Zero Data Loss Recovery Appliance

ORACLE WHITE PAPER | SEPTEMBER 2019

Table of Contents

Introduction

Oracle's Zero Data Loss Recovery Appliance is a new cloud-scale engineered system designed to dramatically eliminate data loss and reduce data protection overhead for all Oracle databases in the enterprise. Integrated with Recovery Manager (RMAN), it enables a centralized, incremental forever backup strategy for hundreds to thousands of databases in the enterprise, using cloud-scale, fully fault-tolerant hardware and storage. The appliance provides databases with sub-second recovery point objectives and continuously validates backups for assured recoverability of Oracle data. Oracle Enterprise Manager enables "single pane of glass" control of all administrative operations on the appliance, providing complete, end-to-end visibility of the Oracle backup lifecycle.

This paper explores the key data protection capabilities and benefits that the appliance brings to Oracle Database environments.

The Vital Role of Business Data Protection

Information technology's role in the modern business is going through a tremendous transformation. Companies are witnessing exponential growth in the amount of data they need to run their operations and at the same time, are increasingly dependent on this data to make critical decisions in real time. They operate more and more in a 24x7 global economy, and as such, any prolonged downtime or slowdown is simply not acceptable for critical systems. Given all these factors, it is more important than ever that a company's IT organization operate a scalable, robust, and non-intrusive data protection strategy that meets all the service level agreements required by the business units. Any data loss, however great or small, is simply not acceptable for today's business critical systems and applications.

Data Protection Challenges

Data protection solutions today largely focus on storage-based mirroring and backup & recovery technologies, with each having their own shortcomings, especially when it comes to protecting databases. These generic solutions treat databases as filesystem data, without an appreciation of the transactional nature of the underlying data.

When it comes to Oracle database backups, the primary questions are: how do I effectively backup my database environments, within ever shrinking backup windows, while at the same time, ensure that recoveries can be done seamlessly with as little data loss as possible? The wide array of backup and recovery technologies in today's market, from both software and hardware approaches, only compounds this challenge in large enterprises with hundreds to thousands of databases.

Let's take a look at a few of today's approaches to database backup and recovery, as shown below.

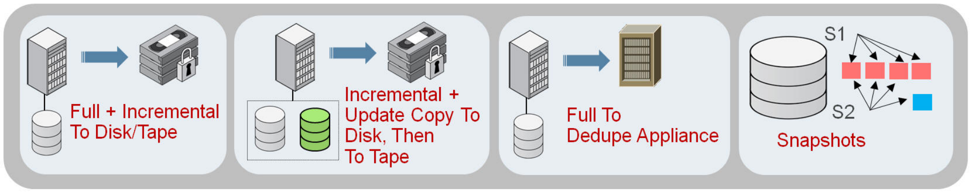

Full + Incremental To Disk/Tape
Incremental + Update Copy To Disk, Then To Tape
Full To Dedupe Appliance
S1
S2
Snapshots

Figure 1: Database Backup and Recovery Approaches

Weekly Full with Daily Incremental

This strategy involves weekly full (level 0) and daily incremental (level 1) backups to disk and/or tape. This means businesses incur the overhead of full backups every week – leading to the notion of “backup windows”, when systems are too stretched to support all production applications at normal performance levels. With archived logs also backed up as part of this strategy, recovery is possible to any point-in-time between the full backup timestamp and last good archived log backup. However, a significant amount of disk and/or tape storage is needed to hold the required number of full and incremental backups.

Incrementally Updated Backups

In this strategy, an initial image copy (level 0) is taken to disk, followed by daily incremental backups. The image copy is then rolled forward by applying incrementals to produce a new on-disk copy that corresponds to the most recent or a previous incremental timestamp. Once a copy is rolled forward, it cannot be rolled back – unless the copies are first archived or storage-based snapshots are taken. Image copies consume the same amount of disk storage as the production data files and thus, can significantly increase overall storage needs, especially for large databases.

Daily Full to Deduplication Appliances

In recent years, backups to deduplication appliances have become more prevalent, with the goal to drive down storage costs through automatic elimination of redundant backup data. In order to drive *down* storage costs, deduplication (i.e. savings) ratios must be driven *up* – thus, storage vendors generally recommend a full backup-only strategy to these appliances. However, for most enterprise databases, a full backup-only strategy is neither effective from a backup window nor system utilization perspective. In addition, restoring a deduplicated backup requires the physical backup to be first rehydrated, which can prolong restore times.

Deduplication appliances are typically based on a single controller architecture, in which the compute power and bandwidth is fixed in a given appliance and cannot be altered per business needs. The user can add additional storage expansion shelves, but they only increase the total storage capacity managed by the system. Once the maximum storage limit is reached in a single appliance, the user has to do a fork lift upgrade to the next higher model or must buy additional appliances. The same fork lift upgrade applies if the user needs additional backup processing throughput. Net-net: due to the physical limits for scaling up throughput on a single system, supporting backups of large Oracle enterprises (e.g. hundreds-thousands of databases) is near-impossible to do with a small number of appliances.

Finally, single controller architecture systems severely limit the resilience of the system. Any single component failure in the controller can render the appliance unusable until the component is replaced.

Storage Snapshots

Storage-based snapshots of production databases are another ‘backup’ strategy where only new and changed data is stored. With this technology, a file snapshot is just a set of pointers to all the unchanged and before-change blocks that make up the file, as of the snapshot time. Since a snapshot is tied with the production storage, it cannot serve as a true backup[1] in event of storage corruption, loss, or site disaster – however, it can be used to quickly

[1] “Snapshots are NOT Backups”, http://www.oracle.com/technetwork/database/features/availability/rman-fra-snapshot-322251.html

create a clone database for dev/QA purposes. Since snapshots are created outside of RMAN, they are not validated for Oracle block correctness, until they are restored and the database is opened.

In summary, several shortcomings come to the fore with today's data protection technologies:

- **Increased Data Loss Exposure**: Data can only be recovered to the last good backup, e.g. hours or days ago. In addition, generic storage systems cannot inherently validate backups at an Oracle block-level for restore consistency.
- **Prolonged Backup Windows**: As databases continue to grow, so do backup windows and that can result in network and storage resources being tied up longer and more frequently, resulting in much less efficient utilization of overall IT resources.
- **Reduced Production Performance**: Longer backup windows means longer impact on production performance, stealing cycles and resources away from more critical production workloads.
- **Fragmented Backup Processes**: Deduplication and storage appliances treat Oracle backups as just generic files, with no connection back to the databases they comprise, leading to lack of visibility and assurance that the backup is healthy and usable, whether it is on disk, tape, or a replica appliance.
- **Reduced Operational Scalability**: Storage appliances cannot easily scale to handle massive backup workloads and concurrent connections from hundreds to thousands of databases across the enterprise.

Simply stated - none of these methods provides a truly comprehensive and efficient Oracle-integrated data protection solution that meets the demands of a large-scale, enterprise Oracle environment. What is needed is a completely new solution architected from the ground-up for transactional data protection of hundreds to thousands of Oracle databases.

