Oracle Secure Backup 12.1
Technical Overview

February 12, 2015
Safe Harbor Statement

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle’s products remains at the sole discretion of Oracle.
Program Agenda

1. Centralized Backup Management
2. Managing the Backup Domain
3. Device and Media Management
4. Backup and Restoring Data
5. Summary
Centralized Backup Management

Oracle Secure Backup
Oracle Secure Backup

Protects Entire IT Environment

• Oracle Database 12c to Oracle 10g
• 25 – 40% faster tape backup
• MySQL Enterprise Edition
• Heterogeneous file systems (UNIX/ Linux / Windows) and NAS devices
• Built-in Oracle Integration
• Centralized management in distributed environments
• Over 75% less expensive than comparable products

RMAN – Oracle Recovery Manager, MEB – MySQL Enterprise Backup, SBT – Oracle’s API for integration with media managers
Centralized Backup Management
Disk, Tape or Disk and Tape Backup Environments

Client / Server Architecture
• Data protection for heterogeneous, distributed servers managed from a central console, Administrative Server
• Media servers may be direct or SAN-attached to tape devices and disk backup target
• Oracle and MySQL databases may be located on any host within the backup domain as supported by the database
Oracle Integrated Solution For Exadata Tape Backup
Oracle Built, Supported and MAA Validated

- Optimized backup performance in Exadata environments
  - About 50% more throughput per IB port
  - Support for RDS / RDMA (Reliable Datagram Socket over Remote Direct Memory Access) over InfiniBand

- More efficient, Oracle-aware backup / restore in NUMA (Non-Uniform Memory Access) machines

For more information, refer to the Maximum Availability Architecture (MAA) white paper:

Oracle Integrated, Optimized Disk Backup
OSB and Oracle ZFS Storage Appliance

Advanced NDMP Integration

- Oracle ZFS Storage Appliance and OSB tight integration offers optimized backup / restore to disk
- Backups travel over an NDMP connection versus NFS to OSB disk pool configured on the Oracle ZFS Storage Appliance
- Eliminates need for an additional OSB media server (UNIX / Linux / Windows) to write backups to a disk pool on the NAS

Backup data over NDMP connection to the Disk Pool on the Media Server
Backup data travels from the Media Server over NFS to the Disk Pool on the NAS
Oracle Secure Backup - Enterprise Backup Software

- Policy-based management across the backup domain
- Management of backups to disk and/or tape throughout their lifecycle
- Oracle integration increases ROI and provides a single-vendor technical resource for increased customer experience
- Low-cost, single-component licensing reduces complexity and saves money
What’s New

Oracle Secure Backup 12.1

• Disk backup capability
• Self-describing backups
• Duplication at the backup image versus tape granularity
• Automated tape device discovery and configuration
• Enhanced catalog browsing / wildcard restore capability / “find” command
• Extended attribute support for Linux and UNIX platforms
Managing the Backup Domain

Policy-Based Management
Multi-level Management via Policies

Global “Defaults and Policies”
- Defines operational behavior across the backup domain
- Use existing settings or modify to meet your specific requirements

Host Policies
- Backup encryption along with key management directives for all backups from host
- Preferred network interface

Media and Lifecycle Management
- Media families establish backup retention to disk and tape
- Vaulting and tape duplication policies automate tape handling throughout lifecycle
## Defaults and Policies

