

Backups

- [Overview](#)
- [Manual Local backups](#)
- [Automated Remote Backups \(Borg\)](#)
- [Automated VM Snapshots](#)
- [Automated External Backups \(S3\)](#)
- [How to Create AWS Access and Secret Key for External backups \(S3\)](#)
- [How to Create Bucket in AWS for External backups \(S3\)](#)

Overview

A robust backup strategy is fundamental to keeping data safe.

By default, Elest.io automates a 3-2-1 backup strategy for all new services.

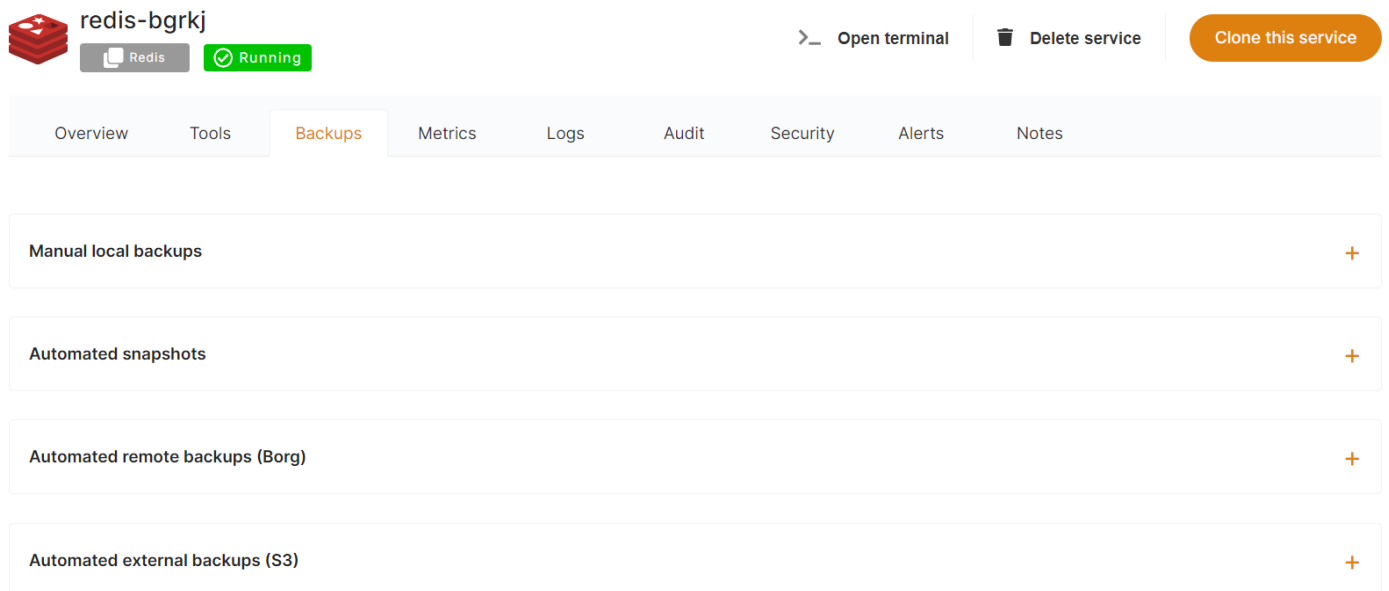
3 copies of your data exist at all times.

2 are kept in geographically distinct data centers in your selected region.

1 backup is kept on-site for fast restoring.

- [Automated remote backups](#)
- [Automated VM Snapshots](#)
- [Local backups](#)
- [External Backups](#)

Each backup type has different retention periods and characteristics.



