TECHNICAL REFERENCE

Oracle Data Management with Rubrik
### TABLE OF CONTENTS

**AUDIENCE** ............................................................................................................................................. 4

**EXECUTIVE SUMMARY** ........................................................................................................................ 4

**CHALLENGES** ........................................................................................................................................ 4

- The Dreaded Day-2 Operations ................................................................................................................ 4
- Balancing Database Performance and Protection ......................................................................................... 5
- Serving the Needs of Secondary Users ......................................................................................................... 5
- The Divide Between DBAs and Backup Administrators .............................................................................. 5

**KEY CAPABILITIES IN RUBRIK FOR ORACLE DATABASE** ........................................................................ 5

- Automated Oracle Data Protection Eliminates the Day-2 Operations Jitter ............................................ 5
- True Incremental Forever Backups Go Easy on Production Host ................................................................ 6
- Rubrik Live Mount Delivers Instant Clones for Secondary Users ............................................................... 6
- Elastic App Service to Promote Co-Stewardship Between DBA and Backup Administrator .................. 6

**INTRODUCTION TO RUBRIK CDM CONCEPTS** .................................................................................. 6

- SLA Domain Policy ........................................................................................................................................ 6
- Envision ......................................................................................................................................................... 8
- Role-Based Access ....................................................................................................................................... 10

**ORACLE DATA MANAGEMENT** ............................................................................................................. 10

- Automated Oracle Data Protection ............................................................................................................... 10
- Protecting Oracle Databases with the Automated Oracle Data Protection .................................................. 10
  - Setup ....................................................................................................................................................... 10
  - Auto Discovery ................................................................................................................................. 12
  - SLA Domain Assignment ...................................................................................................................... 14
  - Oracle Backup Workflow ...................................................................................................................... 16
  - Archive Log Backups ............................................................................................................................ 16
  - Restoring Oracle Databases with Rubrik ............................................................................................... 17
  - Export .................................................................................................................................................... 18
  - Instant Recovery ................................................................................................................................. 20
  - Live Mount .......................................................................................................................................... 21

- Elastic App Services .................................................................................................................................... 22
  - Protecting Oracle Databases with Elastic App Services (Managed Volumes) .................................... 23
  - Setup ....................................................................................................................................................... 23
  - SLA Domain Assignment ....................................................................................................................... 25
  - Oracle Host Configuration ..................................................................................................................... 26
  - Oracle Backup Workflow ....................................................................................................................... 28
  - Restoring Oracle Databases with Elastic App Services .................................................................. 29
  - Restoring from a Managed Volume or Snapshot ............................................................................. 29

- Choosing Between Automated Oracle Data Protection and Elastic App Service .................................. 30
TABLE OF CONTENTS

CONCLUSION....................................................................................................................................... 31
ABOUT THE AUTHORS....................................................................................................................... 31
APPENDIX A: EAS MOUNT OPTIONS.............................................................................................. 32
AUDIENCE
This technical reference is intended for architects and administrators designing data protection, copy data orchestration, and compliance solutions for Oracle databases. This paper will provide a feature walkthrough with relevant use cases on how Rubrik Cloud Data Management may be used for protecting Oracle databases running on physical systems and virtual machines.

EXECUTIVE SUMMARY
Oracle databases are often the driving force behind an organization’s most critical applications - providing a performance driven, relational storage for key transactions. For this reason, businesses cannot afford downtime when it comes to their Oracle database environments.

Rubrik Cloud Data Management (CDM) delivers enterprise grade data protection and DevOps centric automation for Oracle databases. For those organizations looking for a simple, hands off approach to Oracle protection, Rubrik provides Automated Oracle Data Protection. Automated Oracle Data Protection allows automatic discovery of Oracle databases to be coupled with the simplicity of Rubrik SLA domain assignments, completely eliminating the need to manage any RMAN scripts or catalogs. Automated Oracle Data Protection also provides value-add Rubrik benefits such as Automated Live Mount and Instant Recovery to bring near-zero recovery times to Oracle databases.

Elastic App Services (EAS), another Oracle backup technology within Rubrik, can be used for provisioning application aware, dedupe enabled storage for Oracle hosts, allowing Database Administrators (DBAs) the comfort of utilizing native Oracle RMAN toolsets for fast backup and restore operations. EAS also takes full advantage of Rubrik’s SLA policy-based architecture, granting backup administrators a simplistic approach to maintain compliance around any long-term retention and archival requirements.

CHALLENGES
Oracle has long provided a high performing, scalable database solution for organizations to build their business applications. For these reasons, many organizations have chosen Oracle to run their most mission critical applications. As a result, it is imperative for stakeholders in the organization, especially, the database administrator (DBA) to make sure that the Oracle database is not only made highly available, but the data within is also protected against media corruption, user induced errors, and noncompliance. This is why Oracle DBAs take data backup very seriously.

Oracle Recovery Manager (RMAN) is built into Oracle database to provide data backup and recovery. However RMAN by itself can be challenging for DBAs responsible for managing a large number of databases. There are 4 key challenges DBAs face today.

THE DREADED DAY-2 OPERATIONS
Oracle’s RMAN has beyond doubt been the tool of choice for DBAs when it comes to backup and recovery of their databases. Seasoned DBAs may be comfortable to build impeccable scripts to handle the situation in hand for the Day-0 and Day-1, but the problem is in maintaining and managing those across multiple databases, adapting to changes in topology, orchestrating across application stacks and ensuring compliance needs of the business. DBAs prefer to offload database backups to a central backup system so that they can
focus on running the database to meet the business application needs. Thus, the dreaded Day-2 operations need to be managed by backup systems.

**BALANCING DATABASE PERFORMANCE AND PROTECTION**

While data protection is essential, the constant hit on database server by backup tasks may affect its performance. The backup operations can easily consume one CPU core per RMAN channel. If full backups are needed to run on a regular basis, and multiple channels needed to be used for high speed backups - the DBA is forced to make the difficult tradeoff between backup performance and database performance. As modern, global applications are running 24/7, expanding backup windows affect both recoverability and productivity.

