COHESITY

Version 1.1

July 2024

Oracle Data Protection Best Practice Guide

Considerations and Tips to Deploy Cohesity Data Protection for Oracle Servers

ABSTRACT

As Oracle Servers have become critical components of growing enterprise infrastructure, it has become even more important to protect those databases efficiently and reliably. This guide offers practical recommendations and tips to help deploy the appropriate Oracle Data Protection Solution for a customer's environment.

Table of Contents

Tables

Introduction

Successfully restoring an Oracle database means you've protected the data; successfully recovering a server means you've protected the machine; successfully recovering after a disaster means you've protected the business.

A good Cohesity deployment allows the business to securely protect its data and infrastructure. It positions the business to take advantage of evolving technologies like cloud services.

You are at the *Deployment considerations* phase of implementing the Cohesity solution for your Oracle databases. This guide focuses on the deployment and configuration choices you have to make as you set up Cohesity for your Oracle Servers, *prior* to deploying the platform to protect your specific databases.

Audience

This guide is for IT administrators and database administrators (DBAs) who are familiar with managing data protection for Oracle Servers.

Cohesity recommends having familiarity with:

- Oracle Server
- Oracle Real Application Cluster (RAC)
- Oracle Data Guard

See the Oracle Databases section in the online Help for instructions to set up protection for your databases.

Backup and Disaster Recovery (DR) Strategy

Backup Strategy Considerations

Data backup is an essential part of protecting the data, but it's important to really understand what makes a backup strategy successful. It is important to have a second copy of data in case the original copy fails. But that is only part of the story. A good backup strategy is obviously going to create that second copy, but it is more crucial that, when recovery is needed, the data can actually be found and restored quickly.

You can use Cohesity for other types of backups and even create new backup strategies designed to better meet your company's needs.

Cohesity recommends that you plan your Oracle backups using the business's Service Level Agreement (SLA) and disaster recovery (DR) requirements.

Table 1: Prerequisite Planning for Backups

PLAN	DETAILS
Current Methods	Determine how backups are currently being done. Some common methods are: Oracle RMAN, and third-party tools. **Cohesity recommends** all other backup methods be disabled. If multiple backup methods are being used concurrently, conflicts can occur.
Strategy Planning	Determine which type of Oracle backups are needed for the business. Consider the customer's SLA and review the business's Disaster Recovery Plan for RTO and RPO requirements. These will largely define the backup strategy.
Restore Planning	**Cohesity recommends** a periodic restore of a database from its backup. This is an important step in the overall backup strategy because it tests, verifies, and validates the integrity of the backup. A sample set of backups should be restored to a non-production server and evaluated. This step also ensures that at a critical event, the method of restoring a database is valid.
Protecting the Backups	Determine a strategy for protecting all backups. The backups are very valuable and need to be protected from: corruption, deletion, overwriting, and catastrophic loss. Copies of the backups should be moved to an off-site location. Having off-site copies of the backups not only protects the backups, but is also the foundation for a Disaster Recovery Plan. Use replication to maintain off-site copies, in addition to the backups you archive for long-term retention. **Cohesity recommends** protecting all Oracle databases with regularly scheduled Full, Incremental, and Log backups. Protect VMs with a separate VM protection group. Finally, all backups should be replicated to an off-site location and archived.

Cohesity recommends: Use the Cohesity Agent for backups, and disable all other backup jobs or methods, such as Oracle RMAN jobs, which would conflict with the backup process.

Disaster Recovery (DR) Considerations

Cohesity recommends safeguarding all of your backups by using replication and archival.

Taking a backup is only one part of protecting a business. Protecting the business means protecting the data from corruption *and* from catastrophic disaster. This is done by keeping a series of backups, and then in turn moving some of those backups off-site and archiving them under a long-term retention plan.

Protecting the business starts with:

- **Capture and Store** for protection of databases from loss and corruption with regularly scheduled backups.
- **Geo-Protect** for protection from catastrophic loss by replicating the backups to an off-site location.
- **Cost-effective Archive** to protect and hold the backups by archiving the backups to the cloud under a long-term retention plan. Stored on a lower-cost storage tier.

Take Local Snapshots

Maintain enough backups to meet your business requirements. Protect from data corruption over time by maintaining a series of local snapshots. By taking and maintaining several snapshots, you are in position to recover data from its state prior to being corrupted. Snapshots are efficient because they use deduplication and compression.