The screenshot displays the management interface for a Redis service named 'redis-bgrkj'. At the top, there is a service status bar with a Redis icon, the name 'redis-bgrkj', a 'Redis' label, and a green 'Running' indicator. To the right of the status bar are three action buttons: 'Open terminal', 'Delete service', and 'Clone this service'. Below the status bar is a navigation menu with tabs for 'Overview', 'Tools', 'Backups', 'Metrics', 'Logs', 'Audit', 'Security', 'Alerts', and 'Notes'. The 'Backups' tab is currently selected. The main content area lists four backup types, each with a plus sign icon on the right for expansion:

- Manual local backups
- Automated snapshots
- Automated remote backups (Borg)
- Automated external backups (S3)

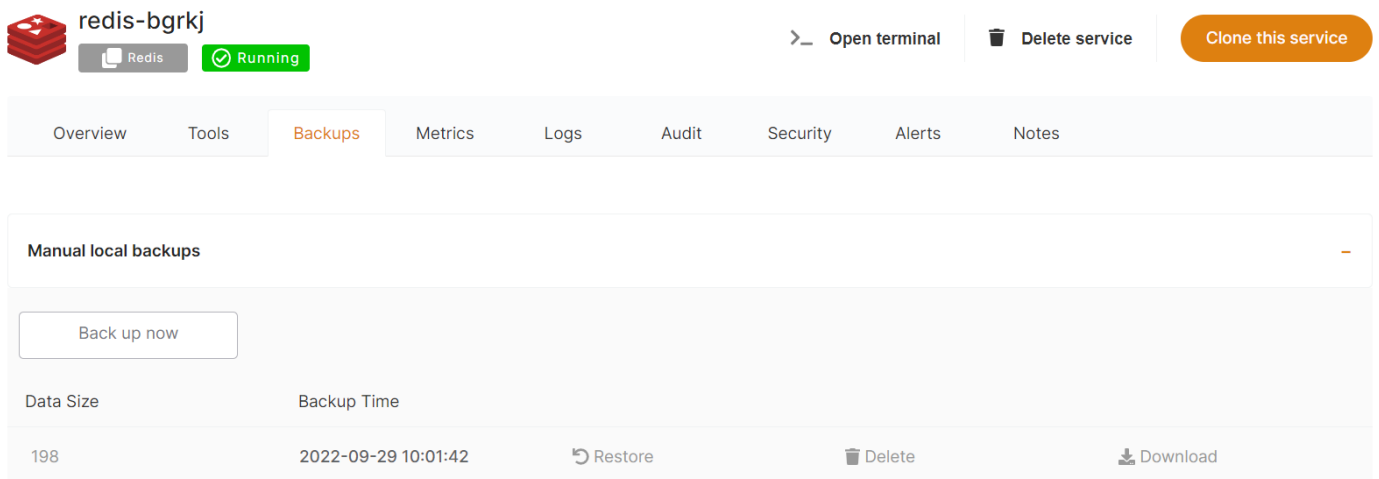
Manual Local backups

Local backups are useful if you need to take a quick backup of a small dataset locally and want to download the backup to your computer, or just be able to restore it later quickly.

Local backups only contain the software's data volume, not the OS or software itself.

Instructions:

From the service dashboard, click on the *Backups* tab, then click on *Manual Local Backups*. From there you can make new manual backups, list existing backups, download, restore or delete previous local backups.



The screenshot shows the service dashboard for 'redis-bgrkj'. At the top, there are buttons for 'Redis', 'Running', 'Open terminal', 'Delete service', and 'Clone this service'. Below this is a navigation bar with tabs for 'Overview', 'Tools', 'Backups', 'Metrics', 'Logs', 'Audit', 'Security', 'Alerts', and 'Notes'. The 'Backups' tab is selected. Underneath, there is a section titled 'Manual local backups' with a 'Back up now' button. Below that is a table with columns for 'Data Size', 'Backup Time', and actions like 'Restore', 'Delete', and 'Download'.

Data Size	Backup Time	Restore	Delete	Download
198	2022-09-29 10:01:42			

You are responsible for deleting manual backups to regain disk space. Elest.io will not automatically delete them.

