

Zero Data Loss Recovery Appliance

Today's storage solutions for protecting business data do not easily meet the needs of mission critical enterprise databases. They can lose up to a day of business data on every restore, do not inherently validate database level recoverability, place a heavy load on production servers during full backups, and cannot scale to meet the needs of ever expanding databases. These challenges are largely due to their fundamental treatment of databases as a set of disjoint files to copy, not as transactional systems with specific integrity and recovery requirements. The business impact is further compounded in the face of ransomware attacks, which can compromise both production and backup data without any detection, holding hostage a company's data and ability to recover.

Oracle's Zero Data Loss Recovery Appliance (Recovery Appliance or RA) is a ground-breaking data protection solution that tightly integrates with the Oracle Database to address these requirements head-on. It eliminates data loss, speeds recovery, and dramatically reduces data protection overhead on production servers. In addition, the Recovery Appliance continually validates the integrity and recoverability of the backup data for cyber resiliency, scales to protect thousands of databases, and protects backups across the full lifecycle, including disk backup, cloud archiving, remote replication and tape archiving.

Today's Database Protection Challenges

The fundamental challenges with today's database protection solutions stem from:

- Backup & recovery methods that are based on a decades-old nightly backup paradigm, where up to a day's worth of data can be lost on every restore, severely impacting transactional consistency across applications and business SLAs
- High backup overhead on production servers and networks by processing all database data during backups, whether it has changed or not, which can degrade application performance
- Ever-increasing backup windows due to non-stop data growth, which prolongs data loss exposure time and increases interference with operational workload windows



Oracle Zero Data Loss Recovery Appliance RA23

Key Features

- Real-Time Redo Transport
- End-to-End Data Validation
- Incremental-Forever Backup Strategy
- Space-Efficient Encrypted Virtual Full Backups
- Backup Operations Offload
- Database-Level Protection Policies
- Database-Aware Space Management
- Cloud-Scale Architecture
- Efficient Replication
- Policy-driven Archive to Cloud/ZFS/Tape
- Unified Management & Control
- Up to 1.57 PB of backup capacity per rack
- Up to 60 TB/hour backup & restore throughput per rack

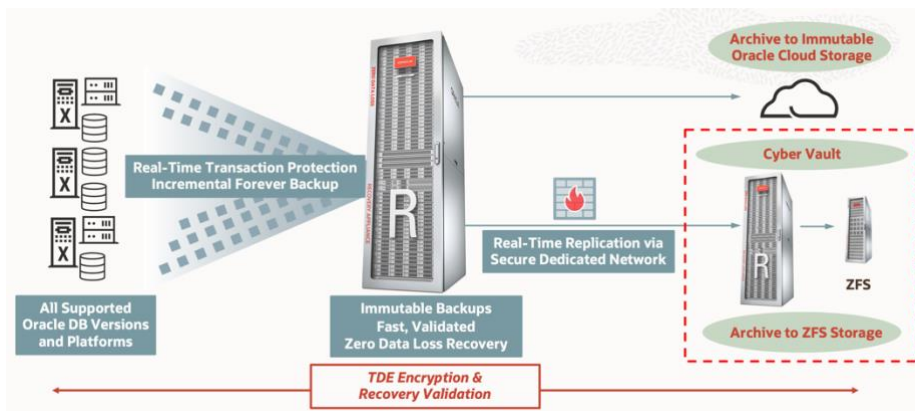
- Backup appliances that cannot scale to protect the hundreds to thousands of databases in the data center, resulting in unconstrained “IT sprawl” incurring excessive deployment and maintenance costs
- Poor visibility and control of the full data protection lifecycle, from disk to cloud to replication or to tape, leading to potential gaps in reporting and recovery

Introducing Zero Data Loss Recovery Appliance

The Oracle Zero Data Loss Recovery Appliance (Recovery Appliance) is the world's first engineered system designed specifically for database protection.

The Recovery Appliance delivers continuous protection for all databases while offloading all backup processing from production servers to minimize overhead.

The appliance can service a small Oracle environment with a starting base rack configuration and is architected to scale-out from there, to support the data protection requirements of hundreds-thousands of databases across the data center.



The Recovery Appliance tightly integrates with the Oracle Database and Recovery Manager (RMAN) to provide data protection capabilities and performance that are not possible with any other data protection solution.

Eliminate Data Loss

Recovery Appliance is designed to cost-effectively minimize data loss exposure by protecting in-flight Oracle Database transactions, which isn't possible with general purpose backup solutions.

Real-Time Redo Transport

Redo logging is the fundamental means of implementing transactional changes within the Oracle Database. All Oracle Database 12c and later version databases can continuously send redo directly from in-memory log buffers to the Recovery Appliance. This provides unique real-time data protection that allows databases to be protected until the last sub-second. Since redo is sent from database shared memory, the overhead on the production systems is extremely low.

Real-Time Redo Transport was first implemented for Oracle's Data Guard technology and has been deployed in thousands of mission-critical databases around the world. The Recovery Appliance extends this technology beyond the top tier of databases in a

Key Benefits

- Eliminate Data Loss
- Fast, Optimized Recovery
- Minimal Impact Backups
- Database Level Recoverability
- Integrated Archive to Cloud
- Cloud-Scale Capacity and Performance

The principal design goal of the Recovery Appliance is to eliminate the loss of critical database data that is still possible using existing data protection solutions.

“We replaced Data Domain with Oracle’s Zero Data Loss Recovery Appliance to enable real-time incremental backup and restore more than US\$850 million in monthly credit card transactions without data loss. We have also reduced average backup size by 30x and increased backup capacity by 65%.”

Iljoon Lee

Senior Manager, IT Team, KEB
Hana Card

simple and cost-effective manner. The Recovery Appliance provides similar levels of data protection as in Data Guard today, for databases that do not necessarily require Data Guard's fast failover and query offload capabilities.

Efficient Replication

Backups on a local Recovery Appliance can be easily and quickly replicated to a remote Recovery Appliance for protection against site outages or regional disasters. The replication topology can be tailored to match the data center's requirements. For example, replication can be set up in a simple one-way topology, two Recovery Appliances can be set up to replicate to each other, or several satellite Recovery Appliances can be set up to replicate to a central Recovery Appliance. If the local Recovery Appliance is not available, restore operations can run directly from a remote Recovery Appliance without staging the data locally.

Appliances may also be setup in a 'Backup Anywhere' paired replication configuration, so that backups taken to either system are automatically synchronized with the other – this provides high availability for backup and recovery operations in event of an outage impacting either of the systems.

In all topologies, only changed blocks are replicated to minimize WAN network usage.

