ORACLE

Zero Data Loss Recovery Appliance Cyber Security Architecture

June 26, 2020 | Version 1.05

PURPOSE STATEMENT

This paper describes the Zero Data Loss Recovery Appliance (Recovery Appliance) cyber security architecture and how it works, along with key best practices for configuration and operational usage.

INTENDED AUDIENCE

This paper is intended for the Database Administrator, Recovery Appliance Administrator or Security Officer. There should be a high-level understanding of Zero Data Loss Recovery Appliance and Oracle Database backup and recovery via Recovery Manager (RMAN).

DISCLAIMER

TABLE OF CONTENTS

INTRODUCTION

Cyber security has become an increasingly critical topic as malware and ransomware attacks continue to occur around the world. One of the many examples occurred in April 2019 when a Ragnar Locker ransomware attack occurred at EDP, a leading electric and gas energy provider in Europe, which resulted in locked systems and stolen files[1]. The Ragnar Locker attack at EDP targeted the operating system, but exemplifies how mission-critical components for businesses, including Oracle Databases, can be vulnerable to cyber-attacks. If these mission-critical databases cannot be accessed, it is costly for business operations and can lead to negative news headlines.

Proactively planning against these types of attacks ensures that the data in your organization is ready for recovery. This level of planning is an extension of disaster recovery (DR) that organizations have been performing for years, but the focus is on having a known good copy of data in a safe and isolated location inside the data center or in a remote bunker location.

The design of this safe location should be structured around the industry principles of information security known as the CIA Triad, which are:

- Confidentiality
- Integrity
- Availability

This paper leverages these principles to describe how the Recovery Appliance is the best solution for Oracle Database protection in a cyber security architecture and how it works, along with key best practices for configuration and operational usage.

CYBER VAULT: ENSURING PROTECTION OF PRODUCTION DATA

One common solution for this safe location that is extremely effective in ensuring cyber security is the concept of a Cyber Vault. A Cyber Vault is a network-isolated (i.e. separated by an "air-gap") group of technology components inside the data center itself. This Cyber Vault is comprised of a variety of components, like firewalls, networking, servers, and storage which retain recovery data for all the various information types that are critical to business operations. The Cyber Vault components periodically perform a rapid synchronization with all the critical production data, but otherwise stay disconnected for up to 24 hours at a time. This isolated and disconnected Cyber Vault allows for a known good and last resort recovery to be performed if the production server environment is compromised due to a cyber-attack.

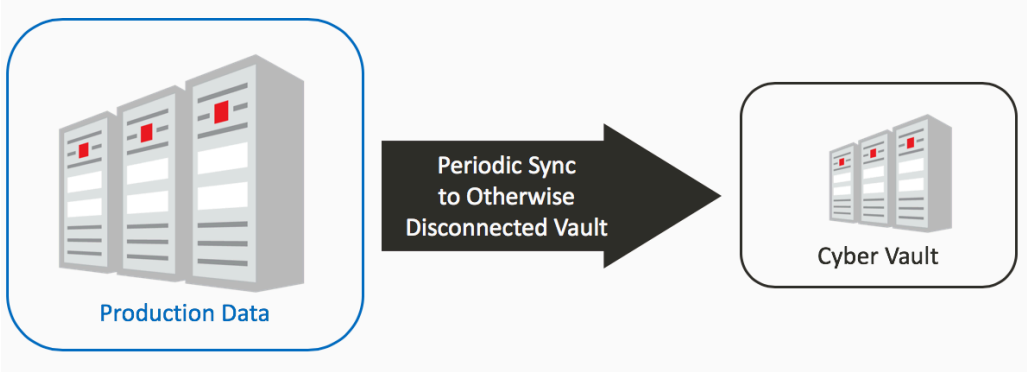

Figure 1 - Cyber Vault Design

Note however that the Cyber Vault should not be considered as a replacement for a company's DR solution. Since the Cyber Vault network is only periodically active for production data synchronization, the data in the Cyber Vault inherently lags behind that of production – therefore, the cyber security architecture is not designed to replace a proper disaster recovery solution. In comparison, the disaster recovery site is designed to be connected to the data center, receiving up to the moment changes, and always ready to take over for production with little or no data loss, and minimal downtime. Always being up to the moment with the latest changes and the lack of isolation makes the disaster recovery site equally as susceptible to a cyber-attack as the production data center.

1 https://www.tripwire.com/state-of-security/security-data-protection/ragnar-locker-ransomware-demands-1580-btc-from-edp/

The Cyber Vault content and configuration are going to vary based on infrastructure and recovery needs, but should contain all the data required to keep your business operational.