Manual backups use the available disk space of your service.

Automated Remote Backups (Borg)

Remote backups are sent to another datacenter in the same continent that your service (Ashburn USA for the US, Germany for EU zone and rest of the world). We use [Borg Backups](#) to do incremental backups with deduplication. It's very fast and efficient. This kind of backup includes only the data, not the software itself.

From the Dashboard, click on the *Backups* tab, then click on *Automated Remote Backups*. From there you can make new manual backups, list existing backups or restore a backup.



appdrag-uptime

ubuntu-20.04

Running

Overview

Tools

Backups

Metrics

Logs

Audit

Security

Alerts

Notes

Manual Local Backups

Automated Remote Backups

Enable/Disable backups

 Disable backup will delete existing backups

Take a backup

Backup Time

Restore

2022-01-24 03:00:03

 Restore

2022-01-23 23:00:03

 Restore

2022-01-23 20:00:03

 Restore

2022-01-23 03:00:04

 Restore

2022-01-22 23:00:02

 Restore

2022-01-22 20:00:03

 Restore

Retention periods depend on your support plan: 7 days on Standard, 14 days on Premium and 30 days on Enterprise.

Partial restoration / mount backups

It's possible to do partial restorations by mounting the backups into the VM and exploring them to copy only few files with this process:

1. Open the terminal and type this:

```
cd /opt/borg;  
./backupMount.sh;
```

2. You can then explore the mounted backups in /mnt/backups-mount from there you can copy some files to your real app folder in /opt/app/
3. **WARNING:** do not forget to unmount the backups after usage with this command:

```
cd /opt/borg;  
./backupUmount.sh;
```

Automated VM Snapshots

VM snapshots are made using the provider's snapshot API and are stored in the same region where you have your service.

It is only available under Support Plans Levels 2 and 3.

It's a full snapshot of the VM, meaning it contains everything: OS, Apps, data, etc.

To make a snapshot

From the Dashboard:

1. Click on the *Backups* tab
2. Click on *Automated Snapshots*

redis-bgrkj

Redis Running

>_ Open terminal Delete service Clone this service

Overview Tools **Backups** Metrics Logs Audit Security Alerts Notes

Manual local backups +

Automated snapshots -

Enable/Disable snapshots ⚠ Disabling snapshots will delete all existing snapshots Disable snapshot

Take a snapshot Refresh

Data Size	Image Size	Backup Time	Status		
20 GB	1.58 GB	2022-09-29 11:04:43	Completed	Restore	Delete

From there you can take new a manual snapshot, list existing snapshots or restore a snapshot.

Retention periods depend on your support plan: 2 snapshots on Level 2, and 4 snapshots on Level 3.

Restoring from a snapshot will overwrite the whole VM with the selected snapshot.

Automated External Backups (S3)

External backups are stored in your S3 bucket, so **you own your backups** directly. Elestio's external backup service is compatible with AWS S3 and any S3-compatible provider.

To enable external backups from the service dashboard click on the *Backups* tab, then click on *Automated External Backups*.

You will have to provide your S3 details. (endpoint, bucket name, API key, secret key)

Before entering the bucket

Please update S3 configuration ✕

Select Provider AWS S3 Other compatible S3 providers

End point

API key

Secret key

Bucket name

Prefix (path in your bucket)

You can click on the "Verify Config" button to validate your settings.

Once activated, you will be able to click on Settings to configure the backups schedule. You can also take an external backup at any time with the "Take a backup" button.

Automated external backups (S3)

Enable/Disable backups ⚠️ Disable backups will delete existing backups Disable backup

Take a backup Refresh Update S3 Config Setting

Key	Data Size	Backup Time			
..backups_2022-03-08-07.47.14.gz	874 KB	2022-03-08 07:47:15	Restore	Download	Delete
..backups_2022-03-08-06.37.55.gz	874 KB	2022-03-08 06:37:55	Restore	Download	Delete
..backups_2022-03-08-06.36.28.gz	874 KB	2022-03-08 06:36:29	Restore	Download	Delete

If you click on Settings, you can configure the backups schedule and a number of backups to retain.

