ORACLE

Strengthen Oracle Database Cyber Defense and Recovery with Zero Data Loss Air-Gapped Backups

Technical Brief

January 2025, Version 1.0

Purpose Statement

This technical brief describes the solutions offered by the Zero Data Loss Recovery Appliance (ZDLRA) to protect Oracle Databases with an Air Gap.

Disclaimer

This document, in any form, software, or printed matter, contains proprietary information that is the exclusive property of Oracle. Your access to and use of this confidential material is subject to the terms and conditions of your Oracle software license and service agreement, which has been executed and with which you agree to comply. This document and information contained herein may not be disclosed, copied, reproduced, or distributed to anyone outside Oracle without prior written consent of Oracle. This document is not part of your license agreement, nor can it be incorporated into any contractual agreement with Oracle or its subsidiaries or affiliates.

This document is for informational purposes only and is intended solely to assist you in planning for the implementation and upgrade of the product features described. It is not a commitment to deliver any material, code, or functionality and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described in this document remains at the sole discretion of Oracle. Due to the nature of the product architecture, it may not be possible to safely include all features described in this document without risking significant destabilization of the code.

Table of Contents

List of Images

Introduction

Modern-day cyber resiliency and ransomware protection solutions have dominated the IT industry in the last several years. As a mitigating factor, companies are increasingly moving to leverage an Air Gap – a logical and/or physical separation of backup copies and storage – to strengthen their Cyber Defense posture.

As applications moved to real-time availability requirements, companies migrated to two or more data center architectures to provide immediate disaster recovery. In this case, the secondary backup is replicated to the opposite data center. This strategy, however, leaves both backup copies vulnerable to an attack since a persistent network exists for replication and, thus, allows for lateral movement of attacks.

As a result, companies are looking for a combination of the protection provided by offsite tape backups while offering immediate recovery for their transactional applications.

To meet these needs, Oracle's Zero Data Loss Recovery Appliance (ZDLRA) offers the best database protection available in the market, with the option of creating a physical Air Gap to isolate access to secured backup copies.

The solution is fundamentally based on two strategies to provide this capability:

- Logical Air Gap – Backups are received by the appliance in real-time and time-locked for immutability, isolating them from any user modifications and deletions. The administration of backups is separated from database administrators, and backups are continuously validated to ensure they have not been tampered. This provides a very high level of protection while backups are immediately accessible to production database hosts to meet low RPO and RTO requirements.
- Physical Air Gap – In a physically Air-Gapped environment (or Cyber Vault), the same data protection capabilities exist as in a logical Air Gap. In addition to those capabilities, the Air-Gapped appliance receives backup copies sent by the production appliance through a highly protected isolated replication network, which is only routable for short random periods throughout the day. This provides an even higher level of protection but does not offer the same RTOs and RPO as a logical Air-Gap since the physical Air-Gapped appliance is generally inaccessible by production systems and thus does not continuously receive the most current production backups.

Logical Air Gap Fundamentals

ZDLRA is designed for and offers the following capabilities in a logical air gap environment:

1. Built on Exadata Software, which is security-hardened and includes security and emergency fixes to address vulnerabilities.
2. Proprietary RMAN backup module that compresses the backup and utilizes the database encryption keys to encrypt the backups. This ensures that backups are encrypted at the source and remain encrypted throughout the backup lifecycle.
3. Separation of duties and a "least privilege user" model to ensure that compromised account credentials have limited ability to affect backups.
4. All system access and changes are audited and can be sent to a central audit log aggregator to detect any discrepancies.
5. Access is established on a per-session basis and can be quickly revoked to stop the spread of an attack.
6. Backup policies are leveraged to ensure recovery window and other backup attributes are consistent across databases.
7. Micro-segmentation can be implemented to ensure that backup accounts and networks are isolated. This ensures that each database has a specific backup user account and backup VLAN to the ZDLRA.
8. Immutability can be configured for tamper-proof backups
9. Continuous data anomaly detection of all backups identifies any issue that can compromise recovery due to cyber or ransomware attacks. Any failures are immediately alerted to the ZDLRA administrator.
10. Changes on the protected databases are sent in real-time to the ZDLRA, supporting zero to sub-second RPOs.
11. Enterprise Manager provides end-to-end backup and recovery management with database protection health monitoring and reporting.

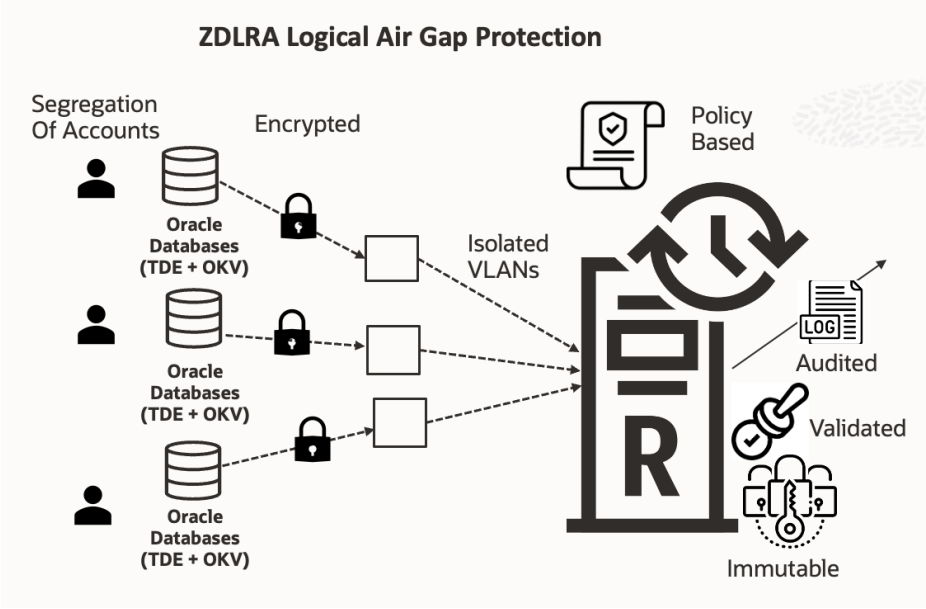

Figure 1: Logical Air Gap capabilities in a Single Recovery Appliance

Physical Air Gap Fundamentals

In order to provide an even higher level of protection, a physical Air Gap is often leveraged as a secondary or tertiary backup.