**SERVING THE NEEDS OF SECONDARY USERS**

A typical day of an Oracle DBAs life doesn't go by without a steady stream of requests from developers, quality assurance teams, and analytics departments looking to gain access to copies of production data for secondary use cases such testing, development and ETL (extract, transform, load) workflows. Often times, the same production database is hit multiple times by secondary workflows and may run for days on end. The DBA needs to be on top of managing SLAs for different departments while also acting as the custodian for the mission critical databases serving the business.

**THE DIVIDE BETWEEN DBAS AND BACKUP ADMINISTRATORS**

Backup administrators often handle the complete protection lifecycle of an organization’s applications, from the backup and restore to the compliance and governance policies set forth by the business. The one thing that seems to break this holistic approach is Oracle database. While a DBA may be open to handoff Day-2 protection tasks to backup administrator, the responsibility still falls on DBA to build the right set of RMAN scripts and to maintain/update those scripts as the database environment changes. This often results in contention as the chance of human error (e.g. DBA forgetting to notify a change to backup admin, backup admin needing to run an immediate backup before an upgrade but forgetting to notify DBA) is high. Oracle database schedules and schedule changes often override everything else because of its mission critical nature, and backup admins may be forced to work around those schedules for the rest of workloads.

**KEY CAPABILITIES IN RUBRIK FOR ORACLE DATABASE**

Before diving deeper into the Oracle Data Management solutions supported by Rubrik, this section will provide a brief overview of key capabilities we designed to eliminate the challenges described in the earlier section.

**AUTOMATED ORACLE DATA PROTECTION ELIMINATES THE DAY-2 OPERATIONS JITTER**

Rubrik’s Automated Oracle Data Protection, introduced in Rubrik CDM 5.0 fully automates Oracle RMAN workflows. Once Rubrik Backup Service (RBS) is installed on an Oracle host or node, all the Oracle databases are automatically discovered and displayed in Rubrik’s web console. Protecting Oracle is now a matter of selecting the desired level of the object (Oracle Real Application Cluster, Oracle Host or a specific Oracle database) and assigning a business SLA. The necessary RMAN scripts are generated during run time so that SLAs dynamically protect newer databases appearing on hosts, thereby taking the stress out of Day-2 operations.
TRUE INCREMENTAL FOREVER BACKUPS GO EASY ON PRODUCTION HOST

Oracle’s Incremental Merge capability is coupled with Rubrik’s revolutionary blob engine to deliver true incremental forever backups at scale for Oracle database, even when you need to retain backups for years. If available, Rubrik will also take advantage of Oracle block change tracking (BCT) during backups so that it no longer needs to scan the entire database for incremental changes. Thus, after the first backup, the DBA never needs to worry about long backup windows negatively affecting performance and productivity of the database.

RUBRIK LIVE MOUNT DELIVERS INSTANT CLONES FOR SECONDARY USERS

Live Mount for Oracle databases deliver near-zero RTOs with instant recovery and live migration. In addition, DBAs can provide instant clones to developers, accelerating application development, testing and ETL (extract, transform, and load) workflows without any impact to production environments.

ELASTIC APP SERVICE TO PROMOTE CO-STEWARDSHIP BETWEEN DBA AND BACKUP ADMIN

With Elastic App Service, backup admins can delegate backup and operational recovery tasks to DBAs, so that DBAs can use existing RMAN workflows. Rubrik delivers high data reduction and immutability without draining compute resources, even in the cloud. Alternatively, granular role based access control and multi-tenant capabilities of Rubrik within its automated data protection may be used for delegating the backup controls for those mission critical databases to back to DBAs.

INTRODUCTION TO RUBRIK CDM CONCEPTS

The following section will review various concepts and components available within Rubrik CDM assisting with Oracle Data Management.

SLA DOMAIN POLICY

A Rubrik SLA Domain Policy is a declarative policy that captures the core objectives for backup and recovery. It eliminates the need to manually configure jobs, tasks, and other items for various object groups. SLA Domain Policies are a core part of the Rubrik architecture and extend across all data types, as shown below.
Let’s walk through the pieces needed to configure an SLA Domain Policy for any object (Oracle specific items will be covered in the next section):

- **Backup Frequency:** this is also known as the Recovery Point Objective (RPO). Simply put, how often are backups taken?
  - For databases, this determines how often a database restore point is synthesized from incremental blocks.

- **Availability Duration:** this is also known as retention: how long are backups retained?
  - For databases, retention times may often be shorter than for other data types unless needed for regulatory or compliance reasons.

- **Archival Policy:** this policy specifies when and where to archive the data. It determines the retention period and where the data is stored during that period. Archive targets can be public cloud (AWS, Azure, or GCP) or on-premises (AWS S3 compatible object stores, NFS, or tape). The policy dictates which archive target is used and when archives are maintained solely in the cloud. If archives are maintained solely in the cloud (past 30 days for instance), the RTO is longer, as the data must be moved back to the Rubrik cluster.
  - For databases, long-term archive required for regulatory or compliance reasons can be stored in a cloud archive.

![Service Level Agreement](image-url)

**Service Level Agreement**

Choose how often we take snapshots and the length of time we keep them.

<table>
<thead>
<tr>
<th>Take Snapshots:</th>
<th>Keep Snapshots:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Every (Hours)</td>
<td>3 Days</td>
</tr>
<tr>
<td>4</td>
<td></td>
</tr>
<tr>
<td>Every (Days)</td>
<td>32 Days</td>
</tr>
<tr>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Every (Weeks)</td>
<td>12 Weeks</td>
</tr>
<tr>
<td>1 Friday</td>
<td></td>
</tr>
<tr>
<td>Every (Months)</td>
<td>4 Quarters</td>
</tr>
<tr>
<td>On</td>
<td>Begin Quarters in</td>
</tr>
<tr>
<td></td>
<td>January</td>
</tr>
<tr>
<td>Every (Quarters)</td>
<td>7 Years</td>
</tr>
<tr>
<td>1 Last day of the year</td>
<td>January</td>
</tr>
<tr>
<td>Every (Years)</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>

Local retention set to 7 years.
• **Replication Policy:** this relates to disaster recovery (DR). Effectively, how long should data be kept at a DR site?
  - For databases, this often is a shorter time frame. In a DR situation, recovery of the most recent state of a database is most common. This policy section allows cost savings by storing only a recent subset of data at a DR site.

