative server. OSB 10.2 backup encryption is available for Oracle9i forward, all editions.
- During restoration of RMAN encrypted backups utilizing password mode, the password must be input to decrypt the backup.
- During restoration within the same backup domain of OSB encrypted backups utilizing passphrase-generated keys, the encrypted backup will be automatically decrypted and restored without user intervention. The passphrase must be input for restoration in a different OSB domain.

As discussed earlier, a transient backup encryption mode is available and defined at the backup not host level. The purpose of transient backups is to provide a one-off encrypted backup using separate encryption keys vs the keys utilized for ongoing encrypted backup operations. For example, a user may want to make an encrypted backup of one or more hosts and send the tapes to an alternate data center for restore and use. For these tapes to be decrypted, the keys must be available but it isn't prudent to send encryption keys that could decrypt more than just that backup. The transient mode is ideal in this scenario since the encryption keys are only used for that backup operation and can be decrypted by supplying the correct passphrase without requiring access to the source OSB administrative server.

### **Policy-Based Media Management**

The term "media management" within OSB refers to managing tapes (volumes). While backup tapes are the most cost effective media especially for long-term storage, tape expenditures in small and large data centers is substantial making tape handling and utilization very important. Tapes are inherently portable often moved from one location to another based on retention time and offsite storage policies.

Oracle Secure Backup 10.2 builds upon the media management concept of media families, tape storage pools, in OSB 10.1 extending policy-based management to include tape duplication, migration and vaulting.

A media management strategy effectively incorporates tape handling from creation to expiration to reuse. A simple strategy may just utilize media families for grouping backups with similar retention periods on the same tapes. More complex tape management requirements may require backup tapes be duplicated with one copy remaining onsite for one month then reused while the second copy be retained offsite for 6 months then returned onsite for reuse. Policy-based media management using Oracle Secure Backup 10.2 can be accomplished in 5 easy steps:

1. Define locations where tapes will be stored
2. Define rotation policies for moving tapes between locations
3. Define media families for grouping backups with similar retention policies on same tape(s)
4. Define tape duplication policies
5. Define location and duplication scans and schedule

Each of the steps can be configured using the command line (obtool) or the Web Tool. Showing how easily these policies may be created; screenshots of the Web Tool are detailed below:

### Step 1 - Define locations in which backup tapes are stored such as “media closet” or “Iron Mountain” etc.:

Apply OK Cancel	
<b>Location</b>	Demo
Customer ID:	
Notification type:	<input checked="" type="radio"/> none <input type="radio"/> Iron Mountain FTP
Mail to:	jane.doe@company.com
Recall time:	2 days
Comments:	The "Demo" location doesn't require a custom vendor format for pick reports. When requesting a tape be returned from this site, it takes approximately 2 days (recall time) to receive the tape.
Apply OK Cancel	

Customer ID and notification type are optional settings associated with 3rd party offsite storage vendors.

For example, if Iron Mountain is the storage vendor, you may input your Iron Mountain customer ID and select Iron Mountain FTP notification type. Rotation reports will then be generated in the correct format along with your customer ID for distribution to Iron Mountain.

The recall time defines the amount of time needed to request and receive back a tape from this location.

Oracle Secure Backup automatically creates a “location” during device configuration for all tape devices referred to as “active locations” as well as a media recycle bin, which may be used as an arbitrary “holding” location when tapes are ready for reuse. OSB uses the recall time (optional setting) to automatically restore

from the tape in closest physical proximity. For example, if one tape was stored at location A with a recall time of 1 hour and its duplicate were stored at location B with a 2 day recall time, OSB would request the tape from location A with the smallest defined recall time.

**Step 2 – Define rotation policies for moving tapes between configured locations:**

Three rotation rules have been defined for the "Test" rotation policy: Move from the tape library (vlib) to the location Demo then returned to the original site location in the Media\_Recycle\_Bin (default location indicating an arbitrary storage location). In this scenario, the Media-Recycle\_Bin has no defined duration meaning tapes may be moved/used at any time.

Defines triggers for when the tape becomes eligible for rotation / movement from current location.

Rotation rule(s)	Location	Event	Duration	Insert into position
vlib : windowclosed : 2 hours Demo : arrival : 6 months Media_Recycle_Bin : arrival : disabled	Demo	firstwrite	disabled	last

**Step 3 – Define media families:**

OSB\_Catalog\_MF and RMAN\_DEFAULT media families are predefined. Use these media families as defined, edit the settings and/or create additional media families. Most environments utilize multiple media families for grouping backups with similar retention methodology and/or retention.

The new "Full" media family is defined to use a Volume ID "unique to this media family" which means the media family name will be used within the volume ID name.

Volume expiration for this media family is "time managed" which associates a retention time with the volume. In contrast, "content managed" expiration associates retention with backup pieces on the tape.