### Fine-Grained Control over the Backup Domain

<table>
<thead>
<tr>
<th>Policy</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backup encryption</td>
<td>policies for backup encryption operations</td>
</tr>
<tr>
<td>Copy instance</td>
<td>copy instance policies</td>
</tr>
<tr>
<td>Daemons</td>
<td>daemon and service control policies</td>
</tr>
<tr>
<td>Devices</td>
<td>device management policies</td>
</tr>
<tr>
<td>Duplication</td>
<td>duplication-related policies</td>
</tr>
<tr>
<td>Index</td>
<td>index catalog generation and management policies</td>
</tr>
<tr>
<td>Logs</td>
<td>log and history management policies</td>
</tr>
<tr>
<td>Media</td>
<td>general media management policies</td>
</tr>
<tr>
<td>Naming</td>
<td>WINS host name resolution server identification</td>
</tr>
<tr>
<td>NDMP</td>
<td>NDMP Data Management Agent (DMA) defaults</td>
</tr>
<tr>
<td>Operations</td>
<td>policies for backup, restore and related operations</td>
</tr>
<tr>
<td>Scheduler</td>
<td>backup scheduler policies</td>
</tr>
<tr>
<td>Security</td>
<td>security-related policies</td>
</tr>
<tr>
<td>Testing</td>
<td>controls for test and debug tools</td>
</tr>
<tr>
<td>Vaulting</td>
<td>policies for media life cycle management operations</td>
</tr>
</tbody>
</table>

### Name | Current Value

- **Login token duration**: 15 minutes
- **Web inactivity timeout**: 15 minutes
- **Web session timeout**: 24 hours
- **Establish SSL communications**: Yes
- **Transmit X.509 certificates**: Yes
- **Encrypt backup data before transmission**: No
- **Public and private key sizes (in bits)**: 512, 768, 1024, 2048, 3072, 4096
- **Trusted hosts**: Yes
- **Minimum user password length**: 8
- **Password grace time**: 3 days
- **Password lifetime**: 180 days
- **Password reuse time**: 1 year
Security – Backup Data and Domain

Policy-Based Management

• Guarding access to the backup domain
  – User-level access control
  – Direct access to tape devices restricted to “Trusted” hosts
  – Embedded SSL technology provides secure transport of backup data and messages between two-way authenticated servers

• Securing backup data – Encrypted backups
  – Backup encryption protects data at rest (on tape or disk)
  – User selectable encryption algorithms AES128, AES192 or AES256
  – Backup encryption policies at backup, host or domain level
User-Level Access Control

<table>
<thead>
<tr>
<th>User</th>
<th>osbuser1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password:</td>
<td>••••••••</td>
</tr>
<tr>
<td>User class:</td>
<td>operator</td>
</tr>
<tr>
<td>Given name:</td>
<td></td>
</tr>
<tr>
<td>UNIX name:</td>
<td>jdoe</td>
</tr>
<tr>
<td>UNIX group:</td>
<td>sysadmin</td>
</tr>
<tr>
<td>NDMP server user:</td>
<td>no</td>
</tr>
<tr>
<td>Email address:</td>
<td><a href="mailto:jdoe@company.com">jdoe@company.com</a></td>
</tr>
</tbody>
</table>

“User Class” assigns the user to a set of Oracle Secure Backup specific privileges.

UNIX name: jdoe
UNIX group: sysadmin

• OSB user may have preauthorized access eliminating the login process
– Performing Oracle database backups using RMAN requires RMAN user preauthorization within OSB
Proven Embedded SSL Technology

Delivers Two Important Security Features

Two-Way Server Authentication

- A unique, identifying X.509 certificate is automatically created during installation
  - The OSB Administrative Server is the Certificate Authority (CA)

Protecting Data While In Transport

- OSB messages and data are encrypted as part of SSL communication
- Encrypted backups are not re-encrypted during transport

SSL decryption upon arrival

Backups written to disk or tape in non-encrypted format
Backup Encryption to Disk or Tape

Host Based or Tape Drive Encryption

OSB Host-based backup encryption:

- Encryption performed on UNIX / Linux / Windows hosts
- Backups encrypted to disk or tape
  - AES128, AES192 or AES256 algorithms

Tape Drive Encryption:

- Encryption performed by LTO or T10000 tape drive - AES256 algorithm
- Backups from NAS hosts may be encrypted
- Offloads encryption processing from the host
- Tape drive compresses then encrypts backups

Seamless Encryption Key Management:

- Encryption policies defined at global, host, volume or backup level
- OSB Key generation: Transparent or passphrase
- Rekey frequency per user policy
- Encryption keys stored centrally on Administrative Server
Backup Retention and Lifecycle Management Policies

