Oracle ST-IT Saves Over $300,000 With Oracle Secure Backup

ORACLE

"Oracle ST-IT has saved over $300,000 in license renewal and annual maintenance costs by replacing our tape backup software with Oracle Secure Backup!"

---Tom Guillot
Senior Manager, ST Development Systems, Oracle

ORACLE

Oracle ST-IT Profile

- **Manages IT infrastructure for Oracle Server Technologies (ST) development organization**
- **Over 5700 concurrent users located on three continents**
- **65 System Administrators**
- **http://www.oracle.com/**

Data Protection Challenges and Objectives

- **Reduce annual maintenance costs for data protection**
- **Use Recovery Manager (RMAN) for Oracle database backup for improved integration with media management software**
- **Improve backup performance for faster more efficient backups**
- **Standard backup strategy across all ST-IT locations**

ST-IT Environment

- **Tape backup provides primary data protection medium**
- **Backup infrastructure managed by system administration organization**
- **Heterogeneous environments with mix of three platforms (Linux, Windows, Solaris) plus NAS devices**
- **Data amount:**
  - **20TB File system**
  - **4TB Oracle database**
- **Application(s):**
  - **OracleAS Discoverer**
  - **Oracle Designer**
  - **Oracle Portal**
  - **Oracle JDeveloper**
  - **Oracle WebServers / Middle Tiers**

OVERVIEW

Oracle ST-IT (Server Technologies - Information Technology) manages several IT environments within Oracle Data Centers located in US, Canada and UK. Protecting Oracle database source code, the family jewels so to speak is one of many responsibilities in ST-IT. For reliability and portability, tape backup remains the cornerstone of ST-IT backup infrastructure. With the release of Oracle Secure Backup in April 2006, Oracle ST-IT began migrating from a 3rd party tape backup utility to Oracle Secure Backup.

By deploying Oracle Secure Backup (OSB), ST-IT saved over $300,000 in license renewal fees and annual maintenance costs. In addition to significant cost savings, ST-IT achieved better performance, especially in NAS environments.

INTRODUCTION

With over 60,000 employees and 200,000+ customers, the Oracle data centers are architected to provide maximum reliability supporting employee productivity and continued growth. As a global corporation, Oracle data centers are located in many countries with IT management organized to support local technical needs while meeting strict Oracle Global IT requirements.

This paper focuses on the Oracle ST-IT organization responsible for the IT infrastructure of the database development organization representing approximately 5700 employees managed by about 65 System Administrators. Database developers and senior management alike rely on ST-IT for server availability, performance and data protection. Reliable backup and restore of Oracle databases, source code, user data and numerous applications are critically important within the Oracle database development organization because IT setbacks could directly effect Oracle database release schedule, adversely impacting customer satisfaction.

ST-IT'S ORACLE SECURE BACKUP DEPLOYMENT

Oracle ST-IT's first introduction to Oracle Secure Backup 10.1 was with the initial beta release utilized for proof of concept (POC) testing. With over 20TB of data to protect, the POC was an important step in the decision-making process determining whether or not to change the tape backup infrastructure. The heterogeneous POC test environment closely modeled actual ST-IT environments,

and it confirmed that OSB met backup and restore requirements for the largest and smallest of environments alike.

Immediately upon GA release of Oracle Secure Backup, ST-IT began migrating to Oracle Secure Backup for tape backup management at the following locations:

Location	# Of Clients	Amount of Data (GB)	Tape Technology
UK	50	2,894	StorageTek L700 with 10 LTO-2 drives (SCSI)
Montreal	6	778	ADIC Scalar 100 with 2 LTO-2 drives (Fibre)
Ottawa	7	252	ADIC Scalar 100 with 2 LTO-2 drives (Fibre)
Burlington	19	1500	StorageTek L180 with 4 DLT-7000 drives (SCSI)
Austin	57	4066	StorageTek L700 with 16 LTO-2 drives (Fibre)

Additional ST-IT locations are planned for migration in the near future but have been delayed due to legacy equipment and Operating System versions not supported by Oracle Secure Backup 10.1.