Policy-driven Archive to Cloud/ZFS/Tape

Integration with Oracle Cloud provides direct access to low cost offsite storage. This reduces the risk associated with movement of physical media, like losing or forgetting to send media offsite. When needed, the recovery process can also start much sooner since there is no need to wait for physical media to arrive.

Archived backups to Oracle Cloud can be stored in native RMAN format and accessed independent of the Recovery Appliance. Use these backups for migration to the cloud, testing, development or to fulfill compliance related requests by instantiating the Cloud database from existing backups. Why spend time allocating on-premises resources when the cloud backup can be recovered directly into an Oracle Cloud Database?

For customers who require on-premises backup archives, the Recovery Appliance offloads full and incremental backups to Oracle ZFS Storage via integration with ZFS OCI object storage interface. Archive and restore operations can be run at 25 Gb or 100 Gb connectivity directly to and from ZFS.

Customers may also offload to tape via 32Gb Fibre Channel Adapters. Data is sent directly to tape libraries using the included Oracle Secure Backup media management software. This allows businesses to continue to use their existing tape libraries while eliminating expensive media manager database backup agents on production servers.

All tape hardware products supported by Oracle Secure Backup are supported by the Recovery Appliance. Alternatively, other vendors' tape backup agents may be deployed on the Recovery Appliance for integration with existing tape backup software, media servers, and processes.

This process for archiving to tape and cloud is completely offloaded to the Recovery Appliance eliminating the impact of creating these backups from production databases. A traditional weekly full and daily incremental archiving strategy can be employed to

The Recovery Appliance allows businesses to expand into cloud storage or protect their tape investments and continue with their current tape-based data retention strategy.

meet extended recovery window requirements, while point-in-time archival backups (similar to RMAN KEEP backup) can be created for compliance retention requirements of months or years. Archiving operations can run all day from the appliance, without slowing production systems, which enables better utilization of resources and lowers cost.

Recovery Reassurance: End-to-End Data Validation

The Recovery Appliance understands internal Oracle Database block formats, which enables deep levels of data validation. All backup data and redo blocks are automatically validated as they are received by the Recovery Appliance, copied to cloud/tape, and replicated. In addition, backup blocks are periodically validated on disk. This greatly increases the success rate of recovery operations – another unique differentiator that is only possible because of the Recovery Appliance’s deep database integration. If a corruption is discovered during validation, the Recovery Appliance’s underlying storage software automatically reads the good block from a mirrored copy and immediately repairs the corrupted block.

In addition, the Recovery Appliance storage software performs periodic inspections of the underlying hard disks. If bad sectors are detected, they are immediately repaired from a mirrored copy and done fully transparent to the user.

All backup data and redo blocks are automatically and independently validated at each stage of the backup lifecycle.

Minimal Impact Backups

Despite the requirement for 24x7 operations, many businesses still need to reserve multi-hour backup windows during which production application performance may be impacted. Backup windows provide no immediate business benefit, but instead compete with business critical reporting and batch workloads for off-hours processing time. In an increasingly global economy, backup windows continue to shrink, while data volumes grow.

Impact of Current Disk-Based Data Protection Solutions

Current disk-based data protection solutions impose large loads on production systems. This impact continuously increases as databases grow. Some key challenges are:

- Deduplication appliances require periodic full backups. Full backups read the entire database which induces heavy impact on production storage, servers, and networks, plus needlessly long backup windows.
- When source-side deduplication is used to reduce network requirements, this has the adverse effect of imposing high CPU and memory loads on production servers.
- During the recovery phase, incremental backups must be applied to the restored data files before the database can be opened. This process can significantly prolong recovery time, as the incrementals can span multiple days of changes, and because the apply operation usually runs across the network.

Incremental-Forever Backup Architecture

The second fundamental design strategy for the Recovery Appliance reduces backup-related processing on production database systems to the absolute minimum – transmitting *only changed data*. With unnecessary backup processing eliminated,

production systems can now focus on their primary goal – serving business critical workloads.

The Recovery Appliance implements an incremental-forever backup architecture to minimize impact on production systems. This architecture is based on two innovative technologies: Delta Push and Delta Store.

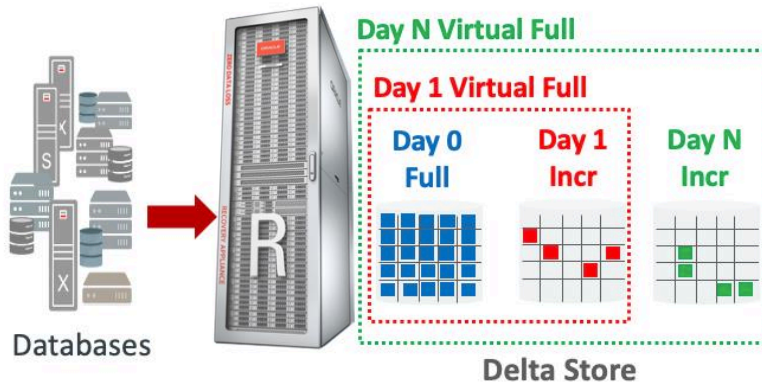


Figure 2. Zero Data Loss Recovery Appliance: Delta Push & Delta Store

With the Recovery Appliance, production database servers do what they are meant to do – serve production workload and not get bogged down with backup and recovery tasks.

Delta Push

With Delta Push, protected databases only send incremental backups containing unique database changes to the Recovery Appliance. There is no need for recurring full backups schedules or operations.. Delta Push is also known as “incremental forever” because, after a one-time full backup, only incremental backups are run on production systems. Effectively, Delta Push is a highly optimized form of source-side deduplication.

Changed blocks on production databases are very efficiently identified using RMAN block change tracking which eliminates the need to read unchanged data.

Special integration between protected databases and the Recovery Appliance eliminates committed undo, unused, and dropped tablespace blocks from the backup stream, significantly reducing overhead and space consumption.

Because Delta Push sends only changed data and not full backups, network traffic is greatly reduced compared to other solutions. This enables low-cost Ethernet to be used for backups. Also, minimizing network traffic allows the Recovery Appliance to be located further away from the protected databases, and even in some cases, across a WAN in a remote data center.

Delta Store

Delta Store represents the “brains” of the Recovery Appliance software engine. Delta Store validates the incoming changed data blocks, and then compresses, indexes and stores them. These changed blocks are the foundation of **Virtual Full Database Backups**, which are space-efficient pointer-based representations of physical full backups as of the point-in-time of an incremental backup. Virtual full backups can

improve storage efficiency by 10 times or more depending on the data set and change rate of the protected database.

