COHESITY

Version 1.1

July 2024

Protect Oracle Databases with Cohesity

Cohesity Oracle Adapter for Linux: Cohesity's Solution for Backup and Restore of Oracle Databases

ABSTRACT

As databases continue to grow in number and size, data centers in today's organizations need different methods and strategies to protect their databases and manage their growing data. Now, with the integration of the Cohesity platform with RMAN, you can use it with our Oracle adapter to add another backup method to your toolbox. Cohesity's adapter-based backup gives you the flexibility to schedule, automate, and manage all your Oracle backups.

Table of Contents

Figures

Tables

Complexity Forces Us to Sink or Swim

Today's complex data center environments lack an easy way to manage all the backups and recoveries, which comprise the foundation of their protection. Administrators often describe the task as similar to keeping many plates spinning at the same time; without an enterprise-level data management solution, you will either sink or swim.

Three essential factors push the demand for efficient data management:

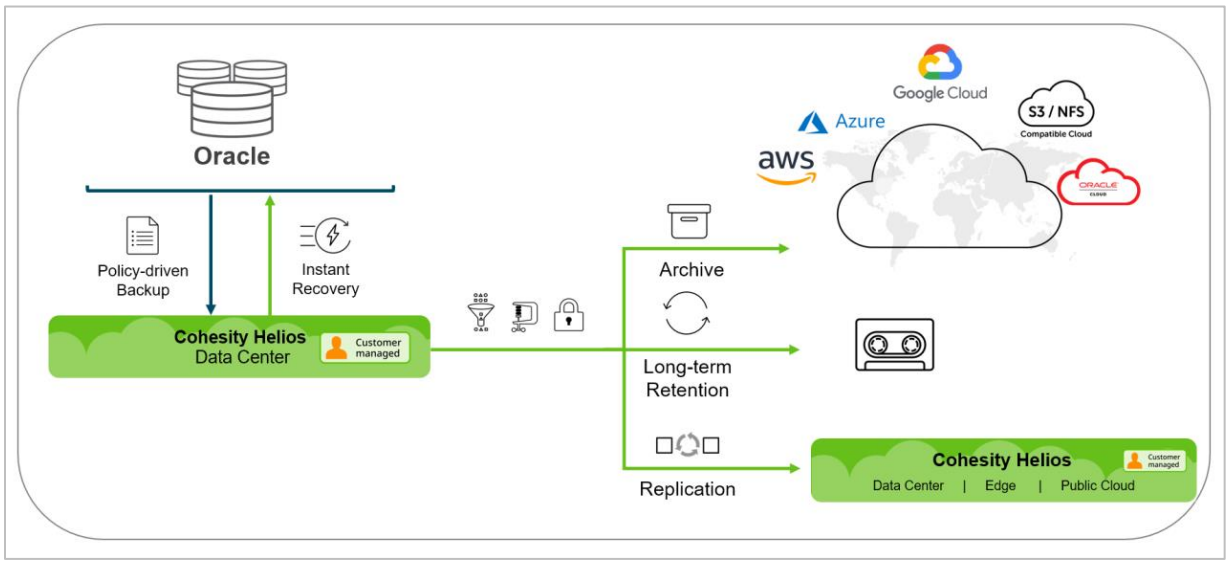
- **The growing number of databases**. The number and kind of backups increase as the demand for protection increases.
- **The increasing size of databases**. Larger databases result in longer backup windows that make it harder to meet your SLAs.
- **The ever-increasing duration and cost of retention**. Managing the storage for backups becomes more complex as company standards and government regulations increase retention requirements.

Cohesity's Adapter for Oracle Databases

Cohesity is a modern, software-defined platform for data management. Taking inspiration from its web-scale architecture and leveraging its unique distributed file system (SpanFS®), Cohesity offers high scalability and reliability.

Cohesity's flexible architecture allows easy expansion, increasing operational simplicity and improving TCO. Cohesity's solution for Oracle works on-premises, in the public cloud, and your remote and branch offices. You choose how to back up your data and where to keep your backups, and for how long.

Figure 1: Cohesity's Adapter Protection for Oracle



Features and Benefits of Cohesity Protection

Cohesity's solution for Oracle includes many features that make your backups much more valuable, including:

- **Flexibility**. Cohesity allows you to browse and search across all your snapshots and restore them to different locations on different servers.
- **Performance to Meet Your SLAs**. Cohesity gives you the backup performance you need to protect your Oracle databases efficiently and securely.
- **Scalability**. Cohesity protection for Oracle is scalable from a single database to several Oracle RAC Instances and even an entire data center with hundreds of Oracle instances.
- **Compression**. Data compression significantly reduces storage usage and data transmission. An efficient storage model leaves you enough room for storing more backups and other important data. By default, Cohesity performs compression on all the data it stores.

  If you also enable *inline* compression, the process co-occurs *as* Cohesity saves the data to storage instead of doing it after saving the data.

- **Encryption at rest, in flight, and in the cloud**. It is vital to protect that data from unauthorized access.
  - **Data-at-Rest**. The Cohesity SpanFS® file system provides full at-rest encryption based on the strong AES-256 CBC (Cipher Block Chaining) standard.
  - **Data-in-Flight**. Cohesity can encrypt all data that is transmitted.
  - **Data-in-Cloud**. Cohesity's CloudArchive provides encryption for data stored in the cloud.

  For details, see Cohesity Security Features in the online Help.
- **Archive to Cloud**. Cohesity's policy-based ability to archive to public clouds like AWS, Azure, and Google Cloud, as well as to any S3-compatible storage, makes it easy to leverage lower-cost long-term retention and protect your data from regional disasters. Cohesity makes it easy to retrieve your organization's information to different geographical locations whenever you need to.
- **Disaster Recovery**. Protect your Oracle universe from disaster by replicating your Cohesity backups to another location that can be ready to failover (and failback, after repairs) as soon as disaster strikes.

In addition, you can deploy Oracle with different configurations. For example, Oracle might run on a cluster or on a Virtual Machine (VM). In such cases, you can use Cohesity *for other Oracle backups* and even *create new backup strategies*. For example, you can protect the Oracle database and the VM it is running on.

Features and Benefits of The Oracle Adapter

Now that you have protected your Oracle database with the Oracle adapter, a host of unique features are available to you.

Table 1: Unique Features Related To The Oracle Adapter

FEATURE	ORACLE ADAPTER USE CASE
Database Cloning	Cohesity DataPlatform provides the ability to clone Oracle databases (Standalone, RAC, and VCS). The Oracle database is cloned at Cohesity Storage Domains and requires no additional storage from the Oracle Host. Likewise, multiple clones from a single source of an Oracle Database backup require little or no extra storage in the Cohesity cluster.
Persistent Mount Points	With this option enabled by default, you can retain the NFS mounts created during the Oracle database backup job after completing the job. Disabling this would remove the NFS mounts after the backup job is completed.
Restore to Alternate Instance	Select this option to restore the database to an alternate location.

FEATURE	ORACLE ADAPTER USE CASE
Download RMAN Logs	Use this option to increase the efficiency of the DBA by providing access to the logs from one location. The Database Administrator can use these to troubleshoot errors and to view the RMAN activity log. The logs increase the DBA's visibility into the Oracle environment.
Restore No Recovery	Select the checkbox if you want to prevent access to the recovered database.
Configurable Pfile	The Pfile parameters option allows you to see the target database parameters before you initiate the restore job. The Pfile inherits some source database parameters to the target database and enables you to edit the target database parameters based on your requirement by specifying the additional parameters as a key=value pair.

Use Cohesity Adapter to Protect Your Oracle Databases

Cohesity offers a policy-based, highly scalable data protection infrastructure for your Oracle data. With a few steps, you can set up Cohesity to meet all your data protection requirements.

Cohesity uses Oracle's RMAN to perform backups of databases on any Oracle instance registered with Cohesity.

Cohesity supports full database server backups, differential (Cohesity incremental) Oracle database, differential backups via a Cohesity incremental, and Oracle archive log backups.

