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.

Envix

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

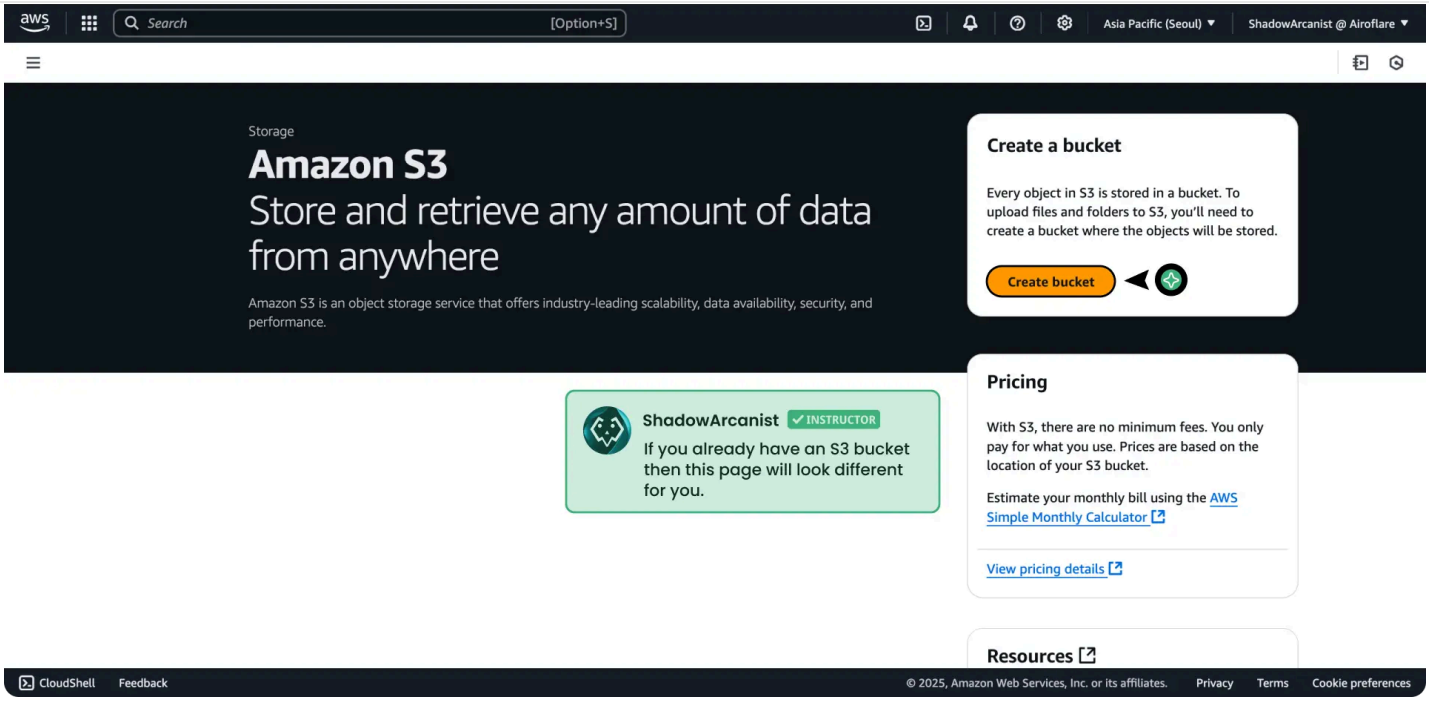
---

1. Create a S3 Bucket

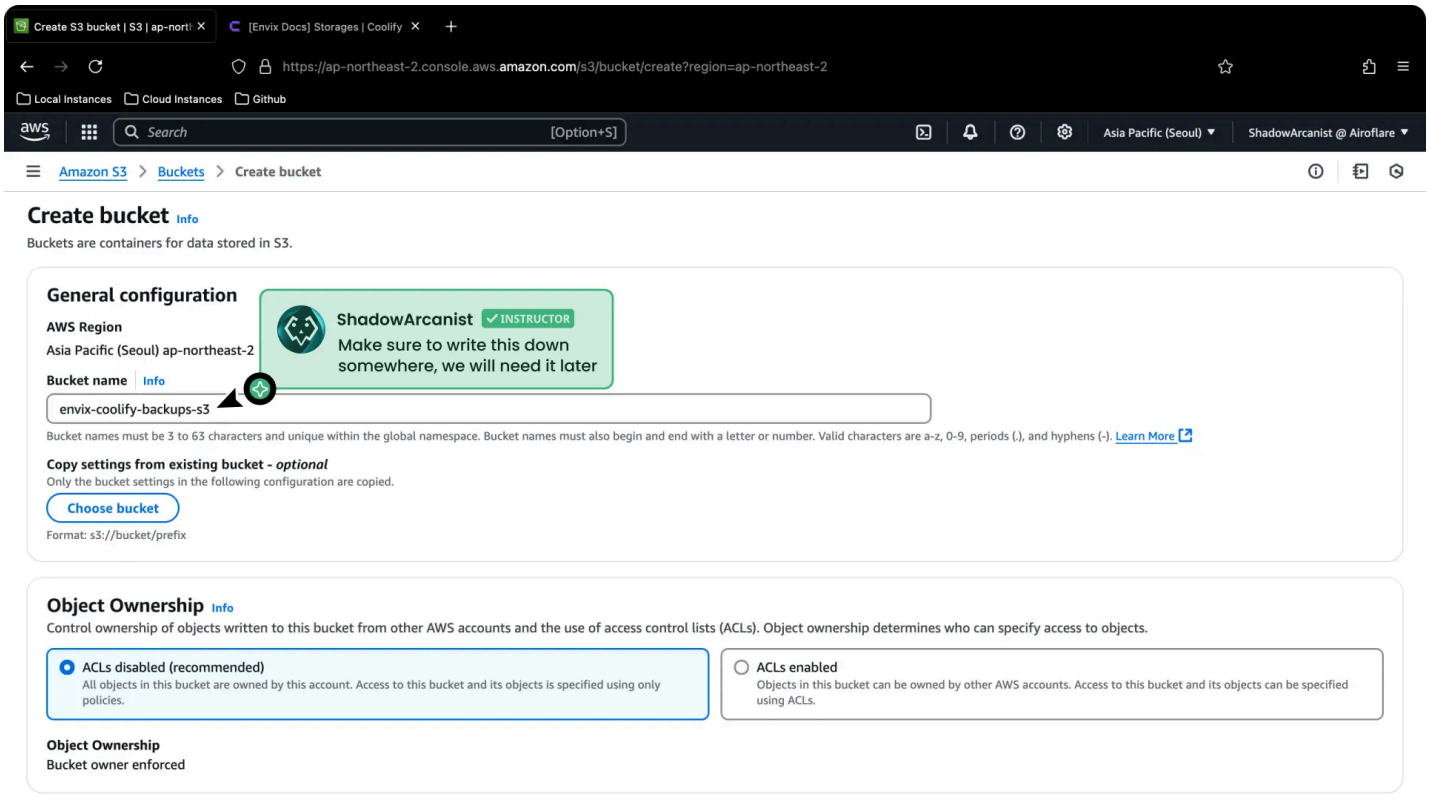
To create your S3 Bucket, follow these steps:

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

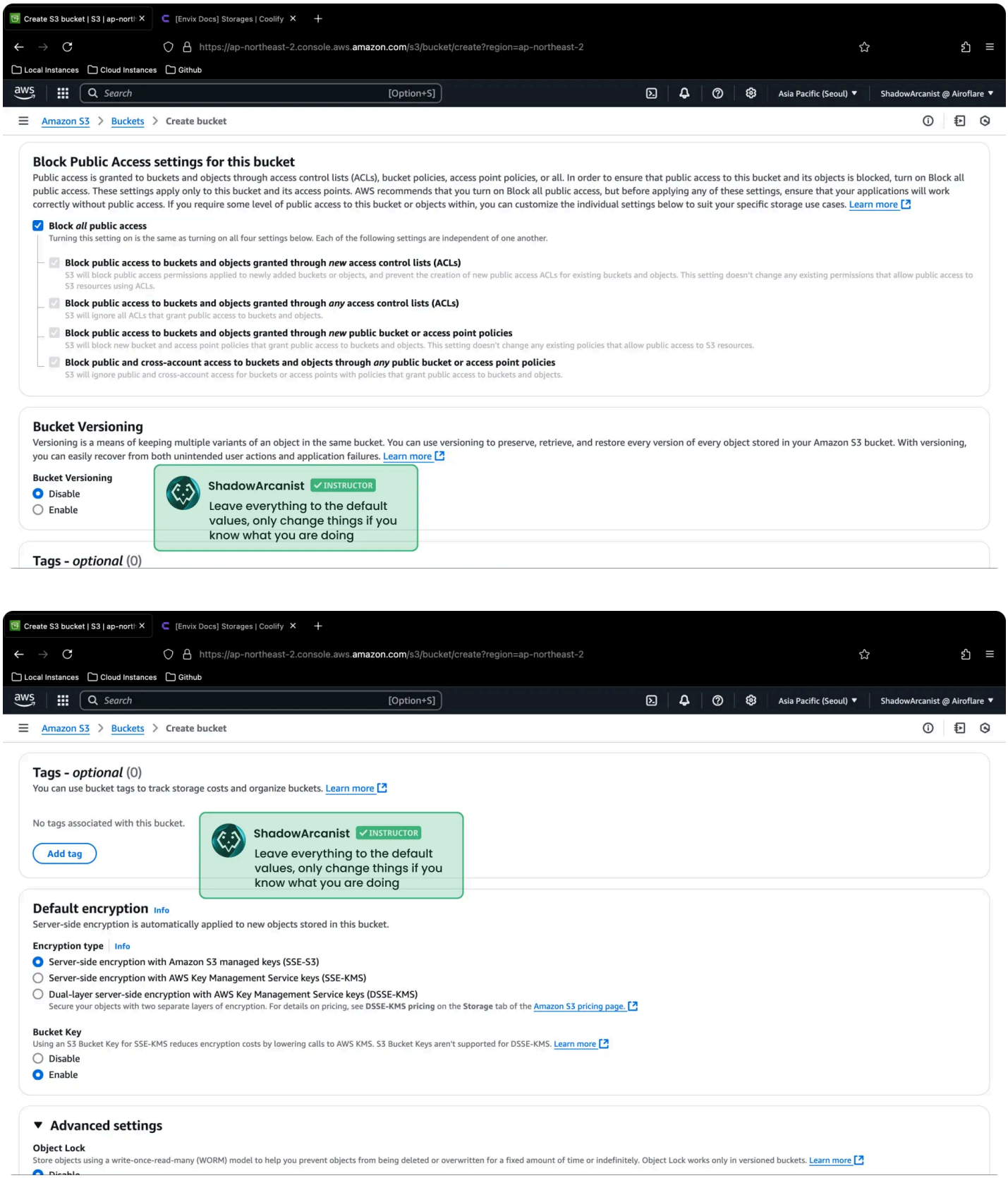
Envix



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

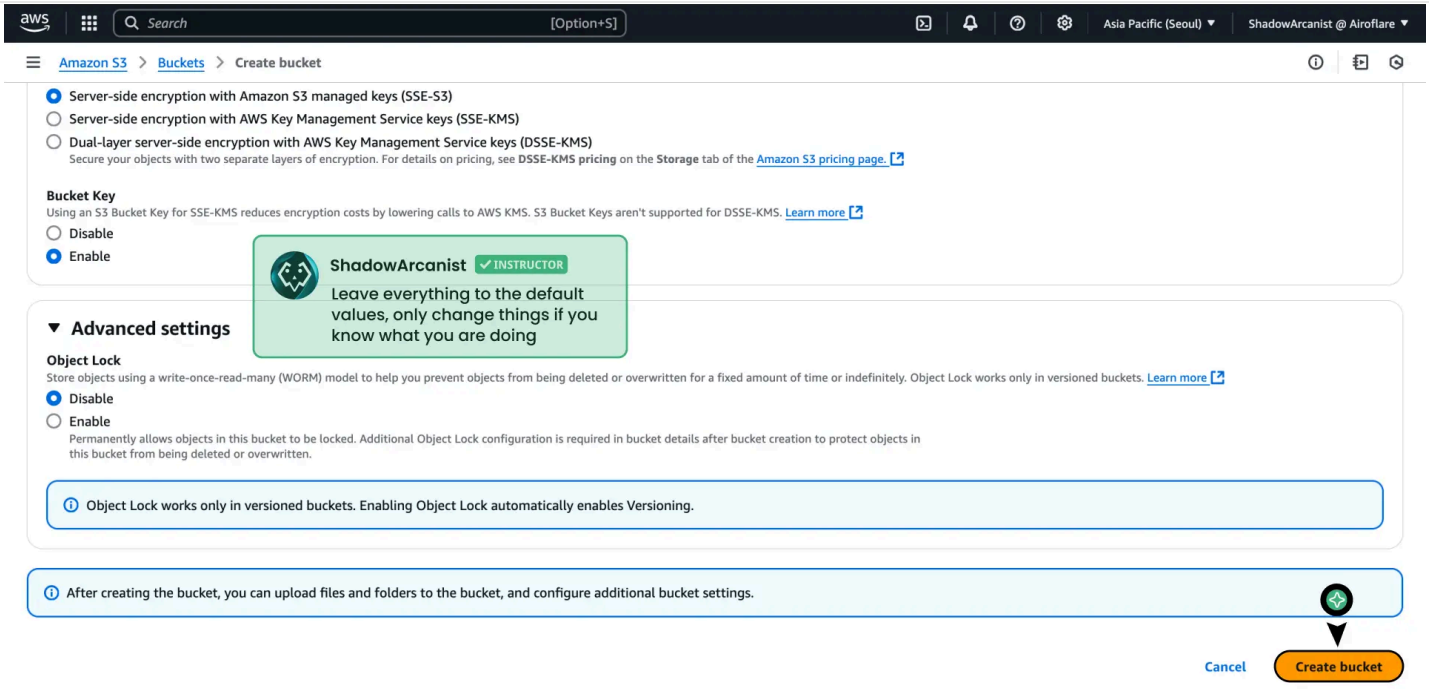


Envix


Create S3 bucket | S3 | ap-north
[Envix Docs] Storages | Coolify
https://ap-northeast-2.console.aws.amazon.com/s3/bucket/create?region=ap-northeast-2
Local Instances
Cloud Instances
Github
Search
[Option+S]
Asia Pacific (Seoul)
ShadowArcanist @ Airoflare
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)

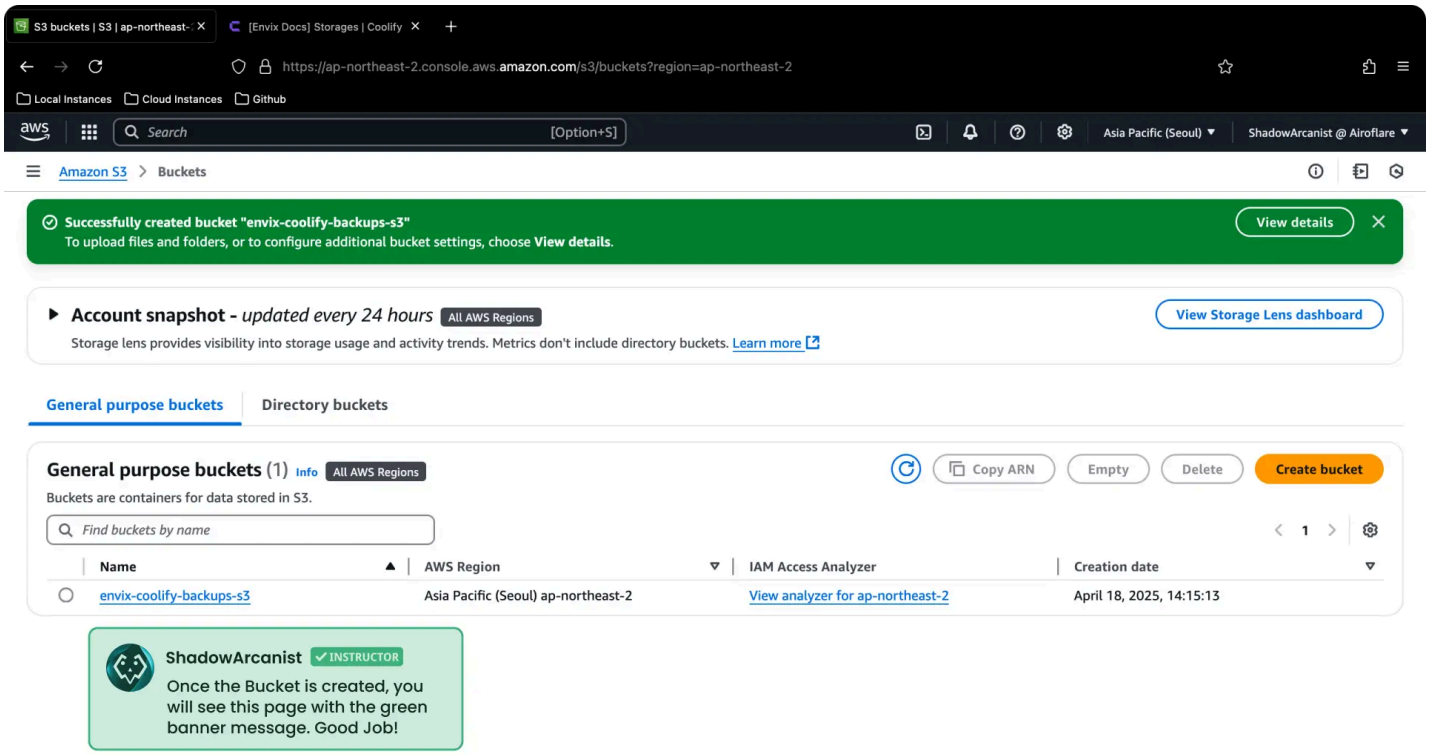
Create S3 bucket | S3 | ap-north
[Envix Docs] Storages | Coolify
https://ap-northeast-2.console.aws.amazon.com/s3/bucket/create?region=ap-northeast-2
Local Instances
Cloud Instances
Github
Search
[Option+S]
Asia Pacific (Seoul)
ShadowArcanist @ Airoflare
Amazon S3 > Buckets > Create bucket
Tags - optional (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

Envix



Click on **Create Bucket** button

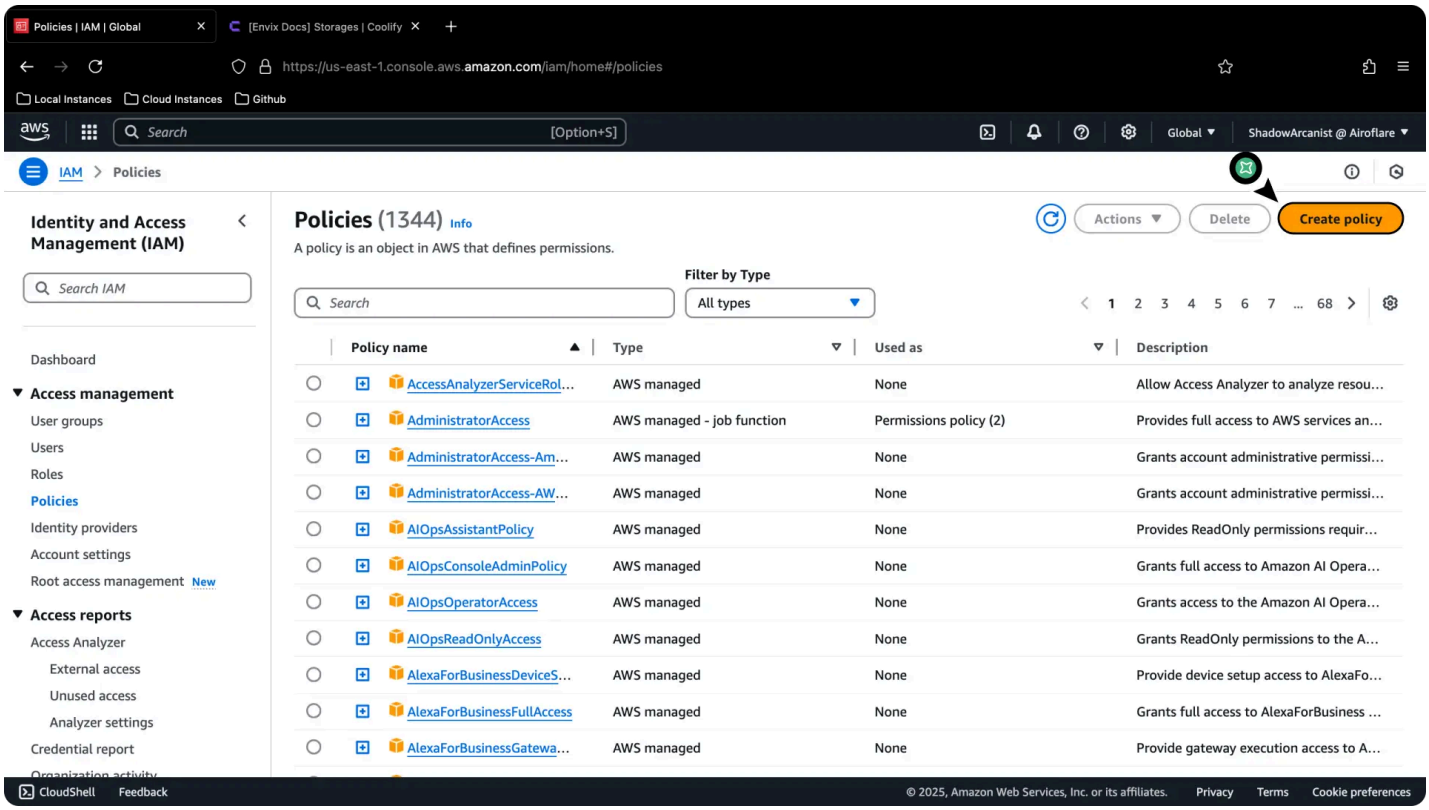
Once the bucket is created you will be redirected to this page:



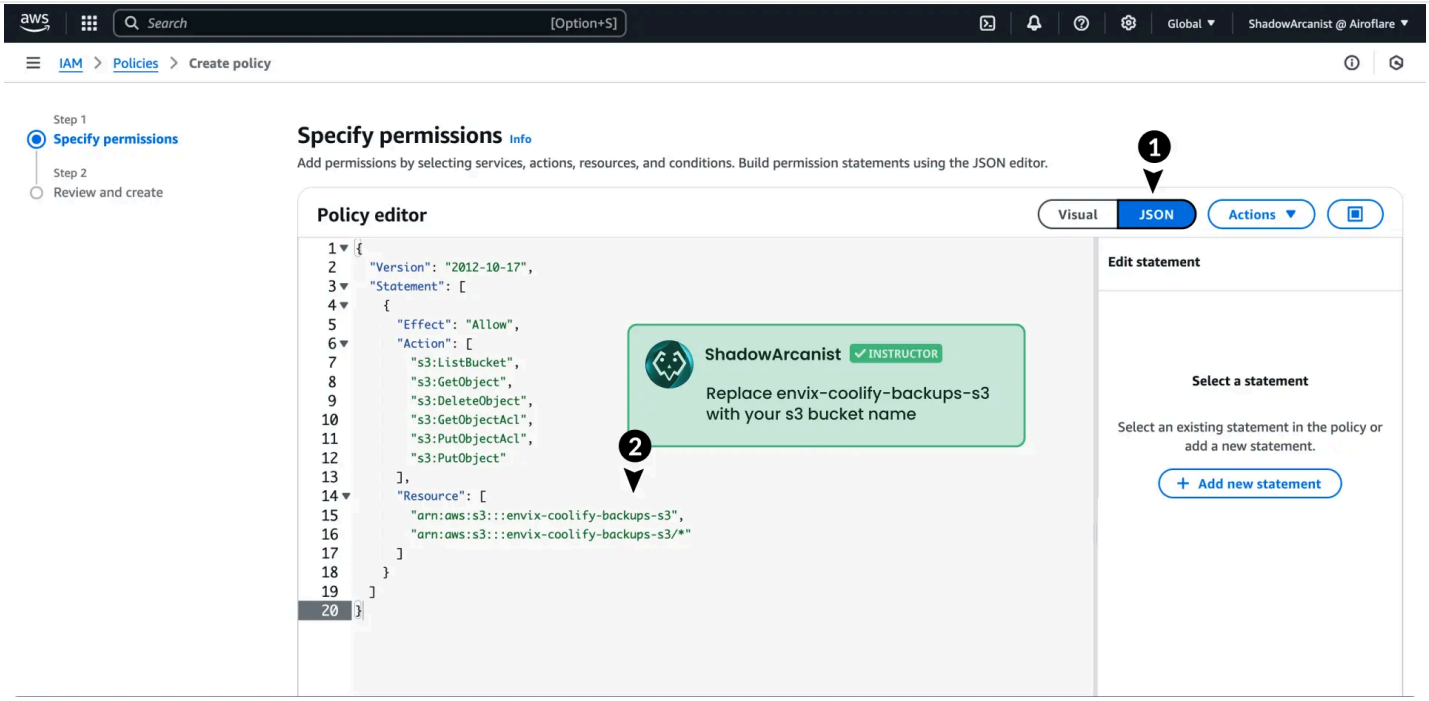
Envix

To create your IAM Policy, follow these steps:

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



Envix



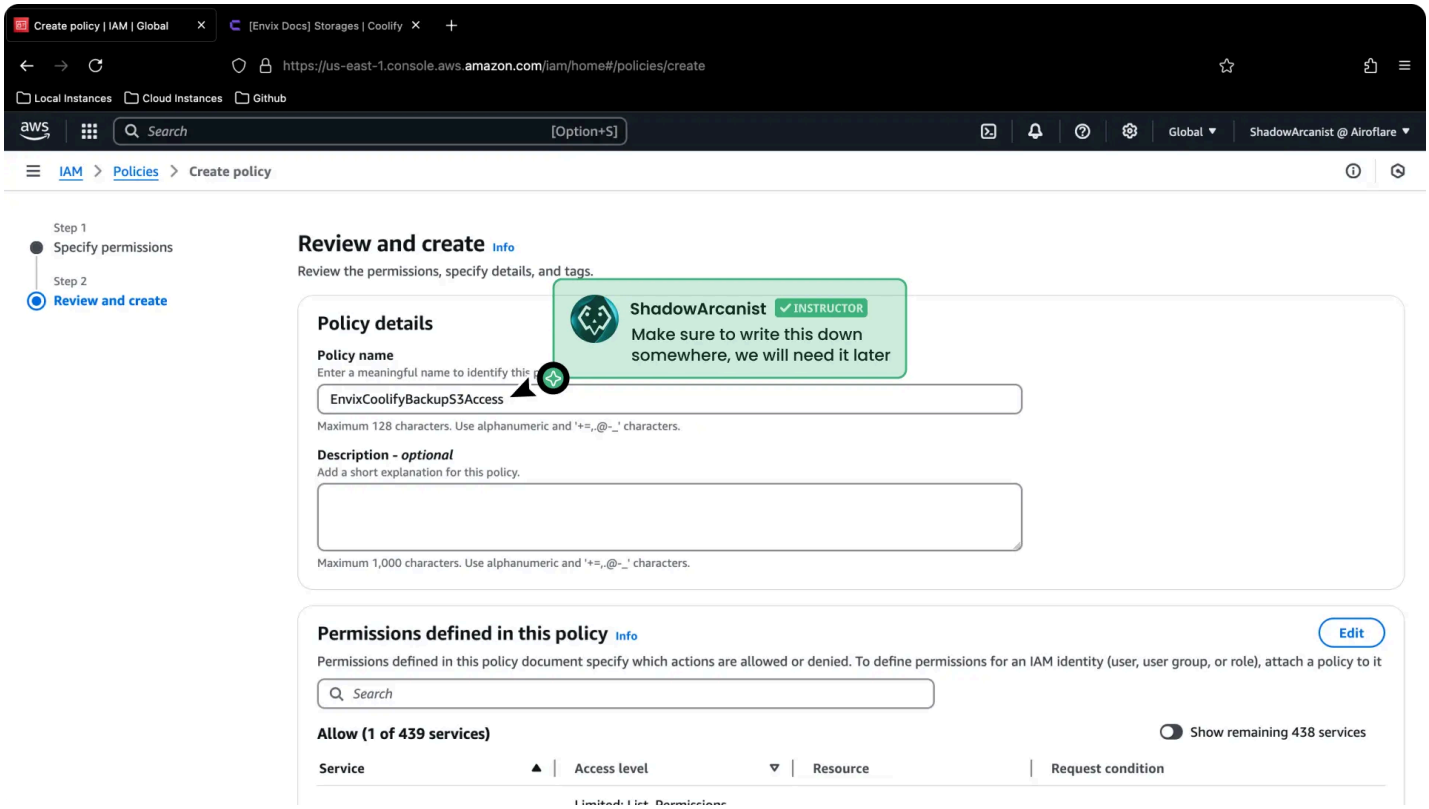
- Click on **JSON** option and copy paste the following code on the policy editor

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.

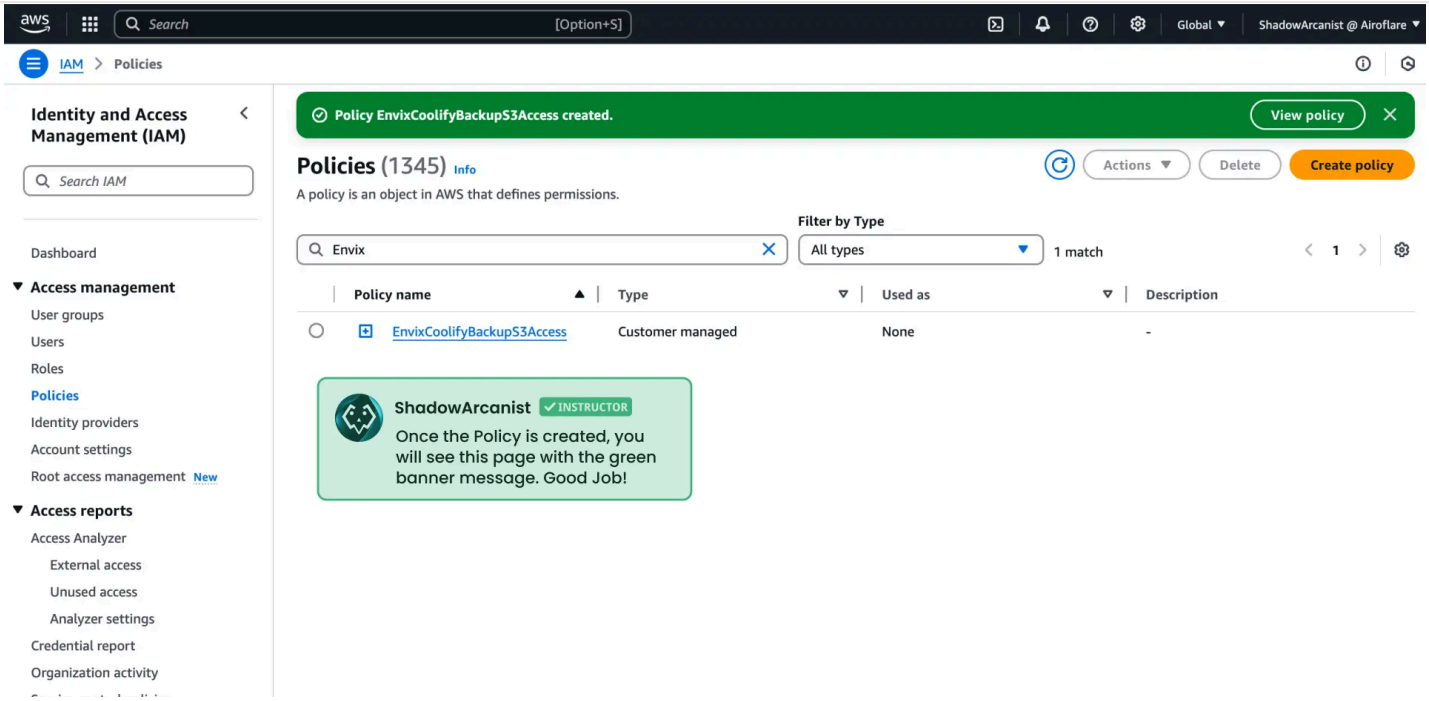
Envix



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:

Envix



Tip

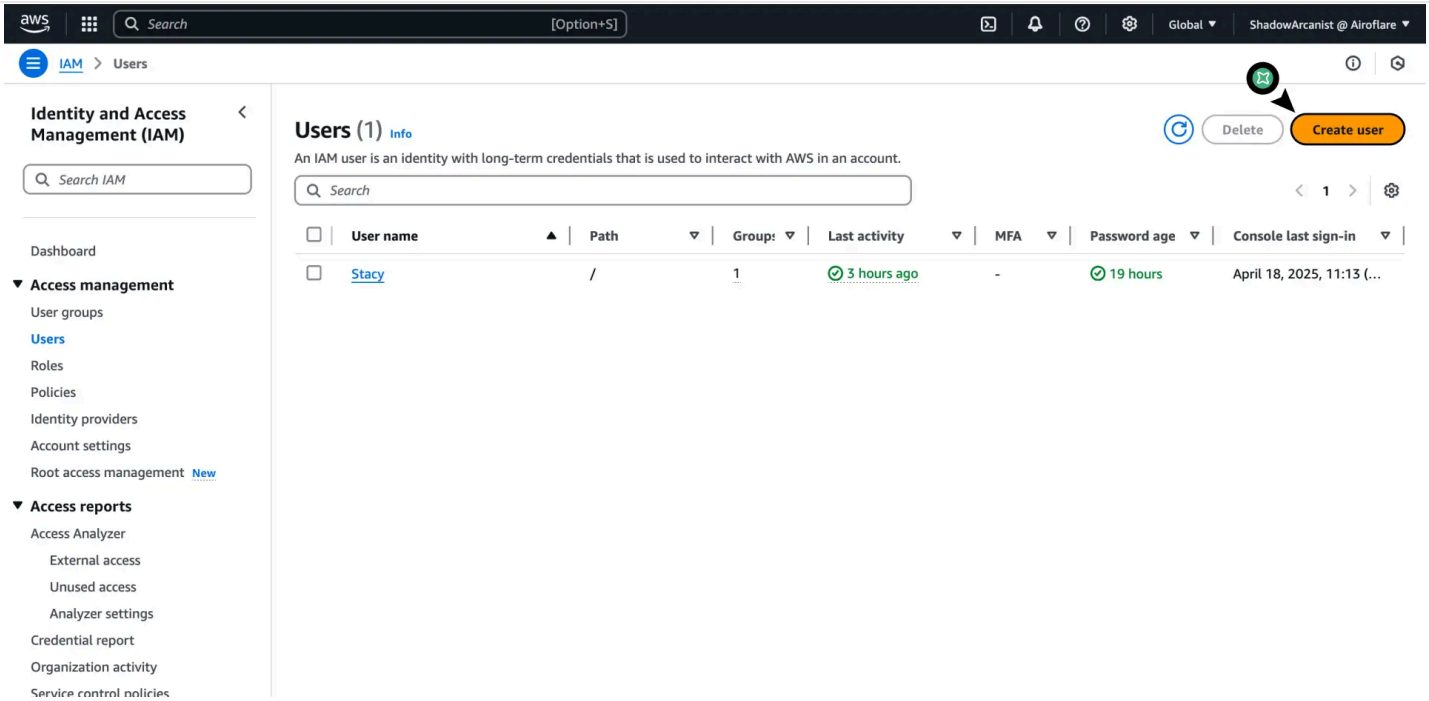
You won't see the policy you just created, you have to search for it's name on the search box.

3. Create a IAM User

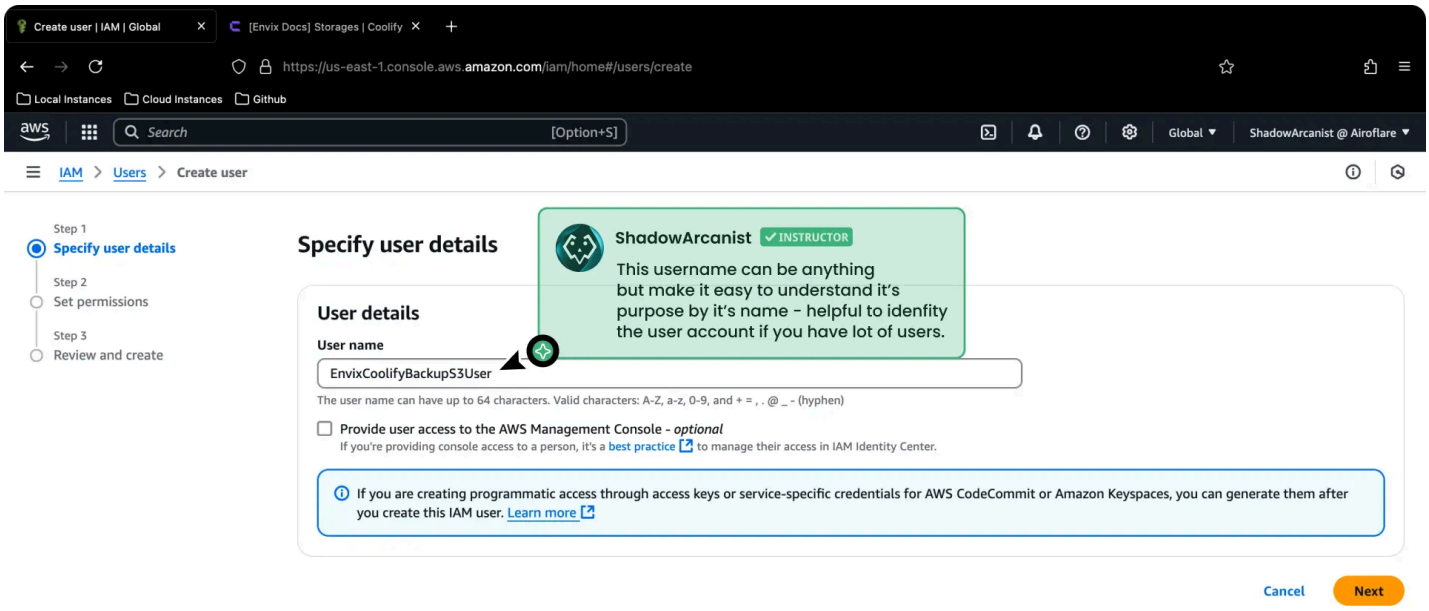
To create your IAM User, follow these steps:

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

Envix

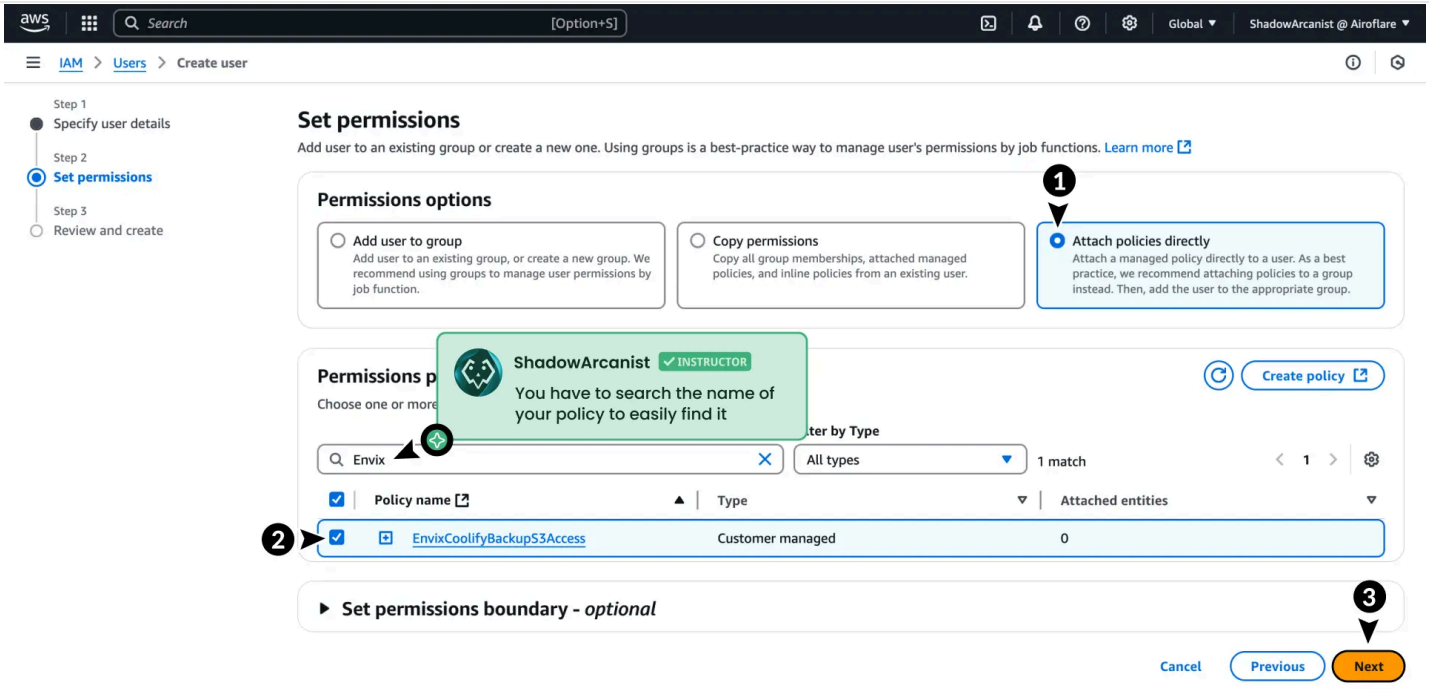


You'll be asked to choose a name for the user:

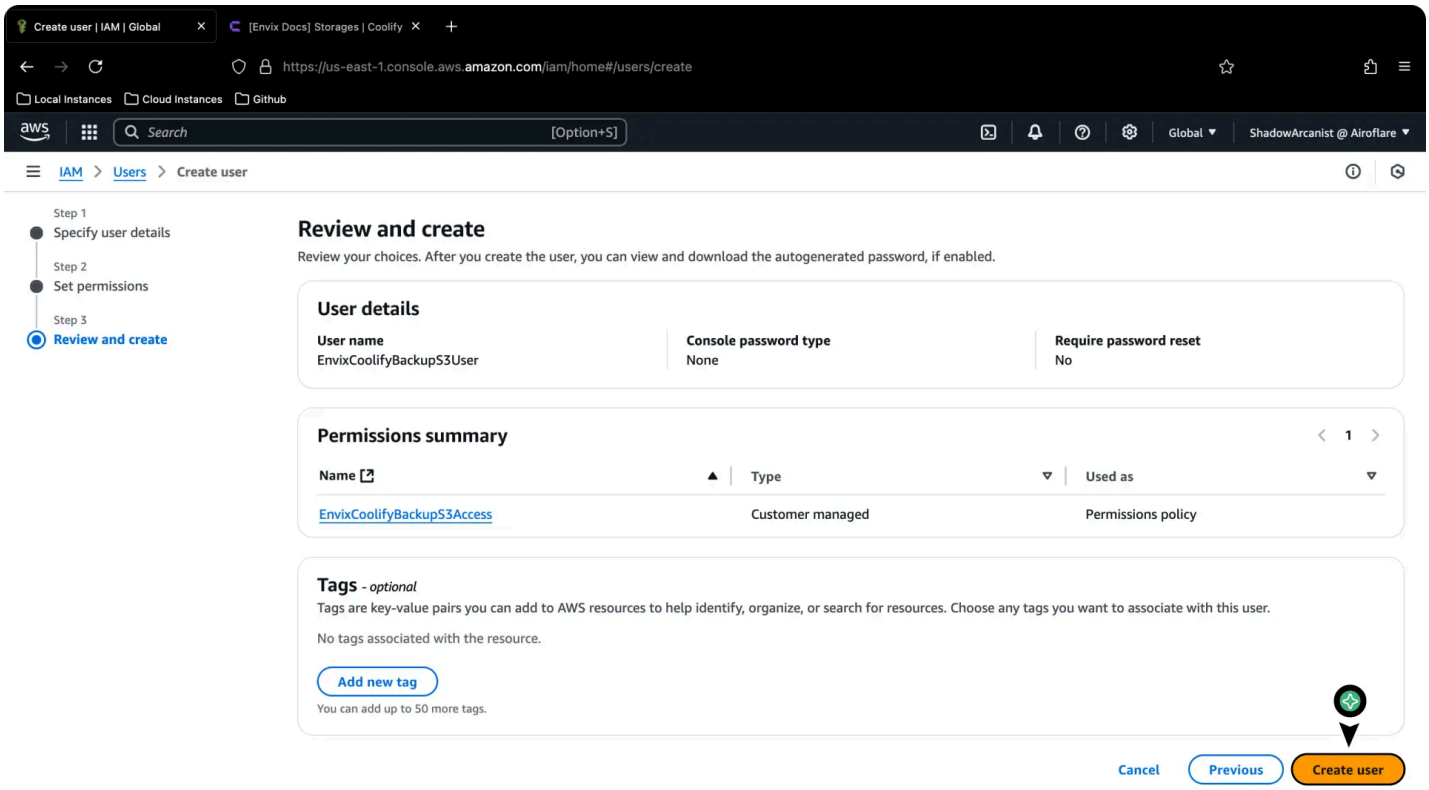


- Click on **Next** button after you have entered a name for the user.

Envix

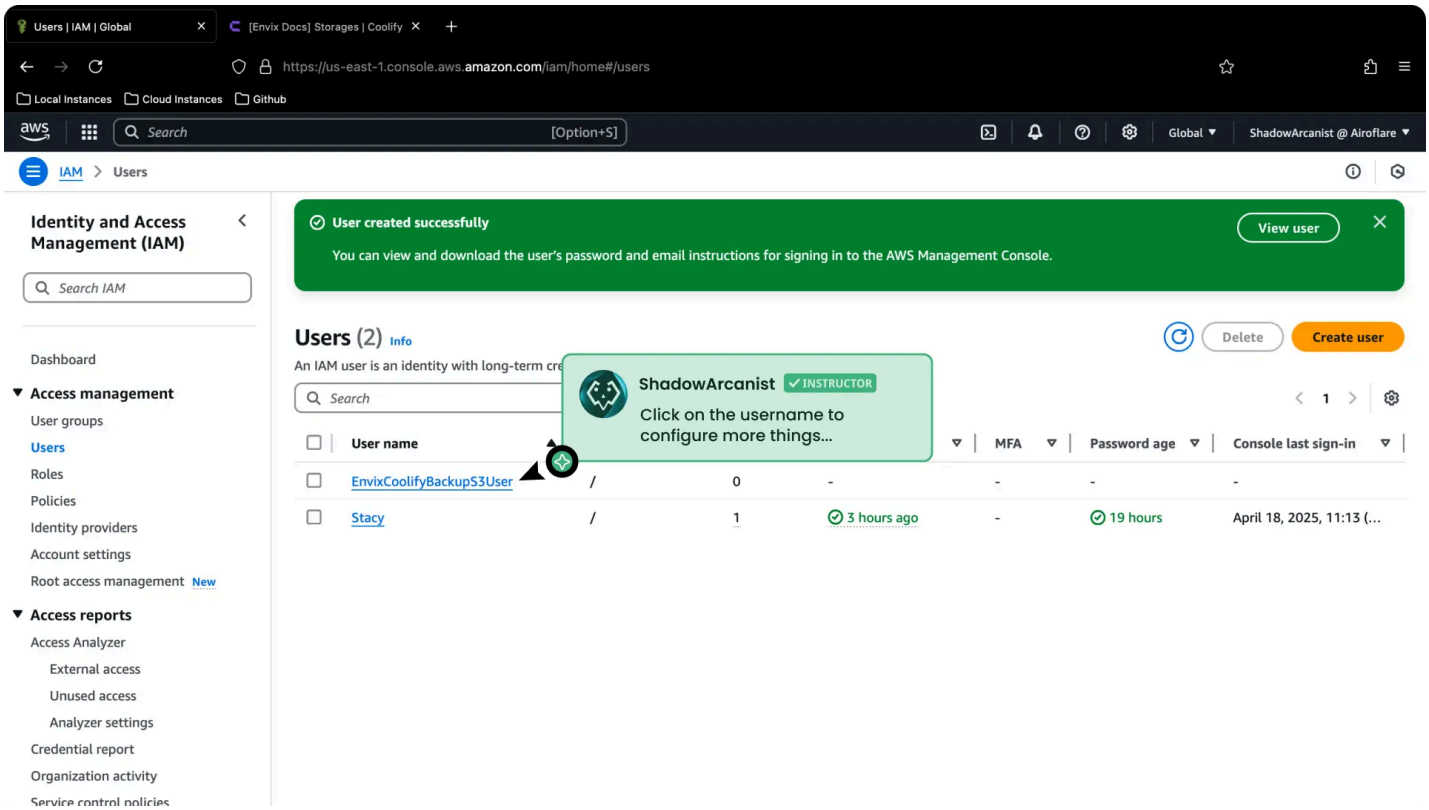


1. Select Attach policies directly option
2. Select the policy we created on the previous step
3. Click on **Next** button



Envix

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

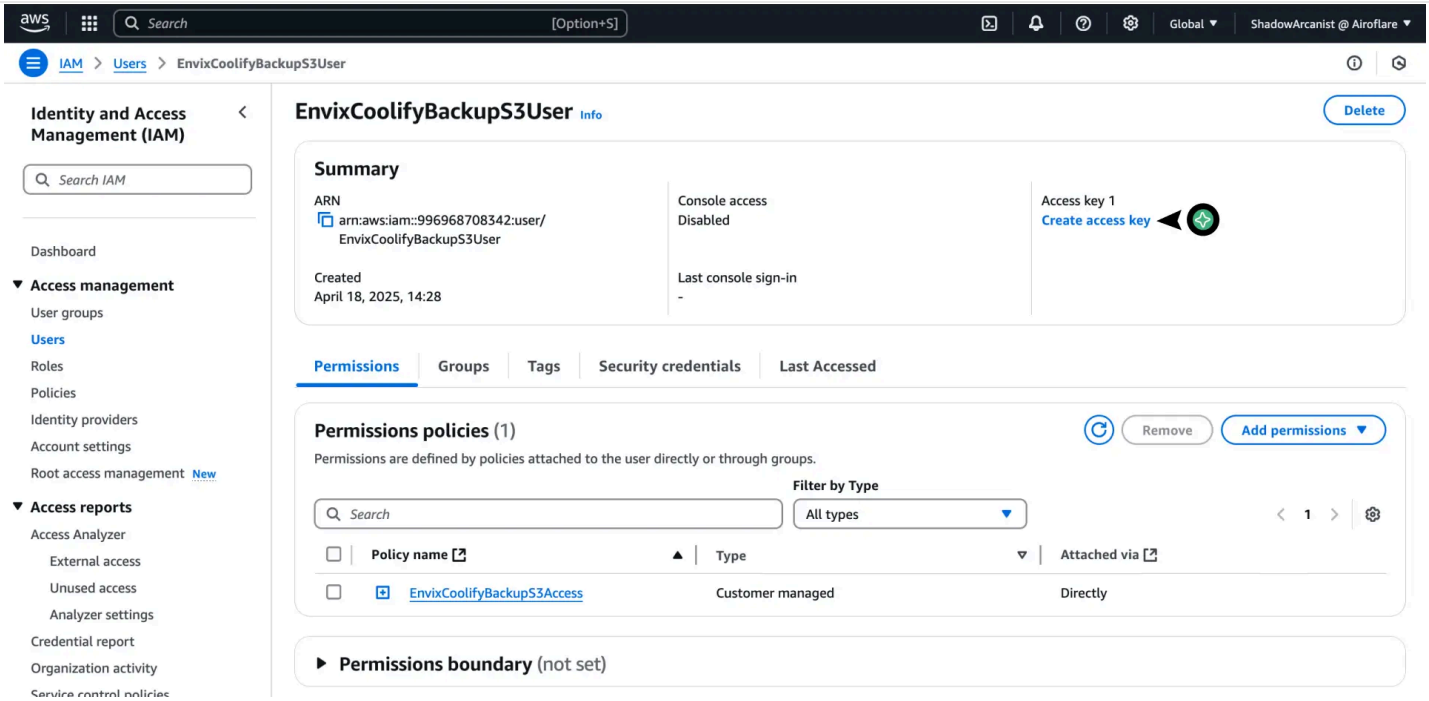


- Click on the username to create an access key.