Zero Data Loss Recovery Appliance

The Zero Data Loss Recovery Appliance is designed to dramatically eliminate data loss and reduce data protection overhead for all Oracle databases in the enterprise. Backup processing is offloaded to the appliance, boosting production performance, while data loss exposure is minimized via real-time redo transport. Oracle Enterprise Manager Cloud Control oversees administration and control of the entire environment, providing "single pane of glass" view of the entire backup lifecycle for each database, whether backups reside on disk, tape, or a replica appliance. The integrated hardware for the appliance, based on the industry-proven Exadata platform, is fully fault-tolerant, offers extremely high performance and scales easily to accommodate the data growth needs of the enterprise.

The key components and workflow within the environment are shown below:

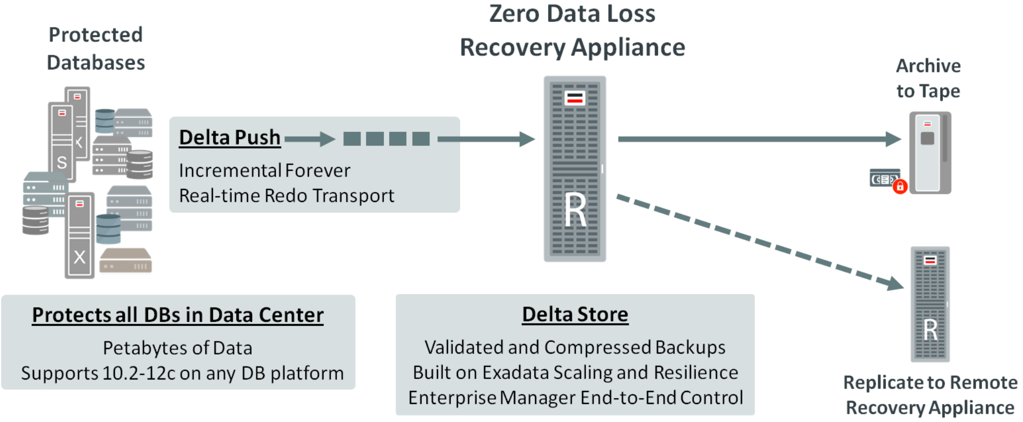

Protected Databases
Zero Data Loss Recovery Appliance
Archive to Tape
Delta Push
Incremental Forever
Real-time Redo Transport
Protects all DBs in Data Center
Petabytes of Data
Supports 10.2-12c on any DB platform
Delta Store
Validated and Compressed Backups
Built on Exadata Scaling and Resilience
Enterprise Manager End-to-End Control
Replicate to Remote Recovery Appliance

Figure 2: Zero Data Loss Recovery Appliance Environment

Recovery Appliance Technology

Architecture

The appliance is natively integrated with Recovery Manager (RMAN) - at the heart of the system is an embedded Oracle Database, running Oracle Real Application Clusters (RAC), that serves as the centralized RMAN Recovery Catalog for all the protected databases. The catalog maintains all backup metadata in Automatic Storage Management (ASM) disk groups running on High Capacity disks in high redundancy mode. The backup data itself is also kept in ASM disk groups, in normal redundancy. The appliance can expand in compute and storage capacity by simply adding additional racks. Backup connectivity into and out of the system is provided through standard 10/25 GigE or InfiniBand ports. For tape archival operations, the appliance comes with pre-installed Oracle Secure Backup (OSB) media management software and a 16 Gb Fibre Channel Card on each compute server to connect directly to tape hardware. Alternatively, other vendors' tape backup agents may be deployed on Recovery Appliance for integration with existing tape backup software and processes. In this configuration, the agents must connect to their specialized media servers that are deployed external to the appliance.

Protected Databases

Databases supported with Recovery Appliance can range from Oracle Database 10g Release 2 through Oracle Database 12c, on any Oracle supported OS platform. A database is made "Recovery Appliance-aware" via installation of the Recovery Appliance Backup Module that integrates with RMAN. No specialized backup agents are required, and if any such agent is currently used for Oracle Database backup purpose, it can be removed. More details on how protected databases are configured for the Recovery Appliance can be found in the section "Protection Policies".

The Recovery Appliance Backup Module allows RMAN SBT channels to be configured to backup/restore data via standard HTTP to/from the Recovery Appliance, as shown below:

```
CONFIGURE CHANNEL DEVICE TYPE SBT PARMS
‘SBT_LIBRARY=/u01/app/oracle/product/12.1.0.0.0/dbhome_1/lib/libra.so,
ENV=(RA_WALLET='location=file:/u01/app/oracle/product/12.1.0.0.0/
dbhome_1/dbs/ba
credential_alias=recoveryappliance2-ingest.company.com:1521/Recovery
Appliance2:dedicated')’
```

Figure 3: RMAN SBT Channel Configuration to Recovery Appliance

In this example, the backup module 'libra.so' allows SBT channels to connect over HTTP to Recovery Appliance 'recoveryappliance2' via the access point 'recoveryappliance2-ingest.company.com' using credentials stored in the Oracle wallet "RA_WALLET".

We will now discuss two unique architectural components of Recovery Appliance - *Delta Push* and *Delta Store*.

Delta Push

Delta Push consists of two processes that are run on each protected database: (i) RMAN incremental backups and (ii) real-time redo transport.

RMAN Incremental Backups

In normal operation, the Recovery Appliance receives regularly scheduled RMAN incremental level 1 backups from each protected database, which consist of just the data file block changes relative to the previous incremental that was taken. At the Recovery Appliance, the incoming backup data is validated to ensure that there are no physical corruptions in the Oracle data blocks, then compressed using specialized block-level algorithms, and finally written to a storage pool contained within one or more pre-configured ASM disk groups.

No regular full backups are needed from the protected database, apart from the initial full. Thus, Recovery Appliance implements an *incremental forever* backup strategy, eliminating traditional backup windows and the associated system impact, while boosting production server performance. More details are discussed in the section “Delta Store”.

Real-time Redo Transport

If the production system and storage are lost, then fundamentally, data can only be recovered to the point-in-time of the last good backup and more specifically for databases, to the last good archived log backup. Since archived logs hold records of all changes that occur in the database, these critical files must be backed up regularly, if not more frequently (e.g. every few hours for active systems) than data files. Frequent backups reduce the potential data loss that is incurred, if the production system is indeed lost and backups need to be recovered. In fact, if a backup is not yet taken after a data file is created and the data file is corrupted or lost, the archived logs on their own can be used to recreate the data file from scratch, during the process of media recovery.

In recognizing the critical nature of redo as it pertains to data loss, Recovery Appliance supports real-time redo transport with Oracle Database 11g and 12c, the first-of-its-kind in the industry to do so, providing data loss protection in the order of sub-seconds. Based on the industry-proven Oracle Data Guard redo transport technology, Recovery Appliance receives incoming redo blocks directly from the memory (SGA) of these protected databases, and writes the logs into a redo staging location (pre-configured ASM disk group), from where they are converted into compressed archived log backups and then written to the delta store. This means frequent, resource-intensive archived log backups are no longer required on the production systems, as in a typical backup strategy. Archived log backups generated by the appliance are recorded in the recovery catalog as normal and can be restored and applied to data files via standard RMAN RECOVER commands.