**OSB Media Families**

- Defines retention based on:
  - Time:
    - Define retention duration within OSB
  - Content:
    - RMAN recovery window parameters determine when backup pieces are no longer needed
- Backup schedules include selected media family

**Tape Specific Media Family Settings**

- Volume ID naming convention
- Write Window (e.g. how long tape may be appended to)
- Associated lifecycle management policies
  - Vaulting and/or duplication
Policy-Based Management of Database Backups

Critical for Consolidated Environments

- Communicates storage parameter settings between RMAN / MySQL and Oracle Secure Backup
- Controls which media family and device(s) are used based on backup type and/or copy number
- Optionally, restrict these backups to specific tape drives
- One or more backup storage selectors may be configured per backup domain or database
Flexibility for System Administration

Easily Adapt to Operational Update Requirements

• Tape management:
  – Extend retention for select backup images or for all backups on a tape
  – Remove specific volumes from the OSB catalog (e.g., lost tape)
  – Set current tape status usable (default), read only, or out of service

• Disable or re-enable backup schedules

• Inventory the entire tape library or a subset of slots

• User-defined before and after scripts allow easy customization to meet company requirements
Device and Media Management
Disk Pools and Tape Devices
Backup Containers – Where Backups are Stored

**Disk Pool**

- File-system directory defined as an OSB disk pool
- OSB will restore from disk versus tape if backup resides on both
- Allows concurrent access for backup / restore operations
  - User defined maximum number of concurrent jobs (streams) per disk pool

**Tape Volume**

- Media such as a T10000D or LTO6 tape
  - OSB assigns a Volume ID upon first write to the tape
  - Tapes may reside in tape drives, libraries or another storage location (e.g. offsite vault)
- OSB supports one concurrent stream per tape drive
Backing up to Disk Storage

Oracle Secure Backup Disk Pools

- User-defined OSB disk pool(s) are associated with a file-system directory accessible to media server(s)
- Fine granularity of user control regarding disk pool management setting include
  - Storage - Capacity, Free space threshold
  - Performance - Number of concurrent streams
- Disk backups may be migrated to or copied to tape leveraging the same or different retention and media lifecycle management
- Optimized performance leveraging NDMP file service with the Oracle ZFS Storage Appliance
Disk Pool Management

• User-Defined disk pool parameters:
  – *Capacity* can either be a set value or left null in which capacity is only limited by the underlying file system
  – *Free-space goal percentage* represents how much available space the disk pool should maintain (default = 10%)
    • Upon reaching this threshold, OSB will purge expired backup images
  – Maximum *number of concurrent* backup/store jobs allowed for the disk pool
  – Blocking and Maximum Blocking Factor

• OSB will only consider disk pool available for use if space is available
Backing up to Tape Devices

- Broad physical and virtual tape device support
- Dynamic drive sharing between media servers
- Support for StorageTek ACSLS (Advanced Cartridge System Library Software)
- Server-less tape duplication with supported VTL devices
- Support and key management for tape drive encryption (LTO and T10000)
Automated Tape Device Discovery and Configuration

• OSB automates device configuration:
  – Discovers devices attached to OSB media servers:
    • Linux, Solaris, Windows and NAS
  – Creates attachpoints for devices based on SCSI mapping of the sg (Linux) or sgen (Solaris) device drivers

• Device configuration can be easily checked via the OSB Device Verify Utility

• Device policy can be enabled to automatically verify device serial numbers to proactively identify configuration issues due to device changes (e.g. drive swap) which could cause configuration issues

New: OSB 12.1
Tape Media and Disk Storage Management

Automated Re-use of Tapes and Deletion of Expired Backups on Disk

• Disk and tape storage is managed based on user-defined retention settings in OSB media families

• Expired backup images remain in the catalog and available for restoration until deleted by OSB due to space pressure

Expired Backup Images Purged:
• Disk pool exceeds space threshold or user-defined free space goal
• User explicitly deletes the backup image(s)
• Backup image is migrated to tape