WHAT SHOULD BE CONSIDERED WHEN DESIGNING THE CYBER VAULT?

In framing these design points for the Cyber Vault, the CIA Triad principles of information security: Confidentiality, Integrity, and Availability will be used. First, let's start with the following basic operational rules for the Cyber Vault:

- *Limit access to the Cyber Vault:* Access to the Cyber Vault should be limited to only a small number of IT staff. Access should only occur with proper change control and auditing, thereby maintaining the **confidentiality** of the Cyber Vault data.
- *Limit the Cyber Vault connection:* The Cyber Vault should remain disconnected as much as possible which will help ensure **integrity**. Connections from the Cyber Vault to the rest of the production data center should be randomized and as short as possible. A regular schedule with a long connection time, is too predictable to protect against intrusion.
- *Limit the number of components:* The number of components that comprise the Cyber Vault should be minimized and designed for resiliency against attacks. A high number of components increases the attack surface and enables additional administration access, which ultimately makes **availability** of the Cyber Vault more difficult to maintain.

In addition to the rules above, the operational activities for the Cyber Vault should also be periodically reviewed. Some of the operational activities are detailed below:

- *Use accounts that are unique to the Cyber Vault*: With a smaller IT staff, a single person may have access outside and inside the Cyber Vault, but the accounts should be separate to maximize **confidentiality**.
- *Ensure that the data being sent to the Cyber Vault is valid:* If you have to fall back to the Cyber Vault due to an attack, you need to be confident in the **integrity** of the data and that it is truly recoverable.
- *Automate as much as possible:* Manual steps in the Cyber Vault means exposure and human interaction which leads to difficulty maintaining **availability**.

Figure 2 - CIA Triad

As a co-requisite, data encryption should be considered during the planning of a Cyber Vault. For the Oracle database, Transparent Data Encryption (TDE) ensures that the data stays secure throughout its lifecycle, from production to backup to Cyber Vault. This is a key requirement in keeping data confidential.

Finally, with data being stored in the Cyber Vault solely for recovery in the event of a cyber-attack, the ideal foundation for this platform is to leverage backups. Database backup solutions have been designed with built-in support for isolation and point-in-time recovery, so for Oracle Databases, the above rules and operational considerations need to be implemented around the usage of Oracle Recovery Manager (RMAN), which is Oracle's database-integrated backup and recovery solution.

Challenges with Traditional Oracle Backup Solutions in the Cyber Vault

Traditional backup technology is designed with the expectation that there is always a network connection to the source database being protected. The Cyber Vault paradigm limits the connectivity between the production and Cyber Vault environments which poses the following challenges for traditional Oracle Database backup operations:

- **Oracle Backup Validation:** To ensure **integrity**, traditional backup solutions rely on RMAN `RESTORE VALIDATE`, to validate the backup. This RMAN connection from the production database network to the Cyber Vault infrastructure for the validation process increases the opportunity for compromised access inside the Cyber Vault.
- **Oracle Backup Expiration:** Traditional solutions that rely on generic storage replication to synchronize the Cyber Vault with production backups can pose risks to recovery operations, since RMAN isn't used to ensure backup **integrity**.
- **Schedule Coordination:** Traditional backup solutions run backup jobs on a schedule. Timing this backup schedule with a random Cyber Vault connection is difficult and may cause data to be substantially out of sync with the data in the Cyber Vault which impacts **availability**.
- **Repeated Full Backups:** Weekly full backups are common practice in traditional backup strategies. These full backups are larger and require a longer Cyber Vault connection time for replication when compared to the daily incremental backups. This longer connection time increases exposure of the Cyber Vault to compromised access thereby decreasing **integrity**.
- **Encrypted Backups:** While TDE effectively secures data at the source, TDE backups can reduce effectiveness of traditional data reduction technologies (deduplication and compression), causing backup sizes to increase significantly. This increased backup size also increases the time period that the Cyber Vault must remain open to replicate the backup, which again increases the potential for compromised access and decreases **integrity**.
- **User Access and Management:** Database administrators drive backup/recovery operations and management. To ensure **confidentiality**, there must be clear separation of duty between production, backup, and Cyber Vault environments, such that no single account has the privilege to delete production data and their corresponding backups.

Net-net, these challenges directly impact the ability to operate production and Cyber Vault environments within the guidance of the CIA Triad framework.

Introducing Zero Data Loss Recovery Appliance

The Zero Data Loss Recovery Appliance (Recovery Appliance in short) is an engineered system designed specifically for Oracle database protection. 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 / tape archiving, and remote replication. The security hardened and resilient platform design of the Recovery Appliance makes it ideal for cyber security architectures.