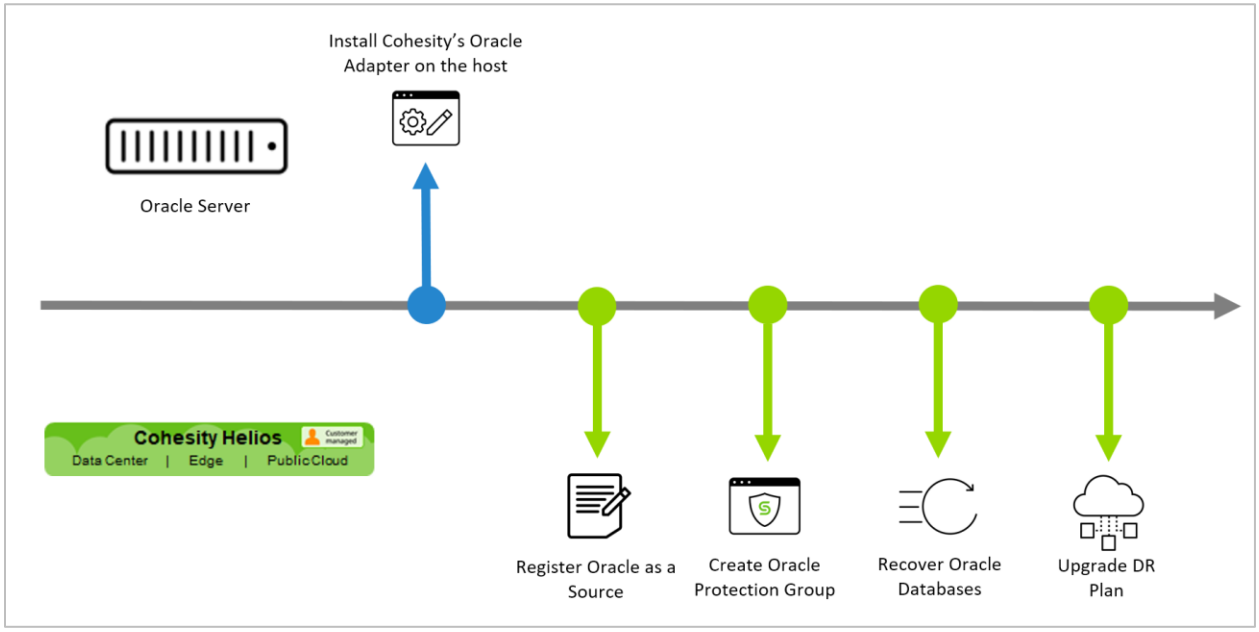
Implementing any enterprise technology is always a process. Therefore, you must understand what makes a backup strategy successful. For example, you must ensure that you have a second copy of backup data in case the original copy fails. But that is only part of the story. When you need to recover your Oracle databases, you must be able to find those backups and restore them quickly. To take full advantage of the many features of Cohesity's solution, be sure you understand each step of the implementation.

To protect your Oracle databases using Cohesity:

1. Install Cohesity's Agent on your Oracle Linux server.
2. Register Oracle as a Cohesity source.
3. Create a Protection Group.
4. Recover protected Oracle Databases.
5. Upgrade your disaster recovery (DR) plan.

NOTE: For more background information, see Appendix A: Terminology and Appendix D: Product Documentation.

Figure 2: Set Up Oracle Data Protection with Cohesity



Complete these steps to protect your Oracle databases. Get started by deploying Cohesity's Linux Agent next!

Deploy the Cohesity Oracle Agent for Linux

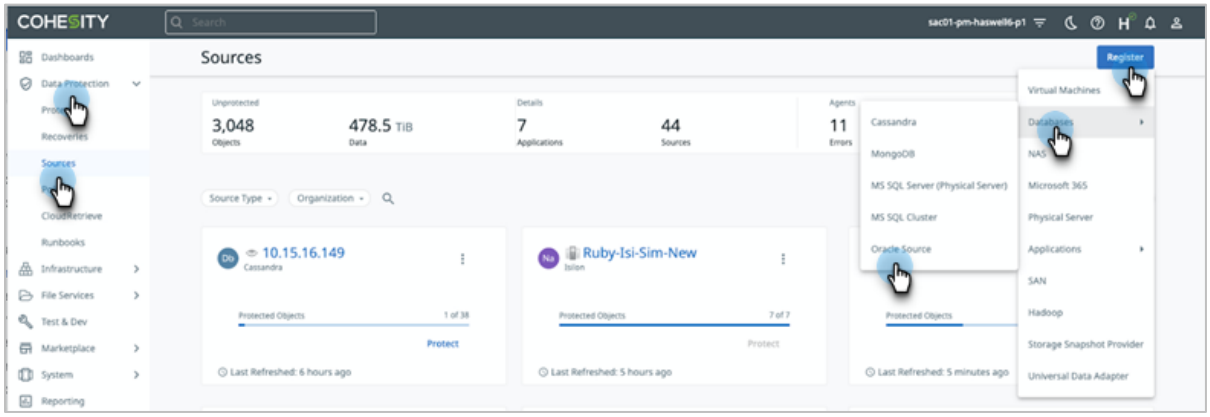
To start the deployment, you need to install the Cohesity Agent on the Oracle host. The Oracle Agent for Linux is designed to work specifically with the Linux operating system. If you have multiple Oracle hosts, you will need to install the agent on each host that you wish to protect.

The Cohesity Agent is lightweight and has a small memory footprint. The agent carries out the tasks you define in the Cohesity Protection Group. It ties together technologies and capabilities of Oracle, like RMAN, and new technologies such as the Cohesity Changed Block Tracker (CBT), so that you can efficiently tackle data management.

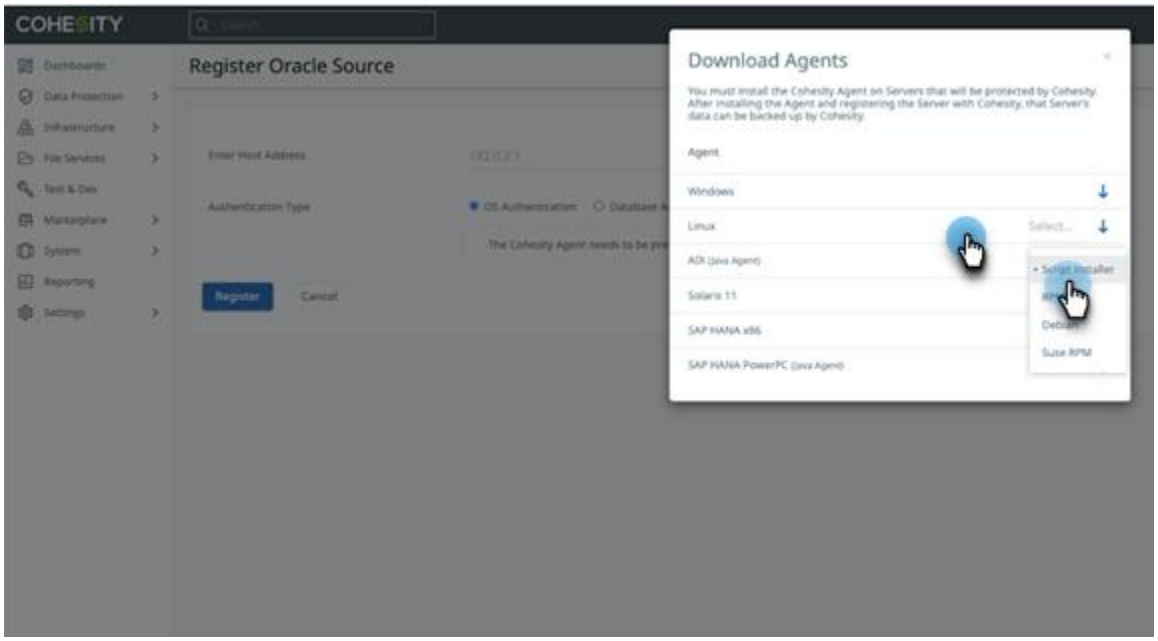
IMPORTANT: You need to install the Cohesity Agent on each Oracle host that you wish to protect.

