COHESITY

**Version 1.0**

**June 2024**

# Protect IBM-DB2 with Cohesity

*Cohesity Solution for Backup and Restore of IBM Db2 Databases with Best Practice*

**ABSTRACT**

*Get an overview of Cohesity Database Protection features, general workflows, options, and the best practices for IBM Db2.*

# Table of Contents

# Figures



# Tables

# IBM Db2 Protection using Cohesity Connector.

IBM Db2 administrators contend with the challenges of Increasing backup duration, rapid data growth, increased storage costs, and the lack of flexibility and storage management tools in IBM Db2 Studio.

In addition to these challenges, today's database protection must encompass more than getting a clean copy. It must include security, storage efficiency, minimized impact on production systems, automation, and scaling.

Cohesity protection for IBM Db2 provides a solution to these challenges. It reduces the complexity of database backups and restores secure, streamlined workflows. You can protect and manage your workloads and execute available protection and recovery workflows with a single pane of glass with a few steps. Cohesity IBM Db2 Connector provides flexible deployment options to make IBM Db2 backups and restores simple and secure.

This guide focuses on IBM Db2 tenant database protection.

The sections in the guide provide an overview of features and options and their related recommendations and best practices.

## Use Cases

You can use this workflow for IBM Db2 protection if you want:

- Automated backup protection
- Protection for your IBM Db2 environment using an on-prem Cohesity cluster
- Simple, specific restore or a Point in Time restore
- A simple UI-based database restored to an alternate host
- To meet your backup SLA
- Faster and more secure backups and restore performance using gRPC
- To move away from script creation and management
- Automated storage configuration and management
- To reduce storage space and the cost of your backups
- Centralized monitoring and reporting
- Immutable, ransomware-proof backups

## Technical Considerations

Consider the following technical aspects before you make significant decisions about your solution.

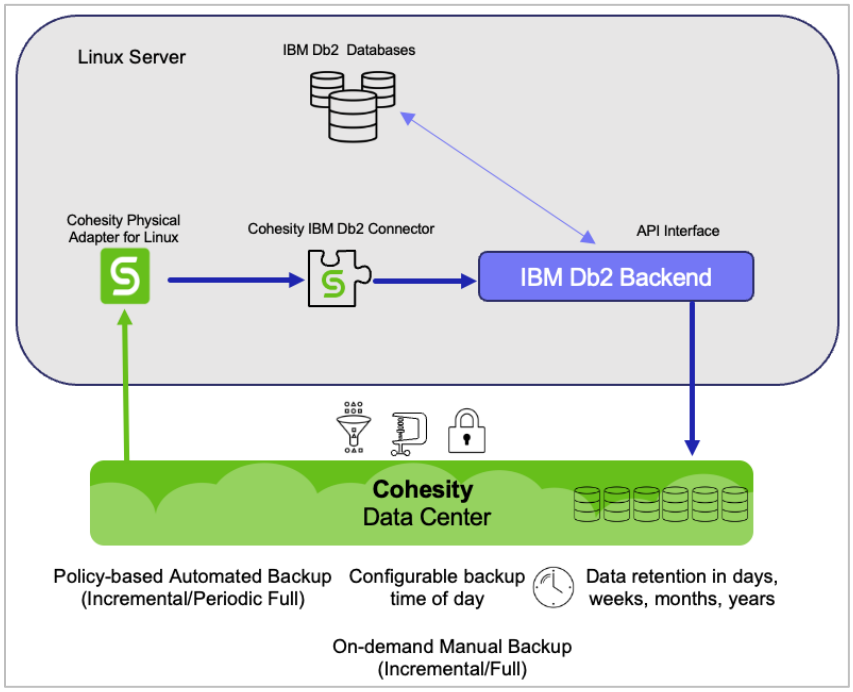
- SSH and NFS mounts are not required.
- Backup and restores use gRPC or secure gRPC protocols for improved performance.
- Backup and restores are balanced based on mounts and concurrency, as defined in the job (there are no scripts to change).
- You can perform point-in-time restores of a database,
- The first backup is always a FULL backup. After a Full backup, the incremental backup goes faster.
- Ensure third-party agents are removed or uninstalled.
- You can protect multiple databases using a single Protection Group.
- Please refer to Plan and Prepare for IBM Db2 Protection for other considerations and ensure you are familiar with the options available.

**SIGNIFICANT**: Cohesity's incremental forever strategy requires enabling the IBM Db2 tracmod option. Tracmon keeps track of database modifications so that Cohesity can detect which subsets of the database pages must be examined by an incremental backup and potentially included in the backup.

## How Cohesity Works with IBM Db2 Databases

Cohesity's Linux Adapter and IBM Db2 Connector natively integrate with databases to provide deployment backup and recovery solutions.

Figure 1: How Cohesity Works with IBM Db2 Databases



The Cohesity cluster can now directly connect to IBM Db2 databases via the IBM Db2 Connector for backup transfers.

Backup types for IBM Db2 databases are Full, Differential, and Log Cohesity, which provide the option to perform a full and incremental[1] backup. The first backup is always full, and successive backups can either be full or incremental based on business requirements.

[1] A Cohesity IBM Db2 incremental backup is the same as a IBM Db2 differential backup.

**NOTE**: You must install the Cohesity Linux Physical Adapter and the IBM Db2 Connector on each database host you want to protect.

## Cohesity IBM Db2 Connector Benefits

1. IBM Db2 backups and restores are optimized for Cohesity's performance.
2. Scale-out architecture — IBM Db2 backup and restores are load-balanced across Cohesity cluster nodes, giving redundancy and protecting against backup failure.
3. Simplification — Cohesity automates IBM Db2 backups [Full/Inc] and restores [specific/pit], which can be conducted through one simple graphical interface for all workflows.
4. Flexibility — Cohesity UI offers flexibility with options in the IBM Db2 backup and restore workflows.
5. Ease of Use — All backup and restore workflows can be used out of the box.
6. Immutability — Cohesity backups cannot be modified or tampered with and are secured from accidental loss or deletion.
7. Security — We support key-based authentication methods.
   gRPC and RPC are secure transport types.