Recovery Appliance Usage in the Cyber Vault

Using the Recovery Appliance in the Cyber Vault offers key differentiators over traditional backup and Cyber Vault solutions:

- Real-time Oracle Database protection - ensures that the latest backup is always ready for the Cyber Vault when the connection is opened. This also eliminates the need to synchronize the backup schedule with the randomized Cyber Vault network opening times.
- Incremental forever paradigm - minimizes the amount of data replicated to the Cyber Vault and helps keep the Cyber Vault connection time window as short as possible.
- Automatic recovery validation and expiration performed internally – validation from production database to Cyber Vault, removing the need of an Oracle database server for validating backup data in the Cyber Vault itself.

- Separation of duty amongst database administrator, Recovery Appliance administrator in production, and Recovery Appliance administrator in the Cyber Vault – appropriate access and management privileges are granted based on role.

These Recovery Appliance capabilities are fully compatible with Oracle Database encryption (TDE) and covered in detail below.

RECOVERY APPLIANCE CYBER SECURITY ARCHITECTURE: OVERVIEW

The Recovery Appliance cyber security architecture example in figure 3 below shows an extension of the production and disaster recovery data center to include the Cyber Vault. In this example, the production and disaster recovery data centers on the left, have their own Cyber Vault on the right. Following the Maximum Availability Architecture[2], each Recovery Appliance protects data from the local Oracle databases. Active Data Guard or Golden Gate will handle keeping the disaster recovery site updated for databases configured for high availability, which is seen on the left. In the middle, databases without Data Guard or Golden Gate will be replicated by the Recovery Appliance to the disaster recovery site. The Recovery Appliances in production and in the disaster recovery site will replicate to their respective Recovery Appliances that are in the local Cyber Vault which is shown on the right. Also, note that there is a separate Oracle Enterprise Manager in production and in the Cyber Vault to ensure separation of management.

Similar to a disaster recovery data center, planning will be required to ensure that the Cyber Vault has the connection bandwidth, performance capabilities and storage capacity required to meet the SLA for your organization. Under-sizing the Cyber Vault can lead to a backlog of backup data to be replicated into the Cyber Vault, or the inability to meet required recovery windows with the Cyber Vault.

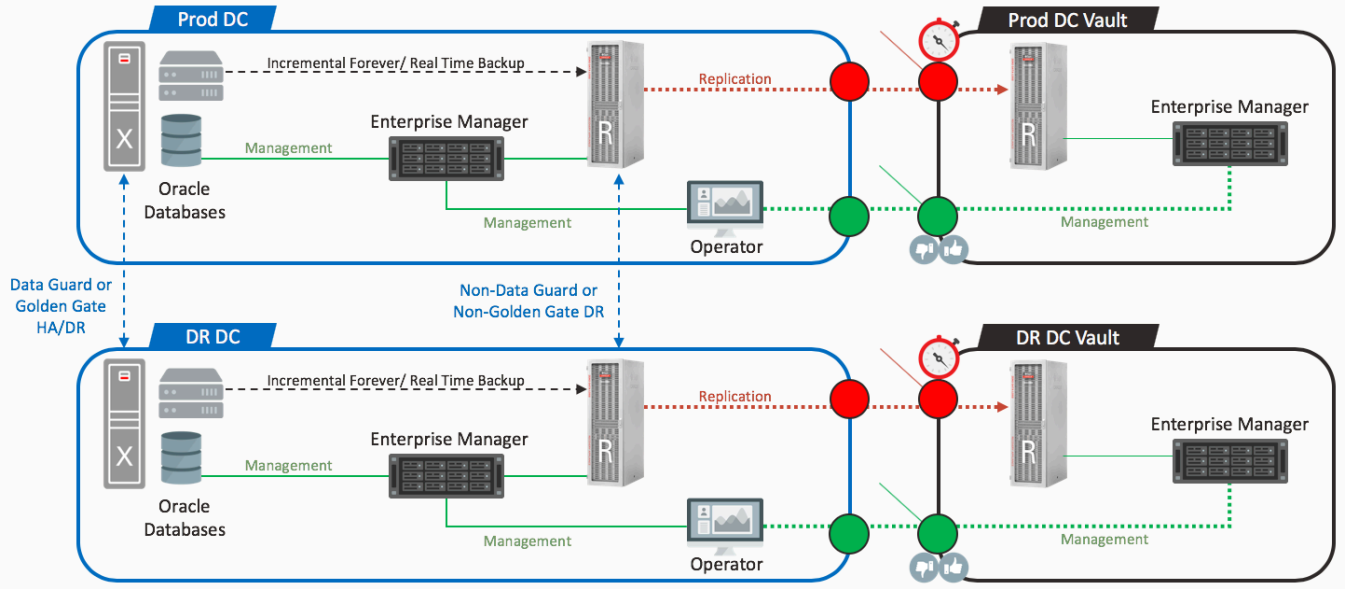

Figure 3 - Recovery Appliance Cyber Security Architecture

Below, the components and functional aspects of the Recovery Appliance cyber security architecture are reviewed with the CIA Triad principles. Some of these are best practices which should already be in place within your data center, but will be reviewed with specific focus on the Recovery Appliance cyber security architecture.