For example, a traditional weekly full and daily incremental backup approach for a 100 TB database with 1% change rate and 30 day recovery window policy would incur:

- Full Backup: (100 TB x 5 backups)
- Incremental Backups: (1 TB x 30 backups)
- Total: 530 TB¹

In comparison, with Recovery Appliance, this would incur:

- Full Backup: 100 TB
- Incremental Backups: (1 TB x 29 backups)
- Total: 129 TB

This represents almost 5X storage consumption savings over traditional backups. When factoring in Recovery Appliance on-disk compression, total savings can reach 10X or more.

The dramatic space efficiency of the Delta Store architecture enables a large number of Virtual Full Backups to be kept online, greatly extending the disk based recovery window.

When a restore operation is required, Delta Store efficiently recreates a physical full backup based on the closest incremental backup time. The restore operation is supported by the massive scalability and performance of the underlying hardware architecture of the Recovery Appliance.

Restoring from a Recovery Appliance eliminates the slow traditional process of restoring a full backup and then sequentially restoring and applying all relevant incremental backups. Restore performance with the Recovery Appliance is more predictable which helps you meet your SLAs.

Faster restores also means (1) faster database test/dev refreshes and (2) faster migrations from legacy OS platforms to modern platforms, such as Oracle Exadata. The Recovery Appliance can be leveraged for minimal downtime, cross-platform and cross-version database migration activities based on innovative virtual full restore technology.

Most Backup Operations Offloaded

Practically all backup-related processing is offloaded to the Recovery Appliance. This includes time-consuming compression, backup deletion, validation, and maintenance operations. This frees production system resources, even outside the backup window, which increases the performance of the production systems.

“I am very relieved we can count on Oracle’s Zero Data Loss Recovery Appliance. We spent so much time with refresh tasks, now the DBA team’s productivity has improved significantly, we have the protection of our Oracle databases under control at any time through Enterprise Manager and the confidence that, in case we need an urgent restore, we will be able to perform it very quickly and up to the latest transaction. .”

Nazrul Islam
Lead Database Architect
Evergry

“Safaricom’s commitment to providing seamless and reliable telecommunication

¹ A weekly full and daily incremental backup approach to maintain point-in-time recovery window policy of ‘R’ days requires an additional 7 days of backups (1 full + 6 incremental backups) for a total of ‘R+7’ days of backups maintained on storage. This is due to database recovery design where at least one full backup *greater than R days old* must be retained for restore operations, which is then recovered forward using incremental and archived log backups into the start of the R days recovery window.

To summarize, with Real-Time Redo Transport and Delta Push, protected databases do the minimum possible backup-related work – transmitting only the changed data to the Recovery Appliance. All other backup and recovery related processing, including cloud and tape backup, is handled by the Recovery Appliance. This is one of the core architectural innovations of the Recovery Appliance, above and beyond today’s backup solutions.

Database Protection as a Private Cloud Service

The third design strategy of the Recovery Appliance provides a cloud-scale database protection service enabling you to efficiently protect tens to thousands of databases in a data center. Several Recovery Appliance technologies make this possible.

Policy-Based Data Protection Management

The Recovery Appliance introduces the concept of a protection policy, which defines recovery goals that are enforced on a per-database basis on the appliance and on cloud or tape. Using protection policies, databases can be easily grouped by recovery service tier. The Recovery Appliance includes predefined “Platinum”, “Gold”, “Silver”, and “Bronze” policies, which can be customized to support various business service level agreements. For example, database backups under the Gold policy target a 35 day recovery window on a local Recovery Appliance and 90 days on cloud, while backups managed under the Silver policy target a 10 day recovery window on a local Recovery Appliance and 30 days on tape. Tiered protection policies are also independently applied on the remote replicated Recovery Appliance.

As additional databases are created, they can be easily added to one of the existing protection policies. For example, a new Finance database can simply be added to the Gold protection policy, and the policy’s recovery window goals will automatically apply to this database’s backups. With this automated, policy-based framework, organizations can easily implement Database Protection as a Service across the entire enterprise.

Database-Aware Space Management

Using protection policies as the basis, the Recovery Appliance fully manages all backup storage space according to each database’s recovery window goals – e.g. the “Finance Database”, which is a member of the Gold policy, can be recovered within the past 35 days, while the “Products Database”, a member of the Silver policy, can be recovered within the past 10 days. If free space is available in the Delta Store, backups older than the recovery window goal will be retained, effectively extending the recovery window. Upon storage space pressure, the Recovery Appliance purges backups and automatically re-provisions space between databases to meet the recovery window goals for every protected database. The appliance may also purge backups proactively, in advance of any space pressure, based on historical space usage – again, in order to meet recovery windows goals for all databases. Space is purged in a database intelligent fashion with an understanding of the dependencies between data files, redo logs, and control files.

and financial services is powered by the unmatched performance and data protection capabilities of Oracle Exadata and Oracle Recovery Appliance. With these industry-leading solutions, we are able to deliver exceptional customer experiences and ensure the utmost security and integrity of our valuable data assets.” .”

Mark Oyier

Head of Dept.
IT Infrastructure & Enterprise
Safaricom PLC

With the Recovery Appliance, data protection is much better aligned with an application’s business criticality, rather than being limited to the physical bits and bytes level.

“With the Recovery Appliance, we were able to reduce backup configuration times down to 5 min from

This recovery window-oriented space management approach eliminates the need to manage space at an opaque storage-volume level as is typical with generic backup appliances. With this innovative approach, data protection is aligned with each application's business criticality, and manual rebalancing of space is eliminated.

Massive, Cloud-Scale Architecture

The Recovery Appliance is based on the Oracle Exadata architecture and therefore inherits its proven scalability, redundancy, and performance. As additional databases within the enterprise are protected by the Recovery Appliance, compute servers and storage servers can be easily added to the appliance, providing a simple, no-downtime, scale-out data protection cloud that seamlessly supports business growth.

Recovery Appliance Configuration

Base Rack and Full Rack Configuration

The Recovery Appliance RA23 base configuration includes 2 compute servers and 3 storage servers internally connected using 100 Gb/s Remote Direct Memory Access (RDMA) over Converged Ethernet (RoCE). RoCE provides the latest generation in ultra-fast cloud scale networking fabric, allowing one computer to directly access data from another without Operating System or CPU involvement, for high bandwidth and low latency.

A base rack configuration provides a highly available configuration with 274 TB of usable capacity for incoming backups. The base rack can be upgraded incrementally by adding additional storage servers into the rack, up to a maximum of 17 storage servers in a full rack. Each storage server adds 92 TB of usable capacity. The total usable capacity of a full rack is 1.57 PB with an effective capacity of up to **15 Petabytes of Virtual Full Backups**.²

A Recovery Appliance can protect databases whose total size is approximately the same as the available capacity of the appliance for a typical recovery window of 10 days. For example a single full rack configuration with 2 compute servers and 17 storage servers that has 1.57 PB usable capacity can protect approximately 1.57 PB of source database for a 10 day recovery window, storing ten 1.57 PB virtual full backups plus all the redo data generated for that 10 day period. Accurate sizing of the Recovery Appliance depends on several factors related to protected databases including the initial database size and growth rate, storage consumed by temp and undo, free space, database change rate, redo generation rate, desired recovery window, and compressibility of the database.