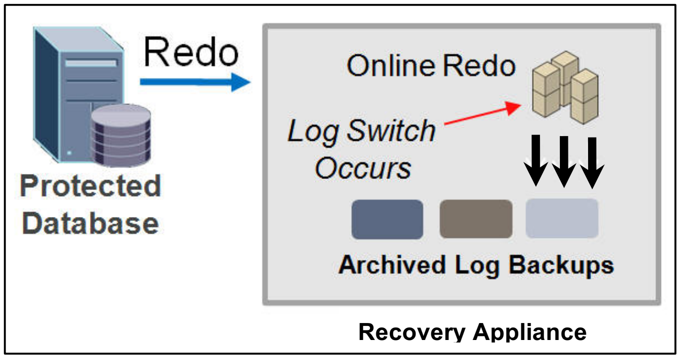


Figure 4: Recovery Appliance Real-Time Redo Transport

If there is an unexpected termination in the redo stream, the appliance has the ability to close the incoming redo stream and create a *partial archived redo log*, thereby preserving data loss protection. Upon detecting that the redo stream has restarted, the appliance automatically retrieves all missing archived logs from the protected database to preserve the recovery window goal.

Delta Store

The Delta Store is the key processing engine for Recovery Appliance, creating and storing *virtual full backups*, based on the Delta Push incremental backups. Delta Store technology converts an incoming incremental level 1 backup into a virtual representation of an incremental level 0 (i.e. full) backup, as of the level 1's point-in-time. For example, an incremental level 1 backup **Day1_Incr** as of time **Day1** is converted into a virtual full backup **Day1_VB**, which is simply a set of metadata maintained in the recovery catalog with references to the data file blocks from the incremental backup **Day1_Incr** and to blocks from previous incremental backups, going all the way back to the initial incremental level 0 backup. In effect, the blocks referenced by the virtual full make up the physical full backup set that can be restored to the point-in-time **Day1**. Thus, Delta Store enables Recovery Appliance to create a "full backup" at the *cost* of only an incremental, consuming a fraction of the time and storage consumption of a standard full backup operation, as shown below.

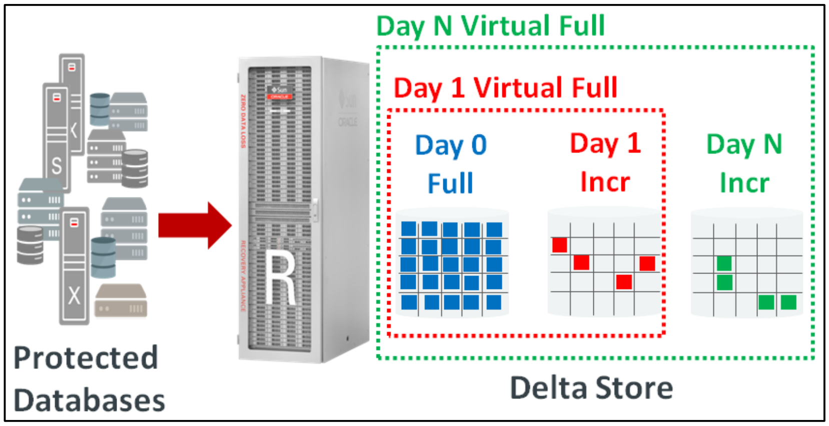


Figure 5: Delta Store Virtual Full Backups

Since the protected database uses familiar RMAN BACKUP commands, all virtual full backups show up as normal incremental level 0 backups in the recovery catalog, and can be used by future RMAN restore operations as needed. When a protected database issues an RMAN RESTORE, the Recovery Appliance responds by reading the appropriate virtual full backup blocks, constructing the physical full backup sets, and then sending the backup sets to the database, where they are restored. The figure below illustrates how a physical full backup set at Day 'N' is created from its virtual full backup, which references blocks from Day 1, 2, and 'N' incremental backups.

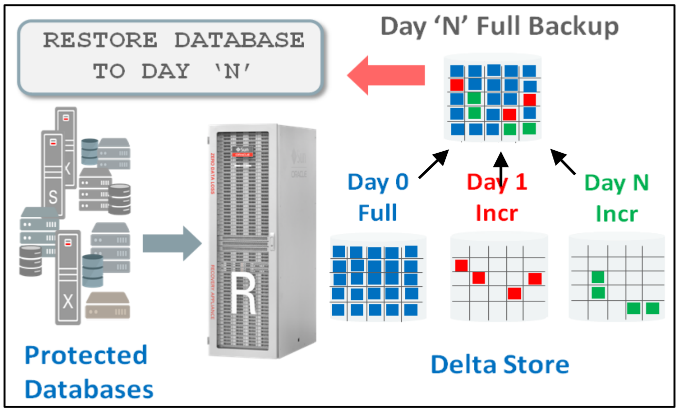


Figure 6: Day 'N' Virtual Full Restore

Net-net, the notion of virtual full backups is completely transparent to RMAN and the protected database – DBAs continue to utilize their existing RMAN skill set with Recovery Appliance.

Replication

The RMAN transparency model also holds when replicating a local Recovery Appliance's backups to a secondary Recovery Appliance, for protection against server or site outage. After an incremental backup is received by the local Recovery Appliance, it is automatically queued for forwarding to a secondary Recovery Appliance, i.e. just the changed blocks are replicated, not full backups. When the incremental is received at the replica Recovery Appliance, a virtual full is created on the system as normal, with new backup records created in its own recovery catalog and propagated back to the local Recovery Appliance's catalog.

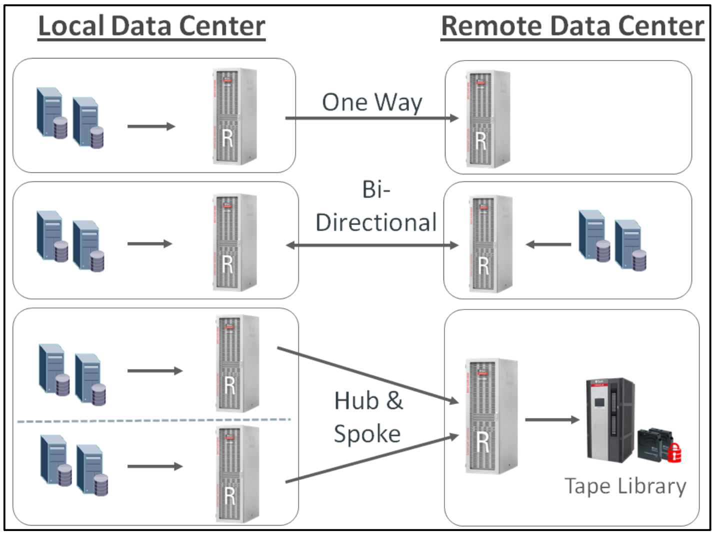


Figure 7: Recovery Appliance Replication Models

Since records of the replicated backups in the secondary Recovery Appliance are also maintained in the local Recovery Appliance, any virtual full backup requests that cannot be satisfied by the local Recovery Appliance are automatically forwarded to the replica Recovery Appliance, where the physical backup sets are constructed as normal and sent back to the protected database. Again, DBAs continue to utilize RMAN as normal, without needing to understand where or how the backup sets originated.

Autonomous Tape Archival

In contrast to disk-only backup systems, Recovery Appliance is an excellent fit in the IT organizations that have continued to rely on tapes for long-term retention and archival purposes. As previously discussed, the Recovery Appliance comes with pre-installed Oracle Secure Backup software and a 16 Gb Fibre Channel Card on each compute server to connect directly to tape hardware. When the Recovery Appliance executes a copy-to-tape job for a virtual full, the physical backup sets are first constructed, then pushed to tape via a built-in SBT interface. Once the tape backups complete, the appropriate backup metadata is written to the recovery catalog. All tape copy operations are performed by the Recovery Appliance with *zero* impact on the production system.