# Cohesity Features

The IBM Db2 Connector supports IBM Db2 databases with a range of features.

## Backup and Restore Features for IBM Db2

You can find IBM Db2 Backup and Restore features at IBM Db2 Protection.

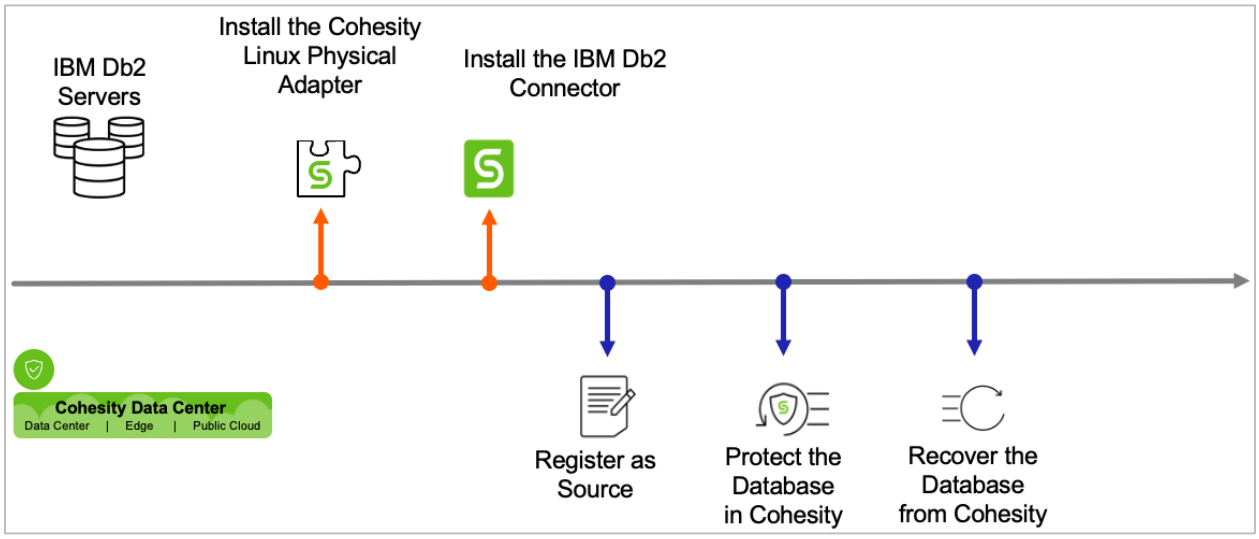
Table 1: Backup and Restore Features for IBM Db2

| Feature | Linux |
|---|---|
| Full Backup | Yes |
| Incremental Backup | |
| Log Backup | |
| Restore Snapshot Same Host | |
| Restore Point In Time Same Host | |
| Restore Point in Time Alternate Host | |
| Custom options for Backup | |
| Custom options for restore | |
| Policy or on-demand backups | |
| Offline Backups | |

## Deployment Steps

Install the Cohesity Physical Adapter for Linux and the IBM Db2 Connector on each database host you want to protect.

Figure 2: The Adapter and IBM Db2 Installation




Once you install both components on the database host, you can register the database as a source.

# Physical Adapter Installation

Cohesity recommends installing the Linux Physical Adapter before the IBM Db2 Connector.

Downloading and installing the Linux Physical Adapter and the IBM Db2 Connector on a server allows you to register IBM Db2 as a source with the Cohesity cluster.

Before you register your IBM Db2 deployment as a source with Cohesity and protect IBM Db2 databases, ensure the following prerequisites:

- Supported IBM Db2 Versions
- Port Requirements
- Considerations

## Download and Install the Linux Physical Adapter

The RPM installer is available and recommended. If you choose to use the Script Installer, follow the steps:

Table 2: Steps to install the Cohesity Physical Adapter for Linux

| Action | How To |
|---|---|
| Download the Agent Installer | From the download agent window, select the **Script Installer** and download it to the server you want to protect. |
| Navigate to the downloaded directory. | As the root user (required) with local system privileges on that server, change the directory to the location of the installer package. |
| Make the installer executable | Make the installer executable, for example:<br>`chmod +x cohesity_agent_X.X_linux_x64_installer` |
| Install the agent | `rpm -ivh el-cohesity-agent-6.8.1_u6-1.x86_64.rpm` |
| Location | • Installation directory : `/home/<username>/cohesityagent or /root/cohesityagent`<br>• Log file: `/home/cohesityagent/cohesityagent/logs` |

More details about the Cohesity adapter install are found in Download and Install the Linux Agent and Linux Agent installer options.

# IBM Db2 Connector Installation

The IBM Db2 Connector is available as a data source agent on the Cohesity Download portal. Download the respective data source agent for the Cohesity IBM Db2 Connector and copy it to the IBM Db2 host.

Table 3: Install the IBM Db2 Connector

| Operation | Install User | Install Command Syntax |
|---|---|---|
| IBM Db2 Database Connector Install | sid<adm> | Using rpm -ivh:<br>sudo rpm -ivh cohesity-db2-connector-<version> .x86_64.rpm |

Download the Database Connector for IBM Db2 from the Cohesity Download portal.