SLA Domains may be placed on the Oracle host or RAC cluster or applied per database. If placed at the host/RAC level, the subordinate databases will inherit the SLA Domain.

As illustrated by the screenshots above, the policy architecture is straightforward to configure, yet powerful. Please see the Rubrik User Guide for a more thorough walkthrough of SLA Domain details.

**ENVISION**

Rubrik Envision, a customizable visual analytics and reporting tool meets the diverse reporting needs of Rubrik customers. Users can create a variety of reports by selecting specific attributes and measures, as well as by defining any relevant filters. Reports may be saved in the Report Gallery and sent out via email periodically.

Collectively, these reports help customers optimize operations, enhance capacity and performance, plan for growth, and track compliance.

A report contains attributes and measures. Attributes describe the objects being reported upon. For example, the “Name” attribute could describe the name of a specific workload. Measures are quantitative measurements. For example, the “Duration” of a data protection task could describe how long the task took to complete.
In a given report, the measures define what the user is interested in viewing. The attributes describe how the measures will be broken down to categorize and contextualize the data. Finally, filters determine the data that is considered to compute the report's measures.

The following table gives an example of an Envision report that an Oracle DBA may generate. The report is intended to provide Protection Task Details.

<table>
<thead>
<tr>
<th>Chart 1</th>
<th>Daily Protection Tasks by Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attributes</td>
<td>Task Type</td>
</tr>
<tr>
<td>Measures</td>
<td>Task Count by Status</td>
</tr>
<tr>
<td>Chart Type</td>
<td>Stacked Horizontal</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chart 2</th>
<th>Failed Tasks by Database</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attributes</td>
<td>Object Name</td>
</tr>
<tr>
<td>Measures</td>
<td>Failed Tasks</td>
</tr>
<tr>
<td>Chart Type</td>
<td>Vertical</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table</th>
<th>Protection Tasks Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attributes</td>
<td>Task Status, SLA Domain, Task Type, Object Type, Location, Object Name</td>
</tr>
<tr>
<td>Measures</td>
<td>Start Time, End Time, Duration, Data Transferred, Data Stored, Dedupe Ratio, Logical Dedupe Ratio</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Filter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date</td>
</tr>
<tr>
<td>Task Status</td>
</tr>
<tr>
<td>SLA Domain</td>
</tr>
<tr>
<td>Object Type</td>
</tr>
<tr>
<td>Location</td>
</tr>
<tr>
<td>Object Name</td>
</tr>
<tr>
<td>Cluster Location</td>
</tr>
<tr>
<td>Task Type</td>
</tr>
</tbody>
</table>
ROLE-BASED ACCESS

Rubrik provides granular control along with integration into existing directory services (Active Directory) to make Rubrik a natural fit for multi-tenant environments.

It is possible to logically partition and secure customer environments in a multi-tenant fashion. This is achieved by the concept of having a central organization with the ability to procure resources on behalf of tenant organizations. An organization is created and managed by a Global Admin who has the power to assign a subset of the privileges to an Organization or Org Admin.

There are multiple Rubrik resources managed within an organization such as SLA domains, fileset templates, archival and replication targets, and protected objects (virtual machines, SQL databases, Oracle databases, Windows / Linux hosts, NAS shares, and Managed Volumes). On top of that, you can use the Role-Based Access Control (RBAC) privileges to provide granular privileges.

As an example, a Database Administrator persona may be created with the ability to manage, protect, and recover selected Oracle databases. This can then be granularly scoped to include only specific databases.

ORACLE DATA MANAGEMENT

Rubrik provides two methods of protecting Oracle databases, both of which utilize native RMAN tools to generate and restore backups.

AUTOMATED ORACLE DATA PROTECTION

Automated Oracle Data Protection extremely simplifies applying data protection policies around Oracle databases. Leveraging the Rubrik Backup Service (RBS), a small, lightweight agent installed on either Linux or UNIX hosts, Rubrik is able to auto discover all of the Oracle real application clusters, hosts, databases and tablespaces within the environment. From there, Rubrik’s intelligent and automated SLA policy engine works to protect Oracle environments at any level - RAC, host or database. Rubrik’s Automated Oracle Data Protection provides a very low barrier to entry as it pertains to Oracle Data Management - there is no need to understand the complexities of RMAN, nor manage large and complex RMAN recovery catalogs. Once the data has landed on the Rubrik cluster, DBAs and Backup Administrators are granted the same fast and efficient recovery processes which they are used to with Rubrik, including the ability to Live Mount multiple point in time copies of their Oracle Databases and perform Instant Recovery and Live Migration - ensuring organizations are able to recover from an outage in a near instant fashion.

Protecting Oracle Databases with the Automated Oracle Data Protection

The following will go through the protection and restoration processes of using the Rubrik’s Automated Oracle Data Protection in detail:

Setup

Rubrik supports Oracle 11GRI and above for use with Automated Oracle Data Protection, installed on both standalone servers and Real Application Clusters (RACs) configured with shared storage.

To provide integrated Oracle functionality, Rubrik utilizes the Rubrik Backup Service (RBS), an non-intrusive agent which has been signed and configured to only communicate with its associated Rubrik cluster. RBS requires no reboot upon installation, and is able to auto-update without intervention.

