

≡ On this page > 5. Setup S3 in Coolify



Coolify offers automated backups of your instance to an AWS S3 bucket, giving you a hands-off, reliable way to safeguard your configuration and data.

## Why use AWS S3 with Coolify?

1. **Enterprise-grade durability & availability** – S3 is designed for 99.999999999% durability and automatic replication across multiple facilities, so your backups are always safe and accessible.
2. **Cost-effective, pay as you go pricing** – Only pay for the storage and requests you actually use, with built-in lifecycle rules (e.g., transition to Glacier) to optimize long-term costs.
3. **Seamless integration** – Coolify's backup scheduler hooks directly into S3's API, eliminating the need for custom scripts or third-party tools and ensuring backups run on a schedule.



1. **Strict data residency or on-prem requirements** – If your regulations mandate keeping backups entirely within a private data center, S3's public cloud model may not comply.
2. **No external network access** – In environments where outbound internet is blocked, Coolify cannot push snapshots to an S3 endpoint.

#### Example Data

The following data is used as an example in this guide. Please replace it with your actual data when following the steps:

- **S3 Bucket Name:** envix-coolify-backups-s3
- **IAM Policy Name:** EnvixCoolifyBackupS3Access
- **IAM Username:** EnvixCoolifyBackupS3User
- **Endpoint:** <https://s3.ap-northeast-2.amazonaws.com>

## 1. Create a S3 Bucket

To create your S3 Bucket, follow these steps:

Visit <https://console.aws.amazon.com/s3> and Click on Create Bucket button



AWS Search [Option+S] Asia Pacific (Seoul) ShadowArcanist @ Airoflare

# Amazon S3

Storage Store and retrieve any amount of data from anywhere

Amazon S3 is an object storage service that offers industry-leading scalability, data availability, security, and performance.

**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**

**Pricing**

With S3, there are no minimum fees. You only pay for what you use. Prices are based on the location of your S3 bucket.

Estimate your monthly bill using the [AWS Simple Monthly Calculator](#)

[View pricing details](#)

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

You'll be asked to choose a name, object ownership, and so on.

Create S3 bucket | S3 | ap-northeast-2 | Envix Docs | Storage | Coolify

https://ap-northeast-2.console.aws.amazon.com/s3/bucket/create?region=ap-northeast-2

Local Instances Cloud Instances Github

Amazon S3 > Buckets > Create bucket

### Create bucket Info

Buckets are containers for data stored in S3.

**General configuration**

**AWS Region**: Asia Pacific (Seoul) ap-northeast-2

**Bucket name**: envix-coolify-backups-s3

**ShadowArcanist ✓ INSTRUCTOR**: Make sure to write this down somewhere, we will need it later

Bucket names must be 3 to 63 characters and unique within the global namespace. Bucket names must also begin and end with a letter or number. Valid characters are a-z, 0-9, periods (.), and hyphens (-). [Learn More](#)

**Copy settings from existing bucket - optional**: Only the bucket settings in the following configuration are copied.

**Choose bucket**

Format: s3://bucket/prefix

**Object Ownership Info**

Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.

**ACLs disabled (recommended)**: All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.

**ACLs enabled**: Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.

**Object Ownership**: Bucket owner enforced



[Create S3 bucket | S3 | ap-norti](#) [\[Envix Docs\] Storage | Coolify](#)

https://ap-northeast-2.console.aws.amazon.com/s3/bucket/create?region=ap-northeast-2

Local Instances Cloud Instances Github

aws Search [Option+S]

Amazon S3 > Buckets > Create bucket

**Block Public Access settings for this bucket**

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to this bucket and its objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to this bucket or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

**Block all public access**

Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

- Block public access to buckets and objects granted through new access control lists (ACLs)**  
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.
- Block public access to buckets and objects granted through any access control lists (ACLs)**  
S3 will ignore all ACLs that grant public access to buckets and objects.
- Block public access to buckets and objects granted through new public bucket or access point policies**  
S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.
- Block public and cross-account access to buckets and objects through any public bucket or access point policies**  
S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

**Bucket Versioning**

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. [Learn more](#)

**Bucket Versioning**

Disable  
 Enable

**ShadowArcanist ✓INSTRUCTOR**  
 Leave everything to the default values, only change things if you know what you are doing

**Tags - optional (0)**

[Create S3 bucket | S3 | ap-norti](#) [\[Envix Docs\] Storage | Coolify](#)

https://ap-northeast-2.console.aws.amazon.com/s3/bucket/create?region=ap-northeast-2

Local Instances Cloud Instances Github

aws Search [Option+S]

Amazon S3 > Buckets > Create bucket

**Tags - optional (0)**

You can use bucket tags to track storage costs and organize buckets. [Learn more](#)

No tags associated with this bucket.