# Cohesity Database Source Registration

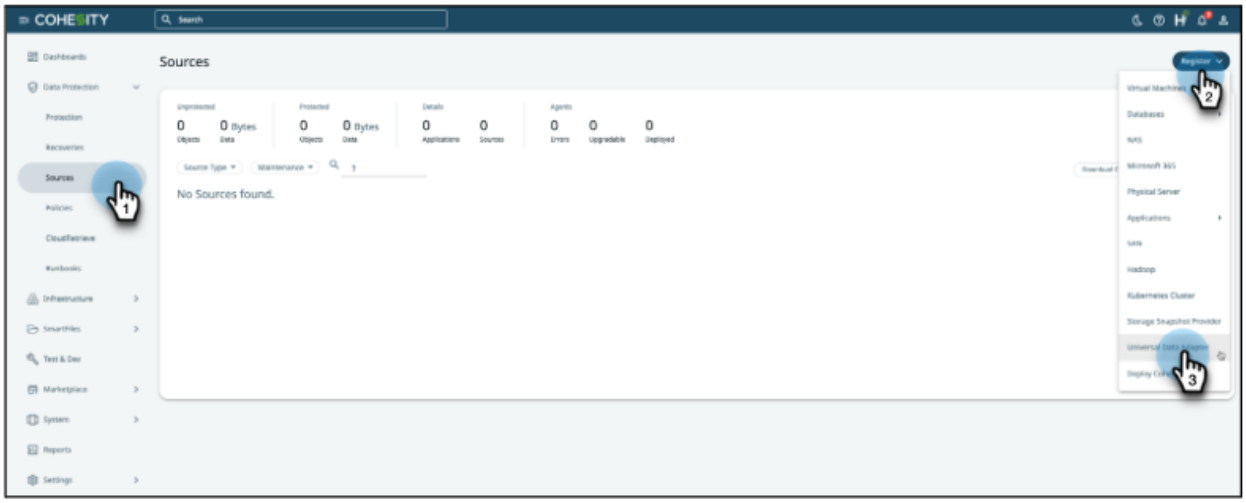
After you install the Cohesity Adapter and the IBM Db2 Connector, you must first register your database as a source on Cohesity, as shown in the screenshots below.

## Register The Database As A Source

To protect your tenant databases with Cohesity, register them as a Cohesity source. Once they're registered in Cohesity, you can add them to a Protection Group and configure the settings for your databases.

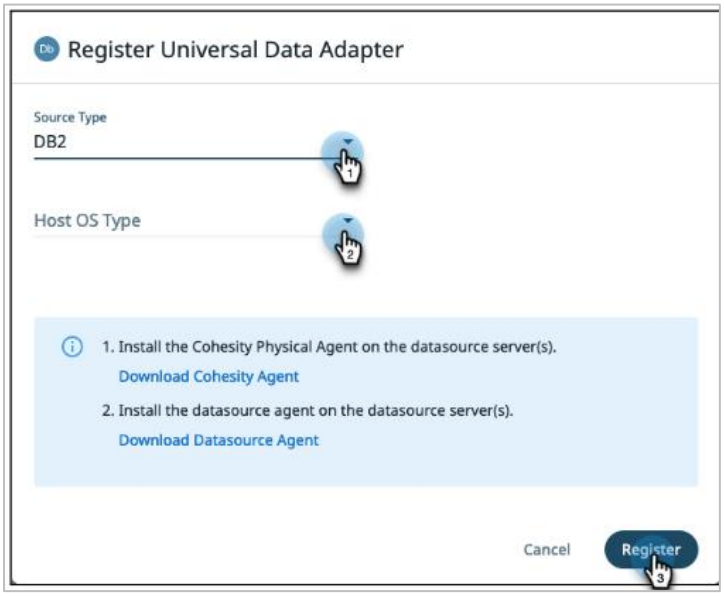
To register your database as a Source in Cohesity:

1. Navigate to **Sources** > **Register** > **Universal Data Adapter**.

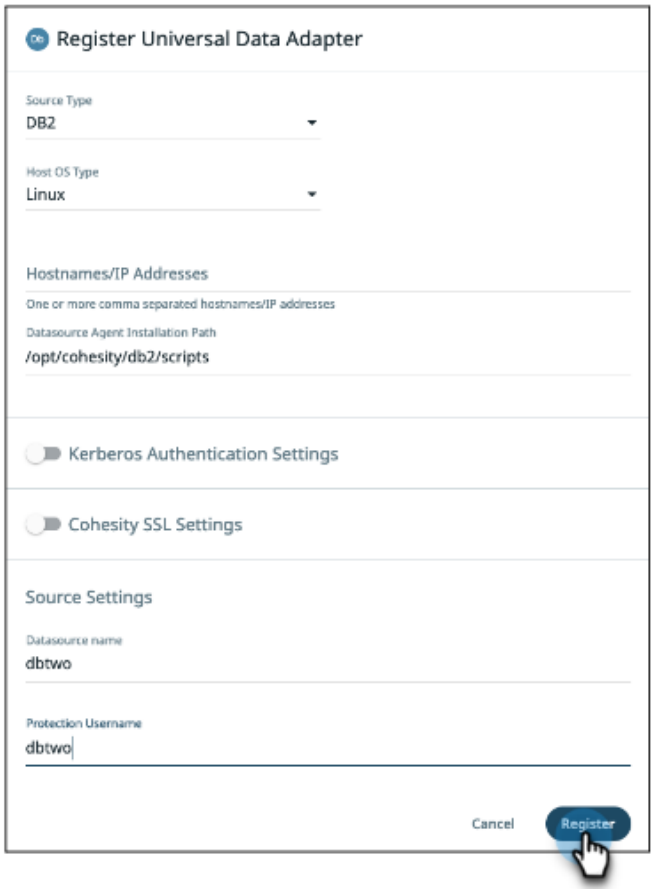



The **Register Universal Data Adapter** form will guide you through the types of databases and their host operating systems it supports.

2. In the **Register Universal Data Adapter** form, select IBM Db2 from the **Source Type** drop-down list. Then, select Linux from the **Host OS Type** drop-down list, which is the type of OS the host is running.




3. A completed form will automatically expand with more options.
4. Complete all the fields in the form and click **Register**.