RBS may be downloaded directly from within the Rubrik cluster UI by navigating to Servers & Apps -> Oracle DBs. The dialog presented provides download access for RBS in both rpm and deb packaging, as well as associated rpms
for the supported AIX versions. It should be noted that once installed RBS is only used for automated database
discovery and to orchestrate various backup and restore workflows. The streaming of data, still handled natively by
RMAN, is configured to output to NFS exports pointing to the Rubrik cluster. For these reasons, an NFS Client and
NFS Utilities must also be available on the Oracle host.

Note: If using Oracle Real Application Clusters (RAC), the RBS must be installed on all nodes within the cluster in order to
provide automated discovery.

Once RBS has been installed, the process of adding the Oracle host to the Rubrik cluster can be continued (Servers &
Apps -> Oracle DBs). Adding an Oracle host to a Rubrik cluster requires the following:

- The IP or Hostname of the Oracle host being added.
- A OS DBA user with SYSDBA privileges. This user is used to query databases for auto discovery and perform
  various database level activities. The user is configured on a per-host basis and by default attempts to use the
  “oracle” user.
**Note:** The Operating System DBA user can be modified any time by editing the Oracle host within the Rubrik cluster.

### Auto Discovery

RBS is required in order to perform automated discovery of Oracle hosts, RAC, and databases. Once RBS has been installed and the Oracle host has been added to the Rubrik cluster, the databases and associated database metadata is discovered and the list of running instances and tablespaces is auto discovered. In order for databases to be automatically discovered they must be in an **OPEN** or **MOUNTED** state and must be listed within the `/etc/oratab` file. If using RAC with Automated Storage Management (ASM) an entry must exist for the `GRID_HOME` in the `/etc/oratab` file.

**Note:** If no databases happen to exist on the Oracle host, an empty `/etc/oratab` file with the proper permissions must be created in order to add the host to the Rubrik cluster.

The Oracle hosts and databases can be shown in two different views within the Rubrik cluster. The **Hosts/Clusters** view organizes the Oracle inventory grouped by either standalone Oracle hosts or RAC clusters. Selecting the name of either a host or cluster will subsequently provide further detail around the selected object.
The **All DBs** view displays a complete list of every Oracle database known to the Rubrik cluster, along with their corresponding number of instances and tablespaces. Selecting the name of a database will display the respective database overview page.
SLA Domain Assignment

SLA Domain Policies can be applied at the Oracle host/RAC Cluster or database level. The following visual walkthrough illustrates this concept and showcases how simple it is to configure the Oracle specific options.

A list of auto-discovered Oracle inventory at the server level:

![Image of Oracle inventory list]

Database level visibility is also available.

![Image of Oracle inventory list]

**Note:** SLA Domains are inherited from their parent objects. For instance, if an SLA domain is assigned at the Oracle host level, all subsequent databases on that host will receive the same SLA domain. The inherited policy may be overridden by assigning another policy directly on one of the child items.
Selecting either a host, cluster, or database and selecting **Manage Protection** will allow the selection of an SLA Domain policy. In addition, frequency and retention of the Oracle archive log backups are required in order to successfully recover an Oracle database.

**Note:** Since Rubrik uses both full database and archive logs to perform database restorations, the Oracle archive log retention is required before an SLA Domain can be applied. Without an archive log backup schedule, the database will remain greyed out within the Rubrik UI.

The **Advanced Settings** dialog allows for the determination of the number of RMAN channels to configure and use during the backup process. An RMAN channel represents one stream of data from the Oracle host. While Oracle recommends utilizing one channel per CPU core, the Rubrik cluster will balance channels across all of the nodes within the cluster. Hence it is recommended that the number of channels be the lower of either the number of cores on the Oracle host or the number of nodes in the Rubrik cluster.

Advanced Settings also allow for setting priority of RAC nodes which will process backups. Rubrik will attempt to use the highest ordered node to process a backup. In the event that this node is unavailable the next node in the list will be utilized, and so on, and so forth. This allows DBAs the ability to dedicate certain nodes to be used just for backup, ensuring other nodes, which may be serving production data, are not impacted during backup events.
Oracle Backup Workflow

In order for an Oracle backup to take place, the following prerequisites must be met:

- RBS is installed and configured to run under an account with **SYSDBA** privileges.
- Oracle database is in an **OPEN** or **MOUNTED** state.
- Oracle database is listed in the `/etc/oratab` file.
- **ARCHIVELOGMODE** is enabled on the Oracle database.

Once all prerequisites are met, Rubrik will proceed with the backup processes. There are two separate jobs which run on the Rubrik cluster to process the backup of an Oracle database, Database backups and Archive Log backups. These processes run separately and at different times from each other. Rubrik handles the scheduling and maintenance of all their associated tasks.

Database backups are governed by the backup frequencies and retentions set forth within the assigned SLA Domain and are created using RMANs incremental merge setting. While only needing to transfer the incrementally changed data, the deltas are merged with the previous restore point to create a conceptual full backup for the new restore point.

Archive Log Backups

Archive log backups are completely separate form the database backups and are governed by the frequencies and retentions configured within the Log backup settings of the applied SLA Domain. Unlike database backups, each log backup is completely independent from the previous backup as there is no concept of incremental when parsing Archive Logs. Once the RMAN log backup has been completed, the archive logs are then deleted from the source host.
Rubrik will automatically manage the archive logs, associating them with the respective database backups so that DBAs do not need to manually manage the backup processes.

**Restoring Oracle Databases with Rubrik**

When it comes to restoration of databases, DBAs often need to recover to an exact point in time. Simply restoring a daily backup is not sufficient when dealing with high-transactional, constantly changing databases, and can result in lost productivity and more drastic, lost data. This is why Rubrik parses archive log backups alongside the full database backups, allowing for DBAs and backup administrators to simply select nearly any point in time during the backup retention period as shown below.

The process of restoring an Oracle database to any point in time is accomplished by first restoring the closest preceding full database snapshot before the selected recovery point, and then applying the appropriate archive logs to essentially move that database forward until the recovery point is reached. As shown below, to support the selected restore point, first the database backup at S2 will be restored, and then archive logs 4, 5, and 6 will be applied. This process is completely orchestrated by Rubrik.