[Add tag](#)

**ShadowArcanist ✓INSTRUCTOR**  
 Leave everything to the default values, only change things if you know what you are doing

**Default encryption** [Info](#)

Server-side encryption is automatically applied to new objects stored in this bucket.

**Encryption type** [Info](#)

Server-side encryption with Amazon S3 managed keys (SSE-S3)  
 Server-side encryption with AWS Key Management Service keys (SSE-KMS)  
 Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)  
 Secure your objects with two separate layers of encryption. For details on pricing, see DSSE-KMS pricing on the Storage tab of the [Amazon S3 pricing page](#).

**Bucket Key**  
 Using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. S3 Bucket Keys aren't supported for DSSE-KMS. [Learn more](#)

Disable  
 Enable

**Advanced settings**

**Object Lock**  
 Store objects using a write-once-read-many (WORM) model to help you prevent objects from being deleted or overwritten for a fixed amount of time or indefinitely. Object Lock works only in versioned buckets. [Learn more](#)

Disable

The screenshot shows the 'Create bucket' wizard on the AWS S3 console. The 'Bucket Key' section is highlighted, showing options for SSE-KMS encryption. A callout box from 'ShadowArcanist' says: 'Leave everything to the default values, only change things if you know what you are doing'. The 'Advanced settings' section includes 'Object Lock' and 'Bucket Policy'. A note at the bottom says: 'Object Lock works only in versioned buckets. Enabling Object Lock automatically enables Versioning.' Another note says: 'After creating the bucket, you can upload files and folders to the bucket, and configure additional bucket settings.' A large orange 'Create bucket' button is at the bottom right.

Click on Create Bucket button

Once the bucket is created you will be redirected to this page:

The screenshot shows the AWS S3 'Buckets' page. A green banner at the top says: 'Successfully created bucket "envix-coolify-backups-s3"'. Below it, an 'Account snapshot' section provides storage usage information. The 'General purpose buckets' tab is selected, showing a table of buckets. One row for 'envix-coolify-backups-s3' is selected, showing details like Region (Asia Pacific (Seoul) ap-northeast-2), IAM Access Analyzer (View analyzer for ap-northeast-2), and Creation date (April 18, 2025, 14:15:13). A callout box from 'ShadowArcanist' says: 'Once the Bucket is created, you will see this page with the green banner message. Good Job!'



To create your IAM Policy, follow these steps:

Visit <https://console.aws.amazon.com/iam/home#/policies> and Click on Create Policy button

The screenshot shows the AWS IAM Policies page with 1344 policies listed. The left sidebar includes sections for Identity and Access Management (IAM), Access management, and Access reports. The main area displays a table of policies with columns for Policy name, Type, Used as, and Description. The 'Create policy' button is highlighted with a yellow arrow.

Policy name	Type	Used as	Description
<a href="#">AccessAnalyzerServiceRolePolicy</a>	AWS managed	None	Allow Access Analyzer to analyze resources
<a href="#">AdministratorAccess</a>	AWS managed - job function	Permissions policy (2)	Provides full access to AWS services and resources
<a href="#">AdministratorAccess-Account-Wide</a>	AWS managed	None	Grants account administrative permissions
<a href="#">AIOpsAssistantPolicy</a>	AWS managed	None	Provides ReadOnly permissions required by AI Ops
<a href="#">AIOpsConsoleAdminPolicy</a>	AWS managed	None	Grants full access to Amazon AI Operations
<a href="#">AIOpsOperatorAccess</a>	AWS managed	None	Grants access to the Amazon AI Operations
<a href="#">AIOpsReadOnlyAccess</a>	AWS managed	None	Grants ReadOnly permissions to the AI Operations
<a href="#">AlexaForBusinessDeviceSetupAccess</a>	AWS managed	None	Provide device setup access to Alexa For Business
<a href="#">AlexaForBusinessFullAccess</a>	AWS managed	None	Grants full access to Alexa For Business
<a href="#">AlexaForBusinessGatewayAccess</a>	AWS managed	None	Provide gateway execution access to Alexa For Business



**Specify permissions** Info

Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.