Fully Scale-out Architecture

If additional capacity is required beyond a full rack, a second base rack can be connected via 100 Gb/s RoCE. The second rack includes its own pair of compute servers which add connectivity and processing power to the configuration. As with the first rack, storage capacity can be easily expanded by incrementally adding storage servers. Up to 18 fully configured racks can be connected together into a single

weeks and decrease the backup volume by 40%.”

Christoph Lutz
Head Architect
Swisscom

“The Recovery Appliance delivers Data Protection as a Service (DPaaS), accelerates database performance and enables companies to recover to levels of extreme granularity.”

Jason Buffington,
Senior Analyst
Mark Peters,
Practice Director & Senior Analyst
Monya Keane, Research Analyst
Enterprise Strategy Group

Zero Data Loss Recovery Appliance allows capacity and throughput expansion with fully scale-out storage and compute servers.

² Effective capacity is calculated based on a 10% daily change rate.

appliance, providing 28.2 PB of usable capacity, i.e.

282 Petabytes of Virtual Full Backups.

The power and flexibility of the Recovery Appliance scale-out architecture is revealed when there is a need to support additional databases, or when business data grows. Storage, compute, and network capacity is incrementally added in a balanced fashion that maintains high performance. This architecture is far superior to traditional backup appliances which are usually limited to two controllers and therefore cannot scale storage, networking, and compute in a balanced, bottleneck-free fashion.

Performance Characteristics

The combination of extremely high throughput compute, network and storage together with the unique database integration of the Recovery Appliance enables performance levels that easily support the data protection needs of an entire data center.

A single full rack Recovery Appliance RA23 with 2 Compute Servers and 17 Storage Servers can achieve a sustained backup and restore rate of up to 60 TB/hour³. In other words, it can receive 60 TB/hour of change data and convert that into **600 TB/hour** of virtual backups, assuming a 10% change rate. Recovery Appliance achieves rates far exceeding other solutions through unique efficiencies by only reading, sending, and processing changed blocks unlike others, which must first determine what's changed.

As racks are added to the configuration, both performance and capacity increase linearly. An 18-rack Recovery Appliance achieves Virtual Full Backup rates of up to **10 Petabytes/hour**, and 1 PB/hour of Delta Ingest and Restore.

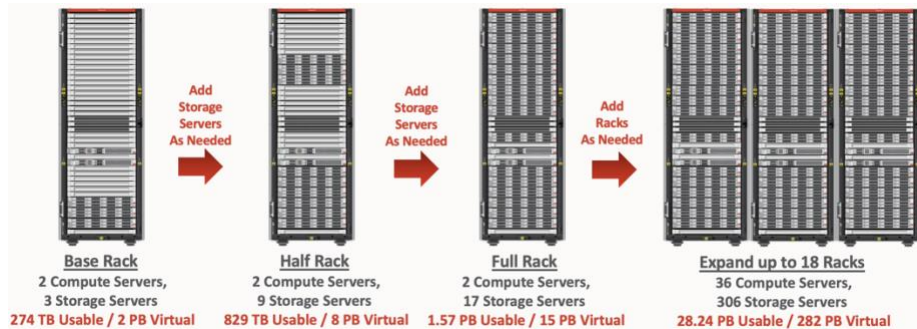


Figure 3. Recovery Appliance RA23 Scale-out Rack Configurations

Starting with RA23, the Recovery Appliance can be configured with 100Gb top of rack (ToR) switches to create a dedicated backup/recovery network for Exadata-hosted protected databases. This eliminates the need for Recovery Appliance to share a data center backup network and optimizes overall throughput, which can be especially beneficial for large database backup volumes. This network configuration is achieved by connecting Exadata systems to 100Gb ToR switches installed in the Recovery Appliance as shown below.

Recovery Appliance supports up to **15 Petabytes of Virtual Full Backups** in a single Full Rack, and **over 282 Petabytes of Virtual Full Backups** in a maximum configuration of 18 Full Racks.

A single Recovery Appliance Full Rack supports Virtual Full Backups running at an effective rate of up to **600 TB/hour**, while an 18-Full Rack configuration supports up to **10 Petabytes/hour**.

³ Exadata X10M-EF 4 DB nodes +10 storage cells with RA23 14 storage server configuration using Space-Efficient Encrypted Backups

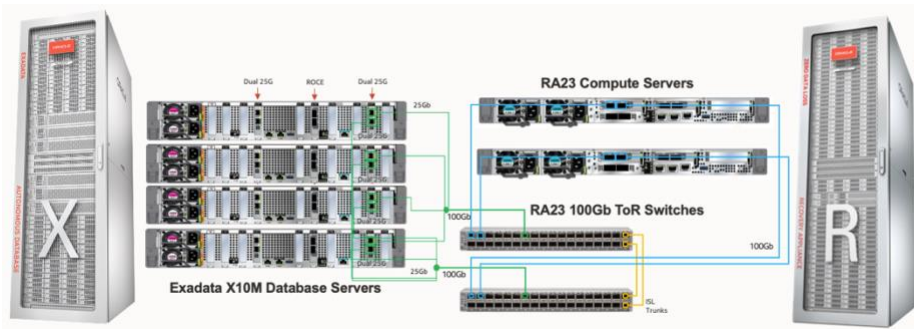


Figure 4. Recovery Appliance RA23 100Gb ToR Switches Configuration

Software Configuration

All software needed to run the Recovery Appliance is included in a single software license:

- Backup, recovery, and replication
- Embedded Oracle database for metadata and RMAN recovery catalog
- RMAN backup module for Recovery Appliance
- Storage software
- Archive to Cloud software
- Oracle Secure Backup software
- Special use ASO and ACO licenses for encryption and compression
- Oracle Enterprise Manager monitoring and management

As is usual with Oracle licenses, Recovery Appliance licenses are fully transferrable to new appliances. Because the license metric is the storage disk drive and not terabytes of storage, newer appliances with much larger disk drives and faster processors will be able to use existing licenses.

End-to-End Management of Data Protection

Data protection administration tasks are typically scattered across multiple fragmented management islands that correspond to IT roles – e.g. database administrators, backup administrators and storage administrators. Therefore, it is often nearly impossible for a DBA to determine whether a backup initiated using RMAN has reached its destination (e.g. tape) without any problems in the intermediate layers.