Once a point in time for recovery has been selected with Rubrik, the ellipsis menu can be used to display the associated recovery methods.
There are three recovery options for Oracle databases: Export, Instantly Recover, and Mount.

**Export**

The Export option within Rubrik allows for an entire Oracle database or tablespaces to be restored to a target host. The datafiles, log files and other parameter files are copied from the Rubrik cluster to the target to perform database recovery.

**Note:** The term Export in the Rubrik UI means restore, and should not be confused with export known to Oracle DBAs use in data pump workflows.

In order to perform an Export with Rubrik the following prerequisites must be met:

- The target Oracle RAC, RAC node or standalone host must have RBS installed and must be registered within the Rubrik cluster.
- The source and target must have the same $ORACLE_HOME definition and be running identical Oracle versions.
- To support RAC export, the oratab must have the ASM grid configuration for the RAC.
- There must not be an instance on the target with the same database SID as the export option creates a database with the exact same name and SID.
- Enough resources (capacity, memory, compute) must be available on the target host to run the database and perform the recovery.

Export can be performed in two different modes: Automated and DBA Managed.
Automated Export

During an automated export Rubrik will completely restore the Oracle database files, and recover the database. On top of simply moving the data, Rubrik will also create and startup the database instances, updating the local `oratab` file with the proper information for the newly restored database. It should be noted that Automated Export doesn’t support restorations to the same Oracle host in the initial release. To do this, the DBA Managed Export should be utilized.

![Automated Export Diagram]

**DBA Managed Export**

During a DBA Managed Export, rather than completely restoring a database to an Oracle host, Rubrik will only copy the database files to a specified location and expose the RMAN recovery scripts. This provides flexibility to the DBA, allowing for the creation of customized RMAN scripts to recover from the exposed backup images. This also allows for the DBA to maintain complete control over the recovery process and utilize any advanced RMAN recovery options such as block level recovery if they wish to do so. DBA Managed Exports are supported on both alternate and the same Oracle hosts.

![DBA Managed Export Diagram]
The process of performing an Export is as follows:

1. A point-in-time is selected for recovery and the Export option clicked.
2. RBS executes the RMAN scripts generated by Rubrik and restores the selected database.
3. Restored database is added to `/etc/oratab`.

### Tablespace Exports

Aside from completely exporting a database, Rubrik can also export individual tablespaces back to the original Oracle host. Tablespaces bring benefits such as quotas, performance, capacity allocation; however, in terms of data management, the main benefit is tablespace exports allow DBAs to restore only certain portions of the database without having to take the complete database offline.

The following applies to the exporting of tablespaces with Rubrik:

- **SYSAUX, SYSTEM, and UNDOTB** cannot be restored at the tablespace level.
- Before recovery takes place, the targeted tablespace must be manually dropped.
- Enough resources (capacity, memory, compute) must be available on the original Oracle host to perform the recovery. RMAN will create an auxiliary database during recovery, storing control files temporarily on the host in order to extract the desired tablespace.

### Instant Recovery

While the Export option performs a traditional type restore, creating a database by copying data from the Rubrik cluster to an Oracle host, the Instant Recovery option does this without the need to copy all of the associated data. Instead, Instant Recovery utilizes the storage on the Rubrik cluster to host the Oracle datafiles, while all other components are restored to the original Oracle location. This allows for a much faster recovery after a complete database failure, allowing DBAs to reach a near instantaneous RTO and granting access to a recovered database in a smaller amount of time no matter the size of the database. Once a database has been instantly recovered, DBAs can simply migrate the datafiles from the Rubrik cluster back to the storage of their choosing by utilizing native SQL commands such as `MOVE DATAFILE`.

**Note:** Instant Recovery has the potential to be a destructive operation, therefore Rubrik will instruct DBAs to manually drop the original database before proceeding. Rubrik safeguards accidental Instant Recovery by throwing an error if it is attempted while the original database still exists.

Depending on the registration status of the Oracle host within the Rubrik UI, Instant Recovery will be issued from either the **Database Overview** page or the **Relic (Snapshot Management)** page. The process to complete an Instant Recovery within Rubrik is as follows.

1. A point-in-time is selected for recovery and the **Instant Recovery** option clicked.
   - If the original database still exists, the UI will not proceed until the original database is dropped. Once dropped, a host refresh will need to be initiated.
2. Rubrik will restore all the database components required to create a database on the original Oracle host, leaving the datafiles on the Rubrik cluster.
3. Oracle datafiles for the restored database are served from the Rubrik cluster in a RW copy of the backup image. The original backup image remains in a read-only state.

While instant recovery grants DBAs a near-zero RTO by not having to copy datafiles, the end goal is to remove the storage dependency on the Rubrik cluster and migrate all data back to the Oracle storage. To do this, DBAs can use the native `ALTER DATABASE MOVE DATAFILE` command included in Oracle 12c and higher to live migrate the datafiles from the Rubrik cluster to a production storage location of their choosing, at a time of their choosing. For Oracle version before 12c, the database will need to be taken offline in order to process the migration, however the DBA maintains control of when they want this to happen.

**Live Mount**

The Rubrik Live Mount recovery option is similar to that of Instant Recovery, however rather than creating the database on the original Oracle host, any registered Oracle host may be utilized. This allows for many duplicate point-in-time copies of the original database to be created, without affecting the original database at all. Like Instant Recovery, only non datafile components are restored to an Oracle host, meaning these duplicate point-in-time copies can be created in a nearly instantaneous fashion. Live Mount point-in-time copies enable many different use-cases such as testing and development, quality assurance, ETL, and even granular item-level recovery using Oracle data pump.
The process of performing a Live Mount within Rubrik is as follows:

1. A point-in-time is selected for recovery and the Live Mount option clicked.
2. Rubrik creates and executes the scripts required to perform the Live Mount.
3. The database structure is created on the target node, while the datafiles remain on the Rubrik cluster.
4. The database is added to `/etc/oratab` on all target nodes.