**Policy editor**

Visual **JSON** Actions ▾

```

1 {  

2   "Version": "2012-10-17",  

3   "Statement": [  

4     {  

5       "Effect": "Allow",  

6       "Action": [  

7         "s3:ListBucket",  

8         "s3:GetObject",  

9         "s3:DeleteObject",  

10        "s3:GetObjectAcl",  

11        "s3:PutObjectAcl",  

12        "s3:PutObject"  

13      ],  

14      "Resource": [  

15        "arn:aws:s3:::envix-coolify-backups-s3",  

16        "arn:aws:s3:::envix-coolify-backups-s3/*"  

17      ]  

18    }  

19  ]  

20 }

```

**Edit statement**

**Select a statement**

Select an existing statement in the policy or add a new statement.

+ Add new statement

- Click on **JSON** option and copy paste the following code on the policy editor

### Policy Permissions

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:ListBucket",
        "s3:GetObject",
        "s3:DeleteObject",
        "s3:GetObjectAcl",
        "s3:PutObjectAcl",
        "s3:PutObject"
      ],
      "Resource": [
        // replace envix-coolify-backups-s3 with your bucket name on below two lines
        "arn:aws:s3:::envix-coolify-backups-s3",
        "arn:aws:s3:::envix-coolify-backups-s3/*"
      ]
    }
  ]
}
```

Scroll down till the bottom of the page and click on the Continue button.



Create policy | IAM | Global    [Envix Docs] Storages | Coolify

Local Instances Cloud Instances Github

AWS Search [Option+S]

IAM > Policies > Create policy

Step 1  
Specify permissions  
Step 2  
Review and create

### Review and create Info

Review the permissions, specify details, and tags.

**Policy details**

**Policy name**  
Enter a meaningful name to identify this policy  
**EnvixCoolifyBackupS3Access**

Maximum 128 characters. Use alphanumeric and '+=\_,@\_-.' characters.

**Description - optional**  
Add a short explanation for this policy.

Maximum 1,000 characters. Use alphanumeric and '+=\_,@\_-.' characters.

**Permissions defined in this policy Info** Edit

Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it.

**Allow (1 of 439 services)** Show remaining 438 services

Service	▲   Access level	▼   Resource	Request condition
Limited list of permissions			

Once you have entered the name, scroll down till the bottom of the page and click on the **Continue** button.

Once the Policy is created you will be redirected to this page:



aws | [Option+S] | Global | ShadowArcanist @ Airoflare

IAM > Policies

**Identity and Access Management (IAM)**

Search IAM

**Policies (1345) Info**  
A policy is an object in AWS that defines permissions.

Filter by Type: Envix | All types | 1 match

Policy name	Type	Used as	Description
EnvixCoolifyBackupS3Access	Customer managed	None	-

**ShadowArcanist ✓ INSTRUCTOR**  
Once the Policy is created, you will see this page with the green banner message. Good Job!

**Access management**

- User groups
- Users
- Roles
- Policies**
- Identity providers
- Account settings
- Root access management New

**Access reports**

- Access Analyzer
- External access
- Unused access
- Analyzer settings
- Credential report
- Organization activity

**Tip**

You won't see the policy you just created, you have to search for its name on the search box.

### 3. Create a IAM User

To create your IAM User, follow these steps:

Visit <https://console.aws.amazon.com/iam/home#/users> and Click on Create user button



Screenshot of the AWS IAM console showing the 'Users' page. A callout points to the 'Create user' button.

**Identity and Access Management (IAM)**

- Dashboard
- Access management**
  - User groups
  - Users** (selected)
  - Roles
  - Policies
  - Identity providers
  - Account settings
  - Root access management [New](#)
- Access reports**