The Recovery Appliance solves this problem with fully automated, unified data protection management.

Unified Management Through Enterprise Manager Cloud Control

The Recovery Appliance provides a centralized, end-to-end view into the data protection lifecycle using Oracle Enterprise Manager Cloud Control – from the time the backup is initiated using RMAN, to the time it is stored on disk, cloud, tape, and/or replicated to another Recovery Appliance in a remote data center. All backup locations are tracked by the Recovery Appliance, so that RMAN restore and recovery operations can retrieve the most appropriate backups, wherever they reside. Only the Recovery

“Enterprises need to protect vital data for their critical business applications in real time without the downtime or data loss often experienced when using traditional approaches. The

Appliance can provide this level of end-to-end visibility into the data protection lifecycle, including granular storage and performance metrics.

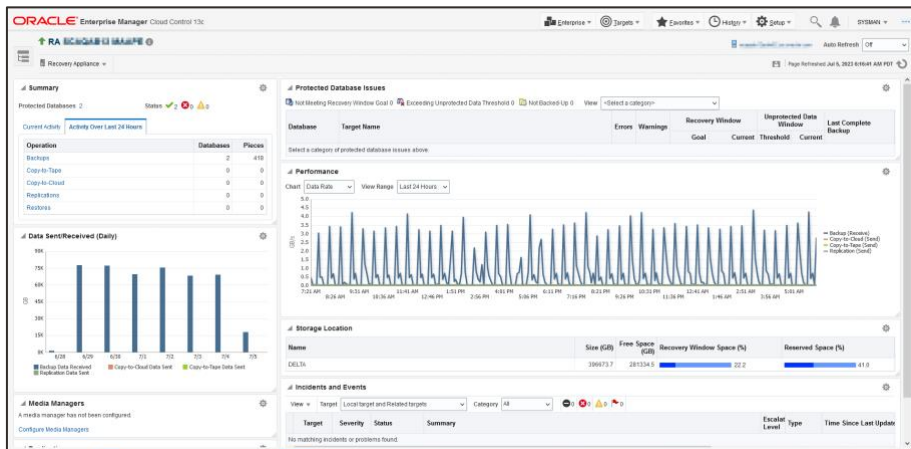


Figure 5. Centralized Protection Management – Storage & Performance Metrics

Zero Data Loss Recovery Appliance meets this demand with a simple, yet powerful solution that easily scales to protect databases enterprise-wide and meet ever-stringent recovery point objectives.”

Laura Dubois,
Program Vice President
Storage Practice
IDC

The Recovery Appliance delivers advanced storage monitoring and reporting to effectively manage current and future throughput, in addition to capacity requirements based on data growth. The amount of space needed for each database under Recovery Appliance management is predictively calculated based on its historical backup space usage and recovery window goal. Space needed is prominently displayed for each database in Enterprise Manager and the appliance aggregates total space needed for all databases as a percentage of total storage available, thereby taking the guesswork out of accommodating data growth. Want to know when capacity will be exceeded based on current data growth? Look no further than the Recovery Appliance Capacity Reports, available with Oracle Analytics Server (OAS), which provide summary and detailed information on storage utilization, average and maximum throughput for 7, 31, and 365 days plus detailed information on CPU, Memory and IOPS. In addition, warnings can be generated if space needed is within 15% (or other user configurable threshold) of total available space.

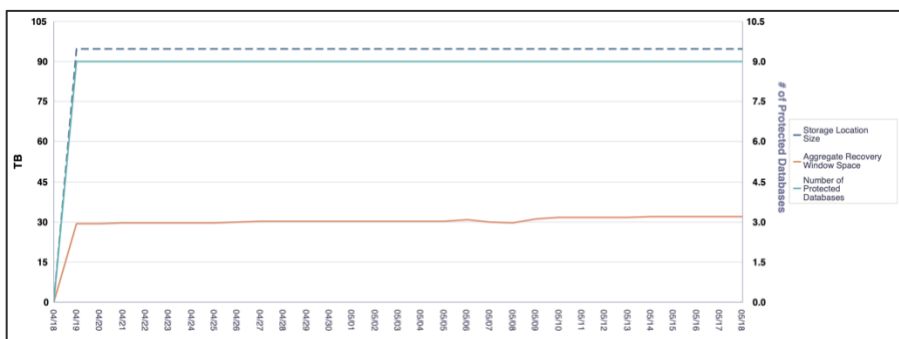


Figure 6. Capacity Planning – Protected Databases & Historical Space Usage

The simplicity of unified management for Oracle Database data protection is demonstrated through the streamlined manner in which databases are added to Recovery Appliance protection management:

- To add a new database, the Recovery Appliance Administrator uses the Enterprise Manager “Add Protected Database” wizard to associate the database with an appropriate protection policy and establish the database’s credentials.
- The Database Administrator then uses the database’s Enterprise Manager Backup Settings page to select the Recovery Appliance as the backup destination, and optionally enables Real-time Redo Transport for continuous data protection.

Resiliency and Recovery from Ransomware

In recent years, cyber-attacks have become a major concern for all customers due to the wide variety of approaches and subversive nature. Malware and ransomware impact to the global economy are staggering – in 2023, ransomware payments exceeded \$1B USD⁴ and the average cost of a data breach was over \$4M USD⁵. Average business downtime from attacks just in the healthcare industry was over 18 days⁶, with many cases stretching into weeks/months. For mission-critical databases, such attacks leading to lost data and system downtime can have far ranging impacts throughout the business in terms of revenue, operations, reputation, and even penalties.

The Recovery Appliance is designed to be fault-isolated from the production database, so if a ransomware attack hits the production database, the appliance is not compromised. This is due to the following key architectural features:

End-to-End Data Validation

While validation is key to detecting corrupt backup data throughout the backup lifecycle, it is equally important for detecting ransomware-attacked data. Since the appliance validates all incoming, on-disk, and replicated backups for Oracle block correctness and recoverability, any backup data maligned by malware or ransomware attack will be detected, recorded, and alerted to the administrator. Action can then be taken in conjunction with the DBAs to disconnect the database from the network and investigate further. Furthermore, replicated backups cannot be deleted or modified by the primary appliance or its administrators – they are independently validated and managed by the replica appliance, thus shielded from any effects of attacks done on the primary appliance. As an alternative or supplementary protection strategy, backups can be archived to Oracle Cloud Storage as a secure location for secondary backup copies, using Oracle Key Vault as key store for backup encryption keys – all backups remain encrypted in Cloud Storage and users require access to the Recovery Appliance and Oracle Key Vault to perform restore operations. The appliance can also archive backups to fibre-attached tape libraries via Oracle Secure Backup – tapes can then be shipped to and stored in a network-disconnected, offsite location that is impervious to ransomware attacks.

