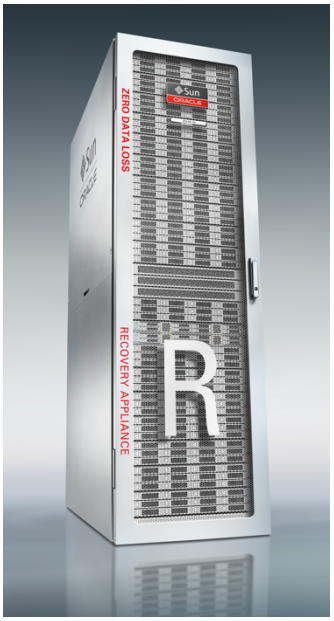
ORACLE DATA SHEET

Zero Data Loss Recovery Appliance X8 / X8M

State-of-the-Art Oracle Data Protection



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, place a heavy load on production servers during backup, do not inherently validate database level recoverability, 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 performance requirements.

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

KEY FEATURES

- Real-Time Redo Transport
- End-to-End Data Validation
- Incremental-Forever Backup Strategy
- Space-Efficient Virtual Full Backups
- Backup Operations Offload
- Database-Level Protection Policies
- Database-Aware Space Management
- Cloud-Scale Architecture
- Efficient Replication
- Policy-driven Archival to Cloud/Tape
- Unified Management & Control

Today's Database Data Protection Problems

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

- Backup and 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
- High backup overhead on production servers and networks for processing all database data during backups, whether it has changed or not
- Ever-increasing backup windows due to non-stop data growth
- Backup appliances that cannot scale to protect the hundreds to thousands of databases in the data center
- Poor visibility and control of the full data protection lifecycle, from disk to cloud to replication or to tape

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 critical 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.

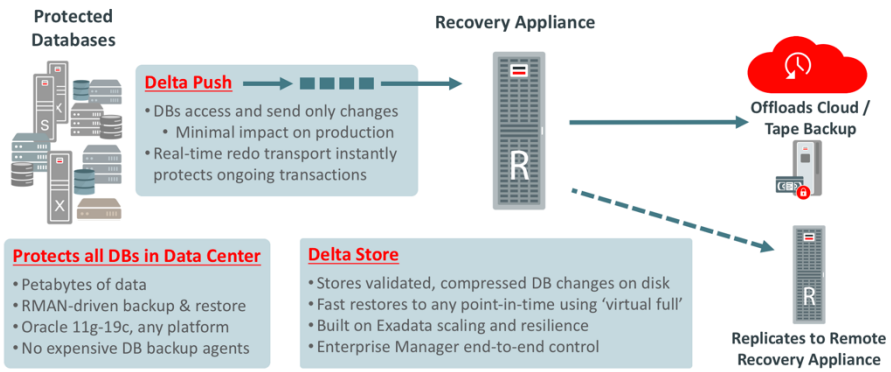


Figure 1. Zero Data Loss Recovery Appliance: Architecture Overview

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

Eliminate Data Loss

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

Real-Time Redo Transport

Redo logging is the fundamental means of implementing transactional changes within the Oracle database. All Oracle Database 11g Release 2 or later 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 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, or two Recovery Appliances can be set up to replicate to each other, or several satellite Recovery Appliances can be set up

KEY BENEFITS

- Eliminate Data Loss
- Minimal Impact Backups
- Database Level Recoverability
- Cloud-scale Data Protection

MANAGEABILITY FEATURES

- Oracle Embedded Integrated Lights Out Manager (ILOM)
- Oracle Enterprise Manger Recovery Appliance Plug-in
- Automatic Disk Scrub and Repair
- RACLI command line management of Recovery Appliance
- SNMP (RFC1157, 3416, 3410, 3414)

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.

KEB HANA CARD

"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 Co., Ltd.

to replicate to a central Recovery Appliance. In all topologies, only changed blocks are replicated to minimize WAN network usage.

If the local Recovery Appliance is not available, restore operations can run directly from a remote Recovery Appliance without staging the data locally.

Policy-driven Archival to Cloud/Tape

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.

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.

Backups stored in the Oracle cloud are in native RMAN format, so they can be 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 tape, the Recovery Appliance offloads full and incremental backups 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, including Oracle's StorageTek Tape, 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 tape and cloud archival is completely offloaded to the Recovery Appliance eliminating the impact of archival backup creation on production databases. Cloud and tape operations can now run all day without slowing production systems, which enables better utilization of resources and lowers cost.

Recovery Reassurance: End-to-End Data Validation

All backup data and redo blocks are automatically validated at each stage.