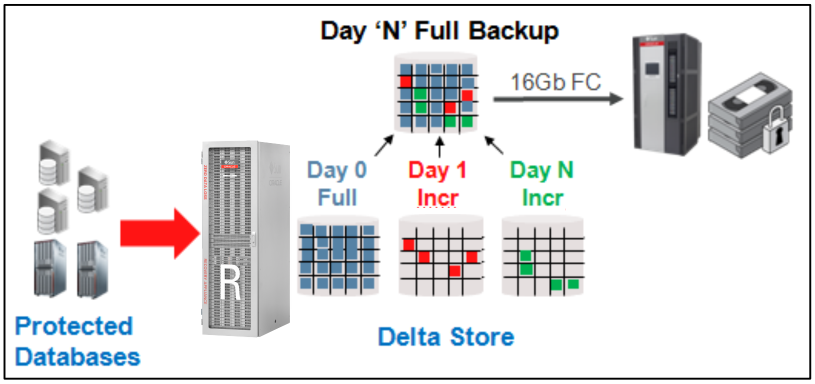


Figure 8: Copy Virtual Full Backup Day 'N' to Tape

A RESTORE request that requires backups from tape is automatically retrieved by the Recovery Appliance – no action is needed by the DBA. Furthermore, since the backups on tape are physical backup sets, these backups can be restored *directly* by the protected databases if needed. The protected database simply needs to be configured with the SBT plug-in module that is included with the Oracle Secure Backup installation, and then SBT channels are allocated as normal to perform the restore operations directly from tape.

Recovery Appliance Operations

Now, let's discuss how the appliance operates, including the role of protection policies and space management aspects of the Delta Store, which are configured and monitored using Enterprise Manager Cloud Control.

Protection Policy

Recovery Appliance introduces the concept of a *protection policy*, which defines granular recovery window goals that are enforced on a per database basis for backups on the local or replica Recovery Appliance and/or tape. Using protection policies, databases can be easily grouped by recovery service tier, e.g. "Gold" tier databases require backups kept for 35 day recovery window goal on the local Recovery Appliance and 90 days on tape, while "Silver" tier databases only require 10 days on the local Recovery Appliance and 45 days on tape. An optional *maximum disk retention* (e.g. in days, weeks, or months) can be defined within a policy, to hard limit the amount of space consumed by the policy's databases. Separate protection policies can also be setup at the replica Recovery Appliance, which will govern the space management of the replicated backups.

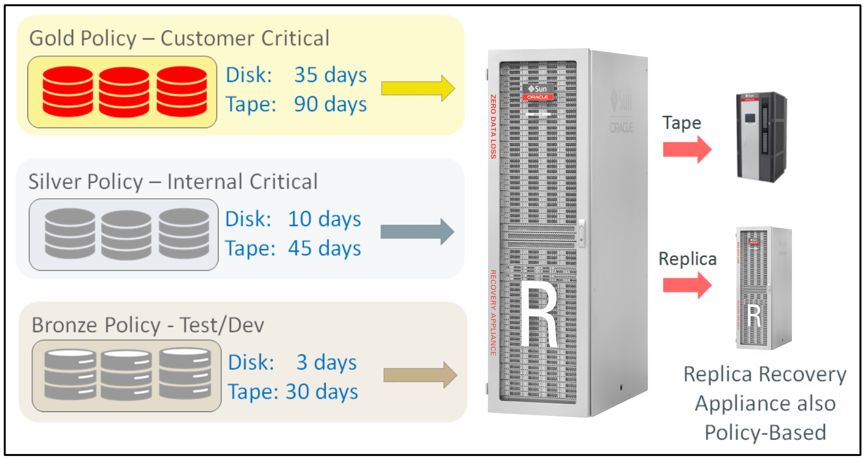


Figure 9: Recovery Appliance – Database Protection as a Service

With this unique implementation, Recovery Appliance introduces the concept of *Database Protection as a Service* through which database protection strategies can easily be implemented based on the criticality of the business application, rather than simply on the availability of storage space.

Space Management & Recovery Windows

Once a protection policy is created, a database can then be assigned to it, along with a minimum *space reservation* (e.g. in GB or TB) that is used by the Recovery Appliance to provision backup space per the defined recovery window goals. The database space reservation defines the minimum amount of space that is always available for use by the database's backups. Space is provisioned by first using any free space and if needed, by purging *obsolete virtual full backups* (i.e. backups no longer needed to meet a database's recovery window goal).

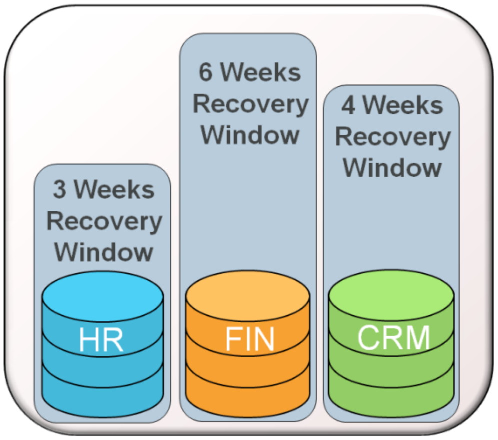


Figure 10: Protection Policy-based Space Management

For example, if the HR database requires 1 TB space today to support a 3 week recovery window, and its backup space needs increase to 2 TB tomorrow due to higher workloads, then the storage location will attempt to meet the additional 1 TB space need by utilizing any available free space and if necessary, by purging obsolete virtual full backups and their corresponding archived log backups associated with other databases (e.g. FIN, CRM). Conversely, after the workloads on HR subside, and it once again requires just 1 TB space to support a 3 week recovery window, then any of its *obsolete virtual full backups* may be purged by the Recovery Appliance, if other databases need additional space to meet their respective recovery window goals. Backups may also be *proactively* purged as needed, in anticipation of future space needs – this 'predictive purging' background process is based on historical space usage patterns.

In the event that all obsolete backups have been purged and certain databases still require additional space to meet their recovery window, then the storage location will begin purging the oldest virtual full backups for each database that is consuming more than its minimum space reservation, prioritized in order of databases with the highest percentage of space overage. Note that in some cases, this action can compromise a database's recovery window goal. If this occurs, the system can alert the administrator that additional capacity is needed in order to maintain the stated recovery windows. The administrator can then take action to add disk capacity and increase space reservation to allow the system to return to a balanced state, where all recovery windows can be satisfied.

In summary, Recovery Appliance fully manages all backup space in order to meet each database's recovery window goal, automatically re-provisioning space as needed and proactively purging backups in advance of future space needs.

Backup Validation

One of the basic principles of a well-rounded backup and recovery strategy is to ensure that the backups created can actually be restored and used successfully. To ensure that there are no physical corruptions within the backed up data blocks and that they can be properly restored, backups must be validated on a regular basis. This typically means running an RMAN `RESTORE VALIDATE` job regularly, along with running periodic full restore and recovery operations to a separate machine. All of these add overhead to an already taxed production system. With Recovery Appliance, incoming backups are automatically validated in-line for Oracle block correctness. Similarly, backups that are replicated to a secondary Recovery Appliance and/or copied to tape are also validated. Furthermore, virtual full backups themselves are periodically validated in-place by a background task running on the appliance. Another benefit is that backup validation operations are now *offloaded* from the production system to Recovery Appliance, thus improving production system performance. Finally, since ASM is used for storing the backup data on the appliance, it is also made fully redundant through ASM mirrored copies, where corrupted blocks discovered by ASM on the primary disk can be automatically repaired by a mirrored copy.