CIA Triad – Confidentiality

Confidentiality from the CIA triad ensures that the data is protected from improper access. Access control and the use of unique accounts are key in the separation of duty described in this section.

[2] https://www.oracle.com/technetwork/database/availability/recovery-appliance-data-guard-2767512.pdf

Separation of Duty

To maintain confidentiality, Recovery Appliance allows administrators to setup separate accounts across the Oracle Database, Recovery Appliance backup, and Cyber Vault environments. This prevents simultaneous deletion of the database and its backups, since two different accounts are setup with different roles. With the addition of the Cyber Vault, there is an added security zone to ensure that the Cyber Vault itself is isolated from tampering.

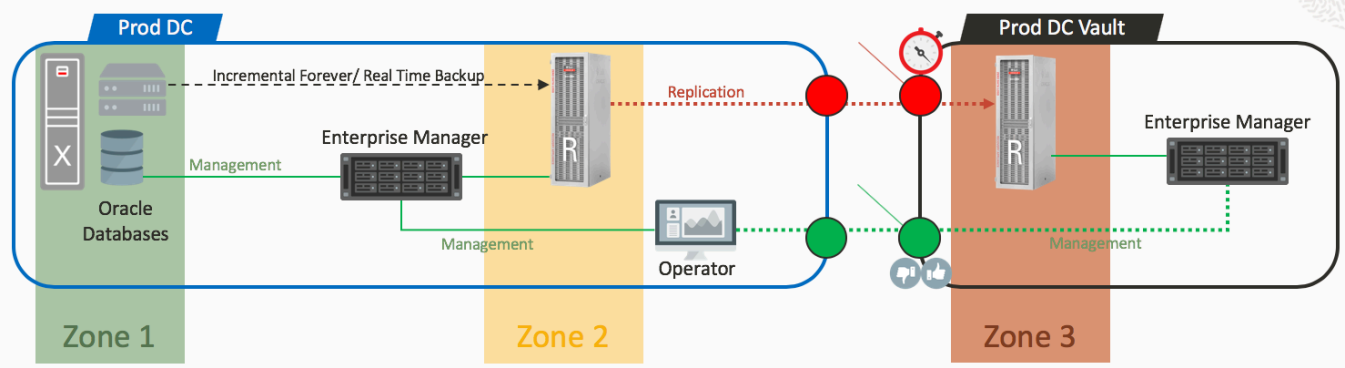

Figure 4 - Recovery Appliance Cyber Security Architecture: Separation of Duty

In this architecture the ability to access, update and make changes is restricted per logical zone. There will be no single account which has access to every zone.

- Zone 1 – Only the Oracle Database administrator can make changes to the databases. They also send the backups and retrieve data for restores via RMAN as a user. There is no administrative access to any Recovery Appliance or the Cyber Vault itself.
- Zone 2 – Recovery Appliance administrators in the production data center can create/edit database protection policies and add/remove Recovery Appliance users for the production data center. They have no access to the Oracle Databases, backup/recovery operations, or the Cyber Vault.
- Zone 3 –Recovery Appliance administrators in the Cyber Vault can create/edit database protection policies and add/remove Recovery Appliance users for the Cyber Vault. They have no access to the databases or the Recovery Appliance in the production data center.

CIA Triad – Integrity

Integrity from the CIA Triad ensures that the data is valid and simplifies management. The sections below describe how the Recovery Appliance provides this functionality.

Validation and Anomaly Detection

To ensure data integrity, the Recovery Appliance has built-in, automated restore validation capabilities that do not rely on connections or user access to an external Oracle Database. Ensuring that backup data is validated is key to being prepared for a future recovery, which means that all data, including TDE databases, must be validated for recoverability at each step of the workflow into the Cyber Vault.