MIGRATING TO ORACLE SECURE BACKUP

Switching from one tape backup software to another is often met with hesitation due to management considerations for legacy tapes. Since tapes written by software A cannot be read or restored by software B, a migration plan from A to B must be considered. In ST-IT, the migration plan was straightforward and easy to implement:

- Switch from 3rd party backup utility to OSB on "X" migration date which varied by site
- Keep 3rd party backup utility installed on one server (HostA) for possible restore needs from legacy tapes
- In event of restore from tapes written prior to migration date, a tape device(s) would be moved from the OSB domain to HostA (previous software master server) for the restoration then moved back to OSB domain
- All restores from backups written after the migration date would be accomplished within the new OSB domain

Once all legacy tapes are expired, HostA will be decommissioned since restores from legacy tapes will no longer be needed.

ORACLE

Oracle ST- IT Environments-- OS and Storage:

- **Linux 32-bit architecture:**
  - **RHAS 3, RHEL 4 and Oracle Enterprise Linux**
- **Windows 32-bit architecture:**
  - **Windows 2000, 2003 and XP**
- **Solaris SPARC 64-bit architecture:**
  - **Solaris 9, 10**
- **Network Appliance (NAS):**
  - **Data ONTAP 7.2.2**
- **EMC Celerra (NAS)**
  - **DART 5.5**
- **Pillar Axiom300 (NAS)**
  - **AxiomONE 2.6**

OSB Terminology:

- **Administrative Server – One per domain housing OSB catalog and scheduling**
- **Media server – Host direct attached to tape devices**
- **Client – Host to be backed up**
- **Backup domain – All hosts / devices managed by OSB Administrative server**
- **Dataset – Defines file system data to backup**

NOTE: Oracle database may reside on any OSB host: Administrative Server, Media Server and/or client. At ST-IT, Oracle databases reside on both OSB media server and multiple client hosts.

NAS BACKUPS ARE 3 TIMES FASTER

In the Austin and UK environments, Networked Attached Storage (NAS) devices are heavily deployed to centralize data management operations. While NAS devices may be backed up using NFS, the preferred data protection methodology is using Network Data Management Protocol (NDMP). While both ST-IT's previous tape backup software and Oracle Secure Backup support NDMP to backup NAS devices, backup performance varied greatly between the two. Using Oracle Secure Backup, NAS backups are 3 times faster than before!

"From a system administrative perspective, an incredible advantage of Oracle Secure Backup is drive sharing across all hosts and probably the biggest win of migrating so far".

----Richard Doogan
Manager ST-IT, Oracle

Since NAS devices house most data, it is easiest to demonstrate the backup of one Network Appliance filer. This NAS backup consists of 5 volumes (src1back through src5back) backing up in parallel to 5 fibre attached LTO-2 tape drives in a StorageTek L700 tape library. Using Oracle Secure Backup, the NDMP backup is about 3 times faster completing within 24 hours as compared to about 70 hours previously. The backup times per volume are listed below:

- src1back - 500GB - 15 hours
- src2back - 510Gb - 15 hours
- src3back - 435GB - 12 hours
- src4back - 565GB - 16 hours
- src5back - 482GB - 24 hours

Since each volume utilized a separate tape drive, once the backup completed that tape drive became available for other backup operations increasing overall backup performance within the environment. With the previous software, NAS attached drives couldn't be shared with non-NAS devices translating to idle drives once the NAS backup completed.

Oracle Secure Backup dynamically allocates tape drives between NAS/UNIX/Linux/Windows media servers ensuring maximum drive utilization. Playing the traffic cop role within the SAN, OSB manages contention between servers and drives automatically allocating the next back/restore job to the next available drive. ST-IT standard practice maintains the same priority level for all backup jobs with the exception of source code backups, which are configured with higher priority meaning the backup job(s) are allocated to the next available tape drive ahead of backup jobs in the queue.