To install the agent:

1. Log in to Cohesity and navigate to **Data Protection** > **Sources** and then on the right-side, click **Register** > **Databases** > **Oracle Source**.



2. Click **Linux** > **Script Installer**.



3. Click the **Download** (↓) button for **Linux**.
   A copy of the Script Installer will be downloaded to your local machine (*cohesity_agent_6.5.1c_linux_x64_installer*). If you are installing it the first time, copy the Oracle Script Installer to all the Oracle hosts you want to protect. On each Oracle host, run the installer.
4. From the command line, run the installer.

   `cohesity_agent_6.5.1c_linux_x64_installer.`

```
#./cohesity_agent_6.5.1d_linux_x64_installer -- --install -I /opt -S root
-G root -c 0
```

There are more ways and options for installing the oracle adapter, see Install the Linux Agent and Credentials and Privileges in the online Help.

You can configure the agent on your Oracle host in several ways, like which service-group or group name to use for the service. You can see a complete listing of these options in Appendix B: Script Installer Options.

When you successfully install the Oracle adapter, your Oracle host is ready to be registered as a Cohesity source.

Register Oracle Server in Cohesity

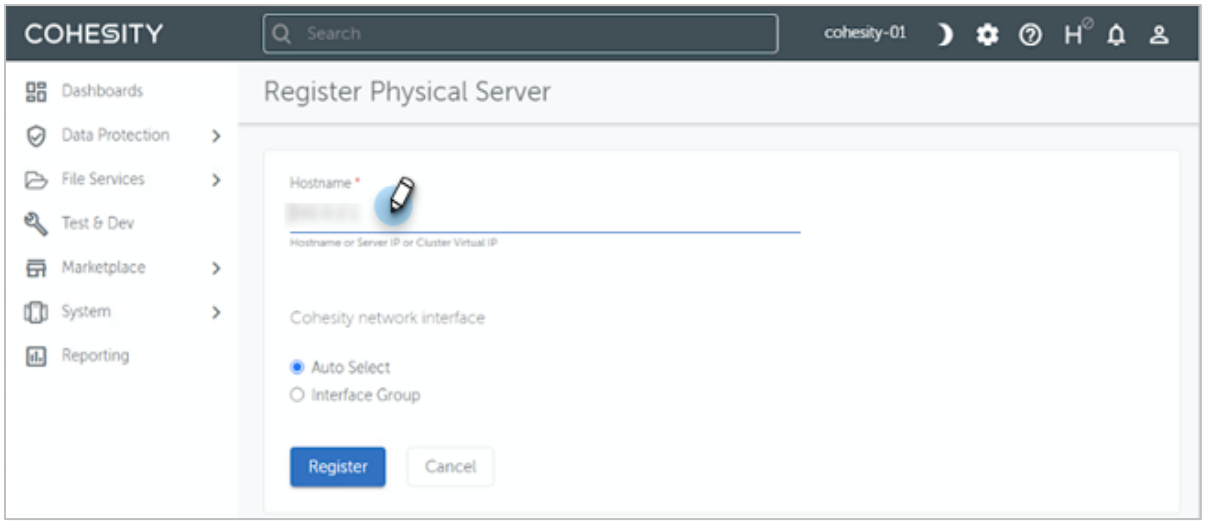
To protect your Oracle databases with Cohesity and take advantage of its many features, you need to register Oracle as a Cohesity source. Once it's registered in Cohesity, you will be able to add it to a Protection Group and configure the settings for your environment.

To register Oracle as a source in Cohesity:

1. Navigate to **Data Protection** > **Sources** > **Register** > **Databases** > **Oracle Source**.

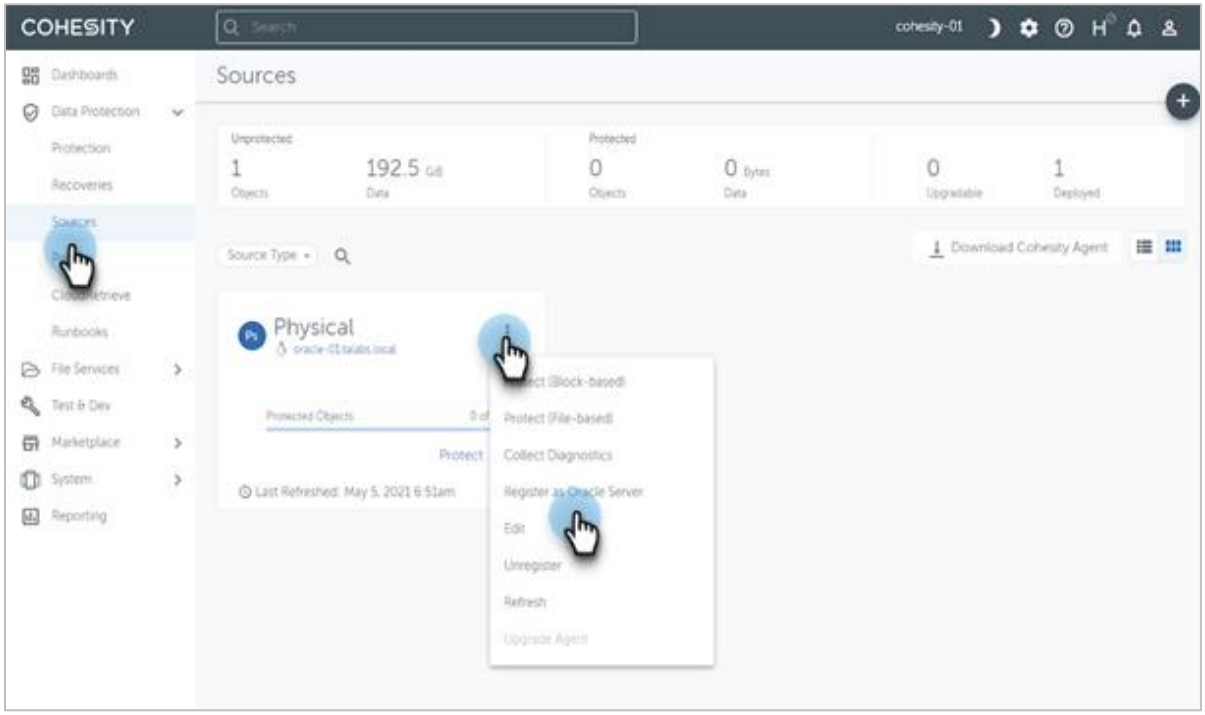
> **NOTE**: Oracle registration is a two-step process of registering the Oracle host first as a Physical source, and then the Oracle application. Cohesity sees the host and the Oracle application so that it has full application awareness.

2. In the **Register Physical Server** form, enter the Oracle IP address.

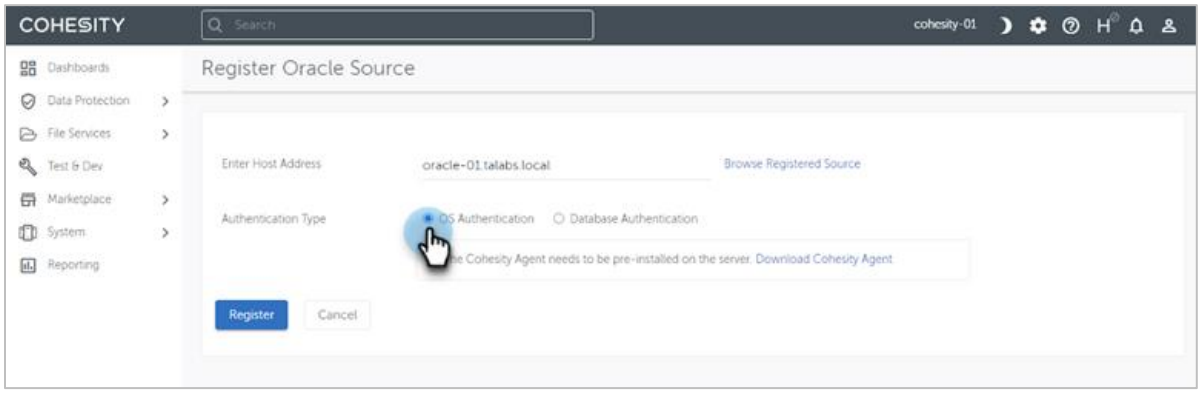


> **TIP**: You can also use the server's Fully Qualified Domain Name (FQDN) as well.