Immutable Backup

⁴ Ransomware Payments Exceed \$1 Billion in 2023, Chainalysis, <https://www.chainalysis.com/blog/ransomware-2024>

⁵ What is the cost of a data breach?, CSO, <https://www.csoonline.com/article/567697/what-is-the-cost-of-a-data-breach-3.html>

⁶ Average downtime caused by ransomware attacks in U.S. healthcare organizations from 2019 to 2023 YTD, Statista, <https://www.statista.com/statistics/1422159/us-healthcare-ransomware-attacks-downtime-average-by-days>

An immutable backup preserves integrity against wrongful/malicious deletion or modification of backup data. This is historically important to meet regulatory compliance requirements and in more recent times, as an additional defense layer against malware and ransomware attacks. Recovery Appliance can enforce immutable backups within a prescribed compliance retention period, whereby delete operations or reduction of retention using documented interfaces will have no effect on those backups. Secondly, backups can be placed into legal hold mode due to government or corporate action, whereby they will be retained indefinitely until the hold is removed. Finally, immutable backups may be archived to OCI or ZFS regulatory compliance buckets for longer-term immutable retention period. Net-net, this architecture effectively offers an end-to-end immutable solution, from backup creation on the local appliance, to replica appliance in DR site, and to cloud storage – all centrally managed and tracked by Enterprise Manager across the entire database environment.

Separation of Duty & Quorum User Approval

Access to the system is controlled via strict separation of duty between DBA and appliance administrator roles. DBAs are only given Virtual Private Catalog (VPC) user roles to backup and recover their privileged databases – they cannot access, modify, or delete backups on the appliance. Recovery Appliance administrators only have access to manage and monitor the system, but cannot backup, recover, or modify protected databases. Furthermore, the appliance restricts named administrative users to documented interfaces, while disallowing SSH and direct OS access – this prevents generic OS users, databases, or other services to be created and installed. Root access is only allowed via quorum user approval, where two other named admin users must approve the root request for specific time period.

Limited Network Access

With regards to network protocols, VPC users can only connect to the appliance via SQL*Net. TLS can be enabled for encrypting in-transit real-time redo via SQL*Net and RMAN backup and restore traffic via the Recovery Appliance Backup Module (HTTPS) – no other access from protected databases is allowed. In addition, the appliance enforces network segregation with the support of VLAN tagged networks, allowing backup and restore traffic to be fully isolated and non-routable between protected databases' specific network zones – in this way, any possibly affected backups would not be exposed to the rest of the enterprise.

Cyber Vault Deployment

To further isolate backups from unauthorized access and lateral movement of ransomware attacks, an appliance can be deployed in a Cyber Vault location, whereby data transmission into the vault is only possible via a private replication network from an appliance residing in production location. This network can be configured as 'air gapped', meaning that connectivity into the vault is generally closed and access is controlled by a firewall, gateway, or other network management facilities. The network is open only for periodic synchronization of the vault with new production backups via replication. Because the appliance utilizes efficient, incremental forever backups and consequently is also used for replication, the open connectivity window is kept very short, minimizing the chances of malicious intrusion. In addition, vault appliance administrator credentials and even Enterprise Manager can be setup

Related Products

- Oracle Database 19c, 21c
- Oracle Cloud Infrastructure Storage
- Oracle ZFS Storage
- Oracle Secure Backup
- Oracle Tape
- Enterprise Manager
- Zero Data Loss Autonomous Recovery Service

completely separate from production and DR appliance administrators, creating a separation of duty layer across locations. All network and replication activities can be initiated from within the vault. For more details on the Cyber Vault deployment, see the Zero Data Loss Recovery Appliance Cyber Security Architecture paper⁷.

Superior Resiliency

The appliance itself offers superior resiliency capabilities against ransomware attacks, when compared with traditional backup appliances. As an Oracle Engineered System built on Exadata hardware and storage, the appliance inherits a resilient architecture for reducing surface of attack on compute and storage servers – this includes hardened password policies, OS and DB user auditing, firewall support, and Oracle ILOM (Integrated Lights Out Management)⁸.

Oracle TDE-Integrated Space-Efficient, Encrypted Backups

Oracle Transparent Data Encryption (TDE) is Oracle’s gold standard for at-rest data encryption and is built into the database kernel, protecting against database bypass attacks coupled with minimal operational and performance impact. It supports the highest levels of cryptography in the industry and meets compliance requirements for regulations, such as GDPR, CCPA, PCI-DSS, and HIPAA. With TDE, data can only be accessed through the database and not read directly from disk, backups, or exports. In fact, Exadata Cloud@Customer mandates use of TDE to protect customer data from Oracle-managed system (DOM0) activities, such as patching and maintenance.

While TDE enables production-to-backup encryption, encryption historically has resulted in a negative effect on storage-based compression methods, due to the scrambled nature of encrypted data. Customers face the dilemma of investing in 2-3X or more backup capacity just to maintain existing retention requirements. For storage products in the market whose value primarily stems from deduplication and compression, encrypted data renders these capabilities moot, bringing into question their overall fit for database environments.

Recovery Appliance, integrated with the TDE data format, preserves database encryption at-rest, while offering the highest backup storage savings in the industry through innovative compression and incremental forever backup capabilities. Space-efficient, encrypted backups can help customers realize 3X backup storage savings and 2X faster backups compared to general purpose storage solutions. This represents a dramatic shift in the data protection industry where customers can now *secure the production to backup lifecycle with TDE at the lowest possible storage consumption with Recovery Appliance*.

Zero Data Loss Recovery

⁷ Zero Data Loss Recovery Appliance Cyber Security Architecture, <https://www.oracle.com/technetwork/database/availability/recovery-appliance-cyber-twp-6729502.pdf>

⁸ Oracle Exadata Security Guide, <https://docs.oracle.com/en/engineered-systems/exadata-database-machine/dbmsq/index.html>

Related Services

The following services are available from Oracle:

- Advanced Customer Services
- Oracle Premier Support for Systems
- Oracle Platinum Services
- Oracle Consulting Services

In the event that a database server is attacked and its backups must be recovered to a different server, Recovery Appliance real-time redo transport allows recovery to the very last transaction prior to the attack occurrence. This is especially important for ransomware attacks, where paying the perpetrators does not always mean your data comes back in pristine condition. With Recovery Appliance, don't pay the ransom – just recover the database to a separate, safe location *with no data loss*.