Expired Backup Images Purged:
• Tape is overwritten or unlabeled

OSB Disk Pool
Self-Describing Backups

OSB Catalog Metadata Included with Backup Images

- Allows tapes and backup metadata to be quickly and easily imported into another OSB domain

New: OSB 12.1
Duplication of Tapes or Backup Images

Policy-based Tape Duplication

• Automated duplication of tapes via duplication policies and schedules
• Migrate or duplicate tapes from VTL to physical tape
• Server-less duplication with supported VTLs
• Duplicated tapes may have same or different retention / lifecycle

Backup Image Copies to Disk/Tape

• Migrate or copy backup from disk to tape or disk to disk
  – Copies to tape may be encrypted
• Copies may have the same or different retention / lifecycle
• Reclaim tape space by copying backups from one tape to another

New: OSB 12.1
Reclaiming Space on Tapes
Migrating Valid Backup Images from One Tape to Another

- Increases tape utilization
  - Valid backup images on partially full tapes may be migrated to another tape thereby freeing up the under-utilized tape for reuse
- Improves lifecycle management of backup images allowing select backups to be copied to another tape thereby extending retention as desired
- Maximizes security of backup copies as selected images may be encrypted during the copy operation

Tape Closed to New Backups

- Empty Space
- Backups No Longer Needed
- Valid Backup Images

Copy valid backup images

Unlabel tape

Tape Available for Reuse

Space available for new backups

Valid Backup Images

New: OSB 12.1
Policy-Based Tape Lifecycle Management

Media Family:
Tape pool foundation, establishes retention

Tape Reuse:
Expired tapes are automatically reused as needed when located with a tape device.

Duplication Policy:
Automates duplication of tapes using the same or differing retention / rotations.

Rotation Policy:
Automates tape rotation between two or more sites.

• OSB manages tapes from first write to reuse based on user-defined media families, duplication and rotation policies.
Tape Rotation and Duplication Policies

Optional: Associate a rotation and / or duplication policy to a media family

### Media Family

<table>
<thead>
<tr>
<th>Media Family</th>
<th>Full_FS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Volume ID used</td>
<td>System default</td>
</tr>
<tr>
<td></td>
<td>Unique to this media family</td>
</tr>
<tr>
<td></td>
<td>Same as for media family</td>
</tr>
<tr>
<td></td>
<td>From file</td>
</tr>
<tr>
<td>Volume expiration</td>
<td>Time Managed</td>
</tr>
<tr>
<td></td>
<td>Content managed</td>
</tr>
<tr>
<td>Write window</td>
<td>1 day</td>
</tr>
<tr>
<td>Appendable</td>
<td>yes / no</td>
</tr>
<tr>
<td>Rotation policy</td>
<td>Tier_1</td>
</tr>
<tr>
<td>Volume duplication policy</td>
<td>Tier_1_Offsite</td>
</tr>
</tbody>
</table>

#### Rotation Policy
- Tapes are moved between locations based on rotation policy
- Defines which locations the tapes will reside and duration at each location
- Trigger for when tapes eligible to move

#### Duplication Policy
- Defines which media family duplicate will use (same or different from original tapes)
- # of duplicate copies needed
- Trigger for when tapes eligible for duplication
Managing Tape Vaulting

• Vaulting scan generates a media movement job
  – “Vault Now” or based on triggers associated with Vaulting Scan Schedules

• Media Movement job includes all tapes eligible for rotation per policy
  – This job can run automatically or have pending status until run by user

• Reporting
  – Pick and distribution reports for each media movement job
  – Location, schedule and exception reports
  – “In transit” and “missing” (as marked by user) reports
Backup and Restoring

File system and Integrated Oracle Database Backups
Protecting Oracle Database Data

Tightly Integrated with Recovery Manager

• Performance optimizations achieving 25 – 40% faster backup directly to tape than comparable products
  – Unused block compression
  – Undo backup compression
  – Optimized buffer allocation between RMAN and OSB
• Encrypted backups using either RMAN or OSB encryption capabilities
• Tape vaulting optimizations with OSB and RMAN
  – RMAN restore database preview identifies offsite backup tapes
  – RMAN restore database preview recall initiates OSB recall of tapes for restoration
• Oracle database backup / recovery management
  – Utilize RMAN command line or Oracle EM (Database or Grid Control) restoring to original or alternate location
Oracle Database Environments