3. In the **Physical** source panel, click the ellipsis, and choose **Register as Oracle Server**.



4. In the **Register Oracle Source** page, choose your **Authentication Type**.



You can use either OS user or DB user authentication to connect to your Oracle source.

See Appendix A Linux Agent Authentication for the pros and cons of authentication types. Select your **Authentication Type**, and click **Register**.

To protect your newly registered Oracle source, you must create a Protection Group for it.

Create a Protection Group

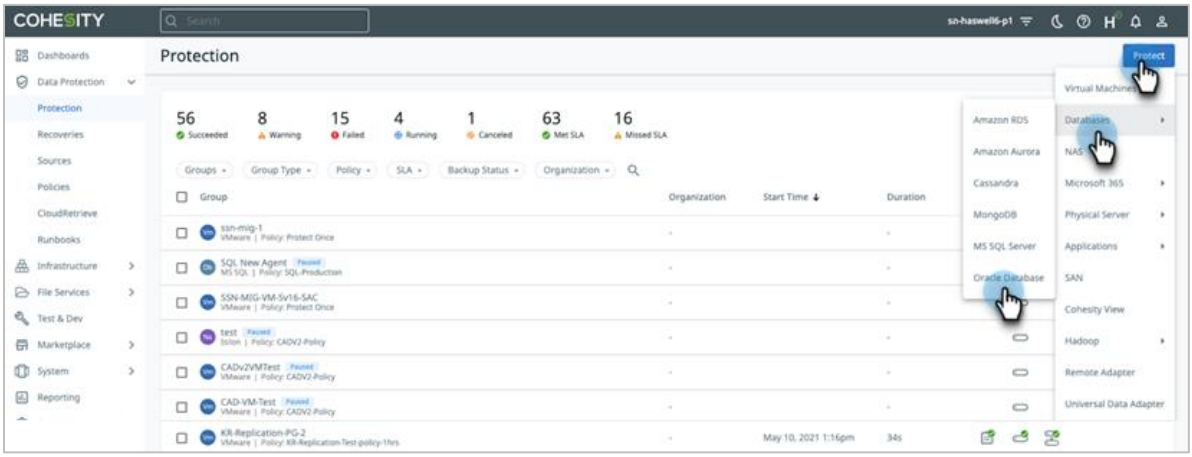
Automation is the only way to stay ahead of the demand curve for backups and data management. In Cohesity, Protection Groups combine operational requirements (objects to protect, indexing, alerts, exclusions, inclusions, etc.) with the business requirements that are defined in a Protection Policy (scheduling, retention, etc.). Multiple Protection Groups can use the same Protection Policy, but each Group can have only one Policy. For more, see About Policies and Protection Groups in the online Help.

Automate your Oracle database backups by building a Protection Group and assigning the Oracle host that you had registered earlier, and applying the Protection Policy that meets your business requirements.

NOTE: Because you can implement Oracle Server configurations across multiple hosts, or as part of a Cluster, you must identify all the Oracle hosts so that you can include them in your Protection Group.

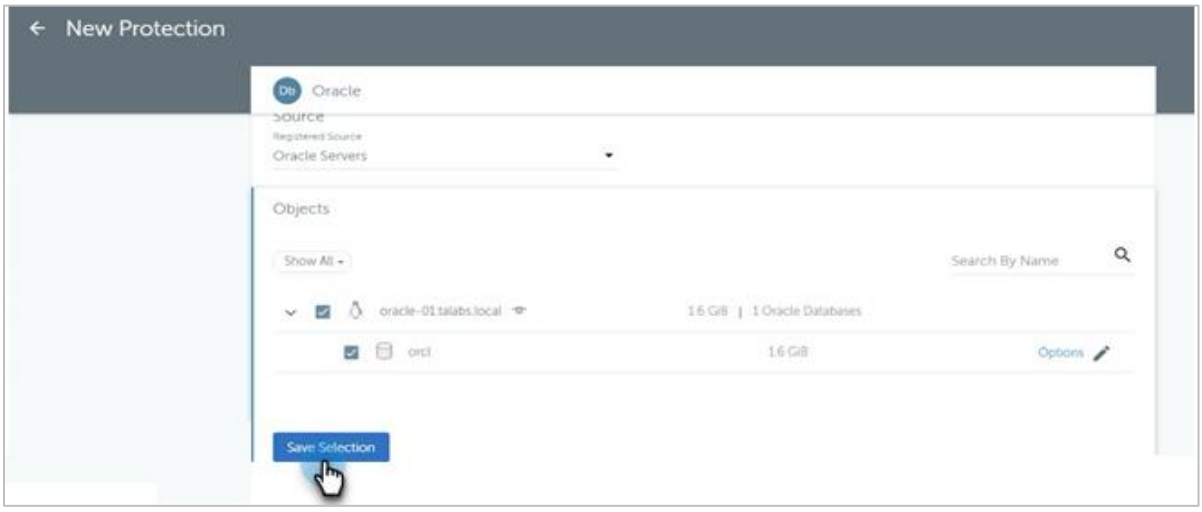
To create a Protection Group:

1. Log in to Cohesity and navigate to **Data Protection** > **Protection**. Then click **Protect** and select **Databases** > **Oracle Database**.



TIP: You can add or remove more Oracle sources to the Protection Group later if you like. In this way, you can build onto the Protection Group to manage all your Oracle servers.

2. In the **Oracle Objects** form, select the Oracle host(s) you registered earlier, and click **Save Selection**.

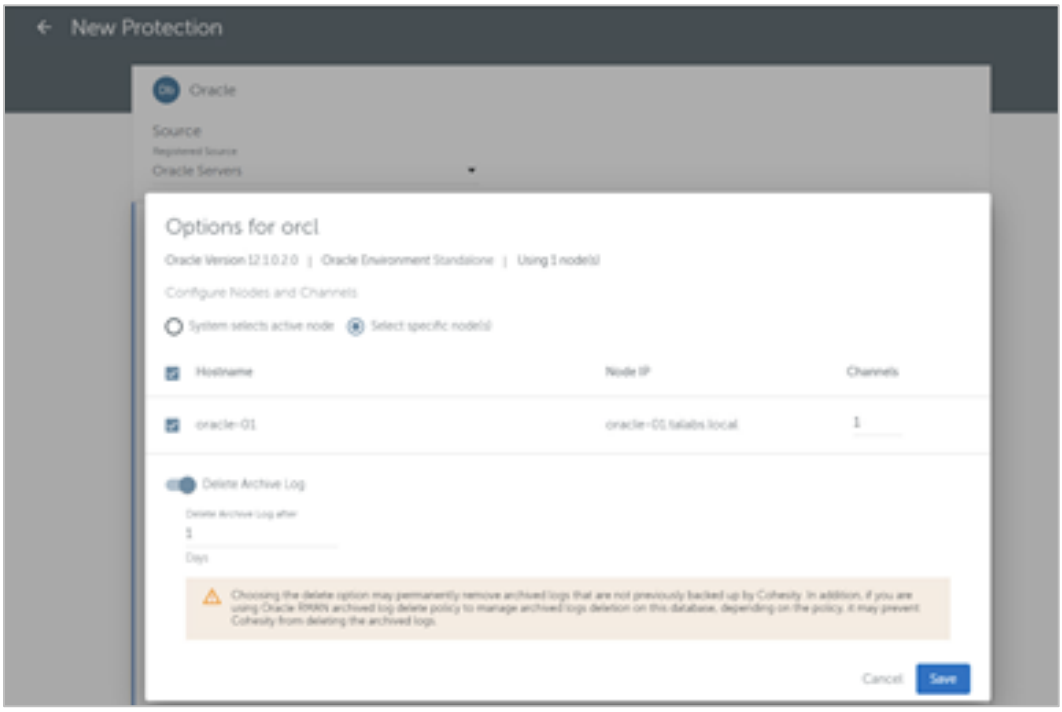


Archive Log Management

1. In the **Sources** page, select the Oracle host on which you want to manage the Archive Log.

> **IMPORTANT**: By default, Cohesity does not delete the old Archive logs after backing them up. To manage the old Archive logs automatically, choose **Delete Archive Log** and specify the number of retention days.