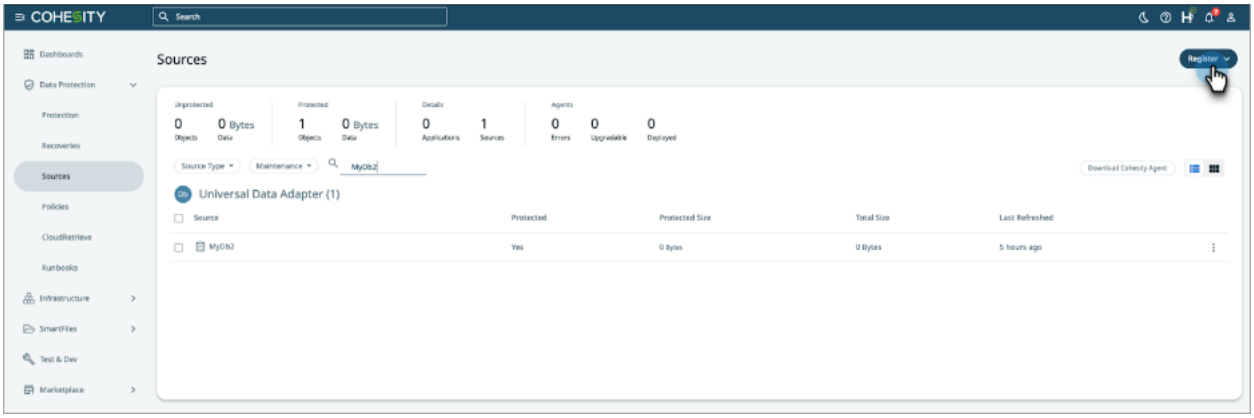
Complete the form options as follows:

a. **Source Type:** Select the database type.
b. **Host OS Type:** A dynamic list of OS types based on the **Source Type**.
c. **Hostname/IP Addresses**. The name or IP address of the host.
d. **Installation Path:** Default Path on the host.
e. **App Authentication:** This does not apply to IBM Db2.

You can find more information about registering your IBM Db2 host at Register and Manage the IBM Db2 Source.

Complete your source registration by clicking **Register.**

Successful Registration




You can update, refresh, and unregister your database source from the **Sources** page.

To protect your newly registered Source, you'll create a Cohesity Protection Group for it in the next chapter.

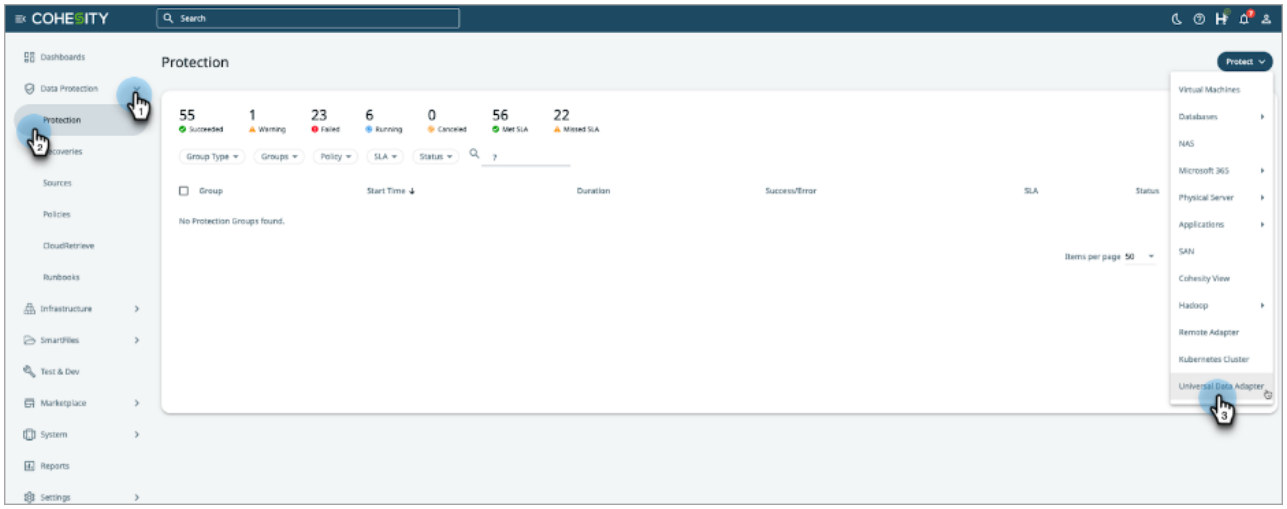
# IBM Db2 Database Protection

After registering the IBM Db2 host as a source on Cohesity, you can start configuring your backups.

## Create a Protection Group

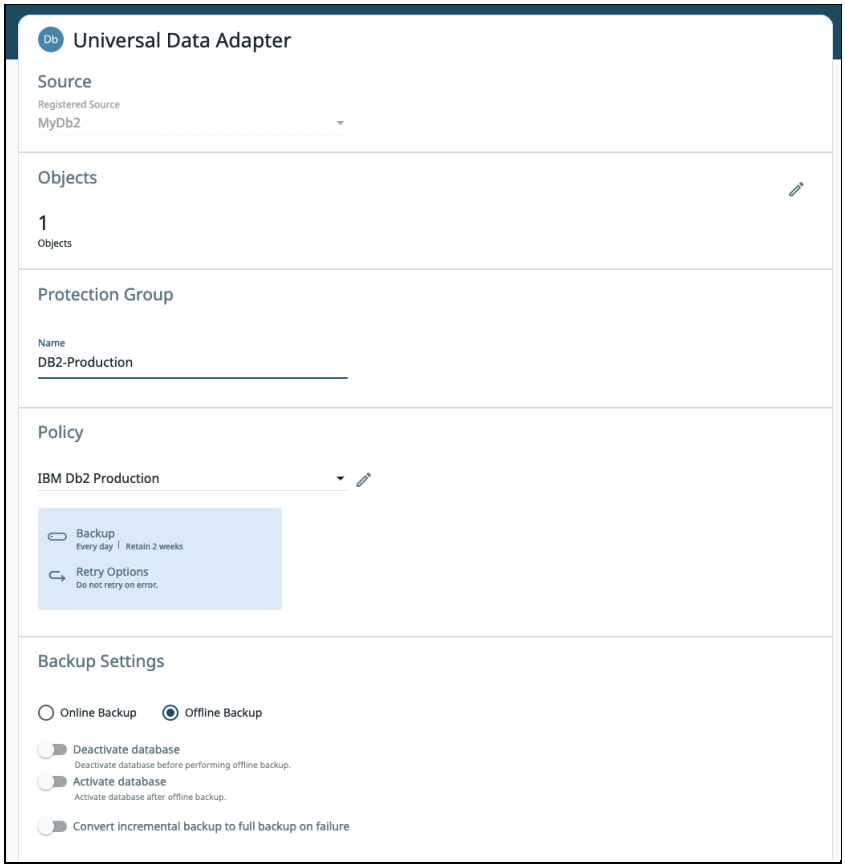
To create a Protection Group:

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



2. In the **New Protection** form, under **Source**, select the Source you registered earlier.

   New Protection Group Form




3. In this form, enter the name of the database in **Objects**.
4. Enter a unique Protection Group **Name.**

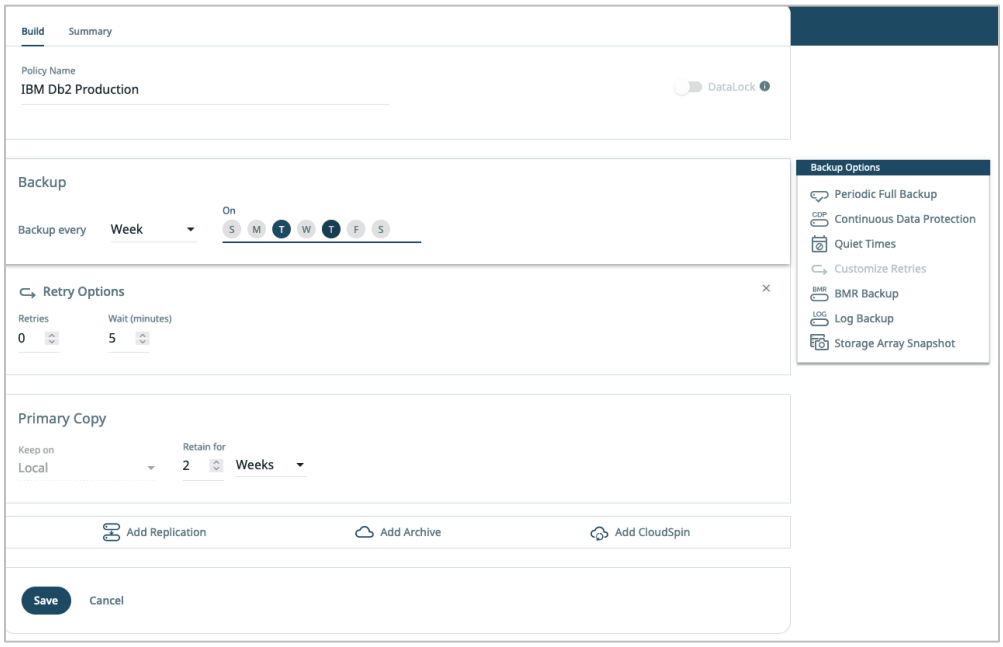
> **TIP**: Give your Protection Group a descriptive name that identifies the kind of data being protected and how it is managed. This will help you identify and manage your backups as your environment grows. Use descriptors such as production (PROD), critical, infrastructure (INFRA), financial, sales, primary, secondary, and employees (EMP).
>
> For example:
>
> | | |
> |---|---|
> | Production_Sales | DataCenter_Dallas_Production |
> | Critical_Infrastructure | Production_ReplicatedTo_DRsite |
> | Archive_LongRetention | Development_User_Data |

5. Continue by selecting a **Policy.**

   You can use the default standard policies or create your own. Policies save time because they reduce the effort required to enter settings repetitively.

   A policy is a reusable set of settings that define how and when objects are protected, replicated, or archived. When configuring a protection group, you select which policy to use.

   Create a Protection Policy Page




**IMPORTANT**: The Policy defaults to an IBM Db2 Incremental backup. You must add a Periodic Full Backup. In this example, a FULL backup is scheduled every Saturday, followed by Incremental backups on M, W, and F. Without the Full backup, you cannot restore the tenant database. The Policy should not contain a log backup.

### Retention for Backups

DBAs maintain a combination of backups to restore a tenant database to any point in time. A good combination of backups consists of FULL, INCREMENTAL, DIFFERENTIAL, and LOG backups.

**IMPORTANT**: Cohesity recommends you take a periodic FULL Backup.

Database restores must begin with a FULL database backup. You can apply a DIFFERENTIAL to FULL and apply LOG backups in sequence to complete the database restore.

**IMPORTANT**: You can elect to prune the IBM DB2 transaction logs before the latest full backup, thus preventing the log archival location from running out of space.

When you apply backups during the tenant database restore process, you are sequentially adding the captured changes to the database:

FULL+DIFF+Log1+Log2+Log3 = Restored tenant database.

**IMPORTANT**: Database backups, differentials, and logs depend on a FULL backup to perform a database restore. IBM Db2 tenant databases require that to restore a database. You must start with a FULL backup and then apply its transaction logs. This means your backup retention policy must keep a FULL backup along with its LOG backups to successfully restore a tenant database.

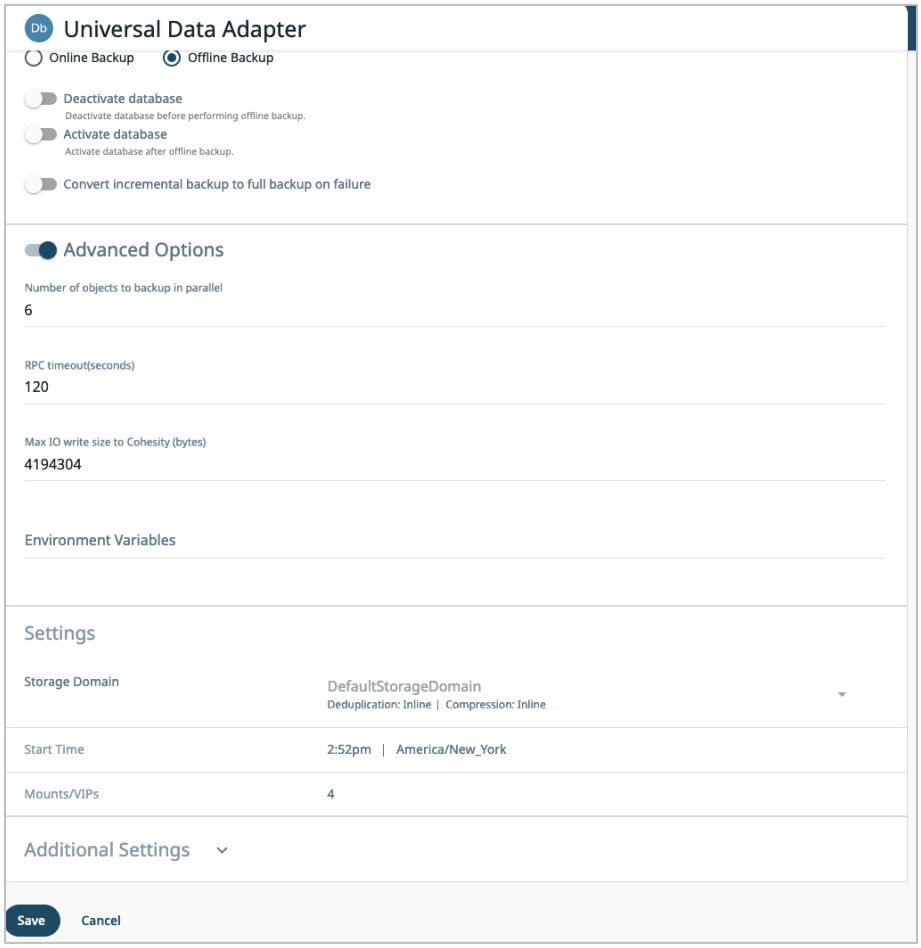
Simply put, a tenant database restore requires a FULL backup to seed the database, then DIFFERENTIAL and/or LOG backups are applied to roll the database forward to the specified point in time.