Update Backup Cycle ✕

Please indicate your preferred period to take the backup.
Select Period Every Day Hourly

Time

Number of backups to retain

Update Setting

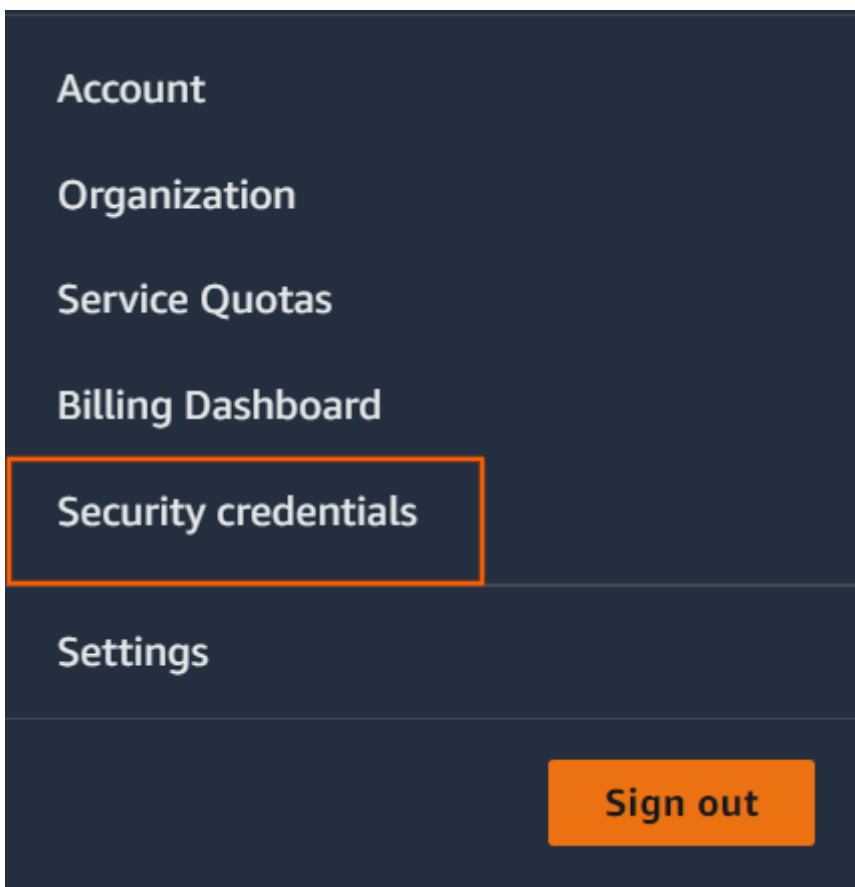
Refresh

If you don't have access to an AWS S3 bucket or an S3 bucket from another provider, you can [deploy Minio](#) to get your own S3 Bucket