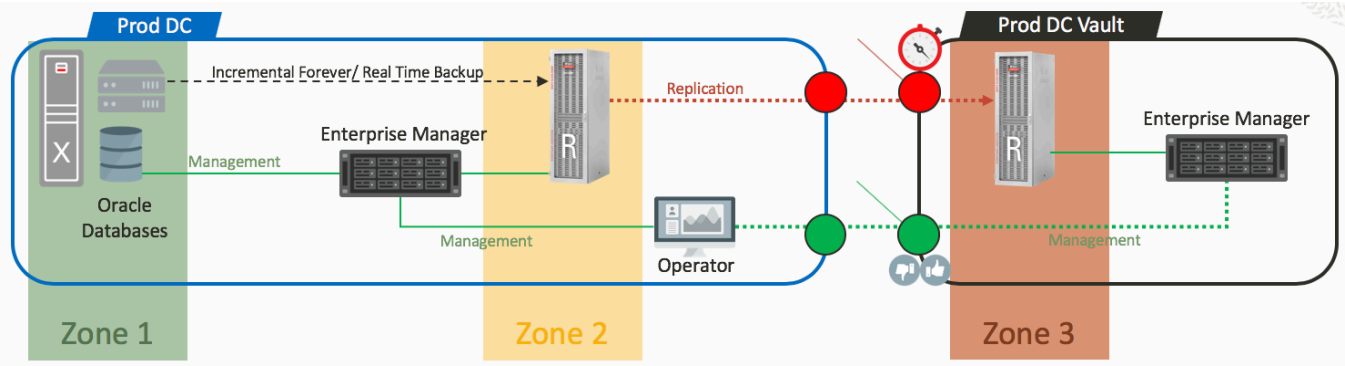

Figure 5 - Recovery Appliance Cyber Security Architecture: Validation & Anomaly Detection

Multi-layer anomaly detection in the architecture ensures that data is valid at all points in the Oracle ecosystem. Each zone indicated above will perform independent checks to prevent invalid or compromised data from entering or exiting the zone and ultimately the Cyber Vault.

- Zone 1 – RMAN will do consistency checks at the database to ensure the backup data is valid before being sent to the Recovery Appliance in the production data center.
- Zone 2 – The Recovery Appliance in the production data center performs checks to ensure that the data is valid and complete.
  - Data is validated when the RMAN database backup arrives on the Recovery Appliance in the production data center.
  - Data replicated from the Recovery Appliance in the production data center is validated again before being sent to the Recovery Appliance in the Cyber Vault.
  - Regular automated validation is scheduled within the Recovery Appliance in the production data center to ensure ongoing validity as the data ages.
- Zone 3 – The Recovery Appliance in the Cyber Vault performs checks to ensure that the data is valid and complete.
  - Data is validated upon arrival into the Recovery Appliance in the Vault from the Recovery Appliance in the production data center.
  - Regular automated validation is scheduled within the Recovery Appliance in the Cyber Vault to ensure ongoing validity as the data ages.

These validation processes are performed automatically and independently on each Recovery Appliance (Production, DR, and Vault) within the environment. If an anomaly is detected during validation, the Recovery Appliance will attempt to automatically remediate the issue. If the automatic remediation fails, the Recovery Appliance will issue an alert to the administrator, who can then work with the production database administrator to halt backups or disconnect the appliance from the network, while the anomaly is investigated.

Compliance and Management Reporting

Oracle Enterprise Manager is the single dashboard for your entire Oracle deployment. In this Cyber Vault architecture, Enterprise Manager is used for management, monitoring and alerting for the Recovery Appliance and for backup automation. This centralized management helps verify the integrity and provide compliance reporting across the entire infrastructure.

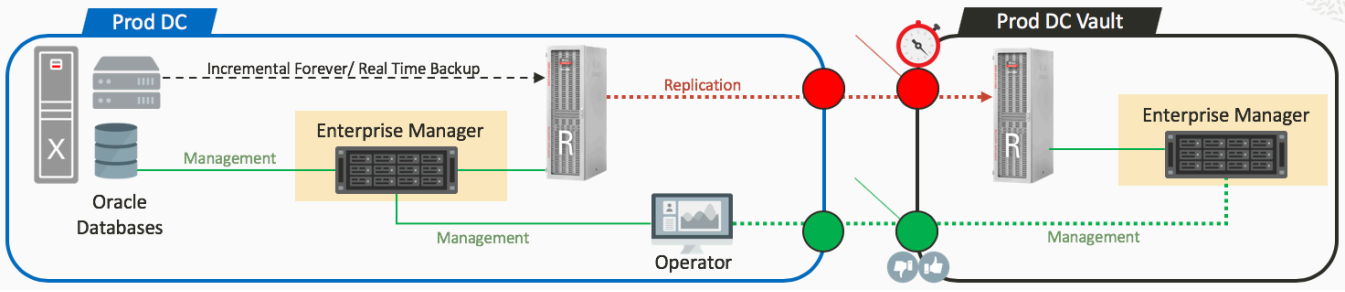

Figure 6 - Recovery Appliance Cyber Security Architecture: Compliance & Management Reporting