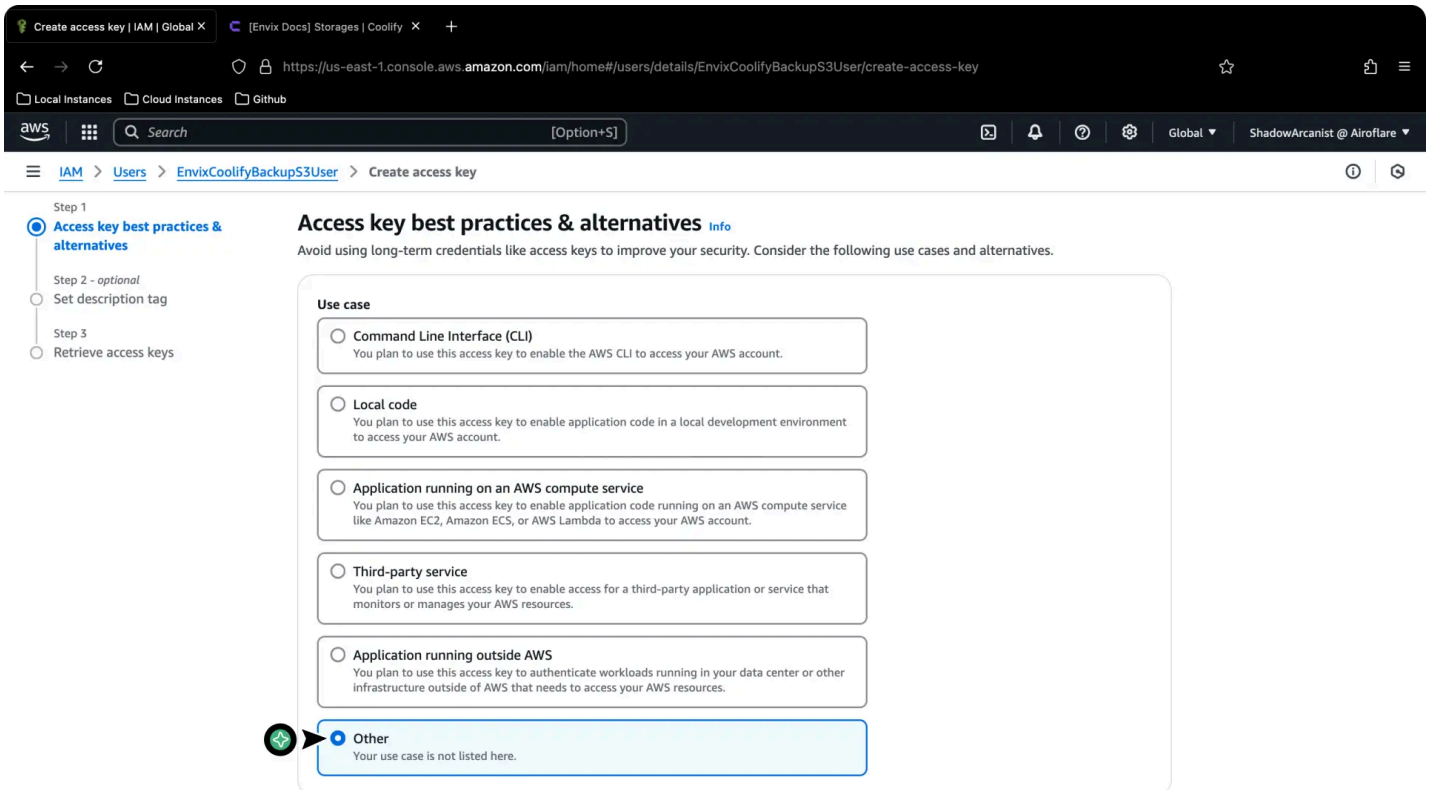
4. Create an Access Key

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

Envix

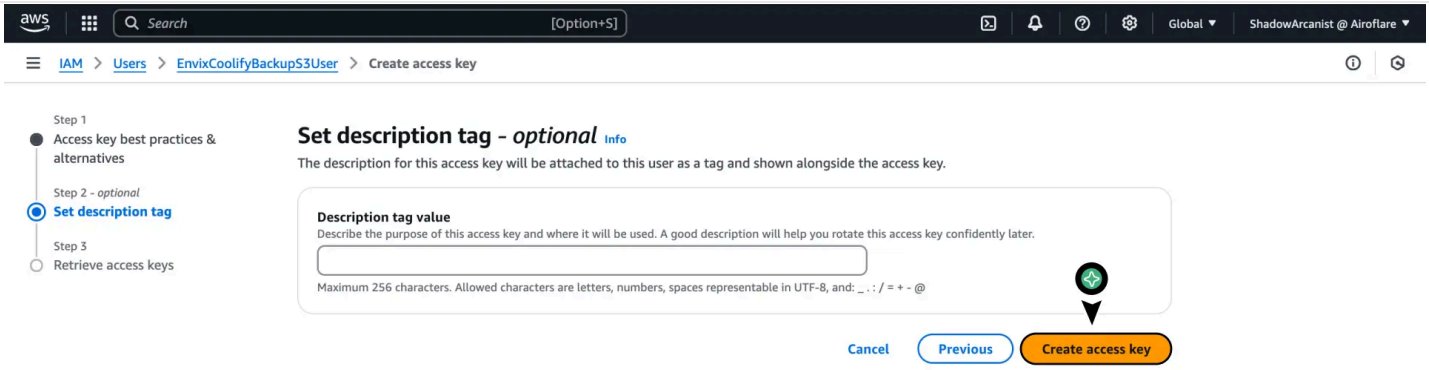


- Click on **Create access key** option to setup a new access key.

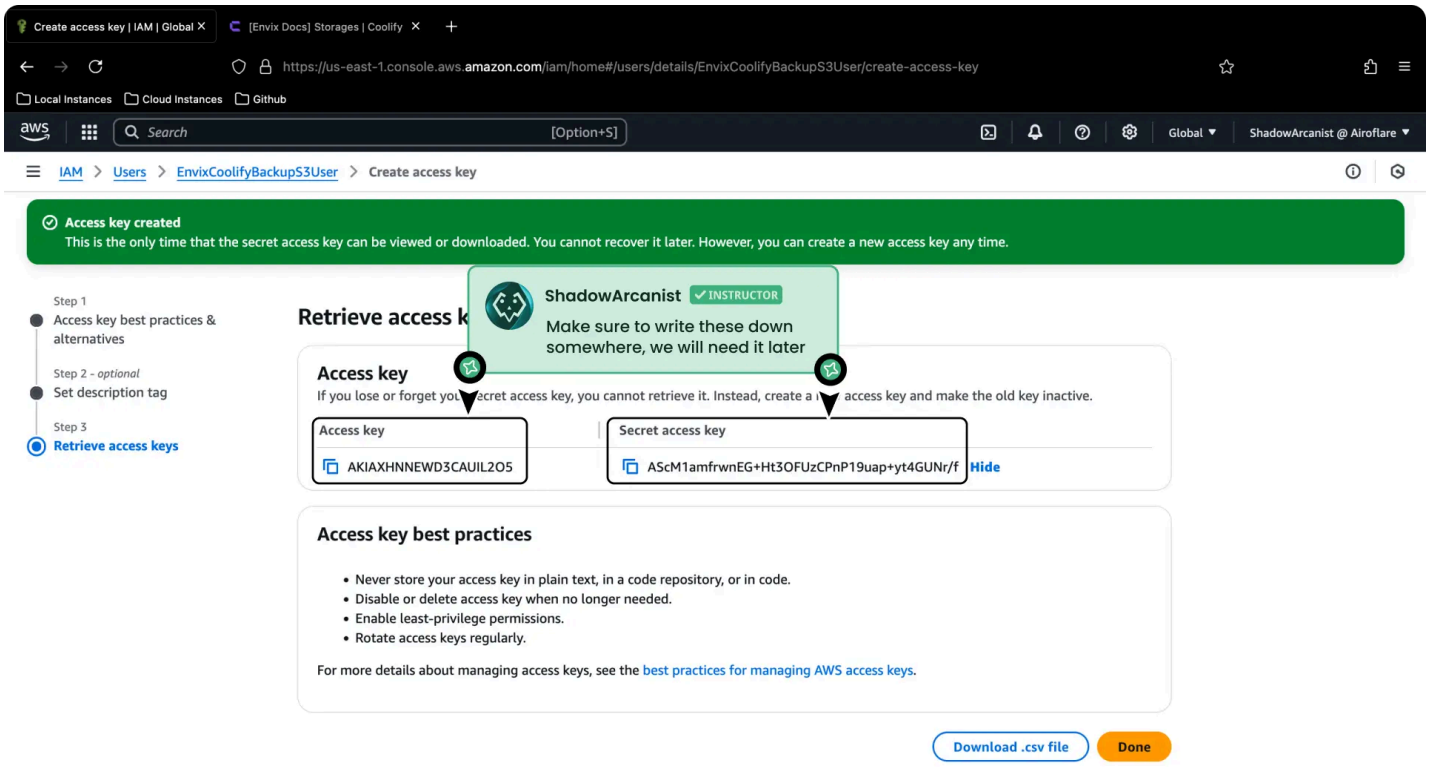


- Choose the **Other** option and click on **Continue** button

Envix



- Click on **Create access key** button.