We recommend retaining two sets of FULL backups with their DIFFERENTIAL.

Once you set the Policy for a Protection Group, Cohesity manages all the databases assigned to that Protection Group similarly.

For more information about Policy features, see Create or Edit a Standard Policy in the online Help.

Continue defining the **New Protection Group** by selecting the remaining settings.



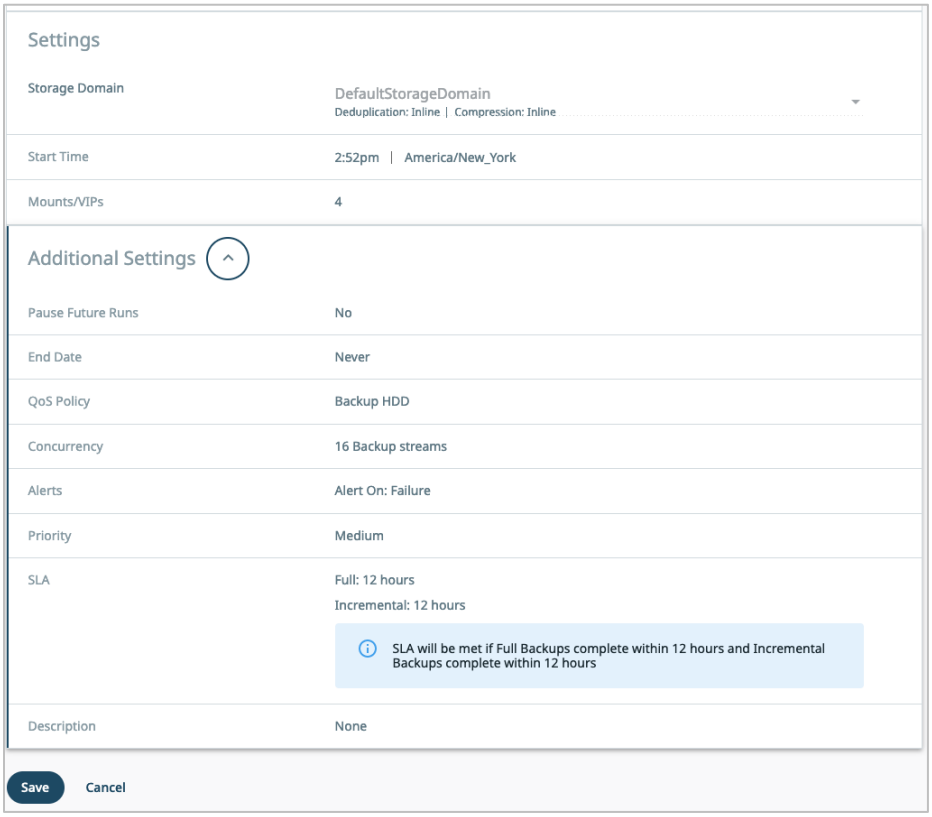
6. **Offline Backup:** enable if you want to periodically perform an online and offline backup on the same database.

   **NOTE**: Offline backups are an Early Access feature. Contact your Cohesity account team to enable the feature.

   **OFFLINE BEST PRACTICES:**

   1. Create a Protection Group for online backup, for example, DB1_online_backup.
   2. Create a different Protection Group for offline backup, for example, DB1_offline_backup.
   3. Always keep the Protection Group, DB1_offline_backup, in a paused state.
   4. Run the Protection Group, DB1_offline_backup, as per the defined schedule in the protection policy.
   5. When you want to perform an offline backup, pause the Protection Group for online backup, DB1_online_backup, and wait for the current protection run to finish before triggering the offline backup.
   6. Perform the offline backup using the RunNow option and bring the database online.
   7. Unpause the Protection Group for online backup, DB1_online_backup.

8. **Storage Domain:** 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.
9. **Start Time**: Take the default.