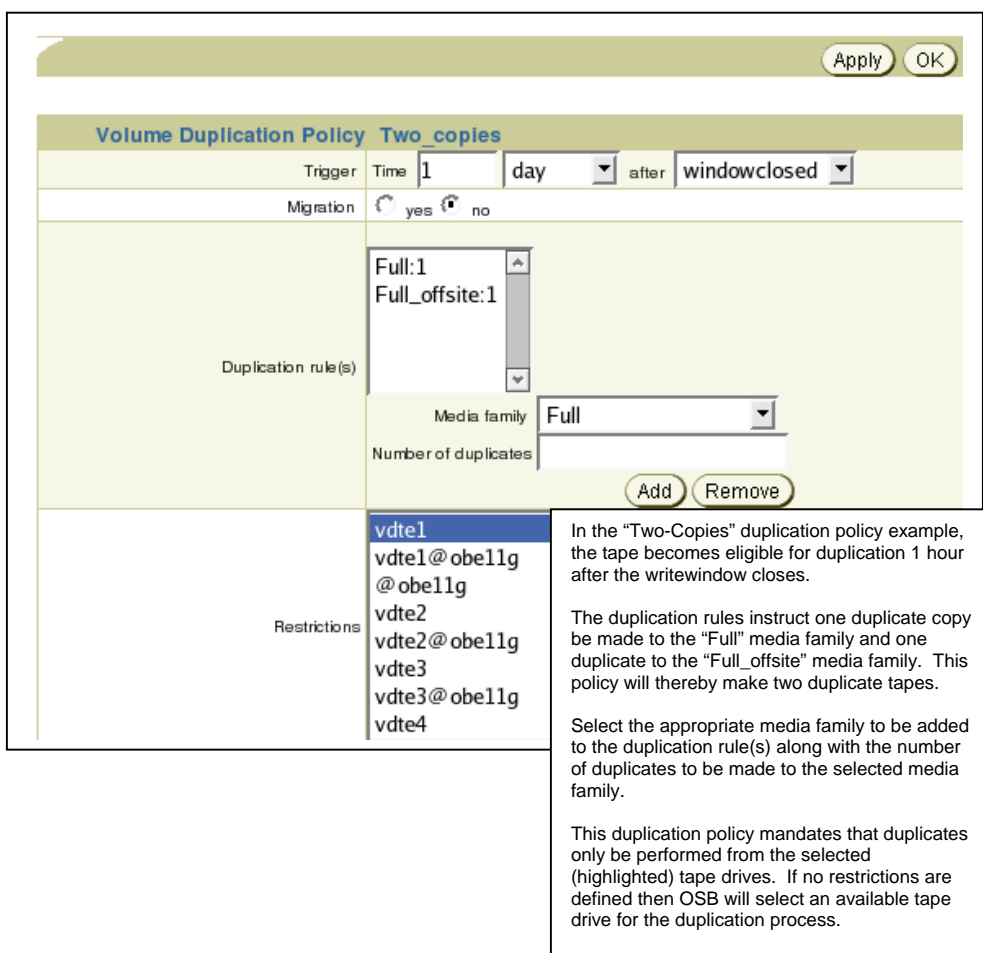
Associate defined rotation and volume duplication policies with a media family automating tape management. In this example, the "Test" rotation policy configured in the previous step is now associated with this media defining movement of all tapes written this media family.

Volume ID used:	System default
	<input checked="" type="radio"/> Unique to this media family
	<input type="radio"/> Same as for media family Full_offsite
	<input type="radio"/> From file
Volume expiration:	<input checked="" type="radio"/> Time Managed
	<input type="radio"/> Content managed
Write window:	1 week
Keep volume set:	3 weeks
Appendable:	<input checked="" type="radio"/> yes <input type="radio"/> no
Rotation policy:	Test
Volume duplication policy:	Two_copies

**Note:** A Write Window (optional) defines how long the tape may be appended. Once the write window closes, the tape can no longer be written to. The actual retention period for a time-managed tape from the first write is the sum of write window time + keep volume set time. In the example above, the tape retention period from the first tape write would be 4 weeks (1 week write window + 3 weeks keep volume set).

#### Step 4 – Define tape duplication policies:

Many organizations have service level agreements requiring select or all backup tapes be duplicated for redundancy or offsite/DR purposes. With Oracle Secure Backup 10.2, duplicate tapes may have the same or different retention as that of the original tape. Since retention methodology is defined within media families, the duplicate tape may use the same or different media family as that of the original thereby allowing separate retention setting for one or more duplicates.



