



Wikibon.com - <http://wikibon.com>

Oracle Backup and Recovery Strategies: Moving to Data-Protection-as-a-Service

by David Vellante - 22 October 2015

<http://wikibon.com/oracle-backup-and-recovery-strategies-moving-to-data-protection-as-a-service/>

Premise

Backup in many Oracle shops specifically, as with many organizations generally, is viewed as a necessary evil with a process that is bolted on as an afterthought. Many IT organizations either under-fund backup or (in some cases) over-engineer backup where rigorous procedures may not be required. Wikibon surveys show that more than 50% of IT organizations consider their backup strategy to be a “one-size-fits-all” approach. Moreover, 1/3 of practitioners in the Wikibon community want to achieve data-protection-as-a-service but they don’t know how to get there.

A blanket approach to backup is inadequate in today’s 24x7x365 world. More attention must be paid to reducing RPO and RTO while at the same time providing greater granularity on an application-by-application basis. Over the last five years, the most effective way to deliver this business objective was to utilize consistent, space-efficient snapshots in a continuous data protection model, combined with off-site replication and best practices in Oracle backup and recovery. New developments have emerged that go beyond this approach and use a changed block time stamp method that reduces the exposure to data loss. This research note reviews best practices for Oracle backup and recovery and introduces new concepts announced earlier this year with Oracle’s Zero Data Loss Recovery Appliance (Recovery Appliance or ZDLRA).

Introduction

Backing up transactional databases such as Oracle is often viewed as a complicated matter. Of particular concern is making sure the appropriate type of backup solution is in place and, importantly, that backups are actually working meaning they can ultimately be recovered. As the saying popularized by storage strategy guru Fred Moore goes, “**Backup is one thing...recovery is everything.**”

An organization’s ability to recover from hardware or software failures, human error, security breaches and other disasters is a fundamental requirement of compliance and governance. Unfortunately, in many organizations, auditors focus on the existence of a process and not its efficacy. Frequently, for example, checks are made to ensure that backups are being performed, however it’s common that little or no attention is paid to testing and periodically validating that backups were successful and data can be completely, accurately restored and recovered.

Given the lack of rigor in many organizations’ auditing and compliance processes, it falls on the database administrator and/or storage admin teams to ensure that proper steps are taken to minimize data loss (i.e. get as close to RPO zero as possible) and assure that an appropriate time to recover can be met on an SLA basis.

Understanding Business Objectives for Recovery

The basics of understanding the requirements for data availability from an application’s perspective are as follows:

The **Recovery Time Objective** (RTO) for an application is the goal for how quickly an organization needs to have an application’s data accurately restored, recovered and available for use after an “event” has occurred, where the event is one that restricts access to application data.

The **Recovery Point Objective** (RPO) for an application describes the point in time to which data must be restored to successfully resume processing (often thought of as time between last backup and when a “problematic event” occurred). RPO defines the amount of data that’s at risk of being lost. The theoretical goal for mission-critical applications is RPO zero—i.e. zero data loss.

RTO and RPO metrics are useful in discussing what technologies, products, processes and procedures are required to meet those goals. Setting the objectives should come from assessing the business impact of applications being unavailable, the consequences of data loss and the budget available to meet these objectives.

Wikibon research shows that leading edge Oracle DBAs and Storage Admins take it upon themselves to ask the following questions:

1. Does my organization understand which data are critical to ensure fluid business operations?
2. Can I guarantee to the Board of Directors that such data is adequately protected?

3. Can critical data be recovered in an acceptable timeframe as defined by the business?
4. How much data can I afford to lose for a specific application if an event occurs?
5. Do I have the systems in place to ensure that if an event occurs, my data loss will be less than that which I can afford to lose?

Adequately addressing these questions will provide a framework for taking steps to protect organizations from critical data loss.