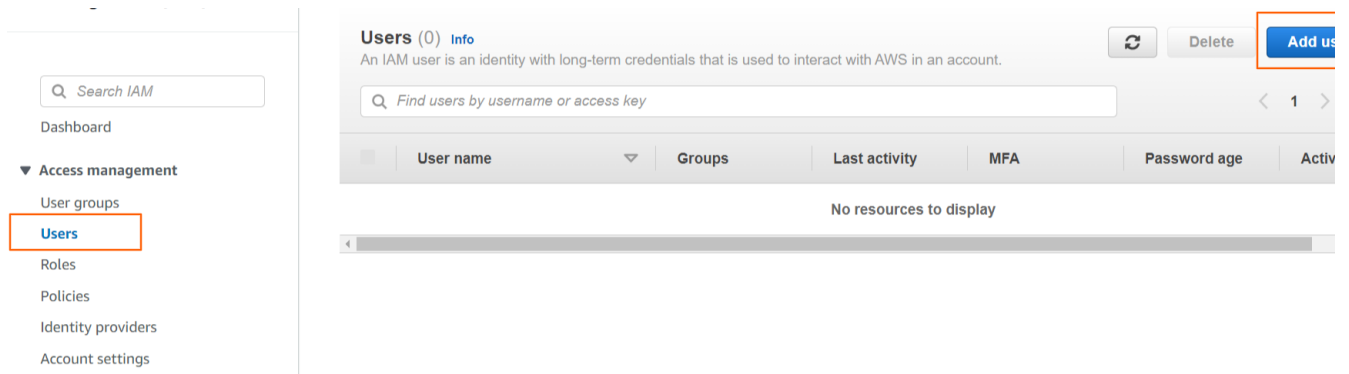
How to Create AWS Access and Secret Key for External backups (S3)

To create your AWS Access and Secret Key, follow these steps.

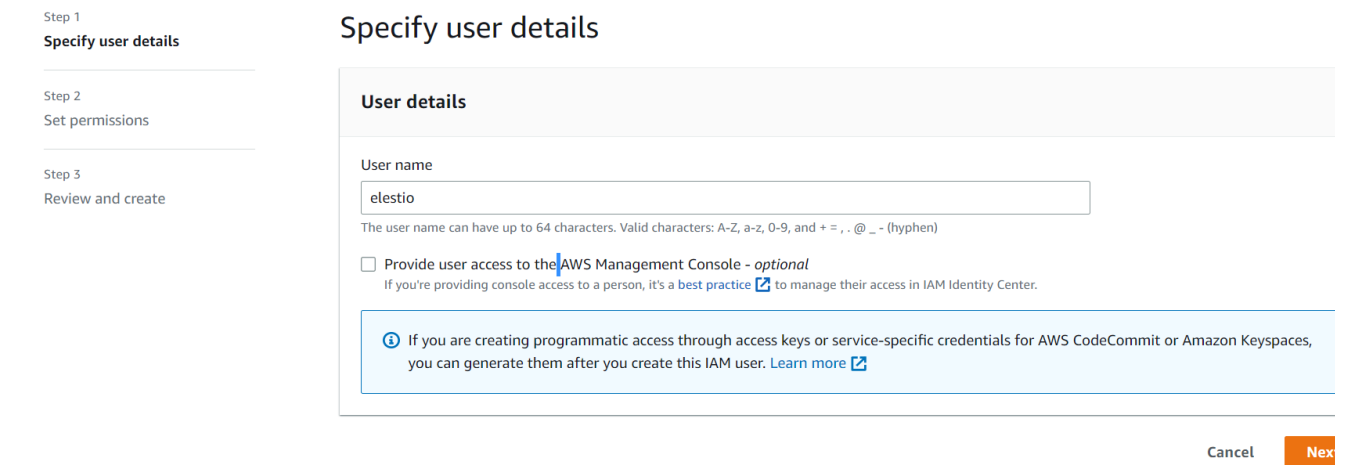
- **Step 1**:- Use your AWS account ID or account alias, your IAM user name, and your password to sign in to the [IAM console](#)
- **Step 2**:- In the navigation bar on the upper right, choose your user name, and then choose **Security credentials**.