Replicate Backups Off-Site

Replicate backups to a second Cohesity cluster. Protect your entire set of Oracle backups from catastrophic loss by replicating them to an off-site location. In a Cohesity protection group, you are able to automatically replicate the Oracle backups stored in the Cohesity cluster to a second off-site Cohesity cluster. As part of replication, Cohesity always performs source-side compression and deduplication first and sends only the changed data over the network for cost-effective disaster recovery.

Archive Backups to the Cloud

Archive to the cloud to take advantage of low-cost, long-term storage. Archive some of the Oracle backups to the cloud as a way to address long-term data retention requirements and lower the cost of storage. Cohesity provides a policy-based method to archive to public clouds (AWS, Azure, Google Cloud Platform) and any S3-compatible storage.

Validate Oracle Backups

Regularly validate backups by restoring or cloning a database. Successfully restoring an Oracle backup is proof that your backup strategy works. Cohesity gives you the advantage of being able to browse and search across all your snapshots, and to restore to different locations on different servers.

Oracle Data Protection Methods

The Cohesity Oracle solution extends the scalability of RMAN and provides the features and tools needed for automating backups, recoveries, and managing your data within a single pane of glass. Cohesity offers three backup methods which are explained below.

Cohesity Oracle Adapter

Cohesity Oracle Adapter integrates with Oracle Recovery Manager (RMAN) to provide application-consistent backup and recovery for Oracle databases. The adapter provides a unified user interface allowing users to manage and provision all the Oracle database protection services, supporting Oracle single instance, RAC, or Oracle Multitenant databases. Additionally Cohesity Oracle Adapter provides an incremental forever backup approach eliminating the need for regular expensive full backups. To learn how to deploy Oracle Data Protection using Cohesity Oracle Adapter, see Oracle Data Protection Deployment Using Cohesity Oracle Adapter. For additional information, see Using Cohesity Oracle Adapter in the online Help.

RMAN NFS Target

Cohesity can be presented as an NFS volume to be used as inline-deduplication Oracle database backup target. Oracle RMAN can use the Cohesity data platform as a deduplication target and automatically leverage Cohesity's QoS policy for optimal data tiering as well as global deduplication and compression to reduce secondary storage consumption. To learn how to deploy Oracle data protection using NFS Target, see Oracle Data Protection Deployment Using RMAN NFS Target. For additional details, see Using RMAN NFS Target in the online Help.

Cohesity Oracle SBT Plug-in

The Cohesity Oracle SBT Plug-in allows you to use Cohesity multi-cloud data platform as target storage for backing up Oracle databases. To learn how to deploy Oracle data protection using SBT Plug-in, see Oracle Data Protection Deployment Using Cohesity Oracle SBT Plug-in. For additional details, see Using SBT Plug-in in the online Help.

Design Decisions and Best Practices

The decision on which method to use for data protection of Oracle on Cohesity depends on the operating system, Oracle configuration, and type of database. For self-managed Cohesity deployments either on-prem or in the cloud, use the following decision process to choose an Oracle DataProtection Method.

Cohesity Oracle Adapter

The Oracle Agent for Linux is designed to work specifically with the Linux operating system. If you have multiple Oracle hosts, you will need to install the agent on each host that you wish to protect.

You might choose the **Oracle Adapter** if you:

1. Want a fully automated data protection method for Oracle databases
2. Don't want to write, manage, or update RMAN scripts
3. Want incremental-forever backups (no need for Periodic fulls)
4. Want to use instant recovery of your Oracle databases
5. Want to create near-instant, zero-cost clones of your Oracle databases for non-prod use cases
6. Want advanced, centralized management and reporting of your Oracle backups

See Cohesity Oracle Adapter for instructions on how to use Oracle Adapter as your data protection method.

RMAN NFS Target

Using NFS mount points is a traditional method of pushing your backups to storage. Using NFS mounts to a Cohesity View allows you to take advantage of Cohesity's unique performance strategy: parallelization.

You might choose to use Cohesity as **RMAN NFS Target** if you:

1. Want to use and manage your own RMAN Scripts
2. Your RMAN scripts are very tightly integrated with your current tools and workflows
3. Use a version of Oracle or OS vendor/version that the Oracle Adapter does not support. Ex - Oracle 9i or RHEL 5.x or HP-UX. See support matrix below for more details.
4. Want to use the SBT plugin.