A physical air-gapped backup is implemented with a timer that protects the backup by disabling incoming networking connections.

A physical air-gapped backup on ZDLRA provides

- Highly optimized replication throughput by leveraging ZDLRA formatted backups that are both encrypted and compressed.
- Continuous Data Anomaly Detection of backups received by the ZDLRA in the vault
- Real-time reporting on the status of backups stored in the vault.
- Immediate restoration to the new environment or Clean Room, utilizing RMAN and the ZDLRA's built-in catalog.

Below is a typical configuration for a ZDLRA implemented with an Air Gap.

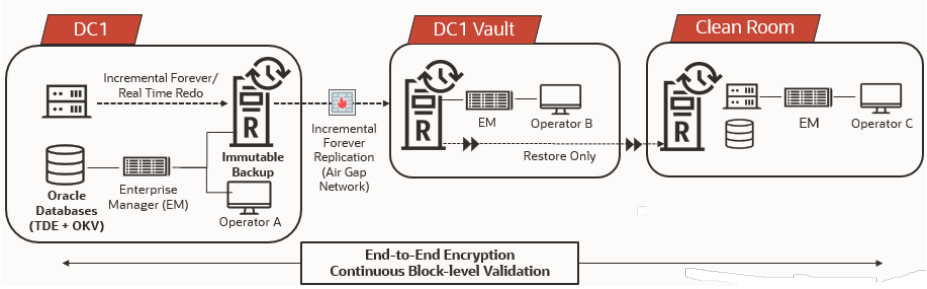

Figure 2: Physical Air Gap Architecture with Recovery Appliance Deployment in Cyber Vault

In this deployment scenario, ZDLRA utilizes:

- Incremental-forever backups to minimize the volume of backup data replicated, allowing the appliance behind the Air Gap to be more quickly synchronized versus replicating weekly full backups in a general-purpose backup strategy.
- Continual validation of replicated backups to check for recoverability and data block anomalies. The vault appliance performs these checks in an isolated network independent of the production appliance.
- Enterprise Manager (EM) provides reporting and alerting to detect issues with the ZDLRA or any discrepancies in replicated backups that could affect the ability to recover databases.
- EM provides viewing and automated reporting of the recovery point and validated recovery window of each database whose backups are stored in the vault.

Summary

By leveraging an Oracle-engineered design, the Zero Data Loss Recovery Appliance is able to provide an Air-Gapped backup solution that is superior in minimizing data loss, while offering highly space-efficient and performant backups when compared to other products in the market. The Recovery Appliance offers a rich set of database-integrated protection features, such as:

- *Zero to sub-second Recovery Point Objective (RPO)*
- *Space-efficient, incremental-forever encrypted backups and replication*
- *Continuous data anomaly checking of backups*
- *Compliance settings to protect backups and backup windows from tampering.*

These are summarized in the below comparison chart versus general-purpose backup appliances:

General-Purpose Backup Appliance	Oracle Recovery Appliance
RTO is typically not published as backup appliances are optimized for backups, not for recovery	RTO is published to ensure your business can meet the required recovery SLAs.
RPO is defined by the timestamp of the last successful archive log sweep	By leveraging Oracle Data Guard real-time redo transport, ZDLRA captures transactional changes as they occur and can recover a database with zero data loss.
Backups are validated by running RMAN restore validation process on each protected database, incurring production resources	ZDLRA is able to perform internal restore validation of all backups stored on the ZDLRA, not requiring production resources
Backup appliances rely on incremental merge backups plus storage snapshots to support incremental forever and point-in-time recovery.	The ZDLRA leverages all recovery features supported by RMAN while providing an incremental forever backup strategy with zero data loss or any point-in-time recovery.

Additional Resources

- Ransomware Protection Blogs
  - *blogs.oracle.com/maa/post/zero-data-loss-recovery-appliance-architectures-for-ransomware-protection-and-cyberresilience*
  - *blogs.oracle.com/maa/post/protect-and-recover-databases-from-ransomware-attacks-with-zero-data-loss-recovery-*

appliance

  - *blogs.oracle.com/maa/post/recovery-appliance-immutable-backups*

- Cyber Security Technical Brief
  - *www.oracle.com/technetwork/database/availability/recovery-appliance-cyber-twp-6729502.pdf*
- Product Webinars
  - *Ransomware Protection and Cyber-Resilient Architectures with Zero Data Loss Recovery Appliance*
  - *Space-Efficient Encrypted Backups*
  - *Ransomware Protection: asktom.oracle.com/pls/apex/asktom.search?oh=13154*
  - *Immutable Backups: asktom.oracle.com/pls/apex/asktom.search?oh=15532*
- Engage with us:
  - *LinkedIn: All Things Backup & Recovery*
  - *Backup & Recovery Office Hours: asktom.oracle.com/pls/apex/asktom.search?office=1341*