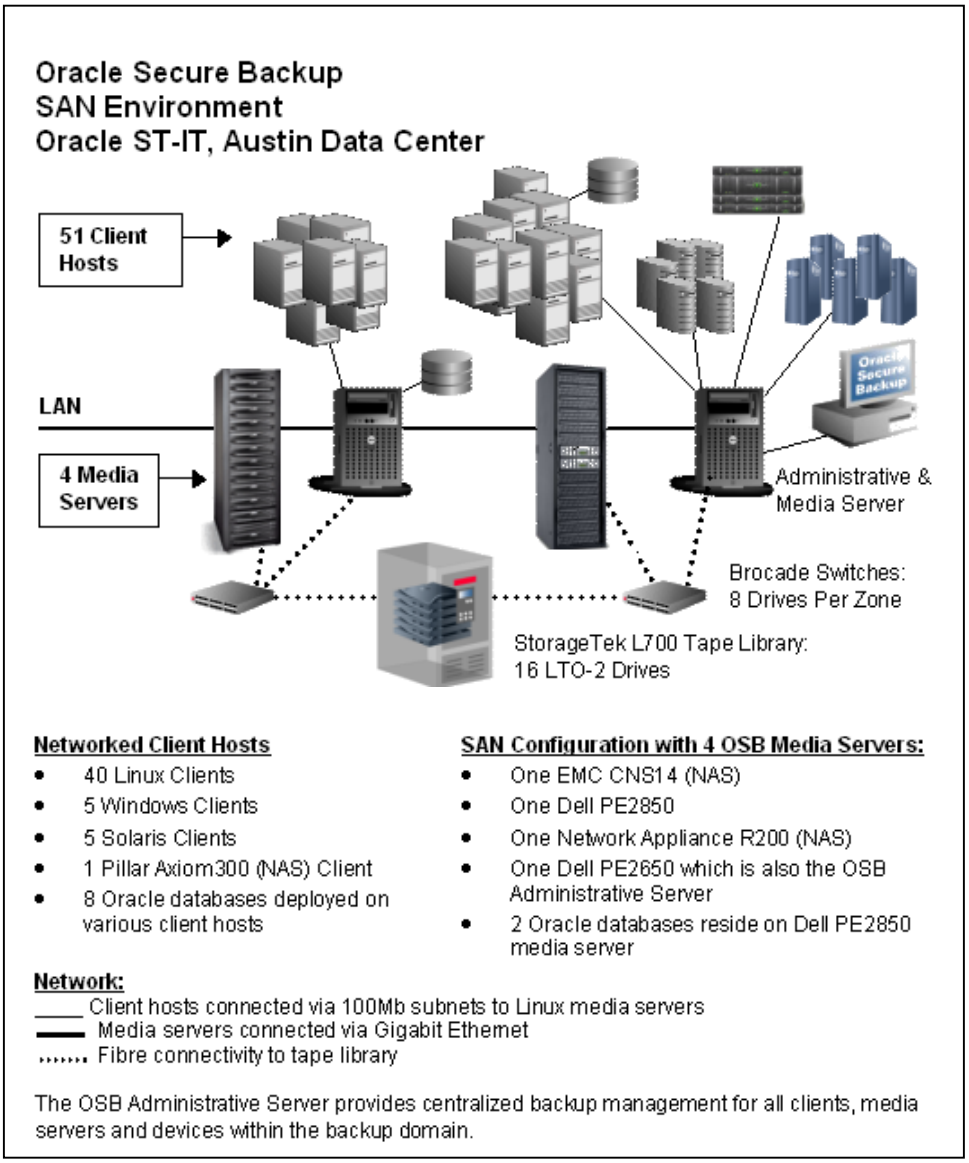
Since Oracle Secure Backup does not restrict sharing of drives or tapes between NAS and UNIX/Linux/Windows hosts, ST-IT was able to configure their environment to more effectively distribute backups between shared tape devices. With improved drive resource utilization, ST-IT has been able to accommodate a 30% increase in backup footprint without purchasing additional tape hardware, which wouldn't have been possible in their old environment.

Prior to OSB, NAS backups had to be confined to specific tapes and devices prohibiting a shared heterogeneous backup infrastructure.

CENTRALIZED TAPE BACKUP MANAGEMENT

Oracle Secure Backup 10.1 provides centralized tape backup management for five ST-IT environments protecting file system data and the Oracle database. Within ST-IT, system administration manages the OSB backup domain at each site, which protects in total about 24TB of data: 80% file system and 20% Oracle database.