Restore and Recovery

Database restore and recovery operations using RMAN are executed in the same fashion with Recovery Appliance, as with any other backup destination. In the most basic form, the commands are simply:

```
RESTORE DATABASE;

RECOVER DATABASE;
```

When `RESTORE` is issued on a protected database, the RMAN client consults the Recovery Appliance catalog to determine the most appropriate incremental level 0 backup (virtual full) to restore, based on the point-in-time desired. The virtual full backups are then requested via the configured SBT channels for Recovery Appliance. The appliance receives the request, constructs the physical backup sets from the appropriate virtual full blocks in the Delta Store, and sends the backup sets to the RMAN client via the same SBT channels. On the RMAN client side, the backup sets are received and validated, and the data file blocks are restored to the production storage location.

When `RECOVERY` is issued, the RMAN client consults the Recovery Appliance catalog to determine the appropriate archived log backups to request in order to recover the restored data files to the point-in-time desired and allow the database to be opened. If redo transport has been enabled, the most current archived logs, including any partial archived logs, will be available from the Recovery Appliance. Thus, the database can be recovered with the most current version of data, as shown below.

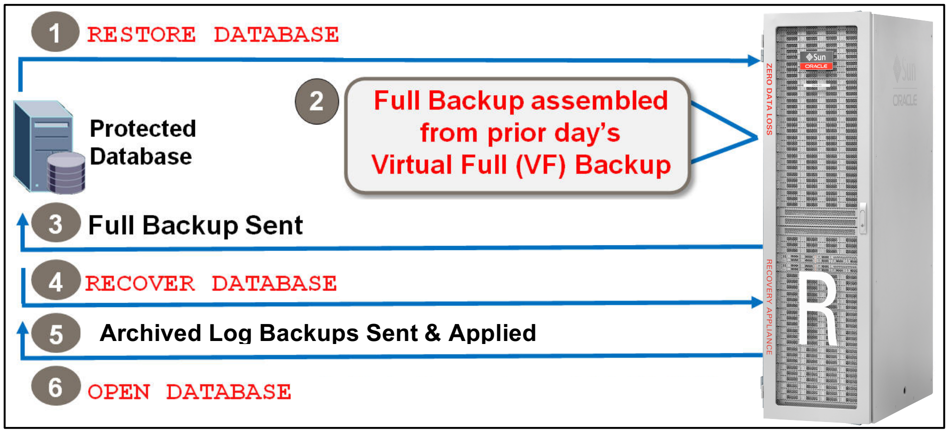


Figure 11: Protected Database Restore & Recovery Procedure

Monitoring & Administration

Oracle Enterprise Manager Cloud Control provides a complete, end-to-end view into the backup lifecycle managed by the Recovery Appliance, from the time the RMAN backup is initiated on the database, to when it is stored on disk, tape, and/or replicated to a secondary appliance. All appliance monitoring and administration functions are enabled via installation of the Enterprise Manager Recovery Appliance plug-in.

Standard metrics such as overall backup volume/performance and aggregate/per-database space consumption are easily accessed from the console.

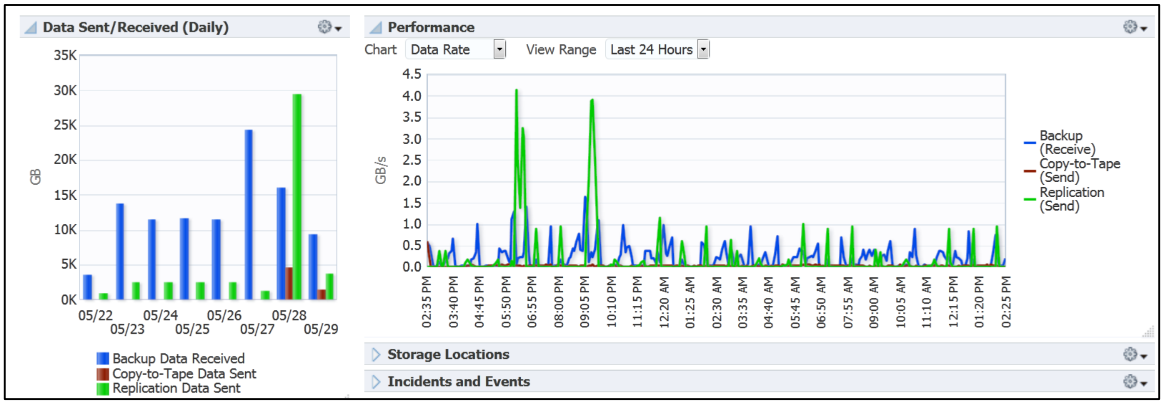
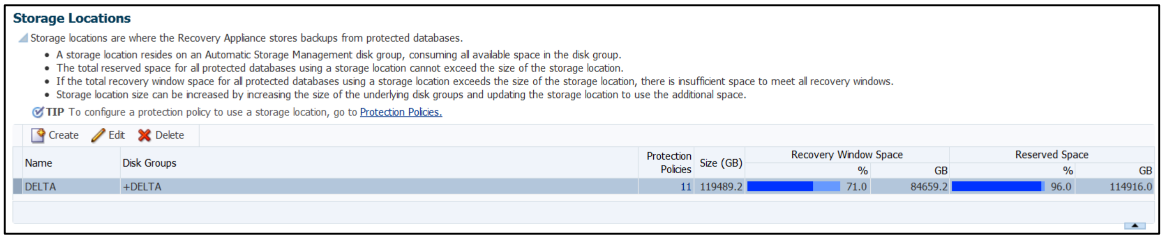


Figure 12: Recovery Appliance Enterprise Manager Home – Overall Performance and Storage Metrics



Storage Locations

Storage locations are where the Recovery Appliance stores backups from protected databases.

- A storage location resides on an Automatic Storage Management disk group, consuming all available space in the disk group.
- The total reserved space for all protected databases using a storage location cannot exceed the size of the storage location.
- If the total recovery window space for all protected databases using a storage location exceeds the size of the storage location, there is insufficient space to meet all recovery windows.
- Storage location size can be increased by increasing the size of the underlying disk groups and updating the storage location to use the additional space.

TIP To configure a protection policy to use a storage location, go to Protection Policies.