OSB and RMAN – Backup Method is the Same

- RMAN / OSB integration via SBT interface is the same regardless of the hardware infrastructure
- Oracle Secure Backup is installed on each server participating in the backup
  - Exadata and Oracle Database Appliance are backed up to over the network
  - UNIX / Linux / Windows database servers may be backed up locally attached tape devices or over the network

UNIX / Linux / Windows host(s) used as Oracle Database servers

Oracle Database Appliance

Oracle Engineered Systems
Oracle Integrated Backup to Disk and/or Tape
Multi-Tiered Strategy for Oracle Database Backups

D2D2T
BACKUP RECOVERY AREA;
BACKUP BACKUPSET;
RMAN can restore seamlessly from disk or tape!
Backup Encryption Policies
May be Defined at the Host Level versus Domain (Defaults and Policies)

- Backup encryption requirements and key management may be defined per host as to:
  - If encryption is required for all backups generated from this host
  - Backup algorithm
  - Rekey frequency and type of key generation

<table>
<thead>
<tr>
<th>Encryption:</th>
<th>allowed</th>
<th>required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Algorithm:</td>
<td>aes128</td>
<td>aes192</td>
</tr>
<tr>
<td>Rekey frequency:</td>
<td>duration 1 month</td>
<td>never</td>
</tr>
<tr>
<td>Key type:</td>
<td>transparent</td>
<td>use passphrase</td>
</tr>
</tbody>
</table>
File System Protection

Distributed, Heterogeneous Platforms and Network Attached Storage (NAS)

- File system backup / restore management
  - EM Cloud Control 12.1.0.1, EM Grid Control 10.2.0.5, EM Database Control 11.2.0.1, OSB web tool or unified command line (obtool)
- Recurring backup schedule or “Backup Now”
  - Full, incremental, and offsite backup levels
- Backup / restore of Network Attached Storage (NAS) devices using Network Data Management Protocol (NDMP)
- Tree-style catalog browsing for restoration to original or alternate location
- Automatic recall of tapes located offsite to perform the restore operation
- Refer to Certifications on My Oracle Support for listing supported platforms, operating systems and NAS devices
## Oracle Environments

File System Backup Methods Vary Based on the Host

### UNIX / Linux / Windows Servers
- OSB is installed on each host
  - Mounted file systems are backed up
- Oracle Engineered Systems - Exalogic and SPARC SuperCluster
  - OSB Administrative Server and/or client roles
- UNIX / Linux / Windows servers
  - OSB Administrative Server, Media Server and/or client roles

### Network Attached Storage (NAS)
- OSB backs up NAS devices using Network Data Management Protocol (NDMP)
  - Software is not installed on the NAS devices
- Can be configured as an OSB Media Server and/or client roles
- ZFS Appliances:
  - Support for NDMP “ZFS” and “DUMP” backup types
- Pillar Axiom 600:
  - OSB supports NDMP “DUMP” backup type
Datasets Define What to Backup

User-Defined Datasets

- Create a dataset to define the hosts, directories and files to backup on the file system(s)
- Use include / exclude statements within a dataset for precise definition of backup content
- Use “exclude oracle database files” directive to avoid backing up Oracle-related files from a file system backup
Enhanced Restore Capabilities

Browse Catalog by Backup ID, Path, File Name or Container

Fine granularity of searching for file(s) to restore.

New: OSB 12.1
Summary

Oracle Secure Backup
Oracle Secure Backup - Backup Software for the Enterprise

Policy-based management across the backup domain

Management of backups to disk and/or tape throughout their lifecycle

Oracle integration increases ROI and provides a single-vendor technical resource for increased customer experience

Low-cost, single-component licensing reduces complexity and saves money
Hardware and Software
Engineered to Work Together