Upon completion of testing, the database can be unmounted within Rubrik. During an unmount operation any changed data is discarded and the space is reclaimed on the Rubrik cluster.

**ELASTIC APP SERVICES**

While Rubrik’s Automated Oracle Data Protection provides an automated, simple, and intuitive way to provide Oracle Data Management, there may be times when DBAs want to continue using their current backup and restore processes, yet leverage the efficiencies around deduplication, archival, retention and replication that Rubrik provides. For this situation, a second type of Oracle Data Management exists: Elastic App Services (EAS).

EAS provides an immutable, storage-efficient, highly available distributed storage repository as a target for DBAs to place existing established backup process on. While appearing to the target as a simple storage volume, EAS reside on the Rubrik CDM platform, providing all of the same data management fundamentals as any other protected object such as:

- **SLA Domain Policy based protection**: EAS volumes can be assigned to an SLA Domain. While the DBA maintains control over the RMAN retention, Backup Administrators are able to assign volumes to an SLA Domain enabling daily, weekly, monthly, quarterly, and yearly snapshots to be maintained. This enables the DBA to leverage RMAN for fast, more recent restores while still complying with governance or long term retention policies set forth by the organization.
• **Archiving**: Easily manage long-term retention of Oracle database backups by aging out older backups and archiving to the public cloud or on-prem object/nfs storage.

• **Replication**: Provides asynchronous replication of Oracle database backups from one location to another allowing near instant recovery at an additional site without having to wait for data rehydration.

• **Immutability**: Once data has been ingested to the Rubrik cluster it remains in an immutable state. This prevents events like ransomware attacks from changing or encrypting backups along with production data.

**Protecting Oracle Databases with Elastic App Services (Managed Volumes)**

The following will go through the setup and configuration of an Elastic App Services Managed Volume for Oracle Data Management in detail.

**Setup**

The process of configuring EAS begins with the creation of a Managed Volume on the Rubrik cluster. A Managed Volume is fixed volume of storage, which can be expanded online at any time, presented to the Oracle host over either NFS or Secure SMB. If using NFS, client names and subnets can be specified to further secure the exported volume. If using SMB, security is handled by domain, usernames, and permitted IP addresses. Also during the creation of the Managed Volume an application tag is applied. Rubrik uses this application tag to provide the most efficient type of deduplication and compression for the volume. If the application tag is omitted or set to Other, a blind, catch all deduplication will be performed. The current application tags available are as follows:

- **Oracle Incremental Merge** - Recommended for most organizations due to its incremental forever approach which reduces backup windows and enable a cost effective approach for utilizing cloud storage for long-term archive.

- **Oracle Backup Set** - For customers wishing to stick with traditional RMAN Backup Sets the Oracle Backup Set may be utilized.

- **SAP HANA**

- **Microsoft SQL Server**

- **Datos IO**

- **MySQL**

- **PostgreSQL**

If utilizing RMAN parallelism, the number of channels is able to be configured during the creation process.
For more information around Elastic App Service and Rubrik see the Elastic App Service overview.
**SLA Domain Assignment**

SLA Domain Policies can be applied at the Managed Volume level within the Rubrik cluster. The following visual walkthrough illustrates this concept and showcases how simple it is to configure and assign an SLA Domain to a Managed Volume.

Once created, the Managed Volume may be assigned to an SLA Domain by selecting Manage Protection.

Depending on the type of RMAN backup utilized, the relationship between the frequency and retention within RMAN backups and the frequency and retention within the SLA Domain may need to be examined. The RMAN frequency can be configured to be more frequent, but never less frequent than that of the SLA Domain base value. The following outlines well matched RMAN and SLA Domain settings:

- RMAN frequency set to take daily backups with seven days retention utilizing Incremental Merge.
- SLA Domain frequency set to take daily backups with 31 days retention.

In this case, the Rubrik cluster will retain a daily snapshot for 31 days of the Managed Volume. Each daily snapshot will contain the most recent 7 days of RMAN incremental merge backups on the day the snapshot was taken. During a restoration process, the DBA will be presented with the most recent 7 days of backups to the point-in-time selected.
Oracle Host Configuration

The following section will outline various requirements that must be performed on the Oracle host to begin using Managed Volumes as a target for RMAN backups.

Mounting Managed Volumes

In order to begin using a Managed Volume as a target for RMAN backups, the exported channels must be mounted on the Oracle hosts file system. The exported channels are retrieved from the Managed Volume overview card by clicking View within the Channels section. The corresponding IPs and Paths can be then utilized to mount the exported channels.

Using the provided IPs and Paths, the Managed Volume channels can then be mounted on the Oracle file system. This can be accomplished using a simple mount command, however for persistence it is recommended that the channels be mounted by modifying the /etc/fstab file on the Oracle host. The following outlines the structure of the mount entries and options for the /etc/fstab file:

<channel_ip>:<channel_path> <mount_point> nfs rw, bg, hard, nointro, rsize=32768, wsize=32768, tcp, actimeo=0, vers=3, timeo= 600 0 0

Where:

- <channel_ip> is the IPv4 address for the channel.
- <channel_path> is the export for the path.
- <mount_point> is the desired mount point for the channel on the local filesystem.

Note: Do not include the 'actimeo=0' option for non-RAC servers or AIX hosts. In addition if using AIX hosts, use 'proto=tcp' in place of tcp. For a more in-depth look at the options recommended for each supported Oracle platform see Appendix A - EAS Mount Options.

Note: If running Oracle 11g or newer Direct NFS (dNFS) is also supported. Refer to Oracle documentation for more information on enabling and using dNFS.
Opening and Closing Managed Volumes

In order to maintain immutability, Rubrik stores Managed Volume snapshots in a read-only state. Before executing any RMAN commands to write to a Managed Volume, the appropriate Rubrik cluster must be instructed to switch the volume to a read-write state. Subsequently, after RMAN has completed the backup process, the Rubrik cluster must be instructed to switch the volume back to a read-only state. While the process of opening and closing volumes can be completed manually using the Rubrik UI, often DBAs choose to embed RESTful API calls within their RMAN scripts to accomplish this, allowing for the backup process to be completely automated from start to finish utilizing a preferred scheduler such as Control-M, Oracle Enterprise Manager, or cron.