**Volume Duplication Policy Two\_copies**

Trigger Time  day after

Migration  yes  no

Duplication rule(s)

- Full:1
- Full\_offsite:1

Media family

Number of duplicates

Restrictions

- vdte1**
- vdte1@obe11g
- @obe11g
- vdte2
- vdte2@obe11g
- vdte3
- vdte3@obe11g
- vdte4

In the "Two-Copies" duplication policy example, the tape becomes eligible for duplication 1 hour after the writewindow closes.

The duplication rules instruct one duplicate copy be made to the "Full" media family and one duplicate to the "Full\_offsite" media family. This policy will thereby make two duplicate tapes.

Select the appropriate media family to be added to the duplication rule(s) along with the number of duplicates to be made to the selected media family.

This duplication policy mandates that duplicates only be performed from the selected (highlighted) tape drives. If no restrictions are defined then OSB will select an available tape drive for the duplication process.

Once created, the duplication policy must then be associated with a media family as shown on the screenshot in step 3.

The duplication policy may be configured as a “migration” by selecting the “yes” option. The migration operation performs tape duplication then deletes the original thereby at the end of the migration. The migration option is particularly advantageous in virtual tape library (VTL) environments. Generally, backups are retained on VTLs for a short time period accommodating restore needs and then are copied to physical tape for long-term and/or offsite storage. In OSB 10.2, the migration is automated first making a physical copy then deleting the original backup on VTL thereby freeing up space for new backups.

### **Step 5 – Define when location and duplication jobs are run:**

Once all policies have been defined, the final step provides fine grain control over when OSB scans the catalog to determine which volumes are eligible to be duplicated or moved based on associated policies. The scan operation creates and places the duplication and rotation jobs in queue to be performed during the duplication window or location scan schedule respectively.

### **Device Support**

New tape devices are qualified on an ongoing basis with Oracle Secure Backup. For most newly supported devices, customers can update two ASCII files obtained from Oracle support as detailed in [Metalink note 420583.1](#) without requiring OSB version upgrade. The [tape device support matrix](#) is available on the OSB website on OTN.

Oracle Secure Backup 10.2 supports Sun/StorageTek ACSLS (Automated Cartridge System Library Software) managed tape devices as listed on the tape device support matrix.

### **Manageability**

The Oracle Secure Backup catalog maintains backup metadata, scheduling and configuration details for the backup domain. Just as it's important to protect the RMAN catalog or control file, the OSB catalog should be backed up on a regular basis. In Oracle Secure Backup 10.2, the catalog backup has been pre-configured:

- Media family - OSB\_Catalog\_MF (all catalog backups will be written to same tape(s))
- Job Summary – OSB-CATALOG-SUM (Daily reports showing status of catalog backup emailed to users)
- Dataset – OSB-CATALOG-DS (Defines all directories/files to backup for file system backups)
- Schedule – OSB-CATALOG-SCHED (Schedule for the catalog backup)

The primary catalog backup configuration settings have been defined with only one step remaining which requires user intervention: Edit the OSB-CATALOG-SCHED trigger(s) specifying when the backup should be performed.

## Performance

Oracle Secure Backup delivers the fastest Oracle database backup to tape! As part of the “Oracle product family”, Oracle Secure Backup has intimate access and integration with Recovery Manager (RMAN) not available outside of Oracle. Two key performance optimizations using Oracle Secure Backup 10.2 and Oracle Database 11g are:

- Eliminates backup of committed undo increasing backup performance and reducing tape consumption. Only non-committed undo will be backed up.
- Optimizes SBT buffer allocation using a shared buffer between SBT and tape (OSB). In past versions, RMAN writes data to the SBT buffer then the media manager copies data from the SBT buffer to the tape buffer. Using a shared buffer (OSB and RMAN only) reduces CPU overhead by up to 30% in internal tests.

**Please note:** These Oracle Secure Backup 10.2 and Recovery Manager 11g performance optimizations are not available with 3<sup>rd</sup> party media management utilities.

In addition to Oracle database backup performance enhancements, Oracle Secure Backup 10.2 has strengthened the data transfer architecture achieving faster performance over that of OSB 10.1 for file system and networked backups. Users are now able to explicitly define TCP/IP buffer size sending larger packet sizes over the network (as desired) further increasing remote backup performance.

## CONCLUSION

Oracle Secure Backup 10.2 provides maximum data protection security, advanced media management and performance for the lowest-cost in the enterprise tape backup industry. Oracle Secure Backup 10.2 key new features:

- Backup encryption - file system and Oracle9i forward
- Vaulting – automates the rotation of tapes between multiple locations
- Tape duplication – automated or OnDemand
- ACSLS support
- Backup performance – 10 – 25% faster database backup to tape performance than competition and up to 30% CPU reduction during the backup
- Migration from VTL to physical tape



Oracle Secure Backup 10.2  
December 2007  
Author: Donna Cooksey

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](http://oracle.com)

Copyright © 2007, Oracle. 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.