Oracle Backup and Recovery Alternatives

To simplify the discussion, this section of the research note focuses on backup approaches that are endorsed and supported by Oracle. There are essentially two types of data protection approaches for backing up Oracle databases:

- User Managed
- Oracle Recovery Manager (RMAN)

User Managed Backup

Prior to Oracle 8, admins had limited backup choices. The primary method was User Managed backups. Since the introduction of RMAN, Oracle has strongly encouraged customers to use this newer utility to simplify backups. However many admins shied away from RMAN because of perceived complexity, but improvements since the introduction of Oracle 9i and in particular 10g have made RMAN the most logical choice for most leading Oracle shops.

User Managed backups are essentially manual backups initiated by the Oracle admin via scripts. By initiating the scripts, a user places Oracle into backup mode. There are two backup modes a user can choose – either a “cold” offline mode or “hot” online backup. In either case, once the backup is complete, the database must be taken out of backup mode.

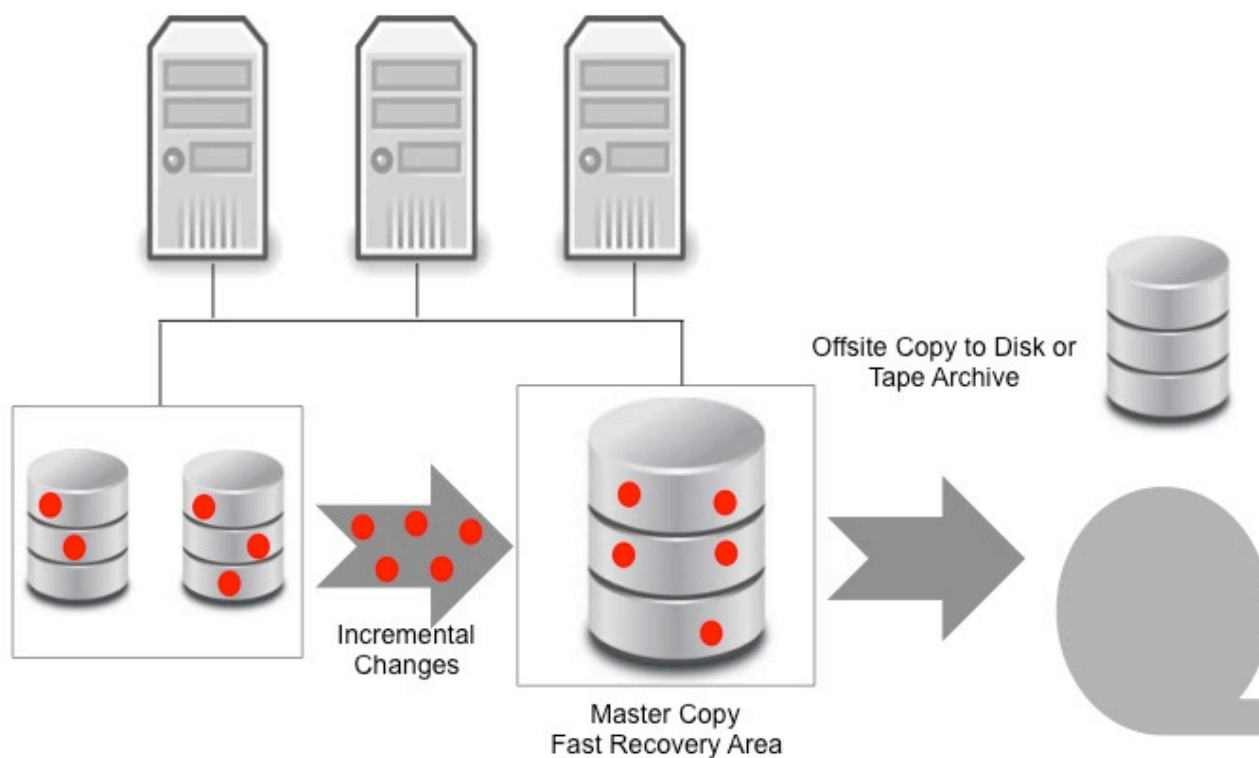
There are two other challenges with User Managed Backups: 1) Recovery is also manual and 2) they don’t support incremental backups. Moreover, the end-to-end process can be complicated and as such, in the last several years, most Oracle shops have moved away from User-managed to an RMAN strategy. While User-Managed backup isn’t widely used by itself, the construct of backup mode is still in play as part of a storage-centric backup approach as discussed later in this research note.