With the number of hosts and platform mix, the ST-IT environment at Oracle's Austin Data Center best demonstrates backup infrastructure architecture achieving maximum utilization of tape resources while minimizing network traffic as depicted below:



For Oracle database backups, the combination of Recovery Manager (RMAN) and Oracle Secure Backup provides online backup to SAN attached tape devices. The two largest, most critical Oracle databases reside on an OSB Linux media server

achieving local access to tape devices, which is generally faster avoiding network contention. The remaining 8 Oracle databases are backed up remotely over the network.

The majority of data resides on NAS storage with heterogeneous servers distributed across the LAN. With over 50 servers and 3 NAS devices and one tape library, ST-IT backup architectural goal was to share tape drive resources between all hosts and offload the majority of backup traffic to a to a Storage Area Network (SAN).

The optimal solution meeting ST-IT goals was determined to be four media servers within the SAN directly accessing tape drives. Since the majority of data resides on two NAS devices, local backups would be both more performant and reduce network bandwidth traffic for backup data. Each NAS media server shares 8 LTO-2 tape drives with a Linux media server. The remaining client hosts are remotely backed up to tape devices accessed by Linux media servers as depicted above.

"By migrating to OSB, our tape drive utilization increased by allowing true heterogeneous drive sharing which accommodated a 30% increase in backup footprint without requiring purchase of new tape drives. With our previous software, drives were under utilized due to NAS sharing restrictions and new drive(s) would be required to scale 30 %"

----Richard Doogan
Manager ST-IT, Oracle

When determining how to configure client host backups, amount of data and proximity of the host to media servers were considerations. The combined amount of backup data from both NAS media servers is more than the combination of UNIX/Linux/Windows server backups. While client host backup data could be directed through the NAS media servers to attached tape drives, the Linux media servers were chosen to better balance the backup load between all four media servers.

CONFIGURING THE SAN ENVIRONMENT

Oracle Secure Backup dynamically shares tape drives increasing drive resource utilization in SAN and non-SAN environments. OSB automatically manages any contention between servers and shared devices. While dynamic drive sharing is most often associated with SAN, OSB provides the flexibility in non-SAN environments to leverage any available tape drive for backup operations effectively sharing the resources or restricting backups to select drives based on user-configuration.

ST-IT has a SAN configuration which load balances backup amounts between four media servers fibre attached to one StorageTek L700 library with 16 LTO-2 drives. For optimal throughput, the SAN is divided into two zones. Each zone includes two media servers (one NAS and one Linux server) connected through a Brocade switch accessing up to 8 drives.

While technically the SAN could have been configured allowing each media server access to all 16 drives, in practice, dividing SAN into zones better balances the resources. In addition, NAS vendors have recommended not exceeding more than 8 concurrent backups, which was accomplished with one NAS per zone.

Device access per media server within the zone is user-configurable allowing full or limited access to drives within the zone. For example, ST-IT could have configured the NAS to limit access to only 6 of the 8 drives within the zone.

Configuring drive access is accomplished by creating a device attachment per drive per media server. A device attachment describes the path between the host and the device itself. In OSB, the first step is to configure the devices then create associated attachments.

An attachment consists of the host name and raw device name making SAN configuration very straightforward. For example, the following attachments would provide access for Host1 and Host2 to the same drive identified by its raw device naming convention (/dev/obt0):

- Host1:/dev/obt0
- Host2:/dev/obt0

In ST-IT environment, 16 attachments per zone were configured: 8 drives * 2 media servers. With Oracle Secure Backup, a SAN configuration is easy to setup especially compared to ST-IT's previous backup software, which had a more complicated installation process, and restricted sharing of NAS attached tape drives.