The API call to open a managed volume for writing with curl is structured as follows:

```
curl -k -X POST -u "<username>:<password>"
'https://<rubrik_host>/api/internal/managed_volume/ManagedVolume::<mv_id>/begin_snapshot'
```

The API call to close the managed volume and mark as read-only utilizing curl is structured as follows:

```
curl -k -X POST -u "<username>:<password>"
'https://<rubrik_host>/api/internal/managed_volume/
ManagedVolume:<mv_id>/end_snapshot'
```

In both the above API calls the following applies:

- `<username>` is a name for the Rubrik cluster account with privileges to modify Managed Volumes.
- `<password>` is the password for the above user account.
- `<rubrik_host>` is the IP or FQDN of one of the nodes within the Rubrik cluster.
- `<mv_id>` is the managed volume id of the desired volume to open/close.

**Note:** Note: The id of the managed volume can be extracted from the URL by navigating to the Managed Volume overview page within the Rubrik UI. For instance, if the URL of the Managed Volume overview page is https://192.168.150.121/web/bin/index.html#/object_details/managed_volume/ManagedVolume:::167bbf90-d0af-4685-b694-cee369536c6e/ then the subsequent managed volume id would be 167bbf90-d0af-4685-b694-cee369536c6e.

Additionally, the opening and closing API calls can be authenticated with a base64 hash rather than including the username and password in plain text. The authentication hash can be created with the following command:

```
echo -n "<username>:<password>" | openssl enc -base64
```
The returned value can then be included within the API calls as follows:

```
curl -k -X POST -H 'Authorization: Basic <encoded_string> ' 'https://<rubrik_host>/api/internal/managed_volume/\ ManagedVolume:::<mv_id>/ end_snapshot'
```

**Note:** To further secure the Oracle backup processes, a non-administrative user account should be created with privileges to only open and close Rubrik Managed Volumes. See the Creating a managed volume user account within the user guide for more information.

**Oracle Backup Workflow**

To automate the complete Oracle backup process the open and close snapshot API calls should surround the existing RMAN backup script. The workflow outlining this process performs as follows:

1. Import and source environment variables
2. Issue API call to open a managed volume for writing
3. Execute RMAN backup script
4. Issue API call to close the managed volume.

The following shows a sample RMAN script utilizing incremental merge with a retention of 7 days, including the calls to open and close a Rubrik Managed Volume which can be scheduled to occur at a specified frequency.

```
#!/bin/bash

source $HOME/.bash_profile

curl -k -X POST -u 'username:password' 'https://rubrik_host/api/internal/managed_volume/ManagedVolume:::7a556a1c-3852-4bcc-a138-f23acd6f0cc/begin_snapshot'

env | sort

rman nocatalog LOG=/home/oracle/rman.log <<EOF
connect target /
set echo on;
show all;
run {
  crosscheck backup;
crosscheck copy;
  configure controlfile autobackup on;
  configure controlfile autobackup format for device type disk to
  '/mnt/clustera_channel0/%F';
  configure retention policy to redundancy 1;
  configure device type disk parallelism 4;
  allocate channel ch0 device type disk format '/mnt/clustera_channel0/%U';
  allocate channel ch1 device type disk format '/mnt/clustera_channel1/%U';
EOF
```
allocate channel ch2 device type disk format '/mnt/clustera_channel2/%U';
allocate channel ch3 device type disk format '/mnt/clustera_channel3/%U';
backup incremental level 1 for recover of copy with tag 'HRDB42' database
plus archivelog delete all input;
recover copy of database with tag 'HRDB42' until time 'SYSDATE-7';
backup as copy current controlfile;
}
delete noprompt obsolete;
EOF

curl -k -X POST -u 'username:password'
'https://rubrik_host/api/internal/managed_volume/ManagedVolume:::7a556a1c-3852-4bcc-a138-f23acd6ff0cc/end_snapshot'

---

Restoring Oracle Databases with Elastic App Services

Rubrik supports two different options for restoring Oracle databases from EAS: Restoring from a managed volume or Snapshot and Retrieving files for media recovery.

**Restoring from a Managed Volume or Snapshot**

Depending on the restore point selected, a Live Mount of a managed volume snapshot may need to occur. For instance, if the requested point-in-time is within the current retention of the RMAN backup script, the restore can be processed from the currently mounted managed volume. If the point-in-time extends beyond that of the RMAN backup script retention, a snapshot, or point-in-time copy of the managed volume will need to be mounted to the Oracle host.

**Restoring from a Managed Volume**

When the desired point-in-time recovery lies within the RMAN Backup scripts retention, the restore process is as follows:

1. Ensure the Managed Volume is currently mounted to the Oracle host.
2. Run an RMAN restore using the files located on the Managed Volume.
3. RMAN will restore the database to the desired point-in-time.

**Restoring from a Managed Volume Snapshot**

If the desired point-in-time recovery falls outside of the RMAN backup retention, a snapshot of the managed volume aligning with the recovery point will need to be mounted on the Oracle host. This process is completed from the managed volume overview page and is performed as follows:

1. The desired point-in-time snapshot of the managed volume is selected within the Managed Volumes snapshot card and Export option is selected.
2. The Rubrik cluster performs a Live Mount of the selected managed volume snapshot, presenting the channel details.
3. The channel details are then used to mount the Managed Volume snapshot on an Oracle database host.
4. An RMAN restore script can then be executed using the files on the Managed Volume snapshot.
5. RMAN will restore the database to the desired point-in-time.
6. The Managed Volume snapshot is then unmounted.
Performing advanced RMAN recovery scenarios

To perform more advanced RMAN recovery, individual files can be pulled from the managed volume or any of its associated point-in-time snapshots. This process is completely isolated to the Rubrik UI and does not require the need to mount or unmount volumes on the Oracle host. The process is completed from the Managed Volume overview page and is performed as follows:

1. From the **snapshots** card, use the **Search by File Name** field to search all database files stored within the Rubrik managed volume.
2. Select the desired database file to use for media recovery, choosing a version, and select **Download**.
3. The file can then be copied to a location where an RMAN media recovery can be performed.