2. On the Oracle host, click the **ellipsis**, then choose **Edit**.



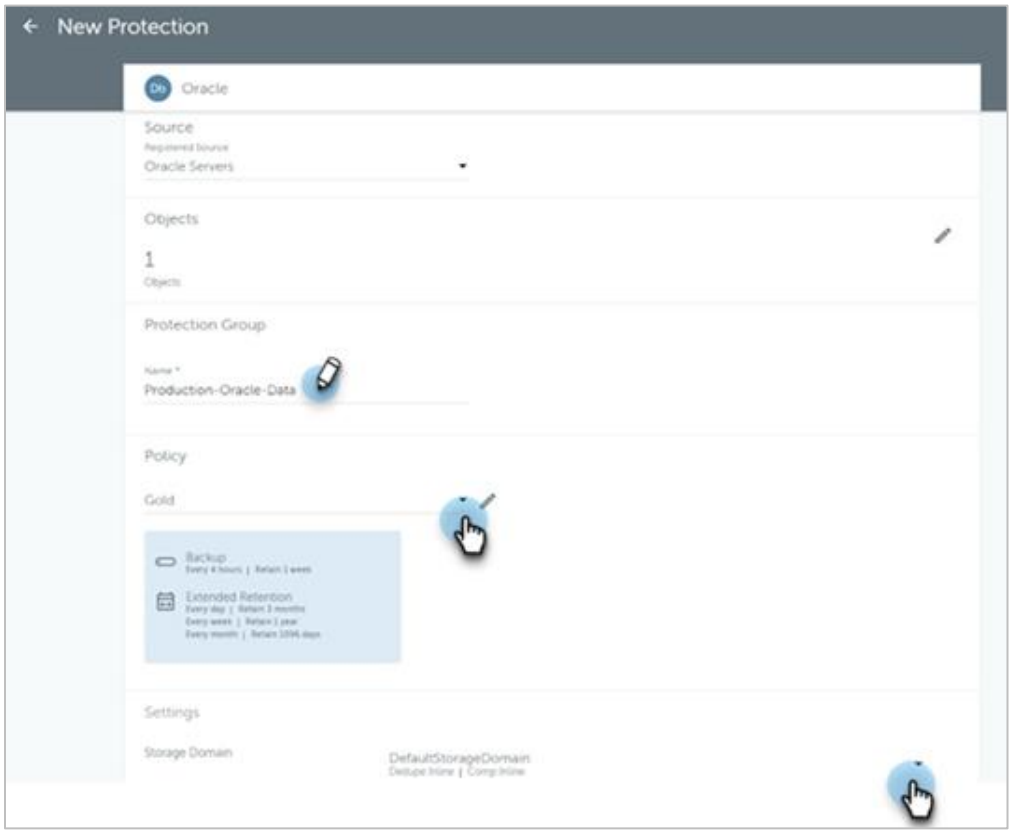
If you want Cohesity to manage the Archive Logs, then In the **Options** form, toggle the **Delete Archive Log** and specify the number of days for its retention.

Archive log management and channel options are listed below.

Table 2: Oracle Source Options

OPTIONS	DESCRIPTION
	LINUX
System Selects Active Node	Cohesity DataPlatform will auto-select an active RAC node and configure the number of RMAN channels for the database object. This option is enabled by default.
Select Specific Nodes	For the RAC database, If you select this option, you can choose the number of RAC nodes and the number of RMAN channels and ports to use for each RAC node of the database object. For a standalone database, if you select this option, you can choose the number of RMAN channels and ports to use for the node of the database object.
Delete Archive Log	Toggle on and specify the number of days after which Cohesity can delete the archived logs on the source database. If you specify the value as "0" days, Cohesity will delete the source archived logs immediately after each successful Cohesity backup. If you choose this option, Cohesity issues RMAN DELETE ARCHIVELOG command to delete archived logs after each successful Cohesity backup. Logs are deleted if they are backed up at least once by RMAN and they are older than the days specified in this option. In addition, if you have archive logs not backed up previously by Cohesity and the time satisfies the log delete eligibility, then Cohesity deletes these logs. However, If you do not enable this option, Cohesity will not delete the archived logs after each Cohesity backup. If you are using the “Oracle RMAN archived log delete policy” to manage archived logs deletion on this database, depending on the policy, it may prevent Cohesity DataPlatform from deleting the archived logs as Oracle manages the policy. If you have upgraded Cohesity DataPlatform (both the Cohesity cluster and Cohesity agent) from a previous version, then the archived logs for the existing Protection Group will not be deleted. Starting with release 6.4.1, the archived logs are not deleted by default.

3. Continue In the same form, and enter a Protection Group **Name** and select the appropriate **Policy**. Then, under **Settings**, select the **Storage Domain**.



TIPS:

- Give your Protection Group a descriptive name that identifies the kind of data being protected and how it is managed. The name will help you identify and manage your Oracle backups as your environment grows. Use descriptors like production (PROD), critical, infrastructure (INFRA), financial, sales, primary, secondary, and employees (EMP). For example:

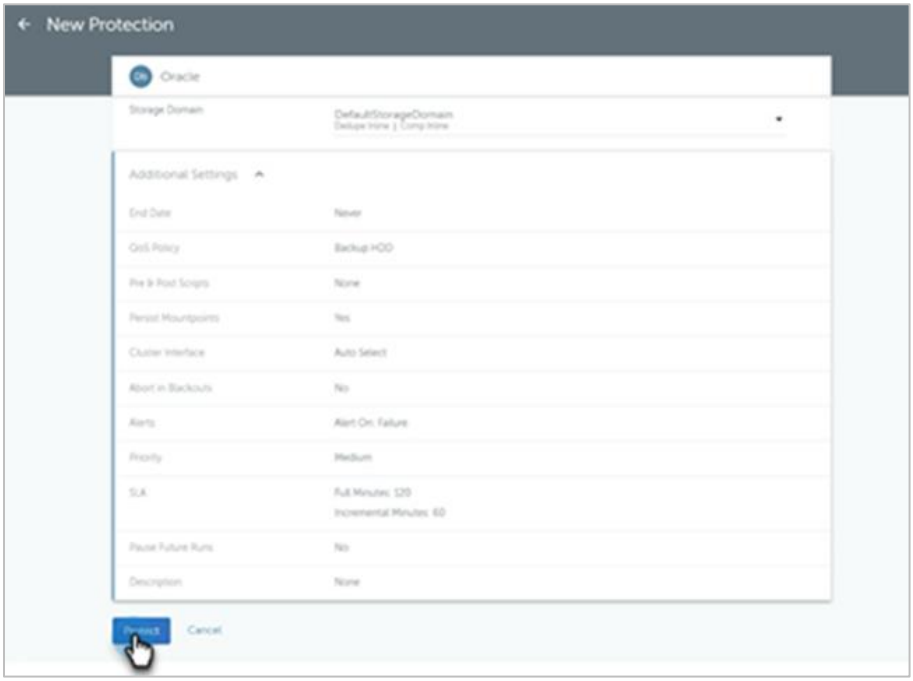
  Production_Sales DataCenter_Dallas_Production

  Critical_Infrastructure Production_ReplicatedTo_DRsite

  Archive_LongRetention Development_User_Data

- Once you set the Policy for a Protection Group, Cohesity conveniently manages all the sources assigned to that Protection Group the same way.
- To create a custom Protection Policy to meet specific scheduling, retry options, log backup, replication, and archiving needs, learn how to Create or Edit a Standard Policy in the online Help.
- For maximum space savings and security, choose a Storage Domain with compression, deduplication, and encryption enabled. For details, see Create or Edit Storage Domains in the online Help.

4. In the same form, configure any **Additional Settings** that you need and then click **Protect**.



NOTE: For details on the **Additional Settings**, see Create a Protection Group in the online Help.