ORACLE SECURE BACKUP

Media Concepts:

- **Media Family – storage classification for grouping backups with like retention policies**
- **Write Window – defines how long a tape may be appended (optional)**
- **Retain Time – defines how long a tape is retained after write window closes or from the first tape write if a write window wasn't defined.**

BACKUP SCHEDULE AND MEDIA RETENTION

With migration to Oracle Secure Backup, ST-IT standardized backup strategy at all locations creating a unified, documented and consistent backup infrastructure. The backup schedule and retention is:

Full Backup

- Every Friday night
- Retention period is one month to one year depending on the data

Incremental Backups

- Monday – Thursday evening
- Retention period is one week to one month depending on the data

Within Oracle Secure Backup, tape retention is best managed by creating a "media family" for each retention policy. At each ST-IT location, the media families are uniformly defined standardizing operational procedures for file system and Oracle database backups.

Media families for file system backups:

- "FullBackups" – 15-day write window, 3 month retain time
- "FullBackupsYear" – 5-day write window, 1 year retain time
- "DailyBackups" – 2-week write window, 2-week retain time
- "OSBcatalog" – 2-week write window, 2-week retain time

For file system backups, media families are defined with a "retain time" which is often referred to as time-managed volumes. The "retain time" added to the write window time defines the total retention period for the tape. For example, the

media family "DailyBackups" sets the tape retention for 28 days (2 weeks + 2 weeks) from the date of the first tape write.

It is important to note that retention periods for file system backup tapes are set at the tape level and not at the level of individual content (backup images) on tape.

Media families for Oracle database backups:

- "DBFull" – 15-day write window, content managed retention
- "DBFullYear" – 5-day write window, content managed retention
- "DBDaily" – 2-week write window, content managed retention

For Oracle database backups, content managed media families were defined allowing Recovery Manager (RMAN) retention settings to determine when backup images are no longer needed. While time-managed media families could be used for Oracle database backups, content-managed media is intimately integrated with RMAN providing the most efficient retention methodology.

Content-managed tapes are not associated with a specific tape expiration date as are time-managed tapes. Instead, expiration is determined by the content (backup images/pieces) residing on the tape. For tape retention and recycling of content-managed tapes, define RMAN retention policies using either recovery window or redundancy settings. The validity of backup pieces is communicated to OSB when the RMAN "DELETE OBSOLETE" command is issued. OSB uses this information to determine when content-managed tapes may be recycled.

Two important configuration steps for content-managed tapes:

- Maintain RMAN backup metadata for at least as long as desired retention policy (either in control file or RMAN catalog)
    - ST-IT control file record keep time is 30 days
- Regularly issue "DELETE OBSOLETE" command
    - In ST-IT, the RMAN command `"delete obsolete recovery window of 21 days device type sbt"` is issued at the end of each backup

An important difference in managing content vs time-managed tapes is how they are reported within OSB on volume headers or transcripts. For time-managed tapes, the actual tape expiration date is reported (as calculated from first tape write, write window and retain time). For content-managed backups, the retain time is reported as "never-expires" since OSB does not associate a specific expiration date with the tape. In actuality the tape will "expire" and be eligible for reuse once each backup piece on the tape is no longer required to meet RMAN retention periods.

CONCLUSION

From a system administrative perspective, migrating to Oracle Secure Backup was easy with minimal learning curve from our previous backup software, which had been in production for over 6 years. Since system administrators manage the backup infrastructure in ST-IT, Oracle Secure Backup had to meet backup

requirements for both file system and database data in a standardized management framework. Oracle Secure Backup exceeded system administrator requirements and achieved over $300,000 cost savings for the ST-IT organization.

Key advantages achieved by migrating to Oracle Secure Backup:

- Achieved substantial cost savings
    - Both initial/renewal licensing and ongoing maintenance fees
    - Better drive resource utilization accommodating a 30% increase in backup footprint without additional tape hardware
- Increased drive utilization allowing NAS devices to share drives with UNIX/Linux/Windows servers, leading to 3 times faster backup
- Increased media utilization since NAS/UNIX/Linux/Windows data may be written to same tape
- Improved scalability since servers can be added to OSB domain without any licensing fees
- Increased system administrator productivity with ease of use and integration with Oracle Enterprise Manager Grid

Oracle Secure Backup - Oracle ST-IT: Case Study
July 2007
Author: Donna Cooksey, Principal Product Manager, Oracle Corporation
Contributing Author: Richard Doogan, ST-IT Manager, Oracle Corporation

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
www.oracle.com