Enterprise Manager provides functionality to help you understand the state of backups in production and in the Cyber Vault. These are some highlighted capabilities for scheduling, alerting and real-time monitoring:

- Database Recoverability
- Active System Alerts
- Overall System Activity
- System API Audit History

The Cyber Vault leverages a separate Enterprise Manager installation to ensure that management is isolated. The Enterprise Manager in the production data center has no knowledge of and manages no components in the Cyber Vault. Similarly, the Enterprise Manager in the Cyber Vault has no knowledge and manages no components in the production data center. Regular alerting and reporting from inside the Cyber Vault should be done via one-way SMTP messages from the Cyber Vault.

For an added level of security, the addition of a management network gateway shown in green above should be considered. This management gateway will limit the ability to make management changes to the Cyber Vault environment without the proper change control to open the gateway.

CIA Triad – Availability

Availability from the CIA Triad ensures that the Cyber Vault is ready for a recovery operation. The section describes how update-to-date data retained in the Cyber Vault on a resilient platform is ready for a recovery operation.

Synchronizing the Vault with Latest Backups

The Recovery Appliance real time redo capability produces backups that are always available for the Cyber Vault. This eliminates the troublesome synchronization process with the backup schedule and the Cyber Vault replication network gateway that opens randomly. The most current backup data is automatically transferred to the Cyber Vault the moment the Cyber Vault replication gateway opens.

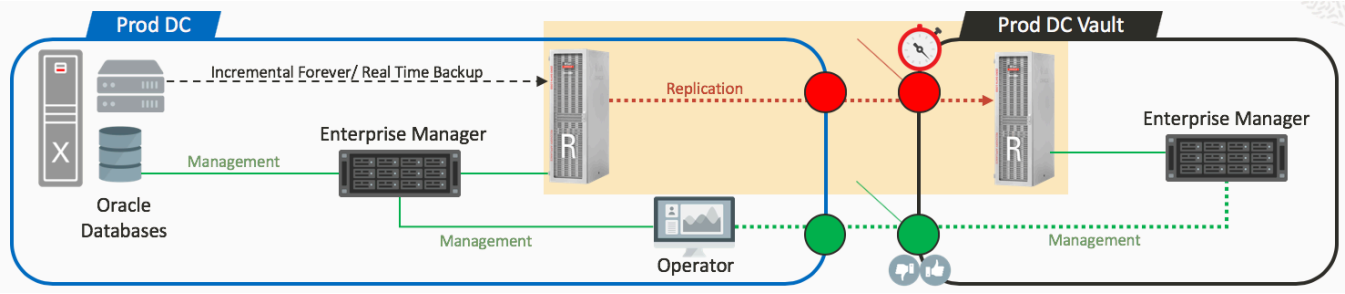

Figure 7 - Recovery Appliance Cyber Security Architecture: Synchronizing the Vault with Latest Backups

This replication network should be an isolated connection between the Recovery Appliance in the production data center and the Recovery Appliance in the Cyber Vault. The replication network gateway should be controlled from inside the Cyber Vault to limit the ability for the Cyber Vault to be compromised from the outside production data center. When the Cyber Vault gateway is opened, the Recovery Appliance will start sending all queued changes since the last Cyber Vault synchronization event to the current time.

The timeframe the Cyber Vault is open should also be as short as possible. The Recovery Appliance leverages incremental forever technology, which will only move the database changes since the last backup into the Cyber Vault, thereby minimizing the amount of time the Cyber Vault has to stay open. To further optimize the workflow, the Cyber Vault opening can be coordinated with the Recovery Appliance replication to ensure the smallest connection window and eliminate errors caused by abrupt network disconnection. These are the high-level steps to coordinate the process:

- Open the replication network gateway between the production data center and the Cyber Vault
- The Cyber Vault resumes the replication from the Recovery Appliance in the data center to the Recovery Appliance in the Cyber Vault
- Monitor the replication tasks for completion on the Recovery Appliance production data center
- When the replication tasks are complete, the Cyber Vault pauses the replication on the Recovery Appliance in the data center
- Close the network connection between the data center and the Cyber Vault

Following these steps will tightly coordinate opening the Cyber Vault gateway and synchronizing the changes between the Recovery Appliance in the production data center and the Recovery Appliance in the Cyber Vault. Otherwise the Cyber Vault gateway timer would arbitrarily keep the Cyber Vault connection open after the Recovery Appliance replication has completed.