RMAN Backup

RMAN is the preferred backup approach within Oracle and is considered a best practice. The RMAN utility bundled with Oracle databases for no extra charge. Unlike User Managed backups, RMAN is fully integrated with the Oracle database and has end-to-end visibility on the backup, restore and recovery process. RMAN backups can be done with a single command or via Oracle’s Enterprise Manager interface and virtually all popular backup software products integrate with RMAN.

While RMAN has gained popularity over the last few years, up until a few years ago it was still new to some shops. In the early 2000’s, practitioners reported early problems with RMAN, however improvements over the last several database releases have made RMAN the most practical solution for most environments.

Figure 1: Incremental Updated Backup Model with Fast Recovery Area – Source Wikibon



With the introduction of Oracle 10g, RMAN capabilities expanded beyond the meat and potatoes full backup strategy with the introduction of incremental backups (See Figure 1), which take an RMAN full image copy of a database on disk and allows it to be updated in-place and on the fly. This enables the creation of a full backup valid to the point of the incremental simply by merging the incremental with the “master” copy. This approach achieves an incremental forever strategy by saving incremental updates versus taking a full disk image. However this approach has the drawbacks of space consumption using image copies and it isn’t really feasible to keep more than about a week of recovery from disk as the image copy must be rolled forward using the incrementals before the full is brought to the point of the last incremental backup. While this process can be automated, it’s overhead-intensive.

Also with 10g, Oracle introduced Flash Recovery Area (FRA), which was re-named Fast Recovery Area. FRA stores recovery-related files (e.g. redo logs, control files, copy data, RMAN backups, etc.), in a single location so they can be automatically managed by the database. This simplified RMAN backups because it relieved the DBA from having to worry about disk space management, numerous configuration parameters and hunting down files during a recovery.

RMAN has continued evolving with 11g and 12c database versions providing the flexibility and automation needed to keep pace with more stringent backup and recovery requirements. For example with Oracle database 12c, RMAN provides table-level restore granularity, which was widely a requested enhancement that Wikibon practitioners indicate further simplified backup. Most commercial backup applications are integrated with RMAN and Oracle also offers its Cloud Backup Service for database backup to the Oracle public cloud. Oracle has also introduced its Zero Data Loss Recovery Appliance discussed later in this note.

Third Party Hardware Innovations

Snapshot Technology

Prior to the acquisition of Sun Microsystems, which was completed in early 2010, Oracle was exclusively a software company and as such focused on providing software infrastructure products for tasks such as backup, rather than specialized hardware. Oracle's strategy was to partner with backup providers and storage hardware and software companies such as Symantec, EMC, NetApp, HP and others who specialized in backup. Oracle's goal was to improve the cost and efficiency of its infrastructure offerings, including backup. Notably, Oracle continues to maintain partnerships with such companies today, however they also compete directly with these suppliers.

Snapshot technologies became very popular in the early 2000s for taking a fast "picture" of data on storage at a given point-in-time with negligible impact. Storage hardware companies began introducing the idea of taking frequent snapshots to rapidly create point-in-time copies of data which initially was targeted at test/dev environments. Snapshots use the master copy of data and then take point-in-time snaps using pointers back to the master data. Snapshots are virtual, not physical copies and as such they are space efficient. Snapshots are maintained on the same physical storage system where a copy is created when a write command is initiated by the array.

Some organizations began to expand use snapshots to the backup arena. For shops using User Managed backups, the appeal of this model was it was faster than doing daily or weekly full backups and it created the perception that frequent snaps lowered RPO.

However practitioners began to realize there were several problems with using snapshot technology as a primary backup method for production data. Three main issues include:

- Database performance problems
- Availability concerns using the same storage array for production and backup
- The recovery restore process tends to be error-prone and risky. As well, many backups are not successful and without good reporting, many users were exposed to further data loss.