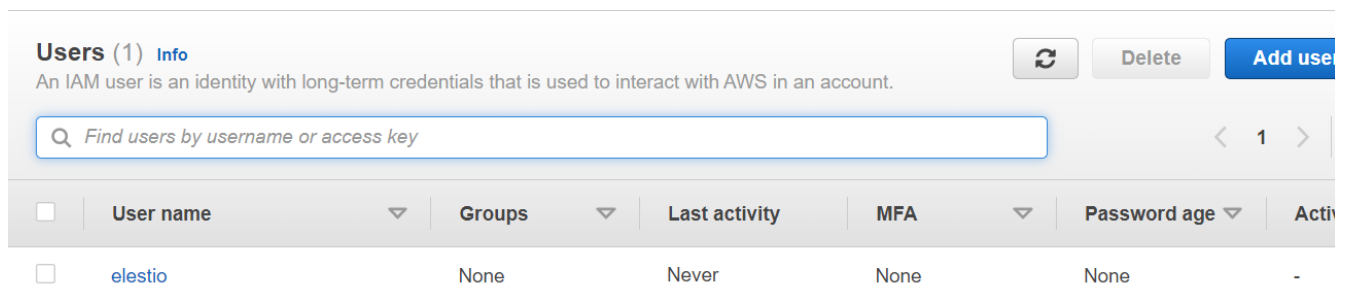
- **Step 3**:- If you want to create the AWS Access and Secret credentials with the root user, skip to **step 4**; otherwise, click **Users** on the left side of access management and then **Add users**.



Enter your AWS Account access user name and click Next, Next, Next and Create User to proceed.



After clicking the Create User button, you will be taken to the user list. Choose your created user name from the user list and click on it.



Navigate to **Security Credentials** under User Details.

Permissions | Groups | Tags | **Security credentials** | Access Advisor

Permissions policies (0) Refresh Remove Add permissions

Permissions are defined by policies attached to the user directly or through groups.

Find policies < 1 >

Policy name ↗	Type ▲	Attached via ↗
No policies		

- **Step 4:-** Select **Create access key** from the **Access keys section**. If you already have two access keys, this button is disabled, and you must delete one before creating a new one.

Access keys (0)

Use access keys to send programmatic calls to AWS from the AWS CLI, AWS Tools for PowerShell, AWS SDKs, or direct AWS API calls. You can have a maximum of two access keys (active or inactive) at a time. [Learn more](#) [↗](#)

Create access key

Access key ID	Created on	Access key last used	Region last used	Service last used	Status
No access keys					

As a best practice, avoid using long-term credentials like access keys. Instead, use tools which provide short term credentials. [Learn more](#) [↗](#)

Create access key

- On the **Access key best practices & alternatives** page, choose your use case to learn about additional options which can help you avoid creating a long-term access key. If you determine that your use case still requires an access key, choose **Other** and then choose **Next**.
- (Optional) Set a description tag value for the access key. This adds a tag key-value pair to your IAM user. This can help you identify and rotate access keys later. The tag key is set to the access key id. The tag value is set to the access key description that you specify. When you are finished, choose to **Create access key**.

For Non-Root Users:- Choose **Command Line Interface** as an alternative and check the box, then click Next and **Create Access Key**.

Step 1
Access key best practices & alternatives

Step 2 - optional
Set description tag

Step 3
Retrieve access keys

Access key best practices & alternatives

Avoid using long-term credentials like access keys to improve your security. Consider the following use cases and alternatives.

Command Line Interface (CLI)
You plan to use this access key to enable the AWS CLI to access your AWS account.

Local code
You plan to use this access key to enable application code in a local development environment to access your AWS account.

Application running on an AWS compute service
You plan to use this access key to enable application code running on an AWS compute service like Amazon EC2, Amazon ECS, or AWS Lambda to access your AWS account.

Third-party service
You plan to use this access key to enable access for a third-party application or service that monitors or manages your AWS resources.

Application running outside AWS
You plan to use this access key to enable an application running on an on-premises host, or to use a local AWS client or third-party AWS plugin.

Other
Your use case is not listed here.



Alternatives recommended

- Use [AWS CloudShell](#), a browser-based CLI, to run commands. [Learn more](#)
- Use the [AWS CLI V2](#) and enable authentication through a user in IAM Identity Center. [Learn more](#)

I understand the above recommendation and want to proceed to create an access key.

For Root User:- Check the box and click **Create Access Key**.