See RMAN NFS Target for instructions on how to use RMAN NFS Target as your data protection method.

Cohesity Oracle SBT Plug-in

The Source-Side Deduplication feature in the Cohesity Oracle SBT Plug-in extends the capabilities of RMAN by allowing storage-efficient deduplication to take place on the Oracle host *before* data is copied to Cohesity. This reduces the number of transferred blocks, resulting in faster backups and reduced network traffic between Oracle hosts and the Cohesity View during backup.

You might choose to use the **SBT plugin** if you:

1. Want to use source-side dedupe to reduce network load
2. Don’t want to create or manage NFS mounts for data protection
3. Cannot use the NFS protocol in your environment
4. The SBT plugin is supported for Linux and AIX operating systems.

See Cohesity Oracle SBT Plug-in for instructions on how to use Cohesity Oracle SBT Plug-in as your data protection method.

Selecting a Deployment Option

Now use the table below to choose a Deployment Option for Oracle Data Protection based on your environment and preferred backup method. Click the appropriate link to know more about the backup methods.

Table 2: Oracle Data Protection Selection

OPERATING SYSTEM	SINGLE INSTANCE	RAC	STANDBY / DATAGUARD	MULTI-TENANCY (CDB/PDB)	ORACLE TDE
Linux (RHEL, Centos, OEL 6/7/8), (SuSE/SLES 11, 12, 15)	Oracle Adapter*, RMAN SBT, or RMAN NFS Target				
Windows (2012, 2012 R2, 2016, 2019)	Oracle Adapter RMAN SBT, or RMAN SMB Target	RMAN SBT, or RMAN SMB Target			
AIX 7.1, 7.2	Oracle Adapter, RMAN SBT, or RMAN NFS Target		RMAN SBT, or RMAN NFS Target		
HPUX (All)	RMAN NFS Target				
Solaris (All)					
Other DB and OS (Ex - Oracle 10, RHEL 5)					

* CDB/PDB supports only 6.6.0x and later

* Oracle supported by version (Oracle Adapter(11gR2 and above), SBT(11gR2 and above), RMAN-NFS(all version)

* See Cohesity Software Support Matrix to validate your specific configuration details.

Additional Decision Criteria

If the OS and Cohesity feature set combination yields a single approach, follow that. If presented with more than one approach, please read the following to help guide your decision.

Oracle Adapter Considerations

Cohesity Oracle Adapter uses RMAN incremental merge backup method which is an incremental forever technology. It supports all sizes of databases. However incremental forever does not mean it is always faster than full backup. It depends on the database size, change rate, and your Cohesity platform. If a customer is expecting Oracle adapter backup to be faster than full backup, then use following size recommendations as a general guidance. If the database size is not in this range, more tuning on agent or platform will be required. The following databases are ideal candidates to use Oracle Adapter:

- You can use Cohesity Oracle Adapter for all the supported configurations irrespective of the database size
- Databases with a change rate greater 3 - 5 TB between successive backups may need additional configurations in the adapter. Cohesity recommends customers contact Cohesity to get the additional tuning parameters reviewed.
- Automatic scheduling of database backups with out-of-box parallelism to meet backup SLA.
- Both databases and the Cohesity cluster are in the same facility, either both on-prem or both in cloud. Cohesity recommends the source and Cohesity cluster should be in the DC for best performance.
- A cold database backup is not supported by Oracle Adapter
- Cohesity Adapter before 6.6.0c doesn't support concurrent database and archive logs backup tasks. Not too frequent archive log backups. Consider running archivelog once every two hours or four hours.

RMAN Target Considerations

Databases that do not meet the above Oracle Adapter criteria should use one of the RMAN Target solutions (RMAN SBT or RMAN NFS). Here are some considerations around using Cohesity as an RMAN target. This would require a small change for the DBAs.

1. The database team would like to use their preferred RMAN scripts.
2. The change to the database team is minimal. Cohesity replaces the existing storage tier.
3. This solution requires more Cohesity storage than the Oracle Adapter.