  - Access Analyzer
  - External access
  - Unused access
  - Analyzer settings
  - Credential report
  - Organization activity
  - Service control policies

**Users (1) Info**

An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

User name	Path	Group	Last activity	MFA	Password age	Console last sign-in
Stacy	/	1	3 hours ago	-	19 hours	April 18, 2025, 11:13 (...)

[Edit](#) [Delete](#) [Create user](#)

You'll be asked to choose a name for the user:

Screenshot of the 'Create user' wizard Step 1: Specify user details.

**Specify user details**

**User details**

User name: **ShadowArcanist** ✓ INSTRUCTOR

This username can be anything but make it easy to understand its purpose by its name - helpful to identify the user account if you have lot of users.

The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ \_ - (hyphen)

Provide user access to the AWS Management Console - optional

If you're providing console access to a person, it's a **best practice** [to manage their access in IAM Identity Center](#).

ⓘ If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keyspaces, you can generate them after you create this IAM user. [Learn more](#)

[Cancel](#) [Next](#)

- Click on **Next** button after you have entered a name for the user.



Screenshot of the AWS IAM 'Create user' wizard - Step 2: Set permissions.

**Set 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, and inline policies 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.

**Permissions policy search**

Choose one or more policies to attach to this user. You have to search the name of your policy to easily find it.

Search bar: Envix

Policy name	Type	Attached entities
EnvixCoolifyBackupS3Access	Customer managed	0

**Set permissions boundary - optional**

**Next**

1. Select Attach policies directly option
2. Select the policy we created on the previous step
3. Click on Next button

Screenshot of the AWS IAM 'Create user' wizard - Step 3: Review and create.

**Review and create**

Review your choices. After you create the user, you can view and download the autogenerated password, if enabled.

**User details**

User name: EnvixCoolifyBackupS3User	Console password type: None	Require password reset: No
-------------------------------------	-----------------------------	----------------------------

**Permissions summary**

Name	Type	Used as
EnvixCoolifyBackupS3Access	Customer managed	Permissions policy

**Tags - optional**

Tags are key-value pairs you can add to AWS resources to help identify, organize, or search for resources. Choose any tags you want to associate with this user.

No tags associated with the resource.

**Create user**



Once the Policy is created you will be redirected to this page:

The screenshot shows the AWS IAM 'Users' page. On the left, there's a sidebar with 'Identity and Access Management (IAM)' and sections for 'Access management' (User groups, Users, Roles, Policies, Identity providers, Account settings, Root access management) and 'Access reports' (Access Analyzer, External access, Unused access, Analyzer settings, Credential report, Organization activity, Service control policies). The main area displays 'Users (2)'. A green callout box highlights the 'EnvixCoolifyBackupS3User' row, which includes the username, MFA status (None), Password age (3 hours ago), and Console last sign-in (April 18, 2025, 11:13...).

User	MFA	Password age	Console last sign-in
EnvixCoolifyBackupS3User	-	3 hours ago	April 18, 2025, 11:13...
ShadowArcanist	-	-	-
Stacy	1	19 hours	April 18, 2025, 11:13...

- Click on the username to create an access key.

## 4. Create an Access Key

After you have clicked on the username on previous step, you will be redirect to this page:



Envix

Screenshot of the AWS IAM User Details page for 'EnvixCoolifyBackupS3User'.

**Summary**

- ARN:** arn:aws:iam::996968708342:user/EnvixCoolifyBackupS3User
- Console access:** Disabled
- Created:** April 18, 2025, 14:28
- Last console sign-in:** -

**Access key 1** [Create access key](#)

**Permissions** [Groups](#) [Tags](#) [Security credentials](#) [Last Accessed](#)

**Permissions policies (1)**

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

Policy name	Type	Attached via
<a href="#">EnvixCoolifyBackupS3Access</a>	Customer managed	Directly

**Permissions boundary (not set)**

- Click on **Create access key** option to setup a new access key.

Screenshot of the 'Create access key' wizard Step 1: Access key best practices & alternatives.

**Step 1**

**Access key best practices & alternatives**

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

**Use case**

- 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 authenticate workloads running in your data center or other infrastructure outside of AWS that needs to access your AWS resources.
- Other**  
Your use case is not listed here.

- Choose the **Other** option and click on **Continue** button



Envix

Screenshot of the AWS IAM 'Create access key' wizard Step 2 - optional: Set description tag.

**Step 1**  
 Access key best practices & alternatives  
 Step 2 - optional  
 Set description tag  
 Step 3  
 Retrieve access keys

**Set description tag - optional** Info  
 The description for this access key will be attached to this user as a tag and shown alongside the access key.

**Description tag value**  
 Describe the purpose of this access key and where it will be used. A good description will help you rotate this access key confidently later.  
 Maximum 256 characters. Allowed characters are letters, numbers, spaces representable in UTF-8, and: \_ . : / = + - @

 Save

**Create access key**

- Click on Create access key button.

Screenshot of the AWS IAM 'Create access key' wizard Step 3: Retrieve access keys.

**Access key created**  
 This is the only time that the secret access key can be viewed or downloaded. You cannot recover it later. However, you can create a new access key any time.

**Retrieve access key**  
 **ShadowArcanist ✓ INSTRUCTOR**  
 Make sure to write these down somewhere, we will need it later

**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: AKIAHNNEWD3CAUIL205  
 Secret access key: AScM1amfrwnEG+Ht3OFlUzCPnP19uap+yt4GUNr/

**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** **Done**

- Save the Access Key and Secret Access Key somewhere safe and click on Done button



Envix

somewhere safe.

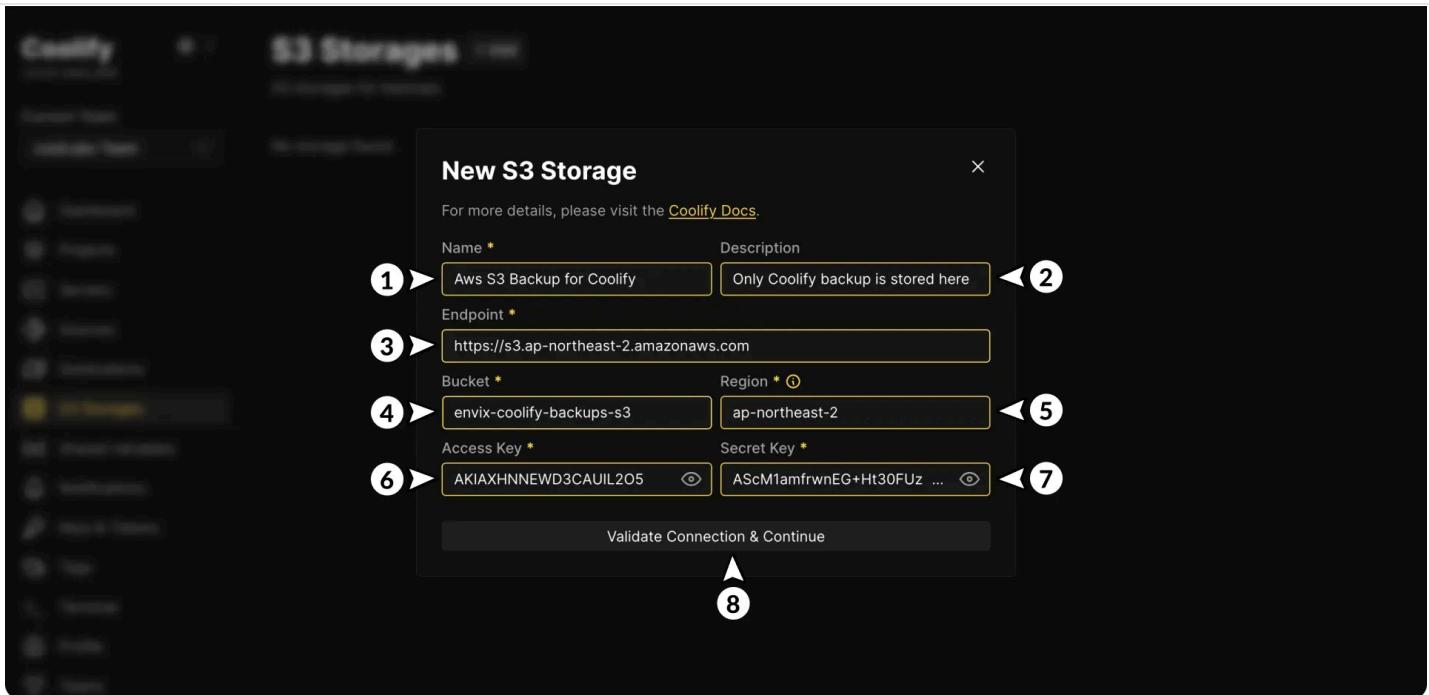
## 5. Setup S3 in Coolify

To create your setup S3 in Coolify, follow these steps:

In your Coolify dashboard:

A screenshot of the Coolify v4.0.0-beta.408 dashboard. The left sidebar has a dark theme with white icons and text. The 'S3 Storages' option is highlighted with a yellow box and a circled '1'. A second circled '2' points to the '+ Add' button located at the top right of the main 'S3 Storages' section. The main area displays the heading 'S3 Storages' and the subtext 'S3 storages for backups.' followed by 'No storage found.' The browser address bar shows the URL https://coolify.shadowarcanist.pvt/storages.

1. Go to the **Storage** section in the sidebar.
2. Click **Add** button



1. Give a name for the S3 storage (this can be any name)
2. Give a short description for the storage (optional)
3. Enter the endpoint without your bucket name: `https://s3.YOUR_REGION_NAME.amazonaws.com`
4. Enter the name of the S3 bucket you created.
5. Enter your S3 bucket's region