Finally, a time-based circuit breaker could also be added to the replication gateway to ensure that the Cyber Vault is not left open longer than allowed by the security rules for your organization. If the Cyber Vault replication network is closed before the synchronization is complete, the Recovery Appliance replication will resume where it left off during the next randomly scheduled Cyber Vault synchronization.

Backup Data Retention

The Recovery Appliance understands the interdependency of the Oracle Database backups. It is more complex than just deleting files based on time in a traditional, non-RMAN aware Cyber Vault solution, since backups often rely on one another to complete the recovery. Just one missing backup piece could mean that recovery to a specified point in time is lost.

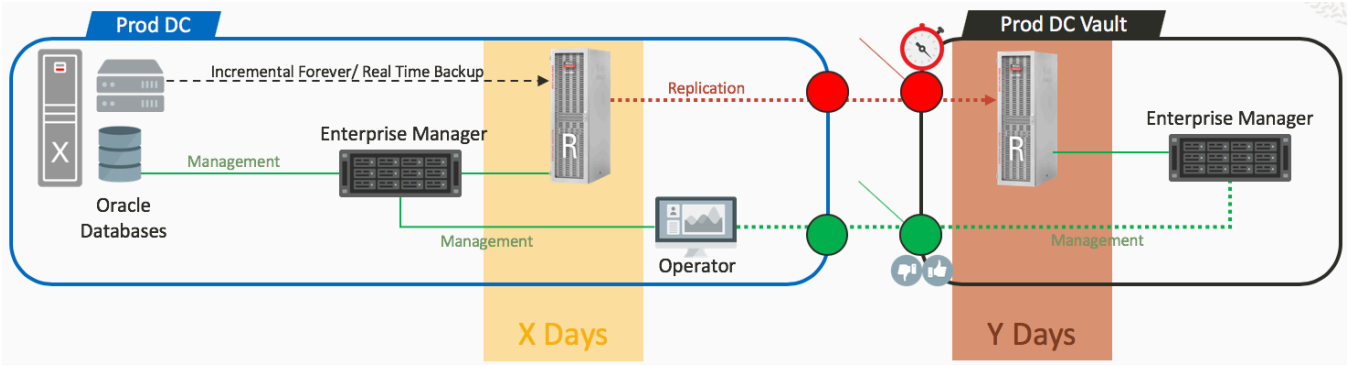

Figure 8 - Recovery Appliance Cyber Security Architecture: Backup Data Retention

Each Recovery Appliance in the environment (Production, DR, and Vault) maintains the defined recovery window with independent retention policies and settings. The Recovery Appliance can manage this data retention without having to leverage a RMAN connection to an external Oracle Database. The DBA does not have the ability to change these policies and can be restricted from deleting any backups on the Recovery Appliance via the appliance administrator setting `ALLOW_BACKUP_DELETION` to `FALSE` in the relevant protection policy.

Data Recovery

The Recovery Appliance can backup and recover data to any platform supported by the Oracle database. This eases the planning required for recovery operations since the data is available for recovery to any known good location during a cyber event.

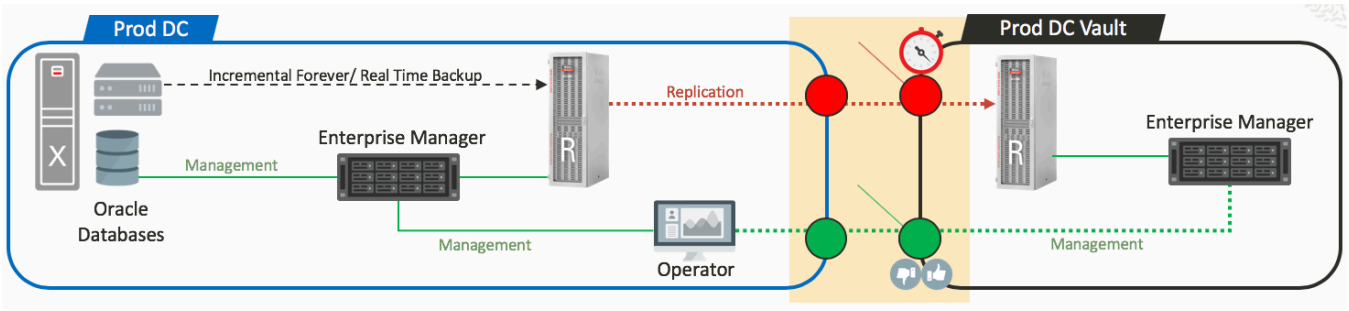

Figure 9 - Recovery Appliance Cyber Security Architecture: Data Recovery

To ensure preparedness for an actual recovery, perform Recovery Manager (RMAN) `RESTORE VALIDATE` and actual restore testing to a predefined known good location. This known good location may be a clean room or an alternate host in your data center. Access to the Recovery Appliance in the Cyber Vault can be limited to the individual database that needs to be recovered, which helps limit overall Cyber Vault exposure. Practicing recovery procedures from the Cyber Vault will ensure the proper steps are established for connecting to the Cyber Vault and retrieving data. Planning and testing your procedure is essential for any recovery during a cyber-attack event.