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, as they are copied to tape, and as they are replicated. In addition, backup blocks are periodically validated on disk. This ensures that recovery operations will always restore valid data – 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.

Minimal Impact Backups

Despite the requirement for 24x7 operations, many businesses still need to reserve multi-hour backup windows during which production jobs are 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 design goal for the Recovery Appliance is to reduce backup-related processing on production database systems to the absolute minimum – transmitting *only the 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.

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

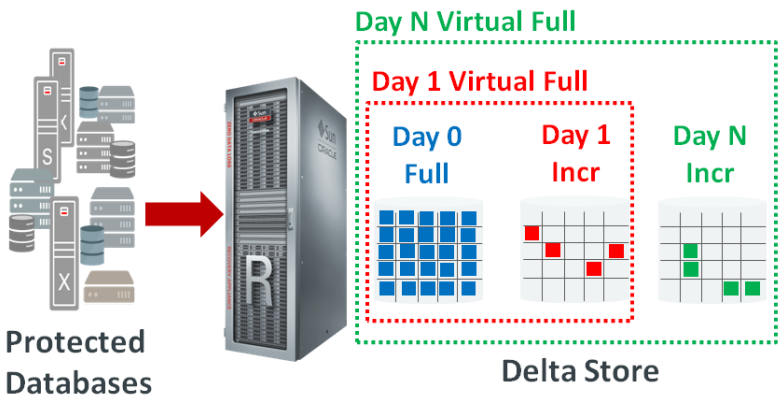


Figure 2. Zero Data Loss Recovery Appliance: Delta Push & Delta Store

Delta Push

With Delta Push, protected databases only send incremental backups containing unique changes to the Recovery Appliance. There is no need for recurring full backups. 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. Expensive dedicated Fibre Channel or Fibre Channel over Ethernet backup networks are not needed. 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.

ENTERPRISE STRATEGY GROUP

"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, ESG

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 TB[1]

In comparison, with Recovery Appliance, this would incur:

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

[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.

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.

Zero Data Loss Recovery Appliance can massively scale at cloud level.

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.

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.

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 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.

Cloud-Scale Database Protection as a Service

The third design goal for the Recovery Appliance is to provide a cloud-scale database protection service for tens to thousands of databases in a data center. Several Recovery Appliance technologies make this possible.

Policy-Based Data Protection Management

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.

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 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 tape, 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 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.

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

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

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 base configuration includes 2 compute servers and 3 storage servers internally connected using high speed InfiniBand with X8 or 100 Gb/s Remote Direct Memory Access (RDMA) over Converged Ethernet (RoCE) with X8M. 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.

With X8 and X8M, Recovery Appliance capacity has increased, now supporting up to **9.5 Petabytes of Virtual Full Backups** in a single Full Rack, and **over 170 Petabytes of Virtual Full Backups** in a maximum configuration of 18 Full Racks.

With X8 and X8M, the base configuration usable capacity has increased, providing a highly available configuration with 155 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 18 storage servers in a full rack. Each storage server adds 53 TB of usable capacity. The total usable capacity of a full rack is 949 TB with an effective capacity of up to ***9.5 Petabytes of Virtual Full Backups***.[2]

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

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 18 storage servers that has 949 TB usable capacity can protect approximately 949 TB of source database for a 10 day recovery window, storing ten 949 TB 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 in X8 beyond a full rack, a second base rack can be connected via high-speed InfiniBand. With X8M, a second rack is 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 appliance, providing 17 PB of usable capacity, i.e. ***170 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 Recovery Appliance Full Rack supports Virtual Full Backups running at an effective rate of up to **240 TB/hour**, while an 18-Full Rack configuration supports **4 Petabytes/hour**.

A single full rack Recovery Appliance with 2 Compute Servers and 18 Storage Servers is able to support Virtual Full Backups running at an effective rate of up to ***240 TB/hour***. This rate far exceeds that of other products on the market and is only possible because the Recovery Appliance only needs to read, send, and process changed data and therefore performs much less work than other products.

A single rack Recovery Appliance can achieve a sustained Delta Ingest rate of up to 24 TB/hour. In other words, it can receive 24 TB/hour of change data, and convert it into ***240 TB/hour*** of virtual backups. It is able to support a restore rate of up to 24 TB/hour.

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 ***4 Petabytes/hour***, and 432 TB/hour of Delta Ingest and Restore.

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
- Oracle Secure Backup software
- 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.

IDC

"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 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 solves this problem with fully automated, unified data protection management.