Specifically, as it relates to database performance, doing copy-on-writes creates multiple input/output operations – one to overwrite the change to the original database block and one to create the copy in a new location. In addition, as the array gets full and more and more writes occur, fragmentation in the data layout occurs. This can be problematic because while the database may issue an I/O request that theoretically can be served in a sequential manner (advantageous for spinning disk drives), the storage array must service that request over a fragmented dataset, resulting in many small block random I/Os, which can negatively impact database performance. Flash storage can address this performance issue, but as we'll discuss later, it introduces new bottlenecks to the backup process.

System availability is also a concern with snapshotting technology. Because copies are done on the same physical array, any outage in that array creates a problem for data accessibility. Wikibon practitioners reported that snapshot technology was very good for non-production systems such as test/dev, however they began to realize that unless they made copies to a secondary physical media their data was not fully protected. Once a copy was made to a separate media from the production disk array, the storage reductions of snapshots went out the window as all blocks, not just changed, had to be copied to a remote location.

Hardware vendors began to understand the value of RMAN integration, and started integrating with the utility and building plug-ins, making snapshots a more viable backup solution that many Oracle customers use today. Performance issues notwithstanding, many organizations have used their existing arrays as a convenient means of backing up data. However because customers recognized the need to copy data to a secondary device, it became an expensive and often complicated proposition to protect data using a primary storage device to perform disk-based backup. In addition, snaps often include the entire volume meaning a staging area must be used to restore the whole volume, then restore any datafile(s) from that staging area. This negates space savings of snaps plus highlights the potentially manual, multi-step backup and restore process.

Data De-Duplication Devices

Realizing snapshots had certain limitations in backup environments, storage vendors began to introduce and popularize in-line,

high performance data de-duplication systems specifically designed to both replace tape as a primary backup medium, and address the overhead problems described above with snapshotting technology.

Data de-duplication (AKA purpose-built backup appliances – PBBAs) use a form of data reduction to dramatically reduce the amount of storage required to back up data. Ratios of data reduction depend on workload but often customers can achieve 3, 5, or even 10:1 reduction ratios for database and even higher for file system backups. PBBAs identify duplicate files and blocks inside the backup stream to avoid storing duplicates on the backup appliance. The de-duplicating process is transparent to the application, making them an attractive approach.

These appliances can make disk-based backup significantly less expensive by reducing storage consumption and while tape is still cheaper, the convenience of disk-based backup and recovery was attractive to many customers.

There were two broad ways in which the de-duplication occurred, one on the server side and one after the data was pushed over the network into the backup appliance. The latter, popularized by Data Domain, became the dominant choice, because it didn't necessitate any changes to the backup application or process. Whereas the former, advocated initially by companies like EMC/Avamar (prior to EMC's acquisition of Data Domain), would perform data reduction prior to pushing data over the network to the storage device.

While seemingly simpler and more attractive, in order to store a gigabyte, the system has to push a gigabyte over the network and then the appliance does its magic and de-duplicates the data. Some vendors like Data Domain did this operation in-line and others like NetApp and Ocarina (acquired by Dell) chose to perform the de-duplication as a post-process operation, which added overhead to the end-to-end backup process.

Data Domain's approach became the dominant PBBA method within Oracle environments and, as with snapshot methods, vendors realized the benefits of integrating with RMAN and began to do so. And while RMAN supports incremental backup, many practitioners chose to stick with full disk backups to simplify recovery and achieve higher de-duplication ratios. Even though recovery was automated with RMAN, there was overhead in applying incremental changed data to the full copy. As such, given the cost reduction afforded by PBBAs, many practitioners choose to simply take a full backup daily.

PBBAs were highly beneficial and delivered significant ROI in the early days by simplifying backup and relegating tape to an archive medium. By storing data on disk, restores were simpler and faster, and this approach was often viewed as more attractive than primary disk-based snapshots.