Your new Oracle Protection Group is now active and running and appears on the **Protection** page. For more on optimizing your protection, see Cohesity Oracle Best Practices below.

Now that you have created a Protection Group for your Oracle databases, you can add other Oracle sources or change the Protection Policy and settings. In this way, Cohesity manages all your Oracle sources in this Protection Group the same way. For example, to replicate all the backups to an off-site target, simply add replication to the Policy that is assigned to this Protection Group.

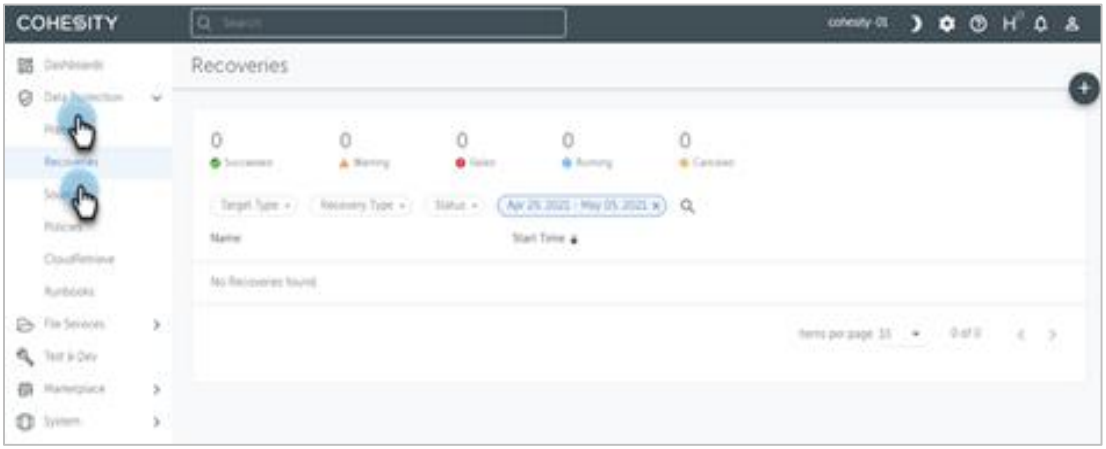
TIP: In larger environments, build two or three different Protection Groups with different configurations to manage several Oracle hosts. This model helps keep your data management simpler even as your environment grows.

Recover Oracle Databases

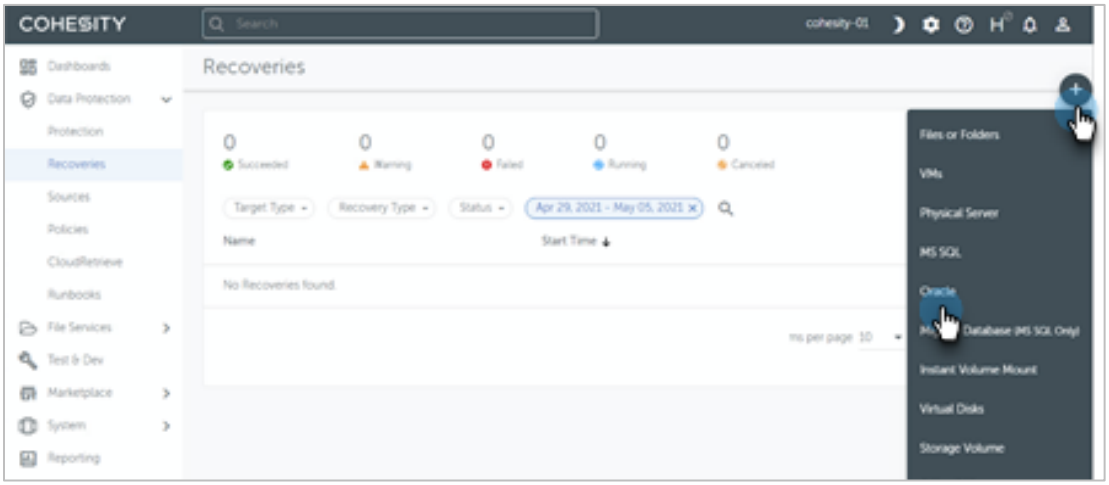
For the DBA, restoring the database starts with a restore of the FULL backup and then a Differential and hundreds of individual log files. This is a slow process and very time-consuming. In the same way, an Oracle DBA manually performs the restore sequence, Cohesity knows to look for the FULL backup, the Differential (if any) in between the full and Log backups, and then the Logs to walk the restore forward to a point in time. Cohesity makes the Oracle database restore process easy.

To recover Oracle databases:

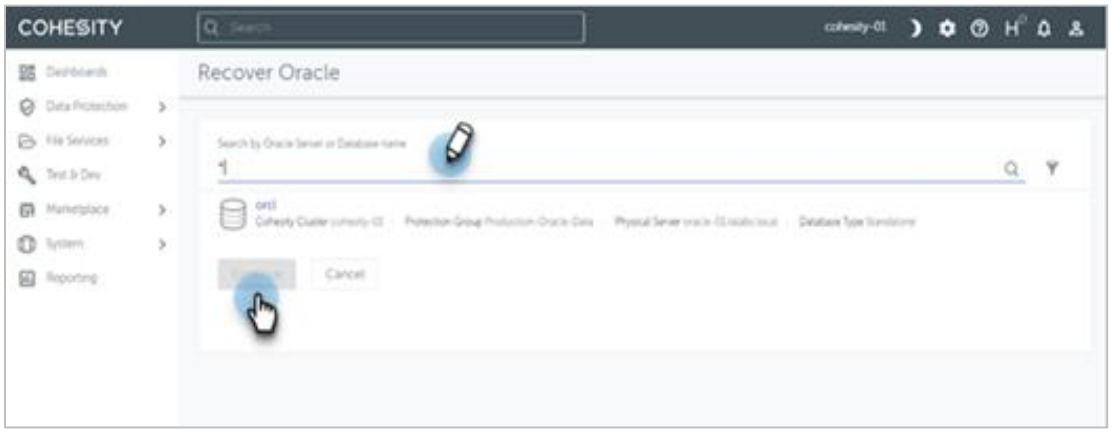
1. Log in to Cohesity and navigate to **Data Protection** > **Recoveries**.



2. On the **Recoveries** page, click the (**+**) and select **Oracle**.



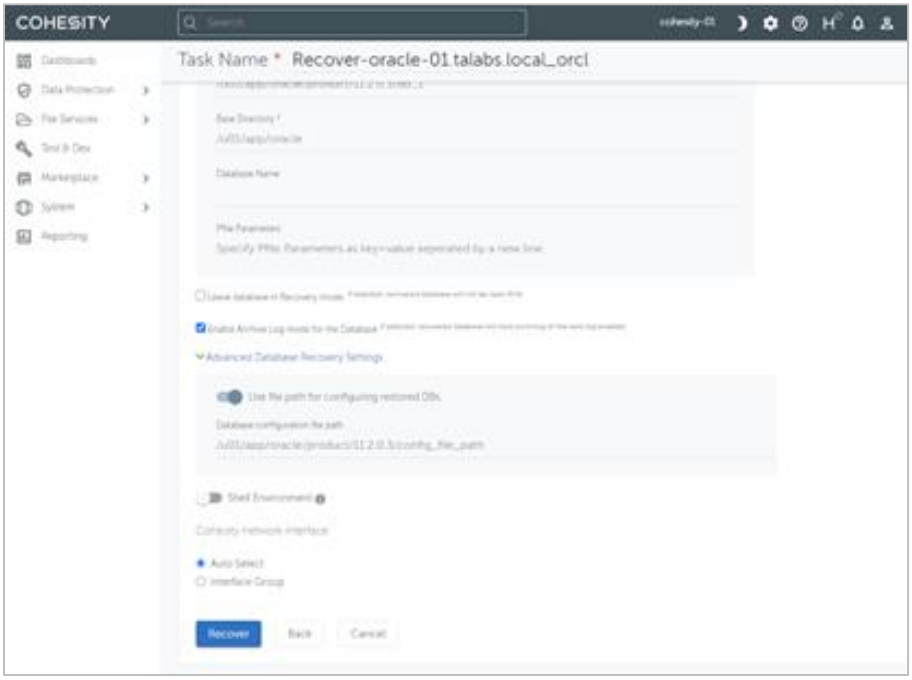
3. In the **Recover Oracle** form, enter a search term to locate your database backup. After locating, click **Continue**.