CHOOSING BETWEEN AUTOMATED ORACLE DATA PROTECTION AND ELASTIC APP SERVICE

Rubrik recommends the use of Automated Oracle Data Protection where the following matters:

- **Simplicity** - Rubrik automatically discovers and protects Oracle environment. No need to build and manage complex RMAN scripts.

- **Instant Recovery and Live Migration** - The ability to run Oracle using data files served directly by Rubrik when production storage is down, enabling DBAs to Live Migrate data files back to preferred storage while Oracle database is serving users.

- **Automated Live Mount** - Built-in automated workflows for provisioning instant clones for Test/Dev and ETL use cases.

Elastic App Service is recommended where the following matters:

- **Control** - DBAs prefer to have full control over when a given database is backed up, but wants backup team to drive data life cycle management, disaster recovery and compliance SLAs.

- **Custom Workflows** - DBAs prefer to use native or traditional methods to protect their Oracle databases. For example, a DBA may prefer to use RMAN backup set instead of image copies that Automated Oracle Data Protection provides, DBAs may prefer to manage their own central recovery catalog for RMAN, or some legacy databases may need offline backup methods.

- **Legacy Systems** - EAS is recommended in environments or configurations where Automated Oracle Data Protection is not supported. For example, Oracle database versions less than 10g, retired operating environments like HP-UX etc.

Note: To further secure the Oracle backup processes, a non-administrative user account should be created with privileges to only open and close Rubrik Managed Volumes. See the Creating a managed volume user account within the user guide for more information.
CONCLUSION

Rubrik is able to provide both speed and simplicity to Oracle Data Management with two different options for backup. Rubrik provides DBAs and backup administrators with choice: For those wishing to offload RMAN catalog management and take advantage of near-zero RTO capabilities such as Rubrik Instant Recovery and Rubrik Live Mount, the automated Oracle protection can be leveraged. For those wishing to maintain complete control over backup and recovery processes, yet still take advantage of Rubrik’s policy-driven protection for long term retention and archival, Elastic App Services can be used.

While robust and full-featured, Rubrik’s support for Oracle Data Management extends the Rubrik focus on simplicity, understanding customers true operational requirements, and solves a number of data protection challenges.

ABOUT THE AUTHORS

Mike Preston is a Technical Marketing Engineer at Rubrik. He blogs on blog.mwpreston.net as well as various other tech related news sites. He is a Toronto VMUG Leader and author of Troubleshooting vSphere Storage. You can find him on Twitter @mwpreston.

Abdul Rasheed is Sr. Director of Product at Rubrik, where he is focused on building data management solutions DBMS, NoSQL and Big Data workloads. With his heart in technology and mind in business, he brings over a decade of experience in solving business critical problems through software solutions. Prior to Rubrik, Rasheed held positions in Pure Storage and Veritas Software. #UMNproud from Carlson School of Business.
### APPENDIX A - EAS MOUNT OPTIONS

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>rw</td>
<td>Mounts the managed volume as read/write.</td>
</tr>
<tr>
<td>bg</td>
<td>Background mount option - proceeds to re-attempt the mount process in the background if the initial mount fails.</td>
</tr>
<tr>
<td>hard</td>
<td>Requires NFS client to wait for NFS server to return to availability if it becomes unavailable.</td>
</tr>
<tr>
<td>nointr</td>
<td>Prevents system signals from interrupting file operations.</td>
</tr>
<tr>
<td>rsize=32768</td>
<td>Sets larger block size for reads.</td>
</tr>
<tr>
<td>wsize=32678</td>
<td>Sets larger block size for writes.</td>
</tr>
<tr>
<td>tcp proto=tcp</td>
<td>Requires NFS to utilize TCP protocol. For Linux, use option value ‘tcp. For AIX, utilize option value ‘proto=tcp’.</td>
</tr>
<tr>
<td>actimeo=0</td>
<td>Use this parameter with Linux-hosted RAC servers. Permits caching of directory and file attributes.</td>
</tr>
<tr>
<td>vers=3</td>
<td>Instructs to utilize NFSv3.</td>
</tr>
<tr>
<td>timeo=600</td>
<td>Specifies the time an NFS client waits before retrying a failed response (in tenths of seconds).</td>
</tr>
</tbody>
</table>

Mount options for managed volume NFS exports on Solaris:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>rw</td>
<td>Mounts the managed volume as read/write.</td>
</tr>
<tr>
<td>bg</td>
<td>Background mount option - proceeds to re-attempt the mount process in the background if the initial mount fails.</td>
</tr>
<tr>
<td>hard</td>
<td>Requires NFS client to wait for NFS server to return to availability if it becomes unavailable.</td>
</tr>
<tr>
<td>nointr</td>
<td>Prevents system signals from interrupting file operations.</td>
</tr>
<tr>
<td>rsize=32768</td>
<td>Sets larger block size for reads.</td>
</tr>
<tr>
<td>wsize=32678</td>
<td>Sets larger block size for writes.</td>
</tr>
<tr>
<td>proto=tcp</td>
<td>Requires NFS to utilize the TCP protocol.</td>
</tr>
<tr>
<td>noac</td>
<td>Prevents data and attribute caching.</td>
</tr>
<tr>
<td>forcedirectio</td>
<td>Copies data directly to user space buffer rather than caching in kernel.</td>
</tr>
<tr>
<td>vers=3</td>
<td>Instructs to utilize NFSv3.</td>
</tr>
<tr>
<td>suid</td>
<td>Allows for the opening of device-special files on the mounted filesystem.</td>
</tr>
</tbody>
</table>