Name	Disk Groups	Protection Policies	Size (GB)	Recovery Window Space		Reserved Space	
				%	GB	%	GB
DELTA	+DELTA	11	119489.2	71.0	84659.2	96.0	114916.0

Figure 13: Storage Location – Total Size, Recovery Window Space, Reserved Space

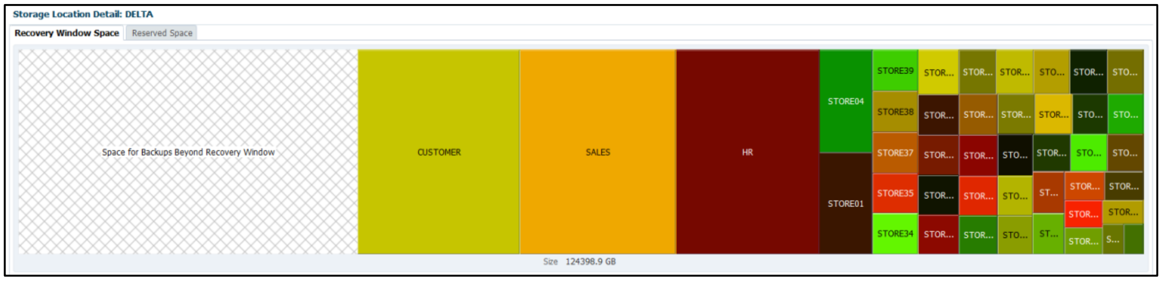
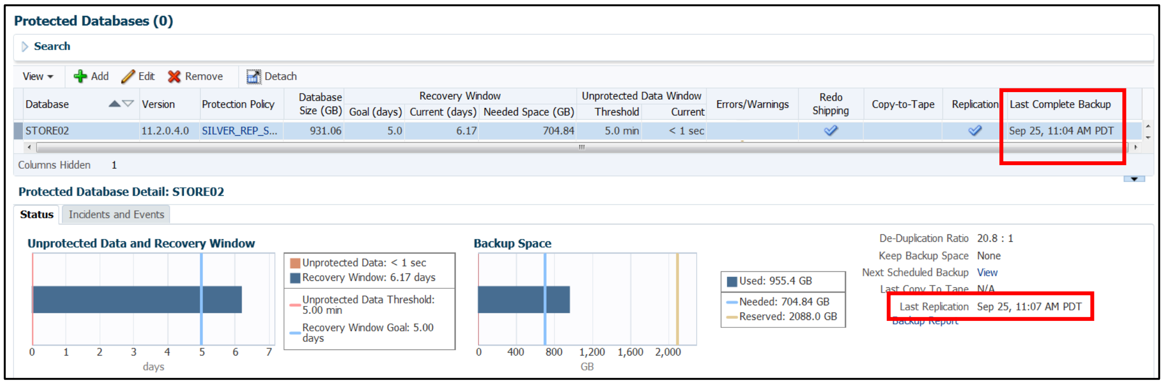


Figure 14: Storage Location Detail – Per-Database Backup Space Needed to Meet Recovery Window Goal

End-to-end monitoring of the entire database backup lifecycle can be done through a single console, e.g. time of last completed backup to the appliance, time of last copy to tape and replication, and next scheduled backup to the appliance.



Protected Databases (0)

Search

View ▾ Add Edit Remove Detach

Database	Version	Protection Policy	Database Size (GB)	Recovery Window			Unprotected Data Window		Errors/Warnings	Redo Shipping	Copy-to-Tape	Replication	Last Complete Backup
				Goal (days)	Current (days)	Needed Space (GB)	Threshold	Current					
STORE02	11.2.0.4.0	SILVER_REP_S...	931.06	5.0	6.17	704.84	5.0 min	< 1 sec		✓		✓	Sep 25, 11:04 AM PDT

Columns Hidden 1

Protected Database Detail: STORE02

Status | Incidents and Events

Unprotected Data and Recovery Window

Unprotected Data: < 1 sec
Recovery Window: 6.17 days
Unprotected Data Threshold: 5.00 min
Recovery Window Goal: 5.00 days

Backup Space

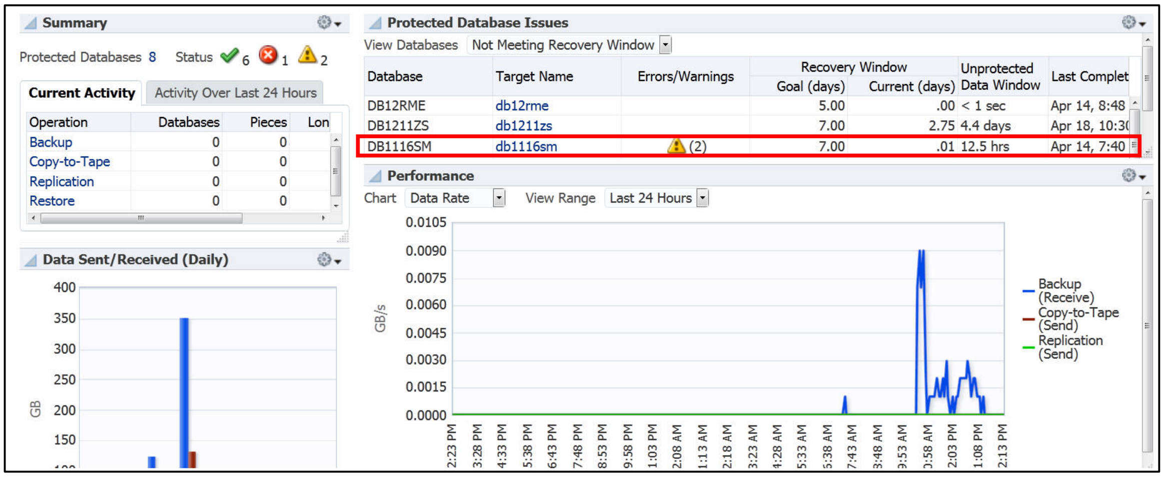
Used: 955.4 GB
Needed: 704.84 GB
Reserved: 2088.0 GB

De-Duplication Ratio	20.8 : 1
Keep Backup Space	None
Next Scheduled Backup	View
Last Copy To Tape	N/A
Last Replication	Sep 25, 11:07 AM PDT

Backup Report

Figure 15: Protected Database Detail

As database recovery window goals form a core component of Recovery Appliance protection policies, administrators can immediately see whether any databases are currently not meeting their goals from the Recovery Appliance home page, and then drill into the protected database page to determine how much additional space is needed to meet those goals.



Summary

Protected Databases 8 Status ✓ 6 ☒ 1 ⚠ 2

Current Activity | Activity Over Last 24 Hours

Operation	Databases	Pieces	Lon
Backup	0	0	
Copy-to-Tape	0	0	
Replication	0	0	
Restore	0	0	

Data Sent/Received (Daily)

Protected Database Issues

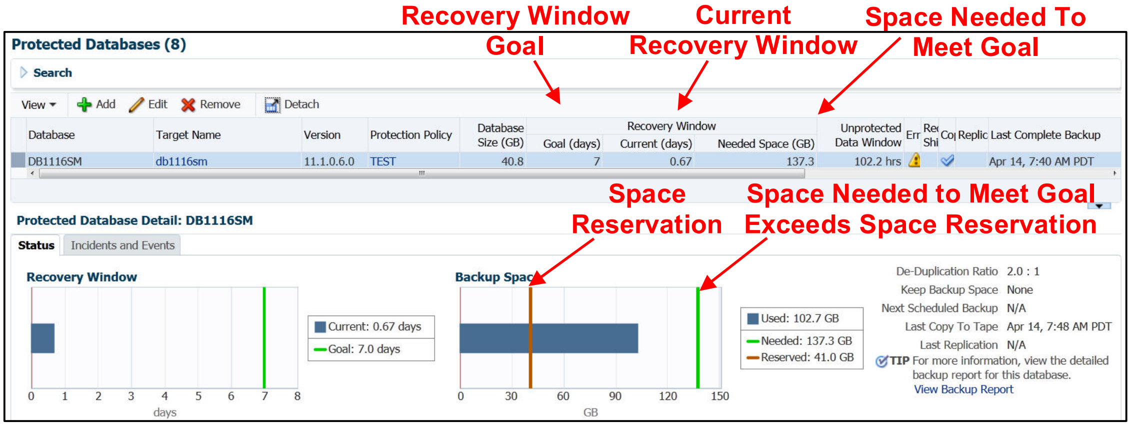
View Databases: Not Meeting Recovery Window

