Back up a database

The backup options for Redis Enterprise Cloud databases depend on your plan:

- Flexible and Annual subscriptions can perform backups on-demand and schedule daily backups that occur during a set hour.
- Paid Fixed plans can perform backups on-demand and schedule backups that occur every 24 hours.
- Free plans do not back up automatically.

Backups are saved to pre-defined storage locations available to your subscription.

Backup locations need to be available before you enable database backups. To learn more, see Set up backup storage locations.

Here, you'll learn how to store backups using different cloud providers.

Enable backups

To enable backups for a database:

1. Sign in to the Redis Cloud admin portal. (Create an account if you don't already have one.)
2. If you have more than one subscription, select the target subscription from the list. This displays the Databases tab for the selected subscription.
3. Select the database to open the Database page and then select Edit database.
4. In the **Durability** section of the **Configuration** tab, locate the **Remote backup** setting:
When you enable **Remote backup**, additional options appear. The options vary according to your subscription.

### Interval
- **Every 24 hours**
- **Set backup time**

### Backup time
- **12am (00:00) (UTC)**

### Storage type
- **FTP**

### Setting name | Description
--- | ---
**Interval** | Defines the frequency of automatic backups. Paid fixed accounts are backed up every 24 hours. Flexible and Annual subscriptions can be set to 24, 12, 6, 4, 2, or 1 hour backup intervals.

**Set backup time** | When checked, this lets you set the hour of the **Backup time**. *(Flexible and Annual subscriptions only)*

**Backup time** | Defines the hour automatic backups are made. Note that actual backup times will vary in order to minimize customer access disruptions. *(Flexible and Annual subscriptions only)*

**Times are expressed in Coordinated Universal Time (UTC).**

**Storage type** | Defines the provider of the storage location, which can be: AWS S3, Google Cloud Storage, Azure Blob Storage, or FTP (SFTP).

**Backup destination** | Defines a URI representing the backup storage location.

### Back up data on demand

Once backups are enabled, you can back up your data at any time. Use the **Backup Now** button in the **Durability** section.

**Backup now**

Backups need to be enabled before the button appears.

### Set up backup storage locations

Database backups can be stored to a cloud provider service or saved to a URI using FTP/SFTP.

When stored to a cloud provider, backup locations need to be available on the same provider in the same region as your
Your subscription needs the ability to view permissions and update objects in the storage location. Specific details vary according to the provider. To learn more, consult the provider’s documentation.

The following sections help set things up; however, provider features change frequently. For best results, use your provider’s documentation for the latest info.

AWS Simple Storage Service

To store backups in an Amazon Web Services (AWS) Simple Storage Service (S3) bucket:

1. Sign in to the AWS Management Console.
2. Use the Services menu to locate and select Storage > S3. This takes you to the Amazon S3 admin panel.
3. If you do not already have a bucket for backups, select the Create Bucket button in the upper, right corner of the Buckets panel.
   1. When the Create bucket screen appears, enter a name for your bucket.
   2. Set AWS Region to an appropriate region.
   3. Set other properties according to your company standards.
   4. When finished, select the Create bucket button near the bottom of the screen.
4. Use the Buckets list to locate and select your bucket. When the settings appear, select the Permissions tab, locate the Access control list (ACL) section, and then select the Edit button.
5. When the Edit access control list (ACL) screen appears, locate the Access for other AWS accounts section and then select the Add grantee button.
   1. In the Grantee field, enter: fd1b65415aa5ea3a310265ddb13b156c7c76260dcb87e037a8fc290c3c86b614
   2. In the Objects list, enable Write.
   3. In the Bucket ACL list, enable Read and Write.
   4. When finished, select the Save changes button.

Once the bucket is available and the permissions are set, use the name of your bucket as the Backup destination for your database’s Remote backup settings. For example, suppose your bucket is named backups-bucket. In that case, set Backup destination to s3://backups-bucket.

GCP Storage

For Google Cloud Platform (GCP) console subscriptions, store your backups in a Google Cloud Storage bucket:

2. In the admin console menu, locate the Storage section than select Cloud Storage > Browser.
3. Create or select a bucket.
4. Select the overflow menu (three dots, stacked) and then select the Edit Bucket Permissions command.
5. Select the Add members button and then add:
   service@redislabs-prod-clusters.iam.gserviceaccount.com
7. Save your changes.

8. Verify that your bucket does not have a set retention policy.

   To do so:
   1. View the details of your bucket.
   2. Select the Retention tab.
   3. Verify that there is no retention policy.

   If a policy is defined and you cannot delete it, you need to use a different bucket.

Use the bucket details Configuration tab to locate the gsutil URI. This is the value you’ll assign to your resource’s backup path.

**Azure Blob Storage**

To store your backup in Microsoft Azure Blob Storage, sign in to the Azure portal and then:

1. Create an Azure Storage account if you do not already have one
2. Create a container if you do not already have one
3. Manage storage account access keys

Set your resource’s Backup Path to the path of your storage account.

The syntax for creating the backup varies according to your authorization mechanism. For example:

```
abs://:storage_account_access_key@storage_account_name/container_name/[path/]
```

Where:

- **storage_account_access_key**: the primary access key to the storage account
- **storage_account_name**: the storage account name
- **container_name**: the name of the container, if needed.
- **path**: the backups path, if needed.

To learn more, see Authorizing access to data in Azure Storage

**FTP Server**

To store your backups on an FTP server, set its Backup Path using the following syntax:

```
<protocol>://[username]:[password]@[hostname]:[port]/[path]/
```

Where:

- **protocol**: the server’s protocol, can be either ftp or ftls.
- **username**: your username, if needed.
- **password**: your password, if needed.
- **hostname**: the hostname or IP address of the server.
- **port**: the port number of the server, if needed.
• **path**: the backup path, if needed.

The user account needs permission to write files to the server.

**Updated**: September 29, 2021