Practitioners however began to realize there were two main problems with PBBAs including:

1. Once the one-time benefit of data reduction was achieved, the ongoing [return on asset \(ROA\)](#) utilization was offset by the need to purchase more PBBAs – for both new growth and off-site replication. Typically, PBBAs have a fixed unit of scale up capacity and performance and once limits are hit, new systems must be purchased to accommodate growth. “PBBA Creep” started to catch the attention of CFOs who thought this was primarily a one-time capital investment;
2. Wikibon users reported that sometimes, PBBAs couldn't deliver their desired de-dupe ratios on Oracle databases because the ordering of blocks could change in the backup making it difficult to identify duplicates. PBBA vendors began to recommend that users perform full backups where higher de-dupe rates could be achieved.

The Time Machine for the Enterprise

Prior to the acquisition of Sun Microsystems, which was completed in early 2010, Oracle was exclusively a software company and as such focused on providing software infrastructure products for tasks such as backup, rather than specialized hardware. Oracle's strategy was to partner with backup software providers such as Symantec, EMC, NetApp, HP and others who specialized in tape backup or other storage products. Notably, Oracle continues to maintain partnerships with such companies today, however they also compete directly with these suppliers.

Last fall at Oracle OpenWorld and again in January of 2015, Oracle showcased a new lineup of roughly ten appliances, ranging from Exa- systems, a flash storage systems, a Big Data Appliance and a new Super Cluster system. Also positioned in this portfolio was the Oracle Zero Data Loss Recovery Appliance (ZDLRA). The appliance is an integrated data protection system designed for database recovery to address some of the challenges described above with traditional backup approaches.

The ZDLRA is being positioned by Oracle as a direct competitor to third party solutions such as purpose-built data deduplication appliances.

To summarize and add color to the discussion above, DBAs and Oracle admins today struggle with the following:

- Massive data growth
- Exposure to data loss and/or corrupted backup data
- Unreliable backups and a lack of recovery visibility
- Complexity of managing fragmented backup silo's
- Challenges to meet tighter backup windows
- Backup overhead impacting application performance

For years, Wikibon practitioners have been saying that traditional methods of backup using a “one-size-fits-all” approach are inadequate for protecting the myriad database-based applications that have wide-ranging RPO and RTO requirements. As Oracle customers in the Wikibon community move toward database-as-a-service models (DBaaS), they have begun to re-think backup and recovery. Specifically, they are moving toward a [data-protection-as-a-service model](#) consistent with DBaaS and cloud.

Oracle Zero Data Loss Recovery Appliance

As mentioned previously, Oracle's practice prior to the Sun acquisition was to partner with hardware companies to develop more integrated solutions. Indeed the first instantiations of Exadata combined Oracle software with HP server technology. These early Exadata systems were replaced by what Oracle calls “Engineered Systems,” an integrated, fault tolerant system that uses Oracle software, servers, storage and networking.

Oracle's R&D strategy is to leverage the “Red Stack” across its entire hardware and software portfolio. As such it has repurposed the Exadata platform along with new software capabilities to launch an Engineered System specifically designed for Oracle database backup and recovery. ZDLRA is an integrated system that centralizes Oracle database data protection across the Oracle portfolio.