SEC 17a-4(f) Independent Auditor Assessment Report

The proliferation of cyber and ransomware attacks has been particularly felt by the financial services sector and with it, a renewed focus on the enforcement of SEC Rule 17a-4(f), which establishes requirements for the recording and retention of electronic records. All major financial institutions that are based or support operations in the United States can be subject to this regulation, comprised of five main requirements:

- Prevent overwriting or erasing the backup for required retention period (Immutability)
- Automatically verify the quality and accuracy of the backup
- Uniquely store the backup
- Maintain readily available indexes for reporting and backup retrieval
- Store a duplicate copy of the backup

Cohasset Associates, a leading information governance consulting firm, performed an independent assessment of the Recovery Appliance capabilities to confirm that customers can successfully meet these regulatory requirements. The report⁹ details each requirement and how Recovery Appliance meets each one. It is available to all customers, whether in financial services sector or in other regulated industries that require a similar product assessment.

Oracle Database Protection in Public Cloud

As customers consider their direction to cloud, database protection capabilities offered by the Recovery Appliance are now available with the Zero Data Loss Autonomous Recovery Service for Oracle Database services running on OCI. The Recovery Service helps organizations meet the business-critical need to reduce ransomware risk, financial requirements for improved operational efficiency, and user expectations for cloud service simplicity. For more information and resources, see the [announcement blog](#)¹⁰ and [product website](#)¹¹.

Summary: Redefining Oracle Database Protection

Existing data protection solutions fail to meet the demands of critical databases because they treat databases as simply generic files to copy rather than as transactional systems with specific data integrity, performance and availability requirements. With today's

⁹ Oracle Zero Data Loss Recovery Appliance SEC 17a-4(f) Compliance Assessment Report, Cohasset Associates, <https://www.oracle.com/a/ocom/docs/engineered-systems/recovery-appliance-compliance-assessment-report.pdf>

¹⁰ Introducing Oracle Database Zero Data Loss Autonomous Recovery Service, <https://blogs.oracle.com/maa/post/introducing-recovery-service>

¹¹ Oracle Database Zero Data Loss Autonomous Recovery Service, <https://www.oracle.com/recovery-service>

legacy solutions, business data is lost, end users are impacted, and deployment and management are complex and fragmented.

Oracle's Zero Data Loss Recovery Appliance tightly integrates advanced data protection technologies with Oracle Database to address these challenges for on-premises environments. It also serves as the foundation for the new Zero Data Loss Autonomous Recovery Service, offering similar capabilities for cloud databases. The Recovery Appliance redefines the database protection landscape with an innovative, state-of-the-art approach that:

- **Eliminates Data Loss:** Unique database integration enables continuous transport of redo data to the appliance, providing real-time protection for the most recent transactions so that databases can be restored without data loss.
- **Protects Data from Disasters:** The Recovery Appliance can replicate data in real-time to a remote Recovery Appliance and regularly archive backups to cloud or tape, in order to protect business data from site outages. Database blocks are continuously validated to eliminate data corruption at any stage of transmission or processing.
- **Eliminates Production Impact:** Backup algorithms integrated into Oracle Database send only changed data to the appliance minimizing production database impact, I/O traffic, and network load. All expensive backup processing is offloaded to the appliance. Unproductive backup windows no longer apply and don't hamper business continuity.
- **Offloads Archive Operations:** The Recovery Appliance can directly archive backups to low-cost cloud or tape storage, offloading production database servers. Archive operations can run both day and night to improve resource utilization.
- **Enables Restore to Any Point-in-Time:** The database change data stored on the appliance can be used to efficiently create Virtual Full Database copies at any desired point in time.
- **Delivers Cloud-Scale Protection:** A single Recovery Appliance can serve the data protection requirements of thousands of databases in a data center or region. Capacity expands seamlessly to Petabytes of storage, with no downtime. Organizations can now implement Database Protection as a Service using a policy-based approach, which provides administrators with end-to-end visibility into the state of enterprise database protection at any time.
- **Defend against Ransomware Attacks:** The appliance is a separate, independently managed system apart from the production database, and designed for resiliency against ransomware attacks. All incoming, stored, and outgoing backup data are continually validated for Oracle block correctness – this ensures that any compromised data is immediately alerted. Immutable retention periods can be configured on database-level, preventing malicious deletion or modification of critical backups. With respect to user access, separation of duty is strictly enforced between DBA and appliance administrator – DBAs can only backup/restore with no access to delete backups or modify the appliance, while conversely, administrators manage the appliances, but have no privilege to backup/restore databases. Furthermore, replicated backups are independently managed and validated from the primary backups, and thus will not be affected by any misaligned

data due to attacks on the primary appliance. System access itself is secured and logged via named administrator user model, which restricts access to day-to-day operations, and disallows root access. For further isolation of backup data, the appliance can be deployed in an air gap Cyber Vault location with separate user access credentials and when needed, efficiently synchronized with production backups via incremental-forever replication.

Built on the industry-leading Exadata platform, the appliance offers resiliency and monitoring capabilities through hardened password policies, fine-grained access control, comprehensive auditing, and secure lights-out management.

As another Oracle on Oracle advantage, Recovery Appliance backups integrate with Oracle Transparent Data Encryption (TDE), where database-native encryption is preserved throughout the backup lifecycle at the lowest possible backup space consumption. This is achieved through innovative TDE-aware backup compression and incremental forever strategy, offering 3X or more space savings compared to other general purpose backup solutions.

Finally, if the production database itself is compromised by an attack, Recovery Appliance can be used to restore all data, including all transactions up to the moment of the attack, to a separate, safe location.

Recovery Appliance RA23 Server Hardware

SERVER TYPE	STORAGE	NETWORK
Compute Server (2x per rack)	2 x NVMe Flash SSD (hot swappable)	<ul style="list-style-type: none"> • 2 x Dual Port 10/25 Gb Ethernet SFP28 <ul style="list-style-type: none"> ○ 2 x 10/25 Gb optical (ingest) ○ 2 x 10/25 Gb optical (replication) • 2 x Dual Port 100 Gb Ethernet QSFP28 <ul style="list-style-type: none"> ○ 2 x 100 Gb optical (ingest) ○ 2 x 100 Gb optical (replication) • 1 x Quad Port 10 Gb Ethernet RJ45 <ul style="list-style-type: none"> ○ 2 x 10 Gb copper (ingest) ○ 2 x 10 Gb copper (replication) • Sun Storage Dual 32 Gb Fibre Channel PCIe Universal HBA, QLogic for tape connectivity (optional) • 2 x 100 Gb QSFP28 RoCE Fabric ports • 1 x 1 Gb copper Ethernet port (mgmt) • 1 x ILOM Ethernet port • Maximum of 2 x 10 Gb, 2 x 25 Gb Ports, or 2 x 100 Gb Ports for ingest network • Maximum of 2 x 10 Gb, 2 x 25 Gb Ports, or 2 x 100 Gb Ports for replication network
Storage Server	12 x 22 TB 7,200 RPM disks 2 x NVMe Flash Acceleration Cards	<ul style="list-style-type: none"> • 2 x 100 Gb QSFP28 RoCE Fabric ports • 1 x 1 Gb copper Ethernet port (mgmt) • 1 x ILOM Ethernet port

¹ All servers include redundant hot swappable fans and power supplies.