Unified Management Through Enterprise Manager Cloud Control

The Recovery Appliance provides a complete, 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, tape, and/or replicated to another Recovery Appliance in a remote data center. All backup locations are tracked by the Recovery Appliance catalog, so that any RMAN restore and recovery operation can retrieve the most appropriate backups, wherever they reside. Only the Recovery Appliance can provide this level of end-to-end visibility into the data protection lifecycle.

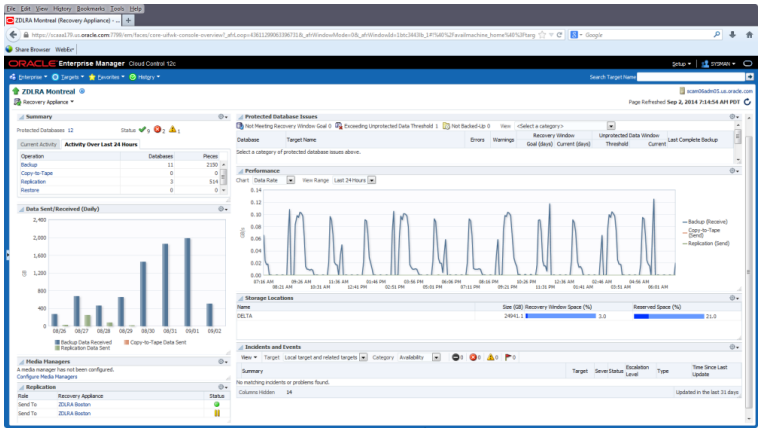


Figure 3. Recovery Appliance: End-to-End Data Protection Management

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

RELATED PRODUCTS

- Oracle Database 11g, 12c, 18c, 19c
- Oracle Secure Backup
- Enterprise Manager

RELATED SERVICES

The following services support the Zero Data Loss Recovery Appliance:

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

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 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.

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 Against Cyber-Attacks

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 attack cases are doubling year over year according to leading industry analysts, with millions of malware infections and thousands of ransomware attacks per day.[3] 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 cyber-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 cyber-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

[3] Source: Symantec 2018 Internet Security Threat Report, Panda Research, PWC, Juniper Research

Oracle Secure Backup - tapes can then be shipped to and stored in a network-disconnected, offsite location that is impervious to cyber-attacks.

Separation of Duty

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 does not expose or allow creation of local users, databases, or other services.

Limited Network Access

With regards to network protocols, VPC users can only connect to the appliance via SQL*Net, while HTTP(S) is used for RMAN backup and restore traffic via the Recovery Appliance Backup Module – no other protocols are employed. 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.

Superior Resiliency

The appliance itself offers superior resiliency capabilities against cyber-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)[4].

Zero Data Loss Recovery

Finally, 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 cyber-attacks, such as ransomware, 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*.

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 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 head-on. The Recovery

[4] Oracle Exadata Security Guide, https://docs.oracle.com/en/engineered-systems/exadata-database-machine/dbmsq/index.html

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 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 hamper business continuity.
- **Offloads Archival**: The Recovery Appliance can directly archive backups to low-cost cloud or tape storage, offloading production database servers. Archival 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.
- **Fault-Tolerance against Database Cyber-Attacks:** The appliance is a separate, independently managed system apart from the production database, and thus isolated from database attacks. Furthermore, all incoming, stored, and outgoing backup data is continually validated for Oracle block correctness – this ensures that any compromised data is immediately alerted. 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 maligned data due to attacks on the primary appliance. The appliance provides various resiliency and monitoring capabilities by leveraging industry-leading Exadata infrastructure for hardened password policies, fine-grained access control, comprehensive auditing, and secure lights-out management. 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 X8 / X8M HARDWARE SPECIFICATION

Base Rack

2 x Compute Servers, each with the following connectivity for use by protected databases, replication, or tape backups:

- *1 x 1 Gb copper Ethernet Port (mgmt)*
- *2 x 10 Gb copper Base-T Ethernet Ports or 2 x 10/25 Gb optical SFP+/28 LOM Ethernet Ports*
- *Sun Dual 10/25 Gb Ethernet SFP+/28 PCIe 2.0 Low Profile Adapter incorporating Intel 82599 10/25 Gb Ethernet controller and supporting pluggable SFP+ Transceivers. ROHS-5.*
  - *2 x 10/25 Gb optical Ethernet Ports*
- *Sun Storage Dual 32 Gb Fibre Channel PCIe Universal HBA, QLogic for tape connectivity (optional)*
  - *2 x 32 Gb Fibre Channel Ports*
- *Maximum of 2 x 10 Gb or 2 x 25 Gb Ports for ingest network*
- *Maximum of 2 x 10 Gb or 2 x 25 Gb Ports for replication network*

Each compute server additionally contains:

- *2 x 24-core Intel Xeon 8260 processors (2.4GHz)*
- *384 GB Memory*
- *(X8 only): 2 x QDR (40 Gb/s) 2 Ports*
- *(X8M only) 2 x 100 Gb/s QSFP28 RoCE Fabric Ports*
- *Oracle Integrated Lights Out Manager (ILOM)*
- *2 x Redundant Hot-Swappable Power Supplies*
- *Redundant Hot-Swappable Fans*
- *Disk Controller HBA with 1 GB Supercap-backed Write Cache*

---

3 x Storage Servers each with:

- *12 x 14 TB (raw) 7,200 RPM disks*

Each storage server additionally contains:

- *2 x 16-core Intel Xeon 5218 processors (2.3GHz)*
- *192 GB Memory*
- *2 x PCI flash cards*
- *Oracle Integrated Lights Out Manager (ILOM)*
- *2 x Redundant Hot-Swappable Power Supplies*
- *(X8 only) 2 x QDR (40Gb/s) InfiniBand Ports*
- *(X8M only) 2 x 100 Gb/s QSFP28 RoCE Fabric Ports*
- *Redundant Hot-Swappable Fans*
- *Disk Controller HBA with 1 GB Supercap-backed Write Cache*

(X8 only) 2 x 36-port QDR (40 Gb/s) InfiniBand Switches

- *Each InfiniBand switch has 6 ports available for external connectivity*

(X8M only) 2 x 36-port 100 Gb/s RoCE Switches

Management Connectivity

- *Ethernet switch for administrative connectivity to servers*
  - *2 x 1 GbE copper uplink ports available for connectivity to data center management network*

Rack Infrastructure Hardware:

- *42U Rack*
- *2 x Redundant Power Distributions Units (PDUs)*

Included Spare Parts Kit Contains:

- *1 x 14 TB disk*
- *1 x PCI flash card*

RECOVERY APPLIANCE CONFIGURATIONS

Rack Size	Compute Servers	Storage Servers	Usable Capacity (Normal Redundancy)	Usable Capacity (High Redundancy)
Base	2x servers	3x servers	155 TB	95 TB
+ Storage Servers	n/a	Up to 15x servers	53 TB per storage server	32 TB per storage server

Maximum of 18x storage servers in a single rack.
Full Rack Usable Capacity:

- Normal Redundancy: 949 TB
- High Redundancy: 587 TB

Full Rack Backup & Restore Throughput:

- 4 x 25 Gb: 24 TB/hour
- 4 x 10 Gb: 12 TB/hour

RECOVERY APPLIANCE X8 ENVIRONMENTAL SPECIFICATION

Component	Base Rack	Full Rack
Height Width Depth	78.74" – 2000 mm 23.66" – 601 mm 47.13" – 1197 mm	
Weight	909.8 lbs (412.7 kgs)	2055.3 lbs (932.3 kgs)
Maximum power usage Typical power usage [1]	• 4.3 kW (4.4 kVA) • 3.0 kW (3.0 kVA)	• 14.5 kW (14.7 kVA) • 10.1 kW (10.3 kVA)
Cooling at maximum usage Cooling at typical usage	• 14,560 BTU/hr (15,360 kJ/hr) • 10,192 BTU/hr (10,752 kJ/hr)	• 49,312 BTU/hr (52,024 kJ/hr) • 34,519 BTU/hr (36,417 kJ/hr)
Airflow at maximum usage [2] Airflow at typical usage [2]	• 674 CFM • 472 CFM	• 2,283 CFM • 1,598 CFM
Acoustic Noise Operating	• 9.4B	• 9.4B

Temperature Operating: 5º C to 32º C (41º F to 89.6º F), as measured by an industry grade temperature measurement device directed at the front bezel of the servers

Humidity Operating: 10% to 90% relative humidity, non-condensing

Altitude Operating: Up to 3,048m, max. ambient temperature is de-rated by 1º C per 300m above 900m

[1] Typical power usage varies by application load.

[2] Airflow must be front-to-back.