Cyber Attack Resiliency

Recovery Appliance offers superior resiliency capabilities against cyber-attacks compared to traditional solutions. As an Oracle Engineered System built on the Exadata infrastructure, the Recovery Appliance inherits a resilient architecture for reducing the surface area 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)[3]. The network access protocols into the appliance are also limited to SQL*Net and HTTP(S). To further isolate the network, VLAN tagging is supported, allowing

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

backup/restore traffic to be on non-routable network zones. Finally, the entire Recovery Appliance infrastructure is maintained with a single patch deployment, so all compute, storage, and networking components are patched together, reducing the risk of overlooking a critical security fix for any individual component.

CONCLUSION

Cyber security is a growing conversation which requires additional planning for architecture, isolation and recovery. Starting to plan early will prepare you for the inevitable requirement to protect mission-critical Oracle Databases.

The Recovery Appliance is the premier solution for Oracle Database protection and provides you with essential functionality for a CIA Triad based cyber security design. Adding the Recovery Appliance to your overall cyber solution architecture will:

- Enforce separation of duty across production and Cyber Vault network zones for **Confidentiality**.
- Ensure **Integrity** by performing self-contained validation and anomaly detection on multiple layers, along with end-to-end reporting and alerting across the architecture.
- Ensure that backups are always **Available** for synchronization into the Cyber Vault and available for immediate recovery in case of a production cyber-attack.

FOR FURTHER READING

Database Cyber-Attack Protection with Zero Data Loss Recovery Appliance

(https://blogs.oracle.com/maa/db-cyber-attack-protection-with-zdlra)

This Backup and Recovery blog provides additional highlights for using the Recovery Appliance in a Cyber Security Architecture.

AskTom - ZDLRA Cyber Security Architecture

(https://asktom.oracle.com/pls/apex/f?p=100:551:::NO:RP,551:P551_CLASS_ID:6970&cs=1A7B7BD978C2601B5343F9262A9F958B6)

This AskTom session covers the cyber security architecture in a webcast format with explanations of each concept above.

Zero Data Loss Recovery Appliance Data Sheet

(https://www.oracle.com/technetwork/database/availability/recovery-appliance-ds-2297776.pdf)

The data sheet provides additional operational, sizing and environmental details for the Recovery Appliance.

Managing Recovery Appliance Administrator Accounts

(https://docs.oracle.com/en/engineered-systems/zero-data-loss-recovery-appliance/19.2/ampdb/config_pdb.html#GUID-24DBD077-B1F8-4EE6-9A8F-1CA273197DC2)

This link to the documentation shows how to manage access accounts, which is a key tenant to ensuring separation of duty on the Recovery Appliance.

Pausing Recovery Appliance Replication

(https://docs.oracle.com/en/engineered-systems/zero-data-loss-recovery-appliance/19.2/amagd/amagd_dbms.html#GUID-4443AF42-7726-4AB9-9974-208615D62381)

This documentation link provides information about the procedure `PAUSE_REPLICATION_SERVER`, which will be used to pause replication between the Recovery Appliance in the Cyber Vault and in the production data center. Use of this procedure will optimize the closure process for the Cyber Vault.

Resuming Recovery Appliance Replication

(https://docs.oracle.com/en/engineered-systems/zero-data-loss-recovery-appliance/19.2/amagd/amagd_dbms.html#GUID-696560C2-4872-4D6D-BF8E-E79CA0FA5809)

This documentation link provides information about the procedure `RESUME_REPLICATION_SERVER`, which will be used to resume Recovery Appliance replication when the Cyber Vault is opened. Use of this procedure will optimize the connection time between the Recovery Appliance in the Cyber Vault and in the production data center.

Prevent the Database Administrator from Deleting Backups

(https://docs.oracle.com/cd/E55822_01/AMAGD/amagd_packages.htm#AMAGD1334)

This documentation link describes the procedure `CREATE_PROTECTION_POLICY`, which includes the `allow_backup_deletion` parameter. The `allow_backup_deletion` parameter is used to ensure there is a separation of duty between the database administrator and backup administrator, preventing the databases administrator from deleting backups on the Recovery Appliance.

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

Zero Data Loss Recovery Appliance Cyber Security Architecture
July 2020