6. Enter your Access Key
7. Enter your Secret Access Key
8. Click on **Validate Connection & Continue** button

Once the Bucket is validated you will be redirected to this page:



**Coolify** v4.0.0-beta.408

Storage Details Save Validate Connection Delete

Aws S3 Backup for Coolify

Usable

Name	Description
Aws S3 Backup for Coolify	Only Coolify backup is stored here

Endpoint \* Bucket \* Region \*

https://s3.ap-northeast-2.amazonaws.com envix-coolify-backups-s3 ap-northeast-2

Access Key \* Secret Key \*

..... (eye) ..... (eye)

ShadowArcanist ✓ INSTRUCTOR

Once the Storage is connected, you will see this page with the green banner message. Good Job!

Dashboard Projects Servers Sources Destinations S3 Storages Shared Variables Notifications Keys & Tokens Tags Terminal Profile Teams

Then go to **settings** page and click on **Backup**

Create access key | IAM | Global [Envix Docs] Settings | Coolify +

https://coolify.shadowarcanist.pvt/settings/backup

Local Instances Cloud Instances Github

v4.0.0-beta.408

Current Team coolLabs Team

Dashboard Projects Servers Sources Destinations S3 Storages Shared Variables Notifications Keys & Tokens Tags Terminal Profile Teams

**Settings**

Instance wide settings for Coolify.

Configuration Backup Transactional Email OAuth

ShadowArcanist ✓ INSTRUCTOR

If you are not seeing a lot of options in this page, then you probably will see a button called "Enable Backup", click on it.

**Backup** Save

Backup configuration for Coolify instance.

UUID	Name	Description
jokksgssogco4w4sk0ogocwo	coolify-db	Coolify database

User coolify Password .....

**Scheduled Backup** Save Backup Now

Backup Enabled  S3 Enabled

**Settings**

Frequency 0 0 \* \* \* Timezone UTC

**Backup Retention Settings**

Settings

**Scheduled Backup**

- 1 Backup Enabled
- 2 S3 Enabled
- 3 Frequency: 0 0 \* \* \*
- 4 Timezone: UTC

Local Backup Retention		
Number of backups to keep	Days to keep backups	Maximum storage (GB)
30	30	70

S3 Storage Retention		
Number of backups to keep	Days to keep backups	Maximum storage (GB)
90	90	40000

1. Enable S3
2. Select your S3 storage
3. Select the frequency of the backup (you can use this [website](#) if you are new to cron)
4. Setup Backup Retentions
5. Click on **Backup Now** button (just to check if everything works)

You can see the backups stored on your S3 from the execution logs:



v4.0.0-beta.408

Setting a value to 0 means unlimited retention.

- The retention rules work independently - whichever limit is reached first will trigger cleanup.

### Local Backup Retention

Number of backups to keep ⓘ	30	Days to keep backups ⓘ	30	Maximum storage (GB) ⓘ	70
-----------------------------	----	------------------------	----	------------------------	----

### S3 Storage Retention

Number of backups to keep ⓘ	90	Days to keep backups ⓘ	90	Maximum storage (GB) ⓘ	40000
-----------------------------	----	------------------------	----	------------------------	-------

### Executions

Cleanup Failed Backups

**Success**

Started: 2025-04-05 03:52:57 UTC  
 Ended: 2025-04-05 03:52:57 UTC  
 Duration: 00m 00s  
 Finished 1 week ago  
 Database: coolify  
 Size: 526839 B / 514.49 kB / 0.502 MB  
 Location: /data/coolify/backups/coolify/coolify-db-hostdocke

Backup Availability:  Local Storage  S3 Storage

**ShadowArcanist ✓ INSTRUCTOR**

If the backup is stored on S3 then you will see this tag here

Download Delete

Now you're done! Your Coolify instance is set up to automatically backup and store them on your Aws S3 bucket safely.

#### Note

If this guide doesn't resolve your issue, please join the Coolify Discord server and seek assistance there.

## Links



[Coolify Support Server](#)



[Author's Website](#)