IAM > Security credentials > Create access key

Step 1
Alternatives to root user access keys

Step 2
Retrieve access key

Alternatives to root user access keys

Root user access keys are not recommended

We don't recommend that you create root user access keys. Because you can't specify the root user in a permissions policy, you can't limit its permissions, which is a best practice.

Instead, use alternatives such as an IAM role or a user in IAM Identity Center, which provide temporary rather than long-term credentials. [Learn More](#)

If your use case requires an access key, create an IAM user with an access key and apply least privilege permissions for that user. [Learn More](#)

Continue to create access key?

I understand creating a root access key is not a best practice, but I still want to create one.

Cancel **Create access key**

- **Step 5:-** On the **Retrieve access keys** page, choose either **Show** to reveal the value of your user's secret access key, or **Download .csv file**. This is your only opportunity to save your secret access key. After you've saved your secret access key in a secure location, choose **Done**.

Step 1
Alternatives to root user access keys

Step 2
Retrieve access key

Retrieve access key

Access key
If you lose or forget your secret access key, you cannot retrieve it. Instead, create a new access key and make the old key inactive.

Access key	Secret access key
<input type="text"/>	<input type="text"/> Hide

Access key best practices

- Never store your access key in plain text, in a code repository, or in code.
- Disable or delete access key when no longer needed.
- Enable least-privilege permissions.
- Rotate access keys regularly.

For more details about managing access keys, see the [Best practices for managing AWS access keys](#).

[Download .csv file](#) [Download](#)

- **Step 6:-** Now grant **Administration** access to the newly created keys.

“ Elestio requires a **AmazonS3FullAccess** permission to manage your external backups for service.

Navigate to permission in the user details to add the permission and select **Add Permission**

Permissions | Groups | Tags | Security credentials | Access Advisor

Permissions policies (0) [Refresh](#) [Remove](#) [Add permissions](#)

Permissions are defined by policies attached to the user directly or through groups.

< 1 >

Policy name ↗	Type	Attached via ↗
No policies		

Select the **Attach policies directly** Tab to attach permission.

Add permissions

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. [Learn more](#)

Permissions options

Add user to group

Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.

Copy permissions

Copy all group memberships, attached managed policies, inline policies, and any existing permissions boundaries from an existing user.

Attach policies directly

Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

Now Enter **AmazonS3FullAccess** into the search box and then select the **AmazonS3FullAccess** permission from the results.

Policy name	Type	Attached entities
AmazonS3FullAccess	AWS managed	0

If you only want to grant access to your bucket which you choose for backups instead of **AmazonS3FullAccess**, click Create Policy, paste this JSON policy in the JSON tab, and attach it.

```
{
  "Id": "BucketPolicy",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllAccess",
      "Action": "s3:*",
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::elestio",
        "arn:aws:s3:::elestio/*"
      ]
    }
  ]
}
```

Note:- If your bucket name is not elestio, then put your bucket name in place of elestio.

After Selecting both Click **Next** and then click **Add permission** to proceed.

Review

The following policies will be attached to this user. [Learn more](#)

User details

User name
elestio

Permissions summary (1)

Name	Type	Used as
AmazonS3FullAccess	AWS managed	Permissions policy

Cancel

Previous



Add permission

Follow these steps if you already have an access key and want to activate it instead of creating a new one.

- In the **Access keys** section, find the key to activate.

Access keys (1)
Use access keys to send programmatic calls to AWS from the AWS CLI, AWS Tools for PowerShell, AWS SDKs, or direct AWS API calls. You can have a maximum of two access keys (active or inactive) at a time. [Learn more](#)



Actions ▼ Create access key

Access key ID	Created on	Access key last used	Region last used	Service last used	Status
	11 minutes ago	None	N/A	N/A	 Inactive

- To activate the key, go to **Actions** and select **Activate**.