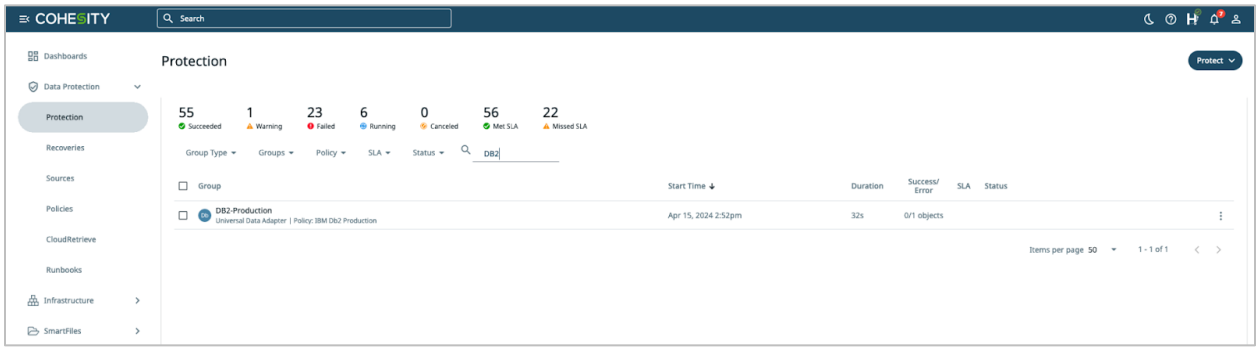


10. **Mounts/VIPS:** Enter the number of VIPs on your Cohesity cluster.
11. **Concurrency:** Enter two times the number of VIPS. We recommend you use a multi-stream approach, which dramatically shortens the backup time compared to a single stream. You may want to experiment with the number of streams in your backup to determine the optimal performance gain for a multi-stream approach.

**IMPORTANT**: You can balance performance between the number of VIPs and backup streams using **Concurrency**.

After you have completed the Settings, if you need to change any additional settings on the New Universal Data Adapter Protection Group page, scroll down and click Edit on the right.

Your new Protection Group is active and running and appears on the **Protection** page.




Now that you have created a Protection Group for your tenant databases, you may change the Protection Policy and settings. This way, Cohesity manages all your tenant databases in this Protection Group.

For example, keep your tenant backups for a longer period of time and increase the retention setting in the Policy assigned to this Protection Group.

**IMPORTANT**: A policy change is not retroactive to previous backup runs but only applies to the next runs.

# IBM Db2 Database Restore

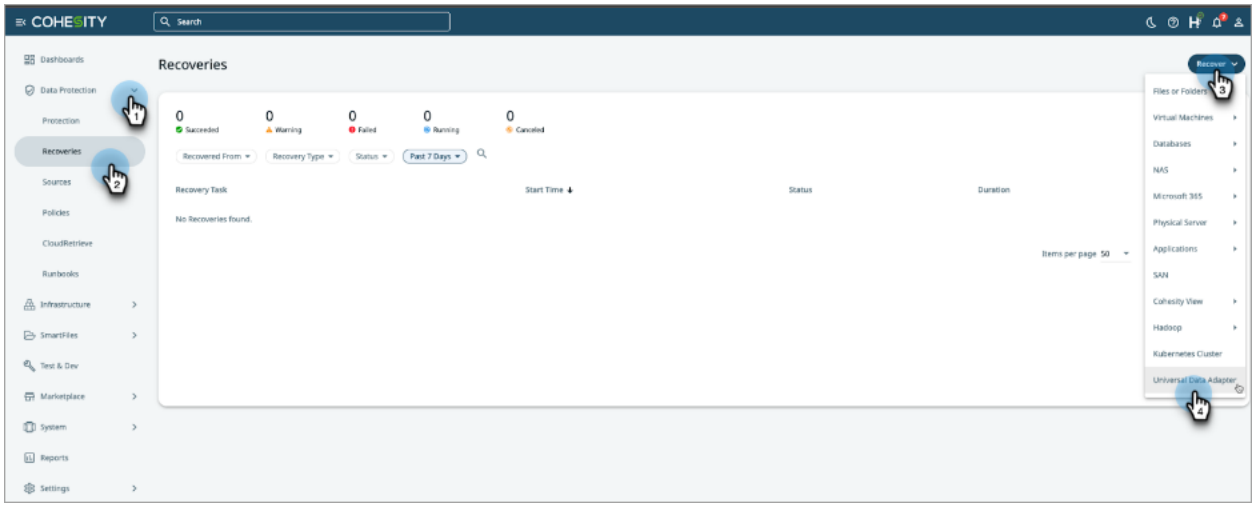
Cohesity allows you to restore tenant databases to their original or alternate locations.

IBM Db2 requires you to create an empty database into which you will restore the data.

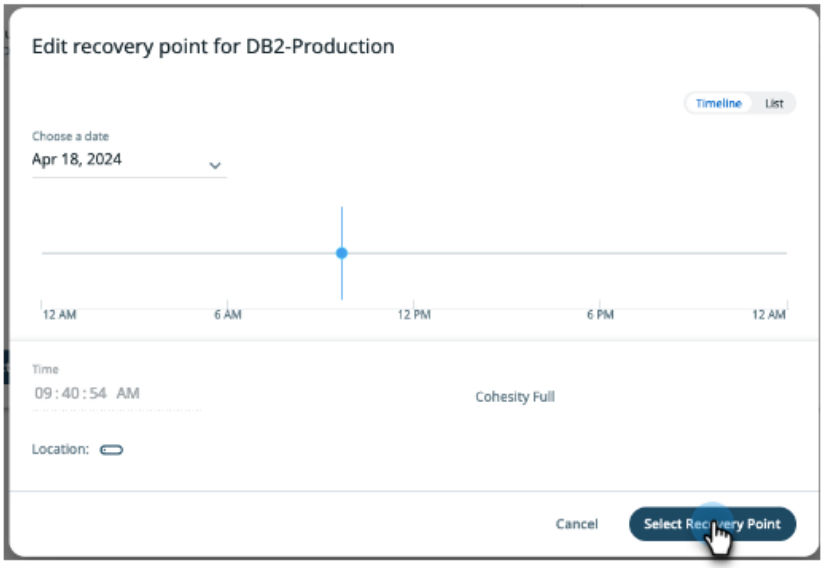
## Restore Specific Backup

To restore the database:

1. Log in to Cohesity, navigate to **Data Protection** > **Recoveries**, and click **Recover** > **Universal Data Adapter**.