Recovery Appliance RA23 Configurations

RACK SIZE	COMPUTE SERVERS	STORAGE SERVERS	USABLE CAPACITY (NORMAL REDUNDANCY)	USABLE CAPACITY (HIGH REDUNDANCY)
Base Rack	2 x compute servers	3 x storage servers	274 TB	174 TB
+Storage Servers	N/A	Up to 14 additional storage servers	92 TB per storage server	60 TB per storage server

¹ Each rack is 42 RU (Rack Units) in height, has 2x redundant Power Distribution Units (PDUs), 2x 36-port 100 Gb/s RoCE switches and 1x 48-port Management Ethernet switch for administration.

Maximum of 17x storage servers in a single rack.

Full Rack Usable Capacity:

- **Normal Redundancy: 1.57 PB**
- **High Redundancy: 1 PB**

Full Rack Backup & Restore Throughput:

- **4x 100 Gb (2x 100Gb LACP bonded per compute): 35 TB/hour**
- **4x 25 Gb (2x 25Gb LACP bonded per compute): 24 TB/hour**
- **4x 10 Gb (2x 10Gb LACP bonded per compute): 12 TB/hour**

Recovery Appliance RA23 Storage Server Environmental Specifications

METRIC	SPECIFICATION
Height	3.42 in (86.9 mm)
Width	17.52 in (445.0 mm)
Depth	29.88 in (759.0 mm)
Acoustic Noise (operating)	8.1 B
Weight	69 lb (31.3 kg)
Maximum Power Usage	0.5 kW (0.5 kVA)
Typical Power Usage ¹	0.4 kW (0.4 kVA)
Cooling at Maximum Usage	1,825 BTU/hour
	1,926 kJ/hour
Cooling at Typical Usage	1,278 BTU/hour
	1,348 kJ/hour
Airflow at Maximum Usage ²	85 CFM
Airflow at Typical Usage ²	59 CFM

Operating temperature/humidity: 5 °C to 32 °C (41 °F to 89.6 °F), 10% to 90% relative humidity, non-condensing
 Altitude Operating: Up to 3,048 m, max. ambient temperature is de-rated by 1° C per 300 m above 900 m
¹ Typical power usage varies by application load
² Airflow must be front-to-back

Recovery Appliance RA23 Environmental Specifications

Metric	BASE RACK	FULL RACK
Height	78.74" – 2000 mm	
Width	23.66" – 601 mm	
Depth	47.13" – 1197 mm	
Acoustic Noise (operating)	9.1 B	9.5 B
Weight	922.8 lb (418.6 kg)	2,060.0 lb (934.4 kg)
Maximum Power Usage	4.0 kW (4.1 kVA)	11.5 kW (11.8 kVA)
Typical Power Usage ¹	2.8 kW (2.9 kVA)	8.1 kW (8.2 kVA)
Cooling at Maximum Usage	13,782 BTU/hour (14,540 kJ/hour)	39,339 BTU/hour (41,502 kJ/hour)
Cooling at Typical Usage	9,647 BTU/hour (10,178 kJ/hour)	27,537 BTU/hour (29,052 kJ/hour)
Airflow at Maximum Usage ²	638 CFM	1,821 CFM
Airflow at Typical Usage ²	447 CFM	1,275 CFM
Operating temperature/humidity: 5 °C to 32 °C (41 °F to 89.6 °F), 10% to 90% relative humidity, non-condensing Altitude Operating: Up to 3,048 m, max. ambient temperature is de-rated by 1° C per 300 m above 900 m ¹ Typical power usage varies by application load. ² Airflow must be front-to-back.		

Recovery Appliance RA23 Regulations and Certifications

Regulations ^{1,2,3}	Product Safety:	UL/CSA 60950-1, EN 60950-1, IEC 60950-1 CB Scheme with all country differences UL/CSA 62368-1, EN 62368-1, IEC 62368-1 CB Scheme with all country differences
	EMC	
	Emissions:	FCC CFR 47 Part 15, ICES-003, EN55032, KN32, EN61000-3-11, EN61000-3-12
	Immunity:	EN55024, KN35
Certifications ^{2,3}	North America (NRTL), CE (European Union), International CB Scheme, HSE Exemption (India), BSMI (Taiwan), CCC (PRC), EAC (EAEU including Russia), KC (Korea), RCM (Australia), VCCI (Japan), UKCA (United Kingdom)	
European Union Directives ³	2014/35/EU Low Voltage Directive. 2014/30/EU EMC Directive, 2011/65/EU RoHS Directive, 2012/19/EU WEEE Directive	
¹ All standards and certifications referenced are to the latest official version. For additional detail, please contact your sales representative. ² Other country regulations/certifications may apply. ³ In some cases, as applicable, regulatory and certification compliance were obtained for the shelf-level systems only.		

Recovery Appliance Support Services


- Hardware Warranty: 1 year with a 4 hr web/phone response during normal business hours (Mon-Fri 8AM-5PM), with 2 business day on-site response/Parts Exchange
- Oracle Premier Support for Systems includes Oracle Linux support and 24x7 with 2 hour on-site hardware service response (subject to proximity to service center)
- Oracle Premier Support for Operating Systems
- Oracle Customer Data and Device Retention
- System Installation Services
- Software Configuration Services
- Oracle Platinum Services
- Business Critical Service for Systems
- System Upgrade Support Services including hardware installation and software configuration
- Oracle Auto Service Request (ASR)

Optional Customer Supplied Ethernet Switch Installation in Recovery Appliance

Each Recovery Appliance rack has 2U available at the top of the rack that can be used by customers to optionally install their own client network Ethernet switches in the appliance rack instead of in a separate rack. Some space, power, and cooling restrictions apply.

Connect with us

Call **+1.800.ORACLE1** or visit **oracle.com**. Outside North America, find your local office at: **oracle.com/contact**.

 blogs.oracle.com

 facebook.com/oracle

 twitter.com/oracle

Copyright © 2024, Oracle and/or its affiliates. All rights reserved. This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

This device has not been authorized as required by the rules of the Federal Communications Commission. This device is not, and may not be, offered for sale or lease, or sold or leased, until authorization is obtained.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group. 0424

Disclaimer: If you are unsure whether your data sheet needs a disclaimer, read the revenue recognition policy. If you have further questions about your content and the disclaimer requirements, e-mail REVREC_US@oracle.com.