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

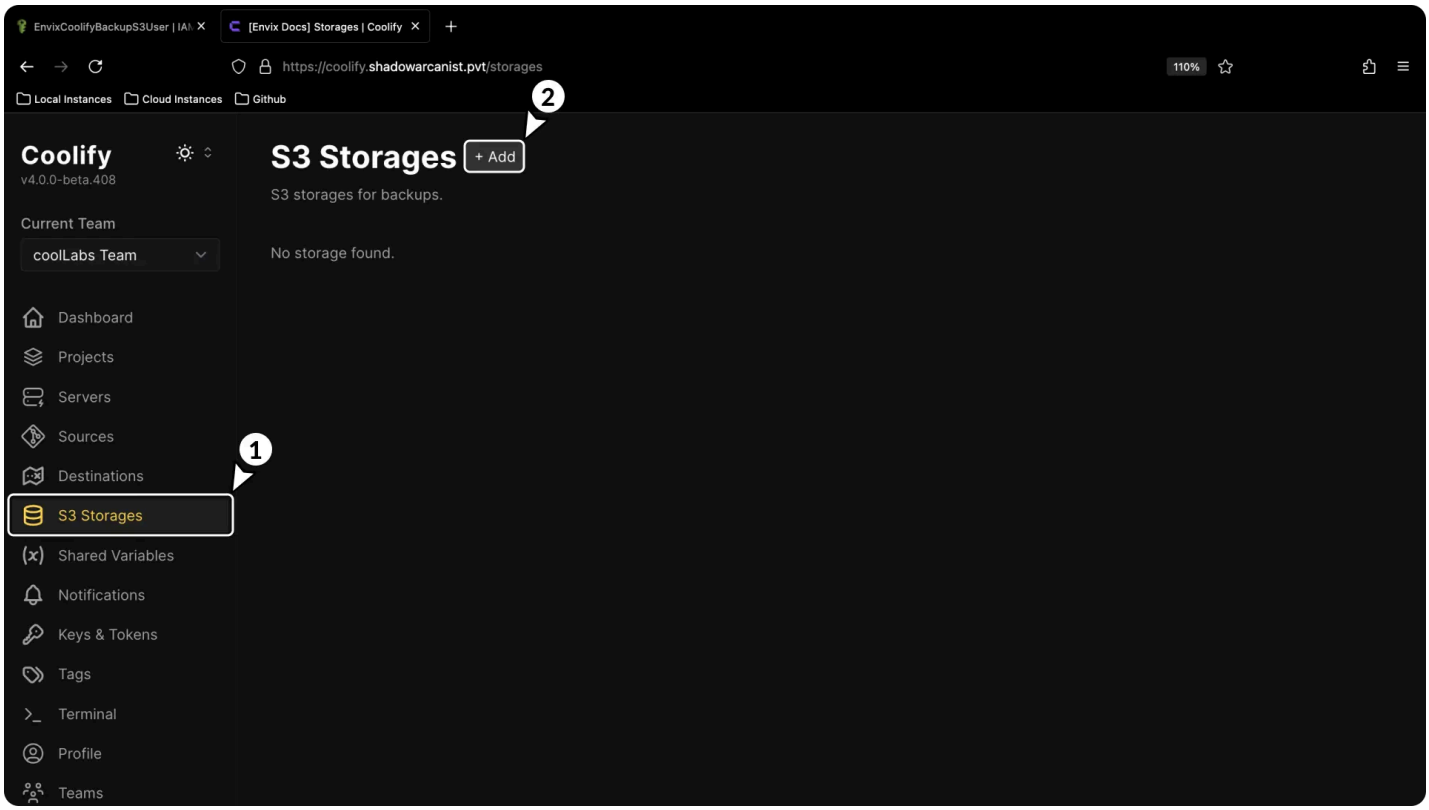
Envix

somewhere safe.

5. Setup S3 in Coolify

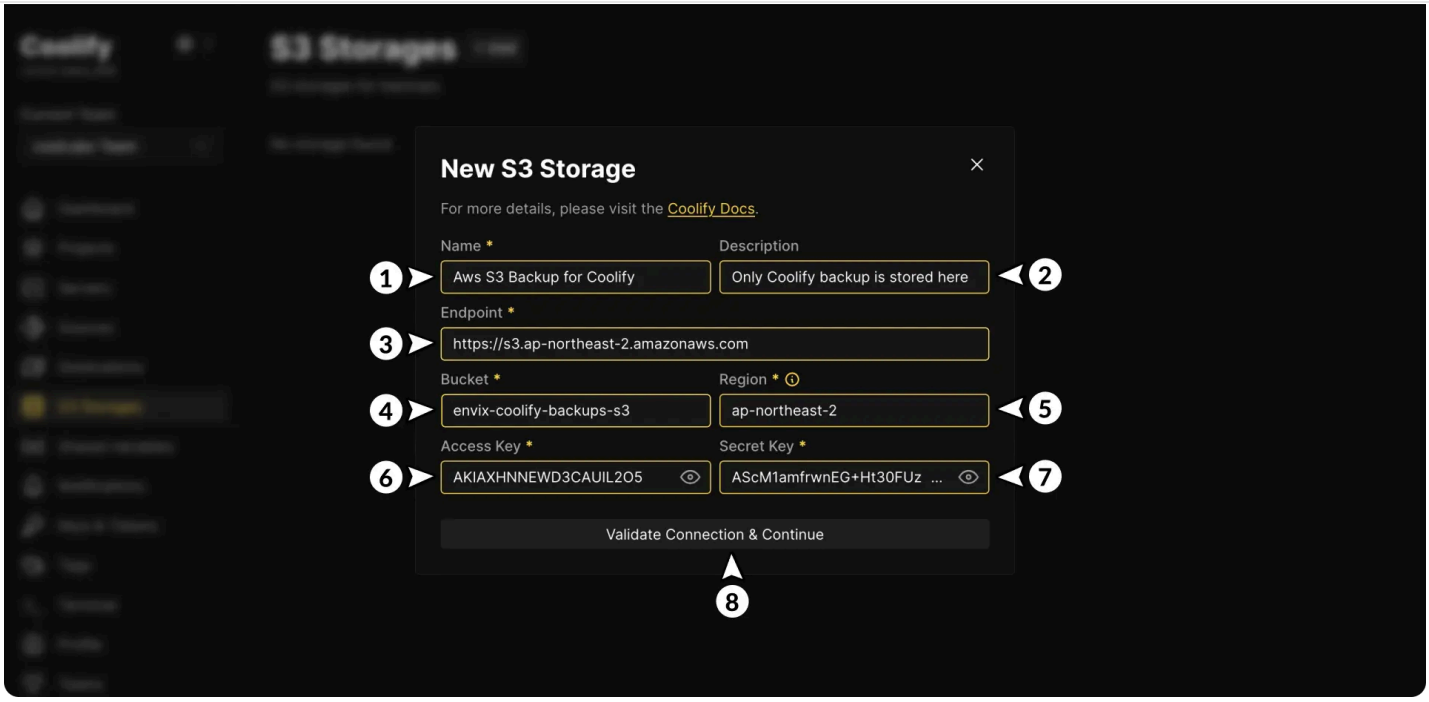
To create your setup S3 in Coolify, follow these steps:

In your Coolify dashboard:



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

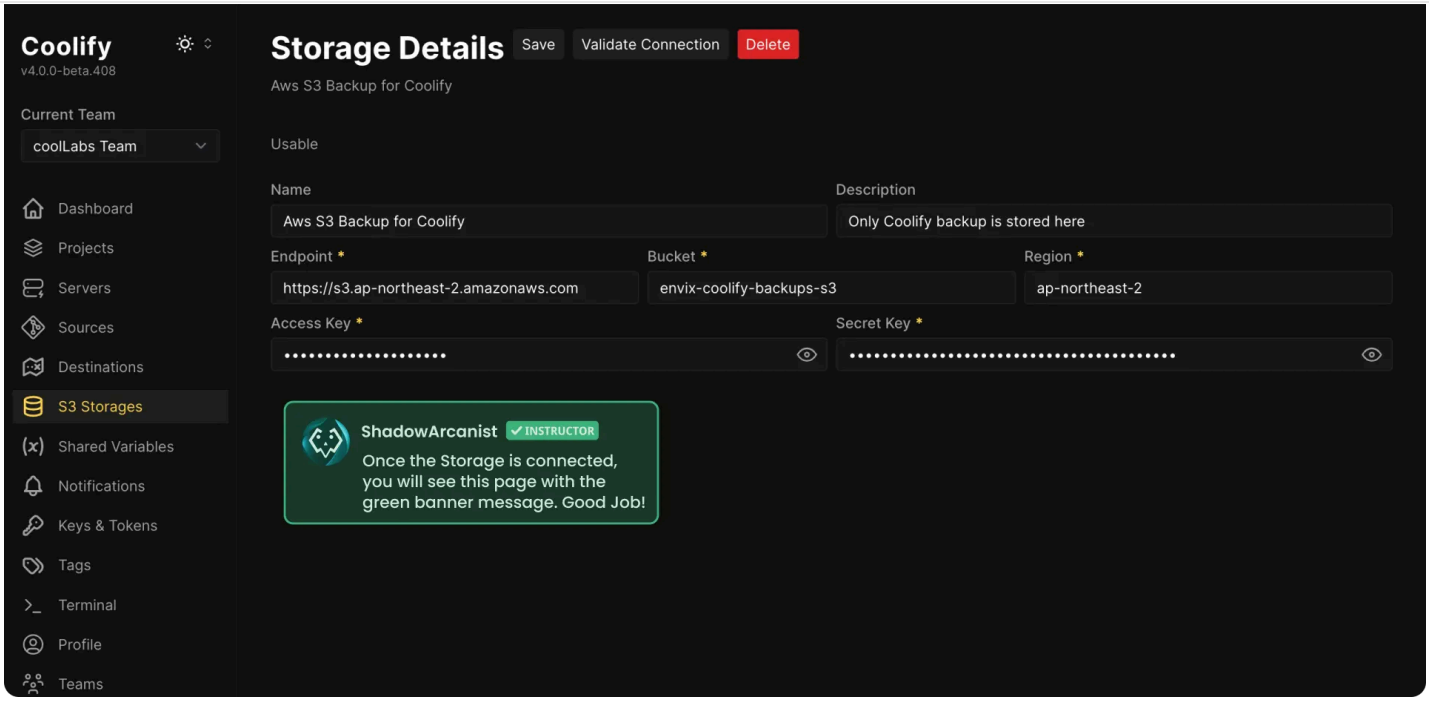
Envix



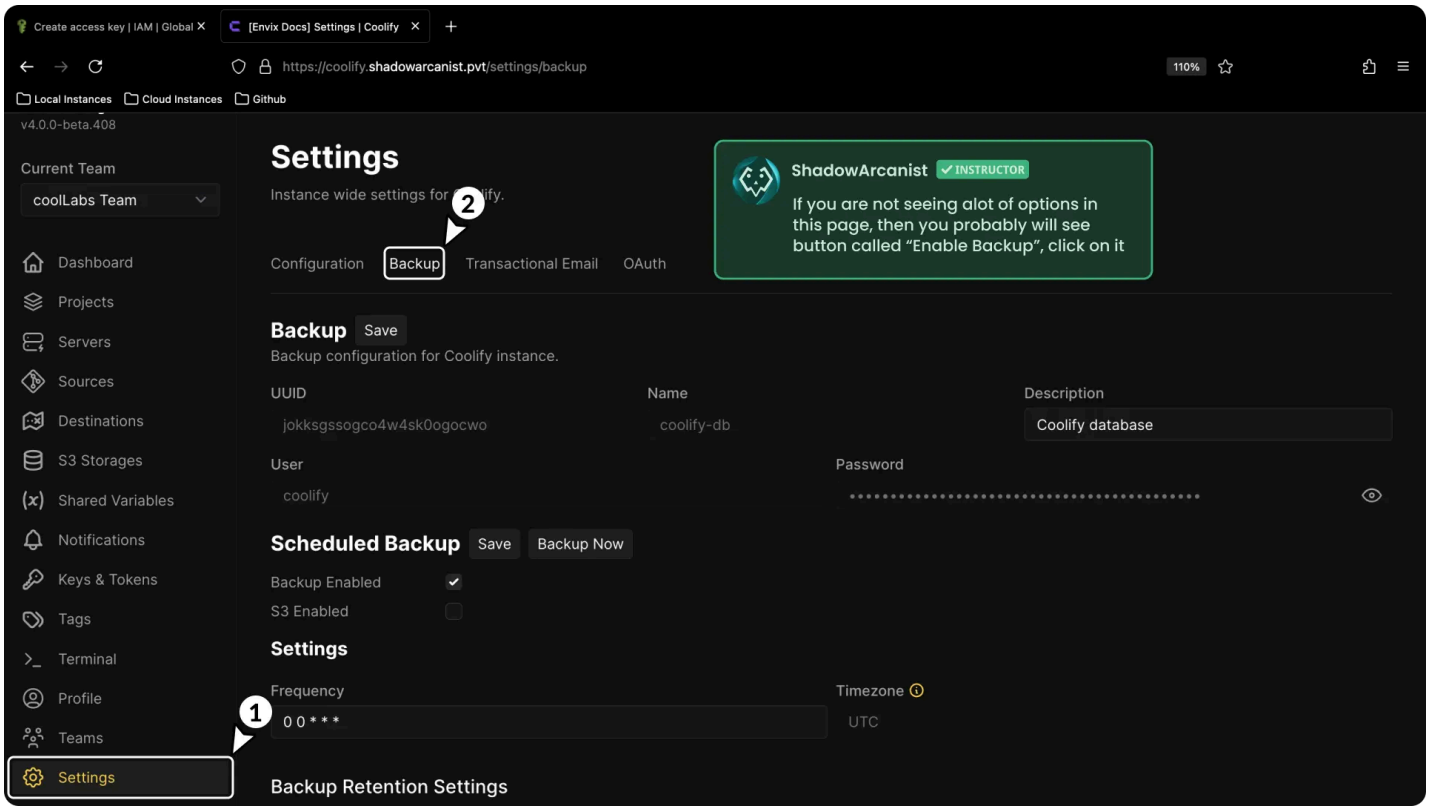
1. Give a name for the S3 storage (this can be any name)
2. Give a short description for the storage (optional)
3. Enter the endpoint without your bucket name: `https://s3.YOUR_REGION_NAME.amazonaws.com`
4. Enter the name of the S3 bucket you created.
5. Enter your S3 bucket's region
6. Enter your Access 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:

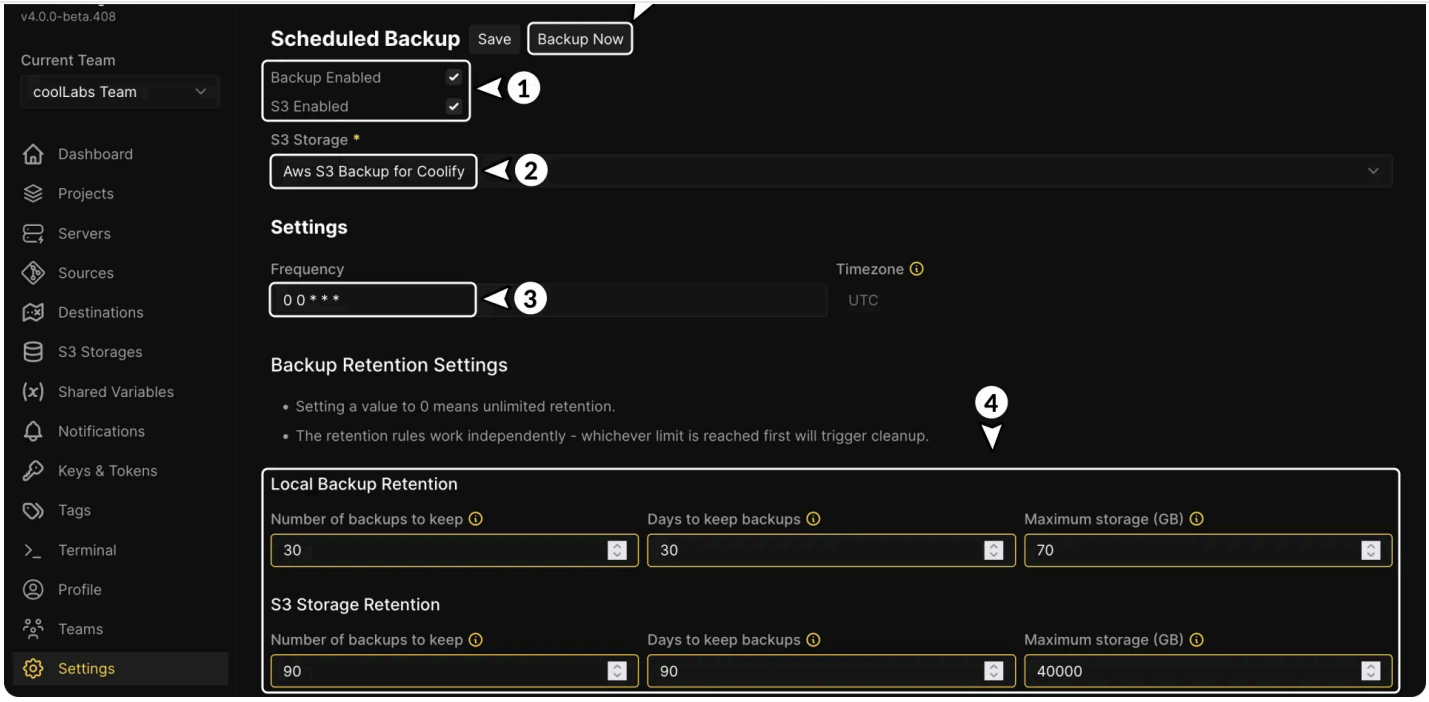
Envix



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



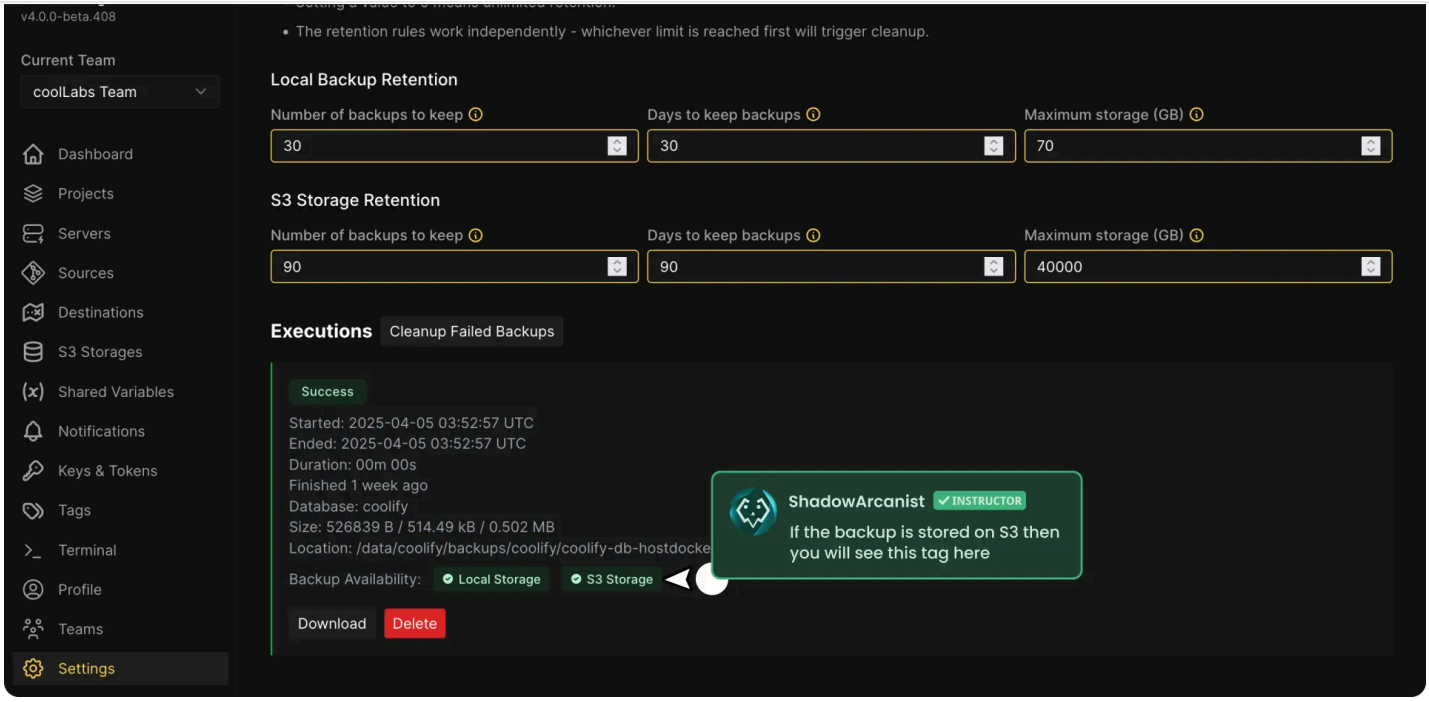
Envix



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:

Envix



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