4. In the **Task Name** form, select the **Restore to Original Server Instance** and enter **Oracle Instance** on which you need to restore the backup. If you need a different backup (point in time), click the backup listed under **Recover Point** to select an earlier backup.

5. In the Task Name form, select the **Settings**.

6. Scroll down to view the settings in full.



Upgrade Your Disaster Recovery Preparedness

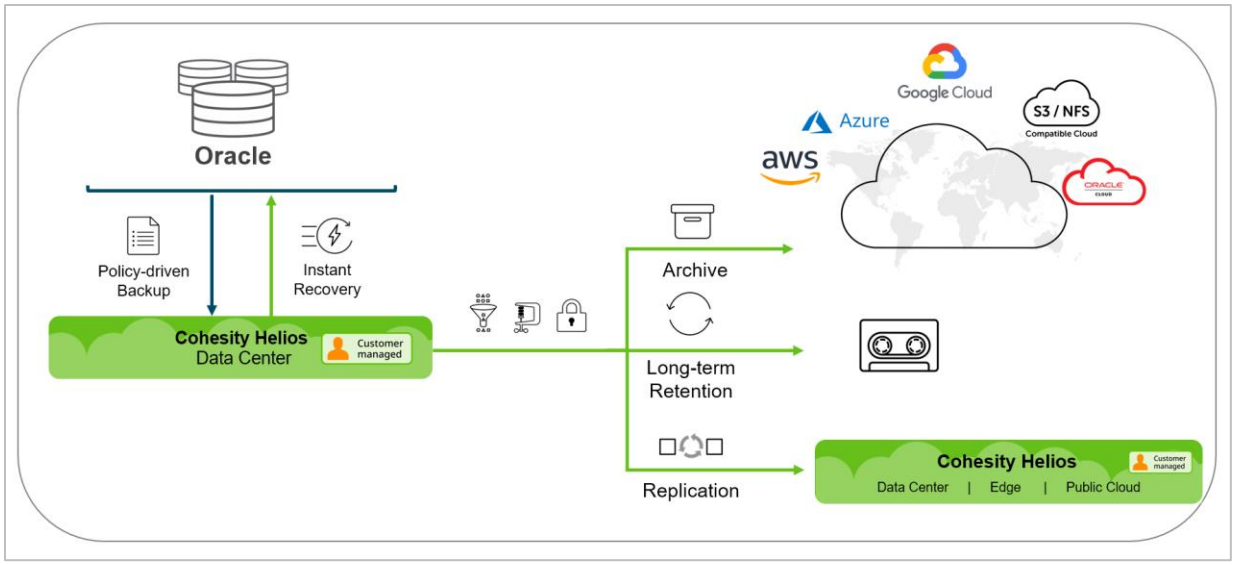
Disaster Recovery (DR) and business continuity are closely related plans that help proactively protect a business's infrastructure and data. Taking Oracle backups is only one part of protecting your business; you must also protect the data from corruption and catastrophic disaster. You can achieve this by keeping a series of backups replicating those backups off-site and archiving them under a long-term retention plan.

Cohesity gives you the foundation to build a DR plan to protect your business:

- **Capture and Store**. Protect your Oracle databases from loss and corruption with regularly scheduled backups.
- **Geo-redundancy**. Replicate your Oracle backups to an off-site location to protect them from catastrophic loss and disaster.
- **Cost-effective Archival**. Archive your Oracle backups to the cloud and store them on lower-cost storage tiers for long-term retention.

Use a Protection Group to schedule regular Oracle backups and assign a Protection Policy to include archiving and replicating those backups for long-term retention and disaster recovery.

Figure 3: Oracle Backups in Cohesity are Available to Replicate and Archive



Take Local Snapshots

Protect your Oracle backups over time by maintaining a series of *local* Cohesity snapshots.

Use Cohesity Protection Groups to schedule and automate Oracle backup management.

Replicate Backups Off-Site

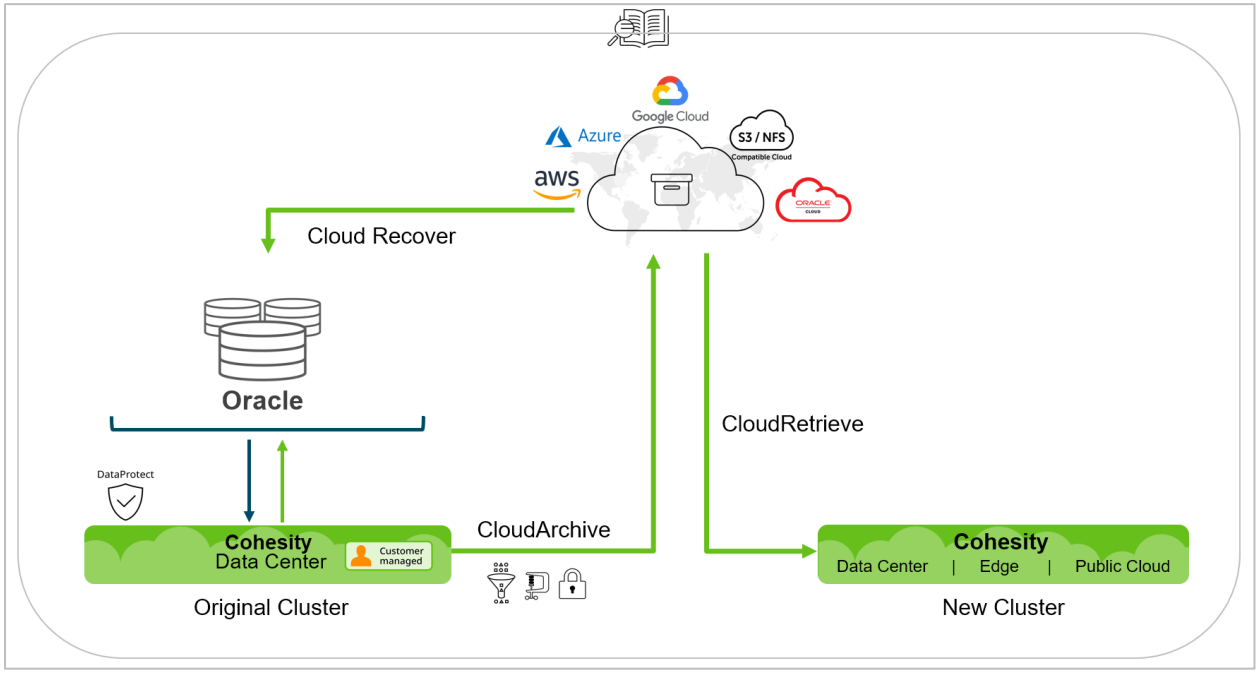
Protect your entire set of Oracle backups from catastrophic loss by replicating your Oracle backups to an off-site location. Choose a Protection Policy for your Protection Group that automatically copies the Oracle backups to a second, off-site Cohesity cluster. By default, deduplication and compression are enabled for replication, so that Cohesity sends *only the changed data* over the network, producing a significant reduction in network traffic and cost.

Archive Backups to the Cloud

Archive your Oracle backups to the cloud as a way to address long-term data retention requirements and simultaneously lower the cost of storage. Cohesity provides a policy-based method to archive to public clouds (AWS, Azure, and GCP), as well as to any S3-compatible storage.

With Cohesity CloudArchive, Cloud Recover, and CloudRetrieve, your Oracle backups are available for recovery to their original Cohesity cluster or onto a different Cohesity cluster, for geo-redundancy and disaster recovery.

Figure 4: Cohesity CloudArchive, Cloud Recover, and CloudRetrieve Provide Disaster Recovery



Cohesity Best Practices for Oracle Protection

Configuring the right Cohesity settings dramatically improves the performance of your backups, and the efficiency of your storage and archives. Manage your backups by choosing the optimal settings for deduplication, compression, and encryption.