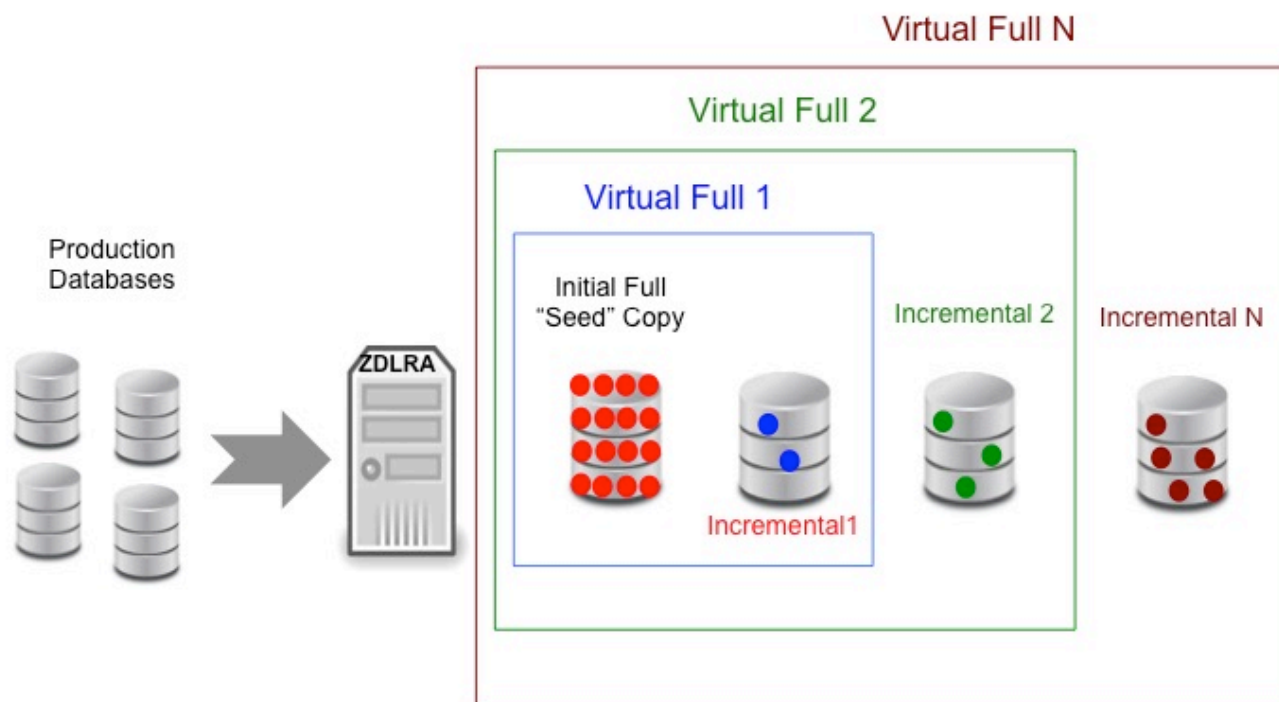
Oracle positions Recovery Appliance as having the following capabilities:

- Creating an environment where data is not lost
- Providing end-to-end status visibility on all protected databases providing assurances that data can be recovered
- Removing current backup overheads and windows with the goal of accelerating database performance
- Allowing DBAs to define granular classes of service for different data based on value of information
- Fully automating the end-to-end data protection process including offsite replicas and tape archives

Practitioners should note that even with ZDLRA (and other methods touting zero data loss), the possibility of data loss is minimized but still exists. For example, if a catastrophic disaster occurs before data is shipped off-site to a distance protected from the local disaster, data could be lost. While there really is no such thing as zero data loss, in our view, the ZDLRA gets closer to “RPO Zero” than any other solution we've seen that was specifically designed for Oracle.

Oracle's recovery appliance uses the concept of incremental forever backups (see Figure 3). In this approach, an initial “seed copy” of the production database is created. Once that process takes place, future backups only capture changed blocks from the database at variable time intervals set by the Oracle admin as well as continuous logging of transactions. Oracle refers to this process as “Delta Push” which includes RMAN incremental backups plus real-time redo log transport. Other than the first full backup, no other fulls are required which eliminates the concept of a backup window as we know it.

Figure 2: Oracle Recovery Appliance (ZDLRA) Incremental Forever Concept – Source Wikibon and Oracle Technical Documentation



ZDLRA indexes all backups creating a pointer-based representation that stores the corresponding metadata within its catalog. During restore, the appliance constructs a virtual full backup to the point of the incremental which is then sent to the database server along with any necessary archived log backups for point-in-time recovery. The virtual full restore capacity gives users the same level of service as if a daily full backup had been performed, without the overhead or performance impacts.

Specifically, unlike conventional incremental approaches, which have to restore and apply/merge the string of incrementals to create a consistent copy of the database (automated but overhead-intensive), the ZDLRA, assembles a full virtual copy so only archived log backups need be applied for point-in-time recovery on the database server. This allows the database to be up and running much more quickly.

With real-time redo transport enabled, RPO is reduced from hours/days (time since last backup) to sub-seconds. Essentially this creates a time stamp for each written block, which creates a “time machine” for backup and recovery. Note: This feature is only available for 11g and 12c database versions.