Database	Target Name	Errors/Warnings	Recovery Window		Unprotected Data Window	Last Complet
			Goal (days)	Current (days)		
DB12RME	db12rme		5.00	.00	< 1 sec	Apr 14, 8:48
DB1211ZS	db1211zs		7.00	2.75	4.4 days	Apr 18, 10:3(
DB1116SM	db1116sm	⚠ (2)	7.00	.01	12.5 hrs	Apr 14, 7:40

Performance

Chart: Data Rate View Range: Last 24 Hours

Figure 16: Recovery Appliance Enterprise Manager Home – ‘STORE26’ Not Meeting Recovery Window Goal



Recovery Window Goal

Current Recovery Window

Space Needed To Meet Goal

Space Reservation

Space Needed to Meet Goal Exceeds Space Reservation

Protected Databases (8)

Search

View ▾ | Add | Edit | Remove | Detach

Database	Target Name	Version	Protection Policy	Database Size (GB)	Recovery Window Goal (days)	 Current (days)	 Needed Space (GB)	Unprotected Data Window	Err	Re Shi	Co	Replic	Last Complete Backup
DB1116SM	db1116sm	11.1.0.6.0	TEST	40.8	7	0.67	137.3	102.2 hrs	⚠		✓		Apr 14, 7:40 AM PDT

Protected Database Detail: DB1116SM

Status | Incidents and Events

Recovery Window

- Current: 0.67 days
- Goal: 7.0 days

Backup Spac

- Used: 102.7 GB
- Needed: 137.3 GB
- Reserved: 41.0 GB

De-Duplication Ratio	2.0 : 1
Keep Backup Space	None
Next Scheduled Backup	N/A
Last Copy To Tape	Apr 14, 7:48 AM PDT
Last Replication	N/A

TIP For more information, view the detailed backup report for this database.

View Backup Report

Figure 17: 'DB1116SM' Needs Additional Space to Ensure Recovery Window Goal Can Be Met

The console also provides a complete view into the data protection status of each database and immediately alerts the Recovery Appliance administrator of any backup or appliance issues - for example, if a backup has not been processed in "3 days" or if the storage location cannot accommodate a particular database's recovery window goal due to insufficient free space. Similarly, if corrupted backups are discovered, the administrator need to be immediately notified so that the backups can be repaired from a good copy on tape or the replica appliance, or by taking a new full backup right away to ensure complete recoverability.

EM Cloud Control provides a rich set of status reports to the Recovery Appliance administrator and DBA for capacity planning and maintaining stated recovery window goals. For example, administrators can receive reports on historical space and network usage to identify backup volume and throughput trends that may necessitate adding additional systems in the future in order to meet all recovery window goals and backup window requirements.

	Last 7 Days
Storage Growth Rate (GB/day, average)	**5810.78**
Days Until Capacity is Exceeded*	**5.12**

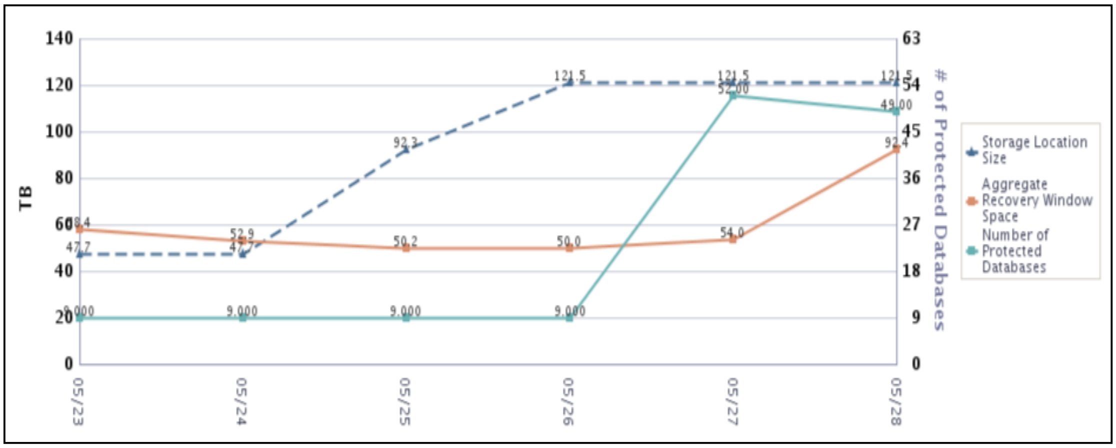


Figure 18: Recovery Appliance Storage Capacity Planning Report

Administrators can also receive reports on specific databases that are currently not meeting recovery windows. Finally, at the protected database-level, DBAs can receive customized backup history reports, so they can quickly identify problems such as failed or missing backups.

Scaling to Accommodate Data Growth

The Recovery Appliance can easily scale to accommodate growing number of protected databases, backup traffic, and storage usage by simply adding compute and storage servers. The Base Rack includes 2 compute servers and 3 storage servers providing up to 155 TB usable capacity for backups. The Base Rack can be upgraded on a per-storage server basis up to a maximum of 18 storage servers with 949 TB usable capacity, providing effective capacity of up to 9.5 Petabytes of virtual full backups with a 240 TB/hr virtual backup rate (24 TB/hr sustained delta ingest). If additional compute servers are required, a second Base Rack is setup and connected via Infiniband or 100GbE RDMA over Converged Ethernet (RoCE) to the first rack – storage capacity can then be easily expanded, as done in the first rack. Up to 18 fully configured racks can be connected together, providing up to 17 Petabytes of usable capacity, effectively storing 170 Petabytes of virtual full backups, with a 4 Petabytes/hr virtual backup rate (432 TB/hr delta ingest rate). A full rack can restore up to 24 TB/hr, and 18 fully configured racks can restore up to 432 TB/hr. Please refer to the Recovery Appliance Data Sheet[2] for additional specifications.