- **Use inline deduplication**. *Deduplication* (enabled by default) prevents duplicate blocks of repeated data from being stored, dramatically reducing your storage consumption.

  With *inline deduplication*, the process occurs as Cohesity is saving the blocks, instead of waiting until *after* Cohesity has written the data to its Storage Domain. Therefore, we recommend that you use deduplication and, wherever possible, enable inline deduplication.

- **Use inline compression**. Compressing your data significantly reduces the space needed to store your backups and frees up space for more backups and other important data.

  With inline compression, the process occurs as Cohesity is saving the blocks, instead of waiting until *after* Cohesity has written the data to its Storage Domain. Both compression and inline compression are enabled by default, and we recommend you take advantage of them. For details, see Create or Edit Storage Domains in the online Help.

- **Use Encryption**. When a platform governs access to data across the systems in your environment, it is crucial to protect the data it manages. Therefore, we recommend you enable encryption — at rest, in flight, and in the cloud — for all your Oracle backups. For more, see Cohesity Security Features in the online Help.

- **Keep multiple snapshots to guard against corruption**. We recommend you maintain five to seven local snapshots of your backups.

  When you capture and store your backups like this, you protect your data from corruption over time. By taking and maintaining several backups, you are in a position to recover data from its state *prior* to being corrupted. Snapshots are efficient because they capture just the changed blocks of data and then use deduplication and compression.

  We recommend protecting all your Oracle servers with regularly scheduled backups, and then moving some of those backups off-site and archiving them under a long-term retention plan for disaster recovery.

- **Validate the backups**. We recommend a periodic restore of an Oracle database in a test environment from its backup. This is an important step in the overall backup strategy because it tests, verifies, and validates the integrity of the backup. Restore a sample from the snapshot set to a non-production server and evaluate it. In addition to confirming that the right data is backed up properly, this practice also ensures that you have already validated your method of restoring objects *before* a critical event necessitates it.

- **Verify Logging and Auditing operations**. You must log and audit changes on an Oracle Server. Cohesity logs its recovery process. In Cohesity, navigate to **Data Protection** > **Recoveries** and click into your Oracle database recovery task to view detailed logs.

- **Shelter in the cloud**. We recommend archiving to the cloud for low-cost, long-term storage and protection from regional disasters.

Cohesity provides a policy-based method to archive to public clouds (AWS, Azure, and Google Cloud Platform) or any S3-compatible storage. This makes it easy to change policies, meet regulatory requirements, and retrieve your data to different geographical locations.

- **Use replication to defend against site disaster loss**. Protect your entire set of Oracle backups from catastrophic loss by replicating them to a different geographical site. Cohesity can automatically replicate the Oracle database backups stored in the Cohesity cluster to a second, off-site Cohesity cluster.

  Cohesity replication always performs source-side deduplication and compression first and sends only the changed data over the network for cost-effective disaster recovery. As such, Cohesity replication is an essential part of every disaster recovery (DR) plan.

- **Be prepared *before* disaster hits with a DR plan**. One of the best things you can do to protect your Oracle server is to include it when you create your DR plans.

Appendix A: Linux Agent Authentication

Oracle Adapter capabilities align differently under different authentication types.

Determine the authentication needed for your environment.

Figure 5: Permissions for The Oracle Adapter on Linux

OPERATION	AUTHENTICATION REQUIRED	CAPABILITY
Backup	OS user authentication or DB user authentication	RAC multi-node and multi-channel require DB user authentication.
Recovery or Restore to Original Server (Overwrite)	OS user authentication or DB user authentication	Restoring data to the same server overwrites the original database.
Recovery or Restore to Alternate Server Database Cloning	OS user authentication	DB Recovery or Restore into a different server assuming the Oracle binaries already exist. The target oracle server has free space to store the newly created database files in case of alternate restore.
Cloning	OS user authentication	DB clones into a different server assuming the Oracle binaries already exist. Clone without SYSDBA privilege is not supported.

Appendix B: Script Installer Options

The script installer gives you options to install and manage.

Usage

```
cohesity_agent_6.5.1c_linux_x64_installer -- [-i|--install] [options]

cohesity_agent_6.5.1c_linux_x64_installer -- [-u|--update-uninstall]
[options]

cohesity_agent_6.5.1c_linux_x64_installer -- [-U|--full-uninstall] [options]

cohesity_agent_6.5.1c_linux_x64_installer -- [-v|--version]

cohesity_agent_6.5.1c_linux_x64_installer -- [-s|--single-mode] [options]
```

Options

OPTIONS	DESCRIPTION
-i, --install	Install/Uninstall Cohesity Linux Agent.
-U, --full-uninstall	Uninstall Cohesity Linux Agent including service-user account and its home directory contents. This is a destructive operation; use it with care.
-u, --update-uninstall	Uninstall Cohesity Linux Agent. This option preserves user, group, and agent config. Useful when upgrading software.
-S --service-user [user]	Username to use for service. [Default: cohesityagent]
-G --service-group [group]	Groupname to use for service. [Default: cohesityagent]
-c --create-user [0|1]	Whether to create --service-user or not. [Default: 1] This option is used with --install option only.
-I --install-dir [dir]	Cohesity Agent installation dir.
-L --install-log-file [file]	[Default: /home/<username>/cohesityagent or /root/cohesityagent]
-s --single-mode	Filename in which installer logs should be saved.

OPTIONS	DESCRIPTION
--skip-mountpoint-check	[Default: /tmp/cohesity_agent_installer_<time_in_seconds>_<pid>.log]
-d --debug	Install Cohesity Linux Agent for single-mode mode operation.
-y --yes-all	Skip checks performed on installation directory's filesystem mountpoint.
-a --agent-options [options]	Enables shell script debugging with set -x [Default: off]
--skip-lvm-check	Accept 'yes' answer to all questions in the installer. [Default: off]
-h, --help	This is useful for performing silent install/uninstall.

Sample Usage

Install:

```
cohesity_agent_6.5.1c_linux_x64_installer -- --install
```

Silent Install:

```
cohesity_agent_6.5.1c_linux_x64_installer -- --install -y
```

Upgrade:

```
cohesity_agent_6.5.1c_linux_x64_installer -- --install
```

Uninstall:

```
cohesity_agent_6.5.1c_linux_x64_installer -- --full-uninstall
```

Single mode Install:

```
cohesity_agent_6.5.1c_linux_x64_installer -- --single-mode --install-dir
/tmp/linux_agent --agent-options "--self_monitoring_enabled=false --
cluster_id=123456 --cluster_incarnation_id=1234"
```

Appendix C: Terminology

You must understand several concepts and terms as you learn how to take advantage of all of Cohesity's Oracle database protection features.

- **Protection Group**. A collection of objects from your registered sources that share a recurring backup schedule of Protection Runs. Use a Protection Group to identify which Oracle databases to protect. When you create a Protection Group, you associate it with a Cohesity Protection Policy.
- **Protection Policy**. A reusable collection of settings that define how and when objects are backed up, replicated, and archived.
- **Cohesity Replication**. Replication automatically makes copies of snapshots captured by Protection Runs on one Cohesity cluster and puts the copies on a second Cohesity cluster.

Appendix D: Product Documentation

Review these Oracle sections in our online Help for in-depth details:

- Oracle Adapter Requirements
- Cohesity Oracle best Practices
- Oracle Adapter Troubleshooting

Your Feedback

Was this document helpful? Send us your feedback!

About the Authors

Scott Lorenz is a Solutions Engineer at Cohesity. In his role, Scott focuses on business-critical applications, databases, cloud storage, and enterprise data protection. Scott has over 26 years' experience as an enterprise DBA.

Other essential contributors included:

- Bart Abicht, Staff Technology Writer and Editor at Cohesity
- Subash Babu, Staff Technology Writer and Editor at Cohesity

Document Version History

VERSION	DATE	DOCUMENT HISTORY
1.0	June 2021	First release
1.1	July 2024	Republished

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.