Access keys (1)
Use access keys to send programmatic calls to AWS from the AWS CLI, AWS Tools for PowerShell, AWS SDKs, or direct AWS API calls. You can have a maximum of two access keys (active or inactive) at a time. [Learn more](#)

Actions ▲ Create access key

Access key ID	Created on	Access key last used	Region last used	Service last used	Status
	11 minutes ago	None	N/A	N/A	 Inactive

Deactivate
Activate
Delete

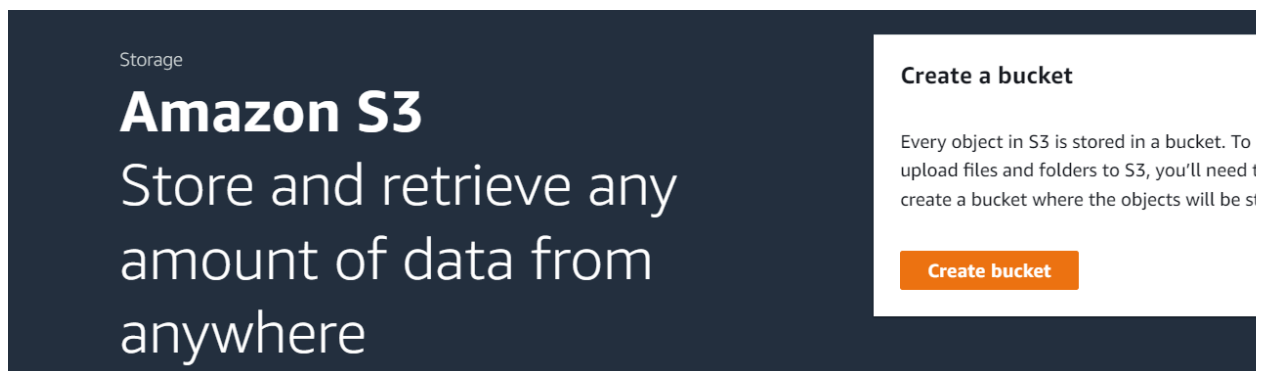
Before adding keys to elestio, you must grant Administration access to them.

“ View our [documentation](#) to learn how to create Bucket in AWS S3.

How to Create Bucket in AWS for External backups (S3)

To create your bucket for backups, follow these steps.

- **Step 1:-** Use your AWS account ID or account alias, your IAM user name, and your password to sign in to the [IAM console](#)
- **Step 2:-** Search for S3 in the **Services** section of the navigation menu on the top left, or just click [here](#) to go.
- **Step 3:-** Click the **Create Bucket** button for the next step.



Storage

Amazon S3

Store and retrieve any amount of data from anywhere

Create a bucket

Every object in S3 is stored in a bucket. To upload files and folders to S3, you'll need to create a bucket where the objects will be stored.

Create bucket

- **Step 4:-** Give your bucket a name in the **Bucket name** column, and in the **AWS Region** column, choose the region where you want to create it.

Create bucket [Info](#)

Buckets are containers for data stored in S3. [Learn more](#)

General configuration

Bucket name

Bucket name must be globally unique and must not contain spaces or uppercase letters. [See rules for bucket naming](#)

AWS Region

Copy settings from existing bucket - *optional*

Only the bucket settings in the following configuration are copied.

- **Step 5:-** After you've completed both columns, scroll down and click the **Create Bucket** button to create it.
- **Step 6:-** Your bucket will be created and listed in buckets following these successful steps.

► **Account snapshot** [View Storage Lens d](#)
Storage lens provides visibility into storage usage and activity trends. [Learn more](#)

Buckets (2) [Info](#)

Buckets are containers for data stored in S3. [Learn more](#)

	Name ▲	AWS Region ▼	Access ▼	Creation date
<input type="radio"/>	elestio	EU (Ireland) eu-west-1	Bucket and objects not public	April 21, 2023, 20:14:47 (UTC+05:00)