RECOVERY APPLIANCE X8 STORAGE SERVER ENVIRONMENTAL SPECIFICATION[1]

Component	Specification
Dimensions	• Height: 3.4 in. (86.9 mm) • Width: 17.5 in. (445.0 mm) • Depth: 29.9 in. (759.0 mm)
Weight	• 76.7 lbs. (34.8 kgs)
Power at maximum usage Power at typical usage [2]	• 0.7 kW (0.7 kVA) • 0.5 kW (0.5 kVA)
Cooling at maximum usage Cooling at typical usage	• 2,317 BTU/hour / (2,444 kJ/hour) • 1,622 BTU/hour / (1,711 kJ/hour)

Airflow at maximum usage [3] Airflow at typical usage [3]	• 107 CFM • 75 CFM
Acoustic Noise Operating	• 8.2B
Temperature Operating: 5º C to 32º C (41º F to 89.6º F)	
Humidity Operating: 10% to 90% relative humidity, non-condensing	
Altitude Operating: Up to 3,048 m, max. ambient temperature is de-rated by 1º C per 300 m above 900 m	
[1] The storage server environmental specifications are for a single server, standalone environment. Once the storage server is added to a Recovery Appliance X8 rack, the rack environmental specifications will take precedence. [2] Typical power usage varies by application load. [3] Airflow must be front-to-back.	

RECOVERY APPLIANCE X8M ENVIRONMENTAL SPECIFICATION

Component	Base Rack	Full Rack
Height Width Depth	78.74” – 2000 mm 23.66” – 601 mm 47.13” – 1197 mm	
Weight	907.4 lbs (411.6 kgs)	2052.9 lbs (931.2 kgs)
Maximum power usage Typical power usage [1]	• 4.3 kW (4.4 kVA) • 3.0 kW (3.1 kVA)	• 14.5 kW (14.8 kVA) • 10.1 kW (10.3 kVA)
Cooling at maximum usage Cooling at typical usage	• 14,676 BTU/hr (15,483 kJ/hr) • 10,273 BTU/hr (10,838 kJ/hr)	• 49,428 BTU/hr (52,147 kJ/hr) • 34,600 BTU/hr (36,503 kJ/hr)
Airflow at maximum usage [2] Airflow at typical usage [2]	• 679 CFM • 476 CFM	• 2,288 CFM • 1,602 CFM
Acoustic Noise Operating	• 9.1B	• 9.6B
Temperature Operating: 5º C to 32º C (41º F to 89.6º F), as measured by an industry grade temperature measurement device directed at the front bezel of the servers		
Humidity Operating: 10% to 90% relative humidity, non-condensing		
Altitude Operating: Up to 3,048m, max. ambient temperature is de-rated by 1º C per 300m above 900m		
[1]Typical power usage varies by application load. [2] Airflow must be front-to-back.		

RECOVERY APPLIANCE X8M STORAGE SERVER ENVIRONMENTAL SPECIFICATION[1]

Component	Specification
Dimensions	• Height: 3.4 in. (86.9 mm) • Width: 17.5 in. (445.0 mm) • Depth: 29.9 in. (759.0 mm)
Weight	• 76.7 lbs. (34.8 kgs)
Power at maximum usage Power at typical usage [2]	• 0.7 kW (0.7 kVA) • 0.5 kW (0.5 kVA)
Cooling at maximum usage Cooling at typical usage	• 2,317 BTU/hour / (2,444 kJ/hour) • 1,622 BTU/hour / (1,711 kJ/hour)

Airflow at maximum usage [3] Airflow at typical usage [3]	• 107 CFM • 75 CFM
Acoustic Noise Operating	• 8.2B
Temperature Operating: 5º C to 32º C (41º F to 89.6º F)	
Humidity Operating: 10% to 90% relative humidity, non-condensing	
Altitude Operating: Up to 3,048 m, max. ambient temperature is de-rated by 1º C per 300 m above 900 m	

[1] The storage server environmental specifications are for a single server, standalone environment. Once the storage server is added to a Recovery Appliance X8M rack, the rack environmental specifications will take precedence.

[2] Typical power usage varies by application load.

[3] Airflow must be front-to-back.

RECOVERY APPLIANCE X8 / X8M REGULATIONS & CERTIFICATIONS

Regulations[1,2,3]:

- Safety: UL/CSA 60950-1, EN 60950-1, IEC 60950-1 CB Scheme with all country differences
- EMC Emissions: FCC CFR 47 Part 15, ICES-003, EN55032, EN61000-3-11, EN61000-3-12
- EMC Immunity: EN55024

Certifications[2,3]:

- North America (NRTL), European Union (EU), International CB Scheme, HSE Exemption (India), BSMI (Taiwan), CCC (PRC), EAC (EAEU including Russia), RCM (Australia), VCCI (Japan)

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 at the time the data sheet was written. 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.

ORACLE

CONTACT US

For more information about the Zero Data Loss Recovery Appliance, visit oracle.com/recoveryappliance or call +1.800.ORACLE1 to speak to an Oracle representative.

CONNECT WITH US

blogs.oracle.com/oracle

facebook.com/oracle

twitter.com/oracle

oracle.com

Hardware and Software, Engineered to Work Together

Oracle is committed to developing practices and products that help protect the environment