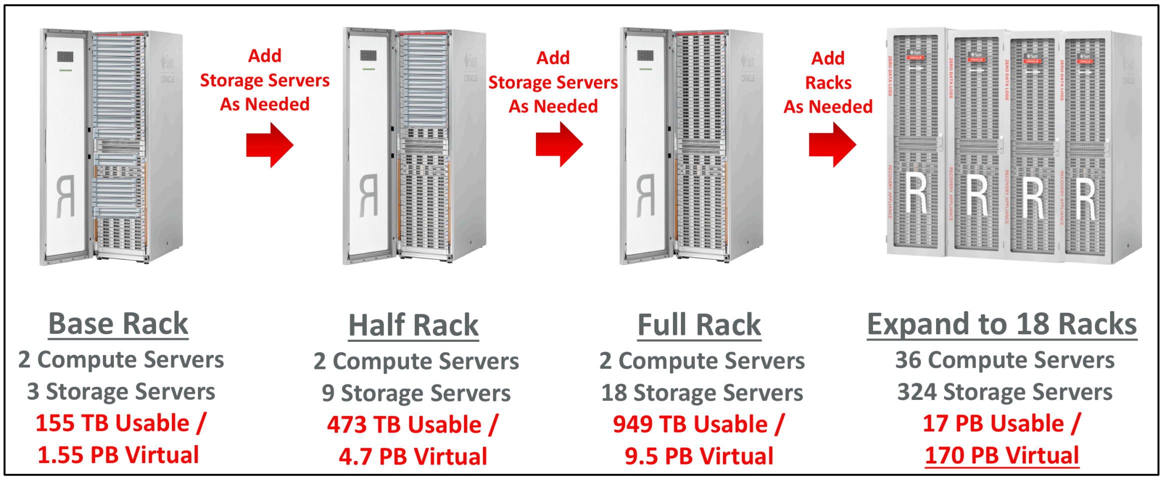


Figure 19: Recovery Appliance Rack Configurations

Related Technologies

Let’s now take a look at how Recovery Appliance complements related Oracle products and solutions.

Maximum Availability Architecture

The Maximum Availability Architecture (MAA) is Oracle’s best practice blueprint for deploying Oracle High Availability products and features[3]. For the database, the architecture features High Availability technologies, including RAC, ASM, and Flashback, along with Disaster Recovery solutions such as RMAN, Active Data Guard, and GoldenGate, as shown below.

[2] Zero Data Loss Recovery Appliance Data Sheet, http://www.oracle.com/technetwork/database/availability/recovery-appliance-ds-2297776.pdf

[3] Maximum Availability Architecture, http://www.oracle.com/goto/maa

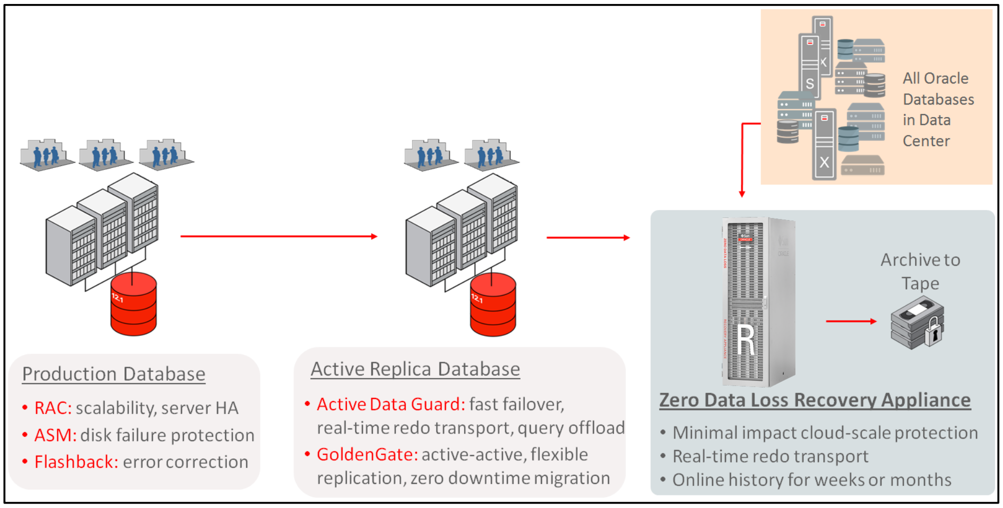

All Oracle Databases in Data Center
Archive to Tape
Production Database
• RAC: scalability, server HA
• ASM: disk failure protection
• Flashback: error correction
Active Replica Database
• Active Data Guard: fast failover, real-time redo transport, query offload
• GoldenGate: active-active, flexible replication, zero downtime migration
Zero Data Loss Recovery Appliance
• Minimal impact cloud-scale protection
• Real-time redo transport
• Online history for weeks or months

Figure 20: Recovery Appliance & Maximum Availability Architecture

As can be seen, the Recovery Appliance serves as the consolidated backup store for all databases within the data center, whether primary or standby databases. While Active Data Guard standby database provides zero data loss and fast failover capabilities for a specific production database, Recovery Appliance offers an efficient and reliable backup foundation for all databases, along with data loss protection in the order of sub-seconds for Oracle Database 11g and 12c. As discussed previously, the appliance can run backup copies to tape, thus providing centralized, enterprise tape archival. In the event of a local storage outage or even double site failure, the Recovery Appliance stands ready as a reliable backup store to service critical database restores whenever needed.

ZS4 Backup Appliance

The ZFS Storage Appliance ZS4-BA is a low-cost backup appliance for Oracle and non-Oracle environments alike. Featuring RAID-Z and compression for storage efficiency, the ZS4-BA also supports read-only and read-writable snapshots for development and testing purposes, along with a built-in database snapshot tool. While a ZS4-BA can be a cost-effective backup destination to support a small number of protected databases, Recovery Appliance is the choice for large-scale database protection across the entire data center, via real-time redo transport and tight integration with RMAN.

Oracle Multitenant

Oracle Database 12c Multitenant is a new database option which allows multiple databases running on separate machines to be consolidated (“plugged”) into a single, larger “container” database, thus allowing each individual “pluggable database” to better reap utilization of the aggregate compute and memory resources on a single machine than when they were run separately. RMAN supports backup and restore of the individual pluggable and container databases. In particular, once databases have been consolidated, container-level backups are a more efficient method to backup all pluggable databases versus running individual RMAN backup sessions for each database – restores can then be done for specific pluggable database(s), without affecting the status of the other pluggable databases.

The Recovery Appliance fully supports multitenant databases with the *incremental forever* backup strategy. RMAN handles all the necessary translations of a pluggable database into its composite data files and the appliance simply receives, stores, and catalogs the incremental backups as standard virtual full backups.

Summary

Oracle's Zero Data Loss Recovery Appliance extends the intelligence, robustness and resilience of an Oracle database to a specialized Engineered System. It redefines the data protection market with an innovative, never-before-seen architecture, leveraging Oracle-aware incremental forever strategy to eliminate data protection overhead and integrating with redo transport capabilities to dramatically reduce data loss exposure.

Start with a massively scalable repository that records all transactional changes across hundreds to thousands of databases, without incurring the time or impact of traditional backup windows. Boost production system performance by removing virtually all data protection overhead. Add the ability to quickly recover any database to any point-in-time or within sub-seconds of the current time in the event of a media loss or disaster. Deploy on a high-performance, cost-efficient, cloud-scale architecture to scale above and beyond modern enterprise demands. Finally, manage the entire infrastructure in a fully database and RMAN-aware manner, with the ability to track all backups throughout their lifecycle, from creation, to archival, to obsolescence. And with all these innovations, reap much higher business ROI for your enterprise Oracle backups by significantly reducing network consumption, disk storage, tape infrastructure, and management personnel costs.

Get back control of your database backup processes. Get back peace of mind by ***knowing*** the status and health of all your backups at all times. Take a test drive of the Zero Data Loss Recovery Appliance today and witness the advent of a ***New Era in Oracle Data Protection***.

ORACLE

Oracle Corporation, World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065, USA

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200

CONNECT WITH US

blogs.oracle.com/oracle
facebook.com/oracle
twitter.com/oracle
oracle.com

Hardware and Software, Engineered to Work Together