By reducing complexity in the backup infrastructure Oracle is advocating a standardized, incremental forever backup strategy, which at the same time can be tailored to different needs of protected databases. Oracle advises its customers to create a protection policy on the appliance for each tier of database, (e.g. mission, business-critical, etc.), logically consolidating systems which have the same recovery SLAs. Databases can then be managed as a group for recovery settings, replication, scheduling copy to tape archive, alerting thresholds and other repeatable tasks.

Discussions with Oracle product executives confirm that name “Recovery Appliance” was chosen to emphasize that the appliance was designed for recovery and not just retention of flat files. To this end the ZDLRA provides real-time recovery status for all databases in the form of current recovery window (i.e. the amount of time that has lapsed since the last point-in-

time recovery) and current unprotected data window (data loss exposure) for visibility into the full recovery spectrum. NOTE: If real-time redo transport is enabled, the data loss exposure will be sub-second and if not then the time since the last backup will determine the data loss exposure.

Storage is managed by the appliance with out-of-the box alerting, monitoring and reporting on usage by database and for the appliance as a whole. Capacity management is another “feature” of its recovery focused design. Storage is dynamically allocated to best meet the user-defined recovery windows (set in the protection policy) for all databases which in effect allows Oracle admins to manage space based on business requirements rather than arbitrary storage quotas.

The appliance scales to usable capacity of 580TB in a single rack and 10+PB fully racked (18 racks in a single appliance configuration). Wikibon has not evaluated benchmarks however Oracle claims performance scales linearly with each additional rack providing 12TB/hr of backup and restore. Oracle highlights restore performance as being about on par with backup rates.

On balance, the ZDLRA represents the most integrated, end-to-end backup and recovery system designed specifically for Oracle database that we’ve seen to date. Oracle has taken a different approach than that of other appliances by focusing on recovery with an attempt to automate the backup process and eliminate the guesswork out of whether backups can be both restored and recovered. Database data-protection-as-a-service seemingly extends Oracle’s database as a service model to data protection and effectively simplifies backup and restore management Oracle databases at scale.

Wikibon users should note that we have not validated Oracle’s claims with ZDLRA customers, as the product is relatively new but we have asked Oracle to provide references so that we can conduct in-depth interviews.

Gotchas

Oracle aggressively markets its advantage over competitors, specifically citing integration capabilities that are unique to Oracle. While true, practitioners should weigh the degree to which they can leverage these benefits and assess the ability of competitors to simulate Oracle’s capabilities through RMAN integration and developing similar features within their own storage systems. Regardless, for the heavy Oracle user it’s hard to argue that Oracle products are not more tightly integrated than competitive alternatives— they clearly are as such.

The drawbacks of ZDLRA are similar to those we’ve noted with other Oracle appliances. The benefits of end-to-end integration are significant but narrow in their value proposition as they are designed specifically for Oracle environments. While Oracle hints at supporting other platforms and has provided hooks to VMware as an example, Oracle almost exclusively targets its own base of database and application customers with optimized storage offerings. As a result, this limits what we refer to as Return on Asset leverage – i.e. the ability to utilize infrastructure to support a wider application portfolio running on heterogeneous platforms; meaning Oracle hardware tends to be less a fungible asset.

Action Item:

The enterprise technology industry is changing dramatically as seen by the ascendancy of Amazon Web Services and the recently announced Dell acquisition of EMC. IT organizations must begin to place bets for the future to become more cloud-like within their own IT operations, meaning more agile and focused on creating value closer to the business. From a backup perspective, this means moving toward data-protection-as-a-service where granular backups can support very fast restore times and extremely low RPOs (close to RPO Zero). In our view, Oracle intends to apply its Exadata playbook to backup and do in backup what it has done with Exadata for critical production databases. For serious Oracle database customers, the Oracle Zero Data Loss Appliance appears to re-define best practice in data protection and warrants earnest evaluation by Oracle DBAs and admins.

LEGAL

© 2007 - 2015 SiliconANGLE Media, Inc. All rights reserved.

This document and its contents is restricted for the private use of Wikibon Premium Members.

External use without written permission is forbidden.