-

Appendix A: Cohesity Cluster and Oracle Server Settings

It is important to understand the processing settings in the Cohesity cluster that is protecting your Oracle databases. Choosing the optimal settings for deduplication, compression, and encryption can dramatically improve the performance of your Cohesity backups and archives.

Deduplication

Cohesity recommends leaving deduplication enabled and setting it to **Inline**, to reduce storage costs.

Deduplication: (Enabled by default.) When Deduplication is on, Cohesity eliminates duplicate blocks of repeating data stored on the Cohesity cluster, dramatically reducing the amount of storage space needed to store the data.

Inline Deduplication: Optionally toggle on. When Inline Deduplication is on, the deduplication occurs as the Cohesity cluster is saving the blocks to the partition. (There can also be additional deduplication after the Cohesity cluster has saved the blocks to the partition.) When Inline Deduplication is off, deduplication occurs *after* the Cohesity cluster has written the data to the partition and might ultimately be slower.

Compression

Cohesity recommends that you enable Inline Compression in the Cohesity platform. This also takes advantage of Cohesity deduplication, by allowing it to identify block patterns in the data.

Compression: (Enabled by default.) When Compression is on, the Cohesity cluster compresses all the data stored in the Storage Domain, reducing the amount of space needed to store the data.

Inline Compression: (Enabled by default.) If Inline Compression is on, the compression occurs as the Cohesity cluster is saving the blocks to the partition. If Inline Compression is off, the compression occurs *after* the Cohesity cluster has written the data to the partition and might ultimately be slower.

> **NOTE**: The first backup might appear slower but the benefits of deduplication will kick in starting with the subsequent backup, and the reduction in the volume of data outweighs any performance drop experienced while taking the first backup.

For more details, see Manage Storage Domains in the online Help.

Encryption

Cohesity recommends that data encryption be enabled for any data being sent to an External Target, to the public cloud, or any time sensitive data is being handled.

Data-at-Rest Security

The Cohesity SpanFS® file system provides full at-rest encryption based on the strong AES-256 CBC (Cipher Block Chaining) standard.

Data-in-Flight Security

The data being transmitted from a Cohesity cluster to another cluster is encrypted for security. Examples of data movement include: replicating between remote offices; and transmitting data to a public cloud.

Data-in-Cloud Security

Cohesity's CloudArchive includes encryption. This functionality moves data from an on-premises cluster to cloud storage. For cold data, which is rarely accessed but must be retained, this is a far more economical solution. While encryption for CloudArchive operations can be turned off, Cohesity strongly recommends keeping it on, especially when working with External Targets in the public cloud.

For more, see Cohesity Security Features in the online Help

Oracle Server Database settings

Cohesity recommends enabling archiving for the Oracle database so that a point in time recoveries can be made.

Appendix B: Documentation

For in-depth details see the below in the online Help:

- Oracle Adapter Requirements
- Cohesity Oracle Adapter Documentation
- Cohesity Oracle Best Practices
- Oracle Adapter Troubleshooting

Your Feedback

Was this document helpful? Send us your feedback.

About the Authors

This document was authored by the Database Solution Architecture team of: Diana Yang, Dave Porco, Sanjay Dhruv, and Matthew Ellis.

Other significant contributors include:

- Scott Lorenz, Solutions Engineer
- Aditya Tandon, Director, Product Management
- Janell Filkin, Implementation Specialist
- Kevin Hill, Mgr, Solutions Architects
- Saad Jafri, Product Solutions Architect
- Sunil Moolchandani, VP, Product Solutions
- Steve Lee, Technical Staff
- Karthick Radhakrishnan, Sr. Manager, Technical Marketing
- Subash Babu, Staff Technology Editor

Document Version History

VERSION	DATE	DOCUMENT VERSION HISTORY
1.1	July 2024	Republished
1.0	June 2022	First release

ABOUT COHESITY

Cohesity radically simplifies data management. We make it easy to protect, manage, and derive value from data -- across the data center, edge, and cloud. We offer a full suite of services consolidated on one multicloud data platform: backup and recovery, disaster recovery, file and object services, dev/test, and data compliance, security, and analytics -- reducing complexity and eliminating mass data fragmentation. Cohesity can be delivered as a service, self-managed, or provided by a Cohesity-powered partner.

Visit our website and blog, follow us on Twitter and LinkedIn and like us on Facebook.