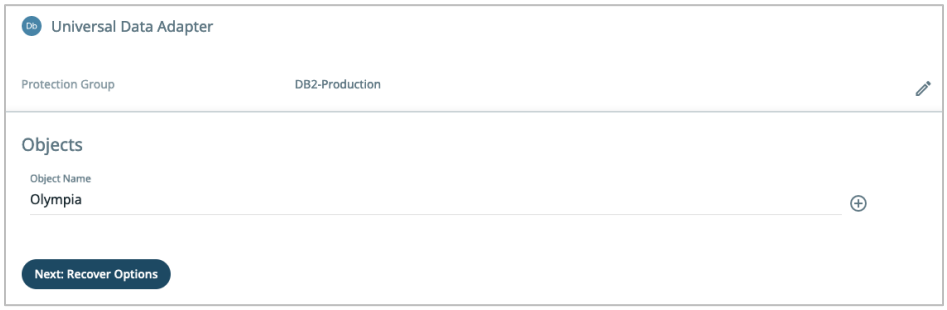

2. Search for the backup. You can start with the wildcard "*****" to get a general listing.
3. Using the **Edit Recovery Point** form, choose a recovery point and click **Select Recovery Point**. FULL, Incremental, and DIFFERENTIAL snapshots are shown as blue dots.



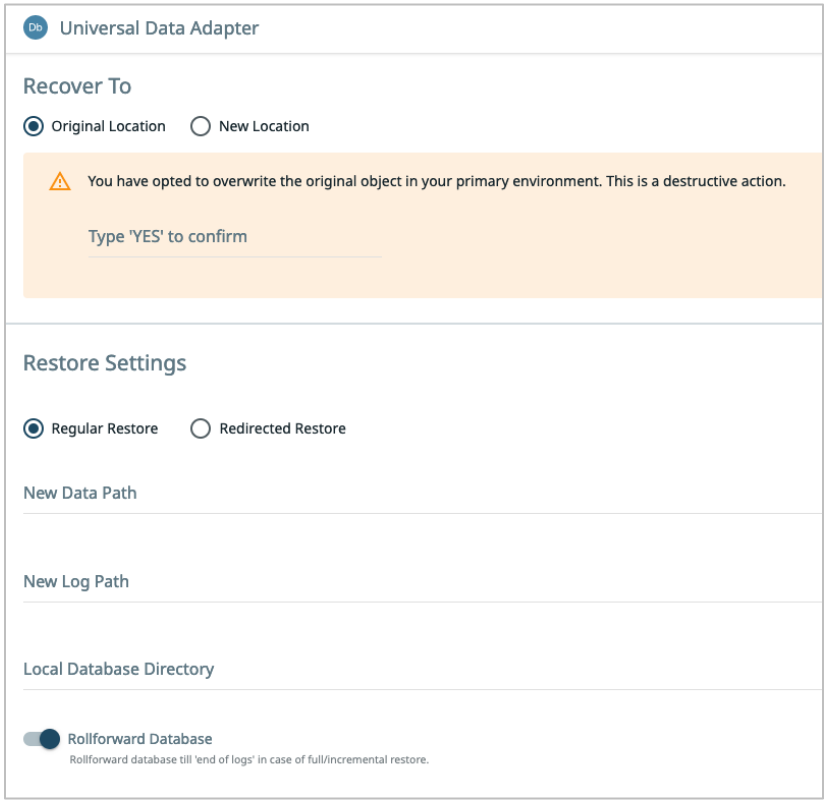
**Select a Recovery Point:** Use the slider to choose a valid date.

- The timeline shows 24 hours with valid backups.
- Each blue dot on the timeline represents FULL, Incremental, or DIFFERENTIAL backup points.
- Blue dots can sometimes be clumped together if the backups are taken frequently.
- The green line represents valid log ranges.
- Gaps in the green line represent breaks in the log chain.
- When positioned in an invalid range, the slider will snap back to the latest valid time.

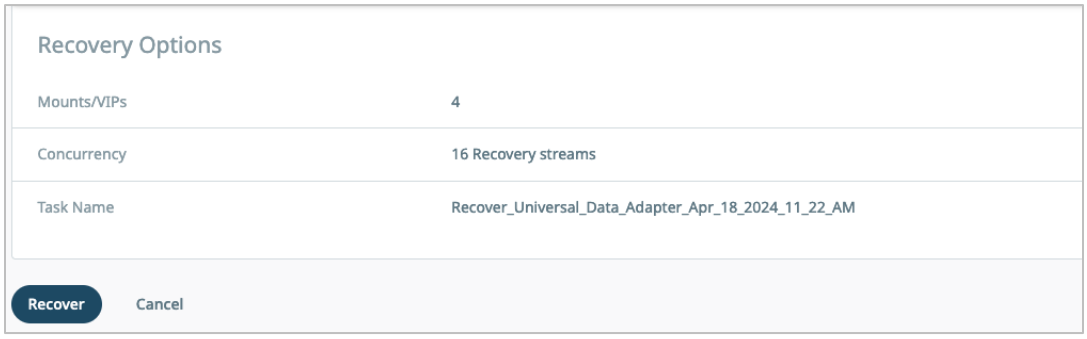
4. Select the recovery point and complete the recovery options.




5. Enter the name of the database in **Objects**.
6. **Recover As**: Select **New Object** to restore to an alternate server.



**IMPORTANT**: If you choose to restore to a **New Location**, IBM Db2 requires that you create the empty object on the target server before initiating a restore.




7. **Mount/VIPs:** Equal to the number of VIPs on the Cohesity cluster.
8. **Concurrency:** Enter two times the number of VIPs for best performance.

# Your Feedback

Was this document helpful? Send us your feedback!

# About the Authors

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

Other essential contributors included:

- Roland Kastner is a Solutions Architect.
- Diana Yang is a Principal Solutions Architect

# Document Version History

| VERSION | DATE | DOCUMENT HISTORY |
|---|---|---|
| 1.0 | June 2024 | First Release |

# ABOUT COHESITY

Cohesity is a leader in AI-powered data security and management. Aided by an extensive ecosystem of partners, Cohesity makes it easier to protect, manage, and get value from data – across the data center, edge, and cloud. Cohesity helps organizations defend against cybersecurity threats with comprehensive data security and management capabilities, including immutable backup snapshots, AI-based threat detection, monitoring for malicious behavior, and rapid recovery at scale. Cohesity solutions are delivered as a service, self-managed, or provided by a Cohesity-powered partner. Cohesity is headquartered in San Jose, CA, and is trusted by the world's largest enterprises, including six of the Fortune 10 and 42 of the Fortune 100.

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